REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE KASDI MERBAH OUARGLA

Département d'Electronique et télécommunication

Mémoire

Présenté pour obtenir

LE DIPLOME DE MASTER

FILIERE : **ELECTRONIQUE**

Spécialité : électronique des systèmes embarqués

Présenté par :

HAMANA Abdelhak

GOSSA Youcef

Stéganographie d'une images numérique

Soutenu le : …/…/ 2021

Devant Les Jury :

Mr. KORICHI Maarouf	**MCB**	Présidente	UKM , Ouargla
Mme. CHARIF Fella	MAA	Examinatrice	UKM, Ouargla
Mr. BENCHABANE Abderrazak	MCA	Encadreur	UKM, Ouargla

Année Universitaire 2020/2021

Remerciement

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

Tout d'abord, ce travail ne serait pas aussi riche et n'aurait pas puavoir le jour sans l'aide et l'encadrement de ***Mr BENCHABANE*** *on le remercie pour la qualité de son encadrement exceptionnel, pour sa patience, sa rigueur et sa disponibilité durant notre préparation de cemémoire.*

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

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

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

Dédicace

Avant toute considération, nous remercions le Grand Dieu

le tout puissant qui, nos a aidé pour
achever ce travail.

nous dédions à nos parent

qui ont consenti beaucoup de sacrifices qui nous ont toujours soutenu et

encouragé tout au long de notre vie, nous demandons à dieu la protégée et réserve-leur une longue vie.

A notre très chères sœurs et frères,

Et à tout les familles de HAMANA et GOSSA .

N'oubliions pas mes chers collègues : à tous les membres du Département Electronique .

Hamana abedhak

Gossa youcef

الملخص :مع التغيرات المستمرة في مجال تكنولوجيا المعلومات والاتصالات ،أصبح أمن الكمبيوتر قضية رئيسية للشركات وجميع المشاركين من حوله . إخفاء المعلومات هو جزء من الإجراءات الأمنية لمنع محاولات التسلل .يمكن أن تستخدم طرق متعددة لنقل البيانات مثل الصور، الصوت الفيديو .... إلخ.

في هذا العمل البحثي قمنا بإنشاء برنامج لإخفاء المعلومات كالرسائل النصية في الصور وكيفية استخراج الرسائل المخفية من الصور ،قمنا بذالك باستخدام خوارزمية (LSB (Least Significant Bit .
تم تطبيق هذه الخوارزمية على عدة صور وحققت نتائج ممتازة في استرجاع الرسائل النصية المخفية دون إحداث أي تشويه في الصور.
كلمات المفتاحية : التورية ،خوارزمية ، الصور الرقمية ،أمن المعلومات ، معالجة الصور .

résumé : Avec les évolutions permanentes du domaine des technologies de l'information et de la communication, la sécurité informatique est devenue un enjeu majeur pour l'entreprise et son entourage. La dissimulation d'informations fait partie des mesures de sécurité pour empêcher les tentatives d'intrusion. Il peut utiliser une variété de méthodes pour transmettre des données, telles que des images, de l'audio, de la vidéo... etc. Dans ce travail de recherche, nous avons créé un programme pour masquer les informations textuelles dans l'image et comment extraire les informations cachées de l'image .Nous avons utilisé l'algorithme LSB (bit le moins significatif) pour terminer ce travail. L'algorithme a été appliqué à plusieurs images et a obtenu d'excellents résultats dans la récupération d'informations textuelles cachées sans provoquer de distorsion de l'image.

Mots-clés : Stéganographie , algorithme, images numériques, sécurité de l'information, traitement d'image.

Abstract : With the continuous development of information and communication technology, IT security has become a major issue facing companies and their entourage. One of the security measures to prevent intrusion attempts is to hide information. It can use a variety of methods to transmit data, such as pictures, audio, video, etc. In this research work, we created a program to hide the text information in the image and how to extract the hidden information from the image. We use the LSB (Least Significant Bit) algorithm to complete this work. The algorithm has been applied to multiple images, and has achieved excellent results in recovering hidden text information without causing image distortion.

Keywords: Steganography, algorithm, digital images, information security, image processing

Table des matières

Liste des Figures

Liste des Tableaux

Abréviations

API : Application Programing Interface

BMP : Bitmap

dB : Décibel

DCT : Discrete Cosine Transform

DES : Data Encryption Standard

DWT : Discrete Wavelet Transform

GHz : Gigahertz

Go : Gigaoctet

HTML : Hypertext Markup Language

HTTP : Hypertext Transfer Protocol

IDC : International Data Corporation

IDE : Integrated Development Environment

JDK : Java Development Kit

JPEG : Joint Photographic Experts Group

JRE : Java Runtime Environment

JVM : Java virtual machine

Ko : Kilooctet

LSB : Least Significant Bit

Mo : Mégaoctet

MSE : Mean Square Error

OS : Operating System

PNG : Portable Network Graphics

PSNR : Peak Signal-to-Noise Ratio

RAM : Random Access Memory

RGB : Red Green Blue

RLE : Run Length Encoding

SDK : Software Development Kit

INTRODUCTION GÉNÉRALE

Introduction générale

Les images sont un support d'information très important, comme on dit : les images valent Plus que mille mots. Compte tenu de l'importance de l'image et de sa grande quantité d'informations, le monde s'intéresse de plus en plus aux images. En fait, les images ont touché de nombreux domaines de notre vie : la médecine, la météo, les télécommunications, la cartographie, la géologie, etc. Avec le développement des outils informatiques, plusieurs techniques de traitement d'images sont apparues.

Aujourd'hui, avec le développement des médias numériques et d'Internet, La communication, qui facilite le partage et la transmission de données numériques, en introduisant par conséquent, de nouvelles formes de piratage de fichiers et de nouveaux défis en matière de sécurité doivent être traités. De plus, la question de la protection des contenus multimédias numériques n'est pas une solution satisfaisante et n'est pas encore connue. Il est facile de modifier ou de copier les médias ou même de réclamer leur droit d'utiliser.

Pour réduire la duplication des œuvres multimédias et assurer la confidentialité des transmissions, des nouvelles méthodes ont été développé. Ce sont les méthodes qui cachent les informations à transmettre. La dissimulation d'informations vise à cacher des informations à quiconque en entrant un autre support, qui peut être du texte, une image, de l'audio ou de la vidéo. Les applications de la dissimulation se distinguent par leurs objectifs. En stéganographie, le but est de cacher les messages dans les médias numériques, permettant aux partenaires de communiquer de manière secrète, le média n'a aucun contact avec le message à envoyer.

La stéganographie présente trois caractéristiques principales pour caractériser son utilisation : la robustesse, la sécurité et la capacité. La robustesse garantit que les informations secrètes ne seront pas détruites et ne réduiront pas considérablement l'image. La sécurité est conçue pour garantir que les images ne seront pas affectées par les informations secrètes insérées. La quantité de définition de la capacité peut être intégrée dans les médias sans information significativement dégradée. Ces trois caractéristiques sont étroitement liées. Il existe quelques techniques pour découvrir les supports stéganographiques : c'est le cas de la stéganalyse est aussi appelée stéganalyse.

Dans notre projet, nous allons introduire une méthode de dissimulation d'informations "Stéganographie" qui cache le message (texte) dans l'image, Le but de notre projet est d'insérer un message (texte) dans une image, et La perception humaine ne peut pas détecter les petits changements introduits dans l'image destiné à contenir ce message. Pour atteindre ces objectifs, Notre mémoire est organisé autour de trois chapitres :

Chapitre 1 : en gardant la généralité du traitement d'images, nous allons introduire quelques concepts de base des images numériques.

Chapitre 2 : Ce chapitre est une introduction à la stéganographie, y compris l'histoire de la stéganographie depuis sa création, la définition des concepts utilisés en sténographie, langage et technologie, puis les éléments qui cachent les informations, et le but et les avantages de la technologie.

Chapitre 3 : Dans ce chapitre, nous avons proposé une application de la stéganographie par substitution LSB.

CHAPITRE 1

Chapitre 1

Généralités sur les images numériques

1.1. Introduction

L'image constitue l'un des moyens les plus importants qu'utilise l'homme pour communiquer. C'est un moyen de communication universel dont la richesse du contenu permet aux êtres humains de tout âge et de toute culture de se comprendre.

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.

De ce fait, le traitement d'images est l'ensemble des méthodes et techniques opérant sur celles-ci, dans le but d'améliorer l'aspect visuel de l'image et d'en extraire des informations jugées pertinentes.

1.2. Définition d'une image

L'image est une représentation d'une personne ou d'un objet par la peinture, la sculpture, le dessin, la photographie, le film, etc. C'est aussi un ensemble structuré d'informations qui, après affichage sur l'écran, ont unesignification pour l'œil humain. Elle peut être décrite sous la forme d'une fonction I(x, y) de brillance analogique continue,définie dans un domaine borné, Les eléments x et y sont les coordonnées spatiales d'un point de l'image et I est une fonction d'intensité lumineuse et de couleur. Sous cet aspect, l'image est inexploitable par la machine, ce qui nécessite sa numérisation [2].

1.3. Image numérique

Contrairement aux images obtenues à l'aide d'un appareil photo, ou dessinées sur du papier, les images manipulées par un ordinateur sont numériques (représentées par une série de bits). L'image numérique est l'image dont la surface est divisée en éléments de tailles fixes appelés cellules ou pixels, ayant chacun comme caractéristique un niveau de gris ou de couleurs prélevé à l'emplacement correspondant dans l'image réelle, ou calculé à partir d'une description interne de la scène à représenter [2].

La numérisation d'une image est la conversion de celle-ci de son état analogique en une image numérique représentée par une matrice bidimensionnelle de valeurs numériques $f(x, y)$ où :

- x, y : coordonnées cartésiennes d'un point de l'image.

- $F(x, y)$: niveau de gris en ce point

Pour des raisons de commodité de représentation pour l'affichage et l'adressage, les données images sont généralement rangées sous formes de tableau de n lignes et p colonnes. Chaque élément $I(x, y)$ représente un pixel de l'image et à sa valeur est associé un niveau de gris codé sur m bits (2^m niveaux de gris ; 0 = noir ; 2^m-1 = blanc). La valeur en chaque point exprime la mesure d'intensité lumineuse perçue par le capteur [3].

1.4. Caractéristique d'une image numérique

L'image est un ensemble structuré d'informations caractérisé par les paramètres suivants:

1.4.1 Pixel

Contraction de l'expression anglaise " Picture Eléments ": éléments d'image, le pixel estle plus petit point de l'image, c'est une entité calculable qui peut recevoir une structure etune quantification. Si le bit est la plus petite unité d'information que peut traiter un ordinateur, le pixel est le plus petit élément que peuvent manipuler les matériels et logiciels d'affichage ou d'impression. La lettre A, par exemple, peut être affichée commeun groupe de pixels dans la figure ci-dessous :

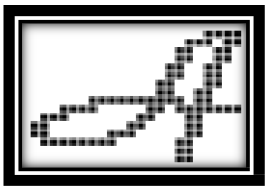

Figure 1.1 Groupe de pixel

La quantité d'information que véhicule chaque pixel donne des nuances entre images monochromes et images couleurs. Dans le cas d'une image monochrome, chaque pixel est codé sur un octet, et la taille mémoire nécessaire pour afficher une telle image est directement liée à la taille de l'image.

Dans une image couleur (R.V.B.), un pixel peut être représenté sur trois octets : un octet pour chacune des couleurs : rouge (R), vert (V) et bleu (B) [4].

1.4.2 Dimension

C'est la taille de l'image. Cette dernière se présente sous forme de matrice dont les éléments sont des valeurs numériques représentatives des intensités lumineuses (pixels). Le nombre de lignes de cette matrice multiplié par le nombre de colonnes nous donne le nombre total de pixels dans une image [5].

1.4.3 Résolution

La résolution est définie par un nombre de pixels par unité de longueur de l'image à numériser en dpi (dots per inch) ou ppp (points par pouce). On parle de définition pour un écran et de résolution pour une image. Plus le nombre de pixels est élevé par unité de longueur de l'image à numériser, plus la quantité d'information qui décrit l'image est importante et plus la résolution est élevée (etplus le poids de l'image est élevé) [6].

La résolution d'une image correspond au niveau de détail qui va être représenté sur cette image. Pour la numérisation il faut considérer les 2 équations suivantes :

- (X*résolution) = x pixels
- (Y*résolution) = y pixels

Où X et Y représentent la taille (pouce ou cm, un pouce=2,54 centimètres) de la structure à numériser, où résolution représente la résolution de numérisation, et où x et y représentent la taille (en pixels) de l'image [7].

Figure 1.2: Résolution D'image

1.4.4 La taille d'une image

Pour connaître la taille d'une image, il est nécessaire de compter le nombre de pixels quecontient l'image, cela revient à calculer le nombre des cases du tableau, soit la hauteur decelui-ci que multiplie sa largeur. La taille de l'image est alors le nombre des pixels que multiplie la taille (en octet) de chacun de ces éléments.

Exemple : pour une image de 240 X 420 en True Color :

- Le nombre de pixels : 240 X 420 = 100800
- La taille de chaque pixel : 24 bits / 8 = 3 octets
- Le poids de l'image est égal à : 100800 X 3 = 302.400 égal 302.400/1024 = 295Ko

1.4.5 Bruit

Un bruit (parasite) dans une image est considéré comme un phénomène de brusque variation de l'intensité d'un pixel par rapport à ses voisins, il provient de l'éclairage des

dispositifs optiques et électroniques du capteur [8].

1.4.6 Histogramme

L'histogramme des niveaux de gris ou des couleurs d'une image est une fonction qui donne la fréquence d'apparition de chaque niveau de gris (couleur) dans l'image. Pour diminuer l'erreur de quantification, pour comparer deux images obtenues sous des éclairages différents, ou encore pour mesurer certaines propriétés sur une image, on modifie souvent l'histogramme correspondant Il permet de donner un grand nombre d'information sur la distribution des niveaux de gris (couleur) et de voir entre quelles bornes est repartie la majorité des niveaux de gris (couleur) dans les cas d'une image trop claire ou d'une image trop foncée.

Il peut être utilisé pour améliorer [11] la qualité d'une image (Rehaussement d'image) enintroduisant quelques modifications, pour pouvoir extraire les informations utiles de celle-ci.

1.4.7 Contours et textures

Les contours représentent la frontière entre les objets de l'image, ou la limite entre deux pixels dont les niveaux de gris représentent une différence significative. Les textures décrivent la structure de ceux-ci. L'extraction de contour consiste à identifier dans l'image les points qui séparent deux textures différentes [12].

1.4.8 Luminance

C'est le degré de luminosité des points de l'image. Elle est définie aussi comme étant le quotient de l'intensité lumineuse d'une surface par l'aire apparente de cette surface, pour un observateur lointain, le mot luminance est substitué au mot brillance, qui correspond à l'éclat d'un objet. Une bonne luminance se caractérise par :

- **Des images lumineuses (brillantes).**
- **Un bon contraste** :

Il faut éviter les images où la gamme de contraste tend vers le blanc ou le noir; ces imagesentraînent des pertes de détails dans les zones sombres ou lumineuses.

- **L'absence de parasites**.

1.4.9 Contraste

C'est l'opposition marquée entre deux régions d'une image, plus précisément entre les régions sombres et les régions claires de cette image. Le contraste est défini en fonction des luminances de deux zones d'images.

Si L1 et L2 sont les degrés de luminosité respectivement de deux zones voisines A1 et A2

d'une image, le contraste C est défini par le rapport :

$$C = \frac{L_1 - L_2}{L_1 + L_2}$$

1.4.10 Images à niveaux de gris

Le niveau de gris est la valeur de l'intensité lumineuse en un point. La couleur du pixel peut prendre des valeurs allant du noir au blanc en passant par un nombre fini de niveaux intermédiaires. Donc pour représenter les images à niveaux de gris, on peut attribuer à chaque pixel de l'image une valeur correspondant à la quantité de lumière renvoyée. Cettevaleur peut être comprise par exemple entre 0 et 255. Chaque pixel n'est donc plus représenté par un bit, mais par un octet. Pour cela, il faut que le matériel utilisé pour afficher l'image soit capable de produire les différents niveaux de gris correspondant.

Le nombre de niveaux de gris dépend du nombre de bits utilisés pour décrire la" couleur " de chaque pixel de l'image. Plus ce nombre est important, plus les niveaux possibles sont nombreux.

1.4.11 Images en couleurs

Même s'il est parfois utile de pouvoir représenter des images en noir et blanc, les applications multimédias utilisent le plus souvent des images en couleurs. La représentation des couleurs s'effectue de la même manière que les images monochromes avec cependant quelques particularités. En effet, il faut tout d'abord choisir un modèle de représentation. On peut représenter les couleurs à l'aide de leurs composantes primaires. Les systèmes émettant de la lumière (écrans d'ordinateurs,...) sont basés sur le principe de la synthèse additive :

Les couleurs sont composées d'un mélange de rouge, vert et bleu (modèle R.V.B.) [5].

- **La représentation en couleurs réelles**

Elle consiste à utiliser 24 bits pour chaque point de l'image. Huit bits sont employés pourdécrire la composante rouge (R), huit pour le vert (V) et huit pour le bleu (B). Il est ainsipossible de représenter environ 16,7 millions de couleurs différentes simultanément. Celaest cependant théorique, car aucun écran n'est capable d'afficher 16 millions de points. Dans la plus haute résolution (1600 x 1200), l'écran n'affiche que 1 920 000 points. Par ailleurs, l'œil humain n'est pas capable de distinguer autant de couleurs.

- **La représentation en couleurs indexées**

Afin de diminuer la charge de travail nécessaire pour manipuler des images en 24 bits, onpeut utiliser le mode de représentation en couleurs indexée. Le principe consiste à

déterminer le nombre de couleurs différentes utilisées dans l'image, puis à créer une table de ces couleurs en attribuant à chacune une valeur numérique correspondant à sa position dans la table. La table, appelée palette, comporte également la description de chacune des couleurs, sur 24 bits.

- **Autres modèles de représentation**

Le modèle R.V.B. représentant toutes les couleurs par l'addition de trois composantes fondamentales, n'est pas le seul possible. Il en existe de nombreux autres. L'un d'eux est particulièrement important. Il consiste à séparer les informations de couleurs (chrominance) et les informations d'intensité lumineuse (luminance). Il s'agit du principe employé pour les enregistrements vidéo. La chrominance est représentée par deux valeurs (selon des modèles divers) et la luminance par une valeur.

1.5. Qualité de l'image numérique

Elle dépend, d'une part, de la qualité des images d'origine et, d'autre part, des moyens misen œuvre pour convertir un signal analogique en signal numérique. Elle dépend aussi de :

La qualité des périphériques de numérisation de l'image, du nombre de niveaux de gris ou de couleurs enregistrées, etc. La qualité de l'affichage à l'écran : définition de l'écran, nombre de teintes disponibles simultanément, calibrage de l'écran, etc.

Les critères d'appréciation de la qualité d'une image, tels que cités succinctement ci-dessus, dépendent largement de la structure même de l'image réaliste ou conceptuelle et de son mode de représentation (bitmap ou vectorielle).

1.6. Différents types d'image numérique

Les images numériques sont classés selon le format hors la multitude des formats vient de la volonté de chacun des fabricants de logiciel d'imposer le sien car on trouve très peude différences hormis quelques-uns sont compressés [13] et les autres ne le sont pas maisaussi ce qui change, ce sont les en-têtes du fichier.

1.6.1 Les formats vectoriels

Les formats vectoriels sont en fait une suite d'objets géométriques (rond, carré, droite, image clipart) défini par leurs coordonnées polaires. Le format les plus connus sont : DXF(Autocad) ; SYLK ; Lotus PIC et Lotus DDIF ; cependant, départ le fait qu'ils soient vectoriels ces formats supportent les images de type de photo. Ainsi hormis dans le secteur

du dessin industriel avec le logiciel Autocad, les images vectorielles sont peu utilisées, au profit des métas fichiers [10].

Les avantages

Les fichiers vectoriels sont adaptés au stockage d'images de forme géométrique (cercle, carré, droit...) ou qui peuvent facilement être transformé en forme géométrique comme texte et certains formats sophistiqués s'intègrent des objets en 3 dimensions. Les objets vectoriels peuvent aisément dimensionner pour l'interface de sortie.

La plupart des formats sont en ASCII ce qui se permet de les modifier directement avec un simple éditeur de texte. Il est généralement facile d'effectuer un rendu d'un fichier vectoriel puis de le convertir en bitmap. La qualité restée est la bonne dans ce cas.

Les inconvénients

Les fichiers vectoriels peuvent difficilement stocker les images complexes comme de photographie ou la couleur peut varier d'un point à l'autre.

L'apparence d'une image vectoriel peut énormément varier en fonction du logiciel qui l'interprète cela dépend en fait des algorithmes utilisés pour l'affichage. La reconstitution d'une image à partir des vecteurs peut prendre beaucoup de temps qu'une image bitmap de complexité égal.

1.6.2 Les formats méta fichiers

Les métas fichiers sont très vite repandus. Ils offrent la possibilité d'intégrer à la fois des images bitmap et des objets vectoriels. Les formats les plus connus sont : EPS Mackintosh ; PICT RIF et WMF. Les métas fichiers ont les facilités de les porter d'une plateforme à une autre. Les données étant stockées la plupart de temps, en ASCII, les problèmes d'ordre de bit n'apparaissent pas. L'ASCCII offre aussi une plus grande aptitude à la compression des fichiers.

Les avantages

Les métas fichiers ont des avantages des fichiers bitmap et des fichiers vectoriels. La plupart des formats sont binaires quelques-uns sont orientés, le partage d'un ordinateurà un autre se fait généralement sans encombre. Les métas fichiers peuvent généralement être compressés avec un gain important.

Les inconvénients

Avec un nouveau format il y a risque de créer de nombreux problèmes lors d'échange dedonnées avec d'autres logiciels.

L'exemple d'une image en méta fichier en format WMF. Le format WMF est un méta format en effet, il est utilisé pour stocker des images vectorielles, des images bitmap sur disque ou en mémoire afin de les utiliser ultérieurement sans Windows.

Un fichier contient une suite d'objet chacun décrit par un en-tête. Le format WMF peut contenir 65535 objets au maximum. Le type possible pour chaque objet (cercle, carré, bitmap..) est défini dans la librairie Windows

1.6.3 Les formats bitmap:

Les images bitmap sont des images où les données sont représentées par un tableau à deux dimensions (où "matrice") de pixels (points de couleur). L'écran fournit une représentation visuelle de l'image en la balayant de gauche à droite (largeur de l'image : axe des abscisses) et de haut en bas (hauteur de l'image : axe des ordonnées).

BMP : format de Windows et d'OS/2 pour les PC sous Dos et Windows. Sa structure étant élémentaire, on peut choisir un codage de 1 à 24 bits par pixel[21(*)], soitdu noir et blanc aux 16 millions de couleurs et, dans certains cas, appliquer une compression sans pertes RLE.

FPX (Flashpix) : développé par Kodak, Hewlett-Packard, Live Picture et Microsoft. L'idée est d'obtenir avec un format Bitmap des possibilités de zoom comparables aux formats vectoriels. Le fichier est en fait plusieurs mêmes images avec des résolutions différentes. Dans les démos proposées par Live Picture, on charge d'abord une image à faible résolution, et en cliquant sur n'importe quelle zone, on zoome, c'est-à-dire que le navigateur va chercher un morceau de la même image à plus haute résolution, et ainsi desuite. Pour utiliser ce format sur le Web, il faut télécharger un plug-in chez Live Picture.Ce format peut être compressé en JPEG mais il reste plus lourd que le JPEG seul.

Pour l'instant son usage est peu répandu et on a bien du mal à faire fonctionner le plug-inà partir d'une image issue de PSP.

GIF (Graphiclnterchange Format) : développé par CompuServe. Ce format très courant sur le Web permet une très bonne compression non destructrice basé sur l'algorithme

LZW. On trouve actuellement deux formats (chez PSP par exemple), le GIF 87A, vieux, et le GIF 89A qui a permis les GIF Animés, en fait une suite d'images GIF à la durée d'affichage variables. GIF gère la transparence, on le voit ici.

JPG (JPEG) Joint Photographic Expert Group. C'est un format donnant de bons résultats pour la photographie, mais qui utilise une compression destructrice sur 8 bits en niveaux de gris ou 24 bits en couleurs. Il existe un format progressif optimisé [9].

PCD (Photo CD) créé par Kodak, Tout comme FlashPix, du même Kodak, il code l'image sous plusieurs définitions. On ne le voit guère.

PCX (Picturee Xchange) le format défini par PC Paintbrush de Zsof que tout le monde a sûrement déjà manipulé. Il accepte les modes de couleur RVB, indexées, niveaux de griset N&B. De plus il veut bien qu'on le compresse PCX prend en charge le mode de compression RLE.

PNG (Portable Network Graphic). Il se veut le remplaçant de GIF sur lequel certains veulent mettre un copyright. Il utilise comme GIF la compression LZW. Mieux que GIF ou net, il gère les images 24 bits, comme le Jpeg ou net, mais garde la transparence plus l'entrelacement (affichage progressif), ne lui manque plus que l'animation. De plus, il commence à être reconnu par de nombreux programmes, dont mon IE 5.0 et mon PSP (quand même !)

PSD (Photoshop Document) le format de Photoshop. Il gère tous les types d'images du N&B au CMJN, même le multicouche et d'autres trucs d'enfer !

PSP : le format de Paint Shop Pro. Equivalent de PSD.

TIF (Tagged Image File Format) le format basique, récupérable partout même sur Mac (quoique le passage de PC à Mac ne soit pas toujours évident). C'est souvent le format par défaut donc récupéré à la sortie d'un scanner. Pour ceux qui veulent tout compresser, on peut utiliser la LZW.

Tableau 1.1 : tableau comparatif

	Type (matriciel/ vectoriel)	Compression des données	Nombre de couleurs supportées	Affichage progressif	Animation	Transparence
JPEG	matriciel	Oui, réglable (avec perte)	16 millions	Oui	Non	Non
JPEG2000	matriciel	Oui, avec ou sans perte	4 milliards	Oui	Oui	Oui
GIF	matriciel	Oui, Sans perte	256 maxi (palette)	Oui	Oui	Oui
PNG	matriciel	Oui, sans perte	Palettisé (256 couleurs ou moins) ou 16 millions	Oui	Non	Oui (couche Alpha)
TIFF	matriciel	Compression ou pas avec ou sans pertes	de monochrome à 16 millions	Non	Non	Oui (couche Alpha)
SVG	vectoriel	compression possible	16 millions	* ne s'applique pas *	Oui	Oui (par nature)

1.7 Conclusion

Dans ce chapitre, on a essayé de présenter quelques notions de bases liées au domaine de l'image numérique et de son traitement, en donnant quelques définitions élémentaires portant sur ce sujet, et qui seront sûrement des points essentiels dans la suite de notre travail.

CHAPITRE 2

Chapitre 2

La Stéganographie

2.1 Introduction

Dans les temps anciens, les ancêtres voulant se communiquer leurs secrets, ils ont cherché tous les moyens possibles pour cacher ces messages avant de les envoyer dans la clandestinité aux autres. Mais cela a eu des temps à autres des problèmes sur les expéditeurs même des messages, car leurs secrets étaient découverts et mis au porté de tous et surtout celle de leurs ennemis. Ils ont cherché à cacher les messages dans des objets afin de les faire passe pour authentiques bien que comportant un secret.

Beaucoup d'astuces ont été utilisés pour cacher la messagerie contre une classe bien définie de personnes.

2.2 Définition de la Stéganographie

La Stéganographie (un mot qui vient du grec steganos, couvert et graphein, écriture) [*] c'est l'art de cacher un message au sein d'un autre message de caractère anodin, de sorte que l'existence même du secret en soit dissimulée. Alors qu'avec la cryptographie habituelle, la sécurité repose sur le fait que le message ne sera pas compris. Avec la stéganographie, la sécurité repose sur le fait que le message ne serapas sans doute pas détecté. En effet, La majeure partie des fichiers informatiques (images, sons, texte, disquettes) contiennent des zones de données non utilisées ou insignifiantes. La stéganographie informatique consistera à les remplace par des informations [*].

2.3 Historique d'utilisation la stéganographie

La stéganographie est un art exploité et connu depuis l'Antiquité. Il y eut diverse technique de cryptage reposant surdes principes méconnus des espions. Vous trouvez ci-dessous quelques dates et utilisations de cette discipline.

Hérodote relate le fait : qu'Histiée rasa la tête d'un esclave afin d'y tatouer un message et attendit la repousse des cheveux, rendant ainsi le message invisible. Au fils du temps, la stéganographie a été très souvent employée et s'est ouverte à un grand nombre de formes. Une représentation chronologique, illustrée à la figure 2.1, retrace certains de ses utilisations dans l'histoire. Certaines d'entre-elle seront détaillée par la suite [*].

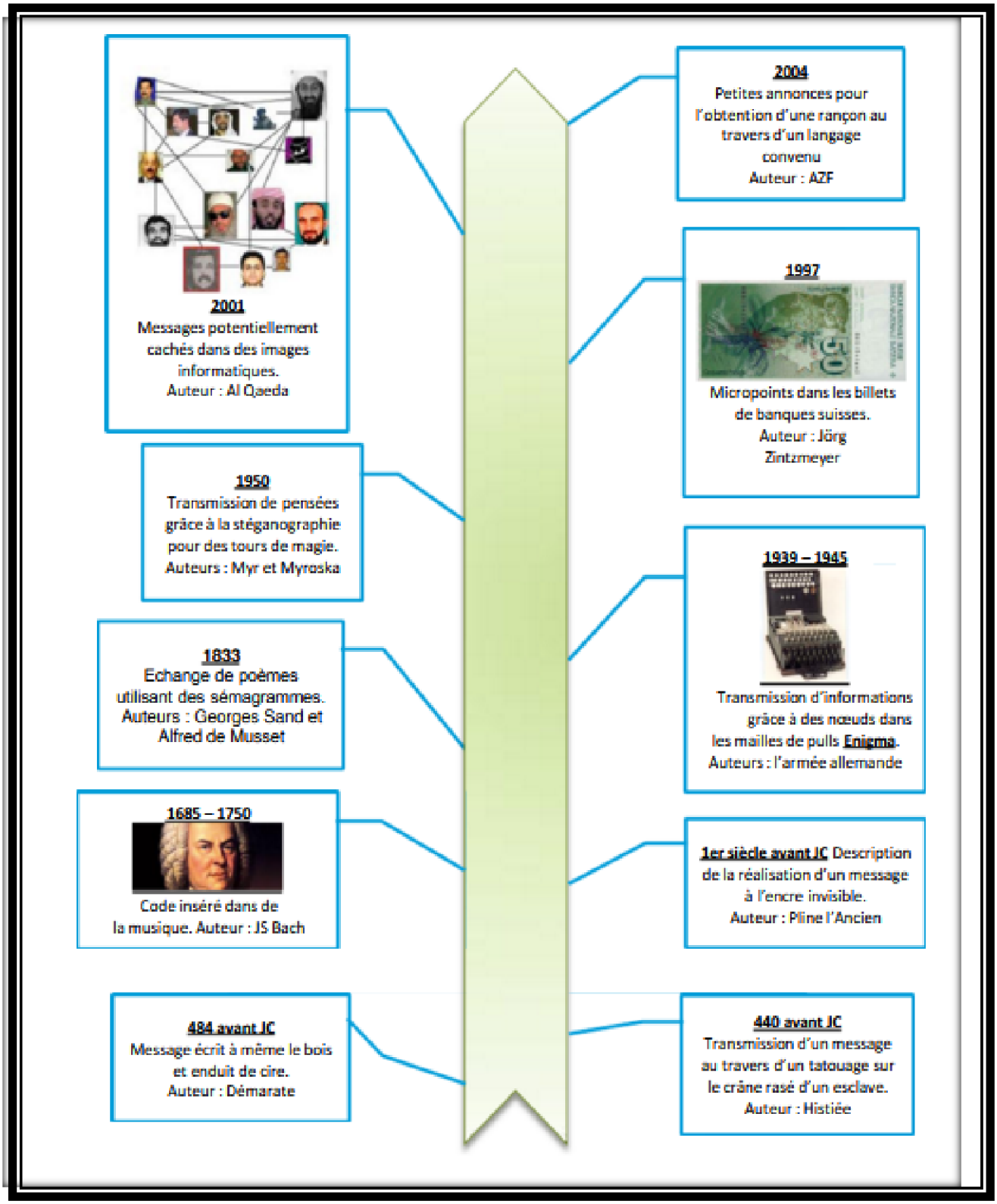

Figure 2.1 Historique de la stéganographie

2.4 Architecteur de la stéganographie

Dans une architecture stéganographie que, il y a principalement deux éléments' un côtéun processus de dissimulation, de l'autre un processus de recouvrement. Un processus de dissimulation simplifiée peut être donné par le schéma de la figure 2.2 :

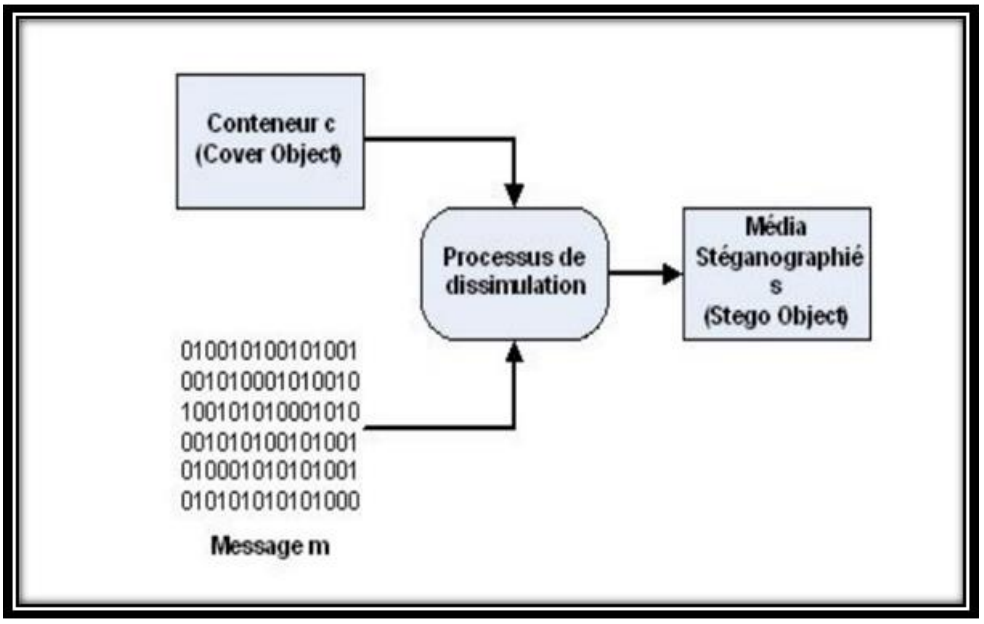

Figure 2.2 processus de la stéganographie

Il existe trois types de protocoles de stéganographie, correspondant de près à ce qui existe en cryptographie. La stéganographie pure est un système dans lequel le secret de dissimulation des données ne réside que dans l'algorithme utilisé à cet effet. La découverte de cet algorithme rompt la dissimulation de la communication. Ceci revient à mettre en place de la "sécurité par l'obscurité".

La stéganographie à clé secrète est similaire à la cryptographie symétrique, l'échange de données confidentielles nécessite, au préalable, l'échange d'une clé secrète que l'on ne partagera qu'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 nesoit pas compromise. Cette clé aura une influence sur la manière de "cacher" l'information.

La stéganographie à clé public, quant à elle, est similaire à la cryptographie asymétrique. La personne voulant envoyer des données à un autre interlocuteur, sans éveiller de soupçons, utilisera la clé pub li c de ce dernier. La clé publique étant à priori connue de tout le monde, il n'y aura pas besoin d'échange préalable "sécurisé".

La personne recevant ce message sera la seul à pouvoir en extraire son contenu à l'aide des a clé privée. Voici un schéma plus complet du processus stéganographique :

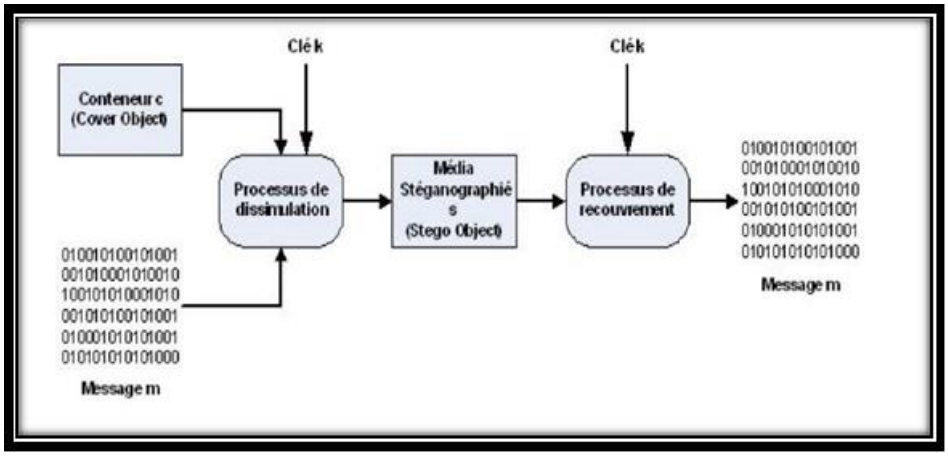

Figure 2.3 schéma complet du processus de la stéganographie

2.5 Caractéristique de la stéganographie

Trois critères permettent de classer les algorithmes stéganographique : La capacité, latransparence et la robustesse. La capacité correspond à la masse de données qui peut être insérée dans un conteneur,relativement à la taille de celui-ci. La transparence permet de quantifier le bruit généré par le processus de dissimulation,et par la même l'invisibilité de notre message. La robustesse spécifie la capacité qu'à notre message stéganographié de rester intacte après que le conteneur ait subit des modifications (filtrage, etc.. .).

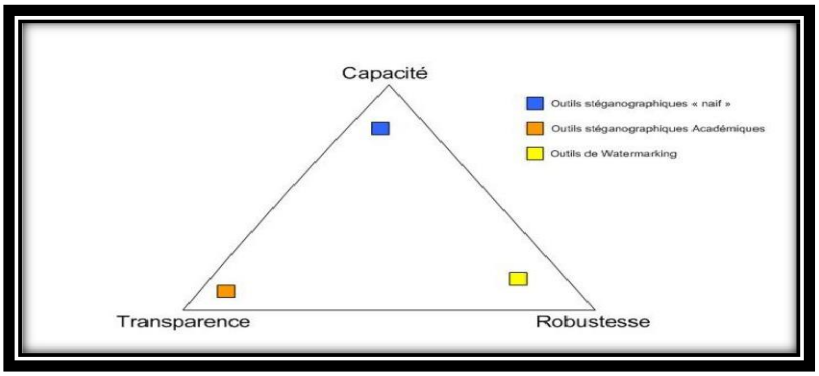

Figure 2.4 caractéristique de la stéganographie

Ces trois critères ne peuvent pas être maximisés simultanément. Chacun d'entre eux aura une influence sur l'autre. Par exemple, la capacité va en contradiction avec la transparence. Sur la figure 2.4, des outils ont été placés afin de définir la caractéristique principale.

Les outils de stéganographie dit naïfs correspondent à la grande majorité des outils disponibles sur internet. Ils cachent les informations dans les conteneurs sans réellementse préoccuper de la facilité à détecter ces données, ni les influences que ces données peuvent avoir sur le conteneur d'un point de vue statistique.

Les outils de stéganographie académique sont quant à eux développé par des équipes

de recherches (notamment l'équipe de Fridrich). Leur objectif est de faire évoluer en parallèle stéganographie et stéganalyse. Leur objectif principal est d'arriver à des algorithmes totalement transparents (pour les méthodes actuelles), afin de pouvoir en déduire des méthodes de stéganalyse encore plus performantes. De récentes recherches portent sur la maximisation de l'espace de dissimulation disponible. Ces outils arriveront peut-être à allier transparence à capacité dans un avenir proche.

Pour finir, les outils de watermarking, utilisé principalement pour la protection de droit d'auteur, sont principalement développé afin d'avoir une très grande robustesse. Contrairement à la stéganographie, leurs adversaires sont de type actif. Le contenu du watermarking ne leur servant en rien, leur unique objectif est la suppression pure et simple de ce dernier.

2.6 Définition de la stéganalyse

Contrairement à la cryptanalyse, dont le but est de récupérer les données ayant été cryptée, la stéganalyse n'a pas comme objectif de retrouver les données dissimulées à l'aide d'un algorithme stéganographique.

Elle consiste uniquement en la détection de contenu stéganographié, ce qui n'est déjà pas une mince affaire. En détectant si un média sert de conteneur stéganographique, des artefacts laissés par un algorithme particulier pourront éventuellement être retrouvé. En connaissance de cet algorithme, il sera possible de lancer une attaque par dictionnaire, voir force brute, afin de déterminer la clé stéganographique.

Plusieurs catégories de méthodes peuvent être utilisées dans cette optique. La plus simple consiste en la détection de signature d'un logiciel donné. Certains programmes laissent derrière eux, de manière intentionnelle ou par erreur de conception, des artefacts permettant de caractériser leur passage. Cette façon de faire possède l'avantage de directement fournir le nom de l'application utilisée pour la dissimulation de donnée. Par contre, chaque application doit faire l'objet d'une analyse spécifique.

La détection d'irrégularité statistique est une autre catégorie d'analyse. Elles se basent sur la quantification de distorsion du média analysé, comparativement à des distributionsstatistiques théorique représentant un média de base. Sa grande force est de pouvoir détecter un large panel d'application se basant sur la même technique stéganographique.

La catégorie permettant le scope de détection le plus large est donné par les outils de stéganalyse universelles. Se basant sur des réseaux neuronaux, leur capacité dépend uniquement de la qualité de la base d'entraînement, ainsi que du bon choix des

caractéristiques sensées qualifiée le média.

2.7 Techniques Stéganographiques

Cette partie va s'atteler à détailler quelques techniques stéganographique utilisée couramment dans les images. A noter que certaines de ces techniques sont transposables aux autres domaines que sont l'audio et la vidéo [*]. Il est possible d'établir une hiérarchie au niveau des techniques stéganographique.

En partant du moins sécurisé, cette hiérarchie serait :

- L'ajout du message à la fin du fichier.
- L'ajout du message dans les espaces inutilisés du conteneur.
- Ajout du message dans les données de l'image de manière séquentielle.
- Ajout du message dans les données de l'image en utilisant une séquence pseudo aléatoire.
- Ajout du message dans les données de l'image en utilisant une séquence pseudo aléatoire, en prenant soin de modifier les données inutilisées afin de ne pas être visible d'un point de vue statistique

Ces cinq points peuvent être regroupés en deux catégories distinctes. Pour les deux premiers points, ils correspondent à la technique dite de fusion. Pour ce qui est du reste, ils peuvent être regroupés dans ce qui a trait à la modification LSB.

Ces deux techniques vont être détaillées ci-dessous

2.7.1 LSB

La technique du LSB, signifiant Least Significant Bit, est de loin la technique la plus répandue. 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 donnéespar 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 base sur l'insensibilité du système visuel humain a un faible changement de couleurs.

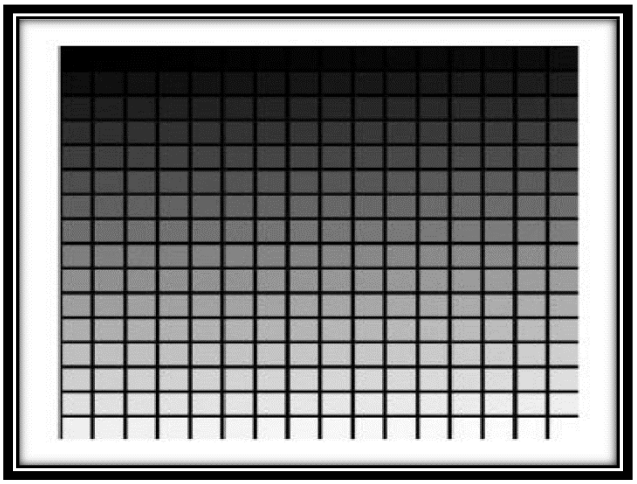

Figure 2.5 mire de 256 niveaux de gris

Comme cela peut être mis en évidence à l'aide de la figure, le changement du bit de poids faible correspond à un déplacement horizontal d'une case dans la mire. Aucun changement n'est perceptible.

Plusieurs types de modifications peuvent être effectués sur ces LSB. La plus répandue consiste simplement à remplacer ces bits par les bits du message que l'on souhaite dissimuler. Appelée "LSB Replacement" dans la littérature, cette technique semble à première vue très efficace, cependant comme cela sera détaillé plus loin dans le document, elle possède le gros désavantage de modifier de manière significative les statistiques du conteneur.

Un exemple de cette méthode peut être donné à l'aide de la matrice C suivante représentant un conteneur de 4 éléments sur 4.

$$C = \begin{bmatrix} 00 & 00 & 10 & 10 \\ 01 & 11 & 10 & 00 \\ 00 & 11 & 10 & 00 \\ 00 & 00 & 00 & 00 \end{bmatrix}$$

Pour simplifier, chaque élément est codé sur 2 bits uniquement. Si l'on souhaite dissimuler le message m dans notre conteneur, une première remarque sera sur la taille maximum du message qui sera égal au nombre d'éléments dans la matrice. Cela est vrai pour autant que l'algorithme se limite à la modification du seul bit de poids faible.

M (max)= 1001 1010 0011 1001

Dans le cas du conteneur C, la taille maximale est donc de 16 bits. La matrice stéganographié résultant du processus sera.

$$S_{replacement} = \begin{bmatrix} 01 & 00 & 10 & 11 \\ 01 & 10 & 11 & 00 \\ 00 & 10 & 11 & 01 \\ 01 & 00 & 00 & 01 \end{bmatrix}$$

En comparant S à C, on remarque que l'opération consiste donc uniquement en une sur écriture du bit de poids faible.

La seconde méthode est appelée "LSB Matching". Elle diffère de ce qui précède par le fait qu'elle ne modifie pas obligatoirement tous les bits de poids faible.

Le principe consiste à comparer la valeur du bit de poids faible à la valeur du bit à dissimuler. S'ils correspondent, aucun changement n'est effectué. Dans le cas contraire, une incrémentation/décrémentation de manière aléatoire de la valeur de l'élément de 1 sera effectuée. Cela aura pour incidence de codé la valeur désirée au niveau du LSB.

En reprenant la même matrice C que précédemment,

$$C = \begin{bmatrix} 00 & 00 & 10 & 10 \\ 01 & 11 & 10 & 00 \\ 00 & 11 & 10 & 00 \\ 00 & 00 & 00 & 00 \end{bmatrix}$$

Dans laquelle le message m max suivant est à dissimuler.

M max = 1001 1010 0011 1001

Le résultat de l'application de cette méthode à la matrice de base C sera cette fois

Cette matrice est un des résultats possible, le choix entre l'incrémentation et la

$$S_{matching} = \begin{bmatrix} 01 & 00 & 10 & 01 \\ 01 & \mathbf{00} & 11 & 01 \\ 00 & 10 & 11 & \mathbf{11} \\ 01 & 00 & 00 & \mathbf{11} \end{bmatrix}$$

décrémentation étant fait de manière aléatoire. En gras sont mis en évidence des erreurs pouvant provenir du processus. Par exemple, l'incrémentation d'une valeur 11 aura pour conséquence sont passage à 00. L'écart des valeurs étant trop élevé, le résultat de l'opération risque d'être visuellement décelable. L'algorithme doit donc veiller à ce que ce genre de situation ne soit pas autorisée (autorisé uniquement l'incrémentation lorsquela valeur est la plus petite possible par exemple).

Comparativement à la méthode précédente, cette dernière est moins sensible aux ana-lyses statistiques. Du faite de l'incrémentation/décrémentation aléatoire des valeurs des éléments, cette méthode n'ajoutera pas les mêmes distorsions statistiques que le "LSBReplacement".

Dans les deux cas, le choix de l'image hôte est un point essentiel dans l'optique d'obtenir la meilleure transparence possible. Les images contenant peu de couleurs sont a proscrire. Certains experts recommandent l'utilisation d'image en niveau de gris comme meilleurs conteneurs. Il conseille l'utilisation d'images non compressées.

Par la suite vont être détaillées les deux plus grands domaines d'application de la technique du LSB que sont, d'une part, le domaine spatial et de l'autre, le domaine de la transformée en cosinus discret.

2.7.2 Domaine Spatial

Dans le domaine spatial, la dissimulation du message est directement effectuée au niveau du codage des pixels. Une image peut être représentée à l'aide d'une matrice de pixel. Chaque pixel est représenté à l'aide de 1 à 32 bits. Ce nombre dépend de la représentation des couleurs utilisées. le codage sur 8 bits ou 24 bits. Sur 8 bits, deux méthodes de codage sont utilisées. Dans le cadre d'une image en niveaux de gris, chaque pixel code directement le niveau de gris approprié. Dans celui d'une image couleurs, on utilise le mécanisme d'image indexée. Au sein de chaque pixel est codée une valeur correspondant à l'index de la couleur à utiliser dans la palette de couleurs définie. Pour ce qui est du codage sur 24 bits, on utilise généralement le RGB (Red Green Blue)pour la représentation des couleurs. Chaque pixel est codé à l'aide d'un triplé de byte spécifiant chacune des composantes principales. Dans ce type de représentation, il est possible de dissimuler 3 bits par pixel (1 par composante) sans aucun impact visuel.

Figure 2.6 A gauche, image originale. A droite, image contenant un PDF de 32 Kbdissimulé à l'aide d'Invisible Secrets 4

Les fichiers généralement utilisé sont au format BMP et GIF. Cette technique est très utilisée car elle facile à mettre en œuvre. Elle permet de directement ajouter les données à l'image, sans avoir à passer par un mécanisme de compression /décompression comme ce serait le cas pour la modification des coefficients DCT.Crée sa propre implémentation

devient très facile, cela permet de s'affranchir de l'utilisation d'un produit existant et par la même occasion, d'éviter la détection de signature étant attribuée à ce programme (technique encore très utilisée dans les outils dedétection). De plus, il est possible de vraiment contrôler la manière dont seront dissimulées les données au sein du conteneur. Il sera possible de facilement implémenté des mécanismes permettant de déjouer les tentatives d'analyse statistiques.

L'inconvénient majeur provient des formats utilisés. Les images au format JPEG sont, de loin, les plus répandue sur Internet. Le simple fait d'envoyé une image au format BMP peut attirer l'attention, et de ce fait, mettre à néant tous les efforts de dissimulation de données. Ainsi, les outils permettant la dissimulation de données dans le format JPEG constitue une des meilleures solutions offertes.

2.7.3 Domaine de la Transformée en Cosinus Discret (DCT)

Comme souligné dans la section précédente, les images au format JPEG représentent la grande majorité des images circulant sur le réseau des réseaux. Une image envoyé à son collègue en utilisant ce format est devenu quelque chose d'anodin. Dans ce contexte,ce format semble être un conteneur de choix pour des communications secrètes.

La dissimulation d'information dans des formats de compression à perte se révèle, cependant, plus difficile. Ce type de compression utilisant les mêmes données redondantes (n'ayant aucun impact sur la perception du média) que celle utilisée dans leprocessus de dissimulation.

Afin d'assurer un maximum de transparence, les modifications doivent avoir lieu dans le domaine des Transformées en Cosinus Discret et non dans le domaine spatial. D'un point de vue compression cela permet d'éliminer les hautes fréquences (saut brusque de couleur) qui ne sont que difficilement décelable par l'œil humain.

En ce qui concerne la stéganographie par modification des coefficients DCT, elle intervient après la phase de quantification de l'algorithme de compression

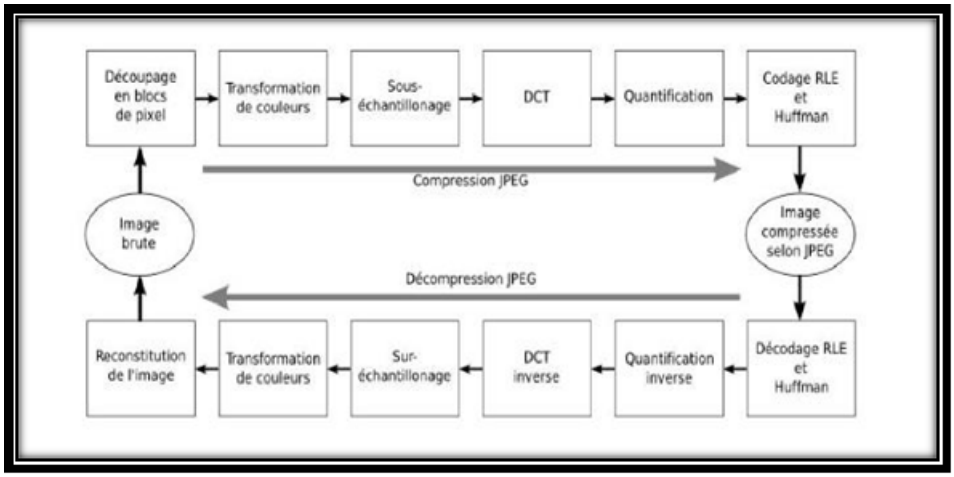

Figure 2.7 Schéma Bloc du processus de compression/décompression JPEG

Pendant ce processus, la plupart des coefficients étant ramenés à zéro, tout effort de dis- simulation intervenant avant la quantification serait rendu inutilisable. Un autre facteur à prendre en compte, et de ne pas modifier les propriétés de compression. Après quantification, les matrices de coefficients passent par un algorithme de compression sans perte, le codage de Huffmann. Afin de ne pas modifier les informations, aucun coefficient étant égal à 1 ou 0 ne devra être modifié. Si l'on remplace un coefficient à 1 par 0, cela engendrera un meilleurs taux de compression, ce qui n'est pas souhaité.

De cela découle un des gros inconvénients de cette méthodologie. Une matrice de coefficients étant principalement composée de 0, et ceux-ci ne pouvant pas être modifiés, la capacité du conteneur s'en retrouve fortement réduite. De plus, contrairement à la modification dans le domaine spatial, implémenté une telle technique se révèle plus ardu.Il est en effet nécessaire de coder tout le compresseur JPEG, ce qui n'est pas une tâche aisée. La dissimulation dans les coefficients DCT ne se révèle pas non plus performante d'un point de vue transparence. Quelques méthodes de stéganalyse dans le domaine spatial ont rapidement été adaptées au domaine DCT. Malgré ces inconvénients, la très forte distribution de ce format est un avantage majeur. De nombreuse personne (surtout du domaine académique) l'on comprit, est des outils, telF5 ou Outguess ont vu le jour.

2.7.4 Algorithme Outguess

Développer par Niels Provos, à qui l'on doit notamment le document, cette algorithme avait comme objectif de passer totalement inaperçu lors d'une analyse statistique des χ 2.

Il travaille sur les fichiers de type JPEG en effectuant une sur écriture des LSB au niveau des coefficients DCT. Cependant, pour ne pas modifier les propriétés de compression, il modifie uniquement les coefficients étant différent de 1 ou 0.

Afin de paraître invisible lors d'analyse statistique du premier ordre (analyse des histogrammes de valeur DCT), l'algorithme opère en deux étapes

En première passe, il modifie les LSB des coefficients DCT de manière pseudo-aléatoire. Ceci est défini à l'aide d'une clé.

En deuxième passe, il parcourt les coefficients DCT non modifiés afin d'adapter leur valeur de tel sorte que l'histogramme des coefficients après modification soit égal à celui du fichier d'origine.

Afin de pouvoir être sûr de retrouver l'histogramme d'origine après la manipulation, il effectue un calcul de la taille maximal des données à dissimuler en fonction de l'image. Ceci est, bien sûr, effectué avant le début des opérations.

Figure 2.8 A gauche, image originale. À droite, image contenant le fichieroutguess.h stéganographié avec Outguess

Comme il peut être remarqué sur la figure, aucune différence n'est visuellement apparente. Fridrich a défini une méthode permettant de détecter de manière viable les contenus stéganographié à l'aide d'Outguess.

2.7.5 Fusion

Cette technique, que l'on peut considérer comme de la stéganographie naïve, consiste à ajouter les données à cacher au fichier. Pour ce faire, cette méthode utilise des emplacements inutilisés ou non lu par la plupart des décodeurs d'image.

On distingue deux fonctionnements : L'ajout de données en fin de fichier et l'ajout au niveau des en-têtes de fichier.

L'ajout en fin de fichier est rendu possible par le fait que la plupart des décodeurs d'image ne lisent pas le fichier image dans son ensemble. Pour la plupart des formats d'image disponible, un certaine chaîne de bits est définie afin de marqué la fin de l'image.

L'ajout en fin d'image appond simplement après cette chaîne les données dissimulées. Aucune limitation de taille n'est imposée, cependant un fichier image de 20 Mbytes risque

de ne pas passer inaperçu.

Pour ce qui est de l'ajout dans les en-têtes, certains formats comme le bitmap définissent un champ permettant de spécifier l'offset à partir duquel l'image commencera.

En spécifiant un offset un peu plus long il est possible de cacher entre deux les données à dissimuler.

Cela peut aussi être fait à l'aide d'ajout de commentaire, pour le JPEG par exemple

Figure 2.9 A gauche, image originale. A droite, image contenant des données

La (figure 2.9) montre l'ajout de données en temps que commentaire dans une image JPEG. Pour confirmer qu'aucune limitation de taille n'est imposée, un fichier PDF de 1.57 MByte a été dissimulé sans problème.

Malgré le fait qu'aucune limitation de taille n'est imposée pour cette technique, elle tient plus du gadget que de la stéganographie. Une simple vérification de la consistance des fichiers, avec des vérifications ciblées aux endroits permettant la dissimulation permet d'éradiquer toutes tentatives de communication cachée.

2.8 Conclusion

La stéganographie est un ancien moyen de cacher des messages sans qu'un lecteur nonautorisé en prenne connaissance. Elle a souvent été dans l'ombre. La stéganographie est en fait un monde vaste et varié mais totalement inconnu du grand public.

LE TROISIÈME CHAPITRE

Introduction

Dans les chapitres précédentes, nous avons présenté les différentes notions de l'image numérique et la stéganographie de l'image. Donc, dans ce chapitre nous présenterons la mise en œuvre de notre application , nous commençons tout d'abord par une présentation du langage de programmation choisi . Ensuit nous mention les détailles d'implémentation de cette application . On termine ce chapitre par une synthèse sur nos résultats obtenus.

3.1 L'outil utilisé dans l'application

3.1.1 Langage de programmation

Pour la réalisation de cette application, nous avons utilisé le langage Java; Le Java est un langage de programmation expressément conçus pour être utilisés dans l'environnement distribué de l'Internet. Il a été conçu pour avoir le «look and feel» du langage C ++, mais il est plus simple à utiliser que C ++ et applique un modèle de programmation orienté objet. Java peut être utilisé pour créer des applications complètes qui peuvent fonctionner sur un seul ordinateur ou être répartis entre les serveurs et les clients dans un réseau. Il peut également être utilisé pour construire un petit module d'application ou applet pour une utilisation dans le cadre d'une page Web. Applets permettent à un utilisateur de la page Web pour interagir avec la page. [15]

NetBeans est un environnement de développement intégré basé sur Java (IDE). Le terme désigne également le cadre de la plate-forme d'application sous-jacente de l'EDI.

L'IDE est conçu pour limiter les erreurs de codage et de faciliter la correction d'erreur avec des outils tels que les NetBeans FindBugs pour localiser et résoudre les problèmes communs de codage Java et Debugger pour gérer du code complexe avec des montres de terrain, points d'arrêt et suivi de l'exécution. Bien que le NetBeans IDE est conçu spécifiquement pour les développeurs Java, il prend également en C / C ++, PHP, Groovy et HTML5 en plus de Java, JavaScript et JavaFX. [16]

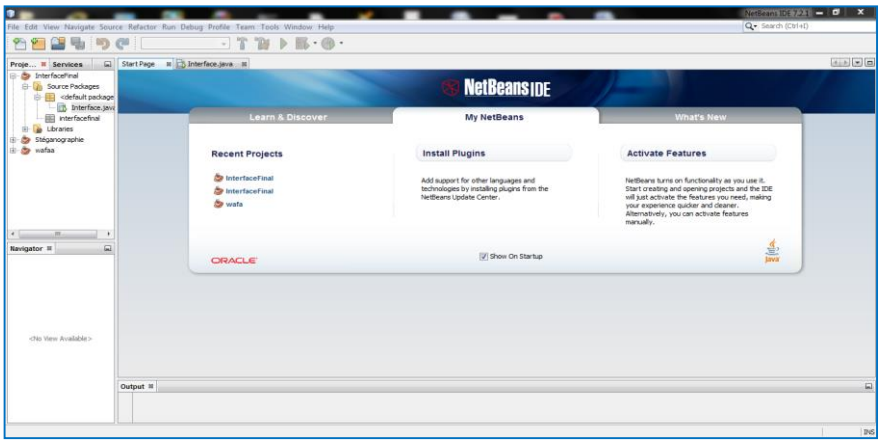

Figure 3.1 :Interface de NetBeans.

3.1.2 La Méthode utilisé

Il existe de nombreuses techniques de stéganographie. Dans notre travail nous avons choisir la forme la plus simple de la stéganographie numérique (et probablement la plus commune) qu'est la méthode LSB (le deux bit le moins significatif). Les valeurs binaire à dissimulé est introduite dans le dernier deux bit de poids faible d'un octet de l'image. Le changement global à l'image est si infime que cela ne peut pas être vu par l'œil humain. Un exemple de cette méthode peut être donné figure 3.2 .

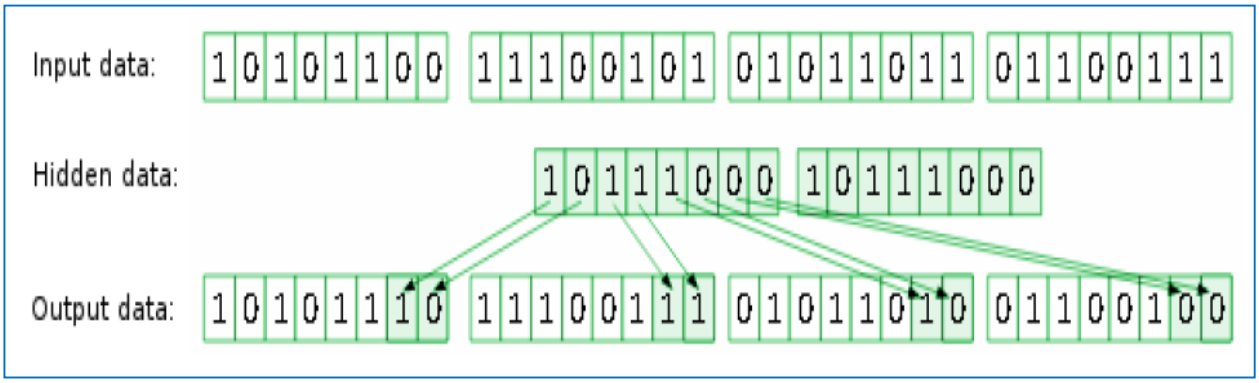

Figure 3.2: L'application de la LSB en utilisant un bit le moins significatif.

3.2 Les algorithmes

Il existe deux algorithmes séquentiels, utilise une technique encodé et décodé.
Voici les deux algorithmes

- Algorithme pour insérer le texte :

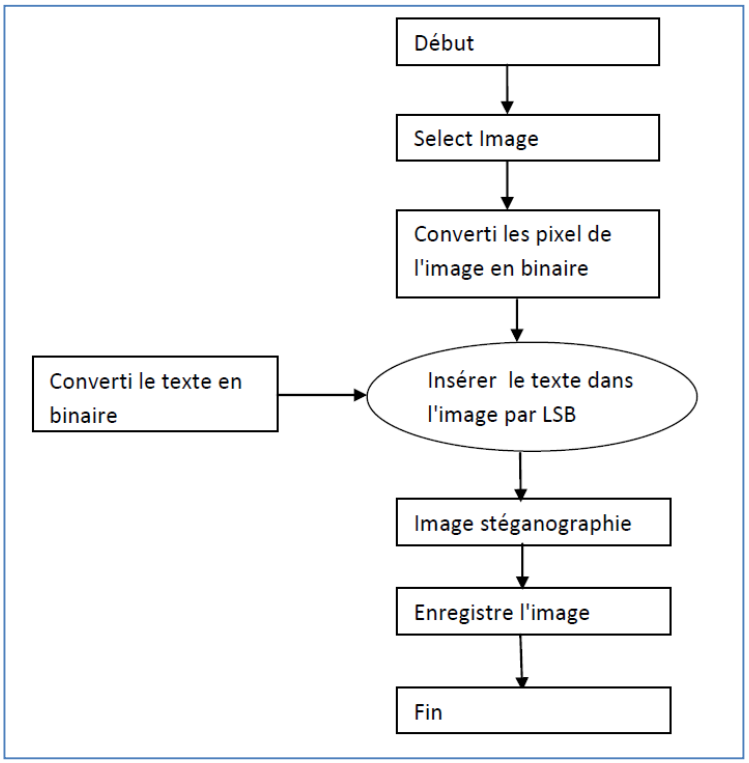

Figure 3.3: Algorithme d'insertion.

- Algorithme méroire pour extraire le texte :

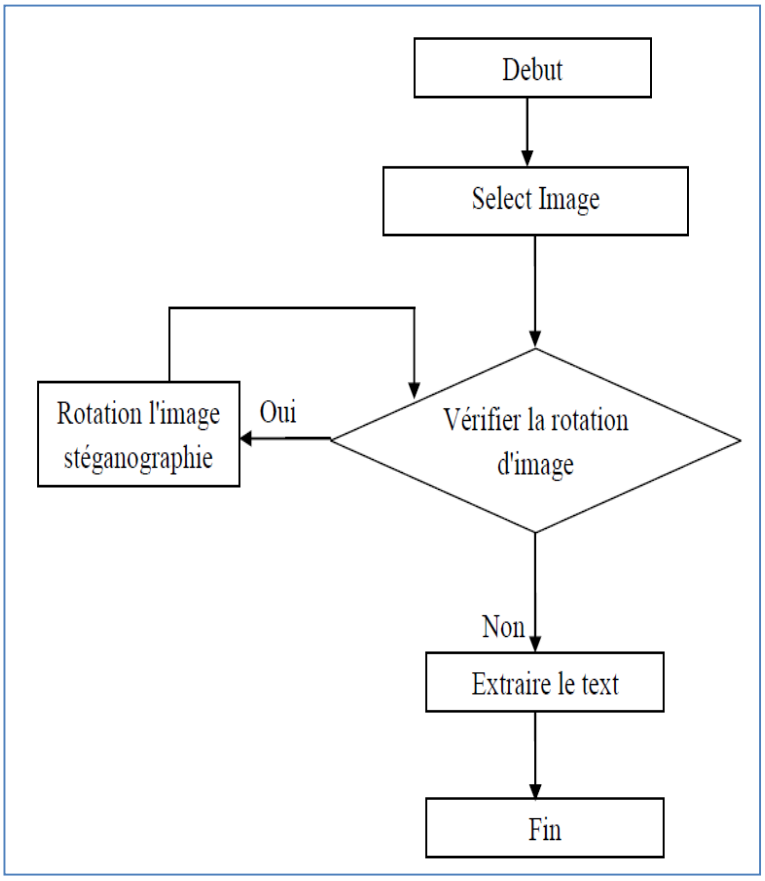

Figure 3.4: Algorithme d'extraction.

3.3 Résultat Obtenu

Les Interfaces graphiques

- L'interface est composée de deux partie : partie encoder, et partie décodé, comme il est présenté dans la figure suivante :

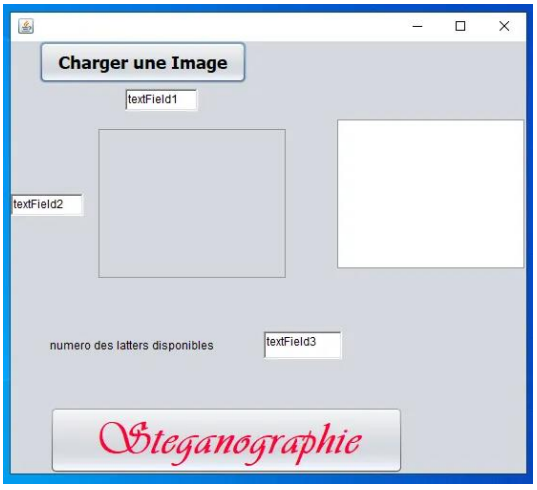

Figure3.5: Interface de l'application.

- La boîte de dialogue suivante apparaît: où sont le choix d'une image spécifique.

Cliquer sur le bouton « Open », l'utilisateur choisie une image.

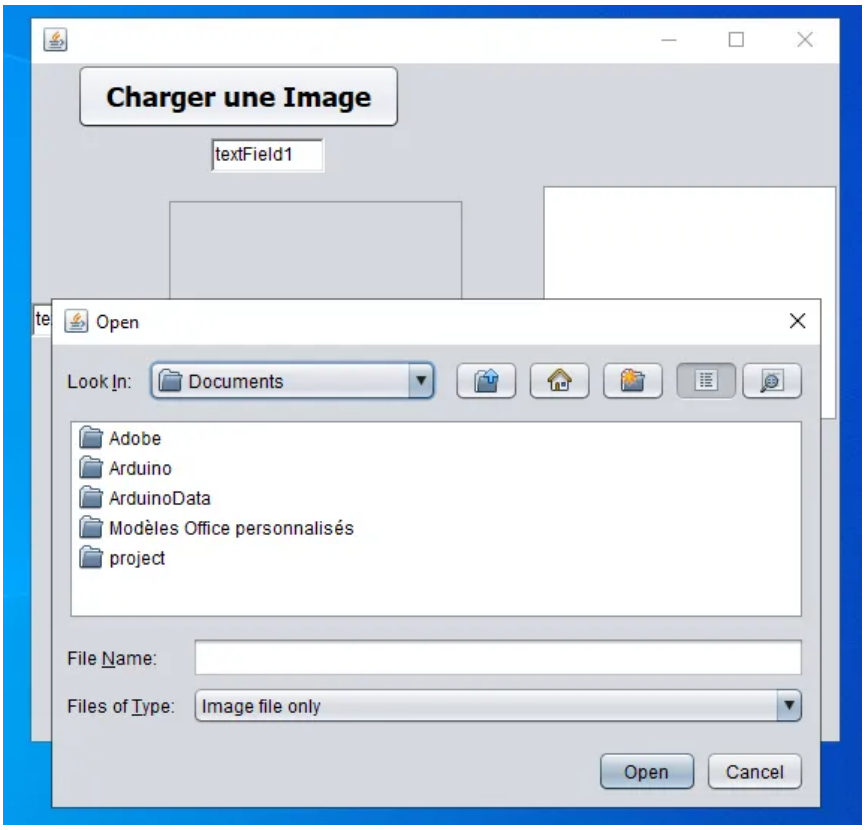

Figure 3.6: Interface de sélection d'image

- L'interface suivante s'affiche : aller Dissimuler le texte dans l'image

Figure 3.7: Interface de dissimuler le texte dans l'image.

- La boîte de dialogue suivante s'affiche : aller chercher l'image là où elle est enregistrée dans La place de votre choix.

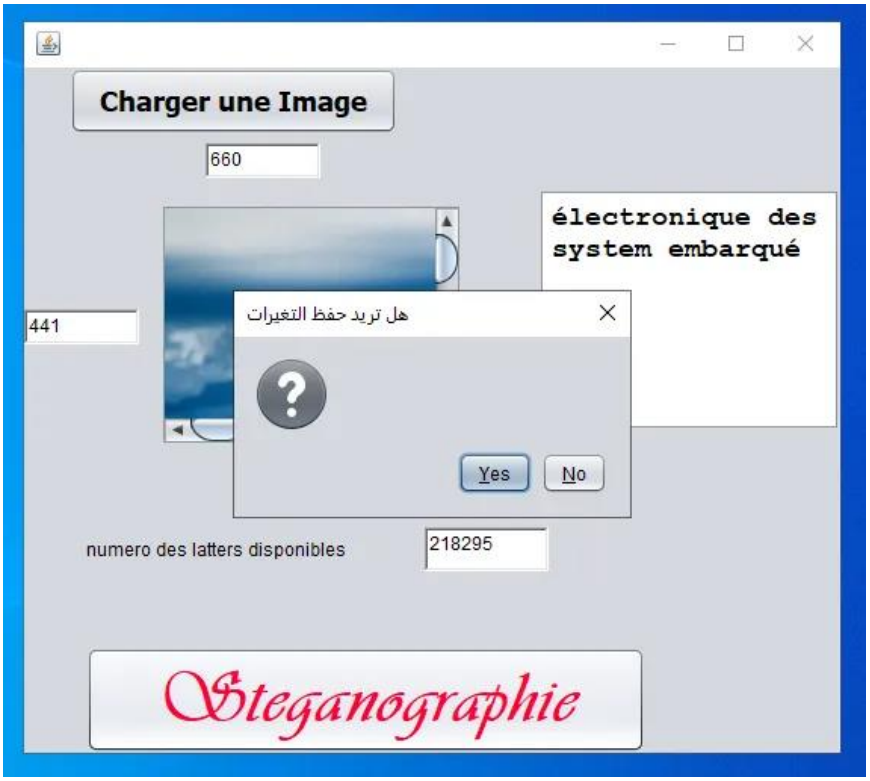

Figure 3.8: Interface de Sauvegardé l'image stéganographie.

- La boîte de dialogue suivante apparaît: où sont le choix d'une image stéganographie Cliquer sur le bouton « Open ».

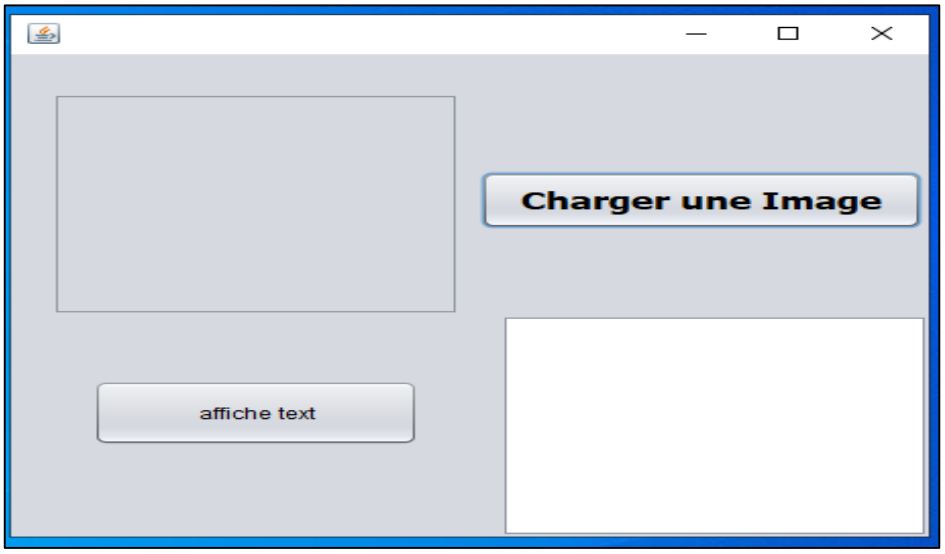

Figure 3.9: Interface de Sélection l'image stéganographie.

- Afficher l'image encodé dans partie décodé pour extraire le texte .

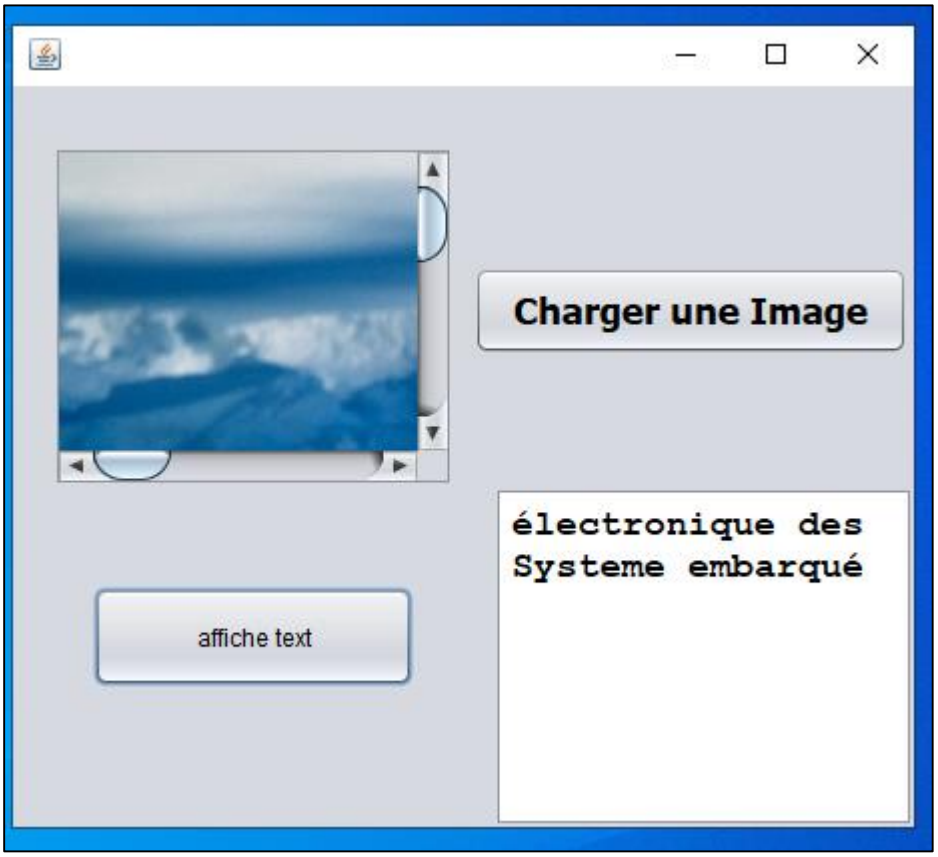

Figure 3.10: Interface de Extraire le texte .

- En la fin, le résultat obtenu de la stéganographie c'est :

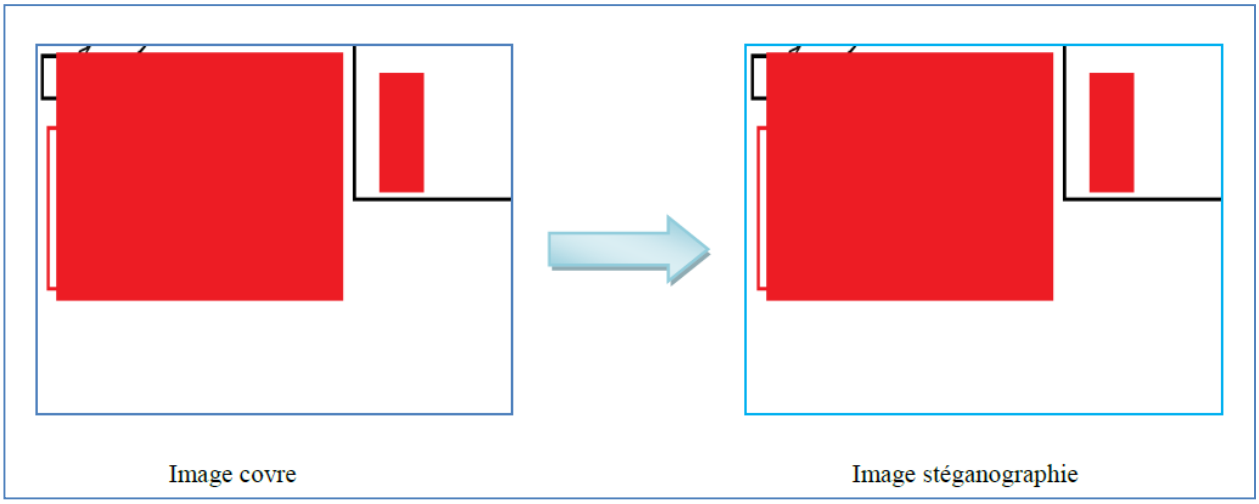

Figure 3.11: A gauche image original à droite image stéganographie.

.Il est impossible, à l'oeil, de distinguer l'image qui cache le message, et l'image initiale.

Figure 3.12 : *Image originale*

Figure 3.13 : *Image stéganographiée*

Quantification perceptuelle :

La définition de la stéganographie stipule que les changements dans le milieu de couverture doivent rester imperceptibles. Pour remplir cette condition, ou pour pouvoir mesurer efficacement la distorsion introduite par l'algorithme de stéganographie, il est nécessaire d'utiliser une technique développée sous la forme d'un algorithme objectif de mesure de qualité d'image.

PSNR :

(Signl de Peak Signal to Noise Ratio) c'est une mesure de similarité utilisée en image numérique. Il s'agit de quantifier la performance des codeurs en mesurant la qualité de reconstruction de l'image tatouée par rapport à l'image originale.

Il est mesuré en dB à partir de la relation suivante :

$$\mathrm{PSNR} = 10.\log_{10}[\frac{(\max(x))^2}{\mathrm{MSE}}]$$

- x : est le signal original
- y : est le signal modifié.
- n : est la dimension commune aux deux vecteurs considérés.
- MSE (Mean Square Error) : est l'erreur quadratique moyenne calculé par cette formule :

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{n}(xi - yi)^2$$

Tableau 3-1 : Les formules des MESE et PSNRE

Assessment	Description	Formula
MSE	Mean Square Error	$MSE = \frac{1}{n}\sum_{i=1}^{n}(xi - yi)^2$
PSNR	Signl de Peak Signal to Noise Ratio	$PSNR = 10.\log_{10}[\frac{(max(x))^2}{MSE}]$

Tableau 3-2 : Comparaison des images avant et après stéganographie

Image originale	PSNR	MSE	Image stéganographie	PSNR	MSE
	**72.6217**	**7.0158e-04**		**72.6115**	**7.0230e-04**
	**69.4178**	**9.6655e-04**		**69.4613**	**9.6235e-04**
	**69.3507**	**9.7305e-04**		**69.3417**	**9.7393e-04**

	**69.3536**	**9.7278e-04**		**69.3690**	**9.7127e-04**

- **Commenter sur les résultats.**

Après avoir utilisé la stéganographie sur les images, nous avons calculé le MSE et le PSNR et nous avons comparé ces valeurs (MSE et PSNR) ., Le tableau ci dessous montre que la différence entre les (MSE et PSNR) avant et après l'utilisation de cette stéganographié est quasi nulle et n'affecte pas la purté de l'image. Raison pour la quelle nous pouvons dire que notre algorithme de stéganographie fonctionne bien car il est pratique regardant les résultats obtenus

Remarque :

Cette application calcule le nombre de caractères qu'elle peut cacher dans l'image, car ce dernier est calculé par l'équation incluse.

$$\frac{(L * W) * 2(R\ Bit + G\ Bit + B\ Bit\ )}{8\ Bit}$$

Conclusion

Dans ce chapitre, nous avons proposé une application de stéganographie par substitution LSB des deux derniers bit de chaque valeur colorimétrique de l'image pour inséré une message, aussi on faire une algorithme qui calqué la MSE et PSNR pour voire la performance de méthode LSB ,cependant elle reste sensible à toute forme de compression va qu'on opère sur le domaine sp .

CONCLUSION GÉNÉRAL

Conclusion général

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 créer une application implémente en java en utilisant la méthode LSB.

Le premier chapitre résume les concepts de base du traitement d'images, impliquant L'image numérique comme sa définition, ses caractéristiques et types, sa formation et Son format. Alors une brève explication pour vous faire comprendre les outils qui constituent Des images considérées comme le support que nous avons dans notre travail Masquer les données

Dans le deuxième chapitre, nous avons commencé la technique de la stéganographie et nous avons De son histoire, d'où vient-il. Puis sa définition et ses principes généraux Pour permettre une bonne compréhension du principe de fonctionnement du système de stéganographie, nous avons encore une fois Parlé de la référence technique et du support utilisé pour mettre en œuvre un tel système, et enfin Nous concluons ce chapitre par un aperçu de la stéganalyse, qui inclut la détection La présence d'informations cachées ou d'une autre expression est l'opération inverse Stéganographie. Bien que dans le chapitre précédent nous ayons fait une implémentation et Représente le résultat obtenu à partir de l'algorithme de stéganographie LSB

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

Référénces

[1] **YAOVI GAGOU**, " Cours traitement d'image," dans Université de Picardie Jules Verne, 2008.

[2**] S. Mohanty, N. Ranganathan,** and **K. Namballa**. « VLSI Implementation of Visible Watermarking for a Secure Digital Still Camera Design ». In17th International Conference on
VLSI Design, , 2004.

[3] **M. Bergounioux**. Quelques méthodes mathématiques pour le traitement d'image. In *Cours MASTER*, 2009.

[4] **Y. Hu, J. Huang, S. Kwong**, and **Y. Chan**. « Image Fusion Based Visible Watermarking Using Dual-Tree Complex Wavelet Transform ». InIWDW'2003,

[5**] Danielle CH AN TEGREL**, " *Traitement numérique de l'image,* " Académie de Poitiers,
2004.

[6] http://www.eclairement.com/Image-numerique-quel format.2007.

[7] D. Lingrand. *Introduction au traitement d'images*. Vuibert, 2008.

[8] **D. Zheng, Y. Liu, J. Zhoa,** and **A. Saddik**. « A survey of RST Invariant Image Watermarking Algorithms. »ACM Computing Surveys, 39(2), 2007.

[9] Jean **Luc Le Luron**. « Les images numériques, généralités ». 2003.

[10] **Cocquerez J-P., Philippe S**., (1995). Analyse d'images :filtrage et segmentation. Edition Masson, Paris, France.

[11] **INTECO.N.T.C** ; «Stéganographie, l'art de cacher l'information » ; (http://www.usatoday.com/tech/news/2001-02-05-binladen.htm).

[12] **Ahmed Amine NAIR**; « Hybridation des réseaux de neurones avec les essaims de particules (MLP-PSO) :Application à la vérification de la signature » ; Université des Sciences et de la Technologie d'Oran ; 2011

[13] **J. Fridrich** and M. Goljan, "Digital image steganography using stochastic modulation", SPIE Symposium on Electronic Imaging, San Jose, CA, 2003.

[14] **T. Morkel** , **J. H. P. Elloff**, M.S. Olivier, "An Overview of Image Steganography".

[15] **Provos, N**. & **Honeyman**, P., "Hide and Seek: An introduction to steganography", IEEE Security and Privacy Journal, 2003.

[16] **Johnson**, N.F. & **Jajodia**, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.

[17] **N. Provos** and **P. Honeyman**, "Detecting Steganographic Content on the Internet," Proc. 2002 Network and Distributed System Security Symp., Internet Soc., 2002.

[18] **D. McCullagh**, "Secret Messages Come in .Wavs," Wired News, Feb. 2001, www.wired.com/news/politics/ 0,1283,41861,00.html.

[19] **Trivedi M C Sharma** S and **Yadav** V K 2016 Analysis of several image steganography techniques in spatial domain: a survey. In; Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS '16). ACM. Article 84.

[20] **Wu D-A** and **Tsai** W-H 2003 A steganographic method for images by pixel-value differencin g.Pattern Recognit. Lett. 24(9–10):1613–1626

[21] **Jin-Suk Kang**, **Yonghee You**, **Mee Young Sung**. "Steganography using Block-based Adaptive Threshold". Computer Science 2007.