UNIVERSITÉ KASDI MERBAH OUARGLA

Faculté des Technologies D'information et de communication

Département d'informatique et technologie d'information

Mémoire de Fin d'Etudes

En vue de l'obtention d'un

MASTER PROFESSIONNELLE

Domaine : Mathématiques et informatique

Filière : Informatique

Spécialité : sécurité de réseaux

Thème

Sécurité des échanges par stéganographie d'image numérique

Directeur de mémoire : Dr. Khaldi Amine

Présenté par :

M^elle^ Benhelal Radia

M^elle^ Benras Nour Elhouda

Soutenu publiquement le *:* **14/06/2023**

Devant le jury :

Mr : Kahlessenane Fares	MCB	Présidente	Univ.K.M-Ouargla
Mr : Khaldi Amine	MCB	Encadreur	Univ.K.M-Ouargla
Mr : Euschi Salah	MCB	Examinateur	Univ.K.M-Ouargla

Année universitaire : 2022/2023

DÉDICACE

Aucun dédicace aucun mot ne pourrait exprimer mon respect ma considération et mes profonds sentiment envers eux je pris mon dieu de les bénir de veiller sur eux j'espère qu'ils seront toujours fiers de moi.

Grâce à dieu tout puissant .Je dédier ce modeste travail tous d'abord à ma chère mère Khadra. Merci de m'avoir soutenu tant moralement que matériellement pour que je Puisse attendre mon but, et de vos prières pour moi.

A mon cher père El Hadi qui ont toujours souhaité notre réussit et qui m'ont permis d'atteindre mes objectifs dans mes études et de ma vie, celle qui matant bercé, tant donné et tant enseigné, toi qui m'a guidé dans le droit chemin, toi qui m'a appris que rien est impossible.

A Ma chère sœur : Asma

A Mon cher frères : Zineddine

Au reste de ma famille « Benhelal et Bouhafs»

A mes meilleure amies qui m'ont toujours ouvert les portes de l'espoir surtout mon binôme Nour Elhouda qui est soufré beaucoup plus atouts ma famille.

A toute la promotion master II 2022/2023. Option Administration et sécurité des réseaux du Département de l'informatique et technologies de l'information, Faculté des Nouvelles Technologies de l'information et la Communication

DÉDICACE

Aucun dédicace aucun mot ne pourrait exprimer mon respect ma considération et mes profonds sentiment envers eux je pris mon dieu de les bénir de veiller sur eux j'espère qu'ils seront toujours fiers de moi.

Grâce à dieu tout puissant .Je dédier ce modeste travail tous d'abord à ma chère mère Meriem. Merci de m'avoir soutenu tant moralement que matériellement pour que je Puisse attendre mon but, et de vos prières pour moi.

Au reste de ma famille «Benras»

A mes meilleure amies qui m'ont toujours ouvert les portes de l'espoir surtout mon binôme Radia.

A toute la promotion master II 2022/2023. Option Administration et sécurité des réseaux du Département de l'informatique et technologies de l'information, Faculté des Nouvelles Technologies de l'information et la Communication

Remerciements

Nous tenons tout d'abord, à remercier Allah notre créateur qui nous a donné la force pour réussir dans notre modeste travail.

Nous adressons tout d'abord nos sincères remerciements au Pr. Khaldi Amine, Maître de conférences A l'université KASDI Merbah -Ouargla, pour avoir accepté de diriger ce mémoire en Assurant l'encadrement tout au long de la réalisation de cette étude ; ce qui sans ses incitations de précieuses nous n'avons pas réalisé cela.

Nous remercions également tous les enseignants de département de d'informatique et technologie d'information de l'Université KASDI MERBAH-Ouargla.

Merci à toute personne ayant contribué de près ou de loin à l'élaboration de ce travail.

Résumé:
Avec le développement des technologies de l'information et des échanges électroniques, en outre, le principal problème reste au niveau des échanges de données sur Internet, la garantie de confidentialité des informations est devenue très faible. Dans ce contexte, de nombreuses solutions informatiques sont apparues, mais elles sont encore insuffisantes, ce qui a conduit à l'émergence de la stéganographie de l'information comme solution complémentaire afin de contribuer à la sécurité des images partagées sur le réseau. Le travail présenté est reflété dans notre mémorandum sur la stéganographie dans images numérique, visant à renforcer la sécurité et la protection des droits d'auteur, et à assurer la confidentialité des communications entre deux parties. Nous avons abordé une méthode puissante pour tatouer des images numériques, qui est LSB, où la présence du message secret dans l'image stego est pratiquement imperceptible et indétectable. En particulier, il est nécessaire de s'assurer que la qualité de l'image ne se dégrade pas visuellement, nous voulons donc présenter une application pratique qui peut fournir des performances entre la capacité d'insertion, l'imperceptibilité et la robustesse et du stéganographie. Pour que le processus soit efficace, il doit être robuste, imperceptible et une statistique invisible.

Mots clés : Stéganographie, Image numérique ,Bit le moins significatif .

الملخص:
مع تطور تكنولوجيا المعلومات و التبادلات الالكترونية علاوة على ذلك تظل المشكلة الرئيسية في مستوى تبادل البيانات على شبكة الانترنت , اصبح ضمان سرية المعلومات ضعيف جدا . على اثر هذا السياق ظهرت العديد من الحلول الحاسوبية لكنها لا تزال غير كافية , مما أدى الى ظهور علم اخفاء المعلومات كحل مكمل من أجل المساهمة في أمن الصور المشتركة على الشبكة .يتجلى العمل المقدم في مذكرتنا الوشم الرقمي للصور مستهدفين تعزيز أمن و حماية حقوق النشر و ضمان سرية التواصل بين طرفين .تطرقنا لطريقة قوية للوشم في الصور الرقمية و هي LSB، حيث يكون وجود الرسالة السرية في صورة ستيجو غير محسوس و غير قابل للكشف عمليا . من الضروري على وجه الخصوص ضمان عدم تدهور جودة الصورة بصريا , لذلك نرغب في تقديم تطبيق عملي يمكنه ان يوفر الأداء بين السعة من الإدراج وعدم الإدراك وقوة اخفاء المعلومات .لكي تكون العملية فعالة يجب أن تكون قوية و غير محسوسة و إحصائية غير مرئية.

الكلمات المفتاحية: إخفاء المعلومات, صورة رقمية , بت أقل دلالة .

Abstract:

With the development of information technologies and electronic exchanges, moreover, the main problem remains at the level of data exchanges on the Internet, the guarantee of confidentiality of information has become very weak. In this context, many computer solutions have appeared, but they are still insufficient, which has led to the emergence of information steganography as a complementary solution to contribute to the security of images shared on the network. The work presented is reflected in our memorandum on steganography in digital images, aimed at strengthening security and copyright protection, and ensuring the confidentiality of communications between two parties. We have covered a powerful method for watermarking digital images, which is LSB, where the presence of the secret message in the stego image is virtually unnoticeable and undetectable. In particular, it is necessary to ensure that the image quality does not degrade visually, so we want to present a practical application that can provide performance between insertion capacity, imperceptibility and robustness and du steganography. For the process to be effective, it must be robust, unnoticeable, and an invisible statistic.

Keywords : Steganography, Digital Image , least significant bit .

Table des matières

Chapitre III Résultats et discussion

Liste des Figures

Liste des Figures

Liste des tableaux

Introduction Générale

La maîtrise des flux d'informations est un enjeu central pour la sécurité d'un système, c'est-à dire : Entreprise, pays, particulier. De nos jours, le réseau informatique et Internet sont de plus en plus complexes et partagés des médias numériques fait l'objet de manipulations illicites. Se pose alors le véritable problème de la sécurisation de la transmission des informations. Le transfert de données confidentielles et sensibles ne peut se faire avec de tels risques, sauf avec la disponibilité du coffre-fort. Plusieurs méthodes ont été publiées Pour surmonter ce problème, le cryptage a toujours été la méthode efficace appliquée pour protéger et sécuriser les informations en envoyant des données cryptées. C'est comme ça que ça se passe Des solutions pour protéger la confidentialité des données, pour assurer leur sécurité. Mais cette protection ne fonctionne que pendant sa transmission et sa distribution. Une fois que les données sont claires, elles ne contiennent protection. Dans ces circonstances, nous avons appliqué d'autres techniques de protection, ce sont des techniques de Tatouage qui visent à assurer une protection permanente. Ces techniques visent à introduire un message caché dans un support de manière imperceptible, c'est la science de la stéganographie.

Stéganographie possède trois grandes propriétés qui caractérisent son utilisation : La robustesse, la sécurité et la capacité. La robustesse assure que l'information secrète ne peut
Pas être détruite et sans dégrader fortement l'image. La sécurité vise à ce que l'image stégo ne Soit pas perturbée par l'information secrète insérée. La capacité définit la quantité D'information qui peut être intégrée dans le support sans détérioration visible. Ces Trois caractéristiques sont en relation étroite et inverse [3]. Dans notre projet, nous allons introduire une méthode de masquage des informations de stéganographie pour masquer un message dans une image et nous avons utilisé, testé un algorithme. Le but de notre projet est d'insérer du texte dans une image où la perception humaine ne peut pas détecter les petits changements apportés à l'image qu'elle est censée contenir. Le premier chapitre donne une idée générale sur la représentation des images numériques ainsi il donne quelques notions de base, et une définition de ses différentes propriétés. Dans le deuxième chapitre, notre étude porte spécifiquement sur la stéganographie d'information dans les images numériques, nous introduisons la « stéganographie » Principes et ces caractéristiques. Ensuite, nous avons abordé cette fonctionnalité et l'avons comparée au tatouage numérique, et à la fin de ce

chapitre, nous avons parlé de La stéganalyse. Le troisième chapitre est exclusivement consacré à la présentation de notre méthode de travail, nous avons d'abord procédé à une démonstration des outils et méthodes utilisés, Puis nous avons présenté l'application de stéganographie et les résultats obtenus.

Chapitre I

Généralité sur l'image numérique

Introduction:

L'image peut utiliser comme un utile de communication entre eux. Elle est très utile dans tous les domaines tel que scientifique, l'astronomie….. etc.

L'image est l'élément le plus impactant des éléments composants vos supports de communication. Viennent ensuite les textes et le format du support. Que notre cerveau percute immédiatement à la vue d'une photo.[1]

Le traitement d'images désigne une discipline de l'informatique et des mathématiques appliquées qui étudie les images numériques et leur transformation dans le but d'améliorer leur qualité ou d'en extraire de l'information.[2]

Dans Ce chapitre, on va présenter quelques concepts de base sur les images numériques comme : la définition D'image numérique, ses types et caractéristiques, sa formation et en dernier lieu ces différents formats.

I.1 Image numérique:

La notion d'image très large, c'est une représentation concrète ou abstraite d'un objet, d'un être vivant ou encore d'un concept. [3]

L'image numérique désigne toute image (dessin, icône, photographie…) acquise, créée, traitée et stockée sous forme binaire. Créée directement par des programmes informatiques. Elle signifie un tableau de pixel et chaque pixel est codé par un nombre binaire pour un niveau de gris, ou par trois nombres binaires qui correspond à une nuance de rouge, de vert et de bleu (codage RVB). [4]

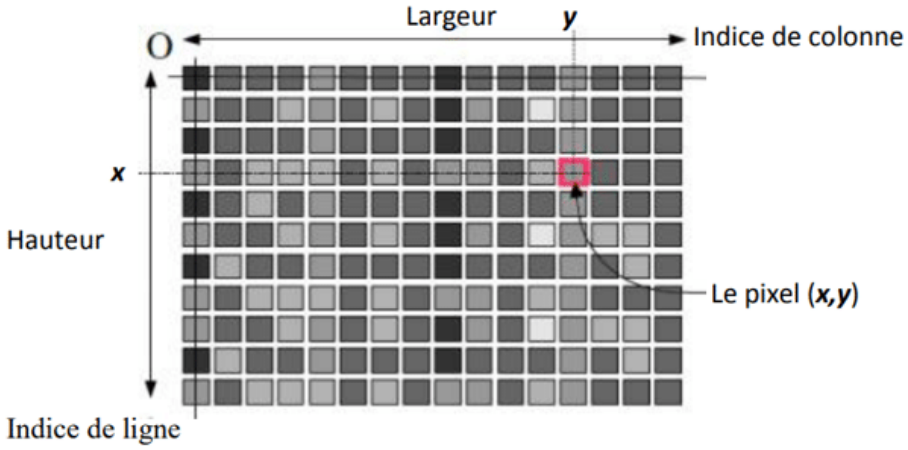


Figure I.1 : Représentation d'une image numérique [5]

I.2 Représentation de l'image numérique:

L'image numérique est constituée d'un ensemble de points appelés pixels. Un pixel (abréviation de Picture élément) est défini comme le plus petit élément constitutif d'une image numérique matricielle. Pour une image à deux tons, noir et blanc, le pixel peut être codé par un seul bit codant (0 pour noir ou 1 pour blanc). Pour des images en nuances de gris ou en couleurs le pixel peut être codé par 2, 4, 8, 16, 24 ou 32 bits. [6]

I.2.1 L'échantillonnage:

L'échantillonnage est une étape fondamentale qui doit prendre en compte Le contenu de l'image à analyser. Intuitivement, on conçoit bien qu'une structure fine, c'est-à-dire une partie de l'image comportant des oscillations avec De petites périodes spatiales, nécessitera plus de pixels qu'une partie présentant Moins de variation.[6]

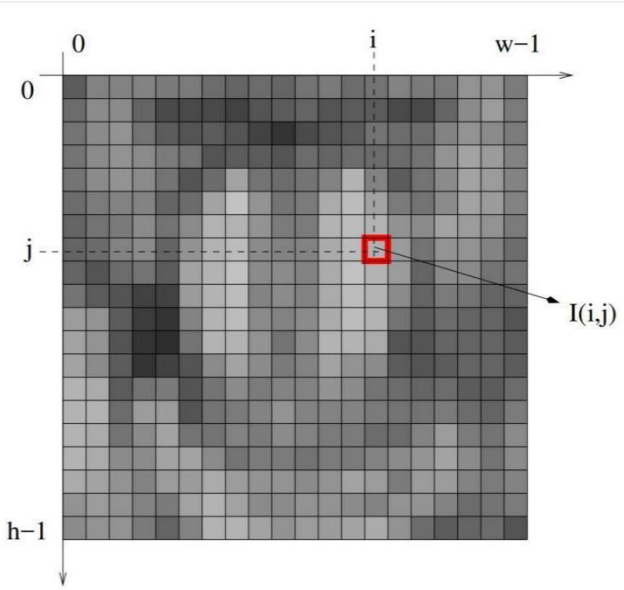


Figure I.2 : Représentation de l'échantillonnage[5]

I.2.2 La 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 apparaître des distorsions dans les images.[6]

I.3 Les Types d'image:

I.3.1 Image vectorielle:

Une image vectorielle est une image numérique qui peut être agrandie ou rétrécie à l'infini sans jamais perdre de sa qualité. Les images vectorielles sont créées à partir de formules mathématiques et sont essentiellement constituées de formes géométriques qui peuvent être étirées ou courbées à souhait.[7]

Figure I.3 : Image vectorielle **[**8]

- **Avantage:**

- Les images vectorielles peuvent être agrandies ou rétrécies à l'infini sans perdre de leur qualité.
- Les éléments mathématiques des vecteurs permettent de créer des lignes nettes et des courbes parfaites, ce qui est idéal pour créer un design épuré et symétrique**.**
- Les fichiers vectoriels sont généralement moins gros que les fichiers matriciels.[7]

- **Inconvénients:**

- Les vecteurs ne permettent pas de créer des dégradés de couleurs ou des effets d'ombres complexes. Les designs vectoriels sont donc plus plats et font parfois penser aux bandes dessinées.
- Les vecteurs sont par nature nets et précis. Il peut donc être difficile de créer un design imparfait rappelant les illustrations réalisées à la main.

- Les logiciels vectoriels ne sont pas aussi intuitifs que les autres médiums artistiques et nécessitent un certain temps d'apprentissage.[7]

I.3.2 Image matricielle:

Une image matricielle est un « objet » numérique constitué de pixels, c'est-à-dire de tous petits carrés de couleur composés d'un mélange de lumière rouge, verte et bleue (également connus sous le nom de sous-pixels). Ces pixels forment une grille statique.[7]

Figure I.4: Image matricielle **[**8**]**

- **Avantage:**

- Les images matricielles sont idéales pour mettre en avant les nuances de couleurs, les dégradés et les ombres d'une image (lorsque vous éditez une photo ou une image réaliste), car elles contiennent une grande quantité d'informations sur la couleur.
- Vous pouvez zoomer sur une image matricielle pour modifier l'image pixel par pixel.
- De nombreux effets de textures fonctionnent mieux (ou seulement) avec les images matricielles.[7]

- **Inconvénients:**

- Le fait que les images matricielles contiennent une grande quantité de pixels et de couleurs signifie qu'il peut être difficile de masquer une portion d'une image seulement.
- Les fichiers matriciels prennent plus de place que les fichiers vectoriels.
- Les images matricielles ne peuvent pas être agrandies à l'infini. Il faudrait par exemple un immense fichier contenant une très grande quantité de pixels pour créer un panneau publicitaire à partir d'une image matricielle.
- Vous devez déterminer à l'avance la taille de l'image dont vous aurez besoin, et perdez donc l'option de changer l'échelle plus tard si vos besoins venaient à changer. [7]

I.3.3 Image à niveaux de gris :

Niveaux de gris d'une image numérique C'est une image dans laquelle chaque pixel de couleur est converti en un pixel gris Puis l'image devient noir et blanc ce qui est unique, c'est qu'il fournit moins d'informations pour chaque pixel. 256 valeurs possibles pour chaque pixel.[8]

I.3.4 Images en couleur :

La photo couleur se compose en fait de trois photos Il est représenté par le rouge, le vert et le bleu chacune de ces trois images est appelée un canal..

[8]

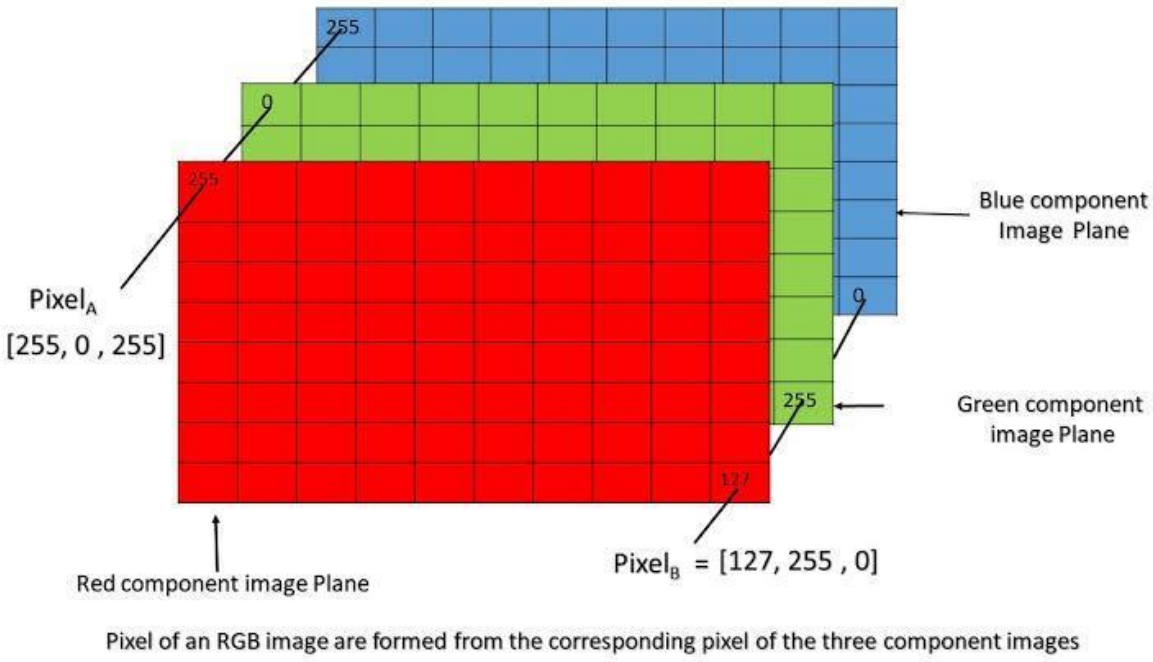


Figure I.5: Présentation des pixels couleur

I.4 Caractéristiques des images numériques:

- **Le pixel :**

Le pixel sont le plus petit composant d'une image numérique Il existe dans une matrice à deux dimensions (Largeur et hauteur). [9]

- **La définition :**

La dimension ou la définition de l'image correspond à la taille de cette image, et c'est sous la forme d'une matrice dont les éléments sont des valeurs numériques, le nombre total de pixels dans une image est égal :

Le nombre de lignes de la matrice × le nombre de colonne [9].

Figure I.6: Image de 30 x 20 pixels : faible définition Dimension réelle sur le document : 2 x 1,33 pouces

Figure I.7 : Image de 120 pixels par 80 pixels : haute définition Dimension réelle sur le document : 2 x 1,33 pouces

- **La résolution :**

La résolution de l'image est le nombre de pixels par pouce qu'elle contient (1 pouce = 2,54 cm). Il est exprimé en "DPI", plus il y a de pixels (ou de points) par pouce, plus l'image contient d'informations (plus elle est précise). Exemple pour comprendre : Une résolution de 200 dpi signifie que l'image a 200 pixels de largeur et 200 pixels de hauteur, donc elle est composée de 40 000 pixels (200 x 200 dpi). Grâce à cette formule, il est facile de connaître la taille maximale d'impression [10,11].

I.5 Codage et représentation des couleurs :

Est essentiel d'avoir un moyen de choisir la bonne couleur qui est utilisable. Bien que la gamme de couleurs possible soit très large et que la chaîne de traitement de l'image passe par différentes extensions : par exemple un numériseur (scanner), puis un fichier, un logiciel de retouche photo et enfin une imprimante. Il faut donc pouvoir représenter efficacement la couleur pour assurer la cohérence entre ces différentes couleurs périphériques. Il existe de nombreux espaces colorimétriques donc les plus célèbres sont :

- **Le codage RGB :**

L'écran utilise un codage RVB (Rouge, Vert, Bleu). Ce système, basé sur la combinaison additive des couleurs, représente chacune avec ses niveaux de rouge, de vert et de bleu. Chacun de ces niveaux est encodé avec un nombre allant de 0 à 255. On trouve donc 256 x 256 x 256 = 16 777 216 couleurs. 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. [11]

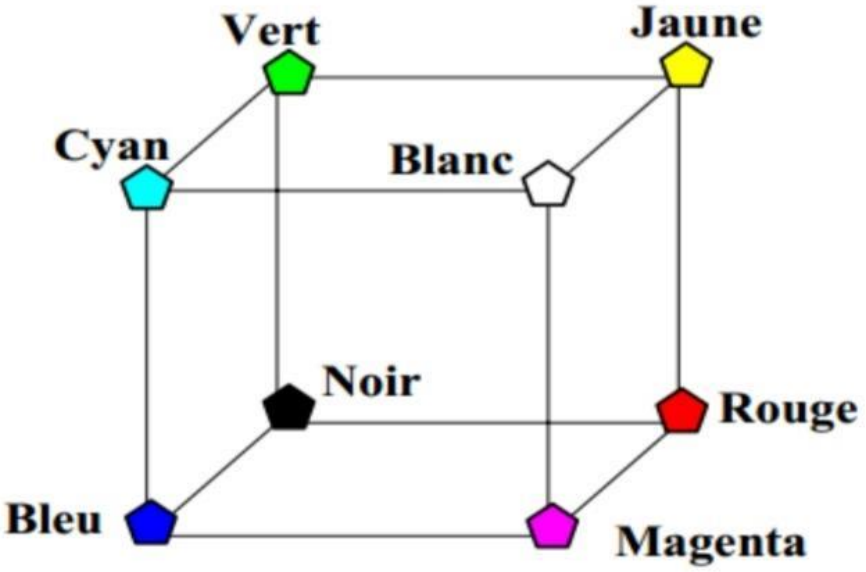


Figure I.8 : Le codage RGB

• Le codage TSL (HSL) :

Le système **T**einte – **S**aturation –**L**uminosité (Hue-Saturation-Luminance en Anglais) a été conçu pour faciliter le choix des couleurs grâce à un codage naturel, plus proche de nos habitudes. Chaque couleur est définie par trois paramètres:

La Teinte: couleur choisie sur un cercle chromatique déroulant toutes les couleurs du rouge au violet. (0 à 360°)

La Saturation: l'intensité de la couleur (0 à 100%)
La Luminosité: couleur plus ou moins claire. (0 à 100%)[12].

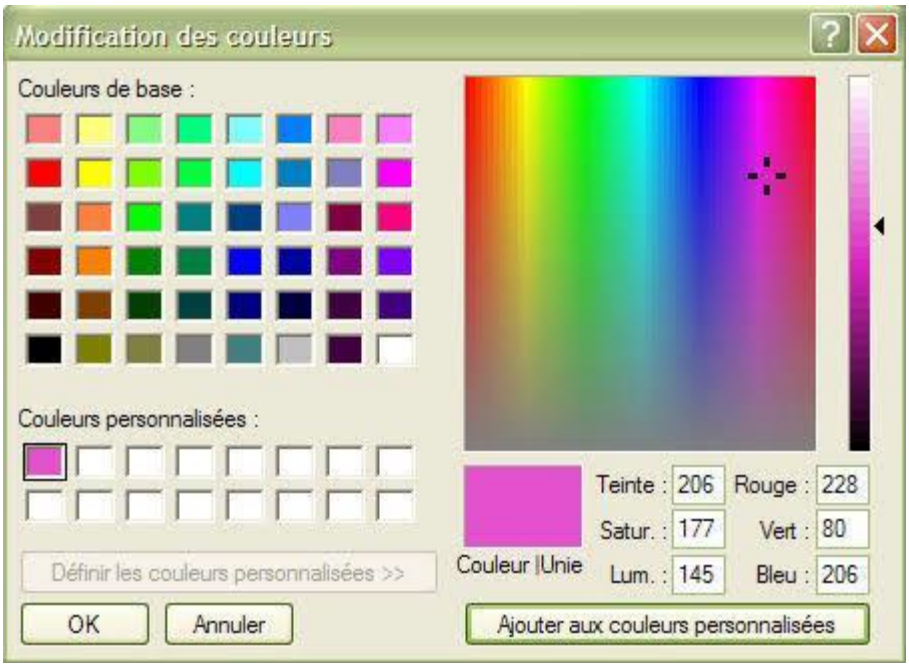


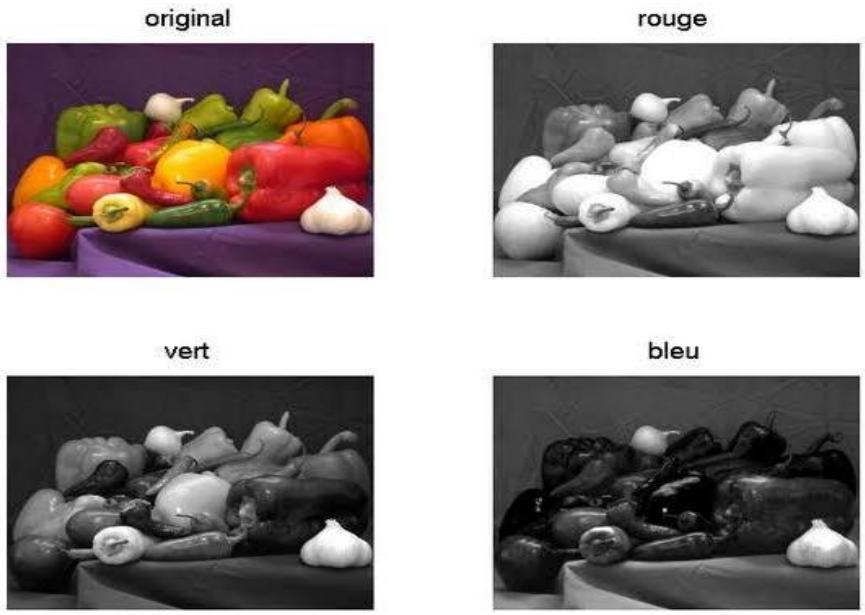
Figure I.9: Représentation graphique du codage HSL

- **Codage CMY :**

Le codage CMY (Cyan, Magenta, Yellow), est utilisé principalement pour l'impression et basé sur la synthèse soustractive contrairement au RGB.
Ce modèle consiste à décomposer une couleur en valeurs de Cyan, de Magenta et de Jaune[13].

- **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 (chro-minance : 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[14].



FigureI.10 : 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[14] :

$$Y = 0.299R + 0.587G + 0.114B$$
$$U = -0.615R - 0.289G + 0.436B = 0.492\ B - Y$$
$$V = 0.615R - 0.515G - 0.100B = 0.877(R - Y)$$

I.6 Déférents formats d'images :

- **Le format PNG :**

Le format .png est idéal pour les images, mais ne convient pas à l'impression. Vous pouvez modifier une image sans perte de qualité. Cependant, cela reste un format d'image à basse résolution. Son principal inconvénient est sa taille qui le rend très long à télécharger. Par exemple, il est au moins 7 fois plus lourd qu'un fichier .jpeg .

Il ne permet pas l'animation ou le stockage de plusieurs fichiers dans un seul fichier, en fait grâce au format .png, vous pouvez enregistrer votre image avec plus de couleurs sur un fond transparent pour une vue plus claire.

- **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 . 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. [15]

- **Le format GIF (Graphics Inter change Format) :**

Développé par **Compuserve**, il présente deux avantages principaux :
Portabilité et indépendance par rapport au système d'exploitation, facilité et rapidité de lecture. Ce format est utilisé pour les images 8 bits, avec ou sans transparence, fortement compressées pour réduire le temps de transfert des fichiers. [16]
Il convient mieux aux images qui ne nécessitent pas une grande palette de couleurs (niveaux de gris ou 256 couleurs). Le format GIF permet de stocker plusieurs images bitmap dans un seul fichier. Une telle application qui s'est avérée très efficace est WEB.

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

Il s'agit d'un format de fichier bitmap utilisé comme format de fichier natif pour l'application **PC Paintbrush**. Développé par **ZSoft** Corporation , Il a été adopté comme format de fichier d'imagerie principal avant l'avènement de BMP, JPEG et PNG Les fichiers PCX sont plus petits car ils sont compressés à l'aide de l'encodage RLE (Run Length Encodingdans) dans les données d'image [16] .

- **Le format CGM (Computer Graphics Meta file) :**

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

- **Le format BMP :**

BMP est le format d'image standard créé par Microsoft et IBM, et utilisé par Windows par programme bitmap.

Conçu spécifiquement pour les ordinateurs (PC) et pour une utilisation dans l'environnement Windows et OS / 2.

C'est un format ouvert et non compressé, il est lourd et ne prend pas en charge les calques ou la transparence [15].

- **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.

Conclusion :

Dans ce chapitre, nous avons essayé de résumer les concepts de base de Le traitement numérique de l'image, et nous avons introduit les concepts d'image numérique et ses différentes propriétés (définition, résolution, poids, etc.) ainsi que la représentation des couleurs.

Chapitre II
La Stéganographie

Introduction :

Développement technologique au fil du temps dans le domaine de l'informatique et des télécommunications soulevé de nombreux problèmes de sécurité de l'information. Dans notre travail, nous nous concentrerons sur la question de la sécurité de l'envoi d'informations confidentielles sous Forme numérique, principalement basée sur la science du camouflage et de la dissimulation [17].

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, de telles sortes 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 [18].

Dans ce chapitre, nous allons parler sur la stéganographie, sa définition, son principe, ses différents types et domaines, ainsi que ses caractéristiques…etc.

II.1 Définition de la stéganographie :

La stéganographie est une technique consistant à dissimuler un message ou des données à l'intérieur d'un autre fichier (texte, image, audio, vidéo…). Elle diffère en cela de la cryptologie, où le message n'est pas caché mais rendu inintelligible sans un code de décryptage [19].

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 [20].

Figure II.1 : Exemple de stéganographie à l'aide de lait

II.2 Structure d'une communication secrète:

La stéganographie complète repose sur deux procédés :

- **La dissimulation :**

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

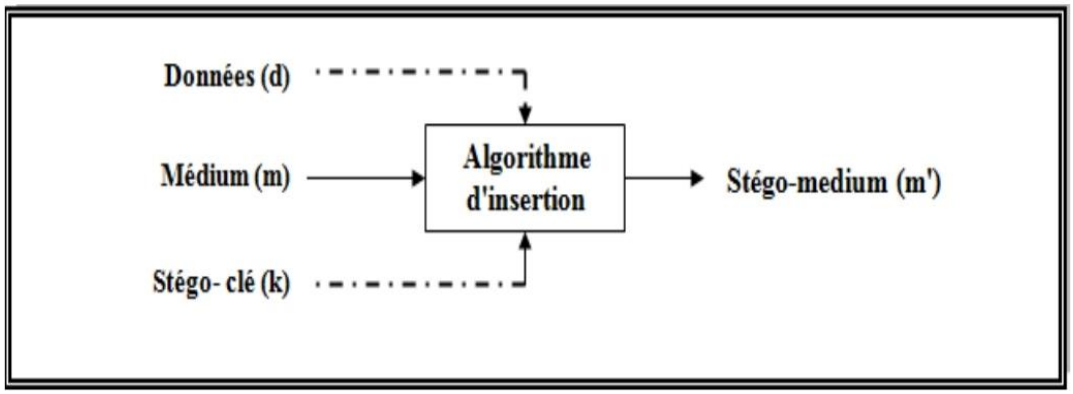


Figure II.2 : dissimulation des données dans le médium [21].

- **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 médium) dans le stégo-médium, sans pour autant vouloir l'extraire comme illustre la figure suivante :

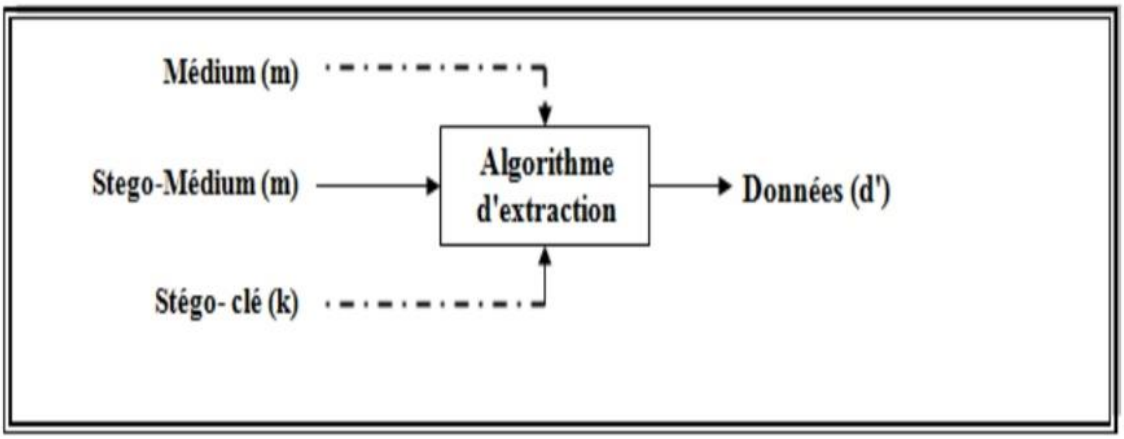


Figure II.3 : Extraction des données du médium [21].

II.3 Les différents types et supports de Stéganographie :

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

II.3.1 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 étrange [22].

Il existe plusieurs formes de stéganographie linguistique :

a) **Sémagrammes :**

C'est la forme la plus connue [17], il utilise uniquement des symboles et des signes pour masquer les informations. Il est en outre classé en deux manières [22]:

1) Sémagrammes visuels : Un sémagramme visuel utilise des objets physiques utilisés quotidiennement pour transmettre un message. Par exemple : le positionnement des articles sur un site Web particulier.

2) 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 [22].

a) Open Code :

Cela cache un message dans un message de transporteur légitime d'une manière qui n'est pas évidente pour un observateur sans méfiance [23].
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 [17].

b) Ponctuation :

Les prisonniers de guerre ont utilisé la ponctuation (points et virgules) pour transmettre des messages à leurs familles [17].

c) Nulle :

Chiffrement couvert : Le chiffrement couvert ou caché cache ouvertement un message dans le support du support afin qu'il puisse être récupéré par quiconque connaît le secret de la façon dont il a été caché.

*Cryptage nul : Le cryptage nul masque le message selon un ensemble de règles, telles que "lire les cinq mots" ou "regarder la troisième lettre de chaque mot".

*Cryptage du réseau : le cryptage du réseau utilise un modèle utilisé pour couvrir le message du transporteur, Les mots qui apparaissent dans les trous des dés sont le message caché.

Avec pour principe de mettre en avant certains personnages pour le texte avec une piqûre d'aiguille ou la hauteur des lettres. Alors assez pour assemblez ces lettres surlignées pour former un mot ou une phrase pour le premier cas, et dans le second cas, deux tailles de caractères sont utilisées, et la lettre est constituée d'un fichier les lettres sont soit en minuscules, soit en majuscules, selon l'accord adopté pour l'échange [17] [23].

II.3.2 La stéganographie technique :

La stéganographie technique utilise des outils spéciaux, des dispositifs ou des méthodes scientifiques pour cacher un message. Dans ce type, on peut utiliser de l'encre invisible, des micropoints, des méthodes informatiques ou diverses cachettes pour garder le message secret [24]

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 [25].

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 [25] :

- 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 [22].
- 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 [22].

- 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 [22].

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 [22].

II.4 Caractéristiques:

Le système de tatouage et stéganographie est caractérisé à trois limitations importantes :
la capacité, Sécurité (in-détectabilité), la robustesse dirige son utilisation [26]:

II.4.1 La capacité :

La capacité d'une méthode de stéganographie est définie par la taille en bits d'une marque qui peut être intégré dans un document de taille donnée. De ce fait, on déduit que la capacité d'insertion relative est la relation entre la taille du message secret et la taille du médium utilisé [27].

II.4.2 L'imperceptibilité :

Une marque est dite imperceptible si toute personne est incapable de faire la différence entre le support original et le support marqué. C'est à dire la différence ne doit pas être visible. L'objectif est qu'une tierce personne en dehors des personnes concernées par le message ne détecte pas l'existence de l'information cachée des tests visuels sont pratiqués pour certifier ce caractère d'invisibilité. Lors de ces tests, des supports marqués et non marqués sont présentés aléatoirement aux sujets qui doivent déterminer lequel a la meilleure qualité.

II.4.3 La robustesse :

Spécifie la capacité qu'a notre message reste intacte après que le conteneur ait subit des modifications [30].

II.5 Domaines de stéganographie :

La stéganographie est divisée en deux domaines, spatial et fréquentiel. Dans le domaine spatial, le message secret est inséré dans les pixels de l'image porteuse, tandis que dans le domaine fréquentiel, les pixels sont transformés en coefficients, et le message secret est inséré dans ces coefficients. [17]

II.5.1 Domaine spatial :

La stéganographie spatiale consiste à faire changer des 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 répandue. Elle consiste à cacher un message secret dans les bits de poids faible des pixels de l'image, de sorte que les distorsions apportées par le processus d'insertion restent non perceptibles. Les variations de la valeur du LSB sont quasiment imperceptibles. L'insertion de bits de message secret peut être faite séquentiellement ou de façon pseudo aléatoire. La stéganographie par substitution de LSB et la stéganographie par correspondance de LSB sont des exemples de techniques de stéganographie dans le domaine spatial.[17]

II.5.2 Domaine fréquentiel :

Le message est inséré dans les coefficients transformés de l'image, ce qui a pour effet d'apporter plus de robustesse contre les attaques. La stéganographie fréquentielle est une technique essentielle de dissimulation de l'information secrète la plupart des systèmes de stéganographie opèrent dans le domaine fréquentiel, va ainsi permettre de cacher l'information dans des zones de l'image moins sensibles à la compression, au recadrage et aux divers traitements de l'image. [17]

II.6 Utilisation de la stéganographie :

1- La stéganographie peut être une solution qui la rend applicable pour envoyer des nouvelles et des données sans être censuré et sans craindre que les messages soient bloqués et remontent jusqu'à nous.

2- Il est simplement la stéganographie utilisé pour enregistrer des données sur un emplacement. Par exemple, plusieurs sources d'informations comme les informations bancaires privées, certains secrets militaires, peuvent être enregistrées dans une source de couverture. Lorsqu'il est nécessaire de dévoiler les données secrètes dans la source de couverture, cela peut simplement révéler les informations bancaires et il sera impossible de valider l'existence des secrets militaires à l'intérieur.

3- La stéganographie peut être généralement utilisée pour effectuer un tatouage. Bien que le concept de filigrane ne soit certainement pas de la stéganographie. Plusieurs approches stéganographique sont utilisées pour enregistrer des filigranes dans les données.

4- Le transport d'informations réactives est une autre utilisation clé de la stéganographie. Il permet de transporter des informations réactives au-delà des oreilles indiscrètes sans qu'ils comprennent qu'aucune information réactive ne les a transmises. Le concept d'utilisation de la stéganographie dans le transport de données ne peut être utilisé que pour n'importe quelle approche de transport de données, du courrier électronique aux images sur les sites Internet.

5 - Elle peut être couplée aux moyens de communication actuels, la stéganographie peut être utilisée pour accomplir des échanges cachés. Les gouvernements s'intéressent à deux types de communications cachées telles que celles qui soutiennent la sécurité nationale et celles qui ne le font pas. La stéganographie numérique prend en charge le grand caché pour les deux types. Les entreprises peuvent avoir les mêmes préoccupations concernant les secrets commerciaux ou les nouvelles données sur les produits. [31]

II.7 Les techniques de la stéganographie :

Examinons de plus près un échantillon des techniques disponibles:

- 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.

- **Bit le moins significatif:**

(LSB) Cette phrase sonne presque comme un dénigrement. Cependant, dans ce cas, il s'agit de pixels. Les pixels de l'image en niveaux de gris sont divisés en huit bits, et le dernier bit le huitième est appelé le bit le moins significatif. Les pirates utilisent ce bit pour intégrer du code malveillant car la valeur globale du pixel sera réduite d'un seul et l'œil humain ne peut pas détecter la différence dans l'image. Ainsi, personne n'est même conscient que quelque chose ne va pas, et que l'image porte quelque chose de dangereux à l'intérieur.

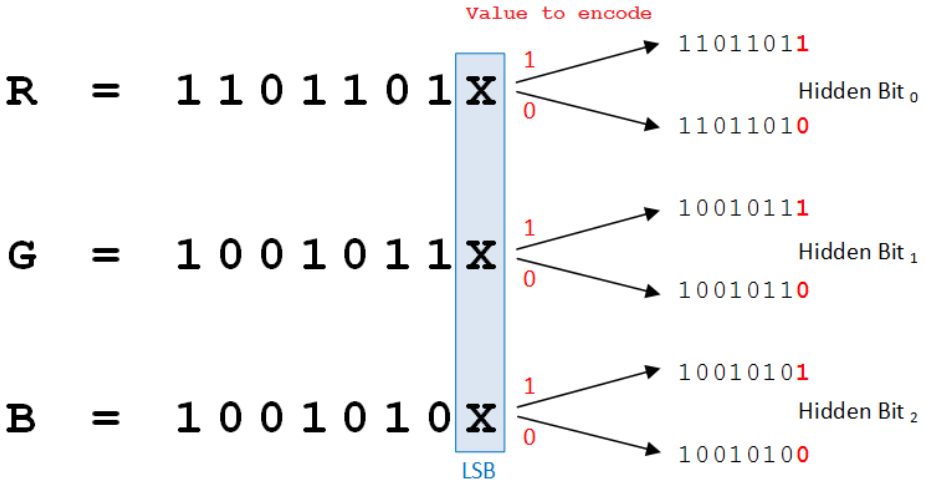


Figure II.4: Exemple de conversion LSB **[**33**]**

- Technique basée sur la palette :

Comme la technique du bit le moins significatif, la technique basée sur la palette s'appuie également sur des images. Les pirates intègrent leur message dans des images basées sur des palettes telles que des fichiers GIF, ce qui rend difficile la détection de l'attaque par les chasseurs de menaces de cyber sécurité ou les pirates éthiques.[32]

II.8 Comparaison entre les techniques de la dissimulation de données:

II.8.1 Stéganographie vs Cryptographie:

La stéganographie ou couverture de l'écriture, est une méthode dans laquelle une méthode secrète est convertie en faux message. Cette technique permet de garder un message secret. Il est assez difficile à utiliser et à comprendre. La structure des données reste inchangée en stéganographie. Il est utilisé dans le texte, l'audio, la vidéo ou les images. [34]

La cryptographie, ou écriture secrète, est une méthode dans laquelle une méthode secrète est convertie en texte chiffré et envoyée à une autre personne qui déchiffre ensuite le texte chiffré en texte brut. La cryptographie peut être classée comme cryptographie à clé symétrique ou cryptographie à clé asymétrique. [34]

II.8.2 Stéganographie vs tatouage numérique :

Le tatouage est l'art d'altérer un média (un texte, une image, un son, une vidéo...) de sorte qu'il contienne un message le plus souvent en rapport avec le média et le plus souvent de manière imperceptible et robuste. [35]

• La stéganographie est l'art de dissimuler au sein d'un support anodin une information qui bien souvent est sans rapport avec le support hôte. Cette dissimulation se fait de sorte que la présence même du message soit insoupçonnée. Autrement dit, la dissimulation doit être indétectable visuellement et statiquement. [35]

II.9 La métrique d'évaluation algorithme de stéganographie :

Le PSNR est une mesure de distorsion utilisée en image numérique, tout particulièrement en compression d'image. Elle permet de quantifier la performance des codeurs en mesurant la qualité de reconstruction de l'image compressée par rapport à l'image originale. [36]

II.9 La stéganalyse:

C'est un processus inverse de la stéganographie vise à révéler toute donnée cachée dans un support. il y a deux méthodes de détection des fichiers modifiés. L'une s'appelle l'analyse visuelle, qui implique comparer un fichier suspect avec la copie originale. Il entend révéler la présence de communication secrète par inspection, soit visuellement, soit à l'aide d'un système informatique, décomposant généralement l'image en ses plans de bits. Bien que cela la méthode est très simple, elle n'est pas très efficace ; la plupart du temps, la copie originale est indisponible. [17]

Conclusion:

Dans ce chapitre, nous avons présenté une explication simple sur la stéganographie, et nous avons mentionné quelques points importants dans notre sujet, tels que l'art sur la stéganographie des images numériques et ses différents types.

Chapitre III

Application et discussion

Introduction:

Dans ce chapitre, nous présentons l'implémentation et la conception de notre application à partir de la stéganographie.
Nous avons expliqué en détail toutes les étapes pour réaliser cette application et les outils utilisés dans celle-ci. L'étude vise à évaluer les performances de notre algorithme du Stéganographie.

III.1 Outils utilisés:

Nous avons implémenté notre application stéganographique, dans l'environnement de programmation Netbeans, qui permet de créer des applications complètes. Il peut également servir à créer un petit module d'application.

III.1.1 Java:

Java est un langage de programmation et une plate-forme de calcul Lancé par Sun Microsystems en 1995.Il s'agit d'un langage de programmation rapide, sécurisé et fiable qui permet de tout coder, des applications mobiles aux logiciels d'entreprise en passant par les applications de big data et les technologies côté serveur.[37]

III.1.2 Netbeans:

Netbeans est un environnement de développement intégré (EDI), placé en open source par Sun en juin 2000 sous licence CDDL (Common Développement and Distribution License) et GPLv2. En plus de Java, Netbeans permet la prise en charge native de divers langages tels le C, le C++, le JavaScript… Etc. Il offre toutes les facilités d'un IDE moderne (éditeur avec coloration syntaxique, projets multi-langage, refactoring, éditeur graphique d'interfaces et de pages Web). Compilé en Java, Netbeans est disponible sous Windows, Linux, Mac OS X ou sous une version indépendante des systèmes d'exploitation. Netbeans constitue par ailleurs une plateforme qui permet le développement d'applications spécifiques (bibliothèque Swing (Java)). L'IDE Netbeans s'appuie sur cette plate-forme.

III.2 Méthode utilisé :

Il existe des 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 dernier 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.

III.2.1 Présentation de la méthode:

III.2.1.1 La méthode LSB :

La méthode de stéganographie dite LSB consiste à manipuler les bits de poids faible d'un fichier afin de cacher informations dans celui-ci sans altérer son apparence. Est la technique de Stéganographie d'image la plus connue [39].

La méthode d'insertion de données sur les bits de poids faible ou LSB. Son principe est d'utiliser le dernier bit de chaque nombre définissant l'intensité d'une couleur primaire d'un pixel, pour les données à dissimulées. Ainsi, trois bits peuvent être encodés dans chaque pixel, et la différence de couleur obtenue est imperceptible pour l'œil [40].

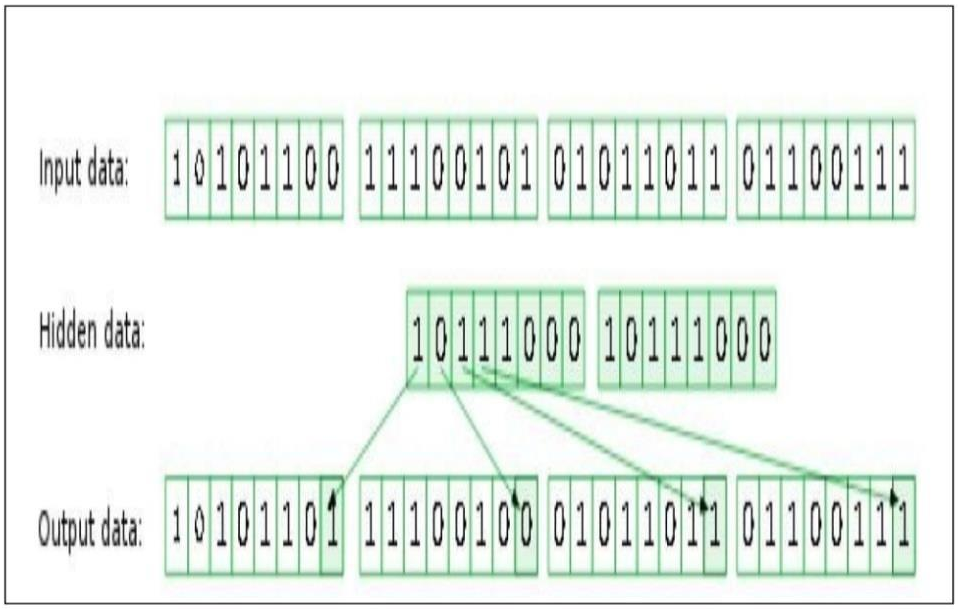


Figure III.1 : méthode LSB

III.2.1.2 L'architecture de la méthode LSB :

Dans une architecture stéganographique, il y a principalement deux éléments. D'un côté un processus de dissimulation, de l'autre un processus de recouvrement.

III.2.2 Insertion d'un message:

L'algorithme de la technique proposée se déroule comme suit:

Étape 1 : Nous insérons une image couleur RGB.

Étape 2 : Convertir le texte en Binary.

Étape 3 : Pour chaque pixel R (I, j), B (I, j), G (I, j), Remplacer le bit de poids faible de R (I, j) par le premier bit de texte.

Étape 4 : Remplacer le bit de poids faible de G (I, j) par le deuxième bit de texte.

Étape 5 : Remplacer le bit de poids faible de G (I, j) par le troisième bit de texte.

Étape 6:Convertir les couleurs au système décimal.

Étape 7 : Après avoir ajouté les nouvelles couleurs, nous enregistrons l'image .

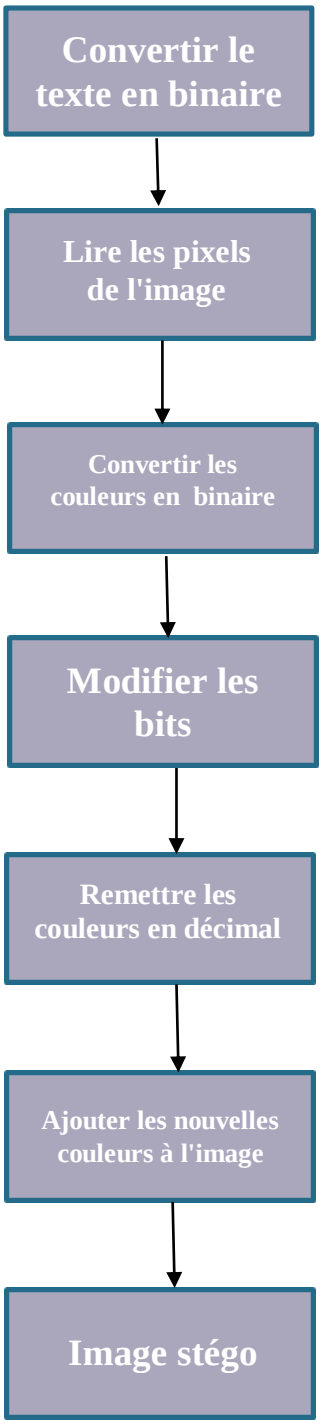


Figure III.2 : Organigramme d'insertion du texte

III.2.3 Extraction d'un message :

L'extraction de la marque se fait sans recours à l'image originale.

Étape 1 : Lire l'image dans laquelle le message est caché.

Étape 2 : Lire les pixels de l'image Pour chaque pixel R, G et B.

Étape 3 : Conversion des couleurs au système Binary.

Étape 4 : Lire le dernier bit de chaque couleur.

Étape 5 : Transformé les bits en une suite de caractères lisible

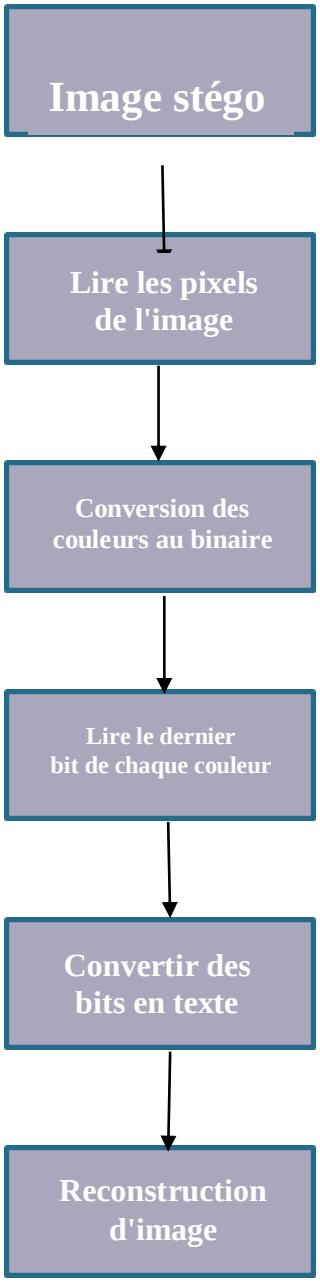


Figure III.3 : Organigramme d'extraction du texte

III.3 Présentation de l'application réalisée:

Dans cette partie, nous présentons les caractéristiques matérielles utilisés dans notre travail:

III.3.1 Les Caractéristiques matérielles:

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

Un ordinateur HP EliteBook2570p caractérisé par :

- **Processeur : Intel (R) Core(TM) i5-3210M CPU @ 2,50 GHz**
- **RAM : 4,00 GO de RAM**
- **Système d'exploitation : Windows 10 Professionnel**

III.3.2 Interface graphique :

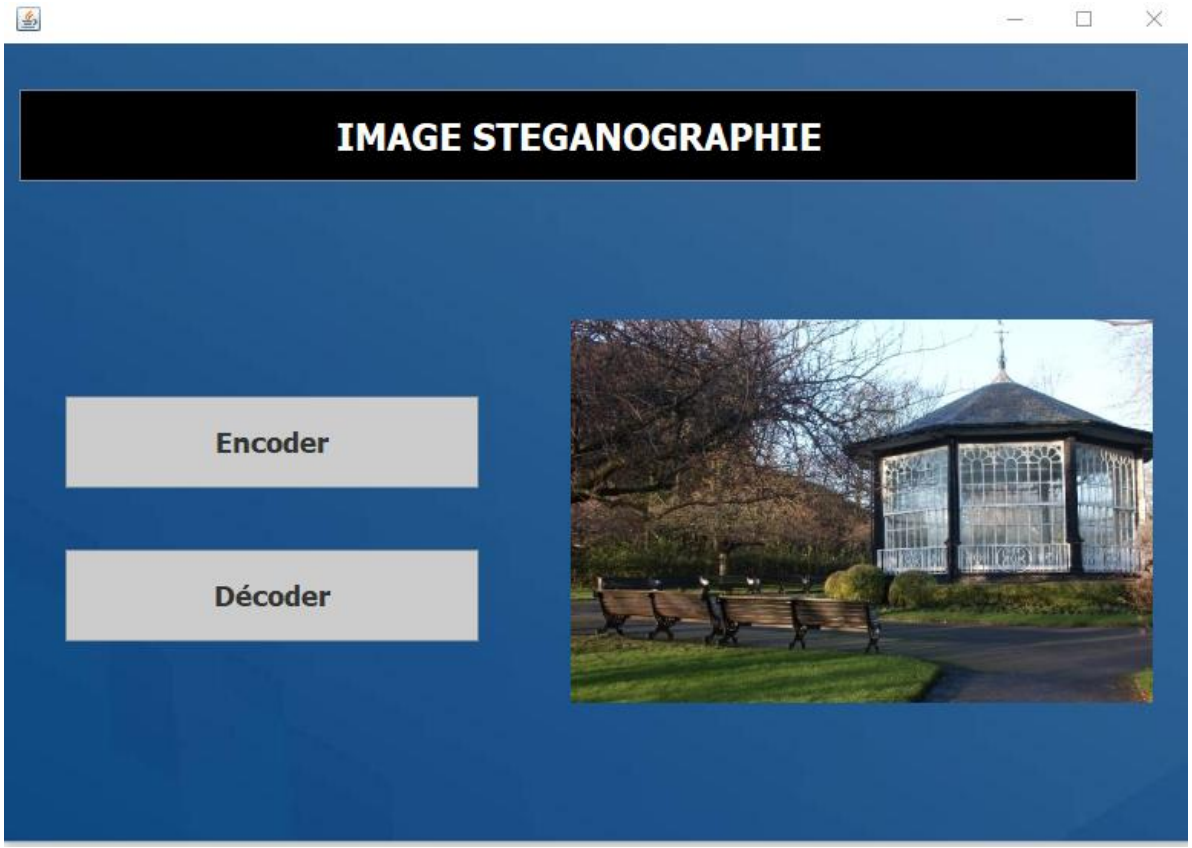


Figure III.4 : Interface graphique de l'application

L'interface de notre application contient deux boutons, le premier est "Encoder" et le deuxième "Décoder", comme il est présenté dans la figure précédente.

-Si nous appuyons sur le bouton "ENCODER", cela nous mènera à l'interface de cacher les messages.

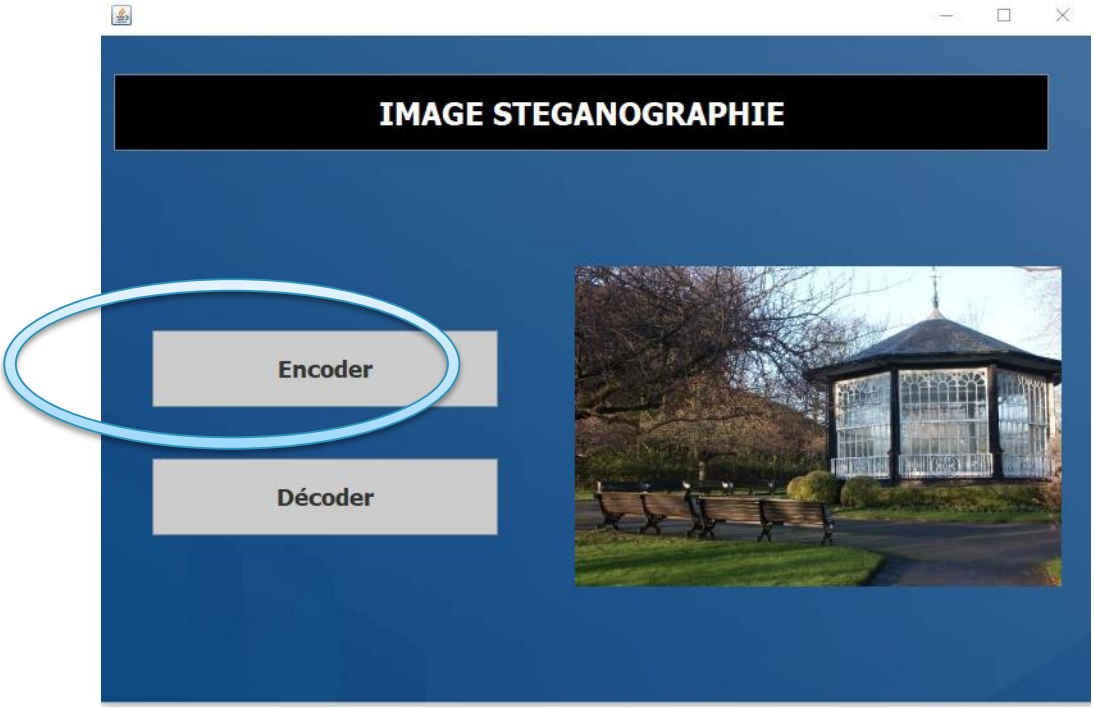


Figure III.5: Bouton pour la page de cacher un message

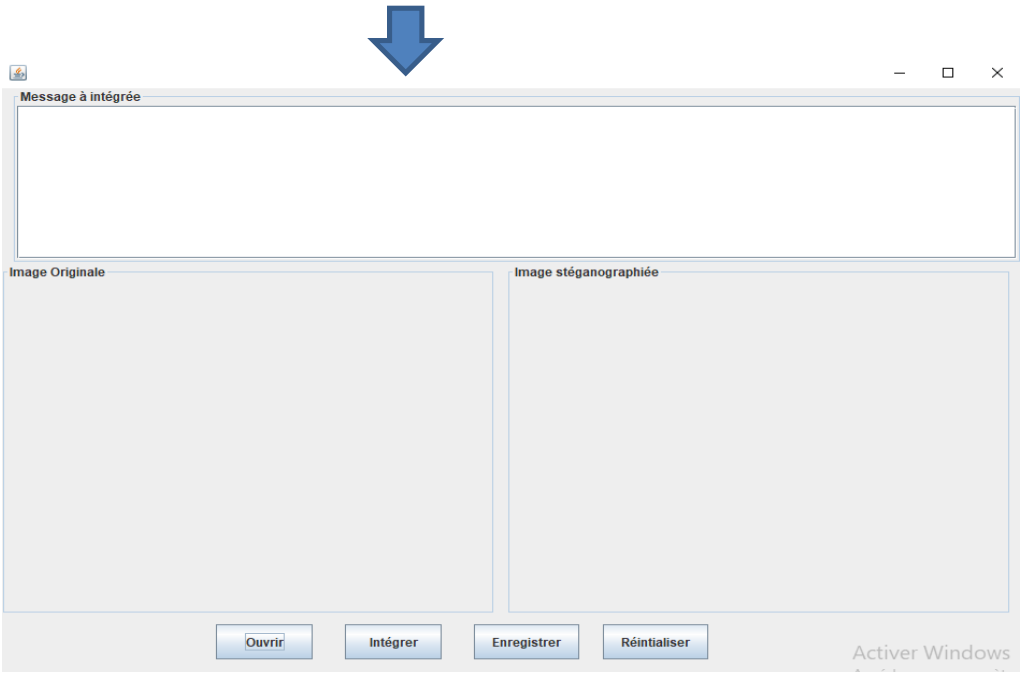


Figure III.6: Interface de cacher un message

- Et si nous appuyons sur le bouton "DECODER", cela nous mènera à l'interface de détecter les messages cachés.

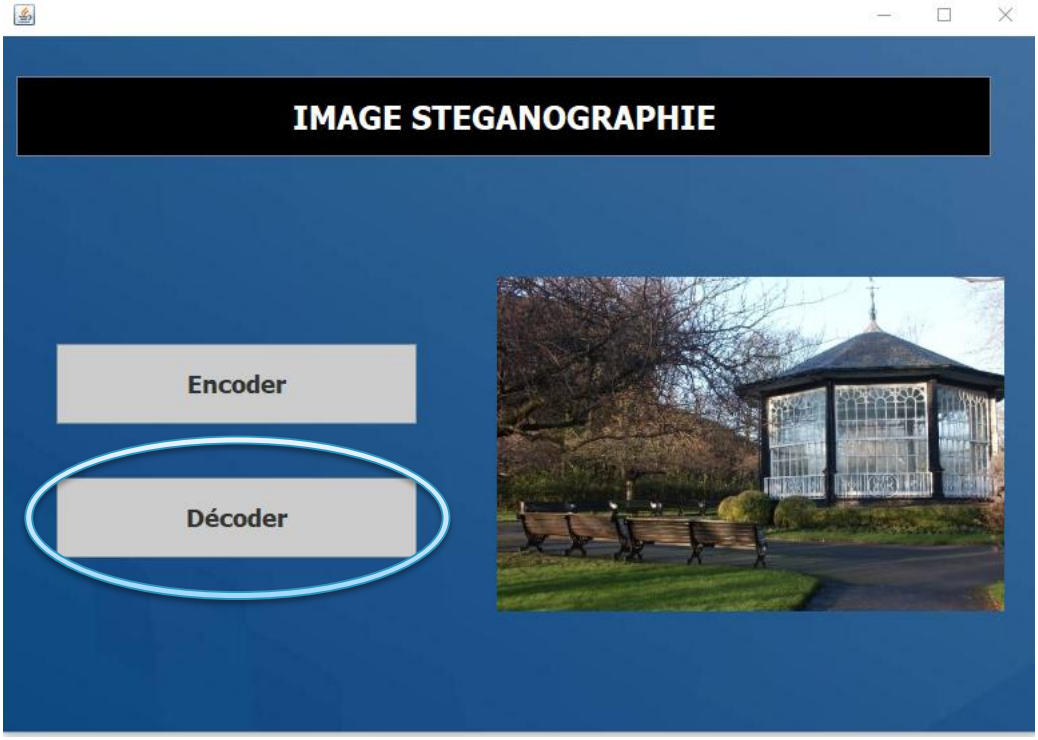


Figure III.7: Bouton pour la page de décoder le message

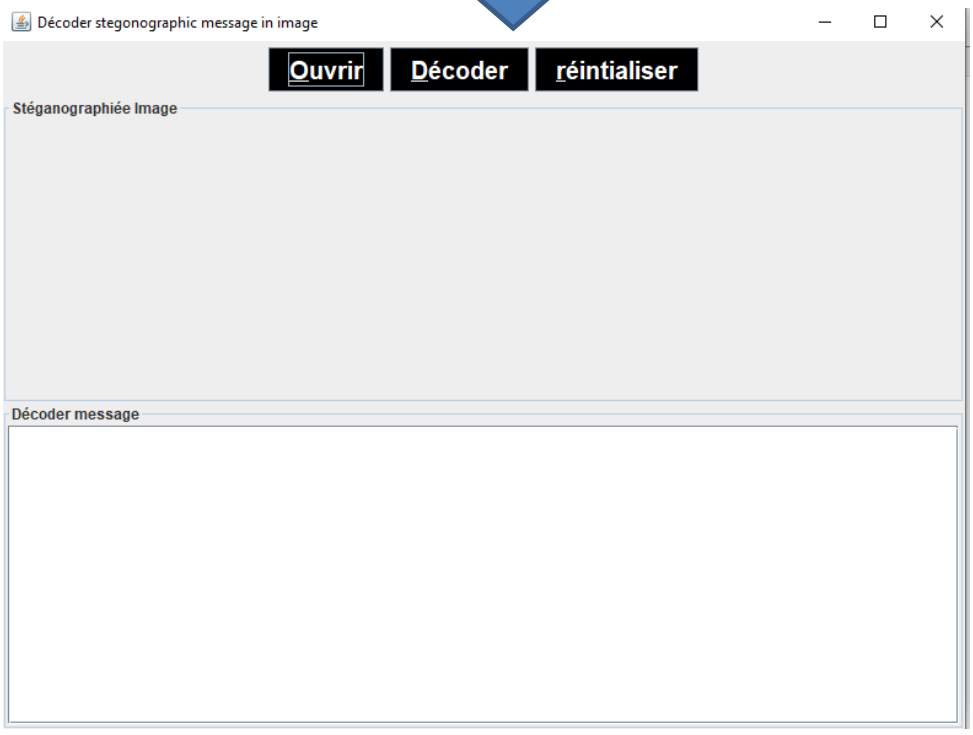


Figure III.8: Interface de décoder le message

III.3.3 Processus d'insertion d'un message secret:

- La boite suivante apparaît : ici L'utilisateur choisit l'image 'PNG' dans laquelle il cachera le message, cliqué sur le bouton "Ouvrir".

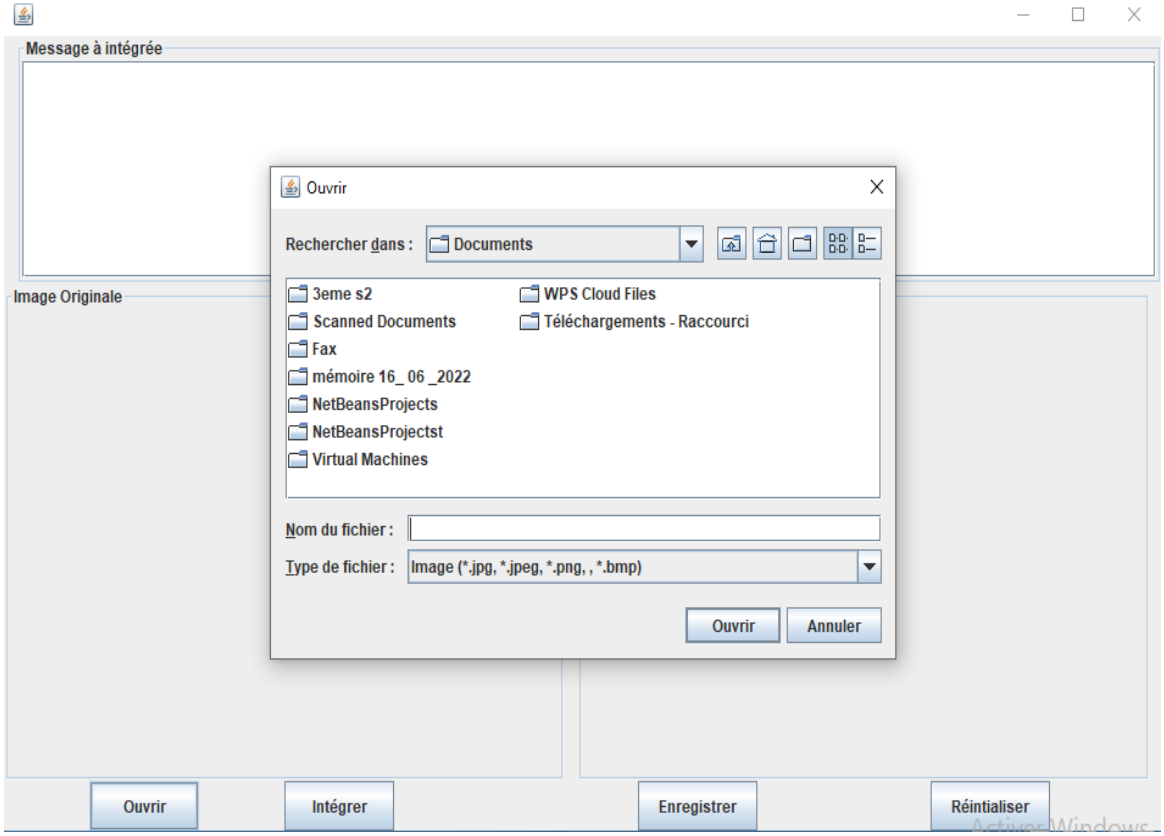


Figure III.9: Interface de sélection d'image

L'interface suivante s'affiche: nous allons cacher le message à l'intérieur de l'image. Écrit le message dans la boite "Message à intégrer "puis cliquer sur "intégrer".

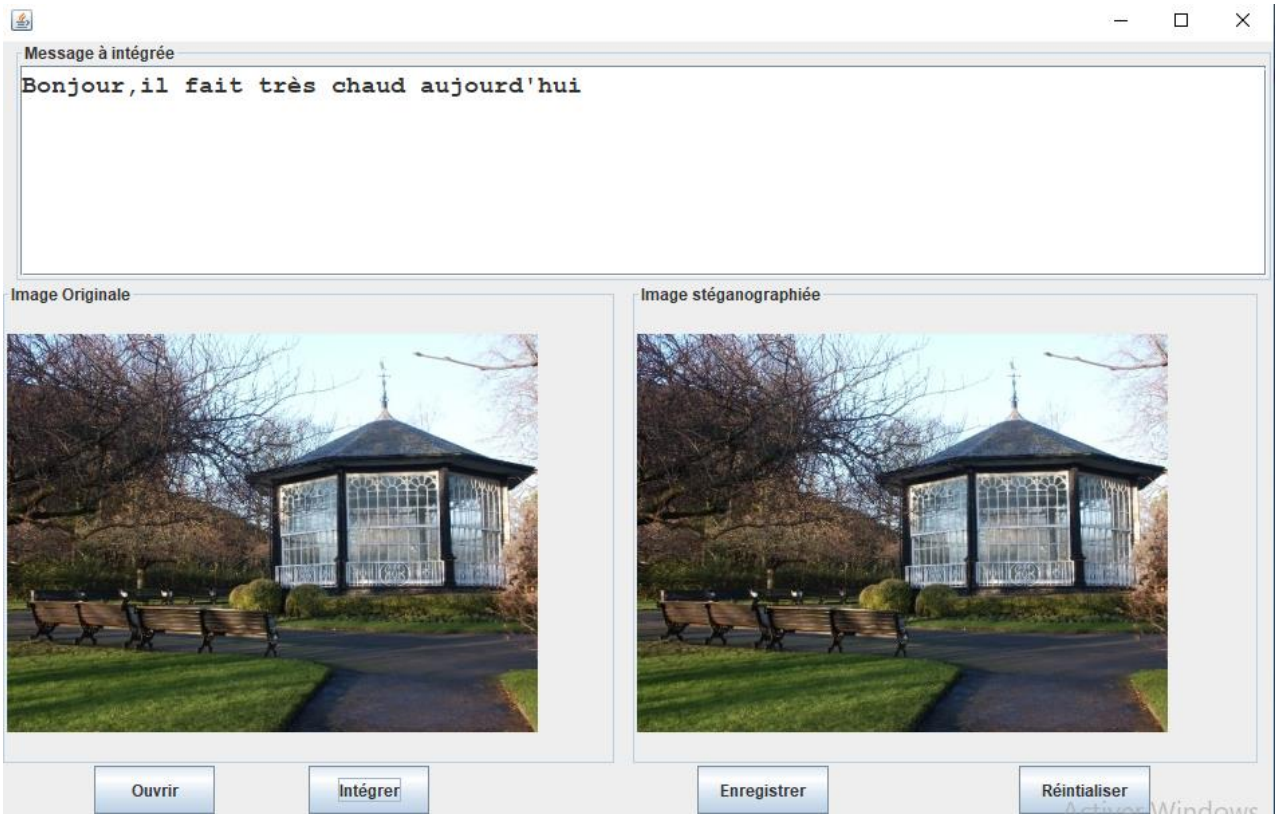


Figure III.10: Interface de dissimuler le texte dans l'image

- La boite suivante s'affiche: Nous choisissons où nous voulons enregistrer l'image dans laquelle nous avons caché le message.

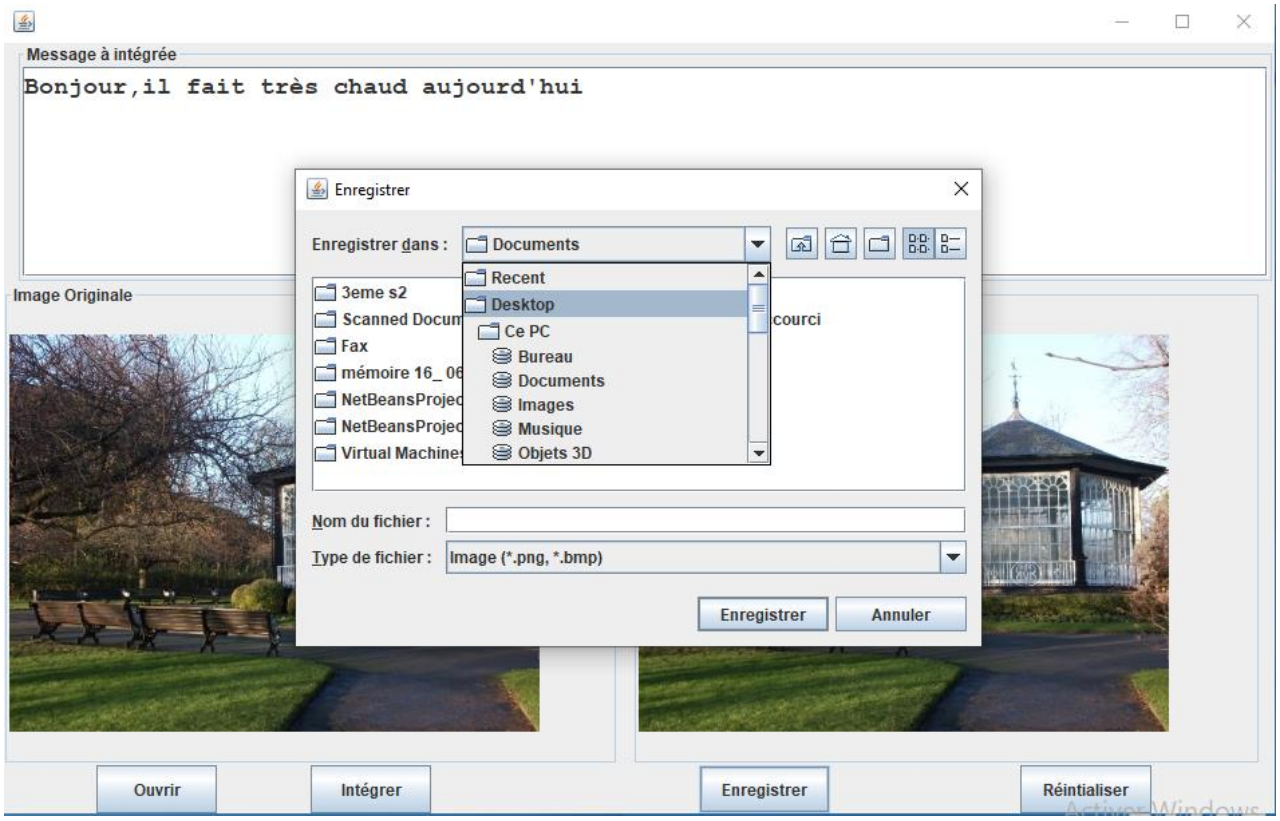


Figure III.11: Interface de sauvegardé l'image stéganographie

III.3.4 Processus d'extraction d'un message secret:

- La boite suivante apparait: Ici, nous choisissons l'image dans laquelle nous avons caché le message, cliqué sur le bouton "Ouvrir".

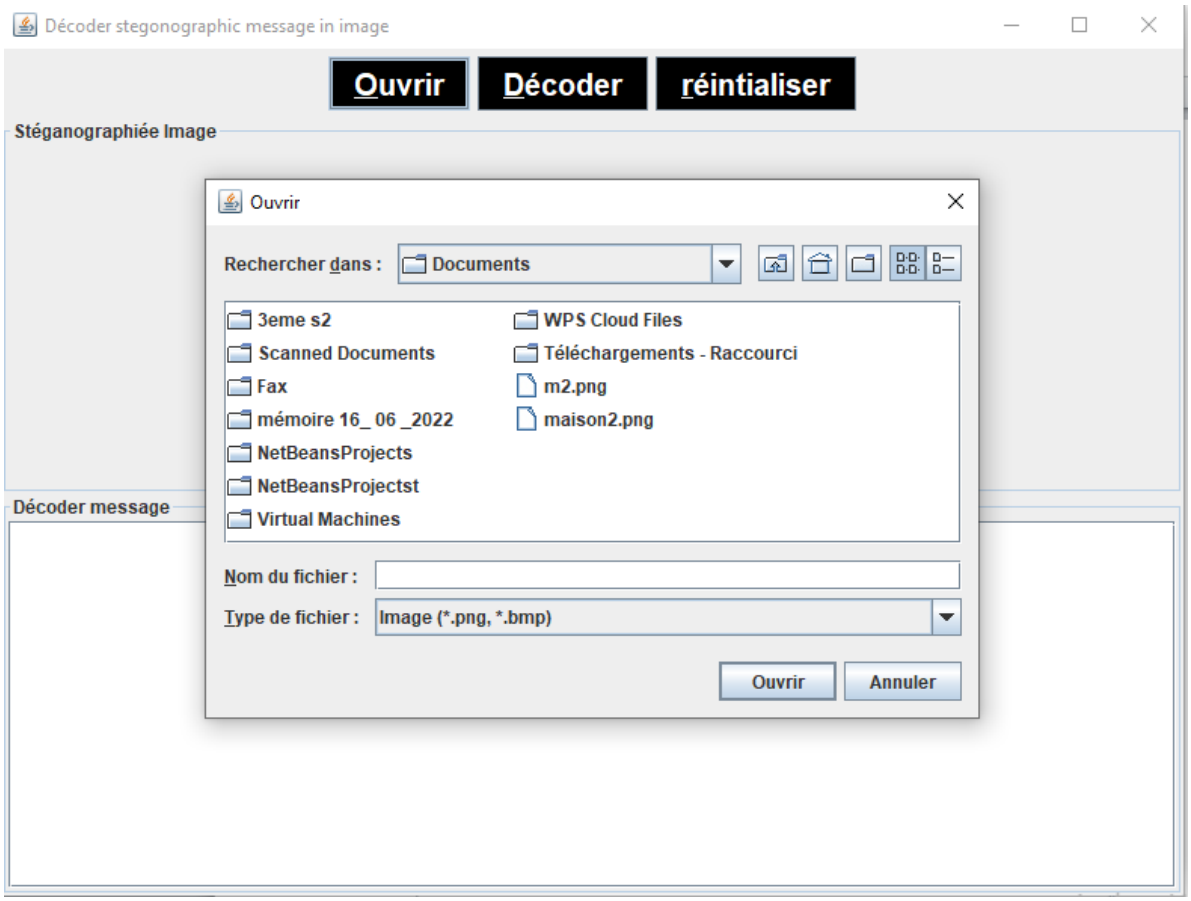


Figure III.12 : Interface de sélection l'image stéganographie

- On retrouvera l'image sur laquelle on cachait le message dans la boite " Stéganographiée image", et le message caché à l'intérieur de l'image que nous trouvons dans la boite "Décoder message". Cliquer sur le bouton "Décoder" afin d'obtenir le message caché.

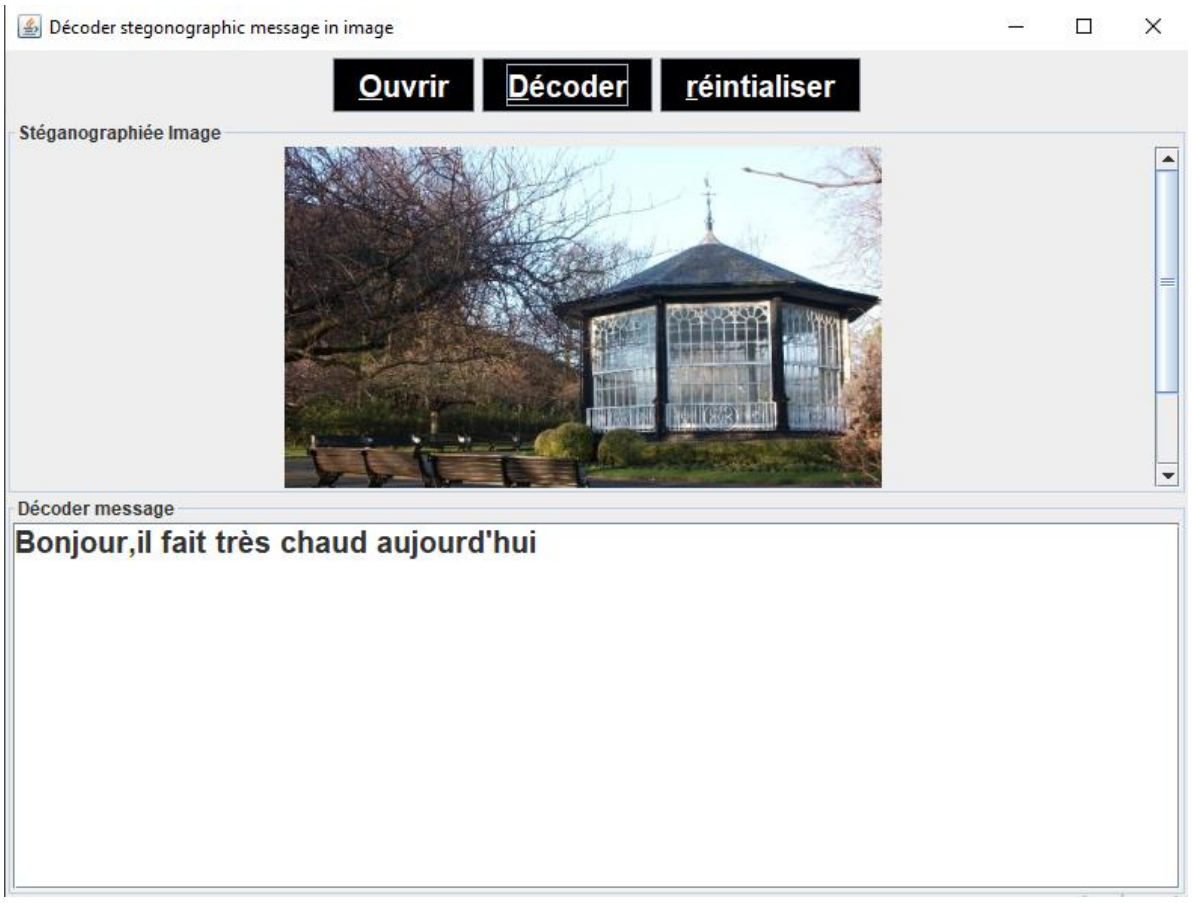


Figure III.13 : Interface d'extraire le message

III.4 Résultat obtenu:

Dans cette section, nous évaluons les performances de notre méthode en termes d'imperceptibilité, de puissance et de robustesse. Nous démontrons également la capacité de notre algorithme à inclure. A la fin, le résultat obtenu de la stéganographie c'est :

- Il est impossible à l'œil de détecter la différence entre eux.

Figure III.14: Image original

FigureIII.15: Image stéganographie

III.4.1 Propriété d'imperceptibilité :

Afin de tester la propriété d'imperceptibilité de notre méthode de Stéganographie, plusieurs les images couleur RGB de différentes tailles sont marquées d'un texte similaire. Pour évaluer concrètement la qualité de notre méthode, on utilise quelques métriques d'évaluation parmi eux PSNR.

Image	taille	PSNR
Image 1	396×297	96.14
Image 2	396×297	97.40
Image 3	396×297	93.82
Image 4	396×297	95.17

Tableau III.1 : Mesures de la qualité d'images Stéganographie

III.4.2 Capacité :

C'est le nombre maximal de bits qui peuvent être cachés dans le médium de couverture. Elle est souvent calculée par la capacité d'insertion relative définie par :

Nombre de lignes x Nombre de colonnes

Conclusion:

En guise de conclusion de ce chapitre, nous avons présenté les méthodes, programmes et outils qui ont été utilisés dans notre application, puis nous avons expliqué la phase d'inclusion et la phase d'extraction. à partir de notre algorithme, nous montrons à la fin les résultats obtenus à partir de certaines expériences sur des images de filigranes (Watermarks).

Conclusion Générale

Conclusion Générale

Avec avènement des utilisations illégales de documents numériques et le manque de confidentialité des données, la stéganographie a été mis en œuvre comme une technologie pour la sécurité des images et des données.

Afin d'atteindre ensemble confidentialité et authentification, Un meilleur compromis doit être trouvé entre deux critères :
L'imperceptibilité et la robustesse pour assurer l'authentification et la protection des images.

Cette mémoire présentée travaille sur une partie importante, qui est la dissimulation d'informations, en insérant spécifiquement un message secret dans une image numérique. Au départ, nous avons étudié le concept de l'image numérique, ses caractéristiques, ses types, etc.

Le deuxième chapitre résume la définition de la stéganographie de l'information et son principe général qui permet d'obtenir un système de dissimulation de son fonctionnement, et nous reparlons des différentes techniques et supports utilisés pour créer ce type de système.

Dans notre dernier chapitre après avoir étudié une assez grande variété de techniques de tatouage, nous nous sommes retrouvés avec mise en œuvre de la méthode LSB.

Nous avons programmé un algorithme de stéganographie pour détecter l'existence d'un fichier message caché dans une image. Nous avons mis en place une application qui fonctionne là-dessus et l'avons testée avec plusieurs images numériques, nous avons obtenu des résultats satisfaisants dans une certaine mesure.

Références bibliographiques

[1] Site internet de L'intérêt de l'image dans votre communication (publika.com)

[2] Site internet de Traitement d'images — Wikipédia (wikipedia.org)

[3 **]** Site internet de (PDF) Qu'est-ce qu'une image numérique ? (researchgate.net)

[4] Site internet de Image numérique — Wikipédia (wikipedia.org)

[5] Site internet de 1 -Représentation d'une image numérique[23] | Download Scientific Diagram (researchgate.net)

[6] Poly_Chap1_Intro.pdf (ensta-paris.fr)

[7] Site internet de Quelle est la différence entre images matricielles et vectorielles ? - 99designs

[8] Site internet de *http://imagenumerique.pagesperso-orange.fr/codagecouleur.htm.*

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

[10] 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.

[11] 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.

[12]Site internet de https://www.google.com/url?sa=t&source=web&rct=j&url=http://primatice.phpnet.org/logiciels/chromoweb/aide/codage.htm&ved=2ahUKEwiViZO08_bAhXGVKQEHT5eBK8QFnoECA4QAQ&usg=AOvVaw24Y5qPcRfiVj3bmco1-Lm9.

[13] 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.

[14]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.

[15] 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.

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

[17] 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.

[18] wikipedia.org https://fr.wikipedia.org› wiki › Stéganographie – Wikipédia .

[19] futura-sciences.com https://www.futura-sciences.com › t… Définition | Stéganographie | Futura Tech.

[20] G. Simmons. « The History of Subliminal Channels ». IEEE Journal on Selected Areas in Communications, Vol 16, No. 4 : pp.452-462. May 1998.

[21] 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.

[22] 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.

[23] David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 161–168, 2012. © CS & IT-CSCP 2012 DOI : 10.5121/csit.2012.2217 DIGITAL IMAGE STEGANALYSIS FOR COMPUTER FORENSIC INVESTIGATION Nanhay Singh, Bhoopesh Singh Bhati, R. S. Raw Ambedkar Institute of Advanced Communication Technologies and Research, Delhi, India.

[24] International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 – May 2014 .

[25] 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.

[26] K. Loukhaoukha, "Tatouage num´erique des images dans le domaine des ondelettes Bas´e sur la d´ecomposition en valeurs singuli`eres et l'optimisation multi-objective,"2010.

[27] K. Stefan and A. Fabien, "Information hiding techniques for steganography and digital watermarking," Artech House, London, UK, 2000.

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

[29] 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.

[30] l . Bougerne : « la sélection des caractéristiques parallèle pour la stéganalyse ». Thèse de Doctorat, Université de Annaba. Soutenue en 2017.

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

[32] Site internet de What is Steganography? A Complete Guide with Types & Examples (simplilearn.com)

[33] Site internet de LSB-Steganography - Python program to steganography files into images using the Least Significant Bit (kitploit.com)

[34] Site internet de (PDF) A Comparison of Different Data Hiding Techniques (researchgate.net)

[35] Site internet de Présentation PowerPoint (lirmm.fr)

[36] Y. A. Al-Najjar, D. C. Soong et al., "Comparison of image quality assessment: Psnr, hvs, ssim, uiqi," Int. J. Sci. Eng. Res, vol. 3, no. 8, pp. 1–5, 2012.

[37] Site internet de Qu'est-ce que Java et pourquoi en ai-je besoin ?

[38] Site internet de NetBeans — Wikipédia (wikipedia.org)

[39] Stéganographie LSB en Langage C(le 11 décembre 2019 par FORGEOUX Victor).

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

[41]Stéganographie et stéganalyse – LIRMM.