الجمهورية الجزائرية الديمقراطية الشعبية

MINISTERE DE L'ENSEIGNEMENT SUERIEUR ET DE LA RECHERCHE SCIENTIQUE

UNIVERSITE **DR. Y**AHIA **F**ARES **D**E **M**EDEA

FACULTE **D**ES **S**CIENCES **E**T **D**E **L**A **T**ECHNOLOGIE

Département du Génie Electrique
Et de l'informatique



Mémoire de Fin D'Etude

Présenté pour l'obtention du Diplôme de Master en Génie Electrique

Option : Système Intelligents et Communicants

THEME

La stéganographie par la méthode de codage d'Huffman et de Modification de direction

Proposé et dirigé par :

BAILICHE Mohamed Amine

Préparer et présenté par :

KHELIDJ Said
HAMADOU Rabah

Année Universitaire 2014-2015

Dédicace

Avant tout, je remercie le grand Dieu, qui nous a aidés à élaborer ce modeste travail.
Je dédie ce modeste travail :

A ma chère et tendre mère

A celle qui a tout souffert, sans me faire souffrir, qu'elle trouve dans ce mémoire le témoignage de ma reconnaissance et de mon affection pour tous les sacrifices, l'extrême amour et la bonté qu'elle m'a offert pour me voir réussir.

A mes frères

Djamel, Nassim et Mohammed

A les hommes que je dois ma réussite, mon bonheur, et tous les respects ;

Qu'ils trouvent ici l'expression de mon affection et une récompense des sacrifices consentis pour moi

A mes sœurs

Nawel ,Meriouma et Assia

En témoignage de mon profond amour et respect, auxquels je souhaite le succès et le bonheur.

Que dieu nous protègent et nous préserve le bonheur et la santé

A mes amis

Yahia, hamza ,Mounir, Youcef, Moussa et

A mon binôme Hamadou Rabah

A tous mes ami(e)s, tous ceux que j'aime, tous ceux qui m'aiment et tous ceux qui me sont chers.

Khelidj Said

Dédicace

Avant tout, je remercie le grand Dieu, qui nous a aidés à élaborer ce modeste travail.

Je dédie ce modeste travail :

A ma chère et tendre mère

A celle qui a tout souffert, sans me faire souffrir, qu'elle trouve dans ce mémoire le témoignage de ma reconnaissance et de mon affection pour tous les sacrifices, l'extrême amour et la bonté qu'elle m'a offert pour me voir réussir.

A mon cher père

A l'homme que je dois ma réussite, mon bonheur, et tout le respect ;

Qu'il trouve ici l'expression de mon affection et une récompense des sacrifices consentis pour moi

A mes frères et mes amis

Farhat, Mahieddine , Monir ,Ahmed,toiti,khaled et

A mon binôme Khelidj Said

A tous mes ami(e)s, tous ceux que j'aime, tous ceux qui m'aiment et tous ceux qui me sont chers.

Rabah Hamadou

Rabah Hamadou

Remerciments

Nous remercions tout d'abord, Allah qui nous a donné la force et le courage afin de parvenir à élaborer ce modeste travail.

Nous tenons à remercier de tout cœur notre encadreur

Monsieur Bailiche Mohamed Amine et témoigner toute notre reconnaissance pour ses conseils judicieux, de ses remarques objectives et surtout de ses gentillesses permanentes.

Nos vifs remerciements à tous les enseignants qui ont contribués à notre formation, et ainsi tous les gens de prés et de loin qui ont aidé à l'élaboration de ce sujet.et à tous nos professeurs et travailleurs de l'université YAHIA FARES – MEDEA-

Et enfin, que nos chers parents et familles, et bien avant tout, trouvent ici l'expression de nos remerciements les plus sincères et les plus profonds en reconnaissance de leurs sacrifices, aides, soutien et encouragement afin de nous assurer cette formation de Master dans les meilleures conditions.

الملخص

الهدف من مشروعنا هو تصميم ومحاكاة لطريقة مستخدمة في إخفاء البيانات في صورة ما المعروفة باسم إخفاء المعلومات(stéganographie). هذه الطريقة هي أسلوب هجين و التي تعتمد على أسلوب ترميز هوفمان و أسلوب EMD.

يتم تطبيق الأسلوب المختلط على صورتين وخمس رسائل نصية (من 1024 إلى 16383 حرفا). MSE وPSNR والتأثير البصري للضوضاء في الصور هي المعايير المستخدمة للحكم على أداء الأسلوب.

الكلمات المفتاحية: طريقة إخفاء(stéganographie)، تشفير، الاختباء، ترميز هوفمان ، EMD.

Résume

Le but de notre projet est l'étude et la simulation d'une méthode utilisée dans le cache des données dans une image connue sous le nom stéganographie. Cette technique est une méthode mixte qui est basée sur le codage Huffman et sur la technique EMD.

La méthode mixte est appliquée sur deux images et cinq messages texte (de 1024 à 16383 caractères). MSE et PSNR et l'effet visuel du bruit sur les images sont les critères utilisés pour juger la performance de cette méthode.

Les mots clés: stéganographie, Cryptographie, dissimulation, codage Huffman, EMD.

Abstract

The goal of our project is the design and simulation of a method used in data hiding in a image known as steganography. This technique is a hybrid method which is based on Huffman coding and the EMD technic.

The mixed method is applied to two images and five text messages (from 1024 to 16383 characters). MSE and PSNR and visual effect of noise on the images are the criteria used to judge the performance of this method.

Keywords: Steganography, Cryptography, hiding, Huffman coding, EMD.

Sommaire

Liste des figures……..I

Liste des tables…….……..II

Liste des abréviations……..……..III

Introduction générale…….....1

Chapitre I : Généralité sur la sécurité informatique

I.Introduction :……..……..3

II. Définition de la sécurité informatique…….……...……3

III. Objectif de la sécurité informatique :…….……...3

IV. Les menaces contre les solutions utilisées en sécurité informatique ……...……...4

IV.1.Défaillance matérielle 4

IV.2.Défaillance logicielle 4

IV.3.Piratage de communication 4

IV.3.1. .Définition de communication : 4

IV.3.2. Les types de communication : 5

IV.3.2.1. Communication par message textuel : 5

IV.3.2.2. Communication par message textuel virtuellement : 5

IV.3 .3.1 Les solutions de piratage : 5

IV.3 .3.1. La cryptographie : 5

IV.3 .3.1.2. Les types de cryptographie : 5

IV.3 .3.1.2.1. Cryptographie à clé publique : 6

IV.3 .3.1.2.2. Cryptographie à clé secret (privé) 8

LISTE DES FIGURES

V. Conclusion 9

Chapitre II : La technique de stéganographie:

I. Introduction……10

II. Définition de stéganographie.....10

III. Le principe de Stéganographie……..10

IV. Les domaines de stéganographie……..10

IV. 1. Domaine spatial ……..…….....10

IV.2. Domaine fréquentiel……..……..11

V. Les techniques utilisées……...……11

V.1.Cacher un texte dans un autre.……..…..……11

V.2. Cacher une image dans une autre…….……..…12

V.3. Cacher un texte dans une page web…….…….14

V .4. Cacher un texte dans un fichier audio……..……15

V.5. Cacher un texte dans une image……...……17

VI. Conclusion……...……..18

Chapitre III : La technique mixte de codage d'Huffman et de modification de direction

I.Introduction 19

II. Définition de codage 19

III.Codage de Huffman. 21

III.1. Définition 21

III.2. Algorithme de compression 21

III.3. Algorithme de décompression..... 23

IV. Méthode de modification de direction(EMD) 23

IV.1. Définition.. 23

LISTE DES FIGURES

IV.2. La technique de codage 24

IV .3. Algorithme de cache (EMD).. 24

IV.4. Récupération des codes cacher 25

IV.5. Algorithme d'extraction..... 26

V. Les avantages et les inconvénients de la technique mixte..... 27

V. 1. Les avantages 27

V. 2. Les inconvénients. 27

VI. Conclusion.. 27

Chapitre IV : La dissimilation des données et l'analyse de résultat

I. Introduction……..……...…28

II. les étapes de réalisation……..28

II.1. Schéma général pour la cache de message……..……..28

II.2. Schéma général pour la récupération de message …….....……...29

II.3. Schéma général de codage d'Huffman ……..…….....30

II.4. Schéma de la technique EMD ……..……...…31

II.5. Schéma détaillé d'EMD_décaché ……..……...32

II.2. Le cas d'utilisation ……..…….....….33

II.2.1. Définition de cas d'utilisation …….....…….……..…33

III.1. Présentation de l'interface……..……..……..……....34

III.2. Présentation et Analyse des résultats……..……....…….35

III.2.1. Définition de Matlab ……..……..…..35

III.2.2. La base de données (image, Message)……..…...……36

IV. résultat et discussion ……..……..……..……37

V. Conclusion ……..……43

LISTE DES FIGURES

***** Chapitre I *******

Figure I. 1: Schéma générale de chiffrement et déchiffrement. 6
Figure I. 2: Chiffrement par clé publique 6
Figure I. 3: Exemple numérique pour le chiffrement et déchiffrement de l'algorithme RSA ... 8
Figure I. 4 : Chiffrement par clé privé. 9

****** Chapitre II *******

Figure II. 1 : exemple de technique de stéganographie 11
Figure II. 2 :l'image masque (lena). 13
Figure II. 3:l'image à cacher (rue). 13
Figure II. 4:l'image masque (lena). 13
Figure II. 5:l'image récupérable. 14
Figure II. *6:* Exemple de stéganographie sur fichier audio avec Stools4 (choix du fichier audio). 15
Figure II. 7: Exemple de stéganographie sur fichier audio avec Stools4 (cache de données). 16
Figure II. 8: Exemple de stéganographie sur fichier audio avec Stools4 (découvre de données). 16
Figure II. 9:l'image originale (avant la cache de texte). 18
Figure II. 10:l'mage bruité (après la cache de texte). [2] 18

*****Chapitre III********

Figure III. *1:* le code ASCII. 20
Figure III. 2:l'arbre du Huffman 22
Figure III. 3:l'arbre du Huffman de décompression. 23
Figure III. 4:Le chéma de cachement du texte. 25
Figure III. 5: La méthode d'extraction de l'information. 26

LISTE DES FIGURES

*****Chapitre IV******

Figure IV.1: L'organigramme général de la stéganographie..... 28
Figure IV.2: l'organigramme général pour la récupération de message……... 29
Figure IV.3: l'organigramme détaillé pour le codage de Huffman……... 30
Figure IV.4: l'organigramme détailler pour la technique EMD…….. 31
Figure IV.5:l'organigramme de (Emd_decacher).....32
Figure IV.6: Diagramme de cas d'utilisation…….…...33
Figure IV.7: le menu de l'émetteur ……...…34
Figure IV.8: le menu de récepteur …….....35
Figure IV.9: Lena 512……..…….36
Figure IV.10: Baboon……..…….36
Figure IV.11: Lena 256……..……...37
Figure IV.12: Baboon 256 ……..……...…37
Figure IV.13: L'mage couvre ……..……..37
Figure IV.14: L'image stegano.bmp……..……38
Figure IV.15 : résultat de PSNR sur image Lena…….…… 39
Figure IV.16 : résultat de MSE sur image Lena……..…….40
Figure IV.17 : résultat de PSNR sur image Baboon……..…….…….41
Figure IV.18 : résultat de MSE sur image Baboon……..…….42

LISTE DES TABLEAUX

Chapitre III

Table III.1 : Table des codes……..……..22

Chapitre IV

Table IV.1 : Table des codes d'Hoffman de message secret…….…...……38

Table IV.2 : Résultat de la méthode proposée d'image de Lena……..…..…39

Table IV.3 : Dégradation de bruit sur l'mage Lena…….……...……40

Table IV.4 : Résultat de la méthode proposée d'image de Baboon……..…….……41

Table IV.5 : Dégradation de bruit sur l'image Baboon……..…..……42

Liste d'abréviation

ASCII : American Standard Code for Information Interchange

RSA: Rivest Shamir Adlmeman.

EMD: Exploiting Modification Direction.

MSE: Mean Square Error.

PSNR: Peak Signal to Noise Ratio.

m : message claire.

C : text Chiffré.

KSB: Key Secret of Boob.

KPB: Key Public of Boob.

Introduction générale :

La communication est l'action de communiqué, de transmettre et de faire participer, donc on peut dire que la communication est un élément banal de notre vie.

Pour cette raison l'humaine après l'antiquité il a pensé à des méthodes pour sécuriser ces communication set plus précisément celles qui contient des informations secret.

Ces méthodes sont utilisé de manier considérable dans les guères entre les peuples, par exemple Démarrât ancien roi de spart « il prit une tablette double, en gratta la cire, puis il écrive sur le bois même les projets de Xerxès, ensuite il recouvrit de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis. » (Livre VII, 239), c'est la première méthode qui permette de réaliser une transmission d'un message secret.

Parmi les méthodes anciens utilisés aussi, la méthode qui consiste à remplacer chaque A dans le message par un D, chaque B par un E, et ainsi de suite à travers l'alphabet. Seul quelqu'un qui connaissait la règle "décalé de 3" pouvait déchiffrer le message.

Avec le progrès de l'information et leur outils de transmission et surtout l'arrivée d'internet et les nouvelles technologies il doit être obligé de développer et d'améliorer de manière considérable la communication par messages textuels.

Plusieurs entités utilise cette technologie pour communiquer et transmettre les données « messages, chat, sms, ….etc. », donc les gouvernements, les services secret, les armées cherchons toujours des méthodes plus sécurisé et fiable dans le but de sécurisé ces communications.

Cependant la nouvelle technologie est vulnérable, les failles de sécurité sont fréquentes, c'est ainsi que la sécurité de transmissions des informations avec la communication par messages textuels, pris une importante place dans la société actuelle, parce que aujourd'hui il y'a de plus en plus d'information qui doivent rester secrètes ou confidentiels, en effet par les banque, par les services secret ou un mot de passe ne doivent pas être divulgués et personne ne doit pouvoir les déduire .c'est pour cette raison ce genre d'information il doit être sécuriser.

Afin de traité ce problème, on a choisi un sujet très important à savoir, il s'agit d'assuré la communication par message textuel .alors comment peut-on assurer cette communication ?

Pour atteindre cet objectif nous avons diviser notre travail comme suit :

Commençons par une introduction générale.

Dans le chapitre I, on s'est intéressé aux généralités sur la sûreté de la communication par message textuel.

Le chapitre II est un état de l'art sur la méthode de Stéganographie.

Dans le chapitre III nous présentons les deux techniques utilisées pour construire notre projet et on détaille leur fonctionnement et algorithmes.

Le chapitre IV présente la conception de notre, ainsi que la présentation et l'analyse de résultats obtenus.

Finalement nous terminons par une conclusion générale.

CHAPITR I

Généralité sur la sécurité informatique

I. Introduction :

Avec le progrès de l'information et leurs outils de transmission et surtout l'arrivée d'internet et les nouvelles technologies il devient nécessaire de développer et d'améliorer de manière considérable la communication.

Pour cette raison l'homme pensé à des méthodes pour sécuriser ces communications et plus précisément celles qui contient des informations secrètes, quelle sont ces méthodes ; et quelle est le taux de leur efficacité.

II. Définition de la sécurité informatique :

La sécurité informatique est l'ensemble des techniques qui assurent l'arrivé des informations confidentielles au destinataire sans comprendre ou voir le contenu de message par intermédiaire par ce qu'il est chiffré ou bien caché sur la vision humain et cette dernière est la moderne technique dans le domaine de sécurité informatique.

III. Objectif de la sécurité informatique :

La sécurité informatique moderne s'attaque d'une façon générale aux problèmes de sécurité des communications :

- **Confidentialité *:*** Mécanisme pour transmettre des données de telle sorte que seul le destinataire autorisé puisse les lire.
- **Intégrité *:*** Mécanisme pour s'assurer que les données reçues n'ont pas été modifiées durant la transmission.
- **Authentification *:*** Mécanisme pour permettre d'identifier des personnes ou des entités et de certifier cette identité.
- **Non-répudiation *:*** Mécanisme pour enregistrer un acte ou un engagement d'une personne ou d'une entité de telle sorte que celle-ci ne puisse pas nier avoir accompli cet acte ou pris cet engagement.

IV. Les menaces et les solution utilisées en sécurité informatique :

Il ne faut pas perdre de vue que la sécurité est comme une chaîne, guère plus solide que son maillon le plus faible. En plus de la formation de la sensibilisation permanente des utilisateurs, la politique de sécurité peut être découpée en plusieurs parties :

IV.1.Défaillance matérielle:

Tout équipement physique est sujet à défaillance (usure, vieillissement, défaut…) L'achat d'équipements de qualité et standard accompagnés d'une bonne garantie avec support technique est essentiel pour minimiser les délais de remise en fonction. Seule une forme de sauvegarde peut cependant protéger les données.

La solution est donc :

- Choisir le matériel qui a la meilleure qualité.
- Choisir le matériel qui a la plus grand duré de vie.
- Acheter la marque originale.

IV.2.Défaillance logicielle:

Tout programme informatique contient des bugs. La seule façon de se protéger efficacement contre ceux-ci est de faire des copies de l'information à risque. Une mise à jour régulière des logiciels et la visite des sites consacrés à ce type de problèmes peuvent contribuer à en diminuer la fréquence.[1]

Les solutions proposées sont :

- Installation des logiciels et matériels confiances.
- Effectuer les Mises à jour toujours.
- Utilisation des procédures de sécurité permanant.

IV.3.Piratage de communication

IV.3.1. .Définition de la communication :

La communication est l'action de communiqué, de transmettre et de faire participer Donc la communication est un élément banal de notre vie. Le besoin de communication est si fondamental qu'il explique, en partie, que les gens racontent leur vie à un inconnu dans le train, et ce fait encore plus surprenant, qu'ils rependent à ceux qui s'introduisent dans leur propre domicile pour les interroger.

IV.3.2. Les types de communication :

IV.3.2.1. Communication par message textuel :

C'est la communication qui prendre le texte comme support pour échanger l'information.

IV.3.2.2. Communication par message textuel virtuellement :

La communication virtuelle, aussi appelée communication méfiée par ordinateur, cyber communication ou netspeak est une forme de communication textuelle utilisant des dispositifs numériques comme transmetteur et médiateur. Elle est utilisée notamment dans les SMS, la messagerie instantanée, les forums, le courrier électronique et le Web. [2]

IV.3 .3. Les solutions de piratage :

IV.3 .3.1.1. La cryptographie :

Étude des méthodes permettant de transmettre des données d'une manière confidentielle et les sous titres suivante vont détailler le mot cryptographie.

Terminologie :

- ✓ Cryptage (chiffrement) : transformation d'un message clair en un message crypté.
- ✓ Décryptage (déchiffrement) : transformation inverse du cryptage qui permet de retrouver a partir d'un message crypté, le message clair correspondant.

Cryptologie est une science mathématique qui comporte deux branches :

Cryptanalyse est l'étude des procédés cryptographique dans le but de trouver des faiblesses et de casser les algorithmes de cryptage.

Un système cryptographique est un quintuplé (P, C, K, E, D) où :

P est l'ensemble fini des clairs.

C'est l'ensemble fini des chiffres.

K est l'ensemble fini des clés (Key)

E est l'ensemble fini des règles de chiffrement

D est l'ensemble fini des règles de déchiffrement.



Figure I. 1: Schéma générale de chiffrement et déchiffrement.

IV.3 .3.1.2. Les types de cryptographie :

Selon la clé de cryptage on peut distinguer deux types de cryptographie sont :

IV.3 .3.1.2.1. Cryptographie à clé publique :

Principe :

Chaque entité possède 2 clés distinctes (une privée, une publique) avec

Impossibilité de déduire la clé privée à partir de la clé publique. De ce fait, il est possible de distribuer librement cette dernière. Deux clé sont utilisées:[3]

- **kpb: clé publique**
- **ksb: clé privé.**

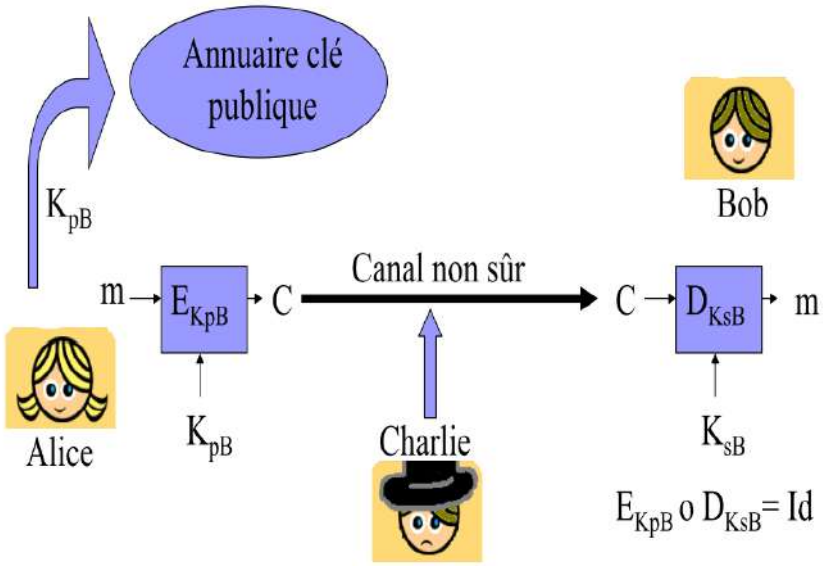


Figure I. 2: Chiffrement par clé publique

On prend comme un exemple l'algorithme RSA (Rivest Shamir Adleman)

- **Algorithme :**

✓ .Génération de 2 nombres premier P et Q.

✓ .Calcule de n=P*Q.

✓ .Calcule de Q(n) = (P-1)*(Q-1).

✓ .Déterminer e tel que 3<e<Q(n) et (e , Q(n))=1.

✓ .Calculer d tel que e*d=1 modulo Q(n).

✓ . On a une clé publique (e, n).

✓ . On obtient une clé privée (d, n).

✓ .On chiffre la suite des caractères un après l'autre comme suit $C=M^e \bmod(n)$.

✓ .On déchiffre le message comme suit $M=C^d$ modulo (n).

On prend comme un exemple l'algorithme RSA

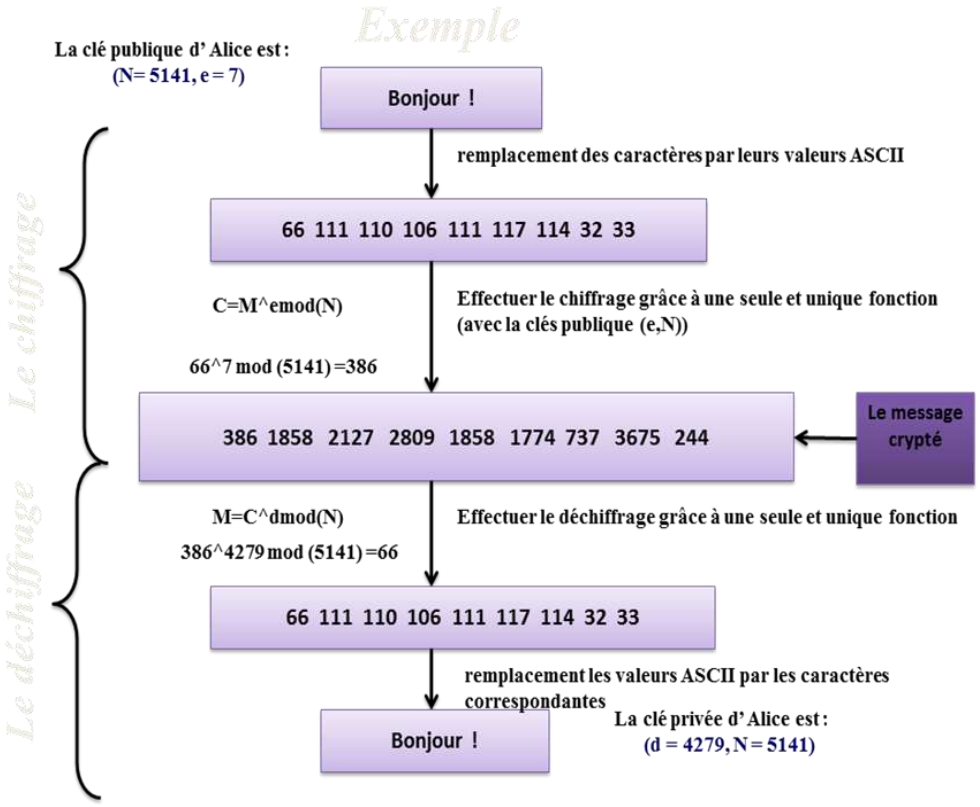


Figure I. 3: Exemple numérique pour le chiffrement et déchiffrement de l'algorithme RSA

IV.3 .3.1.2.2. Cryptographie à clé secret (privé) :

Est une ancienne, simple et plus rapide que clé publique, elle se base sur les formules arithmétiques et décalage circulaire entre les caractères.

Algorithme :

- ✓ . La clé K doit connu avant par Alice et Bob.
- ✓ . Alice et Bob doit accepter la fonction de codage et de décodage. [3]

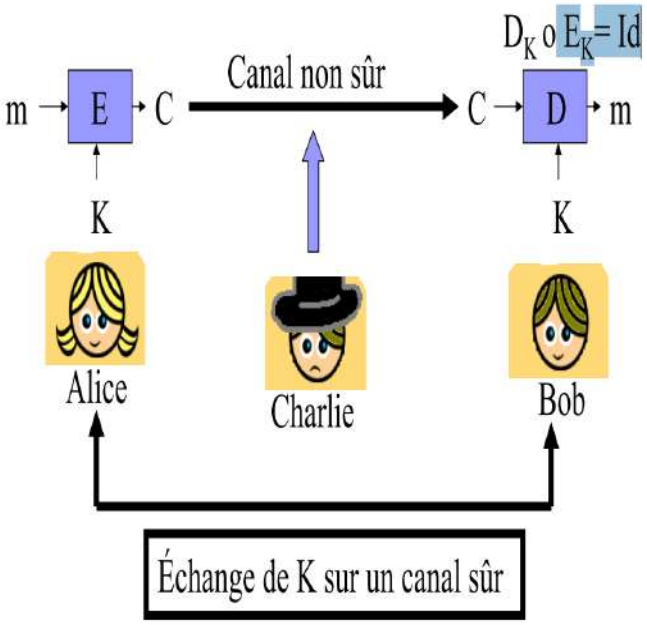


Figure I. 4 : Chiffrement par clé privé.

On prend comme un exemple l'algorithme de césar qui baser sur le décalage, On choisi que la clé k=décalage de 3 alphabétique, le nombre de caractère est de 26, le message « Said ».On obtient un message crypté comme suit :

« Said » devient « vdlg ».

V. Conclusion :

Comme l'informatique est en développement quotidien, les menaces aussi sont en développement ; c'est pour ça qu'on considère que les solutions précédentes restent des solutions anciennes et de base, mais la meilleur solution contre l'attaque dans notre époque ce n'est pas de cacher de sens d'information confidentielle mais c'est de cacher la donnée complètement et ça ce qu'on appelle la technique de stéganographie que l'on va détailler au deuxième chapitre.

CHAPITR II

La technique de stéganographie

I. Introduction :

Comme on a vu en premier chapitre que la Stéganographie est une technique moderne de sécurité informatique appliqué contre le piratage d'information en communication. Dans ce chapitre on va détailler et discuter sur ce que l'on appelle la stéganographie, le fonctionnement, les techniques utilisées.

II. Définition de stéganographie:

Si la cryptographie est l'art de cacher le sens d'un message, la stéganographie, moins connue et même absente de la plupart des dictionnaires, est l'art d'en cacher le contenu et de la dissimulation de communication. Son objectif est de pouvoir dissimuler des données qui doivent être tenues secrètes dans un support paraissant Anodin. Ces données ne doivent pouvoir être récupérées que par une personne ayant Connaissance de l'algorithme utilisé pour la dissimulation, ainsi que de l'éventuel clé saisie.

III. Le principe de Stéganographie :

Son principe est de développer un outil qui permette d'assurer la communication par le message qui contient l'information sécrète avec les critères suivants :

- Garantir la confidentialité.
- Garantir l'intégrité.
- Assurer que l'œil humaine ne peut pas détecter la présence de message.

IV. Les domaines de stéganographie :

IV. 1. 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.

On utilise généralement le RGB (Red Green Blue) pour la représentation des couleurs. Chaque pixel est codé à l'aide d'un triplé d'octet spécifiant chacune des composantes principales.

IV.2.Domaine fréquentiel :

Constatant la mauvaise performance des algorithmes de marquage dans le domaine spatial vis-à-vis de certaine modification, la plupart du temps étant involontaire comme entre autres de la compression JPEG, de nombreuses méthodes ont été développées à partir de connaissance acquise en traitement de signal.

V. Les techniques utilisées :

V.1. Cacher un texte dans un autre texte:

Pour cacher un texte dans un autre texte, il doit prendre leurs codes (ASCII ou codage de Huffman,..) en suite on transforme le texte des caractères en texte binaire et on choisit l'algorithme pour cacher les codes de texte sécrète dans les codes de texte à transmettre.

On prend comme un exemple les 3 caractères 'A','B' et 'C'.

Soit le code ASCII de « A » en binaire sur 8 bit « 01000001 »

Le code ASCII de « B » en binaire sur 8 bit « 01000010 »

Le code ASCII de « C » en binaire sur 8 bit « 01000011 »

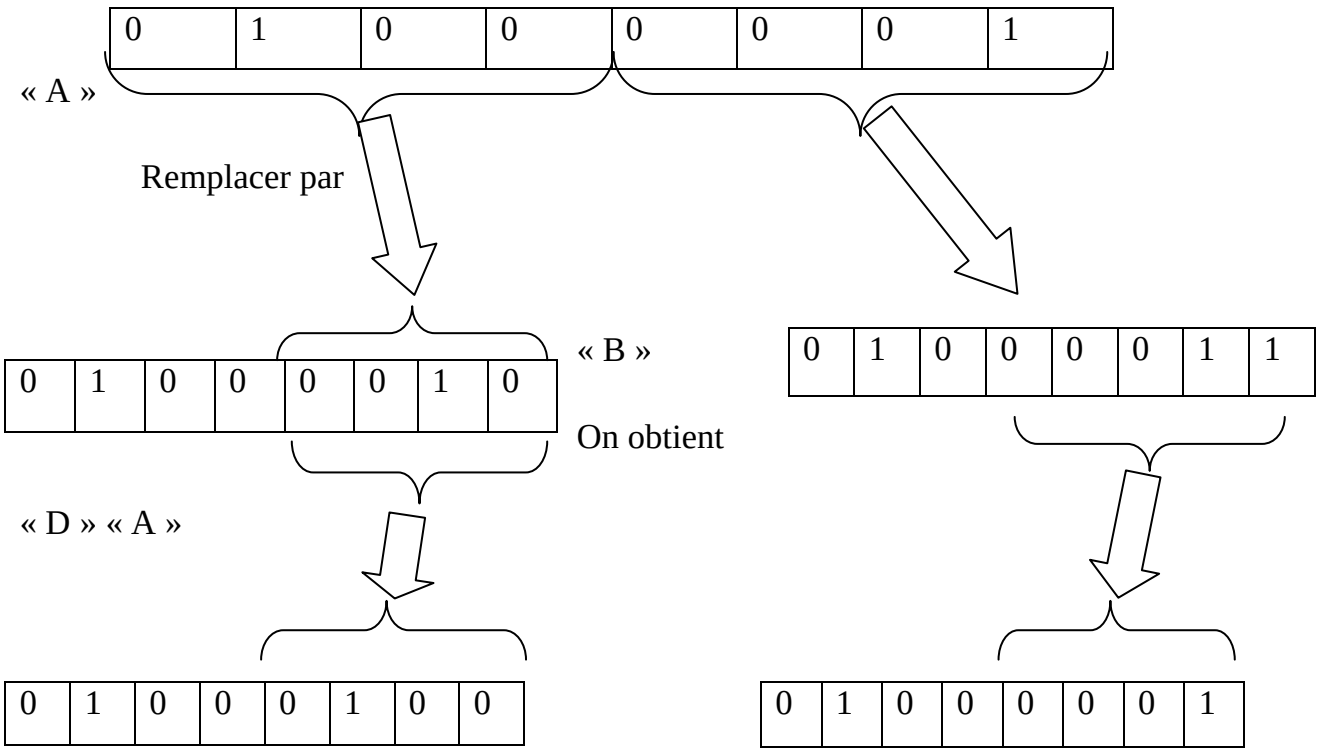


Figure II. 1 : exemple de technique de stéganographie

On choisit l'algorithme LSB donc on remplace les 4 dernier bit de B par les 4 premier bit de A et les 4 dernier bit de C par les 4 dernier bit de A enfin on obtient « 01000100 » et « 01000001 » donc le message qui cache notre donné et « «DA ».

Remarque : le texte que l'on utilise comme un masque doit être plus grand que le texte à envoyer.

V.2. cacher une image dans une autre image:

Pour cacher une image dans une autre image, il n'y a pas grand-chose à expliquer : au lieu de coder les bits d'un texte sur les bits de poids faible de l'image support, il suffit de coder les bits des couleurs de chaque pixel à la place. On se rend compte néanmoins que l'on doit dans ce cas avoir une image support beaucoup plus grande que l'image à masquée du fait que l'on sépare une couleur primaire d'un pixel sur 1 pixel et le tiers d'un autre (de quoi insérer 8 bits en utilisant les deux derniers de chaque couleur primaire). Ou alors, il faut utiliser plus de bits pour chaque couleur de chaque pixel mais dans ce cas, il faut faire attention à ne pas prendre une trop grande partie de la couleur sinon l'image une fois l'autre image stéganographie risque d'être visiblement différente de l'originale. [4]

On prend comme un exemple:

Soit un octet de l'image qui cache 01101011et un octet de l'image que l'on souhaite cacher 10011101.Le but est de remplacer les bits de poids faible de l'image qui cache par les bits de poids fort de l'image qu'on souhaite cacher. Ainsi, on obtiendra l'octet 01101001.

Il a réalisé le programme cacher_im3 qui réalise cette opération. Il prend en argument d'entrée l'image qui cache et celle qu'on veut cacher. Il appelle trois fois le sous programme cacher_im1 qui s'occupe du traitement pour chacune des composantes RVB.et réalisé un autre programme qui permet de récupérer l'image cachée, trouver_im3 qui permettre de faire passer les bits de poids faible en bits de poids forts d'une nouvelle image, et va nous permettre ainsi de retrouver notre image dissimulée.



Figure II. 2 :l'image masque(lena).



Figure II. 3:l'image à cacher (rue).



Figure II. 4:l'image masque (lena).

s1 et s2 correspondent respectivement à l'image porteuse et l'image cachée, qui, au passage, n'ont plus leur bits de poids faible. il me reste juste à afficher s2



Figure II. 5:l'image récupérable.

V.3. Cacher un texte dans une page web:

La méthode de stéganographie la plus simple qui soit est sûrement celle qui consiste à cacher du texte dans une page (x) HTML. Ce langage de développement web interprète en effet de manière identique un, deux ou trois voire beaucoup plus d'espaces. Il suffit donc, par exemple d'associer une valeur numérique à chaque lettre de l'alphabet et de mettre entre chaque mot autant d'espaces que la valeur de la lettre numérique à inscrire. [5]

On prend comme un exemple le message suivant :

I L L U S I O N

9 12 12 21 19 9 15 14

Voilà ce que cela donnerait dans le code HTML de la page :

Bienvenue sur mon site ! J'espère que vous y trouverez votre bonheur!

Et ce que les visiteurs verront sur la page du site

Bienvenue sur mon site ! J'espère que vous y trouverez votre bonheur!

Avantage : facile à cacher et il suffit d'un simple navigateur pour afficher le code source et retrouver le texte stéganographie.

Inconvénient : L'ouverture, l'enregistrement avec un logiciel d'édition comme Front Page peut suffire à perdre les données!

V .4. Cacher un texte dans un fichier audio:

Les fichiers audio sont encore une meilleure manière de cacher de l'information grâce à leur taille. En effet, même au format MP3 qui est l'un des plus répandus et ayant une des meilleures compressions, un fichier de 3-6 Mo est tout à fait usuel. Si nous respectons toujours la règle d'or (volume des informations à cacher < 20-25% de données).Avec des fichiers audio, nous n'allons plus jouer sur les palettes de couleurs comme avec les images, mais sur les pistes de son qui peuvent s'inverser.Quelques exemples de logiciels permettant de mettre en œuvre ce genre de techniques sont MP3-st égo ou Stools4 (mais qui ne gère quels fichiers au format wav). L'avantage certain de la stéganographie sur fichiers audio sur celle sur des images est que la quantité d'informations qui peuvent être cachées y est plus importante grâce à la taille du support, ainsi que les techniques de dissimulation qui sont plus nombreuses.

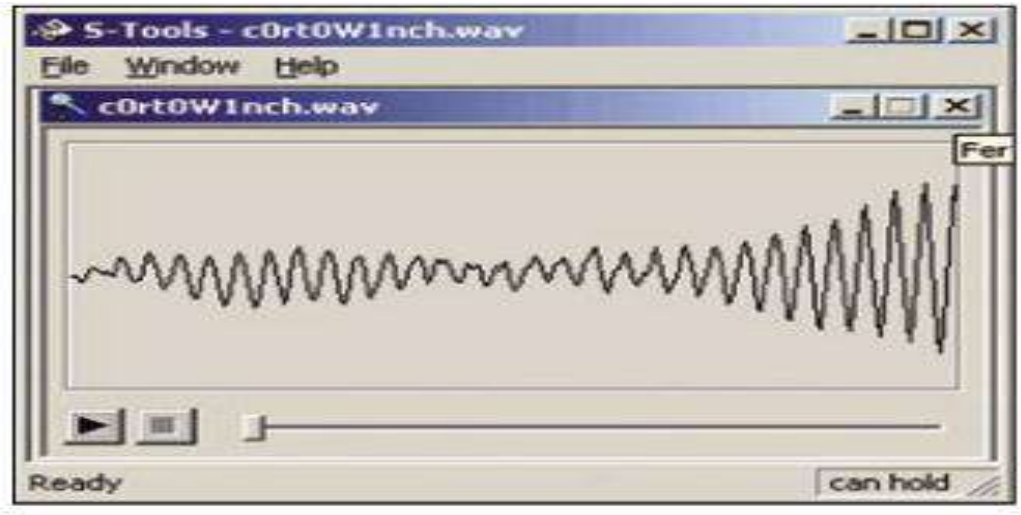


Figure II. *6:*Exemple de stéganographie sur fichier audio avec Stools4 (choix du fichier audio).

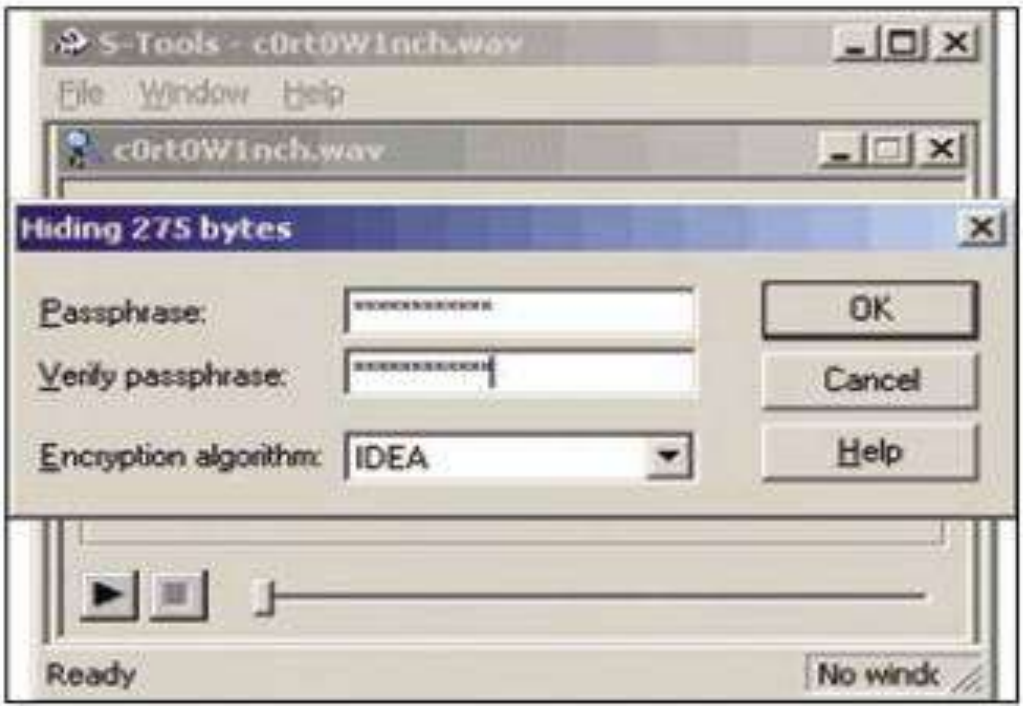


Figure II. 7: Exemple de stéganographie sur fichier audio avec Stools4 (cachede données).

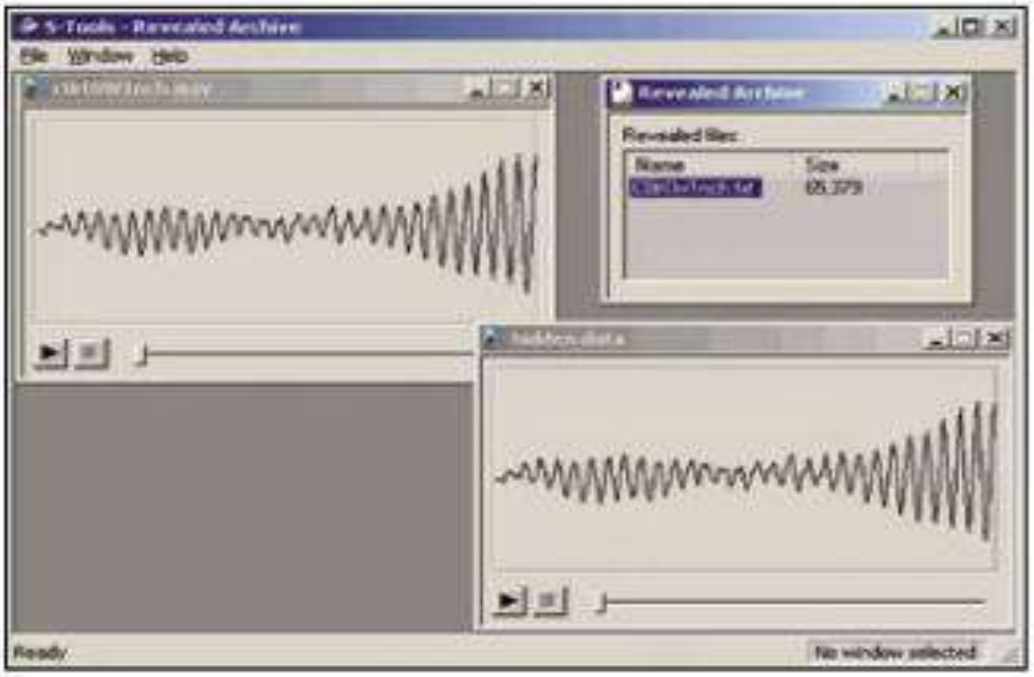


Figure II. 8: Exemple de stéganographie sur fichier audio avec Stools4 (découvre de données).

V.5. Cacher un texte dans une image:

On commence d'abord par la sélection d'image d'un format qui doivent être notre couvre, ensuite on propose un algorithme pour cacher le texte que l'on veut cacher dans cette image.

L'application de ce algorithme ignore les derniers bits du poids faible (LSB) pour chaque composent de pixels et les remplacer par des bits de notre donnée qui on veut la caché.

L'algorithme se passe par une suite des opérations pour réaliser l'objectif de remplacement transforme les pixels sous la forme binaire :

On prend comme un exemple les pixels suivant :

Soit (pixel=328965 => rouge = 5, vert=5et bleu=5)

Donc (rouge=00000101, vert=00000101et bleu=00000101), transforme le texte aussi sous la forme binaire :

Soit les caractères a b c => a= 01100001, b=01100010, c= 01100011) Après la préparation du couvre et le message on a caché dans chaque pixel un caractère de la manière suivant : Pixel original: (r7 r6 r5 r4 r3 r2 r1 r0, g7 g6 g5 g4 g3 g2 g1 g0, b7 b6 b5 b4 b3 b2 b1 b0). Caractère :(c7 c6 c5 c4 c3 c2 c1 c0).On a fait le Déplacement de trois bits de caractère dans les trois derniers bits de l'octet de la couleur rouge, le même pour le vert et deux bit restant dans l'octet de la couleur bleu. Donc on a obtenu un nouveau pixel sous la forme suivante :(r7 r6 r5 r4 r3 c7 c6 c5, g7 g6 g5 g4 g3 c4 c3 c2, b7 b6 b5 b4 b3 b2 c1 c0).Si on a le pixel (rouge=11100001=225, vert=01100100=100et bleu= 01100100=100) avec le caractère (a= 01100001) et on a appliqué le fonctionnement de l'algorithme le résultat fournit est comme suite :Pixel (rouge=11100011=227, vert= 01100000=96et bleu= 01100101=101)On a remarqué le changement de la valeur du couleur original ne dépasse pas +7 ou -7 donc l'œil humaine ne peut pas détecter le changement de la couleur. [2]



Figure II. 9: l'image originale (avant la cache de texte).



Figure II. 10**:** l'mage bruité (après la cache de texte). [2]

VI. Conclusion :

La stéganographie est un domaine important de la sécurité des communications qui existe depuis l'Antiquité comme la cryptographie. Il y'a plusieurs techniques qui sont limitées par les limites de l'esprit humain. Depuis le développement de l'informatique, la stéganographie a très nettement évoluée vers le monde moderne et permet de cacher des informations de manière beaucoup plus sophistiquée et sécurisée que les techniques moins récentes mais qui sont toutes aussi efficaces quand elles sont utilisées dans le bon contexte.

CHAPITR III

Le technique mixte codage d'Huffman et modification de direction

I. Introduction :

Comme on a vu au chapitre précédent qu'il y a plusieurs techniques et algorithmes utilisés pour cacher un message dans une image (la stéganographie), et parmi ces algorithmes on a les algorithmes de codage pour coder le message et des techniques pour l'intégrer dans l'image, et dans ce chapitre on va voir le codage de Huffman et la technique de modification de direction (EMD) bien détailler.

II. Définition de codage :

Le codage est un technique qui permet d'établir une correspondance sans ambiguïté de passer d'une représentation (dite externe) d'une information à une autre représentation (dite interne: sous forme binaire) de la même information, suivant un ensemble des règles biens précisées.

Le principe des algorithmes de codage statistique est d'utiliser les probabilités d'occurrences de chaque symbole dans une séquence de symboles émanant de la source. Dans le cadre de ce cours nous examinerons dans cette catégorie deux algorithmes.

Prenant l'exemple du codage ASCII :

La norme ASCII (on prononce généralement « aski ») établit une correspondance entre une représentation binaire des caractères de l'alphabet latin et les symboles, les signes, qui constituent cet alphabet. Par exemple, le caractère a est associé à 1100001 (97) et A à 1000001 (65). La norme ASCII permet ainsi à toute sorte machines de stocker, analyser et communiquer de l'information textuelle. En particulier, la quasi-totalité des ordinateurs personnels et des stations de travail utilisent l'encodage ASCII. Le code ASCII de base représentait les caractères sur 7 bits (c'est-à-dire 128 caractères possibles, de 0 à 127).

- Les codes 0 à 31 ne sont pas des caractères. On les appelle caractères de contrôle car ils permettent de faire des actions telles que :
- retour à la ligne (Carriage return)
- bip sonore (Audible Bell)
- Les codes 65 à 90 représentent les majuscules

• Les codes 97 à 122 représentent les minuscules (il suffit de modifier le 6ème bit pour passer de majuscules à minuscules, c'est-à-dire ajouter 32 au code ASCII en base décimale).[6]

Le code ASCII a été mis au point pour la langue anglaise, il ne contient donc pas de caractères accentués, ni de caractères spécifiques à une langue. Le code ASCII a donc été étendu à 8 bits pour pouvoir coder plus de caractères (on parle d'ailleurs de code ASCII étendu...). Cette norme s'appelle ISO-8859 et se décline par exemple en ISO-8859-1 lorsqu'elle étend l'ASCII avec les caractères accentués d'Europe occidentale, et qui est souvent appelée Latin-1 ou Europe occidentale.[6]



Figure III.1: le code ASCII.

III. Codage de Huffman:

III.1. Définition :

Les probabilités d'apparition des symboles sont placées dans un tableau trié par ordre décroissant de probabilités. L'algorithme de Huffman est implémenté suivant une structure d'arbre.

Le principe de cet algorithme consiste à regrouper les deux symboles de probabilités la plus faible pour en faire un nouveau symbole dont la probabilité est la somme des probabilités de ces deux symboles. On itère cette opération et à chaque étape le nombre de symboles diminue. On construit de cette manière un arbre dont les feuilles sont les symboles à coder et les embranchements les codages intermédiaires.

III.2. Algorithme de codage:

Étape 1 : Construire une table contenant différentes lettres et leurs nombres de fréquence.

Etape 2 : Assortir les lettres dans un ordre croissant selon leurs nombres de fréquence.

Étape 3 : Ajouter les premiers nombres à deux fréquences et puis ré- arrangé la table encore.

Étape 4 : Répéter l'étape 3 jusqu'à ce qu'un nombre à fréquence unique soit réalisé.

Étape 5 : Construire l'arbre de Huffman en assignant à chacun des paires de branches avec (0.1) pour toutes les branches de l'arbre.

Étape 6: Récrire les lettres selon ce qui précède Arbre de Huffman.

Étape 7: Construire la table finale contenant toutes les lettres secrètes avec leurs codes.

Etape 1et 2

Lettre	Fréquence
T	1
H	1
I	2
S	2

étape 3,1^{er} itération

Lettre	Fréquence
I	2
S	2
T, H	2

2eme itération

3eme itération

Lettre	Fréquence
I,S	4
T,H	2

Lettre	Fréquence
I,S,T,H	6

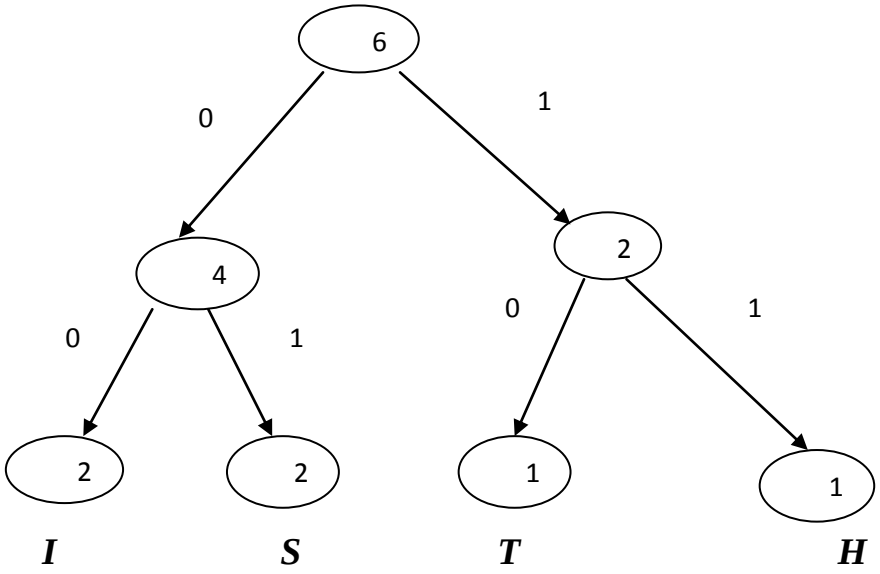


Figure III. 1:l'arbre du Huffman.

Lettre	*Code*
I	*(00)*
S	*(01)*
T	*(10)*
H	*(11)*

Table III.1:*Table des codes*

III.3. Algorithme de décodage:

On appelle la traduction d'un code v en un texte w la décompression de v en w. La méthode de Huffman se sert d'un arbre binaire aux feuilles duquel se trouvent les caractères à coder. La décompression applique L'algorithme suivant : elle part de la racine de l'arbre et suit le chemin indiqué par le booléen (faux pour gauche et vrais pour droit). Dés qu'on arrive à une feuille, on ajoute au résultat le caractère associé à cette feuille et on recommence le décodage à la racine de l'arbre. Quand le code est parcouru en entier, on a reconstruit le texte.

Par exemple, considérons l'arbre :

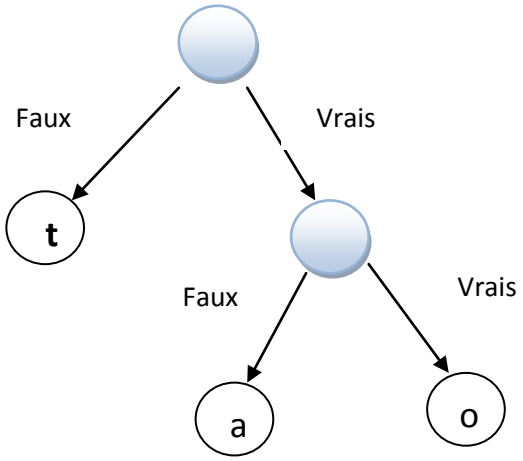


Figure III. 2: l'arbre du Huffman de décompression.

La décompression du code [faux; vrais; faux; vrais; vrais] donne le texte suivant :

['t' ;'a' ; 'o']

IV. Méthode de modification de direction(EMD):

IV.1. Définition :

Cette méthode cache chaque chiffre des codes de Huffman dans l'image segmentée de couverture en augmentant une valeur de groupe par 1 si **S** inferieur ou égale à **n**,ou en la diminuant par 1 si **S** est supérieur à n ou bien ne change pas si **d** égale à **f** ou **S =0**.

IV.2. La technique de cache :

S=(d-f)mod(2*n+1).

f=[∑ (gi * i)] mod (2*n+1).

Sachant que :

d: le code Huffman du caractère que l'on veut cacher dans ce groupe.

S: spécifie la position de la valeur de groupe qui sera modifiée.

n: le nombre des valeurs de groupe.

Exemple :

Soit : **n=4**.

- Le code Huffman de '**a**' est **d= 3.**

- Le groupe **g=[99,110,120,130]**

Donc :

f =(99 * 1 +110 * 2 + 120 *3 +130 * 4) mod (9)=2.

S=(3 - 2) mod 9 = 1.

Alors **S** inférieur à **n.**

Donc **g(s)=g(1)+1.**

Et le groupe devient **g=[100,110,120,130].**

IV .3.Algorithme de cache (EMD):

Entrée : couvrir l'image (g1, g2, ..., GN), chiffres du codage de Huffman **d**.

Sortie: stego-image

Etape1: For i=1:n

f=(sum(gi * i)) mod (2n+1)

End

Etape 2 : Si f = d alors s = d - mod f (2n+1)

Etape 3 : Si s < n alors augmentent g par 1

Etape 4 : si s > n alors diminuent g (2n+1-s) par 1

Etape 5 : Répéter 1 à 4 jusqu'à ce que tous les chiffres du message secret soient traités.

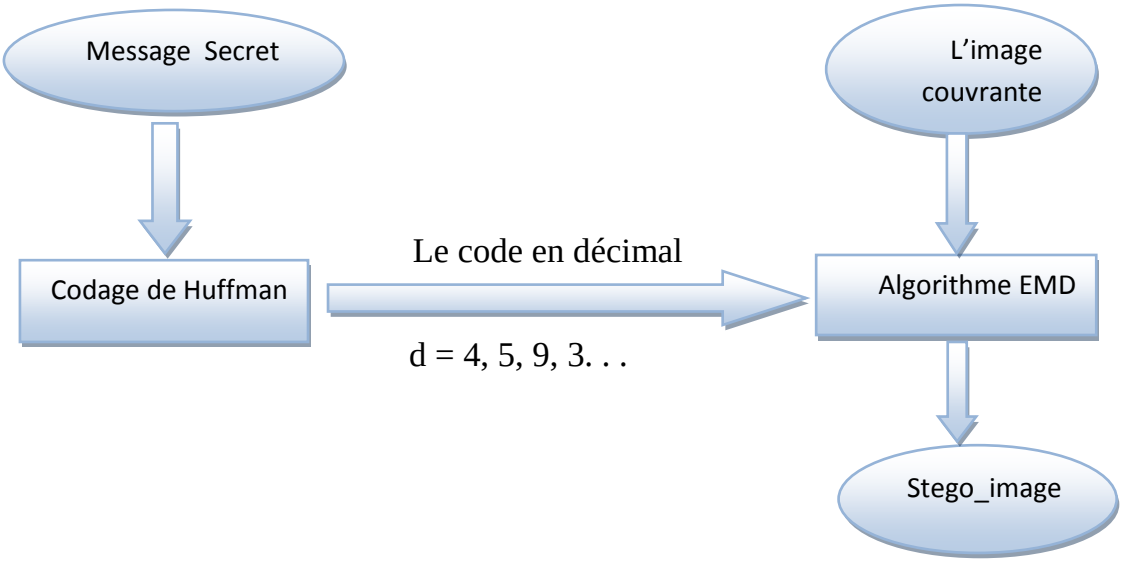


Figure III. 3: Schéma Le cachement du texte. [8]

IV.4. Récupération des codes cachés :

Comme on a reçu la stego_image, on commence par la décomposition de sa matrice en sous tableaux de 20 éléments, en suit on les applique l'algorithme EMD d'extraction pour obtenir le code de Huffman **d=[∑ (g(i) * i)] mod (2 * n + 1)**, en suit on prend ce code et on utilise le dictionnaire de Huffman pour savoir le caractère cachée.

On prend le résultat de l'exemple précédent **g=[100,110,120,130], n=4 .**

On calcule **d=(100 * 1 + 110 * 2 + 120 * 3 + 130 * 4) mod(9) = 3.**

Ensuit après l'utilisation de dictionnaire d'Huffman pour **d=3** on obtient le caractère **' a '**.

IV.5. Algorithme d'extraction :

Entrée : Stego-image

Sortie : Données secrètes

Etape 1: Pour i=1 : n

d=(sum(gi' * i)) mod (2n+1)

End.

Etape 2 : Converti (d) au binaire.

Etape 3 : Décoder ce nombre binaire à la lettre originale en employant le décodage de Huffman.

Etape 4 : Répéter 1-3 jusqu'à la fin du texte

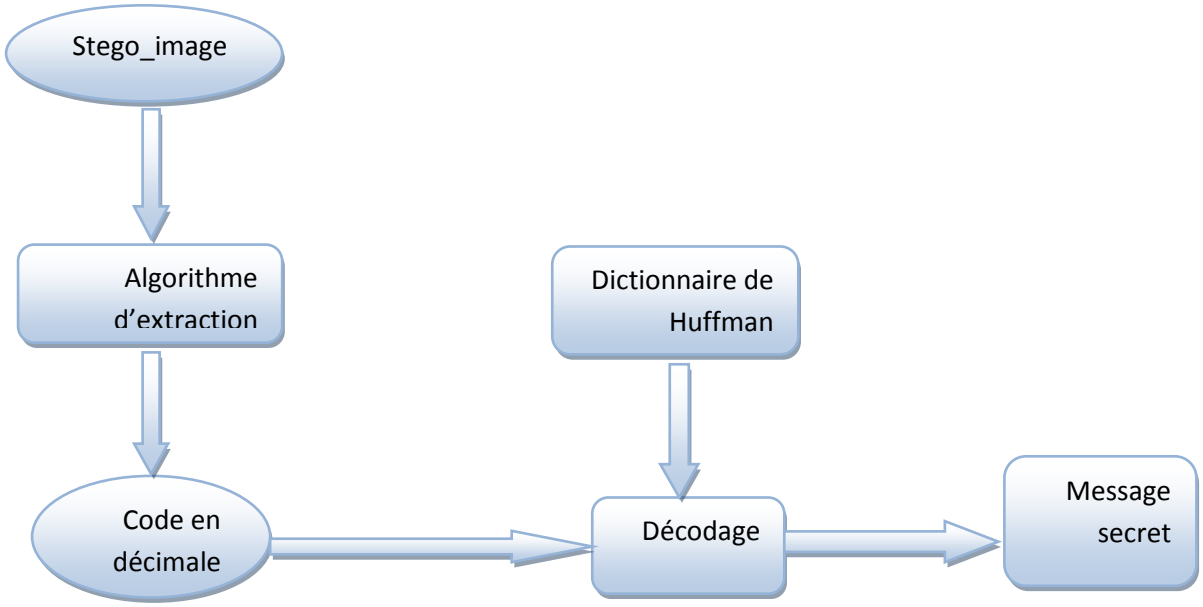


Figure III. 4: La méthode d'extraction de l'information. [8]

V. Les avantages et les inconvénients de la technique mixte:

V. 1. Les avantages :

- ✓ Technique d'utilisation simple et efficace.
- ✓ Moins de bruit appliquer sur l'image finale (les changements est invisible sur l'oille humain).

V. 2. Les inconvénients:

- ✓ L'image ne peut pas cacher un message de longue taille si le code d'Huffman maximal et plus grand, **d <= 2 * n + 1**.
- ✓ Le bruit est peut être élevé si **d** maximal plus petit (main invisible par l'œil humain). **[8]**

VI. Conclusion :

Dans ce chapitre, on a étudier une technique de masquage des données, elle utilise le codage de Huffman et la méthode EMD. Les messages secrets sont chiffrés, comprimés et inclus dans des images de couverture avec une sécurité élevé sans compromettre la qualité des stego-images.

CHAPITR IV

Simulation et Analyse Des résultats

I. Introduction:

Dans les chapitres précédent on a discuté théoriquement sur les techniques utilisés dans notre projet " le technique mixte codage Huffman et méthode EMD " et dans ce chapitre on va détailler pratiquement dans une application réalisée par le langage Matlab capable de réaliser et traiter notre application (stéganographie).

II. les étapes de réalisation:

La réalisation de cette application se compose de deux grandes parties (partie de cache et la partie de récupération).

II.1. Schéma général pour la cache de message :

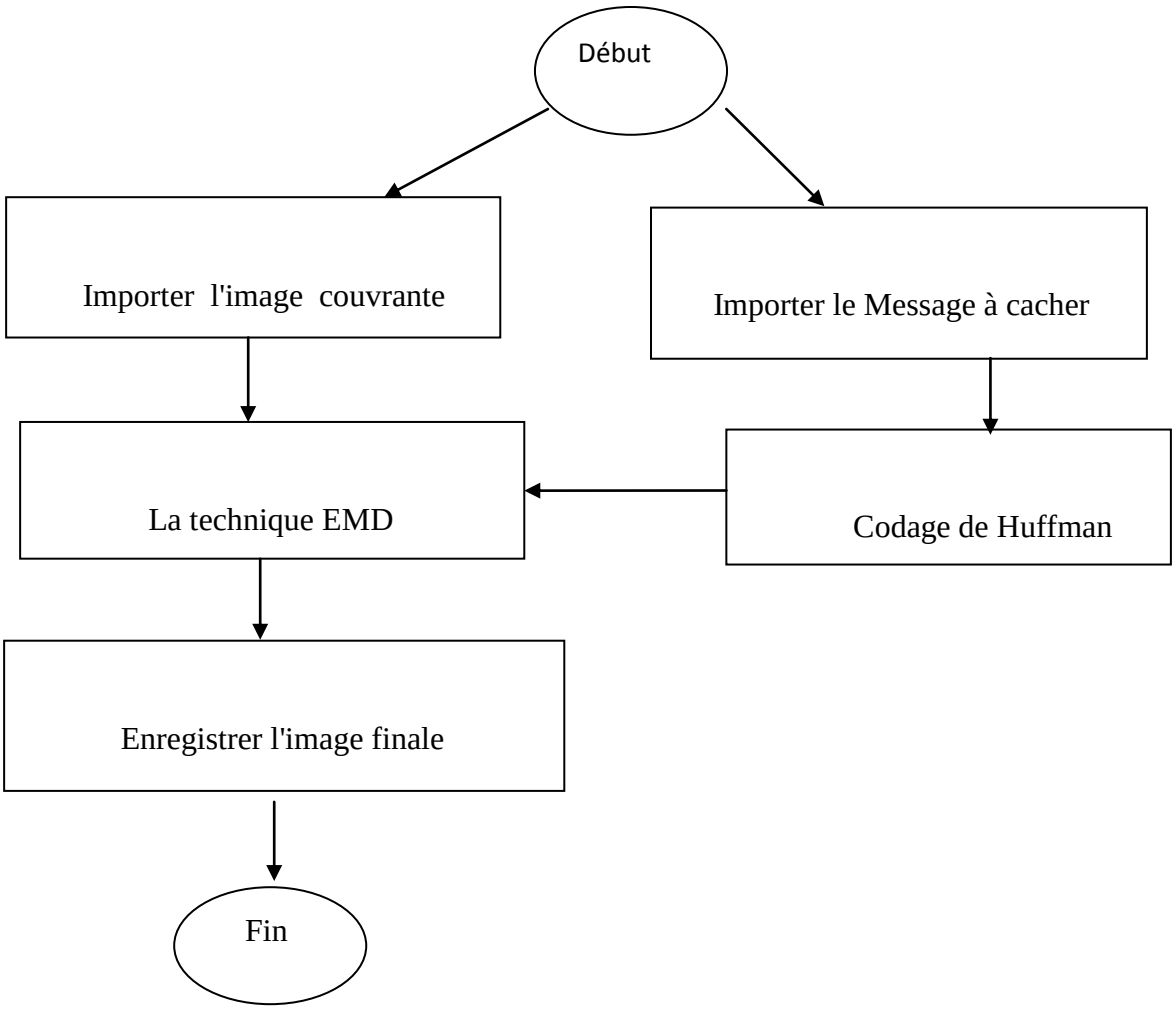


Figure IV.1: L'organigramme général de la stéganographie.

- ✓ . Lire l'image par la fonction de matlab imread();
- ✓ .saisir le message ou bien l'ouvrier de fichier.txt;
- ✓ .coder le message par le codage d'Huffman par la fonction 'huffman(tab)';
- ✓ .cacher les code d'Huffman dans l'image par la technique EMD, par la fonction emd_cacher(code);
- ✓ . enregistrer l'image final par la fonction matlab 'imwrite()' sous le nom "stegano.bmp"

II.2. Schéma général pour la récupération de message :

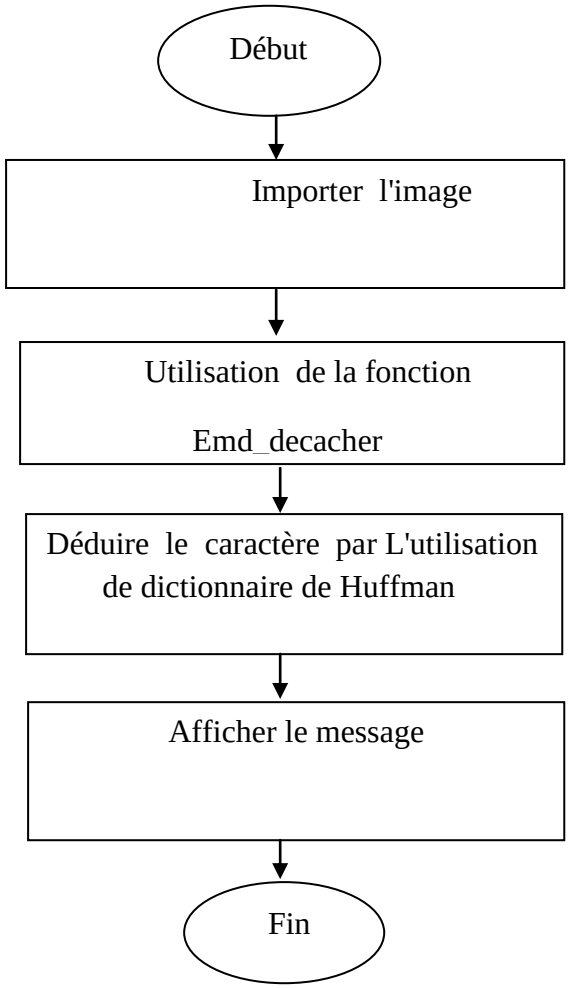


Figure IV.2: l'organigramme général pour la récupération de message**.**

- ✓ . Lire l'image de nom "stegano.bmp" par la fonction imread();
- ✓ .récupérer les codes d'Huffman par la fonction Emd_decacher(g');
- ✓ .récupérer les caractères de message par le dictionnaire d'Huffman.
- ✓ .afficher le message s'il est petit ou l'écrire sous un fichier.txt.

II.3. Schéma général de codage d'Huffman :

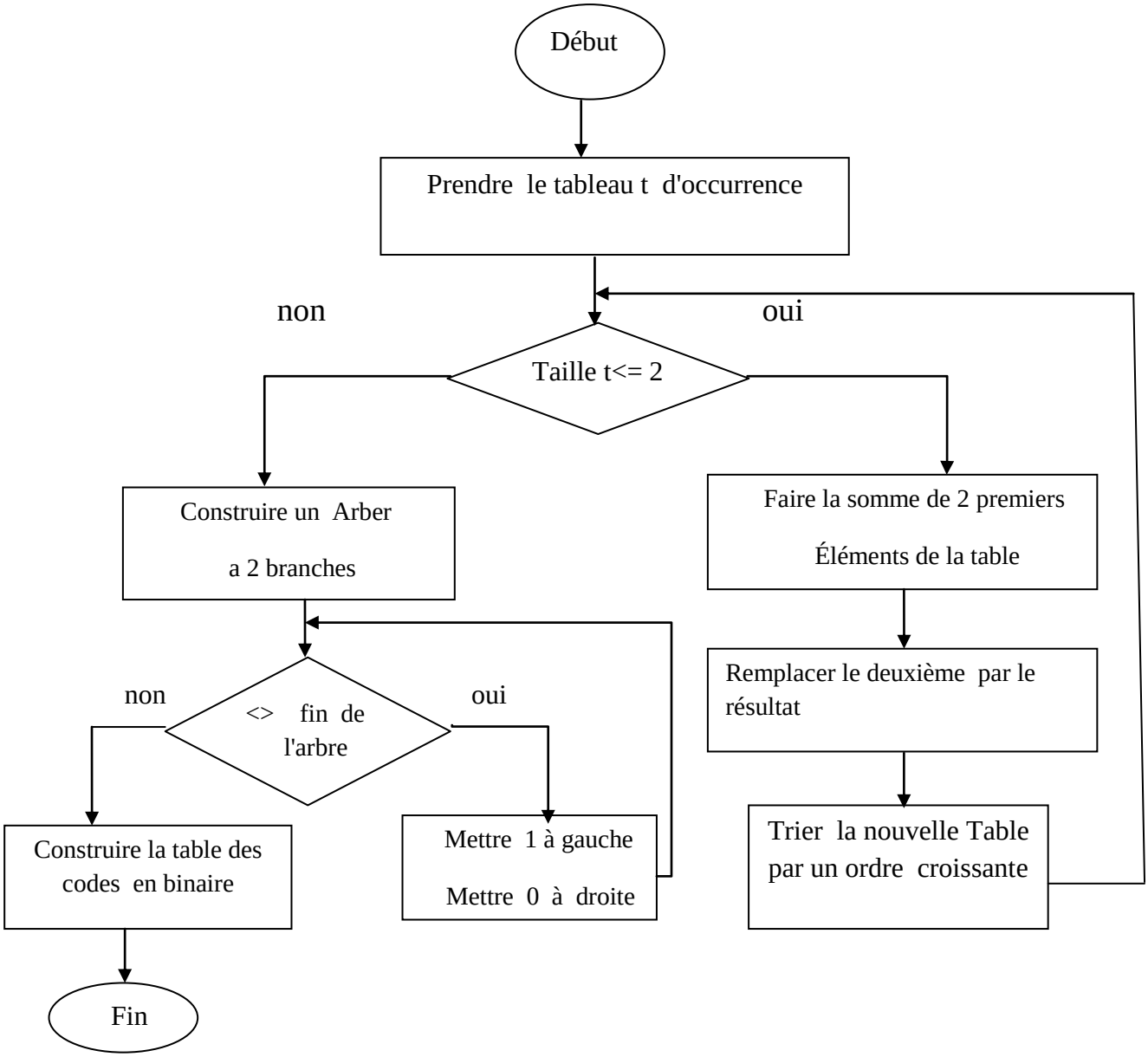


Figure IV.3: l'organigramme détaillé pour le codage de Huffman.

- ✓ Lire la table d'occurrence
- ✓ Répète les opérations suivantes jusqu'à les deux derniers éléments de la table.
  - Sommer les deux premiers éléments de la table.
  - Remplacer la deuxième valeur par le résultat.
  - Trier la nouvelle table.
  - Fin.
- ✓ Construire un arbre à deux branches.

- ✓ Mettre 1 à la gouache.
- ✓ Mettre 0 à la droite.
- ✓ Construire la table des codes.
- ✓ Fin.

II.4. Schéma de la technique EMD :

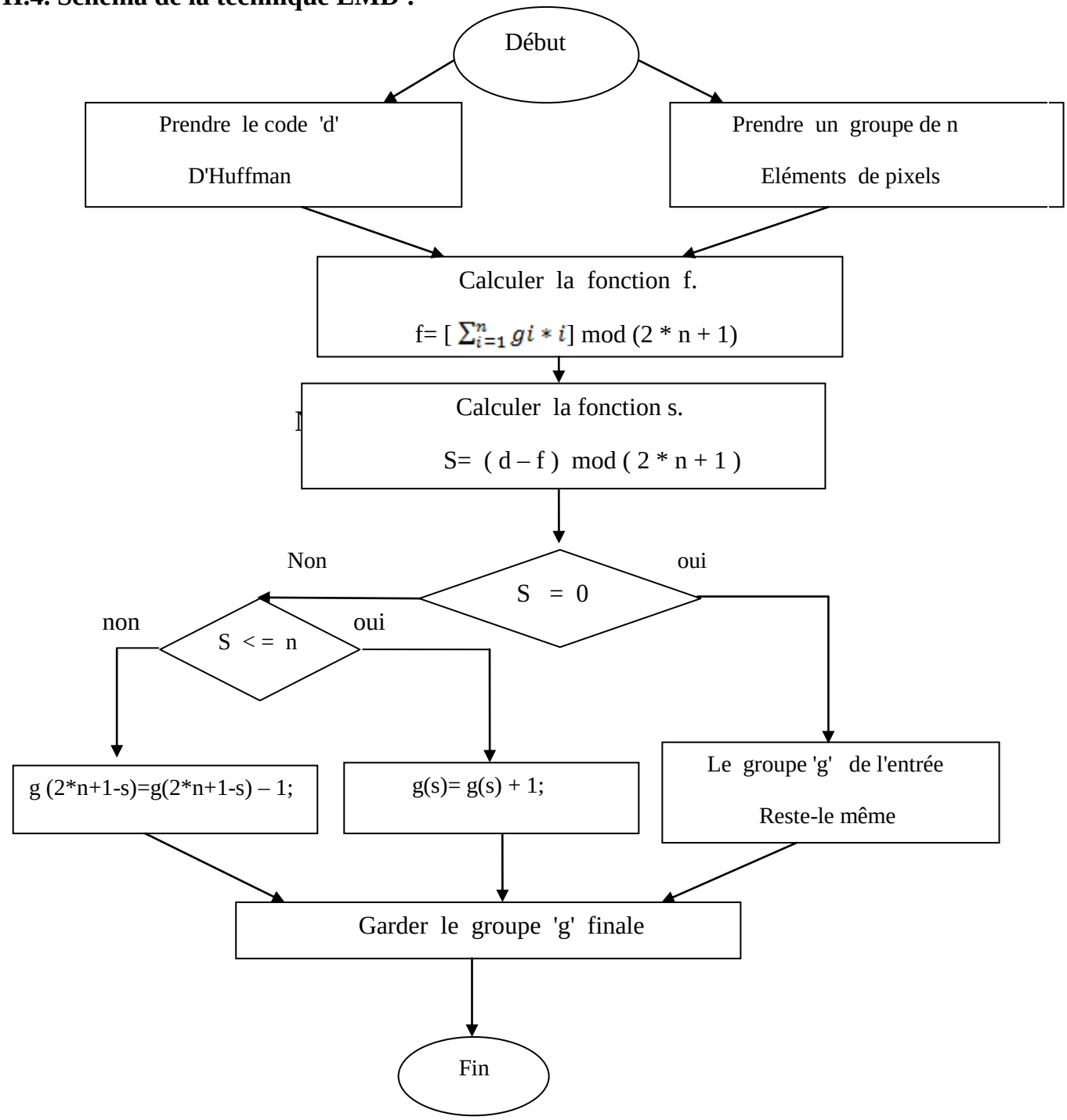


Figure IV.4: l'organigramme détailler pour la technique EMD.

- ✓ Lire un groupe g de n pixel.
- ✓ Lire le codage de Huffman.
- ✓ Calculer f=$[\sum_{i=1}^{n}(gi * i)]\ mod\ (2 * n + 1)$.
- ✓ Calculer s=(d-f) mod 2n+1 .

If s=0

Group g ne change pas

Sinon

Si s<=n incrémenter par 1

G(s) = g(s) +1

Sinon décrémenter par 1

G (2n+1-s) =g (2n+1-s)-1

End.

- ✓ Garder le groupe final g.

II.5. Schéma détaillé d'EMD_décaché:

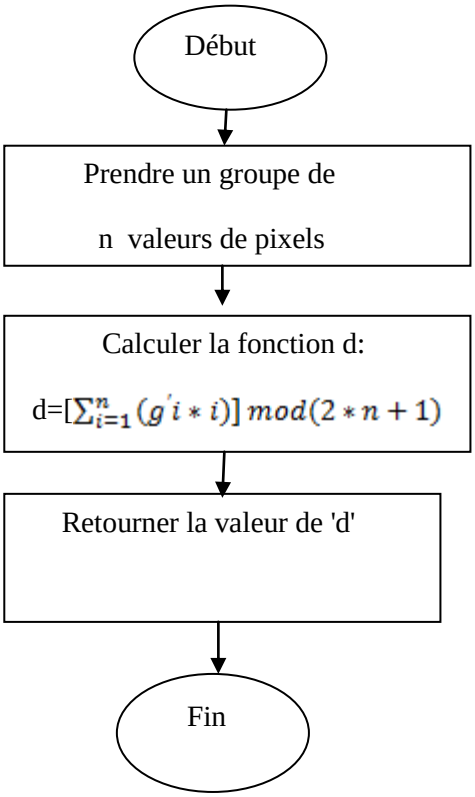


Figure IV.5:l'organigramme de (emd_decacher(g').

- ✓ .pendre un groupe de n valeur de pixel.
- ✓ .calculer le code d'Huffman par la fonction d=$[\sum_{i=1}^{n}(g'i*i)]\ mod(2*n+1)$.
- ✓ .Retourner le code d.

II.6. Le cas d'utilisation :

II.6.1. Définition de cas d'utilisation:

Un cas d'utilisation est une manière spécifie que d'utiliser un système. Les acteurs sont à l'extérieur du système ; ils modélisent tout ce qui interagit avec lui. Un cas d'utilisation réalise un service de bout en bout, avec un déclenchement, un déroulement et une fi n, pour l'acteur qui l'initie.

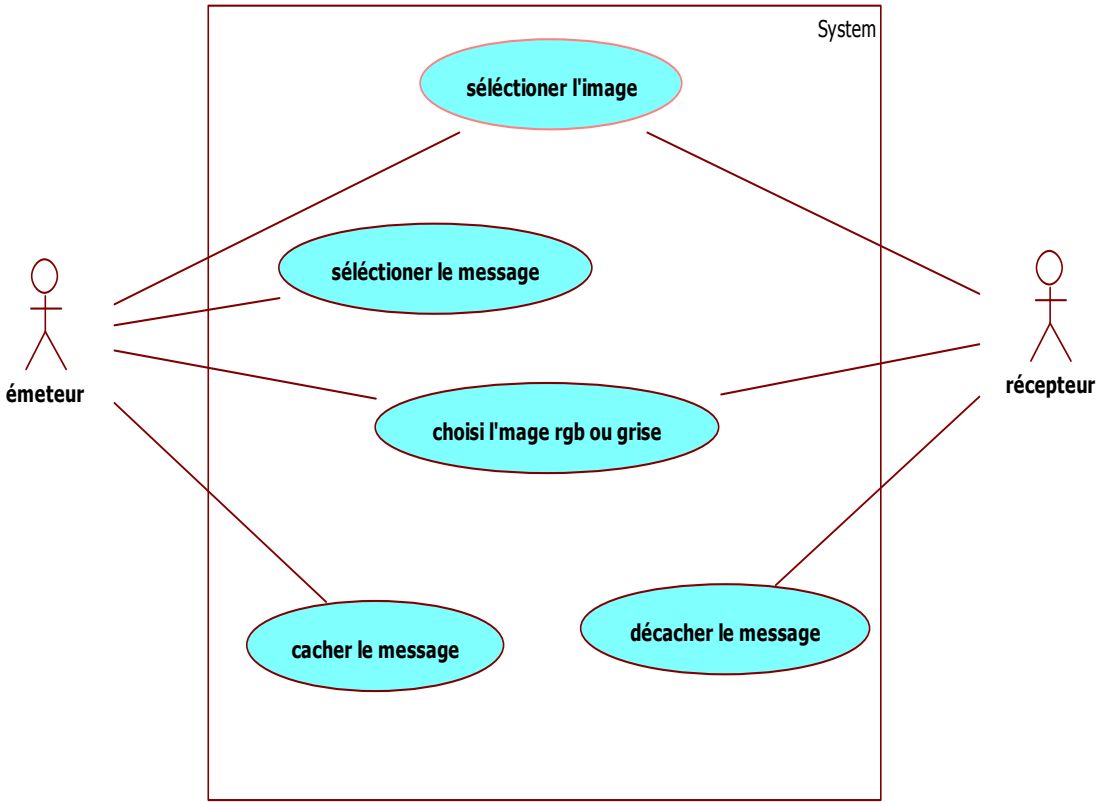


Figure IV.6**: Diagramme de cas d'utilisation.**

- **Sélectionner l'image :** l'émetteur choisi le couvre message (image) et le récepteur choisir l'image qui la déjà recevoir**.**
- **Sélectionner le texte** : l'émetteur choisir le secret texte pour intégrer dans le couvre.

- **Choisi le type d'image:** l'émetteur choisi le type de l'image (image en couleur (rgb) ou noir et blanc (grise)) pour cacher le texte et le récepteur doit regarder au couleur de l'image qui la choisi ensuit sélectionnera le type selon les couleurs.
- **Cacher le message :** l'émetteur appuyer sur le bouton (cacher) pour cacher le texte dans l'image.
- **Extrait ou d'écacher le message :** le récepteur appuyer sur le bouton (extraire le message) pour récupérer le texte.

III.1. Présentation de l'interface:

Cette application se compose de deux parties fondamentales un pour cacher le message et l'autre pour le récupérer, et on a représenté le premier par une figure sous le nom "emeteur" et le deuxième par une figure de nom "récepteur".

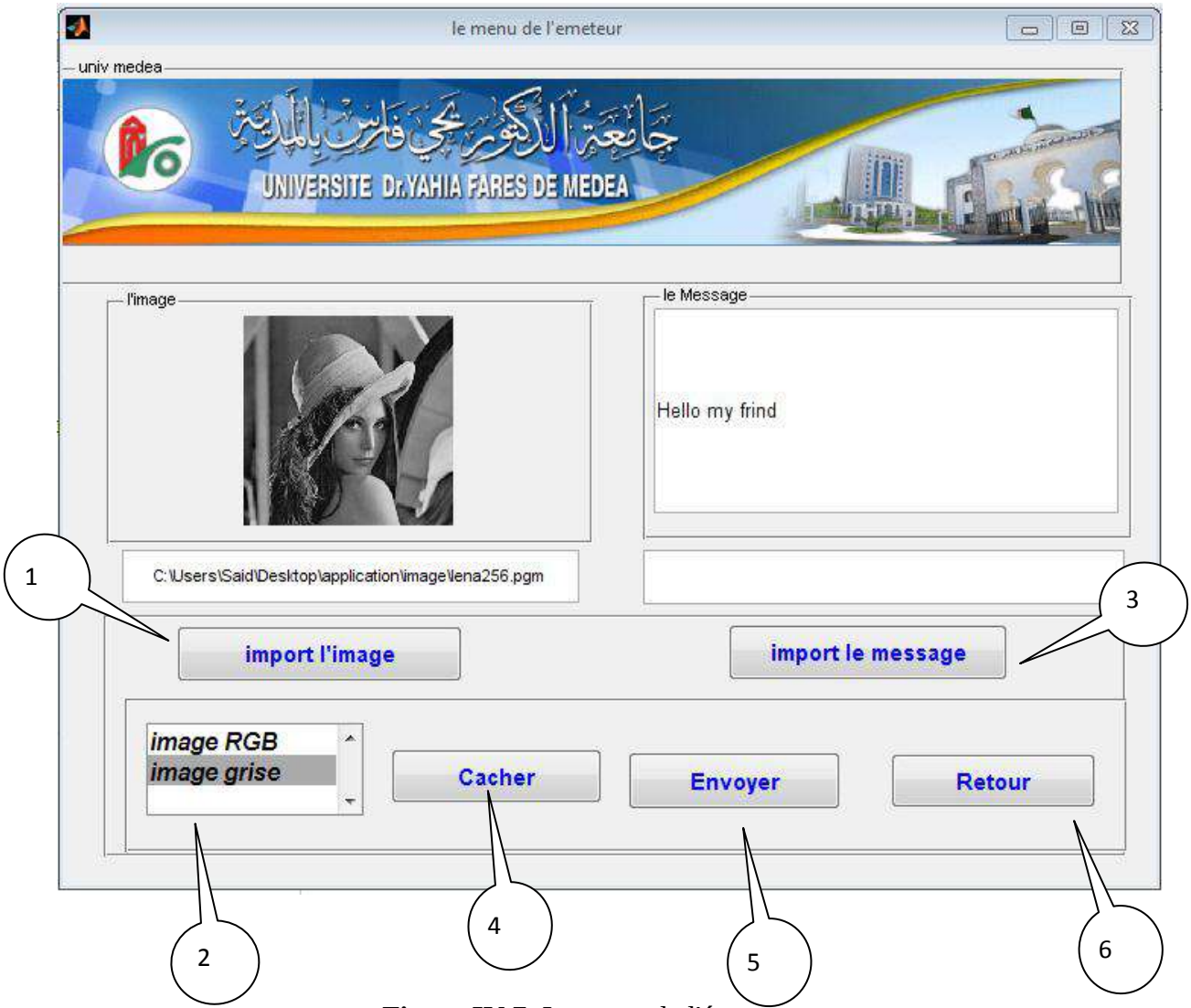


Figure IV.7: Le menu de l'émetteur.

1- Importer l'image à utiliser comme couvre.
2- Choisir le type de l'image noir et blanc (grise) ou coloré(RGB).
3- Importer ou bien saisir un message à cacher.
4- Cacher le message dans l'image.
5- Enregistrer l'image finale sur le bureau sous le nom "stegano.bmp".
6- Faire le retour au menu principal.



Figure IV.8: Le menu de récepteur.

1- Importer l'image de nom "stegano.bmp".
2- Choisir le type de cette image.
3- Faire la récupération de message caché dans cette image.
4- Faire la sortie de l'application.
5- Faire le retour au menu principal.

III.2. Présentation et Analyse des résultats:

III.2.1. Logiciel Matlab :

MATLAB est le langage de haut niveau et un environnement interactif utilisé par des millions d'ingénieurs et de scientifiques du monde entier. Il vous permet d'explorer et

de visualiser des idées et collaborer dans toutes les disciplines, y compris traitement du signal et de l'image, les communications, les systèmes de contrôle et finance computationnelle.

Vous pouvez utiliser MATLAB dans des projets tels que la modélisation de la consommation d' énergie pour construire les réseaux électriques intelligents , développement des algorithmes de contrôle pour les véhicules hypersoniques , l'analyse des données météorologiques pour visualiser la trajectoire et l'intensité des ouragans , et exécutant des millions de simulations pour identifier le dosage optimal pour les antibiotiques .

III.2.2. La base de données (image, Message):

Les données utilisées dans cette étude seront expliquées brièvement. Ces données ont inclus quatre images standard aux niveaux de gris des tailles 512*512 pixels, et 256*256 pixels. Celles-ci incluent : Lena, baboon. Ces images sont employées comme images de couverture. En outre, ces images contiennent différentes niveaux de gris qui donne la possibilité d'obtenir des résultats précis pour évaluer l'imperceptibilité. Puis, l'attaque est appliquée sur ces images après le processus d'encastrement. Habituellement, ces images sont employées dans toutes les études qui traitent le masquage de données.



Figure IV.9: lena512.

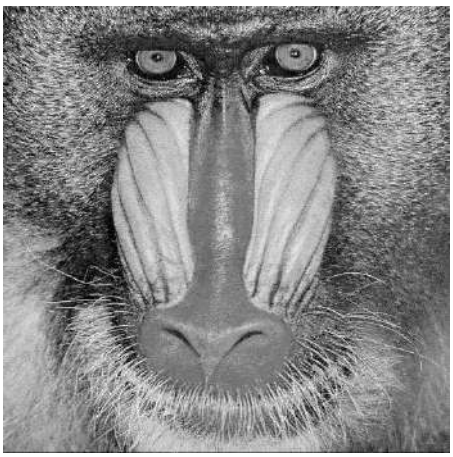


Figure IV.10:baboon512.



Figure IV.11: lena256.

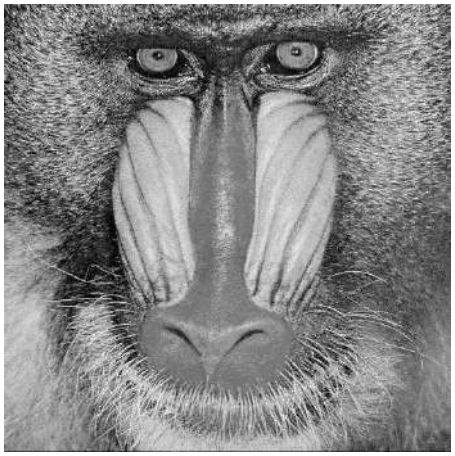


Figure IV.12:baboon256.

En outre, un texte arbitraire est employé comme message secret. Pour évaluer la qualité de la stego-image, le rapport signal/bruit maximal suivant (PSNR) est utilisé:

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}} .$$

Sachant que le MSE se rapporte à l'erreur de moyenne carrée entre deux Pixel.

$$MSE = \sum_{i=1}^{r*c*k} \frac{(g_i - g'_i)^2}{(r * c * k)}$$

Ou. r, c, k: sont les dimensions de l'image.

IV. résultat et discussion:

On veut cacher le message clair: "Hello my frind " dans l'image "lena.pgm" et pour faire ça on utilise la figure de nom émetteur de l'interface graphique.



Figure IV.13 :.l'image couvre

Le caractère	Le code d'Huffman (binaire)	Le code d'Huffman (décimal)
'H'	101100	44
'e'	111110	62
'l'	111011	59
'o'	100010	34
' '	100101	37
'm'	100011	35
'y'	101111	47
'f'	111100	60
'r'	101000	40
'i'	111111	63
'n'	100100	36
'd'	111010	58

Table IV.1. Table des codes d'Huffman de message secret.



Figure IV.14: L'image stegano.bmp.

Pour la récupération de message on prend l'image "stegano.bmp" et on utilise le menu de récepteur de l'interface graphique et on a obtenu le texte " Hello my frind".

On a utilisé l'image de " lena.pgm" de taille 512*512 avec 5 messages clair de taille déférents et comme le bruit est invisible par l'œil humain on est besoin de calculer le bruit appliqué au l'image "stegano.bmp".

Les messages	La taille de message(caractère)	MSE	PSNR
Secret1.txt	1024	0.3247	53.0164
Secret2.txt	2048	0.3259	52.9997
Secret4.txt	4095	0.3288	52.9614
Secret8.txt	8183	0.3337	52.8977
Secret16.txt	16383	0.3442	52.7625

Table IV.2.Résultat de la méthode proposée d'image de Lena.

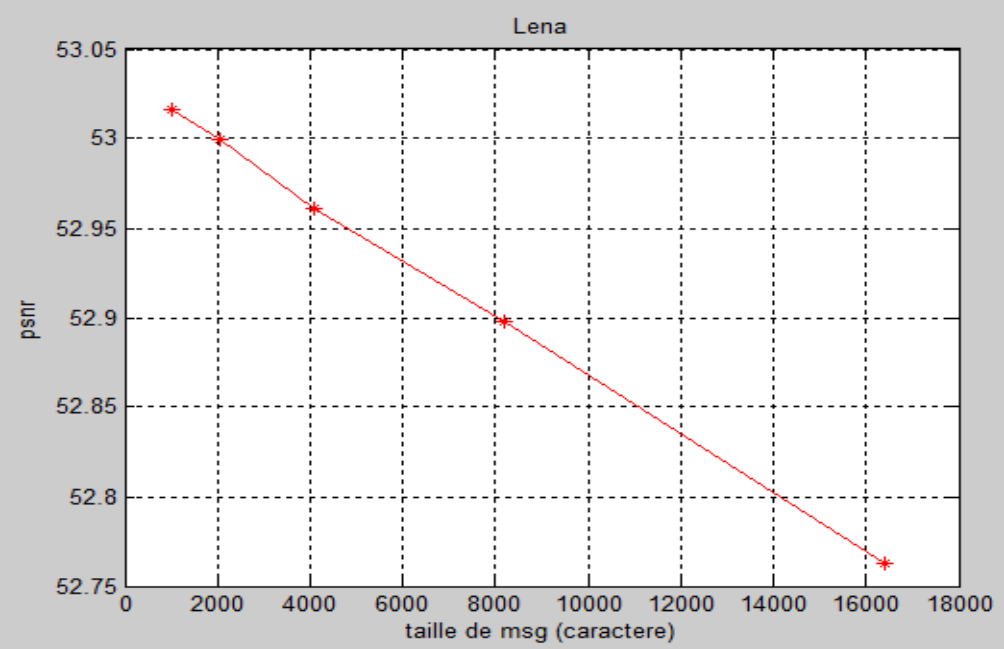


Figure IV.15 : résultat de PSNR sur image Lena.

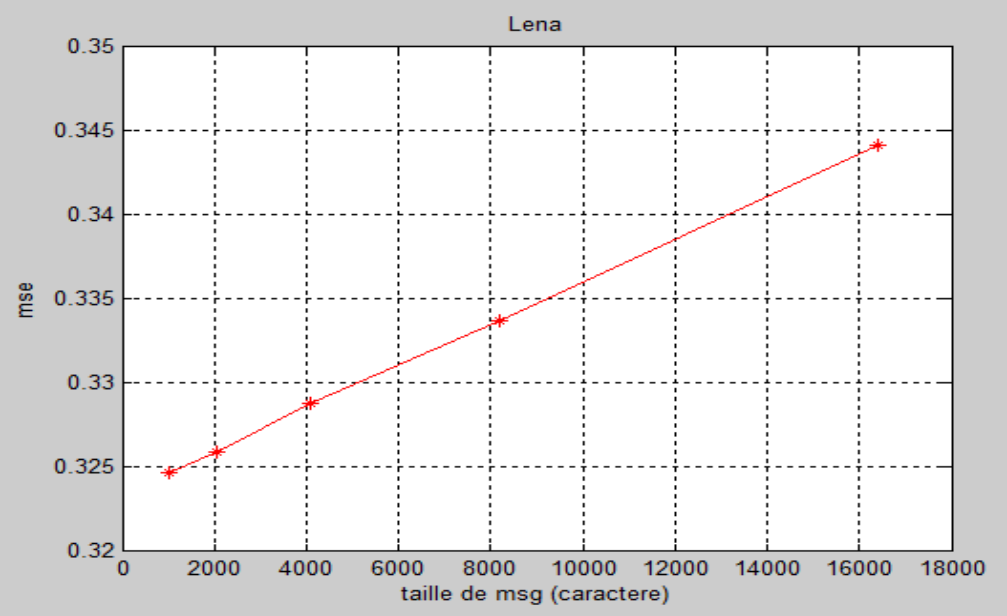


Figure IV.16 : résultat de MSE sur image lena.

			
Image original	Contient secret2	Contient secret8	Contient secret16
A	B	C	D

Table .IV.3. : Image Lena avec des messages secrets de différentes tailles.

On observe que l'effet de bruit dans les images B,C et D qui contient des messages secrets de tailles respectivement 2048 caractères ,8183 caractères et 16383 caractères, est non visibles par l'œil humain malgré la taille importante des messages (16383 caractères).

Les messages	La taille de message (caractère)	MSE	PSNR
Secret1.txt	1024	0.2677	53.8547
Secret2.txt	2048	0.2690	53.8331
Secret4.txt	4095	0.2716	53.7914
Secret8.txt	8183	0.2765	53.7142
Secret16.txt	16383	0.2870	53.5520

Table IV.4. Résultat de la méthode étudiée d'image de Baboon.

On a pris 5 message de taille différents comme des messages du test, et 2 images (Lena et baboon) comme des couvres de ces textes, et on a gardé les valeurs de PSNR, MSE, et la taille de message pour tracer le graphe de PSNR par apport la taille de message.

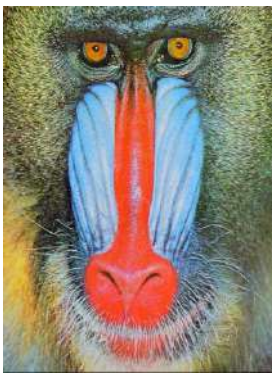
			
Image original	Contient secret2	Contient secret8	Contient secret16
A	B	C	D

Table. IV.5 : Image Baboon avec des messages secrets de différentes tailles.

On observe que le bruit sur les images B,C et D qui contient des messages secrets de tailles respectivement 2048 caractères ,8183 caractères et 16383 caractères, n'as pas d'effet visuel, et il y a aucune dégradations visibles sur les trois images B,C et D .

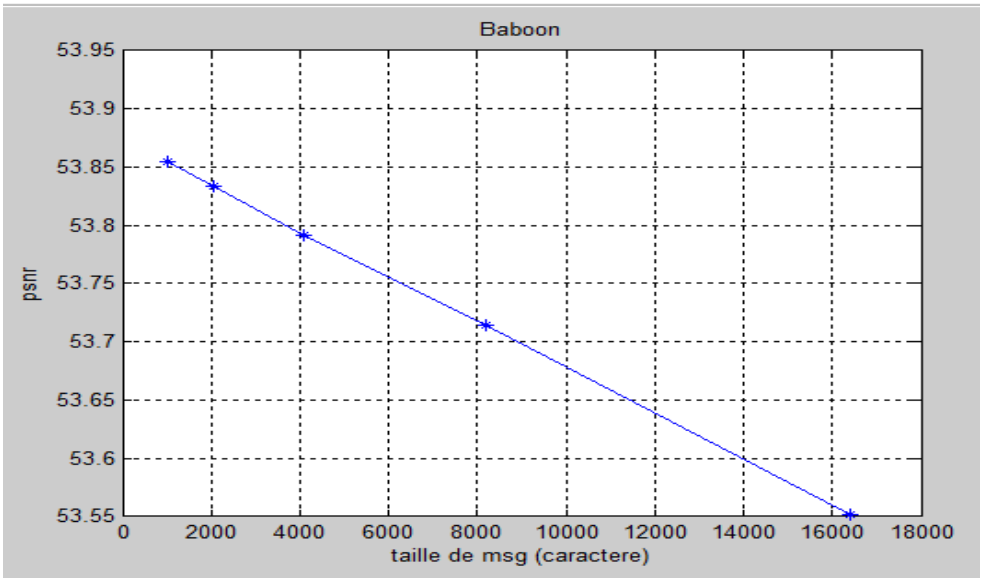


Figure IV.17 : résultat de PSNR sur image Baboon.

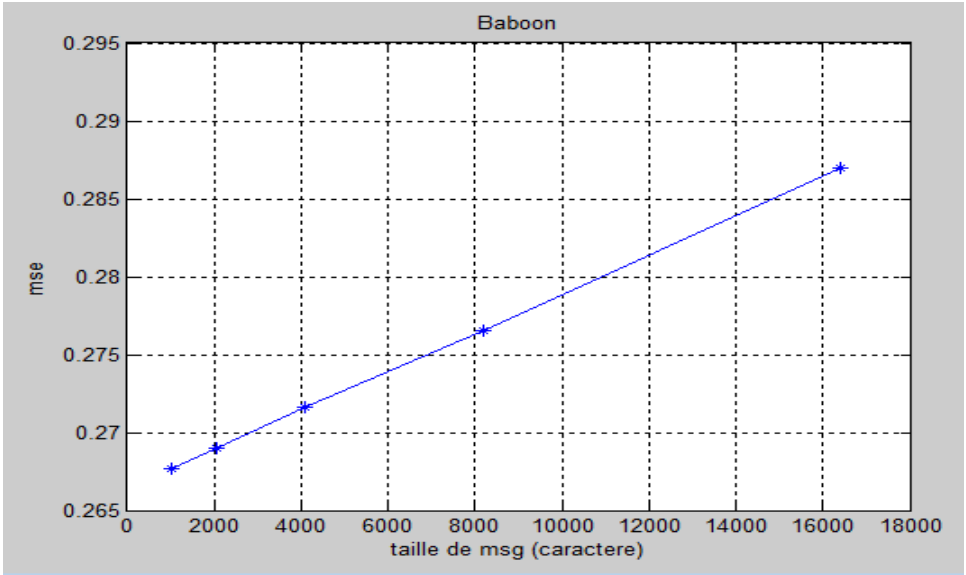


Figure IV.18 : résultat de MSE sur image Baboon.

V. Conclusion :

Dans ce chapitre on a vu le résultat de dissimulation de côté d'exactitude et de bruit, et on déduit que le technique mixte codage d'Huffman et la modification de direction qu'il est fiable et efficace par ce que on ne peut pas voir les changements sur l'image bruité par la vision humain.

Conclusion générale

Conclusion général:

Jusqu'à présent, il y avait peu de méthodes de dissimulation de données offrant une grande capacité de messages secrets et bonne stego qualité d'image. Par conséquent, une efficacité de données cachant régime fondé sur la méthode EMD généralisée avec un procédé d'incrustation simple a été proposée dans le présent document.

Le schéma étudié ne pas exiger que l'expéditeur de transformer le message secret dans une forme de numéro spécial avant de l'intégrer, de sorte que la méthode a une meilleure capacité que celle du schéma EMD .Selon notre analyse, non seulement maintient les avantages de EMD, mais maintient également une bonne qualité d'image stego.

La capacité d'insertion est supérieure à 1 bpp lorsque la taille bloc augmente dans le schéma étudié. En d'autres termes, cette technique est un excellent système de cache des données.

BIBLIOGRAPHIE

[1] Lescop Yves [SÉCURITÉ INFORMATIQUE].

[2] mémoire de M.Oihal,Y.Zibani et M.Khalfaoui [Conception et réalisation d'un outil pour sécuriser la communication par message textuel] Octobre 2003.

[3] Marine Minier INSA Lyon [Cryptographie : de la théorie à la pratique] novembre 2005.

[4] ROGERIE . Grégory[La steganographie] Janvier 2002.

[5] Bénoni . Martin [Steganographie techniques] Avril 2007.

[6] S. Mouline [Codage d'information] décembre 2006.

[7] MVOGO NGONO Joseph [Principes généraux de codage entropique d'une source] juin 2011.

[8] Ali m-Ahmad1a, Ghazali Bin Sulong1b, Mohd. Shafry B. Mohd. Rahim1c, Saparudin2, [A 2-tier Data Hiding Technique Using Exploiting Modification Direction Method and Huffman Coding], ACEEE Int. J. on Information Technology, Vol. 02, No. 02, April 2012

Les messages de test:

Secret1:

Data protection and securing the personal information has become an important issue within the human digital life. Therefore, the demand of having a secure method to transfer the secure data is dramatically increasing. Steganography is one of the most widespread approaches of securing data which insists on concealing the secret data inside another data in a way that nobody suspects to its existence. Generally, any type of files can be used to convey the secret data. Nevertheless, common files like images that are used more frequently have the higher priority to be selected for this job. It is obvious that when a part of data as a secret message is embedded into a file, the quality of the container will be decrease. the steganographic algorithm used also influences the effectiveness of the system. In the interest of creating ever more secure algorithms and to account for some of the intrinsic weaknesses methods will be examin of forerunning algorithms, several classes of methods have emerged in th literature**.**

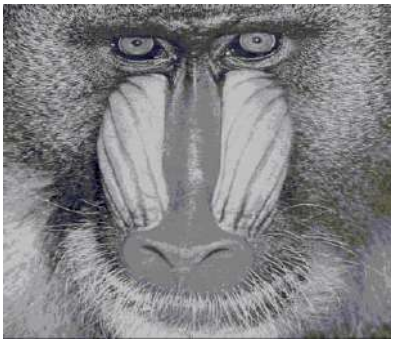
secret2, secret4, secret8, secret16, secret32.

Sont le message secret1 dupliqués 2, 4,8,16 et 32 fois successivement .

Les images:



Lena



Baboon