الجمهورية الجزائرية الديمقراطية الشعبية

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE YAHIA FARES DE MEDEA
FACULTE DE LA TECHNOLOGIE

Département du Génie Électrique



Projet de fin d'études

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

Spécialité* : *système de télécommunications

THEME

Implémentation d'une méthode Stéganographique appliquée sur les signaux de paroles

Présenté par :

- BAHRIA Nawfal
- BEN KEBIR Billel

Encadré par :

- KHEDDAR Hamza

Année Universitaire **2016-2017**

Dédicace

Je dédie ce travail en signe de respect et de reconnaissance :

A celle qui a tout donné, tout sacrifié, à la femme qui règne sur mon cœur, " ma mère ".

A celui qui m'a toujours dirigé, guidé, aidé et encouragé afin de me voir affronter la vie avec sérénité et courage, à l'homme qui a toujours souhaité me voir à la hauteur, " mon père ".

A mes sœurs et toute la famille.

A Mohamed, Nesrine, Sohila

A toute la famille BEN KEBIR et BELHADJ sans exception

A mes chers amis Selman,Abdelfetah, Abdelhak, Issam, Krimou, Haitham, Abdallatif, Yaçine,Youcef ,Ayham *et à tous mes amis.*

A mes très chers collègues et toute la promotion 2017.

A la fin, je dédie très chaleureusement ce travail à mon cher ami et mon binôme BAHRIA Nawfal

Billel

Dédicace

Au-delà des personnes, des lieus et des temps, je dédie ce travail avec ma profonde conviction, à tous ce qui ont toujours cru et sans doute à la science. Cette lumière qui éclaire les esprits et leurs permet transcender les limites installées par les sociétés et les cultures dans leurs périodes de dégénérescence.

Je dédie ce travail à mes parents.

A mes frères.

A toute ma famille

A mes collègues et amis à l'université de Médéa.

A tous les enseignent de l'électronique et promotion (2016-2017).

A tous les membres de la famille

Amine ……

Nawfal

Remerciement

Tout d'abord nous remercions Dieu pour nous avoir guidés vers le chemin de la lumière et du savoir, pour nous avoir donné le courage et la volonté afin de pouvoir réaliser ce travail, puis nos parents pour leurs soutiens et leurs sacrifices.

Nous tenons à remercier vivement tous ceux qui nous ont aidés à élaborer Ce mémoire et en particulier notre Encadreur Mr. KHEDDAR Hamza pour son aide et ses orientations précieuses.

Nous tenons également à remercier les membres du jury, pour l'honneur Qu'ils nous ont accordé, en acceptant de juger notre travail.

Nous remercions aussi l'ensemble des enseignants de l'institut de Génie Électrique qui ont contribué à notre formation.

Que tous ceux et celles qui nous ont apporté leur soutien et qui nous ont Aidé de près ou de loin pour l'achèvement de ce projet trouvent ici l'expression De notre vive et sincère reconnaissance, en particulier nos familles et nos amis

ملخص :

تطورت الشبكات الرقمية في خضم السنوات الأخيرة أصبحت حتمية لا يمكن الاستغناء عنها فيما يخص الاتصلات المعاصرة، بث إشارات في هذه الشبكات يحتمل مشاكل عدة و التي لم تحل إلى حد الساعة و كمثال لهذه المشاكل أمن البث، الخصوصية، حالة الشئ المرسول، دقة الإرسال.

الهدف من مشروعنا هو دراسة و محاكاة لتطبيق طريقة على الإشارة الصوتية . هذه الطريقة تستخدم لإخفاء المعلومة في إشارة كلام ، تعرف باسم الستيغانوغرافيا.

الكلمات المفتاحية :

كريبتوغرافيا، تشفير، ستيغانوغرافيا، نظام وشم، نظام بث ستيغانوغرافي، غلاف، نطاق التردد، ملف ستيغو، نظام السمع البشري، نوعية إدراك الكلام.

Résumé :

Les réseaux numériques ont fortement évolué ces dernières années et sont devenus inévitables pour les communications modernes. La transmission des signaux sur ces réseaux soulève un nombre important de problèmes qui ne sont pas encore tous résolus comme par exemple, la sécurité, la confidentialité, l'intégrité et l'authenticité des signaux audio pendant leur transmission. Le but de notre projet est l'étude, la simulation et l'implémentation d'une méthode stéganographique sur les signaux audio. Cette méthode est utilisée pour cacher des données dans un signale parole, elle est connue sous le nom: stéganographie audio.

Mots clés :

Stéganographie, système de transmission stéganographique, fichier stego, le système auditif humain, la qualité perceptuelle de la parole.

Abstract:

Digital networks have evolved greatly in recent years and have become inevitable for modern communications. The transmission of signals on these networks raises a number of problems which are not yet solved, such as the security, confidentiality, integrity and authenticity of the audio signals during their transmission. The aim of our project is the study, simulation and implementation of a steganographic method on audio signals. This method is used to hide data in a speech signal, it is known as: audio steganography.

Key words:

Steganography, steganographic transmission system, stego file, human auditory system, the perceptual quality of speech.

TABLE DE MATIERES

Table de matières ..... **I**

Liste des Figures ..... **IV**

Liste des tableaux ..... **VI**

Liste des Acronymes ..... **VII**

INTRODUCTION GENERALE **1**

CHAPITRE I: SYSTEME DE TRANSMISSION SECURISE

Introduction

I.1.Systeme de transmission numerique **2**

I.2.Cryptographie **4**

I.3.Systeme de tatouage **6**

I.4.Systeme de transmission steganographique **7**

I.4.1. *Définition de stéganographie* 7
I.4.2. *Systeme de transmission steganographique* 8
I.4.3. *La steganographie classique* 9
I.4.4. *La Stéganographie moderne* 9
I.4.5. *Architectures steganographique* 9

I.5.Systeme de transmission steganographique de la parole **10**

I.6.Methodes steganographiques audio **11**

I.6.1. *Méthode LSB* 11
I.6.1.1. Codage de parité 12
I.6.1.2. Codage de phase 12
I.6.1.3. Spectre étalé 13
I.6.1.4. La technique de dissimulation d'écho 13

I.7.Classification des systemes steganographiques de la parole **13**

I.7.1. *Selon la clé* 14
I.7.1.1. Stéganographie à clé publique 14
I.7.1.2. Stéganographie à clé secret (privé) 14
I.7.2. *Selon les domaines de stéganographie* 14
I.7.2.1. Domaine de fréquence 14
I.7.2.2. Domaine temporel 15

I.7.2.3. Mode de compression 15

I.8.Steganalyse **15**

Conclusion

CHAPITRE II : STEGANOGRAPHIE BASEE SUR LE CODAGE.

Introduction

II.1.Stéganographie de la parole **17**

II.1.1. *L'utilisation d'un fichier audio comme une couverture* 18

II.2.Méthodes de steganographie audio **19**

II.2.1. *Cacher dans un domaine temporel* 20
II.2.1.1. La méthode LSB 20
II.2.1.2. Dissimulation d'écho (Echo Hiding) 20
II.2.1.3. Cacher dans les intervalles de silence 21
II.2.2. *Cacher dans le domaine de transformation* 21
II.2.2.1. Etalement du spectre (SS) 22
II.2.2.2. Transformée d'ondelettes discrètes 22
II.2.2.3. Insertion de tonalité 22
II.2.2.4. Codage de phase 23
II.2.2.5. Codage d'amplitude 23
II.2.2.6. Domaine cepstral 24
II.2.3. *Domaine de codage* 24
II.2.3.1. Incorporation pré-codage (pre-coding techniques) 24
II.2.3.2. Incorporation dans la phase de codage (In-coding techniques) 25
II.2.3.3. Techniques d'incorporation après codage (post-coding techniques) 26
II.2.4. *Avantages et inconvenients de differentes methodes steganigraphiques* 27
II.2.4.1. Temporel 27
II.2.4.2. Transformée (fréquentiel) 27

Conclusion

Chapitre III : IMPLEMENTATION D'UNE METHODE STEGANOGRAPHIQUE.

Introduction

III.1.Evaluation de la qualite perceptuelle de la parole **29**

III.1.1.*Mesure de distorsion spectrale (SD)* 29
III.1.2.*Evaluation perceptuelle de la qualité vocale (PESQ)* 30

III.2.Description des signaux de parole utilisés dans les tests **31**

III.3.Description de la méthode utilisée **32**

III.4.Déroulement des tests 34

III.5.Résultats de simulation 35

III.5.1.*Variation de type du filtre* 35
III.5.2.*Variation de l'ordre de filtrage* 39
III.5.3.*Variation de fréquence porteuse fp* 40

III.6.Interprétations des résultats 41

III.6.1.*Interprétation des résultats après la variation du type de filtre* 41
III.6.2.*Interprétation des résultats après la variation de l'ordre de filtrage* 41
III.6.3.*Interprétation des résultats après la variation de la fréquence porteuse* 42

Conclusion

Conclusion générale 43

Bibliographie 44

Annexe A 46

LISTE DES FIGURES

Figure I.1 : *Chaine de transmission numerique classique*.....3

Figure I.2: *Domaines inclus dans la cryptologie*.....5

Figure I.3: *Protocole de chiffrement*.....6

Figure I.4: *Schéma de principe d'un systeme de tatouage*. 7

Figure I.5 : *La relation entre la steganographie et la cryptographie*.....8

Figure I. 6: *Schéma simplifie de steganographie*. 10

Figure I.7: *Modele steganographique audio de base*. 10

Figure I.8 : *Exemple d'une methode lsb.* 11

Figure I.9 : *Code parite.* 12

Figure I.10 : *Codage de phase.*.....13

Figure I.11*: Chiffrement par cle secret*. 14

Figure II.1: *Flux de production de steganographie audio.* 18

Figure II.2: *Types de steganographie* 19

Figure II.3: *Dissimulation d'echo*.....21

Figure II.4 : *Incorporation pre-codage*. 25

Figure II.5 : *Incorporation dans la phase de codage*. 26

Figure II.6 : *Incorporation apres codage*. 26

Figure III.1: *Schéma synoptique permettant l'estimation de la distance perceptuelle pesq*. ..31

Figure III.2 *:(a) Signal de message de base, (b) Signal de message secret.* 32

Figure III.3: *(a) Diagramme a blocs du systeme de domaine frequentiel, (b) Principe de filtrage utilise au niveau de l'emetteur.* 33

Figure III.4 : *Schéma de la simulation* 34

Figure III.5 : (a) *Spectre de signal couverture*, (b) *Spectre de message secret*.....34

Figure III.6 : *Les spectres resultants lors de l'utilisation de filtre butter* 36

Figure III.7 : *Les spectres resultants lors de l'utilisation de filtre Besself*.....37

Figure III.8 : *Les spectres resultants lors de l'utilisation de filtre Ellipap* 38

Figure III.9:*Résultats obtenus (PSEQ) de variation de type filtres* 39

Figure III.10: *PSEQ obtenu en fonction de l'ordre de filtrage.* 40

Figure III.11: *PESQ obtenu en fonction de la fréquence porteuse.* 41

LISTE DES TABLEAUX

Tableau II.1*: Comparaison des methodes dans le domaine temporel.*.....27

Tableau II.2: *Comparaison des differentes methodes du domaine des transformations*.....28

Tableau III.1: *Limites des evaluations de la qualite de parole* 31

Tableau III.2 *: Résultats obtenue apres la variation de type du filtre.*.....35

Tableau III.3 : *Résultats obtenue apres la variation de l'ordre de filtrage*.....39

Tableau III.4 *: PESQ obtenu apres la variation de frequence porteuse*. 40

LISTE DES ACRONYMES

BPF: **B**and **P**ass **F**ilter

HAS: **H**uman **A**udition **S**ystem

LPC: **L**inear **P**rediction **C**oding

LPF: **L**ow **P**ass **F**ilter

LSB: **L**east **S**ignificant **B**it

MSB: **M**ost **S**ignificant **B**it

PESQ : **P**erceptual **E**valuation of **S**peech **Q**uality

Introduction générale

Depuis la naissance des grandes civilisations, Le problème d'échange des données secrètes est toujours existé. La cryptographie offre un moyen efficace pour protéger les données secrètes en les rendant inintelligibles aux personnes non autorisées qui peuvent détruire la communication entre les deux parties. Une communication contenant un message secret entre deux personnes doit sembler une autre chose aux yeux de la personne qui contrôle le canal.

Pour ce genre de scénario, la stéganographie représente la solution alternative à la cryptographie. La stéganographie, ou la science de communication secrète, est un procédé permettant de cacher un message secret au sein d'un médium hôte (original, cover), de telle sorte que le médium résultant (stego) semble inaffecté (dissimulation indétectable) par l'insertion du message secret. Autrement dit, l'objectif est de rendre difficile, ou impossible, la distinction entre un médium original et un médium modifié par l'insertion d'un message secret.

De manière analogue à la cryptographie, dont la discipline duale est la cryptanalyse visant à décrypter le message chiffré, la stéganographie a également comme discipline duale à la stéganalyse. L'objectif principal de la stéganalyse est de détecter la présence de message caché, et aussi dans la mesure du possible, d'avoir accès à son contenu.

Pour atteindre cet objectif nous avons divisé notre travail comme suivant :

Le premier chapitre, rassemble les concepts et les outils de base qui seront nécessaires à la compréhension de la suite du mémoire et les systèmes de transmission sécurisés.

Le deuxième chapitre présente les méthodes stéganographiques basées sur le codage.

Le troisième chapitre s'articule sur le principe d'implémentation de notre méthode stéganographique avec les critères d'évaluation et interprétations.

Nous terminons ce manuscrit par une conclusion générale de ce travail, ainsi que les perspectives envisagées.

CHAPITRE I

SYSTEME DE TRANSMISSION SECURISE

Introduction

L'information est partagée globalement sur Internet, sous forme numérique. Il y a des problèmes et des défis lors de la transmission des informations des expéditeurs aux récepteurs. Le problème majeur est la protection des données numériques contre toute forme d'intrusion, de pénétration et de vol. Le défi majeur consiste à élaborer une solution pour protéger l'information et assurer la sécurité pendant la phase de transmission. Trois éléments de la sécurité de l'information sont utilisés : la confidentialité, l'intégrité et la disponibilité.

Comme par exemple la confidentialité garantit que l'information est cachée contre tout accès non autorisé. Cela pourrait se faire par des techniques de dissimulation de l'information, à savoir la cryptographie et la stéganographie.

L'intégrité concerne la prévention, la détection et la dissuasion de la modification non autorisée de l'information. Une attaque d'intégrité est potentiellement plus dangereuse qu'une attaque de confidentialité.

La disponibilité concerne la prévention, la détection ou la dissuasion du refus d'accès aux informations essentielles.

I.1. Système de transmission numérique

Une chaîne de transmission classique est schématisée à la figure I.1. Le signal à transmettre, produit par une source d'information quelconque, est noté s et le paramètre temporel n.

La première opération consiste à comprimer s à l'aide d'un codeur de source. Le signal produit est noté x. Le signal comprimé x est plus simple à transmettre : la longueur moyenne de sa représentation en symboles transmissibles sur le canal est plus faible que celle de s.

Selon l'application, la compression peut être réalisée avec pertes, de sorte que x n'est pas une représentation exacte de s. Dans ce cas, les pertes sont mesurées par la distorsion D_f(s, x) entre s et la meilleure approximation qui peut être reconstituée à partir de x. La figure I.1 représente une chaine de transmission numérique classique:

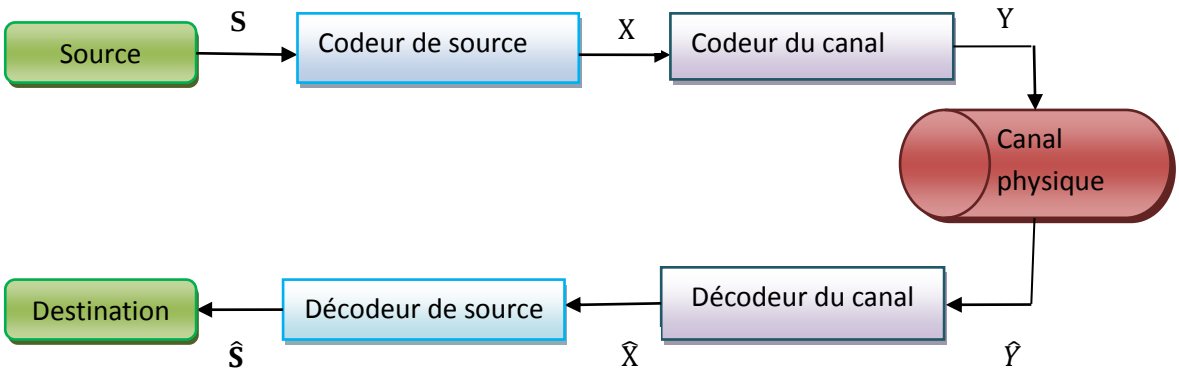


Figure I.1 : Chaîne de transmission numérique classique**.**

Le codage de source (compression) est réalisé via la quantification (scalaire ou vectorielle) dans le cas de compression de données avec pertes, les paramètres importants dans la quantification sont le débit et la distorsion. Les données seront transmises à travers un canal bruité, ce bruit cause des erreurs à la réception, une solution classique est de protéger les données source par un codeur de canal approprié, le codage de canal provoque une redondance (parité) qui assure la détection et la correction des erreurs causés par le canal de transmission, donc le codage de source et le codage de canal ont des buts contradictoires, le codage de source supprime de la redondance et le codage de canal ajoute une redondance structurée afin de l'exploiter à la réception.

La valeur R(D) signifie le taux de distorsion (Rate Distorsion) c'est le nombre minimal de bits nécessaires pour représenter la sortie s avec une distorsion D. Quant au bloc suivant, sa forme suggère une opération inverse. En effet, le codeur de canal introduit une redondance structurée afin de protéger x contre les dommages causés par le canal. C'est l'opération de codage contre les erreurs. Le signal produit est noté y.

Contrairement à la redondance présente dans s, celle est présentée dans y a une structure simple, en ce sens qu'elle est plus facilement exploitée en réception pour combattre les erreurs. Typiquement, ce codeur prend en entrée un vecteur ou une séquence de K valeurs tirées d'un alphabet fini, et produit en sortie N valeurs dans le même alphabet, avec $K < N$.

Au récepteur, les opérations inverses doivent être effectuées. D'une part, le décodeur de canal essaye de retrouver le signal x à partir du signal (éventuellement) corrompu $\hat{y}$. Le signal retrouvé est noté $\hat{x}$. D'autre part, le décodeur de source tente $\hat{x}$ quant à lui de reconstituer s au mieux à partir de $\hat{x}$. Le signal reconstitué est noté $\hat{s}$.

Si le canal n'a engendré aucune erreur, la distorsion globale $D_f(\hat{s},s)$ est celle du schéma de (codage/décodage) de source, le codec de source, et vaut donc $D_f(s,x)$. Par contre, si le canal a introduit des erreurs et si le décodeur de canal n'est pas parvenu à les corriger, l'entrée $\hat{x}$ du décodeur de source est corrompue ($\hat{x} \neq x$). Et dès lors, la distorsion globale est en général supérieure à celle du codec de source est donné par la formule (1):

$$D_f(\hat{s},s) \geq D_f(s,x) \qquad (I.1)$$

Il s'agit d'une transmission numérique "classique" car les conceptions des codecs de source et de canal sont séparées. Cette approche est souvent désignée codage en tandem (Tandem Coding), car l'on conçoit d'abord le codeur de source afin d'atteindre la meilleure performance entre le débit et la distorsion. Après on ajoute un codeur de canal suffisamment performant pour corriger presque toutes les erreurs. Ce codage en tandem suit le théorème de Shannon [1].

Comme on a dit précédemment que la transmission de l'information est susceptible d'être pirater à partir du canal d'une chaine de transmission, pour cela plusieurs techniques sont utilisées pour lutter contre cet effet, parmi eux on trouve la cryptographie, stéganographie, et tatouage.

I.2. Cryptographie

L'origine de la cryptologie mot réside dans la Grèce antique. La cryptologie est un mot composé de deux éléments : «cryptos », qui signifie caché et « logos » qui signifie mot. La cryptologie est aussi vieille que l'écriture elle-même, et a été utilisée depuis des milliers d'années pour assurer les communications militaires et diplomatiques. Par exemple, le célèbre empereur romain Jule César utilisait un algorithme de chiffrement pour protéger les messages à ses troupes. Dans le domaine de l'un de cryptologie peut voir deux visions, la cryptographie et la cryptanalyse. Le cryptographe cherche des méthodes pour assurer la sûreté et la sécurité des conversations, alors que le cryptanalyse tente de défaire le travail ancien en brisant ses systèmes. La cryptographie traditionnelle est l'étude des méthodes permettant de transmettre des données de manière confidentielle, par contre la cryptanalyse est l'étude des procédés cryptographiques, qui dépendent d'un paramètre appelé clé. Différents varient de cryptologie sont illustrés sur la figure I.2 [2].

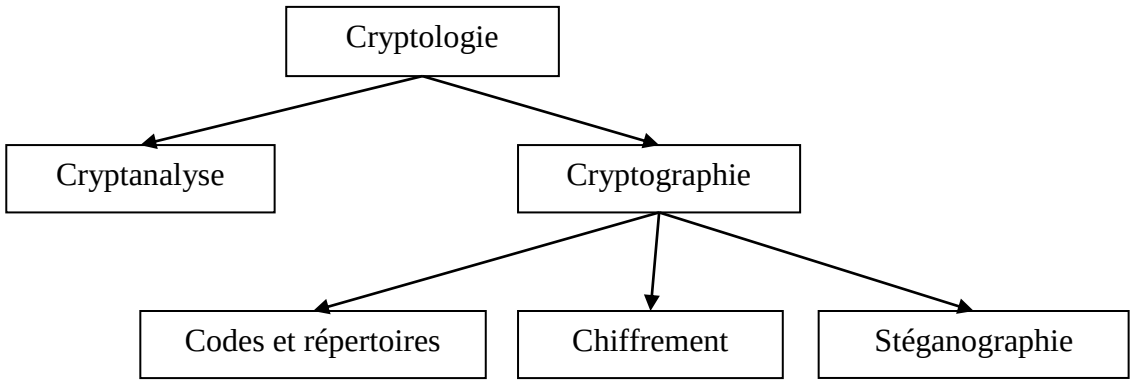


Figure I.2: Domaines inclus dans la cryptologie.

- **La cryptologie** : Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse.
- **La cryptographie** : La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.
- **Le chiffrement** : Le chiffrement consiste à transformer une donnée (texte, message, audio...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire. La fonction permettant de retrouver le texte clair à partir du texte chiffré porte le nom de déchiffrement.
- **Le texte chiffré** : Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.
- **La clef** : Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement. Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux opérations.
- **La cryptanalyse** : Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.
- **Le cryptosystème** : Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné. La figure suivante (Figure I.3) schématise les étapes d'un crypto-système [3].

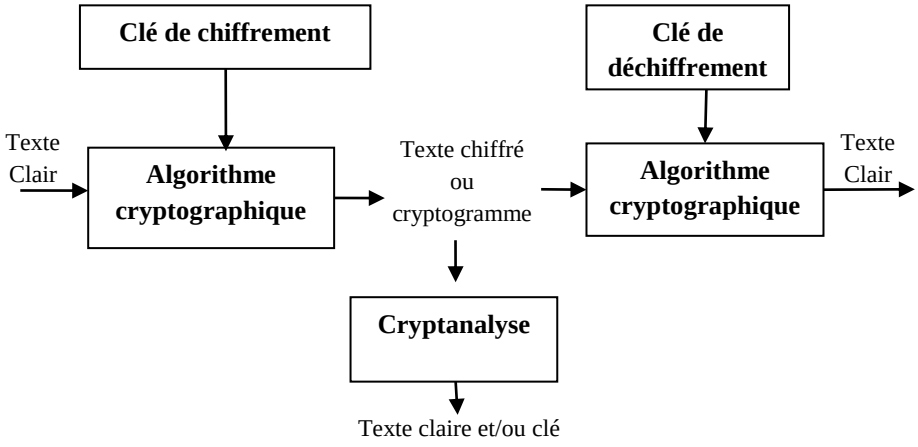


Figure I.3: Protocole de chiffrement.

I.3. Système de tatouage

Le schéma de principe, présenté par la figure I.4, reprend les trois étapes classiques d'une chaine de communication : l'émetteur, où le signal de tatouage est construit, le canal siège de perturbations classiquement appliquées au signal audio et le récepteur, qui extrait l'information cachée du signal audio reçu.

L'émetteur vise à insérer de manière imperceptible une information binaire, séquence de L bits $\{b_l\}$, au signal audio $x(n)$. Cette insertion est effectuée dans un domaine d'insertion approprié: une transformation T extrait du signal audio $x(n)$ un vecteur de Ns caractéristiques, noté x et également appelé signal hôte.

L'information binaire est interprétée par une étape de codage de source qui associe à chaque K-uplet binaire un représentant m parmi M. Ce représentant est associé de manière unique aux bits émis et est choisi dans un dictionnaire de source. Il est ensuite inséré dans le signal audio à l'aide d'une fonction d'insertion f. Cette fonction d'insertion construit dans un premier temps le vecteur de tatouage t, homogène aux caractéristiques du signal audio x, à l'aide d'un dictionnaire de canal qui réalise l'association bijective entre le vecteur de tatouage t et le représentant m. Elle insère dans un deuxième temps le vecteur de tatouage t (souvent en l'ajoutant) au vecteur audio x. Le débit de transmission est alors de $R = K$ bits par vecteur. L'ensemble de ces deux étapes - codage de source et insertion - définit la stratégie d'insertion. Lorsqu'elle prend en compte la connaissance a priori du signal audio, elle devient informée.

La stratégie d'insertion conduit finalement au signal audio tatoué $y(n)$. Ce signal est obtenu par transformation inverse du vecteur de caractéristiques y défini dans le domaine

d'insertion vers le domaine temporel. Le signal de tatouage $t(n)$ est alors défini comme la différence entre le signal audio tatoué y(n) et le signal audio original $x(n)$:

$$y(n) = x(n) + t(n) \quad \text{(I. 2)}$$

Le récepteur traite le signal audio reçu $\hat{y}$(n), i.e. $y(n)$ éventuellement détérioré par le canal de transmission, en le projetant dans l'espace d'insertion.

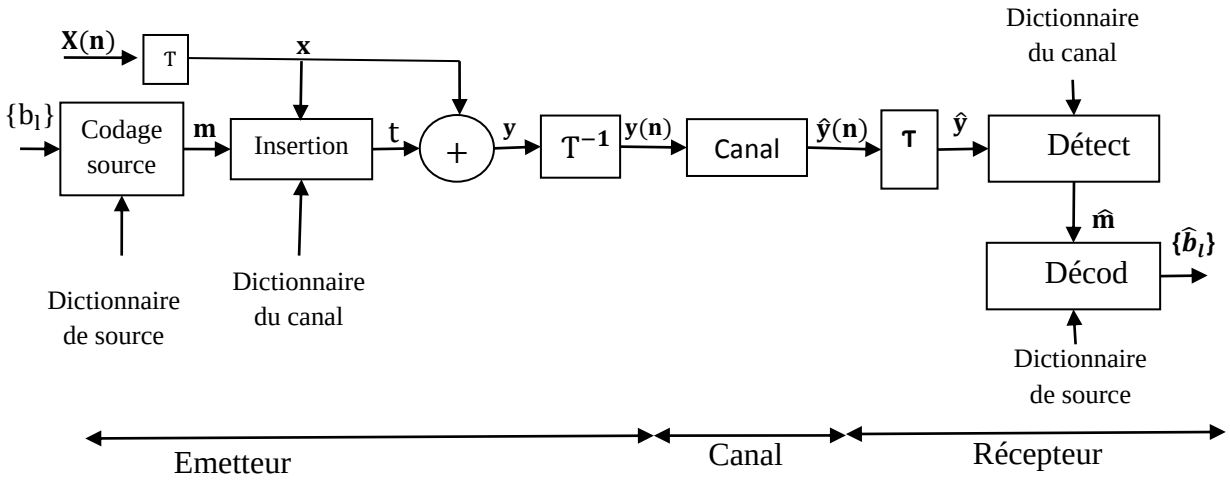


Figure I.4: Schéma de principe d'un système de tatouage.

Une étape de détection, dépendante de la fonction d'insertion choisie mais indépendante du signal audio original est mise en œuvre pour décider du représentant $\widehat{m}$. Cette étape peut faire intervenir des prétraitements qui projettent le signal reçu dans un espace de détection, différent de l'espace d'insertion. Une fois le représentant $\widehat{m}$ décide, le codage de canal est ensuite inversé, donnant lieu à l'information binaire reçue $\widehat{b}$ [4].

I.4. Système de transmission stéganographique

Le système de stéganographie a pour but de sécuriser la communication et d'en cacher l'existence à la fois, on l'expliquera dans les étapes suivantes.

I.4.1. Définition de stéganographie

Comme la cryptographie est l'art de cacher le sens d'un message. On définit la stéganographie, en parallèle comme l'art de cacher l'existence de message ou de communication. Son objectif est de pouvoir dissimuler des données qui doivent être tenues secrètes dans un support de communication paraissant publique. 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. Le but principal de la stéganographie est de communiquer avec sécurité [5].

I.4.2. Système de transmission stéganographique

La stéganographie est l'art de la dissimulation de communications. Contrairement à la cryptographie, la stéganographie n'a pas pour objectif de sécuriser une communication, mais d'en cacher l'existence même. Les deux disciplines ont donc chacune leur propre domaine de compétence. Dans certaines situations, le faite même de vouloir transmettre des données de manière chiffrée sera jugé comme suspect. De la même manière, de plus en plus de pays mettent en place de forte restriction concernant la longueur des clés cryptographiques, ainsi que la cryptographie en elle même. Le regain d'intérêt actuel pour la stéganographie provient de ces restrictions imposées à la cryptographie. D'une manière générale, la stéganographie arrive en renforcement au chiffrement de données. Pour permettre de garantir une confidentialité maximum, les données sont tout d'abord chiffrées avant d'être dissimulées à l'aide d'un processus stéganographique [6]. La figure I.5 résume la relation entre la cryptographie et la stéganographie :

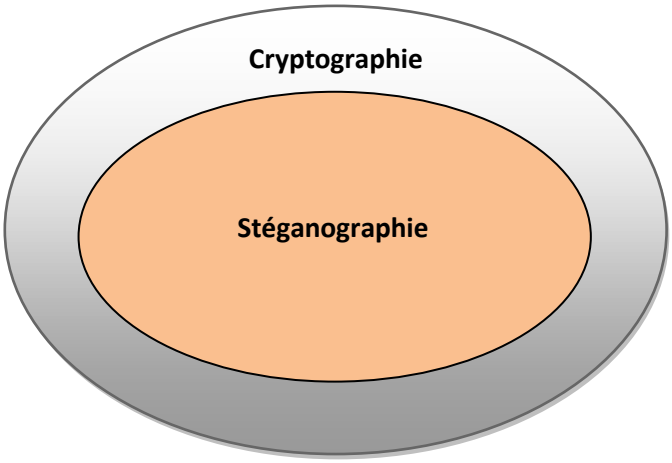


Figure I.5 : La relation entre la stéganographie et la cryptographie.

I.4.3. La Stéganographie classique

La stéganographie classique ne s'intéresse généralement qu'à la récupération de l'information, la couverture est utilisée uniquement pour la transporter. Cette couverture devrait être un fichier dont la transmission ne pose pas de suspicion. Il existe un cas particulier de stéganographie où la couverture et les informations cachées sont importantes.

C'est le cas lorsque l'incorporation d'informations servant de signature d'auteur protège une propriété numérique. C'est généralement appelé tatouage [7].

I.4.4. La Stéganographie moderne

La stéganographie dite moderne, c'est-à-dire adaptée aux données numériques, est relativement jeune. En pleine expansion, elle suit depuis le milieu des années 90 un essor corrélée celui d'internet. La première étape est bien évidemment de définir précisément l'objet que l'on va étudier. Le lecteur pourra se référer à d'excellents ouvrages traitant par la dissimulation d'information. Bien que la communauté des stéganographes se soit constituée dans les années 90, G. J. Simmons pose en 1983 le socle de la stéganographie moderne en définissant la notion de canal subliminal. Pour illustrer son propos, il reprend le problème de deux prisonniers. Deux prisonniers souhaitent établir un plan d'évasion. Pour ce faire, ils ont la possibilité de se transmettre des messages. Cependant, ces messages transitent à travers le gardien, qui a donc accès au contenu. Tout contenu jugé inapproprié sera détruit, et pourra engendrer une lourde sanction. Dans cette optique, le contenu doit donc paraître anodin aux yeux du gardien. Cette situation rend inutilisable la cryptographie, car un contenu indéchiffrable attirera l'attention du geôlier [6]. La stéganographie a donc comme objectif de pouvoir entretenir des communications sécurisées, sans pour autant attirer l'attention d'autrui.

I.4.5. Architectures stéganographique

Dans une architecture stéganographique, il y a principalement deux éléments. D'un côté un processus de dissimulation, de l'autre un processus de recouvrement [6]. Un processus de dissimulation simplifié peut être donné par le schéma suivant :

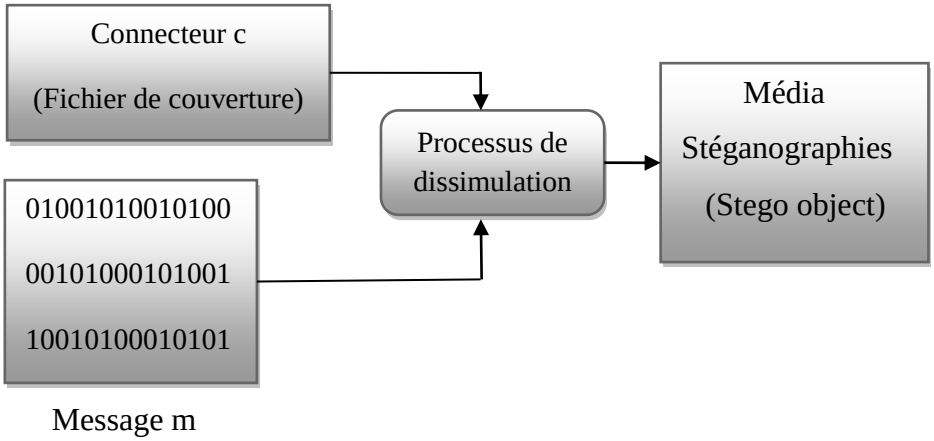


Figure I. 6: Schéma simplifié de Stéganographie.

I.5. Système de transmission stéganographique de la parole

Le modèle de base de la stéganographie audio se compose de couverture (fichier audio), message et mot de passe. Le porteur est également connu sous le nom de dossier de couverture, qui cache les informations secrètes.

Fondamentalement, le modèle de base de la stéganographie audio est montré par la figure I.7. Le message est les données que l'expéditeur souhaite le garder confidentiel. Le message peut être texte simple, image, audio …..Etc.

Le mot de passe est connu sous le nom de clé stego, qui garantit que seul le destinataire a la clé de décodage correspondante qui sera capable d'extraire le message secret d'un fichier de couverture. Le dossier de couverture avec les informations secrètes est connu comme un stego-fichier.

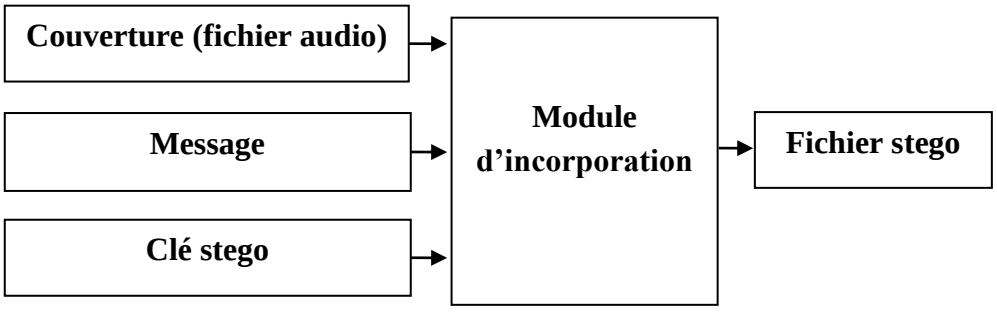


Figure I.7 : Modèle stéganographique audio de base.

Le processus de dissimulation de l'information consiste à suivre deux étapes :

- Identification des bits redondants dans un fichier de couverture. Les bits redondants sont les bits qu'ils peuvent modifiés sans corrompre la qualité ou détruire l'intégrité du fichier de couverture.
- Pour incorporer les informations secrètes dans le fichier de couverture, les bits redondants dans le fichier de couverture sont remplacés par les bits de l'information secrète.

I.6. Méthodes stéganographiques audio

Il y a eu de nombreuses techniques pour cacher des informations ou des messages en audio de telle manière que les modifications apportées au fichier audio sont perceptiblement indiscernables [8] :

I.6.1. Méthode LSB

Une méthodologie très populaire est l'algorithme LSB (Least Significant Bit), qui remplace le bit le moins significatif dans certains octets du fichier de couverture pour masquer une séquence d'octets de données cachées. C'est généralement une technique efficace dans les cas où la substitution LSB ne provoquer une dégradation significative de la qualité, comme dans les bitmaps 24 bits.

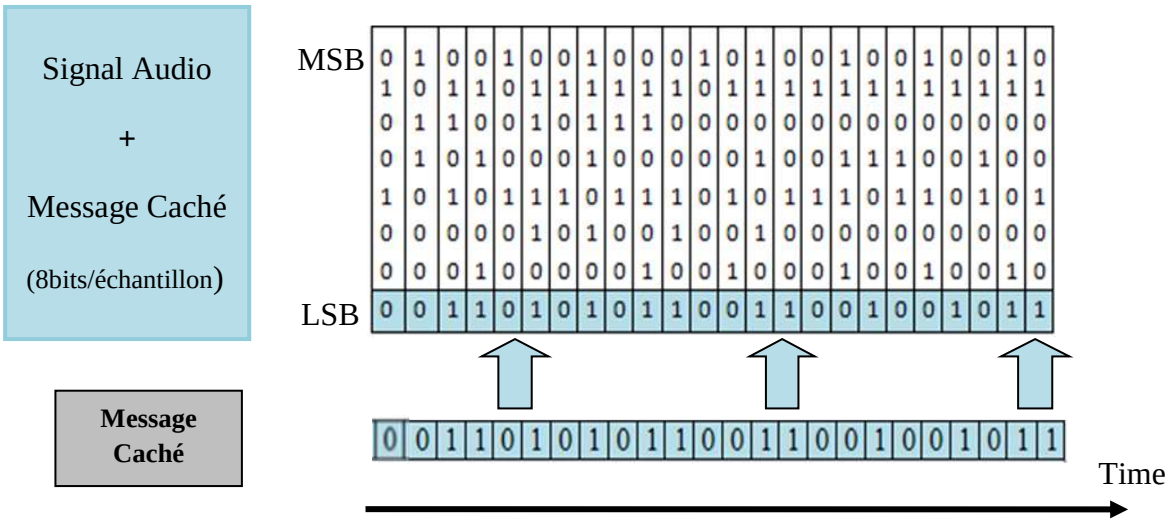


Figure I.8 : Exemple d'une méthode LSB.

I.6.1.1. Codage de parité

Le codage de parité est l'une des techniques audio stéganographiques robustes. Au lieu de briser un signal en échantillons individuels, cette méthode brise un signal en échantillons séparés et incorpore chaque bit du message secret dans un bit de parité. Si le bit de parité d'une région sélectionnée ne correspond pas au secret bit à coder, le processus inverse le LSB d'un des échantillons dans la région.

Un exemple de codage de parité est illustré par la figure I.9 :

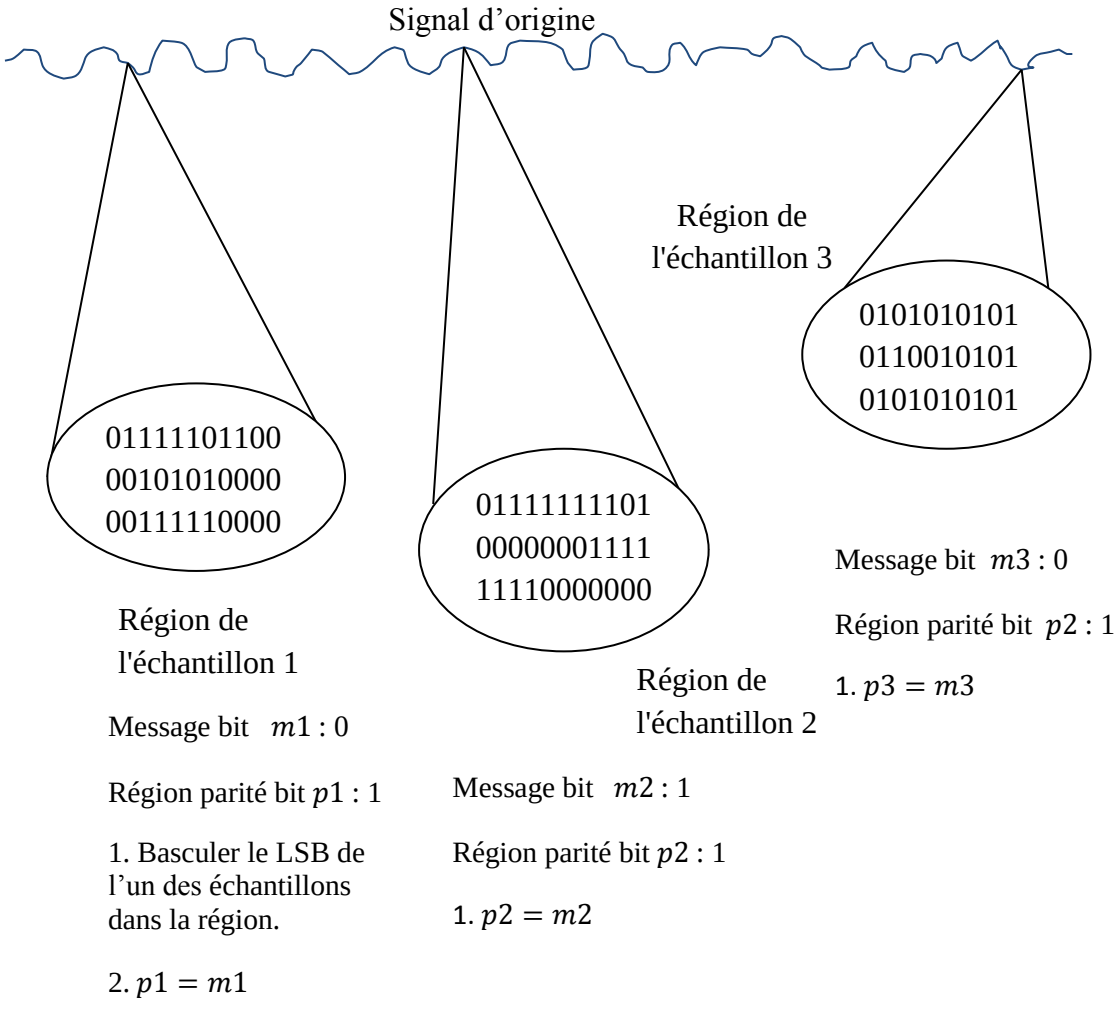


Figure I.9 : Code parité.

I.6.1.2. Codage de phase

La technique de codage de phase fonctionne en remplaçant la phase d'un segment audio initial par une phase de référence qui représente l'information secrète. La phase des segments restants est ajustée pour préserver la phase relative entre les segments. En termes de rapport signal / bruit, le codage de phase est l'une des méthodes de codage les plus efficaces.

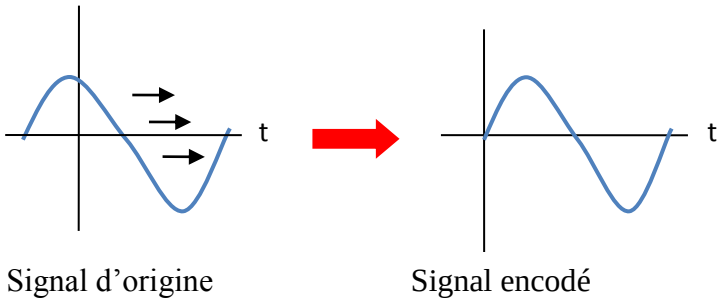


Figure I.10 : Codage de phase.

I.6.1.3. Spectre étalé

Dans la stéganographie audio, la méthode du spectre étalé de base (Spread Spectum) tente de diffuser des informations secrètes à travers le spectre de fréquence du signal audio. Ceci est similaire à un système qui utilise une implémentation de LSB qui diffuse les bits de message au hasard sur l'ensemble du fichier son. Cependant, contrairement au codage LSB, la méthode (Spread Spectrum) diffuse les informations secrètes sur le spectre de fréquences du fichier son à l'aide d'un code indépendant du signal. En conséquence, le signal final occupe une largeur de bande supérieure à ce qui est effectivement nécessaire pour la transmission.

I.6.1.4. La technique de dissimulation d'écho

La technique de dissimulation d'écho intègre des informations secrètes dans un fichier sonore en introduisant un écho dans le signal discret. L'écho caché a des avantages de fournir un taux de transmission de données élevé et une robustesse supérieure par rapport à d'autres méthodes. Un seul bit d'information secrète pourrait être codé si un seul écho était produit à partir du signal original. Par conséquent, avant le début du processus de codage, le signal original est divisé en blocs. Une fois le processus de codage terminé, les blocs sont concaténés ensemble pour créer le signal final.

I.7. Classification des systèmes stéganographiques de la parole

On trouve dans la parole une certaine classification des systèmes stéganographiques comme suivant :

I.7.1. Selon la clé

Selon la clé de cryptage on peut distinguer deux types de stéganographie :

I.7.1.1. Stéganographie à clé publique

Chaque entité possède 2 clés distinctes (une privée **Sk**, une publique **Pk**) avec impossibilité de déduire la clé privée à partir de la clé publique. De ce fait, il est possible de distribuer librement cette dernière.

I.7.1.2. Stéganographie à clé secret (privé)

Est une ancienne, simple et plus rapide que la clé publique, elle se base sur les formules arithmétiques et décalage circulaire entre les caractères. [5]

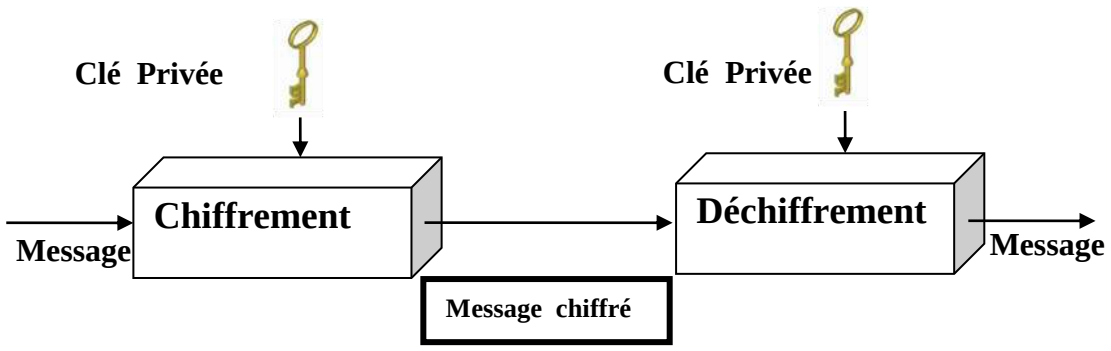


Figure I.11: Chiffrement par clé secret.

I.7.2. Selon les domaines de stéganographie

Il existe trois types de domaines stéganographiques :

I.7.2.1. Domaine de fréquence

Dans le domaine fréquentiel, il existe certaines techniques utilisées dans la stéganographie audio, comme l'insertion de la tonalité, le codage de phase et les techniques de spectre étalé. Dans les techniques d'insertion de tonalité, les tonalités de faible puissance sont masquées en présence d'une plus forte. C'est une méthode robuste mais à faible capacité d'intégration. Dans la méthode de codage de phase, les bits de message secret sont intégrés comme déphasage dans le spectre de phase de l'audio de couverture originale. Cette méthode a une bonne robustesse, mais a également une faible capacité et ne survit pas au filtrage passe-bas. Les

techniques de propagation du spectre calculent le seuil de masquage de fréquence en utilisant un modèle psycho-acoustique, où le signal de données est propagé par un code de séquence M et le signal de propagation est intégré dans l'audio sous le seuil de masquage de fréquence. Cette méthode augmente la transparence, mais elle occupe une large bande passante [9].

I.7.2.2. Domaine temporel

Sous le domaine temporel, les techniques incluent la technique de bit (LSB), le codage de parité et les techniques de dissimulation d'écho. La méthode LSB modifie le bit le plus bas du support de couverture pour intégrer le message secret. C'est l'une des méthodes les plus simples, mais il peut être facilement attaqué. Dans la technique de codage de parité, la parité de chaque groupe d'échantillons est calculée, si elle ne correspond pas au bit du message, le bit le plus bas de l'un des échantillons individuels du groupe est modifié pour rendre le bit de parité égal à Bit de message. Cette technique est également facile à extraire. Dans la méthode de dissimulation Echo, un petit écho est introduit dans des parties de l'audio de la couverture avec une manipulation de trois paramètres: taux de décroissance, décalage et amplitude pour rendre l'écho inaudible, mais la capacité d'inclusion ici est faible [9].

I.7.2.3. Mode de compression

C'est une opération où l'information peut être réduite sans difficulté pour diminuer l'espace et le temps de transmission. Ces informations peuvent être une image, Texte, audio, fax, vidéo, etc. Il existe deux types de techniques de compression qui sont les suivantes :

a. ***Compression sans perte*** : elle réduit la quantité de données source transmises de telle sorte que lorsque des données compressées sont décompressées, aucune altération se produite.

b. ***Compression avec perte*** : elle ne redéveloppe pas une copie exacte des informations après la phase de décompression. Ici, certaines informations sont perdues après la décompression. MP3 est utilisé pour compresser le flux continu de son en petits fichiers [10].

I.8. Stéganalyse

Contrairement à la cryptanalyse, dont le but est de déchiffrer les données ayant été chiffrées. La plupart des techniques stéganalyse recherche des artefacts crées par le processus de cacher un message. Une technique simple de stéganographie couramment utilisée est la

méthode LSB, où les bits les moins significatifs (LSB) de valeurs de données dans un fichier multimédia sont modifiés afin de cacher un message. Plusieurs catégories de méthodes peuvent être utilisées dans cette optique. La plus simple consiste à la détection de signature d'un logiciel donné. Certains programmes laissent derrière eux, de manière intentionnelle ou par erreur de conception, des artefacts permettant de caractériser leur passage. Cette façon de faire possède l'avantage de directement fournir le nom de l'application utilisée pour la dissimulation de donnée. Par contre, chaque application doit faire l'objet d'une analyse spécifique.

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

La catégorie permettant le scope de détection le plus large est donnée par les outils de stéganalyses universelles. Se basant sur des réseaux neuronaux, leur capacité dépend uniquement de la qualité de la base d'entraînement, ainsi que du bon choix des caractéristiques sensées qualifiée le média [6].

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.

Dans certains cas, cette technique aussi peut être détectée, alors on ajoute des types de codage qu'on va les voir dans le chapitre 2.

CHAPITRE II

STEGANGRAPHIE BASEE SUR LE CODAGE

Introduction

Aujourd'hui, la stéganographie est une méthode principale utilisée pour protéger les données, pour envoyer de manière fiable des informations secrètes, et pour cacher l'existence de la communication. En plus, les techniques d'incorporation stéganographiques des données secrètes se basent sur les techniques de codage.

Les techniques modernes de la stéganographie exploitent les caractéristiques des médias numériques en les utilisant comme supports (couvertures) pour contenir des informations cachées. Les couvertures peuvent être de différents types, y compris : l'image, l'audio, la vidéo, le texte et le datagramme IP.

II.1. Stéganographie de la parole

Un exemple de stéganographie audio est illustré sur la Figure II.1, où le support de couverture utilisé est un fichier audio numérique. L'expéditeur incorpore des données de n'importe quel type dans un fichier de couverture numérique à l'aide d'une clé pour produire un fichier stego, de telle sorte qu'un observateur ne peut pas détecter l'existence du message caché. Par la suite, le récepteur traite le fichier stego reçu pour extraire le message caché. Une application évidente d'un tel système stéganographique est une communication cachée utilisant un signal audio de couverture inoffensif, comme des conversations par téléphone ou par vidéoconférence. Pour minimiser la différence entre la couverture et le stego-medium, les récentes techniques de stéganographie utilisent des limites naturelles dans les perceptions auditives et visuelles humaines. Cependant, la stéganographie audio exploite la propriété de l'effet masquant du Système Auditif Humain (HAS) (voire Annexe A).

D'une autre coté diverses caractéristiques influencent sur la qualité des méthodes stéganographiques audio. Les propriétés les plus importantes incluent la robustesse au bruit, la compression et la manipulation du signal, ainsi que la sécurité et la capacité de dissimulation des données cachées. Généralement, la robustesse et la capacité ne coexistent guère dans le même système stéganographique en raison du déséquilibre des compromis entre ces deux critères où les niveaux de robustesse accrus entraînent une diminution de la capacité de dissimulation des données [11].

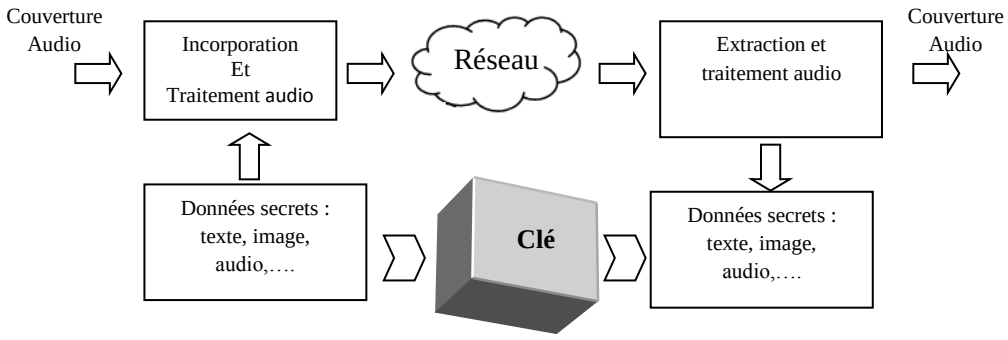


Figure II.1: Flux de production de stéganographie audio.

II.1.1. L'utilisation d'un fichier audio comme une couverture

L'importance particulière de cacher des données dans des fichiers audio provient de la présence dominante des signaux audio en tant que vecteurs d'information circulant dans les réseaux informatiques comparativement aux autres types de données (images, texte, vidéo).

Puis, la plupart des efforts de la stéganalyse sont davantage orientés vers les images numériques, ce qui laisse la stéganalyse audio relativement inexplorée.

Aussi, La dissimulation de données dans les fichiers audio est particulièrement difficile en raison de la sensibilité de HAS. Ces propriétés ont conduit les chercheurs à explorer l'utilisation des signaux audio en tant que transporteurs pour camoufler les données [11].

Divers paramètres influent sur la qualité des systèmes stéganographiques audio, ces paramètres sont:

- *Taux de dissimulation*: mesuré en bit/sec et se réfère à la quantité de données cachées (en bits) dans un signal de couverture audio.
- *Imperceptibilité*: ce concept repose sur les propriétés de HAS, qui est mesurée par l'évaluation perceptive de la qualité de la parole (PESQ) [12]. L'information cachée est imperceptible parce que l'auditeur n'est pas capable de distinguer entre le signal de couverture et le signal stego-audio.
- *Amplification*: permet d'augmenter l'amplitude du signal audio qui pourrait modifier les données cachées si une attaque malveillante est destinée.
- *Filtrage*: permet de supprimer/ajouter malicieusement les données cachées en coupant ou bien en ajoutant une partie sélectionnée du spectre.
- *Quantification*: ce paramètre modifie la quantification d'origine du signal audio. Par exemple, un signal audio de 16 bits est quantifié à 8 bits puis revenir à 16 bits dans une tentative de détruire les données cachées.

- *Sous-échantillonnage*: De manière similaire à l'opération ci-dessus, ce paramètre déclenche la fréquence d'échantillonnage du signal audio à un autre, c'est-à-dire un signal audio large bande échantillonné de 16 kHz à 8 kHz et retourne à 16 kHz.
- *Ajout de bruit*: l'ajout de bruit tel que le bruit blanc gaussien AWGN (Additif White Gaussian Noise) au signal audio dans une tentative de détruire les données cachées.
- *Codage et décodage*: cette opération réduit la quantité de données en supprimant des informations redondantes ou inutiles. Ainsi, un message caché peut être complètement détruit. Ceci est également vrai si le fichier audio est converti en un autre format. Par exemple, modifie un fichier « WAV » en un fichier « MP3 » avant qu'il n'atteigne le récepteur.
- *Transcodage*: c'est le processus de décodage du signal audio avec un décodeur différent de celui utilisé dans l'opération de codage.

II.2. Méthodes de stéganographie audio

Trois approches importantes d'intégration de données existants, à savoir cacher : dans *le domaine temporel*, dans le *domaine de fréquence* / *ondelettes* et dans le domaine de *codage* [11]. La Figure II.2 récapitule les domaines utilisés par la stéganographie audio.

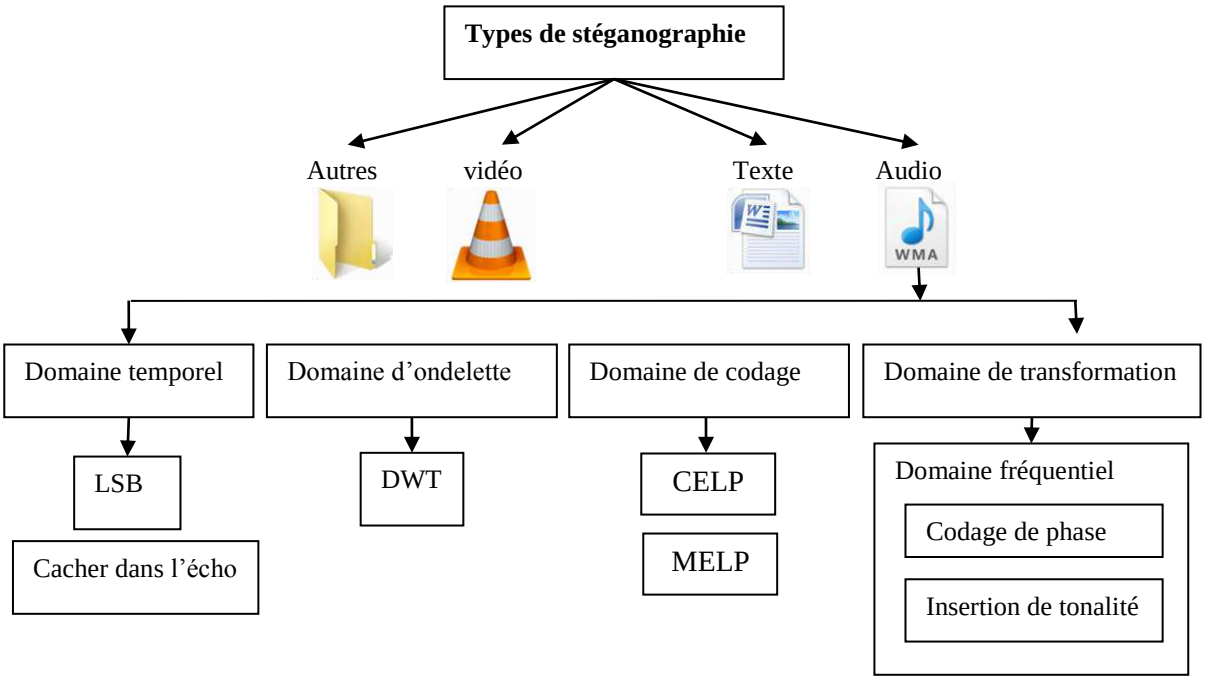


Figure II.2: Types de stéganographie.

II.2.1. Cacher dans un domaine temporel

La majorité des méthodes de domaine temporel utilisent des techniques de codage à faible bit, que nous décrivons ensuite [11].

II.2.1.1. La méthode LSB

LSB (Least Significant Bit), est l'une des premières méthodes utilisées pour la dissimulation d'informations. Traditionnellement, elle est basé sur l'intégration de chaque bit du message à caché dans le bit le moins significatif de la couverture audio de manière déterministe, Ainsi, pour un audio échantillonné de 16 kHz, 16 kbps de données sont cachées. La méthode LSB permet une capacité d'incorporation élevée pour les données et est relativement facile à mettre en œuvre ou à combiner avec d'autres techniques de dissimulation. Cependant, cette technique se caractérise par une faible robustesse à l'ajout de bruit qui réduit ses performances de sécurité, car elle devient vulnérable même à des attaques simples. La filtration, l'amplification, l'ajout de bruit et la compression à perte du stego-audio vont très probablement détruire les données. En outre, comme les données sont intégrées de manière très déterministe, un attaquant peut facilement découvrir le message en supprimant simplement l'ensemble du plan LSB (cf. chapitre I) [11].

II.2.1.2. Dissimulation d'écho (Echo Hiding)

Cette méthode incorpore les données dans les signaux audio en introduisant un court écho sur le signal hôte, l'écho ici est une résonance. Par conséquent, le problème de la sensibilité HAS au bruit additif est évité. Une fois l'écho ajouté, le signal stego conserve les mêmes caractéristiques statistiques et perceptuelles. Les données sont cachées en manipulant trois paramètres du signal d'écho: l'amplitude initiale, le décalage (retard) et le taux de désintégration afin que l'écho ne soit pas audible (Figure II.3).

Pour un délai jusqu'à 1 ms entre le signal d'origine et l'écho, l'effet est indistinguable. En plus de cela, les taux d'amplitude et le taux de désintégration pourraient être définis sur des valeurs sous le seuil audible de l'oreille humaine. L'inconvénient de cette méthode est la limitation de la taille du signal d'écho induit qui restreint ses domaines d'application connexes. Par conséquent, la quantité limitée d'œuvres qui enquêtent sur l'application de cette méthode.

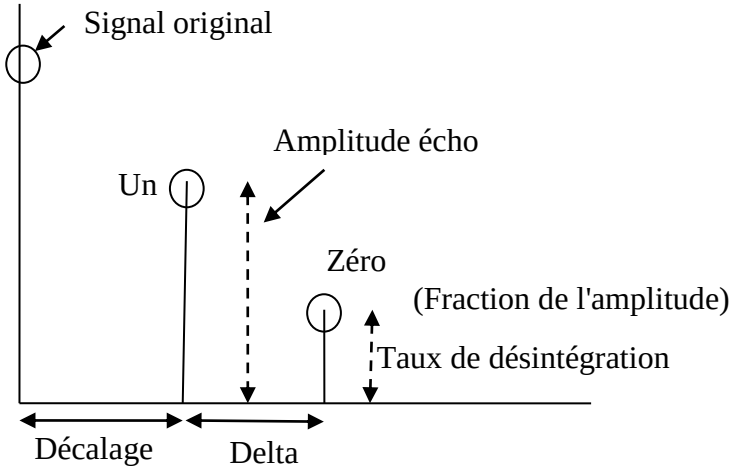


Figure II.3: Dissimulation d'écho.

En raison du faible taux d'intégration et de la sécurité, et au mieux de notre connaissance, aucun système de stéganographie audio basé sur la dissimulation d'écho n'a été présenté dans des travaux de recherche récents.

II.2.1.3. Cacher dans les intervalles de silence

Cette technique insère un intervalle de silence dans le signal audio original pour intégrer les données secrètes. Les valeurs qui représentent la longueur des intervalles de silence sont diminuées d'une valeur telle que 0 <valeur < 2^n où n est le nombre de bits requis pour représenter un élément des données à cacher [13]. Le fichier audio du transporteur est ensuite envoyé au récepteur ayant les nouvelles longueurs pour ses intervalles de silence.

La récupération des données se fait via :

$$info_recuperée = mod\ (longueur_altéré\ , 2^n) \quad (1)$$

II.2.2. Cacher dans le domaine de transformation

Le système auditif humain a certaines particularités qui doivent être exploitées pour cacher les données efficacement. Le phénomène "effet de masquage" masque les fréquences les plus faibles près des résonnants les plus résistants. Plusieurs méthodes dans le domaine de la transformation ont été proposées dans la littérature comme décrit ci-après. Pour atteindre l'intelligibilité, ces méthodes exploitent l'effet de masquage de fréquence de la HAS

directement en modifiant explicitement uniquement les régions masquées ou indirectement en modifiant légèrement les échantillons de signaux audio [11].

II.2.2.1. Etalement du spectre (SS)

Cette technique diffuse les données secrètes sur le spectre de fréquence du fichier audio en utilisant un code spécifique indépendant du signal réel. Fondamentalement, les données secrètes sont multipliées par un code connu uniquement par les parties communicantes, puis intégrées dans le fichier audio du transporteur. L'avantage de la méthode SS est sa vitesse de couverture des données. Cependant, son inconvénient est qu'il introduit du bruit et des distorsions sur le fichier audio [13].

II.2.2.2. Transformée d'ondelettes discrètes

La transformée en ondelettes discrètes (DWT) est une technique multi-échelle et multi-résolution pour décomposer le signal sur différents composants temps-fréquence. Une méthode stéganographique est proposée dans la référence mentionnée où une DWT masque les données (des coefficients d'ondelettes) dans LSB.

L'imperceptibilité des données cachées est faible dans DWT. Chaque fois que les coefficients d'ondelettes entières sont disponibles, un seuil auditif est utile pour améliorer l'intelligibilité. DWT fournit un taux élevé de dissimulation de données. Néanmoins, la procédure d'extraction de données au récepteur n'est pas toujours précise.

Dans cette technique, les données secrètes sont intégrées dans les bits les moins significatifs des coefficients d'ondelettes des signaux audio. Souvent, les données secrètes sont choisies pour être cachées dans les coefficients d'ondelettes entiers et non dans des sections silencieuses du signal audio de manière à favoriser l'imperceptibilité du fichier audio. L'inconvénient de la Transformée d'onde discrète est que des données secrètes peuvent être perdues pendant le processus de récupération, car cette technique n'est pas exacte [14].

II.2.2.3. Insertion de tonalité

Le système auditif humain (HAS) ne détecte pas de signaux audio lorsqu'on a des puissances de tonalité plus faibles se situent près de tonalités très élevées. L'insertion de tonalité profite de cette fonctionnalité pour la dissimulation de données. Étant donné qu'un bit est prévu de se cacher dans un segment audio, deux fréquences de f_0 et f_1 sont sélectionnées et une paire de sons est crée dans cette zone. Chaque fréquence a une fréquence masquée, par

exemple p_{f0} pour f_0 et p_{f1} pour f_1. Considérant qu'il y a n trames et la puissance de chaque segment est désignée par pi où $i = 1,\ldots,n$.

La valeur de chaque fréquence masquée est définie sur une valeur prédéfinie qui est le rapport de la puissance générale de chaque segment audio p_i. Une extraction de données correcte à partir de données stéganographie est obtenue lorsque les sons sont insérés à des fréquences connues et à faible niveau de puissance.

La procédure de détection des données cachées des tonalités insérées est effectuée en calculant la puissance de chaque segment,p_i y compris la puissance de p_{f0} pour f_0 et p_{f1} pour f_1. Si le rapport $\frac{p_i}{p_{f0}} > \frac{p_i}{p_{f1}}$, le bit caché est supposé "0". Sinon, il est considéré comme "1" Ainsi, les données cachées sont extraites. Tel qu'il est perçu, la capacité de dissimulation des données de la méthode d'insertion de la tonalité est faible. Certaines attaques peuvent être tolérées par une méthode d'insertion de la tonalité, par exemple, le filtrage passe-bas et la troncature des bits. Néanmoins, les attaquants peuvent simplement détecter les sons et extraire les données cachées. Semblable à LSB, ce problème peut être résolu en modifiant quatre ou plusieurs paires de fréquences dans un ordre clé [11].

A partir de la Figure II.2, il est clair que la méthode d'insertion de la tonalité appartient au domaine fréquentielle. La méthode d'insertion de tonalité exploite une propriété de masquage en fréquence pendant la transmission des données secrètes [15].

II.2.2.4. Codage de phase

Le codage de phase exploite l'insensibilité de HAS à la phase relative de différents composants spectraux. Ce codage est basé sur le remplacement des composants de phase sélectionnés du spectre du signal audio original par des données cachées. Pour assurer l'inintelligibilité, la modification des composants de phase devrait être limitée. Il convient de mentionner que, parmi les techniques de dissimulation des données, le codage de phase tolère une meilleure distorsion du signal [11].

II.2.2.5. Codage d'amplitude

Cette technique cache les données secrètes dans l'amplitude du spectre de la parole tout en ne pas distordre le signal audio couverture. Il est basé sur la recherche des régions spectrales de parole ayants de grandeur est inférieur à une certaine valeur [13].

II.2.2.6. Domaine cepstral

Connu aussi comme domaine logarithmique spectrale, les données de cette méthode sont incorporées dans les coefficients de cepstrum, (i.e. Les coefficients LPC, MFCC,…etc.), qui tolèrent les attaques de traitement de signal les plus courantes (Bruit additif, filtrage, compression….etc.). En outre, l'altération cepstral à des fréquences qui se trouvent dans les régions masquées perceptiblement de la majorité des trames audio de couverture, garantit l'in-audibilité des trames audio stego résultants. Le signal de couverture est d'abord transformé en domaine cepstral, puis les données sont incorporées dans le coefficient de cepstrum sélectionné en appliquant des manipulations moyennes statistiques [11].

II.2.3. Domaine de codage

Pour catégoriser et évaluer les méthodes de la stéganographie audio en tenant compte la robustesse, la sécurité et la capacité de dissimulation qui tournent autour de ces méthodes existantes de stéganographie, l'environnement de transmission et l'application en cours utilisée sont aussi considérés. La communication cachée, par exemple, nécessite un haut niveau de robustesse en raison du passage des données par l'un des codeurs existants qui peuvent affecter fortement l'intégrité des données transmises. Le processus encodeur réduit la quantité de données du signal audio en éliminant les données redondantes ou inutiles. En passant par l'un des codeurs, le signal audio transmis est codé en fonction du taux de compression puis décompressé à l'extrémité du décodeur, mais le signal de données du côté du récepteur n'est pas exactement le même que celui de l'expéditeur, ce qui affecte la correction et la récupération des données cachées. Trois groupes d'incorporation distincts sont utilisés lors de la conception du système stéganographique [11].

II.2.3.1. Incorporation pré-codage (pre-coding techniques)

Les méthodes pré-codeur s'appliquent aux domaines temporels et fréquentielles où l'intégration des données se produit avant le processus de codage. La plupart des méthodes appartenant à la classe d'incorporation pré-encodeur ne garantit pas l'intégrité des données cachées sur le réseau. L'addition de bruit dans ses différentes formes (par exemple : WGN) et une compression de débit élevée induite par l'un des processus de codage tels que CELP (G.729), AMR (G.722), ACELP (G.723), LPC affectera probablement l'intégrité des données cachées. Dans d'autres méthodes, les données cachées résistent uniquement à quelques manipulations audio telles que le redimensionnement, le sous-échantillonnage, le filtrage, etc.

Et elles ne tolèrent que l'ajout de bruit ou la compression de données à un taux très bas. Un taux de dissimulation (incorporation) élevé peut être obtenu avec des méthodes conçues pour des environnements sans bruit [11].

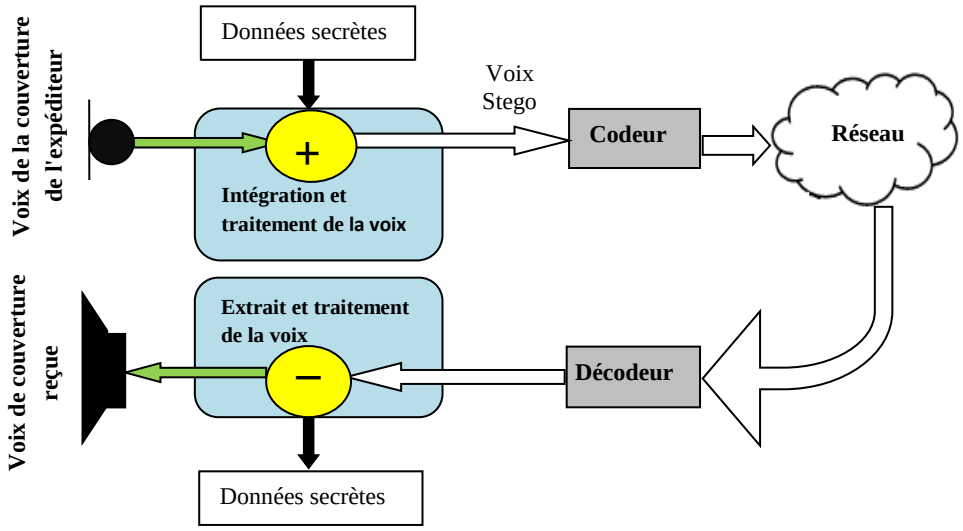


Figure II.4 : Incorporation pré-codage.

II.2.3.2. Incorporation dans la phase de codage (In-coding techniques)

La robustesse des données intégrées est le principal avantage de cette approche qui est basée sur l'opération d'intégration de données dans le code-book (dictionnaire) des codecs.

L'information transmise est cachée dans le paramètre code-book après une opération de quantification. Ainsi, chaque paramètre de signal audio a une double signification: valeur de données cachées et paramètre de code-book audio. L'un des inconvénients de cette méthode se pose lorsque les paramètres codés traversent un réseau tel que le GSM qui possède par exemple un décodeur / codeur vocal dans le réseau d'accès radio (BST, BSC, TRAU) et / ou dans le réseau central (MSC). Dans cette configuration, les valeurs de données cachées seront modifiées. Ces modifications peuvent également se produire lorsqu'un algorithme de rehaussement vocale est activé dans le réseau d'accès radio et / ou dans le réseau central [11].

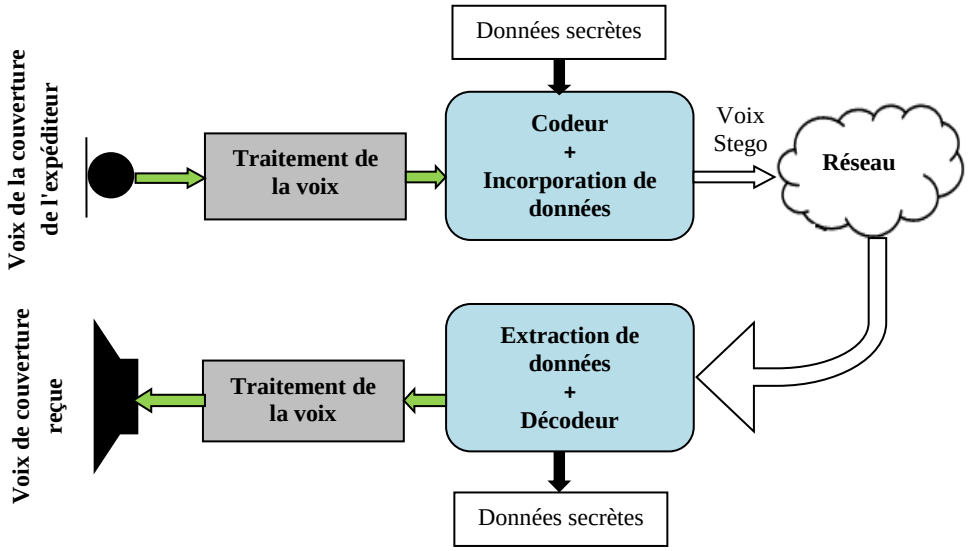


Figure II.5 : Incorporation dans la phase de codage.

II.2.3.3. Techniques d'incorporation après codage (post-coding techniques)

Dans cette approche, les données sont intégrées dans le bit-Stream résultant du processus de codage et extraites avant le décodeur. Étant donné que le bit-Stream est plus sensible aux modifications que le signal audio original, la capacité de dissimulation doit être maintenue petite pour éviter la perception intrinsèque des données. En outre, le transcodage peut modifier les valeurs de données intégrées et donc modifier l'intégrité du système stéganographique. Cependant, l'un des côtés positifs de ces méthodes est l'exactitude de la récupération de données [11]. Un exemple est présenté dans la référence précédente, ils ont appliqué le concept de cette méthode sur le codeur AMR à un débit de $12{,}2 kbit/s$ pour cacher 2 $kbit/s$ de données dans les bits-Stream.

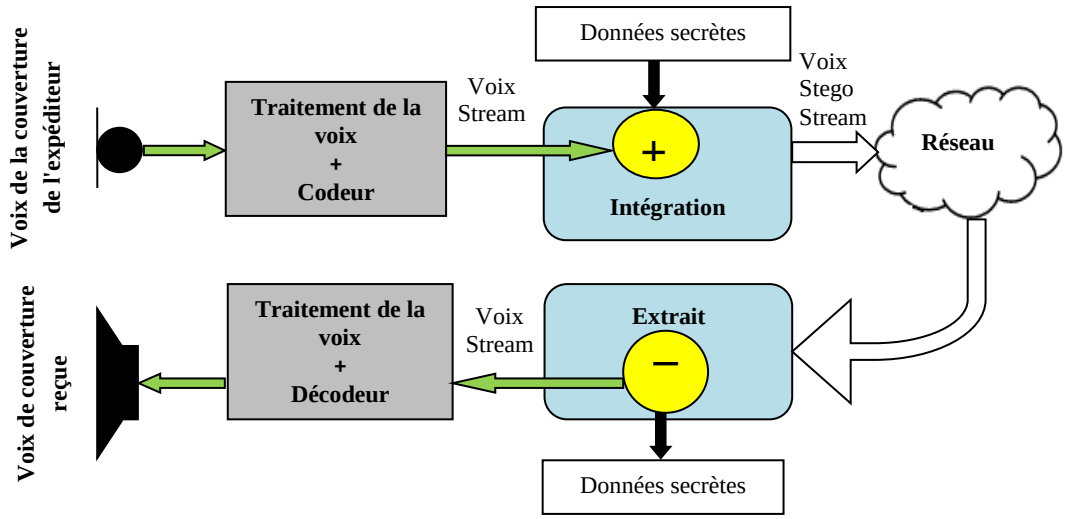


Figure II.6 : Incorporation après codage.

II.2.4. Avantages et inconvénients des différentes méthodes stéganographiques

Généralement chaque méthode stéganographique contient des avantages et tout de même des inconvénients :

II.2.4.1. Temporel

La robustesse et la sécurité ne soient pas les principales caractéristiques des méthodes stéganographiques du domaine temporel, la technique LSB classique et ses variantes fournissent un moyen ou bien une simple méthode pour masquer les données.

La tolérance à l'ajout de bruit à des niveaux faibles et certains critères de robustesse ont été réalisés avec les méthodes des variantes LSB, mais à une capacité de dissimulation très faible.

Pour le maintenant, seules quelques techniques de dissimulation de domaine temporel ont été développées. Une évaluation des systèmes stéganographiques basés sur ces techniques est présentée dans le tableau II.1 [11].

Tableau II.1: Comparaison des méthodes dans le domaine temporel.

propriétés de la méthode	LSB conventionnel (classique)	Variantes LSB	Intervalles de silence
Imperceptibilité	*	*	*
WGN additif	-	*	*
Compression	-	-	*

II.2.4.2. Transformée (fréquentiel)

Il a été prouvé que la dissimulation dans le domaine fréquentiel plutôt que le domaine temporel donnera de meilleurs résultats en termes de rapport signal sur bruit (SNR).

Les techniques de stéganographie audio dans le domaine transformé bénéficient de l'effet de masquage de la fréquence.

La plupart des algorithmes de dissimulation de données basés sur le domaine transformé utilisent un modèle perceptif pour déterminer la quantité de données à cachées autorisée pour éviter la distorsion du signal stego. Un grand nombre de domaine de transformation ont été présentés au cours de la dernière décennie et dans une certaine mesure, ces techniques ont réussi à réaliser la sécurité et la robustesse des données cachées contre des manipulations de

signaux audio simples telles que l'amplification, le filtrage ou le sous-échantillonnage, comme indiqué dans le Tableau II.2 [11].

Tableau II.2: Comparaison des différentes méthodes du domaine des transformations.

Propriétés de la méthode	Insertion de tonalité	Codage de phase	Codage d'amplitude	Domaine Cepstral	Etal. de spectre	DWT
Imperceptibilité	*	*	*	*	*	*
Amplification	-	*	-	*	-	-
Ajout de bruit	-	-	-	*	*	-
Filtrage passe-bas	*	*	-	*	-	-
sous-quantification	-	*	-	-	-	-
sous-échantillonnage	*	-	-	-	-	-
Compression	-	*	-	*	-	-

Conclusion

Dans ce chapitre, diverses techniques de stéganographie audio sont discutées comme des méthodes potentielles pour cacher des signaux audio numériques de données. Pour fournir une meilleure protection au contenu des données, de nouvelles techniques de stéganographie ont été développées dans des travaux de recherche récents, les exigences spécifiques de chaque méthode d'intégration de données varient d'une application à une autre chacune de ces méthodes a des points de force et de faiblesse.

.

CHAPITRE III

IMPLEMENTATION D'UNE METHODE STEGANOGRAPHIQUE DANS LE DOMAINE FREQUENTIEL APPLIQUE AUX SIGNAUX DE PAROLE

Introduction

Nous présentons dans cette partie, notre étude de réalisation et les critères d'évaluation appliqués sur des signaux choisis. Notre but est de masquer parfaitement le message secret dans le signal de base.

Pour évaluer la qualité perceptuelle du signal reconstruit, nous avons choisi les méthodes objectives, connues sous le nom de PESQ (perceptual evaluation of speech quality).

Rappelons que celle-ci a été décrite dans la recommandation P.862 de l'ITU-T (union internationale des télécommunications), elle est basées sur la modélisation de l'audition et tient compte de certaines caractéristiques de la perception humaine. Les différents tests effectués et les résultats obtenus seront illustrés et commentés.

III.1. Evaluation de la qualité perceptuelle de la parole

La qualité vocale peut être mesurée en utilisant des méthodes subjectives ou objectives, les mesures subjectives utilisent souvent le MOS (Mean Opinion Square). Cependant cette procédure est lente et difficile à mettre en œuvre. Ainsi, les notes des participants pour une condition de test donnée sont moyennées pour obtenir la note moyenne d'opinion, qui permet d'exprimer l'effet subjectif sur l'évaluation de la qualité vocale.

De plus, la perception de la qualité vocale dépend du contexte et de l'environnement dans lesquels est placée la personne qui juge. De même, l'environnement (bruit, informations visuelles ou sonores supplémentaires) influence le jugement de la qualité. Ainsi, les conditions à tester sont définies en fonction de l'objectif visé. Le participant est amené à évoluer dans un ou plusieurs contextes (écoute, locution et conversation) [16].

III.1.1. Mesure de distorsion spectrale (SD)

La distorsion spectrale est une mesure objective, souvent utilisée pour évaluer la performance des quantificateurs dans les codeurs fonctionnant à très bas débit. Cette mesure de distorsion donne une bonne corrélation avec la perception humaine [17]. La SD se calcule sur un intervalle de bande limité, son expression, est donnée, pour une i trame par :

$$SD_i = \sqrt{\frac{10}{n_1 - n_2} \sum_{n=n_0}^{n_1} \left[log_{10} \left(\frac{S(f_n)}{\hat{S}(f_n)} \right) \right]^2} \qquad (III.1)$$

$S(f_n)$ et $\hat{S}(f_n)$ sont respectivement les spectres de puissance originaux S (f_n) et quantifiés $\hat{S}(f_n)$ du filtre de synthèse LPC. Une FFT sur 256 points est appliquée pour calculer les deux spectres de puissance $S(f_n)$ et $\hat{S}(f_n)$ de la $i^{ème}$ trame du signal de parole.

La SD moyenne est évaluée pour toutes les trames des fichiers traités, son expression donnée par :

$$\overline{SD} = \frac{1}{M}\sum_{i=1}^{M} SD_i \quad \text{(M nombre de trames)} \qquad \text{(III. 2)}$$

En général, une $\overline{SD}$ d'environs 1dB indique que la distorsion perçue pendant la quantification est négligeable. Paliwal et Atal [16] ont établi que la SD moyenne n'est pas suffisante pour mesurer la transparence d'un quantificateur. Ils ont introduit la notion des trames spectrales externes ou (outliers frames). Par conséquence nous pouvons obtenir une qualité de codage transparente si les conditions suivantes sont maintenues.

- La SD moyenne est d'environ 1dB.
- Le pourcentage des trames ayant une SD entre 2 et 4 est moins de 2%.
- Aucune trame ne doit avoir une SD qui dépasse 4 dB.

III.1.2. Evaluation perceptuelle de la qualité vocale (PESQ)

La méthode PESQ est utilisée pour la prédiction de la qualité subjective pour la téléphonie et pour les codeurs vocaux. Elle est destinée à évaluer l'influence de certains facteurs tels que la perte de paquets, le délai variable et les distorsions dues aux erreurs de canal qui sont mal évaluées par les méthodes classiques (RSB, RSB segmental, distorsion spectrale, etc.).

La méthode PESQ est conçue pour comparer une version de référence (originale) à celle obtenue par synthèse à partir de cette référence, c'est le cas par exemple des dégradations que subit cette référence après transmission ou après une compression. L'idée de base du PESQ est de transformer les formes d'onde en une représentation perceptuelle, similaire à la représentation des paramètres utilisés par les vocodeurs à bande étroite. En d'autres termes, la différence entre les paramètres de ces représentations est évaluée à l'aide d'un modèle cognitif en vue d'estimer la distance de perception entre les deux signaux : le signal original et le signal synthétique (décodé) sont présentés par la figure III.1 [16].

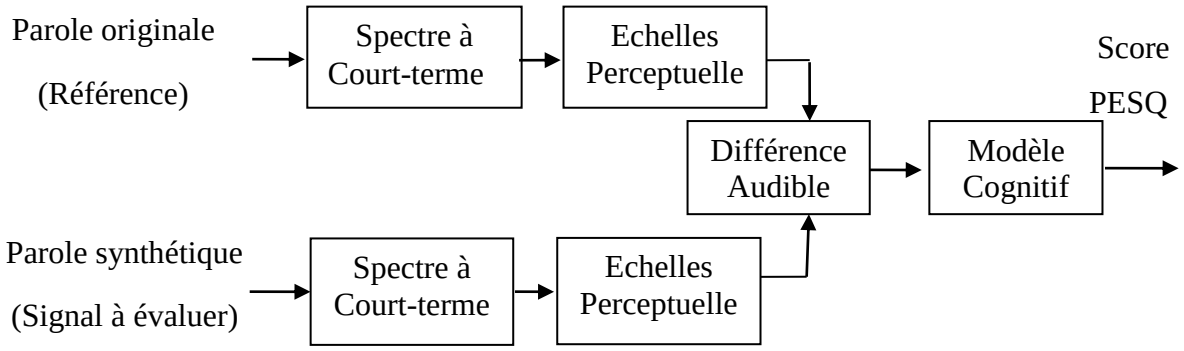


Figure III.1: Schéma synoptique permettant l'estimation de la distance perceptuelle PESQ.

Le tableau III.1 donne un aperçu des limites des évaluations de la qualité selon la recommandation P.862 [12] :

Tableau III.1: Limites des évaluations de la qualité de parole selon la recommandation P.862.

Valeur du PESQ	Evaluation de la qualité de parole
3 ≤PESQ≤ 4	Très acceptable
2.5 ≤PESQ ≤3	Acceptable
2 <PESQ≤ 2.5	Basse
PESQ< 2	Inacceptable (l'intelligibilité est perdue)

III.2. Description des signaux de parole utilisés dans les tests

Pour tester et valider nos méthodes, nous avons utilisé un matériau linguistique formé de corpus multilingues. Le premier est composé de phrases arabes PAPE (Phrases Arabes Phonétiquement Equilibrées) conçues au niveau de laboratoire LCPTS de l'université USTHB. Ce corpus contient un total de 60 phrases, soit 10 phrases prononcées par 3 locuteurs féminins et 3 locuteurs masculins.

La fréquence d'échantillonnage du signal parole des fichiers était de 10 kHz, nous avons dû effectuer un sous-échantillonnage de toute la base de données à 8 kHz, pour se mettre dans les conditions de la téléphonie. Pour la langue française et anglaise, nous avons utilisé les phrases célèbres, phonétiquement équilibrées : « la bise et le soleil » et « the sun and the wind» [18].

III.3. Description de la méthode utilisée

Notre méthode stéganographique est basée sur la dissimulation fréquentielle. Au niveau de l'émetteur, elle consiste d'abord à lire deux fichiers de parole (i.e. format wav) choisis de la base de données proposée. Le premier est le signal de base (signal de couverture) qui contient le message caché, l'autre est le message secret qui sera caché dans le signal de base.

La figure III.2 représente les tracés des deux signaux en fonction de temps.

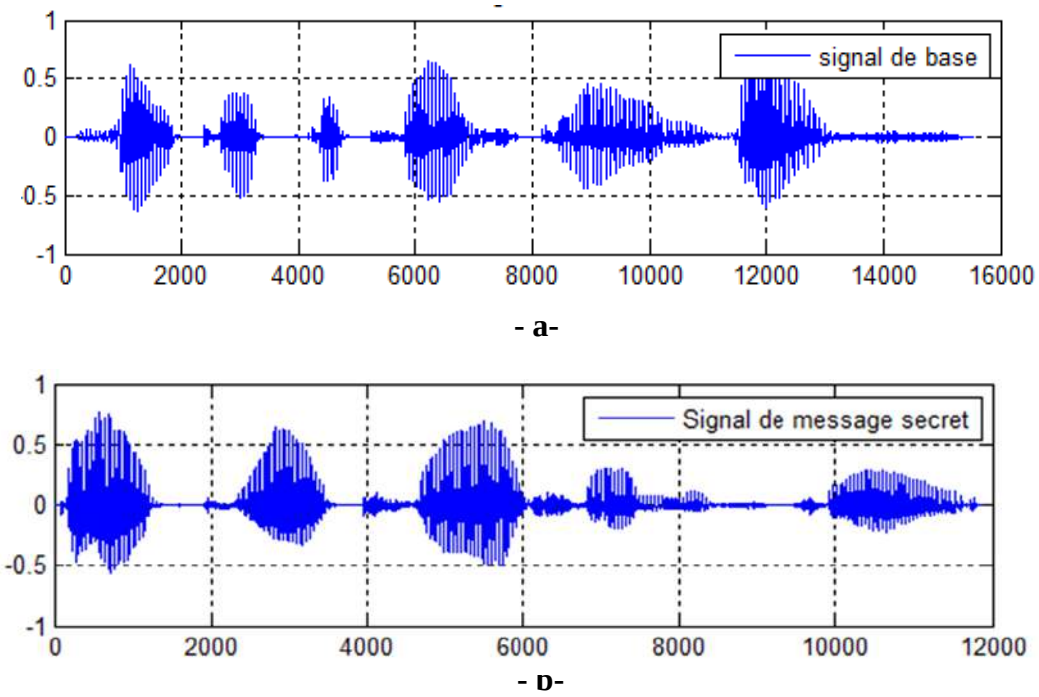
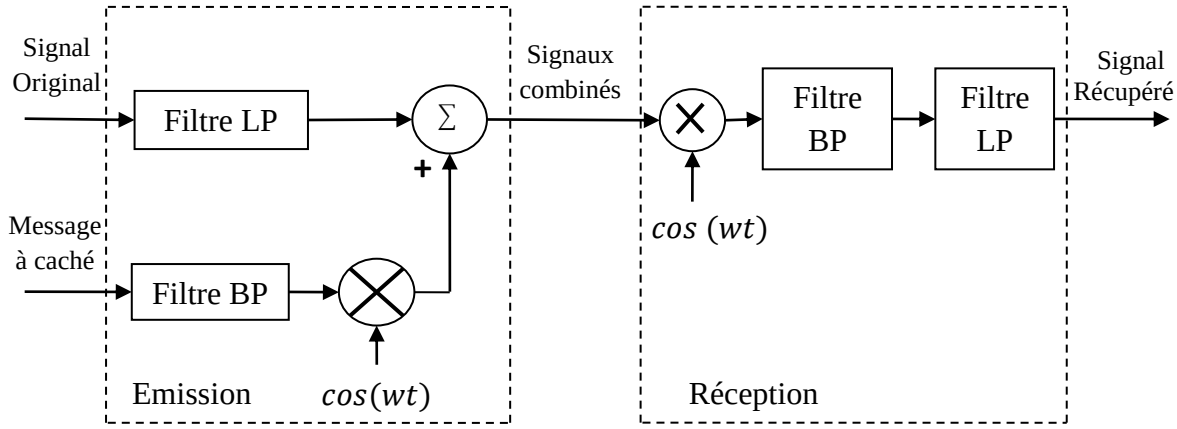
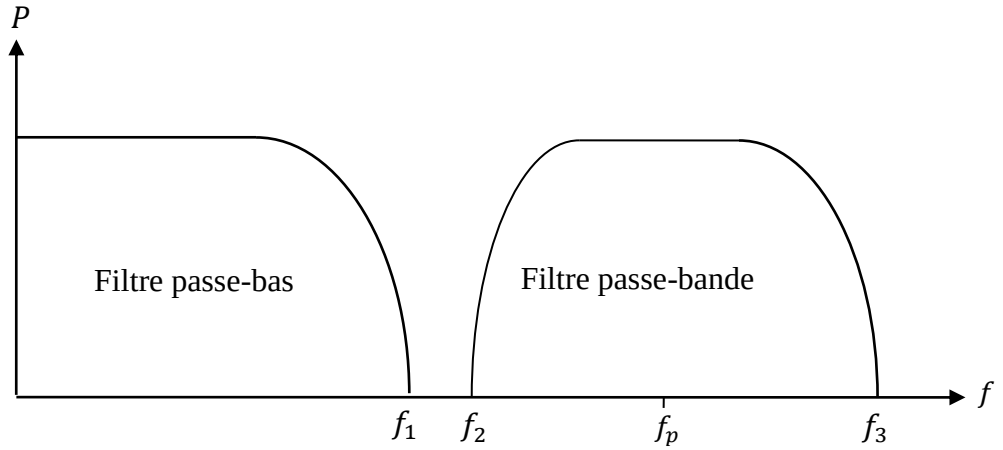


Figure III.2 :(a) Signal de message de base, (b) Signal de message secret.

Ensuite, le signal de couverture sera filtré par un filtre passe-bas qui laisse passer les basses fréquences inférieur à la fréquence de coupure $f_1$choisie. Le message secret subira un filtrage passe bande qui ne laisse passer qu'une bande ou un intervalle de fréquences compris entre une fréquence de coupure basse f_2 et une fréquence de coupure haute f_3 du filtre pour limiter la bande de message caché. Le signal filtré passe-bande subit une modulation en cosinus pour éviter les chevauchements entre les deux signaux. Par la suite on va additionner ces derniers pour les envoyer via un canal de transmission. Les Figure III.3 (a) et (b) illustrent le principe de cette méthode, ce schéma est très célèbre dans les littératures mais on a changé quelques paramètres pour améliorer les résultats :



-a-



-b-

Figure III.3: (a) Diagramme à blocs du système de domaine fréquentiel,

(b) principe de filtrage utilisé au niveau de l'émetteur.

A la réception, pour extraire le signal caché, nous démodulons le message secret en utilisant une démodulation en cosinus avec la même fréquence porteuse utilisée à l'émission.

Ensuite, on utilise un filtre passe-bande filtrant le signal combiné au-dessus et au-dessous du signal caché par les fréquences de coupures f_2 et $f_3$respectivement. Enfin, La phase de démodulation introduit un bruit additif, alors on doit filtrer le signal démodulé et filtré le résultat par un filtre passe-bas avec une fréquence de coupuref_1. La Figure III.3 (a) illustre le principe de cette méthode au niveau de récepteur.

Remarque :

On a utilisé une modulation en sinus mais aucun résultat trouvé.

III.4. Déroulement des tests

Pour évaluer la performance de la technique de stéganographie proposée et décrit précédemment, nous avons effectué plusieurs simulations à l'aide de la base de données proposée (PAPE). Les mesures PESQ sont reliées aux variations de trois paramètres : *le type de filtre*, *l'ordre de filtrage*, et *la fréquence porteuse*. La figure III.4 résume les étapes des tests.

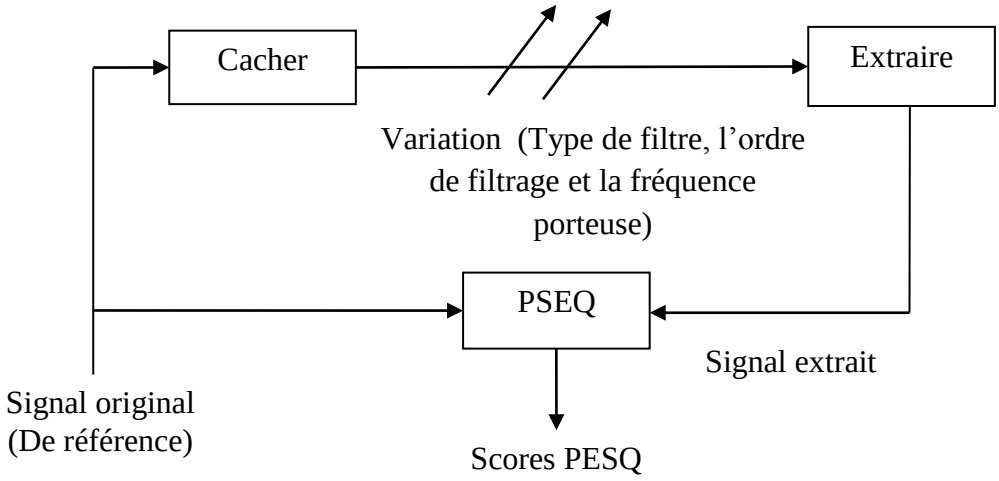
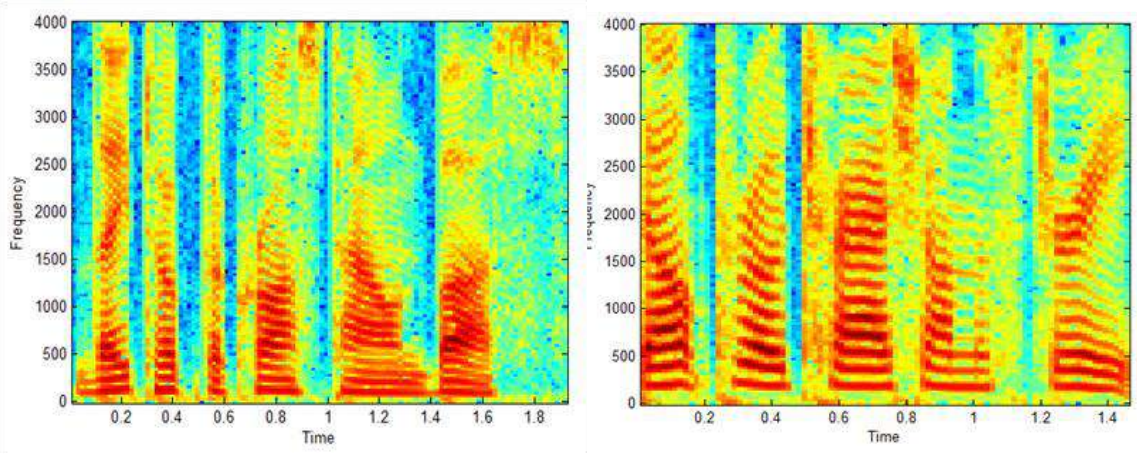


Figure III.4 : Schéma de la simulation**.**

Une autre astuce peut nous aider à évaluer nos résultats est la comparaison entre les spectrogrammes de signaux cachés émis et reçus. Ces spectrogrammes sont représentés dans le domaine fréquentiel où une transformation temporelle fréquentielle est utilisée. Cette transformation se base sur la SFFT. Pour un premier pas, voici les spectrogrammes des sons utilisés et qui ne changent pas pendant toutes les manipulations (figure III.5) :



-a- **-b-**

Figure III.5 : (a) Spectre de signal couverture, (b) Spectre de message secret.

Le logiciel utilisé pour l'implémentation de notre algorithme de stéganographie audio est le Matlab (Matrix Laboratory).

III.5. Résultats de simulation

Pour chaque paramètre on prend quatre essais au maximum, les tests reliés à chaque paramètre seront représentés sous forme des tableaux.

III.5.1. Variation de type du filtre

Pour cette manipulation on va changer le type de filtre en gardant la fréquence porteuse et l'ordre de filtre fixe. Le tableau III.2 résume les différentes valeurs de PESQ obtenues pour chaque type de filtre. La figure III.6, figure III.7, figure III.8 représentent respectivement les spectrogrammes de : signal de base filtré passe-bas, signal de message secret filtré passe-bande, signal combiné (stego), et le signal reconstitué (message secret), pour chaque type de filtre.

Tableau III.2 : Résultats obtenue après la variation de type du filtre.

Type de filtre / Incorporation		Butter	Besself	Ellipap
Message	Couverture	PESQ		
Masculin	Masculin	2,636	2,662	0,952
Féminin	Féminin	2,734	0 ,908	0,807
Féminin	Masculin	3,023	1,799	1,263
Masculin	Féminin	2,486	1 ,025	0,799
La moyenne		2,720	1,598	0,955

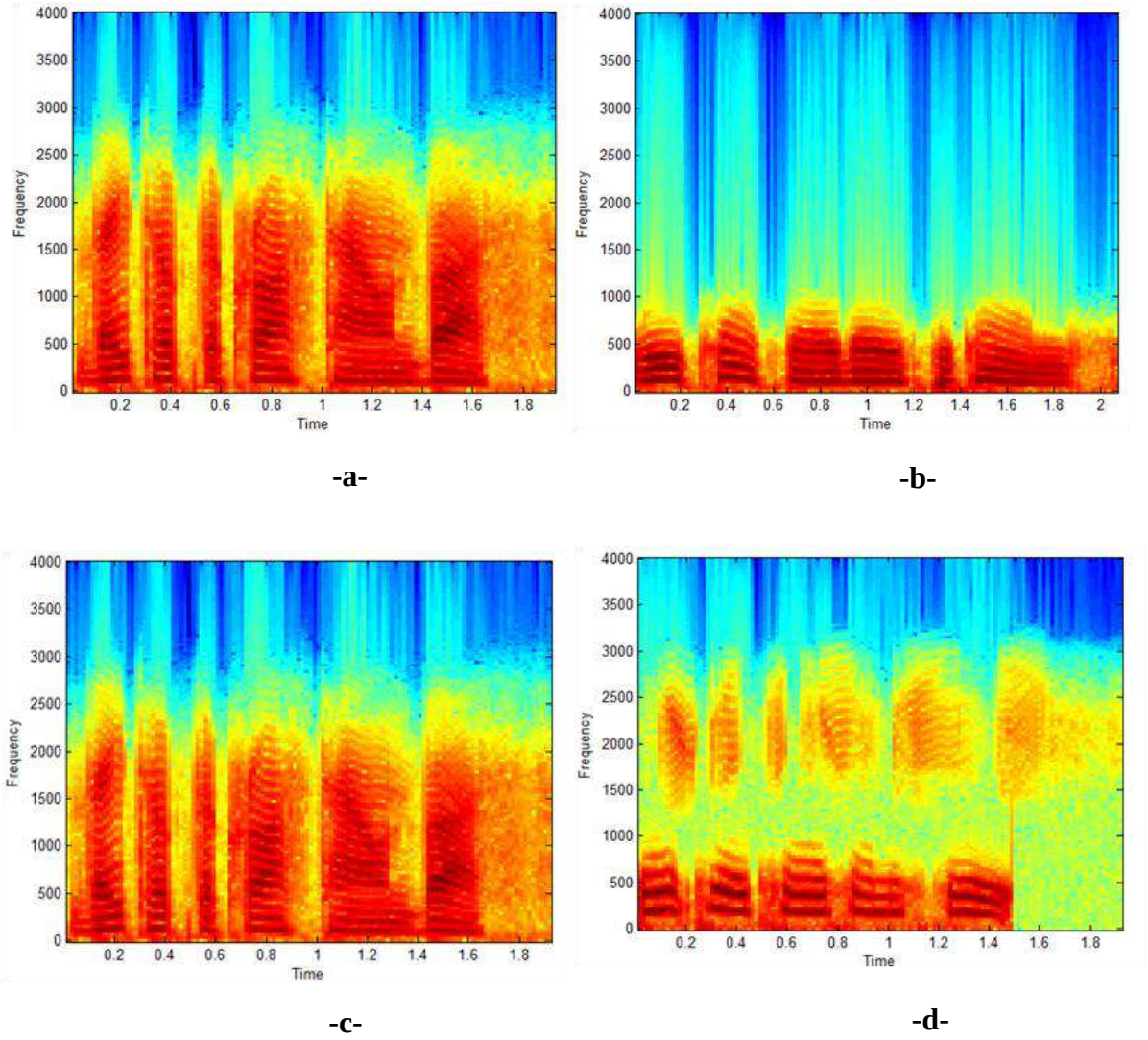


Figure III.6 : Les spectres résultants lors de l'utilisation de filtre butter

- *(a) signal de base filtré passe-bas.*
- *(b) signal de message secret filtré passe-bande.*
- *(c) signal combiné (stego).*
- *(d) signal reconstitué (message secret).*

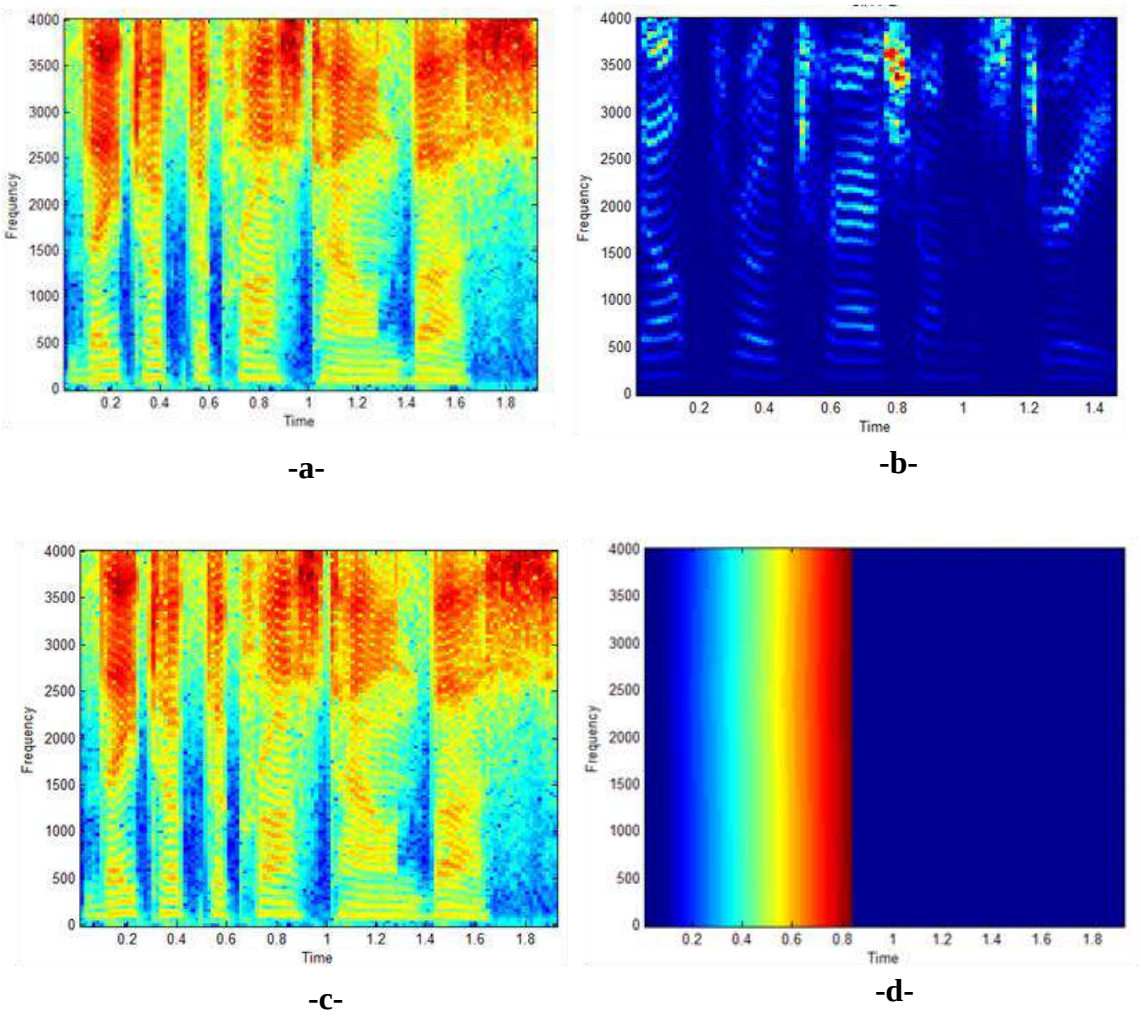


Figure III.7 : Les spectres résultants lors de l'utilisation de filtre Besself

- *(a) signal de base filtré passe-bas.*
- *(b) signal de message secret filtré passe-bande.*
- *(c) signal combiné (stego).*
- *(d) signal reconstitué (message secret).*

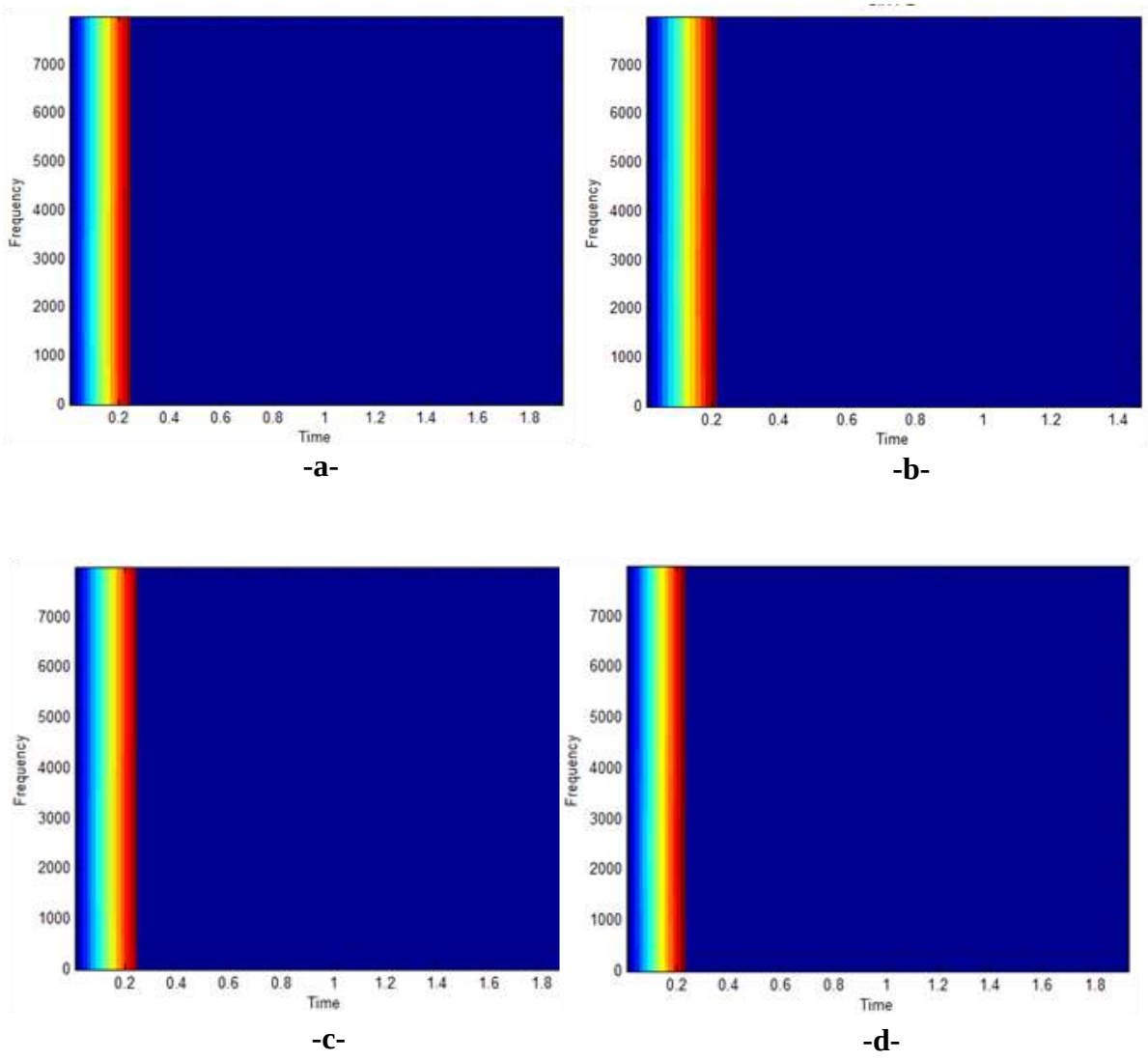


Figure III.8 : Les spectres résultants lors de l'utilisation de filtre Ellipap

- *(a) signal de base filtré passe-bas.*
- *(b) signal de message secret filtré passe-bande.*
- *(c) signal combiné (stego).*
- *(d) le signal reconstitué (message secret).*

La figure III.9 présente les valeurs de PESQ obtenus à partir de chaque type de filtre choisis :

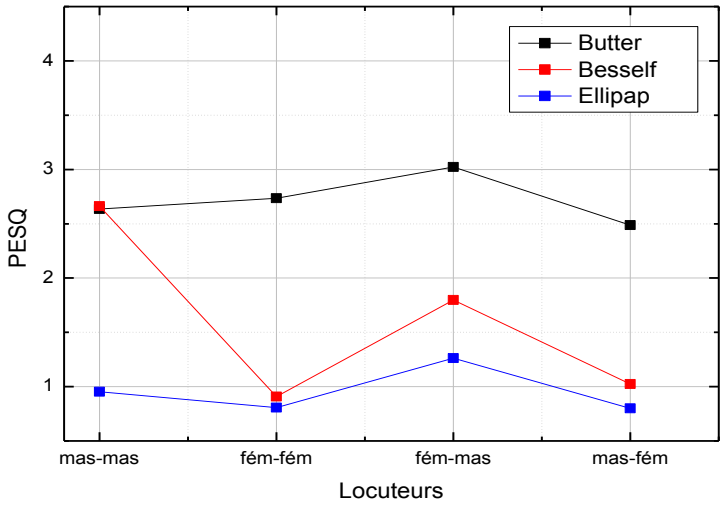


Figure III.9:Résultats obtenus (PSEQ) de variation de type filtres.

III.5.2. Variation de l'ordre de filtrage

Dans cette manipulation, on a choisi le filtre Butter et également on a varié l'ordre de filtrage. Donc Les résultats illustrés sont présentés à partir le Tableau III.3, la figure III.10 exprime la variation de PESQ en fonction de l'ordre choisi :

Tableau III.3 : Résultats obtenue après la variation de l'ordre de filtrage.

L'ordre du filtre / Incorporation		3	6	9	10
Message	Couverture	PESQ			
Masculin	Masculin	1,928	2,471	2,599	2,636
Féminin	Féminin	2,173	2,613	2,690	2,734
Féminin	Masculin	2,231	2,621	2,811	2,839
Masculin	Féminin	2,011	2,358	2,473	2,452
La moyenne		2,085	2,515	2,643	2,665

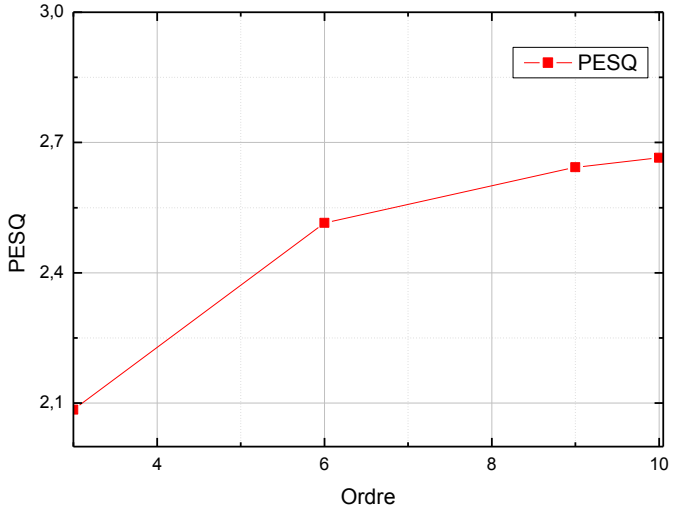


Figure III.10: PSEQ obtenu en fonction de l'ordre de filtrage.

III.5.3. Variation de la fréquence porteuse f_p

Ici, on a varié la fréquence porteuse en émission et en réception tout en conservant le type et l'ordre du filtre, le Tableau III.4 Illustre les variations dues aux changements de la fréquence :

Tableau III.4 : PESQ obtenu après la variation de fréquence porteuse.

f_p du filtre / Incorporation		2500	3050	4000	6000
Message	Couverture	PESQ			
Masculin	Masculin	0,671	1,571	2,636	0,622
Féminin	Féminin	0,421	1,478	2,734	0,740
Féminin	Masculin	1,064	1,789	2,839	0,817
Masculin	Féminin	0,663	1,806	2,452	1,033
La moyenne		0,704	1,661	2,665	0,803

Remarque :

Pour le filtre de Bessel et le filtre élliptique, on a varié l'ordre de filtrage et la fréquence porteuse, mais aucune amélioration trouvée.

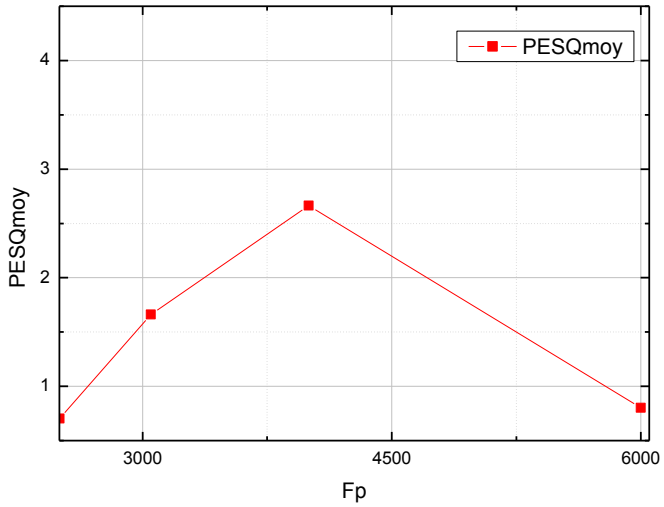


Figure III.11: PESQ obtenu en fonction de la fréquence porteuse.

III.6. Interprétations des résultats

Nos résultats seront interprétés selon la variation de: type de filtre utilisé, l'ordre de filtrage et la fréquence porteuse.

III.6.1. Interprétation des résultats après la variation du type de filtre

Selon les valeurs de PESQ obtenues, le meilleur filtre utilisé pour notre simulation est le filtre Butter (PESQ moyen égale 2,720). L'incorporation des fichiers parole féminins dans les fichiers parole masculins nous donne une valeur de PESQ importante (PESQ égale 3,023), et ce type d'incorporation est le meilleur type comparativement aux autres types à savoir, Masculin-masculin, Masculin-féminin, féminin-féminin, qui donnent des valeurs de PESQ 2.636, 2.486, 2.734 respectivement.

Concernant les filtres Besself et Ellipap, le spectre du signal reçu à la réception est différent que celui émis (perdu) pour les mêmes conditions utilisées avec le filtre Butter qui nous a donné un bon résultat. On peut expliquer ça, que notre signal a perdu ses caractéristiques.

III.6.2. Interprétation des résultats après la variation de l'ordre de filtrage

D'après les évaluations mentionnées précédemment (cf. partie III.5.1). Le filtre Butter se présente comme étant le meilleur type de filtrage pour extraire le message secret. La variation de l'ordre de filtrage donne des améliorations importantes où l'ordre 10 nous donne un bon

score PESQ qui est égale à 2.665 (PESQ> seuil d'intelligibilité). Au-delà de l'ordre 10, l'intelligibilité commence à se dégrade.

III.6.3. Interprétation des résultats après la variation de la fréquence porteuse

A partir de la figure III.11, on constate que la fréquence porteuse choisie 4000 (la moitié de la fréquence d'échantillonnage) est le meilleur choix pour transmettre et recevoir le message secret. Ce dernier donne une valeur de PESQ égale à 2,665 (PESQ> seuil d'intelligibilité) comparativement avec les autres fréquences porteuses choisis 2500, 3050, 6000 qui donnent des valeurs moyenne de PESQ 0.704, 1.661et 0.803 respectivement.

Conclusion

Dans ce chapitre, nous avons présenté une méthode de masquage dont le but d'incorporer un signal audio dans un autre signal audio équivalent où le récepteur est toujours capable de récupérer le message secret de parole envoyé intelligiblement.

Conclusion générale

Ce travail a tout d'abord permis de présenter la méthode stéganographique la plus utilisées dans la littérature, et de montrer ses limitations.

Différentes modifications et améliorations ont été proposées et réalisées. Plus particulièrement, afin d'assurer la sécurité du contenu du message secret, nous avons développé et implémenté une méthode de stéganographie fréquentielle. Cette dernière a été effectuée dont le but de prouver sa robustesse et son résistance contre des attaques de traitement de signal.

Nous avons introduit les concepts de base et les outils mathématiques nécessaires pour la compréhension des recherches menées dans ce mémoire. Nous avons étudié les méthodes stéganographique basée sur codage les plus répandues, La sécurité du contenu du message, lors de sa détection par un adversaire. D'après notre étude le filtre Butter se présente comme étant le meilleur type de filtrage comparativement aux autres types de filtres: Besself et Ellipap. L'ordre de filtre joue aussi un rôle très important pour extraire correctement et nettement le signal caché. L'extraction de ce dernier est basée sur une fréquence porteuse connue seulement par les deux extrémités de conversation communiquant d'une manière secrète. Le domaine fréquentiel est important pour implémenter cette méthode, mais peut être une amélioration sera trouvée si on l'implémente dans le domaine temporel.

BIBLIOGRAPHIE

[1] A.SAHNOUNE, "Mise en œuvre d'un algorithme de codage conjoint source/canal ", mémoire de magister, Juillet 2008, Département: électronique Laboratoire Signal &Communications, École Nationale Polytechnique.

[2] http://dspace.univ-tlemcen.dz/handle/112/6836 (Consulté le 31/05/2017)

[3] R.Dumont, "Cryptographie et sécurité informatique", Mémoire, 2010, Université de liège faculté des sciences appliquées.

[4] C.BARAS, " Tatouage informé de signaux audio numériques", Mémoire de doctorat, Décembre 2005, école nationale supérieure des télécommunications spécialité : signal et images.

[5] S. KHELIDJ, R. HAMADOU, " La stéganographie par la méthode de codage d'Huffman et de modification de direction», Mémoire de master, 2014, faculté des sciences et de la technologie département du génie électrique et de l'informatique, université Dr. yahia fares de Médéa.

[6] M. Ould Medeni,"Application des codes correcteurs d'erreurs en stéganographie", thèse de doctorat**,** Juillet 2012.université Mohammed v-Agdal

[7] Annual Review of Network Management and Security, Volume 1

[8] Jayaram P1, Ranganatha H R2, Anupama H S,"information hiding using audio steganography – a survey " ,August 2011, Department of computer science and engineering, Bangalore, INDIA, the international journal of multimedia & its applications (IJMA) Vol.3, No.3.

[9] Said E. El-Khamy, "A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption",November 2016, Springer DOI 10.1007/s11042-016-4113-8

[10] S.Satapathy, A.Joshi N.Modi, N. Pathak "advances in intelligent systems and computing", Proceedings of international conference on ICT for sustainable development ICT4SD 2015 Volume 1.

[11] F. Djebbar "Comparative study of digital audio steganography techniques", 2012, UAE university, UAE.

[12] ITU-T, Recommendation P.862, “Perceptual evaluation of speech quality (PESQ), an objective method for end-to-end speech quality assessment of narrowband telephone networks and speech codecs”. 2001.

[13] Y.Bassil, "a two intermediates audio steganography technique", November 2012, Journal of emerging trends in computing and information sciences (CIS).

[14] M.NEMATOLLAHI, "Highlights digital watermarking techniques based on their applications", 2011, Islamic Azad University (IAU), Dubai, UAE.

[15] A.SUHAIB "Audio steganography using tone insertion technique", September 2014, Sudan university of science and technology college of graduate studies.

[16] H.KHEDDAR, B.BOUDRAA, "Etude comparative de méthodes de correction de pertes de paquets en transmission de la voix sur IP(VoIP)".Mémoire magister, année 2012, laboratoire LCPT université USTHB.

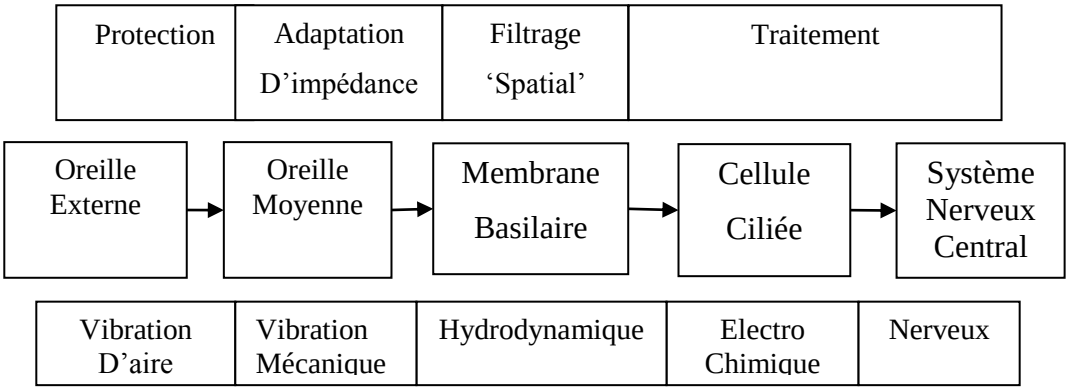
[17] M. Saidi “codage par description multiple en MELP pour la VoIP”. Mémoire magister, année 2010, laboratoire LCPT université USTHB.

[18] M. Boudraa, B.Boudraa, B. Guérin,"Twenty lists of ten arabic sentences for assessment", Acustica, vol. 86, pp. 870-882, 2000.

ANNEXE A

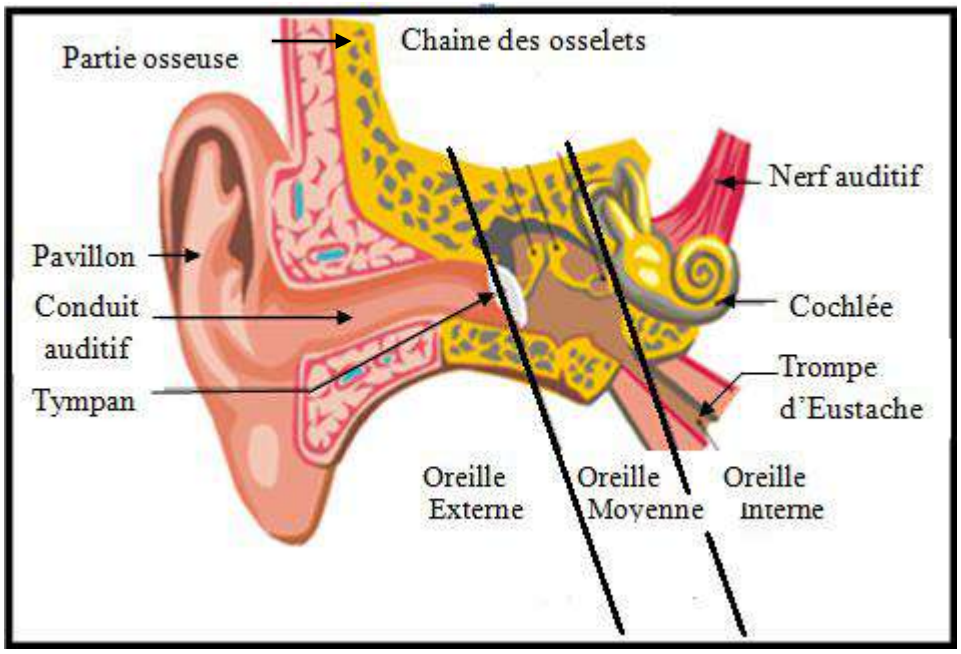
Le système auditif humain (HAS)

La figure suivante illustre de façon synoptique le fonctionnement de l'appareil auditif :



Il comprend l'oreille externe, l'oreille moyenne et l'oreille interne. L'oreille externe capte le signal en forme de différences de pression de l'air et joue un rôle de protection. Le mécanisme de l'oreille moyenne (marteau, étrier, enclume) transmet le signal sonore à la cochlée. La vibration mécanique de cette zone transmet le signal à l'oreille interne. Cette dernière contient la membrane basilaire et supporte l'organe de Corti qui est raccordé au nerf auditif à l'aide des cellules ciliées. Les cellules ciliées génèrent des impulsions électrochimiques associées aux vibrations de la membrane.

La transmission de l'information est faite après plusieurs transformations du signal (mécaniques, hydrauliques, électriques) dès son entrée dans le système auditif jusqu'à son arrivée au cerveau. En ce qui concerne la réponse en fréquence du système. Le rôle principal est joué par la membrane basilaire située dans la cochlée. Ses caractéristiques géométriques et mécaniques font de cette membrane un système de résonance qui possède des caractéristiques particulières. Pour un système résonant à deux dimensions, la spécification de sa géométrie (sa forme et sa taille) va déterminer ses modes de résonance. En réalité le HAS est schématisé comme suivant :


Partie osseuse
Chaine des osselets
Nerf auditif
Pavillon
Conduit auditif
Tympan
Cochlée
Trompe d'Eustache
Oreille Externe
Oreille Moyenne
Oreille interne