REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE AMMAR TELIDJI LAGHOUAT

Faculté des sciences

Département de mathématiques et informatique

Mémoire en vue de l'obtention du Diplôme de Master de

recherche en informatique

Option :Réseaux, system et application répartie

Thème :

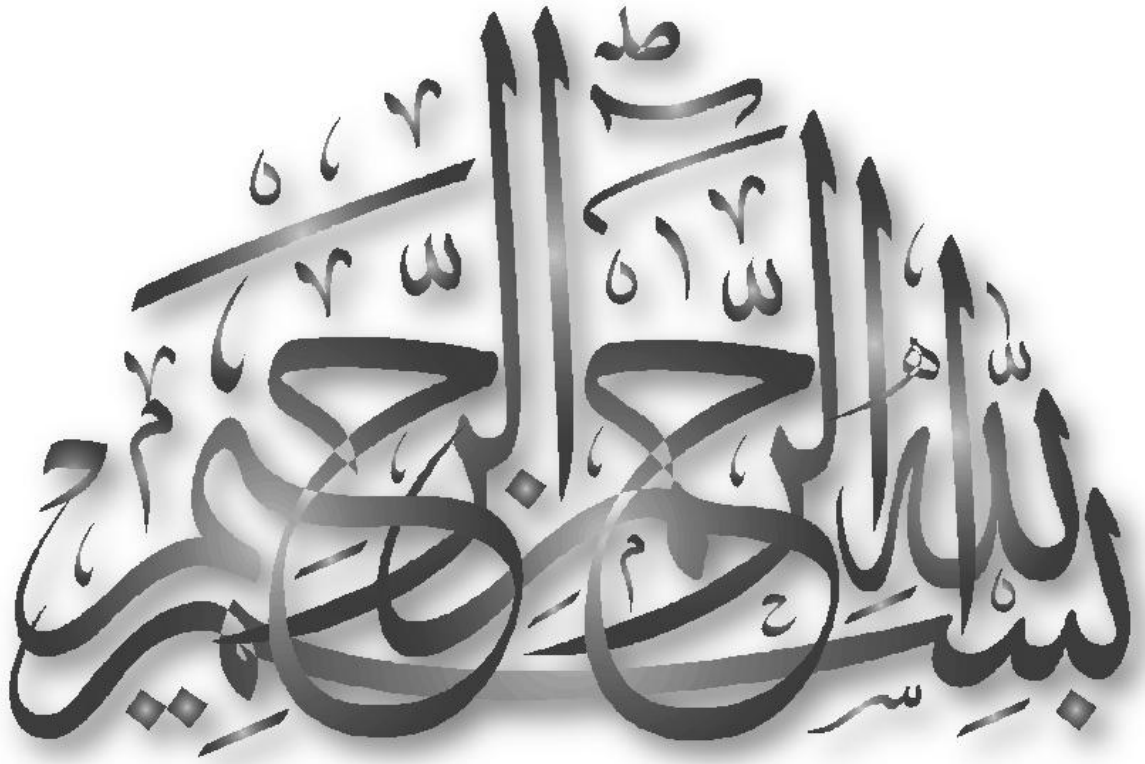
L'implementation d'une nouvelle technique de stéganographie VOIP

Présenté Par : Melle Boutassouna Khadidja

Soutenu devant le jury composé de :

Dr. Bendouma Taher	Président	université de Laghouat
Mr. Chaib Noureddine	Examinateur	Université de Laghouat
Mr. Kechna Lakhdar	Examinateur	Université de Laghouat
Dr. Bensaad Lahcen	Encadreur	Université de Laghouat

Année Universitaire : 2013-2014


بسم الله الرحمن الرحيم

Dédicaces

Je dédie ce mémoire à :

La mémoire de ma mari Cheknane Mourad.

ma mère est la lumière de mes yeux, l'ombre de mes pas et le bonheur de ma Vie mes parents, qui ma apporté son appui durant toutes mes années d'étude, pour son sacrifice et soutien qui m'ont donné confiance, courage et sécurité.

A mon cher père qui ma appris le sens de la persévérance tout au long de mes études, pour son sacrifice ses conseils et ses encouragements.

- *A mes très chères sœurs : Wafa et Masouad et Assia et Rabia et Amine et Sara et Hadda*
- *A mes Grands frères : Djamel et Lamine et Mostapha et Aissa et Mouse et Ahmed*

A toute ma grande famille Boutassouna sans exception

A tous mes amis et surtout fatima qui m'a aidé beaucoup .

J'exprime ma reconnaissance à tous ceux qui ont contribué de prés ou de loin à accomplir ce modeste travail.

Remerciement

Je tiens à remercier tout d'abord « Allah » le tout puissant, de m'avoir donné le courage, la volonté, la force et la patience afin de parvenir à terminer ce modeste travail.
Je voudrai adresser l'expression de ma gratitude, ma profonde sympathie ainsi que mes vifs remerciements à :

- *à mon promoteur le monsieur* ***Mr. Bensaad.*** *pour avoir dirigée et guidée ce travail. Je le remercie surtout pour son entière disponibilité et ainsi que pour la marque de confiance qu'il m'a donnée pour accomplir cette étude.*

- *à qui m'a fait l'honneur de présider le jury, à . pour avoir accepté de faire partie de ce jury.*
- *à tous les professeurs qui m'ont donné le meilleur d'eux même en contribuant à augmenter mon savoir durant mes études.*

Enfin, je remercier toutes personnes qui m'a aidé et encouragé de près ou de loin, à la réalisation de ce mémoire et durant mon chemin universitaire.

Merci

Résumé

La sécurité de l'information a considérablement évolué rapidement au cours des dernières années. La dissimulation de l'information est un moyen efficace pour cacher les données secrètes. Le plus grand défi de la stéganographie est comment faire pour augmenter la quantité d'informations qui peuvent être cachées dans le canal de l'hôte sans affecter les propriétés de ce canal tout en gardant cette transmission secrète invisible à des tiers non autorisés. Pour faire face à ce défi, beaucoup de méthodes, de médias, des techniques et des algorithmes sont introduits. Un nouveau moyen de communication et prometteur qui peut être utilisé comme un hôte pour la stéganographie est la VoIP (Voice over Internet Protocol).

Cette thèse porte sur des techniques stéganographique disponibles qui peuvent être utilisés pour créer des voies secrètes pour les flux VoIP. Sur cette base, dans cette thèse ont suggéré une technique pour améliorer la stéganographie VOIP et on teste les résultats qui montrent que notre méthode ne fait pas nuire la qualité de la parole qui en fait un bon candidat pour servir à des fins différentes.

Les mots clés : dissimulation de l'information, la stéganographie , des données secrètes, VoIP.

Abstract

The information security has considerably evolved rapidly over the past years. Information hiding is an effective way for securing secret data. The biggest challenge of steganography is how to increase the amount of information to be embedded in the host channel without affecting the properties of this channel while keeping this secret transmission invisible to third parties not allowed. To meetthis challenge, many methods, media, techniques and algorithms are introduced. A new means of communication and promising that can be used as a host for steganography is Voice over Internet Protocol(VOIP).

This thesis focuses on available steganographic techniques that can be used to create secret channels for VoIP streams. On this basis, in this thesis have suggested a technique to improve VOIP steganography and testing results that show that our method does not affect the quality of the floor which makes it a good candidate to serve different purposes.

Keywords: Information Hiding, steganography, secret information, VOIP.

ملخـــص

أمن المعلومات قد تطور إلى حد كبير على مدى العقود الماضي, إن تقنية الكتابة الخفية هي واحدة من الطرق الأساسية التي يمكن أن تحافظ على سرية البيانات . و يجب الإشارة أن التحدي الأكبر لإخفاء المعلومات يكمن في كيفية زيادة مقدار المعلومات التي تكون جزءا لا يتجزأ من القناة الحاملة للمعلومات بدون التأثير على خصائص هذه القناة مع الإبقاء على سرية هذا الإرسال الغير المرئي للأطراف غير المصرح لها. واجهة هذا التحدي، هناك العديد من الأساليب، ووسائل الإعلام، التي تسمح بإدخال تقنيات وخوارزميات في واحدة من وسائط الاتصالات الجديدة . يمكن استخدام الصوت عبر"بروتوكول الإنترنت" كناقل لإخفاء المعلومات .

وتتركز هذه الأطروحة على احدى تقنيات الكتابة الخفية المتوفرة و التي يمكن استخدامها لإنشاء قنوات سرية لتيارات الصوت عبر بروتوكول الإنترنت. وعلى هذا الأساس، تقترح هذه الأطروحة أسلوباً لتحسين إخفاء المعلومات عبر الإنترنت. و نتائج الاختبارات تظهر أن لدينا أسلوب لا يؤثر على نوعية الكلام الذي يجعله مرشح جيد لأغراض مختلفة.

الكلمات المفتاحية : اخفاء المعلومات , الكتابة الخفية , أمن المعلومات, الصوت عبر برتوكول الانترنت

Table des matières

Table des figures

La table des codes sources

La Liste Des Abréviations

DSP Digital Signal Processor

HAS Human Auditory System

HICCUPS Hidden Communication System for Corrupted Networks

iLBC Internet Low Bitrate Codec

LACK Lost Audio PaCKets Steganography

LSB Least Significant Bit

PDU Protocol Data Unit

PESQ Perceptual Evaluation Speech Quality

RTCP Real Time Control Protocol

RTP Real Time Protocol

SS Spread Spectrum

VOIP Voice over IP

1 Introduction générale

1.1 Préambule :

Le 11 Janvier 2014 à 09h des pirates informatiques ont réussi à infiltrer le réseau et obtenir l'accès aux cartes de crédit des américains de la grande distribution Target. Et après l'enquête, 110 millions de personnes sont concernées par cette escroquerie.

se rend compte que des pirates informatiques ont réussi à infiltrer leurs réseaux et d'obtenir l'accès aux cartes de crédit de 40 millions de consommateurs. Avant cela, il y a une autre attaque et suit, le 21 Mars 2014 à 16h les services secrets canadiens soupçonnent la France d'être derrière une opération de piratage informatique à grande échelle, à l'aide d'un implant espion opérationnel depuis près de cinq ans, selon une note secrète révélée par le journal Le Monde. Principalement visées, des institutions iraniennes liées au programme nucléaire, mais aussi des pays "amis" comme le Canada, la Norvège, l'Espagne ou la Côte d'Ivoire.

Toutes ces réactions ont un seul incident, il suffit à démontrer comment la sécurité et la vie privée sont importantes pour les gouvernements et la population en générale. En fait depuis que l'homme a commencé à écrire et envoyer des messages, il était dans le besoin de secret et d'une vie privée pour cacher ses informations secrètes ou partager avec des personnes spécifiques sans les autres. La stéganographie et la cryptographie sont reposées sur l'idée de sécurité de l'information .

Cette thèse se concentre uniquement sur la stéganographie qui est devenu l'un des domaines de recherche les plus étudies ces dernières années en raison de son importance dans

la résolution de nombreux problèmes difficiles non seulement dans le domaine civil, comme la protection du droit de l'auteur, la protection bancaire, les secrets de communication et de l'éducation, ainsi que dans d'autres domaines.

1.2 Motivation :

L'explosion des réseaux de communication et l'arrivée d'Internet exige une propagation des nouvelles technologies pour faire naître une grande circulation de l'information (image, texte, son, vidéo,...).

La stéganographie est une technologie très importante pour l'avenir de la sécurité de l'Internet et de la protection des renseignements personnels sur des systèmes ouverts. Une des raisons de son utilisation est que la cryptographie est parfois interdite par la loi où d'utiliser un cryptage. Par exemple, les Etats-Unis considèrent les produits cryptographiques comme des bombes à sous-munitions et interdit l'exportation de crypto-systèmes forts . Une autre raison est que la cryptographie n'est pas toujours sûre, par exemple, dans certains systèmes de VOIP phrases parlées cryptées peuvent être révélées sans rien savoir sur le processus du chiffrement [Shu13].

Donc l'objectif de la stéganographie est d'envoyé de manière fiable les informations cachées secrètement, la stéganographie d'aujourd'hui est considérée comme une sous discipline de la communication des données dans le domaine de sécurité. Elle peut être utilisée pour dissimuler des données importantes dans un autre fichier de sorte.

L'idée principale est d'améliorer une technique disponible. Le nombre limité de recherches dans ce domaine a fait ajouter plus de difficultés à terme.
Le fait qu'il y a un nombre limité de recherches à sur ce domaine m'a permis la motivation du choix de ce sujet afin d'ajouter ma contribution à ce champ nouvellement étudié.

1.3 Objectifs :

Dans notre travail, on s'intéresse à étudier la stéganographie VOIP.
Les objectifs de ce projet sont :

1 : Etudier la stéganographie audio, analyser ses techniques actuelles et discuter leurs performances en termes de capacité et d'autre critères.

2 : Proposer des moyens efficaces pour améliorer la capacité des données secrètes en stéganographie VOIP .

3 : Développer un système simple qui effectue la stéganographie VoIP en utilisant le codec ILBC est une technique LSB.

1.4 La structure du mémoire :

Ce mémoire est structuré en quatre Chapitres :

Chapitre 02 : Présentation des origines de la science stéganographie et en vue générale de la cryptographie qui ont de différents concepts théoriques. En mettant l'accès sur le principe de la stéganographie, différents Supports et techniques de la stéganographie (l'image, texte, audio, réseau , VOIP). Pour la VOIP on présente ses principes fondamentaux et leur architecture, compression de la Voix (iLBC).

Chapitre 03 : Contient les états de l'art de chacun des domaines auxquels on va travailler sur la stéganographie audio et VOIP. Un aperçu globale du principe d'un système de stéganographie audio, en expliquant les différentes méthodes de stéganographie audio et ses critères de comparaison. Autre direction en expliquant la stéganographie de la VOIP qui est basée sur notre travail.

Chapitre 04 : Consiste à modéliser et implémenter l'approche proposée, Enfin, nous terminons le mémoire par donner des conclusions sur le travail et par exposer certaines perspectives de notre recherche.

2

Préliminaires de la stéganographie

Le réseau Internet a tellement évolué qu'il est devenu un outil essentiel de communication. Cependant, cette communication met de plus en plus en jeu des problèmes stratégiques liés à l'activité des entreprises sur le Web. Les transactions faites à travers le réseau peuvent être interceptées, d'autant plus que les lois ont du mal à se mettre en place sur Internet, il faut donc garantir la sécurité de ces informations, c'est la stéganographie qui s'en charge. Le mot stéganographie vient du grec 'steganos' (caché ou secret) et 'graphy' (écriture ou dessin), littéralement, 'écriture cachée' .[PEL04]

Dans ce chapitre, nous allons essayer de présenter brièvement la cryptographie et la stéganographie en les définissant et donnant leurs principales caractéristiques et stéganographie qui peuvent être perçues dans une telle applique. Ensuite, nous exposerons les grandes techniques des applications de la stéganographie.

2.1 Historique :

La stéganographie est un art exploité connu depuis l'Antiquité. Vous trouverez la figure (2.1) quelques dates et utilisations de cette discipline. Il est bien entendu que cette description n'est pas exhaustive. Sa première mention est relatée en **440 JC**. Hérodote relate le fait qu'Histiée rasa la tête d'un esclave fidèle afin d'y tatouer un message et attendit la repousse des cheveux, rendant ainsi le message invisible. Suite aux instructions de l'esclave. La stéganographie a été très souvent employée et s'est ouverte à un grand nombre de formes. Une représentation chronologique, à la page suivante, retrace certaines de ses utilisations dans l'histoire..

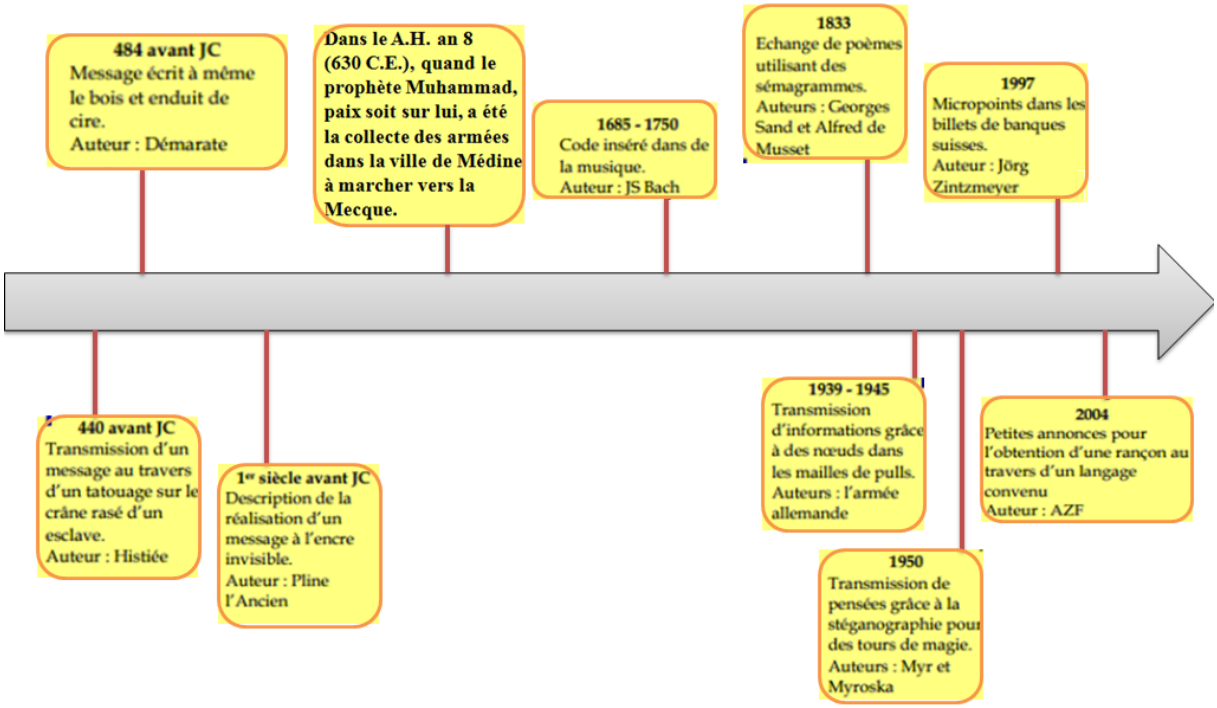


FIGURE 2.1 – L'historique de la stéganographie [DEN05].

2.2 La cryptographie :

La définition de cryptographie : La cryptographie est un ensemble de techniques qui protègent un message en le transformant en un autre message, cette transformation modifie l'information contenue dans le message original pour rendre l'information transmise non compréhensible. Les cryptographes inventent des méthodes de chiffrement de plus en plus complexes, composées d'une fonction de chiffrement et d'une fonction de déchiffrement[HS06].

La fonction de chiffrement permet de chiffrer un message donné **m** par une clef **k**, un paramètre de la fonction de chiffrement. Nous notons **mk** le message **m** chiffré par la clef **k** [HS06]. La fonction de déchiffrement permet à partir d'un message chiffré mk de retrouver le message original m connaissant la clef de déchiffrement **k** [DEN05] .

m → fonction de chiffrement+clef → {m}k

mk → fonction de déchiffrement+clef → m

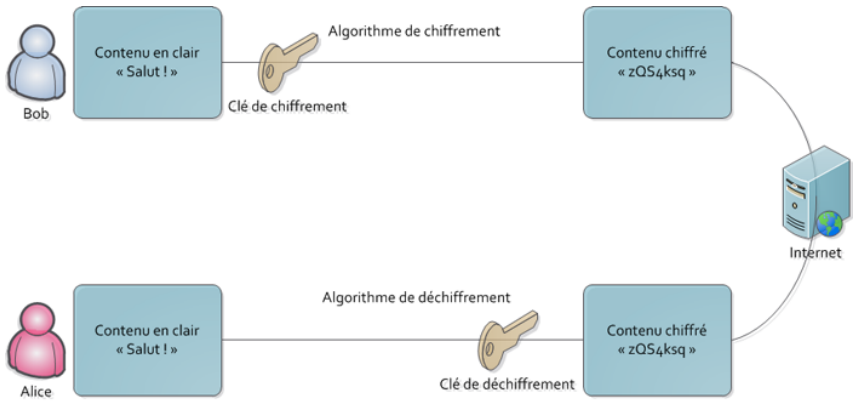


FIGURE 2.2 – Méthodes de chiffrement et déchiffrement dans le réseau.

Les Algorithmes Chiffrement : On résume les types des algorithmes des chiffrements de cryptographie La figure(2.3).

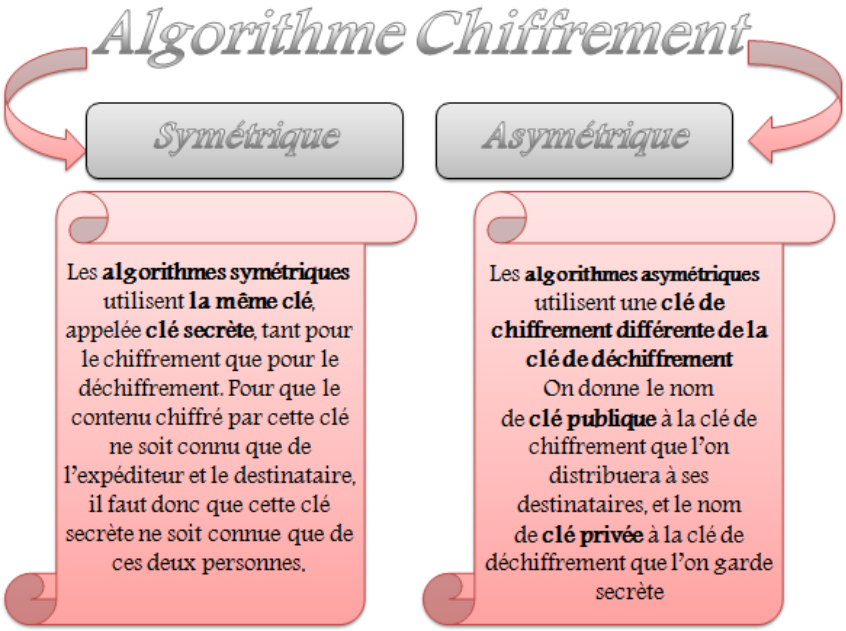


FIGURE 2.3 – Les Algorithmes des chiffrements.

2.3 La stéganographie :

Grâce aux moyens informatiques dont nous disposons, nous pouvons exprimer toute notre créativité et stéganographie à loisir tout en éveillant au minimum l'attention. En effet l'information numérique à l'état brut peut généralement subir de nombreuses compressions destructives par élimination de données inutiles [HS06]. L'idée est alors de remplacer ces données inutiles, ces bruits de fond parasites par des données plus utiles qui seront en fait les données que l'on veut cacher.

Pour cacher des données, on peut utiliser toute sorte de types de fichiers numériques : images, sons, vidéos. Dans la figure(2.4) on peut expliquer un peu la discipline de sécurité des données numériques .

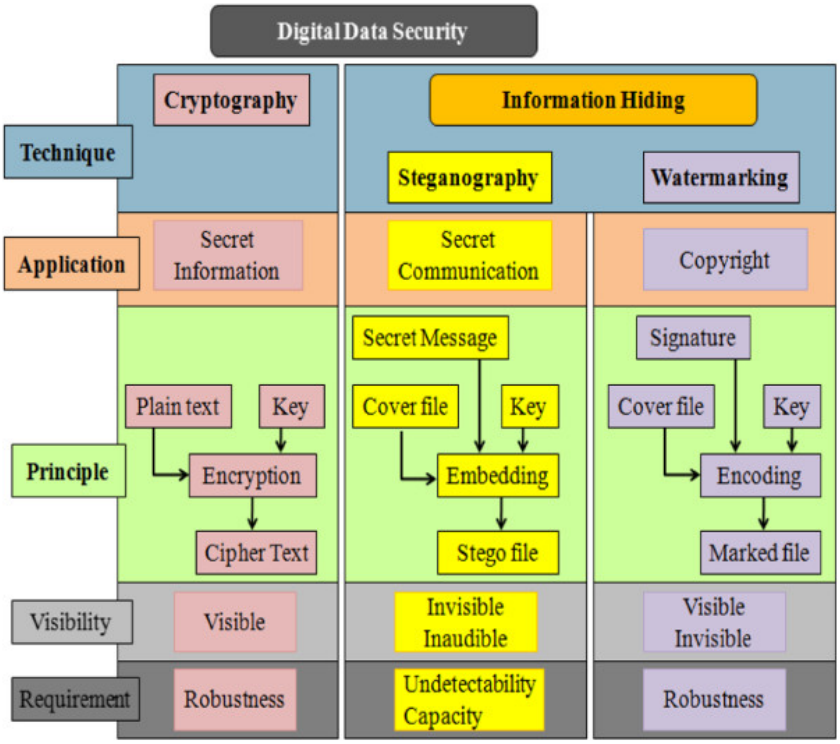


FIGURE 2.4 – Discipline de sécurité des données numériques[DAMH12].

La stéganographie fait partie du domaine de la dissimulation d'information, donc nous allons d'abord expliquer ce qu'est la dissimulation d'information, puis distinguer brièvement le principe de la stéganographie.

2.3.1 La dissimulation d'information :

Il désigne le fait de cacher une information dans un support. Dans le domaine de la dissimulation d'information[GUI12], il faut trouver le juste équilibre entre :

- La capacité, c'est-à-dire la quantité d'informations que l'on peut incorporer dans un support.
- L'imperceptibilité, c'est-à-dire les chances que le stégo-médium soit détecté « non stégo» par un attaquant.
- La robustesse, c'est-à-dire l'aptitude de préservation des données cachées face aux modifications, volontaires ou non, du stégo-médium (compression, filtrage, etc.).

2.3.2 Principe d'un système de la stéganographie :

La stéganographie est aussi l'art et la science de dissimuler un message dans un message quelconque. [Lu96] Les informations du message caché ne sont pas véritablement chiffrées, elles sont le plus souvent seulement cachées dans la masse des bits qui forment une image, un son, un flux audio ou vidéo. Evidemment, rien n'empêche, en plus, de chiffrer le message avant de le dissimuler dans une image ou un son. La stéganographie étudie les techniques pour communiquer de l'information de façon cachée.

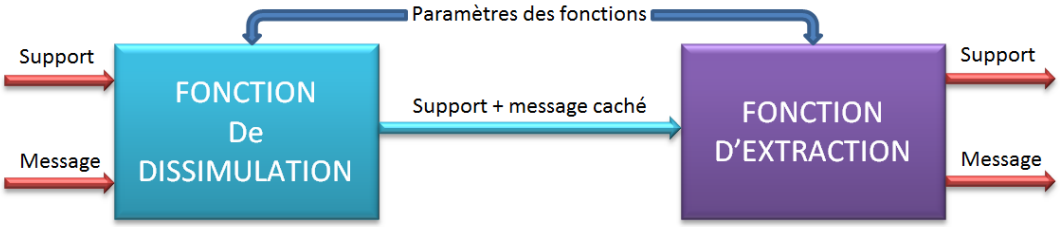


FIGURE 2.5 – Un système de stéganographie .

2.4 Les différences entre la stéganographie et la cryptographie :

L'une des principales difficultés lorsque on aborde la stéganographie est de la distinguer de la cryptographie. La stéganographie est une sous-discipline de la dissimulation d'informations. Cette dernière, déjà très ancienne, consiste à dissimuler un message, que l'on désire transmettre confidentiellement, dans un flux de données d'apparence anodine, de façon que sa présence soit imperceptible. Comme dans le cas de la cryptographie, permet d'échanger des messages avec un correspondant sans que des personnes non autorisées ne puissent en prendre connaissance. Mais alors qu'avec la cryptographie traditionnelle, la sécurité repose sur le fait que le message est incompréhensible, en matière de stéganographie, la sécurité repose sur la remise en question même de l'existence du message [PEL04]. Le tableau(2.1)représente les différences entre la stéganographie et la cryptographie [Ben14].

TABLE 2.1 – Différences entre la stéganographie et cryptographie .

Stéganographie	Cryptographie
Se cache un message dans un autre message et ressemble à un fichier normale, de vidéo ou sonore...etc	Le message est chiffré, ressemble à un fouilli sans signification des caractères.
Une collection d'images graphiques, fichiers vidéo ou des fichiers audio...etc sur un disque ne peut pas regard soupçonneux.	Une collection de caractères aléatoires sur un disque peut sembler suspecte.
Une espionne intelligente peut détecter quelque chose de suspect d'un soudain changement de format de message (par exemple, du texte images graphiques).	Une espion intelligente peut détecter une communication secrète d'un message qui a été codé par chiffrement.
Requiert attention lors de la réutilisation des images ou des fichiers audio.	Requiert attention lors de la réutilisation des touches.

2.5 Supports et techniques de la stéganographie :

Nous passons en revue aux différents supports numériques utilisés pour dissimuler des Données : le texte, l'image et le son, page HTLM ,les réseaux de la télécommunication (VOIP, WALN).

2.5.1 Texte :

Il s'agit du premier médium sur lequel ce type de stéganographie a été appliqué , voici des différentes techniques [eNHSeABeAM06] :

- Trous sous les lettres importantes.
- Changement de type d'écriture.
- Utilisation des synonymes.
- Changement des règles de grammaires.
- Jeu sur les espaces .

Exemple : Méthode des "espaces" (entre les mots) Cette méthode est basée sur le Jeu sur les espaces, nous allons coder notre texte dans le nombre d'espaces entre chaque mot. On se met d'abord d'accord sur une convention :

Un espace entre deux mots suivi de deux espaces entre les deux mots suivants ⇔ 0.
deux espaces entre 2 mots suivi d'un espace entre les 2 mots suivants ⇔ 1
Pour mieux comprendre voici un exemple avec le texte suivant :

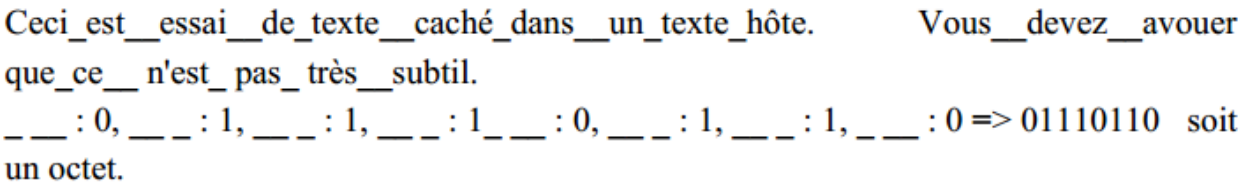


FIGURE 2.6 – Méthodes des "espaces" (entre les mots)[eNHSeABeAM06].

Le rapport texte à coder sur texte hôte. Il vous faut 2 mots pour un bit, donc pour une phrase de 20 mots (20*7=240 bits), il faut un texte hôte de 480 mots. [eNHSeABeAM06].

2.5.2 Image :

Une image est constituée de points (ou pixels) qui sont autant de données permettant à l'ordinateur de recréer l'image lors de la lecture du fichier.
Il est possible d'insérer des nouvelles des bits dans ces données, afin de constituer un message caché dans l'image initiale.
« Chaque pixel est constitué de trois couleurs : le rouge, le vert et le bleu. Certains de ces points peuvent être remplacés par une autre information sans que les changements apportés dans l'image soient perceptibles à l'œil humain ».
Pour pouvoir lire ce message caché, la personne recevant l'image doit connaître la clé permettant de lire les informations contenues. Sans cette clé privée, il est impossible de lire le contenu caché, et l'image garde tout son mystère. [eNHSeABeAM06]
la figure (2.7)représente le principe de la stéganographie.

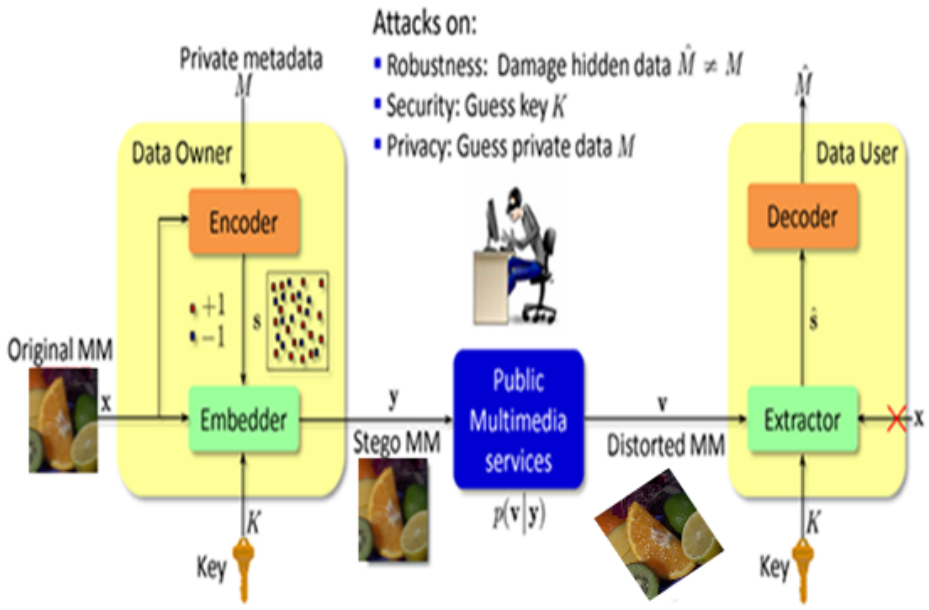


FIGURE 2.7 – Application de la Stéganographie d'un texte dans une image [eNHSeABeAM06].

2.5.3 HTML :

Certains logiciels de stéganographie se proposent de cacher des messages dans des pages HTML [Ben06], ils ne font que toucher au source pour camoufler le fichier secret en insérant des espaces entre balises, variant minuscules et majuscules dans les balises,... Astucieux mais cela peut toutefois se détecter par une analyse statistique et même par un coup d'oeil au source .

Exemple : Dans toute page HTML comme celle-ci, il y a (ou il peut y avoir) des indications qui n'apparaissent pas sur l'écran des navigateurs ce sont les balises 'META' (Les balises META servent à placer des métadonnées (metadata) dans une page HTML. On placera ces informations dans l'élément head, et elles ne seront pas affichées sur la page).

2.5.4 Audio :

La stéganographie, en général, dépend de l'imperfection des systèmes auditifs et visuels humains HAS. [Shu13] Audio stéganographie exploite le phénomène de dissimulation psychoacoustiques (La psychoacoustique est la branche de la psychophysique qui relie les sensations auditives de l'être humain aux sons qui parviennent à ses oreilles.

Elle fait appel à l'acoustique, qui étudie la nature et les propriétés des ondes sonores, à la physiologie de l'audition, à la psychologie et aux sciences cognitives). De faibles variations, imperceptibles pour l'oreille, dans les basses fréquences ou ce que l'on appelle le bruit de fond peuvent contenir une grande quantité d'informations. Un grésillement infime peut cacher des secrets.
Evidemment, ce bruit doit de préférence être transmis de façon numérique sans quoi les vrais pertes de transmission pourraient effacer entièrement le message caché. Afin de rester indécelable, le bruit artificiel doit posséder les propriétés statistiques d'un vrai bruit de fond.

2.5.5 Les réseaux de télécommunication :

Toutes les informations se cachant des techniques qui peuvent être utilisés pour échanger des stéganogrammes dans les réseaux de télécommunication peuvent être classées sous le terme général de réseau stéganographie. Cette nomenclature a été initialement introduite par Krzysztof Szczypiorski en 2003. [BJS10a] contrairement aux méthodes stéganographiques typique qui utilisent les médias numériques (images, fichiers audio et vidéo) comme une couverture pour les données cachées, réseau stéganographie utilise les éléments de contrôle des protocoles de communication et leurs fonctionnalités de base intrinsèque.
En conséquence, ces méthodes sont plus difficiles à détecter et à éliminer. [JL10a] Réseau steganographiques typiques méthodes impliquent la modification des propriétés d'un protocole de réseau unique. Une telle modification peut être appliquée à la PDU .[Szc10][Chu][Ali10] les relations de temps entre le PDU échangées, [DK10] ou les deux (méthodes hybrides).[MS10]
En plus, il est possible d'utiliser la relation entre deux ou plusieurs protocoles de réseau différents pour permettre des communications secrètes. Ces applications se classent sous le terme inter-protocole stéganographie[BJS10b] . Stéganographie réseau couvre un large éventail de techniques, qui comprennent entre autres :

1-WLAN stéganographie :

l'utilisation de méthodes qui peuvent être exercées pour transmettre des stéganogrammes dans les réseaux sans fil locaux. Un exemple concret de la stéganographie WLAN est une protocole (WLAN) comme couverture pour une communication stéganographique se trouve en 2003, Krzysztof Szczypiorski1 a introduit une méthode de construction

d'un canal caché à l'aide de paquets WLAN délibérément endommagés pour la communication. Kraetzer et coll. a introduit, en 2006 une approche de stéganographie WLAN qui fonctionne sans générer des paquets réseau corrompu , et le HICCUPS est un système stéganographique avec allocation de bande passante pour réseaux moyens partagés. système caché Communication pour réseaux corrompus [Szc10].

2-La Stéganographie de la Voice-over-IP :

- Voix sur IP :

La voix sur IP, ou VOIP pour Voice over IP est une technique qui permet de communiquer par la voix (ou via des flux multimedia : audio ou vidéo) sur des réseaux compatibles IP, qu'il s'agisse de réseaux privés ou d'Internet, filaire ou non satellite, Wi-Fi, GSM, UMTS ou LTE. La VOIP concerne le transport de la voix sur un réseau IP.Cette technologie est complémentaire de la téléphonie sur IP [MS10].

- Architecture de transmission VOIP :

Le principe de la téléphonie sur IP est la numérisation de la voix, c'est-à-dire le passage d'un signal analogique à un signal numérique. Celui-ci est compressé en fonction des codecs choisis, cette compression a comme but de réduire la quantité d'informations qui est transmise sur le réseau. Le signal obtenu est découpé en paquets. A l'arrivée, les paquets transmis sont réassemblés . Le signal de données ainsi obtenu est décompressé puis converti en signal analogique afin que l'utilisateur puisse écouter le message d'origine [WAN07].
La technologie de la voix sur IP (VOIP pour Voice over IP) nous présente une architecture découpée en 8 grandes étapes, la figure(2.8) suivante :

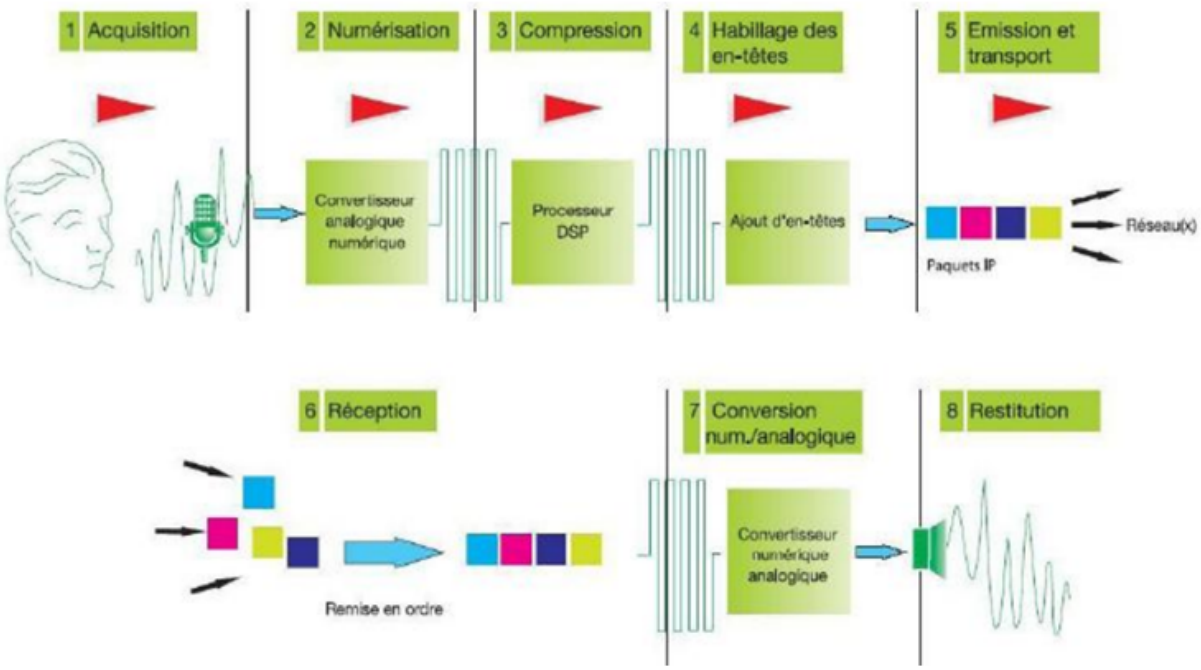


FIGURE 2.8 – Transmission de voix dans un système de VOIP [Shu13].

*** Acquisition du signal :** La VOIP suppose la transformation d'un signal continu analogique (la voix) en un signal discret numérique (composé d'une série de chiffres). La première étape consiste naturellement à capter la voix à l'aide d'un micro, qu'il s'agisse de celui d'un téléphone ou d'un micro casque.

*** Numérisation :** La voix passe alors dans un convertisseur analogique numérique qui réalise deux tâches distinctes :

- l'échantillonnage du signal sonore, c'est-à-dire un prélèvement périodique de ce signal.
- la quantification, qui consiste à affecter une valeur numérique (en binaire) à chaque échantillon. Plus les échantillons sont codés sur un nombre de bits important, meilleure sera la qualité (on parle de «résolution») de la conversion.

  Généralement, la voix est échantillonnée à 8 kHz et chaque échantillon est codé sur 8 bits, ce qui donne un débit de 64 kbit/s .

*** Compression :** Le signal une fois numérisé peut être traité par un DSP qui va le compresser, c'est-à-dire réduire la quantité d'informations (bits) nécessaire pour l'exprimer. Plusieurs normes de compression et décompression (Codec) sont utilisées pour la voix.

L'avantage de la compression est de réduire la bande passante nécessaire pour transmettre le signal.

*** Habillage des en-têtes :** Les données (brutes) qui sortent du DSP doivent encore être enrichies en informations avant d'être converties en paquets de données à expédier sur le réseau. Trois (couches) superposées sont utilisées pour cet habillage :

- La couche IP correspond à l'assemblage des données en paquets. Chaque paquet commence par un en-tête indiquant le type de trafic concerné, ici du trafic TCP.
- La deuxième couche UDP/TCP, consiste à formater très simplement les paquets. Il est nécessaire que l'on ne perde pas de temps à réémettre des paquets perdus. Le protocole TCP a donc été écarté au profil du protocole UDP qui ne gère pas les demandes d'acquittement et de retransmission de paquets perdus ou erronés. C'est ce qu'on appelle un protocole sans correction d'erreur. Mais dans un soucis de qualité
- La couche RTP / RTCP Pour palier l'absence de fiabilité d'UDP /TCP, un formatage RTP est appliqué de surcroît aux paquets. Il consiste à ajouter des entêtes d'horodatage et de synchronisation pour s'assurer du réassemblage des paquets dans le bon ordre à la réception. RTP est souvent renforcé par RTCP qui comporte, en plus, des informations sur la qualité de la transmission et l'identité des participants à la conversation.

*** Emission et transport :** Les paquets sont acheminés depuis le point d'émission pour atteindre le point de réception sans qu'un chemin précis soit réservé pour leur transport. Ils vont transiter sur le réseau (réseau local, réseau étendu voir Internet) en fonction des ressources disponibles et arriver à destination dans un ordre indéterminé.

*** Réception :** Lorsque les paquets arrivent à destination, il est essentiel de les replacer dans le bon ordre et assez rapidement.

*** Conversion numérique analogique :** La conversion numérique analogique est l'étape réciproque de l'étape 2, qui permet de transformer les données reçues sous forme de série discrète en un signal électrique (continu).

*** Restitution :** Dès que, la voix peut être retranscrite par le haut-parleur du casque, du combiné téléphonique ou de l'ordinateur.

Dans le cadre de la téléphonie VOIP, on ne cherche qu'à transmettre la voix. Les besoins sont donc très différents. Pour pouvoir transiter sur Internet, la voix doit être codée et séparée en paquets. Ces paquets seront ensuite transmis au destinataire, qui va les décoder et restituer le son à l'autre personne. Le travail du codec est donc d'effectuer toutes ces opérations.

De nombreux codecs ont été mis au point pour effectuer ce travail. Parmi les plus utilisés dans le cadre de la téléphonie VOIP, on peut choisir ILBC. à travers ce point on doit expliquer codec ILBC .

- Description des iLBC : iLBC soumis à Force de travail IETF (Internet Engineering) en 2002 et la spécification finale (RFC 3951)[Lin04b] a été publiée en 2004. C'est un codec de discours libres open source adaptée à la communication vocale robuste sur IP.
iLBC a été développé par Global IP Solutions (GIPS) qui était alors racheté par Google en 2011 [Ben14]. C'était autrefois le freeware avec commercial limité utilisé, mais depuis 2011, il est disponible sous une licence open source dans le cadre du projet open source WebRTC (Web Real-Time Communication est une interface de programmation Le but du WebRTC est de lier des applications comme la voix sur IP, le partage de fichiers en pair à pair.)[Ben14].

- iLBC Format de trame : Le nombre total d'octets utilisés pour décrire une trame de discours 20 ms est correspond 304 bits, qui s'inscrit en 38 octets et se traduit par un débit binaire de 15.20 kbit/s. Dans le cas d'une longueur de trame de discours de 30 ms, le total nombre de bits utilisés est 400, qui s'inscrit dans les 50 octets et se traduit par une débit binaire de 13,33 kbit/s. [Ben14] Dans la définition de bitstream, les bits sont répartis en trois classes selon leur erreur de bit ou perte sensibilité.
les bits plus sensibles (classe 1) sont d'abord placés dans,le bitstream pour chaque trame.
Les bits moins sensibles (classe 2) sont placés après les bits de classe 1.
Les bits moins sensibles (classe 3) sont placés à la fin du bitstream pour chaque trame.

Dans les cas de longueur de trame 20/30 ms pour chaque classe on a :

- les bits classe 1 occupent un total de 6/8 octets (48/64 bits).
- la classe 2 bits occupent 8/12 octets (64/96 bits) .
- la classe 3 bits occupent 24/30 octets (191/239 bits)

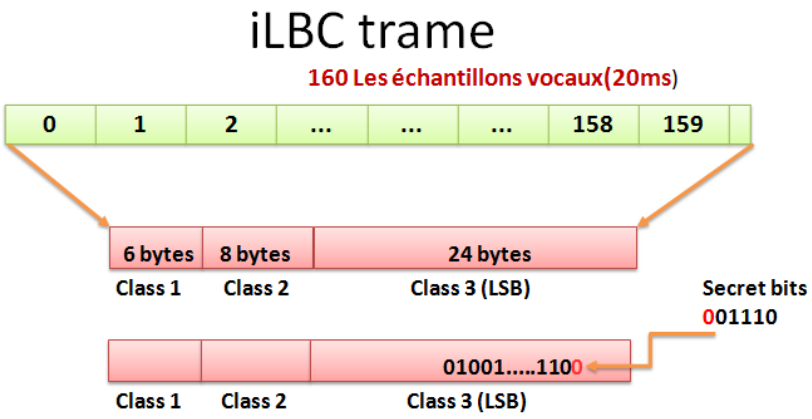


FIGURE 2.9 – iLBC trame 160 Les échantillons vocaux(20ms)

- Pourquoi choisir iLBC : iLBC trame ont été choisis en tant qu'objets de couverture en raison de plusieurs techniques appropriées et des raisons non techniques tels que :

- Les trames sont indépendantes, que ceci le rend parfait pour modifier certains ou la totalité des trames, puisque nous sommes sûr l'erreur introduite ne seront pas repropagées à les trames suivantes comme il est mentionné dans son mémoire descriptif [Lin04a].
- Bits de la trame sont classés, peu de catégories trois représentent le LSB comme décrit dans la spécification [Lin04a]. Il est facile pour nous pour savoir où se cache depuis les bits sont déjà classés. Google est derrière iLBC que Google pousse le codec à utiliser largement et il est déjà inclus dans certains de leurs produits comme Google Talk (Application de VOIP), Chrome (navigateur Web), Android (smartphone système d'exploitation), et WebRTC .
- Utilisation large en raison de ses fonctions, comme la qualité de la voix, débit faible,libre etc., iLBC est devenu largement utilisé dans de nombreuses applications de VOIP. [Ben14]

Stéganographie VOIP Stéganographie VOIP couvre un large éventail d'informations cachant des techniques, y compris les techniques populaires basées sur IP ou TCP et d'autres protocoles.

L'idée principale est d'utiliser des champs libres, redondantes ou inutilisés de ces protocoles. Il existe de nombreuses techniques qui pourraient servir à cacher des communications dans les différentes couches du trafic VOIP. L'un d'eux est en profitant des champs de données non utilisées ou rarement utilisées. [JL10b]

2.6 Terminologie :

- **Le medium de couverture ou la couverture-objet :** il s'agit du médium dans lequel seront dissimulées les informations. Il peut s'agir d'un texte, d'une image, d'un son, d'une vidéo, VOIP
- **Secret :** se sont les informations qui vont être cachées dans le médium de couverture. Il peut s'agir de n'importe quel type de données.
- **Stego-object ou stego-medium :** on appelle ainsi le médium de couverture après dissimulation des données à l'intérieur .
- **stéganogramme :** Message transmis confidentiellement dont la présence et la signification sont dissimulées à l'aide de techniques stéganographiques.
- **Steganalyse :** Steganalyse est l'art et la science de l'arrêt ou la détection de l'utilisation de toutes les techniques de stéganographie mentionnées plus tôt.

2.7 Conclusion :

En résumé, dans ce chapitre, on a essayé de fournir une vue générale sur la Stéganographie, de donner un aperçu sur les supports type stéganographie et leurs applications, nous pencher sur la notion la Stéganographie audio et VOIP en générale, et donner une vue globale sur la notion VOIP et son architecture. Puisque, méthode codec ILBC , et de présentes certaines descriptions détaillées des iLBC. Dans le chapitre suivant, en particulier dans Les méthodes connues de la stéganographie audio et nous envisagerons l'analyse détailles de la Stéganographie VOIP .

3

État de l'art de la stéganographie audio et VOIP

La propagation d'utilisation des données numériques de nombreuses applications dans la vie réelle ont exhorté des nouveaux moyens pour assurer leur sécurité, pour atteindre une secrète efficace en mettant en œuvre des techniques de steganograhie .On s'intéresse à étudier deux techniques VOIP stéganographie et audio. Stéganographique audio polyvalent méthodes ont été proposées. Les système stéganographique vise à obtenir de manière sûre et robuste pour dissimuler un taux élevé de données secrètes. VOIP stéganographie est un réseau en temps réel de la stéganographie, qui utilise des protocoles de VOIP et de la circulation comme un canal caché pour cacher des messages secrets. Récemment, il y a eu une augmentation notable dans l'intérêt de la stéganographie VOIP en raison du volume de trafic VOIP, qui s'est avéré rentable d'utiliser.

Nous nous concentrons dans ce chapitre sur la stéganographie audio numérique, qui est devenue une source importante de données se cachant dans les télécommunications comme la voix sur IP, cible et technologie de conférence audio, etc.. .Plusieurs critères de cacher l'information conduit à une grande variété de méthodes de conception du système. Nous discutons sur des défis de la stéganographie VOIP et certaines caractéristiques.

3.1 La stéganographie audio :

Pour cacher les fichiers de données en signaux audio comme vecteurs d'informations. Pratique de la dissimulation de renseignements est censée être une couverture qui sert à cacher les messages et ne doit pas déclencher toute suspicion d'opposants .
En fait, la disponibilité et la popularité des fichiers audio rendent admissibles à porter

des informations cachées. La plupart des efforts de steganalyse sont plus orientés vers des images numériques, laissant steganalyse audio relativement inexploré. Les données cachées dans des fichiers audio sont particulièrement difficiles en raison de la sensibilité des HAS. En plus, il y a certaines distorsions du signal, au point qu'ils seraient ignorées par les auditeurs dans la plupart des cas [FH11]. Ces propriétés ont amené les chercheurs à explorer l'utilisation des signaux audio comme transporteurs pour cacher des données . Les altérations des signaux audio pour fin d'incorporation de données peuvent affecter la qualité de ces signaux.

*** Le système de la stéganographie audio :** La stéganographie audio est représentée dans la Figure(3.1), l'expéditeur dissimule les données de n'importe quel type dans un fichier numérique de la couverture à l'aide d'une clé pour produire un fichier stego, de telle sorte qu'un observateur ne peut détecter l'existence du message caché .
A l'opposé, le récepteur traite le stego-fichier reçu pour extraire le message caché[DAMH12]. L'application d'un tel système de cacher un message secret à l'aide de la couverture de l'information du signal audio est sans danger, tels que les téléphones ou des conversations vidéo conférence [DAMH12].

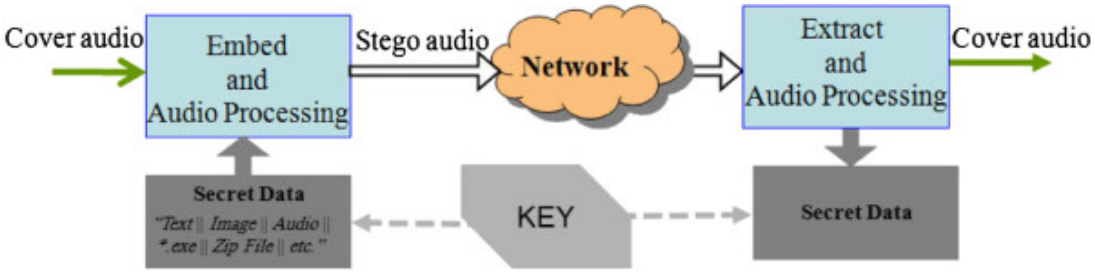


FIGURE 3.1 – Flux audio de la stéganographie [DAMH12] .

3.2 Méthodes de la stéganographie audio :

Présente quelques méthodes couramment employées pour cacher des informations secrètes en audio. Certaines de ces méthodes nécessitent des connaissances techniques de traitement du signal, analyse de Fourier et autres zones de niveau élevé en mathématiques. Lors du développement d'une méthode de dissimulation de données pour l'audio, l'une des premières considérations est les environnements probables que le signal sonore se rendra entre le codage et le décodage (sans chiffre et avec chiffrement).

- **Codage avec chiffrement :** est un processus qui cache le message dans l'audio.

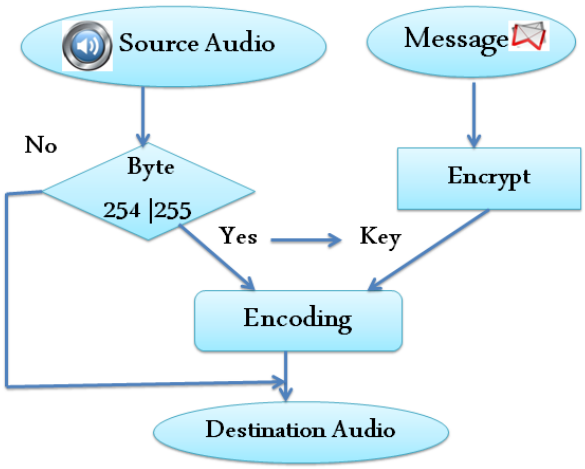


FIGURE 3.2 – Flux L'encodage audio.

- **Décodage avec déchiffrement :** est un processus de récupération de message de l'audio .

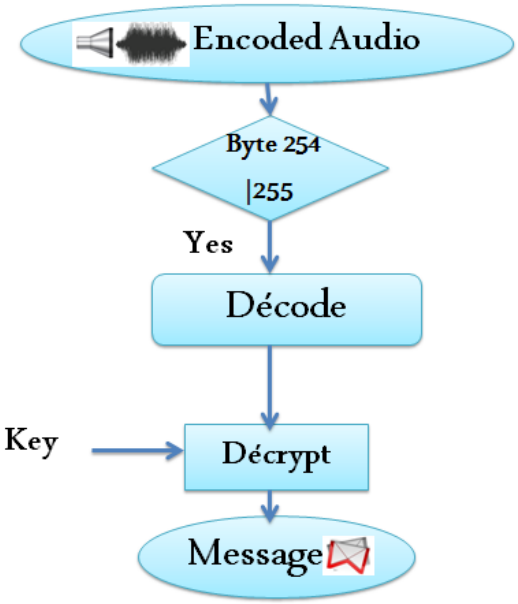


FIGURE 3.3 – Flux décodage audio.

Il existe plusieurs méthodes permettant d'ajouter des informations stéganographiques en fichiers audio .

3.2.1 Least Significant Bit :

LSB (Least Significant Bit)[PS11] est l'une des premières méthodes utilisées pour cacher plus d'informations. Il est basé sur la dissimulation de chaque bit du message dans le bit le moins significatif dans la couverture-objet (l'audio) d'une manière déterminante la Figure(3.4) comment le message « HEY » est codé dans un échantillon de qualité CD 16 bits à l'aide de la méthode LSB [PS11]. Voici de l'information secrète «HEY» consiste à dissimuler dans le fichier audio. Tout d'abord que les informations secrètes «HEY» et le fichier audio sont convertis en flux binaire. La colonne moins significative du fichier audio est remplacée par le flux de bits d'information secret « HEY ». Après la dissimulation des informations secrètes « HEY », le fichier obtenu est appelé Stego-fichier .

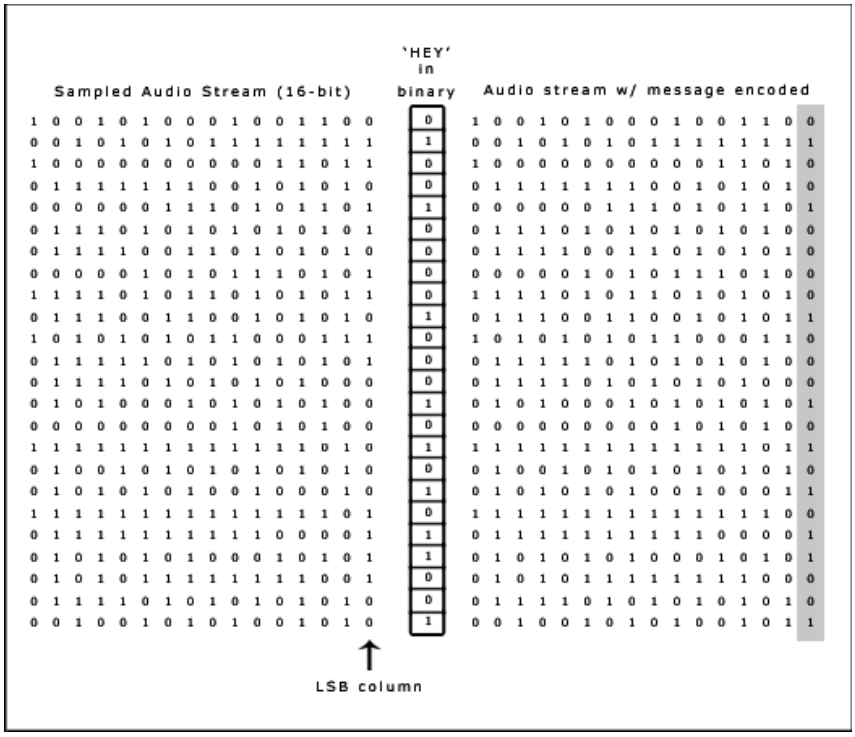


FIGURE 3.4 – Diagramme de LSB, processus de codage .

La méthode LSB permet l'encastrement de grande capacité pour les données 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 ajout de bruit qui réduit ses performances de sécurité puisqu'il devient vulnérable même aux attaques simples. Filtration, amplification, ajout de bruit et une compression de l'audio-stego détruira très probablement les données.

En plus, étant donné que les données sont dissimulées d'une manière très déterminante, un attaquant peut facilement découvrir le message en retirant simplement l'ensemble du plan LSB [Kha12]. Dans [Sep04] une stratégie simple de la LSB a été appliquée à dissimule un message vocal dans une communication sans fil. Bien que cette méthode permet d'obtenir l'imperceptibilité à dissimulation des taux élevés, la sécurité et la robustesse des données cachées sont facilement compromises. Dans une tentative d'augmenter la capacité de cacher tout en minimisant l'erreur sur stego l'audio.[Sep02]

Exemple : Si la valeur d'échantillon initial était de 4 qui est représentée en binaire par « 0100 », et le bit pour être caché dans la quatrième couche LSB est 1, au lieu d'avoir la valeur 12 = '1100' produite par l'algorithme LSB classique, le produit de l'algorithme propose un échantillon qui possède la valeur 3 = '0011', qui est beaucoup plus proche de la valeur d'échantillon initial(4) [Sep04].

3.2.2 Codage de la parité :

Codage de la parité[PS11], Au lieu de décomposer un signal en échantillons individuels, codage de la parité décompose un signal en régions distinctes d'échantillons et encode chaque bit du message secret dans le bit de parité de la région. Si le bit de parité, d'une zone sélectionnée ne correspond pas au bit secrète à encoder, le processus permet d'inverser le LSB de l'un des échantillons dans la région.

Ainsi, l'expéditeur a plus d'un choix dans le bit secret de codage, et le signal peut être modifié de manière plus discrète.

Le processus de décodage des extraits du message secret en calculant et en alignant les bits de parité des régions utilisées dans le processus de codage. Une fois de plus, l'expéditeur et le récepteur peuvent utiliser une clé secrète partagée comme une graine dans un générateur de nombres pseudo-aléatoires pour produire le même ensemble de régions de l'échantillon.[PS11]

En utilisant les trois premiers bits du message « HEY » est codé par le codage de la parité [Lu96] à La figure (3.5).

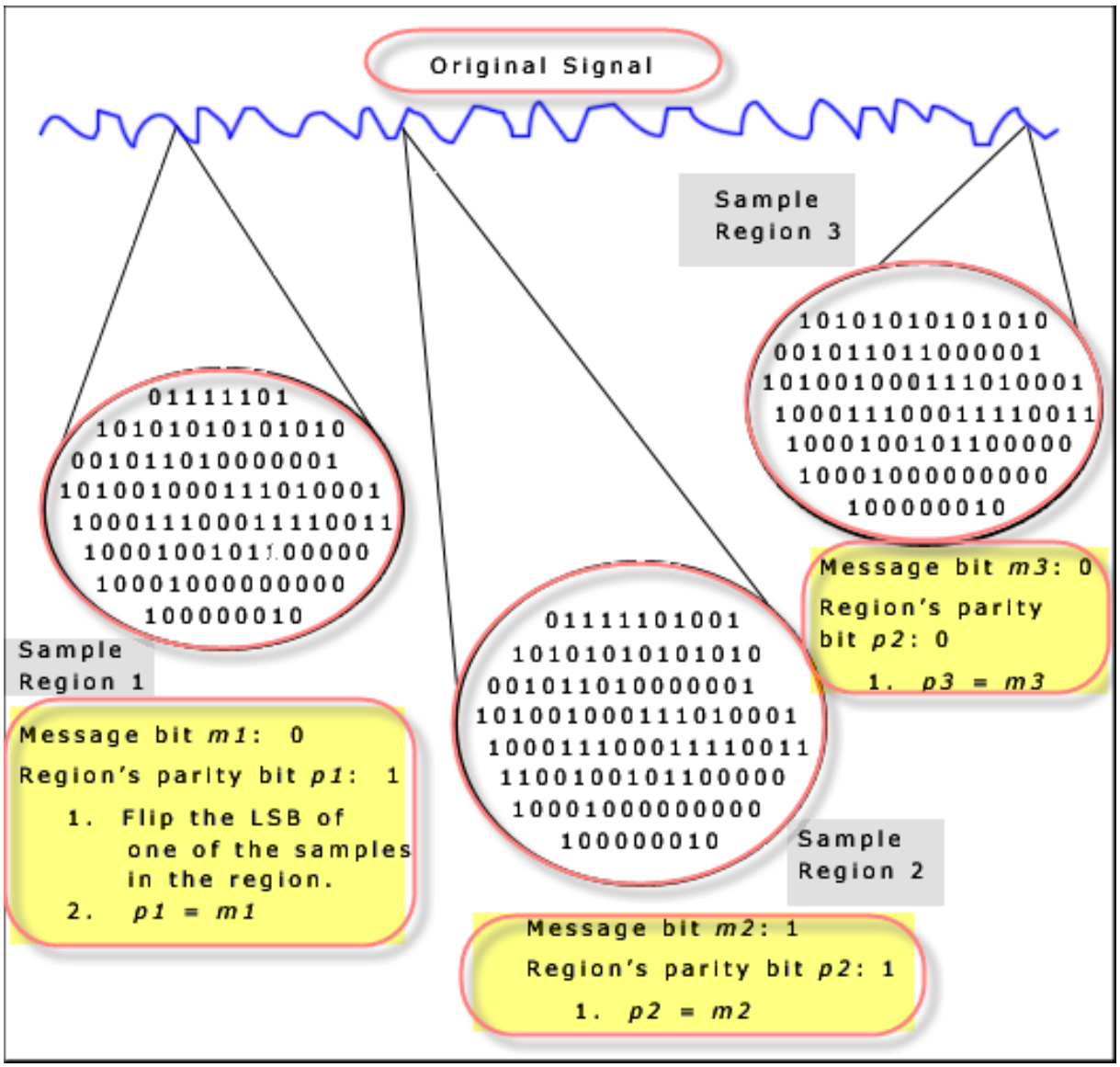


FIGURE 3.5 – Trois premiers bits du message ≪HEY ≫ est codé la par méthode de codage de la parité .

3.2.3 Étalement de spectre :

Dans [Lu96], la méthode steganographie audio de spectre (SS)[PS11] de propagation des informations secrètes à travers le spectre de fréquence du signal audio. Ceci est similaire au système utilisé le message du bit LSB qui s'étendait au hasard sur l'intégralité du fichier audio. Cependant, contrairement à la LSB codage, la méthode d'étalement du spectre propage les informations secrètes sur le spectre de fréquence du fichier audio à l'aide d'un code qui est indépendant du signal réel [Lu96]. Ainsi, le signal final occupe une largeur de bande qui est plus que ce qui est vraiment nécessaire pour la transmission. La méthode d'étalement du spectre est capable de contribuer à une meilleure performance

dans certains domaines par rapport à la LSB de codage. Codage de parité ce qu'il offre un taux de transfert moyen et haut niveau de robustesse contre les techniques d'épilation. Toutefois, la méthode d'étalement du spectre a un inconvénient principal, elle peut introduire des bruit dans un fichier audio [Lu96]. Les étapes de l'étalement du spectre sont indiquées à la Figure(3.6).

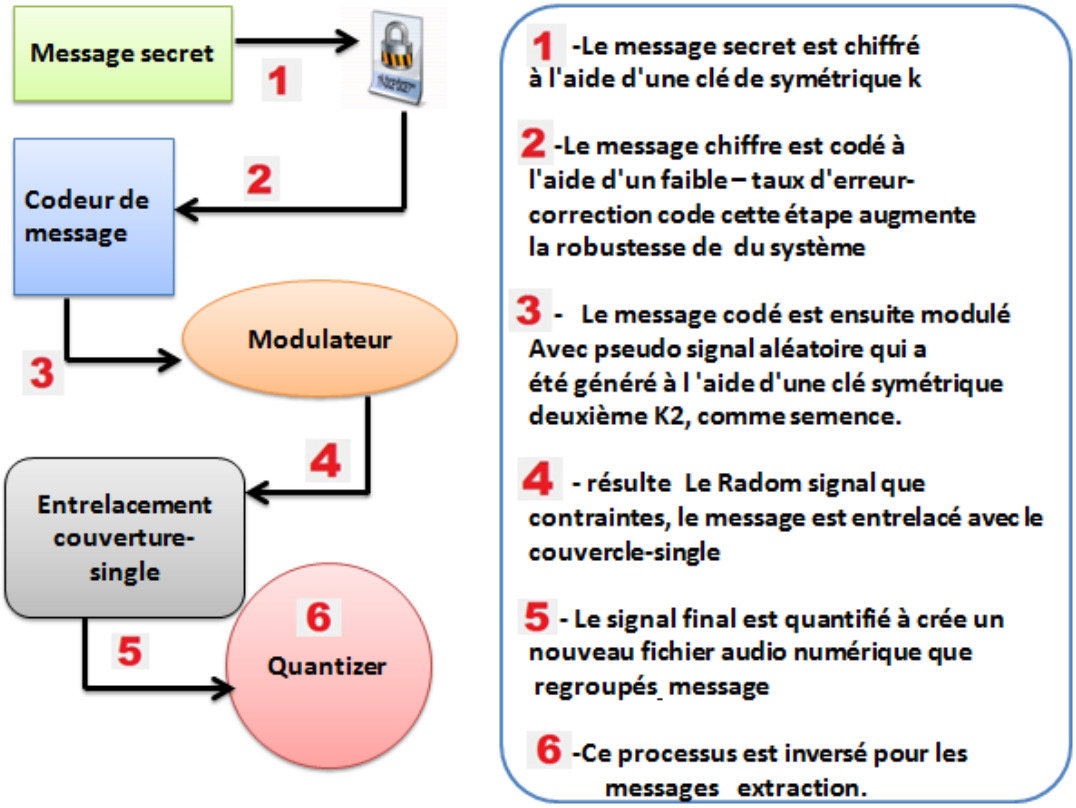


FIGURE 3.6 – Etalement de spectre (Spread Spectrum).

La méthode SS a le potentiel de meilleurs résultats dans certains domaines de la LSB de codage. Codage de la parité et codage de la phase sont des techniques qui fournissent des taux de transfert de données modérément tout en maintenant un haut niveau de robustesse. Toutefois, la méthode SS partage un inconvénient LSB avec de la codage parité qu'elle peut introduire des bruits dans un fichier audio.

3.3 Critères de comparaison :

Différents paramètres influencent la qualité des systèmes stéganographiques audio. En plus, la quantité des données cachées et son niveau d'imperceptibilité et robustesse contre la suppression ou la destruction de données dissimulées reste la propriété plus critique dans un système stéganographique. Les critères de robustesse sont évalués par l'intermédiaire de la survie des données cachées de bruit, de compression et de manipulations du signal audio (par exemple, filtrage, ré-échantillonnage, re-quantification). nous allons discuter des critères de comparaison choisis entre couverture-objet et les signaux stego. Nous nous concentrons uniquement sur les propriétés de ces méthodes qui ont été évaluées. Ces propriétés sont répertoriées comme suit[DAMH12] :

- **Taux de dissimulation :** mesuré en bits/s et se réfère à la quantité de données cachées (en bits) au sein d'un signal audio de la couverture et correctement extraite.
- **Imperceptibilité :** Ce concept est basé sur les propriétés de la HAS qui est mesurée au moyen de l'évaluation perceptuelle de qualité vocale (anglais : Perceptual Evaluation of Speech Quality, PESQ)(est un outil permettant d'évaluer la qualité de la voix transmise par un système de télécommunication).

  Les informations cachées sont imperceptibles si un écouteur est incapable de distinguer entre le signal audio et le signal de stego-audio. Le test PESQ produit une valeur comprise entre 4,5 et 1.

  Valeur PESQ 4,5 signifie que le discours mesuré n'a aucune déformation, c'est exactement la même que la Langue source.

  Une valeur de 1 indique la dégradation plus sévère.

  Une autre mesure qui est largement utilisée est le niveau de distorsion dans les signaux audio et il est capturé par le biais de SegSNR(segement de rapport signal sur bruit est un indicateur de la qualité de la transmission d'une information)[Mei10] Il est important que le processus de dissimulation s'effectue sans dégradation importante ou perte de la qualité perçue le signal de couverture.
- **Amplification :** Ce critère conduit à augmenter l'amplitude du signal audio qui pourrait altérer les données cachées, si une attaque malveillante est destinée.

- **Filtrage :** Malicieusement supprime les données cachées par la tronçonneuse la partie sélectionnée du spectre.[DAMH12]
- **Re-quantification :** Ce paramètre modifie la quantification initiale du signal audio. Par exemple, un signal audio 16 bits est quantifié à 8 bits et 16 bits à tenter de détruire les données cachées.
- **Ré-échantillonnage :** De la même façon que l'opération précédente, modifier la fréquence d'échantillonnage du signal audio à un autre, c'est-à-dire amplitude, signal audio large bande échantillonné à 16 kHz et 8 kHz et retour à 16 kHz.
- **Ajout de bruit :** Ajout de bruit au signal audio dans le but de détruire les données cachées,c'est-à-dire , WGN (White Gaussian Noise) un bruit blanc gaussien.
- **Codage/décodage :** Cette opération réduit la quantité de données en supprimant les informations inutiles ou redondantes. Ainsi, un message caché peut être complètement détruit. Ceci est également vrai si le fichier audio est converti en un autre format. Compression mp3, par exemple, modifie un fichier (.wav) à un fichier MP3 avant qu'elle atteigne le récepteur.
- **Transcodage :** C'est le processus de décodage du signal audio avec un décodeur qui est différent de celui utilisé dans l'opération de codage .

Par ces connaissances de base sur l'audio, et il y a beaucoup de données redondantes, ce qui facilite en quelque sorte à trouver des endroits pour cacher les données dans des fichiers audio et les paquets VOIP, l'idée de cette approche,c'est qu' on doit évaluer la recherche dans la VOIP qu'on va voir dans la section suivante.

3.4 La stéganographie de la VoIP :

VoIP est l'un des services du monde IP qui change le paysage des télécommunications ensemble. En raison de sa popularité, il devient une cible naturelle pour la stéganographie. Dans [ML12] ils proposent de nom stéganographique techniques appliqués à**"steganophony"** trafic VoIP. Ce terme, s'il est accepté, il se rapport aux renseignements cachés dans n'importe quelle couche de la pile de protocoles de TCP/IP Figure(3.7).

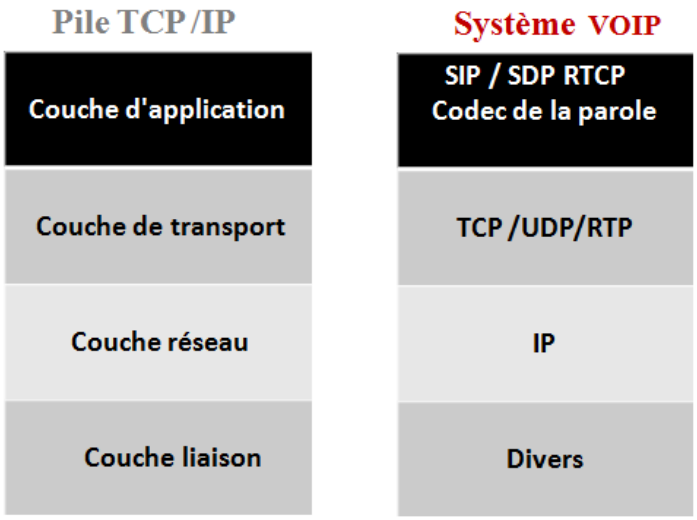


FIGURE 3.7 – Protocoles et pile VOIP [ML12] .

Pour les systèmes de VOIP, quatre scénarios possibles de communication cachée peuvent être considérés, comme à la figure(3.8) Le premier scénario 1 sur la figure(3.8) est le plus fréquent, l'expéditeur et le destinataire effectuent VOIP conversation lors de l'échange en même temps stéganogrammes [PS11]. Le chemin de la conversation est le même que le chemin d'accès de données cachées. Dans les trois scénarios (marqués 2, 3, 4)dans la figure(3.8) qu'une partie du chemin VOIP-to-end est utilisée pour une communication cachée à la suite de mesures prises par les nœuds intermédiaires, l'expéditeur et/ou le récepteur est en principe, pas au courant de l'échange de données sténographiques.

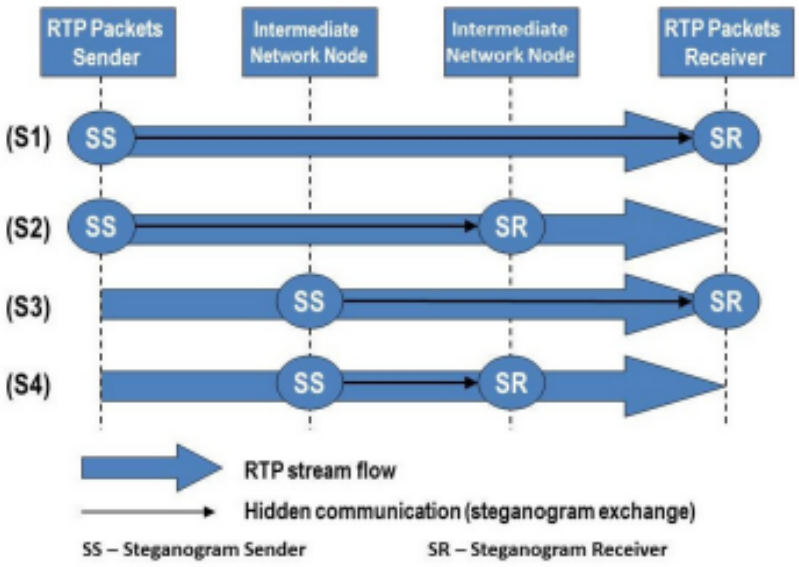


FIGURE 3.8 – Scénarios de communication cachée pour VOIP[PS11].

Donc, Steganophony peut-être classée en trois groupes figure (3.9)[PS11] :

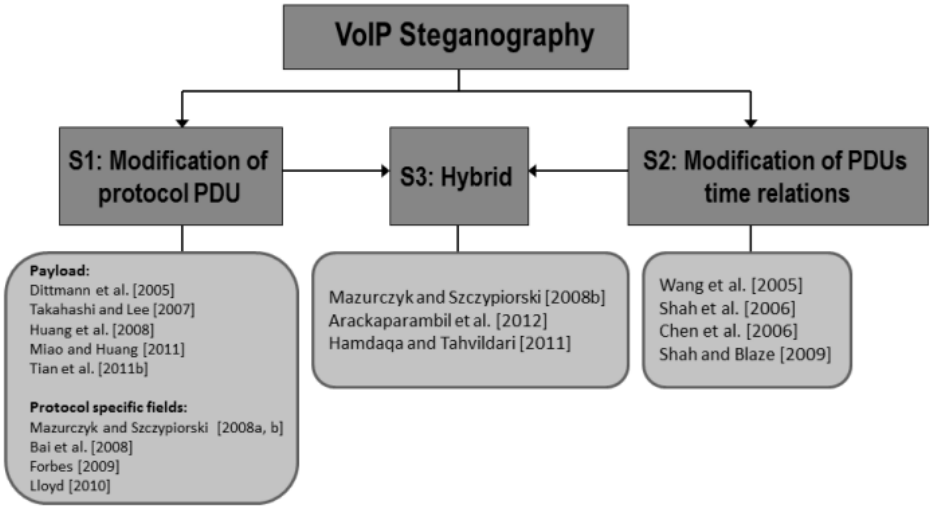


FIGURE 3.9 – Classification de sténographie VOIP avec des méthodes exemplaires [PS11].

(S1) Méthodes stéganographiques qui modifient les paquets les en-têtes de protocole réseau ou champs de charge utile.

(S2) Méthodes stéganographiques qui modifient les relations de temps des paquets, par exemple en agissant sur l'ordre de la séquence de Paquets RTP, modifiant leur retard inter-packet ou en introduisant des pertes intentionnelles.

(S3) Méthodes stéganographiques hybrides [ML12], qui modifient le contenu des paquets et leurs relations de temps. Un exemple d'une telle solution est la méthode LACK.[ML12]

Certains traits caractéristiques des méthodes de groupe S1 :

- Méthodes de stéganographie qui utilisent des champs spécifiques de protocole généralement donnent une capacité relativement élevée de stéganographie. Détection et mise en œuvre est relativement simple.

  Inconvénient : perte potentielle de certaines des fonctionnalités de protocoles.
- Méthodes stéganographiques qui utilisent généralement la charge utile des paquets rendement inférieur stéganographique capacité et sont plus difficiles à mettre en œuvre et à détecter.

  Inconvénient : la détérioration potentielle de la qualité de la voix.

Certains traits caractéristiques des méthodes de groupe S2 :

- Expéditeur-destinataire de synchronisation requise.
- La stéganographie a une faible capacité et plus difficile à détecter que dans le cas des méthodes qui utilisent le protocole domaines spécifiques.
- Mise en œuvre simple.

Inconvénient : éventuelle détérioration de la qualité de conversation.

Caractéristiques des méthodes de groupe S3 : Méthodes hybrides de la stéganographie du groupe S3 peuvent s'appliquer à toutes les modifications utilisées par les méthodes de groupe S1 et S2. Un exemple de méthodes hybrides LACK [ML12] est basée sur la modification du contenu des paquets et dépendance de leur temps.

3.5 La technique de la stéganographie VOIP base sur la méthode LSB :

Étonnamment, beaucoup d'efforts de recherche sont toujours dévoués pour améliorer la LSB. il faut noter que technique peuvent être appliquée avec succès également aux autre VOIP méthodes de la stéganographie pour augmenter leur indétectabilité, robustesse ou stéganographique bande passante. Liu et al. en 2012 [LIU12] ont adopté moins bits significatifs LSB pour cacher le secret donné. Cette approche peut augmenter d'environ 30 % de la bande passante de la stéganographie tout en présentant le moindre coût de stéganographique que la méthode classique de LSB.
[Ben14]Les dernières recherches à proposées la nouvelle technique pour cacher l'information dans VOIP, nous encouragent de choisir cet axe, et sera permis d'ajouter certaines techniques. Notre méthode est semblable aux méthodes LSB déjà connues. (Il utilise les frames d'iLBC en tant qu'objets de la couverture).

3.6 Conclusion :

En conclusion, la stéganographie est une méthode efficace et fascinante de cacher des données qui ont été utilisées tout au long de l'histoire. Stéganographie audio en particulier résout les problèmes clés provoqués par la nécessité d'un système de communication sécurisé qui peut garder le secret des informations transmises, même lors du passage par le

biais de canaux de l'insécurité. Bien qu'en temps réel, notamment VOIP, la stéganographie est relativement compliqué, les précédentes recherches et les études ont facilité la mission pour trouver les techniques plus adaptées, pratiques et efficaces pour mettre en œuvre une technique de stéganographie VOIP avec capacité maximale.

En raison du manque de recherches et d'études, les possibilités d'améliorer l'actuel et les nouvelless techniques libérées de stéganographie VOIP qui consiste à améliorer la capacité de discussion, il faudrait une étude afin de déterminer la meilleure méthode de modèle en temps réel de la stéganographie pour VOIP qui fournit la bonne sécurité et la capacité de stockage sans sacrifier les performances en temps réel.

Cet objectif pourrait être atteint en utilisant des approches bien conçues pour fournir un compromis raisonnable entre l'information adéquate se cachant l'exigence (bonne sécurité et une capacité suffisante). Et bien cela sera détaillé dans le chapitre suivant.

4

L'implémentation de La technique Proposée

Fournir des méthodes et des techniques pour masquer les données dans un milieu très populaire comme VOIP est un objectif difficile. Il est évident qu'il y a des limites sur la quantité de données secrètes qui devraient être couvert dans la VOIP sans affecter le flux global de la voix au cours de l'appel VOIP. Le fait qu'il y ait des limites sur le taux de données secrètes rend plus difficile d'introduire des techniques sûres et pratiques qui offrent le plus grand taux de données entrave.

Ce chapitre fournit une technique, qui va être réalisé selon le procédé tel qu'il est illustré à la figure(4.1) . La procédure d'analyse et de l'implémentation de cette technique est divisée en trois phases. Tout d'abord, l'analyse de technique de la stéganographie VOIP proposée. Deuxièmement, l'implémentation et les testes. Enfin, suggérer de renforcer des capacités dans ce domaine de recherche.
Chaque phase à sa propre activité qui sera expliquée dans les sections suivantes :

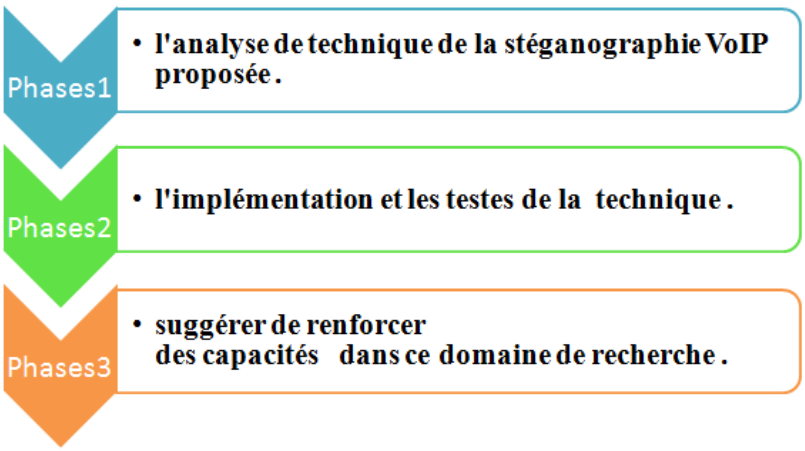


FIGURE 4.1 – Phases d'analyse et de l'implémentation de technique.

4.1 Technique proposée :

nous commençons à décrire les bases de notre méthode,l'iLBC stocke les bits les moins significatifs de la trame ILBC en niveau de classe 3.

Notre technique est basée sur la technique Mr. Mohamed Lahcen Bensaad en Mars 2014 qui est basée sur la modification des bits de cette classe dans tout ou une partie des trames pour cacher des données [Ben14].

Etant donné que nous changeons seulement les bits les moins significatifs, ce changement ne devrait pas affecter la qualité du signal et la différence devrait être inaudible. Parce que les trames sont indépendantes, l'erreur introduite ne se propage pas.

Pour augmenter la sécurité de notre méthode, nous pouvons choisir pour ne pas cacher des bits dans chaque trame, mais seulement dans quelques trames sélectionnées.

Ces trames sélectionnées peuvent être choisies à l'aide d'un PRNG (Pseudo Random Number Generator) qui génère les numéros de séquence des trames à utiliser, en plus pour augmenter la sécurité on doit utiliser un autre Générateur limité qui génére les numéros de séquence bits de la classe 3 bits occupés 24/30 octets (191/239 bits), pour cacher le côté réception on doit également utiliser les mêmes générateurs pour trouver les numéros de séquence des trames stego et les séquences des bits stego pour extraire les données de leur part.

Au niveau du récepteur, on exécute la procédure avec l'extraction des données, la question qui se pose, quelle est la condition d'arrêt de cette procédure ? Pour répondre à cette question, on va ajouter à la méthode précédente :

* Envoyer la longueur de donnée secrète.
* Commencer par les données secrètes .
* Utiliser un générateur aléatoire pour les bits cachés.
* l'extraction de la taille de données secrètes avant l'extraction de la donnée secrète.

4.2 Description de la technique :

L'architecture générale de la technique de stéganographie VOIP est illustrée à la figure(4.3). Chaque donnée secrète transmise au cours de l'appel VOIP sera traitée et intégrée selon cette architecture.

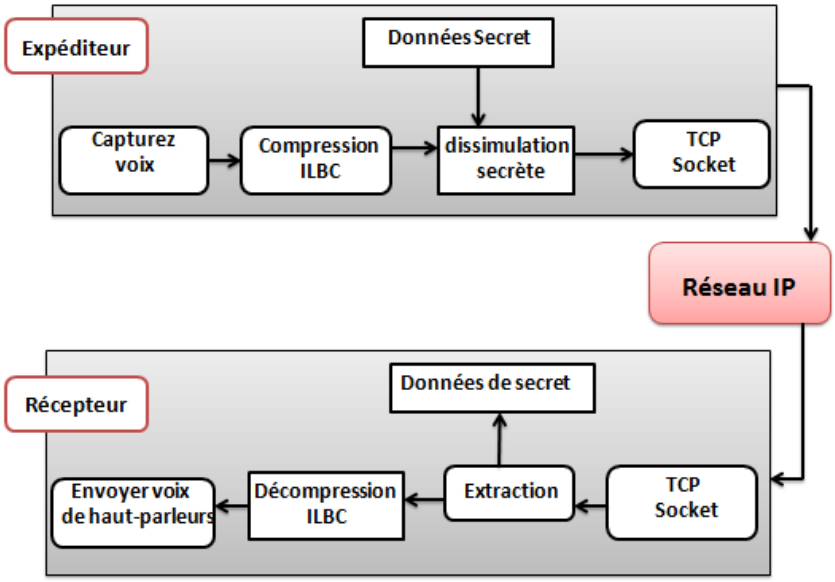


FIGURE 4.2 – Architecture Général de la technique .

On veut détailler les procédures au niveau d'expéditeur lorsqu'il veut envoyer une donnée secrète à la figure (4.3), même chose au niveau de la récepteur, quand il veut recevoir une donnée stego à la figure (4.10) .

4.2.1 Les procédures au niveau expéditeur :

1 : choisir le type des données secrètes (image, texte, vidéo)..

2 : Calculer la taille des données .

3 : Convertir les données secrètes en flux binaire (1010101.....).

4 : Lancer le générateur pour définir la séquence des trames stego pour cacher des données secrètes .

5 : Capture d'une voix.

6 : Compression de la voix à l'aide de ILBC .

7 : Dans cette étape, on sélectionne les paquets qui sont identifiés par les mêmes valeurs du générateur.

8 : Envoi premièrement les bits qui correspondent à la taille de données Secrétes.

9 : Dans cette étape on envoi la séquence des bits secréts par des paquets stego, qui sont sélectionnés à l'aide de générateur.

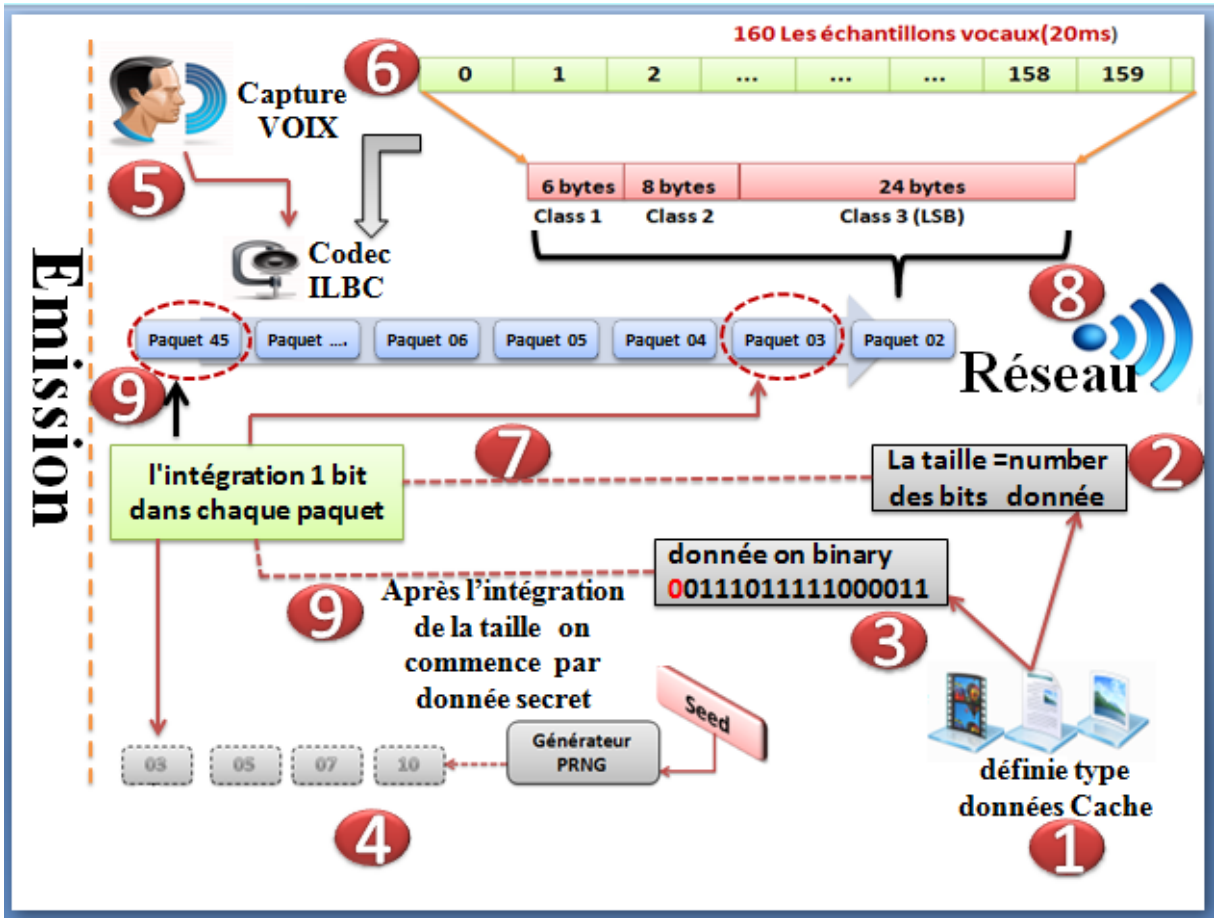


FIGURE 4.3 – Les procédures au niveau expéditeur.

4.2.2 Les procédures au niveau réception :

1 : Lancer le générateur pour définir la séquence des trames stego pour extraire les données secrètes .

2 : Recevoir la voix .

3 : Commencer à extraire la taille de donnée secret (c'est-à dire en extraire un bit pour chaque paquet stego jusqu'à 32 bits)

4 : Décompression ILBC .

5 : Convertir le sequence des bits de la taille on entier .

6 : Commencer a extraire les données secrètes.

7 : Collection des bits secrètes .

8 : Exécuter le procédure couverte vers type de la donnée .

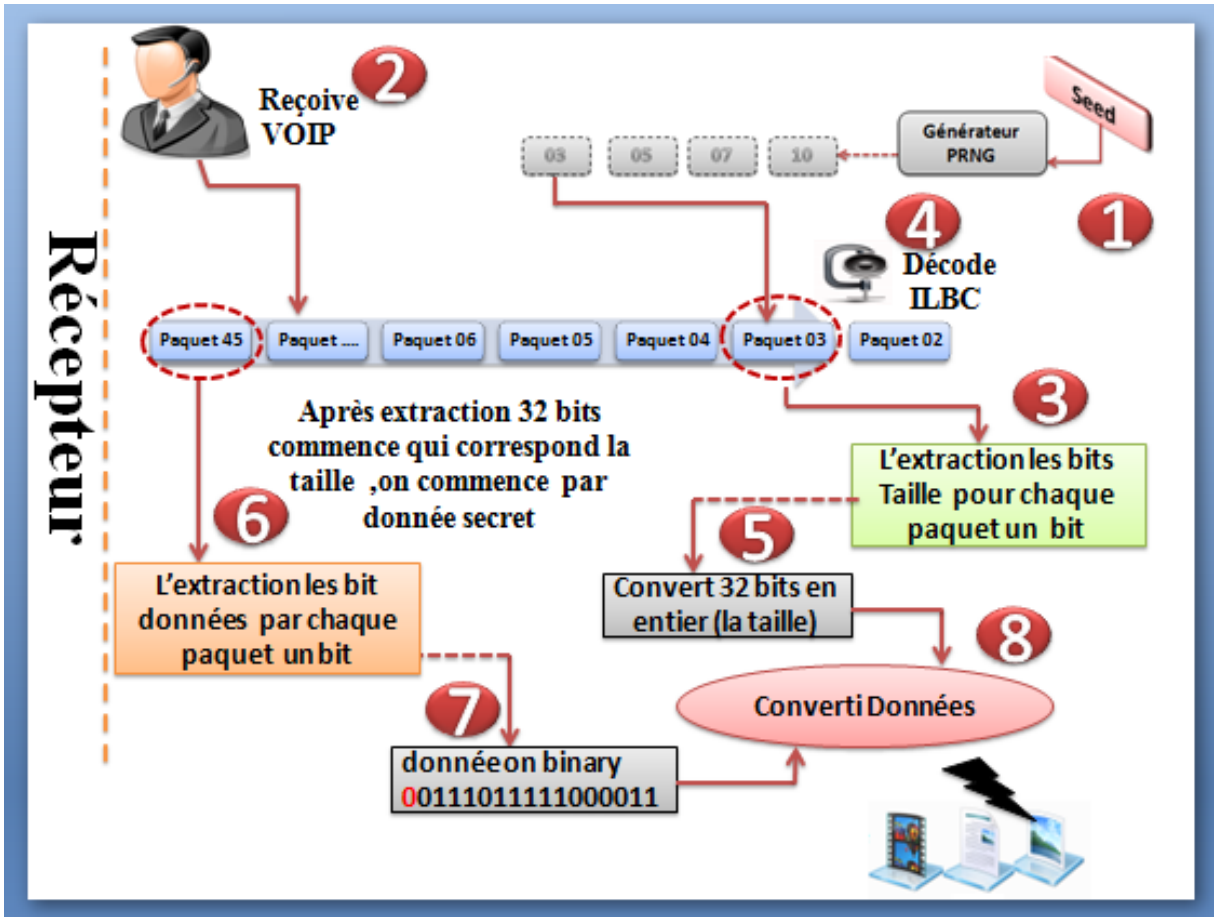


FIGURE 4.4 – Les procédures au niveau Récepteur .

4.2.3 Procédure appel VOIP :

Au début de la construction de la technique de stéganographie VOIP, il est évident que nous devons commencer avec la mise en œuvre appel VoIP. Il existe plusieurs façons de mettre en œuvre un appel VOIP, les plus connus sont client-serveur et point à point basés. L'appel VOIP dans cette technique se compose de trois étapes : initialisation d'appel, effectuant la conversation et mettre fin à l'appel à la figure(4.9).

Chacune de ces étapes à ses propres messages qui sont transférés entre l'expéditeur et le récepteur. Les sections suivantes décrivent ces étapes en détails.

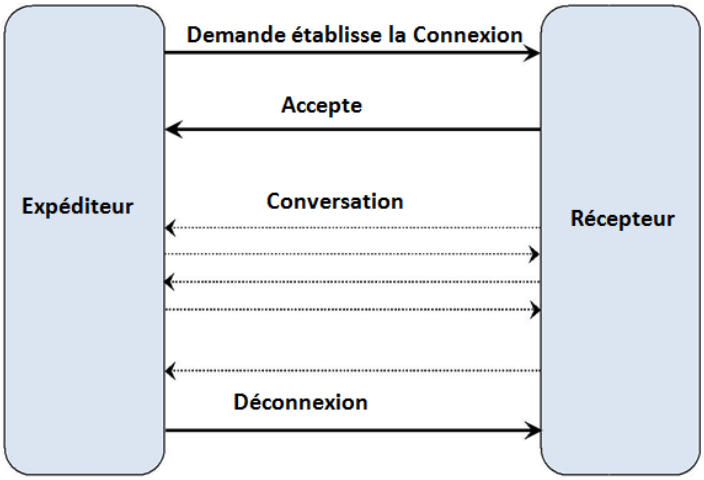


FIGURE 4.5 – Procédure d'appel VOIP.

*** Initialiser appel VOIP :**

L'initialisation de VOIP appel commence lorsqu'un point de terminaison (l'expéditeur) Envoie une demande établie d'une connexion à l'autre extrémité (le récepteur) à l'aide de l'adresse IP du destinataire. L'autre extrémité reçoit ce message de demande et au choix soit d'accepter cette connexion ou ne pas accepter comme elle est illustrée à la figure(4.9). Dans le cas où le récepteur n'accepte pas la connexion, un message d'état occupé sera transféré à l'expéditeur qui prendra une fin à la session d'appel en conséquence.
Si le récepteur accepte la connexion ,l'étape d'initialisation est faite et les deux parties débutera la prochaine (conversation).

*** Conversation VOIP :**

Il s'agit de l'appel VOIP réel dans lequel la voix et données incorporées seront transférés. Après un message OK étant renvoyé à l'expéditeur, les deux parties commenceront à envoyer et recevoir simultanément les signaux vocaux entre eux. Dans ce technique, cela fait à l'aide de multi-thread. Deux threads dédiés (envoyer et recevoir) sont conçus pour accomplir la conversation bidirectionnelle simultanée.

-Thread " Envoyer " : Le thread « Envoyer » servira à envoyer des signaux vocaux à l'autre extrémité par les deux points de terminaison. Figure(4.6) montre les tâches du thread « Envoyer » qui sont :

- Capturer des signaux vocaux du microphone et leur prélèvement dans les codes PCM. Cette tâche est effectuée à l'aide de Microsoft Direct Sound.
- Compresser les échantillons de voix PCM 8 kHz/16 bits (160 échantillons pour trames de 20 ms, 240 échantillons de trames de 30 ms) d'algorithme de codec ILBC audio. Cette étape se fait automatiquement.
- Dans le cas des dissimulation des données secrètes à l'intérieur des échantillons de voix, la menace de « Envoyer » pour cela, à l'aide d'une fonction séparée d'encastrement.
- Paquets voix données en paquets TCP et envoyez-les au récepteur.

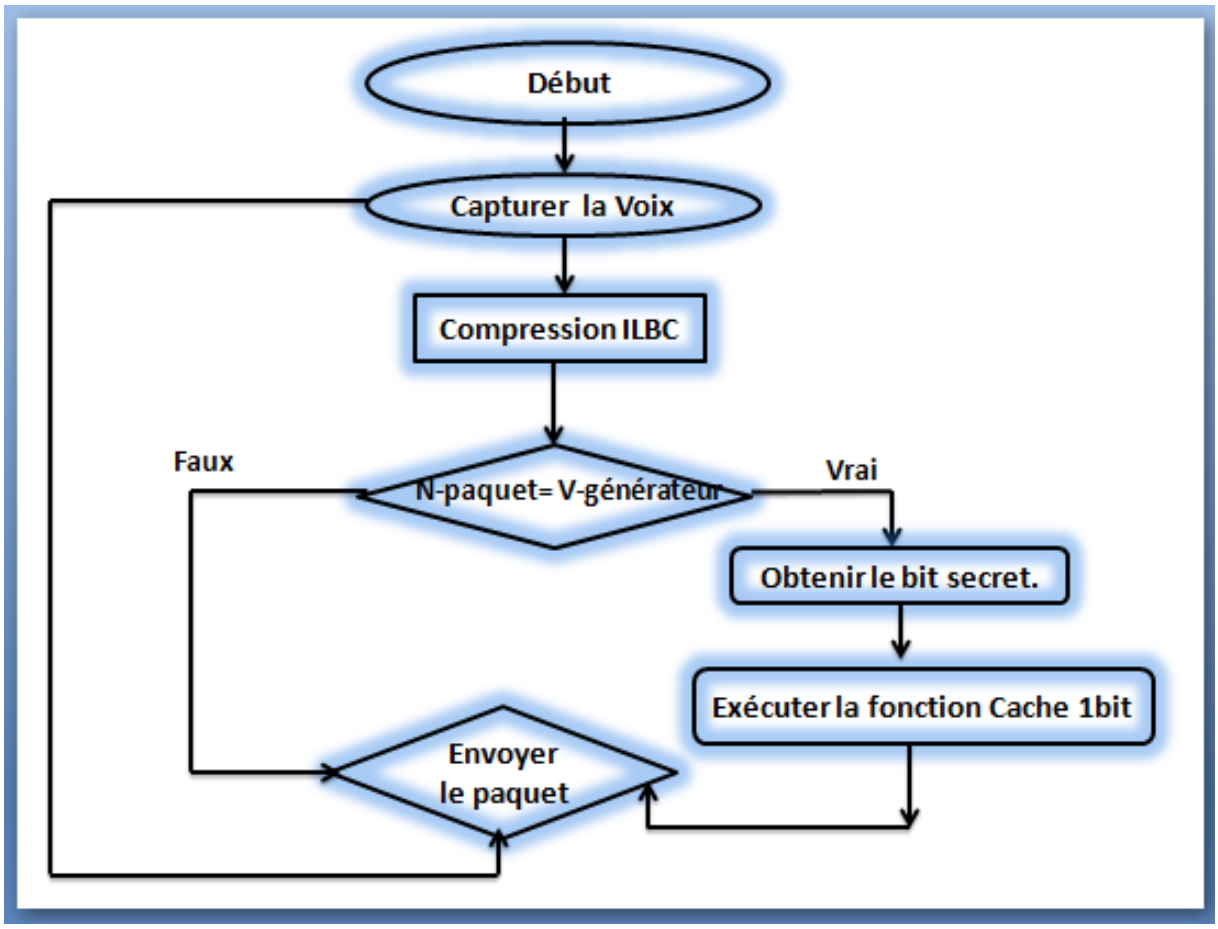


FIGURE 4.6 – Organigramme de la thread « Envoyer »

les mots clés :**N-paquet :**numéro de paquet . **V-générateur :** valeur de générateur.

- Thread " recevoir " : Tout comme le thread « Envoyer », le fil de « Recevoir » serviront par les deux points de terminaison pour recevoir les signaux de voix de l'autre point de fin. Par défaut, l'opération et ordre de « Recevoir » thread sera au contraire ceux du

thread « Envoyer ». Figure 4.7 affiche les tâches du thread « Receive » qui sont :

- Recevoir des paquets TCP provenant de cet expéditeur et extraire les données de voix.
- S'il y a des données cachées, incorporées à l'intérieur des voix-données, le fil de « Recevoir » extrait des données cachées à l'aide d'une fonction d'extraction séparée.
- Décompressez les ILBC données reçus dans des échantillons de voix PCM 16 bits à l'aide d'algorithme de codec audio ILBC. Cette étape est également faite manuellement sans l'aide du codec lui-même.
- Régénérer les signaux audio de données vocales et envoyez les aux enceintes. Cette tâche est effectuée à l'aide de Microsoft DirectSound. En attendant, les données extraites cachées (le cas échéant) seront affichées sur l'interface graphique du récepteur.

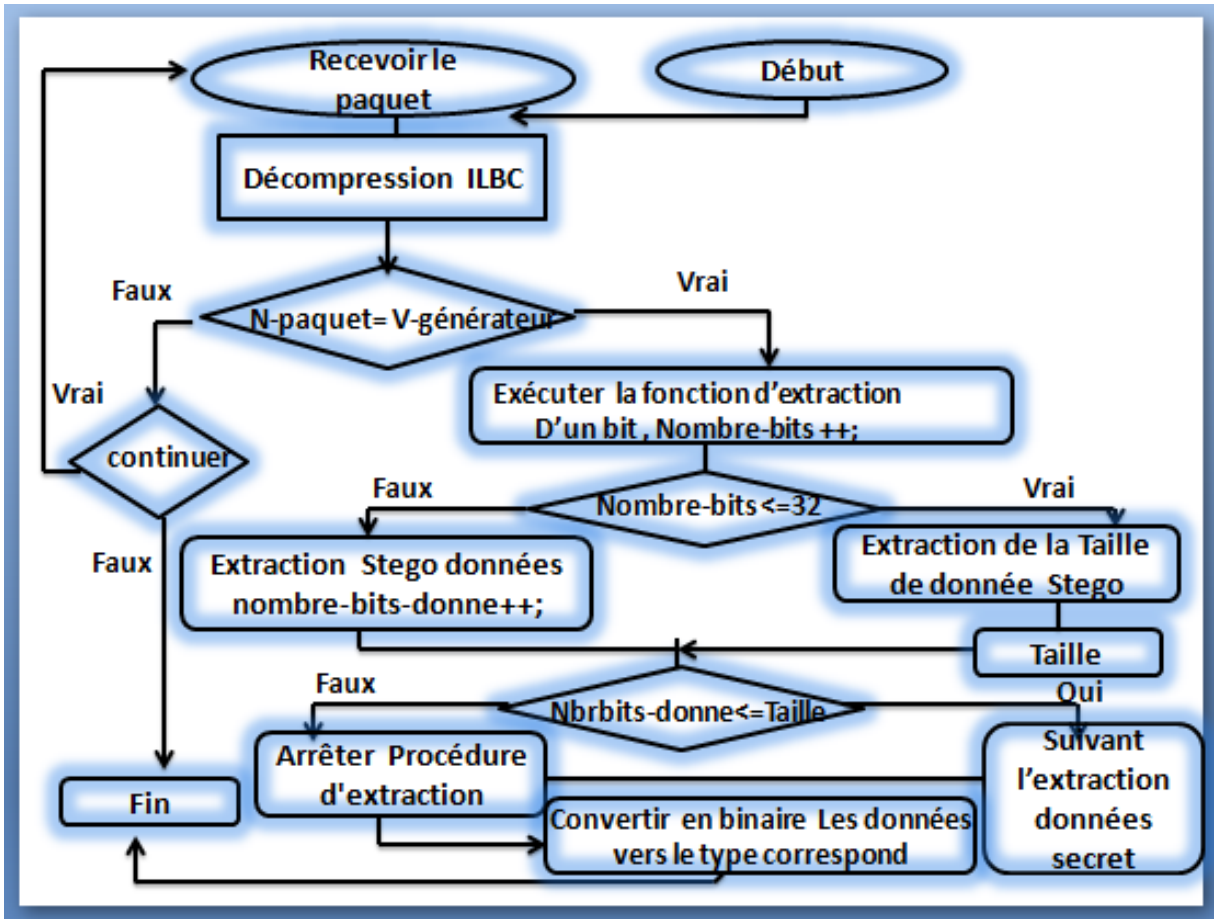


FIGURE 4.7 – Organigramme de la Thread de « Recevoir » .

*** Terminant appel VOIP :**

Lorsqu'une des parties communicantes Appuyez sur le bouton « Raccrocher » dans l'interface utilisateur, un message sera envoyé à l'autre partie, ce qui signifie que l'appel VOIP doit s'arrêter.

4.3 l'implémentation de la technique :

on a déjà vu les quatre scénarios de la communication cachée de la VOIP dans le chapitre précédent pour cela on va implémenter la technique proposée qui est basée sur le premier scénario à la figure (3.8).

4.3.1 Dissimulation et Extraction des données secrètes :

Les techniques utilisées pour intégrer des données dans les flux de la VOIP sont des variantes de LSB stéganographie et méthode codec ILBC ces dernière sont très importantes pour la classification de la structure qui permet la facilite de classe les bits moins significatifs, le changement de bits signifie une erreur de codec signifie. Bien que cette méthode soit la façon la plus simple de cacher des données sur n'importe quel support et échoue contre de nombreuses attaques et techniques de stéganalyse, il est une technique efficace et pratique pour être utilisée dans un tel simple approche .

*** Processus de dissimulation :**

Cette fonction est le responsable de cacher des données en données de signal vocal. Il incorpore des données à l'aide de la méthode LSB de codec ilbc et deux Générateur aléatoire .(1) -Générateur spécifier la séquence de paquet stego . (2) -Générateur spécifier le séquencé de bits stego .
n'oublie pas la taille de données secrètes qu'on envoie d'abord , avant les données cette fonction travaille selon l'algorithme suivant :

Étape 1 : Spécification des données secrétés et la taille de ces données et convertir en un tableau de bits(tabBit).

Étape 2 : Spécification des deux générateurs (1 : paquet stego no limite en tableau A1) et (2 : la localisation des bits stego limite entre 112 bits et 192 bits en tableau A2).

Étape 3 : Capture de la voix et compression par ILBC .

Étape 4 : Obtenir des couverts données secrètes l'aide Condition Si l'identifiant de paquet capture égale à la valeur du générateur des paquets .

Étape 5 : Spécification de la localisation des bits cachés au niveau de classe 3 de codec ILBC(localisation des bits cachés).

Étape 6 : Insérez 1 bit du tableau de donné secrètes en localisation des bits de l'octet du tableau de données de la voix.

Étape 7 : Incrémenter les index de A1 et A2.

Étape 8 : Répétez l'étape(4 ,5,6,7)jusqu'à la fin de l'A1.

le code suivant, il bien explique cette fonctionnalité .

Listing 4.1– Procédure de l'intégration données secrètes

```
// "1: Génerateur : spécifier les paquets Stego".
1.   A1=audio.getValueTrame();
// "2 : Génerateur : spécifier les Bits Stego".
2.   A2=audio.getValuBits();
//"3: spécifier le données secret et en convert en flux binaire".
3.   tabBit= audio.encodeleght();
4.     while (!socket.isClosed()){
5.             try {
6.      Thread.sleep(20);
7.      if(audio.isRecording()){
      //" Numero  de paquet Courant "
8.        isCapture ++;
     //" Caputre Voix "
9.        audio.capture(encdataI);
       //" test si Numero Paquet=Paquet-stego "
10.           while(isCapture==A1[indexPaStego]){
11.     //"Obtenir bits cache "
12.             bitEmbedded=tabBit[indexbits];
13.             System.out.println( "Le bits cache  :"+ A2[indexbits]);
       //"Exécute la fonction cache d'un seul bit"
14.             hiddingBit(encdataI,A2[indexbits],bitEmbedded);
      //" l'incrémentation des index de A1 et A2".
15.             indexbits++; indexPaStego++;
16.             System.out.println("Le bit cacher :" + bitEmbedded + " dans le  " +
    encdataI + "N° Paquet " + isCapture);
17.
18.           }
19.
20.      out.write(encdataI);
21.      out.flush();
22.      System.out.println( " N° Paquet  envoyer    :" + isCapture);
23.     }
24.     }
25.             catch (Exception e) {
26.     System.out.println(" problèmes parce que dépasse de capture en 20 ms ")
27.           }
28.
29.       }
```

Pour le fonction **hiddingBit** c'est-à-dire "cacher un bit" on donne leur code suivant .

Listing 4.2– Procédure de cache un bit de données secrètes

```
1. public byte hiddingBit(byte[] encdata, int pos, int val) {
2.    int posByte = pos/8;
3.    int posBit = pos%8;
4.    byte oldByte = encdata[posByte];
5.      System.out.println("oldbit "+oldByte);
6.         oldByte = (byte) (((0xFF7F>>posBit) & oldByte) & 0x00FF);
7.     System.out.println("newbit "+oldByte);
8.          byte newByte = (byte) ((val<<(8-(posBit+1))) | oldByte);
9.            encdata[posByte] = newByte;
10.      return newByte ;
11.      }
```

*** Processus d'extraction :**

Cette fonction est le responsable de l'extraction des données secrètes les données de signal de voix reçues. cette fonction travaille selon l'algorithme suivant :

Étape 1 : Spécifier du même Générateur (1 : paquet stego en tableau A1) et (2 : la localisation des bits stego en tableau A2).

Étape 2 : Obtenir le signal vocal reçu et Décompression par ILBC .

Étape 3 : Obtenir des couverts de données secrètes stego à l'aide de Condition Si l'identifiant de paquet reçu égale à la valeur du générateur paquet .

Étape 4 : Spécification de la localisation du bit caché au niveau de classe 3 de codec ILBC localisation des bits .

Étape 5 : Extraire un bit le LSB d'un octet du tableau de données de voix et l'enregistrer dans un tableau de bits A3.

Étape 6 : Incrémenter les index de A1,A2.A3,nombre de bits, taille.

Étape 7 : Répétez l'étape (3,4,5,6,7) jusqu'à la Condition (nombre bits taille inférieur ou égal à 32).

Étape 8 : si(nombre bits taille = 32) convertir 32 bits en interger pour definir la taille de donnée.

Étape 9 : Obtenir des couverts de données secrètes stego Condition méme condition étape 3 .

Étape 10 : Extraire LSB d'un bit du tableau de données de voix et l'enregistrer dans un tableau de bits A4

Étape 11 : Incrémenter les index de A1,A2,A4 le nombre des bits extraits .

Étape 12 : Répétez l'étape (5,6,7) jusqu'à la Condition (numbre bits ¡= la taille).

Étape 13 : Si (nombre bits = la taille)on convertie la données extraites vers le type concerné .

Listing 4.3– Processus d'extraction données secrètes

```
1.  while ( !socket.isClosed() ) {
2.            try {
3.                Thread.sleep(2);
4.                in.read(encdata, 0, encdata.length);
5.         if (audio.isPlaying()) {
         //"Numero paquet Courant"
6.              it++;
         // "le signal vocal reçu"
7.              audio.play(encdata);
          //"test si Numero Paquet=Paquet-stego"
8.              if (it==A1[indexPaqS]){
9.    System.out.println( " Localisation de Le bits extraire:"+A2[indexBitS]);
10.                    nbrbits++;//nombre des bits extraire
//"***** Execute les procedures  de l'extraction les bits de la taille*****"//
11.                 if (nbrbits<=32){//"La condition pour atteindre le taille"
12.               bits=ExtractBit(encdata,A2[indexBitS]); //extraire 1 bits
13. System.out.println( " le bit obtenu   " + bits+" à data" + encdata + "Paquet
    stego N° :"+ it);
14.              //"On collecte les bits dans une tableau "
15.        seqBit=CollectionBits();
       //" l'incrémentation des index de A1 et A2 ".
16.               indexPaqS++;indexBitS++;
           // " déterminer la taille "
17.               if (nbrbits==32){
18.               taille = Integer.parseInt(seqBit,2);
19.               System.out.println(" La taille de donnée: "+taille);
20.                }
21.              }
//"******Exécuter les procédures d'extraction des données secrètes********"//
22.                        else if(nbrbits>32){
23.                            nbrbitstxt++;
24.                        if (nbrbitstxt<=taille){
                  //"obtenue le bits secret"
25.                 bits=ExtractBit(encdata,A2[indexBitS]);
    // "on organise les bits pour chaque 7 bits par 1 seul caractère"
26.                 organisation-bits(bits);
       // "l'incrémentation des index de A1 et A2"
27.               indexPaqS++;indexBitS++;
 //"la condition d'arrét la procédé de l'extraction "
28.                 if (nbrbitstxt==taille){
29.                     txt = Convert-bits-to-data(bits);
30.                   System.out.println( "La texte  :"+ txt);
31.                   }}
32.                      }
33.
34.                      }
35.
38.               System.out.println( "Paquet  recivie N° :"+ it);
39.                    }
40.            }catch (Exception e) {
     System.out.println(" problèmes parce que dépasse de recevoir en 20 ms ")
41.               }
42      }
```

Pour le fonction **ExtractBit** c'est-à-dire "d'extraction d'un bit" on donne leur code suivant .

Listing 4.4– Processus d'extraction un bit des données Secret

```
1.  public  int ExtractBit(byte[] data, int pos){
2.      int posByte = pos/8;
3.      int posBit = pos%8;
4.      byte valByte = data[posByte];
5.      int valInt = valByte>>(8-(posBit+1)) & 0x0001;
6.      System.out.println("bits is extect "+valInt);
7.      return valInt;
8.   }
```

4.3.2 Scénarios d'exécution :

Les étapes à suivre dans l'application :

1 : On commence par l'établissement de connexion.

FIGURE 4.8 – Établissement de connexion

2 : Commencer la conversation entre l'éxpéditeur et le récepteur en exécutant les deux procédures dissimulation et extraction. Au niveau expéditeur on clique sur le bouton caché exécute les procédures de la dissimulation de texte écrit dans de champ textes cachés. Au niveau récepteur on clique sur le bouton extraire qui doit lancer les procédures d'extraction text et affiche dans champ concerné .

FIGURE 4.9 – L 'interface principale

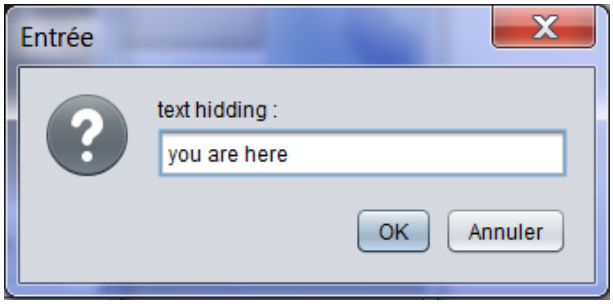


FIGURE 4.10 – L 'interface de cacher une text par exemple.

4.4 Les tests et discussion de résultats :

Après la conception et l'implémentation de la technique stéganographie VOIP, l'ensemble de toutes les performances et les résultats détaillés de ce technique est testé et enregistré. on va discuter et analyser les résultats finaux et les résultats associés à cette application ainsi que les résultats de la technique mis en œuvre.

*** Critères des tests :**

Nous avons effectué plusieurs tests pour voir l'effet de la modification des bits sur la qualité du signal. La procédure est la suivante :

- Enregistrer une phrase en PCM.
- Coder (compresser) le PCM données à l'aide d'iLBC.

On a déjà vu des critères de comparaison choisis entre couverture-objet et les signaux stego, nous allons choisir trois critères qui sont :

*** Taux de dissimulation :**pour la méthode de dissimulation des données LSB Ainsi, pour un 1kHz échantillons audio, 1 kbit/s de données sont cachées. en plus le codec ILBC en 20 ms il y'a 38 octets.

*** Imperceptibilité :** on remarque que La voix de forme d'onde dessin sont identiques dans le cas avec stego et sans stego (single PCM et single codec ILBC).

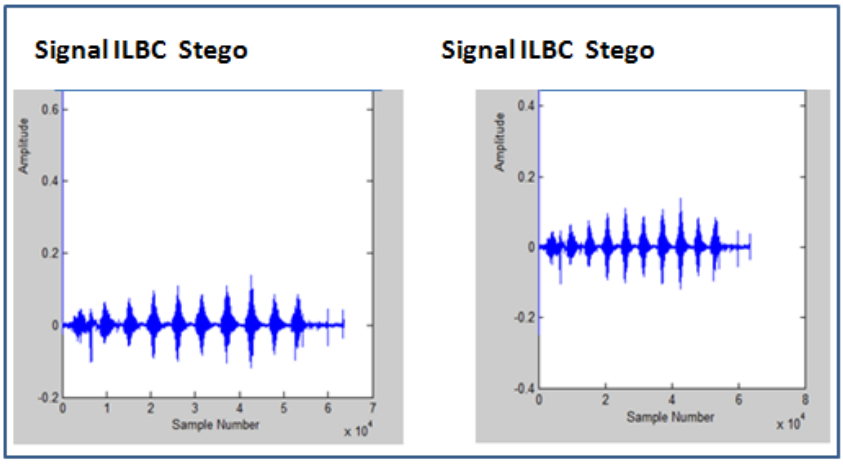


FIGURE 4.11 – Signal ILBC sans Stego et avec Stego .

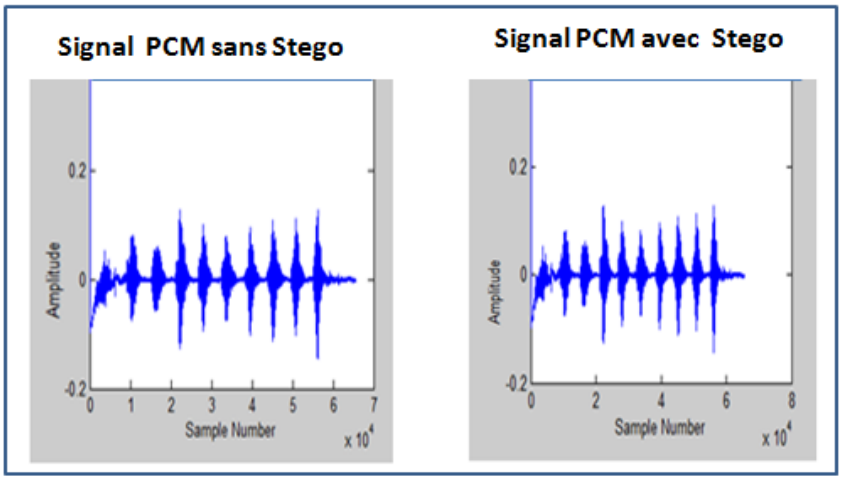


FIGURE 4.12 – Signal PCM sans Stego et avec Stego

*** Encodage/décodage :**

la première technique : est caché 32 bits dans un seul paquet .

la deuxième technique : est caché un bit dans chaque paquet . pour les deux techniques on teste la quantité de données cachées (en bits) et en plus l'imperceptibilité. D'après La voix de formes d'onde dessin on remarque qu'une modification est effectuée au niveau des signaux (ILBC).

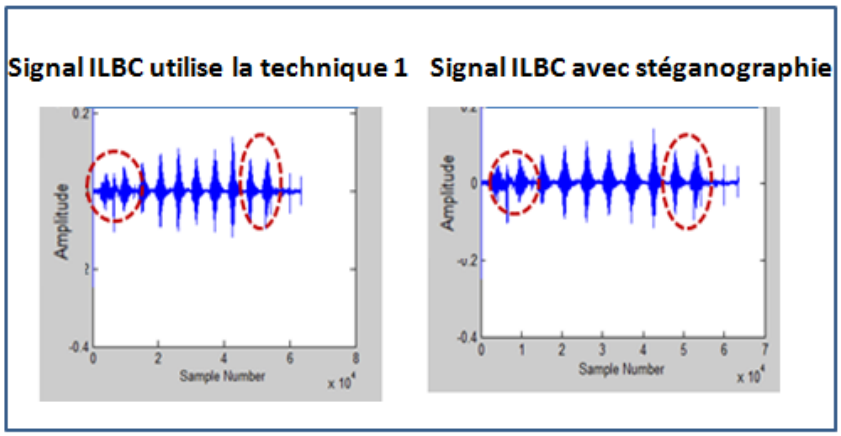


FIGURE 4.13 – Signal ILBC en utilisent technique 1 et 2 .

* Ces observations confirment que notre méthode ne dégrade pas la qualité signal lorsque vous utilisez uniquement les bits les moins significatifs de l'armature (bits de classe 3). Nous ne devons pas oublier également qu'iLBC utilise la compression avec perte, cela signifie qu'il dégrade la qualité du signal. Par conséquent, modifier le signal de plus pour cacher des données pas toujours à considérer comme dégradant la qualité. Parce que le changement peut affecter le signal de manière positive. Dans sa forme en comparaison de sa forme après l'encodage du signal avec iLBC cachée un seul bit pour chaque paquet et tous 32 bits dans 1 seul paquet.

4.5 Les suggestions de renforcement de la technique :

Il existe des facteurs qui limitent notre recherche qui sont les suivants :

- Il n'existe pas un système sécurisé parfaitement. Il y' a toujours la notion mise à jour .
- Le système de la stéganographie VOIP, qui est caractérise par exemple, par la transmission en temps réel, caractère bidirectionnel et vaste quantité de données rendent médium très approprié pour cacher des données secrètes. Qui pose un grand problème pour grader ces propriétés et même chose au niveau du système de la stéganographie. il faudrait une étude afin de déterminer la meilleure méthode de modèle en temps réel de la stéganographie ,il suggérée de renforce des capacités dans ce domaine de recherche.

4.6 Conclusion :

Au cours de ce chapitre, nous avons discuté de l'analyse et la mise en oeuvre de la technique de stéganographie VOIP. Nous avons commencé avec la conception et l'application d'appel VOIP, qui est la base de nos supports de communication. Après cela, nous avons déménagé dans les méthodes d'incorporation et extraction utilisées dans cette technique, et qu'elle utilise principalement la technique de LSB. Ensuite, nous avons expliqué la forme d'onde en fonction de dessin qui est utilisé pour dessiner les formes d'onde des signaux avant et après l'incorporation.

Enfin, nous avons expliqué quels sont les résultats de cette technique et comment ils sont présentées. Après cela, on doit tester les résultats de l'implémentation suivant les Critères de Comparaison pour Assurer la bonne sécurité et la capacité de stockage sans sacrifier les performances en temps réel.

Conclusion générale et perspectives

Au cours de ce mémoire, nous avons présenté les résultats de notre recherche dans le domaine de la stéganographie VOIP, et on a essayé d'atteindre les objectifs de la thése prédéfinis et nous avons expliqué comment s'assurer que les objectifs sont atteints en testant les résultats de cette recherche. Par une contribution principale qui permet de développer une technique de stéganographie qui sert à contester la capacité de dissimulation les informations en VOIP stéganographie, en utilisant plusieurs techniques LSB.
Selon les résultats définitifs et la discussion et la technique mis en œuvre de la revue analyse,on a introduit deux nouvelles techniques permettant d'améliorer la capacité de la stéganographie VOIP, en plus a robustesse.

Comme perspectives :

Il serait envisageable de faire la Mise en œuvre de la technique la VOIP pour pertinents ouvrir de nouveaux horizons et apportent de nombreuses idées pour améliorer ce système.

Cette technique était axé sur la stéganographie LSB et la compression ILBC et les améliorations suggérées pour améliorer la capacité des données de charge utiles. Des techniques non testées théoriques rend la stéganographie VOIP un domaine intéressant pour approfondir l'étude .

Bibliographie

[Ali10] Akbas E. Ali. A new text steganography method by using non-printing unicode characters. 2010.

[Ben06] Mohamed Lahcen Bensaad. New and intelligent embedding algorithm and new techniques for information hiding in web pages. Master's thesis, Graduate School Hunan University ChangSha, P.R. China, 2006.

[Ben14] Mohamed Lahcen Bensaad. *Steganography and Digital Watermarking.* PhD thesis, University of Amar Teldji Laghouat, 2014.

[BJS10a] Wojciech Mazurczyk Bartosz Jankowski and Krzysztof Szczypiorski. Information hiding using improper frame padding. 2010.

[BJS10b] Wojciech Mazurczyk Bartosz Jankowski and Krzysztof Szczypiorski. Information hiding using improper frame padding. 2010.

[Chu] Vincent Chu. *ASCII Art Steganography.*

[DAMH12] Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim, and Habib Hamam. Comparative study of digital audio steganography techniques. *EURASIP Journal on Audio, Speech, and Music Processing 2012*, 04 :1687–4722–2012–25, 9 October 2012.

[DEN05] Jenny DENTAND. *STEGANOGRAPHIE.* Travail de diplome, 2005.

[DK10] Kundur D. and Ahsan K. Practical internet steganography : Data hiding in ip. 2010.

[eNHSeABeAM06] A. ALI-PACHA et N. HADJ-SAID et A. BELGORAF et A. MHAMED. Steganographie : Securite par dissimulation. *Universite des Sciences et de la Technologie d Oran USTO Institut National des Telecommunications Evry- Paris*, Vol, 16 n 01 :101,110, 2006.

[FH11] K. Abed-Meraim F.Djebbar, B. Ayad and H. Hamam. A view on latest audio steganography. *7th IEEE Internationl Conference on Innovations in Information Technology, Abu Dhabi, UAE*, 2011.

[GUI12] Antoine GUILMAIN. La steganographie au quebec : Lumieretechnique,ombres juridiques. *Automne/Fall*, Lex Electronica, vol. 17.2 :9, 2012.

[HS06] N. HADJ-SAID. Steganographie : Securite par dissimulation. *Universite des Sciences et de la Technologie Oran USTO, Institut National des Telecommunications Evry Paris*, Vol 16 :103, Annee 2006.

[JL10a] Krzysztof Szczypiorski Jozef Lubacz, Wojciech Mazurczyk. Vice over ip the voip steganography threat. 2010.

[JL10b] Krzysztof Szczypiorski Jozef Lubacz, Wojciech Mazurczyk. Vice over ip the voip steganography threat. 2010.

[Kha12] Swati Malviya Manish Saxena Dr. Anubhuti Khare. Audio steganography by different methods. *International Journal of Emerging Technology and Advanced Engineering*, Volume 2 :317–376, July 2012.

[Lin04a] S. Andersen A. Duric H. Astrom R. Hagen ; W. Kleijn J. Linden. Internet low bit rate codec. *Internet Engineering Force Task*, Rfc 3951 :62, 64, 65, 67, 68, 2004.

[Lin04b] S. Andersen ; A. Duric ; H. Astrom ; R. Hagen ; W. Kleijn ; J. Linden. Internet low bit rate codec. internet engineering force task. 2004.

[LIU12] K. TIAN H. . LIU, J. ZHOU. Least-significant-digit steganography in low bit-rate speech. *In proc. of the 47th IEEE International Conference on Communications (ICC), Ottawa, Canada,*, pages 1–5, 2012.

[Lu96] W. Bender D. Gruhl N. Morimoto A. Lu. Techniques for data hiding. 1996.

[Mei10] Patrick Philippe Meier. *Steganography 2.0 : Digital Resistance against Repressive Regimes*. irevolution.wordpress.com., Retrieved 17 June 2010.

[ML12] Wojciech Mazurczyk and Jozef Lubacz. Lack voip steganographic method. 2012.

[MS10] Wojciech Mazurczyk and Krzysztof Szczypiorski. Steganography of voip streams. *Lecture Notes in Computer Science (LNCS) 5332,*

Springer-Verlag Berlin Heidelberg, Proc. of The 3rd International Symposium on Information Security (IS'08), Monterrey, Mexico, Retrieved 16 June 2010.

[PEL04] Remy ALLAIS Francois DUMONT Alexandre PELTIER, editor. *Projet de veille technologique - La Steganographie*. 23 juin 2004.

[PS11] Jayaram P and Ranganatha H R Anupama H S. Information hiding using audio steganography a survey. 2011.

[Sep02] N. Cvejic T. Seppiinen. Increasing the capacity of lsb-based audio steganography. 2002.

[Sep04] Nedeljko Cvejic Tapio Seppanen. Reduced distortion bit-modification for lsb audio steganography. *Proceedings of International Conference on Multimedia*, vol 2 :336–338, 2004.

[Shu13] Nikita Negi Jyoti Shukla. Steganography and transcoding voice stream over voip. *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3 :917 ,921, September 2013.

[Szc10] Krzysztof Szczypiorski. Hiccups : Hidden communication system for corrupted networks. 2010.

[WAN07] WU W WANG, C. Information hiding in real-time voip streams. *In Proc. of 9th IEEE Int Symp Multimedia (ISM 2007)*, pages 255–262, 2007.