UNIVERSITE KASDI MERBAH OUARGLA
Faculté des nouvelles technologies de l'information et de la communication
Département de l'informatique

Mémoire
MASTER ACADEMIQUE
Domaine : Math et Informatique
Filière : Informatique
Spécialité : RCS

Présenté par :
M.BENDJERIOU RAMZI M. ARAR ABDELHAKIM

Thème :

Une étude comparative entre la stéganographie JPEG et la stéganographie tcp/ip pour une meilleure technique de dissimulation des données

Devant le jury :

Mr. Med kamel Benkaddour	MA (A)	Président	UKM Ouargla
Mr. Boukhamla akram	MA (B)	Encadreur/rapporteur	UKM Ouargla
Mr. Fares Kahlesnane	MA (A)	Examinateur	UKM Ouargla

Année universitaire 2016/2017

Dédicace

Je dédie ce modeste travail en premier lieu à ma chère mère et chère père qui ont consenti beaucoup de sacrifices qui m'ont toujours soutenu et encouragé tout au long de ma vie, je demande à dieu la protégée et réserve-leur une longue vie.

A ma très chère sœur, farida, khouloud,siham,wafa,manal.

A mes très chers frères, lhadj elsaid.

A mes grands-pères abdelkader et Mabrok ((la miséricorde de Dieu)), mes grande mère messouda ((la miséricorde de Dieu)) et Fatima Zohra.

A tous mes oncles :
Ibrahim,Mohemmed,Azozi,Kamel,Abdelhafid,Ali,Abdelhalim leurs maris et leur enfants.

A toutes mes tantes : siyda, Samia, Saffa, Ouarda, Salima, samira et leurs maris et leurs enfants, mes tantes Sabah et Atika, EL Zohra ((la miséricorde de Dieu)).

A tout la famille d'ARAR et BENNEDJMA

A mon cher binôme BEN DJERIO RAMZI

A Tous les amis de sport « Génération qui monte », étude et travail et les amis de la chambre(A33)

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

ARAR ABDELHAKIM

Dédicace

Je dédie ce modeste travail en premier lieu à ma chère mère et chère père qui ont consenti beaucoup de sacrifices qui m'ont toujours soutenu et encouragé tout au long de ma vie, je demande à dieu la protégée et réserve-leur une longue vie.

A ma très chère soeur, fatima elzahra elbatoul, yamna .

A mes très chers frères, yazid.

A mes grands-pères mouhamed elsghire (matras) ((la miséricorde de Dieu)) et rabeh osmane.

Mes grande mère y amna kafi

A mes tante : Rahima.

A tout la famille de BENDJERIOU et OSMANE.

A mon cher binôme ARAR ABDELHAKIM.

A Tous les amis de djil eldokana eldahabi .

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

BEN DJERIO RAMZI

Remerciement

Tout d'abord, nous remercions ALLAH pour la volonté, la force, la santé et la patience qu'Il nous a donné afin de réaliser ce travail.

Nous tenons particulièrement à remercier notre encadreur Mr Boukhamla AKRAM pour se précieux conseil et son sens d'organisation et le suivi qu'il nous apporté durant ce travail.

Nous remercions toute la noble famille en particulier les parents et particulièrement l'ensemble des enseignant département l'informatique.

Enfin, nous remercions toute personne qui a à des degrés divers, contribué sur le plan intellectuel, technique, moral, affectif ou encoure Materials à l'achèvement de ce travail.

Résumé

Avec l'évolution du domaine de la technologie de l'information et de la communication, la sécurité informatique est devenue un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent. La stéganographie fait partie des moyens de sécurité contre les tentatives d'intrusion. Elle peut utiliser plusieurs mediums pour transférer secrètement les données telles que les images, audio, vidéo, trame tcp/ip etc.

Dans ce travail de mémoire nous avons appliqué la stéganographie sur un support de réseau qui est la trame tcp/ip. Ceci est faite par l'introduction du message à dissimuler dans un des champs non utilisés généralement et qui passent aussi inaperçu par l'intrus. Dans ce mémoire, nous avons dissimulé les données dans deux champs de la tram tcp/ip qui sont « IP Identification » du protocole IP et « Sequence Number » du protocole TCP. Ainsi, nous avons renforcé l'aspect sécurité par l'ajout de l'option de cryptage par un algorithme qui est AES. Nous remarquons que les résultats obtenus sont satisfaisants du fait qu'on peut partitionner les données à envoyer par plusieurs trams qui ne sont pas volumineux, aussi les champs utilisés ne sont généralement pas inspectés par les intrus.

- **Mots clé :** stéganographie, canal caché, trame tcp, trame ip, Numéro ISN, Identification IP, image JPEG, algorithme, cryptage.

ملخص

مع مجال تغير تكنولوجيات المعلومات والإتصالات أصبح أمن الكمبيوتر قضية رئيسية بالنسبة للشركات وكدلك لجميع الجهات الفاعلة حوله.إخفاء المعلومات هو جزء من الإجراءات الأمنية ضد محاولات التسلل.فإنه يمكن إستخدام عدة وسائل لنقل البيانات مثل الصور والصوت والفيديو والترام .....إلخ.

في هده المدكرة إستعملنا إخفاء المعلومات على وسيط الشبكة الدي هو الترام ويتم دلك من خلال رسالة مخبئة في الحقول التي لا يشيع إستخدامها وتمر دون أن يلاحظها أحد حتى من قبل الدخيل أيضا هدين الحقلين هما:

« IP Identification » du protocole IP.

« Sequence Number » du protocole TCP .

أيضا في هده المدكرة قمنا بتعزيز جانب السلامة من خلال إضافة جانب التشفير بخوارزمية:

AES

نلاحظ أن النتائج التي تم الحصول عليها مرضية لأنه يمكن للمرء تقسيم البيانات التي سيتم إرسالها من قبل مجموعة من الترام التي ليست ضخمة، وبالتالي فإن الحقول المستخدمة لا يتم تفتيشها عموما من قبل الدخلاء.

الكلمات الدالة : قناة مخفية, إطار TCP, إطار IP, رقم ISN, تحديد IP, صورة JPEG, الخوارزمية, التشفير.

Abstract

With the evolution of the field of information and communication technology, computer security has become a major challenge for companies and for all the actors that surround it. Steganography is part of the means of security against intrusion attempts. It can use several mediums to secretly transfer data such as images, audio, video, trame tcp / ip etc.

In this memory work, we applied the steganography on a network support which is the tcp / ip trame. This is done by introducing the message to be concealed in one of the fields not used generally and which also pass unnoticed by the intruder. In this brief, we hid the data in two fields of the tcp / ip trame which are "IP Identification" of the IP protocol and "sequence number" of the TCP protocol. Thus, we have strengthened the security aspect by adding the encryption option by one of the two algorithms which are AES and SHA. We note that the results obtained are satisfactory because we can partition the data to be sent by several trams which are not bulky, so the fields used are not generally inspected by the intrude.

- **Key words:** steganography, Hidden channel, TCP frame, IP frame, ISN Number, IP Identification, image JPEG, algorithm, encryption.

Table des matières :

Introduction generale……1

I. Chapitre : Definition & Historique

1.Introduction……4

2.Historique……....5

3.La stéganographie……8

3.1. Les modes de stéganographie……..8

3.1.1. Stéganographie linguistique ……....8

3.1.2. Stéganographie technique ……9

3.2. Les différents types de technique stéganographie……9

3.2.1. Stéganographie pure……..9

3.2.2. Stéganographie clé secret……10

3.2.3. Stéganographie clé publique ……..10

4.Buts et intérêts……11

5. Propriétés des systèmes de stéganographie……...11

5.1. Capacité……..11

5.2. Sécurité……...12

5.3. Robustesse……..12

6. Stéganalyse ……...12

7.Conclusion……13

II. Chapitre : stéganographie image JPEG

1. Introduction……..14

2. Représentation d'image……14

3. Format d'image……15
4. Domaines de stéganographie……16
4.1. Domain spatial……...16
4.2. Domain fréquentiel……17
4.2.1. Introduction au format JPEG……18
4.2.2. Algorithmes et transformation……..19
4.3. Algorithmes……21
5. Logiciel de stéganographie……...26
6. Stéganalyse……...27
6.1. Analyse x^2……27
6.2. Zhang et Ping……29
6.3. Logiciel de stéganalyse……..29
7. Conclusion……...30

III. Chapitre : stéganographie tcp/ip

1. Introduction…….……31
2. Paquets et protocoles réseau……32
3. Les canaux cachés dans les protocoles TCP/IP……33
3.1. IP……33
3.2. TCP……35
4. Stéganographie dans les paquets TCP/IP……..……...37
5. Architecteur du système stéganographie proposé……38
5.1. Description du module ANA……38
5.2. Description du module BOB……..40
6. Mécanisme de détection des canaux cachés TCP/IP……41
6.1. SVM……...41
6.2. Analyse des canaux cachés et prédiction des attaques……..….41
7.Comparaison……...42
8. Conclusion...…….43

V .Chapitre : Conception & Implémentation

1. Introduction……..……44
2. Les outillés utilisées…….44
2.2. Les champs utilisés……44
2.2. Les algorithmes de cryptage……..44
2.3. Le langage de programmation……44
3.Application de messagerie…….45
4. Organigramme de l'application……49
5. Conclusion……50

Coclusion generale…..……51
Reference……..52

Listes des figures :

Fig.1 : L'écriture invisible----------p.5
Fig.2 : Le disque de Phaistos----------p.6
Fig.3 : Représentation chronologique retrace certaine utilisation de stéganographie dans l'histoire----------p.7
Fig.4 : Processus de stéganographie pure----------p.9
Fig.5 : Stéganographie à clé secret----------p.10
Fig.6 : Stéganographie à clé publique----------p.10
Fig.7 : Schéma compression/décompression JPEG----------p.18
Fig.8 : Format la chaine à inverse avec JSTEG----------p.22
Fig.9 : Modification des coefficient DCT par JSTEG----------p.23
Fig.10 : En-tête IPV4----------p.34
Fig.11 : Canal caché utilisent IP identification champ----------p.35
Fig.12 : En-tête de paquet TCP----------p.36
Fig.13 : Canal utilisent le numéro de séquence TCP----------p.37
Fig.14 : Transfert de l'information d'A vers B en utilisent la stéganographie----------p. 38
Fig.15 : Diagramme aves fonctionnalité ANA----------p.39
Fig.16 : Diagramme aves fonctionnalité BOB----------p.40
Fig.17 : L'interface de l'application messagerie----------p.45
Fig.18 : Fenêtre pour choisir l'interface----------p.46
Fig.19 : Établie la connexion----------p.46
Fig.20 : Champs de message----------p.47
Fig.21 : Les champs de cryptage----------p.48
Fig.22 : Organigramme de l'application----------p.49

Introduction générale

Le contrôle des flux d'information est un problème central pour la sécurité d'un système quel qu'il soit : une entreprise, un État, un particulier ; tous ont des documents à préserver du regard d'autrui. Cela entraîne, par exemple, la volonté de s'assurer de la confidentialité de transfère d'information, de nos jours pris en charge via des mécanismes cryptographiques. À défaut de savoir exactement ce qui peut arriver à la communication, on peut se prémunir des indiscrétions en chiffrant les données. Cependant, ces mécanismes cryptographiques peuvent ne pas être disponibles où seule une cryptographie faible pouvait être utilisée sans disposition spéciale. Dans ces conditions, assurer la confidentialité relève d'autres techniques, notamment de la stéganographie.

Étymologiquement, « stéganographie » a pour signification « écriture cachée ». Autrement dit, l'objectif principal est de communiquer sans que cela voix. Pour cela, il n'y a pas de mystère, il doit déjà exister une communication que la stéganographie va détourner de son utilisation classique afin de pouvoir inclure de l'information additionnelle aussi discrètement que possible. Malheureusement, les algorithmes stéganographiques sont très dépendants de la structure des données dans lesquelles se fait l'insertion : c'est assez logique, les modifications devant être imperceptibles, il faut altérer les données dans les endroits les plus discrets, ce qui dépend fortement du type des données (audio, image…) et de leur format de représentation (JPEG, GIF, MP3…). Donc, contrairement à la cryptographie, nous avons affaire à un ensemble de techniques très variées dépendant des différents formats, même si certaines caractéristiques peuvent perdurer d'un format à l'autre pour un même type de données.

Parmi les types de support utilisés par la stéganographie on trouve la trame TCP/IP qui est un outil qui permet de véhiculer les informations à dissimuler à travers les champs trouvés dans la trame TCP/IP.

Problématique:

Actuellement, le cryptage seul est un moyen de moins en moins sûr pour faire circuler des données. Certaines méthodes sont même inutiles tant elles sont faciles à "cracker". Évidemment, certains algorithmes actuels sont extrêmement sûrs, mais peuvent présenter des failles d'implémentation. Mais surtout, un fichier crypté attire plus l'attention qu'un autre on se dit que s'il est crypté, ce n'est pas pour rien. C'est là le point fort de la stéganographie. Avant même d'essayer de trouver du texte dans une image ou un support informatique, encore faut-il savoir qu'elle en contient. La différence infirme entre le support d'origine et sa version trafiquée est impossible à remarquer à l'œil nu. De plus, il suffit de créer un support soi-même afin que personne ne puisse le comparer avec un autre étant donné qu'il est unique. Il est donc impossible (ou presque, car rien n'est impossible, notamment dans le domaine de l'informatique) de savoir qu'il contient du texte. Pour un peu plus corser les choses, on peut même entrer des données cryptées dans l'image (pour les paranos).

Objectif de ce travail :

En stéganographie numérique, plusieurs approches ont été proposées afin d'améliorer la performance et la confidentialité du processus, que se soit par les outils qui transportent l'information à dissimuler, ou bien par les algorithmes de dissimulation. Cependant, en ce qui nous concerne, notre objectif est de renforcer l'aspect sécurité dans le cas de la stéganographie par trame tcp/ip, pour cela nous avons fait une étude sur la stéganographie tcp/ip, qui a été achevée par une application de dissimulation de l'information cryptée dans les champs de la trame tcp/ip, afin de la comparer avec la stéganographie par image.

Organisation du mémoire :

Chapitre I : Définition et historique

Ce chapitre est une introduction à la stéganographie qui contient un historique de la stéganographie depuis son apparition, des définitions des concepts utilisés par la sténographie linguistique et technique, puis les différents éléments intervenant dans la dissimulation d'informations, ainsi que les buts et les intérêts de cette technique.

Chapitre II : Stéganographie image JPEG

Dans ce chapitre, nous allons parler de la stéganographie utilisée dans l'image Jpeg. Nous allons discuter les domaines de la stéganographie, ainsi les algorithmes de transformation

implémentés par la stéganographie dans l'image. Quelques logiciels de stéganographie et aussi de stéganalyse ont été présentés aussi dans ce chapitre.

Chapitre III : Stéganographie TCP/IP

Ce chapitre aborde la stéganographie dans la trame TCP/IP qui est un type de support d'information. Nous allons fait une présentation des champs de la trame TCP/IP, puis une présentation de processus utilisés dans la stéganographie TCP/IP et aussi dans la stéganalyse.

Chapitre IV :

Ce chapitre Offres l'application réalisée qui permette de dissimuler un message dans un champ qui est généralement non utilisé lors du transfert des données, ainsi pour renforcer la sécurité, nous allons crypter le message à envoyer par un algorithme de cryptage (AES).

Chapitre I:

Definition & Historique

I. 1.Introduction :

La stéganographie est l'art de la dissimulation : son objet est de faire passer inaperçu un message dans un autre message.

La stéganographie en grec signifie « écriture couverte ». La stéganographie est le processus de dissimulation de l'information dans d'autres sources d'information comme le texte, l'image ou le fichier audio, de sorte qu'il n'est pas visible à la vue naturelle.

La stéganographie a pour avantage de faire transiter des informations (cryptées ou non) sans attirer l'attention car ces informations sont contenues dans d'autres informations classiques (textes, images, trames TCP, codes sources, morceaux de musique, ...).

Les principaux formats de fichiers utilisés pour la stéganographie sont le texte, les images, l'audio, Vidéo, protocole.

Sa force est principalement basée sur deux idées simples : nos sens (œil, ouïe) ne sont pas capables de détecter d'infimes changements dans une image ou un son, et à priori nous ne savons pas à l'avance que tel fichier renferme de l'information cachée.

I. 2.Historique :

Dans son Enquête, l'historien grec Hérodote (484-445 av. J. -C.) rapporte ainsi une anecdote qui eut lieu au moment de la seconde guerre médique. En 484 avant l'ère chrétienne, Xerxès, fils de Darius, roi des Perses, décide de préparer une armée gigantesque pour envahir la Grèce.

Quatre ans plus tard, quand il lance l'offensive, les Grecs sont depuis longtemps au courant de ses intentions. C'est que Démarate, ancien roi de Sparte réfugié auprès de Xerxès, a appris l'existence de ce projet et décide de transmettre l'information à Sparte: «il prit une tablette double, en gratta la cire, puis écrivit sur le bois même les projets de Xerxès ; ensuite il recouvrit de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis ». Un autre passage de la même œuvre fait aussi référence à la stéganographie : au paragraphe 35 du livre V, Histiée incite son gendre Aristagoras, gouverneur de Milet, à se révolter contre son roi, Darius, et pour ce faire, «il fit raser la tête de son esclave le plus fidèle, lui tatoua son message sur le crâne et attendit que les cheveux eussent repoussé ; lorsque la chevelure fut redevenue normale, il fit partir l'esclave pour Milet»[26].

Les plus connu des procédés de stéganographie :

- **L'écriture invisible au jus de citron :**

Ecrire un message à l'aide d'une plume trempée dans du jus de citron permet de rendre le message invisible.

Fig. 1 : l'écriture invisible

- **Le disque de Phaistos :**

En 1908, sur une plaine crétoise de la Messara, une équipe d'archéologues italiens exhument au milieu des ruines millénaires du palais de Phaistos un disque d'argile recouvert sur ses deux faces de pictogrammes inconnus. Le disque de Phaistos est en argile cuite très fine, un peu irrégulier. Son diamètre varie de
15,8 cm à 16,5 cm, son épaisseur de 16 à 21 mm sur chaque face une ligne en spirale fait fonction de guide, comme les lignes d'un cahier d'écolier moderne.

Fig. 2 : Le disque de Phaistos

- En Chine, on écrivait le message sur de la soie, qui ensuite était positionnée dans une petite boule recouverte de cire. Le messager avalait ensuite cette boule.

- Durant la Deuxième Guerre mondiale, les agents allemands utilisaient la technique du micro point de Zapp, qui consiste à diminuer la photo d'une page en un point d'un millimètre ou même moins. Ce point est ensuite positionné dans un texte normal. Le procédé est évoqué dans une aventure de Blake et Mortimer, S. O. S. Météores.

Actuellement, l'accent a été mis sur diverses formes de stéganographie numérique. Généralement, il a un certain nombre de technologies numériques que la communauté est concernée, à savoir les fichiers texte, images fixes, images de films, et audio.

- Avec l'avènement de l'informatique et le développement des échanges électroniques, les possibilités de cacher un message se sont multipliées : on peut cacher un message dans une image, un site internet, un programme, une musique. La stéganographie a aussi trouvé des

applications commerciales, avec le tatouage numérique. On cache un message dans une image ou une musique, pour identifier son origine, et aussi pour empêcher qu'elle ne soit dupliquée à l'insu de son propriétaire.

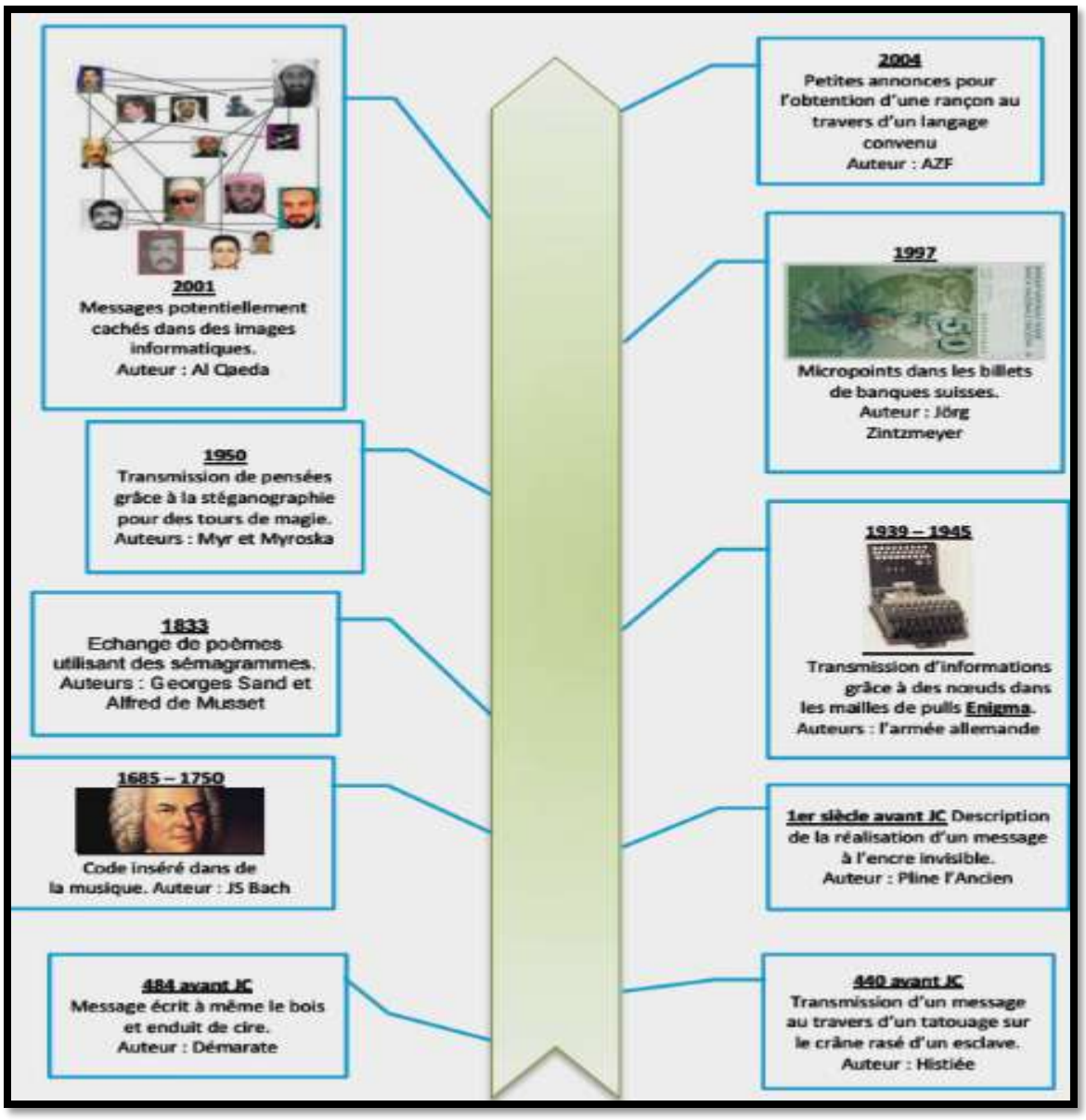

Fig.3 : Représentation chronologique retrace certaines utilisations de la stéganographie dans l'histoire.

I. 3.La stéganographie :

I .3.1. Les modes de stéganographie :

Il existe deux modes de stéganographie :

- La sténographie linguistique.
- La stéganographie technique.

I .3.1.1. La sténographie linguistique :

La littérature sur la stéganographie linguistique, dans laquelle les propriétés linguistiques d'un texte sont modifiées pour cacher l'information, est faible par rapport à d'autres médias. La raison probable est qu'il est plus facile d'apporter des modifications aux médias non linguistiques dans lesquels le message secret sera indétectable par un observateur. Les différentes formes de la stéganographie linguistique sont :

- **Sémagramme :**

La forme la plus connue en stéganographie linguistique est le Sémagramme. De cette manière, le système sténographique échappe totalement à l'observateur. Alfred de Musset est l'utilisateur le plus connu de ce procédé. Il a entretenu, entre 1833 et 1834, une relation secrète avec Georges Sand au travers de poèmes qu'il lui envoyait.

- **Acrostiche :**

Ce procédé permet de transmettre des données au travers de lettres initiales dans chaque vers de poème et qui, lus de haut en bas, forment un mot ou une expression. Elle a de nombreuses variantes (mot placé dans des vers ou des chapitres…).

- **Ponctuation :**

L'utilisation de points, hauteur de lettres et virgules par les prisonniers de guerre a également permis de transmettre des messages à leur famille.

- **Nulles :**

Les codes camouflés, aussi appelés les nulles, consistent à marquer d'un signe particulier certaines lettres d'un texte (par des piqûres d'aiguilles sur ou sous les lettres). Il suffit alors de rassembler les lettres marquées pour former un mot.

- **Insertion d'erreurs :**

Mise en valeur de l'information au travers d'erreurs ou de formes de style dans un texte.

Ces différents procédés restent néanmoins difficiles et longs à réaliser et laissent vite suspecter la possibilité d'un message dissimulé. De nombreuses censures ont été ainsi appliquées afin de limiter l'usage de ces techniques

I .3.1.2. La stéganographie technique :

La stéganographie technique regroupe toutes les techniques qui ne jouent pas sur les mots. La stéganographie technique est intéressante car elle permet de dissimuler des données dans plusieurs types de médias et La stéganographie sous diverses formes.

- **Audio :**

Afin de transmettre de l'information de manière cachée dans du son, différentes techniques existent et se basent sur le fait qu'un son affecte la perception d'un autre : un son plus fort peut en cacher un autre, un son peut être caché temporairement lorsqu'il est moins fort et qu'il est placé avant ou après un son plus fort.

- **Images, vidéo :**

Enfin, une image ou une vidéo peuvent également contenir un message. Une image est constituée de pixels. Il est possible d'insérer des bits du message secret à l'intérieur sans que ces modifications soient perceptibles à l'œil humain.

- **La stéganographie sous diverses formes :**

Cette technique étant l'art de cacher de l'information dans d'autres informations, il est possible d'utiliser cette idée dans le domaine des réseaux informatiques, principalement via des canaux cachés ou tunneling sur presque toutes les couches du modèle OSI (IP, TCP, ICMP, HTTP, DNS, ...) comme nous allons le voir ci-dessous.

I .3.2.Les différents types de techniques stéganographie :

I) .3.2.1. Stéganographie pure :

La stéganographie pure est le processus d'incorporation des données dans l'objet sans utiliser de clés privées. Ce type de stéganographie dépend entièrement du secret.

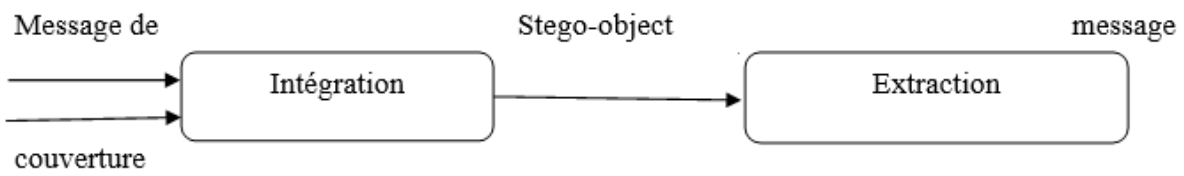

Fig. 4 : Processus de stéganographie pure

Ce type de stéganographie ne peut pas fournir la meilleure sécurité parce qu'il est facile pour extraire le message si la personne non autorisée connaît la méthode d'incorporation. Il a un avantage à réduire la difficulté de partage des clés.

I) .3.2.2. Stéganographie clé secrète :

La stéganographie clé secrète est un autre procédé de stéganographie qui utilise la même procédure autre que l'utilisation de clés sécurisées. Il utilise la clé individuelle pour incorporer les données dans l'objet qui est similaire à la clé symétrique. Pour le décryptage il utilise la même clé qui est utilisée pour le cryptage.

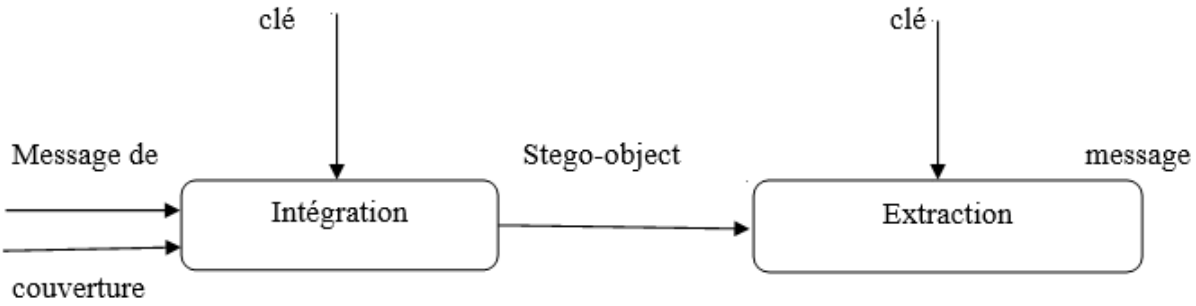

Fig. 5 : stéganographie à clé secrète.

Ce type de stéganographie offre une meilleure sécurité par rapport à la stéganographie pure. Le problème principal de l'utilisation de ce type de système stéganographie est le partage de la clé secrète. Si l'attaquant connaît la clé, il sera plus facile de déchiffrer et d'accéder à l'information originale.

I .3.2.3. Stéganographie à clé publique :

La stéganographie à clé publique utilise deux types de clés : une pour le chiffrement et une autre pour le décryptage. La clé utilisée pour le cryptage est une clé privée et pour le décryptage, c'est une "clé publique" et est stockée dans une base de données publique.

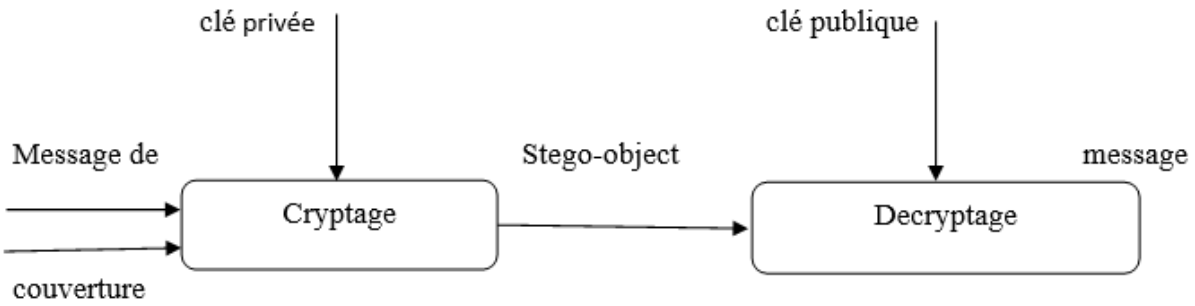

Fig. 6 : Stéganographie à clé publique.

I. 4. Buts et intérêts :

a) La protection des possesseurs de copyrights :

Cette dernière limite ainsi les droits de copies pour les DVD et CD audio.

b) Une discrétion des transmissions :

En utilisant la stéganographie, il est possible de cacher les communications qui peuvent exister entre l'émetteur et le destinataire. Ainsi, contrairement au cryptage Où les données sont illisibles, aucune relation ne peut être suspectée. Ce moyen est très intéressant pour l'armée notamment.

c) La connaissance de la stéganographie :

Le fait de connaître les différentes techniques possibles et employées pourra permettre au service de l'ordre et des lois de détecter les origines des fuites, de tenter de trouver la provenance de messages.

d) L 'anonymat :

Ce système rend impossible la détermination de l'identité de la personne émettrice ainsi que la mise en place d'une surveillance. Cela peut avoir des côtés positifs comme lors d'élections ou de transferts de données bancaires Où il est primordial de permettre l'anonymat des communications. Cependant, cela risquerait également de donner l'occasion aux terroristes de profiter de ce paramètre qui deviendrait alors une faiblesse.

e) La liberté :

Transmissions de données, cover-Channel éliminant toute censure, ou surveillance. En effet, il est possible de passer par des protocoles anodins pour communiquer et passer à travers un firewall, et ce, même pour des communications non-autorisées.

I. .5. Propriétés des systèmes de stéganographie :

I .5.1. Capacité :

La capacité d'insertion d'un système de stéganographie est définie par la taille en bits du message secret qui peut être intégré dans un média de taille donnée. La capacité d'insertion relative est le rapport entre la taille du message secret à dissimuler et la taille du médium utilisé.

I .5.2. Sécurité :

Toutes les exigences de sécurité pour les systèmes cryptographiques peuvent (doivent) également être considérées pour les systèmes de stéganographie. Cela signifie que la sécurité de stéganographie ne doit pas s'appuyer seulement sur l'algorithme, qui devrait être publique, mais sur le caractère secret de la clé. Dans la stéganographie, il ne devrait pas être possible de distinguer une image d'origine d'une image stego si la clé est inconnue. Par ailleurs, les modifications apportées sur l'image originale afin de pouvoir incorporer le message secret ne devrait pas modifier les propriétés statistiques de l'image. La technique qui étudie la sécurité des systèmes de stéganographie est la stéganalyse.

I) .5.3. Robustesse :

Elle quantifie la résistance du message dissimulé aux diverses attaques (transformations) apportées au médium stégo.

I. 6. Stéganalyse :

Actuellement, il existe une technique permettant d'attaquer les méthodes de stéganographie. Celle-ci est appelée la stéganalyse. Elle peut être appliquée par deux types de personnes. L'attaquant actif, qui connait la présence de l'information et tente de la modifier ou de l'extraire et l'attaquant passif, c'est-à-dire la personne qui arrive à déceler la présence du message et qui ne fait que constater sa présence.

I. 7.Conclusion :

La stéganographie transmet des secrets à travers des couvertures apparemment inoffensives dans le but de dissimuler l'existence d'un secret. La stéganographie d'image numérique et ses dérivés augmentent leur utilisation et leur application.

Dans les domaines où la cryptographie et le cryptage fort sont interdits, les informaticiens examinent la stéganographie pour contourner ces politiques et transmettre le message de manière dissimulée.

Comme pour d'autres grandes innovations de l'ère numérique : la lutte entre les cryptographes et la cryptanalyse, les experts en sécurité et les pirates informatiques, les maisons de disques et les pirates, la stéganographie et la stéganalyse développeront continuellement de nouvelles techniques pour se contrer.

Chapitre II:
stéganographie image JPEG

II. 1.Introduction :

Les fichiers d'image qui sont communs sur Internet aujourd'hui sont un très bon moyen pour la stéganographie numérique. Ils sont facilement et fréquemment partagés sur Internet par courrier électronique, affichage sur les sites, et d'autres moyens numériques. Ils sont de grande taille ce qui rend plus facile d'intégrer des informations de telle sorte qu'il n'est pas remarqué par l'utilisateur non informé. Les techniques sténographiques exploitent les propriétés des images et sont utilisées pour manipuler des bits dans l'image et intégrer des informations.

II. 2.Représentation d'image :

Les images numériques sont représentées sous forme de tableaux de valeurs de pixels. Un pixel est un point d'une image. La valeur numérique de chaque pixel est stockée en n octets et représente une couleur numérique. Chacun des n octets définit la quantité d'intensité lumineuse dans chacune des couleurs primaires : rouge, vert et bleu (RVB) et peut contenir Valeurs de 0 à 255 (valeurs pouvant être stockées en 8 bits 28). Par exemple, 255 pour la valeur rouge et 0 pour le bleu et le vert rendront la couleur rouge. D'autres valeurs proches de 255 pour la composante rouge et 0s pour le bleu et le vert rendront également une nuance de rouge qui peut sembler être de la même couleur à l'oeil humain.

La grande taille des fichiers d'image peut être attribuée à la façon dont les pixels sont représentés. Par exemple, une image de 24 bits (3 octets par pixel) de 600 pixels de large et 600 pixels de hauteur serait constituée de 600 × 600 × 24 bits (8 640 000 bits). Certains des pixels peuvent être ajustés en valeur pour correspondre à des lettres sans effet notable sur l'apparence de l'image.

Les fichiers d'image volumineux sont souvent comprimés pour une transmission plus rapide. Il existe deux types de compression, sans perte et avec perte. La compression sans perte maintient toutes les informations de l'image lors de la compression. Il est utilisé pour les fichiers GIF entre autres. La compression avec perte qui est utilisée pour les fichiers JPEG peut entraîner une perte d'information. Le logiciel de stéganographie utilise différentes techniques pour traiter des images en fonction de leur algorithme de compression.

Lors de la sélection d'une image pour la stéganographie, l'image et la palette de couleurs sont considérées. Les images avec de grandes zones de couleur unie sont plus susceptibles d'afficher des variations qui peuvent se produire en raison de l'incorporation de messages. Les messages intégrés seront moins susceptibles d'être remarqués dans des images et des images de niveaux de gris avec des variations de couleurs subtiles.

II. 3.Format d'images :

Il existe de multiples types d'images numériques. Il est important de connaître leurs spécificités car les manipulations apportées peuvent avoir ou non une incidence sur l'image. Nous nous concentrerons essentiellement sur les trois formats les plus utilisés :BMP, GIF et JPEG.

Chaque format a ses caractéristiques.

- **Format BMP (Windows bitmap) :** est un format universel, non compressé, développé par Microsoft et IBM. Il permet une restitution fidèle des couleurs de l'image d'origine, la contrepartie est le poids élevé du fichier généré.

- **Format GIF (Graphics Interchange Format) :** également très répandu dans le web, ce format propriétaire utilise un système de couleurs indexées. Il est ainsi possible de n'utiliser que des valeurs chromatiques spécifiques, ce qui permet d'optimiser au maximum le poids du visuel. En contrepartie, l'apparence de visuels affichant de nombreuses couleurs se trouve fortement dégradée. Ce format permet également de créer des animations image par image.

Le format GIF est un format qui utilise une compression sans perte de qualité.

- **Format JPEG (Joint Photographic Experts Group) :** très utilisé dans le web, ce format a été établi par un comité d'experts qui édite des normes de compression pour les images fixes. Ce format compressé altère grandement la qualité des images d'origine, mais permet d'avoir une restitution relativement fidèle des couleurs et un poids de fichier relativement léger. Alors est une compression avec perte (perte de qualité).

II.4.Domaines de stéganographie :

Il existe deux classifications de méthodes de stéganographie d'image : domaine spatial et domaine fréquentiel. Les techniques dans le domaine spatial incorporent les messages secrets directement dans les valeurs d'intensité des pixels d'image. Dans le domaine de la fréquence, les images sont d'abord manipulées avec des algorithmes et des transformations, puis les messages sont incorporés dans l'image. Les méthodes dans le domaine spatial sont considérées comme les plus simples mais également plus sensibles aux attaques par stéganalyse, moins robustes. Le domaine spatial est parfois appelé le domaine de l'image. Le domaine de fréquence est également connu sous le nom de domaine de transformation.

II .4.1. Domaine spatial :

Dans la stéganographie de domaine spatial, nous traitons directement la valeur de pixel de l'image qui est un bit de message secret qui est inséré dans l'image en modifiant la valeur de pixel de l'image. La stéganographie de domaine spatial la plus courante et la plus populaire est la méthode d'insertion du bit de poids faible (LSB). Pour mieux comprendre la méthode LSB, considérons l'exemple suivant :

Un exemple clair du résultat de l'incorporation de la lettre 'A' dans une image à 24 bits. Dans cet exemple, 3 pixels (9 octets) d'une image contiennent les valeurs binaires :

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

La valeur binaire pour la lettre 'A' est 10000011. L'insertion de la valeur binaire pour la lettre 'A' dans les 3 pixels entraîne :

(00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

La méthode LSB de base a une implémentation simple et une grande capacité. Cependant, il a peu de robustesse et de pros pour certaines attaques, comme le filtrage passe-bas et la compression.

II .4.2. Domaine fréquentiel :

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

Dans le domaine de transformation ou la stéganographie du domaine fréquentiel avant poser le message secret, l'image de couverture est transformée en son domaine fréquentiel en utilisant l'une des méthodes appropriées telles que la transformation rapide de Fourrier, la Transformée de Cosinus Discrète ou la Transformée de Wavelet Discrète. Dans le domaine transformé, le JPEG est la stéganographie la plus courante qui utilise le coefficient DCT pour intégrer des informations secrètes. Comme nous le savons, la compression JPEG est basée sur la transformée en cosinus discrète (DCT) et réduit la redondance visuelle pour obtenir de bonnes performances de compression. Par conséquent, la capacité d'incorporation fournie par la stéganographie JPEG est relativement plus petite que celle fournie par les autres méthodes stéganographique, mais la sécurité dans la stéganographie JPEG est très élevée, il est difficile de faire de la stéganalyse sur les stego-images qui utilisent la stéganographie de domaine de transformation.

Une tentative a été faite pour étudier les paramètres de haute capacité et de sécurité de la stéganographie en utilisant une transformation en ondelettes discrète. Donc, si nous utilisons la Transformée de Wavelet Discrete (DWT), nous pouvons atteindre les deux paramètres importants pour la stéganographie Capacité et sécurité.

Nous nous intéressons à présent aux algorithmes utilisés pour des images compressées au format JPEG, c'est-à-dire à des algorithmes qui opèrent dans le domaine fréquentiel. Dans cette sous-section, nous introduirons brièvement le format JPEG, puis présenterons des algorithmes utilisés pour de telles images.

II .4.2.1. Introduction au format JPEG :

Le schéma 7 décrit la chaîne de compression au format JPEG. Après des étapes facultatives de changement d'espace colorimétrique et de sous-échantillonnage, les tableaux de pixels de chaque canal de couleur sont découpés en blocs de 8×8 pixels. La transformée en cosinus discrète est ensuite appliquée à chaque bloc. On obtient ainsi des blocsde8×8 coefficients DCT. Chaque coefficient est ensuite quantifié en utilisant la table de quantification associée (présente dans l'entête du fichier). Le reste de la compression consiste à coder les tableaux de coefficients.

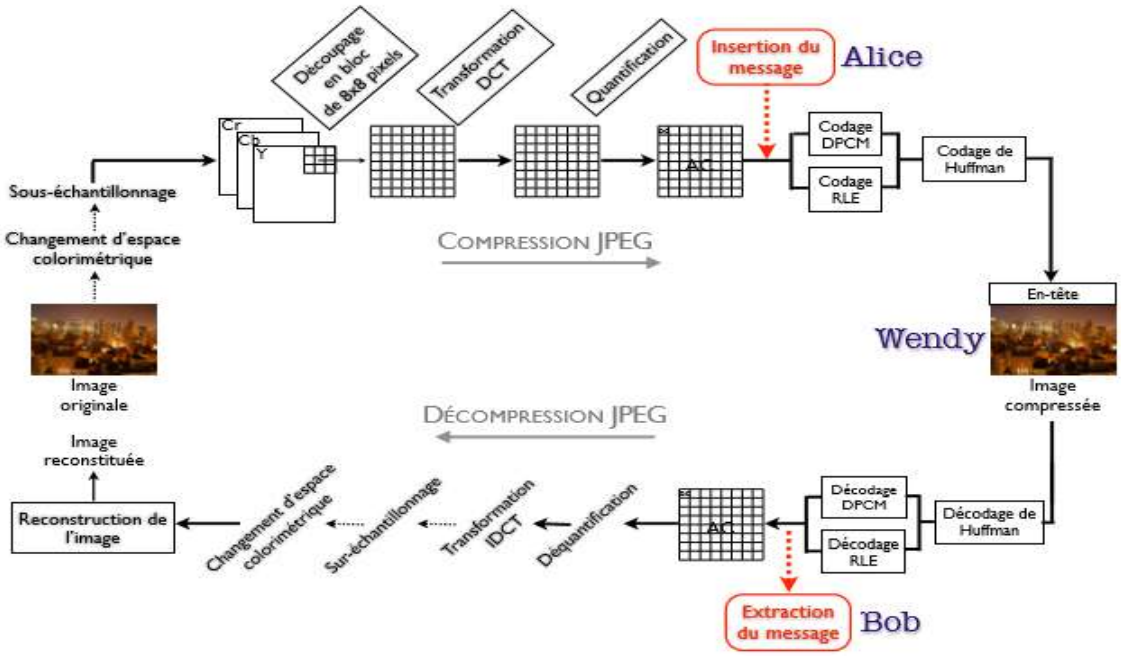

Fig.7 : Schéma compression/décompression JPEG.

La perte d'information liée à la compression apparaît lors de l'étape de quantification. C'est pourquoi les algorithmes insèrent le message dans les coefficients DCT quantifié (comme indiqué sur le schéma (fig. 7)). Ainsi, lors de l'insertion, tout se passe comme si une compression d'image était réalisée, mais après l'étape de quantification, les bits d'un message sont insérés dans les coefficients DCT quantifié.

II .4.2.2. Algorithmes et Transformations :

- **La transformée de cosinus discrète (DCT) :**

Les coefficients DCT sont utilisés pour la compression JPEG [2] [3]. Il sépare l'image en parties d'une importance différente. Il transforme un signal ou une image du domaine spatial en domaine fréquentiel. Il peut séparer l'image en composants à haute, moyenne et basse fréquence. En sous-bande de basse fréquence, une grande partie de l'énergie du signal est à basse fréquence, qui contient les parties visuelles les plus importantes de l'image alors que dans les sous-bandes à haute fréquence, les composantes haute fréquence de l'image sont généralement supprimées par des attaques de compression et de bruit [4]. Donc, le message secret est intégré en modifiant les coefficients de la sous-bande de fréquence moyenne, de sorte que la visibilité de l'image ne sera pas affectée.

Algorithme pour intégrer un message secret :

- Étape 1 : Lire l'image de couverture.
- Étape 2 : lire le message secret et le convertir en binaire.
- Étape 3 : L'image de couverture est divisée en 8 × 8 bloc de pixels.
- Étape 4 : Travailler de gauche à droite, de haut en bas soustrayez 128 dans chaque bloc de pixels.
- Étape 5 : DCT est appliqué à chaque bloc.
- Étape 6 : Chaque bloc est compressé dans le tableau de quantification.
- Étape 7 : Calculez LSB de chaque coefficient DC et remplacez par chaque bit de message secret.
- Étape 8 : Écrivez l'image stego.
- Étape 9 : calculer l'erreur carrée moyenne (MSE).

Algorithme pour récupérer un message secret :

- Étape 1 : Lire l'image stego.
- Étape 2 : l'image Stego est brisée en 8 × 8 bloc de pixels.
- Étape 3 : Travailler de gauche à droite, de gauche à droite soustrayez 128 dans chaque bloc de pixels.
- Étape 4 : DCT est appliqué à chaque bloc.

- Étape 5 : chaque bloc est compressé à l'aide d'un tableau de quantification.
- Étape 6 : Calculer LSB de chaque coefficient de DC.
- Étape 7 : Récupérer et convertir chaque 8 bits en caractère.

- **La transformée DCT s'exprime par :**

$$DCT(i,j) = \frac{2}{N} c(i)c(j) \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} pixel(x,y) COS\left[\frac{(2x+1)i\pi}{2N}\right] COS\left[\frac{(2y+1)j\pi}{2N}\right]$$

- **Équation 1 : Transformée DCT directe.**

- **Et la transformée DCT inverse s'exprime par :**

$$pixel(x,y) = \frac{2}{N} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} c(i)c(j)\ DCT(i,j) COS\left[\frac{(2x+1)i\pi}{2N}\right] COS\left[\frac{(2y+1)j\pi}{2N}\right]$$

- **Équation 2 : Transformée DCT inverse.**

- **Dans les deux cas, la constante vaut :**

$$C(X)=\begin{cases}\frac{1}{\sqrt{2}} & pour\ x = 0\\ 1 & pour\ x > 0\end{cases}$$

- **Équation 3 : Définition de la constante C.**

- **Un exemple avec un bloc quelconque est :**

$$\begin{bmatrix} 52 & 55 & 61 & 66 & 70 & 61 & 64 & 73 \\ 63 & 59 & 55 & 90 & 109 & 85 & 69 & 72 \\ 62 & 59 & 68 & 113 & 144 & 104 & 66 & 73 \\ 63 & 58 & 71 & 122 & 154 & 106 & 70 & 69 \\ 67 & 61 & 68 & 104 & 126 & 88 & 68 & 70 \\ 79 & 65 & 60 & 70 & 77 & 68 & 58 & 75 \\ 85 & 71 & 64 & 59 & 55 & 61 & 65 & 83 \\ 87 & 79 & 69 & 68 & 65 & 76 & 78 & 94 \end{bmatrix}$$

- **On applique la transformée et on obtient :**

$$\begin{bmatrix} -415 & -30 & -61 & 27 & 56 & -20 & -2 & 0 \\ 4 & -22 & -61 & 10 & 13 & -7 & -9 & 5 \\ -47 & 7 & 77 & -25 & -29 & 10 & 5 & -6 \\ -49 & 12 & 34 & -15 & -10 & 6 & 2 & 2 \\ 12 & -7 & -13 & -4 & -2 & 2 & -3 & 3 \\ -8 & 3 & 2 & -6 & -2 & 1 & 4 & 2 \\ -1 & 0 & 0 & -2 & -1 & -3 & 4 & -1 \\ 0 & 0 & -1 & -4 & -1 & 0 & 1 & 2 \end{bmatrix}$$

II .4.3. Algorithmes :

- **JSteg :** JSteg, créé par Derek Upham [5], L'algorithme JSteg est reconnu comme le premier outil de stéganographie commercialement disponible pour les images JPEG (le premier algorithme qui insère des messages dans les fichiers JPEG compressés). [6]. L'algorithme applique la Transformée de Cosinus Discrete aux blocs d'image et incorpore séquentiellement les données dans les LSB des coefficients DCT. L'incorporation séquentielle et l'absence de toute clé secrète rendent l'algorithme susceptible d'écouter, car seule la connaissance de la procédure d'intégration est suffisante pour décoder le message caché. En outre, JSteg est facilement stéganalyse à l'aide de l'attaque $\chi 2$. En outre, comme l'algorithme utilise le DCT, il est extrêmement nécessaire de traiter les coefficients DCT avec des soins et de l'intelligence sensibles afin d'empêcher l'algorithme de laisser des signatures statistiques significatives [7]. Cependant, JSteg a fourni une capacité d'intégration de 12% [8].

Le principe utilisé est la substitution des bits de poids faible des coefficients DCT quantifié par les bits du message. Il est à noter que les coefficients valant 0 ou1 ne sont pas utilisés

cardes coefficients non nuls apparaîtraient dans les hautes fréquences, ce qui est contraire au principe même de la compression JPEG (qui code efficacement les 0 présents dans les hautes fréquences), cela mènerait donc à des artefacts perceptibles et statistiquement détectables.

Méthode d'insertion :

La méthode d'insertion consiste à remplacer le bit de poids faible de chaque coefficient DCT (différent de 0 ou 1) par un bit du message à insérer. Le format de la chaîne à insérer dans les LSBs avec l'outil JSteg (Fig. 8) est défini comme suit : A est codé sur 5 bits, et renseigne la longueur (en bits) du champ B, B représente une suite de n bits$\in$ {0,31} qui exprime la taille (en octets) du fichier à insérer,

C représente les bits du message à insérer.

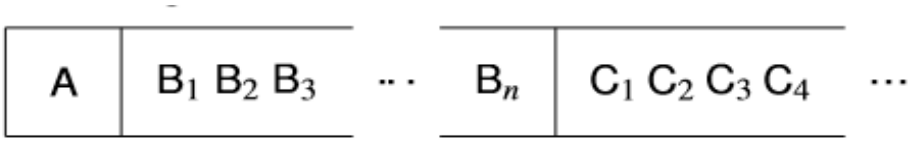

Fig.8 : Format de la chaîne à insérer avec JSteg.

Il faut en effet pouvoir récupérer des informations sur la taille d'un message pour que l'extraction du message puisse être réalisée correctement.

Méthode d'insertion de l'algorithme JSteg :

1. Chaîne à insérer mise au bon format.
2. Début de la compression JPEG de l'image de couverture. Arrêt après l'étape de quantification.
3. Substitution des LSB des coefficients par les bits de la chaîne à insérer dans les coefficients DCT, {0,1}.
4. Fin de la compression JPEG.

Nous pouvons observer sur la(fig.9) que les modifications sont effectuées par paires de valeurs lors de la substitution des LSBs. Par exemple, pour la paire (2,3), si un 0 doit être inséré dans un coefficient dont la valeur est 2, il n'y a pas de modifications car le LSB de 2 est 0. En revanche un0doitêtreinsérédansun3, le bit de poids faibleétant1, le coefficient est

modifié en substituant le LSB valant 1 par 0. La nouvelle valeur du coefficient est donc 2. De même, si un 1 doit être inséré dans un 2, le coefficient devient 3.

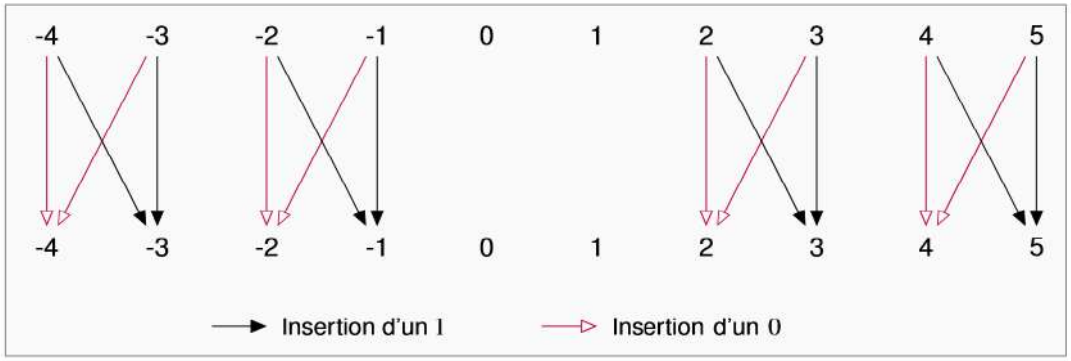

Fig. 9 : Modifications des coefficients DCT par JSteg.

- **F5 :** L'algorithme F5 a été inventé par Andreas Westfeld, l'algorithme F5 a été proposé comme une technique de stéganographie qui permet une plus grande capacité d'intégration et une meilleure sécurité en même temps [8]. Le F5 diffère de la plupart des autres techniques de stéganographie dans le fait qu'il n'écrase pas les LSB des coefficients / pixels DCT plutôt qu'il augmente / diminue la valeur des coefficients DC en fonction des besoins. L'algorithme prend en considération que le basculement des LSB soit au niveau du pixel, soit au niveau du coefficient de courant continu altère les propriétés statistiques de l'image et peut servir de moyen d'analyser l'algorithme. F5 utilise un chevauchement permutai et un codage matriciel pour disperser l'effet d'encastrement et intégrer les données respectivement. F5 est la première implémentation de la méthode de codage matricielle. F5 s'intègre à un taux de 3,8 bits par changement et est sécurisé contre la plupart des attaques statistiques comme l'attaque d'histogramme, l'attaque $\chi 2$, la détection de blocage, etc. De plus , **elle** : possède une capacité d'intégration élevée. Cependant, F5 est resté un algorithme difficile à casser jusqu'à Fridrich et al. F5 estimé en estimant l'histogramme original de l'image de couverture à partir de l'image stego [10]. Il se décompose en décompressant l'image stego dans le domaine spatial, en le recadrant de 4 pixels dans les deux sens et en recomprimant en utilisant le même facteur de qualité que l'image stego.

L'implémentation de l'algorithme est la suivante :

Algorithme F5 : 1. Début de la compression JPEG de l'image de couverture.

Arrêt après l'étape de quantification.

2. Initialisation du générateur de nombre pseudo-aléatoire avec une clé.

3. Calcul de la permutation qui désignera le chemin à suivre pour l'insertion du message, en fonction d'un nombre aléatoire calculé précédemment et du nombre de coefficients DCT, à l'aide du générateur.

4. Calcul des paramètres du codage de Hamming en fonction de la capacité du medium de couverture et du message à insérer, afin de répartir au mieux les modifications.

5. Insertion du message avec le codage de Hamming.

6. Fin de la compression JPEG.

Insertion d'un message :

Le message à insérer est découpé en paquets de k bits. L'insertion du message se fait de la manière suivante :

Méthode d'insertion pour F5 :

1. Remplir un tampon avec n coefficients DCT non nuls.

2. Calculer le syndrome s du tampon.

3. Sommer k bits du message avec s.

4. Si la somme est nulle, le tampon n'est pas modifié.

Sinon la somme correspond à l'index du coefficient du tampon dont il faut décrémenter la valeur absolue.

5. Si un effondrement apparaît, retour à l'étape 3 en éliminant le 0 produit et en prenant un coefficient non nul supplémentaire dans le tampon.

Sinon avancer aux prochains coefficients non nuls situés après le tampon.

S'il y a encore des données à insérer, recommencer depuis l'étape 1.

- **OutGuess :** L'algorithme a été développé par N. Provos et al. [6] en tant qu'amélioration de la méthode JSteg existante. Outguess utilise un PRNG (Pseudo Random Number Generator) pour randomiser les pixels dans lesquels l'encastrement est supposé être effectué. Il ignore l'incorporation en coefficients DCT avec les valeurs 0 et 1 car ils forment une paire de valeur lorsque leur LSB change et il n'existe aucun moyen de distinguer entre un coefficient DCT zéro et un zéro stéganographique. L'algorithme, après l'incorporation, modifie les coefficients DCT non modifiés pour préserver l'histogramme de l'image originale. Ainsi, OutGuess est à l'abri des attaques comme l'attaque visuelle, l'attaque d'histogramme et l'attaque $\chi 2$. Cependant, Fridrich et al. [9] ont réussi à stéganalyse OutGuess en calculant le blocage de l'image. L'algorithme de stéganalyse pour OutGuess utilise le fait que, comme OutGuess utilise l'incorporation LSB des coefficients DCT et qu'il modifie aléatoirement les coefficients quantifiés, la discontinuité spatiale à la limite de chaque bloc 8X8 augmentera.

II. 5.Logiciel de stéganographie JPEG :

Les systèmes logiciels ont été développés pour intégrer les messages stego dans les images. Ces systèmes utilisent certaines des techniques stéganographique expliquées. Beaucoup de systèmes disponibles sont gratuits et peuvent être téléchargés en lecture seule, parmi ceux-ci JSteg, JPHide, S-Tools et autres. Ces systèmes ont des forces et des faiblesses qui ont été explorées dans la littérature.

Dans cette section, nous explorerons JSteg-JPeg.

- **JSteg-Jpeg :** JPeg-JSteg est disponible en articles gratuits et peut être facilement téléchargé à partir de sites de stéganographie sur Internet. Le logiciel JPeg-JSteg (JSteg) a été développé par Derek Upham. JSteg s'exécute à l'invite DOS en utilisant les commandes cjpeg et djpeg. Bien que JSteg produit des images stego sous forme de fichiers jpeg, il ne lit pas le format du fichier jpeg. Les images de couverture sont converties en utilisant la commande DOS djpeg vers le fichier d'image Targa (.tga extension de fichier). L'image de couverture convertie au format d'image Targa et le fichier texte caché sont entrés dans JSteg à l'aide de la commande DOS cjpeg qui produit l'image stego. L'algorithme utilisé dans JPeg-JSteg remplace séquentiellement le LSB des coefficients DCT des images stego avec des bits du message caché à intégrer. Selon Niels Provos et Peter Honeyman, l'algorithme utilisé par JSteg peut être décrit par le pseudo code suivant [4] :

Msg = hidden message Get next LSB from message

Pic = cover image Replace DCT LSB with message LSB

Output = stego image End if

While more characters in msg do: DCT into stego image

Get next DCT coefficient End While.

If DCT coefficient! =0 and DCT coefficient! =1

L'algorithme utilisé dans JPeg-JSteg insère les données secrètes stéganographique dans l'image de couverture pendant l'algorithme de compression jpeg après la DCT et la quantification des coefficients DCT et avant l'étape de codage Huffman. L'algorithme incorpore également un champ de longueur dans l'image stego qui sert à extraire le message caché.

II .6.Stéganalyse :

Steganalysis se réfère à l'ensemble des techniques conçues pour détecter les contenus cachés dans les médias numériques.

II .6.1. Analyse χ2 : ont une analyse χ2 actuelle pour détecter les messages cachés. Ils ont montré qu'un canal de couleur L-bit peut représenter 2L des valeurs possibles.

Si nous divisons ces valeurs en paires 2L-1 qui ne diffèrent que dans les LSB, nous considérons tous les modèles possibles de bits voisins pour les LSB. Chacune de ces paires s'appelle une paire de valeur (PoV) dans la séquence.

Lorsque nous utilisons tous les champs LSB disponibles pour cacher un message dans une image, la distribution des valeurs impaires et égales d'un PoV sera la même que la distribution 0/1 des bits de message. L'idée de l'analyse χ2 est de comparer la distribution de fréquence théoriquement attendue des PoV avec les observés réels. Cependant, nous n'avons pas l'image originale et donc la fréquence attendue. Dans l'image d'origine, la fréquence théoriquement attendue est la moyenne arithmétique des deux fréquences dans un PoV. Comme nous le savons, la fonction d'intégration affecte uniquement les LSB, donc cela n'affecte pas la distribution du PoV après un encastrement. Compte tenu de cela, la moyenne arithmétique reste la même dans chaque PoV, et nous pouvons dériver la fréquence attendue par la moyenne arithmétique entre les deux fréquences dans chaque PoV.

Ont montré que nous pouvons appliquer le χ2 (chi carré de test) sur ces Pics pour détecter les messages cachés. La formule générale de l'χ2 est [12] :

$$\chi^2 = \sum_{i=1}^{\nu+1} \frac{(f_i^{obs} - f_i^{exp})^2}{f_i^{exp}},$$

Équation 4 : La formule générale de l'χ2

Où ν est le nombre de PoVs analysés, $f_i^{o_{bs}}$ et $f_i^{e_{xp}}$ sont les fréquences observées et les fréquences attendues respectivement.

La probabilité de se cacher, ph, dans une région est donnée par les compliments de la distribution cumulative

$$ph = 1 - \int_0^{\chi^2} \frac{t^{(\nu-2)/2} e^{-t/2}}{2^{\nu/2}\Gamma(\nu/2)} dt,$$

Équation 5 : La probabilité de se cacher ph.

Où Γ (·) est la fonction Euler-Gamma. Nous pouvons calculer cette probabilité dans différentes régions de l'image.

Cette approche ne peut détecter que les messages séquentiels cachés dans les LSB des premiers pixels disponibles, puisqu'il considère uniquement la valeur des descripteurs. Il ne prend pas en compte que, pour différentes images, la valeur de seuil pour la détection peut être assez distincte [15].

Simplement mesurer les descripteurs constitue une mesure statistique de faible ordre. Cette approche peut être vaincue par des techniques qui maintiennent des profils statistiques de base dans le processus de dissimulation [15, 14].

Des techniques améliorées telles que la Randomisation Progressive (PR) [13] traitent des problèmes de statistiques d'ordre inférieur en regardant le comportement des descripteurs selon des régions sélectionnées (régions caractéristiques).

II .6.2. Zhang et Ping :

En 2003, T. Zhang and X. Ping [16] ont proposé une méthode afin de détecter l'utilisation de JSteg (version séquentielle et aléatoire).

Deux ensembles de valeurs L et R sont définis de la manière suivante, pour i un coefficient DCT :

$$L = \{i > 0 | i \text{ pair}\} \cup \{i < 0 | i \text{ impair}\},$$

$$R = \{i > 0 | i \text{ impair}\} \cup \{i < 0 | i \text{ pair}\}.$$

La proportion p de la capacité utilisé par JSteg randomisé est :

$$p = \frac{1}{h(1)} \cdot \left(\sum_{r \in R} h(r) - \sum_{l \in L} h(l) \right),$$

Équation 6 : La proportion p de la capacité.

Avec h(k) qui représente le nombre de coefficients DCT ayant pour valeur k.

II .6.3. Logiciel de Stéganalyse :

Les systèmes logiciels ont également été développés pour détecter les messages stego incorporés dans des images utilisant la stéganographie. Beaucoup des outils de stéganographie disponibles sont spécifiques au logiciel utilisé pour intégrer le message stego. Un exemple de ce logiciel est **StegDetect**. StegDetect a été développé par Niels Provos.

StegDetect peut être utilisé pour détecter les images jpeg qui ont été modifiées à l'aide de JSteg, Outguess, F5 et autres. Les outils auxquels StegDetect ciboule utilisent toutes une variation de bits de modification après l'application de la transformée DCT. [17] StegDetect utilise la connaissance de la technique utilisée par le logiciel de sténographie pour intégrer le message dans son mécanisme de détection. StegDetect peut être téléchargé sous DOS sous forme de données gratuites depuis Internet.

II. 7. Conclusion :

Pour masquer les informations confidentielles, la stéganographie peut être utilisée efficacement. L'objectif de toute méthode de Steganographic est de cacher des informations secrètes maximales qui sont à l'abri des attaques externes et ne doit pas non plus transmettre le fait que le support de couverture porte des informations secrètes. Cette thèse a utilisé la technique de substitution LSB pour le domaine temporel et différentes transformées pour le domaine fréquentiel.

Dans les méthodes de domaine spatial, on peut avoir une capacité de charge utile élevée. Les techniques de détection de bord utilisées dans les méthodes actuelles ne reconnaissent pas les nuances de la région de bord, qui peuvent aussi être considérées comme incorporant les bits supplémentaires. Le nombre de pixels de bord peut être augmenté en identifiant les bords et les nuances des bords.

Les méthodes de domaine Transformé sont très robustes. Ils intègrent les bits de message dans les régions qui sont très insensibles à la compression, à la filtration ou à la transformation. Mais leur capacité de charge utile est faible. En outre, les qualités visuelles de l'image Stego sont médiocres. Le domaine spatial est mieux comparé au domaine transformé.

Chapitre III :
stéganographie TCP/IP

III).1.Introduction :

Depuis que Lampson a proposé le concept de canal secret en 1973, canal caché a été considérée comme une question importante dans le domaine de la sécurité de l'information. Selon Lampson, "un canal de communication est caché s'il n'est ni conçu ni destiné à transférer de l'information". Un travail ultérieur définit un canal caché comme « un canal de communication qui permet à un processus de transférer des informations d'une manière qui viole la politique de sécurité du système ». Cette définition est maintenant plus communément acceptée. Initialement, les canaux secrets ont été identifiés comme une menace pour la sécurité sur les systèmes monolithiques, c'est-à-dire mainframes, mais récemment l'accent a été déplacé vers les canaux cachés dans les protocoles de réseau informatique.

Une analogie commune employée pour discuter de la dynamique des communications secrètes est connue comme le « problème du prisonnier ». Il s'agit de deux prisonniers, appelés ici pour Simplicité Alice et Bob, qui ont besoin de communiquer les uns avec les autres afin de concevoir un plan d'évacuation. Elle implique également une directrice, Wendy, qui supervise toutes les communications des interprètes, et peut les surveiller de deux façons :

- Elle peut examiner tous les messages, et les laisser passer ou les nier sur la base de ce qu'elle voit. Il s'agit d'une approche passive.
- Elle peut modifier légèrement le message pour s'assurer que ce n'est pas précisément ce qui a été envoyé, sans changer la signification du message. En modifiant le message, il est supposé qu'elle pourrait frustrer toute tentative d'incorporer un message secret dans la communication. Il s'agit d'une approche active.

Idéalement, les prisonniers trouvent un moyen de communiquer qui ne suscite pas de soupçons du directeur. Mais le directeur doit accepter qu'il existe un risque qu'une certaine communication secrète puisse être tentée, et poser et l'hypothèse de la façon dont il pourrait fonctionner. Covert canal est différent de la cryptographie que son objectif principal est de cacher l'existence de la transmission tandis que la cryptographie ne masque pas l'existence du message, mais le transformer dans une forme qui est seulement lisible par le récepteur. En cryptographie, il n'est pas question de masquer la communication. Canal caché dans les protocoles réseau informatique et la stéganographie sont étroitement liés, mais souvent confondus. La stéganographie implique la dissimulation de l'information dans un contenu

audio, visuel ou textuel. Alors que la stéganographie nécessite une certaine forme de contenu comme couverture, le canal caché nécessite un certain protocole de réseau en tant que porteur.

Etant donné que les canaux de communication en réseau sont des canaux de communication qui ne sont pas conçus ni destinés à exister, les flux de communication doivent être intégrés dans des canaux autorisés. Ils peuvent être basés sur des protocoles existants à partir de couches basses OSI (par exemple, IP, TCP, UDP) vers des couches hautes d'OSI (par exemple, HTTP, SMTP). L'idée générale des canaux secrets repose sur l'idée que l'information peut être transférée dans des champs redondants ou inutilisés de protocoles de réseau. La fiabilité, la rapidité et la robustesse des protocoles de communication permettent la mise en œuvre de ces canaux sur les réseaux. Depuis que les analystes de sécurité de réseau ont commencé à penser à la communication de canal secrète, deux termes ont été introduits, le stockage et le timing canal caché. Dans le canal caché de stockage, l'un des processus écrit directement ou indirectement dans un emplacement de stockage particulier alors que d'autres lectures de processus forment cet emplacement. Plusieurs d'outils utilisent les protocoles TCP, IP, ICMP et HTTP pour établir des canaux cachés de stockage. Dans ces protocoles, des champs inutilisés sont utilisés pour transmettre les informations. D'une certaine façon, la stéganographie peut être considérée comme une forme de canal de stockage caché. Le canal temporel de synchronisation implique de modifier les caractéristiques temporelles pour masquer les informations. Plus précisément, il peut être fait en modulant les délais inter-paquets. Dans cet travaille, nous allons détecter les canaux cachés dans les trame TCP/IP (champs TCP ISN et ID IP).

III).2. Paquets et protocoles réseau :

Les informations stockées sur des supports électroniques sont normalement stockées à l'aide d'un code binaire. La norme la plus utilisée est l'ASCII. Dans le domaine des réseaux pour transmettre des informations, les octets sont regroupés en ensembles plus grands appelés paquets.

Pour grouper plusieurs octets dans des paquets, il est nécessaire que les moyens de confinement soient établis. Encapsulation définissent à la fois le début et la fin du paquet ainsi que d'autres attributs qui permettent d'apporter cohérence au paquet. Cette création de paquet suit certaines règles déjà établies appelées protocoles. Il existe plusieurs protocoles à

diverses fins pour l'échange d'informations sur internet ; La norme plus courant est appelée TCP / IP.

Le protocole TCP / IP ajoute les données à communiquer, certaines informations connues sous le nom d'en-tête qui décrivent le type d'information et la manière de la traiter.

Certaines parties ou champs de l'en-tête d'un paquet TCP / IP ne sont généralement pas utilisés dans la plupart des messages transmis. Dans ces champs, il est possible de cacher des informations.

Pour masquer les informations dans les en-têtes de chaque paquet IP, il est nécessaire de considérer que ce protocole consiste réellement en un ensemble de protocoles et tous sont présents à la fois dans l'émetteur et le récepteur. Cette pile de protocoles est présente dans tous les ordinateurs utilisant internet ; Depuis sa création il y a plus de trente ans, certains champs ne sont plus utilisés ou peuvent être modifiés sans modification de l'information ou sans affecter la bonne transmission des données.

III).3. Les canaux cachés dans les protocoles tcp/ip :

III) .3.1. IP :

Version 4 du protocole Internet, c'est-à-dire IPv4 est un protocole de couche réseau. Les rubriques sont destinées à fournir des données essentielles au destinataire de l'information. Les en-têtes IP contiennent des informations pour que les paquets soient correctement adressés. C’est un support intéressant pour les canaux secrets. L'en-tête du datagramme IP est représenté sur la fig. 10.

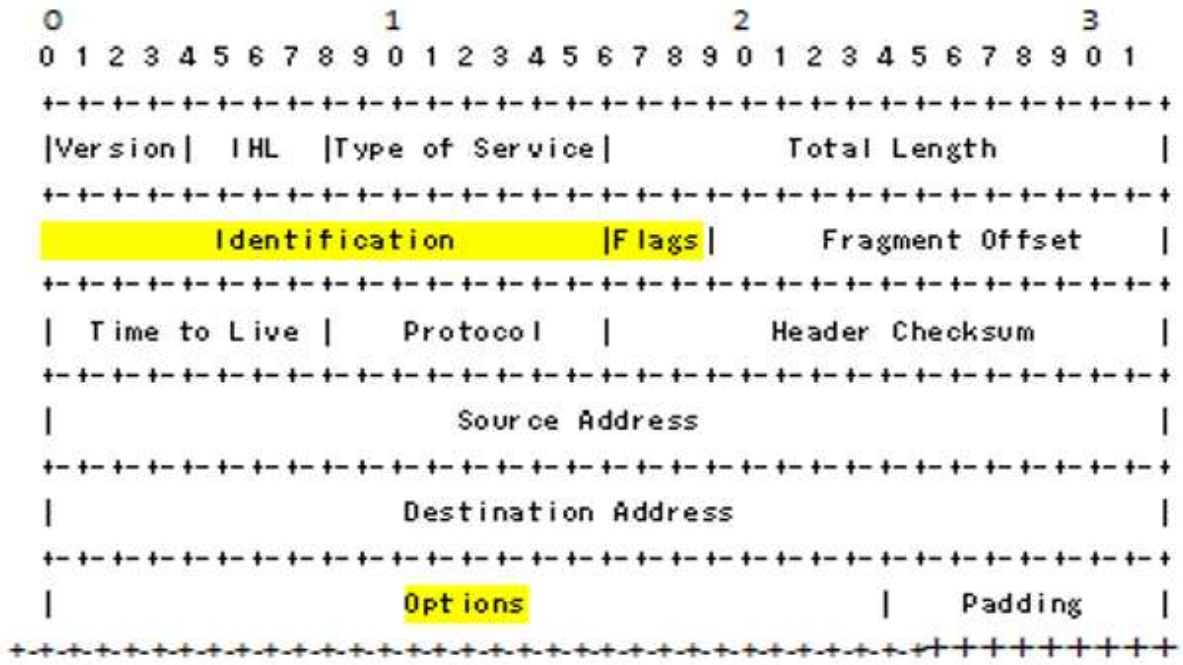

Fig.10 : En-tête IPv4

- **Champ "IP Identification" :**

Le champ d'identification 16 bits est utilisé pour identifier de façon unique le datagramme IP pour le réassemblage du datagramme en cas de fragmentation. La valeur de ce champ doit être choisie au hasard par la source. Un adversaire peut cacher 16 bits de données dans ce champ et l'envoyer à tout autre système en réseau. Rowland a proposé d'utiliser le champ d'identification IP (IPID) pour construire des canaux secrets [20]. La figure 11 montre un processus de canalisation unidirectionnelle sur un champ d'identification IP.

- **Champ "IP flags" :**

Un champ dans l'en-tête IP de 3 bits utilisé en fragmentation, le premier bit est réservé ; Le deuxième bit est appelé ne pas fragmenter (DF) ; Si la valeur de ce bit est un, le paquet ne doit pas être fragmenté, une valeur de zéro signifie que le paquet peut être fragmenté si nécessaire. Le troisième bit est appelé plus fragment ; Une valeur d'un indique que ce paquet n'est pas le dernier bit, mais il y a plus de fragments après lui et si zéro signifie qu'il est le dernier fragment ou qui est unique. Mukul exploite la redondance qui se produit quand il n'y a pas de fragmentation pour cacher un peu dans DF.

➢ **Champ "IP option" :**

Le champ d'option 24 bits est facultatif pour chaque datagramme IP. L'option IP comprend des dispositions relatives aux horodatages, à la sécurité et au routage spécial. Mais en plus d'être facilement détectable, les paquets avec cette option présente peuvent voyager au maximum 20 hots, donc il est peu utile dans l'Internet ouvert.

➢ Il est important de noter que certains champs d'en-tête sont sujets à changement sans affecter le routage. L'un d'eux est l'identifiant IP. Lorsqu'un paquet de données est trop grand, il est nécessaire de le fragmenter et tous les segments doivent avoir le même identifiant IP, qui normalement sera augmenté par unité, mais n'importe quel nombre peut être utilisé et le protocole fonctionnera toujours correctement lors de l'assemblage du paquet d'origine.

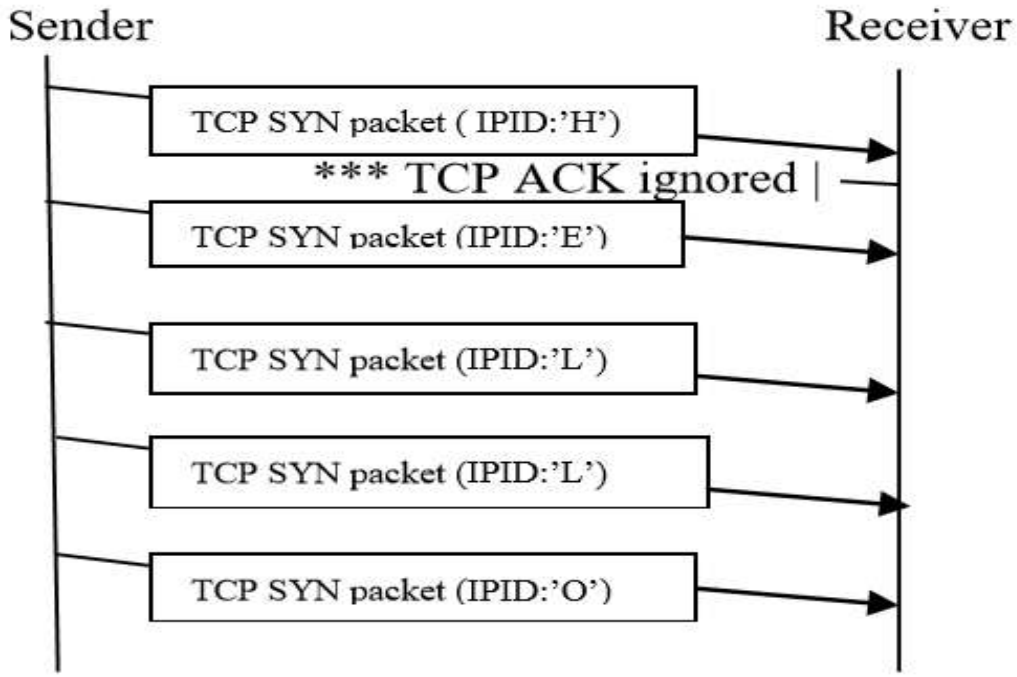

Fig.11 : canal cachée utilisent ip identification champ.

III) .3.2. TCP :

Le protocole de contrôle de transmission, TCP, est utilisé pour la transmission des données fiables ; Tous les ordinateurs connectés à Internet utilisent TCP. Dans les en-têtes de TCP, les numéros de séquence « ISN » et d'accusé de réception « ACK » sont utilisés pour indiquer

combien de données sont envoyées et combien ont été reçues. Au début de la transmission, les deux numéros sont arbitrairement assignés, de sorte que le premier paquet envoyé peut contenir des informations cachées dans ces numéros, parce qu'à cette occasion ils n'ont aucun but.

L'en-tête d'un paquet TCP est représenté à la figure 12.

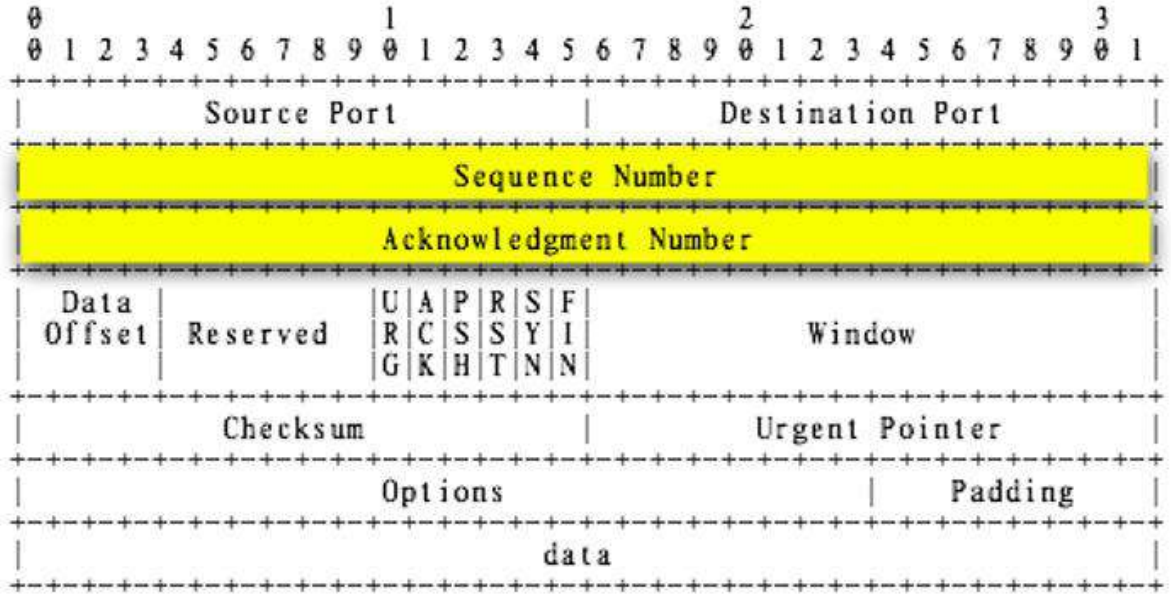

Fig.12 : En-tête de paquet TCP.

- **Champ "TCP sequence number ISN":**

Le champ de numéro de séquence TCP 32 bits est utilisé comme un numéro d'identification pour prévoir le réassemblage de paquets à l'arrivée à l'extrémité du récepteur et la fiabilité de l'aide par demande de retransmission de paquets individuels. Le premier paquet dans la session TCP contient un numéro de séquence aléatoire initial, ou ISN. L'hôte récepteur reconnaît généralement sa réception en répondant avec un paquet SYN / ACK, en utilisant ISN + 1 comme numéro d'accusé de réception. Au lieu d'utiliser un ISN aléatoire, cependant, ce champ peut également contenir une valeur non aléatoire sans perturber le mécanisme TCP. Nous pouvons cacher jusqu'à 32 bits de données dans ce champ et l'envoyer à tout autre système en réseau. La figure 13 montre un scénario d'exemple pour la communication secrète utilisant le champ de numéro de séquence TCP.

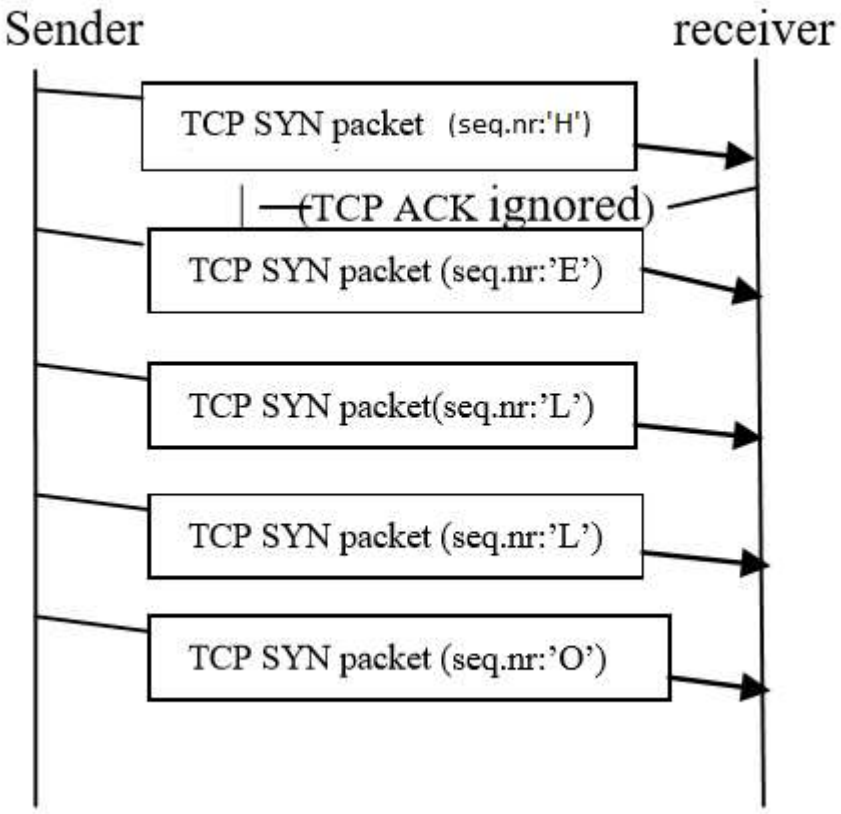

Fig.13 : Canal cachée utilisant le numéro de séquence TCP.

III).4. Stéganographie dans les paquets TCP / IP :

On suppose qu'A et B partagent ouvertement des informations sur un réseau informatique et utilisent des données cachées incorporées dans les protocoles TCP / IP pour communiquer des informations secrètes. Les données sont cachées par un algorithme stéganographie qui prend comme entrée un message secret Ck, une séquence de paquets réseau Pk (connue sous le nom de séquence de paquets de réseau secrète) et éventuellement une clé secrète pour générer une séquence stego de paquets réseau Sk (contenant Pk en portant Cache Ck). Le message secret Ck, caractérisé en tant que séquence de paquets réseau Sk est envoyé par le réseau informatique à B et il se déplace à travers un canal non idéal. B estime les informations secrètes pour produire C * k (Fig.14).

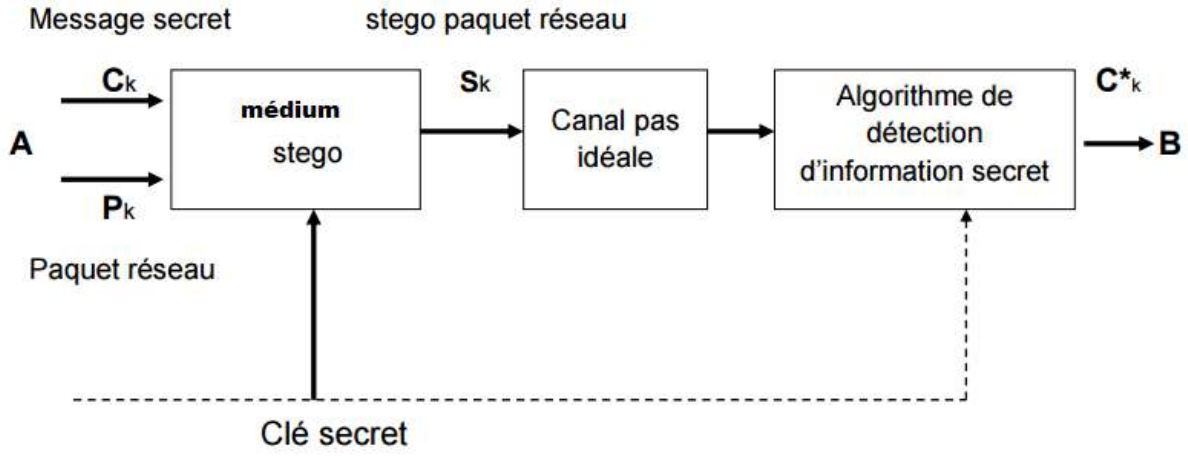

Fig.14 : Transfert de l'information d'A vers B en utilisant la stéganographie.

III).5. Architecture du système stéganographie :

Dans cette section, la conception d'un système stéganographie est appelé Mukul [22]. Ce système est conçu comme une application stéganographie sur des paquets TCP / IP pour envoyer un message secret d'un hôte source vers un hôte de destination en utilisant comme en-têtes de porteurs des paquets TCP / IP traversant le réseau, avec la particularité d'éviter toute suspicion. La conception du système Mukul est composée des modules suivants : ANA qui traite de la dissimulation et l'envoi du message, BOB qui traite de la réception et la récupération du message.

III) .5.1.Description du module ANA :

Le module ANA se compose essentiellement d'un sniffer et d'un injecteur de paquets. Les principales tâches de l'ANA sont de coder le message à envoyer secrètement, de capturer les paquets TCP / IP qui traversent le réseau et de sélectionner les paquets appropriés pour les écrire des bits secrètes. L'injecteur prend également soin d'envoyer sur le réseau stego-paquets pour transmettre le message secret à l'hôte de destination.

La fonctionnalité de ce module est décrite dans la séquence suivante : Il commence à lire le message secret en format texte brut et à le coder pour la transmission. De l'ANA, à travers un

sniffer, les paquets réseau en mode promiscuité sont lus avec l'intention de capturer tous les paquets qui traversent le réseau.

Les paquets capturés sont analysés afin de sélectionner ceux qui conviennent à la dissimulation des données. Les attributs de paquet fournissant cette éligibilité sont : Ils sont destinés à la destination de l'information cachée, ont des bits inutilisés et ne portent pas de données segmentées, c'est-à-dire qu'ils sont uniques.

Le message secret est reçu et les bits possibles sont cachés dans les champs d'en-tête IP et TCP identifiés comme étant appropriés pour l'expédition.

A partir d'ANA, à travers une buse, les stego-paquets sont injectés au réseau avec des données cachées dans des en-têtes et d'autres données.

Dans la Fig. 15, le diagramme avec la fonctionnalité ANA est présenté.

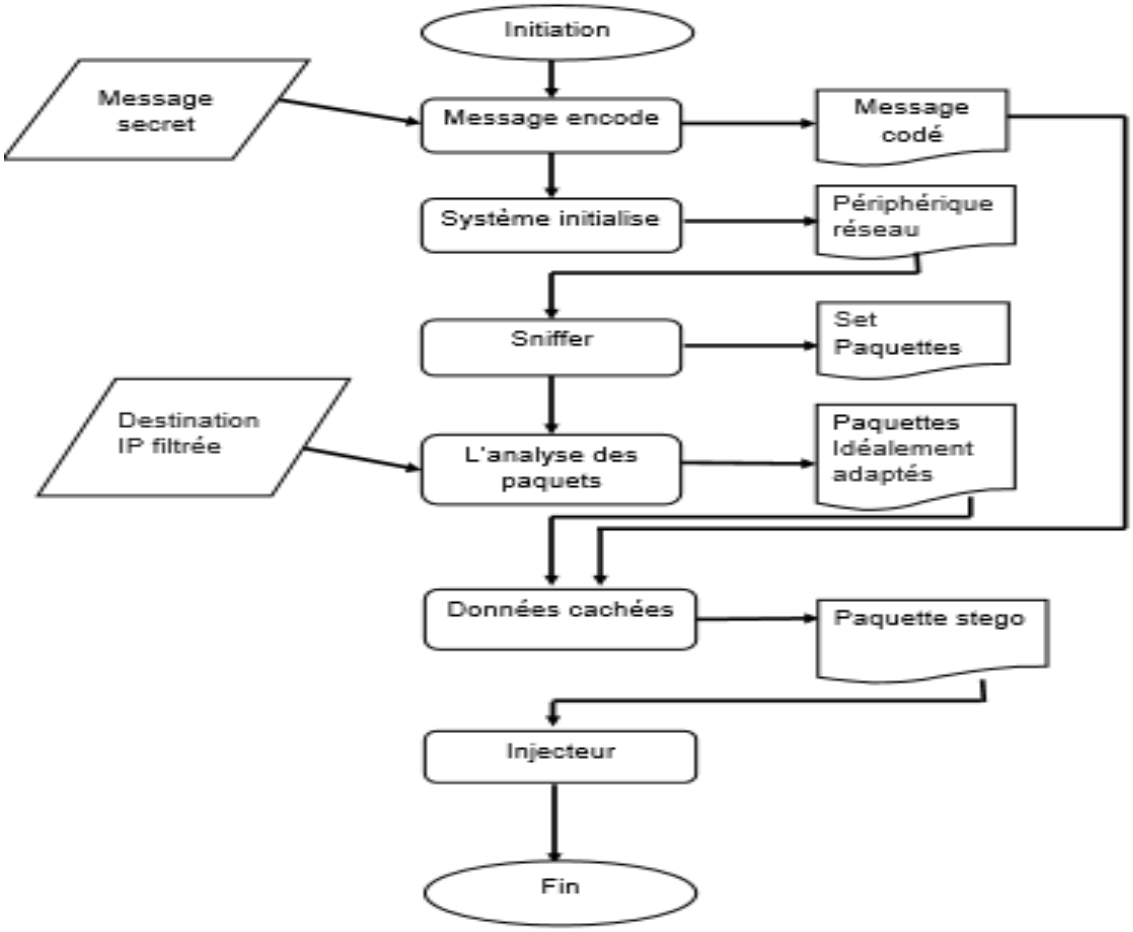

fig.15 : le diagramme avec la fonctionnalité ANA.

III) .5.2Description du module BOB :

Le module BOB consiste essentiellement en un sniffer qui renifle le réseau pour des paquets contenant des bits secrets pour les extraire, décrypter et récupérer le message original.

La fonctionnalité de ce module est décrite ci-dessous :

Dans le module BOB, le sniffer fonctionne pour capturer des paquets TCP / IP dirigés spécifiquement vers ce nœud (mode normal) et dont le nœud source est spécifiquement le nœud émetteur où ANA est en cours d'exécution.

Lorsque tous les paquets ont été capturés au niveau du nœud récepteur, BOB décompresse le message caché et l'affiche en texte clair.

Dans la Fig. 16 le diagramme avec la fonctionnalité BOB s'affiche.

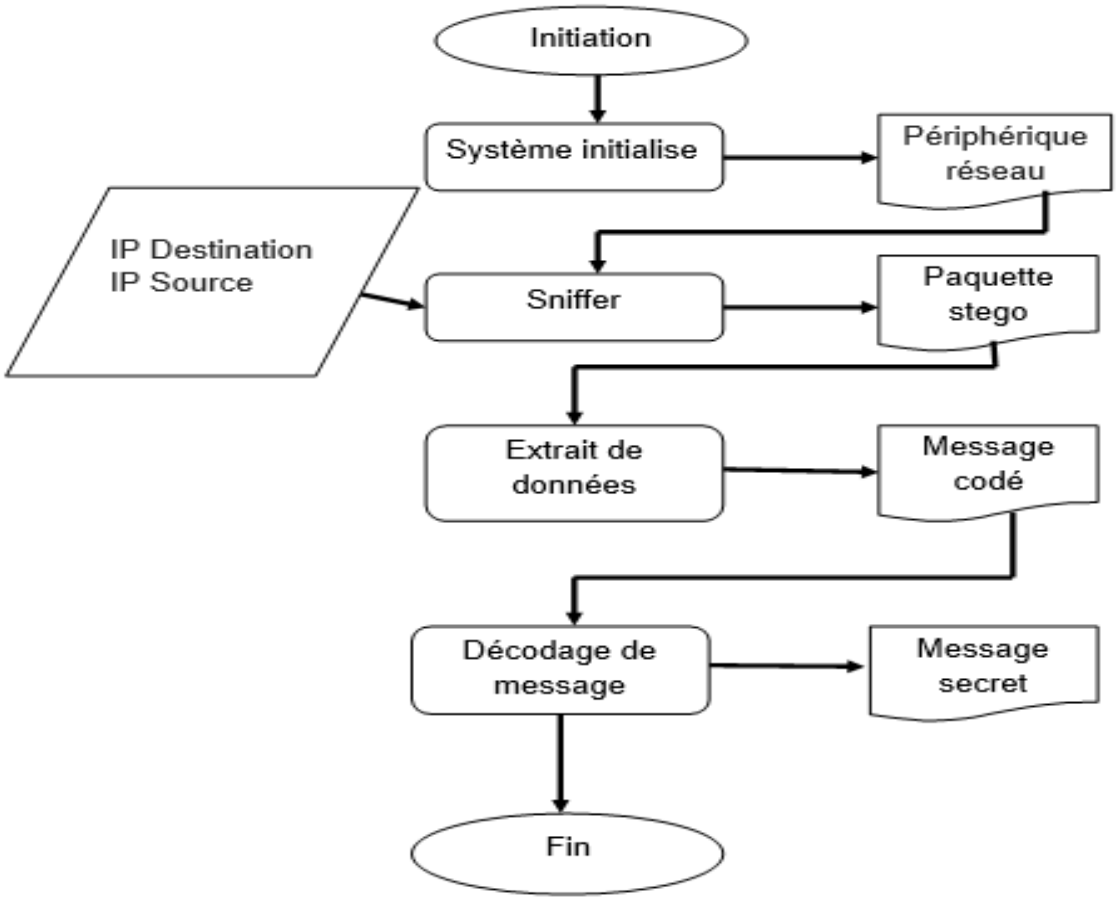

Fig.16 : le diagramme avec la fonctionnalité BOB.

III).6. Mécanismes de détection de canaux cachés TCP / IP :

III) .6.1. SVM :

T. Sohn a proposé un mécanisme de détection basé sur la machine à vecteur de soutien pour détecter le canal caché dans l'identification IP forgée et le champ TCP ISN. Ils ont utilisé le programme Covert_tcp pour Linux 2.4 comme un outil de génération de canaux cachés pour l'en-tête TCP / IP. Les paquets eux-mêmes sont masqués comme trafic TCP / IP commun. Au moment de la formation SVM, ils ont collecté des paquets TCP / IP normaux à l'aide d'un outil de vidage tcp et de paquets TCP / IP anormaux (y compris des champs cachés) générés à partir de « covert_tcp » et ensuite testés pour le champ Identification IP de l'en-tête IP et du champ numéro de séquence de l'en-tête TCP.

III) .6.2. Analyse des canaux cachés et prédiction des attaquants :

Le canal caché TCP / IP nécessite une modification des champs d'en-tête de paquet pour transférer des informations sans affecter la communication normale. Les informations peuvent être intégrées à l'aide de la modification de certains champs d'en-tête ou en utilisant des champs d'en-tête qui nécessitent des nombres aléatoires. On peut utiliser des champs d'en-tête inutilisés pour coder les informations à transmettre en cachette.

Pour ce faire, nous sélectionnons deux champs obligatoires, le champ ID IP du champ IPv4 et TCP ISN de TCP pour incorporer des données cachées. Le caractère aléatoire de ces champs rend les attaquants difficiles à prédire ces nombres.

Au début, les paquets de données sont capturés par notre outille « Wireshark 1.8.6 » et stockés dans une base de données. Ensuite, un jeu de données de caractéristiques est créé et utilisé pour la formation. Le jeu de données de caractéristiques est obtenu en utilisant la méthode ci-dessus et un outil nommé « NetScan Pro » outil qui est un générateur de paquets outil utilisé pour générer des paquets TCP avec des informations cachées intégrées dans ISN et les champs d'en-tête IP.

III) .7.Comparaison :

- **IMAGE JPEG :**

Le processus d'intégration d'informations pendant la compression JPEG entraîne une image stego avec un haut niveau d'invisibilité, puisque l'intégration se fait dans le domaine de la transformation. JPEG est le format de fichier image le plus populaire sur Internet et les tailles d'image sont petites en raison de la compression, ce qui en fait l'algorithme le moins suspect.

Capacité : En raison de l'utilisation des coefficients DCT (compression d'image), la capacité d'encastrement fournier par la stéganographie JPEG est petit.

Sécurité et robuste : Mais la sécurité dans la stéganographie JPEG est très élève il est difficile de faire la stéganalyse sur les stéganographie qui utilisé transformes domaines

(fréquentiel Domain). En raison de l'utilisation d'une équation mathématique ou des algorithmes avec une hauteur robuste. JPEG est exploitée pour rendre les modifications de l'image invisibles à l'œil humain.

- **TCP/IP :**

Dans la stéganographie par tram tcp/ip nous avons des champs que nous utilisons pour cacher des informations. D'entre eux (IP Identification=16 bits et TCP sequence Number ISN=32 bits), Mais ne pas oublier que l'espace pour seul paquet. De là, quelle que soit la taille du message qu'il envoyer ou diviser un group des paquets et puis conclure que la stéganographie par tram tcp/ip nous assure plus d'espace. D'autre part, des informations sécrètes menace de stéganographie par les jeunes professionnelles par ce logiciel utilisé dans l'analyse de réseau comme (Wireshark). Par conséquence, nous devons soutenir la stéganographie tcp/ip avec la cryptographie pour protéger le message. Ce qui signifie connaitre l'existence d'un message mais ne connaissant pas le contenu du message.

III) .8. Conclusion :

Actuellement, la communauté scientifique internationale développe de nouveaux mécanismes de protection des données en raison de l'importance et de la valeur de l'information dans les institutions.
Ce travaille présente la conception d'un système stéganographie qui fournit un outil pour cacher des données dans des paquets réseau TCP / IP comme une alternative sûre et imperceptible de transmission de données.

La quantité énorme de données transmises sur Internet en utilisant les protocoles TCP / IP le rend idéal comme support pour des informations secrètes. Les attaques de chaînes cachées deviennent une menace potentielle pour Internet. Un canal caché utilisant une combinaison inutilisée de champs d'indicateur d'en-tête TCP / IP, des champs réservés ou la modification de certains champs d'en-tête peuvent être facilement détectés. Détecter les canaux cachés intégrés dans les ISN et les ID IP sont les canaux secrets les plus difficiles à détecter en raison de leur comportement aléatoire

Chapitre V:
Conception & Implémentation

V .1. Introduction :

Dans ce chapitre nous allons présenter notre messagerie application à travers des canaux caché dans tcp/ip. Qui inclut stéganographie dans les réseaux.

V .2. Les outillés utilisés :

V .2.1.Les champs utilisés :

- Champ "IP Identification".
- Champ "TCP sequence number ISN".

V .2.2.les algorithms de cryptage:

En raison de faiblesse du stéganographie tcp/ip contre la détection visuelle, nous renforçant cette technique avec algorithme du cryptage.

- **A**dvanced **E**ncryptions **S**tandard (**AES**).

V .2.3. le langage de programmation:

❖ **C# : (**logiciel de développement « Visual Studio »).

C# est un langage élégant et de type sécurisé orienté objet qui permet aux développeurs de créer toute une gamme d'applications sûres et solides exécutées sur .NET Framework. Vous pouvez utiliser C# pour créer des applications clientes Windows, services Web XML, composants distribués, applications client-serveur, applications de base de données et bien plus encore. Visual C# fournit un éditeur de code avancé, des concepteurs d'interface utilisateur pratiques, un débogueur intégré et de nombreux autres outils pour faciliter le développement d'applications basées sur le langage C# et le .NET Framework.

V .3. Application de messagerie :

Dans notre application, nous avons mis l'accent sur la simplicité et la facilité d'utilisation.

La figure [17] représente l'interface de cette application.

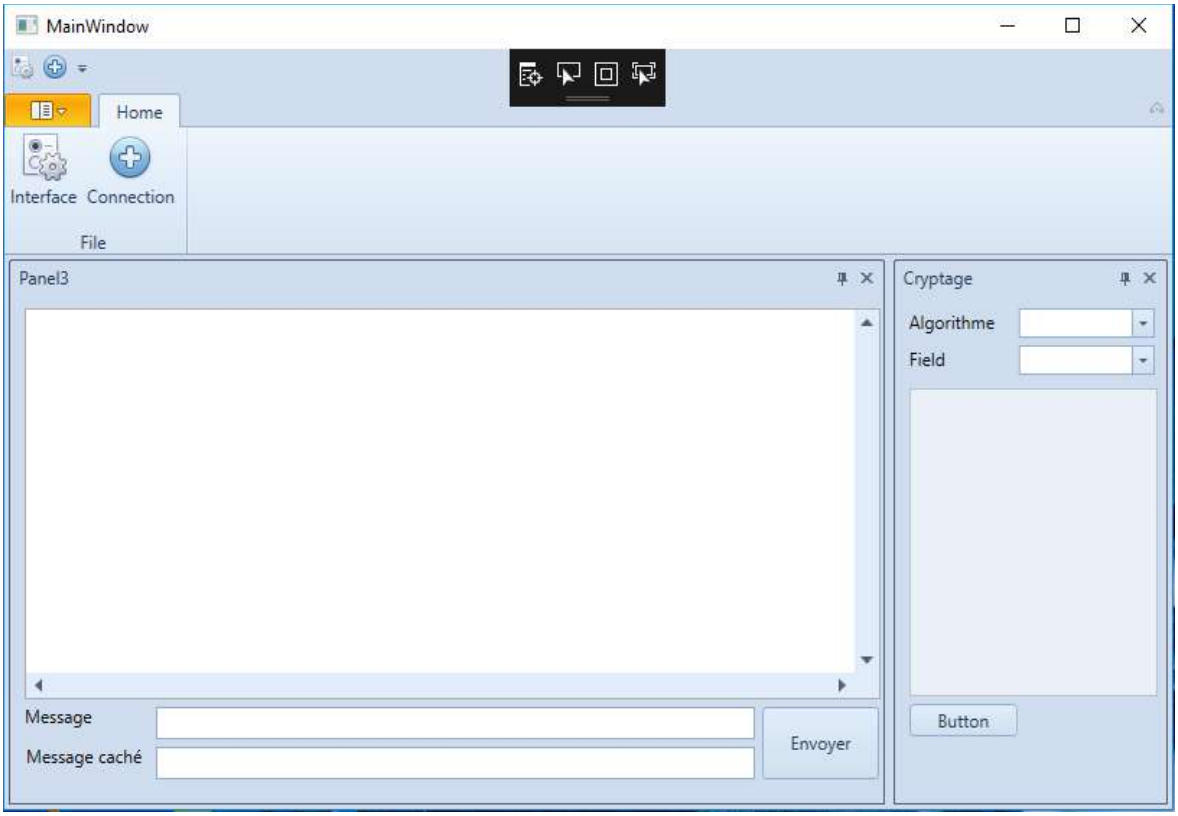

Fig.17 : L'interface du l'application messagerie.

❖ Dans notre application l'utilisateur commence par sélectionne bouton "Interface" pour choisir l'interface de la carte réseau c'est quel que soit sa nature est Ethernet. Parce que l'application ne travaille pas avec les cartes wifi.

Comme il est indiqué dans la figure [18].

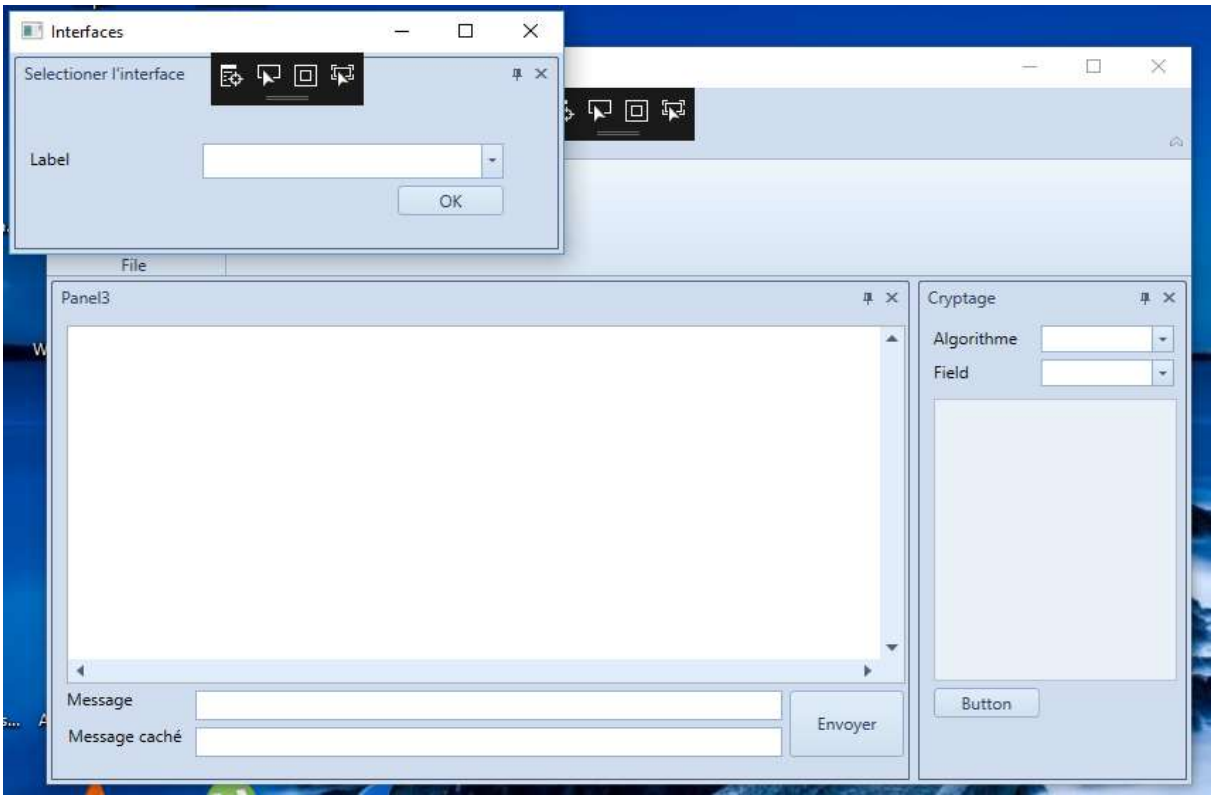

Fig.18 : Fenêtre pour choisir l'interface du la carte réseau.

❖ 2eme chose avec le bouton "connexion" l'utilisateur "émetteur" ajoute l'adresse IP du récepteur dans un autre fenêtre, après cette étape la connexion est établie automatiquement.

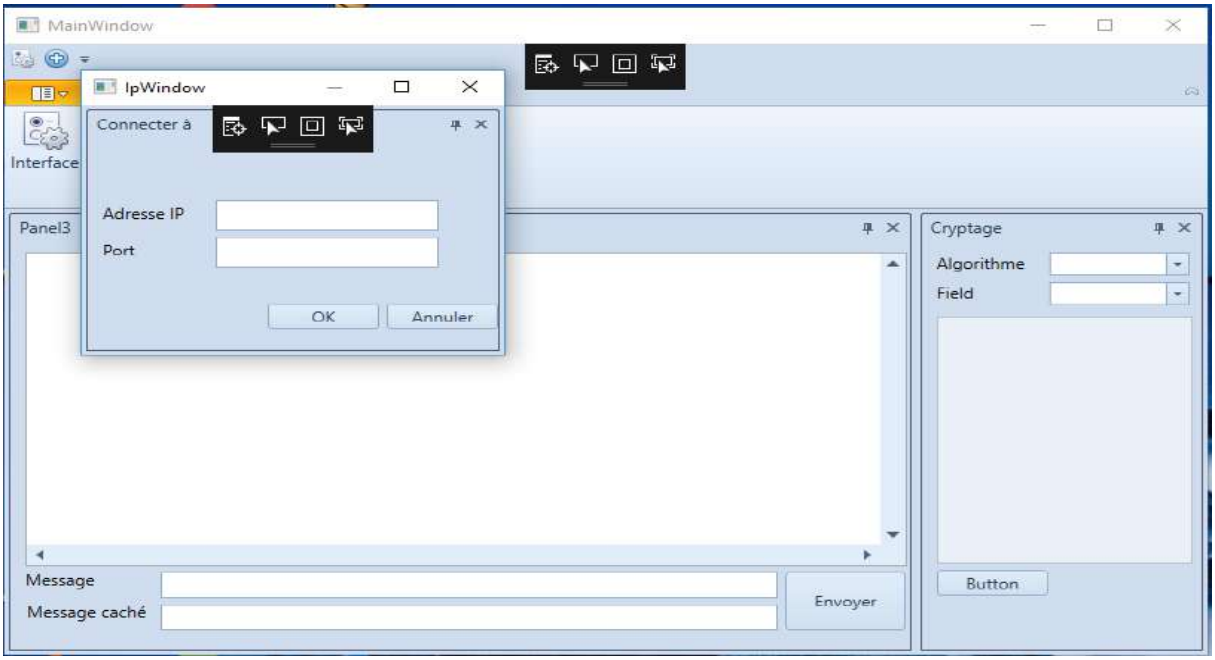

Fig.19 : La connexion du le récepteur.

❖ Maintenant écrite le message secret dans le champ "message caché" et dans le champ "message" écrire n'importe quel message.

Fig.20 : Champs du message.

❖ Avant sélectionner le bouton "envoyer" pour envoyer le message, il faut choisir l'algorithme de cryptage "AES, SHA" et le champ de cacher message "ISN, ID".

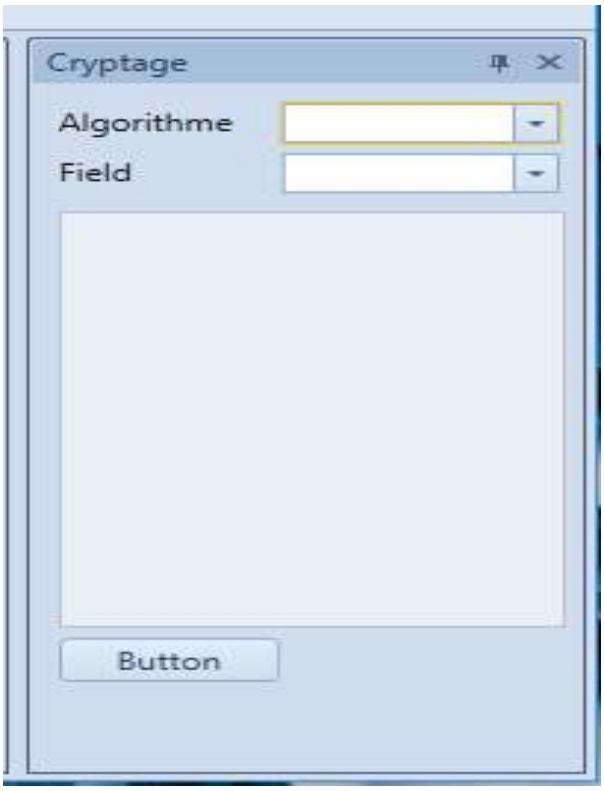

Fig.21 : Les champs de cryptage

V .4. Organigramme de l'application :

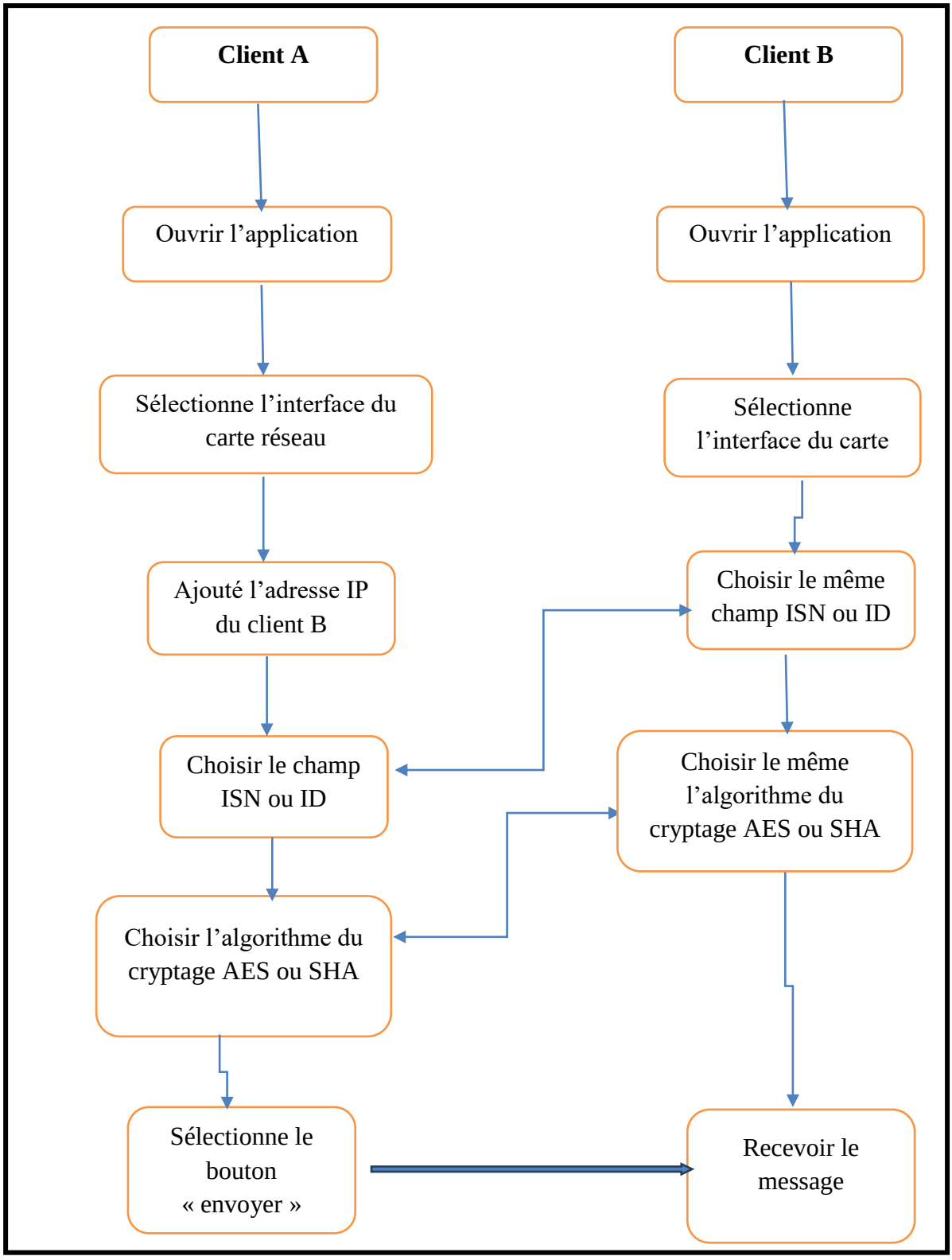

Fig.22 : Organigramme de l'application.

V .5. Conclusion :

Nous avons créé cette application pour montrer à l'utilisateur de cette technique comment les données sont implémentées dans les canaux cachés, avec un exemple simple d'une application de messagerie.

Parce que l'utilisation de cette technique, elle doit être faite dans une couverture d'une grande application de conversation non clairement.

Conclusion générale :

Ce travail de mémoire a été consacré au problème de la dissimulation d'information dans des supports sûrs tels que l'image et la trame TCP/IP. Nous avons tout d'abord présenté dans le premier chapitre une introduction à la stéganographie qui contient un historique de la stéganographie depuis son apparition, des définitions des concepts utilisés par la sténographie linguistique et technique, puis les différents éléments intervenant dans la dissimulation d'informations, ainsi que les buts et les intérêts de cette technique. Après nous avons abordé la stéganographie image Jpeg qui est très utilisée pour dissimuler l'information nous avons cité ces types et ces caractéristiques, ainsi ces algorithmes de transformation et les logiciels utilisés. Après, on a fait une présentation des champs de la trame TCP/IP, puis une présentation de processus utilisés dans la stéganographie TCP/IP et aussi dans la stéganalyse.

Finalement, pour concrétiser les recherches faites sur la stéganographie TCP/IP, nous avons réalisé une application qui permette de dissimuler un message dans un champ de la trame TCP/IP, puis le crypté par un algorithme de cryptage (AES). Les résultats obtenus ont montré que le niveau de sécurité s'élève et que les transactions passent avec simplicité.

Perspectives

Dans nos futurs travaux plusieurs idées peuvent se concrétiser :

- Faire une étude comparative avec d'autres supports d'information
- Etudier l'influence d'augmentation de volume des données à dissimuler.
- Améliorer l'application pour s'adapter aussi pour le réseau WiFi.

Références :

- [1] BATTIKH, Dalia. Sécurité de l'information par stéganographie basée sur les séquences chaotiques. 2015. Thèse de doctorat. Rennes, INSA.

• [2] THOTA, Nageswara Rao et DEVIREDDY, Srinivasa Kumar. Image compression using discrete cosine transform. Georgian Electronic Scientific Journal: Computer Science and Telecommunications, 2008, vol. 17, no 3, p. 35-43.

• [3] WALIA, Ekta, JAIN, Payal, et NAVDEEP, Navdeep. An analysis of LSB & DCT based steganography. Global Journal of Computer Science and Technology, 2010.

• [4] GOEL, Stuti, RANA, Arun, et KAUR, Manpreet. A review of comparison techniques of image steganography. Global Journal of Computer Science and Technology, 2013.

• [5] UPHAM, D. JPEG-JSTEG-Modifications of the independent JPEG groups JPEG software for 1-bit steganography in JFIF output files. 1997.

• [6] PROVOS, Niels et HONEYMAN, Peter. Hide and seek: An introduction to steganography. IEEE security & privacy, 2003, vol. 99, no 3, p. 32-44.

• [7] CHEDDAD, Abbas, CONDELL, Joan, CURRAN, Kevin, et al. Digital image steganography: Survey and analysis of current methods. Signal processing, 2010, vol. 90, no 3, p. 727-752.

• [8] WESTFELD, Andreas. F5—a steganographic algorithm. In: Information hiding. Springer Berlin/Heidelberg, 2001. p. 289-302.

• [9] RAI, Pooja, GURUNG, Sandeep, et GHOSE, M. K. Analysis of Image Steganography Techniques: A Survey. International Journal of Computer Applications, 2015, vol. 114, no 1.

• [10] FRIDRICH, Jessica, GOLJAN, Miroslav, et HOGEA, Dorin. Steganalysis of JPEG images: Breaking the F5 algorithm. In : Information Hiding. Springer Berlin/Heidelberg, 2003. p. 310-323.

• [11] ZITZMANN, Cathel. Détection statistique d'information cachée dans des images naturelles. 2013. Thèse de doctorat. Troyes.

• [12] WESTFELD, Andreas et PFITZMANN, Andreas. Attacks on steganographic systems. In: International workshop on information hiding. Springer, Berlin, Heidelberg, 1999. p. 61-76.

• [13] ROCHA, Anderson et GOLDENSTEIN, Siome. Steganography and steganalysis in digital multimedia: Hype or hallelujah? Revista de Informática Teórica e Aplicada, 2008, vol. 15, no 1, p. 83-110.

• [14] PROVOS, Niels et HONEYMAN, Peter. Detecting steganographic content on the internet. Center for Information Technology Integration, 2001.

• [15] ROCHA, Anderson et GOLDENSTEIN, Siome. Progressive randomization for steganalysis. In: Multimedia Signal Processing, 2006 IEEE 8th Workshop on. IEEE, 2006. p. 314-319.

• [16] ZHANG, Tao et PING, Xijian. A fast and effective steganalytic technique against JSteg-like algorithms. In: Proceedings of the 2003 ACM symposium on Applied computing. ACM, 2003. p. 307-311.

• [17] PROVOS, Niels et HONEYMAN, Peter. Hide and seek: An introduction to steganography. IEEE security & privacy, 2003, vol. 99, no 3, p. 32-44.

• [18] KUNDUR, Deepa et AHSAN, Kamran. Practical Internet steganography: data hiding in IP. Proc. Texas wksp. Security of information systems, 2003.

• [19] FALL, Kevin R. et STEVENS, W. Richard. TCP/IP illustrated, volume 1: The protocols. addison-Wesley, 2011.

• [20] ROWLAND, Craig H. Covert channels in the TCP/IP protocol suite. First Monday, 1997, vol. 2, no 5.

• [21] CAUICH, Enrique, CÁRDENAS, Roberto Gómez, et WATANABE, Ryouske. Data hiding in identification and offset IP fields. In: International Symposium and School on Advancex Distributed Systems. Springer, Berlin, Heidelberg, 2005. p. 118-125.

• [22] Design of a Steganographic System for Hiding Information in TCP/IP Packets Erika Llanes, Roberto Gómez, Maximiliano Canché December 2014.

• [23] SOHN, Taeshik, SEO, J., et MOON, Jongsub. A study on the covert channel detection of TCP/IP header using support vector machine. In : ICICS. 2003. p. 313-324.

• NASSAR, Mohamed, STATE, Radu, et FESTOR, Olivier. Monitoring SIP traffic using support vector machines. In : Recent Advances in Intrusion Detection. Springer Berlin/Heidelberg, 2008. p. 311-330.

• [24] VISHNOI, Vibhor Kumar et KUMAR, Sunil. Detection of TCP/IP Covert Channel based on Naïve-Bayesian Classifier. International Journal Of Engineering And Computer Science ISSN, p. 2319-7242.

- [25] LAMPSON, Butler W. A note on the confinement problem. Communications of the ACM, 1973, vol. 16, no 10, p. 613-615.
- [26] https://fr.wikipedia.org/wiki/St%C3%A9ganographie#Histoire.