الجمهورية الجزائرية الديمقراطية الشعبية
Republique Algerienne Democratique Et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة العربي التبسي - تبسة
Université Larbi Tébessi– Tébessa –
Faculté des Sciences et de la Technologie
Département de génie électrique

MEMOIRE

Présenté pour l'obtention du diplôme de Master Académique

Spécialité : Réseaux et Télécommunications

Présentée par :

-Saker Hiba
-Bouali Fella

Méthodes Stéganographiques Appliquées aux média vidéos

Présenté et soutenu publiquement, le 12/06/2022 devant le jury composé de :

M[me].BOUCHEMHA Amel	MCA	Président
M. HOUAM Lotfi	MCB	Rapporteur
M[me]. OUACIFI Malika	MAA	Examinateur

Promotion : 2021/2022


بسم الله الرحمن الرحيم

Remerciements

Louange à Allah le tout puissant qui m'a accordé la foi, le courage et la patience pour mener à bien ce travail.

Je tiens à remercier infiniment mon encadreur, Dr. HOUAM LOTFI, pour son aide, sans réserve, sa patience et ses conseils précieux qui m'ont été très utiles.

Je remercie également les membres du jury qui m'ont honoré en acceptant de juger et d'enrichir ce travail.

Ces remerciements vont aussi à toute ma famille, et tous mes amis pour leur aide et leur soutien.

Je tiens à remercie également tous mes enseignants.

Un grand merci que toutes nos amies de la promotion, pour leur aide, leur amitié, leur gentillesse et leur soutien moral.

Nous tenons également à remercier monsieur BENJANAH HAKIM, LAMECH pour leur gentillesse et pour l'intérêt qu'ils ont porté à ce travail

Table des Matières

Liste des tableaux

Liste des figures

Introduction Générale

La vidéo est un support d'information très important. Vu l'importance de la vidéo, et la grande quantité d'information qu'elle peut contenir, le monde s'intéresse de plus en plus à la vidéo et tends vers l'universalisation de son utilisation. En effet, la vidéo a touché plusieurs domaines de notre vie : la médecine, la météo, la télécommunication, la cartographie, la géologie, etc.

Le problème d'échange de données secrètes a toujours existé, et ce depuis la naissance des grandes civilisations. La stéganographie offre un moyen efficace pour protéger les données secrètes en les rendant inintelligibles aux personnes non autorisées.

L'objectif de notre travail consiste à insérer un message dans une vidéo et que la perception humaine ne peut pas détecter les petites modifications introduites dans la vidéo qui est destinée à renfermer ce message.

A cet effet, le présent travail est réparti en quatre chapitres décrivant les volets principaux.

Le premier chapitre sera dédié aux généralités sur la stéganographie, et la déférence entre la stéganographie, cryptographie et watermarking.

Le deuxième chapitre sera consacré à la présentation les différentes techniques basée sur les transformations DCT, DWT et LSB.

Le chapitre trois nous avons étudié les domaines de stéganographie où nous avons mis en évidence trois algorithmes l'algorithme LSB du domaine spatial et les algorithmes DCT, DWT du domaine fréquentiel. Et nous avons abordé les étapes de chaque algorithme et leur fonctionnement et ses diagrammes.

Le dernière chapitre va contenir les différents algorithmes proposés et à réaliser ainsi que leurs résultats expérimentaux.

En fin, on termine par une conclusion générale et quelques perspectives.

Chapitre 1
STEGANOGRAPHIE

1.1 Introduction

Les avancées technologiques en informatique et télécommunications ont contribué à soulever plusieurs problèmes liés à la sécurité de l'information.

Nous nous focalisons dans nos travaux sur la question de la sécurité de la transmission d'informations confidentielles sous forme numérique, basées principalement sur la steganographie .

La steganographie est l'art de dissimulation des informations, d'où elle cherche à insérer un message dans un contenu anodin qui peut être une image, une vidéo, ou un son[14], de telles sortes à prendre le processus de dissimulation indétectable. Autrement dit, l'objectif est de rendre difficile ou impossible la distinction entre un document original et un document modifié comportant le message secret. Nous nous intéressons sur les images numériques car ce contenu est majoritairement utilisé lors des échanges numériques.

La steganographie a également comme discipline la steganalyse. Cette dernière a pour but de détecter la présence d'un message caché (secret). Ainsi, en steganalyse l'objectif principal n'est pas d'extraire le message caché, mais plutôt de détecter sa présence.

Dans ce chapitre, nous allons parler sur la steganographie, sa définition, son principe, ses différents types et domaines, ainsi que ses caractéristiques…etc. Ensuite nous allons discuter sur la technique de steganalyse qui consiste à détecter l'existence d'un message secret dans une communication.

1.2 Historique

Les origines de la steganographie remontent à l'antiquité. Son utilisation est décrite par deux fois dans l'Enquête d'Hérodote, un premier passage relate qu'aristagoras fit raser la tête de son plus fidèle esclave et y fit tatouer son message. Une fois les cheveux repoussés, l'esclave pouvait s'en aller transmettre le message, un autre passage fait référence à Démarrât,

ancien roi de Sparte exilé en Perse, qui informa Sparte que les perses préparaient une invitation de la Grèce en écrivant le message sur une tablette en bois puis en recouvrant

Celle-ci de cire. Cela permet de déjouer une attaque qui survient quatre ans plus tard[1,2,3].

En chine antique, on écrivant les messages secrets sur de très fins rubans de soi, qu'en enrobait ensuite dans les petites boules de cire. Ces boules, avalées ensuite par le messager, pouvaient voyager jusqu'au destinataire, d'une manière totalement discrète[4].

Plus subtile encore, l'invention de l'encre sympathique est attribuée au naturaliste Pline l'Ancien, il est toujours utilisé par des organisations mondiales. L'encre sympathique, ou l'encre invisible est un procédé chimique qui consiste a utilisé du jus de citron, du lait ou de chlorate de soude, pour écrire le message secret qui sera invisible à l'œil humain nu. D'où un simple passage sous une source chaude ou un bain dans un réactif chimique, relève le message[4,5].

Il existe une autre technique de dissimulation de message qu'on appelle la steganographie linguistique, dans laquelle on peut utiliser le langage, l'espace entre les mots, l'orthographe, ou encore les repères au niveau de caractères pour cacher un message secret dans un texte. Parmi ses méthodes on trouve l'acrostiche, qui représente un poème dont la première lettre de chaque vers compose un mot ou une phrase [1,4].

L'apparition de la steganographie moderne quant à elle peut être attribuée à G. Simmons qui est en 1984, énonça le problème des prisonniers, dans ce problème Simmons place deux prisonniers qui souhaitent élaborer un plan d'évasion. Cependant tous leurs échanges sont contrôlés par un gardien qui au moindre soupçon placerait un des détenus en zone de confinement. Les deux complices doivent donc trouver un moyen de communiquer sans éveiller les soupçons, c'est ici qu'intervient la steganographie en leur permettant de dissimuler un message caché à l'intérieur d'un autre qui ne semble pas suspect [6].

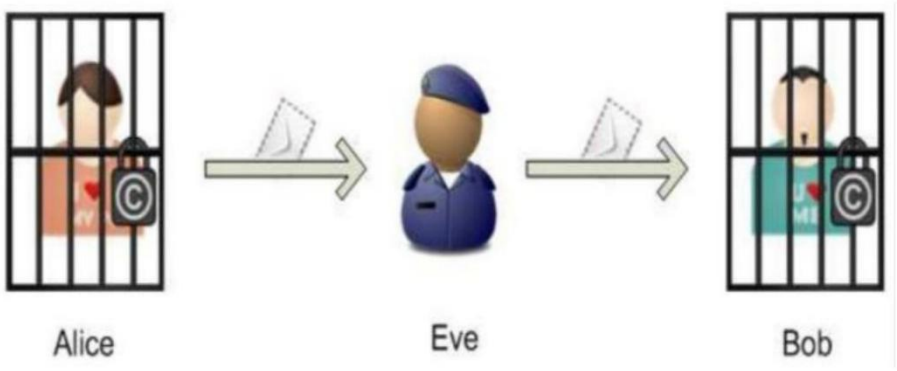


Figure 1. 1 : Exemple d'une communication secrète.

1.3 C'est Quoi la steganographie ?

La stéganographie vient du mot Grec « stéganos » qui veut dire : « dissimulé » et de mot « graphien » signifiant : « écriture », littéralement on traduit par « écriture dissimulée ». Elle consiste à cacher ou dissimuler un message dans un autre, ainsi que le message caché n'est détectable que par la personne connaissant le procédé de dissimulation [7].

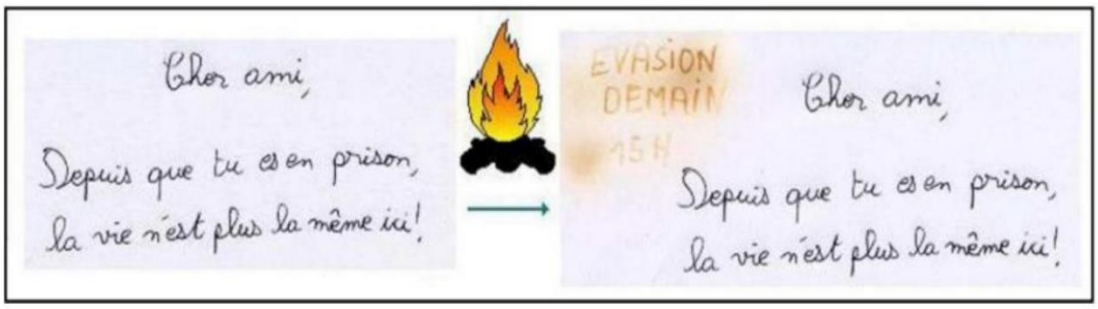


Figure 1. 2 : Exemple de stéganographie à l'aide de lait [8].

C'est Quoi la cryptographie ?

De manière générale, la cryptographie est une technique d'écriture qui consiste à rédiger un message crypté, via l'utilisation de codes secrets ou de clés de décryptage .la cryptographie est principalement utilisée pour protéger un message jugé confidentiel. On l'emploie dans des domaines très divers, comme le monde militaire, l'informatique, la protection de la vie privée, etc.

Il existe de nombreux algorithmes de cryptographie qui permettent de code (et de décoder pour le destinataire) le message .Certains sont considérés comme basiques (on décale par exemple la lettre de l'alphabet d'un nombre déterminé de range vers la droite ou vers la gauche), d'autres proposent un niveau de sécurité presque absolu. Durant la seconde Guerre mondiale, les allemands ont utilisé la cryptographie avec la machine de Lorenz (Enigma) pour communique leurs information militaires en toute sécurité.

1.4 steganoqraphie vs cryptographie

En cryptographie, l'objectif n'est pas de dissimuler des informations dans d'autres, mais plus simplement de rendre l'information que l'on désire transmettre complètement illisible à toute personne ne possédant pas la donnée nécessaire à son décodage. D'autre part la stéganographie permet de cacher le message de sorte qu'il n'y a pas de détection de l'existence du message. Avec la cryptographie, la comparaison est faite entre des parties de texte en clair et des parties du texte chiffré. Dans la steganographie, des comparaisons.

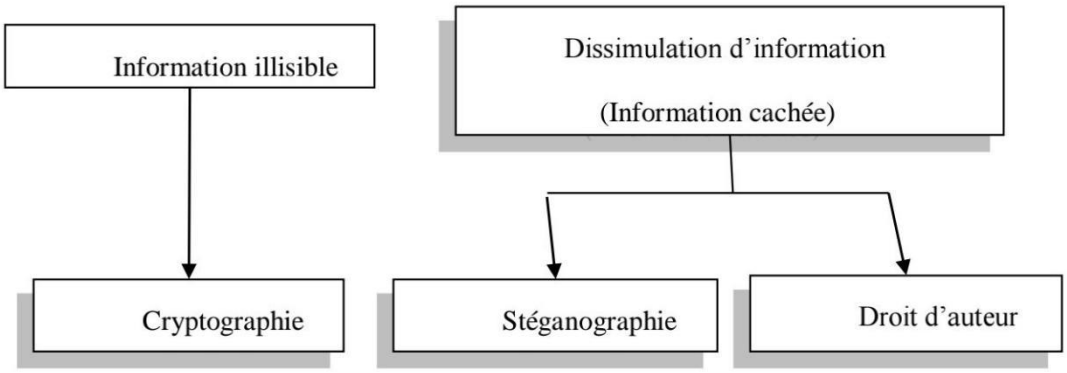


Figure 1. 3 : Diagramme représentant la dissimulation d'information vs cryptographie [27].

Peuvent être faites entre les milieux de couverture, le stego-media, et les parties possibles du message

1.5 steganographie vs Marquage

La steganographie et le marquage sont deux techniques très proches l'une de l'autre, mais qui n'ont pas les mêmes objectifs, ni les mêmes contraintes.

La différence entre la steganographie et le marquage, est que dans la steganographie, l'existence du message caché doit rester secrète alors que pour le marquage seul le message doit rester caché mais son existence (tant qu'on ne peut détecter) peut être connue.

Une autre différence très importante entre la steganographie et le marquage se situe au niveau des attaques qui peuvent avoir lieu contre ces techniques. En steganographie, le pirate va cacher à lire les données dissimulées dans le document, tandis que dans le cas d'un document marqué il va chercher à laver le document de toute signature possible : c.-à-d. supprimer la marque (ou alors il peut essayer d'usurper l'identité de l'auteur en remplaçant la marque).

1.6 Principe

Dans un média couver tel qu'une image ou une vidéo, le message secret peut être du texte brut, du texte chiffré ou une image. Ces médias transitent couramment via l'Internet, et sont un excellent support pour cacher une information secrète.

Nous donnons dans la figure 1.4, le principe de la stéganographie, dans le cas où le média cover est une image numérique (image de Lena) et le message secret lui aussi est une image numérique (image Bateau). Le processus d'insertion dépend d'une clé secrète qui est une information secrète supplémentaire comme un mot de passe. Le système est dit être sécurisé si l'on ne peut distinguer la différence entre une image originale et une image stégo[12].

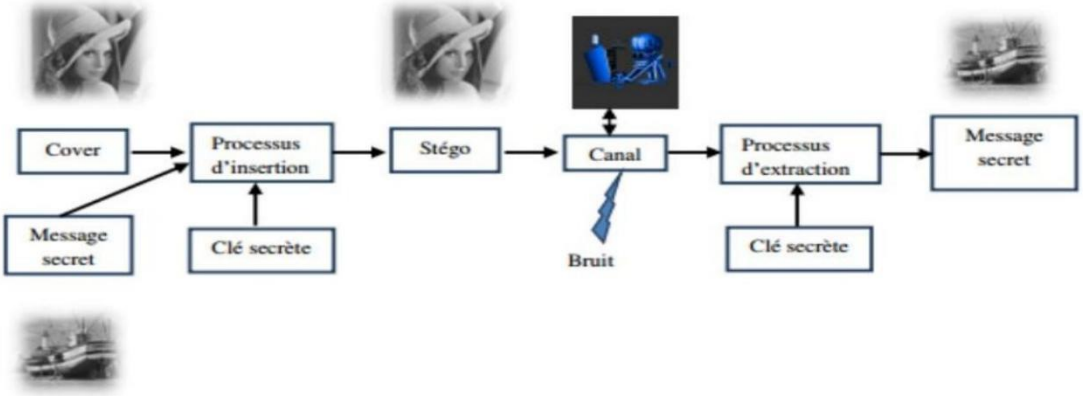


Figure 1. 4: principe de la steganographie.

1.6.1 Structure d'une communication secrète

Le processus complet de la steganographie repose sur deux opérations :

- **La dissimulation**

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

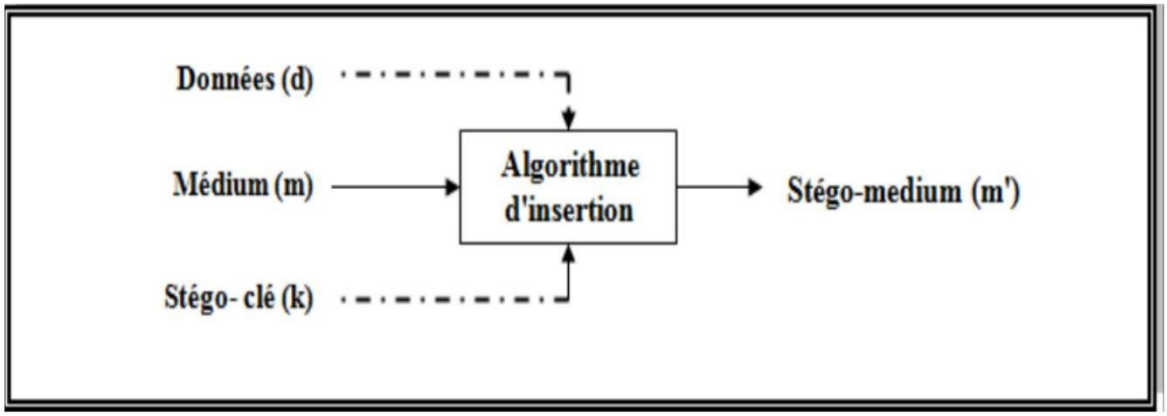


Figure 1. 4:dissimulation des données dans le medium [13].

- **L'extraction**

Consiste à récupérer l'information dissimulée. Le mot détection est également utilisé lorsqu'il s'agit de vérifier la présence d'une information (représentée grâce à un signal, une caractéristique particulière du medium) dans le stégo-medium [24], sans pour autant vouloir l'extraire comme illustre la figure suivante :

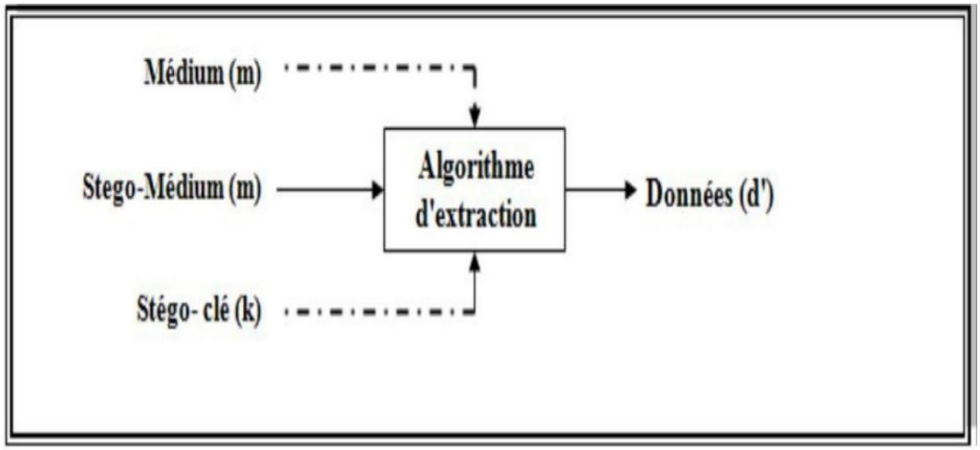


Figure 1. 5 : Extraction des données du medium [13].

1.6.2 Classification des schémas de steganographie

Dans le steganographie il existe trois types de protocoles :

- La steganographie pure :

Est un système dans lequel les données secrètes à dissimulées ne se trouvent que dans l'algorithme utilisé. La découverte de cet algorithme détruit la dissimulation de la communication. Ceci revient à mettre en place de la « sécurité par l'obscurité »[5].

- La steganographie à clé secrète

L'échange de données confidentielles nécessite, au début l'échange d'une clé secrète que l'on ne partagera que avec notre interlocuteur. Il est donc nécessaire d'avoir un canal sécurisé, ou de rencontrer en personne notre interlocuteur, afin d'être certain que cette dernière ne soit pas compromise. Cette clé aura une influence sur la manière de « cacher » l'information[5].

- La steganographie à clé public

La personne voulant envoyer des données à un autre destinataire, sans éveiller de soupçons, utilisera la clé publique de ce dernier. La clé publique étant à priori connue de tout le monde, il n'y aura pas besoin d'échange préalable « sécurisé ». Le destinataire sera le seul à pouvoir en extraire son contenu à l'aide de sa clé privée [5].

1.7 Les différents types et supports de steganographie

On distingue deux types de steganographie : la steganographie linguistique et la steganographie technique

1.7.1 La steganographie linguistique

La technique linguistique est utilisée pour cacher le message dans un texte de couverture (original), d'une manière non-évidente de sorte que la présence du message est indétectable par un étranger [14].

La littérature de la steganographie linguistique, dans laquelle les propriétés linguistiques d'un texte sont modifiées pour cacher l'information, est faible par rapport à d'autres médias. Parce qu'il est plus facile d'apporter des modifications aux médias non linguistiques dans lequel le message secret sera indétectable par un observateur [12].

Il existe plusieurs formes de steganographie linguistique

a) semagramme

C'est la forme la plus connue [12], elle utilise uniquement des symboles et des signes pour cacher les données [14]. Alfred de Musset [12] est le plus intéressé ou 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 [12,15]. Cette forme est devisée en deux catégories [14] :

i. semagramme visuel :

Utilise les objets physiques de chaque jour pour transmettre un message, (Ex : le positionnement des articles sur un site WEB particulier).

ii. semagramme de texte

Ce type est utilisé pour cacher un message en modifiant la forme de texte de l'operateur ou en changeant la taille et le type de police, ou ajouter un espace supplémentaire entre les mots[14].

b) Acrostiche

Ce procédé consiste à transmettre des informations à travers les premières lettres dans chaque vers de poème et qui, lus de haut en bas, pour former un mot ou une expression.Elle a plusieurs variantes (mot placés dans des vers ou des chapitres,…) [12].

c) Ponctuation

Les prisonniers de guerre ont utilisé la ponctuation (points et virgules) pour transmettre des messages à leurs familles [12].

d) Nulle

Les nulles ou les codes camouflés, ayant comme principe de marquer certaines lettres d'un texte par des piqûres d'aiguilles ou encore par la hauteur des lettres. Il suffit alors de rassembler ces lettres marquées pour former un mot ou une expression pour le premier cas, et dans le second cas deux tailles de caractères sont utilisées, le message étant constitué des

lettres soit de petites tailles, soit de grandes tailles selon la convention adoptée pour l'échange [12,15].

1.7.2 La steganographie technique

La steganographie technique utilise des outils spéciaux, des dispositifs ou méthodes scientifiques pour cacher un message. Dans ce type, on peut utiliser l'encre invisible, micro points, méthodes informatiques pour garder le secret du message.

Le message de couverture est le porteur du message tel qu'image, vidéo, audio, texte ou un autre support numérique [16] .La couverture est divisée en blocs et bits du message qui sont cachés dans chaque bloc. L'information est encodée en changeant divers propriétés de l'image de couverture. Les blocs de couverture restent inchangés si le bloc de message est zéro [17].

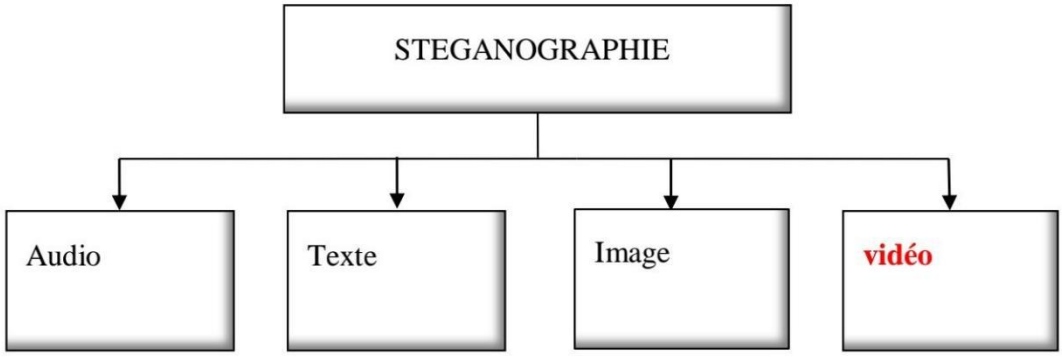


Figure 1. 7: Types de steganographie.

a. steganographie de texte

Dans cette approche, le texte de couverture est produit en générant des séquences de caractères aléatoires, changeant des mots dans un texte, en utilisant des grammaires contextuelles ou en changeant la mise en forme d'un texte existant pour cacher le message. Le texte de couverture généré par cette approche peut se qualifier pour la stéganographie linguistique si le texte est linguistique. Bien que ces méthodes basées sur le texte aient leur propres caractéristiques uniques pour le texte de couverture, mais souffre de divers problèmes d'un point de vue linguistique et de sécurité [18].

b. steganographie de l'image

Cette technique de steganographie est la plus populaire en ces dernières années par rapport à d'autres types de steganographie, à cause de l'inondation des informations d'images électroniques disponibles avec l'avènement de l'appareil photo numérique et la distribution d'Internet en haute vitesse. Ça peut impliquer la dissimulation d'informations dans le bruit produit naturellement dans l'image. La plupart des types d'informations contiennent ce genre de bruit. Le bruit fait référence aux imperfections inhérentes au processus de rendu d'une image analogique en tant qu'image numérique. Dans la steganographie de l'image, nous pouvons cacher le message en pixels d'une image. Un schéma d'image steganographique est un type de système steganographique, où le message secret est caché dans une image numérique avec une méthode de dissimulation. Les différentes méthodes de la steganographie d'image sont [18].

- Méthode de dissimulation de données

Pour utiliser le système il est nécessaire d'avoir un nom d'utilisateur et un mot de passe. Une fois l'utilisateur est connecté dans le système il peut utiliser les données avec la clé secrète pour dissimuler les informations à l'intérieur de l'image choisie [14].

- Méthode d'intégration de données

Une clé secrète est nécessaire pour récupérer les données qui ont été intégrées à l'intérieur de l'image. Ces données ne peuvent pas être récupérer de l'image sans la clé secrète, c'est pour assurer l'intégrité et la confidentialité des données. Le message secret qui est extrait du système est transféré dans le fichier texte, puis ce dernier est compressé dans le zip fichier et le fichier texte zip le convertit en codes binaires [14].

- Méthode d'extraction de données

Elle consiste a récupéré le message original dissimulé dans l'image d'origine, dont une clé secrète est indispensable pour le décodage et l'extraction [14].

c. steganographie audio

La steganographie audio, consiste à dissimuler des messages dans le bruit (audio), ou dans les fréquences que les être humain ne peuvent pas entendre, c'est un autre domaine de dissimulation de données et d'informations qui repose sur l'utilisation d'une source existante comme un espace dans lequel cacher l'information. La steganographie audio peut être

problématique et peut être utile pour transmettre des données secrètes dans un signal audio de couverture inoffensif [14].

1.8 Autres types de supports

- **Vidéo**

Les techniques sont équivalentes à celles utilisées dans les images. Cependant les vidéos sont souvent plus bruitées ce qui facilite l'imperceptibilité des données dissimulées mais les rend aussi moins robustes [6].

- **Systèmes fichiers**

Pour stocker un fichier, le système découpe ce dernier en un nombre de morceaux pour que chaque morceau puisse être logé dans un bloc. Comme la taille d'un fichier a rarement une taille multiple de la taille des blocs, généralement le dernier bloc ne sera pas rempli [6].

Le système de fichier laisse la possibilité d'utiliser des techniques de steganographie. Pour cacher des données, il suffit de les stocker dans ce dernier bloc; si la taille de ces données dépassent l'espace du bloc non rempli, il faut les découper et les stockées sur autant de blocs nécessaires, garder la trace des blocs utilisés et l'ordre pour la récupération.

Le problème de cette technique vient du fait que les fichiers peuvent être modifiés, supprimés, déplacés, etc.

Il existe plusieurs outils dans le web de bas niveau comme b map et slacker, permettant d'analyser en détails les blocs utilisés et récupérer l'espace libre [19].

- **Fichier exécutable**

Les fichiers exécutables peuvent être utilisés pour transmettre un message d'une façon secrète. Lors de la compilation d'un programme, le code source est transformé en un ensemble d'instructions qui sont facile à comprendre par la machine, pout l'exécution, le système d'exploitation lit les sections dont il à besoin. Donc il est possible de bénéficier les parties du code non exécuté [15].

1.9 Propriétés des systèmes de steganographie

La steganographie possède trois grandes propriétés qui dirigent son utilisation

1.9.1 Capacité

La capacité d'insertion d'un système de steganographie 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. Dans le domaine spatial, pour une image numérique, la capacité d'insertion relative peut être exprimée en nombre de bits de message secret insérés par pixel (bpp). Dans le domaine fréquentiel, par exemple insertion dans les coefficients quantifiés d'une image JPEG, la capacité d'insertion relative peut être exprimée par le nombre des bits du message secret à insérer par chaque coefficient DCT quantifié non-nul (bpc).Notons que dans ce cas, comme le nombre de coefficients non-nuls [12,4] dépend du contenu de l'image, la capacité d'insertion est variable d'une image à l'autre.

1.9.2 Sécurité

Toutes les exigences de sécurité pour les systèmes cryptographiques peuvent (doivent) également être considérées pour les systèmes de steganographie. Cela signifie que la sécurité de l'algorithme de steganographiene ne doit pas s'appuyer seulement sur l'algorithme, qui devrait être publique, mais sur le caractère secret de la clé. Dans la steganographie, 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 steganographie est la steganalyse [12].

1.9.3 Robustesse

Elle quantifie la résistance du message dissimulé aux diverses attaques (transformations) apportées au médium stégo [5].

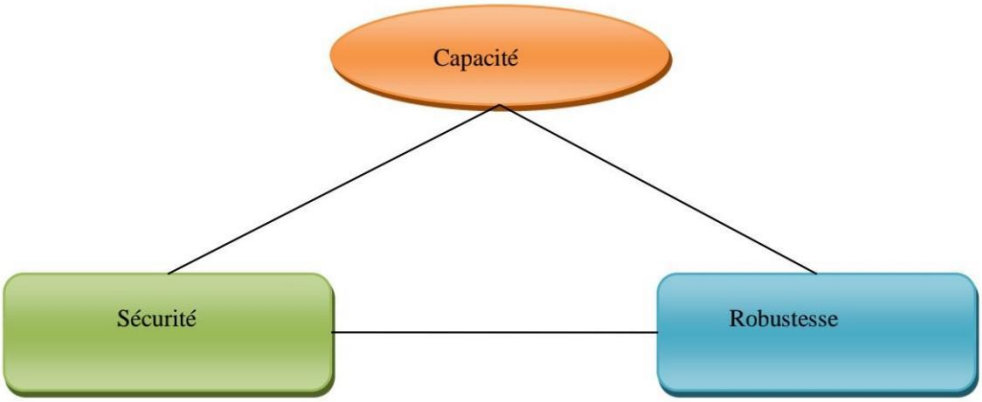


Figure 1. 6 : Triangle des propriétés [5].

1.10 Domaines de steganographie

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

1.10.1 Domaine spatial

La steganographie spatiale consiste à faire changer des bits de pixels de l'image pour insérer les bits du message secret. La technique LSB est l'une des techniques la plus simple et la plus répandue. Elle consiste à cacher un message secret dans les bits de poids faible des pixels de l'image, de sorte que les distorsions apportées par le processus d'insertion restent non perceptibles. La raison est que pour l'œil humain, les variations de la valeur du LSB sont quasiment imperceptibles. L'insertion de bits de message secret peut être faite séquentiellement ou de façon pseudo aléatoire. La steganographie par substitution de LSB et la steganographie par correspondance de LSB sont des exemples de techniques de steganographie dans le domaine spatial [12].

1.10.2 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 steganographie fréquentielle est une technique essentielle de dissimulation de l'information secrète : de nos jours, la plupart des

systèmes de steganographie opèrent dans le domaine fréquentiel. La steganograhie 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 la suite nous rappelons les principes des différentes techniques de transformation dans le domaine fréquentiel [12].

1.11 La steganalyse

Plusieurs études ont été réalisées pour détecter la présence de données ou d'informations cachées à l'aide d'un algorithme de stéganographie .Ce type d'étude forme ce qu'on appelle la stéganalyse ou l'analyse stéganographique. Elle correspond à la discipline duale de la steganographie, donc l'analyse steganographique représente les moyens mis en œuvre pour déceler la présence d'une communication secrète.

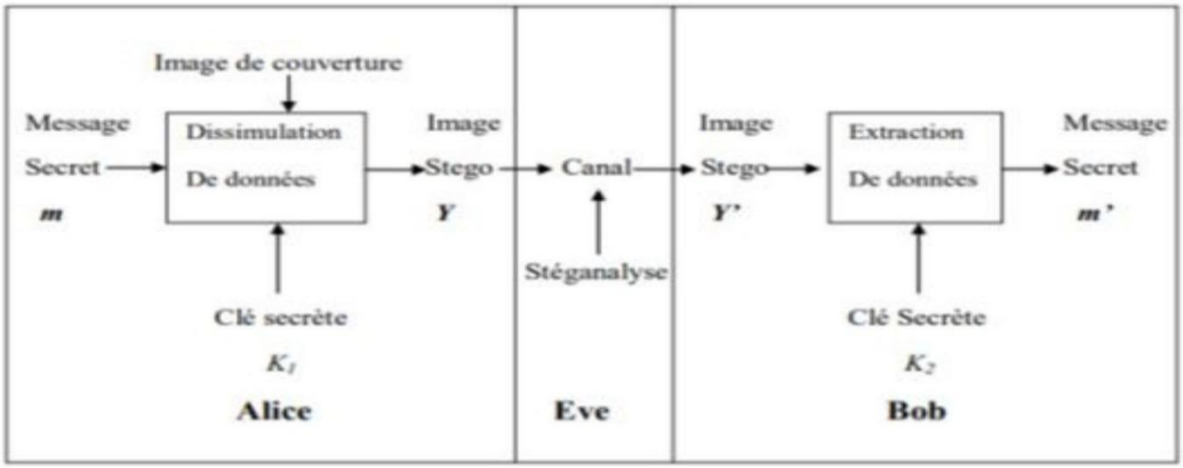


Figure 1. 7 : problème des prisonniers.

1.12 Conclusion

Le travail présenté dans ce chapitre consiste à expliquer la steganographie, les Propriétés des systèmes de steganographie, les Domaines de steganographie (spatiale et fréquentielle).

Chapitre 2
TECHNIQUES DE STEGANOGRAPHIE VIDEO

2.1 Introduction

La steganographie vidéo est un terme d'ingénierie défini comme cachant le massage secret en couverture fichier multimédia comme un fichier vidéo. Ce système peut également être défini comme la dissimulation d'un massage secret derrière un fichier vidéo. La steganographie également identifiée est la compétence et l'apprentissage de l'écriture d'un mot qui est voulu se cacher derrière en choisir un comme fichier multimédia de couverture comme l'audio, la vidéo ou l'image L'œuvre principale de dans cette recherche augmente la capacité de dissimulation des données vidéo[19].

La steganographie est le dessin et la connaissance de l'écriture de messages secrets qui doivent être cachés derrière le fichier de couvertures originales qui peut être audio, vidéo ou image. Voici de nombreuses steganographies comme texte, audio, vidéo et steganographie d'images, qui utilisent ici les performances de l'informatique judiciaire à des fins d'authentification. L'objectif principal est de cacher des informations ou des données secrètes derrière le multimédia fichier comme image et vidéo. Sachez que la vidéo est la combinaison de plusieurs cadres d'images immobiles et audio.

Dans ce chapitre, nous discutons comment cacher (image, texte) à l'intérieur d'une vidéo et les méthodes utilisées pour cela.

2.2 Vidéo

2.2.1 Définition

Nous considérons un flux de vidéo comme une suite d'images 2D. La résolution de la vidéo, exprimée en nombre de pixels, définit la dimension de ces images. La durée du temps entre deux images (Δt) est très petite parce que nous savons que la vitesse de film, en général, est de 24 à 60 images par seconde [3].

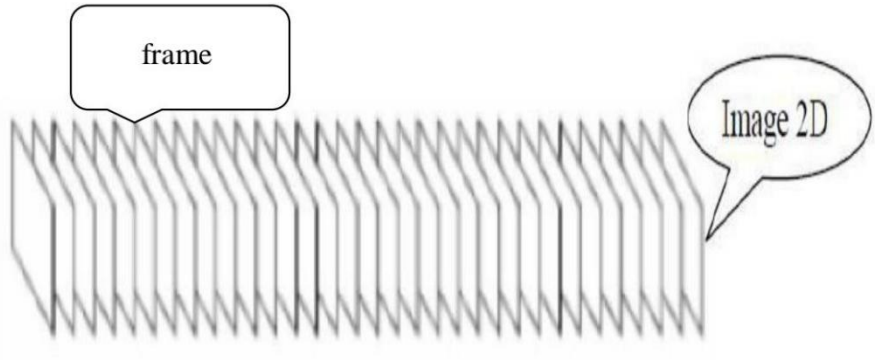


Figure 2. 1 : Représentation d'un flux de vidéo.

2.2.2 Types de vidéo

Le signal vidéo est le signal qui permet de transporter une séquence d'images de la source à un dispositif d'affichage sous forme électrique. Selon la façon dont les signaux sont traités on peut distinguer les deux modes:

- **La vidéo analogique**

Le signal analogique comme un signal électrique dont l'intensité varie dans le temps de façon continue. La qualité du signal final dans ce mode est plus faible car le bruit rajouté au signal lors son traitement altère sa qualité [15].

- **La vidéo numérique**

Est un signal qui porte une information représentée par une suite de valeurs minimales ou maximales correspondant respectivement au 0 et au 1. L'un des facteurs qui avantage le signal numérique par rapport au signal analogique est la facilité de distinguer l'information émise du bruit [15].

2.2.3 Les paramètres clés d'une vidéo

Le stockage et la diffusion d'une vidéo exigent un espace volumineux et un taux de transfert plus élevé. Le contrôle de qualité, et la taille d'une séquence vidéo est déterminé par deux paramètres clés,

- **Le nombre d'images par seconde**

Le nombre d'images du système visuel humain exigé en général 25 ou 30 images par seconde.

- **La résolution**

Ce terme désigne que la quantité de l'information est limitée dans l'image. Autrement, c'est le nombre de pixels qui peuvent être affichés par un dispositif d'affichage.

Trouver le compromis entre ces paramètres et les limitations imposées par la technologie permet d'obtenir une qualité de vidéo optimale [15].

2.3 steganographie appliquées sur les vidéos

2.3.1 Les types de steganographie

La steganographie est appliquée pratiquement avec tous formats de fichiers numériques mais fonctionnent largement avec les images numériques en raison de leur fréquence sur Internet. Il existe cinq grandes catégories de formats de fichiers qui peut être utilisé pour la steganographie, (vidéo, texte, audio, image et protocole) [9].

- **Cacher image dans une vidéo**

Un des exemples les plus étonnants de steganographie est la possibilité de cacher une image dans une vidéo! Nous allons expliquer comment faire, l'applet en bas de la page en donne une réalisation concrète. Une image est constituée de pixels. Chaque pixel est colorié en fonction d'une intensité de rouge R, de vert G (pour green), et de bleu B. L'intensité de rouge, de vert, de bleu de chaque pixel est un nombre compris entre 0 et 255. Chacun de ses nombres s'écrit en base 2 comme une suite de 8 chiffres de 0 et de 1.

Prenons un pixel de la première image, et le même pixel de la cadre. A chaque fois, il est caractérisé par 3 nombres à 8 chiffres en base 2. On va fabriquer un seul pixel qui sera presque colorié comme le premier.]Pour cela, on garde les 4 premiers chiffres de chaque

couleur du pixel de la première image, et on la complète par les 4 premiers chiffres de chaque couleur du pixel de la cadre deuxième, comme sur l'exemple ci-dessous[9].

Image 1	R=01001110	G=01101111	B=11111111
Cadre 1	R=01110011	G=01110110	B=10101010
Cadre fabrique	R=01000111	G=01100111	B=11111010

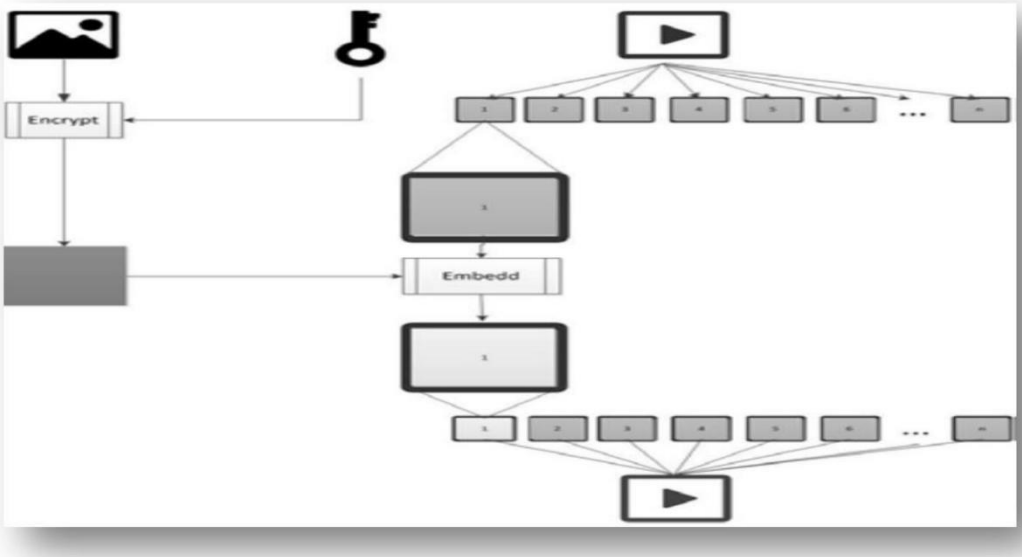


Figure 2. 2 : Processus d'intégration.

La vidéo qu'il a publiée est très proche de la première vidéo. Pour chaque pixel, l'intensité du rouge, du vert et du bleu a été modifiée à un maximum de 16 (zone comprise entre 0 et 255). Cependant, une partie des informations de l'image 2 a été masquée. Nous expliquons comment trouver la première et la deuxième vidéo à partir de la vidéo simulée. Pour chaque main du cadre apocryphe, les premiers chiffres de l'inscription sont regardés en fonction de l'intensité du rouge et du bleu. Ces quatre chiffres formeront les chiffres rouges, verts et bleus de l'i Pixel correspondant à l'image 1a. Puis complétez avec quatre zéros[9]. Les quatre derniers chiffres de la case 2a. Nous complétons cela à nouveau avec quatre zéros :

Image 1	R=01001110	G=01101111	B=11111111
Cadre 1	R=01110011	G=01110110	B=10101010
Cadre fabriquée 1	R=01000111	G=01100111	B=11111010
Cadre retrouvée1	R=01000000	G=01100000	B=11110000
Cadre retrouvée2	R=01110000	G=01110000	B=10100000

Bien sûr, on ne trouve pas toutes les vidéos identiques (pour chaque pixel, on change la valeur d'intensité de la couleur rouge, verte et bleue par un nombre compris entre 0 et 16. La vidéo a perdu de sa qualité, mais est tout à fait reconnaissable ! Cet algorithme naïf peut facilement être amélioré, par exemple, on peut utiliser Exclusif ou pour calculer les 4 derniers nombres de la trame, et ainsi utiliser la première vidéo comme clé, et ce procédé mélange cryptage et steganographie[9].

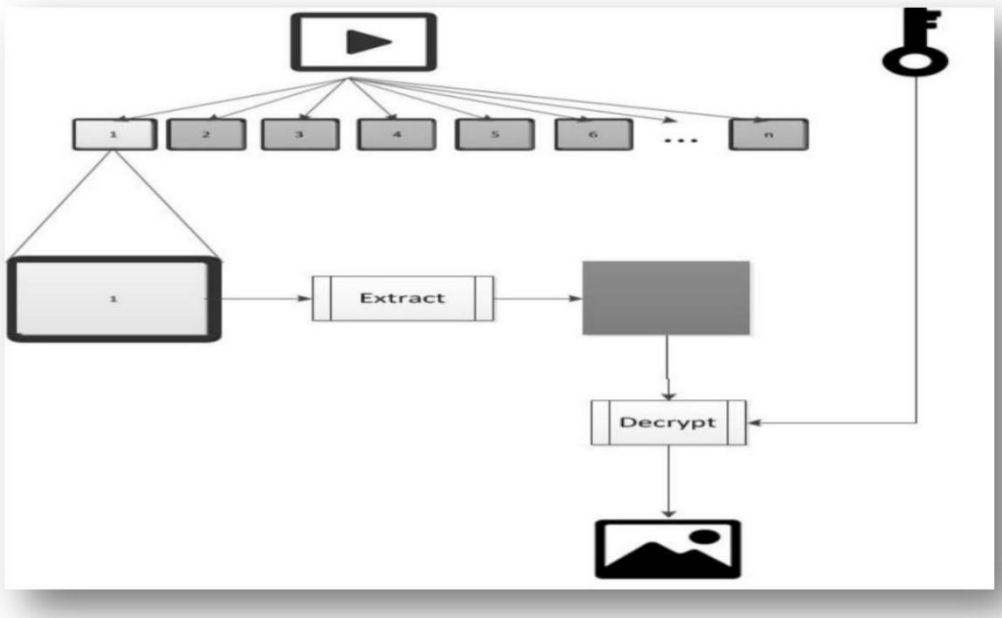


Figure 2. 3 : Processus d'extraction.

- **Cacher un texte dans une vidéo**

On peut cacher un texte dans une vidéo numérique et cela de manière parfaitement invisible à l'œil nu. Cette technique s'appelle le tatouage (watermarking en anglais). Elle est

utilisée notamment pour protéger des vidéos par copyright, mais on peut évidemment aussi transmettre des messages cachés. C'est en fait de la steganographie et simple.

En effet, beaucoup de formats compressent les données et donc modifient les bits de l'image, ce qui a pour effet de détruire le message caché.

Mais avant cela, nous devons passer par une étape importante, qui est :

Chaque caractère du texte à cacher sera représenté par son code ASCII étendu, écrit en base 2. Par exemple, le code ASCII de «A» est 65, ce qui donne en binaire, sur un octet (8 bits): 01000001. Le texte complet sera donc une suite de 0 et de 1, chaque caractère utilisant 8 bits [20].

2.4 Types de techniques steganographie vidéo

Il existe de plusieurs techniques de sténographie vidéo. La meilleure technique est sans s'arrêter la qualité de la steganographie vidéo pour cacher l'information secrète, pour ne pas avoir été détectée par les yeux nus. La vidéo implémentée est connue sous le nom de vidéo "STEGO" qui est envoyée à l'utilisateur répertoire. Plusieurs techniques de steganographie vidéo sont utilisées aujourd'hui, pour ajouter des informations significatives [20].

2.4.1 Vidéo steganographie utilisant la technique LSB

LSB est la meilleure méthode de sécurité des données pour ses résultats passés et présents. C'est le plus simple et moyen le plus efficace pour incuber les massages. En LSB, les valeurs de pixel des potelets vidéo qui sont en octets sont soudainement affectées, après le remplacement du LSB par les bits de données secrets que nous avons inclus. Maintenant, puisque le son LSB de la chanson change de vidéo, il n'est pas non incorporé, et presque la même chose que le fichier vidéo d'origine [20].

- **Principe de LSB**

Le principe de cette technique consiste à substituer les bits de poids faibles (les LSB) des pixels par les bits de message à insérer.

Le sens de parcours des pixels est usuellement choisi par un parcours pseudo-aléatoire (clé secrète k)

2.4.2 Vidéo steganographie utilisant par DCT

La technologie de steganographie vidéo DCT joue un rôle dynamique dans la technique de compression au format de trame JPEG. Par exemple, une vidéo avec le cadre est divisée en carrés de 8x8. Chaque carré a changé DCT qui produit 63 coefficients. Une série multidimensionnelle de résultats. Maintenant le coefficient est arrondi avec une valeur quantifiée. Le filigrane est intégré au milieu bande de fréquence du bloc DCT transportant les composantes basses fréquences. Il est inséré en ajustant les coefficients DCT de l'image et à l'aide de la clé privée [13].

2.4.3 Vidéo steganographie utilisant par DWT

La DWT (discrète wavelet transformation) est maintenant utilisée dans plusieurs présentations pour le signal traitement, tel que la compression de texte, audio, image et vidéo, DWT doit convertir le cadre dans le domaine spatial au domaine fréquentiel, où il est Ils génèrent les coefficients ondulés, Les données d'information ont changé, comme un fichier texte ou image. Dans ce type de transformation, le les coefficients de nodulation séparent les données haute et basse fréquence en pixels en pixels. Le DWT L'approche utilisée dans le travail proposé est le "niveau -2 Son DWT, le plus simple de tous les ondelettes méthodes de transformation." Dans cette transformation, le domaine temporel passe par des valeurs basses et hautes des filtres de passage et les coefficients d'ondelettes de haute et basse fréquence sont générés et la différence et valeurs moyennes de deux pixels prises L Fonctionnement de votre DWT sur le pont Les résultats de l'image dans la formation de 4 sous-bandes, c'est-à-dire bande basse fréquence basse (LL), basse fréquence bande horizontale (HL), bande verticale basse haute fréquence (LH) et bande diagonale haute fréquence (HH). La bande estimée contient les informations les plus significatives sur l'image du domaine spatial et d'autres bandes incluent des informations haute fréquence, telles que des détails de bord, c'est-à-dire le DWT technique [25].

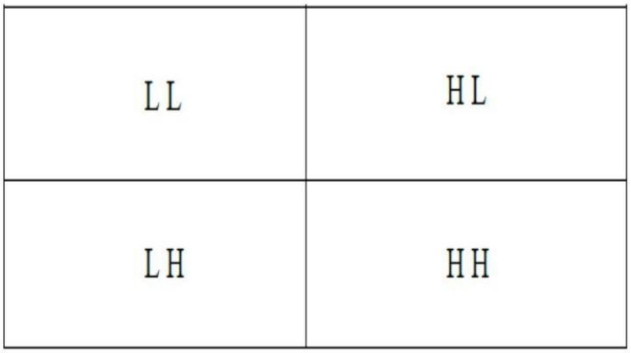


Figure 2. 3 : Sous-bandes formées après l'application de DWT.

2.4.4 Codes hamming

Le code de hamming est l'une des méthodes de code de bloc les plus connues qui peuvent effectuer à la fois la détection et la correction d'erreurs sur un bloc de données. Dans la technique du code de hamming, l'information d'origine sera codée en ajoutant des données supplémentaires avec le minimum de redondance, appelée mot de code, de longueur n bits. La partie ajoutée consiste en des informations de parité de longueur (n-k) bits où k est la longueur du message qui devrait être codé. Dans cet article, le code de hamming (7, 4) est utilisé pour détecter et corriger une erreur de données ou de parité sur un seul bit. Premièrement, le message (m1, m2, m3, m4) de longueur k bits (k=4) est codé en ajoutant trois bits de parité (p1, p2, p3) pour devenir le mot de code de longueur n (n=7), qui est prêt à être transmis. Il existe différentes manières de mélanger les deux types de données (message et parité) et la combinaison générale consiste à placer les bits de parité à la position 2i tels que (p1, p2, m1, p3, m2, m3, m4) où i=0, 1, ...,(n-k-1).

Les codes de hamming sont des codes linéaires, ils ont donc deux matrices : la matrice de contrôle de parité H et la matrice génératrice G, dont ils ont besoin à la fois pour le codage et le décodage. Côté encodage, chaque message M, composé de 4 bits, sera multiplié par la matrice génératrice puis se verra appliquer un modulo de 2 ; le résultat est le mot de code X de 7 bits prêt à être envoyé à travers un canal bruité [24].

2.5 Conclusion

L'insertion dans le domaine fréquentiel et spatiale est une façon plus complexe, mais qui cependant peut être qualifiée de plus robuste que les méthodes d'intégration qui opèrent dans le domaine temporel. Dans ce chapitre, nous avons présenté différentes techniques basées sur les transformations DCT, DWT et LSB.

Chapitre 3
Stéganographie spatiale et frequentielle

3.1 Introduction

La steganographie est l'art et la science de cacher ou dissimuler des informations, dont l'objectif est de transmettre un message de manière dans laquelle aucune personne ne peut détecter l'existence de ce message entre l'émetteur et le récepteur.

Le message secret peut être un texte en clair, un texte chiffré ou des images. L'incorporation du message dans une couverture objet entraine la production d'une vidéo stego.

Il existe plusieurs techniques de steganographie de la vidéo qui sont classées en domaine spatial et domaine fréquentiel (transformé), les techniques du domaine spatial sont des systèmes simples tels que le bit le moins significatif (LSB), d'où le bit le moins significatif est la plus petite valeur d'un nombre binaire. Dans l'algorithme LSB, les données sont cachées dans le moins des parties significatives de l'image de couverture qui sont pas perceptibles lorsqu'elles sont vues avec l'œil humain [18].

Alors que le schéma du domaine fréquentiel est utilisé pour cacher une grande quantité d'informations, il cache les données dans le domaine de fréquence en modifiant la magnitude de toutes les transformées de la vidéo de couverture. On distingue la Transformée en Cosinus Discret (DCT), et la Transformée en Ondelettes qui sont les principaux types, ces transformations ont tous des coefficients associés à leurs pixels. Les données secrètes sont cachées dans ces coefficients qui définissent également comment l'image ou le fichier devrait être transformé [4].

Dans ce chapitre, nous parlerons de quelques algorithmes dans les deux domaines (spatiale et fréquentielle).

3.2 Algorithmes de steganographie

3.2.1 Domaine spatial

3.2.1.1 Bit de poids faible

L'idée est de prendre un message et de le modifier de manière aussi discrète que possible afin d'y dissimuler l'information à transmettre. Le message original est le plus souvent une image. La technique de base --- dite LSB pour Least Significant Bit --- consiste à modifier le bit de poids faible des pixels codant la vidéo : la vidéo numérique est une suite des cadres et chaque cadre est une suite de points, que l'on appelle pixels, et dont on code la couleur à l'aide d'un triplé d'octets, par exemple pour une couleur RGB sur 24 bits.

Chaque octet indique l'intensité de la couleur correspondante --- rouge, vert ou bleu (Red Green Blue) --- par un niveau parmi 256. Passer d'un niveau n au niveau immédiatement supérieur (n+1) ou inférieur (n-1) ne modifie que peu la teinte du pixel, or c'est ce que l'on fait en modifiant le bit de poids faible de l'octet [26].

3.2.1.2 Principe de LSB

Le principe de cette technique consiste à substituer les bits de poids faibles (lesLSB) des pixels par les bits de message à insérer

Le sens de parcours des pixels est usuellement choisi par un parcours pseudo-aléatoire (clé secrète k)

Exemple

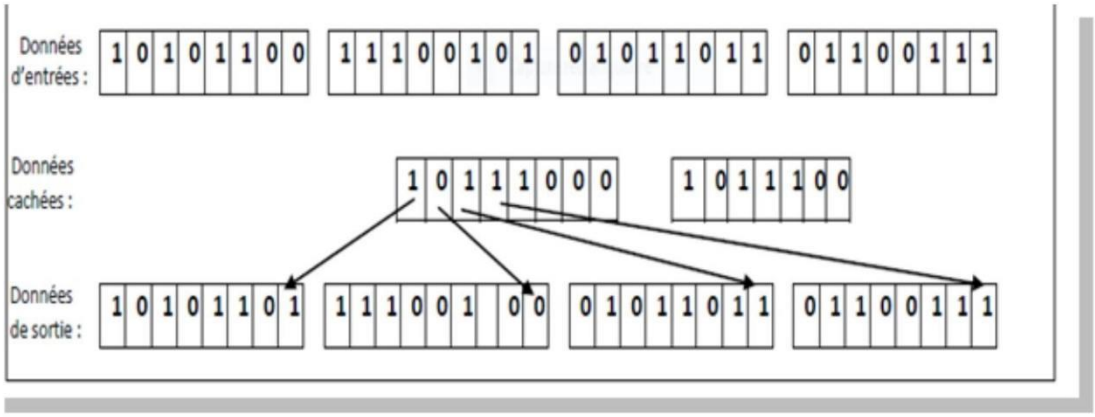


Figure 3. 1 : Exemple d'insertion du message avec la méthode LSB.

➢ Algorithme d'insertion

C'est l'algorithme le plus simple de la dissimulation, le concept de base de la substitution de bits poids faible inclut l'incorporation des données secrètes aux bits qui ont une pondération minimale de sorte qu'elle n'affecte pas la valeur du pixel d'origine [17].

- **Les étapes d'insertion d'un message secret**

Étape 1: Lire la vidéo.

Étape 2 : Diviser la vidéo en cadres.

Étape 3: Lisez l'image de couverture et le message texte qui doit être caché dans l'image de couverture.

Étape 4: Convertissez le message texte au format Ascii puis en code binaire.

Étape 5: Calculez le LSB de chaque pixel de cadre de couverture. (Par la division de chaque pixel par 2. Où le reste de cette division représente le bit de poids faible).

Étape 6: Remplacer cadre de couverture du LSB avec chaque bit du message secret un par un.

Étape 7: Ecrire la vidéo stego.

- **Le Code ASCII (American Standard Code for Information Inter change)**

C'est un Unicode qui permet de coder les caractères en décimal, ce code est standardisé de 256 caractères.

➢ Algorithme d'extraction

L'extraction est définie comme les pixels de mappage à la cadre. Dans la steganographie de la vidéo, le processus d'extraction peut être effectué sur un message qui est vidéo stego. Le destinataire entre vidéo stego et, le cas échéant, la clé steganographique, dans un algorithme d'extraction qui génère le message secret.

Cet algorithme d'extraction est considéré comme l'inverse de l'algorithme d'intégration, bien que les algorithmes d'intégration et d'extraction puissent être créés de telle sorte que l'algorithme d'extraction ne soit pas réellement l'inverse mathématique de l'algorithme d'incorporation. Plusieurs facteurs influencent sur l'efficacité d'un système steganographique, dont le plus important est le choix de la vidéo de couverture [29].

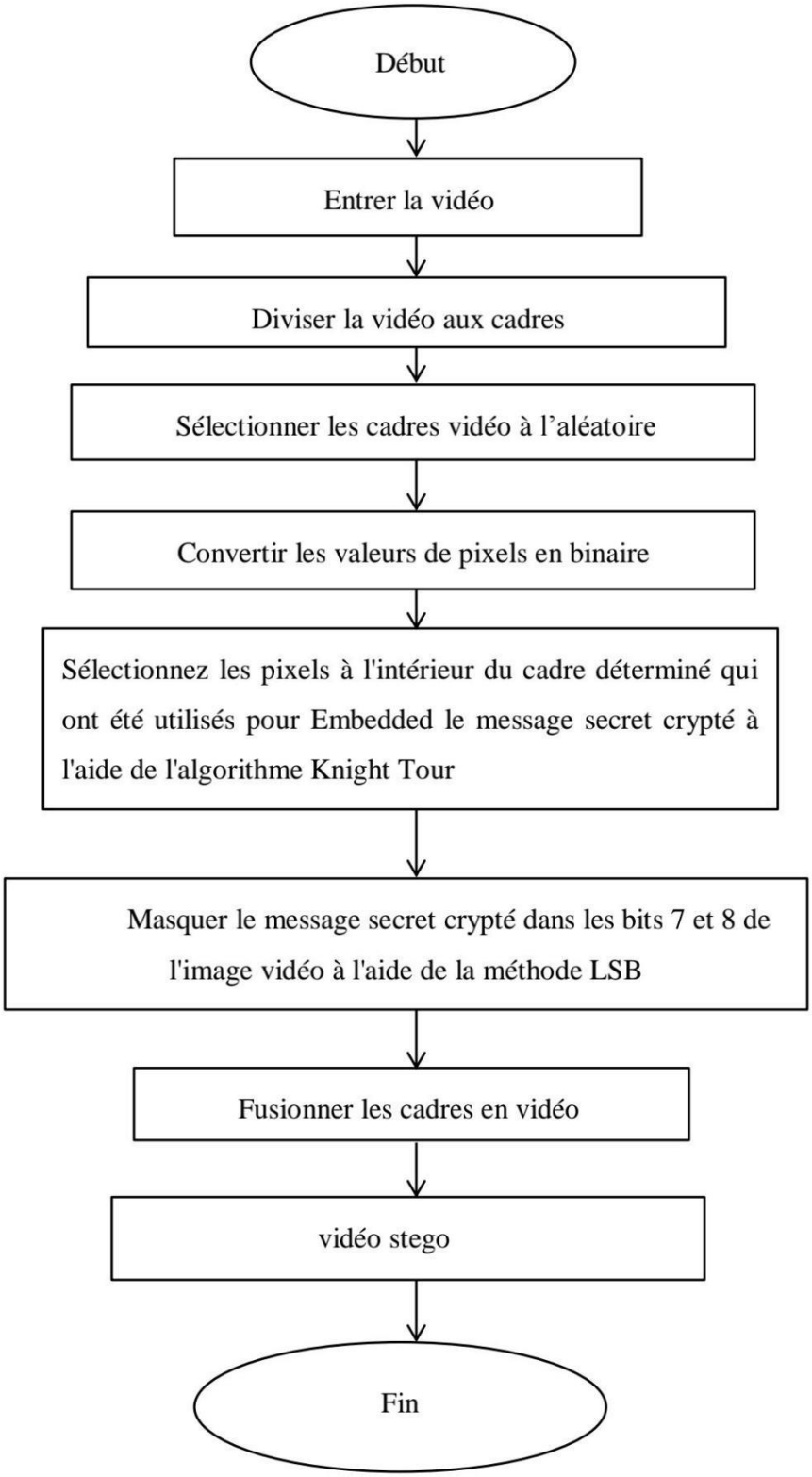


Figure 3. 2 : L'organigramme du processus d'intégration est illustré.

- **Les étapes d'extraction d'un message secret**

Étape 1: Lisez la vidéo stego.

Étape 2: Extraire les bits du message un par un, et reconstruire le code binaire de message.

Étape 3: Convertir ce code binaire en code Ascii, puis décoder ce dernier pour obtenir le message caché (caractères).

- **Une grille de 3 pixels pour une image 24 bits peut être donnée comme suit**

(01010101 01011100 11011000)

(10110110 11111100 00110100)

(11011110 10110010 10110101)

Lorsque le nombre 300 est inséré dans les bits de poids faible de cette partie de l'image.

C: 10000011

- **La grille résultante est la suivante**

(01010101 01011100 11011000)

(10110110 11111100 00110100)

(11011111 10110011 10110101)

Dans l'exemple ci-dessus, le nombre C a été intégré aux 8 premiers octets de la grille et seuls et uniquement 2 bits doivent être modifiés en fonction du message incorporé.

- **Inconvénients**

✓ La facilité de détection.

✓ N'est utilisé que pour les formats compressés sans perte d'information.

3.3 Domaine fréquentiel

3.3.1 Algorithmes à base de DCT

Il existe dans la littérature beaucoup d'approches stéganographiques basées sur la transformée DCT. Nous présentons parmi ces algorithmes les deux méthodes les plus courantes.

- **Ajustement DC**

Cet algorithme traite seulement les images de format JPEG où l'image RGB est convertie en YCbCr [27]. La dissimulation des données n'est réalisée que dans le plan Y qui contient l'essentiel de l'information. Cet algorithme possède comme entrée le message secret et l'image porteuse, et comme sortie l'image dite stégo. Les étapes du traitement sont les suivantes :

1. diviser les fichiers vidéo (.AVI) en cadre.

2. Convertir l'image secrète en binaire.

3. Convertir l'image porteuse depuis l'espace couleur RGB en celui YCbCr, le plan Y étant le seul utilisé par la suite pour cacher l'image secrète.

4. Diviser l'image porteuse en blocs 8*8 pixels.

5. Appliquer la transformée DCT sur chaque bloc.

6. Lire le message secret bit à bit, chaque bit étant caché de la manière suivante :

La position p(1,1) de chaque bloc est utilisée pour calculer la valeur dc donnée par dc= (round(p(1,1)/16)).

Si la valeur de dc est paire et le bit secret à cacher est 0, ou si la valeur de dc est impaire et le bit secret est 1, alors on ne fait aucun changement sur le bloc considéré et on passe au bloc suivant.

7. Répéter les étapes 4 et 5 jusqu'à ce que la valeur de dc soit paire et le bit secret valle 0, ou que la valeur de dc soit impaire et le bit secret valle 1.

8. Remonter les cadres

7. Appliquer la transformation Inverse DCT (IDCT) pour obtenir Vidéo stégo.

8. Sauvegarder le nouveau plan Y de l'image contenant le message secret puis reconvertir l'image en RGB.

Cette méthode possède deux avantages : sa simplicité et sa robustesse. Par contre, sa capacité d'enfouissement est médiocre puisqu'un seul bit peut être intégré dans chaque bloc de 64 pixels. C'est ce point faible que la méthode suivante cherche à améliorer.

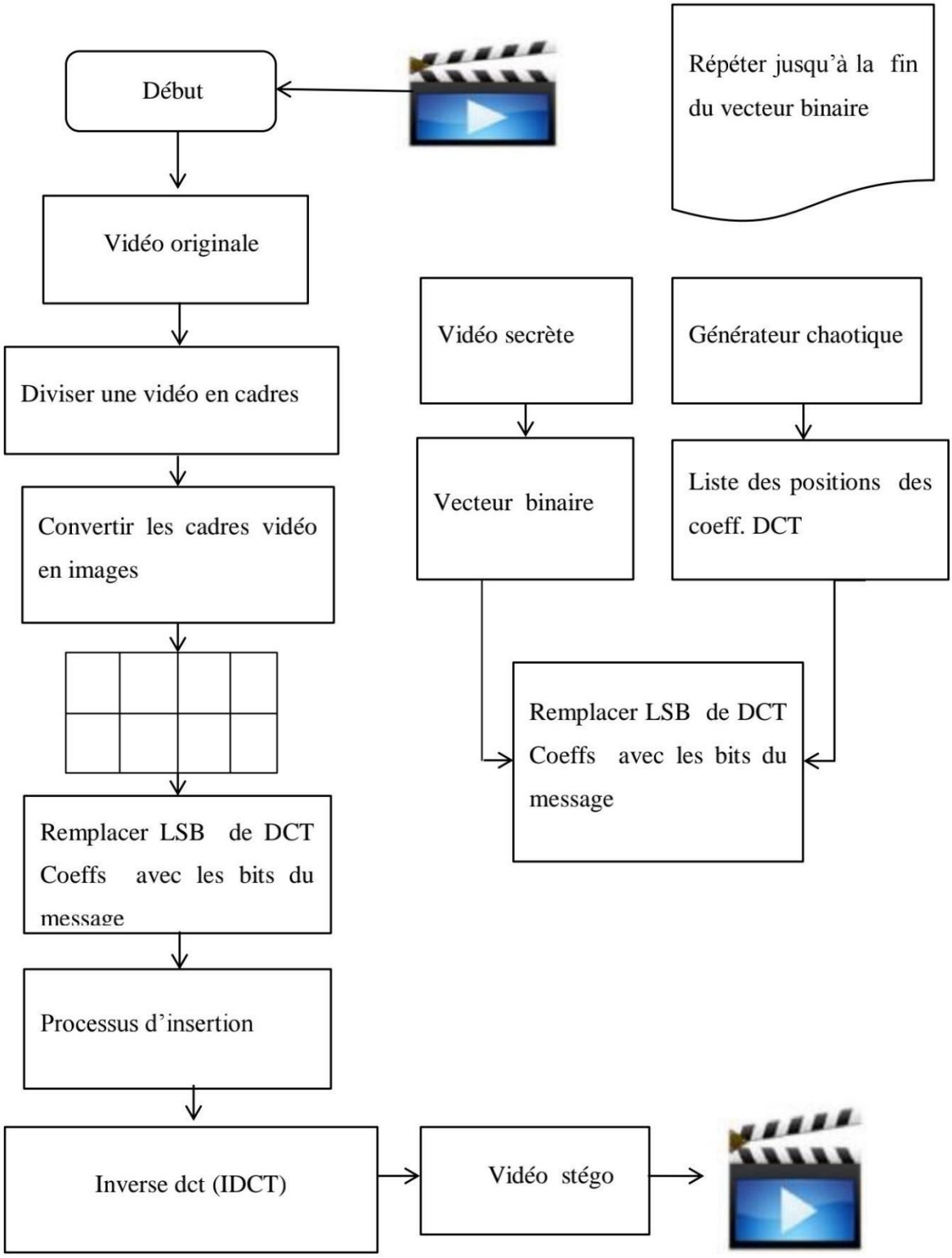


Figure 3. 3 : Diagrammes de Transformées DCT.

La transformée en cosinus discrète est similaire à la Fourier mais elle n'a pas de composante imaginaire. Pour une image de taille M×N la DCT est donnée par :

$$DCT_{kl} = a_k a_l \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} C_{mn} \cos\frac{\pi(2m+1)k}{2M} \cos\frac{\pi(2m+1)l}{2N}$$

$$0 \le k \le M-1 \qquad 0 \le l \le N-1$$

$$a_k = \begin{cases} \frac{1}{\sqrt{M}} & Pour\ k = 0 \\ \sqrt{\frac{2}{M}} & pour\ 1 \le k \le M-1 \end{cases} \qquad a_l = \begin{cases} \frac{1}{\sqrt{N}} & pour\ l = 0 \\ \sqrt{\frac{2}{N}} & pour\ 1 \le l \le -1 \end{cases} \quad (3.1)$$

Ou DCT kl sont les coefficients DCT de la ligne k et la colonne l et C sont les valeurs des pixels de l'image d'origine de la ligne m et la colonne n.

Pour passer du domaine fréquentiel au domaine spatial, il suffit d'appliquer la transformation inverse du cosinus discrète (IDCT) [11].

- **Extraction du message secret**

Pour extraire le message caché on applique les étapes suivantes :

Etape 1 : Lire la vidéo stego.

Etape 2 : Application de la DCT sur la matrice Rouge.

Etape 3 : Parcours de le cadre originale pixel per pixel.

Etape 4 : Si la valeur du coefficient qui correspondant au pixel parcouru est inférieure à 0, on récupère la valeur du bit à poids faible.

Etape 5 : Récupérer et convertir chaque 8 bits en caractères.

3.3.2 Algorithmes à base de DWT

L'utilisation des ondelettes dans la steganographie est récente. Le plus souvent, les techniques proposées conservent le principe du stockage dans les bits les moins significatifs (LSB) mais appliqué aux coefficients de la transformée DWT. Rappelons que l'ondelette divise l'image en des régions de basse (A), de moyenne (H et V), et de haute fréquence (D), ceci pouvant être itéré (plusieurs niveaux). La figure 3.4 montre l'espace de représentation fréquentiel pour une transformée d'ondelette DWT dyadique appliquée sur une image de

niveau 1, 2, et 3. La question principale qui survient lorsque l'on souhaite développer une méthode de steganographie basée DWT est de déterminer quelles bandes fréquentielles (A, H, V, ou D) et quels niveaux (1, 2, ou 3) seront les mieux adaptés. Les différentes techniques existantes vont ainsi principalement se distinguer sur ce point en fonction des applications et objectifs visés : certaines vont cacher les bits secrets dans les basses fréquences, d'autres dans les moyennes, d'autres dans les hautes. Selon, une méthode steganographique cachant l'image secrète dans la bande à basse fréquence (A) possèdera une bonne robustesse puisque la plus grande partie de l'énergie de l'image est stockée dans cette bande. Malgré tout, il existe un risque de dégradation de l'image, si la dissimulation des données n'est pas bien gérée [12, 9, 25].

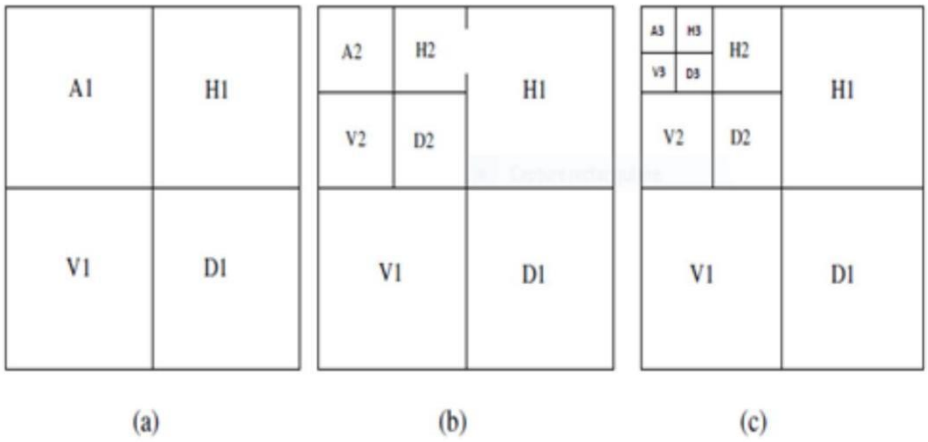


Figure 3. 4 : Décomposition fréquentielle d'une image selon la transformée DWT (a) niveau 1 (b) niveau 2 (c) niveau 3.

- **Les étapes d'extraction d'un message secret**

1. diviser les fichiers vidéo (.AVI) en cadre.

2. Convertir l'image secrète en binaire.

3. Convertir l'image porteuse depuis l'espace couleur RGB en celui YCbCr, le plan Y étant le seul utilisé par la suite pour cacher l'image secrète.

4. Diviser l'image porteuse en blocs 8*8 pixels.

5. Appliquer la transformée DCT sur chaque bloc.

6. Lire le message secret bit à bit.

7. Répéter les étapes 4 et 5 pour chaque block

8. Remonter les cadres

9. Appliquer la transformation Inverse DWT (IDWT) pour obtenir Vidéo stégo.

10. Sauvegarder le nouveau plan Y de cadre contenant le message secret puis reconvertir cadre en RGB.

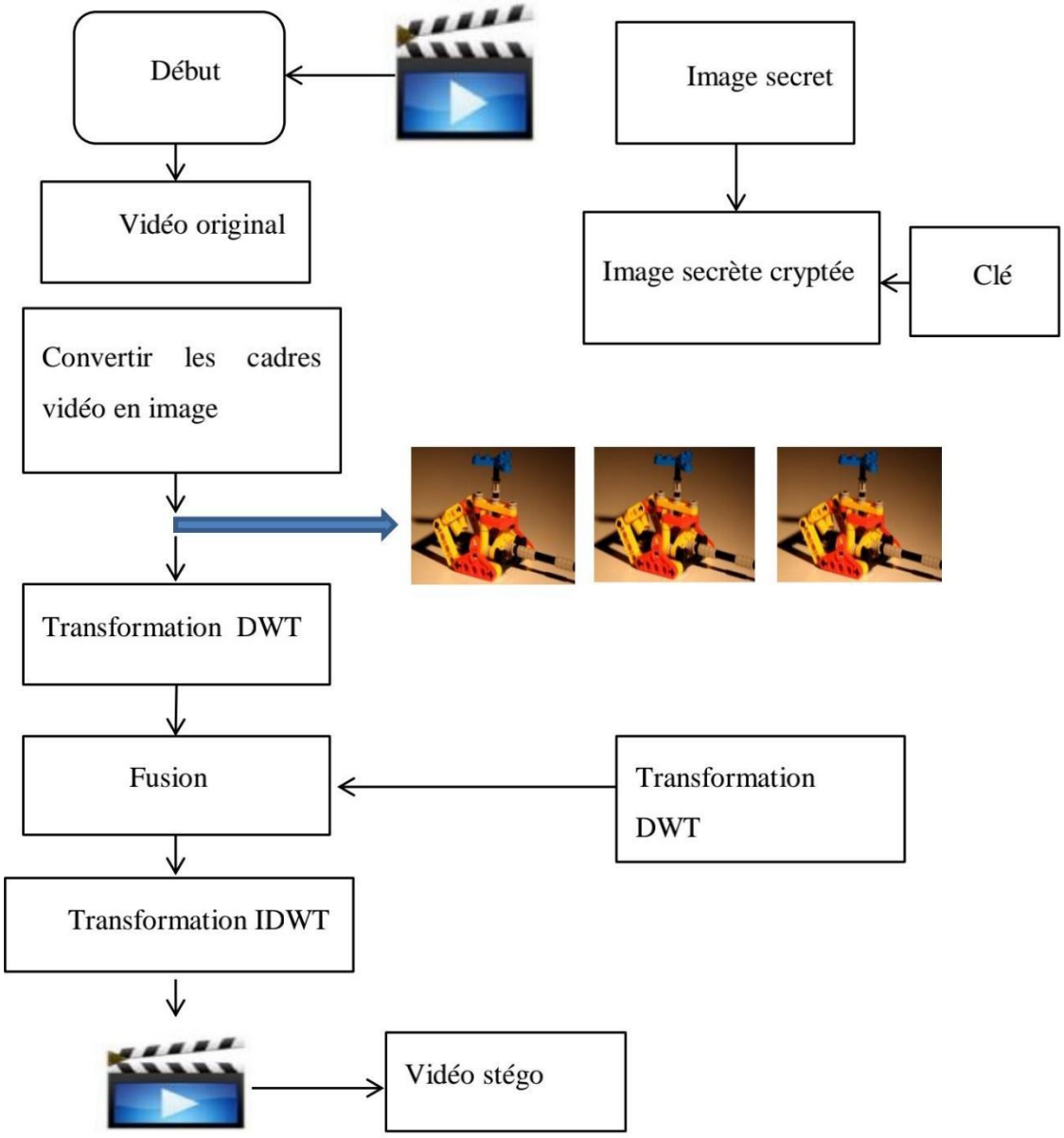


Figure 3. 5 : Diagrammes de Transformées DWT.

3.4 Conclusion

Dans ce chapitre Nous avons étudié les domaines de stéganographie où nous avons mis en évidence trois algorithmes l'algorithme LSB du domaine spatial et les algorithmes DCT, DWT du domaine fréquentiel. Et nous avons abordé les étapes de chaque algorithme et leur fonctionnement et ses diagrammes.

Chapitre 4
Résultats & Discussion

4.1 Introduction

L'objectif principal des algorithmes de stéganographie consiste à fournir des données sécurisées, indétectables et imperceptibles. Les systèmes de dissimilation d'une information dans une image existants sont classés en deux groupes: Les systèmes de dissimilation dans le domaine spatial, Les systèmes de dissimilation dans le domaine fréquentiel [34].

Ce chapitre présent une nouvelle approche de dissimulation d'une information dans une vidéo. Nous montre l'application de notre méthode sur deux vidéos (bunny, small).

notre étude consiste à cacher un message texte à l'intérieur d'une vidéo à l'aide de trois algorithmes(LSB,DCT et DWT), puis nous pouvons calculer des critères, qui sont PSNR et la similarité et le temps d'encodage et de décodage, et nous les comparons pour savoir quel algorithme est le meilleur pour le processus de steganographie à l'intérieur des frame de vidéo.

4.2 Environnement de travail

Dans cette partie, nous présentons les environnements matériels et logiciel utilisés dans notre travail :

1. Environnement matériel

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

Un ordinateur acer caractérisé par :

- Processeur : Intel(R) Core(TM) i3-4005U CPU @ 1.70 GHz
- RAM : 4,00 Go de RAM
- Disque Dur : 500 Go
- Système d'exploitation : Microsoft Windows 10

2. Outils de développements MatlabR2018b

Nous avons implémenté notre système stéganographique, dans l'environnement de Programmation MatlabR2018b, qui permet de manipuler les images avec une grande Simplicité.

MATLAB est un logiciel de calcul numérique, il a été initialement développé à la fin des années 70, pour permettre aux étudiants de travailler à partir d'un outil de programmation de haut niveau et sans apprendre le Fortan ou le C.

MATLAB signifie **Mat**rix **Lab**oratory, il est un langage pour le calcul scientifique, L'analyse de données, leur visualisation, le développement d'algorithmes. Son interface propose d'une part, une fenêtre interactive type console pour l'exécution de commandes, et d'autre part, un environnement de développement intégré (IDE) pour la programmation d'applications.

4.3 Critères de performance

Pour calculer l'imperceptibilité de la stéganographie, de nombreuses métriques sont utilisées. Les métriques montré à quel point le cadre de stago est similaire ou différent du cadre de couverture. Les métriques suivantes sont :

4.3.1 Similarité

En mathématique et en informatique la similarité est un critère important pour l'identification de sous-groupe dans un groupe d'objets, de valeurs (numériques ou non), de données (connues ou reconnues) dans un « espace » ou système...

Du point de vue mathématique, c'est par les différences de distance entre deux données qu'on mesure leur degré de similarité. Dans le champ de l'intelligence artificielle, la similarité est un des critères pour l'analyse informatique de clusters et pour le partitionnement de données (data clustering en anglais).

4.3.2 PSNR

Le calcul en volumes de la qualité de la vidéo stago liée à la vidéo de couverture. La plus le PSNR bien la qualité. Le PSNR est calculé à l'aide de l'équation suivante.

$$PSNR = 20\log_{20} 255 - 10\log_{10} MSE \qquad (6.1)$$

4.3.3 Temps d'encodage

Est le temps de cacher un texte ou une image ... etc, dans les frames du vidéo par les Algorithmes

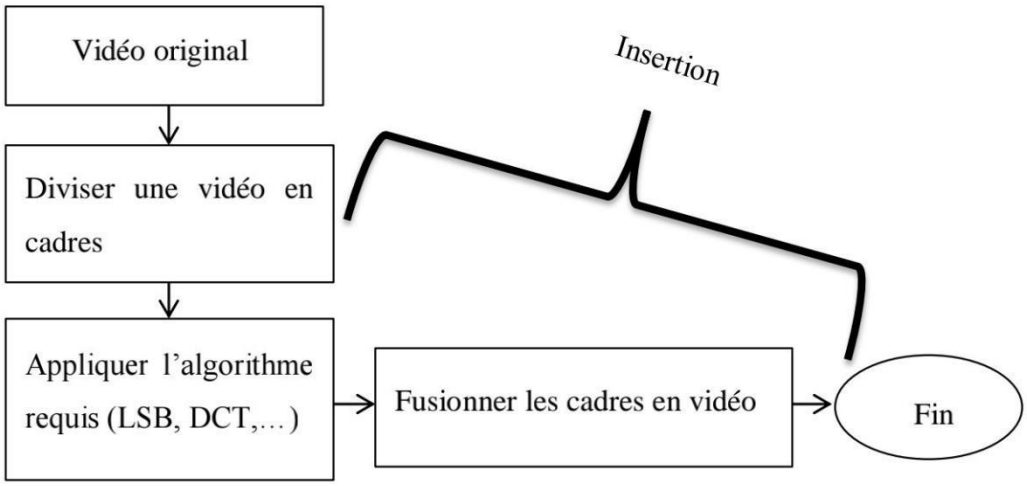


Figure 4. 1 : Temps d'encodage.

4.3.4 Temps de décodage

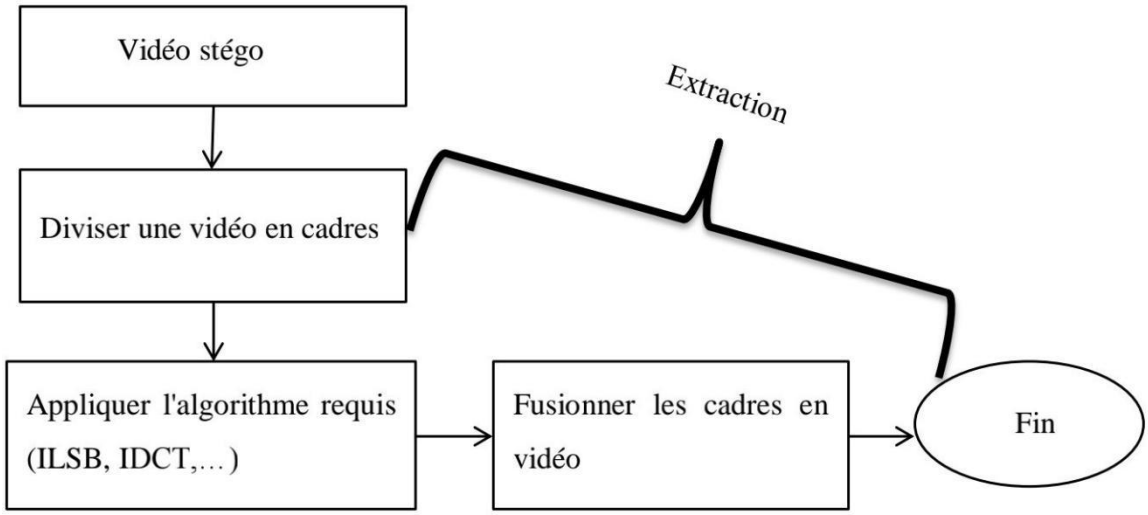


Figure 4. 2 : Temps de décodage.

4.4 Vidéo stéganographie utilisant LSB

Le bit le moins significatif (LSB) est une technique courante et simple pour visualiser des données en vidéo des dossiers. Dans cette méthode, un octet de LSB est remplacé par un bit M. Cette technique convient à la vidéo stéganographie. Pour l'œil humain, la vidéo de la scène ressemble à la vidéo porteuse.

Frame originale (a)

Frame stégo (a)

Frame originale(b)

Frame stégo (b)

Frame originale (c)

Frame stégo(c)

Frame originale (d)

Frame stégo (d)

Figure 4.3 : Frame stego résultante de l'application du LSB.

Nous remarquons que l'image stego ressemble à frame originale, et que le changement n'est pas détectable par l'œil humain, car les bits du message secret sont insérés dans les bits de poids faibles de frame, donc la différence est très petite et indétectable.

Séquence vidéo	**Stego frame**	**Similarité (%)**	**PSNR (dB)**	**Temps d'encodage (s)**	**Temps de décodage (s)**
Bunny_mp4.	Frame1.png	29.16	37.85	0.025	0.053
	Frame16.png	54.77	38.89	0.016	0.0006
	Frame35.png	66.31	39.61	0.021	0.0005
	Frame48.png	39.12	37.03	0.017	0.0006
	Frame60.png	81.68	38.86	0.018	0.0171
	Frame79.png	22.30	39.72	0.018	0.0006
	Frame90.png	48.95	39.86	0.015	0.0005
Small_mp4.	Frame5.png	34.26	41.06	0.02	0.0060
	Frame24.png	35.71	40.48	0.01	0.0005
	Frame49.png	57	41.15	0.01	0.0007
	Frame55.png	14.73	41.07	0.01	0.0005
	Frame60.png	20.53	40.91	0.01	0.0005
	Frame74.png	67.52	41.07	0.015	0.0007
	Frame100.png	32.58	40.65	0.01	0.0005

Tableau4.1 : Résultat obtenait en utilisant la méthode LSB.

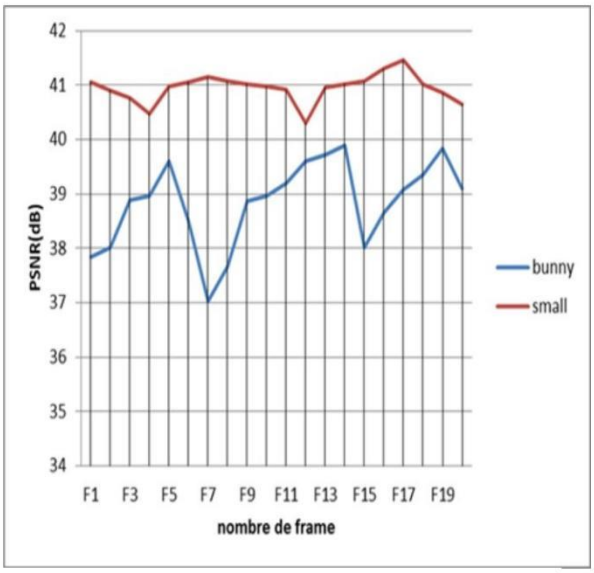


Figure 4. 3 : PSNR de la méthode LSB.

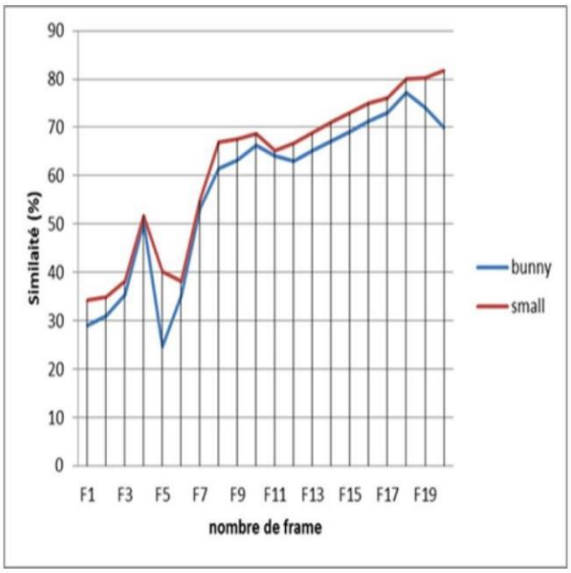


Figure 4. 5: Similarité de la méthode LSB.

D'après le PSNR de la méthode LSB dans la figure 4.4.Nous remarquons les valeurs PSNR de la vidéo (banny) moins par raport le PSNR de la vidéo (small) dans la même figure.

Et pour le graphique de la figure 4.5, Similarité de la méthode LSB qui présente les valeurs de similarité selon les frames de deux vidéos (bunny) (small) nous remarquons que les valeurs sont augmentées toujours dans cette algorithme.

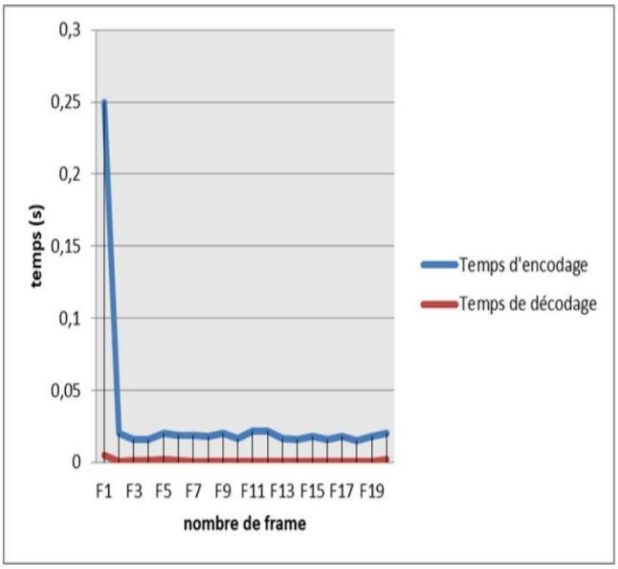


Figure 4.7: Temps d'encodage de la méthode LSB (bunny).

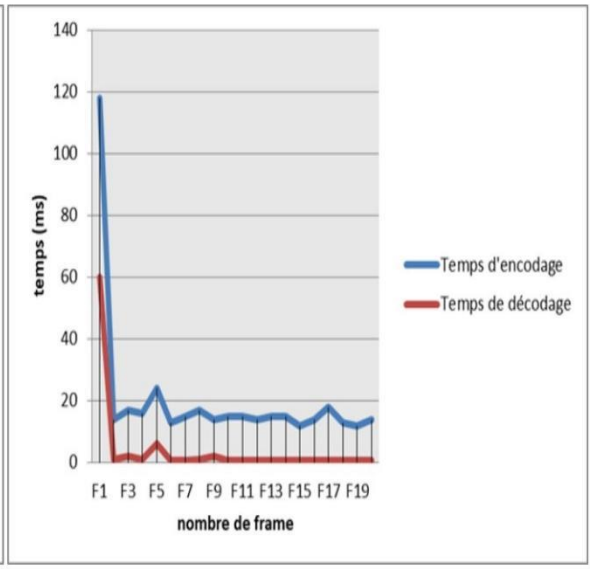


Figure 4. 6 : Temps d'encodage de la méthode LSB (small).

En comparons le Temps d'encodage de la méthode LSB de la vidéo bunny à celle Temps d'encodage de la méthode LSB de la vidéo (small), nous remarquons les valeurs d'encodage (small) supérieur à les valeurs de décodage (bunny).

Ce résultat décrit dans la méthode de LSB, la PSNR, similarité, temps d'encodage et temps de décodage dans la vidéo (bunny) moins para port la vidéo (small) cela est dû à la capacité de chaque vidéo

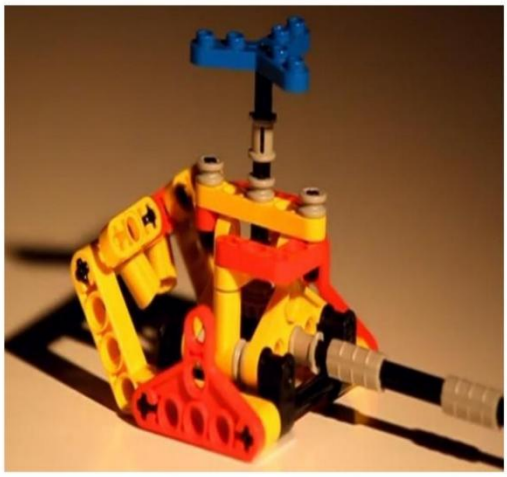
4.5 Vidéo stéganographie utilisant DCT

La technologie DCT joue un rôle crucial dans la technologie de compression et l'image est divisée en carrés de 8 × 8. Chaque carré est transformé par DCT, résultant en un tableau multidimensionnel de 63 sorties de coefficients. Maintenant, les coefficients sont arrondis par le quantificateur. Le filigrane est intégré dans la bande médiane des blocs DCT avec des composants basse fréquence. Il est inséré par réglage du coefficient DCT de l'image et à l'aide de la touche.

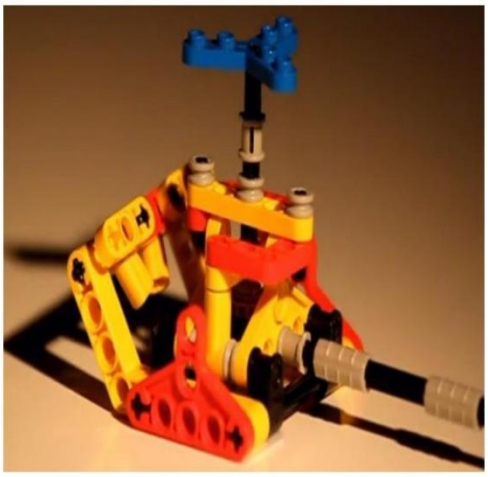
Dans la deuxième expérimentation, nous avons proposé une autre approche qui est plus sécurisée c'est l'approche DCT qui consiste à dissimuler le message seulement dans les bords (contours) de l'image, lorsque on a exécuté le code d'insertion nous avons obtenu les résultats suivants :

Frame originale (a)

Frame stégo (a)



Frame originale (b)



Frame stégo (b)

Frame originale (c)

Frame stégo (c)

Figure 4.8 : frame stego résultante de l'application du DCT.

Séquence de la vidéo	Stego frame	Similarité(%)	PSNR (dB)	Temps d'encodage (s)	Temps de décodage (s)
Bunny_mp4.	Frame1.png	79.12	39.57	2.46	1.32
	Frame16.png	72.72	39.59	2.57	1.28
	Frame35.png	45.45	40.32	2.59	1.61
	Frame48.png	70.04	39.80	2.81	1.41
	Frame60.png	81.15	40.50	2.71	1.34
	Frame79.png	59.09	40.98	3.09	1.66
	Frame90.png	80.23	41.20	3.05	1.24
Small_mp4.	Frame5.png	77.35	41.12	1.95	0.95
	Frame24.png	82.14	46.10	1.87	0.89
	Frame49.png	81.21	47.63	1.90	0.91
	Frame55.png	80.28	47.47	2.03	0.91
	Frame60.png	80.85	46.30	1.88	0.90
	Frame74.png	82.07	46.60	1.87	0.90
	Frame100.png	84.07	47.66	1.89	0.87

Tableau 4. 2 : Résultat obtenu en utilisant la méthode DCT.

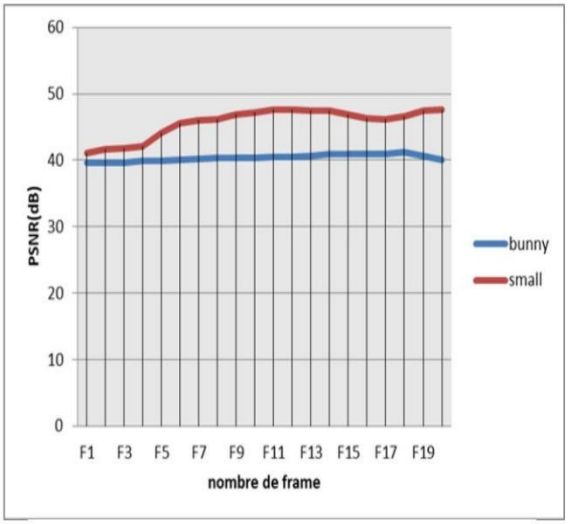


Figure 4. 10: PSNR de la méthode DCT.

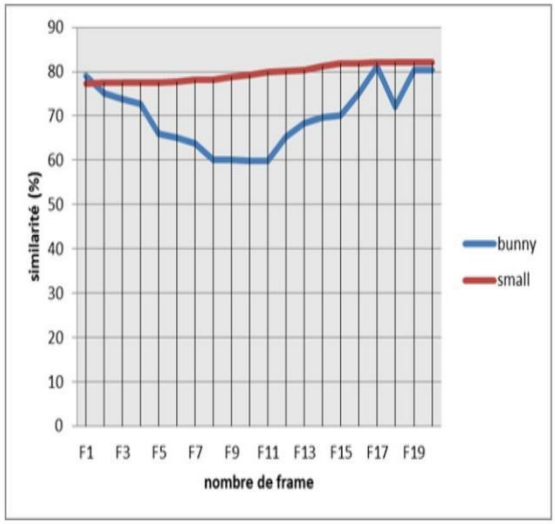


Figure 4. 9 : Similarité de la méthode DCT.

On comparons le PSNR de la vidéo bunny à celle le PSNR de la vidéo small,nous remarqueon les valeurs de PSNR (small) supèrieur à les valeurs de PSNR (bunny) .

Et pour le graphique du figure 4.9.Similarité de la méthode DCT , qui présente les valeurs de similarité selon les frames de deux vidéos (bunny) (small) nous remarquons que les valeurs sont augmentées toujours dans cette algorithme.

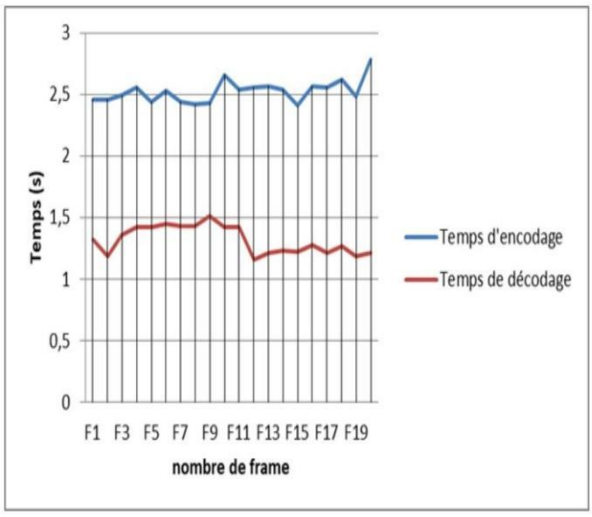


Figure 4. 4 : Temps d'encodage de la méthode DCT (bunny).

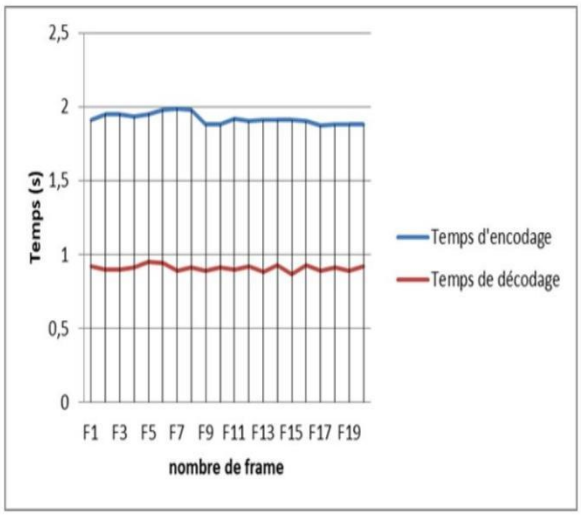


Figure 4. 11 : Temps d'encodage de la méthode DCT (bunny).

En comparons le Temps d'encodage de la méthode DCT de la vidéo bunny à celle Temps d'encodage de la méthode DCT de la vidéo (small), nous remarquons les valeurs d'encodage (small) supérieur à les valeurs de décodage (bunny).

4.6 Vidéo stéganographie utilisant DWT

À l'heure actuelle, DWT a été largement utilisé dans divers domaines d'applications de traitement du signal telles que la compression de la voix, de l'image et de la vidéo. DWT est utilisé pour changer le cadre de l'espace domaine au domaine fréquentiel, et le WC est modifié en texte et autres informations. Cette transformation des coefficients d'ondelettes WC pour diviser les données haute et basse fréquence sur une base de pixel. La méthode DWT est pré-appliquée aux travaux de ce programme. C'est un DWT à deux niveaux, un système de toutes les transformées en ondelettes

Frame originale (a) Frame stégo (a)

Frame originale (b) Frame stégo (b)

Figure 4.13 : frame stego résultante de l'application du DWT.

Séquence de la vidéo	Stego frame	Similarité(%)	PSNR (dB)	Temps d'encodage (s)	Temps de décodage (s)
Bunny_mp4.	Frame1.png	36.33	39.83	0.68	0.34
	Frame16.png	50.20	39.85	0.73	0.30
	Frame35.png	45.00	40.74	0.66	0.30
	Frame48.png	70.00	40.18	0.66	0.31
	Frame60.png	69.11	41.01	0.68	0.32
	Frame79.png	69.33	41.28	0.67	0.32
	Frame90.png	72.94	41.50	0.65	0.30
Small_mp4.	Frame5.png	45.36	39.40	0.45	0.12
	Frame24.png	51.07	39.76	0.53	0.10
	Frame49.png	65.18	40.14	0.47	0.08
	Frame55.png	71.86	40.56	0.53	0.12
	Frame60.png	72.14	41.12	0.57	0.16
	Frame74.png	78.56	41.21	0.49	0.24
	Frame100.png	82.80	41.04	0.45	0.30

Tableau 4. 3 : Résultat obtenu en utilisant la méthode DWT.

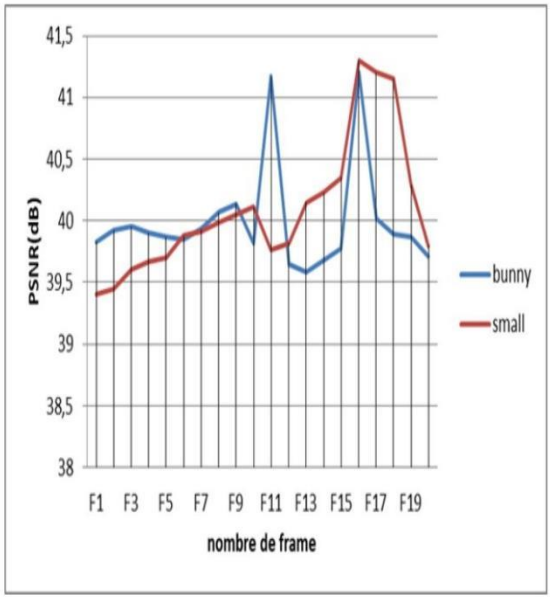


Figure 4. 15: PSNR de la méthode DWT.

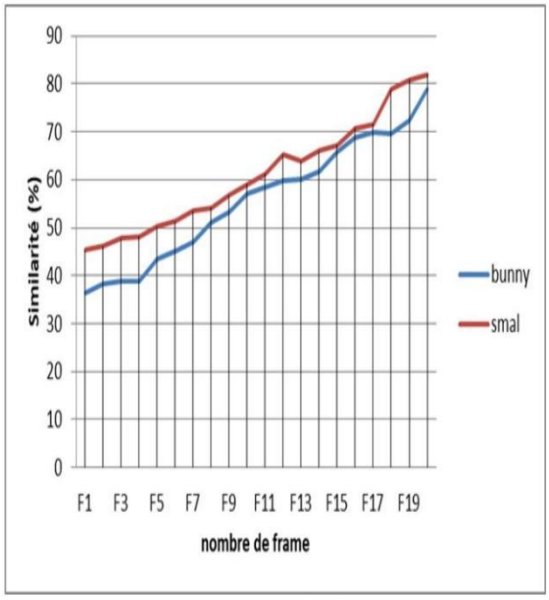


Figure 4.14: Similarité de la méthode DWT.

Dans la figure 4.15.PSNR de la méthode DWT qui présente les valeurs de la critère PSNR selon les frames de deux séquences vidéo (bunny) (small) nous remarquons que les valeurs sont élevées dans les deux séquences.

Dans la figure 4.14 similarité de la méthode DWT qui présente les valeurs de la similarité selon les frames de deux séquences vidéo (bunny) (small) nous remarquons que les valeurs sont augmentées toujours dans les deux séquences et la séquence (small) plus élevée que la séquence (small).

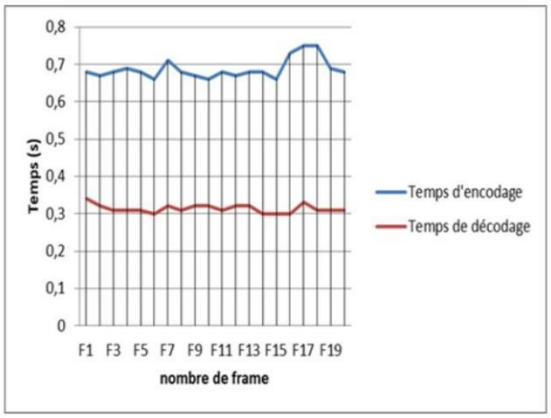


Figure 4. 17: Temps d'encodage et décodage de la méthode DWT (bunny).

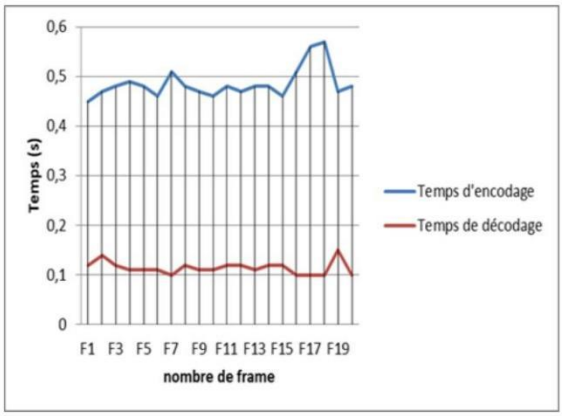


Figure 4. 5 : Temps d'encodage et décodage de la méthode DWT (small).

En comparons le Temps d'encodage de la méthode DWT de la vidéo bunny à celle Temps d'encodage de la méthode DWT de la vidéo (small), nous remarquons les valeurs d'encodage (small) supérieur à les valeurs de décodage (bunny)

4.7 Comparaisons entre LSB, DCT et DWT :

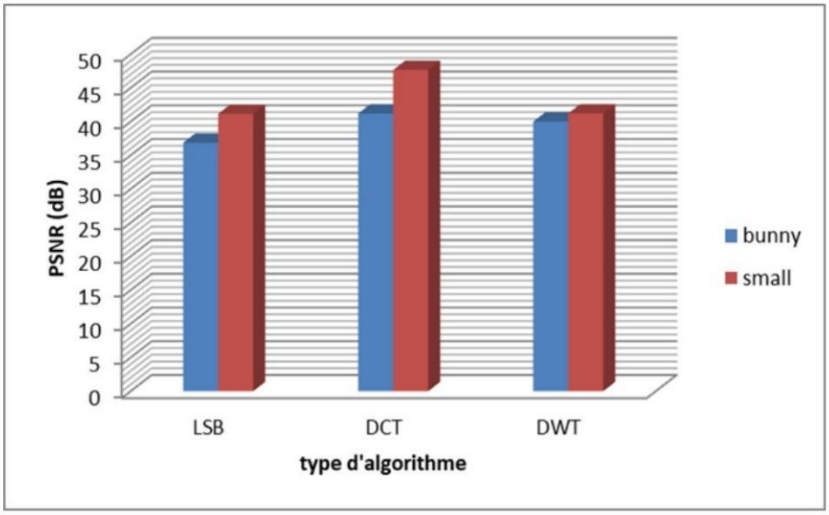


Figure 4. 18: PSNR dès les méthodes DWT, DCT et LSB.

J'aimerais vous présenter un graphique qui présente les valeurs de la critère PSNR selon les frames de deux séquences vidéo 'bunny' en couleur bleu et 'small' en couleur rouge en les trois algorithmes 'LSB' 'DCT' 'DWT' On constate tout d'abord que les valeurs du critère PSNR sont augmentées dans les trois algorithmes et toujours dans la séquence vidéo 'small' sont plus élevés que la séquence vidéo 'bunny' .Aussi nous remarquons que les valeurs de l'algorithme DCT plus haut par rapport de l'LSB et le DWT.Le graphique nous montre donc que le critère PSNR être élevé dans l'algorithme DCT.

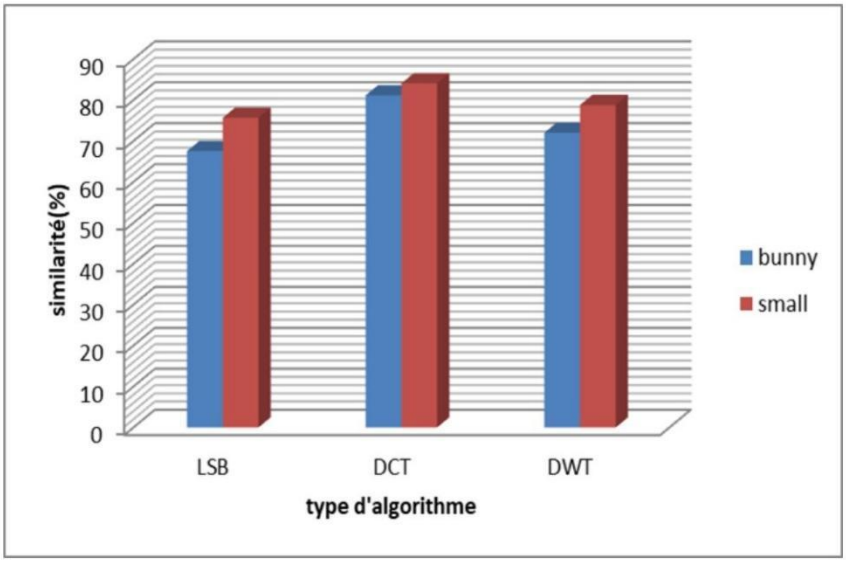


Figure 4. 19 : Similarité dès les méthodes DWT, DCT et LSB.

J'aimerais vous présenter un graphique qui présente les valeurs de la similarité selon les frames de deux séquences vidéo 'bunny' en couleur bleu et 'small' en couleur rouge en les trois algorithmes 'LSB' 'DCT' 'DWT' On constate tout d'abord que les valeurs de la similarité sont augmentées dans les trois algorithmes et toujours dans la séquence vidéo 'small' sont plus élevés que la séquence vidéo 'bunny' .Aussi nous remarquons que la similarité de l'algorithme DCT plus haut par rapport de l'LSB et le DWT.Le graphique nous montre donc que la similarité être élevé dans l'algorithme DCT

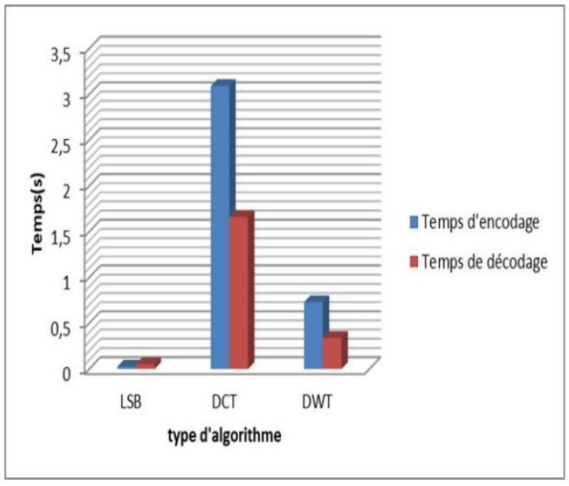


Figure 4. 6 : Temps d'encodage et décodage dès les méthodes DWT, DCT et LSB (bunny).

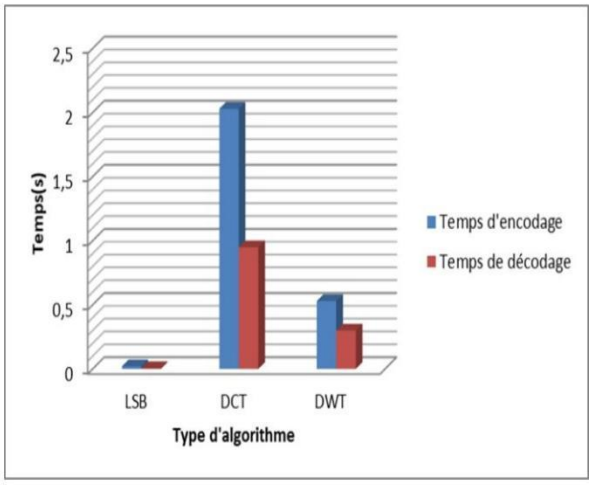


Figure 4. 21: Temps d'encodage et décodage dès les méthodes DWT, DCT et LSB.

J'aimerais vous présenter deux graphiques qui présentent les valeurs de temps d'encodage et le temps de décodage selon les frames de le séquence vidéo 'bunny' pour la figure(4.18), et la séquence vidéo 'small' pour la figure(4.19), en les trois algorithmes 'LSB' 'DCT' 'DWT' On constate tout d'abord que les valeurs du temps d'encodage et de décodage sont très faibles dans l'algorithme LSB dans les deux séquences .Ensuite les valeurs sont très élevées dans les deux séquences vidéo dans l'algorithme DCT .Aussi nous remarquons que le temps d'encodage et de décodage de l'algorithme DWT élevés par rapport l'LSB.

Les deux graphiques nous montrons donc que l'algorithme dct prenait un temps d'encodage et de décodage plus élevé par rapport les deux autres algorithmes.

4.8 Comparative entre les troix méthode

Cette étude introduit certaines méthodes de stéganographie vidéo telles que LSB, DCT et DWT. Il s'agit d'une tentative de calcul et de comparaison de tous les paramètres de la stéganographie vidéo (similarité, PSNR, temps d'encodage, temps de décodage), À partir des résultats ci-dessus, il est conclu que les frames de la vidéo stégo par l'algorithme DCT a une meilleur qualité par rapport à les frames de la vidéo stégo de les autres algorithmes (LSB , DWT) .Il existe une amélioration significative mesurée de PSNR , Similarité, de l'algorithme DCT par rapport l'LSB et la DWT .Les changements de temps d'encodage et de décodage élevés dans l'algorithme DCT par rapport à les 2 autres algorithmes (LSB, DWT)

On conclut donc que l'algorithme DCT est le meilleur algorithme par rapport à l'LSB et la DWT

4.9 Conclusion :

Dans ce chapitre, le travail présenté sert à la dissimulation d'un message secret dans une vidéo numérique. Pour ce faire, nous avons proposé trois systèmes stéganographiques basés sur les algorithmes : LSB, DCT et DWT pour l'insertion des bits de message dans les pixels de frame (cadre) dans le cas de codage, et l'extraction de ces bits dans le cas de décodage. Nos résultats obtenus sous MATLAB indiquent que les Algorithmes utilisés sont efficaces en termes de : non déformation de la vidéo et difficulté de stéganalyse.

Conclusion Générale

Le travail présenté dans ce mémoire, s'inscrit dans le but de la stéganographie et plus précisément l'insertion d'un message secret à l'intérieur d'une vidéo numérique. Dans notre travail, nous avons proposé trois algorithmes de stéganographie pour l'insertion des messages, l'un dans le domaine spatial on parle sur le LSB, l'autre utilise le domaine fréquentiel on parle sur la DCT et le dernier utilise le domaine spatiaux-fréquentielle on parle sur le DWT.

Cette recherche présente quelques méthodes de stéganographie vidéo telles que LSB, DCT et DWT. C'est une tentative de calcul et de comparaison de tous les paramètres de la stéganographie vidéo (Similarité, PSNR. Temps d'encodage, Temps de décodage) et la meilleure technique est la DCT par rapport à LSB et DWT. Le tableau n° 4.1(LSB), 4.2(DCT) et 4.3(DWT) contient les résultats de PSNR, Similarité, Temps d'encodage et Temps de décodage. Le meilleur résultat apparaît dans le tableau n°4.2(DCT). Le PSNR variait entre 39,57 et 41,20 dB qu'en utilisant la DCT. Tous les résultats sont simulés dans le Logiciel MATLAB 2018a.steganography appliqué pour deux vidéos (mp4, bunny et small) utilisées dans cette recherche.

Dans des recherches futures, nous allons essayer de réaliser d'autres systèmes de stéganographie en utilisant d'autres techniques comme la F5,et on va essayer de programmer des algorithmes de stéganalyse pour détecter l'existence d'un message caché, et pourquoi pas, utiliser de nouveaux supports pour cacher notre message tel qu'une audio par exemple .

Résumé:

La sécurité de l'information est devenue un problème primordial pour toute personne.

Une réponse à cette sécurité garantissant la confidentialité dans la communication est offerte par la stéganographie.

La stéganographie est l'art d'incorporer une information (masquée) dans une autre (une couverture). L'élément incorporé de façon masquée doit être plus court que la couverture pour éviter de trop la détériorer. L'information numérique à l'état brut peut généralement subir de nombreuses compressions destructives par élimination de données inutiles. 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, toute sorte de types de fichiers numériques : images, sons, vidéos, trames de données etc..., peuvent être utilisé.

L'objectif essentiel de ce projet est, de faire une synthèse détaillée, en vue d'une étude comparative, de plusieurs algorithmes de dissimulation de données numériques dans des trames ou séquences vidéo. Tous les algorithmes étudiés seront implémentés à l'aide du logiciel de simulation Matlab, et enfin de les comparés.

Mots-Clés : Stéganographie, Sécurité, Données dissimulées, LSB, Stégo-vidéo, Stéganalyse, Vidéo.

Abstract:

Information security has become a primary issue for everyone. A response to this security guaranteeing confidentiality in communication is offered by steganography.

Steganography is the art of incorporating one (hidden) piece of information into another (a cover). The hidden embedded element must be shorter than the cover to avoid damaging it too much. Raw digital information can generally be subject to many destructive compressions by eliminating useless data. The idea is then to replace this useless data, these parasitic background noises by more useful data which will in fact be the data that we want to hide. To hide data, all kinds of types digital files: images, sounds, videos, data frames etc..., can be used.

The essential objective of this project is, to make a detailed synthesis, with a view to a study comparative analysis of several algorithms for concealing digital data in frames or video sequences. All the studied algorithms will be implemented using the simulation Matlab, and finally to compare them.

Key-words: Steganography, Security, Hidden Data, LSB, Stego-video, Steganalysis, Video.

ملخص

اصبح امن المعلومات مشكلة اساسية لكل شخص .يتم تقديم الرد على هذا الامان الذي يضمن السرية في الاتصال عن طريق اخفاء المعلومات .اخفاء المعلومات هو فن دمج معلومة في معلومة اخرى . يجب ان يكون العنصر المدمج بطريقة مخفية اقصر من الغطاء لتجنب اتلافه كثيرا .يمكن للمعلومات الرقمية في حالتها الولية ان تخضع عموما للعديد من الضغوطات المدمرة عن طريق ازالة البيانات غير الضرورية .الفكرة اذن هي استبدال هذه البيانات عديمة الفائدة والتي ستكون في الواقع البيانات التي نريد اخفاءها .لاخفاء البيانات يمكن استخدام جميع انواع الملفات الرقمية الصور والاصوات ومقاطع الفيديو واطارات البيانات وما الى ذلك.الهدف الاساسي لهذا المشروع هو اجراء تجميع مفصل بهدف اجراء دراسة مقارنة لعدة خوارزميات لاخفاء البيانات الرقمية في اطارات او تسلسلات الفيديو .سيتم تنفيذ جميع الخوارزميات التي تمت دراستها باستخدام برنامج محاكاة ماطلاب ثم مقارنتها في النهاية .

Bibliographie

[1] C. Zitzmann : « Détection statique d'information cachée dans des images naturelles ». Thèse doctorat, Université de Technologie De Troyes (France). Soutenue le 24/06/2013.

[2] Hérodot : « L'Enquête » : Livres I à IV, vol. 1 de collection folio. Traduit par A. Barguet. Editions Gallimard, 1985.

[3] Hérodot : « L'Enquête » : Livre V à IX, vol .1 de collection folio. Traduit par A. Barguet. Editions Gallimard, 1990.

[4] S. Kouider : « Insertion adaptative en stéganographie : Application aux images numériques dans le domaine spatial ». Thèse de doctorat, Université de Montpellier II (France). Soutenue le 17/12/2013.

[5] I. Bougerne : « la sélection des caractéristiques parallèle pour la stéganalyse ». Thèse de doctorat, Université de Annaba. Soutenue en 2017.

[6] G.J. Simmons : « the prisoners' problem and the subliminal channel ». In David CHAUM, éditeur, « Advance in Cryptograph », page 51-67. Springer US, 1984.

[7] M. Bouab : «Tatouage d'image basé sur des propriétés psycho visuelle ». Mémoire de magister, option : électronique, Université Mentouri Constantine (Algérie), 2006.

[8] A. Adjila : « Signatures numériques pour fichiers audio (audio watermarking) ». Mémoire de magister, Université Kasdi-Merbah Ouargla (Algérie). Soutenue en 2013.

[9] L. Marvel, C. G. J. Boncelet, C. T. Retter : « Spread Spectrum Image Steganography ». IEEE Transactions on Image processing, vol (8), 1999.

[10] S. O. Akimola, A. A. Olatidoye : « On The Image Quality And Encoding Times Of LSB, MSB And Combined LSB-MSB Steganography Algorithms Using Digital Images ». International Journal Of Computer Science & Information Technology (TJCSIT), vol(7), no 4, August 2015.

[11] B. S. Champakamala, K. Padmini, D. K. Radika : « Least Significant Bit algorithm for image steganography ». International Journal of Advenced Computer Technology, vol(3), No 4.

[12] D. Batikh : « Sécurité de l'information par stéganographie basée sur les séquences chaotiques ».Thèse de doctorat, Université de Beyrouth (LIBAN). Soutenue le 18/05/2015.

[13] J. Barbier : « Analyse de canaux de communication dans un contexte non coopératif ». Thèse de doctorat, école supérieure et d'application des transmissions école polytechnique, Laboratoire de virologie et cryptologie. Soutenue le 28/11/2007.

[14] N. Kaur, S. Behal : « A Survey on Various Types of Steganography and Analysis of Hiding Technique ». International Journal of Engineering Trends and Technology (IJETT), volume (11), Number 8, p-389, May 2014

[15]L. Laimeche : « Détection des informations cachées dans les images numériques basées loi de ZIPF ». Mémoire de magister, Université de Tébessa (Algérie). Soutenu le 10/01/2010

[16]AL-Shatnawi, M. Attalah, and Bader m. Alfawwaz : «An Integrated Image Steganography System With Improved Image Quality». Applied Mathematical Sciences, vol.71(7) (2013) : 3545-3553

[17]B. Souvik and G. Sanyal : « A Robust Image Steganography Using DWT Difference Modulation (DWTDM) ». International Journal of Computer Network & Information security 4.7 (2012)

[18]H. Singh, P. K. Singh, K. Saroha : «A Survey on Text Based Steganography ». Proceeding of the 3rd National conference, INDIAcom-2009 computing for nation development, February 26-27, 2009 Bharati Vidyapeeth's Institute of computer Applications and Management, New Delhi

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

[20]N. Provos : « Defending against statistical steganography ». in proceedings of the 10th conference on USENIX security symposium, vol (10), SSYM'01, Washington, D. C. USENIX Association, 2001

[21]A. Ali. Pacha, N. Hadj-Said, A. Belgoraf, A. M'hamed : « stéganographie : Sécurité par Dissimulation ». Revue de l'information scientifique et technique, vol (6), Numéro 1, p 90-103, 2006

[22]S. Saejung, A. Boondee, J. Preechasuk, C. Chantrapornchai : « On the comparison of digital image steganography algorithm based on DCT and wavelet». In computer science and Engineering conference (ICSEC), p 328-333, (2013)

[23]S. Goal, A. Rana, M. Kaur : « Comparison of image steganography technique ». International Journal of computers and Distributed Systems, Vol 3, Issue I, (2013)

[24]G. S. Sravanthi, B. Sunitha Devi, S. M. Riyazoddin, M. Janga Reddy : « A spatial Domain Image Steganography Technique Based on Plan Bit Substitution Method ». Global Journal of Computer Science and Technology Graphics & Vision, vol (12), Issue 15, Version 1.0, 2012

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

[26] H. Kaur, J. Rani : «A survey on different techniques of steganography ». Conf. ICAET, Punjab, India, 2016.

[27] P. Malathi, T. Gireesh Kumar : « Relating the embedding efficiency of LSB steganography techniques in spatial domain ». 6th International Conference on Advances In Computing & Communications, ICACC 2016, 6-8 septembre 2016, Cochin, India.

		Notations et Abréviations
DCT	:	***D***iscrète ***C***osine ***T***ransformé
LSB	:	***L***east ***S***ignificant ***B***it
DWT	:	***D***iscrète ***W***wavelet ***T***ransformé
RGB	:	**R**ouge **G**reen **B**leu
PSNR	:	**Peak S**ignal **T**o **N**oise **R**atio
ASCII	:	**A**merican **S**tandard **C**ode **F**or **I**nformation **I**nterchange
JPEG	:	**J**oint **P**hotographie **E**xpert **G**roup
IDCT	:	**I**nvers **D**iscrète **C**osine **T**ransform