République Algérienne Démocratique et Populaire
الجمهـــوريـــــــة الجـــزائـريـــــة الديمقراطية الشعبيـــــــــــــة
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique
وزارة التعليـــــــــــــم العـــالـــــــــي و البحـــــــــث العلمـــــــــــــي

Exposé sur :

La Stéganographie

Module : Sécurité Informatique

Réalisé par :

- BOUGHERRA Maha
- BOUZEMBRAK Yasmine

Groupe : 06

Enseignant : Monsieur M.ANANE

SOMMAIRE

Table des matières

I. INTRODUCTION :

Les hommes cherchent depuis l'Antiquité des méthodes pour transmettre des informations secrètement. Celles-ci reposent sur deux grands principes :

- Chiffrement : utilisé pour rendre les informations transmises illisibles pour les personnes tentant de les intercepter mais qui ne cherche pas à dissimuler la transmission du message.
- Dissimulation d'information : utilisé pour rendre la transmission d'information indétectable en la dissimulant à l'intérieur de données transmises en clair.

Ces méthodes peuvent être et sont souvent combinées mais nous allons nous concentrer aujourd'hui sur la dissimulation d'informations plus particulièrement **la stéganographie.**

II. HISTORIQUE :

En effet la stéganographie est l'art de dissimuler des données. Bien que ce qui nous intéresse ici soit en rapport avec l'informatique, il peut être intéressant de revenir un peu en arrière.

L'apparition de la stéganographie est très ancienne, et à peu près contemporaine de celle de la cryptographie. Ainsi on se rend compte que la première forme de stéganographie répertoriée nous vient d'une histoire Grèque signé Herodote et datant du 5eme siècle avant Jésus-Christ.

Ainsi le Conseiller du roi Darius à la cour de Perse, il voulut organiser une révolte contre les Perses vers 500 av J-.C. Pour transmettre son message à Aristagoras, il eut l'idée de raser la tête de son esclave le plus fidèle, de lui tatouer son message sur le crâne et d'attendre que les cheveux repoussent avant de l'envoyer, avec pour consigne de se faire raser les cheveux.

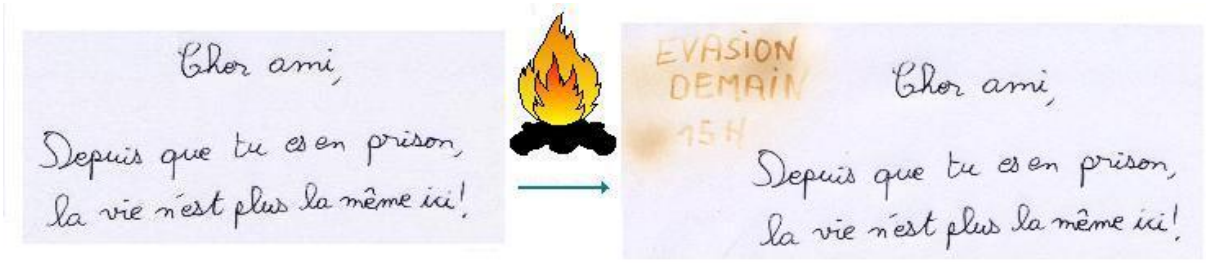
Un autre passage des Histoires relate l'histoire de Demarate, ancien roi de Sparte réfugié auprès du roi des Perses, Xerxès Ier, qui a succédé à Darius. Demarate fut mis au courant d'un projet d'invasion de la Grèce. Il décida alors de prévenir Sparte en toute discrétion en utilisant le stratagème suivant : "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."

Les tablettes étant arrivées à Sparte, la reine Gorgô fit gratter la cire et découvrit ainsi le message de Démarate.

Ces histoires illustrent déjà les deux principales méthodes de stéganographie utilisées au cours des siècles. On pourra essayer de cacher physiquement l'existence d'un message, comme sur le crâne d'un esclave. Ou alors on dissimulera le message sur un support qui

transmet déjà de l'information, comme les tablettes de cire. Ces deux méthodes ont toujours cohabité, même si la seconde fut sans doute plus populaire.

Le plus connu des procédés de stéganographie est sans doute l'utilisation d'encres sympathiques, mentionnée par Pline l'Ancien dès le premier siècle avant J.-C. On écrit, au milieu des textes écrits à l'encre, un message à l'aide de jus de citron, de lait, de certains produits chimiques. Il est invisible à l'œil, mais une simple flamme, ou un bain dans un réactif chimique, révèle le message. L'exemple suivant a été réalisé à l'aide de lait :



1. La technique d'encres sympathiques.

Une autre méthode très répandue de stéganographie est de dissimuler le message dans le texte lui-même. Un des maitres en la matière fut l'abbé Jean Trithème. Il substituait à chaque lettre une phrase religieuse. Le sens final est obscur, mais ce qui n'est qu'une simple substitution se trouve amplifiée par la dissimulation.

A = dans les cieux	N = en paradis
B = à tout jamais	O = toujours
C = un monde sans fin	P = dans la divinité
D = en une infinité	Q = dans la déité
E = à perpétuité	R = dans la félicité
F = sempiternel	S = dans son règne
G = durable	T = dans son royaume
H = sans cesse	U-V-W = dans la béatitude
I-J = irrévocablement	X = dans la magnificence
K = éternellement	Y = au trône
L = dans la gloire	Z = en toute éternité
M = dans la lumière	

III. DEFINITION:

Stéganographie vient du Grec « steganos » (dissimulé), et « graphy » (écriture- dessin) et signifie donc « écriture dissimulée » ou « dessin dissimulé ».

La stéganographie est l'art de la dissimulation. Elle consiste à cacher un message au sein d'un autre message anodin, de sorte que l'on ignore l'existence même du secret. Donc c'est un

ensemble de techniques permettant de transmettre une information en la dissimulant au sein d'une autre information apparemment inoffensive « photo, vidéo, texte, son etc.».

Cette science a toujours été utilisée à des fins d'espionnage et il existe une multitude de techniques stéganographiques. Actuellement elle rencontre un regain d'intérêt à cause des deux faits suivants :

- **Les évènements du 11 Septembre 2001** : Les services secrets américains ont émis l'hypothèse selon laquelle les réseaux terroristes d'Al-Qaida utilisent la stéganographie pour cacher des messages dans des images publiées sur des sites internet. Le gouvernement américain a financé de nombreux programmes de recherche pour mettre au point des web crawlers (ou web spiders) chassant les images suspectes.
- **Les logiciels espions** : Des canaux cachés sont établis par des logiciels pour divulguer des informations à l'insu de l'utilisateur. Par exemple, le logiciel espion décrit dans la partie « *Covert channel* ».

a. Concepts de base :

Trois éléments interviennent dans la dissimulation d'information :

- **Le medium de couverture** : il s'agit du médium dans lequel seront dissimulées les informations. Il peut s'agir d'un texte, d'une image, d'un son, d'une vidéo…
- **Données :** ce sont les informations qui vont être cachées dans le médium de couverture. Il peut s'agir de n'importe quel type de données.
- **Stego-object ou stego-medium** : on appelle ainsi le médium de couverture après dissimulation des données à l'intérieur.

b. Schémas de stéganographie :

De la même façon qu'en cryptographie il existe plusieurs systèmes de stéganographie :

- **La stéganographie pure** : aucune entent préalable n'est nécessaire entre Alice et Bob, il suffit qu'ils utilisent le même algorithme de cryptage.
- **La stéganographie à clé secrète** : Alice et Bob conviennent d'une clé secrète servant à insérer et extraire le message.
- **La stéganographie à clé publique** : l'expéditeur utilise la clé publique du destinataire pour insérer le message et le destinataire l'extrait à l'aide de sa clé publique
  En stéganographie, la clé détermine les portions de l'image ou sera caché le message
  Il est possible de dissimulé des messages cryptés.

La robustesse est peu importante en stéganographie car le médium ne sera pas modifié alors que l'imperceptibilité et la capacité sont très importantes.

IV. LES METHODES DE STEGANOGRAPHIE :

Les méthodes de stéganographie sont potentiellement illimitées, mais aujourd'hui quelques techniques courantes dominent le marché des logiciels de stéganographie. Les messages sont généralement cachés dans des images ou bien des textes.

a. La stéganographie linguistique :

Dans ce cas, le médium de transmission est un texte, tout comme le message à cacher. Cela consiste à placer les mots ou les caractères du message parmi les mots du texte et, par conséquent le message est noyé dans la quantité de mots du médium de couverture, tout en obtenant un texte ayant un sens. La détermination de la position des mots du texte est une tâche fastidieuse demandant une grande maîtrise de la langue. Le placement des mots ou des caractères se fait par:

- Modification des espaces/tabulations entre les mots.
- Alternances MAJUSCULES/minuscules.

Exemple de dissimulation:

Texte à dissimuler: **Bring two cases of beer.**

Le stego-medium: **B**ig **r**umble **i**n **N**ew **G**uinea.

The **w**ar **o**n **c**elebrity **a**cts **s**hould **e**nd **s**oon.
Over **f**our **b**ig **e**cstatic **e**lephants **r**eplicated.

b. La stéganographie technique :

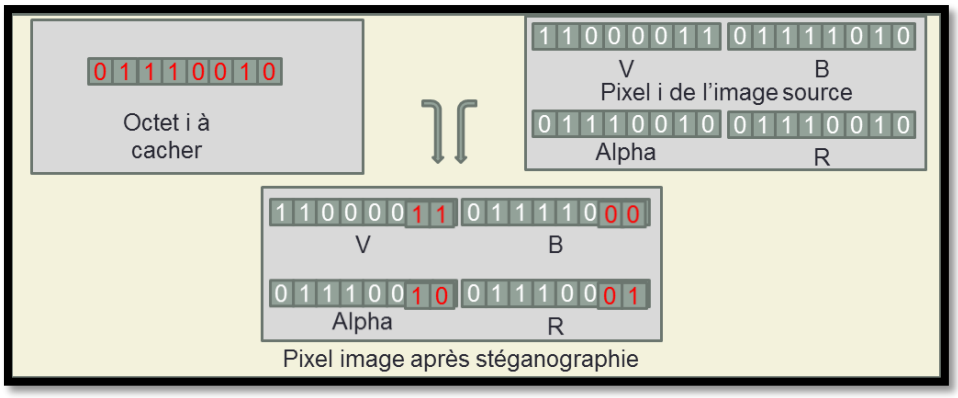
Cette dernière regroupe toutes les techniques qui ne jouent pas sur les mots. Contrairement à la stéganographie linguistique, ce type de stéganographie permet d'utiliser tous types de média de couverture : (image, texte, son, vidéo). Le médium le plus utilisé reste l'image.

L'utilisation des images pour dissimuler des données s'inscrit dans la catégorie de la stéganographie technique. Il faut rappeler qu'une image est formée d'un ensemble de pixels et que chaque pixel est sur 4 octets : R (rouge), V (vert), B (bleu) et Alpha (luminosité). La dissimulation peut être faite sur la base de plusieurs algorithmes différents tous ayant comme objectif : dissimuler les données sans déformer l'image d'une manière visible à l'œil nu.

Pour cela, l'algorithme le plus utilisé est le LSB.

i. L'algorithme LSB « Least Signifiant Bit » :

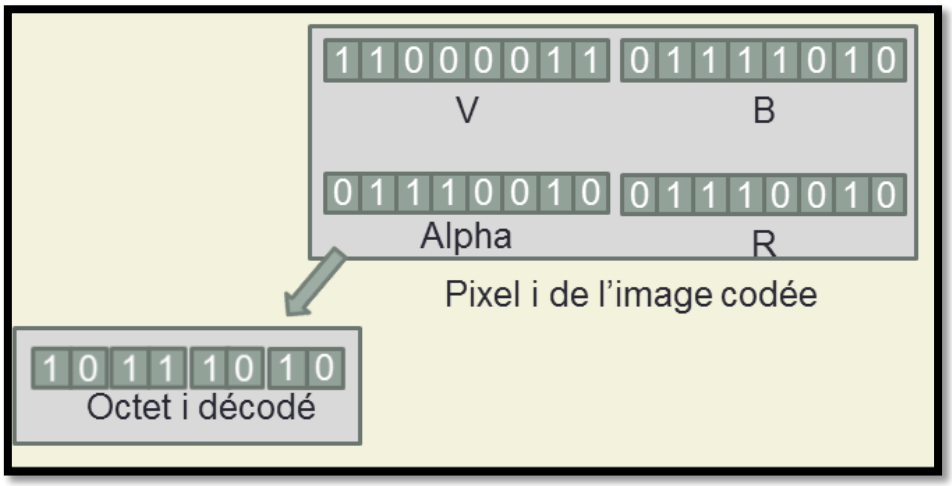
LSB, est l'acronyme de « Last Significant Bit ». Le bit le moins significatif de chaque composante du pixel est remplacé par celui de la donnée à cacher, comme schématisé dans la figure ci-dessous.



2. L'algorithme de dissimulation avec la technique LSB.

Les couleurs ainsi obtenues subissent une très faible variation, imperceptible à vue d'œil.

Lors du décodage, on récupère les bits de poids faibles que l'on concatène pour reconstituer le message caché.



3. L'algorithme de décodage.

ii. Cacher une image dans une autre image :

Soit un octet de l'image qui cache « média de couverture » **0110**1011 et un octet de l'image que l'on souhaite cacher **1001**1101.

Le but est de remplacer les bits de poids faible de l'image qui cache par les bits de poids fort de l'image qu'on souhaite cacher. Ainsi, on obtiendra l'octet **0110**1001.

On effectue des changements sur des détails. Il faut choisir une image qui cache qui présente suffisamment de changements, auquel cas l'image cachée s'apercevra.

V. APPLICATIONS :

- Sécurité pour entreprise et personnel
  - Un employé mal intentionné peut, par exemple, vouloir faire sortir d'une entreprise des données confidentielles. Avec la stéganographie on peut contrecarrer ça.
  - Protection des informations : empêcher les personnes non désirées de lire nos documents privés.
- Des occasions qui ont besoin d'être anonyme :
  - La liberté d'expression en ligne, transmettre des renseignements personnels, Juste élection etc.
  - Services militaires et de renseignements : dans les communications militaires, non détecté par l'ennemi.

Exemples d'application :

- MP3Stego (Fabien A.P.Petitcolas, ComputerLaboratory, University of Cambridge) : peut cacher des données à l'intérieur des fichiers audio MP3.
- EZStego (Stego Online, Stego Shareware, Romana Machado) : C'est un programme software Java qui supporte uniquement les formats GIF et PICT.
- Hide and Seek (Colin Maroney): peut cacher des différents types de données dans des images GIF.
- JPEG-JSTEG (Derek Upham) : peut cacher des données à l'intérieur des fichiers JPEG.

VI. ANALYSE ET SECURITE :

Les principes de Kirchhoff s'appliquent aussi à la dissimulation d'information, la sécurité doit reposer sur la clé et non sur l'algorithme. La stéganographie pure est donc loin d'être sure.

La dissimulation d'information est sure lorsque en appliquant l'algorithme d'extraction on obtient une suite aléatoire que des informations soit dissimulées ou non dans le médium de couverture.

Les attaques sur les documents stéganographiques sont les suivantes :

- **Stego-only attack:** seul le stégo-medium est connu.
- **Known cover attack :** le médium de couverture et le stégo-medium sont disponibles.
- **Known message attack :** certaines parties du message caché sont connues de l'utilisateur. L'attaquant va essayer de retrouver dans le stego medium les parties du

message qu'il connaît afin de faciliter l'analyse des documents futurs. Même avec le message cette attaque est très difficile et généralement considérée comme équivalent à l'attaque stego only.

- **Chosen stego attack**: L'algorithme et le stego medium sont connus.
- **Chosen message attack :** le stéganalyste génère un stego medium à l'aide de l'algorithme et du message de son choix. Le but est d'observer le résultat pour cracker l'algorithme.
- **Known stego attack :** l'algorithme, le médium de couverture et le stego-medium sont connues.

VII. CONCLUSION :

En conclusion, la stéganographie est un domaine important de la sécurité des communications qui existe depuis l'Antiquité comme la cryptographie. Les techniques possibles sont quasi-infinies et uniquement limitées par les limites de l'esprit humain.

Depuis le développement de l'informatique, la stéganographie a très nettement évoluée vers le monde moderne et permet de cacher des informations de manière beaucoup plus sophistiquée et sécurisée que les techniques moins récentes mais qui sont toutes aussi efficaces quand elles sont utilisées dans le bon contexte.

La plupart des techniques présentées ici sont les techniques les plus importantes, il en existe beaucoup d'autres permettant par exemple de cacher du texte dans du son ou dans une vidéo ou une image dans une vidéo, etc mais elles sont plus compliqués.

BIBLIOGRAPHIE/WEBOGRAPHIE :

[1] http://www.lirmm.fr/icar/Presentation/KOUIDER_debut_these.pdf

[2] Stéganographie et Watermarking, Dimitri FOSSIER et Julien THEVENON

[3] Introduction à la Cryptographie et à la Stéganographie, Jean-Max REDONNET

[4] http://www.apprendre-en-ligne.net/crypto/stegano/

[5]Steganography-corporate-environment_4078, Copyright SANS Institute Author Retains Full Rights

[6] ROGERIE Grégory M2 Automatique

[7] Stéganographie, CHENG Yao UE CONF.