ESI

La stéganographie

Réalisé par :Encaré par :

- EMKEIDECHE Narimene -Mr ANANE M.
- BOUKAIOU Ahlem

Section : B Groupe : 04

Année universitaire : 2015/2016

SOMMAIRE

Sommaire

1. Introduction :

La cryptographie est une science qui est basée sur les mathématiques pour le cryptage et le décryptage de données, c'est-à-dire un ensemble des techniques permettant de chiffrer un message afin qu'il ne soit pas comprisque par le destinataire.

Or, il existe d'autres méthodes permettent de cacher nos données, parmi celles la stéganographie, mais qu'est-ce que c'est ? Qu'est-ce que ça veut dire ?

2. Définition :

Le mot stéganographie combine les anciens mots grecs steganos (στεγανός), signifiant "couverts, cachés ou protégés», et graphein (γράφειν) signifie «écriture».

La stéganographie, c'est l'art de dissimulation, elle consiste à cacher un message dans un autre message anodin. Contrairement aux messages chiffrés à l'aide de systèmes cryptographiques pour lesquels on sait qu'une information est dissimulée, les messages cachés à l'aide de systèmes stéganographiques convenablement choisis sont pratiquement indétectables. On peut dissimuler une information dans tout type de support (une image, un vidéo, un son …) de sorte qu'elle ne puisse pas être détectée visuellement.

Donc la cryptographie repose sur le fait que le message ne soit pas compris, mais la stéganographie repose sur le fait que le message ne soit pas trouvé.

3. Histoire :

Bien avant la stéganographie informatique existait la stéganographie sur support physique [1, 3]. Ces techniques consistaient à camoufler l'information secrète dans le support physique même du message anodin.

L'histoire veut que les premières utilisations de la steganographie date du 5eme siècle avant Jésus-Christ. Herodotus, auteur grec, relate les communications secrètes entre deux chefs de guerre qui utilisaient des esclaves pour passer des messages et plans de batailles. L'idée était simple, ils tatouaient sur le crâne des esclaves le message, laisser repousser les cheveux. Les Grecs vont mettre en place plusieurs mécanismes dédiés à la stéganographie. Des trous sur un disque représentant des lettres. Des fils, de couleurs différentes, permettaient de lire un mot. Une autre technique était de percer un petit trou, sur les lettres d'un document pour en faire un message. Une prémisse aux messages enchâssés.

Avec le développement de la chimie, par la suite on utilisait des encres sympathiques pour communiquer des messages en toute discrétion, (l'encre "invisible", souvent du jus de citron, d'ognon ou de chlorure d'ammoniac ou avec une solution de vinaigre et d'alun). Il suffisait d'écrire un message sans importance et d'inscrire entre les lignes quelques mots du message secret à transmettre à l'aide de l'encre sympathique. Passées quelques minutes l'encre sympathique devenait invisible. Le message sans importance n'éveillait pas l'attention et le destinataire légitime était le seul à connaître le procédé : pour lire le message secret, il suffisait de chauffer le papier ou de le tremper dans un bain d'espèce chimique spécifique

Pendant la Seconde Guerre mondiale, la technique des micropoints fut utilisée par les Allemands: une photographie, réduite à la taille d'un point, était imprimée et utilisée comme ponctuation dans un texte dactylographié.

Il y avait ainsi ce qu'on appelle la stéganographie romantique qui consiste a cacher un texte en un autre, par exemple en prenant la première lettre de chaque mot. Un exemple célèbre et amusant est fourni par le fameux échange de lettres entre *George Sand* et *Alfred de Musset*, vers 1830.

4. La stéganographie moderne

De nos jours, il est facile de dissimuler une information dans tout support numérique: un programme exécutable, un fichier son, un fichier image, etc... Un moyen imparable pour communiquer secrètement par Internet

Avec le développement de l'informatique et des réseaux, la stéganographie est devenue un moyen pratiquement imparable de communiquer des informations secrètes sans même qu'on puisse soupçonner qu'un message secret circule.

5. Techniques :

SUBSTITUTIONS : La première catégorie de techniques consiste en la substitution des symboles du message à des symboles inutiles ou redondants du stégo-document. De nombreuses variantes ont été proposées, et nous ne les listerons pas ici, nous résumant à une présentation générique.

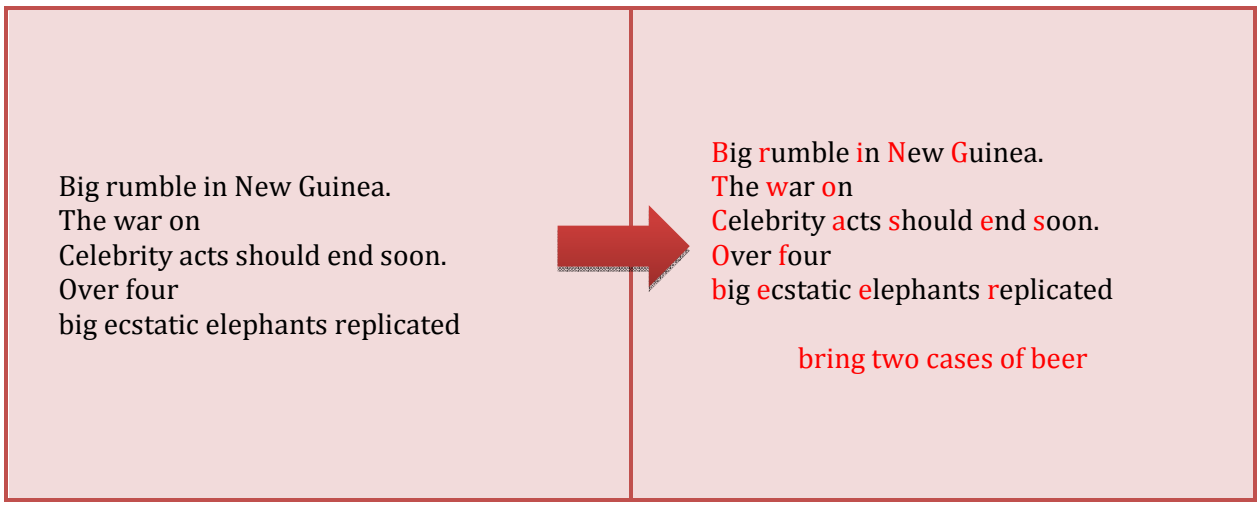
AJOUT : La deuxième catégorie de techniques consiste en l'ajout de données supplémentaire au stégo-document.

6. Méthodes :

6.1. Dissimulation dans un texte :

Pour réaliser cette fonctionnalité il existe plusieurs méthodes citons :

- Modification des espaces / tabulations entre les mots
- Alternances MAJUSCULES / minuscules
- **Marquage des caractères :** Une technique consiste à marquer certains caractères d'un document. Des points peuvent par exemple être placés sous les lettres d'un texte afin de dissimuler un message. Étalées sur un texte de plusieurs pages, ces marques peuvent s'avérer relativement efficaces vis-à-vis d'un œil non-averti. Un ordinateur n'est pas indispensable à la mise en œuvre de cette technique.



6.2. Dissimulation dans une image :

Ainsi on peut cacher une image dans une image ou un texte dans une image selon des techniques graphiquement indetectables comme :

- La méthode DCT pour images compressées JPEG
- La méthode LSB ,le plus populaire méthode pour dissimuler l'information.

La méthode DCT :

Découpage en blocs carrés de côté 8 pixels Application DCT (transformation en cosinus discrète) pour chaque couleur de chacun des pixels de chaque bloc,on obtient 64 DCT coefficients Cette transformation permet de déterminer les coefficients pouvant être modifiés sans impact visuel.

La méthode LSB (Least Significant Bit) ou 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 consiste à modifier le bit de poids faible des pixels codant l'image : une image numérique est une suite de points, que l'on appelle pixels, et dont on code la couleur à l'aide d'un triplet d'octets, par exemple pour une couleur RGB sur 24 bits. Chaque octet indique l'intensité de la couleur correspondante (rouge, vert ou bleu) 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.

Exemple :

1. On a deux images d'origine : un lièvre et une F15 .

2. Prenant un octet de Lièvre et un Octet de F15 .

Lièvre : 10110010 et F15 : 11111001

3. Si pour chaque pixel des deux images :
   - Les deux premiers bits de F15 remplacent les deux derniers de Lièvre.
   - On aura : 10110011
   - On aura l'image résultante est :

   - D'après cette image on extrait :

4. Si on refait la même opération mais en remplaçant 4 bits du poids faible par 4 bits du poids fort on aura comme images :

Et

6.3. Dissimulation dans d'autres types de conteneurs :

- Fichiers audio : par exemple WAV, modification des fréquences inaudibles par l'homme (< 20 Hz ou >20 kHz).
- Fichiers HTML et XML : en utilisant les espaces et commentaires au sein d'un code balisé chargé.

7. Objectifs :

Les deux principaux objectifs de la stéganographie :

- Les sens (œil, ouïe) ne sont pas capables de détecter d'infimes changements dans une image ou un son, et à priori nous ne savons pas à l'avance que tel fichier renferme de l'information cachée.
- Toutefois, le but de la stéganographie est de dissimuler un message sans éveiller l'attention humaine, avec la stéganographie informatique il faut également veiller à ne pas éveiller l'attention des logiciels d'analyse.

8. Domaines d'utilisation :

- Communiquer en toute liberté même dans des conditions de censure et de surveillance
- Contrebalancer toutes les législations ou barrières possibles empêchant l'usage de la cryptographie
- Publier des informations ouvertement mais à l'insu de tous des informations qui pourront ensuite être révélées et dont l'antériorité sera incontestable et vérifiable par tous
- Empêcher des personnes non désirées de lire le contenu des documents privés (Sécurité pour les entreprises et le personnelle).
- La liberté d'expressions en ligne et l'anonymat.
- Vouloir ne pas être détecté par l'ennemie (Services militaires et renseignements).

9. Logiciels de la stéganographie :

- Le site : http://invisiblesecrets.com/

- MP3Stego : Un logiciel conçu pour cacher des données dans un fichier MP3.
- EZStego : Un logiciel conçu avec JAVA qui permet de cacher dans des fichiers de format GIF ou PICT.
- JPEG-JSTEG : Cacher des fichiers dans un JPEG.

10. Stéganalyse :

Ça revient à détecter sil existe une information dissimulée, CAD prendre connaissance de cette information ou éventuellement la détruire

10.1. Les types de steganalyse

Passive identifier la présence Dun secret

Active identifier puis détruire le secret

10.2. La classification des techniques de steganalyse

- Medium hôte connu
- Information secrète connue
- Steganographie connue
- Steganographie choisie
- La modification des LSB dune image produit des variations entre pixel voisins visible sur l'histogramme des composants de couleur de limage.

11. Conclusion :

Cette technique, la stéganographie, consiste à cacher un message dans un support "innocent". Elle peut, de surcroît, se combiner à la cryptographie, qui se charge de dissimuler le sens de la missive et non plus son existence. Le résultat est alors particulièrement efficace. Le message secret s'abrite d'abord derrière son invisibilité. En cas de découverte, il restera à le décoder.

La sécurité de la stéganographie repose sur le fait que le message ne sera sans doute pas détecté.