République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique

Université d'Adrar
Faculté de science et technologie

Département des Mathématiques et Informatique

Mémoire de fin d'études pour l'obtention du diplôme de Master

Option : Réseaux et systèmes intelligents

Thème :

Proposition d'un système de communication d'un message secret en utilisant la stéganographie

Présentée par :
Melle BNOUMACHICH Fatima
Melle BAROUNE Melha

Dirigé par :
Dr TOUABI Abdelkader

Juin 2013

"La sécurité est mon pire ennemie, elle endort mes réflexes et mes initiatives"
Belo-kiu-kiuni
Bernard Werber (Les fourmis)

Remerciement

Nous tenons à remercier :

Allah le tous puissant.

Merci à tous ceux qui ont consacré de leur temps,

pour la bonne cause qui est vers le chemin de la recherche et de la science.

Nous tenons à remercier et à exprimer notre profonde gratitude

aux personnes suivantes:

Nos parents- Nos frères- Notre cher ami Nair- Dr. OMARI Mohammed-

Département d'informatique d'ADRAR et Nos collègues à l'université d'ADRAR.

Nos remerciements vont à toute l'équipe pédagogique qui a assuré les parties théoriques,

pratiques des différents aspects de cette spécialité Master Informatique.

Moi Fatima je remercie Melle Benouda Imane.

Moi Melha je remercie un homme (balance)

qui m'a appris que l'erreur est humaine,

et qu'il faut commettre des erreurs pour apprendre.

Nous n'oublierons pas de remercier Mr Touabi et Mr Kohili

et toutes les personnes

qui auront contribué de près ou de loin à l'élaboration de

ce mémoire.

Fatima & Melha

Résumé

Parmi les risques qu'un informaticien peut rencontrer dans le domaine de son travail le vol des données. Ce phénomène peut être comparé au risque de vols dans la vie courante et comme solution la personne essaye toujours de protéger son trésor en le mettant dans un coffre-fort caché derrière un cadre.

En informatique la solution est la proposition d'un système de communication d'un message secret en utilisant la stéganographie. Ce travail consiste à utiliser la technique de cryptographie pour envoyer des messages codés, hybridé avec la technique de stéganographie qui dissimule et cache la transmission de ce message dans une image.

Chapitre 1

La sécurité informatique

I. Introduction

Depuis des temps très reculés, l'homme avait utilisé diverses méthodes et techniques pour envoyer un message secrètement. Ce sont des méthodes qui transforment le message en clair en un message incompréhensible ou qui cachent le message par une image, un texte ou autres choses sans qu'une personne étrangère puisse s'en apercevoir.

La notion de cryptographie remonte à l'Antiquité durant laquelle les Grecs utilisaient des outils primaires pour envoyer des messages codés. La nécessité de vouloir crypter un message s'est manifestée par la volonté d'empêcher une tierce personne autre que le destinataire à décrypter le message. Plus tard, les outils de cryptographie se sont perfectionnés ainsi que les méthodes de chiffrement dans le but de transmettre plus rapidement et plus efficacement un message.

II. Les objectifs de la sécurité

La sécurité informatique tente de maintenir six principaux critères [1, 2, 3, 4 , 5, 10]

II. 1. La confidentialité

La confidentialité représente le fait que les données informatiques ne sont accessibles que par les personnes autorisées. Le type d'accès s'étalant de la simple connaissance de l'existence de l'objet à la surimpression de celui-ci. La confidentialité reste la notion de sécurité informatique la plus proche du monde réel et semble dès lors la plus claire.

II.2. L'authentification

Dans le cas d'un simple message, le service d'authentification assure que le message provient de l'endroit d'où il prétend venir. Dans un cas d'un échange bidirectionnel, deux aspects sont présents. Il faut assurer que les deux entités sont bien ce qu'elles affirment être. De plus, le service d'authentification doit montrer que la connexion ne peut être brouillée par une troisième entité essayant de se faire passer pour un des deux correspondants.

La plupart des techniques d'authentification se fondent sur l'un des principes de base suivants :

II.2.a L'authentification sur la base de quelque chose que l'on sait

Est la technique de base employée au niveau de systèmes informatiques pour prouver qu'on a le droit de travailler sous un certain nom d'utilisateur, vous devez introduire le mot de passe correspondant à ce nom d'utilisateur.

II.2.b L'authentification sur la base de ce que l'on est

Est utilisée chaque jour pour la reconnaissance de personnes sur la base de la physionomie, du timbre de la voix,… C'est en fait le « mesurage » de caractéristiques biologiques qui permet d'effectuer la reconnaissance. C'est pour cette raison que l'on parle également de techniques « biométriques ».

Dans un environnement informatique, les techniques d'authentification biométriques se fondent également sur le mesurage de caractéristiques biologiques : reconnaissance faciale, balayage de la rétine, reconnaissance de l'empreinte digitale et reconnaissance de la voix.

Les techniques d'authentification biométriques ont une particularité : elles n'indiquent généralement pas de façon univoque si l'utilisateur a été reconnu ou non. Il s'agit habituellement d'un certain « pourcentage » de reconnaissance [6].

II.3. L'intégrité

L'intégrité signifie que l'information ne peut être modifiée que par les personnes autorisées ou seulement par les moyens autorisés. L'intégrité reste un domaine très large couvrant à la fois les modifications, les moyens de modification mais également l'après-modification et donc la consistance.

II.4. La disponibilité

La disponibilité se reflète dans l'information et dans les services. Ce domaine est aujourd'hui en pleine expansion. Il regroupe des sujets aussi variés que les temps de réponse, la tolérance aux fautes, le contrôle de concurrence et le partage équitable de ressources.

II.5. La non-répudiation

La non-répudiation permet au récepteur ou à l'émetteur de ne pas refuser un message transmis. Donc, quand un message est envoyé, le récepteur peut prouver que le message a bien été envoyé par l'émetteur. De même, lorsqu'un message est reçu, l'émetteur peut prouver que le message a bien été reçu par le bon récepteur.

II.6. Le contrôle d'accès

Le contrôle d'accès représente la capacité de limiter et de contrôler les accès aux systèmes et applications via les liens de communication. Pour cela, chaque entité demandant un accès se voit identifiée ou authentifiée afin de lui adapter ses droits d'accès.

Pour aborder les multiples aspects de la sécurité, il faut établir un cadre et une architecture afin de définir un vocabulaire commun qui servira de base à l'examen des concepts.

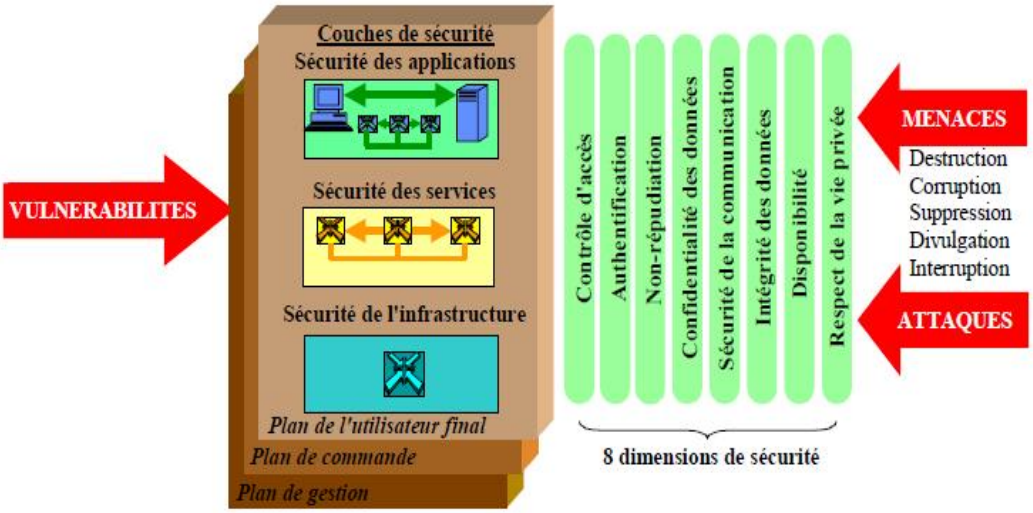


Figure 01 : *Eléments architecturaux de sécurité (Recommandation UIT-T X.805)* [1].

III. Les attaques

Les attaques informatiques délibérées peuvent porter entre autres sur les communications, les machines ou les traitements : 12 moyens de porter atteinte à la sécurité en informatique [6, 7].

III.1 Destruction de matériels ou de supports

On va citer une seule attaque :

- **Sabotage**

Le sabotage porte atteinte à l'intégrité des informations mais surtout à la disponibilité des services.

III.2 Rayonnements électromagnétiques

On va citer une seule attaque :

- **Brouillage**

Utilisée en télécommunication, cette technique rend le SI inopérant. Elle est surtout utilisée par les militaires en temps de crise ou de guerre.

III.3 Écoute passive

On va citer trois types d'attaque :

- **Ecoute**

L'écoute consiste à se placer sur un réseau informatique ou de télécommunication et à analyser et à sauvegarder les informations qui transitent.

- **Interception de signaux compromettants**

L'attaquant va tenter de récupérer un signal électromagnétique et de l'interpréter pour en déduire des informations compréhensibles. L'agresseur se mettra ainsi à la recherche des émissions satellites, et radio, mais aussi des signaux parasites émis par les SI1, principalement par les terminaux, les câbles et les éléments conducteurs entourant les SI.

- **Cryptanalyse**

L'attaque d'un chiffre ne peut se faire que lorsqu'on a accès aux cryptogrammes qui peuvent être interceptés lors d'une communication ou qui peuvent être pris sur un support quelconque. Elle est principalement le fait de services de renseignement.

III.4 Vol de supports ou de documents

Le vol, visible quand l'objet du délit est matériel, est difficile à détecter quand il s'agit de données et encore plus de ressources informatiques.

- **Fraude physique**

Elle peut consister à récupérer les informations oubliées ou non détruites par l'adversaire ou le concurrent.

[1] SI : Système d'information

Comme l'espionnage, la fraude physique va tenter d'enfreindre les mesures de sécurité qui protègent la confidentialité des informations.

- **Vol de matériels**

Le vol de matériels passe généralement par une infraction aux mesures de sécurité protégeant la confidentialité des informations.

- **Vol de micro-ordinateur portable**

Le vol des micro-ordinateurs portables est aujourd'hui pratique courante. De plus, l'utilisation croissante de ces micro-ordinateurs portables, souvent attribués à des hauts responsables de l'organisme a pour conséquence que de plus en plus d'informations sensibles se trouvent exposés sur ces machines attractives.

III.5 Récupération de supports recyclés ou mis au rebut

On va citer une seule attaque :

- **Analyse de support mis au rebus**

Les organismes sont la victime de deux types de scénarios fréquemment utilisés:

- l'un consiste à effectuer une fouille systématique des poubelles ou plus simplement le vol d'éditions oubliées sur les imprimantes partagées, accessibles dans les locaux "publics" de l'organisme ;
- l'autre exploite une lacune souvent présente dans la procédure de ré-attribution ou d'envoi en maintenance des postes de travail. Il consiste simplement à analyser le contenu des données stockées sur la machine par son précédent propriétaire.

III.6 Divulgation

On va citer deux types d'attaque :

- **Chantage**

Soutirer de l'argent à un organisme ou à une personne est d'autant plus tentant que de nombreuses données concernant la vie privée des personnes ou les activités d'une organisation sont gardées sur des ordinateurs. Le chantage peut mettre en cause aussi bien la confidentialité, l'intégrité, que la disponibilité des informations et des services.

- **Hameçonnage ou filoutage (*phishing*)**

Cette technique désigne l'obtention d'informations confidentielles (comme les mots de passe ou d'autres informations privées).

III.7. Informations sans garantie d'origine

On va citer une seule attaque :

- **Canular**

Il est transmis par courrier électronique et annonce la propagation d'un virus imaginaire dont les conséquences se trouvent être, en général, catastrophiques. Bien qu'il soit difficile de considérer ce type d'évènement comme une réelle attaque, elle contribue à la désinformation générale.

III.8 Piégeage du logiciel

On va citer quatre types d'attaque :

- **Bombe**

Une bombe est un programme en attente d'un événement spécifique déterminé par le programmeur et qui se déclenche quand celui-ci se produit.

- **Virus**

Nommé ainsi parce qu'il possède de nombreuses similitudes avec ceux qui attaquent le corps humain, un virus est un programme malicieux capable de se reproduire et qui comporte des fonctions nuisibles pour le SI.

Ses actions ont généralement comme conséquence une dégradation ou une interruption du service fourni.

- **Exploitation d'un défaut (*bug*)**

De nombreuses failles sont présentes dans les logiciels commerciaux.

- **Logiciel espion (*spyware*)**

Un logiciel espion est un logiciel malveillant qui infecte un ordinateur dans le but de collecter et de transmettre à des tiers des informations de l'environnement sur lequel il est installé sans que l'utilisateur n'en ait conscience.

III.9 Saturation du système informatique

On va citer trois types d'attaque :

- **Perturbation**

L'agresseur va essayer de fausser le comportement du SI ou de l'empêcher de fonctionner en le saturant, en modifiant ses temps de réponse ou en provoquant des erreurs. L'agresseur veut désorganiser, affaiblir ou ralentir le système cible.

- **Saturation**

Cette attaque contre la disponibilité consiste à remplir une zone de stockage ou un canal de communication jusqu'à ce que l'on ne puisse plus l'utiliser.

- **Pourriel (*spam*)**

Un spam est un courrier électronique indésirable, contenant ou non une pièce jointe, qui est transmis à une multitude de destinataires n'ayant sollicité aucune demande de la part de l'émetteur.

III.10 Utilisation illicite des matériels

On va citer quatre types d'attaque :

- **Détournement d'utilisation normale**

L'attaque consiste à exploiter un défaut particulier d'implémentation. La technique consiste à exploiter une erreur de programmation de manière à faire exécuter à distance à la machine victime un code malveillant.

- **Mystification**

Dans ce cas, l'attaquant va simuler le comportement d'une machine pour tromper un utilisateur légitime et s'empare de son nom et de son mot de passe.

Un protocole d'authentification de la machine de destination permettra à un utilisateur d'être sûr de son interlocuteur.

- **Asynchronisme**

Ce type d'attaque évoluée exploite le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation.

- **Inférence sur les données**

L'établissement d'un lien entre un ensemble de données non sensibles permet, dans certains cas, de déduire des données sensibles.

III.11 Altération des données

On va citer deux types d'attaque :

- **Interception**

L'interception est un accès avec modification des informations transmises sur les voies de communication.

Les quatre types d'interception sont :

- la destruction de messages,
- la modification de messages (modification de l'information; réagencement de l'information à l'intérieur des messages ou réagencement de la suite des messages),
- l'insertion de messages,
- refus de service (décalage dans le temps d'un message).

- **Balayage (*scanning*)**

Le balayage consiste à envoyer au SI un ensemble d'informations de natures diverses afin de déterminer celles qui suscitent une réponse positive. Cette technique est analogue à celle qui consiste à balayer une gamme de fréquences pour trouver un signal porteur.

III.12. Usurpation de droit

On va citer trois types d'attaque :

- **Les accès illégitimes**

Cette menace est le fait d'une personne qui se fait passer pour une autre en usurpant son identité. Elle vise tout particulièrement l'informatique.

Les accès illégitimes portent atteinte à la confidentialité des informations.

- **Déguisement**

Forme d'accès illégitime, il s'agit d'une attaque informatique qui consiste à se faire passer pour quelqu'un d'autre et obtenir les privilèges ou les droits de celui dont on usurpe l'identité.

- **Substitution**

Ce type d'attaque est réalisable sur un réseau ou sur un système d'information comportant des terminaux distants. L'agresseur écoute une ligne et intercepte la demande de déconnexion d'un utilisateur travaillant sur une machine distante. Il peut alors se substituer à ce dernier et continuer une session normale sans que le système note un changement d'utilisateur.

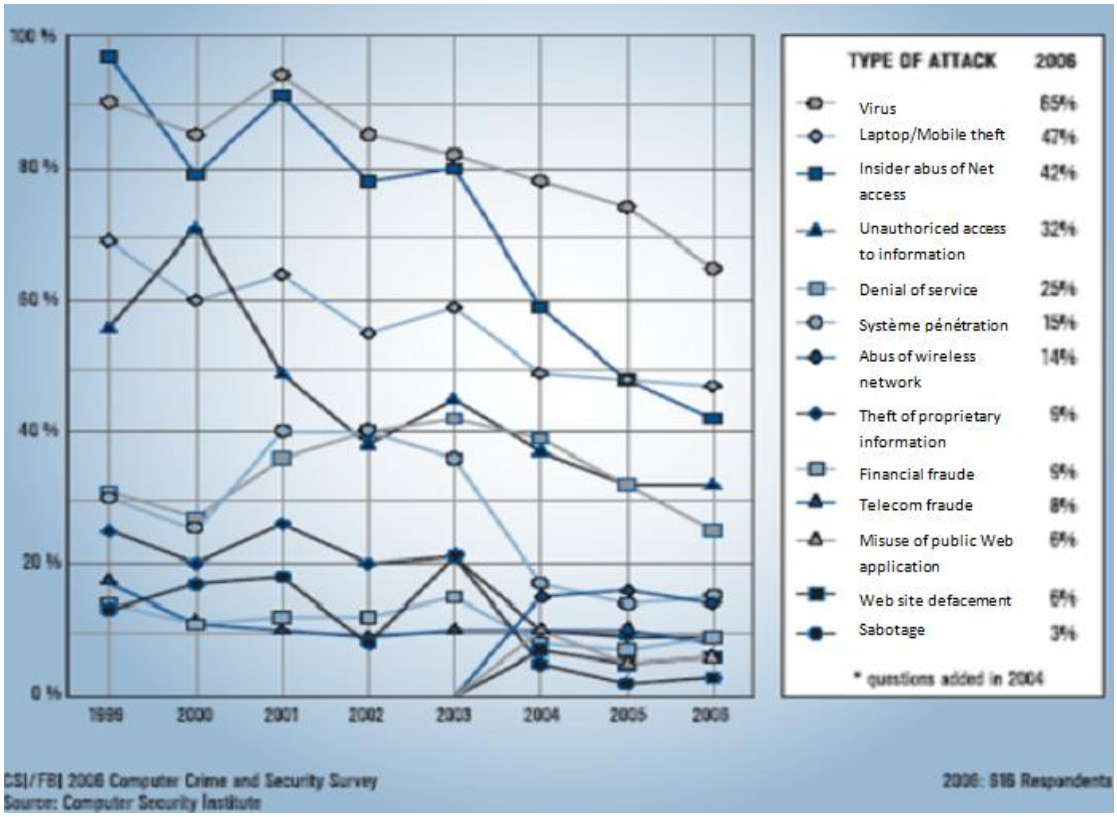


Figure 02 : *Types d'attaques répertoriées en 2006* [8].

Les politiques de sécurité sont des énoncés généraux dictées par les cadres supérieurs décrivant le rôle de la sécurité au sein de l'entreprise afin d'assurer les objectifs d'affaire.

En 2003, le marché de la sécurité réseau était évalué à 45 milliards [5].

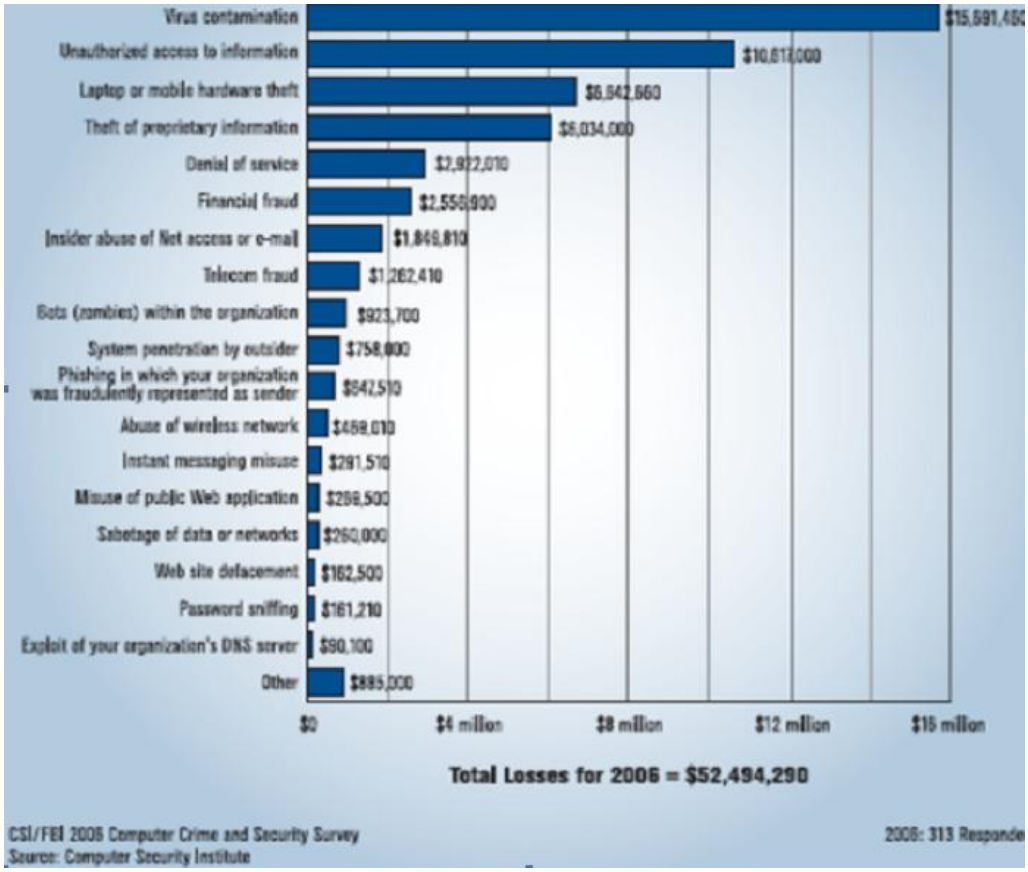


Figure 03 : *Les couts de l'insécurité* [8].

IV. Méthodes de défense

Le but de la sécurité informatique est de préserver la confidentialité, l'intégrité et la disponibilité. Certaines méthodes de défense permettent de prévenir les attaques, d'autres, moins efficaces, ne font qu'une détection ultérieure [11].

III.1. Le cryptage

En transformant les données afin qu'elles deviennent incompréhensibles pour un observateur extérieur, on peut se protéger des interceptions et modifications. En plus de la confidentialité, le cryptage permet donc d'atteindre un certain seuil d'intégrité en tenant compte du fait que des données qui n'ont pas de signification à la lecture peuvent difficilement être modifiées de manière sensée. Le cryptage est un des outils les plus importants de la sécurité informatique mais il ne résoud pas non plus tous les problèmes de sécurité. De plus, il est important de noter qu'un cryptage mal utilisé peut donner un sentiment de sécurité alors qu'il n'en n'est rien.

III.2. Le contrôle software

Les programmes se doivent d'être sécurisés afin d'exclure les tentatives d'attaques extérieures. Que ce soit réfléchi durant la phase de développement, implémenté par le système d'exploitation ou partie restrictive du programme, le contrôle

software touche l'utilisateur assez directement ce qui en fait un des premiers sujets venant à l'esprit.

III.3. Contrôle hardware

Il existe de nombreux appareils assistant la sécurité. Citons des cartes d'implémentation de cryptage, des vérificateurs d'identité et des contrôleurs d'accès disque.

III.4. Politique

Les lois en matière de crime informatique sont aujourd'hui encore assez floues, lentes à se développer. Les communautés informatique n'a pas encore vraiment adopté de standards en matière de comportement éthique. Malgré que certaines organisations poussent de tels développements, ils ne sont encore qu'à leurs balbutiements.

III.5. Contrôle physique

Sans doute le contrôle le plus évident. Il comprend le verrouillage de porte, gardes, backups, planning prévu en cas de catastrophes naturelles. N'oublions pas que les techniques les plus simples sont souvent les meilleures.

III.6. Bonne pratique

Les réseaux informatiques fournissent aux utilisateurs une énorme liberté. Aussi, le public se doit bien souvent encore de comprendre lui-même quels sont les comportements inappropriés en matière de réseau.

V. Conclusion

La sécurité informatique, véritable science régissant le codage de l'information, a connu une réelle explosion avec le développement des systèmes informatiques, passant d'une ère artisanale et confidentielle à des systèmes de très hautes technologies nécessitant une importante puissance de calcul. Elle a connu un plus large essor encore avec l'arrivée des systèmes de communications modernes (Interne) où il y a une nécessité absolue de protéger les données échangées des individus.

Bruce Schneier, l'une des personnalités les plus respectées des milieux de la sécurité informatique, n'a de cesse de le répéter : la sécurité est avant tout un processus, pas un produit. Aucune solution n'est fiable à 100% et rien ne sert, par exemple, d'installer une porte blindée si on laisse la fenêtre ouverte. Il convient d'autre part de ne jamais oublier qu'en matière informatique en générale, et sur l'internet en particulier, l'anonymat n'existe pas. Il arrive fatalement un moment où l'on se trahit, où l'on commet une erreur, ou, plus simplement, où l'on tombe sur quelqu'un de plus fort que soi. La sécurité informatique est un métier, elle ne s'improvise pas.

Bibliographie

[1] ITU-U.I.T ; « *Sécurité dans les télécommunications et les technologies de l'information* » ; Décembre 2003.

[2] http://www.tele.ucl.ac.be/EDU/ELEC2920/1997/securite/html_3.htm. (12/04/2013).

[3] Dr Bart Van den Bosch, Prof Erwin Bellon, André De Deurwaerder Mark Vanautgaerden, Dr Marc Bangels ; « **Recommandations et Critères de qualité pour les systèmes d'information hospitaliers** » ; version 01-décembre 2002.

[4] Asma Zita, Dalila Tlib ; « **Implémentation d'un système de cryptographie en utilisant une Fonction de hachage** » ; Projet fin d'étude pour l'obtention du diplôme licence LMD ; Université d'Adrar ; 2009.

[5] Odile Papini; « **Contrôle d'accès - logique et sécurité** », LSIS. Université de Toulon.

[6] Bureau conseil, Sous-direction des opérations, Direction centrale de la sécurité des systèmes d'information, Secrétariat général de la défense nationale, Premier Ministre ; « **Menaces sur les systèmes informatiques** » ; guide N° 650 ; Maubourg - PARIS; Version du 12 septembre 2006.

[7] Jean Leneutre; « **Concepts fondamentaux de la sécurité** » - INF721; TELECOM- ParisTech ; 2012.

[8] Laurent Bloch, Christophe Wolfhugel; « **Sécurité informatique- Principes et méthodes** » ; 3ème Edition ; © Groupe Eyrolles, 2011.

[9] Ali Pacha, Hadj Said, M'hamed, Belghoraf; « **Chaos Crypto-Système basé sur l'Attracteur de Hénon-Lozi** »; Université des Sciences et de la Technologie d'Oran USTO -Algerie

[10] Erik Bresson; « **Cryptographie, Authentification et échange de clé** »; Université Paris XII, Val de marne (SGDN/DCSSI- Laboratoire de cryptographie).

[11] Arnaud Contes ; « **une architecture de sécurité hiérarchique, adaptable et dynamique pour la grille** » ; Thèse de doctorat ; Université de NICE - Sophia Antipolis ; Septembre 2005.

Chapitre 2

La science des messages secrets

I. Introduction

Où et comment cacher l'information secrète ?

De tout temps, des personnes ont communiqué en essayant de coder leurs informations pour éviter que quelqu'un d'autre que le destinataire puisse comprendre quel était le sujet du message.

De nos jours, la cryptologie est omniprésente puisqu'on la retrouve dans l'univers de l'informatique. En effet, c'est grâce à celle-ci que nos mots de passes et données confidentielles sont protégés des personnes malintentionnées.

Les communications ont toujours constitué un aspect important dans l'acquisition de nouvelles connaissances et l'essor de l'humanité. Le besoin d'être en mesure d'envoyer un message de façon sécuritaire est probablement aussi ancien que les communications elles-mêmes.

D'un point de vue historique, c'est lors des conflits entre nations que ce besoin a été le plus vif. Dans notre monde moderne, où diverses méthodes de communication sont utilisées régulièrement, le besoin de confidentialité est plus présent que jamais à une multitude de niveaux. Par exemple, il est normal qu'une firme désire protéger ses nouveaux logiciels contre la piraterie, que les institutions bancaires veuillent s'assurer que les transactions sont sécuritaires et que tous les individus souhaitent que l'on protège leurs données personnelles.

Le besoin de communications sécuritaires a donné naissance à la science que nous appelons cryptologie.

II. L'évolution de la science des messages secrets (cryptologie)

La science des messages secrets et des codes chiffrés constitue le moyen de défense contre les programmes malveillants.

II.1. Algorithmes de cryptographie symétrique

Les algorithmes de chiffrement symétrique se fondent sur une même clé pour chiffrer et déchiffrer un message.

Le problème de cette technique est que la clé, qui doit rester totalement confidentielle, doit être transmise au correspondant de façon sure. Ces algorithmes sont dits aussi à clé secrète.

II.2. La cryptographie moderne

A partir de ce point, la cryptographie entre dans son ère moderne avec l'utilisation intensive des ordinateurs, c'est-à-dire a partir des années septante. Dans la cryptographie moderne, les textes sont remplacés par des chiffres. Via l'utilisation de la table ASCII, par exemple. Les problèmes sont de plus en plus mathématiques.

II.3. Algorithmes de cryptographie asymétrique

Dans les années 1970, la cryptographie n'est plus seulement l'apanage des militaires. Les banques, pour la sécurité de leurs transactions, sont devenues de grandes consommatrices de messages codes. Les chiffrements disponibles alors, comme le DES, sont sures, eu égard aux possibilités d'attaque contemporaines. Le problème essentiel est alors la distribution des clés, ce secret que l'envoyeur et le destinataire doivent partager pour pouvoir respectivement chiffrer et déchiffrer. Les armées et les états ont recours aux valises diplomatiques pour ces échanges, mais ceci n'est pas accessible aux civils.

En 1976, Whitfield Diffie et Martin Hellman propose une nouvelle façon de chiffrer, qui contourne cet écueil.

En 1977, D.Rivest, A.Shamir et L.Adleman trouvent une solution possible, la meilleure et la plus utilisée à ce jour, la cryptographie RSA.

II.4. Fonctions de hachage

Une fonction de hachage est une fonction qui fait subir une succession de traitements a une donnée quelconque fournie en entrée pour en produire une empreinte servant à identifier la donnée initiale sans que l'opération inverse de décryptage soit possible.

Le terme hachage évite l'emploi de l'anglicisme hash. Le résultat de cette fonction est par ailleurs aussi appelé empreinte cryptographique.

II.5. Cryptanalyse

La cryptanalyse s'oppose, en quelque sorte, a la cryptographie. En effet, si déchiffrer consiste a retrouver le clair au moyen d'une clé, cryptanalyse c'est tenter de se passer de cette dernière.

Même si on décrit les cryptanalyses comme des briseurs de codes, il convient de remarquer qu'un algorithme est considère comme casse lorsqu'une attaque permet de retrouver la clé en effectuant moins d'opérations que via une attaque par force brute. L'algorithme ainsi casse ne devient pas inutile pour autant, mais son degré de sécurité, c'est-a-dire le nombre moyen d'opérations nécessaires pour le déchiffrer, s'affaiblit.

II.6. Stéganographie

Si la cryptographie est l'art du secret, la steganographie est l'art de la dissimulation : l'objet de la stéganographie n'est pas de rendre un message inintelligible a autre que qui de droit mais de le faire passer inaperçu. Si on utilise le coffre-fort pour symboliser la cryptographie, la steganographie revient à enterrer son argent dans son jardin. Bien sûr, l'un n'empêche pas l'autre, on peut enterrer son coffre dans son jardin.

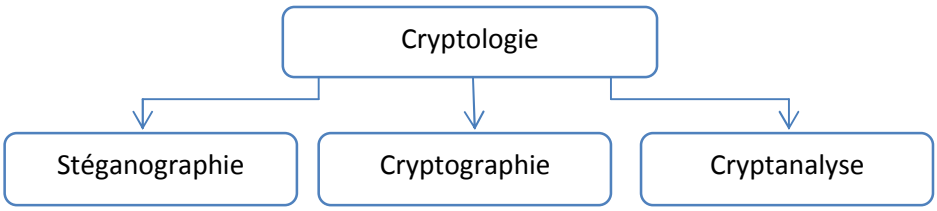


Figure 04 : *L'organigramme du la cryptologie*

III. La cryptographie transposition

Quand Jules César envoyait des messages à ses généraux, il ne faisait pas confiance à ses messagers. Aussi remplaçait-il chaque A dans ses messages par un D, chaque B par un E, et ainsi de suite à travers l'alphabet. Seul quelqu'un qui connaissait la règle "décalé de 3" pouvait déchiffrer ses messages.

Et c'est ainsi que nous commençons :

III.1. Définition de la cryptographie

La cryptographie constitue un des piliers de la cryptologie[1]. Comme l'indique l'étymologie du mot, la cryptologie est la science du secret. La cryptographie peut donc être vue comme la science des écritures cachées. Plus pragmatiquement, on peut définir la cryptographie comme l'étude des techniques permettant s'assurer la confidentialité, l'authenticité et l'intégrité d'un message.

La cryptographie est l'art du cryptage. Crypter un message, on dit aussi chiffrer un message, consiste `a le transformer selon un procédé recélant un certain secret en un message inintelligible appelé cryptogramme[2].

[1] **La cryptologie :** Est la science qui étudie les aspects scientifiques des méthodes de chiffrement et de déchiffrement d'informations.

[2] **Cryptogramme :** Le résultat du processus de chiffrement.

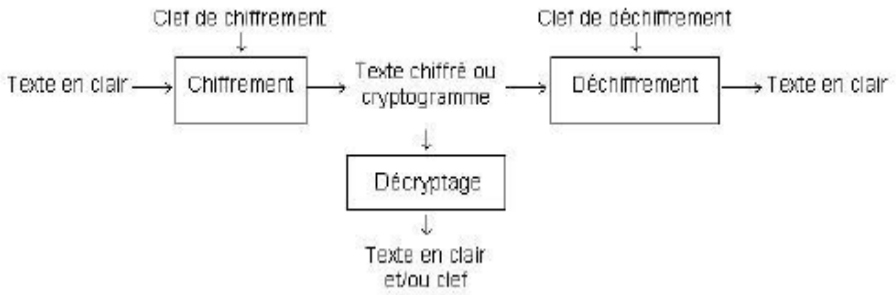


Figure 05 : *Schéma générique de la cryptographie* [1].

III.2. Les technique de cryptographie

Il y a essentiellement trois types de cryptographie qui tous utilisent les mathématiques [6] :

- Système à clé secrète dont le modèle le plus simple est celui de Jules César.
- Système à clé publique dont le modèle le plus simple est appelé RSA[3] .
- Système hybride dont le meilleur exemple est appelé PGP[4] .

III.2.a Systèmes à clé privée

Les systèmes de cryptage à clé secrète, appelés aussi systèmes de cryptage symétrique, sont utilisés depuis plusieurs siècles déjà. C'est l'approche la plus authentique du chiffrement de données et mathématiquement la moins problématique.

Voici quel en est son principe de base. Un expéditeur et un destinataire souhaitant communiquer de manière sécurisée à l'aide du cryptage conventionnel doivent convenir d'une clé et ne pas la divulguer.

Dans la majorité des systèmes de cryptage symétrique la clé de chiffrement et la clé de déchiffrement sont identiques.

La taille des clés utilisées varient selon le besoin et font en standard 64 ou 128 bits.

[3]**RSA** (*Rivest*, *Shamir*, *Adleman*).
[4] **PGP** (*Pretty Good Privacy*).

Figure 06 *: principe du chiffrement à clé secrète* [6].

Ce système nécessite la connaissance de la clé par l'émetteur et par le destinataire. C'est la transmission de cette clé entre les intervenants qui représente la faiblesse inhérente au système. S'ils se trouvent à des emplacements géographiques différents, ils devront faire confiance à une tierce personne ou un moyen de communication sécurisé. Toute personne interceptant la clé lors d'un transfert peut ensuite lire, modifier et falsifier toutes les informations cryptées ou authentifiées avec cette clé [O].

III.2.b Les systèmes cryptographiques à clé privée

Les principaux les procédés à clé privée utilisés actuellement sont : Cryptographie par substitution, Le chiffrement de César, La méthode du ou exclusif simple, Le chiffrement de Vigenère [6].

III.2.c. Exemples de systèmes cryptographiques

La plupart des exemples de cette section sont trop simples pour offrir la moindre sécurité. Leur intérêt est purement pédagogique [3].

Identifions l'alphabet usuel avec Z26 par a = 0, b = 1,…., = 25. On a alors le système cryptographique suivant :

- **Chiffrement par décalage**. $\mathbb{P} = \mathbb{C} = \mathbb{K} = \mathbb{Z}_{26}$. On a $e_k(x) = x + k$ et $d_k(y) = y - k$. Exemple, pour $k = 3$, le texte clair cryptographie est chiffré en *FUBSWRJUDSKLH.* Ce système de chiffrement n'est pas sûr du tout puisque l'espace des clés ne contient que 26 éléments. On peut facilement les essayer une à une jusqu'à trouver la bonne [5].
  Voici (Figure 07) le décalage effectué par César :

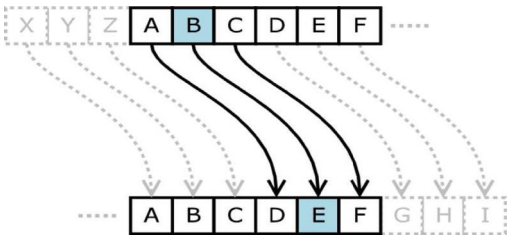


Figure 07: *Principe du chiffre de César* [8].

IV. La stéganographie

IV.1. Introduction (Histoires)

Dans son Enquête, l'historien grec Herodote (484-445 av. J.-C.) rapporte ainsi une anecdote qui eut lieu au moment de la seconde guerre médique. En 484 avant l'ère chretienne, Xerxes, fils de Darius, roi des Perses, décide de préparer une arme gigantesque pour envahir la Grece. Quatre ans plus tard, lorsqu'il lance L'offensive, les Grecs sont depuis longtemps au courant de ses intentions. C'est que Demarate, ancien roi de Sparte refugie auprès de Xerxes, a appris l'existence de ce projet et décide de transmettre l'information a Sparte: « il prit une tablette double, en gratta la cire, puis écrivit sur le bois même les projets de Xerxes ; ensuite il recouvrit de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis . »

Un autre passage de la même œuvre fait également référence à la steganographie : Histiee incite son gendre Aristagoras, gouverneur de Milet, à se révolter contre son roi, Darius, et pour ce faire, « il fit raser la tête de son esclave le plus fidèle, lui tatoua son message sur le crane et attendit que les cheveux eussent repousse ; quand la chevelure fut redevenue normale, il fit partir l'esclave pour Milet ».

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

Dès le Ier siècle av. J.-C., Pline l'Ancien décrit comment réaliser de l'encre invisible ou "encre sympathique".

Les enfants de tous les pays s'amusent à le faire en écrivant avec du lait ou du jus de citron : le passage de la feuille écrite sous un fer à repasser chaud révèle le message.

Durant la Seconde Guerre mondiale, les agents allemands utilisaient la technique du micro point de Zappe, qui consiste à réduire la photo d'une page en un point d'un millimètre ou même moins. Ce point est ensuite place dans un texte normal. Le procède est évoqué dans une aventure de Blake et Mortimer, SOS météores.

IV.2. Définition de la stéganographie

La stéganographie n'est pas vraiment une méthode cryptographique. Elle repose sur le fait que l'information à cacher est mélangée avec de l'information banale de manière à passer inaperçue [7].

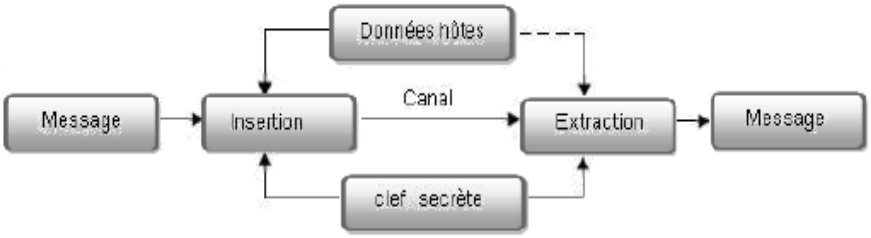


Figure 08 : schéma générique de la stéganographie [1].

IV.3. Techniques de Stéganographie

Il existe autant d'endroits où cacher de l'information qu'il existe de formats et de types de données, les plus fréquemment utilisés étant les plus anodins. Bien qu'on ne s'intéresse ici qu'au cas des images, on peut citer quelques possibilités pour les autres formats [1].

IV.3.a Message transporté dans une image

La stéganographie d'image numérique exploite les limites du système visuel humain (SVH). Ce dernier a une très basse sensibilité aux petits changements dans la luminance, et par conséquent, les variations dans les basses fréquences de l'image peuvent être utilisées pour cacher une grande quantité d'information.

Les approches d'insertion les plus fréquentes sont les suivantes :

- **Usage des bits de poids faible d'une image**

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 Signifiant Bit) 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 pixel, 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 inferieur (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 [2].

Cette technique très basique, s'applique tout particulièrement au format d'image BMP, format sans compression destructive, avec codage des pixels entrelacé sur 3

octets comme énoncé ci-dessus. Réciproquement, tout procédé de compression-décompression d'images avec pertes tel que le format JPEG est susceptible de détruire un message stéganographié de cette façon.

- **Manipulation de la palette de couleurs d'une image**

Certain formats graphiques tel que GIF ou PNG permettent le stockage des couleurs de l'image par référence à une palette de couleurs insérée dans le même fichier.

Ainsi au lieu de stocker Bleu, Blanc, Rouge dans une image du drapeau français, on trouve dans un format de fichier la description de l'objet la suite Couleur1,Couleur2, Couleur3 ainsi qu'une palette qui définit que Couleur1 le Bleu, Couleur2 le Blanc et Couleur3 le Rouge.

La même image peut-être stockée de la façon suivante: Couleur2, Couleur3, Couleur1 avec une palette qui définit que Couleur2 est le Bleu, Couleur3 est le Blanc et Couleur1 est le Rouge.

Ces deux images sont visuellement identiques mais le stockage de celles-ci est différent.

Pour une image contenant 256 couleurs uniques dans sa palette, on a factoriel de 256 façons de stocker cette image. En utilisant un code connu entre l'émetteur et le récepteur de l'image, on peut donc communiquer un message de petite taille cache dans la permutation des couleurs dans la palette de l'image.

- **Message caché dans le domaine de compression d'une image**

Tout semble indiquer que l'on ne peut cacher un message dans un format d'image utilisant une compression avec perte. En réalité la plupart des programmes de stéganographie sérieux s'attaquent justement au format JPEG qui utilise ce type de compression.

L'idée n'est pas de cacher une information dans les couleurs ou dans la palette (puisqu'il n'y en a pas) mais dans les choix de compression. En effet, tout algorithme de compression nécessite une succession de choix.

Avec des algorithmes de compression tel que Zip ou Gzip, on peut choisir la puissance de compression. En consommant plus de temps calcul et/ou plus de mémoire pour les opérations intermédiaires, on peut obtenir de meilleurs résultats de compression. Ainsi deux fichiers compresses de tailles différentes peuvent être décompresses en deux fichiers identiques.

La compression dans le format JPEG est double. La première compression consiste à découper l'image en bloc de 8 fois 8 pixel et de transformer ce carre sous une forme mathématique simplifiée. Cette compression introduit des pertes et la version mathématique peut être légèrement différente de la carre originale tout en étant visuellement très semblable. Une fois tous les blocs compresses, il faut coder les formes mathématiques en consommant le moins possible d'espace. Cette deuxième compression n'introduit pas de perte et est similaire dans les principes a ce que l'on peut retrouver dans Zip ou Gzip. C'est en introduisant dans cette phase des bits d'informations que l'on arrive à transporter un message cache.

IV.3.b.Message transporté dans un texte

Décaler une lettre de quelques pixels ne pose aucun problème sur une imprimante à laser et est pratiquement invisible a l'œil nu. En jouant sur les interlettrages d'un texte très long et à raison de deux valeurs d'espacement correspondant à 1 et 0, il est possible de transmettre un message sous forme papier, qui ne révélera son vrai sens qu'une fois analysé par un scanner ayant une bonne précision.

Historiquement, le procédé fut utilisé dans les années 70 en utilisant non pas des imprimantes laser, mais des imprimantes à marguerite Diablo, qui permettaient de jouer sur l'espacement des caractères au 1/120e de Cryptologie pouce prs.

IV.3.c. Message transporté dans un son

Dans les formats sonores, il existe à peu près les mêmes possibilités de cacher des messages que dans les images.

Dans un fichier sonore au format MIDI, il n'existe pas de palette de couleurs mais bien différentes pistes qui peuvent être permutées.

Dans un fichier sonore avec compression sans perte, on peut cacher de l'information dans des variations imperceptibles du son, les bits faiblement significatifs.

Dans un fichier sonore avec compression avec perte, on peut cacher de l'information dans les choix de compression.

V. Conclusion

La cryptographie ne permet pas, de masquer l'existence des données chiffrées, mais on peut le faire avec la stéganographie alors opter pour des outils de stéganographie permettront de camoufler les fichiers à protéger dans d'autres fichiers

plus anodins (images ou sons, par exemple). On pourra ainsi créer un coffre-fort électronique afin d'y entreposer les données que l'on voudrait sécuriser

Il existe donc de nombreux procédés et méthodes permettant de transmettre des informations de manière sécurisé. À partir du moment où aucun moyen de factorisation rapide ne verra le jour, alors le système RSA restera probablement le système de cryptage /décryptage le plus fiable et le plus sécurisé au monde.

Enfin, comme tout domaine scientifique, la crypto aura grandement évoluée au cours du temps.

Bibliographie

[1] Samia Chikhi; « **Contribution à l'authentification souple d'image digitales par des technique de marquage numérique-Application aux images médicales** » ; thèse doctorat ; Université Montouri de Constantine ; Octobre 2008.

[2] Jean Max Redonnet; « Introduction à la Cryptographie et à la stéganographie » ; Université Paul Sabatier département Sciences Appliquées ; version 0.2, Septembre 2009.

[3] Fridirik Arnault; « **Théorie des Nombre et Cryptographie** » ; Université de Limoge ; Mai 2002.

[4] Jean Marc Manach - journaliste à InternetActu.net ; « **Comment contourner les systèmes de traçabilité** »; version originale d'un article publié dans Hermès n°53: "Traçabilité et réseaux" ; France, 2009.

[5] NAI.N.A. I ; « **Une Introduction à la Cryptographie** » ; 1998.

[6] Fabien Gargne, Christian Knoff et Gaeten Lecourtois ; « **Codage, Compression et Cryptologie** »; Licence d'Informatique; Université de Nice-Sophia Antipolis ; Année 2004–2005

[7] Club.D ; « **Introduction à la Cryptographie** » ; (http://ram-0000.developpez.com); Janvier 2009

[8] Oranci Sevan, Pourroy Louis ; « **Cryptage et le problème du sac à dos** » ; Sujet n°14 ; EPMI.

[9] Arnaud Contes ; « **Une architecture de sécurité hiérarchique, adaptable et dynamique pour la grille** » ; thèse de doctorat; université de Nice - Sophia Antipolis ; Septembre 2005

Chapitre 3

Applications et expériences

I. Introduction

Les problèmes décrits précédemment où et comment caché l'information, représentent des risques en informatique et cela peut être comparé aux risques de voles dans la société (une personne qui essaye de protéger son trésor en le mettant dans un coffre fort qui est caché derrière un cadre). On peut comparer cette personne à un informaticien qui utilise la cryptographie pour envoyer des messages codés hybridé avec la stéganographie qui dissimule et cache la transmission de ce message sous une image.

II. Outils et environnement de développement

Avant de commencer l'implémentation de l'application, il y a lieu d'abord de spécifier les outils utilisés qu'on a suggéré être le bon choix vu les avantages qu'ils offrent.

II.a. Ressources matériel

Nous avons développé notre application sur une machine CoreProcessor TK-55, avec une vitesse de 2,80 GHz, doté d'une capacité mémoire de 2,00 GB de RAM.

II.b. Logiciels

Concernant les ressources logicielles un Microsoft Windows 7 Edition Intégrale est installée sur cet ordinateur, avec un MATLAB 8.0 qui est utilisée pour l'implémentation du travail.

- **Pourquoi Matlab ?**

Le site officiel de MATLAB définit MATLAB avec environnement interactif comme un langage de haut niveau permettant l'exécution de tâches nécessitant une grande puissance de calcul et dont la mise en œuvre sera plus rapide qu'avec des langages de programmation traditionnels tels que le C, le C++ [2].

MATLAB peut être utilisé dans une grande variété d'applications, incluant le traitement du signal et d'images, ainsi que la biologie informatique. Des boîtes à outils supplémentaires (collections de fonctions MATLAB à vocation spécifique, disponibles séparément) élargissent l'environnement MATLAB pour résoudre des catégories particulières de problèmes dans ces domaines d'applications. Les Principales fonctionnalités de Matlab sont :

- Langage de haut niveau pour le calcul scientifique ;
- Environnement de développement pour la gestion du code, des fichiers et des données ;

- Outils interactifs pour l'exploration itérative, la conception et la résolution de problèmes ;
- Outils pour la construction d'interfaces graphiques personnalisées ;
- Fonctions pour l'intégration d'algorithmes développés en langage MATLAB, dans des applications et langages externes, tels que C/C++, Fortran, Java, COM et Microsoft Excel.

III. Corpus

Pour réaliser ce travail qui est une proposition d'un système de communication d'un message secret en utilisant la stéganographie, il est nécessaire de trouver une base de données pour l'application qui sera utilisée dans le domaine de la stéganographie.

III.1 Description de la base de données

La base d'images c'est la base d'image Wang qui contient en général 1000 images séparées en 10 classes, chaque classe contient 100 images, on a pris 6 classes (Rose, Cheval, Nature, Eléphant, Maison, Bus) chaque une contient 20 images de type (JPEG, PNG, BMP, GIF) et de taille 256*384.

III.2 Implémentation

Le but de ce travail est de renforcer la sécurité (en enterrant le coffre-fort) càd crypter un message en utilisant une des techniques de cryptographie à clé secrète puis dissimuler le message dans une image avec la technique de poids faible dans la stéganographie.

III.2.a. Cryptographie

Cette étape consiste à transformer le texte clair en un texte crypté, en utilisant les systèmes cryptographiques à clé privée pour l'implémentation on a choisi le chiffrement par décalage (code de César).

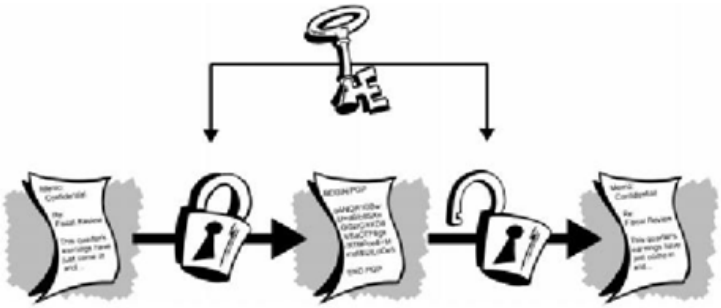


Figure 09 : *chiffrement conventionnel* [5].

- **Code de César**

Avec une clé de 04 (le décalage circulaire fait que le A est remplacé par D, B par E, C par F… comme le montre le tableau 01).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tableau 01 : *Cryptogramme de l'Alphabet en Majuscule*

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Tableau 02 : *Cryptogramme de l'Alphabet en Minuscule*[1]

Exemple

Il devient simple de faire le chiffrement : « Cryptographie » deviens « Fuswrjudsklh ».

III.2.b. Stéganographie

Dans cette étape on a intégré un message qui va être transporté dans une image, la technique de base est LSB[2], qui consiste à modifier le bit de poids faible des pixels codant l'image.

Chaque pixel d'une image est représenté par 3 nombres codés sur 8 bits : R représente l'intensité du rouge (un entier entre 0 et 255), G celle du vert, B celle du bleu.

Figure 10 : *Effet visuel de la modification des bits les moins significatifs des composants RGB d'un pixel* [1].

[1] En Matlab les lettres majuscules et minuscules sont définies différemment.
[2] LSB - Least Signifiant Bit.

Dans cette méthode on va replacer le dernier bit de chaque pixel par un bit du message dont les caractères déjà converti en binaire à l'aide du code ASCCI et bien sûr cette modification sur l'image est imperceptible à l'œil humain.

A	01000001	J	01001010	S	01010011
B	01000010	K	01001011	T	01010100
C	01000011	L	01001100	U	01010101
D	01000100	M	01001101	V	01010110
E	01000101	N	01001110	W	01010111
F	01000110	O	01001111	X	01011000
G	01000111	P	01010000	Y	01011001
H	01001000	Q	01010001	Z	01011010
I	01001001	R	01010010	espace	00100000

Figure 11 : *Un extrait de schéma de codage ASCII* [6].

Exemple: on a les pixels suivants d'une image A

Les pixels	Les pixels en binaire	Cacher message	Message en binaire
166	10100110	10100111	
165	10100101	10100111	
164	10100100	10100101	
165	10100101	10100101	
166	10100110	10100110	
166	10100110	10100110	h: 1101000
165	10100101	10100101	i : 1101001
164	10100100	10100101	
166	10100110	10100110	
164	10100100	10100100	
164	10100100	10100100	
166	10100110	10100110	
166	10100110	10100110	
164	10100100	10100101	

A= 166 165 164 165 166 166 165 164 166 164 164 166 166 164

Message = hi

Message	**hi**
Message en binaire	**h: 1101000** **i : 1101001**

L'algorithme

1. lire image;
2. afficher les pixels de l'image ;
3. le message est affecté dans une variable ;
4. convertir le texte en code ASCII puis en binaire ;
5. convertir les pixels en binaire ;
6. définir le nombre de bit dans le texte ;
7. modifier le bit numéro 8 de chaque pixel et le remplacer par un bit du message.

III.3. Le déroulement de l'expérimentation

Le fonctionnement général de l'implémentation sera représenté dans cette partie.

III.3.a. Etude et analyse

Dans cette étude on doit faire une comparaison entre deux catégories d'image

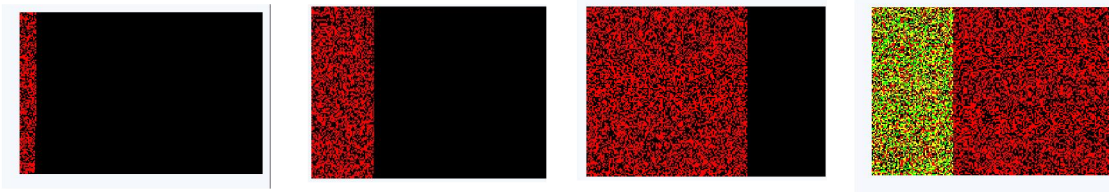
- ✓ Image couleur
- ✓ Image niveaux de gris

Cette comparaison, consiste à calculer le temps d'exécution pour cacher le texte crypté dans l'image[3]. Puis représenter les résultats dans un graphe.

III.3.b. L'intervalle de modification dans l'image

Dans ce cas on utilise quatre codes de texte tel que: code1 (contient 10 lignes), code2 (contient 40 lignes), code3 (contient 100 lignes) et code4 (contient 200 lignes).

[3] Le test est fait sur 4 images de chaque type (BMP, PNG, JPEG, GIF).



Code1 Code2 Code3 Code4

Figure 12: *Intervalle de modification dans l'image*

Il est impossible, à l'œil, de distinguer l'image qui cache le message, et l'image initiale.

Figure 13 : *Image originale*

Figure 14 : *Image stéganographiée*

III.4.c. L'interface de programme

L'étude de l'application est structurée en deux parties : la première est de coder un texte dans une image, la deuxième est de décoder le texte caché dans cette image.

Figure 15 : *L'interface principale.*

- L'interface principale contient deux boutons :
  - Le bouton coder pour cacher le texte dans l'image.
  - Le bouton décoder pour récupérer le texte caché.

- Si on clique sur le bouton coder on trouve l'interface suivante :

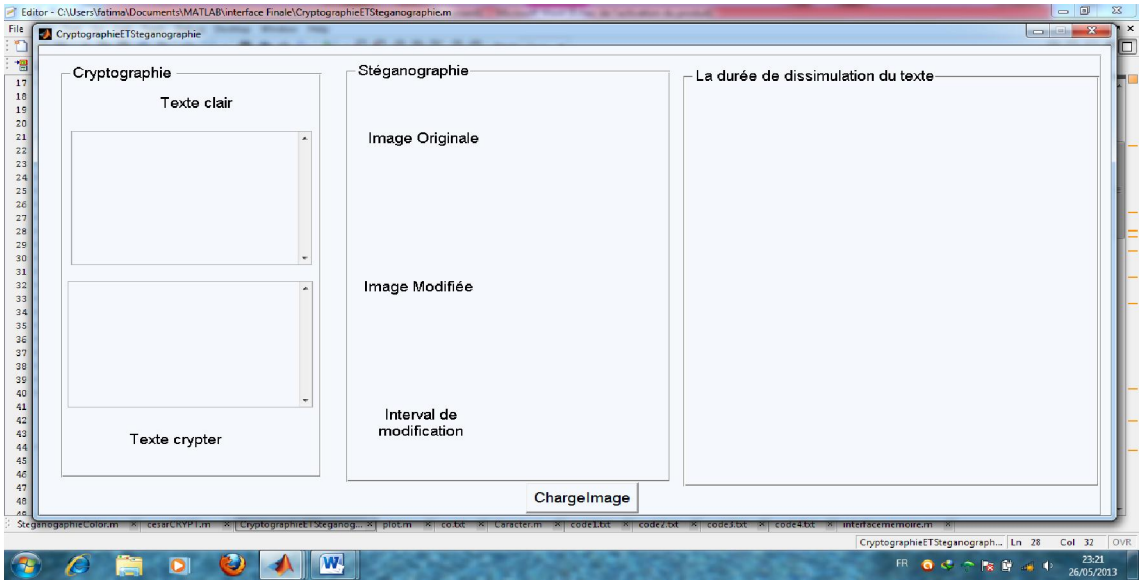


Figure 16 : *L'interface du codage.*

- L'interface du codage contient un bouton (charge image) et trois parties séparées:

  - Cryptographie ;
  - Stéganographie ;
  - la durée de dissimulation du texte.

- Si on clique sur le bouton décoder on trouve l'interface suivante :

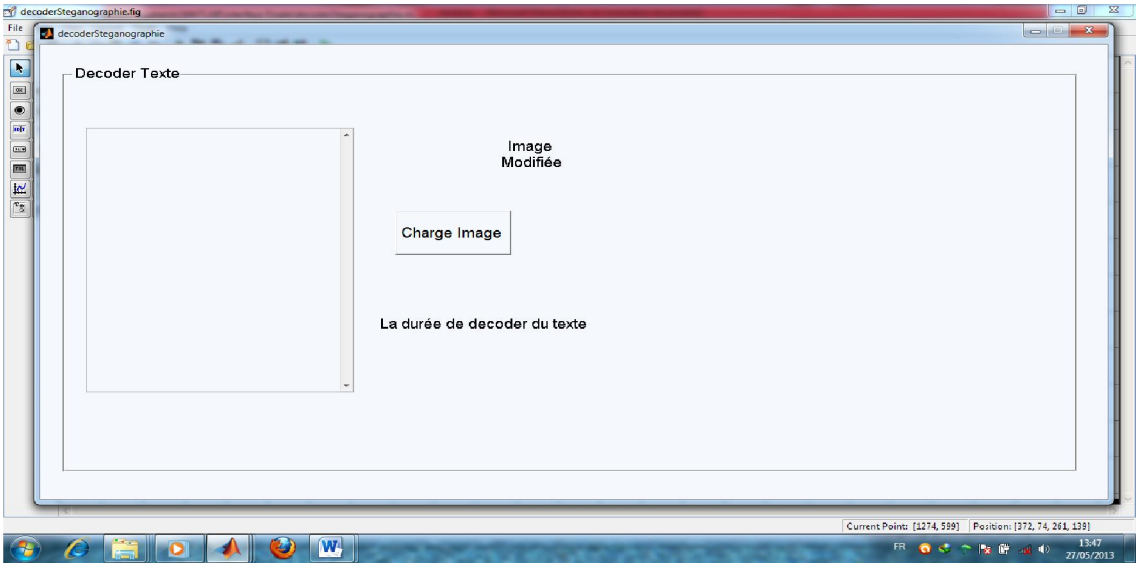


Figure 17 : *L'interface du décodage.*

- L'interface du décodage est séparée en trois parties :

  - image modifiée qui contient le texte.
  - la durée de codage du texte pour afficher le graphe.

- un éditeur de texte pour afficher le texte caché dans l'image.

III.4.d. Comparaisons entre les différents types d'image selon le temps

Image(JPEG)	Le texte caché	Le temps de cache ($\times 10^{-3}$) S
Bus1.jpg	Code1.txt (10 lignes, 810caracter)	0.0001
Chevale18.jpg		0.0003
Elephon9.jpg		0.0001
Maison1.jpg		0.0001
Bus1.jpg	Code2.txt (40 lignes, 3240caracter)	0.0005
Chevale18.jpg		0.0005
Elephon9.jpg		0.0090
Maison1.jpg		0.0005
Bus1.jpg	Code3.txt (100 lignes, 8100caracter)	0.0013
Chevale18.jpg		0.0013
Elephon9.jpg		0.0013
Maison1.jpg		0.0014
Bus1.jpg	Code4.txt (200 lignes, 16200caracter)	0.0026
Chevale18.jpg		0.0026
Elephon9.jpg		0.0027
Maison1.jpg		0.0026

Tableau 03 : *Analyse du résultat de l'image JPEG*

Après l'analyse on obtient les graphes suivants :

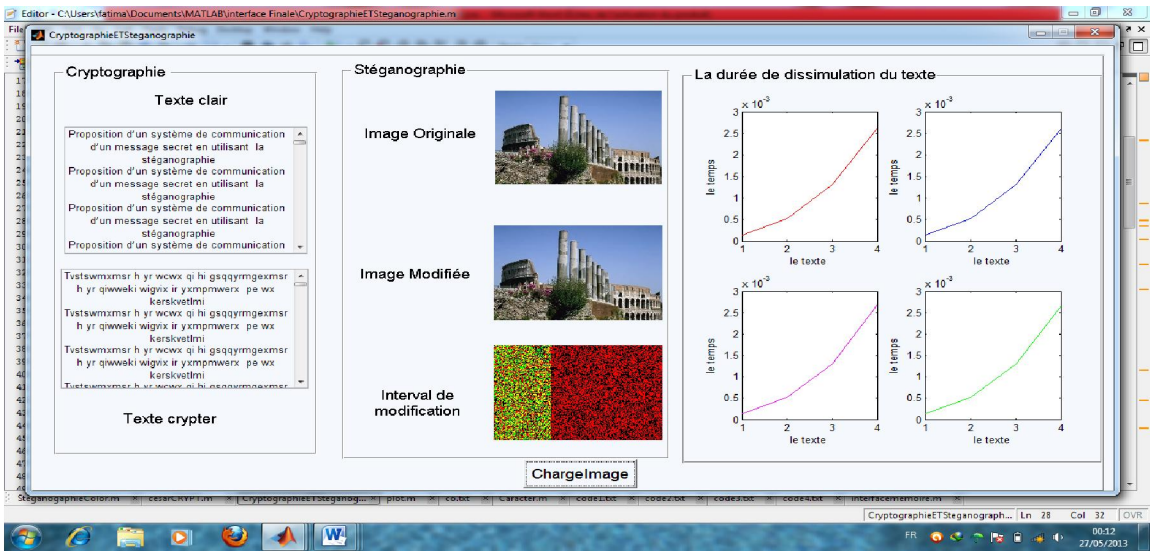


Figure 18 : *Graphe d'analyse de l'image JPEG*

Le graphe rouge représente l'analyse de l'image (bus1.jpg), le bleu représente l'analyse de l'image (chevale18.jpg), le mauve représente l'analyse de (elephon9.jpg) et le vert représente l'image (maison1.jpg).

Image(BMP)	Le texte caché	Le temps de cache ($\times 10^{-3}$) S
Bus11.bmp	Code1.txt (10 lignes, 810caracter)	0.0001
Chevale20.bmp		0.0001
Rose12.bmp		0.0001
Nature8.bmp		0.0001
Bus11.bmp	Code2.txt (40 lignes, 3240caracter)	0.0005
Chevale20.bmp		0.0005
Rose12.bmp		0.0005
Nature8.bmp		0.0005
Bus11.bmp	Code3.txt (100 lignes, 8100caracter)	0.0013
Chevale20.bmp		0.0013
Rose12.bmp		0.0013
Nature8.bmp		0.0013
Bus11.bmp	Code4.txt (200 lignes, 16200caracter)	0.0026
Chevale20.bmp		0.0026
Rose12.bmp		0.0026
Nature8.bmp		0.0026

Tableau 04: *analyse du résultat de l'image BMP*

Après l'analyse on obtient les graphes suivants :

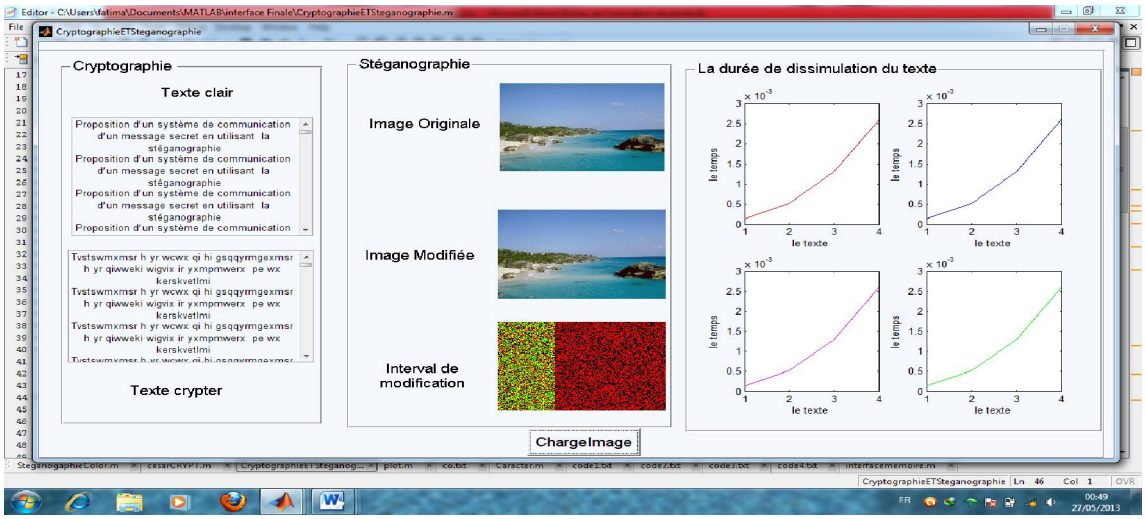


Figure 19 *: Graphe d'analyse de l'image BMP*

Le graphe rouge représente l'analyse de l'image (bus11.bmp), le bleu représente l'analyse de l'image (chevale20.bmp), le muove représente l'analyse de (rose12.bmp) et le vert représente l'image (nateur8.bmp).

Image(GIF)	Le texte caché	Le temps de cache ($\times 10^{-3}$) S
Bus16.gif	Code1.txt (10 lignes, 810caracter)	0.0001
Elephon10.gif		0.0001
Maison6.gif		0.0001
Nature14.gif		0.0001
Bus16.gif	Code2.txt (40 lignes, 3240caracter)	0.0005
Elephon10.gif		0.0005
Maison6.gif		0.0005
Nature14.gif		0.0005
Bus16.gif	Code3.txt (100 lignes, 8100caracter)	0.0013
Elephon10.gif		0.0013
Maison6.gif		0.0013
Nature14.gif		0.0014
Bus16.gif	Code4.txt (200 lignes, 16200caracter)	0.0034
Elephon10.gif		0.0026
Maison6.gif		0.0026
Nature14.gif		0.0027

Tableau 05 : *Analyse du résultat de l'image GIF*

Après l'analyse on obtient les graphes suivants :

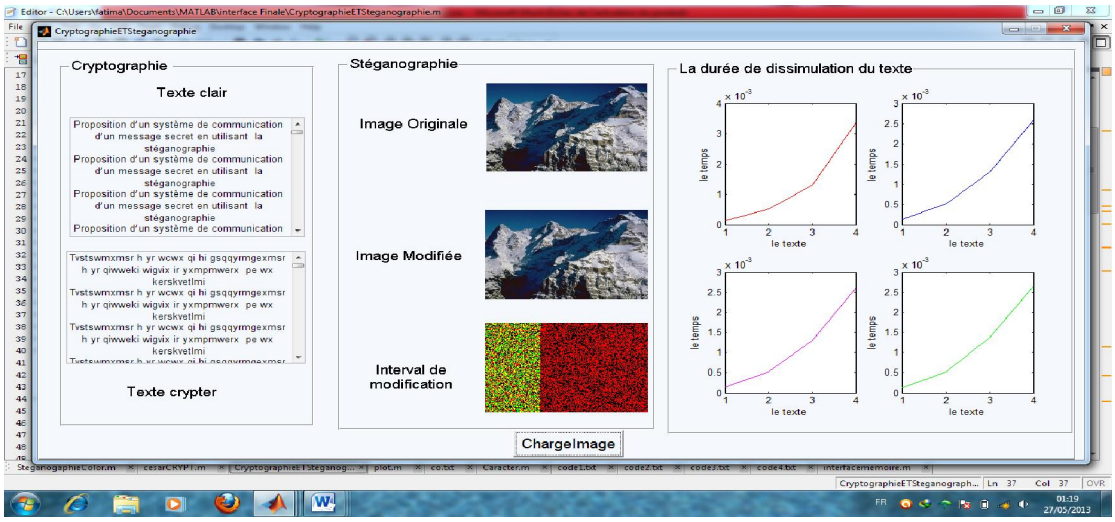


Figure 20 *: Graphe d'analyse de l'image GIF*

Le graphe rouge représente l'analyse de l'image (bus16.gif), le bleu représente l'analyse de l'image (elephon10.gif), le muove représente l'analyse de (maison6.gif) et le vert représente l'image (nature14.gif).

Image(PNG)	Le texte caché	Le temps de cache ($\times 10^{-3}$) S
Chevale1.png	Code1.txt (10 lignes, 810caracter)	0.0001
Maison15.png		0.0001
Nateur2.png		0.0001
Rose20.png		0.0001
Chevale1.png	Code2.txt (40 lignes, 3240caracter)	0.0005
Maison15.png		0.0005
Nateur2.png		0.0005
Rose20.png		0.0005
Chevale1.png	Code3.txt (100 lignes, 8100caracter)	0.0013
Maison15.png		0.0013
Nateur2.png		0.0013
Rose20.png		0.0013
Chevale1.png	Code4.txt (200 lignes, 16200caracter)	0.0026
Maison15.png		0.0037
Nateur2.png		0.0026
Rose20.png		0.0026

Tableau 06 : *l'analyse du résultat de l'image PNG*

Après l'analyse on obtient les graphes suivants :

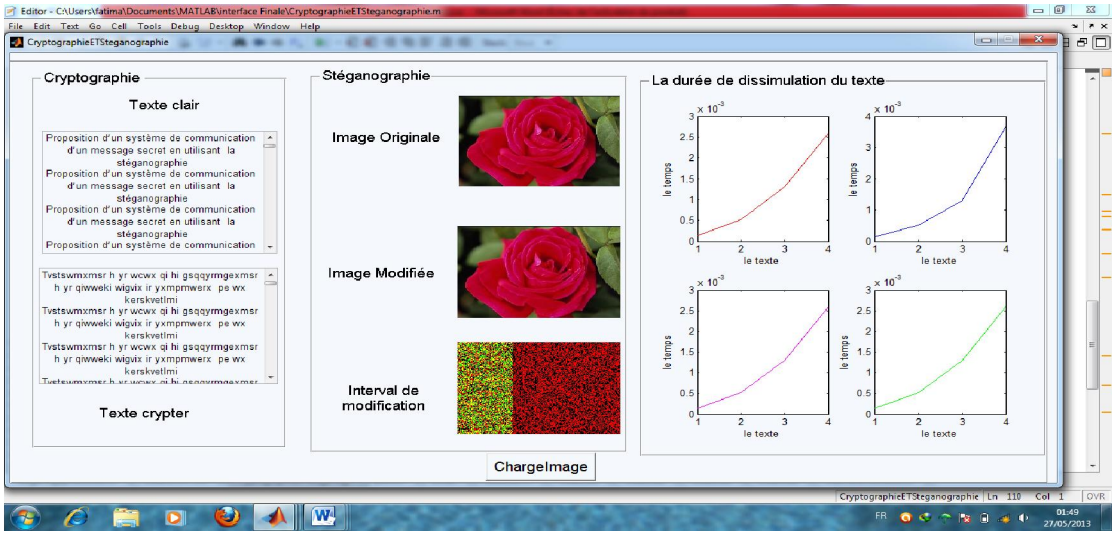


Figure 21 : *Graphe d'analyse de l'image PNG*

Le graphe rouge représente l'analyse de l'image (chevale1.png), le bleu représente l'analyse de l'image (maison15.png), le muove représente l'analyse de (nateur2.png) et le vert représente l'image (rose20.png).

- **Résultats**

Après la comparaison entre les différents types d'image en fonction de la durée du codage, les résultats suivants sont obtenus :

Image	Le texte caché	Intervalle de temps de cache ($\times 10^{-3}$) S
Image.jpg	Code1.txt (10 lignes, 810caracter)	] 0.0001, 0.0003 [
Image.bmp		0.0001
Image.gif		0.0001
Image.png		0.0001
Image.jpg	Code2.txt (40 lignes, 3240caracter)	] 0.0005, 0.0090 [
Image.bmp		0.0005
Image.gif		0.0005
Image.png		0.0005
Image.jpg	Code3.txt (100 lignes, 8100caracter)	] 0.0013, 0.0014 [
Image.bmp		0.0013
Image.gif		] 0.0013, 0.0014 [
Image.png		0.0013
Image.jpg	Code4.txt (200 lignes, 16200caracter)	] 0.0026, 0.0027 [
Image.bmp		0.0026
Image.gif		] 0.0026, 0.0034 [
Image.png		] 0.0026, 0.0037 [

Tableau 07 : *analyse des résultats* des déférents types d'image (JPG, BMP, PNG, GIF)

Selon les résultats précédents on remarque que l'image BMP est la plus vite en terme de codage et dissimulation par rapport aux autres images, après JPEG puis GIF et en dernier PNG. Donc on peut dire que le type BMP est le meilleur dans la stéganographie.

III.3.e. Analyse dès images en niveaux de gris

Comparaisons selon le temps de dissimulation

Image (JPEG)	Le texte caché	Le temps de cache ($\times 10^{-3}$) S
Bus1.jpg	Code1.txt (10 lignes, 810caracter)	0.0001
Chevale18.jpg		0.0003
Elephon9.jpg		0.0001
Maison1.jpg		0.0001
Bus1.jpg	Code2.txt (40 lignes, 3240caracter)	0.0005
Chevale18.jpg		0.0005
Elephon9.jpg		0.006
Maison1.jpg		0.0005
Bus1.jpg	Code3.txt (100 lignes, 8100caracter)	0.0013
Chevale18.jpg		0.0015
Elephon9.jpg		0.0013
Maison1.jpg		0.0013
Bus1.jpg	Code4.txt (149lignes, 12069caracter)	0.0019
Chevale18.jpg		0.0019
Elephon9.jpg		0.0019
Maison1.jpg		0.0020

Tableau 08 : *analyse de l'image JPG en niveaux de gris*

Après l'analyse on obtient le graphe suivant

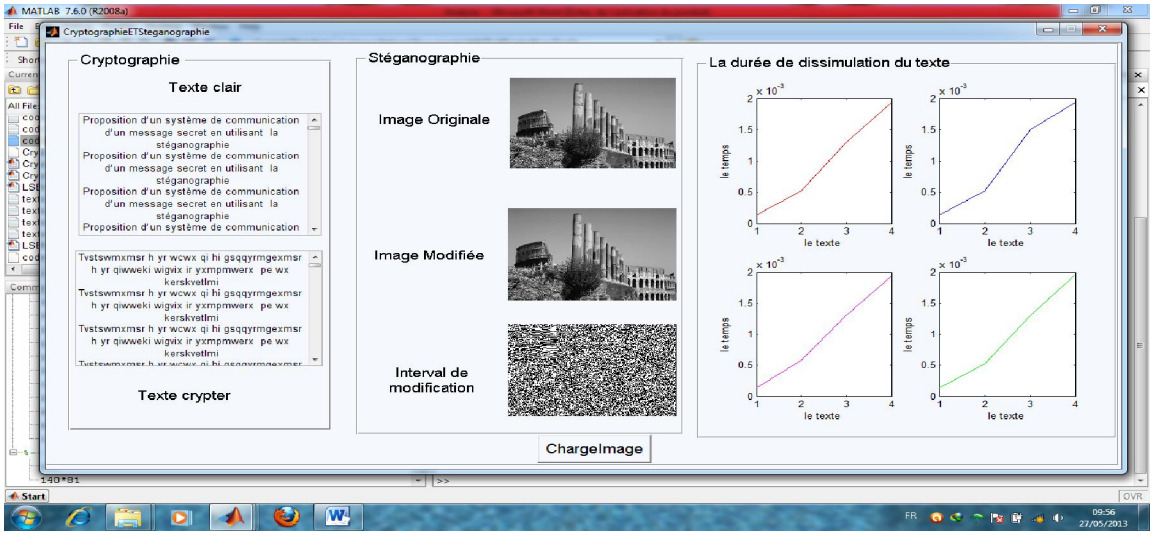


Figure 22 *: Graphe d'analyse de l'image JPG en niveaux de gris*

Le graphe rouge représente l'analyse de l'image (bus1.jpg), le bleu représente l'analyse de l'image (chevale18.jpg), le muove représente l'analyse de (elephon9.jpg) et le vert représente l'image (maison1.jpg). On remarque que l'intervalle de temps est équivalent pour chaque image.

Image (BMP)	Le texte caché	Le temps de cache ($\times 10^{-3}$) S
Bus11.bmp	Code1.txt (10 lignes, 810caracter)	0.0001
Chevale20.bmp		0.0001
Rose12.bmp		0.0001
Nature8.bmp		0.0001
Bus11.bmp	Code2.txt (40 lignes, 3240caracter)	0.0005
Chevale20.bmp		0.0005
Rose12.bmp		0.0005
Nature8.bmp		0.0005
Bus11.bmp	Code3.txt (100 lignes, 8100caracter)	0.0014
Chevale20.bmp		0.0013
Rose12.bmp		0.0013
Nature8.bmp		0.0013
Bus11.bmp	Code4.txt (149lignes, 12069caracter)	0.0020
Chevale20.bmp		0.0020
Rose12.bmp		0.0019
Nature8.bmp		0.0019

Tableau 09 : *l'analyse de l'image (BMP) au niveau de gris*

Après l'analyse on obtient le graphe suivant :

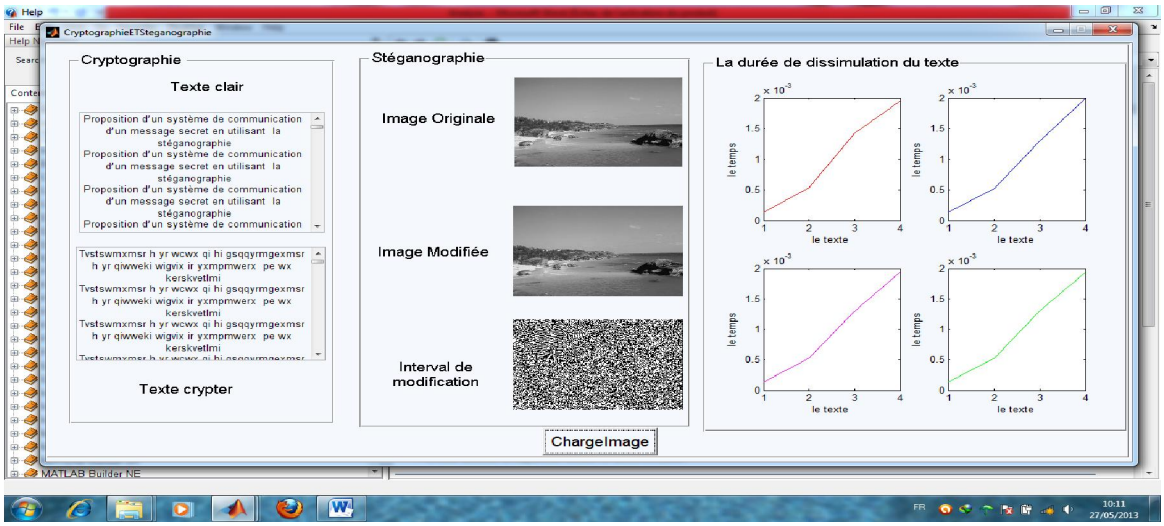


Figure 23 *: Graphe d'analyse de l'image BMP au niveau de gris*

Le graphe rouge représente l'analyse de l'image (bus11.bmp), le bleu représente l'analyse de l'image (chevale20.bmp), le muove représente l'analyse de (rose12.bmp) et le vert représente l'image (nateur8.bmp). On remarque que l'intervalle de temps est équivalent pour chaque image.

Image (GIF)	Le texte caché	Le temps de cache ($\times 10^{-3}$) S
Bus16.gif	Code1.txt (10 lignes, 810caracter)	0.0001
Elephon10.gif		0.0001
Maison6.gif		0.0001
Nateur14.gif		0.0001
Bus16.gif	Code2.txt (40 lignes, 3240caracter)	0.0005
Elephon10.gif		0.0005
Maison6.gif		0.0005
Nateur14.gif		0.0005
Bus16.gif	Code3.txt (100 lignes, 8100caracter)	0.0013
Elephon10.gif		0.0013
Maison6.gif		0.0013
Nateur14.gif		0.0013
Bus16.gif	Code4.txt (149 lignes, 12069caracter)	0.0019
Elephon10.gif		0.0019
Maison6.gif		0.0019
Nateur14.gif		0.0019

Tableau 10: *analyse de l'image (GIF) au niveau de gris*

Après l'analyse on obtient le graphe suivant

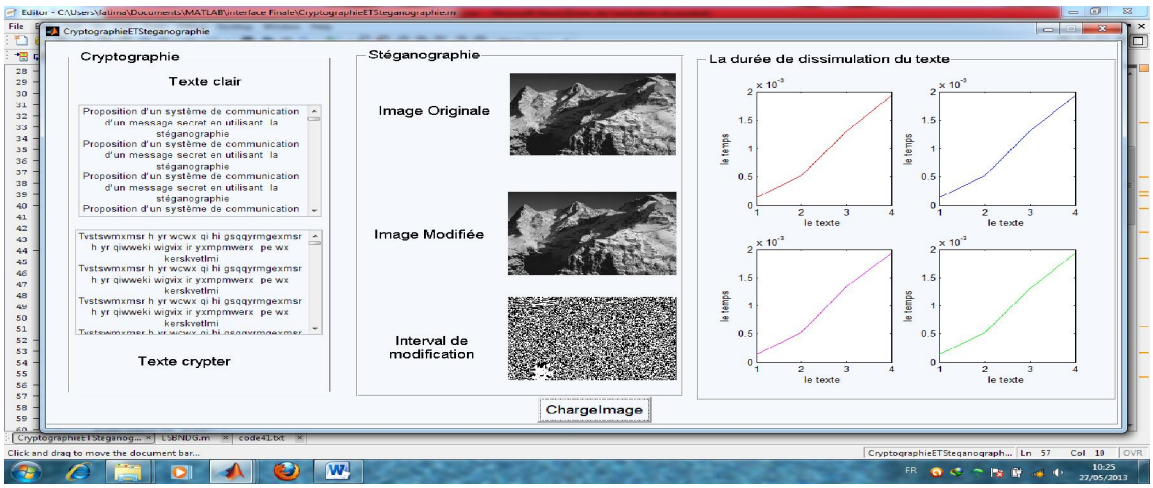


Figure 24 *: Graphe d'analyse de l'image JPEG au niveau de gris*

Le graphe rouge représente l'analyse de l'image (bus16.gif), le bleu représente l'analyse de l'image (elephon10.gif), le muove représente l'analyse de (maison6.gif) et le vert représente l'image (nateur14.gif).On remarque que l'intervalle de temps est équivalent pour chaque image.

Image(PNG)	Le texte caché	Le temps de cache ($\times 10^{-3}$) S
Chevale1.png	Code1.txt (10 lignes, 810caracter)	0.0001
Maison15.png		0.0001
Nateur2.png		0.0001
Rose20.png		0.0001
Chevale1.png	Code2.txt (40 lignes, 3240caracter)	0.0005
Maison15.png		0.0005
Nateur2.png		0.0005
Rose20.png		0.0006
Chevale1.png	Code3.txt (100 lignes, 8100caracter)	0.0013
Maison15.png		0.0013
Nateur2.png		0.0013
Rose20.png		0.0013
Chevale1.png	Code4.txt (149 lignes, 12069caracter)	0.0020
Maison15.png		0.0019
Nateur2.png		0.0019
Rose20.png		0.0019

Tableau 11 : *analyse de l'image (PNG) au niveau de gris*

Après l'analyse on obtient le graphe suivant

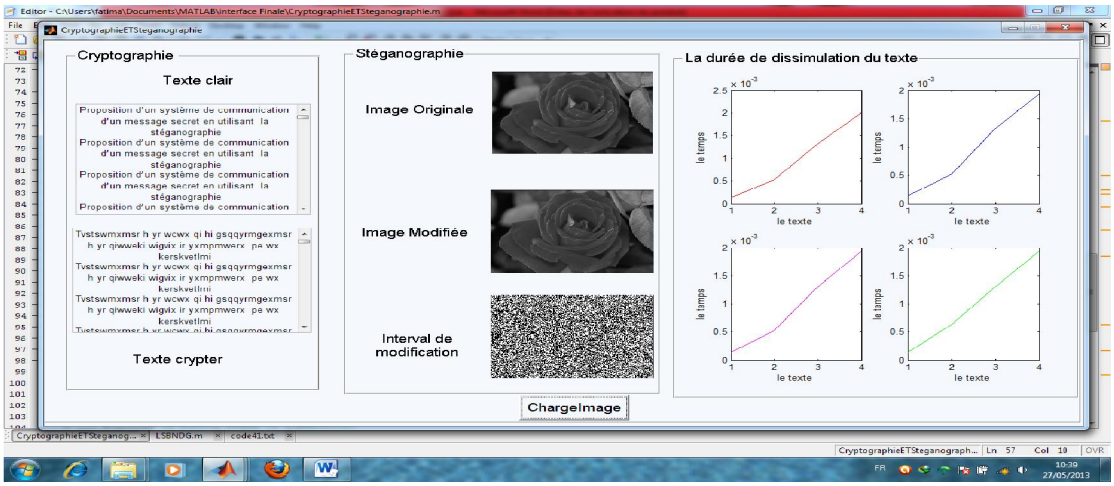


Figure 25 *: Graphe d'analyse de l'image PNG au niveau de gris*

Le graphe rouge représente l'analyse de l'image (chevale1.png), le bleu représente l'analyse de l'image (maison15.png), le muove représente l'analyse de (nateur2.png) et le vert représente l'image (rose20.png).On remarque que l'intervalle de temps est équivalent pour chaque image.

- Comparaison entre les 4 types d'image

Image	Le texte caché	Intervalle de temps de cache ($\times 10^{-3}$) S
Image.jpg	Code1.txt (10 lignes, 810caracter)	] 0.0001, 0.0003 [
Image.bmp		0.0001
Image.gif		0.0001
Image.png		0.0001
Image.jpg	Code2.txt (40 lignes, 3240caracter)	] 0.0005, 0.0006 [
Image.bmp		0.0005
Image.gif		0.0005
Image.png		] 0.0005, 0.0006 [
Image.jpg	Code3.txt (100 lignes, 8100caracter)	] 0.0013, 0.0015 [
Image.bmp		] 0.0013, 0.0014 [
Image.gif		0.0013
Image.png		0.0013
Image.jpg	Code4.txt (149 lignes, 12069caracter)	] 0.0019, 0.0020 [
Image.bmp		] 0.0019, 0.0020 [
Image.gif		0.0019

Image.png		] 0.0019, 0.0020 [

Tableau 12 : *comparaison entre les déférences type d'image (JPG, BMP, PNG, GIF) au niveau de gris*

Selon les résultats précédents on remarque que l'image GIF est la plus vite par port aux autres images, après PNG puis BMP et en dernier JPEG. Donc on peut dire que La GIF est la meilleure dans la catégorie d'image au niveau de gris.

- Comparaison entre l'image colorée est l'image au niveau de gris

Image (PNG)	Le texte caché	Le temps de cache ($\times 10^{-3}$) S
Image coloré	Code1.txt (10 lignes, 810caracter)	] 0.0001, 0.0003 [
	Code2.txt (40 lignes, 3240caracter)	] 0.0005, 0.0090 [
	Code3.txt (100 lignes, 8100caracter)	] 0.0013, 0.0014 [
	Code4.txt (149 lignes, 12069caracter)	] 0.0019, 0.0020 [
Image en niveaux de gris	Code1.txt (10 lignes, 810caracter)	] 0.0001, 0.0003 [
	Code2.txt (40 lignes, 3240caracter	] 0.0013, 0.0015 [
	Code3.txt (100 lignes, 8100caracter)	] 0.0005, 0.0006 [
	Code4.txt (149 lignes, 12069caracter)	] 0.0019, 0.0020 [

Tableau 13 : *analyse des résultats des deux type (colorée et niveaux de gris)*

Observations

On distingue que l'image colorée est plus rapide que l'image au niveau de gris.

- La taille dès images colorées utilisées est (256*384) et après l'analyse et le traitement on trouve que la capacité maximale d'une image pour cacher un texte est 448 lignes (36288 caractères) avec un temps de 0.0061$\times 10^{-3}$ s.

- La taille dès images au niveaux de gris utilisées est (256*384) est après l'analyse et le traitement on trouve que la capacité maximale d'une image pour cacher un texte est 149 lignes (12069 caractères) avec un temps de 0.0020$\times 10^{-3}$ s.

III.3.f. Partie décoder texte

- Comparaisons selon le temps

Image	Le texte décodé	Le temps de décodage ($\times 10^{-3}$) S
Image modifié (colorée)	Texte1.txt (10 lignes, 810caracter)	0.0373
	Texte2.txt (40 lignes, 3240caracter)	0.0905
	Texte3.txt (100 lignes, 8100caracter)	0.1871
	Texte4.txt (200 lignes, 16200caracter)	0.6358

Tableaux 14: *le temps de décoder un texte caché dans une image colorée*

Après l'analyse on trouve le graphe suivant

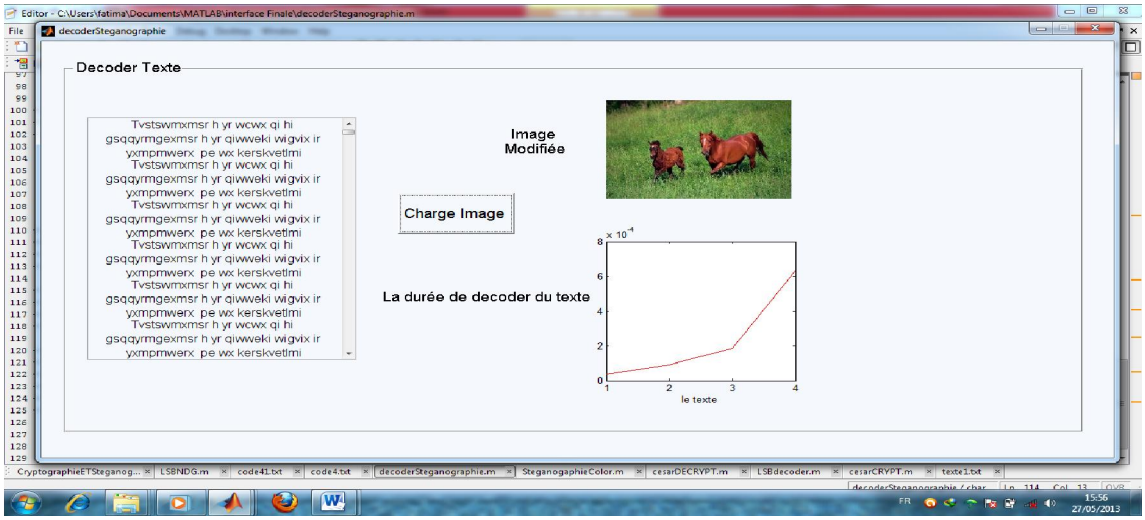


Figure 26 : *Graphe du temps pour l'image colorée*

Image	Le texte décodé	Le temps de décodage ($\times 10^{-3}$) S
Image modifié (niveaux de gris)	Texte1.txt (10 lignes, 810caracter)	0.0364
	Texte2.txt (40 lignes, 3240caracter)	0.01204
	Texte3.txt (100 lignes, 8100caracter)	0.1871
	Texte4.txt (149 lignes, 12069caracter)	0.2701

Tableau15 : *le temps de décoder un texte caché dans une image au niveau de gris*

Après l'analyse on obtient le graphe suivant

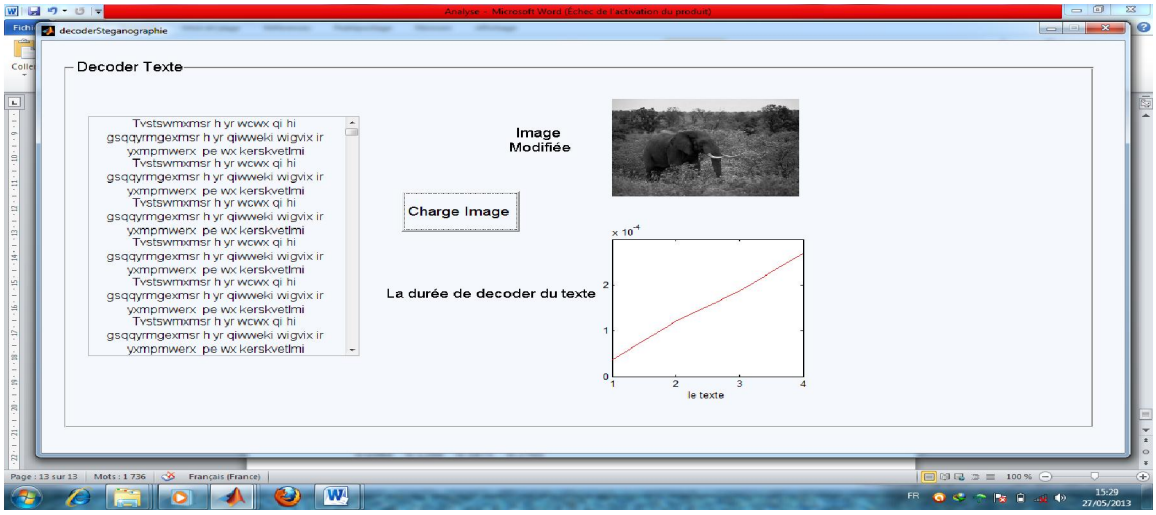


Figure 27 : *Graphe du temps pour l'image Au niveau de gris*

Observation

Après la dissimulation et la récupération du texte on remarque que le temps nécessaire pour coder est inférieur au temps nécessaire pour décoder le texte caché dans l'image.

IV. Conclusion

La réalisation d'un performant système de sécurité dépend des facteurs et des techniques utilisées pour coder et cacher les données.

On a utilisé deux algorithmes, le premier en cryptographie pour coder le message avec une méthode simple qui est le code de César. Et le deuxième en stéganographie pour cacher le message avec la méthode d'usage des bits de poids faible d'une image.

On a pu y arriver à classifier le type d'image qui convient le plus à être utilisée en stéganographie :

- Dans les images colorées on a BMP, JPEG, GIF, puis en dernier PNG.
- Dans les images au niveau de gris on a GIF, PNG, BMP, puis JPEG.

D'après les résultats trouvés, on constate que l'image colorée est plus rapide que l'image niveau de gris et que l'image colorée BMP est la meilleure en terme de dissimulation de données dans une image.

Bibliographie

[1] INTECO.N.T.C ; «**Stéganographie, l'art de cacher l'information** » ; (http://www.usatoday.com/tech/news/2001-02-05-binladen.htm).

[2] Ahmed Amine NAIR; « **Hybridation des réseaux de neurones avec les essaims de particules (MLP-PSO) :Application à la vérification de la signature** » ; Université des Sciences et de la Technologie d'Oran ; 2011.

[5] NAI .N.A.I ; « **Une Introduction à la Cryptographie** » ; 1998.

[6] Fabien Gargne, Christian Knoff et Gaeten Lecourtois ; « **Codage, Compression et Cryptologie** »; Licence d'Informatique; Université de Nice-Sophia Antipolis ; Année 2004–2005

Conclusion générale

La sécurité est avant tout un processus, rien ne sert, par exemple, d'installer une porte blindée si on laisse la fenêtre ouverte. On pourra donc créer un coffre-fort électronique afin d'y poser les données que l'on voudrait sécuriser.

Une information précieuse doit être bien protégée, parce que la perte d'une donnée très importante engendre des dégâts matériels et financiers et pour éviter tout cela des systèmes de protection ont été proposés.

Dans ce travail, en guise d'augmenter la sécurité, une hybridation entre la cryptographie et la stéganographie a été mise en œuvre, en utilisant le code de césar pour "coder les données" et la technique du bit du poids faible pour "cacher les données".

Puisque le temps d'exécution et l'espace mémoire reste toujours le défit de l'informatique, une implémentation est faite dans le but de sélectionner le type d'image qui convient le plus (en terme de rapidité de dissimilation) pour l'envoie d'un message secret en stéganographie.

Sûrement un travail de grande importance peut être fait dans le proche futur, il s'agit de reprendre cette implémentation en utilisant par exemple technique du RSA coté cryptographie qui aboutira sur un système hybride plus fiable et le plus sécurisé.

Table des matières

Chapitre 1 : la sécurité informatique

Chapitre 2 : la science des messages secrets

Chapitre 3 : Applications et expériences

Liste des figures

Liste des Tableaux

Introduction Générale

Dans ce travail, on essayera d'appliquer une méthode de sécurité informatique pour la résorption des vulnérabilités dans un système menacé par plusieurs programmes malveillants.

Il est évident, que les informations qui circulent par voie électronique se sont multipliées depuis l'invention d'internet. Celles ayant une importance militaire ou scientifique devaient être protégées lors des transmissions à travers le réseau. Cette nécessité de crypter les messages n'est pas nouvelle, mais devient cruciale à cause du fait que des informations circulent sur les réseaux internet traversant plusieurs nœuds avant d'arriver à leur destination.

Durant les dernières décades, l'informatique elle-même a connu un nouvel essor, se développant autour du slogan *"Le réseau est l'ordinateur"*. Effectivement, l'usage intensif, des communications, des réseaux et des systèmes distribués a ouvert les portes à de nouvelles attaques, à de nouvelles formes de protection. *La sécurité réseau* définit alors les moyens mis en œuvre pour protéger les données durant leur transmission, ainsi que pour garantir que les données transmises sont authentiques.

Il est important, de savoir que les menaces engendrent des risques et pertes financières, on a : primo la perte de confidentialité de données sensibles et secundo les dommages pour le patrimoine intellectuel.

De nos jours, la cryptologie est utilisée dans de nombreux domaines : militaire, informatique, financier et sécurité. Dans ce travail, on essayera de dissimuler la transmission d'un message sous une image avec une technique de stéganographie, notre but était de prouver la confidentialité et authenticité de cette méthode dans la sécurité réseau.

Organisation du travail :

Le premier chapitre traitera de la sécurité informatique en général. Le deuxième chapitre se concentrera sur la science des messages secrets. Dans le troisième chapitre on expliquera les manières de combiner les techniques de cryptographie et de stéganographie afin d'obtenir la confidentialité et l'authenticité. Enfin, une conclusion pour conclure et suggestions de l'utilisation du travail dans l'envoi des messages.