MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE
LA RECHERCHE SCIENTIFIQUE
UNIVERSITE ABDELHAMID IBN BADIS - MOSTAGANEM

Faculté des Sciences Exactes et de l'Informatique
Département de Mathématiques et d'Informatique
Filière : Informatique

MEMOIRE DE FIN D'ETUDES
Pour l'Obtention du Diplôme de Master en Informatique
Option : **Systèmes d'Information Géographique**

THEME :

Sécurisation des Régions de l'Image Satellite par la Cryptographie

Etudiantes : **SENOUCI Amina**

GHOUAL Denia

Encadrante : BENTAOUZA Chahinez Meriem

Année Universitaire 2015/2016

Résumé

Certaines régions présentes sur l'image sont trop sensibles et importantes ou elle contient des informations critiques, d'où le besoin de les protéger. La cryptographie était une science réservée aux militaires, elle permet de protéger les informations tout en gardant le secret pour garantir la confidentialité. Les travaux de recherche de ce mémoire s'inscrivent dans le cadre de la sécurité des images satellitaires, par algorithme asymétrique RSA, qui est fondé sur l'utilisation d'une paire de clés composée : une clé publique pour chiffrer et une clé privée pour déchiffrer les données confidentielles. L'originalité de ce mémoire consiste à proposer un cryptosystème à base d'algorithme RSA pour assurer les deux services de la sécurité l'authentification et l'intégrité, plus des schémas de tatouage proposés pour renforcer, garantir la sécurité et identifier le propriétaire du document de manière visible.

Mots clés : Cryptage par l'algorithme RSA, Cryptographie, Image satellite, Sécurité.

Abstract

Certain parts present in the image are too sensitive, important or it contains critical information, hence the need to protect. The Cryptography was a science reserved for the military, it helps protect the information while keeping it secret to ensure confidentiality. The research of this memoir is in the context of the security of satellite images, by the asymmetric algorithm called RSA, which is based on the use of a pair of composite keys: a public key to encrypt and a private key to decrypt the confidential data. The originality of this memoir is to provide a cryptosystem based on the RSA algorithm to ensure both the security services, authentication and integrity, plus of watermarking schemes proposed to strengthen, ensure security and identify the owner of the visible document.

Keywords: RSA algorithm Encryption, Cryptography, Satellite, Security.

Chapitre IV : Application et résultat

Conclusion générale

Introduction générale

L'échange de données (paroles, images, signes, signal etc.) pour l'homme est une nécessité.

La sécurité de cette opération devient parfois plus qu'une exigence. Ainsi depuis César à l'ère de l'informatique, le chiffrement de certains messages a toujours été un besoin afin de les cacher à tout intrus non autorisé de façon à s'abriter d'un éventuel usage malveillant. De nos jours, l'ensemble de ces méthodes a été regroupé dans une branche appelée la cryptographie.

La révolution numérique a engendré des moyens plus faciles pour le traitement, le stockage et la transmission des images numériques. Cependant elle a aussi engendré des moyens de falsification, de contrefaçons et d'espionnage très avancés. Le risque est encore plus grand dans un environnement ouvert tel que la transmission des images satellitaires au sol qui soulève un nombre important de problèmes. Nous citons, par exemple la confidentialité, l'authentification et l'intégrité des données :

• Toute information circulant peut être capturée et lue "sniffing", la confidentialité de base sur les concepts qui permettent de s'assurer que l'information ne puisse pas être lue par des personnes non autorisées. La confidentialité est fortement liée à la cryptographie.
• Une personne peut falsifier ses informations numériques personnelles "spoofing", l'authentification est l'ensemble des moyens qui permettent d'assurer que les données reçues et envoyées proviennent bien des entités déclarées.

• Les données peuvent être capturées et modifiées, l'intégrité des données concerne les techniques qui rendent possible la vérification de la non-altération des données, c'est-à-dire le contrôle du contenu.

Dans ces circonstances, il est devenu nécessaire de crypter ces images avant de les transmettre. Pour fournir une meilleure solution aux problèmes de sécurité d'image satellitaire, un certain nombre de techniques pour sécurisé l'image ont été proposées telles que les techniques basées sur algorithme RSA pour assurer l'authentification et les échanges sécurisés des clés, car il très sûre avec l'utilisation de clef de chiffrement élevée, le cryptosystème inclut aussi une procédure basée sur le tatouage numérique (Digital Watermarking) qui apparaît comme étant une alternative pouvant s'avérer efficace et complémentaire pour aider à établir une sécurité supplémentaire, à assurer un accès autorisé, à faciliter l'authentification du contenu ou empêcher la reproduction illégale.

Le travail présenté dans ce mémoire se situe dans le cadre des approches qui proposent l'usage de crypto-système asymétrique (algorithme de chiffrement et de déchiffrement) basé sur RSA pour sécuriser des régions de l'image satellitaire. Ainsi il est organisé comme suit :

- Le premier chapitre contient des notions importantes concernant les images satellitaires notamment : un peu d'historique sur les satellites et ses différents types du système.
- Le deuxième chapitre est un exposé général de la cryptographie, dans lequel on analyse ses techniques et son principe.
- Le troisième chapitre est une présentation théorique d'algorithme de chiffrement asymétrique RSA et le tatouage numérique.

- Dans le dernier chapitre sera consacré pour l'algorithme de chiffrement et de déchiffrement des images satellitaires en utilisant une méthode de chiffrement RSA et un tatouage numérique avec une explication détaillée, leur sécurité et leur performance sont analysées et évaluées.
- Enfin, la conclusion présente le bilan du travail réalisé et les perspectives envisagées.

Liste des figures

Chapitre I

Chapitre II

Chapitre III

Chapitre IV

Liste des tableaux

Chapitre I

Liste des abréviations

SPN : Substitution-permutation network

DES : Data Encryption Standard

AES : Advanced Encryption Standard

ADN : Acide désoxyribonucléique

OTP : One-Time-Pad

DES: Data Encryption Standard.

AES : Advanced Encryption Standard.

IDEA: International Data Encryption Algorithm.

AVC: Advanced Video Coding.

OTP : One-Time-Pad

JPEG : Joint Photographic Expert Group

OFB : Output Feedback

RSA : Rivest-Shamir-Adleman

NASA : National Aeronautics and Space Administration

USGS : United States Geological Survey

TIROS : Television Infrared Observation Satellite

ESSA : Environmental Science Services Administration

ITOS : Improved TIROS Operational Satellite

UHF : Ultra High Frequency

GSM : Global System for Mobile Communications

QKD : Quantum Key Distribution

I.Introduction

De tout temps, l'homme a cherché à se situer dans l'espace, à connaître et à comprendre l'univers qui l'entoure, à explorer le territoire qui s'offre à lui. Il a cartographié toute la surface du globe mais cela ne lui a pas suffit. Les dernières avances technologiques lui ont permit d'envoyer des outils dans l'espaces et ainsi d'obtenir des images satellites de la Terre et de l'Univers [1].

II.Images satellitaires

L'image satellitaire est une image numérique, c'est-à-dire un assemblage de pixels, ou surfaces élémentaires, référencés en ligne et colonnes formant un maillage régulier de la surface totale balayée par le capteur. Chaque pixel contient une somme d'informations codées par les valeurs des comptes radiométriques et les coordonnées en pixels [2].

Les images satellitaires sont le produit d'une technologie qui utilise le rayonnement réfléchir ou émis par un objet dans des intervalles de longueurs d'ondes données.
Ce rayonnement est enregistré par un capteur (caméra ou scanneur) installé à bord d'un satellite.
L'information est transmise à une station de réception terrestre, stockée puis traitée pour réaliser une image satellitaire [3].

III.Télédétection

La télédétection désigne, dans son acception la plus large, la mesure ou l'acquisition d'informations sur un objet ou un phénomène sans que le capteur soit en contact avec l'objet ou le phénomène étudié. La télédétection est une technique qui permet, d'observer et d'enregistrer le rayonnement électromagnétique, émis ou réfléchi, à traiter et à analyser l'information, pour ensuite mettre en application cette information [4].
Toutefois, en pratique, il est surtout utilisé pour les applications spatiales et aéroportées, et concerne essentiellement les techniques mises en œuvre pour l'observation de la surface de la Terre. Ces systèmes nécessitent l'utilisation de capteurs qui sont embarqués sur des ballons, des avions, des navettes ou des satellites [5].
Il existe essentiellement deux formes de télédétection :
La télédétection active : elle utilise des capteurs actifs qui sont à la fois émetteurs et récepteurs (les radars, les lasers etc.)
La télédétection passive : elle utilise des capteurs passifs qui sont uniquement des récepteurs (radiomètres, caméras, etc.), la source d'énergie est le plus souvent le soleil.
De manière plus détaillée, on peut schématiser la télédétection comme un ensemble de 6 étapes clés : [4]

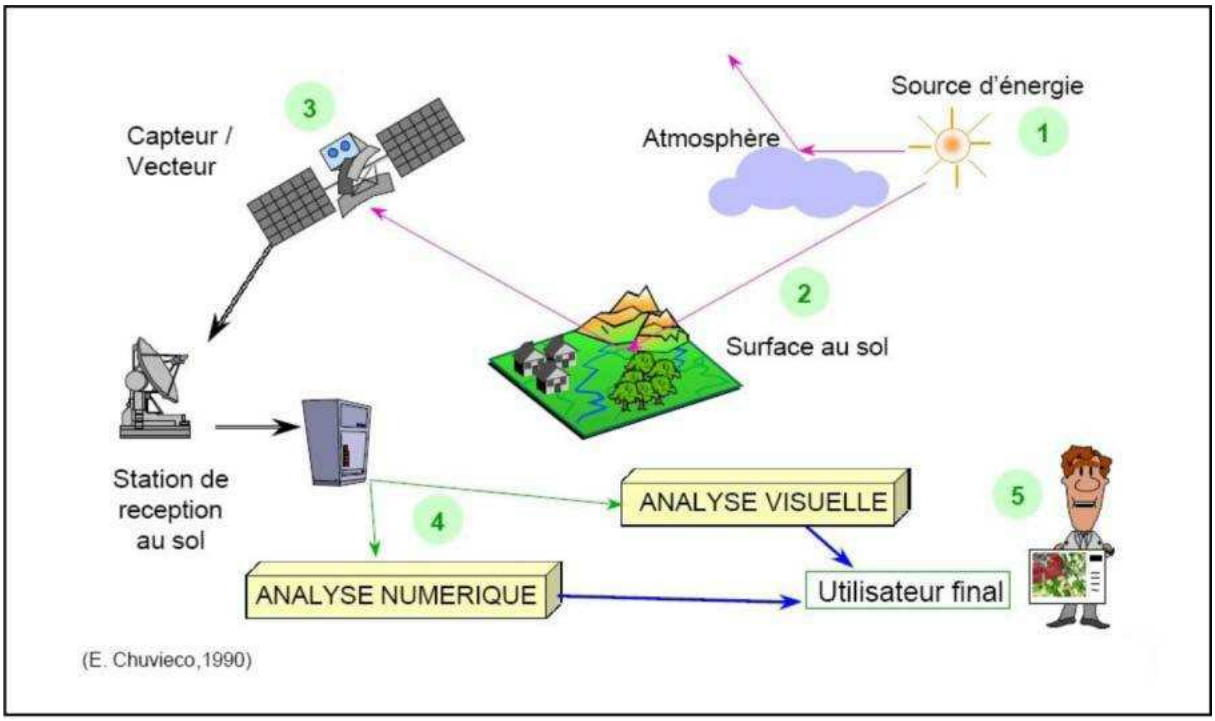


Fig.I.01. Le système de télédétection

A.Source d'énergie ou d'illumination À l'origine de la majorité des processus de télédétection se trouve une source d'énergie (1) pour illuminer la cible.

B.Rayonnement et atmosphère : Durant son parcours entre la source d'énergie et la cible, le rayonnement interagit avec l'atmosphère. Une seconde interaction se produit lors du trajet entre la cible et le capteur.

C.Interaction avec la cible: Une fois parvenue à la cible (2), l'énergie interagit avec la surface de celle-ci. La nature de cette interaction dépend des propriétés de réflexion, d'absorption et de transmission des éléments présents à la surface (particules des sols, organes de la végétation, cristaux de neige, molécule d'eau...), ainsi que de leurs agencements (densité, structure et géométrie).

D.Enregistrement de l'énergie par le capteur : Une fois l'énergie diffusée ou émise par la cible, elle doit être captée à distance (par un capteur (3) qui n'est pas en contact avec la cible) pour être enfin enregistrée sous format numérique.

E.Transmission, réception et traitement: L'énergie enregistrée par le capteur est transmise, souvent par des moyens électroniques, à une station de réception où l'information est transformée en images (numériques ou photographiques).

F.Interprétation, analyse et application: L'image traitée est par la suite analysée (4) et interprétée (5) (interprétation visuelle et/ou numérique) pour extraire l'information que l'on désire obtenir sur la cible afin de mieux la comprendre, d'en découvrir de nouveaux aspects ou pour aider à résoudre un problème particulier [6].

III.1. Historique de la télédétection:

Au début des années 60 les États-Unis ont commencé à placer des télédétecteurs dans l'espace pour l'observation de la météo et plus tard pour des observations de la terre. TIROS (Television Infrared Observation Satellite) était le premier satellite météorologique. Une longue série de satellites météorologiques a suivi celui-ci. 1960 était également le commencement d'un projet militaire de reconnaissance d'image appelé Corona. En 1970 le programme TIROS a été renommé NOAA (National Oceanic and Atmospheric Administration). Jusqu'à aujourd'hui le NOAA AVHRR (Very High Resolution Radiometer) collecte des informations sur la météo en longueur d'ondes visibles, proche infrarouges et thermiques. NOAA-17 a été lancé le 24 juin 2002. Les années 50 et les années 60 étaient également importantes pour le développement organisationnel de la télédétection.
Au début des années 70 le premier satellite spécifiquement conçu pour rassembler des données de la surface terrestre et ses ressources a été développé et lancé : ERTS-1 Earth Resources Technology Satellite-One. Plus tard, en 1975, ce programme a été renommé Landsat. Ce premier satellite de ressources terrestres était en fait un satellite de météo modifié (Nimbus) portant deux types de détecteurs (MSS, RBV) [7].
Dans les années 90, on assiste ainsi à la multiplication des satellites équipés de capteurs actifs, radars en particulier. Dans le domaine du rayonnement visible et infrarouge, les capteurs à très haute résolution spectrale sont aujourd'hui d'utilisation courante dans leur version aéroportée et font leur apparition à bord de satellites.
Les images de télédétection destinées à l'observation fine de la surface terrestre, y compris les photographies aériennes traditionnelles, sont, sous forme numérique, intégrées aux Systèmes d'Information Géographique [8].

III.2. Satellite de télédétection

Un satellite de télédétection est un satellite artificiel qui effectue des observations à distance par réception d'ondes électromagnétiques à l'aide de capteurs passifs ou actifs.
La télédétection par satellite est principalement utilisée en météorologie, climatologie, cartographie, militaires et beaucoup d'autres applications [9].
Parmi ces systèmes de satellite il existe NOAA AVHRR, le module de balayage multi spectral (MSS) et TM (thematique mapper) de LANDSAT, SPOT (satellite pour l'observation de la terre), et le RADAR (Radio Detection and Ranging).

III.2.1. NOAA

Les satellites NOAA (National Oceanic and Atmospheric Administration) ont été fut créent par la NASA pour fournir à United States National Weather Service.
Ces satellites permettent le suivi, à l'échelle globale, de l'étendue des glaces et surfaces enneigées, des températures de surface de l'eau, des profils verticaux de températures atmosphériques et d'humidité.
Les satellites NOAA fonctionnent en binômes sur des orbites polaires opposées, de manière à assurer une couverture totale de la Terre mise à jour au moins toutes les 6 heures. En effet, une même région est survolée 4 fois par jour, en matinée et en soirée par le satellite de numéro pair, de nuit et en début d'après-midi pour le satellite de numéro impair.
En 50 ans, cinq générations de satellites se sont succédées: TIROS (10 satellites), ESSA (9 satellites), ITOS (8 satellites), TIROS-N (3 satellites) et ATN (Advanced TIROS-N, 13 satellites à ce jour).
À bord des satellites NOAA se trouve le Capteur AVHRR (Advanced Very High Resolution Radiometer). Le radiomètre à balayage AVHRR est caractérisé par un champ d'observation

très large. Sa fauchée est de 2940 km et sa résolution de 1 km dans l'IR et 0,5 km dans le visible. L'instrument livre 2 fois par jour des images de nuages du monde entier et offre également des images fréquentes des surfaces des mers et des terres. L'instrument est particulièrement bien adapté pour l'étude de la végétation à l'échelle mondiale.
Le programme POES (Polar Operational Environmental Satellite) regroupe les 2 dernières séries. Actuellement, 5 satellites NOAA sont opérationnels, le dernier de la série, NOAA-19, ayant été lancé en février 2009.

Tableau. I.01. Bandes de NOAA AVHRR

Bande	Largeur de bande	Résolution spatiale	Applications
1 (visible)	0,58 - 0,68 µm	1,1 Km	Cartographie de jour des zones nuageuse et de la surface terrestre
2 (proche IR)	0,725 - 1,00 µm	1,1 Km	Cartographie de jour des zones nuageuse et de la surface terrestre
3A (proche IR)	1,580 - 1,64 µm	1,1 Km	Détection neige et glace
3B (IR)	3,550 - 3,93 µm	1,1 Km	Cartographie de nuit des zones nuageuse et température de surface de la mer
4 (IR)	10,30 - 11,30 µm	1,1 Km	Cartographie de nuit des zones nuageuse et température de surface de la mer
5 (IR)	11,50 - 12,50 µm	1,1 Km	Température de surface de la mer

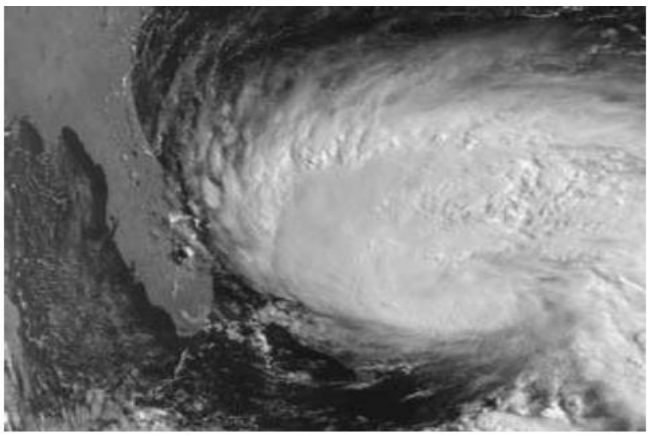


Fig. I.02. Image capturée par NOAA AVHRR [10].

III.2.2. Landsat

Ce programme américain de télédétection spatiale (NASA et USGS) a été le premier programme civil d'observation de la Terre par satellite. Il a commencé avec le lancement du premier LANDSAT en 1972 et se poursuit encore actuellement avec Landsat 7 qui marque une nouvelle orientation dans le programme, afin de réduire le coût des données et d'augmenter la couverture globale de la Terre, ceci dans la perspective de recherches concernant le changement global. Ce programme a donc permis d'engranger des millions de données formant une librairie exceptionnelle des conditions sur Terre depuis presque 40 ans.

Depuis janvier 2009, l'entièreté des images d'archive Landsat est accessible gratuitement via Internet.

a) LANDSAT 1ère série

Les satellites Landsat 1,2 et 3 furent identiques et leur charge utile était constituée de deux instruments optiques, un capteur multispectral (Multi Spectral Scanner - MSS) et une série de cameras vidéo (Return Beam Vidicom - RBV). Ils évoluent à une altitude moyenne de 910 km, sur des orbites polaire héliosynchrone caractérisées par une inclinaison de 99,2°. Tour de la Terre leur prend 103 min et un cycle orbital complet de 18 jours.

Les 3 premiers satellites furent identiques et leur charge utile était constituée de deux instruments optiques, un capteur multispectral (Multi Spectral Scanner - MSS) et une série de cameras vidéo (Return Beam Vidicom - RBV).

- **Capteurs RBV**

Sur les deux premiers satellites, la série de 3 caméras vidéo prenait des images dans le visible et dans l'infrarouge. La résolution était de 80 m pour des images de 185 km sur 185 km. Sur LANDSAT 3, la résolution a été portée à 40 m, mais les caméras ne prenaient plus des images que dans une seule bande spectrale panchromatique (0,5 - 0,75 μm).

- **Capteurs MSS**

Ces scanners mécaniques enregistraient des informations dans quatre bandes spectrales et sur une zone de 185 km sur 185 km. Comme ces instruments ont été développés après les trois caméras RBV, ces bandes ont été numérotées de 4 à 7. Le capteur MSS de LANDSAT 3 comportait une bande spectrale supplémentaire dans l'infrarouge thermique.

- **LANDSAT 2ème série**

Les satellites Landsat 4 et 5 évoluent à une altitude moyenne de 705 km, sur des orbites circulaires quasi polaires caractérisées par une inclinaison de 98,2° (ce qui permet l'héliosynchronisme). Un tour de la Terre leur prend 98,9 min, si bien qu'ils décrivent 14,5 révolutions par jour. Un cycle orbital complet dure 16 jours.

Les 2 satellites de cette série ont été équipés de 2 capteurs multispectraux (Multi Spectral Scanner - MSS et Thematic Mapper - TM).

Capteurs MSS

Ces scanners étaient identiques à ceux des 2 premiers satellites LANDSAT. La seule différence était que les 4 bandes spectrales ont été numérotées de 1 à 4, suite à l'abandon des caméras RBV. L'acquisition de données par le capteur MSS de LANDSAT 5 a été arrêtée en 1992.

Capteurs TM

Ces scanners à haute résolution possèdent 7 bandes spectrales et couvrent toujours une zone de 185 km sur 185 km.

- **LANDSAT 3ème série**

La dernière génération des satellites LANDSAT a commencé par un échec. LANDSAT 6 a été perdu juste après son lancement le 3 octobre 1993. LANDSAT 7 a été lancé en 1999 et est équipé d'un capteur multispectral (Enhanced Thematic Mapper Plus - ETM+).

Cette série des satellites a les même **Caractéristiques orbitales que celles de la série 2.**

Capteur ETM+

Ce scanner est une évolution des TM précédents. Il comporte maintenant une large bande panchromatique à haute résolution [11].

Tableau. I .02. Les satellites Landsat [12].

Satellite	Date de lancement	Altitude moyenne	Cycle orbital	Fauchée	Capteurs, Canaux et résolution spatiale
Landsat 1	Juillet 1972	910 Km	18 jours	185 Km	Caméra RBV (3 canaux, 80 m) Radiomètre MSS (4 canaux, 80 m)
Landsat 2	Janvier 1975	910 Km	18 jours	185 Km	Caméra RBV (3 canaux, 80 m) Radiomètre MSS (4 canaux, 80 m)
Landsat 3	Mars 1978	910 Km	18 jours	185 Km	Caméra RBV (3 canaux, 80 m) Radiomètre MSS (5 canaux, 80 m)
Landsat 4	Juillet 1982	705 Km	16 jours	185 Km	Radiomètre MSS (5 canaux, 80 m) Radiomètre TM (7 canaux, 30 m)
Landsat 5	Janvier 1984	705 Km	16 jours	185 Km	Radiomètre MSS (5 canaux, 80 m) Radiomètre TM (7 canaux, 30 m)
Landsat 6	Octobre 1993	détruit après lancement			
Landsat 7	Avril 1999	705 Km	16 jours	185 Km	Radiomètre ETM + (7 canaux, 30 m), plus canal panchro, 15 m

IV.2.2. SPOT

Le programme de télédétection SPOT (Satellites Pour l'Observation de la Terre) a été mis en place en 1978 par la France, en collaboration avec la Belgique et la Suède.
Depuis 1986, la constellation des satellites Spot fournit des images optiques alliant haute résolution et large champ. Elle offre une capacité d'acquisition qui permet d'obtenir une image de n'importe quel point du globe chaque jour [13].
Tous les satellites SPOT évoluent à une altitude de 820 km, sur des orbites quasi polaires, caractérisées par une inclinaison de 98,7° (ce qui permet l'héliosynchronisme). La période de révolution des satellites SPOT est de 101, 4 min et le cycle orbital a une durée de 26 jours.
L'instrumentation embarquée a évolué au fil des satellites, avec pour objectif majeur d'obtenir de l'imagerie haute résolution de plus en plus performante. Tous les satellites SPOT sont équipés de capteurs jumelés offrant, dans les domaines spectraux du visible et de l'infrarouge proche, une résolution spatiale de 5 à 20 m selon les satellites et selon le mode de fonctionnement.
Les satellites SPOT 4 et 55 avaient également à leur bord un outil d'observation globale "instrument végétation" qui opère dans 4 bandes spectrales et permet de couvrir chaque jour la quasi-totalité des terres émergées, avec une résolution spatiale de l'ordre du km. SPOT 5 dispose en plus d'un instrument destiné à l'imagerie stéréoscopique.
Depuis le début de l'année 2007, les images SPOT 5 ont pris un caractère "grand public" plus affirmé par leur contribution significative à l'amélioration des images offertes par l'outil Google Earth.

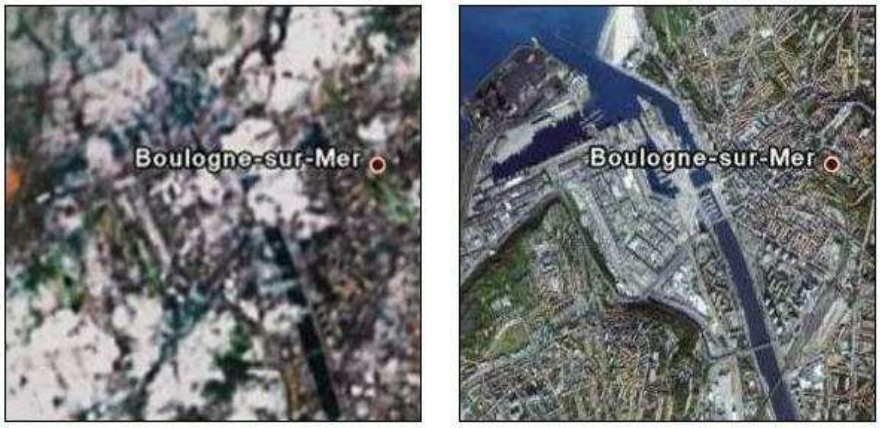


Fig. I.03. Amélioration de la visualisation de la ville de Boulogne sur Mer, sur Google Earth, grâce à l'imagerie SPOT 5, ainsi qu'on peut le voir ci-dessus sur l'image de droite [14].

V.2.2. Radar

Le Radar (RAdio Detection And Ranging), c'est un dispositif d'émission réception d'onde électromagnétique permettant de détecter et de mesurer la distance qui le sépare par rapport à un objet localisé dans l'air, sur terre ou sur mer.
Le Radar génère une onde électromagnétique qui se propage dans l'espace. Lorsque cette onde heurte un objet, elle va se disperser. Une partie de l'onde réfléchie va être reçue par le récepteur du radar.
Connaissant la vitesse de propagation des ondes radio dans l'espace et le temps écoulé entre le moment de l'émission et celui de la réception de l'onde, on peut calculer la distance Radar-Objet volant. Le traitement du signal reçu par le Radar peut fournir d'autres informations pour identifier par exemple la cible détectée.
Un radar est caractérisé par sa plage de fréquence. La bande UHF (300 à 3000Hz) est utilisée par les Radars à longue portée. La bande S (2 à 4 GHz) est très utilisée pour le contrôle aérien. Puisque le RADAR a sa propre source d'énergie, nous pouvons obtenir des images le jour ou la nuit [15].

Fig. I.04. Image de port city de Barcelone captée par RADARSAT-2 [16].

IV.Conclusion

Dans ce chapitre nous avons présenté quelques notions importantes concernant les images satellitaires.
Avec le développement rapide des technologies et des applications spatiales, plusieurs images satellitaires sont prises.
Le chapitre suivant sera consacré à l'analyse de la sécurité par la cryptographie.

I.Introduction

Dans ce chapitre, nous énumérons certaines définitions importantes, termes et terminologies qui faciliteront la compréhension des concepts et des objectifs des travaux de recherche développés dans les sections suivantes.

La cryptographie a évolué en trois périodes historiques :

- **La cryptographie mécanique :** Il s'agit de la cryptographie qui utilise des moyens mécaniques pour chiffrer un message. Cette cryptographie s'étend de l'antiquité jusqu'à la fin de la seconde guerre mondiale environ. De nos jours, elle n'a plus cours.

- **La cryptographie mathématique** : Il s'agit de la cryptographie qui utilise les mathématiques pour chiffrer un message. Cette cryptographie a commencé aux environs de la fin de la deuxième guerre mondiale et c'est celle que l'on utilise de nos jours.

- **La cryptographie quantique :** Il s'agit de la cryptographie dont les bases reposent sur la physique quantique. Nous sommes en train de la voir émerger de nos jours et nul doute qu'elle ne remplace dans les années qui viennent la cryptographie basée sur les mathématiques [17].

II.Terminologie

Dans cette présentation, on va utiliser toujours les mêmes termes. Ce paragraphe présente les termes utilisés ainsi que leur signification.

- Texte en clair : c'est le message à protéger.
- Texte chiffré : c'est le résultat du chiffrement du texte en clair.
- Chiffrement : c'est la méthode ou l'algorithme utilisé pour transformer un texte en clair en texte chiffré.
- Déchiffrement c'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair.
- Clé : c'est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré et pour déchiffrer le texte chiffré en texte en clair. On peut parfaitement concevoir un algorithme qui n'utilise pas de clé, dans ce cas c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé.
- Cryptographie : cette branche regroupe l'ensemble des méthodes qui permettent de chiffrer et de déchiffrer un texte en clair afin de le rendre incompréhensible pour quiconque n'est pas en possession de la clé à utiliser pour le déchiffrer.
- Cryptanalyse : c'est l'art de révéler les textes en clair qui ont fait l'objet d'un chiffrement sans connaître la clé utilisée pour chiffrer le texte en clair.

- Cryptologie : il s'agit de la science qui étudie les communications secrètes. Elle est composée de deux domaines d'étude complémentaires : la cryptographie et la cryptanalyse.
- Décrypter : c'est l'action de retrouver le texte en clair correspondant à un texte chiffré sans posséder la clé qui a servit au chiffrement. Ce mot ne devrait donc être employé que dans le contexte de la cryptanalyse.
- Crypter : en relisant la définition du mot décrypter, on peut se rendre compte que le mot crypter n'a pas de sens et que son usage devrait être oublié. Le mot cryptage n'a pas plus de sens non plus.
- Coder, décoder : c'est une méthode ou un algorithme permettant de modifier la mise en forme d'un message sans introduire d'élément secret. Le Morse est donc un code puisqu'il transforme des lettres en trait et points sans notion de secret. L'ASCII est lui aussi un code puisqu'il permet de transformer une lettre en valeur binaire [17].

III.Définition de la cryptographie

La cryptographie est l'étude des différentes méthodes et techniques mathématiques reliées aux aspects de sécurité de l'information, pour assurer le secret et l'authenticité des messages, elle permet de stocker des informations sensibles ou de les transmettre à travers des réseaux non sûrs (comme Internet) de telle sorte qu'elles ne peuvent être lues par personne à l'exception du destinataire convenu. Elle concerne la transformation d'un message (texte, image, chiffres) intelligible vers un message codé, incompréhensible à tous sauf pour les détenteurs d'un code de déchiffrement [18].

III.1.Principe de la cryptographie

On pourrait croire que pour communiquer des informations confidentielles il suffit d'établir un code secret qui ne soit connu que des interlocuteurs légitimes mais ce n'est cependant pas aisé et nous conduisons à s'observé les fameux principes de Kerckhoffs dans son article « La cryptographie militaire » 1883, qui exprime que la méthode de chiffrement utilisée doit « puisse sans inconvénient tomber entre les mains de l'ennemi » et que « la sécurité d'un chiffrement ne doit pas reposer sur la confidentialité de celui-ci mais uniquement sur la protection de clé [19].

Le chiffrement permet l'échange sûr des renseignements privés et confidentiel. Un texte compréhensible est converti en texte inintelligible.

Le déchiffrement est l'opération inverse du chiffrement, en vue de sa transmission d'un poste de travail à un autre. Sur le poste récepteur, le texte chiffré est reconverti en format intelligible [20].

Les données lisibles et compréhensibles sans intervention spécifique sont considérées comme du texte en clair. La méthode permettant de dissimuler du texte en clair en masquant son contenu est appelée le cryptage.

Cette opération permet de s'assurer que seules les personnes auxquelles les informations sont destinées pourront y accéder. Le processus inverse de transformation du texte chiffré vers le texte d'origine est appelé le décryptage [21].

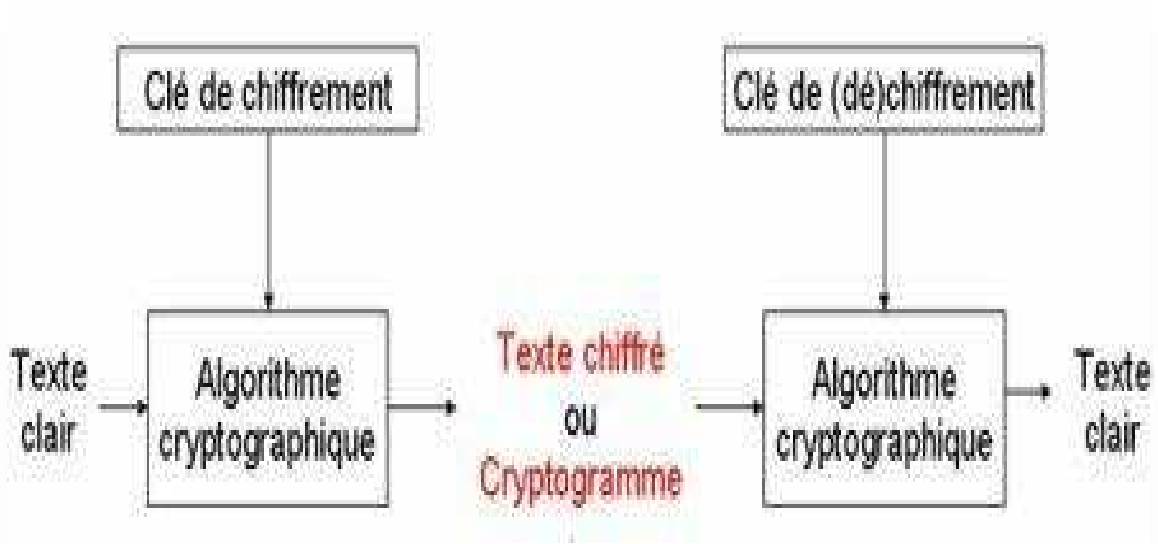


Fig. II.01. Chiffrement et déchiffrement

III.2. Objectif de la cryptographie

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité [22].

Les objectifs fondamentaux de la cryptographie sont :

- **La confidentialité:** Elle consiste à garder des données secrètes pour tous ceux qui ne sont pas autorisés à les connaître.
- **L'intégrité des données:** a pour but de préserver les données de toute altération non autorisée.
- **L'authentification des données:** Consiste à faire le lien entre les données et leur expéditeur. L'authentification des entités consiste à s'assurer de leur identité ou de leur qualité.

- **La non répudiation:** Consiste à éviter que, par la suite, les communicants nient leurs actions: l'émetteur nie avoir envoyé un message et le récepteur nie avoir reçu un message [23].

IV.Evolution de la cryptographie

IV.1. Cryptographie classique

Cette partie traite quelques cryptosystèmes célèbres, avant l'ère des ordinateurs qui ont été les bases pour l'évolution de plusieurs algorithmes de cryptographie utilisés actuellement. Les cryptosystèmes classiques sont regroupés en chiffrement monoalphabétique et polyalphabétique [24].

Après plusieurs siècles d'utilisation de cryptages, on peut citer ces fameuses techniques :

A. La technique du rouleau assyrien

C'est une méthode de chiffrement grecque A Sparte, au IV ème siècle avant notre ère, un bâton d'un diamètre fixé sur lequel on enroule une lanière en cuir et sur la quelle était écrit le texte en clair Ensuite pouvait être envoyée (sans le bâton) au destinataire du message.
les communications entre les chefs des armées et les commandants étaient chiffrées à l'aide d'une Scytale.

Fig. II.02. Scytale grecque [25]

B. Système de César (par décalage)

Le chiffre de César est la méthode de cryptographie la plus ancienne communément admise par l'histoire. César utilisait ce code simple pour transmettre via un message des consignes à ces généraux d'armées sans qu'il puisse être exploité par un quelconque ennemi dans le cas ou le message serait intercepté. Il consiste en une substitution mono-alphabétique : chaque lettre est remplacée ("substitution") par une seule autre ("mono-alphabétique"), selon un certain décalage dans l'alphabet ou de façon arbitraire. D'après Suétone, César avait coutume

d'utiliser un décalage de 3 lettres : A devient D, B devient E, C devient F, etc. Il écrivait donc son message normalement, puis remplaçait chaque lettre par celle qui lui correspondait : [24]

Clair	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
Chiffré	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

Fig. II.03. Table de chiffre de césar.

C.Procédé de Vigenère

Il consiste à changer l'alphabet de substitution à chaque chiffrement d'une lettre, ce qui fait que l'on ne peut tenter de décrypter le message en utilisant la fréquence des lettres. Pour cela, on construit un carré constitué de tous les alphabets décalés d'une lettre.

Ce système utilise la notion de substitution polyalphabétique. Le modèle de Shannon pour ce système est :

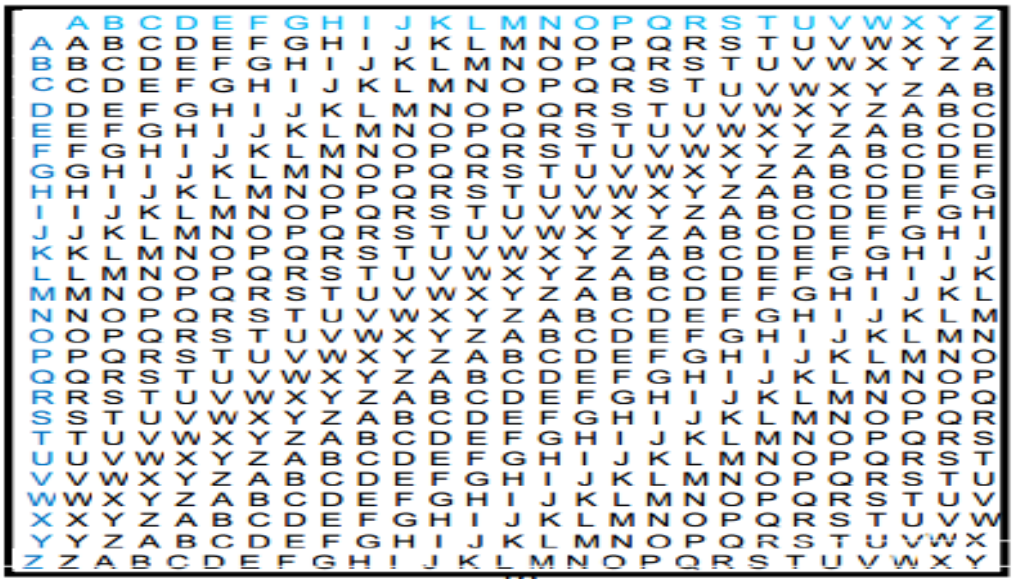
- Pour l'alphabet français : Z 26
- espace des messages : $M = (Z\ 26)\ n$ –
- espace des cryptogrammes : $C = (Z\ 26)\ n.$
- espaces des clefs : $K = (Z\ m)\ r$ (I.12).

Un message $M = [X\ 1, X\ 2, ... X\ n]$ est t crypté par la clef $k = [k1, ..., kr] \in K.$

Le cryptogramme $C = [Y1, Y2, ..., Yn].$

Pratiquement le cryptage est réalisé en utilisant le tableau représenté sur la figure. Pour le texte clair, on écrit immédiatement au dessous la clef, autant de fois que nécessaire par périodicité. Le cryptage de la i^{eme} lettre se fait en repérant l'intersection de la colonne de la

table, correspondante à la lettre du texte claire et de la ligne de la table, correspondante à la lettre de la clef.



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

Fig. II.04. Table du chiffre de Vigenère

D. La machine Enigma

Durant la Seconde Guerre Mondiale, les communications devaient rester secrètes. Pour cela, les Allemands avaient inventé une machine automatisant le cryptage par des procédés mécaniques.
Le cryptage repose ici sur cinq éléments :

- Un tableau de connexions,
- Trois rotors,
- Un réflecteur.

Le tableau de connexions attribue à chaque lettre de l'alphabet une autre lettre de l'alphabet.

Les rotors établissent des connexions entre différentes lettres de l'alphabet et effectue des rotations (d'où le problème du décryptage si on ne connaît pas leur position d'origine). En effet, dès qu'une lettre a été codée, le premier rotor tourne d'un cran; le second rotor tourne d'un cran chaque fois que le premier a fait un tour et le troisième rotor avance d'un cran quand le deuxième a fait un tour.

Le réflecteur, quant à lui effectue des permutations entre les lettres et renvoie la lettre à coder une nouvelle fois à travers les 3 rotors.

Le principe de base des machines Enigma conçues par Scherbius repose sur l'utilisation de rotors qui transforment l'alphabet clair (noté en minuscules) en alphabet chiffré (en majuscules).

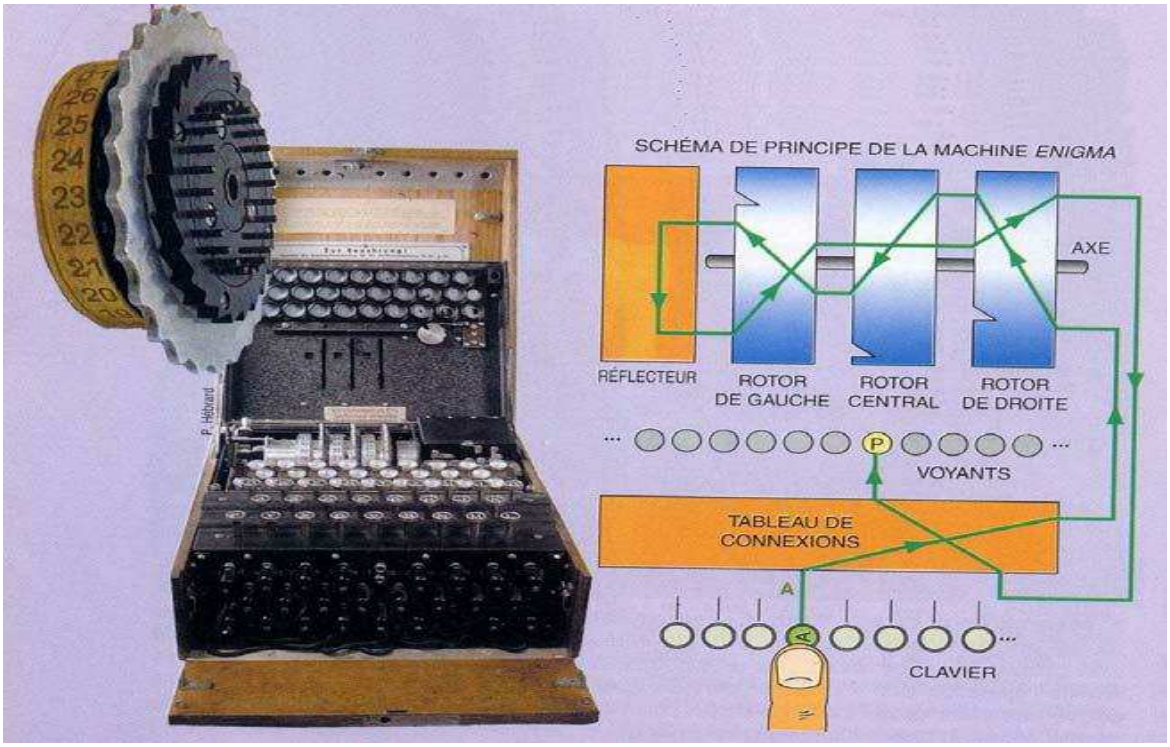


Fig. II.05. La machine d'enigma [8]

IV.2. Cryptographie actuelle

De nos jours pratiquement, la cryptographie est englobée par deux grands algorithmes de chiffrement. On distingue les algorithmes à clef secrète et les algorithmes à clef publique. La sécurité de ces systèmes est calculatoire. Ainsi leur puissance réside dans l'incapacité des calculateurs à les casser dans un temps humainement raisonnable [26].

IV.2.1. Cryptographie symétrique

Le principe du chiffrement dans le cadre de la cryptographie symétrique est d'utiliser la même clé pour chiffrer et pour déchiffrer, Cette clé doit donc rester secrète ce qui amène aussi à parler de cryptographie à clé secrète .En d'autres termes, ici, le secret réside dans la méthode utilisée. Il suffit donc de connaître la clé ou l'algorithme de cryptage pour découvrir le message. Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé [27]. Les cryptosystèmes symétriques les plus utilisés pratiquement sont le DES et le AES.

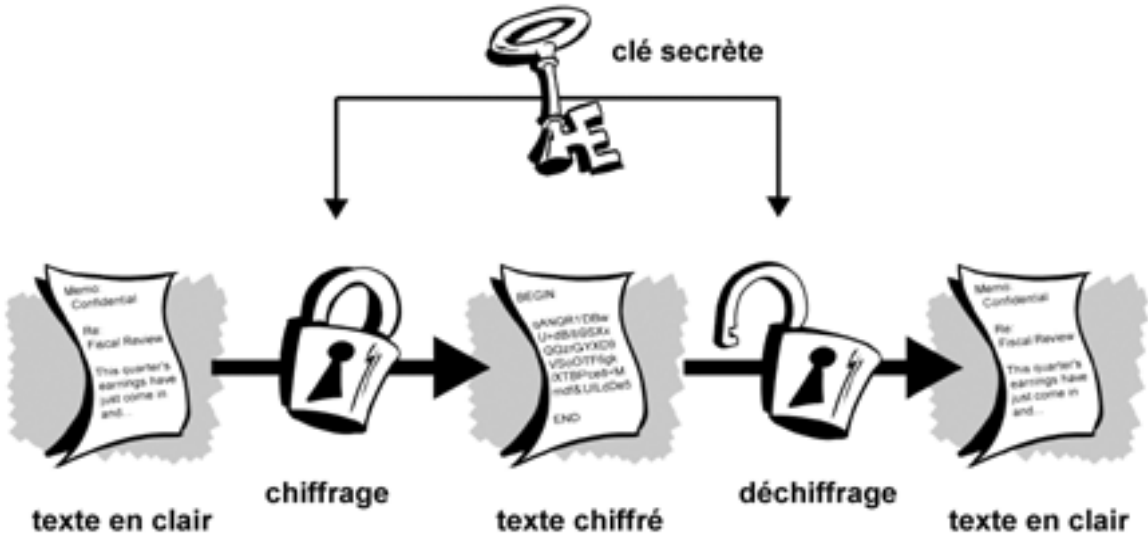


Fig. II.06. Schéma de principe d'un cryptosystème symétrique.

L'avantage principal de ce mode de chiffrement est sa rapidité.

Le principal désavantage réside dans la distribution des clés : pour une meilleure sécurité, on préfèrera l'échange manuel. Malheureusement, pour de grands systèmes, le nombre de clés peut devenir conséquent. C'est pourquoi on utilisera souvent des échanges sécurisés pour transmettre les clés. En effet, pour un système à N utilisateurs, il y aura N. (N − 1)/2 paires de clés [28].

On distingue deux types d'algorithmes, les algorithmes en blocs, qui prennent *n* bits en entrée

et en ressortent *n*, et les algorithmes à flots, qui chiffrent bit par bit sur le modèle du chiffre de Vernam [29].

1. Algorithmes de chiffrement par bloc

Dans un schéma de chiffrement par blocs, le message est divisé en blocs de bits, de longueur fixe. Les blocs sont chiffrés l'un après l'autre. Le chiffrement peut être effectué par substitution et par transposition.

- La substitution permet d'ajouter de la confusion, c'est-à-dire de rendre la relation entre le message et le texte chiffré aussi complexe que possible.
- La transposition permet d'ajouter de la diffusion, c'est-à-dire de réarranger les bits du message afin d'éviter que toute redondance dans le message ne se retrouve dans le texte chiffré.

On distingue le chiffrement par blocs itératifs. Une fonction constituée de combinaisons complexes de substitutions et/ou de transpositions, appelée fonction de tour ou fonction de ronde, est appliquée itérativement. Une itération est appelée un tour ou une ronde. Chaque

ronde prend en entrée la sortie de la ronde précédente et chiffre cette entrée à l'aide de la fonction de ronde et d'une sous-clé de ronde générée à partir de la clé secrète K. La fonction de chiffrement n'est pas la fonction de ronde, mais elle est constituée par l'ensemble de toutes les rondes.

2. Algorithmes de chiffrement par flot

Les schémas de chiffrement par flot et appelé aussi chiffrement en continu, traitent l'information bit à bit, et sont très rapides. Ils sont parfaitement adaptés à des moyens de calcul et de mémoire (cryptographie en temps réel) comme la cryptographie militaire, ou la cryptographie entre le téléphone portable GSM et son réseau.

Leur principe est d'effectuer un chiffrement de Vernam en utilisant une clé pseudo-aléatoire, c'est à dire une clé qui ne soit pas choisie aléatoirement parmi tous les mots binaires de longueur *n*. Cette clé (qu'on appellera par la suite pseudo-aléatoire) est générée par différents procédés à partir d'une clé secrète d'une longueur juste suffisante pour résister.

- **Avantages et inconvénients du chiffrement par bloc et par flot**

Avec un algorithme de chiffrement par bloc, on ne peut commencer à chiffrer et à déchiffrer un message que si l'on connaît la totalité d'un bloc. Ceci occasionne naturellement un délai dans la transmission et nécessite également le stockage successif des blocs dans une mémoire tampon.

Au contraire, dans les procédés de chiffrement par flot, chaque bit transmis peut être chiffré ou déchiffré indépendamment des autres, en particulier sans qu'il soit nécessaire d'attendre les bits suivants.

D'autre part, les chiffrements par flot ne requièrent évidemment pas, c'est-à-dire l'ajout de certains bits au message clair dont le seul objectif est d'atteindre une longueur multiple de la taille du bloc. Ceci peut s'avérer particulièrement souhaitable dans les applications où la bande passante est très limitée ou quand le protocole employé impose la transmission de paquets relativement courts. Un autre avantage du chiffrement par flot est que contrairement aux chiffrements par bloc, le processus de déchiffrement ne propage pas les erreurs de transmission.

Supposons qu'une erreur survenue au cours de la communication ait affecté un bit du message chiffré :

Dans le cas d'un chiffrement à flot, cette erreur affecte uniquement le bit correspondant du texte clair, et ne le rend donc généralement pas complètement incompréhensible.

Par contre, dans le cas d'un chiffrement par bloc, c'est tout le bloc contenant la position erronée qui devient incorrect après déchiffrement. Ainsi, une erreur sur un seul bit lors de la transmission affecte en réalité 128 bits du message clair.

C'est pour cette raison que le chiffrement par flot est également utilisé pour protéger la confidentialité dans les transmissions bruitées [23].

IV.2.2. Cryptographie asymétrique

Le principe de kerckhoffs stipule que le procédé de chiffrement doit être supposé connu de l'adversaire. Il peut être poussé à l'extrême en supposant que la clef de chiffrement est également connue.

Dans le cas du chiffrement symétrique, le procédé ne peut plus assurer la sécurité requise car cette clef permet également de déchiffrer.

En revanche, rien n'impose que la clef de chiffrement permette également de déchiffrer. On peut donc imaginer des systèmes « asymétriques » où les deux clefs sont différentes et où la publication de la clef de chiffrement ne compromet pas la sécurité.

C'est ce que Diffie et Hellman on proposé en 1976. Bien qu'il semble que des services secrets aient connu de tels systèmes avant ces résultats [19].

Dans ces cryptosystèmes, chaque acteur de la communication sécurisée possède 2 clés distinctes (une privée, une publique) avec l'impossibilité de déduire la clé privée à partir de la clé publique qui est distribuée librement. Ce principe est illustré sur la figure (06).

Pour envoyer un message confidentiel à Bob, Alice chiffre le message clair à l'aide de la clé publique de Bob et lui, à l'aide de sa clé secrète, est le seul en mesure de déchiffrer le message reçu [26].

•Avantages et inconvénients du chiffrement à clé publique

L'atout principal de la cryptographie à clé publique réside dans la facilité de gestion du parc des clés des utilisateurs.
En effet, l'augmentation du nombre d'utilisateurs ne complexifie pas le protocole. De plus, l'arrivée de nouveaux utilisateurs et leur intégration demande très peu d'efforts et ne modifie en rien les paramètres des autres. Ainsi, la cryptographie à clé publique résout le problème de distribution des clés que l'on peut rencontrer dans la cryptographie à clé privée.
Toutefois, les techniques asymétriques souffrent de leur grande lenteur. Chiffrer un message est *100* à *1000* fois plus long que certaines techniques symétriques.

IV.2.3. Chiffrement en cryptographie quantiques

La cryptographie quantique, plus correctement nommée distribution quantique de clés, désigne un ensemble de protocoles permettant de distribuer une clé de chiffrement secrète entre deux interlocuteurs distants, tout en assurant la sécurité de la transmission de l'information. Cette clé secrète peut ensuite être utilisée dans un algorithme de chiffrement symétrique, afin de chiffrer et déchiffrer des données confidentielles.

La cryptographie quantique ne constitue donc pas en elle seule un système cryptographique mais en est un élément. Pour avoir un système cryptographique complet, il faudrait associer la QKD à un algorithme de chiffrement conventionnel tel qu'un masque jetable ou code de Vernam [23].

V.Conclusion

Dans ce chapitre, nous avons présenté plusieurs techniques et quelques théories de la cryptographie qui vont nous permettre de comprendre cet axe de recherche.

Nous avons évoqué les notions formelles de sécurité et leurs implications. Nous avons ensuite abordé les différents types de classifications des algorithmes de chiffrement et leurs contextes d'applications.

Nous avons aussi observé que les clefs ont un rôle important et le choix de leur longueur est cruciale pour rendre sûrs les cryptosystèmes.

Ce chapitre a introduit aussi, les principaux algorithmes de cryptage symétrique, asymétrique, par flot et par bloc, ainsi que la cryptographie quantique.

Nous détaillons dans le prochain chapitre l'algorithme standards RSA qui sera utilisé dans notre cryptosystème et avec un tatouage numérique visible. Il est important de comprendre le fonctionnement de cette algorithme pour adapter cet méthode de chiffrement à la sécurité des images satellite.

I.Introduction

Les travaux de recherche de ce chapitre s'inscrivent dans le cadre de la sécurité des images satellitaires, par l'algorithme de RSA. Cet algorithme est fondé sur l'utilisation d'une paire de clés composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles, et le tatouage d'image par image ça sera notre méthode à implémenter pour le tatouage visible, en effet qu'il y a d'autre méthode à citer comme le tatouage d'image par texte.

II.Algorithme asymétrique RSA

Le chiffrement RSA est un algorithme de cryptographie asymétrique, très utilisé et très efficace, fondé sur deux principes mathématiques fondamentaux: la difficulté de factoriser des grands nombres, et l'arithmétique de congruences. [31]

II.1. Vue historique

Le système de cryptage RSA a été inventé en 1977 par Ron Rivest, Adi Shamir et Len Adleman (dont les initiales forment RSA). Ces 3 auteurs avaient décidé de travailler ensemble pour établir qu'un nouveau système de codage révolutionnaire, dénommé «système à clef publique» que W.Diffie et M.hellman venaient d'inventer, était une impossibilité logique (autrement dit, que tout système de cryptage de cette nature présentait des failles). Ils ne réussirent pas dans leur projet, mais, au contraire, découvrirent un nouveau système à clef publique qui supplanta vite celui de W.Diffie et M.Hellman[30].

II.2. Cryptosystème à clé publique

Les algorithmes asymétriques sont basés sur une clef pour le chiffrement et une clef associée différente, pour le déchiffrement. Ces algorithmes ont la caractéristique importante suivante. Il est impossible de trouver la clef de déchiffrement malgré la connaissance de l'algorithme cryptographique et la clef de chiffrement.

II.3. L'algorithme RSA

Le premier système à clé publique solide à avoir été inventé, et le plus utilisé actuellement, est le système RSA. Le RSA est fondé dur deux principes mathématiques fondamentaux: la difficulté de factoriser des grands nombres, et l'arithmétique de congruences.

II.4. Principe de fonctionnement de l'algorithme RSA

Pour qu'Alice puisse échanger sa clé avec Bob, elle doit d'abord la calculer en mettant en œuvre des notions mathématiques remarquables par leur simplicité. L'algorithme RSA est ainsi défini par 03 phases:

- Génération des clés (effectué par la destinataire Alice)
- Chiffrement (effectué par l'expéditeur Bob)
- Déchiffrement (effectué par la destinataire Alice)

II.4.1. Génération des clés

Cette phase peut se résumer en 03 étapes:

1ére étape: Alice choisit au hasard deux grands nombres entiers, naturels, premiers, p et q, ont environ 100 chiffres chacun ou plus pour rendre la factorisation hors de la portée. Dans notre exemple simplifié elle choisit:

p = 31 et q = 53

Et fait leur produit:

n =p*q = 1643

2ème étape: Alice détermine la fonction d'Euler associée à n déjà calculé en utilisant la formule:

$\phi(n)= (p-1)*(q-1)$

$\phi(n)=30*52=1560$

Une fois que la fonction d'Euler déterminée, Alice choisie au hasard sa clé publique « e », cette clé est un nombre premier compris entre 1 et $\phi(n)$ et premier relativement à $\phi(n)$ c'est-à-dire le PGCD (e, $\phi(n)$)=1. Alice fait: e=11

D'où le couple (e, n) constitue la clé publique.

$$\begin{cases} \text{n: c'est le module} \\ \text{e: c'est l'exposant} \end{cases}$$

La clé publique est donc (11, 1643).

3ème étape: Cette dernière étape consiste à trouver la clé privée "d" qui correspond à la clé publique choisie précédemment avec d compris entre 1 et $\phi(n)$, pour se faire, il faut résoudre l'équation suivante:

e.dmod $\phi(n)=1$

c.à.d: $e.d \equiv 1 [\phi(n)]$

Donc: $e.d= K \phi(n) +1$

Selon notre exemple on aura:

$e.d= K \phi(n) +1$

11. d= k.1560+1

Pour k=6 on aura: 11.d= k.1560+1 on aura d= 851

Le couple (d, n) constitue la clé privée

La clé privée est dons (851, 1643)

$$\begin{cases} \text{n: c'est le module} \\ \text{d : c'est l'exposant} \end{cases}$$

En fin, Alice et Bob disposent toutes les clés indispensables au chiffrement et au déchiffrement des messages après la transmission ou la publication de sa clé publique (e, n).

Maintenant, il faut qu'elle conserve sa clé privée (d, n) et qu'elle n'oublie jamais les nombres p et q.

II.4.2. Chiffrement

Bob veut donc transmettre le message M « ANEMONE » à Alice. Il cherche dans l'annuaire la clé de chiffrement qu'Alice a déjà publiée. Il sait maintenant qu'il doit utiliser le système RSA avec les deux entiers n et e (dans notre exemple n= 1634 et e=11).

Il va procéder au cryptage de la manière suivante :

Il transforme en nombres son message en remplaçant par exemple chaque lettre par son rang dans l'alphabet : a= 01, b= 02…..z= 26, il résulte :

M= ANEMONE

M= A N E M O N E

M= 01 14 05 13 15 14 05

Il découpe son message numérisé en blocs de même longueur représentant chacun une taille égale ou inférieure à celle de n ce qui empêche la simple substitution. Dans notre exemple la taille de n est 3, ce qui donne des tranches m_i de 03 chiffres chacune, le message devient :

M= 001 140 513 151 405

M= m_1 m_2 m_3 m_4 m_5

Chaque bloc m_i est chiffré par l'équation :

$$Ci=M_i^e \bmod n$$

Ce qui donne :

$$C_1= m_1^{11} \bmod 1643= 001$$

$$C_2= m_2^{11} \bmod 1643= 109$$

.. . . .

.. . . .

$$C_5= m_5^{11} \bmod 1643= 374$$

$001^{11} \text{mod } 1643 =$	1
$140^{11} \text{mod } 1643 =$	109
$513^{11} \text{mod } 1643 =$	890
$151^{851} \text{mod } 1643 =$	1453
$405^{11} \text{mod } 1643 =$	374

Alors le message chiffré C sera :

C= c_1 c_2 c_3 c_4 c_5

C= 0001 0109 0890 1453 0374

Enfin, Bob a son message chiffré, il peut donc l'envoyer à Alice.

II.4.3. Déchiffrement

Alice reçoit le message de Bob, à partir de p et q, qu'elle a gardés secrets elle calcule la clef d de déchiffrement (c'est sa clef privée). Celle-ci doit satisfaire l'équation:

e.dmod ((p-1) (q-1))=1

Chacun des blocs c_i du message chiffré sera déchiffré par l'équation:

$M_i=C_i^d \text{ mod } n$

Ce qui lui donne :

$1^{851} \text{mod } 1643 =$	1
$109^{851} \text{mod } 1643 =$	140
$890^{851} \text{mod } 1643 =$	513
$1453^{851} \text{mod } 1643 =$	151
$374^{851} \text{mod } 1643 =$	405

M=001 140 513 151 405

M= ANEMONE

Lors du déchiffrement, sachant qu'il faut obtenir des blocs de 2 éléments (grâce au codage particulier de l'exemple). Finalement, Alice prend sa table de correspondance alphabétique pour restituer le message M, elle aura:

01 14 05 13 15 14 05

A N E M O N E

❖ **Résumé**

Le RSA est un algorithme de chiffrement asymétrique fait appel aux notions suivantes:

1.Génération de 2 nombres premiers p et q.
2. Calcul de n=p*q.
3. Déterminer e tel que 3<e< ϕ (n) et PGCD(e, ϕ (n))=1.
4. Calculer d tel que e*d≡1 mod ϕ(n).
5.Clé publique: (e,n).
6.Clé privée: (d,n).
7. p et q doivent rester secrets, voire supprimés.
8.C= M^emod n et M= C^dmod n. [31]

III.Tatouage numérique

III.1. Définition

Un tatouage numérique est une signature ajoutée à un document numérique, de type audio ou visuel en général (mais il peut également être placé sur un fichier texte, une vidéo, voire un modèle 3D). Dans le cas que nous étudions, celui de l'image, le tatouage numérique est un ensemble de bits, appelé marque ou message, ayant pour but d'identifier le propriétaire du document, de manière visible comme on peut le voir, ou de manière invisible à l'œil nu, ne pouvant être détectée qu'au scanner.

III.2. Contraintes d'un schéma de tatouage efficace

Pour être performant et efficace, le tatouage doit vérifier les quatre critères suivants :
• **La visibilité des tatouages :** On peut distinguer deux types de tatouages numériques: les tatouages visibles et les tatouages invisibles.

• **L'Imperceptibilité :** Le tatouage doit être imperceptible, c'est à dire qu'un utilisateur quelconque ne doit pas pouvoir différencier visuellement l'image tatouée de l'image originale.
• **La sécurité:** Comme dans toutes les disciplines proches de la cryptographie, la sûreté du système est assurée uniquement par la confidentialité de la clef K. Si K est inconnue, aucun utilisateur ne doit pouvoir retrouver l'image originale.
• **La robustesse :** Ces techniques utilisées pour le piratage combinent notamment les transformations géométriques, la compression, les filtrages divers et attaques de type cryptographique.

III.3. Tatouage visible

III.3.1. Tatouage d'image par image

Le tatouage d'image par image est notre méthode pour le tatouage visible qui se réalise en plusieurs étapes :

- Chargement d'image à traiter (B)
- Choisir une position aléatoire dans l'image et la lire
- Chargement l'image de tatouage et lire (A)
- Définir (K)

$$image\ resultat = image\ tatouée + \left(\frac{image\ de\ tatouage}{le\ facteur\ de\ luminosité}\right) \quad (2)$$

- C=A+B/K
- Affichage du résultat(C : image tatouée)

Exemple :

$$\mathbf{C} = \underbrace{\begin{pmatrix} 0.51 & 0.47 & 0.30 & 0.43 \\ 0.12 & 0.95 & 0.41 & 0.47 \\ 0.22 & 0.98 & 0.53 & 0.65 \end{pmatrix}}_{\mathbf{A}} + \frac{1}{10}\underbrace{\begin{pmatrix} 0.21 & 0.34 & 0.21 & 0.21 \\ 0.54 & 0.43 & 0.76 & 0.33 \\ 0.46 & 0.44 & 0.66 & 0.54 \end{pmatrix}}_{\mathbf{B}} = \begin{pmatrix} 0.531 & 0.504 & 0.321 & 0.451 \\ 0.174 & 0.993 & 0.486 & 0.503 \\ 0.266 & 1 & 0.596 & 0.704 \end{pmatrix}$$

K : Facteur de luminosité

Fig. III.01. présentation de traitement matriciel pour la méthode du tatouage visible.

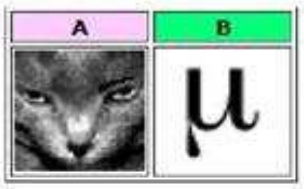


Fig. III.02. Exemple de tatouage image par image dissimilée

Et le facteur de luminance varie en fonction du choix de l'utilisateur.

En mettant en œuvre cet algorithme nous allons rencontrer deux problèmes majeurs :

- Deux images de taille différente.
- Débordement des couleurs.

Le premier problème est résolu par le redimensionnement de la zone tatouée de l'image camouflée selon deux conditions, l'une, si l'image camouflée est plus grande que celle camouflant, le tatouage aura lieu sur toute l'image camouflée. Deux, nous avons le cas opposé, l'image du tatouage sera redimensionnée selon l'image qui va être tatouée.

Le deuxième problème est cependant un peu délicat, étant donné qu'il s'agit des valeurs des couleurs qui sont dans un intervalle de 0 à 255. Ainsi, afin de résoudre ce problème la solution suivante sera appliquée : [32]

$$la\ couleur\ (rouge, vert\ ou\ bleu)\ dans\ un\ pixel\ (i,j) > 255$$
$$couleur\ =\ couleur\ \%\ 255$$

IV.Conclusion

Nous avons présenté dans ce chapitre, la structure détaillée de l'algorithme de chiffrement asymétrique RSA et puis on a présenté les étapes de tatouage d'image par image « image dissimulée » pour le tatouage visible, qu'on va les implémenter dans le chapitre 4.

I. Introduction

Nous avons vu dans les chapitres précédents, les différents systèmes de cryptage, décryptage et leurs fonctionnements.

Ce chapitre porte sur la développement de l'application où on va expliquer le cryptage d'une image en utilisant l'algorithme de chiffrement asymétrique RSA et le tatouage numérique visible, en détaillant les différentes étapes par laquelle une image passe avant d'être cryptée et tatouée, ainsi que l'environnement de programmation, en illustrant des résultats de traitement en se basant sur des analyses et des tests.

II. Environnement de développement

II .1. Les ressources matérielles

- Processeur Intel® Core (TM) i5-2520M CPU @ 2.50GHz
- Mémoire installée (RAM) : 4.00Go

II.2. Ressources logicielles

II.2.1. Système d'exploitation: Windows 10, Windows 7

II.2.2. Editeur utilisé est JAVA NetBeans IDE 8.1

II.2.2.1. Outils de développement

A. Java : Java est un langage de programmation et une plate-forme informatique qui ont été créés par Sun Microsystems en 1995, rachetée plus tard par Oracle Corporation.

Beaucoup d'applications et de sites Web ne fonctionnent pas si Java n'est pas installé et leur nombre ne cesse de croître chaque jour. Java est rapide, sécurisé et fiable. Il est utilisé partout, des ordinateurs portables aux centres de données, des consoles de jeux aux superordinateurs scientifiques, des téléphones portables à Internet, la technologie Java est présente sur tous les fronts. Nous avons opté pour ce langage pour la réalisation de notre application logicielle.

B. NetBeans IDE 8.1 : Les IDE (Integrated Environment Development) sont des programmes qui regroupent un ensemble d'outils pour le développement de logiciels.

De façon générale, un IDE contient un éditeur de texte, un compilateur, des outils automatiques de fabrication, et très souvent un débogueur. Il existe des IDE pour de nombreux langages de programmation, cependant il est très courant qu'un IDE soit conçu

pour un seul langage. Il est également possible qu'un IDE dispose d'un système de gestion de versions et différents outils facilitant la création d'interfaces graphiques [33].

C. WampServer : (anciennement **WAMP5**) est une plateforme de développement Web de type WAMP, permettant de faire fonctionner localement (sans se connecter à un serveur externe) des scripts PHP. WampServer n'est pas en soi un logiciel, mais un environnement comprenant deux serveurs (Apache et MySQL), un interpréteur de script (PHP), ainsi que phpMyAdmin pour l'administration Web des bases MySQL.

Il dispose d'une interface d'administration permettant de gérer et d'administrer ses serveurs au travers d'un tray icon(icône près de l'horloge de Windows).

La grande nouveauté de WampServer 2 réside dans la possibilité d'y installer et d'utiliser n'importe quelle version de PHP, Apache ou MySQL en un clic. Ainsi, chaque développeur peut reproduire fidèlement son serveur de production sur sa machine locale.

- Le 1er mai 2014 est sortie la version 2.5. Cette version intègre Apache 2.4.9, MySQL 5.6.17, PHP 5.5.12, PhpMyadmin 4.1.14, SQLBuddy 1.3.3, XDebug 2.2.5.

- 1er décembre 2015 : Wampserver 3 32bit : Apache 2.4.17, MySQL 5.7.9, PHP 5.6.15, PhpMyAdmin 4.5.1

Wampserver 3 64 bit : Apache 2.4.17, MySQL 5.7.9, PHP 5.6.16 et 7.0.0, PhpMyAdmin 4.5.2 [34].

III. Description de l'application

On peut résumer les étapes de l'application par un schéma général qui va représenter l'architecture de notre programme.

Pour qu'une image satellitaire soit (crypté / décrypté) par notre application, elle doit passer par les étapes présentes dans l'organigramme suivant :

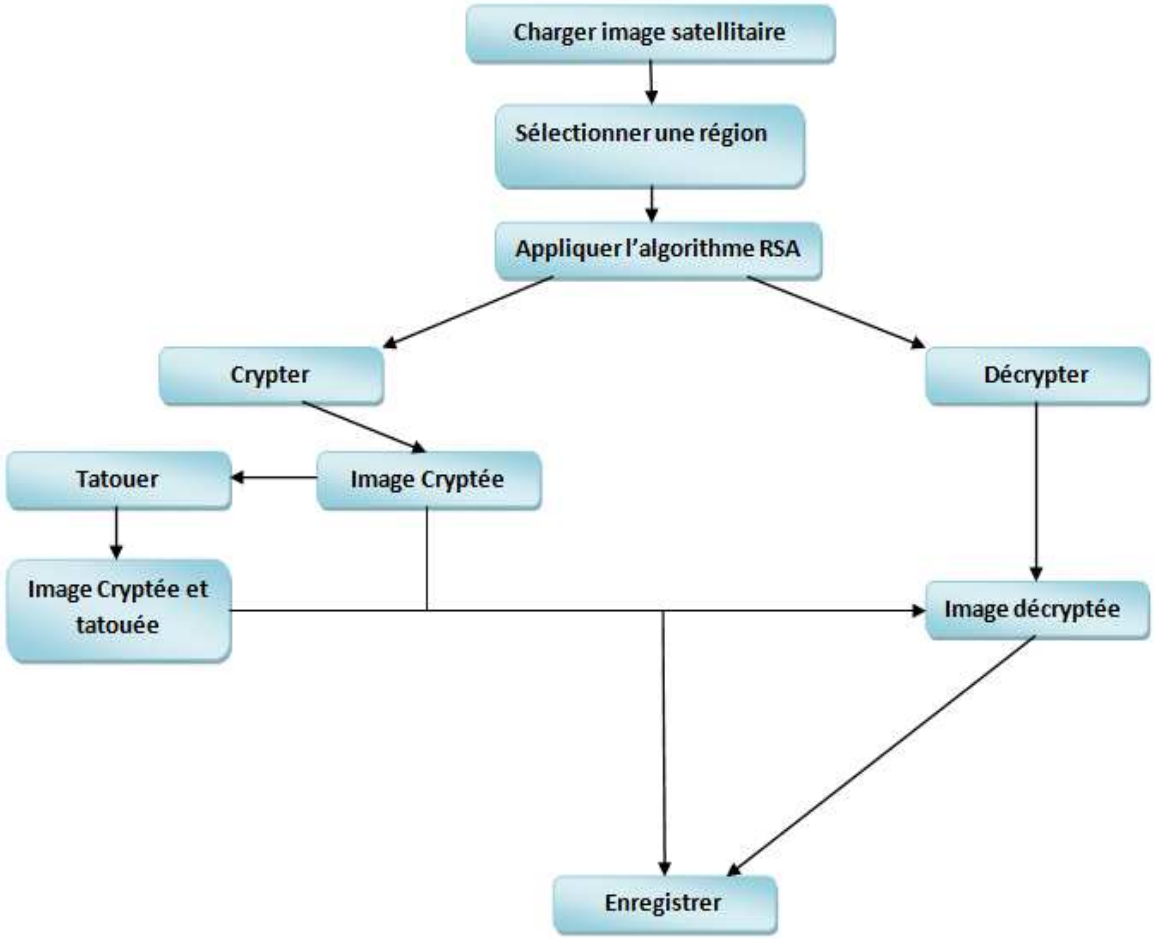


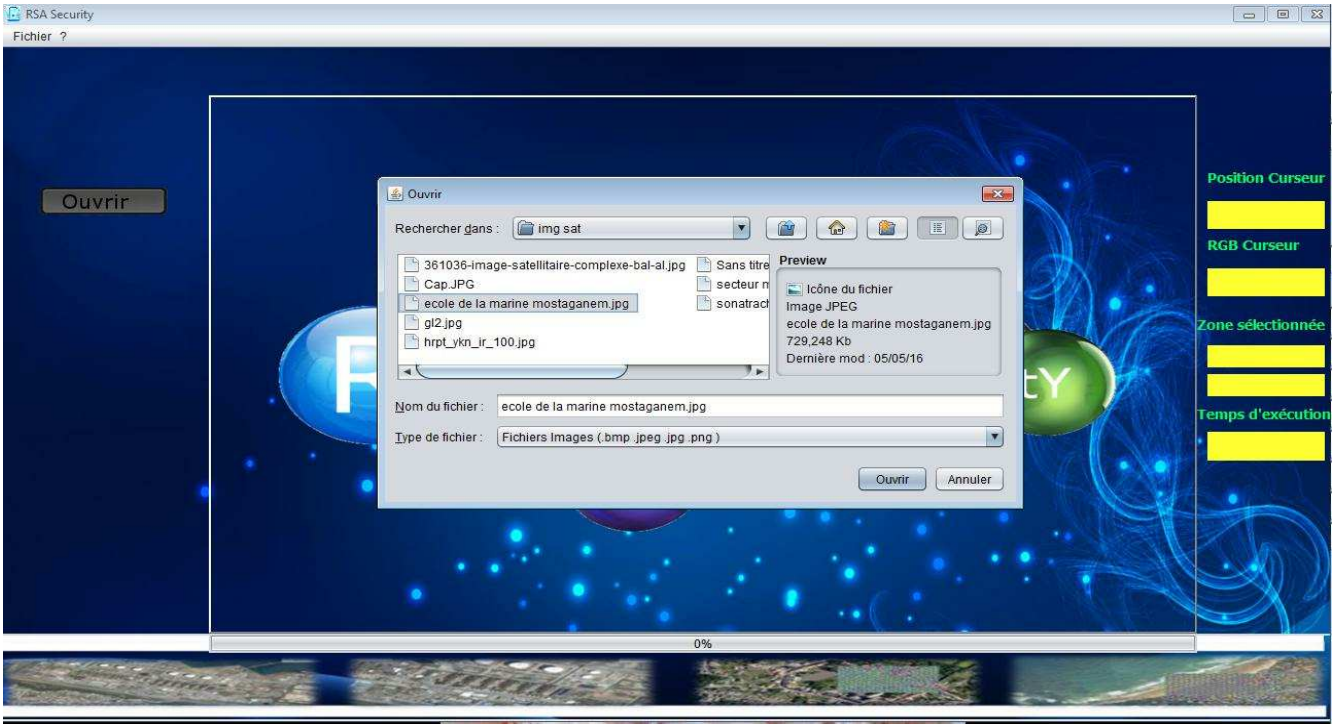
Fig. IV.01.Organigramme de l'application

IV .Description du travail réalisé

Cette partie est consacrée à la description de la phase de la réalisation et d'implémentation de ce projet, on va donc, montrer les différents modules de notre application afin d'illustrer plus clairement les diverses utilisations de l'application.
On commence la présentation de notre application par l'interface d'accueil.

Fig. IV.02. Fenêtre principale

Tous d'abord il faut ouvrir une image en cliquant sur le bouton « Ouvrir ».



On va sélectionner une image satellitaire à partir de google earth de l'année (2016) de système de référence WGS 1984-UTM zone 31.

Fig. IV.03. Ouvrir l'image

IV. 1. Cryptage

Après avoir chargé l'image, on choisit une partie de l'image qu'on veut crypter :

Fig. IV.04. Sélectionner une région de l'image

Puis en appuyant sur le bouton crypter, la fenêtre ci-dessous va être affichée :

Fig. IV.05. Crypter une région de l'image

IV. 2. Tatouage :

Après avoir une image cryptée, on va cliquer sur le bouton Tatouer pour signer l'image.

Fig. IV.06. Tatouage de l'image

On peut enregistrer l'image cryptée pour la décrypter par la suite.

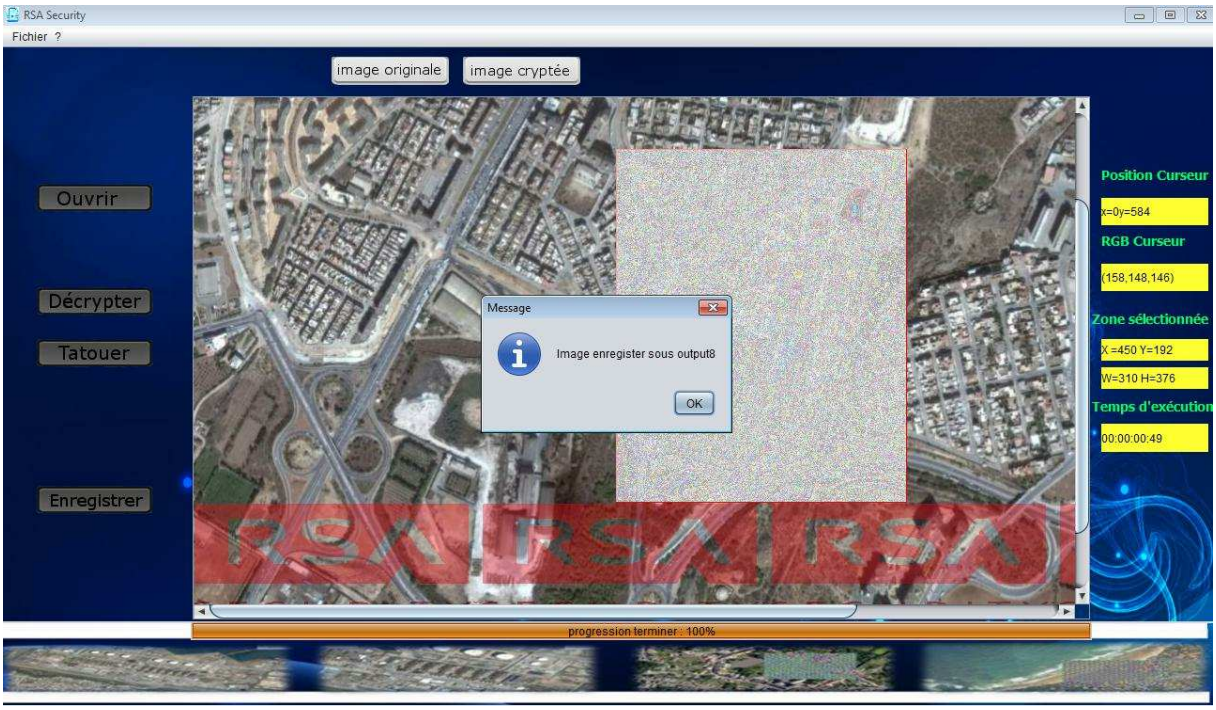


Fig. IV.07. Enregistrement de l'image

Remarque : pour décrypter l'image après avoir quitté le programme il faut d'abord enregistrer l'image cryptée d'une manière automatique dans une base de données qui garde les coordonnés de la sélection cryptée pour faciliter la tâche de décryptage sans sélectionner la partie cryptée.

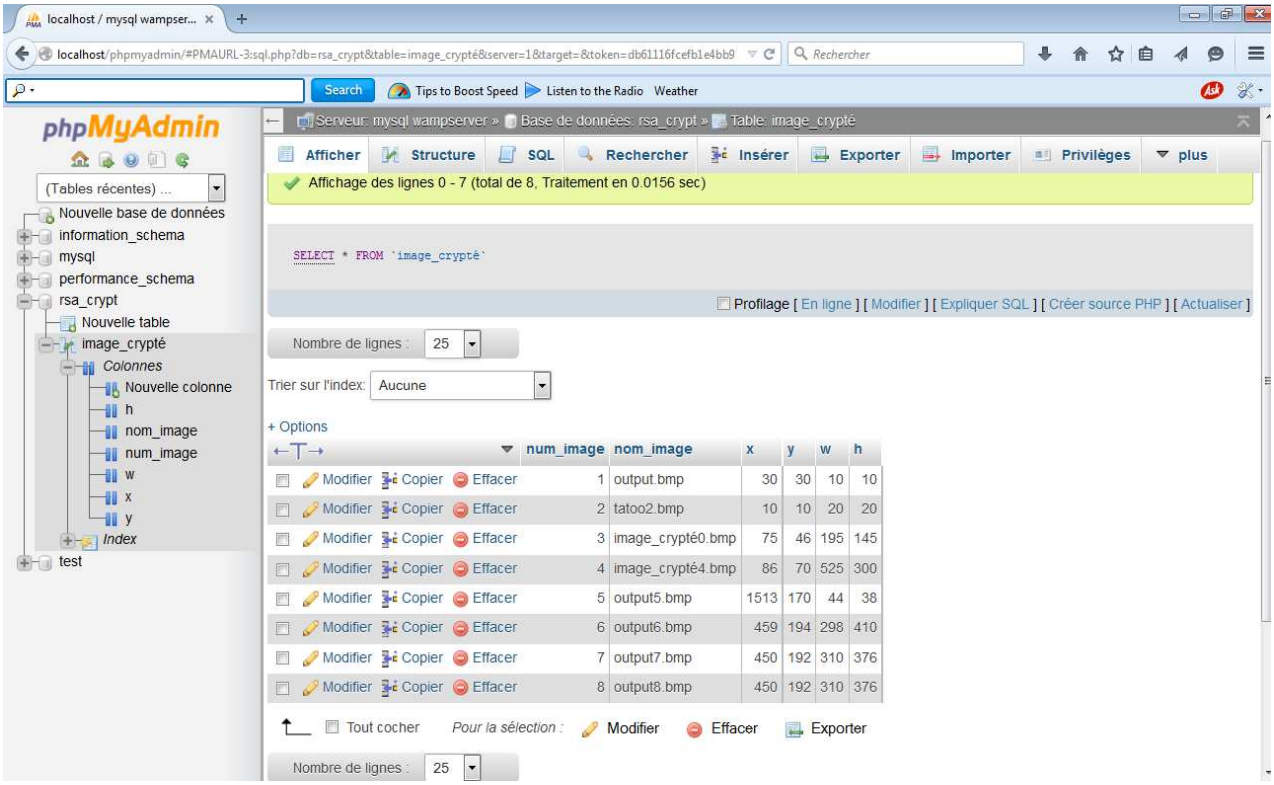


Fig. IV.08. Emplacement dans la BD

IV. 3. Décryptement

Pour décrypter l'image après le cryptage directement c.à.d. avant de quitter le programme en appuyant sur le bouton décrypter, la fenêtre ci-dessous va être affichée :

Fig. IV.09. Région décryptée

On peut aussi décrypter l'image après l'enregistrement dans la base de données.

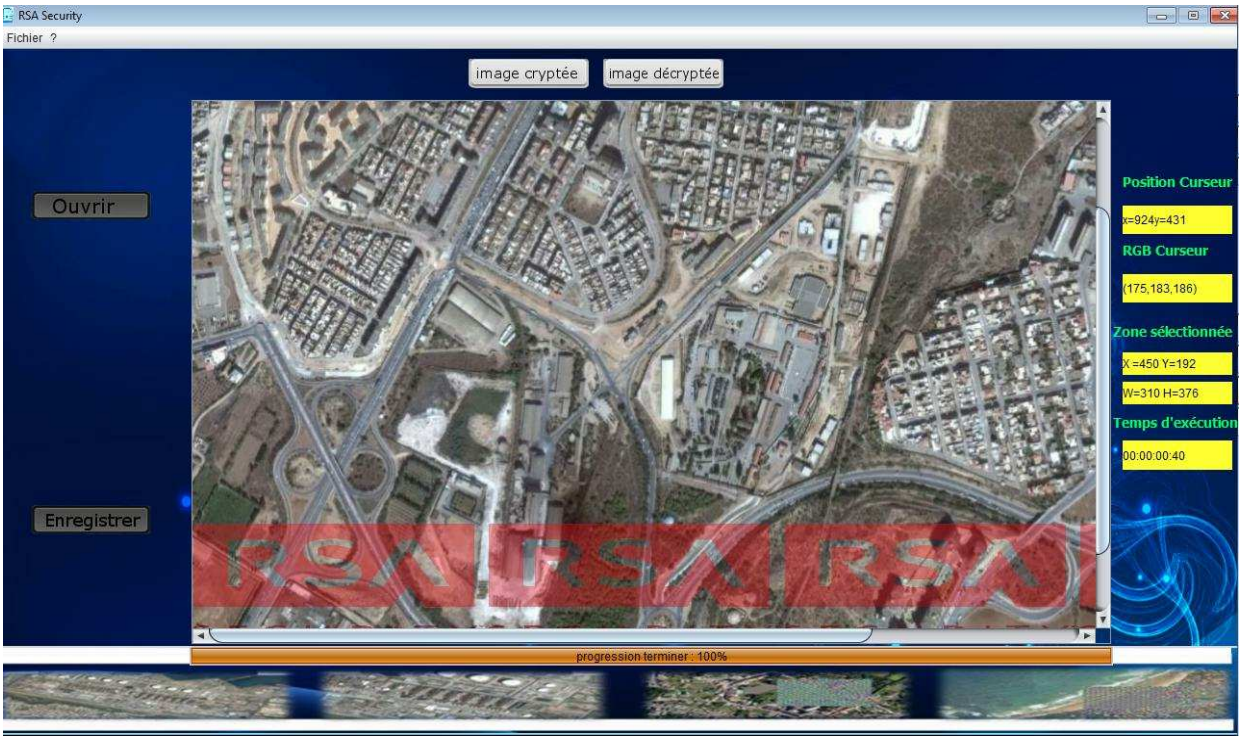


Fig. IV.10. Image décryptée

On peut aussi enregistrer l'image décryptée de la même façon d'enregistrer l'image cryptée et quitter l'application de faire Alt+f4.

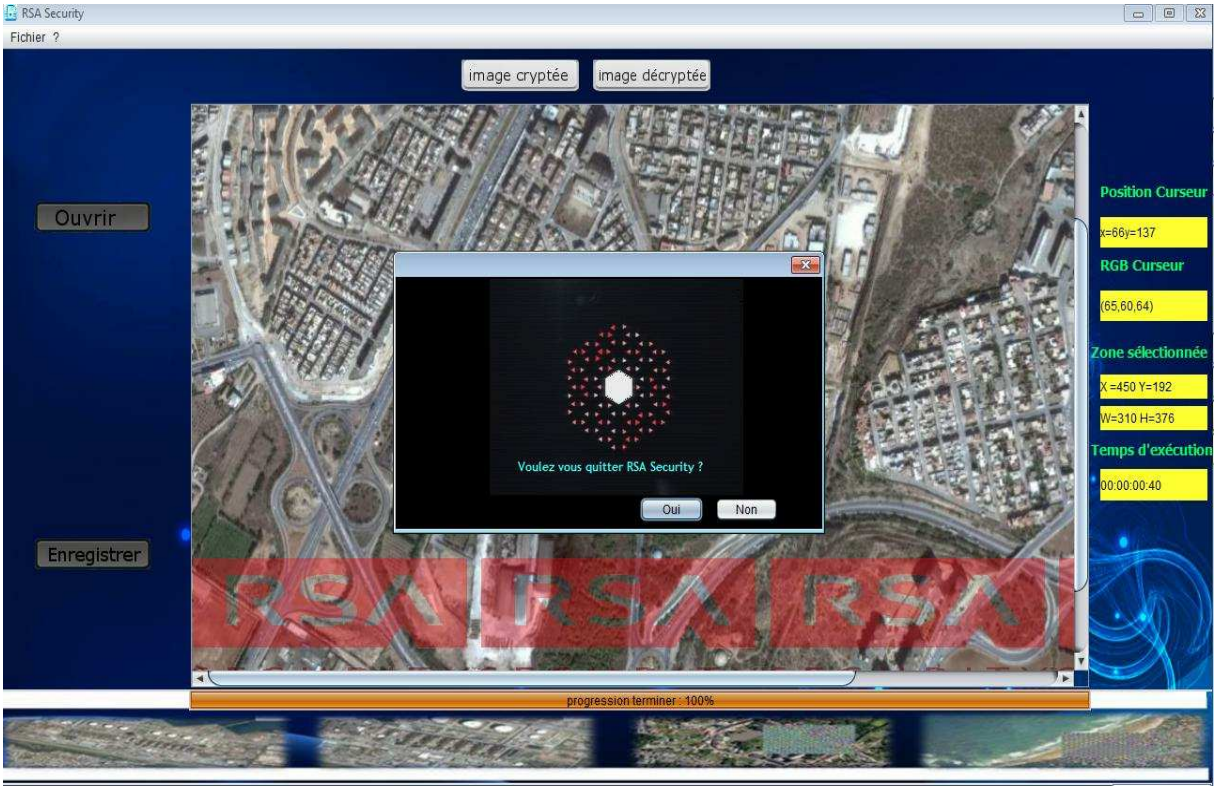
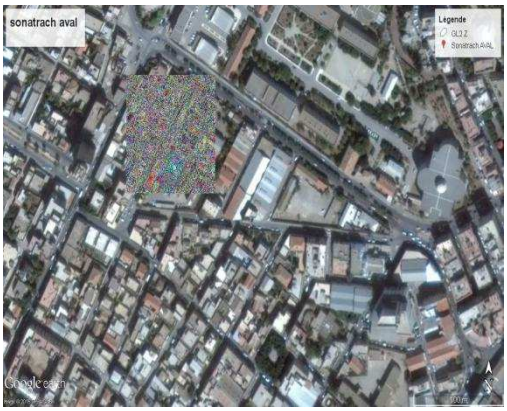
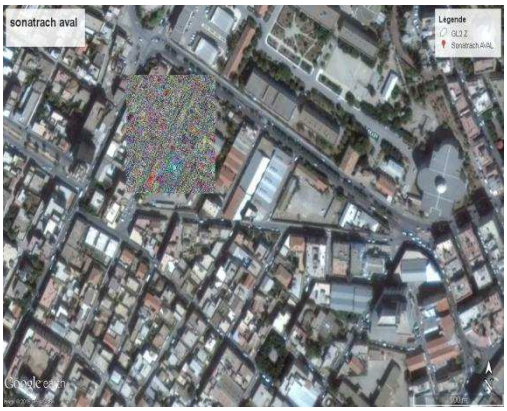


Fig. IV.11. Quitter l'application

V. Résultats

Cryptage de la région			
Image originale	**Image cryptée**	Temps (s)	Taille (px)
		0.12	218 x225

		0.08	218 x225

Décryptage de la région			
Image cryptée	**Image décryptée**	**Temps (s)**	**Taille (px)**
		0.15	218 x225
		0.07	218 x225

❖ Discussion

D'après les résultats obtenus pour l'application de notre cryptosystème asymétrique :

- Il est sécurisé car on ne va pas donner la valeur de la clé publique ni autre valeur car elles sont initialisées dans le programme.
- Aussi le temps d'exécution est très rapide et plus la taille de la région à crypter augmente plus le temps de cryptage est élevé. (mais n'empêche qu'il est toujours rapide).
- Un autre avantage, c'est que le décryptage automatique n'a pas besoin de sélectionner la zone cryptée et sa nous aide à gagner plus de temps et à automatiser le processus de décryptage.
- Pour les images qui ne figure pas dans la bd, on peux procéder manuellement et sélectionner la zone a décrypter.
- De plus, on a identifie nos images cryptées par un logo de tatouage.
- L'image cryptée est sauvegardée directement dans un chemin précis et nommé par un nom unique car les images sont générées automatiquement.

Mais ce qui est le plus important est le fait de ne pas avoir une perte d'information, donc nous sommes aussi satisfait pour les résultats obtenus.

VI. Conclusion

On se basant sur les résultats des tests donné par l'application on peut dire que la méthode proposée répond aux besoins et fonctionne parfaitement par rapport à la qualité d'image et le temps d'exécution, aussi crypter/décrypter avec zéro perte de données, en même temps la sécurité est renforcée car tout est implémenté dans l'application, puisque on envoi que l'image chiffrée, sans donner la clé publique, tout est imbriqué et cacher. Seule l'application permet de déchiffrer les images cryptées, alors on conclut que cette méthode est appropriée aux images satellites.

Conclusion générale

Dans ce mémoire, nous avons abordé la problématique de la sécurisation des images satellitaires, problème qui a pris de plus en plus d'importance depuis le développement d'internet et des réseaux d'échange et la dématérialisation des contenus multimédias, où on a implémenté un cryptosystème avec un tatouage visible pour résoudre ce problème.

Pour réaliser notre projet nous somme passé par les chapitres suivants :

Chapitre I : on a présenté une introduction et quelques notions importantes concernant les images satellitaires. Pour connaitre le plus possible dans le domaine des images satellitaires et quelques moyens de les capter.

Chapitre II : nous avons présenté les principes de base de cryptographie qui vont nous permette de comprendre cet axe de recherche très important qui à pour but de chiffrer l'information dans l'image satellitaire.

Chapitre III : on a présenté les méthodes à implémenter.

Chapitre IV : on a présenté une implémentation de l'application qui se compose en trois méthodes : le cryptage, le décryptage et tatouage visible.

En général, on peut dire que la méthode proposée permet d'atteindre de très bons résultats de point de vue qualité des images et le temps d'exécution. En effet, elle permet de crypter énormément la quantité des informations contenues dans les images satellitaires tout en conservant leurs propriétés originales. Dans plusieurs applications nous n'avons pas intérêt à crypter l'image entière, mais seulement une partie ou une région spécifique. Pour cela on essaye d'adapter notre application pour réaliser cet objectif et l'ensemble des tests effectués montrent la bonne robustesse des différentes combinaisons de l'algorithme de chiffrement aux différents types d'attaques. Puisque les différents tests donnent presque les mêmes résultats, nous nous limitons au test de temps d'exécution.

Puis que la sécurité à 100% en informatique reste toujours impossible, donc le tatouage est devenu comme une nouvelle technique de protection pour empêcher toute évènement non autorisé sur les documents multimédias mais le problème qui se pose est le dé tatouage, malgré les méthodes de ce dernier sont en cours d'être réalisable donc après plusieurs essais , ils vont devenir une réalité et un grand problème.

Comme perspectives, nous proposons un cryptosystème de chiffrement hybride basé sur les deux algorithmes AES et RSA pour assurer les trois grands axes de sécurité: la confidentialité, l'authentification et l'intégrité.

Usage du chaos pour sécuriser la transmission des données via un réseau virtuel.

Bibliographie

[1] Wikiversité, https://fr.wikiversity.org/wiki/Images_satellites/Introduction, Consulté le : 06/03/2016.

[2] Ahmed Tidjani et Ali Khorsi et Ziani, Détection de la végétation à partir d'une image satellitaire, Mémoire en ligne, Université Amar Thelidji Laghouat Algérie, 2010 P.2.

[3] Mireille Delvaux, Cathy Nys, Géographie: lire le monde, De Boeck, Rue de minimes 39, B_1000 Bruxelles, 2002, page 226.

http://www.memoireonline.com/02/14/8724/m_Suivi-par-teledetection-de-l-evolution-des-formations-vegetales-et-du-stock-de-carbone-de-la15.html#_Toc329287452

[4] Zana Inzan OUATTARA, Suivi par télédétection de l'évolution des formations végétales et du stock de carbone de la réserve de faune d'Abokouamékro en vue de son intégration dans le mécanisme redd+, Diplôme d'agronomie approfondie- Option eaux et forêts, Institut national polytechnique Félix Houphouet-Boigny de Yamoussoukro (Côte d'Ivoire), 2012.

[5] Universalis.fr, http://www.universalis.fr/encyclopedie/teledetection/, consulté le : 07/03/2016.

[6] Abdelghani Boudhar, Télédétection du manteau neigeux et modélisation de la contribution des eaux de fonte des neiges aux débits des oueds du haut atlas de Marrakech, Mémoire de Doctorat National, Université Cadi Ayyad , 2009.

[7] M. Steven, D. Freek Remote Sensing Image Analysis: Including the Spatial Domain Springer (livers), (2005).

[8] Claude Kergomard , LA TÉLÉDÉTECTION AÉRO-SPATIALE : UNE INTRODUCTION, Ecole Normale Supérieure Paris

[9] Wikipédia,
htt ps://fr.wikipedia.org/wiki/Satellite_de_t%C3%A9l%C3%A9d%C3%A9tection, Consulté le 07/03/2016.

[10] Notions fondamentales de télédétection un cours tutoriel du Centre spatial canadien, université de Nice-Sofia Antipolis, proposée par le professeur Rao de l'université du Texas en (1974).

[11] EOEdu observation notre planète, http://eoedu.belspo.be/fr/satellites/noaa.htm, consulté le : 26/12/2015.

[12] Eduscol, http://eduscol.education.fr/orbito/system/landsat/land00.htm, consulté le : 26/12/2015.

[13] EOEdu observation notre planète, http://eoedu.belspo.be/fr/satellites/spot.htm, consulté le : 26/12/2015.

[14] Eduscol, http://eduscol.education.fr/orbito/system/spot/spot00.htm, consulté le : 24/12/2015.

[15] Aeronautique.ma, http://www.aeronautique.ma/C-est-quoi-un-RADAR_a1131.html , consulté le 28/12/2015.

[16] EOEdu observation notre planète, http://eoedu.belspo.be/fr/satellites/radarsat.htm, consulté le : 29/12/ 2015.

[17] Developpez.com, http://ram-0000.developpez.com/tutoriels/cryptographie/#L1, 28/03/2016.

[18] Z.Lotmani, Y.Elhomr et C. Bentaouza , Fault-Based Attack of RSA Authentication, Mémoire de Master, Universite Abdelhamid Ibn Badis Mostaganem, 2013 , p.10.

[19] Serge Vaudenay, La fracture cryptographique, Livre, lausanne, PPUR (2011), page 2,3.

[20] Hamzata Gueya, Mise en place d'un IDS en utilisant Snort , Diplôme Européen des études supérieur en informatique et réseau, Miage de Kenitra(Maroc), 2011, P.22. http://www.memoireonline.com/04/15/9036/m_Mise-en-place-d-un-IDS-en-utilisant-Snort8.html

[21] Introduction à la cryptographie, Copyright © 1990- 1998 Network Associates, Amsterdam, page 2.
ftp://ftp.pgpi.org/pub/pgp/6.5/docs/french/IntroToCrypto.pdf

[22] AHMED BELHADJ, souhila, Etude comparative entre la cryptographie à clé secrète et à clé publique appliquée aux textes arabes,Mémoire de Master SIC, Abou Bekr Belkaid Tlemcen, 2014 , p.10.

http://dspace.univ-tlemcen.dz/bitstream/112/6836/1/Etude-comparative-entre-la-cryptographie.pdf

[23] Jean de dieu Nkapkop, Evaluation d'un algorithme de cryptage chaotique des images basé sur le modèle du perceptron, Mémoire de Master en EEA,Université de Ngaoundéré ,2012, P.8,15,16.

[24] TPE : La cryptographie, http://wakaziva.pagesperso-orange.fr/crypto/2.htm, Date de consultation : 16.11.15

[25] Philippe Perret - MSI Groupe Arkoon , Serge Richard (CISSP®) - IBM France ,Cryptographie, CLUSIR Rhône Alpes ,Février 2007
http://www.clusir-rha.fr/sites/default/files/upload/Lyon/SSI/ClusirCryptographie.pdf

[26] Kihal Ahmed Ridha, systèmes chaotiques pour la transmission securisée de données, Mémoire de Magister, Université Mohamed Khider – Biskra, 26/11/2013, P.9, 18,19.

[27] A.Benkredda, H.Benalouda ,C.Bentaouza , Authenticity and Integrity of Digital Mammography Images, Mémoire de Master, Universite Abdelhamid Ibn Badis Mostaganem, 2011, P.13.

[28] Renaud Dumont, Cryptographie et Sécurité informatique, Notes de cours provisoires, Université de Liège, Faculté des Sciences Appliquées, 2009/2010, P.9.

[29] Philippe Perret, Serge Richard, Cryptographie, Clusir Rhône Alpes, 2007, P.36. http://www.clusir-rha.fr/sites/default/files/upload/Lyon/SSI/ClusirCryptographie.pdf

[30] Jean paul Delhaye, La cryptographie RSA vingt ans après, POUR LA SCIENCE - N° 267, Paris, Janvier 2000, Page 104.

[31] M.Boukhatem, application des techniques de cryptage pour la transmission sécurisée d'image MSG, Mémoire de magister en électronique, Université Mouloud Mammeri Tizi-ouzou, 11/03/2015.

[32] A.Tayab Bey, K.Touihr et C.Bentaouza, Authentification des images numériques basées sur le tatouage numérique, Mémoire de Master, Université Abdelhamide Ibn Badis, Mostaganem, juin 2014.

[33] NetBeans, https://netbeans.org/features/index.html , Consulté le 29/04/2016.

[34] Wakipedia, https://en.wikipedia.org/wiki/WampServer , Consulté le 02/05/2016.