République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université 20 Aout- 1955-SKIKDA

Faculté des Sciences

Département d'Informatique

Mémoire de fin d'étude en vue de l'obtention

Du diplôme De master en informatique

Option : M2 RSD

Thème :

Galerie d'image crypté

Réalisé par :

- **Kerbouche Habiba**

Encadré par :

Mr.Bourmel Hakim

Session : juin 2025

Remerciements

Nous tenons tout d'abord à remercier à tout instant ***DIEU*** *tout puissant qui nous a éclairé la vie par le savoir et nous a aidé à réaliser ce travail de fin d'études.*

Nous remercions, après, toute personne qui nous a conseillé, guidé, encouragé et soutenu tout au long de cette année et qui a contribué de près ou de loin à l'aboutissement de ce travail.

En particulier :

Notre encadreur Monsieur Bourmel A-Hakim

Nous tenons aussi remercier les membres du département

Nous remercions aussi nos professeurs qui tout au long des années d'études nous ont transmis leur savoir sans réserve.

Aussi tous nos amis et nos collègues pour leur soutien moral tout au long de la préparation.

Ainsi que nos jurés.

Dédicaces

Louange à dieu tout puissant qui m'a offert toute
La force pour réaliser ce projet.
Je dédie ce travail :

A l'âme pure de mon père, que Dieu lui fasse miséricorde

Je dédie ce fruit de mes efforts à ma maman la plus chère et la plus précieuse de ma vie, qui a éclairé mon chemin de ses conseils, à celle qui a orné ma vie, à celle qui m'a donné la force et la détermination de continuer le chemin, et qui a été la raison de poursuivre mes études, à celle qui m'a appris la patience et la diligence, à celle qui est chère à mon cœur.

Résumé

Avec le développement rapide des réseaux de communication, une grande quantité d'informations, notamment des images, est échangée sur ces réseaux. Étant donné que les images peuvent contenir des données sensibles, leur protection est devenue essentielle. Le chiffrement constitue une solution efficace pour assurer la confidentialité et la sécurité de ces informations.

Les algorithmes de chiffrement jouent un rôle crucial dans la protection des données, en rendant l'accès aux informations extrêmement difficile pour les personnes non autorisées.

Dans ce mémoire, nous présentons une application web permettant d'appliquer et d'évaluer différents algorithmes de chiffrement d'images.

Mots-clés : Image, Chiffrement

Abstract

With the rapid development of communication networks, a large amount of information, including images, is transmitted over these networks. Since images often contain sensitive data, protecting them has become crucial. Encryption offers an effective solution to ensure the security and confidentiality of such information.

Encryption algorithms play a vital role in securing data by providing advanced methods that make unauthorized access extremely difficult.

In this thesis, we present a web application designed to implement and evaluate various image encryption algorithms.

Keywords : Image, Encryption

ملخص

مع التطور السريع لشبكات الاتصال، يتم تبادل كمية كبيرة من المعلومات، بما في ذلك الصور، عبر هذه الشبكات. وبما أن الصور قد تحتوي على بيانات حساسة، أصبحت حمايتها أمرًا ضروريًا. يُعد التشفير حلاً فعالًا لضمان أمن وسرية هذه المعلومات.

تلعب خوارزميات التشفير دورًا أساسيًا في حماية البيانات، حيث تقدم أساليب متقدمة تجعل الوصول غير المصرح به صعبًا للغاية.

في هذا البحث، نقدم تطبيق ويب يهدف إلى تنفيذ وتجربة مختلف خوارزميات تشفير الصور.

الكلمات المفتاحية: صورة، تشفير

Table des matières

Chapitre 4 : Implémentation

Liste des figures

Liste des tableaux

Introduction générale

1. Introduction Générale

À l'ère du numérique, l'information circule à une vitesse fulgurante. Chaque seconde, d'énormes quantités de données sont échangées, stockées ou consultées à travers le monde via des réseaux interconnectés. Si ce phénomène représente un progrès indéniable, il soulève également des préoccupations majeures en matière de confidentialité, de sécurité et de fiabilité des données numériques. Dans ce contexte, la cybersécurité s'impose comme une discipline essentielle à la protection de l'information. Parmi les nombreuses catégories de données manipulées, les images numériques constituent un type de contenu particulièrement sensible et vulnérable.

En effet, les images jouent un rôle central dans divers domaines critiques : en médecine, elles permettent de diagnostiquer et de suivre l'évolution des maladies ; en justice, elles servent de preuves numériques ; dans les réseaux sociaux, elles représentent l'un des principaux vecteurs de communication ; et dans les systèmes de vidéosurveillance, elles assurent la sécurité des espaces physiques. Toute perte, altération ou consultation non autorisée de ces images peut avoir des conséquences graves, tant sur le plan personnel que professionnel.

C'est dans ce cadre que s'inscrit la cryptographie, une science ancienne mais toujours en évolution. Autrefois utilisée principalement pour dissimuler des messages à caractère militaire, elle constitue aujourd'hui un pilier incontournable de la sécurité informatique. La cryptographie repose sur des algorithmes mathématiques qui permettent de transformer un message intelligible en un contenu illisible sans la clé adéquate. Grâce à elle, il est possible de garantir des propriétés fondamentales telles que la confidentialité, l'intégrité, l'authentification et la non-répudiation.

Cependant, si le chiffrement des textes est depuis longtemps maîtrisé, le chiffrement des images numériques pose des défis spécifiques. La taille volumineuse des fichiers image, leur forte redondance et la nécessité de préserver leur qualité visuelle imposent des contraintes particulières en termes de performance, de rapidité de traitement et de résistance aux attaques. De plus, les images nécessitent souvent des traitements adaptés à leur structure bidimensionnelle et à leur codage spécifique (RVB, niveaux de gris, etc.).

Dans cette optique, les systèmes chaotiques se présentent comme une alternative prometteuse aux méthodes de chiffrement classiques. Inspirés par la théorie du chaos en mathématiques, ces systèmes présentent des caractéristiques telles que la sensibilité aux conditions initiales, la pseudo-aléa et la complexité dynamique, qui les rendent particulièrement efficaces pour le chiffrement des images. En effet, la nature imprévisible et hautement non linéaire des systèmes chaotiques permet de générer des clés de chiffrement très robustes, difficiles à reproduire ou à deviner. Ainsi, le chiffrement chaotique permet non seulement de renforcer la sécurité, mais aussi d'accélérer le processus de chiffrement grâce à sa légèreté computationnelle, ce qui en

fait un candidat idéal pour les applications temps réel et les environnements à ressources limitées.

C'est dans ce contexte que s'inscrit le présent mémoire, qui propose une étude ainsi qu'une mise en œuvre concrète de techniques de chiffrement appliquées aux images numériques. Plus précisément, le projet porte sur le développement d'une application en Java dotée d'une interface graphique conviviale, capable de chiffrer et de déchiffrer des images à l'aide de plusieurs algorithmes reconnus : AES (Advanced Encryption Standard), DES (Data Encryption Standard), RSA (Rivest-Shamir-Adleman) ainsi que le chiffrement basé sur le chaos. L'objectif est de combiner la rigueur théorique des techniques cryptographiques avec une solution pratique répondant à de réels besoins en matière de sécurité.

L'implémentation de cette application repose sur l'utilisation de bibliothèques Java dédiées à la cryptographie, ainsi que sur une architecture logicielle modulaire. Elle permet non seulement de transformer les images en données chiffrées, mais aussi de gérer le chargement, l'enregistrement, l'affichage et la conversion des images, notamment en format Base64 afin d'en faciliter le traitement et le transfert.

La réalisation de ce projet suit un plan structuré en plusieurs étapes complémentaires :

Chapitre 1 : Généralités sur la Cryptographie

Ce chapitre présente les fondements de la cryptographie, en retraçant son évolution historique et en exposant les principaux concepts qui la régissent. Il introduit les différentes familles d'algorithmes (symétriques, asymétriques, hybrides), les objectifs de sécurité visés, ainsi que le vocabulaire de base nécessaire à la compréhension des choix techniques opérés.

Chapitre 2 : Image et algorithmes de cryptage d'image

Ce chapitre introduit les notions essentielles relatives aux images numériques : formats usuels, codage des pixels, modes de couleur, compression, etc. Il explore également les approches spécifiques au chiffrement des images, y compris les méthodes classiques et chaotiques, en mettant en lumière les contraintes propres à ce type de données et les solutions adaptées.

Chapitre 3 : Analyse et Conception

Cette section décrit les besoins fonctionnels et techniques de l'application. Des diagrammes UML sont utilisés pour modéliser les cas d'utilisation, les classes et les interactions. Le choix de l'architecture MVC (Modèle-Vue-Contrôleur) est justifié dans un souci de clarté, de modularité et de maintenabilité.

Chapitre 4 : Implémentation

Ce chapitre détaille le développement de l'application : environnement Java, conception de l'interface utilisateur avec Swing, intégration des algorithmes AES, DES, RSA et du modèle chaotique, gestion des fichiers et des conversions. Des exemples concrets, accompagnés de captures d'écran, illustrent le fonctionnement de l'outil développé.

Chapitre 1 :
Généralités sur la Cryptographie

Chapitre 1 : Généralités sur la Cryptographie

1. Introduction

La cryptographie est l'art de rendre un message incompréhensible pour toute personne non autorisée à y accéder. De nos jours, elle constitue l'un des piliers fondamentaux de la sécurité de l'information, en particulier avec l'accroissement du flux de données personnelles, professionnelles et gouvernementales circulant à travers des réseaux publics comme Internet. La cryptographie est omniprésente : des communications téléphoniques aux transactions bancaires, des applications de messagerie aux systèmes d'information médicale. Ce chapitre présente les bases de la cryptographie, son évolution, ses types et ses applications modernes.

2. Etat de l'art

La cryptographie est une science ancienne remontant à 1900 av. J.-C. Initialement utilisée à des fins militaires et diplomatiques, elle a connu un essor considérable avec l'apparition de l'informatique. Parmi les moments historiques marquants, on retrouve :

- L'utilisation des hiéroglyphes non standards dans l'Égypte ancienne.
- La machine Enigma durant la Seconde Guerre mondiale.
- La théorie de Claude Shannon sur la sécurité des systèmes de communication.
- L'apparition des algorithmes modernes comme DES, AES et le chiffrement quantique.

3. Aperçu historique de la cryptographie

La cryptographie est l'art de la communication sécurisée, visant à dissimuler le contenu des messages. Son origine remonte à la Rome antique avec le code de César, qui remplace chaque lettre d'un message par une lettre décalée dans l'alphabet. Bien que simple, ce code présente des limites, notamment un nombre restreint de clés possibles, facilitant le décryptage.

Au fil de l'histoire, la cryptographie a joué un rôle crucial, comme en 1586 lorsque Marie Stuart a utilisé des cryptogrammes pour cacher son implication dans un complot contre Elizabeth I, ce qui a conduit à son exécution après le décryptage de ses messages.

Figure 1 : Aperçu historique de la cryptographie

Un exemple plus moderne est le code ENIGMA, utilisé par les Allemands pendant la Seconde Guerre mondiale. Cette machine complexe, avec une clé changeante quotidiennement, a été décryptée par les Alliés grâce à des efforts menés par Alan Turing et son équipe. Le déchiffrement d'ENIGMA a permis aux Alliés de lire les messages allemands, mais ils ont dû faire des choix difficiles pour ne pas alerter l'ennemi.

Figure 2 : Enigma machine

La cryptographie représente une bataille intellectuelle continue entre les créateurs de codes et les cryptanalystes, influençant des décisions historiques et évoluant avec les avancées mathématiques et technologiques.

4. Concepts fondamentaux

a) Cryptologie

La cryptologie, dérivée du grec signifiant "science du secret", est une discipline qui englobe la cryptographie (écriture secrète) et la cryptanalyse (analyse des codes). Bien qu'elle soit un art ancien, utilisé dès l'époque de Jules César et mentionné dans l'Ancien Testament, elle est devenue une science moderne depuis les années 1970. La cryptologie est interconnectée avec plusieurs domaines, tels que la théorie des nombres, l'algèbre, la théorie de la complexité et la théorie de l'information.

Cryptologie = Cryptographie + Cryptanalyse

b) Cryptographie

La cryptographie, dérivée des mots grecs "kruptus" (secret) et "graphein" (écriture), est l'art de cacher des informations pour les rendre incompréhensibles. Elle englobe les techniques de chiffrement des messages, permettant à deux personnes, Nora et Habiba, de communiquer de manière sécurisée, même sur un canal peu fiable, tout en empêchant un tiers, Rezzak, de comprendre leurs échanges. Ce processus utilise une clé de chiffrement pour coder les messages et une clé de déchiffrement pour les rendre à nouveau lisibles.

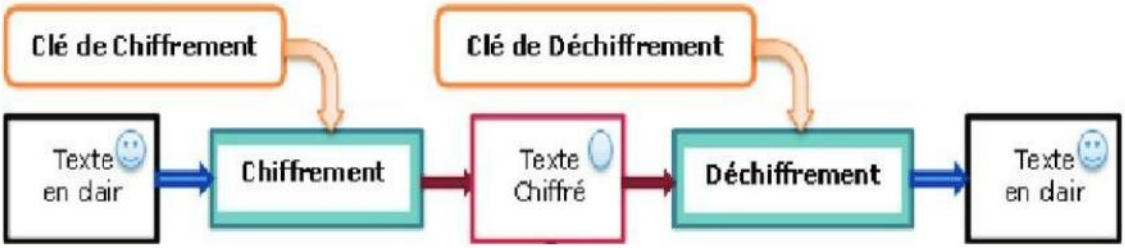

Figure 3 : Schéma général de la cryptographie.

Schéma général de la cryptographie :

1. **Chiffrement** : Transformation d'un texte en clair en texte chiffré.

2. **Déchiffrement** : Transformation inverse permettant de retrouver le texte original.
3. **Clé** : Valeur secrète utilisée dans le processus de chiffrement/déchiffrement.

5. Vocabulaire de base de la cryptographie

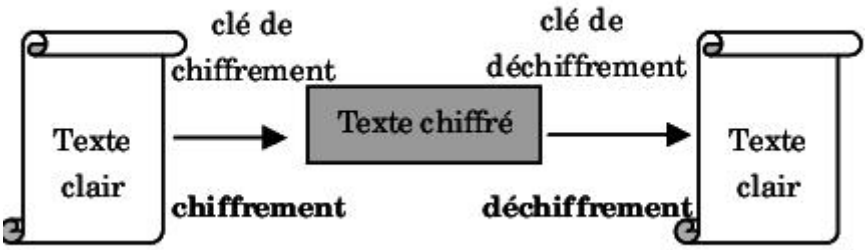

Figure 4: Principe de chiffrement et de déchiffrement

- **Chiffrement**
  Transformation d'un texte en clair en texte chiffré.
- **Déchiffrement**
  Retour du texte chiffré au texte en clair.
- **Clé**
  Information secrète utilisée pour chiffrer et déchiffrer.
- **Algorithme de chiffrement**
  Méthode mathématique pour chiffrer/déchiffrer (ex. : AES, RSA).
- **Texte en clair**
  Ces données sont lisibles et compréhensibles par rapport au texte chiffré.
- **Texte chiffré**
  Le texte chiffré est le résultat de l'utilisation du cryptage pour effacer les données.
- **Crypter**
  Brouiller l'information, la rendre "incompréhensible".
- **Décrypter**
  Trouver un message clair qui correspond au message chiffré sans la clé de déchiffrement.

6. Les objectifs de la cryptographie

La cryptographie est l'étude des techniques mathématiques qui sont utilisées pour accomplir plusieurs objectifs pour garantir la sécurité de communication, ces objectifs sont :

- **Confidentialité**
  Les informations ne sont accessibles qu'aux utilisateurs autorisés.
- **Intégrité**
  Garantit que les informations n'ont pas été manipulées.
- **Authentification**
  Confirme l'authenticité des informations ou l'identité d'un utilisateur.
- **Non-répudiation**
  Empêche un utilisateur de nier des engagements ou des actions antérieurs.

7. Types de cryptographie

En général, il existe deux types de cryptographie :

A. La cryptographie classique

Dans la cryptographie classique, la méthode et la clé de chiffrement ainsi que celle de déchiffrement sont connues par l'émetteur et le destinataire.

Elle comprend des méthodes telles que :

1) **Chiffre de César :** Le chiffre de César est une méthode de chiffrement par substitution dans laquelle chaque lettre d'un texte est décalée d'un certain nombre de positions dans l'alphabet. Par exemple, avec un décalage de 3, la lettre A devient D, la lettre B devient E, et ainsi de suite. Lorsque l'on atteint la fin de l'alphabet, on revient au début (par exemple, Z devient C).
   - Chiffrement (César)

   Formule : $C = (P + k) \mod 26$

   (C) : position de la lettre chiffrée
   (P) : position de la lettre originale

(k) : décalage (clé)

- Déchiffrement

Formule : $P = (C - k + 26) \mod 26$

(P) : position de la lettre originale
(C) : position de la lettre chiffrée

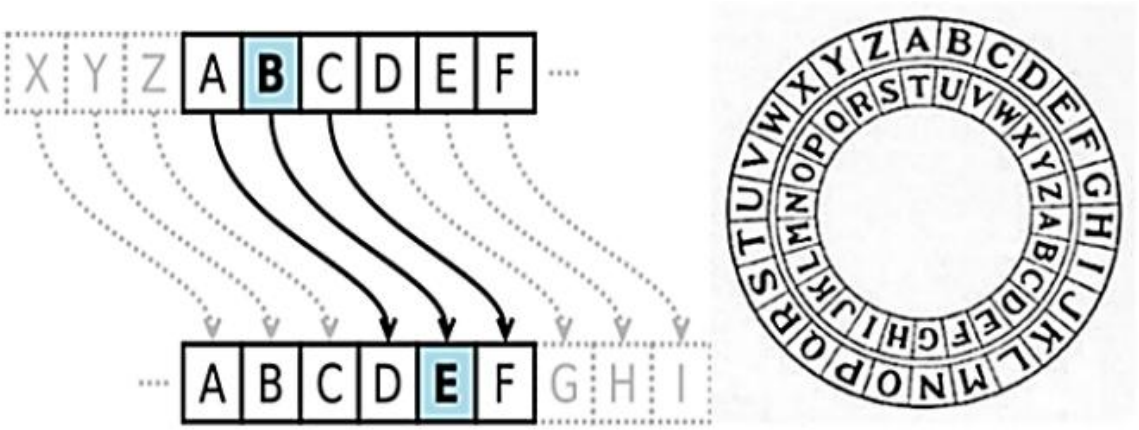

Figure 5 : Chiffrement de césar

2) **Chiffre de Vigenère :** Ce système utilise une série de décalages basés sur un mot-clé. Chaque lettre du texte clair est décalée selon la lettre correspondante du mot-clé, ce qui rend le chiffrement plus complexe que le chiffre de César.

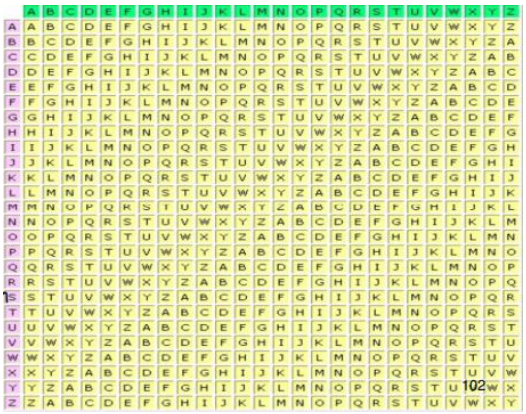

Figure 6 : Chiffre de vigenère

3) Chiffre de transposition :

Principe : Réorganise les lettres d'un message sans les modifier.

Étapes :

- Choisir une clé qui détermine l'ordre de réorganisation.
- Écrire le message dans une grille.
- Lire les lettres selon l'ordre défini par la clé.

Déchiffrement : Reconstituer la grille en utilisant la clé et lire le message dans l'ordre normal.

C'est une méthode de chiffrement basée sur la permutation des lettres.

E	C	R	I	T	U	R	E
2	1	5	4	7	8	6	3
R	A	Y	M	O	N	D	Q
U	E	N	E	A	U	E	S
T	U	N	A	U	T	E	U
R	F	A	N	T	A	S	T
I	Q	U	E				

Figure 7 : Chiffre de transposition

4) Chiffre de Playfair :

Le chiffre de Playfair est une méthode de chiffrement par substitution qui utilise des paires de lettres.

Principe

Clé : Une phrase ou un mot clé génère une grille de 5x5 lettres, combinant I et J.

Chiffrement :

- Diviser le message en paires de lettres.
- Appliquer des règles de substitution selon leur position dans la grille :
- Même ligne : remplacer par les lettres à droite.
- Même colonne : remplacer par les lettres en dessous.
- Rectangle : échanger les lettres aux coins opposés.

Déchiffrement :

- Inverser le processus de chiffrement.

Le chiffre de Playfair offre une sécurité supérieure aux simples chiffres de substitution en utilisant des paires de lettres.

5) Chiffre de Hill :

Le chiffre de Hill est une méthode de chiffrement par substitution utilisant des matrices.

Principe

Clé : Une matrice carrée (2x2 ou 3x3) avec un déterminant non nul et coprime à 26. (Cela signifie que le déterminant de la matrice doit être un nombre qui n'a pas de diviseur commun avec

26, afin d'assurer que l'inverse de la matrice existe dans le contexte du chiffrement.)

Message : Convertir les lettres en vecteurs numériques (A=0, B=1, ..., Z=25).

Chiffrement :

- Diviser le message en blocs correspondant à la taille de la matrice.
- Multiplier chaque vecteur par la matrice clé et appliquer le modulo 26.

$$\begin{pmatrix} C_k \\ C_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_k \\ P_{k+1} \end{pmatrix} \pmod{26}$$

Déchiffrement :

- Utiliser l'inverse de la matrice clé pour retrouver le message original.

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \pmod{26}$$

Le chiffre de Hill permet de chiffrer plusieurs lettres simultanément, offrant une sécurité accrue.

A. La cryptographie moderne

La cryptographie moderne se compose de deux grandes familles selon le principe de Fonctionnement, comme montre la figure

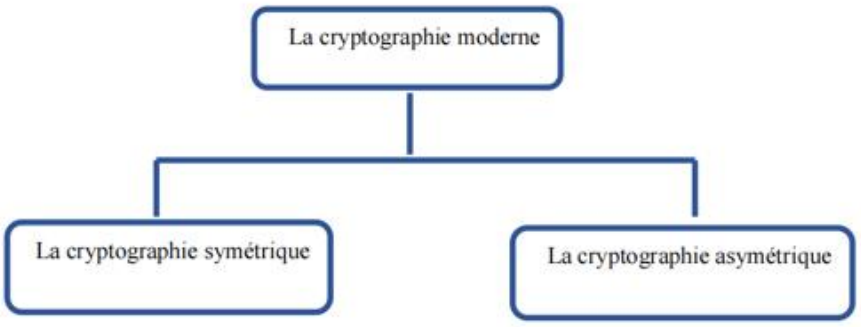

Figure 8 : Les méthodes de la cryptographie moderne.

- Cryptographie symétrique (AES 'Advanced Encryption Standard', DES 'ChaCha20', 3DES).
- Cryptographie asymétrique (RSA'Rivest–Shamir–Adleman', ECC 'Elliptic Curve Cryptography').

1. La cryptographie symétrique (ou à clé secrète)

La cryptographie symétrique, également appelée cryptographie à clé secrète, est l'une des plus anciennes formes de chiffrement. Elle repose sur l'utilisation d'une même clé pour le chiffrement et le déchiffrement du message.

Les algorithmes les plus connus appartenant à cette catégorie sont : AES, DES, 3DES, RC4, etc.

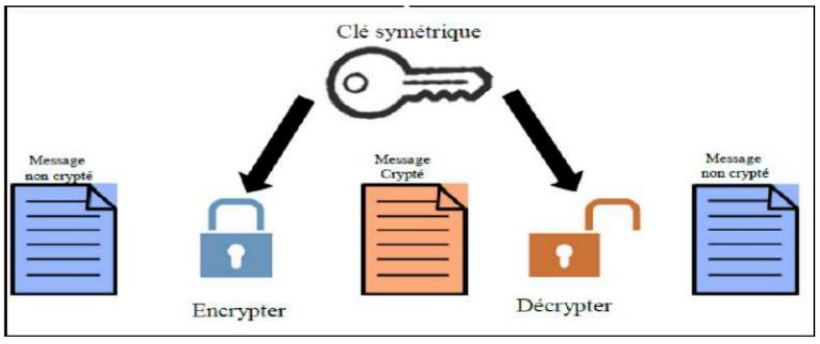

Figure 9 : La cryptographie symétrique

- **Data Encryptions Standard (DES)**

Il s'agit d'un chiffrement symétrique de 64 bits qui utilise 8 bits (un octet) comme contrôles de parité (pour vérifier l'intégrité de la clé). Chaque bit de parité de la clé (1 tous les 8 bits) permet de vérifier un des octets de la clé de parité impaire, c'est-à-dire que chacun octet auquel il appartient. La clé a donc une longueur "utilisable" de 56 bits, ce qui signifie que seuls 56 bits ont été effectivement utilisés dans l'algorithme.

- **Advance Encryptions Standard (AES)**

L'algorithme accepte un bloc de 128 bits (16 octets) en entrée, la longueur de clé est de 128, 192 ou 256 bits. Les 16 octets d'entrée sont permutés selon une table prédéfinie. Ces octets sont ensuite placés dans une matrice 4x4 et leurs lignes sont tournées dans le sens des aiguilles d'une montre. La taille du pas de rotation varie en fonction du numéro de ligne. Une transformation linéaire est ensuite appliquée à la matrice, consistant en une multiplication binaire de chaque élément de la matrice par polynômes de la matrice auxiliaire. Cette multiplication obéit à certaines règles selon GF (28) (groupe de Galois ou corps fini).). La transformée linéaire permet une meilleure diffusion (étalement des bits dans la structure) sur plusieurs décalages.

Les deux principales familles de chiffrement en cryptographie symétrique :

- **Chiffrement par blocs (Bloc cipher) :** L'image est divisée en blocs traités indépendamment, ce qui assure robustesse et sécurité, mais

Peut introduire des artefacts visuels en cas d'attaque partielle (ex : AES en mode CBC).

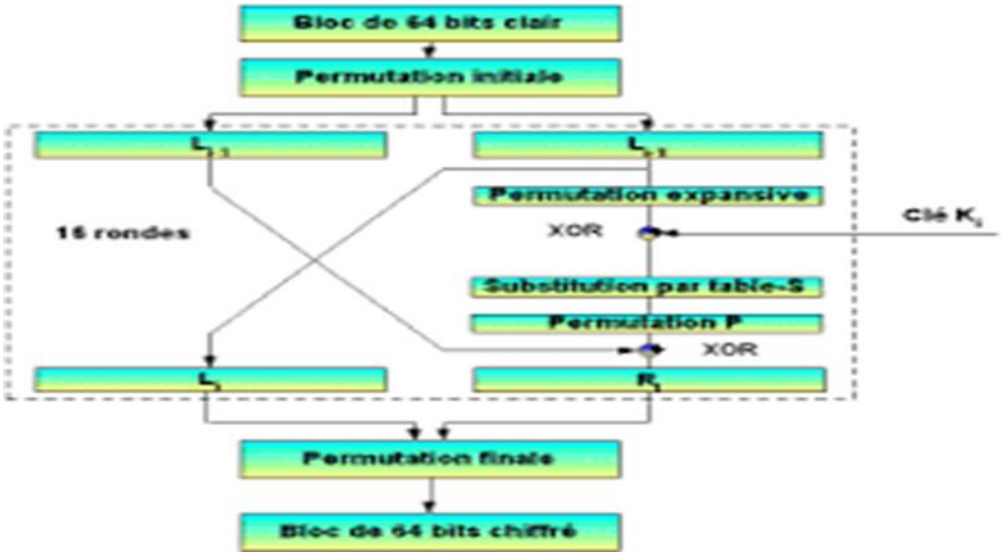

Figure 10 : Chiffrement par blocs.

- **Chiffrement par flux (Stream cipher) :** Chaque pixel est chiffré individuellement selon un flux de clés, ce qui le rend adapté aux images en temps réel et aux applications nécessitant un faible délai (ex : RC4**).**

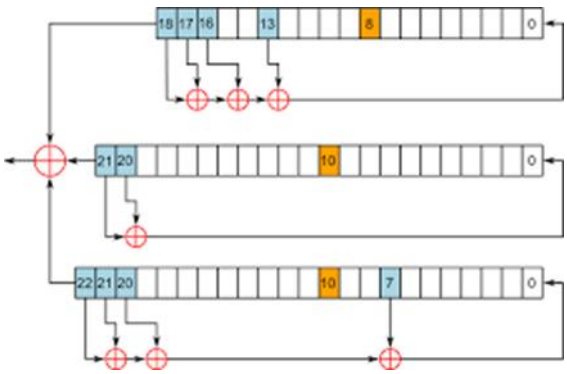

Figure 11 : Chiffrement par flux.

Ces classifications permettent de mieux comprendre les choix d'algorithmes adaptés aux contraintes du chiffrement des images, en fonction du niveau de sécurité, des performances et de l'usage visé.

2. La cryptographie asymétrique ou à clé public

Le principe de chiffrement asymétrique (appelé aussi chiffrement à clés publiques) est apparu en 1976, avec la publication d'un ouvrage sur la cryptographie par Whitfield Diffie et

Martin Hellman. Dans un cryptosystème asymétrique (ou cryptosystème à clés publiques), les clés existent par paires :

- Une clé publique pour le chiffrement.
- Une clé secrète pour le déchiffrement

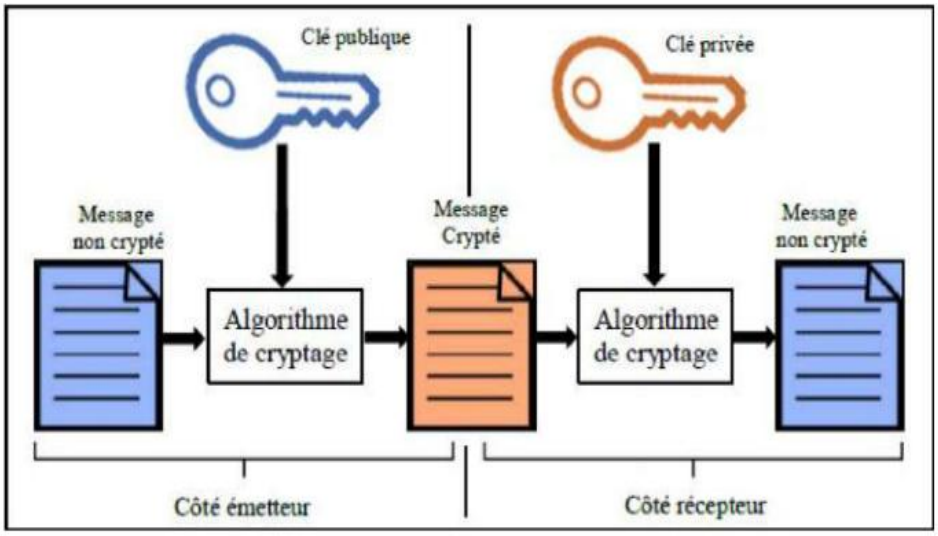

Figure 12 : Cryptographie asymétrique

- **Rivest, Shamir et Adleman (RSA)**

L'algorithme RSA est le premier algorithme qui peut être utilisé à la fois pour le

Chiffrement des données et les signatures numériques. La sécurité de l'algorithme RSA dépend de la difficulté à décomposer de grands nombres. Les deux grands nombres premiers sont utilisés pour construire la clé publique et la clé privée. On estime que la difficulté de deviner le texte en clair à partir de la clé et du texte chiffré est équivalente à la difficulté de factoriser le produit de deux grands nombres premiers

8. Comparaison entre la cryptographie symétrique et asymétrique

Voir le tableau

Critère	Cryptographie Symétrique	Cryptographie Asymétrique
Nombre de clés	Une seule clé secrète	Deux clés (publique et privée)
Sécurité	Moins sécurisée en cas de partage de clé	Plus sécurisée mais plus lente
Vitesse d'exécution	Très rapide	Plus lent en raison des calculs complexes
Exemples d'algorithmes	AES, DES	RSA
Utilisation principale	Chiffrement de données massives	Échange sécurisé de clés et authentification

Tableau 1 : Comparaison entre la cryptographie symétrique et asymétrique

9. Cryptage hybride

A cryptographie hybride fait appel aux deux grandes familles de systèmes cryptographiques : la cryptographie asymétrique et la cryptographie symétrique. Les logiciels comme PGP et GnuPG reposent sur ce concept qui permet de combiner les avantages des deux systèmes.

10. Applications modernes de la cryptographie

- **Blockchain et cryptomonnaies :** Utilisation de la cryptographie pour sécuriser les transactions.
- **Sécurisation des communications :** Protocoles TLS, SSL, VPN.
- **Authentification et contrôle d'accès** : Biométrie, cartes à puce.
- **Stockage sécurisé des données :** Bases de données chiffrées.

11. Cryptographie et intelligence artificielle

- **Utilisation de l'IA en cryptanalyse :** Attaques basées sur la machine learning

- **Chiffrement homomorphique appliqué à l'IA :** Protection des données sensibles tout en permettant leur traitement.

12.Les types d'attaques

Différents types d'attaques de chiffrement sont décrits ci-dessous :

- **Attaque par texte chiffré uniquement :** Le cryptanalyste analyse plusieurs messages chiffrés avec le même algorithme pour tenter de récupérer le texte en clair ou la clé utilisée, afin de déchiffrer d'autres messages.
- **Attaque en texte clair connu :** Le cryptanalyste a accès à des textes chiffrés ainsi qu'à leurs textes clairs correspondants. Son objectif est de retrouver la clé utilisée pour le chiffrement ou de développer un algorithme pour déchiffrer d'autres messages.
- **Attaque en texte clair choisi :** Ici, le cryptanalyste peut choisir les textes clairs à chiffrer. Cette méthode est plus efficace que l'attaque en texte clair connu, car elle permet de sélectionner des textes qui fournissent des informations plus pertinentes sur la clé.
- **Attaque sur texte chiffré choisi :** Le cryptanalyste choisit des textes chiffrés à déchiffrer, et les résultats lui sont fournis. Par exemple, il peut utiliser un dispositif de déchiffrement automatique pour tenter de retrouver la clé.
- **Attaque par canal auxiliaire :** Exploite des fuites d'informations physiques.
- **Attaque quantique :** Exploite la puissance des ordinateurs quantiques pour casser les algorithmes classiques.

13.Évolutions futures de la cryptographie

- **Cryptographie post-quantique :** Protection contre les ordinateurs quantiques.
- **Zero-Knowledge Proofs :** Authentification sans révélation d'information.
- **Cryptographie basée sur la théorie des réseaux :** Approche émergente pour la sécurisation des systèmes modernes.

14.Conclusion

Ce chapitre a introduit les concepts fondamentaux de la cryptographie ainsi que ses principales techniques. La suite de ce document explorera en détail l'application de la cryptographie aux images et les méthodes de protection associées.

Chapitre 2 : Image et algorithmes de cryptage d'image

Chapitre 2 : Image et algorithmes de cryptage d'image

1. Introduction

Les images numériques représentent une forme cruciale de données sensibles dans de nombreux domaines, tels que la médecine, la justice, la défense et les communications. Protéger ces images contre l'accès non autorisé, l'interception ou l'altération est devenu une exigence incontournable. Le chiffrement d'image offre une solution robuste à ce problème, en rendant le contenu visuel illisible à toute personne ne possédant pas la clé de déchiffrement.

Cependant, appliquer les algorithmes de chiffrement classiques aux images pose plusieurs défis : la taille volumineuse des fichiers, la forte redondance spatiale et la nécessité de préserver la qualité visuelle. Cela a conduit à l'adaptation et à l'optimisation de certains algorithmes de cryptographie, voire au développement de méthodes dédiées.

2. Notions de Base sur l'Image

a) Définition de l'image

Une image peut être définie comme une fonction bidimensionnelle, f (x, y), où x et y sont des coordonnées spatiales (plan), et l'amplitude de f à n'importe quelle paire de coordonnées (x, y) s'appelle l'intensité ou le niveau de gris de l'image à ce point

b) Image numérique

Une image numérique est une image (dessin, icone, photographie...) créée, traitée, stockée sous forme binaire (suite de 0 et de 1). Lorsqu'on agrandit une image numérique, on voit que celle-ci est composée d'un ensemble de "points", appelés pixels.

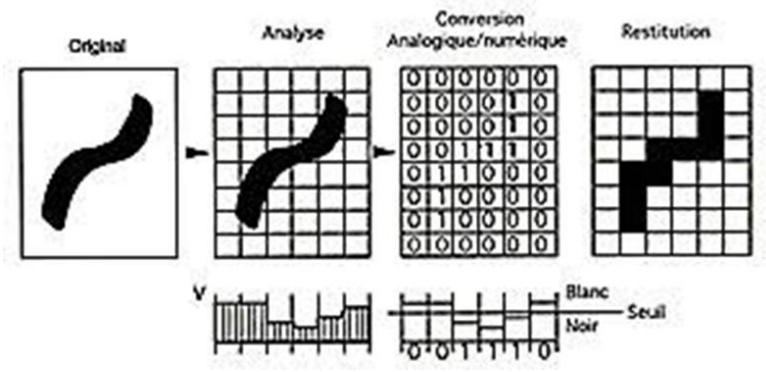

Figure 13 : Image numérique

c) Caractéristiques d'une image numérique

- **Pixel**

Le pixel (abréviation venant de l'anglais : Picture élément) est l'élément de base d'une image ou d'un écran, c'est-à-dire un point. L'ensemble de ces pixels est contenu dans un tableau à deux dimensions (largeur et hauteur) constituant l'image

- **Résolution**

La résolution d'une image numérique. La résolution s'exprime en Pixels par pouce (PPP) en français, Dots per inch (DPI) ou Pixels per inch (PPI) selon les pays. La résolution mesure la densité de pixels dans une image, généralement exprimée en pixels par pouce (ppi) ou en points par pouce (dpi). Une résolution élevée signifie une meilleure qualité d'image, tandis qu'une résolution faible entraîne une perte de détail et un effet pixélisé.

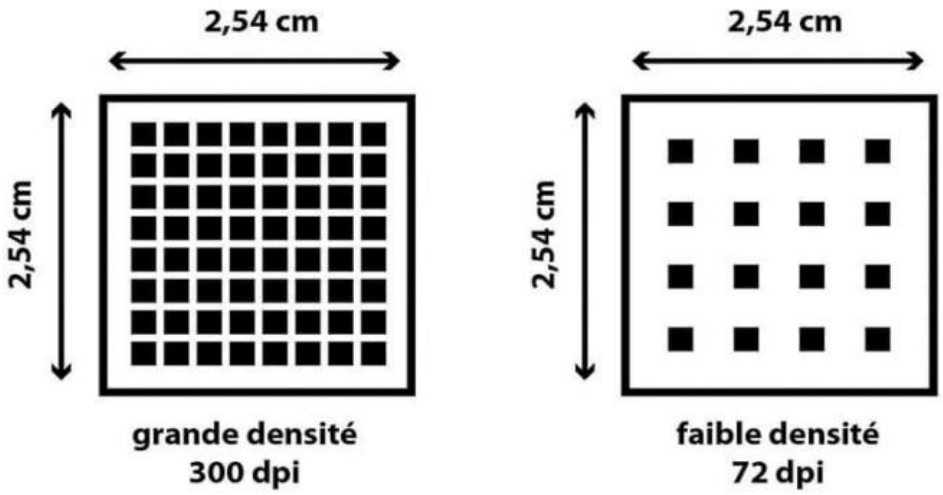

Figure 14 : Schéma explicatif de la résolution de l'image numérique

- **Taille :**

La **taille** d'une image correspond à ses dimensions physiques lorsqu'elle est imprimée ou affichée, exprimées en centimètres ou pouces. Elle ne doit pas être confondue avec la **définition** (nombre total de pixels) ni avec la **résolution** (pixels par pouce, ppp). La taille d'impression d'une image dépend de sa définition et de sa résolution.

3. Types d'image numérique

Il existe deux grandes familles d'images numériques matricielle et vectorielle :

a) Les images matricielles

Les images matricielles (ou bitmap) sont constituées d'une matrice de pixels. Chaque pixel possède une valeur spécifique correspondant à une couleur ou une intensité lumineuse. Ce type d'image est couramment utilisé en photographie et en affichage numérique. Cependant, elles perdent en qualité lorsqu'elles sont agrandies.

b) Les images vectorielles

Les images vectorielles sont composées de formes géométriques définies par des équations mathématiques (lignes, courbes, polygones). Contrairement aux images matricielles, elles peuvent être agrandies sans perte de qualité. Elles sont souvent utilisées pour les logos, les illustrations et les graphiques.

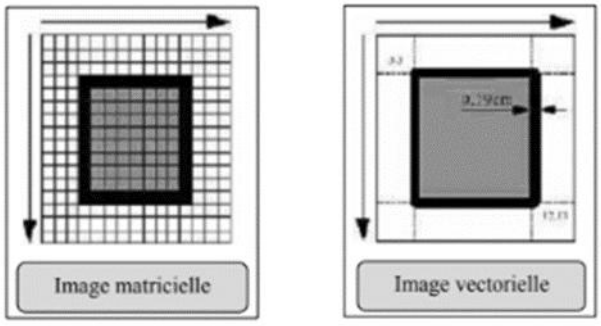

Figure 15 : Les types d'image

4. Types de formats standards d'image

Un format d'image est une représentation informatique de l'image. Il existe un grand nombre de formats standards d'enregistrement d'images. Nous présentons ci-après les formats de Chiers les plus utilisés :

- **JPEG (Joint Photographic Experts Group) :** Format compressé avec perte, idéal pour les photos et images riches en couleurs.
- **PNG (Portable Network Graphics)** : Compression sans perte, supporte la transparence, adapté aux logos et images avec fond transparent.
- **GIF (Graphics Interchange Format) :** Supporte les animations et la transparence, limité à 256 couleurs.
- **BMP (Bitmap) :** Format non compressé, de haute qualité mais volumineux.
- **TIFF (Tagged Image File Format) :** Qualité élevée, sans perte, utilisé en impression et photographie professionnelle.
- **SVG (Scalable Vector Graphics) :** Format vectoriel basé sur XML, idéal pour les icônes et graphiques redimensionnables sans perte de qualité.
- **WebP :** Format optimisé pour le web, offrant une bonne compression avec ou sans perte.
- **HEIF (High Efficiency Image Format) :** Format moderne offrant une meilleure compression que JPEG, utilisé notamment par Apple.

5. Les différents modes de couleurs des images

a) Mode binaire (Noir et Blanc)

Le mode binaire représente une image en utilisant seulement deux couleurs : noir et blanc (0 ou 1). Il est utilisé dans les impressions simples et les images à haute lisibilité.

Figure 16 : Mode binaires (noirs et blancs)

b) Mode niveau de gris

Ce mode représente une image avec des nuances de gris allant du noir au blanc. Chaque pixel peut prendre une valeur correspondant à une intensité lumineuse entre 0 (noir) et 255 (blanc).

Figure 17 : Mode de niveau gris

c) Mode couleur (RVB)

Le mode RVB (Rouge, Vert, Bleu) est basé sur la synthèse additive des couleurs. En combinant différentes intensités de ces trois couleurs primaires, il est possible de reproduire une large gamme de couleurs. Ce mode est largement utilisé pour les écrans et la photographie numérique.

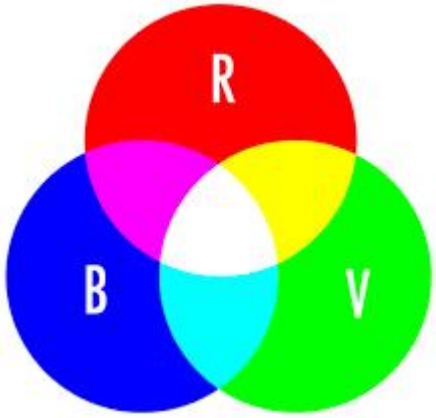

Figure 18 : Représentation des différents modes de couleur en informatique

6. Chiffrement d'image

a) Principe du chiffrement d'image

Le chiffrement d'image est basé sur la modification des valeurs des pixels de manière à ce qu'elles soient illisibles sans la clé de déchiffrement. Ce processus peut également impliquer la modification des bits des pixels pour les rendre aléatoires. En plus de l'opérateur XOR, d'autres techniques comme la permutation ou le chiffrement par blocs peuvent être utilisées.

7. Méthodes de chiffrement d'images

Les images numériques diffèrent des données textuelles en raison de leur taille plus volumineuse et de la possibilité de compression avec perte. Ainsi, les méthodes de chiffrement des images sont adaptées et se divisent en deux grandes catégories :

a) Méthodes dans le domaine spatial

Le chiffrement agit directement sur les pixels en détruisant leur corrélation, rendant l'image incompressible.

Deux approches existent :

- Considérer le pixel comme l'unité de base.
- Travailler au niveau des bits d'un pixel (par exemple, 8 bits pour une image en niveaux de gris).
- La reconstruction de l'image d'origine est possible sans perte d'informations.

b) Méthodes dans le domaine fréquentiel

- Basées sur la transformation des fréquences de l'image.
- Le déchiffrement entraîne généralement une perte d'informations.

8. Défis du chiffrement des images

- **Équilibre entre sécurité et efficacité :** Les algorithmes de chiffrement robustes (RSA, AES) nécessitent une puissance de calcul élevée, ce qui peut poser problème pour les grandes images.
- **Maintien de la qualité d'image :** Lorsqu'une image est chiffrée et compressée, une perte de détails peut survenir, ce qui est critique pour les images médicales ou judiciaires.
- **Vitesse de chiffrement et de déchiffrement :** Certaines applications (comme la diffusion vidéo sécurisée) nécessitent un chiffrement rapide sans délai excessif.
- **Risques de cyberattaques :** Les images chiffrées peuvent être ciblées par des attaques, comme les attaques par force brute (Brute Force) ou l'analyse de motifs (Pattern Analysis) pour tenter de casser le chiffrement.

9. Critères de sélection d'un algorithme de chiffrement d'image

Pour être efficace, un algorithme de cryptage d'image doit répondre à plusieurs critères essentiels :

Sécurité : il doit résister aux attaques classiques (force brute, analyse statistique, attaque par texte clair connu, etc.).

Efficacité : le temps de chiffrement et de déchiffrement doit être raisonnable, surtout pour les images de grande taille.

Maintien de la qualité : le processus de chiffrement ne doit pas altérer de manière significative la qualité perceptible de l'image.

Sensibilité à la clé : une légère modification de la clé doit produire un résultat chiffré complètement différent.

Résistance à la compression : dans certains cas, l'image chiffrée peut être compressée ; l'algorithme doit garantir la décompression correcte sans perte de sécurité.

10. Objectifs du Chiffrement d'Images

Le chiffrement des images vise à rendre les informations qu'elles contiennent inaccessibles aux personnes non autorisées. Ce processus de protection doit être réalisé de manière à maintenir, dans la mesure du possible, la qualité de l'image tout en assurant un niveau de sécurité élevé.

11. Principaux algorithmes utilisés pour le chiffrement d'image

a) AES (Advanced Encryption Standard)

L'AES est une méthode de chiffrement symétrique par blocs, largement adoptée pour sa robustesse et son efficacité. Il fonctionne sur des blocs de 128 bits et accepte des clés de 128, 192 ou 256 bits.

Avantages :

- Très sécurisé et certifié pour des usages gouvernementaux.
- Vitesse de traitement élevée, adaptée aux applications en temps réel.
- Facilement implémentable dans différents langages et plates-formes.

Inconvénients :

- Conçu initialement pour les données textuelles ; nécessite une adaptation pour les données d'image (ex : en travaillant directement sur les octets de l'image)

b) DES (Data Encryption Standard)

Le DES est l'un des plus anciens algorithmes symétriques à clé secrète, fonctionnant sur des blocs de 64 bits avec une clé de 56 bits.

Avantages :

- Simplicité de mise en œuvre.
- Historiquement important dans l'évolution de la cryptographie.

Inconvénients :

- Clé courte, vulnérable aux attaques par force brute.
- Aujourd'hui considéré comme obsolète pour des applications sensibles.

c) RSA (Rivest-Shamir-Adleman)

RSA est un algorithme de cryptographie asymétrique basé sur la factorisation de grands nombres premiers. Il utilise une paire de clés : une publique pour chiffrer et une privée pour déchiffrer.

Avantages :

- Excellente sécurité grâce à la complexité mathématique.
- Idéal pour le partage de clés dans les systèmes hybrides.

Inconvénients :

- Lourd en calcul, surtout pour les grands fichiers image.
- Pas adapté pour chiffrer directement de grandes images; souvent utilisé pour chiffrer la clé d'un algorithme symétrique.

d) Chaos (Chiffrement basé sur les systèmes dynamiques)

Le chiffrement chaotique repose sur les propriétés des systèmes dynamiques non linéaires comme la sensibilité aux conditions initiales, l'imprévisibilité et la pseudo-aléa. Ces propriétés permettent de générer des séquences complexes et difficilement prévisibles, idéales pour brouiller l'image.

Dans notre projet, un système chaotique simple (carte logistique) est utilisé pour générer un masque pseudo-aléatoire. Ce masque est appliqué à l'image d'origine pour permuter les pixels et modifier leurs valeurs via une opération XOR. Cela rend l'image chiffrée totalement illisible sans connaître les paramètres du système chaotique.

Avantages :

- Très grande sensibilité à la clé (petite variation ⇒ grand changement)

- Rapidité d'exécution
- Bonne efficacité pour des images de grande taille

Inconvénients :

- Moins standardisé que AES/RSA
- La sécurité dépend fortement du choix des paramètres initiaux

Cette méthode offre un bon compromis entre simplicité, rapidité et sécurité, surtout lorsqu'elle est combinée avec d'autres méthodes comme l'encodage en Base64 ou l'usage hybride RSA-AES.

12. Comparaison entre les algorithmes

Algorithme	**Type**	**Sécurité**	**Vitesse**	**Adaptation aux images**
AES	Symétrique	Élevée	Rapide	Bonne (avec adaptation)
DES	Symétrique	Faible (obsolète)	Moyenne	Moyenne
RSA	Asymétrique	Très élevée	Lente	Faible (clé uniquement)
Chaos	Non-linéaire / dynamique	Moyenne à élevée (selon paramétrage)	Très rapide	Très bonne

Tableau 2 : Comparaison entre les algorithmes

13. Application pratique dans le projet

Dans le cadre de notre projet, les trois algorithmes suivants ont été implémentés dans une application Java :

AES pour le chiffrement rapide et sécurisé des images.

DES à des fins comparatives, malgré ses faiblesses.

RSA utilisé pour sécuriser les clés (approche hybride).

Ce choix permet d'évaluer la performance, la sécurité et la flexibilité de chaque méthode dans le contexte spécifique du traitement d'images numérique

Nous avons également implémenté un algorithme basé sur le chaos, utilisant la carte logistique pour effectuer une permutation et diffusion des pixels. Cette méthode a montré de très bons résultats en termes de vitesse et de complexité visuelle des images chiffrées.

14. Conclusion

Le choix de l'algorithme de chiffrement est déterminant pour garantir la sécurité des images numériques sans compromettre leur qualité ni leurs performances d'utilisation. En combinant plusieurs techniques (comme dans les approches hybrides), il est possible de bénéficier des avantages de chaque méthode tout en atténuant leurs faiblesses Ainsi, une compréhension fine des caractéristiques des algorithmes AES, DES, RSA, ainsi que des méthodes émergentes comme le chiffrement chaotique, permet de choisir une solution adaptée aux besoins spécifiques en matière de sécurité, de performance et de qualité d'image.

.

Chapitre 3 : Analyse et Conception

1. Introduction

La phase d'analyse et de conception constitue un pivot fondamental dans le processus de développement logiciel. Elle permet de transformer les besoins exprimés par le client ou l'utilisateur en une architecture technique solide et cohérente. Ce chapitre présente en détail l'analyse des besoins de notre système de chiffrement d'images, sa modélisation à l'aide de diagrammes UML, ainsi que l'architecture logicielle retenue.

L'objectif de l'application étant de fournir une solution sécurisée, intuitive et extensible pour le chiffrement et le déchiffrement d'images, il est impératif d'identifier clairement les fonctionnalités attendues, d'anticiper les contraintes non fonctionnelles, et de structurer les composants selon une approche modulaire et maintenable.

2. Analyse des Besoins

2.1. Exigences Fonctionnelles (EF)

Les exigences fonctionnelles définissent les comportements attendus du système. Elles sont formulées à partir des scénarios d'usage les plus courants et des objectifs du projet. Pour notre application, les EF suivantes ont été identifiées :

EF1 – Importation d'image : L'utilisateur peut parcourir le système de fichiers pour sélectionner une image à manipuler.

EF2 – Affichage d'image : L'image sélectionnée est affichée dans l'interface utilisateur, en mode clair ou chiffré.

EF3 – Chiffrement d'image : L'utilisateur peut choisir un algorithme (AES, DES ou RSA) pour chiffrer l'image. Le résultat peut être visualisé et exporté.

EF4 – Déchiffrement d'image : À partir d'un fichier chiffré ou d'une chaîne Base64, l'utilisateur peut restaurer l'image originale.

EF5 – Génération et gestion des clés : Le système permet de générer, charger et sauvegarder des clés cryptographiques (spécialement pour RSA).

EF6 – Exportation et enregistrement : Les images claires ou chiffrées peuvent être sauvegardées sur le disque.

EF7 – Visualisation Base64 : L'utilisateur peut consulter la représentation texte Base64 de toute image chargée ou chiffrée.

2.2. Exigences Non Fonctionnelles (ENF)

Les ENF représentent les contraintes de qualité du système :

ENF1 – Sécurité : Les données traitées doivent être protégées efficacement contre toute compromission.

ENF2 – Performance : Le temps de traitement (chiffrement/déchiffrement) doit rester raisonnable, même pour des images de taille importante.

ENF3 – Extensibilité : L'architecture doit permettre l'ajout de nouveaux algorithmes ou fonctionnalités avec un minimum de modifications.

ENF4 – Portabilité : L'application doit être compatible avec tous les systèmes dotés de la JVM (Windows, Linux, macOS).

ENF5 – Ergonomie : L'interface doit être intuitive, responsive et adaptée à un usage non technique.

3. Modélisation UML du Système

La modélisation UML permet de formaliser la structure et le comportement du système avant son implémentation. Elle garantit une meilleure communication entre les développeurs et facilite la détection d'erreurs conceptuelles précoces.

3.1. Diagramme de Cas d'Utilisation

Ce diagramme décrit les fonctionnalités accessibles à l'utilisateur :

Acteur :

Utilisateur

Cas d'utilisation :

Charger une image

Chiffrer une image (AES / DES / RSA/ Chaos)

Déchiffrer une image

Afficher l'image (claire / chiffrée)

Générer / charger / sauvegarder des clés

Afficher ou copier la version Base64

Comparer

Réinitialiser

Enregistrer le résultat

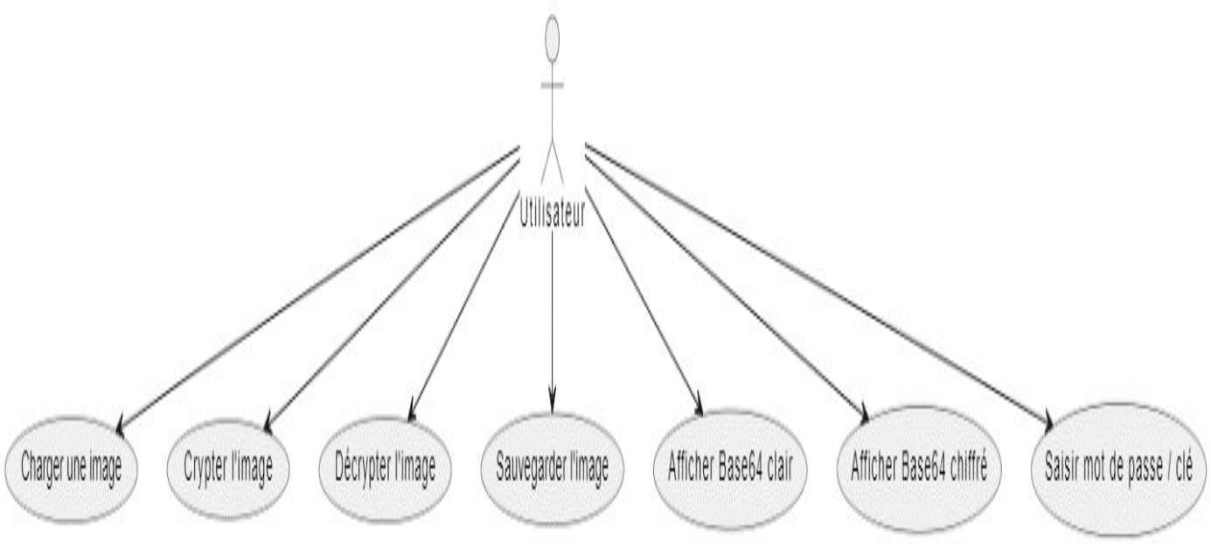

Figure 19 : Diagramme de cas d'utilisation

3.2. Diagramme de Classes

Ce diagramme structure les classes principales et les relations entre elles :

CryptoImageApp : Classe principale de l'interface graphique. Elle gère les événements utilisateur et coordonne les autres composants.

CryptoUtils : Fournit les fonctions de chiffrement/déchiffrement pour AES, DES, RSA et Chaos.

ImageUtils : Gère le traitement des images (conversion en byte[], affichage, encodage/décodage Base64).

KeyUtils : S'occupe de la génération, sauvegarde et récupération des clés RSA.

Cette structure reflète une séparation claire des responsabilités, favorisant la maintenabilité et la testabilité

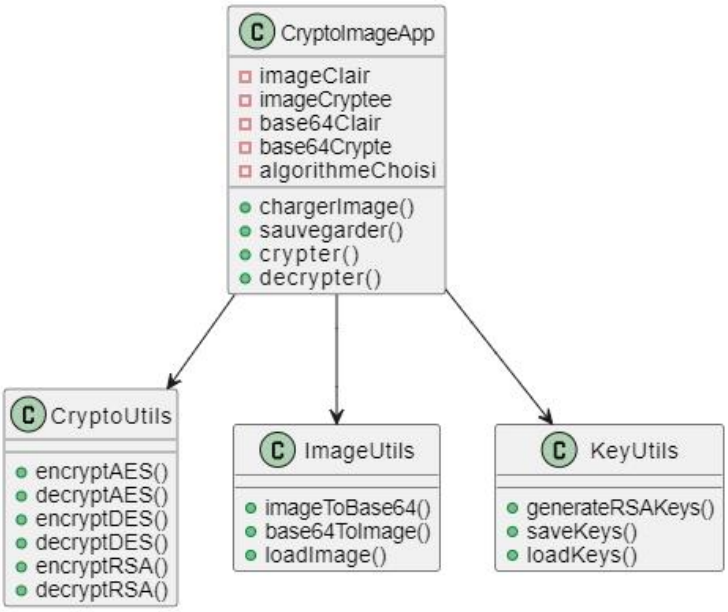

Figure 20 : Diagramme de classe

3.3. Diagramme de Séquence – Exemple : Chiffrement d'une Image

Scénario :

1. L'utilisateur clique sur "Chiffrer".
2. Le contrôleur (CryptoImageApp) appelle ImageUtils pour convertir l'image en tableau d'octets.
3. La méthode de chiffrement est invoquée dans CryptoUtils avec la clé appropriée.
4. Le résultat est renvoyé au contrôleur et affiché à l'écran.
5. La version Base64 est aussi générée pour affichage ou export.

Ce diagramme permet de vérifier que les objets coopèrent efficacement pour accomplir la tâche.

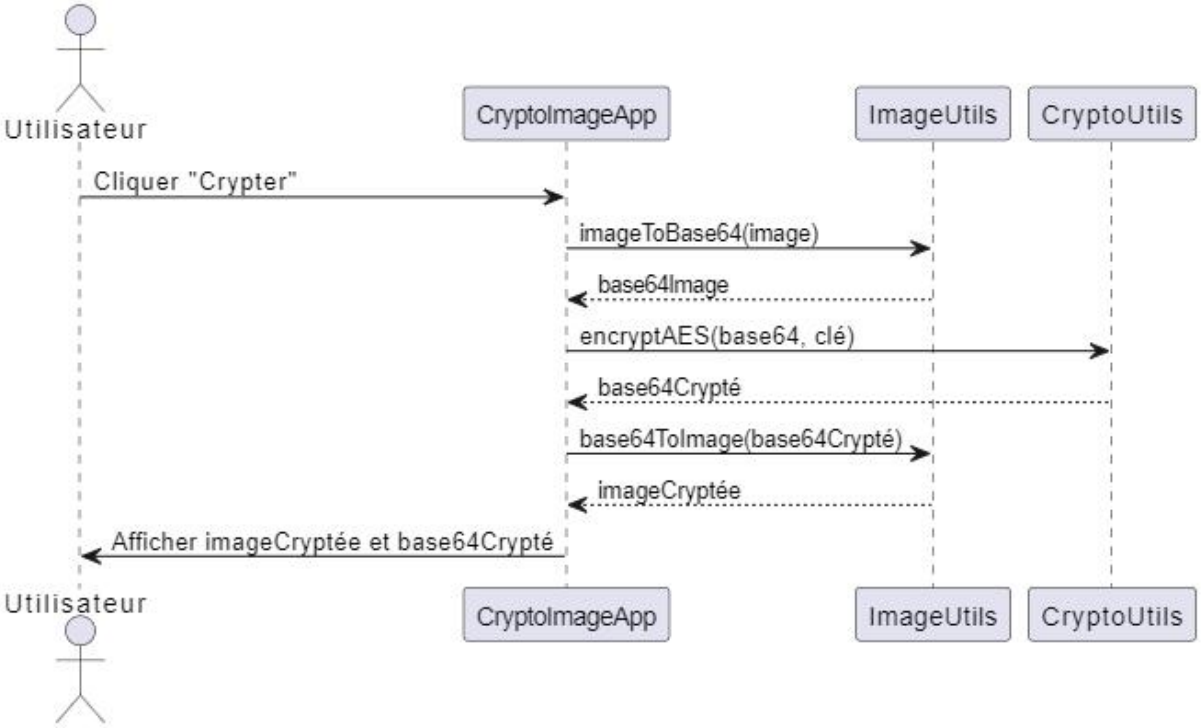

Figure 21 : Diagramme de séquence

3.4. Diagramme d'Activité – Chiffrement

- Début → Sélection de l'image → Choix de l'algorithme → Clé renseignée ou générée → Chiffrement exécuté → Résultat affiché (image + Base64) → Fin

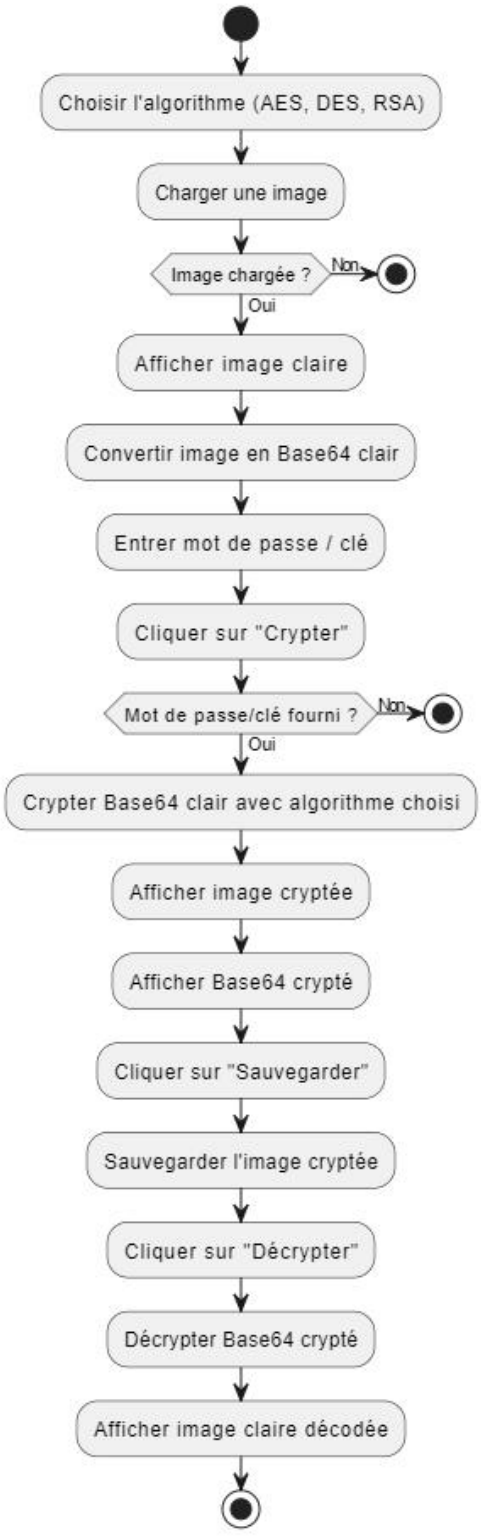

Figure 22 : Diagramme d'activité

4. Architecture du Système

4.1. Architecture Logicielle :

Modèle MVC Étendu

L'architecture adoptée est une déclinaison du modèle MVC (Modèle-Vue-Contrôleur), enrichi par des composants utilitaires :

Modèle : Gère les données métiers (images, clés, résultats chiffrés). Il centralise également les traitements cryptographiques.

Vue : Interface utilisateur Swing, offrant une interaction intuitive avec l'utilisateur.

Contrôleur : Fait le lien entre actions utilisateur et logique métier. Il coordonne les appels aux services du modèle et met à jour la vue.

Modules complémentaires

Utils : pour des traitements spécifiques (conversion Base64, lecture/écriture de fichiers, etc.)

Comparer : module indépendant pour la mesure des performances.

Cette structure rend le système facilement testable, modulaire et évolutif.

4.2. Technologies et Outils Utilisés

Justification	Choix technique	Élément
Portabilité, robustesse, POO	Java	Langage
Interface moderne, native, simple à intégrer	Java Swing + FlatLaf	GUI
Standard de sécurité Java	JCA / JCE	Chiffrement
Intégré, fiable	java.util.Base64	Encodage
Affichage graphique des performances	JFreeChart	Visualisation
Compatibilité et simplicité de manipulation	Fichier image + texte Base64	Stockage

Tableau 3: Technologie et Outils Utilisés

L'utilisation d'API standard garantit la fiabilité du système et sa conformité aux bonnes pratiques de sécurité.

4.3. Sécurité et Protection des Données

Algorithmes éprouvés : AES (256 bits), RSA (2048 ou 4096 bits), DES (à des fins pédagogiques), Chaos.

Mode de chiffrement : ECB pour la simplicité ; CBC ou GCM envisagés pour des versions futures.

Gestion des clés :

Clés symétriques générées dynamiquement.

Clés RSA sauvegardées dans des fichiers .key chiffrés.

Possibilité de protéger les clés avec mot de passe.

Approche hybride : Chiffrement de l'image avec AES, puis chiffrement de la clé AES avec RSA (modèle standard dans les systèmes modernes).

Authentification future : Signature des images et vérification d'intégrité via hachage SHA-256.

5. Conclusion

Dans ce chapitre, nous avons procédé à une analyse exhaustive des besoins du système, en distinguant les aspects fonctionnels et non fonctionnels. La modélisation UML nous a permis de formaliser les interactions et la structure logique du système, préparant ainsi une implémentation robuste et cohérente. L'architecture logicielle choisie, basée sur le modèle MVC enrichi, offre un haut degré de modularité et facilite les évolutions futures du projet.

La sécurité, pierre angulaire du système, a été abordée de manière rigoureuse, avec des algorithmes standards, une gestion responsable des clés et une perspective d'améliorations futures (authentification, signature, protocoles hybrides). L'ensemble constitue une base solide pour l'implémentation qui sera abordée dans le chapitre suivant.

Chapitre 4 :
Implémentation

Chapitre 4 : Implémentation

1. Introduction

Ce chapitre présente l'implémentation de l'application de chiffrement et de déchiffrement d'images, développée en Java. Cette application concrétise les concepts théoriques des chapitres précédents, en particulier ceux relatifs aux algorithmes cryptographiques symétriques (AES, DES), asymétriques (RSA), et chaotiques (Chaos).

L'interface graphique a été réalisée à l'aide de la bibliothèque Java Swing. L'application suit le modèle MVC (Modèle – Vue – Contrôleur), garantissant une bonne séparation des responsabilités et facilitant la maintenance.

1. Environnement de Développement

L'environnement de développement a été soigneusement choisi pour optimiser la productivité et assurer la compatibilité avec les bibliothèques nécessaires. Les détails sont les suivants :

- **Langage de programmation : Java** Standard Edition 8 ou version ultérieure
- **Interface graphique :** Java Swing
- **Environnement de développement intégré (IDE) :** NetBeans IDE
- **Librairies :**

❖ **Java Cryptography** Extension (JCE) pour la manipulation des algorithmes AES, DES, et RSA
❖ **java.util**.Base64 pour l'encodage et le décodage Base64
❖ **javax.imageio** pour la lecture et l'écriture d'images
❖ Générateur de nombres chaotiques personnalisé pour l'algorithme Chaos

1.1. Environnement matériel

Le développement a été réalisé sur un ordinateur ayant les caractéristiques suivantes :

- **Processeur** : Intel(R) Core (TM) i3-3110M CPU @ 2.40GHz
- **Mémoire vive (RAM)** : 4.00 Go
- **Disque dur** : 500 Go HDD
- **Résolution d'écran** : 1366 x 768 pixels

2.2. Environnement logiciel

2.2.1. Système d'exploitation

Système utilisé : Windows 8.1 Famille, 64 bits, architecture x64

2.2.2. Langages de programmation

2.2.2.1. Java

Java est un langage de programmation orienté objet, développé par James Gosling et Patrick Naughton chez Sun Microsystems, et lancé officiellement en mai 1995. En 2009, Oracle a acquis Sun Microsystems et a pris en charge le développement de Java.

Java se distingue par sa compilation en bytecode, qui peut être exécuté sur n'importe quel système d'exploitation via la machine virtuelle Java (JVM). Cela permet une grande portabilité des applications. La syntaxe de Java est inspirée de C++, mais elle est simplifiée, éliminant des concepts complexes comme les pointeurs et l'héritage multiple, bien que les interfaces fonctionnelles introduites dans Java 8 permettent une forme d'héritage multiple.

Java est largement utilisé pour le développement d'applications client-serveur, notamment grâce aux applets et aux servlets, ainsi qu'aux JavaServer Pages (JSP). Il a également donné naissance à divers outils et technologies, tels que JavaOS, l'Environnement d'exécution Java (JRE), et des environnements de développement comme Eclipse.

La version la plus récente, Java 23, est sortie en septembre 2024, et la prochaine version LTS, Java 25, est attendue pour septembre 2025. La portabilité du bytecode Java dépend de la qualité des JVM sur chaque système d'exploitation.

Java : choisi pour sa portabilité, sa richesse en bibliothèques, et sa compatibilité avec les interfaces graphiques via Swing.

Java permet également une manipulation facile des fichiers binaires et des flux de données, essentiels pour le traitement des images et le chiffrement.

Figure 23 : Logo de JAVA

2.2.2. Logiciel utilisé

2.2.2.1 NetBeans

NetBeans IDE est un environnement de développement intégré gratuit et à code source ouvert destiné au développement d'applications sous Windows, Mac, Linux et Solaris.

L'environnement IDE simplifie le développement d'applications Web, d'entreprise, de bureau et mobiles utilisant les plates-formes Java et HTML5. Il offre également une assistance pour le développement d'applications PHP et C/C++.

Figure 24 : Logo de NetBeans

- Justification du choix de NetBeans :

NetBeans offre une interface conviviale, une intégration fluide avec Java SE, une gestion facile des bibliothèques externes et une prise en charge native de Swing. Il permet aussi le débogage visuel, l'exécution rapide du projet, et une gestion efficace des erreurs de compilation.

2. Architecture Générale

L'architecture est basée sur le modèle MVC :

CryptoImageApp.java : Interface graphique, gestion des événements

CryptoUtils.java : Fonctions de chiffrement/déchiffrement (AES, DES, RSA, Chaos)

ImageUtils.java : Gestion des images et encodage Base64

KeyUtils.java : Gestion des clés

3. Fonctionnalités Implémentées

3.1. Chargement d'une image

L'utilisateur peut importer une image de son système de fichiers. L'image est chargée en tant qu'objet BufferedImage, affichée dans la fenêtre principale et encodée en Base64 pour une visualisation textuelle.

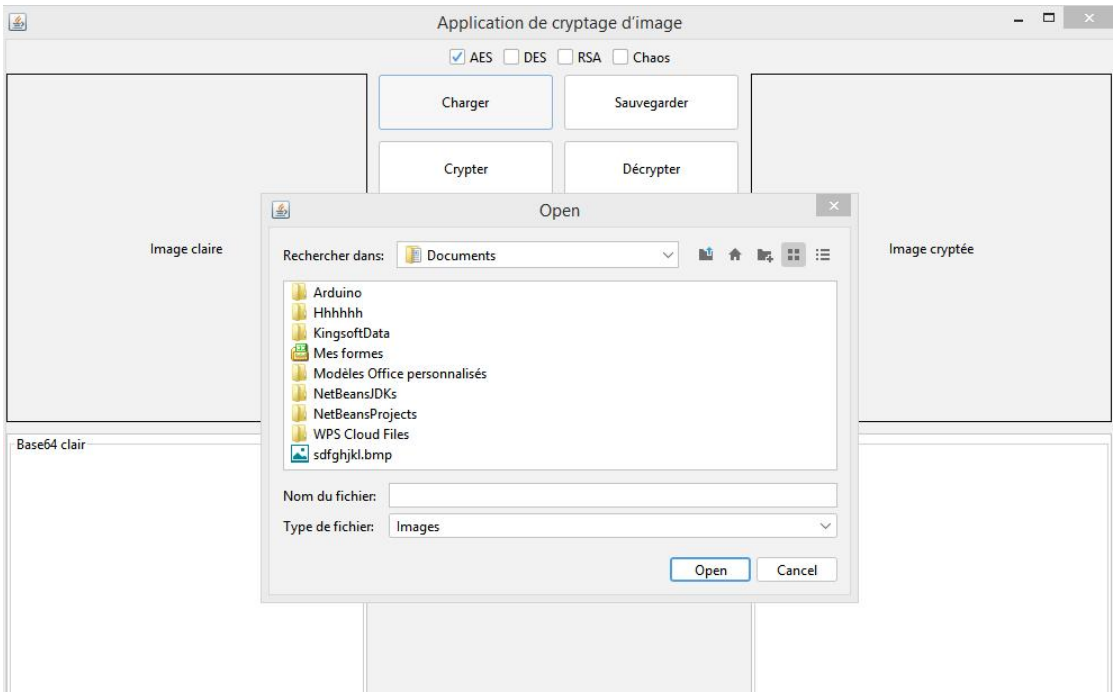

Figure 25 : Chargement d'une image

3.2. Chiffrement

L'utilisateur choisit l'un des quatre algorithmes :

AES / DES : Clé symétrique dérivée du mot de passe

RSA : Clé publique/privée

Chaos : Utilise une séquence chaotique (ex. : Logistic Map) pour brouiller les pixels

L'image est transformée en tableau de bytes, puis chiffrée selon l'algorithme sélectionné.

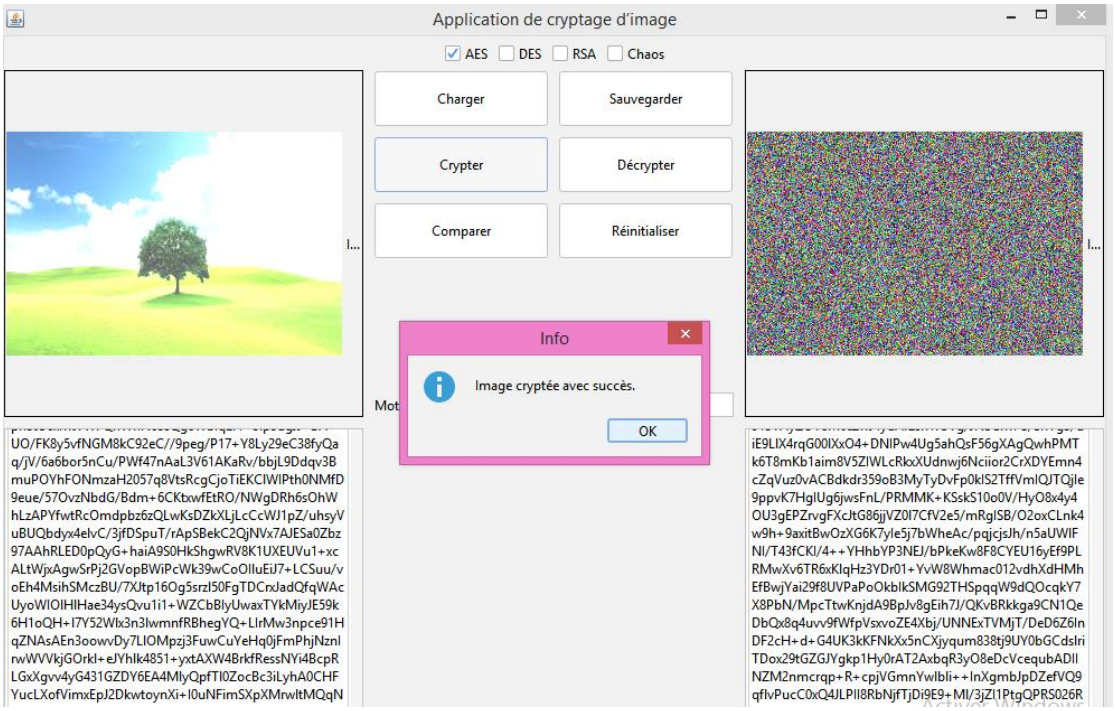

Figure 26 : Chiffrement

3.3. Déchiffrement

L'image chiffrée est reconstruite à l'aide de la clé ou des paramètres appropriés. Résultat affiché dans la zone « Image claire ».

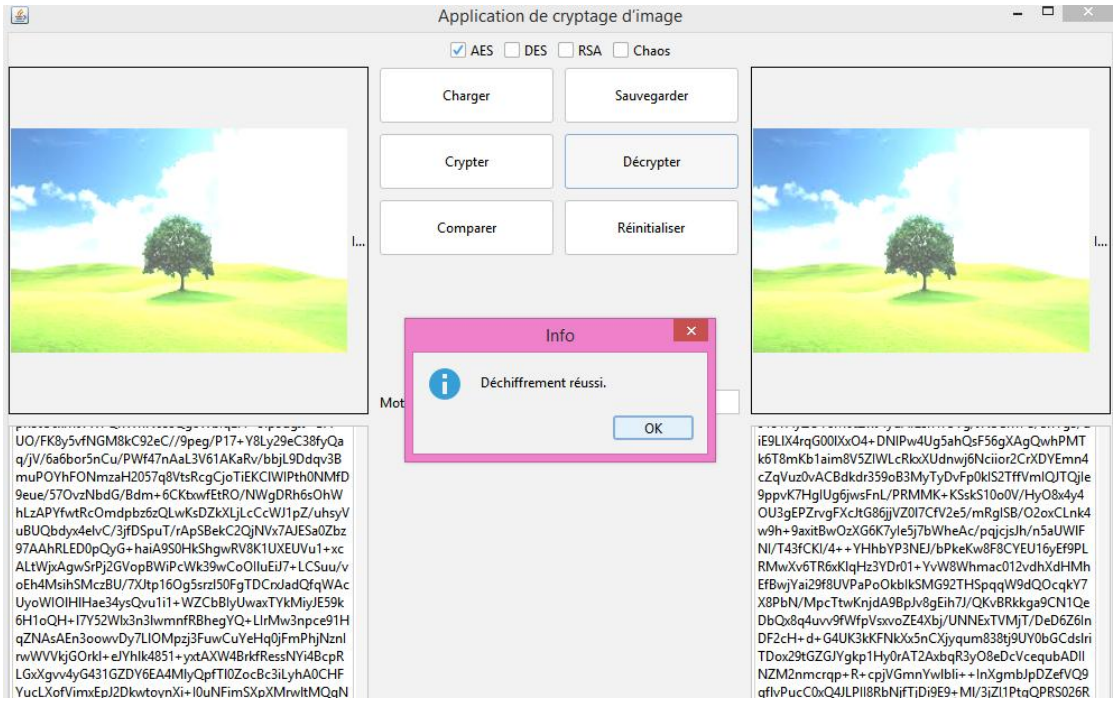

Figure 27 : Déchiffrement

3.4. Conversion Base64

Les représentations Base64 de l'image claire et chiffrée sont affichées pour consultation ou copie.

3.5. Sauvegarde

L'utilisateur peut sauvegarder :

- L'image chiffrée (binaire ou Base64)
- L'image déchiffrée ou originale

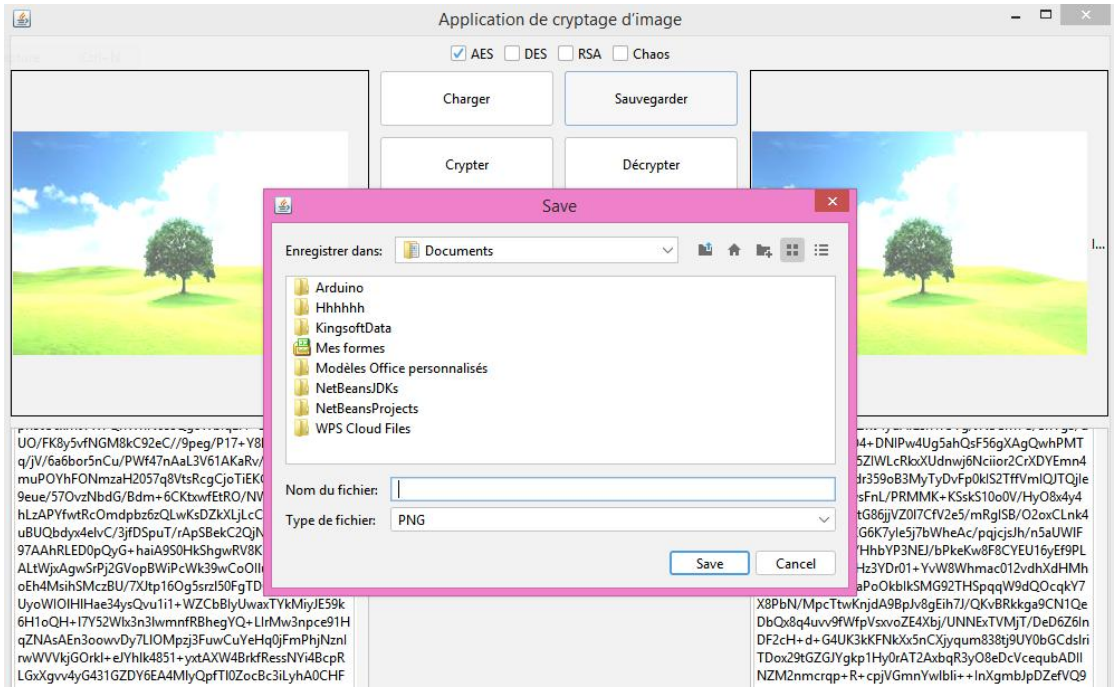

Figure 28 : Sauvegarder

3.6. Interface Graphique

L'interface (voir image) est composée de :

- Deux zones d'affichage d'image (claire et chiffrée)
- Deux zones texte pour Base64 clair et chiffré
- Un champ de saisie pour la clé ou mot de passe

Boutons fonctionnels :

Charger, Crypter, Décrypter, Sauvegarder, Réinitialiser, Comparer

Quatre cases à cocher pour sélectionner l'algorithme : AES, DES, RSA, Chaos

Elle a été conçue pour être simple, intuitive et ergonomique.

4. Résultats et Tests

Les tests ont été réalisés sur des images PNG, JPG, BMP :

- Fidélité parfaite entre image d'origine et image déchiffrée
- Conversion correcte en Base64
- RSA adapté aux images moyennes via découpage en blocs
- Chaos performant sur la confusion visuelle de l'image chiffrée

L'algorithme Chaos montre une bonne efficacité en termes de sécurité visuelle, mais son implémentation doit être soignée pour permettre un déchiffrement précis.

5. Conclusion

L'application démontre l'efficacité de la cryptographie dans la protection d'images numériques. Grâce à l'intégration des algorithmes AES, DES, RSA et Chaos, elle offre une flexibilité de choix selon les besoins de sécurité ou de performance.

Elle constitue une base solide pour des améliorations futures : chiffrement de vidéos, intégration web, ajout de signatures numériques ou stockage sécurisé sur le cloud.

Conclusion générale

1 Conclusion Générale

Importance de la Cryptographie dans le Monde Numérique

À l'ère numérique, la cryptographie s'impose comme un pilier fondamental de la sécurité de l'information. Avec l'explosion des échanges de données sur Internet et dans les systèmes connectés, la protection de ces informations est devenue une nécessité absolue. Les images numériques, en particulier, constituent une catégorie de données hautement sensibles, pouvant contenir des informations personnelles, médicales ou juridiques. Leur protection est essentielle pour garantir la confidentialité, l'intégrité et l'authenticité des échanges numériques.

La cryptographie permet de rendre les données inaccessibles à toute personne non autorisée, en les transformant en un format illisible sans la clé appropriée. Grâce à des algorithmes puissants comme AES (Advanced Encryption Standard) et RSA (Rivest-Shamir-Adleman), il est possible d'assurer une communication sécurisée, même dans des environnements à haut risque comme les systèmes de santé, les transactions financières ou les plateformes gouvernementales.

Synthèse des Résultats

Dans le cadre de ce mémoire, nous avons développé une application de chiffrement d'images numériques, permettant de chiffrer et déchiffrer des images à l'aide de plusieurs algorithmes de cryptage. Ce projet a permis de valider la faisabilité technique et l'efficacité des méthodes de chiffrement appliquées aux images, tout en maintenant une excellente fidélité entre l'image originale et l'image déchiffrée. Cela est particulièrement crucial dans des domaines tels que la médecine, où la précision visuelle ne doit souffrir d'aucune altération.

L'application dispose d'une interface graphique intuitive et ergonomique, qui rend l'outil accessible même aux utilisateurs non spécialistes. Ce choix de conception souligne l'importance de proposer des solutions sécurisées, mais également conviviales, pour favoriser leur adoption dans des contextes professionnels ou éducatifs.

Les Défis Rencontrés

Malgré les résultats positifs, plusieurs défis techniques ont émergé.

Le premier concerne le compromis entre la sécurité et la performance. Les algorithmes de chiffrement robustes tels qu'AES et RSA exigent des ressources computationnelles importantes, notamment pour le traitement des images de grande taille. Cette exigence peut affecter les performances en temps réel ou sur des appareils à ressources limitées.

Un autre défi majeur est la gestion sécurisée des clés de chiffrement. La robustesse du système repose en grande partie sur la protection de ces clés. Il est donc nécessaire d'intégrer des mécanismes fiables de génération, de stockage et de distribution des clés, tout en assurant leur confidentialité face aux tentatives d'attaque ou de compromission.

Perspectives d'Amélioration

Les résultats obtenus dans ce projet ouvrent plusieurs perspectives prometteuses :

L'une des améliorations envisageables est l'intégration de techniques de chiffrement avancées, comme le chiffrement homomorphique, qui permettrait de traiter les données sans les déchiffrer, tout en maintenant leur sécurité.

Une piste tout aussi intéressante est le chiffrement chaotique, qui repose sur des systèmes dynamiques sensibles aux conditions initiales. Ce type de chiffrement présente des avantages notables, notamment une complexité non linéaire élevée, une forte diffusion et une capacité à générer des séquences pseudo-aléatoires efficaces. Il est particulièrement adapté au chiffrement des images en raison de sa légèreté et de son efficacité face aux attaques statistiques et par analyse différentielle.

Par ailleurs, une refonte de l'interface web en version responsive et multiplateforme améliorerait l'accessibilité de l'outil, en particulier dans un contexte mobile ou collaboratif. L'ajout de fonctionnalités complémentaires, telles que la signature numérique, les certificats de sécurité ou encore la gestion multi-utilisateurs, renforcerait la fiabilité et l'adaptabilité de l'application à des environnements professionnels exigeants.

Conclusion Finale

En conclusion, ce mémoire a mis en évidence l'importance cruciale de la cryptographie dans la protection des données numériques, notamment les images. À travers la conception et la réalisation d'une application pratique, nous avons démontré la possibilité de combiner des concepts théoriques robustes avec une solution logicielle fonctionnelle.

Ce projet met également en lumière la nécessité d'une vigilance constante face aux nouvelles menaces et évolutions technologiques. Le domaine de la cryptographie est en perpétuelle mutation, notamment avec l'émergence de l'informatique quantique, qui remet en question les algorithmes classiques. Il est donc indispensable de poursuivre les recherches vers des approches plus sûres, plus rapides et mieux adaptées aux réalités du monde numérique actuel.

Conclusion générale

La sécurité des images numériques restera un enjeu critique dans les années à venir. En poursuivant les travaux entamés ici, en intégrant des techniques innovantes telles que le chiffrement chaotique, et en développant des solutions flexibles et fiables, il est possible de répondre efficacement aux défis de demain.

Bibliographie

Bibliographie

[1] W. Stallings, "Cryptography and Network Security", Pearson.

[2] National Institute of Standards and Technology (NIST), FIPS PUB 197, "Advanced Encryption Standard (AES)", 2001.

[3]. Schneier, B. (1996). Applied Cryptography. John Wiley & Sons.

[4]. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.

[5]. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography. CRC Press.

[6]. NIST (2022). Post-Quantum Cryptography Standardization. U.S. Department of Commerce.

[7]. Stallings, W. (2020). Cryptography and Network Security. Pearson.

[8]. NIST. (2001). AES Standard. FIPS Pub 197.

[10]. Kerckhoffs, Auguste. La Cryptographie militaire. (1883). Principe fondamental sur la sécurité reposant sur la clé secrète.

[11]. Shannon, Claude E. Communication Theory of Secrecy Systems. Bell System Technical Journal, 1949. Théorie de la sécurité des systèmes de communication.

[12]. Diffie, Whitfield, et Martin Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, 1976. Introduction de la cryptographie à clé publique.

[13]. Rivest, Ronald L., Adi Shamir, et Leonard M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 1978. Algorithme RSA.

[14]. Stallings, William. Cryptography and Network Security: Principles and Practice. Pearson. Ouvrage de référence sur les algorithmes symétriques (DES, AES) et asymétriques.

[15]. Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley. Explications détaillées des algorithmes classiques et modernes.

[16]. Kahn, David. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner, 1996. Histoire de la cryptographie, y compris la machine Enigma.

[17]. Biham, Eli, et Adi Shamir. Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, 1993. Analyse cryptographique du DES.

[18]. Boneh, Dan. Cryptography. Lecture notes, Stanford University. Cours moderne sur la cryptographie asymétrique et les systèmes hybrides.

[19]. Gollmann, Dieter. Computer Security. Wiley. Concepts fondamentaux de la sécurité informatique et cryptographie.

[20]. Bennett, Charles H., et Gilles Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984. Introduction à la cryptographie quantique.

[21]. Kocarev, Ljupco. Chaos-based Cryptography. IEEE Circuits and Systems Magazine, 2001. Cryptographie chaotique.

[22]. National Institute of Standards and Technology (NIST). FIPS PUB 197 : Advanced Encryption Standard (AES). 2001. Norme officielle AES.

[23]. Rivest, Ronald. The MD5 Message-Digest Algorithm. RFC 1321, 1992. Algorithme de hachage souvent utilisé en cryptographie.

[24]. www.mémoireonline.com

[25]. Bibliothèque de l'Université Cornell, Didacticiel d'Imagerie Numérique – Terminologie de Base, 2003. Présentation des noti

[23]. Avi Dixit, Dahale Bhagwan, Pratik Dhruve, Image Encryption Using Permutation and Rotational XOR Technique, SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, pp. 01–09, 2012.

[24]. A. Bayad, Introduction à la cryptographie, Université d'Évry Val d'Essonne, 2008.

[25]. Disponible sur : https://www.maths.univ-evry.fr

[26]. DR. Abdelhabib Bourouis, Sécurité informatique, Université Larbi Ben M'Hidi, Oum El Bouaghi, Année 2014/2015.

[27]. Jean De Dieu Nkapkop, Joseph Effa, Monica Borda, Laurent Bitjoka, Mohamadou Alidou, Chaotic Encryption Scheme Based on A Fast Permutation and Diffusion Structure, University of Ngaoundéré, Cameroon, 2015.

[28]. LESCOP Yves, La sécurité informatique, Post BTS R2i, 2002.

Disponible sur : http://ylescop.free.fr/mrim/cours/securite.pdf

[29]. Mme L. Saoudi, Initiation à la cryptographie, support de cours du module Sécurité informatique, Département d'informatique, Université de Msila, Année 2015/2016.

[30]. O. Poutarédy, Différences entre image Bitmap et image vectorielle, Site des enseignants en Arts Appliqués de l'académie d'Orléans-Tours, 2015.

[31]. R. Dumont, Cryptographie et Sécurité informatique, Notes de cours provisoires, Université de Liège, 2009–2010.

[32]. S. Belkacem, Chaos based image watermarking, Thèse de Doctorat en Sciences en Electronique, Université de Batna 2.

[33]. Principe de base de la cryptographie, Université Tlemcen, disponible sur : http://dspace.univ-tlemcen.dz/bitstream/112/1046/8/chapitre2.pdf

[34]. Cryptage complet/partiel d'une image/vidéo par un signal sinusoïdal, Ounzar Asma, Université Larbi Ben M'hidi, Oum El Bouaghi, Soutenance 2014-2015.