République algérienne démocratique et populaire

Ministère de l'Enseignement supérieur et de la Recherche scientifique

Université 20 Août Skikda

Faculté des Science

Département : informatique

MEMOIRE DE FIN D'ETUDE

Présenté en vue de l'obtention du Diplôme de Master

THÈME

Proposition d'un Algorithme de Cryptage des Données

- ***Présenté par :*** ***Djamai Soheib***
  Khouder abde rahmane

Membres du jury

Président du jury : Zeghida Djamel

Encadreur : Dr. Bouremel Abdelhakim

Examinateur : Belaid Hassina

Année universitaire 2023/2024

Remerciements

Avant tout nous tenons à remercier le bon Dieu le tout puissant,

Le très miséricordieux qui nous a donné la force et le courage de réaliser ce modeste travail.

Nous tenons très sincèrement à remercier mes très chers parents dont leur soutien et le conseil

Nous ont toujours affiché une clairvoyance de la vie. En préambule à ce mémoire, il m'est

Agréable de citer et adresser mes remerciements les plus sincères aux personnes qui m'ont

Apporté leurs aides et qui ont contribué à l'élaboration et au bon déroulement de ce travail :

J'ai remercié également tous ceux et celles qui ont participé de près ou de loin à l'aboutissement de cette

Concrétisation À tout le corps enseignants et le personnel du département informatique

Qui ont contribués de près ou de loin à ma formation.

Aux membres de jury qui auront à juger et ce travail et d'avoir accepté de l'examiner.

Merci Beaucoup

DÉDICACE

Nous dédions ce modeste travail aux êtres qui me sont les plus chers,

Nous citons : Les parent les plus chers au monde, que dieu les garde et les protégés.

A tous nos Amis sans exception

RÉSUMÉ

Ce document présente une technique permettant d'assurer la sécurité des fichiers de chiffrement en employant des algorithmes basés sur le chaos en relation avec l'algorithme chaotique AES. Après une introduction générale, le document se concentre sur des images et des vidéos détaillées utilisées comme informations complémentaires. Ensuite, il explore les principes du cryptage des données et du chaos qui y sont introduits par le mensonge. La conception et le développement de l'algorithme « AES Chaotique » sont proposés en détail, y compris des fonctionnalités de sécurité avancées et des fonctions d'objectifs de performance. Le même processus de mise en œuvre algorithmique est appliqué avec un résultat qui aboutit aux principes qui régissent l'utilisation de cette méthode innovante sur le mouvement vers le chaos et le cryptage des dons.

Les mots clé :

Chaos, Sécurité de cryptage, Transmission sécurisée, Algorithme AES

ABSTRACT

This document introduces a technique for ensuring the security of encryption files by employing chaos-based algorithme in relation to the AES Chaotic algorithm. After a general introduction, the document is focused on detailed pictures and videos used as supportive information. After he explored principles of cryptage of donnees and chaos that are introduced into it by lies. The design and development of "AES Chaotic" algorithm is offered in detail including advanced security features and performance objective functions. Same algorithmic implementation process is applied with an outcome that results into the principles that govern use of this innovative method on movement into chaos and cryptage of donations.

Key words:

Chaos, Encryption Security, Transmission security, Algorithme AES

Chapitre IV Implémentation

Liste des tableaux

Liste des figures

Introduction général

Introduction générale

Depuis les débuts de la civilisation, l'humanité a été préoccupée par la nécessité de préserver le secret. Le secret a été particulièrement crucial lors des luttes pour le pouvoir, puis il a évolué pour répondre aux besoins militaires et diplomatiques.

Au cours des dernières décennies, les systèmes de communication ont été complètement transformés par les nouvelles technologies et les réseaux, tant dans les transmissions numériques qu'analogiques. Aujourd'hui, des millions d'octets d'informations confidentielles sont transmis par des canaux de communication non sécurisés, et la révolution d'Internet a facilité l'échange d'informations, rendant difficile le maintien du secret.

Les informations peuvent être interceptées à tout moment par des personnes non autorisées. Les algorithmes de chiffrement traditionnels comme AES, DES ou RSA sont devenus insuffisants pour assurer la sécurité. La cryptographie, science ancienne, suscite un intérêt croissant dans de nombreux domaines (paiements sécurisés, emails confidentiels, signatures électroniques, etc.).

Face à ces défis, deux alternatives ont été développées au cours de la dernière décennie :

- La cryptographie quantique, dérivée des principes fondamentaux de la mécanique quantique

- Le codage chaotique, basé sur l'utilisation de systèmes non linéaires présentant une sensibilité extrême aux conditions initiales

L'utilisation du chaos pour sécuriser les données, notamment les images numériques, fait l'objet d'études approfondies depuis plusieurs années. Le chaos, avec ses propriétés de bruit pseudo-aléatoire et de sensibilité aux paramètres, offre des perspectives intéressantes pour masquer et confondre les informations dans les transmissions sécurisées.

Le chaos est un phénomène qui émerge des systèmes non linéaires. Il se caractérise par un comportement limite qui présente une apparence de bruit pseudo-aléatoire. Cette propriété du chaos permet de l'utiliser pour masquer ou brouiller des informations dans le cadre de transmissions sécurisées.

En effet, les signaux chaotiques possèdent des propriétés statistiques et spectrales très proches de celles d'un véritable bruit aléatoire. Leur fonction d'auto corrélation présente également un pic étroit, caractéristique d'un processus aléatoire. Cela rend ces signaux chaotiques très difficiles à distinguer d'un bruit authentique.

De plus, les systèmes chaotiques sont extrêmement sensibles aux conditions initiales. Une légère variation d'un paramètre peut entraîner un comportement complètement différent du système. Cette propriété de sensibilité aux paramètres permet de complexifier davantage le comportement chaotique, améliorant ainsi le niveau de confidentialité.

Le principe de la cryptographie par chaos consiste à utiliser ces signaux chaotiques pour masquer l'information à transmettre. À l'émission, le message est mélangé avec un signal chaotique généré localement. À la réception, un générateur de chaos synchronisé avec l'émetteur permet de retrouver le message original par soustraction du signal chaotique.

La sécurité repose alors sur la connaissance des paramètres définissant la dynamique chaotique, qui constituent la clé secrète du système. Cette approche offre ainsi une alternative intéressante aux méthodes de cryptographie classique, en exploitant les propriétés uniques des systèmes non linéaires chaotiques [1] [2][3].

Ce travail se compose de trois chapitres :

1. Notions et concepts de base de la cryptographie

2. Notions et concepts de base des systèmes chaotiques

3. Implémentation de l'approche proposée

Chapitre I

Représentation de l'image et la vidéo

I.1.Introduction

Les images et les vidéos occupent une place prépondérante dans notre vie quotidienne, que ce soit dans les médias, les communications ou les loisirs. Avec l'avènement des technologies numériques, la manière dont nous capturons, stockons, partageons et visualisons les informations visuelles a radicalement changé. Les images numériques sont devenues omniprésentes, utilisées dans divers domaines allant de la photographie professionnelle à la communication quotidienne via les réseaux sociaux. Les vidéos, quant à elles, sont essentielles non seulement pour le divertissement, mais aussi pour l'éducation, le marketing et la communication interpersonnelle.

I.2. Notions de Base des Images

I. 2.1 Définition d'une Image Numérique

Une image numérique est une représentation visuelle de données en format binaire, composée de pixels (éléments d'image). Chaque pixel est un minuscule point de couleur, et la combinaison de millions de ces points forme l'image que nous voyons sur les écrans numériques. Les images numériques peuvent être créées par divers dispositifs tels que des caméras numériques, des scanners, des téléphones portables et des logiciels de graphisme.

Les images numériques sont stockées sous forme de matrices de valeurs, où chaque valeur correspond à l'intensité et/ou la couleur d'un pixel particulier. Les images en niveaux de gris utilisent une seule valeur pour chaque pixel, représentant l'intensité lumineuse. Les images en couleur, quant à elles, utilisent plusieurs valeurs par pixel, généralement trois, correspondant aux composantes rouge (R), verte (G) et bleue (B) de la couleur, formant ainsi un modèle de couleur RGB.

I.2.2 Types d'Images Numériques

Il existe deux principaux types d'images numériques :

1-Images matricielles (raster images) : Elles sont composées de pixels disposés en une grille rectangulaire. Chaque pixel a une couleur spécifique, et la qualité de l'image dépend de la résolution, c'est-à-dire du nombre de pixels par unité de surface. Les formats courants incluent JPEG, PNG, BMP, et GIF.

2-Images vectorielles (Victor images) : Elles sont constituées de formes géométriques telles que des lignes, des courbes et des polygones, définies par des formules mathématiques.

Contrairement aux images matricielles, les images vectorielles peuvent être redimensionnées sans perte de qualité. Les formats courants incluent SVG, EPS, et PDF.

I.2.3 Paramètres Fondamentaux des Images

***Résolution* :** La résolution d'une image correspond au nombre de pixels horizontaux et verticaux qui la composent. Plus la résolution est élevée, plus l'image aura de détails fins et de netteté. Les résolutions courantes sont exprimées en pixels (ex : 1920 x 1080, 3840 x 2160, etc.).

***Profondeur de couleur* :** La profondeur de couleur, aussi appelée nombre de bits par pixel, détermine le nombre de couleurs pouvant être représentées dans une image. Plus la profondeur est grande, plus la palette de couleurs est riche. Les valeurs typiques sont:

* 1 bit/pixel : 2 couleurs (noir et blanc)

* 8 bits/pixel : 256 couleurs

* 16 bits/pixel : 65 536 couleurs

* 24 bits/pixel : 16,7 millions de couleurs (couleur vraie)

Espace colorimétrique : L'espace colorimétrique définit la façon dont les couleurs sont représentées numériquement. Les principaux espaces sont :

- RVB (Rouge, Vert, Bleu) : Additif, utilisé pour les écrans

- CMJN (Cyan, Magenta, Jaune, Noir) : Soustractif, utilisé pour l'impression

- Niveaux de gris : Représentation en noir et blanc

Taille du fichier : *La* taille du fichier image dépend de la résolution, de la profondeur de couleur et du format utilisé. Plus ces paramètres sont élevés, plus la taille du fichier sera grande. Les formats de compression comme JPEG permettent de réduire significativement la taille tout en préservant une qualité acceptable.

Métadonnées : Les métadonnées sont des informations supplémentaires stockées avec l'image, comme les paramètres de prise de vue (EXIF), les annotations, les balises, etc. Elles permettent de décrire, gérer et organiser les images.

I.3. Formats de Fichiers Image

Les images numériques peuvent être enregistrées et stockées dans divers formats de fichiers, chacun ayant ses propres caractéristiques et usages spécifiques. Voici les détails sur trois des formats de fichiers image les plus couramment utilisés : JPEG, PNG et BMP.

I.3.1 JPEG (Joint Photographic Experts Group)

* Description : Le format JPEG est l'un des formats de fichiers image les plus populaires et largement utilisés. Il est particulièrement adapté aux photographies et aux images avec des dégradés de couleur lisses.

*Compression : JPEG utilise une compression avec perte (lossy), ce qui signifie que certaines données d'image sont perdues lors de la compression pour réduire la taille du fichier. Le taux de compression peut être ajusté, offrant un équilibre entre la qualité de l'image et la taille du fichier[33].

- Avantages :

* Taille de fichier réduite, ce qui permet un stockage et un transfert rapides.
* Bonne qualité d'image pour des taux de compression modérés.
* Large compatibilité avec la plupart des logiciels et des appareils.

- Inconvénients :

* Perte de qualité d'image à chaque sauvegarde successive.
*Moins efficace pour les images avec des zones de couleur unie ou des détails fins.

I.3.2 PNG (Portable Network Graphics)

*Description : Le format PNG est un format d'image sans perte, couramment utilisé pour les graphiques en ligne, les logos et les images nécessitant une transparence.

* Compression : PNG utilise une compression sans perte (lossless), ce qui signifie que toutes les données d'image sont préservées et aucune qualité n'est perdue lors de la compression.

- Avantages :

- Prise en charge de la transparence, permettant de superposer des images sans bordure visible.
- Maintien de la qualité d'image originale, même après plusieurs sauvegardes.

- Idéal pour les images avec des zones de couleur unie, des lignes nettes et des textes.

- Inconvénients :

- Taille de fichier plus grand par rapport aux images JPEG.
- Moins adapté aux photographies en raison des tailles de fichiers plus importantes.

I.3.3 BMP (Bitmap)

* Description : Le format BMP est l'un des formats d'image les plus simples et les plus anciens. Il stocke les données d'image sous forme de matrice de pixels sans compression.

*Compression : BMP peut être compressé ou non compressé, mais la version non compressée est la plus courante, ce qui entraîne des tailles de fichier très importantes.

- Avantages :

- Structure de fichier simple et facile à manipuler.
- Qualité d'image originale préservée, sans perte due à la compression.
- Compatible avec la plupart des systèmes d'exploitation et logiciels.

- Inconvénients :

- Taille de fichier très grande, ce qui n'est pas pratique pour le stockage et le transfert.
- Pas de support pour la transparence ou les fonctionnalités avancées comme l'animation [4].

I.4. Résolution d'Image

I.4.1 Définition de la Résolution

La résolution d'une image fait référence au nombre de pixels qui composent cette image, généralement exprimée en pixels par pouce (PPI) ou en pixels par centimètre (PPC). La résolution est un indicateur clé de la qualité et de la clarté d'une image numérique. Plus la résolution n'est élevée, plus le nombre de pixels est grand, ce qui permet d'obtenir des détails plus fins et une image plus nette.

I.4.2 Influence de la Résolution sur la Qualité

La résolution d'une image a une influence directe sur sa qualité visuelle. Voici quelques points clés concernant cette influence :

- **Détails et Netteté :** Une résolution plus élevée permet de capturer et d'afficher plus de détails. Les images avec une haute résolution sont plus nettes et plus claires, même lorsque vous les agrandissez.

- **Taille de Fichier :** Les images avec une haute résolution ont généralement une taille de fichier plus grande, car elles contiennent plus de données. Cela peut affecter le stockage et la vitesse de transfert des fichiers.
- **Impression :** Pour les impressions de haute qualité, une résolution élevée est essentielle. Une image avec une faible résolution peut apparaître floue ou pixélisée lorsqu'elle est imprimée.

- **Affichage à l'Écran :** La résolution optimale pour les écrans varie en fonction de la taille et de la résolution de l'écran lui-même. Par exemple, une image destinée à être affichée sur un écran 4K doit avoir une résolution plus élevée pour tirer pleinement parti des capacités de l'écran

I.4.3 Applications Différentes Résolutions

Les différentes résolutions d'image sont utilisées pour diverses applications en fonction des besoins spécifiques en matière de qualité et de taille de fichier :

- **Web et Réseaux Sociaux :** Pour les images destinées à être partagées en ligne ou sur les réseaux sociaux, une résolution de 72 PPI est généralement suffisante. Cela permet de réduire la taille du fichier tout en maintenant une qualité acceptable pour l'affichage à l'écran.
- **Photographie Professionnelle :** Les photographes professionnels utilisent souvent des résolutions très élevées (300 PPI ou plus) pour capturer des détails fins et garantir une qualité optimale pour les impressions en grand format.
- **Impression de Documents :** Pour l'impression de documents tels que des brochures ou des flyers, une résolution de 150 à 300 PPI est recommandée. Cela garantit que les images restent nettes et détaillées lorsqu'elles sont imprimées.
- **Imagerie Médicale :** Les images médicales, comme les radiographies ou les scans, nécessitent des résolutions très élevées pour permettre une analyse détaillée et précise. Ces images sont souvent stockées en haute résolution pour ne pas perdre de détails cruciaux.
- **Graphisme et Design :** Les graphistes utilisent des résolutions élevées pour créer des illustrations et des designs qui peuvent être redimensionnés sans perte de qualité. Les fichiers vectoriels, par exemple, peuvent être agrandis ou réduits à n'importe quelle résolution sans devenir pixélisés [6].

I.5. Compression d'Image

I.5.1 Compression Avec Perte

La compression avec perte (lossy compression) est une méthode de réduction de la taille des fichiers d'image en éliminant certaines données jugées non essentielles. Cette méthode est souvent utilisée lorsque la réduction de la taille du fichier est plus importante que la préservation de la qualité d'image maximale.

- **Principe :** La compression avec perte fonctionne en supprimant les détails fins et les informations redondantes ou moins perceptibles pour l'œil humain.
- **Exemples :** JPEG (Joint Photographic Experts Group) est le format de compression avec perte le plus couramment utilisé. Il offre un bon équilibre entre qualité d'image et taille de fichier.
- **Avantage :**
  - Réduction significative de la taille du fichier.
  - Idéal pour les images destinées au web et aux réseaux sociaux.
- **Inconvénients :**
  - Perte de qualité d'image, surtout après plusieurs sauvegardes successives.
  - Peut introduire des artefacts de compression, comme des blocs ou des halos autour des objets.

I.5.2 Compression Sans Perte

La compression sans perte (lousses compression) est une méthode de réduction de la taille des fichiers d'image sans aucune perte de qualité. Tous les détails de l'image originale sont préservés, et il est possible de reconstruire exactement l'image d'origine à partir du fichier compressé[34].

- **Principe :** La compression sans perte fonctionne en utilisant des techniques qui éliminent les redondances dans les données d'image sans supprimer aucune information.
- **Exemples :** PNG (Portable Network Graphics) et TIFF (Tagged Image File Format) sont des formats couramment utilisés pour la compression sans perte.
- **Avantage :**
  - Aucune perte de qualité d'image.

- Idéal pour les images nécessitant une haute fidélité, comme les illustrations, les logos et les images médicales.

- **Inconvénients :**
  - Taille de fichier plus grande par rapport à la compression avec perte.
  - Moins efficace pour les photographies et les images complexes avec de nombreuses variations de couleur.

I.5.3 Algorithmes de Compression Courants

Différents algorithmes de compression sont utilisés pour réduire la taille des fichiers d'image tout en maintenant une qualité acceptable. Voici quelques-uns des algorithmes les plus courante:

- **JPEG :**
  - Utilise la transformation en cosinus discrète (DCT) pour convertir l'image en blocs de fréquence, puis applique une quantification pour réduire les détails moins perceptibles.
  - Idéal pour les photographies et les images web.
  - Compression avec perte.
- **PNG :**
  - Utilise une compression basée sur l'algorithme de déflation, combinant les techniques de LZ77 et de codage de Huffman.
  - Supporte la transparence et est idéal pour les images avec des zones de couleur unie et des lignes nettes.
  - Compression sans perte.
- **GIF :**
  - Utilise la méthode de compression LZW (Lempel-Ziv-Welch), adaptée aux images avec un nombre limité de couleurs (jusqu'à 256).
  - Supporte l'animation et la transparence.
  - Compression sans perte, mais avec une palette de couleurs limitée.
- **TIFF :**
  - Peut utiliser plusieurs types de compression, y compris LZW et ZIP (Deflate).

  - Idéal pour l'archivage et les applications professionnelles où la qualité de l'image est cruciale.
  - Compression sans perte.
- **WebP :**
  - Développé par Google, combine des techniques de compression avec et sans perte.
  - Offre une meilleure compression par rapport à JPEG et PNG tout en maintenant une qualité élevée.
  - Utilisé principalement pour le web [11].

I.6. Notions de Base des Vidéos

I.6.1 Définition d'une Vidéo Numérique

Une vidéo numérique est une séquence d'images en mouvement enregistrées et stockées sous forme numérique. Chaque image, appelée frame, est capturée à un intervalle de temps spécifique et enregistrée avec des informations audio et vidéo synchronisées. Ensemble, ces frames créent une illusion de mouvement lorsqu'elles sont lues à une vitesse suffisante.

- **Captation :** Les vidéos numériques sont capturées à l'aide de caméras numériques, caméscopes ou même par des dispositifs comme les smartphones.
- **Stockage :** Les vidéos sont enregistrées sous forme de fichiers numériques dans des formats spécifiques compatibles avec les systèmes de stockage et de diffusion.

I.6.2 Paramètres Fondamentaux des Vidéos

Pour comprendre et manipuler les vidéos numériques, il est important de connaître certains paramètres clés :

- **Résolution :** La résolution d'une vidéo détermine la qualité visuelle et est mesurée en pixels. Par exemple, 1920x1080 (Full HD) et 3840x2160 (4K) sont des résolutions courantes.
- **Cadence (Frame Rate) :** Le taux de rafraîchissement d'une vidéo, mesuré en frames par seconde (fps), indique combien de frames sont affichées chaque seconde. Les valeurs standard incluent 24 fps, 30 fps et 60 fps.

- **Format de Compression :** Les vidéos utilisent des codecs (encodeurs/décodeurs) pour compresser et décompresser les données vidéo et audio. Des formats comme H.264, H.265 (HEVC), et VP9 sont couramment utilisés.

I.6.3 Types de Vidéos Numériques

Il existe plusieurs types de vidéos numériques, adaptées à différents besoins et utilisations :

- **Vidéos en Direct (Streaming) :** Diffusées en temps réel sur Internet via des plateformes de streaming comme YouTube, Twitch, et Netflix.
- **Vidéos HD (Haute Définition) :** Offrent une qualité supérieure avec des résolutions de 720p (HD), 1080p (Full HD), et plus.
- **Vidéos 4K et Ultra HD :** Offrent une résolution encore plus élevée pour une expérience visuelle immersive.
- **Vidéos 360° et Réalité Virtuelle (VR) :** Capturées avec des caméras spéciales pour une vue panoramique et une immersion totale.
- **Vidéos à Cadence Élevée (Slow Motion) :** Enregistrées à une cadence plus élevée pour ralentir le mouvement et capturer des détails minutieux [16].

I.7. Formats de Fichiers Vidéo

Les vidéos numériques sont souvent enregistrées et stockées dans différents formats de fichiers, chacun ayant ses propres caractéristiques en termes de qualité, de taille de fichier et de compatibilité. Voici trois formats de fichiers vidéo couramment utilisés :

I.7.1 MP4 (MPEG-4 Part 14)

- **Description :** MP4 est un format de conteneur vidéo largement utilisé pour stocker des flux audio, vidéo, sous-titres et des données de métadonnées.
- **Compression :** Utilise des codecs vidéo comme H.264 pour la vidéo et AAC pour l'audio, offrant une bonne qualité à des tailles de fichier relativement petites.
- **Avantage :**
    - Large compatibilité avec les appareils et les plateformes.
    - Supporte la diffusion en continu et les vidéos en ligne.

- **Inconvénients :**
    - Peut avoir des limitations avec certains codecs moins répandus.

I.7.2 AVI (Audio Video Interleave)

- **Description :** AVI est un ancien format de conteneur développé par Microsoft, capable de contenir des données audio et vidéo non compressées ou compressées avec des codecs comme DivX et XviD.
- **Compression :** Peut utiliser une variété de codecs pour la vidéo et l'audio, permettant une flexibilité dans la qualité et la taille du fichier.
- **Avantage :**
    - Bonne qualité vidéo avec peu de compression.
    - Supporte les sous-titres et les pistes audio multiples.
- **Inconvénients :**
    - Taille de fichier généralement plus grande que d'autres formats plus récents.
    - Moins efficace pour la diffusion en continu et les applications modernes.

I.7.3 MKV (Matroska MultiMedia Container)

- **Description :** MKV est un format de conteneur open source capable de contenir des vidéos, des pistes audio, des sous-titres et des métadonnées dans un seul fichier.
- **Compression :** Peut utiliser divers codecs vidéo comme H.264, H.265 (HEVC), VP9 et codecs audio comme AAC, MP3, et FLAC.
- **Avantage :**
    - Supporte les vidéos de haute qualité et les résolutions élevées comme 4K et plus.
    - Prise en charge des sous-titres et des pistes audio multiples.
- **Inconvénients :**
    - Moins compatible avec certains appareils et lecteurs comparé aux formats plus populaires comme MP4.

I.8. Fréquence d'Images

I.8.1 Définition de la Fréquence d'Images

La fréquence d'images, aussi appelée cadence d'images ou frame rate en anglais, désigne le nombre d'images individuelles affichées par seconde lors de la lecture d'une vidéo. Elle est mesurée en frames par seconde (fps). Plus la fréquence d'images est élevée, plus la vidéo paraît fluide et naturelle[37].

- **Mesure :** La fréquence d'images indique combien de frames sont affichées chaque seconde. Par exemple, une vidéo à 24 fps affiche 24 images différentes chaque seconde.
- **Importance :** Une fréquence d'images élevée contribue à une expérience visuelle plus fluide et réaliste, en particulier pour les mouvements rapides ou complexes.

I.8.2 Effets sur la Fluidité Vidéo

La fréquence d'images influence directement la fluidité et la qualité visuelle d'une vidéo :

- **Fluidité :** Une fréquence d'images plus élevée produit une vidéo plus fluide, en particulier pour les mouvements rapides ou les actions dynamiques.
- **Clarté :** Une fréquence d'images plus basse peut entraîner des images saccadées ou des artefacts visuels, surtout lors de scènes rapides ou d'actions complexes.
- **Adaptation :** La fréquence d'images optimale peut varier en fonction du type de contenu et de l'application. Par exemple, les films sont souvent enregistrés à 24 fps pour un effet cinématographique, tandis que les vidéos de sport peuvent être capturées à des fréquences plus élevées pour capturer chaque détail du mouvement.

I.8.3 Applications Différentes Fréquences

Différentes fréquences d'images sont utilisées pour diverses applications et types de contenus [38]:

- **24 fps :** Standard cinématographique traditionnel utilisé dans les films et les productions vidéo.
- **30 fps :** Utilisé couramment pour la télévision, les vidéos en ligne et les jeux vidéo pour un bon compromis entre qualité et flux de travail.

- **60 fps :** Idéal pour les contenus nécessitant une haute fluidité, comme les vidéos de sport, les jeux vidéo en haute définition, et les contenus VR.

  120 fps et plus : Utilisé pour les ralentis ultra-fluides et les applications de capture de mouvement où chaque détail est critique [20].

I.9. Sécurité des Images et Vidéos

I.9.1 Menaces et Risques

La sécurité des images et vidéos numériques est confrontée à diverses menaces et risques[39] :

- **Piratage et Accès Non Autorisé :** Risque de vol d'images et de vidéos via des piratages de compte en ligne ou des accès non autorisés aux périphériques de stockage.
- **Altération et Manipulation :** Possibilité de modification non autorisée d'images et vidéos pour diffuser de fausses informations ou altérer la réputation.
- **Fuites de Données :** Risque de diffusion involontaire ou malveillante d'images et vidéos sensibles.
- **Intrusions Physiques :** Accès non autorisé aux dispositifs de capture et de stockage d'images et vidéos.

I.9.2 Techniques de Protection

Pour protéger les images et vidéos contre ces menaces, plusieurs techniques sont utilisées :

- **Chiffrement :** Utilisation de techniques de chiffrement pour sécuriser les fichiers d'images et vidéos pendant le stockage et le transfert.
- **Watermarking :** Intégration de marques invisibles ou visibles dans les images et vidéos pour identifier leur propriétaire et décourager la reproduction non autorisée.
- **Gestion des Accès :** Mise en place de contrôles d'accès stricts pour limiter qui peut voir, modifier ou télécharger des images et vidéos.
- **Surveillance et Détection :** Utilisation de logiciels de surveillance pour détecter les tentatives de piratage ou d'accès non autorisés.
- **Sauvegarde Sécurisée :** Stockage sécurisé et sauvegarde régulière des fichiers d'images et vidéos pour éviter la perte de données en cas de problème.

I.9.3 Outils et Solutions

Divers outils et solutions sont disponibles pour renforcer la sécurité des images et vidéos :

- **Logiciels de Chiffrement :** Comme VeraCrypt, BitLocker pour le chiffrement des fichiers.
- **Plateformes de Gestion de Droits Numériques (DRM) :** Offrent des solutions intégrées pour protéger le contenu multimédia.
- **Services Cloud Sécurisés :** Fournissent un stockage sécurisé avec des mesures avancées de sécurité des données.
- **Applications de Watermarking :** Comme Adobe Photoshop, qui permettent d'ajouter des waters marks aux images.
- **Firewalls et Logiciels de Sécurité :** Protègent les périphériques et les réseaux contre les intrusions et les attaques [22].

I.10. Conclusion

En conclusion, la sécurisation des images et vidéos numériques est devenue une préoccupation cruciale face aux multiples menaces telles que le piratage, la manipulation et les fuites de données. Pour répondre à ces défis, l'utilisation de techniques avancées comme le chiffrement, le watermarking, et la gestion des accès est essentielle. Ces méthodes permettent de protéger efficacement le contenu visuel contre les accès non autorisés et les altérations malveillantes, assurant ainsi la confidentialité, l'intégrité et la disponibilité des médias numériques. En combinant ces approches avec des outils modernes de sécurité informatique et une gestion proactive des risques, il est possible de garantir une utilisation sécurisée et responsable des images et vidéos dans l'environnement numérique d'aujourd'hui. Dans le chapitre suivant nous proposons une nouvelle méthode de cryptage d'image et des vidéos.

Chapitre II

Cryptage de Donnée

II.1. Introduction au Cryptage

Le cryptage, également connu sous le terme de chiffrement, est une technique essentielle pour la sécurité des données dans le monde numérique. Il consiste à transformer des informations lisibles en un format illisible pour toute personne n'ayant pas accès à une clé spécifique, assurant ainsi la confidentialité et l'intégrité des données. Le cryptage joue un rôle crucial dans diverses applications, allant de la protection des communications personnelles à la sécurisation des transactions financières et des données sensibles des entreprises.

II.2Historique du Cryptage

Le cryptage, ou chiffrement, remonte à l'Antiquité avec des techniques primitives utilisées pour sécuriser les communications militaires et diplomatiques. Depuis lors, il a évolué avec l'avènement des mathématiques et de la cryptanalyse, menant au développement d'algorithmes sophistiqués pour sécuriser les données sensibles[40].

II.3 Importance du Cryptage dans la Sécurité des Données

Le cryptage joue un rôle crucial dans la sécurité des données en protégeant leur confidentialité contre les accès non autorisés et les interceptions malveillantes. Il est essentiel dans divers domaines tels que les transactions financières, les communications gouvernementales, et la protection des informations personnelles en ligne.

II.4.Objectifs du Chapitre

Ce chapitre vise à explorer les fondements théoriques du cryptage, les différents types d'algorithmes utilisés, ainsi que leurs applications pratiques dans la sécurisation des données numériques. Il examinera également les défis contemporains et les avancées technologiques qui façonnent l'avenir du cryptage dans un monde de plus en plus connecté et numérique {1] [2] [3].

II.5.. Concepts Fondamentaux de la Cryptographie

II.5.1 Définitions Clés

La cryptographie est l'art et la science de protéger l'information en la transformant en un format illisible pour quiconque n'est pas autorisé à y accéder. Voice Quelques definitions clé[41]:

- **Chiffrement :** Processus de conversion de données lisibles en un format chiffré à l'aide d'un algorithme et d'une clé, rendant les données illisibles sans la clé de déchiffrement correspondante.
- **Déchiffrement :** Processus inverse du chiffrement, permettant de récupérer les données lisibles à partir du texte chiffré à l'aide de la clé appropriée.
- **Clé de Chiffrement :** Paramètre utilisé avec l'algorithme de chiffrement pour transformer les données. La sécurité du chiffrement dépend souvent de la complexité de la clé.

II.5.2. Types de Cryptographie

Il existe principalement deux types de cryptographie, chacun avec ses propres applications et méthodes :

- **Cryptographie Symétrique :** Utilise la même clé pour le chiffrement et le déchiffrement. Exemples : AES (Advanced Encryptions Standard), DES (Data Encryptions Standard).
- **Cryptographie Asymétrique :** Utilise une paire de clés distinctes, une publique et une privée. La clé publique est utilisée pour le chiffrement et peut être partagée librement, tandis que la clé privée est utilisée pour le déchiffrement et doit être gardée secrète. Exemples : RSA (Rivest-Shamir-Alderman), ECC (Elliptic Curve Cryptography).

II.5.3. Terminologie Courante

Pour comprendre la cryptographie, il est important de connaître quelques termes couramment utilisés :

- **Algorithme de Chiffrement :** Méthode mathématique utilisée pour transformer les données en un format chiffré.
- **Cryptanalyse :** Science de décrypter ou de briser le chiffrement pour accéder aux données sans autorisation.
- **Hachage :** Processus de transformation de données en une valeur de hachage, généralement utilisé pour vérifier l'intégrité des données.

- **Signature Numérique :** Utilisée pour vérifier l'authenticité et l'intégrité des données en ligne en utilisant des techniques de cryptographie asymétrique[18].

II.6. Algorithmes de Chiffrement Symétrique

II.6.1 Introduction aux Algorithmes Symétriques

Les algorithmes de chiffrement symétrique utilisent la même clé pour le chiffrement et le déchiffrement des données. Ils sont efficaces pour assurer la confidentialité des données en les rendant illisibles sans la clé appropriée. Voici quelques concepts clés[42]:

- **Clé de Chiffrement :** Utilisée pour transformer les données en texte chiffré.
- **Processus :** Le même algorithme est utilisé pour chiffrer et déchiffrer, nécessitant une distribution sécurisée de la clé.

II.6.2 DES (Data Encryptions Standard)

- **Description :** Le DES est un ancien algorithme de chiffrement symétrique développé dans les années 1970 par IBM. Il utilise une clé de 56 bits pour le chiffrement des blocs de données.
- **Sécurité :** Bien que robuste à l'époque de sa création, DES est maintenant considéré comme vulnérable aux attaques de force brute en raison de la taille relativement petite de sa clé.

II.6.3 AES (Advanced Encryptions Standard)

- **Description :** AES est un algorithme de chiffrement symétrique moderne adopté par le gouvernement des États-Unis comme standard de chiffrement. Il utilise des clés de 128, 192 ou 256 bits pour le chiffrement.
- **Sécurité :** AES est considéré comme sûr et efficace contre les attaques modernes en raison de la taille de ses clés et de sa structure.

II.6.4 Algorithmes Symétriques Modernes

Les algorithmes symétriques modernes sont conçus pour offrir une sécurité élevée tout en optimisant les performances. Voici quelques examples:

- **Twa Fish :** Un algorithme de chiffrement symétrique robuste avec une structure similaire à AES, utilisant des clés de 128, 192 ou 256 bits.

- **Blow Fish :** Ancien mais toujours utilisé dans certains contextes, avec une taille de clé variable jusqu'à 448 bits.
- **ChaCha20 :** Un algorithme de chiffrement à flux développé par Daniel J. Bernstein, utilisé pour des applications nécessitant une vitesse élevée et une sécurité robuste[30].

II.7. Algorithmes de Chiffrement Asymétrique

II.7.1 Introduction aux Algorithmes Asymétriques

Les algorithmes de chiffrement asymétrique utilisent une paire de clés distinctes : une clé publique pour le chiffrement et une clé privée pour le déchiffrement. Ce type de cryptographie offre des avantages significatifs en termes de sécurité et de gestion des clés par rapport aux algorithmes symétriques.

II.7.2 RSA (Rivest-Shamir-Adleman)

- **Description :** RSA est l'un des premiers et des plus populaires algorithmes de chiffrement asymétrique, nommé d'après ses inventeurs : Ron Rivest, Adi Shamir et Leonard Adleman.
- **Fonctionnement :** Basé sur la difficulté de factoriser de grands nombres premiers, RSA utilise une paire de clés : une clé publique pour le chiffrement et une clé privée pour le déchiffrement.
- **Applications :** Utilisé pour sécuriser les communications Internet, les transactions financières et la création de signatures numériques.

II.7.3 ECC (Elliptic Curve Cryptography)

- **Description :** ECC est une technique de chiffrement asymétrique basée sur les courbes elliptiques, offrant une sécurité comparable à RSA mais avec des clés plus courtes, ce qui économise des ressources.
- **Avantages :** ECC est plus efficace en termes de taille de clé et de puissance de calcul requise par rapport à RSA, ce qui le rend idéal pour les environnements avec des ressources limitées comme les appareils mobiles et l'IoT.
- **Applications :** Utilisé dans les protocoles de sécurité comme TLS (Transport Layer Security), PGP (Petty Good Privacy) et dans les systèmes de paiement sécurisé.

II.7.4 Comparaison des Algorithmes Asymétriques

Les différences entre RSA et ECC résident principalement dans la taille des clés, la performance et la résistance aux attaques :

- **RSA :**
  - Clés plus grandes (ex. 2048 bits et plus).
  - Utilisation généralisée et large compatibilité.
  - Convient aux applications nécessitant une sécurité forte et des signatures numériques robustes.
- **ECC :**
  - Clés plus courtes (ex. 256 bits).
  - Performances élevées avec une sécurité similaire à RSA.
  - Idéal pour les dispositifs avec des ressources limitées et les applications nécessitant une efficacité énergétique[32].

II.8. Protocoles de Chiffrement

II.8.1 SSL/TLS (Secure Sockets Layer/Transport Layer Security)

- **Description :** SSL/TLS sont des protocoles de sécurisation des communications sur Internet. TLS est la version plus récente et sécurisée de SSL.
- **Fonctionnement :** Assure la confidentialité et l'intégrité des données transmises entre des applications sur un réseau, comme les navigateurs web et les serveurs.
- **Applications :** Utilisé pour sécuriser les transactions en ligne, les communications par email, et d'autres protocoles Internet.

II.8.2 IP sec (Internet Protocol Security)

- **Description :** IPsec est un ensemble de protocoles utilisés pour sécuriser les communications IP à travers des réseaux non sécurisés comme Internet.
- **Fonctionnement :** Offre des services de sécurité au niveau du réseau, incluant l'authentification, le chiffrement et la gestion des clés pour protéger les paquets IP.
- **Applications :** Utilisé pour les connexions VPN (Virtual Private Network) pour sécuriser les communications à distance entre des réseaux ou des appareils individuels.

II.8.3 SSH (Secure Shell)

- **Description :** SSH est un protocole de réseau sécurisé qui permet une communication sécurisée et une gestion à distance sur des réseaux non sécurisés.
- **Fonctionnement :** Utilisé pour établir une connexion sécurisée en fournissant l'authentification forte et le chiffrement des données transitant entre les ordinateurs connectés.
- **Applications :** Principalement utilisé pour l'accès à distance aux serveurs et aux systèmes informatiques via une interface en ligne de commande.

II.8.4 Protocol PGP (Pretty Good Privacy)

- **Description :** PGP est un logiciel de cryptographie utilisé pour la protection de la confidentialité et l'authentification des données.
- **Fonctionnement :** Utilise une combinaison de chiffrement symétrique et asymétrique pour assurer la confidentialité des communications par email et la vérification de l'identité des utilisateurs.
- **Applications :** Utilisé pour sécuriser les emails, les fichiers et autres communications sensibles nécessitant une protection robuste[15].

II.9. Techniques de Cryptage Avancées

II.9.1 Chiffrement Homomorphique

- **Description :** Le chiffrement homomorphique permet d'effectuer des opérations sur des données chiffrées sans avoir besoin de les déchiffrer préalablement. Cela permet de maintenir la confidentialité des données tout en effectuant des calculs sur celles-ci.
- **Applications :** Utilisé dans des domaines tels que le calcul sécurisé en cloud, l'analyse de données confidentielles, et la protection de la vie privée.

II.9.2 Cryptographie Quantique

- **Description :** La cryptographie quantique repose sur les principes de la mécanique quantique pour sécuriser les communications. Elle utilise des propriétés fondamentales des particules subatomiques pour garantir la sécurité des échanges d'information.

- **Avantages :** Offre une sécurité inconditionnelle basée sur les lois de la physique quantique, rendant impossible l'interception ou la copie des données sans perturber leur état.
- **Applications :** Principalement explorée pour les communications ultra-sécurisées et la distribution de clés quantiques.

II.9.3 Cryptographie Basée sur le Chaos

- **Description :** La cryptographie basée sur le chaos exploite le comportement imprévisible des systèmes dynamiques non linéaires pour générer des clés de chiffrement et masquer les données sensibles.
- **Fonctionnement :** Utilise des équations chaotiques pour générer des séquences de chiffrement complexes, ce qui rend difficile la prévision du comportement du système sans connaître les conditions initiales exactes.
- **Applications :** Utilisée pour sécuriser les transmissions de données dans des environnements où la robustesse et la complexité sont cruciales.

II.9.4 Autres Techniques Émergentes

Il existe d'autres techniques émergentes dans le domaine de la cryptographie avancée, telles que :

- **Réseaux de neurones pour le chiffrement :** Utilisation de réseaux de neurones artificiels pour créer des algorithmes de chiffrement robustes et adaptatifs.
- **Blockchain et sécurité :** Utilisation des technologies de blockchain pour renforcer la sécurité des transactions et des échanges de données.
- **Chiffrement post-quantique :** Développement d'algorithmes capables de résister aux attaques des ordinateurs quantiques futurs[7][20].

II.10. Cryptographie Basée sur le Chaos

II.10.1 Introduction au Chaos

Le chaos, dans le contexte de la cryptographie, se réfère à l'utilisation de systèmes dynamiques non linéaires et imprévisibles pour le chiffrement des données. Ce domaine

exploite le comportement complexe et pseudo-aléatoire des systèmes chaotiques pour sécuriser les communications et les informations sensibles.

II.10.2 Principes Fondamentaux des Systèmes Chaotiques

- **Non-linéarité :** Les systèmes chaotiques sont caractérisés par des relations non linéaires entre leurs variables, ce qui contribue à leur comportement imprévisible.
- **Sensibilité aux Conditions Initiales (ICIS) :** Une petite variation dans les conditions initiales d'un système chaotique peut conduire à des résultats très différents à long terme, renforçant la sécurité du chiffrement.
- **Pseudo-aléatoire :** Bien que déterministes, les séquences générées par des systèmes chaotiques semblent aléatoires, ce qui rend difficile la reconstruction des données originales sans la clé de déchiffrement appropriée.

II.10.3 Utilisation du Chaos dans le Cryptage de Données

- **Génération de Clés :** Les systèmes chaotiques peuvent être utilisés pour générer des clés de chiffrement en exploitant leur capacité à produire des séquences de nombres pseudo-aléatoires.
- **Chiffrement :** Les données sont transformées à l'aide de fonctions chaotiques, où la clé de chiffrement est déterminée par les conditions initiales du système chaotique.
- **Applications :** Utilisé pour sécuriser les communications sans fil, les transmissions de données sensibles, et dans les systèmes nécessitant une forte résistance aux attaques cryptographiques traditionnelles.

II.10.4 Avantages et Inconvénients de la Cryptographie Chaotique

- **Avantage :**
  - Sécurité robuste grâce à la complexité et à l'imprévisibilité des systèmes chaotiques.
  - Capacité à générer des clés de chiffrement de manière efficace et sécurisée.
  - Adaptabilité aux environnements dynamiques et aux applications nécessitant une sécurité élevée.
- **Inconvénients :**
  - Défi de la gestion des paramètres chaotiques et des conditions initiales pour assurer une sécurité fiable.

- Complexité de l'implémentation et nécessité d'une expertise spécialisée pour concevoir des systèmes chaotiques cryptographiquement robustes.
- Sensibilité aux erreurs de conception et à la sélection inappropriée des paramètres chaotiques pouvant compromettre la sécurité[3][2].

II.11. Mise en Œuvre du Cryptage

II.11.1 Intégration dans les Applications

- **Description :** L'intégration du cryptage dans les applications implique l'incorporation de techniques et d'algorithmes cryptographiques pour sécuriser les données sensibles et les communications.
- **Processus :** Comprend la sélection appropriée des algorithmes de chiffrement, la gestion des clés, et l'implémentation des protocoles de sécurité pour assurer la confidentialité et l'intégrité des données.
- **Applications :** Répandue dans les systèmes de paiement en ligne, les applications de messagerie sécurisée, et les plateformes de stockage de données sensibles.

II.11.2 Outils et Bibliothèques de Cryptographie

- **Description :** Les outils et bibliothèques de cryptographie offrent des fonctionnalités prêtes à l'emploi pour l'implémentation sécurisée des protocoles cryptographiques.
- **Exemples :**
  - **Opens SL :** Bibliothèque open-source offrant des implémentations de nombreux algorithmes de chiffrement et de protocoles de sécurité.
  - **Bounty Castle :** Bibliothèque Java offrant des API pour le chiffrement, les signatures numériques, et la gestion des certificats.
  - **Crypto++ :** Bibliothèque C++ offrant une large gamme d'algorithmes cryptographiques pour les applications haute sécurité.

II.11.3 Meilleures Pratiques de Mise en Œuvre

- **Sélection des Algorithmes :** Choisir des algorithmes cryptographiques adaptés aux exigences de sécurité et aux performances de l'application.
- **Gestion des Clés :** Mettre en œuvre des pratiques de gestion des clés sécurisées, y compris la génération, le stockage et le renouvellement périodique des clés.

- **Audit de Sécurité :** Effectuer des audits réguliers de sécurité pour détecter et corriger les vulnérabilités potentielles dans l'implémentation du cryptage.
- **Formation du Personnel :** Sensibiliser et former le personnel aux bonnes pratiques de sécurité informatique et à l'utilisation correcte des techniques de cryptage[21][26].

II.12. Attaques Contre les Systèmes de Cryptage

II.12.1 Attaques par Force Brute

- **Description :** Les attaques par force brute consistent à essayer toutes les combinaisons possibles de clés jusqu'à trouver celle qui permet de déchiffrer les données chiffrées.
- **Méthode :** Utilisation de puissance de calcul élevée pour tester des millions de combinaisons par seconde.
- **Contre-Mesures :** Utilisation de clés longues et complexes, limitation du nombre de tentatives de connexion, et utilisation de techniques de détection d'activité suspecte.

II.12.2 Attaques par Analyse Différentielle

- **Description :** Les attaques par analyse différentielle visent à exploiter les faiblesses dans les algorithmes de chiffrement en observant les différences dans les résultats chiffrés en fonction des entrées.
- **Méthode :** Analyse statistique des différences entre les entrées et les sorties chiffrées pour déduire des informations sur la clé secrète.
- **Contre-Mesures :** Utilisation d'algorithmes résistants à l'analyse différentielle, comme AES, et adoption de bonnes pratiques de conception d'algorithmes cryptographiques.

II.12.3 Attaques sur les Protocoles

- **Description :** Les attaques sur les protocoles visent les faiblesses dans la conception ou l'implémentation des protocoles de communication sécurisée, comme SSL/TLS ou IPsec.
- **Méthode :** Exploitation de vulnérabilités dans les négociations de clés, les échanges de certificats, ou les failles de sécurité connues dans les versions spécifiques des protocoles.

- **Contre-Mesures :** Mises à jour régulières des protocoles pour corriger les vulnérabilités, utilisation de configurations sécurisées, et surveillance active des activités suspectes.

II.12.4 Contre-mesures et Défenses

- **Défenses Actives :** Utilisation de chiffrement robuste et de clés longues, intégration de mécanismes de détection d'intrusion pour identifier les activités malveillantes.
- **Audit de Sécurité :** Réalisation régulière d'audits de sécurité pour détecter et corriger les vulnérabilités potentielles dans les systèmes de cryptage.
- **Formation et Sensibilisation :** Sensibilisation continue des utilisateurs et formation sur les bonnes pratiques de sécurité informatique pour réduire les risques d'attaques réussies [18].

II.13. Applications du Cryptage

II.13.1 Sécurisation des Communications

- **Description :** Le cryptage est largement utilisé pour sécuriser les communications, en garantissant que seuls les destinataires autorisés peuvent accéder aux informations échangées.
- **Méthodes :** Utilisation de protocoles comme SSL/TLS pour sécuriser les connexions Internet, VPN pour les réseaux privés virtuels, et chiffrement des emails pour la confidentialité des communications.

II.13.2 Protection des Données Stockées

- **Description :** Le cryptage est essentiel pour protéger les données sensibles stockées sur des périphériques de stockage ou des serveurs, réduisant ainsi les risques de vol ou de compromission des données.
- **Applications :** Chiffrement des disques durs, bases de données cryptées, et fichiers sensibles pour assurer leur sécurité contre les accès non autorisés.

II.13.3 Cryptage dans les Transactions Financières

- **Description :** Le cryptage est crucial dans les transactions financières pour garantir l'intégrité et la confidentialité des données financières sensibles, comme les informations de carte de crédit et les transactions en ligne.
- **Solutions :** Utilisation de protocoles sécurisés comme HTTPS pour les paiements en ligne, chiffrement des données de transaction, et utilisation de clés de chiffrement robustes pour sécuriser les échanges d'informations financières.

II.13.4 Cryptage dans les Services Cloud

- **Description :** Le cryptage dans les services cloud est essentiel pour sécuriser les données sensibles stockées et traitées à distance via des services cloud publics ou privés.
- **Utilisation :**
    - **Chiffrement des Données :** Les données sont chiffrées avant d'être envoyées vers le cloud, assurant qu'elles restent sécurisées même en cas d'accès non autorisé.
    - **Gestion des Clés :** Utilisation de méthodes sécurisées pour générer, stocker et gérer les clés de chiffrement afin de contrôler l'accès aux données.
    - **Conformité et Réglementation :** Répondre aux exigences de conformité et de réglementation en matière de protection des données, telles que le RGPD en Europe ou HIPAA aux États-Unis [35].

II.14. Conclusion

La cryptographie joue un rôle crucial dans la sécurisation des données et des communications dans notre monde numérique moderne. En résumé, ce domaine essentiel de la sécurité informatique offre une série d'outils, d'algorithmes et de protocoles qui garantissent la confidentialité, l'intégrité et l'authenticité des informations sensibles.

Chapitre III :

Conception et analyse de notre algorithme de cryptage

III.1. Introduction

Ce chapitre concerne la partie analyse et conception. Pour l'élaboration des différents diagrammes qui vont représenter les différents aspects (statiques, dynamiques et fonctionnels) associée à notre site d'application, on va suivre une démarche pragmatique et simplifiée, cette démarche est inspirée des étapes du processus UP qui utilise UML.

III.2. Démarche simplifiée pour l'analyse

La démarche est structurée en cinq (5) étapes :

Etape 1 : Etude préliminaire

- Présentation générale du projet.
- Définition des grands choix techniques.
- Recueil des besoins fonctionnels.
- Recueil des besoins opérationnels.
- Description du contexte du système :
  - Identification des acteurs.
  - Identification des messages.
  - Réalisation du diagramme de contexte.

Etape 2 : Identification et représentation des cas d'utilisation.

Etape 3 : Description et représentation des scénarios.

Etape 4: Elaboration du diagramme de classe.

Etape 5 : Elaboration du diagramme d'état transition (étape optionnelle).

Dans ce qui suit, nous allons appliquer les étapes de la démarche pour développer notre système [1][2][3].

III.2.1. Etude préliminaire

Cette étape permet de positionner précisément le champ du système étudié et de déterminer les besoins fonctionnels et opérationnels ; en utilisant principalement le texte.

III.2.1.1. Présentation générale du projet

Le domaine d'étude spécifie pour notre projet est : la conception et la réalisation d'un site web et une application web pour le cryptage et décryptage d'une vidéo par l'Algorithme

AES/chaos qui offre quelque fonctionnalité à ses utilisateur (choisir vidéo, encrypter vidéo, décrypter vidéo).

III.2.1.2. Définition des grands choix techniques

Afin d'obtenir un système qui répondre aux aspirations de ses utilisateurs, nous avons opté pour les techniques suivantes :

- ✓ L'outil de modélisation : UML (Unifie Modeling langage).
- ✓ Le processus de développement à suivre : UP (unifié processus) :
- ✓ La plateforme disponible : **windows10.**
- ✓ L'architecture du système : **client/serveur.**
- ✓ Le langage de programmation : **python**, **css.**
- ✓ Le langage de modélisation : **UML2.0.**
- ✓ Le processus de développement : **UP simplifié.**
- ✓ L'environnement : **VSCODE.**

III.2.1.3. Recueil des besoins fonctionnels

Nous nous intéressons à modéliser et réaliser une application site Web pour crypter et décrypter une vidéo qui peut regrouper les fonctionnalités suivantes :

Coté utilisateur

- ✓ **Consultation des différentes rubriques**

  L'utilisateur accède à la page d'accueil du site d'application de cryptage puis parcourir les répertoires pour choisir une vidéo et le crypter, après le cryptage on peut télécharger la vidéo pour la lecture, l'opération de décryptage est comme l'opération de cryptage se fait par sélectionner le vidéo crypté pour décrypter.

Coté serveur

La vidéo uploader est crypté/décrypter par le système qui est l'algorithme de cryptage AES/chaotique

III. 2.1.4. Recueil des besoins opérationnels

Les besoins opérationnels sont ceux liés à l'exploitation du système et qui assurent son efficacité.

Dans notre application les exigences non fonctionnelles sont des onglets :

- ✓ **Contact us**

  Les Coordonnées tel : le numéro du téléphone ou l'email

- ✓ **Home**

  Pour retour a la page d'accueille

- ✓ **Services**

- ✓ **About us :**

  Quelques informations qui concernent les développeurs du site

III.2.1.5. Description du contexte du système

a- Identification des acteurs

Les acteurs principaux sont :

* L'utilisateur/client

Personne qui accède le site d'application pour crypter ou décrypter une vidéo puis le télécharger après la fin de l'opération.

b- Identification des messages

On va détailler les différents messages échangés entre le système et l'extérieur.

*L'utilisateur/client

Consulter services

Parcourir les répertoires

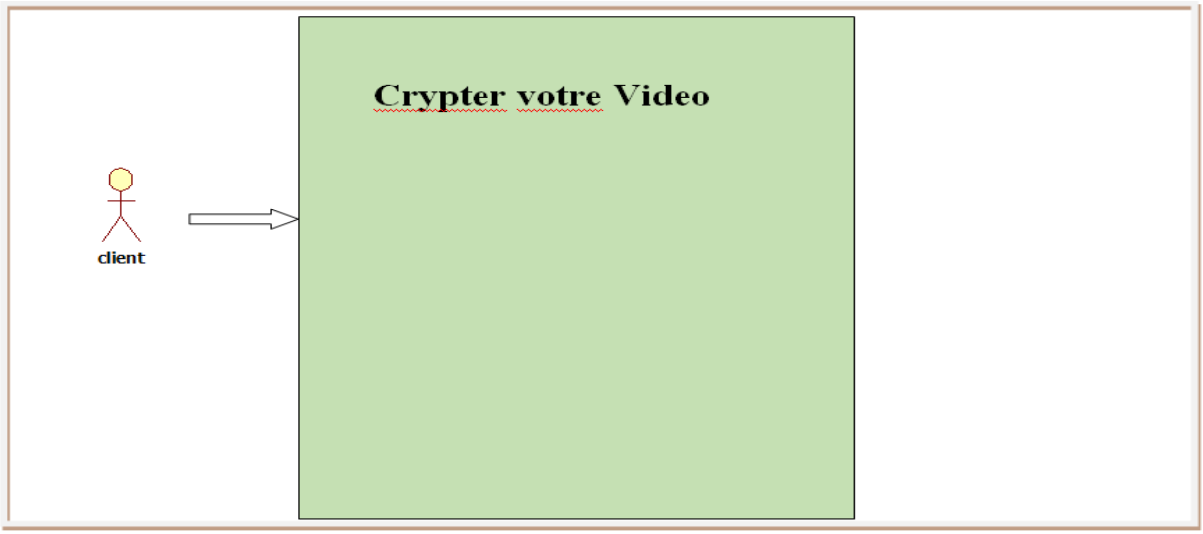
selectionner un fichier(vidéo)

Demande de cryptage/décryptage la vidéo sélectionnée

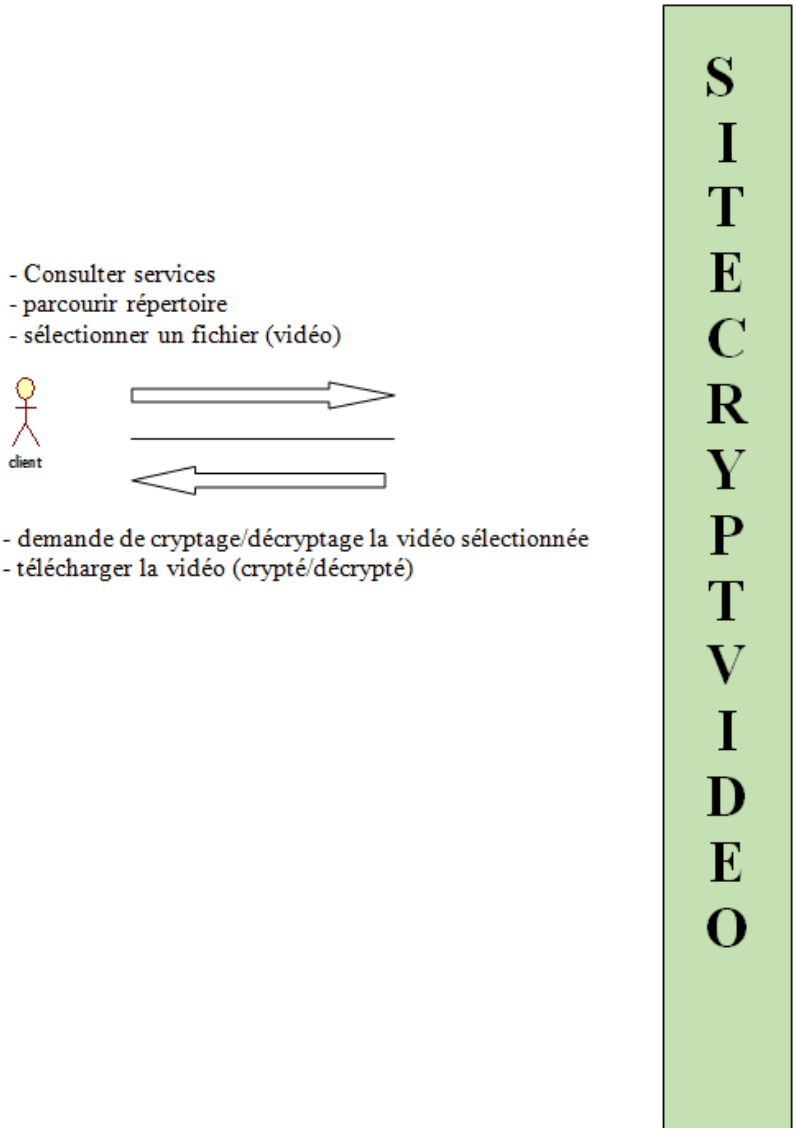
Télécharger la vidéo (crypté/décrypté)

c- Réalisation du diagramme de contexte

- ➢ **Diagramme de contexte statique**


Crypter votre Video
client

➢ **Diagramme de contexte dynamique**



III.2.2. Identification et représentation des cas d'utilisation

III.2.2.1. Identification des cas d'utilisation

Pour le client/l'utilisateur

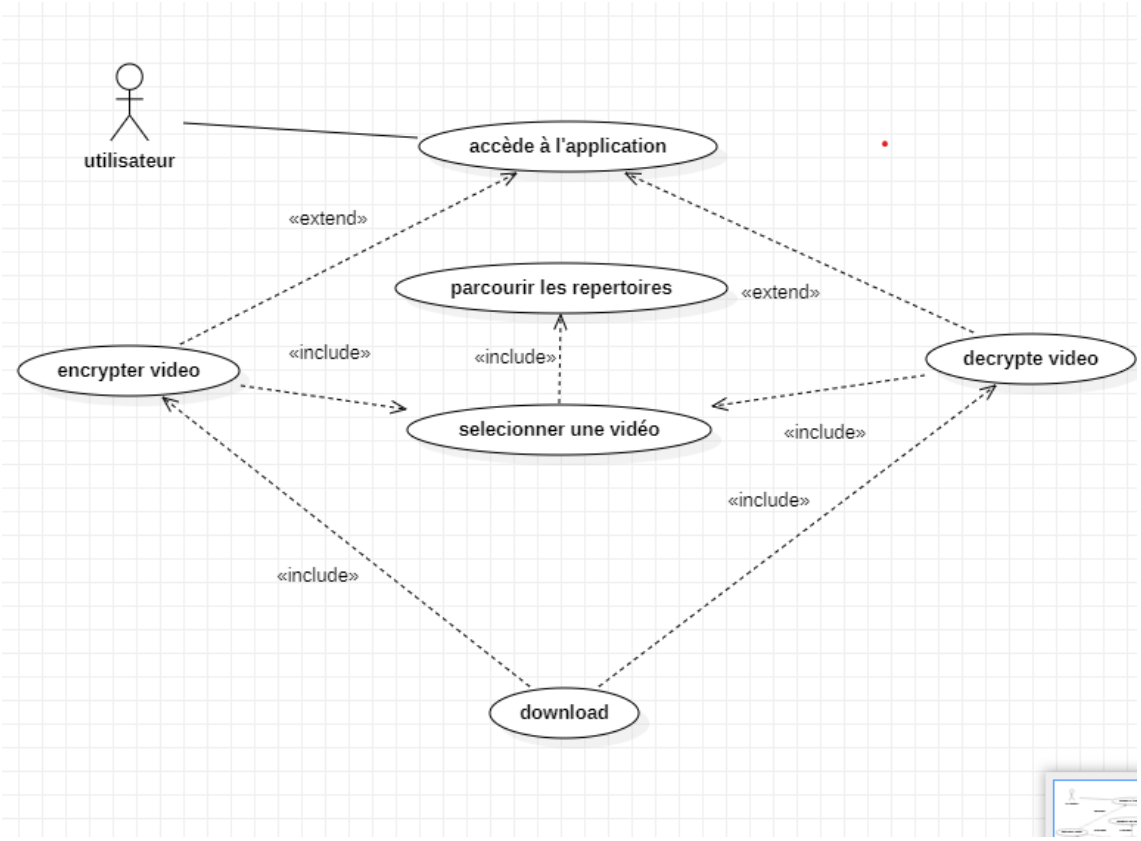
- l'utilisateur parcourir les répertoires
- l'utilisateur sélectionne une vidéo
- crypter/décrypter la vidéo

-télécharger la vidéo

III.2.2.2. Représentation des cas d'utilisation

Représente les fonctions du système du point de vue des utilisateurs. [7]

Les cas d'utilisation de notre système sont :



III.2.3. Description et représentation des scénarios

- **Format d'une fiche descriptive**

Tableau III.1 : Format d'une fiche descriptive

Nom du cas d'utilisation
Liste des acteurs (primaire/secondaire)
Objectif du cas d'utilisation
Scénario nominal
Scénario alternatif

Tableau III.2 : Fiche descriptive du cas d'utilisation « accéder à application »

Nom : accéder à application du site.
L'acteur : l'utilisateur/client.
L'objectif : Permet au des clients de voir les fonctionnalités du site.
Scénario nominal : - Le système affiche la liste des services ou les fonctionnalités - Si l'utilisateur est intéressé par le cryptage/décryptage, il faut choisit une vidéo ... - Le système affiche le bouton de téléchargement à la fin de l'opération.
Scénario alternatif : - L'utilisateur abandonne la page de site d'application.

Tableau III.3 : Fiche descriptive du cas d'utilisation « choisir un fichier »

Nom : choisir un fichier.
L'acteur : utilisateur.
L'objectif : Permet de sélectionner une vidéo a partir le parcours les répertoires .
Scénario nominal : - Le système affiche un bouton pour parcourir les répertoires. - L'utilisateur sélectionne une vidéo.
Scénario alternatif : - L'utilisateur abandonne la page de site d'application ou annuler la sélection.

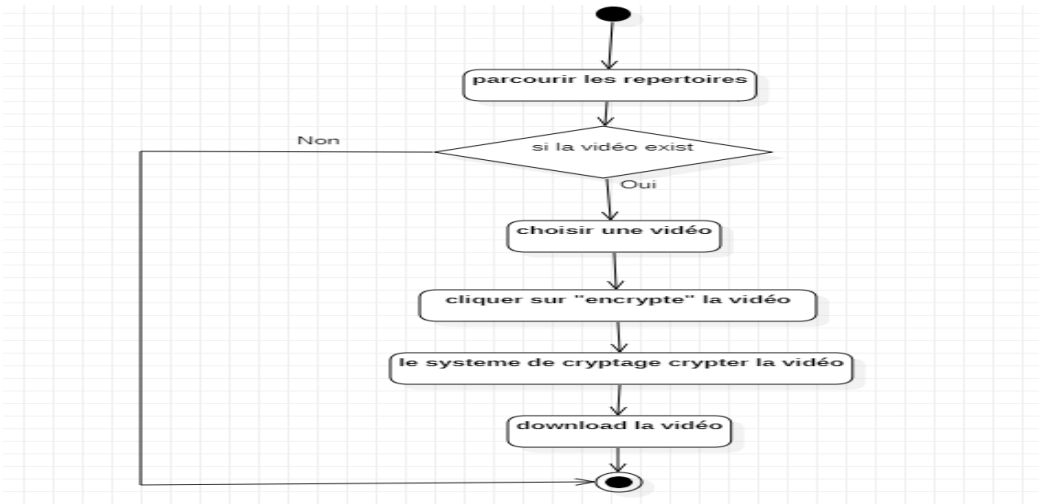
Tableau III.4 : Fiche descriptive du cas d'utilisation « Encrypte/décrypté »

Nom : Encrypte/décrypte vidéo.
L'acteur : l'utilisateur/client.
L'objectif : Permet à l'utilisateur crypter ou décrypter une vidéo
Scénario nominal - Le système affiche deux boutons un pour crypter et l'autre pour décrypter. - L'utilisateur après le parcours et la sélection une vidéo le crypter/décrypter - Le système prend certains de temps pour terminer l'opération. - Télécharger la vidéo « encrypter/décrypter » lors l'apparition du bouton « download ».
Scénario alternatif : L'utilisateur abandonne la page de site d'application ou annuler l'opération de « cryptage/décryptage ».

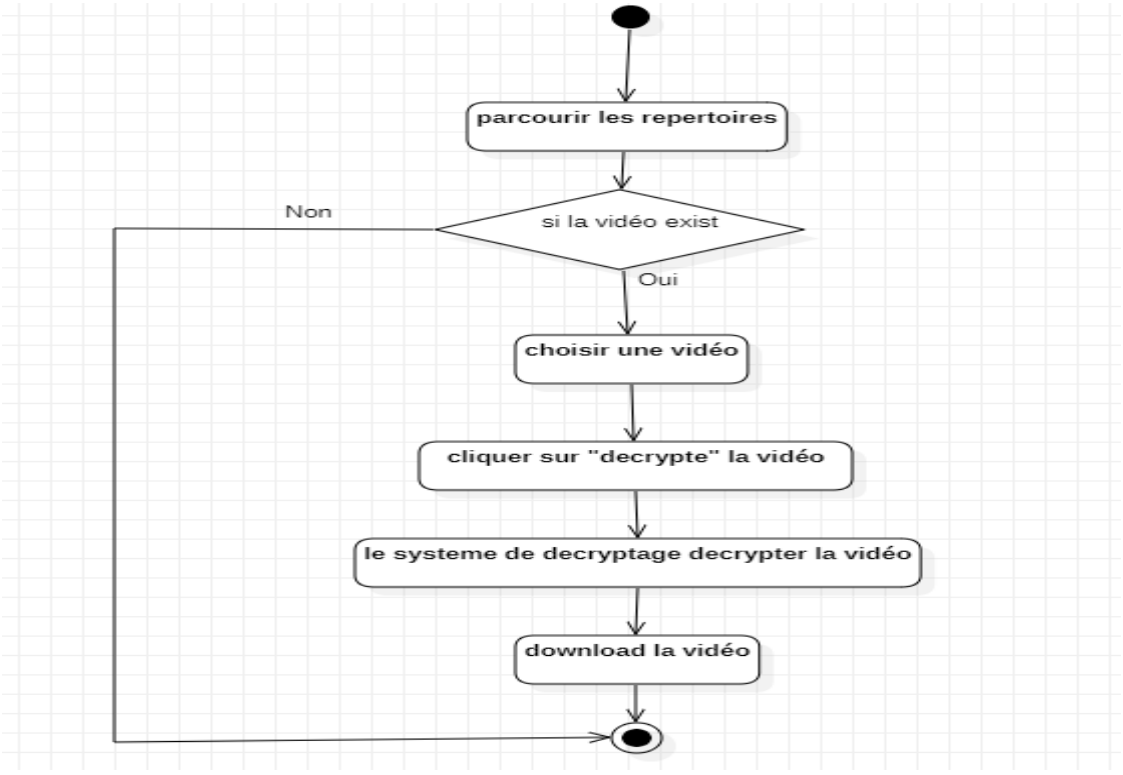
III.2.4. Diagramme d'activité

Représente le comportement d'une méthode ou d'un cas d'utilisation ou un processus métier. [7]

2.4.1. Diagramme d'activité « encrypter »



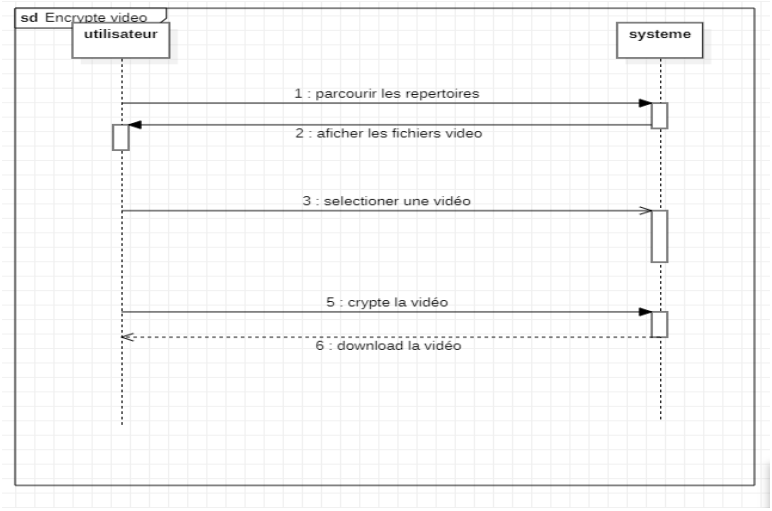
III.2.4.2. Diagramme d'activité « décrypter » :



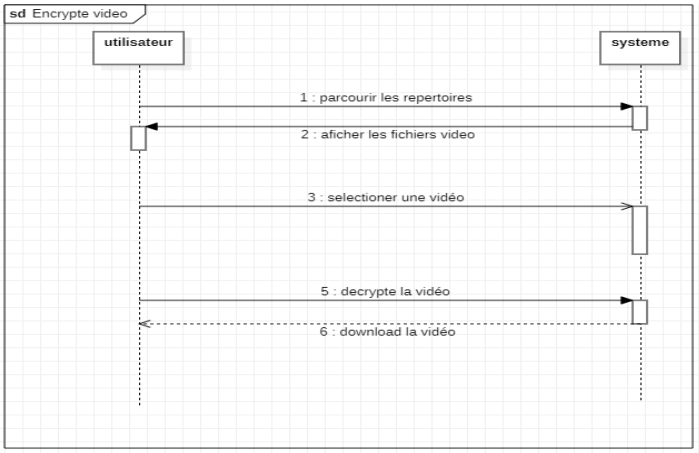
III.2.5. Diagramme de séquence

Représente des objets et leur interaction d'une manière temporelle. [7]

III.2.5.1. Diagramme de séquence « Crypter la vidéo »

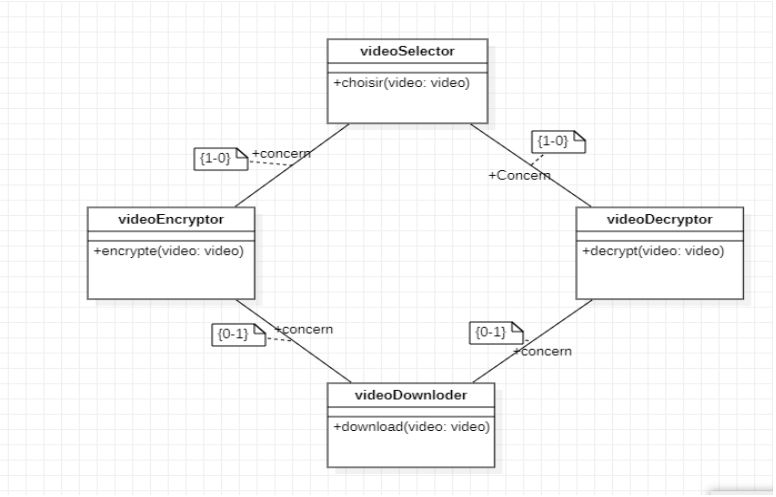


III.2.5.2. Diagramme de séquence « décrypte la vidéo »



III.3. Diagramme de classe

Représente la structure statique en termes de classe et relation. [7]



III.4. Conclusion

Dans ce chapitre, nous avons détaillé la conception et l'analyse de notre algorithme de cryptage AES chaotique. Nous avons commencé par une étude préliminaire pour définir les besoins fonctionnels et opérationnels de notre système, suivie de l'identification et de la représentation des cas d'utilisation pertinents.

Nous avons ensuite décrit et représenté les scénarios d'utilisation, élaboré les diagrammes de classe, et exploré les diagrammes d'état-transition, d'activité et de séquence pour mieux comprendre les interactions et les dynamiques de notre système. Chaque étape a permis de préciser les exigences et les fonctionnalités nécessaires pour développer une solution de cryptage robuste et efficace.

Enfin, cette analyse approfondie nous a permis de concevoir un système intégré et cohérent, utilisant les principes du chaos pour renforcer la sécurité des données cryptées. Cette approche innovante ouvre de nouvelles perspectives pour la protection des informations sensibles et répond aux exigences croissantes de sécurité dans le contexte des communications modernes.

Ainsi, ce chapitre établit les fondations solides pour la mise en œuvre et le développement de notre algorithme de cryptage AES chaotique, garantissant une sécurité renforcée pour les utilisateurs et les applications.

Chapitre IV

Implémentation

IV.1. Introduction

Après l'analyse des besoins et la définition de la méthodologie de conception, on programme l'essentiel de notre conception via un environnement adéquat.

Dans ce chapitre, on décrit les logiciels utilisés, on présente aussi quelques exemples des interfaces utilisateurs représentant l'application qui ont été réalisées.

IV.2. Langages de programmations

IV.2.1. Langage HTML (Hyper Texte Markup langage)

L'Hyper Texte Markup langage, généralement abrégé HTML, est le format de données conçu pour représenter les pages web. C'est un langage de balisage qui permit de décrire de l'hypertexte, d'où est son nom.

Il ne s'agit pas d'un langage de programmation au sens propre, mais d'un simple langage de description d'une page web qui permit de structurer sémantiquement et de mettre en forme le contenu des pages, d'inclure des ressources multimédias dont des images, des formulaires de sis…etc. [36].

IV.2.2. Langage Python

Python est le langage de programmation open source le plus employé par les informaticiens. Ce langage s'est propulsé en tête de la gestion d'infrastructure, d'analyse de données ou dans le domaine du développement de logiciels. En effet, parmi ses qualités, Python permet notamment aux développeurs de se concentrer sur ce qu'ils font plutôt que sur la manière dont ils le font. Il a libéré les développeurs des contraintes de formes qui occupaient leur temps avec les langages plus anciens. Ainsi, développer du code avec Python est plus rapide qu'avec d'autres langages.

Il reste aussi accessible pour les débutants, à condition de lui consacrer un peu de temps pour la prise en main. De nombreux tutoriels sont d'ailleurs disponibles pour l'étudier sur des sites Internet spécialisés ou sur des comptes YouTube. Sur les forums d'informatique, il est toujours possible de trouver des réponses à ses questions, puisque beaucoup de professionnels l'utilisent.

A quoi sert le langage Python ?

Les principales utilisations de Python par les développeurs sont :

- La programmation d'applications
- La création de services web
- La génération de code
- Le méta programmation

Techniquement, ce langage servira surtout pour le Scripting et l'automatisation (interaction avec les navigateurs web).

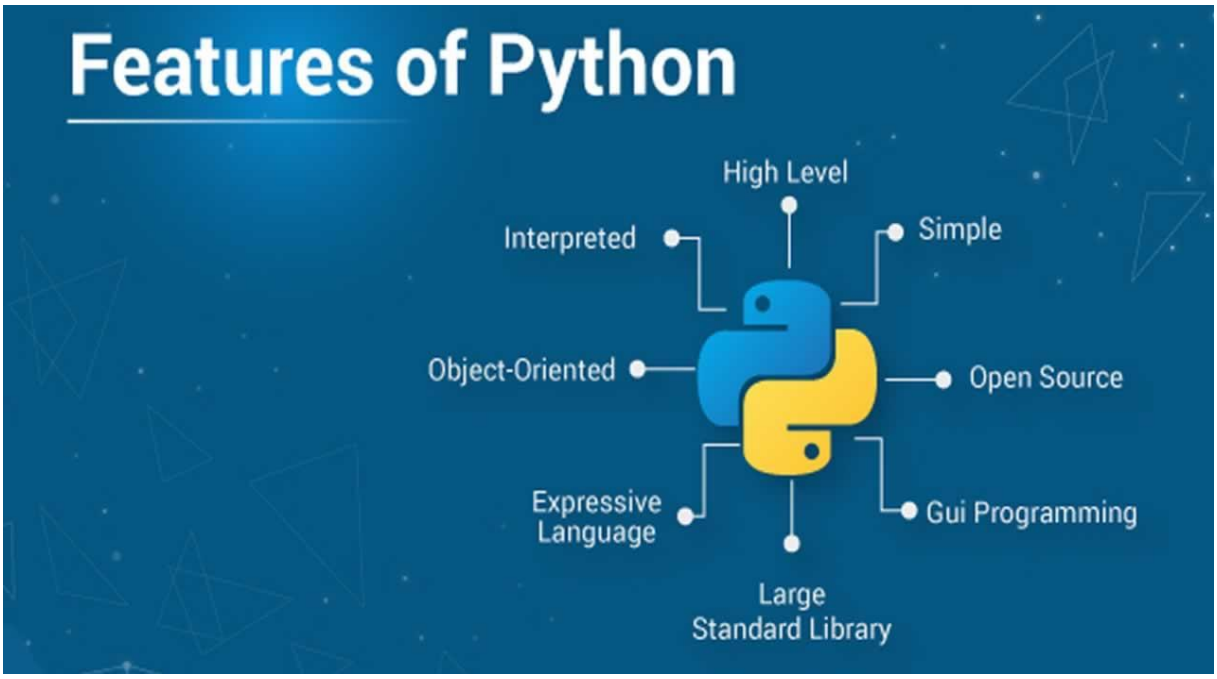


Figure IV.1. Facture du python

IV.2.3. JavaScript

Le JavaScript est un langage de script incorporé sans un document HTML. Ce langage est un langage de programmation qui permet d'apporter des améliorations aux langages HTML en permettant d'exécuter des commandes du coté client. C'est-à-dire au niveau du navigateur et non du serveur web.

IV.2.4. Serveur Apache

Apache est le serveur http le plus utilisé au monde. Le point fort d'Apache est de fonctionner avec des modules, que l'on peut soit ajouter statiquement à la compilation en le spécifiant auparavant, soit charger dynamiquement au démarrage du logiciel en l'ajoutant dans le fichier de configuration.

IV.3. Outil d'implémentation

IV.3.1. Visual Studio Code

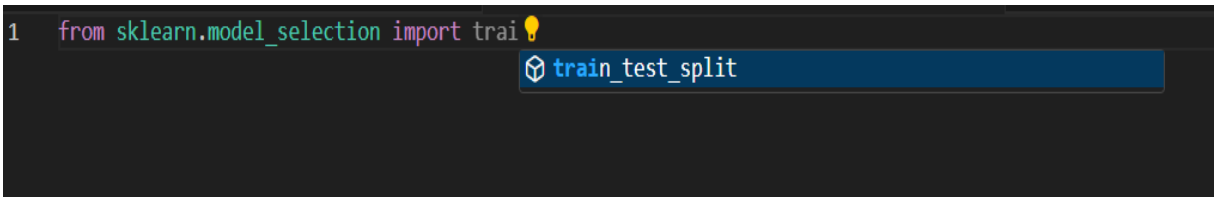
Visual Studio Code, souvent appelé **VS Code**, est un éditeur de code simple d'usage qui offre de nombreux avantages. Ci-après nous donnons trois grandes fonctionnalités proposées par VS Code. Tout d'abord, **la coloration syntaxique** est une fonctionnalité clé qui **améliore la lisibilité du code.** Elle consiste à mettre en évidence automatiquement les différentes parties du code en fonction de leur rôle, simplifiant ainsi la compréhension de la structure[37].

```
1  import numpy as np
2
3  def my_function():
4      return "Hello World"
5
6  my_function()
```

Un autre avantage est **la détection d'erreurs.** Les éditeurs de code, y compris VS Code, sont capables de signaler les incohérences dans le code, par de petites vaguelettes rouges soulignant les parties de code problématiques par exemple, **ce qui facilite grandement la correction des erreurs de programmation.** Les erreurs détectées peuvent être des problèmes d'indentation, l'utilisation de variables définies nulle part dans le code qui précède, etc.

```
1  import matplotlib.pyplot as plt
2    import numpy as np
3
4  def f(x):
5    return np.exp(x)
```

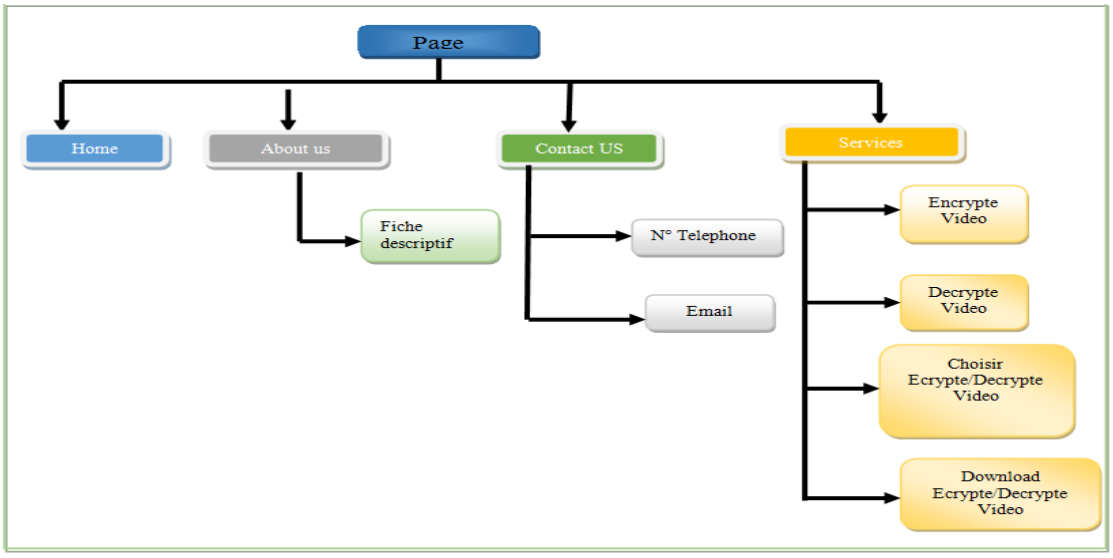
Enfin, **l'autocomplétions** est une fonctionnalité qui propose des suggestions de code en temps réel, ce qui peut **accélérer le processus de codage** en évitant de taper manuellement chaque instruction. Cela peut être particulièrement utile si vous débutez en programmation et ne connaissez pas nécessairement par cœur à la lettre près le nom de toutes les fonctions que vous souhaitez utiliser.



Ce qui fait de VS Code un éditeur adapté aux débutants est **sa simplicité d'utilisation.** L'interface de l'éditeur est conviviale et intuitive, ce qui signifie que vous n'aurez pas à passer beaucoup de temps à configurer des paramètres complexes. **Une fois installé, vous êtes prêt à coder.**

IV.4. Architecture du site

IV.4.1. Plan du site



IV.4.2. Présentation de quelque interface de site d'application

- **Page d'accueille**

C’est la première interface qui apparait lors du démarrage de site, à partir de cette page on peut faire mes opérations **différentes** (choisir, crypter, décrypter vidéo et télécharger vidéo) applications constituant cette application du site**.**

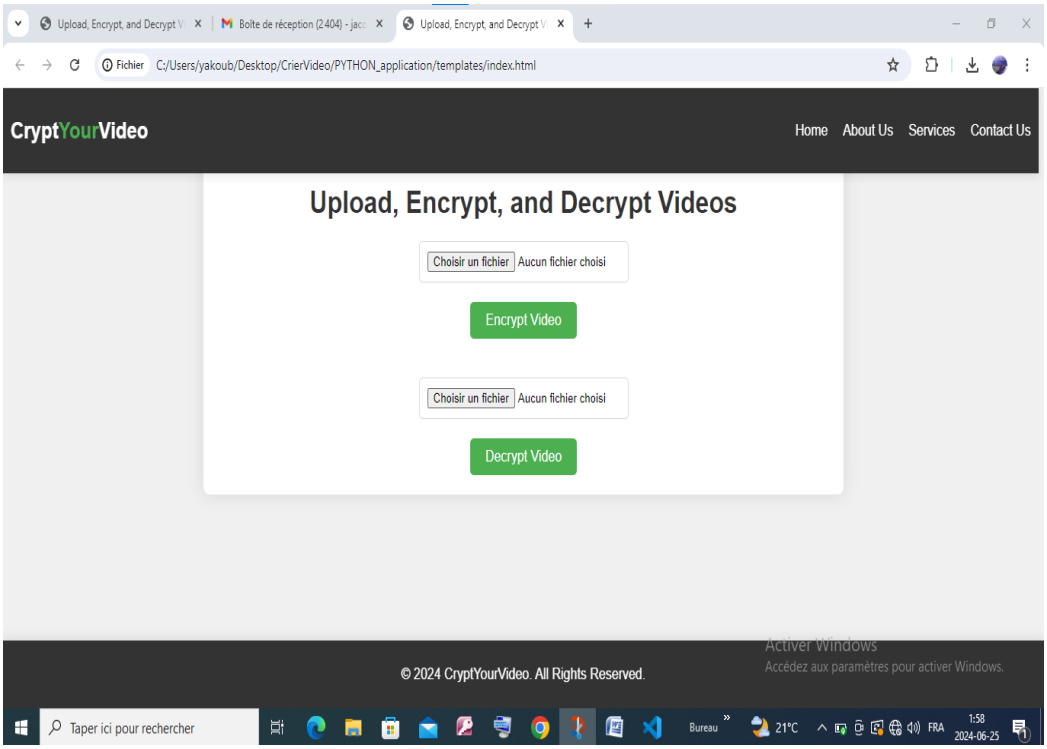


Figure IV.2. Page d’accueil d’application du site

Cette interface illustre comment parcourir les répertoires des fichiers pour choisir une vidéo afin de l’opération de (cryptage décryptage) vidéo.

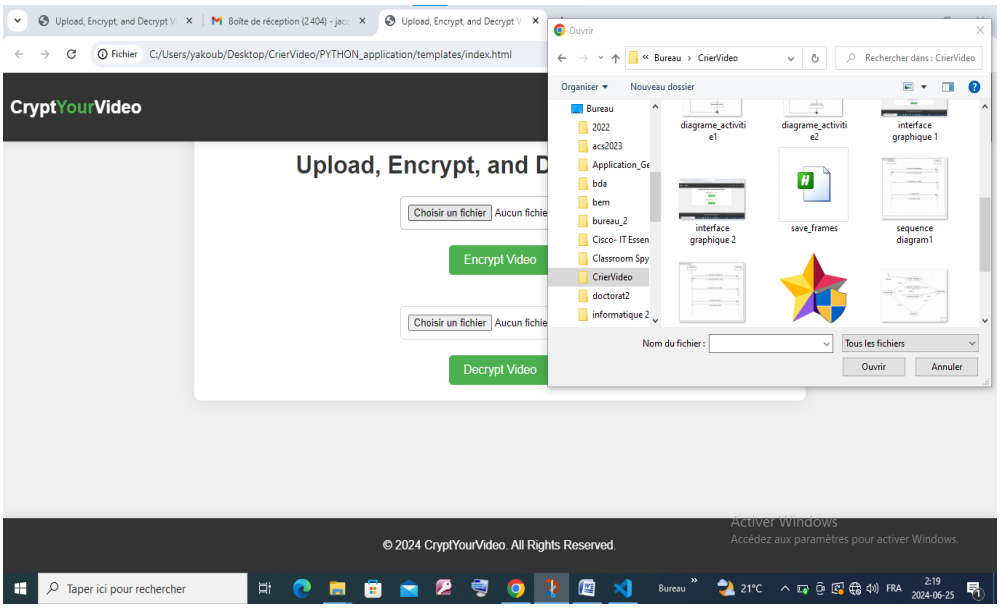


Figure IV.3. Choisir une vidéo pour crypter/décrypter.

➢ **Crypter une vidéo :**

Cette interface est illustrée comment l'interface deviendra après le cryptage du vidéo sélectionné (nouvelle bouton va apparaitre) nommé « Download Encrypté Vidéo.

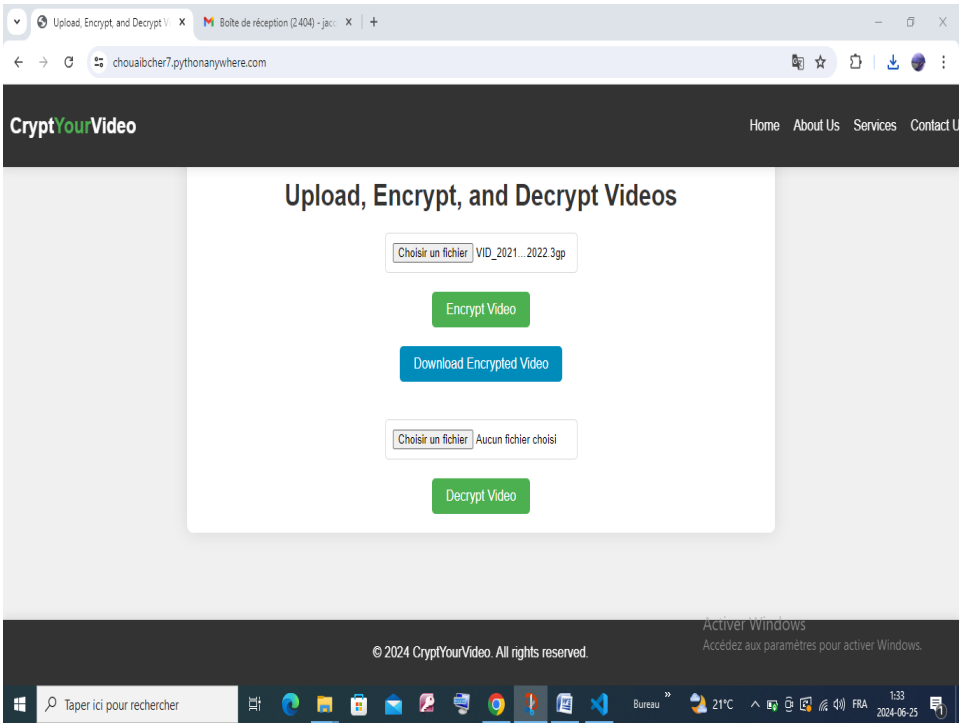


Figure IV.4 crypter et télécharger la vidéo cryptée.

➢ **Décrypter une vidéo :**

Cette interface est illustré comment l'interface deviendra après le cryptage du vidéo sélectionné (nouvelle bouton va apparaitre) nommé « Download Décrypte Vidéo ».

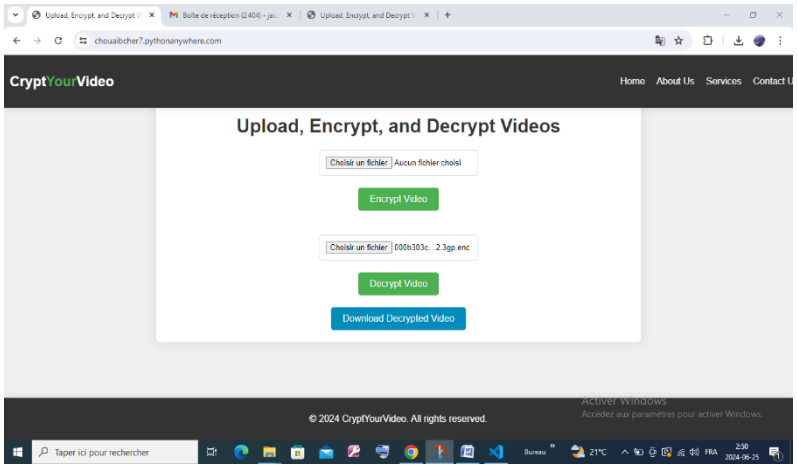


Figure IV.5 : décrypter et télécharger la vidéo décryptée.

➢ **<u>Partie du code (fonction de cryptage) :</u>**

Cet interface est présenté la fonction responsable à le cryptage d'une vidéo sous le langage Python.

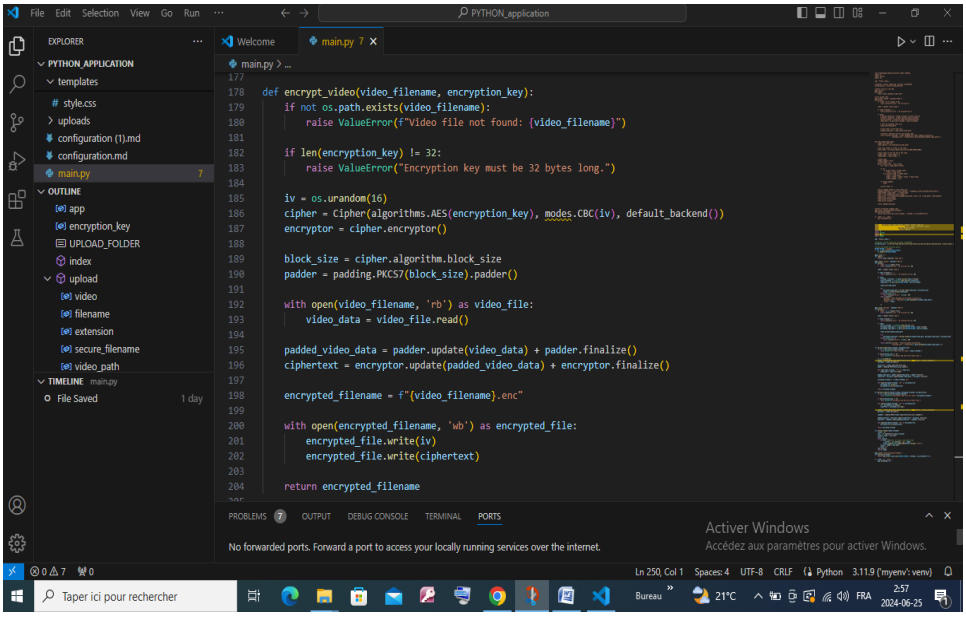


Figure IV.6 : Code python de la fonction de cryptage vidéo.

➢ **<u>Partie du code (fonction de décryptage) :</u>**

Cette interface est présenté une partie du code de la fonction responsable à le décryptage d'une vidéo sous le langage Python

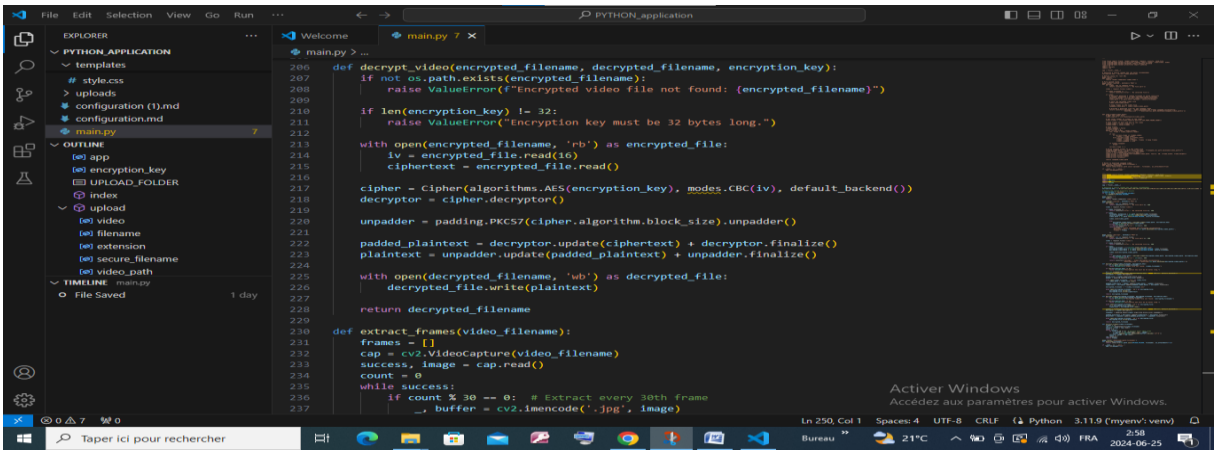


Figure IV.7. Partie du Code python de la fonction de décryptage vidéo.

IV.5. Conclusion

Ce chapitre a été consacré dans sa première partie à la présentation des différents outils utilisés pour la réalisation de notre site d'application. Nous avons introduit le maximum des concepts relatifs à l'environnement de développement tels que Visual Studio Code 1.90.2, Python, java Script. Dans la deuxième partie nous avons présenté le dossier technique de notre application (fenêtres, codes…).

Conclusion Général

V.Conclusion générale

Ce projet a exploré en profondeur les concepts fondamentaux des images, des vidéos et de la cryptographie, ainsi que leur mise en œuvre pratique dans le développement d'une application de cryptage basée sur l'algorithme AES chaotique. Chaque chapitre a contribué à éclairer différents aspects essentiels pour comprendre et sécuriser les données numériques dans un environnement moderne.

Dans le premier chapitre, nous avons étudié les caractéristiques des images et des vidéos, allant des formats de fichiers aux paramètres de résolution et de compression. Ce chapitre a posé les bases nécessaires pour comprendre la nature des données sur lesquelles nous avons travaillé, en soulignant l'importance de leur intégrité et de leur sécurité.

Le deuxième chapitre nous a plongés dans l'univers complexe de la cryptographie. À travers une exploration détaillée des algorithmes symétriques et asymétriques, ainsi que des protocoles de chiffrement et des techniques avancées comme la cryptographie quantique, nous avons compris les mécanismes essentiels permettant de sécuriser les communications et les données sensibles.

Le troisième chapitre a présenté une analyse approfondie de l'algorithme de cryptage AES chaotique, depuis sa conception jusqu'à sa modélisation à l'aide de diagrammes UML. Cette étape a été cruciale pour visualiser et planifier l'implémentation de notre solution de cryptage dans un cadre informatique concret.

Enfin, le quatrième chapitre a détaillé la réalisation et l'implémentation pratique de notre application de cryptage, en utilisant des langages de programmation comme HTML, Python et JavaScript, ainsi que des outils modernes tels que Visual Studio Code. Nous avons également exploré l'architecture du site et présenté des interfaces utilisateur clés, démontrant ainsi l'application concrète des concepts théoriques abordés.

En conclusion, ce projet a non seulement enrichi notre compréhension théorique des technologies liées aux images, aux vidéos et à la sécurité des données, mais il a également renforcé nos compétences pratiques en matière de développement logiciel et de gestion de projet. Les défis rencontrés, tant sur le plan conceptuel que technique, ont été surmontés grâce à une méthodologie rigoureuse et à l'application de meilleures pratiques. À l'avenir, ces

connaissances nous guideront vers de nouvelles innovations dans le domaine de la sécurité des données numériques et de la cryptographie.

Références Bibliographiques

Références Bibliographiques

[1] Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos, 16(08), 2129-2151.

[2] "Cryptography and Chaos" - Guanrong Chen, Yaobin Mao, Shiguo Lian

[3] "Chaotic Cryptography: Theory, Algorithms and Applications" - Shujun Li, Guanrong Chen, Xuanqin Mou [4]"Digital Image Processing" - Rafael C. Gonzalez, Richard E. Woods

[5] Yang, T. (2004). A survey of chaotic secure communication systems. Proceedings of the IEEE, 90(5), 1681-1707.

[6]"The JPEG 2000 Suite for Image Coding" - Touradj Ebrahimi, Michael Kunt

[7]https://creativemarket.com/blog/difference-between-jpg-png-bmp-tiff-images

[8] Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos, 16(08), 2129-2151.

[9] "PNG: The Definitive Guide" - Greg Roelofs

[10]https://www.adobe.com/ca_fr/creativecloud/file-types/image/comparison/bmp-vs-png.html

[11] Rabbani, M., & Jones, P. W. (1991). Digital image compression techniques (Vol. 7). SPIE optical engineering press. [12] "Image Compression and the Discrete Cosine Transform" - Majid Rabbani, Paul W. Jones

[13] https://www.boldcreative.fr/les-fichiers-image/

[14] "Cybersecurity Law" - Jeff Kosseff

[15] IEEE Security & Privacy

Références Bibliographiques

[16] Li, Z. N., Drew, M. S., & Liu, J. (2014). Fundamentals of multimedia. Springer.

[17] "Fundamentals of Multimedia" - Ze-Nian Li, Mark S. Drew, Jiangchuan Liu

[18] Lian, S., Sun, J., & Wang, Z. (2005). A block cipher based on a suitable use of the chaotic standard map. Chaos, Solitons & Fractals, 26(1), 117-129.

[19] https://themeisle.com/blog/lossy-vs-lossless-compression/

[20] "Lossless Compression Handbook" - Khalid Sayood

[21] Journal of Cybersecurity

[22]https://www.usherbrooke.ca/admission/fiches-cours/GEI760/techniques-avancees-de-cryptographie/

[23] https://www.apprendre-en-ligne.net/crypto/bibliotheque/PDF/florin.pdf

[24] Said, A., & Pearlman, W. A. (1996). A new, fast, and efficient image codec based on set partitioning in hierarchical trees. IEEE Transactions on Circuits and Systems for Video Technology, 6(3), 243-250.

[25] https://www.veritas.com/fr/ch/information-center/encryption

[26] https://www.youtube.com/watch?v=WaAv5_XbYg0

[27] Grgic, S., & Grgic, M. (2003). Performance analysis of image compression using wavelets. IEEE Transactions on Industrial Electronics, 48(3), 682-695.

[28] https://hal.science/hal-02096839/document

[29] 7. "Lossy Image Compression Domain" - Amir Said, William A. Pearlman

[23] https://link.springer.com/article/10.1007/s00034-022-02149-6

Références Bibliographiques

[24]https://fastercapital.com/fr/contenu/Techniques-de-cryptage---protection-des-donnees-contre-l-attaque-du-151.html

[25]https://www.usherbrooke.ca/admission/fiches-cours/GEI760/techniques-avancees-de-cryptographie/

[26] ACM Transactions on Privacy and Security (TOPS)

[27] "Fundamentals of Image, Audio, and Video Processing Using MATLAB" - Sonja Grgic, Mislav Grgic

[28] https://www.irif.fr/_media/users/ylg/crypto.pdf

[29] https://www.iso.org/fr/securite-de-l-information/cryptographie

[30] Cryptography Engineering: Design Principles and Practical Applications" - Niels Ferguson, Bruce Schneier, Tadayoshi Kohno

[31] Said, A., & Pearlman, W. A. (1996). A new, fast, and efficient image codec based on set partitioning in hierarchical trees. IEEE Transactions on Circuits and Systems for Video Technology, 6(3), 243-250.

[32] Daemen, J., & Rijmen, V. (2002). The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media. [33]"Image Compression and Encryption Techniques Using Block-Based Compression

[34]https://www.packtpub.com/product/cryptography-in-python-the-definitive-guide/9781786461896

[34] Rabbani, M. (2002). JPEG2000: Image compression fundamentals, standards and practice. Journal of Electronic Imaging, 11(2), 286-287.

[35]https://www.pearson.com/us/higher-education/program/Stallings-Cryptography-and-Network-Security-Principles-and-Practice-7th-Edition/PGM120061.html

Références Bibliographiques

[36] "Handbook of Image and Video Processing" - Alan C. Bovik

[37] Ebrahimi, T., & Kunt, M. (1995). Visual data compression for multimedia applications. Proceedings of the IEEE, 83(2), 253-268.

[38] Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos, 16(08), 2129-2151.

[39] Sayood, K. (2017). Lossless compression handbook. Academic press.

[40] "Cryptography and Network Security: Principles and Practice" - William Stallings

[41] "Multimedia Systems: Algorithms, Standards, and Industry Practices" - Ralf Steinmetz, Klara Nahrstedt

[42] "Chaos-Based Cryptography: Theory, Algorithms and Applications" - Ljupco Kocarev, Shiguo Lian

Résumé

La corrosion de l'acier AISI 420 est un problème majeur dans les entreprises, et nous avons mené de nombreuses expériences de corrosion sans et avec inhibiteurs. L'utilisation d'inhibiteurs est l'une des méthodes les plus largement utilisées pour protéger les métaux contre la corrosion, cependant, la plupart de ces inhibiteurs sont toxiques. Grands nombreux des chercheurs s'intéressent à trouver de nouvelles façons de prévenir la corrosion à base d'extraits de plantes respectueux de l'environnement pour protéger le métal.

Ce travail porte sur l'étude et l'inhibition de la corrosion de l'acier AISI 420 dans l'eau de mer. Nous avons choisi comme inhibiteur le café, le poivre noir et le curcuma. On étudié l'effet du temps d'immersion et la concentration de l'inhibiteur sur la corrosion de l'acier inox AISI 420 dans l'eau de mer, nous avons également calculé la vitesse de corrosion et Efficacité d'inhibiteur des inhibiteurs, et les résultats ont montré que l'efficacité inhibitrice de la corrosion atteint une valeur maximale d'environ 48 % pour une concentration de (0.75g/l) de poivre noir.

Mots clés : acier AISI 420, inhibiteurs de corrosion, café, poivre noir, curcuma eau de mer.

ملخص

يعد تآكل الفولاذ المقاوم للصدأ مشكلة كبيرة في الشركات، وقد أجرينا العديد من تجارب التآكل بدون أو باستخدام مثبطات. يعد استخدام المثبطات من أكثر الطرق المستخدمة على نطاق واسع لحماية المعادن من ألتآكل إلا أن معظم هذه المثبطات سامة. يهتم العديد من الباحثين بإيجاد طرق جديدة لمنع التآكل باستخدام مستخلصات نباتية صديقة للبيئة لحماية المعدن.

يركز هذا العمل على دراسة وتثبيط تآكل الفولاذ في مياه البحر بدون مثبط ومع مثبط. لقد اخترنا أيضًا مياه البحر كوسيلة أساسية وغمرناها بالقهوة والفلفل الأسود. قمنا بدراسة تأثير وزمن الغمر وتركيز المانع في عملية تآكل الفولاذ في مياه البحر، كما قمنا بحساب معدل التآكل وكفاءة المثبط للمثبطات، وأظهرت النتائج تفاعل مثبط التآكل.

كلمات مفتاحية مثبطات ألتآكل كالقهوة الفلفل الأسود، كركم ماء البحر.AISI 420 فولاذ