République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université20Août1955–Skikda
Facultés des sciences-Département d'informatique

Mémoire pour l'obtention du diplôme de Master en Réseaux et Systèmes Distribués

Thème

Réalisation d'une application web de démonstration d'algorithmes de chiffrement d'images/vidéos

Présenté par
Amel BOUAFFAR

Supervisé par
Mr Abdelhakim BOUREMEL
Mr Mohamed Akram SBAGHDI

Année Universitaire 2022- 2023

Résumé

Avec le grand développement de l'utilisation des réseaux de communication, beaucoup des informations sont transmets sur ce réseau tel que les images et les vidéos sont des informations qui ont besoin de protection, Donc la meilleure solution pour ce problème est l'utilisation de chiffrement.

Les algorithmes de chiffrement jouent un rôle essentiel dans la sécurité des données. Ils offrent des méthodes avancées pour chiffrer, rendant ainsi leur accès difficile pour les personnes non autorisées.

Dans ce mémoire, nous présentons une application web pour essayer les algorithmes de chiffrement d'image et vidéo basé sur permutation les pixels et décalage les couleurs ou une combinaison entre les deux.

Mots clés

Chiffrement, Image, Vidéo.

Abstract

With the great development of the use of communication networks, a lot of information is transmitted over this network such as images and videos are information that need protection, so the best solution to this problem is the use for encryption.

Encryption algorithms play a crucial role in data security. They offer advanced methods to encrypt, thus making their access difficult for unauthorized people.

In this memory, we present a web application to try the image and video encryptions algorities based on pixel permutation and color shift or a combination between the two.

Keywords

Encryption, Image, Video.

Remerciements

Au terme de ce travail, je voudrais d'abord remercier Allah de m'avoir donné la santé et la volonté dans la réalisation de ce projet.

Je tiens à remercier particulièrement mon second encadreur, Mr ***SBAGHDI Mohamed Akram****, pour son encadrement, sa patience, ses conseils très judicieux, ses encouragements et sa disponibilité tout au long de mon projet.*

Je remercie également mon encadreur ***Mr BOURMEL Abdelhakim,*** *pour ses précieux conseils et son judicieux choix de ce thème qui m'a apporté de nouvelles connaissances dans ce large domaine.*

J'exprime toute ma gratitude aux membres du jury pour avoir accepté de juger mon travail, ainsi que tous les enseignants du département d'informatique.

Merci infiniment.

Amel

Dédicaces

Je dédie ce travail à

Mes très chers parents, pour leur soutien et tous les efforts
Qu'on m'a donnés le long de mon parcours

Je dédie ce travail aussi à

Mes sœurs : Amira, Meriem

Et à mon frère : Islam

Et à Tesnime, Nourssine

Enfin, à toutes celles et tous ceux qui ont contribué de près
ou de loin à l'accomplissement de ce travail.

Amel

Table des Matières

Résumé

Abstract

Remerciements

Dédicaces

Table des Matières

Liste des Figures

Liste des abréviations

Chapitre 2 : Généralités sur la Cryptographie

Liste des Figures

Liste des abréviations

PAL Phase Alternating Line.

NTSC National Television System Committee.

SECAM Séquentie**l** Couleur à Mémoire.

2D 2 Dimensional.

JPEG Joint Photographic Experts Group.

PNG Portable Network Graphic.

GIF Graphic Interchange Format.

RGB Red Green Blue.

URL Localisateur Unifoeme de Ressource.

SSO Single Sign On.

HTTP Hyper Text Transfer Protocol.

DES Data Encryption Standard.

AES Advanced Encryptions Standard.

GF Groupe de Galois ou corps fini.

RSA Rivest Shamir Adleman.

ECC Elliptic Curve Cryptography.

1D 1 Dimensional.

HTML Hyper Text Markup Language.

CSS Cascading Stale Sheets.

JS Java Script.

UI User Interface.

DOM Document Object Model.

TERP Application Transparente Programmation Réactive.

GPU Graphic Processing Unit.

WEB Worker Education Program.

WEBGL Web Graphic Library.

UX User eXperience.

PWA Progressive Web App.

WEBRTC Web Real Time Communication.

VS Visual Studio.

Introduction Générale.

Introduction Générale

Suite au développement de l'informatique et des télécommunications, La communication en ligne est devenue un élément essentiel de la société moderne. Avec la montée du cyber attaques et de la surveillance en ligne, la sécurité des données est plus importante que jamais. Et avec tant d'informations personnelles et sensibles qui sont transmises en ligne, il est crucial d'avoir des méthodes solides en place pour protéger contre l'accès non autorisé. Ce problème est généralement résolu par le chiffrement, qui garantit que seules les personnes autorisées peuvent accéder au contenu multimédia.

Le chiffrement est le processus de conversion d'informations en un format illisible appelé texte chiffré, afin de les rendre sécurisées et confidentielles. Il est largement utilisé pour protéger la confidentialité des données, notamment lors des communications en ligne, du stockage de données sensibles et des transactions financières.

Le chiffrement a plusieurs techniques et méthodes tel que chiffrement clé publique, chiffrement clé privé, chiffrement basé sur le chaos.

Dans ce travail, nous allons proposer une application web pour essayer les algorithmes de chiffrement d'images et vidéos, qui sont essentiellement basé sur permutation les pixels et décalage les couleurs ou une combinaison entre les deux.

Ce mémoire est organisé cinq chapitres :
Dans le **premier chapitre** parle sur Notions de base.
Le **deuxième chapitre** est consacré aux principes de cryptographie en générale.
Le **troisième chapitre** est dédié à analyse et conception.
Le **quatrième chapitre** sur Réalisation et implémentation.
Le **dernier chapitre** présent l'amélioration possibles sur l'application.

Chapitre 1 :

Notions de base.

1. Introduction

Chaque jour, d'énormes quantités de contenus sont publiées sur web et notamment sur les réseaux sociaux. Par conséquent, il devient de plus en plus difficile d'attirer l'attention des internautes. Grâce à ses graphismes et au niveau visuel de la vidéo, il augmente efficacement et dynamiquement la capacité mémoire du consommateur. Il vous permet à la fois d'attirer et de fidéliser vos clients. Les vidéos sont un excellent moyen d'engager les clients et même de déclencher un achat. Il est particulièrement apprécié pour la facilité d'absorption des informations et inspire un grand engagement même des plus paresseux. [1]

2. Image numérique

Une image numérique est essentiellement une collection de pixels, chaque pixel représentant un point de couleur dans l'image. Les pixels sont organisés dans une matrice 2D, où chaque pixel est identifié par ses coordonnées de ligne et de colonne. Chaque pixel contient des informations sur sa couleur, sa luminosité et d'autres propriétés visuelles.

3. Pixel

Le pixel est l'unité de base de la définition d'une image numérique matricielle. Le terme "pixel" est dérivé de l'anglais "picture element". [11]

Les pixels forment une matrice 2D en une image complète et leur manipulation modifie l'apparence et les propriétés de l'image numérique.

4. Les différents formats d'image

4.1. JPEG

Le format JPEG est le plus couramment utilisé pour les images, en particulier les images d'appareils photo numériques. Sa particularité est la compression des données, ce qui signifie que toutes les informations sont visibles et effacent celles que nos yeux ne peuvent pas voir. [19]

4.2. PNG

PNG est un format qui permet une compression sans perte, c'est-à-dire qu'il prend en charge des images de haute qualité pour une utilisation numérique tout en préservant la couleur et la netteté de l'image d'origine. Contrairement au JPEG, le PNG prend également en charge les images avec des arrière-plans transparents. [19]

4.3. GIF

Vous avez probablement déjà entendu parler de ce format, grâce à sa fonctionnalité la plus populaire qui a pris d'assaut Internet : l'animation. GIF utilise un algorithme de compression sans

perte, qui est idéal pour stocker des graphiques multicolores tels que des graphiques, des logos ou des formes simples. [19]

5. Définition de la vidéo

La vidéo est une séquence d'images à une certaine vitesse. L'œil humain à la propriété de pouvoir résoudre environ 20 images par seconde. De cette façon, lors de la visualisation de plus de 20 images par seconde, l'œil peut croire une image en mouvement. La fluidité vidéo est caractérisée par le nombre d'images par seconde.

D'autre part, la vidéo au sens multimédia est généralement accompagnée de son, c'est-à-dire de données audio.

6. Type de vidéo

Il existe deux types de vidéo :

6.1. Vidéo Analogique

La vidéo analogique, représentant l'information comme un flux continu de données analogiques, destiné à être affichées sur un écran de télévision basé sur le principe du balayage. Il existe plusieurs normes pour la vidéo analogique. Les trois principales sont : PAL, NTSC, SECAM. [2]

6.2. Vidéo Numérique

La vidéo numérique consiste à afficher une succession d'images numériques. Puisqu'il s'agit d'images numériques affichées à une certaine cadence, il est possible de connaître le débit nécessaire pour l'affichage d'une vidéo, c'est-à-dire le nombre d'octets affichés (ou transférés) par unité de temps.

Ainsi le débit nécessaire pour afficher une vidéo (en octets par seconde) est égal à la taille d'une image que multiplie le nombre d'images par seconde. [2]

7. Notions sur la vidéo

Une vidéo est une série d'images fixes avec 3 caractéristiques :

• Le nombre de bits réservés pour l'espace couleur (8 bits pour les images en noir et blanc et 24 bits pour les images en couleurs)

• Le nombre de pixels que comporte chaque image

• Le nombre d'image par seconde.

8. Le besoin du cryptage vidéo

Le cryptage des vidéos est important pour les raisons suivantes :

• Pour empêcher la visualisation indésirable de la vidéo transmise.

• Pour protéger les messages multimédias privés.

• Le cryptage vidéo est utile pour sécuriser les vidéos utilisées dans des services tels que l'apprentissage par vidéoconférence.

• Pour protéger les vidéos médicales pouvant contenir des informations privées d'un patient.

• Pour sécuriser les vidéos provenant des applications de l'internet.

9. Les espaces couleurs

Ce sont des représentations des couleurs d'une image on site parmi ces espaces :

9.1. L'espace RGB

Dans l'espace couleur RGB, chaque pixel est représenté par trois nombres qui indiquent les proportions relatives de rouge, de vert et de bleu. Ce sont les trois couleurs primaires additives de la lumière.

Chaque couleur est codée sur 8 bits, ce qui donne la possibilité d'avoir plus de 16 millions de couleurs différentes. [3]

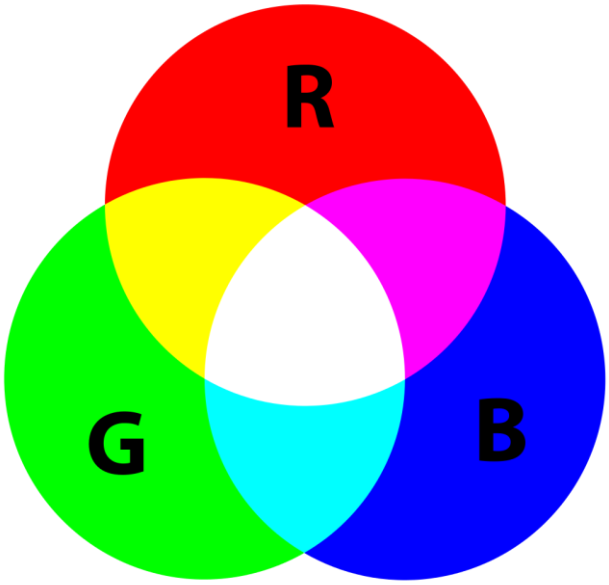

Figure 1.1 : L'espace RGB.

9.2. L'espace YUV

YUV est un système de codage couleur généralement utilisé dans le cadre d'un pipeline d'images couleur. Encode une image couleur ou une vidéo en gardant à l'esprit la perception humaine, ce qui permet de réduire la bande passante pour les composants de chrominance afin

que les erreurs de transmission de la perception humaine ou les artefacts de compression puissent être masqués plus efficacement. [12]

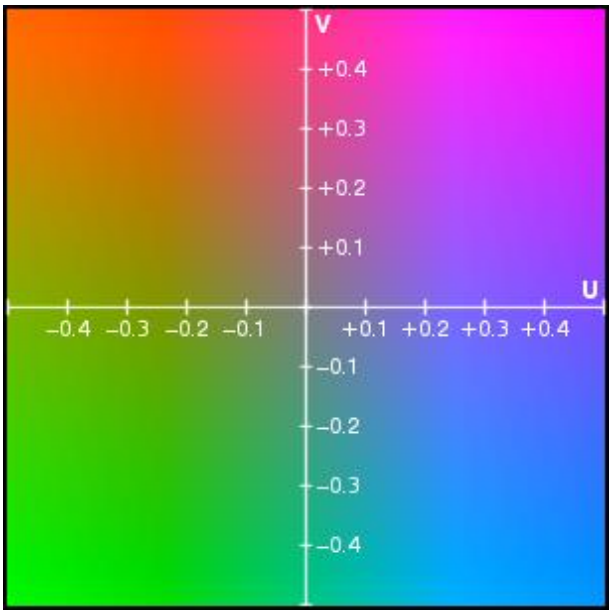

Figure 1.2 :L'espace YUV.

9.3. L'espace Y Cb Cr

Cette norme a été développée lorsqu'il était nécessaire d'assurer la compatibilité entre les récepteurs de télévision noir et blanc et les récepteurs couleur.

Les luminophores rouge (R), vert (anglais : green (G)) et bleu (B) sont juxtaposés pour former une couleur qui doit transmettre trois composantes et trois signaux. Cependant, le noir et le blanc ne contiennent qu'une seule teinte, qui est en niveaux de gris. Ainsi les trois signaux transmis ne sont pas les trois composantes RGB, mais la nuance de gris Y ou Y', et la différence entre cette nuance et les deux autres composantes.

10. Confidentialité et authenticité des données

La confidentialité en ligne fait référence au niveau de confidentialité et de sécurité des informations personnelles publiées en ligne. Il s'agit d'un terme générique qui fait référence à divers facteurs et techniques utilisés pour protéger les données, les communications et les préférences sensibles et privées.

La confidentialité et l'anonymat en ligne sont importants pour les utilisateurs, d'autant plus que le commerce électronique continue de se développer. Les atteintes à la vie privée et les menaces à la sécurité sont des considérations standard lors du développement de toutsite Web. [5]

10.1. Les risques de sécurité [6]

Les vidéos sont devenues un élément essentiel de la communication. Cependant, il y a quelques considérations de sécurité à garder à l'esprit lors de l'utilisation de ce type de technologie. Par exemple, les appels vidéo peuvent être piratés et accéder à des données ou informations sensibles.

Voici les raisons les plus courantes pour lesquelles des données sont volées :

- **Pour compromettre la sécurité**

Dans certains cas, des données sont volées pour compromettre les systèmes de sécurité ou accéder à des informations sensibles.

- **Pour des raisons politiques**

Dans d'autres cas, les données sont volées afin d'obtenir un avantage en politique ou en diplomatie.

- **Pour l'espionnage industriel**

Les PDG et les influenceurs commerciaux partagent souvent des informations sensibles telles que des idées marketing, des stratégies commerciales et des tendances du secteur. Les concurrents pourraient trouver une incitation à « écouter »une réunion importante.

- **Pour un gain financier**

Souvent, les données sont volées afin de les revendre sur le marché noir ou d'extorquer de l'argent au propriétaire.

- **Pour faire des ravages**

Dans certains cas, les données sont volées simplement pour semer le chaos ou perturber les systèmes.

- **Pour un gain personnel**

Parfois, des données sont volées pour exploiter des relations personnelles ou obtenir un avantage déloyal.

11. Les solutions de sécurité [7]

La sécurisation des vidéos est un sujet complexe. Une expertise des différentes techniques de protection est indispensable. Voici les méthodes pour sécuriser les vidéos:

- **Referrer**

  La vidéo est accessible uniquement à partir d'une URL de lecture.

- **Token**

  Un lien crypté unique diffuse la vidéo pour chaque demande.

- **Geo-restriction**

  La vidéo n'est accessible que dans certains pays.

- **L'authentification unique (en anglais ou SSO)**

  La vidéo n'est accessible que pour des utilisateurs authentifiés.

- **Encryption**

  La vidéo est cryptée, empêchant une copie valide localement.

- **DRM**

  La vidéo comprend des instructions de validité.

- **Watermarking**

  La vidéo comprend un système d'identification invisible.

12. Web

Le Web ou World Wide Web en anglais est un système d'information accessible via Internet. Il vous permet de visualiser et de partager des informations sur différents sites Web. Ces pages sont écrites dans un langage de balisage appelé HTML, qui permet d'organiser le contenu afin qu'il soit plus facile pour l'utilisateur de naviguer. Les pages web sont reliées par des hyperliens, vous pouvez donc passer d'une page à l'autre d'un simple clic. [18]

12.1. Application web

Une application Web est un logiciel qui s'exécute dans un navigateur Web. Ils utilisent des applications Web pour contacter les clients de manière pratique et sécurisée. Les fonctions de site Web les plus courantes telles que les paniers d'achat, la recherche et le filtrage de produits, la messagerie instantanée et les flux de médias sociaux sont intrinsèquement des applications Web qui permettent d'accéder à des fonctionnalités complexes sans qu'il soit nécessaire d'installer ou de configurer un logiciel.[23]

12.2. Pourquoi une application web

Le principal avantage est qu'il est disponible partout, vous pouvez vous connecter depuis n'importe quel ordinateur et retrouver toutes vos données synchronisées. Aucune pré-installation n'est nécessaire sur un poste de travail ou une tablette (contrairement à un logiciel ou une application mobile), les sauvegardes sont réalisées de manière centralisée sur le serveur et il n'est plus nécessaire de mettre à niveau tous les postes de travail.

Si la station est remplacée, la mise en œuvre sera beaucoup plus simple et rapide. L'application web vous permet de créer des comptes multiutilisateurs en créant des identifiants et des mots de passe. [24]

13. Conclusion

Dans ce chapitre, nous avons parlé sur l'image et vidéo en général, les problèmes de sécurité et les solutions et le web.

Le chapitre qui suit est consacré aux principes de cryptographie en générale.

Chapitre 2 : Généralité sur la cryptographie.

1. Introduction

Les besoins quotidiens en matière de sécurité ne cessent de croître. Pour cette raison, de nombreuses personnes ont développé des systèmes cryptographiques pour répondre à ces besoins.
Le but principal de la cryptographie est de permettre à deux personnes de communiquer sur un canal non sécurisé de telle sorte qu'un adversaire, un tiers, qui a accès aux informations circulant sur le canal de communication, ne puisse pas comprendre ce qui est échangé. Le canal peut être, par exemple, une ligne téléphonique ou un autre réseau de communication. [10]

2. Historique

Anciennement considérée comme un art, la cryptographie est désormais reconnue comme une science à part entière.
Les premières utilisations connues de la cryptographie remontent à l'Antiquité, où la plus ancienne trace de message chiffré a été retrouvée sur une table en argile sur les bords du Tigre en Irak. Au fil des années, les motivations militaires ont conduit les Hommes à développer de nouvelles méthodes de chiffrement plus robustes afin d'éviter que les tactiques ou plans de bataille ne tombent dans les mains de l'ennemi. Les Spartiates ont ainsi inventé le premier dispositif militaire connu : la scytale, ou bâton de Plutarque. La scytale en elle-même est un bâton de bois, dont le diamètre est connu uniquement de l'émetteur et du destinataire du message.
En 1883, Auguste Kirckhoffs énonce un principe fondateur de la cryptographie moderne
« Les mécanismes de chiffrement et de déchiffrement doivent pouvoir être rendus publics, la confidentialité des messages doit être garantie uniquement par le secret d'une clé ».

De nos jours, en plus de l'amélioration des méthodes classiques, de nouvelles techniques de chiffrement sont introduites, telles que : la cryptographie quantique qui consiste à chiffrer une clé en utilisant des photons envoyés par fibre optique, et toute tentative d'interception de la clé modifie la polarisation des photons ; et la cryptographie chaotique qui se base sur des instabilités de natures inhabituelles des systèmes no
Linéaires.

Ce fut alors la découverte des signaux chaotiques qui ont un comportement déterministe mais qui font penser à des allures pseudo-aléatoires. Le principe de la cryptographie chaotique est alors de noyer le message en clair dans un signal chaotique. Pour le chiffrement et le déchiffrement, on doit alors disposer au niveau de l'émetteur et du récepteur du même signal chaotique pour pouvoir récupérer le message chiffré. [9]

3. Cryptographie

La cryptographie est une technique de protection de l'information et des communications par l'utilisation de codes afin que seuls ceux à qui l'information est destinée puissent la comprendre et la traiter. Empêcher l'accès non autorisé aux informations. Préfixe "crypte" ; signifie "caché" ; et le suffixe graphique signifie "écrire".

En cryptographie, les techniques de sécurité de l'information reposent sur des concepts mathématiques et une série de calculs basés sur des règles, appelés algorithmes, pour transformer les messages d'une manière qui les rend difficiles à décrypter. Ces algorithmes sont utilisés pour générer des clés cryptographiques, des signatures numériques, des contrôles de confidentialité, la navigation sur le Web et pour protéger les transactions sensibles telles que les transactions par carte de crédit et de débit. [8]

4. Types de cryptographie

En général, il existe deux types de cryptographie :

4.1. La cryptographie classique

La cryptographie classique fait référence aux techniques de chiffrement et de déchiffrement utilisées avant l'avènement de l'informatique moderne. Elle englobe un ensemble de méthodes et de protocoles de cryptographie qui ont été développés et utilisés principalement entre l'Antiquité et le début du XXe siècle.

La cryptographie classique repose généralement sur des méthodes de substitution et de transposition :

4.1.1. Chiffrement par substitution

Le chiffrement par substitution est l'une des méthodes de base de la cryptographie. Il s'agit d'une technique de chiffrement où chaque lettre ou groupe de lettres du message clair est remplacé par une autre lettre ou groupe de lettres selon une règle de substitution spécifique. Cette substitution peut être basée sur une clé secrète.

Il existe différents types de chiffrement par substitution, notamment :

4.1.1.1. Chiffrement par substitution mono-alphabétique

Le cryptage mono-alphabétique est l'une des méthodes de cryptage les plus anciennes. Chaque lettre du texte est remplacée par un symbole spécifique (ce symbole peut être une autre lettre de l'alphabet). Sachant que deux lettres différentes doivent être chiffrées avec deux caractères différents pour que le message soit déchiffré de manière unique. [22]

4.1.1.2. Chiffrement par substitution poly-alphabétique

Elle consiste à utiliser plusieurs alphabets décalés pour crypter un message. L'algorithme de substitution poly alphabétique le plus connu est le chiffre de Vigenère. L'idée de Vigenère est de changer une lettre par une autre lettre comme le chiffre de César, mais pas par décalage, il fonctionne par ajouter une clé à plusieurs reprises dans le texte en d'air en utilisant la convention : A=0, B=1,... 2-25, et l'addition est effectuée modulo 26. [25]

4.1.1.3. Chiffrement par substitution homophonique

Dans ce type de chiffrement, chaque lettre du message clair peut être remplacée par plusieurs symboles ou lettres du texte chiffré. Cela rend plus difficile l'analyse statistique et la cryptanalyse. Le chiffre de Playfair est un exemple courant de chiffrement par substitution homophonique.

4.1.2. Chiffrement par transposition

Le chiffrement par transposition (ou le chiffrement par permutation) consiste à faire un réarrangement de l'ordre des lettres qui cache le sens initial. Cette méthode demande de découper le texte clair en blocs de taille identique, et applique la même permutation sur chacun des blocs. [25]

4.2. La cryptographie moderne

La cryptographie moderne fait référence aux méthodes et aux techniques de chiffrement développées à partir de la seconde moitié du XXe siècle jusqu'à nos jours. Elle repose sur des algorithmes mathématiques et des protocoles sophistiqués, offrant une sécurité bien plus robuste que les techniques de cryptographie classique.

La cryptographie moderne se compose de deux grandes familles selon le principe de fonctionnement :

- La cryptographie symétrique.
- La cryptographie asymétrique.

Comme montré dans la figure :

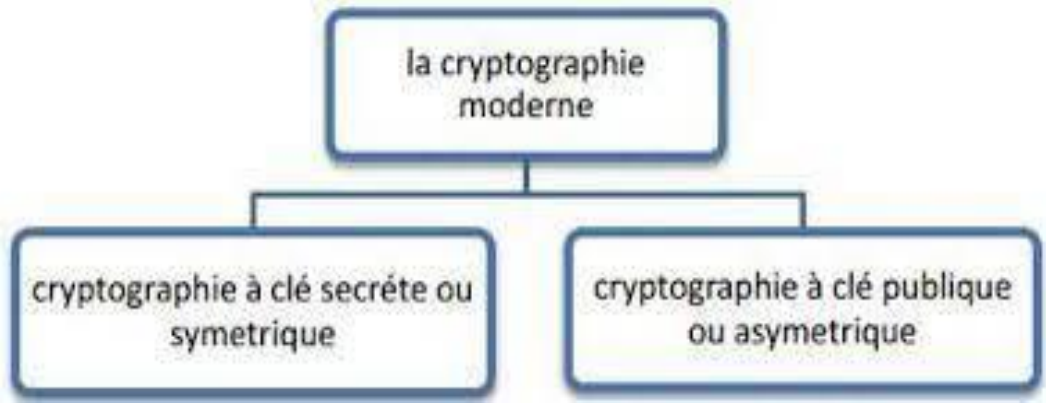

Figure 2.1 : Cryptographie moderne.

4.2.1. Cryptographie à clé symétrique

Les cryptographies symétriques, également appelées cryptographies à clé secrète, sont des techniques de chiffrement où une seule et même clé est utilisée à la fois pour chiffrer et déchiffrer les données. La clé doit être gardée secrète et connue uniquement par les parties légitimes impliquées dans la communication.

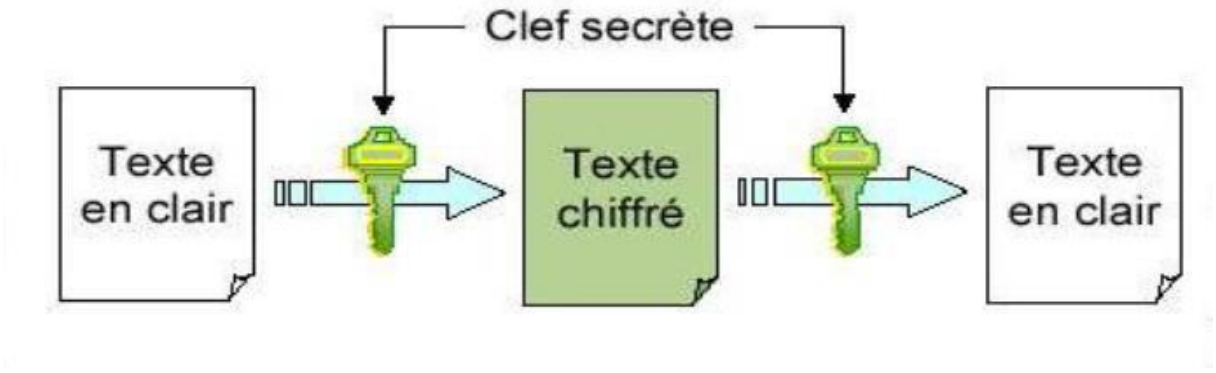

Figure 2.2 : Cryptographie symétrique.

- **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. [4]

- **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. [4]

4.2.2. Cryptographie à clé asymétrique

La cryptographie à clé asymétrique, également connue sous le nom de cryptographie à clé publique, est une méthode de chiffrement qui utilise une paire de clés distinctes pour le processus de chiffrement et de déchiffrement. Cette paire de clés se compose d'une clé publique et d'une clé privée, qui sont mathématiquement liées.

La cryptographie à clé asymétrique est utilisée dans de nombreux domaines, notamment les protocoles de sécurité des communications, les certificats numériques, les signatures numériques, les systèmes de messagerie sécurisée et les transactions en ligne.

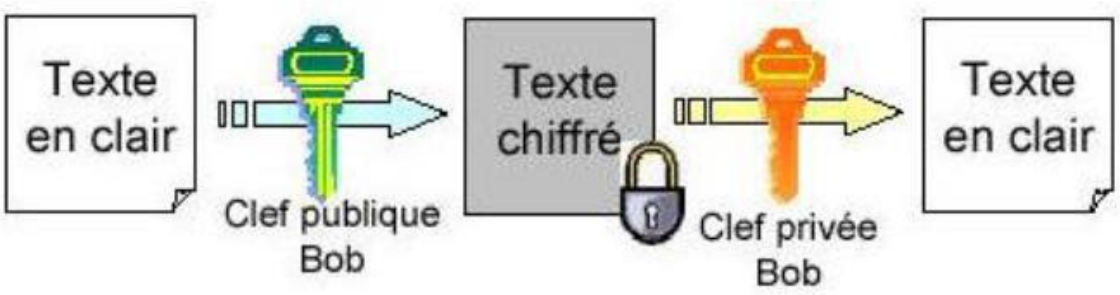

Figure 2.3 : Cryptographie asymétrique.

- **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. [3]

- **La cryptographie à courbe elliptique (ECC)**

La cryptographie des courbes elliptiques englobe un ensemble de techniques cryptographiques qui exploitent une ou plusieurs propriétés des courbes elliptiques, ou plus généralement une variante abélienne. [12]

L'opération de base de l'algorithme ECC est la multiplication scalaire k.P. où k est un entier et P est un point sur la courbe elliptique. [3]

5. Vocabulaire de base de la cryptographie

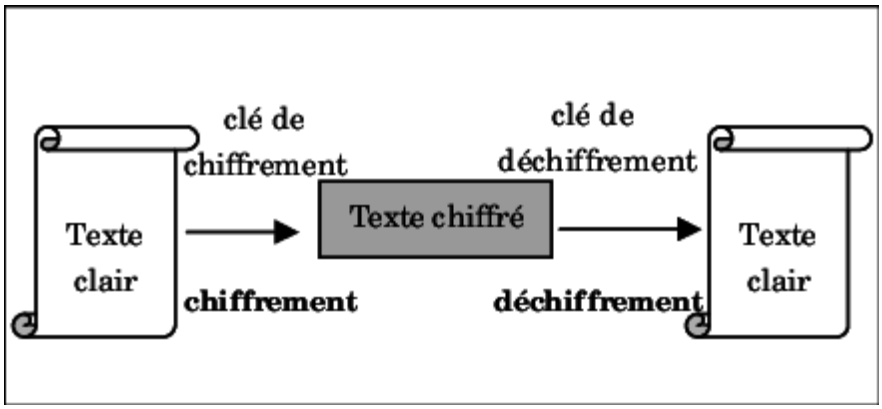

Figure 2.4 : Principe de chiffrement et déchiffrement.

- **Texte claire**

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.

- **Chiffrement**

Il s'agit d'une méthode ou d'un algorithme qui n'empêche toute personne autre que l'expéditeur et le destinataire de comprendre les données.

- **Déchiffrement**

Il s'agit d'une fonctionnalité qui vous permet de trouver des données claire à partir de données chiffrées à condition de connaître la clé de déchiffrement.

- **Clé**

Il s'agit d'un ensemble de paramètres pour l'algorithme de chiffrement ou de déchiffrement sur lequel le secret est basé. Cette combinaison d'algorithmes complexes et de clés valides peut garantir une solution sécurisée et fiable.

- **Crypto système**

Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.

- **Crypter**

Brouiller l'information, la rendre "incompréhensible".

- **Décrypter**

Trouver un message clair qui correspond au message chiffré sans la clé de déchiffrement.

- **Cryptographie**

Cette branche rassemble toutes les méthodes qui permettent de chiffrer et de déchiffrer un texte en clair pour le rendre inintelligible à ceux qui n'ont pas laclé pour le déchiffrer.

- **Cryptanalyse**

C'est l'art de divulguer un texte en clair chiffré sans connaître la clé utilisée pour chiffrer le texte en clair.

6. But de la cryptographie

6.1. Confidentialité

Les informations ne sont accessibles qu'à la personne à qui elles sont destinées et aucune autre personne n'y a accès. [8]

6.2. Intégrité

Les informations ne peuvent pas être modifiées pendant le stockage ou en transit de l'expéditeur au destinataire prévu sans qu'une modification des informations ne soit détectée. [8]

6.3. Authentification

L'identité de l'expéditeur et du destinataire est confirmée. La destination/source de l'information est également confirmée. [8]

6.4. Non-répudiation [10]

C'est un fait qu'un événement (action, transaction) ne peut être nié. Elle Contient :

6.4.1. Non-répudiation d'origine

L'expéditeur ne peut pas nier qu'il a écrit le message, et si c'est le cas, il peut prouver qu'il ne l'a pas écrit.

6.4.2. Non-répudiation de réception

Le destinataire ne peut contester la réception du message et il peut prouver qu'il ne l'a pas réutilisé si c'est effectivement le cas.

6.4.3. Non-répudiation de transmission

L'émetteur du message ne peut nier avoir envoyé le message et il peut prouver qu'il ne l'a pas fait si c'est effectivement le cas.

7. Cryptanalyse [11]

Le cryptanalyse est la technique consistant à dériver du texte en clair à partir d'un texte chiffré sans avoir la clé de chiffrement. Tenter de comprendre un message spécifique s'appelle une attaque.

Une attaque est généralement caractérisée selon les données qu'elle nécessite :

- **Attaque sur texte chiffré seul**

Le cryptanalyse a des copies chiffrées des messages, il peut faire des hypothèses sur les messages originaux qu'il n'a pas. L'analyse cryptique est plus difficile en raison du manque d'informations disponibles.

- **Attaque à texte clair connu**

Le cryptanalyse comprend des messages en texte brut ou des parties d'un message ainsi que des versions cryptées. La cryptanalyse linéaire entre dans cette catégorie.

- **Attaque à texte clair choisi**

Le cryptanalyse contient des messages en clair, elle peut utiliser un algorithme pour créer des versions cryptées de ces messages, qui peuvent ensuite être considérées comme une boîte noire. Le cryptanalyse différentielle est un exemple d'attaque de triche en clair.

- **Attaque à texte chiffré choisi**

Le cryptanalyse a des messages chiffrés et a besoin d'une version texte de certains de ces messages pour effectuer l'attaque.

8. Méthodes de chiffrement des images

L'objectif du chiffrement d'image est de fournir une sécurité visuelle du contenu en clair d'une image.

Les images sont différentes du texte. Bien qu'en théorie on puisse utiliser des méthodes de cryptage traditionnelles pour crypter directement les images numériques, cela n'est toujours pas fortement recommandé pour deux raisons principales. Premièrement, la taille de l'image est généralement beaucoup plus grande que la taille du texte. Par conséquent, le cryptage direct des données d'image à l'aide de méthodes conventionnelles prend beaucoup de temps. La seconde est pour le texte déchiffré, qui doit être identique au texte original. [20]

Pour atteindre cet objectif, différentes techniques de chiffrement d'images ont été proposées, se divisant généralement en deux grandes catégories : les méthodes basées sur le domaine spatial et les méthodes basées sur le domaine fréquentiel.

8.1. Méthode dans le domaine spacial

Le terme domaine spatial fait référence au plan de l'image lui-même, et les approches de cette catégorie sont basées sur la manipulation directe des pixels de l'image. Avec ces algorithmes, le cryptage général casse généralement la corrélation entre les pixels, rendant ainsi les images cryptées incompressibles. [20]

8.2. Méthodes dans le domaine fréquentiel

Pour ce type de méthodes, il est toujours nécessaire de convertir les valeurs de pixels de l'image claire en composantes de fréquence spécifiques avant un traitement ultérieur. [20]
Cette conversion est généralement effectuée à l'aide d'une transformée dans le domaine fréquentiel telle qu'une transformée de Fourier ou une transformée en cosinus discrète.

9. Techniques de cryptage vidéo

Il existe différents schémas de cryptage pour les vidéos, qui peuvent être un cryptage complet ou un cryptage sélectif :

9.1. Approche naïve

Il s'agit d'une méthode de cryptage complète utilisant des systèmes de cryptage traditionnels. Le moyen le plus simple consiste à crypter chaque octet de l'intégralité du flux vidéo à l'aide d'un schéma de cryptage standard tel que DES ou AES. Cependant, pour les films lourds, cet algorithme n'est pas adapté car il est très lent, surtout lors de l'utilisation du Triple DES. En raison du processus de cryptage, la latence augmentera, ce qui ne convient pas au cryptage vidéo en temps réel. [3]

9.2. Algorithme de permutation pure

Il se contente de brouiller les octets dans les trames du flux vidéo par permutation.

9.3. Algorithme de permutation en zigzag

Dans cette approche, au lieu de projeter des blocs 8x8 sur un vecteur 1x64 dans un ordre en zigzag, il projette un seul bloc 8x8 sur un vecteur 1x64 en utilisant une liste permutée aléatoirement (clé). [3]

9.4. Algorithme de cryptage basé sur chaos

C'est algorithme le plus populaire pour effectuer le cryptage et le décryptage, car il s'agit d'un algorithme à faible coût adapté à une grande quantité de donnée.

10. Conclusion

Dans ce chapitre, nous avons présenté l'historique et la généralité de cryptographie. Nous avons débuté par les types de cryptographie, terminologies, But de la cryptographie et les Techniques de cryptage vidéo et l'image.

Chapitre 3 : Analyse et Conception.

1. Introduction

Dans ce chapitre on va présenter deux parties principales : analyse et conception de l'application.

2. Analyse et Conception

2.1. Analyse

L'application doit être accessible et partageable facilement pour le maximum d'appareils. Voici quelques besoins fonctionnels de cette application :

1-Pour réaliser cette opération, il est possible de charger une image, de la chiffrer et potentiellement de la déchiffrer ultérieurement. Le chargement de l'image peut se faire soit à partir du disque, en spécifiant le chemin du fichier et en utilisant une bibliothèque appropriée pour la lecture des données de l'image, soit à partir d'une webcam ou d'une caméra en utilisant une bibliothèque ou un framework adapté. Pour chiffrer l'image, il faut choisir un algorithme de chiffrement, et l'utiliser pour transformer les données de l'image en données chiffrées. Pour déchiffrer l'image, il est nécessaire de conserver en sécurité la clé de chiffrement utilisé et de l'appliquer ultérieurement avec l'algorithme de déchiffrement correspondant pour restaurer les données d'origine de l'image.

2- Dans le cadre du processus de chiffrement d'une image, il est également possible de sauvegarder l'image chiffrée sur le disque ou dans un emplacement de stockage choisi. Une fois que l'image a été chiffrée à l'aide d'un algorithme approprié, vous pouvez utiliser une bibliothèque ou une fonctionnalité du langage de programmation de votre choix pour enregistrer les données chiffrées sur le disque dur ou dans un autre emplacement de stockage. Cela vous permet de conserver l'image chiffrée en sécurité et de pouvoir la récupérer ultérieurement si nécessaire. Vous pouvez spécifier le chemin et le nom du fichier de sortie, ainsi que les options de stockage appropriées pour répondre à vos besoins spécifiques. Assurez-vous de prendre en compte les mesures de sécurité appropriées pour protéger les données chiffrées pendant le stockage.

3-Lorsqu'il s'agit de configurer le chiffrement d'une image, il est possible de personnaliser plusieurs aspects importants. Tout d'abord, vous pouvez choisir l'algorithme de chiffrement à utiliser, en fonction de vos besoins spécifiques en termes de sécurité et de performances. Ensuite, vous pouvez sélectionner l'algorithme de génération de nombres pseudo-aléatoires pour créer des clés de chiffrement sécurisées. Certains langages de programmation proposent des générateurs de nombres aléatoires crypto graphiquement sûrs. En outre, vous avez la possibilité de choisir un mot de passe fort pour le chiffrement de l'image, qui servira à dériver une clé de chiffrement.

Veillez à utiliser un mot de passe complexe, avec une combinaison de lettres, de chiffres et de caractères spéciaux, pour renforcer la sécurité du chiffrement. Enfin, la qualité du chiffrement dépendra de plusieurs facteurs, l'algorithme de chiffrement lui-même et les mesures de sécurité mises en place. Assurez-vous de suivre les meilleures pratiques en matière de chiffrement pour garantir la robustesse et la sécurité de votre processus de chiffrement d'image.

4- Lorsque vous effectuez le chiffrement d'une image, il peut être intéressant d'avoir la possibilité de visualiser l'exécution de l'algorithme étape par étape. Cela permet de mieux comprendre le fonctionnement de l'algorithme de chiffrement et de voir comment il transforme les données de l'image. En visualisant chaque étape du processus, vous pouvez observer les manipulations effectuées sur les pixels de l'image, les transformations appliquées et les résultats obtenus. Elle peut être extrêmement utile pour l'apprentissage et la compréhension approfondie des mécanismes internes de l'algorithme de chiffrement, ainsi que pour le débogage et l'optimisation éventuelle du code.

2.2. Conception

• L'application est codée en deux tiers seulement : le client (le navigateur) et le serveur (hébergeur du code HTML+CSS+JS, il ne comporte aucune logique seulement pour servir des fichiers) et pour pouvoir être accessible la solution doit être une application web hébergée sur serveur accessible publiquement à travers l'internet.

• L'application est séparée en plusieurs pages : une pour chaque type de média ou objectif une page pour le chiffrement d'image et une pour le chiffrement de vidéo.

• Pour la page du chiffrement d'image la page est composée de 4 parties :

1- **Configuration du chiffrement :** vous bénéficiez d'un contrôle précis sur les paramètres de chiffrement, facilitant ainsi l'adaptation du processus de chiffrement à vos besoins spécifiques.

2- **Gestion de l'entrée :** charger image / prendre une photo et la possibilité de réduire la taille de l'image pour économiser du temps pour les appareils les moins puissants. Une partie pour les métadonnées de l'entrée et finalement une partie pour un visuel de l'entrée.

3-**Les actions possibles et la configuration de ces actions :** Lorsque vous travaillez avec des images chiffrées, il est essentiel d'avoir un ensemble d'actions disponibles et de pouvoir les configurer selon vos besoins spécifiques. Parmi ces actions, vous pouvez inclure le chiffrement de l'image, le déchiffrement de l'image, ainsi que la possibilité de prendre la sortie chiffrée et de l'utiliser en tant qu'entrée directe pour le déchiffrement ultérieur. Cette fonctionnalité permet d'économiser du temps et de simplifier le processus de déchiffrement.

4- **Gestion de la sortie :** Il est important de prendre en compte la gestion de la sortie résultante. Cela comprend plusieurs aspects tels que la sauvegarde de l'image chiffrée sur le disque ou dans un emplacement de stockage spécifié. Vous pouvez définir le chemin et le nom du fichier de sortie pour enregistrer l'image chiffrée de manière appropriée.

- Pour la page du chiffrement de vidéo :

1- Configuration du chiffrement.

2- Gestion de l'entrée : Lorsque vous gérez l'entrée d'une image pour un processus de traitement ou de chiffrement, plusieurs aspects sont importants à prendre en compte. Tout d'abord, la taille de l'image joue un rôle crucial, car elle peut influencer les performances et les ressources nécessaires pour traiter l'image. Ensuite, si vous avez la possibilité de choisir la caméra à utiliser, d'une caméra externe ou d'un autre périphérique d'acquisition d'images. Enfin, si vous souhaitez offrir un aperçu visuel de la caméra, vous pouvez inclure une fonctionnalité d'affichage en temps réel de la vidéo provenant de la caméra choisie.

3- Gctions démarrer/arrêter le chiffrement/déchiffrement : Nous pouvons inclure des fonctionnalités permettant de démarrer et d'arrêter le chiffrement ou le déchiffrement des images. Cela offre un contrôle total sur le processus en permettant d'initier ces opérations selon besoins spécifiques.

4- Visuel du chiffrement en temps réel.

5- Visuel du déchiffrement en temps réel.

- Les éléments de chaque page peuvent être cachés pour gagner de l'espace sur l'écran.

2.2.1. Diagramme d'activité

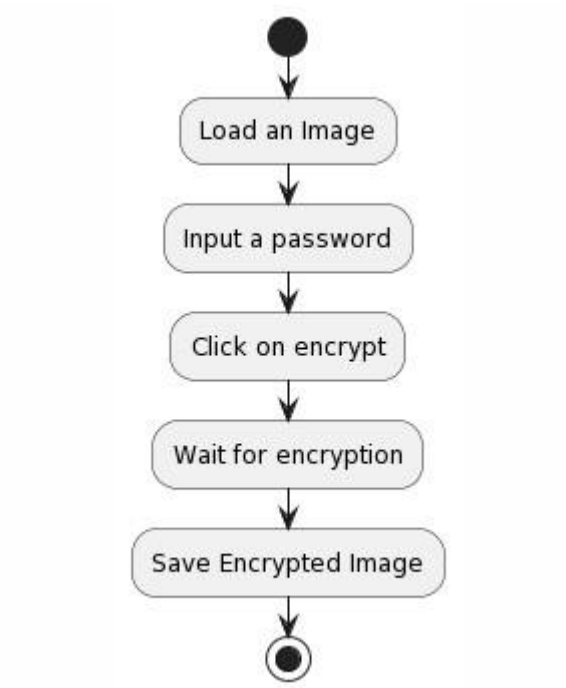

Figure 3.1 : Diagramme d'activité de chiffrement.

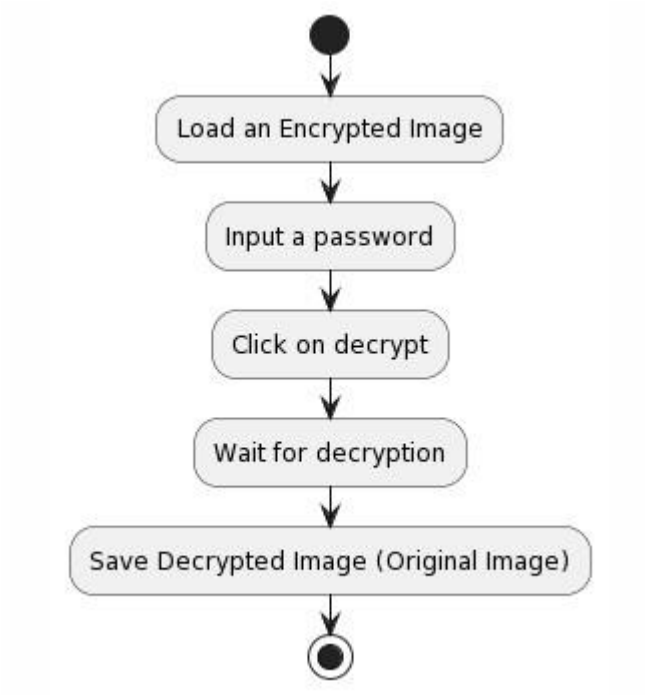

Figure 3.2 : Diagramme d'activité de déchiffrement.

Chapitre 4 : Réalisation et implémentation.

1. Technologies et Environnement de travail

Le langage choisi pour la création de notre application est Type Script avec certains Technologies.

Le gestionnaire de packages choisi est pnpm, car plus efficace que yarn et npm pour l'installation, la liaison et la mise en cache des packages.

L'éditeur de code choisi est VS Code, qui est un éditeur de code source développé par Microsoft.

La création et la compilation de notre application est faite grâce à vitejs. Qui est un outil de développement web léger et rapide qui vise à améliorer l'expérience de développement front-end.

1.1. Langages

1.1.1. Type Script

Type Script est un langage de programmation orienté objet fortement typé, développé en 2012 par Microsoft. C'est aussi un sur ensemble de JavaScript. Cela signifie que tout code valide en JavaScript l'est également en Type Script et qui nous rapporte des fonctionnalités en plus, comme le typage statique optionnel, des classes et des interfaces (programmation orientée objet). C'est un langage qui a explosé en popularité en 2019 et continue sa folle course en 2022. [13]

1.2. Technologies

1.21. React UI

Une bibliothèque de composants d'interface utilisateur React est un outil logiciel ou un système qui contient des composants prédéfinis à utiliser dans des applications et des sites Web basés sur React. Ces bibliothèques de composants permettent d'accélérer le développement de logiciels tout en offrant de nombreux avantages aux développeurs et aux entreprises.

Les composants de la bibliothèque de composants peuvent être des tableaux, des graphiques, des boutons, des cartes, des couleurs, etc. En outre, vous pouvez personnaliser de nombreux outils en fonction de leur conception ou de leur style et les utiliser dans vos applications. [14]

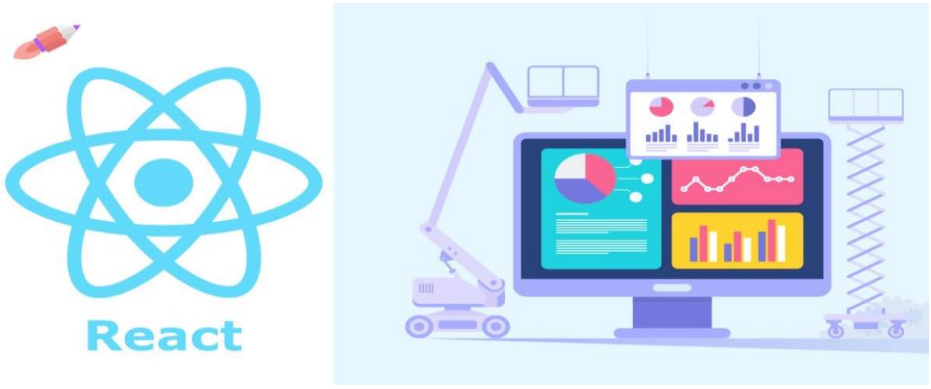

Figure 4.1 : React UI.

1.2.2. Tailwind CSS

Tailwind CSS est un framework qui permet aux développeurs de personnaliser complètement et facilement la conception de leur application ou de leur site Web. Grâce à cette structure CSS, il est possible de créer un design d'interface dans le fichier HTML lui-même.

Ce type de programmation n'entre pas en conflit avec les pratiques recommandées par le W3C telles que la séparation des feuilles de style HTML et CSS. [15]

1.2.3. React Router

React Router est un système de bibliothèque standard construit sur React et utilisé pour créer des itinéraires dans une application React à l'aide du package React Router. Fournit une URL synchrone dans le navigateur avec des données à afficher sur le site Web.

React Router est un processus qui redirige l'utilisateur vers différentes pages en fonction de son action ou de sa demande. Le routeur ReactJS est principalement utilisé pour développer des applications Web d'une seule page. React Router est utilisé pour définir plusieurs routes dans une application.

Lorsqu'un utilisateur entre une URL spécifique dans le navigateur et que le chemin de l'URL correspond au "chemin" dans le fichier du routeur, l'utilisateur sera redirigé vers ce chemin spécifique. [16]

Figure 4.2 : Logo de React Router.

1.2.4. MobX

MobX est une bibliothèque de gestion d'état simple, évolutive et puissante. Comme React, qui utilise un DOM virtuel pour rendre les éléments de l'interface utilisateur dans nos navigateurs, réduisant ainsi le nombre de mutations DOM, MobX fait la même chose mais dans notre état d'application.

MobX a été construit en utilisant TFRP (Transparent Reactive Application Programming). Nous pouvons la considérer comme une bibliothèque réactive : elle rend l'état de notre application cohérent et sans erreur en utilisant un graphe d'état de dépendance réactif qui n'est mis à jour qu'en cas de besoin. [17]

Figure 4.3 : Logo de Mobx.

1.2.5. React-icons

React-icons est une petite bibliothèque pour vous aider à ajouter des icônes (de toutes les différentes bibliothèques d'icônes). Expose les icônes de votre application en tant que composants, ce qui les rend plus faciles à utiliser et vous permet de les personnaliser pour qu'elles correspondent au style général de votre application. React -icons utilise les fonctions ES6 pour importer des icônes dans votre application React, et vous permet d'importer uniquement les icônes de chaque bibliothèque que vous utilisez réellement. [21]

2. Structure du code

Le dossier racine de l'application contient les fichiers de configuration.

Le dossier 'src' contient le code de l'application.

Il est structuré comme suit :

- Les pages de l'application dans le dossier pages.
- Les composants réutilisables dans le dossier composants.
- Toute logique réutilisable dans le dossier utils.

3. Compilation et Déploiement

- La compilation de l'application avec la commande 'vite build' :

Cette commande permet de regrouper tous les fichiers sources d'application et de les transformer en un ensemble de fichiers optimisés prêts à être déployés.

- Une fois le dossier 'dist' (qui contient l'application compilée sous forme de fichier HTML, CSS et JavaScript) il est envoyé chez l'hebergeur pour être servi par un serveur de fichier HTTP, permettant ainsi l'accès à l'application par n'importe qui possédant le lien menant vers ce serveur.
- Cet envoi de fichier est fait grâce à la commande scp basé sur ssh.
- La compilation et le déploiement sont exécutés séquentiellement par une seule commande ('build_deploy') créé spécialement pour simplifier ce processus.

4. Aperçus visuels

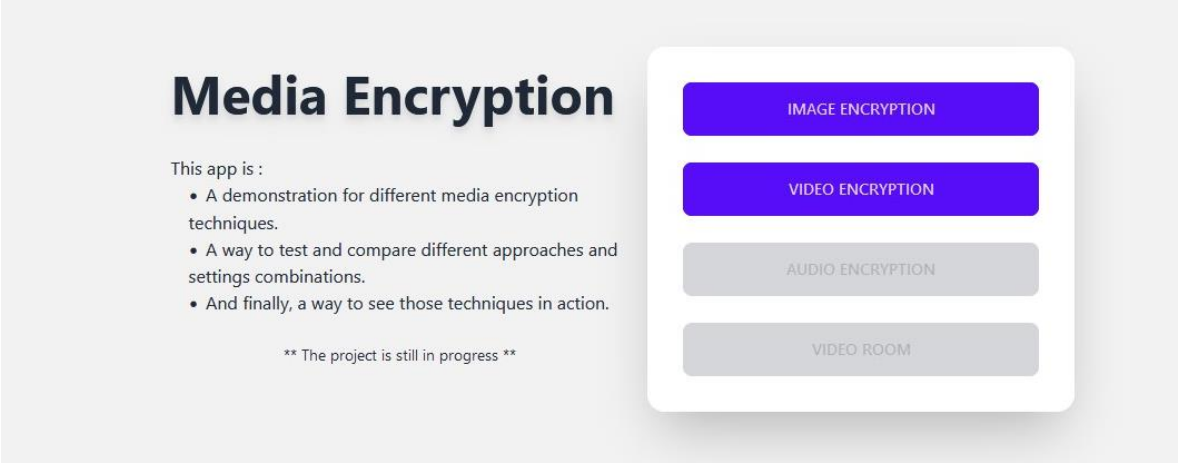

Figure 4.4 : La fenêtre principale.

1. Image encryption : Pour entrer à la fenêtre de chiffrement l'image.
2. Video encryption : Pour entrer à la fenêtre de chiffrement la vidéo.

4.1. La fenêtre de chiffrement et déchiffrement l'image

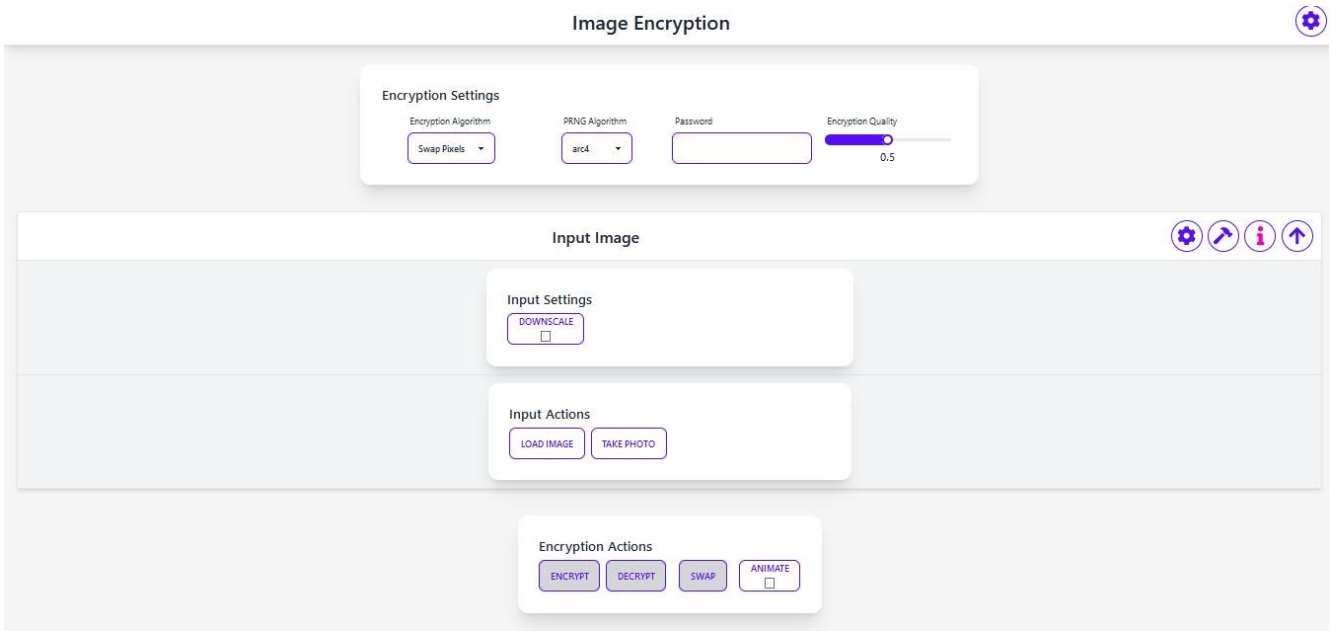

Figure 4.5 : La fenêtre de chiffrement déchiffrement l'image.

4.2. La fenêtre de chiffrement et déchiffrement la vidéo

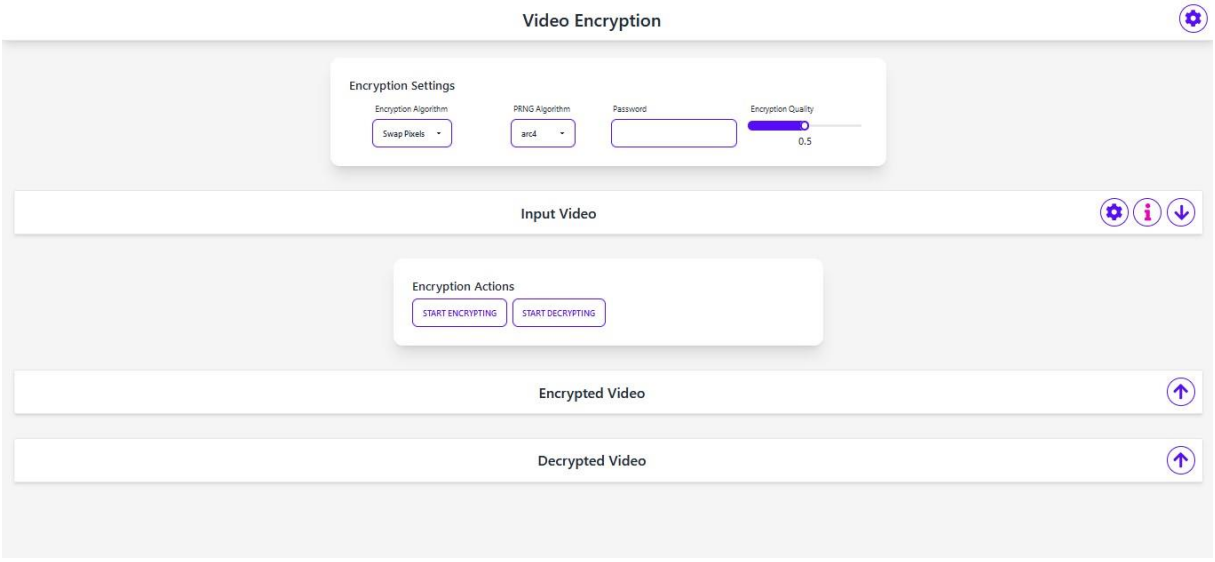

Figure 4.6 : La fenêtre de chiffrement déchiffrement la vidéo.

5. Conclusion

Dans ce chapitre, nous avons vu les technologies et environnement de travail et aperçus visuels de l'application.

Conclusion Générale et Perspectives.

Conclusion Générale

Aujourd'hui, le monde connu un grand développement dans le domaine de réseaux de communication. Donc, la plupart des recherches se concentrent sur l'amélioration des méthodes du chiffrement pour augmenter le taux de sécurité et de confidentialité des données.
Le chiffrement joue un rôle crucial dans protéger la confidentialité des données et en les rendant illisibles pour toute personne non autorisée.
Dans ce mémoire nous avons présenté une application web pour essayer les algorithmes de chiffrement d'image et vidéo basé sur permutation les pixels et décalage les couleurs ou une combinaison entre les deux.

En termes de perspectives, voici quelques idées pour améliorer l'application :
-Interface utilisateur conviviale.
-Ajouter la possibilité de choisir parmi différents algorithmes de chiffrement pour les images et les vidéos.
-Possibilité d'ajouter des algorithmes et de voir leur code sources au travers de l'application sans recompiler tout le code.
- Possibilité d'ajouter des formats d'images et de vidéo, même propriétaire.
- Ajout du chiffrement audio.
- Ajout d'une partie de mise en situation réelle de ces applications.
- Ajouter une page pour afficher le temps d'exécution et la qualité des algorithmes sous forme de graphiques.

Bibliographie.

Bibliographie

[1] La vidéo sur le web, pourquoi, 17 février 2021, https://www.declic-communication.fr/la-video-sur-le-web-pourquoi/

[2] Vidéo et imagerie numérique, https://web.maths.unsw.edu.au/~lafaye/CCM/video/video.htm

[3] AMAROUCHE Badis, Compression et Cryptage des vidéos : application en IoT, Mémoire de Master, Université de Jijel, Faculté des Sciences et Technologie, 2020-2021, P23, P42, 43, 44.

[4] MEDJAHDI Nasreddine, Cryptage Chaotique Basé Sur l'Attracteur Clifford, Mémoire de Master, Université Abou Bakr Belkaid– Tlemcen,
Faculté des Sciences, 2017, P8, 9.

[5] Qu'est-ce que la confidentialité sur Internet ? - définition de techopedia, 2023, https://fr.theastrologypage.com/internet-privacy

[6] L'équipe Crewdle, Sécurité des appels vidéo - Pourquoi c'est important, 13 juillet 2022, https://fr.crewdle.com/blogue/importance-de-la-securite-des-appels-video

[7] 7 méthodes pour sécuriser vos vidéos, 24 novembre 2020,https://www.journaldunet.com/solutions/dsi/1495683-7-methodes-pour-securiser-vos-videos/

[8] KHEMIJA Salah Eddine, GUENDOUZ Abdelouahab, BADAOUI Abderraouf, Etude des suites chaotiques et leurs applications encryptage d'images, Mémoire de Licence, Université de Bordj Bou Arreridj, Faculté des Sciences et Technologie, 2020-2021, P14,15.

[9] KADDOURI Mohammed, Conception et Réalisation d'un Crypto-Système pour la Sécurisation des Données Médicales, Mémoire de Master, Université Jijel, Faculté des Sciences et Technologie, 2020-2021, P4, 5.

[10] HADDI Asmaa, GUESMIA soumeya,Cryptographie chaotique : application sur les images, Mémoire de Master, Université Dr Moulay Tahar de Saida, Faculté de Technologie, 2020, P6 ,7.

[11] Wkipedia, https://fr.wikipedia.org/

[12]Système de couleurs YUV, https://www.hisour.com/fr/yuv-color-system-25916/

[13]Ion Luca, Utilisation du React avec TypeScript, 22 juin 2022, https://www.globalis-ms.com/actualites/react-typescript/

[14] Durga prasad achrya, Bibliothèques de composants React UI, 14 novembre 2022, https://kinsta.com/fr/blog/bibliotheque-composants-react-ui/

[15] Tailwind CSS, le framework totalement personnalisable, 22 mars 2021, https://www.numendo.com/blog/framework/tailwind-css-framework-totalement-personnalisable/

[16] React Router, https://www.javatpoint.com/react-router

[17] Le guide de MobX, 19 avril 2021, https://blog.arcoptimizer.com/le-guide-de-mobx

[18] Lelah, Le Web : une définition, https://commentouvrir.com/tech/le-web-une-definition/

[19] Marie Kaddouch, Les différents formats d'images et comment les utiliser**,** 9 juin 2022, https://fr.wix.com/blog/formats-fichiers-comment-utiliser

[20] LOUZZANI Noura, Contribution à l'amélioration de la transmission sécurisée des images à base du chaos, Mémoire de Doctorat, Université Badji Mokhtar – Annaba, Faculté de Technologie, 2022, P29, 30.

[21] Miracle Ugorji, How to use react-icons to install Font Awesome in a React app, 20 septembre 2021, https://www.freecodecamp.org/news/how-to-use-react-icons/

[22]Chiffrement Mono alphabétique, 12 mai 2018, https://tmonseigne.github.io/Chiffre_Mono/

[23] Qu'est-ce qu'une application Web**,** https://aws.amazon.com/fr/what-is/web-application/

[24] Application web, https://www.syloe.com/glossaire/application-web/

[25] LEMMOUCHI Chahra,Utilisation d'une rotation 3D et des
Systèmes chaotiques pour le cryptage d'images, Mémoire de master, Université de d'oum el bouaghi, Faculté de sciences, 2013, P8.