RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE ECHAHID HAMMA LAKHDAR - EL OUED
FACULTÉ DES SCIENCES EXACTES
Département D'Informatique

Mémoire de Fin D'étude
Présenté pour l'obtention du Diplôme de

MASTER ACADEMIQUE

Domaine : **Mathématique et Informatique**
Filière : **Informatique**
Spécialité : **Systèmes Distribués et Intelligence Artificielle**

Présenté par :
- **Tliba Rahma**
- **Gherghout Fatima**

Thème

Protection hiérarchique des dossiers médicaux par cryptage homomorphique

Soutenue le 09-06- 2022 Devant le jury:

M.	Othmani Samir	MCA	Président
M.	Soltani Khaled	MAA	Rapporteur
M.	Laouid Abdelkader	MAA	Encadreur

Année Universitaire: 2021/2022

Dédicaces

♡ ♡ *À l'exemple du dévouement et de la sincérité ... mon père bien - aimé .* ♡ ♡

♡ ♡*À qui tu as offert mon bonheur et mon réconfort sur son bonheur...ma mère généreuse* ♡ ♡

♡ ♡ *À ceux qui m'aident et me soutiennent chaque jour ... mon cher époux.* ♡ ♡

♡ ♡ *À celui qui m'a donné espoir et patience .....j'aime mon cœur nidal.* ♡ ♡

♡ ♡*A celui qui représente le courage ... ma petite joulia* ♡ ♡

♡ ♡ *A tous ceux qui me souhaitent bonne chance Je vous dédie ce travail* ♡ ♡

♡ ***TLIBA RAHMA*** ♡

Dédicace

♡ ♡*Je dédie ce travail à un symbole d'amour et de dévotion à ma mère* ♡ ♡

♡ ♡*bien-aimée à ceux qui m'ont donné bienveillance, sacrifice et altruisme, mon cher père à l'exemple du don, de la fierté et du sacrifice* ♡ ♡

♡ ♡ *mes sœurs et frères , à toutes mes amies et copines* ♡ ♡

♡ ♡ *à tous ceux qui m'aiment avec sincérité et affection, je vous dédie ce travail* ♡ ♡

♡ ***FATIMA GHERGHOUT*** ♡

Remerciements

Tout d'abord nous remercions notre Dieu qui nous a donné la force et la volonté pour élaborer ce travail.
Nous vifs remerciements à notre encadreur Dr. « LAOUID Abdelkader Qui était chargé de fournir des conseils et des orientations pour chaque petite et chaque grande dans ce mémoire Nous adressons nos sincères remerciements à tous les enseignants du département d'informatique Université Echahid Hamma Lakhdar El - Oued . Aussi à nos collègues de la promotion 2021-2022 . On remercie également tous ceux qui ont participé de près ou de loin à élaborer ce travail

Résumé

Le dossier médical du patient devient un enjeu majeur dans la gestion des établissements de santé,c'est-à-dire que la confidentialité des dossiers médicaux du patient et la protection de leurs données nominatives contre l'accès par des tiers non autorisés sont indispensable.
Ce mémoire vise à définir une nouvelle fonction de cryptage qui assure un cryptage hiérarchique pour respecter la confidentialité des dossiers médicaux. Dans cet objectif, nous concevrons et développerons un système qui protège le dossier médical via un degré élevé de confidentialité du patient est assuré en utilisant la technologie de cryptage homomorphe.

Mots Clés: Protection des données; Chiffrement; Dossier médicaux.

Abstract

The patient's medical record is becoming a major issue in the management of health establishments, that is to say that the confidentiality of the patient's medical records and the protection of their personal data against access by unauthorized third parties are essential.
This thesis aims to define a new encryption function that provides hierarchical encryption to respect the confidentiality of medical records. For this purpose, we will design and develop a system that protects the medical record via a high degree of patient confidentiality is assured using homomorphic encryption technology.

Keywords: Data protection, encryption, Medical records

Table des matières

Liste des figures

Liste des tableaux

Introduction

Internet a changé notre vie quotidienne de plusieurs façons de tel sort que le réseau informatique devient un moyen de communication mondial. Ce dernier a permis aux individus et aux institutions du monde entier de partager et d'échanger des informations, qui peuvent être (textes, images, vidéos, des dossiers...)

Les fichiers numériques contiennent un énorme type d'informations qui entrent dans les communications modernes, car ils sont largement utilisés dans plusieurs domaines tels que (commerce électronique, affaires militaires, dossiers médicaux, etc.), et ainsi la sécurité des fichiers devient une question fondamentale, que ce soit en termes de stockage ou de technologie. Le transfert, l'échange et le cryptage sont l'une des méthodes les plus efficaces pour fournir un environnement sécurisé pour l'échange et la protection des informations.

Il est clair que nous ne pouvons pas utiliser de méthodes de cryptages classiques ou les méthode asymétrique pour crypter les images numériques, de sorte que ces types prennent beaucoup de temps pour effectuer des opérations complexes ou ne sont pas considérés comme très sécurisés.

Les dossiers médicaux sont constitués d'images et d'informations et ces données sont généralement considérées comme données sensibles. Dans ce sens, nous cherchons à proposer une solution qui prenne la les contraintes de la cryptographie et les la sensibilité de ces données. Nous avons observé que le problème qui se pose est comment concevoir un système de cryptage pour assurer la sécurité de ce type de données ainsi qu'un ensemble d'opérations de cryptage.

Le problème est de savoir comment concevoir un système de cryptage pour assurer la sécurité de ce type de données ? Afin de répondre à ce problème, nous avons développé et implémenté un système de chiffrement qui cache le message m en le segmentant aléatoirement(m=m'+m").

où m est une fusion entre un fichier texte, qui se présente sous la forme d'un ensemble de bits, et une image médicale, qui se présente sous la forme d'un ensemble de pixels.

Où nous avons organisé le contenu de cette thèse comme suit Dans le premier chapitre nous avons parlé des généralités sur le chiffrement et des principaux aspects et de la

terminologie qui s'y rattachent, ainsi que du chiffrement symétrique et asymétrique, et nous avons abordé le chiffrement homomorphique, ses types et son histoire....etc.

Dans le deuxième chapitre : nous parlerons des dossiers médicaux et de leurs composants, puis nous irons aux bases de l'image numérique, et nous décrirons un aperçu des images numériques, leurs composants et types, et les outils élémentaires d'analyse d'une Algorithme de cryptage d'image.
Dans le troisième chapitre, nous allons présenter notre algorithme proposé, l'expliquer et clarifier le principe de son fonctionnement. Dans le quatrième chapitre, nous présenterons notre application vérifiée et les différentes étapes d'évaluation pour démontrer la sécurité et l'efficacité de l'algorithme proposé, puis nous terminerons par la conclusion générale et quelques perspectives pouvant aider à améliorer le système dans le futur.

Chapitre 1

Généralité sur la cryptographie

Introduction

De manière générale, la sécurité de l'information est un domaine très vaste qui regroupe tous les aspects de la protection de l'information. Pour assurer sa sécurité, celle-ci doit être cryptée, qui est une méthode d'écriture où un message crypté est écrit à l'aide de codes secrets ou de clés de cryptage. Le cryptage est principalement utilisé pour protéger un message considéré comme confidentiel. Cette méthode est utilisée dans un grand nombre de domaines, tels que la défense, l'informatique, la protection de la vie privée, etc. Il existe de nombreux algorithmes de chiffrement qui peuvent être utilisés pour chiffrer (et déchiffrer pour le destinataire) le message. Certains d'entre eux sont considérés comme basiques (par exemple, la lettre de l'alphabet est décalée vers la droite ou vers la gauche avec un certain nombre de notes), tandis que d'autres offrent un niveau de sécurité quasi absolu. Ainsi dans ce chapitre nous irons à une introduction aux généralités sur la cryptographie, après un bref historique de la cryptographie nous examinerons les grands systèmes cryptographiques moderne.

1.1 La sécurité De L'information

C'est un ensemble de moyens techniques permettant de réduire la vulnérabilité d'un système informatique face à des menaces soudaines [20].

1.2 Définition Du Cryptage

C'est la conversion des données d'un format lisible en un format crypté. Les données chiffrées ne peuvent être lues ou traitées qu'après avoir été déchiffrées. Le chiffrement est la pierre angulaire de la sécurité des données. C'est le moyen le plus simple et le plus important de s'assurer que les informations du système informatique ne sont pas volées ou lues par quelqu'un qui souhaite les utiliser à des fins malveillantes ,Comme le montre dans **Figure 1.1** [13] .Le cryptage des données pour le sécuriser est largement utilisé par

les utilisateurs individuels et les grandes entreprises dans le but de protéger l'utilisateur informations transmises entre le navigateur et le serveur. Un programme de cryptage de données, également appelé « algorithme de cryptage » ou simplement « cryptage », est utilisé pour développer un schéma de chiffrement qui ne peut théoriquement être pénétré que par une puissance de calcul massive [17].

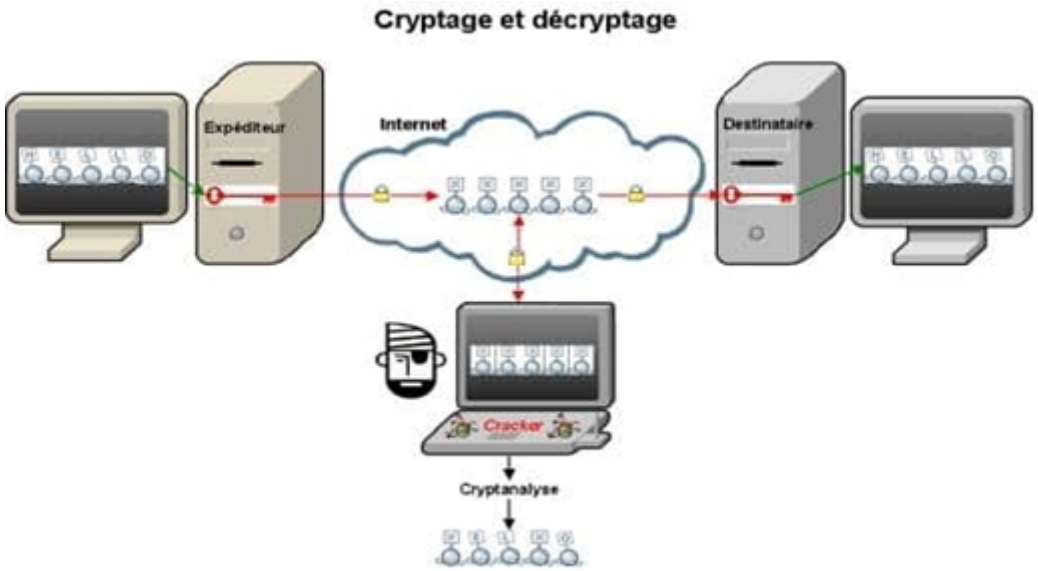

Figure 1.1: Schéma de cryptage

1.3 Historique De Cryptage

Dans ce qui suit, nous mentionnons les étapes par lesquelles l'histoire du chiffrement est passée :

1.3.1 La Cryptographie Est Ancienne

La cryptographie a été découverte depuis l'antiquité, lorsque la plupart des civilisations l'utilisaient comme moyen de remplacer le symbole, qui est la forme de base du cryptage dans les écrits égyptiens anciens et en Mésopotamie, où un exemple réaliste de l'utilisation du cryptage était découvert depuis l'antiquité, et cet exemple remonte à la tombe du noble égyptien Khnumhotep II, qui a survécu il y a environ 3900. Le remplacement du symbole dans l'inscription de ce noble égyptien avait pour but d'améliorer l'attractivité linguistique de son Le cryptage a également été utilisé pour fournir une protection adéquate aux informations importantes et sensibles. L'exemple le plus frappant est l'utilisation d'un écrivain de cryptage il y a environ 3500 ans dans un pays de Mésopotamie pour cacher son été lié aux émaux de poterie, et cette formule a également été utilisé dans les tablettes d'argile. L'histoire de la cryptographie et de ses utilisations pour assurer la protection des informations militaires dangereuses est également évidente.L'exemple le plus frappant

en est l'utilisation du chiffrement pour chiffrer les messages dans la ville de Sparte en Grèce et empêcher les ennemis d'accéder à leur contenu. a également utilisé le cryptage, l'exemple le plus marquant de ce cryptage romain, appelé cryptage César, qui concerne la transformation de lettres en lettres cryptées à travers un nombre spécifié d'endroits en dessous des lettres de l'alphabet latin.

1.3.2 Nouvelle Cryptographie

lorsque nous parlons de l'histoire de la cryptographie récemment, nous entendons par là l'ère de l'ordinateur et la propagation des ordinateurs, où avec l'invention de l'ordinateur, la cryptographie est devenue plus sophistiquée et avancée qu'aupar avant, comme le cryptage mathématique 128 bits est plus fort que les anciens cryptages, qui ont été adoptés pour divers systèmes informatiques et appareils sensibles. Depuis 1990, les informaticiens ont commencé à développer une forme de cryptage moderne et sophistiquée jusqu'à ce qu'ils atteignent la science du codage quantique, qui vise à élever le niveau de protection par rapport à ce qui est disponible dans le cryptage moderne, et récemment, il y a eu une tendance à utiliser le cryptage techniques dans le monde des monnaies numériques afin que ces monnaies bénéficient des techniques de cryptage moderne, notamment la fonction de hachage, les signatures numériques, ainsi que la cryptographie à clé publique, et la priorité à utiliser ces techniques pour assurer la sécurité et la protection des données sur la blockchain réseau et pour authentifier diverses transactions numériques, en plus de cela, une autre forme de cryptage moderne est apparue, connue sous le nom d'algorithme Elliptical Curve Digital Signature ou "ECDSA" qui prend en charge Bitcoin et divers systèmes de cryptage, car il vise à fournir plus la sécurité et la protection des monnaies numériques et s'assurer qu'elles ne sont utilisées que par les propriétaires légitimes [3] .

1.4 Terminologie De La Cryptographie

Il existe plusieurs de termes en cryptographie , notamment

- **Texte en clair** : c'est une information non chiffrée .
- **Texte chiffré** : appelé également cryptogramme , c'est le résultat du chiffrement du texte en clair .
- **Chiffrement** : c'est la méthode ou l'algorithme utilisé pour transformer un texte en clair en texte chiffré .
- **Déchiffrement** : c'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair .
- **Clé** : Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et / ou déchiffrement . Dans le cas d'un algorithme symétrique , la clef est identique

lors des deux opérations . Dans le cas d'algorithmes asymétriques , elle diffère pour les deux opérations .

- **Cryptographie** : cette branche regroupe l'ensemble des méthodes qui permettent de chiffrer et de déchiffrer un texte en clair afin de le rendre incompréhensible pour quiconque n'est pas en possession de la clé à utiliser pour le déchiffrer
- **Cryptanalyse** : est Fart de révéler les textes en clair qui ont fait l'objet d'un chiffre ment sans connaitre la clé utilisés pour chiffrer le texte en clair .
- **Cryptologie** : il s'agit de la science qui étudie les communications secrètes . Elle est composée de deux domaines d'étude complémentaires : la cryptographie et la cryptanalyse
- **Coder , Décoder** : est une méthode ou un algorithme permettant de modifier la mise en forme d'un message sans introduire d'élément secret [25] .
- **Cryptage Homomorphe** : c'est un système de cryptage capable d'effectuer des opérations significatives sur les messages cryptés sans accéder au message d'origine [21] .

1.5 Objectifs Du Cryptage

Aujourd'hui, le cryptage est utilisé non seulement pour maintenir la confidentialité des données, mais également pour garantir leur intégrité et leur authenticité, de sorte que le cryptage résout quatre problèmes différents et importants.

- **Confidentialité** : est le fait de rendre des informations incompréhensibles pour protéger le contenu des informations stockées ou transmises à des personnes autres que les seules parties à une transaction.
- **D'intégrité** : mécanisme permettant de s'assurer que les données reçues par le récepteur n'ont pas été modifiées ou altérées lors de la transmission.
- **L'authentification** : est un mécanisme permettant d'identifier des personnes ou entités et de certifier leur identité Toute assurance à chacun des expéditeurs que son interlocuteur est bien celui qu'il croit Un contrôle d'accès par exemple par mot de passe qui doit être crypté ne peut autoriser l'accès aux ressources qu'aux personnes autorisées
- **Non-Répudiation** : Cela signifie la capacité de vérifier que l'expéditeur et le destinataire sont les deux parties qui prétendent avoir respectivement envoyé ou reçu le message, en d'autres termes, la non-répudiation, c'est-à-dire s'assurer qu'aucun des expéditeurs ne peut refuser la transaction . [30]

1.6 Attaques Sur Un Chiffrement

Il existe plusieurs types d'attaques. Par exemple, le système de chiffrement dépend des enregistrements transformés. On suppose que l'attaquant connaît la forme des répétitions linéaires en plus de la fonction du pluriel, mais pas les conditions initiales des itérations qui composent la clé du code. On doit distinguer entre les types d'attaques d'un adversaire et les buts des attaques d'un adversaire . On distingue habituellement quatre méthodes d'attaque :

- **Une Attaque Par Texte Chiffré Connu** consiste uniquement à trouver la clé de déchiffrement à partir d'un ou d'un seul texte chiffré
- **Une Attaque Sur Un Clair Connu** consiste à trouver une ou plusieurs clés de déchiffrement, connaissant le clair correspondant
- **L'attaque Sur Le Texte En Clair Choisi** consiste à trouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, que l'attaquant a la capacité de générer à partir des textes en clair.
- **L'attaque Sur Le Texte Chiffré Choisi** consiste à trouver une clé de décodage à partir d'un ou plusieurs textes cryptés, où l'attaquant a la possibilité de générer des textes normaux [9].

1.7 Types De Chiffrement

Il existe deux méthodes de cryptage, la plus courante étant le cryptage symétrique et asymétrique.. Les deux noms indiquent si la même clé est utilisée ou non pour le chiffre

1.7.1 Cryptographie Symétriques

Ceci est également connu sous le nom de cryptage par clé privée. La clé utilisée pour le chiffrement est la même que celle utilisée pour le déchiffrement, Comme le montre dans **Figure 1.1** [7] , ce qui rend cette méthode préférable aux utilisateurs individuels et aux systèmes fermés. Sinon, la clé doit être envoyée au destinataire. Cependant, cela augmente le risque d'être piraté s'il est intercepté par un tiers, tel que des pirates. Mais cette méthode est plus rapide que la méthode asymétrique [17].

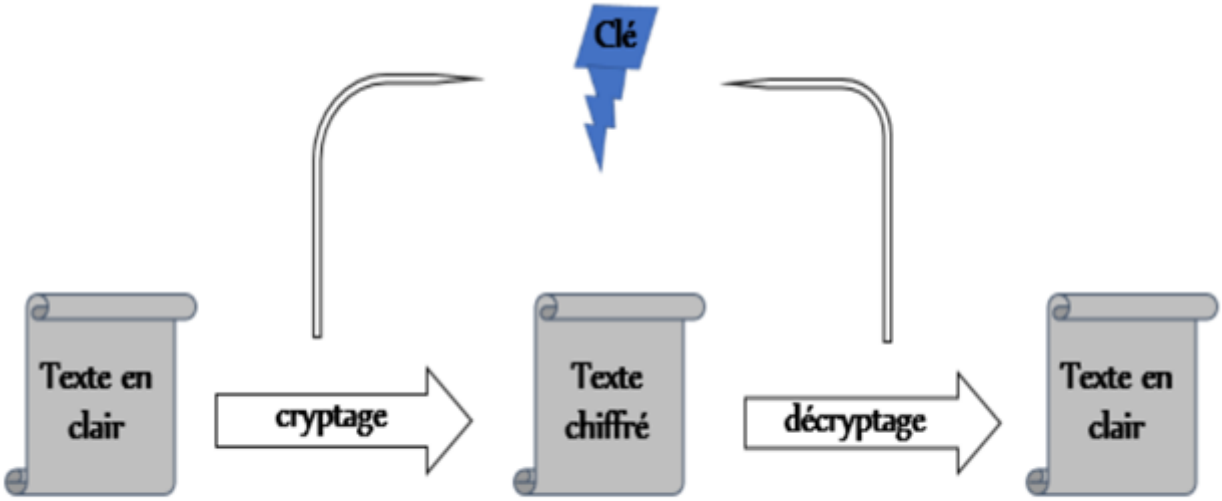

Figure 1.2: Cryptographie Symétriques

1.7.2 Cryptographie Asymétrique

Cette méthode utilise deux clés différentes, une publique et une privée, qui sont liées arithmétiquement. Les deux clés sont fondamentalement de grands nombres, et elles sont liées mais ne sont pas identiques, d'où le nom "asymétrique".
La clé privée est gardée secrète par le propriétaire et la clé publique est soit partagée entre les destinataires autorisés, soit rendue publique. Les données chiffrées avec la clé publique du destinataire ne peuvent être déchiffrées qu'avec la clé privée correspondante.[17] Comme le montre dans **Figure 1.1** [7] .

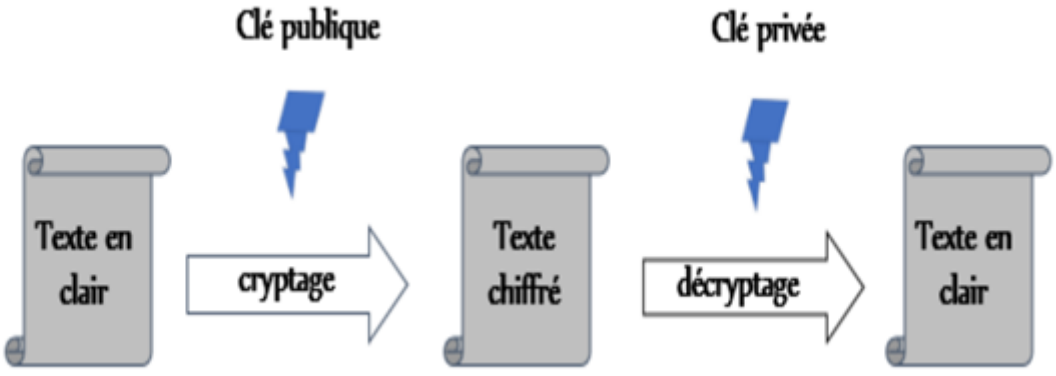

Figure 1.3: Cryptographie Asymétrique

1.8 La Cryptographie Homomorphe

Dans ce qui suit, nous donnerons la définition cryptographie d'homomorphe, son histoire, et ses types :

1.8.1 Définition De La Cryptographie Homomorphe

C'est une forme de cryptage avec certaines propriétés algébriques qui permet la création d'opérations arithmétiques spéciales sur le texte chiffré pour obtenir une correspondance cryptée lors du décryptage à la suite d'opérations effectuées sur le texte d'origine, ce qui signifie que le décodage du résultat de ce processus est sur données non cryptées. Cette fonctionnalité permet d'attribuer des opérations arithmétiques à un agent externe, sans accéder à ses données ou résultats Le service de Cloud computing peut être appelé pour effectuer des calculs en garantissant la confidentialité des données traitées [14].

1.8.2 Historique La Cryptographie Homomorphe

Des schémas de chiffrement homomorphes ont été développés en utilisant différentes approches. Plus précisément, les schémas de chiffrement entièrement homomorphes sont souvent regroupés en générations correspondant à l'approche sous-jacente.

- **Pré-FHE** Le problème de la construction d'un schéma de chiffrement entièrement homomorphe a été proposé pour la première fois en 1978, moins d'un an après la publication du schéma RSA. Pendant plus de 30 ans, on ne savait pas s'il existait une solution

- **FHE De Première Génération**

  Craig Gentry, utilisant la cryptographie basée sur un réseau, a décrit la première construction plausible d'un schéma de chiffrement entièrement homomorphe. Le schéma de Gentry prend en charge à la fois les opérations d'addition et de multiplication sur les textes chiffrés, à partir desquels il est possible de construire des circuits pour effectuer des calculs arbitraires. La construction commence à partir d'un peu schéma de cryptage homomorphe, qui se limite à évaluer des polynômes de faible degré sur des données cryptées ; il est limité car chaque texte chiffré est bruyant dans un certain sens, et ce bruit augmente à mesure que l'on ajoute et multiplie les textes chiffrés, jusqu'à ce que finalement le bruit rende le texte chiffré résultant indéchiffrable. Gentry montre ensuite comment modifier légèrement ce schéma pour le rendre amorçable, c'est-à-dire capable d'évaluer son propre circuit de déchiffrement puis au moins une opération de plus. Enfin, il montre que tout schéma de chiffrement amorçable quelque peu homomorphe peut être converti en un chiffrement entièrement homomorphe grâce à une auto-incorporation récursive. Pour le schéma "bruyant" de Gentry, la procédure

d'amorçage "rafraîchit" efficacement le texte chiffré en lui appliquant la procédure de déchiffrement de manière homomorphe, obtenant ainsi un nouveau texte chiffré qui chiffre la même valeur qu'auparavant mais a moins de bruit. En "rafraîchissant" périodiquement le texte chiffré chaque fois que le bruit devient trop important, il est possible de calculer un nombre arbitraire d'additions et de multiplications sans trop augmenter le bruit. Gentry a basé la sécurité de son schéma sur la dureté supposée de deux problèmes: certains problèmes du pire des cas sur des treillis idéaux et le problème de la somme des sous-ensembles clairsemés (ou de faible poids). Doctorat de Gentry. la thèse fournit des détails supplémentaires. L'implémentation Gentry-Halevi du cryptosystème original de Gentry a signalé un temps d'environ 30 minutes par opération de bit de base. Des travaux de conception et de mise en œuvre approfondis au cours des années suivantes ont amélioré ces premières implémentations de plusieurs ordres de grandeur en termes de performances d'exécution.
En 2010, Marten van Dijk, Craig Gentry, Shai Halevi et Vinod Vaikuntanathan ont présenté un deuxième schéma de chiffrement entièrement homomorphe, qui utilise de nombreux outils de construction de Gentry, mais qui ne nécessite pas de réseaux idéaux. Au lieu de cela, ils montrent que la composante quelque peu homomorphe du schéma idéal basé sur un réseau de Gentry peut être remplacée par un schéma quelque peu homomorphe très simple qui utilise des nombres entiers. Le schéma est donc conceptuellement plus simple que le schéma de réseau idéal de Gentry, mais a des propriétés similaires en ce qui concerne les opérations homomorphes et l'efficacité. La composante quelque peu homomorphe des travaux de Van Dijk et al. est similaire à un schéma de cryptage proposé par Levieil et Naccache en 2008,et également à celui qui a été proposé par Bram Cohen en 1998.

Cependant, la méthode de Cohen n'est même pas additivement homomorphe. Le schéma Levieil – Naccache ne prend en charge que les additions, mais il peut être modifié pour prendre également en charge un petit nombre de multiplications. De nombreux raffinements et optimisations du schéma de Van Dijk et al. ont été proposés dans une séquence d'œuvres de Jean-Sébastien Coron, TancrèdeLepoint, Avradip Mandal, David Naccache et Mehdi Tibouchi. Certains de ces travaux comprenaient également des implémentations des schémas résultants

- **FHE De Deuxième Génération**
  Les cryptosystèmes homomorphes de cette génération sont dérivés de techniques développées à partir de 2011-2012 par ZvikaBrakerski, Craig Gentry, Vinod Vaikuntanathan et d'autres. Ces innovations ont conduit au développement de cryptosystèmes quelque peu et totalement homomorphes beaucoup plus efficaces. Ceux-ci inclus:

- Le schéma Brakerski-Gentry-Vaikuntanathan (BGV, 2011), s'appuyant sur les techniques de Brakerski-Vaikuntanathan
- Le schéma basé sur NTR0U de Lopez-Alt, Tromer et Vaikuntanathan (LTV, 2012)
- Le schéma Brakerski/Fan-Vercauteren (BFV, 2012), s'appuyant sur le cryptosystème invariant à l'échelle de Brakerski ; Le schéma basé sur NTRU de Bos, Lauter, Loftus et Naehrig (BLLN, 2013), s'appuyant sur le cryptosystème invariant d'échelle de LTV et de Brakerski ; La sécurité de la plupart de ces schémas est basée sur la dureté du problème d'apprentissage (en anneau) avec erreurs (RLWE), à l'exception des schémas LTV et BLLN qui reposent sur une variante trop étendue du problème de calcul NTRU. Cette variante NTRU s'est ensuite révélée vulnérable aux attaques de réseau de sous-champs, c'est pourquoi ces deux schémas ne sont plus utilisés dans la pratique. Tous les cryptosystèmes de deuxième génération suivent toujours le plan de base de la construction originale de Gentry, à savoir qu'ils construisent d'abord un cryptosystème quelque peu homomorphe, puis le convertissent en un cryptosystème entièrement homomorphe en utilisant le bootstrap. Une caractéristique distinctive des cryptosystèmes de deuxième génération est qu'ils présentent tous une croissance beaucoup plus lente du bruit lors des calculs homomorphes. Des optimisations supplémentaires par Craig Gentry, Shai Halevi et Nigel Smart ont abouti à des cryptosystèmes avec une complexité asymptotique presque optimale : effectuer des opérations sur des données chiffrées avec un paramètre de sécurité a une complexité de seulement . Ces optimisations s'appuient sur les techniques Smart-Vercauteren qui permettent de regrouper de nombreuses valeurs de texte en clair dans un seul texte chiffré et de fonctionner sur toutes ces valeurs de texte en clair de manière SIMD.Bon nombre des avancées de ces cryptosystèmes de deuxième génération ont également été portées sur le cryptosystème sur les nombres entiers.Une autre caractéristique distinctive des schémas de deuxième génération est qu'ils sont suffisamment efficaces pour de nombreuses applications, même sans invoquer l'amorçage, fonctionnant plutôt en mode FHE nivelé.
- **FHE De Troisième Génération**
  En 2013, Craig Gentry, Amit Sahai et Brent Waters (GSW) ont proposé une nouvelle technique pour construire des schémas FHE qui évite une étape coûteuse de "relinéarisation" dans la multiplication homomorphe.ZvikaBrakerski et Vinod Vaikuntanathan ont observé que pour certains types de circuits, le cryptosystème GSW présente un taux de croissance du bruit encore plus lent, et donc une meilleure efficacité et une sécurité renforcée. Jacob Alperin-Sheriff et Chris Peikert ont ensuite décrit une technique de bootstrap très efficace basée sur cette observation. Ces techniques ont été encore améliorées pour développer des variantes en anneau efficaces du cryptosystème GSW : FHEW (2014) et TFHE (2016). Le schéma FHEW a été le premier à montrer qu'en actualisant les textes chiffrés après chaque opération,

il est possible de réduire le bootstrapping. temps à une fraction de seconde. FHEW a introduit une nouvelle méthode pour calculer les portes booléennes sur des données cryptées qui simplifie grandement le bootstrap et a mis en œuvre une variante de la procédure de bootstrap. L'efficacité de FHEW a été encore améliorée par le schéma TFHE, qui implémente une variante en anneau de la procédure d'amorçage en utilisant une méthode similaire à celle de FHEW

- **FHE de quatrième génération**
  En 2016, Cheon, Kim, Kim et Song (CKKS) ont proposé un schéma de chiffrement homomorphe approximatif qui prend en charge un type spécial d'arithmétique à virgule fixe communément appelée arithmétique à virgule flottante par blocs. Le schéma CKKS comprend une opération de remise à l'échelle efficace qui réduit un message chiffré après une multiplication. À titre de comparaison, un tel redimensionnement nécessite un amorçage dans les schémas BGV et BFV. L'opération de remise à l'échelle fait du schéma CKKS la méthode la plus efficace pour évaluer les approximations polynomiales et constitue l'approche préférée pour la mise en œuvre d'applications d'apprentissage automatique préservant la confidentialité. Le schéma introduit plusieurs erreurs d'approximation, à la fois non déterministes et déterministes, qui nécessitent un traitement spécial dans la pratique. Un article de 2020 de Baiyu Li et Daniele Micciancio traite des attaques passives contre CKKS, suggérant que la définition standard IND-CPA peut ne pas être suffisante dans les scénarios où les résultats de décryptage sont partagés. Les auteurs appliquent l'attaque à quatre bibliothèques de chiffrement homomorphes modernes (HEAAN, SEAL, HElib et PALISADE) et rapportent qu'il est possible de récupérer la clé secrète à partir des résultats de déchiffrement dans plusieurs configurations de paramètres. Les auteurs proposent également des stratégies d'atténuation pour ces attaques et incluent une divulgation responsable dans l'article suggérant que les bibliothèques de chiffrement homomorphe ont déjà mis en œuvre des atténuations pour les attaques avant que l'article ne soit rendu public. De plus amples informations sur les stratégies d'atténuation mises en œuvre dans les bibliothèques de chiffrement homomorphe ont également été publiées[18].

1.8.3 Les Types De Chiffrement Homomorphe

Voici les types de cryptage [27] :

1.8.3.1 Chiffrement Homomorphe Additif

Dans un contexte de chiffrement additif, un serveur distant pourra retourner le résultat d'une opération d'addition sur les messages en clair en faisant le calcul sur des messages chiffrés, sans disposer de la clé secrète.

$$\begin{aligned} \mathbf{ENC}(\mathbf{X}+\mathbf{Y}) &= \mathrm{Enc}(\mathbf{X}) + \mathrm{Enc}(\mathbf{Y}) \\ \prod_{i=1}^{n} \mathrm{ENC}\left(\mathbf{m_i}\right) &= \mathrm{ENC}\left(\sum_{i=1}^{n} m_i\right) \end{aligned} \tag{1.1}$$

En d'autres termes, soient: Encp une fonction de chiffrement à clé publique p. Decs une fonction de déchiffrement à clé secrète s. Alors :

$$\mathrm{Dec}_s\left(\mathrm{Enc_p}(\mathbf{m}) \times \mathrm{Enc_p}(\mathbf{n})\right) = \mathbf{m}+\mathbf{n} \tag{1.2}$$

Les chiffrements qui réalisent cette propriété de chiffrement Homomorphe additif sont : Paillier et Goldwasser-Micalli.

- **Chiffrement Homomorphe De Paillier**
  Le crypto système de Paillier est un crypto système asymétrique, conçu par Pascal Paillier en 1999. Ce crypto système est celui qui a la plus grande bande passante, appelée aussi taux d'expansion : rapport entre la longueur du clair et la longueur du chiffré.

- **chiffrement homomorphe de GM**
  Le crypto système de Goldwasser-Micalli (GM) est un algorithme asymétrique de cryptographie à clé publique, développé par Shafi Goldwasser et Silvio Micali en 1982. Goldwasser et Micali ont introduit la notion de chiffrement probabiliste, tout système de chiffrement doit intégrer de l'aléa dans le processus de chiffrement pour être considéré comme sûr. Le schéma de GM qui repose sur la difficulté du problème de la résiduosité quadratique n'est pas efficace : les textes chiffrés peuvent être des centaines de fois plus longues que les textes d'origine.

1.8.3.2 chiffrement homomorphe multiplicatif

Par analogie avec ce qui précède, un système basé sur le chiffrement homomorphe multiplicatif permet de n'effectuer que des produits sur les clairs, sans disposer de la clé secrète. Définition : Un chiffrement homomorphe est multiplicatif si :

$$\begin{aligned} \mathbf{ENC}(\mathbf{X}+\mathbf{Y}) &= \mathrm{Enc}(\mathbf{X}) + \mathrm{Enc}(\mathbf{Y}) \\ \prod_{i=1}^{n} \mathrm{ENC}\left(\mathbf{m_i}\right) &= \mathrm{ENC}\left(\prod_{i=1}^{n} m_i\right) \end{aligned} \tag{1.3}$$

En d'autres termes, soient : EncP une fonction de chiffrement à clé publique p. DecS une fonction de déchiffrement à clé secrète s.Alors:

$$\mathrm{Dec}_s\left(\mathrm{Enc_p}(\mathbf{m}) \times \mathrm{Enc_p}(\mathbf{n})\right) = \mathbf{m} \times \mathbf{n} \tag{1.4}$$

Parmi les algorithmes Homomorphes permettant ce type d'opération, nous citons RSA

et El Gamal.

- **Chiffrement Homomorphe De RSA**
  Le premier système à clé publique à être proposé fut celui de Ronald Rivest, Adi Shamir et Leonard Adleman connu sous le nom RSA. Cet algorithme a été décrit en 1978. Parmi tous les systèmes cryptographiques asymétriques à l'heure actuelle, RSA est considéré comme des plus solides, si ce n'est solide. Il a résisté à des années de cryptanalyse intensive et il est encore jugé assez robuste pour protéger les échanges bancaires et autres données critiques. Ce niveau de sécurité réside dans la difficulté de factoriser des grands nombres. Retrouver le texte en clair à partir d'une clé et du texte chiffré est supposé équivalent à la factorisation du produit des deux nombres premiers.

- **Chiffrement Homomorphe D'el GamalLe**
  crypto système d'El Gamal est une méthode de cryptographie à clé publique inventée par Taher ElGamal en 1985. Sa sécurité repose sur la difficulté de calculer le logarithme discret.

1.8.3.3 Chiffrement Complètement Homomorphe

avec le chiffrement chiffrement partiellement homomorphe, complètement homomorphe nous pouvons réaliser tout type de calcul sur les données chiffrées stockées dans le Cloud sans les déchiffrer. L'application de ce chiffrement complètement Homomorphe constitue une brique importante dans la sécurité du Cloud. Contrairement au Plus généralement, on pourrait sous-traiter des calculs sur des données confidentielles à des serveurs situés dans Cloud tout en gardant la clé secrète qui permet de déchiffrer le résultat du calcul. En 2014, le chiffrement homomorphe devient très prometteur : la commission européenne appelle dans son dernier appel à projet ICT à utiliser le chiffrement homomorphe dans des applications à l'horizon 2020. Le projet HEAT a réuni avec succès les chercheurs de pointe sur ce sujet en Europe (des universités de Leuven, Bristol et du Luxembourg) ainsi que des partenaires industriels spécialisés en cryptographie avancée (Crypto Experts, NXP et Thales) intéressés par le chiffrement homomorphe .
Définition : Un système de chiffrement complètement homomorphe est un crypto système permettant de faire des calculs sur les données chiffrées sans les déchiffrer. Formellement, si ci(respectivement c2) est un chiffrée de m1 (respectivement m2) il existe deux opérations et $\odot$ tel que :

$$\mathrm{Dec}\left(c_1 \square c_2\right) = \mathrm{Dec}\left(c_1\right) \odot \mathrm{Dec}\left(c_2\right) = m_1 \odot m_2$$

a été initié par Craig Gentry, ensuite DGHV une nouvelle version de son algorithme appliquée sur les entiers a vu le jour en 2010.

- **Chiffrement De Graig Gentry** La première construction d'un système complètement homomorphe a été décrite par Gentry en 2009 où il utilise des idéaux d'anneaux de polynômes. La sécurité de ce schéma repose sur les réseaux idéaux Pour chiffrer un message, l'idée est d'ajouter du bruit, c'est-à-dire des petites erreurs. La clé secrète permet de supprimer ce bruit, à condition qu'il ne soit pas trop gros. Les opérations homomorphes qui sont effectuées impactent également ce bruit, les bruits vont grossir. On ne pourra déchiffrer le message que si les bruits initiaux sont choisis très petits. Pour dépasser cette limitation sur le nombre d'opérations, et lorsque le bruit devient trop 17 important, Gentry applique la méthode de "bootstraping" ou d'amorçage. Si le déchiffrement était suffisamment efficace, on pouvait alors changer de clé publique pour réduire le bruit. On commence par utiliser une première clé, puis, quand le bruit devient trop important, on utilise une seconde clé pour rechiffrer le même message. Le bruit ou (l'erreur) e dans un idéal I d'un anneau R est définit par : e = k|£|cR. Le message est alors chiffré en ajoutant ce bruit au message.

1.8.3.4 Chiffrement Partiellement Homomorphe

On dira d'un crypto système qu'il est partiellement homomorphe lorsque son espace fonctions évaluables est une restriction de l'espace des fonctions calculables. Par exemple, le crypto système à clé publique RSA est partiellement homomorphe vis-à-vis de la multiplication. En effet, si (x,y) est un couple d'entiers, on a alors l'égalité suivante :

$$\begin{aligned} \varepsilon(\mathbf{x}) \cdot \varepsilon(\mathbf{y}) &= \mathbf{x}^{\mathrm{e}} \cdot \mathbf{y}^{\mathrm{e}} \bmod \mathbf{N} \\ &= (\mathbf{x} \cdot \mathbf{y})^{\mathrm{e}} \bmod \mathbf{n} \\ &= \varepsilon(\mathbf{x}, \mathbf{y}) \end{aligned} \tag{1.5}$$

- **Chiffrement De Benaloh** L'algorithme de Benaloh est détaillé ci - dessous :
  Algorithme Benaloh : Génération des clés : r la taille des blocs , p et q deux grand nombres premiers tel que :
  $\mathrm{r} \mid \mathrm{p}-1, \mathrm{pgcd}\left(\mathrm{r}, \frac{p-1}{r}\right) = 1$ et $\mathrm{pgcd}(\mathrm{r}, \mathrm{q}-1) = 1$
  Calculer : $\mathrm{N} = \mathrm{pq}$
  Choisir : $\mathrm{y} \in Z_N^*$ au hasard tel que : $\frac{(p-1)(q-1)}{r} \bmod N \neq 1$
  La clé publique : $(\mathrm{y}, \mathrm{r}, \mathrm{N})$
  La clé privée : (p, q)
  Chiffrement : pour $m£Z_{\mathrm{r}}$ Choisir $u \in Z_N^*$ au hasard Calculer $\mathrm{c} = \mathrm{X}_{\mathrm{m}}^{\mathrm{m}}\mathrm{u}^{\mathrm{r}} \bmod \mathrm{N}$
  Déchiffrement: doit faire une recherche exhaustive pour trouver quel if $\{0, \ldots, \mathrm{p}-1\}$
  Vérifie : $\left(\mathrm{y}^{-1}\mathrm{c} \bmod \mathrm{N}\right)^{\frac{(p-1)(q-1)}{r}} \bmod \mathrm{N} = 1$
  le chiffrement de Benaloh est homomorphe pour l'addition :
  $\mathrm{Dec}_{\mathrm{sk}}\ ((C_1 * C_2) \bmod N) = (m_1 + m_2) \bmod r$

1.8.4 Applications Du Encryption Homomorphe

Le chiffrement Homomorphique est important car il permet d'effectuer des calculs sur des données chiffrées. Cela signifie que le traitement des données peut être externalisé sans avoir à faire confiance à un tiers pour sécuriser correctement les données. Sans la clé de déchiffrement appropriée, les données d'origine ne sont pas accessibles. Il existe de nombreuses applications potentielles de la cryptographie Homomorphic dans le monde réel. Son importance se voit dans de nombreux défis commerciaux majeurs auxquels sont confrontées les entreprises de tous les secteurs.

1.8.4.1 La Vie Privée Des Consommateurs Dans La Publicité

Bien que la publicité soit souvent indésirable, elle peut être utile lorsqu'elle est adaptée aux besoins des utilisateurs, par exemple par le biais de systèmes de recommandation ou de publicité géolocalisée. Cependant, de nombreux utilisateurs sont préoccupés par la confidentialité de leurs données, en l'occurrence leurs préférences ou leur localisation. Il y avait plusieurs approches à ce problème. Jeckmans et al. Dessinez un scénario où l'utilisateur veut des recommandations pour un produit. Le scénario est conçu autour d'un réseau social où les recommandations sont basées sur les goûts des amis de l'utilisateur sous condition de confidentialité. Le système proposé met en œuvre un processus de clonage homogène pour permettre à l'utilisateur d'obtenir des recommandations d'amis sans révéler l'identité du recommandeur. Armknecht et Strufe ont introduit un système de recommandation où l'utilisateur reçoit des recommandations cryptées sans que le système ne soit au courant du contenu. Ce système est basé sur un schéma de clonage hautement symétrique mais très efficace développé à cet effet. Cela permet le calcul d'une fonction qui sélectionne l'annonce pour chaque utilisateur tandis que l'annonce reste cryptée. Dans une autre méthode de publicité personnalisée, l'appareil mobile envoie la position de l'utilisateur au fournisseur, qui renvoie ensuite à l'utilisateur des publicités personnalisées, telles que des coupons de réduction pour les magasins à proximité. Bien sûr, cela permettra probablement au fournisseur de tout surveiller sur les habitudes et les préférences de l'utilisateur. Cependant, ce problème peut être résolu par un cryptage symétrique à condition que les publicités proviennent d'un tiers (ou de plusieurs parties) et qu'il n'y ait pas de collusion avec le fournisseur [5].

1.8.4.2 Système Médical

Afin d'améliorer la qualité des soins de santé, le dossier de santé électronique est la meilleure approche pour maintenir les dossiers des patients. Un dossier médical électronique (DSE) est un enregistrement des détails médicaux d'un patient au format numérique. Cette méthode présente plusieurs avantages par rapport aux documents

papier. Le dossier de santé électronique nous aide à conserver un grand nombre de dossiers, y compris l'efficacité et la mise à jour rapide des dossiers avec précision . Ce système de dossiers médicaux comprend des résultats de laboratoire, des listes de médicaments, des tests de diagnostic, des évaluations physiques, des notes sur les antécédents et des outils de gestion de la santé des patients. Un même dossier patient peut être consulté par plusieurs utilisateurs. Ces données sont stockées dans le cloud public. Il existe de nombreux problèmes de sécurité dans le cloud computing et c'est pourquoi la confidentialité doit être prise en considération. En raison du nom, de l'adresse et d'autres dossiers médicaux du patient, il peut y avoir un risque de vol, d'accès non autorisé et de violation de données. Ces registres doivent être tenus efficacement. L'accès de tiers à ces enregistrements peut être autorisé en cryptant le message d'origine à l'aide d'algorithmes de cryptage. Les unités de santé peuvent nécessiter que certaines opérations soient effectuées sur des données stockées dans le cloud et se rapprochent des fournisseurs de services cloud. Dans ce cas, les propriétaires doivent divulguer les données originales. Il doit donc y avoir une approche pour effectuer des opérations sans exposer le message d'origine. Le chiffrement symétrique permet d'effectuer le calcul sur un texte chiffré, puis les résultats des opérations effectuées par le propriétaire peuvent être déchiffrés. Désormais, le propriétaire des données peut recevoir le même message que s'il était exécuté sur deux textes en clair. La propriété homomorphe fournit un moyen de préserver les données d'origine en permettant à un tiers d'effectuer des opérations sur les données chiffrées [28].

1.8.4.3 Secteur Financier

Dans le secteur financier, les clients et les entreprises travaillent avec des informations confidentielles. De ce fait, les fonctions calculées sur les données ainsi que les données elles-mêmes doivent rester privées. "Par exemple, les données sur les sociétés, les cours des actions ou leur performance ou leur inventaire sont souvent pertinentes pour prendre des décisions d'investissement. Les données peuvent même être diffusées en continu, reflétant les informations les plus récentes nécessaires à la prise de décisions à des fins commerciales". En raison de ces facteurs, les fonctions nécessaires pour effectuer ces calculs sur ces données doivent être exclusives. Ces informations peuvent contenir de nouveaux modèles prédictifs de performance du cours des actions qui peuvent être le résultat de recherches coûteuses menées par des analystes financiers. Comme on pouvait s'y attendre, la plupart des entreprises aimeraient garder ces modèles privés pour rester compétitives dans leurs domaines respectifs et pour protéger leurs investissements. Si une technique de cryptage FHE est incorporée, certaines de ces fonctions peuvent être évaluées en privé. Par exemple, un client peut télécharger une version cryptée de la fonction dans le cloud, comme un programme dans lequel certaines des évaluations sont des entrées cryptées en texte brut. Les données de streaming peuvent être cryptées avec la clé publique du client et téléchargées sur le cloud. Le service cloud évaluerait alors la

fonction privée en appliquant la description chiffrée du programme aux Linnuts chiffrés qu'il reçoit. Après traitement, le cloud renvoie ensuite la sortie chiffrée au client [26].

Conclusion

Dans ce chapitre, nous avons présenté en général quelques concepts de base et l'histoire du chiffrement, les différents types de chiffrement, les attaques de chiffrement ainsi que le chiffrement homomorphe et certaines de ses utilisations et son histoire.

Chapitre 2

Cryptage des dossiers médicaux

Introduction

Aujourd'hui le dossier médical numérique est largement utilisé, et donc la sécurité de ces informations est importante, grâce au développement des techniques d'échange de ces données. Dans ce chapitre, nous parlerons du dossier médical et de ses composants, des bases de l'image et de ses différents types, puis nous aborderons les outils de base pour l'analyse de l'algorithme de cryptage d'image, tels que l'espace clé, l'histogramme, etc., et enfin on termine avec les dernières techniques de cryptage nécessaires à une image

2.1 Définition Dossier Médical

Le dossier médical du patient est la base de tout système de santé informatisé, car il représente un point central où sont extraites toutes les données médicales du patient liées à la fourniture de ses soins de santé ,S'il s'agit d'un référentiel d'informations qui comprend toutes les informations sur les patients. L'un des avantages du dossier médical électronique est qu'il se caractérise par la précision de son contenu et la facilité d'accès par le biais des systèmes de gestion des établissements médicaux et des réseaux d'information, ainsi que par l'Internet international qui permet la communication entre les utilisateurs, y compris les médecins et les patients de différents pays de le monde [1].

2.2 Avantages Du Dossier Médical Numérique

Le dossier médical numérique du patient présente plusieurs avantages qui font que chaque établissement médical n'abandonne pas son application. Se débarrasser du papier qui est devenu une menace pour les organismes de santé en raison des multiples effets négatifs, tels que : (mouvements lents, difficulté à récupérer l'information et un grand nombre de données perdues). Le dossier de santé numérique est le point de rencontre de tous les systèmes, pour contenir le dossier médical numérique sur tous les résultats médicaux, les diagnostics, les traitements effectués pour le patient et les médicaments

qui lui sont donnés. Il offre la possibilité de créer une communication entre les individus et les équipes fournissant des services de santé, y compris les médecins, les infirmières et les administrateurs. Les dossiers médicaux numériques contiennent de nombreuses informations qui contribuent au développement de la recherche scientifique, et fournissent des rapports et des statistiques médicales et administratives qui servent les activités de l'hôpital. Fournit la possibilité de relier les hôpitaux entre eux. Aide à améliorer et à l'exactitude des données enregistrées dans le dossier de santé. Il contribue à améliorer la qualité des soins de santé prodigués au patient en fournissant les informations nécessaires en temps opportun . Augmenter l'efficacité des services de santé et réduire les coûts en accélérant l'échange de information [1].

2.3 Composantes D'un Dossier Médical

Le dossier médical contient toutes les informations personnelles et administratives du patient, les informations de diagnostic médical, les antécédents pathologiques, les actes thérapeutiques effectués et les approbations de ces actes, les résultats des analyses médicales, les radiographies, les traitements médicamenteux et non pharmacologiques, Allergie médicamenteuse ou allergie à certaines substances, groupe sanguin, mesures corporelles et taux vitaux...etc. Nous en concluons que le dossier médical numérique est divisé en deux parties [24].

2.3.1 Texte numérique

C'est celui qui est lu sur différentes plateformes numériques, telles que les ordinateurs, les téléphones portables, les tablettes, etc

2.3.2 Image numérique

Dans ce qui suit, nous expliquons l'image numérique et ses types :

2.3.2.1 Définition D'une Image

Une image est une représentation planaire d'une scène ou d'un objet situé dans un espace tridimensionnel et défini par une fonction bidimensionnelle, f(x,y), où x et y sont des coordonnées spatiales (planes), appelées la magnitude de f à n'importe quelle paire de coordonnées (x,y) L'intensité ou le niveau de gris de l'image à ce point [12].

2.3.2.2 Définition Image Numérique

Une image numérique est une image virtuelle qui n'existe que dans la mémoire d'un ordinateur ou dans un fichier sous la forme d'une séquence numérique binaire (1-0) qui décrit l'image telle qu'elle devrait apparaître sur un écran d'ordinateur. Il est constitué de carrés appelés "pixels". Ces pixels se verront attribuer des nombres binaires pour spécifier

des nuances de gris ou des couleurs [11] . Comme le montre dans Figure 2.1 suivante [10] .

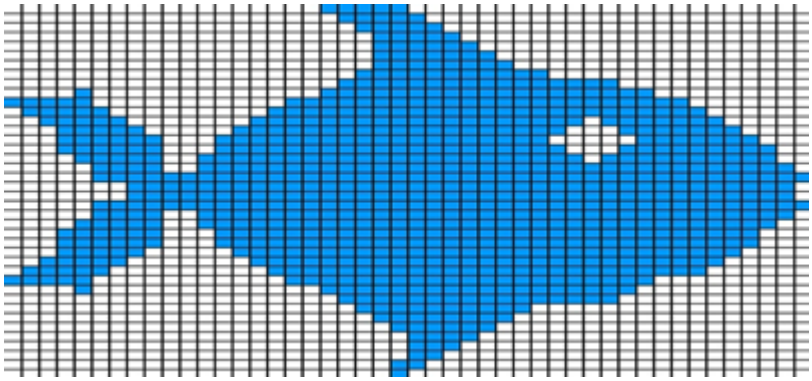

Figure 2.1: Image Numérique

2.3.2.3 Pixel

Le mot pixel provient d'une abréviation de l'expression britannique « PICture Element ». Il est le plus petit élément constitutif d'une image numérique [6] . Comme le montre dans Figure 2.2 suivante [12] .

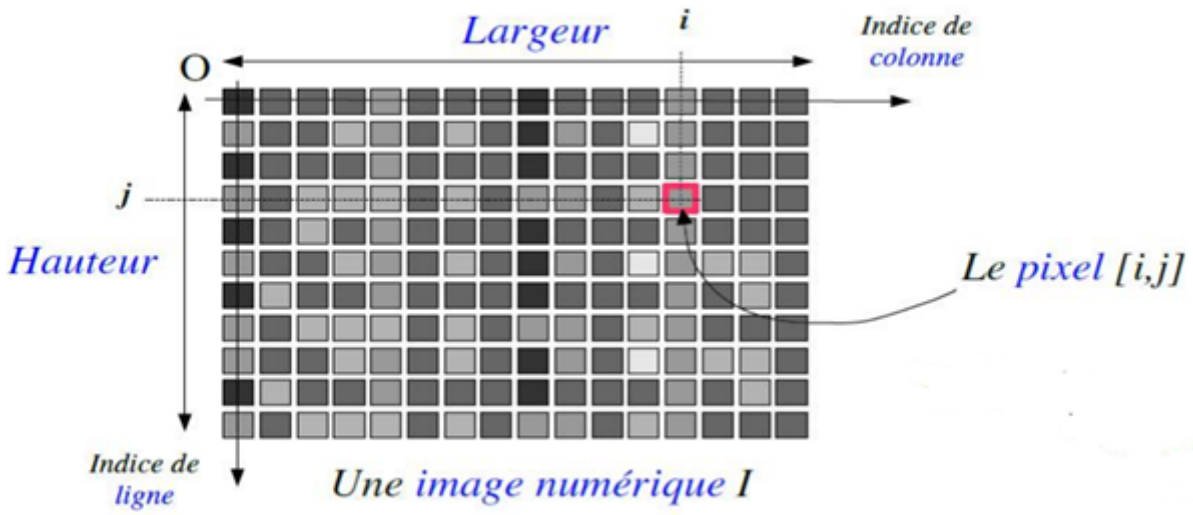

Figure 2.2: Pixeles par lignes et colonnes

2.3.2.4 Types D'images Numériques

Il existe deux types d'images numériques :

- **D'images Vectorielles**
  Formée de lignes calculées de manière géométrique .Lors d'un zoom avant ou arrière, la forme est recalculée en fonction de notre position sans perte de qualité. L'image

vectorielle utilise également la technologie Pixel, mais cette fois, sa position et sa couleur ne sont pas fixes car elle s sont calculées dynamiquement par le logiciel. Autrement dit, pour afficher une ligne par exemple, le programme précise le point de départ, le point d'arrivée puis le chemin à suivre. Ensuite, il calcule et place tous les pixels nécessaires pour afficher cette ligne. Il en va de même pour les formes et les couleurs plus complexes. Cette technique est souvent utilisée pour travailler avec des panneaux graphiques ou créer des logos ou des bandes dessinées [23] [22]. Comme le montre dans Figure 2.3 2.3 suivante [15] .

Figure 2.3: Image vectorielle

- **D'image Matricielle (bitmap)**
  Formée d'une grille composée de points carrés individuels nommés pixels. Plus on zoom, plus les pixels deviennent apparents. Chacun pouvant avoir une couleur différente. Une image matricielle est càractérisée notamment par : Sa dimension en pixels Sa résolution Son mode colorimétrique - Nous traiterons seulement d'images matricielles, car les images numérisées sont matricielles. [23] Comme le montre dans Figure 2.4 2.4 suivante [15] .

Figure 2.4: Image Matricielle

2.3.2.5 Codage Des Images

pixel représente un point de l'image (dans un espace colorimétrique prédéfini). Un pixel est codé suivant la qualite de l'image

- **L'image Binaire**
  Dans une image en noir et blanc (image binaire), un seul bit suffit pour coder le

point (0 pour noir, 1 pour blanc) comme mentionné sur la Figure 2.5 suivante [12] .

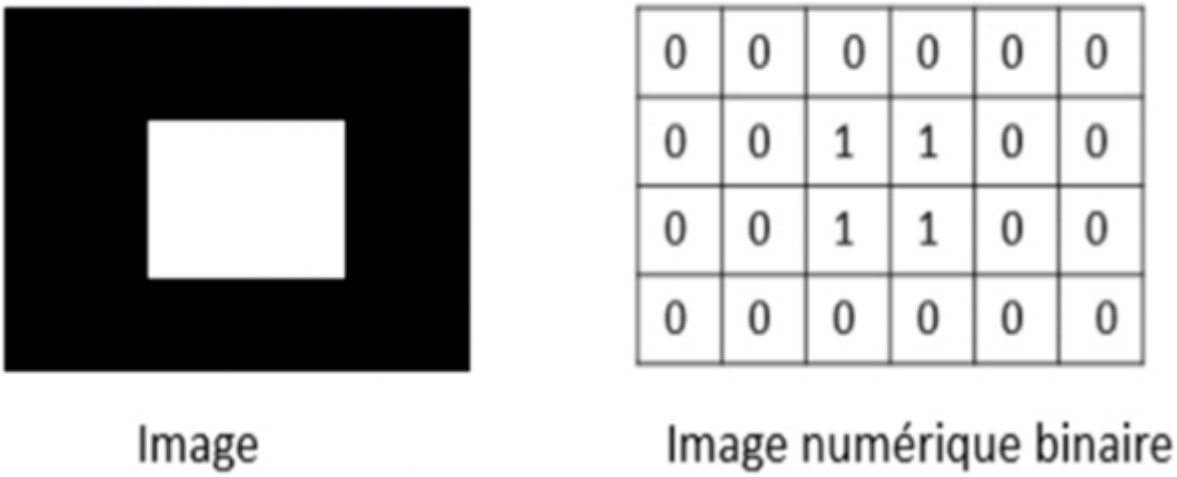

Figure 2.5: Représentation numérique d'une Image binaire

- **L'image En 256 Nuances De Gris**
  Dans une image en 256 nuances de gris, chaque pixel est représenté par un octet (8 bits). Nous ne code ici que le niveau de l'intensité lumineuse, généralement sur un octet (28 = 256 valeurs). Par convention, la valeur zéro représente le noir (intensité lumineuse nulle) et la valeur 255 le blanc (intensité lumineuse maximale) comme mentionné sur la Figure 2.6suivante [12] .

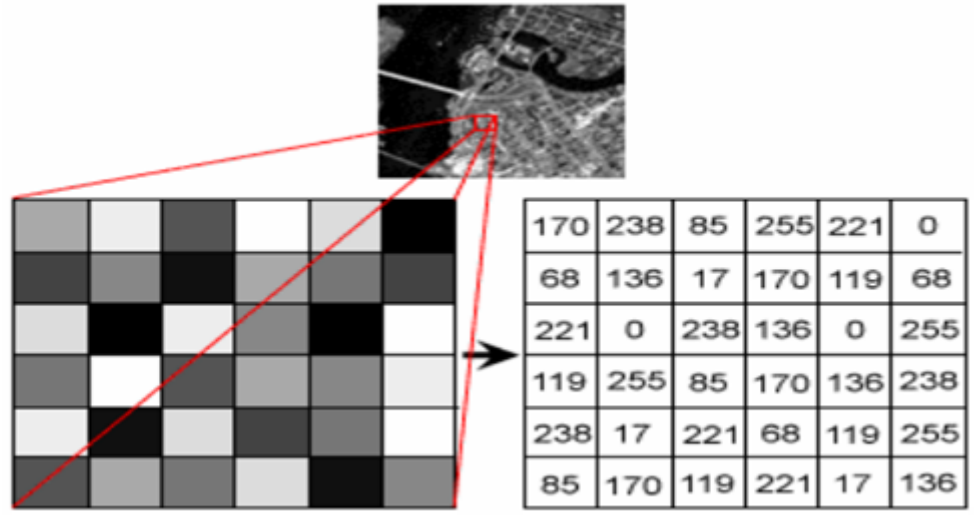

Figure 2.6: Représentation numérique d'une image niveau de gris.

- **Image Couleur (RVB)**
  Dans image en couleurs chaque pixel possédé une couleur décrite par la quantité

de ces 3 composants : rouge(R), vert(V) et bleu (B), chacune de ces couleurs est codée sur l'intervalle [0, 255].) La combinaison de ces trois couleurs donne un point lumineux (un pixel) d'une certaine couleur. Done Le système RVB est une des façons de décrire une couleur en informatique. Par exemple :Le triplet (255, 255, 255) donnera du blanc (255, 0, 0) un rouge pur, 100, 100, 100 un gris, etc. Le premier nombre donne la composante rouge, le deuxième la composante verte et le dernier la composante bleu[1]. comme mentionné sur **la Tableu 1.1** suivante :

Couleur	Blue	Vert	Rouge
Noir	0	0	0
Nuance de noir	1	0	0
Rouge	0	0	255
Vert	0	255	0
Bleu	255	0	0
Gris	128	128	128
Blanc	255	255	255

Tableau 2.1: **Représentation numérique d'une Couleur**

2.4 Les Outils élémentaires D'analyse D'un Algorithme De Cryptage D'image

Dans ce qui suit, nous mentionnons les outils de base pour analyser l'algorithme de chiffrement d'image :

2.4.1 Espce De Clé

La taille de l'espace de clé est nécessaire pour assurer la sécurité contre l'attaque par force brute. Par exemple, si la taille de clé est 512 bit, alors l'espace de clé fournit c'est 2512 (E 10154 Clé combinaisons possibles). Ainsi, si un ordinateur fait 1010 calculs par seconde, il faudra environ de 10136 d'ans pour trouver la clé.

2.4.2 Histogramme

L'histogramme est une représentation graphique qui permet de connaître la répartition de l'intensité lumineuse d'un pixel de sorte qu'il fournit de nombreuses informations sur la répartition des niveaux de gris (couleur) et de connaître les frontières qui sont réparties entre la plupart des niveaux de gris. niveaux (couleur) dans le cas d'une image très claire ou très sombre comme mentionné sur la Figure 2.7 et la Figure 2.8 suivante :

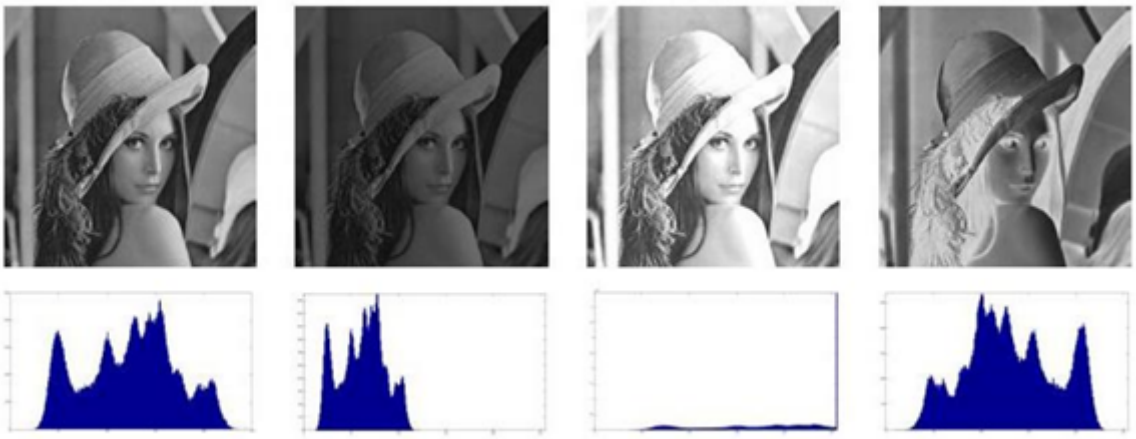

Figure 2.7: Histogramme relatifs à diverses d'une image en niveau de gris.

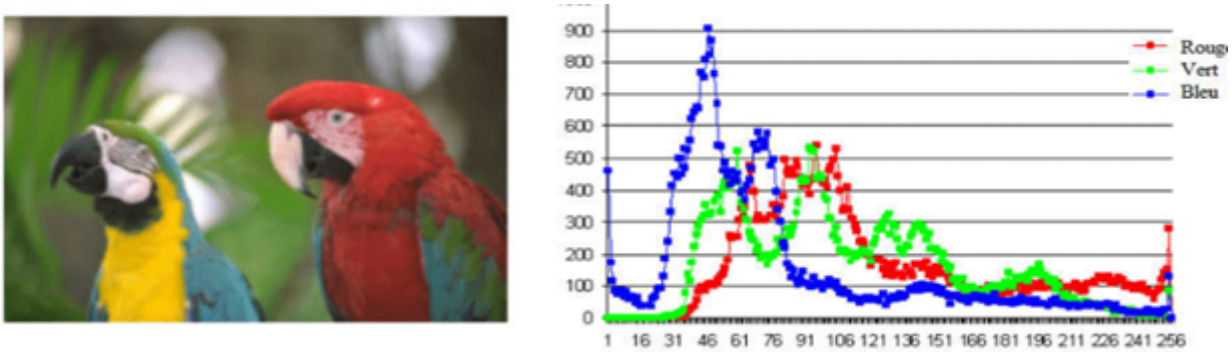

Figure 2.8: Histogramme d'une image Couleur.

Dans un contexte de chiffrement d'image, l'histogramme de l'image chiffrée doit être uniforme pour assurer la sécurité contre l'attaque , autrement dit l'attaquant ne peut pas extraire information à partir de cet histogramme. Par exemple, La Figure 2.9 est l'histogramme de l'image originale et la Figure 2.10 est l'histogramme de l'image cryptée. La Figure 2.9 montre que l'histogramme plus uniforme qui est hautement souhaitable [4]
.

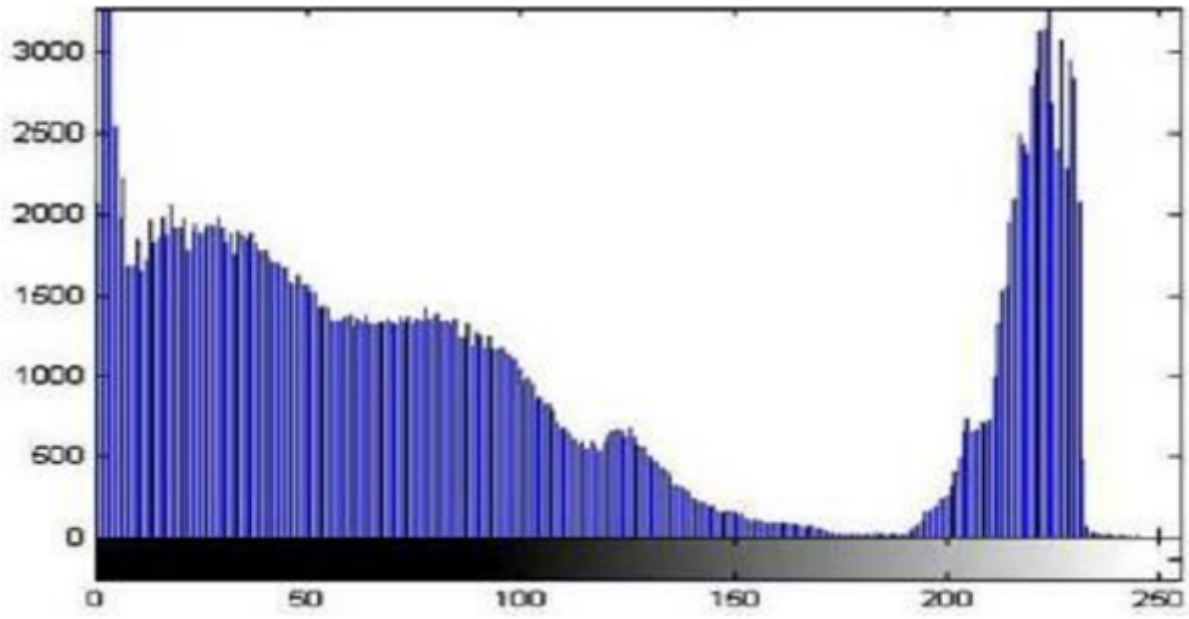

Figure 2.9: Histogramme D'une Image Original.

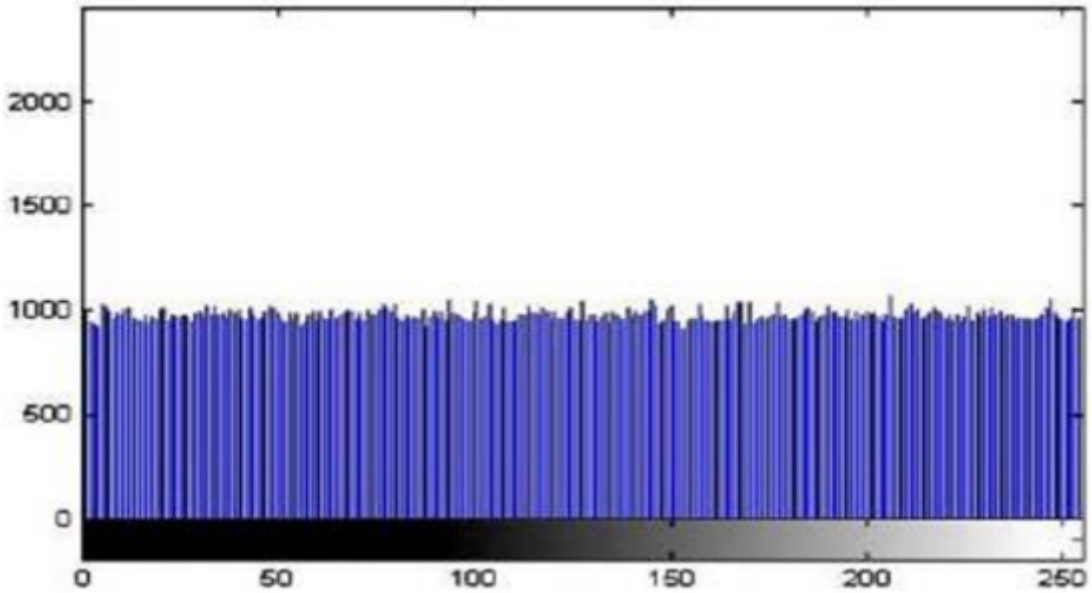

Figure 2.10: Histogramme D'une Image Cryptée.

2.4.3 La Corrélation Entre Les Pixels Adjacents

La corrélation est une technique qui permet de comparer deux images pour estimer les déplacements des pixels d'une image par rapport à une autre image de référence Les pixels adjacents d'une image standard ont une forte corrélation. Un bon schéma de cryptage d'image doit supprimer une telle corrélation afin d'assurer la sécurité contre l'analyse

statistique.

$$r = \frac{\mathrm{cov(x, y)}}{\sqrt{\mathrm{D(x)}\sqrt{\mathrm{D(y)}}}} \tag{2.1}$$

et

$$\mathrm{cov(x, i)} = \frac{1}{\mathrm{N}} \sum_{\mathrm{i}=1}^{\mathrm{N}} \left((\mathrm{x_i} - \mathrm{E(x)})\right) \left(\mathrm{y_j} - \mathrm{E(y)}\right) \tag{2.2}$$

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_\mathrm{i}, D(x) = \sum_{i=1}^{N} (\mathrm{xi} - \mathrm{E(x)})^2 \tag{2.3}$$

Si corrélation $\approx$ 1 , cela signifie que l'Image - clair et de Image - Chiffrée sont très dépendantes Si corrélation $\approx \pm 0$, cela signifie que le Image - Chiffrée et l'image - clair ne sont pas corrélés .
Ainsi , plus faible est la valeur de corrélation , la qualité de cryptage est meilleure [4].

2.4.4 L'entropie

L'entropie de Shannon , est une fonction mathématique qui permit de mesures de l'aléatoire de l'information Pour tout message codé sur M bits , la limite supérieure de l'entropie est M. La formule :

$$H(M) = -\sum_{i=1}^{n} p_\mathrm{i} x \log_2 p_\mathrm{i} \tag{2.4}$$

Où pi définit la probabilité d'un pixel et N est le nombre de bits dans chaque pixel . Donc pour un chiffrement d'images au niveau de gris , La valeur de l'entropie doit être très proche de 8 Parce que si l'entropie est inférieure à 8 , il existe des degrés prévisibilité , donc on ne peut pas assurer la sécurité contre l'analyse statistique . De sorte que entropie devrait idéalement être 8 [4] .

Conclusion

ans ce chapitre, nous avons essayé de donner un bref aperçu des concepts de base du dossier médical et de ses caractéristiques et composantes. Nous décrivons brièvement les définitions, les types d'images et le codage couleur, puis décrivons les outils de base pour analyser l'algorithme de codage d'image tels que l'espace clé et l'histogramme, la relation entre les pixels adjacents, et le dernier est l'entropie. Dans le chapitre suivant, nous expliquerons la méthode que nous avons développée pour chiffrer le dossier médical.

Chapitre 3

Méthode Proposée

Introduction

En ce chapitre concerne la proposition en générale, en utilise l'encryption homomorphe sur les dossiers médicaux tel que les dossiers médicaux sont constitués d'images et de fichiers texte.
La proposition est basée sur l'application de l'algorithme de cryptage à la fois à une image et à un fichier et sur leur fusion en une seule image cryptée pour augmenter l'efficacité du chiffrement et du déchiffrement.
Le schéma de chiffrement homomorphe générale montre dans la figure 3.1 ci-dessous.

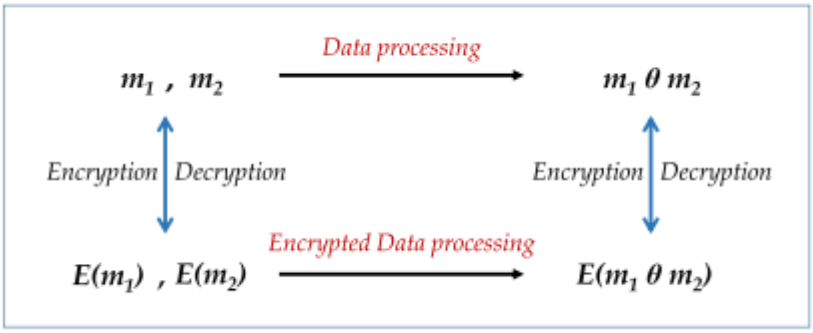

Figure 3.1: Un schéma de chiffrement homomorphe

Les schémas de chiffrement homomorphe partiellement n'incluent qu'un seul type d'opération, comme l'addition ou la multiplication ; Dans notre proposition, nous nous appuierons sur l'addition un nombre illimité de fois. Cependant, les schémas de chiffrement sont quelque peu homomorphe.
Prend en charge les opérations d'addition et de multiplication et effectue plusieurs fois. Une variété d'opérations homogènes avec des fonctions aléatoires, qui est l'idée la plus fondamentale de la similarité de chiffrement [16].

3.1 Schéma globale

Voici la figure 3.2 ci-dessous qui illustre de manière simplifiée le principe de la proposition.

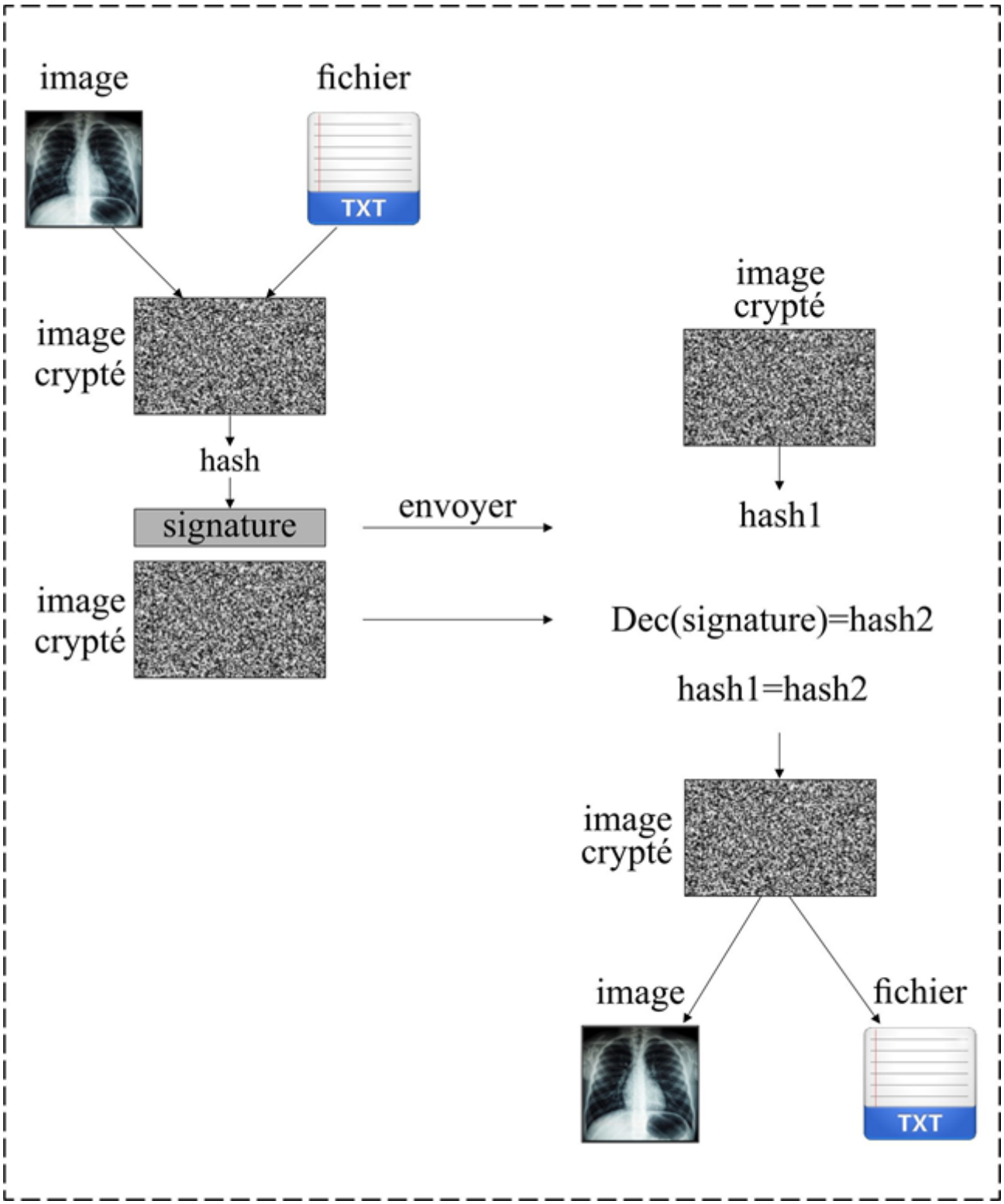

Figure 3.2: Clarifier le principe de la proposition.

L'image illustre de manière simplifiée le principe de la proposition, où l'image originale

et le fichier original sont combinés en appliquant un algorithme de cryptage pour obtenir une image fusionnée cryptée qui est envoyée par l'expéditeur.
Lorsque vous obtenez l'image cryptée, le hachage est extrait pour celui-ci, puis une signature numérique est créée à l'aide d'un algorithme RSA et envoyez ensuite l'image cryptée et la signature numérique avec elle au destinataire.

3.2 Processus de signature numérique

Explication détaillée du processus de signature numérique est présentée dans la figure 3.3 ci-dessous

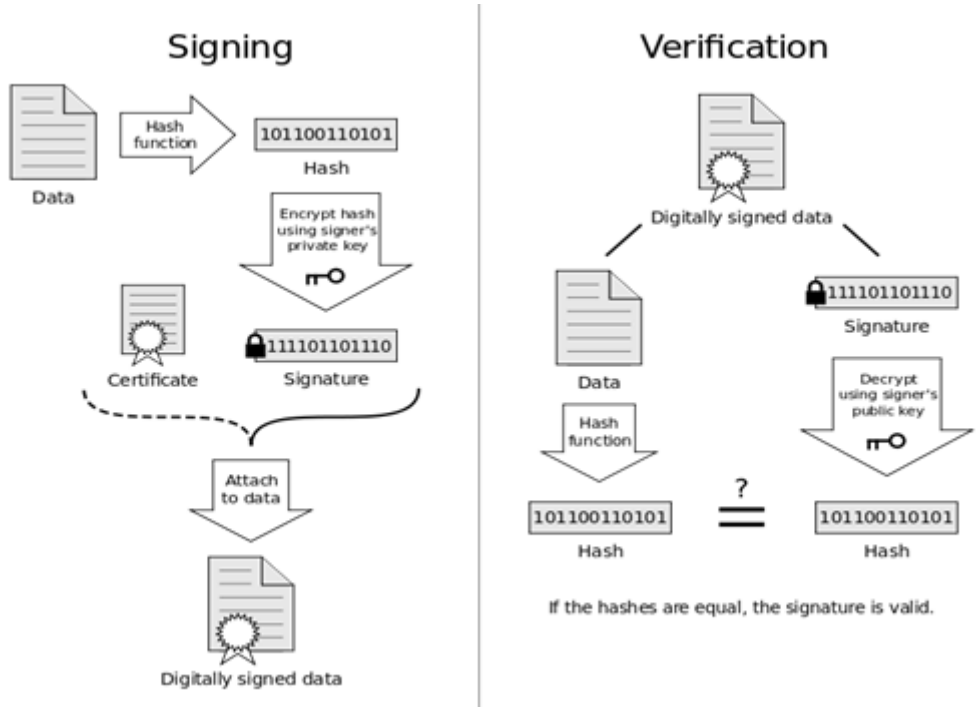

Figure 3.3: Image de processus de signature numérique.

Pour RSA, il n'y a pas de différence mathématique entre une clé privée et une clé publique, il est possible d'utiliser la clé privée pour le chiffrement et la clé publique pour le déchiffrement, contrairement au chiffrement asymétrique. Ainsi, seul le propriétaire de la clé privée peut chiffrer un message pour obtenir ce qui aura le rôle de la signature et chacun peut essayer de déchiffrer la signature pour voir si le résultat obtenu correspond au message initial.
Voici le scénario suivant qui explique en détail ce processus:

- Alice choisit une fonction de hachage que nous noterons H;
- Pour le chiffrement choisi, Alice a généré une clé privée Kpr et une clé publique Kpb;

- Elle transmet la clé publique Kpb et la fonction de hachage H à Bob par un canal éventuellement non sécurisé (H et Kpb n'ont pas besoin d'être secrets) ;
- Elle garde la clé privée Kpr secrète.

3.3 Réception du message signé

Bob réceptionne le message signé. Pour vérifier l'authenticité du message:

- il produit un condensat du texte clair en utilisant la fonction de hachage d'Alice : H(M) ;
- il déchiffre la signature en utilisant la fonction de déchiffrement RSA D avec la clé publique Kpb (là encore l'utilisation est volontairement impropre)
- soit : DSm=D(Kpb,SM) ;
- il compare DSm avec H(M).

Dans le cas où la signature est authentique, DSm et H(M) sont égaux car, de par les propriétés du chiffrement symétrique :

$$\mathbf{D}_{\mathrm{Sm}} = \mathbf{D}\left(\mathrm{K}_{\mathrm{pb}}, \mathbf{S}_{\mathbf{M}}\right) = \mathbf{D}\left(\mathrm{K}_{\mathrm{pb}}, \mathbf{C}\left(\mathrm{K}_{\mathrm{pr}}, \mathbf{H}(\mathbf{M})\right)\right) = \mathbf{H}(\mathbf{M}) \tag{3.1}$$

Le message est alors authentifié.

3.4 Le Processus d'extraction des valeurs de l'image et du fichier

une explication détaillée du processus d'extraction des valeurs de l'image et du fichier, comme indiqué dans la figure 3.4 ci-dessous.

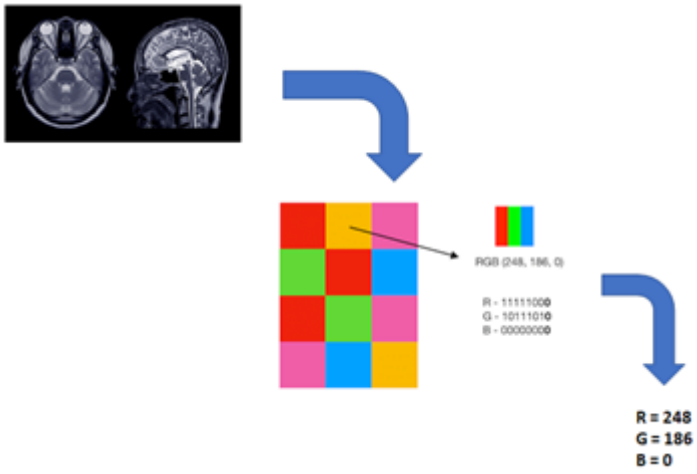

Figure 3.4: Extraire chaque pixel de l'image et prendre les Valeur de Le R.G.B

Pour l'image, nous prenons chaque pixel et extrayons les valeurs de couleur R,G et B tel que leur plus grande valeur soit 256.
Convertir un fichier texte en valeurs binaires comme montre dans la figure 3.5 ci-dessous.

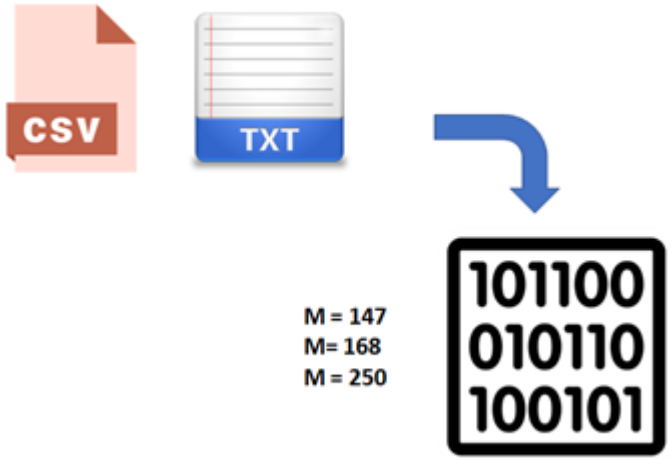

Figure 3.5: Convertir Un fichier Texte en Valeurs binaires.

Concernant le fichier texte, il est converti en valeurs binaires et nous prenons tous les 8 bits et les représentons avec une valeur M telle que sa plus grande valeur puisse être 256 , qui sera combinée avec d'autres valeurs de l'image consistant en R,G,B.

3.5 Générer les clés de chiffrement et déchiffrement

Algorithme 01 Générer les clés initialise:

$\max M1 = 256$
$\max M2 = 256$
$\max M3 = 256$
$\max M4 = 256$
$rk = random(> MaxM)$
$kl = random(> rk)$
$k2 = \max M1^{*}k1 + rk$
$k3 = max\_M2 * k2 + rk$
$\min = \max M1 * k1 + \max M2 * k2 + \max M3 * k3 + \max M4 + 1$
$\max = (\max M1^{*}k1 + \max M2 * k2 + \max M3 * k3 + \max M4) * 1000$
$p =$ svmpy.randprime (min, max)
$q =$ sympy.randprime (min, mak)
$n = p * q$
$r =$ random()
$kbl = kl + r^{*}p$
$kb2 = k2 + r^{*}p$

$kb3 = k3 + r^*p$

Algorithme de génération de clés privées et publiques tel que pour que les valeurs des pixels et les caractères de fichier texte soient il peut prendre la plus grande valeur et est 256.
Nous notons également que le générateur dépend des valeurs aléatoires ou pseudo-aléatoires dans la génération des valeurs afin que les valeurs soient fortes.

Nous avons 3 clés privées k1, k2 et k3 qui sont déchiffrées et gardées secrètes par le générateur de clés, c'est-à-dire qu'elles ne sont pas distribuées et 3 clés publiques kb1, kb2 et kb3 avec lesquelles le cryptage est effectué et distribué au public jusqu'à ce que le processus de cryptage soit terminé.

3.6 Les processus de chiffrement et de déchiffrement

Dans cette partie nous expliquons les étapes en détaille les processus de chiffrement et de déchiffrement

3.7 Algorithme de chiffrement

def crypt pixel(R,G,B,M):

$$C = ((R^*kb1) + (G^*kb2) + (B^*kb3) + M)\,\%n \tag{3.2}$$

Après avoir calculé le processus de cryptage, nous obtenons la valeur C est divisée en trois parties C1,C2 et C3 et chaque valeur représente une série R,G et B afin d'obtenir le pixel approprié pour l'image cryptée.
Une infographie montrant le processus de chiffrement d'un seul pixel dans la figure 3.6 ci-dessous.

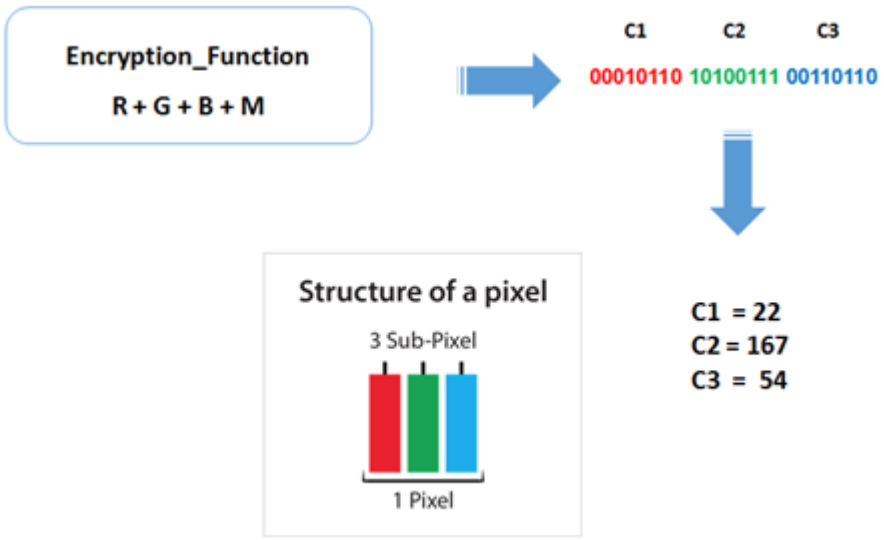

Figure 3.6: Processus de cryptage à un seul pixel

3.8 Algorithme de déchiffrement

def decrypt pixel(C):

$$D = (((C\%p)\%(k3-1))\%(k2-1))\%(kl-1)$$
$$M4 = (((C\%p)\%k3)\%k2)\%kl$$
$$M1 = ((((C-M4)\%p)\%k3)\%k2)\%(kl-1)$$
$$M2 = ((((C-M4-M1*k1)\%p)\%k3)\%(k2-1))$$
$$M3 = D-(M1+M2+M4)$$
return $M1, M2, M3, M4$

Les clés privées k1,k2 et k3 sont utilisées pour extraire des valeurs R,G,B et M Ici, après application de l'algorithme, on obtient les valeurs de R,G et B des images et M du fichier texte.
Une illustration du processus de déchiffrement. Une explication du processus de décodage est présentée dans le Figure 40 ci-dessous.

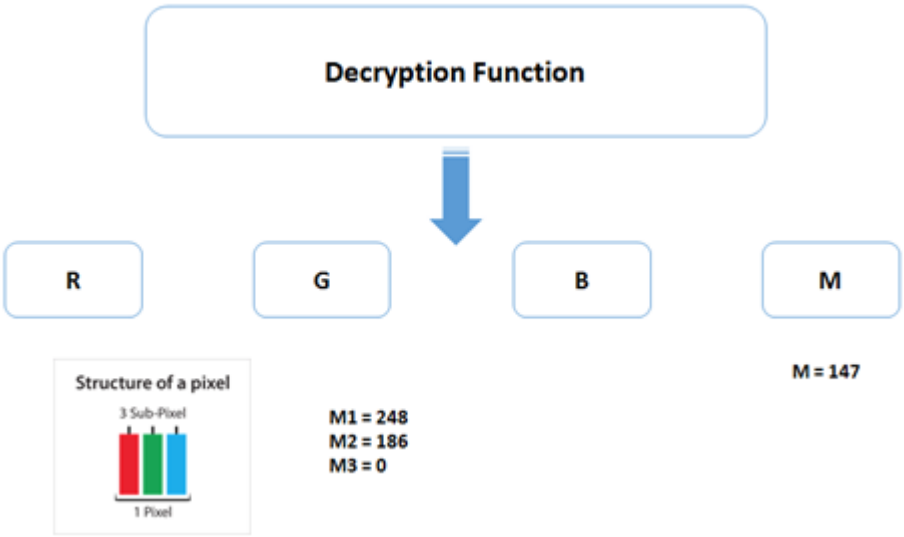

Figure 3.7: Processus de déchiffrement

Conclusion

ans ce chapitre, nous avons présenté notre proposition pour objectif chiffrement et déchiffrement des dossiers médicales. Nous avons utilisé méthode homomorphe qui compose par une fragmentation et addition des données et des clés. Dans le chapitre suivant, nous discuterons de l'application et de l'implémentation de cet algorithme et afficher ses résultats.

Chapitre 4

Implémentation Et Analyses

Introduction

Après avoir expliqué dans le chapitre précédent l'algorithme proposé pour le cryptage et le décryptage des dossiers médicales en détail, nous commençons maintenant dans ce dernier chapitre la partie de la réalisation de l'algorithme dans une application pratique puis analysons les résultats obtenus pour vérifier la solidité et la sécurité de l'algorithme, nous présentons notre application vérifiée et les différents standards à travers un ensemble de critères que nous évoquerons successivement.

4.1 Environnement de développement

Dans cette partie nous allons citer l'environnement logiciel (Software) et matériel(Hardware) utilisés.

4.1.1 Environnement logiciel

Nous utilisions l'environnement Python pour exécuter des fichiers notre approche. • Python Python est un langage de programmation interprété et multiplateforme. Il encourage la programmation déterministe structurée, fonctionnelle et orientée objet. Caractéristiques écriture dynamique puissante, gestion automatique de la mémoire par ramasse-miettes et système de gestion des exceptions. Nous avons utilisé Python dans notre projet de traitement et de codage d'images car il Riche en bibliothèques prêtes à l'emploi qui facilitent le processus de programmation de nous concentrons d'avantage sur l'idée du projet. Voici quelques bibliothèques de traitement d'image pratique et librement disponible en Python, nous l'avons utilisé dans un fichier projet : Numpy, SciPy, Matplotlib, PIL/Pillow, OpenCV, Scipy.

4.1.2 Environnement matériel

L'application a été développée sur un PC(Desktop HP modèle : HP Pavilion Desktop Computer) ayant les caractéristiques suivantes :

- Processeur Intel Core i7-7700 CPU@ 2.30GHz 2.29 GHz.
- Mémoire installée (RAM) : 16,00 Go.
- Disque Dure : HDD 1TB et 256GB SSD.
- Carte graphique : Intel HD Graphics 630.
- Système d'exploitation : Windows 10 Professionnel 64 bit.

Nous avons travaillé sur une gamme de différents dossiers médicaux tels que:

- Les données sont un petit sous-ensemble d'images provenant des archives d'imagerie du cancer. Ils consistent en la tranche médiane de toutes les images CT prises où l'âge, la modalité et les étiquettes de contraste valides ont pu être trouvés. Il en résulte 475 séries de 6 9 patients différents. [19]
- L'ensemble de données se compose de 15264 (512x512) images radiographiques thoraciques pour le train et de 400 images pour l'ensemble de test. L'ensemble de données contient des classes positives et négatives pour indiquer les cas positifs et négatifs de COVID-19. [8]

4.2 L'interface principale de l'application

L'interface principale de l'application, qui comprend de nombreuses opérations nécessaires, qui comprend le cryptage, le décryptage et la signature d'images envoyées pour protéger son contenu de toute altération et un ensemble d'analyses pour les résultats.

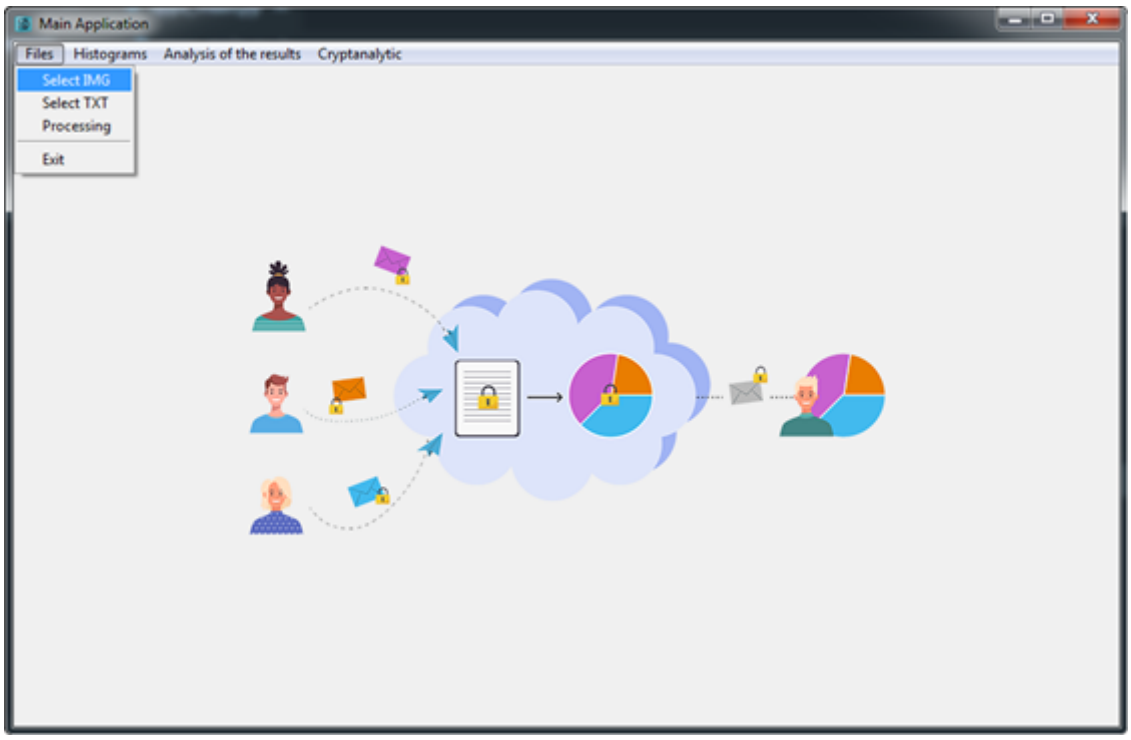

Figure 4.1: L'interface principale de l'application.

4.3 Critères d'évaluation

Un bon système de cryptage doit résister à tous les types d'attaques connus, il existe donc des simulations numériques réalisées à l'aide de différentes échelles de notation démontrer la sécurité et l'efficacité de l'algorithme proposé. Nous présenterons les plus importants tels que : Mesure de distorsion (PSNR), Mesure de similarité structurelle (SSIM), histogramme, entropie, nombre de taux de pixels changeants (NPCR), corrélation entre pixels adjacent.

4.3.1 Le nombre de taux de pixels changeants (NPCR) et le l'intensité modifiée moyenne unifiée (UACI):

Le nombre de taux de pixels changeants (NPCR) et le l'intensité modifiée moyenne unifiée (UACI) sont les deux plus courantes quantités utilisées pour évaluer la force du cryptage des images algorithmes/chiffres par rapport aux attaques différentielles. Classiquement, un score NPCR/UACI élevé est généralement interprété comme une haute résistance aux attaques différentielles. Cependant, il n'est pas clair quelle est la hauteur du NPCR/UACI pour que le chiffrement d'image ait en effet un haut niveau de sécurité. Dans cette partie , nous abordons ce problème en établir un modèle mathématique pour des images idéalement cryptées puis dériver les attentes et les variances du NPCR et de l'UACI sous ce modèle. De plus, ces valeurs théoriques sont utilisées pour forment des hypothèses statistiques NPCR et UACI tests. Valeurs critiques des tests sont par conséquent dérivés

et calculés à la fois symboliquement et numériquement. Par conséquent, la question de savoir si une donnée Le score NPCR/UACI est suffisamment élevé pour ne pas être discernable à partir d'images idéalement cryptées est répondu par comparant les scores NPCR/UACI réels avec les scores critiques correspondants valeurs. Résultats expérimentaux utilisant le NPCR et l'UACI les tests aléatoires montrent que de nombreux cryptages d'images existants les méthodes ne sont en fait pas aussi bonnes qu'elles le prétendent, bien que certaines méthodes réussissent ces tests de caractère aléatoire. La représentation mathématique des tests NPCR et UACI est présentée comme suit:

$$\begin{aligned} NPCR &= \frac{\sum C(i,j)}{N \times M} \\ UACI &= \sum \frac{|C_1(i,j) - C_2(i,j)|}{255 \times N \times M} \end{aligned} \tag{4.1}$$

Où C1 et C2 sont les images de chiffrement produites à partir de deux images qui diffèrent juste d'un pixel avec un peu. La taille de C est N * M, et C est définie par l'équation suivante :

$$C(l,m) = \begin{cases} 1, \text{ if } C_1(i,j) = C_2(i,j) \\ 0, \text{ otherwise} \end{cases} \tag{4.2}$$

Pour le chiffrement par blocs qui est un chiffrement déterministe qui préserve la longueur, la notion de sécurité sémantique a récemment été étudiée en bourrant des bits de bruit dans l'image simple, cela produira une image chiffrée aléatoire. Dans notre travail, nous considérons la notion d'indiscernable pour le chiffrement par blocs. Notez que le déchiffrement d'une image chiffrée conduit à une image originale sans perte, grâce au déterminisme des chiffrements par blocs. La perte ne concernera que les bits affectés au cours du processus randomisé. les résultats expérimentaux avec différentes images colorées avec le test ci-dessus. Ces tests sont effectués 100 fois pour chaque échantillon d'image. Comme le montre , les valeurs de NPCR et UACI de notre méthode sont dépassant l'idéal qui est de 99,60 % pour NPCR et 33,46% pour UACI.

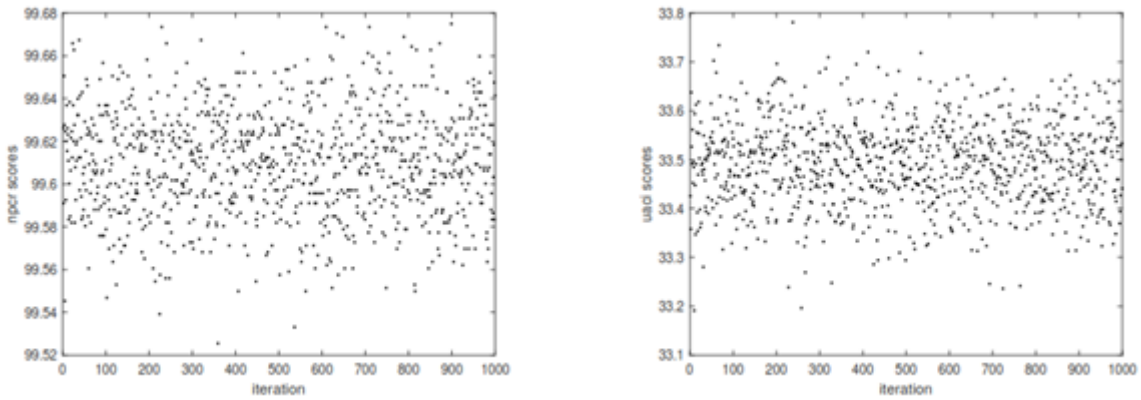

Figure 4.2: Distribution de sensibilités d'image

En effet, le score de NPCR est de l'ordre de 99,61%, et le score de L'UACI est d'environ 33,47 % pour notre algorithme de chiffrement d'image proposé. Les résultats de ces tests indiquent la grande sensibilité au changement d'image simple même avec de minuscules le changement peut changer complètement l'image chiffrée correspondante. Par conséquent, l'algorithme proposé peut fournir une haute sécurité contre les attaques différentielles.
Une illustration montrant les étapes de chiffrement et de déchiffrement et le processus de fusion d'une image et d'un fichier texte, et le résultat est une image cryptée.
La figure 4.3 ci-dessous montre le processus de fusion d'une image et d'un fichier texte.

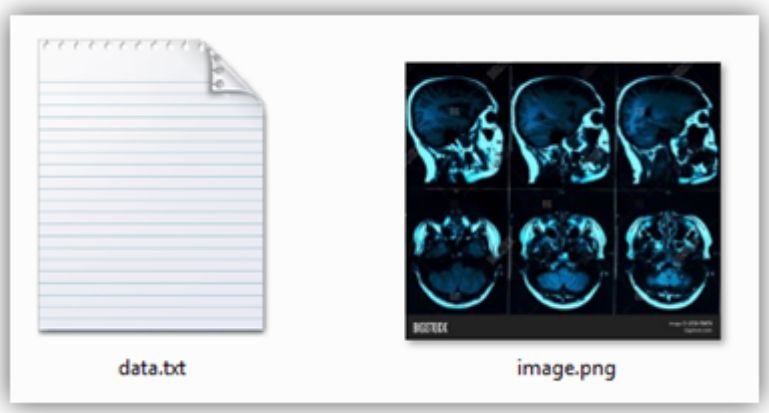

Figure 4.3: Dossier Médical Original.

La figure 4.4 suivante montre le résultat de la fusion, qui a été encodé

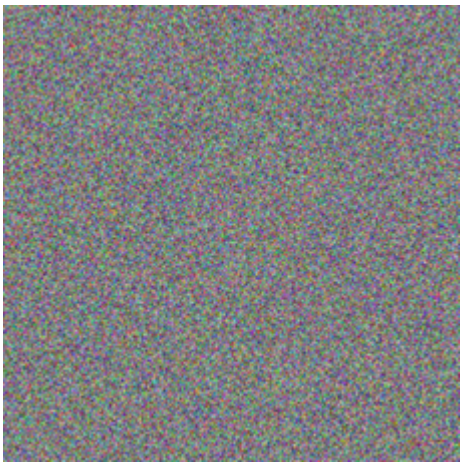

Figure 4.4: Image cryptée.

Le processus inverse de décodage de l'image pour obenir le fichier de données et de décodage de l'image est illustré dans la **La figure 4.5**

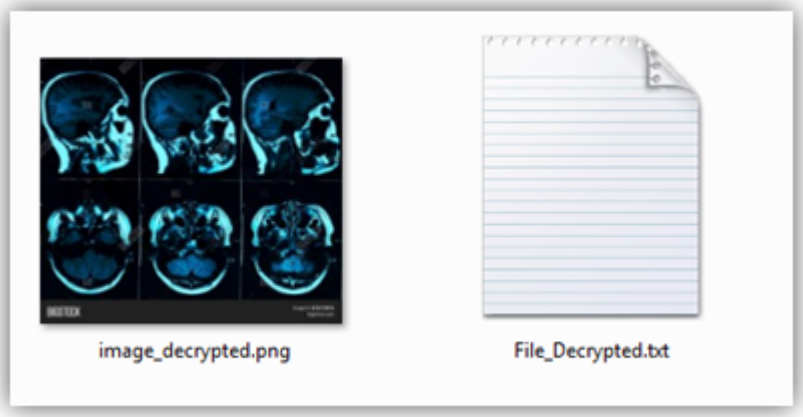

Figure 4.5: Dossier Médical décrypté.

Le processus inverse de déchiffrement de l'image crypter pour obtenir fichier de données et image décrypter.

4.3.2 L'histogramme

L'histogramme d'une image fait référence à un graphique du pixel valeurs d'intensité. L'histogramme est un graphique montrant le nombre de pixels dans une image à différentes valeurs d'intensité trouvé dans l'image [2].
Cette image claire illustrée à la figure 4.6 ci-dessous

Figure 4.6: Image Original.

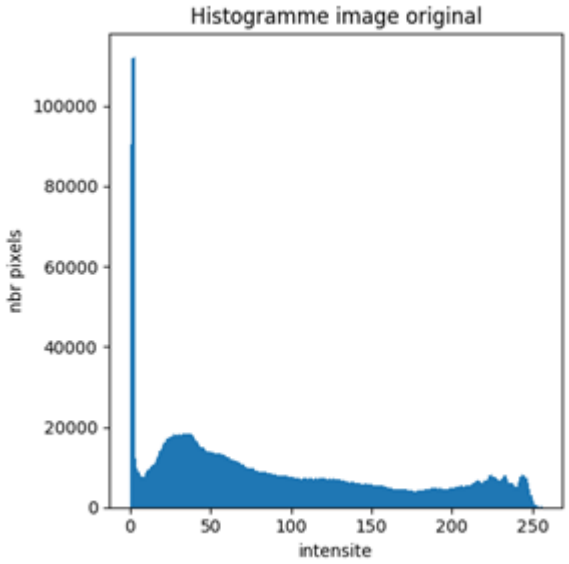

Figure 4.7: histogramme d'une image Original.

Cette image crypté illustrée à la figure 4.8 ci-dessous

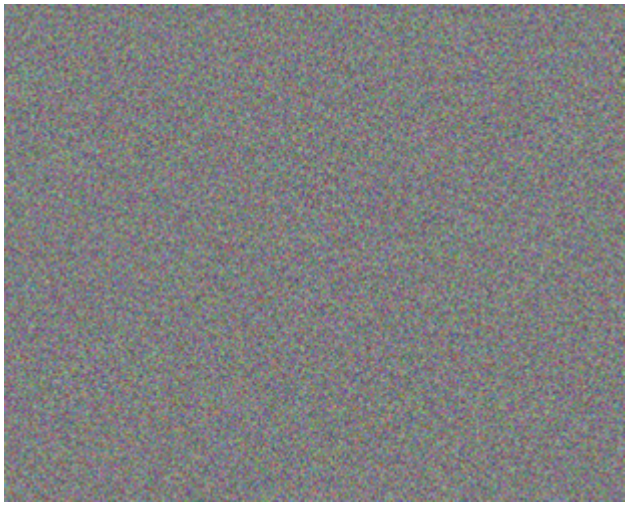

Figure 4.8: Image cryptée.

comparaison entre l'histogramme de l'image original et l'histogramme de l'image crypté

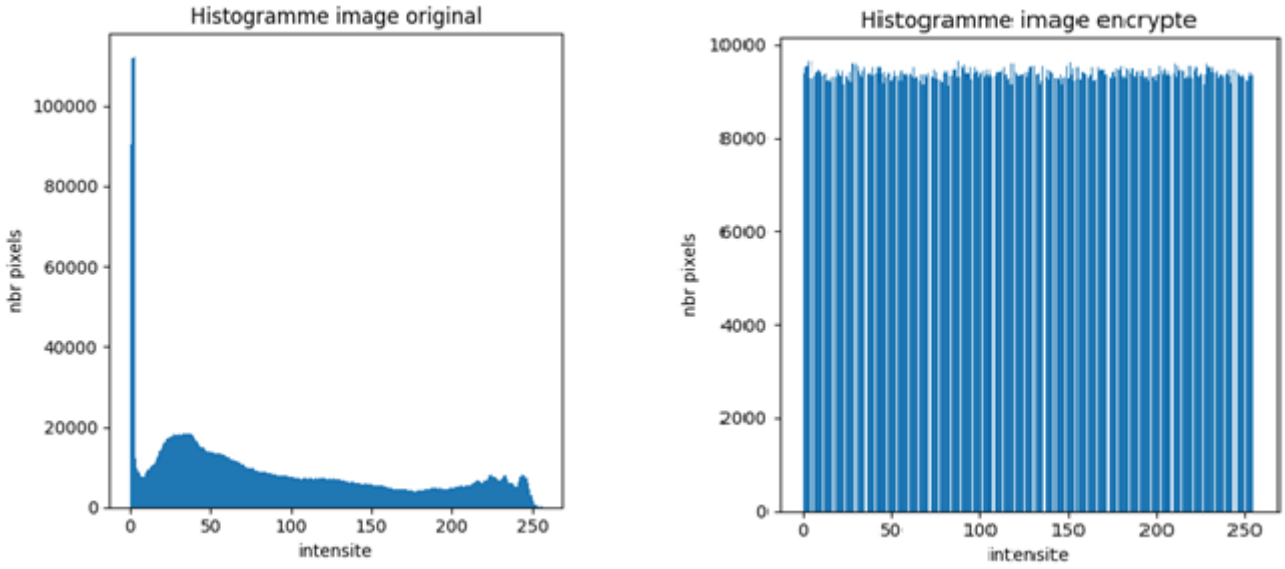

Figure 4.9: Comparaison D'histogrammes.

Cette image claire illustrée à la figure 4.10 ci-dessous

Figure 4.10: Image Original.

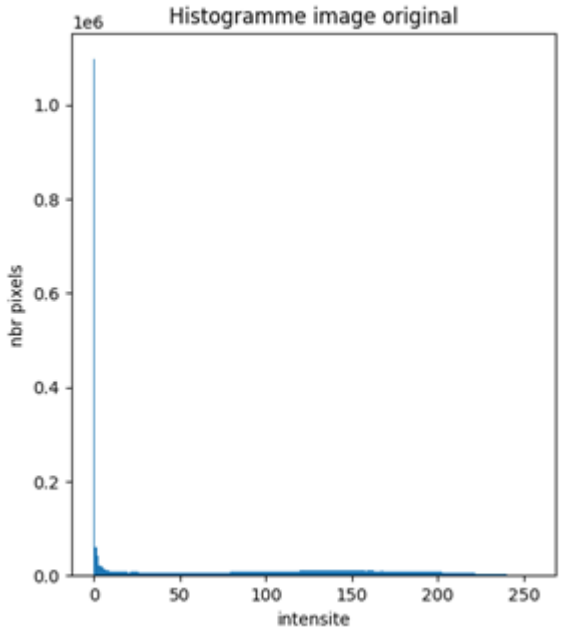

Figure 4.11: L'histogramme d'une image original.

Cette image crypté illustrée à la figure 4.12 ci-dessous

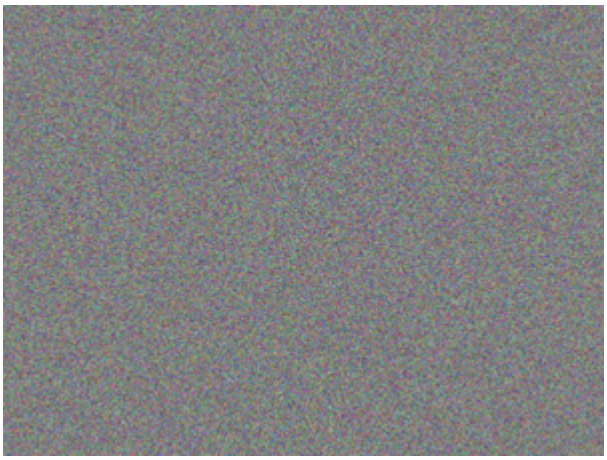

Figure 4.12: Image cryptée.

comparaison entre l'histogramme de l'image original et l'histogramme de l'image crypté

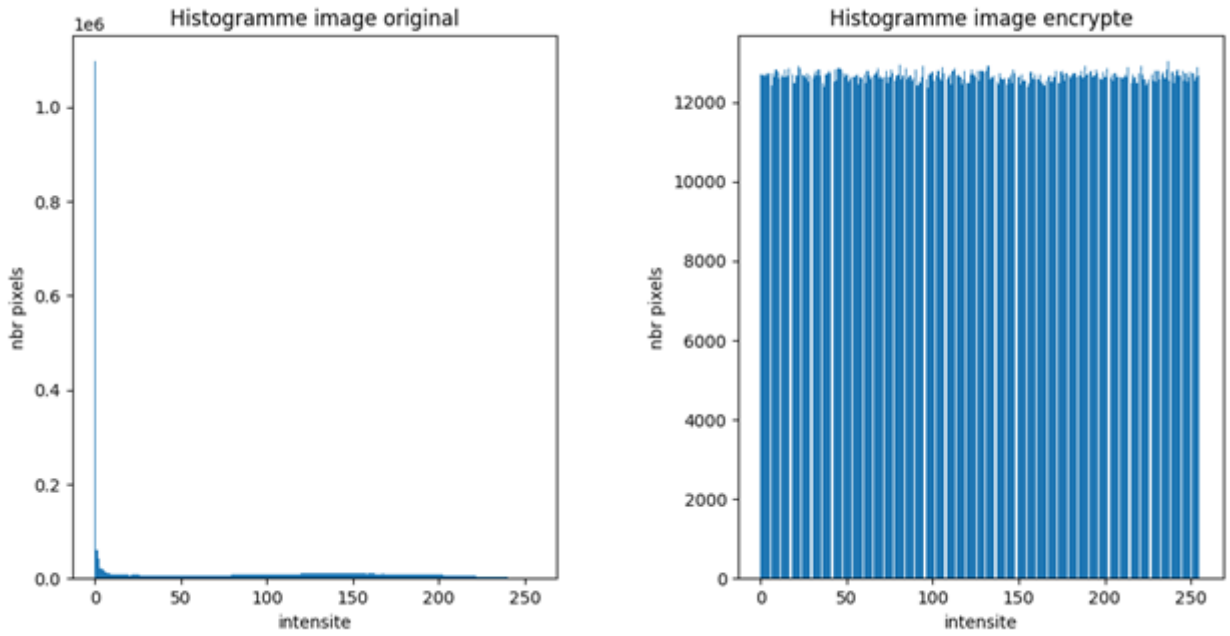

Figure 4.13: Comparaison Des histogrammes.

Le résultat montre que les histogrammes des images cryptées sont uniformes après cryptage. L'attaquant ne peut donc pas extraire d'informations de l'histogramme de l'image cryptée. Aussi il n'y a aucune relation ou similitude entre les histogrammes des images cryptées et les histogrammes des images claires, ni en couleur ni en intensité. Nous ne pouvons donc pas prédire l'image réelle ou son histogramme à partir de l'histogramme de l'image cryptée.

4.3.3 Mesure de distorsion PSNR (Signale de Peak Signal to Noise Ratio)

est une mesure de distorsion utilisée en image numérique, tout particulièrement en compression d'image. Elle permet de quantifier la performance des codeurs en mesurant la qualité de reconstruction de l'image compressée par rapport à l'image originale. Le PSNR est défini par la formule suivante:

$$PSNR = 10 \cdot \log_{10} \left(\frac{d^2}{EQM} \right) \tag{4.3}$$

où d est la dynamique du signal (la valeur maximum possible pour un pixel), dans le cas standard d'une image codée sur 8-bits, d=255.
EQM est l'erreur quadratique moyenne, elle est définie pour 2 images Io et Ir de taille

m×n par la formule suivante:

$$EQM = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left(I_o(i,j) - I_r(i,j) \right)^2 \tag{4.4}$$

La figure 4.14 montre mesure de distorsion

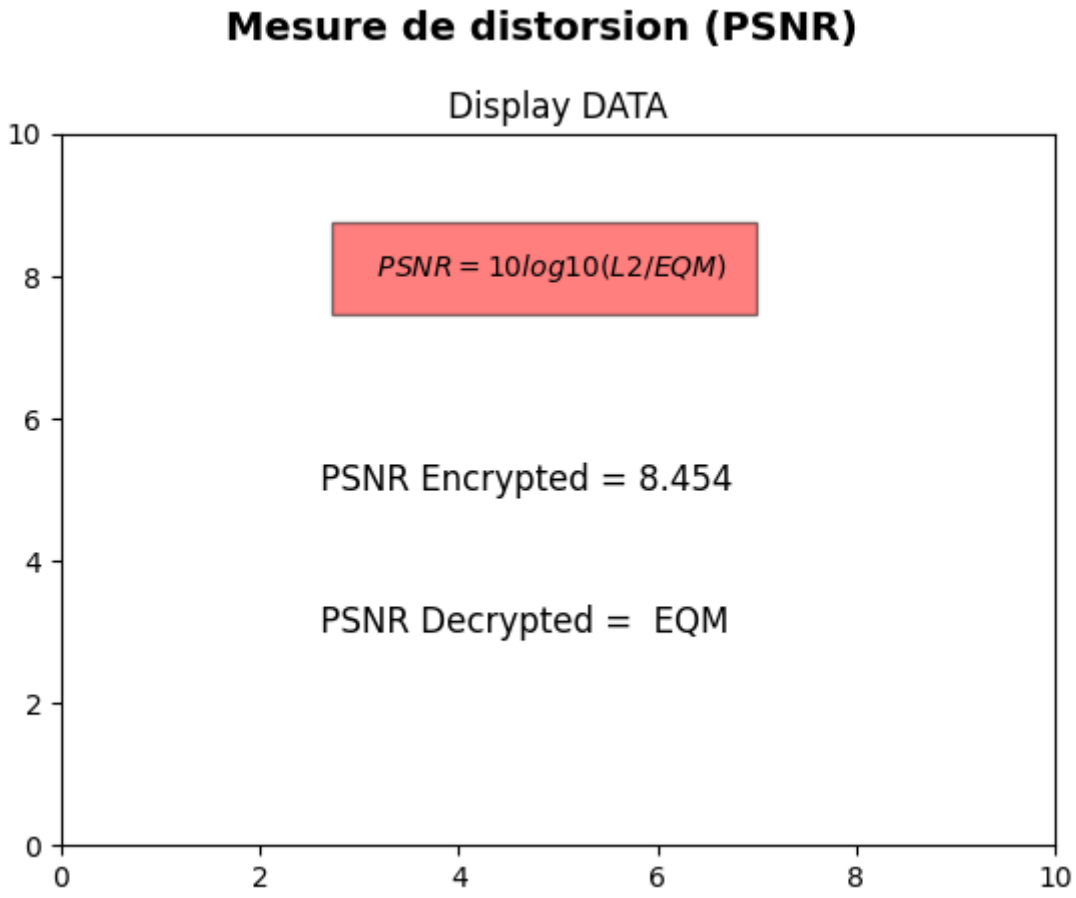

Figure 4.14: Mesure De Distorsion (PSNR).

Le résultat de notre application indique que le taux de distorsion est complet entre l'image d'origine et l'image cryptée. En ce qui concerne l'image originale et l'image décrypté le résultat est les deux images sont identiques, et donc l'erreur quadratique moyenne est égale à zéro.

4.3.4 mesure similarité structurelle (SSIM)

SSIM est une mesure de similarité entre deux images numériques. Elle a été développée pour mesurer la qualité visuelle d'une image compressée, par rapport à l'image originale. L'idée de SSIM est de mesurer la similarité de structure entre les deux images, plutôt qu'une différence pixel à pixel comme le fait par exemple le PSNR. L'hypothèse sous-jacente est que l'œil humain est plus sensible aux changements dans la structure

de l'image. La métrique SSIM est calculée sur plusieurs fenêtres d'une image. La mesure entre deux fenêtres x et y de taille NxN est :[31]

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)} \tag{4.5}$$

le SSIM (Structural Similarité Index) est un modèle basé sur la perception qui considère la dégradation de l'image comme un changement perçu dans les informations structurelles, tout en intégrant également des phénomènes perceptifs importants, y compris des termes de masquage de luminance et de masquage de contraste et contours.
La figure 4.15 ci-dessous montre similarité structurelle (SSIM)

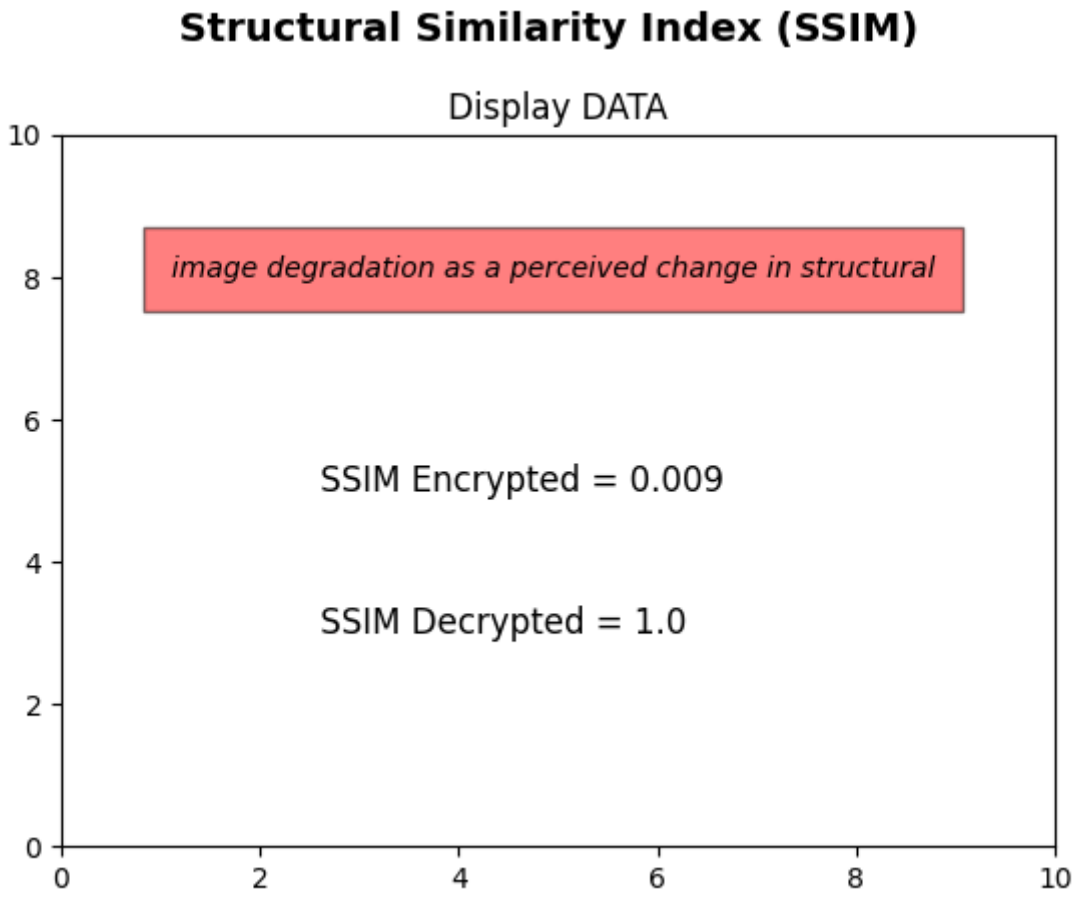

Figure 4.15: Structural Similarity Index (SSIM).

Le résultat dans l'application montre la valeur SSIM d'une image originale et la même image est cryptée: 0.009 cela signifié que les 3 paramètres : Luminance, Contraste et Contours Ils sont totalement différent. Quant à l'image originale et la même image après décryptage était la valeur: 1.0 de tout ce qui le résultat est les deux images sont identiques à travers Luminance, Contraste et Contours.

4.3.5 Entropie

L'entropie est une mesure statistique du hasard dans la théorie de l'information [29]. La performance d'un système de cryptage est mesurée en obtenant une valeur de l'entropie proche de la valeur 8.
La valeur entropie de différentes images selon notre système est décrite dans la figure 4.16 suivante:

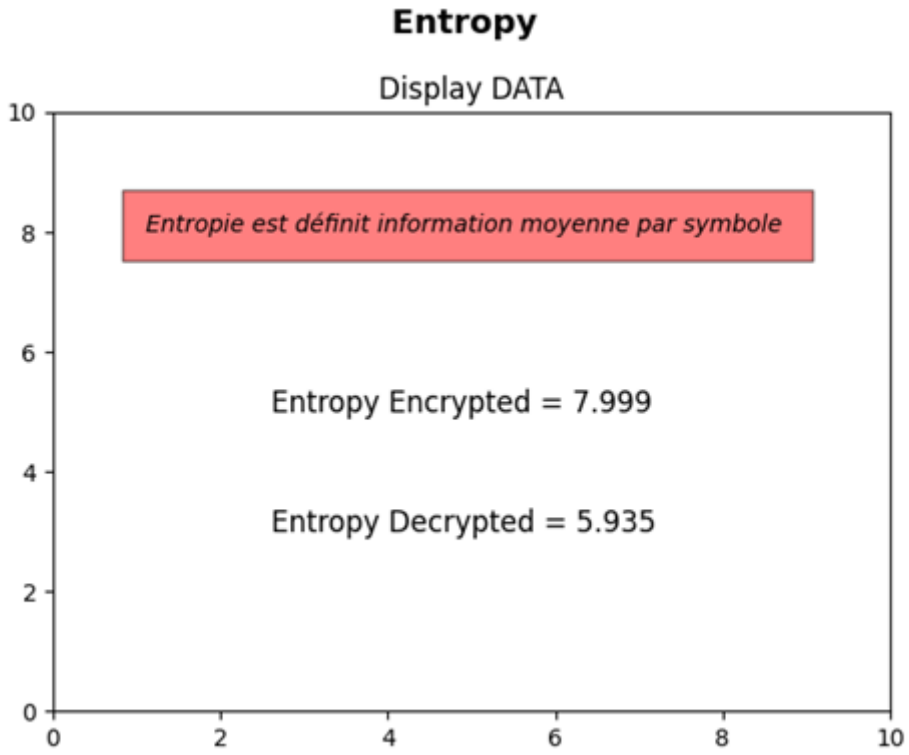

Figure 4.16: Entropy .

Le résultat montre qu'après de simuler ensemble d'images, la valeur d'entropie moyenne des images cryptées est de 7.99725, c'est-à-dire qu'elle est plus proche de la valeur 8. Cela montre qu'il est difficile, ou dire qu'il est impossible d'avoir une prévisibilité.

4.4 Discussion

On remarque que la taille des images et qu'elles sont cryptées est grande par rapport aux images originales, en effet, toutes les valeurs de pixel sont remplies comme décrit précédemment dans l'histogramme, très logique car l'image original est combinée avec le fichier texte afin d'obtenir l'image cryptée. Quant aux images après le décryptage et aux images originales la taille est presque égale.

Conclusion

ous avons présenté dans ce chapitre notre application réalisée, et les différents outils utilisés dans son développement. Nous avons également terminé par un ensemble d'analyses et des tests pour les résultats expérimentaux qui montrent la résistance de notre algorithme de chiffrement. Selon l'analyse de notre méthode, dispose d'une sécurité de haut niveau contre les différents types d'attaques. Ainsi, l'analyse prouve la sécurité et l'efficacité.

Conclusion Générale

Avec les grands progrès en informatique, les dossiers médicaux numériques sont généralement transférés et stockés en format électronique. Au fil du temps, la confidentialité du dossier médical est devenue indispensable.
Dans ce mémoire, nous avons conçu un système de cryptage efficace pour assurer la sécurité de ce type de données. Une méthode de fragmentation aléatoire a été proposé pour assurer un chiffrement asymétrique , ainsi que l'algorithme RSA pour créer la signature numérique de l'image.
Pour analyser la méthode proposée , nous avons effectué un ensemble de tests sur, l'histogramme , l'entropie , entre les pixels adjacents et mesure de distorsion ... etc. Les analyses montrent la méthode proposée a une bonne robustesse et les résultats expérimentaux montrent aussi l'efficacité de cette technique et dans la future on peut améliorer notre approche en prenant en compte le facteur de la rapidité de chiffrement tout en conservant d'un niveau des performances.
Comme perspective de ce travail, nous aimerions continuer à utiliser de nouvelles idées telles que l'application de cet algorithme dans la vie réelle

Bibliographie

Bibliography

[1] "Patient file-erp-linkitt hospital-management-program-accounts" – Mar 2021.

[2] T. Acharya et A. K. Ray – *Image processing: principles and applications*, John Wiley & Sons, 2005.

[3] M. K. Adomey – "Introduction to cryptography".

[4] A. Akram – "Conception et implémentation d'un système hybride pour la sécurité de données: application aux images numériques", *Mémoire présenté pour l'obtention Du diplôme de Master Académique, UNIVERSITE MOHAMED BOUDIAF-M'SILA, année* **2017** (2016).

[5] F. Armknecht, C. Boyd, C. Carr, K. Gjøsteen, A. Jäschke, C. A. Reuter et M. Strand – "A guide to fully homomorphic encryption", *Cryptology ePrint Archive* (2015).

[6] G. Bouthaina – "Représentation d'une image numérique", (2020).

[7] B. CHENENE – "Chiffrement des vidéos numériques", Thèse, UNIVERSITE MOHAMED BOUDIAF-M'SILA FACULTE DES MATHEMATIQUES ET DE L . . . , 2019.

[8] C. Competition – "Covid-19 x-ray image classification covid-19 cases classification from chest x-ray images", (2021).

[9] D. B. . G. Dartois – "cryptographie paris 13", (2010).

[10] R. C. a. R. E. W. GONZALES – "igital image processing", **ISBN013505267X** (2008).

[11] R. C. Gonzalez et R. E. Woods – "August 31", *Digital Image Processing Third Edition. Prepared by Pearson Education* (2007), p. 142–161.

[12] M. Hamoud – "Image , son , vidéo codage et transmission", (2020).

[13] M. Ilhem et G. N. E. Houda – *Cryptographie homomorphe pour les réseaux «vehicular cloud computing»*, Mémoire, Université Abou Bekr Belkaid - Tlemcen, 2017.

[14] — , *Cryptographie homomorphe pour les réseaux «vehicular cloud computing»*, Mémoire, Université Abou Bekr Belkaid - Tlemcen, 2017.

[15] S. web réalisé et référencé par Imedias : www.imedias.pro – "Les images vectorielles - images matricielles - image numériques", Feb 2022.

[16] M. Kara, A. Laouid, M. A. Yagoub, R. Euler, S. Medileh, M. Hammoudeh, A. Eleyan et A. Bounceur – "A fully homomorphic encryption based on magic number fragmentation and el-gamal encryption: Smart healthcare use case", *Expert Systems* **39** (2022), no. 5, p. e12767.

[17] Kaspersky – "What is data encryption? definition and explanation", Dec 2021.

[18] D. N. Kuate – "Cryptographie homomorphe et transcodage d'image/video dans le domaine chiffré", Thèse, Université Paris Saclay (COmUE), 2018.

[19] K. Mader – "Ct images from cancer imaging archive with contrast and patient age", (2017).

[20] C. A. MIKHAEIL – "Les auteurs", (2021).

[21] T. Perret – "qu'est-ce que le chiffrement homomorphe ?", *citation 6* (2022).

[22] L. Robichaud – "Différences entre image bitmap et image vectorielle".

[23] — , "L'image numérique pixels et couleurs".

[24] S. Sassi et C. Verdier – "Présentation et visualisation des documents médicaux", *Document numérique* **12** (2009), no. 3, p. 37–58.

[25] B. Schneider – "Cryptographie appliquée. 2 eme édition, 2001".

[26] A. Schools, A. B. Model, A.-B. Model, A. Colony, A. B. Colony, A. N. Network, A. Computing, B. Data, B. V. O. Local, C. Albicans et al. – "Complex adaptive systems, publication 3 cihan h. dagli, editor in chief conference organized by missouri university of science and technology 2013-baltimore, md", *Procedia Computer Science* **20** (2013), p. 553–558.

[27] M. Tebaa – "Chiffrement homomorphe appliqué au cloud bancaire", (2015).

[28] A. Vengadapurvaja, G. Nisha, R. Aarthy et N. Sasikaladevi – "An efficient homomorphic medical image encryption algorithm for cloud storage security", *Procedia computer science* **115** (2017), p. 643–650.

[29] G. Wang, Q. Liu, Y. Yao et A. Skowron – "Rough sets, fuzzy sets, data mining, and granular computing", *RSFDGrC, Springer 2003, Chongqing, China* (2003), p. 41–48.

[30] R. Yende – "Support de cours de sécurité informatique et crypto.", (2018).

[31] L. Zhang, L. Zhang, X. Mou et D. Zhang – "A comprehensive evaluation of full reference image quality assessment algorithms", *2012 19th IEEE International Conference on Image Processing*, IEEE, 2012, p. 1477–1480.