: N° d'ordre
: N° de série

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 :

- **ABID Sara**
- **ABDREBBI Saida**

Thème

Protection asymétrique des images médicales

Soutenue le14-06- 2022 Devant le jury:

M.	YAGOUB Mohammed Amine	MCB	Président
M.	KHELAIFA Abdennacer	MAA	Rapporteur
M.	LAOUID Abdelkader	MCA	Encadreur

Année Universitaire: 2021/2022

Dédicace

Nous remercions notre Seigneur de lui avoir donné la capacité d'écrire et de penser,

La force de croire en lui, et la patience jusqu'au bout du rêve et du bonheur.

Nous dédions cet acte humble à celui qui nous a donné la vie, un symbole

La tendresse qu'ils ont sacrifiée pour notre bonheur et notre réussite pour notre sécurité...

A notre père et notre mère, l'école de notre enfance, qui nous ont accompagnés tout au long de ces années d'études, qui tout au long de notre vie ont eu à cœur de nous encourager à nous Aider et à nous protéger.

Que Dieu les bénisse et les garde.

A notre chère soeur...

pour notre frère...

A nos amis....

A tous ceux qui nous aiment...

Nous dédions ce travail...

❖ ***ABID SARA***

Dédicace

Je dédie cette humilité à ceux qui ont été la raison de mon travail de la vie :
Au printemps tendresse qui Fatigué sur mon éducation et de l'éducation ma chère mère;
Pour la couronne de ma tête qui a planté ne récoltera Dieu précieux fait le lieu de repos du paradis : mon cher père;
A tous sœurs, frères et leurs fils.
A mon cher époux pour son encouragement continue;
A ma chère amie Nabila;
A toute ma famille et ma famille de mari;
A ma binôme Sarah, qui a partagé avec moi la préparation et la réalisation de ce travail;
A mes chers amies de ma camarades de classe
A Dr Ibrahim qui m'a beaucoup aidé à compléter mon travail
Ainsi qu'a Tous Ceux qui me sont Chers ....

❖ ***ABDREBBI SAIDA***

Remerciement

Tout d'abord nous remercions notre Dieu qui nous a donné

la force et la volonté de mener à bien ce travail.

Nous adressons nos sincères remerciements à notre encadrant

Dr.« LAOUID Abdelkader »

Qui était chargé de fournir des conseils et des orientations

pour chaque petit et chaque grand dans cette 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. Nous

remercie également tous ceux qui ont participé de près ou

loin de développer ce travail.

Résumé

Après que la révolution scientifique a envahi le monde et avec les nouveaux outils de développement scientifique moderne, il est nécessaire, pour chaque personne, de protéger ses informations personnelles liées à sa vie quotidienne. Dans ce sujet, il reste encore quelques problèmes, notamment la rapidité du cryptage de déchiffrement, la taille du cryptage des images et la façon dont les clés peuvent être partagées par une route sécurisée.

Ce projet de fin de cycle vise à proposer une nouvelle version du chiffrement asymétrique basé sur la fragmentation des nombres magiques. Le chiffrement de chaîne est transformé en blocs de blocs puis en un nombre décimal ; Enfin, l'image normale de ces blocs est bien chiffrée par un algorithme MNF-G.

Mots clés :

Image, Cryptage d'image, Décryptage d'image, Sécurité, Préservation de la confidentialité.

abstract

After the scientific revolution invaded the world and with the new tools of modern scientific development, it is necessary for every person to protect their personal information related to their daily life. In this topic, there are still some issues, including the speed of decryption encryption, the size of image encryption, and how keys can be shared through a secure route.

This end-of-cycle project aims to propose a new version of asymmetric encryption based on the fragmentation of magic numbers. The string cipher is transformed into blocks of blocks and then into a decimal number; Finally, the normal image of these blocks is well encrypted by an MNF-G algorithm.

Keywords :

Image, Image encryption, Image decryption, Security, Privacy preserving

ملخص

بعد أن اجتاحت الثورة العلمية العالم وباستخدام الأدوات الجديدة للتطور العلمي الحديث ، أصبح من الضروري لكل شخص حماية معلوماته الشخصية المتعلقة بحياته اليومية. في هذا الموضوع، لا تزال هناك بعض المشكلات ، بما في ذلك سرعة فك التشفير وحجم تشفير الصورة وكيف يمكن مشاركة المفاتيح بواسطة مسار آمن.

يهدف مشروع نهاية الدورة هذا إلى اقتراح نسخة جديدة من التشفير غير المتماثل بناءً على تجزئة الأرقام السحرية. يتم تحويل تشفير السلسلة إلى كتل من الكتل ثم إلى رقم عشري ؛ أخيرًا ، يتم تشفير الصورة العادية لهذه الكتل جيدًا بواسطة خوارزمية MNF-G

الكلمات المفتاحية:

الصورة، تشفير الصور، فك تشفير الصور، الأمن، الحفاظ على الخصوصية.

TABLE DES MATIÈRES

Sommaire **iv**

Table des figures **vi**

Introduction générale **1**

1 Cryptage d'images en générale **2**

1.1 Introduction . . . 3

1.2 Cryptographie . . . 3

1.2.1 Cryptage symétrique . . . 3

1.2.2 Cryptage asymétrique . . . 5

1.3 Objectifs de la cryptographie (A quoi sert la cryptographie) . . . 7

1.3.1 La confidentialité . . . 7

1.3.2 L'authentification . . . 7

1.3.3 L'intégrité . . . 7

1.3.4 La non répudiation . . . 7

1.3.5 Contrôle d'accès . . . 7

1.4 L'imagerie en général . . . 7

1.4.1 Définition de l'image . . . 7

1.4.2 L'image numérique . . . 8

1.4.3 Types d'image numérique . . . 8

1.5 Imagerie médicale . . . 10

1.5.1 Définition . . . 10

1.5.2 Types d'imagerie médicale . . . 10

1.6 Cryptage d'images . . . 13

1.6.1 Mécanismes de cryptage des images médicales . . . 14
1.6.2 Quelques techniques de cryptage d'images . . . 15
1.7 Conclusion . . . 18

2 Etat de l'art **19**
2.1 Introduction . . . 20
2.2 Travaux connexes . . . 20
2.3 Conclusion . . . 24

3 La méthode proposée **25**
3.1 Introduction . . . 26
3.2 Schéma global . . . 26
3.2.1 MNF-G . . . 26
3.3 Schémas partiels et leur explication . . . 28
3.3.1 L'image originale . . . 28
3.3.2 Algorithme de cryptage . . . 29
3.3.3 Algorithme de décryptage . . . 30
3.3.4 Image decrypte . . . 30
3.4 La méthode de chiffrement par fragmentation . . . 31
3.5 Conclusion . . . 33

4 Implémentation et analyse **34**
4.1 Introduction . . . 35
4.2 Environnement de développement . . . 35
4.2.1 Environnement logiciel . . . 35
4.2.2 Environnement matériel . . . 36
4.2.3 Critères d'évaluation . . . 36
4.2.4 L'histogramme . . . 38
4.2.5 Entropie . . . 40
4.2.6 Analyse de sensibilités . . . 40
4.3 Conclusion . . . 43

Conclusion générale **44**

Bibliographie **45**

TABLE DES FIGURES

1.1 Image numérique 8
1.2 Radiographie du thorax IRM 11

2.1 Schéma global du modèle basée sur des clés pour la sécurité des images médicales . . 21
2.2 Asymmetric image encryption scheme based on the quantum logistic map and cyclic modulo diffusion. 22

3.1 La protection d'une image 27
3.2 Diagramme montrant comment lire les données d'image. 28
3.3 Graphique montrant comment décrypter chaque pixel. 29
3.4 Algorithme decryptage. 30
3.5 L'architecture de cloud computing proposée 31
3.6 Propriété homomorphe 32

4.1 Caractéristiques de l'ordinateur sur lequel nous avons travaillé le projet de fin d'études. 36
4.2 pseudo-code illustre les intervalles des valeurs des variables. 37
4.3 Une illustration montrant la taille des variables impliquées dans l'espace de clé 37
4.4 Une comparaison entre l'histogramme d'une image originale et une image cryptée. . . 38
4.5 L'interface principale de l'application 39
4.6 figure montre l'upload image cryptée vers le cloud 39

INTRODUCTION GÉNÉRALE

Les informations médicales sont, bien sûr, plus que de simples données d'imagerie médicale. Par exemple, une image médicale est une image du corps humain ou de parties de celui-ci prise à des fins thérapeutiques personnelles ou de recherche. Les scientifiques ont travaillé dur pour assurer la sécurité de cette image. en créant des mécanismes de cryptage efficaces afin d'assurer la confidentialité des données, la disponibilité et la fiabilité. L'un des problèmes les plus importants auxquels sont confrontées les images médicales est le problème du maintien de la confidentialité, qui à son tour a posé un véritable défi aux informaticiens et aux mathématiciens, et l'expansion des problèmes de confidentialité des données et des algorithmes.Les données sont également exposées aux attaques. l'attaquant est de manipuler, voler ou détruire des informations sensibles. Pour protéger les images médicales de ces attaques et problèmes, nous avons proposé un système de cryptage asymétrique qui améliore la confidentialité, la disponibilité et la fiabilité. Notre sujet d'étude est divisé en quatre chapitres :

Dans **le premier chapitre**, Dans celui-ci, nous avons traité de la définition du cryptage en général, puis mentionné ses types et des exemples de chaque type. Nous avons également défini l'image médicale et l'image, mentionné leurs types et exemples.

Dans **le deuxième chapitre**, Nous avons mentionné quelques-unes des recherches effectuées antérieurement pour la protection des images médicales et identifié leurs forces et leurs faiblesses. Nous avons également expliqué l'idée sur laquelle repose le système proposé et identifié ses avantages.

Dans **le troisième chapitre**,nous mettons en évidence le schéma général et les éléments de base du système Discutez de chaque partie de ce tableau.

Dans **le quatrième chapitre**, dans ce chapitre, nous présenterons l'application de l'algorithme et créez une application qui simule les étapes en détails. Ensuite, nous effectuons une chaîne d'analyse des résultats.

CHAPITRE 1

CRYPTAGE D'IMAGES EN GÉNÉRALE

1.1 Introduction

Après la révolution scientifique, le codage est devenu l'une des premières applications de l'informatique, car il a envahi divers domaines (éducation, commerce, médecine, astronomie...etc). Tous recherchent plus de protection pour leurs données transmises, qu'elles soient professionnelles ou privées, ce qui a conduit à l'émergence de la cryptographie. Ces dernières années, les méthodes de cryptage se sont multipliées. Dans ce chapitre, nous allons expliquer les concepts, mettre en évidence les images médicales asymétriques, les expliquer et montrer les problèmes auxquels elles sont confrontées.

1.2 Cryptographie

La cryptographie est une méthode de protection des informations et des communications par l'utilisation de codes, de sorte que seuls les destinataires des informations puissent les lire et les traiter. Le préfixe « crypt- » signifie « caché » ou « coffre-fort » et le suffixe « -graphie » signifie « écriture » [1].

1.2.1 Cryptage symétrique

Le chiffrement symétrique, également appelé chiffrement à clé privée, se produit lorsque les données sont chiffrées et déchiffrées par l'expéditeur et le destinataire à l'aide de la même clé secrète. Cela signifie que la clé doit être transmise de manière sécurisée afin que seul le destinataire puisse y accéder. Voici comment fonctionne le processus de protection des informations par chiffrement symétrique :

1. L'expéditeur (ou le destinataire) choisit un algorithme de chiffrement, génère une clé, informe le destinataire (ou l'expéditeur, selon le cas) de l'algorithme sélectionné et envoie la clé sur un canal de communication sécurisé.
2. L'expéditeur crypte le message avec la clé et envoie le message crypté au destinataire.
3. Le destinataire reçoit le message crypté et le décrypte en utilisant la même clé.

Il y a pas mal de chiffres identiques parmi eux : DES (Data Encryption Standard), AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), RC4 (Rivest cypher4).

1.2.1.1 Les points forts du chiffrement à clé symétrique L'avantage le plus notable du chiffrement symétrique est sa simplicité, car il utilise une seule clé pour le chiffrement et le déchiffrement. En tant que tels, les algorithmes de chiffrement symétriques sont beaucoup plus rapides que les algorithmes asymétriques et nécessitent moins de puissance de traitement.

1.2.1.2 Faiblesses du chiffrement à clé symétrique Le fait que la même clé soit utilisée pour le chiffrement et le déchiffrement est la principale faiblesse des systèmes de chiffrement symétriques.

La nécessité de transmettre la clé à l'autre partie est une faille de sécurité car si elle tombe entre de mauvaises mains, les informations seront décryptées. Par conséquent, une attention particulière doit être accordée aux moyens possibles d'intercepter la clé et d'améliorer la sécurité de la transmission.

1.2.1.3 Exemples d'algorithmes de chiffrement symétrique Il existe de nombreux chiffres symétriques. Voici quelques exemples parmi les plus connus.

1.2.1.4 Chiffrement à bloc : La différence est située dans la division des données en blocs de taille généralement fixe. taille de bloc entre 32 et 512 bits.

— **DES** (Data Encryption Standard) est un algorithme de cryptage développé par IBM et approuvé par le gouvernement américain en 1977 comme standard officiel. La taille de bloc pour DES est de 64 bits. Actuellement considéré comme obsolète et inutilisé [2].

— **3DES** (Triple DES) a été créé en 1978 sur la base de l'algorithme DES pour éliminer le principal inconvénient de ce dernier : la petite longueur de clé (56 bits), qui peut être craquée par force brute. La vitesse de 3DES est trois fois plus lente que celle de DES, mais la sécurité cryptographique est beaucoup plus élevée. L'algorithme 3DES est basé sur DES, il est donc possible d'utiliser des programmes créés pour DES pour l'implémenter. Il est toujours utilisé, notamment par l'industrie du paiement électronique, mais est progressivement remplacé par des algorithmes plus récents [3].

— **AES** (norme de chiffrement avancé). Cet algorithme de chiffrement avec une taille de bloc de 128 bits et une clé de 128/192/256 bits a été développé en 2001 en remplacement du DES. Il est actuellement considéré comme l'un des chiffrements symétriques les plus efficaces et les plus sûrs et est donc largement utilisé [4].

1.2.1.5 Cryptanalyse et amélioration d'un schéma efficace et sécurisé de protection des images médicales Des mécanismes conjoints sécurisés de compression et de cryptage d'images médicales sont proposés dans en utilisant des transformées multi-échelles et des techniques de cryptage à clé symétrique. Les transformées multi-échelles impliquées dans cet article sont la transformée en ondelettes, la transformée en bandelettes et la transformée en courbes. Les techniques de cryptage impliquées dans cet article sont l'algorithme international de cryptage de données (IDEA), Rivest Cipher (RC5) et Blowfish. La technique de codage utilisée dans cet article est le codage par bloc intégré avec troncature (EBCOT). Des résultats expérimentaux sont obtenus pour les travaux proposés et évalués à l'aide de divers paramètres tels que le rapport signal/bruit maximal (PSNR), l'erreur quadratique moyenne (MSE), l'indice de qualité d'image (IQI) et l'indice de similarité structurelle (SSIM), la différence moyenne (AD), corrélation croisée normalisée (NK), contenu structurel (SC), différence maximale (MD), erreur quadratique moyenne laplacienne (LMSE) et erreur absolue normalisée (NAE).

Il est justifié que les approches proposées dans cet article donnent de bons résultats.

Un nouveau cadre de cryptage pour image médicale avec filigrane basé sur un système hyperchaotique

Une trame de cryptage d'image médicale avec filigrane basée sur un système hyperchaotique est proposée dans cet article. Les informations médicales, telles que les informations privées des patients, les données nécessaires au diagnostic et les informations pour l'authentification ou la protection des dossiers médicaux, sont intégrées dans les régions d'intérêt (ROI) dans les images médicales avec des données réversibles basées sur un histogramme de différence à haute capacité -schéma de masquage. Après cela, les images médicales filigranées sont cryptées avec des systèmes hyperchaotiques. Du côté récepteur, le récepteur avec la clé de cryptage peut décrypter l'image pour obtenir des images similaires pour le diagnostic. Si le destinataire dispose en même temps de la clé de dissimulation des données, il peut extraire les informations privées intégrées et récupérer de manière réversible l'image médicale d'origine. Des expériences et des analyses démontrent qu'une capacité d'intégration élevée et une faible distorsion ont été obtenues dans le processus de masquage des données, et, en même temps, une sécurité élevée a été acquise dans la phase de cryptage.

1.2.2 Cryptage asymétrique

Le chiffrement asymétrique, également connu sous le nom de cryptographie à clé publique, est un système de chiffrement qui utilise deux clés. La clé publique peut être envoyée sur un canal non sécurisé et est utilisée pour chiffrer le message. Une clé privée connue uniquement du destinataire est utilisée pour déchiffrer le message.

La paire de clés est mathématiquement liée l'une à l'autre, vous pouvez donc calculer la clé publique en connaissant la clé privée, mais pas l'inverse voici comment fonctionne le chiffrement asymétrique :

1. Le destinataire choisit un algorithme de chiffrement et génère une paire de clés publique et privée.
2. Le destinataire transmet la clé publique à l'expéditeur.
3. L'expéditeur crypte le message avec la clé publique et envoie le message crypté au destinataire.
4. Le destinataire reçoit le message chiffré et le déchiffre à l'aide de sa clé privée.

Les points forts du chiffrement à clé asymétrique

L'avantage le plus notable du chiffrement symétrique est sa simplicité, car il utilise une seule clé pour le chiffrement et le déchiffrement. En tant que tels, les algorithmes de chiffrement symétriques sont beaucoup plus rapides que les algorithmes asymétriques et nécessitent moins de puissance de traitement.

Faiblesses du chiffrement à clé asymétrique

Cette méthode de cryptage présente également des inconvénients. Les exemples incluent une complexité plus élevée, une vitesse plus faible et une demande accrue de ressources de calcul. De plus, malgré la haute sécurité de la cryptographie asymétrique, elle est toujours vulnérable à une attaque de l'homme du milieu (MITM), dans laquelle un attaquant intercepte la clé publique envoyée par le destinataire à l'expéditeur. Ensuite, l'attaquant crée sa propre paire de clés et se fait passer pour un destinataire en envoyant une fausse clé publique à l'expéditeur que l'expéditeur croit être la clé publique envoyée par le destinataire. L'attaquant intercepte les messages chiffrés de l'expéditeur au destinataire, les déchiffre avec sa clé privée et les rechiffre à l'aide de la clé publique des destinataires, Il envoie le message au destinataire. De cette façon, aucun des participants n'était au courant qu'un tiers interceptait le message ou le remplaçait par un faux message. Cela met en évidence la nécessité d'une authentification par clé publique.

Exemples d'algorithmes de chiffrement asymétrique

Voici des exemples d'algorithmes de chiffrement asymétrique bien connus :

— RSA (Rivest Shamir Adleman), le plus ancien algorithme de chiffrement asymétrique, a été publié en 1977 et porte le nom de ses créateurs, les scientifiques américains du Massachusetts Institute of Technology (MIT) Ron Rivest, Adi Shamir et Leonard Adleman. Il s'agit d'un algorithme relativement lent souvent utilisé dans les systèmes de chiffrement hybrides en combinaison avec des algorithmes symétriques.

— DSA (Digital Signature Algorithm) a été créé en 1991 par le National Institute of Standards and Technology (NIST) aux États-Unis. Son utilisé pour l'authentification de signature numérique. Une signature électronique est créée avec une clé privée dans cet algorithme mais peut être vérifiée avec une clé publique. Cela signifie que seul le propriétaire de la signature peut créer la signature, mais que n'importe qui peut vérifier son authenticité.

Diffie-Hellman a été publié en 1976 par lescryptographes américains Whitfield Diffie et MartinHellman. C'est un protocole cryptographique qui permet àdeux ou plusieurs parties d'obtenir une clé privéepartagée en utilisant un canal de communication nonsécurisé. La clé est utilisée pour chiffrer le reste del'échange à l'aide d'algorithmes de chiffrementsymétriques. Le schéma de distribution des clés via descanaux sécurisés proposé par Diffie et Hellman aconstitué une percée importante en cryptographiepuisqu'il a supprimé le principal problème de lacryptographie classique, la distribution des clés.

1.3 Objectifs de la cryptographie (A quoi sert la cryptographie)

La cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

1.3.1 La confidentialité

La confidentialité permet d'assurer que seuls les utilisateurs autorisés ont accès aux informations. Le texte chiffré ne doit être lisible que par les destinataires légitimes. Il ne doit pas pouvoir être lu par un intrus.

1.3.2 L'authentification

L'authenticité est l'assurance que l'expéditeur d'un message est bien celui qu'il prétend être. C'est le domaine de la signature numérique et de la cryptographie à clé publique en général.

1.3.3 L'intégrité

C'est un service qui traite de la modification non autorisée des données. Cette propriété fait référence aux données qui n'ont pas été modifiés, détruites ou perdues de manière malveillante ou accidentelle.

1.3.4 La non répudiation

La non-répudiation est un moyen de garantir que l'expéditeur d'un message ne peut pas plus tard nier l'envoie du message et que le destinataire ne peut pas nier la réception du message .

1.3.5 Contrôle d'accès

Il existe de nombreuses approches différentes pour gérer l'accès aux ressources. Le contrôle d'accès basé sur les rôles est le plus notable et le plus courant. Par défaut, toutes les demandes qui ne remplissent pas les conditions spécifiées se voient refuser toutes les autorisations pour les utilisateurs dans le but d'assurer une sécurité complète après cela, les administrateurs accordent les privilèges requis aux rôles appropriés.

1.4 L'imagerie en général

1.4.1 Définition de l'image

Une image peut être définie comme une fonction bidimensionnelle, $f(x, y)$, où x et y sont des coordonnées spatiales (plan), et l'amplitude de f à n'importe quelle paire de coordonnées

(x, y) s'appelle l'intensité ou le niveau de gris de l'image à ce point [5] .

1.4.2 L'image numérique

Une image numérique est composée de cases appelées pixels [6] Ces pixels seront affectés de nombres binaires permettant de définir des teintes de gris ou des couleurs [7].

FIGURE 1.1 – Image numérique

Les attributs des images

• **Pixel :** C'est le plus petit élément d'une matrice de points ou d'un matériau générateur d'image, c'est-à-dire que c'est le plus petit élément qui peut être représenté et contrôlé dans ses propriétés à partir de l'image des composants sur les écrans avec leurs différentes technologies, et le plus petit élément qui peut être numérique et stocké dans des scanners ou dans un capteur d'appareil photo numérique. [8].

• **Définition :** La définition ou la dimension d'une image est le nombre total de ces pixels [9].

• **La taille :** La taille de l'image est la place qu'elle occupe dans le codage binaire. Son unité est l'octet [10].

Taille = nombre d'octets pour chaque pixel * définition.

• **Résolution :** La résolution indique le niveau de qualité de l'image. Plus la résolution est élevée, meilleure est la qualité de l'image.

La résolution d'une image est définie par le nombre de pixels par unité de longueur dpi (dot per inch) Résolution = définition/longueur.

1.4.3 Types d'image numérique

Il existe deux types d'images numériques :

Matricielle (bitmap)

Une image bitmap est composée en mode point [11]. Formée d'une grille composée de pixels. Plus on zoom, plus les pixels deviennent apparents[12]. Les formats d'images bitmap : BMP, PCX, GIF,JPEG, TIFF. Les photos numériques et les images scannées sont de ce type [13].

Avantages

Le mode de codage des images bitmap (24 bits, codage RBG)les rend adaptées au fonctionnement des principaux périphériques, notamment les controleurs d'écran "true colors" (point allumé ou non, codé sur x bits). Elles conviennent fort bien aux images complexes, principalement d'origine analogique, qui ne peuvent être codées qu'en mode point.

Inconvénients

— Plus lourd que le format vectoriel. Une image matricielle prend plus de place en mémoire.

— Elles supportent mal les opérations de redimensionnement, réduction ou agrandissement. Les deux opérations se traduisent par une perte d'information.

Vectorielle

C'est une image numérique composée d'objets géométriques individuels (segments de droite, polygones, arcs de cercle, etc.) définis chacun par divers attributs de forme, de position, de couleur, etc. (définis de manière mathématique). Par exemple, une image vectorielle d'un cercle est définie par des attributs de types : position du centre, rayon... Ces images sont utilisées pour réaliser des schémas ou des plans mais pas exclusivement [14].

Avantages

Les fichiers qui la composent sont petits, les redimensionnements sont faciles sans perte de qualité.

Inconvénients

Une image vectorielle ne permet de représenter que des formes simples. Elle n'est pas donc utilisable pour la photographie notamment pour obtenir des photos réalistes.

Représentation des couleurs

Une image numérique est un tableau de points représentant les couleurs (pixels). Usuellement on distingue 3 grands types de couleurs pour une image numérique :

— Le noir et blanc.

— Les niveaux de gris.

— La couleur.

Image noir et blanc Le noir et blanc est le plus simple .Un seul bit suffit pour coder l'information, par exemple 0 pour le noir et 1 pour le blanc[15].

Niveaux de gris Le codage dit en niveaux de gris permet d'obtenir plus de nuances que le simple noir et blanc. [10]. On utilise en générale 8 bits, ce qui donne 256 nuances de gris possibles pour le pixel, de 0 (noir) à 255 (blanc).

Image coleurs La couleur de chaque pixel est définie par 3 composantes : Rouge, Vert et Bleu(système RVB ou RGB en anglais). L'intensité de chaque composante est codée sur 8 bits,donc chaque composante. à une valeur comprise entre 0 (absence de couleur) et 255(intensité maximale de la couleur). Ainsi la couleur d'un pixel nécessite 24 bits (3 octets) pour être codée.

1.5 Imagerie médicale

1.5.1 Définition

L'imagerie médicale regroupe l'ensemble des moyens physiques ou des techniques utilisés par la médecine pour le diagnostic mais aussi pour le traitement d'un grand nombre de pathologies pour visualiser les cellules d'un organisme (corps humain) [5].

1.5.2 Types d'imagerie médicale

Parmi les méthodes d'imagerie médicales les plus couramment employées en médecine, on peut citer d'une part les méthodes tomographiques basées soit sur les rayons X (radio- logie conventionnelle, tomodensitom être ou CT-scan, angiographie,...) soit sur la résonance magnétique (IRM), les méthodes échographiques utilisant les ultra-sons, et enfin les méthodes optiques utilisant les rayons lumineux [10].

FIGURE 1.2 – Radiographie du thorax IRM

1.5.2.1 Tomodensitométrie Un scanner, communément appelé scanner, peut créer une image détaillée de l'intérieur du corps à l'aide de rayons X et d'ordinateurs. Ils sont différents d'une radiographie car ils produisent une image en coupe transversale du corps, similaire à une IRM, ce qui les rend plus aptes à regarder les tissus mous et des parties plus précises de l'image qu'une radiographie ne pourrait pas [16].

Avantages

— Un scanner est assez court il ne prend que 10 à 20 minutes environ.

— Les résultats sont très rapides par rapport à certains autres types de numérisation.

— Les tomodensitogrammes sont indolores, car ils ne sont pas chirurgicaux.

Inconvénients

— Comme pour de nombreux scanners, votre corps est exposé à des radiations. Plus le corps du patient est examiné de près, plus il sera exposé aux radiations.

— Cependant, ils sont conçus pour réduire l'exposition aux rayonnements. Il existe un risque de réaction allergique au colorant utilisé.

1.5.2.2 IRM , imagerie par résonance magnétique Une IRM, également appelée IRM, est une image en coupe détaillée d'une partie du corps. Il est similaire à un scanner, mais avec une qualité supérieure, il est donc plus facile de voir les différences dans les tissus [17].

Avantages

— Les examens IRM sont indolores et sûrs, car les champs magnétiques et les ondes radio n'ont aucun effet négatif connu sur le patient.

— Il n'implique aucune exposition aux rayons X, il peut donc être utilisé par les femmes enceintes et les enfants si nécessaire.

Inconvénients

— Une IRM entoure une grande partie du corps, ce qui met les personnes claustrophobes mal à l'aise.

— Le métal ne peut pas pénétrer à l'intérieur du scanner IRM, de sorte que les personnes portant certains implants tels que les stimulateurs cardiaques ne peuvent pas les utiliser.

1.5.2.3 Tomographie par émission de positrons TEP Un PET scan peut créer une image tridimensionnelle de l'intérieur du corps. Il peut être combiné avec un scanner et une IRM pour créer une image plus claire pour montrer ce qui se passe. Il peut également se concentrer sur des parties spécifiques du corps, montrant à quel point une partie du corps fonctionne bien. L'image ci-dessous montre comment un PET scan et un CT scan peuvent être combinés [18].

Avantages

— Le glucose saturé radioactif a été utilisé pour le glucose, de sorte que le corps le traite de la même manière. Le scan ne prend que 30 minutes environ.

— Une TEP peut détecter des changements métaboliques au niveau cellulaire qui se produisent dans un organe ou un tissu, ce que la TDM ou l'IRM ne peuvent pas.

Inconvénients

— Une TEP vous expose à des radiations, qui peuvent conduire à un cancer.

— Cependant, le montant est très faible. Demi-vie du traceur radioactif.

— Les patients doivent éviter les personnes qui ne doivent pas être exposées aux radiations, telles que les femmes enceintes, pendant quelques heures après l'examen.

1.5.2.4 Imagerie par ultrasons L'échographie utilise des ondes à haute fréquence pour montrer ce qui se trouve à l'intérieur d'une partie du corps. Il est également connu sous le nom d'échographie [19].

Avantages

— l n'y a généralement pas de séquelles d'une échographie. Cela signifie que l'activité normale peut être reprise immédiatement après.

— Les résultats apparaissent en temps réel, il n'est donc pas nécessaire d'attendre.

Inconvénients

— Certains couvre-sondes contiennent du latex, ce qui peut poser problème si le patient est allergique au latex.

— L'échographie endoscopique peut provoquer des maux de gorge, des ballonnements ou, dans les cas extrêmes, des saignements internes.

1.5.2.5 Imagerie par rayons X Une radiographie est une procédure très courante utilisée pour obtenir des images de l'intérieur du corps. Le rayonnement est utilisé dans la partie rayons X du spectre électromagnétique [20].

Avantages

— L'appareil n'entoure pas tout le corps, il ne causera donc pas d'anxiété chez les personnes souffrant de claustrophobie.

— La procédure ne prend que quelques minutes.

Inconvénients

— Certains agents de contraste peuvent provoquer des effets secondaires indésirables.

— Les rayons X exposent le patient à des rayonnements indésirables, qui peuvent entraîner un cancer, mais la quantité de rayonnement émise est minime.

1.6 Cryptage d'images

Le cryptage des images médicales est considéré comme l'un des les domaines les plus prédominants des systèmes cryptographiques qui doit être fait avec des algorithmes qui nécessitent moins de temps et moins de coût. Par le processus de cryptage d'une image, il est essentiel d'appliquer un algorithme de chiffrement symétrique ou asymétrique pour l'image d'entrée pour être convertie en une image chiffrée en utilisant clés symétriques ou asymétriques. Les chiffrements symétriques utilisent un clé pour le processus de chiffrement et de déchiffrement tout en étant asymétrique les chiffrements utilisent des clés différentes pour le chiffrement et le déchiffrement.

Le cryptage des images médicales peut être effectué à l'aide de différents algorithmes utilisant différents paramètres. Cryptage de les images médicales peuvent être réalisées par brouillage à grande vitesse [21], peu diffusion sage xor, cartes chaotiques et bord et ainsi de suite. La performance de l'algorithme qui a été utilisé pour chiffrer les images médicales peuvent être analysées à l'aide de mesures telles que le pic rapport signal sur bruit, taux d'erreur sur les bits, fidélité et carré moyen erreur.

L'objectif principal du cryptage des images médicales est de :

— Transmission sécurisée des dossiers médicaux des patients.

— Garantir la confidentialité et l'intégrité.

— Éviter les changements dans les images médicales qui peuvent conduire au faux diagnostic.

— Résister aux attaques et menaces de cyber sécurité.

1.6.1 Mécanismes de cryptage des images médicales

✓ **Le brouillage** [22] est une méthode de cryptage des données et mécanisme d'authentification utilisé pour protéger les données médicales image ou toute information d'être volé, distribué et modification. C'est l'une des méthodes de protection contre la copie qui sont largement utilisés. En général, le brouillage modifie la format compréhensible du texte au format non compréhensible afin d'éviter la visualisation illégale de données confidentielles. Le processus de brouillage est maintenant automatisé grâce à l'utilisation de brouilleurs qui sont très utilisés dans les télécommunications systèmes. Ce brouilleur remplace une séquence de données dans d'autres séquences et par conséquent la séquence reste brouillée et incompréhensible. Le brouillage est principalement utilisé pour deux les raisons :

— Pour assurer la récupération des données confidentielles.

— Pour s'assurer qu'aucune donnée n'est modifiée ou perdue pendant transmission.

✓ **La diffusion** est le processus où un seul changement de bit peut conduire à de sérieux changements dans le texte d'entrée. Un peu de changement dans le le texte en clair devrait éventuellement changer cinquante pour cent des bits dans le texte chiffré qui est généré et de même un changement de bit dans le texte chiffré devrait changer la moitié du texte en clair.
La diffusion peut être effectuée en utilisant bitwise xor et modulo arithmétique. Alors que xor au niveau du bit offre une plus grande efficacité dans cas des plates-formes matérielles, l'arithmétique modulo fournit vitesse d'exécution plus rapide dans le cas de plates-formes logicielles. La diffusion fait souvent référence à la propriété de redondance qui le changement de texte en clair peut changer le texte chiffré. La transposition est une technique importante de diffusion où

il existe une dépendance entre les bits d'entrée et de sortie. Dans un bon processus de diffusion, le retournement d'un bit en entrée doit changer essentiellement la moitié des bits dans le texte chiffré résultant

1.6.2 Quelques techniques de cryptage d'images

La cryptographie joue un rôle majeur dans la réalisation de cet objectif. En raison de la popularité croissante et du besoin Pour crypter les images, de nombreuses méthodes ont été inventées pour le même. Certains d'entre eux incluent le système de chaos. Notre objectif dans cette courte revue est de fournir un bref résumé du contenu et de rechercher des documents de manière simple afin que les lecteurs puissent comprendre et choisir la technologie qui répond le mieux aux besoins individuels. Nous mentionnons brièvement chaque méthode .

Chiffrement basé sur le chaos

Utiliser de vrais nombres aléatoires [23] Le résumé de Hongjun Liu, Kadir, Xiabo Sun se concentre principalement sur la véritable génération de nombres aléatoires. la séquence / le motif est dit vraiment aléatoire s'il passe tous les tests statistiques de caractère aléatoire, ce que nous pourrions trouve jamais. L'image cryptée doit être imprévisible et reproductible par une personne non autorisée. la nouveauté ici est la génération de clés à usage unique par la valeur de hachage du bruit environnemental véritablement aléatoire (à l'aide d'un enregistreur vocal numérisé). Un système d'équations, c'est-à-dire le système de Liu, est utilisé pour améliorer l'état chaotique al–déjà atteint. Comme l'entrée requise varie à chaque fois, cette méthode est très résistante aux attaques externes. Même bien que les calculs nécessaires pour créer un état chaotique soient complexes, les opérateurs utilisés ici sont très simples pour la mise en oeuvre .

Utilisation du système chaotique de Chen [23]. Cette méthode estime que le cryptage sélectif des quatre plans de bits supérieurs d'une image peut entraîner un bon niveau de sécurité. Le brouillage et la diffusion des pixels dans l'image sont effectués. La méthode proposée par ZhouFeng Chen, Wei Zhao, Jiang, Chong Fu est sécurisée contre les attaques par force brute et est sensible à la clé et efficace. même en termes de vitesse. Le succès de cette méthode peut être limité en raison des opérations courantes qu'elle utilise. Cela rend les attaques externes vulnérables malgré un temps d'exécution réduit .

Utilisation du décalage cyclique [24]. Dans cette méthode, les lignes et les colonnes sont brouillées de manière aléatoire à l'aide d'une carte logistique 1D. La diffusion de pixels peut être effectuée un certain nombre de fois. Chacun des processus brouillés (tel qu'un brouillage

de lignes) est pris comme une image séparée et enfin, toutes les images ainsi produites sont XOR-ed pour obtenir l'image cryptée. La méthode proposée par des professeurs de l'Université de Sastra vise à améliorer les lacunes de la séquence cyclique génération par Wang. Cependant, le caractère aléatoire de la ligne ou de la colonne, quant à la manière dont elles peuvent être sélectionnées, peut créer confusion car aucun algorithme pour une telle sélection n'a été proposé.

Transformée d'Arnold

Dans cette méthode, le récepteur doit sélectionner et envoyer une image de référence en plus de l'image d'origine qui doit être sécurisé. L'image cryptée finale ressemblera à l'image de référence. Cette référence l'image est le double de la taille de l'image nécessaire pour être cryptée. La transformée discrète en ondelettes peut également être utilisée pour crypter l'image. Le schéma proposé par V M Manikandan et V Masilamani est utilisé de telle manière que le les valeurs de pixel de l'image avant le cryptage sont comprises entre (0 et 255). La transformation d'Arnold a un périodique spécial propriété qui assure qu'après j (j $<$ maximum de longueur, largeur de l'image) itérations, la matrice brouillée sera transformée en celle d'origine. L'utilité de cette méthode est que l'image cryptée sera ressembler à une image naturelle sans produire l'image conventionnelle semblable à du bruit. Et le destinataire obtient son image à partir de l'image réelle.

Arnold et Logistique [25] La méthode de Jinshan Wang, Xiaodong Wang, Changjiang Zhang estime que pour obtenir le filigrane robuste, le filigrane doit être intégré dans les composants basse fréquence de l'image. Premièrement le l'image donnée est brouillée à l'aide de la transformation d'Arnold. Ensuite, les cartes logistiques sont utilisées pour le brouillage. L'image originale est décomposée par une transformée discrète en ondelettes. L'image en filigrane est mélangée par la transformation d'Arnold. Cette l'image filigranée est intégrée dans les coefficients basse fréquence du domaine d'ondelettes stationnaire discret et l'image filigranée finale est obtenue. L'image reconstruite finale a une bonne qualité visuelle ; ainsi, ce le procédé présente une bonne invisibilité et une bonne robustesse au bruit, à la rotation et à la compression.

Opération de séquence d'ADN [26]

Cette méthode est proposée par Xiuli Chai, Yran Chen, Lucie Vroyde. Une séquence d'ADN se compose de quatre bases d'acide nucléique, c'est-à-dire A (Adénine), C (Cytosine), G (Guanine) et T (Thymine). A, T et G, C sont complémentaires. Comme zéro et un sont complémentaires dans un système binaire, 00 et 11, 10 et 01 sont complémentaires. Huit des 24 règles de

codage de type satisfont à la règle complémentaire de Watson et Crick. Cette méthode traite Codage ADN pour coder l'image. Le hachage SHA-256 de l'image plane est utilisé pour générer le secret externe clé. La permutation des pixels est exécutée suivie d'une diffusion au niveau de l'ADN. Cette méthode est résistante à toutes sortes de attaques par force brute, entropie et attaques différentielles.

Arnold et Logistique [27] La méthode de calcul de l'ADN prend en charge un parallélisme élevé et utilise le concept de densité d'informations. La permutation brouille la position d'une image, tandis que la diffusion donne des informations sur la redondance de l'image. Cet article de Radhika K et M K Nalini combine des séquences d'ADN et des systèmes chaotiques. Dans cette méthode, le l'image est divisée en blocs. Ils sont ensuite convertis en matrices binaires et le codage de l'ADN est appliqué à leur. Ensuite, le brouillage des blocs est effectué et les blocs sont divisés en sous-blocs de taille égale. Ces les blocs sont ensuite ajoutés par addition d'ADN puis recombinés. Cette méthode conduit à un système hyper-chaotique qui résiste aux attaques différentielles et à l'entropie.

Niveau de bit Arnold [28] Il existe des formules prédéfinies pour l'utilisation de l'hyperchaos. Cette méthode par Wembo Zheng, Fei-Yue Wang et Kunfeng Wang utilisent les équations du système hyperchaotique de Chen. En outre, il existe un ensemble particulier de règles établies pour le codage ADN d'une image couleur. Cette méthode utilise les règles disponibles pour l'addition, la soustraction, et XOR-ing. Le système hyper-chaotique est utilisé pour la génération de clés secrètes. L'image cryptée est en outre remplacée par une image aléatoire générée artificiellement qui aide à augmenter la sécurité de l'image souhaitée. Une caractéristique intéressante de cette méthode est que le cryptage se fait de manière parallèle pour les deux, l'image à crypté ainsi que pour l'image artificielle aléatoire à générer. Cette méthode est résistante à l'attaque différentielle, à l'attaque par force brute.

1.7 Conclusion

Dans ce chapitre, nous avons donné un bref aperçu des concepts et des objectifs du cryptage et de ses types, cryptage symétrique et asymétrique, et nous avons clarifié le concept d'images médicales et d'images et mentionné leurs types.

CHAPITRE 2

ETAT DE L'ART

2.1 Introduction

Les images médicales sont des données importantes et sensibles dans les systèmes informatiques médicaux. Pour transmettre des images médicales sur un réseau non sécurisé, il est nécessaire de développer un algorithme de cryptage sécurisé. Parmi les trois principales caractéristiques des services de sécurité (à savoir la confidentialité, l'intégrité et la disponibilité), la confidentialité est la caractéristique la plus essentielle de l'échange d'images médicales entre cliniciens. Nous verrons certaines des recherches présentées, et nous mentionnerons les avantages que chaque travail a obtenus, et les défauts derrière ceux-ci que nous devons améliorer.

2.2 Travaux connexes

Avec le développement rapide dans le domaine du cryptage des images médicales, les chercheurs ont analysé un certain nombre d'algorithmes de cryptage basés sur des systèmes chaotiques. Mais il y a une difficulté, c'est-à-dire un petit espace de clé et une faible sécurité dans les cryptosystèmes chaotiques 1-D.
Pour surmonter cette difficulté, il existe des modèles de sécurité alternatifs Il a été proposé dans les travaux suivants...

Étudiez ce travail [29] des images médicales très sûres avec peu de sous-clés, où initialement peu de sous-clés sont données avec une logistique chaotique et des cartes de tente. Selon le processus chaotique (fonction C), la sécurité Il a été étudié en tant que diffusion ainsi que confusion.

Sur la base des conditions initiales, différents nombres aléatoires ont été générés pour chaque carte à partir de cartes chaotiques. Un algorithme d'optimisation adaptative de la sauterelle avec PSNR et fonction de fitness du coefficient de corrélation a été proposé pour choisir la clé secrète et publique optimale du système parmi les nombres aléatoires. La raison derrière le choix du processus adaptatif est d'améliorer l'investigation de haute sécurité du modèle proposé actuel par rapport aux méthodes existantes. Enfin, les résultats de la stratégie proposée ont été comparés aux méthodes de sécurité et aux œuvres littéraires existantes, mais se sont avérés très performants.

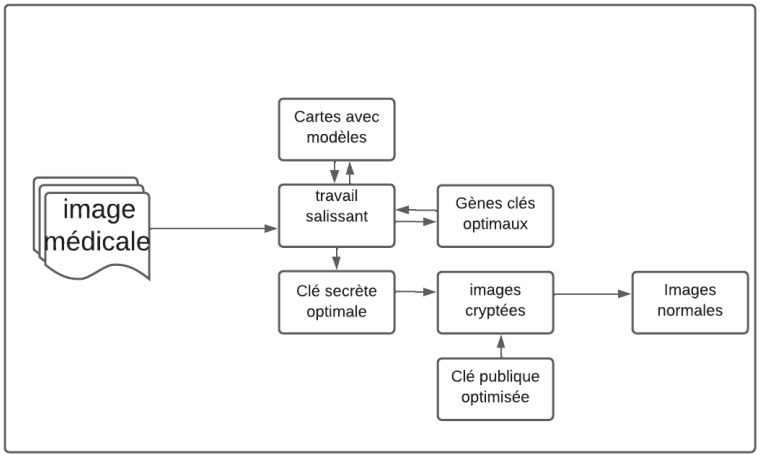


FIGURE 2.1 – Schéma global du modèle basée sur des clés pour la sécurité des images médicales

✓ **Avantages :** Les résultats de l'enquête de test ont déduit que le cryptage d'image à la lumière du PSNR, du CC, de l'entropie, etc., démontre les avantages d'un vaste espace de clés et d'une sécurité de haut niveau tout en maintenant une efficacité à des niveaux satisfaisants. Ainsi, un tour de chiffrement avec l'algorithme proposé est suffisant pour s'opposer à une attaque exhaustive, une attaque différentielle et une attaque statistique. De plus, la même taille d'image cryptée et décryptée confirme la moindre distorsion de l'image.

Dans cette étude[30], un nouveau schéma de cryptage d'image asymétrique basé sur l'algorithme Rivest-Shamir-Adleman (RSA) et la transformation d'Arnold est proposé. Tout d'abord, l'algorithme RSA à clé publique asymétrique est utilisé pour générer les valeurs initiales d'une carte logistique quantique. Deuxièmement, les paramètres de la carte d'Arnold sont calculés. Ensuite, une opération de brouillage d'Arnold est effectuée sur l'image simple pour obtenir le masquage approximatif des informations d'image. Troisièmement, chaque ligne et chaque colonne de l'image sont respectivement prises comme des unités différentes, puis la diffusion OU exclusif (XOR) est appliquée. Enfin, le flux de clés généré est utilisé pour effectuer une opération de diffusion modulo cyclique de bout en bout pour toutes les lignes et colonnes afin de produire l'image chiffrée finale. De plus, le flux de clés est lié à l'image en clair, ce qui peut améliorer la capacité à résister à l'attaque en clair choisie et à l'attaque en clair connue. Les résultats des tests montrent également que l'algorithme de chiffrement proposé a une forte sensibilité simple et une sensibilité clé.

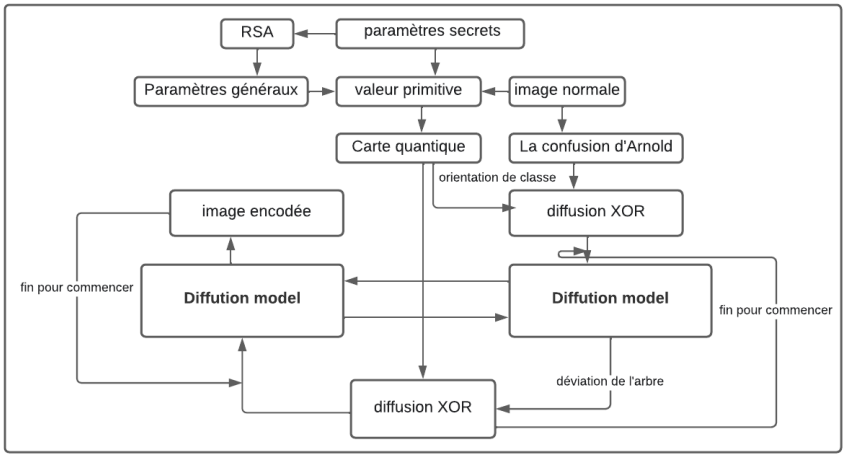


FIGURE 2.2 – Asymmetric image encryption scheme based on the quantum logistic map and cyclic modulo diffusion.

✓ **Négatives :** Le flux de clés est généré uniquement en fonction des clés secrètes ; Il est difficile d'assurer la gestion sécurisée des clés. Compte tenu de cela, cet article combine la carte logistique quantique, la transformation d'Arnold et la technologie de diffusion avec RSA pour concevoir un schéma de chiffrement asymétrique.

✓ **Avantages :** visant à réaliser une haute sécurité, une forte anti-attaque et plus adaptée à la transmission réseau. Les innovations de cet article sont :

1. Extraire les informations textuelles de l'image simple pour en faire un message clair.
2. Générer le message chiffré par RSA et produire les conditions initiales du système quantique par un nouveau modèle mathématique.
3. Mettre à jour les conditions initiales par les informations textuelles de l'image en clair pour améliorer la dépendance du texte en clair.
4. Construire une opération de diffusion modulo cyclique de bout en bout.

L'algorithme Goldreich Goldwasser Halevi (GGH) [31] peut être un bon choix pour chiffrer les images médicales car l'algorithme et les données sensibles sont représentés par des matrices numériques. De plus, l'algorithme GGH n'augmente pas la taille de l'image et, par conséquent, sa complexité restera aussi simple que O(n2). Cependant, l'un des inconvénients de l'utilisation de l'algorithme GGH est l'attaque Chosen Cipher Text. Dans notre stratégie, cette lacune de l'algorithme GGH a été prise en considération et a été améliorée en appliquant le rembourrage (c'est-à-dire le tour d'escargot XORing), avant le processus de cryptage GGH. Pour évaluer leurs performances, trois critères de mesure sont pris en compte : (i) Number of Pixels Change Rate (NPCR), (ii) Unified Average Changing Intensity (UACI) et (iii) Effet d'avalanche.

Les résultats sur trois tailles d'images différentes ont montré que l'approche GGH de rembourrage a amélioré l'UACI, le NPCR et l'avalanche de près de 100 , 35 % et 45 %, respectivement, par rapport à l'algorithme GGH standard. De plus, les résultats rendront le rembourrage GGH résistant au texte chiffré, au texte chiffré choisi et aux attaques statistiques. De plus, l'augmentation de l'effet d'avalanche de plus de 50 % est une réalisation prometteuse par rapport aux complexités accrues de la méthode proposée en termes de processus de cryptage et de décryptage.

La quantité de données visuelles numériques (image, vidéo et objet 3D) a augmenté rapidement sur Internet. La sécurité des images, des vidéos et des objets 3D devient de plus en plus importante pour de nombreuses applications, par exemple la transmission confidentielle, la vidéosurveillance, les applications militaires et médicales. Par exemple, la nécessité d'un diagnostic rapide et sécurisé est vitale dans le monde médical. De nos jours, la transmission de données visuelles est une routine quotidienne et il est nécessaire de trouver un moyen efficace de les transmettre sur les réseaux. Deux grands groupes de technologies ont été développés à cet effet. La première est basée sur la protection du contenu par chiffrement. Dans ce groupe, le déchiffrement correct des données nécessite une clé. Le deuxième groupe fonde la protection sur le tatouage numérique ou la dissimulation des données, visant à intégrer secrètement un message dans les données. Afin de ne pas augmenter le temps de traitement, ces deux approches doivent être combinées avec l'étape de compression. De nos jours, le défi consiste à effectuer simultanément par exemple le chiffrement et la compression des images.

Les travaux présentés dans ce tutoriel[32] démontrent comment les algorithmes de chiffrement permettent de sécuriser l'imagerie médicale. L'objectif principal est de garantir la protection des images médicales lors de leur transmission, mais également une fois ces données numériques archivées. Le défi qui s'ensuit est de s'assurer qu'un tel codage résiste à des traitements sévères tels que la compression.

- une nouvelle méthode de crypto-filigrané pour le transfert sécurisé d'images médicales.
- une nouvelle méthode réversible rapide pour le transfert sécurisé des images.
- une méthode réversible de masquage des données pour les images cryptées.

✓ **Avantages :** Cette méthode est particulièrement adaptée aux images médicales où l'on peut associer le diagnostic du patient à l'image médicale concernée à des fins de transfert en toute sécurité . Les mots clés de ce travail sont la transmission d'images rapide et sûre, la compression sans perte, le masquage réversible des données, le cryptage partiel, la protection des images et le traitement des images en temps réel.

2.3 Conclusion

Ces méthodes et les travaux présentés se sont heurtés à de nombreux obstacles et inconvénients qui ont conduit à de mauvaises performances, parmi lesquels le manque de sécurité et de fiabilité requis, en plus de la difficulté d'assurer la confidentialité des messages, c'est pourquoi nous a proposé un nouveau travail dans le monde de l'informatique, qui est la protection des images médicales asymétriques de manière Algorithmique MNF-G qui offre un pourcentage élevé de sécurité, de confidentialité et de fiabilité par rapport aux travaux que nous avons vus précédemment. Dans cette section, nous avons précisé certains des travaux antérieurs présentés en matière de protection des images médicales, et mentionné les avantages et les inconvénients de chaque travail.

CHAPITRE 3

LA MÉTHODE PROPOSÉE

3.1 Introduction

Dans ce chapitre, nous présentons la méthodologie sur laquelle le système est basé, en commençant par mettre en évidence le schéma général et les éléments de base du système, puis en discutant de chaque partie de ce schéma.

3.2 Schéma global

Cette section propose un schéma de chiffrement qui vise à fournir un schéma sécurisé et robuste sans limites Le nombre d'opérations d'addition et de multiplication est homogène. Le processus de cryptage est déclenché en incluant l'image médicale originale qui sera traitée dans le système, elle est lue, puis l'algorithme cryptographique (MNF-G) est appliqué à l'image Ventsal cryptée et c'est la première étape du processus. La deuxième étape consiste à décoder la scène appliquée à l'image obtenue grâce à l'algorithme de décodage, nous montrant l'image décodée.

3.2.1 MNF-G

Fragmentation des nombres magiques et cryptage El-Gamal (MNF-G) ; pour commencer, l'image brute est convertie en blocs de bits ; puis, en décimal ; enfin, l'image brute bien être chiffrée ces blocs par l'algorithme MNF-G. Le résultat expérimental montre que l'algorithme proposé peut chiffrer/déchiffrer avec succès des images et qu'il a un bon effet de chiffrement. L'image cryptée développée par ce système sera entièrement différente par rapport au fichier image d'origine et conviendra à la transmission sécurisée sur Internet [33].

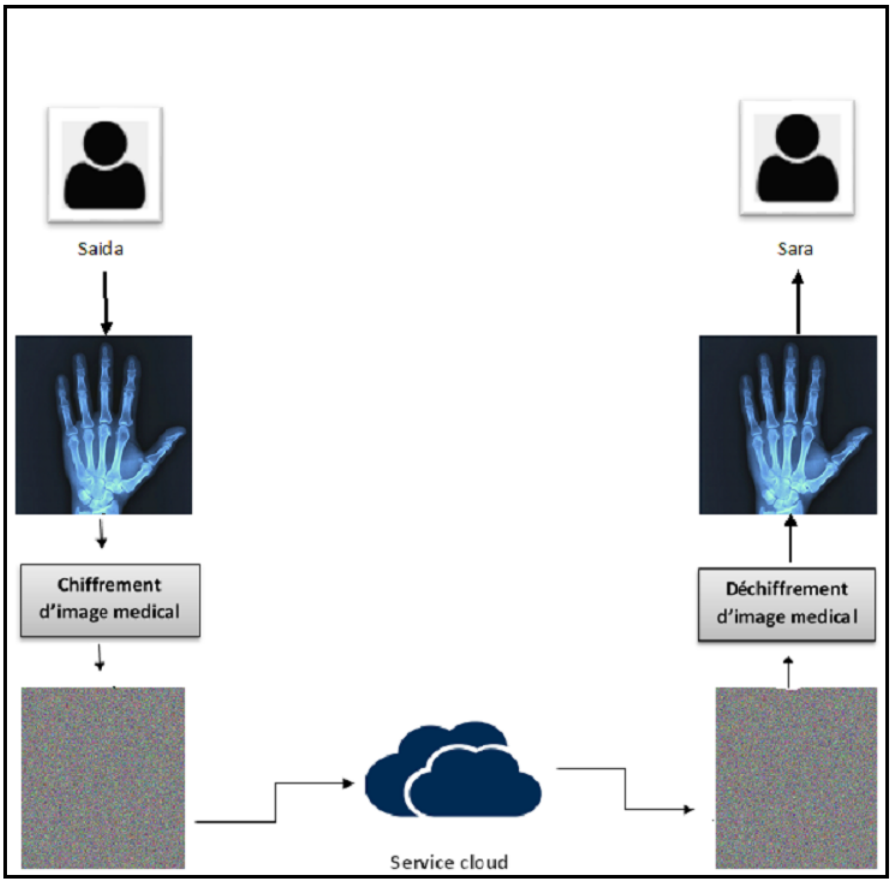


FIGURE 3.1 – La protection d'une image

3.3 Schémas partiels et leur explication

3.3.1 L'image originale

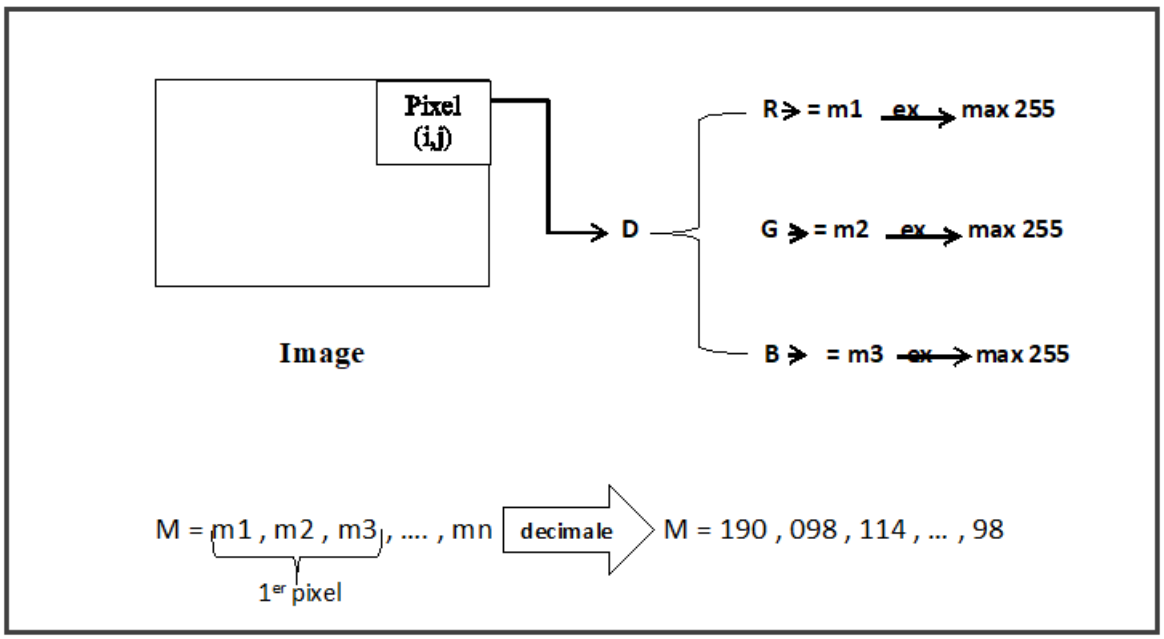


FIGURE 3.2 – Diagramme montrant comment lire les données d'image.

L'image est un ensemble de pixels dans une surface bidimensionnelle, chaque pixel est disposé et traité séquentiellement en lisant et en convertissant la valeur de chaque pixel du système décimal au système binaire.

3.3.2 Algorithme de cryptage

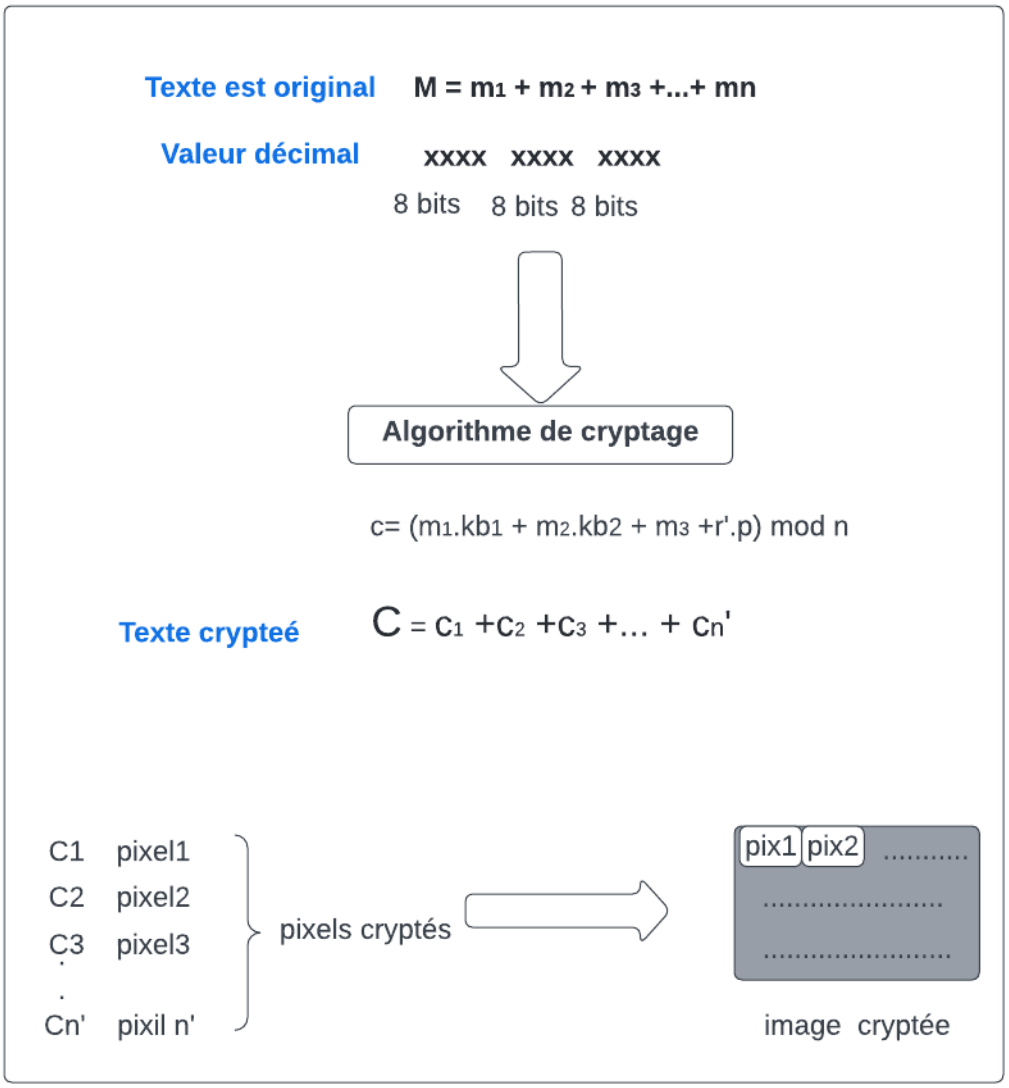


FIGURE 3.3 – Graphique montrant comment décrypter chaque pixel.

Le cryptage asymétrique du système proposé permet à Alice d'envoyer un texte chiffré à Bob en utilisant la clé publique partagée, qui fonctionne comme indiqué $pk = k + r \times p$ et le cryptage de $c = (m' + m'' \times pk) \mod n$, i.e., $c = m' + m'' \times (k + r \times p) = m' + m'' \times k + r' \times p$. $m' < p \rightarrow c \mod p = m' + (m'' \times k) \mod p$ et $m'' < p \rightarrow (m'' \times k \times k^{-1}) \mod p = m''$

Pour obtenir l'image cryptée, chaque nouveau pixel qui a été calculé à partir de l'algorithme de cryptage doit être remplacé et chaque nouveau pixel est placé à sa place, nous atteignons donc le résultat souhaité, qui est une image cryptée.

3.3.3 Algorithme de décryptage

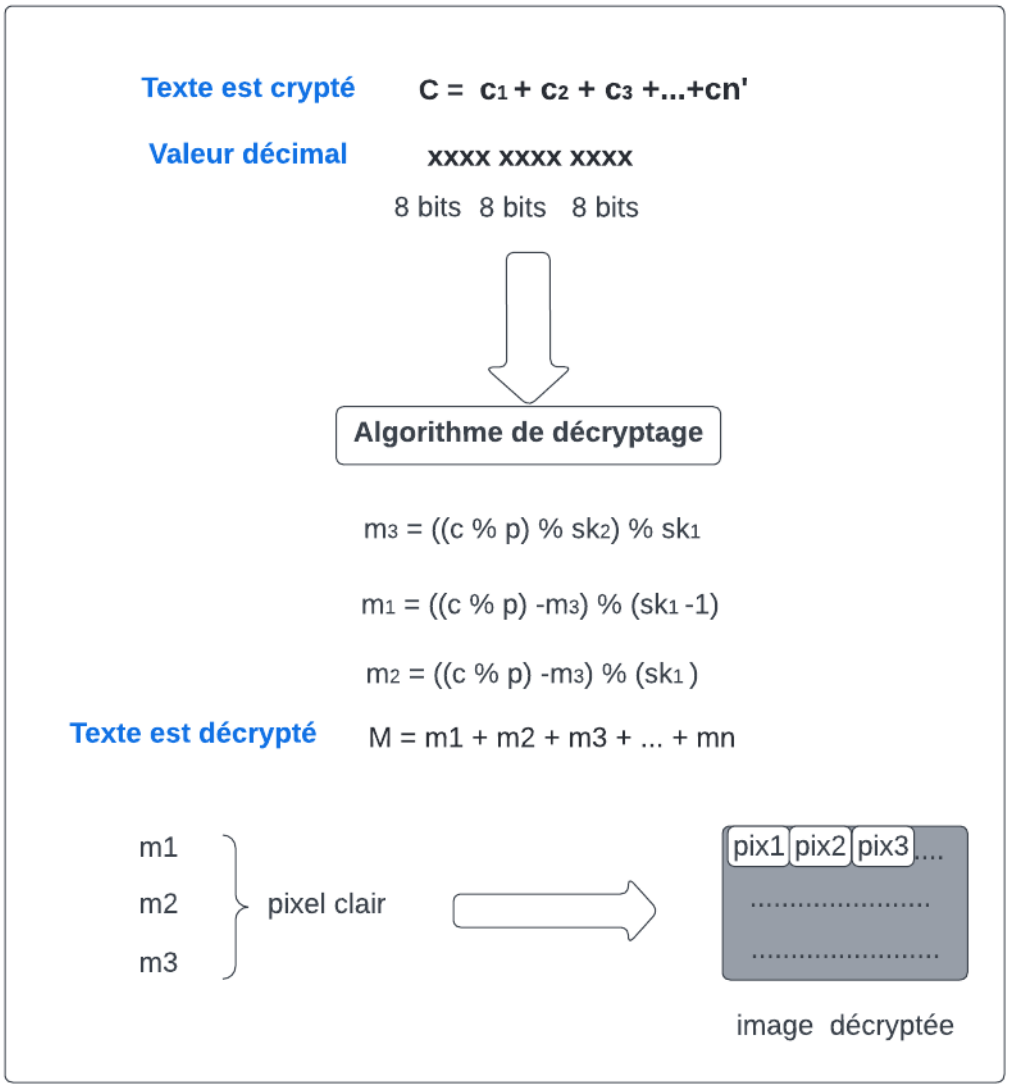


FIGURE 3.4 – Algorithme decryptage.

$c = (c_+, c_\times)$ et $c_+ = m' + m'' \times k + r \times p$. Dans un premier temps, nous extrayons m de c_+, puisque $m \times k < p$. Alors $c_+ \mod p = m' + m'' \times k$ car $r \times p \mod p = 0$ et depuis $m \times k \mod (k-1) = m$ alors $Dec(c_+) = m$.

3.3.4 Image decrypte

Mais à ce stade, après avoir obtenu l'image cryptée, elle doit être décryptée via l'algorithme de décryptage, donc notre résultat sera une image décryptée, qui est très similaire à l'image originale, et nous aborderons cette partie, qui est la rapport de similarité dans le dernier chapitre.

3.4 La méthode de chiffrement par fragmentation

Cette section propose un schéma de chiffrement qui vise à fournir un schéma sécurisé et robuste sans limites Le nombre d'opérations d'addition et de multiplication est homogène. La technique monolithique proposée peut être conçue avec L'architecture de cloud computing illustrative illustrée à la figure ce qui suit est un schéma de codage linéaire conçu pour garantir une propriété d'addition homogène.

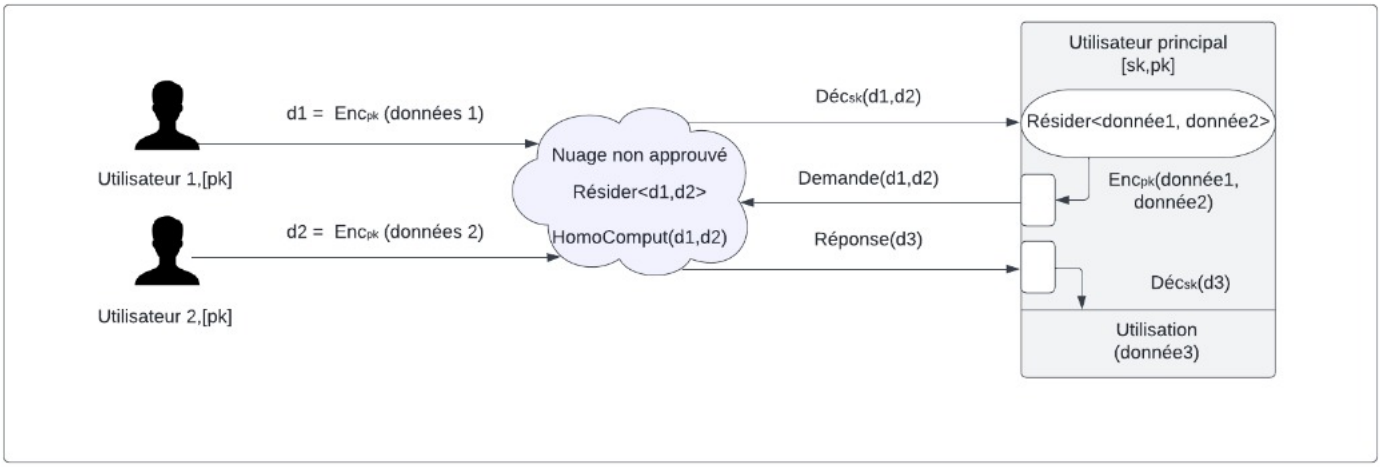


FIGURE 3.5 – L'architecture de cloud computing proposée

Nous nous concentrons sur la façon de fournir un codage linéaire asymétrique cela réduira et accélérera le temps de cryptage et maintiendra le cryptage fort et sécurisé contre les attaques. nous Commencez l'explication du diagramme proposé avec la notation périodique linéaire suivante :

$$c = (m + r \times p) \mod n \tag{3.1}$$

Où $n = p \times q$. La faiblesse de l'équation (1) est sujette à une attaque de texte brut connue. Pour faire face à cette faiblesse et autre type d'attaques, nous introduisons à l'équation (1) quelques améliorations comme suit :

$$c = (m \times k + r \times p) \mod n \tag{3.2}$$

En fait, c'est l'origine du mode de cryptage El-Gamal [5]. Néanmoins, Equation (3.2) est encore faible car lorsque quelqu'un peut obtenir deux textes bruts, il pourra récupérer p puis obtenir toutes les autres entités chiffrées. L'objectif principal du schéma de chiffrement proposé est de masquer le texte brut avant d'utiliser Equation 3.2 en fragmentant aléatoirement m en deux parties m' et m'' tels que $m = m' + m''$ de sorte qu'il devient difficile pour un attaquant de

retrouver les m' et m'' utilisés dans le but d'extraire p. Par conséquent, l'équation de chiffrement proposée sera la suivante :

$$c = (m' + m'' \times k + r \times p) \mod n \tag{3.3}$$

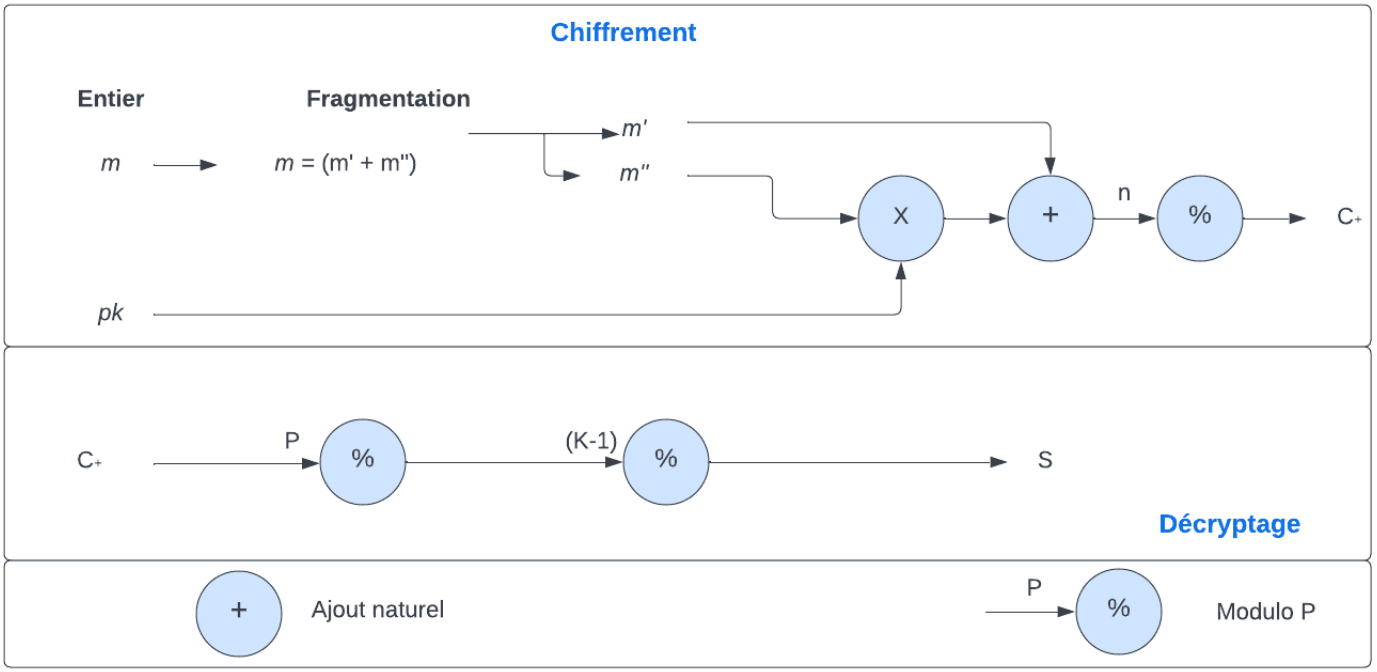


FIGURE 3.6 – Propriété homomorphe

— P est l'anneau du texte brut $\mathbb{Z}_p$

— C est l'anneau de texte crypté $\mathbb{Z}_n$

— K est le porte-clés

— $Enc()$ est la fonction de cryptage $Enc_{pk} : P \longrightarrow C$ with $pk \in K$

— $Dec()$ est la fonction de déchiffrement $Dec_{sk} : C \longrightarrow P$ avec $sk \in K$

3.5 Conclusion

Dans ce chapitre, nous avons présenté un schéma illustrant la méthodologie de traitement des images médicales par le système. L'application de l'algorithme décrit dans ce chapitre et la présentation des résultats expérimentaux font l'objet du chapitre suivant.

CHAPITRE 4

IMPLÉMENTATION ET ANALYSE

4.1 Introduction

Après le troisième chapitre, dans lequel nous avons discuté en détail de la proposition de l'algorithme, maintenant dans ce chapitre nous nous appuierons sur l'application de l'algorithme et la création d'une application qui simule les étapes en détail. Puis nous effectuons une série d'analyses des résultats afin de vérifier la force et la rents critères A travers un ensemble de critères.

4.2 Environnement de développement

Un aperçu du matériel utilisé dans le développement d'applications, l'analyse et le suivi des résultats. Il contient l'environnement logiciel (Software) et matériel(Hardware) utilisés.

4.2.1 Environnement logiciel

Nous utilisions l'environnement Python pour exécuter des fichiers notre approche. Python est un langage de programmation interprété et Plate-forme multiple. Il encourage la programmation déterministe structurée, fonctionnelle et orientée objet. Il propose une écriture dynamique puissante et une gestion automatique de la mémoire via la récupération de place du système et la gestion des exceptions. Nous avons utilisé Python dans notre projet pour le traitement et le codage d'images car il Riche en bibliothèques prêtes à l'emploi qui facilitent le processus de programmation pour que nous nous concentrions davantage sur l'idée du projet. Voici quelques bibliothèques de traitement d'image pratiques et librement disponibles en Python que nous avons utilisées dans un fichier de projet : Numpy, SciPy, Matplotlib, PIL/Pillow, OpenCV et Scipy.

4.2.2 Environnement matériel

FIGURE 4.1 – Caractéristiques de l'ordinateur sur lequel nous avons travaillé le projet de fin d'études.

4.2.3 Critères d'évaluation

Un bon système de cryptage doit résister à toutes sortes d'attaques connues, il existe donc des simulations numériques qui ont été réalisées à l'aide de différentes mesures d'évaluation pour montrer la sécurité et l'efficacité de l'algorithme proposé. Nous présenterons les plus importants comme : l'espace clé, l'histogramme, l'entropie, la corrélation entre pixels adjacents.

Espace de clés

Un bon algorithme de chiffrement doit être sensible aux clés de chiffrement et l'espace clé doit être suffisamment grand pour rendre les attaques de force brute impossibles. La clé utilisée dans notre schéma est des nombres pseudo aléatoires qui été généré par les paramètres R,G,B la taille de la clé secrète est dépende par La taille de la clé secrète dépend de la taille de chaque composant de la clé, comme chacun, alors chaque élément dans les nombres pseudo aléatoires est codé sur 24 bits.

```
Espace de clés :

max_M1 = 256
max_M2 = 256
max_M3 = 256

rk = random > 256

k1 = random > 1000

k2 = max_M1*k1 + rk

min = max_M1*k1+max_M2*k2+max_M3 + 1

max = (max_M1*k1+max_M2*k2+max_M3)*1000

kb1 = k1+r*p

kb2 = k2+r*p
```

FIGURE 4.2 – pseudo-code illustre les intervalles des valeurs des variables.

La valeur maximale de chaque M est 256, le K1 il prend une valeur aléatoire là où il est supérieur à 1000, $K2 = Max\_M1 * K1 + rk$ tel que rk il prend une valeur aléatoire là où il est supérieur à 256.

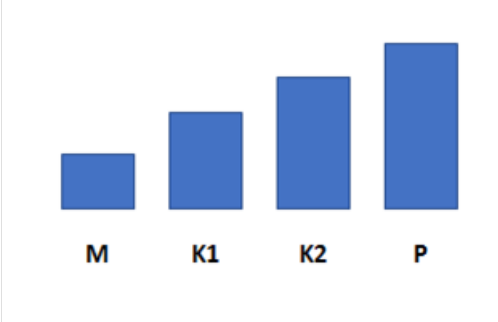
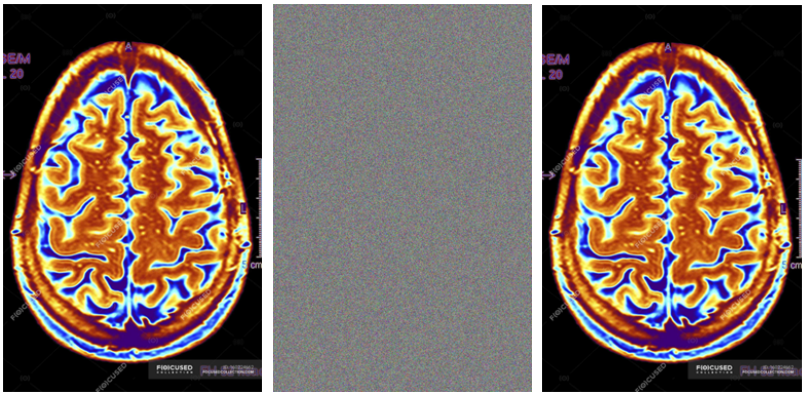


FIGURE 4.3 – Une illustration montrant la taille des variables impliquées dans l'espace de clé



Une illustration montrant les étapes de chiffrement et de déchiffrement d'images pour qu'au stade du cryptage, l'image soit téléchargée dans le cloud pour être stockée ou partagée.

4.2.4 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.

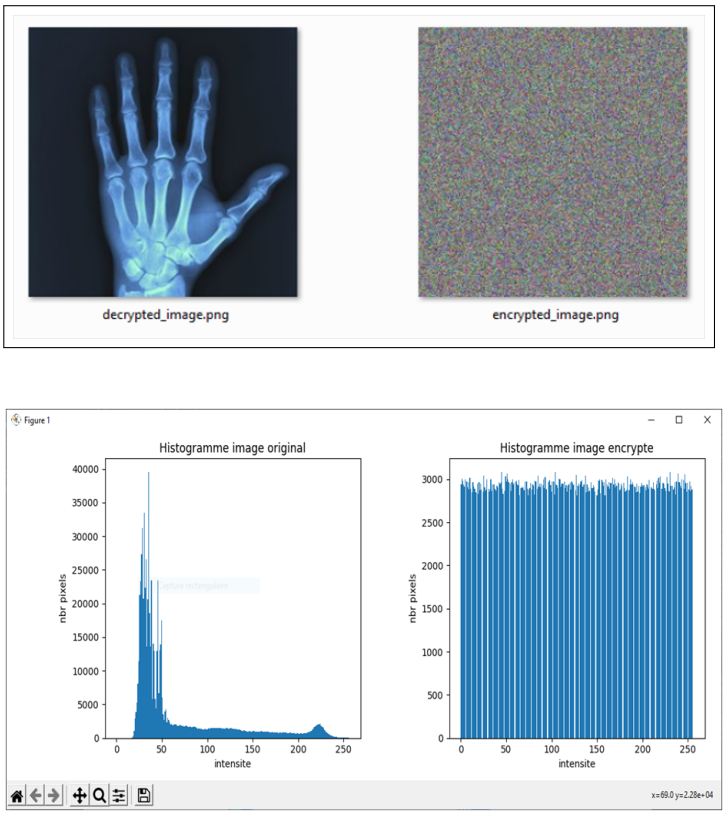


FIGURE 4.4 – Une comparaison entre l'histogramme d'une image originale et une image cryptée.

Nous pouvons clairement remarquer que l'histogramme des images cryptées a une distribution uniforme des valeurs de pixels (tous les pixels ont la même chance d'apparition), ceci est prouvé que le système proposé n'est pas vulnérable à l'attaque d'histogramme.

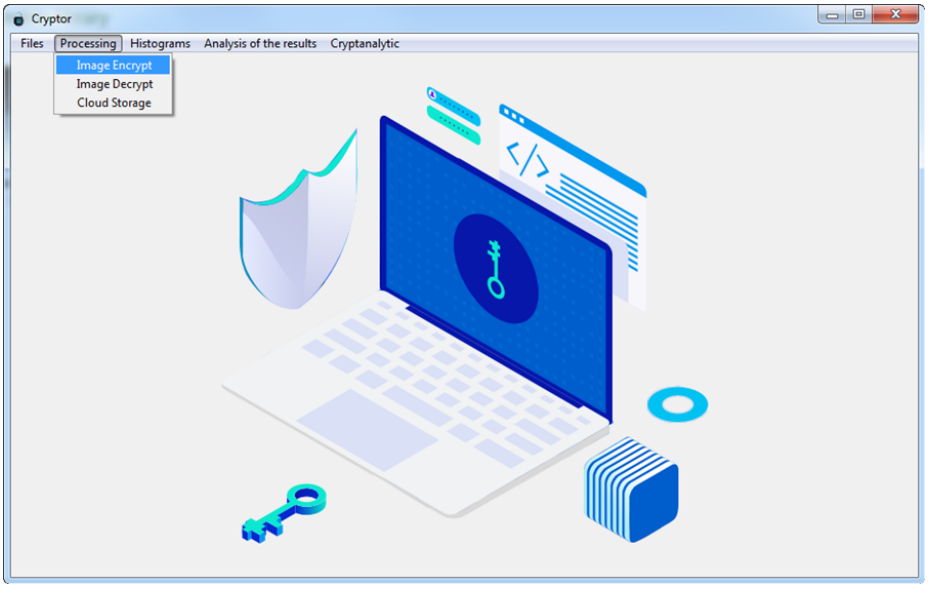


FIGURE 4.5 – L'interface principale de l'application

L'interface principale de l'application, qui comprend de nombreuses opérations de base, qui comprend le cryptage, le décryptage et l'upload d'images dans le cloud et un ensemble d'analyses pour les résultats.

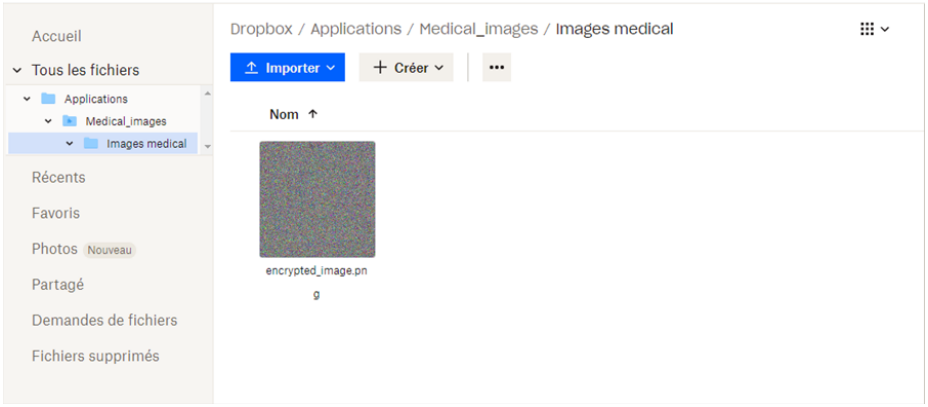


FIGURE 4.6 – figure montre l'upload image cryptée vers le cloud

Cette image montre l'uploadvers le sauvgarde en cloud de manière sécurisée, car il est crypté afin de s'assurer que nos données sont strictement confidentielles vis-à-vis du fournisseur tiers du service cloud.

Parce que l'application finale dépend principalement des services cloud pour stocker les données d'une part ou via le processus d'échange, Une explication simple du processus d'échange ou de stockage entre chacun des médecins et l'établissement ou entre médecins et autres médecins, ici le processus de protection des données est très efficace.

4.2.5 Entropie

L'entropie est une mesure statistique du hasard dans la théorie de l'information. 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 le tableau suivant :

Images de test	**Image en clair**	**Image en Cryptée**
Image médical 1	6.528	7.999
Image médical 2	7.6435	7.9958
Image médical 3	7.358	7.9961
Image médical 4	7.1307	7.9981

TABLE 4.1 – Un tableau décrivant l'entropie de différentes images

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.

4.2.6 Analyse de sensibilités

Le nombre de taux de pixels changeants **(NPCR)** et l'intensité modifiée moyenne unifiée **(UACI)** sont deux tests standardisés utilisés pour examiner la sensibilité d'une image simple-contre une attaque différentielle. La représentation mathématique des tests NPCR et UACI est présentée comme suit [34] :

Le nombre de taux de pixels changeants

$$\boxed{\mathbf{NPCR} = \frac{\sum C(i,j)}{N*M}}$$

l'intensité modifiée moyenne unifiée

$$\boxed{\mathbf{UACI} = \sum \frac{|C_1(i,j)-C_2(i,j)|}{255*N*M}}$$

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 :

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

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.
Un bon système de cryptage doit avoir une valeur de NPCR > 99.6094% et un UACI >36.91%, ce qui est assuré par notre système.

PSNR

PSNR (Peak Signal to Noise Ratio), c'est une mesure de distorsion utilisée en image numérique, est calculé à l'aide de l'erreur quadratique moyenne (EQM) qui devrait idéalement être aussi faible que possible pour un déchiffrement sans perte [34]. Le PSNR est calculé comme suit :

Peak Signal to Noise Ratio

$$\boxed{PSNR_{dB} \; = 10 \log_{10} \; (\tfrac{L_2}{EQM})}$$

où d est la dynamique du signal. Dans le cas standard d'une image où les composantes d'un pixel sont codées sur 8 bits, d = 255.

EQM est l'erreur quadratique moyenne et est définie pour 2 images Io et Ir de taille m×n comme :

$$\textbf{EQM} \; = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (||I_0(i,j) - I_r(i,j)||^2)$$

Les valeurs typiques de PSNR pour des images de bonne qualité fluctuent entre 30 et 40 dB.
Si le PSNR est utile pour mesurer la proximité de l'image compressée comparé à l'original au niveau du signal, il ne prend pas en compte la qualité visuelle de reconstruction et ne peut être reconnu comme une mesure objective de la qualité visuelle d'une image.
La valeur PSNR d'une image médical claire et la même image est cryptée est : **7.187** Dans la même formulation, nous avons calculé la valeur PSNR d'une image médical claire et de la même image après le décryptage, nos résultats montrent que le taux de distorsion entre l'image originale et l'image cryptée est complètement différant. Dans le cas de l'image originale et de l'image décryptée, le résultat est que les deux images sont identiques, donc l'erreur moyenne

quadratique est nulle.

SSIM

Le SSIM (Structural Similarity Index) est un modèle basé sur la perception qui considère ladégradation de l'image comme un changement perçu dans les informations structurelles, tout en intégrant également des phénomènes perceptifs importants, y compris des termes de masquagede luminance et de masquage de contraste et contours. Les informations structurelles sont l'idéeque les pixels ont de fortes interdépendances, en particulier lorsqu'ils sont spatialement proches.

Ces dépendances contiennent des informations importantes sur la structure des objets dans lascène visuelle [35].

La formule de calcul de la méthode et le suivant :

Structural Similarity Index

$$SSIM_{(x,y)} = \frac{(2\mu_x\mu_y + c_1)(2\sigma + c_2)}{(2\mu_x^2\mu_y^2 + c_1)(2\mu_x^2\mu_y^2 + c_2)}$$

La valeur SSIM de l'image d'origine est affichée dans le logiciel, et la même image est encodée : **0,009** signifie que les trois paramètres de luminosité, de contraste et de contour sont tous très différents.

La valeur : **1,0** pour l'image d'origine et la même image après décodage, ce qui signifie que les deux images sont identiques en termes de luminosité, de contraste et de contour.

Tailles images

Nous avons crypté et décrypté un ensemble d'images et enregistré leurs tailles avant et après le processus de cryptage. Le tableau suivant montre ces valeurs :

Images de test	Image original	Image Crypté	Image Décrypté
Image médical 1	168 ko	733 ko	171 ko
Image médical 2	541 ko	2.29 Mo	580 ko
Image médical 3	306 ko	1.71 Mo	334 ko
Image médical 4	673 ko	1.57 Mo	676 ko
Image médical 5	859 ko	2.32 Mo	861 ko

TABLE 4.2 – Un tableau décrivant l'entropie de différentes tailles images

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.
Quant aux images après le décryptage et aux images originalesla taille est presque égale.

4.3 Conclusion

Dans ce chapitre, nous avons présenté notre implémentation de l'algorithme proposé et les différents outils utilisés dans son développement. Nous avons également réalisé un ensemble d'analyses et de tests de résultats empiriques qui montrent la résistance de notre algorithme de chiffrement.
Selon notre analyse de la proposition, il a un haut niveau de sécurité contre divers types d'attaques. Ainsi, l'analyse prouve l'innocuité et l'efficacité.

CONCLUSION GÉNÉRALE

dans la littérature, la nature de la sécurité du cloud a conduit les chercheurs à faire face à la question de l'homomorphisme. De nombreux pro- les schémas homomorphes posés émettent un bruit hautement randomisé lors des opérations homomorphes, en raison de génération de bruit. En fait, peu de schémas proposés sont pratiques à exécuter sur des cryptogrammes. Au vu du visage défis homomorphes, nous avons préféré dans cet article rechercher un schéma de chiffrement léger. MNF-G intro- FHE basé sur la fragmentation des nombres magiques et le cryptage El-Gamel crée un nouveau terme dans la cryptographie asymétrique où la fragmentation offre un cryptage linéaire pour permettre d'effectuer homomorphie pratique sur les entiers, ce chiffrement est adapté aux caractéristiques des villes intelligentes. Les premières analyses et résultats montrent sa faisabilité et son efficacité par rapport aux autres schémas proposés. Comme travaux futurs, nous avons l'intention faire une étude approfondie pour implémenter MNF-G dans un environnement IoT

BIBLIOGRAPHIE

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[2] D. E. Standard *et al.*, "Data encryption standard," *Federal Information Processing Standards Publication*, vol. 112, 1999.

[3] R. P. Adhie, Y. Hutama, A. S. Ahmar, M. Setiawan *et al.*, "Implementation cryptography data encryption standard (des) and triple data encryption standard (3des) method in communication system based near field communication (nfc)," in *Journal of Physics : Conference Series*, vol. 954, no. 1. IOP Publishing, 2018, p. 012009.

[4] E. BENSIKADDOUR *et al.*, "Développement d'un crypto-système basé sur le standard aes et la théorie du chaos pour le chiffrement des images satellitaires à bord d'un satellite d'observation de la terre." Ph.D. dissertation, 2019.

[5] N. Mati, D. Laouar *et al.*, "Cryptage d'images médicales," Ph.D. dissertation, University of Jijel, 2020.

[6] R. Caloz and C. Collet, *Précis de télédétection-Volume 3 : Traitements numériques d'images de télédétection.* PUQ, 2001, vol. 3.

[7] J. Sachs, "Digital image basics," *Digital Light & Color*, vol. 1996, 1999.

[8] J.-L. Peyron, "Lexique," *Revue forestière française*, vol. 45, no. S, pp. 243–254, 1993.

[9] G. Damiand, "Définition et étude d'un modèle topologique minimal de représentation d'images 2d et 3d," Ph.D. dissertation, Université Montpellier II-Sciences et Techniques du Languedoc, 2001.

[10] A. Aimeur, "Conception et implémentation d'un système hybride pour la sécurité de données : application aux images numériques," Ph.D. dissertation, FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE DEPARTEMENT D'INFORMATIQUE, 2017.

[11] F. Jeannot, "Vectorisation stylisée de dessins d'un manuscrit copte du 14e siècle par algorithme de tracing."

[12] G. Demésy, "Modelisation electromagnetique tri-dimensionnelle de reseaux complexes. application au filtrage spectral dans les imageurs cmos." Ph.D. dissertation, Université Paul Cézanne-Aix-Marseille III, 2009.

[13] S. Moussa, "Image denoising : étude comparative des méthodes de filtrage d'image."

[14] M. A. C. Chenikhar, "Contribution à l'analyse et la reconaissance des plaques d'immatriculation algériennes," Ph.D. dissertation, Universite laarbi tebessi tebessa, 2019.

[15] C. Ngô, "Chapitre 8 codage source," in *Énergie, entropie, information, cryptographie et cybersécurité*. EDP Sciences, 2021, pp. 109–128.

[16] A. Jankowski and G. Ferretti, "Tomodensitométrie volumique : principe, paramètres," *Revue des maladies respiratoires*, vol. 27, no. 8, pp. 964–969, 2010.

[17] B. Kastler, P. Anstett, B. Kastler, and D. Vetter, *Comprendre l'IRM*. Elsevier, 2011.

[18] E. Liozon, J. Monteil, K. Ly, and E. Vidal, "Place de la tomographie par émission de positrons (tep) au [18f] fdg dans l'exploration et la surveillance des vascularites," *La Revue de médecine interne*, vol. 31, no. 6, pp. 417–427, 2010.

[19] M. Gesnik, "Imagerie fonctionnelle par ultrasons de la rétine et des fonctions visuelles cérébrales," Ph.D. dissertation, Paris Sciences et Lettres (ComUE), 2017.

[20] E. Payot, "Reconstruction vasculaire tridimensionnelle en imagerie par rayons x," Ph.D. dissertation, Paris, ENST, 1996.

[21] A. Mourad, "Crypto compression d'image par cryptage partiel," Ph.D. dissertation, Université Mouloud Mammeri, 2015.

[22] V. Pavithra and C. Jeyamala, "A survey on the techniques of medical image encryption," in *2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*. IEEE, 2018, pp. 1–8.

[23] H. Liu, A. Kadir, and X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," *IET Image Processing*, vol. 11, no. 5, pp. 324–332, 2017.

[24] C. Fu, Z.-f. Chen, W. Zhao, and H.-y. Jiang, "A new fast color image encryption scheme using chen chaotic system," in *2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*. IEEE, 2017, pp. 121–126.

[25] C. Zhang, J. Wang, and X. Wang, "Digital image watermarking algorithm with double encryption by arnold transform and logistic," in *2008 Fourth International Conference on Networked Computing and Advanced Information Management*, vol. 1. IEEE, 2008, pp. 329–334.

[26] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using dna sequence operations," *Optics and Lasers in engineering*, vol. 88, pp. 197–213, 2017.

[27] K. Radhika and M. Nalini, "Biometric image encryption using dna sequences and chaotic systems," in *2017 International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT)*. IEEE, 2017, pp. 164–168.

[28] W. Zheng, F.-Y. Wang, and K. Wang, "An acp-based approach to color image encryption using dna sequence operation and hyper-chaotic system," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, 2017, pp. 461–466.

[29] K. Shankar, M. Elhoseny, E. D. Chelvi, S. Lakshmanaprabu, and W. Wu, "An efficient optimal key based chaos function for medical image security," *IEEE Access*, vol. 6, pp. 77 145–77 154, 2018.

[30] G. Ye, H. Wu, K. Jiao, and D. Mei, "Asymmetric image encryption scheme based on the quantum logistic map and cyclic modulo diffusion," *Mathematical Biosciences and Engineering*, vol. 18, no. 5, pp. 5427–5448, 2021.

[31] M. Sokouti, A. Zakerolhosseini, and B. Sokouti, "Medical image encryption : an application for improved padding based ggh encryption algorithm," *The open medical informatics journal*, vol. 10, p. 11, 2016.

[32] W. Puech, "Image encryption and compression for medical image security," in *2008 First Workshops on Image Processing Theory, Tools and Applications*. IEEE, 2008, pp. 1–2.

[33] M. E. Kahla, M. Beggas, A. Laouid, M. Kara, and M. AlShaikh, "Asymmetric image encryption based on twin message fusion," in *2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP)*, 2021, pp. 1–5.

[34] U. Sara, M. Akter, and M. S. Uddin, "Image quality assessment through fsim, ssim, mse and psnr—a comparative study," *Journal of Computer and Communications*, vol. 7, no. 3, pp. 8–18, 2019.

[35] D. Slezak, M. Szczuka, I. Duentsch, and Y. Yao, *Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing : 10th International Conference, RSFDGrC 2005, Regina, Canada, August 31-September 3, 2005, Proceedings, Part I.* Springer, 2005, vol. 3641.