République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université 8Mai 1945 – Guelma
Faculté des Sciences et de la Technologie
Département d'Electronique et Télécommunications

Mémoire de Fin d'Etude

Pour l'Obtention du Diplôme de Master Académique

Domaine : **Sciences et Techniques**

Filière : **Télécommunications**

Spécialité : **réseaux de Télécommunications**

Etude et simulation d'un crypto-système basé sur l'algorithme AES-GCM : Application au cryptage des images médicales

---

Présenté par :

MOUSSAOUI Lina

CHOUAICHIA Safa

Sous la direction de :

Dr. BOUKHAROUBA Abdelhak

Juin 2023

Remerciements

Avant toute chose, nous rendons grâce à Allah le tout puissant qui nous a fait ouvrir les portes du savoir, qui nous a donné le courage, la volonté, la force nécessaire durant tout notre cursus pédagogique. Notre profonde gratitude à nos parents pour leur soutien moral indéfectible. Nous tenons à remercie notre encadreur Dr boukharouba Abdelhak, pour son aide, ses conseils, et ses orientations pour l'accomplissement de ce mémoire. Nous remercions également les membres du jury qui nous ont honorés en acceptant l'invitation d'évaluer ce modeste travail. Enfin, nous tenons à exprimer notre reconnaissance à tous nos amis et collègues pour le soutien moral et matériel.

Dédicace

J’aimerais dédier ce travail à mes très chers parents ; pour leurs amour, confiance, compréhension et patience envers moi. Je ne pourrai jamais assez-vous remercier

A mes chers frères : Ammar et Mohammed pour leur présence dans ma Vie pour leurs encouragements permanents, et leur soutien moral

A ma chère tante Karima qui m’a toujours était là pour moi

A mon binôme Safa qui m’a toujours encouragé durant la réalisation de ce mémoire

A mes chères amies (Amani, Wissal, Ahlem, soumia, Malak)

A tous mes enseignants qui ont fait leurs possibles Pour nous Donner le maximum d’informations Concernant notre étude

Lina

Dédicace

J’aimerais dédier ce travail à mes très chers parents ; pour leurs amour, confiance, compréhension et patience envers moi. Je ne pourrai jamais assez-vous remercier

A mes chères sœurs : Hassina, Meriem, marwa, Hawa, Lina, Yasmine et sirine pour leur présence dans ma Vie pour leurs encouragements permanents, et leur soutien moral

A ma cher frère Ahmed qui m’a toujours était là pour moi

A mon binôme Lina qui m’a toujours encouragé durant la réalisation de ce mémoire

A mes chères amies (Wissal, Ahlem, soumia,lidia ,assma)

A tous mes enseignants qui ont fait leurs possibles Pour nous Donner le maximum d’informations Concernant notre étude

Safa

Résumé

Grâce aux avancées technologiques dans les techniques de transmission, la communication est désormais capable de transmettre des informations importantes, y compris des images, qui nécessitent un système de transmission et de protection robuste. Dans ce mémoire, nous présentons un système de transmission d'images médicales basé sur un cryptosystème utilisant la méthode AES-GCM.

Enfin, nous présentons les résultats expérimentaux, y compris les tests statistiques, qui démontrent l'efficacité de notre méthode.

تلخيص

بفضل التقدم التكنولوجي في تقنيات الإرسال، أصبح الاتصال الآن قادرًا على نقل المعلومات المهمة، بما في ذلك الصور، والتي تتطلب نظام نقل وحماية قوي. في هذه الأطروحة، نقدم نظامًا لنقل الصور الطبية يعتمد على نظام تشفير باستخدام طريقة AES-GCM.

أخيرًا، نقدم النتائج التجريبية، بما في ذلك الاختبارات الإحصائية، والتي توضح فعالية طريقتنا.

Table des matières

Chapitre II : Cryptage des images médicales par la technique AES-GCM.

Chapitre III : Résultats de simulation

Liste des figures

Liste Des Tableaux

Liste des abréviations

AAD : Les données supplémentaires d'authentification (AAD)

Bit : Un chiffre binaire : 0 ou 1.

Octet : Une séquence de 8 bits.

RBG : Random Bit Generator

OU exclusif (XOR) : L'addition bit à bit, modulo 2, de deux chaînes de bits de même longueur.

ICB : Bloc de compteur initial

IV (Initialization Vector) : Vecteur d'initialisation

AES : Standard de chiffrement avancé.

DSS : Norme de signature numérique.

DES : Standard de signature numérique.

GCM :(Galois Counter mode) Mode de compteur de Galois.

RC4 : Chiffrement de Rivest 4.

ECB : Mode de chiffrement en bloc électronique.

CBC : Mode de chiffrement par blocs avec chaînage.

OFB : Rétroaction de sortie.

CFB : Rétroaction de chiffrement.

JPEG : Groupe d'experts en photographie jointe.

TIFF : Format de fichier d'image balisée.

GIF : Format d'échange d'images.

PNG : Graphique en réseau portable.

NPCR : Taux de changement normalisé des pixels.

UACI : Intensité Moyenne de Changement Unifiée.

Introduction générale

Introduction

Depuis des temps immémoriaux, les êtres humains ont cherché des moyens de transmettre des messages de manière confidentielle. Avec l'accélération fulgurante du développement des technologies de l'internet et de la communication, la transmission d'images en général, et d'images médicales en particulier, est devenue un élément clé de la diffusion de l'information. Dans le cadre de notre projet de fin d'études, nous nous concentrons sur la protection des images médicales.

Au fil de l'histoire, l'humanité a cherché à transmettre des informations de manière sécurisée. Le chiffrement de l'information a été utilisé comme outil de sécurité pour les stratégies militaires et les échanges de données confidentielles. De nos jours, le transfert sécurisé d'informations est nécessaire et largement utilisé dans le monde numérique. Les réseaux numériques ont connu une forte évolution ces dernières années et sont devenus indispensables pour la communication moderne. La transmission d'images soulève de nombreux problèmes, tels que la confidentialité, l'authentification et l'intégrité des données :

- Toute information circulante peut être capturée et lue « Sniffing », La confidentialité se base sur les concepts qui permettent de s'assurer que l'information ne puisse pas être lue par des personnes non autorisées. La confidentialité est fortement liée à la cryptographie.

- Une personne peut falsifier ses informations numériques personnelles « Spoofing », l'authentification est l'ensemble des moyens qui permettent d'assurer que les données reçues et envoyées proviennent bien des entités déclarées.

- Les données peuvent être capturées et modifiées, l'intégrité des données concerne les techniques qui rendent possible la vérification de la non-altération des données, c'est-à-dire le contrôle du contenu.

Ce mémoire s’articule autour de trois chapitres :

-Le premier chapitre représente généralité sur le cryptage de l’image.

-Le deuxième chapitre est basé sur le Cryptage des images médicales par la technique AES-GCM.

- Le troisième chapitre est consacré sur la simulation et les résultats.

Chapitre I :

Généralités sur le cryptage de l'image

I.1 Introduction

L'invention des techniques de chiffrement à clé publique a créé un véritable bouleversement dans le monde de la cryptographie, car elle a permis de chiffrer des données sans avoir besoin d'échanger un secret préalablement sécurisé, de produire une signature numérique pour identifier l'auteur d'un message, et même de jouer à pile ou face par téléphone. Cependant, malgré ces avancées, de nombreux problèmes demeurent sans solution et de nouveaux défis sont apparus à mesure que les progrès de l'informatique et les efforts des cryptanalystes ont permis de briser certains systèmes considérés comme sûrs auparavant. Aujourd'hui, les systèmes de chiffrement à clé publique qui résistent encore à la cryptanalyse sont très rares.

Aujourd'hui, la sécurité informatique est devenue une préoccupation majeure pour les professionnels de l'informatique. La plupart des développeurs se concentrent sur les techniques de cryptage pour garantir la sécurité des données. La cryptographie est devenue une science à part entière, combinant les mathématiques, l'informatique et parfois la physique. Elle est utilisée chaque fois que des données sensibles sont échangées.

Dans ce chapitre nous allons décrire le concept de la cryptographie et ses deux types : la cryptographie symétrique et asymétrique ainsi que les algorithmes de chiffrement les plus utilisés et connus.

I.2 Concepts de base

I.2.1 Définition de la cryptologie

La cryptologie est un mot composé qui tire son origine du grec : cryptos qui signifie secret et Logie qui signifie science. En fait, c'est la science du secret et ne peut être vraiment considérée ainsi que depuis peu de temps. Elle englobe la cryptographie, l'écriture secrète et la cryptanalyse, l'analyse de cette dernière. On peut dire que la cryptologie est un art ancien et une science nouvelle : un art ancien car Jules César l'utilisait déjà et il fit son apparition dans l'ancien testament sous la forme du code Atbash ; une science nouvelle parce que ce n'est que depuis les années 1970 qu'elle est devenue un thème de recherche scientifique. Cette discipline est liée à beaucoup d'autres, par exemple la théorie des nombres, l'algèbre, la théorie de la complexité, la théorie de l'information, ou encore les codes correcteurs [1].

I.2.2 Définition de La cryptographie

Le terme cryptographie vient en effet de deux mots grecs : Kruptus qu'on peut traduire comme secret et Graphein pour écriture. La cryptographie est l'art de cacher l'information pour qu'elle soit incompréhensible, elle désigne l'ensemble des techniques qui permettent de chiffrer les messages, son objectif principal est de permettre à deux personnes alice et Bob de communiquer à travers un canal peu sécurisé de telle sorte qu'un opposant Eve ne puisse pas comprendre ce qui est échangé, on utilise une clé appelée clé de chiffrement pour le processus de chiffrement. Pour rendre l'information à nouveau compréhensible on utilise une clé appelée clé de déchiffrement [2].

I.2.1 Terminologie

Les principaux termes utilisés dans la cryptographie sont :

Cryptologie : C'est une science mathématique regroupant la cryptographie et la cryptanalyse.

Cryptographie : La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer Des données de manière confidentielle sur un support donné.

Cryptogramme : Texte chiffré : Ciphertext : est le résultat de l'application d'un chiffrement d'un texte clair.

Texte clair : Plaintext : le message à chiffrer.

Chiffrement : la fonction permettant de transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et ainsi que le destinataire

Déchiffrement : la fonction permettant de retrouver le texte clair à partir du texte chiffré.

Clé : une clé est un paramètre utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement). On distingue généralement deux types de clefs :

Clés symétriques : il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou à clé secrète.

Clés asymétriques : il s'agit de clés utilisées dans le cas du chiffrement asymétrique ou à clé publique. Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement.

Cryptanalyse : Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.

Cryptosystème : un Cryptosystème est constitué d'un algorithme cryptographique ainsi que toutes les clés possibles et tous les protocoles qui le font fonctionner. Un modèle de cryptosystème est représenté sur la figure (I.1) [2] [3].

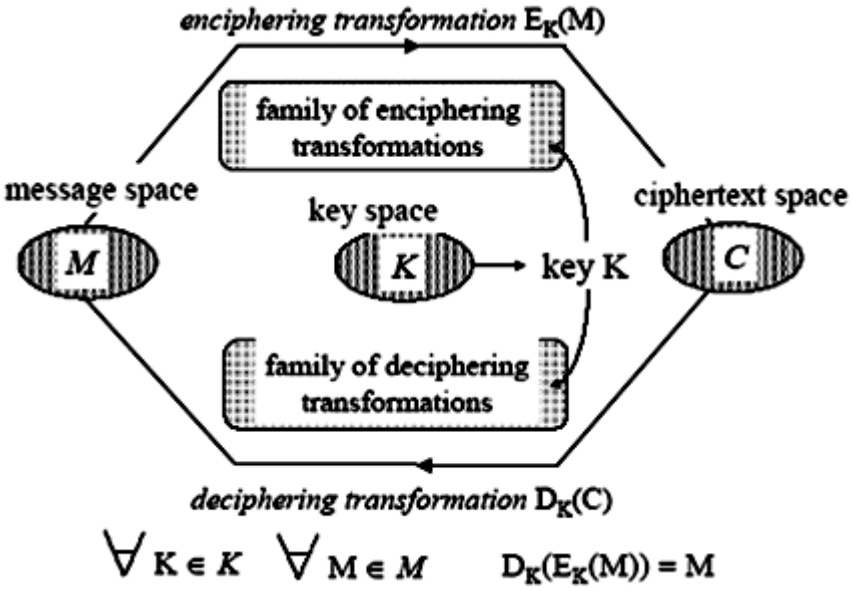


Figure I. 1 : Une représentation d'un Cryptosystème[4].

I.2.3-Cryptanalyse

La cryptanalyse est la technique qui consiste à déduire un texte en clair d'un texte chiffré sans posséder la clé de chiffrement. Le processus par lequel on tente de comprendre un message en particulier est appelé une attaque.

Une attaque est souvent caractérisée par les données qu'elle nécessite :

• Attaque sur texte chiffré seul (ciphertext-only en anglais) : le cryptanalyste possède des exemplaires chiffrés des messages, il peut faire des hypothèses sur les messages originaux qu'il ne possède pas. La cryptanalyse est plus ardue de par le manque d'informations à disposition.

• Attaque à texte clair connu (known-plaintext attack en anglais) : Le cryptanalyste possède des messages ou des parties de messages en clair ainsi que les versions chiffrées. La cryptanalyse linéaire fait partie de cette catégorie.

• Attaque à texte clair choisi (chosen-plaintext attack en anglais) : Le cryptanalyste possède des messages en clair peut créer les versions chiffrées de ces messages avec

l'algorithme que l'on peut dès lors considérer comme une boîte noire. La cryptanalyse différentielle est un exemple d'attaque à texte clair choisi.

• Attaque à texte chiffré choisi (chosen-ciphertext attack en anglais) : Le cryptanalyste possède des messages chiffrés et demande la version en clair de certains de ces messages pour mener l'attaque [5].

I.3 Histoire de la cryptographie

Voici donc un rapide descriptif des faits marquants et des hommes qui ont permis l'apparition et l'évolution de la cryptographie :

- Vers 1900 av. J.-C., un scribe égyptien a employé des hiéroglyphes non conformes à la langue correcte dans une inscription.

- Quatre siècles plus tard, vers 1500 av. J.-C., une tablette mésopotamienne contient une formule chiffrée pour la fabrication de vernis pour les poteries.

- Cinq siècles avant notre ère, des scribes hébreux mettant par écrit le livre de Jérémie ont employé un simple chiffre de substitution connu sous le nom d'Atbash.

- En 487 av. J.-C., les grecs emploient un dispositif appelé la scytale, un bâton autour duquel une bande longue et mince de cuir était enveloppée et sur laquelle on écrivait le message. Le cuir était ensuite porté comme une ceinture par le messager.

Le destinataire avait un bâton identique permettant d'enrouler le cuir afin de déchiffrer le message.

- A partir1226 d'une timide politique de cryptographie apparait dans les archives de

Venise, ou des points ou des croix remplacent les voyelles dans quelques mots épars (répandu).

Citons quelque repère de la cryptographie moderne :

-1975 conception du standard de chiffrement de données adopté en1977.

- 1976 Diffie et Hellman introduisent l'idée de système à clé publique.

- 1978 inventions de RSA le premier système concret de cryptographie a clé publique.

-1985 inventions du système cryptographie el Gamal.

-1991 adoptions du premier standard de signature, ISO9796, basé sur RSA.

-1994 adoption du DSS, standard de signature basé sur l'algorithme discret.

-2000 adoption de rijndeal comme AES (successeur du DES) [6].

I.4 Cryptographie classique

La cryptographie classique a été conçue avant la création des ordinateurs et qui ont donné les concepts et les bases pour l'évolution de plusieurs algorithmes symétriques encore utilisés de nos jours. Les crypto-systèmes classiques sont groupés en chiffrement mono alphabétique et poly alphabétique. Le chiffrement mono alphabétique est très primaire, il s'agit d'une substitution simple. Chaque lettre est remplacée par une autre lettre ou symbole conformément à un certain algorithme [6].

I.4.1 Les scytales des Spartiates

Un procédé de chiffrement avait été imaginé par les Spartiates, dans le souci de protéger la confidentialité de leurs informations. Le principe consistait à enrouler une lanière de cuir ou de papyrus autour d'un bâton de bois de diamètre fixé, puis à écrire le message en travers des spires, c'est-à-dire parallèlement à l'axe du bâton. Une fois déroulée, la lanière contenait donc un texte illisible, sauf pour le correspondant connaissant le diamètre adéquat. Ce mécanisme porte le nom de permutation, puisqu'il consiste à mélanger les lettres du message, sans modifier ces lettres. Des historiens comme Thucydide ou Plutarque signalent l'utilisation de ce procédé au Vème siècle avant notre ère [7].

Figure I. 2: Le Scytale Spartiate [7]

I.4.2 Chiffrement de César

Le chiffrement de César est la méthode de cryptographie la plus ancienne communément admise par l'histoire. Il consiste en une substitution mono-alphabétique : chaque lettre est

remplacée ("substitution") par une seule autre ("mono-alphabétique"), selon un certain décalage dans l'alphabet ou de façon arbitraire. D'après Suétone, César avait coutume d'utiliser un décalage de 3 lettres : A devient D, B devient E, C devient F, etc. Il écrivait donc son message normalement, puis remplaçait chaque lettre par celle qui lui correspondait Dans les formules ci-dessous, p est l'indice de la lettre de l'alphabet, k est le décalage est représenté sur la figure (I.3) [8].

Pour le chiffrement, on aura la formule : C = E(p) = (p + k) mod 26

Pour le déchiffrement, il viendra : p = D(C) = (C − k) mod 26

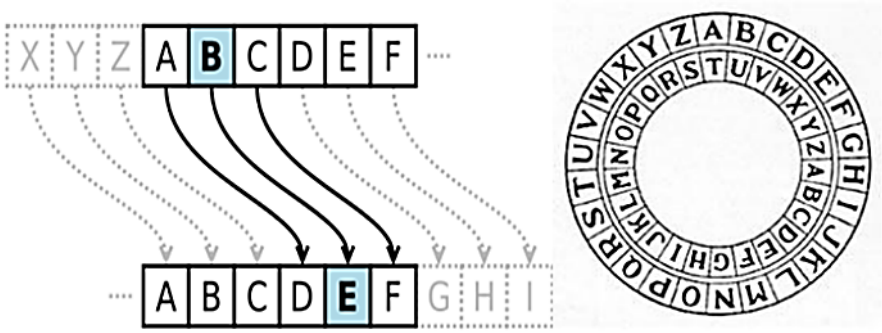


Figure I. 3 : Chiffrement de César [8]

I.4.3 Le chiffre de Hill

Le chiffre publié en 1929 par Lester S. Hill (1891-1961) est un chiffre polygraphique), c'est-à dire qu'on ne déchiffre pas les lettres les unes après les autres, mais par paquets. Nous étudierons un seul cas qui est le cas de groupement biographique du chiffre de Hill, puisque nous grouperons les lettres deux par deux, mais on peut imaginer des paquets plus grands, par exemple des paquets de trois lettres.

Chiffrement Les lettres sont d'abord remplacées par leur rang dans l'alphabet. Les lettres et Pk+1 du texte clair seront chiffrées Ck et Ck+1 avec la formule ci-dessous : [9]

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

Ce qui signifie, pour fixer les idées, que les deux premières lettres du message clair (P1 et P2) seront chiffrées (C1 et C2) selon les deux équations suivantes : [9]

C1 ≡ aP1 + bP2 (mod 26)

C2 ≡ cP2 + dP2 (mod 26) [9].

1.4.4 Blaise de Vigenère (1523-1596)

Diplomate français, se familiarisa avec les écrits d'Alberti, Trithème et Porta à Rome, où, âgé de vingt-six ans, il passa deux années en mission diplomatique. Au début, son intérêt pour la cryptographie était purement pratique et lié à son activité diplomatique. Une dizaine d'années plus tard, vers 1560, Vigenère considéra qu'il avait mis de côté assez d'argent pour abandonner sa carrière et se consacrer à l'étude. C'est seulement à ce moment-là qu'il examina en détail les idées de ses prédécesseurs, tramant grâce à elles un nouveau chiffre, cohérent et puissant. Bien qu'Alberti, Trithème, Bellaso et Porta en aient fourni les bases, c'est du nom de Vigenère que ce nouveau chiffre fut baptisé, en l'honneur de l'homme qui lui donna sa forme finale.

Le chiffre de Vigenère est une amélioration décisive du chiffre de César. Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message. On peut résumer ces décalages avec un carré de Vigenère. Ce chiffre utilise une clef qui définit le décalage pour chaque lettre du message (A : décalage de 0 cran, B : 1 cran, C : 2 crans, ..., Z : 25 crans). [10]

Exemple : chiffrons le texte "CHIFFRE DE VIGENERE" avec la clef "BACHELIER" (cette clef est éventuellement répétée plusieurs fois pour être aussi longue que le texte clair) [10].

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

I.5 Objectifs de la cryptographie

La cryptographie est l'étude des techniques mathématiques qui sont utilisées pour accomplir plusieurs objectifs pour garantir la sécurité de communication, ces objectifs sont [3]:

➢ La confidentialité : Il doit être possible pour le récepteur de l'image de garantir son origine. Une tierce personne ne doit pas pouvoir se faire passer pour quelqu'un d'autre.

➢ L'intégrité : Le récepteur doit pouvoir s'assurer que le message n'a pas été modifié durant sa transmission. Une tierce personne ne doit pas pouvoir substitue un message légitime (ayant pour origine l'émetteur) par un message frauduleux.

➢ L'authentification : Offrir au récepteur d'un message la possibilité de vérifier l'identité de l'émetteur pour but de garantir qu'aucune usurpation d'identité n'a eu lieu.

➢ La non-répudiation : Un émetteur ne doit pas pouvoir nier l'envoi d'un message [3].

I.6 Classification de cryptographie

Dans la cryptographie moderne toute la sécurité est basée sur la clé et non dans les détails des algorithmes utilisés. On trouve principalement deux grandes familles de cryptographie moderne : la cryptographie symétrique ou à clé secrète et la cryptographie asymétrique ou à clé publique [11].

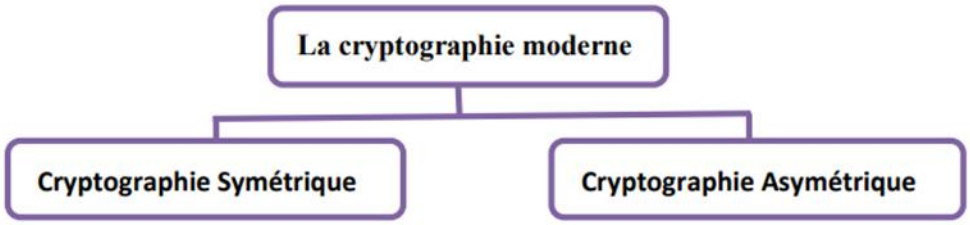


Figure I. 4: Les méthodes de la cryptographie moderne [11].

I.6.1 Cryptage symétrique

Le cryptage à clé privée ou symétrique est basé sur une clé (ou algorithme) partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages. Les algorithmes de chiffrement les plus connus sont : Kerberos, DES (Data Encryption Standard).

Le principal problème est le partage de la clé : Comment une clé utilisée pour sécuriser peut-être transmise sur un réseau insécurisé ? La difficulté engendrée par la génération, le stockage et la transmission des clés (on appelle l'ensemble de ces trois processus le management des clés : Key management) limite le système des clés privées surtout sur Internet est représenté sur la figure (I.5) [12].

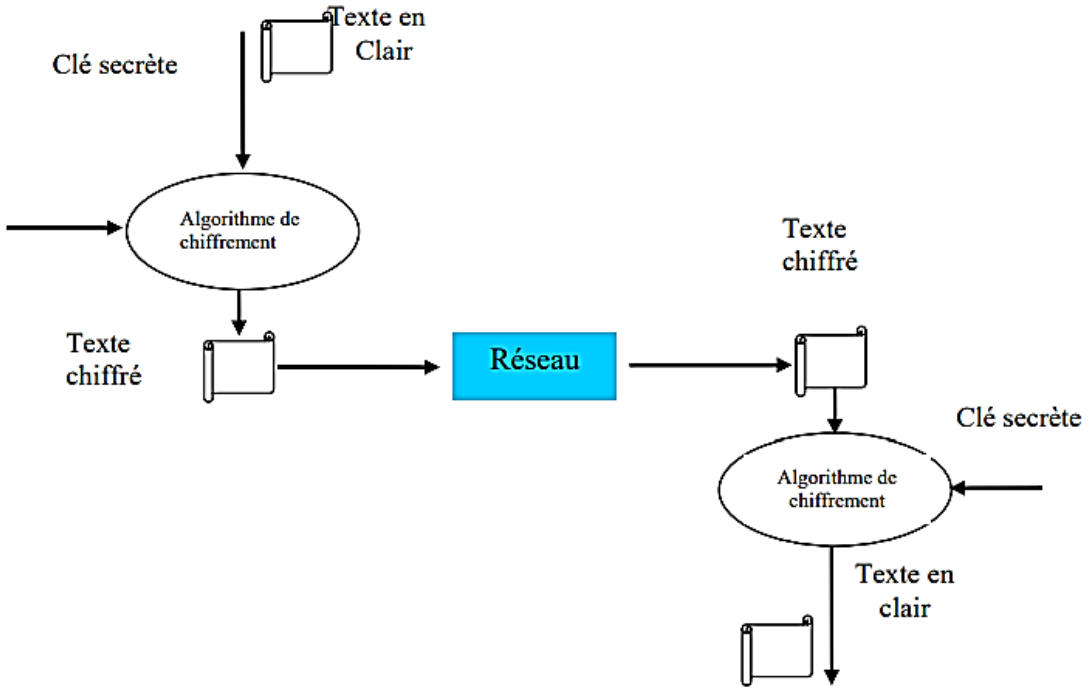


Figure I. 5 : Algorithme de chiffrement symétrique [11].

I.6.2 Les catégories de la cryptographie symétrique

Les schémas de chiffrement symétrique peuvent être classés en deux catégories, le chiffrement par flux et le chiffrement par bloc [11].

I.6.2.1 Chiffrement par flux

Le chiffrement par flux est aussi appelé chiffrement en continu. L'opération de chiffrement par flux s'opère sur chaque élément du texte clair (caractère, bits) au fur et à mesure de leurs arrivées. Sa structure repose sur un générateur de nombres pseudo-aléatoires dont la sortie est couplée via un XOR avec l'information à chiffrer. Ces nombres pseudo aléatoires produits à partir d'une clé secrète est représenté sur la figure (I.6) [3] [13].

Algorithmes de cryptographie symétrique par flot :

- A5 : utilisé dans les téléphones mobiles de type GSM pour chiffrer la communication par radio entre le mobile et l'antenne-relais la plus proche.

- RC4 : le plus répandu, conçu par Ronald Rivest, utilisé notamment par le protocole

WEP, un algorithme récent de Eli Biham – E0 utilisé par le protocole Bluetooth [5].

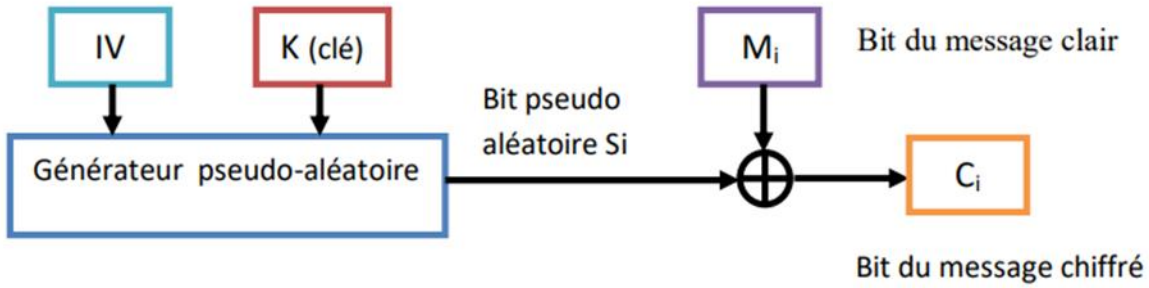


Figure I. 6 : Schéma de chiffrement par flux [5]

I.6.2.2 Le cryptage par bloc (Block Cipher)

C'est une des deux grandes catégories de chiffrements modernes en cryptographie symétrique. Il consiste à un découpage des données en blocs de taille généralement fixe (souvent une puissance de deux comprise entre 32 et 512 bits). Les blocs sont ensuite chiffrés ses uns après les autres. Le chiffrement par bloc utilise quatre modes opératoires : Electronic Code Book (ECB), Cipher Block Chaining (CBC), Output Feedback (OFB) et Cipher Feedback (CFB) [5].

1.Le mode ECB

Le ECB (Electronic CodeBook) le chiffrement est appliqué directement et indépendamment à chaque bloc du message en clair. La séquence résultante des blocs de sortie est le message chiffré est représenté sur la figure (I.7)[14].

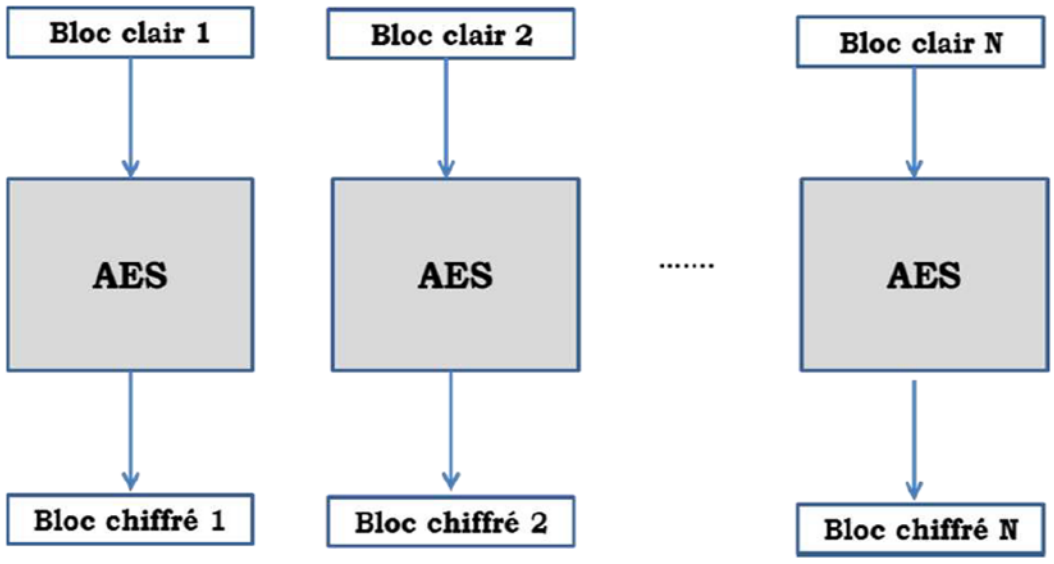


Figure I. 7 : Mode ECB [14].

2.Mode CBC

Le mode CBC, illustré dans la Figure. Est le mode dans lequel le bloc en clair, avant d'être chiffré, est XOR avec le bloc précédemment chiffré. Un vecteur initial doit être utilisé pour initialiser le processus. Ce vecteur remplace le premier bloc qui n'est pas encore défini est représenté sur la figure (I.8) [14].

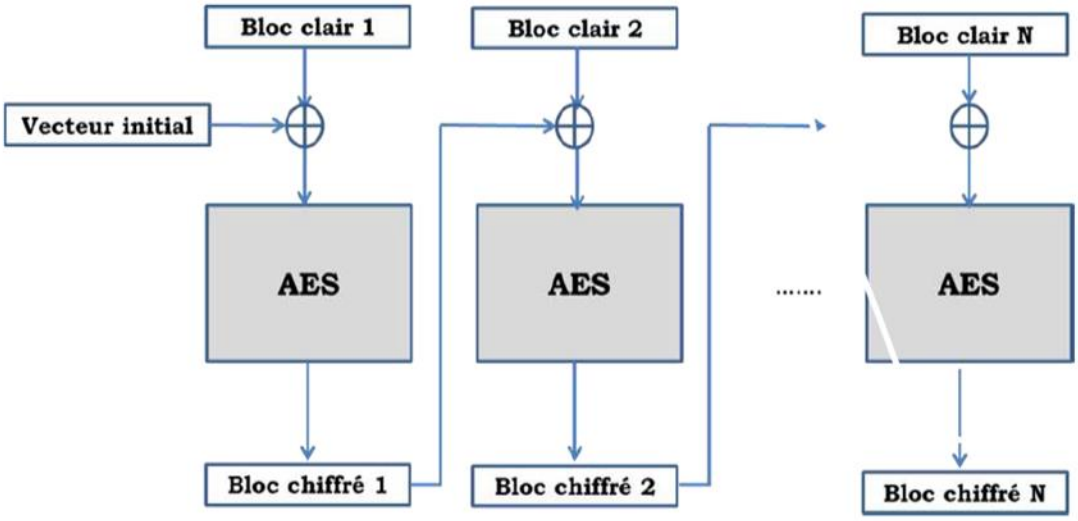


Figure I. 8 : Mode CBC [15]

3.Le mode CFB

Dans le mode de chiffrement CFB (Cipher Feedback), un vecteur d'initialisation est chiffré par l'algorithme de chiffrement. Le résultat est ajouté au texte clair par l'opérateur

Exclusif OR pour obtenir le texte chiffré, ensuite on fait la même chose, sauf au lieu d'utiliser un vecteur d'initialisation, on utilise le texte chiffré de l'opération précédant [15].

4.Mode OFB :

Dans ce mode (Figure), un vecteur initial est initialement chiffré pour démarrer le processus, le flux de clé en sortie de ce bloc sera réinjecté en entrée pour calculer le prochain flux de clé est représenté sur la figure (I.9) [16].

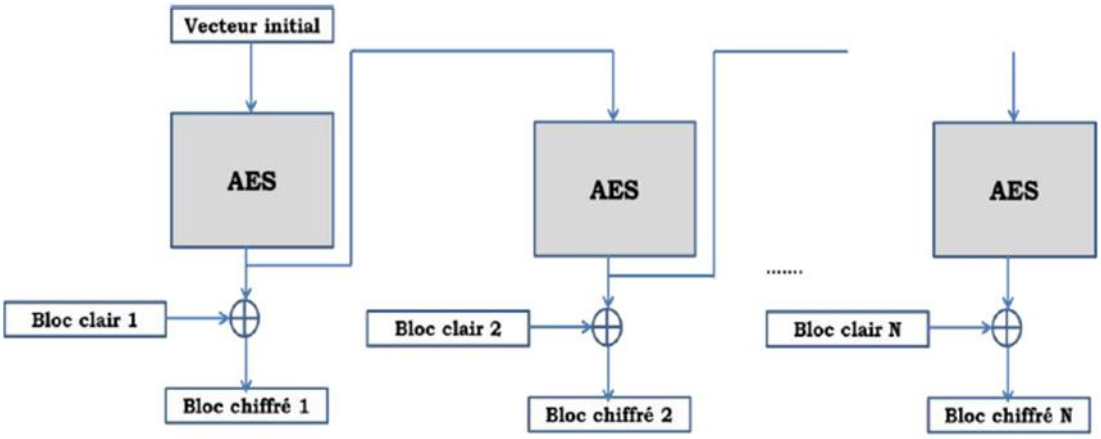


Figure I. 9 : Mode OFB [16]

En utilisant ce mode, le prétraitement du flux de clé est possible car il ne dépend pas de message en clair [16].

I.7 Les algorithmes les plus connus dans la cryptographie symétrique

I.7.1 L'algorithme DES (Data Ecryption Standard)

L'algorithme DES transforme un bloc de 64 bits en un autre bloc de 64 bits. Il manipule des clés individuelles de 56 bits, représentées par 64 bits (avec un bit de chaque octet servant pour le contrôle de parité).

Ce système de chiffrement symétrique fait partie de la famille des chiffrements itératifs par blocs, plus particulièrement il s'agit d'un schéma de Feistel (du nom de Horst Feistel à l'origine du chiffrement Lucifer)

Le DES est basé sur les attributs fondamentaux de fonctions cryptographiques telles que substitution (confusion) et transposition (diffusion), opération OU exclusif, décalage et swap Ping.

Le DES se compose de 16 tours et chaque tour utilise une seule clé ronde et que les clés sont générées à partir du générateur de la clé ronde. Le générateur de clé ronde crée le 48 bits clés pour chaque tour [16].

D'une manière générale, on peut dire que DES fonctionne en trois étapes :

Permutation initiale et fixe d'un bloc (sans aucune incidence sur le niveau de sécurité) ;

Le résultat est soumis à 16 itérations d'une transformation, ces itérations dépendent à chaque tour d'une autre clé partielle de 48 bits. Cette clé de tour intermédiaire est calculée à partir de la clé initiale de l'utilisateur (grâce à un réseau de tables de substitution et d'opérateurs XOR). Lors de chaque tour, le bloc de 64 bits est découpé en deux blocs de 32 bits, et ces blocs sont échangés l'un avec l'autre selon un schéma de Feistel. Le bloc de 32 bits ayant le poids le plus fort (celui qui s'étend du bit 32 au bit 64) subira une transformation ; le résultat du dernier tour est transformé par la fonction inverse de la permutation initiale est représenté sur la figure (I.10) [17].

1.Etapes de l'algorithme DES

Le message est découpé en blocs de 64 bits.

— Une permutation initiale est faite sur le bloc de 64 bits (permutation).

— Le bloc de 64 bits est découpé en deux blocs de 32 bits, et ces blocs sont échangés l'un avec l'autre selon un schéma de Feistel.

— Une extension du bloc de taille 32 bits à 48 bits est appliquée. — Une opération XOR est faite entre la clé de 56 bits et le bloc de 48 bits (Ronde).

— les 48 bits sont ensuite divisés en 8 blocs de 6 bits, chaque vecteur étant finalement traité grâce à une table d'expansion

— Des transpositions sont faites sur des blocs de 32 bits grâce à une table de substitution (S-BOx).

— L'algorithme consiste en fait en 16 itérations de cryptage, et dans chaque nouvelle itération, une nouvelle clé est utilisée. A la fin de la 16ème itération, les deux blocs de 32 bits de gauche et de droite sont réunis en un seul bloc de 64 bits (permutation inverse) [17].

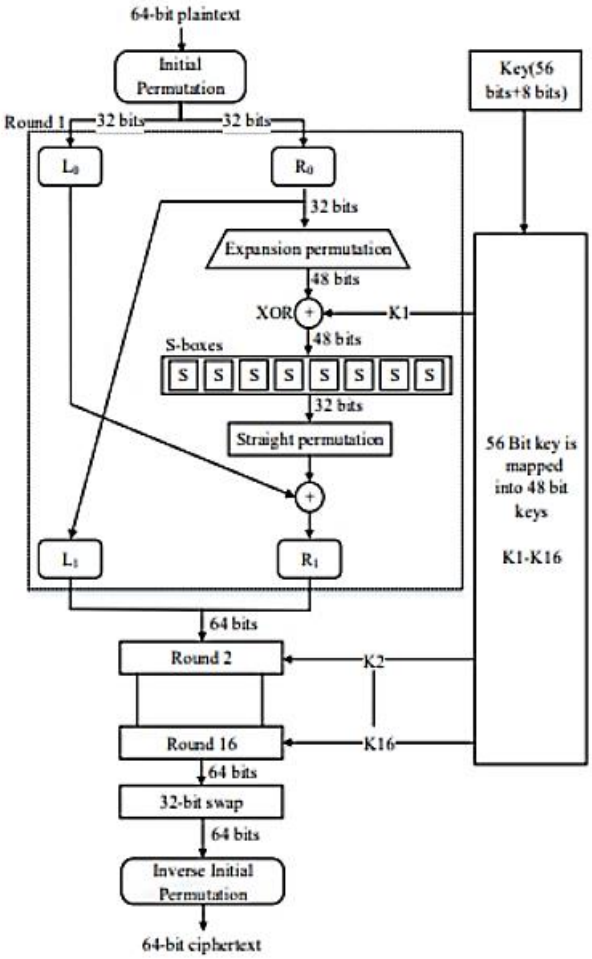


Figure I. 10 : représentation générale du DES [17]

I.7.2 AES [18]

La faiblesse de l'algorithme DES ; un autre algorithme qui s'appelle triple DES a été inventé, puis un autre algorithme AES de chiffrement symétrique plus puissant a été développé en 2000.

Les étapes de cet algorithme sont résumées en :

— Permutation : Un bloc de données de 16, 24v ou 32 octets sont permutés ensuite placés dans une matrice.

— L'opération SubBytes : consiste à substituer chaque élément de la matrice via une SBox.

— L'opération Shiftrows : cette étape implique un décalage à gauche sur les éléments de la matrice.

— L'opération MixColumns : en effectuant une opération mathématique sur chaque colonne de la matrice de données et mettant le résultat dans une nouvelle matrice.

— L'opération Addroundkey : Cette étape consiste à faire un XOR entre la matrice qui contient la clé et le bloc de donnees.

I.8 Avantages et inconvénients de la cryptographie symétrique [11]

Tableau I. 1 : Avantages et Inconvénients de chiffrement symétrique.

Avantages	Inconvénients
Chiffrement / Déchiffrement rapide	Problème d'échange de la clé secrète
Volumes importants de données à chiffrer	n (n-1)/2 Clés pour n partenaires
Clés relativement courtes	Pas de signature électronique
Utilise peu de ressources systèmes	

I.9 Cryptographie Asymétrique

La cryptographie asymétrique, ou cryptographie à clé publique repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de chiffrer le message et l'autre de le déchiffrer. Ainsi, l'expéditeur peut utiliser la clé publique du destinataire pour chiffrer un message que seul le destinataire (en possession de la clé privée) peut le déchiffrer, garantissant la confidentialité du contenu.

Inversement, l'expéditeur peut utiliser sa propre clé privée pour chiffrer un message, le destinataire peut déchiffrer avec la clé publique ; c'est le mécanisme utilisé par la signature numérique pour authentifier l'auteur d'un message. Dans la cryptographie asymétrique impossible de trouver la clé privée à partir de la clé publique est représenté sur la figure (I.11) [2].

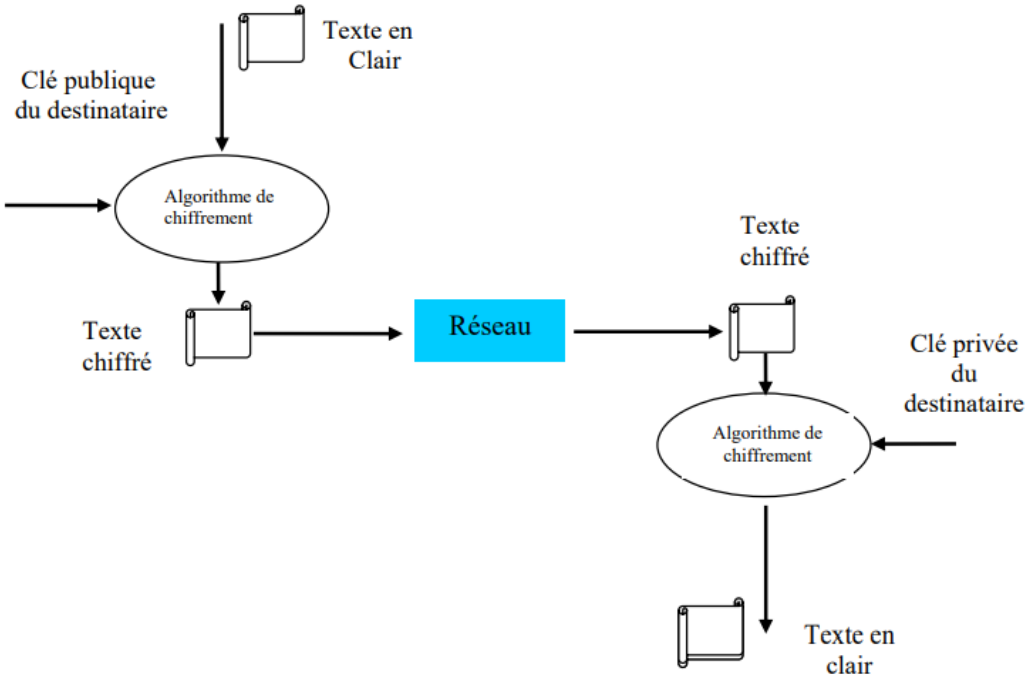


Figure I. 10: algorithme de chiffrement asymétrique [11].

I.10 Les algorithmes les plus connus dans la cryptographie asymétrique

I.10.1 L'algorithme RSA (Ron Rivest, Adi Shamir, et Len Adlmen) [19]

Le principe

Le premier système à clé publique solide à avoir été inventé, et le plus utilisé actuellement, est le système RSA. Publié en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman de l'Institut de technologie du Massachusetts (MIT), le RSA est fondé sur la difficulté de factoriser des grands nombres, et la fonction à sens unique utilisée est une fonction "puissance"

L'algorithme de chiffrement

Départ :

Il est facile de fabriquer de grands nombres premiers p et q (+- 100 chiffres)

Etant donné un nombre entier n = p*q, il est très difficile de retrouver les facteurs p et q

(1) Création des clés

La clé secrète : 2 grands nombres premiers p et q

La clé secrète : 2 grands nombres premiers p et q

• La clé publique : n = p*q ; un entier e premier avec (p-1) (q-1)

(2) Chiffrement : le chiffrement d'un message M en un message codé C se fait suivant la transformation suivante :

$$C = M^e \ mod \ n$$

(3) Déchiffrement : il s'agit de calculer la fonction réciproque

$$C = C^d \ mod \ n$$

$$tel \ que \ e.d = 1 \ mod \ [(p-1)(q-1)]$$

La signature électronique :

Après la confidentialité de la transmission d'un message subsiste un problème : son authenticité.

Alice voudrait bien envoyer un message M à Bob de telle façon que celui-ci soit sûr qu'elle est réellement l'émettrice du message, et qu'un intrus ne tente pas de venir semer la confusion.

Le système RSA fournit une solution à ce problème :

Rappelons les données :

• Alice seule détient la clé secrète d et diffuse la clé publique (n,e)

• Alice va se servir de la clé publique pour chiffrer le message M

(1) Alice accompagne son message chiffré de sa signature, qui correspond à :

$$M^d$$

(2) Bob va donc voir si l'égalité (Md)e mod n = M est vérifiée. Si c'est le cas, Alice est bien l'émettrice du message [19].

I.11 Avantages et inconvénients de la cryptographie asymétrique [11]

Tableau I. 2 : Avantages et Inconvénients de chiffrement asymétrique.

Avantages	Inconvénients
Authentification des messages par signature électronique	lent à l'exécution en raison de la charge de calcul
Pas besoin de partager des clés secrètes via une voie de transmission sécurisée	Attaques par substitution de clé possibles
n paires de clés pour n partenaires	la longueur de clé largement augmentée

I.12 Notions de base sur l'image

I.12.1 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 [20].

I.12.2 L'image numérique

Une image numérique est composée des cases appelées « pixels ». Ces pixels seront affectés de nombres binaires permettant de définir des teintes de gris ou des couleurs [20].

I.13 Les attributs des images Pixels

I.13.1 Le pixel

Représente la plus petite unité d'une image numérique appelé en anglais (Picture Elément). Les nombres des pixels de ligne et les nombres des colonnes déterminent la démentions de l'image, et chaque pixel représente valeur (couleur) [20].

I.13.2 La taille

La taille de l'image est la place qu'elle occupe dans le codage binaire. Son unité est « l'octet ».

Taille = nombre d'octets pour chaque pixel × définition [20].

I.14 Les formats d'images

Pour représenter une image, on peut la décrire à l'aide de fonctions mathématiques (Représentation vectorielle) ou par l'ensemble des points qui la composent (représentation matricielle) [21].

I.14.1 Image vectorielle

Une image vectorielle peut être agrandie ou rétrécie sans dégradation car l'image sera recalculée précisément en fonction de la taille souhaitée. En général, le fichier correspondant est peu volumineux [21].

1- Le format Scalable Vector Graphics (SVG) est un format ouvert d'image vectorielle ; il est surtout utilisé en cartographie et sur les téléphones portables.

2- Le format Dessin de l'Open Document Format (ODF) est un format ouvert de dessin vectoriel ; il est utilisé par l'application Draw d'Open Office [21].

I.14.2 Image matricielle

Une image matricielle se dégrade si on l'agrandit : la pixellisation devient visible. En fonction de la taille de l'image et du nombre de couleurs utilisées, le fichier correspondant peut devenir volumineux. Pour transiter sur Internet, on utilisera des formats matriciels compressés [21].

I.15 Les formats Matriciels

I.15.1 JPEG

JPEG (Joint Photographic Experts Group) est une méthode de compression avec perte, Les images JPEG compressées sont généralement stockées dans le format de fichier JFIF (JPEG Interchange File Format). Le format de fichier d'image est le plus utilisé. Les formats JPG est plus utilisé dans les appareils photo numériques et les pages Web [20].

I.15.2 TIFF

Le format TIFF (Tagged Image File Format), Il permet de stocker des images de haute qualité en noir et blanc, couleurs RVB jusqu'à 32 bits par pixels. Il supporte aussi les images indexées faisant usage d'une palette de couleurs, les calques et les couches alpha (transparence) [20].

I.15.3 GIF

GIF (Graphics Interchange Format), C'est un format léger pour les animations. Et de transparence compression efficace Très répandu sur le Web malgré ses faiblesses et un problème de droit sur son format de compression. À déconseiller pour les photos [20].

I.15.4 PNG

Le format de fichier PNG (Portable Network Graphics), Il permet de stocker des images en noir et blanc (jusqu'à 16 bits par pixels), en couleurs réelles (True color, jusqu'à 48 bits par pixels) ainsi que des images indexées, faisant usage d'une palette de 256 couleurs. Il offre enfin une couche alpha de 256 niveaux pour la transparence [20].

I.16 Cryptage d'image

Pour crypter une image, il faut avoir une fois de plus recours aux bits. Chaque pixel possède une couleur : celle-ci est définie par un nombre entier, converti par la suite en binaire. Le principe de cryptage est simple : par exemple, il s'agit d'"additionner" deux images, une image-clé et l'image qu'on veut crypter, grâce à l'opérateur bit à bit XOR [22].

I.17 Méthodes de cryptage d'images

Il existe deux grandes différences entre les données textuelles et les images numériques. Les méthodes de cryptage de texte pour la plupart des cas inapplicable au cryptage des images. La principale différence réside dans la taille, en effet la quantité d'informations contenues dans l'image est beaucoup plus volumineuse que celles contenues dans les données textuelles. La seconde différence concerne la perte de données, lorsqu'une technique de compression est appliquée. Contrairement aux images, l'utilisation d'une méthode de compression avec perte est totalement interdite lors du chiffrement d'un texte, par conséquent, les chercheurs ont étudié plusieurs méthodes de chiffrement d'image avec/sans perte. D'autre part, les algorithmes de chiffrement des images peuvent être classés selon le domaine d'application : les méthodes du domaine spatial ou bien celle du domaine fréquentiel [22].

I.17.1 Méthodes dans le domaine spatial

Dans le domaine spatial, on applique le schéma de cryptage sur le plan d'image lui-même, et les approches de cette catégorie sont basées sur une manipulation directe des pixels d'une image. Dans ces algorithmes, le chiffrement détruit la corrélation entre les pixels et rend les images cryptées incompressibles.

Les pixels de l'image peuvent être reconstruits (récupérés) complètement par un processus inverse sans aucune perte d'information

Les algorithmes de cryptage d'image dans le domaine spatial existants peuvent être classés en deux catégories.

- Dans la première catégorie, un pixel est considéré comme le plus petit élément, et une image numérique est considérée comme un ensemble de pixels.

- Toutefois, dans la deuxième classe, un pixel peut être en outre divisé en bits, sur lesquels des opérations au niveau de bits sont effectuées. Par exemple, un pixel dans une image en niveaux de gris est généralement constitué de 8 bits [22].

I.17.2 Méthode dans le domaine fréquentiel

Les schémas de cryptage dans le domaine fréquentiel sont basés sur la modification de la fréquence de l'image en utilisant une transformation, ainsi, la reconstruction des pixels de l'image originale dans le processus de décryptage cause généralement une perte d'information [23].

I.18 Conclusion

Étant donné que la sécurité des réseaux mobiles est une nécessité, nous lui avons consacré tout un chapitre dans lequel nous avons mis le point sur les algorithmes de cryptographie ainsi que leur fonctionnement. Les deux systèmes cryptographiques de base à clé secrète et à clé publique souffrent de problèmes et chacun a ses spécificités. La force des algorithmes à clés publiques réside dans la distribution des clés alors que les algorithmes à clés secrètes sont très performants en vitesse de chiffrement.

Chapitre II :

Cryptage des images médicales par la technique AES-GCM.

II.1 Introduction

Tout à fait, dans le domaine des télécommunications, la sécurité des données est un enjeu crucial pour protéger les informations personnelles et confidentielles des utilisateurs. Les images médicales, par exemple, contiennent souvent des informations sensibles sur la santé des patients, ce qui en fait une cible particulièrement attractive pour les cybercriminels.

Les techniques cryptographiques sont une solution efficace pour protéger les données contre les menaces. Le chiffrement permet de rendre les données illisibles pour les personnes non autorisées, tandis que l'intégrité assure que les données n'ont pas été modifiées en transit. L'authentification permet de vérifier l'identité de l'émetteur et du destinataire des données.

Dans ce chapitre nous commence par expliquer Les concepts fondamentaux de l'image médicale en particulier ainsi que la technique AES et AES-GCM [24].

II.2 Imagerie Médicale

L'imagerie médicale fait référence à plusieurs technologies différentes qui sont utilisées pour visualiser le corps humain afin de diagnostiquer, surveiller ou traiter des conditions médicales. Toutes les modalités d'imagerie ont en commun que la condition médicale devient visible par une certaine forme de contraste, ce qui signifie que la caractéristique d'intérêt (telle qu'une tumeur) peut être reconnue dans l'image et examinée par un radiologue qualifié [25].

II.3 Imagerie Analogique Et Imagerie Numérique

Il existe deux façons de représenter les informations [26] :

II.3.1 L'imagerie analogique

Tout à fait, la représentation analogique de l'information implique que les signaux sont représentés sous forme de quantités physiques continues, telles que des ondes sonores, des signaux électriques, ou des variations de la lumière. Les phénomènes naturels sont continus, et donc la représentation analogique est souvent utilisée pour capturer et stocker ces phénomènes.

Un exemple courant de support analogique est la cassette vidéo ou audio. Les signaux audio ou vidéo sont enregistrés sur la bande magnétique sous forme d'ondes continues. Lors de la lecture de la cassette, les signaux sont lus par une tête de lecture qui convertit les variations magnétiques en signaux électriques continus, qui sont ensuite amplifiés et envoyés aux haut-parleurs ou à l'écran.

Cependant, la représentation analogique peut présenter des limitations en termes de qualité et de précision, car les signaux peuvent être affectés par des interférences électromagnétiques, du bruit ou des perturbations environnementales. De plus, les supports analogiques ont une durée de vie limitée et peuvent se détériorer avec le temps.

C'est pourquoi, avec l'avènement du numérique, de nombreux systèmes de stockage et de traitement de l'information sont maintenant basés sur la représentation numérique, qui utilise des valeurs discrètes pour représenter l'information. Cela permet une plus grande précision, une meilleure qualité et une plus grande durabilité des données stockées [24].

II.3.2 L'imagerie numérique : numérisation

On peut numériser les images (digitalisation en anglais), c'est à dire transformer l'information initiale en une matrice de nombre. On peut donc passer d'une image analogique à une image numérique par la numérisation [24].

Dans la numérisation, il y a deux étapes :

1. Un codage spatial (échantillonnage spatial) : L'image va d'abord être divisée en pixels (Picture elements) qui sont des petites surfaces élémentaires de l'image. Lorsque l'on est en présence d'une image de côté N et M, on aura une image divisée en NxM pixels.

2. Un codage en intensité (quantification) : Dans chaque pixel on va pouvoir mettre un nombre qui correspond à la valeur moyenne de l'intensité en ce point.

On se retrouve alors avec une matrice de nombre qui comprend la totalité des renseignements nécessaires. On enregistre donc ces nombres à l'aide d'ordinateurs (Ainsi l'imagerie médicale c'est beaucoup développée parallèlement au développement des ordinateurs), on est alors capable de retranscrire cette matrice de nombre en une image visuelle. Pour ce faire, on associe chaque nombre enregistré à un niveau de gris.

On a donc une intensité qui varie par palier, les images numériques contiennent donc une information discrète et non continue.

II.4 Différents types d'imagerie médical

Un service d'imagerie de nos jours est constitué d'une multitude de modalités que nous citerons ci-dessous.

II.4.1 Tomodensitométrie (TDM)

Cette procédure d'imagerie utilise est une modalité d'imagerie volumétrique basée sur l'absorption des rayons X est représenté sur la figure (II.1).

La TDM permet la reconstruction d'une carte d'absorbeur en deux ou trois dimensions.

La tomodensitométrie dépasse largement l'imagerie par rayons X par projection dans le contraste des tissus mous, mais la résolution spatiale d'un tomodensitogramme (scanner) clinique du corps entier est nettement inférieure à celle de l'imagerie par rayons X simple. Néanmoins, la tomodensitométrie peut révéler de petites tumeurs, des détails structures dans l'os trabéculaire ou le tissu alvéolaire des poumons. [25]

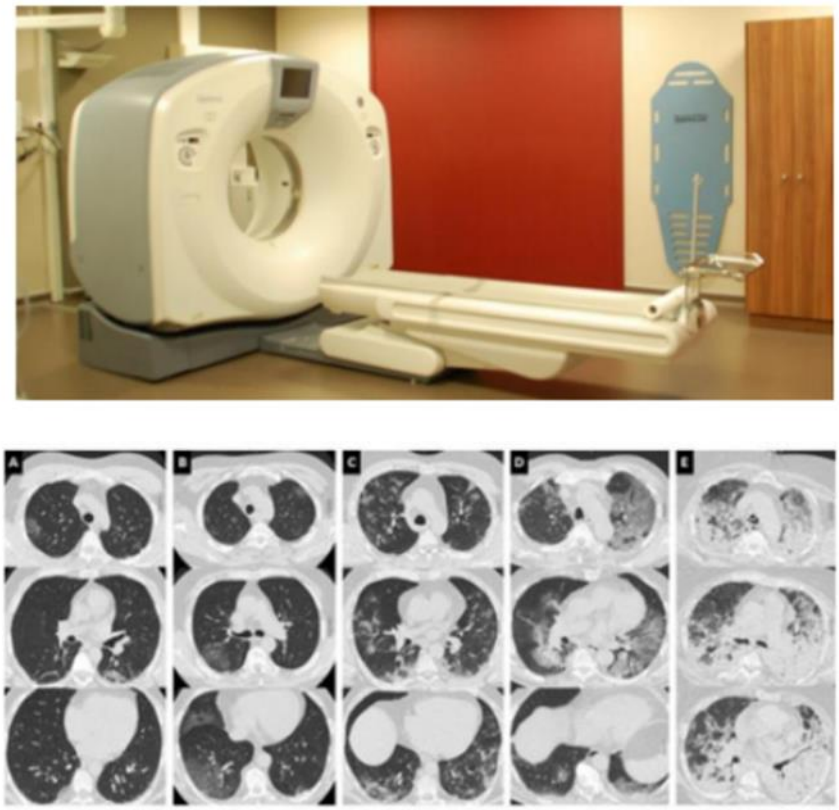


Figure II. 1 : Schéma d'un scanner (en haut) et un échantillon d'images (en bas) [27].

II.4.2 Radiographie

Est la plus ancienne modalité d'imagerie médicale, qui a trouvé sa place dans la pratique médicale peu de temps après la découverte des rayons X en 1895. Les rayons X sont des photons de haute énergie, et l'interaction atomique avec les électrons de la couche interne est fondamentale à la fois pour la production de rayons X et la génération de contraste de rayons X est représenté sur la figure (II.2).

Le contraste des tissus mous est relativement faible, mais l'os et l'air offrent un excellent contraste. Les images aux rayons X peuvent révéler des caractéristiques très subtiles, mais ont des effets très nocifs sur la santé pour des durées d'exposition longues ou répétées et/ou pour de fortes intensités.

L'imagerie par rayons X est utilisée pour diagnostiquer les fractures osseuses, les maladies pulmonaires, Etc [28].

Figure II. 2 : Schéma d'un système de radiographie (à gauche) [28]et un échantillon D'images radio-graphiques (à droite) [27].

II.5 L'imagerie par résonance magnétique (IRM)

Est une modalité d'imagerie volumétrique parallèle, dans une certaine mesure, à la tomodensitométrie. Cependant, les principes physiques sous-jacents sont fondamentalement différents de la TDM. Là où la tomodensitométrie utilise des photons de haute énergie et l'interaction des photons avec les électrons de la couche atomique pour la génération de contraste, l'IRM est basée sur l'orientation des protons à l'intérieur d'un champ magnétique puissant. Cette orientation peut être manipulée avec des ondes radio fréquences résonantes, et le retour des protons à leur état d'équilibre peut être mesuré. Les constantes de temps de relaxation dépendent fortement des tissus et l'IRM présente un contraste supérieur des tissus mous, dépassant de loin celui du TDM est représenté sur la figure(II.3) [26].

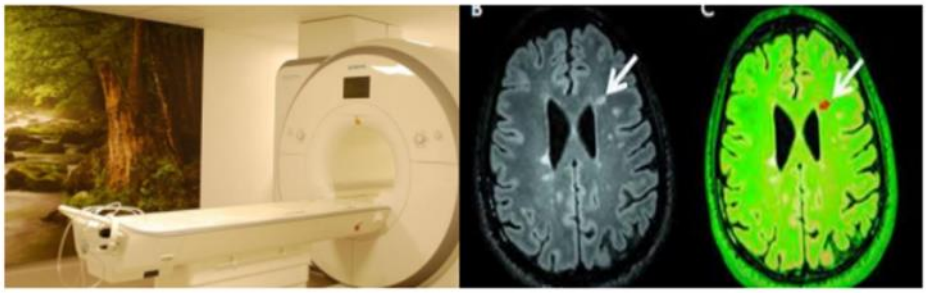


Figure II. 3 : Schéma d'un système d'IRM [27] (à gauche) et un échantillon d'image (à droite) indiquant les formes progressives de sclérose en plaques (SEP) [29].

II.6 Imagerie par ultrasons

L'imagerie par ultrasons utilise les propriétés des ondes sonores dans les tissus.

Les ondes de pression dans la gamme des mégahertz inférieurs traversent les tissus à la vitesse du son, étant réfractées et partiellement réfléchies aux interfaces. Le contraste échographique est donc lié à des inhomogénéités échogènes dans les tissus.

Les images échographiques montrent un bon contraste des tissus mous, mais échouent en présence d'os et d'air. Bien que les images ultrasonores puissent être générées avec des circuits purement analogiques, les appareils à ultrasons modernes utilisent un traitement d'image informatisé pour la formation, l'amélioration et la visualisation des images. L'imagerie par ultrasons est très populaire en raison de son instrumentation peu coûteuse et de sa facilité d'application.

Cependant, un examen échographique nécessite la présence d'un opérateur expérimenté pour ajuster divers paramètres pour un contraste optimal, et les images échographiques nécessitent généralement un radiologue expérimenté pour interpréter l'image [25] .

II.7 Architecture de l'algorithme AES

L'algorithme peut être employé avec les trois longueurs principales différentes indiquées Ci-dessus, et peuvent désigner sous le nom de "AES-128", de "AES-192", et de "AES-256 ».

Pour chacun la taille de bloc (données) d'entrée et de sortie est toujours de 128 bits.

Pour les trois cas de l'algorithme, la longueur de clé et le nombre de rondes (tours) sont

Définit dans le tableau 2.1[30] :

Tableau II. 1 : Combinaisons Clé-Bloc-Ronde

	Longueur de Clé (NK : Mot 32bits)	La taille de bloc (NK : Mot 32bits)	Nombre de rondes (Tour) (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

La figure (II.4) montre la structure de l'algorithme de chiffrement AES de façon plus détaillée. Avant d'entrer dans les détails, nous pouvons faire quelques remarques sur La structure de l'algorithme :

- Une caractéristique remarquable de cette structure est qu'elle n'est pas une structure de Feistel.
- La clef qui est fourni en entrée est élargie en une matrice de quarante-quatre Mots 32 bits, w [i]. Quatre mots distincts (128 bits) servent pour assurer le chiffrement pour chaque tour ; elles sont indiquées dans la figure (II.4).

Quatre phases différentes sont utilisées pour chaque tour : une de permutation et trois de substitution :

• « Substitute bytes » utilise une boîte S pour effectuer une substitution octet par octet
• « ShiftRows » Une simple permutation entre les octets
• « MixColumns » Une substitution qui rend l'utilisation de l'arithmétique autour GF 2^8
• « AddRoundKey » un simple XOR entre le bloc courant avec une partie de la clef étendue

- L'étape de « AddRoundKey » est la seule qui utilise la clef. Pour cette raison, la procédure de chiffrement commence et se termine par une étape de « AddRoundKey ».
- Chaque étape est facilement réversible. Pour « Substitute bytes », « ShiftRows », « MixColumns » une fonction inverse est utilisée dans l'algorithme de déchiffrement. Pour l'étape de « AddRoundKey », l'inverse est réalisé par XOR : $A \oplus B \oplus B = A$.
- L'algorithme de chiffrement n'est pas identique à l'algorithme de déchiffrement, ceci est une particularité de l'Aes.
- La tour finale de chiffrement et le déchiffrement se compose seulement de trois étapes. Encore une fois, ceci est une particularité de la structure de l'Aes [31].

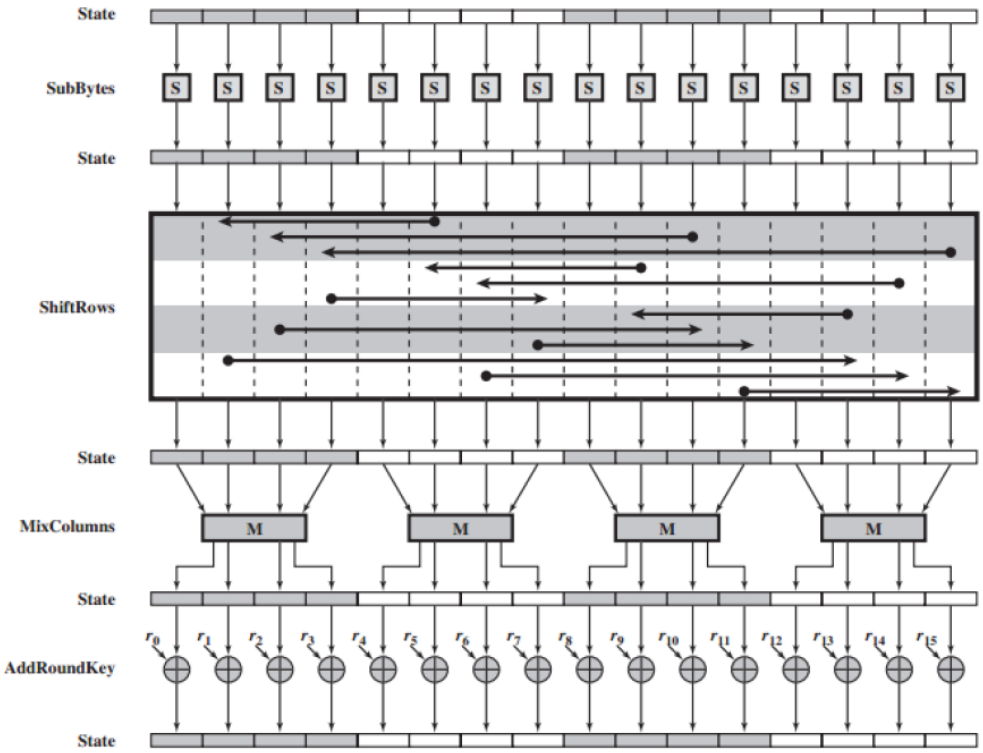


Figure II. 4 : les tours de chiffrement de l'AES [31]

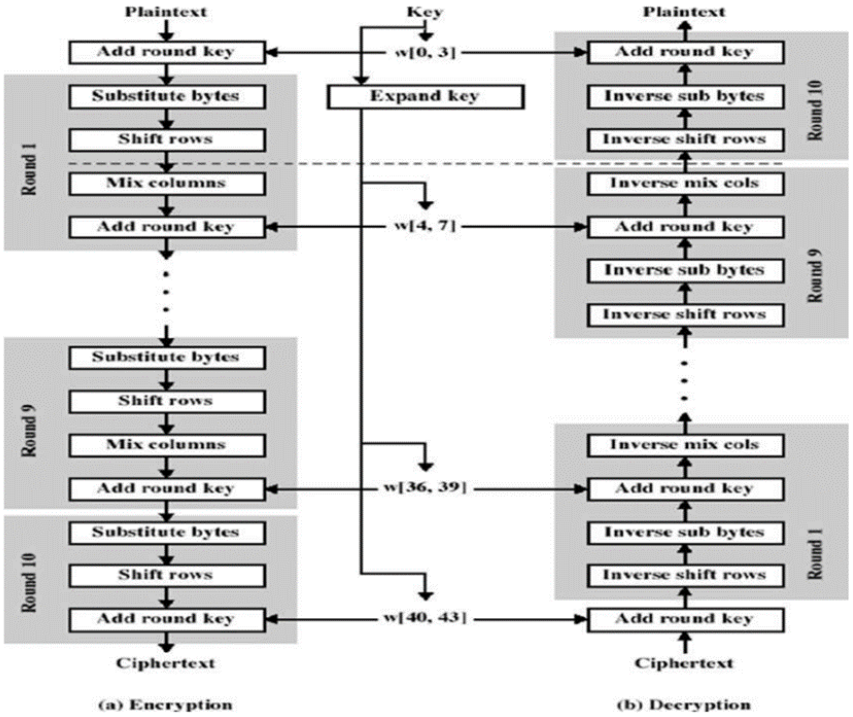


Figure II. 5 : Algorithme AES.[31]

II.7.1 Chiffrement

a. La substitution (S-Box /SubByte)

La transformation de SubByte (Figure II.6) est une substitution non linéaire d'un bloc de 8-bits (byte) qui fonctionne indépendamment sur chaque byte de bloc en utilisant une table de substitution (boîte de substitution). Cette boîte de substitution (Figure II.7), qui est inversible, une seule boîte est suffisante pour toute la phase de chiffrement [32].

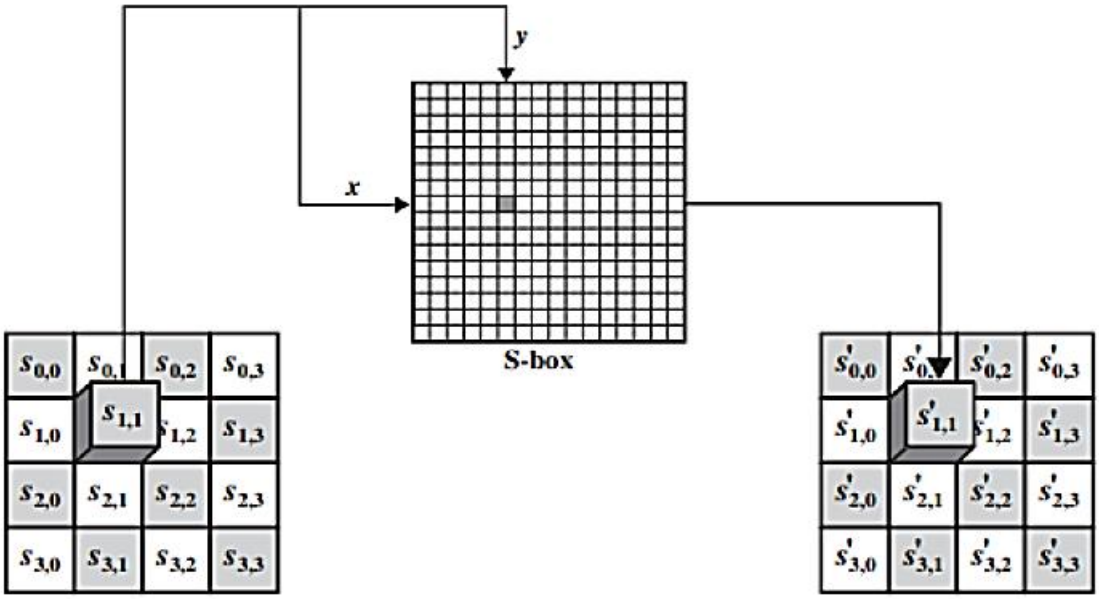


Figure II. 6 : Table d'état des clés [32].

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure II. 7 : S-Box inversible [30].

b. Le décalage de rangées (ShiftRows)

Cette étape augmente la diffusion dans la ronde selon la figure (II.8) [30] :

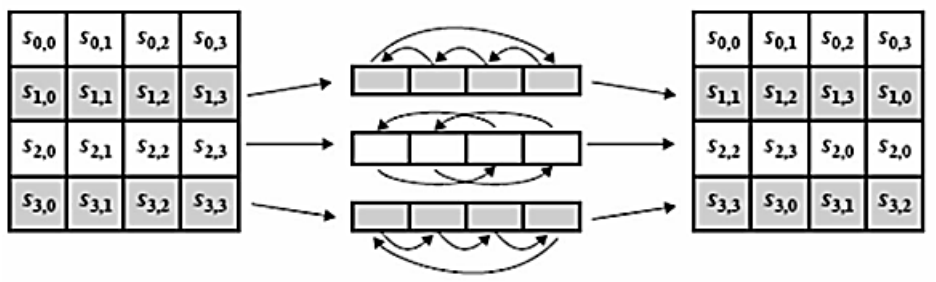


Figure II. 8 : Schéma de l'étape ShiftRow[30]

Selon la taille des blocs de message (c'est-à-dire la valeur de Nb), les décalages ne seront pas toujours identiques.

– La ligne 0 n'est jamais décalée,

– La ligne 1 est décalée de C1,

– La ligne 2 est décalée de C2,

– La ligne 3 est décalée de C3

Tableau II. 2 : Décalage selon la taille des blocs de messages [30].

	C1	C2	C3
Nb=4	1	2	3
Nb=6	1	2	3
Nb =8	1	3	4

C-Mélange des colonnes (MixColumns) :

Une différence sur 1 byte d'entrée se propage sur les 4 bytes de sortie. On a donc encore une étape de diffusion. La matrice utilisée est définie par Rijndael. Elle contiendra toujours ces valeurs [30], qui est illustré par la figure (II.9) :

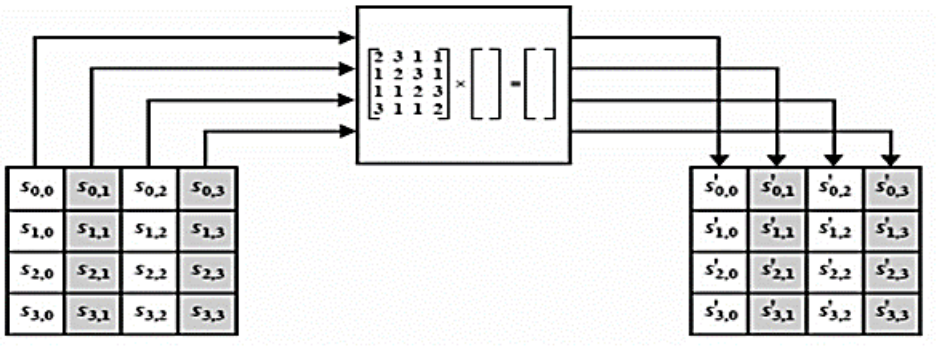


Figure II. 9 : Etape du MixColumn[30].

d. Addition d'une clé de ronde (AddRoundKey)

C'est un simple $\oplus$ des clés. Il s'agit d'additionner des sous-clés aux sous-blocs correspondants suivant la figure (II.10) [30] :

Figure II. 10 : AddRound Key [8]

e. Génération (extension) des clés

Après avoir subi une extension (Key Expansion), la clé sera découpée en sous-clés (appelées clés de rondes), comme indiqué à la figure (II.11) [30].

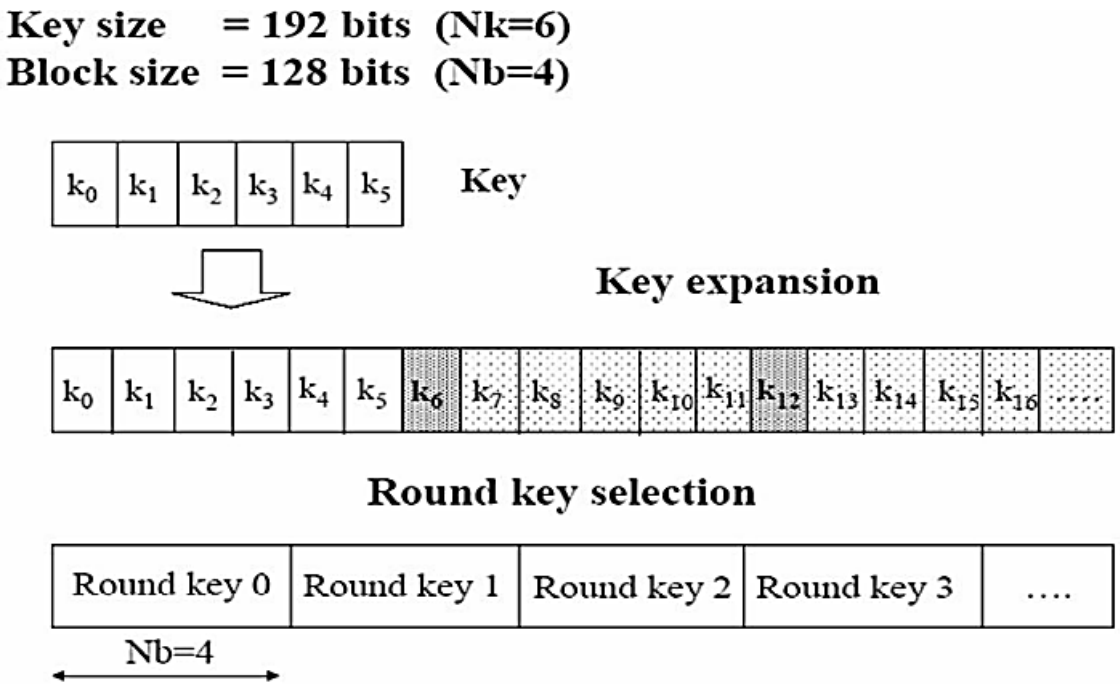


Figure II. 11: Schéma des opérations effectuées sur la clé [30]

II.8 L'AES-GCM

L'AES-GCM (Advanced Encryption Standard / Galois Counter Mode) est un mode de chiffrement par bloc en cryptographie symétrique. Il s'agit d'un algorithme de chiffrement authentifié conçu pour assurer l'intégrité et l'authenticité des données ainsi que la confidentialité et est relativement courant en raison de son efficacité et de ses performances. Le débit GCM sur des canaux de communication à haut débit peut être réalisé avec des ressources matérielles raisonnables, GCM est défini pour les chiffrements par blocs avec une taille de bloc de 128 bits [33].

GCM est un mode de fonctionnement de chiffrement par bloc qui utilise le hachage universel sur un champ galois binaire pour fournir un chiffrement authentifié, il peut être implanté dans le matériel pour attendre des vitesses élevées avec un faible cout et une faible latence.

Les implémentations logicielles peuvent atteindre d'excellente performances en utilisant des opérations de champ basée sur des tables.

Il utilise des mécanismes qui sont soutenu par une base théorique bien comprise et sa sécurité découle d'une seule hypothèse raisonnable sur la sécurité du chiffrement par blocs [33].

II.9 Éléments de GCM

GCM signifie "Galois/Counter Mode", qui est un mode de fonctionnement pour les chiffrements par blocs. Le mode GCM combine la confidentialité d'un chiffrement par blocs avec l'authenticité d'un code d'authentification de message (MAC). Voici les éléments clés du mode GCM :

1. Chiffrement par blocs : GCM est conçu pour fonctionner avec n'importe quel chiffrement par blocs, tel que AES, qui est un algorithme de chiffrement à clé symétrique largement utilisé.

2. Compteur : GCM utilise un compteur pour générer une valeur unique pour chaque bloc de texte en clair. Le compteur est chiffré à l'aide du chiffrement par bloc et combiné avec le texte en clair pour produire le texte chiffré.

3. Multiplication de champ de Galois : GCM utilise une multiplication de champ de Galois pour générer la balise d'authentification. Cette multiplication est effectuée dans un champ spécial appelé champ de Galois (GF), qui est un champ fini utilisé dans la théorie de codage algébrique.

4. Balise d'authentification : GCM génère une balise d'authentification qui fournit l'authentification et l'intégrité du message. La balise d'authentification est générée en effectuant une multiplication de champ de Galois sur le texte chiffré et une valeur dérivée de la clé.

5. Vecteur d'initialisation (VI) : GCM utilise un vecteur d'initialisation pour démarrer le compteur à une valeur aléatoire. Le VI doit être unique pour chaque opération de chiffrement pour empêcher les attaquants de deviner la valeur du compteur.

6. Nonce : GCM utilise un nonce comme partie de l'entrée pour générer la balise d'authentification. Le nonce doit être différent pour chaque opération de chiffrement, mais n'a pas besoin d'être secret.

Ensemble, ces éléments permettent à GCM de fournir la confidentialité, l'authenticité et l'intégrité des messages chiffrés.[34]

II.10 Chiffrement par bloc

Les opérations de GCM dépendent du choix d'un chiffrement par bloc symétrique sous-jacent et peuvent donc être considérées comme un mode de fonctionnement (mode, abrégé) du chiffrement par bloc. La clé GCM est la clé de chiffrement par bloc (la clé, abrégée).

Pour une clé donnée, le chiffrement par bloc sous-jacent du mode se compose de deux fonctions qui sont inverses l'une de l'autre. Le choix du chiffrement par bloc inclut la désignation de l'une des deux fonctions du chiffrement par bloc comme fonction de chiffrement direct, comme dans la spécification de l'algorithme AES dans la référence [35]. GCM n'utilise pas la fonction de déchiffrement inverse.

La fonction de chiffrement direct est une permutation sur des chaînes de bits de longueur fixe ; les chaînes sont appelées blocs. La longueur d'un bloc est appelée taille de bloc. La clé est notée K, et la fonction de chiffrement direct résultante du chiffrement par bloc est notée CIPHK.

Le chiffrement par bloc sous-jacent doit être approuvé, la taille de bloc doit être de 128 bits, et la taille de la clé doit être d'au moins 128 bits. La clé doit être générée de manière uniforme au hasard, ou presque uniformément au hasard, c'est-à-dire de telle sorte que chaque clé possible soit (presque) également susceptible d'être générée.

Par conséquent, la clé sera fraîche, c'est-à-dire différente de toute clé précédente, avec une forte probabilité. La clé doit être secrète et doit être utilisée exclusivement pour GCM avec le chiffrement par bloc choisi [35].

II.11 Deux fonctions GCM

Les deux fonctions qui composent GCM sont appelées chiffrement authentifié et déchiffrement authentifié. La fonction de chiffrement authentifié chiffre les données confidentielles et calcule une étiquette d'authentification à la fois sur les données confidentielles et sur toutes les données supplémentaires non confidentielles. La fonction de déchiffrement authentifié déchiffre les données confidentielles, sous réserve de la vérification de l'étiquette.

Une implémentation peut restreindre l'entrée aux données non confidentielles, c'est-à-dire sans aucune donnée confidentielle. La variante résultante de GCM s'appelle GMAC. Pour GMAC, les fonctions de chiffrement et de déchiffrement authentifié deviennent les fonctions

de génération et de vérification d'une étiquette d'authentification sur les données non confidentielles [34].

II.11.1 Fonction de chiffrement authentifié

Données d'entrées : Après avoir sélectionné un chiffrement par blocs approuvé et une clé, il y a trois chaînes d'entrée pour la fonction de chiffrement authentifié :

• un texte en clair, noté P ;

• des données supplémentaires authentifiées (AAD), notées A ;

• un vecteur d'initialisation (IV), noté IV.

Le texte en clair et les données supplémentaires authentifiées (AAD) sont les deux catégories de données que GCM protège. GCM protège l'authenticité du texte en clair et des données supplémentaires authentifiées ; GCM protège également la confidentialité du texte en clair, tandis que les données supplémentaires authentifiées sont laissées en clair. Par exemple, dans un protocole de réseau, les données supplémentaires authentifiées peuvent inclure des adresses, des ports, des numéros de séquence, des numéros de version du protocole et d'autres champs qui indiquent comment le texte en clair doit être traité.

Le vecteur d'initialisation (IV) est essentiellement un nonce, c'est-à-dire une valeur qui est unique dans le contexte spécifié, ce qui détermine une invocation de la fonction de chiffrement authentifié sur les données d'entrée à protéger [34].

Données de sorties :

Les deux chaînes de bits suivantes constituent les données de sortie de la fonction de chiffrement authentifié :

• Un texte chiffré, noté C, dont la longueur en bits est la même que celle du texte en clair.

• Un tag d'authentification, ou tag, en abrégé, noté T.

La longueur en bits du tag, notée t, est un paramètre de sécurité. En général, t peut prendre l'une des cinq valeurs suivantes : 128, 120, 112, 104 ou 96. Pour certaines applications, t peut être 64 ou 32.

Une implémentation ne doit pas prendre en charge des valeurs pour t qui diffèrent des sept choix de la phrase précédente. Une implémentation peut limiter son support à seulement l'une de ces valeurs. Une seule valeur fixe pour t choisie parmi les choix pris en charge doit être associée à chaque clé [34].

II.11.2 Fonction de déchiffrement authentifié

Après avoir sélectionné un chiffrement par blocs approuvé, une clé et une longueur de tag associée, les entrées pour la fonction de déchiffrement authentifié sont les valeurs de IV, La sortie est l'une des suivantes :

• Le texte en clair P qui correspond au texte chiffré C.

• Un code d'erreur spécial, noté FAIL dans ce document.

La sortie P indique que T est le tag d'authentification correct pour IV, A et C ; sinon, la sortie est FAIL [34].

II.12 Primitives pour la confidentialité et l'authentification

Le mécanisme pour la confidentialité du texte en clair dans GCM est une variation du mode compteur, avec une fonction d'incrémentation particulière, notée inc32, pour générer la séquence nécessaire de blocs de compteur. Le premier bloc de compteur pour le chiffrement du texte en clair est généré en incrémentant un bloc qui est généré à partir de l'IV.

Le mécanisme d'authentification dans GCM est basé sur une fonction de hachage appelée GHASH1, qui comporte une multiplication par un paramètre fixe appelé la sous-clé de hachage, dans un champ Galois binaire.

La sous-clé de hachage, notée H, est générée en appliquant le chiffrement par blocs au bloc "zéro". L'instance résultante de cette fonction de hachage, notée GHASHH, est utilisée pour compresser un encodage des données supplémentaires authentifiées et du texte chiffré en un seul bloc, qui est ensuite chiffré pour produire le tag d'authentification.

GHASH est une fonction de hachage avec clé mais pas, à elle seule, une fonction de hachage cryptographique. Cette recommandation n'approuve GHASH que pour une utilisation dans le contexte de GCM [34].

Les valeurs intermédiaires dans l'exécution des fonctions GCM doivent être secrètes. En particulier, cette exigence exclut un système dans lequel GCM est implémenté en utilisant la sous-clé de hachage publiquement pour une autre fin, par exemple comme une valeur imprévisible ou comme une valeur de vérification d'intégrité sur la clé [34].

II.13 Fonction GHASH

1.Étapes :

1. Soit X1, X2, ..., Xm-1, Xm la séquence unique de blocs telle que X = X1 || X2 || ... || Xm-1 || Xm.

2. Soit Y0 le "bloc zéro",0^{128}.

3. Pour i = 1, ..., m, soit Yi = (Yi-1 ⊕ Xi) • H.

4. Retourner Ym.

En effet, la fonction GHASH calcule X1•Hm ⊕ X2•Hm-1 ⊕ ... ⊕ Xm-1•H2 ⊕ Xm•H. Décrit des méthodes pour optimiser les implémentations de GHASH à la fois en matériel et en logiciel.

La fonction GHASH est illustrée dans la FigureII.12 ci-dessous, sans le bloc zéro, Y0, dont le XOR avec X1 ne modifie pas X1[34].

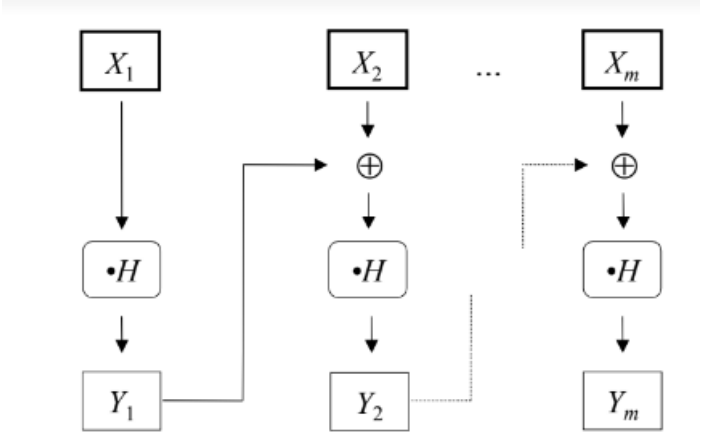


Figure II. 12 : fonction de **GHASHH** [35].

II.14 Fonction GCTR [35]

1.Étapes

1. If X is the empty string, then return the empty string as Y.
2. Let $n = \lceil \text{len}(X)/128 \rceil$.
3. Let $X_1, X_2, \ldots, X_{n-1}, X_n^*$ denote the unique sequence of bit strings such that
   $X = X_1 \| X_2 \| \ldots \| X_{n-1} \| X_n^*$;
   $X_1, X_2, \ldots, X_{n-1}$ are complete blocks.[2]
4. Let $CB_1 = ICB$.
5. For $i = 2$ to n, let $CB_i = \text{inc}_{32}(CB_{i-1})$.
6. For $i = 1$ to $n-1$, let $Y_i = X_i \oplus \text{CIPH}_K(CB_i)$.
7. Let $Y_n^* = X_n^* \oplus \text{MSB}_{\text{len}(X_n^*)}(\text{CIPH}_K(CB_n))$.
8. Let $Y = Y_1 \| Y_2 \| \ldots \| Y_n^*$.
9. Return Y.

Dans les étapes 1 et 2, la chaîne d'entrée de longueur arbitraire est partitionnée en une séquence de blocs autant que possible, de sorte que seule la chaîne la plus à droite dans la séquence puisse être un "bloc partiel". Dans les étapes 3 et 4, la fonction d'incrémentation de 32 bits est itérée sur le bloc initial d'entrée de compteur pour générer une séquence de blocs de compteur ; le bloc d'entrée est le premier bloc de la séquence. Dans les étapes 5 et 6, le chiffrement par blocs est appliqué aux blocs de compteur et les résultats sont XORés avec les blocs (ou bloc partiel) correspondants de la partition de la chaîne d'entrée. Dans l'étape 7, la séquence de résultats est concaténée pour former la sortie.

La Figure II.13 ci-dessous illustre la fonction GCTR [34].

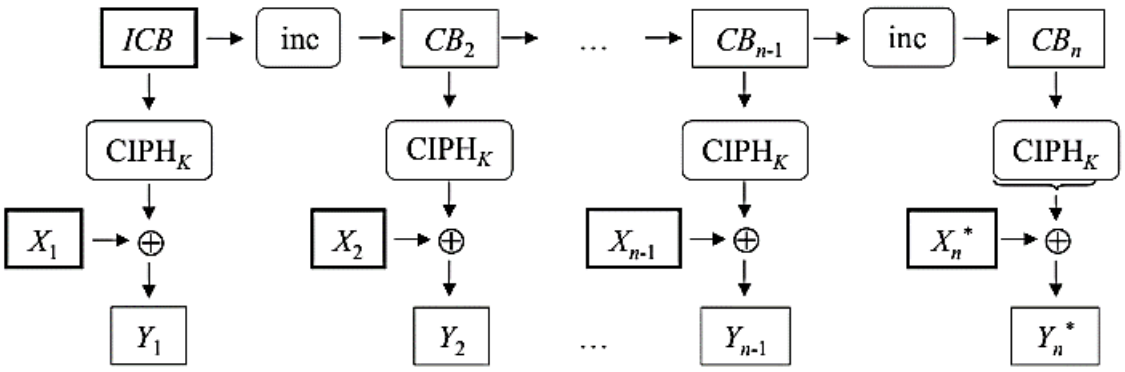


Figure II. 13 : LA FOCTION GCTRK [35]

II.15 Algorithme pour la fonction de chiffrement authentifié

1.Étapes

1. Let $H = \text{CIPH}_K(0^{128})$.
2. Define a block, J_0, as follows:
   If len(IV)=96, then let $J_0 = IV \| 0^{31} \| 1$.
   If len(IV) ≠ 96, then let $s = 128\lceil \text{len}(IV)/128 \rceil - \text{len}(IV)$, and let
   $J_0 = \text{GHASH}_H(IV \| 0^{s+64} \| [\text{len}(IV)]_{64})$.
3. Let $C = \text{GCTR}_K(\text{inc}_{32}(J_0), P)$.
4. Let $u = 128 \cdot \lceil \text{len}(C)/128 \rceil - \text{len}(C)$ and let $v = 128 \cdot \lceil \text{len}(A)/128 \rceil - \text{len}(A)$.
5. Define a block, S, as follows:
   $$S = \text{GHASH}_H(A \| 0^v \| C \| 0^u \| [\text{len}(A)]_{64} \| [\text{len}(C)]_{64}).$$
6. Let $T = \text{MSB}_t(\text{GCTR}_K(J_0, S))$.
7. Return (C, T).

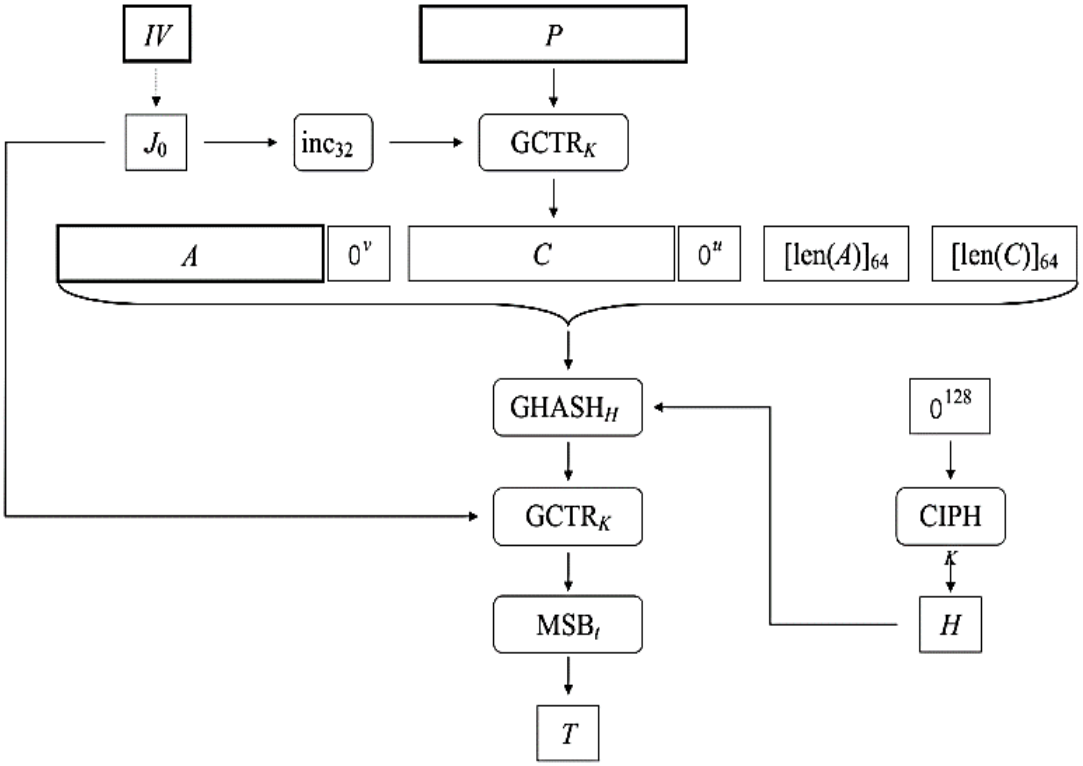


Figure II. 14 : GCM-AEK (IV, P, A) = (C, T) [34].

II.16 Algorithme pour la fonction de déchiffrement authentifié

1.Étapes

1. If the bit lengths of IV, A or C are not supported, or if $\text{len}(T) \neq t$, then return FAIL.
2. Let $H = \text{CIPH}_K(0^{128})$.
3. Define a block, J_0, as follows:
   If $\text{len}(IV)=96$, then $J_0 = IV \,\|\, 0^{31} \,\|1$.
   If $\text{len}(IV) \neq 96$, then let $s = 128\lceil \text{len}(IV)/128\rceil - \text{len}(IV)$, and
   $J_0 = \text{GHASH}_H(IV \| 0^{s+64} \| [\text{len}(IV)]_{64})$.
4. Let $P = \text{GCTR}_K(\text{inc}_{32}(J_0), C)$.
5. Let $u = 128 \cdot \lceil \text{len}(C)/128 \rceil - \text{len}(C)$ and let $v = 128 \cdot \lceil \text{len}(A)/128 \rceil - \text{len}(A)$.
6. Define a block, S, as follows:
   $$S = \text{GHASH}_H(A \,\|\, 0^v \,\|\, C \,\|\, 0^u \,\|\, [\text{len}(A)]_{64} \,\|\, [\text{len}(C)]_{64})$$
7. Let $T' = \text{MSB}_t(\text{GCTR}_K(J_0, S))$.
8. If $T = T'$, then return P; else return $FAIL$.

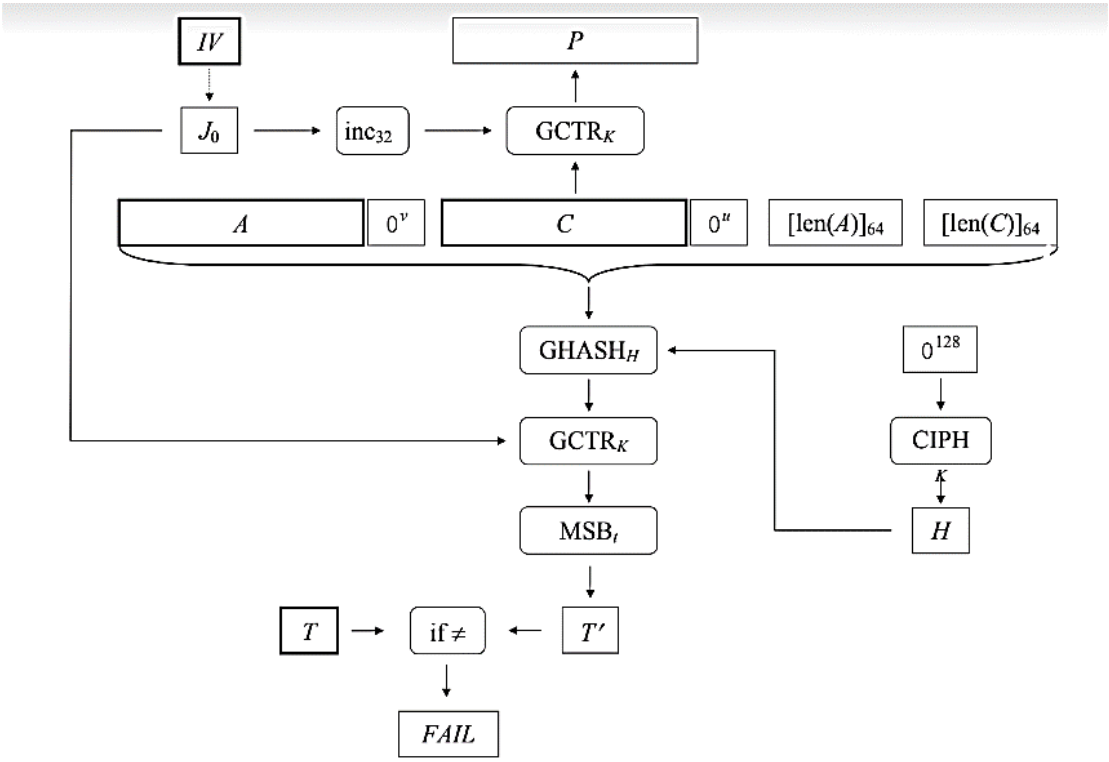


Figure II. 15 : GCM-ADK (IV, C, A, T) = P or FAIL [34].

II.17 Conclusion

Tout à fait, ce chapitre a couvert deux sujets importants en informatique : la cryptographie et le traitement D'image médicale avec la technique AES-GCM.

En conclusion, la technique de cryptage AES-GCM offre une solution robuste et sécurisée pour la transmission d'images médicales sensibles. En utilisant cette méthode de chiffrement pour protéger les images médicales, on peut s'assurer que les données des patients sont sécurisées et confidentielles. Cependant, il est important de souligner que la sécurité des données médicales dépend également de la mise en place de protocoles de sécurité appropriés pour la gestion des clés de chiffrement et la protection des données médicales pendant leur stockage et leur transmission.

Chapitre III :

Résultats de simulation

III.1 Introduction

Après avoir exposé nos méthodes de cryptage et de transmission d'image dans les chapitres précédents, nous abordons maintenant la réalisation et l'analyse de notre application. Cette dernière utilise la norme de cryptage évolué AES (Advanced Encryption Standard) en mode Galois/Counter (GCM) pour garantir la confidentialité et l'authentification de l'origine des données.

Dans ce chapitre, nous décrivons notre application concrète ainsi que les différents outils nécessaires à son développement.

III.2 Schéma générale de l'application

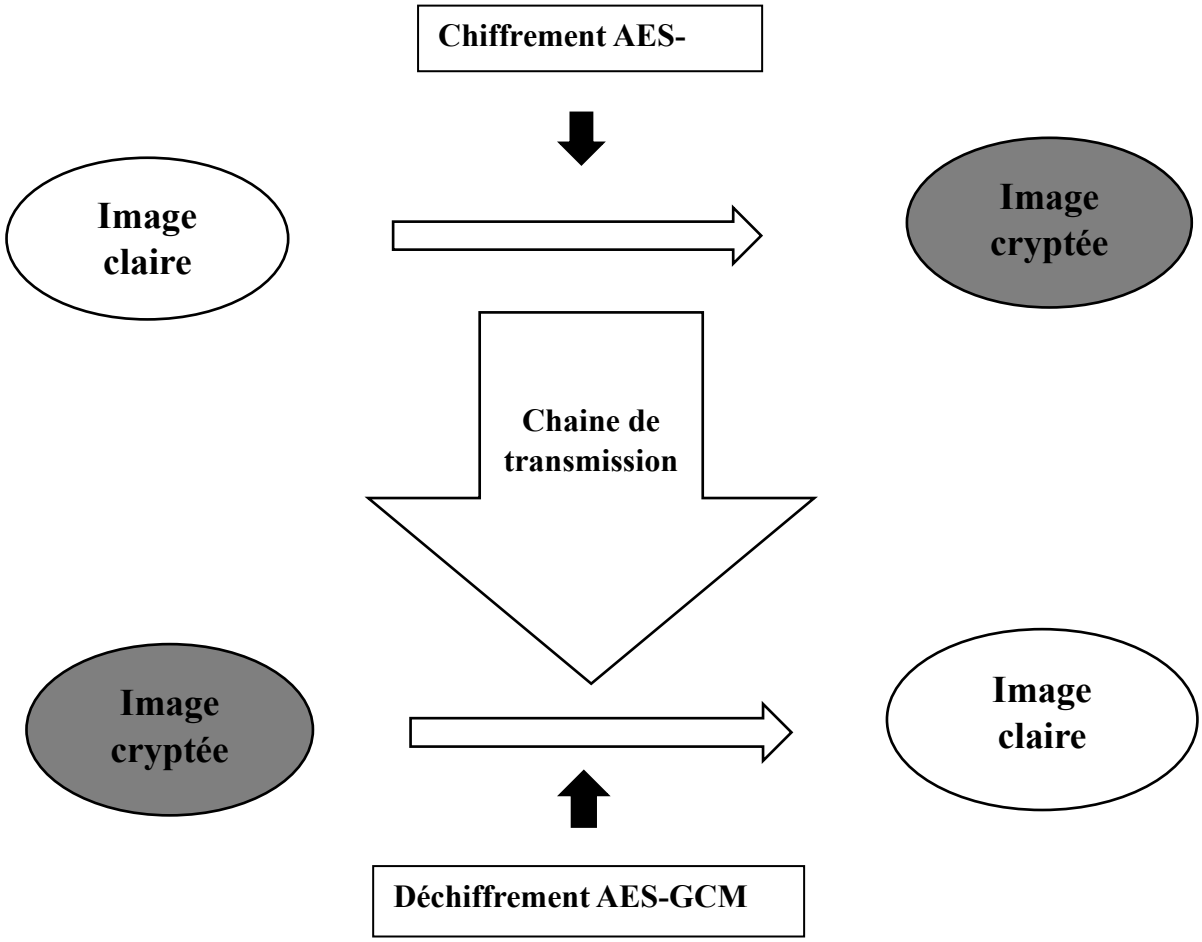


Figure III. 1 : Schéma générale de l'application

III.3 Présentation et comparaison des deux méthodes (AES) Et (AES-GCM)

III.3.1 AES

En plus de fournir un niveau de sécurité élevé, le système AES est capable de chiffrer et déchiffrer rapidement de grandes quantités de données, ce qui le rend adapté à une utilisation dans des dispositifs grand public tels que les ordinateurs portables, aussi bien au niveau du matériel (hardware) que du logiciel (software) [36].

III.3.2 AES-GCM :

AES-GCM est réputé résistant aux attaques d'adversaires qui peuvent choisir de manière adaptative le texte source. Toutefois, la principale préoccupation en matière de sécurité est qu'une clé ne doit jamais être dupliquée. Cette préoccupation peut être partiellement résolue en désactivant l'utilisation d'AES-GCM avec des clés configurées de manière statique.

Bien que le chiffrement en mode GCM présente des avantages évidents par rapport à AES, certains utilisateurs peuvent ne pas lui accorder suffisamment de confiance pour le recommander. Nous pouvons répondre à cette préoccupation en nous concentrant sur l'application concrète de l'algorithme AES-GCM et en examinant ses propriétés pour vérifier qu'il est sans erreur. Nous pourrons ensuite évaluer son fonctionnement et ses avantages par rapport à un système de chiffrement AES [36].

Les figures au-dessous montrent plusieurs images médicales au niveau de gris :

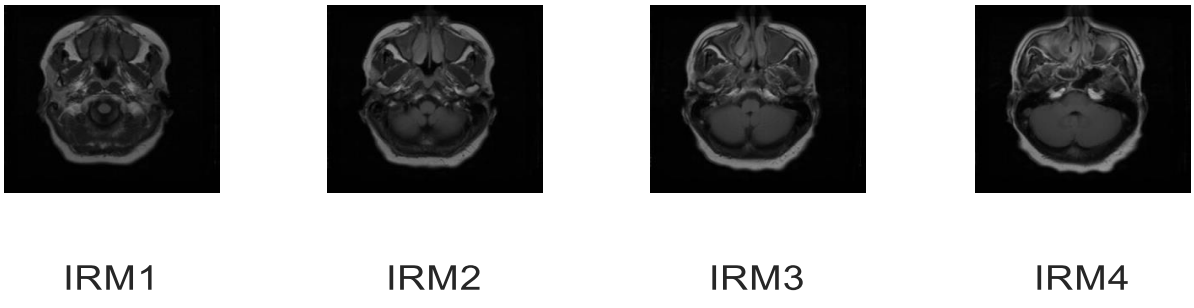


Figure III. 2 : images médicales au niveau de gris.

III.4 Chiffrement et déchiffrement AES-GCM

La figure au-dessous montre nos images au niveau de gris sont cryptées et décryptées en utilisant la méthode AES-GCM.

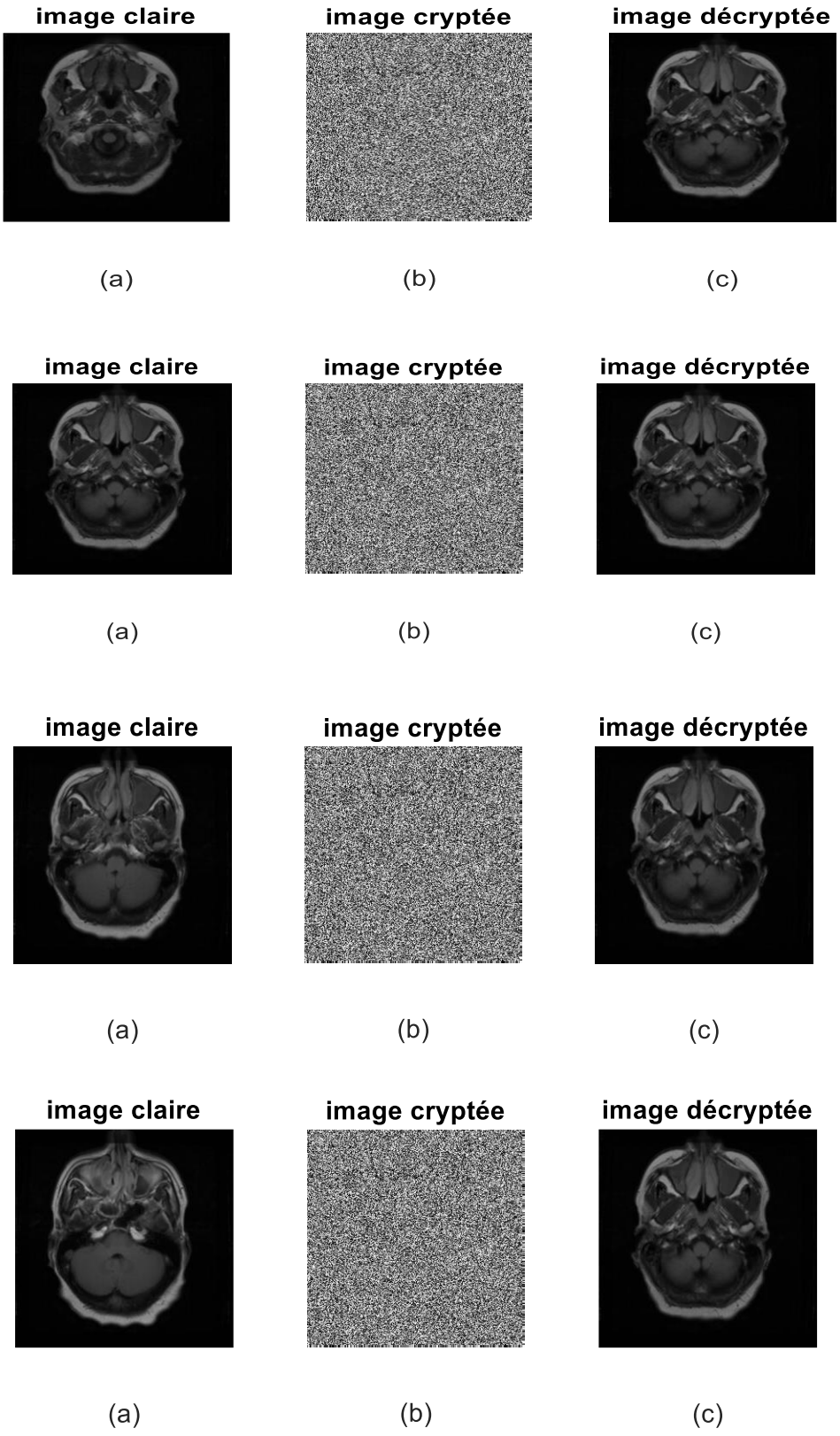


Figure III. 3 : Des images médicales cryptées et décryptées en utilisant la méthode AES-GCM.

III.5 Les tests statistiques

On utilise des différents tests pour nos images cryptés et décryptées tell que : l'histogramme, la corrélation, l'entropie, NPCR et UACI

III.5.1 L'histogramme

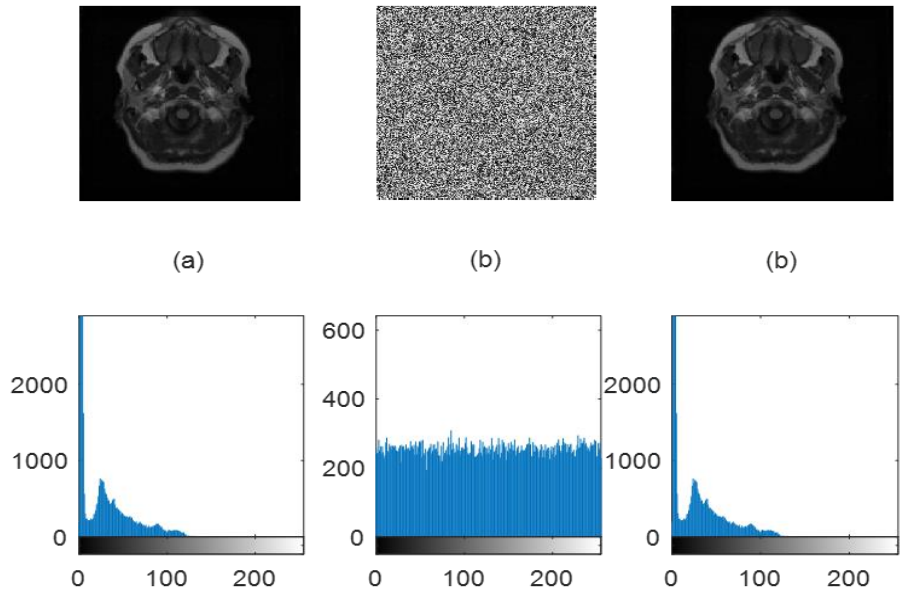
L'histogramme est une représentation graphique qui permet de connaître la répartition des intensités lumineuses des pixels [23].

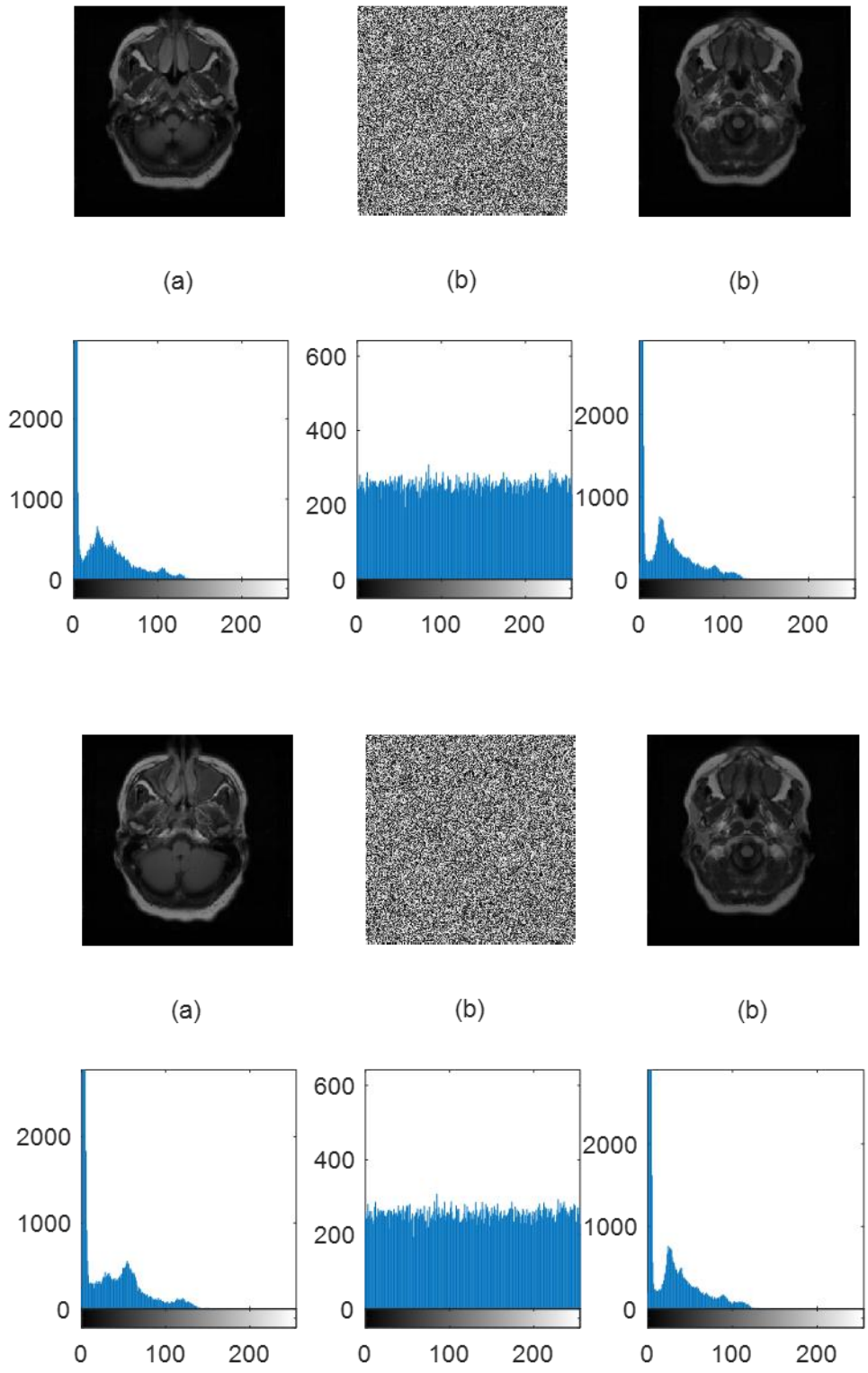
Cinq images ont été utilisées dans l'analyse, Les tracés des histogrammes des images et les images cryptées sont montrés dans les figures au-dessous en utilisant les deux méthodes (AES) et (AES-GCM) [36] :

- L'axe horizontal en abscisses représente le niveau de gris de chaque image.

- L'axe vertical en ordonné représente le nombre de pixel de chaque image.

Les figures si dessus nous montre les histogrammes des images claires, cryptée et décryptée.




(a)
(b)
(b)
2000
1000
0
600
400
200
0
100
200
(a)
(b)
(b)

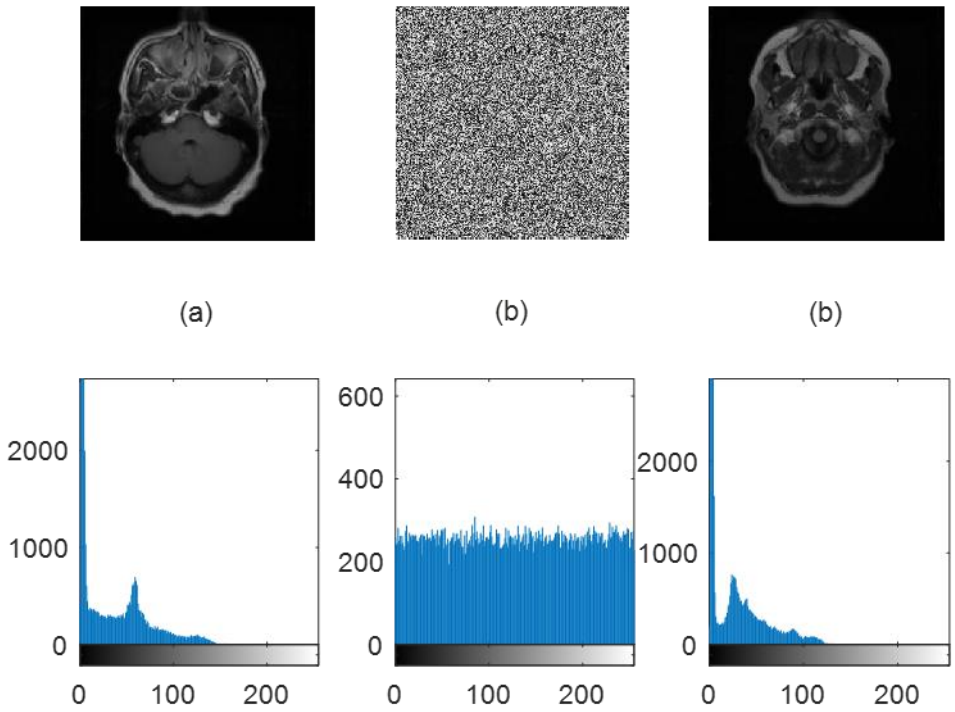


Figure III. 4: les histogrammes des images claires, chiffrées et déchiffrée.

Les résultats montrent que l'histogramme de l'image chiffrée est homogène après le chiffrement, de manière que l'attaquant ne peut extraire aucune information de l'histogramme de l'image chiffrée [36].

Les histogrammes des images cryptées illustrées sur la figure 3.4 Sont presque uniformes, ce qui suggère que le système proposé a pu sécuriser les données médicales sans divulguer aucune information sur les données sources, ce qui rend difficile pour les pirates de se procurer les données médicales sensibles [38].

De plus, les histogrammes des images décryptées présentées sont presque similaires aux histogrammes d'image d'origine, ce qui montre que le mécanisme proposé a pu récupérer les données médicales d'origine sans aucune modification significative ne soit apportée à l'image d'origine [38].

III.5.2 Les paramètres d'évaluations

III.5.2.1 L'entropie

L'entropie est une mesure statistique du caractère aléatoire qui peut être utilisée pour caractériser la texture de l'image d'entrée [36].

Son équation est :

$$H(m) = \sum_{i=0}^{2^{n-1}} p(m)_i log_2 \frac{1}{p(m_i)}$$

$$H(m) = -\sum_{i=0}^{2n-1} pi \log_2(pi)$$

Où pi définit la probabilité d'un pixel et n est le nombre de bits dans chaque pixel.

Tableau III. 1 : Les valeurs d'entropie des images claires, cryptée et décryptée.

Image	Type	Entropie de L'image Claire	Entropie de L'image Cryptée	Entropie de L'image Décryptée
Image « IRM-1 »	Niveau de Gris	5.0545	7.9888	3
Image « IRM-2 »	Niveau de Gris	5.0989	7.9888	3
Image « IRM-3 »	Niveau de Gris	5.2869	7.9888	3
Image « IRM-4 »	Niveau de Gris	5.3543	7.9888	3

La valeur d'entropie doit être très proche de 8, car si l'entropie est inférieure à 8, il y a un degré de prévisibilité, et pour une image chiffrée de 256 symboles, elle ne peut pas fournir de sécurité contre les attaques d'entropie [36].

III.5.2.2 Corrélation

Pour étudier la corrélation entre les pixels.

$$r_{xy} = cov(x, y) / (\sqrt{D(x)D(y)}$$

Tel que : $D(x) = \frac{1}{n}\sum_{i=1}^{N}\big(x_i - E(x)\big)^2$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i)$$

$$cov(x,y) = \frac{1}{n} = \sum_{i=1}^{N} ((x_i - E(x)(y_i - E(y))$$

La corrélation d'images est une technique expérimentale permettant 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 [38].

Les coefficients de corrélation de chaque paire ont été calculées en utilisant les formules suivantes :

$$r_{xy} = cov(x,y)(\sqrt{D(x)D(y)}$$

Tel que : $D(x) = \frac{1}{n}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i)$$

$$cov(x,y) = \frac{1}{n} = \sum_{i=1}^{N} ((x_i - E(x)(y_i - E(y))$$

Tel que :

r : la corrélation.

cov : la covariance.

E : l'espérance mathématique.

D : la variance.

x, y : les valeurs des pixels des images.

Les figures ci-dessus montrent les courbes des corrélations entre les images :

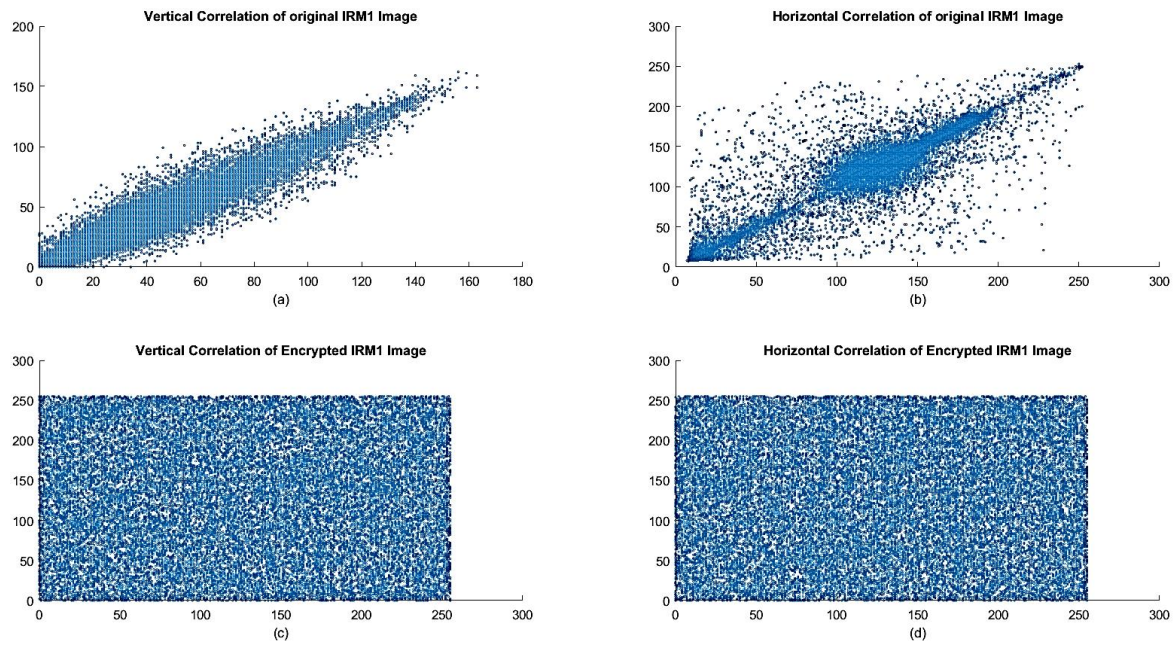


Figure III. 5: les corrélations de l'image IRM-1 claires, chiffrées et déchiffrée.

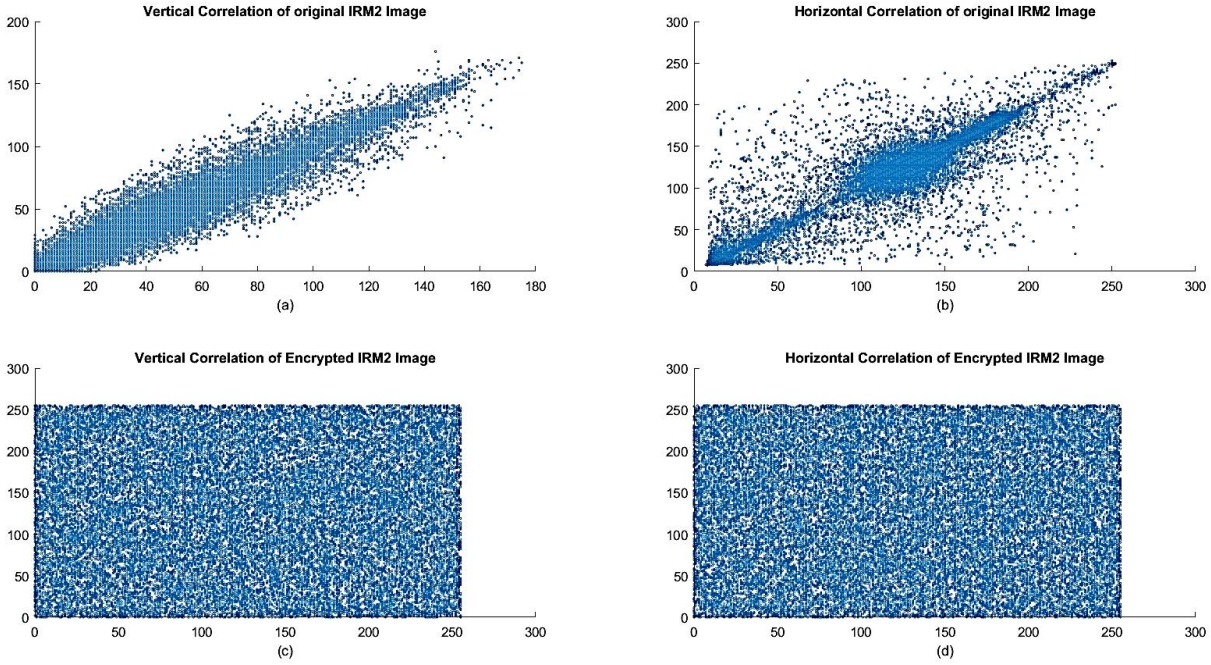


Figure III. 6: les corrélations de limages IRM-2 claires, chiffrées et déchiffrée.

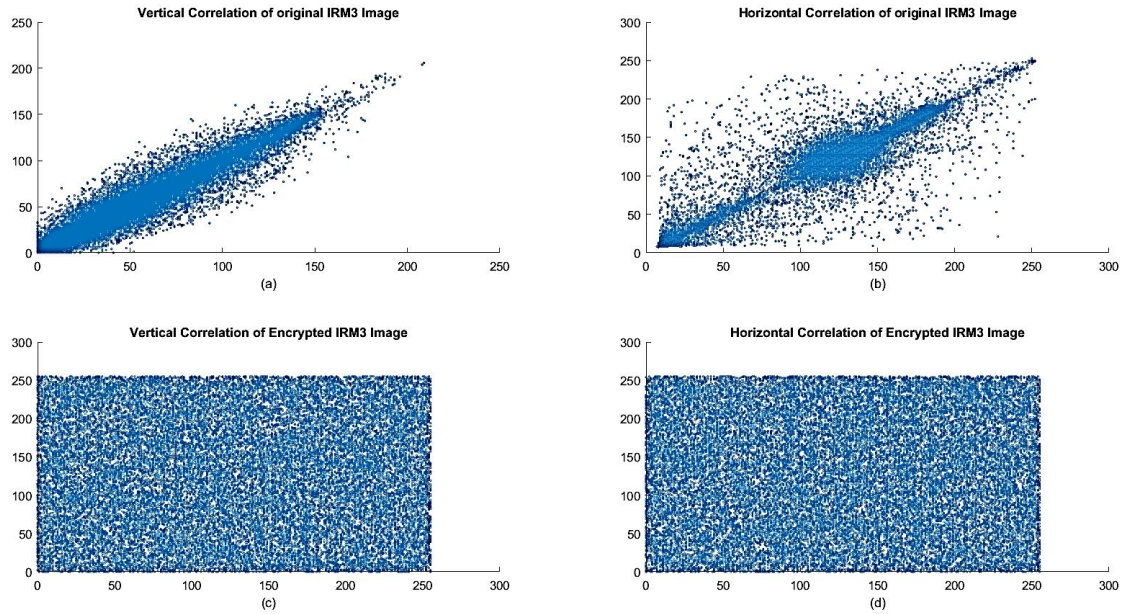


Figure III. 7: les corrélations de limages IRM-3 claires, chiffrées et déchiffrée.

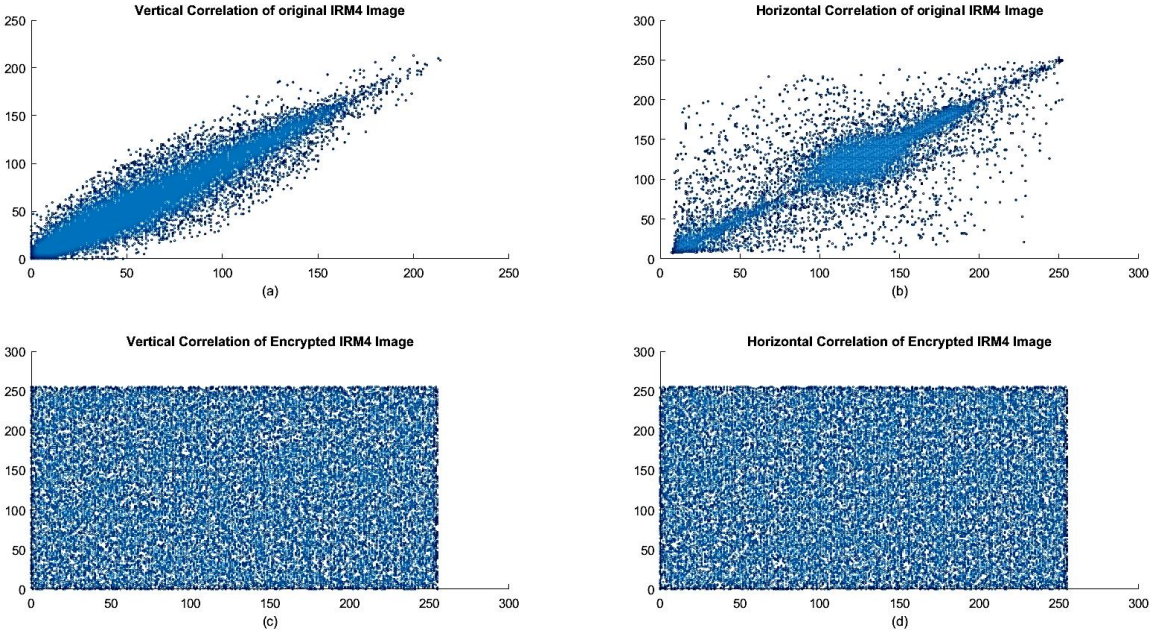


Figure III. 8: les corrélations de limages IRM-4 claires, chiffrées et déchiffrée.

Les pixels de l'image Cryptée comme le montre la figure 3.8 sont distribués et la corrélation entre eux est presque égale à zéro, ce qui suggère que le Crypto système proposé a réussi à rompre efficacement la corrélation entre les pixels de l'image originale et à les disperser en sécurisant les données d'image médicale contre tout accès non autorisé.

III.6 Conclusion

Ce chapitre résume l'essentiel de nos recherches sur la protection des images et comment

Bien transmettre sans l'influence des erreurs et du bruit de canal, nous proposons un nouvel Algorithme de cryptage d'image basé sur la méthode AES et AES – GCM

Conclusion générale

Conclusion :

Aujourd'hui, le monde a fait de grands progrès dans le domaine des réseaux de communication. Par conséquent, la plupart des recherches se sont concentrées sur l'amélioration de la cryptographie et des méthodes de transmission pour accroître la sécurité et la confidentialité des données.

La méthode que nous introduisons dans cette mémoire est appelée cryptage d'image basé sur la méthode AES et AES-GCM et nous évaluons ses performances en utilisant l'algorithme sur Matlab R2016b.

Cela nous a conduit à effectuer un ensemble de tests qui ont montré une bonne robustesse de notre algorithme, nous avons donc obtenu plusieurs résultats satisfaisants à partir de ces simulations, évaluant les paramètres : entropie, corrélation, NPCR et UACI ont été utilisés pour montrer Crypter l'image et l'image d'origine, donc nous obtenons un cryptage efficace pour crypter notre image.

Le travail entrepris dans cet article ne constitue pas une fin en soi, mais ouvre plutôt la porte à de futures contributions. Nous allons globalement améliorer notre approche de tous les formats d'images, et nous espérons continuer à utiliser de nouvelles idées pour mieux contribuer à optimiser la rapidité des opérations de cryptage et transmission.

Les résultats expérimentaux ont montré que l'algorithme proposé présente un niveau élevé de sécurité et de performance

Références

Références

[1] Schneier.B, " Cryptographie appliquée : Algorithme, protocoles et codes sources en C". Thèse de doctorat, Université ferhat abbas setif-1, 2001.

[2] Nawal. N, "Conception et réalisation d'un système collaboratif pour les experts métier à Base d'agent et des algorithmes de cryptage". Thèse de doctorat, Université ahmes ben bella d'oran, 2017.

[3] Dumont. R, " Cryptographie et Sécurité informatique", livre informatique, 2009 - 2010.

[4] Dumont. R, " Cryptographie et Sécurité informatique", Mémoire de master, Université de Liège, 2010

[5] Bekkouche. T, "Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes". Thèse de doctorat, Université ferhat abbas setif-1.,2010

[6] Guermat. N, "Implémentation d'un algorithme de cryptage sur un circuit FPGA ", Mémoire de master, Université Mohamed Boudiaf - M'sila,2017

[7] Mahdi .H," étude et comparaison des principaux systèmes de cryptage et les techniques y afférentes", Mémoire de master, Université mohamed boudif, m'sila ,2015

[8] Hacini. S, "Implémentation d'algorithmes de Cryptographie", Mémoire de master,Université Abou Bakr Belkaid– Tlemcen Faculté, 2013-2014

[9] Hill Lester. S, "Cryptography in an Algebraic Alphabet", American Mathematical Monthly-N36-P306à312, 1929.

[10] https://www.apprendre-en-ligne.net/crypto/vigenere/index.html

[11] Lebsir. N, "Cryptosystème Hybride Avancé pour les Réseaux Mobiles Application pour la gestion des comptes bancaires", Mémoire de master ,Université Mohammed Seddik Ben Yahia de Jijel.

[12] Boutiouta. A, "sécurité et géstion de la mobilité dans le réseau GSM". Thèse d'ingéniorat Institue de télécommunication d'ORAN 2006.

[13] B. Rabab, "Sécurité des images Numériques compressées JPEG", Thèse de doctorat, Université Djillali Liabès de Sidi Bel Abbes, 2019.

[14] J. Katz and Y. Lindell, "Introduction to modern cryptography", CRC press, 2007.

[15] Heys. H, “Analysis of the statistical cipher feedback mode of block ciphers”, IEEE Transactions on Computers, Vol. 52, No. 1, 2003.

[16] L. Bouchenafa, F. Z. Haroun et A. Krobba, “Amélioration de la sécurité du système de vérification du locuteur dans un environnement mobile”, Mémoire de master , Universite Yahia Fares - Medea, 2021.

[17] A. Belarbi, A. Benaida, "Étude comparative de systèmes cryptographiques", Mémoire de master, Université Tahar Moulay - Saida, 2021.

[18] Vincent. R, Joan .D. "Advanced encryption standard. Proceedings of Federal Information Processing Standards Publications", National Institute of Standards and Technology, pages 19–22, 2001.

[19] Kebir. B, Rahmouni. S, "Développement d’une application pour l’échange des messages sécurisés", Mémoire de master, Université Abou Bakr Belkaid– Tlemcen, 2015.

[20] Khouildat. H, Djebaili .K,"Méthode de cryptage d’image basée sur la permutation et la matrice de Householder . diplôme de master,Faculté des Nouvelles Technologies de l’information, 2019

[21] Boumachta-I, "Application du protocole d’EL GAMAL:Chiffrement /déchiffrement d’images", Mémoire de master, Université badji mokhtar annaba , 2018.

[22] Belkadi .I ,Amiar .n, "Cryptage d’image par considération des plans de bits des pixels séparément par ordre de leurs poids avec une clé publique de taille", Mémoire de master,Université larbi ben m’hidi ,2017-2018

[23] H. Frikha et I. Tellouche, "Cryptage des images médicales à la base des cartes chaotiques", Mémoire de master, Universite Mohamed Seddik Ben Yahia - Jijel, 2022.

[24] M. A. Haidekker, "Medical imaging technology", Springer New York, NY, 2013.

[25] I. Peretti, “Bases physiques de l’imagerie médicale : imagerie analogique / imagerie Numérique”, Polycopie de cours, CHU Lariboisière-Fernand Widal, faculté de Médecine Paris Diderot, 2016.

[26] http://www.radiologieperpignan.fr/wpcontent/uploads/photogallery/Photos,(2020) consulté le 15-05-2023.

[27] E. Cherrier, “Estimation de l’état et des entrées inconnues pour une classe de systèmes non linéaires”, Thèse de doctorat, Institut National Polytechnique de Lorraine,2006.

[28] J. Hodel, "Formes progressives de sclérose en plaques : place actuelle de l’IRM pour le diagnostic positif et différentiel", Revue neurologies.fr, 2018.

[29] M. Mahmoud, "Evaluation des images chiffres par l’algorithme AES-128 et AES-256", Mémoire de master Université Larbi Tébessi – Tébessa, 2021.

[30] M. Boukhatem, "Application des techniques de cryptage pour la transmission sécurisée d’images MSG", Mémoire de master, Université mouloud mammeri – tizi ouzou, 2015.

[31] Z. A. Alaoui Ismaili, A. Moussa, " Self-Partial and Dynamic Reconfiguration Implementation for AES using FPGA", International Journal of Computer Science Issues (IJCSI), Volume 1, pp 33-40, August 2009.

[32] Serge WACKER – C2I niveau, Les formats d'images numériques, http://www.montpellier.iufm.fr/technoprimaire, consulté le : 02/04/2022.

[33] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: Galois / Counter Mode (GCM) and GMAC", NIST Special Publication 800-38D, November 2007.

[34] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", NIST FIPS 197-upd1, November 26, 2001.

[35] N. Arbaoui, N. Attala, "Cryptage et transmission des images satellitaires avec des canaux AWGN", Memoire de master, Université –Ain Temouchent- Belhadj Bouchaib, 2022

[36] http://www.photofiltrestudio.com/doc/histogramme.htm, consulté le : 05/06/2022

[37] A. Beloucif, "Contribution à l’étude des mécanismes cryptographiques", Thèse de doctorat, Université de Batna2, 2016.

[38] H. A. Zenasni. Y, Saim, "Chiffrement des images médicales par un crypto système basé sur la théorie du chaos", Mémoire master, Université Abou bekr belkaid – Tlemcen, 2021.