الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة عين تموشنت بلحاج بوشعيب
Université –Ain Temouchent- Belhadj Bouchaib
Faculté des Sciences et de Technologie
Département D'électronique et des Télécommunications

Mémoire de Fin d'Etudes

En vue de l'obtention du diplôme de Master en Télécommunication

Domaine : SCIENCES & TECHNOLOGIES
Filière : TELECOMMUNICATION
Spécialité : RESEAU ET TELECOMMUNICATION

Thème :

Cryptage et transmission des images satellitaires avec des canaux AWGN

Présenté par : Mr.Arbaoui Nadir
Mlle.Attala Nabila

Soutenu en Juin 2022 devant le Jury :

Dr Moulessehoul Wassila	M.C.B	U.A.T	Président
Dr.Slimani. Zohra	M.C.A	U.A.T	Examinateur
Dr Bengana Abdelfatih	M.C.A	U.A.T	Encadrant
Melle Abdi Hadjer	Doctorante	U.A.B.T	Co-Encadrante


بسم الله الرحمن الرحيم

DEDICACE01 :

J'aimerais dédier ce travail à mes très

Chers parents pour leur soutien

Et tous les efforts Qu'on m'a donnés le long de mon parcours

A mes chers frères : Zakaria, Ibrahim et Fayçal pour leur présence dans ma vie pour leurs encouragements permanents, et leur soutien moral

A mes tous mes proches

A mon binome nadir qui ma toujours

Soutenu et encouragé durant la réalisation de ce mémoire

A mes amies (malak, rachida, ghizlen, hanane, sara, houaria)

A tous mes enseignants qui ont fait leurs possibles

Pour nous Donner le maximum d'informations

Concernant notre étude

Attala Nabila

DEDICACE02 :

J'aimerais dédier ce travail à mes très

Chers parents pour leur soutien

Et tous les efforts Qu'on m'a donnés le long de mon parcours

A mon frère (Miloud), et ma belle sœur (aicha) pour leur présence dans ma vie.

A mon binome Nabila de son soutien tout au long de notre parcours universitaire et ses encouragements à moi

A mes tous mes proches amis

A tous mes enseignants qui ont fait leurs possibles

Pour nous Donner le maximum d'informations

Concernant notre étude

Araboui Nadir

Remerciement :

Avant tous, nous tenons à remercier Allah de nous avoir donné la chance de suivre le

Chemin de la science.

A l'issue de ce modeste travail, nous tiens à exprimer nos sincères

Remerciements à :

Notre encadreur, monsieur Bengana Fetih qui nous a guidés dans notre travail, et nous a beaucoup aidé par ses Orientations et ses précieux conseils pour l'élaboration De cette étude.

Je remercie aussi Melle Abdi Hadjer, pour sa collaboration en nous fournissant des données précises sur cette étude

Nous souhaitons aussi adresser nos remerciements à tous les enseignants de département de la science et technologie (Filière télécommunication) Qui ont participé à notre formation

Nous exprimons toute nos gratitude et nos respect aux membres de jury qui

Nous feront l'honneur d'apprécier ce modeste travail.

Résumé

Le développement des techniques de transmission utilisé dans la communication a permis de transmettre des informations importantes, telles que les images. Par conséquence, ces informations nécessitent un système de transmission et de protection robuste.

Dans ce mémoire, nous proposons un système pour la transmission des images satellitaire en utilisant une cryptosystème basé sur la méthode AES-GCM, Aussi, une technique de transmission se concentre sur l'OFDM, qui est une solution éprouvée et simple à implémenter. Finalement, on s'intéresse aux résultats expérimentaux tels que les tests statistiques et les tests différentiels montre l'efficacité de notre méthode.

Mots clés : cryptage d'image, clé, AES-GCM, image satellitaire, transmission d'image

Abstract

The development of transmission techniques used in communication has made it possible to transmit important information, such as images. Consequently, this information requires a robust transmission and protection system.

In this work, we propose a system for the transmission of satellite images using a crypto-system based on the AES-GCM method, also, a transmission technique focuses on OFDM, which is a proven and simple solution to implement.

Finally, we are interested in experimental results such as statistical tests and differential tests showing the effectiveness of our method.

Keywords: Image Encryption, Key, AES-GCM, satellite image, image transmission

ملخص

لقد أتاح تطوير تقنيات الإرسال المستخدمة في الاتصال نقل المعلومات المهمة ، مثل الصور. وبالتالي ، تتطلب هذه المعلومات نظام نقل وحماية قوي.

في هذه الأطروحة، نقترح نظامًا لنقل صور الأقمار الصناعية باستخدام طريقة تشفير تعتمد على طريقة AES-GCM ، وهو حل مجرب وبسيط للتنفيذ. أخيرًا، نحن مهتمون بالنتائج التجريبية مثل OFDMكما تركز تقنية الإرسال على ، الاختبارات الإحصائية والاختبارات التفاضلية التي توضح فعالية طريقتنا.

الكلمات المفتاحية: تشفير الصور ، المفتاح ، وضع عداد جالوا المتقدم للتشفير القياسي ، صورة الأقمار الصناعية ، نقل الصور

Table des matières

Liste des figures

Liste des tableaux

Introduction Générale

Introduction Générale:

Le monde connaît un développement rapide dans le domaine des technologies de l'information et des réseaux de communication, en particulier la croissance rapide des informations multimédia telles que la vidéo et les images transmises via ces réseaux.

La question est : comment protéger et transmettre des images sur des canaux de communication non sécurisés ? Par conséquent, il est nécessaire de crypter l'image avant de la transmettre via le réseau, puis d'appliquer la technologie de transmission basée sur la méthode OFDM.

Le domaine du chiffrement d'images a parcouru un long chemin dans ces dernières années, avec l'émergence de multiples techniques, dont chacune n'est pas garantie d'être exempte de faiblesses ou insensible aux méthodes d'attaque. C'est pourquoi les chercheurs développent constamment de nouveaux crypto systèmes pour minimiser ces problèmes.

Ceci est très attractif pour les utilisateurs, il est donc temps de voir quelles performances les techniques de modulation OFDM apporteront aux liaisons sans fil. Cette technique présente des avantages majeurs qui peuvent se résumer ainsi :

- Sélectivité en fréquence à haute immunité.
- Haute efficacité spectrale.
- Batailles multivoies.

Notre mémoire est organisé comme suit:

Dans le premier chapitre, nous présentons les concepts fondamentaux et la terminologie de la cryptographie dans un premier temps, puis nous présentons ces différents types, ainsi nous décrivons notre méthode utilisée pour le cryptage d'images, Enfin, nous présentons l'image satellitaire.

Le deuxième chapitre nous présentons un état de l'art sur les différents types de techniques d'accès multiples, Ensuit nous montrons en détaille notre méthode utilisée de l'OFDM et sa performance.

Le troisième chapitre commence par une description de logiciel utiliser, Puis nous présentons les résultats de cryptage et la transmission de différents types d'images montrent l'efficacité de nos méthodes.

CHAPITRE I
Chiffrement et Cryptage

Chapitre I

Chiffrement et cryptage

1. Introduction :

Avec le développement rapide de l'utilisation des réseaux de communication, une grande quantité d'informations, telles que des images numériques [1] , est transmise sur ce réseau. Dans ce cas, la nécessité de protéger et de protéger les informations personnelles est très importante, donc la meilleure solution à ce problème est d'utiliser un système de cryptage. [2]

2. Terminologie de la cryptographie

2.1 Cryptographie :

•La cryptographie est une science mathématique qui comprend deux branches : la cryptographie et la cryptanalyse [3]

2.1.1 Cryptographie :

• D'une manière générale, la cryptographie est une technique d'écriture qui utilise un chiffrement ou une clé de chiffrement pour écrire des messages chiffrés. La cryptographie est principalement utilisée pour protéger les messages considérés comme confidentiels. [4]

2.1.2 Cryptanalyse :

• Contrairement à la cryptographie, son but est de trouver du texte clair à partir du texte chiffré en déterminant l'erreur de l'algorithme utilisé [3].

2.1.3 La Clef :

C'est le paramètre en cause et autorisant les opérations de chiffrement et/ou de déchiffrement [3]

Le principe d’un algorithme de chiffrement ce montre dans la figure ci-dessus :

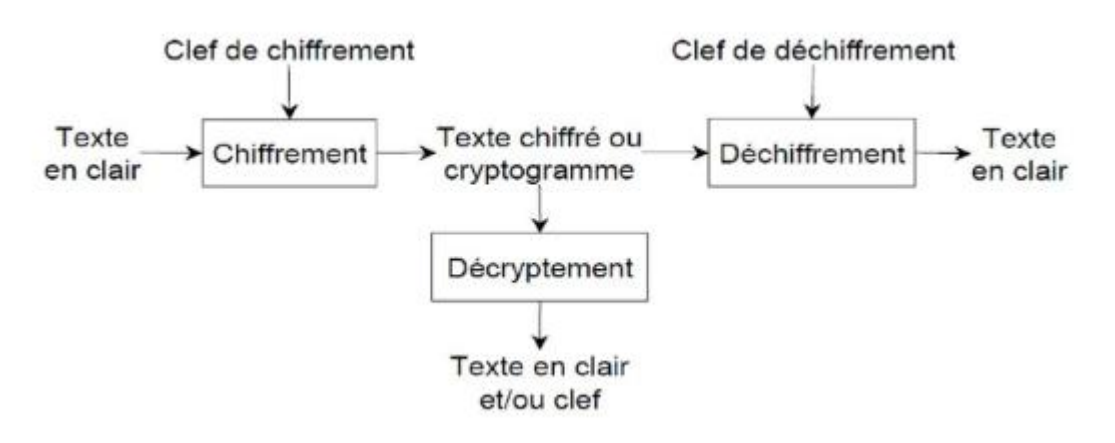

Figure 1.1: Principe générale d'un algorithme de chiffrement. [2]

3. Les différents types de cryptographie :

- Nous pouvons regrouper les systèmes de chiffrement en deux catégories:

3.1 La cryptographie classique :

Dans la cryptographie classique, la méthode et la clé de chiffrement ainsi que celle dedéchiffrement sont connues par l'émetteur et le destinataire. La plupart des méthodes dechiffrement classiques reposent sur deux principes essentiels : la substitution et transposition.

La figure ci-dessus montre les différentes méthodes de la cryptographie classique :

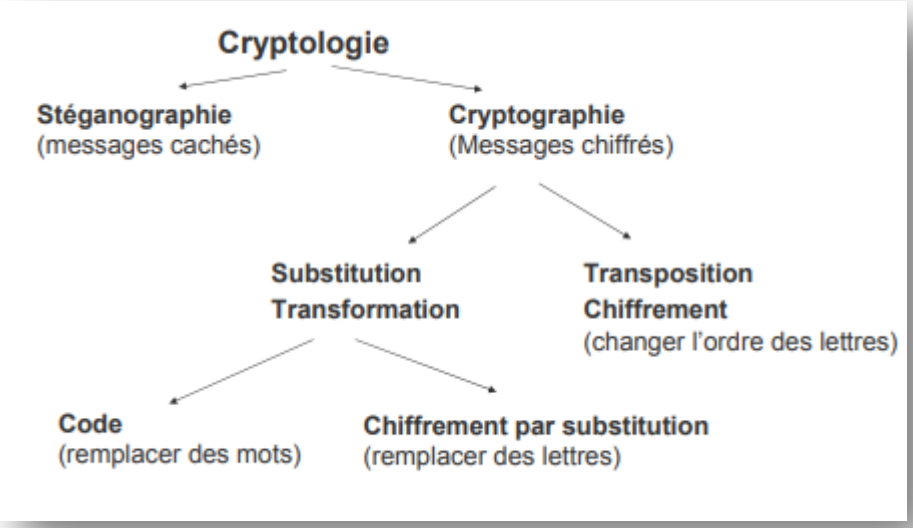

Figure 1.2: La cryptographie classique

3.1.1 Le chiffrement par substitution :

Le chiffrement à substitution remplace les lettres du message clair par des symboles (caractères, chiffres, signes, etc) définis à l'avance. En général, pour des raisons pratiques chaque lettre du message clair est remplacée par une lettre différente.

L'espace des clés est constitué par l'ensemble des substitutions des 26 lettres de l'alphabet. Pour une substitution □ donnée [1] :

$E\pi(x1, x2, x3,..., xn) = \pi(x1)\ \pi\ (x2)\ \pi\ (x3,)...\ \pi\ (xn).$

Et

$D\pi\ (x1, x2, x3,..., xn) = \pi\ -1(x1)\ \pi\ -1(x2)\ \pi\ -1(x3,)...\ \pi\ -1(xn).$

Exemple sur le chiffrement par substitution :

- **Exemple 1** : chiffrage par décalage (ou de César)

  C'est un chiffrement par substitution avec comme permutation [1] :

  x -> p(x) = x+b mod(26)

  Pour un $0 \leq b < 26$

- **Exemple 2** : chiffrage linéaire

  C'est un chiffrement par substitution avec comme permutation [1] :

  x -> p(x) = ax+b mod(26)

  Pour un $0 \leq b, a < 26$ et PGCD (a, 26) = 1

- **Exemple pratique** chiffre de César

  Soit le texte codé :

  « L FDPH L VDZ L FRQTXHUHG »

  Il y a 26 clés possibles donc on peut les essayer toutes :

On trouve la substitution [1] :

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Defghijklmnopqrstuvwxyzabc

Qui Donne:

« I came I saw I conquered»

3.1.2 Le chiffrement par transposition :

Le chiffrement par transposition (ou le chiffrement par permutation) consiste à faire un réarrangement de l'ordre des lettres qui cache le sens initial. Cette méthode demande de découper le texte clair en blocs de taille identique, et applique la même permutation sur chacun des blocs [3].

Exemple sur le chiffrement par transposition :

- chiffrage par transpositions rectangulaires.

Pour effectuer un chiffrement par transposition rectangulaire, on commence par se mettre d'accord sur un mot-clé. Choisissons pour notre exemple le mot « NABILA ». On classe alors les lettres du mot « NABILA »par ordre alphabétique, et on attribue à chaque lettre son numéro dans l'ordre alphabétique. Ainsi, on donne à A le numéro 1, au premier B le numéro 2, au deuxième B le numéro 3, au H le numéro 4, etc.…. [11]

On crée ensuite un tableau de la façon suivante :

- la première ligne est constituée par les lettres de la clé;
- la deuxième ligne est constituée par les numéros qui leur sont associés;
- on complète ensuite le tableau en le remplissant avec les lettres du message à chiffrer. On écrit sur chaque ligne autant de lettres que de lettres dans la clé. Eventuellement, la dernière ligne n'est pas complète. [11]

Par exemple, si on veut chiffrer "je vais partir à la forêt", le tableau que l'on construit est le suivant :

N	A	B	I	L	A
6	1	3	4	5	2
J	E	V	A	I	S
P	A	R	T	I	R
À	L	A	F	O	R
Ê	T				

Ensuite, on écrit d'abord le contenu de la colonne numérotée 1, puis le contenu de la colonne numérotée 2, etc.… Le message chiffré obtenu est alors :

« EALTS RRVRA ATFII OJPÀÊ »

3.2 La cryptographie moderne :

La cryptographie moderne se compose de deux grandes familles selon le principe de fonctionnement, comme montre la figure 1.3 [2] :

•La cryptographie symétrique.

.•La cryptographie asymétrique.

La figure ci-dessus montre les différents types de la cryptographie moderne :

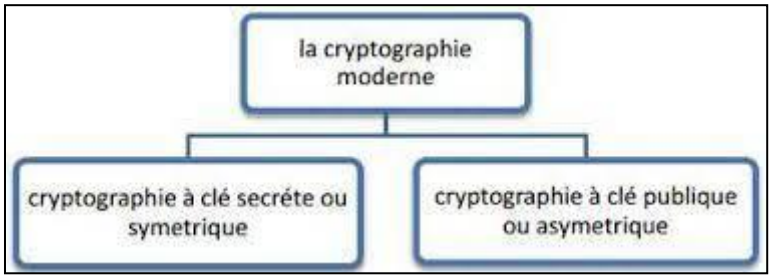

Figure 1.3: Système de la cryptographie moderne. [2]

3.2.1. La cryptographie symétrique ou à clé secrète :

La cryptographie symétrique, également dit à clé secrète (contraire à la cryptographie asymétrique), est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé [11]

.Les algorithmes les plus répandus sont : RC4 DES, AES,AES-GCM, 3DES…etc

La figure ci-dessus présente le principe de la cryptographie symétrique :

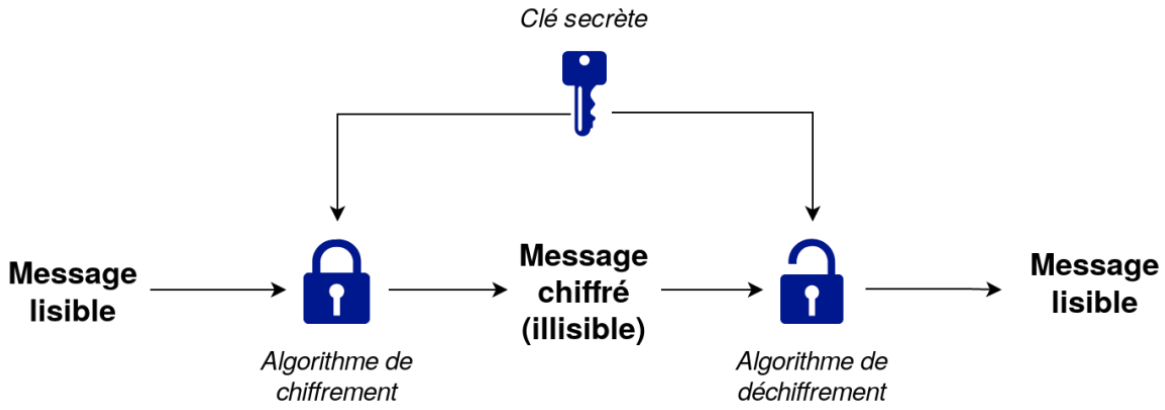

Figure 1.4 : La cryptographie symétrique [7].

3.2.1.1 le chiffrement AES :

Le chiffrement AES (Advanced Encryption Standard) est une norme ou spécification de chiffrement par bloc, c'est un algorithme de chiffrement symétrique c'est à dire qu'une même clé permet de chiffrer et de déchiffrer le contenu [12], l'AES utilise également des clés de 192 et 256 bits pour le chiffrement à haut rendement.

AES est implémenté dans des logiciels et du matériel à travers le monde pour chiffrer les données sensibles, Il est essentiel pour la sécurité informatique, la cybersécurité et la protection des données électroniques, mais on le trouve de plus en plus tous les jours, pour le chiffrement de base de données ou de stockage de données. [15]

Par exemple, nous utilisons AES pour crypter les fichiers ou la protection par mot de passe

des disques durs ou le stockage des mots de passe (tels que les gestionnaires de mots de passe), les fichiers PDF ou les fichiers ZIP. Pour protéger ses données. [15]

Le schéma suivant explique comment AES permet de chiffrer et déchiffrer symétriquement des données :

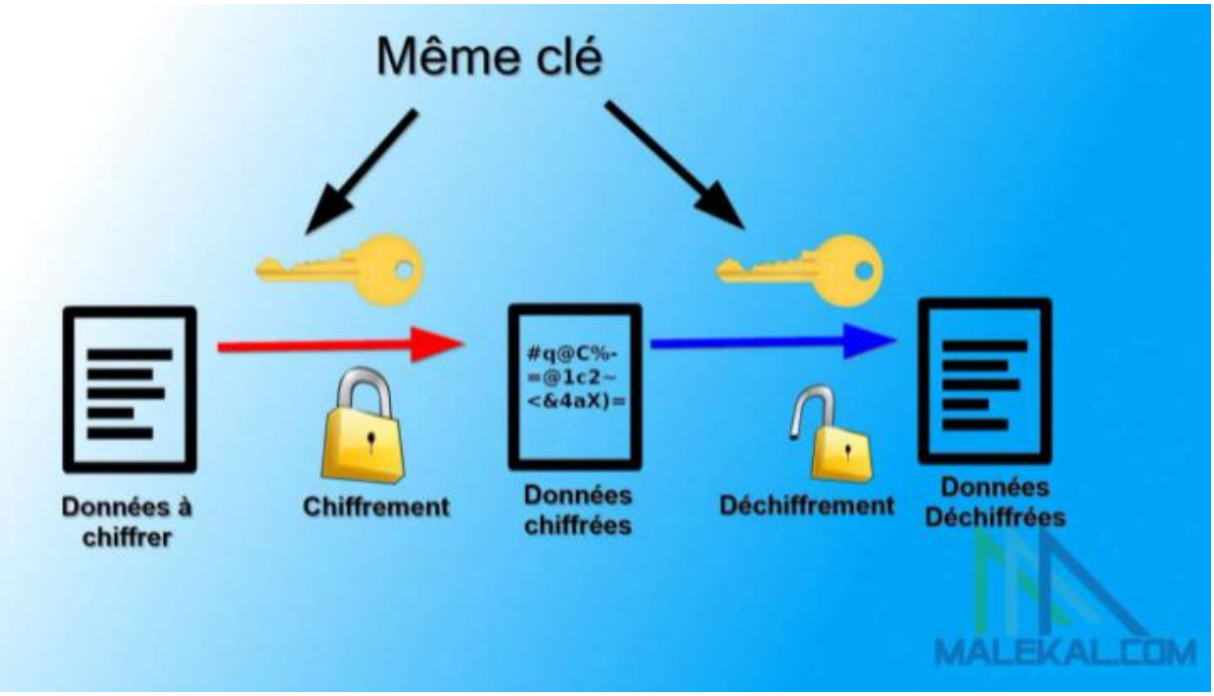

Figure 1.5 : cryptographie symétrique méthode AES [2].

3.2.1.2 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. [18]

- **Fonctionnement et particularités d'AES-GCM :**

- Le chiffrement AES-GCM est un standard libre de droits. Par conséquent, il peut être utilisé librement, sans avoir besoin de brevet.

- Il est de type symétrique.
- Il s'agit d'un système de chiffrement par blocs de 128 bits. Cela signifie que des blocs de 128 bits sont transformés en blocs cryptés de même taille.
- Le cryptage AES-GCM supporte différentes tailles de clé : 128, 192 ou 256 bits. En fonction de ces tailles de clé, le nombre d'opérations nécessaires par séquence pour le cryptage des blocs diffère :
    - 10 pour 128 bits,
    - 12 pour 192 bits,
    - et 14 pour 256 bits.

Les figures au-dessous montrent l'architecture de l'AES-GCM :

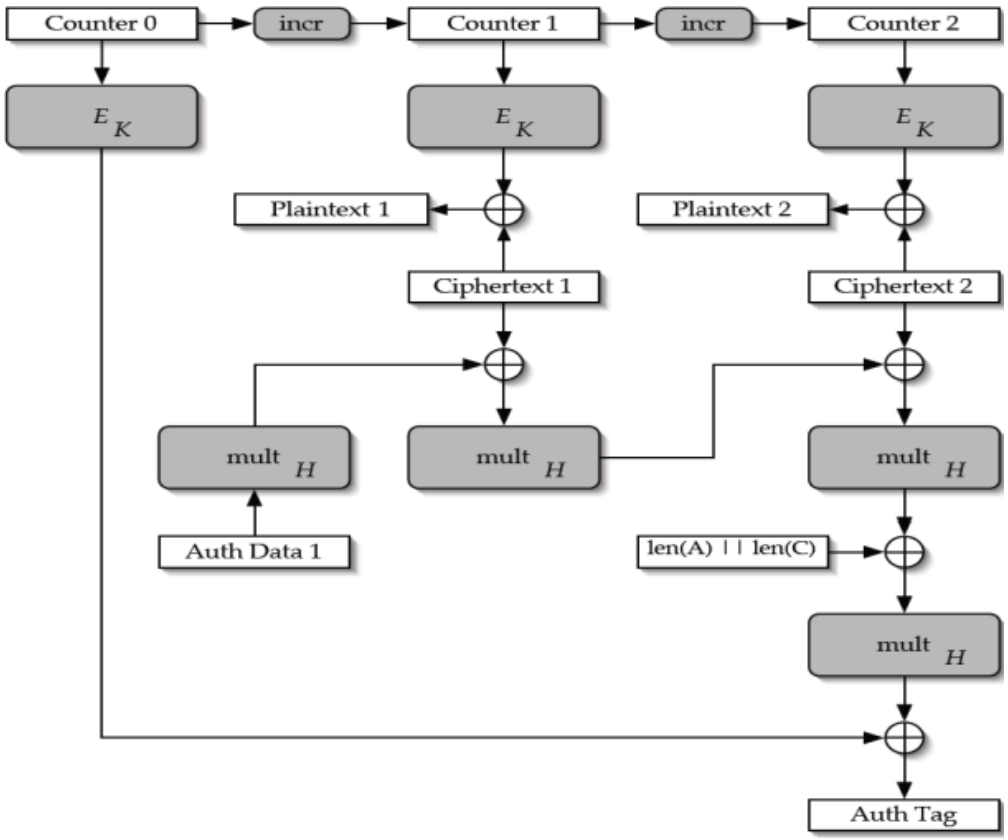

Figure 1.6 : Architecture de l'AES-GCM. [21]

3.2.1.3 Le chiffrement DES :

DES est un algorithme de chiffrement par blocs de bas niveau qui convertit un texte en clair en blocs de 64 bits et les convertit en texte chiffré à l'aide de clés de 48 bits, Il s'agit d'un algorithme de chiffrement symétrique qui combine transpositions et substitutions [20] ,le DES a été choisi comme norme au Etats-Unis en 1975 et est devenu le système cryptographique le plus utilisé dans le monde. [1]

Les DES a été critiqué à cause de la taille trop faible de ses clés.[1]

- **Inconvénient :**

Aujourd'hui, le D.E.S. est fortement menacé par les puissances de calcul des ordinateurs. Il n'est en effet pas impossible de balayer la plupart des clés pour casser le code. Un nouveau système, le A.E.S est prévu pour le remplace, Malgré tout, le DES est un algorithme très bien conçu : il a plutôt bien résisté à 30 ans de cryptanalyse

3.2.1.4 Avantages et inconvénients du chiffrement symétrique :

- **Les avantages**

Les chiffrements symétriques sont faciles à mettre en œuvre et peuvent être effectués en une fraction de seconde. Œil. De plus, il est si simple qu'il peut être utilisé par tous les âges et tous les horizons. [5]

- **L'inconvénient** Autrement dit, la clé secrète doit être partagée avec le destinataire et la clé secrète est chiffrée avec le mot de passe de l'utilisateur. Assurez-vous donc que le mot de passe n'est pas facile à deviner. Si vous cryptez tous vos e-mails avec la même clé, tous vos e-mails cryptés seront compromis si quelqu'un apprend la clé. [5]

3.2.2. La cryptographie asymétrique ou à clé public :

Le principe de chiffrement asymétrique (appelé aussi chiffrement à clés publiques) estapparu en 1976, avec la publication d'un ouvrage sur la cryptographie par Whitfield Diffie et Martin Hellman. Dans un cryptosystème asymétrique (ou cryptosystème à clés publiques), les clés existent par paires [14]:

•Une clé publique pour le chiffrement.

•Une clé secrète pour le déchiffrement.

La figure ci-dessus présente le principe de la cryptographie asymétrique :

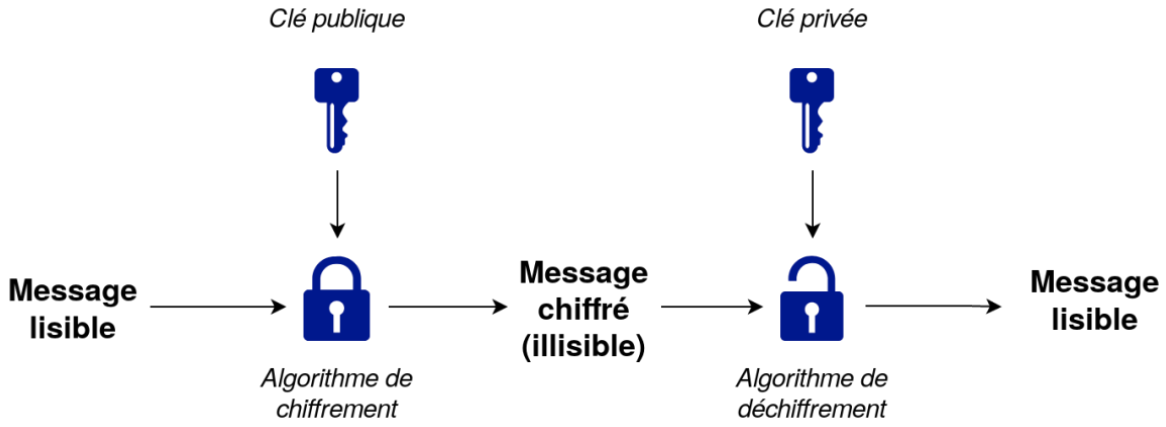

Figure 1.7 : Cryptographie asymétrique [7].

3.2.2.1 Avantages et inconvénients du chiffrement asymétrique :

- **L'avantage** du chiffrement asymétrique est qu'il n'oblige pas l'utilisateur à transmettre une clé (secrète) comme le chiffrement symétrique, éliminant ainsi le besoin de distribuer la clé. Le chiffrement asymétrique prend en charge les signatures numériques qui vérifient l'identité du destinataire. En outre, il garantit que les messages ne sont pas altérés en transit.[5]

- **l'inconvénient** du chiffrement asymétrique est qu'il prend beaucoup de temps et nécessite plus d'efforts. De plus, vous ne pouvez envoyer des e-mails cryptés que si l'autre partie a déjà créé une paire de clés. On peut dire que l'autre partie doit bien comprendre la situation. Enfin, si vous perdez votre clé privée, vous la perdez pour toujours. Les clés privées ne sont pas récupérables [5].

4. La cryptographie visuelle :

En général, La cryptographie visuelle est un domaine de la cryptographie dans lequel on utilise ou l'on transmet une image, dont le but est de pouvoir crypter une image en images cryptées n'ayant aucune ressemblance ou corrélation avec l'originale. [10]

La figure ci-dessus montre un model de cryptage d'image :

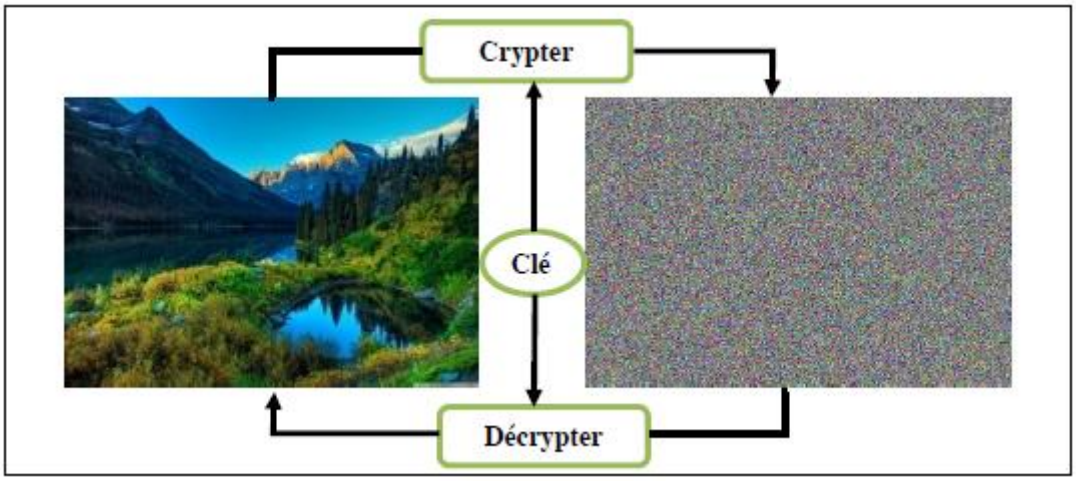

Figure 1.8: Cryptage d'image .

5. Définition de l'image :

L'image est définie comme une fonction bidimensionnelle f(x, y), où x et y sont des coordonnées spatiales (planaires), et la magnitude de f à n'importe quelle paire de coordonnées (x, y) est l'intensité ou le niveau de gris de l'image à ce point [16]

5.1 Les différents formats d'images :

5.1.1 JPEG :

JPEG (Joint Photographic Experts Group) Les images JPEG ou JPG 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 [2], Ce format est standard et universel. Il peut être lu par n'importe quel outil informatique (tablette, ordinateur, téléphone portable) partout dans le monde. [17]

5.1.2 PNG :

Le format PGN est le format graphique idéal pour les documents interactifs comme les pages web [1], mais il ne convient pas à l'impression. Il ne provoque aucune perte, ce qui signifie que vous pouvez toujours le modifier sans perdre en qualité. Pour autant, il reste un format de faible résolution. [17]

5.1.3 GIF :

GIF (Graphics Interchange Format), Il permet la création d'animations avec plusieurs séquences d'image, 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 [18].

5.1.4 TIFF :

Format TIFF (Tagged Image File Format), qui permet le stockage d'images en noir et blanc de haute qualité avec des couleurs RVB jusqu'à 32 bits par pixel. Il prend également en charge les images indexées à l'aide de palettes, de calques et de canaux alpha (transparence). [19]

6. L’image satellitaire :

L'imagerie satellitaire (également connue sous le nom d'imagerie spatiale) fait référence à l'acquisition d'images depuis l'espace par des capteurs placés sur des satellites. Visuellement,

les images satellites sont très similaires aux photos, mais elles contiennent plus d'informations. [10]

Les images satellites sont des fichiers qui contiennent diverses informations liées à des objets tels que le sol et la végétation, en ce sens que le traitement est effectué de manière à mettre en évidence des informations spécifiques à l'utilisation des terres et à la végétation. [20]

6.1 Résolution d'image satellitaire :

D'une façon général lorsque nous parlons de résolutions dans le domaine des satellites de télécommunications la télédétection, Il y a quatre résolutions différentes: spatiale, spectrale, temporelle et radiométrique.

6.1.1 Résolution spatiale :

La résolution spatiale est la taille du plus petit élément qui peut être distingué dans une image. Il est généralement défini comme la taille en pixels. Sur une image, les objets pouvant être reconnus dépendront de la résolution spatiale du capteur utilisé. En général, plus on augmente la résolution spatiale, plus la surface visible par le capteur est réduite : une image à très haute résolution couvrira une surface plus petite qu'une image à résolution moyenne. Lors du choix des images à examiner, il faut choisir le bon compromis en fonction de la taille du plus petit objet que l'on souhaite observer et de l'échelle à laquelle on souhaite observer le processus afin de classer les images satellites enregistrées [32] :

- Basse résolution
- Moyenne résolution
- Haute résolution (HRS)
- Très haute résolution (THRS)

6.1.2 Résolution spectrale :

La résolution est que le capteur utilise une petite fenêtre de longueur d'onde. Lorsque la résolution spectrale est bonne, alors les fenêtres des différents canaux du 0capteur sont étroites. [33]

6.1.3 Résolution radiométrique :

Les caractéristiques radiométriques décrivent l'information contenue dans une image par la sensibilité d'un capteur au signal émis par la scène [26]. Généralement cette valeur est comprise entre 8, 11, 12, 14 et 16 bits, qui correspondent à 256, 2047, 4095, 16384 et 65535 niveaux de gris pour chaque bande spectrale. La résolution radiométrique décrit donc la capacité de reconnaissance des différences dans l'énergie électromagnétique. [33]

7. Cryptage d'image :

Pour avoir un bon cryptage d'image, il faut détenir 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. [10]

- **Exemple** :

1er pixel de l'image à crypter (1)	01110011
1er pixel de l'image clé (2)	10100101
(1) XOR (2) 1er pixel de l'image cryptée	11010110

8. Conclusion :

Dans ce chapitre, nous avons expliqué les terminologies de base de la cryptographie, Puis nous avons cité les différents types de cryptage, ainsi nous décrivons notre méthode utilisée pour le cryptage d'images Enfin, on termine par les images satellitaires et ces résolutions.

Dans le chapitre suivant, nous allons présenter en général un état de l'art sur les différentes techniques de transmission ainsi notre méthode proposée.

CHAPITRE II
La transmission

Chapitre II

La transmission

1. Introduction :

Les systèmes de communications sans fils : L'émetteur, le récepteur et un canal radio via lequel les informations provenant de l''emetteur sont véhiculées au récepteur.

Ces dernières années, de nombreuses solutions de communication numérique ont vu le jour, et les systèmes de transmission traditionnels dans lesquels l'information est transmise en continu dans le temps ont concurrencé de nouvelles façons de transmettre l'information simultanément. Transferts "parallèles". Ces nouvelles méthodes visent à mieux utiliser le canal de propagation (OFDM) ou un ensemble de ressources de transmission entre utilisateurs (CDMA). Actuellement ces différentes approches tendent à être combinées (MC-CDMA) afin d'obtenir le meilleur rendement de transmission. [16]

Les systèmes de transmission doivent fournir des services qui nécessitent la transmission de données tout en assurant une grande mobilité des utilisateurs. Pour cela, de nouvelles techniques de traitement du signal doivent être mises en œuvre [4]. Alors dans ce chapitre Nous présentons une chaine de transmission OFDM une de ces approches qui consiste actuellement un axe important de la recherche dans ce domaine. [4] [9]

2. Le canal de transmission :

Le mot « canal de communication » n'a pas toujours le même sens et varie selon la façon dont les gens se positionnent dans une perspective de communication, de théorie de l'information ou de théorie de la communication. Pour nous, la notion de canal de transmission est attachée à toutes les sources d'interférences qui affectent le signal transmis, c'est-à-dire l'environnement physique utilisé pour la transmission et les équipements d'émission et de réception, tels que l'amplification fonctionnelle, la conversion de fréquence, etc. ou des antennes d'émission et de réception. [37]

3. la transmission numérique :

Avant de passer aux systèmes de transmission, faisons quelques rappels sur la transmission numérique. Soit l'expression générale de l'enveloppe complexe d'un signal numérique à transmettre [36] :

$x(t) = \sum_{q=-\infty}^{+\infty} d_q . \psi(t - qt),\ d_q = b_q + jc_q$

(2.1)

Avec :

La fonction $\psi(t)$ est une forme d'onde qui est prise en considération dans l'intervalle [0, T[puisque *t* doit vérifier la relation : *qT <= t <(k+1) T* [37].

b_q et c_q : symboles supposés non corrélés. A chaque ensemble de n élément binaire issu du message, on associe un symboleb_q, respectivementc_q, qui prend leurs valeurs dans un alphabet *A* à 2M éléments $A = \{\pm V, \pm 3V, \pm(2p+1)V, \ldots . \pm(2M-1)V\}$ avec $M = 2^n$ proviennent du découpage en paquets de n digits du train binaire issu du codeur [6] [37].

Les types de modulation les plus fréquemment rencontrés sont les suivants [6] [37] :

- MDA (*Amplitude Shift Keying ASK*) : Modulation par Déplacement d'Amplitude.
- MDP (*Phase Shift Keying PSK*) : Modulation par Déplacement de Phase.
- MDPD (*Differential Phase Shift Keying DPSK*) : Modulation par Déplacement de Phase Différentiel.
- MAQ (*Quadrature Amplitude modulation QAM*) : Modulation d'amplitude de deux porteuses en quadrature.
- MDF (*Frequency Shift Keying FSK*) : Modulation par Déplacement de Fréquence.

Les symboles b_q et c_q sont indépendantes et identiquement distribuées (i-i-d) sur l'alphabet a, leurs moyennes sont nulles et leurs variances sont égales à [36] [37] :

$$\sigma_b{}^2 = \sigma_c^2 = \frac{2}{M} \sum_{p=0}^{(\frac{M}{2}-1)} (2p+1)^2 \qquad (2.2)$$

Après sommation, on aura :

$\sigma_b{}^2 = \sigma_c^2 = \frac{M^2-1}{3}$ (2.3)

$$\psi(t) = p_T(t) \times g_0(t) = \delta(t) \times p_T(t) \times g_0(t) = \delta(t) \times g_e(t) \quad (2.4)$$

Tel que :

$g_0(t)$ Réponse impulsionnelle du filtre d'émission de mise en forme, exemple filtre1⁄2 Nyquist.

$p_T(t) \times g_0(t)$ Réponse impulsionnelle du filtre d'émission équivalent supposé adapter au filtre de réception.

T Temps symbole, T = nT_b, T_b durée d'un bit.

$p_T(t)$ Fonction porte de durée T et d'amplitude N.

Si maintenant, on veut transmettre plusieurs signaux de plusieurs utilisateurs (figure 3.1) on a :

$$x(t) = \sum_{j=0}^{N_u-1} x_j(t) \qquad avec \quad x_j(t) = \sum_{q=-\infty}^{+\infty} d_{qj}.\delta(t\text{-}qT) \times g_e(t) \quad (2.5)$$

Tel que : N_u est le nombre des utilisateurs.

La schéma ci-dessus montre le principe de la transmission multi-accès :

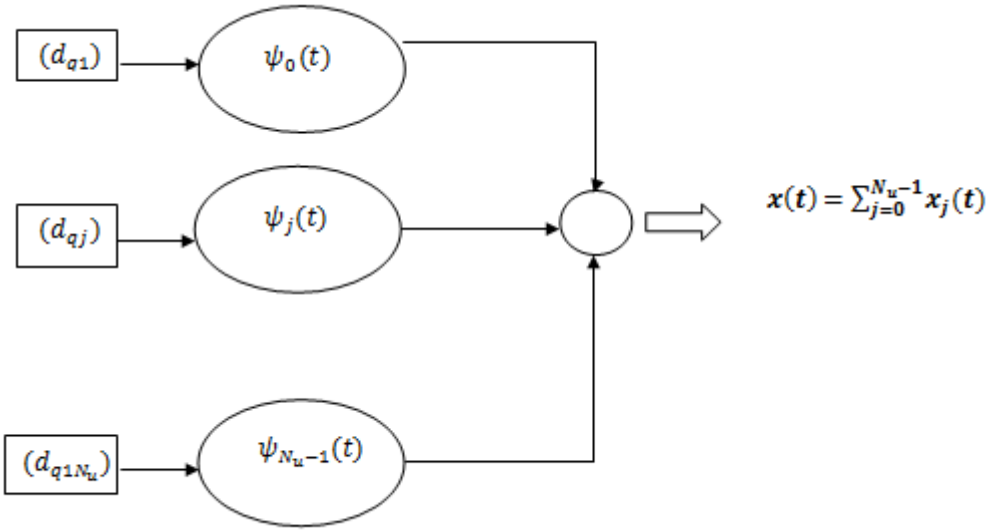

Figure 2.1: Transmission multi-accès. [37]

De l'expression (2.5), On obtient plusieurs méthodes de transmission de chaque utilisateur, Ces méthodes sont appelées techniques d'accès par multiplexage.

4. Définitions des principales techniques d'accès multiples :

La modulation multiporteuse principale transforme une étape de déconvolution dans le domaine temporel avec une égalisation simplifiée dans le domaine fréquentiel pour récupérer le signal transmis [4]. Les systèmes de communication ont été conçus à l'origine en attribuant à chaque couple émetteur/récepteur un canal de transmission "physique". Afin d'augmenter la capacité du réseau et d'optimiser l'utilisation des ressources en fréquence dans la pratique, diverses techniques d'accès multiple ont vu le jour. Ainsi, l'accès multiple par répartition dans le temps, l'accès multiple par répartition en fréquence et le multiplexage en longueur d'onde sont des techniques de multiplexage qui ont été mises en œuvre dans les réseaux radiofréquences ou les systèmes optiques. [29]

4.1 Techniques d'accès multiples :

L'idée originale des ces Techniques est de permettre à plusieurs équipements d'accéder à une ressource commune partagée selon une technique de répartition dans le temps (TDMA) ou selon une technique de répartition en fréquences (FDMA) ou encore par détection de porteuse (CDMA).

Dans la figure 2.2, nous présentons les différentes techniques d'accès multiples :

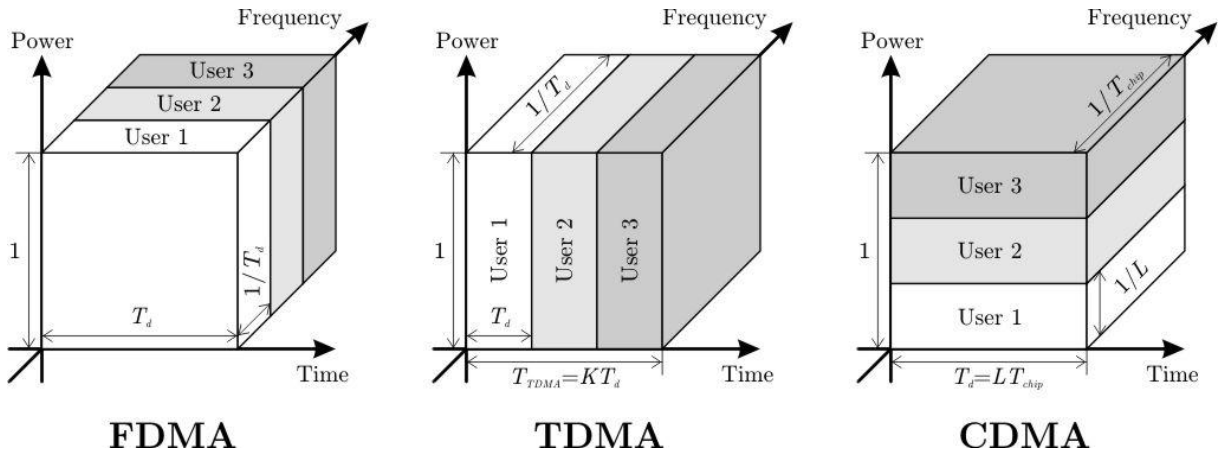

Figure 2.2 : techniques d'accès multiples [22].

4.2 Caractéristiques des Différentes techniques d'accès multiples :

- Les systèmes d'accès multiples sont basés sur l'orthogonalité des signaux.

- FDMA (Frequency Division Multiple Access) [36]:

  - Utilise différentes fréquences pour transmettre un signal.
  - Les différents utilisateurs partagent la même durée temporelle et sont séparés par des mêmes intervalles de bandes fréquentielles régulières Δf.

- TDMA (Time Division Multiple Access) [36]:

  - Intervalles de temps distincts (time slot)
  - Les différents utilisateurs partagent la même bande fréquentielle et sont séparés par des mêmes intervalles de temps réguliers $\Delta t = T_s$.

- CDMA (Code Division Multiple Access) [36] :

  - différent codes.
  - Les différents utilisateurs partagent la même durée temporelle et la même bande fréquentielle et sont séparés par des codes orthogonaux.

5. Système TDMA (Time division multiple access):

La TDMA est une technique d'accès multiple par répartition dans le temps. À la différence de FDMA et CDMA, dans TDMA la division des appels se produit sur la base du temps. Le système numérise d'abord les appels, puis combine ces conversations en un flux numérique unifié sur un seul canal radio. Maintenant, il divise chaque canal cellulaire en trois tranches de temps, ce qui signifie que trois appels sont mis sur une seule fréquence, puis un intervalle de temps est attribué à chaque appel pendant la conversation, un espace régulier dans un flux numérique. Les utilisateurs émettent successivement l'un après l'autre, chacun utilisant son propre intervalle de temps. Ceci permet à plusieurs stations de partager le même support de transmission (par exemple un canal de fréquence radio) tout en n'utilisant qu'une partie de sa capacité de canal. [15]

Cette technique permet à trois utilisateurs différents d'utiliser une fréquence en même temps (Figure 2.6), il n'est pas nécessaire d'utiliser trois fréquences différentes comme dans FDMA. Dans FDMA, au lieu d'occuper un seul canal radio pour un seul appel, TDMA

achemine efficacement trois appels simultanément. Cette technologie est utilisée dans notre système GSM. [15]

La figure ci-dessous représente le principe de fonctionnement de la TDMA :

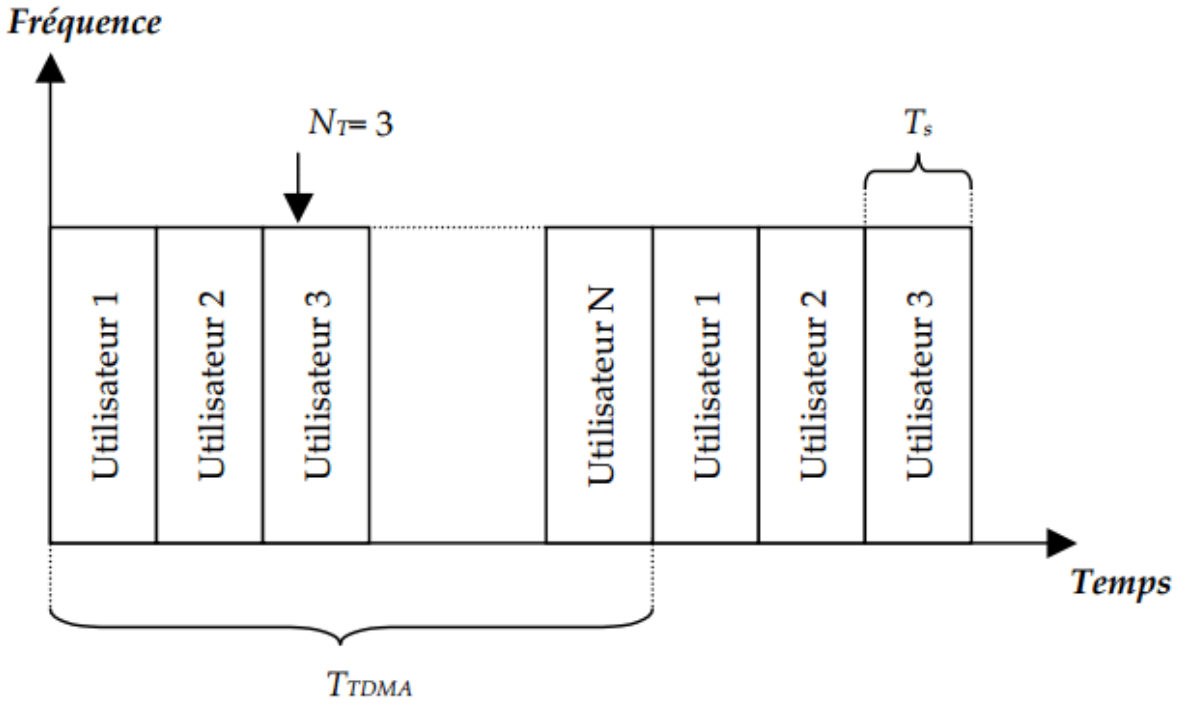

Figure 2.3: Principe de fonctionnement du TDMA

6. Accès multiple par répartition de codes (CDMA) :

L'Accès Multiple par Répartition de Codes (AMRC) appelé aussi Code Division Multiple Access (CDMA), également connu sous le nom de Code Division Multiple Access (CDMA), est une technologie de multiplexage plus récente que TDMA et FDMA. Dans cette technique d'accès multiple, les utilisateurs partagent le même espace de fréquence et transmettent sur le même créneau horaire, dans ce cas chaque émetteur se voit attribuer un code, également appelé signature ou séquence de code, qui permet la transmission d'informations à partir d'autres utilisateurs sans perturber le message. La réduction des MAI n'est obtenue que dans le cas de l′utilisation de séquences de codes strictement orthogonaux. [30]

La figure (2.4) représente le Schéma d'un multiplexage par code (CDMA) :

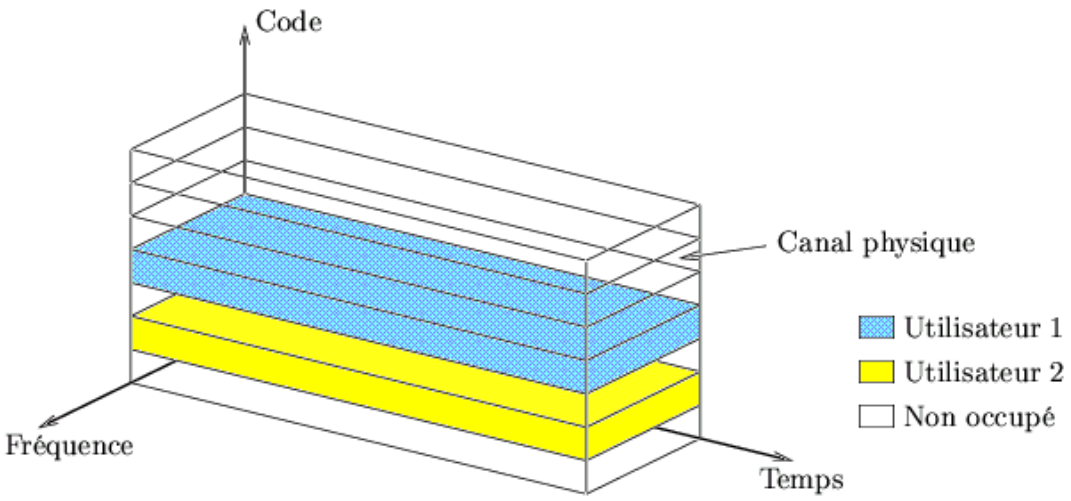

Figure 2.4 : Schéma d'un multiplexage par code (CDMA) [31]

Le CDMA permet à différents utilisateurs de transmettre leurs données sur n'importe quelle fréquence sans synchronisation entre eux. En effet, contrairement aux technologies TDMA, FDMA et WDM, la capacité de multiplexage du CDMA n'est pas limitée par des paramètres physiques (intervalles de temps disponibles, fréquences ou longueurs d'onde disponibles, etc.), mais par la capacité à générer les plus grandes séquences de code qui soient. La séquence de code utilisée dans les systèmes CDMA consiste en une série d'impulsions appelées "chips" afin de les distinguer des "bits" de la séquence de données. [1]

L'étalement du spectre est l'un des avantages proposés pour les systèmes CDMA. L'application du CDMA dans le domaine de la communication par radiofréquence. D'un autre coté, la puissance d'un signal, après codage, est étalée sur toute la largeur de la bande de fréquence disponible. De ce fait deux caractéristiques importantes apparaissent [1] :

- Étant donné que la puissance du signal est répartie sur la bande de spectre disponible, le signal CDMA peut être confondu avec le bruit du canal, ce qui le rend difficile à détecter par les utilisateurs non affectés. [1]

- Les signaux CDMA étendus sont plus résistants à l'évanouissement sélectif en fréquence.
- Les signaux CDMA (codés) sont plus résistants aux interférences pouvant survenir lors de la transmission. Lors du décodage, la puissance de ce brouilleur est répartie sur les bandes spectrales disponibles, et le signal utile est reconstruit. Cependant, si le nombre de brouilleurs est important, la puissance générée par ces derniers sera plus importante, ce qui affectera la qualité du signal recherché après décodage. [30]

La figure suivante représente l'effet de l'étalement de spectre sur la présence d'un brouilleur :

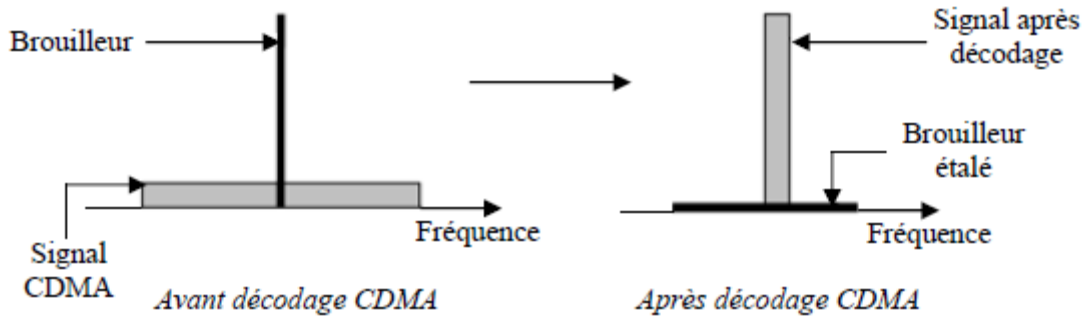

Figure 2.5 : Effet de l'étalement de spectre sur la présence d'un brouilleur. [1]

6.1 Différentes techniques du (CDMA) :

La technologie CDMA est destinée à être utilisée dans les systèmes de communication numérique sur les fréquences radio dans le cadre d'applications militaires. Profitant de la capacité de multiplexage accrue tout en utilisant les propriétés d'étalement du spectre propres à la technologie, l'objectif est de rendre la transmission plus robuste à la présence d'interférences et moins susceptible d'être interceptée (Figure 2.5). [8]

Le CDMA peut transmettre et concaténer autant de signaux que possible pour générer des séquences de code, tant que ces séquences satisfont aux propriétés d'auto- et d'intercorrélation appropriées. Ces conditions de la fonction de corrélation permettent de contrôler et de

minimiser le MAI qui se traduit en partie par une augmentation du taux d'erreur binaire (BER) lors de la détection et du décodage. [8]

Le schéma ci-dessous montre les différentes techniques du CDMA :

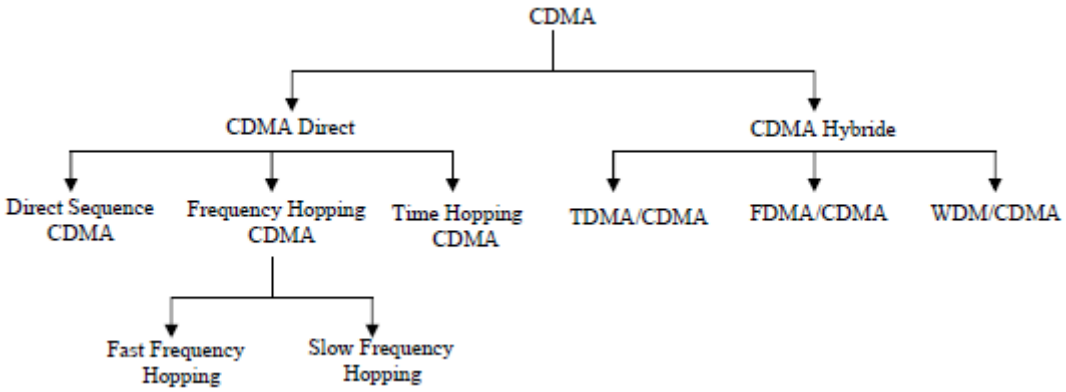

Figure 2.6 : Différentes techniques CDMA.

Certaines études associent le CDMA à d'autres techniques de multiplexage (TDMA, FDMA, WDM, etc.). Deux types de codage CDMA est clair. Le premier, appelé CDMA direct, comprend le CDMA à séquence directe, le CDMA à saut de fréquence (lent ou rapide) et le CDMA à saut temporel. La seconde, appelée CDMA hybride, combine le multiplexage de code avec d'autres techniques de multiplexage de manière plus hiérarchique. L'arbre représenté sur la figure (2.6) rassemble toutes ces classifications [30]

6.2 Avantages et inconvénients du CDMA :

Avantage :

- Possibilité d'attribuer la même bande de fréquence à différents utilisateurs. La différence entre les signaux des différents utilisateurs est déterminée par le code d'étalement attribué à chaque utilisateur. [4]

- L'immunité du signal transmis est également assurée en raison du niveau de puissance réduit du brouilleur en raison d'un fonctionnement prolongé. [4]
- Une bonne robustesse d'interception est assurée puisque seul le couple TX/RX connaît le code d'extension. [4]
- Diversité des voies empruntées : Pour un usager donné, il est possible de bénéficier de l'énergie des voies secondaires. [4]

Inconvénients :

- Allocation de spectre inefficace : cet inconvénient est dû au fait qu'une large bande passante est allouée, ce qui rend beaucoup plus difficile l'allocation d'une bande passante étroite. [4]
- Dégradation des performances dans les environnements multiutilisateurs : le BAM est ajouté au signal reçu lorsque le canal détruit de manière significative l'orthogonalité des différents codes d'utilisateur. [4]

7. Le système DS-CDMA :

Le DS-CDMA étant choisi pour véhiculer la troisième génération des systèmes de communication sans fil, c'est un élément important dans l'établissement des performances est la caractérisation du canal de communication. [34]

7.1 Modélisation du système DS-CDMA :

Dans un système DS-CDMA, le signal porteur de l'information (le signal de données) est directement modulé par un signal code numérique à temps discret et à valeurs discrètes appelé code d'étalement. [34]

La figure 2.7 montre un modèle en bande de base d'un système de communication DS-CDMA :

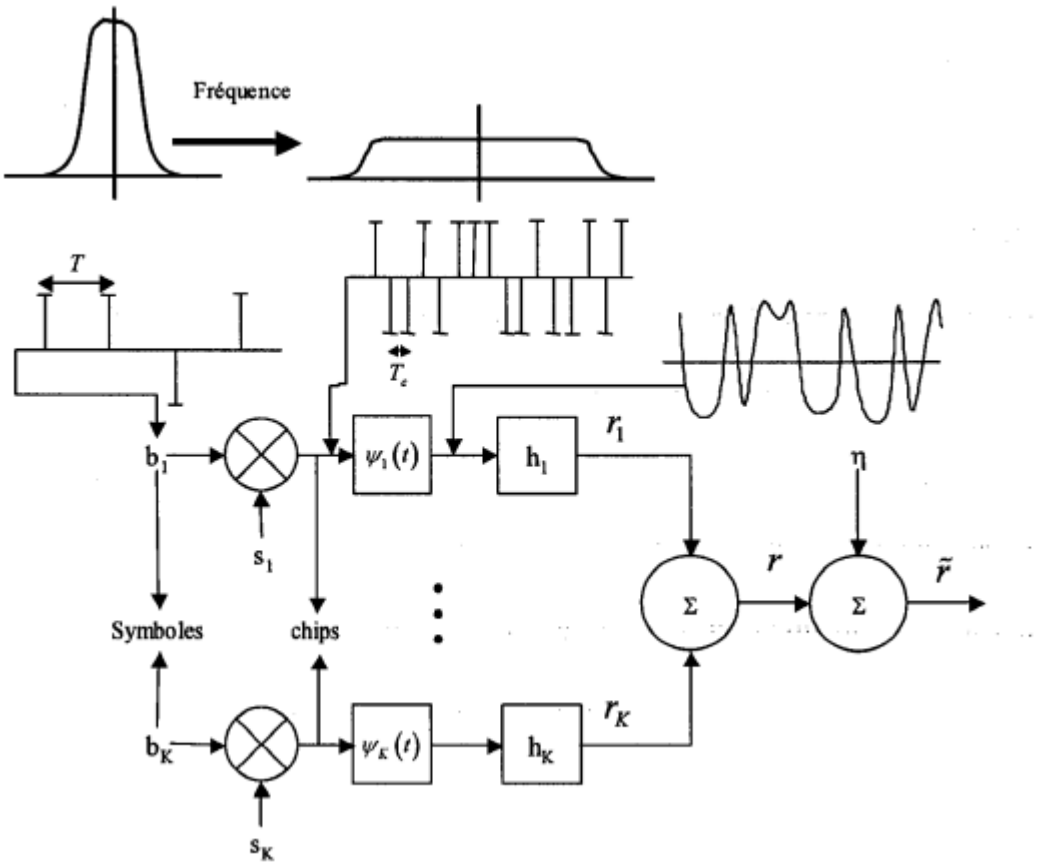

Figure 2.7 : Modèle en bande de base d'un système DS-CDMA. [34]

8. Les systèmes MC-CDMA :

A travers les techniques combinant les modulations à porteuses multiples et l'étalement de spectre, le système Mc-cdma est de loin le plus étudié. Depuis son apparition en 1993, le Mc-cdma a tout d'abord fait l'objet de nombreuses comparaisons avec des systèmes utilisant la technique Ds-cdma. Ces comparaisons ont largement démontré la supériorité des systèmes Mc-cdma vis-à-vis des systèmes Ds cdma. En plus de ces études comparatives, des travaux, principalement réalisés sur liaison descendante, ont cherché à optimiser les systèmes Mc-cdma an d'améliorer leurs performances. Ainsi, les sensibilités des systèmes Mc-cdma vis-à-vis des décalages Doppler ou des erreurs de synchronisation ont été évaluées. [40]

Le système MC-CDMA est une combinaison entre le système CDMA et les techniques multi-porteuses. Les porteuses sont orthogonales et la séquence PN qui permet de différencier les différents usagers est de longueur égale au nombre de porteuses. En effet chaque chip de la

séquence PN est appliqué à une porteuse. Les différentes porteuses véhiculent la même séquence d'information. [36]

Nous représentent dans la figure ci-dessous le Bloc du diagramme MC-CDMA :

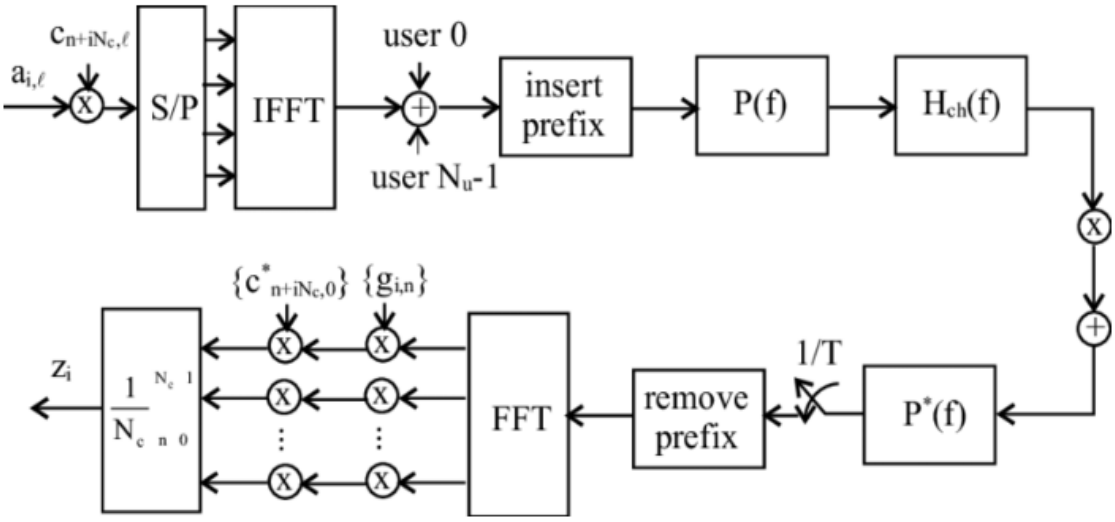

Figure 2.8 : Un Bloc du diagramme MC-CDMA. [41]

9. Système OFDM :

Chacune de ces techniques que nous venons d'évoquer est parfaitement adaptée aux besoins lorsqu'elle est bien optimisée, il est donc difficile de choisir la bonne, alors choisissez en fonction de certains critères. [9]

Parmi les critères qui ont guidé notre de choix :

- Adaptabilité à un environnement intérieur quasi-stationnaire.
- Mise en œuvre simple et faible coût.
- Efficacité des canaux multivoies.
- Utilisation optimale de la bande passante

Une question peut se poser de savoir si l'OFDM présente des avantages par rapport au CDMA, et la réponse est oui, les systèmes OFDM peuvent atteindre une efficacité spectrale légèrement supérieure à celle du CDMA. Cependant, des architectures de récepteur avancées comprenant des méthodes pratiques sont mises en œuvre pour aligner les systèmes CDMA avec OFDM. [9]

9.1 Présentation de l'OFDM :

Les origines de l'OFDM remontent à 1930, lorsque les célèbres laboratoires de recherche Bell ont développé une nouvelle technologie d'accès aux canaux radio, qui a hérité du FDM bien établi, connu sous le nom d'OFDM (Orthogonal Frequency Division Multiplexing). Au milieu des années 1960, puis abandonné lors du développement de la théorie de l'égalisation pour les systèmes à porteuse unique (moins complexe), l'OFDM a été adopté par le projet de diffusion numérique DAB (Digital Audio Broadcasting) car il était de retour vers le milieu des années 1980, au projet de la radiodiffusion numérique DAB (Digital Audio Broad casting).

En effet, contrairement à l'OFDM, les systèmes à porteuse unique ne répondent pas aux conditions de résistance aux trajets multiples à faible taux d'erreur sur les bits et à haut débit requises pour cette nouvelle application [23] . Depuis lors, l'OFDM a été la technologie dominante car elle est utilisée dans de nombreuses normes telles que la diffusion numérique terrestre ou DAB, la norme de télévision numérique terrestre ou DVB-T, la technologie ADSL et les réseaux sans fil. Normes WLAN g (WIFI), 802.16g (WIMAX) et HIPERLAN [24] définies par IEEE 802.11a, 802.11. Enfin, l'OFDM est parfaitement adapté aux communications mobiles et semble incontournable pour les standards de troisième et quatrième génération, notamment lorsqu'on le combine avec des systèmes CDMA (Code Division Multiple Access) ou multi-antennes MIMO (Multiple Input Multiple Output) problématiques associées) [14] [25].

9.2 Principe de la modulation OFDM :

L'OFDM implique la division d'un signal numérique à transmettre sur un grand nombre de porteuses. Tout se passe comme si les signaux à transmettre étaient combinés sur un grand

nombre de systèmes de transmission indépendants (ex : émetteurs) et sur des fréquences différentes (multiplexage de fréquence). [26]

Afin de garder les fréquences des porteuses aussi proches que possible pour transmettre le maximum d'informations sur une portion fréquentielle donnée, l'OFDM utilise des porteuses orthogonales entre elles. Les signaux de différentes porteuses se chevauchent mais n'interfèrent pas les uns avec les autres du fait de l'orthogonalité, et les signaux à transmettre sont généralement répétés sur des fréquences porteuses différentes. Par conséquent, dans un canal de transmission à plusieurs chemins, certaines fréquences seront corrompues en raison d'une combinaison destructive de chemins, et le système pourra toujours récupérer les informations perdues sur d'autres fréquences porteuses qui ne sont pas corrompues [24].Chaque porteuse est modulée indépendamment en utilisant des modulations numériques : BPSK (*Binary Phase Shift Keying*), QPSK (*Quadrature Phase Shift Keying*), QAM-16 (*Quadrature Amplitude Modulation*), QAM-64.

La figure suivante décrit le principe de base de la modulation OFDM:

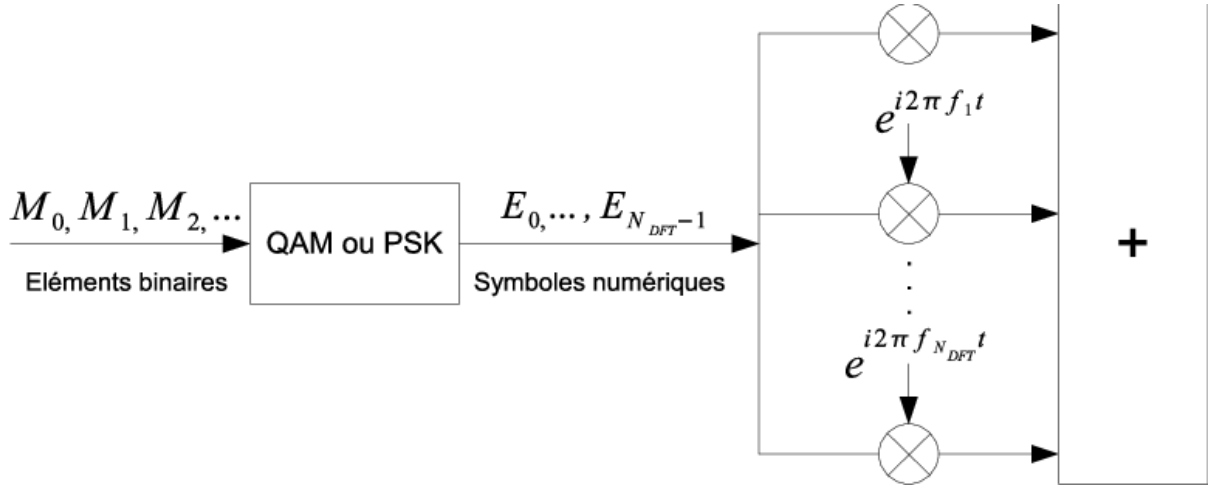

Figure 2.9 : Modulation OFDM avec Nc=3 sous-porteuse. [27]

9.2.1 Principe de l'orthogonalité :

L'orthogonalité est la propriété fondamentale qui permet de transmettre des signaux d'informations multiples dans un même canal et de les détecter sans interférence.

En Mathématique, l'orthogonalité de deux fonctions f(t) et g(t) dans l'intervalle [a, b] est définit par la relation [35]:

$$\int_a^b f(t).g(t).dt = 0 \qquad (2.6)$$

9.2.1.1 L'orthogonalité temporelle :

Le signal OFDM est composé d'une somme de *N* sinusoïdes de fréquences Respectives fk=k/Tu transmises durant une durée *Tu*.

Chaque sous-porteuse $gk(t)$ peut se mettre sous la forme [35] :

$$\text{gk(t)} = \begin{cases} \sin\left(2\pi k.\ \frac{t}{Tu}\right) & 0 \leq t < Tu \\ 0\ ailleur \end{cases} \qquad \text{Pour k= [0,1,……. N-1]} \qquad (2.7)$$

Ainsi deux sou-porteuses gi(t) et gj(t) , de fréquences respectives fi et fj , définis par l'expression (2.7), sont orthogonales sur l'intervalle [0, Tu [.

9.2.1.2 L'orthogonalité fréquentielle :

Chaque sous-porteuse transmet la durée Tu. Cela revient à appliquer une porte de durée Tu sur la sous-porteuse dont le contenu spectral est un sinus s'annulant à la première fréquence f-1=fk – 1/Tu et f+1= fk +1/Tu .

Les fréquences sont respectivement égales à fk-1 et fk+1. La figure (2.9) montre le spectre de la sous-porteuse K pour la bande Δf= 1/Tu .

Par conséquent, nous obtiendrons l'enveloppe spectrale représentée sur la figure (2.10). La figure (2.9) montre que la position entre chaque sous-porteuse 1/Tu permets d'organiser ces sous-porteuses de telle sorte qu'à la valeur maximale d'une sous-porteuse donnée les autres

sous-porteuses soient nulles : c'est une condition d'orthogonalité dans le domaine fréquentiel. Par conséquent, cette condition permet une occupation idéale du spectre et évite les interférences entre les sous-porteuses (IEP) [38].

Les figures ci-dessous montrent le spectre d'orthogonalité des sous-porteuses en OFDM :

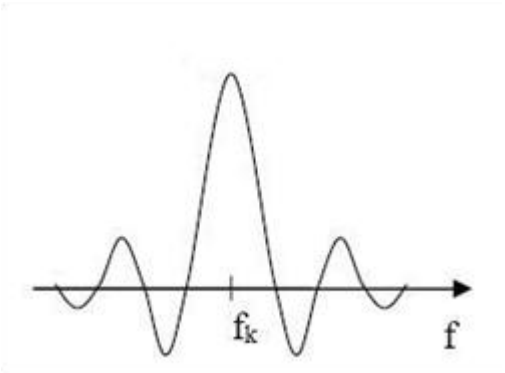

Figure 2.9 : Le spectre d'une sous-porteuse. [39]

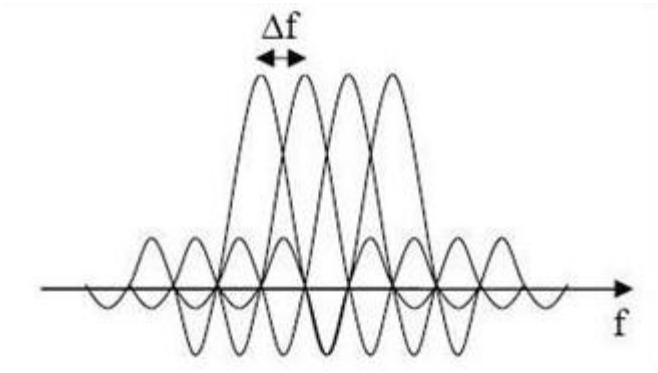

Figure 2.10 : Principe d'orthogonalité des sous-porteuses en OFDM [39].

La bande passante du spectre d'un symbole OFDM est constante et s'écrit B= N/Tu

Tel que N : le nombre maximal de sous-porteuses.

Alors, chaque sous-porteuse a une bande passante de Bsp = B/N

9.3 Signal OFDM :

La modulation multiporteuse OFDM a pour principe de répartir les symboles complexes $C_k$sur N sous-porteuses[14]. Le symbole complexe C_k est issu d'un alphabet fini correspondant à une modulation donnée. [28]

L'expression suivante exprime un signal OFDM dans l'intervalle de temps [0, Ts [[28] :

$$x(t) = \frac{1}{N}\sum_{k=0}^{N-1} C_k \, e^{j2\pi k\Delta \mathrm{ft}}, \; 0 \le t \le T_s \qquad (2.8)$$

Tel que C_k est un symbole numérique, qui est sélectionné dans l'ensemble de constellations modulées numériquement de la technologie M-QAM, modulé par $K^{éme}$, Δf est le nombre de sous-porteuses It est mis à $1/T_s$ pour générer des sous-porteuses orthogonales, où T_s est la durée du symbole OFDM. Nous avons vu que les signaux OFDM peuvent être générés par une opération de transformée de Fourier rapide inverse (IFFT) suivie d'une conversion numérique-analogique. En d'autres termes, nous pouvons remplacer la variable t dans (2.8) par la variable n/N et nous obtenons l'expression suivante :

$$x(n/N) = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} C_k \, e^{f2\pi k\Delta \mathrm{f}\frac{\mathrm{n}}{\mathrm{N}}}, \; 0 \le n \le N-1 \qquad (2.9)$$

Où le terme de droite dans l'équation (2.9) est l'opération IFFF. Alors, elle s'écrit sous la forme :

$$x(n) = IFFT(C_0, C_1, \ldots., C_{N-1}) \qquad (2.10)$$

9.4 Avantages et inconvénients de l'OFDM :

Avantage :

- Le principal intérêt de l'OFDM est la simplicité de l'égalisation de la distorsion du canal. Contrairement aux systèmes monoporteuse, où la correction d'atténuation de canal nécessite une inversion de matrice, ce qui est souvent difficile à réaliser, l'OFDM offre la possibilité d'égaliser cet effet en multipliant simplement par un coefficient d'égalisation sur chaque sous-porteuse possible. [13]
- Aussi, dans un système monoporteuse, lorsque la fréquence d'échantillonnage augmente, le nombre de coefficients de canal à estimer augmente également, donc la complexité du récepteur augmente également, ce qui n'est pas le cas en OFDM, quelle que soit la fréquence d'échantillonnage. [13]
- L'OFDM, d'autre part, utilise efficacement la bande de fréquence allouée en utilisant des porteuses orthogonales. [13]

Inconvénients :

- L'OFDM est très sensible aux erreurs de synchronisation. Ceux-ci créent un IEP et détruisent l'orthogonalité des sous-porteuses. [4]
- De plus, l'OFDM est sensible à la distorsion non linéaire introduite par l'amplificateur de puissance de l'émetteur. [4]

10. Canal a bruit blanc additif gaussien (AWGN) :

Le modèle de canal le plus couramment utilisé pour la transmission numérique analogique, à savoir C'est aussi l'un des plus faciles à générer et à analyser, qui est le canal de bruit blanc additif gaussien (BBAG, AWGN) anglais ‘Additive White Gaussian Noise). Ce bruit simule le bruit provenant de sources internes (bruit dus à des défauts d'équipement, etc.) et des bruits extérieurs (bruit d'antenne, etc.). Cependant, ce modèle est associé à la transmission filaire car il représente la transmission Presque parfait de l'émetteur au récepteur. [42]

Écrivez ensuite le signal reçu sous la forme :

$$Y(t) = x(t) + B(t) \quad (2.11)$$

Le schéma ci-dessous représente un modèle de canal AWGN :

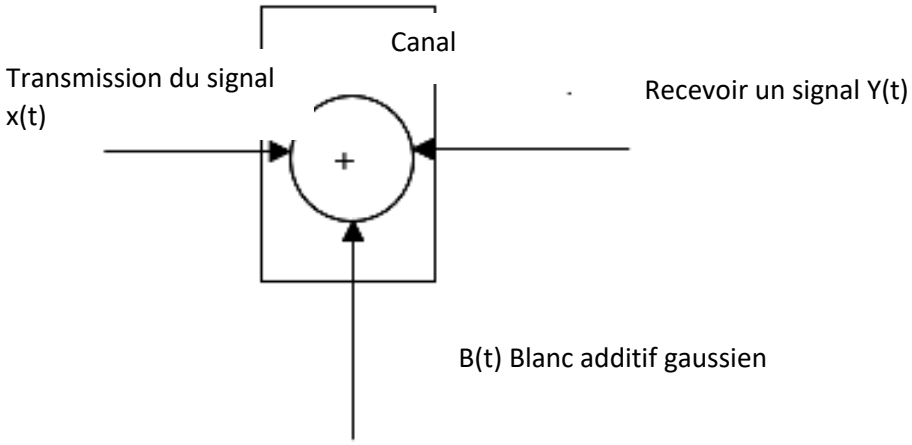

Figure 2.11 : modèle d'un de canal AWGN

La figure ci-dessous montre un schéma montrant un émetteur-récepteur OFDM :

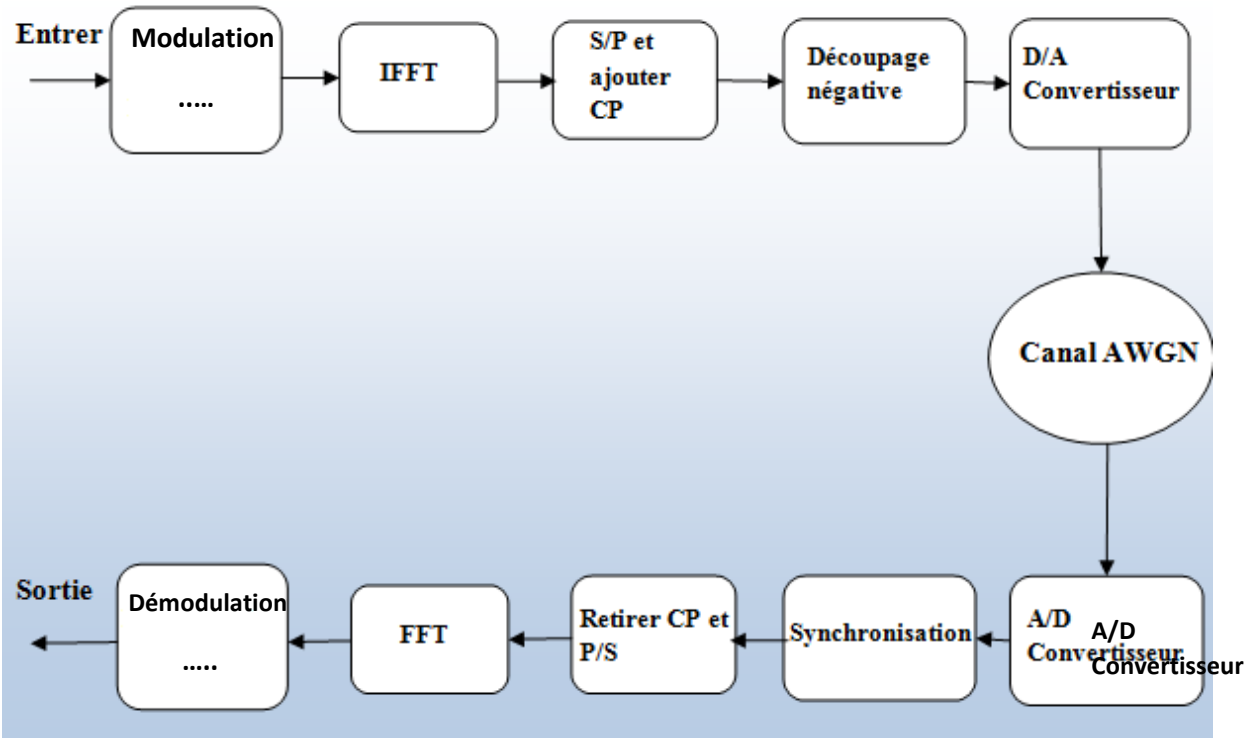

Figure 2.12 : Schéma montrant un émetteur-récepteur OFDM

11. Conclusion :

Nous finirons ainsi ce chapitre dans lequel notre étude se concentre sur la technique spécifique de l'OFDM, solution éprouvée et simple à implémenter, nous avons justifié notre choix de cette technique par rapport à d'autres techniques bien connues. Parce qu'il favorise une utilisation optimale de la bande passante disponible et offre une efficacité spectrale élevée.

Nous avons décrit notre approche, et maintenant nous sommes prêts à aborder le chapitre suivant, où nous présenterons et analyserons les différents résultats obtenus.

CHAPITRE III
Simulation et Résultats

Chapitre III

Simulation et Résultat

1. Introduction :

Après avoir présenté dans les chapitres précédents nos méthodes de cryptage et la transmission d'image, nous entamons maintenant la partie de la réalisation et de l'analyse de notre application.

Cette application décrit l'utilisation de la norme de chiffrement évolué (AES, Advanced Encryptions Standard) dans le mode Galois/compteur (CGM, Galois/Counter Mode) pour assurer la confidentialité et l'authentification de l'origine des données, ainsi allons étudier les performances de la technique de transmission d'un système de communication OFDM.

Dans ce chapitre, nous présentons notre application réalisée et les différents outils nécessaires pour le développement.

2. Résultats expérimentaux :

2.1 Environnement matérielle:

Notre application est développée sur un PC avec les caractéristiques suivantes :

- Processeur : Intel(R) Core(TM) i7-10510U CPU @1.80GHz 2.30 GHz.
- Mémoire (RAM) : 16,00 Go.
- Système d'exploitation : Windows 7 Professionnel 64 bit.

2.2 Environnement logiciel:

Nous avons implémenté notre application avec le langage de programmation Matlab avec la version Matlab R2017b (64-bit).

3. Les Méthodes sur logiciel développé:

Notre application permet d'illustrer le processus de cryptographie, et donc la transmission des systèmes de communication OFDM, et sur la base de nos recherches et de l'analyse des résultats obtenus, nous présentons deux méthodes de réalisation de tests pour démontrer leur efficacité et la sécurité applicative.

Schéma générale de l'application :

La figure ci-dessous représente le schéma général de notre application :

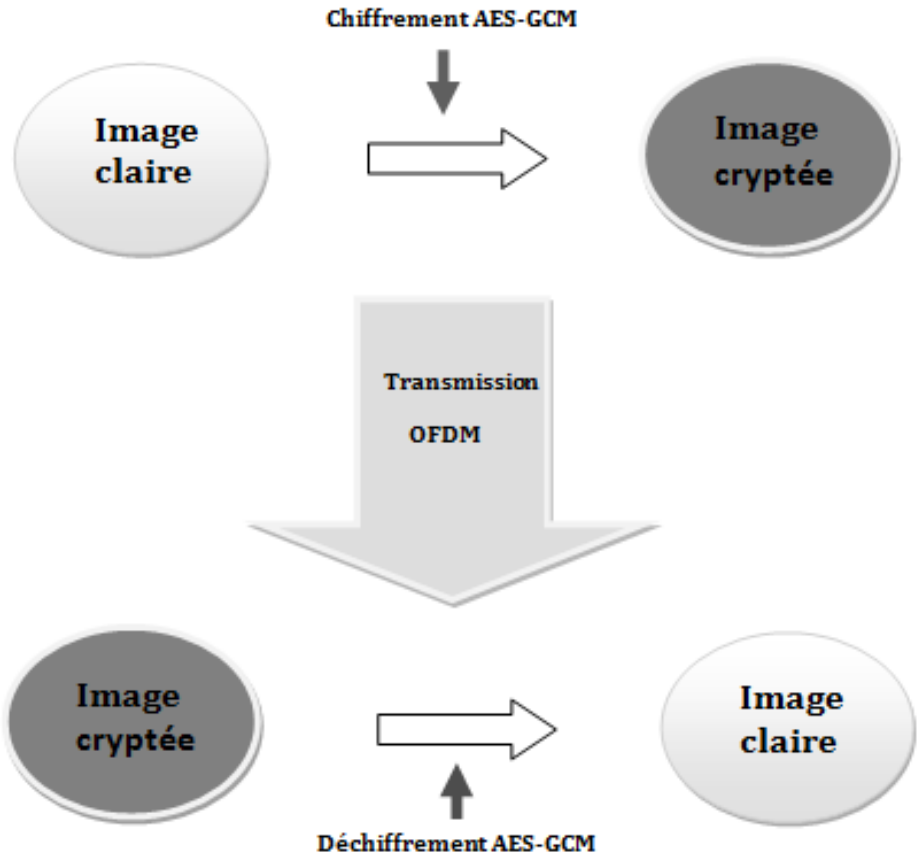

Figure 3.1 : Schéma générale de l'application

Code proposé :

```
clear all;
close all;
clc;

%% declaration
image = imread('aa.jpg');
image = double((imresize(image,[256,256])));
image = image(:,:,1);
%
key=[0;1;2;3;4;5;6;7;8;9;10;11;12;13;14;15;16;17;18;19;20;21;22;23;24;25;26
;27;28;29;30;31];
% taille_clef=input('entrer la taille de la clef:');
key=round(rand(1,128));
[m,n]=size(image);
%% Chiffrement
 %% logistic map
   % r = 3.7;
  %  x0 = 0.7;
% [Image_Crypt,in] = logistic_map(image,r,x0);
%
secretKey='5b0efc93842eca9a89eb5d652018d5713d02a5881be9241be29b8e80c9db4a4e
';
% iv='6a75d6d0bc29918ffe1fc1c1';
%[Image_Crypt,authTag] = ImageEncryption(secretKey,iv,Image_Crypt,'AES
image');

Image_Crypt = uint8(Image_Crypt);
%%



%% Déchiffrement
[Image_DeCrypt,authTagResult] =
ImageDecryption(secretKey,iv,Image_Crypt,'AES image',authTag);

%Image_DeCrypt = logistic_map_invers(Image_DeCrypt,in);
Image_DeCrypt = reshape(Image_DeCrypt,[m n]);
Image_DeCrypt = uint8(Image_DeCrypt);

%% Evaluation
Image_Crypt = reshape(Image_Crypt,[m n]);
image = reshape(image,[m n]);
figure(2)

 subplot(1,2,1);imhist(uint8(image));
 subplot(1,2,2);imhist(Image_Crypt);
%  axis([0 200 0 7000])
 Image_Crypt_entropy=entropy(Image_Crypt)
 Image_entropy=entropy(uint8(image))
 image=uint8(image);
 results = NPCR_and_UACI( image, Image_Crypt, 1, 220 )
 %%
 A=double(image);
 A2=double(Image_Crypt);
   x1 = A(:,1:end-1,:);
```

```
    y1 = A(:,2:end,:);
    Corr_horizontal= corr2(x1,y1)
%     Vertical
    x2 = A(1:end-1,:);
    y2 = A(2:end,:);
    Corr_Vertical = corr2(x2,y2)
%     diagonal
    x3 = A(1:end-1,1:end-1);
    y3 = A(2:end,2:end);
      Corr_diagonal = corr2(x3,y3)
 %%
    x4 = A2(:,1:end-1,:);
    y4 = A2(:,2:end,:);
    Corr_horizontal= corr2(x4,y4)
%     Vertical
    x5 = A2(1:end-1,:);
    y5 = A2(2:end,:);
    Corr_Vertical = corr2(x5,y5)
%     diagonal
    x6 = A2(1:end-1,1:end-1);
    y6 = A2(2:end,2:end);
      Corr_diagonal = corr2(x6,y6)
%% Affichage
figure(1);
subplot(1,3,1);imshow(image,[]);
subplot(1,3,2);imshow(Image_Crypt,[]);
subplot(1,3,3);imshow(Image_DeCrypt,[]);
%%
figure(3);
subplot(3,2,1),grafik(x1,y1),title('Horizontal');
 subplot(3,2,3),grafik(x2,y2),title('Vertical');
 subplot(3,2,5),grafik(x3,y3),title('Diagonal');
    subplot(3,2,2),grafik(x4,y4),title('Horizontal');
    subplot(3,2,4),grafik(x5,y5),title('Vertical');
    subplot(3,2,6),grafik(x6,y6),title('Diagonal');
%% Initializing parameters
% L=input('Length Of OFDM Data = ');
% Ncp=256*0.0625;
%  Ncp=2;

%% Transmitter
img=imread('aa.jpg');
img = rgb2gray(img);
img = imresize(img,[256 256]);
in=double(img);

N=numel(in);
in2=reshape(in,N,1);
bin=de2bi(in2,'left-msb');
Tx_data=reshape(bin',numel(bin),1);
len=length(Tx_data);
%%%%% padding zeroes to input %%%
z=len;
while(rem(z,2) || rem(z,4)|| rem(z,6))
    z=z+1;
    Tx_data(z,1)=0;
end

% data generation
% Tx_data=randi([0 15],L,Ncp);
%%%%%%%%%%%%%%%%%%% QAM modulation %%%%%%%%%%%%%%%%%%%%%%
```

```
%% QAM modulation
%%mod_data=qammod(Tx_data,16);
%% PSK modulation
%%mod_data= pskmod(Tx_data,4,pi/4);
%% BPSK modulation
bpskModulator = comm.BPSKModulator ;
mod_data =bpskModulator (Tx_data) ;
% Serial to Parallel
s2p=mod_data.';
% IFFT
am=ifft(s2p);
% Parallel to series
p2s=am.';
% Cyclic Prefixing
% CP_part=p2s(:,end-Ncp+1:end); %Cyclic Prefix part to be appended.
CP_part=p2s(:,end+1:end); %Cyclic Prefix part to be appended.
cp=[CP_part p2s];

%%  Reciever

% Adding Noise using AWGN
SNRstart=0;
SNRincrement=1;
SNRend=30;
c=0;
r=zeros(size(SNRstart:SNRincrement:SNRend));
PSNR=zeros(size(SNRstart:SNRincrement:SNRend));
for snr=SNRstart:SNRincrement:SNRend
    c=c+1;
    noisy=awgn(cp,snr,'measured');
% Remove cyclic prefix part
%     cpr=noisy(:,Ncp+1:Ncp+Ncp); %remove the Cyclic prefix
    cpr=noisy(:,1:end); %remove the Cyclic prefix
% series to parallel
    parallel=cpr.';
% FFT
    amdemod=fft(parallel);
% Parallel to serial
    rserial=amdemod.';
%%%%%%%%%%%%%%%%%%%% QAM demodulation %%%%%%%%%%%%%%%%%%%%
%% QAM modulation
     %%Umap=qamdemod(rserial,16);
bpskdeModulator = comm.BPSKDemodulator;
%% PSK modulation
     %%Umap= pskdemod(rserial,4,pi/4);
    %% BPSK modulation
    Umap =bpskdeModulator(rserial);
    %%
% Calculating the Bit Error Rate
    [n, r(c)]=biterr(Tx_data,Umap);
    PSNR(c)=psnr(Tx_data,Umap);
%     if PSNR(c)==inf
%         PSNR(c)=60;
%     end

end
%% Plotting BER vs SNR
figure(1)

snr=SNRstart:SNRincrement:SNRend;
semilogy(snr,r,'-o');
```

```
grid;
title('OFDM Bit Error Rate .VS. Signal To Noise Ratio');
ylabel('BER');
xlabel('SNR [dB]');

%%

Umap=reshape(Umap(1:len),8,N)';
Umap=bi2de(Umap,'left-msb');
Umap=(reshape(Umap(1:N),size(in,1),size(in,2)));

figure(3);
imshow(Umap,[]);
```

3.1 Présentation et comparaison des deux méthodes (AES) Et (AES-GCM) :

3.1.1 AES:

En plus de garantir un haut niveau de sécurité, le système AES peut chiffrer et déchiffrer rapidement de grandes quantités de données et peut donc être utilisé dans des appareils grand public tels que les ordinateurs portables, sur des matériaux comme (hardware) ou sur logiciel (software).

3.1.2 AES-GCM:

AES-GCM est apparemment à l'abri des adversaires qui peuvent choisir de manière adaptative le texte source. La considération de sécurité la plus importante est qu'il ne duplique jamais une clé. Ce problème est en partie résolu en désactivant l'utilisation d'AES-GCM avec des clés configurées de manière statique.

Le chiffrement en mode GCM présente des avantages évidents par rapport à AES, mais il semble que certains utilisateurs ne lui fassent pas assez confiance pour le recommander. La réponse peut se concentrer sur l'application que nous vous donnerons sur les propriétés de l'algorithme AES-GCM et voir comment la technique reste sans erreur, puis nous verrons comment elle fonctionne et les avantages par rapport à celle-ci d’un système de chiffrement (AES).

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

Figure3.2: Images satellitaires au niveau de gris

Les figures au-dessous montrent des images au niveau de gris de Lena et cameraman :

Figure3.3: des images au niveau de gris de Lena et cameraman

3.2 Résolution des images satellitaire :

Typiquement, la résolution spatiale est donnée par la taille des pixels. La résolution radiométrique est une suite de valeurs discrètes correspondant à la luminosité. La résolution temporelle utilisée pour un projet particulier n'est qu'une mesure de la fréquence à laquelle les mêmes données sont obtenues.

La résolution spectrale représente les données prises dans une certaine longueur d'onde.

Le tableau ci-dessous montre quelque résolution de nos images satellitaire :

Image	**Résolution spatiale**	**Résolution spectrale**	**Résolution radiométrique**
Image (A)	Haute résolution de 10 à 30m	bande du vert	16 levels (8 bits)
Image (B)	haute résolution de 10 à 30m	bande du vert	16 levels (8 bits)
Image (C)	haute résolution de 10 à 30m	bande du vert	16 levels (8 bits)

Tableau 3.1 Résolution des images satellitaire

3.3 Chiffrement et déchiffrement AES:

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

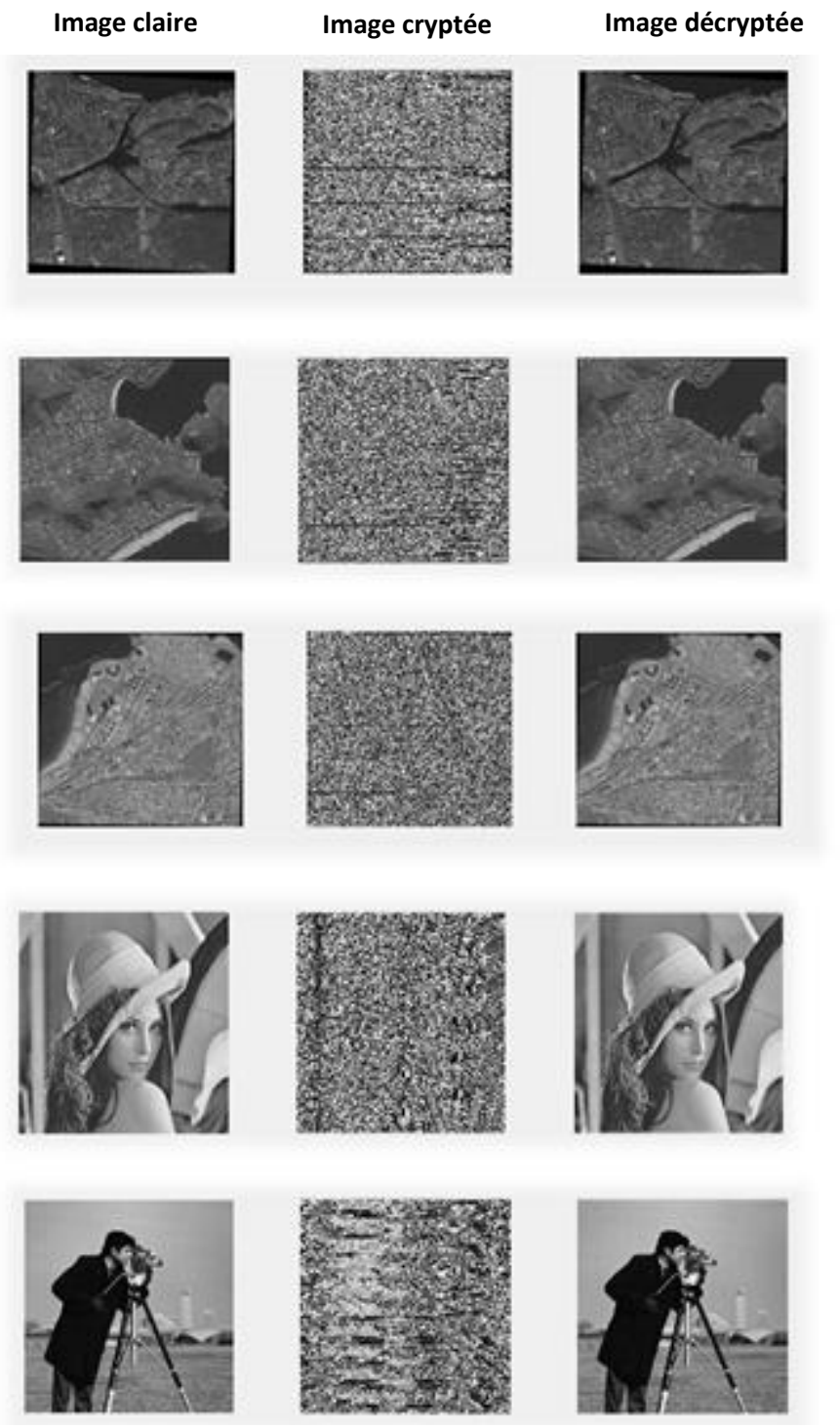

Figure 3.4 : Des images cryptées et décryptées en utilisant la méthode AES.

3.4 Chiffrement et déchiffrement AES-GCM :

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

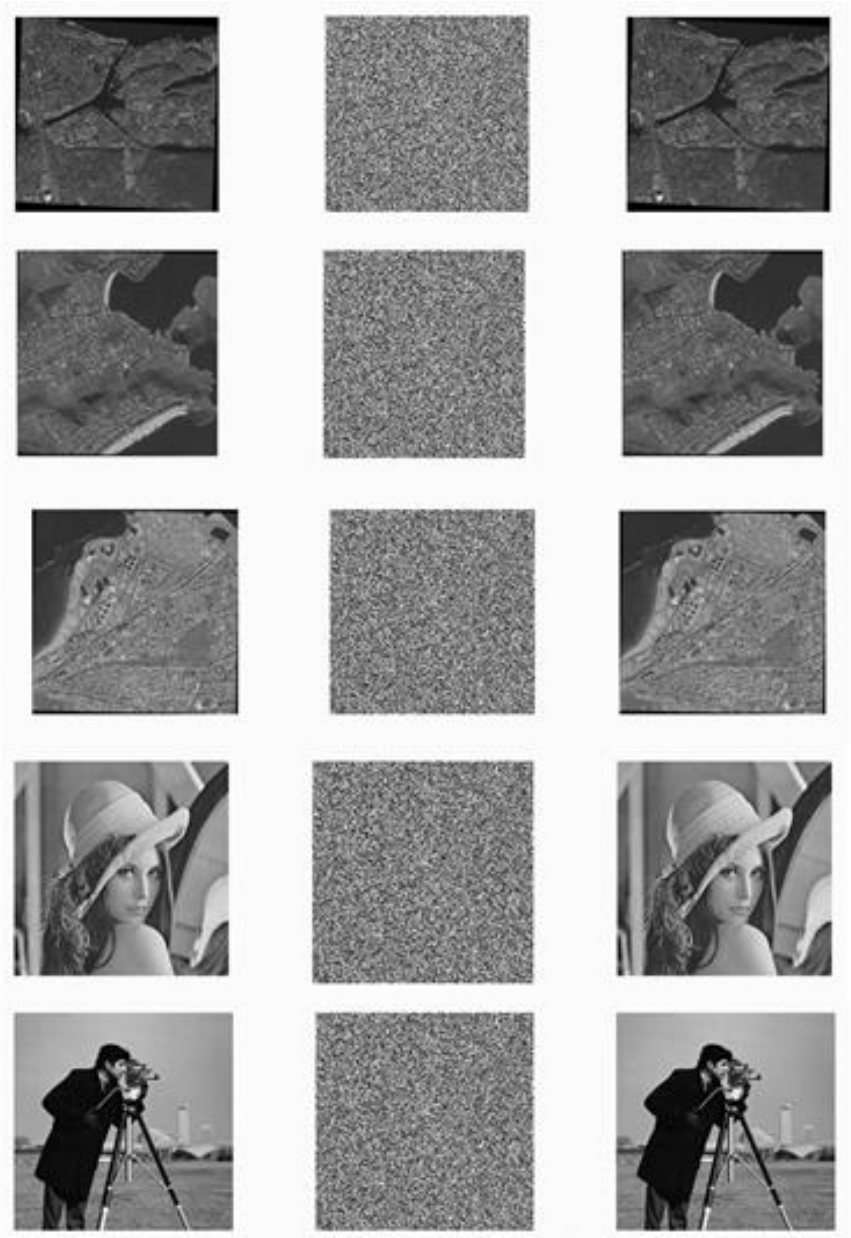

Figure 3.5 : Des images cryptées et décryptées en utilisant la méthode AES-GCM.

4. Les tests statistiques:

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

4.1. L'histogramme :

L'histogramme est une représentation graphique qui permet de connaître la répartition des intensités lumineuses des pixels [43]

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) :

- 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.

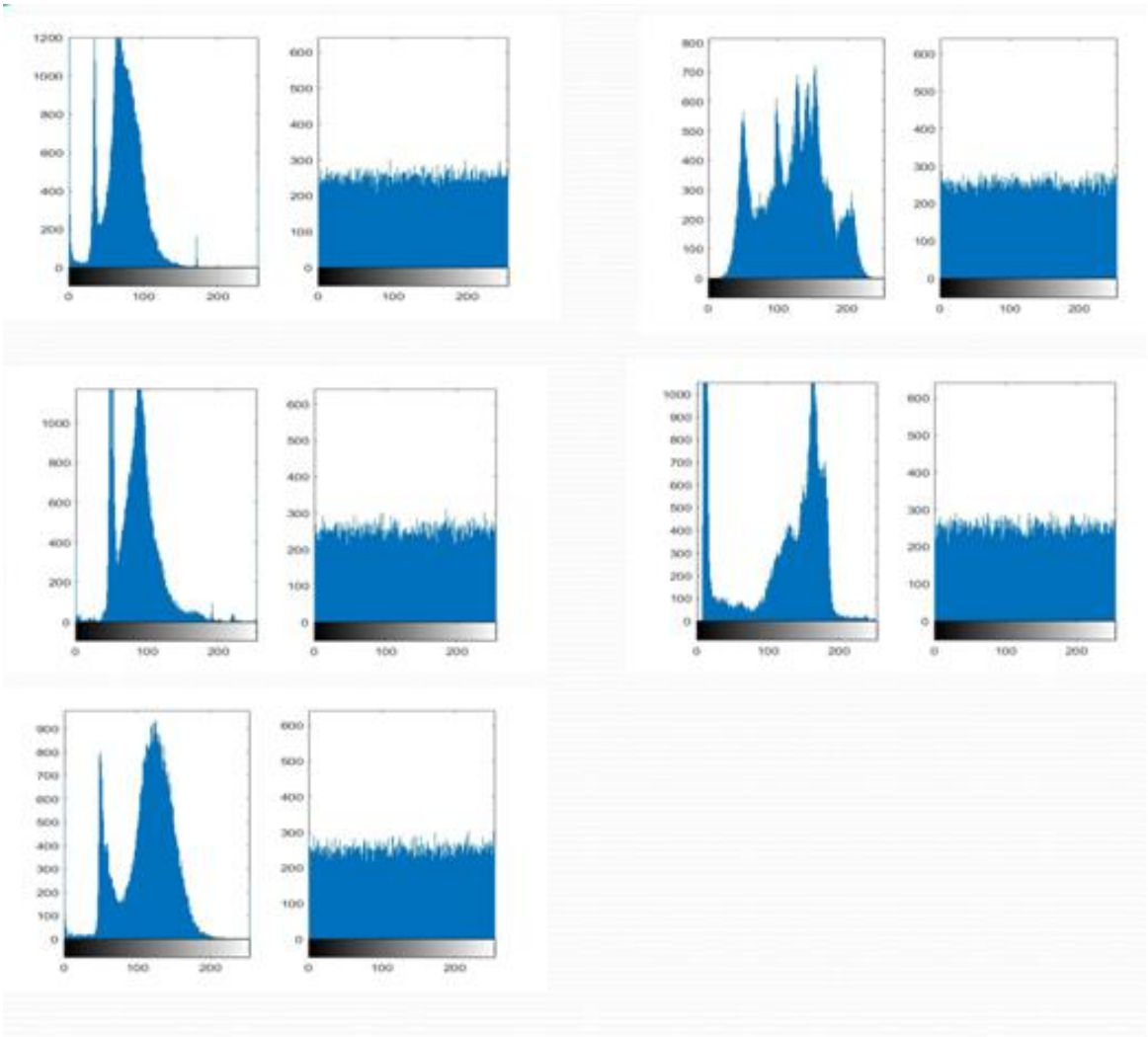

Figure 3.6 **:** les histogrammes des images claires et chiffrées.

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

4.2 Les paramètres d'évaluations :

Le tableau ci-dessous montre les paramètres d'évaluations et leurs équations :

Nom	Rôle	Equation

L'entropie	L'entropie est une mesure statistique du caractère aléatoire qui peut être utilisée pour caractériser la texture de l'image d'entrée.	$H(m) = \sum_{i=0}^{2^{n-1}} p(m)_i log_2 \frac{1}{p(m_i)}$
Corrélation	Pour étudier la corrélation entre les pixels.	$r_{xy} = cov(x,y)/(\sqrt{D(x)D(y)}$ tel que : $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$ $E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i)$ $cov(x,y) = \frac{1}{N} = \sum_{i=1}^{N}((x_i - E(x)(y_i - E(y)))$
NPCR	Le NPCR mesure le pourcentage de pixels différents dans les deux images.	$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100$
UACI	UACI (intensité unifiée moyenne évolutive)	$UACI = \frac{1}{M \times N}[\sum_{i,j} \frac{(c1(i,j) - c2(i,j)}{255}] \times 100$

Tableau 3.2: Les paramètres d'évaluations

4.2.1 L'entropie:

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.

Le tableau ci-dessous montre les valeurs de l'entropie de nos images au niveau de gris et leurs valeurs chiffrées :

Image	**Type**	**Entropie de l'image claire**	**Entropie de l'image claire**	**Entropie de l'image Chiffré avec (AES)**	**Entropie de l'image Chiffré avec (AES-GCM)**
Image «A»	Niveau de gris	6.5772	6.5772	6.5804	7.9979
Image «B»	Niveau de gris	6.6583	6.6583	6.6604	7.9968
Image «C»	Niveau de gris	7.0533	7.0533	7.0543	7.9974
Lena	Niveau de gris	7.4579	7.4579	7.4589	7.9977
cameraman	Niveau de gris	7.0853	7.0853	7.0867	7.9972

Tableau3.3: Les valeurs d'entropie des images et des images cryptée.

4.2 .2 La corrélation :

Les pixels voisins dans les images nettes sont connus pour être fortement corrélés, mais dans les images cryptées avec les meilleurs algorithmes de cryptage, ces pixels deviennent faiblement corrélés. [44]

Pour étudier la corrélation, nos images sont chiffrées à l'aide de deux algorithmes de chiffrement proposés. Ensuite on calcule les coefficients de corrélation de l'image et de l'image cryptée de chaque méthode dans les trois directions (verticale, horizontale et diagonale)

- **Pour l'AES:**

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

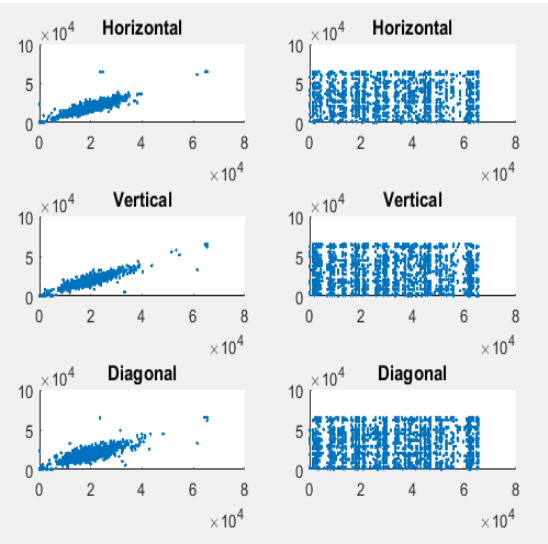

Figure 3.7: les corrélations horizontale, vertical et diagonal de l'image «A» et de son image cryptée.

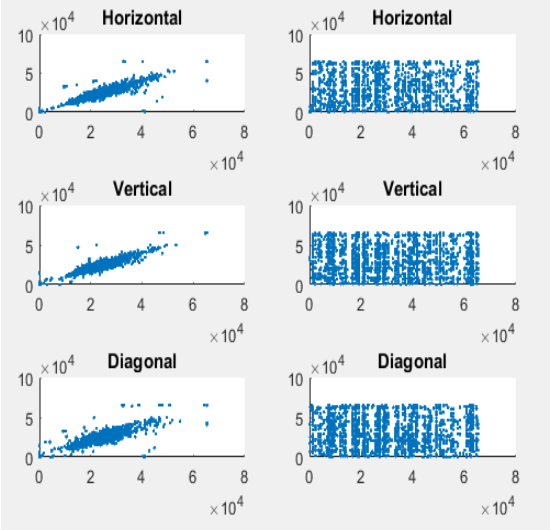

Figure 3.8: les corrélations horizontale, vertical et diagonal de l'image «B» et de son image cryptée.

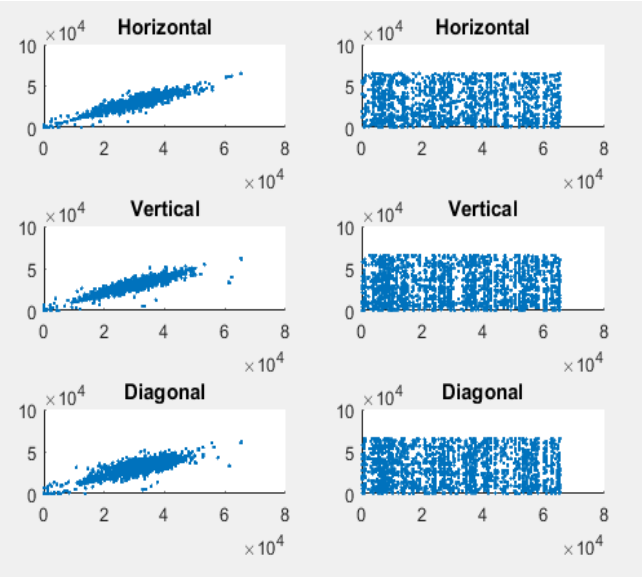

Figure 3.9: les corrélations horizontale, vertical et diagonal de l'image «C» et de son image cryptée.

Les résultats de calcul dans les tableaux ci-dessous:

Corrélation	Image «A»	Image cryptée
Diagonal	0.8762	0.0102
Horizontal	0.9329	0.1574
Vertical	0.9466	0.0131

Tableau3.4: Coefficients de corrélation entre l'image «A» et l'image chiffrée.

Corrélation	Image «B»	Image cryptée
Diagonal	0.8858	-0.0017
Horizontal	0.9276	0.1327
Vertical	0.9555	6.9881e-04

Tableau3.5: Coefficients de corrélation entre l'image «B» et l'image chiffrée.

Corrélation	Image «C»	Image cryptée
Diagonal	0.8911	0.0019
Horizontal	0.9499	0.0605
Vertical	0.9440	0.0037

Tableau3.6: Coefficients de corrélation entre l'image «C» et l'image chiffrée.

- **Pour AES-GCM:**

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

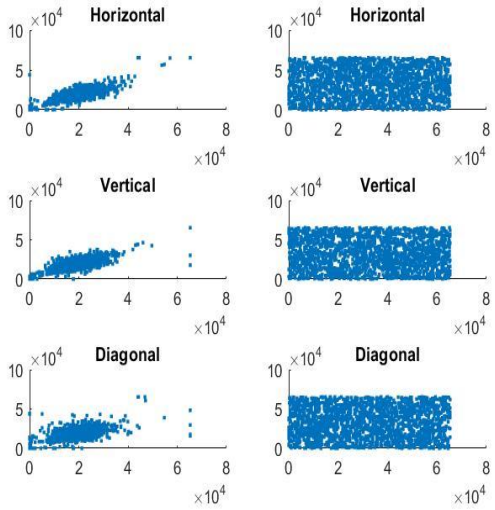

Figure 3.10: les corrélations horizontale, vertical et diagonal de l'image «A» et de son image cryptée.

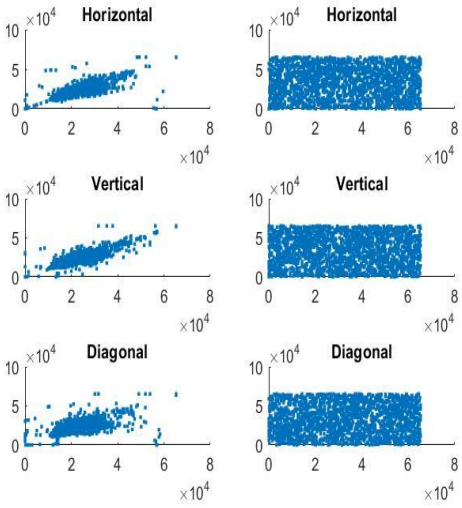

Figure 3.11: les corrélations horizontale, vertical et diagonal de l'image «B» et de son image cryptée.

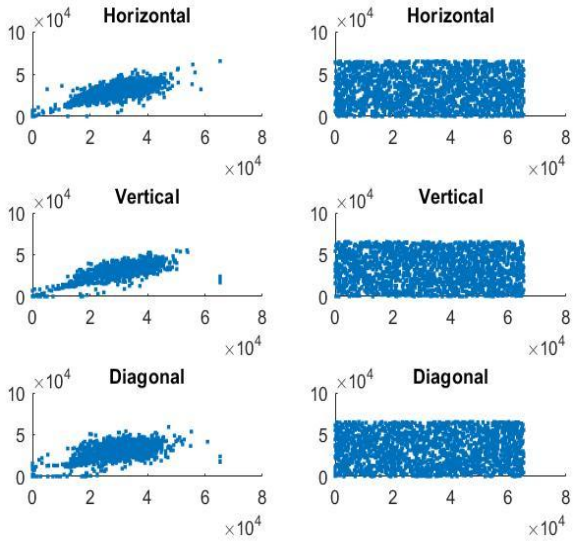

Figure 3.12: les corrélations horizontale, vertical et diagonal de l'image «C» et de son image cryptée.

Les résultats de calcul dans les tableaux ci-dessous:

Corrélation	Image «A»	Image cryptée
Diagonal	0.8762	0.0059
Horizontal	0.9329	0.0034
Vertical	0.9466	0.0038

Tableau3.7: Coefficients de corrélation entre l'image «A» et l'image chiffrée.

Corrélation	Image «B»	Image cryptée
Diagonal	0.8858	-0.0012
Horizontal	0.9276	0.0072
Vertical	0.9555	0.0066

Tableau3.8: Coefficients de corrélation entre l'image «B» et l'image chiffrée.

Corrélation	Image «C»	Image cryptée
Diagonal	0.8911	2.3659e-04
Horizontal	0.9499	0.0015
Vertical	0.9440	0.0047

Tableau3.9: Coefficients de corrélation entre l'image «C» et l'image chiffrée.

➢**Pour l'AES :**

La figure ci dessus montre les courbes des corrélations de l'image origine et l'image cryptée de Lena et cameraman:

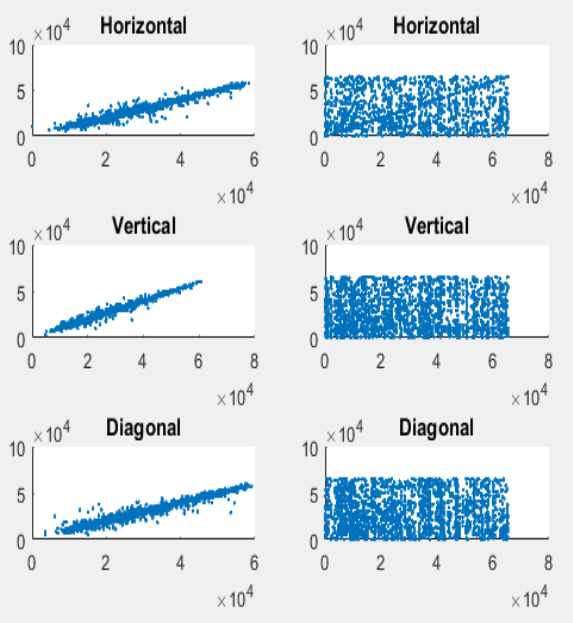

Figure 3.13: les corrélations horizontale, vertical et diagonal de Lena et de son image cryptée.

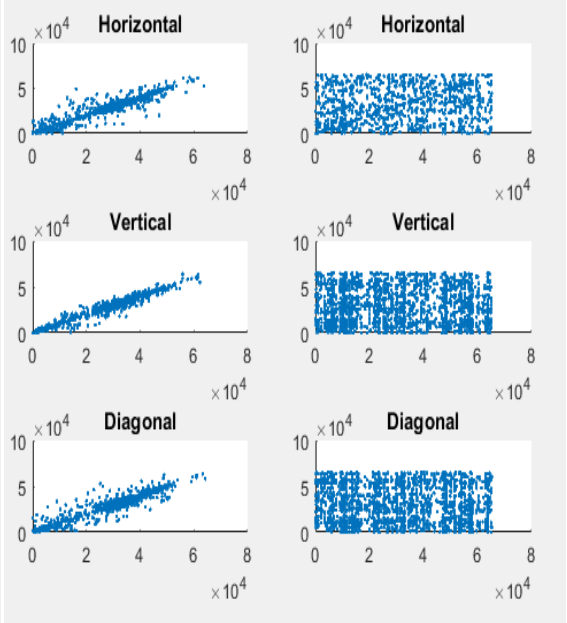

Figure 3.14: les corrélations horizontale, vertical et diagonal de cameraman et de son image cryptée.

Les résultats de calcul dans les tableaux ci-dessous:

Corrélation	Image Lena	Image cryptée
Diagonal	0.9758	0.0056
Horizontal	0.9850	0.2260
Vertical	0.9928	0.0051

Tableau3.10: Coefficients de corrélation entre l'image Lena et l'image chiffrée.

Corrélation	Image cameraman	Image cryptée
Diagonal	0.9735	0.0225
Horizontal	0.9833	0.4333
Vertical	0.9901	0.0264

Tableau3.11: Coefficients de corrélation entre l'image cameraman et l'image chiffrée.

➢ **Pour l'AES-GCM :**

La figure ci dessus montre les courbes des corrélations de l'image origine et l'image cryptée de Lena et cameraman:

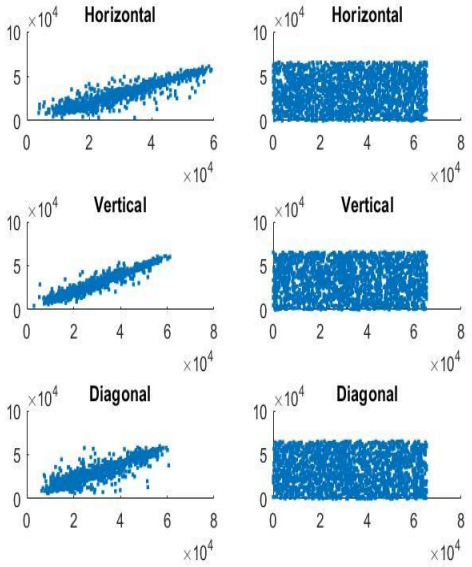

Figure 3.15: les corrélations horizontale, vertical et diagonal de l'image «Lena» et de son image cryptée.

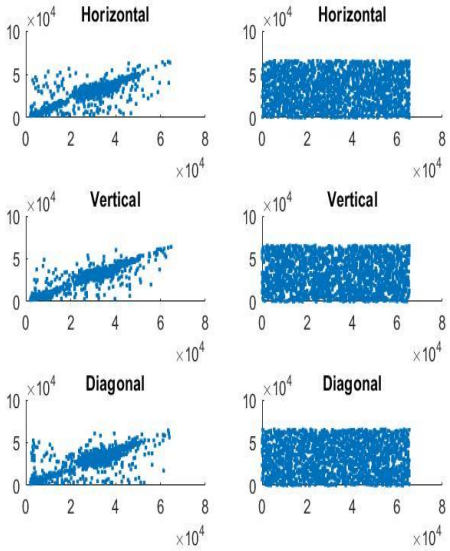

Figure 3.16: les corrélations horizontale, vertical et diagonal de l'image «cameraman» et de son image cryptée.

Les résultats de calcul dans les tableaux ci-dessous:

Corrélation	Image Lena	Image cryptée
Diagonal	0.9758	-5.3695e-04
Horizontal	0.9850	2.8562e-04
Vertical	0.9928	-0.0055

Tableau3.12: Coefficients de corrélation entre l'image Lena et l'image chiffrée.

Corrélation	Image cameraman	Image cryptée
Diagonal	0.9735	-0.0060
Horizontal	0.9833	-0.0021
Vertical	0.9901	0.0040

Tableau3.13: Coefficients de corrélation entre l'image cameraman et l'image chiffrée.

4.2.3 NPCR :

NPCR (taux de changement de nombre de pixels) entre deux images de même taille pour mesure le pourcentage de pixels différents dans les deux.

Le tableau ci-dessous montre les valeurs de NPCR de nos images origines et chiffrées avec les deux méthodes :

Nom	Type	La valeur de NPCR pour (AES)	La valeur de NPCR pour (AES-GCM)
Image «A»	Niveau de gris	99.61	99.59
Image «B»	Niveau de gris	99.54	99.56
Image «C»	Niveau de gris	99.12	99.61
Lena	Niveau de gris	99.31	99.60
Cameraman	Niveau de gris	99.47	99.65

Tableau 3.14: Les valeurs de NPCR entre deux images claires et chiffrées.

4.2.4 UACI :

Le tableau ci-dessous montre la liste des valeurs UACI entre deux images (origine et chiffrées) avec les deux méthodes :

Nom	Type	La valeur d'UACI pour (AES)	La valeur d'UACI pour (AES-GCM)
Image «A»	Niveau de gris	35.38	33.62
Image «B»	Niveau de gris	31.53	33.20
Image «C»	Niveau de gris	32.32	32.32
Lena	Niveau de gris	33.96	33.12
Cameraman	Niveau de gris	38.57	33.57

Tableau 3.15: Les valeurs de UACI entre deux images origine et chiffrées.

5. Etude comparative et interprétation des résultats :

Dans cette étude, nous comparons notre algorithme proposé avec une autre technique de chiffrement d'image. Nous analysons d'abord les résultats de la comparaison :

➢ Les résultats de tableau (3.3) montre que les valeurs de l'entropie des images chiffrées avec les méthodes proposée (AES-GCM) est plus proche à la valeur 8 que la 2éme méthode (AES). Cela montre qu'il est difficile d'avoir la prévisibilité d'information dans notre méthode (l'AES-GCM) que l'autre (L'AES).

➢On sait que la corrélation étudier la corrélation entre les pixels, alors les valeurs des coefficients de corrélation dans notre méthodes son très faibles dans les trois niveaux (diagonal, horizontal, vertical) que la 2éme méthode, Cela indique quel l'algorithme proposé supprimé avec succès la corrélation des pixels adjacent que l'autres algorithme.

- Les résultats des tableaux (3.1) (3.15) ce montres que les valeurs de NPCR et UACI sont élevées dans notre algorithme, alors elle résiste au attaques différentielles.

6. Simulations et résultats du BER en fonction du rapport signal sur bruit (SNR):

Pour réaliser la simulation de la transmission OFDM, nous avons considéré l'approche suivante :

- Simuler les performances pour différentes valeurs de l'intervalle de garde ou préfix cyclique (NCP= 256)**.**
- Simuler les performances pour différents modulation (pour QAM-16, PSK, BPSK).
- Simuler les performances pour un canal à bruit blanc gaussien (AWGN).

Les tableaux ci-dessous montrent les valeurs de BER en fonction du rapport signal sur bruit (SNR) pour une transmission d'un système communication OFDM pour différents modulation (QAM-16, PSK, BPSK) de nos images :

- **1er image satellitaire :**

SNR	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
QAM-16	0.251	0.236	0.223	0.208	0.194	0.178	0.161	0.143	0.124	0.105	0.086	0.067	0.050	0.046	0.030	0.018
PSK	0.212	0.180	0.145	0.112	0.081	0.055	0.034	0.018	0.009	0.003	0.001	3.0135e-04	6.1988e-05	1.9073e-06	0	0
BPSK	0.078	0.056	0.038	0.022	0.125	0.006	0.002	7.781e-04	2.365e-04	4.005e-05	3.814e-06	0	0	0	0	0

Tableau 3.16: Les valeurs de BER en fonction du rapport signal sur bruit (SNR) pour les 3 modulations

La figure suivante représente les résultats de simulation du BER en fonction du rapport signal sur bruit (SNR) pour un canal AWGN pour les 3 modulations de la 1ère image satellitaire :

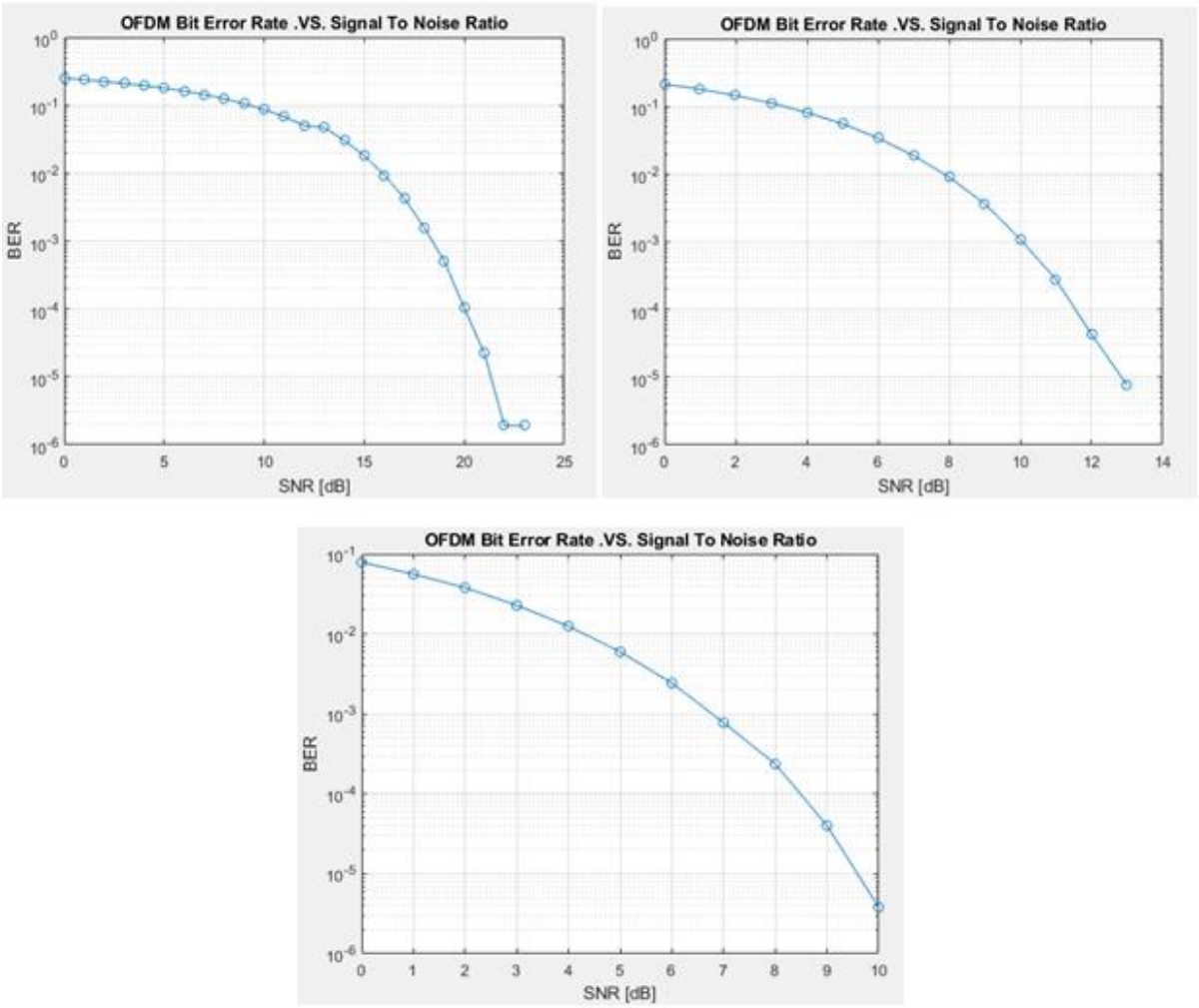

Figure 3.17 : BER en fonction de SNR pour un Canal AWGN des trois modulations.

- **2éme image satellitaire :**

SNR	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
QAM-16	0.257	0.2422	0.2229	0,2214	0,1999	0,1782	0,1665	0,1446	0,1227	0,1006	0,0886	0,0667	0,0049	0,00459	0,029	0,017
PSK	0,213	0,1779	0,145	0,111	0,081	0,055	0,033	0,018	0,009	0,003	0,001	0,0002	4,95e-05	3,81e-06	0	0
BPSK	0.079	0.056	0.037	0.023	0.012	0.006	0.002	8.296e-04	1.583e-04	3.242e-05	3.814e-06	1.907e-06	0	0	0	0

Tableau 3.17: Les valeurs de BER en fonction du rapport signal sur bruit (SNR) pour les 3 modulations

La figure suivante montre les résultats de simulation du BER en fonction du rapport signal sur bruit (SNR) dans un canal AWGN pour les 3 modulations de la 2éme image satellitaire :

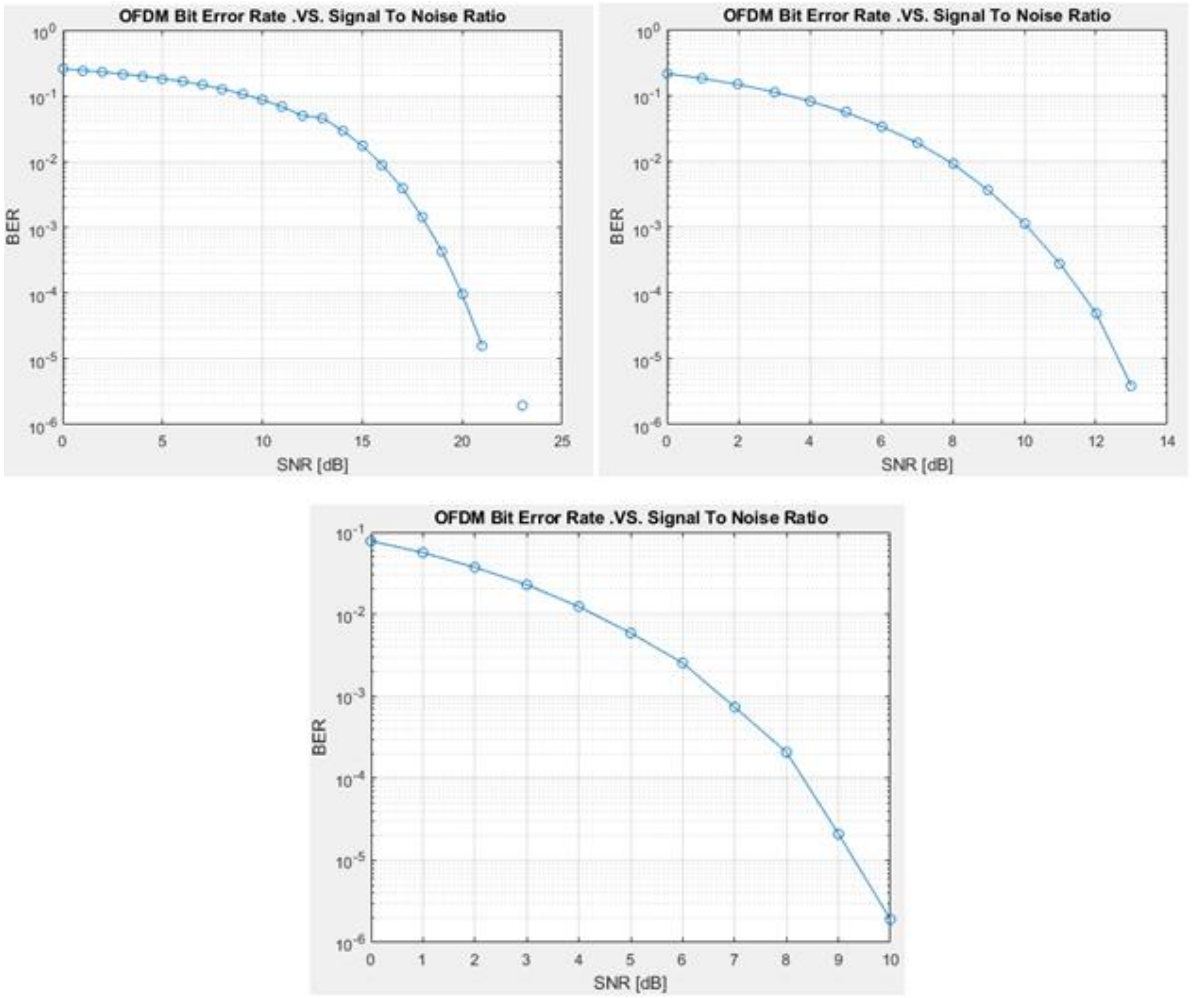

Figure 3.18 : BER en fonction de SNR pour un Canal AWGN des trois modulations

- **3éme image satellitaire :**

SNR	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
QAM-16	0,257	0,244	0,230	0,215	0,200	0,184	0,166	0,147	0,127	0,106	0,086	0,067	0,049	0,046	0,029	0,016
PSK	0,212	0,179	0,145	0,111	0,081	0,055	0,033	0,018	0,009	0,003	0,001	0,0003	6,67e-05	7,62e-06	0	0
BPSK	0.078	0.056	0.037	0.023	0.012	0.005	0.002	8.316e-04	1.983e-04	3.623e-05	1.907e-09	0	0	0	0	0

Tableau 3.18: Les valeurs de BER en fonction du rapport signal sur bruit (SNR) pour les 3 modulations

La figure suivante représente les résultats de simulation du BER en fonction du rapport signal sur bruit (SNR) dans un canal AWGN pour les 3 modulations :

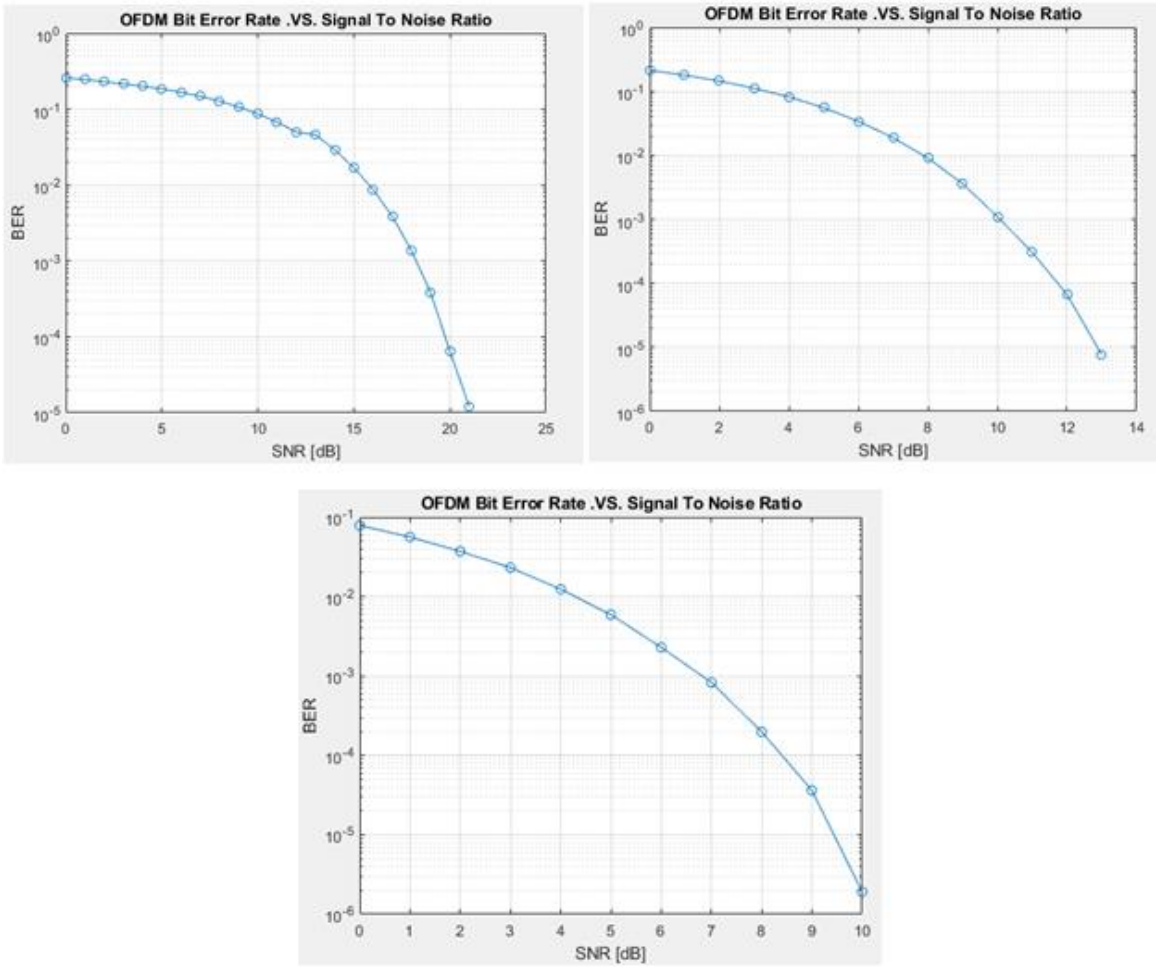

Figure 3.19 : BER en fonction de SNR pour un Canal AWGN des trois modulations

- **Image de Lena :**

SNR	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
QAM-16	0,258	0,244	0,231	0,216	0,200	0,184	0,166	0,147	0,127	0,107	0,087	0,067	0,049	0,045	0,028	0,016
PSK	0,212	0,178	0,144	0,112	0,081	0,055	0,034	0,018	0,008	0,003	0,001	0,000	5,62e-05	1,23e-05	1,90e-06	0
BPSK	0.078	0.056	0.037	0.022	0.012	0.006	0.002	8.392e-04	1.792e-04	5.722e-05	5.722e-06	0	0	0	0	0

Tableau 3.19: Les valeurs de BER en fonction du rapport signal sur bruit (SNR) pour les 3 modulations de l'image de Lena.

La figure suivante représente les résultats de simulation du BER en fonction du rapport signal sur bruit (SNR) dans un canal AWGN pour les 3 modulations de l'image de Lena :

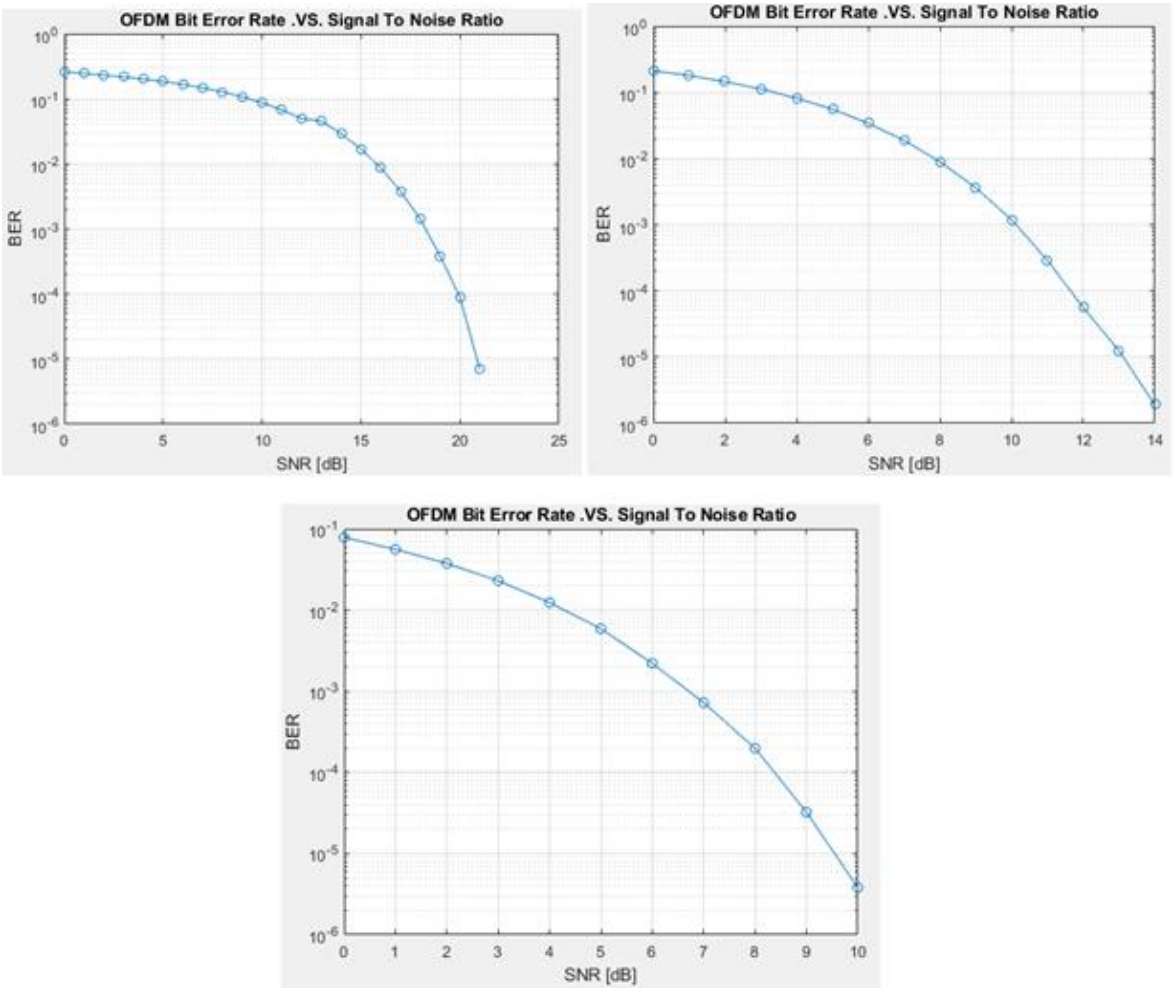

Figure 3.20 : BER en fonction de SNR pour un Canal AWGN des 3 modulations de Lena

- **Image cameraman :**

SNR	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
QAM-16	0,256	0,2411	0,2228	0,2213	0,1999	0,1783	0,1665	0,1446	0,1227	0,1006	0,0886	0,0067	0,0066	0,0046	0,029	0,017
PSK	0,213	0,178	0,1145	0,1112	0,0881	0,0654	0,0433	0,0218	0,0008	0,0003	0,0001	0,0001	5,43e-05	5,72e-06	3,81e-06	0
BPSK	0.078	0.056	0.0237	0.0122	0.0012	0.0005	0.0002	7.553e-04	2.0240e-04	3.0351e-05	1.9907e-06	0	1.9907e-06	0	0	0

Tableau 3.20: Les valeurs de BER en fonction du rapport signal sur bruit (SNR) pour les 3 modulations de l'image de cameraman.

La figure suivante représente les résultats de simulation du BER en fonction du rapport signal sur bruit (SNR) dans un canal AWGN pour les 3 modulations de l'image de cameraman :

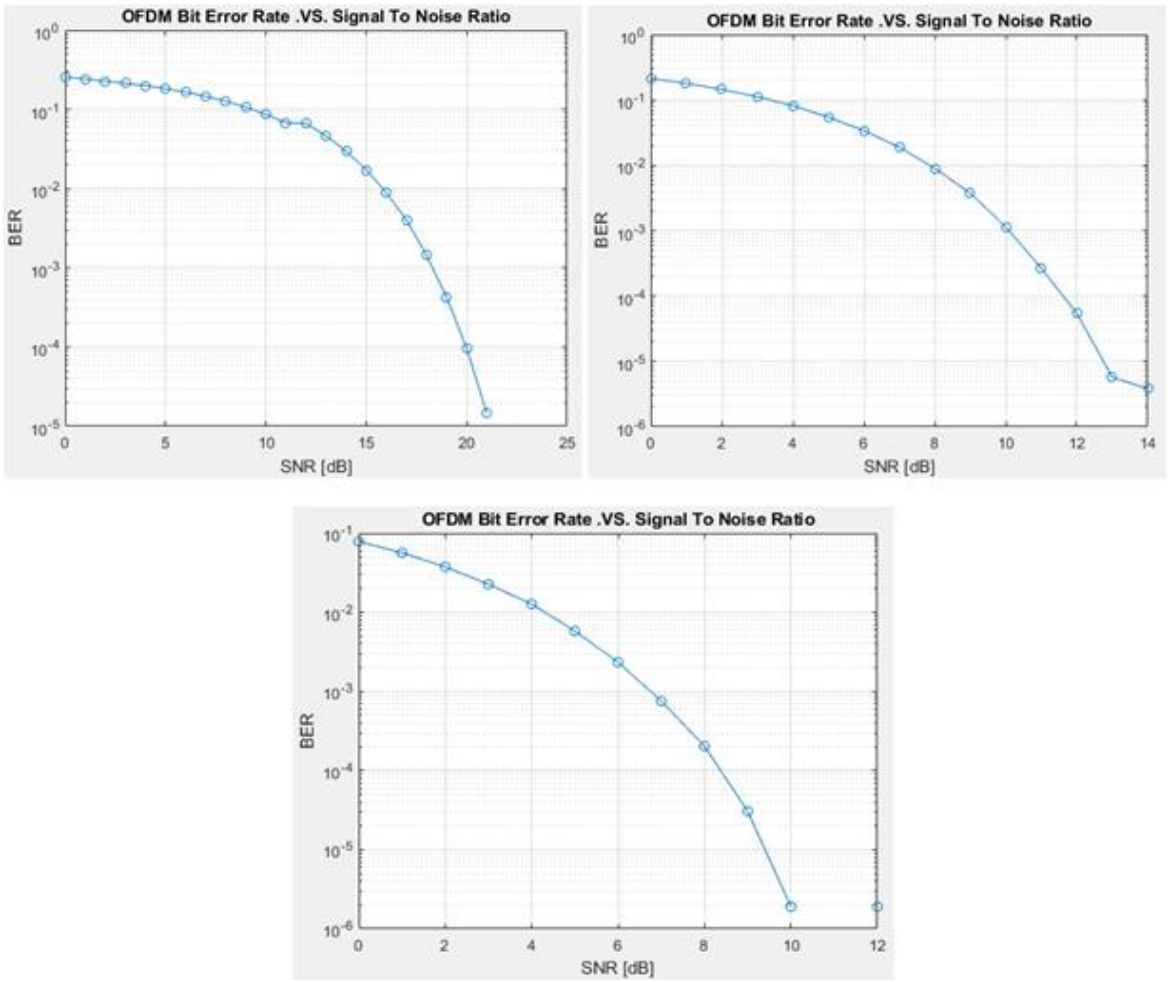

Figure 3.21 : BER en fonction de SNR pour un Canal AWGN des 3 modulations de cameraman.

6.1 Interprétation des résultats :

Dans les figures et les tableaux précédant, nous avons montré la variation du BER en fonction de l'Eb/No pour trois modulations (QAM-16, PSK et BPSK), Nous avons constaté que le BER reste presque nul même en présence d'un bruit du canal, alors on voie que la meilleur modulation c'est la **(BPSK)** parce que toutes ces valeurs dans les tableaux sont presque nul que les deux autres modulations.

7. 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. - GCM, et l'étude de l'effet du bruit de canal sur la transmission OFDM.

Les simulations réalisées dans ce travail nous permettent de voir les avantages de notre méthode en calculant les paramètres d'évaluation pour un bon cryptage, cette étude permet également d'analyser le BER en termes de rapport signal sur bruit (SNR) avec une modulation BPSK, Nous avons dit que même s'il y a un bruit de canal, il reste également nul, ce qui permet de prédire la qualité des transmissions OFDM.

Conclusion Générale

Conclusion Générale

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-GCM et l'une des transmissions pour les systèmes de communication OFDM, et nous évaluons ses performances en utilisant l'algorithme sur Matlab R2015b.

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.

Notre algorithme peut également analyser le BER en termes de rapport signal sur bruit (SNR), qui reste également nul avec une modulation BPSK., permettant de prédire la qualité des transmissions OFDM.

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.

Référence

Références

[1] www.docplayer.fr, consulté le : 02/03/2022

[2] https://www.malekal.com/quest-ce-que-le-chiffrement-aes-et-comment-ca-marche/, consulté le : 02/03/2022

[3] R. Dumont, Année 2009 – 2010 Cryptographie et Sécurité informatique, Notes de cours provisoires, Université de Liège,

[4] https://www.oracle.com/fr/security/qu-est-ce-que-la-cryptographie.htm, consulté le : 01/03/2022

[5] www.blog.mailfence.com, consulté le : 01/03/2022

[6] dspace.univ-tlemcen.dz, consulté le : 01/03/2022

[7] https://librecours.net/module/culture/intro-chiffrement/chiffrement-sym.xhtml, consulté le : 02/03/2022

[8] www.mcours.net, consulté le: 20/03/2022

[9] depositum.uqat.ca, consulté le: 22/03/2022

[10] http://www.cryptage.org/images-cryptees.html, consulté le: 07/04/2022

[11] G. Labouret. Année 2001, « Introduction à la cryptographie. HSC - Herve Schauer Consultants » - Cabinet de consultants en sécurité informatique, Http://www.hsc.fr/.

[12] www.malekal.com, consulté le: 22/03/2022

[13] www.cnria.cci.ucad.sn, consulté le: 22/03/2022

[14] www.ummto.dz, consulté le: 30/03/2022

[15] https://www.malekal.com/quest-ce-que-le-chiffrement-aes-et-comment-ca-marche/, consulté le : 07/04/2022

[16] www.Easytp.cnam.fr, consulté le: 02/04/2022

[17] https://blog.hubspot.fr/marketing/differents-types-fichiers-image, consulté le : 17/04/2022

[18] Les formats d'images numériques, Serge WACKER – C2I niveau 1, http://www.montpellier.iufm.fr/technoprimaire, consulté le: 02/04/2022.

[19] Image file formats. Wikipedia, Https://en.wikipedia.org/wiki/Image_file_formats, consulté le : 17/04/2022

[20] MOUSSELMEL Z et HOUTIA C , Année (2019/2020) , Mémoire de fin d'étude , Préparé par C , Encadré par Mr. OUAHAB

[21] https://www.semanticscholar.org/paper/Implementation-of-AES-GCM-encryption-algorithm-for-Arun-Vanisree/2c8c50103faa588b649abe4747c446d8549aa65c, consulté le : 17/04/2022

[22] https://i0.wp.com/blog.oureducation.in/wp-content/uploads/2013/05/fdma_tdma_cdma.jpg?ssl=1, consulté le :04/05/2022

[23] Adrien Renoult, Année 1 décembre 2000 « Analyse des performances d'un système multi-utilisateurs OFDM codé sans accès orthogonal », Université de Cergy-Pontoise.

[24] Lang, S.; Rao R.; Daneshrad, B, Année 6-12, June 2004 « Design and development of a 5.25 GHz software defined wireless OFDM communication platform,"IEEE Commun. Mag., vol. 42, no. 6, pp. »

[25] Olivier BERDBER, Année 20 Décembre 2002. « Optimisation et stratégies d'allocation de puissance des systèmes de transmission multi-antennes », Université de Bretagne Occidentale,

[26] A.B. Ben Jemâa, Année 2004 « etude comparative des estimators du canal WSSUS en standard DVB-T », rapport de mémoire de master, Ecole Nationale d'Ingénieur de Tunis, 2004.

[27] https://www.researchgate.net/figure/Principe-theorique-de-la-modulation-OFDM_fig3_30512361, consulté le :06/05/2022

[28] K Fazel and S Kaiser, Année 2008« Multi-Carrier and Spread Spectrum Systems», . New York: John Wiley & Sons.

[29] Mounia LOURDIANE, Année le 31 janvier 2005 « CDMA à séquence directe appliqué aux communications Optiques », Paris le 31 janvier 2005.

[30] Melal.K, MAGISTER, Année Novembre 2008, en Micro -Ondes Pour Systèmes de télécommunications « Analyse des méthodes d'égalisation des techniques CDMA »

[31]http://www.telecom.ulg.ac.be/teaching/notes/multimedia/node63_ct.html, consulté le : 07/05/2022

[32]https://cms.geobretagne.fr/sites/default/files/documents/fiches_2_comprendre_une_image_satellitaire_1.pdf, consulté le : 10/05/2022

[33] GHANIMA.D, Année 13 septembre 2014/2015 Doctorat en Sciences en physique, thème « Comparatif de méthodes avancées pour la fusion d'images satellites.

[34] ADEL OMAR.D, Année OCTOBRE 2004, DOCTORAT EN GÉNIE ÉLECTRIQUE ,thème « MÉTHODE DE DÉTECTION À USAGERS MULTIPLES POUR LES SYSTÈMES DE COMMUNICATION DS-CDMA ».

[35] A.B. Ben Jemâa,Année 2004 « étude comparative des estimators du canal WSSUS en standard DVB-T », rapport de mémoire de master, Ecole Nationale d'Ingénieur de Tunis.

[36] Mr. BENDELHOUM .M.S, Année 13 décembre 2018 « Évaluation des performances des images compressées par l'algorithme TOD-SPIHT, et transmises via le système MC-CDMA » Thèse de Doctorat en Sciences Spécialité : Télécommunications

[37] M BenyarouAnnée 2013, "Optimisation des systèmes multi-antennes : appliqués aux systèmes MC-CDMA," Thèse de Doctorat, Université de Tlemcen.

[38] HADDADI.b FACI.s , Année juillet 2015 « Etude et simulation sous MATLAB de la

4G LTE, Mémoire de Fin d'Etude de MASTER ACADEMIQUE » en Génie électrique: Télécommunication et réseaux.

[39] http://adslproject.free.fr/prefixe_cyclique.htm, consulté le : 17/05/2022

[40] Stéphane.n. Année janvier 2004 « Etude et optimisation des techniques MC-CDMA pour les futures générations de systèmes de communications hertziennes ».

[41] https://www.researchgate.net/figure/Block-diagram-for-MC-CDMA_fig3_3897448, consulté le :17/05/2022

[42] BENYEKKOU Amine ILYES BENSALAH Mohamed Noureddine, Année 27 /08/ 2020, «EFFET DU BRUIT DU CANAL SUR LA TRANSMISSION OFDM». Université Abdelhamid Ibn Badis de Mostaganem– Faculté des Sciences et de la Technologie.

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

[44]Ounzar Asma, Année2014/2015 « Cryptage complet/partiel d'une image/vidéo par un signal sinusoïdal » Université Larbi Ben M'hidi Oum El Bouaghi,