République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université 8 Mai 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 et Télécommunications**

Sécurisation de la Couche Physique OFDM Dans un Réseau de Capteurs : Application sur les Images Médicales

---

Présenté par :
ELHACHI HANA

Sous la direction de :
Dr. ABED DJAMEL

Juillet 2019

Remerciement

mon remerciement et mon gratitude sont destinés à Dieu qui m'a permis de réussir et de poursuivre le chemin de savoir et de m'avoir donné la capacité, la volonté et la force afin de mener à bien ce projet de fin d'étude.

Ainsi qu'a Dr ABED Djamel qui a fait honneur à son engagement par : ses conseils, ses remarques précieuses, sa patience et sa sincérité qui nous ont aidé d'arriver à ce travail.

Je remercie également les membres de jury, qu'ils trouvent à travers ces expressions mes sincères remerciements pour l'honneur qui m'a fait en acceptant d'examiner ce travail.

Un grand merci à tous les enseignants qui ont contribués à ma formation depuis l'école primaire jusqu'aux études universitaires.

Enfin, je remercie énormément tous ceux qui ont participé de près ou de loin et qui ont contribué à l'élaboration de ce travail.

MERCI

To My family and Technological World.

Elhachi Hana

Résumé

L'engouement du grand public pour les objets communicants et l'évolution des réseaux de capteur a entrainé le besoin de transférer de manière sécurisée des quantités d'informations multimédia. D'autre part le format de modulation OFDM est devenu un standard dans la couche physique de la plupart des solutions de communications sans fil.

Les réseaux de capteurs sans fil multimédia (WMSNs) connaissent actuellement un essor spectaculaire, tant dans le domaine académique qu'industriels. Parallèlement à l'aspect de compression des données et conservation d'énergie au niveau de WMSNs, la sécurisation de la couche physique dans ces réseaux ouvre une voie innovante en direction de la cryptographie à une faible complexité. Toutefois, en raison de limitations en puissances, parmi les solutions envisagées pour cette nouvelle couche physique sécurisée on trouve l'utilisation des cartes chaotiques.

L'objectif de ce travail est d'appliquer des cartes chaotiques pour crypter /décrypter les composantes I-Q des symboles complexes dans le modulateur /démodulateur OFDM. Afin de valider cette technique, l'étude est élargie à la transmission des images médicales sur la nouvelle couche physique. Différentes métriques ont été utilisés pour quantifier les performances de la sécurité de transmission.

Mots clés : Réseaux de Capteurs sans Fil Multimédia (WMSNs), Cryptographie chaotique, Cryptographie des Images.

Abstract

The enthusiasm of the general public for communicating objects and evolution of sensor networks has led to the need to transfer securely amounts of multimedia information. On the other hand, the OFDM modulation format has become a standard in the physical layer of most wireless communications solutions.

Wireless Multimedia Sensor Networks (WMSNs) are experiencing a dramatic expansion, both in the academic world industrial. In addition to the aspect of data compression and energy conservation at WMSNs, securing the physical layer in these networks opens an innovative path towards cryptography at low complexity. However, due to power limitations, the solutions considered for this new secure physical layer include the use of chaotic maps.

The goal of this work is to apply chaotic maps to encrypt / decrypt the I-Q components of complex symbols in the OFDM modulator / demodulator. In order to validate this technique, the study is extended to the transmission of medical images on the new physical layer. Different metrics have been used to quantify the performance of the transmission security.

Keywords : Multimedia Wireless Sensor Networks (WMSNs), Chaotic Cryptography, Image Cryptography.

ملخص

حاجة الجمهور العام لتوصيل الأشياء أدت الى تطوير شبكات الاستشعار وحاجته إلى نقل معلومات و وسائط مختلفة بشكل آمن من ناحية أخرى، أصبح تنسيق التشكيل OFDM معيارًا في الطبقة المادية لمعظم الحلول الاتصالات اللاسلكية.

تعرف شبكات الاستشعار اللاسلكية متعددة الوسائط (WMSNs) حاليا ارتفاع مذهل ، سواء في المجالات الأكاديمية والصناعية. بالإضافة إلى جانب ضغط البيانات والحفاظ على الطاقة في شبكات WMSN ، فإن تأمين الطبقة المادية في هذه الشبكات يفتح طريقًا مبتكرًا نحو التشفير في ظل تعقيد منخفض .ومع ذلك ، نظرًا لقيود الطاقة ، تشمل الحلول التي تم أخذها في الاعتبار هذه الطبقة المادية الآمنة الجديدة استخدام البطاقات الفوضوية.

الهدف من هذا العمل هو تطبيق خرائط فوضوية لتشفير / فك تشفير مكونات I-Q للرموز المعقدة في المغير / أداة إزالة التشكيل .OFDM من أجل التحقق من صحة هذه التقنية ، تم تمديد الدراسة لنقل الصور الطبية على الطبقة المادية الجديدة .تم استخدام مقاييس مختلفة لقياس أداء أمان الإرسال.

كلمات البحث :شبكات الاستشعار اللاسلكية متعددة الوسائط (WMSNs) ، تشفير الفوضى ، تشفير الصور **كلمات البحث:**.

Table des Matières

Liste des Figures

Liste des Tableaux

Liste des Acronymes

OFDM :	1st Generation
WSN :	2nd Generation
3G :	3rd Generation
4G :	4th Generation
3GPP :	3rd Generation Partnership Project
ACE	Active Constellation Extension
AMPS :	Advanced Mobile Phone System
CEPT :	Conférence Européenne des Postes et Télécommunications
CP :	Cyclic Prefix
CDMA :	Division Multiple Access
DFT :	Discrete Fourier Transform
DFTS :	Direct Fourier Transform Spread
DCS:	Digital Communication System
EDGE :	Enhanced Data rates for GSM Evolution
EPC :	Evolved Packet Core
ETSI :	European Telecommunications Standard Institute
FDMA :	Frequency Division Multiplexing Access
GSM :	Global System for Mobile Communication
GPRS :	General Packet Radio Services
HSPA :	High Speed Packet Access
HSPA+ :	High Speed Packet Access+
I-FDMA :	Interleaved frequency division multiple access
IDFT :	Inverse Discrete Fourier Transform
LTE :	Long Term Evolution
L-FDMA:	Localized Frequency Division Multiple Access
NMT:	Nordic Mobile Telephone
OFDMA:	Orthogonal Frequency Division Multiple Access
PAPR :	Peak-to-Average Power Ratio
PCS :	Personal Communications Services
PTS :	Partial Transmit Sequences
RNC :	Radio Network Controller
RC :	Root Cosine
RRC :	Raised Root Cosine
SNR :	Signal Noise Ratio
SLM :	Selected Mapping
TACS :	Total Access Communication System
TI :	Tone Injection
TR :	Tone Reservation
UMTS :	Universal Mobile Telecommunications System

Introduction Général

Les facilités de déploiement des capteurs sans fil et la baisse de leur coût ont permis de généraliser l'utilisation de réseaux de capteurs sans fil. Aujourd'hui on retrouve ce type de réseau aussi bien dans la surveillance industrielle, que dans la mesure de données environnementales, la domotique, la détection d'incendie, le milieu médical ou bien encore dans le domaine militaire.

La plupart de ces applications ont pour mission de surveiller une zone et d'obtenir une réaction quand elles détectent une donnée critique. La divulgation de ces données critiques peut ne pas avoir une grande incidence dans des domaines tels que la domotique ou bien la capture d'événement environnemental. Sa confidentialité peut par contre être indispensable dans d'autres applications, comme pour le secret médical d'un patient à l'hôpital ou pour la sécurité du territoire dans le domaine militaire.

Les solutions utilisées dans les réseaux ad hoc classiques, ne peuvent pas s'appliquer stricto sensu aux réseaux de capteurs sans fil, car ces dispositifs sont limités par leur batterie et leur puissance de calcul. Il est donc nécessaire de développer un outil de protection efficace des données transférées contre les intrusions arbitraires. Le cryptage des données est très souvent le seul moyen efficace pour répondre à ces exigences.

Dans ce projet, nous étudions principalement la stratégie de sécurisation de la couche physique pour les réseaux de capteur sans fils basé sur le chaos. Notre objectif est d'améliorer la sécurité des données transmises tout en sécurisé la technique de transmission OFDM. La plupart des travaux rapportés dans la littérature concentrent leur attention sur l'amélioration de la sécurité au niveau des couches supérieur. Comme la sécurité est la fonction des couches supérieures, la couche PHY est également vulnérable à de telles attaques par déni de service. Un adversaire détecte des trames transmises pour perturber le réseau et / ou bloquer le trafic transitant par le réseau. Il est approprié d'introduire la sécurité PHY afin de rendre le réseau robuste contre de telles attaques. Pour parvenir à une transmission

sécurisée dans une communication sans fil, diverses approches sont suggérées dans la littérature.

La méthode de cryptage basée sur le chaos est considérée comme un bon candidat pour assurer une sécurité fiable de la couche physique. Nous allons s'intéresse à la sécurisation des données images, qui sont considérées comme des données particulières en raison de leurs tailles et de leurs informations qui sont de natures bidimensionnelles et redondantes. Ces particularités des données rendent les algorithmes développés dans la littérature inutilisables sous leurs formes classiques, à cause des contraintes de la vitesse et de la perte de l'information qui peuvent être causées par un cryptosystème classique. Les méthodes de cryptage basées sur le chaos sont l'une des méthodes qui combinent à la fois rapidité et haute sécurité. En utilisons une séquence de brouillage chaotique pour améliorer la sécurité de la transmission d'image.

Ce mémoire est organisé comme suit :

Les deux premiers chapitres regroupent des généralités sur réseaux de capteur sans fils et la technique OFDM on citant les grandes caractéristiques de chacun. Le troisième chapitre est consacré à la cryptologie. Nous présentons les différents algorithmes de chiffrement classique et moderne, on rappelant quelque algorithme dédié au cryptage d'image. Le quatrième chapitre donne une description générale sur les systèmes dynamiques et chaotiques ainsi que leurs utilisations à des fins de chiffrement sont évoqués. Le cinquième chapitre est consacré à la simulation et l'analyse des résultats.

Chapitre I

État de l'Art sur les Réseaux de Capteurs

Chapitre I

État de l'Art sur les Réseaux de Capteurs

I.1 Introduction :

Depuis longtemps, l'être humain cherche à concrétiser son confort, son bienêtre, sa santé, sa sécurité, et l'innovation dans sa vie. Il a trouvé dans les capteurs une pierre pour construire ce chemin. De nos jours, les capteurs sont partout : dans les rues, dans les maisons, dans les bureaux, dans la voiture, aux frontières d'un pays, sous l'eau, dans les barrages et dans les forêts **[I.1]**.

Un capteur est un dispositif qui permet de détecter et mesurer des quantités physiques tel que la température la pression des quantités lumineuse… et les convertissent vers des signaux électriques traitables par des équipements électroniques. Les capteurs sans fils sont utilisés fréquemment pour relever des informations dans des environnements hostiles auxquels l'homme n'a pas toujours accès. C'est pourquoi on considère qu'une fois qu'ils sont déployés, les capteurs sont autonomes. Leur durée de vie est donc la durée de vie de leur batterie.

I.2 Généralité sur les Réseaux de Capteurs

Un réseau de capteurs sans fil (WSN) est un système distribué de grande échelle mettant en communication un grand nombre d'entités autonomes communément appelées « capteurs sans fil », autant simplement « capteurs ». Ces capteurs forment donc les nœuds du réseau. Dans un scénario d'application classique, plusieurs nœuds capteurs sont déployés dans un certain environnement pour mesurer certains phénomènes physiques et faire remonter les informations collectées à une station de base, nommée le nœud puits (une porte

d'entrée vers le monde extérieur qui fait l'interface entre le réseau de capteurs et l'utilisateur des données). Dans le cas le plus simple, les capteurs seront dans le voisinage direct du puits (un réseau de type étoile à un saut). Cependant, dans le cas d'un réseau à grande échelle, les capteurs ne sont pas tous dans le voisinage du puits et les messages seront acheminés du nœud source vers le puits en transitant par plusieurs nœuds, selon un mode de communication multi-sauts. **[I.2]**

- **Applications militaires** : La surveillance de territoire ou de frontière à des fins militaires a été la première application des réseaux de capteurs. Dans le même objectif militaire, des nœuds capteurs peuvent être dispersés sur un terrain adverse afin de l'analyser avant d'y envoyer des troupes.
- **Applications environnementales** : Les réseaux de capteurs peuvent être utilisés pour surveiller les changements environnementaux accidentels ou naturels**.**
- **Applications médicales :** Les capteurs peuvent être implantés dans ou sur le corps pour surveiller un patient et son état de santé.
- **Application en génie civil :** Les capteurs peuvent être utilisés pour contrôler les vibrations susceptibles d'endommager la structure d'un bâtiment, d'un pont ou d'un barrage.
- **Application en domotique :** Les réseaux de capteurs peuvent être utilisés pour détecter les intrusions, capter la température, et toute information utile pour assurer confort et sécurité dans une maison.
- **Application en agriculture :** les capteurs mesurent l'humidité du sol ou d'autres paramètres sur la culture afin d'irriguer ou traiter avec précision les seuls endroits nécessaires.
- **Autres applications :** En industrie, les capteurs peuvent remplacer RFID pour contrôler les stocks de produit, contrôler les flux, surveiller des équipements ; en urbanisme, les capteurs peuvent détecter les déplacements, compter les véhicules, détecter les matières dangereuses dans le circuit d'alimentation en eau, …etc.

I.3 Architecture d'un Capteur sans fils :

Un nœud capteur contient quatre unités de base : l'unité de captage, l'unité de traitement, l'unité de transmission, et l'unité de contrôle d'énergie. Il existe également d'autres modules supplémentaires, suivant son domaine d'application, tels qu'un système de localisation (GPS), ou bien un système générateur d'énergie (cellule solaire). On peut même trouver des micro-capteurs, un peu plus volumineux, dotés d'un système mobilisateur chargé de déplacer le micro-capteur en cas de nécessité **[I.3]**. On peut voir sur la Figure I.1 les différents composants qui constituent un capteur.

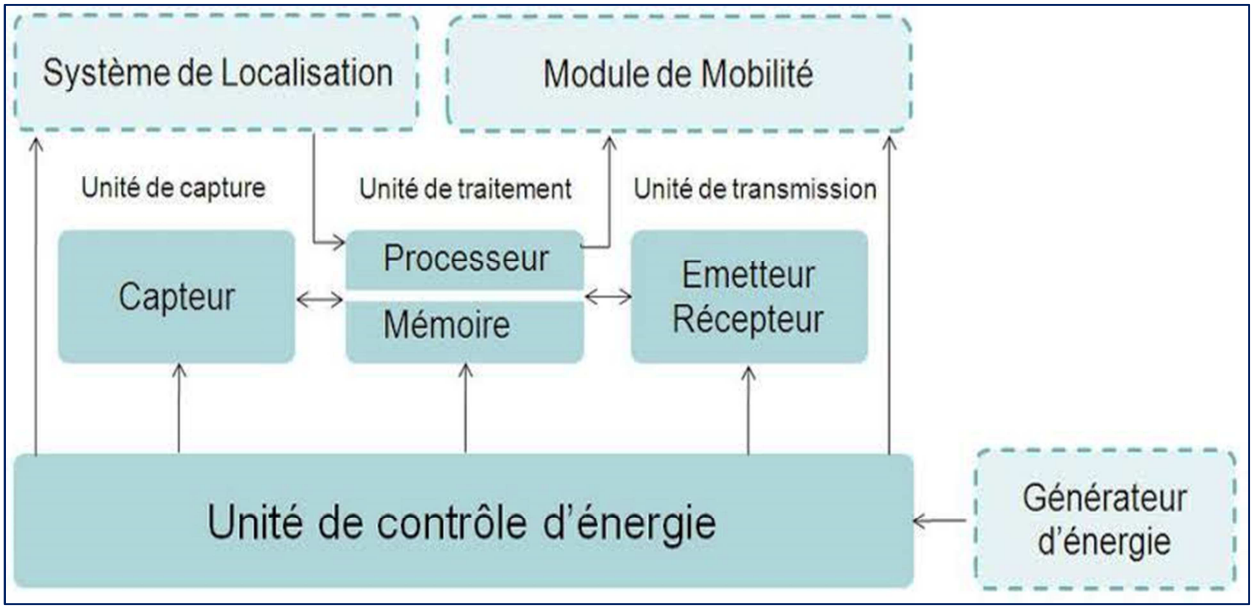

Figure I.1 : Architecture d'un Capteur sans Fils.

Pour être plus précis chaque groupe de composants possède son propre rôle :

- **Unité de Traitement**

  Chaque nœud du réseau est équipé d'un microcontrôleur à faible consommation. Il peut atteindre une fréquence de 104 MHz (pour les nœuds capteurs multimédia). Les modes de fonctionnement dépendent du type du microcontrôleur. Deux éléments principaux peuvent influencer sur le volume de données traitées par cette unité qui sont : la taille de la donnée captée (par le nœud lui-même) et les données reçues de ces voisins dans le réseau **[I.4]**.

- **Unité de Transmission**

  Cette unité de transmission est responsable d'effectuer toutes les émissions et réceptions des données sur un medium sans fil, elle est la plus consommatrice en termes d'énergie et possède quatre modes de fonctionnement : émission « Tx », réception « Rx », repos « *idle* » et mode sommeil « *Sleep* ». La portée de communication dépend de la technologie sans fil (entre 10 et 100 m) **[I.3]**. **[I.4]**

- **Unités de Captage**

  Il existe différents types de capteurs génériques comme les capteurs de température, d'humidité, de présence (localisation), etc. Le capteur est généralement composé de deux sous-unités : le récepteur (reconnaissant l'analyste) et le transducteur (convertissant le signal du récepteur en signal électrique). Le capteur est responsable de fournir des signaux analogiques, basés sur le phénomène observé, au convertisseur Analogique/Numérique. Ce dernier transforme ces signaux en un signal numérique compréhensible par l'unité de traitement.

- **Unités de Control d'Énergie**

  Les nœuds d'un réseau de capteurs sont généralement inaccessibles, de ce fait, la durée de vie du réseau dépend complètement de celle de la source d'énergie du nœud capteur **[I.5]**. Celle-ci est influencée considérablement par la contrainte de taille des nœuds. Afin d'étendre la durée de vie totale du réseau, il est possible d'utiliser des systèmes de rechargement d'énergie basés sur l'extraction de cette énergie à partir de l'environnement observé. Les cellules solaires sont un exemple typique de ces systèmes.

I.4 Réseaux de Capteurs sans fil

Les réseaux de capteurs sans fil sont des réseaux ad-hoc spécifiques avec un nombre de nœuds plus conséquents, une énergie limitée et une puissance de calcul plus faible que les réseaux ad-hoc classiques. Ce sont ces particularités que nous introduisons dans la partie suivante. [I.6]

- **Topologie :**

  La topologie que l'on retrouve classiquement au sein des réseaux de capteurs sans fil est un ensemble de nœuds qui sont déposés de manière hétérogène sur une zone ou des objets. Tous ces nœuds communiquent entre eux. Les réseaux de capteurs sans fil sont le plus souvent reliés à une ou plusieurs bases pour récupérer les informations circulant sur le réseau, et de les stocker ou bien de les envoyer directement via une liaison internet, GSM…etc. Ces bases peuvent être par exemple un ordinateur portable ou un capteur de puissance plus importante que les autres nœuds classiques.

- **Routage :**

  Le routage consiste à découvrir un chemin entre les deux nœuds donnés, afin de ne mobiliser que les nœuds intermédiaires réellement nécessaires à l'acheminement des messages. Ces derniers sont ensuite transportés grâce à des communications le long d'un chemin sélectionné. Pour limiter le nombre de communications coûteuses en énergie, les réseaux de capteurs sans fil utilisent des protocoles de routage efficaces.

- **La Tolérance aux Fautes**

  Dans les réseaux de capteurs sans fil, un ou plusieurs capteurs peuvent ne pas fonctionner correctement. En effet les capteurs sont des entités sensibles aux altérations d'états comme des phénomènes climatiques (humidité, chaleur, électromagnétisme) ou du fait d'une batterie faible. Dans ce cas de figure, le réseau doit être capable de détecter ce type d'erreur est d'y remédier, en cherchant par exemple à modifier ses tables de routage pour trouver un autre chemin permettant de transmettre l'information et de maintenir le réseau toujours opérationnel.

- **Mise à l'Échelle**

  Le nombre de capteurs utilisés dans les réseaux de capteurs sans fil peut varier de quelques entités à plusieurs dizaines de milliers. C'est d'ailleurs la principale utilité des réseaux de capteurs qui doivent pouvoir s'auto organiser à une grande échelle et être efficace quel que soit le nombre.

- **Une Énergie Limitée**

  Les capteurs sont équipés de batteries avec une énergie limitée. De plus, les réseaux de capteurs sans fil sont souvent déployés dans des zones difficiles d'accès pour l'homme. Il est donc difficile de pouvoir changer les batteries des capteurs. Si le nombre des capteurs dépasse la centaine d'entités. La consommation de l'énergie des réseaux de capteurs sans fil doit être la plus préservée possible.

- **Faible Puissance de Calcul**

  La faible puissance des capteurs ne permet pas d'utiliser des algorithmes complexes dans les réseaux de capteurs sans fil, et particulièrement dans la compression et la cryptographie. La faiblesse de la puissance de calcul est aussi préjudiciable pour le temps de réponse du réseau. Si l'on demande à un capteur d'effectuer de nombreux calculs, sa réactivité va sensiblement se détériorer.

I.5 Architecture d'un Réseau de Capteurs

Le réseau de capteurs sans fil est généralement caractérisé par un déploiement dense avec des centaines voire des milliers de nœuds. Lorsque deux entités ou nœuds d'un réseau veulent communiquer ensemble, deux situations sont possibles : soit ils sont voisins et peuvent directement échanger des messages, soit ils sont trop éloignés l'un de l'autre, auquel cas les messages doivent être retransmis de proche en proche. Les nœuds sont généralement dispersés sur un champ de surveillance d'une manière arbitraire (Figure I.2), chacun de ces nœuds a la capacité de collecter les données, les router vers le nœud puits (sink), et par la suite vers l'utilisateur finale via une communication multi-sauts. Le nœud puits peut communiquer avec le nœud coordinateur de tâches (utilisateur) par Internet ou par satellite.

L'architecture du réseau est présentée dans la **Figure I.2**. Le WSN est caractérisé par sa capacité d'auto organisation, de coopération, de rapidité de déploiement, et de faible coût. **[I.4] [I.5]**

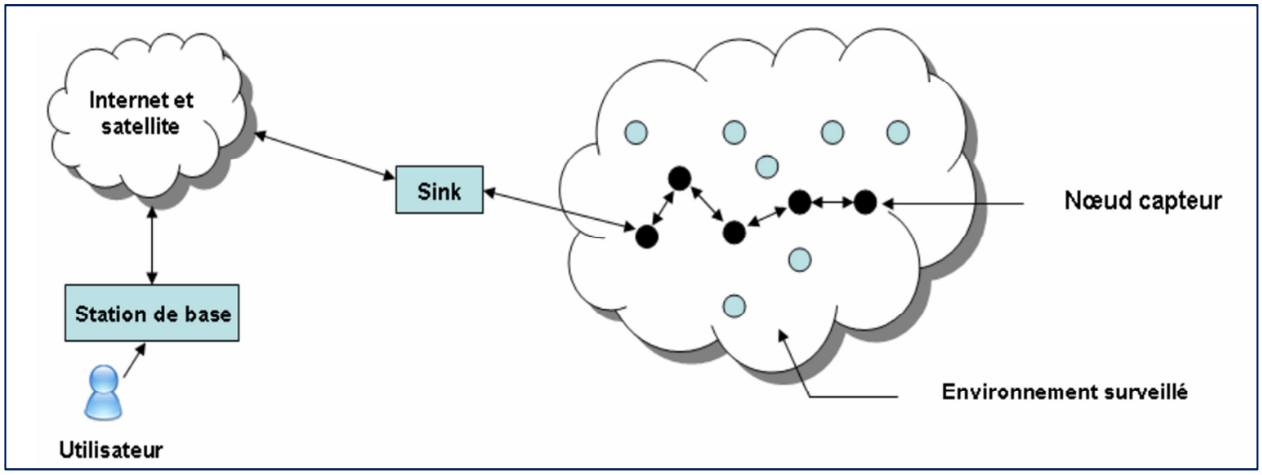

Figure I.2 : Architecture d'un Réseau de Capteurs sans Fils.

Chaque nœud ainsi que tous les autres capteurs du réseau utilisent une pile protocolaire illustré par la Figure I.3. Cette pile prend en charge le problème de consommation d'énergie, intègre le traitement des données transmises dans les protocoles de routage, et facilite le travail coopératif entre les capteurs. Elle est composée de la couche application, transport, réseau, liaison de données, physique, ainsi que de trois niveaux qui sont : le niveau de gestion d'énergie, de gestion de tâches et le niveau de gestion de mobilité **[I.5]**.

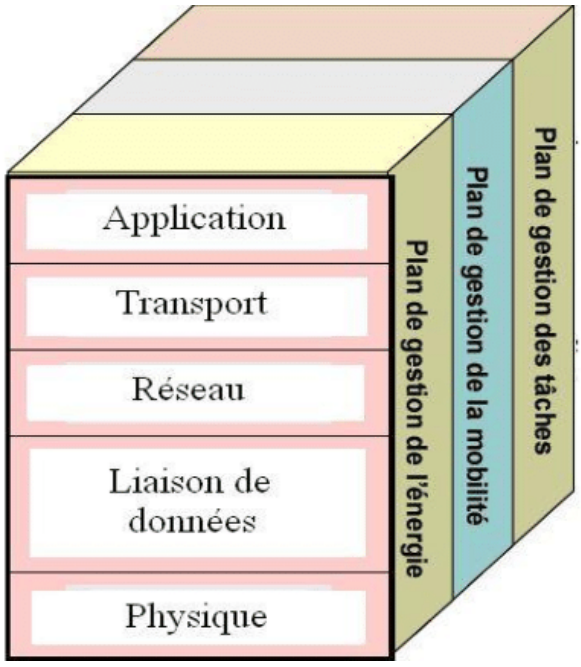

Figure I.3 : Pile Protocolaire dans les Réseaux de Capteurs **[I.7]**.

Suivant la fonctionnalité des capteurs, différentes applications peuvent être utilisées et bâties sur la couche application. La couche transport, quant à elle, sert à maintenir le flux de données en cas de nécessité dans les applications utilisées, particulièrement lors d'une connexion avec Internet, tandis que la couche réseau s'occupe du routage des données fournies par la couche transport. Comme l'environnement des réseaux de capteurs est bruyant et les nœuds peuvent être mobiles, la couche MAC doit garantir une faible consommation d'énergie et un taux de collision minimum entre les données diffusées par les nœuds voisins **[I.5]**. Enfin, la couche physique doit assurer des techniques d'émission, réception et modulation de données simples mais robustes.

- **Niveau de Gestion d'Énergie**

  Les fonctions intégrées à ce niveau consistent à gérer l'énergie consommée par les capteurs, dès lors, un capteur peut par exemple éteindre son interface de réception dès qu'il reçoit un message d'un nœud voisin afin d'éviter la réception des messages dupliqués. De plus, quand un nœud possède un niveau d'énergie faible, il peut diffuser un message aux autres capteurs pour ne pas participer aux tâches de routage, et conserver l'énergie restante aux fonctionnalités de captage.

- **Niveau de Gestion de Mobilité**

  Ce niveau détecte et enregistre tous les mouvements des nœuds capteurs, d'une manière à leur permettre de garder continuellement une route vers l'utilisateur final, et maintenir une image récente sur les nœuds voisins, cette image est nécessaire pour pouvoir équilibrer l'exécution des tâches et la consommation d'énergie.

- **Niveau de Gestion des Tâches**

  Lors d'une opération de captage dans une région donnée, les nœuds composant le réseau ne doivent pas obligatoirement travailler avec le même rythme, cela dépend essentiellement de la nature du capteur, son niveau d'énergie et la région dans laquelle il a été déployé. Pour cela, le niveau de gestion des tâches assure l'équilibrage et la distribution des tâches sur les différents nœuds du réseau.

I.6. Réseaux de Capteurs d'Images

Si le paradigme des réseaux de capteurs sans fil a été défini il y a déjà une vingtaine d'années, l'engouement pour les réseaux de capteurs d'images est plus récent. Le développement des micros caméras et microphones a observé une forte évolution au cours des dernières années, avec les évolutions des téléphones mobiles. Ces dispositifs deviennent de plus en plus petits et bon marché, et fournissent de plus en plus de performances en termes de rapidité et de qualité du signal.

Comparés aux réseaux de capteurs classiques qui manipulent des données scalaires (mesure de température, d'humidité, etc.), les réseaux de capteurs d'images ont quelques différences très importantes. Ces différences sont dues évidemment à la complexité et la nature du signal capturé **[I.8] [I.9]**.

- **Capture du Signal :** La complexité du matériel est multipliée par rapport aux captures de phénomènes simples. En effet, un capteur de caméra CMOS est normalement composé de nombreux capteurs photo-sensibles que capturent les différentes intensités pour chaque pixel. Tandis que pour la capture d'un signal de lumière un seul photo-capteur est suffisant, pour capturer une image nous avons besoin de beaucoup plus (normalement un par pixel) [I.8]. Cette évidence entraîne avec elle un coût supplémentaire en énergie et en temps de capture.

- **Le Volume des Données :** d'information associé à une image est de plusieurs ordres de grandeurs supérieur à une information scalaire simple, et cela change tout. En effet, les données fournies par un capteur traditionnel sont codées généralement sur quelques bits (sur la carte d'acquisition MTS 400 de Crossbow par exemple, les valeurs de température et l'humidité sont fournies sur 14 bits par le convertisseur analogique/numérique, les valeurs de luminosité sur 12 bits). Par conséquent, elles peuvent être transportées sur un seul paquet et la compression des données n'a donc pas vraiment d'intérêt. Une image est au contraire représentée sur plusieurs milliers d'octets et donc son transport nécessite typiquement plus d'un paquet. La compression des données d'image

est une nécessité pour réduire le nombre de paquets à émettre, d'autant qu'en pratique, le nombre de paquets générés par une image est très grand car la contrainte énergétique propre aux réseaux de capteurs impose de construire de paquets de petite taille.

- **Besoins de Mémoire :** Comme nous l'avons dit, tandis que pour le codage d'un signal simple sollicite quelques bits d'information, le codage d'une image numérique conduit à l'emploi de plusieurs centaines ou milliers d'octets. En particulier, la quantité de mémoire nécessaire dépend principalement de deux facteurs clés : La résolution de l'image et le format noir et blanc ou en couleur.

- **Tolérance aux Pertes :** les images naturelles possèdent une certaine tolérance aux pertes de paquet puisqu'il y a des corrélations spatiales entre les pixels voisins. Cela veut dire que le protocole de communication n'a pas besoin de fournir un service de transport totalement fiable, et des économies d'énergie peuvent être trouvées à ce niveau. Précisons toutefois que la tolérance aux pertes de paquets diminue si l'image est compressée avant transmission puisque l'opération de compression vise à éliminer les corrélations spatiales entre les pixels. [I.9]

- **Le rayonnement des Capteurs :** la plupart des capteurs traditionnels ont un champ de perception omnidirectionnelle, c'est-à-dire que l'orientation du capteur n'a pas d'impact sur la valeur de la grandeur physique mesurée. Des nœuds très proches les uns des autres peuvent alors être considérés comme redondants puisque les mesures qu'ils fournissent sont les mêmes. Le champ de vision des caméras est par contre restreint en direction et donc l'hypothèse que des capteurs voisins sont implicitement redondants ne tient plus. La réduction de la consommation d'énergie par contrôle de la topologie (réduction de la topologie par mise en sommeil des nœuds redondants) est donc plus complexe à mettre en œuvre dans les réseaux de capteurs d'image.

I.7. Applications de Réseaux de Capteurs d'Images

Les réseaux de capteurs d'image concernent un vaste champ d'applications, en fait toutes celles qui touchent à la détection, la reconnaissance, la localisation et le dénombrement d'objets par la vision. Les applications militaires (détection d'intrusions, espionnage de l'ennemi) sont les premières concernées. Parmi ces nombreuses applications dans le domaine militaire on cite à titre d'exemple le projet déployé en 2003 par une équipe de l'Université de l'état d'Ohio sur la base MacDill de l'US air force à Tampa, Floride. Ce réseau permet de détecter et classifier trois types de cibles : des personnes non armées, des soldats et des véhicules. Il était constitué de 90 nœuds équipes d'un capteur magnétique (pour la détection des métaux), d'un radar Doppler et d'une caméra **[I.8]**.

Les réseaux de capteurs d'image sont aussi très utiles pour l'observation de la faune et de la flore en milieu naturel. Le projet PODS développé par l'université de Hawaii avait pour objectif d'identifier les raisons pour lesquelles certaines plantes menacées poussent dans certaines régions mais pas dans d'autres. Les capteurs d'images nommés PODS sont déployés dans le parc national des volcans d'Hawaii. PODS collecte la température chaque 10 minutes et les images sont collectées chaque heure et ensuite transmises à l'utilisateur final.

Le projet BearCam est un autre exemple d'application pour l'observation de la nature. Le but de ce projet était de surveiller les ours bruns à la sortie de leur sommeil hivernal. Le système aide les biologistes à collecter des données pour leurs études de l'effet de la présence de l'être humain sur le comportement des ours.

De même dans **[I.10]**, un réseau de capteurs pour surveiller la reproduction des oiseaux a été réalisé. Un système composé d'une vingtaine de capteurs d'image Cyclops a été déployé dans la réserve des Montagnes James San Jacinto (Californie).

Des capacités de vision sont aussi nécessaires dans les applications de surveillance d'objets mobiles pour les différencier par leur forme, leur couleur et faciliter leur repérage géographique.

I.8 Conclusion

On conclusion, les besoins d'applications pour les réseaux de capteurs sans fil deviennent de plus en plus nombreux. La demande aujourd'hui concerne notamment les applications militaire, environnementales, médicale ou domotique. Le réseau de capteurs sans fil est généralement caractérisé par sa faible consommation énergétique, faible puissance de calcul, une grande condensation des nœuds qui peuvent dialoguer entre eux via un protocole de routage bien précis.

Pendant les dernières années un nouveau type des capteurs a été développé, c'est le capteur d'image. Comparés aux réseaux de capteurs classiques on peut distinguer quelques différences entre les deux tels que la nature des données traité, le volume, l'architecture et le nombre des nœuds, la présence du mémoire…etc.

Chapitre II

La Couche Physique OFDM

Chapitre II

La Couche Physique OFDM

II.1 Introduction

La transmission multi porteuse OFDM (Orthogonal Frequency Division Multiplexing) est une technique de modulation numérique qui joue sur l'efficacité et la rentabilité de transmission dans un canal multi-trajets. L'OFDM transmit les données en utilisant un grand nombre de porteuses pour une bande étroite. L'espace de fréquence et de synchronisation de la porteuse est choisi de telle sorte que les porteuses sont orthogonales pour éviter les interférences. Cette technique est utilisée pour la première fois dans les systèmes d'audiovisuels, sous ses deux formes, radiodiffusion numérique DAB (Digital Audio Broadcasting) et la diffusion de vidéo numérique DVB (Digital Video Broadcasting). Cette modulation a été très sollicitée ses dernières années et elle a été proposée dans plusieurs normes de télécommunications, à titre d'exemple, citons les réseaux locaux (WLAN-Wireless Local Area Network) IEEE 802.11 et les réseaux métropolitains (WMAN - Wireless Metropolitan Area Network), IEEE 802. 16 et la liaison descendante en LTE (Long Term Evolution) **[II.1] [II.2]**.

Les premiers modèles d'OFDM ont été présentés par Chang en 1966 et Saltzberg en 1967. Cependant, l'OFDM a été développé dans les travaux de Chang et Gibby en 1968, Weinstein et Ebert en 1971, Peled et Ruiz en 1980, et Hirosaki en 1981. Ces derniers ont prouvé leurs capacités à créer le principe de modulation et démodulation du signal à l'aide d'une technique avancée en traitement numérique du signal, la FFT (Fast Fourier Transform). Entre autres, un certain intérêt a été suscité pour la combinaison de la technique de transmission d'OFDM et l'accès multiple par répartition des codes (CDMA) dans les systèmes de canaux multiples par Hara et Prasad en 1997**.** L'OFDM est un domaine de recherche pertinent, elle été adoptée

comme technique de modulation pour plusieurs standards de communications filaires et sans fil.

II.2. Principe de la Modulation Multi-Porteuses

Soit à transmettre des symboles avec une durée de symbole noté T_S , une largeur de bande occupée B. Typiquement B est de l'ordre de T_S^{-1}. Pour un canal de transmission avec un délai de propagation τm, la récupération d'un symbole transmis sans interférence entre symboles ISI (lnterSymbol interférence) est seulement possible si la condition $\tau m \ll T_S$ est satisfaite.**[II.3]**

Comme conséquence, le débit binaire possible $R_b = log_2 (M) T_S^{-1}$ pour une modulation monoporteuse est limité par le délai de propagation du canal. L'idée la plus simple d'une transmission multiporteuse, pour surmonter cette limitation, est de diviser le flux des données sur K flux avec un taux de données réduit et de transmettre ces flux de données sur des sous-porteuses adjacentes (Figure II.1). Pour un $K = 8$, cela peut être vu comme une transmission parallèle dans le domaine fréquentiel qui n'affecte pas la totalité de la bande passante nécessaire. Chaque sous-porteuse a une bande passanteB/K. On note aussi que le facteur K n'est pas choisi arbitrairement, car une longue durée de symbole peut aussi rendre la transmission sensible au temps d'incohérence du canal liée à la fréquence Doppler maximale $Dmax$ · Donc, la condition, $V_{max} T_S \ll 1$ doit être satisfaite.

Les deux conditions peuvent être valides simultanément, si le facteur de $k = V_{max} \tau m$ satisfait la condition $k \ll 1$. Pour un facteur k donné assez petit, on doit admettre qu'il existe une durée symbole et que les deux doivent satisfaire les exigences pour avoir les meilleures conditions pour le canal. On doit choisir après, cette durée symbole optimale correspondant au canal.

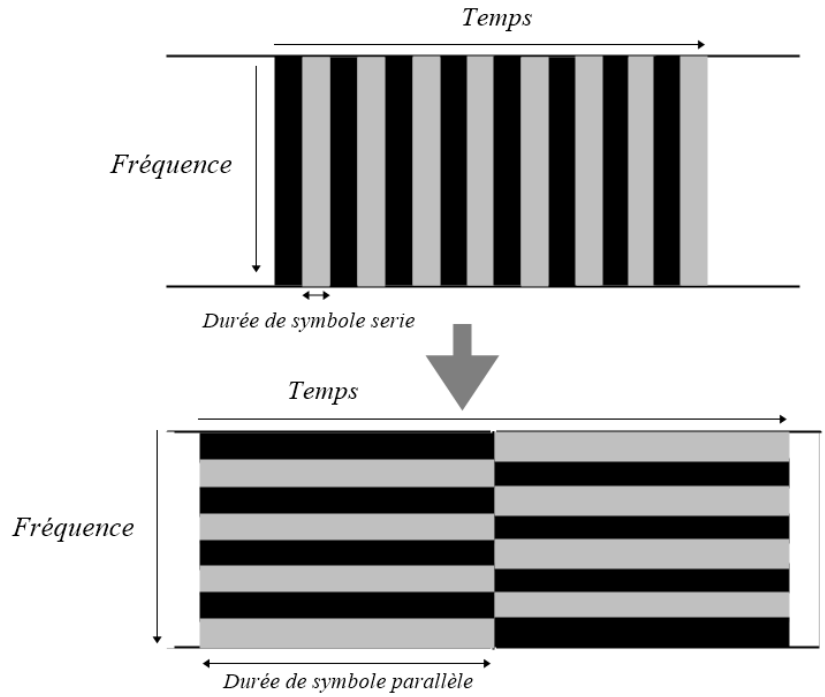

Figure II.1 Concept de Multi-porteurs

La Figure ci-dessous (Figure II.2) montre la classification des modulations multi-porteuses selon la décomposition de la bande uniforme ou non-uniforme.

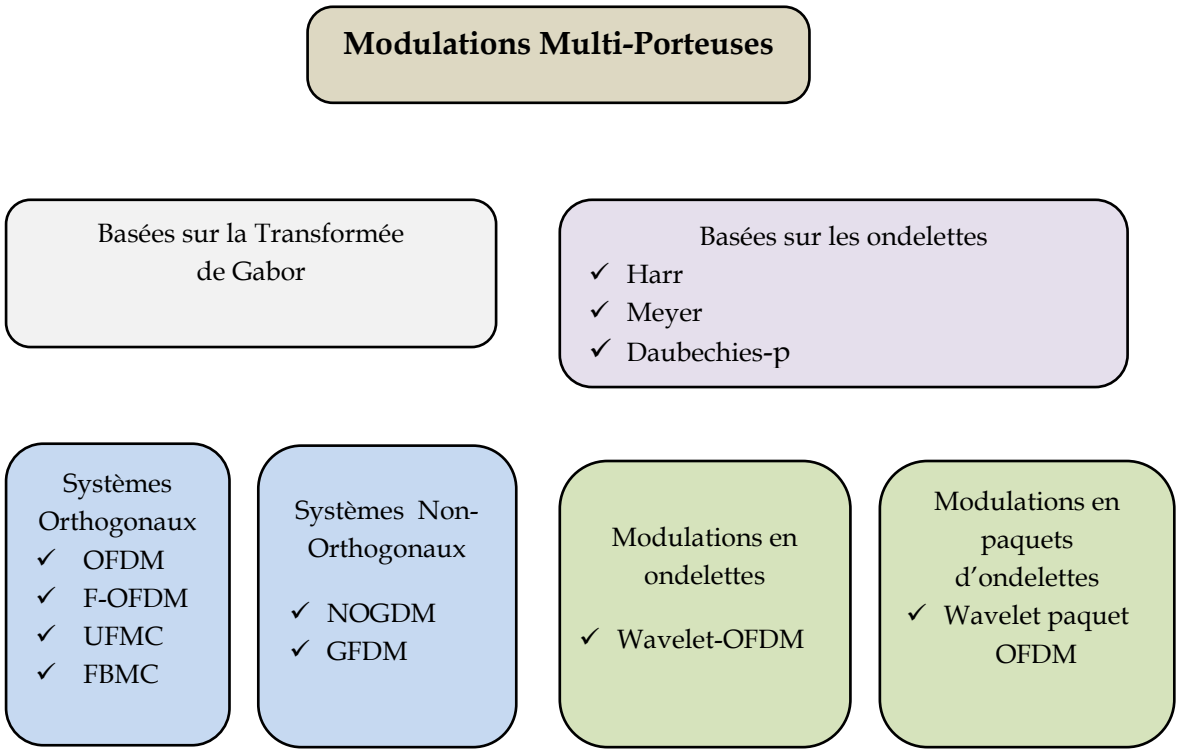

Figure II.2 : Classification des Modulations Multi-Porteuses

II.3. Notion d'Orthogonalité

Dans la Figure II.3 illustre des fonctions de forme rectangulaire espacées avec un intervalle de garde Δ sur un intervalle de temps t entre a et b. Ces fonctions sont linéairement indépendantes.

Il est évident que :

$$\int_a^b f(t)g(t)dt = 0 \qquad (II.1)$$

Et que

$$\int_a^b g(t)h(t)dt = 0 \qquad (II.2)$$

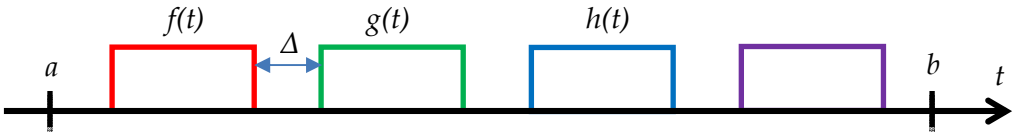

Figure II.3 : Base Orthogonale en Temps

Donc, ces fonctions forment une « *base orthogonale* » à *N*-dimension (autant que de fonctions sur le segment temporel {*a*,*b*}) dans un espace fonctionnel à *N*-dimensions, paramétré en temps sur un support {*a*,*b*}.

La transformée de Fourier (TF) de la fonction rectangulaire ou porte $\Pi_{TU}(t)$ d'amplitude A et de largeur T_U est un sinus cardinal donné par l'équation suivante :

$$TF\{A\Pi_{T_U}(t)\} = A\frac{\sin(\pi f T_U)}{\pi f} = AT_U Sinc(fT_U) \qquad (II.3)$$

Il est donc possible d'associer à une base orthogonale temporelle de fonctions porte $\Pi_{TU}(t)$, une base orthogonale fréquentielle de sinus cardinaux par transformation de Fourier de chaque porte. La Figure II.4 représente un exemple de base orthogonale en fréquence dérivée de la base orthogonale en temps décrite précédemment.

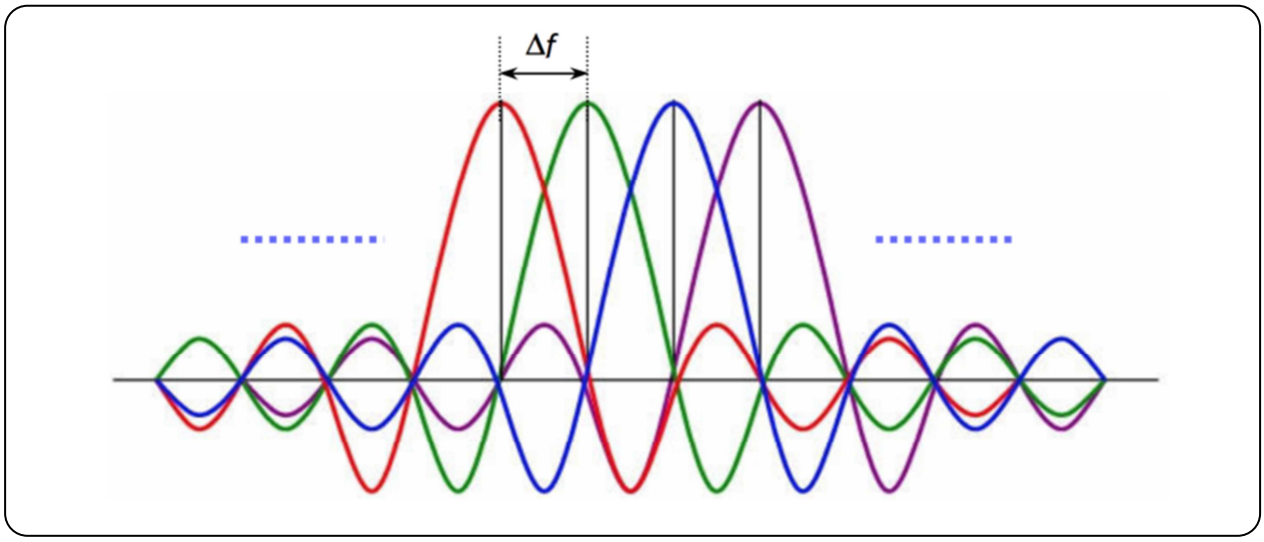

Figure II.4 : Base Orthogonale en Fréquence

L'espacement en fréquence entre les *N*-sinus cardinaux (sous-porteuses) de la base orthogonale fréquentielle est défini par :

$$\Delta F = \frac{1}{T_U} \qquad (II.4)$$

II.4. Principe de la modulation OFDM

Contrairement à la modulation mono-porteuse qui consiste à transmettre les données en série sur toute la bande de fréquence disponible, le principe de la modulation OFDM est de répartir les données numériques sur un nombre prédéfini de sous-porteuses ayant toutes la même largeur de bande et orthogonales entre-elles. Les données sont alors transmises en parallèle sur des sous-porteuses situées dans la bande utile. La condition d'orthogonalité permet d'éviter que les sous-porteuses se perturbent mutuellement à cause des interférences. Les données sont regroupées par symboles. Un symbole OFDM est une séquence de N symboles numériques répartis sur N sous-porteuses orthogonales. Soit $\{f_k\}$ l'ensemble des N sous-porteuses considérées pour la modulation OFDM tel que [II.4]:

$$f_k = f_0 + k\frac{1}{T_s}, \quad 0 \leq k \leq N-1 \qquad (II.5)$$

Où T_s représente la durée d'un symbole OFDM.

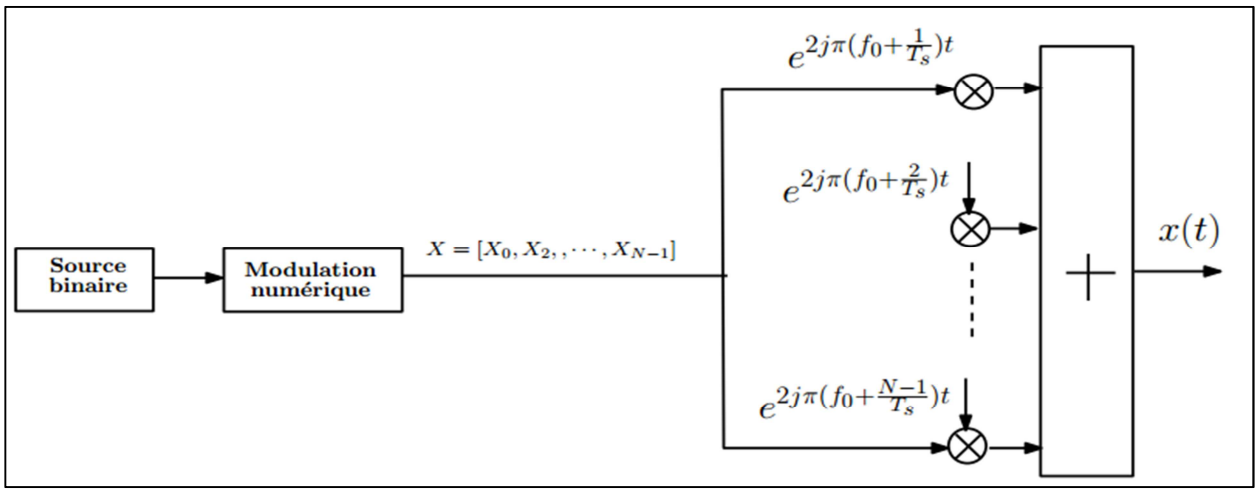

Figure II.5 : Principe de la Modulation OFDM

La Figure II.5 illustre le principe de la modulation OFDM. Sur cette figure, les données à transmettre sur les N sous-porteuses sont regroupées par séquence de N symboles avant d'effectuer la modulation OFDM. En effet, soit $X = [X_0, \cdots, X_k, \cdots, X_{N-1}]$ une séquence de N symboles complexes à transmettre. Chaque symbole X_k est un nombre complexe généralement obtenu à partir d'une modulation numérique par exemple de type QAM. Le $k^{ième}$ symbole X_k module la $k^{ième}$ sous-porteuse f_k. L'enveloppe complexe du signal $x(t)$, correspondant à l'ensemble des N symboles ré-assemblés, est la représentation temporelle du signal OFDM tel que :

$$x(t) = \sum_{k=0}^{N-1} X_k e^{2j\pi f_k t}, 0 \leq t < T_s \qquad \text{(II. 6)}$$

La Figure II.4 représente un exemple de spectre d'un symbole OFDM lorsque $N = 4$. Les fréquences sont orthogonales si l'espace entre deux fréquences consécutives est de $\Delta_f = 1/Ts$. Chaque sous-porteuse f_k est modulée par un symbole numérique (QAM) pendant une période correspondant à une fenêtre rectangulaire de durée T_s, de telle sorte que son spectre soit un sinus cardinal, fonction qui s'annule tous les multiples de Δ_f . Ainsi, lorsque l'échantillonnage de la $k^{ième}$ sous-porteuse est réalisé à la fréquence f_k, le maximum d'amplitude est obtenu sans interférence avec les autres sous-porteuses. Cette condition d'orthogonalité permet de garantir une occupation spectrale optimale et de simplifier les processus d'égalisation du canal radio.

II.5. Implémentation numérique de la modulation OFDM

Le signal $x(t)$ représenté à l'équation (II.6) est un signal continu dans le temps. L'implémentation numérique de la modulation OFDM consiste à discrétiser le signal *x(t)* afin d'effectuer les traitements numériques nécessaires. Dans l'intervalle de temps [*0; Ts],* on considère la période d'échantillonnage Te tel que $Ts = NTe$, ainsi, l'écart fréquentiel $\Delta_f = \frac{1}{\mathrm{NTe}}$ et $f_k = k\Delta_f = \frac{k}{\mathrm{NTe}}$. En discrétisant ce signal aux instants nTe et en le ramenant en bande de base, on obtient ses échantillons xn par la relation suivante :

$$x(n) = \sum_{k=0}^{N-1} X_k e^{2j\pi n\frac{k}{N}}, \qquad 0 \leq n < N \qquad (II.7)$$

Où $X_k$représente un symbole complexe issu de la modulation numérique et N représente le nombre de sous-porteuses.[II.5]

L'équation II.7 montre que les échantillons $\{x_\mathrm{n}\}$ sont obtenus par la Transformée de Fourier Inverse Discrète (TFID) des symboles $\{X_\mathrm{k}\}$. À noter que le symbole OFDM est périodique, de période fondamental N, c'est-à-dire que $x_{n+N} = x_n, \forall\, n \in [0,\cdots, N-1]$.

En choisissant le nombre de sous-porteuses N comme une puissance de 2, c'est-à-dire $N = 2^m$, on peut réaliser cette transformée de Fourier à l'aide de l'algorithme Inverse Fast Fourier Transform (IFFT). La Figure II.6 illustre l'architecture simplifiée d'un modulateur OFDM numérique.

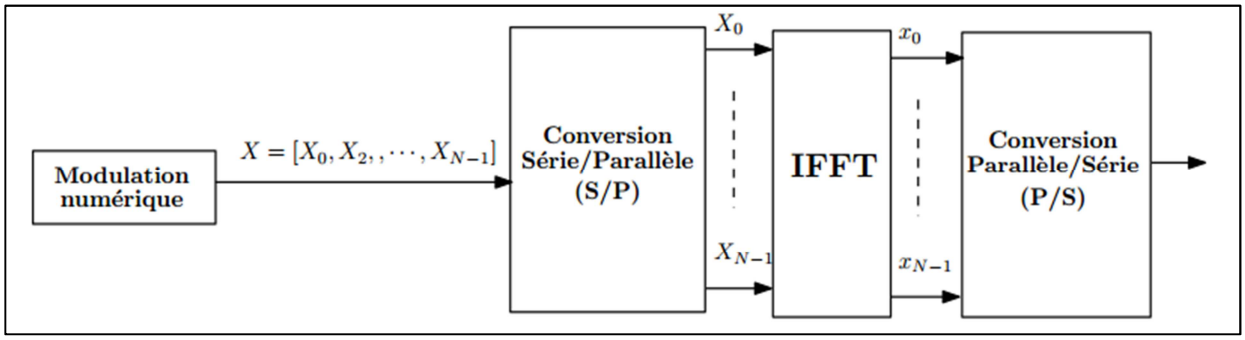

Figure II.6 : Architecture d'un Modulateur OFDM

En réception, la démodulation OFDM est réalisée à l'aide de l'algorithme FFT (Fast Fourier Transform). Les composantes fréquentielles du symbole démodulé $X = [X_0,\cdots, X_{N-1}]$ s'obtiennent par la relation suivante :

$$X_k = \frac{1}{N}\sum_{n=0}^{N-1} x_n e^{-2j\pi n\frac{k}{n}}, \quad 0 \leq k < N \qquad \text{(II. 8)}$$

Où x_n sont les échantillons du symbole OFDM initial et N représente le nombre de sous-porteuses

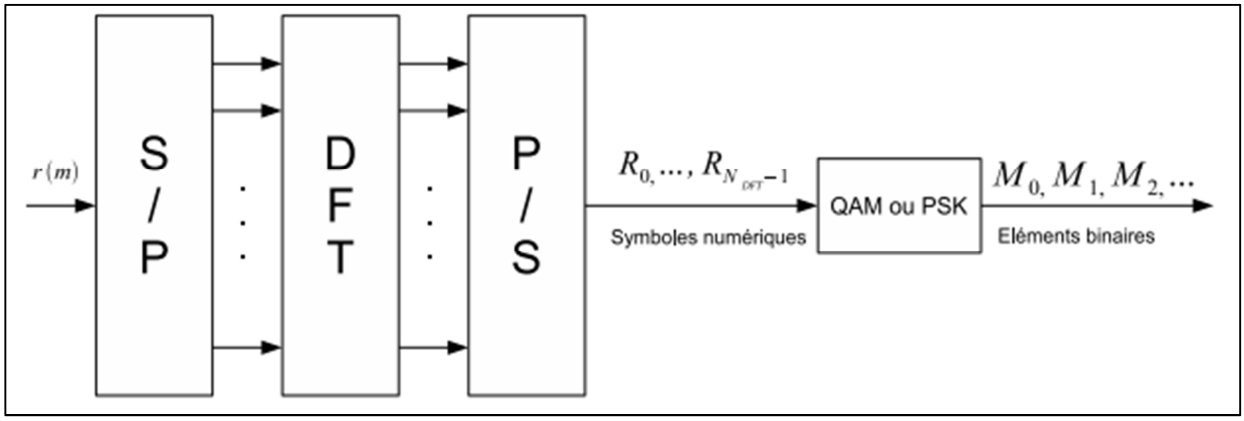

Figure II.7 : Principe de la Démodulation OFDM

II.6. Intervalle de garde :

Comme nous l'avons vu, les symboles subissent des échos et un symbole émis parvient au récepteur sous forme de plusieurs symboles atténués et retardés. Un symbole émis lors d'une période kT_S peut se superposer à un écho provenant du symbole émis à la période $(k-1)\,T_s$. Il se produit alors des interférences. Pour éliminer les interférences inter symboles (ISI), un intervalle de garde d'une durée Δ est rajouté pour chaque symbole OFDM. Chaque symbole est précédé par une extension périodique du signal lui-même. On choisit la durée de l'intervalle de garde de telle sorte qu'elle soit supérieure par rapport à une durée de retard maximal causé par les phénomènes de propagation à trajets multiples et qu'un symbole ne puisse pas interférer avec le prochain symbole, la durée du symbole totale transmis est alors $T = T_S + \Delta$. Pour que les interférences soient éliminées. [II.6]

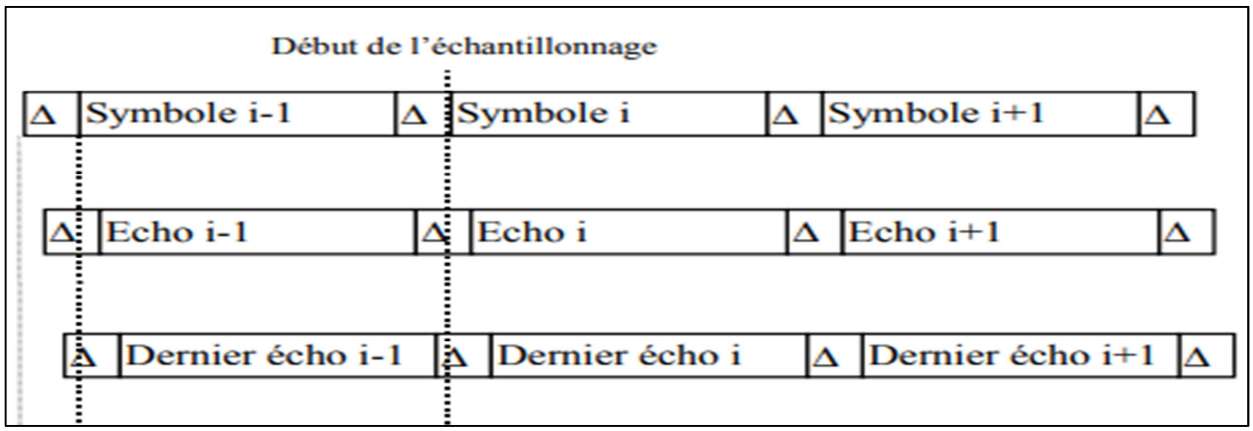

Figure II.8 : Principe de l'Intervalle de Garde

La Figure II.8 illustre l'insertion d'un intervalle de garde dans un symbole OFDM. Les échantillons ajoutés au début du symbole pour former un intervalle de garde est la copie exacte des derniers échantillons du symbole OFDM. L'avantage de cette recopie est que chaque signal, issu d'un trajet multiple, possédera toujours un nombre entier de sinusoïdes sur la durée d'une trame OFDM sans son préfixe. Si le préfixe inséré au début d'une trame OFDM est muet (sans aucun signal), des interférences entre sous canaux (ICI) vont se produire. Afin d'éviter ces interférences, le préfixe ne doit pas être muet, mais être la recopie des derniers symboles de la trame OFDM. Dans le domaine fréquentiel, la sommation des signaux de la sous-porteuse issus des divers trajets ne détruira pas l'orthogonalité des sous-porteuses, elle introduira seulement un léger déphasage. Les interférences ISI se produisent lorsque le retard relatif est plus long que l'intervalle de garde.

Malheureusement, l'insertion d'un intervalle de garde diminue le taux de symbole, mais si le nombre de sous-porteuses est assez grand, la durée de symbole TS devient assez importante par rapport à l'intervalle de garde. Par conséquent, le débit binaire sera réduit de peu. [II.7]

II.7. Le codage de canal

Lors de la phase de transmission sur le canal, les informations peuvent être perdues pour le récepteur. Dans de remédier à cela et d'améliorer la qualité de la transmission, il devient alors nécessaire d'utiliser un codage correcteur d'erreur. Dans un codage de canal, on introduit de la redondance dans le message à transmettre, suivant une loi

donnée. Cette redondance permet au récepteur de reconstituer sous certaines conditions les informations perdues lors de la transmission et cela grâce à la corrélation qui les lie aux informations correctement reçues. Ce procédé est appelé COFDM. Les codes utilisés pour effecteur l'opération de codage de canal se classent dans le cas général en deux catégories : les codes en blocs et les codes convolutifs. Pour le premier, on associe à chaque bloc de *Ne* d'information, le codeur *Ns* bits codés. Le codage d'un bloc est indépendant des précédents. Pour le second, à Ne bits d'information le codeur associe *Ns* bits codés, mais différemment du cas précédent, le codage d'un bloc de Ne bits dépend pas seulement du bloc présent mais également de tous les blocs précédents. Le rendement du code est défini par le rapport $R = (Ne/Ns) < 1$. Le codeur introduit donc de la redondance qui se traduit par une augmentation du débit d'un facteur $1/R$ entre l'entée et la sortie du codeur. [II.8]

II.8. Chaîne de transmission :

Le diagramme en bloc de la chaîne de transmission OFDM est représentée en figure II.9. [II.9]

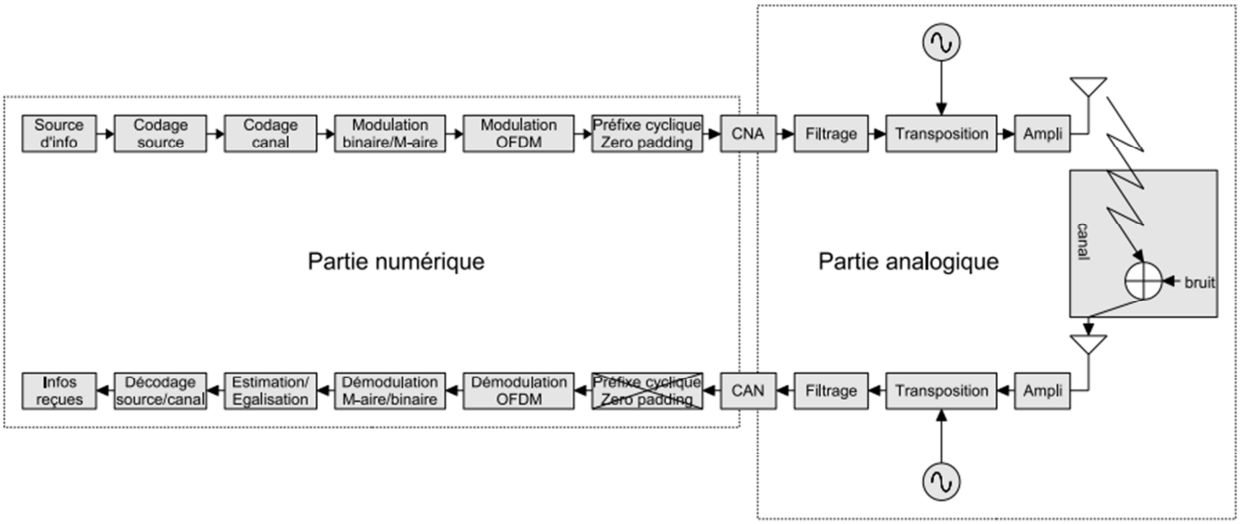

Figure II.9 : Diagramme en Bloc de la chaine de Transmission OFDM

- **Chaîne d'émission :**

Source d'information : Les éléments d'entrée de notre chaîne ce sont des données physiques spécifiques à émettre ou bien des données générées aléatoirement, avant de les transmettre sous forme binaire il faut tout d'abord les convertir en un signal électrique à l'aide d'un capteur sans fil.

Codage source : Le principe est simple, le codage consiste à utiliser des algorithmes pour compresser les données, afin de réduire la taille et le temps de propagation

Codage canal : ce codage consiste à ajouter une redondance pour protéger les bits d'information contre des éventuels parasites introduits par le canal, on utilise généralement des codes convolutif tels que code gray et le code viterbi

Modulation binaire/M-aire : Pour ce type de transmission les modulations QAM sont préférées et les plus utilisable par rapport à la modulation M-PSK car l'efficacité en puissance de la premier est plus grande que celle de la second.

Modulation OFDM : Modulation multiporteuses comprenant une conversion série/parallèle, une IFFT et une conversion parallèle/série.

Insertion du préfixe cyclique ou du zero padding (intervalle de garde) : pour éviter les interférences entre symboles on ajoute une redondance ou des zéros à chaque symbole OFDM.

Conversion numérique/analogique : le signal numérique est converti en un signal électrique analogique.

Filtrage : le but principal de ce filtrage est de supprimer les répétitions du spectre obtenues lors de la conversion numérique/analogique.

Transposition : la transposition en fréquence est effectuée pour porter le signal de la bande de base autour de la fréquence porteuse. Cette transposition est obtenue grâce à des mélangeurs et à un ou plusieurs oscillateurs locaux.

Amplificateur de puissance : pour assurer la détection du signal émis au niveau de récepteur il faut l'amplifier avant de le transmettre, pour qu'il puisse résister l'atténuation du canal.

Antenne d'émission : le signal électrique est transformé en une onde électromagnétique qui se propage dans espace libre.

Canal de propagation : le canal correspond à l'environnement physique dans lequel l'onde du signal se propage ; dans le cas des télécommunications mobiles, ce milieu est l'air. Il introduit plusieurs sortes de distorsions comme l'effet Doppler ou l'effet multitrajets. !!

- **Chaîne de réception :**

Antenne de réception : l'onde électromagnétique est transformée en un signal électrique. Mais l'antenne capte aussi du bruit thermique dont la puissance est proportionnelle à la bande passante de l'antenne.

Amplificateur faible bruit : le signal qui a subi l'atténuation du canal est amplifié.

Transposition : le spectre du signal qui est centré autour de la fréquence porteuse est ramené en bande de base. Cette transposition est obtenue grâce à des mélangeurs et à un ou plusieurs oscillateurs locaux.

Filtrage : le signal électrique bande de base est filtré afin d'éviter le repliement spectral lors de l'échantillonnage effectué par la conversion analogique/numérique.

Conversion analogique/numérique : le signal électrique analogique est converti en un signal numérique.

Démodulation OFDM : l'opération duale de la modulation est réalisée grâce à la FFT.

Estimation et Égalisation : la dispersion du canal est estimée grâce à des symboles connus du récepteur. Les symboles reçus affectés par le canal sont ensuite compensés.

Démodulation M-aire/binaire : les symboles reçus sont reconvertis en paquets de bits.

Décodage canal et décodage source : cette étape supprime les redondances ajoutées l'émission et corrige certaines erreurs. Les données sont ensuite décompressées en insérant les redondances enlevées lors du codage source à l'émission.

Informations : les données sont transformées de forme électrique en forme physique.

II.9. Avantages et inconvénients de l'OFDM :

Le procédé de modulation OFDM a été principalement conçu pour lutter contre le phénomène de multitrajets :

- Egalisation peu complexe : obtenue grâce à l'ajout d'un intervalle de garde qui permet de supprimer très simplement l'influence des multitrajets qui est un des problèmes majeurs des systèmes monoporteuses lorsque le débit de transmission augmente.
- L'utilisation de la bande de fréquence allouée est optimale par orthogonalisation des porteuses.
- Canal invariant localement : obtenu car la bande passante de chaque sous-porteuse est choisie petite devant la bande de cohérence du signal OFDM. On obtient donc un évanouissement fréquentiel lent du canal.
- Algorithme de la modulation simple et bien connu et peu complexe : la FFT (Fast Fourier Transform).
- Un bon codage et un bon entrelacement permettent une meilleure qualité de la transmission.

Néanmoins malgré ce grand nombre d'avantages, la modulation OFDM présente également quelques inconvénients :

- L'orthogonalité des sous-porteuses est l'élément clef de la modulation OFDM. Le bruit de phase ou le désaccord en fréquence entre les oscillateurs locaux de l'émetteur et du récepteur (appelé Offset fréquentiel) impliquent une perte d'orthogonalité entre sous porteuses et une forte dégradation des performances du système.
- Système très sensible au déséquilibre entre les voies I et Q. Fluctuation importante de l'enveloppe qui implique une dynamique élevée. Le déséquilibre

IQ entraîne des interférences mutuelles entre paires de sous porteuses symétriques et implique une forte dégradation des performances du système global. [II.10]

II.10. Domaines d'application de l'OFDM :

Grace à ses caractéristiques, L'OFDM offre des possibilités intéressantes de surpasser les capacités de système CDMA et de fournir la méthode d'accès sans fil pour les systèmes 4G. Le multiplexage en fréquence est bénéfique pour les transmissions dans des canaux sélectifs en fréquence qui comportent des trajets multiples. C'est pourquoi on trouve cette technique dans les normes de diffusion numérique du son dans des mobiles DAB, de télévision numérique terrestre DVB-T, de communications numériques hauts débits ADSL (Asynchronous Digital Subscriber Line) sur la boucle locale téléphonique et ses dérivés , ainsi que dans l'étude des normes de communications pour réseaux locaux à l'intérieur des bâtiments de type BRAN (Broadband Radio Access Network), qui est prévu pour des débits allant jusqu'à 54 Mbps. Grâce à sa fiabilité OFDM sera adoptée pour l'ATM sans fils… etc. [II.11]

- **DAB (Digital Audio Broadcasting)**

La DAB est la nouvelle norme numérique de radiodiffusion. La DAB a été normalisé en 1995 par l'institut européen de normes de télécommunications (ETSI) comme première norme employant la modulation OFDM.

La DAB est le seul système à offrir des débits de données élevés en restant facile à recevoir sur des appareils mobiles ou portatifs.

Paramétres	Mode de Transmission			
	I	II	III	IV
Largeur de bande	1,536 MHz	1,536 MHz	1,536 MHz	1,536 MHz
Modulation	DQPSK	DQPSK	DQPSK	DQPSK
Bande de fréquence (réception mobile)	≤375 MHz	≤1,5 GHz	≤3 GHz	≤1,5 GHz
Nombre de sous-canaux	1536	384	192	768
Durée de symbole	1000µs	250µs	125µs	500µs
Durée d'un intervalle de garde	246µs	62µs	31µs	123µs
Durée totale de symbole	1246µs	312µs	156µs	623µs
Distance maximale de transmission	96Km	24Km	12Km	48Km

Le tableau II.1 : montre les paramètres de transmission pour différents modes de DAB.

Le tableau II.1 montre les paramètres de transmission pour différents modes de DAB. En peut distinguer quatre modes de transmission, se change en fonction de quelque paramètres tels que La largeur de bande de transmission la vitesse de récepteur la tolérance aux trajets multiples exigée.

- **HiperLAN 2 et IEEE802.11 a :**

HiperLAN2 est une norme de réseau local fil représente la version deuxième de la norme **HiperLAN**. Elle est soutenue par l'H2GF (HiperLAN 2 Global Forum) fondé en 1999 par Bosch, Dell, Ericsson, Nokia, Telia et Texas Instrument. Au niveau physique, le standard HiperLan2 utilise la bande de fréquences comprise entre 5,15 et 5,25 Ghz, celle-ci est divisée en 9 porteuses de 200 Mhz de largeur chacune (un espacement de 20 Mhz étant prévu entre les porteuses) . Cette deuxième version propose un débit de pointe à 54 Mbps et utilise, au niveau physique, le protocole OFDM (Orthogonal Frequency Division Multiplexing).

IEEE802.11a (baptisée WiFi 5) permet d'obtenir débit de 54 Mbit/s (théoriquement) avec une portée de 10m, cette norme s'appuie sur un multiplexage de type OFDM. Elle spécifie 52 canaux de sous-porteuses radio dans la bande de fréquences des 5Ghz (bande U-NII ou Unlicensed – National Information Infrastructure) huit combinaisons, non superposées pour le canal principal. [II.12]

L'IEEE802.lla et l'HiperLan 2 ont un certain nombre de points communs : les débits annoncés sont les mêmes (25 Mb/s pratiquement), les fréquences utilisées sont aussi identiques. De plus, la couche physique de deux normes utilise l'OFDM (Orthogonal Frequency Division Multiplexing). Il subsiste toutefois des différences entre les 2 normes au niveau de la structure des données qui empêche la compatibilité. La différence la plus importante est la gestion de l'accès à l'A.P. En effet l'IEEE 802.1l.a à besoin de plus de temps pour établir la connexion au PC que l'HiperLan 2. [II.11]

Norme	**802,11a**	**HiperLAN 2**
Spectre	5,2 GHz	5,2 GHz
Type de modulation	OFDM	OFDM
Débit physique max	54 Mbps	54 Mbps
Débit binaire max , couche 3	32 Mbps	32 Mbps
Contrôle de l'accés au médium de transmission (MAC)		TDMA/TDD
Type de connexion	Non Orineté-conn	Orienté-connexion

Tableau I.2 : Sommaire de caractéristique d'IEEE802.11b, d'IEEE802.11a et de HIPERLAN2

La technique OFDM est une technologie fiable pour la transmission de données ultrarapide et donc, peut être utilisée pour des réseaux à fréquence unique avec des grands échos "actifs". De tels réseaux peuvent être vus comme un arrangement cellulaire d'émetteurs qui émettent le même signal sur la même fréquence très stable et soigneusement synchronisée et avec le même chronométrage de symbole.

II.11. Conclusion

Nous avons vu durant ce chapitre, une présentation général de la technique de transmission OFDM, est l'une des types de modulation multi-pouteuses les plus connue et utilisable dans le domaine de télécommunications, à cause de ses avantages tel que la suppression très simplement de l'influence des multitrajets qui est un des problèmes

majeurs des systèmes monoporteuses. Parmi ses application en trouve dans des mobiles DAB , de télévision numérique terrestre DVB-T, de communications numériques hauts débits ADSL…

Chapitre III

Généralité sur la Cryptographie

Chapitre III

Généralité sur la Cryptographie

III.1. Introduction

Dès que les hommes apprirent à communiquer, ils durent trouver des moyens d'assurer la confidentialité d'une partie de leurs communications. Ils ont fourni, à travers des époques successives, des efforts autant physiques qu'intellectuels pour pouvoir trouver une technique de communication efficace et appropriée.

En effet, les modes de télécommunications sont en évolution continue avec la recherche permanente de meilleurs débits, de facilité d'utilisation, de mobilité améliorée et surtout d'une confidentialité élevée. Il se pose donc un réel problème quant à la sécurité lors de la transmission de données. Pour des raisons éthiques, le transfert des données délicates ne peut se faire avec un tel risque et doit donc se protéger. La protection la plus adaptée pour ce type de communication réside dans la cryptographie. Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des données c'est-à-dire de les rendre inintelligibles sans une action spécifique. Cependant et malgré toutes ses évolutions et ses mises en œuvre, elle est toujours entravée par quelques défauts citant en particulier la taille des clés et la résistance contre les attaques avancées**.** L'objectif principal de ce chapitre est d'introduire à la cryptographie avec ses grandes branches, classiques et modernes utilisée dans la transmission et le stockage sécurisé de données.

III.2. Historique

Les origines de la cryptographie semblent remonter à plus de 4000 ans en Egypte. Plusieurs indications archéologiques tendent à montrer que les « écritures secrètes » sont en fait anciennes que l'invention de l'écriture elle-même. Polybius développa un système de codage des lettres de l'alphabet consistant à remplacer chaque lettre de l'alphabet par deux nombres, donnant la ligne et la colonne où se trouve cette lettre dans une matrice. Jules César utilisait une simple méthode de substitution de lettres pour communiquer secrètement avec ses généraux : c'est un chiffre par décalage, etc.
C'est cependant au cours de la seconde guerre mondiale que la cryptographie s'inscrit véritablement comme élément central des stratégies militaires. Le cas le plus connu est certainement l'histoire entourant le décodage du code Enigma par les Polonais et les Britanniques. Une conjonction d'espionnage classique et d'efforts de mathématiciens polonais permet de déduire la clé utilisée et ainsi de décoder les messages encodés avec Enigma. **[III.1]**
On trouve apparemment bien moins de détails sur les efforts cryptographiques durant la guerre froide, probablement parce que ces informations sont encore « Top Secret ».

On en est maintenant à l'époque moderne où le champ d'application de la cryptologie s'est élargi et a trouvé un regain d'actualité avec toutes les applications nouvelles suscitées par l'utilisation de l'Internet. La révolution d'Internet et l'utilisation de plus en plus d'informations massives sous forme numérique facilitent les communications et rendent de ce fait plus fragiles les informations que l'on détient, c'est pourquoi il devient nécessaire de protéger le contenu de certains messages des inévitables curieux. En effet, les réseaux ouverts créent des brèches de sécurité et il est plus aisé à un adversaire d'accéder aux informations. Dans une communication à distance, des questions cruciales se posent et leurs réponses s'imposent ; comment être sûr :

- que l'on parle à la bonne personne (authenticité),
- que nos propos ne sont pas altérés (intégrité),
- que la conversation n'est pas espionnée (confidentialité),

Alor la cryptographie n'est pas seulement l'action de chiffrement d'un message mais elle doit assurer les trois propriétés suivantes : confidentialité, intégrité, authenticité.

II.3. Vocabulaires de Base

Comme toute science, la cryptographie possède son propre langage. Dans ce qui suit les mots clés de domaine cryptographique **[III.1] [III.2] [III.3].**

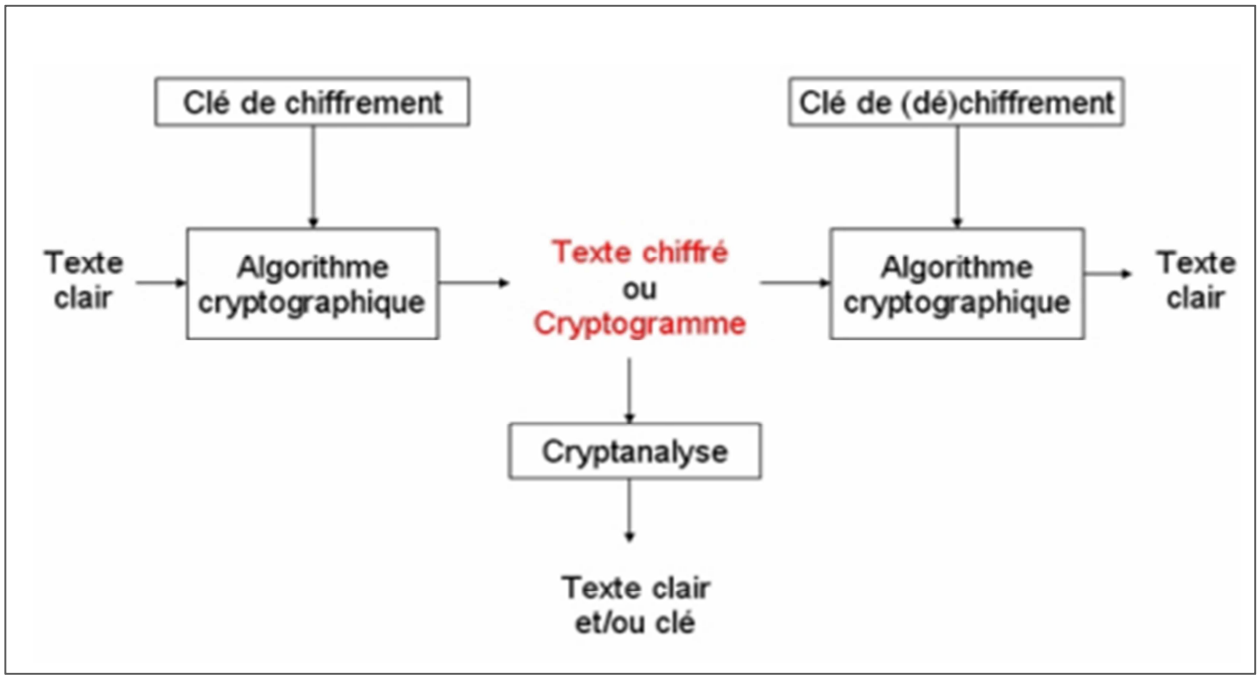

Figure III.1 : Principe de Chiffrement.

- **Cryptologie** représente la science mathématique comportant deux branches : la cryptographie et la cryptanalyse
- **La cryptographie** est l'art de rendre inintelligible, de crypter, de coder, un message pour ceux qui ne sont pas habilités à en prendre connaissance. Le chiffre, le code est le procédé, l'algorithme, la fonction, qui permet de crypter un message.
- **La cryptanalyse** C'est l'art d'étude des crypto systèmes en cherchant leurs familles et leurs vulnérabilités afin de retrouver des messages clairs correspondant à des messages chiffrés sans avoir à connaître les clés utilisées dans le chiffrement. Lorsque tous les éléments de la méthode utilisée pour coder des messages sont repérés, on dit qu'on a cassé ou brisé le système cryptographique utilisé. Plus un système est difficile à briser, plus il est sûr
- **Chiffrement :** Le chiffrement consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le

message et celui qui en est le destinataire. La fonction permettant de retrouver le texte clair à partir du texte chiffré porte le nom de déchiffrement.

- **Texte chiffré :** Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.
- **Clef :** Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement. Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux opérations.
- **Cryptosystème :** Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.

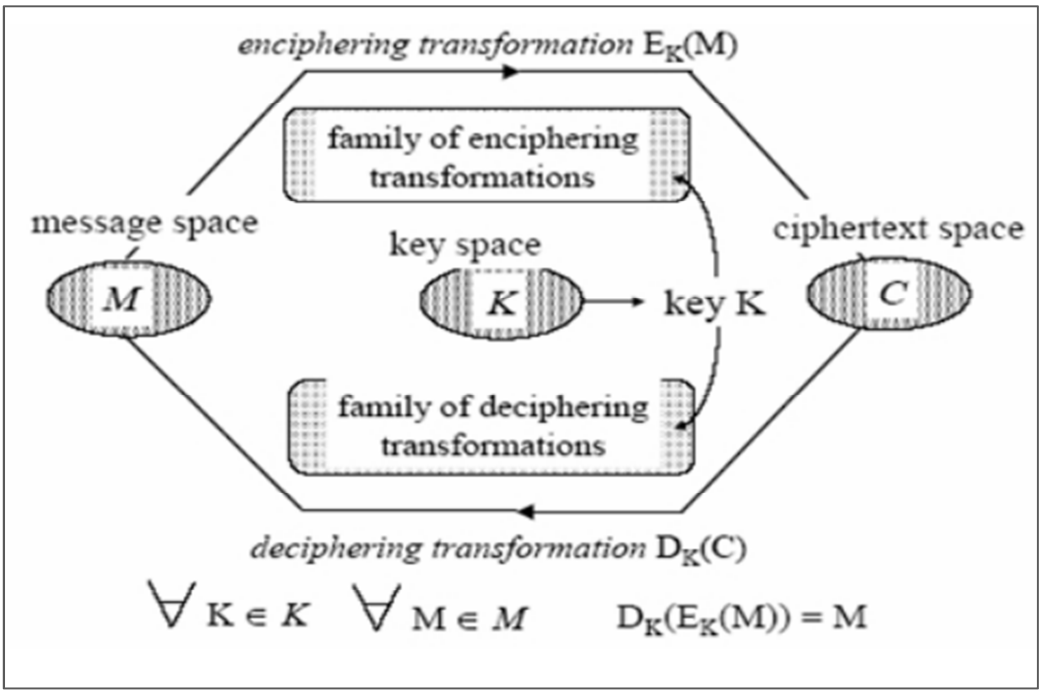

Figure III.2 : Schéma d'un cryptosystème

II.4. Cryptosystème à Clé Symétrique

Ce type de cryptographie est utilisée depuis déjà plusieurs siècles, reconnue sur le terme « cryptographie à clefs privées ». C'est l'approche la plus authentique du chiffrement de données et mathématiquement la moins problématique. **[III.4]**

La clef servant à chiffrer les données peut être facilement déterminée si l'on connaît la clef servant à déchiffrer et vice-versa. Dans la plupart des systèmes symétriques, la clef

de cryptage et la clef de décryptage sont une seule et même clef. Parmi les propriétés de ce système **[III.1]** :

- La clé doit rester secrète.
- Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé.
- La taille des clés est souvent de l'ordre de 128 bits. Le DES en utilise 56, mais l'AES peut aller jusque 256, (détaillée par la suite).
- L'avantage principal de ce mode de chiffrement est sa rapidité.
- Le principal désavantage réside dans la distribution des clés : pour une meilleure sécurité, on pratiquera à l'échange de manière manuelle. Malheureusement, pour de grands systèmes, le nombre de clés peut devenir conséquent. C'est pourquoi on utilisera souvent des échanges sécurisés pour transmettre les clés. En effet, pour un système à N utilisateurs, il y aura N. (N − 1)/2 paires de clés.

Les principaux types de crypto systèmes à clefs privés utilisés aujourd'hui se répartissent en deux grandes catégories : les cryptosystèmes par flots et les crytosystèmes par blocs, sont détailles dans la partie suivante.

II. 5. Cryptosystème à Clé Asymétrique

La cryptographie asymétrique ou encore dite à clé publique utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que de l'utilisateur et qui est sensé d'être en mesure de faire signature ou déchiffrement. L'autre est publique diffusée en général dans un annuaire et donc accessible par quiconque afin de permettre aux interlocuteurs de mettre en œuvre les opérations réciproques (vérification de signature ou chiffrement de message). Parmi les propriétés de ce système : **[III.4] [III.1]**

- la notion de code à clef publique fondé sur la notion de fonction à sens unique (facile à calculée, mais extrêmement difficile de déduire la fonction inverse)

- Ce cryptage présente l'avantage de permettre le placement de signature numérique dans le message et ainsi permettre l'authentification de l'émetteur grâce à la fonction de hachage.

- Le principal avantage consiste à résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé puisque la clé privée n'est connue que par l'utilisateur.
- Les algorithmes se basent sur des concepts mathématiques tels que l'exponentiation de grands nombres premiers (RSA), le problème des logarithmes discrets (ElGamal).
- La taille des clés s'étend de 512 bits à 2048 bits en standard. Dans le cas du RSA, une clé de 512 bits n'est p lu s sûre au se ns "militaire" du terme, mais est toujours utilisable de particulier à particulier.
- Au niveau des performances, le chiffrement par voie asymétrique est environ 1000 fois plus lent que le chiffrement symétrique.
- Cependant, à l'inverse du chiffrement symétrique où le nombre de clés est le problème majeur, ici, seules n paires sont nécessaires. En effet, chaque utilisateur possède une paire (SK, PK) et tous les transferts de message ont lieu avec ces clés.
- La distribution des clés est grandement facilitée car l'échange de clés secrètes n'est plus nécessaire. Chaque utilisateur 2 conserve sa clé secrète sans jamais la divulguer. Seule la clé publique devra être distribuée **[III.1]**.

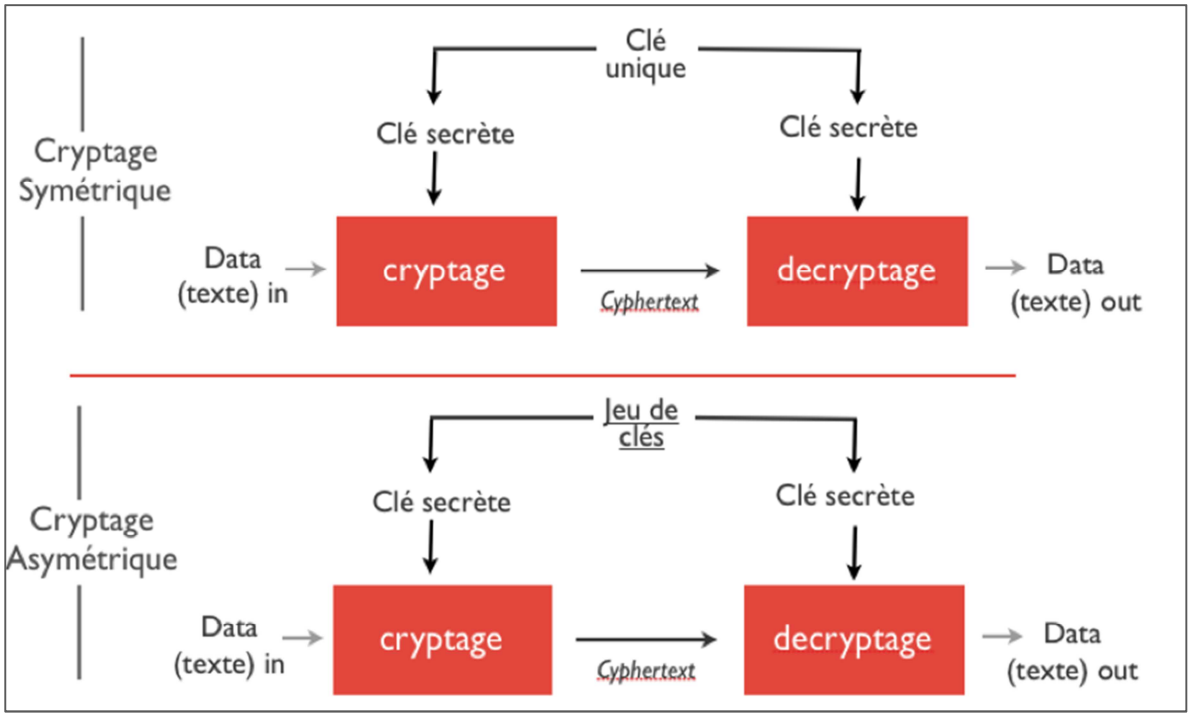

Figure III.3 : schéma d'un Cryptosystème à clé symétrique Vs asymétrique.

II. 6. Qualités d'un Cryptosystème

Traditionnellement le but principal de la cryptographie est de dissimuler un message aux yeux de certains utilisateurs pour assurer leur fiabilité et confidentialité au travers d'un canal peu sur. Après quelques années, les fonctions de la cryptographie se sont étendues pour englober de nouvelles fonctions en plus de la fiabilité et la confidentialité **[III.3]**. Les qualités demandées à un système cryptographique sont résumées par les mots clefs suivants : confidentialité, intégrité et l'authentification. Il s'agit de les garantir pour assurer une transmission sécurisé des données échangées.

- **Confidentialité :**

Elle est la propriété qui assure que l'information est rendu inintelligible aux individus, entités, et processus non autorisée. Dans le cas de systèmes à clés symétrique, la même clé est utilisée. Ce type de chiffrement nécessite un échange sûr préalable de la clé K entre les entités A et B. Par contre dans un cryptosystème asymétrique, cet échange préalable n'est pas nécessaire. Chaque entité possède sa propre paire de clés.

- **Intégrité :**

Vérifier l'intégrité des données consiste à déterminer si les données, ressources, traitements ou services n'ont pas été altérées durant la communication de manière fortuite ou intentionnelle. C'est ici qu'interviennent les fonctions de hachage.

- **Authentification**

L'authentification consiste à assurer l'identité d'un utilisateur c.à.d. de garantir à chacun de correspondant que son partenaire est bien celui qu'il croit être. On distingue deux types d'authentification : **[III.1] [III.5]**

  - Le contrôle d'accès : C'est l'opération permettant d'être certain de l'identité d'une personne utilisateur pour permettre l'accès à des ressources uniquement pour la personne autorisée (par exemple l'utilisation d'un mot de passe pour un disque dur).
  - Authentification de l'origine des données : Elle sert à prouver que les données reçues ont bien été émises par l'émetteur déclaré. Dans ce cas,

l'authentification désigne souvent la combinaison de deux services, l'authentification et l'intégrité.

II.7. Principe de Kerckhoffs

Pour briser un cryptosystème, un opposant cherche à obtenir deux éléments d'information :

- Quel est le type de système de codage utilisé ?
- Quelle est la clé d'encodage utilisée ?

Bien entendu, son travail est simplifié (mais certainement pas terminé) s'il connait le type de système utilisé. Avec le temps cette information finit par circuler. Cette hypothèse de travail est appelée **le principe de Kerckhoffs [III.3]**. Ce principe consiste à affirmer que la sécurité d'un système de chiffrement ne devrait pas être fondée sur le secret de la procédure utilisée, mais essentiellement sur le secret de la clé. Auguste Kerckhoffs écrit en janvier 1883 dans le « Journal des sciences militaires » un article intitulé « La cryptographie militaire », où il disait :

« Il faut bien distinguer entre un système d'écriture chiffrée, imaginé pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux. Ceux-ci, en effet, ne peuvent, à leur gré et à un moment donné, modifier leurs conventions ; de plus, ils ne doivent jamais garder sur eux aucun objet ou écrit qui soit de nature à éclairer l'ennemi sur le sens des dépêches secrètes qui pourraient tomber entre ses mains.

Un grand nombre de combinaisons ingénieuses peuvent répondre au but qu'on veut atteindre dans le premier cas ; dans le second, il faut un système remplissant certaines conditions exceptionnelles, conditions que je résumerai sous les six chefs suivants :

- le système doit être matériellement, sinon mathématiquement, indéchiffrable.
- il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénients tomber entre les mains de l'ennemi.

- la clé doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants.
- il faut qu'il soit applicable à la correspondance télégraphique.
- il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes.
- enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer ».

II.8. La Cryptographie Classique

Cette section est consacrée aux systèmes cryptographiques qui ont été conçus avant la création des ordinateurs et qui ont donné les concepts et les bases pour l'évolution de plusieurs algorithmes symétriques encore utilisé dans nos jours. Dans le schéma ci-dessous figurent les différentes branches de la cryptographie classique **[III.1] [III.4]**

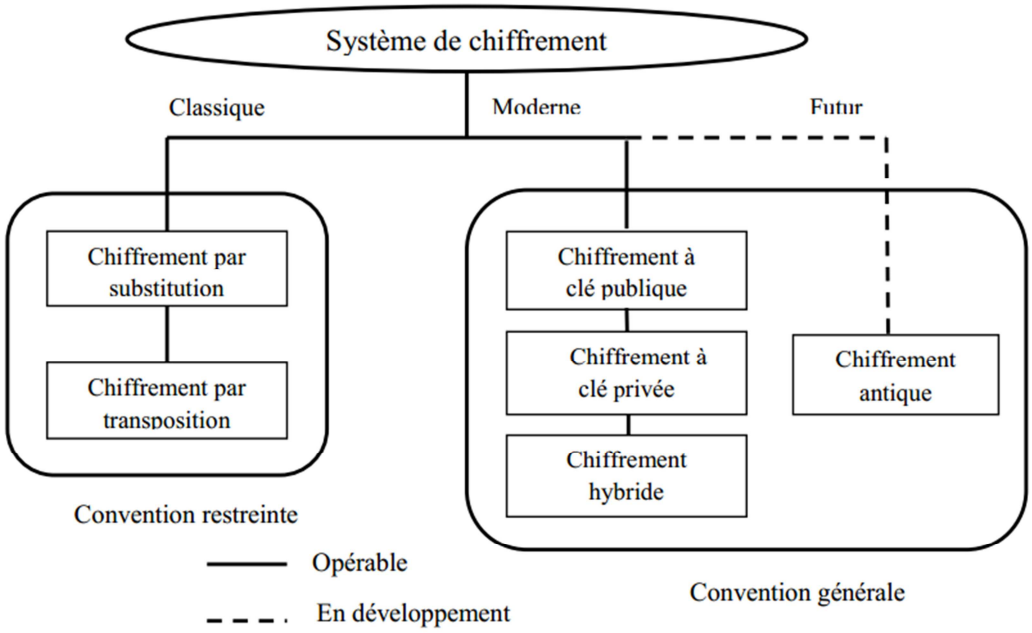

Figure III.4 les différentes branches d'un système de chiffrement

II.8.1. Cryptographie par substitution

- **Substitution monoalphabétique**

Le principe est simple, il suffit de remplacée chaque lettre par une autre. À l'époque, Il était considéré parmi les techniques les plus fiable et populaires. Il a été longtemps utilisé par les armées grâce à sa simplicité mais cela provoque un problème d'intégrité, il est évident que la sûreté de ce codage est quasi nulle et qu'il pourrait être déchiffré par n'importe quelle personne qui y mettrait le temps nécessaire.

- **Substitution poly-alphabétique**

Au lieu de remplacer une lettre par une même autre lettre dans tout le message comme dans la substitution simple, elle est remplacée périodiquement par différentes lettres. L'exemple le plus fameux de chiffre poly-alphabétique est sans doute le chiffre de Vigenère, qui a résisté aux cryptanalystes pendant trois siècles.

- **Substitution par poly-grammes**

Au lieu de substituer des caractères, on substitue par exemple des digrammes : groupe de n caractères par un autre groupe de n symboles. Pour se faire, deux moyen sont utilisés : soit par table (Chiffre de Playfair) ou par transformation mathématique (Chiffre de Hill).

II.8.2. Cryptographie par transposition

C'est un système simple, il consiste à changer l'ordre des lettres du message à chiffrer entre elles, afin de le rendre inintelligible. Un message de n lettres pourra être transposé dans n! Positions différentes, par conséquent ce système devient peu sûr pour de très brefs messages car il y a peu de variantes. Plusieurs variations de transposition sont utilisées, parmi eux on trouve :

- **Transposition simple (à base matricielle)**

  Elle consiste à écrire le texte en clair dans une matrice de n colonnes (une lettre dans chaque case), et ensuite de construire le texte chiffré en prenant les lettres à partir de cette matrice colonne par colonne. La clé dans ce cas est le nombre n.

- **Transposition avec substitution simple**

  L'idée dans ce cas est de combiner la transposition avec une substitution simple. Il s'agit ainsi de chiffrer le message clair par une méthode de substitution simple, et en suite d'en appliquer une transposition. Une autre astuce est souvent utilisée qui consiste à appliquer une fonction de permutation sur l'ordre d'arrangement des colonnes. On cite à titre d'exemple : le chiffre de DELASTELLE.

II.9. La cryptographie moderne

II.9.1. Cryptographie à clefs privés

Les principaux types de cryptosystèmes à clefs privés utilisés aujourd'hui se répartissent en deux grandes catégories : les cryptosystèmes par flots et les crytosystèmes par blocs **[III.6].**

II.9.1.1. Chiffrement par flot

Le chiffrement par flot crypte séparément un caractère individuel, en utilisant une transformation qui varie au fur et à mesure du temps. L'idée principale du système est de produire un flux de clefs $z = z_1, z_2, z_3, \dots, z_n$ et d'utiliser z, conjointement avec le texte clair $x = x_1, x_2, x_3, \dots, x_n$ pour générer le texte chiffré $y = y_1, y_2, y_3, \dots, y_n$. Parmi les techniques les plus connue le chiffrement de masque jetable.

- **Masque jetable (one-time pad)**

Ce chiffre appelé aussi chiffre de Vernam ou encore le chiffrement parfait ; est un algorithme de cryptographie inventé par Gilbert Vernam en 1917 **[III.1].** La sécurité de ce système est basée sur la génération complètement aléatoire des clés, cela le rend le seul chiffrement qui soit théoriquement incassable. Par conséquence, si le cryptanalyste ne possède aucune information sur laquelle son attaque va appuyer, tous les masques seront équiprobables.

L'inconvénient majore de cette technique centré sur l'importante difficulté de mise en œuvre pratique, elle ne peut être utilisée pour chiffrer des flux importants de données à cause de la taille de la clé nécessitant des générateurs aléatoires pour sa création.

Il consiste à combiner le message en clair avec une clé présentant les caractéristiques suivantes :

- Choisir une clé K_M aussi longue que le texte à chiffrer.
- Utiliser une clé constituée de caractères choisis aléatoirement.
- Ne jamais utiliser 2 fois la même clé (d'où le nom de masque jetable).
- Pour chiffrer un message faire le ou exclusif du message et de la clé : $C=M \oplus K_M$.
- Pour déchiffrer un message l'opération est la même : $M= C \oplus K_M = M \oplus K_M \oplus K_M$.

II.9.1.2. Chiffrement par blocs

Le chiffrement par bloc chiffre un groupe de caractères (bloc) simultanément en employant des transformations fixes sur tous les blocs **[III.1].** Il est considéré comme un cas particulier du chiffrement par flot ou $zi=k \ \forall \ i \geq 1$.

L'idée générale du chiffrement par blocs est la suivante :

1. Remplacer les caractères par un code binaire
2. Découper cette chaîne en blocs de longueur donnée
3. Chiffrer un bloc en l'"additionnant" bit par bit à une clef.
4. Déplacer certains bits du bloc.
5. Recommencer éventuellement un certain nombre de fois l'opération 3.
6. Passer au bloc suivant et retourner au point 3 jusqu'à ce que tout le message soit chiffré.

- **Réseau de Feistel**

Il s'agit d'une construction qui s'appuie sur des principes simples d'opérations répétées des permutations et substitutions des blocs de données, Figure III.5. La clef k est utilisée pour générer une séquence de n sous-clefs qui seront employées dans dons chaque ronde. Le bloc d'entrée est séparé en deux partie A et B. une fonction f est appliquée à une des deux moitiés. Une ronde de Feistel calcul A_i B_i à partir de A_{i-1} B_{i-1} selon :

$$A_i=B_{i-1} \text{ et } B_i=A_{i-1} + f(B_{i-1}, k_i)$$

Le résultat est alors combiné avec l'autre moitié à l'aide d'un ou exclusif. L'inversion est très simple et il suffit d'appliquer la même transformation dans l'ordre inverse des sous-clefs. **[III.6]**

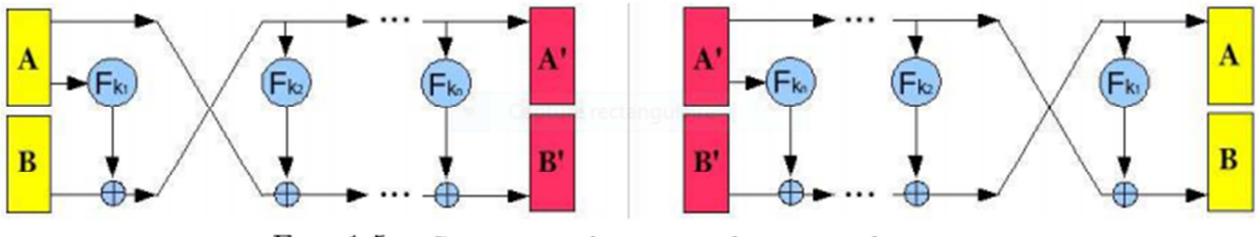

Figure III.5 : Cryptage et décryptage du réseau de Feistel.

- **DES (Data Encryption Standard)**

Le DES est un algorithme de chiffrement symétrique par blocs a été adopté comme un standard en 1976 par le NBS, néanmoins il a été élaboré au début des années 1970 par Horst Feistel [III.6], il permet de chiffrer des mots de 64 bits à partir d'une clef de 56 bits (56 bits servant à chiffrer + 8 bits de parité servant à vérifier l'intégrité de la clef en réalité) à l'aide d'un réseau de Feistel à 16 rondes.

- **AES (Advanced Encryption Standard).**

L'AES est un système cryptographique symétrique, son principe repose sur une suite d'opérations de permutation et de substitution. Il est considéré comme une amélioration ou une mise à jour du système DES. Contrairement à AES ce n'est pas un réseau de Feistel mais un réseau de substitution-permutation. AES travaille sur des blocs de 128 bits avec des clefs de longueur 128, 192 ou 256 bits. A l'origine AES pouvait travailler sur des blocs de longueur Nb × 32 bits où Nb variait de 4 à 8, finalement la taille de blocs d'AES a été fixée à 128 bits et donc Nb a été fixé à 4. Le passage à une clé de 128 bits minimum rend impossible dans le futur prévisible les recherches exhaustives de clefs. Si on suppose que l'on a un algorithme capable de comparer en une seconde 256 clef (i.e de casser DES en une seconde) il lui faudra 149 mille milliards d'années pour casser AES. **[III.2]**

II.9.1.3. Cryptographie à clefs public

Tous les algorithmes évoqués jusqu'à présent sont symétriques en ce sens que la même clef est utilisée pour le chiffrement et le déchiffrement. L'idée de base des cryptosystèmes à clefs publiques est d'utiliser des clefs de chiffrement et déchiffrement différentes, non reconstructibles l'une à partir de l'autre :

- une clef publique pour le chiffrement
- une clef secrète pour le déchiffrement

Ce système est basé sur une fonction à sens unique, soit une fonction facile à calculer dans un sens mais très difficile à inverser sans la clef privée.

- **RSA**

L'algorithme le plus célèbre d'algorithme à clef publique a été inventé en 1977 par Ron Rivest Adi Shamir et Len Adleman **[III.4]**. RSA est basé sur la difficulté de factoriser un grand nombre en produit de deux grands facteurs premiers. L'algorithme fonctionne selon les étapes suivantes :

1. génération des clefs :
   - grâce à un algorithme de test de primalité probabiliste, deux grands nombres premiers p et q, sont générés au hasard, avec n = pq.
   - Un nombre entier e premier avec (p-1)(q-1) est choisi.
   - L'entier d est l'entier de l'intervalle [2, (p-1)(q-1)[tel que ed soit congrue à 1 modulo (p-1)(q-1), c'est-à-dire tel que ed-1 soit un multiple de (p-1)(q-1).
2. distribution des clefs :
   Le couple (n, e) constitue la clef publique.
   Le couple (n, d) constitue la clef privée.
3. chiffrement du message :
   Pour crypter un message, il faut tout d'abord représenté le message sous la forme d'un ou plusieurs entiers M compris entre 0 et n-1. On calcule C= M^e mod n grâce à la clef publique (n, e).

4. déchiffrement du message :

Pour déchiffrer le message C, il sefis calculer, grâce à sa clef privée, C^d mod(n) afin d'obtenir le message initial M.

Malheureusement, RSA est un algorithme très lent, beaucoup plus lent que n'importe quel système symétrique, et d'autant plus que les nombres utilisés sont grands. De plus, il est aujourd'hui facilement cassable.
Il est donc préférable de l'utiliser pour envoyer de manière sécurisée une clef secrète, qui permettra de déchiffrer le message, avec AES plus rapide que RSA. **[III.7]**

- **Chiffrement d'ElGamal**

Le cryptosystème d'ElGamal utilise un nombre premier p, avec grand diviseur premier q de p−1, et un générateur g du sous-groupe cyclique G d'ordre q de $\mathbb{F}_P^*$, tous publics. Des destinataires multiples peuvent établir des clefs publiques compatibles à partir d'une triplette (p, q, g) donné. En particulier, le destinataire A choisi un élément k au hasard dans l'anneau résiduel $\mathbb{Z}/q\mathbb{Z}$ et calcule $h = g^k$dans $\mathbb{F}_P^*$. Il publie la clef publique (p, q, g, h), et retient k pour sa clef privée. Pour chiffrer un message m de $\mathbb{F}_p$, l'expéditeur B choisit un l au hasard dans $\mathbb{Z}/q\mathbb{Z}$, calcule la paire [III.8]

$$(r, s) = (g^l, mh^l) \in \mathbb{F}_p^* \times \mathbb{F}_p \qquad \text{(III.1)}$$

Qu'il envoie à A. Pour déchiffrer ce texte chiffré, A calcule

$$r^k = g^{kl} = h^l \; et \; puis \; s(r^k)^{-1} = sh^{-l} = m \qquad \text{(III.2)}$$

On remarque que le choix aléatoire de l associe des textes chiffrés multiples à un message donné.

L'avantage majeur de ce cryptosystème sur RSA est qu'il se généralise facilement à un groupe abélien arbitraire. En particulier, il a donné naissance à la cryptographie à base de courbes elliptiques.

III.10. Cryptage d'images

Dans ce monde numérique, une image est une collection de pixels ayant différentes valeurs d'intensité. Chaque image est composée de n * m nombre de pixels, où n est le nombre de lignes et m le nombre de colonnes. Un pixel (élément d'image) est un petit bloc qui représente la quantité d'intensité de gris à afficher pour cette partie particulière de l'image. Pour la plupart des images, les valeurs en pixels sont des entiers allant de 0 (noir) à 255 (blanc)

Dans cette section, nous exposerons comment il est possible d'appliquer les algorithmes présentés précédemment à des images en niveaux de gris. Ces algorithmes standard doivent être modifiés afin d'être applicables efficacement sur les images. Une différence essentielle entre les données texte et les données image est que la taille des données image est beaucoup plus grande que les données texte. Le temps est un facteur très important pour le cryptage des images. Nous le trouvons à deux niveaux, l'un est le temps de chiffrer, l'autre est le temps de transférer des images. Pour le minimiser, la première étape consiste à choisir une méthode robuste, rapide et simple pour implémenter un cryptosystème. Un autre critère important concerne la méthode de compression : elle diminuera la taille des images sans perte de qualité.

II.10.1. Le chiffrement de Vigenère :

La formule originale du chiffrement Vigenere pour le chiffrement et le déchiffrement est

$$C = (P + K) \, mod \, 26 \tag{III.3}$$

$$P = (C - K) \, mod \, 26 \tag{III.4}$$

La valeur de 26 est la représentation du nombre de lettres de A à Z, qui est ensuite représenté par les chiffres de 0 à 25 indiquant la position des lettres dans l'ordre alphabétique **[III.9]**. L'intensité du pixel étant une valeur numérique comprise entre 0 et 255, la formule initiale de Vigenere doit ensuite être modifiée pour s'adapter à cette nouvelle plage de valeurs. La formule modifiée à des fins de chiffrement est

$$C = (P + K) \, mod \, 256 \tag{III.5}$$

$$P = (C - K) \, mod \, 256 \tag{III.6}$$

Ce processus de cryptage et de décryptage est appliqué à toutes les valeurs d'intensité dans chaque pixel. De plus, un décalage circulaire binaire est appliqué pour améliorer le résultat de chiffrement du chiffrement de Vigenere. Cette étape est nécessaire car le résultat de chiffrement de Vigenere affiche encore visuellement l'image d'origine, bien que mathématiquement ait montrée des données différentes. La méthode circulaire utilisée pour le processus de décalage de bits ne fait l'objet d'aucune rotation, comme illustré à la Figure III.6

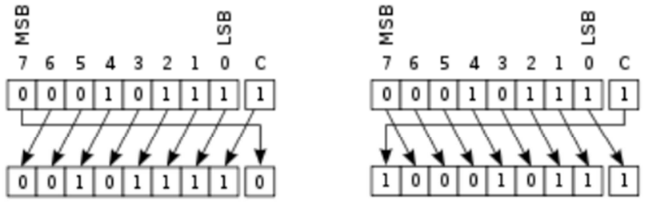

Figure III.6 : tourner sans porter

Dans cette opération, un bit est soumis à une rotation, comme si les extrémités gauche et droite du registre étaient jointes. Toute valeur aux extrémités droites est prise et placée aux extrémités gauches du registre (Figure III.6.b), et inversement.**[III.9]**

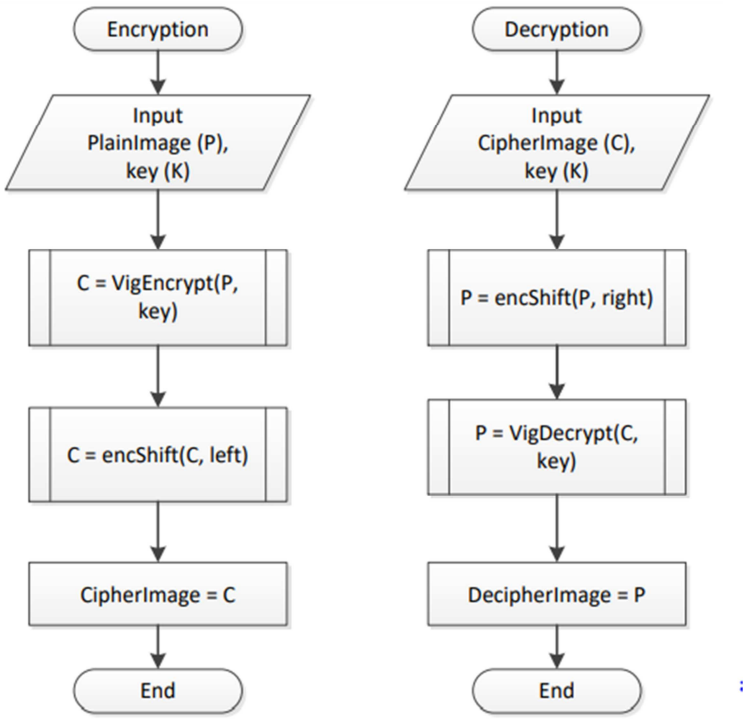

Figure III.7 : Organigramme pour le cryptage et le décryptage

II.10.2. Masque jetable

Cette méthode de cryptographie nécessite d'une image M (la cléf) dont les pixels, uniquement noirs ou blancs, ont été tirés aléatoirement, et d'une image S de même taille, elle aussi composée uniquement de pixels noirs ou blancs, mais qui représentent le secret. **[III.10]**

À l'aide d'un logiciel de dessin ou d'un programme, on opère le «ou exclusif» entre les pixels de M et ceux de S. Cela donne une image chiffrée C. En clair : pour chaque emplacement de pixel, si le pixel de M est le même que celui de S, on dessine sur C un pixel blanc, sinon on dessine un pixel noir. Le message chiffré C résulte ainsi d'un XOR entre le masque M et le secret S, c'est-à-dire :

$$C = M\ XOR\ S. \qquad (III.7)$$

II.10.3. Cryptage et décryptage d'images à l'aide de RSA

L'idée de base de la création du cryptosystème RSA est pour chiffrer et déchiffrer les données texte, pour appliquer cette technique de cryptographie sur les images il faut tout d'abord la diviser en plusieurs blocs de tailles égales (division de premier niveau) et en mélangeant chaque bloc du même niveau. Notre équation donnée ci-dessous ($III.8$)la décrit plus clairement **[III.11]** :

$$frame = \sum_{l=0}^{l=N} \sum_{m=0}^{m=N} B_{im} \qquad (III.8)$$

Où B= bloc d'une image.

Dans l'équation (III.9), le premier bloc d'image partiellement cryptée (de la division de premier niveau) a été repris et divisé en plusieurs grilles (division de second niveau). Les grilles sont ensuite mélangées.

$$B_{im} = \sum_{n=0}^{n=N} \sum_{r=0}^{n=N} G_{nr} \qquad (III.9)$$

Où G= grilles d'un bloc.

La division de second niveau de l'image partiellement cryptée ou également appelée division basée sur une grille est en outre prise en pixels, ce qui est dérivé de l'équation (III.10). Au même niveau, le brassage est à nouveau effectué.

$$G_{11} = \sum_{x=0}^{x=K} \sum_{y=0}^{y=K} p_{xy} \qquad (III.10)$$

Où $P =$ pixel dans un grille.

Le cryptage final de toute image partiellement cryptée est effectué dans l'équation (III.11). Dans cette équation, cette approche a crypté l'ensemble de l'image partiellement cryptée à partir de plusieurs niveaux. Ici, nous utilisons le cryptosystème RSA pour le cryptage final afin d'obtenir les pixels cryptés.

$$p_{ij} \rightarrow p'_{ij} \qquad (III.11)$$

Où p_{ij} = pixel original, p'_{ij} pixel crypté par RSA.

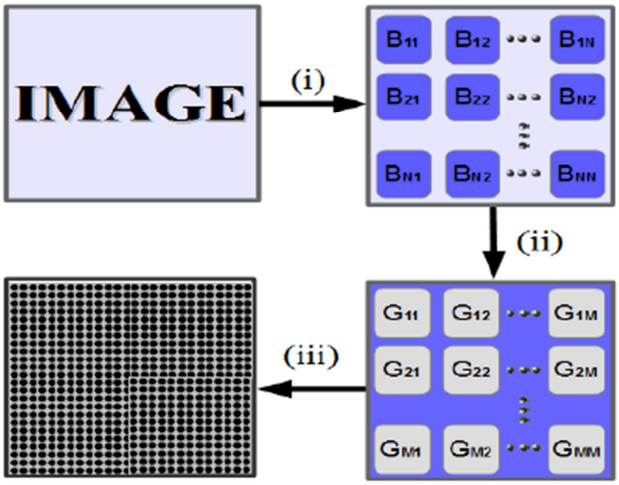

Figure III.8 : principe de chiffrement d'image par RSA

Où (i), (ii) et (iii) représente les étapes de cryptage RSA.

Après le cryptage de l'image pixel par pixel, la transmission de l'image cryptée est effectuée.

Lorsqu'il est reçu par le récepteur, le récepteur effectue l'opération complète dans l'ordre inverse, c'est-à-dire qu'il ne considère l'image cryptée que comme un groupe de pixels.

III.4 Conclusion

Dans ce chapitre nous avons montré qu'il existait de nombreuses algorithmes afin de sécuriser la transmission et le stockage des données soit textuelles ou image. Nous avons présenté les techniques et quelque théorie de la cryptographie. Nous avons tout d'abord évoqué les notions de base de la cryptographie, ensuite abordé les différent types de classification des algorithmes de chiffrement. Ce chapitre a introduit aussi les principaux algorithmes de cryptage symétrique, asymétrique, par flot et par bloc et quelques algorithmes de chiffrement d'image.

Chapitre IV

Les Systèmes Dynamiques et Chaotiques

Chapitre IV
Systèmes Dynamiques et Chaotiques

IV.1. Introduction

La mise en place d'interfaces de visualisation à distance de données médicales connaît actuellement une forte demande. Ces interfaces permettent d'accéder aux dossiers des patients contenant des données textuelles et images. Le développement de ces systèmes rencontre deux types de problèmes. Le premier concerne la qualité des données transmises. En effet, pour des raisons de temps de transfert au travers du réseau toutes les données, et en particulier les images, sont comprimées. Le deuxième problème concerne l'aspect sécurité. Pendant le transfert des données, il ne faut absolument pas qu'une image soit dissociée du nom du patient concerné pour éviter toute confusion d'appartenance à la réception de celle-ci. De plus, pour des raisons de confidentialité, pendant le transfert, ces données doivent être rendues illisibles et non déchiffrables, donc cryptées. **[IV.1]**

Dans ce chapitre, on s'intéresse à la sécurisation des données images et plus particulièrement image médicale, qui sont considérées comme des données particulières en raison de leurs tailles et de leurs informations qui sont de natures bidimensionnelles et redondantes. Ces particularités des données rendent les algorithmes développés dans la littérature inutilisables sous leurs formes classiques, à cause des contraintes de la vitesse et de la perte de l'information qui peuvent être causées par un cryptosystème classique. Ainsi, des travaux récents pour la sécurisation des données images ont été orientés vers la conception des nouveaux algorithmes qui assurent une sécurité fiable tout en minimisant le coût de temps de calcul et la perte

d'information. Nous citons par exemple, les algorithmes qui sont basés sur les signaux chaotiques. **[IV.2]**

Pour définir un comportement chaotique. Nous présentons dans ce chapitre, tout d'abord un bref rappel sur les systèmes dynamique en citons quelque caractéristiques numériques et graphiques du ces systemes (Les attracteur, bifurcation et Exposant de Lyapunov). Ensuite nous faisons une étude sur les systèmes chaotiques et leurs applications pour le chiffrement/déchiffrement des données.

IV.2. Systèmes Dynamiques

En général, un système dynamique décrit des phénomènes qui évoluent au cours du temps de façon à la fois : [IV.3]

- Causale, où son avenir ne dépend que de phénomènes du passé ou du présent
- Déterministe, c'est-à-dire qu'à partir d'une condition initiale donnée à l'instant présent va correspondre à chaque instant ultérieur un et un seul état futur possible.

L'évolution déterministe du système dynamique peut alors se modéliser de deux façons distinctes

- Une évolution continue dans le temps, représentée par une équation différentielle ordinaire.
- Une évolution discrète dans le temps, l'étude théorique de ces modèles discrets est fondamentale, car elle permet de mettre en évidence des résultats importants, qui se généralisent souvent aux évolutions dynamiques continues. Elle est représentée par le modèle général des équations aux différences finie.

IV.3. Les attracteurs

Les systèmes d'équations différentielles sont une forme efficace de modélisation des systèmes en général. Les systèmes dynamiques sont décrits sous forme générale par les équations différentielles :

$$\frac{\mathrm{dx(t)}}{\mathrm{dt}} = f(x(t), \mu), \tag{IV.1}$$

Où x est le vecteur variable d'état et μ est le vecteur des paramètres.

L'espace de phase $(x_1, x_2, ..., x_n)$ d'un système dynamique est un espace mathématique dont les axes de coordonnées représentent chacune des variables d'états $x_i, i = \overline{1,n}$ nécessaires pour spécifier entièrement l'état de ce système à chaque instant. La solution de (IV.1), avec les conditions initiales $x\,(t_0) = x_0$, décrit dans l'espace des phases une courbe appelée trajectoire de phase représentant l'évolution du système **[IV.4]**. Pour une vision globale et plus claire, illustrons le concept d'attracteur par l'exemple du système de Lorenz dans l'espace d'état :

$$\begin{cases} \dot{x_1} = -10x_1 + 10x_2 \\ \dot{x_2} = rx_1 - x_2 - x_1x_3 \\ \dot{x_3} = -\frac{8}{3}x_3 + x_1x_2 \end{cases} \tag{IV.2}$$

Où r est un paramètre.

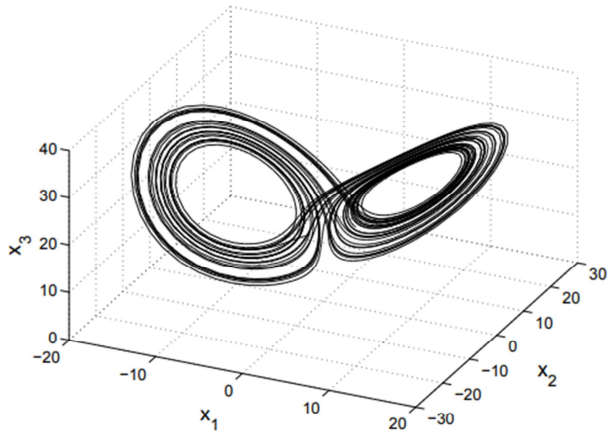

Figure IV.1 : Trajectoires de phase du système de Lorenz dependent du paramètre r $(r = 25)$

En général, les attracteurs sont classés dans une des catégories suivantes :

- **Point fixe :** Les points fixes constituent probablement la catégorie d'attracteur la plus simple représenté par un point dans l'espace d'état, parce qu'elle n'évolue plus avec le temps. La Figure IV.2 gauche présente les trajectoires de phase pour

r = 7 à partir des deux conditions initiales quelconque. Les coordonnées des points fixes en fonction du paramètre r sont : $(\sqrt{10(r-1)}, \sqrt{10(r-1)}, r-1)$ et $(-\sqrt{10(r-1)}, -\sqrt{10(r-1)}, r-1)$.

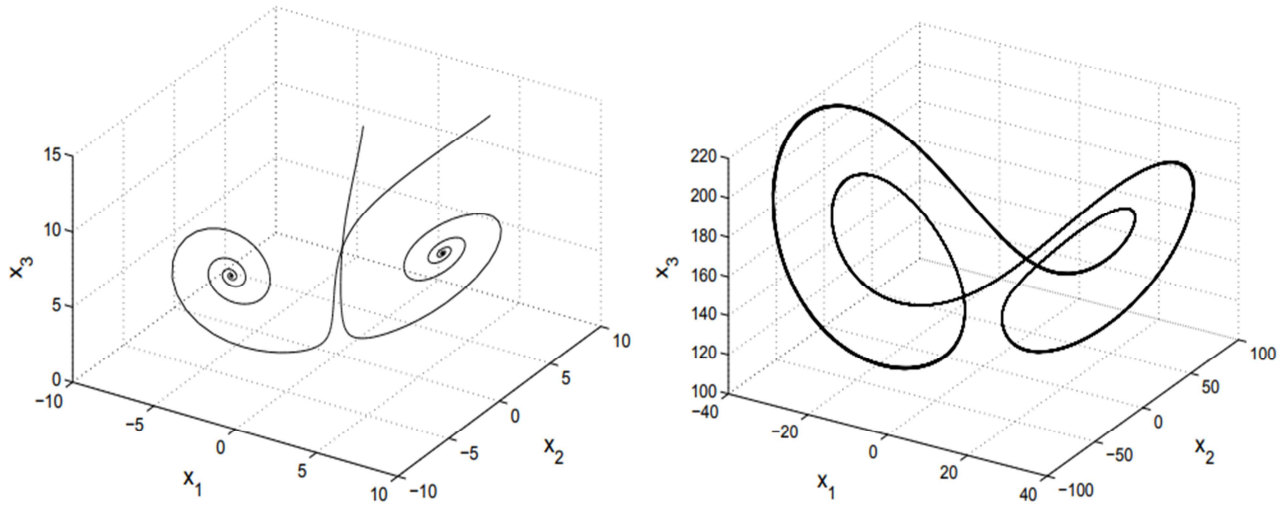

Figure IV.2 : Trajectoires de phases du système de Lorenz dépendant du paramètre r (r=7 pour la figure gauche et r=160 pour la figure droite.)

- **Le cycle limite périodique :** un cycle limite est une trajectoire de phase fermée. Ce mouvement est périodique et associé à un nombre fini de fréquences.
- **L'attracteur quasi-périodique :** un phénomène quasi-périodique, c'est à dire qui combine des phénomènes périodiques indépendants l'un de l'autre, est identifier avec un tore dans l'espace des phases.

La section de Poincaré est définie par l'ensemble des points d'intersection d'un plan avec la trajectoire du vecteur d'état dans l'espace des phases. La section de Poincaré est particulièrement adaptée à l'étude des régimes apériodiques puisqu'elle distingue clairement les régimes quasi-périodiques des régimes chaotiques, par la présence d'une courbe fermée.

- **L'attracteur chaotique :** on observe que la trajectoire dans l'espace des phases reste confinée dans une région bien définie, après une période transitoire de durée variable (ce type d'attracteur sera détaillé par la suite)

IV.4 Exposant de Lyapunov

Le chaos est caractérise par une divergence de deux trajectoires très proches. Cette propriété est utilisée pour tester la présence du chaos. Nous allons exposer comment calculer le taux de divergence entre l'évolution de trajectoires issues de conditions initiales proches au sein de cet espace borné qu'est l'attracteur**.[IV.5]**

Soit un système dynamique autonome :

$$x_{(k+1)} = f(x_k) \tag{IV.3}$$

On considère d'abord que ce système est de dimension n = 1. Soient deux conditions initiales très proches, x_0 et x'_0. La trajectoire issue de la condition initiale x_0 est $x_k = f_k(x_0)$, et celle issue de la condition initiale x'_0 est $x'_k = f^k(x'_0)$.

Si les trajectoires x_k et x'_k s'écartent à un rythme exponentiel après k itérations, alors :

$$|x'_k - x_k| = |x'_0 - x_0| \, exp(k\lambda) \tag{IV.4}$$

$\lambda \in R$ correspond au taux de divergence des deux trajectoires. Il vient :

$$\lambda = \frac{1}{k} \ln \left| \frac{x'_k - x_k}{x'_0 - x_0} \right| \tag{IV.5}$$

Si l'on considère que les deux conditions initiales sont très proches, leur différence

$\epsilon = |x'_0 - x_0|$ tend vers 0 et, lorsque k tend vers l'infini, il vient :

$$\lambda_L = \lim_{k\to\infty} \frac{1}{k} \lim_{\epsilon\to 0} \ln \left| \frac{x'_k - x_k}{x'_0 - x_0} \right| \tag{IV.6}$$

Cette relation est équivalente à :

$$\lambda_L = \lim_{k\to\infty} \frac{1}{k} \lim_{\epsilon\to 0} \ln \left| \frac{x'_k - x_k}{x'_{k-1} - x_{k-1}} . \frac{x'_{k-1} - x_{k-1}}{x'_{k-2} - x_{k-2}} \dots \frac{x'_1 - x_1}{x'_0 - x_0} \right| \tag{IV.7}$$

Ce qui réécrit aussi :

$$\lambda_L = \lim_{k\to\infty} \frac{1}{k} \lim_{\epsilon\to 0} \sum_{i=0}^{k-1} \ln \left| \frac{x'_{i+1} - x_{i+1}}{x'_i - x_i} \right| = \lim_{k\to\infty} \frac{1}{k} \lim_{\epsilon\to 0} \sum_{i=0}^{k-1} \ln \left| \frac{f(x'_i) - f(x_i)}{x'_i - x_i} \right| \quad \text{(IV.8)}$$

Finalement, cette relation devient :

$$\lambda_L = \lim_{k\to\infty} \frac{1}{k} \sum_{i=0}^{k-1} \ln \left| \frac{df(x_i)}{dx_i} \right| \quad \text{(IV.9)}$$

Le terme λ_L est appelé exposant de Lyapunov de la trajectoire $x_k = f_k(x_0)$ ne doit pas être confondu avec λ ou λ_i, valeur propre d'un système linéaire. λ_L mesure le taux moyen de convergence ou de divergence de deux trajectoires issues de conditions initiales très proches. S'il est positif, les trajectoires divergent. Très souvent dans la littérature, si $\lambda_L > 0$, le système est dit chaotique. Intuitivement cela reflète la sensibilité aux conditions initiales.

La relation (IV.9) se généralise aux systèmes de dimension $n > 1$, qui possèdent alors n exposants de Lyapunov. Chacun d'entre eux mesure le taux de divergence suivant un des axes de l'espace de phase. On a alors $x_k = f_k(x_0)\ avec\ x_k = [x_k^{(1)} \dots x_k^{(n)}]T \in Rn\ et\ f = [f_1 \dots f_n]^T$. Les n exposants de Lyapunov λ_{Li} s'écrivent :

$$\lambda_{Li} = lim_{k\to\infty} \frac{1}{k} ln\,|\lambda_i (J_k \dots J_1)|, i = 1, \dots, n \quad \text{(IV.10)}$$

$\lambda_i (J_k \dots J_1)$ représente la iéme valeur propre du produit des matrices $(J_k \dots J_1)$. Les J_k sont les matrices jacobiennes1 issue de la linéarisation de f autour de x_k .

Une condition nécessaire pour qu'un système à temps discret soit chaotique est qu'au moins un de ses exposants de Lyapunov soit positif.

IV.5 Bifurcation

Un autre ensemble de concepts utile à l'analyse des systèmes dynamiques est la théorie de la "bifurcation". Ce concept renvoie à l'étude des changements de comportement d'un système lorsque les paramètres de ce dernier changent. La bifurcation signifie un changement qualitatif de la dynamique du système, qui résulte du changement d'un

des paramètres du système **[IV.6]**. Par exemple, déstabilisation d'un équilibre stable, apparition ou disparition d'un cycle ou d'un attracteur, ...

La valeur pour laquelle la bifurcation se produit est nommée le point de bifurcation.

IV.6 Différents Types de Bifurcations

Dans cette section, on considère trois types de bifurcations locales : la bifurcation de doublement de période, la bifurcation de Neimark et la bifurcation point selle (ou col)/noeud. Ces bifurcations sont locales car elles peuvent être analysées par la linéarisation du système au voisinage d'un point dynamique contemporain avec des programmes en Pascal, Fortran et Mathematica.

IV.6.1 Bifurcation nœud-col

C'est la bifurcation associé à l'équation :

$$x'(t) = f\big(x(t)\big) = \mu x + \alpha x^2(t) \qquad \text{(IV.11)}$$

Avec α et μ les paramètres de contrôle.

Supposons $\alpha > 0$. Pour un paramètre $\mu < 0$, il y a deux points d'équilibres, racines de $\mu + \alpha x^2 = 0$. Si $\mu > 0$, il n'y a aucun point fixe.

Etudient la stabilité des points d'équilibre dans le cas où $\mu > 0$. Notons x^* l'un des deux points d'équilibre, on a donc $f(x^*) = 0$. On introduit une petite perturbation $u(t)$ ajouté au point fixe :

$$x(t) = x^* + u(t) \qquad \text{(IV.12)}$$

Puis nous effectuons un développement de Taylor de f à l'ordre 1 au voisinage de x^* :

$$x'(t) = u'(t) = f(x^* + u) = f'(x^*)u(t) + O(u^2) \qquad \text{(IV.13)}$$

En posant $\lambda = f'(x^*)$, l'équation différentielle obtenue u` = λu s'intègre en $u(t) = u(0)\exp(\lambda t)$. L'étude de la stabilité est simple : si $\lambda > 0$ alors le point d'équilibre est instable et si $\lambda < 0$ alors le point est stable **[IV.7]**. Ainsi la stabilité des points d'équilibres dépend de la pente de la fonction f des points considérés **[IV.7]**.

Tous l'information peux se résumer sur le diagramme de bifurcation dans le plan (x, μ).

En pointillé, le fixe est instable et en trait plein il est stable.

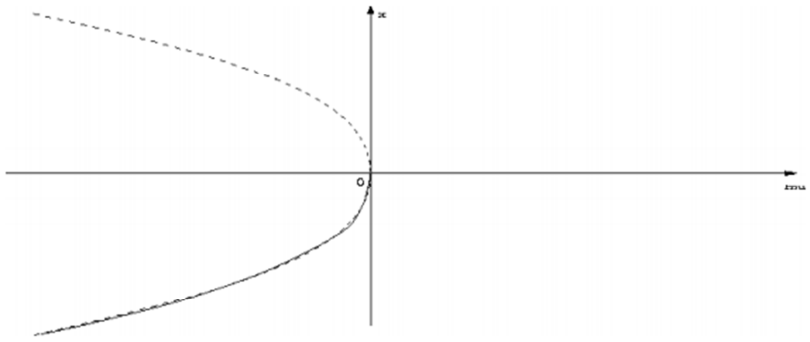

Figure IV.3 : Diagramme de la bifurcation nœud-col.

Si $\alpha < 0$ (on parle de bifurcation super-critique) l'étude est symétrique.

IV.6.2 Bifurcation fourche

C'est la bifurcation associé à l'équation :

$$x'(t) = f\big(x(t)\big) = \mu x + \alpha x^3(t) \qquad \text{(IV.14)}$$

Avec α et μ les paramètres de contrôle. On supposera $\alpha < 0$.

En appliquant la méthode utilisée pour la première bifurcation, nous présentons directement le diagramme de bifurcation dans le plan (x, μ) :

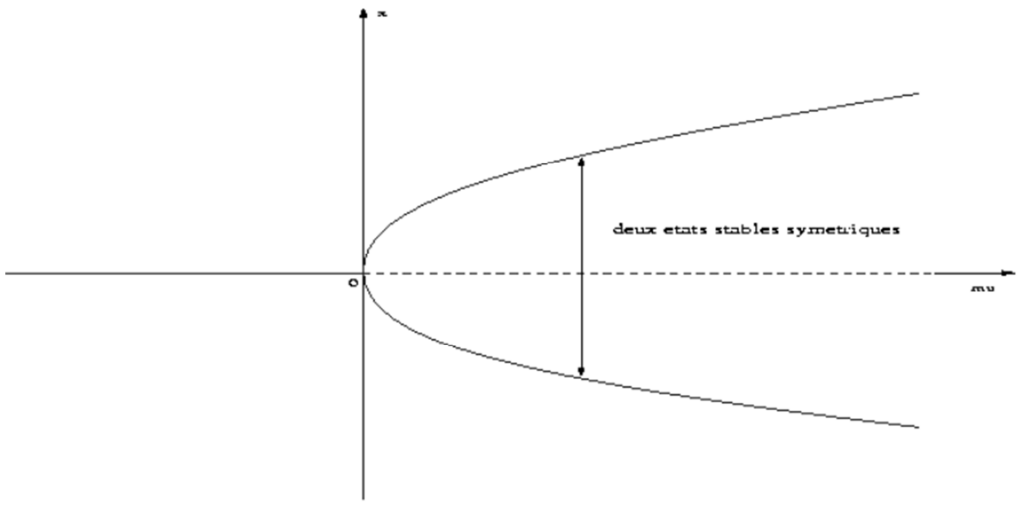

Figure IV.4 : Diagramme de la bifurcation fourche.

Nous partons d'un système où le paramètre μ est négatif. Le système possède alors un point d'équilibre stable ($x = 0$) attracteur. Lorsque nous faisons augmenter progressivement μ jusqu'à la valeur 0, le système se déstabilise, le point d'équilibre perd sa stabilité, il y a bifurcation. Augmentant encore μ, on voit apparaitre alors deux points d'équilibres stables **[IV.7]**. Il existe une symétrique de centre 0 des solutions, si $x(t)$ est solution du système alors $-x(t)$ en est une aussi. Il y a dédoublement du point d'équilibre (cf. le dédoublement de période pour les systèmes dynamique discrets).

IV.6.3 Bifurcation de hopf

C'est la bifurcation associé à l'équation dans le plan complexe :

$$z'(t) = f\big(z(t)\big) = (\mu + i\omega)z(t) - |z|^2 z(t) \qquad \text{(IV.15)}$$

Pour étudier cette équation, on écrit la variable z sous la forme $z(t) = x(t)\exp(i\Theta(t))$. L'équation s'exprime sous la forme d'un système :

$$\begin{cases} x' = \mu x - x^3 \\ \theta' = \omega \end{cases} \qquad \text{(IV.16)}$$

La première équation n'est autre qu'une bifurcation fourche de paramètre de contrôle μ. Le diagramme de bifurcation dans l'espace (Re(z), Im(z),μ) est le suivant :

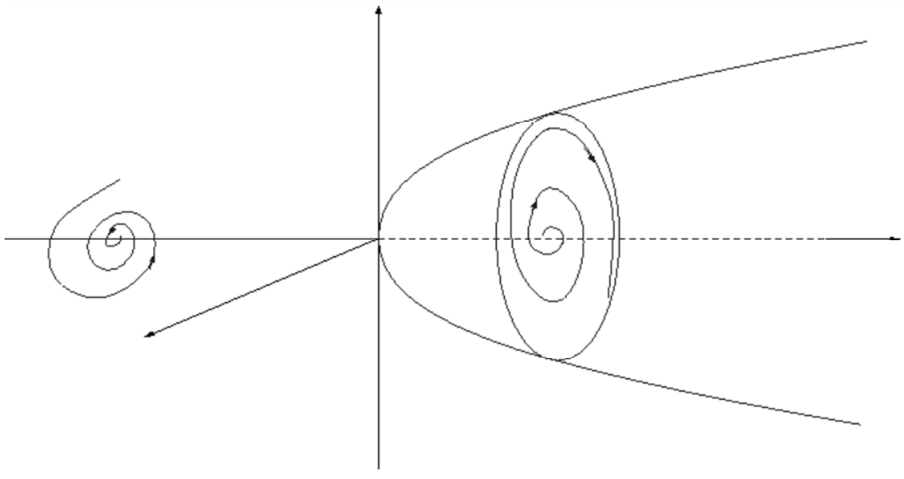

Figure IV.5 : diagramme de Bifurcation de hopf.

Nous partons d'un système où le paramètre μ est négatif. Le système possède un point d'équilibre stable sui correspond ici à un point puits : les trajectoires s'enroulent en

spirale vers l'origine. Lorsque $\mu = 0$, ce point d'équilibre perd sa stabilité. Puis lorsque $\mu > 0$, il se forme alors une trajectoire périodique stable ou **cycle limite**.

La bifurcation de Hopf correspond à une instabilité oscillatoire.

IV.7. Système Chaotique

IV.7.1 Découverte du chaos

La découverte de la dynamique chaotique des systèmes non-linéaires remonte aux travaux d'Henri Poincaré sur la mécanique céleste et la mécanique statistique, vers 1900. Ils ont alors suscité peu d'intérêt et sont tombés dans l'oubli. Il fallut attendre 1963 qu'Edward Lorenz, un météorologue du Massachusetts Institute of Technology, mette en évidence le caractère chaotique des conditions météorologiques et par conséquent des mouvements turbulents d'un fluide comme l'atmosphère. Alors qu'il cherchait à déterminer des conditions météorologiques futures à partir de données initiales sur son ordinateur, il constata qu'une modification minime des données initiales (de l'ordre de un pour mille) entrainait des résultats radicalement différents. Après avoir modélise le mouvement des masses d'air par des relations (très simplifiées) de thermodynamique et de mécanique des fluides, il a programmé son ordinateur de façon à obtenir une simulation numérique. A l'époque, cela prenait beaucoup de temps. Un jour, pour ne pas recommencer les calculs depuis le début, il décida de reprendre son listing et de rentrer en tant que conditions initiales des valeurs prises au cours de la simulation de la veille. L'ordinateur lui donnait une précision à cinq chiffres, cependant trois chiffres significatifs lui semblaient largement suffisants pour ce genre de mesures physiques. Il tronqua donc ces nombres et repris le calcul. Les résultats qui suivirent furent le "déclic". D'abord la simulation semblait redonner les mêmes valeurs, mais au bout d'un moment rien ne concordait, tout se passait comme si le mouvement représenté par ces valeurs changeait complétement de trajectoire et ce, à cause d'une approximation de l'ordre de 10^{-4} ! **[IV.4]**

Cette anecdote est à la base de ce que l'on appelle maintenant le chaos : une infime variation des conditions initiales d'un système bouleverse complétement son évolution. Lorenz venait de mettre en exergue la sensibilité aux conditions initiales. Il expliqua

d'ailleurs très joliment cette notion à l'aide de l'image suivante : le battement d'ailes de quelques papillons peut provoquer es tempêtes aux antipodes.

IV.7.2. Sémantique de la Théorie du Chaos

Le mot chaos n'a pas ici le même sens que l'usage dans la vie courante. On retrouve trace de ce mot du grec Khaos dans les écrits de Christine de Pisan (Chemin de long estude) qui définit le chaos comme :

" Un état de confusion des éléments ayant précédé l'organisation du monde "

Au XVIème siècle Desportes, le décrit dans ses Elegies comme :

" Toute sorte de confusion, de désordre "

Le chaos, dans son sens familier aujourd'hui, c'est le désordre et la violence, mais aussi l'inintelligibilité. Loin de ces considérations historiques et mythologiques, Chaos : un terme souvent utilisé comme métaphore du désordre. Il est défini comme un processus pseudo-aléatoire produit dans des systèmes dynamiques non linéaires [IV.6]. Il est non périodique, non convergent et extrêmement sensible à la condition initiale. En général, le modèle de système chaotique est donné comme

$$x(n) = f(x(n-1)) \qquad \textbf{(IV.17)}$$

Où x (n) est une séquence chaotique générée par la carte non linéaire f, x (0) est la condition initiale. **[IV.8]**

Et la théorie du Chaos a vu le jour dans les travaux d'Henri Poincaré à la fin du XIXe siècle et c'est dans les années soixante qu'elle fut redécouverte après la publication d'un article qui allait révolutionner le monde des sciences. Le chaos est devenu un champ d'exploration de la science.

IV.7.3. Chaos Déterministe

Le chaos est défini par un comportement lié à l'instabilité et à la non-linéarité dans des systèmes dynamiques déterministes. La relation entre l'instabilité et la chaoticité est alors que le système manifeste une très haute sensibilité aux changements de conditions

est ce qu'affirmait Poincaré dans le chapitre sur le Hasard de son ouvrage intitulé Science et Méthode : «Une cause très petite, qui nous échappe, détermine un effet considérable que nous ne pouvons pas ne pas voir, et alors nous disons que cet effet est dû au hasard. (...). Il peut arriver que de petites différences dans les conditions initiales en engendrent de très grandes dans les phénomènes finaux. Une petite erreur sur les premières produirait une erreur énorme sur les derniers. La prédiction devient impossible et nous avons le phénomène fortuit». **[IV.6]**

La théorie du chaos selon Keller est « l'étude qualitative du comportement apériodique instable d'un système dynamique déterministe » qui admet le manque d'une définition générale d'un système dynamique chaotique considère qu'un tel système possède trois propriétés essentielles. Premièrement, il est radicalement sensible aux conditions initiales. Deuxièmement, il peut faire preuve d'un comportement hautement désordonné et troisièmement, malgré cette dernière caractéristique de désordre, un système dynamique chaotique est déterministe c'est-à-dire qu'il obéit à des lois qui décrivent complètement son mouvement.

IV.8. Sensibilité aux Conditions Initiales

La sensibilité aux conditions initiales constitue sans aucun doute la caractéristique essentielle du comportement chaotique d'un système : l'évolution est par conséquent imprévisible à long terme. Pour une condition initiale $x0 = x(0)$, la trajectoire chaotique suit la courbe en trait plein, sur l'exemple de la Figure IV.6. Par contre, une petite variation δx de cette condition initiale entraîne une autre trajectoire (la courbe en pointillés). **[IV.4]**

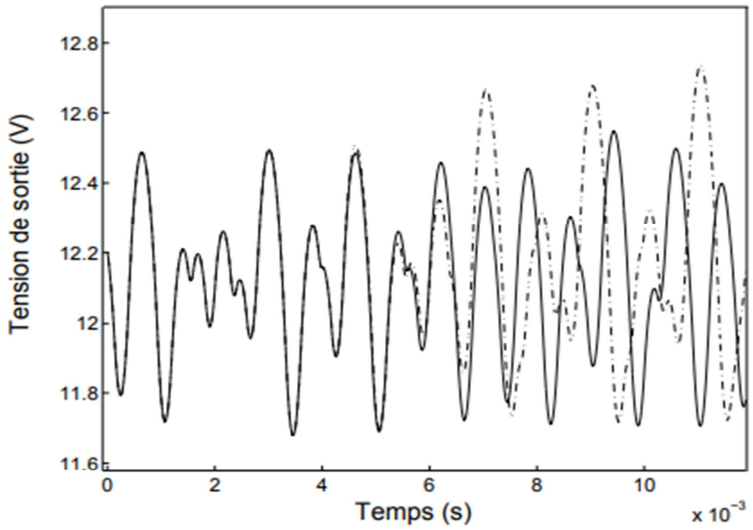

Figure IV.6 : Trajectoires temporelles de la tension de sortie v(t) du convertisseur Buck en fonction de deux conditions initiales presque identiques.

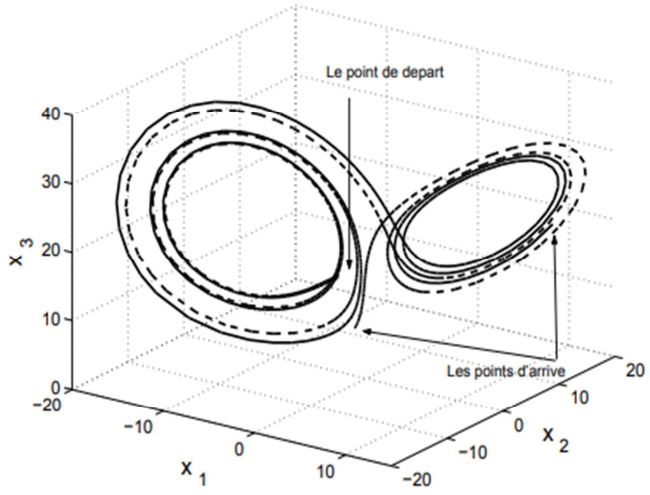

Figure IV.7: Trajectoires de phase du système de Lorenz en fonction de deux conditions initiales presque identiques

Le système chaotique est donc sensible à une toute petite perturbation de la condition initiale x0. Même si les points de départ sont presque identiques, les trajectoires se séparent assez rapidement. Pour illustrer la sensibilité aux conditions initiales d'un système chaotique, reprenons l'exemple du système de Lorenz avec r = 25. La Figure IV.7 présente deux trajectoires de phase avec des conditions initiales distinctes, mais

presque identiques (x_{10} ; x_{20} ; x_{30}) = (0 ; − 5 ; 16, 6) et (x_{10} ; x_{20} ; x_{30}) = (0, 1; − 5 ;16,65). Au début (pour t = 0), les séries temporelles sont confondues. Après quelques itérations, une des trajectoires tourne autour d'un point fixe ($\sqrt{10(r-1)}$; $\sqrt{10(r-1)}$; r − 1), alors que l'autre trajectoire tourne autour d'un second point fixe ($-\sqrt{10(r-1)}$; $-\sqrt{10(r-1)}$; r − 1).

IV.9. Attracteur Chaotique (ou étrange)

Il est contenu dans un espace fini. Son volume est nul. Sa dimension est fractale et non entière ; sa trajectoire est complexe ; presque toutes les trajectoires sur l'attracteur ont la propriété de ne jamais passer deux fois par le même point. En d'autres termes, chaque trajectoire est apériodique ; deux trajectoires proches à un instant " t " voient localement leur distance augmenter à une vitesse exponentielle. Ce phénomène traduit la sensibilité aux conditions initiales ; toute condition initiale appartenant au bassin d'attraction, c'est-à-dire à la région de l'espace des phases dans laquelle tout phénomène dynamique sera "attiré " vers l'attracteur, produit une trajectoire qui tend à parcourir de façon spécifique et unique cet attracteur. Une " définition " d'un attracteur étrange peut être formulée : Un sous-ensemble borné A de l'espace des phases est un attracteur étrange pour une transformation T de l'espace s'il existe un voisinage U de A ; c'est à dire que pour tout point de A il existe une boule contenant ce point et contenue dans R vérifiant les propriétés suivantes :

Attraction : U est une zone de capture, ce qui signifie que toute orbite par T dont le point initial est dans U ; est entièrement contenue dans U : De plus, toute orbite de ce type devient et reste aussi proche de A que l'on veut.

Sensibilité : les orbites dont le point initial est dans R sont extrêmement sensibles aux conditions initiales.

Fractal : A est un objet fractal.

Mélange : Pour tout point de A, il existe des orbites démarrées dans R qui passent aussi près que l'on veut de ce point.

L'une des propriétés géométriques la plus remarquable d'un attracteur étrange est qu'un "zoom" répété indéfiniment sur l'une de ses parties reproduit toujours le même motif feuilleté.

IV.10. Cartes Chaotiques

En mathématiques, une carte chaotique (ou map chaotic en anglais) est une fonction qui présente une sorte de comportement chaotique. Il prend souvent la forme d'une fonction itérée et intervient dans l'étude de systèmes dynamiques. Les cartes chaotiques peuvent être paramétrées par un paramètre à temps continu ou à temps discret. Selon Alligood et al, une carte chaotique est fonction de son domaine, le point de départ de la trajectoire (l'état à partir duquel le système démarre) est appelé la condition initiale. Les cartes chaotiques illustrent clairement les déclarations de nombreuses caractéristiques du comportement chaotique, telles que la sensibilité aux conditions initiales, le comportement complexe et l'évolution de l'information dans un comportement déterministe et imprévisible. Plusieurs cartes chaotiques à une dimension (1-D), à deux dimensions (2-D) et à trois dimensions (3-D) sont proposées dans la littérature. Dans cette sous-section, nous allons décrire brièvement certaines cartes chaotiques, telles que la carte logistique, tente et sine **[IV.9].**

IV.10.1. Carte Logistique

Une récurrence logistique est un exemple simple de suite dont la récurrence n'est pas linéaire. Souvent citée comme exemple de la complexité pouvant surgir de simple relation non linéaire, cette récurrence fut popularisée par le biologiste Robert May en 1976. Sa relation de récurrence est :

$$x_{n+1} + 1 = \mu x_n \, (1 - x_n) \qquad \text{(IV.18)}$$

Elle conduit, suivant les valeurs de μ, à une suite convergente, une suite soumise à oscillations ou une suite chaotique.

Elle est la solution en temps discret du modèle de Verhulst. Le terme «logistique» provient de l'ouvrage de Pierre François Verhulst qui appelle courbe logistique la solution en temps continu de son modèle. Il écrit en 1845 dans son ouvrage consacré à ce phénomène : « Nous donnerons le terme de logistique à cette courbe ». L'auteur

n'explique pas son choix mais « logistique » a même racine que logarithme et logistikos signifie « calcul » en grec. **[IV.10]**

Comportement selon μ :

Dans le modèle logistique, la variable notée ici xn désigne l'effectif de la population d'une espèce. En faisant varier le paramètre μ, plusieurs comportements différents sont observés :

- Si $0 \leq \mu \leq 1$, l'espèce finira par mourir, quelle que soit la population de départ.
- Si $1 \leq \mu \leq 3$, la population se stabilisera sur la valeur $\frac{\mu-1}{\mu}$ quelle que soit la population initiale.
- Si $3< \mu \leq 1+\sqrt{6}$ (approximativement 3,45), la population oscillera entre deux valeurs. Ces deux valeurs sont indépendantes de la population initiale.
- Si 3,45 < μ <3,54 (approximativement), la population oscillera entre quatre valeurs, là encore sont indépendantes de la population initiale.
- Si μ est légèrement plus grand que 3,54, la population oscillera entre huit valeurs, puis 16, 32, etc.
- Vers μ = 3,57, le chaos s'installe. Aucune oscillation n'est encore visible et de légères variations de la population initiale conduisent à des résultats radicalement différents.
- La plupart des valeurs au-delà de 3,57 présentent un caractère chaotique, mais il existe quelques valeurs isolées de μ avec un comportement qui ne l'est pas. Celles-ci s'appellent parfois les iles de la stabilité. Par exemple autour de la valeur 3,82, un petit intervalle de valeurs de μ présente une oscillation entre trois valeurs et pour μ légèrement plus grand, entre six valeurs, puis douze, etc. ces comportements sont encore indépendants de la valeur initiale.
- Au-delà de μ = 4, la population quitte l'intervalle [0,1] et diverge presque pour toutes les valeurs initiales.

Un diagramme de bifurcation permet de résumer tout cela :

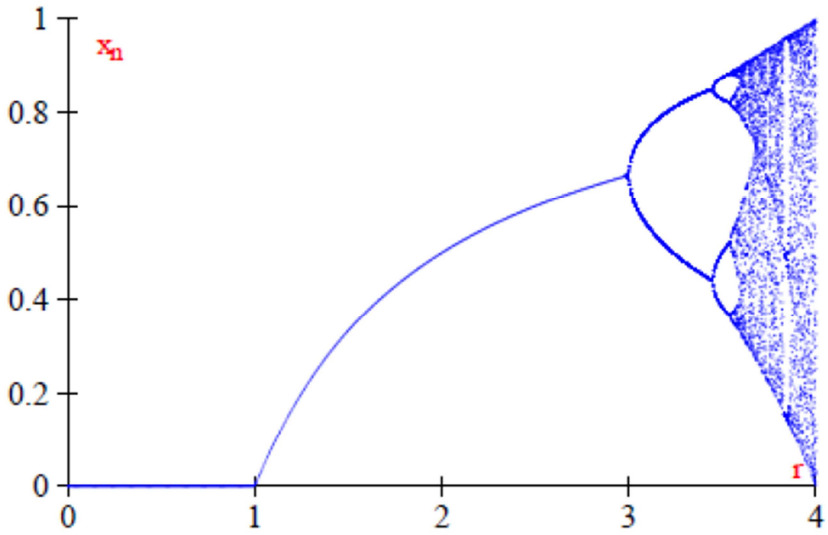

Figure IV.8 : Diagramme de bifurcation de la récurrence logistique dont l'axe horizontal porte les valeurs du paramètre μ (noté r), tandis que l'axe vertical montre les valeurs limites possibles.

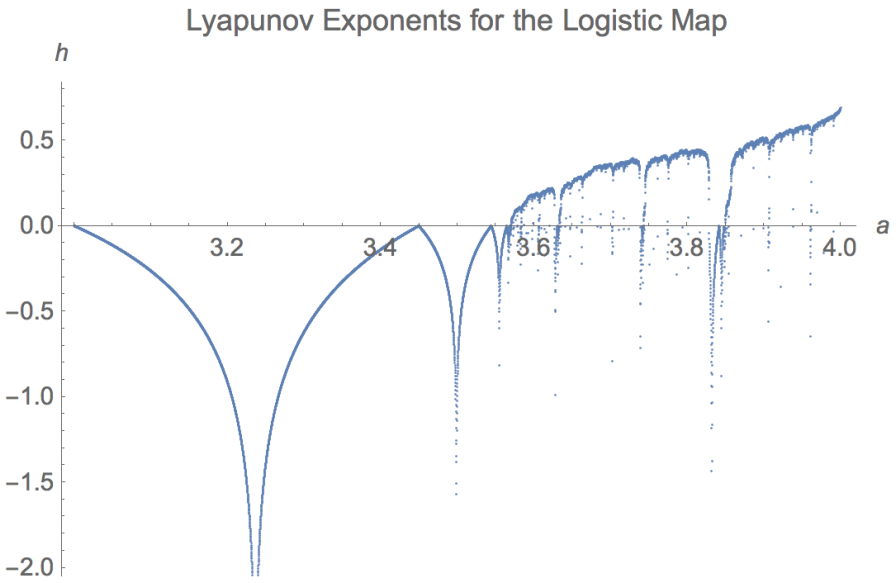

Figure IV.9 Lyapunov Exponent d'une carte logistique

IV.10.2. Carte Tent

L'une des fonctions les plus simples du chaos récemment étudiée pour les applications de cryptographie est la carte des tentes.**[IV.11]**

$$T(x) = \begin{cases} rx & x > 0.5 \\ r(1-x) & x < 0.5 \end{cases} \qquad \text{(IV.19)}$$

Définir une carte itérative par $x_{n+1} = T(x_n)$

La carte des tentes est construite à partir de deux lignes droites, ce qui simplifie l'analyse par rapport aux systèmes véritablement non linéaires.

Bien que la forme de la carte des tentes soit simple et que l'équation concernée soit linéaire, pour certains paramètres, ce système peut afficher un comportement très complexe et même des phénomènes chaotiques. Figues. 2 à 4 montrent la simulation de la carte des tentes. Les résultats de la simulation comprennent trois parties. Il est décrit comme suit : laissez la valeur initiale : x0 = 0.3, itération de la boucle = 30. Le paramètre r peut être divisé en trois segments, qui peuvent être examinés par des expériences dans les conditions suivantes :

- Lorsque r ∈ [0,1] comme le montre la Figure IV.11, les résultats du calcul prennent la même valeur après plusieurs itérations sans comportement chaotique.
- Lorsque r ∈ [1,1.4], le système apparaît périodicité, comme illustré à la Figure IV.12.
- Alors que r ∈ [1.4,2], il devient un système chaotique avec une périodicité disparue, comme le montre la Figure IV.13,

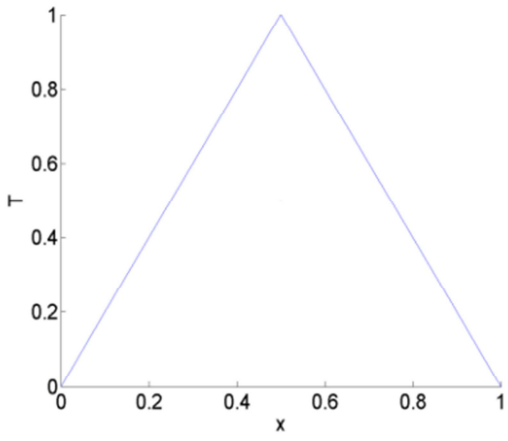

Figure IV.10 : la courbe d'une carte Tent

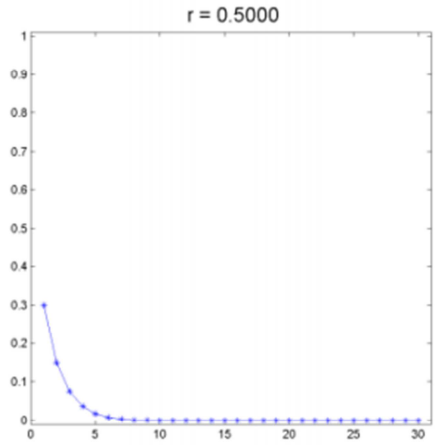

Figure IV.11 : propriété d'itération lorsque r=0.50

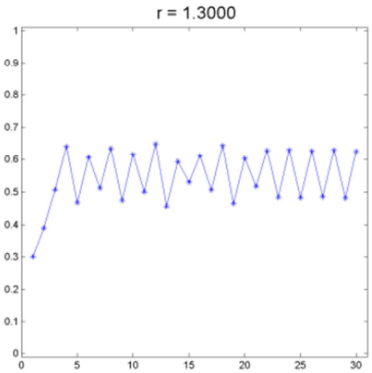

Figure IV.12 : propriété d'itération lorsque r=1.30

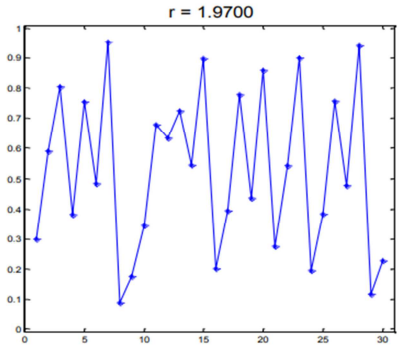

Figure IV.13 : propriété d'itération lorsque r=1.97

Le diagramme de bifurcation de la carte des tent, est illustré dans la Figure IV. 14.

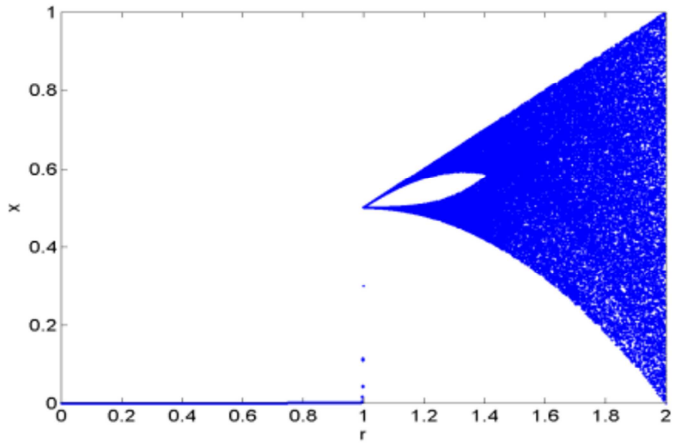

Figure IV.14 : le diagramme de bifurcation d'une carte Tent

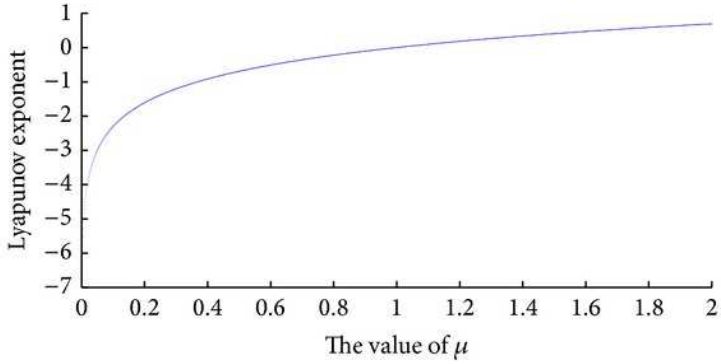

Figure IV.15 : Lyapunov Exponet d'une carte Tent

IV.10.3. Carte Sine

La récurrence sine d'une (01) dimension a pour représentation d'état :

$$x_{n+1} = \lambda \, sin(\pi x_n) \qquad \text{(IV.20)}$$

Avec $\lambda = 1$ le comportement chaotique est généré par une manière très similaire à la fonction logistique. Comme la récurrence logistique, la carte sine est quadratique au voisinage de $x = 0{,}5$. Elles ont une distribution probabiliste et une évolution vers le chaos par doublement de période presque identique. Les fenêtres se produisent périodiquement dans le même ordre. **[IV.10]**

Elle a le même nombre de Feigenbaum que la carte logistique. Malgré les similitudes, il existe quelques différences, l'exposant de Lyapounov est d'environ cinquante pour cent plus petit. Les bifurcations par doublement de période survenir plus tôt, et les fenêtres périodiques sont plus larges par rapport à la carte logistique.

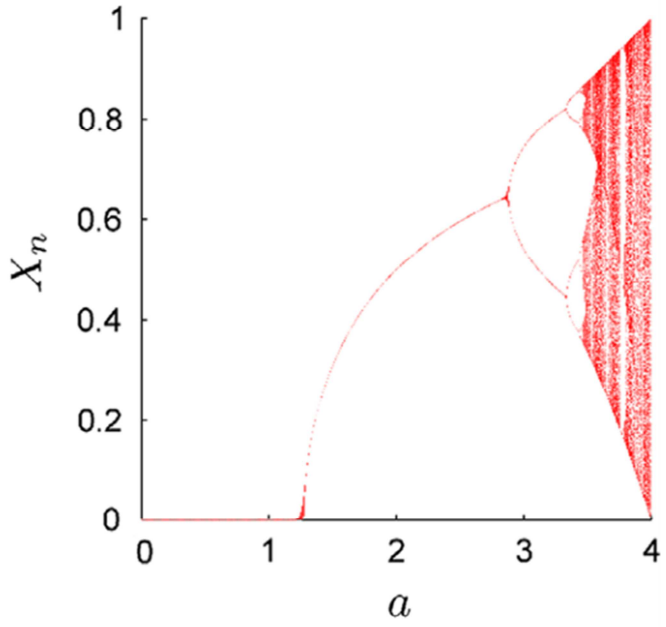

Figure IV.16 : Diagramme de bifurcation d'une carte sine.

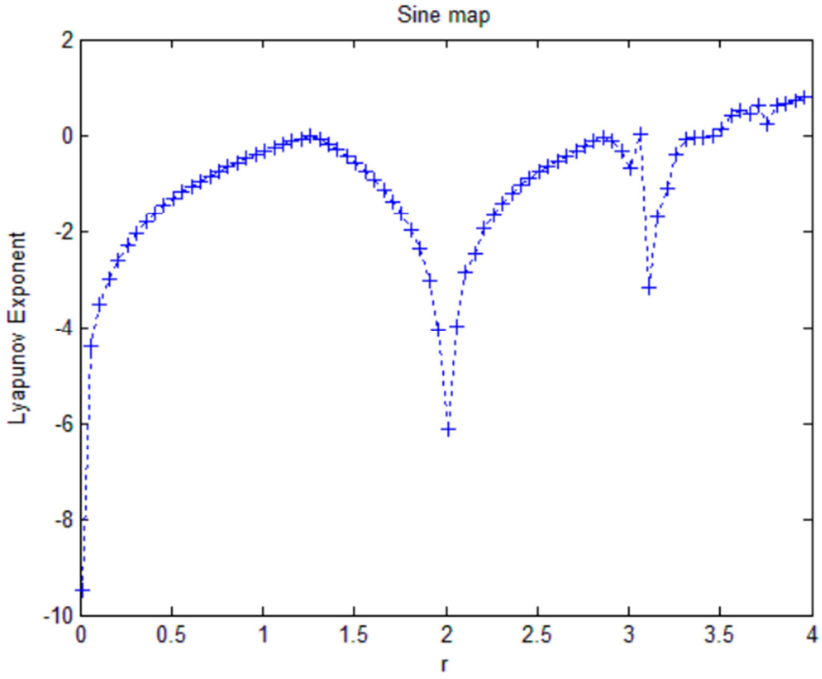

Figure IV.17 : Lyapunov Exponet d'une carte sine.

IV.11. Relation Entre Le Chaos Et Les Cryptosystèmes

Tout d'abord, nous notons qu'il y a une forte ressemblance entre les systèmes chaotiques et les cryptosystèmes symétriques à chiffrement par bloc. Pour commencer, un cryptosystème est dit bon s'il satisfera les trois caractéristiques suivantes :

- Transformation aléatoire des données nettes aux données chiffrées sans garder aucune information sur les données nettes,
- Soit fortement sensible aux données nettes de telle sorte qu'un plus petit changement dans les données nettes engendre des données chiffrées complètement différentes,
- Soit aussi fortement sensible à la clef de telle sorte qu'un plus petit changement dans la clef donne une naissance à des nouvelles données chiffrées complètement différentes.

Une autre caractéristique importante des cryptosystèmes symétriques et qu'ils utilisent quelques fonctions de chiffrage en mode itératif qui est une condition pratique pour certains cryptosystèmes populaires. **[IV. 2]**

En ce qui concerne les caractéristiques particulières des systèmes chaotiques, notons qu'un système chaotique est constitué de quelques fonctions de base f qui sont itérées sur un ensemble X. Le fonctionnement d'un tel système consiste à remplir les conditions suivantes :

- Soit un mélangeur, ceci signifie que l'ensemble X devrait être aléatoirement mélangé par la répétition de l'action de f,
- Soit sensible à l'état initial de telle sorte qu'une légère modification dans les états initiaux engendra des états complètement différents,
- Soit sensible aux certains paramètres de contrôle et un léger changement dans ces paramètres causera un changement dans les propriétés de la carte chaotique.

En comparant entres les particularités d'un cryptosystème et les caractéristiques d'un système chaotique, il est évident que le chiffrage et le chaos montrent des similarités remarquables, si nous considérons que les données nettes correspond à un état initial, la clef correspond à l'ensemble des paramètres, et la fonction de chiffrage correspond à la fonction de base f. Cependant, il y a une différence importante entre ces deux concepts. En fait, le cryptosystème travaille sur des ensembles finis (discrets), alors que le système chaotique est conçu pour travailler sur des ensembles infinis (continus). C'est probablement la raison principale pour laquelle la relation entre le chaos et le chiffrage a été restée inaperçue.

IV.12. Chiffrement par Chaos

La cryptographie basée sur le chaos est l'utilisation de la théorie du chaos dans les systèmes cryptographiques. Depuis les années 1980, l'idée d'utiliser des systèmes chaotiques pour concevoir des systèmes cryptographiques suscite de plus en plus d'attention. On peut le trouver dans l'article classique de Shanon sur la théorie des systèmes de confidentialité. Les bonnes propriétés dynamiques des systèmes chaotiques impliquent de bonnes propriétés cryptographiques des systèmes cryptographiques. De plus, la méthode de base pour conférer aux cryptosystèmes de bonnes propriétés cryptographiques implique un quasi-chaos. La théorie du chaos et la dynamique non linéaire ont été utilisées dans la conception de primitives cryptographiques, notamment des algorithmes de chiffrement d'images, des fonctions de hachage, des générateurs de

nombres pseudo-aléatoires sécurisés, des chiffrements de blocs, des chiffreurs de flux, des filigranes et des stéganographies. **[IV.9]**

Les primitives cryptographiques chaotiques sont généralement réalisées par la combinaison de deux opérations appelées confusion et diffusion, qui sont bien modélisées par la théorie du chaos. Les deux opérations sont effectuées à plusieurs reprises jusqu'à ce que le niveau de sécurité suffisant soit atteint. La qualité de la sécurité est testée par sa capacité à défendre différents attaques comprenant l'attaque en texte clair connue, l'attaque statistique, l'attaque différentielle, l'attaque par force brute, etc.

La plupart des algorithmes cryptographiques reposent sur l'utilisation de cartes chaotiques unimodales, leurs paramètres de contrôle et leurs conditions initiales comme clés. De nombreuses cartes chaotiques sont proposées dans la littérature et s'appliquent à la cryptographie de plusieurs manières.

IV.12.1. Cryptage par Addition

Cette méthode est la première chronologiquement à utiliser la synchronisation du chaos. L'idée repose sur l'observation des signaux chaotiques. Le principe est alors très simple : il suffit d'additionner directement le signal Informationnel (t) au signal chaotique Cx (t) et de le récupérer ensuite par synchronisation chaotique (voire Figure IV.18). Le même système est utilisé à la fois à l'émetteur et au récepteur, avec la différence que le récepteur est contrôlé par le signal émis pour obtenir la synchronisation. Au niveau du récepteur, après synchronisation grâce au signal reçu, on récupère le message original par une simple soustraction. Par conséquent, un intrus ne soupçonnera pas qu'un message est transmis, même s'il intercepte le signal $y(t)$ (porteuse chaotique plus le message), donc il ne cherchera pas à appliquer des techniques de décryptage**.[IV.12]**

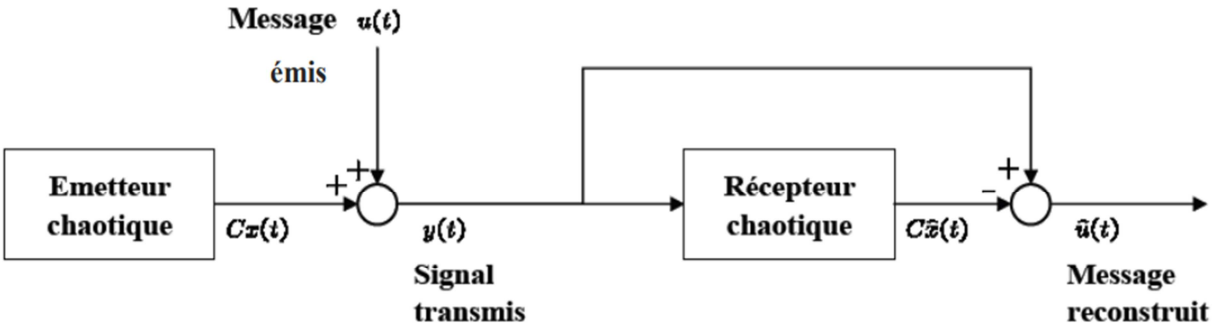

Figure IV.18 : Cryptage par addition

Le principal avantage de cette méthode réside dans la simplicité du cryptage. On peut souligner que cette technique peut être appliquée à des messages continus ou discrets. L'inconvénient de cette méthode est qu'afin de garantir la synchronisation le message doit être au moins de 20 à 30 dB inférieur à la sortie de l'émetteur. Toutefois, en présence d'un bruit de canal d'une puissance proche de celle du message, il devient difficile de détecter l'information. De plus, cette méthode reste sensible aux attaques extérieures, et l'usage du canal de transmission est inefficace du point de vue de l'énergie transmise par rapport à la qualité d'information fournie.

IV.12.2. Cryptage par Commutation

Cette méthode (en anglais Chaos Shift Keying, CSK) est utilisée pour transmettre un message binaire (voir Figure IV.19). L'émetteur est composé de deux systèmes chaotiques et pour chaque niveau de message m(t) (0 ou 1), l'un des systèmes envoie sa sortie sur la ligne de transmission. Ainsi, le signal transmis commute entre deux attracteurs étranges. Le récepteur est constitué de deux systèmes chaotiques identiques à ceux de l'émetteur. Pour chaque valeur du message, l'un des deux systèmes se synchronise avec l'émetteur et un bloc de comparaison permet de relever la valeur du message notée m0 (t).**[IV.13]**

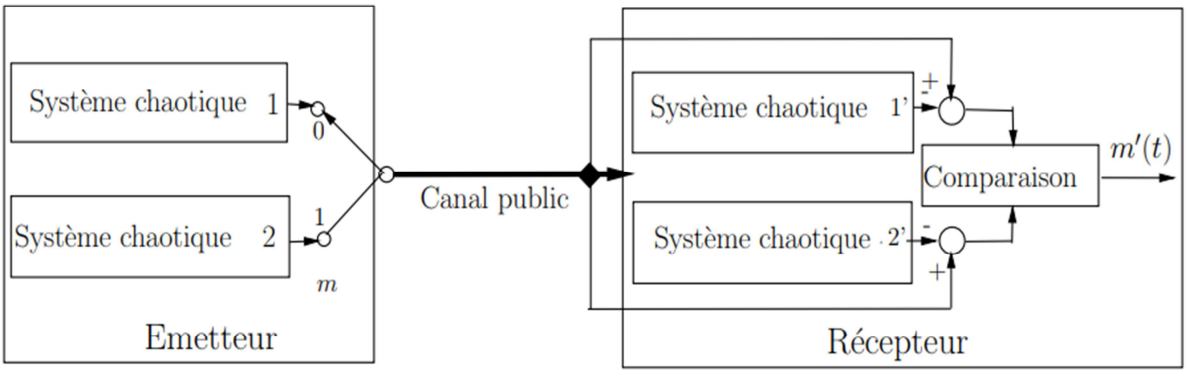

Figure IV.19 : Principe de cryptage par commutation.

IV.12.3. Cryptage par Modulation

Cette technique, utilise le message contenant l'information pour moduler un paramètre de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma correspondant est présenté à la Figure IV.20.

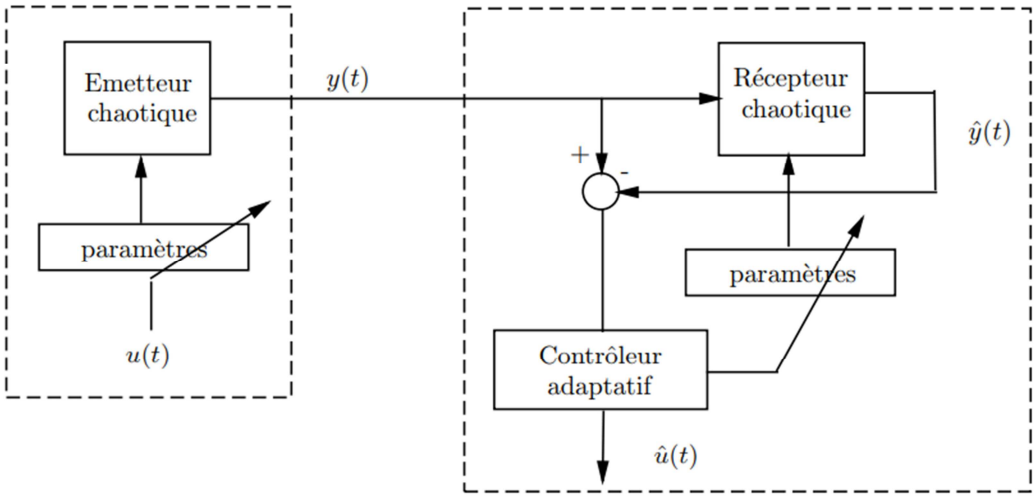

Figure IV.20 : Principe de cryptage par modulation

Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre(s) impose à la trajectoire de changer continûment d'attracteur, et de ce fait, le signal transmis est plus complexe qu'un signal chaotique "normal". Cependant, la façon d'injecter le message et

donc la fonction de modulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur. Il est important de souligner que cette technique exploite pleinement les qualités des systèmes chaotiques. Elle n'a pas d'équivalent parmi les systèmes de communication "classique". **[IV.13]**

IV.13. Conclusion

Pour conclure, les systèmes chaotiques sont des systèmes dynamiques qui évoluent dans une région bornée, qui possèdent une infinité de trajectoires non périodiques denses. Ils sont caractérisés par un comportement instable et non-linéaire, définit par une équation mathématique. Le comportement chaotique résulte de la grande sensibilité du système à l'état initial. Les formes d'onde chaotiques ont été largement utilisées dans divers domaines de recherche tels que la modulation de signaux et le cryptage chaotique de données de télécommunication

Chapitre V

Transmission des Images Médicales sur une Couche Physique OFDM Sécurisée

Chapitre V

Transmission des Images Médicales sur une Couche Physique OFDM Sécurisée

V.1. Introduction

Ces dernières années, la transmission d'images numériques sur Internet et sur les réseaux sans fil s'est développée rapidement, en raison des développements fascinants du traitement des images numériques et des communications en réseau. Il est nécessaire de protéger les informations d'image communiquées contre toute utilisation illégale, en particulier pour les personnes qui exigent l'enregistrement et la transmission de systèmes sécurisés fiables, rapides et robustes, telles que les bases de données d'images militaires, les vidéoconférences confidentielles, les systèmes d'imagerie médicale, les albums de photographies privées en ligne, etc. Cependant, la théorie des nombres ou des concepts algébriques basés sur des chiffrements traditionnels, tels que la norme DES (Data Encryption Standard), la norme AES (Advanced Encryption Standard), l'algorithme développé par Rivest, Shamir et Adleman (RSA), dont la plupart sont utilisées pour du texte ou des données binaires, ne semblent pas être idéales pour le cryptage d'images. En raison des images numériques qui sont généralement de très grande taille et volumineuses, le chiffrement de telles données volumineuses avec les chiffrements traditionnels entraîne une charge supplémentaire considérable, et est trop coûteux pour les applications en temps réel, qui nécessitent des opérations en temps

réel, telles que l'affichage, la découpe, la copie. , contrôle du débit binaire ou recompression. Dans une image numérique, les pixels adjacents ont souvent des valeurs d'échelle de gris similaires et des corrélations fortes, ou les blocs d'image ont des motifs similaires. Une telle redondance extrêmement élevée des images. **[V.1]**

Dans ce chapitre nous allons s'intéresser à la transmission des images médicales par la technique OFDM sécurisé basé sur le chaos, on utilisant une séquence d'embrouillage.

V.2. Cryptage d'image par chaos

Le cryptage d'image basé sur le chaos est devenu l'une des méthodes de cryptage efficaces et excellentes. En effet, les cartes chaotiques ont une sensibilité élevée à leurs valeurs initiales, à leurs paramètres de contrôle, à leurs propriétés chaotiques, à leur non-convergence et à leur ergodicité. Par conséquent, de nombreux algorithmes de chiffrement d'images chaotiques ont été développés en utilisant directement les cartes chaotiques existantes pour processus de chiffrement. En général, un algorithme de chiffrement d'image basé sur le chaos contient deux parties : un système chaotique et un chiffrement d'image. Les cartes chaotiques dans les algorithmes de cryptage d'image peuvent être divisées en deux catégories : une dimension (1D) et multi-dimension (MD). Les cartes chaotiques de MD ont de plus en plus d'applications en sécurité d'image en raison de leurs structures complexes et de leurs paramètres multiples. Cependant, plusieurs paramètres augmentent la difficulté de leur mise en œuvre matériel / logiciel et de la complexité de calcul. Les systèmes chaotiques 1D, en revanche, ont une structure simple et sont faciles à mettre en œuvre. Mais ils ont également trois problèmes, à savoir : (1) la gamme limitée ou / et discontinue de comportements chaotiques ; (2) la vulnérabilité à une analyse à faible coût de calcul à l'aide de fonctions d'itération et de corrélation ; et la distribution non uniforme des données des séquences chaotiques en sortie. Il est donc nécessaire de développer de nouveaux systèmes chaotiques offrant de meilleures performances chaotiques. **[V.2]**

V.3. Principe de sécurisation d'une chaine l'OFDM

Un système de communication basé sur la modulation OFDM avec une séquence chaotique est présenté à la figure V.1. Dans notre schéma, les parties réelle et imaginaire

des données de fréquence des signaux OFDM sont cryptées à l'aide d'une séquences d'embrouillage. La séquences de brouillage est produite à partir d'une carte chaotique lostique. Tous d'abord, les données d'image d'entrée (pixels) sont converties à des données binaire (vecteur ligne ou colone) en suite, ces données binaires doivent regroiper en symboles de données QPSK, puis subissent une transformation série-parallèle (S / P). Après cela, les parties réelle et imaginaire du signal de données sont multipliées par une séquence chaotique pour assurer la transmission de l'image.

Le récepteur peut récupérer le signal reçu car il peut obtenir suffisamment d'informations pour générer des séquences chaotiques identiques dans l'émetteur. Sans connaissance de la clé sécurisée, l'indiscret ne peut pas récupérer les informations de données à partir du signal reçu.

Dans cette section, la séquence de brouillage basée sur une carte chaotique est utilisée pour chiffrer les données d'image transmises. La séquence d'embrouillage peut être obtenues par un générateur de bits pseudo-aléatoire basé sur la carte chaotique utilisée. La description détaillée de chaque étape du processus de chiffrement et de déchiffrement proposé est donnée ci-dessous.

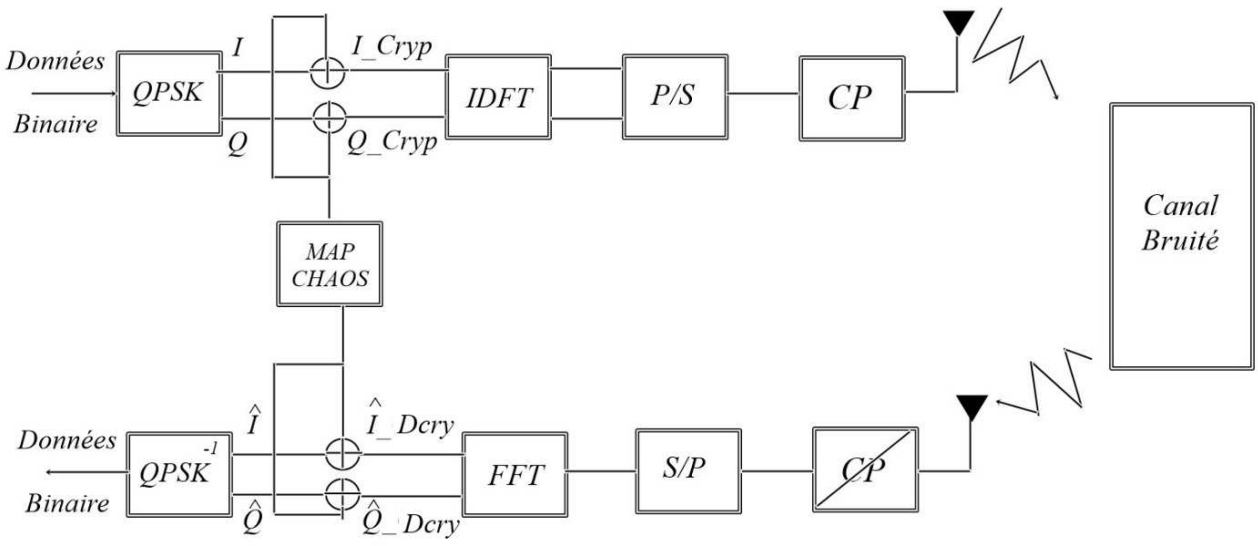

Figure V.1 : principe de sécurisation d'une chaine OFDM

V.4. La Procédure de Chiffrement d'Image

L'algorithme utilisé dans ce projet, basé sur le chaos dans le cadre d'une architecture de cryptage en flux. Il fournit une méthode de chiffrement et de déchiffrement d'une image médicale en respectant les conditions suivant :

- L'image sélectionnée doit être une image noir et blanc où les pixels sont représentés en niveau de gris.
- La taille d'image doit être égale à 256x256 pixels.

L'algorithme de chiffrement utilisé comprend deux grandes étapes : premièrement, la génération des séquences chaotiques par un générateur de flux pseudo-aléatoire contrôler par une carte chaotique, pour chiffrer les données réelles et imaginaires des symboles OFDM. Evidemment, toute cryptosystème admet une clef soit privée soit publique afin de chiffrer des données soit textuelle ou images, dans notre cas la clef est privée, elle se représente sous forme d'une paire regroupe la valeur initiale et le paramètre chaotique (r), cette paire n'est pas choisie arbitrairement, par contra elle sera choisie après une étude théorique précise (détailles par la suite) afin de déterminer les valeurs optimales pour obtenir une séquence chaotique. Une fois la clef est entrées par l'utilisateur une séquence chaotique (logistique) est générée. Deuxièmement, lorsque la clef est générée on peut masquer les données image à l'aide de cette séquence, la procédure de cryptage sera détalais étape par étape dans les sections suivante.

V.4.1. Génération de Séquence Chaotique

Les algorithmes de chiffrement d'images basés sur le chaos ont montré des performances supérieures. Les systèmes chaotiques ont de nombreuses propriétés importantes et la plupart des propriétés sont liées à certaines exigences telles que la confusion, la diffusion cryptographie **[V.1]** et la forte sensibilité aux conditions initiales ces propriétés pousse les chercheur vers la cryptographie chaotique.

L'image cryptée correspondante est formée en masquant ces données avec un flux de clé aléatoire généré à l'aide d'une carte chaotique de flux pseudo-aléatoire**. [V.3]**

Cette carte chaotique, dépend des valeurs de x_0 et le paramètre chaotique (a). Ces valeurs sont sécrétées et sont ensuite utilisées comme clé de chiffrement.

La carte chaotique est définit par une équation mathématique, génère également des séquences aléatoire fortement dépendantes de l'entrée (x_0, a) et utilisées pour masquer le flux de données de l'image en clair, une petite variation de cette valeur initial peut produit une séquence totalement défirent, par conséquent un échec de déchiffrement.

Il faut prendre en considération que les prévisions à court terme d'une carte chaotique peuvent être précises, mais les prévisions à long terme sont absolument impossibles, et cette prévision dépend du paramètre chaotique. Pour assurer une bonne confidentialité du système cryptographique on choisit la clef selon deux conditions :

- Le paramètre chaotique a, r ou μ doit inclue dans un intervalle où la prévision est complétement impossible, cette valeur est obtenue à l'aide d'un diagramme de Bifurcation.
- L'exposant de Lyapunov doit être positif, pour indique que le système dynamique est chaotique.

La section suivante est pour but de déterminer la clef optimale qui répond aux ces conditions, on utilisant le diagramme de Bifurcation et Lyapunov Exponents de chaque carte.

Pour ce schéma, une cartes logistique est utilisée, définit par l'équation V.1 **[V.4]**

$$x_{n+1} = a x_n (1 - x_n) \qquad \text{(V.1)}$$

L'équation (V.1) est une récurrence logistique simple dont elle n'est pas linéaire. Souvent citée comme exemple de la complexité, Elle conduit, suivant les valeurs de a, à une suite convergente, une suite soumise à oscillations ou une suite chaotique **[V.5].** Cette carte est souvent utilisée dans les cryptosystèmes, La Figure (V.2), présente le diagramme de bifurcation et de Lyapunov Exponent, obtenues par un code Matlab, de l'équation logistique qui justifie le choix du paramètre r = 3.9999

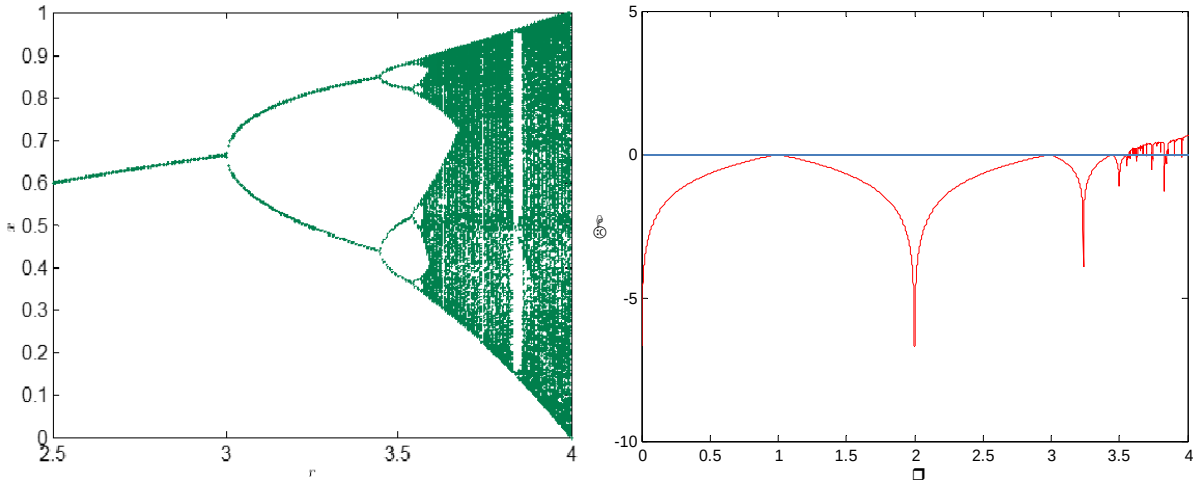

Figure V.2 : diagramme bifurcation (gauche) et Lyapunov exponent (droite) de la carte logistique (a noté r)

Lorsque la séquences d'embrouillage x(n) est préte, nous allons l'utilisée directement dans la cryptographie.

V.4.2. Cryptage d'image

Avant passé au chiffrement l'image originale doit être convertir en un flux de données binaire ces données doivent moduler par un modulateur de phase QPSK. Ensuite, les sémboles réstitué de la modulation sont converties en une séquence de symboles $S = [S(1)\ S(2)\ \dots\ S(m)]^T$

A l'aide d'un convertiseur série/parallele. Dans notre schéma, les parties réelle et imaginaire des données de fréquence sont d'abord cryptées par la séquence d'embrouillage. La partie réelle du vecteur de données S est cryptée par la séquence d'embrouillage x. La partie réelle chiffrée du signal Z peut être exprimée par :

$$Real\,(z(m)) = Real\,(S(m)) * x(m) \qquad \text{(V.2)}$$

De même façon, la partie imaginaire des signaux de données est à nouveau cryptée par la même séquence d'embrouillage x. La partie imaginaire cryptée de Z peut être exprimée sous la forme :

$$Im\,(z(m)) = Im\,(S(m)) * x(m) \qquad \text{(V.3)}$$

La séquence de données $z(m)$ est ensuite transmise par modulation IFFT pour générer le temps discret Z correspondant, qui peut être écrit sous la forme suivante **[V.5]**:

$$\boldsymbol{Z(n) = \frac{1}{N}\sum_{k=0}^{N-1} z(k) exp\left(\frac{j2\pi kn}{N}\right)} \quad \text{(V. 4)}$$

Après l'insertion d'un préfixe cyclique (CP) dans Z, le signal OFDM est transmis sur le canal sans fil.

Du côté du récepteur, le signal discret reçu r (n) peut être écrit comme suit :

$$r(n) = \hat{Z}(n) + w(n) \quad \text{(V.5)}$$

Après la suppression du CP, le signal reçu r (n) peut ensuite être transformé dans le domaine fréquentiel par l'unité FFT. La sortie FFT peut être représentée comme :

$$\boldsymbol{R(k) = \sum_{k=0}^{N-1} r(k) exp\left(\frac{-j2\pi kn}{N}\right), \quad 0 \leq k \leq N-1} \quad \text{(V. 6)}$$

$$\boldsymbol{R(k)} = \hat{z}(k) + W(k) \quad \text{(V.7)}$$

Où W(k) est le bruit gaussien complexe additif, produit à cause du canal de transmission. Enfin, les données restitués peuvent être déchiffrées par la séquence de brouillage a et b, après la séparation des parties réelles et imaginaires du signal reçu. Le signal résultant est converti en données d'image d'origine.

V.5. Résultats de Simulation

Cette partie est consacrée à la présentation des résultats de simulation sous Matlab, permettant d'illustrer les performances du système de chiffrement utilisé.

Pour assurer la fiabilité de notre système, quatre métriques seront testées, l'histogramme, mesure de PSNR et de BER, qualité d'image décrypté au niveau du récepteur

V.5.1. Analyse d'Histogramme

Le test d'un histogramme, tel qu'il est exprimé par V.8, est l'un des critères importants de l'analyse de sécurité. Il représente le nombre de pixels correspondant à chaque intensité

de couleur et la façon de distribution des pixels dans une image **[V.5].** Plus l'histogramme est uniforme, plus le système de cryptage des images est sécurisé.

$$x^2 = \sum_{k=1}^{256} \frac{(O_k - E_k)}{E_k} \qquad (V.8)$$

Où k est le nombre de niveaux de gris, O_k est la fréquence d'occurrence observée de chaque niveau de gris et E_k est la fréquence d'occurrence prévue de chaque niveau de gris.

L'analyse par histogramme est utilisée pour illustrer les propriétés de confusion et de diffusion supérieures de l'image cryptée **[V.2]**. L'image d'origine et l'image cryptée, ainsi que leurs histogrammes correspondants, sont respectivement illustrés aux figures (V.3)

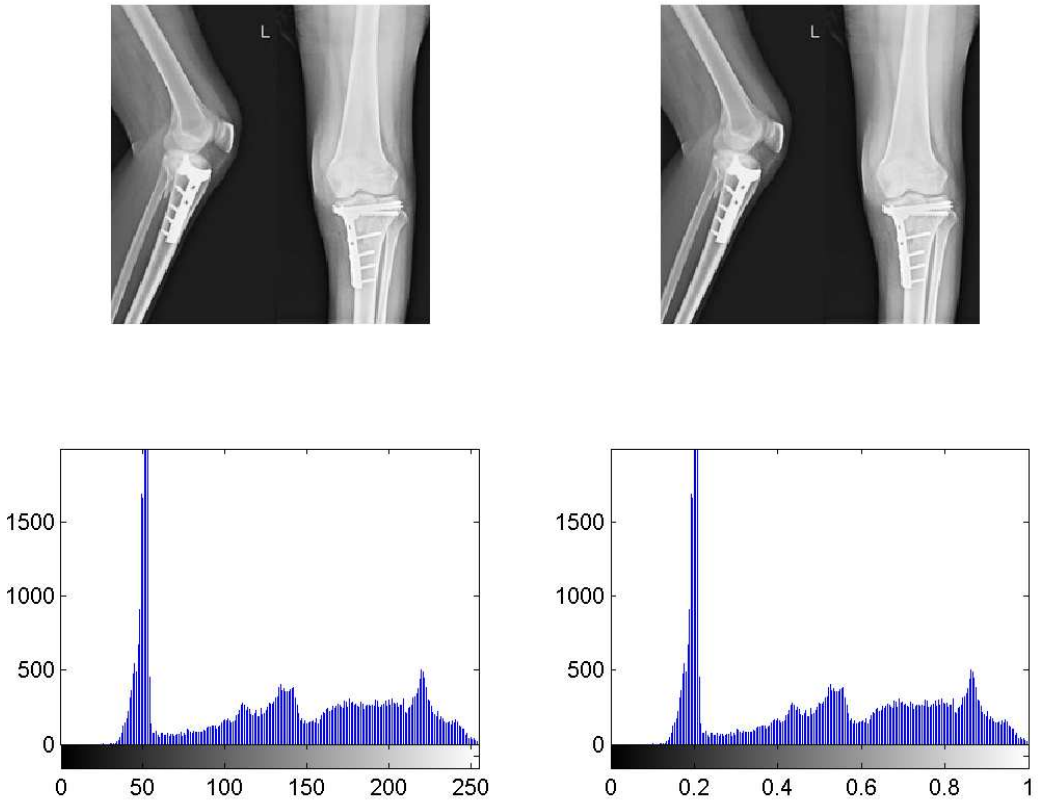

Figure V.3 : image médicale crypté par une carte logistique et son histogramme associer.

A partir des histogrammes de la Figure **(V.3)**, on remarque que l'image chiffrée a la même distribution des pixels de celui d'image originale. L'algorithme de chiffrement utilisé génère des séquences chaotiques positives quel que soit la clef utilisée et ces

éléments varient entre [0,1], cela montre le changement d'intensité des pixels dans l'image crypté. Mais ce résultat n'est pas suffisant pour sécuriser des données image.

Pour une bonne distribution des pixels d'image crypté, la carte chaotique utilisé doit génère des valeurs aléatoire non corrélés positif et négatif, une carte logistique modifiée peut être utilisé à la place de la carte logistique simple dans des applications cryptographique.

- **Carte Logistique Modifier**

La récurence proposée pour remplacer la carte logistique est définit dans l'itervale x_{n+1}: [0,2] → [−1,1] par l'équation (V.9) :

$$x_{n+1} = 1 - a{x_n}^2 \qquad \text{(V.9)}$$

Le diagramme de bifurcation et Lyapunov exponent d'une carte logistique modifiée, **[V.5]** illustré dans la Figure V.4.

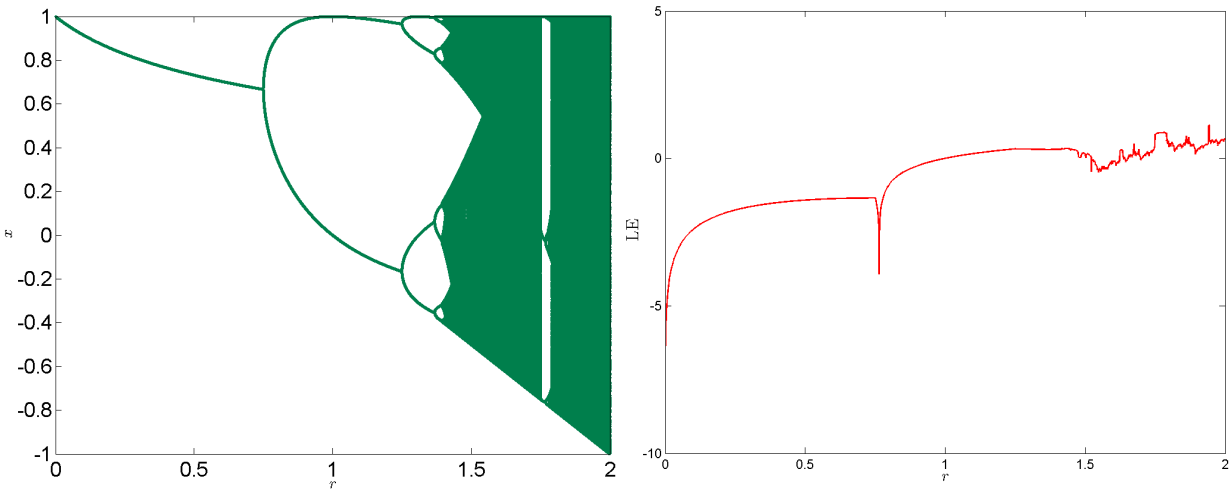

Figure V.4 : Le diagramme de bifurcation et Lyapunov exponent d'une carte logistique modifiée

En raison des propriétés de la carte modifié telles que la grande sensibilité aux conditions initiales et le paramètre chaotique, les séquences générées ont une bonne caractéristique aléatoire alors que la complexité de ce processus est relativement faible. La FigureV.4 montre le digramme de bifurcation, où le signe des valeurs de sortie alterne aléatoirement entre le positif et le négatif, cela permette de mieux distribuer les pixels de l'image originale au cours de chiffrement. Les résultats d'utilisation de cette carte dans notre système sont montrés dans la Figure V.5.

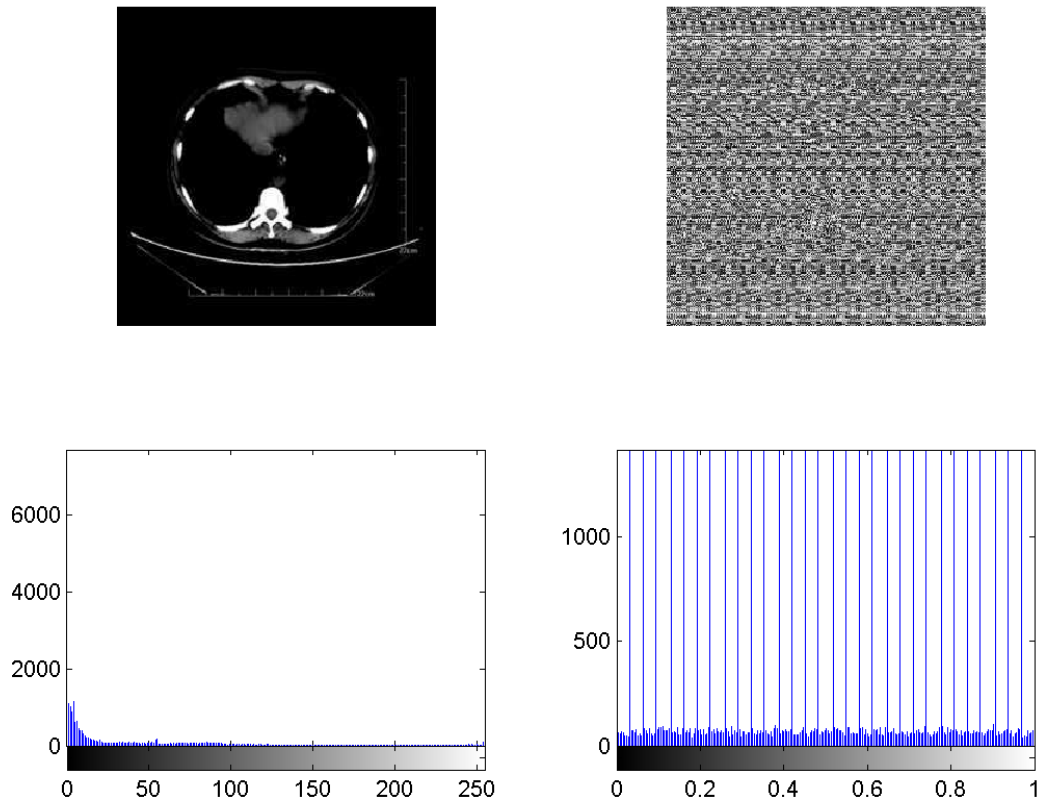

Figure V.5 : l'image crypté et décrypté par carte logistique modifié et son histogramme.

L'histogramme de l'image originale (Fig. V.5 (gauche)) est clairement démontré qu'il est doté d'un histogramme très incliné. L'histogramme de l'image chiffrée (Figure. V.5 (droite)) devient assez gros est presque uniforme. Ainsi, le schéma crypté proposé est efficace.

V.5.2. Analyse de Qualité par Vision

L'analyse par histogramme des images originale et chiffrées est très importante, mais n'est pas suffisante. Une autre métrique testée pour assurer la confidentialité du système, on parle de la qualité de vision (d'image).

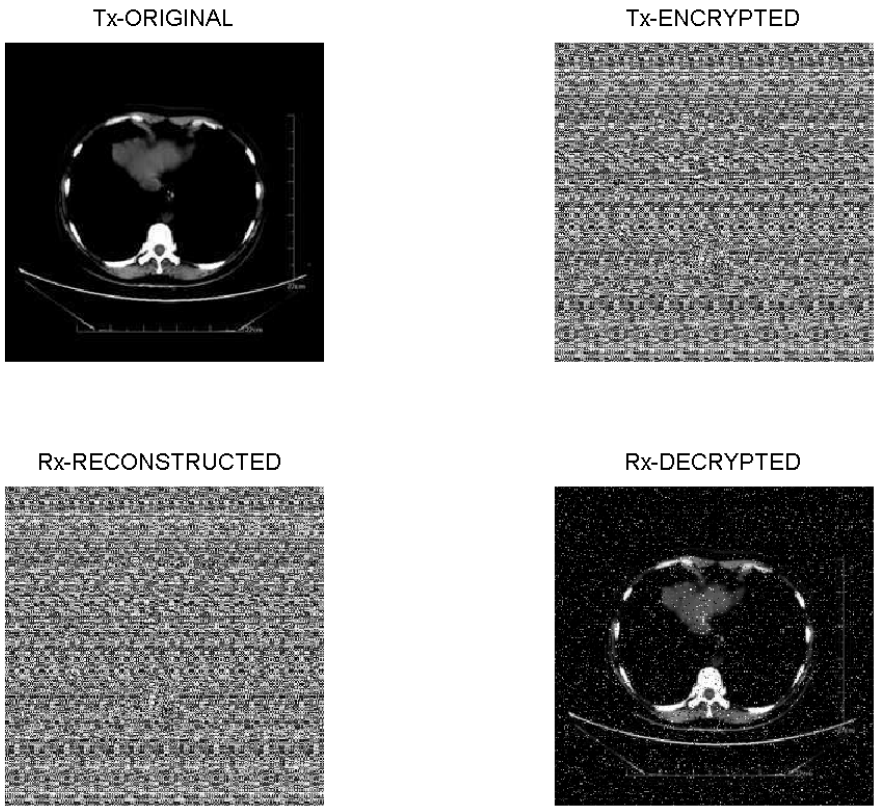

Figure V.6 : représentation d'image médicale au niveau d'émetteur (originale et crypté) au niveau de récepteur (reçus et décryptage)

La Figure V.6 représente les différentes images restituent au cours de la transmission, les deux premiers sont récupérés au niveau d'émetteur, les deux derniers au niveau de récepteur, d'après la Figure en observe que l'image décrypté n'est pas de bonne qualité à cause de bruit de canal et l'effet du séquences chaotiques utilisé dans le chiffrement.

Comme on a dit précédemment l'image chiffrée obtenue par un simple produit entre les symboles QPSK et les séquences chaotiques, ses éléments varient entre -1 et 1 avec une précision élevé, cela crée un bruit important additionne avec le bruit de canal, pour récupérer l'image avec une bonne qualité il faut augmenter la puissance de signale de sortie par conséquent augmenter La valeur du SNR.

$$SNR = \frac{Puissance\ du\ signal}{bruit} \qquad (V.10)$$

Malheureusement, cette solution n'est pas sympathique dans les systèmes de télécommunications et surtout dans les applications des réseaux de capteurs, à cause de leur limitation énergétique. Dons la section suivante une des solutions optimale de ce problème est proposé.

V.5.3. Analyse de PSNR

Tous d'abord, il faut connaitre que tout traitement appliqué à une image peut entraîner une perte importante d'informations ou de qualité. Les performances de récupération sont évaluées à l'aide de la mesure objective standard PSNR (rapport signal / bruit de crête). Le PSNR est généralement adopté comme métrique de performance dans un système de transmission. Plus le PSNR de l'image est élevé, meilleure est la qualité **[V.6]**. Le PSNR mesuré entre l'image original I_{Orige}et l'image décrypté $I_{décry}$est défini par :

$$PSNR(I_{Orige}, I_{décry}) = 10log_{10}\left(\frac{255^2}{MSE(I_{Orige}, I_{décry})}\right) \qquad (V.11)$$

Avec

$$MSE(I_{orige}, I_{décry}) = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(I_{Orige_{ij}} - I_{décry_{ij}})^2 \qquad (V.12)$$

Où M, N sont les dimensions de l'image originale.

La valeur PSNR se rapproche de l'infini lorsque la MSE approche de zéro. Cela montre qu'une valeur PSNR supérieure fournit une qualité d'image supérieure. À l'autre bout de l'échelle, une petite valeur du PSNR implique de grandes différences numériques entre les images. La figure (V.7) représente la courbe du PSNR associé à notre système cryptographique.

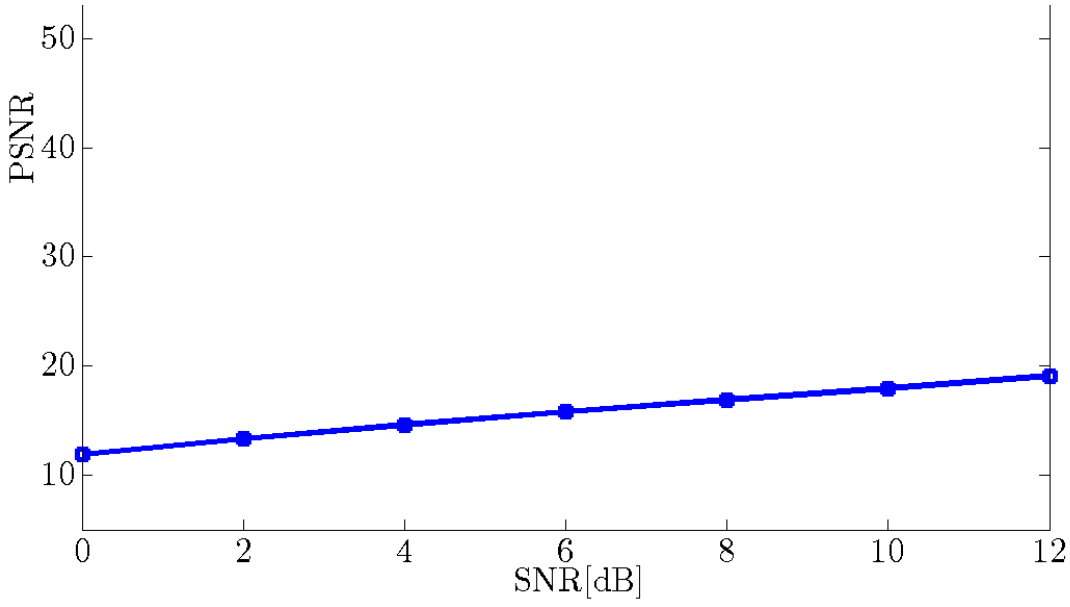

Figure V.7 : PSNR de notre système

Afin de récupéré une image de qualité raisonnable dans un système de transmission sans fils, il faut avoir au moins un PSNR de 40, mais d'après la Figure V.7 en remarque que cette valeur ne dépasse pas 20 c'est pour ça la qualité d'image décrypté est faible.
L'une des solutions les plus optimale et simple pour augmenter la qualité d'image est d'appliquer une fonction signe, sgn (), sur la séquence chaotique pour chiffrer les parties réelles et imaginaires du signal QPSK.

$$a(n) = \text{sgn}(x(n)) ;$$

Par conséquent la séquence d'embrouillage produit a contienne que des signe positif et négatif {−1, 1}. Les figures V.8 et V.9 montre les résultats associer à cette modification.

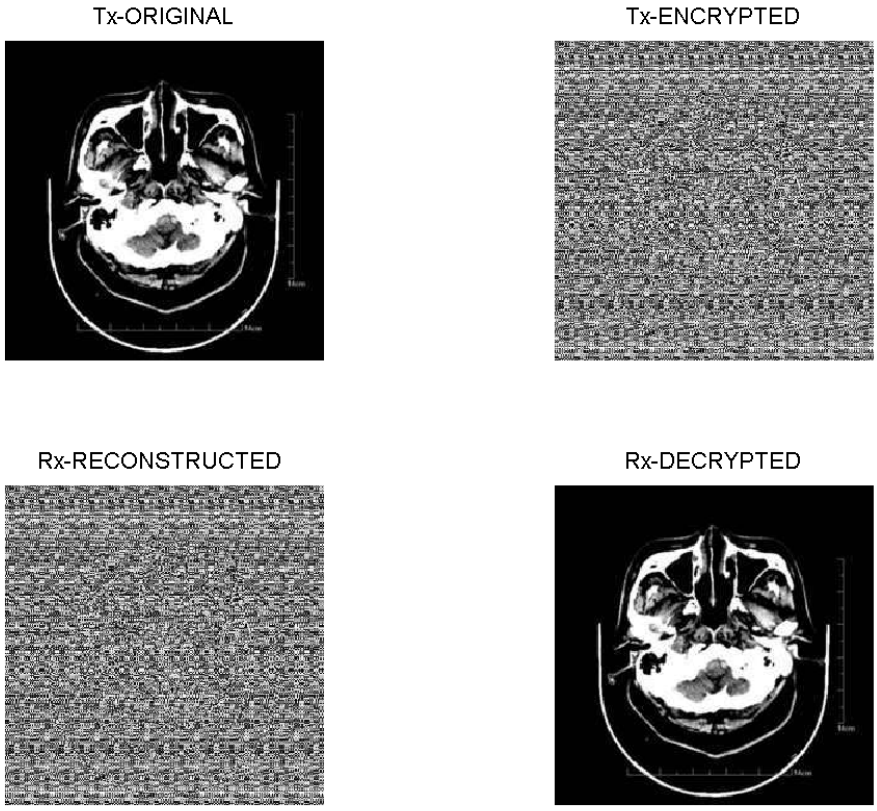

Figure V.8 : l'effet de la carte logistique modifié à la qualité d'image au niveau de récepteur

D'après la Figure V.8, l'utilisation de la fonction sgn() offre des résultats acceptable pour diminue le bruit et décrypté l'image corecctement.

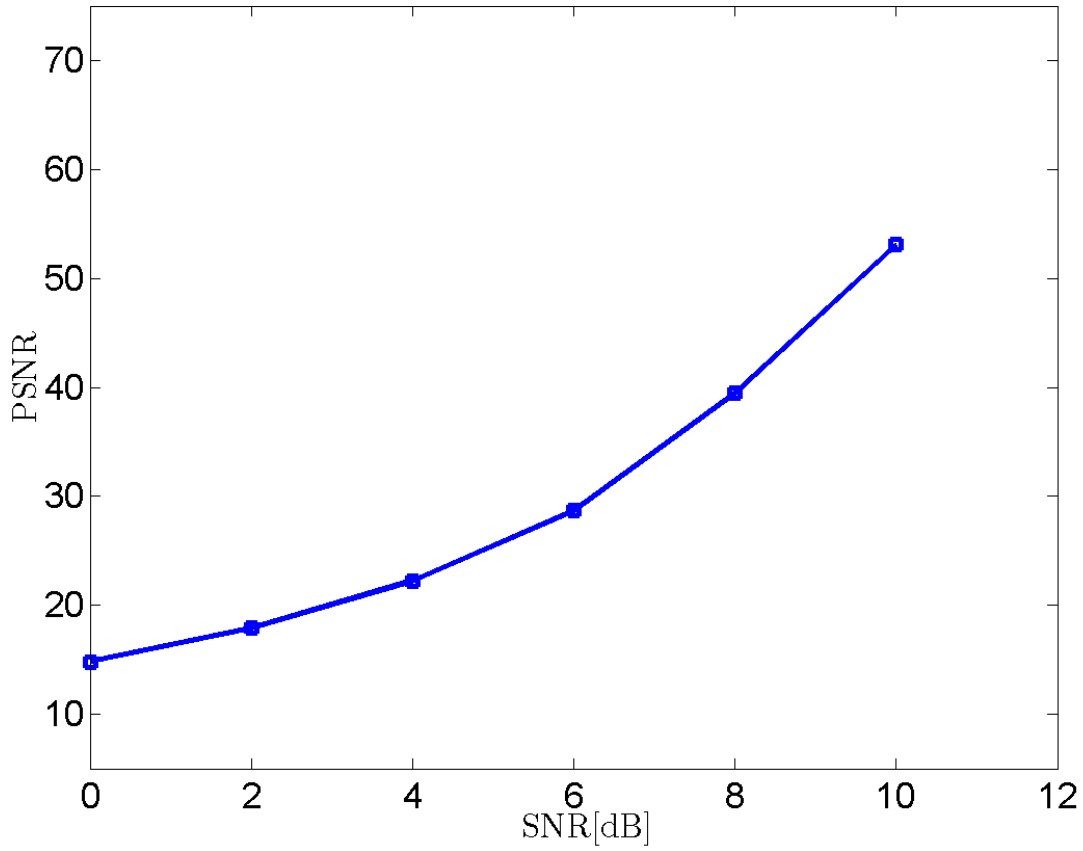

Figure V.9 : l'effet de l'utilisation de la fonction sgn() sur le PSNR

D'après la figure V.9, le PSNR dépasse les 50, cela est largement suffisent pour récupérer une image de bonne qualité avec une puissance acceptable (10 dB)

V.5.4. Analyse de BER

Les phénomènes parasites (bruit) perturbent le canal de transmission et peuvent affecter les informations en modifiant un ou plusieurs bits du message transmis, introduisant ainsi des erreurs dans l'image crypté. On appelle taux d'erreur binaire le rapport du nombre de bits reçus en erreur au nombre de bits total transmis.

$$Te = Nombre\ de\ bits\ en\ erreur\ /\ Nombre\ de\ bits\ transmis$$

Parmis les métrique utilisé pour tester la fiabilité d'un système cryptographique, le mesure de taux d'erreur binaire, au niveau de récepteur. La figure V.10 illustre les la valeur de BER des systèmes simulés en présence de bruit AWG.

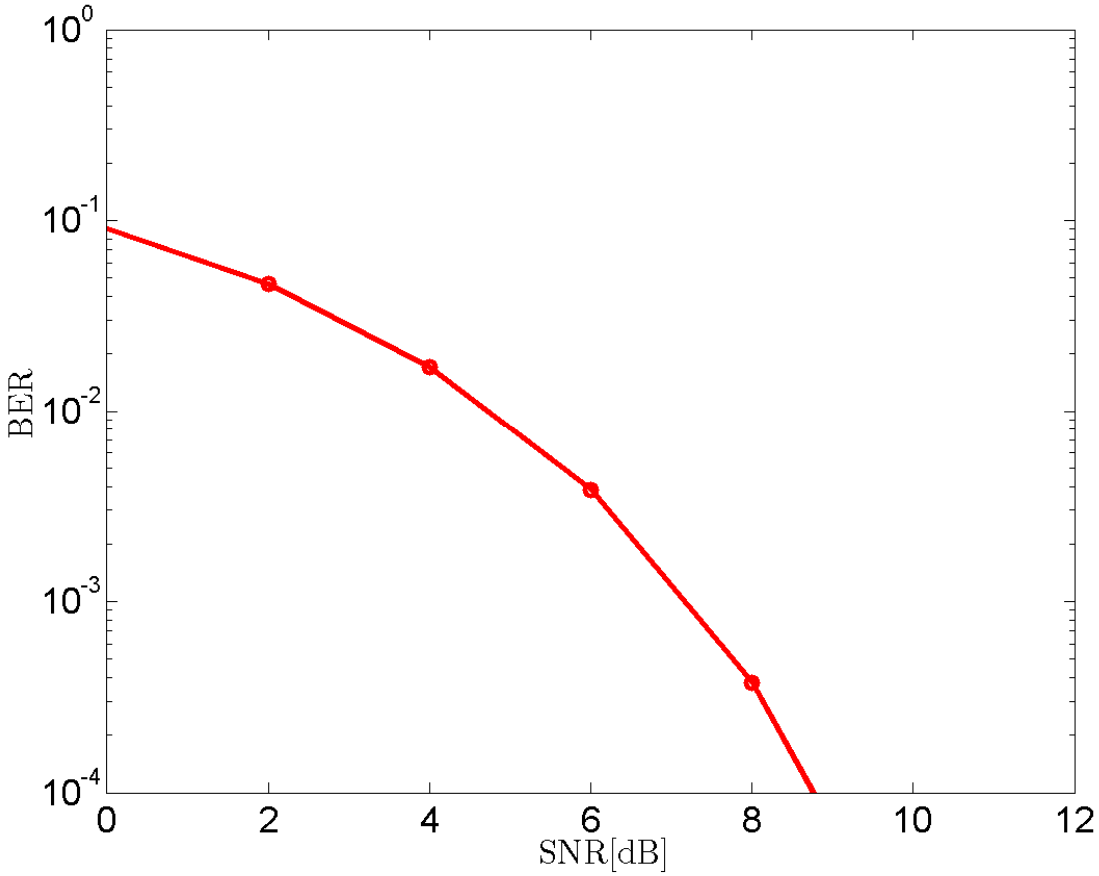

Figure V.10 : l'effet de l'utilisation de la fonction sgn() sur le BER

Dans un système cryptographique fiable, la courbe du BER diminue, à cause de la réduction des erreurs lorsque l'image est décrypté d'une façon correcte, cela est très remarquable dans la Figure V.10

V.5.5. Sensibilité à la clef

La sensibilité des clés est l'un des critères importants des algorithmes de chiffrement d'image. Elle est caractérisée par un petit changement dans la clé qui donne une naissance à des nouvelles données chiffrées complètement différentes **[V.7]**. La sensibilité des clés peut être observée sous deux aspects :

(i) si des clés légèrement différentes sont appliquées pour chiffrer les images identiques, des images de chiffrement complètement différentes doivent alors être produites ;

(ii) si une différence minime existe dans la clé de déchiffrement, l'image chiffrée ne peut pas être déchiffrée correctement.

Dans ce projet nous allons appliquer le deuxième aspect, Afin de mesurer cet élément dans le schéma proposé

La clef (a, x_0)utilisée dans le chiffrement :

$$\begin{cases} x_0 = 0.655124569745628 \\ a = 2 \end{cases}$$

La clef (a, x_0)utilisée dans le chiffrement :

$$\begin{cases} x_0 = 0.655124569745627 \\ a = 2 \end{cases}$$

Les résultats obtenus sont montrées dans la Figure V.11

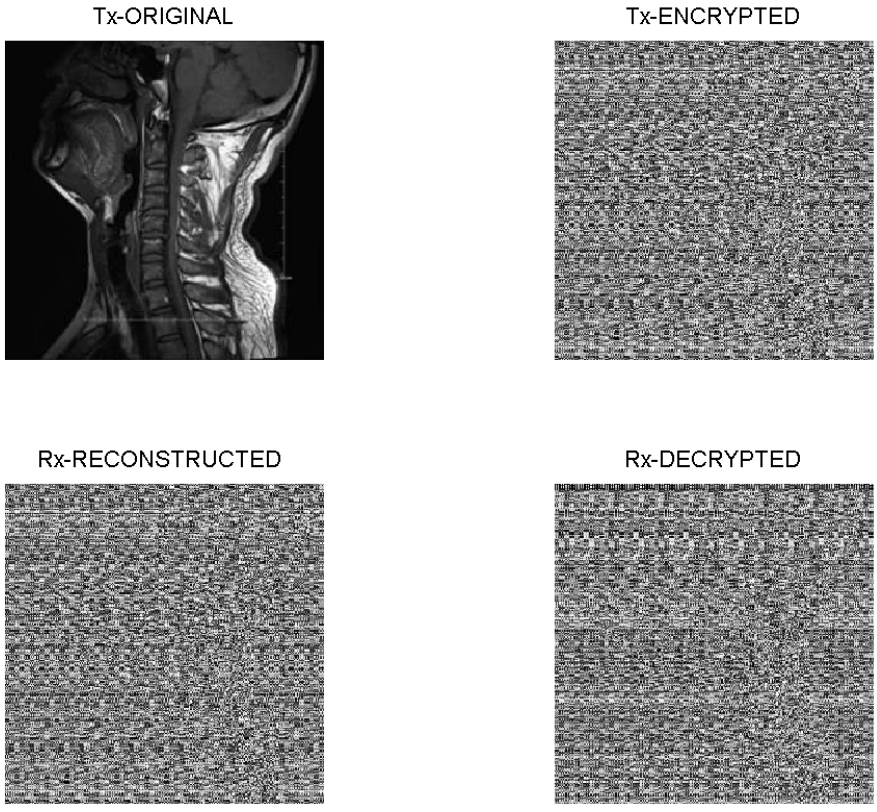

Figure V.11 : image crypté et décrypté par des clefs différent (variation dans le les conditions initiale x_0)

Il est clairement observé qu'une petite variation dans les conditions initiales entraînait un changement significatif dans la séquence de décryptage, par conséquent un échec décryptage. Le deuxième changement touche le paramètre de contrôle a, l'image décryptée avec cette clef est illustrée à la figure V.12

La clef (a, x_0)utilisée dans le chiffrement :

$$\begin{cases} x_0 = 0.655124569745628 \\ a = 2 \end{cases}$$

La clef (a, x_0)utilisée dans le chiffrement :

$$\begin{cases} x_0 = 0.655124569745628 \\ a = 1 \end{cases}$$

Les résultats obtenus sont montrées dans la Figure V.12

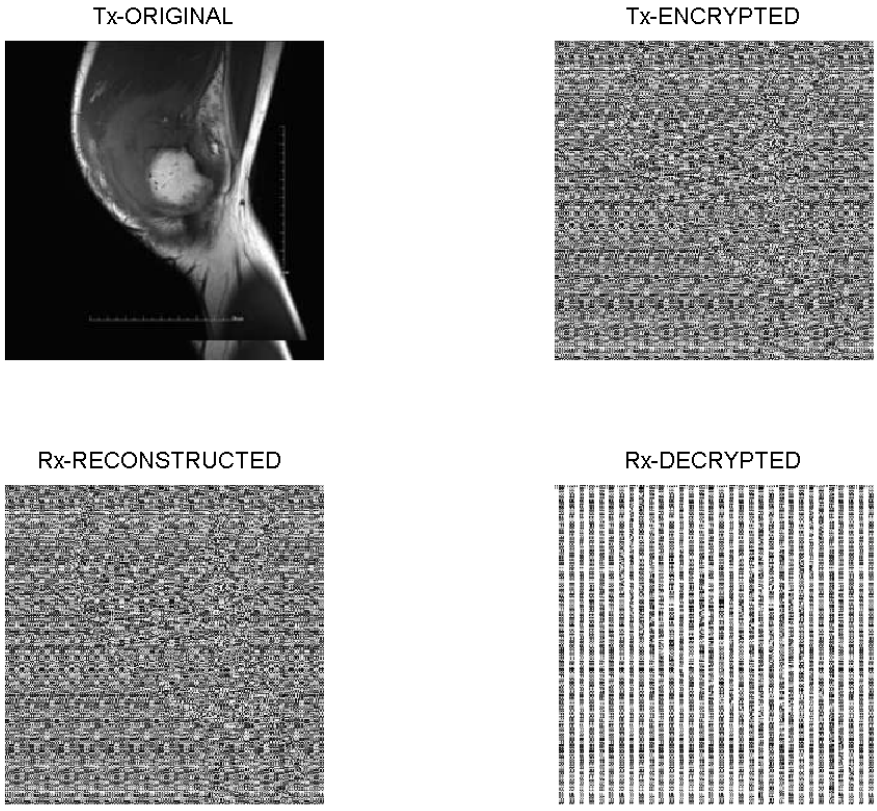

Figure V.12 : image crypté et décrypté par des clefs différente (variation dans le paramètre chaotique).

Lorsqu'on modifie la valeur du paramètre chaotique correspondante à la clef de déchiffrement, une séquence chaotique totalement différente est générée pour déchiffrée l'image réceptrice,

Les deux figures V.13 V.14 montrent l'effet de variation des clefs à la valeur du PSNR et BER,

Dans le schéma utilisé, plus la qualité visuelle de l'image chiffrée est élevée, plus la valeur de PSNR sera grande, mais lorsqu'en utilise une clef de déchiffrement modifié de celle du chiffrement la valeur du PSNR reste nulle quel que soit la puissance du signal émis, comme illustre la Figure V.13

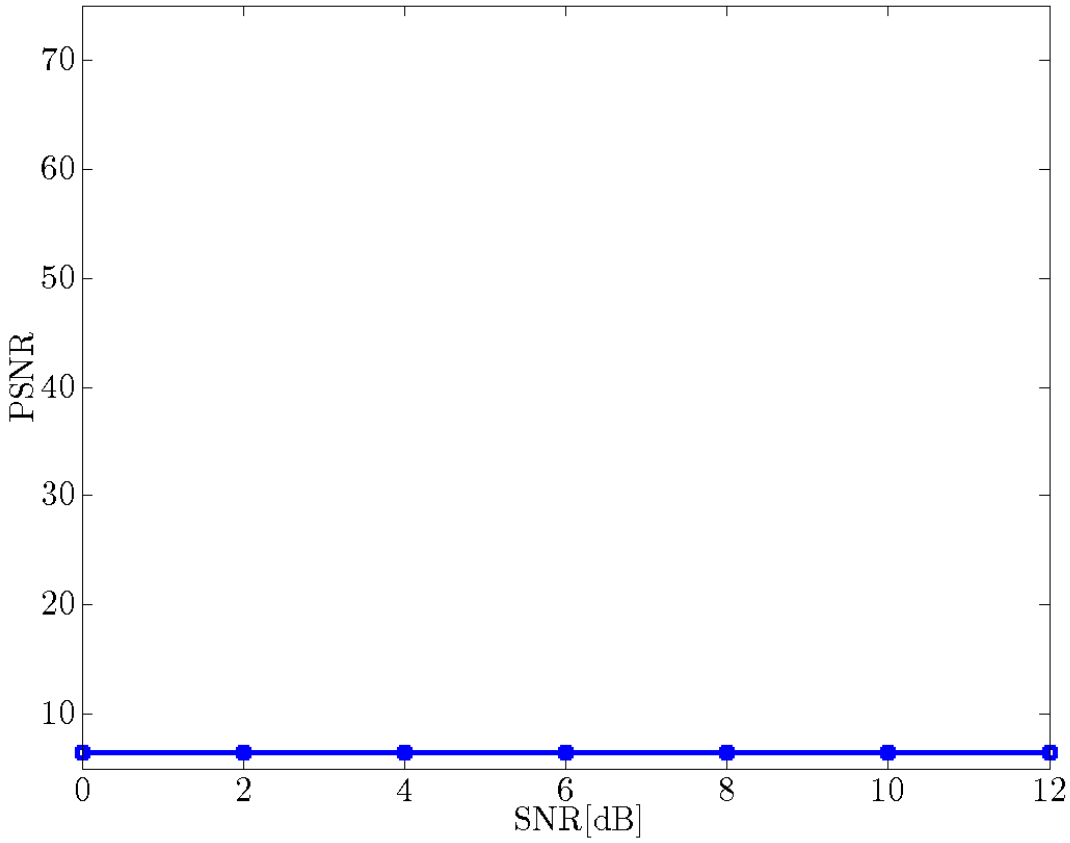

Figure V.13 : PSNR d'un cryptosystème à clefs différent.

Lorsque le PSNR reste nulle, ceci indique qu'il y a une grande différence entre l'image originale et décrypté, et le processus de décryptage n'est pas appliqué correctement à cause du changement des clefs. Malgré que la variation de clef de déchiffrement est très

petite (10^{-15}) par rapport à la clef de chiffrement, mais cela produit une clef totalement déférente.

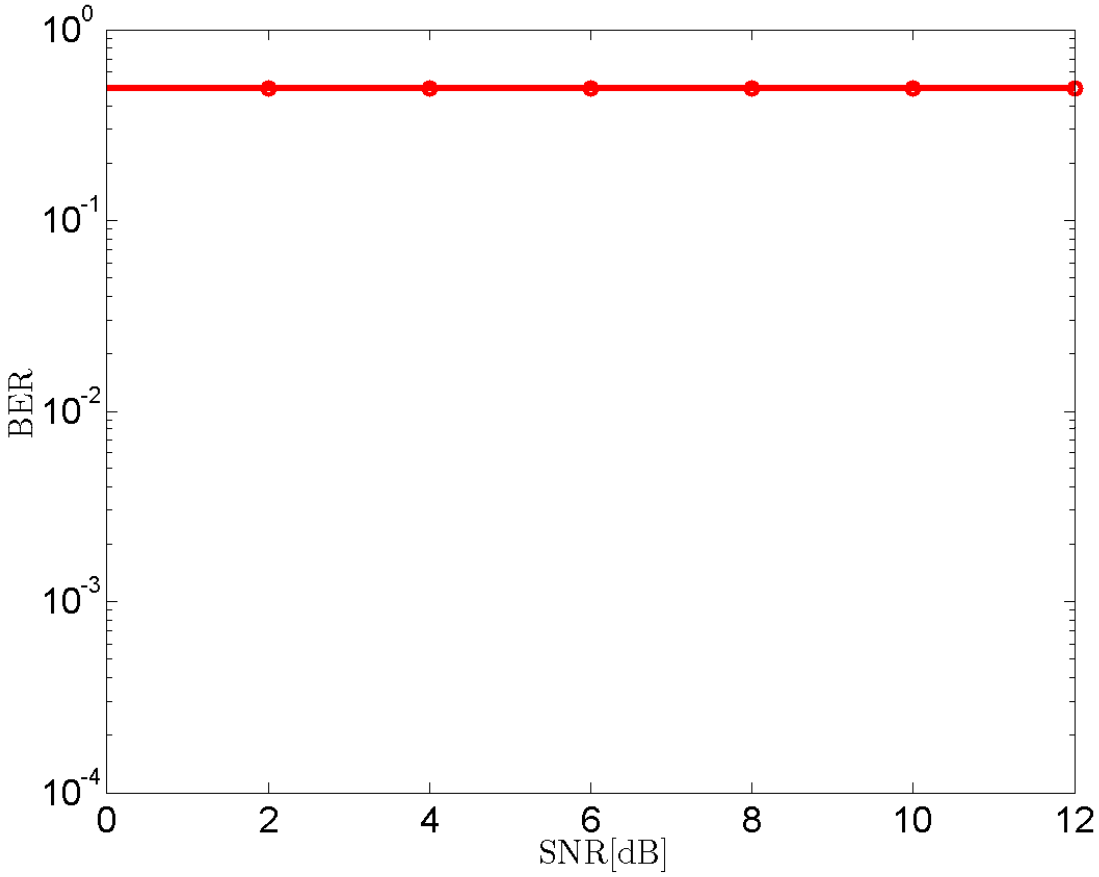

Figure V.14 : BER d'un cryptosystème à clefs différent.

La petites variation des clefs de chiffrement dans notre système résulte un BER constant pour quel que soit la puissance du signal, cela indique que le nombre des erreurs entre les pixels originaux et crypté reste constant.

V.6. Conclusion

En conclusion, cette étude a présenté un schéma de transmission d'image médicale sécurisée dans un réseau de capteurs sans fil basé sur le chaos par la technique OFDM avec une séquence d'embrouillage générer à base d'une carte chaotique, le choix de la carte utilisée dans notre système n'est pas arbitraire par contre il faut choisir une carte

utile et efficace pour masquer les données images, prenant comme titre d'exemple la carte logistique modifier.

Le chiffrement de la couche physique peut améliorer efficacement la sécurité de la transmission d'images. Les résultats de la simulation vérifient que la séquence de brouillage de la carte logistique modifié peut conduire à une transmission sécurisée des images dans la couche physique.

De plus, dans notre projet, la carte logistique modifier a été utilisé pour réduire le bruit et améliorer les performances de BER du système, ce que confirment les résultats de la simulation. Ainsi, le schéma étudié et testé peut améliorer efficacement la transmission d'images sécurisée pour les réseaux de capteur sans fils basés sur technique OFDM.

Conclusion Générales

Conclusion Générale

Ce manuscrit a pour principaux objectifs, d'une part l'étude des réseaux de capteurs multimédia (WMSNs : Wireless Multimedia Sensor Networks), et d'autre part l'évaluation des performances de la couche physique OFDM dans un contexte de sécurisation avec des carte chaotiques.

Ces dernières années marquent un tournant vers les chaos dans les activités de recherche sur la cryptographie des données. Désormais, les crypto-systèmes basés sur des approches chaotiques. La cryptographie chaotique se présente donc comme une technologie attractive pour la sécurisation de la couche physique dans les WMSNs.

Le premier chapitre consiste à une étude globale sur les réseaux de capteurs on citant sa grande caractéristique telle que la faible consommation énergétique, faible puissance de calcul…

Nous nous somme s'intéressés dans le second chapitre à l'étude des performances de modulation OFDM (principe de modulation, implémentation numérique, chaine de transmission, ses avantages et inconvénients, domaine d'application…)

Le troisième chapitre s'est attaché à présenter les différents algorithmes de chiffrement classique et moderne, avec quelque algorithme de cryptage d'image.

Le quatrième chapitre nous avons évoqué d'abord quelques notions en temps continu ou en temps discret. Par la suite, soient nous nous sommes intéressés à une classe particulière de systèmes non linéaires qui sont dits chaotiques.

Dans le chapitre cinq, les performances de la couche physique OFDM en combinaison avec la technique de cryptage chaotique obtenues par simulations ont été étudiés. En a montré l'efficacité de la méthode proposée en transmission sécurisée à travers plusieurs métriques et pour différentes images médicales.

Références Bibliographiques

Références Bibliographiques

[I.1] Wassim Drira, Chakib Bekara, Maryline Laurent « Sécurité dans les réseaux de capteurs sans fil : conception et implémentation », Rapport de recherche, Institut Mines-Télécom-Télécom SudParis-CNRS). 2008, pp.55

[I.2] Cristian Duran-Faundez. « Transmission d'images sur les réseaux de capteurs sans fil sous la contrainte de l'énergie. Réseaux et télécommunications ». Université Henri Poincaré - Nancy I, 2009. Français

[I.3] FARES Abdelfatah « développement d'une bibliothèque de capteur », rapport de recherche, université Montpellier 2, 2008

[I.4] Youssouf Zatout. « Conception et évaluation de performances d'un réseau de capteurs sans fil hétérogène pour une application domotique. » Université Toulouse le Mirail - Toulouse II, 2011. Français.

[I.5] Lyes KHELLADI & Nadjib BADACHE « Les réseaux de capteurs : état de l'art ».rapport de recherche, université USTHB, 2004.

[I.6] Cédric Demoulin, Marc Van Droogen broeck « David Martins, Hervé Guyennet. État de l'art - Sécurité dans les réseaux de capteurs sans fil. », 2008 : 3rd conference on Security of Network Architectures and Information Systems, 2008, France..

[I.7] HALLALI Nabila, MEKHNACHE Salima, « simulation du routage dans les réseaux de capteurs sans fils » mémoire master, université de Bejaia, 2017

[I.8] Leila Makkaoui. Compression d'images dans les réseaux de capteurs sans fil. Réseaux et télécommunications, Université de Lorraine, 2012. Français

[I.9] John G.Van Bosse, Fabrizio U. Devetak "signaling in Telecommunication networks". Edition Wiley, 2nd Edition 2006

[I.10] Cristian Duran-Faundez. « Transmission d'images sur les réseaux de capteurs sans fil sous la contrainte de l'énergie ». Réseaux et télécommunications [cs.NI]. Université Henri Poincaré - Nancy I, 2009. Français. <tel-00417505>

[II.1] Helmi BEN HNIA, Abdennaceur KACHOURI, Ossama BEN BELGHITH, Lotfi KAMOUN « Etude des performances de la modulation OFDM pour l'utilisation dans les systèmes de communication sans fils de la 4G » Laboratoire d'Electronique et des Technologies de l'information (L.E.T.I), March 15-20, 2004 – TUNISIA

[II.2] SAMI AGREBI, « implémentation FPGA d'une FFT à base d'arithmétique logarithmique pour les systèmes OFDM », mémoire master, L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRESQ, 2012

[II.3] THAMERI FAROUK « Simulation et Implémentation en temps réel de la technique OFDM en utilisant le processeur DSP C6713 » MEMOIRE DE MASTER, UNIVERSITE MOHAMED BOUDIAF - M'SILA, 2016

[II.4] Hermann Sohtsinda, « Approche conjointe canal et ampli_cateur d'_emission pour l'allocation dynamique de puissance dans les syst_emes MIMO-OFDM » thèse de doctorat, Université de Poitiers, 2017. Français.

[II.5] Annick Le Glaunec « MODULATIONS MULTIPORTEUSES »

[II.6] Farhi Nabila, Helaimia Souhaila « Etude et Simulation d'une Transmission de Type OFDM Pour Les Communications Sans Fil », mémoire master, UNIVERSITE LARBI TEBESSI – TEBESSA, 2016

[II.7] Mohamed larbi tayebi " performances des systems OFDM dans les canaux radio-mobiles", paf, FROC01n1912090617, 17390FR00001B/12/P

[II.8] Sylvain Traverso. « Transposition de fréquence et compensation du déséquilibre IQ pour des systèmes. multiporteuses sur canal sélectif en fréquence. » Traitement du signal et de l'image. Université de Cergy, Pontoise, 2007. Français. <tel-00412562>

[II.9] Mathilde BRANDON, " OPTIMISATION CONJOINTE DE MÉTHODES DE LINÉARISATION DE L'ÉMETTEUR POUR DES MODULATIONS MULTI-PORTEUSES " Université de Cergy-Pontoise, France.

[II.10] GALYNA PISKONOVA « TRANSMISSION OFDM POUR LA TÉLÉPHONIE CELLULAIRE » UNIVERSITÉ DU QUÉBEC, MONTRÉAL, 19 DÉCEMBRE 2003

[II.11] Fabrice LEMAINQUE « tout sur les réseaux sans fils » DUNOD, N° d'imprimeur 428185Z-Dépôt légal : avril 2009, France

[III.1] Renaud Dumont, « Cryptographie et Sécurité informatique » Université de Liège, 2010

[III.2] Daniel Barsky & Ghislain Dartois, « Cryptographie », cour, 1 octobre 2010

[III.3] SOUICI Ismahane, « Sécurisation évolutionnaire du transfert d'images » thèse de doctorat, université BBADJI MOKHTAR-ANNABA, 2013

[III.4] Jonathan BLANC, Adrien DE GEORGES « techniques de cryptographie », Licence Informatique, 2004

[III.5] Site web https://moodle.utc.fr/pluginfile.php/16777/mod_resource/content/0/SupportIntroSecu/co/CoursSecurite_13.html , (21/03/2019)

[III.6] José Marconi Rodrigues. « Transfert sécurisé d'Images par combinaison de techniques de compression cryptage et de marquage ». Université Montpellier II - Sciences et Techniques du Languedoc, 2006. Français. <tel-00115845>

[III.7] William Puech, Gouenou Coatrieux. « Codage hybride cryptage-marquage-compression pour la de l'information médicale ». A. Naït-Ali, Christine Cavaro-Menard. Compression des images et des signaux médicaux, Hermès-Lavoisier, Traité IC2, pp.269-298, 2007.

[III.8] David Kohel, Igor E. Shparlinski. « Théorie des nombres et cryptographie. Arithmétique et dynamique. » Chaires Jean Morlet 2014, SMF Journée Annuelle, 27, pp.1-23, 2014,

[III.9] Arief Susanto, Tutik Khotimah, Muhammad Taufik Sumadi, Joko Warsito, Rihartanto « Image encryption using vigenere cipher with bit circular shift » International Journal of Engineering & Technology, 7 (2.2) (2018) 62-64

[III.10] Jean-Paul DELAHAYE « La cryptographie visuelle » Pour la Science - n° 416 - Juin 2012

[III.11] Binay Kumar Singh, Sudhir Kumar Gupta « Grid-based Image Encryption using RSA » International Journal of Computer Applications (0975 – 8887), Volume 115 – No. 1, April 2015

[IV.1] M.MADANI, Y.BENTOUTOU « Cryptage d'images médicales à la base des cartes chaotiques » Conference Paper · December 2015

[IV.2] Z. Amrani, S Chitroub et A. Boukhari « Cryptage d'Images par Chiffrement de Vigenère Basé sur le Mixage des Cartes Chaotiques » 4th International Conference on Computer Integrated Manufacturing CIP'2007

[IV.3] BENHABIB Chouaib, « ETUDE D'UN SYSTEME CHAOTIQUE POUR LA SECURISATION DES COMMUNICATIONS OPTIQUES » mémoire master, L'UNIVERSITE DE TLEMCEN , 2014

[IV.4] Cristina MOREL, Analyse et contrôle de dynamiques chaotiques, application à des circuits électroniques non-linéaires. » THÈSE DE DOCTORAT, l'Université d'Angers, 2005

[IV.5] Floriane Anstett. « Les systèmes dynamiques chaotiques pour le chiffrement : synthèse et cryptanalyse » thèse de doctorat, Université Henri Poincaré - Nancy I, 2006. Français

[IV.6] Tayeb Hamaizia, « Systemes Dynamiques et Chaos Application à l'optimisation à l'aide d'algorithme", thèse de doctorat, Université de Constantine -1-, 2013

[IV.7] Eric Goncalvès da Silva. « Introduction aux systèmes dynamiques et chaos » . Engineering school. Institut Polytechnique de Grenoble, 2004, pp.23. cel-00556972

[IV.8] Jiancheng Zou, ChangZhen Xiong, Dongxu Qi1, Rabab K. Ward, « The Application of Chaotic Maps in Image Encryption », 2005 IEEE.,

[IV.9] Ons Jallouli. « Chaos-based security under real-time and energy constraints for the Internet of Things. » Signal and Image processing. UNIVERSITE DE NANTES, 2017. English

[IV.10] Goumidi Djamal Eddine « Fonction logistique et standard chaotique pour le chiffrement des images satellitaires » mémoire magister, Université Mentouri de Constantine (UMC), 2010

[IV.11] Mohammed A. AlZain, Osama S. Faragallah, « Efficient Chaotic Tent Map-based Image Cryptosystem » *International Journal of Computer Applications* (0975 – 8887), Volume 167 – No.7, June 2017

[IV.12] MEGHERBI OUERDIA, « Etude et réalisation d'un système sécurisé à base de systèmes chaotiques » MEMOIRE DE MAGISTER, UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU, 2013

[IV.13] Hamid HAMICHE, « Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques, Application à la Transmission Sécurisée de Données » tèse de doctorat, UNIVERSITÉ MOULOUD MAMMERI DE TIZI-OUZOU, 2011

[V.1] Yicong Zhou , LongBao, C.L.PhilipChen « A new 1D chaotic system for image encryption » Department of Computer and Information Science, University of Macau, Macau 999078, Signal Processing97(2014)172–182 China

[V.2] Elham Hassani, Mohammad Eshghi « Image Encryption Based on Chaotic Tent Map in Time and Frequency Domains » *The ISC Int'l Journal of Information Security*, January 2013, Volume 5, Number 1 (pp. 97{110)

[V.3] Abdellah Menasri, « CHAOS ET BIFURCATIONS DANS LES SYSTEMES DYNAMIQUES EN DIMENSIONS n (n > 1) » thèse de doctorat, UNIVERSITE LARBI BEN M.HIDI, 2016

[V.4] M.MADANI, Y.BENTOUTOU « Cryptage d'images médicales à la base des cartes chaotiques » All content following this page was uploaded by Mohammed Madani on 12 December 2015

[V.5] Wei Zhang, Chongfu Zhang, Wei Jin, Chen Chen, Ning Jiang, and Kun Qiu, « Chaos Coding-Based QAM IQ-Encryption for Improved Security in OFDMA-PON » *IEEE PHOTONICS TECHNOLOGY LETTERS*, VOL. 26, NO. 19, OCTOBER 1, 2014

[V.6] Alain Horé, Djamel Ziou " Image Quality metrics: PSNR vs. SSIM", 2010 international on Pattern Recognition, IEEE, 2010

[V.7] Hidayet Oğraş, Mustafa Türk «A Secure Chaos-based Image Cryptosystem with an Improved Sine Key Generator » *American Journal of Signal Processing* 2016, 6(3): 67-76, DOI: 10.5923/j.ajsp.20160603.01