République Algérienne Démocratique et Populaire

Ministère de L'enseignement Supérieur et de la Recherche Scientifique

UNIVERSITÉ MOHAMMED SEDDIK BENYAHIA – JIJEL

Faculté des sciences et de la technologie

Département d'électronique

Projet de fin d'étude pour l'obtention du diplome de

MASTER

En Télécommunications option Systéme des Télécommunications

Théme

Transmission sécurisée Des images médicales par DS-CDMA

Réalisé par :

Mme. BELAL Samira

Encadré par :

Dr. MESSADI Manel

Promotion : 2020/2021

Remerciement

Nous remercions avant tout DIEU Allah tout puissant pour la volonté, le courage et la patience qu'il nous a donnée afin de réaliser ce modeste travail.

Nous exprimons notre plus grande reconnaissance et notre respect à notre encadreur Dr. MESSADI-Manel pour avoir accepté de diriger ce travail, de nous avoir guidé et soutenu avec patience et pour les précieux conseils.

Nos vifs remerciements vont également aux membres du jury, d'avoir accepté de examiner notre travail et de l'enrichir par leurs propositions.

Nous souhaitons également adresser nos remerciements à l'ensemble des enseignants du département d'électronique, qui ont contribué à notre formation durant cinq années d'études.

Enfin, nous remercions toutes les personnes qui ont participé, de près ou de loin, à la réalisation de ce modeste travail.

Dédicace

Grâce à dieu tout puissant, qui m'a donné le courage, la volonté, la force pour réaliser ce mémoire, que nul ne peut se faire sans son désir.

Je dédie ce modeste travail en signe de respect et de reconnaissance

À ma très chère mère, quoi que je fasse ou que je dise, je ne saurai point te remercier comme il se doit, ton affection me couvre ta bienveillance me guide et ta présence à mes côtés a toujours été ma source de force pour affronter les différents obstacles.

À l'âme de mon père décédé il y a trois ans présent toujours dans mon cœur.

A toute personne de ma famille

A Tous ceux que j'aime et qui m'aiment

A tous mes amis.

" Le futur appartient à ceux qui croient à la beauté de leurs rêves" Eleanor Rosevelt.

SAMIRA

Liste des figures

Liste des Tableaux

Liste des abréviations

CDMA : Code Division Multiple Acess

DS-SS: Direct Sequence Spread Spectrum (L'étalement de spectre par séquence directe)

GSM : Global System for Mobile Communications

SNR : Signal to Noise Ratio

BPSK : Binary Phase Shift Keying: signal binaire modulé en phase

DS-CDMA : Direct-Sequence CDMA : CDMA à séquence directe

FH-CDMA : Frequency-Hopping CDMA : CDMA à saut de fréquence

IAM : Interférences d'Accès Multiple

OVSF : Orthogonal Variable Spreading Factor Codes

PN : Pseudo-Noise sequences : Séquences pseudo aléatoires

TDMA : Time Division Multiple Access : Accès multiple par répartition temporelle

UMTS : Universal Mobile Telecommunications System

WDM : Wavelength Division Multiplexing : Multiplexage par longueur d'onde

FDMA : Frequency Division Multiple Access : Accès multiple par répartition de fréquences

TEB : Taux d′Erreur Binaire.

AWGN : Additive White Gaussian Noise : bruit blanc additive gaussien

SOMMAIRE

Chapitre 4

Simulation et discussion des résultats

Introduction générale

Aujourd'hui, le réseau téléphonique transporte de la voie mais également des images et des données. Ainsi l'homme peut communiquer n'importe où, sans avoir à rester figer avec notamment l'apparition des systèmes de téléphonie sans fil.

Dans les applications civiles, la résistance à un brouillage intentionnel n'est pas un critère déterminant dans le choix de la technologie de multiplexage. On cherche cependant à rendre le système de communication résistant à des interférences non volontaires : les interférences entre utilisateurs, les interférences liées à des phénomènes de réflexion et la présence d'un bruit additif.

Dans le cas du CDMA, le signal émis ressemble beaucoup à du bruit parce que l'on utilise des codes longs pseudo-aléatoires. Le signal est étalé uniformément sur un large spectre : on ne détecte aucun pic en amplitude pour une fréquence donnée. Ceci permet de masquer la présence ou non d'une communication.

La transmission de données caractérise une communication d'un signal porteur d'informations, établie entre un émetteur et un récepteur par l'intermédiaire d'un canal de transmission.

Le CDMA, étant une méthode de multiplexage à étalement de spectre, le brouillage efficace doit se faire sur toute la bande de fréquences utilisées, ce qui n'est pas envisageable car cela consommerait une puissance colossale, la résistance aux interférences et pour le niveau de sécurité qu'elle offre. Chaque utilisateur a un code d'étalement ou une signature qui lui est propre. Le nombre d'utilisateurs est lié au nombre de séquences d'étalement générées par une famille de code donnée.

Le CDMA consiste donc à étaler ou à redistribuer le signal sur une très grande bande passante, jusqu'à le rendre ″invisible″ pour les autres utilisateurs qui partagent la même bande passante. A la réception, l'opération d'étalement exécutée lors de l'émission est répétée pour ″dés étaler″ le signal en bande de base tandis que les autres signaux transmis sont perçus par le récepteur comme étant du bruit.[1]

Elle permet à plusieurs utilisateurs d'un réseau de partager le même canal de transmission sans gestion de temps ni de fréquence, cette technique apporte un accès multiple et un partage de ressource flexible, reconfigurable et sécurisé.

Il semblerait que le CDMA soit plus performant que les autres méthodes de multiplexage au niveau des zones de recouvrement des cellules, ses principales contraintes sont le cout d'acquisition, la maintenance du réseau et le prix élevé des terminaux.

Le cryptage d'image basé sur le chaos est devenu l'un des plus efficaces, et d'excellentes méthodes de cryptage. C'est parce que les systèmes est chaotique ont une sensibilité élevée à leurs valeurs initiales paramètres de contrôle, propriété chaotique, non-convergence et ergodiques des états.

La cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Le verbe crypter est parfois utilisé mais on lui préfèrera le verbe chiffrer.

Le fait de coder un message de telle façon à le rendre secret (chiffrement), la méthode inverse, consistant à retrouver le message original (déchiffrement).

La cryptographie chaotique est récente et a démontré une fiabilité de la sécurité tant bien qu'elle a démontré une grande résistance à la cryptanalyse, comme elle est parfaitement combinée avec le maintien des attributs nécessaires aux algorithmes de chiffrement[2].

Sachant qu'il y a deux types de fonctions chaotiques, part celles qui ont un comportement purement chaotique et qui ne sont pas modélisables, et d'autre part les fonctions chaotiques déterministes qui sont modélisables par des systèmes d'équations qu'on nomme « systèmes dynamiques non linéaires », et ce sont ces dernières qui sont utilisées dans le chiffrement chaotique car leurs attracteurs sont sous forme fractale et rendent l'évolution des trajectoires totalement dépendantes des conditions initiales, et il est donc impossible de prédire ces trajectoires sans connaitre leurs états initiaux, ce qui rend le comportement chaotique imprévisible, et leur sécurité quasi-totale.[3]

Et pour les introduire dans le chiffrement il faut d'abord choisir une fonction chaotique ensuite il faut superposer le signal chaotique au flux de données à transmettre selon l'une des techniques choisies pour le cryptage par chaos, dans notre mémoire on a utilisé le cryptage par addition, cette méthode est la première à utiliser la synchronisation du chaos, l'idée repose sur l'observation des signaux chaotiques, le principe est d'ajouter le message utile m(t) au signal chaotique Cx(t) et de le récupérer ensuite par la synchronisation chaotique à travers le canal de transmission. Au niveau du récepteur autorisé, ainsi, après la synchronisation grâce au signal reçu, le message original est extrait à l'aide d'une opération de soustraction.

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.

Le cryptage et la communication sécurisée est l'un des champs d'applications prometteur des systèmes chaotiques, en effet la cryptographie chaotique peut s'effectuer sous différents schémas, il s'agit de définir la façon d'introduire le message dans l'émetteur.

Dans le cadre de notre mémoire de fin d'études, on s'intéresse la transmission des images médicales à travers une transmission DS-CDMA, et comme les images médicales sont des informations confidentielles, on propose l'application d'une technique de cryptage hybride a base du chaos pour augmenter la sécurité des données.

Notre travail dans ce mémoire est composé de quatre chapitres complémentaires :

Le premier chapitre est consacré à l'état de l'art sur DS-CDMA avec une introduction à différentes techniques du multiplexage, utilisation et application du CDMA, Caractéristiques globales d'un système DS-CDMA et on termine par présenter les avantages et inconvénient et l'accès multiple a cette technique.

Dans le deuxième chapitre, on détail les séquences d'étalements du spectre tel que le code de Walsh et Hadamard, code d'Ovsf, et Kasami avec présentations de leurs différentes propriétés.

Dans le troisième chapitre, on introduit les systèmes chaotiques et leurs propriétés, puis on détail quelques techniques du cryptage chaotique

Dans le dernier chapitre on présente les différents résultats de simulation et leurs interprétations.

Enfin, on termine par une conclusion générale

Chapitre I

État de l'art sur DS-CDMA

Chapitre 1 :

État de l'art sur DS-CDMA

1.1 INTRODUCTION

Le CDMA était destiné initialement aux systèmes de communications numériques sur radiofréquences dans le cadre d'applications militaires. Profitant ainsi d'une augmentation de la capacité de multiplexage tout en utilisant les propriétés d'étalement de spectre propre à cette technique, l'objectif était de rendre les transmissions plus robustes à l'apparition de brouilleurs et moins vulnérable aux interceptions éventuelles.

Le CDMA permet de coder et de transmettre autant de signaux qu'il est possible de générer des séquences de code à la seule condition que ces séquences satisfassent à des propriétés d'auto et d'inter corrélation adaptées. Ces conditions sur les fonctions de corrélation permettent de contrôler et de minimiser les IAM responsables, en partie, de l'augmentation du Taux d'erreurs Binaires (TEB) lors de la détection et du décodage [4].

Le principe de base du CDMA est une modulation directe du message à transmettre par une séquence de code affectée à un utilisateur donné, cette manière de faire a donné naissance à ce qui est communément appelé CDMA à étalement du spectre à Séquence Directe.

1.2 Différentes techniques CDMA et leurs caractéristiques

Le CDMA était destiné initialement aux systèmes de communications numériques sur radiofréquences dans le cadre d'applications militaires. Profitant ainsi d'une augmentation de la capacité de multiplexage tout en utilisant les propriétés d'étalement de spectre propre à cette technique, l'objectif était de rendre les transmissions plus robustes à l'apparition de brouilleurs et moins vulnérable aux interceptions éventuelles.

Le CDMA permet de coder et de transmettre autant de signaux qu'il est possible de générer des séquences de code à la seule condition que ces séquences satisfassent à des propriétés d'auto et d'inter corrélation adaptées. Ces conditions sur les fonctions de corrélation permettent de

contrôler et de minimiser les IAM responsables, en partie, de l'augmentation du Taux d'erreurs Binaires (TEB) lors de la détection et du décodage [5].

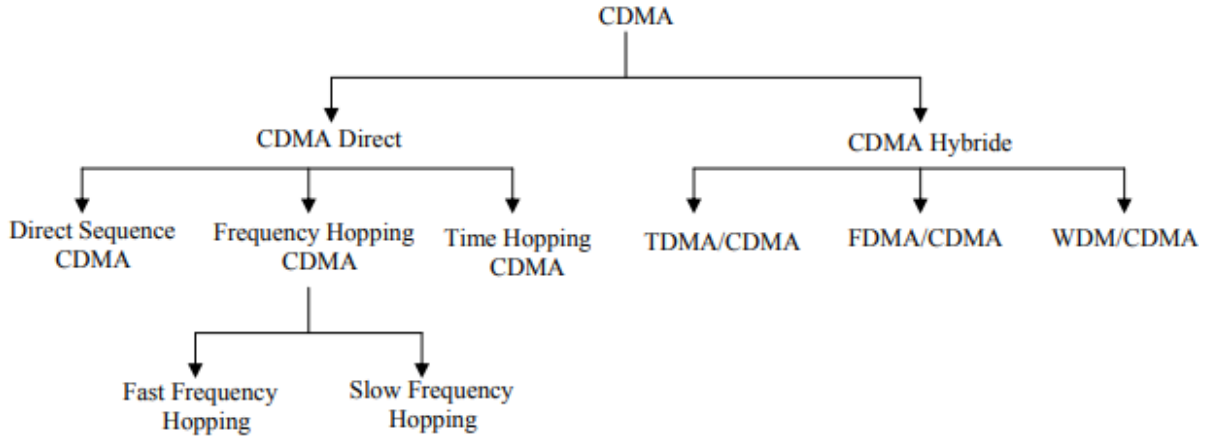


Figure 1.1 : Différent technique CDMA.

Pour obtenir de meilleures performances, plusieurs études ont associé le CDMA aux autres techniques de multiplexage (TDMA, FDMA, WDM …etc.).

1.2.1 Le partage en fréquence (FDMA)

Le partage en fréquence est également appelé FDMA (Frequency Division Multiple Access). Le principe du FDMA est de réserver à chaque usager une portion du spectre disponible, qui sera utilisée pendant toute la durée de la communication. La technique FDMA est la technique la plus ancienne [6].

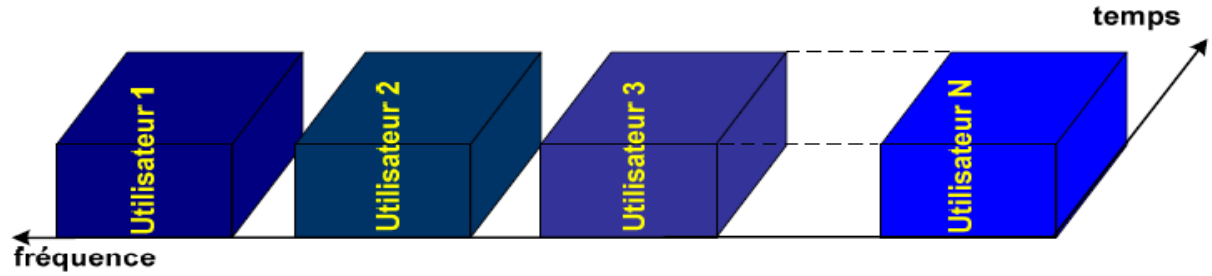


Figure1.2 : Représentation temps-fréquence du FDMA.

1.2.2 Le partage en temps (TDMA)

Le partage en temps ou TDMA (Time Division Multiple Access) est une alternative de FDMA. Les usagers d'un système TDMA utilisent tous la même bande de fréquence. Le partage de la ressource est effectué au travers de l'allocation d'un intervalle de temps propre à chaque usager.

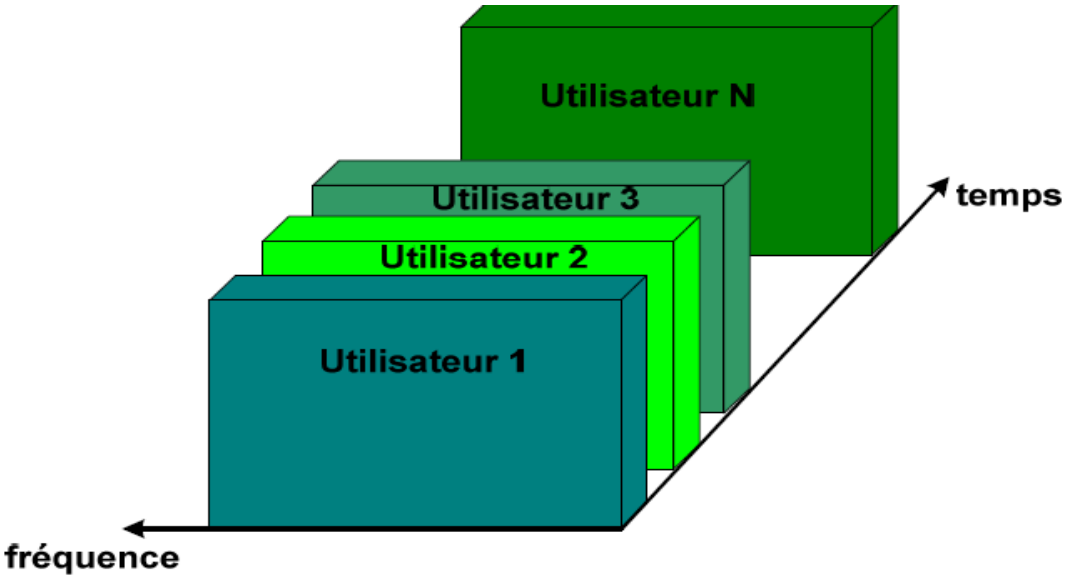


Figure1.3 : Représentation temps-fréquence du TDMA.

1.2.3 Multiplexage par longueurs d'onde WDM [7]

Le multiplexage en longueur d'onde (Wavelength Division Multiplexing en anglais) est une technique utilisée en transmissions optiques qui permet de faire passer plusieurs ondes de longueur d'onde différentes sur une seule fibre optique. On multiplexe ainsi plusieurs signaux optique sur une seul fibre, en sortie on sépare les différentes ondes au moyen d'un démultiplexeur (DEMUX). Pour pouvoir multiplexer les n sources, il faut préalablement changer leurs longueurs d'ondes en utilisant des transpondeurs.

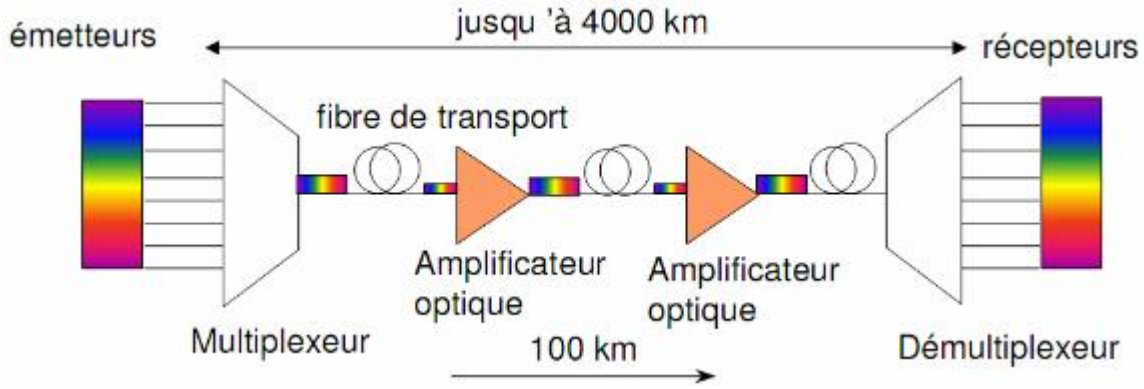


Figure1.4 : Principe du multiplexage en longueur d'onde.

1.2.4 Le partage en code (CDMA)

Le partage en code appelé AMRC ou CDMA. Ce partage est radicalement différent des deux partages précédents (TDMA, FDMA). Les usagers d'un système CDMA utilisent tous la même bande de fréquence au même instant. La séparation entre les différents usagers étant assurée par un code propre à chacun.

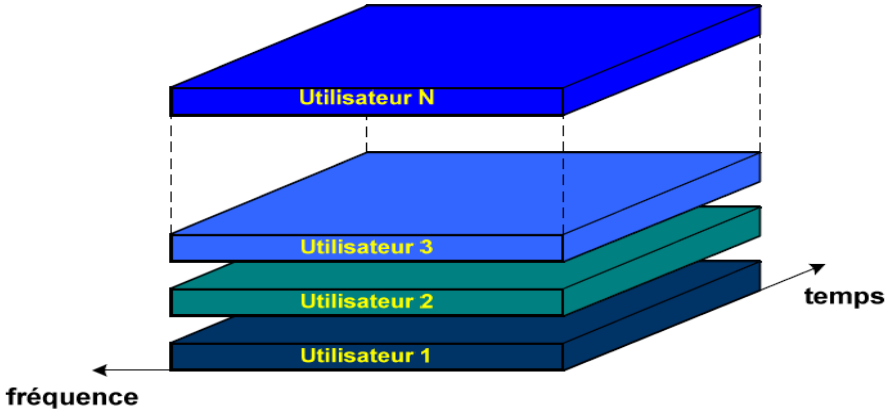


Figure1.5 : Représentation temps-fréquence a L'accès CDMA.

Le principe de base du CDMA est une modulation directe du message à transmettre par une séquence de code affectée à un utilisateur donné, cette manière de faire a donné naissance à ce qui est communément appelé CDMA à étalement du spectre à Séquence Directe.

Il existe deux principales variétés de CDMA [8] :

- ✓ FH-CDMA (Frequency Hop). Dans ce système, on fait de l'évasion de fréquence : la clé de chaque utilisateur code pour une suite de fréquences qui feront alternativement office de porteuse. Ce système ressemble à un multiplexage fréquentiel dans lequel l'attribution des fréquences varierait rapidement (par rapport au débit d'informations à transmettre).
- ✓ DS-CDMA (Direct Sequence). C'est à ce type de CDMA qu'on fait généralement référence quand on parle de CDMA, et c'est celui que nous avons étudié aussi bien théoriquement qu'expérimentalement. Ici, on multiplie directement le message à transmettre par une le code (séquence pseudo-aléatoire). L'étalement spectral du signal codé vient de ce que la fréquence du code est largement supérieure à la fréquence d'envoi des données.

1.3 Fonctionnement du CDMA

L'accès multiple par division de code est une approche entièrement différente de l'accès multiple par division temporelle. CDMA, après avoir numérisé les données, répartit la date sur toute la bande passante disponible. Plusieurs appels se chevauchent les uns aux autres sur un canal qui est affecté avec un code de séquence unique. L'AMRC est une forme de technique d'étalement du spectre, ce qui signifie que les données peuvent être envoyées en petits morceaux sur un certain nombre de fréquences disponibles à utiliser à tout moment dans la plage spécifiée.[9]

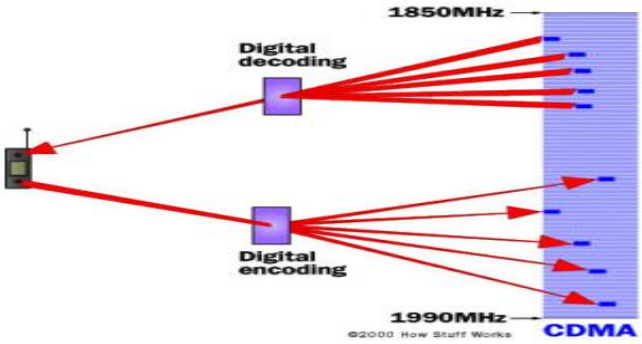


Figure1.6 : fonctionnement du CDMA.

Toutes les données des utilisateurs peuvent être transmises de la même manière que celles d'un segment de spectre à large bande. Les signaux des utilisateurs sont répartis sur toute la bande passante par un code d'étalement unique. À l'extrémité du récepteur, le même code est utilisé pour récupérer le signal. Huit et dix appels distincts sont effectués dans le même espace de canal qu'un appel analogique.

1.4 Applications du CDMA dans la technologie [10]

En raison des avantages inhérents de l'AMRC celui-ci émerge comme un gagnant dans la bataille de la technologie et des services sans fil. CDMA permet un développement et l'utilisation beaucoup plus importants de périphériques à large bande tels que les modems sans fil pour ordinateurs portables, les unités de système GPS et d'autres appareils innovants. À des fins commerciales, CDMA prend en charge la fourniture de services push to talk et push to email à haute vitesse. Push to talk donne au mobile la possibilité d'être utilisé comme un appareil walky-talky. Ces services sont exemptés des frais de service imposés par les exploitants qui rendent l'AMRC rentable. CDMA est considéré comme le mode de communication sans fil le plus élevé, et est responsable du mode rapide et sûr d'échange de données tel que la 3G. Récemment, CDMA a fusionné avec la technologie GSM pour donner un service Internet 4G ou LTE haut débit.

1.5 Définition d'un système DS-CDMA

D'abord le CDMA (Code Division Multiple Access) ou l'AMRC est une méthode utilisée pour multiplexer plusieurs communications sur un seul support de transmission (en utilisant une même bande de fréquence) par le biais de plusieurs codes (ayant une certaine orthogonalité).

Ceci n'est possible qu'en effectuant un étalement de spectre. On parle alors de système DS-CDMA lorsque celui-ci utilise la méthode de séquence directe comme méthode d'étalement de spectre.

1.6 Caractéristiques globales d'un système DS-CDMA

Un système DS-CDMA ne nécessite pas l'allocation de fréquence ni la synchronisation entre les utilisateurs, Chaque usager dans un système DS-CDMA possède un accès complet à toute la bande de fréquence, à n'importe quel moment. Cependant ceci se fait au détriment de la qualité de communication qui se dégrade avec le nombre croissant des usagers du système (augmentation du taux d'erreur binaire) [11].

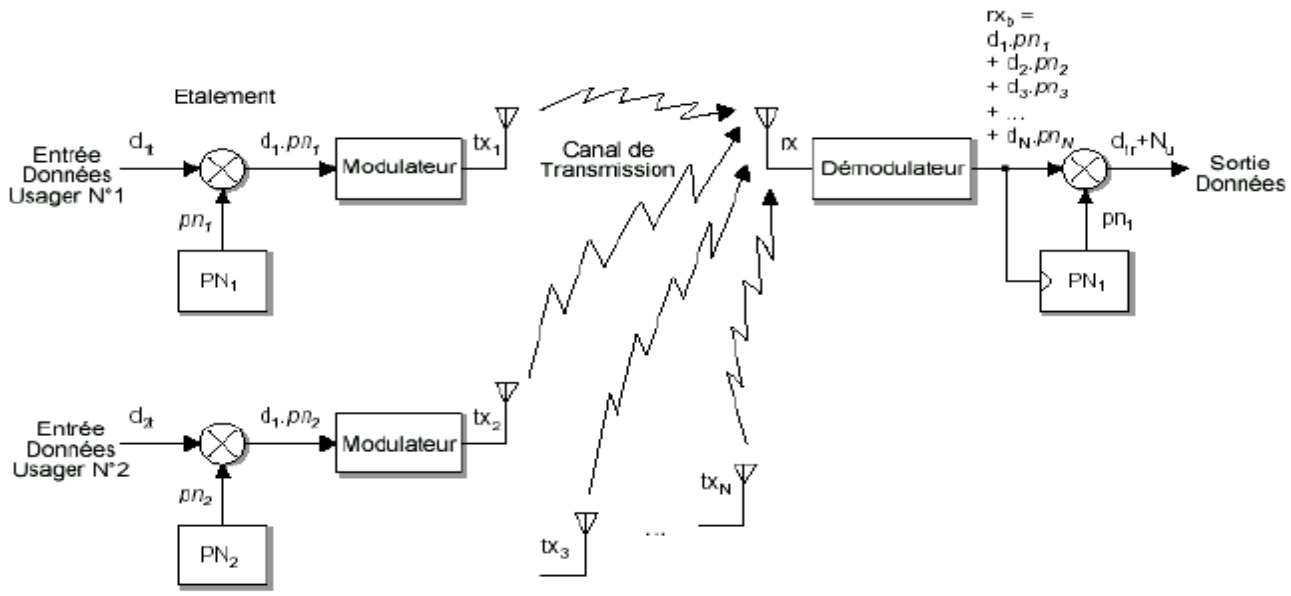


Figure 1.7 : Principe d'un système DS-CDMA.

Pour que le récepteur puisse désétaler le signal reçu y(t), il faut qu'il : Connaît le code c(t) utilisé par l'émetteur. Synchronisé le code du signal reçu et le code généré localement. Le signal pseudo-noise c(t) apparaît aléatoire et doit être imprévisible Le débit (chip rate) de c(t) est plus grand que le débit (bit rate) de message m(t). L'autocorrélation de c(t) doit être très faible : Petite similitude de c(t) par rapport à ses versions retardées donc meilleur résistance

aux fadings Multi-trajets. Dans CDMA, il faut aussi que l'inter-corrélation entre deux codes différents c1(t) et c2(t) soit faible ce qui fait interférence négligeable entre les différents signaux multiplexés par accès multiple.

Au sein d'un système DS-CDMA, chaque utilisateur :

♦ possède son propre code pseudo aléatoire PN (Psedo Noise) : qui répondent aux propriétés de corrélation et d'orthogonalité.

♦ utilise la même bande de fréquence radio.

♦ peut émettre indépendamment des autres utilisateurs (d'une manière asynchrone ou synchrone vis-à-vis des autres utilisateurs).

Les codes les plus utilisés (à cause de leurs performances) sont :

- ✓ les codes de Gold, Kasami (pour les systèmes DS-CDMA asynchrones).
  (Les codes de Gold sont une catégorie importante de séquence générant un ensemble de codes ayant de bonnes propriétés d′intercorrélation).
- ✓ les codes Walsh-Hadamard (pour les systèmes DS-CDMA synchrones).

1.7 Accès multiple par répartition de code par séquence direct DS-CDMA:

L'accès multiple par répartition de code, ou CDMA, est une technique de multiplexage définie comme étalement de spectre. Cette dernière permet par l'étalement de la puissance sur une large bande de fréquence du canal, de mieux résister aux évanouissements sélectifs en fréquences et de donner au signal à transmettre la forme d'un bruit le rendant difficilement détectable par des récepteurs [5].

Pour le CDMA, l'utilisation de séquences d'étalement comme codes permettant de distinguer les différents utilisateurs donne, de plus, l'avantage d'exploiter simultanément l'ensemble de la bande de fréquence et des intervalles de temps. Il en résulte une meilleure gestion des ressources disponibles. Les conditions posées sur l'orthogonalité des séquences de code permettent de réduire les interférences entre utilisateurs et partagent le même espace fréquentiel et transmettent sur les mêmes intervalles temporels, Il s'agit dans ce cas, d'affecter à chaque émetteur un code qui lui permet de transmettre des informations en évitant d'interférer avec les messages provenant d'autres utilisateurs, la réduction des IAM(interférence à accès multiple n'est obtenue que dans le cas de l'utilisation de séquences de codes strictement orthogonaux. La figure schématise la répartition des utilisateurs sur la bande de fréquence et dans le temps en fonction de la distribution des séquences des codes

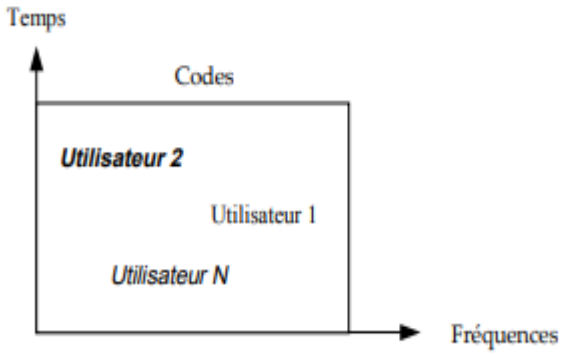


Figure1.8 : Schéma d'un multiplexage par code (CDMA).

Les séquences des codes utilisées dans les systèmes CDMA sont composées d'une série d'impulsions nommées ″chips″ afin d'être distinguées des ″bits″ qui composent une séquence de données. L'étalement de spectre est un des avantages mis en avant pour l'utilisation du CDMA dans le domaine des communications radiofréquences. En effet, la puissance d'un signal, après codage, est étalée sur toute la largeur de la bande de fréquence disponible. De ce fait deux caractéristiques importantes apparaissent :

− La puissance du signal étant étalée sur la bande spectrale disponible, le signal CDMA peut être confondu avec le bruit du canal et sera donc difficilement détectable par un utilisateur non concerné.

− Le signal CDMA étalé est plus résistant aux évanouissements sélectifs en fréquence est plus résistant (après codage) aux brouilleurs pouvant se présenter au cours de la transmission. Lors du décodage, la puissance de ce brouilleur est étalée sur la bande spectrale disponible alors que le signal utile est reconstitué. Toutefois, si le nombre de brouilleurs est importante, la puissance générée par ces derniers sera plus importante et affectera la qualité du signal utile obtenu après décodage.

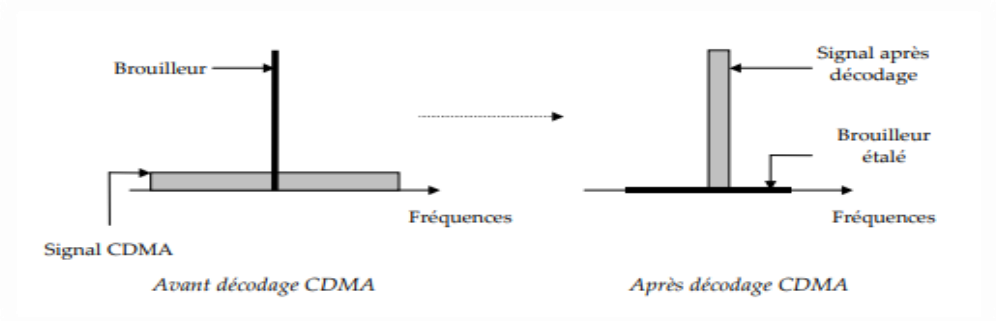


Figure1.9 : Effet de l'étalement du spectre sur la présence d'un brouilleur.

Dans le CDMA à séquence directe (DS-CDMA), les données associées à un utilisateur sont modulées en phase, en fréquence ou en amplitude. Le signal résultant est par la suite codé par une séquence de code, par exemple une séquence pseudo aléatoire, puis superposé aux autres signaux traités de la même manière.

Comme la montre la Figure, un signal binaire modulé en phase BPSK (Binary Phase Shift Keying) x(t) est codé par une séquence pseudo-aléatoire ou Pseudo Noise (PN) pn(t).

Le résultat de ce codage est représenté par le signal g(t), ce dernier est superposé aux autres signaux provenant des autres émetteurs et ayant subi un traitement similaire et est transporté par le canal de transmission. Le codage des données s'effectue donc de manière ″directe″, sans faire intervenir d'autres paramètres comme la fréquence ou la longueur d'onde. Il est, bien sûr, tout à fait possible de coder les données avant d'appliquer la modulation, d'amplitude, de phase ou de fréquence souhaitée [12].

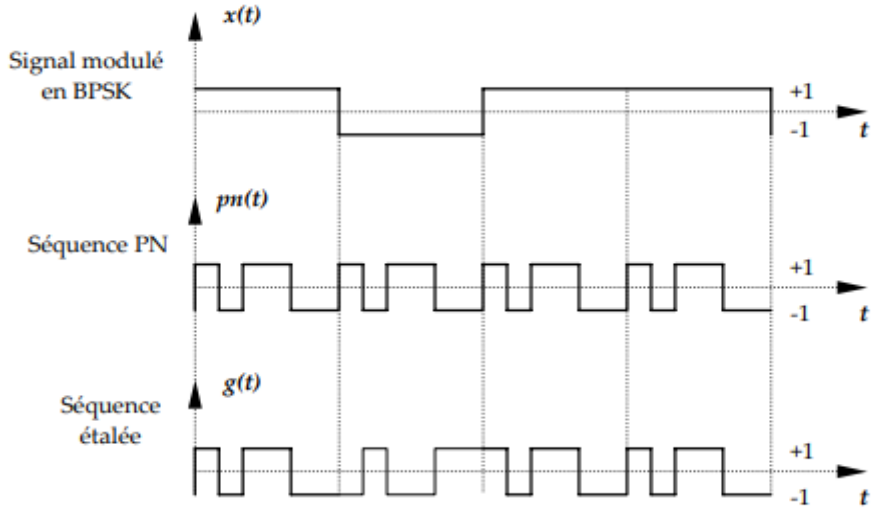


Figure 1.10 : Schéma d'un codage CDMA par séquence directe (DS-CDMA).

Certains avantages du CDMA semblent immédiatement capitalisables dans les réseaux optiques à haut débit. Nous pouvons citer le partage des ressources, la possibilité d'implémentation par des réseaux dits ″tout-optiques″, la non-nécessité de synchronisation entre les différents émetteurs …etc.

1.8 Avantages et inconvients du DS-CDMA

1.8.1 Quelques avantage : [13] [14]

La technique de l'étalement de spectre consiste à moduler le signal contenant l'information puis a "l'étaler" de manière à ce que le spectre du signal émis occupe une bande de fréquence

très supérieure à celle nécessaire à la transmission de l'information. L'étalement de spectre par rapport aux modulations a bande étroite, présente de nombreux avantages:

- bonne résistance aux perturbations bande étroite : lors de l'émission des perturbations bande étroite peuvent s'ajouter au signal étalé. Le récepteur réalise l'opération inverse de l'étalement. Le signal étalé est ainsi transformé en signal bande étroite alors que les perturbations a bande étroite sont étalées. De cette façon, la puissance des perturbations devient négligeable devant celle du signal utile reconstitué.

- La capacité des systèmes DS-CDMA est limitée par les interférences, tandis que l'AMRT et l'AMRF sont limitées par la bande passante disponible (hard limit capacity).
Ainsi la limite est floue car l'addition d'un utilisateur résulte en une légère dégradation des performances. Quand le système est très chargé, il n'y a pas de blocage (théoriquement) contrairement aux autres types d'accès multiple. Une autre conclusion qu'on peut tirer de ce fait est que toute réduction sur l'interférence due à l'accès multiple (MAI : Multiple Access Interférence) est récompensée directement par une augmentation de la capacité.
- faible brouillage des émissions classiques à bande étroite : les signaux à bande étroite peuvent cohabiter sur la même bande de fréquence que ceux générés par un système à étalement de spectre, sans perturber de façon importante un système par rapport à l'autre. La puissance de ces signaux est étalée sur une bande de fréquence importante leur densité spectrale de puissance est donc très faible comparée à celle des signaux a bande étroite.
- insensibilité aux effets des trajets multiples : contrairement aux transmissions bande étroite, l'étalement de spectre permet de lutter efficacement contre l'effet des trajets multiples de propagation. Les creux de Fading résultant de ces trajets multiples peuvent absorber Complètement le spectre d'une modulation bande étroite. Dans le cas d'une modulation large bande, sous réserve que cette bande soit supérieure à la bande de cohérence du canal radio seule une partie du signal disparaıt.
- faible probabilité d'interception : le signal ayant les caractéristiques d'un bruit aléatoire dont le niveau peut être inférieur à celui du bruit thermique, la communication est difficilement détectable. De plus, si le signal était détecté, seuls les récepteurs possédant les paramètres de la séquence d'étalement pourront accéder à l'information.
– multiplexage et adressage sélectif : plusieurs émissions peuvent cohabiter dans la même bande de fréquence dans la mesure où les codes d'étalement relatifs à chacun des signaux sont orthogonaux, c'est à dire dans la mesure où ils présentent une inter-corrélation voisine de zéro. La séquence d'étalement affectée à chaque signal constitue sa clé de codage. Ce signal ne peut

être exploité que si le récepteur possède la même clé de codage, Cette propriété se nomme l'Accès Multiple à Répartition par les séquences d'étalement.

- Le plus grand avantage du DS-CDMA par rapport aux systèmes conventionnels est que celui-ci peut réutiliser le spectre tout entier à travers toutes les cellules étant donné qu'il n'y a pas de concept d'allocation de fréquence dans ce système. Ceci augmente la capacité du système DS-CDMA dans une large proportion (à cause de la réduction du facteur de réutilisation des fréquences).

-Effet de sectorisation : dans les systèmes AMRT et AMRF, la sectorisation est effectuée pour atténuer l'interférence co-canal. Cependant, l'efficacité globale de ces systèmes décroît (car on ne peut pas utiliser les mêmes fréquences pour les secteurs d'une même cellule). D'un autre côté, la sectorisation augmente la capacité des systèmes DS-CDMA.

Cette sectorisation peut être faite tout simplement par l'introduction de 3 équipements radio similaires dans les 3 secteurs. La réduction de l'interférence mutuelle ainsi effectuée se traduit par une augmentation de la capacité (dans un facteur de 3 environ).

1.8.2 Inconvénients liés à cette technique

– Encombrement spectral important qui rend souvent l'attribution de fréquences difficile, en effet le signal a toujours la même puissance mais celle-ci est répartie différemment, Il faut alors utiliser un sous-système permettant de contrôler la puissance.

– Complexité accrue des systèmes qui rend leur coût plus élevé par rapport à celui des systèmes à bande étroite.

– La synchronisation de la séquence d'étalement de l'utilisateur concerné dans le récepteur avec celle de l'émetteur dans un environnement perturbé par les autres utilisateurs, cela afin de démoduler correctement les données utiles. Suivant la technique utilisée pour résoudre cette synchronisation, le récepteur sera plus ou moins complexe.

Ce type d'émetteur-récepteur, utilisant l'étalement de spectre, est principalement utilisé dans les systèmes CDMA, c'est à dire dans un environnement multi-utilisateurs.

1.9 Conclusion

Au cours de ce chapitre, nous avons rappelé les différentes techniques d'accès multiple couramment employées dans le domaine des communications dans les réseaux sans fil. Nous avons montré qu'il existe des différentes méthodes d'accès de type TDMA, FDMA

et WDM..., Comme on a étudié l’état de l’art de la technique d’accès CDMA a séquence direct (SD-CDMA) et son importance par rapport aux autres.

Chapitre 2 :

État de l'art sur les séquences d'étalement

Chapitre 2 :

État de l'art sur les séquences d'étalement

2.1 INTRODUCTION

L'approche traditionnelle dans les communications numériques consiste à transmettre le plus d'information possible dans une bande de fréquence la plus étroite possible. Par contre, au sein du concept de l'étalement de spectre (SS:Spread Spectrum) [15] l'information à transmettre est étalé à travers une bande de fréquence beaucoup plus large que celle nécessaire avec l'approche traditionnelle.

2.2 Chaine de transmission

Dans la chaine de transmission des données, le bloc "étalement de spectre" se trouve entre le bloc "codage canal" et le bloc "canal" comme le montre le schéma. Le bloc "reconstruction signal" est le bloc inverse du bloc "étalement de spectre". Il transforme le signal large bande en signal bande étroite et donne, en sortie, les bits probablement émis.

Le principe de l'étalement de spectre consiste à répartir l'énergie du signal à émettre sur une bande de fréquence plus large que celle réellement nécessaire à la transmission du signal utile. Les deux principales techniques de modulation par étalement de spectre sont la séquence directe (Direct Séquence Spread Spectrum) et le saut de fréquence (Frequency Hopping Spread Spectrum). Dans le cas de la séquence directe, l'énergie du signal est répartie sur toute la bande de fréquence disponible, alors que pour le saut de fréquence, la bande de fréquence disponible est divisée en un grand nombre de sous-canaux. La fréquence porteuse se déplace alors d'un sous-canal à l'autre par des sauts discrets pseudo-aléatoires.

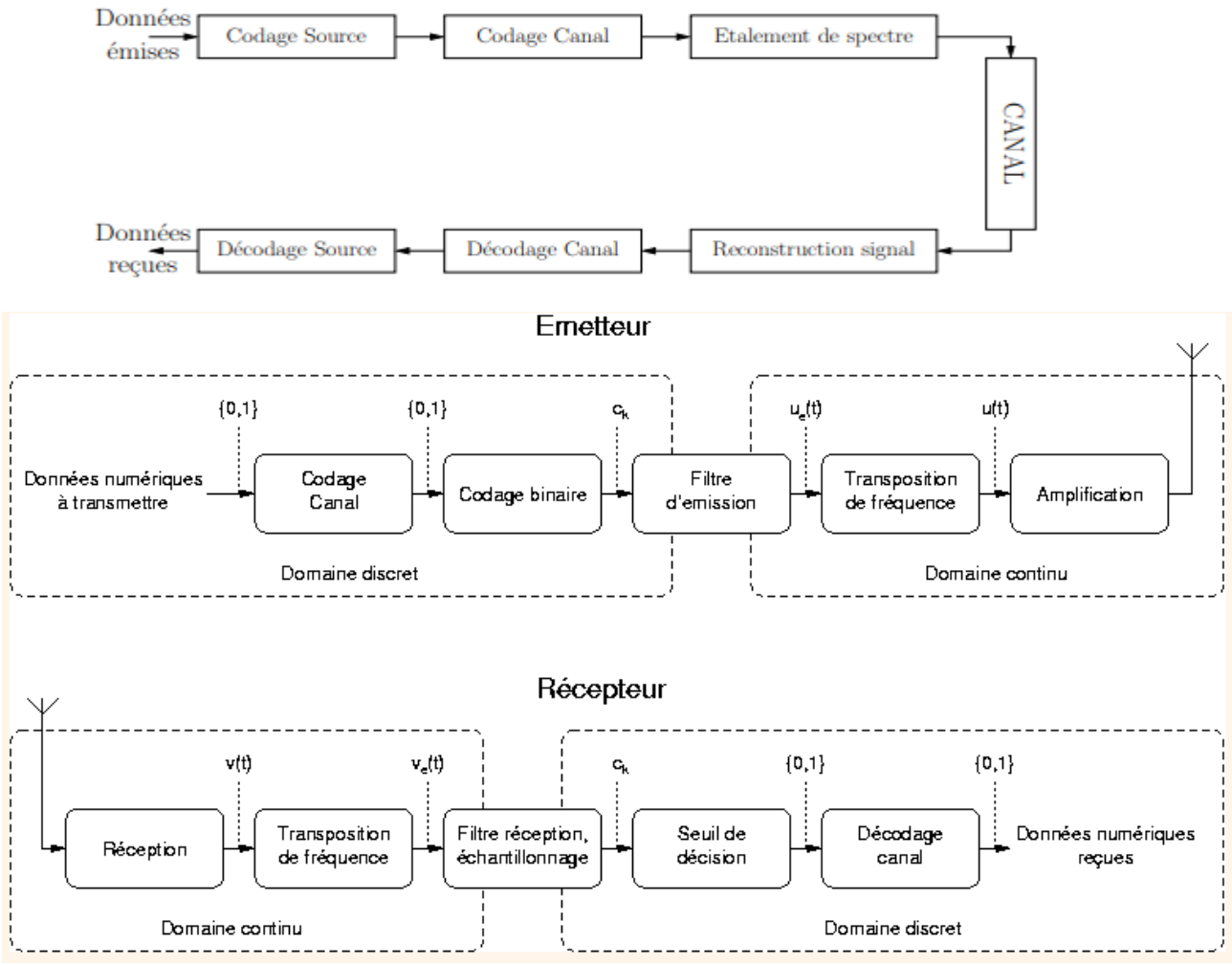


Figure 2.1 : Schéma d'une chaine de transmission.

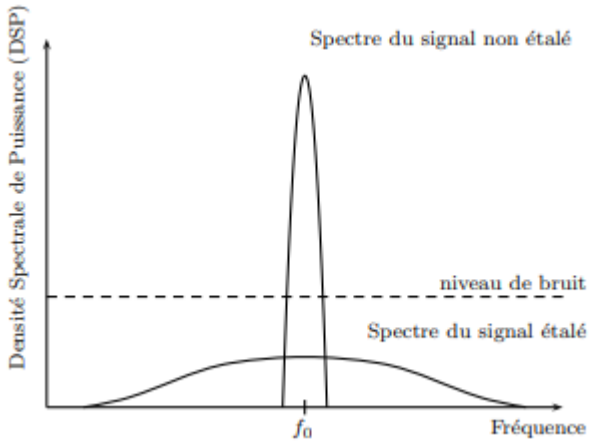


Figure 2.2 : Comparaison signal bande étroite / signal étalé.

2.3 Les séquences d'étalement :

Une séquence d'étalement est une suite d'éléments binaire, cadencé à un rythme largement supérieur au débit des données d'information à traiter. La multiplication de ces dernières avec une séquence d'étalement fait que les données obtenues après cette opération sont étalées à travers une large bande largement supérieure à celle requise pour la transmission des données d'information [11][15].

- ✓ **Le chip** : L'étalement de spectre est effectué par une fonction qui est indépendante de l'information à transmettre. Cette fonction est matérialisée par une séquence d'étalement et chaque élément binaire de cette séquence d'étalement est appelé "chip".
- ✓ **La longueur d'une séquence :** Une séquence d'étalement est caractérisée par sa longueur qui n'est autre que le nombre de "chip" contenu dans une période toute entière de la séquence.
- ✓ **Le Gain de traitement (Processing Gain) ou le Facteur d'étalement :** C'est le rapport entre la bande de fréquence occupée par le signal étalé par rapport à celle occupée par les bits d'informations. C'est encore le rapport entre les débits de la séquence d'étalement et des bits d'informations.

$$Gp = \frac{Rc}{Rs} = \frac{Ts}{Tc} \tag{2.1}$$

Ce rapport reflète la robustesse du système face aux interférences et les brouillages à bande étroite. En pratique, ce facteur est choisi comme un entier.

2.4 Étalement du spectre par séquence directe :

Dans les systèmes de communications radiofréquences, le CDMA est utilisée dans les pays d'Amérique du Nord et de la norme UMTS de la troisième génération de téléphonie mobile européenne aujourd'hui en cours de déploiement. Les études liées à la transposition des techniques CDMA dans les systèmes de communications optiques, profiter de la très large bande passante disponible sur le canal optique, le CDMA optique a aussi pour ambition d'augmenter la capacité de multiplexage en augmentant le nombre d'utilisateurs au prix d'une dégradation supportable de la qualité de la liaison et ce en exploitant simultanément les intervalles de temps et la bande de fréquence. Il permet aussi une transmission asynchrone des différents signaux sans recourir à des configurations et des protocoles de synchronisation. Un accès rapide est susceptible d'être apporté par des dispositifs passifs que sont les codeurs/ décodeurs optiques évitant ainsi la bande passante réduite des conversions optique - électrique / électrique - optique. Il est possible de distinguer en optique deux approches du CDMA optique, une première dite cohérente et une seconde appelée approche non-cohérente [16].

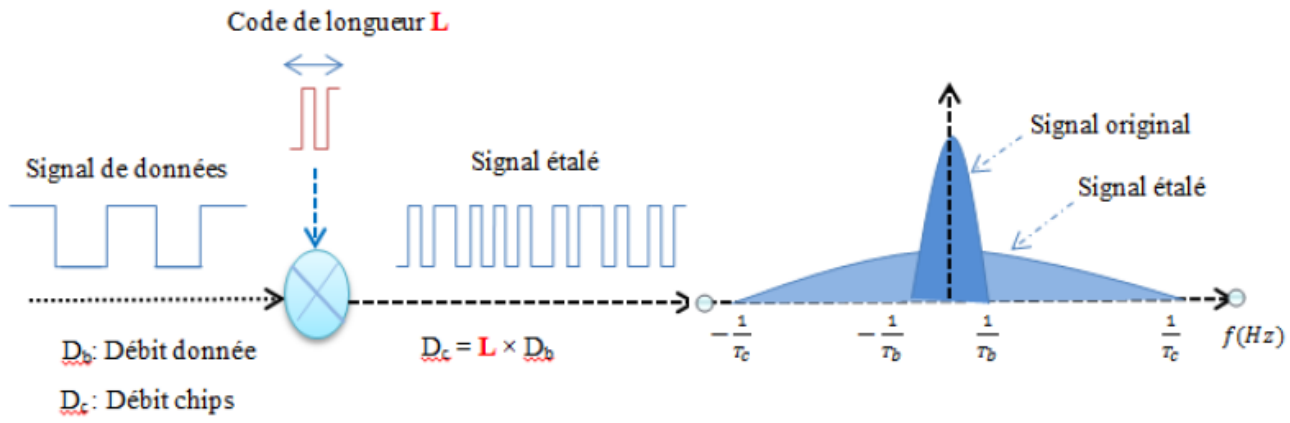


Figure 2.3 : Principe de l'étalement du spectre.

Le CDMA attribue à chaque utilisateur un code d'étalement, appelé aussi «signature» constitué d'une suite de bits rapides appelés «chips».

Le débit après codage est celui des données utilisateurs multiplié par la longueur de la séquence de code figure suivante. Cette technique permet la transmission des données tout en évitant l'interférence avec les messages des autres utilisateurs (désignées interférer accès multiple (IAM).

Cette réduction des IAM est conditionnée par l'utilisation exclusive des séquences des codes orthogonaux. Au niveau du récepteur, une opération inversée est effectuée pour «dés étaler» le signal en bande de base alors que les autres signaux transmis (interférents) sont identifiés comme étant un bruit.

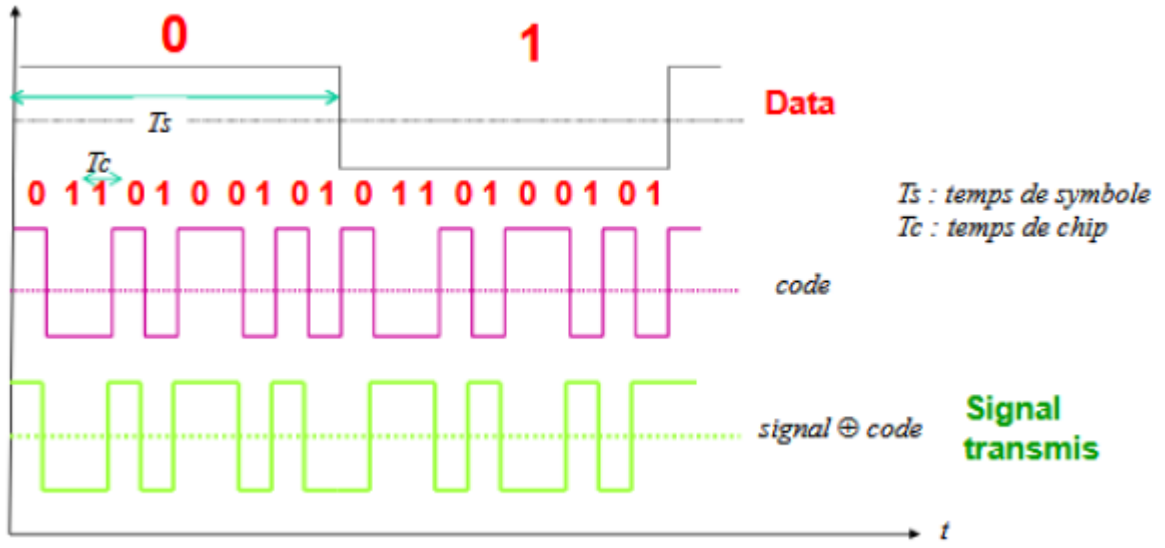


Figure 2.4: Diagramme du codage des données d'un utilisateur.

Le CDMA offre la possibilité de transmettre simultanément des données aux différents utilisateurs sur une même bande de fréquence et en même temps.

2.5 Le but d'étalement de spectre

Pourquoi étaler le spectre ?

L'étalement de spectre est une technique basée sur l'élargissement de la bande spectrale d'un signal par une multiplication de la largeur de son occupation spectrale par une quantité appelée gain de codage.

Théoriquement, pour chaque milieu de transmission, la capacité du canal C en [b/s], exprimée à partir de la bande passante du canal [0, W] et du rapport signal/bruit (SNR) est donné, conformément au théorème de Shannon-Hartley, par :

$$C = B \log_2(1+SNR) \tag{2.2}$$

Cette équation donne un taux de transfert maximum pour un Taux d'Erreur Binaire (TEB) nul à la condition qu'un procédé de codage adapté soit mis en œuvre, B représente la bande Passante du canal en Hertz et SNR représente le rapport signal/bruit.

Par conséquent, la capacité maximale peut être augmentée en agissant d'une part sur la largeur de bande de manière linéaire et/ou sur le rapport SNR de façon logarithmique.

Pour une capacité maximale donnée (souhaitée), il est possible de réduire la bande passante et/ou de diminuer le rapport signal/ bruit en admettant un TEB non nul.

Dans le cas du CDMA le bruit provient principalement des autres utilisateurs dont on cherche toujours à accroître le nombre. Un système CDMA fonctionne avec de faibles rapports signal à bruit. Cela est rendu possible par la large bande passante, l'équation:

$$\frac{C}{B} = \frac{1}{\ln(2)}.\ln(1+SNR) = 1.443\ln(1+SNR) \tag{2.3}$$

L'étalement du spectre permet un rapport SNR très faible, la puissance de signal peut être inférieure au niveau de bruit .Pour un SNR<<1 :

$$\frac{C}{B} \approx 1.443 \quad (SNR) \qquad \text{Et par approximation : } \frac{C}{B} \approx (SNR) \tag{2.4}$$

La dépendance de la capacité relativement au rapport signal/ bruit est maintenant linéaire.

Les autres signaux étalés sur le même support sont considérés comme du bruit.

2.6 Propriétés des codes orthogonaux

- ✓ L'orthogonalité est parfaite pour des signaux synchronisés.
- ✓ L'étalement n'est pas homogène mauvaises propriétés pour des signaux non synchronisés.
- ✓ mauvaise résolution temporelle pour le RAKE (Récepteur multi-trajet).
- ✓ le nombre de codes est relativement faible: ne peut pas être utilisé pour plusieurs sources, car on retombe sur un problème de planification de codes, au lieu de planifier des fréquences.
- ✓ l'orthogonalité garantie les zéro interférences entre les canaux.

2.7 Méthodes de séparation des utilisateurs dans un système DS-CDMA

Il y a deux méthodes pour séparer les utilisateurs dans un système DS-CDMA :

- ✓ Accès multiple orthogonal (utilisé dans les systèmes DS-CDMA synchrones à l'aide de codes orthogonaux)
- ✓ Accès multiple non orthogonal (utilisé dans les systèmes DS-CDMA asynchrones à l'aide des codes non orthogonaux)

2.7.1 Notion d'orthogonalité des codes [9][16]

Dans le cas général, on dit que deux signaux périodiques de période T sont orthogonaux quand la valeur de leur fonction d'inter-corrélation est nulle pour un décalage de temps nul:

$$\int_0^I S_1(t)S_2(t)dt = 0 \qquad (2.5)$$

Donc deux codes c 1(n) et c 2(n) de longueur N (c'est à dire de période (NTc) sont dits orthogonaux si on a : $\sum_{n=0}^{N-1} C_1(n)C_2(n) = 0$

(2.6)

Si un ensemble de codes ne satisfait pas à l'égalité précédente, ces codes sont dits non orthogonaux.

2.7.2 Propriétés d'auto-corrélation

La fonction d'auto-corrélation d'un code c quelconque est définie comme l'ensemble de nombre de conformité moins le nombre de différence dans une comparaison terme à terme pour une période entière du code avec une version décalée du code lui-même, en fonction du retard τ [17].

$$Rc(\tau) = \int_{-NcTc/2}^{NcTc/2} c1(t+\tau).c2(t+\tau)dt \qquad (2.7)$$

Idéalement, cette fonction d'auto-corrélation devrait être semblable à celle du bruit blanc : maximale quand il n'y a pas de décalage, et nulle autrement. Elle traduit donc, l'aptitude du code à combattre efficacement les effets des propagations par trajets multiple, étant donné que ceux-ci introduisent des images du signal original mais décalées dans le temps (retard).

2.7.3 Propriétés d'inter-corrélation

C'est la mesure de la conformité entre 2 codes différents ci et cj. Quand cette fonction Rc (τ) prend la valeur zéro pour tout τ, les codes sont dits orthogonaux. La fonction d'inter-corrélation décrit donc l'interférence entre les codes c_i et c_j :

$$R_c(\tau) = \int_{-N_c T_c/2}^{N_c T_c/2} c_i(t).c_j(t+\tau)dt \qquad (2.8)$$

Idéalement, cette fonction ne devrait avoir une valeur non nulle que pour i = j. Cette fonction traduit donc l'aptitude du code considéré à combattre les interférences introduites par les autres codes employés dans le système.

2.8 Les codes d'étalement utilisent dans un système DS-CDMA

Les codes orthogonaux consistent en un ensemble de séquences dans lequel toutes les inter-corrélations par paires sont nulles. Un tel ensemble est caractérisé par l'égalité suivante :

$$\sum_{K=0}^{M-1} Q_i(K\tau)Q_j(K\tau) = 0 \ \ pour \ \ i \neq j \qquad (2.9)$$

M : est la longueur de chaque séquence de l'ensemble.

Q_i et Q_j : Sont les i^e et j^e membres de l'ensemble.

τ : est la durée d'un bit.

Remarque : les systèmes CDMA reposent à la fois sur des codes orthogonaux de longueurs variables et de longueurs fixes. Chaque utilisateur mobile emploie une des séquences de l'ensemble comme code d'étalement, donnant lieu à une inter-corrélation nulle entre tous les utilisateurs.

2.8.1 Les codes utilisés pour l'accès multiple orthogonal [10][12][18]

2.8.1.1 Le code de Walsh

Les codes de Walsh sont les codes orthogonaux les plus couramment utilisés avec CDMA. Un ensemble de codes de Walsh de longueur n comprend les n lignes d'une matrice de Walsh ' w ', soit n codes de longueur n. La matrice de Walsh est définie récursivement comme suit :

$$W_1 = (0) \qquad W_n = \begin{pmatrix} W_{\frac{n}{2}} & W_{\frac{n}{2}} \\ W_{\frac{n}{2}} & \overline{W}_{\frac{n}{2}} \end{pmatrix}$$

n : est la dimension de la matrice de walsh W_n.

$W_{\frac{n}{2}}$: matrice de dimension $\frac{n}{2}$.

$\overline{W}$ représente le complément logique de W et W (1)=0 [11][18]

Le 4ième quadrant $\overline{W}_{\frac{n}{2}}$ de la matrice W_n est représenté avec une barre, cette dernière représente la négation logique des bits de la matrice $W_{\frac{n}{2}}$. Autrement dit $\overline{W}_{\frac{n}{2}}$ est le complément de $W_{\frac{n}{2}}$.

Exemple : matrices de walsh de dimension 2, 4, 8

$W_1 = (0)$

(a) 1 x 1

$$W_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \qquad W_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \qquad W_8 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

(b) 2 X 2 (c) 4 X 4 (d) 8 X 8

Remarque : dans chaque cas (b, c, d), la 1ière ligne de la matrice ne comprend que des 0 et les autres lignes comprennent n/2 Zéro et n/2 un.

Les codes sont donnés par les lignes de la matrice. Il résulte de cette définition par exemple que :

$$W_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Ces séquences peuvent être représentées sous forme bipolaire par un simple remplacement des valeurs [0,1] par les valeurs [-1 , +1].

$$W_4 = \begin{bmatrix} -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$$

Ces séquences ont l'avantage d'être parfaitement orthogonales et elles permettent donc de s'affranchir des interférences d'accès multiples lorsque la synchronisation entre l'émetteur et le récepteur est parfaite [18].

La fonction d'autocorrélation ne comporte pas un pic unique ce qui complique la synchronisation. La fonction d'intercorrélation soit égale à zéro. Par conséquent l'intérêt d'utiliser des codes orthogonaux est perdu lorsque tous les utilisateurs ne sont pas synchronisés sur la même horloge.

Il va donc falloir synchroniser les données avec les séquences sur une même base de temps et avoir un nombre entier de séquences pour conserver les propriétés d'orthogonalité des fonctions de Walsh et récupérer toute l'information.

2.8.1.2 Codes Hadamard [12] [18]

Les séquences d'étalement de Hadamard sont des séquences binaires orthogonales qui se construisent récursivement à partir d'une matrice 2x2 de la manière suivante :

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad H_{2n} = \begin{bmatrix} H_{2(n-1)} & H_{2(n-1)} \\ H_{2(n-1)} & -H_{2(n-1)} \end{bmatrix}$$

2.8.2 Les codes utilisés pour l'accès multiple non orthogonal [10] [18]

2.8.2.1 Les codes OVSF

Ce sont des codes orthogonaux a facteur d'étalement variable (OVSF : Orthogonal Variable Spreading Factor). Ils sont utilisés pour séparer les différents canaux physiques d'un utilisateur. L'utilisation de ces codes OVSF permet de modifier le facteur d'étalement, même si ces derniers sont de longueurs différentes. Les codes OVSF ont les propriétés suivantes :

- Les séquence sont rigoureusement orthogonales (c'est-`a-dire que l'inter-corrélation entre deux séquences de code est nulle),
- Les séquences ne sont pas toutes de même longueur, ce qui différent gain de traitement, en fonction du débit des données à transmettre.

Les codes OVSF sont appelés codes de Walsh puisqu'ils sont générés en appliquant La transformée de Walsh-Hadamard définie par :

$$H_1 = (1) \qquad H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}$$

On peut ainsi facilement se rendre compte que deux séquences situées au même niveau hiérarchique de l'arbre sont parfaitement orthogonales lorsqu'elles sont alignées.

En revanche, deux codes situent sur une même branche de l'arbre, l'un étant, par exemple, le fils de l'autre, ne sont pas forcément orthogonaux. Il en résulte qu'un code C2n,i de l'arbre ne peut être utilisé que si aucun autre code appartenant aux sous branches générées à partir de C2n,i n'est utilisé. Cette contrainte est nécessaire pour Maintenir l'orthogonalité entre les codes utilises par le système de transmission. Cette contrainte a l'inconvénient de limiter le nombre de codes utilisables. Ainsi, si on utilise les huit codes de SF=8, plus aucun code de l'arbre ne peut être alloue.

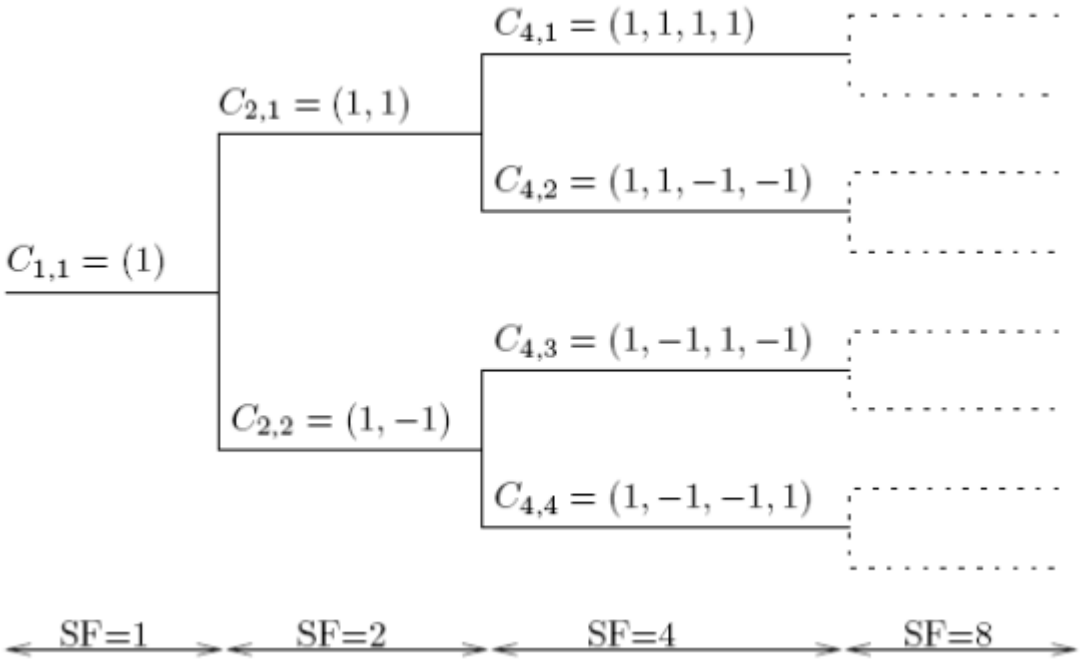


Figure 2.5 : Arbre des codes d´étalement pour générer les codes OVSF.

2.8.2.2 Les séquences de Kasami

Un autre ensemble important de séquences aléatoires réunit les séquences de Kasami, lesquelles servent dans certains systèmes de 3ième génération. Elles sont définies par une procédure analogue à celle utilisée pour les codes de Gold. Il existe des petits et des grands ensembles de Kasami :

- ✓ **les petits ensembles de Kasami**

pour n pair, nous pouvons générer un petit ensemble contenant $M=2^{n/2}$ séquences distinctes chacune de période $N=2^n-1$.

Un ensemble est définie en débutant par une ML-séquence (a) de période N et en procédant à une décimation avec $a'=2^{n/2}+1$, il en résulte une séquence (a') de période $q=2^{n/2}-1$. Nous répliquons ensuite une seule période de (a'q) fois pour produire une séquence de longueur $N = (2^{n/2}+1)(2^{n/2}-1)$.

Enfin nous gênerons l'ensemble de kasami en combinant par XOR N bits de a et N bits a' ainsi que tous les résultats des $2^{n/2}-1$ étapes de décalages des bits de (a').

- ✓ **les grands ensembles de kasami**

Un grand ensemble de kasami inclut à la fois des séquences de Gold et le petit ensemble de kasami en tant que sous ensemble.

On définit un tel ensemble en commençant par la génération d'une ML séquence (a) de période N, suivie de sa décimation avec $2^{n/2}+1$ pour former (a') et d'une autre décimation $2^{n+2/2}+1$ pour former L'ensemble est ensuite forme en combinant par XOR (a), (a')et (a'') avec diffèrent décalages de (a') et (a'').

2.9 Conclusion

Le choix de la famille des codes d'étalement de spectre est très important dans la mesure où ils possèdent des propriétés de corrélation et d'orthogonalité différentes. En effet, pour qu'une famille de codes soit utilisée dans un environnement à accès multiple comme le CDMA ils doivent lutter efficacement contre les interférences engendrées par les différents utilisateurs et cela est assuré par les bonnes propriétés d'auto et d'inter-corrélation.

Chapitre 3 :

Cryptage par le chaos

Chapitre 3 :

Cryptage par le chaos

3.1 Introduction

De nos jours, dans le langage commun « Chaos » décrit un état de désordre et d'irrégularité. Dans le langage scientifique le terme « chaos » définit l'état d'un système dynamique dont le comportement ne se répète jamais, qui est très sensible aux conditions initiales et impossibles à prédire sur le long terme. Dans le siècle passé, plusieurs chercheurs se sont intéressés aux comportements inhabituels des systèmes dynamiques non linéaires et on à découvert que certains systèmes présentaient des instabilités de nature très étrange, cela fait la découverte des signaux chaotiques qui ont un comportement complètement déterministe mais qui font penser à des allures pseudo-aléatoires. Ce concept a émergé dans la seconde partie des années 1970 en tant que science des phénomènes non linéaires complexes montrant certaines caractéristiques communes [19].

Il faut aussi noter que le comportement chaotique observé dans le temps n'est dû, ni à une source extérieure de bruit, ni à un degré infini de liberté, ni à un caractère stochastique, autrement dit ce comportement est intrinsèque. Le concept moderne du chaos déterministe est de plus en plus utilisé dans des contextes scientifiques, on peut ainsi trouver le chaos dans plusieurs domaines d'application comme les mathématiques, la physique, la chimie, la biologie.

3.2 Définition du Chaos

Le chaos tel que les scientifique le comprend ne signifie pas l'absence d'ordre; il se rattache plutôt à une notion d'imprévisibilité, d'impossibilité de prévoir une évolution à long terme du fait que l'état final dépend de manière si sensible de l'état initial [19][8].

Le terme «chaos» définit un état particulier d'un système dont le comportement ne se répète jamais, très sensible aux conditions initiales et imprédictible à long terme. Le chaos apparaît pour la première fois dans l'étude des systèmes dynamiques non linéaires. Dès lors, des chercheurs d'horizons divers ont alors commencé à s'intéresser à des problèmes non linéaires jusqu'alors restés sans solution parce qu'imprédictibles et regroupés sous la

dénomination de chaos. Le chaos a ainsi trouvé de nombreuses applications dans les domaines tant physique que biologique, chimique ou économique, toutefois, ce sont les circuits électriques et surtout électroniques qui vont jouer un rôle important dans la tentative de compréhension du phénomène chaotique et d'élaboration des propriétés du chaos [20].

Les chercheurs et en particulier les ingénieurs, considèrent ce phénomène comme perturbateur et à l'origine des défaillances des systèmes qu'ils conçoivent. Ils s'intéressent donc d'abord à le contrôler afin de le modifier.

Une fois ces phénomènes mieux connus et mieux expliqués grâce aux ordinateurs, l'intérêt est par la suite porté sur la possibilité d'utiliser les signaux chaotiques dans les systèmes de communications sécurisées. Des études sont ainsi menées dans le but d'obtenir des générateurs de chaos générant des signaux de plus en plus complexes. Ces études sont menées dans le cadre de la théorie des systèmes dynamiques.

3.3 Caractéristiques du système chaotiques

a) Sensibilité aux conditions initiales

Tout d'abord, ils sont extrêmement sensibles aux perturbations. On peut illustrer ce fait par l'effet papillon. Popularisé par le météorologue Edward Lorenz, Le papillon de Lorenz possède une caractéristique importante : quelles que soient les valeurs initiales choisies, on obtient toujours comme représentation graphique un objet géométrique dont la forme ressemble à un papillon. Deux conditions initiales différentes même très rapprochées produiront deux tracés totalement différents, donc l'évolution d'un système dynamique chaotique est imprédictible en ce sens qu'elle est sensible aux conditions initiales. Ainsi, deux trajectoires de phases initialement voisines s'écartent toujours l'une de l'autre, et ceci quelle que soit leur proximité initiale [21]. Il est en particulier clair que la moindre erreur ou simple imprécision sur la condition initiale interdit de décider à tout temps quelle sera la trajectoire effectivement suivie et, en conséquence, de faire une prédiction autre que statistique sur le devenir à long terme du système. Ainsi, bien que l'on traite de systèmes déterministes, il est impossible de prévoir à long terme leurs comportements. La seule manière est d'opérer effectivement l'évolution du système. Si cette simulation se fait informatiquement, un problème de précision sur les conditions initiales se pose alors : de petites erreurs d'arrondissement dues à la précision du type de la variable codant ces conditions initiales peuvent exponentiellement s'amplifier de telle sorte que la trajectoire de phases obtenue n'est pas représentative de la réalité.

Illustrons ce phénomène de SCI par une simulation numérique. On affecte à un système chaotique deux conditions initiales très proches. Dans un premier temps, les deux systèmes évoluent de la même manière ; mais, très vite, leur comportement devient différent. Ceci est illustré dans la figure suivante.

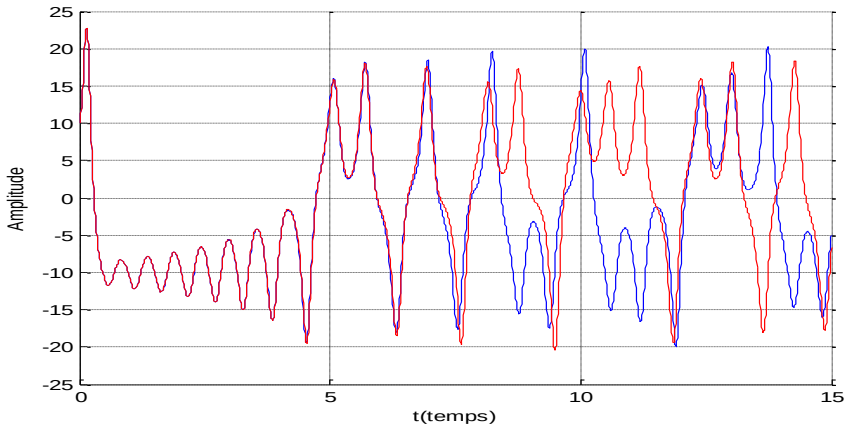


Figure 3.1: Évolution dans le temps pour deux conditions initiales très proches.

b) Aspect aléatoire

Les courbes précédentes (Figure 3-1) illustrent la sensibilité aux conditions initiales. Cependant, une autre caractéristique des systèmes chaotiques peut être observée sur les courbes précédentes.

En effet, un système chaotique évolue d'une manière qui semble aléatoire. La courbe suivante permet de comparer une évolution simple, périodique et donc prédictible d'un système classique avec l'évolution plus complexe, non périodique et non prédictible d'un système chaotique. [22]

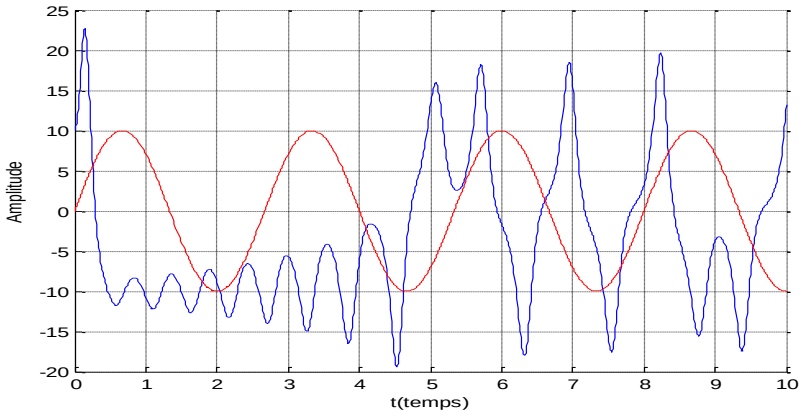


Figure 3.2: Évolution dans le temps d'un système chaotique, comparé à une sinusoïde.

.

C) Systèmes Chaotiques Et Méthode De Lyapounov

Lyapounov [23] [24], dans ses études, s'attachait à déterminer si une solution pour un système dynamique pouvait être stable ou non pour tous les temps d'observation. La méthode habituelle pour étudier la stabilité, par exemple la stabilité linéaire, ne convenait pas par le fait de l'existence d'une sensibilité aux conditions initiales. Lyapounov s'est donc intéressé à définir une autre méthode permettant d'établir ou non cette stabilité en étudiant notamment les divergences dues aux erreurs par l'étude des divergences entre les orbites du système.

Les exposants de Lyapounov mesurent le taux de divergence des orbites voisines et Lyapounov a démontré qu'il y avait en fait autant d'exposants qu'il n'y avait de dimensions dans l'espace de phase du système étudié. Par ailleurs, parmi les exposants retenus pour un système donné, on a l'habitude de prendre généralement l'exposant le plus élevé.

D'une manière générale, Lyapounov part de la formule suivante :

$$\left|\frac{E_n}{E_0}\right| = \left|\frac{E_n}{E_{n-1}}\right|\left|\frac{E_{n-1}}{E_{n-2}}\right|\cdots\left|\frac{E_1}{E_0}\right| \quad \text{D'où} \quad \frac{1}{n}\ln\left|\frac{E_n}{E_0}\right| = \frac{1}{n}\sum_{k=1}^{n}\left|\frac{E_k}{E_{k-1}}\right| \tag{3.1}$$

Le terme $\left|\frac{E_k}{E_{k-1}}\right|$ décrit en fait combien une petite erreur E_k en x_k, soit la $k^{ième}$ itération, est augmentée ou diminuée dans l'itération suivante. L'amplification est d'ailleurs dépendante de la taille de l'erreur. Lyapounov a découvert ensuite que cette erreur tendait vers une limite dont la formule est la suivante :

$$\lambda(x_0) = \lim_{x\to\infty}\frac{1}{n}\sum_{k=1}^{n}\ln\left|f'(x_{k-1})\right| \tag{3.2}$$

Si $\lambda < 0$: l'orbite est attractive vers un point fixe ou une orbite périodique stable. Il caractérise les systèmes dissipatifs. Ce type de système exhibe une stabilité asymptotique ; de plus l'exposant est négatif, plus la stabilité n'est grande. Les points fixes et points périodiques super stables ont un exposant de Lyapounov λ qui tend vers $-\infty$.

Si $\lambda = 0$: l'orbite est un point fixe neutre. Un système physique avec un tel exposant est dit conservateur. Dans cette situation, les orbites gardent une séparation constante.

Si $\lambda > 0$: l'orbite est instable et chaotique. Tous les points voisins vont être visités. Ces points sont dits instables. Pour un système discret, on a un ensemble de points avec aucun rapport de liaison. Pour un système continu, l'espace de phase est un ensemble de lignes croisées.

Dans le tableau suivant nous allons présenter la classification des régimes permanents en fonction du spectre Lyapounov :

Régime permanent	**Attracteur**	**Spectre**	**Exposants Lyapounov**
point d'équilibre	point	Composante continue	$0 > \lambda_1 \geq .... \geq \lambda_n$
périodique	Courbe fermée	Fréq. Fondamentale +harmoniques entières	$\lambda_1 = 0$ $0 > \lambda_2 \geq ... \geq \lambda_n$
Quasi-périodique	tore	Composantes fréquentielles en rapport irrationnel	$\lambda_1 = ... = \lambda_i = 0$ $0 > \lambda_{i+1} \geq ... \geq \lambda_n$
chaotique	fractale	Spectre large	$\lambda_1 > 0$ $0 \geq \lambda_2 \geq ... \geq \lambda_n$

Tableau (1.1) : Classification des régimes permanents en fonction du spectre Lyapounov [23].

3.4 La Différence entre Chaos et les paramètres aléatoires

La différenciation entre chaotique et aléatoire nous a paru le point le plus important de la compréhension du chaos. En effet, on a toujours tendance à considérer qu'un phénomène tire son imprédictibilité du nombre trop importants de paramètres en jeu dans sa description, ce qui nous pousse à en donner une approche probabiliste qui, pour être parfaitement satisfaisante, garde par définition une marge d'aléatoire. Le mouvement Brownien en est un exemple, ce mouvement n'est pas chaotique mais aléatoire, c'est-à-dire qu'il réagit par une loi probabiliste [25].

Quant au phénomène chaotique qui est décrit de manière déterministe, c'est-à-dire avec des outils mathématiques qui devrait permettre une approche précise et a priori certaine. On constate même qu'il n'y a rien qui lie le chaos et l'aléatoire puisque même une approche probabiliste de l'évolution d'un système chaotique n'aboutirait à rien.

3.5 Techniques De Cryptage Par Le Chaos

L'utilisation du chaos pour sécuriser les informations est venue à base de ses caractéristiques et de son comportement. Comme on a vu que le chaos déterministe génère des comportements dynamiques d'apparence aléatoires, donc il était possible d'utiliser ce phénomène comme porteur d'information en télécommunication.

Le principe de chiffrement par chaos consiste à transmettre un message à travers un signal chaotique d'un émetteur vers un récepteur connaissant les conditions initiales pour extraire le message original [22][25].

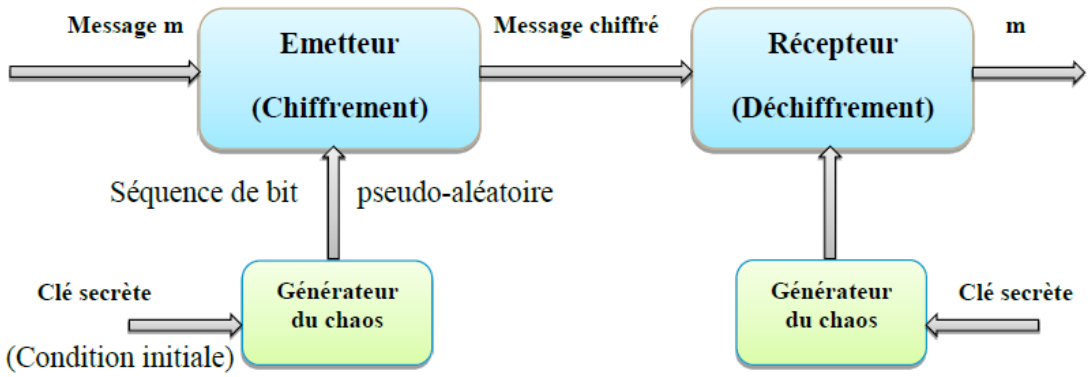


Figure 3.3 : Principe de la communication sécurisée à base du chaos.

Le chiffrement par chaos qui est le masquage, cette méthode consiste à cacher un signal d'information dans un signal chaotique ayant un spectre plus répandu et qui a une allure pseudo-aléatoire. On va cacher le message C dans un signal chaotique dont la formule sera : $y = x + C$, Le message C serra difficile à déchiffré lors de son trajet sur le canal public.
A la réception on verra que le récepteur connaisse les conditions initiales et il va déchiffrer facilement le message original.

Depuis les techniques de cryptage par le chaos ont gagné en performance au prix d'une plus grande complexité, on trouve dans la littérature plusieurs techniques avancées pour le cryptage de l'information par le chaos, les plus souvent rencontrées sont :

- Cryptage par addition (masquage chaotique).
- Cryptage par commutation.
- Cryptage par inclusion.

3.5.1 Cryptage par addition

La première et la plus simple des méthodes de cryptage, illustrée dans la figure, développé en 1993. Elle consiste en deux systèmes chaotiques identiques, l'émetteur et le récepteur.
Le signal chaotique c(t) est l'une des variables d'état du système dans l'émetteur.

Le message d'information (le signal utile qui doit être crypté) m(t), qui est très faible devant c(t), est ajouté au signal c(t) et donne le signal transmis s(t), Comme c(t) est très complexe et m(t) est beaucoup plus petit que c(t), alors il est difficile de séparer m(t) du signal s(t) sans connaître c(t).

Le récepteur est constitué d'un système chaotique identique à l'émetteur et d'un simple soustracteur, après la synchronisation des deux systèmes chaotiques (émetteur et récepteur), le message est extrait à l'aide d'une opération de soustraction.

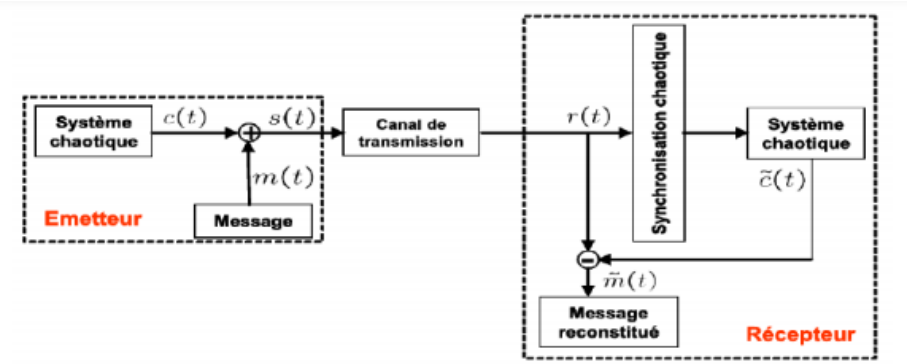


Figure 3.4 : Schéma de communication par addition.

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.

3.5.2 La méthode par inclusion

Dans cette méthode, le signal information m est inclus dans la structure du système chaotique de l'émetteur qui admet la représentation d'état suivante :

$$\begin{cases} x_{k+1} = f(x_k, m) \\ y = h(x_k, m) \end{cases} \quad (3.3)$$

Seule la sortie$y$ est transmise au récepteur, $x_k$étant un vecteur d'état interne qui n'est pas accessible.Le récepteur a pour représentation d'état générale :

$$\begin{cases} \hat{x}_{k+1} = g(\hat{x}_k, y) \\ \hat{m} = d(\hat{x}_k, y) \end{cases} \quad (3.4)$$

Le récepteur doit être synthétisé de telle sorte que l'information m puisse être reconstruite avec pour seule donnée la sortie de l'émetteur y. En effet, l'état interne x_k n'est pas directement transmis au récepteur, mais est nécessaire pour reconstruire l'information. La fonction g est choisie de telle sorte que $\hat{x}_k = x_k$, quel que soit $\hat{x}_0$ et indépendamment de l'information m qui joue le rôle d'une entrée externe au système dynamique [18].

La restauration de l'information se fait principalement par deux techniques, reposant soit sur les observateurs à entrées inconnues, soit sur l'inversion du système émetteur.

3.6 Conclusion

Dans ce chapitre, on introduit les systèmes chaotiques comme on a présenté on détail quelques techniques du cryptage chaotique. Nous avons présenté les propriétés permettant de caractériser les systèmes chaotiques, telle que la sensibilité aux conditions initiales, aspect aléatoire et l'exposant de Lyapunov.

Chapitre 4 :

Simulation et discussion des résultats

Chapitre 4 :

Simulation et discussion des résultats

4.1 Introduction

De nos jours, l'image médicale acquise dans un hôpital ou dans un centre d'imagerie peut être partagée entre plusieurs professionnels de santé afin de faciliter la prise en charge des patients et permettre l'amélioration de la gestion de l'information médicale. Ce partage est souvent effectué sur des réseaux peu sûrs, exposant l'image médicale à plusieurs menaces de sécurité, qui peuvent être exprimées en termes de pertes de données, de falsification, d'erreurs, et/ou d'attaques d'où un besoin accru en termes de sécurité.

4.2 Représentation global du système de simulation d'une transmission DS-CDMA

Pour répondre à cette problématique, dans le cadre de ce chapitre, on va s'intéressé a la simulation d'une transmission DS-CDMA avec deux utilisateurs dans le canal pour la transmission des images médicales. Le schéma global du système est représenté sur la figure suivante :

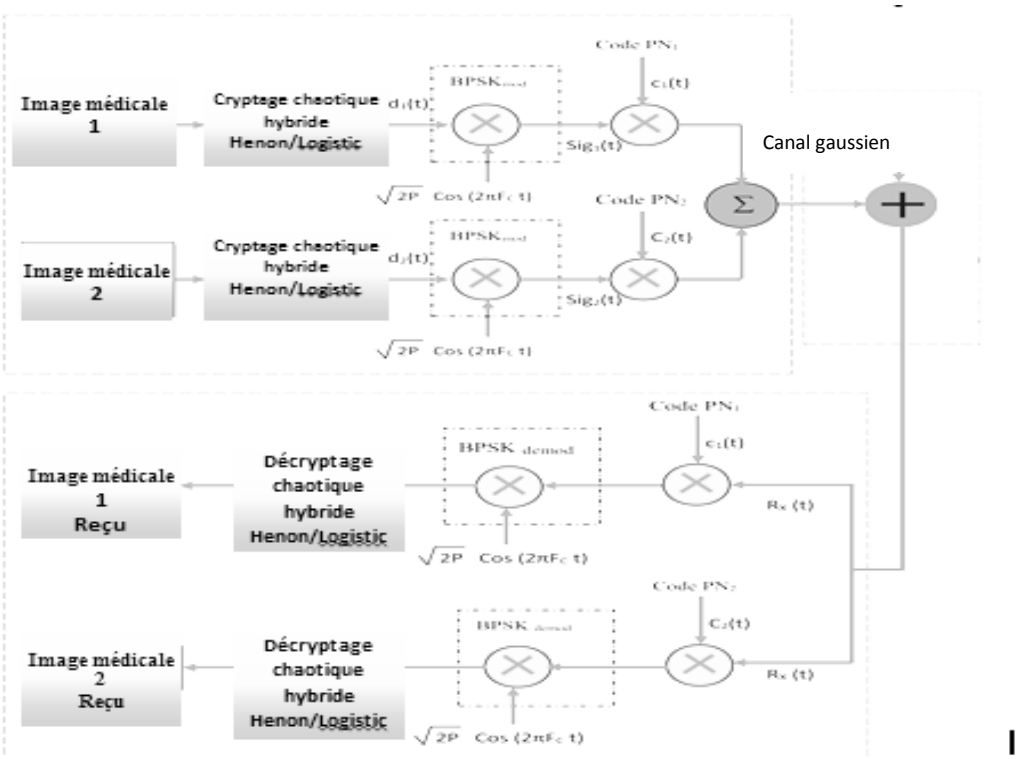


Figure 4. 1 : Schéma général de l'approche proposée.

Dans ce travail, nous modélisons un système de transmission DS-CDMA système avec deux accès. Les deux utilisateurs auront deux images médicales à transmettre à leurs correspondants. Un bloc de cryptage hybride est ajouté au niveau de chaque utilisation afin de crypter chaque image. Le principe de base de ce système de cryptage repose sur l'association du système chaotique de Hénon, de la fonction logistic et de la fonction XOR. Dans la première partie de ce chapitre, on va présenter les résultats du cryptage des deux images à transmettre.

4.3 Résultats De Simulation :

4.3.1 Résultats du cryptage d'image médicale :

A) premier utilisateur :

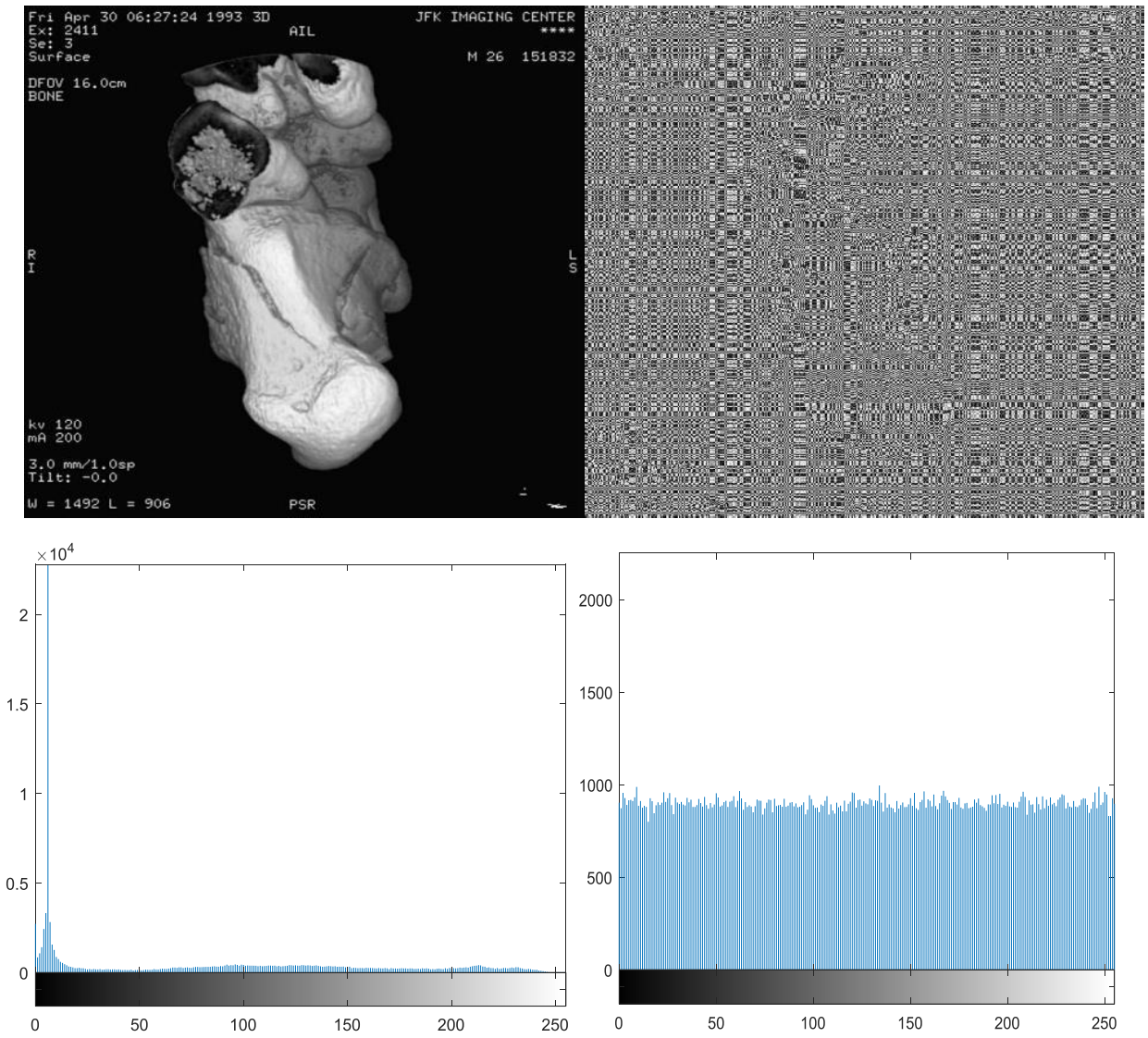


Figure 4.2 : Image original 1 et image crypté 1.

B) deuxième utilisateur :

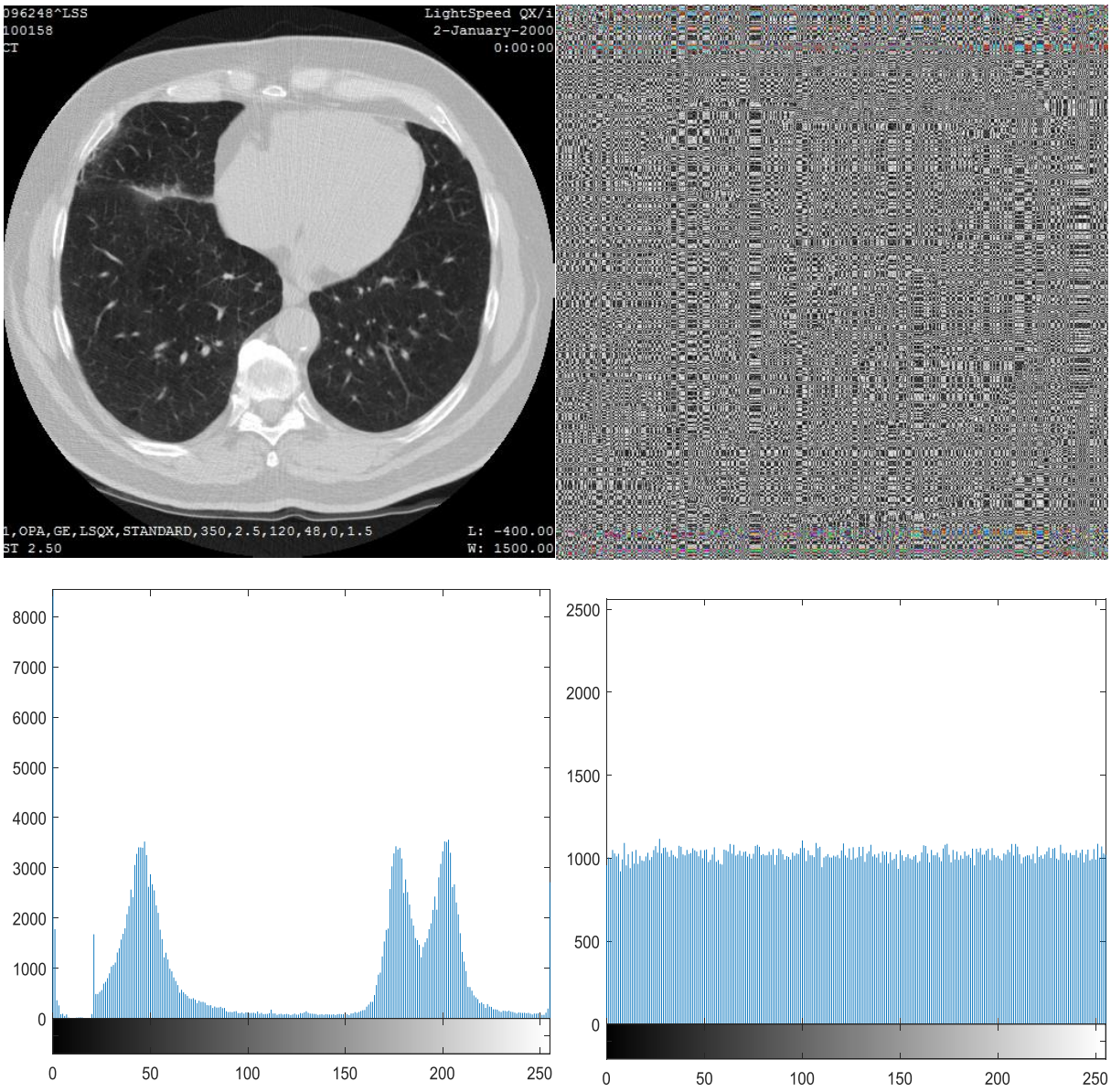


Figure 4.3 : Image original 2 et image crypté 2.

Un histogramme est la distribution des intensités des pixels d'une image, c'est-à-dire le nombre de pixels pour chaque intensité lumineuse. Les figures 4-2 et 4-3 représentent les résultats du cryptage des deux images. Nous pouvons apercevoir que la distribution des pixels des images cryptées est uniforme et considérablement différente de celle de l'image originale.

4.3.2 Présentation des résultats de simulation transmission DS-CDMA avec valeurs différentes de SNR et de N (code d'étalement) :

Dans la deuxième partie de ce chapitre, on va simuler une transmission DS-CDMA pour différentes valeurs de SNR et de la longueur du code d'étalement (N).

a) Transmission DS-CDMA avec SNR=10db :

N=8

N=16

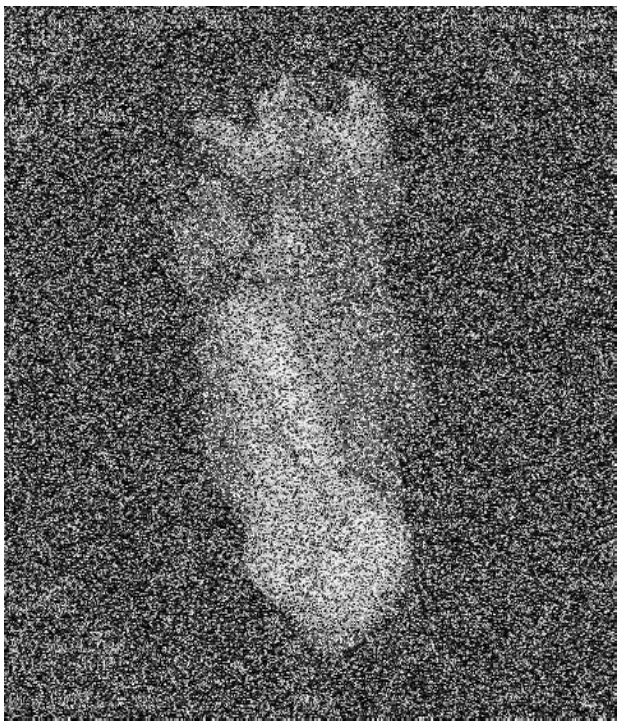
N=32

Figure 4.4 : Image 1 reçu à travers un canal gaussien avec un SNR=10db.

B) Transmission DS-CDMA premier utilisateur avec SNR=5db :

N=32

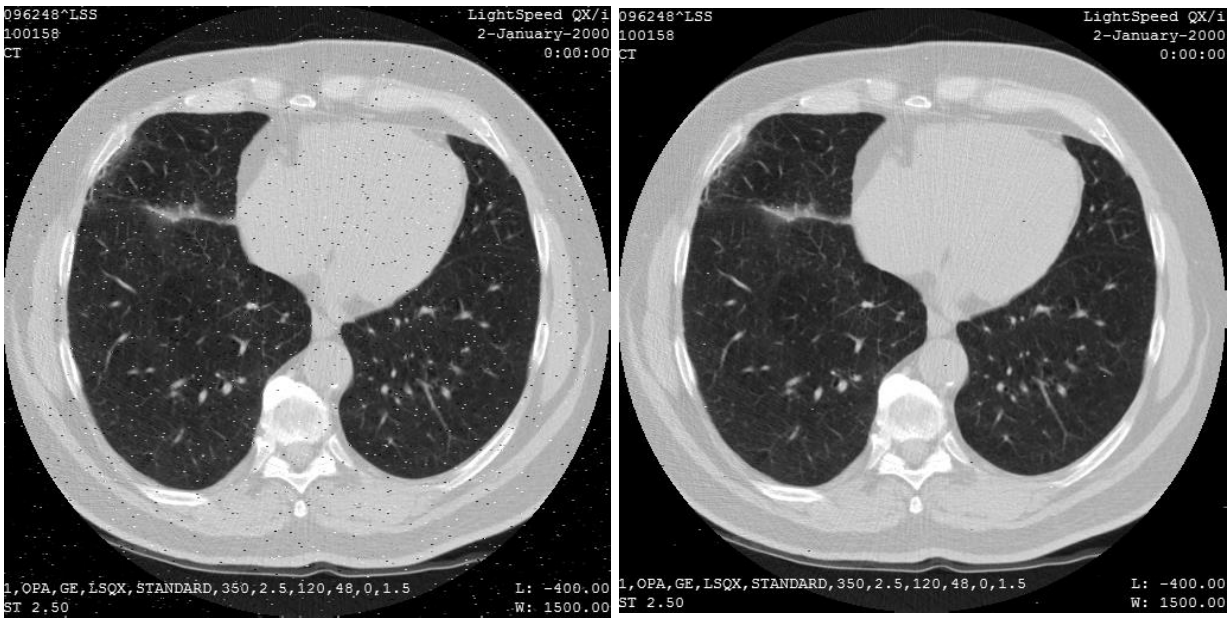
N=16



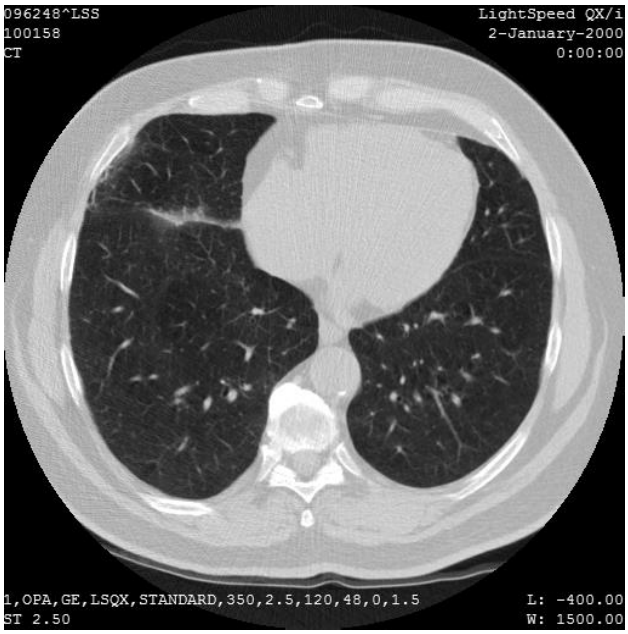
N=8

Figure 4-5 : Image 1 reçu à travers un canal gaussien avec un SNR=5db.

C) Transmission DS-CDMA deuxième utilisateur avec SNR=10 db:



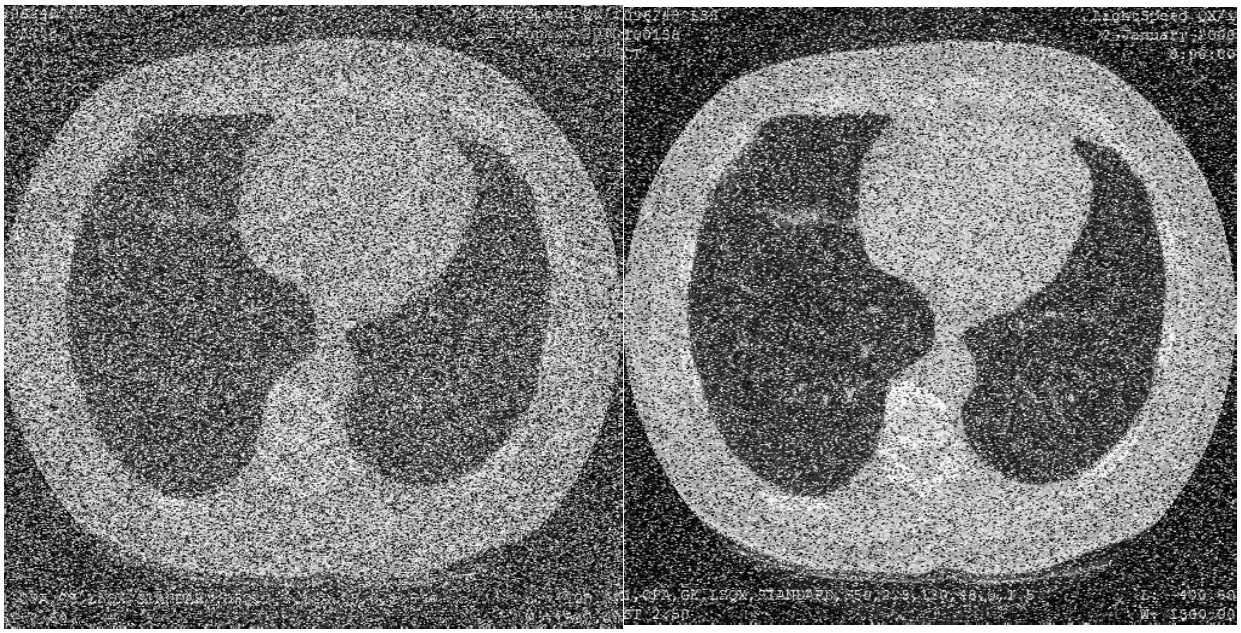
N=8 **N=16**



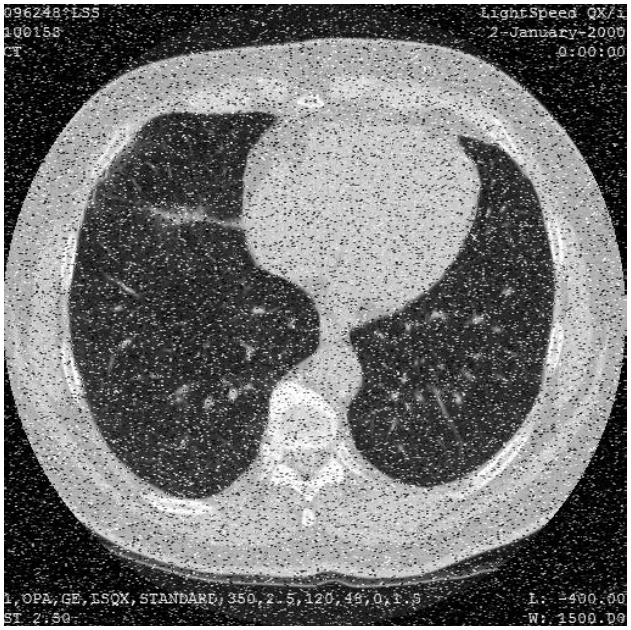
N=32

Figure 4.6 : Image 2 reçu à travers un canal gaussien avec un SNR=10db.

D) Transmission DS-CDMA deuxième utilisateur avec SNR=5db :



N=8 **N=16**



N=32

Figure 4.7 : Image 2 reçu à travers un canal gaussien avec un SNR=5db.

D’après les figures 4.4, 4.5 , 4.6 et 4.7 on remarque que le système DS-CDMA est robuste contre les bruit du canal et que à chaque fois la longueur du code d’étalement (N) augmente la qualité de l’image reçu augmente aussi.

4.4 Conclusion

Dans ce chapitre, nous avons présenté les différents résultats de simulation de l’approche proposée comme nous avons pu le voir, le système de cryptage assure un bon chiffrement d’information et le système DS-CDMA est une bonne technique pour la transmission des images surtout dans le cas d’un canal bruité ce qui se traduit par une diminution du taux d’erreur et une amélioration des performances du système DS-CDMA.

Conclusion générale

L’objectif de ce mémoire est l’étude d’une transmission sécurisée d’information (image couleur ou médicale) par un système DS-CDMA. Le succès de l'accès multiple par répartition de code (CDMA) dans les réseaux cellulaires a entraîné un intérêt grandissant de la part des chercheurs, Ces réseaux CDMA offrent un certain nombre d'avantages, tels que la transmission asynchrone, le potentiel d'une sécurité accrue, le contrôle de la qualité du service, etc., qui permettent au réseau de répondre aux exigences de flexibilité, d'évolutivité, d'efficacité et donc de rentabilité.

Les performances d'un tel système dépendent donc du choix du ou des codes utilisés. Les codes d'étalement les plus utilisés dans un système DS-CDMA sont indiqué.
Les propriétés de chaque code permettent donc de les suggérer pour des usages spécifiques dans un système DS-CDMA, de plus les codes orthogonaux permettent d'avoir de meilleures performances en termes de capacité du réseau de téléphonique.

Dans le premier chapitre, nous avons abordé la technique du multiplexage par séquence direct DS-CDMA et ses performances dans la transmission de l’information.
Dans le deuxième chapitre, nous avons détaillé les séquences d’étalements, les différents codes d’étalement du spectre par séquence directe et les codes orthogonaux tels que le code de Walsh -Hadamard et les code non- orthogonaux tel que les codes OVSF et Kasami .

Tandis que dans le troisième chapitre, nous avons abordé les systèmes chaotiques et les techniques de cryptage.

Dans le dernier chapitre, on a exposé les résultats de simulation. Ces résultats illustrent les performances du système de transmission étudié pour la transmission des images médicales.
Comme suite à ce travail on propose l’implémentation de l’approche étudier sous carte FPG pour une applications temps-réel.

Bibliographie

[1] S. Renaud *« Etude des Potentialités du Chaos pour les systèmes de Télécommunications, Évaluation des performances de systèmes à accès Multiples à répartition par les Codes (CDMA) séquences d'étalement Chaotique* » Thèse université de Limoges /2001.

[2] A. Tanenbaum, "*Réseaux*/ Dunod / Prentice Hall, Article Universitaire de Londres 1997.

[3] A.B. Zer & E. Akin « *Tools For Dectecting Chaos » Institut des Sciences et Technologies*», Université Sakarya, Jornal 9 Cilt, 1 Say1, Turquie /2005.

[4] M. Lourdiane « *CDMA à séquence directe appliqué aux systèmes de communications optiques* » Thèse de Doctorat Université de Paris/2005.

[5] Kh. Melal « *Analyse des méthodes d'égalisation des techniques CDMA* » Mémoire de Master présenté à l'Université De Batna /2008.

[6] M.TEKFI REZKI et M. SAAD AMMAR « *Etude des techniques à étalement de spectre Application à la CDMA* », Mémoire de fin d'études, université Mouloud MAMMERI, Tizi-Ouzou 2008/2009.

[7] F.Bouguerra « *Contribution à l'optimisation des télécommunications dans les réseaux mobiles* » Mémoire de Magister présenté à l'université de BATNA, 2011.

[8] H. Khouildat « *Méthode de cryptage d'image basée sur la permutation et la matrice de Householder* » Mémoire de Master Présenté à l'université de Ouargla, 2019 .

[9] H.Leib «PCS Third generation CDMA systems, Study of the physical layer», McGill University – Department of Electrical and Computer Engineering, August 2001, disponible en téléchargement sur http://www.tsp.ece.mcgill.ca

[10] J.ANDRY « *LE DS-CDMA ET SES APPLICATIONS DANS LE SYSTEME DE TELEPHONIE MOBILE* », mémoire de fin d'études, université de D'Antananarivo, 2002.

[11] J.Meel, "*Spread Spectrum*", De Nayer Instituut, Belgique, Octobre 1999, disponible en téléchargement sur http://www.sss-mag.com

[12] M.DJENOURI et M-Hichem.CHIKHI « *communication sécurisé par chao*s » Mémoire de fin d'étude présenté à l'université de BLIDA /2014.

[13] M. KANDOUCI et B. KORICHI « *Data mining pour l'étude des performances du système CDMA à accès multiple* » Mémoire de master université de SAIDA 2019/2020.

[14] C . Boulanger and L . Ouvry « *Tabu search : an efficient tool for designing DS-CDMA spreading sequences* » IEEE ISSSTA 98 proceedings, 2-4 September 1998, Sun City.

[15] M.KRIM « *Implémentation des séquences chaotiques sur les systèmes de communication moderne Etalement de spectre à séquence directe DS-SS* » Thèse présenté à l'université d'Oran 2018/2019.

[16] H.DJELLAB « *Evaluation des performances de la technique CDMA dans la transmission optique* » Thèse présenté à l'université de Annaba /2018.

[17] H. Deng «*Synthesis of binary sequences with good autocorrelation and crosscorrelation properties by simulated annealing* » IEEE Transactions on Aerospatial and Electronic Systems, vol . 32, pp. 98-107, Janvier 1996.

[18] H.LARIBI et S.AISSA MADAOUI « *Etude d'un système OCDMA avec les codes Hadamard pour les signaux optiques incohérents* » université ABOU BEKR BELKAID TLEMCEN / 2016.

[19]Y.NASSER « *Sensibilité des Systèmes OFDM-CDMA aux Erreurs de synchronisation en Réception Radio Mobile*» présenté par » Thèse présenté à l'institut National Polytechnique de Grenoble – INPG / 2006.

[20] C.Morel « *Analyse et contrôle de dynamiques Chaotiques, application à des circuits électroniques non-linéaires* » Thèse de Doctorat de l'école Doctorale d' Angers /2005.

[21] YAGOUB Imad Eddine, « *Systèmes dynamiques discrets et chaos* » université du havre, Année 2010/2011, International Journal of Circuit: Theory ans Applications, vol. 24, pp. 551–579, 1996.

[22] S. BELKACEM, « *Chaos based image watermarking* », Thèse Présentée à l'université de Batna 2 en Electronique /2015.

[23] A.Berkane, « *Transmission sécurisée à base de la synchronisation impulsive de deux systèmes chaotique discrets* », Mémoire de Master en électronique industriel, Université Mouloud Mammeri Tizi-Ouzou /2016.

[24] O. Megherbi, « *Etude et réalisation d'un système sécurisé à base de systèmes chaotique* » Thèse de magister, Université Mouloud Mammeri Tizi-Ouzou /2013.

[25] A.Amirouche, L.Bourahmoune, «*Conception et étude d'un système de transmission sécurisée de données à base d'un système chaotique d'ordre fractionnaire*» Mémoire de Fin d'Etudes de Master, Université Mouloud Mammeri de Tizi-Ouzou /2015.

Résumé

Depuis quelques années, le besoin de systèmes de communications plus rapides et plus sures se fait sentir. Le partage entre utilisateurs de la très grande bande passante nécessite des techniques d'accès adaptées. Afin de répondre à ces besoins, un certain nombre de techniques de multiplexage, dont le CDMA ont été développées.

Dans ce travail, nous avons étudié un système de transmission sécurisé des images médicale par DS-CDMA, le choix de ce système de transmission est dû au fait que le CDMA est robuste contre les bruits du canal et offre la possibilité de transmettre plusieurs images en même temps, Les résultats de simulations montrent clairement l'efficacité de l'approche présenter.

Mots clefs : système chaotique, multiplexage CDMA, étalement du spectre, chiffrement, sécurisation de l'information.

ملخص:

وفي السنوات الأخيرة، كانت هناك حاجة إلى نظم اتصالات أسرع وأكثر أمانا. يتطلب مشاركة عرض النطاق الترددي العالي جدا بين المستخدمين تقنيات وصول مكيفة. ولتلبية هذه الاحتياجات، تم تطوير عدد من التقنيات المتعددة، بما في ذلك CDMA.

في هذا العمل، درسنا نظام آمن لنقل الصور الطبية من قبل DS-CDMA، واختيار هذا النظام انتقال يرجع إلى حقيقة أن CDMA قوية ضد ضجيج القناة، ويقدم إمكانية نقل عدة صور في نفس الوقت، ونتائج المحاكاة تظهر بوضوح فعالية النهج الحالي.

الكلمات المفتاحية : نـظـام الفوضى ، CDMA تعدد ، انتشار الطيف ، والتشفير ، وأمن المعلومات.

Abstract: In recent years, the need for faster and safer communications systems has been felt. Sharing the very high bandwidth between users requires adapted access techniques. In order to meet these needs, a number of multiplexing techniques, including CDMA have been developed.

In this work, we studied a system of secure transmission of medical images by DS-CDMA, The choice of this transmission system is due to the fact that the CDMA is robust against the noises of the channel and offers the possibility of transmitting several images at the same time, The results of simulations clearly show the effectiveness of the approach present.

Keywords: Chaos system, CDMA multiplicity, spectrum spread, encryption, and information security.