الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahleb – Blida

Institut D'Aéronautique et des études spatiales

Département des études spatiales

جامعة سعد دحلب- البليدة

معهد الطيران و الدراسات الفضائية

قسم الدراسات الفضائية

Mémoire présenté en vue de l'obtention du diplôme de

Master académique en télécommunications spatiales

Thème :

Etalement de spectre par la séquence carte logistique et son application dans le système de communication DS-SS

Proposée et encadré par :
Dr KRIM Mohamed

Réalisé par :
Osmani Redouane
Nettari Adam

Membres de Jury :

- Mme. AZINE Houria — Présidente
- Mme. DEHOUCHE Siham — Examinatrice

Année universitaire : 2020-2021

Dédicace :

C'est avec un énorme plaisir, un cœur ouvert et une immense joie que je dédie ce modeste travail à :

- *Mes très chers et magnifiques parents qui m'ont bien soutenu et aidé tout au long de mon parcours jusqu'à en arriver jusqu'ici.*

- *« Lily », une personne très chère pour moi et qui m'a vraiment soutenu dans les moments difficiles et qui a été tout le temps présente pour me remonter le moral d'une manière ou d'une autre.*

- *Mon binôme « Adem » avec qui j'ai collaboré pour mener à bien ce modeste travail.*

- *Toutes celles et ceux qui ont contribué de près ou de loin à l'accomplissement de ce modeste travail.*

Osmani Redouane

إهداء

إلى الرائع بن دريس المتوكل على الله ...

عادة الخيبات لا تهدى و لكن (مَا عِندَكُمۡ يَنفَدُۖ وَمَا عِندَ ٱللَّهِ بَاقٖۗ وَلَنَجۡزِيَنَّ ٱلَّذِينَ صَبَرُوٓاْ أَجۡرَهُم بِأَحۡسَنِ مَا كَانُواْ يَعۡمَلُونَ)[گ: ٩٦].

من هذا المنبر **أهدي لك :**

- (وَإِن يَمۡسَسۡكَ ٱللَّهُ بِضُرّٖ فَلَا كَاشِفَ لَهُۥٓ إِلَّا هُوَۖ وَإِن يَمۡسَسۡكَ بِخَيۡرٖ فَهُوَ عَلَىٰ كُلِّ شَيۡءٖ قَدِيرٞ ۝ وَهُوَ ٱلۡقَاهِرُ فَوۡقَ عِبَادِهِۦۚ وَهُوَ ٱلۡحَكِيمُ ٱلۡخَبِيرُ)[گ: ١٧ - ١٨]
- (وَإِن يَمۡسَسۡكَ ٱللَّهُ بِضُرّٖ فَلَا كَاشِفَ لَهُۥٓ إِلَّا هُوَۖ وَإِن يُرِدۡكَ بِخَيۡرٖ فَلَا رَآدَّ لِفَضۡلِهِۦۚ يُصِيبُ بِهِۦ مَن يَشَآءُ مِنۡ عِبَادِهِۦۚ وَهُوَ ٱلۡغَفُورُ ٱلرَّحِيمُ)[گ: ١٠٧]
- (مَّا يَفۡتَحِ ٱللَّهُ لِلنَّاسِ مِن رَّحۡمَةٖ فَلَا مُمۡسِكَ لَهَاۖ وَمَا يُمۡسِكۡ فَلَا مُرۡسِلَ لَهُۥ مِنۢ بَعۡدِهِۦۚ وَهُوَ ٱلۡعَزِيزُ ٱلۡحَكِيمُ)[ے: ٢]
- (وَمَا بِكُم مِّن نِّعۡمَةٖ فَمِنَ ٱللَّهِۖ ثُمَّ إِذَا مَسَّكُمُ ٱلضُّرُّ فَإِلَيۡهِ تَجۡـَٔرُونَ ۝ ثُمَّ إِذَا كَشَفَ ٱلضُّرَّ عَنكُمۡ إِذَا فَرِيقٞ مِّنكُم بِرَبِّهِمۡ يُشۡرِكُونَ)[گ: ٥٣ - ٥٤]
- (وَإِذَا مَسَّ ٱلۡإِنسَٰنَ ٱلضُّرُّ دَعَانَا لِجَنۢبِهِۦٓ أَوۡ قَاعِدًا أَوۡ قَآئِمٗا فَلَمَّا كَشَفۡنَا عَنۡهُ ضُرَّهُۥ مَرَّ كَأَن لَّمۡ يَدۡعُنَآ إِلَىٰ ضُرّٖ مَّسَّهُۥۚ كَذَٰلِكَ زُيِّنَ لِلۡمُسۡرِفِينَ مَا كَانُواْ يَعۡمَلُونَ)[گ: ١٢]
- (وَمَا بِكُم مِّن نِّعۡمَةٖ فَمِنَ ٱللَّهِۖ ثُمَّ إِذَا مَسَّكُمُ ٱلضُّرُّ فَإِلَيۡهِ تَجۡـَٔرُونَ ۝ ثُمَّ إِذَا كَشَفَ ٱلضُّرَّ عَنكُمۡ إِذَا فَرِيقٞ مِّنكُم بِرَبِّهِمۡ يُشۡرِكُونَ)[گ: ٥٣ - ٥٤]
- (۞وَأَيُّوبَ إِذۡ نَادَىٰ رَبَّهُۥٓ أَنِّي مَسَّنِيَ ٱلضُّرُّ وَأَنتَ أَرۡحَمُ ٱلرَّٰحِمِينَ ۝ فَٱسۡتَجَبۡنَا لَهُۥ فَكَشَفۡنَا مَا بِهِۦ مِن ضُرّٖۖ وَءَاتَيۡنَٰهُ أَهۡلَهُۥ وَمِثۡلَهُم مَّعَهُمۡ رَحۡمَةٗ مِّنۡ عِندِنَا وَذِكۡرَىٰ لِلۡعَٰبِدِينَ)[ٹ: ٨٣ - ٨٤]
- (وَإِذَا مَسَّكُمُ ٱلضُّرُّ فِي ٱلۡبَحۡرِ ضَلَّ مَن تَدۡعُونَ إِلَّآ إِيَّاهُۖ فَلَمَّا نَجَّىٰكُمۡ إِلَى ٱلۡبَرِّ أَعۡرَضۡتُمۡۚ وَكَانَ ٱلۡإِنسَٰنُ كَفُورٗا)[گ: ٦٧]
- (وَإِذَآ أَذَقۡنَا ٱلنَّاسَ رَحۡمَةٗ مِّنۢ بَعۡدِ ضَرَّآءَ مَسَّتۡهُمۡ إِذَا لَهُم مَّكۡرٞ فِيٓ ءَايَاتِنَاۚ قُلِ ٱللَّهُ أَسۡرَعُ مَكۡرًاۚ إِنَّ رُسُلَنَا يَكۡتُبُونَ مَا تَمۡكُرُونَ)[گ: ٢١]
- (أَمَّن يُجِيبُ ٱلۡمُضۡطَرَّ إِذَا دَعَاهُ وَيَكۡشِفُ ٱلسُّوٓءَ وَيَجۡعَلُكُمۡ خُلَفَآءَ ٱلۡأَرۡضِۗ أَءِلَٰهٞ مَّعَ ٱللَّهِۚ قَلِيلٗا مَّا تَذَكَّرُونَ)[ہ: ٦٢]
- (يَوۡمَ يُكۡشَفُ عَن سَاقٖ وَيُدۡعَوۡنَ إِلَى ٱلسُّجُودِ فَلَا يَسۡتَطِيعُونَ ۝ خَٰشِعَةً أَبۡصَٰرُهُمۡ تَرۡهَقُهُمۡ ذِلَّةٞۖ وَقَدۡ كَانُواْ يُدۡعَوۡنَ إِلَى ٱلسُّجُودِ وَهُمۡ سَٰلِمُونَ)[□: ٤٢ - ٤٣]

Remerciements :

Nous tenons à remercier tout d'abord DIEU qui nous a donné la santé, le courage et la patience durant toutes ces années pour en arriver là.

Nous remercions très chaleureusement notre promoteur Dr. Krim Mohamed pour avoir dirigé nos travaux. Merci pour vos échanges scientifiques, vos conseils et votre rigueur.

Nous tenons à exprimer notre profonde gratitude à tous les enseignants de la spécialité et le Professeur LILA.MOUFFAK le responsable de la spécialité en particulier.

Nous remercions également tous les membres du jury pour nous avoir honoré par leur présence et pour avoir accepté d'évaluer ce travail de mémoire.

Nous tenons aussi à remercier nos parents respectifs, nos frères et amis.

Enfin, nous remercions tous ceux qui ont participé de près ou de loin à l'achèvement de ce travail.

Résumée :

Dans le monde moderne des réseaux et télécommunications, la transmission des données est très importante aussi délicate. Certains problèmes peuvent apparaitre au bout du Transfer des données en générale, pour la transmission d'une image numérique associée au niveau de sécurité des données à envoyer. Cela signifie que les données filigranées étaient moins sécurisées. Dans plus de technique de sécurité, est ajouté en utilisant une séquence de carte chaotique et une clé. Cette séquence carte chaotique présente de nombreux avantages dans les applications d'étalement étendu. Les résultats de la simulation montrent que la qualité de l'image étalée est obtenue à partir du rapport signal sur bruit de crête PSNR et de l'indice de similarité structurelle MMSIM sont l'évaluation des qualités de l'image Elatée.

Mots-clés :

Séquence de cartes chaotiques, étalée PSNR et SSIM.

Abstract:

In the modern world of networks and telecommunications, the transmission of data is very important as delicate. Some problems may appear at the end of the data transfer in general, for the transmission of a digital image associated with the level of security of the data to be sent. This meant that the watermarked data was less secure. In more security technique, is added using chaotic card sequence and key. This chaotic map sequence has many advantages in wide spread applications. The results of the simulation show that the quality of the stretched image is obtained from the peak signal to noise ratio PSNR and the structural similarity index MMSIM are the evaluation of the qualities of the stretched image.

Key words:

Chaotic map sequence spread PSNR and SSIM.

ملخص :

في عالم الشبكات والاتصالات الحديث، يعد نقل البيانات مهمًا جدًا بقدر ما هو دقيق. قد تظهر بعض المشاكل في نهاية نقل البيانات بشكل عام، لنقل صورة رقمية مرتبطة بمستوى أمان البيانات المراد إرسالها. هذا يعني أن البيانات ذات العلامة المائية كانت أقل أمانًا. في مزيد من التقنية الأمنية، يتم إضافة تسلسل البطاقة الفوضوي والمفتاح. يتميز تسلسل الخرائط الفوضوي هذا بالعديد من المزايا في التطبيقات واسعة الانتشار. تظهر نتائج المحاكاة أن جودة الصورة الممتدة يتم الحصول عليها من إشارة الذروة إلى نسبة الضوضاء

كلمات مفتاحية :

تسلسل الخرائط الفوضوي، انتشار PSNR وSSIM

Table des Matières

Chapitre 1 : Système d'étalement de spectre par chaos Dans le domaine sécurisation

Chapitre 2 : Générateur de Nombre issu de Carte Chaotique

Chapitre 3 : L'Evaluation de qualité d'image par l'Etalement de Spectre

Glossaire

- **DS-SS:** Direct-Sequence Spread Spectrum.
- **PRNG:** Pseudorandom Number Generator.
- **CPRNG:** Chaotic Pseudo Random Number Generator.
- **PSNR:** Peak Signal-To-Noise Ratio.
- **MSSIM:** Mean Structural Similarity.
- **PN:** Pseudo Noise.
- **NPWLCM:** New Piecewise Linear Chaotic Map.
- **RGB:** Red Green Blue.
- **OSI:** Open Systems Interconnexion.
- **FH-SS:** Frequency Hopping Spread Spectrum.
- **OFDMA:** Orthogonal Frequency-Division Multiple Access.
- **CDMA:** Code Division Multiple Access.
- **TDMA:** Time Division Multiple Access.
- **FDMA:** Frequency Division Multiple Access.
- **LFSR:** Linear Feedback Shift Registers.
- **BER:** Bit Error Rate.
- **BPSK:** Binary Phase Shift Keying.
- **SF:** Spreading Factor.
- **PSK:** Phase Shift Keying.
- **ASK:** Amplitude Shift Keying.
- **FSK:** Frequency Shift Keying.
- **QAM:** Quadrature Amplitude Modulation.
- **QPSK:** Quadrature Phase Shift Keying.
- **OVSF:** Orthogonal Variable Spreading Factor Codes**.**
- **PA:** Power Amplifier.
- **RNG:** Random Number Generator.
- **XOR:** Exclusive OR.
- **GPS:** Global Positioning System.
- **PWLCM:** Piece Wise Linear Chaotic Map.
- **SNR:** Signal To Noise Ratio.
- **PWLCM:** Piecewise Linear Chaotic Map.
- **LSB:** Least Signification Bit.
- **ISR:** Integrated Sidelobe Ratio.
- **PSR:** Peak Sidelobe Ratio.
- **PSL:** Peak Sidelobe Level.
- **DF:** Discrimination Factor.
- **DS-CDMA**: Direct Sequence CDMA.
- **MF:** Merit Factor.
- **DF:** Discrimination Factor.
- **AWGN:** Additive White Gaussian Noise.
- **MSE:** Mean Squared Error.
- **PSNR:** Peak Signal-To-Noise Ratio.

TABLE
DES FIGURES

TABLE
DES TABLEAUX

Introduction générale

Introduction générale

Aujourd'hui, les nouvelle technique de communications créé un aspect important dans l'acquisition de nouvelles connaissances de l'humanité. La demande et le besoin constant d'être en mesure d'échange de donnée en tout sécurité est aussi ancien que les communications elles-mêmes. Eventuellement ça nous ramène à l'étude de l'amélioration de système communication moderne à l´étalement de spectre issu par des séquences carte chaotiques.

La communication sécurisée chaotique est l'une des applications les plus importantes de la théorie du chaos. Alors, comment pouvons-nous sécuriser un système de communication de donnée en utilisant le système chaotique dans l'étalement de spectre (DS-SS) ? Initialement dans le domaine de la communication sécurisée chaotique il y a deux types de systèmes de cryptage chaotique : l'un est le système sécurisé chaotique analogique basé sur la synchronisation chaotique, l'autre est le système de cryptage numérique basé sur la séquence pseudo-aléatoire chaotique avec de nombreuses utilisations comme dans la communication militaire [1].

Les séquences chaotiques des générations des nombres aléatoires basés sur une carte chaotique sont importantes dans tous les aspects de la dissimulation de l'information avec la cryptographie [2] et le spectre étendu (ou étalé) [3]. Un générateur de nombres pseudo-aléatoires (PRNG) est un algorithme déterministe qui, à l'entrée d'une courte graine aléatoire, produit une séquence plus longue qui est calculatoire-distinguable d'une séquence aléatoire uniformément choisie. De nombreuses méthodes existent pour générer des séquences chaotiques. La carte logistique est la carte non linéaire discrète la plus étudiée car elle a été utilisée dans de nombreux domaines scientifiques. En outre, le fait que cette carte discrète a une distribution algébrique connue.

Dans les systèmes de communication à spectre étalé a séquence chaotique, un utilisateur différent peut se voir attribuer différentes séquences générées avec des conditions initiales différentes. Pour des raisons d'amélioration d'un système d'étalement de spectre certaines techniques ont été proposées, y compris l'étalement d'images basées sur la carte logistique, afin de fournir une meilleure solution au problème de sécurité de l'image numérique. L'utilisation de la séquence chaotique doit sembler absolument aléatoire. Ce pseudo-aléatoire chaotique générateur de nombres (CPRNG) a été discuté dans [4].

Par conséquent, nous avons besoin d'un générateur numérique chaotique avec des propriétés importantes telles que l'équilibre sur {0,1}; longueur du cycle long; complexité linéaire élevée; comme l'autocorrélation et corrélation croisée près de zéro [5]. Avec ces

propriétés, la séquence de chaos peut être utilisée comme générateur de nombres aléatoires. Un des systèmes simples est utilisé pour générer une séquence chaotique dans la carte logistique et une nouvelle carte logistique étudiée, cette dernière nécessite des tests d'algorithme ont été effectués sur la base de l'étalement et mépriser le temps moyen, la taille de l'espace clé, et l'analyse de sensibilité clé. En outre, nous avons effectué une analyse aléatoire du flux de clés généré par cet algorithme, et une analyse de distribution uniforme des valeurs de pixels dans les images couleur qui ont été étalé. Notre algorithme fournit des tests très importants statiques le rapport signal-bruit (PSNR) et les valeurs de similitude structurelle moyenne (MSSIM) pour les images couleur (RGB).

Pour ce faire nous avons présenté ce mémoire de la façon suivante :

En plus d'une introduction générale et une conclusion générale, qui résume notre étude, le présent travail effectué en trois chapitres comme suite.

- Dans le *premier chapitre* nous avons présenté des systèmes d'étalement spectres étendus basés sur le générateur chaotique. A ce sujet, nous rappelons tout d'abord, la structure des DS-SS systèmes et spécialement celle de type de séquence PN chaotique.
- Dans le *deuxième chapitre,* portera sur on présente à la réalisation de générateurs nombre issue des cartes chaotiques. Puis, nous montrons l'effet de l'analyse du comportement d'un système non linaire chaotique, à travers l'étude de sa sensibilité aux conditions initiales par générateur chaotique. Ensuite, nous présentons leurs performances, selon les tests d'évaluation, avant de conclure.
- Dans le *dernier chapitre,* Nous présentons les simulations du système énuméré l'étalement de spectre par l'utilisation des deux types de carte chaotique sous MATLAB. Ensuite nous analysons les résultats obtenus, en démontra l'intérêt de l'approche de DS-SS systèmes basés chaos proposés tant en termes de gain de temps qu'en termes de sécurité et seulement dans systèmes chaotiques, et la garantie de la qualité du perfectionnement du générateur de séquence pour l'étalement du système de transmission d'image couleur RGB avant de conclure. Certaines d'entre elles sont présentées en conclusion, ainsi qu'un bilan de nos travaux effectués.
- *Finalement,* ce travail est terminé par conclusion générale.

Chapitre 1 :

Système d’étalement de spectre par chaos Dans le domaine sécurisation

1. Introduction :

Dans ce chapitre, on va concentrer principalement sur l'application de la théorie de chaos pour les systèmes de communications à l'étalement de spectre à séquence direct DS-SS et la théorie de chaos dans la sécurité des systèmes communications.

1.1. Système de communication par étalement de spectre :

1.1.1. Système de Communications :

Un système de communications sécurisées à base du chao représente une application prometteuse de l'estimation d'état des systèmes non linéaires. A partir d'un message contenant de masque de la donnée, l'émetteur génère un signal qui est transmis au récepteur par le canal. Le récepteur reconstruit et traite le message original, grâce à une "clé" partagée avec l'émetteur.

La Figure (1.1) Montre les différentes couches de basse d'un système de communication moderne [6].

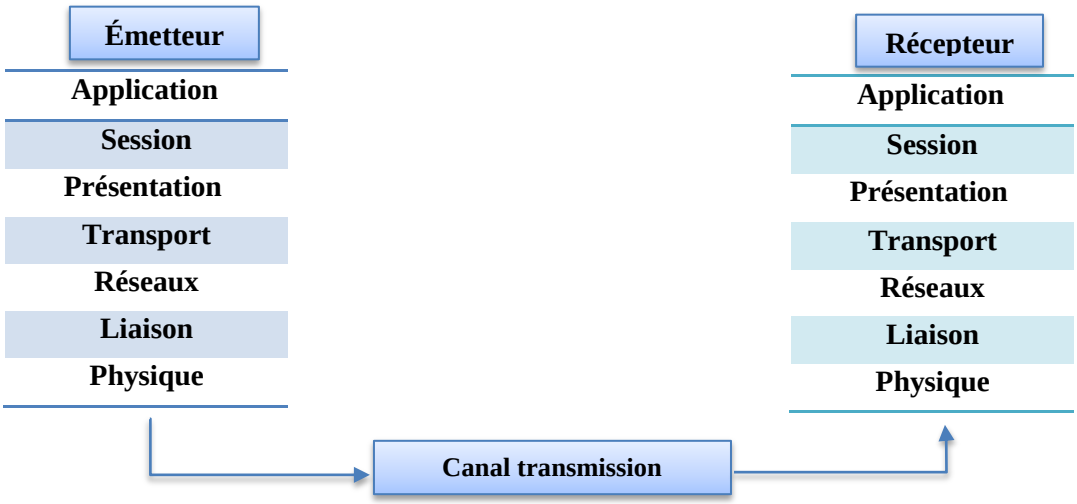


Figure 1.1 : Architecture de base d'un système de communication
En 7 couches **(**Modèle OSI**)**.

1.1.2. Les différentes couches du modèle OSI :

Le modèle OSI (ou Open Systems Interconnexion) décrit sept couches avec les noms de : couches physiques, liaison, réseau, transport, session, présentation et application.

Les différents protocoles qui définissent le réseau et les communications sont donc distribues dans chaque couche, selon leur utilité. Il est d'usage de diviser ces sept couches en deux : les couches basses, qui gèrent des fonctionnalités de base, et les couches hautes, qui contiennent les protocoles plus élaborés [7] :

1- **Couche application :** Le point d'accès aux services réseaux, elle n'a pas de service propre spécifique et entrant dans la portée de la norme.

2- **Couche Session :** elle permet de gérer les connexions et déconnexions et la synchronisation entre deux processus.

3- **Couche Présentation :** chargé du codage des données à transmettre. Elle s'occupe des conversions d'alignement et du chiffrement ou de la compression des données transmises.

4- **Couche Transport :** En charge de la liaison d'un bout à l'autre. S'occupe de la segmentation des données en petits paquets et vérifie éventuellement. Qu'elles ont été transmises correctement.

5- **Couche Réseau :** s'occupe de tout ce qui a trait à internet : l'identification des différents réseaux à interconnecter, la spécification des transferts de données entre réseaux, leur synchronisation, etc. Cette couche qui s'occupe du routage, la découverte d'un chemin de transmission entre récepteur et émetteur, ce chemin qui passe par une série de machines ou de routeurs qui transmettent l'information directement. Le protocole IP est Le protocole principal de cette couche.

6- **Couche Liaison** : s'occupe de la transmission d'un flux de bits entre deux ordinateurs, par l'intermédiaire d'une liaison point à point ou d'un bus. Pour simplifier, elle s'occupe de la gestion du réseau local. Elle prend notamment en charge les protocoles MAC, ARP, et quelques autres.

7- **Couche physique** : La couche physique s'occupe de la transmission physique des bits entre deux équipements réseaux. Elle s'occupe de la transmission des bits, leur encodage, la synchronisation entre deux cartes réseau, etc. Elle définit les standards des câbles réseaux, des fils de cuivre, du WIFI, de la fibre optique, ou de tout autre support électronique de transmission., elle propose plusieurs types de codage de l'information : DS-SS, FH-SS, OFDM.

Un problème toujours posé dans le domaine est le problème de la sécurité, avec l'avancement de la technologie des systèmes de transmission modernes, il y a un besoin croissant pour des modèles de communication sécurisés.

La sécurité au niveau de la couche physique est d'introduire des stratégies efficaces de communication sécurisée en ajoutant un niveau de sécurité à l'information théorique Ces méthodes peuvent améliorer la sécurité des systèmes disponibles. Il convient de mentionner que la sécurité de la couche physique peut être combinée avec les méthodes de sécurité existantes sous le nom de spectre étalé afin d'améliorer le niveau général de la sécurité des systèmes communications.

Les systèmes de téléphonie mobile de la troisième génération (3G) utilisent la technique d'accès multiples CDMA basée sur l'étalement de spectre. Cette technique offre une solution plus flexible, par rapport à celles des deux techniques TDMA et FDMA, et surtout un débit utilisateur beaucoup plus important, due à la largeur de bande allouée au signal émis, permettant ainsi des services multimédias très attractifs. En plus, l'étalement de spectre possède des qualités très avantageuses, telles que la résistance au brouillage intentionnel et surtout une parfaite protection contre l'interception de la communication par des intrus. C'est pour toutes ces raisons que l'usage initial de cette technique fut très attractif.

1.1.3. L'Étalement de spectre :

La transmission d'information par canal hertzien utilise classiquement des systèmes fonctionnant à bande (de fréquence) serrée, ce qui permet un multiplexage fréquentiel efficace du canal. Dans les systèmes à étalement de spectre, on va rechercher au contraire à ce que le signal radiofréquence occupe un spectre le plus large possible, ce qui à puissance d'émission égale donne une densité spectrale de puissance proportionnellement plus faible, de l'ordre de grandeur du bruit ambiant.

1.1.4. Type d'étalement de spectre :

Pour un système de communication à spectre étendu, plusieurs techniques peuvent être utilisées Pour réaliser l'opération d'étalement de spectre, il existe deux principales techniques :

A) ***Étalement de Spectre à sauts de fréquence (FH-SS)*** **:** s'effectuera à un usage de toute bande de fréquence pendant toute la conversation.

B) Étalement de Spectre à Séquence Directe (DS-SS) : En multipliant les données transmises par un code dont le débit est supérieur à celui des données.

Notre intérêt est principalement à l'étalement de spectre par séquences directes. Le système DS-SS représente la technologie de transmission la plus sécurisée. Les signaux sont transmis à une intensité faible sur toute la largeur du spectre.

1.1.5. Étalement de Spectre par Séquence Direct (DS-SS) :

Le système d'étalement de spectre à séquence directe DS-SS (ou DS-SS : Direct-Séquence Spread Spectrum), vise à diminuer la densité spectrale de puissance du signal à émettre en l'étalant sur une bande de fréquence de très grande largeur. Il constitue une technique d'accès particulièrement souple. Nous aurons par suite l'étalement par séquence direct qui est basé par le choix de code d'étalement : Le Code de Séquence PN, LFSR et Le code Gold.

Dans la pratique, l'information sur la bande de base est numérisée le Modulo-2 aussi ajouté à la séquence du code et ensuite modulé habituellement par le changement de phase PSK (ou PSK : Phase Shift Keying au taux de code [8].

La figure (1.2) illustre la sous-classe du système à spectre étalé à séquence directe.

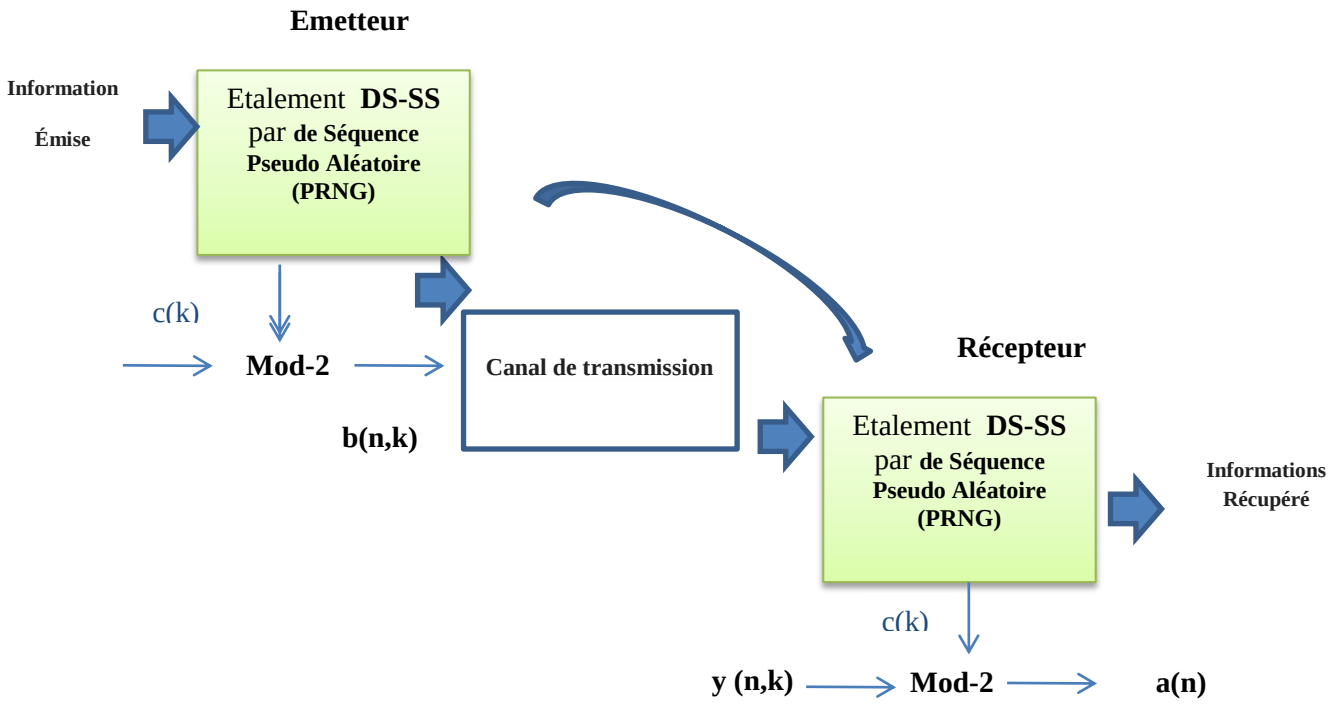


Figure 1.2 : Sous-classe du système à spectre étalé à séquence directe principe de base .

Les systèmes (DS-SS) arrivent leur capacité d'accès multiple en utilisant de grands ensembles de séquences avec trois propriétés de base qui sont appliquées à une séquence binaire périodique comme test pour l'apparition du hasard [9] :

- **Propriété d'équilibre** : Dans chaque période de la séquence, le nombre de binaires *1s* doit être différent du nombre de *0s* binaires d'au plus un chiffre. En d'autres termes, les séquences sont équilibrées de sorte que chaque élément de l'alphabet de séquence se produit avec la même fréquence.
- **Exécuter la propriété** : Un aléatoire est défini comme une séquence du même chiffre binaire. L'apparition d'un chiffre binaire différent marque le début d'une nouvelle exécution. La longueur de l'exécution est considérée comme un nombre de chiffres dans l'exécution. Pour la propriété d'exécution aléatoire, dans chaque période, environ la moitié des traits de chaque chiffre binaire doit être de longueur à *1*, environ un quart de la longueur à *2*, un huitième de la longueur à *3*, et ainsi de suite.
- **Propriété de corrélation** : Les séquences aléatoires sont souvent décrites en termes de leurs propriétés de corrélation. Une séquence de brouillage dans un système DS-SS doit avoir de faibles valeurs d'auto corrélation hors pointe pour permettre l'acquisition rapide de séquences au niveau du récepteur et pour minimiser l'auto-interférence due à des acquisitions par trajets multiples. En outre, les corrélations croisées sont suffisamment petites parmi ces séquences à tous les retards pour minimiser l'interférence à accès multiple.

1.1.6. Principe d'Étalement à Séquence Directe :

La techniques DS-SS vise à réduire la densité spectrale de puissance du signal à émettre en l'étalant sur une bande de fréquence de très grande largeur. Le procédé DS-SS de modulation à étalement de spectre constitue une technique d'accès particulièrement souple. Il permet, entre autre :

- De transmettre simultanément des signaux à bande étroite émis par divers utilisateurs dans la même bande de fréquence et sans coordination.
- réalisation d'un système de communication à accès multiples à répartition par le code (CDMA). Chaque utilisateur communique via une signature (code personnel) qui permet de distinguer son signal de ceux des autres personnes.
- De partager contre l'interférence intensionnelle (brouillage).

- De réduire la possibilité de détecter le signal en le cachant dans le bruit de fond.
- D'assurer, par un traitement original, une protection contre les interférences aléatoires dues aux trajets multiples engendrés par la propagation. Ce dernier point engendre un intérêt tout particulier dans le domaine radio mobile [10].

Notons que cette dernière est la plus utilisée dans les transmissions de type CDMA. Dans ce cas, on parle de transmission DS-CDMA, dont le principe sera détaillé dans les sections suivantes.

Pourquoi étaler le spectre ?

Considérons le théorème de Shannon et Hartley concernant la capacité d'un canal de communication [11].

$$C = B.log_2\ (1 + \frac{S}{N}) \qquad \textbf{(1.1)}$$

Ou , C : la capacité maximale d'un canal en bits par seconde (bit/s ou bps),

B étant la bande passante du canal en Hertz et

$\frac{S}{N}$ le rapport de puissance signal/bruit.

Dans le cas de la technique de CDMA, le bruit est constitué par les autres utilisateurs dont on cherchera à augmenter le nombre. Il en résulte qu'en règle générale un système CDMA opère sur des rapports signal à bruit faibles, voire très faibles. Par changement de base des logarithmes l'équation (1.1) devient :

$$\frac{C}{B} = \frac{1}{\ln(2)} \ln\left(1 + \frac{S}{N}\right) = 1.443 \ln\left(1 + \frac{S}{N}\right) \qquad \textbf{(1.2)}$$

Si la puissance du signal est inférieure à la puissance du bruit, on peut simplifier et linéariser l'expression (1.1), en appliquant le développement en série de Maclaurin de ln(1+x) :

$$\frac{C}{B} = 1.443[\frac{S}{N} - \frac{1}{2}\left(\frac{S}{N}\right)^2 + \frac{1}{3}\left(\frac{S}{N}\right)^3 - \cdots \qquad \textbf{(1.3)}$$

Puisque l'étalement du spectre permet un rapport $\boldsymbol{\frac{S}{N}}$ très faible et que la puissance du signal utile pouvant être inférieure au niveau du bruit. Pour un $\boldsymbol{\frac{S}{N}} \ll 1$, l'équation (1.1) devient alors :

$$\frac{C}{B} = 1.443\left(\frac{S}{N}\right) \quad \textbf{(1.4)}$$

Et par approximation on obtient

$$\frac{C}{B} \approx \frac{S}{N} \; ou \; \frac{N}{S} \approx \frac{B}{C} \quad \textbf{(1.5)}$$

Remarque 1:

La bande étalée permet donc la transmission de signaux perturbés par d'autres signaux considérés alors comme du bruit, c'est-à-dire la transmission de signaux sur le même support. Le nombre de canaux utilisés à un instant donné pourra varier de façon souple puisque l'augmentation du nombre d'utilisateurs se traduira simplement par une augmentation, pour tous, du taux d'erreur. Ceci permet en téléphonie de maintenir une qualité de service sensiblement égale pour tous, (plutôt qu'une dépréciation totale pour un utilisateur) ajustable et relativement facile.

Exemple d'application :

On décrit ci-dessous un exemple d'étalement par séquence directe (Direct Séquence Spread Spectrum) figure (1.3).

- Le message A de l'émetteur A, représentée par une séquence de +1, -1 traduisant la séquence de bits 1 et 0 logiques, est multiplié par un code CA d'une séquence de +1 et –1 de chips judicieusement choisie, et dont les transitions sont m fois plus fréquentes. Un autre message B de l'émetteur B multiplié par un code CB.
- Les séquences produits A*CA et B*CB sont ajoutées et transmises.
- A la réception, le destinataire du message A multiplie la séquence reçue par le code CA, la même opération pour le destinataire du message B. Figure (1.3).

Si les codes sont bien choisis, sur la durée d'un bit, (donc de m chips), la moyenne de CA.CA et de CB.CB est égale à m/2, tandis que CA.CB a une moyenne nulle : Les codes CA et CB sont dits orthogonaux, (produit scalaire=0).

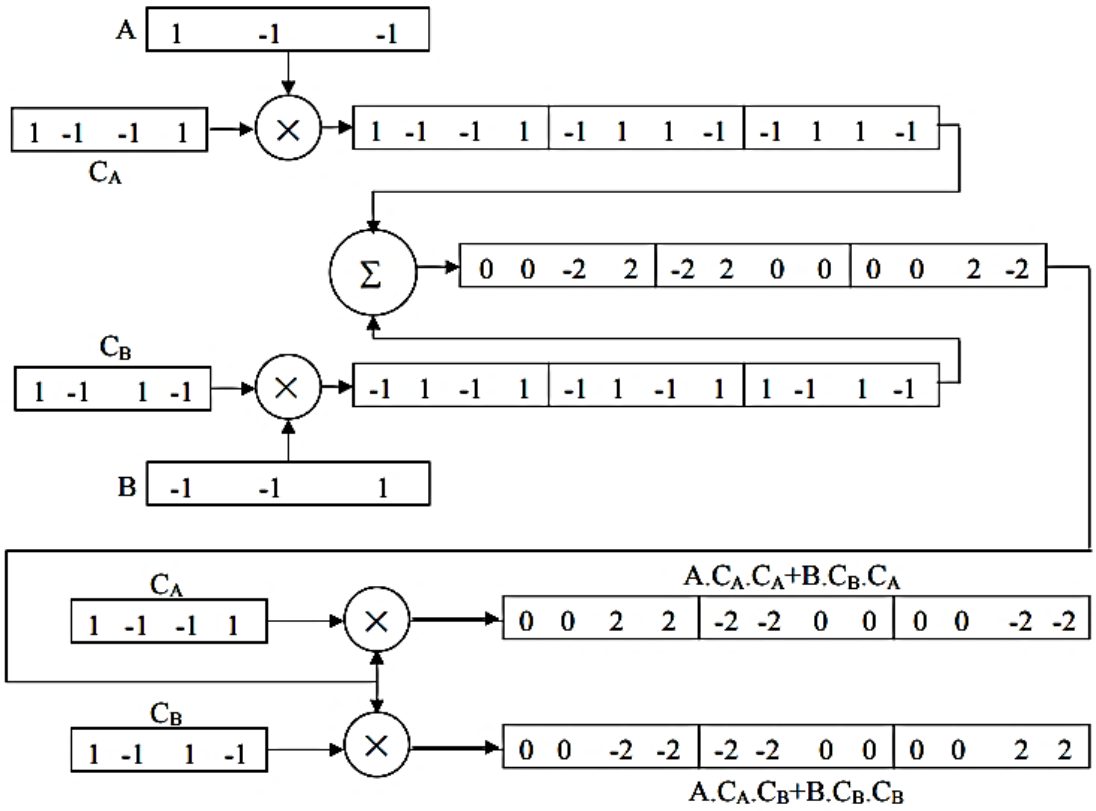


Fig. 1.3. Exemple d'étalement par séquence directe.

Remarque 2:

- La séquence somme est transmise sur trois niveaux d'amplitudes avec deux émetteurs. Quatre avec trois émetteurs etc. La moyenne sur chaque durée d'un bit est nulle.
- Lorsque le nombre d'émetteurs est plus important, la distribution des amplitudes s'apparente à une distribution Gaussienne (comme le bruit Gaussien).
- En réception les signaux sur chaque durée d'un bit de message ont une moyenne non nulle, ce qui permet la reconstitution du signal par simple filtre passe-bas. On préfère en fait mesurer la corrélation : la somme des produits code * signal reçu sur la durée d'un bit.
- Les codes sont choisis tels que leur produit scalaire CA.CB soit nul et CA.CA soit maximum (codes orthogonaux = produit scalaire nul). On rappelle qu'un produit scalaire est la somme des produits des composantes correspondantes : $u_1v_1 + u_2v_2$ pour deux vecteurs U et V de composantes u_1, u_2 et v_1, v_2. Cette notion de produit scalaire n'est pas limitée aux vecteurs dans le plan, mais est général. Le code est ici un vecteur dont les composantes sont les chips.

- Si l'on effectue une moyenne non pas sur les chips d'une période mais à cheval, les moyennes seront globalement plus faibles, donc ceci permet de synchroniser la réception pour certains systèmes, en recherchant la position où l'on obtient (en valeur absolue) un maximum. Les codes sont dans ce cas choisis tels que le produit scalaire d'un code par lui-même décalé soit pratiquement nul. A partir des spécifications techniques de certains standards [12], [13], [14].

1.1.7. Présentation Formelle de l'Étalement de Spectre à Séquence Directe :

Le diagramme de blocs de la figure (1.4) illustre un système de communication [15]. La rangée supérieure de blocs représente : Transmission des informations à la donnée binaire d_t avec le taux de symboles, *Rs = 1 / Ts* [bits/sec] (qui est égal au taux de bits R_b pour BPSK) (voir figure 1.2). La séquence directe du spectre étendu est multipliée par les informations à transmettre par un flux R_b le code pseudo-aléatoire ou le code pseudo-bruit (PN_t avec taux de puce, Rc = 1 / Tc [bits/sec]), également appelé signature, ayant un débit Rc [16], [17].

Le rapport entre le débit du signal étalé et le débit du signal non étalé est appelé facteur d'étalement SF (SF : Spreading Factor) peut s'écrire sous formes [18], [19] :

$$SF = \frac{T_c}{R_b} = \frac{T_b}{T_c} = N \qquad \textbf{(1.6)}$$

A noter que $T_b=1/R_b$: le temps du symbole ou période du signal et $T_c=1/R_c$ sera aussi bien la tempe rectangulaire du code appelé chip ou période de chip. Le N et typiquement un intégrant plus volumineux qui est égale à « 1 ».

La figure (1.4), représenté le schéma de principe d'un système de communication à spectre étendu par séquence directe est

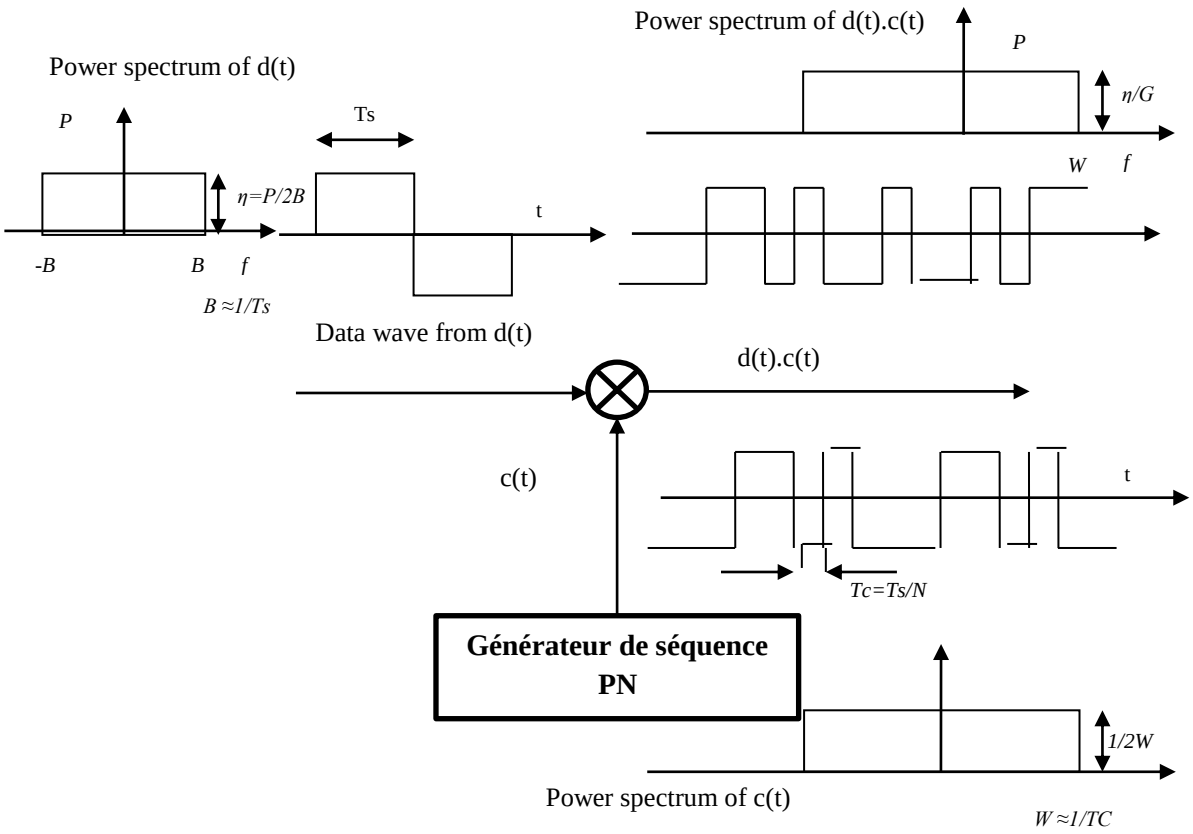


Figure 1.4 : Techniques de l'étalement de spectre à séquence directe (DS-SS)

La figure (1.5) représenté la technique de l'étalement de spectre à séquence directe (DS-SS)

La technique de l'étalement est faite par la modulation du signal utile. Il est multiplié par un signal pseudo-aléatoire d'une bande large, appelé le code d'étalement ou « la séquence des chips ». Le cas le plus simple d'une chaine de transmission à spectre étalé est celui de la modulation BPSK, donnée dans la figure (1.5).

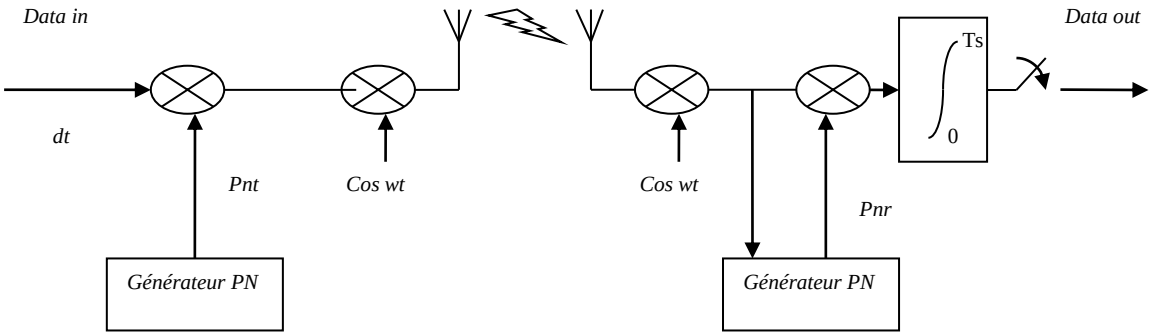


Figure 1.5 : Chaine de transmission DS-SS-BPSK.

1.1.8. Étalement de Spectre à l'Emission :

L'étalement est basé à la multiplication pure du signal numérique binaire BPSK par le code pseudo-aléatoire (voir la figure 1.5). L'éffet de la multiplication du signal d_t par le code Pn_t est d'étalement, en bande de base, le signal de largeur de bande ≈Rs sur une bande Rc par un facteur N « Processing Gain », ou N est le nombre de chips par symbole (pour des codes court, c'est la longueur de symbole). le facteur de proportionnalité entre la largeur de bande du signal de données et celle du signal étalé.

1.1.9. Les Etalements de Spectre à Réception :

Au récepteur, le signal étalé doit être multiplié par la même séquence PN (code Pn_t) qu'à l´émetteur pour être détecte :

- Si $Pn_r = Pn_t$ (et les deux séquences sont synchronisées), alors le signal binaire peut être récupère. L'effet de cette multiplication est de détaler le signal, c'est-à-dire de ramener la largeur de bande du signal à Rs.
- Si $Pn_r \neq Pn_t$ ou si $Pn_r = Pn_t$ et les deux séquences ne sont pas synchronisées, le signal reçu n'est pas détalé, et le récepteur ne peut pas récupérer le signal émis.

1.2. La Séquence des Chips :

Pour un système de communication à spectre étendu, la bande spectrale du signal transmis est étalée au moyen de code indépendant de donnée à transmettre. Ces signaux ou variables pseudo - aléatoire sont des grandeurs absolument déterminées mais dont le comportement paraît aléatoire et possède des propriétés statistiques bien définies. De telles grandeurs sont utilisées pour la simulation de phénomènes aléatoires ou la génération de signaux à fonction de corrélation très pointue utilisée pour tester la synchronisation au niveau du récepteur. La technique d'étalement de spectre nécessite la génération des séquences pseudo - aléatoire (PN), vérifiant certaines conditions [20] :

1. Simple à produire (pour une reconstruction facile au niveau du récepteur).
2. Possède les mêmes propriétés d'un signal aléatoire (donner au signal l'allure d'un bruit).

3. De longue période (difficile à reconstruire par l'indésirable).

Une génération de code Pseudo-aléatoire est le noyau pour les systèmes à spectre étalé. Les séquences M classiques et les séquences Gold n'accordent pas, car leur nombre et leur sécurité ne conviennent pas aux systèmes DS-SS. Ces séquences sont produites par des registres à décalage et par nature périodique. Donc, ces séquences sont moins nombreuses et limitent également la sécurité. On utilise une technique appelée « Chips », de corriger la perte d'information. Réduire au minimum le bruit de fond et les interférences locales. Pendant la transmission de données, chaque bit est ajouté à l'aide d'un exclusif ou (XOR) avec une séquence de 11 bits par exemple le code Barker {10110111000} qui possède des propriétés mathématiques qui le rendent idéal pour moduler les ondes radio. Le code PN tel que décrit par l'écaillage figure (1.6). Les séquences aléatoires peuvent être déterminées car nous avons une connaissance suffisante de l'algorithme utilisé pour la génération et l'état initial du générateur de nombres aléatoires [21].

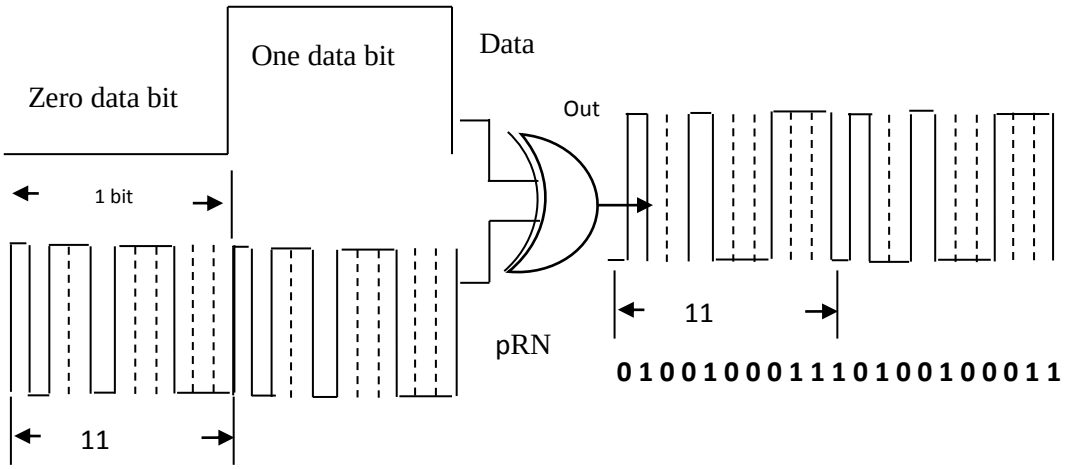


Figure 1.6 : Exemple chips de code PN.

Tableau. 1.1. Caractéristiques de quelques standards de télécommunication.

Standard	Bande de Fréquence(MHz)	Débit (bps)	Technique d'accès	Facteur d'étalement
IS-95	824-894 896-894	1.2288M	DS-CDMA	256
BLEUTOOTH	2400-2483.5	1M	FH-CDMA	79
UMTS	1900-2025 2110-2200	3.84M	DS-CDMA	4,8,…,256
CDMA2000	824-894 869-894	1.22883M 3.6864M	DS-CDMA	4,8,…,128 4,8,…,256
WLAN	2400-2484	11M	DS-CDMA	13
ZIGBEE	868-868.6 902-928 2400-2483.5	20K 40K 250K	DS-CDMA	1 10 16

1.2.1 Exemples du Choix de Code d'Étalement :

Il existe un grand nombre de techniques qui existent pour construire des codes ayant de bonnes propriétés :

1.2.1. Générateur pseudo aléatoire :

Définition de PNRG : Un générateur de nombres aléatoires (RNG) est un dispositif capable de produire une séquence de nombres qui ne peut pas être « facilement » dessiner des propriétés déterministes (Donald, Knuth, 1998), de sorte que cette séquence peut être appelée « séquence de nombres aléatoires ». Car des données aléatoires sont présentes dans de nombreux autres domaines. Certaines zones peuvent se contenter d'un générateur de données pseudo-

aléatoires et utilisent cette approche plus ou moins un danger parfait. Ils se retrouvent dans la simulation de jeu, l'analyse d'échantillonnage, la prise de décision et la sécurité informatique.

Informations de base Blackledge et Ptitsyn définissent un générateur de nombres pseudo-aléatoires (PRNG) comme un « Algorithme déterministe qui, à l'entrée d'une semence courte (une condition initiale), génère une séquence généralement beaucoup plus longue qui est indiscernable d'une chaîne uniformément choisie » [22].

Le générateur de nombres pseudo-aléatoires le plus connu est :

Un code de pseudo-bruit (code PN) ou code de bruit pseudo-aléatoire (code PRN) est un code qui a un spectre similaire à une séquence aléatoire de bits mais qui est généré de manière déterministe. Les séquences les plus couramment utilisées dans les systèmes à spectre étalé à séquence directe sont les séquences de longueur maximale basé à générateur LFSR, les Gold codes, les codes Kasami et les codes Barker ……

1.2.1.1. Générateur LFSR :

- **Définition de LFSR :** Un registre à décalage binaire LFSR (Linear Feedback Shift Register), comme celui décrit à la figure (1.7), représente l'une des manières les plus courantes pour générer des codes pseudo-aléatoires PN et périodique de $= 2^{n} - 1$. Son fonctionnement est le suivant : une fois que les différents états du registre sont initialisés, le bit en sortie est calculé à chaque coup d'horloge en additionnant en modulo 2 tous les bits présents à chaque état. Les bits sont ensuite décalés de manière circulaire pour réinitialiser les états de sorties.

$$f(x) = x^{n} + \alpha_{n-1}x^{n-1} + \alpha_{n-2}x^{n-2} + \cdots \alpha_{1}x^{1} + 1 \qquad \textbf{(1.9)}$$

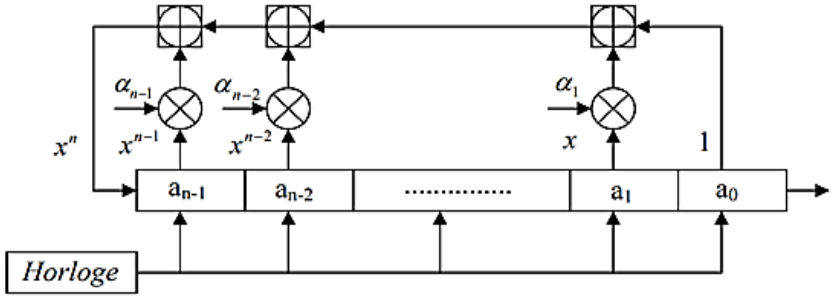


Figure 1.7 : schéma générique d'un registre à décalage à n états

où Les coefficients αi peuvent prendre deux valeurs 1 ou 0. Ainsi, lorsqu'il y a une connexion physique, α_i = 1et lorsque α_i = 0, il n'y a pas de connexion. Le polynôme irréductible générant une m-séquence est appelé « primitif ».

1.2.1.2. Générateur Gold code :

Définition :

Le générateur du Gold Code est un générateur de séquence pseudo aléatoire, qui utilise deux Pseudos aléatoires Bit Séquence (PBRS) pour générer une séquence de Gold Code. PBRS est utilisé pour répartir le spectre du signal d'entrée et chaque signal d'entrée peut être modulé inégalement en utilisant différents PBRS. Le bloc logique principal du Gold Code est composé du registre de changement de vitesse linéaire (LFSR) et de la porte XOR [23], [24], [25], [26], comme le montre la figure (1.8).

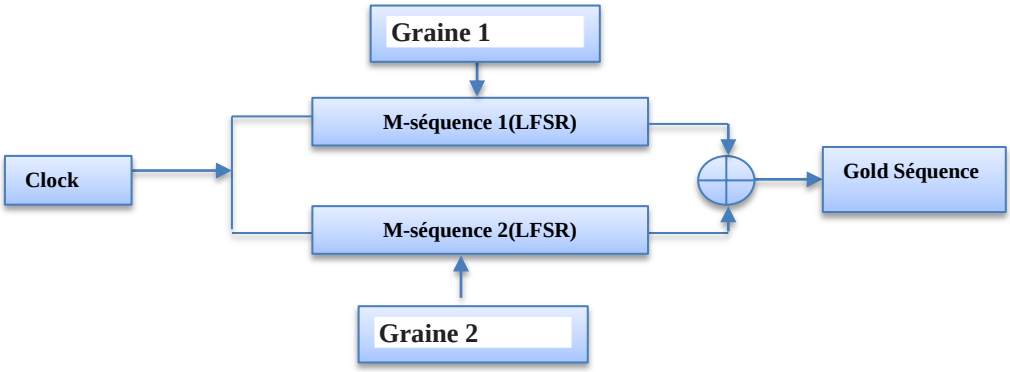


Figure 1.8 : Générateur du code Gold à base de LFSR**.**

Les deux m-séquence doit maintenir la même relation de phase jusqu'à ce que tous les ajouts sont la performance. Un léger changement de phase, même dans l'une des m-séquences, produit une séquence Gold différente tous ensemble. Gold Code sont non maximaux et par conséquent ils ont une propriété d'autocorrélation médiocre par rapport à celui des m-séquences sous-jacentes.

1.2.2. Les Générateurs Chaotiques :

1.2.2.1. Définitions de Chaos :

- **À Quoi Sert le Chaos ?** Comme on ne peut prédire le comportement à long terme des systèmes chaotiques, on a longtemps cru que le chaos serait incontrôlable et inutilisable. Pourtant, ces 30 dernières années, des chercheurs ont réussi à mettre certains phénomènes en équation et ont remarqué qu'il existe un côté déterministe dans ce qui apparaît être à première vue aléatoire.
- **Définition Larousse :** n.m. (gr. Khaos). Confusion générale des éléments de la matière, avant la création du monde. [26]
- **Définition E. Lorenz :** Un système agité par des forces où seules existent trois fréquences indépendantes, peut se déstabiliser, ses mouvements devenant alors totalement irréguliers et erratiques [26].
- **Définition scientifique :** On définit un phénomène chaotique comme étant un phénomène déterministe qui n'est pas périodique et qui se caractérise par une hypersensibilité aux conditions initiales. C'est cette sensibilité qui fait que le phénomène est si imprévisible.
- **Définition de Pseudo-Chaotique :** Le pseudo-chaotique est obtenu lorsqu'un système dynamique chaotique est simulé en utilisant des algorithmes arithmétiques de précision finie [27].

1.2.2.2. Théorie du Chaos :

Il n'est pas rare d'entendre quelqu'un qualifier une situation de chaotique. Cette qualification porte par nature l'idée que cette situation relève du désordre ou de la plus grande confusion. Les phénomènes dans lesquels on ne pouvait déceler à priori aucune logique a progressivement été regroupés sous le terme de chaos [28], [29], [30]. Il n'existe pas de définition rigoureuse du chaos mais par chaos, il faut admettre la notion de phénomène imprévisible et erratique.

Cependant, depuis une vingtaine d'années, on attribue le terme chaos à des comportements erratiques qui sont liés à des systèmes simples pouvant être régis par un petit nombre de variables entre lesquelles les relations décrivant leur évolution peuvent être écrites. Ces systèmes sont donc déterministes bien qu'imprévisibles.

La théorie du chaos, déjà entrevue par Jacques Hadamard et Henri Poincaré au début du XX^{e} siècle, a été définie à partir des années 1960 par de nombreux scientifiques. On appelle chaotiques des phénomènes complexes, dépendant de plusieurs paramètres et caractérisés par une extrême sensibilité aux conditions initiales : par exemple, les volutes décrites par la fumée d'une cigarette, ou la trajectoire d'un ballon qui se dégonfle. Ces courbes ne sont pas déterminées, modélisées par des systèmes d'équations linéaires ni par les lois de la mécanique classique ; pourtant, elles ne sont pas nécessairement aléatoires, relevant du seul calcul des probabilités : elles sont liées au chaos dit déterministe.

L'imprédictibilité est présentée dans de tels systèmes, qui n'en sont pas moins munis d'un ordre sous-jacent. Les signaux chaotiques peuvent être obtenus à partir de circuits non linéaires où interviennent des paramètres. Géométriquement, ces phénomènes dynamiques sont représentés dans un espace dont la dimension, qui peut être supérieure à celle de l'espace à trois dimensions, dépend du nombre de paramètres choisis pour les décrire.

À chaque instant, l'état du phénomène est représenté par un point dans cet espace appelé espace des phases. L'évolution du système est décrite par la trajectoire de ce point. Pour les phénomènes les plus simples, ce point est attiré vers un point d'équilibre ou une courbe limite, près desquels il repasse périodiquement que les mathématiciens appellent ces courbes limites des attracteurs étranges.

1.2.2.3. Système Dynamique :

Un système chaotique est un système déterministe qui présente un comportement de systèmes non linéaires avec certaines caractéristiques distinguées [31], [32]. Ce système est caractérisé par leur grande sensibilité aux conditions initiales et certain propriétés comme l'périodicité, le comportement pseudo aléatoire et la haute complexité [33]. Il y a beaucoup de définitions pour le système chaotique, qui est en simple terme « Un système qui devient apériodique (non-linéaire) si son paramètre, la variable interne, les signaux externes, la variable de contrôle ou même la valeur initiale est choisi d'une manière spécifique », Nous appelons ce

comportement imprévisible d'un système déterministe comme la théorie du chaos ou le système du chaos.

Un système dynamique consiste en un ensemble d'états possibles, avec une loi qui détermine de façon unique l'état présent du système en fonction de ses états passés. Aucun élément aléatoire n'est admis dans notre définition d'un système dynamique déterministe. Au lieu d'être appelé système dynamique, un tel modèle est souvent appelé un processus aléatoire ou stochastique. Les applications diverses de cette théorie dans divers domaines de recherche s'augmentent progressivement.

Pour obtenir une appréciation pour une base du système dynamique non linéaire, la théorie chaotique considère trois types de systèmes dynamiques [34].

1. Systèmes dynamiques autonomes :
2. Les systèmes dynamiques non autonomes diffèrent des systèmes autonomes parce que le champ de vecteur est une fonction de X et de t, et l'état initial ne peut pas être arbitrairement placé à zéro ;
3. Des systèmes dynamiques de temps discret sont définis par l'équation d'état, $X_{k+1} = f(x_k), k = 0,1,,3$ ou $X_n \in R^n$ s'appelle l'état, et f trace l'état X_k au prochain état X_{k+1}. Commençant par un état initial X_0 les applications répétées de la carte provoquent une séquence des points $\{ X_k = 0,1,2, \dots \}$ appelée une orbite du système à temps discret.

La théorie chaotique est basée sur le troisième type du système dynamique lorsqu'elle fonctionne dans l'état chaotique.

1.2.3. Les Cartes Chaotiques les plus Utilisées :

Les cartes chaotiques sont des systèmes dynamiques définis en réel par des relations de récurrence suivant :

$$x_i(n) = f\big(x_1(n-1), x_2(n-1), .., x_m(n-1)\big), \quad i = 1,2,, \dots \qquad \textbf{(1.11)}$$

Ou $x \in S, f: S^m \to S^m$ est une fonction de m-démentions, $S^m \subset [0,1]^m \, ou \, [-1,1]^m$.

Certaines cartes chaotiques monodimensionnelles, comme :la carte logistique, la carte PWLCM, et la carte kew tent et des cartes chaotiques bidimensionnelles telle que : les cartes Cat, Standard, Hénon et Lozi.

Dans cette étude, nous avons concernons surs des cartes chaotiques et utilisées pour la conception de générateurs de nombres aléatoires et comme algorithme de spectre étendu (voir le chapitre 2).

1.2.4. Les Conditions D'obtention du Chaos :

Les conditions d'obtention du chaos sure sont les suivantes [35] :

1- **La non linéarité :** Un système chaotique est un système dynamique non linaire .un système linaire, ne peut pas être chaotique.
2- **Le déterminisme** : Un système chaotique a des règles fondamentales déterministes et non probabilistes. Le déterminisme est la capacité à prédire le futur d'un phénomène à partir d'un événement passé ou présent l'évolution irrégulière du comportement d'un système chaotique est dû aux non linéarités.
3- **La sensibilité aux conditions initiales** : De très petits changements sur l'état initial peuvent mener à des comportements radicalement différents dans son état final.
4- **L'imprévisibilité** : En raison de la sensibilité aux conditions initiales.

1.2.5. Différence entre Chaos et Pseudo-Chaos :

Blackledge et Ptitsyn engendre deux considérations théoriques importantes qui doivent être prises en compte lors de la conception des nombres pseudo-chaotique. Tout d'abord, il est important de faire la différence entre le chaos et le pseudo-chaos. Alors que les cartes chaotiques se composent de variables d'état infiniment précises, les orbites calculées dans toute simulation pratique doivent être représentées avec une longueur binaire finie (dans ce cas, 32 bits). Cela signifie que les différences fondamentales entre le chaos et le pseudo-chaos sont les suivantes [36], [37].

- Il existe un nombre fini d'états dans tout le système pseudo-chaotique (c'est-à-dire stocke l'état avec une précision finie).
- La fonction itérée est évaluée par des méthodes d'approximation où le résultat est arrondi (ou tronqué) à une précision finie, et
- Le système pseudo-chaotique peut être observé pendant une période de temps finie.

Cette distinction est importante parce que, comme le disent *Blackledge et Ptitsyn*, le pseudo chaos est toujours une « mauvaise approximation du chaos, parce que le modèle approché ne converge pas vers le modèle original ». Le problème de base est que l'arrondissement est appliqué pendant l'itération et l'accumulation d'erreur provoque l'original et les processus approchés pour diverger. Ainsi, en général, le pseudo-chaos est une mauvaise approximation du chaos parce que le modèle approché ne converge pas vers le modèle original et, formellement, peut présenter des propriétés non chaotiques, y compris des trajectoires qui finissent par devenir périodiques apparaissent dès que deux états sont arrondis à la même valeur approximative. En conséquence, l'exposant de Lyapunov et l'entropie d'information de Kolmogorov-Sinai discuté plus tôt peut s'approcher à « 0 ». Pour cette raison, il n'est pas possible de transformer directement des générateurs chaotiques continus en générateurs à base numérique qui nécessitent des approximations numériques pour être résumées dans la figure (1.9)

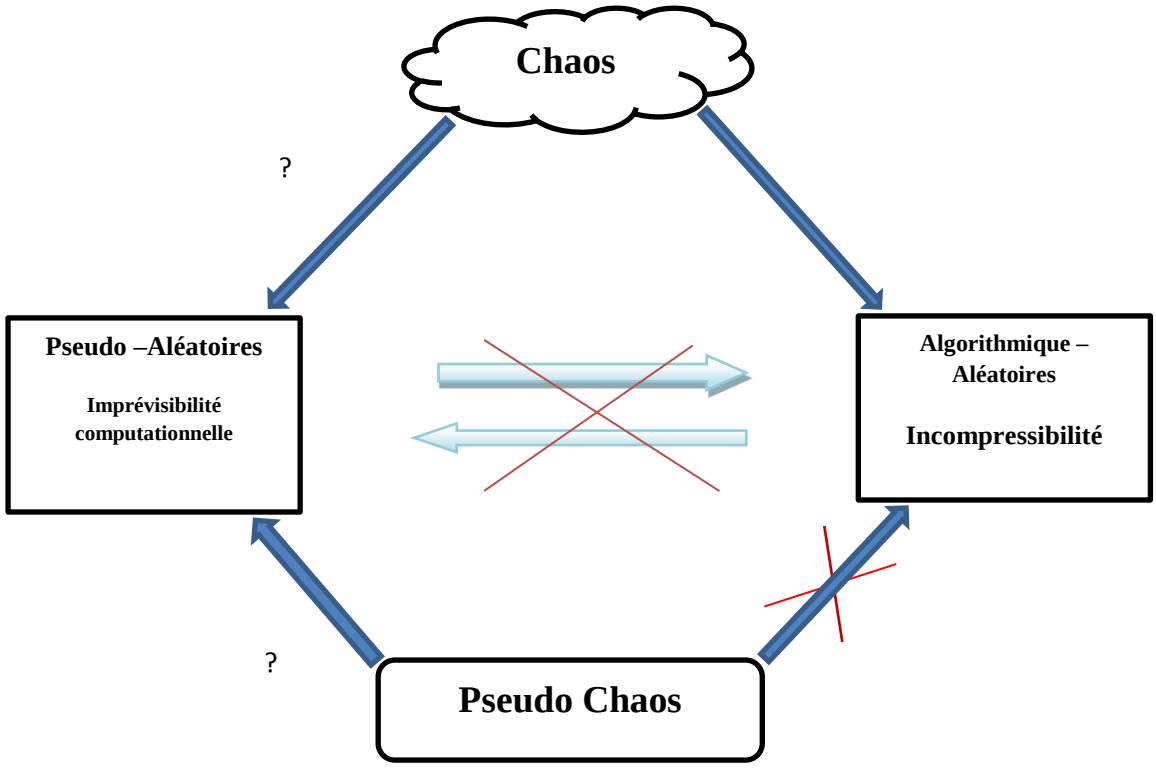
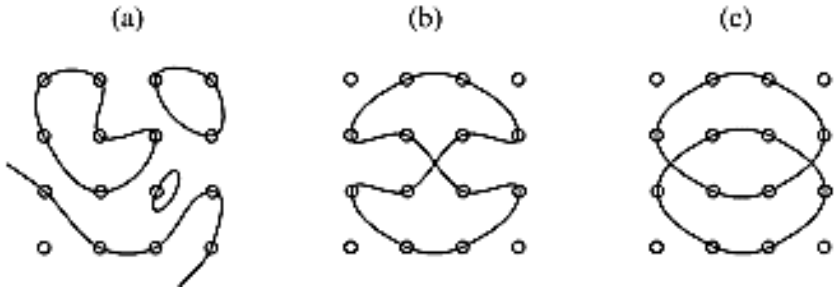


Figure 1.9 : Propriétés des systèmes chaotiques et pseudo-chaotiques**.**



- Orbites dangereusement courtes (impropres à la cryptographie);
- (b) Une seule orbite) le meilleur choix pour la cryptographie);
- (c) Orbites multiples de même longueur (également adaptées au cryptage).

Figure 1.10 : Exemples d'orbites d'un système pseudo-chaotique.

Ainsi, pour utiliser la théorie du chaos pour des applications en cryptographie, une étude doit être entreprise de systèmes pseudo chaotiques. En général, un système pseudo-chaotique produit des orbites de longueurs différentes (parfois appelées orbites de longueur aléatoire) comme illustré sur la figure 1.10 (a). Bien entendu, de tels schémas constituent une vulnérabilité grave, car un système peut avoir des textes en des clés faibles résultant en des textes cryptés reconnaissables. Si un système a un attracteur stable pour toutes les conditions et paramètres initiaux, et que toutes les orbites ont presque la même longueur (Figure.1 .10 (c)), il ya plus de chances de développer un schéma de cryptage sécurisé. Néanmoins, de nombreuses orbites réduisent l'espace de recherche requis pour la cryptanalyse. Un crypto système idéal a une seule orbite traversant tout l'espace d'état (Figure 1.10 (b)).

Une autre étape importante dans l'évaluation d'un système pseudo-chaotique est d'estimer l'exposant de Lyapunov d'une orbite typique pour un temps ne dépassant pas sa période. Cependant, l'analyse des orbites périodiques dépend de façon critique de l'ordre dans lequel les orbites sont considérées [38]. Deux critères de classement sont considérés dans la littérature, tous deux correspondant à une mesure de Lebesgue: ordonnancement selon la taille du système et ordre selon une période minimale ou au sein d'une période sur une base lexicographique. Si le système pseudo chaotique a une précision finie σ, alors la divergence exponentielle donnée par l'équation (1.12).

$$e^{n\lambda} = \frac{f^n(x_0+\varepsilon)-f^n(x_0)}{\varepsilon} \quad , n \longrightarrow \infty, \varepsilon \longrightarrow 0 \qquad \textbf{(1.12)}$$

Sera éventuellement limitée par ε = σ. Habituellement, la fonction (1.12) croît exponentiellement pendant les premières itérations, puis augmente linéairement jusqu'à ce qu'elle se stabilise enfin à une certaine valeur finie.

1.2.6. Évaluation des Générateurs Chaotiques :

Rappelons, que le chaos peut être généré par tout système dynamique non linéaire. En effet, des simples équations de récurrence sont capables de générer des dynamiques chaotiques riches, si les paramètres de contrôle sont bien positionnés. Dans beaucoup d'équations de récurrences simples, le bon choix de ces paramètres se fait grâce au diagramme de bifurcation et à l'exposant de Lyapunov [39]. Dans la littérature, il y a énormément de cartes et générateurs chaotiques mono et multidimensionnels qui sont utilisés dans diverses applications telles que : sources pseudo- aléatoires, communication et sécurité de l'information, contrôle et automatique, etc…

L'implémentation pratique de ces cartes et générateurs chaotiques engendre certaines faiblesses liées à la dégradation des dynamiques chaotiques telles que : périodicité, points fixes pour certaines valeurs de la clé secrète, non uniformité, temps de calcul important. La quantification des performances des cartes et générateurs de séquences chaotiques se fait grâce à des tests au niveau du signal (plan de phase, auto et inter corrélation, histogramme, mesure des orbites, etc.…).

1.2.7. Domaine d'application du chaos :

La théorie du chaos représente le premier pas vers l'unification des sciences. Le concept moderne du chaos déterministe est de plus en plus utilisé dans les contextes scientifiques variant des mathématiques et physiques des systèmes dynamiques et jusqu'aux variations temporelles complexes de tous types (exemples : chimie, biologie, physiologie, économie et même dans la psychologie).

- **Biologie**

En biologie la théorie du chaos permet d'expliquer les variations des populations animales, et aussi dans la médecine pour la prévision des crises d'épilepsie.

- **Economie**

En économie, les mouvements commerciaux et les marchés financiers, ainsi que les cycles économiques, peuvent être expliqués en partie par la théorie du chaos, qui permet de modéliser des expériences aléatoires complexes, d'où l'utilisation en finance, pour modéliser les variations des cours de la Bourse.

- **Informatique**

En informatique, des procédés de compression d'images ont été mis au point à partir des fractales. Des images de synthèse, au cinéma ou dans le domaine des jeux vidéo.

- **Télécommunication**

L'utilisation du chaos pour sécuriser les télécommunications est un sujet d'études depuis plusieurs années. Le chaos est obtenu à partir de systèmes non linéaires ; il correspond à un comportement stable, apériodique et éventuellement borné, de ces systèmes, ce qui le fait apparaître comme du « bruit » pseudo aléatoire. Il peut donc être utilisé pour masquer ou mélanger les informations dans une transmission sécurisée. L'originalité repose sur la prise en compte des propriétés de signaux chaotiques issus soit d'équations différentielles soit de récurrences discrètes non linéaires [40].

Alors que L'idée d'utilisations du chaos dans les communications sécurisées à multiutilisateurs sont souvent basées sur le contrôle et l'utilisation adéquate des d'orbites périodiques instables, l'idée principale est de se servir du squelette d'un attracteur chaotique comme un réservoir d'ondes potentiels de communications. De cette façon, le nombre d'utilisateurs, pourvus chacun d'un code propre dans le même canal.

L'intérêt des attracteurs multi-plis réside dans leur possibilité de permettre de générer des orbites plus courtes (par un chaos plus compliqué) et donc une transmission plus rapide des messages, ainsi qu'une meilleure sécurité dans les communications.

1.2.8. Système de Transmission (DS-SS) par chaos analogique :

L'intérêt d'utiliser des signaux chaotiques dans les transmissions analogiques réside dans deux propriétés fondamentales du chaos [41].

- Un signal chaotique est obtenu à partir d'un système déterministe ; il est donc possible de le reconstituer en se plaçant dans les mêmes conditions que celles qui ont contribué à le créer et ainsi de récupérer l'information au départ (sensible aux conditions initiales ce qu'on a vu dans le premier chapitre).

Un système chaotique engendre un signal à large spectre et peut donc permettre de transmettre des signaux très variés.

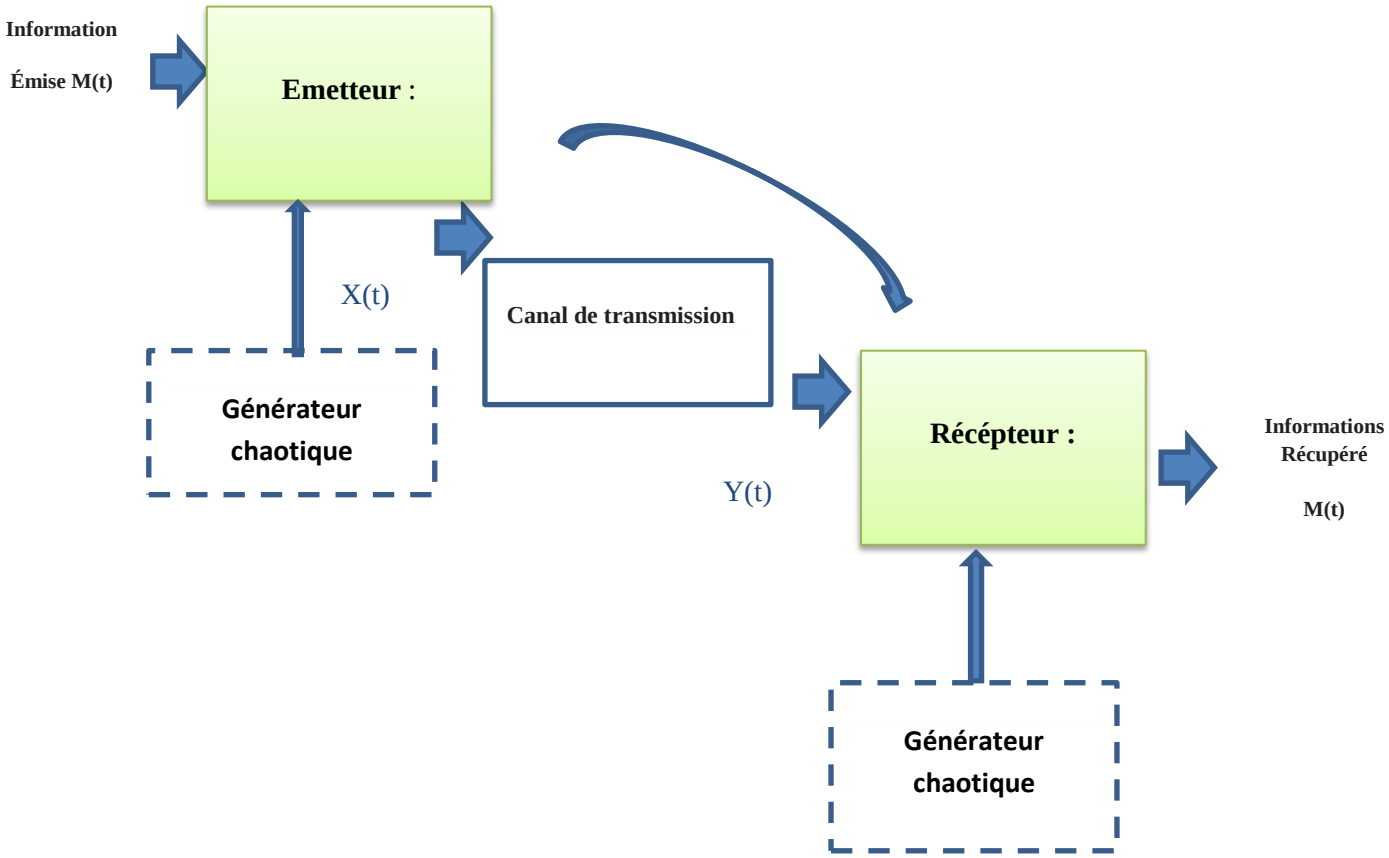


Figure 1.11: Principe de la communication sécurisée à base du chaos.

1.2.9. Principe de transmission par chaos analogique :

Le principe de transmission par chaos analogique repose sur ces deux propriétés comme indiqué dans la figure (1.11). Il consiste à mélanger l'information M(t) avec une séquence chaotique issue d'un système chaotique émetteur, décrit généralement par une représentation d'état. Seule la sortie y(t) de l'émetteur est transmise au récepteur via un canal public. Ce dernier

a pour rôle d'extraire l'information originale à partir du signal reçu y(t). La récupération du signal M(t) exige une synchronisation entre l'émetteur et le récepteur. Cela est possible grâce au comportement déterministe des systèmes chaotiques.

1.3. Théorie de chaos dans la sécurisation :

1.3.1. Système chaotique dans les systèmes sécurisés :

La cryptographie est une méthode traditionnelle qui fournit des mécanismes de sécurisés à différentes couches. En exploitent les propriétés de la couche physique on peut développer des systèmes de communication sécurisées efficaces. Ce nouveau paradigme peut augmenter la sécurité des systèmes existants en introduisant un niveau de sécurité de l'information théorique sur les systèmes. La sécurité de la couche physique a un rôle complémentaire et peut être intégrée aux solutions de sécurité existantes pour améliorer les systèmes de communication.

1.3.2. Principe de la Cryptographie :

Le diagramme principal de la communication sécurisée par le chaos est montré sur la figure (1.12). Le principe est de masquer une information par des signaux chaotiques et de l'envoyer vers le récepteur sur un canal de transmission. L'information cryptée est récupérée au niveau du récepteur. La clé du système de transmission est l'ensemble des paramètres des deux générateurs chaotiques à l'émission et à la réception qui doivent être synchronisés, c'est à dire

X = Y.

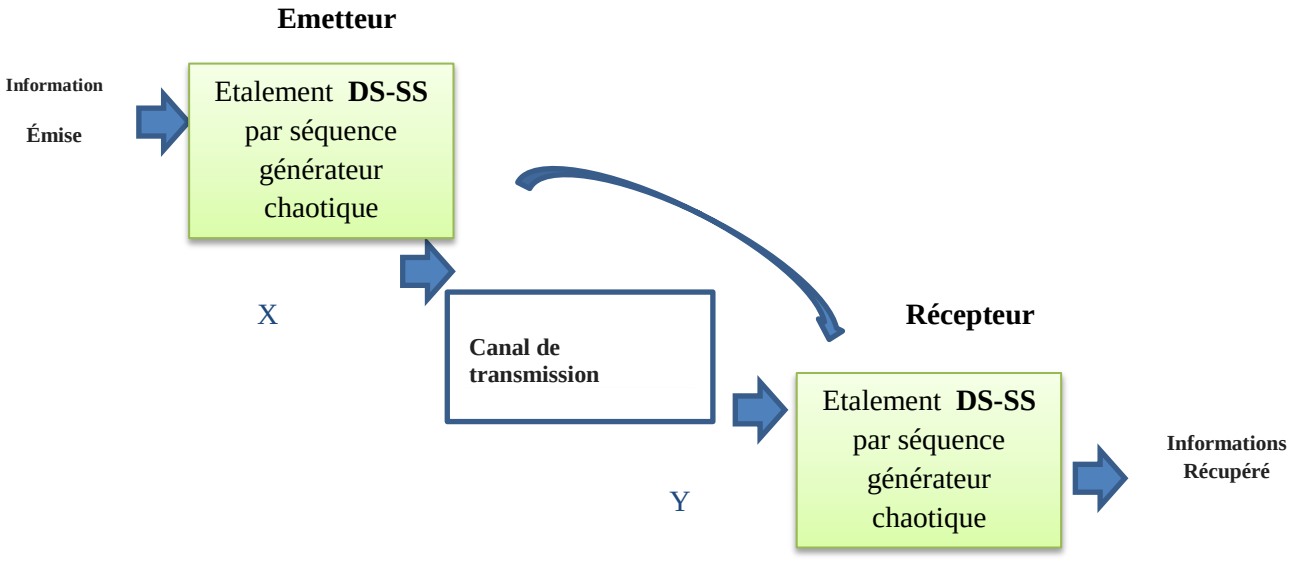


Figure 1.12: Principe de la communication sécurisée à base du chaos.

Les problèmes de sécurité qui apparaissent dans les systèmes de communication sécurisée à base du chaos peuvent être divisés en quatre domaines fondamentaux comprenant la confidentialité, l'intégrité, l'authentification et la non-répudiation.

- La **confidentialité** confirme que les parties légitimes reçoivent avec succès l'information attendue alors que les informations sont sécurisées contre les espions.
- **L'intégrité** confirme aux parties qui communiquent qu'un message n'a pas changé au cours de la transmission.
- **L'authentification** garantit que le récepteur légitime de l'information est en mesure d'identifier l'émetteur.
- La **non-répudiation** empêche la répudiation des entités de participer à la communication.

1.3.3. La Sécurisation au niveau de la couche physique :

La couche physique dont a un rôle est de transmettre le flux de l'information sur un canal de communication. La mise en œuvre du codage de canal au niveau de la couche physique consiste à fournir un milieu exempt d'erreurs pour les couches supérieures.
Les solutions de sécurité peuvent être utilisées dans différentes couches.

Tout d'abord, afin d'atténuer le brouillage de canal, les techniques de modulation à spectre étalé [42] peuvent être utilisées sur la couche physique. Sur la couche réseau, les mécanismes d'authentification peuvent être mis en œuvre pour empêcher l'accès non autorisé. Par conséquent, le brouillage de canal et l'accès non autorisé, qui sont vulnérables à la couche physique et à la couche de liaison, respectivement, sont manipulés par des solutions de sécurité sur leurs couches respectives. En outre, l'espionnage qui est une vulnérabilité de la couche physique peut être traditionnellement traité en exploitant les propriétés de la couche physique. L'objectif d'une communication sécurisée est que le récepteur légitime devrait récupérer le message sans erreurs alors que personne d'autre ne devrait acquérir l'information.

1.3.4. Evaluation d'Étalement de Spectre par Séquence Chaotique Direct :

Les signaux chaotiques peuvent être employés à cet effet. L'idée de base consiste à remplacer le générateur de séquences pseudo-aléatoires employé dans les techniques d'étalement conventionnelles par une dynamique chaotique, puisque les séquences chaotiques possèdent des propriétés similaires aux séquences d'étalement.

La figure 1.13 illustre la sous-classe du système à spectre étalé à séquence chaotique directe.

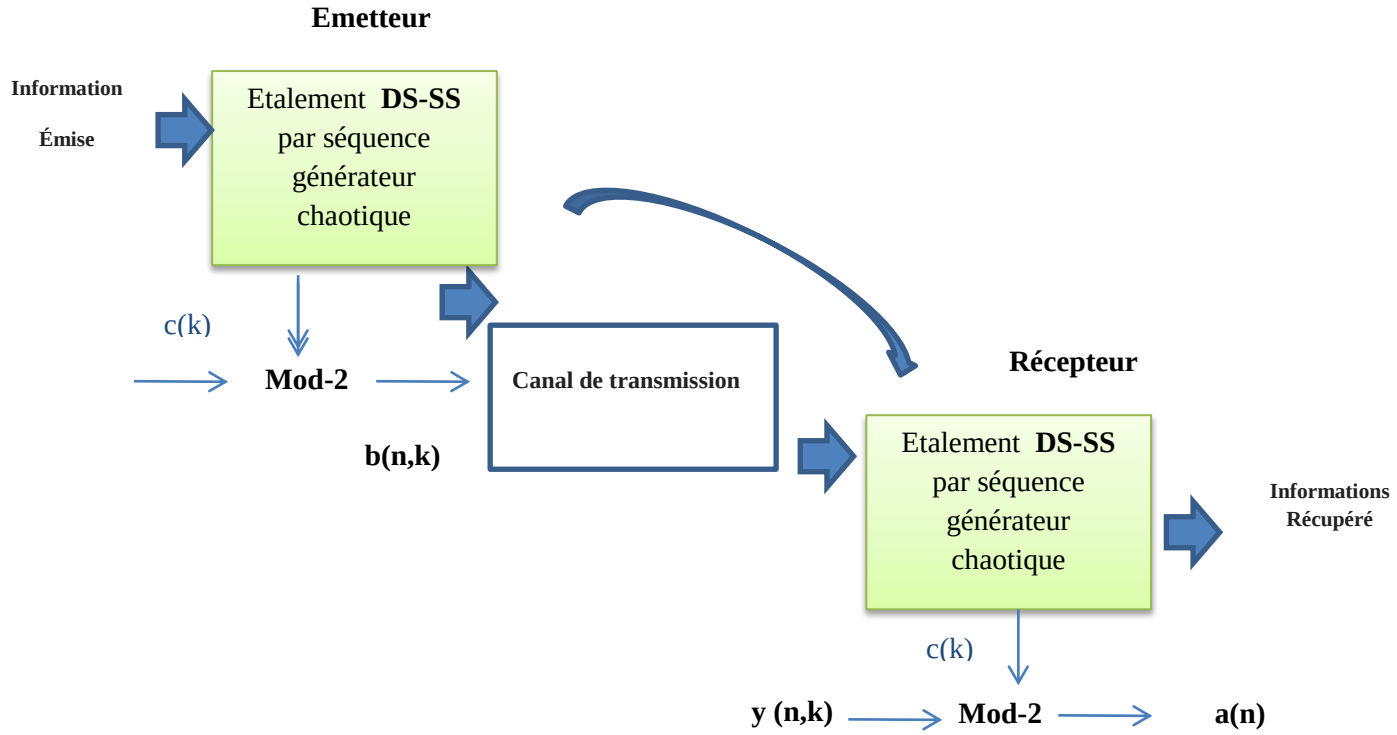


Figure 1.13 : Modèle d'un système de communication a étalement de spectre à séquence chaotique direct.

Les transmissions à base de chaos permettent de crypter et d'étaler le spectre du signal en même temps dont les informations sont transmises. La plupart d'entre elles présentent des inconvénients communs et partagent les mêmes difficultés de réalisation [43] :

- **Faible degré de confidentialité** : L'application d'une synchronisation consiste à transmettre une information suffisante sur le processus chaotique pour chiffrement.
- **Dégradation des propriétés des systèmes chaotiques** : La force du couplage appliqué aux systèmes chaotiques lors du processus de synchronisation, sert à tolérer l'effet du bruit de transmission et corriger les éventuelles perturbations dues aux incertitudes des paramètres
- **Faible robustesse contre le bruit** : En présence du bruit les performances de synchronisation dans les transmissions sécurisées par systèmes chaotiques se dégradent

1.4. Conclusion :

Ce chapitre avait comme objectif l'introduction de quelques notions élémentaires concernant la méthode d'étalement de spectre, le générateur de nombre aléatoire, les théories de chaos ainsi systèmes dynamiques, par la suite nous avons présenté la route vers le chaos et nous avons cité les domaines d'application des systèmes chaotiques et nous allons présenter les différentes techniques de sécurité du système de transmission par le chaos.

Le chapitre suivant est donc consacré à la description de générateur de nombre issus de carte chaotique.

Chapitre 2 :

Générateur de Nombre issu de Carte Chaotique

2.1. Introduction :

Dans ce chapitre, on étudie en bref la théorie des systèmes chaotiques, et les différentes cartes chaotiques, En suite, introduire quelque notion fondamentale relatives aux systèmes dynamiques.

2.1.1. Systèmes dynamiques :

- **Définition 1 :**

Un système dynamique défini des phénomènes qui changer au cours du temps. Aussi il est défini à partir d'un ensemble de variables qui forment le vecteur d'état :

$$X = \{x_i \in R\}, i = 1...n,$$

Ou,

n : représente la dimension du vecteur.

- **Formes d'un système dynamique :**

Deux formes essentielles d'un système dynamique sont :

- **Causale,** forme système dynamique ne dépond que de phénomène du passé ou présent.
- **Déterministe,** forme retrouver à partir d'une « Condition Initiale » donnée à l'instant « Présent » va correspondre à chaque instant ultérieur un et un seul état « Futur » possible.

2.2. La carte Chaotique utilise :

De nombreuses méthodes ont été développées pour concevoir des algorithmes l'étalement étendu de l'image en utilisant deux type des cartes chaotiques sont :

2.2.1. La carte Chaotique :

Les systèmes dynamiques à temps discrets sont d'un type particulier de systèmes dynamiques non linéaires généralement décrits comme une carte itérative par l'équation (2.1) :

$$M : R^k \rightarrow R^k$$

$$x_{n+1} = M(x_n); n = 0,1,2\ldots \qquad (2.1)$$

Où x_{n+1} : l'état suivant. Et x_n : l'état du système au temps n,

k : la dimensionnalité de l'espace d'état,

n : désigne le temps discret,

2.2.2. La carte logistique :

La carte logistique (ou Logistic Map) est devenue un système dynamique discret très utilisé spécialement en télécommunication.

Définition 2:

Robert May montré que la carte logistique a des comportements chaotiques.

La carte logistique est définie par l'équation (2.2) [44] :

$$x_{n+1} = M(x_n) = \mu x_n(1 - x_n) \qquad (2.2)$$

Avec : $x_n \in [0,1]$ et μ entre 0 et 3.999

La clé μ varie entre les valeurs suivantes :

- μ entre 1 et 3, c'est-à-dire entre 0 et 2, la séquence x_n converge vers $\frac{\mu-1}{\mu}$μ
- et on rattrapé une séquence x_n convergée à *n.*
- μ pour plus de 3, la séquence x_n peut, dans la plage μ comprise entre 2, 4, 8, 16 ... valeurs ou être chaotique.

Définition 3:

Diagramme du Cobweb **est** une procédure spécialement adaptée pour l'analyse qualitative du comportement d'une fonction itérative f à une dimension. Ce diagramme est utile pour déterminer l'évolution des itérations de la fonction f pour une condition initiale de donnée et pour une valeur de paramètre donnée.

La figure 2.1, présente l'attracteur de l'équation logistique, qui justifie le choix du paramètre μ entre 0 et 3.999**.**

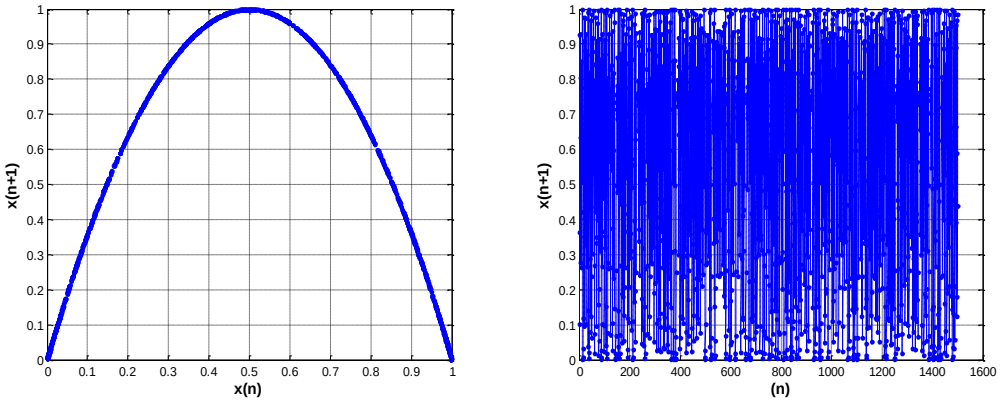


Figure 2.1 : Diagramme Cobweb (à gauche) et Forme d'onde du domaine temporel (droite) pour la carte logistique (N = 1500, μ=4, x0=0.1).

2.3.1. Nouvelle carte logistique (New Logistic Map):

La fonction nouvelle carte logistique a une récurrence non linaire. La relation de récurrence qui proposé à l'Atelier International sur les Théories Chaos-Fractales et Applications par Sun, Y. et G.Y. Wang [45].

Définition 4 :

Ce nouveau système dynamique déterministe non linaire, définie sur l'intervalle

[0, N], tel que N qui est strictement supérieur à 1, est donnée par :

$$x_{n+1} = \mu . x_n - x_n^2/K \tag{2.3}$$

Elle conduit, selon les valeurs de μ, à une suite convergente, une suite soumise à oscillations ou une suite chaotique et K constant.

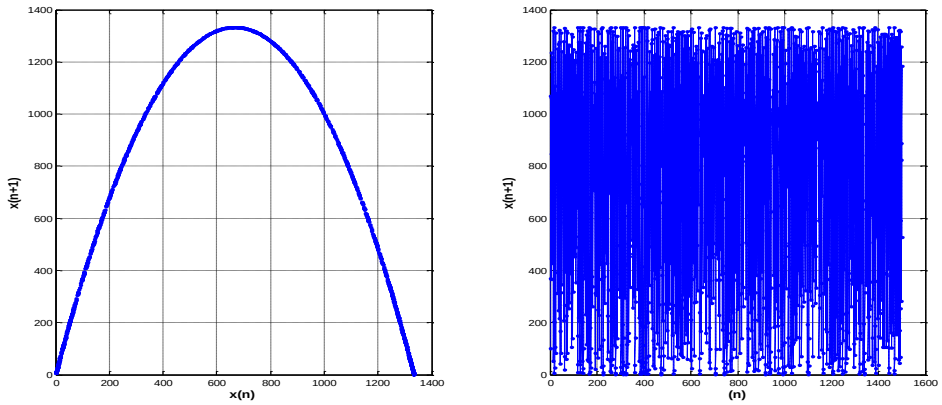


Figure 2.2 : Diagramme Cobweb (à gauche) et Forme d'onde du domaine temporel (droite) pour la nouvel carte logistique (N = 1500, μ=4, x_0=100, K=1000).

La figure (2.2), présente l'attracteur de l'équation logistique, qui justifie le choix du paramètre μ entre 0 et 3. 999.Lorsque μ = 3.999≈4 et que la valeur du paramètre *n* est réglée sur toute valeur autre que zéro sans limitation K = *1000*, et la valeur initiale est donnée comme x_0 = 100.

Exemple des types des cartes chaotiques :

Type de carte chaotique	Formule mathématique	Conductions des paramètre
Tent map	$x_{n+1} = F(x_n, q) = \begin{cases} \frac{x_n}{q} & 0 \le x_n < q \\ \frac{1-x_n}{1-q} & q \le x_n < 1 \end{cases}$	$q \in (0, 0.5)$, $x_n \in [0 \quad 1]$
Piecewise Linear Chaotic Map (PWLCM)	$x_{n+1} = F(x_n, q) = \begin{cases} \frac{x_n}{q} & 0 \le x_n < q \\ \frac{x_n - q}{0.5 - q} & q \le x_n < 0.5 \\ F(1-x_n, q) & 0.5 \le x_n < 1 \end{cases}$	$q \in (0 , 0.5)$, $x_n \in [0 \quad 1]$
Bernoulli's shift map	$x_{n+1} = f(x_n) = \mathrm{mod}(\lambda . x_n, 1) = \begin{cases} \lambda x_n & \le x_n \le 1/2 \\ \lambda x_n - 1 & 1/2 \le x_n \le 1 \end{cases}$	$x_n \in [0 \quad 1] \quad , \lambda \ge 1$

Tableau 2.1 : Quelques types des cartes chaotiques. [46]

2.3.2. Générer des séquences chaotiques binaires :

Méthode proposée :

Cette méthode comprend les étapes suivantes :

1. **Premièrement**, la séquence $\{x_n\}$ est générée par la méthode de la carte chaotique qui doit être amplifiée par un facteur d'échelle *n* et par la méthode de sous-séquence de parties entières $\lfloor f(x) \rfloor$ par la relation suivantes : ***floor(f(x))***.
2. **Deuxièmes,** la séquence résultante x_n a un niveau fini égal à (*m'*) défini sur (*mod m'*) et est transformé en séquence binaire.
3. **Troisièmes** on sélectionne les valeurs appropriées de (*n'*) et (m'), différentes séquences x_n peuvent être générées pour différentes conditions initiales.

Dans ce travail, les séquences binaires $\{x_n\}$ sont générées à partir d'une séquence chaotique en utilisant le modèle montré à la figure (2.3).

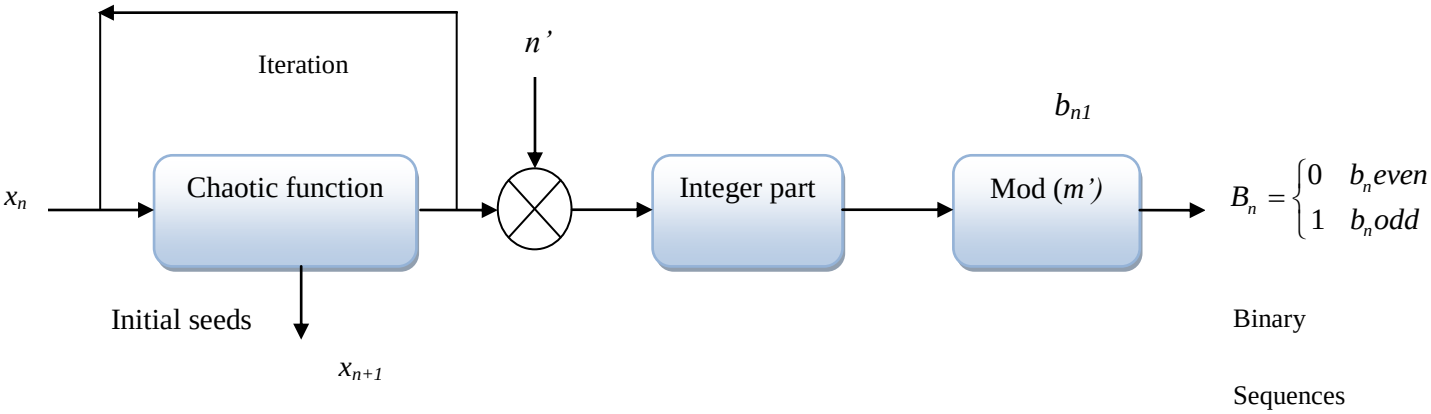


Figure 2.3 : Modèle pour générer une séquence binaire à partir d'une fonction chaotique

4. **Quatrièmes,** Séquence binaire chaotique :

A partir de ce modèle de la figure (2.3) nous avons trouvé la séquence chaotique par l'équation (2.4) :

$$b_n = \lfloor x_{n+1} . n' \rfloor . \bmod m' \qquad m' \leq n' \tag{2.4}$$

Nous générons une autre séquence $\{x_n\}$ pseudo-aléatoire B_n de nombres naturels séquences de n bits donnée par l'Encodage Séquence Chaotique binaire (LSB: Least Signification Bit).

$$B_n = \begin{cases} 0 & b_n even \\ 1 & b_n odd \end{cases} \text{ And } n \in [0 \quad N], \text{ N: Iterations} \tag{2.5}$$

2.3.3. Système d'évaluation de séquence chaotique :

Les propriétés quantitatives pour assurer que le flux-clé $\{s_i\}_0^\infty$ produit par $f(x_n)$ est un nombre aléatoire séquence chaotique avec les propriétés suivantes :

A. **Sensibilité aux conditions initiales.**

B. **Bifurcation.**

C. **Exposants de Lyaponov.**

D. **Rapport Ratio Sidelobe Peak (PSR) et Rapport Ratio Sidelobe intégré (ISR).**

A) Sensibilité aux conditions initiales :

Une caractéristique de la sensibilité aux conditions initiales du système chaotique, qui peut fournir des signaux qui ont des quantités de classe aléatoire non liées, et adapté pour déterminer et produire une régénération [47],[48].

Définition 5 :

Plus précisément, pour *f (x)*, l'application commence par deux valeurs initiales qui sont proches, disons *x* et *y* telles qu'une grande quantité et génèrent les orbites des deux premiers points.

$$E(n) = |f^n(x) - f^n(y)| \qquad (2.6)$$

Ou *n* : Itération.

1. Exemple 1: sensibilité de la nouvelle carte logistique

- La figure (2.4) et la figure (2.5), représente la sensibilité de la nouvel carte Logistique, avec un coefficient μ = 3.999, la longueur N = 100, la valeur initiale des deux séquences de nouvel carte logistique est respectivement 100 et 101, et leur différence une ε est supérieur à zéro ($\varepsilon > 0$).

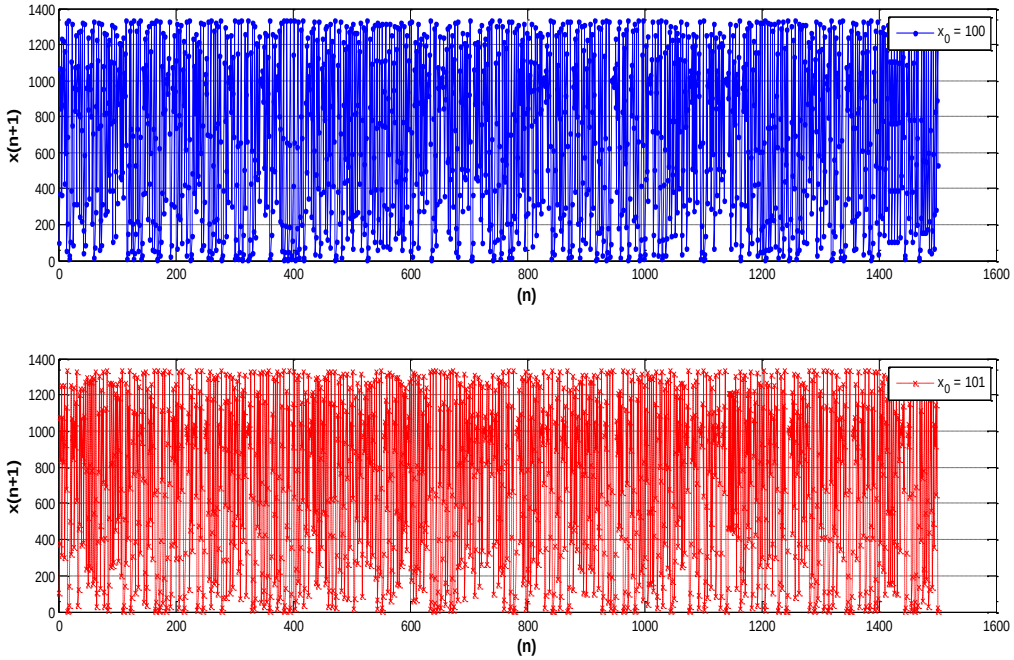


Figure 2.4: Évolution deux fonctions nouvel carte logistique (x_0=100, x0=101, μ=3.999)

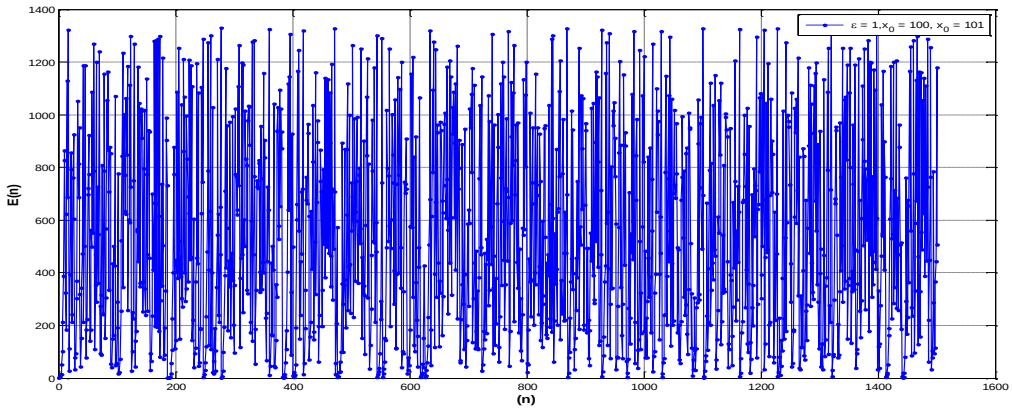


Figure 2.5 : *Sensibilité de la fonction nouvel carte logistique (x_0=100, x0=101, μ=3.999)*

2. Exemple 2: Sensibilité de la carte logistique

La figure (2.6) et la figure (2.7), représente la sensibilité de la carte Logistique, avec un coefficient $\mu = 3.999 \approx 4$, la longueur N = 100, la valeur initiale des deux séquences carte logistique chaotique est respectivement $x_{0=}0.09$ et $x_{0=}0.1$, et leur différence une εest supérieur à zéro ($\varepsilon > 0$).

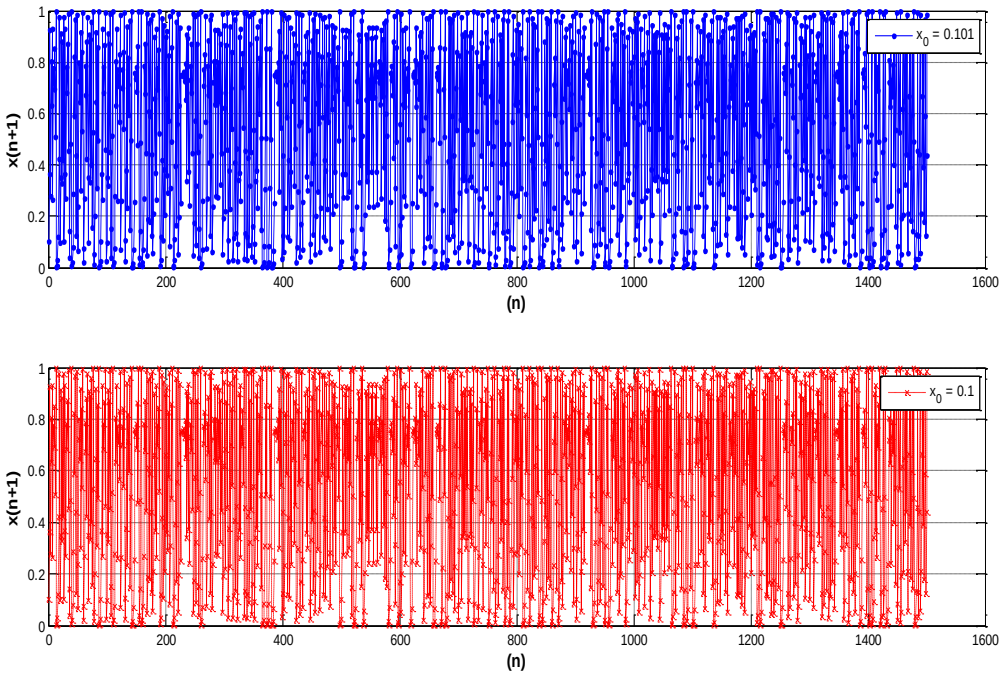


Figure 2.6: Évolution deux fonctions carte logistique (x_0=0.101, x0=0.1, μ=3.99)

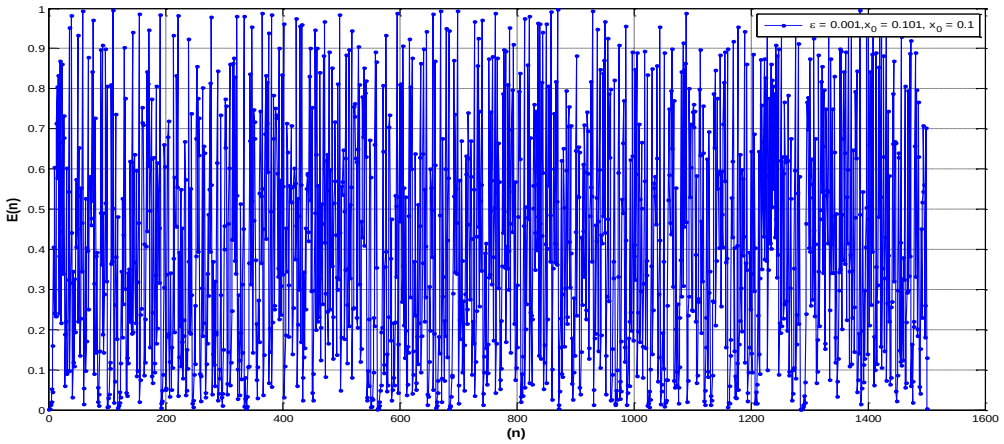


Figure 2.7 : Sensibilité de la fonction carte logistique (x_0=0.101, x0=0.1, μ = 3.999)

B) Bifurcation :

Définition 6 :

Un changement qualitatif de nature dans le comportement d'un système dynamique est appelé « Bifurcation », elle surgit lorsqu'un paramètre de contrôle franchit une valeur critique. Ainsi un système dynamique non linaire est confronté à bifurquer vers le chaos, lorsqu'on fait varier progressivement l'un de ses paramètres de contrôle, selon trois scénarios de transition possible [49]:

1. **L'intermittence.**
2. **Le doublement de période (cascade sous harmonique)** .
3. **La quasi-périodicité.**

La figure (2.8) et la figure (2.9) montrent que le paramètre de bifurcation μ est représenté sur l'axe horizontal du graphique et l'axe vertical montre les valeurs possibles de population et à long terme de la fonction logistique.

Les résultats sont obtenus à partir des simulations sous Matlab.

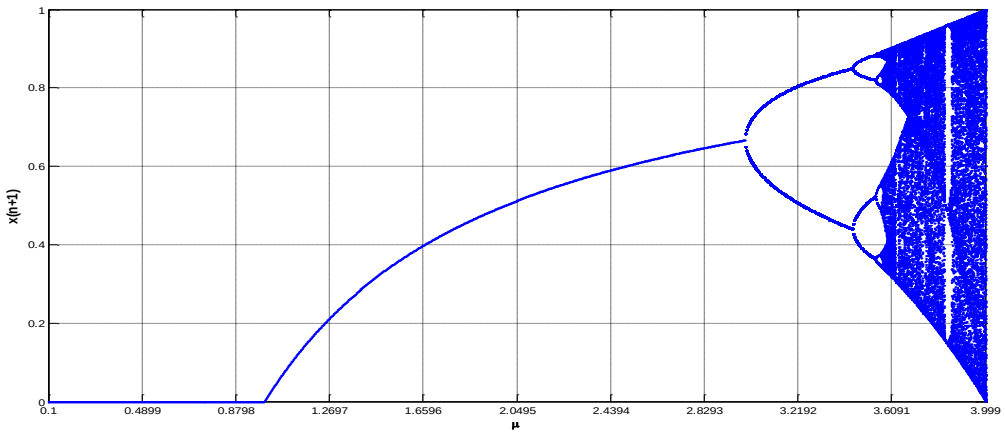


Figure 2.8 : Diagramme de bifurcation pour la carte Logistique de $0.1 \leq \mu \leq 3.999$.

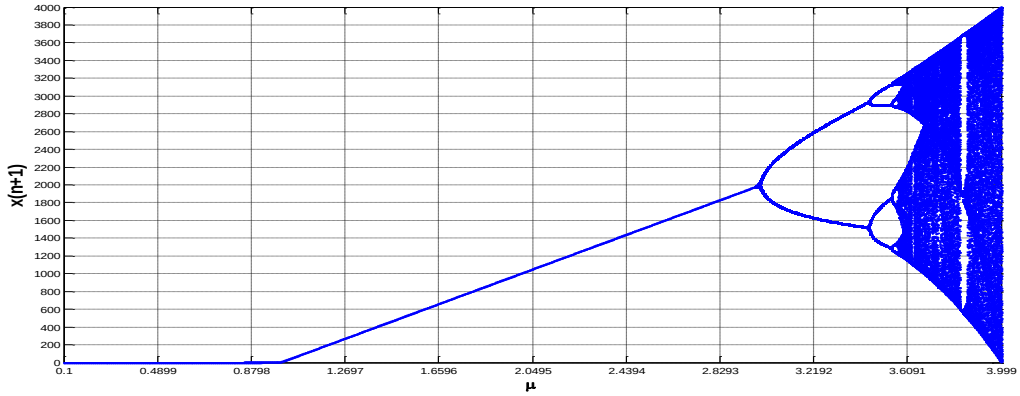


Figure 2.9 : Diagramme de bifurcation pour la nouvelle carte Logistique

de $0.1 \leq \mu \leq 3.999$

La figure (2.8) n'est pas similaire à la figure (2.9), qui est le diagramme de bifurcation pour la carte logistique et la nouvelle carte logistique. Les deux diagrammes peuvent également être différents l'un de l'autre.

C) Exposant de Lyaponov :

Le russe **Alexander Lyapunov** qui a introduit la quantité appelée Exposant de lyaponov (LE) [50]. Cet exposant est de quantifier à quelle vitesse le comportement dynamique d'un système est susceptible de différer en fonction des conditions initiales appliquées que nous produisons sur elle.

Définition 7 :

Exposant de lyaponov (LE), définie par le commencement des conditions de ε_0 de telle que sorte $f(x_0)$ devient $f(x_0+\varepsilon_0)$ après $(n+1)$ en des états successive, le changement de celle-ci $f(x_n)$ sera écrit $f(x_n+\varepsilon_n)$ telle sorte que devient successifs après x_0 et x_n soit quantifiée par l'équation (2.9) :

$$\ln\left|\frac{\varepsilon_n}{\varepsilon_0}\right| = \ln\left|\frac{\varepsilon_n}{\varepsilon_{n-1}}\right|.\left|\frac{\varepsilon_{n-1}}{\varepsilon_{n-2}}\right|....\left|\frac{\varepsilon_1}{\varepsilon_0}\right| = \sum_{i=1}^{n}\left|\frac{\varepsilon_i}{\varepsilon_{i-1}}\right| \tag{2.7}$$

$$\text{Ou :}\quad \left|\frac{\varepsilon_i}{\varepsilon_{i-1}}\right| = \left|\frac{f(x_{i-1}+\varepsilon_{i-1})}{\varepsilon_{i-1}}\right| \xrightarrow{\varepsilon_{i-1}} \left|f'(x_{i-1})\right| \tag{2.8}$$

Le composant de Lyapunove d'un 1D map $x_{n+1} = f_\mu(x)$ est défini par l'équation (2.9):

$$\lambda_L(x) = \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n} ln\,|\,f'(x_k)\,| \tag{2.9}$$

- **Exemple 1 : Exposant de lyaponov (LE) de la carte logistique**

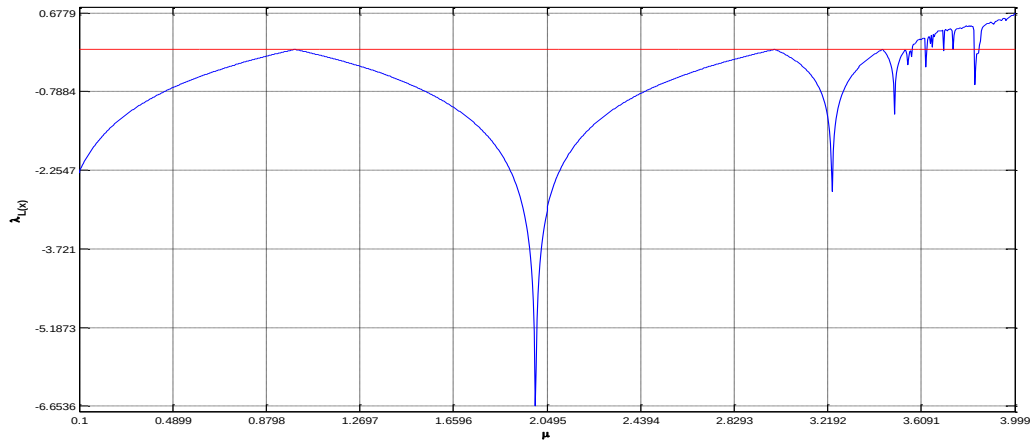


Figure 2.10 : Le composant de Lyapunove pour la carte logistique de.1 ≤μ ≤ 3.999.

, N = 1500, x_0=0.1

- **Exemple 2 : Exposant de lyaponov (LE) de la nouvelle carte logistique**

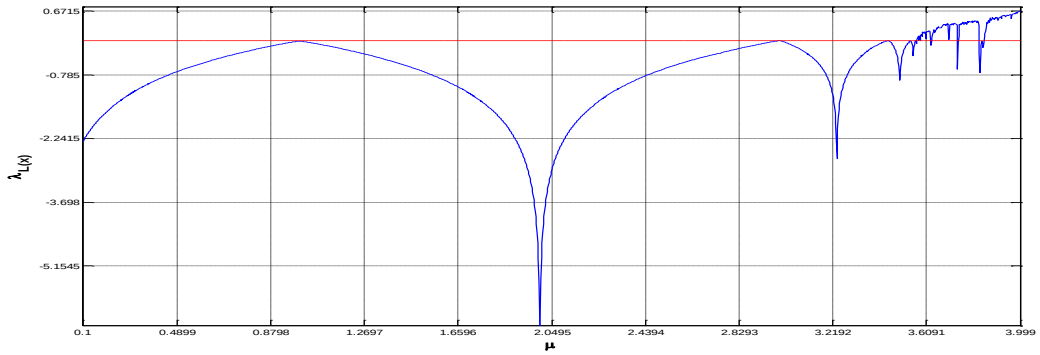


Figure 2.11 : Le composant de Lyapunove pour la nouvelle carte logistique de

- $0.1 \leq \mu \leq 3.999$, K=1000, N = 1500, x_0=100.

On remarque que les deux figures (2.10) et (2.11) sont identiques c.à.d:

- Dans un système avec Exposant de lyaponov (LE) supérieure à zéro **(**LE> 0), le trajet diverge exponentiellement et donc la dépendance sensible présente un système par rapport aux conditions initiales. Aussi si LE <0, le système est dispersif dans le sens que la trajectoire converge et si *LE = 0*, le système est conservateur
- Les deux types carte logistiques des deux exemples (1et2) ont un comportement chaotique **(**LE> 0).

Interprétation des résultats :

- On peut interpréter de résultat de la figure (2.8), la figure (2.9), la figure (2.10), et la figure (2.11) la sensibilité des cartes chaotiques (carte logistique et nouvel carte logistique) à sa valeur initiale x_0 indique également que: selon la valeur de λ, la dynamique du système peut changer de manière attrayante en périodicité ou en chaos. Un diagramme de bifurcation est un résumé visuel de la succession du doublage de période produit lorsque λ augmente.
- Finalement le comportement des deux c'est un système chaotique.

D) Rapport PSR (Peak Sidelobe Ratio) et Rapport ISR (integrate dSidelobe Ratio):

Le rapport PSR (ou PSR : PeakSidelobe Ratio) l'une des mesures de performance les plus couramment utilisées est le rapport Ratio SidelobePeak. Il est le plus grand lobe latéral dans la corrélation d'une séquence. Le rapport PSR est défini à partir du diagramme d'auto-corrélationr_{cc} *(m)* en tant que rapport de l'amplitude de lobe latéral de pic maximum à l'amplitude de crête du Sidelobe principal et est exprimé en décibels. Considérons une séquence binaire réelle de longueur N,$\{b_k\}_{m=0}^{N-1}$, $b_k = \pm 1$. Le rapport Peak Sidelobe (PSR) est donné par deux étapes comme suit:

- **Étape 1 :** Le Lobe principal (ou ML : Main Lobe) est définie comme la valeur absolue maximale de la fonction d'autocorrélation (ACF).

$$ML = \max_{m\neq 0}(r_{AC}(m)) \tag{2.10}$$

- **Étape 2** : Les Sidelobes latérales (PSL :Peak Sidelobe Level) qui sont décrites comme des valeurs maximales de ACF, sauf à une valeur absolue. PSL qui est désigné comme maximum de sidelobes latéraux.

$$PSL = \max_{m\neq 0}(|r(m)|) \tag{2.11}$$

L'autre ratio important est le rapport des lobes latéraux de crête, PSLR (Peak Sidelobe Level Ratio). Là encore, deux définitions possibles existent. Dans le premier cas, le Sidelobe latéral de corrélation croisée le plus élevé est comparé à la sortie de corrélation croisée de pic.

$$PSLR_1 = \frac{1}{r(0)^2}\max_{m\neq 0}(|r(m)|)^2 \tag{2.12}$$

$$PSLR_{dB} = 10 * log_{10}(PSLR_1) \tag{2.13}$$

Dans la deuxième définition, le Sidelobe latéral de corrélation croisée de crête est comparé à l'auto-corrélation de pic, à savoir.

$$PSLR_2 = \frac{1}{N^2}(\max_{m\neq 0}|r(m)|)^2 \tag{2.14}$$

$$PSLR_{dB} = 10 * log_{10}(PSLR_2) \tag{2.15}$$

Le facteur de discrimination DF est défini comme le rapport du pic principal dans l'auto-corrélation à l'amplitude maximale absolue parmi les lobes latéraux [51].

$$DF = \frac{r(0)}{\max_{m\neq 0}|r(m)|} \tag{2.16}$$

Au décalage *m=0*, la fonction d'auto-corrélation d'un processus aléatoire de moyenne nulle ne se réduit à la variance:

$$r_{AC}(0) = \lim_{N\to\infty} \frac{1}{N}\sum_{M=0}^{N-1}|R_{AC}(m)|^2 = \sigma^2 \tag{2.17}$$

- **Rapport ISR (integrated Sidelobe Ratio):**

Le rapport ISR (Integrated Sidelobe Ratio) est défini comme le rapport de l'énergie totale dans le lobe latéral à l'énergie dans le pic principal du modèle d'auto-corrélation et est exprimé en décibels.

$$ISLR_{dB} = 10 * log_{10}(\frac{2\sum_{m=1}^{N-1} r^2(m)}{r^2(0)}) \tag{2.18}$$

$$E = 2\sum_{m=1}^{N-1} r^2(m) \tag{2.19}$$

Où *E* : Signifie l'énergie d'une séquence

Le facteur de mérite MF (Merit Factor) est défini comme le rapport de l'énergie dans le pic principal de l'auto-corrélation à l'énergie dans les lobes latéraux [52].

$$MF = \frac{r^2(0)}{2\sum_{m=1}^{N-1} r^2(m)} \tag{2.20}$$

2.4. Test de séquence chaotique par Rapport PSR (Peak Sidelobe Ratio) et Rapport ISR (integrated Sidelobe Ratio)

2.4.1. Test fait sous simulation au MATLAB :

Une séquence est définie comme une bonne séquence si ISR évalué pour cette séquence est aussi minimal que possible. Ainsi une recherche complète des bonnes séquences doit être faite en variant les conditions initiales dans chaque méthode de cartographie et de toutes les séquences générées, les meilleures séquences sont sélectionnées en fonction du PSR et ISR.

Le tableau 2.2 Montre les résultats de la comparaison du facteur de discrimination (DF) et du facteur de mérite (MF) pour les séquences binaires avec la carte logistique, et modèle de

la carte logistique de Sung et Wang avec la sortie de la séquence binaire de longueur L[th] (N), $\{b_k\}_{m=0}^{N-1}$.

Longueur de séquence	**Carte Logistique** (x_0=0.100001; λ =4)		**Nouvelle carte logistique** (K=15000 ; x_0=100; λ =4)	
	MF	**DF**	**MF**	**DF**
10	0.3637	0.4517	0.0793	0.3697
20	0.4432	0.3430	0.1981	0.3242
30	0.2123	0.2795	0.2216	0.2971
40	0.2859	0.2976	0.3577	0.2939
50	0.3783	0.2887	0.5959	0.3194
60	0.5866	0.3133	0.5195	0.3006
70	0.7806	0.3228	0.5550	0.2989
80	0.8516	0.3179	0.6469	0.2744
90	0.9847	0.3255	0.6190	0.2765
100	1.0482	0.3256	0.5917	0.2763

Tableau 2.2 : Comparaison du facteur de discrimination (FD) et du facteur de mérite (MF) pour les séquences binaires avec deux types des cartes chaotiques.

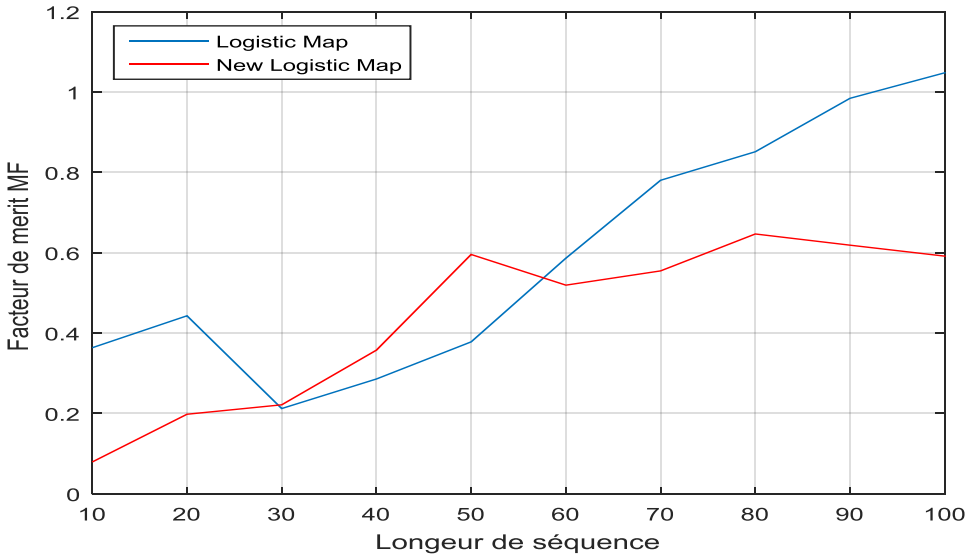


Figure 2.12 : Facteur de mérite (MF) en fonction de la longueur de séquences générées

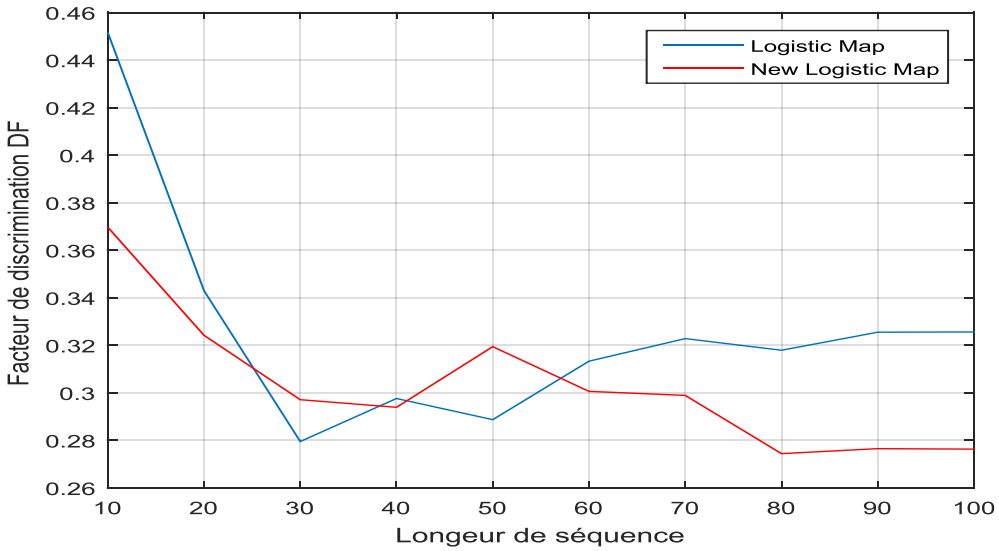


Figure 2.13 : Facteur de Discrimination (DF) en fonction de la longueur des séquences générées

Les propriétés d'analyse statistique, couplées à la fonction Autocorrélation , ont étudié la performance sous le bruit de l'AWGN, la radio de lobe latéral de crête (PSR) et la radio de lobe latérale intégrée (ISR) a générée par la séquence chaotique, ce qui en fait un choix parfait pour cette génération aléatoire de bits .

Longueur de séquence	**Carte Logistique** ***(x_0=0.100001; λ =4)***		**Nouvelle carte logistique** ***(K=15000 ; x_0=100; λ =4)***	
	$PSLR_{dB}$	$ISLR_{dB}$	$PSLR_{dB}$	$ISLR_{dB}$
10	-20,183	-17,3557	-21,7496	-20,489
20	-24,9437	-20,8566	-26,2034	-23,3759
30	-29,1852	-25,8177	-29,6213	-26,6898
40	-32,2146	-29,3777	-31,6196	-28,1877
50	-33,7733	-30,557	-33,6638	-30,338

Tableau.2. 3 : Comparaison du facteur la radio de lobe latéral de crête (PSR) et la radio de lobe latérale intégrée (ISR) pour les séquences binaires avec deux types des cartes chaotiques.

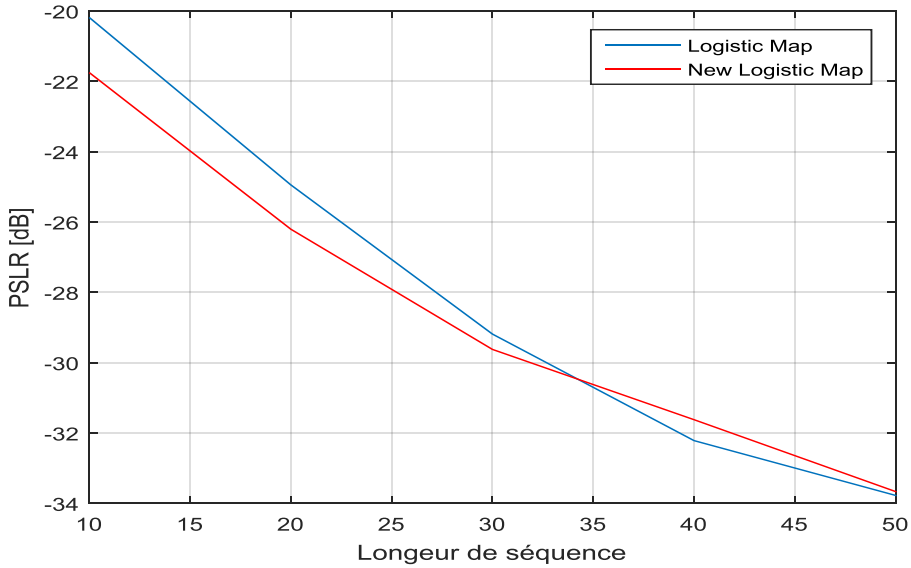


Figure 2.14 : PSR de phasage d'arbre en fonction de la longueur des séquences générées

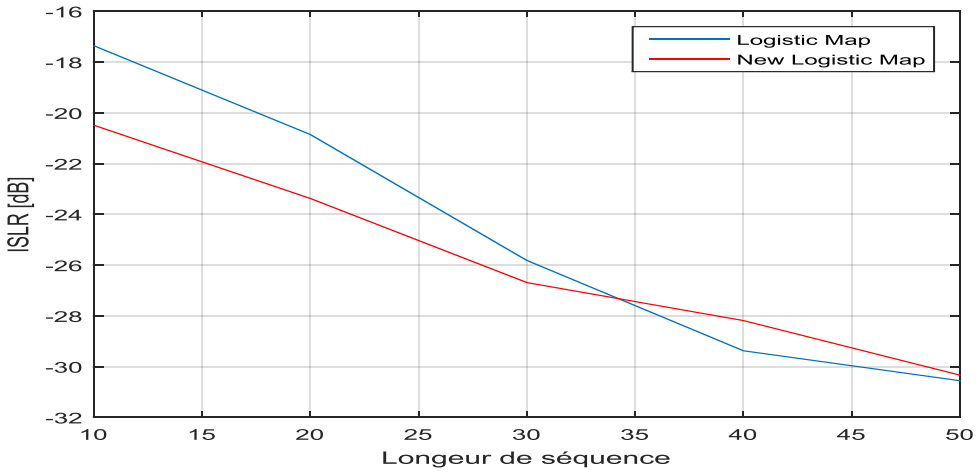


Figure 2.15 : ISR phasage d'arbre en fonction de la longueur des séquences générées.

La courbe de variation d'ISR pour les bonnes séquences modulées (phase modulée de BPSK) à des longueurs allant jusqu'à 50 est montrée sur la figure (2.15) L'ISR des bonnes séquences ne se révèle pas satisfaisant en particulier à des longueurs plus élevées. A partir de l'intrigue, il est entendu que l'ISR des séquences générées en utilisant la carte chaotique, l'amélioration de nouvelle carte logistique est meilleure que celle de la carte logistique.

La performance des séquences modulées est maintenant comparée à celle des séquences binaires modulées générées en utilisant la méthode de carte chaotique. Le graphique de comparaison du PSR des séquences binaire et modulé est montré sur la figure (2.14) Le PSR de la séquence modulée diminue à mesure que la longueur de la séquence

augmente. De bonnes séquences binaires ont été générées en utilisant les deux types des cartes chaotiques. A des longueurs différentes, de bonnes séquences ont été obtenues et il a été trouvé que le PSLR diminue avec la longueur de la séquence.

Remarque :

- Une séquence est définie comme une bonne séquence si le RIS évalué pour cette séquence est le minimum possible. Bien que le processus de génération de séquences binaires d'arbres soit assez général et facile par les deux types de cartes logistiques, toutes les séquences générées sont bonnes pour l'application dans d'étalement de spectre.
- Ainsi, une recherche complète de bonnes séquences doit être effectuée en faisant varier les conditions initiales dans chaque type de cartes logistiques et à partir de toutes les séquences générées, les meilleures séquences sont sélectionnées sur la base du PSR et de l'ISR.

2.4.2. Les avantages de l'application :

1. Les cartes logistiques sont utilisées dans la sécurité de l'information comme : Le chiffrement par flux, et par bloc, le hachage, la sténographie et le tatouage numérique.
2. Les cartes logistiques sont des candidats potentiels en tant que générateurs de nombres pseudo aléatoires et peuvent supplanter les générateurs pseudo-aléatoires traditionnels tels que : les séquences PN à longueur maximale, les générateurs de Gold et de Kasami, etc.
3. Le comportement carte logistique de ces systèmes rend leurs utilisations très importantes pour les systèmes de communication sécurisés.
4. L'avantage d'utiliser des signaux chaotiques dans ces systèmes réside dans des propriétés fondamentales des signaux et systèmes chaotiques :
    - Un signal chaotique est obtenu à partir d'un processus purement déterministe ; il est donc possible de le reconstituer en se plaçant dans les mêmes conditions que celles qui ont contribué à le créer.
    - Un système chaotique engendre un signal à large spectre bande et peut donc permettre de transmettre des signaux très variés.
    - Deux trajectoires de signaux chaotiques issues d'un même système chaotique, mais obtenues à partir de conditions initiales différentes, nombre des codes pour l'étalement des spectres très grand, etc...

2.5. Conclusion :

Nous constatons à travers cette chapitre comparative entre deux types de cartes logistique avec les même systèmes unidimensionnels étudiés sont capables à générer un comportement chaotique, cette perte de chaoticité entraine la dégradation de qualité des séquence générés, et la réduction de l'espace des paramètres valides, et par conséquent des récurrences au l'étalement de spectre qui peuvent causer de nombreuses failles de sécurité et utilise dans le system symbolique .La récurrence carte logistique et nouvelle carte logistique possèdent de meilleurs propriétés quantitatives et les deux récurrences génèrent des comportements uniformes sur l'intervalle [0,1], qui demeurent chaotiques pour toutes les valeurs de leurs paramètres de contrôle comprises dans les intervalles [0,1] et ($\lambda \geq 1$) respectivement. Ces deux systèmes de carte logistique seront utilisés pour la conception de notre algorithme de l'étalement de spectre par séquence direct.

A la fin nous avant présenté l'utilisation des cartes logistique chaotique dans l'étalement des images (RGB).

Chapitre 3

L’Evaluation de qualité d’image par l’Etalement de Spectre

3.1. Introduction

Ce chapitre est dédié à la présentation des résultats de simulation d'implémentation les points théoriques à travers des programmations sous MATLAB dans le système d'étalement de Spectre à séquence directe DS-SS.

L'objectif de ce chapitre est sans aucun doute l'évaluation de la qualité des images par l'étalement du spectre à séquence directe DS-SS, Ce dernier est considéré comme un outil essentiel pour faciliter la transmission du diagnostic dans l'image RGB.

Notre algorithme fournit des tests statiques très importants : le rapport signal sur bruit de pointe PSNR (PSNR : Peak Signal-To-Noise Ratio) et la similarité structurelle moyenne MSSIM (ou MSSIM : Mean Structural Similarity).

3.1.1. Quelque concepts et définitions :

- **Définition d'une image :**

La définition d'une image correspond à sa dimension, exprimée en pixels. Le pixel est la plus petite composante d'une image numérique. Il est possible de particulariser chaque pixel en grossissant fortement l'image. Normalement, plus une image comporte de pixels, plus elle est détaillée.

Image RGB Signifie "Rouge Vert Bleu". RVB fait référence à trois teintes de lumière qui peuvent être mélangées pour créer différentes couleurs. La combinaison de lumière rouge, verte et bleue est la méthode standard de production d'images couleur sur des écrans, tels que des téléviseurs, des écrans d'ordinateur et des écrans de smartphone [53].

Les images satellitaires utilisées :

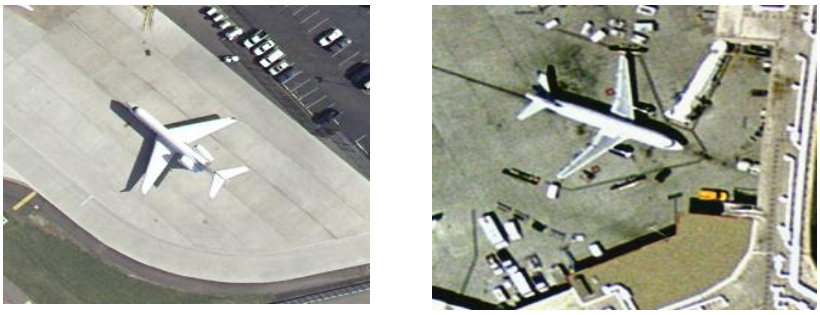


Figure 3.1 : Image satellitaire

3.2. Amélioration du système à étalement de spectre par la séquence de carte logistique chaotique avec application sur une image RGB :

3.2.1. La méthode de revente d'images de spectre étendu sous simulation au MATLAB

Une expérience de l'étalement d'images est conçue en utilisant le système algorithmique proposé, où la séquence chaotique générée est utilisée pour diffuser l'image pour quelques concepts et définitions). Supposons que la taille de l'image RGB soit (M × N), où (M, N) : Le nombre de lignes et la colonne de pixels.

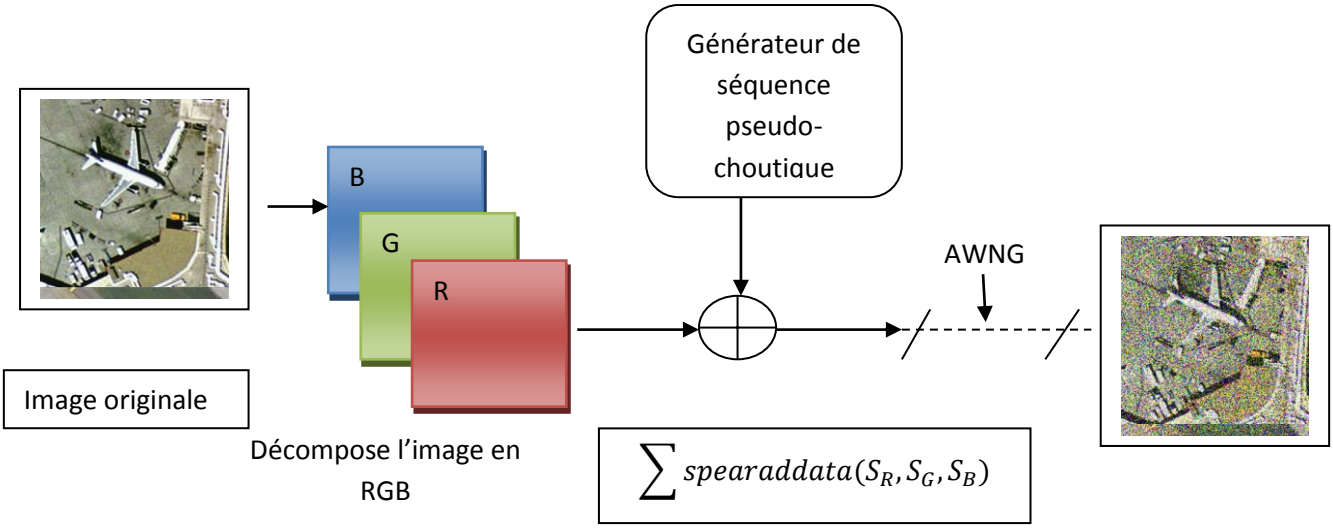


Figure 3.2 Les étapes complètes de diffusons par le générateur pseudo chaotique.

3.2.2. Les procédés d'épandage illustrés à la figure13 sont décrits aux étapes 1 à 5 :

Etape 1 : Dans un premier temps, nous choisissons M=N=256. Les images couleurs sont représentées par trois canaux de couleurs distincts : Le canal rouge (R) le canal vert (G) et le bleu (B).

Étape 2 : Au lieu de séparer chaque canal, une étape de mixage de canaux est utilisée pour mélanger les données de différents canaux et ainsi fournir un aspect de confusion supplémentaire dans l'image accélérée résultante.

Étape 3 : Ce tableau résultant est segmenté en blocs de 256 bits contigus (8 octets par bloc). Chaque pixel est représenté dans un canal donné par 1 octet donc nous les collectons un par un d'un canal à l'autre en utilisant le mécanisme de mixage suivant.

- Le premier octet est le bleu (B) et est étalé en le multipliant par une longue séquence de code PN (Pseudo Noise) de carte chaotique, chaque bit d'information contient un nombre de chips (First spread of The 8 chips) pour obtenir l'image étalé séquence SR (Spreaded Red) et le premier octet est le vert (G) qui s'étale en le multipliant par une longue séquence de code PN chaotique (Pseudo Noise).
- Chaque information de bit contient un nombre de chips (Second spread of The 8 chips séquence SG) qui obtiennent l'image d'étalé séquence étaler vert SG (spreaded Green) et le premier octet est le spread rouge en le multipliant par une longue séquence de code PN (Pseudo Noise).
- Chaque information de bit contient un certain nombre de séquences chips PN (Troisième étalement des 8 chips) et obtenons respectivement l'image du étalé séquence bleu SB (Spreaded Blue) puis nous revenons pour prendre le deuxième octet bleu étendu en le multipliant par la première propagation des 8 puces SR. L'octet vert se propage en multipliant-il avec le deuxième écart des 8 jetons et l'octet rouge (R) étalé en le multipliant avec le troisième écart des 8 chips.

Étape 4: L'additif de l'étalement du signal avec le canal Additive White Gaussian Noise (AWGN).

Etape 5 : Le signal est reçu de manière synchrone et image étalée

3.2.3 Critères d'évaluation et simulation de l'expérience de base :

Le rapport signal-bruit (PSNR) et la similitude structurelle (SSIM) sont l'évaluation des qualités de l'image à transmisse.

Jusqu'ici, nous devons savoir comment évaluer la qualité d'image issue code carte logistique. soit I(i,j) (i=1,2,…,N, j=1,2,…,M) l'image idéale, et $\hat{I}$ (i,j) (i=1,2,…,N, j=1,2,…,M) soit l'image étalée . La différence totale peut s'écrire comme suit :

$$E = \sum_{i=1}^{j=N} \sum_{i=1}^{j=M} \hat{I}(i,j) - I(i,j) \qquad (3.1)$$

La formule de l'erreur quadratique moyenne (MSE) est la suivante :

$$MSE = \frac{1}{M.N} \sum_{i=1}^{j=N} \sum_{i=1}^{j=M} \left(I(i,j) - \hat{I}(i,j) \right)^2 \quad (3.2)$$

Le rapport signal-bruit de crête (PSNR) a été déterminé à l'aide de l'équation (3.3):

$$PSNR = 10 \log_{10} \left(\frac{(dynamics\ of\ image)^2}{MSE} \right) \quad (3.3)$$

L'indice de similitude structurelle (SSIM) : La similitude compare la luminosité, le contraste et la structure entre chaque paire de vecteurs où l'indice de similitude structurelle (SSIM) entre deux signaux x et y est donné par l'équation (3.4) :

$$SSIM(x,y) = I(x,y).c(x,y).s(x,y) \quad (3.4)$$

L'indice de similarité structurelle moyenne (MSSIM) est exprimé comme suit :

$$MSSIM(I, \hat{I}) = 1/M \sum_{I=1}^{M} SSIM(I_i, \hat{I}_i) \quad (3.5)$$

3.3. Les résultats expérimentaux sur l'image couleur bruyante basée sur le modèle de couleur RGB :

Les algorithmes proposés dans le chapitre 2 appliqués dans ce chapitre étaient les suivants : nouvelle carte linéaire logistique chaotique (1er générateur) ; carte logistique chaotique (2éme générateur) sur l'image couleur de test (TIF) de taille 256*256 x 3 codée par 8 bit de couleurs (R G B). L'importance de notre travail réside dans la possibilité de réduire les chips de l'étalement pour lesquelles la qualité d'image reste améliorée.

Les images de résultats sont montrées dans la tableau 3.1 Les résultats ci-dessous existent dans MATLAB.

1- Séquence 1er générateur de langueur 24 carte logistique

PN1=[1 0 1 1 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0 1 1 0 0 0]

2- Séquence 2éme générateur de langueur 24 carte logistique

PN2=[0 0 1 1 1 0 0 0 1 1 1 0 1 0 1 1 1 0 1 0 1 1 0 1]

Le tableau 3.1, suivant représente la comparaison entre deux résultats de simulation dont la carte logistique nouvelle et la classique

Type de image original	**Etalement du spectre DS-SS (1st générateur) carte logistique**	**Etalement du spectre DS-SS (2nd générateur) nouvelle carte logistique**
		
IMAGE 1	PSNR : 54.27 SNR : 46.0517 MSE : 26.31 MMSIM: 0.94974	PSNR : 64.09 SNR : 46.0517 MSE : 5.41 MMSIM: 0.997

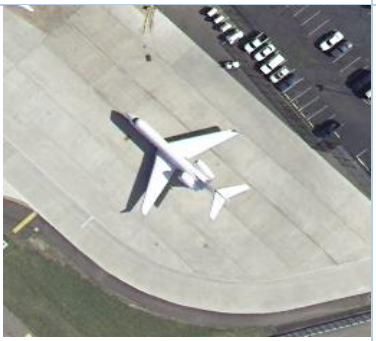



IMAGE 2	PSNR : 70.58 SNR : 46.0517 MSE : 27.56 MMSIM: 0.9559	PSNR : 69.42 SNR : 46.0517 MSE : 6.25 MMSIM: 0.99505

Tableau 3.1: *comparaison entre la simulation d'une image satellitaire avec l'ancienne et la nouvelle carte logistique*

3.3.1. Simulations des Mesures des deux qualités d'images étalées :

Les deux résultats de simulations représentent les deux sections A et B :

A. Simulation de l'image 1 :

1) 1er générateur

SNR	SNR (db)	PSNR	MSE	MMSIM
1	0	32.48	40.14	0.042603
3	21.9722	45.16	25.22	0.6038
5	32.1888	53.59	26.19	0.9066
8	41.5888	55.93	26.52	0.96048
10	46.0517	54.27	26.56	0.94974

Tableau 3.2 : la performance comparée à l'exécution : MSE, PSNR et MSSIM.de l'image originale et étalée générée par le 1er générateur

2) 2éme générateur

SNR	SNR (db)	PSNR	MSE	MMSIM
1	0	32.39	39.99	0.061147
3	21.9722	41.07	14.26	0.76377
5	32.1888	47.15	8.10	0.96726
8	41.5888	50.22	7.33	0.99418
10	46.0517	51.09	7.25	0.997

Tableau 3.3 : la performance comparée à l'exécution : MSE, PSNR et MSSIM.de l'image originale et étalée générée par le 2éme générateur

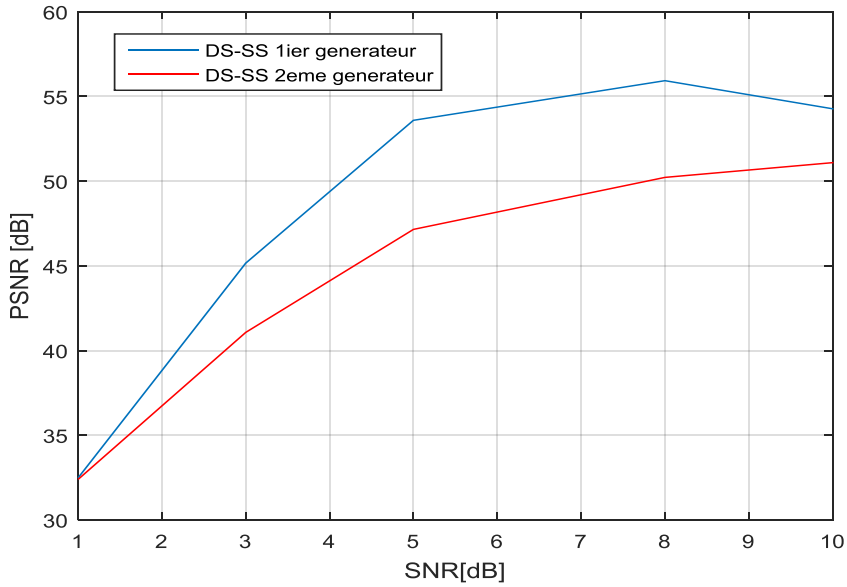


Figure 3.3: PSNR vers SNR et séquence d'étalement différente (DS-SS)

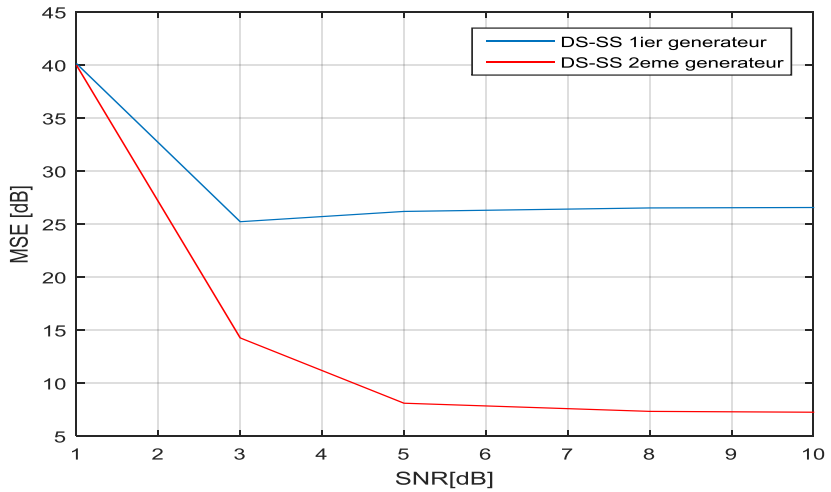


Figure 3.4 : MSE au SNR et séquence d'étalement différente (DS-SS).

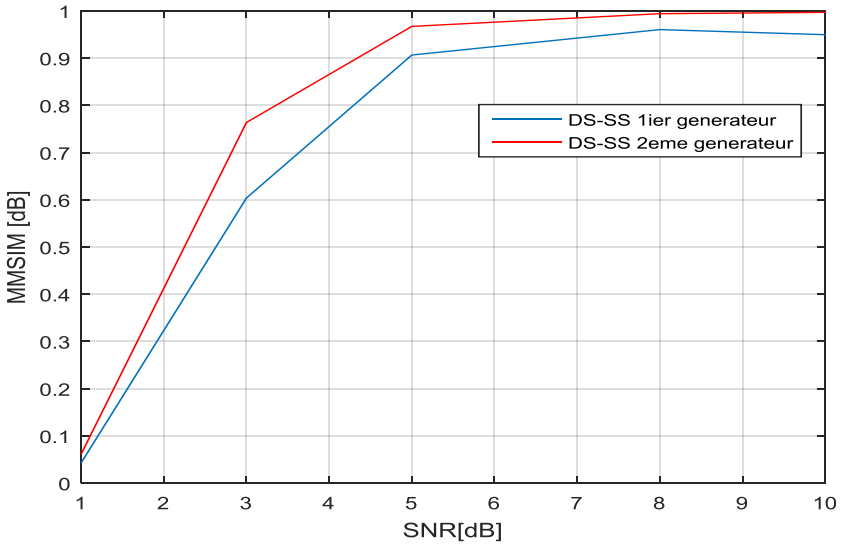


Figure 3.5 : Moyenne de SSIM au SNR et séquence d'étalement différente (DS-SS)

B. Simulation de l'image 2 :

1) 1er générateur

SNR	SNR (db)	PSNR	MSE	MMSIM
1	0	32.36	38.54	0.04189
3	21.9722	42.34	26.09	0.53415
5	32.1888	54.89	27.19	0.86412
8	41.5888	67.66	27.52	0.94776
10	46.0517	70.58	27.56	0.9559

Tableau 3.4 la performance comparée à l'exécution : MSE, PSNR et MSSIM.de l'image originale et étalée générée par le 1er générateur

2) 2éme générateur :

SNR	SNR (db)	PSNR	MSE	MMSIM
1	0	32.29	38.77	0.059668
3	21.9722	38.97	13.26	0.65449
5	32.1888	51.68	7.10	0.9418
8	41.5888	65.04	6.33	0.99078
10	46.0517	69.42	6.25	0.99505

Tablaue 3.5: la performance comparée à l'exécution : MSE, PSNR et MSSIM.de l'image originale et étalée générée par le 2éme générateur

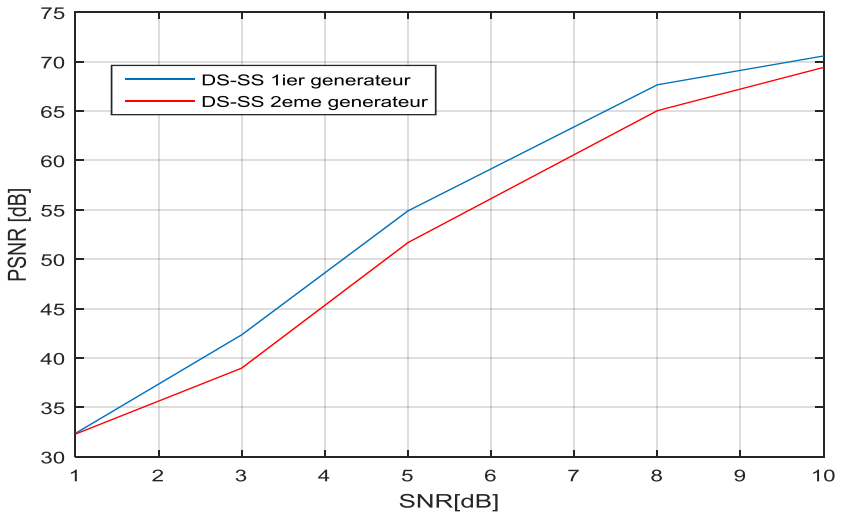


Figure 3.6 : *PSNR vers SNR et séquence d'étalement différente (DS-SS)*

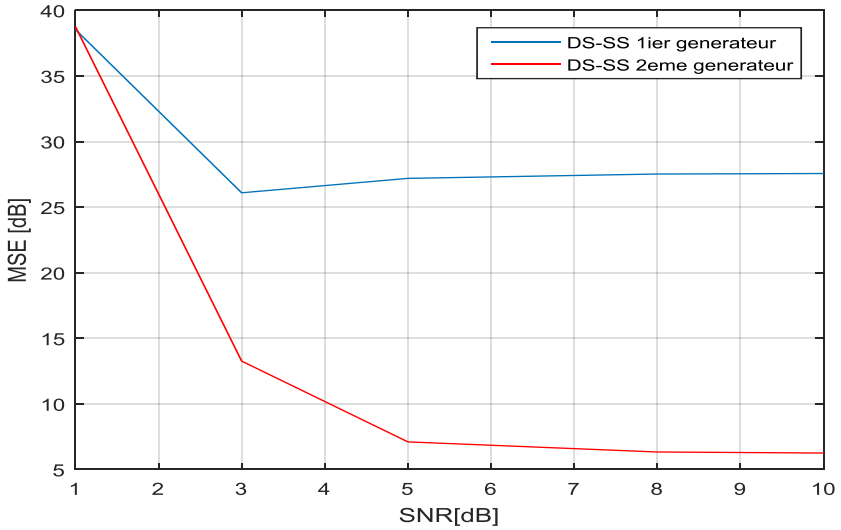


Figure 3.7 : *MSE à SNR et séquence d'étalement différente (DS-SS).*

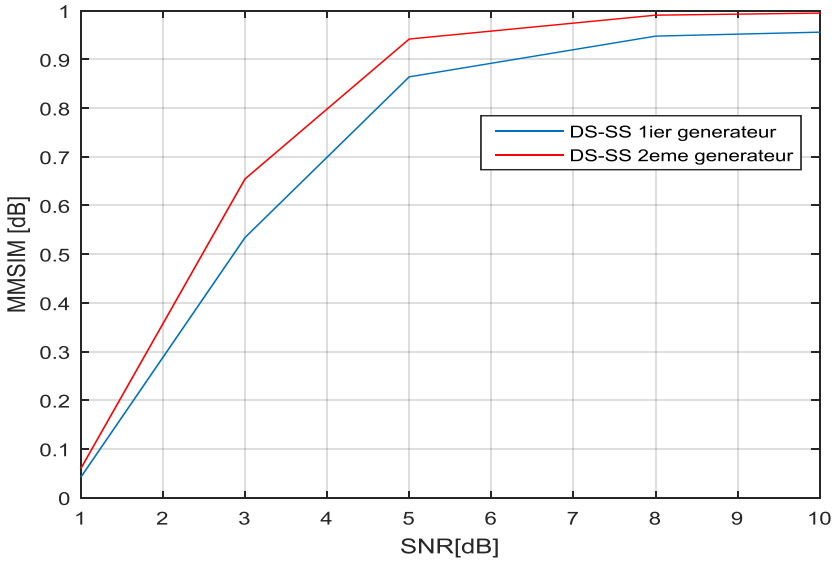


Figure 3.8: *Mean SSIM to SNR and different spreading sequence (DS-SS)*

Interprétation des résultats :

Une diminution exponentielle de l'erreur quadratique moyenne (MSE) est observée à la figure17 à mesure que la puissance augmente à la première étape. Les3 dB se rapportent à une diminution de la puissance ; le MSE s'approche à l'opposé près de 5db avec le 1er générateur, le MSE s'approche à l'opposé près de 5 db avec le 2ème générateur. En l'absence de bruit, les deux images sont identiques, et donc le MSE est Zéro. Dans ce cas, le PSNR est infini (voir figure 3.6). Les résultats obtenus sont également représentés sur les figures 3.7 et 3.8.

Cependant, le SSIM est meilleur pour l'original à certains SNR. Nous montrons ensuite la comparaison pour le 1er générateur et les algorithmes du 2ème générateur. Les expériences sont réalisées avec le 2ème générateur. La qualité de diffusion de l'image avec l'aide PSNR est très simple par rapport à MMSIM. L'efficacité de l'algorithme proposé en termes de qualité d'image accélérée pour le faible débit binaire. Il est clair que la différence entre PSNR et MSSIM est supérieure et inférieure pour le premier algorithme et les deux algorithmes. D'où la nouvelle performance chaotique et la taille de la clé du troisième 1er générateur. Ces propriétés sont adaptées à différentes applications telles que la sécurité.

3.5. Conclusion :

Nous concluons que les résultats obtenus sont très satisfaisants en termes de rapport d'étalement et de qualité d'image d'étalement. Ensuite le système de communication numérique pseudo générateur de chaos est basé dans le DS-SS et est très important. Ils ont des points forts différents et sont tout aussi importants. Ils sont basés sur deux cartes logistiques et de la séquence PN qui a été utilisée dans le système proposé et doivent être protégés dans le cas de l'utilisation des différentes méthodes.

Enfin on peut dire que cette méthode a bien agit pour l'amélioration de la qualité d'image transmise dans le système amélioré DS-SS.

Conclusion générale

Conclusion générale

Dans ce mémoire, nous avons étudié et expliquer le principe de fonctionnement des générateurs de séquences chaotiques en addition à l'amélioration de la qualité des systèmes de communications d'étalement de spectre par séquence direct DS-SS avec une application sur des images satellitaire.

Le but de ce projet de fin d'étude est de mettre en œuvre une amélioration de la sécurité d'un système de communication et l'évaluation de qualité d'image satellitaire par l'étalement DS-SS chaotique.

Les titres développés se présentent dans les points principaux qui se résument comme suit :

En premier chapitre nous avons présentés les généralités pour les transmissions à spectre étalé (DS-SS) à raison de sécurisations de ces systèmes, les générateurs de nombres aléatoires et leur sécurité par les cartes chaotiques, après on a passé à la définition des éléments principaux adjoints aux pseudos aléatoires plus la présentation des différents types des générateurs de nombres aléatoires existantes. On a encore ajouté le revenu de la description pour les générateurs chaotique issu de carte logistique, à l'étalement de spectre par la séquence direct pour la résolution du problème de sécurité au bout de la transmission par les cartes chaotiques. On a montré également la faisabilité de cette méthode dans la génération des cartes logistiques à travers deuxième chapitre.

Le deuxième point examine l'idée de chao issu des cartes logistiques et leur amélioration du système DS-SS. Cette participation a plusieurs concepts à savoir le choix des systèmes chaotiques convenables aux systèmes d'étalement par séquence directe. La présentation binaire avec la procédure d'extraction des

bits pseudo aléatoire. Premièrement une comparaison entre deux types de cartes qui sont : la carte logistique et la nouvelle carte logistique ***Sun, Y. et G.Y***. Wang. Ces deux systèmes chaotiques ont été utilisés pour la conception de notre algorithme de l'étalement de spectre par séquence direct. Après on a analysé que la nouvelle carte logistique ***Sun, Y. et G.Y. Wang***, possède de meilleures propriétés quantitatives.

Finalement, pour terminer on a interprété cette application dans une image d'un avion (RGB) où on a suggéré en perspective d'ajouter cette technique pour améliorer la sécurité par rapport à la carte chaotique précédente et la synchronisation qui peut être une bonne solution pour augmenter les performance.

Références Bibliographiques

[1] Yong Z .Plaintext Related Image Encryption Scheme Using Chaotic Map. TELKOMNIKA Indonesian Journal of Electrical Engineering. 2014 ;12 (1):635 -643.

[2] Michael L. Pseudo randomness and Cryptographic Applications, Princeton University Press, 1996.

[3] Don T. Principles of Spread-Spectrum Communication Systems, Springer Science Media, USA. 2005

[4] Stephen J. Chapman .Essentials of MATLAB Programming. Second Edition. Australia. 2009.

[5] Math Works Symbolic Math Toolbox™ 5 User's Guide. U.S. 2008

[6] Ahmadreza Amirzadeh. Amélioration de la sécurité et de la fiabilité des systèmes de communication sans fil. Maîtrise en génie électrique Maître ès sciences (M. Sc.). Québec, Canada. 2017

[7] Les réseaux informatique les modèles OSI et TCP wikilivres wikibooks.org

[8] Alfred J. Menezes , Paul C. van Oorschot Scott A. Vanstone. APPLIED CRYPTOGRAPHY. USA:Massachusetts Institute of Technology. 1996.

[9] Behrouz F athi .Vajargah , Rahim Asghari . A Pseudo Random Number Generator Based on Chaotic Henon Map (CHCG) . IJMCE international journal of machatronics Electrical and computer Technology . 2015 ; 5(15) : 2120-2129.

[10] René Parfait, les réseaux de télécommunication, Lavoisier, 2002.

[11] Amel Aissaoui, 'Synchronisation Adaptative du code PN Dans les systèmes de communication DS/SS ', juin 2008.

[12] 3GPP-201, 'TS.25.201 UMTS; Physical layer-general description' 3GPP Technical Specification, Tech. Rep. March 2001, version 4.0.0.

[13] IEEE 11.B, 'IEEE Standard 802.11b,' IEEE Standardization, Tech. Rep., 1999.

[14] IEEE 15.1,'IEEE Standard 802.15.1, Specification of the Bluetooth system, version 1.2, ' IEEE Standardization, Tech. Rep., November 2003.

[15] Amit T, Abhishek Z, Rohit H. Pseudo Chaotic Sequence Generator based DS-SS Communication System using FPGA. International Conference on Industrial Automation and Computing. United Kingdom. 2014: 13-18.

[16] Glaviaux A. Information Theory and codage. UK: ENST Bretagne National High School of Telecommunications of Brittany. 1990; VII: 2-10

[17] Meel J. Spread Spectrum (SS) Introduction. Iwt Hobu-Fonds. De Nayer Institute Belium. 1999.

[18] Wai M Tam; Francis C M Lau; Chi Kong Tse. Digital communications with chaos: multiple access techniques and performance. UK; Elsevier. 2007: 8.

[19] Vilas.S.Bagad .Wireless communication . Technical publications Pune. Faculty ,nstitute Of Telecommunication Management , Ex-Faculty Sinhgad College of Engineering ,Pune. First Edition 2009.

[20]IKHLEF ISMAHENE .l'analyse Du Systeme d'acquisition Multi-Porteuse A Sequence Directe (Mc-Ds-Cdma) Dans Un Canal Rayleigh. Thèse Doctorat En Sciences . Universite mentouri de constantine.

[21] Marie-Line Zani-Demange. Les liaisons radio. Communication par radiofréquences. Solutions. MESURES 793 . 2007.

[22] Deng .Lih. Yuan. Efficient and portable multiple recursive generators of large order. Modeling Comput. 2005.15(1):1–13.

[23] Youssef M. Modeling. Simulation and Optimization of Receiver Architectures of the W-Cdma Technical Access. Phd thesis. France: Ecole Doctorale IAEM – Lorraine. DFDE- E University Paul Verlaine – Metz. 2009.

[24] KRIM M . A. ALI PACHA . Implémentation Des Générateurs Pseudo Aléatoire : Etudes Et Applications. MEMOIRE EN VUE DE L'OBTENTION DU MAGISTER OPTION : Systèmes de Communication Modernes (SCM). Université des Sciences et de la Technologie d'Oran MOHAMED Boudiaf. 2010

[25] I.Anusha , T.Sarath Babu . Acquisition of Long Pseudo Code in DSSS Signal. IJMER International journal of modern Engineering Research. 2013; 3(4): 2062-2065.

[26] Zeraoulia Elhadj**.** Etude de quelques types de systemes chaotiques : généralisation d'un modele issu du modele de chen .These presentee pour l'obtention du doctorat en sciences en mathématiques université mentouri de constantine de ssciences .2006

[27] Ljupco Kocarev; et al . Chaos-based cryptography. Studies in computational intelligence, vol. 354. Berlin : Springer, 2011.

[28] A. Ali-Pacha A, N. Hadj-Said, B. Belmekki, A. Belghoraf. Chaotic Behaviour for the Secrete key of Cryptographic System. Revue Elsevier Science : Chaos, Solitons & Fractals, Volume 23/5 pp. 1549-1552. Available online October 2004.

[29] A. Ali-Pacha, N. Hadj-Said, A. M"Hamed, A. Belghoraf, .Lorenz's Attractor Applied to the Stream Cipher (Ali-Pacha Generator). Revue Elsevier Science : Chaos, Solitons & Fractals, Volume 33/5 pp.1762-1766. Available online August 2007.

[30] A. ALI-PACHA, N. HADJ-SAID, A. M'HAMED , A. BELGHORAF.Chaos Crypto-Système basé sur l'Attracteur de Hénon-Lozi. Université des Sciences et de la Technologie d'Oran USTO BP 1505 El M'Naouer Oran 31036 ALGERIE Https://pdfs.semanticscholar.org/5c99/50a82b2731d7ea4edd6700325a7e9eaa39d0.pdf.

[31] John S Nicolis. Chaos and information processing - A heuristic Outline. World Scientific Amzon France 1991.

[32] Ali Bulent .Caubel. Applied chaos theory : a paradigm for complexity**.** Boston : Academic Press . 1993.

[33] Gonzalo Alvarez, and Shujun .Li .*Some basic cryptographic requirements for chaos-based cryptosystems*. *International Journal of Bifurcation and Chaos*. 2006; 16(8): 2129-2151.

[34] Andaç B. Beam Coding With Spread Spectrum Orthogonal Gold Codes In Underwater Acoustic Systems. Thesis Master of Science in electrical and electronics engineering. Bilkent university; 2015.

[35] Yu-Gunany yang ,Qian-Qiant Zhao . Novel pseudo-random number generator based on quantum random walks .Scientific Reports. 2016; 6: 20362 : 1-11.

[36] Naim Khodor. Application des fonctions génératrices de chaos à la réalisation de codeurs de canal . These docteur. françe : l'universite de limoges. 2010.

[37] M. Bloch et J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Royaume-Uni : Cambridge University Press, 2011.

[38] R. Ursulean, Reconsidering the generalized Logistic map as a pseudo random bit generator, ELECTRONIKA IR ELECTROTECHNIKA,.2004; 7(56):10-13.

[39] Naim Khodor. Application des fonctions génératrices de chaos à la réalisation de codeurs de canal . These docteur. Françe : l'universite de limoges. 2010.

[40] Mahalinga V Mandi, Ramesh S, Santhosh Kula, Santosh Kumar S, Dileep D, Yajnesh P. An FPGA implementation of a pseudo chaotic direct sequence spread spectrum (DS-SS) communication system. International Journal of nonlinair science. 2009; 8(4): 387-401.

[41] BELLAHBIB HadhoumNadjet ,ABDELLI Ikram. « L'EXPLOITATION DU CHAOS NUMERIQUE DANS LES TRANSMISSIONS SECURISEES» Master en Télécommunications, Option : Technologies des Systèmes de Télécommunication. UNIVERSITE ABOU-BEKR BELKAID- TLEMCEN. juin 2017

[42] M. Bloch et J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Royaume-Uni : Cambridge University Press, 2011.

[43] ABDERRAHIM nassibawafa. Étude et conception d'un modèle chaotique dédié aux transmissions chiffrées, thèse de doctorat, UNIVERSITE ABOU-BEKR BELKAID, 2015.

[44] Robert M. M. Simple Mathematical Models with very Complicated Dynamics. Nature.1976; 1-9.

[45] Hua X, Shubin W, Xiandong M. Logistic Map Study on One Modified Chaotic System Based. *Research Journal of Applied Sciences*. 2013; 5(3): 898-904.

[46] KRIM M . A. ALI PACHA . Implémentation Des Générateurs Pseudo Aléatoire : Etudes Et Applications. MEMOIRE EN VUE DE L'OBTENTION DU MAGISTER OPTION : Systèmes de Communication Modernes (SCM). Université des Sciences et de la Technologie d'Oran MOHAMED Boudiaf. 2010

[47] R. Muraoka,D.covarrubias ,A.Arvizu&j.Mendieta .Design and Implementation of a CDMA Transmitter for Mobile Cellular Communications. JART Journal of pplied Research and Technology. 2003, 1(2):127-136.

[48] Wai M Tam; Francis C M Lau; Chi Kong Tse. Digital communications with chaos: multiple access techniques and performance. UK; Elsevier.2007: 8.

[49] R. Zhu and Y. Ma (eds.), Information Engineering and Applications, Lecture Notes in Electrical Engineering 154, DOI: 10.1007/978-1-4471-2386-6-107, Springer-Verlag London Limited 2012.

[50] F.Alin.contribution à la prédiction et au contrôle des comportements apériodiques dans les convertisseurs électromécaniques : application de la théorie du chaos .thèse de doctorat .Reims 2005.
[51] Pallavisini.A. A Radio Frequncy Interference System for Chaos Cryptography applied to Radio Transmissions .DOCTOR Thesis. France. Engineering sciences physics.University Doctor Rank. 2007.

[52] K.RajaRajeswari ,P.SrichariP.Rajesh Kumar ,M.Murrali,VJagan Naveen , G.MammadhaRao .New figures of merit for range resolution radar using hamming and euclideau distance concepts . Proceedings of the7th wseas International Conference On Multimedia Systems & Signal Processing, China.2007.139-145.

[53] techterms.com