République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université 8 Mai 1945 – Guelma

Faculté des Sciences et de la Technologie
Département d'Electronique et Télécommunications

THÈSE

En Vue de l'obtention du diplôme de

DOCTORAT

Filière : Electronique et Télécommunications

Présentée par

Amara Korba Karima

Intitulée

La Sécurité des Réseaux de Capteurs sans fil Multimédia par des Systèmes Chaotiques

---

Soutenue le 08/09/2022 devant le Jury composé de :

Président du jury :	Pr. BOUDJEHEM Badreddine	Univ. De Guelma
Directeur de Thèse :	Pr. ABED Djamel	Univ. De Guelma
Co-directeur de thèse :	Pr. FEZARI Mohamed	Univ. De Annaba
Rapporteurs :		
Pr. MOUSSAOUI Abdelkrim		Univ. De Guelma
Pr. LAKEL Rabeh		Univ. De Annaba
Invité : M. Mehallel Elhadi (MCA)		Univ. De Djelfa

Année Universitaire : 2021/2022

مخبر التحكم المتقدم

Advanced Control Laboratory

La Sécurité des Réseaux de Capteurs sans fil Multimédia par des Systèmes Chaotiques

Amara Korba Karima

Pour citer cette thèse

AMARA KORBA, K. La Sécurité des Réseaux de Capteurs sans-fil Multimédia par des Systèmes Chaotiques (Doctoral dissertation, Université 8 mai 1945 de Guelma). Google citation

Publications:

1. Korba, K.A., Abed, D. & Fezari, M. Securing physical layer using new chaotic parametric maps. Multimed Tools Appl 80, 32595–32613 (2021). https://doi.org/10.1007/s11042-021-11226-y.
2. Amara Korba, K., Djamel, A., Mohamed, F. et al. New chaotic map for real-time medical imaging system in e-Health. J Ambient Intell Human Comput (2022). https://doi.org/10.1007/s12652-022-04107-1.

Remerciements

Au terme de ce travail, je remercie « الله سبحانه وتعالى » de m'avoir donné la volonté et le courage qui m'ont permis de réaliser ce travail, puisse-t-il me guider dans le droit chemin.

Je tiens à remercier toute ma famille, en particulier ma chère Mère, mon frère Raouf et mes oncles Abdelkrim et Abdelmalek pour leurs aides si précieuses, mon frère Adel ainsi qu'à ma sœur Nora, mon neveu et mes nièces pour leur appui indéfectible tout au long de mon parcours de doctorat et sans qui tout cela n'aurait pas pu être possible.

Je voudrais aussi remercier mes deux encadrants *M.* Abed Djamel et *M.* Fezari Mohamed pour toutes leurs aides, leurs conseils, ainsi que leurs encouragements.

*J'*ai effectué les travaux de recherche au sein du Laboratoire de contrôle avancé (LABCAV) du Département de L'électronique, Université du 08 Mai 1945 Guelma.

*M*es remerciements les plus vifs vont à *M*onsieur Boudjehem Djalil le Directeur du laboratoire pour ces remarques très utiles tout au long de mon parcours de thèse.

Je tiens à remercier les membres de mon jury : *M.* MOUSSAOUI Abdelkrim, *M*LAKEL Rabeh, qui m'ont honoré en acceptant de soigneusement étudier ce manuscrit et qui m'ont fait l'honneur d'évaluer ce travail, je remercie tout autant, *M.* BOUDJEHEM Badreddine, d'en avoir accepté la présidence.

Et enfin Je tiens à remercier toutes les personnes qui m'ont soutenu, encouragé et ont contribué au bon déroulement de cette thèse.

Résumé

Titre : La Sécurité des Réseaux de Capteurs sans-fil Multimédia par des Systèmes Chaotiques

L'objectif principal de cette thèse est la conception de nouvelles cartes chaotiques pour la transmission sécurisée des images dans la couche physique des réseaux de capteurs multimédia sans fil. Pour pallier les défauts des cartes chaotiques standard et créer une dynamique chaotique plus complexe, nous proposons l'hybridation entre deux cartes en cascade. Les cartes chaotiques discrètes utilisées sont : la nouvelle carte cubique qui a été développée, la carte du chat d'Arnold et la carte sinus

Dans cette thèse, deux nouvelles conceptions de cartes paramétriques en cascade ont été développées ; la carte chaotiques 3D Cubique-Sinus et la carte 2D Cubique-Cat, la première carte a été utilisée comme générateur chaotique de nombre pseudo aléatoire pour le chiffrement d'images avec deux techniques ; la cryptographie et la stéganographie la deuxième carte a été utilisée pour le chiffrement de la modulation d'amplitude en quadrature (QAM).

Des simulations de la complexité dynamique ont été effectuées pour les nouvelles cartes proposées ainsi qu'une simulation de transmission en OFDM des images chiffrées.

Une analyse des valeurs PSNR et BER pour l'évaluation de la qualité de transmission a été présentée. Les résultats expérimentaux d'analyse de la sécurité des images chiffrée et de la qualité des images obtenues après transmission montrent clairement l'efficacité et la robustesse des méthodes proposées dans cette thèse.

Mots clés : Chiffrement chaotique, Multiplexage par répartition orthogonale de la fréquence (OFDM), Sécurité de la couche physique, Stéganographie.

Abstract

Title: Secure Wireless Multimedia Sensor Networks using Chaotic Systems.

The main purpose of this thesis is to generate new chaotic maps to secure the transmission of images in the physical layer of wireless multimedia sensor networks. To overcome the flaws of standard chaotic maps and create more complex chaotic dynamics, we suggest hybridization between two cascading maps.

The discrete chaotic maps used are: the new cubic map that has been developed, the Arnold's cat map and the sine map.

In this thesis, we generate two new chaotic parametric cascaded maps 3D Cubic-Sine map and 2D Cubic-Cat map, the first map was used as a chaotic pseudo-random number generator for image encryption with two techniques; cryptography and steganography the second map was used for quadrature amplitude modulation scrambling (QAM).

Simulations of complexity dynamics were carried out for the new maps proposed as well as a simulation of transmission using OFDM for the encrypted images with an analysis of the PSNR and BER values as evaluation parameters of the transmission's quality.

The experimental result's analysis of the security of the encrypted images and their quality obtained after transmission clearly show the effectiveness and the robustness of the methods proposed in this thesis.

Keywords: Chaotic encryption · Multicarrier frequency-division multiplexing (OFDM), Physical layer security, Steganography.

الملخص

العنوان: أمن شبكات الاستشعار اللاسلكية المتعددة الوسائط بواسطة نظم الحركة العشوائية (الفوضى)

الهدف الرئيسي من هذه الأطروحة هو ابتكار تصاميم لبطاقات أو لخرائط فوضوية جديدة لتأمين إرسال الصور عن طريق التشفير في الطبقة المادية لشبكات استشعار الوسائط المتعددة اللاسلكية(WMSNs) . الطريقة المقترحة للتغلب على أوجه القصور في البطاقات الفوضوية القياسية أو الكلاسيكية لتحسينها وخلق ديناميكيات فوضوية أكثر تعقيدًا هي استخدام التهجين أو المزيج بين بطاقتين بالتسلسل أو بالتعاقب.

البطاقات التي تم استخدامها هي ثلاث بطاقات أحادية الأبعاد: بطاقة المكعبة الجديدة التي تم ابتكارها وتطويرها، بطاقة أرنولد القط وبطاقة الجيب الكلاسيكية.

في هذه الأطروحة، نقترح تصميمان لبطاقتين جديدتين هجينين معلمتين: البطاقة ثلاثية الأبعاد: المكعبة – الجيبية والبطاقة ثنائية الأبعاد المكعبة – أرنولد القط، تم استخدام البطاقة الأولى كمولد أرقام شبه عشوائي لتشفير الصور بتقنيتين؛ التشفير والتورية بمقاربة جديدة، تم استخدام البطاقة الثانية لتشفير تعديل السعة التربيعية (QAM).

تم إجراء محاكاة لديناميكيات البطاقات الجديدة المقترحة بالإضافة إلى محاكاة بتقنية، تعدد الإرسال باستخدام الترددات المتعامدة (OFDM)«او اف دي ام» للصور المشفرة مع تحليل قيمPSNR ، BER لتقييم جودة الإرسال.

تظهر بوضوح النتائج التجريبية التي تم الحصول عليها لتحليل أمان الصور المشفرة وجودة الصور عند الاستقبال فعالية وقوة الأساليب المقترحة في هذه الرسالة.

الكلمات المفتاحية: التشفير الفوضوي، تعدد الإرسال باستخدام الترددات المتعامدة (OFDM)" او اف دي ام" ، أمن الطبقة المادية، التورية أو ستيغانوغرافي

Table des matières

Liste des figures

CHAPITRE I

CHAPITRE II

CHAPITRE III

CHAPITRE IV

Liste des tableaux

Liste des acronymes et abréviations

ADC	Analog-to-Digital Converter	Convertisseur Analogique digitale(numérique)
AWGN	Additive White Gaussian Noise	Bruit additif Blanc Gaussien
AI	Artificial intelligence	Intelligence artificielle
BER	Bit Error Rate	Taux d'erreur binaire
CMOS	Complementary Metal Oxide Semiconductor	Semi-conducteurs à Oxyde de Métal Complémentaire
CPRNG	Chaotic Pseudo Random Number Generator	Générateur chaotique de nombres pseudo-aléatoires
CP	Cyclic prefix	Préfixe cyclique
DAC	Digital-to-Analog Converter	Convertisseur numérique analogique
DL	Deep learning	L'apprentissage profond
DoS	Denial of Service	Déni de service
DSP	Digital Signal Processing	Traitement des signaux numériques
FPGA	Field Programmable Gate Array	Réseau de porte programmable par l'utilisateur.
ISI	Inter-Symbol-Interference	Interférence inter symbole
I/Q	In-phase/Quadrature	Modulation :de phase /en quadrature
IoT	Internet of things	L'Internet des objets
IoMT	Internet of Multimedia Things	Internet des objets multimédias
IoV	Internet of vehicles	L'internet des véhicules
IRDA	Infrared Communication	Communication infrarouge
IEEE	Institute of Electrical and Electronics Engineers	Instituts des ingénieurs électriques et électroniques
LE	Lyapunov Exponent	L'exposant de Lyapunov
MIMO	Multi Input Multi Output	Multi-entrées multi-sorties
ML	Machine learning	L'apprentissage automatique (ML)
NPCR	Number of Pixel Change Rate	Taux de changement du nombre de pixels
OFDM	Orthogonal Frequency Division Multiplexing	Multiplexage par répartition orthogonale de la fréquence
OFDMA	Orthogonal Frequency Division Multiple Access	Accès multiple par répartition orthogonale de la fréquence
OSI	Open Systems Interconnection	Interconnexion de Systèmes ouverts

P / S	Parallel -to- Series Conversion	Conversion Parallèle-Série
PAPR	Peak to Average Power Ratio	Rapport entre puissance crête et puissance moyenne
PHY	Physical Layer	Couche physique
PON	Passive optical network	Réseau optique passif
PRNG	Pseudo Random Number Generator	Générateur de nombres pseudo-aléatoire
PSNR :	Peak Signal to Noise Ratio	Rapport signal sur bruit de crête
QAM	Quadrature Amplitude Modulation.	La modulation d'amplitude en quadrature
QoS	Quality of Service	Qualité de Service
RNG	Random Number Generator	Générateur de nombre aléatoire
S / P	Series-to-Parallel Conversion	Conversion Série-Parallèle
SISO	Single Input Single Output	Une seule entrée et une seule sortie
SNR	Signal to Noise Ratio	Rapport signal/bruit
SoC	System on Chip	Système sur puce ou système mono-puce
SCMOS	Scientific CMOS	Scientifique CMOS
TinyOS	Tiny Operating System.	Système d'exploitation minuscule
UACI	Unified Average Changing Intensity	Changement moyen de l'intensité unifiée
UWB	Ultra-Wide band	Ultra-large Bande
UAVs	Unmanned Aerial Vehicle e	Réseaux de véhicules aériens sans pilote
VC	Visual cryptography	La cryptographie visuelle
Wi-Fi	Wireless Fidelity	Fidélité sans fil
WMSNs	Wireless Multimedia Sensors Networks	Réseaux de capteurs multimédias sans fil
XOR :	Exclusive OR	OU exclusif

Introduction générale

De nos jours, les capteurs ont été déployés dans tout l'environnement de la vie quotidienne, intégrés dans les téléphones intelligents, les montres intelligentes et d'autres terminaux sans fil, deviennent des nécessités de la vie quotidienne moderne. Avec les progrès de l'Internet des objets multimédias (IoMT) et de l'intelligence artificielle (IA), davantage de dispositifs de détection sans fil seront utilisés, les données multimédias sont une opportunité pour le développement des technologies basées sur les réseaux sans fil. Les recherches sur les WMSNs portent principalement sur le matériel ; la capacité de chargement et de calcul, les protocoles de routage des communications mais aussi sur la sécurité de l'information.

Les mécanismes de sécurité, de confidentialité dans les réseaux de capteurs doivent encore être approfondis et renforcés, les données doivent être protégées de manière adéquate pour éviter leurs divulgation et modification à la suite d'attaques passives et actives.

Bien que les systèmes de communications sans fil offrent des avantages significatifs en termes de mobilité ; un environnement de propagation aléatoire ; plusieurs degrés d'entrées et sorties ; une conception de forme d'onde flexible, leurs vulnérabilités, due à la nature de diffusion des ondes radio est un inconvénient en termes de sécurité de transmission. Les menaces de sécurité sont énormes pour les réseaux de capteurs multimédia, causées par la transmission de données sur réseau plus encore lors de la connexion à Internet, tous les capteurs en réseau doivent faire face aux mêmes problèmes, que ce soit pour les expéditeurs ou les destinataires des données.

Afin de protéger les informations véhiculées par les signaux sans fil contre l'extraction par des nœuds malveillants, c'est-à-dire les espions, les techniques de sécurité au niveau de la couche physique ont fourni des solutions prometteuses complémentaires aux techniques conventionnelles, en particulier pour les besoins de communications critiques tels que l'armée, la sécurité publique, la surveillance de la santé et la transmission d'informations privées.

Contrairement aux méthodes de sécurité conventionnelles, les techniques de couche physique visent à rendre le signal sans signification pour les nœuds malveillants dans la couche la plus basse possible avec une gestion et une mise en œuvre prudentes, la sécurité de la couche physique et les techniques de cryptage peuvent fournir une solution de sécurité bien intégrée qui protège efficacement les données de communication confidentielles et privées.

Dans la littérature peu de schémas de chiffrement sont adaptés aux WMSNs, actuellement, la technologie de cryptage à base de chaos a progressivement été appliquée aux champs de sécurité. Ces dernières années le chaos montre de nouvelles directions de recherche pour son application dans les WMSNs. Le développement de nouveaux systèmes chaotiques, qui permettent un haut rendement et une haute performance de sécurité est le principal objectif de cette thèse. Les solutions proposées sont basées sur la conception de nouvelles cartes chaotiques générées à partir du mixage en cascade et en parallèle des cartes chaotiques standards, le but étant de pallier les défauts des cartes chaotiques standards et créer une dynamique chaotique plus complexe.

Une nouvelle carte chaotique nommée cubique a été développée à paramètres variés avec une complexité dynamique exceptionnelle offrant un niveau élevé des séquences chaotiques pseudo-aléatoires et un large espace clé, ensuite nous avons généré deux nouvelles structures en cascade, avec comme noyau la carté cubique développée : la carte tridimensionnelle Cubique-Sinus et la carte bidimensionnelle Cubique-Cat.

Pour assurer la sécurité de la transmission d'images en OFDM au niveau de la couche physique, nous introduisons plusieurs techniques basées sur les nouvelles cartes développées avec une nouvelle approche en sténographie et cryptage des symboles au niveau de la modulation d'amplitude en quadrature (QAM).

Cette thèse est organisée en quatre chapitres, le chapitre I est subdivisé en deux parties, la première partie est consacrée à l'état de l'art sur les réseaux de capteur multimédia où on présente d'abord en détail leurs structures, l'architecture du nœud multimédia ainsi que les protocoles de communication en mettant l'accent sur les technologies clés, les principaux travaux de recherche actuels, les défis et les tendances de développement futures. Ensuite des solutions émergentes sont présentées pour la conception des réseaux de capteurs multimédias optimisés dans différentes technologies. Nous concluons le chapitre par un l'état de l'art approfondi sur la couche physique OFDM en présentant la synthèse des principaux travaux effectués dans la littérature.

Dans le chapitre II, nous présentons les différentes techniques de sécurisation des réseaux de capteurs sans fil en mettant l'accent en deuxième lieu sur les transmissions sécurisées basées sur les cartes chaotiques. Dans le chapitre III, nous présentons les modèles de cartes chaotiques développées par « Mixage en cascade », avec une analyse de leur comportement dynamique. Le chapitre IV est dédié à la présentation des résultats de simulation, les résultats de chiffrement d'images dans une chaine de transmission OFDM sont présentées avec une cryptanalyse du système de transmission proposé, la thèse se termine par une conclusion et quelques perspectives.

I

Chapitre I :
Etat de l'art sur les WMSNs

I.1. Introduction :

Le terme multimédia est défini de diverses façons, pour certains, il s'agit de la combinaison de médias tels que le son et l'image et selon le sens le plus utilisé, un signal multimédia se caractérise par l'intégration d'au moins deux signaux parmi le texte, les graphiques, les images, le son et les séquences vidéo. Ce sens s'étend lentement pour inclure la notion d'interactivité ainsi, un signal de télévision n'est plus considéré comme un signal multimédia pour la simple raison que l'interactivité est inexistante[1].

Le terme réseaux de capteurs multimédias sans fil (WMSNs) désigne des systèmes autoorganisés de dispositifs embarqués appelés les nœuds capteurs déployés pour récupérer, traiter et assembler des flux multimédias de différentes sources.

Le terme réseaux ad hoc désigne un réseau qui n'est pas fondé sur une infrastructure existante, le réseau doit permettre à n'importe quelle paire de nœuds de communiquer en relayant l'information via d'autres nœuds sans l'aide d'un router dans un contexte de mobilité dynamique avec un changement de topologie fréquent.

Les réseaux ad hoc sont conçus pour un usage spécifique et adaptés à un environnement où il n'y a pas ou il n'y a plus d'infrastructure par exemple dans une situation d'urgence : un champ de bataille, catastrophe naturelle ou pour applications orientées utilisateur tels que les conférences, les véhicules ou les drones [2].

L'imagerie aérienne thermique, multispectrale et hyperspectrale, ainsi que le radar ont favorisé le développement des WMSNs sophistiqués avec des tâches multimédias difficiles principalement dans les domaines du contrôle et de la surveillance urbaines et la surveillance des frontières, la reconnaissance, la localisation et le dénombrement d'objets, le suivi des cibles, la surveillance des incendies et de l'environnement. [3].

Les WMSNs sont des outils de mesure efficaces dans un processus de surveillance des changements environnementaux pour l'exercice d'un certain contrôle et prises de décisions sur l'environnement en répondant à ces changements. L'aspect décisionnel peut être inclus à l'intérieur du réseau ou laissé à l'extérieur.

Les WMSNs se composent de nœuds de capteurs comme la brique essentielle de la structure. Dans sa forme basique la plus simple il comporte plusieurs nœuds qui communiquent directement avec la station de base.

Les nœuds de capteurs sont des systèmes autonomes interconnectés, avec des dispositifs de détection intégrés munis de processeurs, une communication sans fil émetteur-récepteur est un circuit d'alimentation où les dispositifs de détection sont des multimédias, tels que des caméras et des microphones, capables de détection et de calcul utilisant logiciel, matériel et algorithmes, ils fonctionnent selon des techniques de traitement de l'information et des protocoles de communication[4].

En fonction des exigences imposées par l'application, et bien évidemment en fonction du type de technologie disponible, les réseaux de capteurs WMSNs peuvent être de deux types :

1) Les réseaux de capteurs d'images :

Des réseaux de capteurs sans fil spécifique constitués de caméras (des capteurs optiques) déployés dans un domaine d'intérêt, ils capturent des images mémorisées en format matriciel ou vectoriel à différents endroits et envoient leurs observations à une station de base ou à un ou plusieurs puits selon la topologie du réseau. Dans ces réseaux, l'un des principaux défis est de traiter et transmettre des images qui représentent des données de grande taille[5].

2) Les réseaux de capteurs de vidéo

Les Wireless Video Sensor Networks (WVSN) en anglais sont des capteurs d'images numériques chargés de prendre des séquences d'images et de transmettre le flux vidéo vers la station de base ou bien le puits selon la topologie du réseau. Une mesure du capteur vidéo fournit un ensemble de données à deux dimensions (2D) qui passe à trois dimensions (3D) en comptant la dimension temporelle. Entrainant par ailleurs une plus grande complexité de traitement et d'analyse des données. En conséquence, des défis particuliers à relever qui ont donné suite à beaucoup de travaux de recherches pour la compression d'image et économie en énergie dans les WSMNs dans le but de prolonger la durée de vie du réseau. Les premiers travaux de recherches ont débuté dans les années 2000 dès lors, quelques travaux plus spécialisés ont été proposés [6].

I.2. Les défis de la recherche et développement des WMSNs

Une prolifération omniprésente des applications multimédias des réseaux de capteurs sans fil pose des défis importants et difficiles en raison des contraintes techniques et financières des nœuds tels que la

consommation d'énergie, le coût et l'incapacité de l'infrastructure du réseau sans fil actuelle à gérer ses énormes quantités de données.

I.2.1. La sécurité

Les menaces à la sécurité, au secret et à la vie privée sont énormes. Pour les réseaux de capteurs, en outre, que ce soit pour les expéditeurs ou les destinataires, les données doivent être protégées de manière adéquate pour éviter la divulgation de la confidentialité et la modification des données contre les attaques passives et actives en transit. La future ère de l'IoT ainsi que les réseaux de capteurs orientés Internet mettent l'accent sur les interactions autonomes entre les objets (capteurs), les rendant «intelligents», mais les assiègent également avec des attaquants [7]. Ainsi, les mécanismes de sécurité, de confidentialité dans les réseaux de capteurs doivent encore être étudiés et renforcés. Ce volet est bien détaillé dans la partie 2 de ce chapitre

I.2.2. La latence

La vision des WMSNs est de fournir des applications multimédias en temps réel à l'aide de capteurs sans fil déployés pour une utilisation à long terme. Par exemple, lorsqu'un intrus pénètre dans la zone de surveillance, le nœud du capteur d'image doit accélérer l'acquisition, accélérer le traitement et transmettre en temps réel. Pour assurer au mieux la qualité de service pour les données et les applications multimédias en temps réel, les WMSNs ont introduit de nouveaux défis dans la hiérarchisation des protocoles de routage multivoie [8].

I.2.3. Les distorsions

Les distorsions de transmission des données d'image induites par les défaillances de canaux pour les WMSNs doivent être pris en considération. Des canaux stables peuvent maintenir une bonne qualité de transmission du flux de données et ainsi minimiser les frais généraux de commutation de canal tels que le délai de commutation, la consommation d'énergie et la perte de données associées. Un protocole de routage proposé permettant de minimiser efficacement la distorsion totale lors du transfert de données vidéos dans les WMSNs est proposé dans [9].

I.2.4. Le codage

Pour le codage d'un signal simple tel que le niveau de température ou la pression un ou deux octets sont suffisants, le codage d'une image numérique conduit à l'emploi de plusieurs centaines ou milliers d'octets. Cette différence de grandeur a des conséquences sur différents facteurs : capture du signal, besoins en mémoire, traitement du signal et transmission de données [10].

Dans Pudlewski et al.,2014 [11], les auteurs listent quatre défis que les concepteurs d'encodeurs vidéo pour les WMSNs doivent surmonter : les contraintes de débit, les contraintes de complexité, les conditions du canal et les contraintes du réseau. La complexité de l'encodeur et la faible résilience aux erreurs de canal constituent les deux limites majeures des systèmes de transmission vidéo codés.

I.2.5. La capacité mémoire

La mesure d'un capteur d'image est composée de nombreuses mesures distinctes, une pour chaque élément photosensible dans le capteur. Toutes les mesures sont du même type (c'est-à-dire l'intensité de la lumière) mais chacun provient d'une source différente déterminée par la lentille optique. Le nombre précis de mesures dépend de la structure et peut aller de six dans un très petit réseau linéaire à plusieurs millions pour un capteur d'image couleur haute résolution. En termes simples, chaque mesure fournit plusieurs points de données au nœud, par exemple un ensemble de valeurs à deux dimensions. Ceci est en contraste avec le signal unidimensionnel typique produit par d'autres types de détection. Ce goulot d'étranglement a conduit à beaucoup de recherches vers de nouvelles mémoires non volatiles, qui doivent être facilement intégrables, rapides, petites, fiables et pas chères. Les principales nouvelles approches technologiques sont listées dans [12].

I.2.6. La compression

La transmission de données multimédias nécessite un stockage énorme et une bande passante élevée. Une solution pour économiser l'énergie et réduire la quantité de données à envoyer est d'utiliser la compression de données. Compresser les données pendant la transmission avec un débit de données plus élevées est l'un des défis à relever pour la recherche actuelle. Les séquences d'images doivent être compressées fortement pour satisfaire à la contrainte de bande passante et des liaisons sans fil. Au cours des dernières décennies, de nombreuses techniques de compression ont été proposées et peuvent être divisées en deux catégories : les méthodes de la transformée en cosinus discrète (DCT) et de la transformée en ondelettes discrète (DWT) [13],[10].

Une nouvelle approche par réseau neuronal est utilisée pour allouer une bande passante maximale pour les nœuds lors des transmissions des données et pour l'affectation dynamique des canaux des nœuds (Bandwidth allocation) est présentée dans [14].

Diverses recherches ont abouti à de nouvelles technologies qui ont permis de transmettre les données avec une faible latence, et une faible consommation d'énergie tel que Millimeter-Wave (mm-wave),

frequency band [15] ; Cognitive Radio Networks (CR) [16] ; Massive-Multiple Input Multiple Output (M-MIMO) [15] ; Coopérative Networks (CR) ; Relay Nodes (RNs) [17].

I.2.7. L'autoréparation

Les dispositifs de collecte de données placés dans des environnements extérieurs sont soumis à des conditions qui peuvent entraîner une dégradation au fil du temps et qui, dans certains cas, peuvent même conduire à un dysfonctionnement. Les appareils sont généralement distribués dans l'environnement avec un accès limité ou difficile, compliquant ainsi tout type de travaux de maintenance. Pour prolonger la durée de vie du réseau de nombreuses études se sont concentrées sur le diagnostic des pannes, elles sont présentées dans un document d'enquête qui classe les méthodes de diagnostic des pannes dans les WMSNs [18]. Un nouveau concept a été introduit celui de l'autoréparation ou le Self-Healing bien détaillé dans l'article [19]

I.2.8. Le bruit et interférence :

Le bruit est l'introduction d'un signal indésirable dans une transmission. La qualité de la transmission est généralement mesurée à l'aide du rapport signal sur bruit (SNR) au niveau du récepteur. Une interférence se produit lorsque plus d'un signal avec la même fréquence est présent dans le système. Cela rend difficile pour le récepteur d'isoler un signal de l'autre. C'est ce qui se passe lors d'une collision et peut conduire à la réception et à l'extraction incorrecte des données numériques [20]

I.2.9. L'énergie

Contrairement aux réseaux de capteur sans fil conventionnel, les WMSNs doivent disposer du multimédia avec un niveau de qualité de service (QoS) [21]. Cette exigence implique une compression de données avancées pour réduire la bande passante et l'utilisation de l'énergie par les nœuds de capteurs.

Dans le domaine du traitement d'images, la consommation d'énergie impliquée par des algorithmes populaires tels que JPEG, JPEG2000 ou SPIHT pourrait être encore plus importante que pour le cas de l'image non compressée, l'énergie est le facteur le plus critique dans les WMSNs, en raison des contraintes induites conduisant à une limitation des ressources en termes de mémoire ou de vitesse du processeur. Cependant on remarque des efforts de recherche pour adapter les algorithmes de compression d'images aux contraintes particulières des réseaux de capteurs sans fil, différentes techniques économes en énergie ont été proposées [22].

I.3. Les technologies émergentes pour les WMSNs

Les WMSNs ont contribué à l'émergence de nombreuses technologies .Parmi les technologies faisant une recherche active ces dernières années on peut citer ; les réseaux de nanocapteurs[23], les réseaux intelligents[24], l'internet des objets[4], les systèmes cybers-physique[25] et l'internet des véhicules[26] avec ses différentes variantes : les communications véhicule-2-véhicule (V2V), véhicule-2-infrastructure (V2I), véhicule-2-réseau (V2N), Du véhicule au cloud (V2C) et véhicule-2-piéton (V2P). La fiabilité, la disponibilité, la vitesse et la faible latence de la 5G ont le potentiel de permettre un environnement Vehicle-to-Everything (V2X).

La Figure I.1 illustre quelques nouvelles technologies émergentes basées sur le concept des WMSNs.

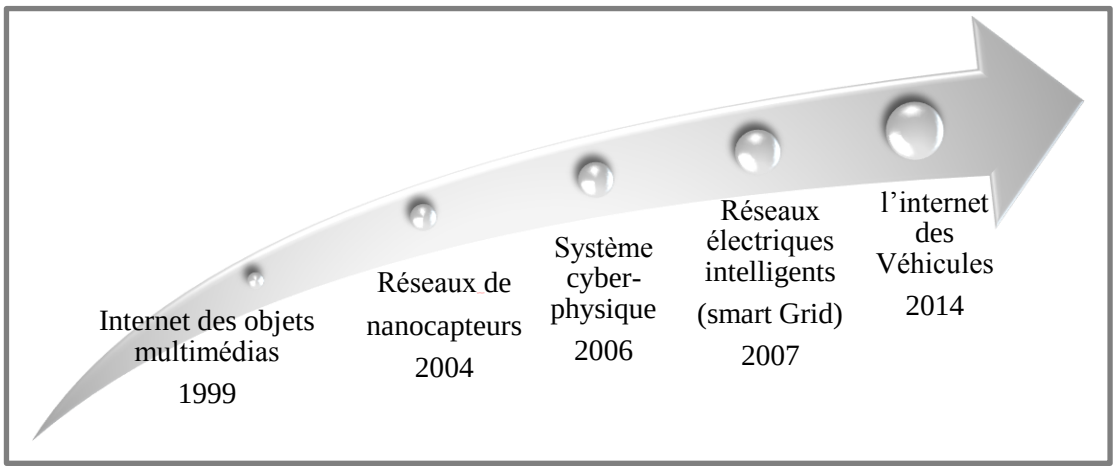


Figure I. 1 Les technologies émergentes issues du concept des WMSNs

La croissance du marché de l'imagerie électronique est propulsée par le développement des nouvelles technologies qui offrent la possibilité d'intégration d'un très grand nombre de transistors MOS dans une seule puce, la technologie est appelée very-large scale integration (VLSI) en anglais, réduisant considérablement le coût, la consommation d'énergie et la taille de la caméra.

La disponibilité croissante des caméras CMOS, SCMOS ou CCD et les processeurs spécialisés de traitement du signal numérique tel que MCU, DSP, FPGA, ASIC/SoC, MPSoC, MPPSoC ainsi que l'augmentation de la recherche et développement (R&D), tant au niveau universitaire qu'au niveau de l'industrie ont permis de développer des nœuds multimédias plus performants[27].

Parmi les technologies innovantes on peut citer et le développement récent des techniques de l'intelligence artificielle (IA), de l'apprentissage automatique (ML), les réseaux de neurones profonds Deep learning (DL), qui sont développées pour diverses applications dans les WMSNs. Ces techniques sont

abordées avec leurs architectures respectives appliquées en particulier, pour l'amélioration de la durée de vie, la réduction de la complexité de calcul, l'efficacité énergétique et pour améliorer la précision du système de surveillance et sa stabilité (improve tracking accuracy and stability) dans[28],[29],[30] .

I.4. Les applications des WMSNs

Les progrès réalisés dans les technologies des capteurs, des appareils mobiles et dans les techniques de traitement de l'information ont créé de nouvelles opportunités d'applications pour les WMSNs, de nos jours le réseau WMSN permet de récupérer, de traiter et de stocker du flux multimédia (audio, vidéo, image) en temps réel ce qui a contribué à son déploiement dans divers nouveaux secteurs. La Figure I.2 illustre l'évolution du marché mondial des applications des WMSNs.

I.4.1. Surveillance du trafic

Les WMSNs embarquent des caméras qui sont déployées pour accroître la capacité d'opération des organismes chargés de l'application de la loi par exemple, de surveiller des zones, des événements publics, des propriétés privées ou des frontières. Les capteurs multimédias peuvent également surveiller le flux des véhicules sur les autoroutes et y extraire des informations globales telles que la vitesse moyenne et le nombre de voitures, des vols, des accidents de voiture ou des violations du trafic et produire des flots d'audio-vidéo pour de futures enquêtes et organisation du trafic urbain.

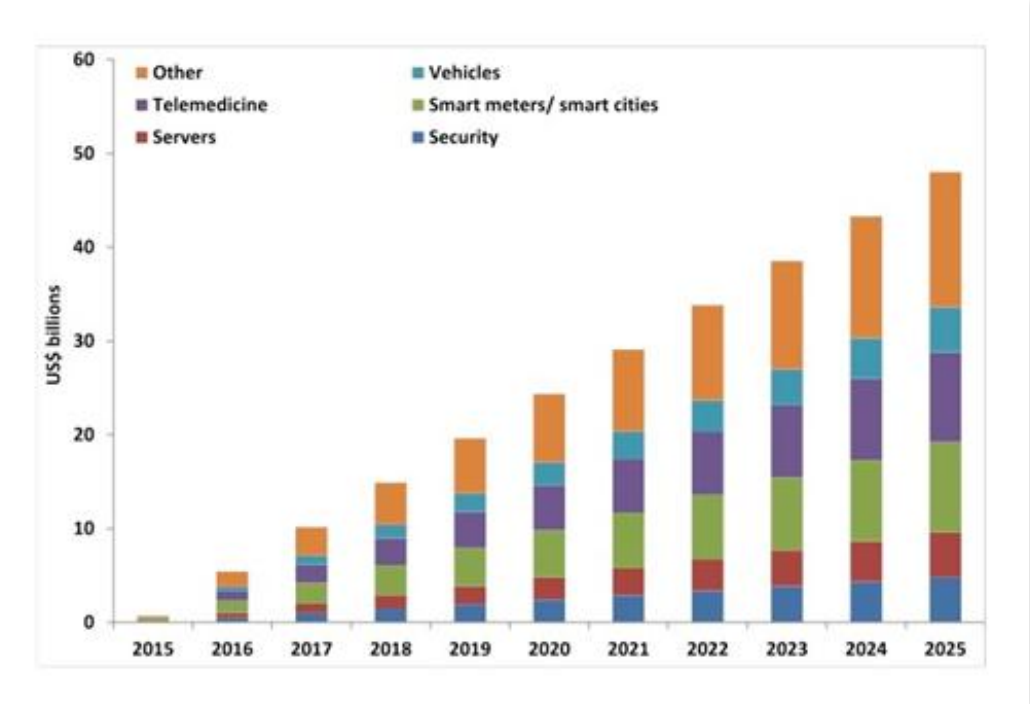


Figure I. 2 Evolution du marché des WMSNs**[31]**

I.4.2. L'Internet des véhicules (IoV)

L'IoV permet aux véhicules d'échanger des informations avec d'autres véhicules ou infrastructures de transport, respectivement appelées communications de véhicule à véhicule (V2V) et communications de véhicule à infrastructure (V2I). Compte tenu de son importance dans les futures villes intelligentes, offrant de nombreuses applications, telles que la conduite autonome, la planification d'itinéraire, la détection mobile, les systèmes d'avertissement d'accident, l'analyse du trafic, les systèmes de transport intelligents, IoV a capté l'intérêt des communautés de recherche. L'interaction entre les entités connectées dans le domaine de l'internet des objets (IoT) implique une infrastructure de trafic intelligente, et une sécurité adaptée[32].

I.4.3. Réseaux de véhicules aériens sans pilote (UAVs)

La conception de réseaux de véhicules aériens optiques sans pilote (UAVONET) pour les drones connaît un énorme intérêt dû à leur capacité de créer des applications importantes dans les transports, la télésurveillance et la surveillance militaire. En effet, les UAV peuvent être utilisés pour assurer la sécurité intérieure et d'autres applications de surveillance civile, telles que la gestion des catastrophes naturelles et dans l'agriculture pour la surveillance des récoltes et le traitement par les pesticides.[33].

I.4.4. Télémédecine

L'image médicale est considérée comme un noyau dur dans le domaine de la télémédecine. Il est utilisé pour le diagnostic dans les hôpitaux. Ainsi, toute modification, même légère, influera sur le diagnostic. Une grande partie des images médicales sont capturées dans les hôpitaux à des fins de diagnostic et de recherche et sont soit transmises par un canal vers une destination particulière, soit stockées puis remises au spécialiste. Transférer des données médicales telles que des résultats radiologiques d'un centre de base de données médicales à un autre centre ou à un radiologue distant soit en temps réel soit en temps non réel. Ces bases de données doivent être protégées contre les attaques intentionnelles et non intentionnelles [34].

Les WMSNs peuvent également être utilisés à des fins de surveillance de l'environnement (CO2 monitoring system) et structurelles, des capteurs vidéo et d'images peuvent être utilisés pour surveiller la santé structurelle des ponts et d'autres structures civiles. Dans les applications industrielles, WMSNs peuvent donner des inspections visuelles pour le contrôle des processus industriels (Machine Heath monitoring) [35].

I.5. Les topologies des WMSNs

La topologie est une organisation physique et logique d'un réseau. La topologie réseau physique définit le positionnement de divers nœuds d'un réseau. La topologie logique, représente la façon dont les données transitent dans les lignes de communication (comment est distribué le droit à la parole).

Ces topologies utilisent des protocoles qui contrôlent et définissent la façon de communiquer avec des règles minimales d'émission et de réception des données dont la taille des paquets, la vitesse de transmission, les types de correction d'erreur, les techniques de négociation et de synchronisation, le mappage des adresses, les processus d'accusé de réception, le contrôle de flux, les contrôles de séquence de paquets, le routage…etc.

I.5.1. La conception des protocoles de routage :

Nous distinguons deux grandes classes de protocoles ad hoc non hiérarchiques : les protocoles topologiques et les protocoles géographiques. La première classe regroupe les protocoles ad hoc basés sur la découverte de la topologie du réseau où les nœuds n'ont aucune connaissance de leur position géographique ni de celle des autres nœuds. Par échanges de messages entre voisins, le protocole de routage arrive à découvrir et à connaitre le les chemins entre les nœuds, ensuite à maintenir la topologie du réseau pour router les paquets, cette identification se fait soit de manière proactive soit de manière réactive. Les protocoles pro-actifs établissent les routes à l'avance en se basant sur l'échange périodique des tables de routage, alors que les protocoles réactifs cherchent les routes à la demande des nœuds.

Dans la deuxième catégorie de protocoles, on trouve les protocoles géographiques ou le georouting pour lesquels chaque nœud doit connaître sa position géographique qui peut être obtenue à l'aide d'un système de géolocalisation tel que le Global Positioning System (GPS), la destination d'un message est spécifiée sous forme de coordonnées. Il peut s'agir des coordonnées d'un nœud (destinataire), où d'une zone entière.

On peut citer par exemple le protocole Minimum energy communication network (MECN) et le Geographic adaptive fidelity (GAF).

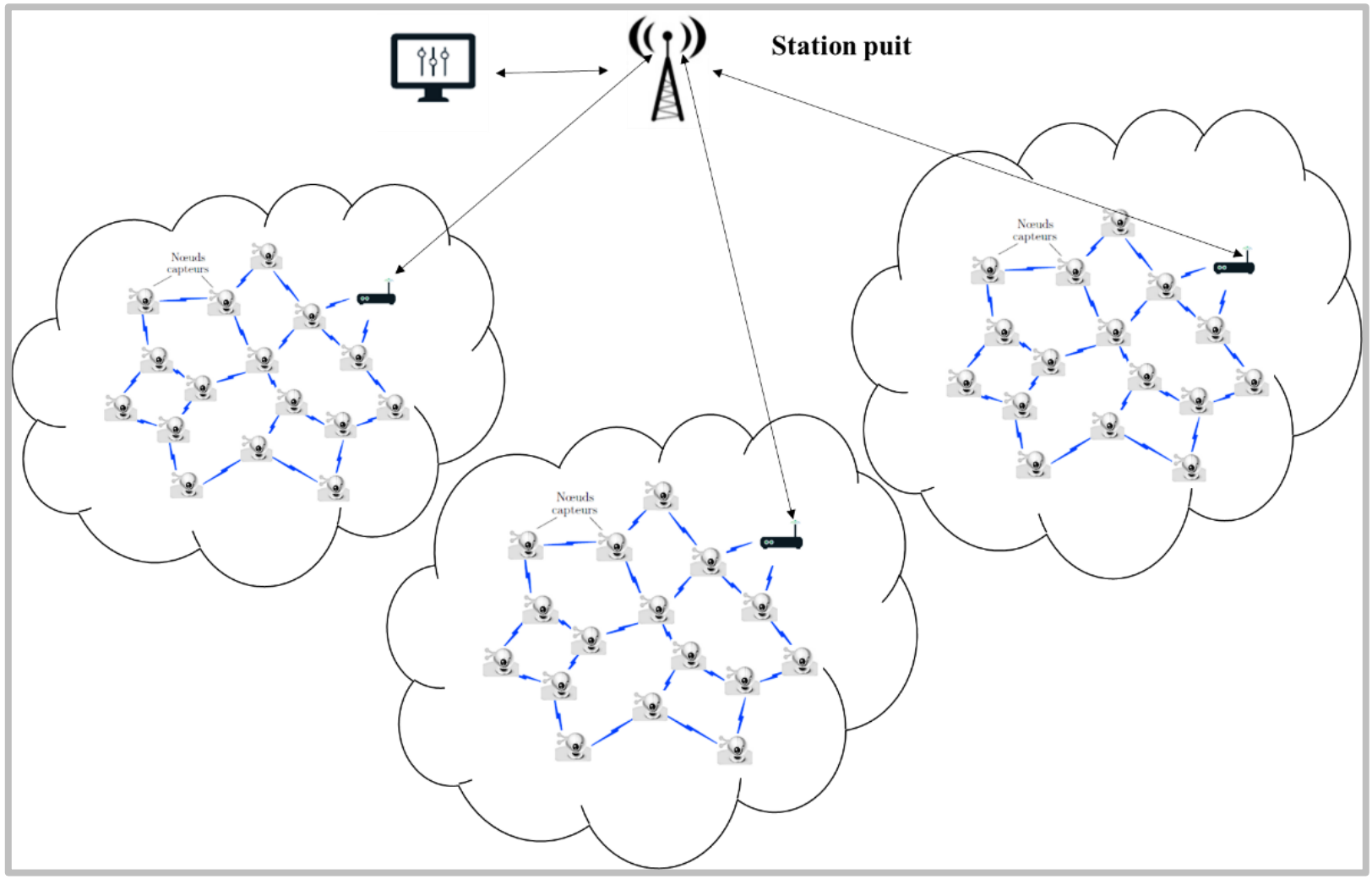


Figure I. 3 Architecture d'un modèle de WMSN avec une topologie hiérarchique en étoile

I.5.1.1. Les fonctions principales d'un nœud dans une topologie hiérarchique

Le capteur nœuds multimédias est capable de récupérer ou collecter des flux vidéo, audio ainsi que des images fixes, de les traiter sous une forme adaptée à la transmission et les envoyer aux nœuds récepteurs ayant le niveau hiérarchique le plus proche selon l'architecture du réseau.

- Le nœud maitre (Cluster head) : pour chaque cluster un coordinateur chargé de collecter les données des nœuds et de les envoyer au récepteur (Station de base ou Sink node).
- Le nœud passerelle (Gateway) : c'est un nœud configuré pour servir de passerelle, chargé d'acheminer les données d'un cluster à un autre.
- Le nœud puit (Sink node) : un nœud récepteur ou une station de base (BS) : est un dispositif similaire aux capteurs nœuds normaux mais avec un stockage et une capacité de calcul plus puissante. L'une des tâches principales du nœud récepteur consiste à collecter les données de la tête des clusters et les envoyer au centre de control. La station de base est interconnectée à un lien de communication externe qui peut être de type : Internet, téléphonique, satellite, etc. Les informations recueillies par cette station de base sont transférées à destination d'un centre de traitement distant pour l'analyse.
- Le centre de contrôle (utilisateurs du réseau) : dans lequel les données peuvent être visualisées grâce à une interface interactive (monitoring) permettant aux utilisateurs d'observer, d'analyser, d'exploiter et de prendre des décisions sur les données de surveillance collectées du réseau de capteurs multimédia. [36]

I.5.1.2. Les topologies hiérarchiques d'un WMSN

Dans le cas le plus simple, les capteurs seront dans le voisinage direct du puits (un réseau de type étoile à un saut). Cependant, dans le cas d'un réseau à grande échelle, les capteurs ne sont pas tous dans le voisinage du puits et les messages seront acheminés du nœud source vers le puits en transitant par plusieurs nœuds, selon un mode de communication multi-sauts. Dans le réseau maillé, les données peuvent « sauter » d'un nœud à un autre. Tous les nœuds peuvent communiquer directement entre eux sans avoir à dépendre d'un puit de communication centrale. Il s'agit de la structure de communication réseau la plus fiable car il n'y a pas de point de défaillance unique. Mais cette structure est très complexe et demande beaucoup de consommation d'énergie.[37],[38].

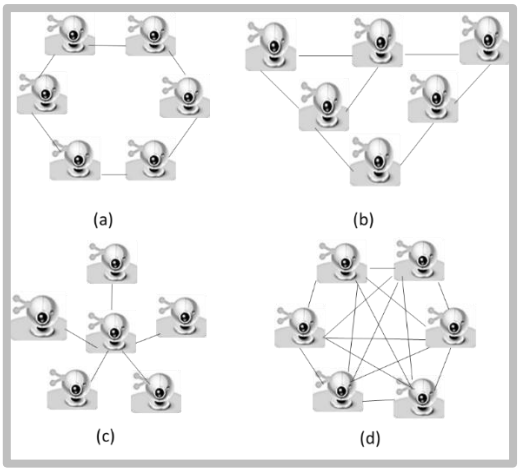


Figure I. 4 Topologies hiérarchiques d'un réseau de capteurs multimédias sans fil (a) Anneau (b) Arbre (c) étoile (d) Maillé

Par conséquent, divers schémas de regroupement (clustering) des nœuds sont proposés ou communément appelés topologies avec des fonctions attribuées à chaque nœud pour gérer le trafic principal dans la collecte des données des capteurs. Nous citons trois types de topologies (maillée, hiérarchique (en arbre), étoile) qui sont illustrées dans la Figue I.4.

Les stratégies de communication entre les capteurs dépendent de plusieurs paramètres tels que les applications et les objectifs du réseau à mettre en place. Cette communication peut être appréhendée de plusieurs façons pour un meilleur aiguillage des informations, différents algorithmes de contrôle de topologie existant dans la littérature sont présentés dans l'article [39].La Figure I.3 décrit l'architecture du réseau de capteurs sans fil multimédia avec une topologie hiérarchique en étoile.

I.5.2. L'architecture matérielle du WMSN

Le WMSN peut être classé en fonction de sa composition (homogène ou hétérogène), de son architecture (mono-niveau ou multi-niveaux). Un WMSN homogène se compose de capteurs ayant la même capacité, la même énergie et le même stockage, mais un WMSN hétérogène se compose de différents types de nœuds ayant différentes capacités de détection, d'énergie, de stockage et de traitement. Les nœuds ayant une meilleure configuration peuvent agir en tant que coordinateur responsable de la plupart des tâches de communication et de traitement afin d'améliorer les performances du réseau[39].

L'architecture réseau de capteurs sans fil multimédia peut être monocouche ou multicouche. Chaque nœud peut exécuter plusieurs fonctions, à partir de la détection d'images, du traitement, du codage, etc. Cependant, ils peuvent communiquer avec le puits (Sink node) de manière à saut unique ou à sauts multiples.

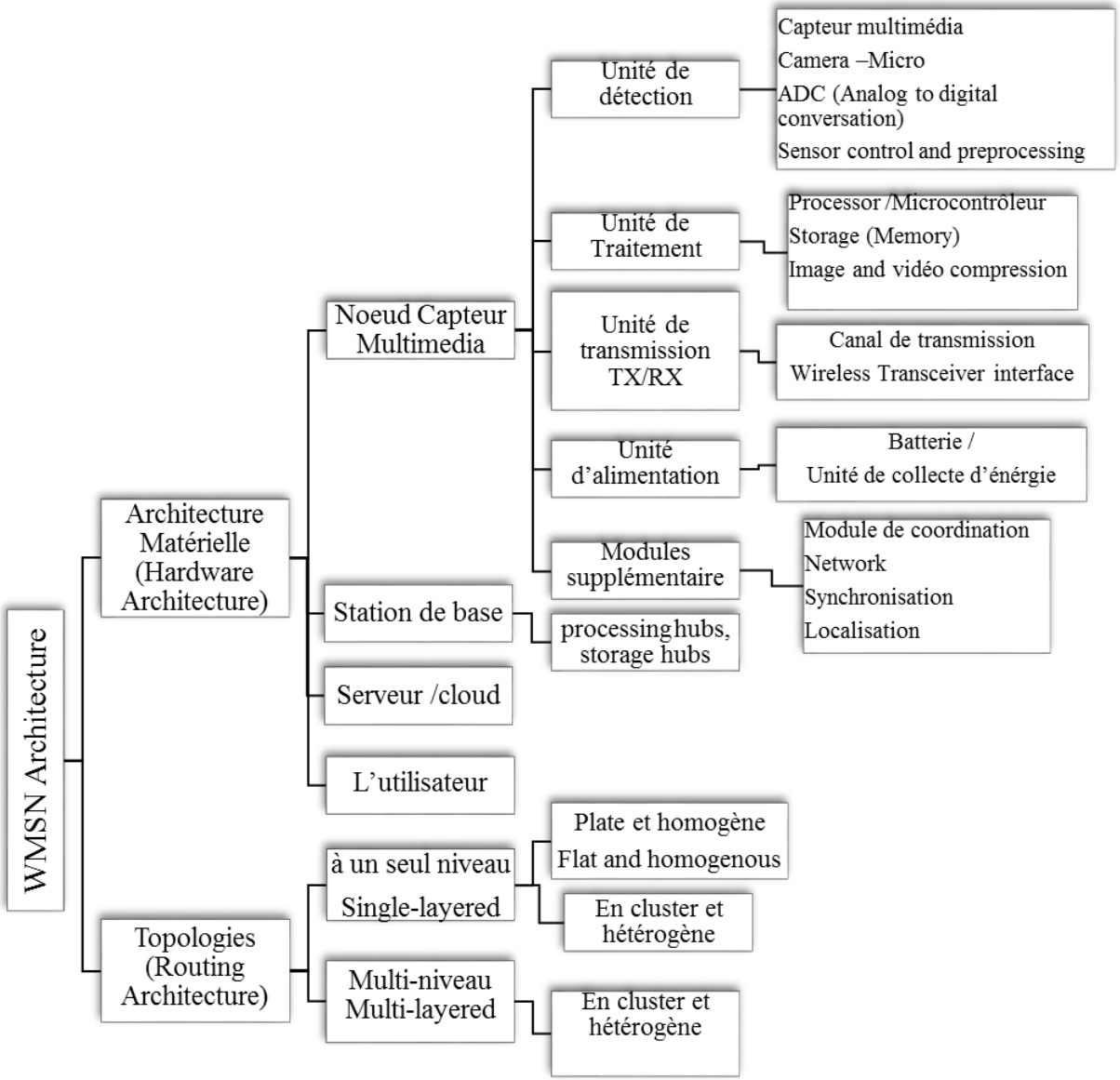


Figure I. 5 Architecture des WMSNs

L'architecture à couche unique peut également être une architecture en cluster, où différents types de capteurs sont regroupés en fonction de leur principe de fonctionnement et les chefs de cluster sont uniquement responsables de la transmission des données au puits. Mais si les données générées par le capteur multimédia sont volumineuses, une architecture plate peut ne pas convenir. Ainsi, le concept multicouche répond à cette problématique. L'architecture multicouche traite essentiellement des capteurs hétérogènes. [39] Figure I.5 illustre les différentes topologies pour les WMSNs.

I.5.2.1. Architecture plate à un seul niveau (Single-tier flat architecture)

Le premier modèle est l'architecture plate à un seul niveau où le réseau est déployé avec des nœuds de capteurs homogènes de mêmes capacités et fonctionnalités. Dans ce modèle, tous les nœuds peuvent exécuter n'importe quelle fonction, de la capture d'images au traitement multimédia en passant par le relais de données vers le récepteur en plusieurs sauts. L'architecture plate à un seul niveau est facile à gérer. De plus, le traitement multimédia est réparti entre les nœuds, ce qui prolonge la durée de vie du réseau [40].

I.5.2.2. Architecture en cluster à un seul niveau

Le deuxième modèle est l'architecture en cluster à un seul niveau est déployé avec des capteurs hétérogènes tel que les capteurs de caméra, audio et des capteurs scalaires. Les données au sein de chaque cluster sont acheminées vers une tête de cluster qui dispose de plus de ressources elle est aussi capable d'effectuer un traitement intensif des données. La tête de cluster est connectée sans fil au nœud passerelle, soit directement, soit via d'autres têtes de cluster de manière multi-sauts [40]

I.5.2.3. Architecture multi-niveau

Le troisième modèle est l'architecture multiniveaux avec des capteurs hétérogènes. Dans cette architecture, le premier niveau déployé avec des capteurs scalaires effectue des tâches simples, comme la détection de mouvement, le deuxième niveau de capteurs de caméra peut effectuer des tâches plus compliquées comme la détection d'objets ou la reconnaissance d'objets, et au troisième niveau, des capteurs de caméra plus puissants et haute résolution sont capables d'effectuer des tâches plus complexes, comme le suivi d'objets. Chaque niveau peut avoir un hub central pour effectuer davantage de traitement des données et communiquer avec le niveau supérieur. Le troisième niveau est connecté sans fil avec l'évier ou la passerelle. Cette architecture peut accomplir des tâches avec différents besoins avec un meilleur équilibre entre les coûts, la couverture, les fonctionnalités et les exigences de fiabilité. D'autre part, l'utilisation d'un seul type de nœud dans un réseau plat homogène n'est pas suffisamment évolutive pour englober toute la complexité et la plage dynamique des applications offertes sur les WMSNs [41].

I.6. Architecture d'un nœud multimédia

Le nœud multimédia (qu'on retrouve dans les publications scientifiques sous le terme anglais Mote) est un composant physique, petit, capable d'effectuer trois tâches parallèles : mesurer une quantité physique, traiter l'information et communiquer avec d'autres nœuds capteurs, leur nombre dans un réseau peut varier de quelques dizaines d'éléments à plusieurs milliers. Remplissant les trois fonctions, un nœud capteur a quatre composants principaux : l'unité de détection ou d'acquisition, l'unité de traitement ou de calcul, l'unité de communication sans fil et l'unité d'alimentation, tel qu'indiqué sur la Figure. I.6.

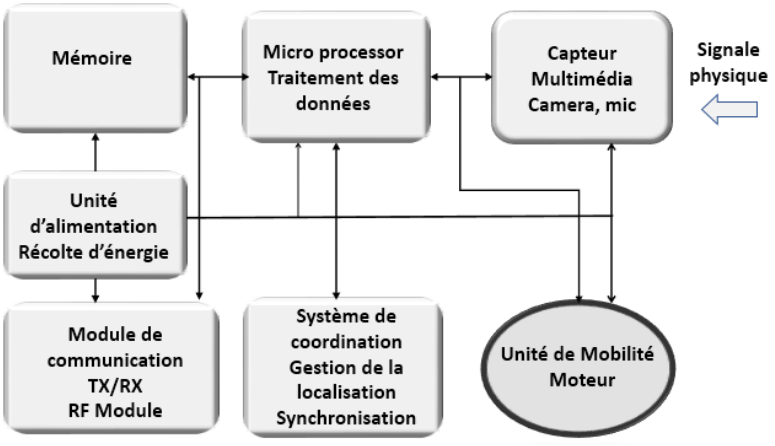


Figure I. 6 Modules conceptuels d'un nœud multimédia mobile

I.6.1. Unité de détection

C'est l'interface réelle avec le monde physique. Elle est constituée généralement de deux sous-unités : un capteur et un convertisseur analogique-numérique (ADC). Le terme « capteur » et « transducteur » ont souvent été utilisés comme synonymes. La norme MC6.1 de l'American National Standards Institute (ANSI) définit un transducteur comme « un dispositif qui fournit une sortie utilisable en réponse à une mesure spécifique » (Instrument Society of America, 1975). Une sortie est définie comme une « quantité électrique », et une mesure est définie comme « une quantité physique », une propriété ou une condition qui est mesurée. En 1975, la norme ANSI indiquait que « transducteur » était préféré à « capteur ». Cependant, la littérature scientifique n'a généralement pas adopté la dénomination de l'ANSI, et donc actuellement « capteur » est le terme le plus couramment utilisé.

Les capteurs produisent presque généralement une sortie électrique, tels que le courant ou la tension, les signaux reçus des mesures du phénomène détecté, peuvent être physiques, chimiques ou biologiques, des signaux analogiques qui sont convertis en un signal électrique puis en un signal numérique par le

convertisseur ADC et sont introduits ensuite à l'unité de traitement .Les capteurs sont classés en différents types en fonction des applications, du signal d'entrée et du mécanisme de conversion, du matériau utilisé et enfin des caractéristiques statiques et dynamiques ; statiques telles que la précision, distorsion et la sensibilité et dynamiques telles que l'hystérésis, le bruit et la portée de fonctionnement .[42].

- **Dispositifs de capture d'images :**

Un capteur d'image est un appareil électronique qui convertit une image optique en un signal électronique. La méthode de conversion varie selon le type de capteur d'image. Aujourd'hui, il existe deux technologies différentes pour capturer des images numériquement, presque tous les capteurs entrent dans l'une de ces deux catégories : Capteurs de Dispositif à Transfert de Charge (CCD) ou des Semi-conducteurs à Oxyde de Métal Complémentaire (CMOS). Un CCD « analogique » effectue la conversion photon-électron Un capteur d'image CMOS (CIS) « numérique » effectue la conversion photon-tension Les capteurs d'image sont utilisés dans les appareils photo numériques et les dispositifs d'imagerie pour convertir la lumière reçue d'un appareil photo ou d'un dispositif d'imagerie en une image numérique, la Figure I.7 définit les caractéristiques de chaque type de capteur [43].

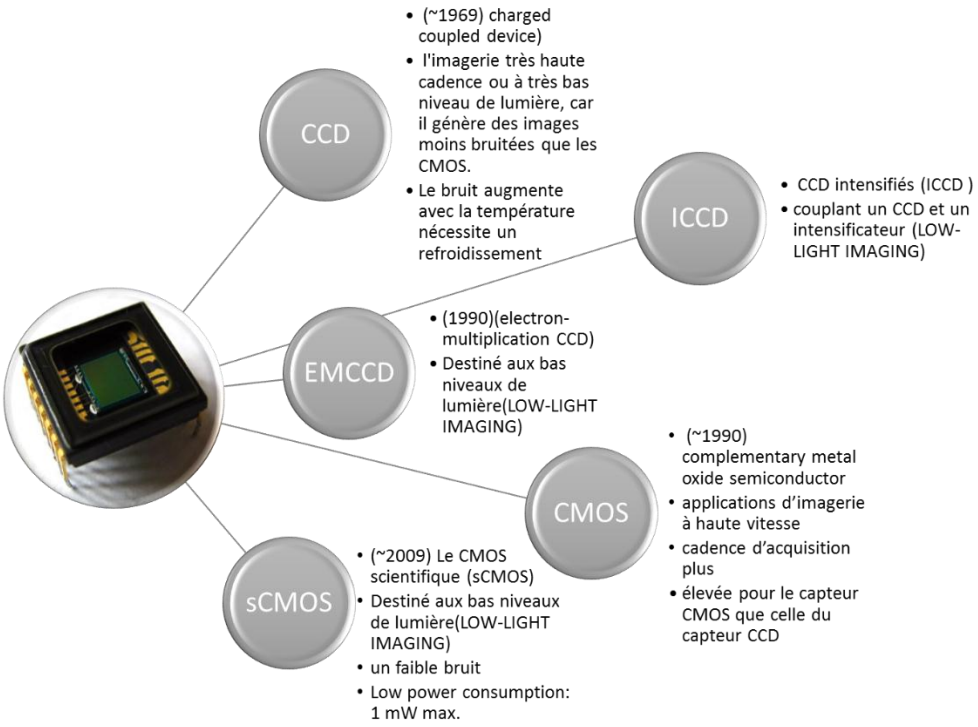


Figure I. 7 Evolution de la technologie des capteurs caméra

Les derniers développements en matière de technologie d'imagerie, les capteurs scientifiques CMOS (sCMOS) offrent simultanément une sensibilité élevée, des vitesses de lecture rapides et un faible bruit. Ces capteurs d'image ont des pixels composés d'une photodiode et d'un amplificateur qui convertit la charge en tension. La tension de chaque pixel est émise en allumant le commutateur un par un, et les données de chaque ligne horizontale sont lues par l'amplificateur de colonne sur puce et A/D en parallèle et simultanément. Il en résulte une vitesse de lecture très rapide tout en maintenant le bruit de lecture très faible. Les innovations repoussent toujours plus loin les limites de flexibilité ou de vitesse en imagerie numérique rapide se poursuivent à un rythme soutenu. Même le récent développement de la photographie à détection compressée (CUP), dont la cadence d'acquisition extrême est de 100 000 Mfps.[44]

- **Dispositifs de capture Audio :**

Il est possible de réaliser un WMSN dont les nœuds capteurs sont configurés pour échantillonner des signaux audios qui sont détectés à partir de leur environnement à l'aide de microphones [45] Ces grands volumes de signaux audio acquis pourraient ensuite être retransmis par les nœuds, une implémentation graphique du système de surveillance peut également fournir à l'utilisateur un retour visuel sur l'activité acoustique actuelle

I.6.2. Unité de traitement (Processing unit)

Elle est généralement composée d'un processeur couplé à une petite unité de stockage. Elle est chargée de recueillir et de traiter les signaux capturés avant de les transmettre aux autres nœuds du réseau, appelé aussi « Un contrôleur » son rôle est de traiter toutes les données pertinentes en exécutant un code. Chaque nœud du réseau est équipé d'un microcontrôleur à faible consommation. Sa fréquence de traitement peut atteindre les 104 MHz (pour les nœuds capteurs multimédia).

Le contrôleur est le cerveau du nœud, il exécute plusieurs tâches de traitement : il gère les données, le routage, le contrôle de l'alimentation, etc. Il gère également la détection et la transmission. L'électronique de cet appareil est assez divers et dépend principalement de l'application. Cela va du microcontrôleur(Un processeur et une mémoire intégrées sur la même puce avec un système d'entrée/sortie).,à la carte Field programmable gate arrays (FPGA), système sur puce (system on chip (SoC)), Complex programmable logic devices (CPLD), etc. [27]

Plus récent le développement de plates-formes matérielles comme l'unité de traitement graphique (GPU). Certaines caméras comportent également des algorithmes intégrés pour fournir déjà des données visuelles encodées et compressées.

Les logiciels des WSMNs sont des plates-formes et des solutions vitales pour les applications telle collecte de données ou surveillance à distance. Les solutions logicielles sont conçues pour répondre aux défis d'interopérabilité qui surviennent en raison de divers appareils hétérogènes, et de gérer un grand volume de données, leur sécurité et leur confidentialité. Des facteurs tels que l'augmentation du nombre de dispositifs et le besoin croissant de surveillance à distance ont conduit à l'adoption croissante de logiciels solutions.

- **Logiciels (System software architecture) :**

Le système d'exploitation dans les WSN est ainsi chargé de faciliter la communication entre les programmeurs et le matériel et de gérer les ressources du système et fournir des interfaces de haut niveau. Ces responsabilités aussi impliquent la gestion de la consommation d'énergie et de toutes les autres ressources. Ceux-ci nécessitent un système d'exploitation qui est généralement moins complexe.

- **TinyOS**

Il s'agit d'un système d'exploitation basé sur les événements, spécialement conçu pour les réseaux de capteurs et systèmes embarqués qui sont utilisés avec les motes Mica et Telos. Il nécessite un minimum de matériel, conçu pour prendre en charge la concurrence requise des réseaux de capteurs. TinyOS est un (OS) open source, développé à l'université de Californie, Berkeley.

- **Contiki** :

Il s'agit d'un système d'exploitation léger pour réseau de capteurs sans fil qui fournit un environnement d'exécution riche pour les petits appareils. Il peut dynamiquement charger et décharger des programmes et services individuels. Bien que le noyau soit piloté par les événements, le système prend en charge le multithreading préemptif qui peut être appliqué processus par processus. Ceci est implémenté en tant que bibliothèque liée uniquement aux programmes qui nécessitent explicitement le multithreading.

Contiki est implémenté en C et a été porté sur plusieurs architectures de microcontrôleurs. Les autres systèmes d'exploitation couramment utilisés pour les WSN incluent SOS, RTOS gratuit, Mantis, LiteOS, modifié systèmes d'exploitation intégrés comme eCOS et uCOS. En plus des systèmes d'exploitation, il existe plusieurs middlewares développés pour WSN. Un middleware est un logiciel qui fournit des services aux applications logicielles au-delà de ceux disponibles à partir du système opérateur. Un middleware facilite la mise en œuvre par les développeurs de logiciels fonctionnalités de communication et

d'entrée/sortie sur les nœuds, afin que l'appareil puisse mieux fonctionner exécutant sa ou ses tâches spécifiques. Parmi les plus courants, citons Agilla et Sensorware.[46]

- **Mise en réseau définie par logiciel (Software-Defined Networking** (SDN))

Est une architecture émergente qui est dynamique, gérable, rentable et adaptable, ce qui la rend idéale pour la nature dynamique à large bande passante des applications d'aujourd'hui. Cette architecture découple les fonctions de contrôle de réseau et de renvoi permettant au contrôle de réseau de devenir directement programmable et l'infrastructure sous-jacente à extraire pour les applications et les services réseau. Le protocole Open Flow® est un élément fondamental pour la création de solutions SDN. Pour une compréhension approfondie de la mise en réseau et des cas d'utilisation basés sur le SDN.[47]

I.6.3. Unité d'émission-réception ou communication (Transceiver unit)

Puisque les nœuds de capteurs ont une mémoire limitée et sont généralement déployés dans des endroits difficiles d'accès, une radio est mise en œuvre pour la communication sans fil pour transférer les données à une station de base (p. ex., un ordinateur portable, un appareil portatif personnel ou un point d'accès à une infrastructure fixe). Cette unité permet de connecter le nœud au réseau sans fil, en envoyant et en recevant les trames de données mesurées, à travers des ondes radio ou optiques. Elle est associée à une technologie de transmission d'information telles que la radiofréquence, transmission optique sans fil [48].

Figure I. 8 Quelques exemples de modules RF : (a) XBee module ; (b) 433 MHz TX/RX modules ; (c) NRF24l01+transeiver ; (d) MRF 49 XA transceiver.**[49]**

Les nœuds captent et communiquent leurs données selon un protocole de communication afin d'atteindre le nœud central de traitement connu sous le nom de « Sink ». Elles prennent en charge le protocole de communication dépendant de la technologie sans fil utilisée, c'est à dire tout ce qui traite de la transmission de messages entre nœuds-capteurs directement à portée : le contrôle d'accès au médium, la mise en forme des trames, l'encodage et le décodage des signaux, etc [49].

- **Les unités de transmission de type radiofréquence**

Comprennent un module possédant une antenne émettrice/réceptrice comme le montre la Figure I. 8 qui permet de communiquer avec les nœuds qui sont proches des circuits de modulation et démodulation, filtrage et multiplexage ; ceci implique une augmentation de la complexité. Concevoir des unités de transmission de type radiofréquence avec une faible consommation d'énergie est un défi car pour qu'un nœud ait une portée de communication suffisamment grande, il est nécessaire d'utiliser un signal assez puissant.

- **Les communications de type optique** :

La lumière est une onde électromagnétique qui peut être utilisée comme support pour la transmission de signaux porteurs d'informations. Pour ce faire, en pratique, on fait varier la puissance optique émise par une source lumineuse au rythme de l'information à transmettre. Les sources optiques convertissent les informations à transmettre en un signal optique par la génération de trains d'impulsions fortement cadencés et qui doivent avoir : Une longueur d'onde précise, une ouverture numérique, un rayonnement élevé sur une petite surface, une longue durée de vie, une grande fiabilité et une haute fréquence modulation de bande.

La source peut être une diode électroluminescente (LED) ou une LED laser (LD). Les diodes LED sont un dispositif composé de deux semi-conducteurs p-n intégrés de manière monolithique. Lorsque la jonction p-n est polarisée, l'énergie est libérée sous forme de lumière (photons). La technologie sans fil optique est robuste vis-à-vis des interférences électriques. Néanmoins, ne pouvant pas établir de liaisons à traverser des obstacles, elles présentent l'inconvénient d'exiger une ligne de vue permanente entre les entités communicantes. Cependant ces applications sont diverses telles que la mise en œuvre des applications de ville intelligente visant la sécurité des aéroports ainsi que la sécurité du transport ferroviaire, des réseaux d'aide à la navigation et de surveillance des événements suspects pour assurer la sécurité à l'intérieur des aéroports.[50]

I.6.4. Unité d'alimentation (Autonomous power supplies)

Elle est l'unité la plus importante puisqu'elle définit la validité (durée de vie) du capteur dans son milieu généralement inaccessible où il est généralement difficile de le réalimenter souvent. Elle comporte une batterie ou une pile et peut être dotée d'une unité d'énergie renouvelable. [51].

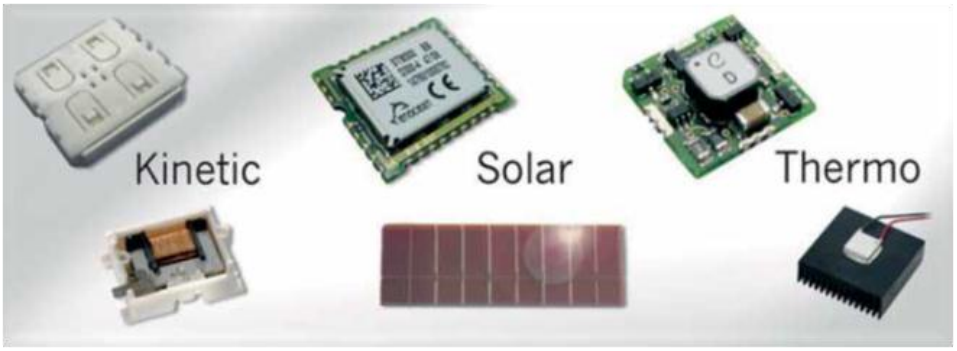


Figure I. 9 Nœuds de capteurs configurés avec des dispositifs de récupération d'énergie ambiante**[51]**

- **La récupération d'énergie ambiante**

La récupération d'énergie ambiante peut être réalisée par génération d'énergie de cellule optique conventionnelle, mais aussi à travers des cristaux piézoélectriques miniatures, micro-oscillateurs, production d'énergie thermoélectrique, ou par réception d'ondes électromagnétiques [48, 49].

Certaines entreprises ont commencé à commercialiser les applications de réseaux de capteurs utilisant des dispositifs d'acquisition d'énergie, par exemple, la société allemande EnOcean a fourni plusieurs dispositifs de récupération d'énergie dont les dispositifs de récupération d'énergie lumineuse, de vibration et dispositifs basés sur la température pour applications d'éclairage de bâtiments intelligents, la surveillance de l'air. La société « UK's Perpetuum» fournit une série de produits qui convertit la mécanique vibration en énergie électrique utilisée pour l'industrie indépendante en énergie, [52]

La récolte de chaleur cryogénique (cryo-heat harvesting) nouvellement annoncée et la récolte thermo acoustique [53] en cours, ainsi que les bons vieux pyroélectriques et la conversion de l'énergie thermique des océans. Cependant, la thermoélectrique [49] a un potentiel évident s'il est recentré. Les nombreuses formes émergentes de récupération de chaleur pour la production d'électricité, cette technologie est intéressante par exemple pour les sociétés pétrolières et gazières qui en ont besoin pour se diversifier. Il intéressera également ceux qui ont des problèmes non résolus de production d'électricité pour les nœuds de l'Internet des objets, les implants, les appareils portables, les micro-réseaux, l'armée, l'aérospatiale, les emplacements éloignés et d'autres applications où les batteries ne peuvent pas être chargées ou changées et

où le photovoltaïque et d'autres formes de récupération d'énergie sont peu pratiques. Une revue bibliographique des technologies de récolte d'énergie en considérant les vingt années d'une ère allant de l'an 2000 à 2020 et décrivant également les technologies de la prochaine génération et l'avenir de la technique de récolte d'énergie est présentée dans [54], [49]

I.6.5. Modules additionnels

Les capteurs sans fil peuvent également être dotés par d'autres modules additionnels relativement moins pertinents et surtout très gourmands en énergie qui sont : un système de géolocalisation et un Mobilisateur (Un système de localisation pour identifier l'emplacement d'un capteur, Un mobilisateur pour déplacer le capteur). Le système de géolocalisation est utilisé pour l'identification de la position géographique (un récepteur GPS par exemple). Tandis que, le support mobile (Mobilisateur) permet la possibilité aux nœuds-capteurs de se déplacer à l'intérieur de la zone à observer. Enfin, s'il est nécessaire qu'un nœud soit maintenu en activité pendant une très longue période de temps, un Générateur de Puissance, tel que des cellules solaires, serait utile afin de tenir le nœud alimenté électriquement sans avoir à changer ses batteries.

I.7. Les types de nœuds sans fil pour les WMSNs

Il existe plusieurs dispositifs de nœud sans fil qui peuvent être utilisés comme nœud pour les WSMNs, Ceux qui sont plus performants en termes de puissance de calcul et de traitement, sont conçus pour traiter le multimédia de manière rapide et efficace. Ces appareils peuvent exécuter différents systèmes d'exploitation (par exemple, Linux, TinyOs et exécuter des applications Java et des micro frameworks .NET) et prennent en charge plusieurs radios avec des débits de données différents (par exemple IEEE 802.15.4, IEEE 802.11, et Bluetooth). Cependant, ces appareils consomment relativement plus d'énergie. Nous citons comme exemple Imote2, la plateforme Stargate et Cyclops.

I.7.1. Carte Stargate :

La carte Stargate est une carte de haute performance, une plate-forme de traitement conçue pour les applications de contrôle et mise en réseau des capteurs sans fil, elle est basée sur le processeur Xscale® d'Intel, compatible avec la famille de réseaux de capteurs sans fil MICAz/ MICA2 de Crossbow, fontionne avec la plate-forme TinyOS intégrée dans la carte. Données disponibles sur le Datasheet dans le site (Web : www. xbow.com) . Elle forme un appareil photo Complet lorsqu'elle est connecté à un capteur caméra (par exemple, une webcam) comme indiqué dans la figure ci-dessous.

Figure I. 10 Un nœud capteur vidéo avec la plateforme Stargate de Cross Bow avec une carte MICAz interfacée avec une Webcam[55].

I.7.2. Imote2 ou (L'Intel Mote 2)

L'Intel Mote 2 est une plate-forme conçue pour les réseaux sans fil et pour des applications nécessitant un CPU/DSP de haut niveau et une liaison sans fil performante et fiable. Les applications cibles incluent la surveillance visuelle, vibration industrielle, surveillance structurelle et acoustique. Caractéristiques disponible sur le Datasheet dans le site Web : [55].

I.7.3. Cyclops

C'est un capteur d'image de base, une combinaison de microcontrôleur, CPLD (dispositif logique programmable complexe) et (static random access memory) SRAM qui nous permet d'accéder aux données d'image à la demande.

Figure I. 11 Un nœud de capteur Cyclops avec une carte Mica z interfacée[56].

La caméra Cyclops a été développée par les laboratoires Agilent et le CENS (Center for Embedded Network Sensing) de l'UCLA. Elle permet la capture et le traitement d'images de faible résolution avec une relativement faible consommation d´énergie [56].Nous pouvons citer aussi d'autres fournisseurs de module capteur d'image, Tel que Panotypes, EyeRis, SeedEyes, Libelium et Citric.

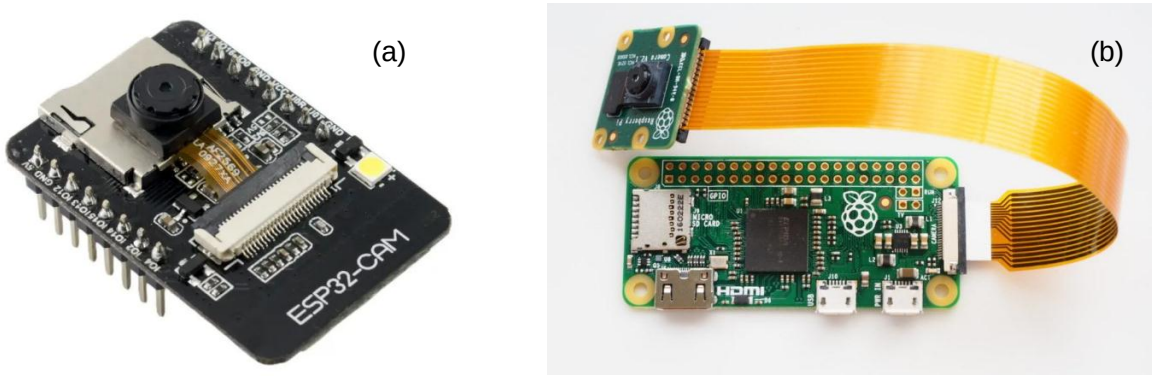


Figure I. 12 (a) le module ESP32-CAM, (b) Raspberry Pi Zéro avec une caméra V2-8 Mégapixel (RPI-CAM-V2)

I.7.4. Réseau de capteurs d'images sans fil à faible coût

- **La carte Arduino** implémentée pour le traitement des données détectées et leur transmission sans fil à l'aide du module XBee (IEEE 802.15.4) est un exemple de méthode alternative ; nous ne pouvons pas mettre en œuvre des techniques de traitement d'images supplémentaires via un microcontrôleur comme nous pouvons le faire avec le FPGA, mais cela produit un temps d'exécution impressionnant de 2,3 s [57].
- **Le ESP32 CAM** C'est un module qui peut être utiliser avec une multitude de projets, et avec Arduino. C'est un module complet avec un microcontrôleur intégré, en plus de la connectivité WiFi + Bluetooth, ce module dispose également d'une caméra vidéo intégrée et d'un emplacement microSD pour le stockage.
- **Raspberry Pi Zéro** Il existe deux nouvelles versions : la Raspberry **Pi Zero W** (RPi Zero W) qui est basé sur un **32- Bit** Broadcom BCM2835 monocœur ARM1176JZF-S SoC @ 1,0 GHz, 512 Mo de RAM, un IEEE 2,4 GHz Interface Wi-Fi 802.11b/g/n, un micro USB en déplacement port, un connecteur mini HDMI et une carte microSD fente et le modèle Raspberry **Pi Zero 2 W** (RPi Zero 2 W) qui est basé sur un RP3A0-AU, qui consiste en l'intégration d'un Cortex-A53 quadricœur Broadcom BCM2710A1 **64 bits** @ 1,0 GHz et 512 Mo de RAM, dans une seule puce. Ce dispose également d'une interface WiFi 2,4 GHz IEEE 802.11b/g/n, un port micro USB On-The-Go, un mini HDMI connecteur et un emplacement pour carte microSD (Web :www.raspberrypi.com).

I.8. Présentation de La couche Physique

Cette couche entre dans la catégorie des couches matérielles, elle comprend les moyens matériels de base d'un réseau de transmission (connexions physiques du réseau - transmission sans fil, cartes d'interface réseau, etc.). Les données de cette couche sont constituées d'un flux de bits définit par le taux de transmission qui est le nombre de bits par seconde.

I.8.1. Les fonctions de la couche physique

La couche physique fournit les services suivants :

* Processus de modulation est la conversion d'un signal d'une forme à une autre afin qu'il puisse être physiquement transmis sur un canal de communication

* Codage des canaux sans fil, qui permet aux données d'être envoyées par des dispositifs matériels optimisés pour les communications numériques

* Synchronisation des bits pour les communications

* Commutation de circuits et commande matérielle de multiplexage de signaux numériques. Détection de porteuse et détection de collision.

* Correction d'erreur directe/codage de canal tel qu'un code de correction d'erreur

* Chiffrement des données [36]

I.8.2. Les standards de la couche physique

Les principaux standards [58] utilisés pour la communication RF dans les WMSNs peuvent être classés selon différents protocoles standard : (IEEE 802.15.4 ZigBee, IEEE 802.15.1 Bluetooth, IEEE 802.11 Wi-Fi, 802.15.3a UWB). ZigBee [59] .Le protocole radio standard le plus couramment utilisé dans les réseaux de capteurs sans fil en raison de sa norme légère et de ses caractéristiques de faible coût et de faible consommation et la norme ZigBee qui prend en charge un débit de données jusqu'à 250 kbps à 2,4 GHz, plus de 65 000 nœuds, une efficacité de codage de 76,52 % et une portée de 10 à 100 mètres, elle est utilisée par la plupart des WMSNs tels que la famille MICA, Tmote sky et imote2.

	ZigBee [62]	Bluetooth [63]	UWB [64]	Wi-Fi [65]	Li-Fi [66]	Laser [5]	IRDA [67]
Norme de protocole IEEE	IEEE 802.15.4	IEEE 802.15.1	IEEE 802.15.3	IEEE 802.11	IEEE 802.11.bb IEEE 802.15.7	_	_
Débit de données (max) par canal PHY-	250Kbps/16channal	3Mbps (V2.0)	250Mps	>867 Mbps (2 antennas) 72.2Mbps (1 antenna)	3.5 Gbps	_	4 Mbits/s.
Portée	0-100m	1-100m	<10m	100 m	10m	_	_
Bande de fréquence	902-928 MHz shares the use of the 2.4 GHz with Wi-Fi and Bluetooth	2.4 GHz	3.1-10.6 GHz	2.4 GHz	100 THz	_	_
Nombre de nœuds	<65000	7	_	30	_	_	_
Énergie	< 10MW (Low) use smart energy	<10 MW (Medium)	_	>100 MW (High)	_	_	_
Modulation	DSSS (Direct Sequence Spread Spectrum) with BPSK/QPSK (Binary/Quadrature Phase shift keying)	FHSS (Frequency hopped spread spectrum) with GFSK (Gaussian Frequency Shift Keying)	On-off keying (OOK) MB-OFDM	QAM-OFDM MIMO	VPPM/OOK/CSK (Pulse position modulation) DCO-OFDM OFDM-based	WON-OCDMA Dual-pulse interval modulation (DPIM) SIMO RC-OFDM	ERPO -OFDM) ACO-OFDM
Applications in WMSNs	Machine industry	Healthcare data physiological data of a patient remotely	_	Smart home or home, automation vehicular, networks	Medical Underwater communication Aircraft	Maritime-terrestrial-air intelligent communication/sensor network	_

Cependant, la norme ZigBee n'est pas adaptée aux applications à haut débit telles que le streaming multimédia sur WMSN. D'autre part, d'autres normes telles que Bluetooth et Wi-Fi ont un débit de données et une efficacité plus élevées comme le montre le Tableau I.1 mais elles consomment plus d'énergie, le Wi-Fi a été utilisé avec le périphérique Stargate dans de nombreux projet[60].

Plusieurs autres solutions ont également été utilisées pour certains scénarios dans les WMSNs. Ces techniques sont la communication optique par exemple l'infrarouge qui n'a pas besoin d'antenne ; cependant, sa capacité de diffusion est limitée, acoustique et par induction magnétique ainsi que les communications utilisant des lasers, ces derniers ont besoin de moins d'énergie ; cependant, ils nécessitent d'être en visé Line of sight (LoS), et en plus ils sont sensibles aux conditions atmosphériques, les micro-ondes et la transmission par satellite sont des exemples de communication en visibilité directe[61]

I.8.3. Présentation de La couche Physique OFDM

I.8.3.1. La chaine de modulation OFDM avec ces différents blocs

Les systèmes de transmission numérique véhiculent de l'information entre une source et un destinataire en utilisant un support physique comme le câble, la fibre optique ou encore, la propagation sur un canal radioélectrique. Les signaux transportés peuvent être soit directement d'origine numérique, ou convertis sous une forme numérique. Le canal qui représente le support physique de transmission des signaux, regroupe également toutes les composantes qui perturbent la transmission à savoir le bruit ambiant en réception, les multi- trajets et les interférences multi-utilisateurs. La tâche du système de transmission est d'acheminer l'information de la source vers le destinataire avec le plus de fiabilité possible. La source émet un message numérique sous la forme d'une suite d'éléments binaires. Le codeur peut éventuellement supprimer des éléments binaires non significatifs (compression de données ou codage de source). Dans le cas d'une modulation numérique, l'information à transmettre se présente sous la forme d'une suite de bits qu'il est possible de grouper par paquets de longueur définie. Le synoptique de la Figure I.13 illustre les différents modules qui composent la chaîne de transmission OFDM.

Le module de mappage, qui mappe les symboles entrants sur des échantillons à valeurs complexes, le modulateur numérique (M-QAM) transforme les données binaires bi de durée Tb en symboles complexes $C_k$de durée $Ts = log2MTb$, où M, appelé ordre de modulation, présente le nombre d'états possibles dans le diagramme de constellation.

.

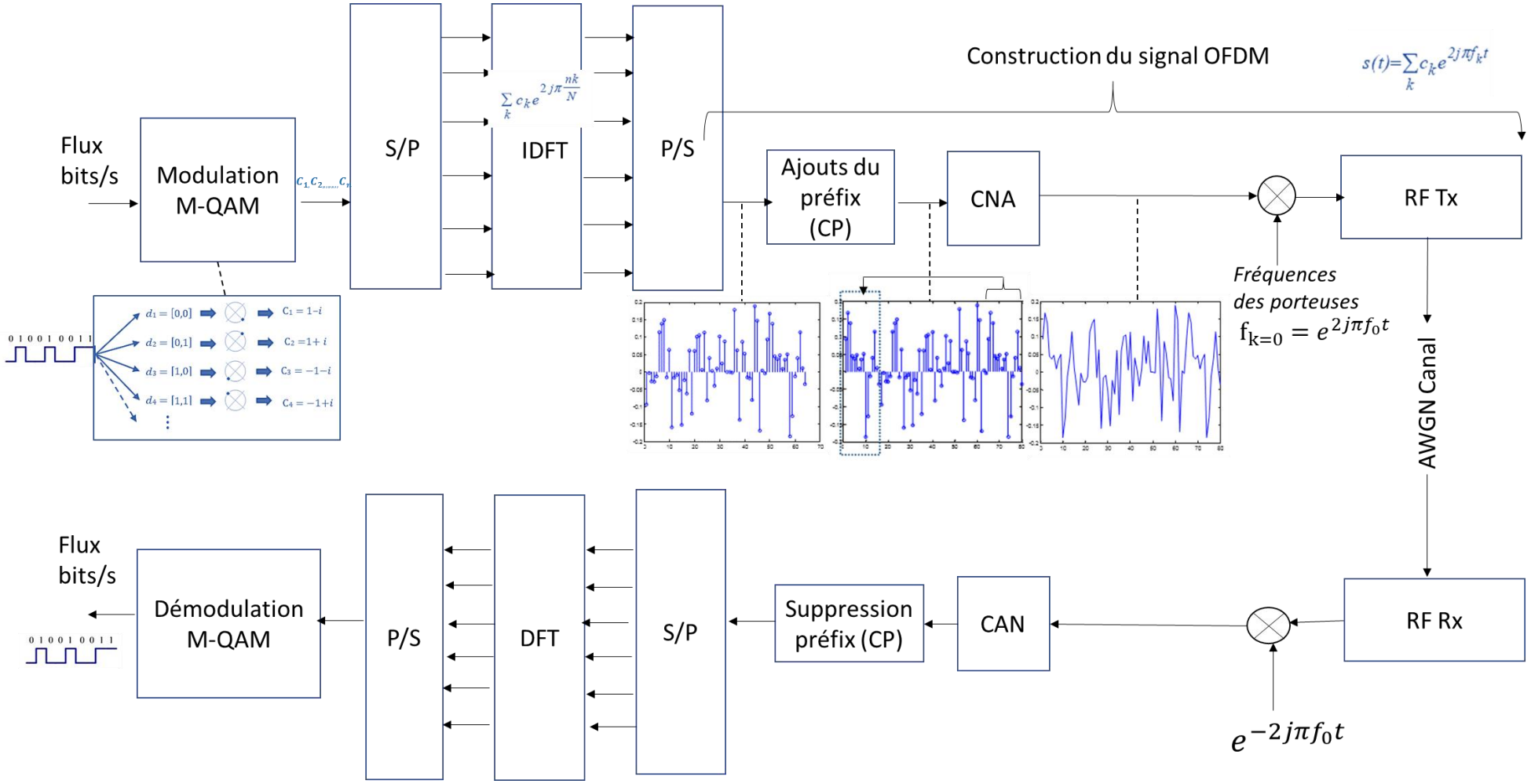


Figure I. 13 Schéma fonctionnel de l'émetteur et du récepteur dans un système OFDM[69]

Le convertisseur série parallèle divise les données à son entrée en des flux de données parallèles à un débits réduit ensuite, les échantillons sont introduits dans le module de la transformée de Fourier discrète inverse (IDFT) qui permet de générer le signal dans le domaine temporel constitué de Nsc échantillons.

Le préfixe cyclique (CP) de longueur Tg est ajouté dans le domaine temporel pour éliminer les interférences entre symboles (ISI) tout en gardant l'orthogonalité entre les sous-porteuses. Après l'IDFT, il y a un convertisseur parallèle-série et enfin le symbole OFDM est transmis à l'étage radiofréquence comportant la conversion numérique/analogique DAC (Digital-to-Analog Converter), qui convertit le signal de la forme numérique à la forme analogique et le transmet sous la fréquence de la porteuse [68].

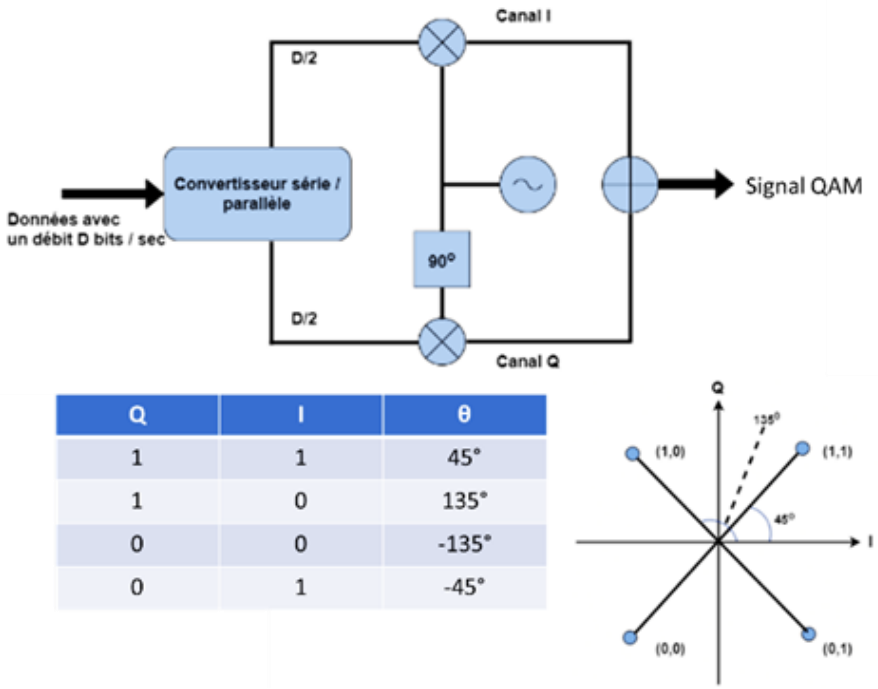
Le canal de transmission est modélisé dans notre système de communication, par un processus additif de bruit blanc gaussien (AWGN). C'est un bruit thermique provenant principalement de l'agitation des électrons au sein des équipements électroniques de réception. Il est dit blanc car l'ensemble de ses composantes fréquentielles sont d'amplitudes égales.

I.8.3.2. La modulation d'amplitude en quadrature

La QAM est une technique de modulation numérique qui utilise les données à transmettre pour faire varier à la fois l'amplitude et la phase d'une forme d'onde sinusoïdale, tout en gardant sa fréquence constante, deux porteuses dont les amplitudes sont modulées indépendamment avec la même fréquence et dont les phases sont décalées de 90° l'une par rapport à l'autre (un quart de cycle, d'où provient le terme quadrature). Ces porteuses sont appelées porteuses en phase (I) et porteuses en quadrature (Q).

La QAM est une extension naturelle de la modulation par déplacement de phase binaire (BPSK) et de la modulation par déplacement de phase en quadrature (QPSK), qui ne varient que la phase de la forme d'onde.

Le nombre de formes d'onde différentes (combinaisons uniques d'amplitude et de phase) utilisées en QAM dépend de la technologie utilisée et peut varier en fonction de la qualité du canal. Avec 16-QAM, par exemple, 16 formes d'ondes différentes sont disponibles. Il existe un équilibre entre le débit de données et le rapport signal / bruit requis. Lorsque l'ordre du signal QAM est augmenté, c'est-à-dire passant de 16QAM à 64QAM, etc., le débit de données augmente, cependant, l'inconvénient est qu'un meilleur rapport signal / bruit est nécessaire pour y parvenir.



Q	I	θ
1	1	45°
1	0	135°
0	0	-135°
0	1	-45°

Figure I. 14 Diagramme de constellation 4 QAM

Un signal de modulation d'amplitude en quadrature (M-QAM) peut être défini par l'équation suivante :

$$S_m(t) = A_m . g(t). \cos(2\pi f_c t + \theta_m) , \mathrm{m} = 1,2,3 \dots \dots , \mathrm{M} \qquad (\mathrm{I}.1)$$

Où $S_m(t)$ représente le signal passe-bande choisi parmi les M formes d'onde possibles, f_c symbolise la fréquence porteuse, g(t) est une impulsion de signal à valeur réelle dont la forme influence le spectre du signal émis, et les A_m, θ_mdésignent l'amplitude et l'angle de phase du m-symbole donné par :

$$\begin{cases} A_m = \sqrt{(A_m^I)^2 + (A_m^Q)^2} \\ \theta_m = tan^{-1}\left(\dfrac{A_m^Q}{A_m^I}\right) \end{cases} \qquad (\mathrm{I}.2)$$

Dans ces équations, A_m^I and $A_m^Q \in \{\pm 1\mathrm{d}, \pm 3\mathrm{d}\dots., \pm(\mathrm{M}-1)\}$ d indiquent les amplitudes I et Q correspondant aux M symboles possibles dans l'espace à deux dimensions Figure I.14.

Le signal passe-bande transmis s(t), qui contient tous les symboles représentés par les M formes d'onde de signalisation possibles pour la QAM, peut être exprimé sous la forme :

$$s(t) = Re\left\{\sum_n I_n g(t - nT_s) e^{j2\pi f_c t}\right\} \qquad (\mathrm{I}.3)$$

Où Ts fait référence à la durée du symbole, (Rs = 1 /Ts) indique le taux de transmission en symboles/seconde) et {In} représente la séquence de symboles porteurs d'informations discrètes et à valeur complexe pour la QAM.

Le diagramme de constellation est une représentation graphique montrant tous les symboles de modulations possibles (ou états de signal) sous la forme d'un ensemble de points de constellation. La position de chaque point du diagramme indique l'amplitude et la phase du symbole correspondant [70]

Comme mentionné, les systèmes QAM sont largement utilisés dans les systèmes de communication modernes où un débit maximal est requis dans des conditions de bande passante limitée, ils ont été largement adoptés pour les applications radio numériques micro-ondes et les modems à bande vocale et utilisés aussi pour la diffusion vidéo numérique par câble (DVB-C), en plus des protocoles sans fil IEEE 802.11.

Etant ainsi considérés comme un moyen alternatif pour augmenter l'efficacité spectrale dans les communications optiques. Plusieurs schémas de chiffrement de la couche physique ont incorporé le chaos numérique pour améliorer la sécurité de la transmission en aval dans OFDM-PON [71],

I.8.3.3. La modulation OFDM

- **Introduction au système Multi-porteurs**

La transmission numérique est le transfert physique de données sur un canal de communication point à point ou point à multipoint tel que des fils de cuivre (canaux guidés et non guidés), des fibres optiques, des canaux de communication sans fil et des supports de stockage.

Les données à transmettre dans les systèmes de communication sans fil sont représentées sous plusieurs formes soit sous la forme d'une tension électrique, une onde radio, une micro-onde ou un signal infrarouge.

Pour transmettre efficacement des signaux ou message sur de longues distances nous utilisons les techniques de modulation. Tous les systèmes de communication sans fil utilisent un schéma de modulation pour mapper le signal d'information sous une forme qui peut être efficacement transmise sur le canal de communication. Un large éventail de schémas de modulation a été développé, le plus approprié selon que le signal d'information est une forme d'onde analogique ou un signal numérique.

La modulation est le processus consistant à faire varier une ou plusieurs propriétés d'une forme d'onde périodique de haute fréquence, appelée signal porteur, avec un signal modulant qui contient généralement l'information à transmettre.

L'objectif principal de la modulation aujourd'hui est de compresser autant de données dans le moins de spectre possible. Cet objectif, connu sous le nom d'efficacité spectrale, mesure la rapidité avec laquelle les données peuvent être transmises dans une bande passante assignée exprimée en termes de bits par seconde par Hz (b/s/Hz). De multiples techniques ont vu le jour pour atteindre et améliorer l'efficacité spectrale. Il existe diverses techniques de modulation analogiques et numériques utilisées pour transmettre les signaux.

L'idée principale de la frequency-division multiplexing (FDM) est venue après le développement du système de communication et la demande croissante sur le besoin d'accélérer le transfert de données.

Cette technologie qui fonctionne en divisant le canal en (sous-canaux) et divise la porteuse en (sous porteuses) pour pouvoir envoyer plusieurs signaux différents sur la même bande en même temps ce qui aide à résoudre plusieurs problèmes précédents ,car en envoyant un signal, puis l'autre avec un retard entre les deux signaux ,cela a causé plusieurs problèmes par le passé, en particulier à la télévision où on envoyait l'image et puis le son et en réception des signaux l'image souvent précède le son .

Mais la technique FDM a eu plusieurs inconvénients, parmi lesquels une partie de la bande est laissée sur les deux côtés de chacune des porteuses pour éviter le chevauchement, cela réduit l'efficacité de cette technique parce qu'une grande partie de la bande est gaspillée sans en bénéficier.

Pour que le signal modulé ait une grande efficacité spectrale, il faut que les fréquences des porteuses soient les plus proches possibles, tout en garantissant que le récepteur soit capable de les séparer et retrouver le symbole numérique émis sur chacune d'entre elles. Ceci est vérifié si le spectre d'une porteuse est nul aux fréquences des autres porteuses.

Il est bien connu que les systèmes de communication traditionnels comportent deux parties, respectivement appelés émetteur et récepteur. Le signal de sortie de l'émetteur est modulé et transmis par le canal public au récepteur qui démodule le signal reçu pour récupérer le signal original. La récupération du message est soumise à une condition essentielle. Cette condition se traduit par le rapport signal utile sur signal transmis qui doit être le plus proche possible de l'unité.

Le terme OFDM a été réservé à une forme particulière de modulation par division de fréquence FDM. Les sous-porteuses dans un signal OFDM sont espacées aussi étroitement que cela est théoriquement possible, tout en maintenant l'orthogonalité entre elles. Le principe du multiplexage en fréquence est de grouper des données numériques par paquets de N, qu'on appellera symbole OFDM et de moduler par chaque donnée une porteuse différente en même temps ce qui revient à répartir un flux de données à haut

débit sur plusieurs flux à faible débit. Ces derniers sont transmis simultanément sur des sous-porteuses orthogonales. La somme de ces sous-porteuses constitue le signal OFDM transmis.

Le signal transmis se propage dans un canal à trajets multiples et subit des distorsions. A la réception, des versions décalées du même signal sont reçues avec des interférences entre symboles OFDM. Pour éliminer cette interférence, un préfixe cyclique (CP) de durée supérieure à l'étalement maximal des retards du canal est ajouté au début de chaque symbole OFDM à l'émission. En réception, les opérations inverses sont réalisées, ainsi que les opérations d'estimation et d'égalisation du canal.[68]

Construction du signal OFDM

La modulation OFDM est la superposition de nombreux signaux indépendants modulés sur des sous-porteuses individuelles avec une bande passante espacée égale. La Figure I.15 montre le chevauchement des sous-porteuses dans le domaine fréquentiel.

Considérons une séquence de N données$C_0, C_1, \dots \dots C_{N-1}$,appelons T_s la durée du symbole c'est-à-dire le temps qui sépare deux séquences de N données. Chaque porteuse modulant une donnée pendant une fenêtre de durée T_s, le spectre total est la somme des spectres individuels obtenus par application de la transformée de Fourier. Chaque donnée $C_k$module un signal à la fréquence f_k, Si C_0 est représenté par l'impulsion rectangulaire de durée T. Le spectre correspondant est l'impulsion « Sinc ». On peut imaginer que la séquence complète est représentée dans le domaine fréquentiel avec la version décalée des impulsions « Sinc ». Ceci est obtenu en multipliant C_k par $e^{2\pi f_k t}$. Cela équivaut à décaler l'impulsion « sinc » dans le domaine fréquentiel vers la droite avec la fréquence f_k, ainsi, le signal composé de sous-bande est obtenu sous la forme complexe $C_k\, e^{2\pi f_k t}$.

Le signal s(t) total correspondant à toutes les données d'un symbole OFDM est la somme des signaux individuels :

$$s(t) = \sum_{k=0}^{N-1} c_k e^{2j\pi f_k t} \qquad (I.4)$$

Le multiplexage est orthogonal si l'espace entre les fréquences est $1/T_s$alors :

$$\begin{cases} s(t) = e^{2j\pi f_0 t} \sum_{k=0}^{N-1} c_k e^{2j\pi \frac{kt}{T_s}}. \\ f_k = f_0 + \dfrac{k}{T_s} \end{cases} \qquad (I.5)$$

Les données numériques C_k sont l'enveloppe complexe du signal modulé définis à partir d'éléments binaires par une constellation (mapping) de modulation d'amplitude en quadrature QAM à plusieurs états (4, 16, 64, de façon générale à 2^q états).

$$Si\ C_k = I_k + jQ_k\ \ alors$$

$$S(t) = Re\big(s(t)\big) = \sum_{k=0}^{N-1} (I_k + Q_k) e^{2j\pi\left(f_0 + \frac{k}{T_s}\right)t} \qquad (I.6)$$

$$S(t) = \sum_{k=0}^{N-1} I_k \cos\left(2\pi\left(f_0 + \frac{k}{T_s}\right)t\right) - Q_k \sin\left(2\pi\left(f_0 + \frac{k}{T_s}\right)t\right) \qquad (I.7)$$

Si le symbole C_k transporte q bits, le débit total est (nombre de bits par seconde) $qN/T_s = qB$, pour une largeur de bande utilisée, le débit ne dépend pas de la durée des symboles ni du nombre de porteuses. Si on augmente la durée des symboles T_s le spectre de chaque porteuse $1/T_s$ devient plus étroit et on peut augmenter le nombre de porteuses.

Le spectre de fréquences tend vers un spectre rectangulaire idéal à mesure que le nombre de porteuses augmente, le canal global se comporte comme un canal sans distorsion.

La Figure I.15 illustre le schéma type de la modulation en OFDM avec trois sous-porteuses, le spectre total est la somme des spectres individuels. L'espace entre chaque sous-porteuse $est\ \frac{1}{T_s}$ ce qui permet, lorsque le spectre d'une sous-porteuse est maximal, d'annuler le spectre de toutes les autres, c'est la condition d'orthogonalité dans le domaine fréquentielle (la condition d'Orthogonalité d'OFDM)[72].

Cette condition d'orthogonalité permet d'avoir un recouvrement sans interférences entre les spectres des différentes sous-porteuses, en effet l'échantillonnage est fait précisément à la fréquence d'une sous-porteuse, la bande en fréquence est occupée de façon optimale, puisque le spectre est presque plat dans cette bande. La bande occupée est à peu près $B = N/T_s$ (en excluant les lobes secondaires de part et d'autre de la bande), chaque sous-porteuse occupant à peu près $1/T_s$.

Le signal parvenant au récepteur s'écrit, sur une durée symbole T_s :

$$y(t) = \sum_{k=0}^{N-1} c_k H_k(t) e^{2\pi j(f_0 + \frac{k}{T_s})t} \qquad (I.8)$$

$H_k(t)$, est la fonction de transfert du canal autour de la fréquence f_k et au temps t.

Puis après échantillonnage

$$z(t_n) = z\left(\frac{nT}{N}\right) = z_n = (-1)^n \sum_{k=0}^{N-1} c_k H_k e^{2\pi j(\frac{k_n}{N})} \qquad (I.9)$$

On voit que z_n est la Transformée de Fourier discrète inverse de $C_k H_k$, la démodulation consiste donc à effectuer une Transformée de Fourier directe discrète.

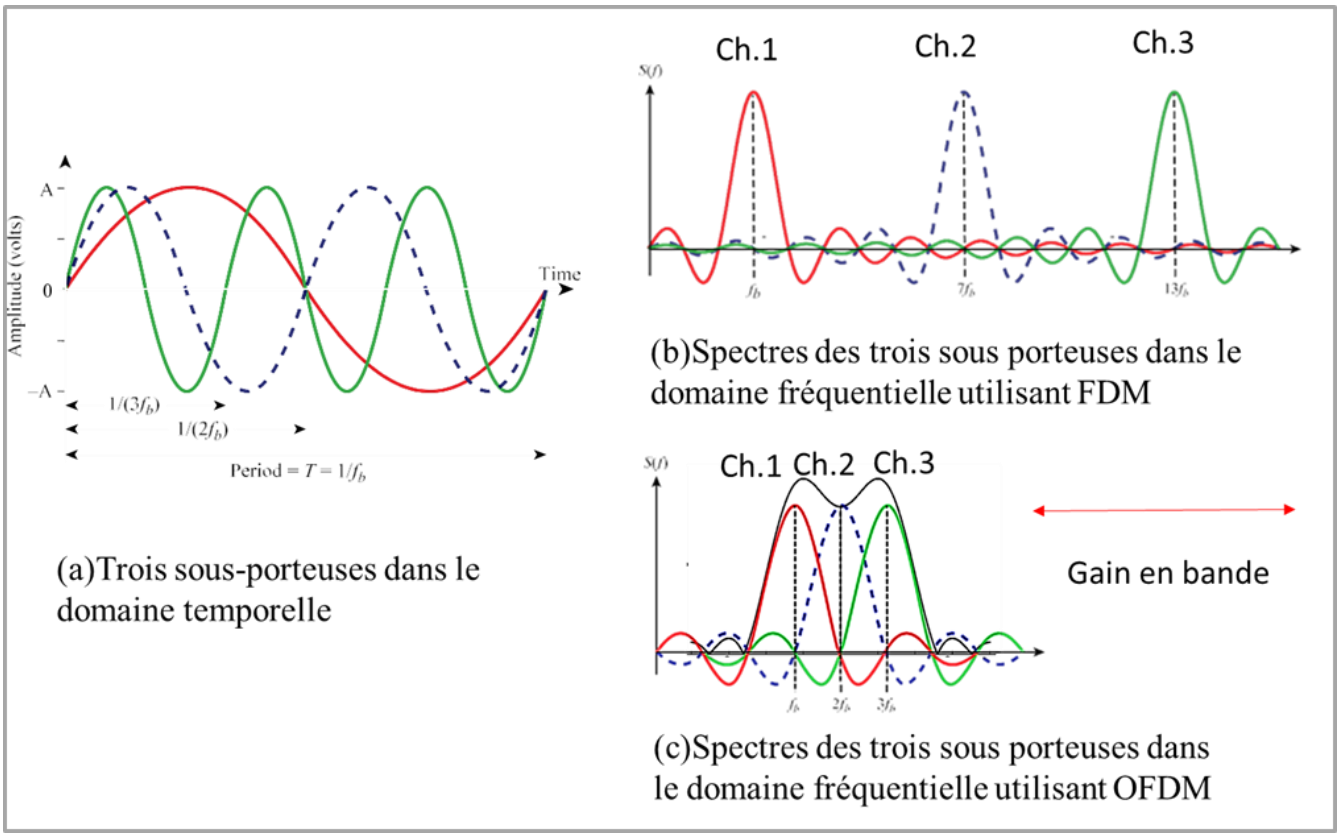


Figure I. 15 Construction du signal OFDM

La démodulation dépend des perturbations subies par le signal après son passage dans le canal. Les modulations multi-porteuses sont particulièrement utiles pour des canaux comportant des échos multiples[68, 73].

OFDM est une bonne solution pour assurer un débit de données élevé dans le milieu sans fil en raison de sa résistance à L'IES ou ISI en anglais pour « Inter-Symbol-Interference », qui est un problème courant limitant la vitesse des transferts de données, en divisant le signal en plusieurs porteuses à bande passante étroite. Il en résulte un faible débit de symboles réduisant la quantité d'ISI.

- **L’OFDM appliqué à la communication multimédia sans fil**

Auparavant, la technologie OFDM a été utilisée pour transmettre des informations sur les canaux FM, la radio numérique (AB), la radiodiffusion télévisuelle numérique locale (DVB-T) et l’ADSL, mais elle est maintenant largement employée surtout dans les systèmes de communications cellulaires et sans fil à large bande passante et à haut débit, notamment le Wi-Fi, LTE et le WiMax, appliquée aux communications acoustiques sous-marines (UAC)[74].L’OFDM à bande étroite est incorporé également dans les émetteurs-récepteurs de communication sur ligne électrique des sous-stations intelligentes du côté BT (Basse tension) pour les messages d'état et d'alarme entre les centrales électriques et les sous-stations.[75].

Dans le but de maximiser l'efficacité spectrale, différentes approches ont été envisagées dans la littérature. Des méthodes telles que l’accès multiple non orthogonal (NOMA) [76]et massive multiples - entrées multiples sorties (MIMO) proposées dans [77]. Le full-duplex intra-bande dans les systèmes de communication sans fil a également montré le potentiel de gains importants en efficacité spectrale ; cependant, il a été entravé par l'auto-interférence qu'elle introduit [78].

II

Chapitre II :
La Sécurité des WMSNs

II.1. Introduction à la sécurité des Réseaux de Capteur sans fil

L'utilisation émergente des réseaux de capteurs multimédias sans fil et des installations de communication sans fil ont accru le besoin de mesures de sécurité du réseau pour protéger différents types de données multimédias pendant la période d'émission en temps réel ou non réel. De nombreux chercheurs s'intéressent de plus en plus à la sécurité des WMSNs en raison des vastes nécessités d'application qui peuvent être étendues sur le smart environnement, surveillance et sécurité, les soins de santé intelligents ; donc exigences de sécurité des données multimédias et la qualité de service (QoS) doivent être satisfaisantes.

L'évaluation des risques de sécurité est mise en avant dans la conception des WMSNs, il n'y a pas de solution unique et complète, en adoptant toutes les mesures de sécurité possibles cela pourrait être coûteux en tous points, (c.-à-d. complexité, coût financier, retard, etc.). Les auteurs dans [79] ont étudié plusieurs travaux de recherche qui traitent de l'efficacité de la mise en œuvre des communications sécurisées des utilisateurs en prenant en compte la confidentialité, l'authentification, l'intégrité des données et la disponibilité des services, ainsi que les attaques et les menaces modernes avec leurs contre-mesures.

De nombreux défis de sécurité à différents niveaux de conception sont à prendre en considération pour concevoir le meilleur modèle en combinant les problèmes de sécurité les plus importants afin d'atteindre des WMSN sécurisés, tel que : la gestion des risques pour trouver la solution de sécurité appropriée est optimale à la phase de conception [80], ou encore la capacité de trouver ou de concevoir un protocole de routage sécurisé [81].

Des solutions innovantes non cryptographiques basées sur la détection et la prévention c'est-à-dire empêcher toute connexion non autorisée au réseau et empêcher toute usurpation ou altération sur les données routées sont présentées dans [82] les auteurs ont étudié le problème de détection d'intrusion (IDS)en considérant des algorithmes issus des domaines tels que Machine Learning (ML) techniques, Deep Learning (DL) techniques, and Swarm and Evolutionary algorithms (SWEVO).

Les exigences de sécurité des WMSNs sont similaires à celles des réseaux informatiques conventionnels, des solutions communes conçues pour les réseaux informatiques et hérités par les WMSNs. La contrainte

principale de tous les algorithmes développer pour les WMSNs est d'avoir une utilisation minimale des ressources et des coûts.

La majorité des solutions sont assurés par une science des techniques mathématiques connue sous le nom de la cryptographie.[83]

II.2. Les techniques de Sécurité Cryptographiques dans les WMSNs

II.2.1. Terminologies de la cryptographie

Dans cette section, nous fournirons des définitions formelles et des explications pour les termes et sous-champs liés à la cryptographie

II.2.1.1. Cryptographie

Le mot remonte aux racines grecques ancien qui a été inventé en combinant deux mots grecs : **κρυπτός**, romanisé : **kryptós** signifiant "caché" ; et **γράφειν** graphein, signifiant "écrire", Kryptós une racine partagée par plusieurs mots anglais, dont "crypt", "cryptic" et "encrypt". La cryptographie par définition est la conversion ou transformation des données sous une forme incompréhensible afin d'en protéger le contenu de l'accès non autorisé. La cryptographie moderne consiste en l'étude des techniques diverses pour la sécurité de l'information basée sur la théorie mathématique avec des outils modernes tel que la technologie informatique.

Le processus de conversion des données est appelé chiffrement, le terme « cryptage » est tiré de l'anglais « Encryption » et le processus de récupération des données chiffrées est appelé déchiffrement.

Un algorithme de chiffrement traite les données d'origine pour les transformer sous une forme incompréhensible, généralement à l'aide d'une clé, qui est également requise pour le processus de déchiffrement[84].

II.2.1.2. Clé de chiffrement

L'information à chiffrer est également appelée message ou « plain message », en anglais. L'information chiffrée est le résultat d'une transformation dépendant du message et d'une information secrète « la clé ».

Les algorithmes de chiffrement sont généralement classés comme algorithmes à clé symétrique et à clé asymétrique. Les algorithmes de chiffrement avec des clés symétriques utilisent la même clé secrète pour le chiffrement et le déchiffrement (Une même clé est utilisée entre deux nœuds, donc n(n-1) /2 clés avec : n nombre des nœuds) alors que les algorithmes de chiffrement avec des clés asymétriques utilisent des clés

différentes, une clé publique pour le chiffrement et une autre clé privée pour le déchiffrement, le nombre de clés générées= 2n.

Les algorithmes à clé asymétrique nécessitent plus de puissance de traitement et de ressources mémoire qu'un nœud de capteur multimédia peut offrir. Contrairement à un nœud de capteur typique dans les (Wireless Scalar Sensor networks) WSSN, cependant avec les progrès de ces dernières années, un nœud de capteur multimédia est devenu suffisamment puissant pour traiter correctement les données multimédia, de sorte que de nombreux chercheurs considèrent que les algorithmes à clé asymétrique sont une solution faisable pour les WMSNs[84].

Dans les algorithmes symétriques, le temps nécessaire pour crypter et déchiffrer les données est comparativement inférieur à celui d'un algorithme asymétrique. Alors que les avantages d'algorithmes asymétriques ne sont nécessaires que pour maintenir la confidentialité des clés privées sans avoir besoin de changer fréquemment de clé comme cela se produit dans le cas de l'algorithme symétrique.

II.2.1.3. Chiffrement et codage

Les opérations de chiffrement et de codage font partie de la théorie de l'information. La différence essentielle réside dans la volonté de protéger les informations et d'empêcher des tierces personnes d'accéder aux données dans le cas du chiffrement.

Le codage consiste à transformer l'information (des données) vers un ensemble de mots. Chacun de ces mots est constitué de symboles. La compression est un codage : on transforme les données vers un ensemble de mots adéquats destinés à réduire la taille mais il n'y a pas de volonté de dissimuler (bien que cela se fasse implicitement en rendant plus difficile d'accès le contenu). On peut aussi considérer que le chiffrement doit résister à un adversaire " intelligent " qui peut attaquer de plusieurs manières alors que le codage est destiné à une transmission sur un canal qui peut être potentiellement bruité. Ce bruit est un phénomène aléatoire qui n'a pas d'" intelligence " intrinsèque mais peut toutefois être décrit mathématiquement[84].

- Le codage et la compression de l'image :

La représentation de base d'une image numérique correspond à un tableau 2-D rectangulaire d'éléments appelés pixels. Il faut donc mémoriser un grand nombre de pixels. Pour une simple image monochrome (en niveaux de gris), il faut mémoriser par exemple typiquement pour une image de 512x512 pixels (soit 256 000 pixels) et 8 bits par pixel pour obtenir une bonne résolution (8 bits pour coder un pixel, ce qui donne

par pixel un nombre de 2^8= 256 valeurs possibles). Pour des images en couleurs de haute résolution, et pour des images animées le nombre de bits nécessaires à la représentation de base devient vite très important à mémoriser ou à transmettre. Le codage d'une image a donc pour but d'obtenir de cette dernière, une représentation qui ne nécessite qu'un nombre très réduit de bits en comparaison de l'image de base[84].

II.2.1.4. Cryptologie

La cryptologie est la science qui étudie les techniques théoriques et pratiques des communications sécurisées. Elle se divise en deux branches apparentées : la cryptographie et la cryptanalyse. Le cryptographe essaie de trouver des techniques pour garantir le secret du message et parfois pour assurer l'authenticité et l'intégrité du message, tandis que le cryptanalyste essaie d'annuler le travail du cryptographe en brisant le secret du message pour récupérer l'original ou en falsifiant un message pour être accepté comme authentique[84].

II.2.1.5. Cryptosystèmes

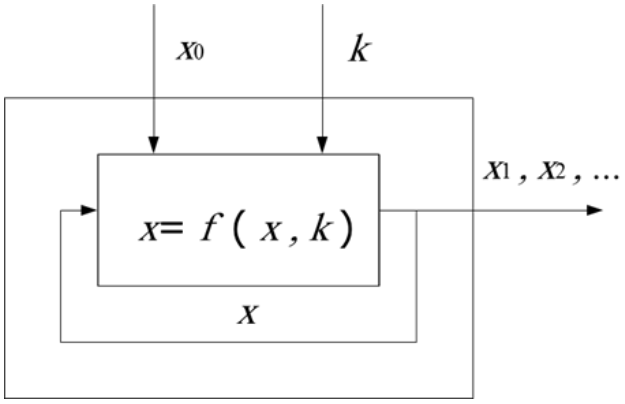


Figure II. 1 Principe du système cryptographique (Lynnyk, 2010).

La cryptographie consiste notamment en l'élaboration de schémas de chiffrement/déchiffrement.Un cryptosystème est l'ensemble des deux méthodes de chiffrement et de déchiffrement.

Du point de vue mathématique, le cryptosystème S = ⟨X , Y, K, f ⟩ est la transformation de l'information

f : X × K → Y, définie sur les espaces X , Y, K, qui sont les états initiaux, les états finaux et les clés respectivement. La condition x ∈ X chiffre des informations utiles. Dans les espaces de cryptographie informatique .

X ⊂ {0, 1}∗, Y ⊂ {0, 1}∗, K ⊂ {0, 1}∗, et la transformation f est donnée par l'algorithme réalisé avec une machine de Turing. La transformation f peut être considérée comme la fonction d'itération de

l'algorithme cryptographique (voir Figure. II.1). Dans ce cas, le cryptosystème génère les séquences d'états x0, x1, x2, ..., xi.

$$\begin{cases} x_i = f(x_{i-1}, k) \\ x_0 \in \mathrm{X}, \mathrm{k} \in \mathrm{K} \end{cases} \qquad (\text{II. } 1)$$

Cette séquence s'appelle une trajectoire ou l'orbite du système. L'orbite globale est déterminée par l'état initial x0 du système et le paramètre k. Une telle transformation ultérieure d'un état par l'application de la même fonction primitive peut être vue dans les chiffrements par blocs, les chiffrements par flux, les générateurs de bits pseudo-aléatoires, etc. Ainsi, un cryptosystème peut être compris comme un système dynamique S = ⟨f , X , K⟩ avec une fonction non linéaire f , l'espace d'états X et l'espace de paramètres K[84].

II.2.1.6. Cryptanalyse

La cryptanalyse effectuée par les attaquants est l'étude du texte chiffré, des techniques de chiffrements et des cryptosystèmes dans le but d'obtenir des informations sur la clé secrète pour "casser" le chiffrement.

La cryptanalyse effectuée par les cryptologue est l'étude des attaques possibles sur les cryptosystèmes , dans le but de s'assurer que le chiffrement est effectivement robuste de déceler d'éventuelles faiblesses et améliorer les techniques de chiffrement.

Il existe de nombreux types d'attaques et de techniques de cryptanalyse, qui varient en fonction de la quantité d'informations dont dispose l'analyste sur le texte chiffré analysé. Certaines méthodes cryptanalytiques incluent:

Une attaque basée sur le fait d'avoir des échantillons du texte brut et du texte chiffré correspondant est appelée attaque en **texte brut connu**. (b)

Lorsqu'un attaquant a la capacité de choisir un texte brut arbitraire et d'obtenir le texte chiffré correspondant, on parle d'attaque en **texte brut choisi**. (c)

Une attaque de **texte chiffré choisi** est donc lorsque l'attaquant peut insérer du texte chiffré choisi dans le système et obtenir le texte brut résultant. (d)

Sinon, les **attaques par force brute** qui sont utilisées en dernier recours, l'attaquant essaie toutes les combinaisons possibles des clés jusqu'à l'obtention d'un texte clair. Cette attaque est la plus coûteuse en temps de calcul et en mémoire.

Une **attaque par canal auxiliaire** dépend des informations collectées à partir du système physique utilisé pour chiffrer ou déchiffrer. Les attaques par canal auxiliaire sont liées au temps nécessaire à un système pour répondre à des requêtes spécifiques, à la quantité d'énergie consommée par le système de chiffrement ou au rayonnement électromagnétique émis par le système de chiffrement[84].

II.2.2.Les techniques de cryptographie standards

Les techniques de cryptographie classiques sont basées sur la théorie des nombres, et en particulier sur la décomposition d'un entier en éléments simples, en utilisant des algorithmes symétriques tel que le DES par exemple et l'algorithmes asymétriques tel que le RSA.

Le D.E.S. est un système de chiffrement par blocs. Cela signifie que D.E.S. ne chiffre pas les données à la volée quand les caractères arrivent, mais il découpe virtuellement le texte clair en blocs de 64 bits qu'il code séparément, puisqu'il concatène. Un bloc de 64 bits du texte clair entre par un coté de l'algorithme et un bloc de 64 bits de texte chiffré sort de l'autre coté. L'algorithme est assez simple puisqu'il ne combine en fait que des permutations et des substitutions. On parle en cryptologie de techniques de confusion et de diffusion.

Aujourd'hui, le D.E.S. est facile à briser par les puissances de calcul des ordinateurs, il est en effet impossible de balayer la plupart des clés pour casser le chiffrement. Un nouveau système de remplacement est le A.E.S. (Advanced Encryption Standard) qui utilise une clé de 128 bits pour le cryptage. Cet algorithme a une structure particulière pour chiffrer et déchiffrer les données ,il est implémenté à la fois matériellement et logiciellement.

Les algorithmes de chiffrement par bloc (AES, DES, 3DES, Blowfish) ainsi que par flux (SALSA20) sont testés en prenant différentes tailles de fichiers audio dans las traveaux de [85].

L'algorithme le plus répandu est l'algorithme RSA. Il a été inventé en 1978 par R.Rivest, A. Shamir et L. Adleman . Il est fondé sur les propriétés des nombres premiers. Le principe est simple : on choisit deux nombres premiers « p » et « q » au hasard. On calcule n = pq et z = (p - 1)(q - 1). On choisit un nombre « d » premier avec « z », et on cherche «e » tel que ed ≡ 1[n]. Le couple (e; n) constitue la clé publique, (d; n) la clé privée. La fonction de cryptage est la multiplication par « e » modulo « n », la fonction de décryptage est la multiplication par « d » modulo « n ». La connaissance de « n » donne théoriquement accès à « p » et « q » qui sont par dénition les facteurs premiers de n. La force de la technique RSA repose sur l'extrême difficulté à factoriser de grands nombres, mais le développement de la puissance de calcul des

ordinateurs et l'utilisation du parallélisme améliorent sans cesse les temps de factorisation. Le choix d'une longueur de clé (la taille de n) est directement lié au niveau de condentialité recherché. En contrepartie, l'algorithme RSA est très lent, ce qui n'est guère pratique pour les données volumineuse : plus la clé est grande, plus les processus de cryptage et de décryptage sont longs. Cette technique est donc réservée aux messages courts.

Cependant il existe d'autres variantes et améliorations dans la taille des clés et la rapidité de cet algorithme standard tel que, les algorithmes CRT RSA, Multi-Prime RSA, Multi-Power RSA, Rebalanced RSA and R-Prime RSA, DUAL RSA ainsi que des cryptosystèmes hybrides (une combinaison d'algorithmes symétriques et asymétriques) tel que RSA-Elliptic , RSA-ECC (Elliptic Curve Cryptography) présentés dans les traveaux de [86].

Ainsi, diverses solutions ont été présentées. Dans [84], Lai et al. Ont examiné et discuté d'importantes méthodes d'authentification cryptographique et de cryptage pour sécuriser les systèmes de distribution des ressources énergétiques (DER), tout en fournissant des recommandations sur l'application de la cryptographie à la DER systèmes. Dans [87], l'article reflète une étude détaillée de la littérature existante sur les techniques d'authentification d'images basées sur le hachage et fournit les solutions les plus optimales basées sur différents paramètres.

Un exemple de technique de chiffrement symétrique par flux est RC4, conçu par Ron Rivest, qui fonctionne en mélangeant un flux binaire pseudo-aléatoire avec les données en utilisant une opération « ou exclusif » . La production des chiffres introduit une démarche qui génère une séquence de nombres présentant des séquences imprévisibles en pratique avec certaines propriétés du hasard. C'est ce qu'on appelle les générateurs pseudos aléatoires.

Les schémas de cryptage standard non chaotiques sont limités pour les données image/vidéo, pour les applications en temps réel . Étant donné qu'il existe une forte demande de cryptage multimédia, cela suscite l'intérêt pour le cryptage chaotique, qui a un plus grand potentiel pour les données multimédias. Les principaux avantages du chiffrement chaotique sont qu'un signal chaotique ressemble à du bruit pour les utilisateurs non autorisés, et que l'évolution temporelle du signal chaotique dépend fortement des conditions initiales et des paramètres de contrôle des fonctions génératrices. De légères variations de ces grandeurs donnent des évolutions temporelles assez différentes. Par conséquent, les états initiaux et les paramètres de

contrôle deviennent des clés dans un chiffrement. De plus, la génération d'un signal chaotique est souvent peu coûteuse, ce qui la rend appropriée pour le cryptage de données volumineuses.

II.2.3. Les algorithmes cryptographiques légers (lightweight cryptographic algorithms)

Les algorithmes cryptographiques légers sont des algorithmes spécifiques conçus et développés pour fournir une sécurité adéquate pour les dispositifs extrêmement limités en ressources tels que les systèmes RFID, les cartes à puce et les réseaux de capteurs sans fil (WSN).

La demande pour de tels algorithmes de cryptage légers augmente parce que les petits appareils informatiques tels que les étiquettes RFID deviennent de plus en plus nombreux. L'implémentation matérielle de ces algorithmes ne peut pas être facilement modifiée ou lue par un intrus. Par conséquent, il offre une mise en œuvre plus sécurisée physiquement par nature. Les algorithmes cryptographiques légers peuvent être divisés en deux types de chiffrements par blocs et chiffrements de flux. Les chiffrements par blocs telque AES, DESL, DESX, DESLX, HIGHT, ICEBERG, CLEFIA, mCRYPTON, TEA, XTEA ainsi aue. Les chiffrements de flux tel que Trivium et Grain,ils sont présentés avec une analyse dans[88].

II.3. La Sécurité Chaotique en Multimédia

II.3.1. Définition du chaos

En 1975, Li et Yorke sont les premiers à formuler le concept du chaos dynamique, et lui ont donné une condition dans les équations aux différences scalaire, « La présence de trois périodes impliquent le chaos ». Par la suite, d'autres chercheurs ont généralisé la définition de (Li et Yorke) du chaos et l'ont appliquée aux équations aux différences dans R^n et ont formulé des conditions dimensionnelles plus élevées assurant son existence.

L'étude théorique approfondie du chaos est loin d'être l'objectif de ce travail de thèse. Dans cette section, nous nous limitons à définir brièvement le phénomène chaotique. Des détails sur la description du chaos et ses caractéristiques seront donnés qui permettent de comprendre les points marquants d'un système chaotique.

Il existe plusieurs définitions possibles du chaos. Aucune définition du terme chaos n'est encore universellement acceptée. Ces définitions ne sont pas toutes équivalentes, mais elles convergent vers certains points communs caractérisant ainsi le chaos.

- Le chaos est un comportement apériodique à long terme dans un système déterministe qui présente une dépendance sensible aux conditions initiales
- Le chaos est un système pseudo-aléatoire déterministe, mais il a aussi une certitude. Sa certitude signifie que sa valeur de sortie est entièrement déterminée par les équations, les paramètres et les conditions initiales. Seules les mêmes conditions initiales peuvent restaurer la séquence chaotique d'origine.
- Le chaos est aussi défini comme un phénomène de vibrations aléatoires, mais qui s'inscrit néanmoins à l'intérieur d'un système déterministe décrit par des équations différentielles non linéaires, en d'autres termes un phénomènes déterministes imprévisibles très sensibles aux conditions initiales

Un système chaotique est décrit par un ensemble d'équations dynamiques non linéaires et déterministes au sens où lorsque la loi d'évolution est connue, le futur du système est parfaitement déterminé dés lorsque l'on connait son état initial.

Bien que ses équations définissent complètement son évolution, il est imprévisible à long terme, le calcul de l'évolution future du système est quasi impossible à cause de sa très grande sensibilité aux conditions initiales. Deux trajectoires (orbites) issues de conditions initiales proches vont vites devenir décolérées et s'écartent de manière exponentielle

Le chaos trouve couramment des applications dans des domaines allant de la physique, des mathématiques et de la chimie, la médecine, l'économie et largement utilisé dans les technologies de communication, il se prête au chiffrement des informations.

L'intérêt de la recherche pour le chaos est motivé en partie par le développement d'ordinateurs modernes à grande vitesse qui a permis une meilleure modélisation des systèmes chaotiques non linéaires avec une vitesse et une précision élevée[89].

II.3.2. Caractéristiques du chaos

II.2.4.2.1. Exposants de Lyapunov

Les exposants de Lyapunov sont des coefficients qui permettent de mesurer la sensibilité aux conditions initiales d'une série temporelle. Par définition, un exposant de Lyapunov est le taux exponentiel moyen de divergence ou de convergence de trajectoires voisines de l'espace des phases. Il mesure le taux local d'expansion de l'espace dans lequel l'expansion est maximale, c'est-à-dire en général vers l'attracteur. Un

attracteur étrange est un attracteur dont l'un au moins de ses exposants de Lyapunov est positif. Autrement dit, le plus grand exposant est positif pour le système chaotique et négatif pour les autres systèmes.

Considérons un système dynamique discret faisant intervenir une application f et deux conditions initiales très proches$x_0\ et\ x_0 + \varepsilon$.

La première itération conduit à :$x_1 + \varepsilon_1 = f(x_0) + (\frac{df(x_0)}{dx})\varepsilon_0)$

D'où l'on décrit : $\varepsilon_1 = \frac{df(x_0)}{dx}\varepsilon_0$

Après n itérations, il vient :

$$\varepsilon_n = \left(\frac{df^n(x_0)}{dx}\right)\varepsilon_0 = \left(\prod_{i=0}^{n-1}\frac{df(x_i)}{dx}\right)\varepsilon_0 \qquad (II.2)$$

Les termes $\left(\frac{df^n(x_0)}{dx}\right)^{\frac{1}{n}}$ caractérisent la divergence. On définit alors l'exposant de Lyapunov par :

$$\lambda(x_0) = lim_{n\to\infty}\frac{1}{n}ln\left|\left(\frac{df^n(x_0)}{dx}\right)\right| \qquad (II.3)$$

Un exposant positif indique que la divergence entre deux trajectoires voisines augmente exponentiellement avec le temps il s'agit bien là d'une caractérisation d'un attracteur étrange.

Il est possible d'étendre cette définition à une dimension plus élevée d'espace des phases.

Pour un espace de dimension P, il y a P exposants de Lyapunov. Chacun d'entre eux mesure le taux de divergence suivant un des axes du système. Ils sont définis à partir de la matrice jacobienne de l'application f au point x_0 et de ses valeurs propres.

Donc L'exposant de Lyapunov [90, 91]pour un système unidimensionnel est donné par :

$$\lambda = lim_{k\to\infty}\frac{1}{k}\sum_{i=1}^{k} ln|f'(x_{i-1})| \qquad (II.4)$$

Nous distinguons 3 cas pour λ :

1) λ< 0 : Si l'exposant de Lyapunov est inférieur à zéro, alors le système attire ver un point fixe ou d'une orbite périodique stable. Ces systèmes sont non conservatifs (dissipatifs). La valeur absolue de l'exposant indique le degré de stabilité.

2) λ >0 : Si l'exposant de Lyapunov est positif, on parle ici des systèmes chaotiques, l'écart entre deux orbites évolue de façon arbitraire, mais ces deux orbites ne passeront jamais par un même point à long terme.
3) λ =0 : Si l'exposant de Lyapunov est positif, on parle ici des systèmes chaotiques, l'écart entre deux orbites évolue de façons arbitraires, mais ces deux orbites ne passeront jamais par un même point à long terme. Pour une carte chaotique unidimensionnelle défini par

$$\begin{cases} x_{k+1} = f(r, x_k) \\ où\ r\ est\ le\ paramètre\ du\ système \end{cases}$$

L'exposant de Lyapunov est comme suit : $\lambda(r) =$

$$lim_{k\to\infty} \frac{1}{N} \sum_{i=1}^{N-1} ln|f'(r, x_k)| \qquad (II.5)$$

Cas d'un système à n–dimension.

On parle ici de spectre de l'exposant de Lyapunov, λ_i (i=1, 2, ... n), ou n présente le nombre d'équations décrivent le système (ou de manière équivalente, le nombre de variables d'état). Commençons par préciser qu'un système n-dimensions possédera n exposants de Lyapunov. Chacun d'entre eux mesure le taux de divergence suivant un des axes du système, de sorte qu'en moyenne un hyper volume initial S évolue selon une loi de type :

$$V_k = V_0 e^{(\lambda_1+\lambda_2+\lambda_3+\cdots\lambda_n)k} \qquad (II.7)$$

Pour avoir du chaos, il est nécessaire qu'au moins un des λ_i soit positif, selon au moins un axe. Mais il faut également que la somme des λ_i soit négative et l'ensemble de la dynamique doit être dissipatif, c'est-à-dire, globalement stable et le taux total de contraction doit l'emporter sur le taux global d'expansion. En effet, dans le cas contraire, le volume initial finirait par remplir tout l'espace dans lequel il est immergé. On n'aurait alors plus d'un attracteur de faible dimension, et donc plus affaire à du chaos déterministe. Pour avoir calculé les λ_i, nous devons calculer la matrice Jacobienne de système multidimensionnel. La matrice Jacobienne d'un système d'équations f^k est la matrice suivante de type (n, p) [92, 93].

$$f^k(x) = \begin{pmatrix} x_1 \\ . \\ : \\ x_p \end{pmatrix} = \begin{pmatrix} f_1^k(x_1, \dots\dots\dots x_p) \\ : \\ . \\ f_n^k(x_1, \dots\dots\dots x_p) \end{pmatrix}, J^k = \begin{pmatrix} \frac{\partial f_1^k}{x_1}, \dots\dots\dots, \frac{\partial f_1^k}{x_p} \\ . \\ . \\ . \\ \frac{\partial f_n^k}{x_1}, \dots\dots\dots, \frac{\partial f_n^k}{x_p} \end{pmatrix} \quad (II.8)$$

Dans notre cas la matrice Jacobienne J^k est une matrice carréé de type (n x n). Si cette matrice est diagonalisable, alors il existe une matrice inversible P s'appelle matrice de passage telle que :

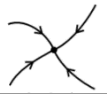
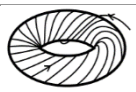
$$D_n^k = P_k^{-1} J^k P \quad (II.9)$$

Où est une matrice diagonale contenant les valeurs propres de J^k .Dénotons celles-ci par

$A_i^k = 1, \dots, n.$ On définit alors les n exposants de lyapunov de la manière suivante :

$$\begin{cases} \lambda_i = lim_{k\to\infty} \frac{1}{k} ln[A_i^k] \\ i = 1, \dots, n \end{cases} \quad (II.10)$$

Tableau II.2. Classification des régimes permanents selon l'exposant de Lyapunov[94]

Etat stable	Flot	Dimension De Lyapunov	Exposant de Lyapunov
Point d'équilibre	Point fixe 	0	$\lambda_n \le \cdots \le \lambda_1 \le 0$
Périodique	Cycle limité 	1	$\lambda_n \le \cdots \le \lambda_2 \le 0$ $\lambda_1 = 0$
Périodique d'ordre 2	Tore 	2	$\lambda_n \le \cdots \le \lambda_3 \le 0$ $\lambda_1 = \lambda_2 = 0$
Périodique d'ordre K	K-tores 	K	$\lambda_n \le \cdots \le \lambda_{k+1} \le 0$ $\lambda_1 = \dots = \lambda_k = 0$
Chaotique Attracteur		Non entier	$\lambda_1 > 0, \sum_{i=1}^{n} \lambda_i < 0$
Hyper-chaotique Attracteur		Non entier	$\lambda_1 > 0, \quad \lambda_2 > 0, \sum_{i=1}^{n} \lambda_i < 0$

II.2.4.2.2. La non-linéraité

Une condition nécessaire à l'apparition du chaos est que le système soit non linéaire. A partir d'un état initial et après un régime transitoire, la trajectoire d'un système dynamique atteint une région limitée de l'espace des phases. Ce comportement asymptotique obtenu pour t, n→∞ est une des caractéristiques les plus importantes à étudier pour tout système dynamique Si dans le cas d'un système linéaire la solution asymptotique est indépendante de la condition initiale et unique, en présence de non-linéarités, il existe une plus grande variété de régimes permanents associés à l'existence d'une infinité de cycles instables, parmi lesquelles on trouve, par ordre de complexité : points fixes, solutions périodiques, solutions quasi-périodiques et chaos, respectivement[100].

II.2.4.2.3. Bifurcation

La bifurcation est généralement désignée comme la transition qualitative d'un comportement régulier à un comportement chaotique, par augmentation du paramètre de contrôle la fréquence du régime périodique double et le nombre d'états stables double, il y a changement de stabilité et l'apparition de nouvelles solutions.

Avec l'augmentation du paramètre les doublements étant de plus en plus rapprochés, on tend vers un point d'accumulation auquel on obtiendrait hypothétiquement une fréquence infinie ce qui conduit à un comportement chaotique du système. L'évolution du point fixe vers le chaos n'est pas progressive mais marquée par des changements discontinus appelés bifurcations menant à des dynamiques de plus en plus complexes.

Dans les applications cryptographiques, le choix de la valeur du paramètre de contrôle détermine l'imprévisibilité du système. Si le paramètre est utilisé comme clé, alors tout l'espace des clés possibles doit générer le comportement chaotique du système[100].

II.2.4.2.4. Sensibilité aux conditions initiales

Les systèmes chaotiques sont extrêmement sensibles aux perturbations. On peut illustrer ce fait par l'effet papillon, popularisé par le météorologue Edward Lorenz. L'évolution d'un système dynamique chaotique est imprédictible en ce sens qu'elle est sensible aux conditions initiales. Ainsi, deux trajectoires de phases initialement voisines s'écartent toujours l'une de l'autre, et ceci quelle que soit leur proximité initiale. Il est en particulier clair que la moindre erreur ou simple imprécision sur la condition initiale interdit de décider

à tout temps quelle sera la trajectoire effectivement suivie et, en conséquence, de faire une prédiction autre que statistique sur le devenir à long terme du système. Ainsi, bien que l'on traite de systèmes déterministes, il est impossible de prévoir à long terme leurs comportements.

L'analyse de toutes sortes d'évolutions temporelles, appelées système dynamique, permet l'étude du chaos. L'état d'un système dynamique est décrit par un certain nombre de quantités dépendantes du temps :$x_1(t), x_2(t), x_3(t), \ldots\ldots\ldots, x_n(t)$ (variables d'état). Au lieu d'étudier séparément ces n variables, il est préférable de représenter le système par un point unique dans un espace à n dimensions[100].

II.2.4.2.5. Sensibilité aux paramètres.

Une petite variation des paramètres de contrôle génère- deux trajectoires chaotiques très différentes même si elles partent de la même condition initiale, les paramètres ont un effet significatif sur le comportement dynamique du système chaotique, a savoir la stabilité , le système sera dans un état différent lorsque les paramètres sont modifiés [100].

II.2.4.2.6. Hyperchaos

Le premier système hyperchaotique à quatre dimensions a été découvert par O.E. Rössler en 1976. Récemment, la génération d'hyperchaos et la réalisation de circuits hyperchaotiques ont attiré l'attention croissante des chercheurs. Le système hyperchaotique a au moins deux exposants positifs de Lyapunov, indiquant que sa dynamique est étendue dans plus d'une direction simultanément. Pour le système continu autonome, la dimension d'un attracteur hyperchaotique doit être d'au moins quatre, cependant, pour un attracteur chaotique, trois dimensions suffisent et il n'a qu'un seul exposant de Lyapunov positif. Par conséquent, par rapport au système chaotique ordinaire, le système hyperchaotique a une dynamique plus compliquée et plus riche afin d'être mieux appliqué dans de nombreux domaines nécessaires au chaos. Dans la communication sécurisée chaotique, un signal chaotique est utilisé pour masquer les messages transmis, et on avait cru que les messages dans cette situation étaient hautement sûrs jusqu'en 1995, lorsque Perez et Cerdeira ont prouvé que le signal chaotique peut parfois être facilement extrait. En effet, le signal chaotique n'a qu'un seul exposant de Lyapunov positif, ce qui signifie que sa dynamique est étendue dans une direction et que sa trajectoire n'est pas très désordonnée. Heureusement, un système hyperchaotique de dimension supérieure peut surmonter ce problème en raison de son caractère aléatoire croissant et de son imprévisibilité plus élevée[100].

II.2.4.2.7. Attracteur

Un attracteur est caractérisé par mouvement irrégulier dans l'espace de phase. (Irregular motion in phase space) « Un espace des phases = l'ensemble des états possibles du système »

La dimension de l'espace des phases = nombre de paramètres nécessaires pour spécifier un état du système ». Cette représentation permet de distinguer un comportement chaotique. Un mouvement régulier correspond à un diagramme simple, un attracteur. Si le mouvement est aléatoire, les points du système remplissent l'espace des phases au hasard : aucune structure n'apparait. Quand le mouvement est chaotique, les points paraissent à première vue aléatoires. Néanmoins, quand on observe le système suffisamment longtemps, on constate que les points dessinent une forme particulière, qui présente une structure feuilletée (fractale). A cause de cette géométrie particulière, ces attracteurs sont qualifiés d'étrange. Ils sont la signature du chaos.

Un attracteur est la zone de l'espace des phases qui attire les trajectoires d'un système dynamique quelconque. L'attracteur le plus simple est un point, c'est l'attracteur d'un système qui évolue à taux constant, d'autres attracteurs peuvent inclure des cycles qui se répètent au cours du temps. Dans le premier cas, le mouvement atteint un état stationnaire ; dans le deuxième cas, le mouvement se reproduit continûment. Dans le cas d'un système chaotique, la trajectoire converge vers une région particulière de l'espace appelée attracteur étrange qui est une signature du chaos[100].

II.3.3. Applications du chaos en communication multimedia

Le développement des systèmes de communication utilisant le chaos a commencé avec :

- **La communication sécurisée basée sur la synchronisation.**

Les systèmes couplés sont modélisés comme des réseaux d'éléments en interaction. La synchronisation fait référence à la tendance à avoir la même dynamique comportementale dans les systèmes couplés.

- **La synchronisation complète**

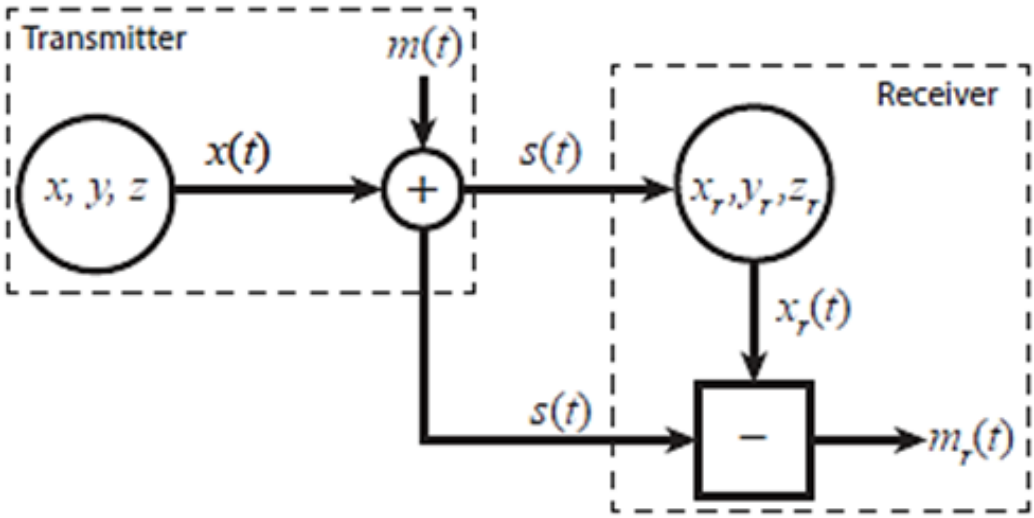


Figure II. 2 Illustration du masquage des messages.**[95]**

Le principe consiste à mélanger l'information $m(t)$ avec une séquence chaotique issue d'un émetteur, décrit généralement par une représentation d'état avec le vecteur d'état $x(t)\ tel\ que\ s(t) = x(t) + m(t)$. Le récepteur a pour rôle d'extraire l'information originale du signal reçu $s(t)$. La récupération de l'information est généralement basée sur la synchronisation des états x(t) de l'émetteur et des états $x_r(t)$ du récepteur Cette méthode est appelée le masquage d'informations. La variation des paramètres de l'émetteur permet de réduire l'erreur de synchronisation [95].

- **La synchronisation de phase**

La notion de synchronisation de phase entre deux circuits chaotiques couplés a fait son apparition en parallèle avec les précédents concepts de synchronisation. Dans ce cas la synchronisation vise à réaliser une cohérence de phase entre les variables d'état des systèmes considérés. Finalement, plus récemment, une nouvelle technique est apparue avec l'emploi des méthodes d'estimation non-linéaire de type filtrage de Kalman, vues comme une généralisation du couplage des systèmes chaotiques.Leur fonctionnement consiste à appliquer un couplage aux systèmes chaotiques (émetteur/ récepteur), par la transmission de quelques composantes du vecteur d'états du système maître, en vue d'unifier leurs comportements. Ainsi selon la nature de liens on distingue : le couplage mutuel ou le couplage unidirectionnel (maître-esclave). Ce dernier

est le plus convenable aux transmissions sécurisées, car il est plus simple à mettre en œuvre, comme il peut être traité comme un problème de conception d'observateur non linéaire, qui supporte plusieurs configurations adaptées aux différentes classes de systèmes chaotiques .[96]

- **Modulation chaotique (Transmissions à porteuses chaotiques)**

  Le concept de base de la communication numérique utilisant une porteuse chaotique est que les bits sont mappés sur des échantillons de fonctions chaotiques émanant d'un ou plusieurs attracteurs chaotiques. Afin d'éviter la périodicité, les symboles sont mappés sur les sorties non périodiques réelles des circuits chaotiques et non sur les paramètres de certaines fonctions d'échantillonnage connues. La principale différence entre une porteuse chaotique et une porteuse périodique classique est que la fonction d'échantillonnage chaotique pour un symbole donné est non périodique, différente d'un intervalle de symbole à l'autre. Ainsi, la forme d'onde transmise n'est jamais périodique, même si le même symbole est transmis à plusieurs reprises.[97]

- **le chaos généré optiquement** .

  Le chaos généré optiquement est utilisé pour des applications pratiques en raison de la vitesse naturelle et du parallélisme des systèmes optiques. Le chaos qui se manifeste dans les systèmes optiques non linéaires, tels que la lumière laser, les formes d'onde d'images optiques et l'acousto-optique [98].

  Le laser chaotique est considéré comme une nouvelle source de signal et largement appliqué dans les domaines de la communication sécurisée, de la génération de nombres aléatoires, de la détection optique. Dans [99] une synthèse donne un aperçu de progrès récents dans la génération de chaos haute performance et de ses applications de mesure uniques. Plusieurs méthodes créatives qui sous-tendent l'optimisation du chaos, notamment l'amélioration de la bande passante, la suppression des signatures de retard temporel et l'intégration photonique, sont respectivement discutées et vérifiées expérimentalement, ensuite l'application de mesure à haute résolution à longue portée de l'analyse chaotique du domaine de corrélation optique Brillion et du réflectomètre optique du domaine temporel chaos est résumée. Des pistes pour la recherche et le développement futurs de lasers chaotiques et de technologies de mesure du chaos sont également prospectées.

- **Le chaos en cryptographie**

les systèmes chaotiques sont largement utilisé dans le domaine des communications sécurisées car ils peuvent rapidement générer des séquences chaotiques qui sont extrêmement sensible aux valeurs initiales et peuvent souvent être réalisés avec des circuits intégrés (CI). Construire des systèmes chaotiques avec un comportement complexe est essentiel dans une communication sécurisée .De nombreuses techniques de cryptage ont été mises au point utilisant les signaux chaotiques issus des récurrences discrètes pour chiffrer les informations, elles serons détaillées dans ce chapitre.

II.3.4. Structure et Conception des cartes chaotiques

II.3.4.1. Définition de la Carte chaotique

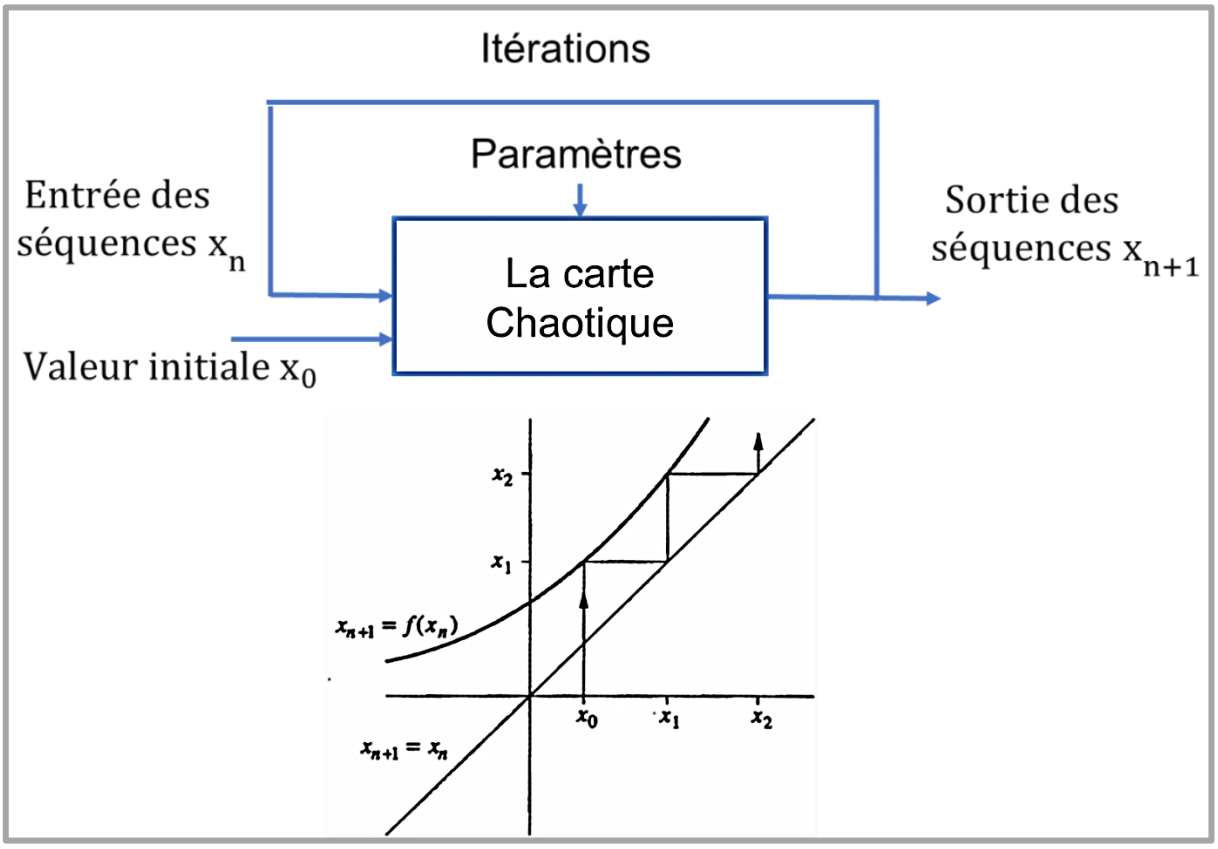


Figure II. 3 Construction par itération d'une carte**[89] .**

La carte chaotique appartient à la classe de systèmes dynamiques dans lesquels le temps est discret, plutôt que continue. Ces systèmes sont connus sous le nom de relations de récurrence, fonctions itérées ou simplement cartes (Map en anglais).

Soit la fonction itérée d'un intervalle I = [a, b] dans lui-même :

$$x_{n+1} = f(x_n, a_i) \qquad (II.11)$$

La séquence x_0 , x_1 , x_3,… est appelée l'orbite de f.

x_0., est appelée la valeur initiale de l'orbite, a_i sont les paramètres de la carte chaotique

La trajectoire de x est la séquence :

$x_0 = x, x_1 = f(x), \dots, x_n = f^n(x), \dots$

Où n est le nombre d'itérations.

$x_1 = f(x_0), x_2 = f(x_1) = f(f(x_0)) \dots, x_n = f^n(x_0), \dots$

$p\ est\ un\ point\ fixe\ si\ f(p) = p.$

$p\ est\ un\ point\ fixe\ périodique\ de\ période\ n\ si\ f^n(p) = p.$

$'f\ '$ Est appelée une carte chaotique si :

1) Les points périodiques sont denses dans I.

2) Transitivité

Étant donné deux sous intervalles ouverts quelconques U1 et U2 dans I

Il existe un point $x_0 \in$ U1 et un n > 0 tel que $f_n(x_0) \in$ U2.

3) Dépendance sensible aux conditions initiales

Il existe une constante de sensibilité, que nous noterons β > 0, telle que pour tout $x_0 \in$ I et tout intervalle ouvert U autour x_0, il existe $y_0 \in$ U et n > 0 els que $f_n(x_0) - f_n(y_0) > \beta$ [89].

La Figure II.3 décrit la technique d'itération graphique pour la visualisation des orbites. Si x_0 est une condition initiale, nous partons d'abord du point $(x_0, x_0) sur\ la\ ligne\ x = y$ et nous nous déplaçons verticalement jusqu'à l'intersection f au point (x_0, x_1) . Puis, déplacez-vous horizontalement jusqu'à (x_1, x_1). En continuant de cette manière, nous pouvons trouver l'orbite entière (Cobwebbing en anglais).

$x_0\ est\ un\ point\ fixe\ stable\ \ si\ |f'(x_0)| < 1$ où $|f'(x_0)|$ est appelé le coefficient de stabilité de x_0.[100]

$x_0\ est\ un\ point\ fixe\ instable\ \ si\ |f'(x_0)| > 1$

Les cartes chaotiques multidimensionnelles sont des systèmes dynamiques définies par des relations de récurrences

$$x_i(n+1) = f(x_1(n), x_2(n), \dots, x_m(n), a_i), i = 1, 2, \dots . m \qquad (II.12)$$

Où $x \in S$, $f : I^m \to I^m$ est une fonction de m-dimensions $I^m \subset [0,1]\ ou\ [-1,1]$

Après un nombre suffisamment grand d'itérations, un paramètre d'entrée initiale sera finalement réparti sur tout l'espace des phases à travers l'orbite de type aléatoire au fil des itérations.

Les paramètres du système et les conditions initiales peuvent être considérés comme la clé privée d'un crypto système chaotique.

On dénombre plus d'une centaine de cartes chaotiques entre le discret et le continue quelques-unes sont d'ordre fractionnel dans des espaces de dimensions différentes (1D, 2D et 3D).

- Les cartes chaotiques unidimensionnelles(1D) discret : Logistic, Skew tent, Chebyshev, Sine.
- Les cartes chaotiques bidimensionnelles (2D) telles que : les cartes Cat, Hénon, Baker sont largement utilisées pour la conception de générateurs de nombre aléatoires et comme fonction de substitution, de permutation, voire de diffusion, dans les différentes couches de crypto-systèmes basés chaos.
- Les cartes chaotiques tridimensionnelles continues (3D) : Lorenz, Chua, Rössler.

Les cartes sont rapides à simuler sur les ordinateurs où le temps est intrinsèquement discret. De telles expériences informatiques ainsi que leurs propriétés de dépendance sensible aux conditions initiales et aux paramètres du système, et les sorties de type aléatoire ont révélé leur adaptation aux processus de confusion et la diffusion de la cryptographie, elles ont donc été utilisées pour construire de robuste crypto systèmes[100].

II.3.4.2. Principe de Mixage des cartes chaotiques

De nouvelles structures ont émergés parmi les quelles ont commencé à être proposés des crypto systèmes chaotiques à base de combinaisons de cartes chaotiques .Pour surmonter la faiblesse de sécurité des cartes chaotiques unidimentionnelles existantes vis-à-vis des comportements chaotiques complexes, de

nombreuses propositions ont été observées telles que l'utilisation de structures en intégrant deux à trois cartes chaotiques 1D traditionnelles dans un seul système.

Cette section présente des modèles de mixage chaotique non linéaire. Les modèles proposés dans la littérature sont présentés dans le tableau I. qui contient, trois opérations non linéaires de base. Chaque opération peut utiliser des cartes chaotiques existantes comme cartes de départ pour générer de nouvelles structures et un grand nombre de nouvelles cartes chaotiques[101].

1) Structure en cascade :

Motivés par l'opération en cascade dans la conception de circuits, la structure proposée est une opération en cascade pour générer de nouvelles cartes chaotiques. Il connecte deux cartes chaotiques 1D en série. La définition de l'opération en cascade est donnée comme suit :

$$x_{i+1} = g\big(f(x_i)\big) \qquad \text{(II. 12)}$$

Sa structure est illustrée dans le tableau I. Comme on peut le voir, f(x) et g(x) sont deux cartes chaotiques 1D qui sont utilisées comme cartes de départ. La sortie de f(x) est introduite dans l'entrée de g(x), et la sortie de g(x) est la valeur itérative, et également renvoyée dans l'entrée de f(x)

L'opération en cascade a les propriétés suivantes : Non-commutativité : l'échange de l'ordre de f(x) et g(x) se traduira par une carte chaotique différente, c'est-à-dire que $f(g(x_i))$et $g(f(x_i))$sont deux cartes chaotiques complètement différentes• L'opération en cascade aboutit généralement à une carte chaotique avec des comportements plus complexes que ses deux cartes de départ, car sa définition contient les concepts mathématiques de ses deux cartes de départ[101].

2) La commutation (Switching)

L'opération de commutation utilise un commutateur pour sélectionner l'une des cartes de départ à exécuter à chaque itération. L'opération de commutation contient une cartes chaotiques normalisées 1D en tant que cartes de départ et un commutateur de commande q. Selon les règles prédéfinies dans q, une carte de départ est sélectionnée pour générer une orbite chaotique à chaque itération. La définition de l'opération de commutation est présentée comme suit

$$x_{i+1} = f_{q_i}(x_i), where \qquad \text{(II. 13)}$$

$$q_i \in \{1,2,\dots,l\}$$

3) La fusion (Structure parallèle)

L'opération de fusion génère de nouvelles cartes chaotiques en mélangeant la dynamique de deux cartes de graine de manière non linéaire. Sa définition est présentée dans comme suit :

$$x_{i+1} = \big(f(x_i i) + g(x_i)\big) mod\ 1 \qquad (II.14)$$

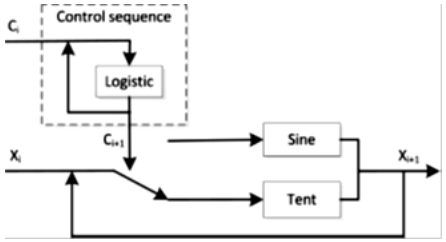
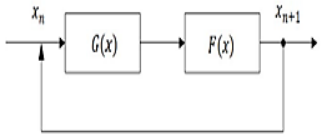
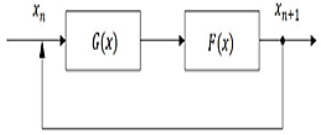
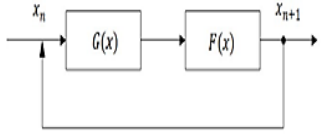
Dans chaque itération, l'entrée est simultanément introduite dans deux cartes de départ, puis les sorties des deux cartes de départ sont combinées par l'arithmétique modulaire. Étant donné que l'entrée est introduite simultanément dans deux cartes de départ et que leurs sorties sont additionnées, l'opération de fusion a la propriété de commutativité. En échangeant les positions de deux cartes de départ, les cartes chaotiques générées sont les mêmes, c'est-à-dire f(x)⊕g(x) = g(x)⊕f(x) [101].

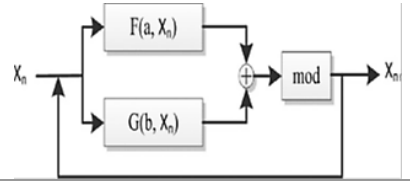
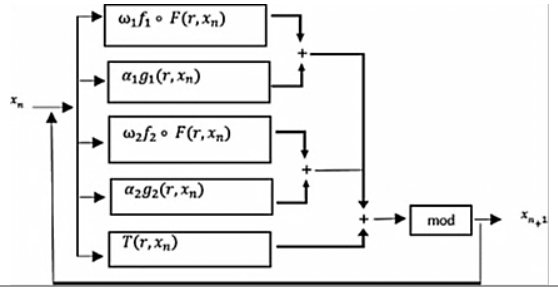
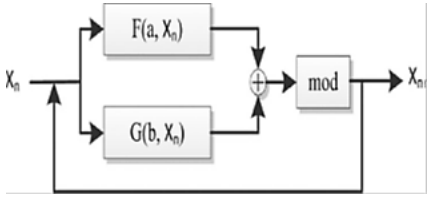
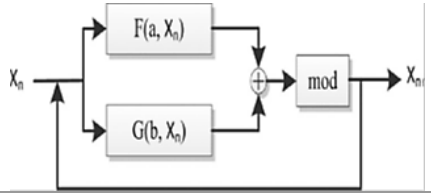
II.3.4.3. Etat de l'art sur le Mixage des cartes chaotiques

Le système chaotique peut être classé en systèmes unidimensionnels et multidimensionnels. Les systèmes chaotiques 1D sont simples et faciles à mettre en œuvre alors que les cartes chaotiques multidimensionnelles ont des structures complexes et de multiples paramètres. Les cartes 1D présentent certaines limitations telles qu'une plage chaotique limitée ou discontinue(fenêtres périodiques dans la plage chaotique), ce qui implique une faible complexité et un espace limité des paramètres, une distribution de données non uniforme dans la séquence chaotique de sortie et la vulnérabilité à certaines attaques. Par conséquent, de nouvelles cartes chaotiques couplées en combinaison de deux jusqu'à trois cartes unidimensionnelles avec de meilleures performances sont développées.

Des algorithmes basés sur des systèmes chaotiques ont commencé à être proposés avec l'importance croissante des études de cryptologie , diverses structure ont été développées récemment, comme la structure cascade, commutation, utilisant des opérations arithmétiques.Une revue de littérature approximative couvrant les dix dernières années a été faite pour montrer le nombre de travaux dans ce domaine basées sur plusieurs structures de combinaison en incorporant deux à trois cartes chaotiques unidimensionnelles (1D) existantes pour générer de nouvelles cartes chaotiques pour le cryptage d'image., elles sont présentées dans le tableau suivant :

Tableau II.3 : Techniques de mixage des cartes chaotiques

Réf	Paramètres de contrôle, valeurs optimales et formules	Structure
[102]	Combinaison des cartes chaotiques 1D:/Logistic/Tent/Sine $x_{i+1} = \begin{cases} T(x) & C_i \geq 0.5 \\ S(x) & C_i < 0.5 \end{cases} \qquad C_i = L(C_{i-1}) = rC_{i-1}(1 - C_{i-1})$	Commutation 
[103]	Logistic/Tent/Sine TL/LT/SS with PRNG $x_{n+1} = F(F(x_n)) or\ x_{n+1} = G(G(x_n))\ \ or\ x_{n+1} = G(F(x_n))$ Modification des paramètres F(x) et G(x) ou même l'ordre de deux cartes de départ.CCS donne une carte chaotique 1-D différente. Par exemple, la Tent-Logistic et Logistic-Tent	 Cascade
[104] [105]	Nous donnons la définition mathématique de la carte 2D-LASM $\begin{cases} x_{i+1} = \sin(\pi\mu(y_i + 3)x_i(1 - x_i)) \\ y_{i+1} = \sin(\pi\mu(x_{i+1} + 3)y_i(1 - y_i)) \end{cases}$	 Cascade
[106]	Mathematiquement , 2D-TCLM est défini comme suit $\begin{cases} x_{n+1} = \begin{cases} (3 + y_n)2\mu x_n(1 - 2\mu x_n) & if\ x_n < 0.5 \\ (3 + y_n)2\mu(1 - x_n)(1 - 2\mu(1 - x_n)) & if\ x_n > 0.5 \end{cases} \\ y_{n+1} = \begin{cases} (3 + x_{n+1})2\mu y_n(1 - 2\mu y_n) & if\ y_n < 0.5 \\ (3 + x_{n+1})2\mu(1 - y_n)(1 - 2\mu(1 - y_n)) & if y_n > 0.5 \end{cases} \end{cases}$ Où (x_n, y_n) sont les valeures itérrratives , μ est le paramètre de contôle μ [0,1].	Cascade 

[107]	**Mixage de cartes 1D avec la combinaison** (Logistic, Tent, Sine) TSS, LTS, LSS $$X_{n+1} = \big(F(a, X_n) + G(b, X_n)\big) mod\ 1$$	Parallèle Fusion 
[108]	**Combinaison des cartes Logistic Tent Sine maps** $x_n = L((r, x_n) = rx_n(1 - x_n)$ $x_n = S((r, x_n) = rsin(\pi x_n)/4$ $$x_{n+1} = T((r, x_n) = \begin{cases} \frac{rx_n}{2} & when\ x < 0.5 \\ \frac{r(1 - x_n)}{2} & when\ x \geq 0.5 \end{cases}$$	Parallèle (Fusion) 
[109]	**Combinaison des cartes Logistic Tent (CLT)** $$Y_n = \begin{cases} mod\left(\mu Y_{n-1} * (1 - Y_{n-1}) + \rho\frac{y_{n-1}}{2}, 1\right); for Y_n < \frac{1}{2} \\ mod\left(\mu Y_{n-1} * (1 - Y_{n-1}) + \rho\frac{(1 - y_{n-1})}{2}, 1\right); for Y_n \geq \frac{1}{2} \end{cases}$$ Cette carte se comporte de manière chaotique dans toute la région de (0.4] **Combined Logistic-Sine map (CLS)** $$Y_n = mod(\mu Y_{n-1} * (1 - Y_{n-1}) + \lambda \sin\frac{\pi Y_{n-1}}{4}, 1)$$ Les deux paramètres de contrôle font que le système se comporte de manière chaotique dans toute la région de (0,4].	Parallèle (Fusion) 
[110]	Combinaison des cartes Logistic sine System (LSS) $$u_{n+1} = LSS\ (r, u_n) = (ru_n(1 - u_n) + (4 - r)\sin\frac{\pi u_n}{4})\ mod 1$$ Où le paramètre r∈ (0,4]	Parallèle (Fusion) 

II.3.5. Les cryptosystèmes basés sur les cartes chaotiques

Dans cette partie nous allons détailler les algorithmes cryptographiques et les principes de conception basés sur le chaos .

les cryptosystèmes basés sur le chaos numérique (également appelés chiffrements chaotiques numériques), sont des processus récurrants qui présentent l'intérêt d'avoir une expression mathématique très simple, tout en conduisant aux régimes dynamiques variés offrent plusieurs avantages, tels que : un niveau de sécurité très élevé, une vitesse élevée en particulier dans les chiffrements de flux, une flexibilité et une modularité accrue, Ils sont plus faciles à mettre en œuvre et sont conçus et implémentées avec une précision de calcul finie pour le chiffrement.

Ces fonctionnalités les rendent plus adaptées au cryptage de données à grande échelle, telles que les images et les vidéos. En effet, avec une taille de bloc fixe, la norme de cryptage avancée (AES) n'est pas adaptée au cryptage vidéo sélectif et aux chiffrements de flux . Par exemple, dans le cryptage sélectif des applications vidéo en temps réel, nous devons attendre d'avoir 128 bits avant de démarrer le processus de cryptage. Ceci est un inconvénient pour la latence du système. Les résultats expérimentaux montrent que les algorithmes de chiffrement basés sur le chaos peuvent résoudre les problèmes de sécurité de manière efficace et adaptative[83].

Les cryptosystèmes chaotiques numériques utilisent un ou plusieurs systèmes chaotiques discrets (cartes chaotiques) directement pour assurer la sécurité plutôt que via une synchronisation chaotique comme dans les cryptosystèmes analogiques. Des processeurs numériques sont utilisés avec les cartes chaotiques mises en œuvre à l'aide d'une arithmétique à précision finie pour le chiffrement.

Généralement, différents algorithmes chiffrent différents volumes de données et obtiennent ainsi une sécurité et une efficacité différentes (temps de calcul). Dans le chiffrement direct, le contenu multimédia ou le contenu compressé est directement chiffré avec un nouveau chiffrement ou un chiffrement traditionnel. Dans le cryptage partiel, seules certaines parties importantes du contenu multimédia sont cryptées, tandis que les autres parties ne sont pas cryptées. Dans le chiffrement par compression conjointe, l'opération de chiffrement est combinée à une opération de compression et elles sont mises en œuvre simultanément. Naturellement, le cryptage direct crypte souvent les plus gros volumes de données et, par conséquent, il offre la sécurité la plus élevée et l'efficacité la plus faible. Le chiffrement partiel et le chiffrement par compression conjointe réduisent les volumes de données chiffrées et obtiennent ainsi une efficacité

supérieure et le niveau de sécurité nécessaire pour une application donnée. Dans le cryptage perceptif, le contenu multimédia est crypté sous le contrôle de la force de cryptage qui détermine la perceptibilité du contenu multimédia crypté. Un cas typique de cryptage perceptif est la prévisualisation multimédia sécurisée, dans laquelle le contenu multimédia est d'abord crypté avec une légère force de cryptage et décrypté après le paiement. En chiffrement scalable, le contenu multimédia scalable est chiffré couche par couche, de manière progressive, selon l'importance des couches. Il peut être utilisé dans le transcodage sécurisé des médias. Lorsque le contenu multimédia crypté est transmis d'Internet vers un mobile à bande passante limitée [83].

II.3.5.1. Confusion et diffusion utilisant le chaos

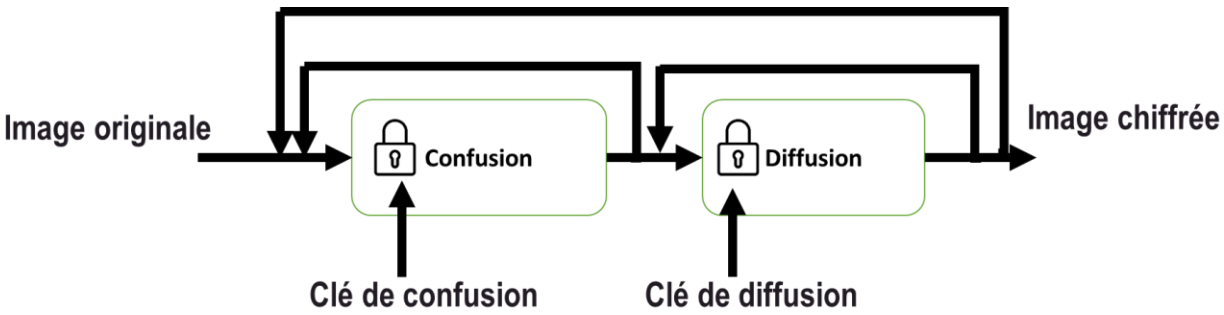


Figure II. 4 Le schéma de cryptage de Fridrich**[111].**

En 1997, un schéma de chiffrement basé sur le chaos a été introduit par Fridrich . C'est devenu la structure de base des cryptosystèmes chaotiques et il a été largement référencé depuis 1997. L'architecture générale d'un tel cryptosystème est illustrée à la Figure II.4.

Afin d'être robuste contre plusieurs types d'attaques, tout cryptosystème doit atteindre des niveaux élévés de confusion et de diffusion. Cela a été expliqué dans le célèbre article de « Shannon » la plupart des algorithmes de chiffrement appliquent cette architecture qui implique ces deux étapes: au cours du processus de cryptage. Généralement, les pixels de l'image sont considérés comme des éléments d'une matrice ,dans l'étape de confusion, une conception basée sur le chaos sera utilisée pour crypter en permutant les pixels de manière non prévisible. et une bonne diffusion qui implique la modification des valeurs de pixel de l'image. Ces deux étapes fournissent un support extrême à tout algorithme de chiffrement qui résiste aux attaques courantes.Au niveau du récepteur, l'image est récupérée en appliquant une diffusion et confusion inverse sur l'image chiffrée[111].

II.3.5.2. Générateurs chaotiques de nombres pseudo-aléatoires

les systèmes chaotiques sont des sources naturelles d'entropie qui peuvent être utilisées pour concevoir des PRNG. La plupart des systèmes générateurs de nombres pseudo-aléatoires basés sur le chaos, sont utilisés en cryptographie afin de brouiller les pixels de l'image par exemple, il s'agit d'extraire les bits pseudo-aléatoires à partir des orbites chaotiques .Ces nombres peuvent être générés à l'aide de virgule flottante (par exemple, double précision), puis une clé binaire est extraite à l'aide de la fonction de quantification. La principale différence entre nombres aléatoires et pseudo-aléatoires est que les nombres pseudo-aléatoires sont nécessairement périodiques alors que les nombres vraiment aléatoires ne le sont pas.

Les conditions initiales et les paramètres de contrôle jouent le rôle de la clé secrète, qui exploite le grand espace de paramètres offert par la forte sensibilité aux conditions initiales et le comportement aléatoire des signaux chaotiques résultants.

Il existe différentes méthodologies pour tirer parti du chaos pour concevoir des PRNG avec la combinaison de plusieurs cartes chaotiques différentes pour générer des nombres aléatoires capables de passer des suites de tests statistiques.Les auteurs dans [112] ont résumé la façon dont les cartes chaotiques sont utilisées pour générer des nombres pseudo-aléatoires et appliquer pour un cryptage multimédia.

II.3.5.3. Les chiffrements de flux utilisant le chaos

Les chiffrements de flux (stream encryption)sont basés sur la génération d'un flux de clé cryptographique infini et sont utilisés pour chiffrer un bit ou un octet à la fois. Les chiffrements de flux ont des besoins en mémoire relativement faibles. Cette section donne un bref aperçu des schémas de chiffrement de flux.

Les chiffrements de flux chiffrent les textes en clair dans des unités plus petites telles que des bits ou des octets. Les chiffrements de flux sont employés lorsque la longueur du texte en clair est inconnue ou lorsqu'une efficacité élevée est souhaitée. Généralement, les chiffrements de flux sont des générateurs de flux de clés pseudo-aléatoires, dans lesquels les flux de clés résultants subissent l'opération OU exclusif (XOR) avec des données. La plupart des chiffrements de flux basés sur le chaos utilisent la trajectoire chaotique de la carte pour calculer le flux de clé résultant.Dans [113] les auteurs ont donné un aperçu du chiffrement récent des flux basés sur des cartes chaotiques. Ils montrent également l'évaluation aléatoire des cartes chaotiques.

Les crypto systèmes basés sur le chaos., impliqués au niveau de la couche physique des systèmes de transmission sont principalement dédiés à la sécurité absolue de distribution des clés secrètes, dans laquelle

la clé peut ensuite être utilisée pour transmettre des informations en toute sécurité par l'algorithme de cryptage.

II.3.5.4. La cryptographie chaotique par Block S-Boxes

Les boîtes de substitution (S-box) sont des composants non linéaires importants dans le crypto système de blocs. La non linéarité joue un rôle important dans la sécurité des crypto systèmes. Les boîtes S sont utilisées pour augmenter la capacité de confusion du chiffrement. Construire des S-box avec une forte fonctionnalité cryptographique est une étape importante dans concevoir des systèmes de chiffrement par blocs. Cependant le S-box présente des données auto-corrélées élevées, dans le cas des médias numériques comme les images, les S-box montrent une mauvaise performance malgré une non-linéarité élevée. Ceci est dû à l'existence d'extrêmes corrélation entre les pixels voisins dans les images, ce qui rend le déchiffrement facile pour les attaquants du point de vue cryptanalytique. Un certain nombre de chercheurs ont proposé différentes méthodes pour la construction de S-box basées sur des cartes chaotiques, de nouveaux algorithmes de cryptage d'image qui fusionne les caractéristiques de systèmes chaotiques, et les S-boxes dynamiques afin de surmonter le problème de forte corrélation des pixels substitués de l'image.

Dans cet article [114] Une analyse de la littérature brute a montré que le nombre d'études liées aux conceptions de boîtes en S basées sur le chaos au cours de la dernière décennie est supérieur à 250. Par conséquent, on pense que les résultats de l'étude apporteront une perspective différente pour la littérature de cryptologie basée sur le chaos.

II.3.5.5. La cryptographie chaotique quantique

La cryptographie quantique est fondée non plus sur des notions mathématiques, mais sur l'hypothèse admise en physique que le comportement des photons (les particules élémentaires de lumière) est régi par les lois de la mécanique quantique. Cette théorie physique, élaborée dans la première moitié du xxe siècle, n'a jamais été mise en défaut et semble donc la meilleure base pour fonder une théorie physique ultime de l'information, et de la cryptographie.

La distribution de clefs grâce aux photons polarisés

Un photon, d'après les principes généraux de la mécanique quantique, se comporte comme une boîte à deux compartiments: à chaque fois qu'on ouvre l'un d'eux pour prendre connaissance de son contenu, le contenu de l'autre compartiment est irrémédiablement détruit (on ne peut donc connaître que le contenu de

l'un des deux compartiments). Pour faire parvenir une clef secrète à son partenaire, l'envoyeur utilise cette propriété. Détaillons la:

L'envoyeur range dans des « compartiments » tirés au hasard, des bits (des 0 et des 1), qui vont définir la clef qu'il veut partager avec le récepteur ;Il émet le flux de photons ainsi créé ; Son partenaire ouvre au hasard un compartiment de chaque photon reçu ;L'émetteur indique alors au récepteur, par un canal quelconque, dans quels compartiments des photons les bits secrets étaient rangés ;Chaque photon qui a été ouvert correctement par le récepteur (à peu près un sur deux), fournit un bit en commun aux deux partenaires. Tous ces bits sont alors utilisés comme clef secrète pour communiquer.

La sécurité du système provient du fait que les deux partenaires peuvent savoir avec certitude s'ils ont été espionnés. En effet, si un intrus a capté des photons et les a lus (c'est-à-dire a ouvert l'un de leurs compartiments) il n'a pu lire en moyenne qu'un bit sur deux, parmi ceux qui ont été envoyés par l'émetteur, et donc, cet intrus est dans l'impossibilité absolue de réémettre le même flux de photons que l'émetteur. Pour savoir si leur communication a été interceptée, les deux partenaires vérifient quelques bits qu'ils possèdent en commun. Si des erreurs apparaissent, ils savent qu'ils ont été espionnés et, bien sûr, dans un tel cas, ils n'utilisent pas la clef qu'ils partagent. Aujourd'hui, les fibres optiques existantes permettent d'utiliser cette méthode sur des distances de quelques dizaines de kilomètres.[115]

La cryptographie quantique, qui repose sur la transmission de clés générés aléatoirement, assure l'inviolabilité des échanges en toutes circonstances. Ces clefs quantique (QKD) générées à partir d'états quantiques, qui sont ensuite utilisées dans des protocoles de chiffrement ,le premier protocole étant mis en place est le BB84 en 1984 par les deux chercheurs Bennett et Brassard. Il est impossible de cloner une information quantique sans qu'elle soit détruite, ou de mesurer un état quantique sans le modifier, la lecture de l'information par un intrus serait immédiatement détectée par les destinataires du message.

Mélanger la clé quantique avec le signal chaotique rendra la sécurité ultime du système.Les auteurs dans [116] presentent une amélioration de la sécurité de la cryptographie quantique en utilisant une technique de tampon unique et un signal chaotique généré par un laser à semi-conducteur avec une rétroaction optique .

II.3.5.6. La cryptographie chaotique visuelle

La cryptographie visuelle a été inventée en 1994 par Moni Naor et Adi Shamir. Elle permet de communiquerdes messages secrets à travers des images et utilise les caractéristiques de la vision humaine pour décrypter les informations cryptées sans utiliser de calcul cryptographique complexe.

La cryptographie visuelle (CV) ou bien le partage de secret visuel est une technique basé sur le partage de la donnée confidentielle en même temps entre un certain nombre de personnes.Elle est basée sur le concept de schéma à seuil (k,n) ou threshold (k,n). Le principe de la CV consiste à garder la donnée dans une image et la diviser en « n » images aléatoires appelées pièces (shares), ombres (shadows) ou bien transparents (transparencies) de telle sorte qu'aucun transparent ne révèle des informations secrètes.Le secret est révélé si est seulement si un nombre $k(2 \leq k \leq n)$ de transparents ou plus sont superposés l'un sur l'autre (opération de décryptage). Le processus de décryptage s'effectue par le système visuel humain .

Plusieurs cobinaisons ont été proposées dans la litterature entre la technique de cryptographie visuelle et la steganographie ou le watermarking[117].

La cryptographie visuelle est une technique cryptographique qui permet de crypter des informations visuelles de manière à ce que le décryptage puisse être effectué par le système visuel humain, sans aucun calcul cryptographique. La cryptographie visuelle dynamique est une méthode alternative de masquage d'image qui n'est pas basée sur la superposition statique des partages, Le procédé ne génère qu'une seule image, et l'image secrète ne peut être interprétée par le système visuel humain que lorsque l'image codée d'origine oscille de manière harmonique dans une direction prédéfinie à une amplitude d'oscillation strictement définie. La faisabilité de la cryptographie visuelle dynamique chaotique est l'un des principaux sujets de la thèse [118], les relations théoriques et les expériences informatiques sont dérivées et discutées en détail. L'invention concerne également un schéma de cryptographie visuelle dynamique basé sur les déformations de l'image de couverture et des schémas de cryptographie visuelle dynamique améliorés avec une sécurité améliorée.

II.3.5.7.La cryptographie chaotique utilisant l'ADN:

La cryptographie ADN est un autre système de pointe en matière de sécurité. ADN signifie Acide désoxyribonucléique. L'ADN représente le plan génétique des créatures vivantes qui contient des instructions pour l'assemblage des cellules. Pour le corps humain, chaque cellule a un ensemble complet de ADN qui est unique pour chaque individu. La cryptographie de l'ADN est un sujet d'étude sur la façon d'utiliser l'ADN comme support d'information et il utilise la biotechnologie comme mesure de transfert de texte clair en texte chiffré. Les données de message en clair chiffrées dans des brins binaires d'ADN en utilisant un alphabet de courtes séquences d'oligonucléotides. Les brins binaires d'ADN soutiennent la faisabilité et l'applicabilité de la cryptographie basée sur l'ADN. Les principales difficultés de la

cryptographie de l'ADN sont l'exigence de technologies biomoléculaires de haut niveau, laboratoire et complexité de calcul. L'auteur de [119] a proposé une approche dynamique basée sur un crypto système chaotique caméléon et les propriétés de chiffrement basé sur l'ADN .

II.4. Les techniques de sécurité basées sur la dissimulation d'informations utilisant le chaos

II.4.1. Définition de la stéganographie

La stéganographie est l'une des nombreuses techniques de dissimulation de données Stéganô du grec « καλύπτουν » signifiant « je couvre » et Graphô du grec « γράφω » signifiant « j'écris » donc « Je couvre ce que j'écris », ce qui consiste à couvrir un message m par un objet de couverture de sorte que le message m reste introuvable. Contrairement à la cryptographie, le but de la stéganographie est de dissimuler l'existence de l'information d'en cacher l'existence même plutôt que de brouiller son contenu.

La théorie de l'information pour la stéganographie a été bien établie en 1998 par Christian Cachin [120] On peut définir cette formule simple : **Couverture(médium) + message-embarqué = stégo-message**

En stéganographie le message secret à cacher en anglais est appelé « secret message » au sein d'un objet de couverture appelé « cover-object » ou medium le résultat donnera un « stego-object ». La définition donnée par Simmons en 1983, est la transmission d'un message au moyen d'un médium avec une tout autre apparence.

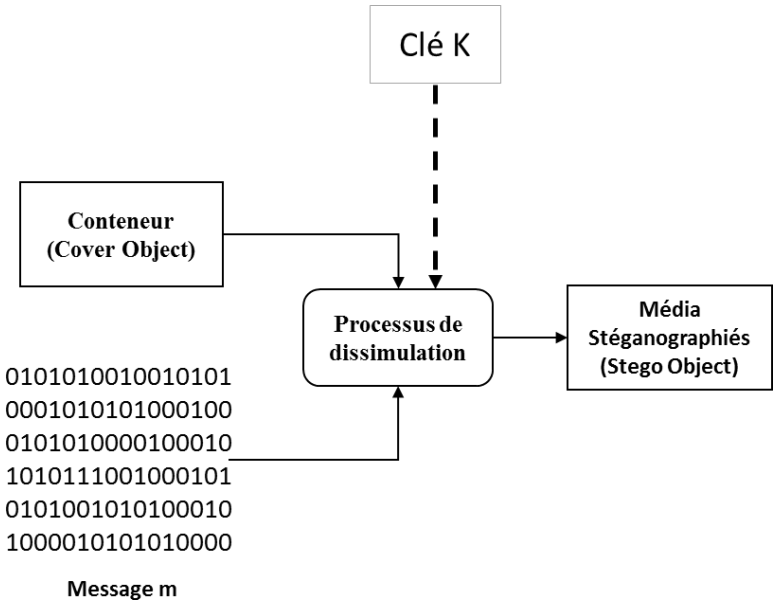


Figure II. 5 Schéma de principe de la stéganographie

Pendant des milliers d'années, différents supports de couverture ont été utilisés tels que la tablette en couches de cire, les cheveux et la peau humaine (Grèce), la technique linguistique tel que l'acrostiche qui est utilisée pour cacher le message dans un texte de couverture (Grande bretagne) les romains utilisaient l'encre invisible, un œuf dur en (Italie). Un scientifique allemand, Gaspart Schott (1608-1666) explique dans son livre « Schola Steganographica » comment dissimuler des messages en utilisant des notes de musique.

II.4.2. Les techniques de la stéganographie moderne

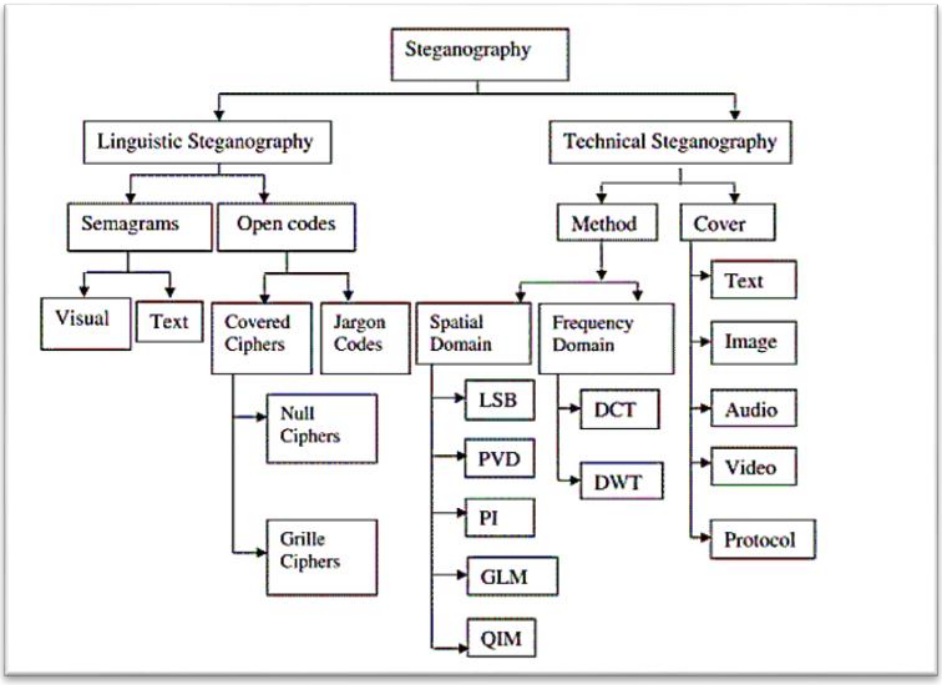


Figure II. 6 Classification des techniques en stéganographie[121].

La stéganographie moderne consiste à utiliser du multimédia numérique comme couverture tel que l'audio, la vidéo et protocole pour transmettre un message secret de façon indétectable

Les techniques de la stéganographie moderne sont classées en deux branches :la stéganographie linguistique et stéganographie techniques dans[121] en examinant les contributions dans chaque catégorie.

1) **Les méthodes techniques**

Les méthodes techniques sont classées en fonction du processus d'extraction qui nécessitent à la fois l'information originale et celle chiffrée afin d'extraire les données embarquées, les schémas dit

aveugles (blind or oblivious en anglais) peuvent récupérer le message caché au moyen uniquement des données chiffrées.[122]

Les méthodes de stéganographie techniques intègrent aussi les méthodes qui sont basées sur le domaine fréquentiel et spatial

- **Domaine fréquentiel**

  Les bits secrets sont cachés sous les coefficients de fréquence des sous-bande après une transformées DWT de l'image en Low-Low, Low-High, High-Low, High-High sous-bandes qui donne les détails des coefficients de l'image, les trois dernières sous-bandes de fréquence sont utilisées pour le masquage des données car dans la sous-bande Low-Low les coefficients sont similaires à l'image d'origine, en utilisant la transformée en ondelettes entières (IWT) : le processus de travail est similaire au DWT. Les données secrètes sont cachées dans les coefficients de l'IWT à l'aide d'une clé secrète. Pour un masquage de données sans perte, IWT est le meilleur choix par rapport à la méthode DWT.

  Le processus d'intégration et de décodage est plus compliqué dans le domaine de transformation plutôt que les techniques qui sont utilisées dans le domaine temporel. Cela améliorera la sécurité du système. Un autre avantage est que la plupart des techniques du domaine fréquentiel sont moins affectées par les attaques de compression, de recadrage, de mise à l'échelle et de rotation. Ainsi, les systèmes basés sur la transformée sont plus efficaces pour préserver la qualité de l'image stégo et la rendent moins détectable dans un canal non sécurisé.

- **La stéganographie spatiale**.

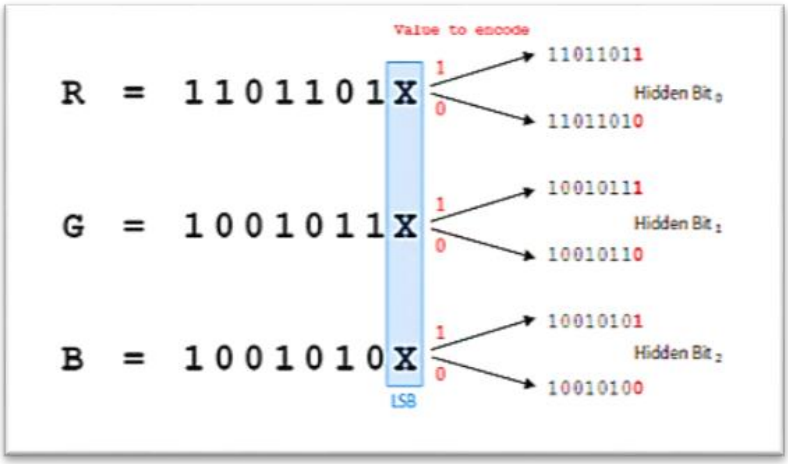


Figure II. 7 Exemple de conversion LSB**[123].**

La technique LSB est l'une des techniques la plus utilisées car l'œil humain ne perçoit pas les variations de la valeur du LSB (Bit de poids faible).

Elle consiste en l'insertion des bits de codage du message secret à la place des bits de poids faible du codage des pixels de l'image de couverture, de sorte que les distorsions apportées par le processus d'insertion restent non perceptibles

Aujourd'hui, lors de la conversion d'une image analogique au format numérique, nous avons généralement le choix entre trois méthodes différentes de représenter les couleurs :

- Chaque pixel est codé sur 3 octets =24 bits : chaque pixel peut avoir une couleur parmi 2^{24} couleurs, et celles-ci sont représentées par des quantités différentes de trois couleurs de base : rouge (R), vert (G), bleu (B), codé sur 8 bits (256 valeurs) chacune c'est à dire : le rouge de 0 à 255, le vert de 0 à 255, le Bleu de 0 à 255.
- Couleur (pixel)codé sur 8 bits : chaque pixel peut avoir une couleur parmi $256 = 2^8$, choisie dans une palette de couleurs.
- Échelle de gris –(pixel)8 bits : chaque pixel peut avoir une des $256 = 2^8$ nuances de gris.

  L'insertion LSB modifie

  Les LSB de chaque couleur dans les images 24 bits, ou bien

  Les LSB de la valeur 8 bits pour images.8 bits

  Exemple : La lettre 'A' a un code ASCII de 65 (décimal), qui est **1000001** en binaire. Il faudra trois pixels consécutifs pour qu'une image 24 bits stocke un 'A' [122]:

  Disons que les pixels avant l'insertion sont :

  10000000.10100100.10110101, 10110101.11110011.10110111, 11100111.10110011.00110011

  Alors leurs valeurs après l'insertion d'un 'A' seront :

  *1000000**1**.10100100.1011010**0**, 1011010**0**.1111001**0**.1011011**0**, 1110011**0**.10110011.00110011*

- **La stéganographie adaptative** la nature adaptative est introduite dans les schémas d'intégration de données de plusieurs manières : dans la sélection les pixels cibles dans l'image de couverture, en utilisant le système visuel humain (HVS), Apprentissage automatique et intelligence artificielle.

II.4.3. Le filigrane ou le tatouage numérique (Digital Watermarking)

Le tatouage numérique est la technique d'intégration d'informations dans un contenu multimédia en modifiant légèrement son contenu. Le tatouage est considéré dans certain cas comme une forme de signature numérique, où l'on ajoute une information appelée marque à l'information initiale.

Le tatouage de l'image numérique est l'art de cacher la marque secrète dans les données d'origine. Les données d'origine sont visibles par tous, alors que les marques (données cachées) ne sont visibles et modifiables que par des utilisateurs autorisés.

Plusieurs applications peuvent utiliser le filigrane ou le tatouage numérique visible, nommé d'après les filigranes que nous avons l'habitude de voir sur les factures ou les mentions légales des documents ou dans les billets de banque ou passeports pour la protection contre les copies par exemple , dans certains cas le but est d'évaluer l'authenticité et l'intégrité du signal hôte ou pour vérifier l'authenticité du propriétaire, protéger les droits d'auteurs ou la traçabilité (fingerprinting en anglais).

II.4.4. La différence entre la stéganographie et le tatouage d'une image

1) En stéganographie, le message caché doit être invisible, tandis qu'en tatouage, il peut être visible ou invisible. Dans le premier cas, une information est introduite dans une autre information afin de la cacher, c'est le principe même de la technique, alors que dans le second cas, l'information introduite n'est pas forcement cachée, elle peut très bien être perceptible, à l'exemple des logos visibles sur des images.
2) En stéganographie, Le message doit être caché de telle manière qu'il ne puisse pas être détecté par des utilisateurs non-autorisés, tandis qu'en tatouage le message caché doit être dissimulé pour qu'il ne soit pas supprimé ou remplacé par des personnes non-autorisées
3) Une attaque dans le cadre de la stéganographie portera sur la détection de l'information potentiellement cachée, alors qu'une attaque dans les cas du tatouage portera sur la suppression de la marque même.

II.4.5. Complémentarité de la stéganographie et de la cryptographie

La cryptographie et la stéganographie ont des objectifs complémentaires et peuvent être utilisées ensemble, Cette approche est communément connue sous le nom de cryptographie métamorphique ou fusion, la stéganographie dissimule l'existence d'un message secret tandis que la cryptographie modifie le format du message (brouille les données secrètes sous une forme), pour prendre une métaphore, la

cryptographie consisterait à enfermer l'information dans un coffre-fort avec une clé, la stéganographie consisterait à cacher le coffre-fort derrière un tableau ;cela dit rien n'empêche de combiner les deux techniques.

Dans [124], les auteurs ont passé en revue plusieurs façons de combiner stéganographie et techniques cryptographiques pour réaliser un système hybride. Dans l'article [125] les auteurs ont tenté de discuter de la méthodologie utilisée par les algorithmes cryptographiques et stéganographiques ainsi que la combinaison des deux, une analyse de la force et la limitation de divers algorithmes proposés a été faite selon les affirmations des auteurs respectifs dans leurs travaux de recherche.

II.5. Analyse de sécurité et évaluation d'un Crypto système

L'analyse de sécurité est la spécialité qui cherche à découvrir la faille d'un crypto système et de récupérer tout ou partie d'un message chiffré (ici nous considérons une image) ou de découvrir la clé de déchiffrement ou l'algorithme. Il existe de nombreuses méthodes pour analyser, en fonction de l'accès de l'expert au texte en clair, au contenu chiffré ou aux différentes parties du crypto système. Voici probablement les types d'attaques les plus largement reconnues contre les images cryptées.

La relation entre l'image originale et cryptée peut être déterminée en analysant statistiquement les données, l'image après cryptage doit être totalement différenciée de l'original, à cause de l'hypothèse de « Shannon ». Il existe quelques approches pour déterminer si l'image chiffrée libère des données sur l'originale ou non.

De nombreux paramètres doivent être pris en compte dans la conception d'un nouvel algorithme de chiffrement adapté aux applications des multimédias, comme présenté ci-dessous :

II.5.1. Analyse de l'espace clé

La longueur de la clé est un paramètre important pour les techniques de sécurité. Cette longueur diffère d'un système à l'autre. L'augmentation de la longueur de la clé offre une plus grande sécurité, garantissant que le destinataire est la seule capable de reconstruire l'image d'origine. La longueur de la clé est généralement mesurée en bits en raison du système binaire. L'utilisation d'un autre système de numérotation peut augmenter le facteur de travail dans le pire des cas de manière linéaire, alors qu'il augmente de manière exponentielle en ajoutant un nouveau chiffre, comme indiqué dans l'équation suivante : longueur de clé $=x^k$où x est la base qui dépend du système de numérotation et k est l'exposant qui dépend du nombre de

positions possibles. Bien qu'une clé puisse rester longtemps inconnue, il est préférable de la mettre à jour régulièrement : aucune clé ne doit être utilisée pendant une période infinie. Plus une clé est utilisée longtemps, plus elle risque d'être compromise.

Essayez de découvrir la clé de déchiffrement en vérifiant toutes les clés imaginables. La quantité de tentatives de découverte indique spécifiquement que l'espace de clé du crypto système devient exponentiel avec la taille de la clé agrégée. Cela implique que la multiplication de la taille de la clé pour un algorithme ne fait pas que doubler le nombre d'opérations obligatoires, mais les met au carré. Un algorithme de cryptage avec une taille de clé de 128 bits caractérise un espace de clés de 2128.

• **Gestion des clés** : les cryptanalystes attaquent les algorithmes de chiffrement via leur gestion des clés. Il est plus facile de casser un algorithme de chiffrement en obtenant la clé lorsqu'une procédure de stockage et de sauvegarde/récupération de clé bâclée est utilisée. La gestion des clés comprend la génération, le transfert et la mise à jour des clés. La création de clés est la première étape de la gestion des clés qui est responsable de la production de clés fortes. Générer des clés faibles signifie que tout le système est faible. Le système devient sensible à la force brute attaque dans laquelle des millions de clés par seconde sont testées. La génération de bonnes clés est obtenue par un processus aléatoire, par exemple à l'aide d'un générateur pseudo-aléatoire. Le processus de production de clés devient plus difficile s'il existe une relation mathématique entre les clés de chiffrement/déchiffrement. Une clé de chiffrement

II.5.2. Analyse de sensibilité de la clé

Un algorithme protégé devrait présenter une sensibilité de clé élevée, ce qui implique que l'image cryptée ne peut pas être déchiffrée par quelques changements dans la clé. La sensibilité de la clé est définie comme les modifications de l'information chiffrée causée par les modifications de la clé, une légère différence dans les clés devrait entraîner de grandes modifications dans l'information chiffrée. La définition mathématique [126] est donnée par les équations suivantes avec K_0 et K_1 les deux clés de chiffrement.

$$\begin{cases} KS = \frac{Dif(C_0,C_1)}{n} x100\% \\ Dif(C_0,C_1) = \sum_{i=0}^{n-} C_{0,i} \oplus C_{1,j} \\ C_0 = E(P,K_0) \\ C_1 = E(P,K_1) \\ Dif(K_0,K_1) = \frac{1}{n} \\ P = P_0, \quad \dots\dots \quad P_{n-1} \qquad image\ d'origine \\ C_0 = C_{0.0}, \dots\dots C_{0,n-1} \qquad image\ cryptée\ avec\ la\ clé\ K_0 \\ C_1 = C_{1,0}, \dots\dots\dots C_{n-1} \qquad image\ cryptée\ avec\ la\ cle\ K_1 \\ K_0 = K_{0,0}, \dots\dots K_{0,n-1} \\ K_1 = K_{1,0}, \dots\dots K_{1,n-1} \end{cases} \quad (II.15)$$

II.5.3. Temps d'exécution

Le temps de traitement est le temps nécessaire pour chiffrer et déchiffrer une image. Plus la valeur du temps de traitement est faible, meilleure sera l'efficacité du cryptage.

Le temps d'exécution d'un chiffrement est un facteur important dans de nombreuses applications. En général, la comparaison entre la vitesse d'exécution d'algorithme de chiffrement proposé et ceux existant dans la littérature est effectuée sur la base des caractéristiques de la CPU, la taille de la mémoire, le système d'exploitation, le langage de programmation, la taille de l'image et en particulier les techniques de chiffrement.

II.5.4. Analyse d'histogramme

Un histogramme utilise un graphique à barres pour profiler l'occurrence de chaque niveau de gris de l'image. L'axe horizontal représente la valeur de niveau de gris. Il commence à zéro et va au nombre de niveaux de gris. Chaque barre verticale représente le nombre d'occurrences du niveau de gris correspondant dans l'image

Pour qu'un algorithme de chiffrement soit robuste, l'histogramme de l'image chiffrée doit avoir deux propriétés :

1) L'histogramme doit être totalement différent de l'image d'origine
2) L'histogramme doit être uniformément distribuée ce qui veut dire que la probabilité de présence de n'importe quel niveau de gris est la même [127].

L'une des attaques de crypto système les plus courantes est celle basée sur une analyse statistique. Un crypto système est considéré comme fort contre ces attaques, si l'histogramme d'image crypté est

uniformément distribué. Le test visuel est nécessaire, mais il n'est pas suffisant. Pour assurer l'uniformité de l'image, le test « chi-square test » est appliqué pour confirmer statistiquement l'uniformité de l'histogramme :

$$\times^2_{exp} = \sum_{i=0}^{Q-1} \frac{(o_i - e_i)^2}{e_i} \qquad \text{(II. 16)}$$

Dans l'équation (2.11), Q est le nombre de niveaux (Q = 256), o_i est la fréquence d'occurrence observée de chaque niveau de couleur (0-255) sur l'histogramme de l'image chiffrée, et $e_i$est la fréquence d'occurrence attendue de la distribution uniforme, donnée ici par $e_i = LxCxQ$. Pour un crypto système sécurisé, la valeur expérimentale du chi-square doit être inférieure à la valeur théorique du chi-square one.

II.5.5. Analyse de corrélation

L'analyse de corrélation est également l'une des attaques statistiques utilisées par la cryptanalyse du crypto système. Il ne doit donner aucune information sur la clé secrète utilisée ni aucune information partielle sur l'image brute d'origine. Cela signifie que l'image cryptée doit être très différente de sa version originale. L'analyse de corrélation est l'une des méthodes régulières et standard pour mesurer cette propriété. En effet, il est bien connu que les pixels adjacents dans les images simples sont très redondants et corrélés. Ainsi, dans les images cryptées, les pixels adjacents doivent avoir une redondance et une corrélation aussi faible que possible. Pour tester la sécurité de tout nouvel algorithme, vis-à-vis de ce type d'attaques, on sélectionne d'abord N paires de pixels adjacents dans les directions horizontales verticales et diagonales à partir de l'image simple et de sa version chiffrée. Ensuite, les équations mathématiques suivantes sont utilisées pour calculer le coefficient de corrélation

$$\rho_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad \text{(II. 17)}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}([x_i - E(x)][y_i - E(y)]) \qquad \text{(II. 18)}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \qquad \text{(II. 19)}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i) \quad \text{(II. 20)}$$

Dans les équations ci-dessus, xi et yi sont les valeurs des deux pixels adjacents dans l'image simple ou l'image chiffrée correspondante.

II.5.6. L'entropie

Les valeurs des pixels de l'image vont de 0 à 255. Dans un algorithme de chiffrement robuste, la probabilité d'occurrence de n'importe quel pixel doit être la même (ou presque). Le comportement aléatoire du message chiffré peut être évalué à l'aide des informations d'entropie définies par :

$$H(C) = \sum_{i=0}^{Q-1} Pro(c_i)x\ log_2 \frac{1}{Prod(c_i)} \quad \text{(II. 20)}$$

Où H(C) est l'entropie de l'image chiffrée C, Pro(ci) est le nombre d'occurrences de chaque niveau (i = 0 ; 1 ; 2 :255). En cas de niveaux de probabilité égaux $Pro(c_i) = 2^{-8}$, l'entropie de l'information est maximale

$$H(c) = \sum_{i=0}^{256-1} pro(c_i)x \log_2 \frac{1}{pro(c_i)} = 8 \quad \text{(II. 21)}$$

Selon l'équation dans [128].

II 5.7. Tests UACI/NPCR

Le taux changement du nombre de pixels (NPCR) et la moyenne unifiée de l'intensité modifiée (UACI) sont les deux quantités les plus couramment utilisées pour évaluer la force des algorithmes de chiffrement et de déchiffrement d'image par rapport aux attaques différentielles. Classiquement, un score NPCR/UACI élevé est généralement interprété comme une résistance élevée aux attaques différentielles.

Dans le cas de la cryptanalyse des images, deux images sont prises pour le test, la deuxième est la même que la première avec une modification d'un pixel spécifique. Une image cryptée est très sensible aux modifications mineures et même la modification d'un seul bit dans l'image d'origine entraînera une image cryptée très différente. Le facteur NPCR mesure le taux de changement du nombre de pixels dans l'image cryptée avec seulement 1 bit changé dans l'image simple. Ce paramètre est calculé par l'équation (II.22) et pour un algorithme de chiffrement idéal, il est considéré comme 1.

Pour deux Images, C1 et C2, dont les images originales correspondantes n'ont qu'une différence d'un pixel. Nous définissons un tableau bidimensionnel D, ayant la même taille que l'images C1/C2, le $D(i,j)$est déterminé à partir de $C_1(i,j)$ et $C_2(i,j)$.

Si $C_1(i,j) = C_2(i,j)$,alors le $D(i,j) = 1$.

Si $C_1(i,j) \neq C_2(i,j)$ le $D(i,j)$ =0.

Le NPCR est défini par l'équation suivante :

$$NPCR = \frac{\sum_{ij} D(i,j)}{wh} x100\% \quad \text{(II. 22)}$$

$$UACI: U(C_1, C_2) = \sum_{i,j} \frac{|C_1 - C_2|}{F.T} \text{ x } 100\% \quad \text{(II. 23)}$$

Où le symbole T désigne le nombre total de pixels dans le texte chiffré, le symbole F désigne la plus grande valeur de pixel prise en charge compatible avec le format d'image chiffré et désigne la fonction de valeur absolue.

Il est clair que le NPCR se concentre sur le nombre absolu de pixels qui change de valeur dans les attaques différentielles, tandis que l'UACI se concentre sur la différence moyenne entre deux images chiffrées appariées. L'intervalle pour les valeurs UACI at NPCR est [0, 1] [129]

III.1. Processus de mixage en cascade pour la carte CSCP

Dans ce chapitre, nous proposons les nouvelles cartes développées couplée en cascade à base de des cartes chaotique standards.

III.1.1. La carte Sinusoïdale

La carte sinusoïdale considérée est l'application unidimensionnelle non linéaire

S : $\mathbb{R} \rightarrow \mathbb{R}$ définie par :

$$S(x) = r \sin(\pi x) \qquad (III.1)$$

La forme itérative est comme suit :

$$x_{n+1} = r \sin(\pi x_n) \qquad (III.2)$$

Où r est entre 0 and 1, x_n est l'entrée/sortie itérative dans l'intervalle [0, 1]

.

Quand r ∈ [0.867, 1], La carte sinusoïdale à un comportement chaotique, elle montre de meilleure comportement chaotique l'lorsque le paramètre r est proche de "1". Figure. III.1.b

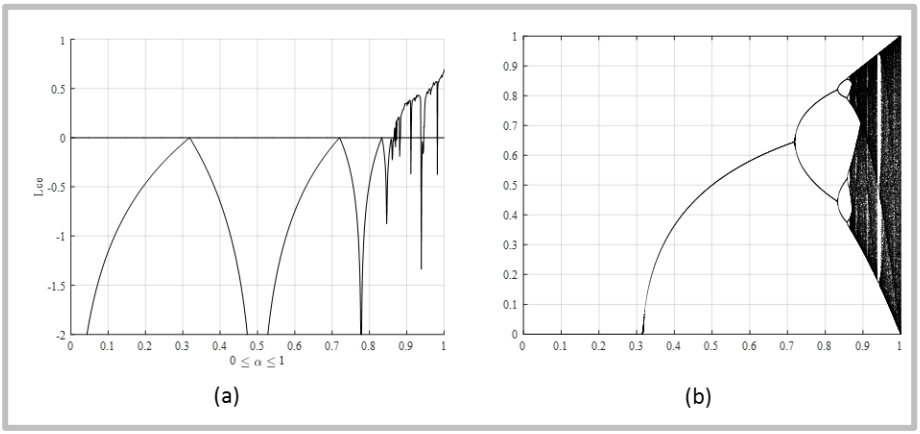


Figure III. 1 La dynamique de la carte sinus (a) Exposant de Lyapunov (b) diagramme de bifurcation

III.1.2. La carte paramétrique Cubique développée

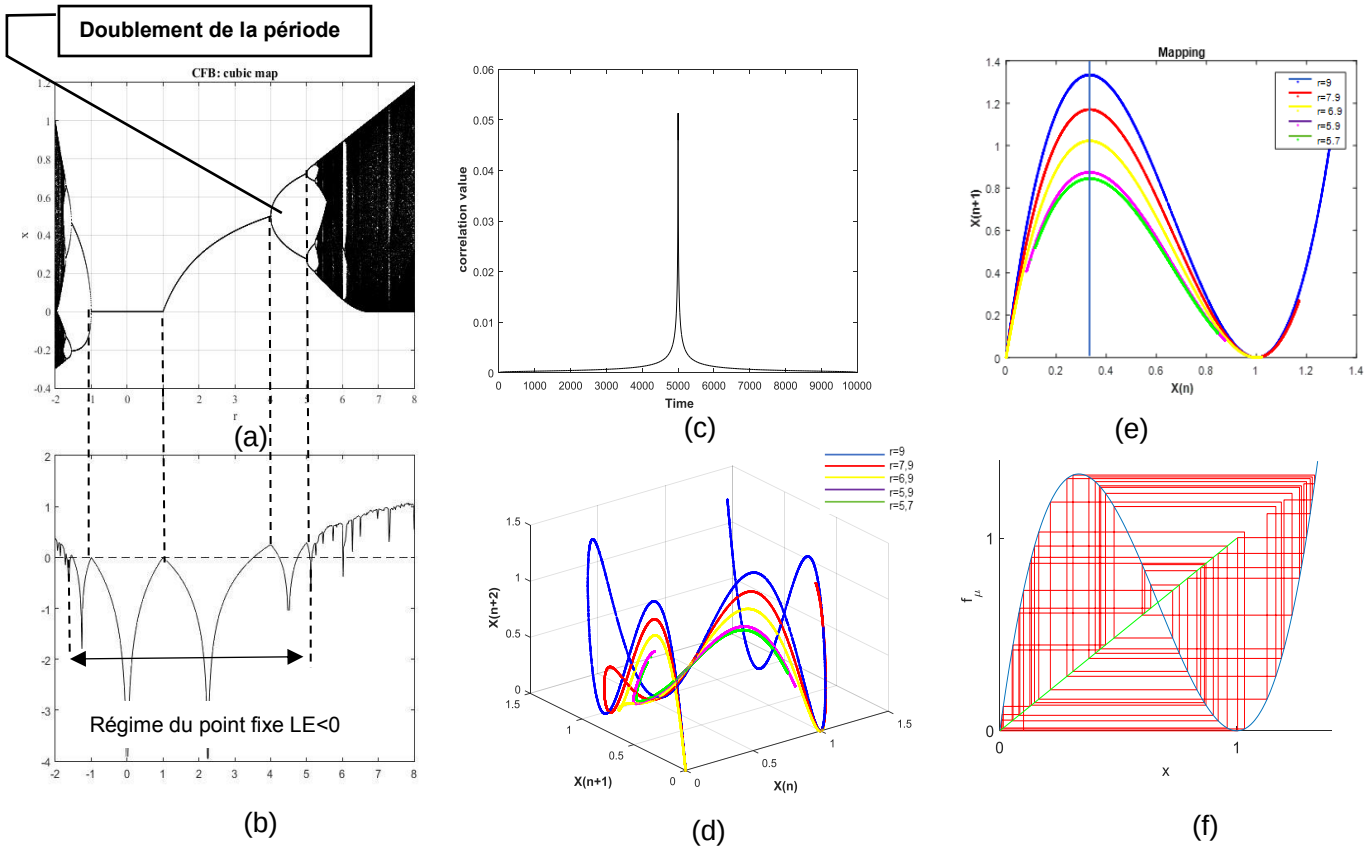


Figure III. 2 Analyse dynamique de la carte développée(a) Bifurcation (b) Exposant de Lyapunov

(c) Autocorrélation de la carte Cubique (α, β) = (1,1), r=6,9, x_0 =0.5.

(d) trajectoire dans l'espace de phase pour r =9, 7.9, 6.9, 5.9, 5.7

(e) itérations graphique (Cob web plot)

(f) Courbes de $f(x_x) = rx_{n-1}(1-x_{n-1})^2$ pour r =9, 7.9, 6.9, 5.9, 5.7

Dans notre étude, nous avons proposé une carte nommée carte « CSCP » avec une structure comportant deux cartes, la carte sinusoïdale traditionnelle combinée en cascade avec une nouvelle carte cubique, dans le but de crée une dynamique chaotique plus complexe, elle montre des propriétés aléatoires, robustes et un comportement chaotique plus complexe, la forme itérative de la carte proposée est la suivante :

La carte cubique considérée est unidimensionnelle non linéaire

F : $\mathbb{R} \rightarrow \mathbb{R}$ définie par :

$$x_{n+1} = rx_n^k(\alpha - \beta x_n)^m \qquad (III.3)$$

Où k, m ∈ R et r ∈ R− {0} puisque le cas r = 0 est trivial.

- Les cas particuliers avec (k, m) = (0, 1) ou (1, 0) donnent la carte « Tent ».

- Pour (k, m) = (1, 1) donne la carte logistique, des cartes qui sont largement exploitées dans les cryptos systèmes.
- Pour (k, m) = (1,2) nous obtenons la nouvelle carte nommée « Cubique »

La carte paramétrique « Cubique » proposée est non-linéaire unidimensionnelle F : $\mathbb{R} \rightarrow \mathbb{R}$ définie par :

$$\begin{cases} C(x) = rx(\alpha - \beta x)^2 \\ Si\ -1 \leq\ x\ \leq 0\ alors\ f(x) \leq\ 0. \\ Si\ 0\ \leq\ x\ \leq\ 1\ alors\ f(x) \geq\ 0. \end{cases} \quad (III.4)$$

Où « α » et « β » sont les paramètres de contrôle.

III.1.2.1. Etude dynamique de la nouvelle carte cubique développée

1) **Diagramme de bifurcation**

Dans ce qui suit nous allons montrer la carte cubique pour différentes valeurs des paramètres r (en gardant α, β=1 fixe). Les points de maximum et de minimum sont :

$\sqrt{\frac{\alpha^2}{\beta^2-2\beta}}$ Et $-\sqrt{\frac{\alpha^2}{\beta^2-2\beta}}$ respectivement quand 0>β>2.

Nous nous concentrons sur la dynamique de la carte cubique puis analysons les points fixes.

Les points fixes de $f(x)$ sont donnés par :

$f(x) = x$ la solution de l'équation nous : 0, 1/β(α-1/$\sqrt{r}$)

Nous avons,

$df/dx = r(\alpha - \beta x)^2 - 2\beta r x(\alpha - \beta x)$

$\therefore \frac{df}{dx}\Big|_{x=0} = r\alpha^2$

Pour 0<r<1 :

Ainsi, le point fixe x=0 est un point attractif (stable), on l'appelle un puits (nœud)

Pour -1<r<0, le point fixe x=0 est nommée source.

$\therefore \frac{df}{dx}\Big|_{1/\beta(\alpha-1/\sqrt{r})} = 3r + 2\alpha\sqrt{r}$

Donc, les points fixes x=1/β(α∓1/$\sqrt{r}$)sont tous les deux stables pour 1<r<4.

Pour r qui se situe entre 5 et 8 où de nombreuses bifurcations se sont produites présentent des transitions vers le chaos à travers, le doublement de la période, le changement des paramètres double la période d'orbite du système, et le système perdra progressivement le comportement périodique et entrera dans le chaos.

Nous concluant que pour α=1 & β=1.

1. Le cas pour r∈ [1.1, 4] La trajectoire de l'équation converge vers un point fixe

$x^* = 1/\beta(\alpha \mp 1/\sqrt{r})$ Comme illustré dans la Figure III.2.a.

2. Le cas pour r ∈ [4.1, 5] On obtient le phénomène du dédoublement de la période et bifurcation illustré dans la Figure III.2.a.

3. Le cas pour r∈ [5.1, 8] On obtient un comportement chaotique comme illustré dans la Figure III.2.a.

2) Autocorrélation

L'autocorrélation fait référence à la corrélation d'une série chronologique avec ses propres valeurs passées et futures ; en d'autres termes, l'autocorrélation est définie comme la représentation mathématique du degré de similitude entre une série chronologique donnée et une version décalée d'elle-même sur des intervalles de temps successifs. C'est la même chose que de calculer la corrélation entre deux séries temporelles différentes (corrélation croisée), sauf que la même série temporelle est utilisée deux fois - une fois dans sa forme originale et une fois décalée d'une ou plusieurs périodes ; c'est aussi un outil mathématique pour détecter des caractéristiques répétitives dans un signal, tels que des caractéristiques périodiques qui sont obscurcies par le bruit.

La forme d'une bonne fonction d'autocorrélation devrait ressembler à une aiguille pointue, comme le montre la Figure III.2 c. le graphe d'autocorrélation a un pic principal net et exceptionnel, et n'a pas de lobe latéral exceptionnel. Vous pouvez noter que la corrélation ne capture que les dépendances linéaires. Vous pouvez avoir des variables aléatoires qui sont fortement dépendantes mais qui ont une très faible corrélation et la plupart des signaux chaotiques de faible dimension auront de nombreux pics d'autocorrélation puisqu'il ne s'agit que d'oscillateurs non linéaires.

La fonction d'autocorrélation de notre carte proposée réalisée par MATLAB montre que les signaux générés ont un comportement chaotique.

3) L'exposant de Lyapunov

Quand r ∈ [5.5, 8], La carte cubique à un comportement chaotique, elle montre de meilleure comportement chaotique l'lorsque le paramètre r est proche de "8". Figure III.2 a.

III.1.3. La Carte paramétrique “CSCP” en cascade développée

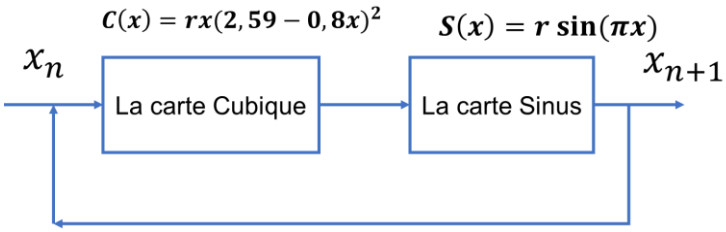


Figure III. 3 La structure en cascade de la carte CSCP

$$x_{n+1} = S(C(x_n)) \quad \text{(III. 5)}$$

S : est la fonction sinusoïdale

C : est la fonction cubique

La forme itérative de la carte CSCP proposée est :

$$x_{n+1} = \text{a } (\sin(\pi r x_n(\alpha - \beta x_n)^2)^p, p = 1 \quad \text{(III. 6)}$$

III.1.3.1. Etude dynamique de la nouvelle carte CSCP développée

1) Diagramme de bifurcation

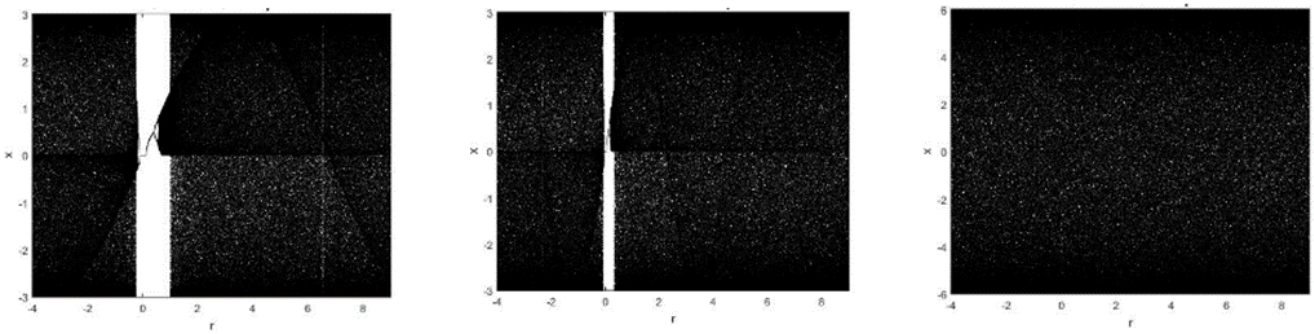


Figure III. 4 La dynamique de la carte CSCP (a) Graphe de bifurcation pour la carte en cascade Cubique-Sinus paramétriques avec les valeurs optimales a = 3 ; α = 10 :36 ; β= 3 :2.

La Figure III.4 présente Le diagramme de bifurcation de la nouvelle carte qui présente une dynamique qui couvre tout l’intervalle de [-4, 9].

2) Autocorrelation

La Figure III.4.b Présente l'Auto-corrélation de la séquence chaotique générée à partir de la carte proposée, il est clair que la carte CSCP a une faible autocorrélation qui implique l'absence de similitude

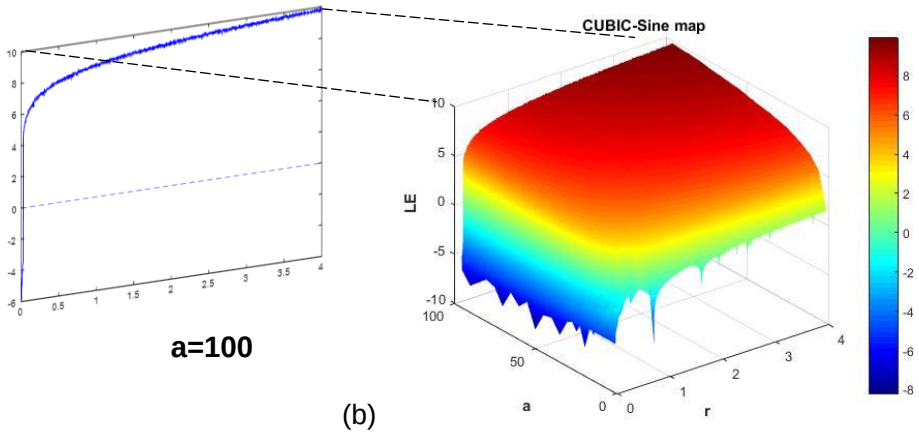
entre ses échantillons ; ce résultat caractérise le caractère aléatoire de notre nouvelle carte. Les Figure III.4.c montre la similitude la plus déroutante entre le chaos et le bruit. Figure III.4.a présente une nette amélioration de la carte de CSCP par degré d'élévation, plus l'exposant augmente plus la forme de « LE » est lisse ce qui signifie que le chaos s'est introduit sans doublement périodiques et sans interruptions, c'est le cas parfait.

3) L'exposant Lyapunov

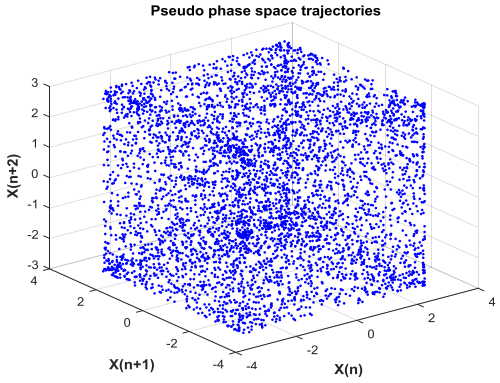
Il est clair que les valeurs négatives de l'exposant de Lyapunov prouvent que le système est en régime de point fixe, lorsque les valeurs de l'exposant de Lyapunov atteignent ses valeurs positives, il est évident que le système montre son comportement chaotique. Dans un crypto système basé sur le chaos, les valeurs des paramètres de contrôle doivent être sélectionnées de telle sorte que la valeur de l'exposant de Lyapunov soit toujours positive. La sensibilité aux conditions initiales peut être mesurée par l'exposant de Lyapunov. Il est très important que la carte chaotique présente des valeurs d'exposant de Lyapunov positives pour toutes les valeurs de son paramètre de contrôle.

Par conséquent, la carte cubique-sinus améliorée semble idéale pour générer des séquences aléatoires ce que démontre les diagrammes d'exposants de Lyapunov de Figure III.4 pour différentes valeurs du paramètre (a). Il est clair que la carte couplée cubique-sinus montre son comportement chaotique pour les valeurs r = 0,032 à 4 lorsque (α, β) = (1,1) et a=100 comme le montre la Figure III.4, plus 'a' augmente plus LE devient positif avec un plus grand intervalle de r le plus proche pour commencer de 0 à 4. La carte paramétrique Cubique-Sinus améliorée montre son comportement chaotique optimal pour les valeurs a = 6, alpha = 10,36, beta = 3,2. De plus, il est prouvé que la carte couplée cubique-sinus paramétrique montre sa suprématie sur la carte couplée sinus-logistique réelle, montre son comportement chaotique pour les valeurs r [-4, 9] comme indiqué sur la Figure III.3.

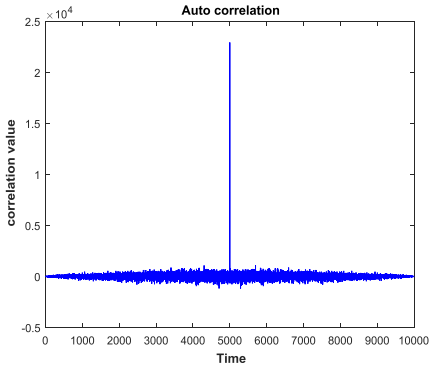
III.1.4. La structure tridimensionnelle de la carte chaotique développée 3D CSCP



(b)



(c)



(d)

Figure III. 5 La dynamique de la carte CSCP (b) Graphe de l'exposant de Lyapunov (c) Auto-corrélation (d)Trajectoire de l'espace de phase

La carte Cubique tridimensionnelles est donnée par les équations suivantes.

$$\begin{cases} x_{n+1} = \sin(\pi l x_n (2.59 - 0.8x_n)^2) + b{y_n}^2 x_n + a z_n^3 \\ y_{n+1} = 2\sin(\pi l y_n (2.59 - 0.8y_n)^2) + b{z_n}^2 y_n + a x_n^3 \\ z_{n+1} = 3\sin(\pi l z_n (2.59 - 0.8z_n)^2) + b{x_n}^2 z_n + a y_n^2 \end{cases} \quad (III.7)$$

Le couplage quadratique et les trois termes constants (l, a, b) rendent la carte Cubique-Sinus 3D plus robuste et sécurisée. Ils représentent une partie de la clé de chiffrement

D'après les diagrammes d'exposant de Lyapunov (LE) de la Figure III.4, il est clair que le La carte couplée cubique-sinusoïdale montre une dynamique chaotique remarquable, plus 'a' augmente plus (LE) devient positif avec un plus grand intervalle de a ∈ [−4, 9] et montre son comportement optimal chaotique

pour la valeur de LE= 9,9115et a=3,96. Les caractéristiques de la carte Cubique-Sinus obtenue par mixage semble idéale pour générer des séquences aléatoires.

III.2. Conception de La Structure du bruit cubique-sinus paramétrique en cascade développée

Dans le système proposé, On applique la fonction XOR à l'image d'entrée avec le bruit chaotique produit basé sur des cartes développées en trois étapes, la Figure III.5 montre la structure du système proposé, l'image transmise à travers un système de transmission OFDM est représenté dans (Figure. IV.5 -c).

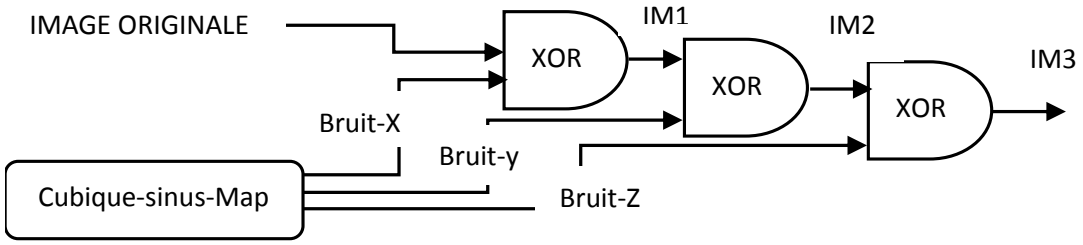


Figure III. 6 Structure du bruit cubique-sinus

Le crypto système a été obtenu selon le processus suivant :

$$\begin{cases} Bruit1(i,j) = mod(z(i)\alpha_1 image\ height, \alpha_2) \\ Bruit2(i,j) = mod(y(i) image\ height, \alpha_3) \\ Bruit3(i,j) = mod(x(i)\alpha_4, image\ height) \\ \alpha_1, \alpha_2, \alpha_3, \alpha_4 \ sont\ les\ paramètres\ de\ contrôle \end{cases} \quad (III.8)$$

L'image chiffrée est obtenue par trois opération « XOR » successives

$$\begin{cases} Im1 = Im - originale\ XOR\ bruit1 \\ Im2 = Im1\ XOR\ bruit2 \\ Im3 = Im2\ XOR\ bruit3 \end{cases} \quad (III.9)$$

Image-Chiffrée = Im-Originale ⊕ bruit1 ⊕ bruit2⊕ bruit3 (III. 10)

III.3. Brouillage de la modulation QAM utilisant la nouvelle carte X

La modulation QAM a été utilisée dans le cryptage sécurisé des données, un brouillage chaotique des symboles au sein de la constellation en utilisant des transformations chaotiques I et Q pour améliorer la sécurité de la couche physique. Les propriétés pseudo-aléatoires du chaos numérique offrant un immense espace clé idéal pour générer un nombre infini de constellations. La cartographie chaotique réalisée est basée sur la structure en cascade de deux cartes chaotiques : la carte « Cat »et une nouvelle carte « cubique

2D ». Dans cette section on propose et démontre expérimentalement un schéma de cryptage des données de la couche physique utilisant un brouillage chaotique des symboles de modulation d'amplitude en quadrature (4 QAM) dans une transmission d'image OFDM.

Les données sécurisées dans la couche physique sont fournies en utilisant un brouillage de la constellation QAM basé sur des transformations chaotiques combinées en cascade avec la carte cubique ensuite avec la carte Cat. La carte numérique résultante de la combinaison est nommée la carte bidimensionnelle « X », le schéma fonctionnel de la technique proposée est illustré dans la Figure III.6., un brouillage chaotique I et Q a été effectué, les symboles QAM sont brouillés parmi les points d'emplacement fixes pour générer une nouvelle position de la constellation QAM.

L'idée de faire un mappage QAM chaotique est réalisée en mappant chaque symbole QAM, de nouvelles valeurs en phase et en quadrature seront évaluées à partir des séquences chaotiques obtenues en utilisant ainsi, un nouvel emplacement de cartographie, dans les dimensions 4 QAM.

Les processus de brouillage des constellations et débrouillage des constellations inverses sont effectués à l'aide de la carte X constitué d'un mixage des deux cartes suivantes :

III.3.1. Carte du chat d'Arnold

Appelée carte du chat d'Arnold en reconnaissance au mathématicien russe Vladimir I. Arnold, qui la découverte et démontré ses effets en 1967 en utilisant une image d'un chat. La carte de chat d'Arnold utilise la théorie de l'algèbre linéaire pour apporter une variation dans la position des pixels de l'image originale, c'est une certaine bijection du tore vers lui-même, Il s'agit d'une transformation qui étire une image composée de n par n pixels. Cette transformation est donnée par l'équation suivante[130] :

$$\begin{bmatrix} I \\ Q \end{bmatrix} = 2 \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} \frac{I+M-1}{2} \\ \frac{Q+M-1}{2} \end{bmatrix} mod(M) - M + 1 \qquad (III.11)$$

III.3.2. La nouvelle carte cubique

$$\begin{bmatrix} I \\ Q \end{bmatrix}^T = 2[a \quad 1] \begin{bmatrix} Q+1 & I+1 \\ \frac{I(2-I)^2}{2} & \frac{Q(2-Q)^2}{2} \end{bmatrix} mod(M) - M + 1 \qquad (III.12)$$

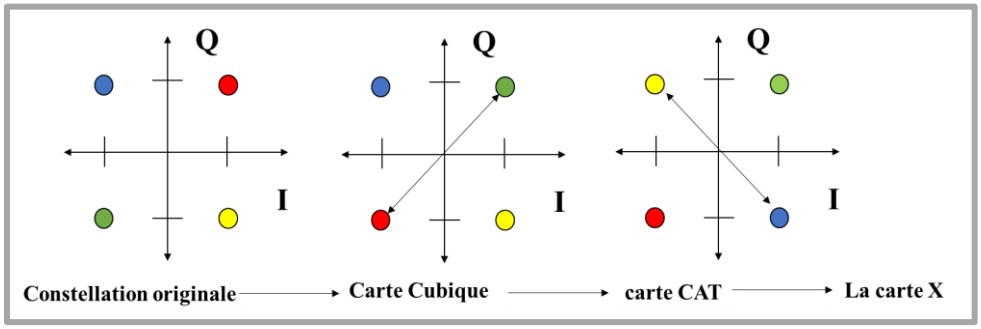
Où « a » et « b » sont les paramètres du système

(I) et (Q), respectivement. Représentent les symboles 4-QAM crypté

Pour a=1, ils peuvent être exprimé comme suit :

$$\begin{cases} I = 2mod(a(q+1) + i(2-i)^2, M) - M + 1 \\ Q = 2mod(a(i+1) + q(2-q)^2, M) - M + 1 \end{cases} \quad \text{(III. 13)}$$

Où En phase (i) et en quadrature-phase (q) sont les branches de la constellation d'origine QAM



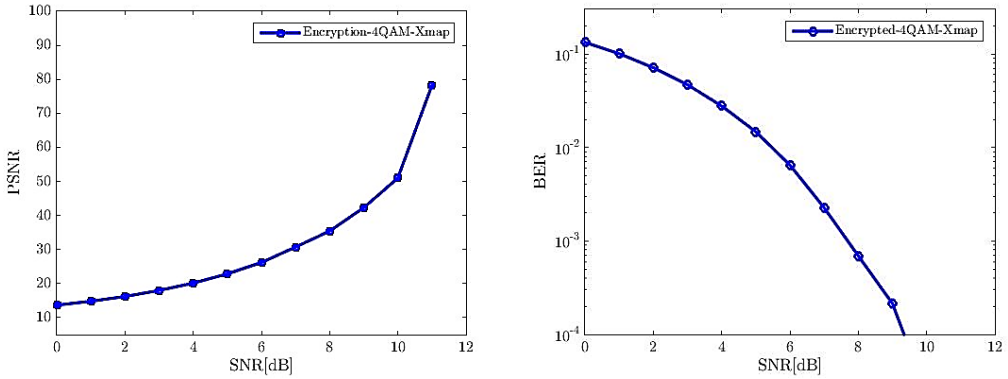


Figure III. 7 (a)Constellation de la carte X 4-QAM(b)Les résultats PSNR & BER.

III.3.3. La nouvelle Carte X

La structure de la constellation illustrée par la Figure III.7 (b) a été obtenue par combinaison en cascade des deux cartes suivantes La

CA: $est\ la\ fonction\ Cat$

C: $est\ la\ fonction\ Cubique$

$$X_{n+1} = CA\big(C(x_n)\big) \qquad (46)$$

La Figure III.7 (b) illustre les résultats du brouillage de la constellation QAM utilisant la nouvelle carte X pour SNR=1dB (BER= 0.1330), pour SNR=11dB (PSNR=78.1094dB et BER=3,6239e-05dB), pour 12dB nous obtenant une valeur infinie du PSNR avec un BER=0 dB.

IV.1. Chaine d'émission réception OFDM adopté

Ce travail de recherche s'inscrit dans le cadre du prolongement des projets de recherche développées par le laboratoire LABCAV de l'université de Guelma notamment avec le travail de mon collègue : Mr BOUCHEMEL Ammar avec sa thèse « Contribution à la transmission des images compressées : Application aux systèmes de télécommunications » dans sa thèse un système de transmission robuste pour les images compressée a été proposé, en intégrant dans la chaine de transmission une nouvelle technique de compression appelée μ-MNLT [131]. Ainsi, L'intégration de notre système de chiffrement a été effectué sur le schéma de transmission qui a été proposé dans le travail cité ci-dessus.

Le Bloc de codage source a été remplacé par le Bloc de chiffrement utilisant les cartes développées avec les trois techniques respectives :

- Chiffrement chaotique par la carte Cubique-Sinus
- Stéganographie par la carte Cubique sinus-bruit
- Chiffrement chaotique de la modulation par la carte Cubique-sinus.

Le tableau suivant représente les paramètres de la simulation de transmission effectuée sur MATLAB

Tableau IV.1 : Paramètres de la transmission OFDM sur Canal avec un bruit additif blanc Gaussien (AWGN).

Propriété	Valeur
Taille de l'image d'origine (1Pixel=8bits)	256 x 256 =65536 Pixels =524288 Bits = Total des bits transmis
Schéma de modulation	4 QAM
Taille FFT 2 bits sont modulés par sous-porteuse	512 512 sous porteuses
Nombre de bits par symbole = log2(4QAM)	2 bits =1 symbole
Nombre de symboles par Bloc (sous bande) Nombre de Bloc =Total bits /longueur d'un bloc	100 6
Longueur d'un block =. Nombre de FFT *Nombre de symbole par block*Nombre de bits par symbole	512*100*2=102400bits

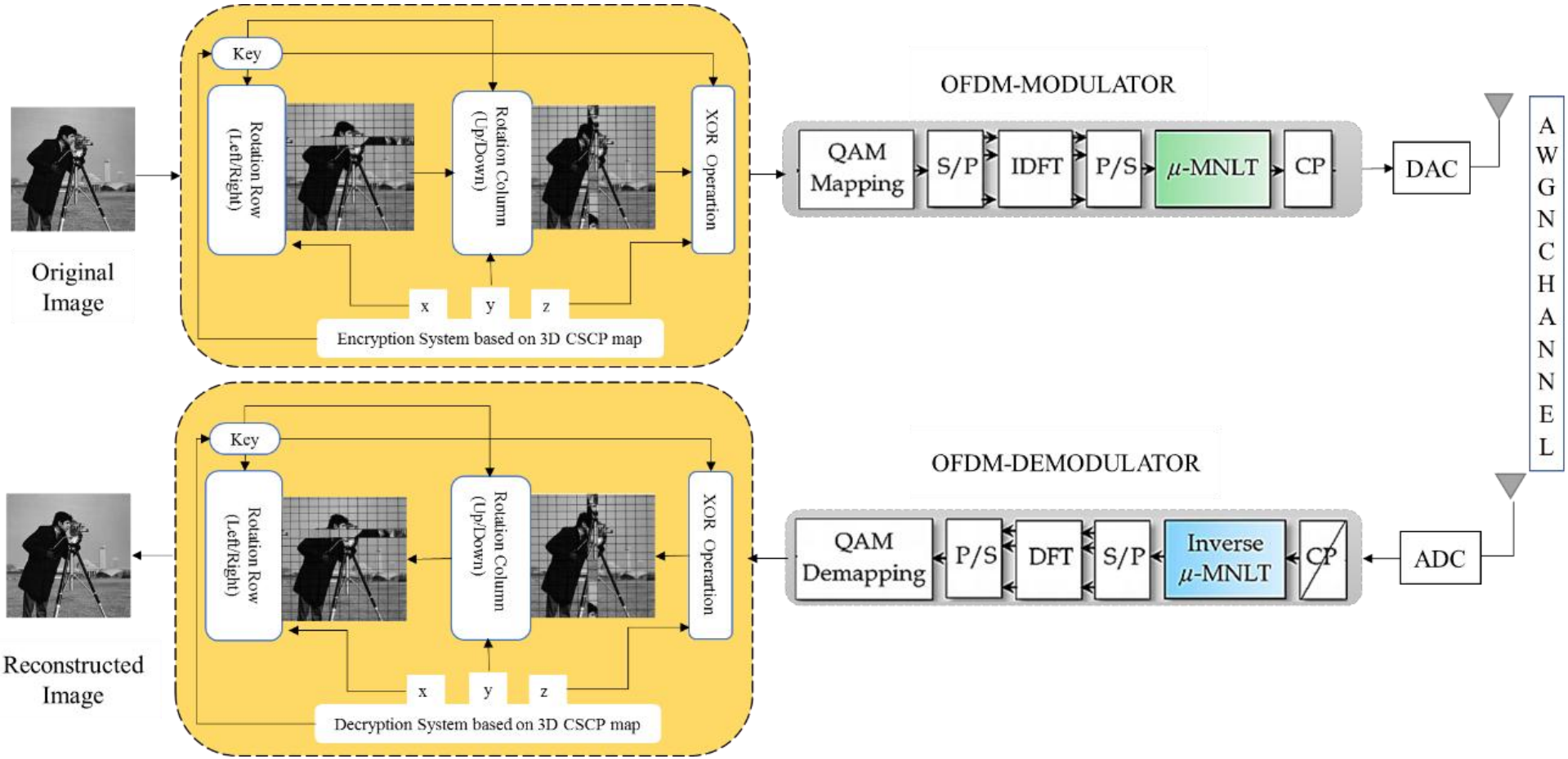


Figure IV. 1 Le schéma de transmission OFDM adopté

Dans nos simulations, nous avons effectué le chiffrement des images de différentes tailles avec l'algorithme de cryptage détaillé dans la Section IV.2, ensuite, les images cryptées ont été transformées en un format binaire pour la transmission (OFDM).

L'image utilisée comme exemple de simulation des résultats est l'image « Cameraman » au format « Tiff » avec une taille de 256 X 256. Le nombre total de pixels est donc 65536. Chaque valeur de pixel est représentée au format entier non signé de 8 bits (uint-8). Initialement cette image n'est pas sous une forme appropriée pour une transmission directe via le système OFDM. Pour transmettre cette image qui est représentée en matrice (signal bidimensionnel) au format 256 x 256, elle est convertie en un vecteur (signal unidimensionnel) de 1 x 65536. Ensuite on applique le processus de chiffrement avec l'une des méthodes détaillées dans la section IV.2. Pour la technique de modulation utilisée 4QAM, nous devons convertir les données vectorielles en données binaires (quatre éléments de signalisation à savoir 00, 01, 10 et 11 0, 1, 2 et 3 respectivement).

Les données sources qui sont sous forme série sont ensuite converties sous forme parallèle par un convertisseur S/P qui divise les données à son entrée en des flux de données parallèles de débits réduits afin d'attribuer les données sur plusieurs sous-porteuses. L'opération IDFT est effectuée. A la sortie, après avoir récupéré les bits numériques, l'image originale peut être reconstruite en effectuant opérations inverses correspondant aux opérations décrites ci-dessus. Le tableau IV.1. Montre les caractéristiques de l'image source ainsi que les propriétés et valeurs correspondantes qui sont prises en compte dans la simulation MATLAB. Le bruit gaussien blanc additif (AWGN) a été pris en compte dans les simulations.

IV.2. L'algorithme de chiffrement adopté

La technique de chiffrement par cryptographie utilisant la carte CSCP développée est illustré à la Figure. IV.1. L'algorithme de chiffrement [132]est illustré dans l'organigramme de Figure IV.3 et consiste en les étapes suivantes :

Une image « Cameraman.tiff » Tagged Image File Format (TIFF) avec une taille de 256*256 en échelle de gris est prise comme exemple d'application. Le mode niveaux de gris Figure IV.2 utilise différentes nuances de gris dans une image. Dans les images 8 bits, il peut y avoir jusqu'à 256 nuances de gris. Chaque pixel d'une image en niveaux de gris a une valeur de luminosité allant de 0 (noir) à 255 (blanc). Dans les

images 16 et 32 bits, le nombre de nuances dans une image est beaucoup plus élevé que dans les images 8 bits.

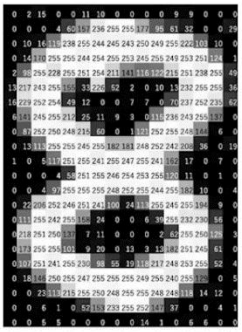


Figure IV. 2 Enregistrement d'une image en mode niveau de gris sur micro-ordinateur.

Tout d'abord, l'image est divisée en blocs de 8 bits. La méthode proposée comprend les éléments suivants

ÉTAPE 1 : Les permutations de pixel des lignes, sont basées sur le tri de la séquence aléatoire par la clé X, Chaque pixel, dans la ligne sont permutés, c'est-à-dire, que leur position est modifiée par rotation à gauche ou à droite selon la séquence pseudo- aléatoire qui génère soit un chiffre pair ou impaire.

ÉTAPE 2 : Les permutations de pixel des colonnes, sont basées sur le tri de la séquence pseudo aléatoire par la clé y, les pixels dans les colonnes sont transférés par rotation vers le haut ou vers le bas en selon la séquence pseudo- aléatoire qui génère soit un chiffre pair ou impair.

ÉTAPE 3 : L'opération XOR s'exécute sur l'ensemble des bits de l'image qui sont divisés en blocs de 8 bits, colonne par colonne et par les séquences générées par la clé z.

La génération des séquences chaotiques (x, y et z) est bien détaillée dans le chapitre III. Comme observé sur la Figure IV.1, il existe un générateur de séquence chaotique 3D cubique-Sinus. La valeur de x, y, z est comprise entre 0 et 1. Ces trois valeurs (x, y et z) sont en fait la clé des séquences chaotiques rendent la confusion 3D beaucoup plus compliquée qu'avec un système unidimensionnel.

:

Génération des clés

Pour utiliser les clés, elles doivent être calculées afin d'être employées à chaque étape. Le code MATLAB pour la génération des clés est comme suit

Function key (m, n as input) % m, n est le nombre de ligne et colonne de pixels par image

X (1) = 0.2150; key x (1) = x (1) %valeur initiale de clé x.

Y (1) = 0.3500; key y (1) = y (1) % valeur initiale de clé y.

Z (1) = 0.7350; key z (1) = z (1) % valeur initiale de clé z.

For j = 2 : m %m est le nombre de ligne

$x(i) =$ sin(πlx(i − 1)((2.59 − 0.8$x(i)^2$) + $by(i)^2x(i) + az(i)^3$;

$y(i) =$ sin(πly(i − 1)(2.59 − 0.8$y(i)^2$) + $bz(i)^2y(i) + ax(i)^3$;

Key x(j) = (floor(x(j) × 100000) mod 255) ; % Extraction de la clé x.

Key y(j) = (floor(y(j) × 100000) mod 255) ; % Extraction de la clé z.

End For

For i = 2 : n %n est le nombre de colonne.

$z(i) =$ sin(πlz(i − 1)((2.59 − 0.8$x(i)^2$) + $bx(i)^2z(i) + ay(i)^3$;

Key z(i) = (floor(z(i) × 100000) mod 255); % Extraction de la clé z

End For

End

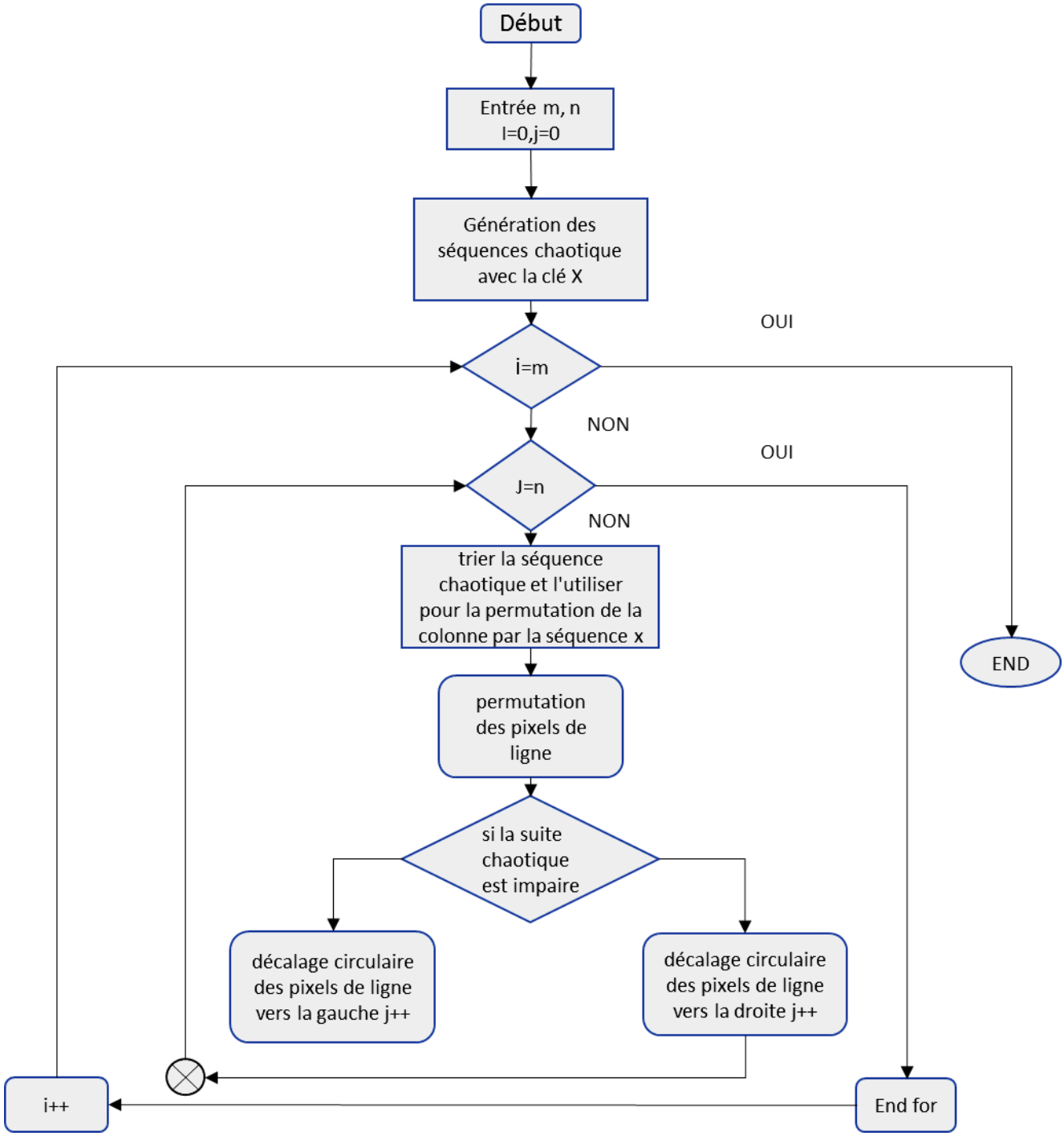
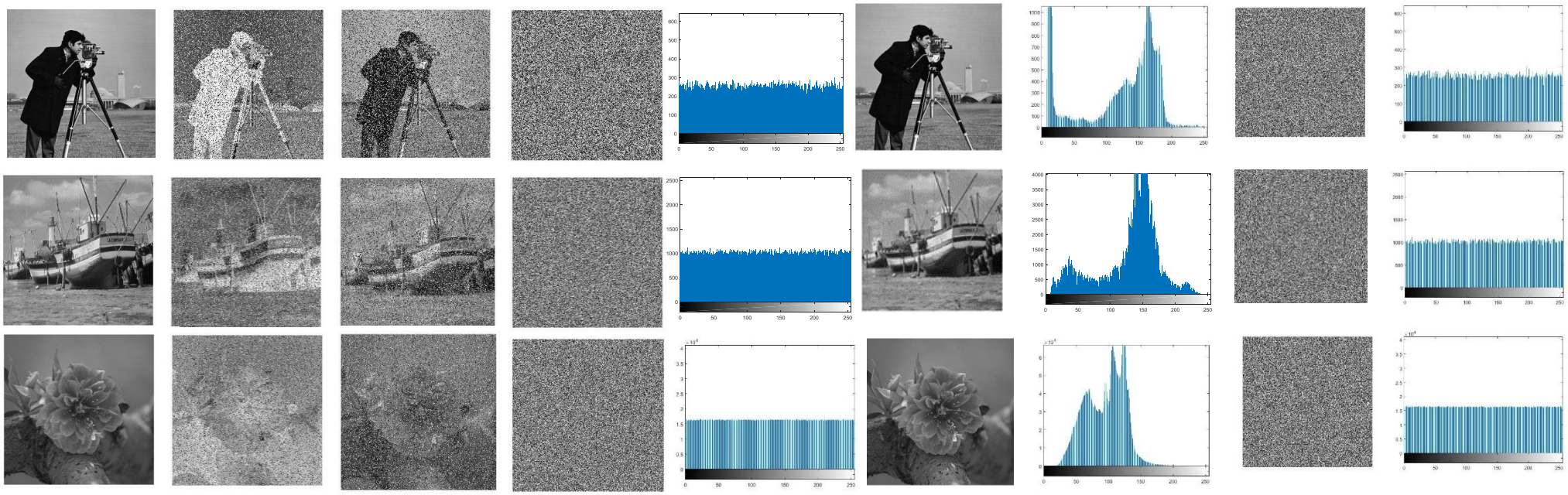


Figure IV. 3 Organigramme de la méthode proposée

Tableau IV.2 : Métrique et résultats de chiffrement d'images de différents formats

	CSCP	CSC Bruit	CSCP	CSC Bruit	CSCP	CSC Bruit
	Cameraman /256x256		*Boat/512x512*		*Flower/2048x2048*	
Entropie image chiffrée	7.9979	7.9977	7.9994	7,9993	7.9999868	7.999957
Corrélation Horizontale	−0,000920	−0,001431	0,00081	−0,00017	0,000227	−0,000112
Corrélation Verticale	−0,002198	−0,004928	−0,00143	0.00004	−0,000092	0,0005302
Corrélation diagonale	−0,001944	−0,007155	−0,00082	−0,00035	0,000363	0,001059
Temps de chiffrement	0.345618	0.024762	1.283834	0.146900	24.881715	1.522180
NPCR (%)	99.6292	99.6124	99.5796	99.6189	99.6111	99.5912
UACI (%)	33.4526	33.4525	33.5461	33.4871	33.4935	30.3150
Espace de clé	2^{328}	2^{382}	2^{328}	2^{382}	2^{328}	2^{382}



(a) (b)

Figure IV.4 Chiffrement des images de différentes tailles avec les deux méthodes (a) Image originale –XOR avec Bruit1-XOR avec le bruit2-XOR avec le bruit3=l'image chiffrée avec la carte CSC Bruit(b) Image originale –Histogramme de l'image originale-image chiffrée-Histogramme de l'image chiffrée avec la carte CSCP

IV.3. L’analyse des performances de Sécurité des Chiffrements

IV.3.1. Analyse des histogrammes

Il ressort du Tableau IV.2, que les histogrammes des images chiffrées sont uniformément distribués par rapport aux histogrammes des images d'origines pour les deux techniques. Ceci rend la cryptanalyse de plus en plus difficile car les images chiffrées ne fournissent aucun élément pour l'exploitation de l'histogramme et permettant de concevoir une attaque statistique. La recherche de similarité entre deux niveaux de pixels est assez difficile ce qui implique une forte résistance aux attaques d'histogrammes. L’uniformité de la distribution est proportionnelle à la taille des images. La répartition est quasi parfaite avec des images de format 2048 x 2048.

IV.3.2 Analyse de corrélations des images originales et chiffrées

Il ressort du Tableau IV.2, et de la Figure IV.4 et d'après les valeurs obtenues, que les pixels adjacents des images chiffrées horizontalement, verticalement et en diagonale ont pour la plupart des valeurs négatives du coefficient de corrélation ce qui indique une bonne distribution aléatoire, ce qui prouve aussi qu’il n'y a pas de corrélation entre les images originales et chiffrées. Il n'y a donc pas de similitude entre les images originales et chiffrées.

IV.3.3 Analyse statistique

Les valeurs obtenues montrent une entropie élevée de la méthode qui est très proche de la valeur idéale de 7,999986 ≈ 8 pour l'image de format (2048 x 2048). Les résultats indiquent que les valeurs d'entropie pour les images chiffrées sont très proches de celles d'une source aléatoire. Par conséquent, l'algorithme de chiffrement proposé est robuste contre les attaques d'entropie. Plus la distribution de valeur de gris est uniforme, plus l'entropie de l'information obtenue est grande, plus la prévisibilité sera faible, et par conséquent le crypto système est considéré comme robuste.

IV.3.4 Analyse de l'espace des clés

Pour le schéma basé sur la carte Cubique -sinus proposé, la clé inclut les conditions initiales (x0, y0, z0) dans la plage de [0,1] et les paramètres de contrôle (a1, a2, a3, l, a, b), la longueur de chaque sous-clé est réglée sur 16 décimales (précision de 10^{-16}), l'espace clé sera de 1096 × 103 = 1099 ≈ 2^{328}, il faudra ≈ 3,2297 × 1081 ans pour casser un chiffre et obtenir la bonne clé.

Pour le schéma proposé avec la carte Cubique-sinus bruit, la clé inclut les conditions initiales (x0, y0, z0) dans la plage de [0,1] et les paramètres de contrôle (a1, a2, a3, l, a, b, α1, α2, α3, α4), la longueur de

chaque sous-clé est définie sur 16 décimales (précision de 10^{-16}), les αi sont définis sur 4 décimales, l'espace clé sera 1096 × 103 × 104×4 = 10115 ≈ 2^{382}. Ce qui implique une sécurité robuste.

Un schéma de cryptage d'images souhaitable devrait avoir un grand espace clé d'au moins 2^{100} pour résister aux attaques de force brute ; est $\approx 2^{1886}$dans les cas du RSA ou El Gamal est $\approx 2^{161}$, quand il est défini sur courbes elliptiques.[133].

IV.3.5 Analyse différentielle

L'influence du changement de pixels sur l'image originale cryptée par l'algorithme proposé est testée en utilisant les facteurs NPCR et l'UACI. La carte CSCP présente les meilleurs résultats avec un NPCR =99.6292 et la différence de l'intensité moyenne entre deux images chiffrées UACI=33.5461.

IV.3.6 Le temps de traitement

Nous utilisons pour tester la vitesse de chiffrement des images un PC portable avec un Processeur Intel Core TM i7-4500U 2,4 GHz avec 8 Go de RAM et MATLAB (R2015a). Les cartes proposées ont une bonne capacité à crypter en temps réel et à fournir un bon niveau de sécurité. Le schéma proposé utilisant Cubique -cat-bruit montre les meilleures performances en termes de coefficients de corrélations et temps de chiffrement avec 0.024762s.

Conclusion

Notre crypto système est basé sur l'architecture confusion/diffusion en utilisant la carte chaotique non linéaire CSCP développée. La carte chaotique CSCP possède des propriétés dynamiques complexe, des propriétés clé pour générer des séquences pseudo-aléatoires durant tout le processus de chiffrement, .la sécurité du schéma proposé repose principalement sur les paramètres des cartes chaotiques utilisées comme clé. Des performances de sécurité satisfaisantes sont atteintes en un seul tour de chiffrement. L'efficacité du chiffrement proposé contre les différentes attaques a été prouvé. Les résultats de ces évaluations peuvent être résumés comme suit :

• L'espace clé pour les deux cartes chaotique cubique sine et cubique -sinus bruit implique une robustesse contre les différentes attaques

• L'efficacité de cette méthode est perceptible avec une taille d'image plus grande.

• Le temps d'exécution diminue considérablement avec La carte Cubique-sinus Bruit qui présente les meilleurs résultats par rapport aux deux autres cartes.

• les systèmes chaotiques proposés sont capables de produire un grand nombre de nouvelles cartes chaotiques.

• La carte cubique -sinus surpasse la carte logistique-sinus largement exploitée dans les cryptos système [105, 108, 134].

• Il est en outre conclu que l'utilisation des schémas cryptographie avec la carte CSCP donne les meilleurs résultats en termes d'entropie mais avec un temps moindre par rapport à la technique de stéganographie. Selon le niveau de sécurité requis, les deux techniques peuvent être combinées, la cryptographie en première couche et la stéganographie en deuxième couche.

IV.4. Simulation et analyse des résultats en transmission OFDM

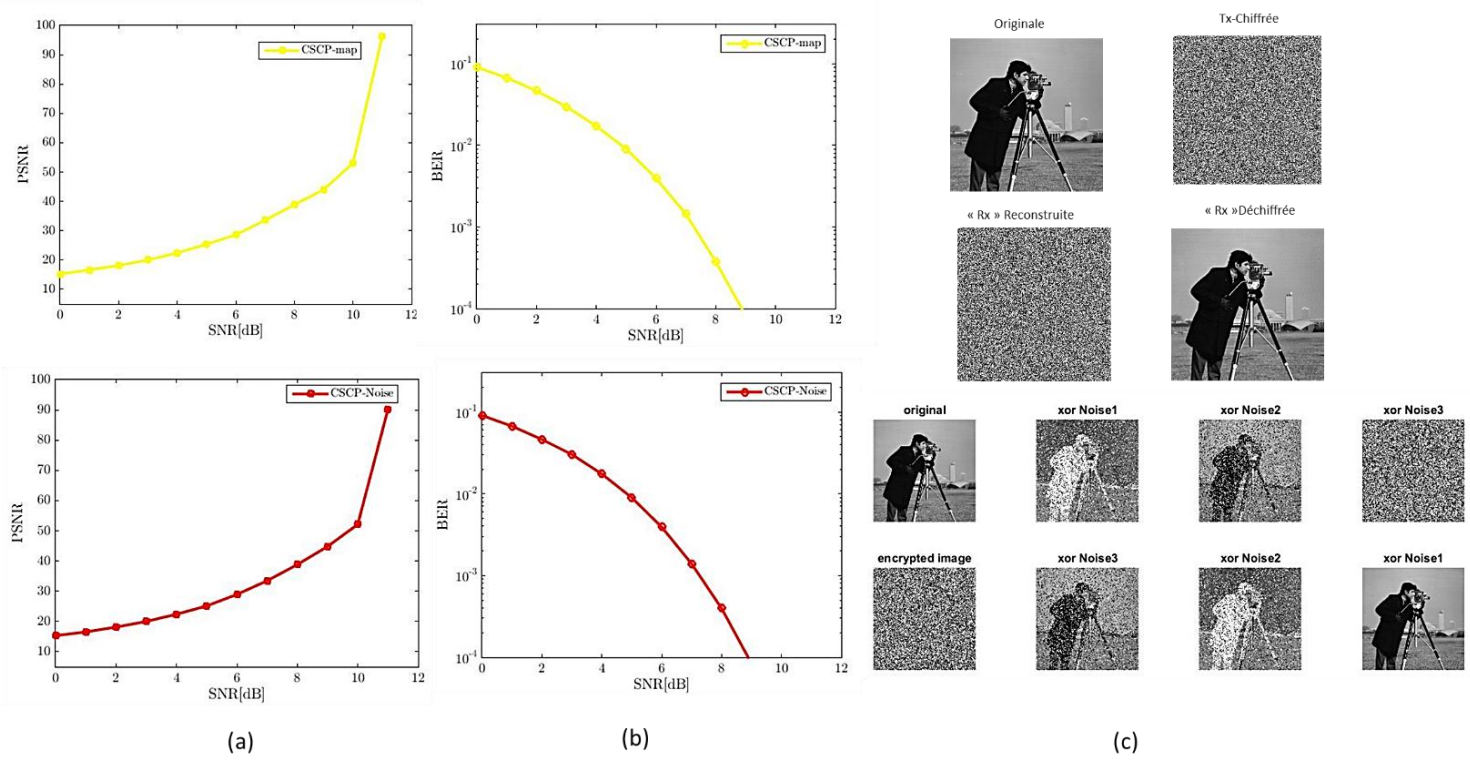


Figure IV. 5.1 Résultat des simulations pour L'image « Cameraman » chiffrée en transmission OFDM (a)PSNR (b)BER (c)Représentation d'image au niveau d'émetteur (originale et chiffrée) et au niveau de récepteur (reçus et déchiffrée)

Les résultats sont obtenus avec le logiciel Matlab, utilisé pour la mise en œuvre de la simulation du système de communication numérique sans fil ainsi que les différentes techniques de sécurisation des images. Pour évaluer la qualité des images décryptées au niveau du récepteur, nous avons utilisé le rapport signal sur bruit de crête (PSNR) et le BER entre l'image originale et l'image décryptée.

La Figure IV. 5 illustre la variation du PSNR de l'image Cameraman 256 x 256 décryptée avec le rapport signal sur bruit (SNR) dans le canal pour la cryptographie et stéganographie. On remarque clairement une dégradation de la valeur du PSNR avec le CSC bruit par rapport au CSCP 7.5 dB sans dégradation du BER, mais le CSC Bruit reste quand même très performant avec un PSNR=88.767 dB.

Tableau IV.3 : Comparaison des résultats en transmission OFDM des trois méthodes

	La carte CSCP	**La carte Cubique Sinus bruit**	**La carte Cubique-Cat**
SNR=1dB	BER= 0,0902748	BER = 1,9073	BER= 0.1330,
SNR=11dB	PSNR=96.2956 et le BER= 1.9073e-06)	PSNR=88.767 dB et BER=1. 9073.e-05dB	PSNR=78.1094dB et BER=3,6239e-05dB

D'après le Tableau IV.3, nous analysons les performances de la transmission d'images selon le modèle d'émetteur-récepteur OFDM avec une comparaison entre le traitement des données à l'aide de différents schémas sécurisés avec la cryptographie, la stéganographie et le Cryptage de la modulation pour identifier la meilleure technique pour la transmission sécurisée des images. D'après les résultats obtenus on peut constater clairement l'efficacité de notre approche par la qualité des images reconstruites selon les valeurs PSNR et BER obtenus. Cependant, la transmission des images via le système de communication effectuée par le brouillage de la modulation QAM montre que la qualité de l'image reçue est moindre dans ce cas et moins efficaces que la sécurisation par stéganographie ou par cryptographie. Les trois méthodes peuvent être intégrées dans le même système selon le degré de sécurité requis.

Conclusion Générale

L'ère moderne où la communication la plus importante se fait par des techniques sans fil utilisant le réseau pour transférer des données, les principales préoccupations portent sur la sécurité des données privées ou de défense des pays. Le chiffrement est un des moyens les plus sûr pour garantir une sécurité digne d'un accès non officiel sur de nombreux terrains. Le chiffrement d'image est d'une ampleur frappante pour la recherche car la communication avec le support d'objets multimédia se développe rapidement.

Diverses techniques de chiffrement ont été utilisés pour chiffrer l'image, chaque technique présente des avantages et des inconvénients, il n'existe pas de solution parfaite néanmoins on peut optimiser des solutions en fonction du niveau de sécurité requis, du temps, du matériel et de l'environnement

Dans cette thèse le cryptage d'image basé sur le chaos a été examiné en détail, reliant les techniques actuelles de cryptographie basée sur les cartes chaotiques. Nous avons abordé également l'exploitation des systèmes chaotiques aux transmissions multimédias sécurisées. En prenant la sécurité à des niveaux élevés comme objectif, nous avons proposé de nouvelles cartes chaotiques appliquées à différentes techniques de sécurisation des images numériques.

Notre approche s'inscrit dans le cadre d'une transmission sécurisée chaotique. Les solutions proposées dans ce contexte traite du domaine de la cryptographie basée sur des dynamiques chaotiques complexes obtenues par mixage des cartes chaotiques en cascade et en parallèle, afin d'augmenter la robustesse de la sécurité dans la transmission des données vis-à-vis des attaques connues, ce travail s'est particulièrement concentré sur trois directions : l'approche cryptographique, la stéganographie et le brouillage de la modulation QAM. Les principales contributions de ce travail sont organisées dans les trois directions mentionnées. Les chapitres de la thèse répondent à quelques questions soulevées par les schémas de sécurité des communications basées sur le chaos.

Notre contribution innovante vient de la génération d'une nouvelle carte chaotique développée et combinée avec d'autres cartes, ainsi que la génération d'un bruit chaotique avec une nouvelle approche d'application en stéganographie. Les résultats expérimentaux sont explorés dans cette thèse pour démontrer l'efficacité de notre approche. Nous illustrons la sécurité du crypto système proposé en utilisant différents types d'image avec différentes tailles, nous confirmons que le crypto système proposé est sécurisé contre différentes attaques : par l'analyse statistique, les attaques différentielles et les attaques par force brute. Les objectifs ont été atteints avec la mise en œuvre des nouvelles cartes chaotiques dans un crypto système efficace en termes de robustesse et de rapidité avec une bonne qualité d'image à la réception dans une transmission (OFDM).

ANNEXE A : Notions de base sur la sécurité en communication.

Les exigences de sécurité pour les WMSNs sont similaires à celles des réseaux informatiques conventionnels, des solutions communes conçues pour les réseaux informatiques et hérités par les WMSNs, Les fonctions de sécurité tels que la confidentialité, l'intégrité, la disponibilité et l'authenticité doivent être remplis par les différents algorithmes et adaptés au WMSNs

La protection des WMSNs est principalement assurée par une démarche globale qui repose sur ces quatre grandes fonctions assurées par des algorithmes opérants aux niveau des différentes couches protocolaires du réseau qui visent à sécuriser le lien entre l'expéditeur/destinataire et à empêcher toute divulgation de contenu multimédia par toute entité non autorisée.

Confidentialité des données

Cela garantit la protection des informations sensibles afin que les utilisateurs non autorisés n'aient pas accès aux informations sensibles. La confidentialité protège la divulgation d'informations dans l'environnement du capteur lorsque des données sont transférées entre les nœuds de capteur ou entre une station de base et les nœuds de capteur. Cela empêche également le type d'attaque d'écoute clandestine (DoS). La plus grande menace pour la confidentialité est l'existence de nœuds compromis, car ces nœuds peuvent être exploités par l'attaquant pour voler des données critiques telles que des clés cryptographiques. Ces clés peuvent être utilisées pour déchiffrer les messages et obtenir des informations sensibles. Si A envoie un message à B, il devrait être impossible pour E d'apprendre le contenu d'un message chiffré sans connaître la clé secrète.

Authentification du nœud capteur

Cette technique sert à vérifier l'identité et distingue principalement les utilisateurs malveillants et le trafic légitime. Dans le cas des réseaux de capteurs sans fil, chaque station de base et le nœud de capteur doivent avoir la capacité d'identifier si la donnée reçue est envoyée par un nœud attaquant ou un nœud légitime. En effet, un attaquant peut tromper le nœud légitime et le forcer à accepter de fausses données. Si de fausses données sont injectées dans le réseau de capteurs, cela peut entraîner un résultat inattendu. Un code d'authentification de message (MAC) joint au message peut être utilisé pour authentifier l'origine de ces fausses informations, il faut que B soit sûr que c'est A (et non E) qui a envoyé les données[135]. L'auteur a proposé dans ce travail [136], le contrôle d'accès CP-ABE libre utilisant la cryptographie à courbe elliptique pour le partage de données dans les applications multimédias. Les données ne sont accessibles que par des utilisateurs spécifiques qui sont authentifiés par le propriétaire des données. Le calcul basé sur l'appariement est remplacé avec un produit scalaire sur des courbes

elliptiques qui réduit les besoins en ressources et en mémoire pour les utilisateurs. Les caractéristiques de la cryptographie et de la stéganographie sont combinées en incorporant du texte cryptographique dans une image qui a amélioré la sécurité des données.

Intégrité des données

Cela empêche les informations d'être altérées pendant le processus de transmission de données dans le réseau de capteurs, lorsque A chiffre un message et l'envoie à B. Si E peut intercepter le message, il peut modifier le message sans que B le sache.

L'utilisation d'informations inexactes ou erronées peut entraîner des conséquences désastreuses, le manque d'intégrité est donc un grave problème. Certaines applications de réseaux de capteurs, telles que les soins de santé ou la surveillance de l'environnement, dépendent fortement du problème d'intégrité. Par conséquent, la protection des informations envoyées dans le réseau contre la modification ou l'interception est de la plus haute importance.

Disponibilité

Les capacités de communication et de calcul sont limitées dans le capteur, donc un calcul qui dépasse la capacité entraîne une consommation d'énergie supplémentaire, mais s'il n'y a pas d'énergie supplémentaire, il n'y aura pas de disponibilité de données supplémentaires. L'effondrement d'un nœud individuel peut avoir un impact sur l'arrivée du réseau. Le capteur peut utiliser son énergie de manière intelligente, rester en veille lorsqu'il y a un état stable pendant une longue période et utiliser une alimentation de secours pour les situations qui exigent un calcul plus que d'habitude.

Sécurisation et gestion du réseau

La gestion de plusieurs composants dans l'ensemble du réseau est nécessaire pour gérer les informations sensibles. Une gestion sécurisée au niveau de la station de base est requise dans les réseaux de capteurs sans fil car la communication depuis les nœuds de capteurs se termine à la station de base. Plusieurs techniques de gestion de distribution de clés sont nécessaires pour établir un réseau sécurisé ainsi que pour maintenir les informations de routage. Dans la technique de clustering, chaque groupe de nœuds ou cluster se compose d'un grand nombre de nœuds, une gestion sécurisée est donc requise pour un échange de données sécurisées.

Vulnérabilités et attaques

Dans la plupart des applications, les capteurs sont répartis sur de grandes surfaces, ce qui implique des difficultés pour un individu de contrôler les composants du réseau. De plus, la communication sans fil permet à un attaquant de déclencher des attaques sans avoir un accès physique à l'appareil.

Au niveau de la couche physique il peut se produire les attaques suivantes : brouillage et falsification. Le brouillage d'attaque consiste en l'interférence du signal radiofréquence que les nœuds capteurs utilisent pour communiquer. L'attaque de falsification se produit en raison de la vulnérabilité physique du capteur nœuds répartis sur de grandes surfaces, donc accessibilité du capteur, les dégats peuvent être divers tel que couper le circuit, apporter des modifications voire remplacement d'un nœud du réseau par un nœud capteur malveillant . Les attaques de couche de liaison peuvent être dues à la collision, lorsque deux nœuds capteurs tentent de transmettre tout en à la même fréquence, dans ce cas le paquet est rejeté et doit être retransmis. L'attaquant peut provoquer des collisions intentionnelles par un nœud de capteur malveillant. Collisions répétées peut conduire à l'épuisement des ressources, ce qui rend les nœuds capteurs indisponibles. Aussi dans le lien L'attaque d'injustice de couche est un type de DoS lorsque l'adversaire provoque une dégradation du temps réel les applications s'exécutent sur d'autres nœuds capteurs par interruption intermittente de la transmission de leurs cadres. Les attaques par déni de service (DoS) consistent à inonder le récepteur sans aucune autre demande de la communication peut être effectuée pendant l'attaque, laissant les nœuds impliqués indisponibles pour de nouvelles connexions.

Dans la couche physique, le brouillage est une attaque par déni de service (DoS) qui peut épuiser les ressources énergétiques des capteurs. En fait, DoS est une attaque populaire dans laquelle des informations sont injectées dans le réseau, ce qui peut rapidement épuiser le traitement, la mémoire et l'énergie ressources des nœuds, compromettant leur fonctionnement. Dans les attaques de brouillage, un ou plusieurs nœuds malveillants interférer avec les fréquences radio utilisées par les nœuds valides. Il peut alors interrompre les transmissions de paquets

Au niveau de la couche physique peuvent se produire les attaques suivantes : brouillage et falsification. Le brouillage d'attaque consiste en l'interférence du signal radiofréquence que les nœuds capteurs utilisent pour communiquer. L'attaque de falsification se produit en raison de la vulnérabilité physique du capteur nœuds répartis sur de grandes surfaces, l'attaquant est susceptibles d'intercepter les informations, de couper le circuit, de modifier voire remplacer carrement un nœud du réseau par un nœud capteur malveillant. Les attaques de couche de liaison peuvent être dues à la collision, lorsque deux nœuds capteurs tentent de transmettre en même temps, dans ce cas le paquet est rejeté et doit être retransmis .L'attaquant peut provoquer des collisions intentionnelles par un nœud de capteur malveillant. Les collisions répétées peuvent conduire à l'épuisement des ressources, ce qui rend les nœuds capteurs indisponibles. Aussi dans le lien l'attaque d'injustice de couche est un type de DoS lorsque l'adversaire provoque une dégradation du temps réel ,les applications s'exécutent sur d'autres nœuds capteurs par interruption intermittente de la transmission de leurs cadres.

ANNEXE B : Evaluation des récepteurs dans une communications numériques OFDM

Le rapport puissance crête/puissance moyenne élevé PAPR

La modulation OFDM conduit souvent à un rapport puissance crête/puissance moyenne élevé (PAPR), l'un des inconvénients majeurs des signaux OFDM, La valeur de la puissance maximale du signal est supérieure à sa puissance moyenne, et des pics de forte amplitude apparaissent. Cette particularité a pour conséquence directe de rendre les symboles OFDM sensibles aux non-linéarités engendrées par les composants, notamment les amplificateurs qui est l'un des facteurs les plus néfastes dans la transmission du signal OFDM, car il provoque saturation de puissance et distorsion non linéaire au niveau du récepteur tout en dégradant la performance de la transmission. Les propriétés pseudo-aléatoires du chaos numérique sont utiles pour la réduction du PAPR des signaux OFDM, ce qui améliore par conséquent les performances de transmission [131].

Si le bloc de N symboles est noté le vecteur $X = [X_0, X_{1,\dots,} X_{N-1}$] pour les signaux OFDM.

Le PAPR du signal à temps discret $x(n)$ par définition est le rapport de sa puissance instantanée maximale à sa puissance moyenne et peut être exprimé :

$$PAPR(x(n)) = 10\log(\max(|x(n)|^2)/E(|x(n)|^2)$$

L'enveloppe complexe des signaux OFDM est

$$x(n) = \frac{1}{\sqrt{N}} \sum_{i=0}^{N_{g-1}} X_i e^{-i\omega t}, 0 \leq n \leq N_g - 1$$

Le rapport signal sur bruit SNR

La qualité d'une transmission est évaluée par le Taux d'Erreurs Binaires (Teb ou BER pour Bit Error Rate), qui permet de juger de l'importance des dégradations subies par le message numérique. Ces dégradations dépendent à la fois du canal de propagation, mais aussi des imperfections de la chaîne de transmission, telles que le bruit additif thermique, les non-linéarités des amplificateurs de puissance ou encore les instabilités des oscillateurs locaux utilisés lors des transpositions de fréquences.

Une manière traditionnelle de comparer les techniques de modulation numérique standard lorsque l'on considère la sensibilité au bruit de canal, supposé être un bruit gaussien blanc additif, consiste à les représenter dans un plan (SNR, BER), où Le SNR du canal par définition est le rapport signal sur bruit du canal de transmission et BER est le taux d'erreur binaire du message décodé :

$$SNR = 10log\frac{P_m}{\sigma_n^2}$$

Où P_m est la puissance du message transmis, et σ_n^2 est la variance du bruit de canal.

Le taux d'erreur binaire BER

Un système de communication numérique souhaitable devrait fournir un faible Taux d'erreur binaire (BER) et un faible rapport signal sur bruit (SNR) du récepteur.

Comme son nom l'indique, un taux d'erreur binaire est défini comme étant le taux auquel les erreurs se produisent dans un système de transmission. Ceci peut être traduit directement par le nombre d'erreurs qui se produisent dans un train d'un nombre déterminé de bits. La définition du taux d'erreur binaire peut être traduit en une formule simple :

$$TEB = \frac{Nombre\ d'erreurs}{Nombre\ totale\ de\ bits\ envoyé\ ou\ transmit}$$

Si le milieu entre l'émetteur et le récepteur est bon ; le rapport signal sur bruit est élevé, le taux d'erreur binaire sera très petit est peut-être insignifiant et sans effet notable sur l'ensemble du système Toutefois, si le bruit peut être détecté, alors le taux d'erreurs binaires devra être pris en considération.

Les principales raisons de la dégradation d'un canal mesurée par la valeur du taux d'erreur binaire correspondant, TEB sont le bruit et les modifications apportées à la trajectoire de propagation. Ces deux effets ont des caractéristiques aléatoire, le bruit suivant une fonction de probabilité gaussien alors que le modèle de propagation suit un modèle de Rayleigh. Cela signifie que l'analyse des caractéristiques du canal sont généralement effectuées en utilisant des techniques d'analyse statistique.

Pour les systèmes à fibres optiques, des erreurs binaires résultent principalement des imperfections dans les composants utilisés pour faire le lien. Celle-ci comprennent le conducteur optique, le récepteur, les connecteurs et la fibre elle-même. Les erreurs binaires peuvent également être introduites à la suite de la dispersion optique et une atténuation qui peut être présente. Aussi le bruit peut être introduit dans le récepteur optique lui-même. Typiquement, ceux-ci peuvent être des photodiodes et des amplificateurs qui doivent répondre à de très faibles variations et par conséquent, il peut y avoir une présence du bruit à des niveaux élevés.

Calcule est estimation du BER

Pour pouvoir caractériser la capacité d'une technique à améliorer le canal de communication entre deux ou plusieurs points, une des données importantes est le rapport entre le nombre d'erreurs commises par l'ensemble émetteur-récepteur et le nombre total de bits transmis (BER). Le calcul analytique de cette valeur, dans le cas d'un canal AWGN, n'est pas toujours possible. Pour les méthodes de modulation

les plus simples, toutefois, il est possible de calculer une limite supérieure à cette valeur, et la limite obtenue ainsi nous sera très utile pour l'interprétation des résultats expérimentaux obtenus.

Le calcul de cette probabilité d'erreur est relativement simple dans le cas des modulations linéaires, puisqu'il s'agit de calculer, pour chacun des symboles, la probabilité de fausse détection. Le signal reçu n'est perturbé que par un bruit blanc gaussien, il s'agit donc de majorer l'aire de la partie marginale de la distribution des valeurs mesurées. [72].

Le taux d'erreur binaire, BER, peut également être défini en termes de probabilité d'erreur P_M., trois autres variables sont utilisées : la fonction d'erreur $d_{\min}^{(e)}$, l'énergie contenue dans un bit ε_{bav} et la densité de puissance spectrale du bruit N_0 (définit comme la puissance du bruit dans une bande de 1 Hz).

Il convient de noter que chaque type de modulation différente a sa propre valeur de la fonction d'erreur. En effet, chaque type de modulation effectue différemment en présence de bruit. En particulier, les systèmes d'ordre supérieur de modulation (par exemple 64QAM, etc.) qui sont en mesure d'effectuer des débits plus élevés ne sont pas aussi robustes en présence de bruit. La baisse des formats de modulation d'ordre (par exemple BPSK, QPSK, etc.) offre la baisse des taux de données mais sont plus robustes.

L'énergie par bit ε_{bav}, peut être déterminé en divisant la puissance de la porteuse par le débit binaire est une mesure de l'énergie avec les dimensions de joules, N_0est une puissance par Hertz.

Dans le cas d'une modulation de type QAM, la probabilité d'erreur par symbole vérifie l'inégalité :

$$P_M < (M-1)Q\left(\frac{d_{\min}^{(e)\,2}}{2N_0}\right)$$

Où $d_{\min}^{(e)}$ est la distance euclidienne minimale entre deux symboles. La fonction Q est définie par la relation :

$$Q(t) = \int_t^{\infty} \frac{1}{\sqrt{2\pi}} e^{-x^2/2}\, dx$$

Correspond bien à l'aire marginale d'une distribution gaussienne. Le cas de l'utilisation d'une constellation rectangulaire permet d'obtenir l'expression suivante, plus directement utilisable :

$$P_M \le 4Q\left(\sqrt{\frac{3k\varepsilon_{bav}}{(M-1)N_0}}\right)$$

Où ε_{bav}/N_0 est le rapport signal à bruit moyen par bit.

Un calcul similaire peut être mené pour des techniques de modulations plus complexes, comme une modulation non linéaire ou une modulation par signaux orthogonaux. Dans ce dernier cas, une limite supérieure de la probabilité d'erreur s'écrit sous la forme simple :

$$P_M \leq (M-1)Q\left(\varepsilon_S / N_0\right) = (M-1)Q\left(\frac{k\varepsilon_b}{N_0}\right)$$

Les facteurs affectant le taux d'erreur binaire, BER

Le taux d'erreur binaire, BER peut être affectée par un certain nombre de facteurs. En manipulant les variables qui peuvent être contrôlées, il est possible d'optimiser un système pour fournir les niveaux de performance requis. Ceci est normalement effectué dans les étapes de conception d'un système de transmission de données de sorte que les paramètres de performance peuvent être ajustés à la phase initiale du concept.

• **Interférence** :

Les niveaux d'interférence présents dans le système sont généralement fixés par des facteurs externes et ne peuvent pas être modifiés par la conception du système. Cependant, il est possible de régler la bande passante du système. En réduisant la largeur de bande du niveau d'interférence peut être réduite. Cependant la réduction de la largeur de bande limite le débit de données pouvant être atteint.

• **Augmentation de la puissance de l'émetteur**

Il est également possible d'augmenter le niveau du système d'alimentation de sorte que la puissance par bit soit augmentée. Cela doit être équilibré en fonction de plusieurs facteurs, l'impact de l'augmentation de la puissance sur la taille de l'amplificateur de puissance e, sur la consommation d'énergie ainsi que sur la durée de vie de la batterie

• **Modulation d'ordre inférieur**

Des régimes d'ordre de modulation plus faibles peuvent être utilisés, mais cela est au détriment du débit de données.

• **Réduire la bande passante**

Une autre approche qui peut être adoptée pour réduire le taux d'erreur binaire est de réduire la bande passante, des niveaux inférieurs de bruit seront reçus et donc le rapport signal sur bruit sera amélioré. Là encore, cela se traduit par une diminution du débit de données réalisables.

Il est nécessaire d'équilibrer l'ensemble des éléments disponibles pour atteindre un taux d'erreur binaire satisfaisant. Normalement, il est impossible de parvenir à toutes les exigences et certains

compromis sont nécessaires. Cependant, même avec un taux d'erreur binaire inférieur à ce qui est nécessaire, idéalement, d'autres compromis peuvent être faits en ce qui concerne les niveaux de correction d'erreur qui sont introduites dans les données transmises. Bien que plus de données redondantes doivent être envoyées à des niveaux plus élevés de correction d'erreur, cela peut aider à masquer les effets de toutes les erreurs de bits qui se produisent, ce qui améliore le taux d'erreur global de bits[137].

Le rapport signal sur bruit de crête PSNR

La fidélité est mesurée par le rapport signal sur bruit de crête, PSNR. Ce qui est généralement exprimé en termes d'échelle logarithmique. Il peut être défini comme suit :

$$PSNR = 10log_{10}(\frac{Peak^2}{MSE})$$

Où MSE est l'erreur quadratique moyenne entre l'image d'origine et l'image reconstruite et le « Peak » est la magnitude maximale possible pour un pixel à l'intérieur de l'image. La valeur de crête est de 255 pour une image de 8 bits/pixel.

Bibliographie

[1] Z.-N. Li, M. S. Drew, and J. Liu, *Fundamentals of multimedia*: Springer, 2004.

[2] H. Ahmadi, F. Viani, and R. Bouallegue, "An accurate prediction method for moving target localization and tracking in wireless sensor networks," *Ad Hoc Networks,* vol. 70, pp. 14-22, 2018.

[3] S. Liu, W. Huang, and Z. Zhang, "Person re-identification using Hybrid Task Convolutional Neural Network in camera sensor networks," *Ad Hoc Networks,* vol. 97, p. 102018, 2020.

[4] S. A. Alvi, B. Afzal, G. A. Shah, L. Atzori, and W. Mahmood, "Internet of multimedia things: Vision and challenges," *Ad Hoc Networks,* vol. 33, pp. 87-111, 2015.

[5] F. Seguel, C. Azurdia-Meza, N. Krommenacker, P. Charpentier, V. Bombardier, and C. Carreño, "Miner video tracking and identification using optical camera communications in a wireless multimedia sensor network," in *2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, 2020, pp. 1-5.

[6] D. G. Costa, "Visual sensors hardware platforms: a review," *IEEE Sensors Journal,* vol. 20, pp. 4025-4033, 2019.

[7] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications," *IEEE Communications Surveys & Tutorials,* vol. 23, pp. 1125-1159, 2021.

[8] M. Z. Hasan, H. Al-Rizzo, and F. Al-Turjman, "A survey on multipath routing protocols for QoS assurances in real-time wireless multimedia sensor networks," *IEEE Communications Surveys & Tutorials,* vol. 19, pp. 1424-1456, 2017.

[9] K. Navin, S. Murugaanandam, S. Nithiya, and S. Sivashankari, "High-End Video Data Transmission in Optimized Routing Framework for Wireless Networks," in *Artificial Intelligence Techniques for Advanced Computing Applications*, ed: Springer, 2021, pp. 391-402.

[10] K. B. Sangeetha and V. Reddy, "A Survey on Performance Comparison of Video Coding Algorithms," in *Soft Computing and Signal Processing*, ed: Springer, 2022, pp. 667-675.

[11] S. Pudlewski, N. Cen, Z. Guan, and T. Melodia, "Video transmission over lossy wireless networks: A cross-layer perspective," *IEEE Journal of Selected Topics in Signal Processing,* vol. 9, pp. 6-21, 2014.

[12] M. Capra, R. Peloso, G. Masera, M. Ruo Roch, and M. Martina, "Edge computing: A survey on the hardware requirements in the internet of things world," *Future Internet,* vol. 11, p. 100, 2019.

[13] A. Bohloulzadeh and M. Rajaei, "A survey on congestion control protocols in wireless sensor networks," *International Journal of Wireless Information Networks,* vol. 27, pp. 365-384, 2020.

[14] A. N. Dhinnesh and T. Sabapathi, "Probabilistic neural network based efficient bandwidth allocation in wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing,* pp. 1-12, 2021.

[15] D. Wu, J. Wang, Y. Cai, and M. Guizani, "Millimeter-wave multimedia communications: challenges, methodology, and applications," *IEEE communications Magazine,* vol. 53, pp. 232-238, 2015.

[16] M. Amjad, M. H. Rehmani, and S. Mao, "Wireless multimedia cognitive radio networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials,* vol. 20, pp. 1056-1103, 2018.

[17] F. H. Awad, "Optimization of relay node deployment for multisource multipath routing in Wireless Multimedia Sensor Networks using Gaussian distribution," *Computer networks,* vol. 145, pp. 96-106, 2018.

[18] Z. Zhang, A. Mehmood, L. Shu, Z. Huo, Y. Zhang, and M. Mukherjee, "A survey on fault diagnosis in wireless sensor networks," *IEEE Access,* vol. 6, pp. 11349-11364, 2018.

[19] Y. Gai, H. Li, and Z. Li, "Self-Healing Functional Electronic Devices," *Small,* vol. 17, p. 2101383, 2021.

[20] N. Li, J.-F. Martínez-Ortega, V. H. Diaz, and J. M. Meneses Chaus, "Probability of Interference-Optimal and Energy-Efficient Analysis for Topology Control in Wireless Sensor Networks," *Applied Sciences,* vol. 6, p. 396, 2016.

[21] G.-M. Su, X. Su, Y. Bai, M. Wang, A. V. Vasilakos, and H. Wang, "QoE in video streaming over wireless networks: perspectives and research challenges," *Wireless networks,* vol. 22, pp. 1571-1593, 2016.

[22] M. Bhalia and A. Bavarva, "Survey on Energy Efficient Approach for Wireless Multimedia Sensor Network," in *Proceedings of Third International Conference on Sustainable Computing*, 2022, pp. 25-34.

[23] E. Zarepour, M. Hassan, C. T. Chou, and A. A. Adesina, "Electromagnetic wireless nanoscale sensor networks," *Emerging Communication Technologies Based on Wireless Sensor Networks: Current Research and Future Applications,* p. 143, 2016.

[24] H. Wang, Y. Qian, and H. Sharif, "Multimedia communications over cognitive radio networks for smart grid applications," *IEEE wireless communications,* vol. 20, pp. 125-132, 2013.

[25] V. Ukani and P. Thakkar, "A Hybrid Video Based IoT Framework for Military Surveillance," *Design Engineering,* pp. 2050-2060, 2021.

[26] J. Jeong and E. Lee, "VCPS: Vehicular cyber-physical systems for smart road services," in *2014 28th International Conference on Advanced Information Networking and Applications Workshops*, 2014, pp. 133-138.

[27] F. Karray, M. W. Jmal, A. Garcia-Ortiz, M. Abid, and A. M. Obeid, "A comprehensive survey on wireless sensor node hardware platforms," *Computer Networks,* vol. 144, pp. 89-110, 2018.

[28] T. Kim, L. F. Vecchietti, K. Choi, S. Lee, and D. Har, "Machine Learning for Advanced Wireless Sensor Networks: A Review," *IEEE Sensors Journal,* 2020.

[29] D. A. Milovanovic, Z. S. Bojkovic, and D. D. Kukolj, "Machine Learning in 5G Multimedia Communications: Open Research Challenges and Applications," in *Research Anthology on Developing and Optimizing 5G Networks and the Impact on Society*, ed: IGI Global, 2021, pp. 204-225.

[30] N. Primeau, R. Falcon, R. Abielmona, and E. M. Petriu, "A review of computational intelligence techniques in wireless sensor and actuator networks," *IEEE Communications Surveys & Tutorials,* vol. 20, pp. 2822-2854, 2018.

[31] www.embeddedcomputing.com. (2021). Available: https://www.embeddedcomputing.com/technology/iot/wireless-sensor-networks/sensor-enabled-nodes-support-the-iot-for-smart-buildings-and-smart-transport

[32] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Dynamic groups and attribute-based access control for next-generation smart cars," in *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*, 2019, pp. 61-72.

[33] J. Li, R. Cheng, J. Zhu, Y. Tian, and Y. Zhang, "Wireless secure communication involving UAV: an overview of physical layer security," in *MATEC Web of Conferences*, 2021, p. 04005.

[34] A. Mahmood, "Adaptive approaches for medical imaging security," 2015.

[35] L. Ngeljaratan and M. A. Moustafa, "Underexposed Vision-Based Sensors' Image Enhancement for Feature Identification in Close-Range Photogrammetry and Structural Health Monitoring," *Applied Sciences*, vol. 11, p. 11086, 2021.

[36] H. M. A. Fahmy, *Concepts, applications, experimentation and analysis of wireless sensor networks*: Springer Nature, 2020.

[37] M. Rahimi, R. Baer, O. I. Iroezi, J. C. Garcia, J. Warrior, D. Estrin, *et al.*, "Cyclops: in situ image sensing and interpretation in wireless sensor networks," in *Proceedings of the 3rd international conference on Embedded networked sensor systems*, 2005, pp. 192-204.

[38] K. Anupama, C. S. S. Reddy, and M. V. Shenoy, "FlexEye—A flexible camera mote for sensor networks," in *2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN)*, 2015, pp. 1010-1015.

[39] P. Singla and A. Munjal, "Topology control algorithms for wireless sensor networks: A review," *Wireless Personal Communications*, vol. 113, pp. 2363-2385, 2020.

[40] A. A. Abba Ari, A. C. Djedouboum, A. M. Gueroui, O. Thiare, A. Mohamadou, and Z. Aliouat, "A three-tier architecture of large-scale wireless sensor networks for big data collection," *Applied Sciences*, vol. 10, p. 5382, 2020.

[41] S. Lohier, A. Rachedi, and Y. Ghamri-Doudane, "A cost function for QoS-aware routing in multi-tier wireless multimedia sensor networks," in *IFIP/IEEE International Conference on Management of Multimedia Networks and Services*, 2009, pp. 81-93.

[42] N. R. Council, *Expanding the vision of sensor materials*: National Academies Press, 1995.

[43] J. Ohta, *Smart CMOS image sensors and applications*: CRC press, 2017.

[44] L. Gao, J. Liang, C. Li, and L. V. Wang, "Single-shot compressed ultrafast photography at one hundred billion frames per second," *Nature*, vol. 516, pp. 74-77, 2014.

[45] R. Mathur, D. N. Chouhan, and T. K. Dubey, "An Overview of Application Scenarios of Voice over Wireless Sensor Networks," *Smart Systems and IoT: Innovations in Computing*, pp. 587-593, 2020.

[46] M. O. Farooq, S. Aziz, and A. B. Dogar, "State of the art in wireless sensor networks operating systems: a survey," in *International Conference on Future Generation Information Technology*, 2010, pp. 616-631.

[47] K. M. Modieginyane, B. B. Letswamotse, R. Malekian, and A. M. Abu-Mahfouz, "Software defined wireless sensor networks application opportunities for efficient network management: A survey," *Computers & Electrical Engineering*, vol. 66, pp. 274-287, 2018.

[48] C. Le Bas, "Système de télésurveillance médicale utilisant la technologie de transmission optique sans fil," Limoges, 2017.

[49] H. A. Alcalá-Garrido, V. Barrera-Figueroa, M. E. Rivero-Ángeles, Y. V. García-Tejeda, and H. R. Pérez, "Analysis and Design of a Wireless Sensor Network Based on the Residual Energy of the Nodes and the Harvested Energy from Mint Plants," *Journal of Sensors*, vol. 2021, 2021.

[50] S. Arnon, "Optical wireless communication in data centers," in *Broadband Access Communication Technologies XII*, 2018, p. 105590J.

[51] M. F. Sanad, A. E. Shalan, S. O. Abdellatif, E. S. A. Serea, M. S. Adly, and M. A. Ahsan, "Thermoelectric energy harvesters: A review of recent developments in materials and devices for different potential applications," *Topics in Current Chemistry*, vol. 378, pp. 1-43, 2020.

[52] R. Morais, S. G. Matos, M. A. Fernandes, A. L. Valente, S. F. Soares, P. Ferreira, *et al.*, "Sun, wind and water flow as energy supply for small stationary data acquisition platforms," *Computers and electronics in agriculture*, vol. 64, pp. 120-132, 2008.

[53] I. Ahmad, L. M. Hee, A. M. Abdelrhman, S. A. Imam, and M. S. Leong, "Scopes, challenges and approaches of energy harvesting for wireless sensor nodes in machine condition monitoring systems: A review," *Measurement*, vol. 183, p. 109856, 2021.

[54] R. S. Rathore, S. Sangwan, O. Kaiwartya, and G. Aggarwal, "Green Communication for Next-Generation Wireless Systems: Optimization Strategies, Challenges, Solutions, and Future Aspects," *Wireless Communications and Mobile Computing*, vol. 2021, 2021.

[55] wsn.cse.wustl.edu. (2021). Available: Intel Mote 2 Engineering Platformhttp://wsn.cse.wustl.edu › Imote2-ds-rev2_2

[56] C. Duran-Faundez, "Transmission d'images sur les réseaux de capteurs sans fil sous la contrainte de l'énergie," Université Henri Poincaré-Nancy I, 2009.

[57] C. Pham, "Low cost wireless image sensor networks for visual surveillance and intrusion detection applications," in *2015 IEEE 12th International Conference on Networking, Sensing and Control*, 2015, pp. 376-381.

[58] I. T. Almalkawi, M. Guerrero Zapata, J. N. Al-Karaki, and J. Morillo-Pozo, "Wireless multimedia sensor networks: current trends and future directions," *Sensors*, vol. 10, pp. 6662-6717, 2010.

[59] S. Zacharias and T. Neve, "Technologies and architectures for multimedia-support in wireless sensor networks," *Smart Wireless Sensor Networks, InTech*, pp. 373-394, 2010.

[60] D. M. Pham and S. M. Aziz, "FlexiS—A Flexible Sensor Node Platform for the Internet of Things," *Sensors*, vol. 21, p. 5154, 2021.

[61] A. Kataria, S. Ghosh, V. Karar, T. Gupta, K. Srinivasan, and Y.-C. Hu, "Improved diver communication system by combining optical and electromagnetic trackers," *Sensors*, vol. 20, p. 5084, 2020.

[62] N. Kenges, E. Ever, and A. Yazici, "Effective Use of Low Power Heterogeneous Wireless Multimedia Sensor Networks for Surveillance Applications Using IEEE 802.15. 4 Protocol," in *35th International Conference on Advanced Information Networking and Applications, AINA 2021*, 2021, pp. 242-251.

[63] A. Kiourtis, A. Mavrogiorgou, and D. Kyriazis, "A Comparative Study of Bluetooth SPP, PAN and GOEP for Efficient Exchange of Healthcare Data," *Emerging Science Journal,* vol. 5, pp. 279-293, 2021.

[64] A. B. Abdallah, "Algorithmes d'optimisation inter-couches pour les réseaux de capteurs sans fil multimédia utilisant la technologie Ultra Wide Band," Conservatoire national des arts et metiers-CNAM; École supérieure des …, 2021.

[65] J. Roja, V. N. Kumar, Y. P. Sai, and S. Reddy, "Implementation of Wi-Fi energy efficient wireless media transmission," *Materials Today: Proceedings,* 2021.

[66] N. S. Kurian, R. Preetha, N. J. Joan, A. Joseph, and M. A. Shree, "LI-FI based Industrial Safety Module," in *2021 5th International Conference on Computing Methodologies and Communication (ICCMC),* 2021, pp. 17-22.

[67] B. A. Vijayalakshmi and M. Nesasudha, "ERPO-OFDM for data transmission and brightness control in visible light communication system," *Optical and Quantum Electronics,* vol. 53, pp. 1-13, 2021.

[68] A. Le Glaunec, "Modulations multiporteuses," *Rapport, Université de Supélec, http://www. supelec-rennes. fr/ren/perso/aleglaun,* 2000.

[69] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM wireless communications with MATLAB*: John Wiley & Sons, 2010.

[70] R. M. Roldán Giraldo, "Quadrature Amplitude Modulated Microware Signal Transmission over a radio-over-f," 2008.

[71] K. Zhang, J. Zhang, G. Gao, and A. Fei, "Physical layer security based on chaotic spatial symbol transforming in fiber-optic systems," *IEEE Photonics Journal,* vol. 10, pp. 1-10, 2018.

[72] M. Pischella and D. Le Ruyet, *Digital Communications 2: Digital Modulations* vol. 2: John Wiley & Sons, 2015.

[73] F. E. Abd El-Samie, *Image encryption: a communication perspective*: CRC Press, 2019.

[74] C.-F. Lin, C.-F. Wu, C.-L. Hsieh, S.-H. Chang, I. A. Parinov, and S. Shevtsov, "Generalized Frequency Division Multiplexing-Based Low-Power Underwater Acoustic Image Transceiver," *Sensors,* vol. 22, p. 313, 2022.

[75] E. Oyekanlu and P. Oladele, "Smart grid communication over DC powerline: Evaluation of powerline communication OFDM PAPR for new types of destabilizing electrical loads," in *2018 First International Colloquium on Smart Grid Metrology (SmaGriMet),* 2018, pp. 1-7.

[76] D. Abed and A. Medjouri, "CS-Based Near-Optimal MUD for Uplink Grant-Free NOMA," *Wireless Personal Communications,* pp. 1-10, 2021.

[77] S. Mekhancha, D. Abed, and A. Boualleg, "Chaotic-precoder based PAPR reduction in MIMO SFBC-OFDM," *International Journal of Electronics Letters,* vol. 9, pp. 140-155, 2021.

[78] A. Hajar, J. M. Hamamreh, M. Abewa, and Y. Belallou, "A spectrally efficient OFDM-based modulation scheme for future wireless systems," in *2019 scientific meeting on electrical-electronics & biomedical engineering and computer science (ebbt),* 2019, pp. 1-4.

[79] M. Ghadi, L. Laouamer, and T. Moulahi, "Securing data exchange in wireless multimedia sensor networks: perspectives and challenges," *Multimedia tools and applications,* vol. 75, pp. 3425-3451, 2016.

[80] H. Hu, H. Zhang, and Y. Yang, "Security risk situation quantification method based on threat prediction for multimedia communication network," *Multimedia Tools and Applications,* vol. 77, pp. 21693-21723, 2018.

[81] I. T. Almalkawi, M. Guerrero Zapata, and J. N. Al-Karaki, "A secure cluster-based multipath routing protocol for WMSNs," *Sensors,* vol. 11, pp. 4401-4424, 2011.

[82] A. Thakkar and R. Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," *Artificial Intelligence Review,* pp. 1-111, 2021.

[83] M. Farajallah, "Chaos-based crypto and joint crypto-compression systems for images and videos," Universite de Nantes, 2015.

[84] C. Lai, P. Cordeiro, A. Hasandka, N. Jacobs, S. Hossain-McKenzie, D. Jose, *et al.*, "Cryptography considerations for distributed energy resource systems," in *2019 IEEE Power and Energy Conference at Illinois (PECI)*, 2019, pp. 1-7.

[85] C. Rathod and A. Gonsai, "A Detailed Comparative Study and Performance Analysis of Standard Cryptographic Algorithms," in *Cyber Security and Digital Forensics*, ed: Springer, 2022, pp. 301-307.

[86] R. Imam, Q. M. Areeb, A. Alturki, and F. Anwer, "Systematic and Critical Review of RSA based Public Key Cryptographic Schemes: Past and Present Status," *IEEE Access,* 2021.

[87] A. S. Shaik, R. K. Karsh, M. Islam, and R. H. Laskar, "A review of hashing based image authentication techniques," *Multimedia Tools and Applications*, pp. 1-28, 2021.

[88] S. Sallam and B. D. Beheshti, "A survey on lightweight cryptographic algorithms," in *TENCON 2018-2018 IEEE Region 10 Conference*, 2018, pp. 1784-1789.

[89] J. M. T. Thompson, H. B. Stewart, and R. Turner, "Nonlinear dynamics and chaos," *Computers in Physics*, vol. 4, pp. 562-563, 1990.

[90] M. Lahcene, "ETUDE ET IMPLEMENTATION SOUS «XILINX SYSTEM GENERATOR» DES CRYPTO-SYSTEMES CHAOTIQUES POUR SECURISER LES SYSTEMES DE COMMUNICATIONS MODERNES," Universite mohamed boudiaf'des sciences et de la technologie d'oran, 2010.

[91] W. Greiner, "Lyapunov exponents and chaos," in *Classical Mechanics*, ed: Springer, 2010, pp. 503-516.

[92] S. L. De Souza and I. L. Caldas, "Calculation of Lyapunov exponents in systems with impacts," *Chaos, Solitons & Fractals,* vol. 19, pp. 569-579, 2004.

[93] P. Góra, A. Boyarsky, and Y. Lou, "Lyapunov exponents for higher dimensional random maps," *Journal of Applied Mathematics and Stochastic Analysis,* vol. 10, pp. 209-218, 1997.

[94] O. Megherbi, "Etude et réalisation d'un système sécurisé à base de systèmes chaotiques," Université Mouloud Mammeri, 2013.

[95] D. Eroglu, J. S. Lamb, and T. Pereira, "Synchronisation of chaos and its applications," *Contemporary Physics,* vol. 58, pp. 207-243, 2017.

[96] L. Messaouda, "Contrôle et synchronisation de quelques types de systèmes dynamiques chaotiques," Abdelhafid boussouf university Centre mila, 2020.

[97] B. Chandrika and S. S. Tangade, "Chaotic modulation and demodulation techniques: a survey," *International Journal for Technological Research in Engineering,* vol. 2, 2015.

[98] F. S. Almehmadi, *Secure chaotic transmission of digital and analog signals under profiled beam propagation in acousto-optic Bragg cells with feedback*: University of Dayton, 2015.

[99] M. Zhang and Y. Wang, "Review on chaotic lasers and measurement applications," *Journal of Lightwave Technology,* vol. 39, pp. 3711-3723, 2021.

[100] L. Kocarev and S. Lian, *Chaos-based cryptography: Theory, algorithms and applications* vol. 354: Springer, 2011.

[101] Z. Hua and Y. Zhou, "Nonlinear chaotic processing model," *arXiv preprint arXiv:1612.05154,* 2016.

[102] Y. Zhou, L. Bao, and C. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal processing,* vol. 93, pp. 3039-3052, 2013.

[103] Y. Zhou, Z. Hua, C.-M. Pun, and C. P. Chen, "Cascade chaotic system with applications," *IEEE transactions on cybernetics,* vol. 45, pp. 2001-2012, 2015.

[104] Z. Hua, Y. Zhou, C.-M. Pun, and C. P. Chen, "Image encryption using 2D Logistic-Sine chaotic map," in *Systems, Man and Cybernetics (SMC), 2014 IEEE International Conference on*, 2014, pp. 3229-3234.

[105] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Information Sciences,* vol. 339, pp. 237-253, 2016.

[106] Z. Hua, Y. Wang, and Y. Zhou, "Image cipher using a new interactive two-dimensional chaotic map," in *Systems, Man, and Cybernetics (SMC), 2015 IEEE International Conference on*, 2015, pp. 1804-1808.

[107] Y. Zhou, L. Bao, and C. P. Chen, "A new 1D chaotic system for image encryption," *Signal processing,* vol. 97, pp. 172-182, 2014.

[108] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Optics & Laser Technology,* vol. 101, pp. 30-41, 2018.

[109] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Computers in biology and medicine,* vol. 72, pp. 170-184, 2016.

[110] X. Chai, Z. Gan, and M. Zhang, "A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion," *Multimedia Tools and Applications,* vol. 76, pp. 15561-15585, 2017.

[111] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and chaos,* vol. 8, pp. 1259-1284, 1998.

[112] R. B. Naik and U. Singh, "A Review on Applications of Chaotic Maps in Pseudo-Random Number Generators and Encryption," *Annals of Data Science,* pp. 1-26, 2022.

[113] E. L. Mohaisen and R. S. Mohammed, "Stream cipher based on chaotic maps," in *2019 First International Conference of Computer and Applied Sciences (CAS)*, 2019, pp. 256-261.

[114] F. Özkaynak, "On the effect of chaotic system in performance characteristics of chaos based s-box designs," *Physica A: Statistical Mechanics and its Applications,* vol. 550, p. 124072, 2020.

[115] univlille1. (2001). *Les codes du futur - Projet Enigma*. Available: https://www.fil.univlille1.fr/~wegrzyno/Enigma_La_Coupole_2001/enigma/futur.html

[116] M. H. Al Hasani and K. A. Al Naimee, "Impact security enhancement in chaotic quantum cryptography," *Optics & Laser Technology,* vol. 119, p. 105575, 2019.

[117] T. Seuti, M. Al Mamun, and A. Sarowar Sattar, "Enhanced Steganography Technique via Visual Cryptography and Deep Learning," in *Proceedings of the International Conference on Big Data, IoT, and Machine Learning*, 2022, pp. 623-636.

[118] R. Baublienė, "Chaotinė vizualinė kriptografija," Kauno technologijos universitetas, 2015.

[119] V. F. Signing, G. G. Tegue, M. Kountchou, Z. Njitacke, N. Tsafack, J. Nkapkop, *et al.*, "A cryptosystem based on a chameleon chaotic system and dynamic DNA coding," *Chaos, Solitons & Fractals,* vol. 155, p. 111777, 2022.

[120] C. Cachin, "An information-theoretic model for steganography," in *International Workshop on Information Hiding*, 1998, pp. 306-318.

[121] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing,* vol. 335, pp. 299-326, 2019.

[122] M. Fortrini, "Steganography and digital watermarking: A global view," *University of California, Davis.[Электронный ресурс].–Режим доступа: http://www-lia. deis. unibo. it/Courses/RetiDiCalcolatori/Progetti00/fortini/project. pdf, свободный (дата обращения: 11.12. 2014),* 2014.

[123] H. Kaur and J. Rani, "A Survey on different techniques of steganography," in *MATEC Web of Conferences*, 2016, p. 02003.

[124] M. Rakhra, R. Kumar, and H. Walia, "A Review on Data hiding using Steganography and Cryptography," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, 2021, pp. 1-4.

[125] R. Joshi, M. C. Trivedi, A. K. Gupta, and P. Tripathi, "Current Trends in Cryptography, Steganography, and Metamorphic Cryptography: A Survey," in *Advances in Computational Intelligence and Communication Technology*, ed: Springer, 2021, pp. 237-247.

[126] S. Lian, *Multimedia content encryption: techniques and applications*: Auerbach Publications, 2008.

[127] F. E. Abd el-Samie, H. E. H. Ahmed, I. F. Elashry, M. H. Shahieen, O. S. Faragallah, E.-S. M. El-Rabaie, *et al.*, *Image encryption: a communication perspective*: CRC Press, 2013.

[128] R. Qumsieh, M. Farajallah, and R. Hamamreh, "Joint block and stream cipher based on a modified skew tent map," *Multimedia Tools and Applications,* vol. 78, pp. 33527-33547, 2019.

[129] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT),* vol. 1, pp. 31-38, 2011.

[130] W. Zhang, C. Zhang, C. Chen, and K. Qiu, "Experimental demonstration of security-enhanced OFDMA-PON using chaotic constellation transformation and pilot-aided secure key agreement," *Journal of Lightwave Technology,* vol. 35, pp. 1524-1530, 2017.

[131] A. Bouchemel, D. Abed, and A. Moussaoui, "Enhancement of Compressed Image Transmission in WMSNs Using Modified $\mu $-Nonlinear Transformation," *IEEE Communications Letters*, vol. 22, pp. 934-937, 2018.

[132] A. Shokouh Saljoughi and H. Mirvaziri, "A new method for image encryption by 3D chaotic map," *Pattern Analysis and Applications*, vol. 22, pp. 243-257, 2019.

[133] C. Guyeux, "Le désordre des itérations chaotiques et leur utilité en sécurité informatique," Université de Franche-Comté, 2010.

[134] W. Liu, K. Sun, Y. He, and M. Yu, "Color Image Encryption Using Three-Dimensional Sine ICMIC Modulation Map and DNA Sequence Operations," *International Journal of Bifurcation and Chaos*, vol. 27, p. 1750171, 2017.

[135] X. Wang, Z. Yan, R. Zhang, and P. Zhang, "Attacks and defenses in user authentication systems: A survey," *Journal of Network and Computer Applications*, p. 103080, 2021.

[136] V. Reshma, S. J. Gladwin, and C. Thiruvenkatesan, "Pairing-free cp-abe based cryptography combined with steganography for multimedia applications," in *2019 international conference on communication and signal processing (ICCSP)*, 2019, pp. 0501-0505.

[137] A. Agarwal, B. S. Kumar, and K. Agarwal, "BER Performance Analysis of Image Transmission Using OFDM Technique in Different Channel Conditions Using Various Modulation Techniques," in *Computational Intelligence in Data Mining*, ed: Springer, 2019, pp. 1-8.