République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université 8Mai 1945 – Guelma
Faculté des Sciences et de la Technologie
Département d'Electronique et Télécommunications

Mémoire de Fin d'Etude

Pour l'Obtention du Diplôme de Master Académique

Domaine : **Sciences et Techniques**
Filière : **Télécommunications**
Spécialité : **Réseaux et Télécommunications**

Etude et simulation d'un système de cryptage d'images à base de chaos

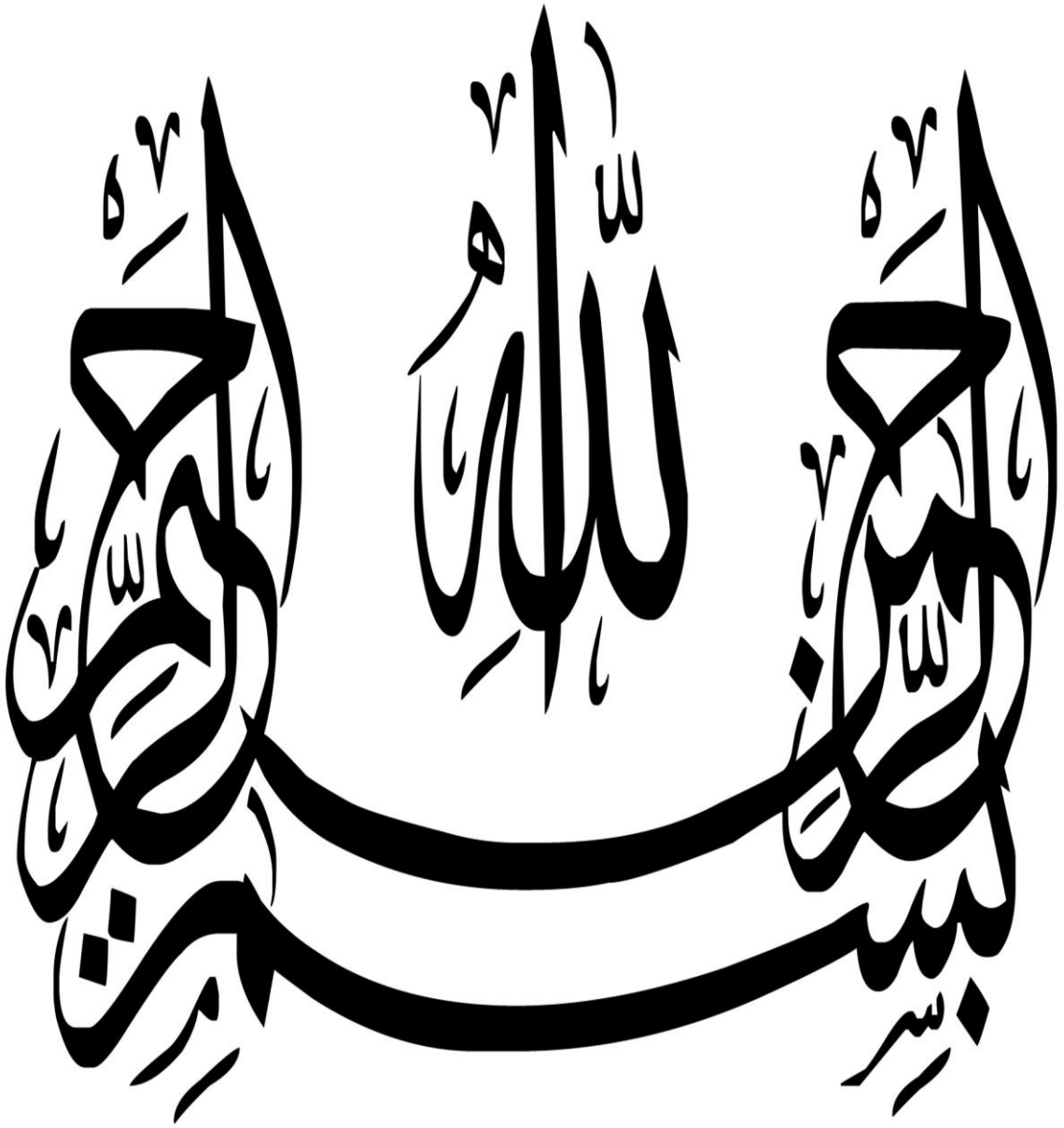
---

Présenté par :

Agaguena Houdjatoulah
Tifouti Miloud

Sous la direction de :
Dr. Bouchemel Ammar

Juin 2023


بسم الله الرحمن الرحيم

قال الله تعالى:

"وقل ربي زدني علما"

سورة طه 114

A mes chers parents. . .
A mes sœurs et frères. . .

A mes amies Mouloud, Oussama, Ibtissem, Dounia et Manel . . .
A tous ceux qui me sont chers. . .

Remerciements

Nous remercions Dieu le Tout Puissant de nous avoir accordé la santé, la volonté et le pouvoir d'entamer et d'achever ce travail.

Et qui ne remercie pas les gens ne remercie pas le bon Dieu

Primo, nous remercions celui qui a été derrière ce travail Monsieur ***Bouchemel Ammar*** *pour ses précieux conseils et son suivi attentif et enrichissant.*

Secundo, nos remerciements vont également aux ***membres du jury*** *pour avoir accepté de juger notre modeste travail.*

Finalement, nous remercions toute personne qui a participé de près ou de loin à l'accomplissement de ce travail, messieurs et mesdames enseignants qui ont veillé à notre formation, à nos collègues avec qui nous avons fait notre cursus universitaire.

Table des Matières

***Chapitre I* : Généralités sur l'image numérique**

Chapitre II Généralité sur la Cryptographie

Liste des Figures

Liste des Tableaux:

Liste des Abréviations

AES: Advanced Encryption Standard
DES: Data Encryption Standard
RSA: nommé par les initiales de ses trois inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman
NPCR: Number of Picture Change Rate
UACI: Unified Average Changing Intensity
PWLCM: Piecewise Linear Chaotic Maps

Introduction générale

Introduction Générale

La cryptographie est une technique permettant à un individu de sécuriser la transmission d'une information à un destinataire, de sorte que cette information ne soit compréhensible que par ce dernier (théoriquement). Dans le passé, l'information était chiffrée ou cryptée à l'aide d'un algorithme spécifique et d'une clé confidentielle, puis déchiffrée en utilisant le même algorithme et la même clé.

Le développement des technologies logicielles et matérielles informatiques représente un danger pour la sécurité des données et des informations confidentielles, telles que les images médicales, ce qui nous pousse à rechercher de nouvelles techniques de protection. De plus, la transmission et le transfert d'images dans l'espace libre et en ligne sont encore insuffisamment protégés, et les techniques de sécurité standard telles que le chiffrement ne conviennent pas aux cas particuliers des images médicales.

Le cryptage d'images est un processus de conversion de l'image originale en une forme inintelligible, compréhensible uniquement par les parties autorisées après avoir effectué une opération de décryptage à l'aide d'une clé secrète. Le cryptage des images est une tâche difficile en raison de la grande quantité de données qu'elles contiennent et de la corrélation entre les pixels, ce qui limite l'utilisation des algorithmes de cryptage traditionnels.

Ainsi, pour obtenir une efficacité et une robustesse contre la violation de la sécurité lors de la transmission des images, les techniques de cryptage d'images basées sur le chaos sont plus appropriées. Ces techniques sont considérées comme plus efficaces en raison de leur faible puissance de calcul et de leur grande sensibilité aux conditions initiales.

L'objectif principal de ce mémoire est de proposer l'utilisation de deux algorithmes basés sur deux cartes chaotiques unidimensionnelles (1D) pour le cryptage des images en niveaux de gris. Les cartes chaotiques 1D considérées dans ce mémoire pour générer une clé aléatoire sont la carte Logistique, la carte Tent et la carte chaotique linéaire par morceaux PWLCM (PiecewiseLinearChaoticMaps). Nous présenterons une étude comparative des performances entre ces deux générateurs de clé afin de sélectionner la carte chaotique qui offre le meilleur niveau de sécurité. Les critères de performances pris en compte pour la comparaison sont l'espace de clé, l'histogramme, l'entropie, cross corrélation et NPCR et UACI.

Ce mémoire est composé de trois chapitres.

Dans le premier chapitre, nous aborderons la discussion sur les images numériques.

Dans Le deuxième chapitre sera une brève introduction aux notions générales de cryptographie, ainsi qu'aux techniques de cryptographie. Nous discuterons également du chaos et de ses propriétés, et présenterons le cryptage d'images à partir de cartes chaotiques unidimensionnelles (1D).

Le troisième chapitre sera consacré à l'application que nous avons réalisée dans le cadre de ce projet, en présentant des exemples et des résultats expérimentaux sur des images synthétiques et médicales.

Chapitre 01
Généralités sur l'image numérique

I.1. Introduction

En raison de l'importance des images numériques et de la valeur des informations qu'elles contiennent, dans ce chapitre, nous allons référer aux concepts de base de l'imagerie à travers les types des images numériques. Ensuite, nous allons parler des méthodes de codage des couleurs dans les images. Puis nous allons parler des formats les plus importantes et les plus célèbres. Enfin nous allons parler des formats les plus importantes de l'imagerie médicale en particulier.

I.2. Notions de base sur l'imagerie

I.2.1. L'image numérique

Une image numérique est une mosaïque de points unicolores (pixels) [1], et peut être définie comme une fonction bidimensionnelle, $f(x, y)$, où x et y sont des coordonnées spatiales (plan) pour chaque pixel [2], Ces pixels seront affectés de nombres binaires permettant de définir des teintes de gris ou des couleurs [3].

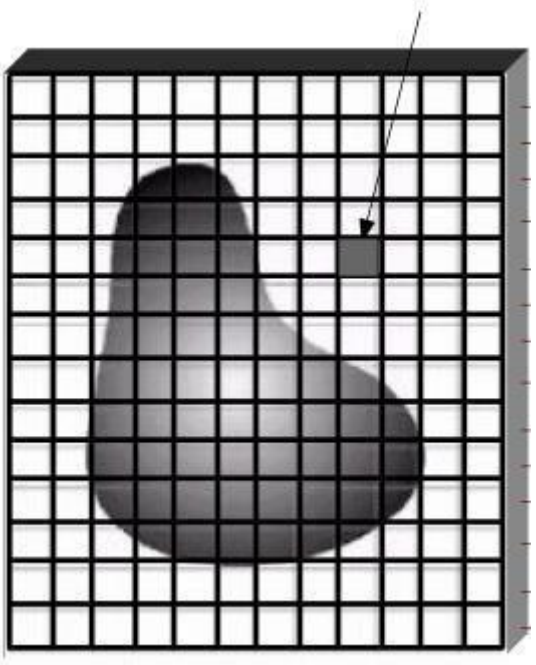


Figure I.1 : Image numérique [4].

I.2.2. Pixel

Les composants élémentaires d'image sont des points appelés pixels (abréviation de PICture Element) pour former une image. Le pixel représente ainsi le plus petit élément constitutif d'une image numérique. L'ensemble de ces pixels est contenu dans un tableau à deux dimensions constituant l'image [5], et chaque pixel à sa propre couleur (valeur).

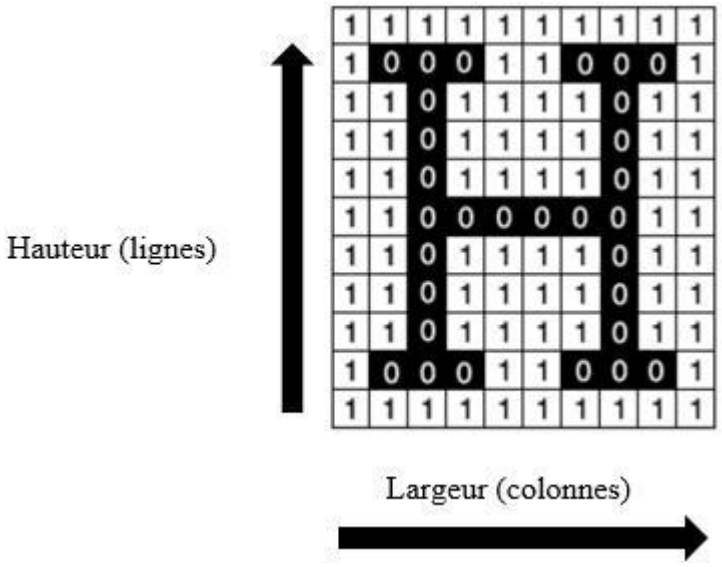


Figure I.2 : Distribution des pixels par lignes et colonnes [6].

I.2.3. Définition

La définition est le nombre de pixels constituants l'image [3].

I.2.4. La taille

La taille de l'image est la place qu'elle occupe dans le codage binaire. Son unité est « L'octet » [3].

Taille = nombre d'octets pour chaque pixel × définition

I.2.5. Résolution

La résolution d'une image est définie par le nombre de pixels par unité de longueur **dpi** (**d**ot **p**er **i**nch = point d'encre par pouce) pour une imprimante ou (**ppp** = **p**ixels **p**ar **p**ouce pour un fichier image). Cette résolution dépendra de la qualité de la numérisation.

Résolution =Définition / Longueur

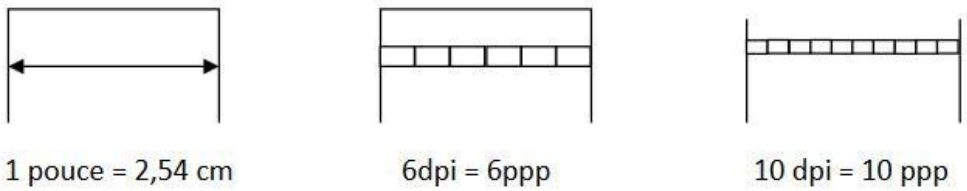


Figure I.3 : Explication de résolution d'une image [3].

I.3. Les différents types d'image

Il existe deux types d'images numériques :

I.3.1. Matricielle (bitmap)

Formée d'une grille composée de pixels. Plus on zoom, plus les pixels deviennent

apparents [6]. Les formats d'images bitmap : BMP, PCX, GIF, JPEG, TIFF. Les photos numériques et les images scannées sont de ce type [7].

I.3.2. Vectorielle

Formée de lignes calculées de manière géométrique. Lors d'un zoom avant ou arrière, la forme est recalculée en fonction de notre position sans perdre de qualité [6].

Le processeur est chargé de "traduire" ces formes en informations interprétables par la carte graphique (images Word, Publisher, CorelDraw - format WMF, CGM, etc.)

Les avantages d'une image vectorielle : les fichiers qui la composent sont petits, les redimensionnements sont faciles sans perte de qualité.

Les inconvénients : une image vectorielle ne permet de représenter que des formes simples. Elle n'est pas donc utilisable pour la photographie notamment pour obtenir des photos réalistes [7].

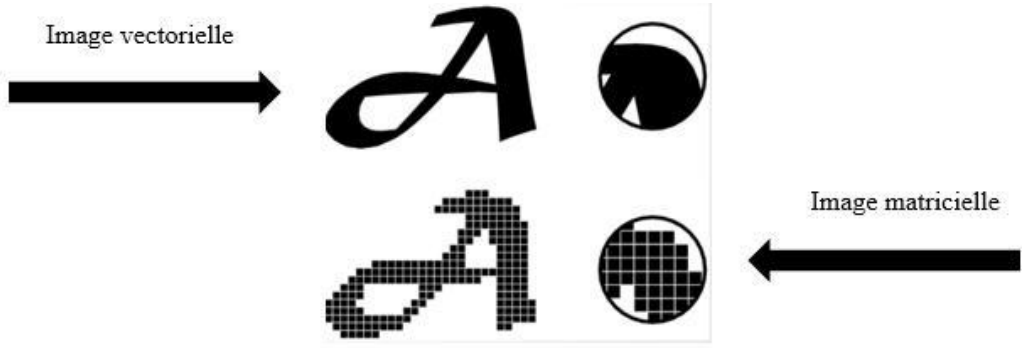


Figure I.4 : Différence entre image vectorielle et image matricielle [6].

I.4. Les différents modes de couleurs des images

I.4.1. Mode binaire

Appelé aussi Mode bitmap (noir et blanc) : Avec ce mode, il est possible d'afficher uniquement des images en deux couleurs pour chaque pixel : noir et blanc. Il utilise une seule couche [5].

- Codage en 1 bit par pixel (bpp) : 2^1= 2 possibilités : [0,1].

1	1	1	1	1	1	1	1	1	1
1	1	1	0	0	0	0	1	1	1
1	1	0	1	1	1	1	0	1	1
1	0	1	1	1	1	1	1	0	1
1	0	1	0	1	1	0	1	0	1
1	0	1	1	1	1	1	1	0	1
1	0	1	0	1	1	0	1	0	1
1	0	1	1	0	0	1	1	0	1
1	1	0	1	1	1	1	0	1	1
1	1	1	0	0	0	0	1	1	1
1	1	1	1	1	1	1	1	1	1

Figure I.5 : Codage binaire (0,1) [5].

Figure I.6 : Image codée en binaire**.**

I.4.2. Mode niveau de gris

I.4.2. Mode niveau de gris

A chaque pixel codé en n bits est affecté un nombre binaire variant de «0 » (pour le noir) à «2n -1 » (pour le blanc), avec n le nombre de bits pour chaque pixel.

Il y aura alors «2^n » niveaux de gris.

Si le codage se fait en 8 bits par pixel, il y aura : 2^n =2^8 =256 niveaux de gris allant du blanc au noir.Si le codage se fait en 16 bits par pixel, il y aura : 2^n =2^{16}=65536 niveaux de gris allant du blanc au noir [3].

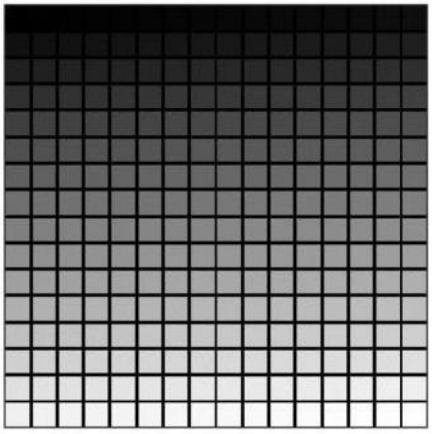


Figure I.7 : Nuance de 256 gris [5].

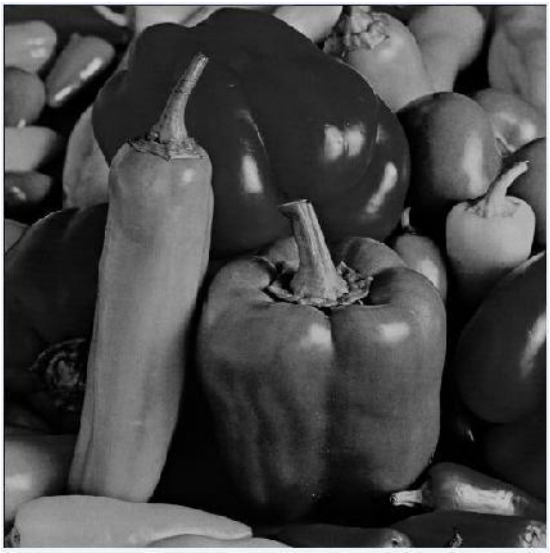


Figure I.8 : Image codée en niveau de gris**.**

I.4.3. Mode couleurs indexées

Permet d'obtenir jusque 256 couleurs fixes, définies à l'avance dans une palette. Il n'utilise qu'une seule couche [5].

Codage en 8 bits par pixel (bpp) : 28 =256 possibilités.

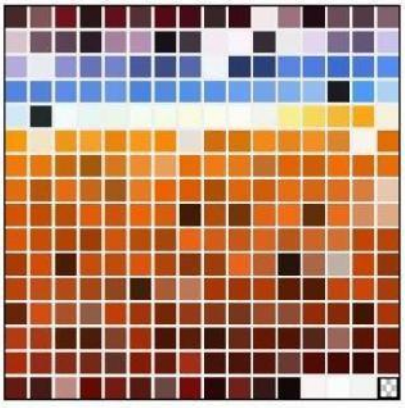


Figure I.9 : Palette de 256 couleurs utilisées [5].

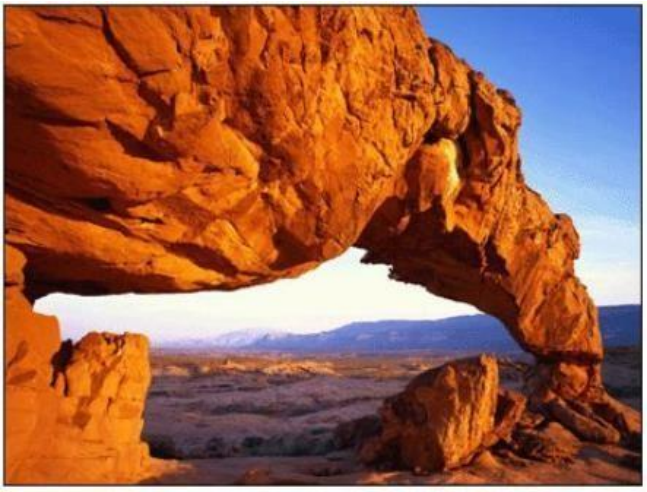


Figure I.10 : Image codée en couleurs indexées [5].

I.4.4. Les modes colorimétriques RVB / CMJN

Afin de créer des images encore plus riches en couleurs (et donc disposer de plus qu'une palette limitée à 256 couleurs), l'idée de mélanger des couleurs primaires en « couches » est arrivée [5].

Il existe deux systèmes de représentation des couleurs par mélange, selon qu'on les reproduit sur un écran d'ordinateur ou sur support papier via une imprimante :

Figure I.11 : Les deux modes colorimétriques [5].

I.4.4.1. Mode couleur RVB (lumière éteinte)

Grâce au mélange des 3 couches de couleur (Rouge, Vert, Bleu), il est possible de reproduire un plus grand nombre de nuances qu'avec une palette en mode couleurs indexées [5].

Avec un codage en RVB 8 bits par couche :

Chaque couche utilise 8bits (1 octet), soit 256 nuances possibles : 8 bits pour le Rouge, 8 bit pour le Vert et 8 bits pour le Bleu.

Donc utilisation de 3 x 8 bits = 24 bits utilisées au total.
=> 256 x 256 x 256 = 2^{24} = 16,7milions possibles

Avec un codage en RVB 16 bits par couche :

Chaque couche utilise le double, soit 16 bits (65535 nuances). 3 x 16 = 48bits utilisées au total. => 65535 x 65535 x 65535 = 4 milliards possibles !

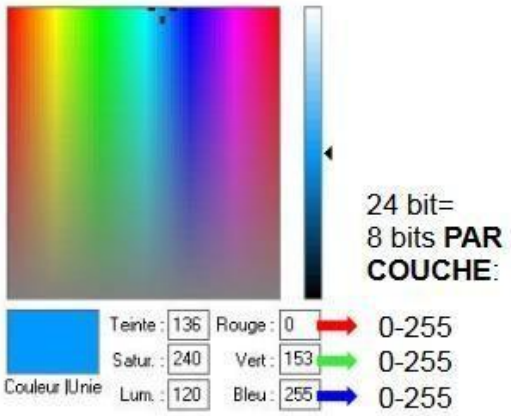


Figure I.12 : Le mode RVB [5].

Figure I.13 : Image codée en couleurs [5].

I.4.4.2. Mode couleur CMJN (support papier)

Comme les écrans d'ordinateur ne peuvent afficher que du RVB, Photoshop sépare les images CMJN en 4 couches (Cyan, Magenta, Jaune et Noir ou chaque couleur est exprimée en pourcentage) et converti le tout en RVB pour être affiché sur l'écran. Cependant pour L'utilisateur, le fichier possède bien 4 couches distinctes sur lesquels il est possible de travailler [5].

Avec un codage en CMJN 8 bits par couche :

Chaque couche utilise 8 bits (soit 256 nuances possibles) : 8 bits pour le Cyan, 8 bits pour le Magenta, 8 bits pour le Jaune et 8bits pour le Noir. Donc utilisation de 4 x 8 bits = 32 bits utilisées au total.

=> 256 x 256 x 256 x 256 = 2^{32}= 4 milliards possibles

Avec un codage en CMJN 16 bits par couche :

Chaque couche utilise le double, soit 16 bits (65535 nuances). 4 x 16 = 64 bits utilisées au total. => 65535 x 65535 x 65535 x 65535 = 264 possibilités

I.5. Format d'enregistrement d'une image

Les formats des images ont une relation avec le type d'image lui-même

I.5.1. Les formats matriciels

Nom du format	Points forts	Points faibles	Note
JPEG **JPEG 2000** **J**oint **P**hotographic **E**xperts **G**roup	Compression Excellente	Compression destructrice	Spécialement conçu pour les photographies, il est cependant à utiliser avec délicatesse tant sa compression peut brouiller l'image. Le format JPEG2000, évolution du format original, peut être réglé pour compresser sans pertes**.**
GIF (**G**raphical **I**nterchange **F**ormat)	Possibilité d'animation et de transparence compression efficace	Limité à 256 couleurs	Très répandu sur le Web malgré ses faiblesses et un problème de droit sur son format de compression. À déconseiller pour les photos
PNG (**P**ortable **N**etwork **G**raphics)	Compression Excellente sans perte. Possibilité de transparence. Standard donc pérenne.	Pas très efficace pour les larges photographies	Format destiné à remplacer le format GIF et ses limitations, mais ayant encore du mail à s'implanter dans les habitudes des développeurs. Peut remplacer les JPEG comme les GIF (sauf en ce qui concerne l'animation)**.**
TIFF (**T**agged **I**mage **F**ile **F**ormat)	Compression sans perte efficace. Couche de transparence	Lourdeur des fichiers non compressés. Format propriétaire.	Format de stockage très utilisé, à éviter pour le Web
BMP (**B**it**ma**p)	Format par défaut de Windows	Disponible uniquement sur la plateforme de Microsoft	Généralement non compressé et de ce fait des fichiers très « lourds »

Table 1.1 : Les formats matriciels [7].

I.5.2. Les formats vectoriels

Nom du format	Points forts	Points faibles	Note
AI (**A**dobe **I**llustrator)	Reconnu par tous les logiciels graphiques	Format propriétaire.	Format standard d'Adobe Illustrator, l'un des plus utilisés du fait de la popularité du logiciel.
PS/EPS (**P**ost**s**cript / **E**ncapsulated **P**ost**s**cript)	Très bien reconnu sur tous les systèmes.	N'a d'intérêt que dans le cadre d'une impression. Fichier très lourd.	Format hybride bitmap/vectoriel, réservé à l'impression. EPS est un fichier PS qui comporte quelques restrictions supplémentaires.
SVG (**S**calable **V**ector **G**raphics)	Format XML donc extensible. Très compressible car format texte. Standard donc pérenne. Permet les animations et la transparence. Peut afficher des images bitmap.	Encore très peu reconnu, car peu d'outils disponibles et manque d'implémentation au sein de navigateurs (besoin d'un plugin).	Promis à un grand avenir malgré un démarrage lent, ce format est souvent cité comme capable de rivaliser avec les premières versions de Flash.
FLA/SWF (Flash)	Très polyvalent, peut utiliser des mp3, des JPEG, des vidéos... Très répandu sur le Web.	Format propriétaire et fermé.	C'est le standard de fait des animations vectorielles sur le Web.
PDF (**P**ortable **D**ocument **F**ormat)	Affiche les documents	Taille prohibitive. Ne peut se lire qu'avec le logiciel Acrobat ou logiciel équivalent.	Version simplifiée de PostScript, il a été conçu pour afficher les documents de la même manière quel que soit le système.
PICT (**Pict**ure)	Format par défaut de Mac OS, donc encore	Disponible uniquement sur la plateforme	N'a plus grand intérêt face aux autres formats existants.

Table 1.2 : Les formats vectoriels [7].

I.5.3. Formats des images médicales

Le standard DICOM (Digital **I**maging and **C**ommunication in **M**edicine**),** Créé en 1985 par :

- l' ACR (American College of Radiology)
- la NEMA (National Electric Manufacturers Association) Les caractéristiques les importants :
  - Standardiser les données transmises entre les différents appareils de radiologie.
  - Format de fichier + protocole de transmission des données (basé sur TCP/IP).
  - Faciliter les transferts d'images entre les machines de différents constructeurs. Eviter d'avoir pour chaque constructeur de matériel d'imagerie un format de données

propriétaire (incompatibilités, coût, perte d'information). Tout numérique possible :

- Pour éviter le tirage des clichés sur papier argentique
- Pour diminuer le coût d'une radiographie.
- Amélioration du suivi médical des patients (transfert d'un établissement de santé à un autre).

Les images au format **DICOM** accompagnant les dossiers médicaux sont lisibles sur tout matériel informatique compatible.

La sécurisation des échanges, via un service appelé "accord de stockage", et différents mécanismes de signature des documents, et la cohérence du rendu des images [8].

I.5.3.1. Les standards de compression

Les standards en compression de données peuvent être classés en deux catégories :

- Ceux qui ne font aucune hypothèse sur la nature des données.
- Ceux qui s'appuient sur une organisation spatio-temporelle particulière (image 2D ou suite d'images 2D).

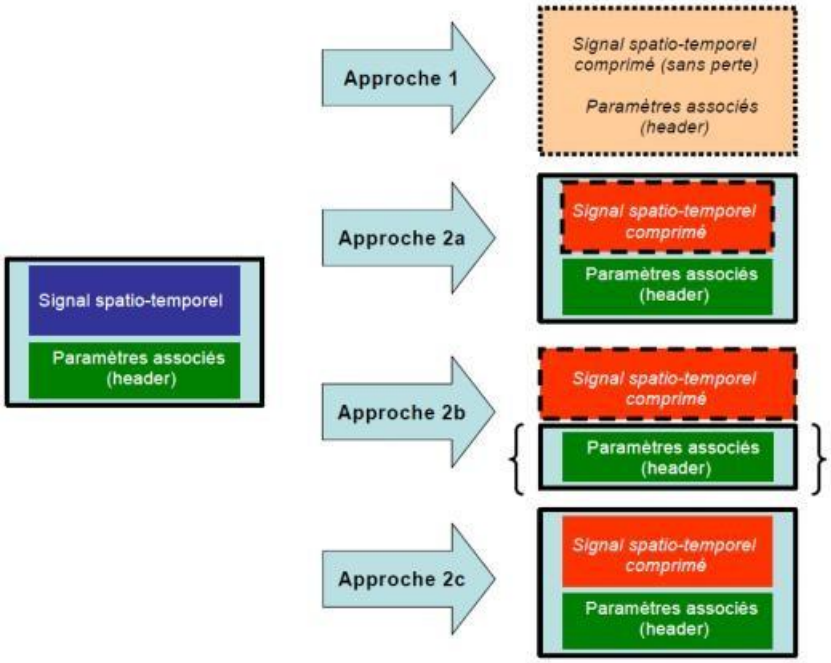


Figure I.14 : Approches généralistes et spécifiques pour la compression d'image [8].

Les avantages et les inconvénients :

	Avantage	**Inconvénients**
Approche 1 "compression généraliste" (ex : gzip, compress)	Généricité Facilité de mise en œuvre Coût très faible	Performances faibles
Approche 2a "compression d'image généraliste" par encapsulation (ex : JPEG, MPEG)	Réutilisation d'implémentations existants pour la compression/ décompression et la virtualisation des images Performances très optimisées Prise en compte du contexte médical (*header* contenant le nom du patient, les paramètres d'acquisition, etc.)	Eventuellement inadaptée à des données très spécifique, ou performances sub-optimales
Approche 2b "compression d'image généraliste" (ex : JPEG, MPEG)	Facilite la diffusion la plus large (hors des services spécialisés, et vers le grand public), au moindre coût (navigateur web)	Pas de prise en compte du contexte médical (*header*)

Approche 2c "compression d'image spécifique"	Peut permettre d'obtenir des performances optimales, découlant d'une très bonne adéquation à la structure des données	Coût de développement inhérent au caractère spécifique

Table 1.3 : Avantages et inconvénients des standards généralistes et standards spécifiques [8].

I.6 Imagerie médicale

L'imagerie médicale fait référence à plusieurs technologies différentes qui sont utilisées pour visualiser le corps humain afin de diagnostiquer, surveiller ou traiter des conditions médicales. Toutes les modalités d'imagerie ont en commun que la condition médicale devient visible par une certaine forme de contraste, ce qui signifie que la caractéristique d'intérêt (telle qu'une tumeur) peut être reconnue dans l'image et examinée par un radiologue qualifié [9].

I.6.1 Imagerie analogique et imagerie numérique

Il existe deux façon de représenter les information [10] :

I.6.2 L'imagerie analogique

La façon analogique qui La façon analogique qui représente l'information comme une quantité physique continue, il faut savoir que les phénomènes qui nous entourent sont quasiment tous continuent et l'lorsqu'un support peut prendre des valeurs continuent comme par exemple une cassette vidéo audio.

I.6.3 L'imagerie numérique

On peut numériser les images (digitalisation en anglais), c'est à dire transformer l'information initiale en une matrice de nombre. On peut donc passer d'une image analogique à une image numérique par la numérisation.

Dans la numérisation, il y a deux étapes :

1. **Un codage spatial (échantillonnage spatial) :** L'image va d'abord être divisée en pixels (Picture elements) qui sont des petites surfaces élémentaires de l'image. Lorsque l'on est en présence d'une image de côté N et M, on aura une image divisée en NxM pixels.
2. **Un codage en intensité (quantification) :** Dans chaque pixel on va pouvoir mettre un nombre qui correspond à la valeur moyenne de l'intensité en ce point

   On se retrouve alors avec une matrice de nombre qui comprend la totalité des renseigne- ments nécessaires. On enregistre donc ces nombres à l'aide d'ordinateurs

(Ainsi l'imagerie médicale c'est beaucoup développée parallèlement au développement des ordinateurs), on est alors capable de retranscrire cette matrice de nombre en une image visuelle. Pour ce faire, on associe chaque nombre enregistré à un niveau de gris. On a donc une intensité qui varie par palier, les images numériques contiennent donc une information discrète et non continue.

I.6.4 Différents type d'imagerie médical

Un service d'imagerie de nos jours est constitué d'une multitude de modalités que nous citerons ci-dessous.

Tomodensitométrie (TDM) : Cette procédure d'imagerie utilise est une modalité d'imagerie volumétrique basée sur l'absorption des rayons X. la TDM permet la reconstruction d'une carte d'absorbeur en deux ou trois dimensions.

La tomodensitométrie dépasse largement l'imagerie par rayons X par projection dans le contraste des tissus mous, mais la résolution spatiale d'un tomodensitogramme (scanner) clinique du corps entier est nettement inférieure à celle de l'imagerie par rayons X simple. Néanmoins, la tomo- densitométrie peut révéler de petites tumeurs, des détails structures dans l'os trabéculaire ou le tissu alvéolaire des poumons [9].

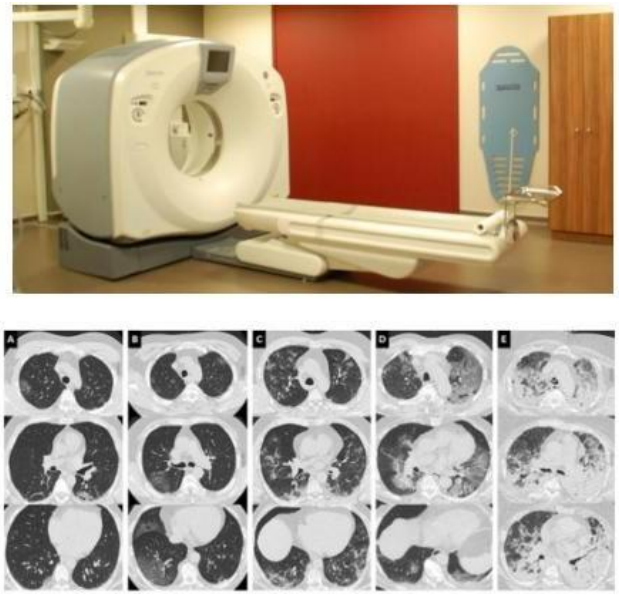


Figure I .15: Schéma d'un scanner (en haut) et un échantillon d'images (en bas) [11].

Radiographie : est la plus ancienne modalité d'imagerie médicale, qui a trouvé sa place dans la pratique médicale peu de temps après la découverte des rayons X en 1895. Les rayons X sont des photons de haute énergie, et l'interaction atomique avec les électrons de

la couche interne est fondamentale à la fois pour la production de rayons X et la génération de contraste de rayons X. Le contraste des tissus mous est relativement faible, mais l'os et l'air offrent un excellent contraste. Les images aux rayons X peuvent révéler des caractéristiques très subtiles, mais ont des effets très nocifs sur la santé pour des durées d'exposition longues ou répétées et/ou pour de fortes intensités.

L'imagerie par rayons X est utilisée pour diagnostiquer les fractures osseuses, les maladies pulmonaires, Etc[12].

Figure I.16: Schéma d'un système de radiographie (à gauche) [13]et un échantillon d'images radio-graphiques (à droite) [11].

L'imagerie par résonance magnétique (IRM) : Est une modalité d'imagerie volumétrique parallèle, dans une certaine mesure, à la tomodensitométrie. Cependant, les principes physiques sous-jacents sont fondamentalement différents de la TDM. La où la tomodensitométrie utilise des photons de haute énergie et l'interaction des photons avec les électrons de la couche atomique pour la génération de contraste, l'IRM est basée sur l'orientation des protons à l'intérieur d'un champ magnétique puissant. Cette orientation peut être manipulée avec des ondes radio fréquences résonantes, et le retour des protons à leur état d'équilibre peut être mesuré. Les constantes de temps de relaxation dépendent fortement des tissus et l'IRM présente un contraste supérieur des tissus mous, dépassant de loin celui du TDM [9].

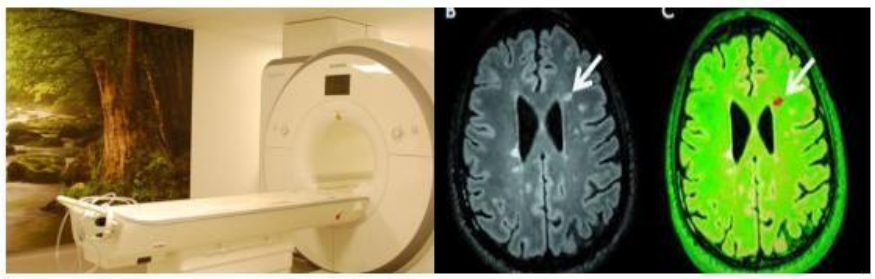


Figure I.17: Schéma d'un système d'IRM [14] (à gauche) et un échantillon d'image

(à droite) indiquant les formes progressives de sclérose en plaques (SEP)

Imagerie par ultrasons : L'imagerie par ultrasons utilise les propriétés des ondes sonores dans les tissus. Les ondes de pression dans la gamme des mégahertz inférieurs traversent les tissus à la vitesse du son, étant réfractées et partiellement réfléchies aux interfaces. Le contraste échographique est donc lié à des inhomogénéités échogènes dans les tissus.

Les images échographiques montrent un bon contraste des tissus mous, mais échouent en présence d'os et d'air. Bien que les images ultrasonores puissent être générées avec des circuits purement analogiques, les appareils à ultrasons modernes utilisent un traitement d'image informatisé pour la formation, l'amélioration et la visualisation des images. L'imagerie par ultrasons est très populaire en raison de son instrumentation peu coûteuse et de sa facilité d'application. Cependant, un examen échographique nécessite la présence d'un opérateur expérimenté pour ajuster divers paramètres pour un contraste optimal, et les images écho-graphiques nécessitent généralement un radiologue expérimenté pour interpréter l'image[9].

Nuclear Imaging : L'imagerie nucléaire est liée à l'imagerie par rayons X et CT en ce sens qu'elle utilise des rayonnements. Cependant, contrairement aux modalités d'imagerie basées sur les rayons X, les composés radioactifs sont incorporés dans le corps en tant que sources de rayonnement. Ces composés radioactifs sont généralement liés à des substances pharmacologi-quement actives (« radiopharmaceutiques ») qui s'accumulent à des sites spécifiques du corps, par exemple dans une tumeur. Avec des techniques de projection ou une reconstruction d'image informatisée volumétrique, la distribution spatiale du produit radio pharmaceutique peut être déterminée. De cette façon, les processus métaboliques peuvent être imagés et utilisés pour un diagnostic. Les reconstructions tridimensionnelles sont obtenues d'une manière similaire à la tomodensitométrie, conduisant à une modalité appelée tomographie par émission monophotonique (SPECT). Une technologie parallèle, la tomographie par émission de positons (TEP), utilise des émetteurs de positons qui provoquent des paires coïncidentes de photons gamma à émettre. Sa sensibilité de détection et son rapport signal sur bruit sont meilleurs que le SPECT. Le SPECT et le PET ont tous deux une résolution nettement inférieure à celle du CT avec des tailles de voxel pas beaucoup plus petites que 1 cm. Souvent, les images SPECT ou PET sont superposées aux images CT ou MR pour fournir une référence spatiale. Une limitation facteur de l'utilisation généralisée des modalités d'imagerie nucléaire est le coût. De plus, les marqueurs radioactifs ont une durée de vie très courte avec des demi-vies de quelques heures seulement, et la plupart des radiophar-maceutiques doivent être produits sur place.

Cela nécessite que les centres d'imagerie nucléaire disposent d'une certaine forme de réacteur pour la génération d'isotopes [9].

I.6.5 Spécificité des images médicales

Des pixels aux voxel : Par rapport à l'image numérique bidimensionnelle dont le processus d'échantillonnage est basé sur les composants de base, les « pixels d'échantillonnage de volume » ajoutent une troisième dimension de « voxels ». Les mécanismes d'imagerie médicale sont reconstitués en termes de [1 . . . X] × [1 . . . Y] × [1 . . . Z] Une image volumétrique modélisée comme une fonction discrète, où chaque emplacement est associé à des informations[15].

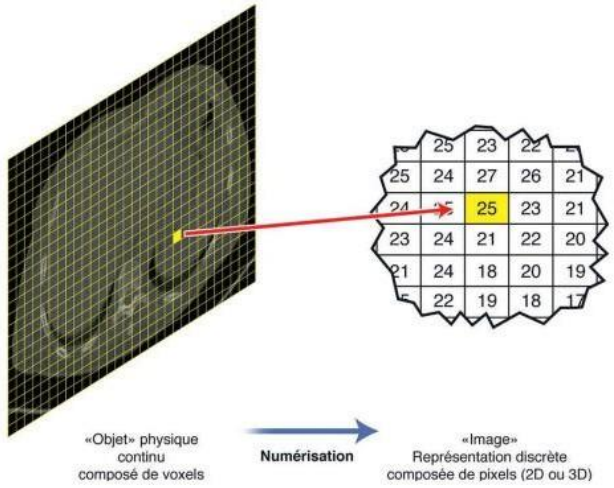


Figure I.18: Numérisation d'un objet en image médical [15].

Taille des images : La taille d'une image médicale dépend du capteur responsable de l'acquisition de la région anatomique à imager. Généralement en tomodensitométrie (technique d'analyse par coupe), les images font du 512 × 512 × 12 bits. En IRM, les formats d'images varient plus que n'importe quelle autre modalité avec des formats matriciels carrés et non carrés (par exemple 64 x 64, 64 x 128, 128 x 128, 128 x 192, 256 x 512, 512 x 512, 512 x 1024, ...).

Résolution spatiale et temporelle : Chaque modalité a différentes capacités pour résoudre les détails fins dans le corps d'un patient. Généralement deux définitions sont données à la résolution spatiale.

- Dans [16] : la résolution réfère a la capacité de voir de petits détails.

- Dans [17] : elle représente la capacité d'un système d'imagerie à représenter distinctement deux objets de plus en plus petits et rapprochés.

D'après ces définitions, un système d'imagerie a une plus grande résolution spatiale s'il peut démontrer la présence d'objets de plus en plus petits dans l'image. Suivant chaque modalité, un ou plusieurs facteurs peuvent causer une limitation de la résolution spatiale.

Bruit : Dans le domaine du traitement du signal et de l'image, le bruit correspond à un phénomène aléatoire qui se surajoute à l'image idéale.

Probablement la meilleure approche pour comprendre le bruit est de réaliser que si l'on acquiert plusieurs fois l'image d'un même objet, immobile et inchangé, on n'observera pas exactement le même résultat : la différence est liée au bruit. De la même manière, en lançant plusieurs fois un dé, on n'obtient pas le même résultat, c'est aléatoire [15].

Contraste : Le contraste dans une image représente la différence entre les niveaux de gris de l'image. Une image uniformément grise n'a pas de contraste, alors qu'une image avec des transitions vives entre un gris obscure et un gris clair démontre un contraste élevé [17].

I.7. Conclusion

Dans ce chapitre, nous avons parlé de l'importance des images numériques et de ses types, les méthodes de codage des pixels des images numériques, les formats connues les plus célèbres et leurs caractéristiques, avec un accent sur les images médical pour la sensibilité des informations contenues.

Bibliographie du chapitre 01

[1] L. Grazide, L'image électronique, http://auch2.free.fr/Documents/Informatique/Image_electronique.pdf, consulté le 09/04/2023.

[2] Rafael C Gonzalez and Richard E Woods. Digital image processing 3rd edition, Pearson Prentice Hall, Upper Saddle River, 2007.

[3] Numeriksciences, http://numeriksciences.fr, consulté le 0914/04/2023.

[4] GREYC IMAGE, Qu'est-ce qu'une image numérique ?, ENSICAEN & Université de Caen & CNRS, https://clouard.users.greyc.fr/fetedelascience/documents/image.pdf , consulté le 10/04/2023.

[5] R. Isdant, Traitement numérique de l'image, 2009, http://raphael.isdant.free.fr/traitement_numerique/2-traitement_numerique_de_l%27image.pdf, consulté le 10/04/2023.

[6] Léon Robichaud, L'image numérique Pixels et couleurs, support de cours, Département d'histoire, Université de Sherbrooke.

[7] Les formats d'images numériques, Serge WACKER – C2I niveau 1, http://serge.wacker.free.fr/technoprimaire/c2i/revisions/formats_image.pdf , consulté le 10/04/2023.

[8] W. Puech Archivage d'images médicales LIRMM, CNRS/ University of Montpellier, France.

[9] Haidekker, Mark A. "Medical imaging technology." (2013).

[10] Salomé Le Gall,Bases physiques de l'imagerie médicale : imagerie analogique / imagerie numérique, Cours 3 UE2, (2016).

[11]://www.radiologieperpignan.fr/wpcontent/uploads/photogallery/Photos,(2020).consulté le 11/04/2023.

[12] Estelle Cherrier,*Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires*.PhD thesis,(2006).

[13] COLARD, J DELPUECH, Les rayons X une révolution dans l'avancé du diagnostic mé- dical(2020).

[14] HODEL, J, Formes progressives de sclérose en plaques : place actuelle de l'IRM pour le diagnostic positif et différentiel,(2018).

[15] DURAND, E BLONDIAUX, E , In imagerie médicale, Elsevier Masson SAS,12p,(2017).

[16] A Naiıt Ali et Christine Cavaro-menard, Compression des images et des signaux médicaux,(2007).

[17] Jerrold T Bushberg,J Anthony Seibert, Edwin M Leidholdt Jr, John M Boone, and Edward J Goldschmidt Jr,The essential physics of medical imaging,Medical Physics,(2003).

Chapitre 02
Généralité sur la cryptographie

II Introduction

II.1 Histoire de la Cryptographie

L'histoire de la cryptographie est fascinante, remontant à environ 2000 avant J.C en Égypte, où les hiéroglyphes étaient utilisés pour orner les tombes et raconter l'histoire de la vie des défunts. Une méthode de cryptographie utilisant l'alphabet hébreu consistait à inverser chaque lettre de l'alphabet d'origine avec une lettre différente de l'alphabet inversé, connue sous le nom de méthode d'Atbash. Vers 400 avant J.C, les Spartiates utilisaient un système de cryptage en écrivant des messages sur des bandes de papyrus ou des lanières de cuir, puis en les enroulant autour d'une scytale, considérée comme l'ancêtre des systèmes de transmission secrète. Jules César a développé une autre méthode simple consistant à déplacer les lettres de l'alphabet, similaire au système d'Atbash, en utilisant un simple décalage.

Au XXe siècle, une nouvelle machine de chiffrement est apparue, capable de créer des messages difficiles à décrypter. Cette machine est connue sous le nom d'Enigma est considérée comme la machine de chiffrement la plus célèbre de l'histoire à ce jour, utilisée par les Allemands. Avec l'avènement des ordinateurs, la cryptographie a connu un développement significatif, donnant lieu à de nombreuses méthodes de cryptage telles que DES, AES, RSA, DSS, et bien d'autres.

Le chaos joue un rôle essentiel dans de nombreux algorithmes de cryptage. Dans ce chapitre, nous allons expliquer le concept du chiffrement et montrer comment il dépend du chaos.

II.2 la cryptographie :

Le terme cryptographie provient des deux mots grecs anciens « Kruptos » qui signifie « cacher » et « graphein » qui signifie « écrire ». Ce qui signifie littéralement, « cacher l'écriture ». Le Petit Larousse donne la définition suivante : « Ensemble des techniques de chiffrement qui assurent l'inviolabilité de textes et, en informatique, de données. »

La cryptographie est l'étude de la techniques mathématiques liées à la sécurité de l'information par sécurité de l'information on entend confidentialité de données, intégrité authentification de données, communicant de données, et non répudiations de données [1].

La figure suivante illustre le schéma du principe général de la cryptographie.

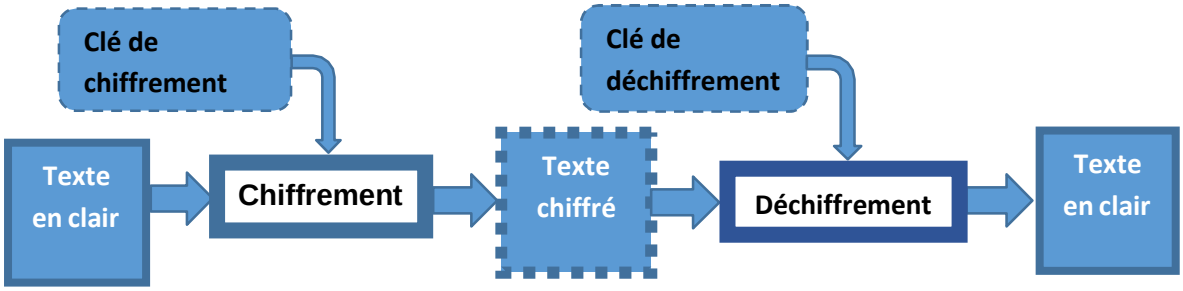


Figure II.1: Schéma général de la cryptographie.

II.2.1 Vocabulaire de base de la cryptographie

On présente quelques définitions et concepts basiques en cryptographie

II.2.1.1 La cryptologie

Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse **[2].**

II.2.1.2 La cryptographie

L'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné [2].

II.2.1.3 La cryptanalyse

Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés [2].

II.2.1.4 Crypto-système

Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné [2].

II.2.1.5 Texte en clair

C'est les données (message, texte,..) à protéger.

II.2.1.6 Le chiffrement

Est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement. [3].

II.2.1.7 Texte chiffré

Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair [2].

II.2.1.8 Le déchiffrement

C'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en un texte en clair [3].

II.2.1.9 Clef

Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement [2]

II.2.1.10 Confusion

La confusion correspond à une volonté de rendre la relation entre la clé de chiffrement et le texte chiffré la plus complexe possible [4].

II.2.1.11Diffusion

La diffusion est une propriété où la redondance statistique dans un texte en clair est dissipée dans les statistiques du texte chiffré. En d'autres termes, un biais en entrée ne doit pas se retrouver en sortie et les statistiques de la sortie doivent donner le moins possible d'informations sur l'entrée [4].

II.2.1.12 Substitution

Les substitutions consistent à remplacer des symboles ou des groupes de symboles par d'autres symboles ou groupes de symboles dans le but de créer de la confusion [4].

II.2.1.13 Permutation (transposition)

Chiffrement par permutation (Un chiffrement par transposition) est un chiffrement qui consiste à changer l'ordre des lettres, le chiffrement par transposition demande de découper le

texte clair en blocs de taille identique. La même permutation est alors utilisée sur chacun des [4].

II.2.2 Objectifs de la cryptographie

La cryptographie est l'étude des techniques mathématiques qui sont utilisées pour accomplir plusieurs objectifs pour garantir la sécurité de communication, ces objectifs sont :

➢ **La confidentialité:**

Il doit être possible pour le récepteur de l'image de garantir son origine. Une tierce personne ne doit pas pouvoir se faire passer pour quelqu'un d'autre.

➢ **L'intégrité:** Le récepteur doit pouvoir s'assurer que le message n'a pas été modifié durant sa transmission. Une tierce personne ne doit pas pouvoir substitue un message légitime (ayant pour origine l'émetteur) par un message frauduleux.

➢ **L'authentification:** Offrir au récepteur d'un message la possibilité de vérifier l'identité de l'émetteur pour but de garantir qu'aucune usurpation d'identité n'a eu lieu.

➢ **La non-répudiation :** Un émetteur ne doit pas pouvoir nier l'envoi d'un message.

II.2.3 La Cryptographie Classique

La cryptographie classique, avant l'avènement des ordinateurs, se base sur les langues naturelles (allemand, anglais, français, etc.). Les outils utilisés consistent à remplacer et transposer les caractères. Les meilleurs systèmes de cette catégorie répètent ces opérations de base. La confidentialité des procédures (chiffrement et déchiffrement) est essentielle, sinon le système est inefficace. On les appelle généralement les méthodes de chiffrement à usage restreint.

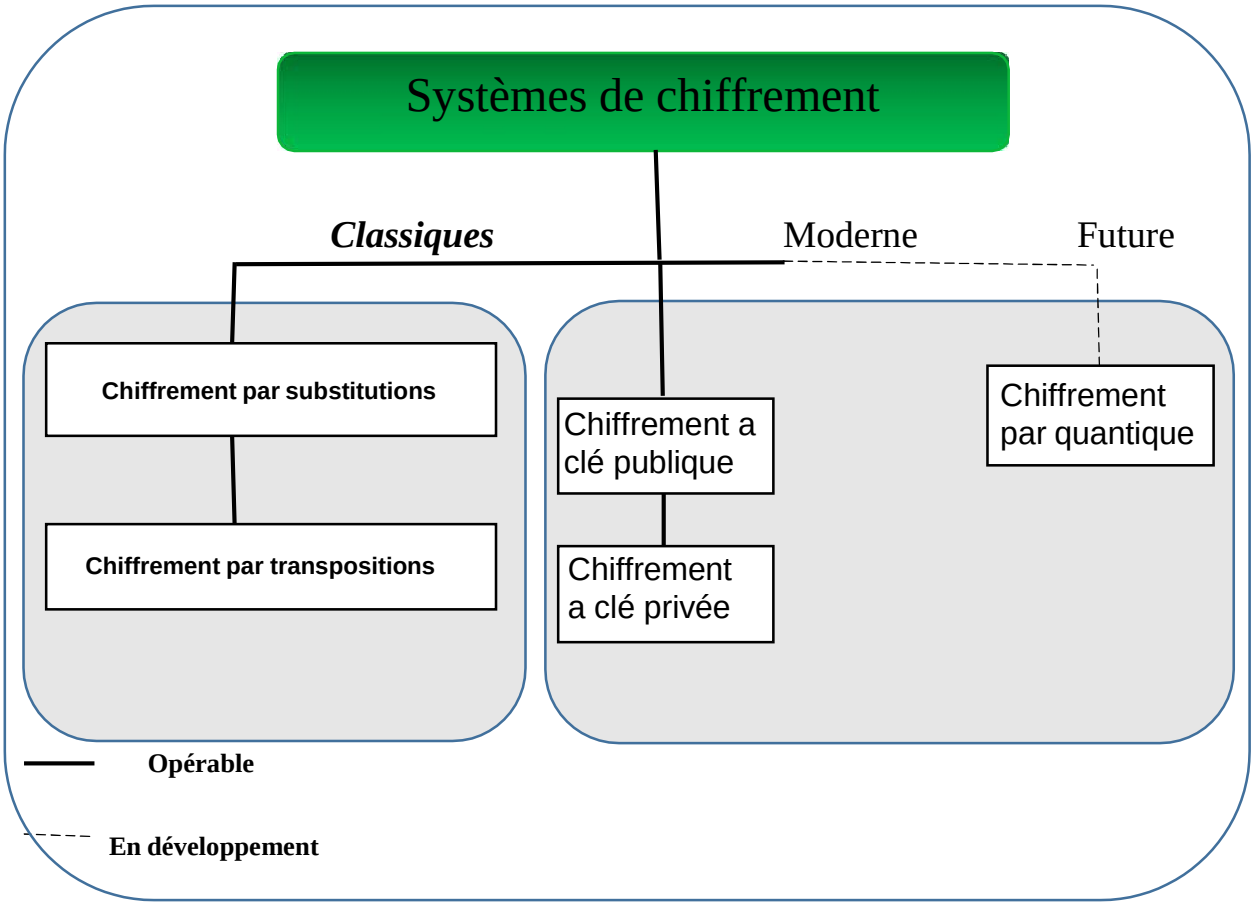


Figure II.2 Principale technique en cryptographie.

II.2.3.1 Le chiffrement classique :

Il existe des centaines de façon de chiffrer des données représentées par l'alphabet classique, tout en gardant les opérations réalisées secrètes. Ici on ne va pas présenter toutes ces méthodes, mais plutôt les concepts mathématiques (connus depuis très longtemps) qui sont à la source de celles-ci. On va ainsi voir que finalement il n'y en a pas tant que l'on pouvait le penser, et surtout qu'elles sont extrêmement **simples**.

a) Substitution :

La substitution consiste effectuer des dérivations pour que chaque caractère du message chiffré soit différent des caractères du message en clair. Le destinataire légitime du

message applique la dérivée inverse au texte chiffré pour recouvrer le message initial. La complexité des systèmes à substitutions dépend de trois facteurs :

- la composition spécifique de l'alphabet utilisé pour chiffrer ou pour communiquer,

- le nombre d'alphabets utilisés dans le cryptogramme,

- la manière spécifique dont ils sont utilisés. [17]

On distingue couramment Plusieurs types de substitutions différentes :

•Substitution mono-alphabétique

Chaque caractère du texte en clair est remplacé par un caractère correspondant dans le texte chiffré. Les exemples les plus célèbres sont les algorithmes de César, Rot13, et bien évidemment le code morse. Ils sont encore utilisés aujourd'hui pour cacher le sens de certains messages (par exemple la solution de certains jeux dans des journaux), mais bien sûr elles sont très peu sûres. En effet avec ce principe, les lettres les plus fréquentes dans le texte en clair restent les plus fréquentes dans le texte chiffré, il ne cache donc pas les fréquences d'apparition des caractères. C'est une faiblesse importante puisque des techniques statistiques peuvent être utilisées pour associer aux lettres les plus fréquentes, une lettre probable et en appliquant une technique sémantique récursive, les algorithmes à base de substitutions mono-alphabétiques sont facilement cassés par les spécialistes. [17]

Exemple : texte en clair=«NON JE NE SUIS PAS FOU »

texte chiffré (avec 5 divisions)=«ABAWR ARFHV FCNFS BH »

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M

Figure II.3: dictionnaire ROT13

•Substitution homophonique

permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères[11]

•Substitution poly-alphabétique

La substitution poly-alphabétique est une méthode de chiffrement consistant à remplacer périodiquement une lettre par différentes lettres, contrairement à la substitution simple où chaque lettre est remplacée par une même autre lettre dans tout le message. L'exemple le plus célèbre de chiffre poly-alphabétique est le chiffre de Vigenère, qui a été utilisé pendant trois siècles et a résisté aux tentatives de cryptanalyse. [11]

b) Transposition :

Avec le principe de la transposition toutes les lettres du message sont présentes, mais dans un ordre différent. Il utilise le principe mathématique des **permutations**. Plusieurs types différents de transpositions existent [17] :

• Transposition simple (à base matricielle)

Elle consiste à écrire le texte en clair dans une matrice de n colonnes (une lettre dans chaque case), et ensuite de construire le texte chiffré en prenant les lettres à partir de cette matrice colonne par colonne. La clé dans ce cas est le nombre n. [17]

•Transposition avec substitution simple

L'idée dans ce cas est de combiner la transposition avec une substitution simple. Il s'agit ainsi de chiffrer le message clair par une méthode de substitution simple, et en suite d'en appliquer une transposition. Une autre astuce est souvent utilisée qui consiste à appliquer une fonction de permutation sur l'ordre d'arrangement des colonnes. On cite à titre d'exemple : le chiffre de DELASTELLE. [11]

II.2.3.2 La cryptographie moderne :

- **Cryptographie à clefs privés**

Chiffrement par flot

Un chiffrement de flux repose sur de simples transformations de chiffrements (tel que l'opération XOR) en utilisant le flux de clé. Le flux de clé pourrait être généré au hasard, ou par un algorithme qui génère le flux de clé à partir d'un premier seed, ou à partir d'un seed et

des symboles de texte chiffré précédents. Ce type de chiffrement arrive à traiter les données de longueur quelconque et n'a pas besoin de les découper. [7]

Masque jetable (one-time pad)

Le chiffre de Vernam, également connu sous le nom de chiffrement parfait, est un algorithme de cryptographie inventé par Gilbert Vernam en 1917. La sécurité de ce système repose sur la génération totalement aléatoire des clés, ce qui en fait le seul chiffrement théoriquement incassable. Par conséquent, si le cryptanalyste ne possède aucune information sur laquelle baser son attaque, tous les masques seront équiprobables. [16]

Chiffrement par blocs

Un chiffrement par bloc est une méthode de cryptage qui décompose le texte en clair en chaînes (appelés blocs) d'une longueur fixe t, et le chiffrement se fait bloc par bloc (un bloc à la fois). Pour les algorithmes de chiffrements par bloc modernes, la taille typique de blocs est 64 bits; assez grande pour empêcher l'analyse et assez petite pour être pratique. Les techniques de cryptage à clé symétrique les plus connues sont des algorithmes de chiffrement par blocs. Il existe deux classes importantes de chiffrement par blocs : les algorithmes de chiffrement par substitution et les algorithmes de chiffrement par transposition. [7]

Réseau de Feistel

Dans ce système de chiffrement, un bloc de texte en clair est découpé en deux ; la transformation de ronde est appliquée à une des deux moitiés, et le résultat est combiné avec l'autre moitié par ou exclusif. Les deux moitiés sont alors inversées pour l'application de la ronde suivante. Un avantage de ce type d'algorithmes est que chiffrement et déchiffrement sont structurellement identiques. [13]. Nous considérerons que pour une certaine clef entrée, ces fonctions sont les suivantes:

Tableau. II. 1: fonctions feistel

entrée	f_1	sortie		entrée	f_2	sortie
00	→	01		00	→	11
01	→	11		01	→	00
10	→	10		10	→	00
11	→	01		11	→	01

On peut "additionner" deux bits à l'aide de la fonction XOR (symbolisée par un + entouré d'un cercle) donnée par le tableau ci-dessous. Il est à noter que l'opérateur XOR est son propre inverse.

XOR	0	1
0	0	1
1	1	0

Notons que ni f_1 ni f_2 ne sont des bijections. À titre d'exemple, chiffrons le message 1101. G désigne la moitié gauche du message à chiffrer, D la moitié droite.

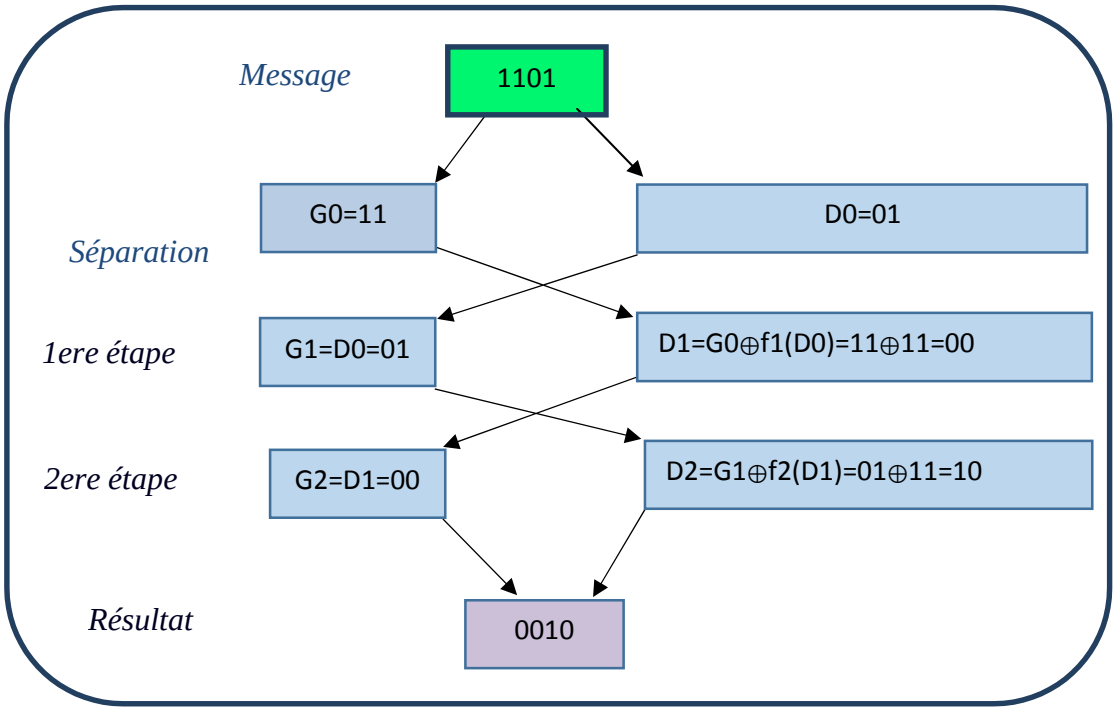


Figure II.4 : réseau de Feistel.

DES (Data Encryptions Standard)

Il s'agit d'un système de chiffrement symétrique par blocs de 64 bits, dont 8bits (un octet) servent de test de parité (pour vérifier l'intégrité de la clé). Chaque bit de parité de la clé (1 tous les 8 bits) sert à tester un des octets de la clé par parité impaire, c'est-à-dire que chacun des bits de parité est ajusté de façon à avoir un nombre impair de '1' dans l'octet à qui il appartient. La clé possède donc une longueur « utile » de 56 bits, ce qui signifie que seuls 56 bits servent réellement dans l'algorithme.

L'algorithme consiste à effectuer des combinaisons, des substitutions et des permutations entre le texte à chiffrer et la clé, en faisant en sorte que les opérations puissent se faire dans les deux sens (pour le déchiffrement). La combinaison entre substitutions et permutations est appelée **code produit**.

La clé est codée sur 64 bits et formée de 16 blocs de 4 bits, généralement notés k_1 à k_{16}. Etant donné que « seuls » 56 bits servent effectivement à chiffrer, il peut exister 2^{56} (soit $7.2*10^{16}$) clés différentes **[1]**. Les grandes lignes de l'algorithme sont les suivantes :

Fractionnement du texte en blocs de 64 bits (8 octets) ;

Permutation initiale des blocs ;

Découpage des blocs en deux parties: gauche et droite, nommées *G* et *D* ;

Etapes de permutation et de substitution répétées 16 fois (appelées **rondes**) ;

Recollement des parties gauche et droite puis permutation initiale inverse. **[11]**

AES (Advanced Encryptions Standard).

L'AES est un système cryptographique symétrique, son principe repose sur une suite d'opérations de permutation et de substitution. Il est considéré comme une amélioration ou une mise à jour du système DES. Contrairement à AES ce n'est pas un réseau de Feistel mais un réseau de substitution-permutation. AES travaille sur des blocs de 128 bits avec des clefs de longueur 128, 192 ou 256 bits. A l'origine AES pouvait travailler sur des blocs de longueur Nb × 32 bits où Nb variait de 4 à 8, finalement la taille de blocs d'AES a été fixée à 128 bits et donc Nb a été fixé à 4. Le passage à une clé de 128 bits minimum rend impossible dans le futur prévisible les recherches exhaustives de clefs. Si on suppose que l'on a un algorithme

capable de comparer en une seconde 256 clef (i.e de casser DES en une seconde) il lui faudra 149 mille milliards d'années pour casser AES **[12]**

- **Cryptographie à clefs public**

RSA

Le premier algorithme déchiffrement à clé publique (chiffrement asymétrique) a été développé par *R.Merckle* et *M.Hellman* en 1977. Il fut vite rendu obsolète grâce aux travaux de *Shamir*, *Zippel* et *Herlestman*, de célèbres cryptanalistes. En 1978, l'algorithme à clé publique de Rivest, Shamir, et Adelman (d'où son nom **RSA**) apparaît. Cet algorithme servait encore en 2002 à protéger les codes nucléaires de l'armée américaine et russe. Le fonctionnement du crypto système RSA est basé sur la difficulté de factoriser de grands entiers.Soit deux nombres premiers *p* et *q*, et *d*, un entier tel que *d* soit premier avec *(p-1)*(q-1)*). Le triplet *(p, q, d)* constitue ainsi la clé privée. La clé publique est alors le doublet (n,e) créé à l'aide de la clé privée par les transformations suivantes : n=p*q et e=1/d mod ((p- 1)(q-1))

Soit *M*, le message à envoyer. Il faut que le message *M* soit premier avec la clé *n*. En effet, le déchiffrement repose sur le théorème d'Euler stipulant que si *M* et *n* sont premiers entre eux, alors : $M^{phi(n)} = 1 \bmod(n)$

$$f(x) = \mathrm{x} + \sum_{n=1}^{\infty} \left(a x_0 \cos\frac{n\pi x}{L} + b_n \sin\frac{n\pi x}{L} \right) \qquad \textbf{(Eq.II.2)}$$

Phi(n) étant l'indicateur d'Euler, et valant dans le cas présent *(p-1)*(q-1)*. Il est donc nécessaire que M ne soit pas un multiple de *p*, de *q*, ou de *n*. Une solution consiste à découper le message *M* en morceaux M_i tels que le nombre de chiffres de chaque M_i soit strictement inférieur à celui de *p* et de *q*. Cela suppose donc que p et q soient grand, ce qui est le cas en pratique puisque tout le principe de RSA réside dans la difficulté à trouver dans un temps raisonnable *p* et *q* connaissant *n*, ce qui suppose *p* et *q* grands [11].

II.3 Classification selon la clé de cryptage

II.3.1 Cryptage symétrique

En chiffrement symétrique, la même clé, appelée clé secrète, est utilisée lors du chiffrement et du déchiffrement d'un message. Ainsi, la sécurité du crypto-système repose sur

l'échange sécurisé de la clé; seuls l'expéditeur et le destinataire du message doivent connaître la clé secrète. Par ailleurs, cette clé doit être de taille suffisamment grande pour se prémunir des attaques par force brute [5].

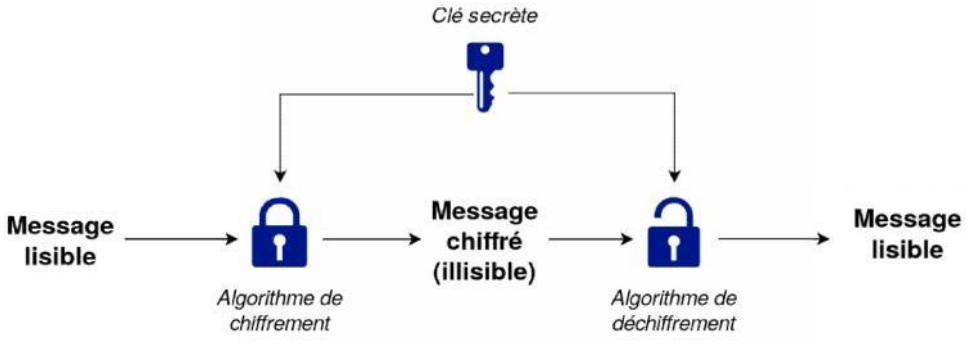


Figure II.5 : Schéma simple d'un chiffrement symétrique.

II.3.1.1 Caractéristiques du cryptage symétrique

- La rapidité d'exécution.

- La simplicité d'implémentation.

- La sécurisation de la chaîne de transmission de la clé.

- La complexité de fonctionnement : une obligation d'avoir le nombre de clés privées égal au nombre de destinataires. [16].

II.3.2 Cryptage asymétrique

Le chiffrement asymétrique, également appelé chiffrement à clé publique, est un facteur essentiel pour l'envoi et la réception de transactions en bitcoins et les transactions dans d'autres crypto monnaies.

Le chiffrement asymétrique utilise un ensemble de deux clés : une clé publique pour le chiffrement et une clé privée pour le déchiffrement, que seule une partie connaît.

La clé privée doit être gardée secrète par le destinataire car toute partie ayant accès à une clé privée ou à une clé publique a accès aux fonds.

Le chiffrement asymétrique est basé sur des algorithmes de chiffrement asymétrique qui sont très difficiles à résoudre [6].

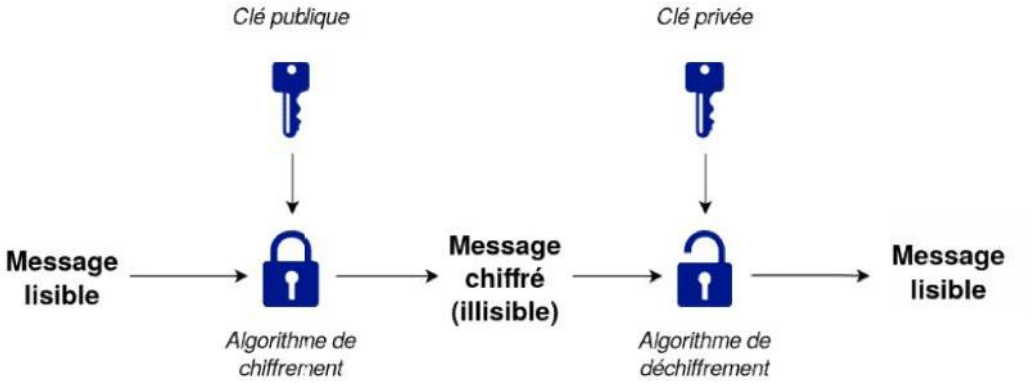


Figure II.6 : Schéma simple d'un chiffrement asymétrique.

II.3.2.1 Caractéristiques du cryptage asymétrique

- L'élimination de la problématique de la transmission de la clé.

- La possibilité d'utiliser la signature électronique.

- L'impossibilité de décrypter le message dans le cas de son interception par une personne non autorisé.

- Une paire de clés (publique/secrète) peut être utilisée plus longtemps qu'une clé symétrique.

- Le temps d'exécution : plus lent que le cryptage symétrique.

- Le danger des attaques par substitution des clés d'où la nécessité de valider les émetteurs des clés.

- Taille des clés, plus grande que celle des systèmes symétriques. [16].

II.4 Le chaotique

II.4.1 Historique de la théorie du Chaos

En 1963 le météorologue Edward Lorenz expérimentait une méthode lui permettant de prévoir les phénomènes météorologiques. C'est par pur hasard qu'il observa qu'une modification minime des données initiales pouvait changer de manière considérable ses résultats. Lorenz venait de découvrir le phénomène de sensibilité aux conditions initiales. Les systèmes répondant à cette propriété seront à partir de 1975 nommés : systèmes chaotiques

Vers la fin du XIXe siècle le mathématicien, physicien et philosophe français Henri Poincaré avait déjà mis en évidence le phénomène de sensibilité aux conditions initiales lors de l'étude astronomique du problème des trois corps [2].

II.4.2 Le Chaos :

Il n'existe pas de définition universellement acceptée du chaos dans la littérature. On peut le décrire comme un phénomène qui se manifeste dans les systèmes dynamiques déterministes non linéaires, où leur évolution semble aléatoire et présente une instabilité fondamentale appelée sensibilité aux conditions initiales. Cette sensibilité rend le système imprédictible à long terme en pratique.

II.4.2.1 Condition obtention chaos :

Le chaos est défini généralement comme un comportement particulier d'un système dynamique qui inclut :

- **la non-linéarité :** l'évolution irrégulière du comportement d'un système chaotique est due aux non linéarités.
- **le déterminisme** : un système chaotique a des règles fondamentales déterministes et non probabilistes.
- **la sensibilité** : le système manifeste une très haute sensibilité aux changements de conditions.
- **l'imprévisibilité :** en raison de la sensibilité aux conditions initiales, qui peuvent être connues seulement à un degré fini de précision.
- **l'irrégularité** : L'ordre caché comprenant un nombre infini de modèles périodiques instables (ou mouvements). Cet ordre caché forme l'infrastructure des systèmes chaotiques [19].

II.5 Les systèmes dynamiques chaotiques

Un système dynamique chaotique est un système déterministe qui montre un Comportement aléatoire par sa dépendance et sa sensibilité à ses conditions initiales. Puisque, dans la pratique, les conditions initiales ne peuvent jamais être spécifiées avec une précision infinie, le comportement d'un système chaotique est imprévisible, et donc, comme un bruit.

Les applications diverses de cette théorie dans divers domaines de recherche S'augmentent progressivement. Pour obtenir une appréciation d'être à la base du système dynamique non linéaire, la théorie chaotique considère trois types de systèmes dynamiques [3]

- Systèmes dynamiques **autonomes**;
- Les systèmes dynamiques **non autonomes** diffèrent des systèmes autonomes Parce que le champ de vecteur est une fonction de x et de t, et l'état initial ne peut pas être arbitrairement placé à zéro ;
- Des **systèmes dynamiques de temps discret** sont définis par l'équation d'état,
  $X_{k+1}= g(X_k)$ $(\mathbf{Eq.\,II.\,2})$ $k = 0,1,2,$ ...où $X_k \in R^n$ s'appelle l'état, et g trace l'état X_k au Prochain état $\{X_{k+1}\}$. Commençant par un état initial x_0 les applications répétées de la carte g (provoquent une séquence des points $\{x_k : k = 0,1,2, \ldots\}$ appelée une orbite du système à temps discret. **[8]**

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

II.6 Utilisation des systèmes dynamiques chaotiques en cryptographie

Les premières applications des systèmes chaotiques en cryptographie sont proposées par Pecora et Carroll comme une possible application de la synchronisation des systèmes dynamiques chaotiques. Dans le cas de ces systèmes dynamiques continus, les méthodes de synchronisation des systèmes chaotiques et de contrôle du chaos s'appliquent principalement à la sécurisation des communications. Kocarev et Parlity mettent en évidence les méthodes de cryptage des messages par la modulation des trajectoires de systèmes dynamiques continus. Quant aux systèmes dynamiques discrets (avec itérations et itérations inverses d'applications chaotiques) abordés initialement par Habutsu et développés par la suite par Kotulski et Szcepanski, ils sont à la base de la construction de clés. [10]

Le tableau suivant illustre parfaitement la correspondance entre la théorie du chaos et la cryptographie.

Tableau.II. 2: La correspondance entre la théorie du chaos et la cryptographie.

Théorie du chaos	Cryptographie
• Système chaotique	•Système pseudo- chaotique
•Transformation non linéaire	•Transformation non linéaire
•Nombre infini d'états	•Nombre fini d'états
•Nombre infini d'itérations	•Nombre fini d'itérations
•Etats initiale	•Plaintext
•Etats finale	•Ciphertext
•conditions initiale (s) et/ou paramètre (s)	•Clé(s)
•Independence asymptotique Des états initiaux et finaux	•Confusion
•Sensibilité aux conditions initiale (s) Et paramètre (s) i.e. mixage	•Diffusion

On considère les systèmes de cryptographie reposant sur la prise en compte des signaux chaotiques issus de récurrences discrètes non linéaires, des systèmes discrets modélisés par une équation de la forme :

$x_{k+1} = f(x_k); x_0 \in I$ **(Eq.II.3)**

où I est l'intervalle unité ou le carré unité, et $f : I \rightarrow I$; le but étant de mettre en évidence les propriétés mathématiques de ces systèmes chaotiques capables d'accroitre la sécurité des crypto-systèmes construits à partir de ces systèmes dynamiques.

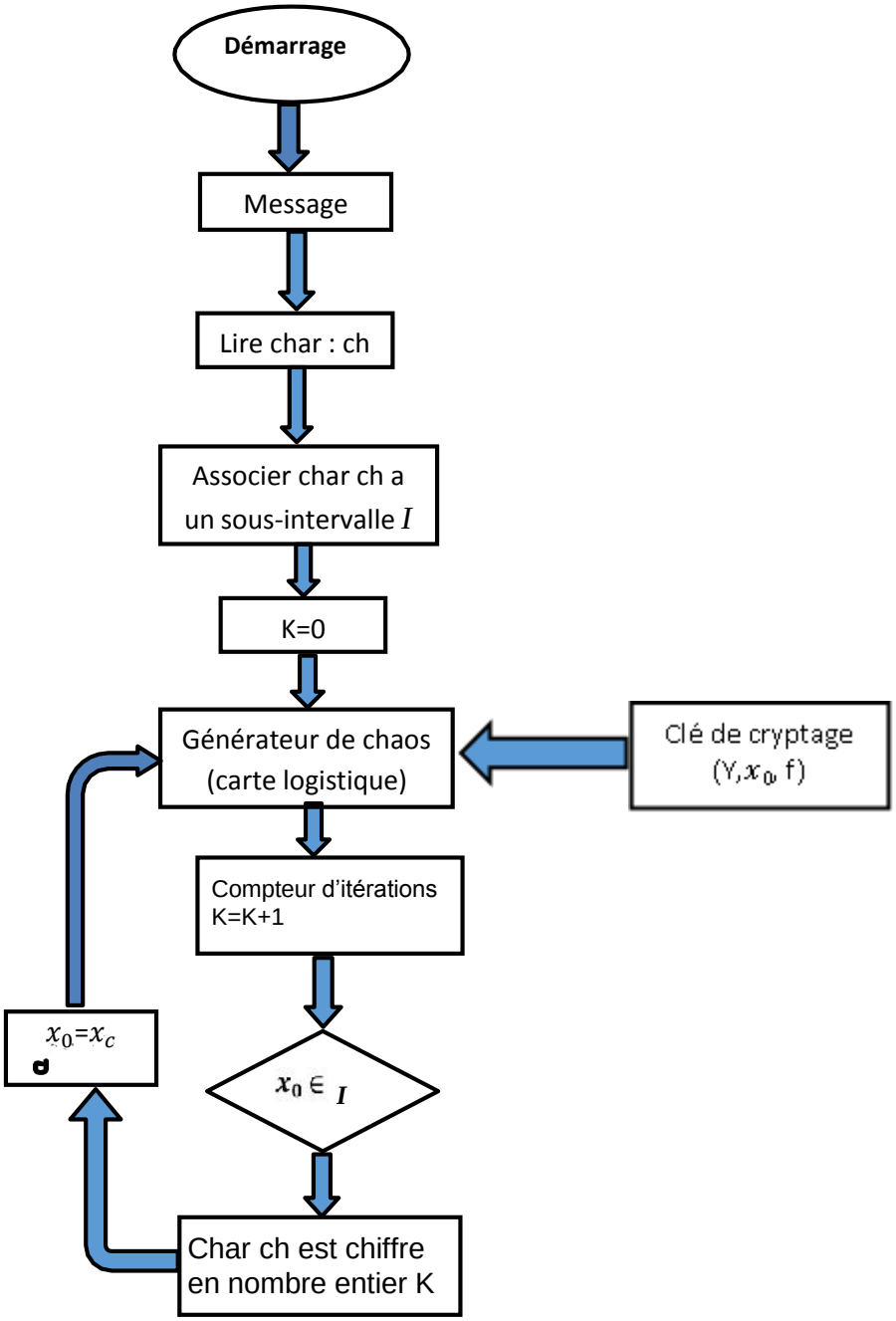


Figure II.7 : Schéma de la méthode de cryptage chaotique

II.6.1Système de Lorenz

Le système de Lorenz est généré par le système d'équations suivant :

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = x(b - z) - y \\ \dot{z} = xy - cz \end{cases} \qquad \textbf{(Eq.II.4)}$$

Cet exemple a été publié en 1963 dans un journal météorologique. Les variables x ,y et z représentent les états du système à chaque instant. a, b, c sont les paramètres du systèmes. Le système présente un comportement chaotique pour a = 12, b = 26, c = 9 et présente un attracteur étrange en forme d'ailes de papillon **[18]**

II.6.2.Exposant.de.Lyapunov

Le mathématicien russe Alexander Markus-Lyapunov (1857-1918) s'est penché sur ce phénomène et a développé une quantité permettant de mesurer la vitesse à laquelle ces petites variations peuvent s'amplifier. Cette quantité appelée « Exposant de Lyapunov (LE) » [20] qui est souvent utilisé pour déterminer si un système est chaotique ou non. L'exposant de Lyapunov (LE) a été largement utilisé dans l'étude des systèmes dynamiques pour mesurer en fait le degré de sensibilité d'un système dynamique, autrement dit, le taux de divergence entre l'évolution de trajectoires issues de conditions initiales proches au sein de cet espace borné qu'est :l'attracteur.étrange.

Le LE est une mesure quantitative possible du chaos, et Lyapunov a démontré que le nombre d'exposants de Lyapunov est égal à la dimension de l'espace des phases. Soit un système discrète unidimensionnel et x_0 et x_0+ε deux conditions initiales très proches supposons qu'elles écartent en moyenne à un rythme exponentielle. On pourra trouver ; un réel λ tel qu'après n itérations on a :

$$|f^n(x_0+\varepsilon)-f^n(x_0)| \cong \varepsilon e^{n\lambda} \quad \text{D'où } n\lambda \cong \ln\frac{|f^n(x_0+\varepsilon)-f^n(x_0)|}{\varepsilon}$$

Et pour ε→0 on a :

$$n\lambda \cong \ln\frac{|f^n(x_0+\varepsilon)-f^n(x_0)|}{\varepsilon} = \frac{1}{n}\ln\left|\frac{df^n(x_0)}{dx_0}\right|$$

$$\cong \frac{1}{n}\ln\left|\frac{df^n(x_0)}{d^{n-1}(x_0)}\right|.\left|\frac{df^{n-1}(x_0)}{d^{n-2}(x_0)}\right|\ldots\left|\frac{df^1(x_0)}{d(x_0)}\right|$$

$$\cong \frac{1}{n}\ln\left|\frac{df(x_{n-1})}{dx_{n-1}}\right|.\left|\frac{df(x_{n-2})}{dx_{n-2}}\right|\ldots\left|\frac{df(x_0)}{dx_0}\right| \cong \frac{1}{n}\sum_{i=0}^{n-1} ln\left|\frac{df(x_i)}{dx_i}\right|$$

Finalement pour $n \to \infty$ on a :

$$\lambda = \lim_{n\to\infty}\frac{1}{n}\left(\sum_{i=0}^{n-1} ln\left|\frac{df(x_i)}{dx_i}\right|\right)$$

(Eq.II.5)

est appelé exposant de Lyapunov il indique le taux moyen de divergence.

- Si $\lambda > 0$ alors il y a une sensibilité aux conditions initiales.
- Si $\lambda < 0$ les trajectoires se rapprochent et on perd l'information sur les conditions initiales. [20]

II.6.3. Diagramme de Bifurcation

Le diagramme de bifurcation est un tracé, qui permet d'évaluer rapidement l'ensemble des solutions possibles d'un système ainsi que leur stabilité en fonction des variations de l'un de ses paramètres. Il permet également de repérer les valeurs particulières du paramètre qui induisent des bifurcations.

Il présente des intervalles sur lesquelles les solutions asymptotiques évoluent continuellement avec le paramètre, et il classe les valeurs du paramètre sur l'axe des abscisses et les valeurs d'une des variables d'état sur l'axe des ordonnées. [20]

II.7 Les cartes chaotiques les plus utilisées.

Les cartes chaotiques sont en effet des systèmes dynamiques définis par des relations de récurrence. Elles sont généralement utilisées pour modéliser des phénomènes complexes et non linéaires dans divers domaines tels que la physique, les mathématiques, l'économie et l'informatique.

II.7.1 La carte logistique

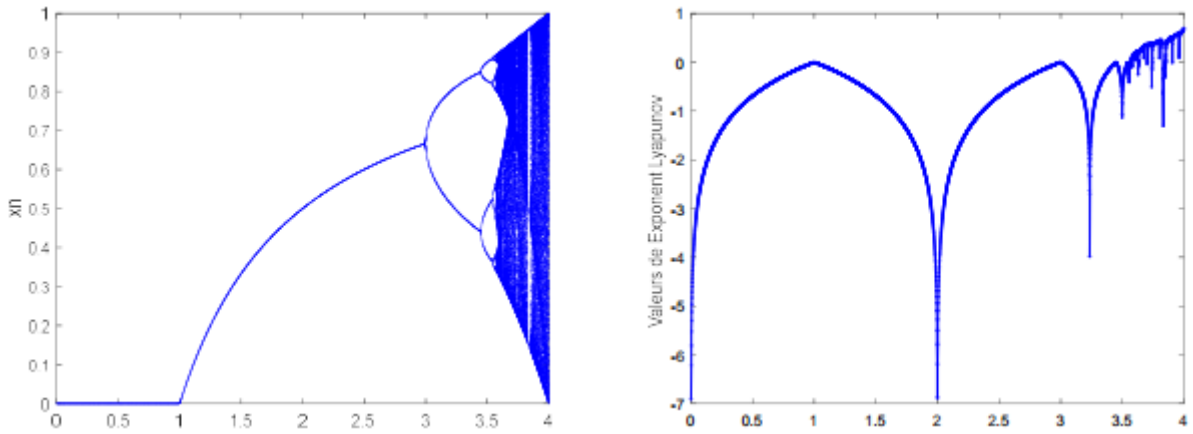
La carte logistique est une cartographie polynomiale, ou le comportement de cette carte est basé sur une très simple équation non linéaire dynamique.

L'équation de la carte chaotique logistique est donnée par :

$$X_{(n+1)} = \mathrm{r}X_{(n)}(1 - X_n) \qquad \textbf{(Eq.II.6)}$$

Où x variable dans l'intervalle [0, 1] et n est le nombre d'itérations, r est un nombre définit dans l'intervalle [0, 4].

La carte logistique est utilisé comme une simple méthode chaotique pour créer la clé de cryptographie, cette clé est un paire de deux variable ($x_{(0)}$, r), le choix de cette paire affecte le résultat du cryptage. **[10]**



(a) **(b)**

Figure II.8 : carte logistique (a) diagramme de bifurcation (b) Exposant Lyapunov

II.7.2 La carte Skew tent

La carte Skew tent est une carte linéaire par morceaux, sera examinée pour l'usage dans le domaine de tatouage , décrite en réel par l'équation suivante :

$$x_n = F_p\,(x(n-1), p) = \begin{cases} x(n-1)/p & si\ 0 \le x(n-1) \le p \\ \frac{x(n-1)}{1-p} & si\ p < x(n-1) \le 0.5 \end{cases} \qquad \textbf{(Eq.II.7)}$$

Et p est le paramètre de contrôle qui varie dans l'intervalle suivant : $p \in [0, 1]$ L'histogramme de cette carte est pratiquement uniforme comparé à celle de la carte Logistique. [9]

II.7.3 La carte Sine

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

$$x_{n+1} = \lambda \sin \pi x_n \qquad \textbf{(Eq.II.8)}$$

Avec λ =1 le comportement chaotique est généré par une manière très similaire à la fonction logistique. Comme la récurrence logistique, la carte sine est quadratique au voisinage de 0,5. Elles ont une distribution probabiliste et une évolution vers le chaos par doublement de période presque identique. Les fenêtres se produis en périodiquement dans le même ordre. Elle a le même nombre de Feigenbaum que la carte logistique. Malgré les similitudes, il existe quelques différences, l'exposant de Lyapounov est d'environ cinquante pour cent plus petit. Les bifurcations par doublement de période survenir plus tôt, et les fenêtres périodiques sont plus larges par rapport à la carte logistique.[19]

II.7.4 La carte de PWLCM (Piecewise Linear Chaotic Maps) :

Le système PWLCM a une très bonne ergodicité et très sensible aux valeurs initiales ce qui est adéquat pour la cryptographie. Le système PWLCM est présenté par l'équation (Eq.II.8).

$$x(i+1) = F_p(x_i) = \begin{cases} x_i/p & \begin{cases} 0 \le x_i \le p \\ p \le x_i \le 0.5 \\ 0.5 \le x_i \le 1 \end{cases} \\ (x_i - p)/(0.5 - p), \\ F_p(1 - x_j), \end{cases} \quad \textbf{(Eq.II.9)}$$

La carte est chaotique si $x \in [0,1)$ et le paramètre de contrôle p ∈ (0,5. 0), les valeurs initiales de cette carte x et les paramètres de contrôle p sont utilisées comme des clés secrètes.

Le système chaotique PWLCM est utilisé à la fois dans la permutation et la diffusion.

Dans la phase de confusion, nous convertissons une séquence aléatoire à une séquence entière en utilisant l'équation suivante :

$$\alpha_i = fix(bits\text{ll}\,(x_{i,}8)) \quad \textbf{(Eq.II.10)}$$

Où fixe(n) retourne la partie entière de n, et bits (n,i) renvoie la valeur entière du résultat de décalage logique à gauche de l'entrée n par i bits..[7].

II.8 Cryptographie Chaotique :

II.8.1 Principe :

La cryptographie chaotique est l'une des alternatives développées durant cette dernière décennie. Elle répond non seulement aux exigences de la sécurité mais elle a démontré une grande résistance à la cryptanalyse, comme elle est parfaitement combinée avec le maintien des attributs nécessaires aux algorithmes de chiffrement. Sachant qu'il y a deux types de fonctions chaotiques, part celles qui ont un comportement purement chaotique et qui ne sont pas modélisables, et d'autre part les fonctions chaotiques déterministes qui sont modélisables par des systèmes d'équations qu'on nomme « systèmes dynamiques non linéaires », et ce sont ces dernières qui sont utilisées dans le chiffrement chaotique car leurs attracteurs sont sous forme fractale et rendent l'évolution des trajectoires totalement dépendantes des conditions initiales, et il est donc impossible de prédire ces trajectoires sans connaitre leurs états initiaux, ce qui rend le comportement chaotique imprévisible, et leur sécurité quasi totale. Et pour les introduire dans le chiffrement il faut d'abord choisir une fonction chaotique, ensuite il faut superposer le signal chaotique au flux de données à transmettre selon l'une des techniques choisies pour le cryptage par chaos.[14].

II.8.2 Système de cryptage par chaos

Un système de cryptage par chaos est constitué de deux parties : le brouilleur et le décrypteur. Ceux ci sont strictement identiques pour assurer de façon optimale le respect des conditions initiales La synchronisation des dispositifs est établie dans le système récepteur qui amorce le chaos en injectant dans sa boucle à retard l'ensemble de l'information à transmettre superposée à la dynamique chaotique. Cet ensemble constitue un système de

cryptage symétrique à clé secrète. L'émetteur et le récepteur possèdent la même clé. La synchronisation va représenter la phase critique de l'opération de décryptage. Du fait de la nature complexe du comportement du signal brouilleur, le moindre écart lors du décodage va entraîner un parasite sur l'information appelé "bruit de déchiffrement' '.Une mauvaise synchronisation rendra illisible' information.

L'idée fondamentale exige que l'émetteur produit un signal chaotique pour masquer le message à transmettre, appelé également le "plaintext". À l'extrémité du récepteur, un second système chaotique est induit pour synchroniser avec le signal entrant masqué, également appelé le "ciphertext". Une simpleopération de soustraction indiquerait alors le message (cleartext). [20].

II.9 Conclusion :

La cryptographie est essentielle pour sécuriser les communications en chiffrant les données, tandis que la cryptographie chaotique utilise le chaos déterministe pour renforcer la sécurité. La génération aléatoire des clés, la gestion sécurisée des clés et la vigilance face aux avancées technologiques sont cruciales pour maintenir la robustesse des systèmes cryptographiques. Comprendre ces domaines est vital pour protéger la confidentialité et l'intégrité des données dans notre monde numérique en constante évolution.

Bibliographie du chapitre 02

[1] Floriane Anstett. Les systèmes dynamiques chaotiques pour le chiffrement : synthèse et cryptanalyse. Thèses, Université Henri Poincaré -Nancy I, July 2006

[2] R. Dumont, Cryptographie et Sécurité informatique, Notes de cours provisoires, Universitéde Liège, 2009 – 2010

[3] BEKKOUCHE TOUFIK.Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes.l'obtention du Diplôme de DOCTORAT EN SCIENCESSoutenue le 14/10/2018

[4] HADJI Faiçal. Conception et réalisation d'un système de cryptage pour les images médicales. Mémoire présenté pour l'obtention Du diplôme de Master Académique UNIVERSITE MOHAMED BOUDIAF - M'SILA ,2017-2018

[5] Pauline Puteaux. Analyse et traitement des images dans le domaine chiffré. Cryptographie et sécurité [cs.CR]. Université Montpellier, 2020. Français.

[6]https://www.bitpanda.com/academy/fr/lecons/qu-est-ce-que-le-chiffrement-asymetrique.

[7] Beloucif Assia Informatique Contribution à l'étude des mécanismes cryptographiques
L'obtention du diplôme de Doctorat en Soutenue le: 22 / 09 / 2016

[8] Mme Samia BELKACEM Thème Chaos based image watermarking THÈSE Présentée pour l'obtention du diplôme de DOCTORAT en SCIENCES en Électronique Université Hadj Lakhdar Batna

[9] Hassan NOURA Conception et simulation des générateurs, crypto-systèmes et fonctions de hachage basés chaos performants ,Mémoire présenté en vue de l'obtention du grade de Docteur de l'Université de Nantes Sous le label de l'Université Nantes Angers Le Mans

[10] Fekhr El Islam Khelil Les systèmes chaotiques pour le chiffrement Mémoire de fin d'études Pour l'obtention du diplôme de Master Université Larbi Ben M'hidi - Oum El Bouaghi

[11]https://web.maths.unsw.edu.au/~lafaye/CCM/crypto/rsa.htm

[12]ELHACHI HANA ,Sécurisation de la Couche Physique OFDM Dans un Réseau de Capteurs : Application sur les Images Médicales ; l'Obtention du Diplôme de Master Académique Université 8 Mai 1945 – Guelma

[13] https://www.apprendre-en-ligne.net/crypto/blocs/feistel.html

[14] ARBANE Dehbia ARAB Katia, « Conception de crypto-systèmes à base de systèmes chaotiques d'ordre fractionnaire : Application au cryptage de la parole», Université Mouloud Mammeri De Tizi-Ouzou, 09 juillet 2018.

[16] https://chat.openai.com/

[17] http://nopb.chez.com/crypto2.html

[18]BOUCHENINE HOUSSAM ,GUERMACHE OUSSAMA Etude de la dynamique et chaotique du

système de Lorenz , Mémoire préparé en vue de l’obtention du diplôme de Master Université de Mila

[19]ELHACHI HANA «Sécurisation de la Couche Physique OFDM Dans un Réseau de Capteurs : Application sur les Images Médicales» Mémoire de Fin d'Etude pour l’Obtention du Diplôme de Master Académique Université de Guelma

[20]Terchoune Fatma Zohra, Mehdad Hanaa Lina Thème :La Cryptographie des images Numériques par des Cartes Chaotiques Unidimensionnelles (1D) Mémoire préparé en vue de l’obtention du diplôme de Master Université de DJELFA

Chapitre 03
Application des cartes chaotiques 1D à la cryptographie des images

III.1. Introduction

Dans le domaine de la cryptographie, de nombreuses techniques de chiffrement d'images ont été proposées par les chercheurs. Dans ce chapitre, nous allons utiliser MATLAB pour simuler deux techniques distinctes de chiffrement et de déchiffrement d'images synthétiques et médicales. Nous allons utiliser des cartes chaotiques unidimensionnelles (1D) pour générer une clé pseudo-aléatoire et évaluer les résultats obtenus. Les cartes chaotiques 1D prises en compte dans cette étude sont la carte Logistique, la carte Tent et la carte chaotique linéaire par morceaux PWLCM (Piecewise Linear Chaotic Maps). Ensuite, nous présenterons une comparaison des performances de ces deux algorithmes de cryptographie afin de déterminer celui qui offre une protection maximale. Pour évaluer cette étude, nous utiliserons des critères tels que l'histogramme, le coefficient de corrélation, l'entropie, le NPCR (Normalized Pixel Change Rate) et l'UACI (Unified Average Changed Intensity) pour évaluer les performances des deux méthodes de cryptage d'images.

III.2. Modèle de simulation utilisé

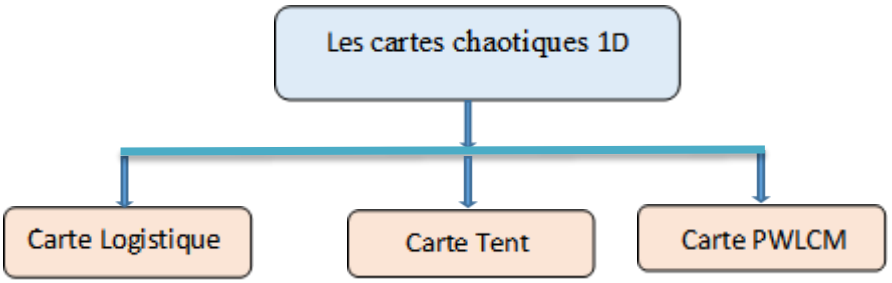


Figure III.1 Classification cartographique chaotique.

Les cartes chaotiques sont des équations mathématiques utilisées pour générer des séquences aléatoires sensibles à leurs conditions initiales et à leurs paramètres de contrôle. Elles sont classées en cartes chaotiques 1D (unidimensionnelles) et cartes chaotiques MD (multidimensionnelles). Les cartes chaotiques 1D sont largement utilisées dans la cryptographie d'images en raison de leur simplicité.

La figure III.1 présente les cartes chaotiques 1D considérées dans ce mémoire

.

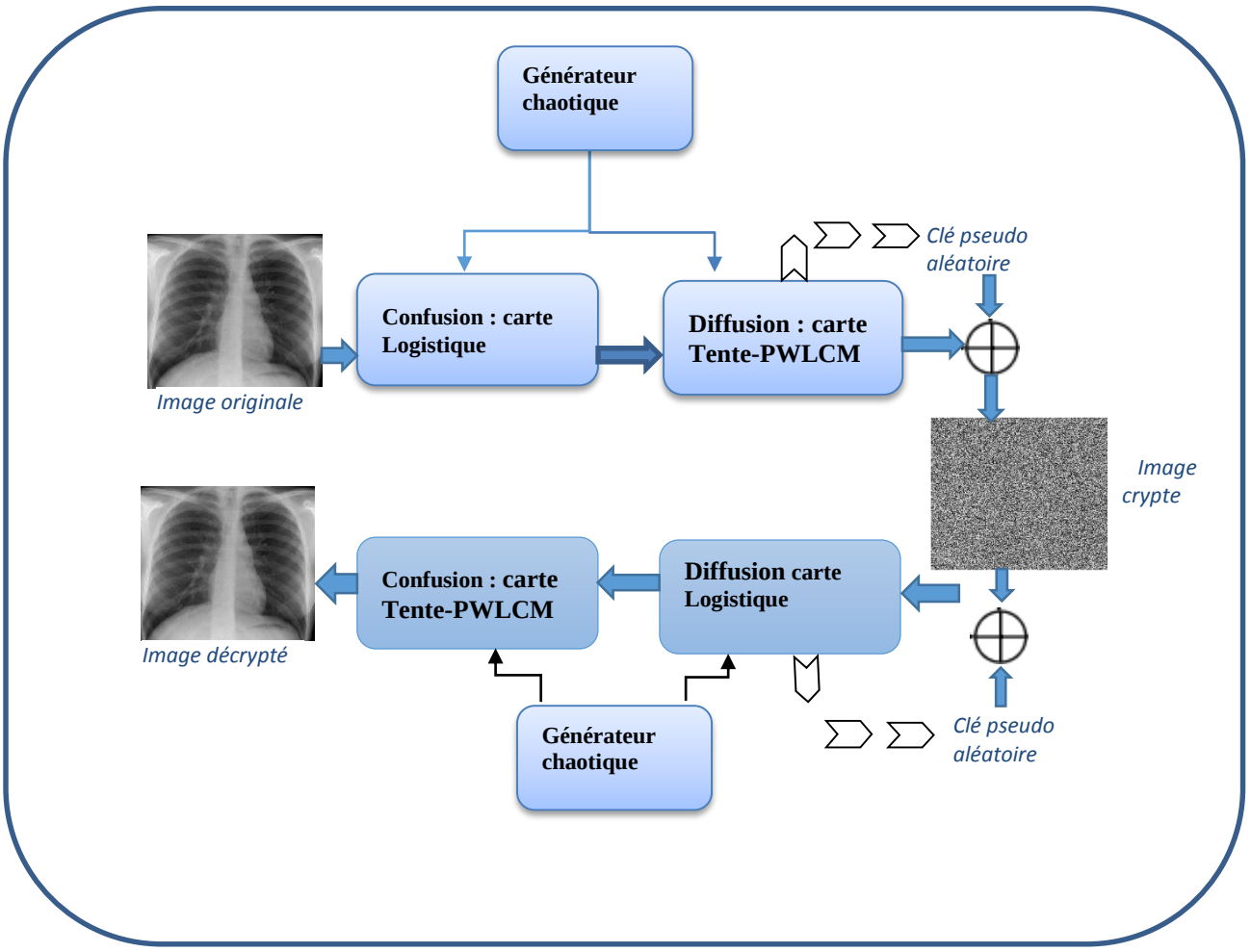


Figure III.2 : Schéma de cryptage utilisé.

Dans le schéma proposé, nous avons utilisé deux algorithmes de cryptographie à base des cartes chaotiques 1D contient deux opérations : la 1ère opération si la confusion pour faire la permutation des pixels en utilisons la carte chaotique logistique, ensuite la 2ème opération si

la diffusion en utilisons la carte Tent ou la carte chaotique PWLCM pour générer un séquence de clés pseudo aléatoire avec même taille d'image, puis faire l'opération XOR élément par élément entre image en clair et le flux de clés pseudo aléatoire généré.

III.2.1. Génération d'un flux de clés chaotiques

1) la 1 ère algorithme : Le premier générateur pseudo-aléatoire est basé sur la carte logistique chaotique (confusion) utilisant la formule mathématique suivante :

$$x(i+1) = \mathrm{r} * x_{(i)} * (1\text{-}x_{(i)}) \quad \textbf{III.}1$$

Les paramètres initiaux sont : (r, x), où r = 3.999 et $0 < x \leq 1$.

De plus, il utilise la carte tente chaotique (diffusion) qui utilise la formule mathématique suivante :

$$x(i+1) = \mathrm{F}(x_i, u) = \begin{cases} ux_n, & si \ \ x_{i<0,5} \\ u(1-x_i), & ailleur \end{cases} \qquad \textbf{III.}2$$

Les paramètres initiaux sont : u = 1.999 et x (1) = 0.5.

2) La 2ème algorithme : Le premier générateur pseudo-aléatoire est basé sur la carte logistique (confusion) et La deuxième générateur basé sur la carte chaotique PWLCM (diffusion) qui utilisent la formule mathématique suivante :

$$x(i+1) = \mathrm{PWLCM}\ (x_i, p) \qquad \textbf{III.}3$$

Les paramètres initiaux sont : p = 0.37 et x (1) = 0.001.

III.2.2.Méthode de chiffrement

Dans cette section, nous allons donner un exemple qui explique clairement les étapes à suivre pour crypter une image en niveau de gris

1. Lecture de l'image d'origine : L'image est lue à partir d'un fichier et stockée dans une variable.

2. Conversion de l'image en niveaux de gris : Si l'image est en couleur, elle est convertie en niveaux de gris à l'aide de la fonction `rgb2gray`.

3. Initialisation des paramètres initiales (r, x(1)) la carte chaotique logistique

4. Génération d'une séquence de nombres chaotiques en utilisant la carte chaotique logistique : La carte logistique est utilisée pour générer une séquence de nombres chaotiques en itérant. Cette séquence est générée pour couvrir la taille totale de l'image (nombre de lignes × nombre de colonnes).

5. Permutation des pixels de l'image en utilisant la séquence de nombres générée : La séquence de nombres chaotiques est triée, et les indices de tri sont enregistrés. Les pixels de l'image sont ensuite permutés en utilisant ces indices, ce qui entraîne un mélange aléatoire des pixels.

6. Initialisation des paramètres pour la carte chaotique de diffusion : Le paramètre `u` est initialisé à une valeur spécifique et la valeur initiale `k(1)`.

7. Génération d'une séquence de clés pseudo-aléatoires en utilisant la carte chaotique de diffusion : La carte de diffusion (carte "tent" ou 'PWLCM') est utilisée pour générer une séquence de clés pseudo-aléatoires de la même taille que l'image. Cette séquence de clés est obtenue en itérant la carte de diffusion et en appliquant des conditions pour déterminer la prochaine valeur de `k(i)` en fonction de la valeur précédente et du seuil 0.5.

8. Application de l'opération XOR entre l'image permutée et la séquence de clés : Chaque pixel de l'image permutée est combiné avec le pixel correspondant de la séquence de clés pseudo-aléatoires en utilisant l'opération XOR (OU exclusif). Cela a pour effet de mélanger davantage les pixels de l'image et d'introduire l'élément de chiffrement.

9. Affichage de l'image chiffrée : L'image chiffrée est affichée à l'aide de la fonction `imshow`.

III.2.3. Méthode de déchiffrement :

1. Répétition des étapes 3 à 7 de la méthode de chiffrement : Les mêmes étapes de génération de la séquence de clés pseudo-aléatoires sont répétées pour obtenir la même séquence de clés utilisée lors du chiffrement.

2. Application de l'opération XOR entre l'image chiffrée et la séquence de clés : L'opération XOR est à nouveau appliquée entre l'image chiffrée et la séquence de clés pour restaurer l'image

d'origine. Étant donné que l'opération XOR est réversible (XOR d'un XOR est égal à la valeur d'origine), cela permet de récupérer les pixels d'origine.

3. Rétablissement de l'ordre des pixels en utilisant la séquence de nombres générée dans la méthode de chiffrement : Les pixels de l'image déchiffrée sont rétablis dans leur ordre d'origine en utilisant la séquence de nombres générée lors de l'étape de permutation dans la méthode de chiffrement.

4. Affichage de l'image déchiffrée : L'image déchiffrée est affichée à l'aide de la fonction `imshow`.

III.3. Résultats expérimentaux

III.3.1. Image niveau de gris et images médicales

Des simulations numériques ont été réalisées pour confirmer les bonnes performances de notre schéma de cryptage. Les figures au-dessous montrent quatre images au niveau de gris de différentes tailles sont cryptées. À l'aide de les cartes chaotiques suggérée.

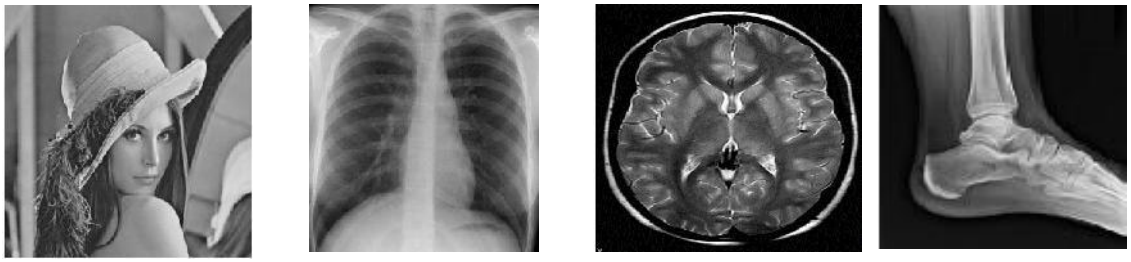


Figure III.3 les images originales

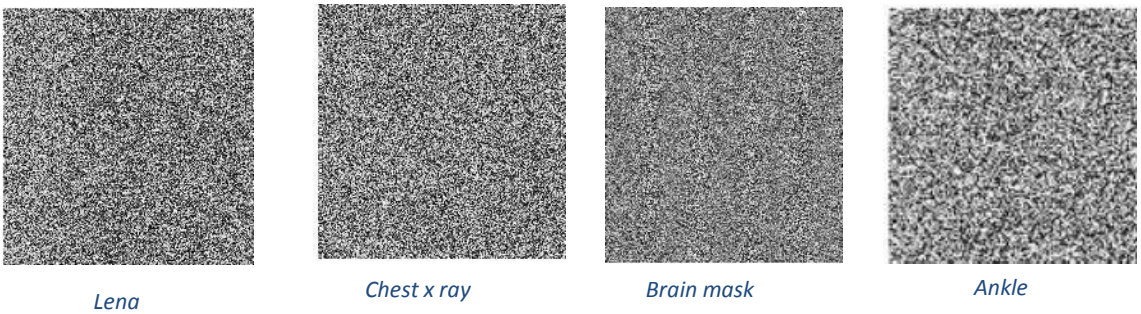
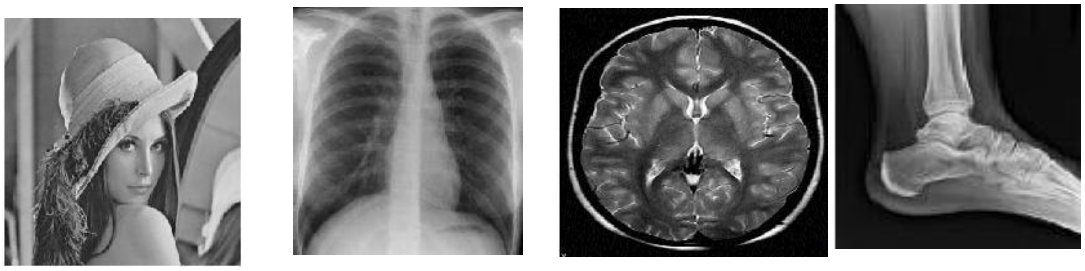
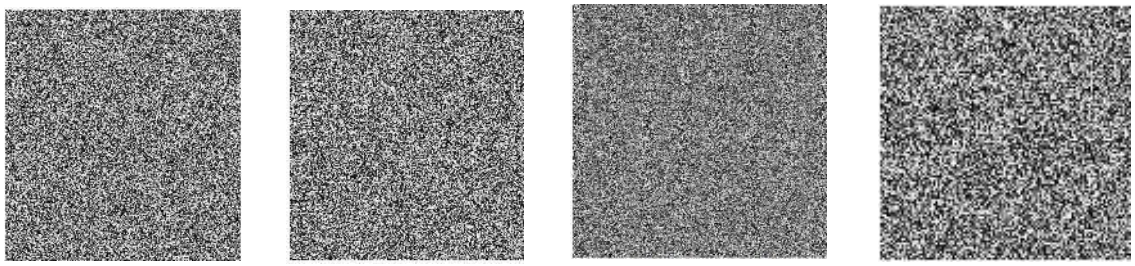


Figure III.4 : Les résultats de cryptage d'images par la carte chaotique logistique et Tente.



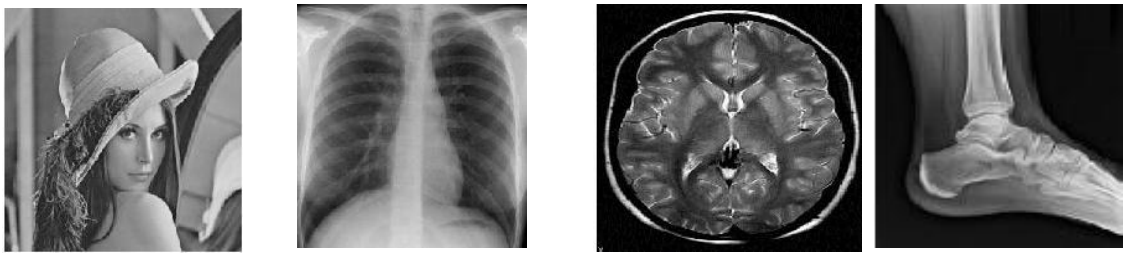
Lena Chest x ray (Thorax) Brain mask Ankle

Figure III.5 : Les résultats de décryptage d'images par la carte chaotique logistiqueTente



Lena Chest x ray(Thorax) Brain mask Ankle

Figure III.6 : Les résultats de cryptage d'images par la carte chaotique logistique et PWLCM.



Lena chest x ray(Thorax) Brain mask Ankle

Figure III.7 : Les résultats de décryptage d'images par la carte chaotique logistique PWLCM.

III.4. Comparaison de Performances

III.4.1. L'espace de clé

Un bon algorithme de chiffrement doit être sensible à la clé de chiffrement, et l'espace de clé doit être suffisamment grand et plus long que la taille de l'image pour rendre une attaque impossible. Dans notre travail, les clés utilisées sont générées par l'un des trois cartes chaotiques considérées dans notre simulation. Ces clés sont des nombres aléatoires de taille n × m (même taille que l'image d'origine). Comme la taille des images est de 256x256 et que chaque élément est codé sur 8 bits, l'espace des clés est de :

$$2^{14*14*14}$$

III.4.2. L'histogramme

Une image-histogramme montre la distribution des pixels dans une image graphique en traçant le nombre de pixels correspondant à chaque intensité de couleur. Dans notre étude, des simulations numériques ont été effectuées pour confirmer les meilleurs résultats parmi les deux algorithmes de chiffrement proposées pour générer les clés. Dans nos simulations, nous avons utilisé l'image de Lena de taille 256x256 comme image en clair. Les figures ci-dessous montrent les résultats des histogrammes avant et après le cryptage par les deux générateurs chaotiques de chiffrement proposés.

Lena

Figure III.8: Image en claire

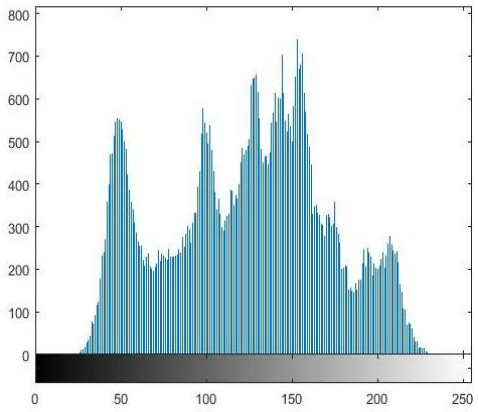
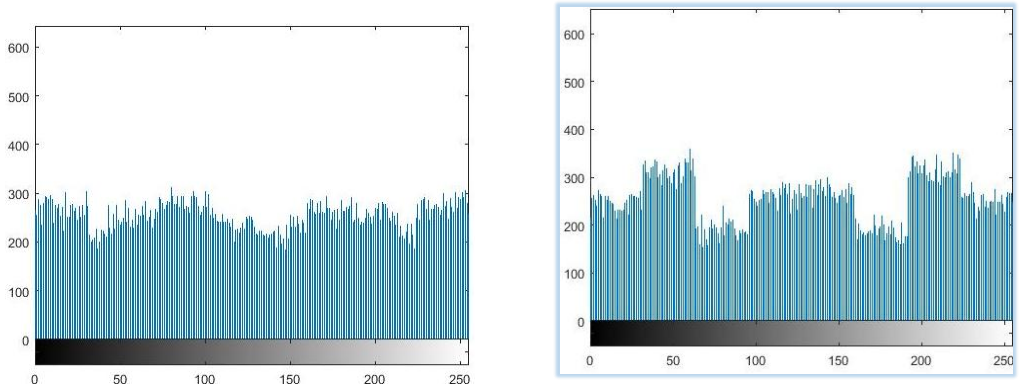


Figure III.9 : L'histogramme d'image de Lena en claire



(a) la 1 ère algorithme Carte logistique et Carte Tent

***(b)* la 2 ème algorithme Carte logistique Carte PWLCM.**

Figure III.10 : L'histogramme d'image chiffrée

Les résultats de simulation montrent que l'histogramme de l'image cryptée par le premier algorithme est presque uniforme et mieux que le deuxième algorithme après le chiffrement. Par conséquent, l'attaquant ne peut pas extraire d'informations de l'histogramme image cryptée pour la 1ère algorithme et difficile par rapport à la 2éme algorithme.

III.4.3 Entropie

La valeur d'entropie de l'image cryptée est calculée en utilisant la fonction "entropy" qui calcule la valeur d'entropie de l'image cryptée.

Une valeur d'entropie élevée indique une plus grande complexité et variabilité des valeurs de pixels dans l'image cryptée. De même, une valeur d'entropie faible indique une plus grande répétitivité des valeurs de pixels dans l'image cryptée. Cette information est importante pour évaluer la qualité du cryptage et sa capacité à protéger les données et à résister aux attaques.

Tableau III.1 : Le test d'entropie des images cryptées à l'aide deux algorithmes.

Chaos / Images	Carte Logistique pour confusion et tente pour diffusion	Carte Logistique pour confusion et PWLCM pour diffusion
	Image Cryptée	Image Cryptée
Lena	**7.991629**	**7.973516**
Ankle	**7.932366**	**7.972995**
Thorax	**7.989692**	**7.988430**
MRI	**7.879694**	**7.986733**
Moyenne	**7,94834525**	**7,9804185**

En comparant les valeurs d'entropie dans le tableau, on peut observer que l'utilisation combinée de la carte logistique et de la carte Tent donne une valeur moyenne d'entropie d'environ 7,94834525, tandis que l'utilisation de la carte logistique avec la carte PWLCM donne une valeur moyenne d'entropie d'environ 7,9804185.

Sur la base de cette comparaison, on peut dire que l'utilisation combinée de la carte logistique et de la carte PWLCM produit une difficulté d'avoir la prévisibilité par rapport à l'utilisation combinée de la carte logistique et de la carte Tent. Cela suggère que la carte logistique et la carte PWLCM peuvent être plus efficaces pour préserver la confidentialité de l'image et résister aux attaques différentielles.

III.4.4. La corrélation entre les pixels adjacents

Les coefficients de corrélation entre les pixels adjacents ont été calculés dans les directions horizontale, verticale et diagonale pour évaluer les relations entre les valeurs de pixels voisins dans les images originales et les images cryptées. Ces coefficients de corrélation fournissent des mesures quantitatives de la similarité ou de la corrélation entre les pixels adjacents.

Dans le code fourni, les images originales sont représentées par la variable "A" et les images cryptées sont représentées par la variable "A2". Les coefficients de corrélation sont calculés en utilisant la fonction "corrcoef" sur les valeurs de pixels voisins dans les différentes directions. Par exemple, les coefficients de corrélation horizontale sont calculés en prenant les pixels adjacents dans la même ligne de l'image.

En analysant les coefficients de corrélation obtenus, on peut évaluer la similarité des images originales et les images cryptées. Une corrélation élevée indique une forte similarité, tandis qu'une corrélation faible indique une faible similarité. Cette analyse fournit des informations sur la qualité du cryptage et l'efficacité des méthodes de confusion et de diffusion utilisées.

Tableau III.2 : Valeurs des coefficients de corrélation des images originales et cryptées par des les deux méthodes de cryptages.

		Carte Logistique pour confusion et tente pour diffusion		**Carte Logistique pour confusion et PWLCM pour diffusion**	
		Image en Clair	**Image Cryptée**	**Image en Clair**	**Image Cryptée**
Lena	**Horizontal**	**0.9423**	**0.0056**	**0.9423**	**-0.0012**
	Vertical	**0.9706**	**-0.0058**	**0.9706**	**-0.0014**
	Diagonal	**0.9705**	**-0.0059**	**0.9705**	**-0.0019**
MRI	**Horizontal**	**0.9602**	**0.0041**	**0.9602**	**0.0017**
	Vertical	**0.9646**	**0.1048**	**0.9646**	**-0.0012**
	Diagonal	**0.9645**	**0.1048**	**0.9645**	**-0.0015**

Thorax	**Horizontal**	**0.9940**	**0.0012**	**0.9940**	**-0.0014**
	Vertical	**0.9950**	**-0.0033**	**0.9950**	**0.0029**
	Diagonal	**0.9950**	**-0.0031**	**0.9950**	**0.0027**
Ankle	**Horizontal**	**0.9130**	**-0.0068**	**0.9130**	**0.0032**
	Vertical	**0.9722**	**0.0950**	**0.9722**	**-0.0162**
	Diagonal	**0.9702**	**0.0966**	**0.9702**	**-0.0173**

Dans le tableau présenté, quatre types d'images claires et chiffrées ont été comparés en utilisant les algorithmes Carte Logistique, Tente et PWLCM pour la confusion et la diffusion. Les coefficients de corrélation entre les pixels adjacents ont été calculés dans les directions horizontale, verticale et diagonale. Si la valeur de corrélation se rapproche de 1, cela signifie que l'image originale et l'image chiffrée sont fortement corrélées. Si la valeur de corrélation se rapproche de 0, cela signifie que l'image chiffrée et l'image originale ne sont pas corrélées.

Selon les résultats du tableau, on peut constater que les valeurs de corrélation des images chiffrées, dans tous les cas de test, sont proches de zéro, ce qui indique une meilleure qualité de chiffrement.

Le calcul des coefficients de corrélation ci-dessous est étayé par la représentation de la distribution des corrélations entre les pixels adjacents horizontaux, verticaux et diagonaux de l'image originale et chiffrée de Lena, en utilisant l'algorithme qui utilise la carte logistique et PWLCM.

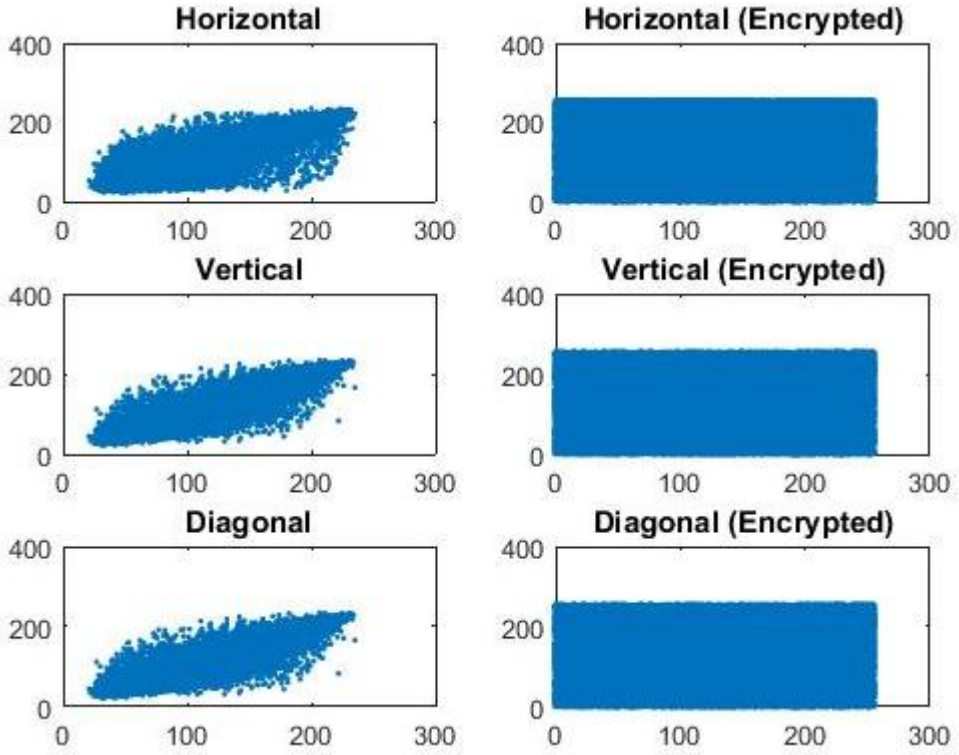


Image originale Image chiffrée

Figure III.11 : La corrélation entre les pixels adjacents dans l'image originale et chiffrée de Lena.

III.4.5 NPCR et UACI

NPCR (Normalized Pixel Change Rate) et UACI (Unified Average Changing Intensity) sont deux critères de calcule la sensibilité de la clé.

- NPCR (Taux de Changement de Pixel Normalisé) : Il est calculé en estimant le pourcentage de changement des valeurs relatives des pixels entre les deux images cryptées. Cela est fait en comptant le nombre de pixels qui diffèrent entre les deux images et en le divisant par le nombre total de pixels dans l'image.
- UACI (Intensité de Changement Moyenne Unifiée) : Il est calculé en estimant l'uniformité des changements absolus des pixels entre les deux images cryptées. Cela est fait en calculant la moyenne des valeurs absolues des changements de pixels et en la divisant par la valeur maximale possible des changements de pixels.

Ces deux mesures sont utilisées pour évaluer le degré de variation de l'image cryptée après le processus de cryptage. Des valeurs élevées de NPCR indiquent une forte variation de l'image, tandis que des valeurs élevées de UACI indiquent une uniformité faible des valeurs de changement des pixels. En général, des valeurs faibles de NPCR et des valeurs élevées de UACI sont

préférables pour préserver la confidentialité de l'image et résister aux attaques.

Tableau III.3 : NPCR et UACI de différentes images utilisant deux algorithmes chaotiques 1D.

Images	Critères	Carte Logistique pour confusion et tente pour diffusion	Carte Logistique pour confusion et PWLCM pour diffusion
Lena	**NPCR**	**99.606323**	**99.551392**
	UACI	**33.711907**	**33.874709**
Thorax	**NPCR**	**99.615479**	**99.444580**
	UACI	**33.506601**	**33.437362**
MRI	**NPCR**	**99.474142**	**99.606075**
	UACI	**33.790347**	**33.881400**
Ankle	**NPCR**	**99.500217**	**99.529190**
	UACI	**33.757673**	**33.920148**
Moyenne	**NPCR**	**99,54904025**	**99,53280925**
	UACI	**33,691632**	**33,77840475**

Suite à l'analyse du tableau fourni, on peut conclure que l'utilisation de "Carte Logistique pour confusion et PWLCM pour diffusion" donne des valeurs plus élevées de NPCR et UACI par rapport à "Carte Logistique pour confusion et tente pour diffusion" presque pour toutes les images analysées. Cela indique que "Carte Logistique pour confusion et PWLCM pour diffusion" présente de meilleures performances dans la résistance aux attaques différentielles par rapport à l'autre.

Il convient de noter qu'il peut y avoir d'autres facteurs qui influencent les performances des algorithmes utilisés dans le cas spécifique, et des études supplémentaires et des tests peuvent être nécessaires pour évaluer les performances de manière plus complète et précise.

Sur la base des résultats présentés, on peut considérer "Carte Logistique pour confusion et PWLCM pour diffusion" comme la meilleure option pour protéger les images contre les attaques différentielles.

III.4.5 Cross Correlation:

La corrélation croisée (Cross Correlation) est une mesure utilisée pour évaluer la similarité entre deux ensembles de données. Dans le contexte du traitement d'images, la corrélation croisée est utilisée pour mesurer le degré de corrélation entre deux images.

Tableau III.4 : de La corrélation croisée

Images	**Carte Logistique pour confusion et tente pour diffusion**	**Carte Logistique pour confusion et PWLCM pour diffusion**
Lena	**-0.012813**	**-0.004738**
Thorax	**0.000464**	**0.002296**
MRI	**-0.001834**	**-0.000468**
Ankle	**-0.002611**	**-0.009108**
Moyenne	**-0,0041985**	**-0,0030045**

Dans le tableau donné, les mesures de corrélation croisée sont comparées pour les images traitées à l'aide des deux algorithmes «1ère algorithme Carte logistique et carte Tente et 2ème algorithme Carte logistique et PWLCM ». La corrélation croisée est une mesure de similarité entre deux images, et des valeurs proches de zéro indiquent une faible corrélation et une bonne dissimulation des informations.

Selon les valeurs de corrélation croisée dans le tableau, on peut conclure que les deux algorithmes, "Carte logistique/Tente" et "Carte logistique/PWLCM", parviennent à obtenir des valeurs de corrélation croisée proches de zéro pour toutes les images testées (Lena, Thorax, MRI, Ankle). Cela suggère que les deux techniques offrent une bonne dissimulation des informations et préservent efficacement la confidentialité des données.

III.5 Conclusion :

Les cartes chaotiques unidimensionnelles sont largement utilisées pour les problèmes de sécurité en raison de leur simplicité et de leur comportement chaotique par rapport à d'autres cartes chaotiques multidimensionnelles qui peuvent être complexes pour la mise en œuvre matérielle et difficiles à analyser. Cependant, les cartes chaotiques unidimensionnelles classiques présentent une gamme réduite de comportements chaotiques. Les résultats expérimentaux ont montré que le système de cryptage par

1ère algorithme Carte Logistique pour confusion et PWLCM pour diffusion possède un grand espace de clés et une sécurité de haut niveau, ainsi que l'analyse et la comparaison de l'entropie et la corrélation des images chiffrées par rapport à 1ème algorithme carte logistique pour confusion et la carte tente pour diffusion assurent une efficacité, une haute protection et sécurité contre les attaques brutes

Conclusion générale

Conclusion Générale

Dans notre mémoire, nous avons abordé les problèmes de sécurité liés aux images médicales, qui sont similaires à ceux rencontrés dans la protection des données médicales en général. Nous avons identifié les aspects clés de la sécurité de l'information médicale tels que la confidentialité, la disponibilité, la fiabilité, l'intégrité et l'authenticité des données.

Pour répondre à ces enjeux, nous avons proposé l'utilisation de deux algorithmes de cryptage d'images basés sur des cartes chaotiques unidimensionnelles (1D). Les cartes chaotiques considérées dans notre étude étaient la carte Logistique, la carte Tentet la carte chaotique linéaire par morceaux PWLCM (PiecewiseLinearChaoticMaps).

L'objectif principal de notre étude était de comparer les performances de ces deux algorithmes en termes de sécurité. Après avoir mené des expériences et analysé les résultats, nous avons constaté que l'algorithme basé sur la carte Logistique chaotique et la carte PWLCM offraient de bonnes performances et étaient bien adaptés au chiffrement en temps réel.

De plus, nous avons observé que l'histogramme des images cryptées était presque uniforme, ce qui rendait difficile pour un attaquant d'extraire des informations à partir de cet histogramme. Les algorithmes utilisés ont également démontré de bons résultats en termes d'entropie et de corrélation entre les pixels adjacents, ce qui renforce leur efficacité et leur sécurité.

En conclusion, notre étude a permis de déterminer que l'algorithme basé sur la carte Logistique chaotique et la carte PWLCM étaient particulièrement performants et adaptés au cryptage d'images médicales. Ces résultats ouvrent la voie à de futures recherches et à l'application de ces techniques de cryptage dans le domaine médical.

Résumé

La cryptographie est connue depuis longtemps comme un outil qui sert à protéger des informations secrètes contre toutes tentations d'usurpation menées par des gens malhonnêtes. Aujourd'hui avec le développement accru des TICs et l'expansion de l'utilisation de données numériques dans diverses applications, il est devenu important de développer des algorithmes cryptographiques permettant de de protéger les données d'image confidentielles contre les accès non autorisés et cela est garantie grâce à la cryptographie chaotique.

Dans ce mémoire de fin d'étude, nous avons utilisé deux algorithmes de cryptage qui peutêtre appliqué aux images normales et médicales en niveaux de gris. Ces algorithmes sont basés sur des cartes chaotiques unidimensionnelles (1D) telles que les cartes chaotiques logistique, Tent et la carte chaotique linéaire par morceaux PWLCM. Après avoir étudié ces algorithmes et mené quelques expériences, nous avons conclu qu'ils offrent de bonnes performances en termes de qualité et sécurité.

Mots-clés : Cryptographie, Cartes chaotiques, Logistique, Tent, PWLCM, chiffrement.

Abstract

Cryptography has long been known as a tool used to protect secret information against any temptations of usurpation carried out by dishonest people. Today with the increased development of ICTs and the expansion of the use of digital data in various applications, it has become important to develop cryptographic algorithms to protect confidential image data against unauthorized access and that is secured through chaotic cryptography.

In this graduation, we used two encryption algorithms that can be applied to normal and medical grayscale images. These algorithms are based on one-dimensional (1D) chaotic maps such as Logistic, Tent chaotic maps and the PWLCM piecewise linear chaotic map. After studying these algorithms and conducting some experiments, we concluded that they offer good performance in terms of quality and security.

Keywords: Cryptography, Chaotic Maps, Logistics,Tent, PWLCM, encryption