

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique



Mémoire de Master

Filière Électronique
Spécialité Instrumentation Biomédicale

présenté par

Belaid Zineddine

&

Zedame Yamina

CRYPTAGE HYPER- CHAOTIQUE APPLIQUE EN IMAGERIE MEDICALE

Proposé par : Mr.CHIKHI Mohamed Lazhar

Année Universitaire 2018-2019

Dédicaces

A mes chers parents

Pour tous les sacrifices qu'ils ont faits et pour tout le soutien qu'ils ont apporté tout au long de mes études.

A mes frères et sœurs et à tous mes amis et collègues,

Mon binôme Y.Zedame

Pour leur encouragement et pour tous les bons moments qu'on a vécus ensemble.

Z.Belaid

Dédicaces

A mes chers parents

Pour tous les sacrifices qu'ils ont faits et pour tout le soutien qu'ils ont apporté tout au long de mes études.

A mes frères et sœurs et à tous mes amis et collègues,

Mon binôme Z.Belaid

Pour leur encouragement et pour tous les bons moments qu'on a vécus ensemble.

Y.Zedame

Remerciements

Tout d'abord, nous tenons à remercier Mr CHIKHI.1 de nous avoir encadrés. ses conseils et son expérience ont beaucoup aidé à la réussite de notre travail.

Nous exprimons notre profonde gratitude à notre chef de filière Mr CHERFA.Y ainsi qu'à tous nos professeurs.

Les travaux présentés dans ce mémoire ont été effectués au Laboratoire LABSET du département d'électronique de l'université de Blida 1. Nos remerciements les plus sincères vont à tous les membres du laboratoire qui nous ont permis de réaliser ce travail dans de très bonnes conditions.

Enfin, nous remercions nos parents pour leur soutien et leurs encouragements pendant toute la période de préparation de ce mémoire.

ملخص:

في هذا العمل ، قمنا بتحليل وتطبيق نظام لنقل الصور الطبية بشكل آمن ، استنادًا إلى تشفير شديد الفوضى عن طريق الارتباك والانتشار. في مرحلة الارتباك ، تقوم آلية جديدة لإعادة ترتيب البكسل استنادًا إلى الوظيفة Logistique ، بإعادة تنظيم كل بكسل للصورة القياسية من خلال استبدالها بوحدة بكسل أخرى. للنشر ، يتم استخدام نظام Chen شديد الفوضى حيث يتم اختيار متغيرات الحالة هذه لتقدير تدفق المفتاح العشوائي الزائف. في فك التشفير ، نستخدم نفس الأنظمة الفوضوية التي لها نفس الظروف لتتمكن من استعادة الصورة الأصلية. يتم تقديم نتائج محاكاة Matlab Simulink وإجراء اختبارات سلامة تجريبية شاملة تشير إلى أن المخطط المقترح هو وسيلة فعالة لنقل الصور الطبية في الوقت الحقيقي عبر الشبكات العامة.

كلمات المفاتيح: فوضى ؛ التشفير؛ نظام التشفير؛ نشر ؛ الارتباك.

Résumé :

Dans ce travail, nous avons analysé et implémenté un système de transmission sécurisée d'images médicales, basé sur le cryptage hyper-chaotique par confusion et diffusion. Dans la phase de confusion , un nouveau mécanisme de réarrangement de pixels basé sur la fonction logistique ,réorganise chaque pixel de l'image standard en l'échangeant contre un autre pixel .Pour la diffusion le système hyper-chaotique de Chen est utilisé où ces variable d'état sont choisis pour la quantification du flux de clés pseudo-aléatoire. Dans le décryptage, nous utilisons les mêmes systèmes chaotique avec les mêmes conditions pour pouvoir récupérer l'image originale .Les résultats de simulation sous environnement Matlab Simulink sont présentés et des tests expérimentaux approfondis de sécurité sont effectués indiquant que le schéma proposé constitue un moyen efficace pour la transmission d'image médicales en temps réel sur des réseaux publics.

Mots clés : Chaos ; cryptographie ; crypto-système ; confusion ; diffusion;

Abstract :

In this work, we analyzed and implemented a system for the secure transmission of medical images, based on hyper-chaotic encryption by confusion and diffusion. In the confusion phase, a new mechanism of pixel rearrangement based on the logistic function, reorganizes each pixel of the standard image by exchanging it for another pixel. For diffusion, Chen's hyper-chaotic system is used where these state variables are chosen for quantization of the pseudo-random key flow. In the decryption, we use the same chaotic systems with the same conditions to be able to recover the original image. Matlab Simulink simulation results are presented and extensive experimental safety tests are performed indicating that the proposed scheme is an effective means for real-time medical image transmission over public networks.

Keywords : Chaos ; cryptography; cryptosystem; confusion ; diffusion;

Résumé	
Remerciements	
Dédicace	
Table des matières	
Liste des symboles	
Liste des abréviations	
Liste des figures	
Liste des tableaux	

Introduction générale	1
------------------------------	----------

Chapitre 1 Généralités sur les systèmes chaotiques

1.1. Introduction	4
1.2. Définition	4
1.2.1. Espaces de phase	5
1.2.2. Point fixe ou point d'équilibre	6
1.3. Stabilité du point fixe	6
1.3.1. Stabilité au sens de Lyapunov	6
1.3.2. Stabilité par méthode indirect de Lyapounov	7
1.4. Chaos	9
1.5. Caractéristiques d'un système dynamique chaotique	10
1.5.1. Bifurcation	10
1.5.2. Diagramme de bifurcation	11
1.5.3. Attracteur étrange	12
1.5.4. Section de Poincaré	15
1.5.5. Les exposants de Lyapunov	17
1.6. Exemples de systèmes chaotiques	18
1.6.1. Système a temps continu	18
1.6.2. Système a temps discret	22
1.7. Conclusion	24

Chapitre 2 Etude du système hyper-chaotique de Chen

2.1. Introduction	25
2.2. Etude du système hyper-chaotique de Chen	25
2.3. Points d'équilibre	27
2.3.1. Stabilité des points d'équilibre	27
2.4. Plan de phase	28
2.5. Exposants de LYAPUNOV	32
2.6. Bifurcation	33
2.7. Attracteur	35
2.8. Section de Poincaré	35
2.9. Conclusion	37

Chapitre 3 Cryptage hyper-chaotique appliqué en imagerie médicale

3.1. Introduction	38
3.2. Système de traitement d'images	38

3.3.	La cryptographie.....	39
3.3.1.	Définition de la cryptographie.....	39
3.3.2.	Historique.....	40
3.3.3.	Terminologies.....	41
3.3.4.	Définition de la clé.....	42
3.4.	Cryptographie et Chaos.....	43
3.5.	Caractéristiques d'une image numérique.....	44
3.6.	Cryptage des images médicales à l'aide des systèmes chaotiques.....	45
3.6.1.	Algorithme de chiffrement.....	45
a.	Phase de confusion.....	46
b.	Phase de diffusion.....	51
3.6.2.	Algorithme de déchiffrement.....	57
3.7.	Intégration du crypto-système proposé.....	58
3.8.	Conclusion.....	60

Chapitre 4 Implémentation et analyses de sécurité

4.1.	Introduction.....	61
4.2.	Analyse différentielle.....	61
4.3.	Analyse de l'espace clef.....	64
4.4.	Test de sensibilité clef.....	65
4.5.	Analyses statistiques.....	68
4.5.1.	Analyse des histogrammes.....	68
4.5.2.	Analyse de l'entropie.....	70
4.5.3.	Analyse de la corrélation.....	71
4.6.	Développement de notre application de cryptage hyper-chaotique.....	74
4.6.1.	Langage de développement.....	74
4.6.2.	Résultat d'exécution.....	75
a.	Cryptage/décryptage des images.....	75
4.7.	Conclusion.....	78
	Conclusion générale.....	79
	Référence.....	81

Liste des symboles :

A	La matrice jacobienne de $f(x)$.
$a(i)$	Le vecteur propre.
a	parametre de bifurcation de système de lorentz.
B	représentent les valeurs d'état du groupe par rapport à la série \bar{x}_1 .
C	Pixel cryptée.
$Df(x)$	Matrice Jacobienne.
I	Le reste de la division.
J	Matrice Jacobienne de système de chen.
K	Paramètre de système de Chen.
M	Nombre de ligne.
N	Nombre de colonne.
N_0	Nombre d'itération pour la diffusion.
$p(i)$	La probabilité d'apparition d'un niveau d'intensité.
$P_{i,j}$	Image originale.
$P_{i,j}(I)$	Pixel de l'image originale, ainsi que son intensité (I).
$P_{h_i,j}$	Image cryptée (ligne).
P_{h_i,I_j}	Image cryptée (ligne, colonne).
$P_{h_i,I_j}(I)$	Pixel de l'image cryptée, ainsi que son intensité (I).
R^n	Espace vectoriel de dimension n .
R^p	Espace vectoriel de dimension p .
u	Vecteur de paramètre du système.
x	Vecteur d'états du système.
\bar{x}	Point fixe.
$\dot{x} = \frac{dx}{dt}$	Dérivée de la variable.
\bar{x}_1	Déduire le groupe de combinaison.
xor	OU exclusif.
λ	La valeur propre.
Σp	Surface de dimension $n - 1$.

Liste des abréviations :

<i>ACM</i>	Rivest Shamir Adleman (Système de cryptage asymétrique).
<i>DES</i>	Data Encryptions Standard.
<i>IDEA</i>	The International Dialects of English.
<i>IBM</i>	International Business Machines
<i>J. C</i>	Jésus crist
<i>NPCR</i>	The number of changing pixel rate.
<i>RSA</i>	A été inventé par Rivest, Shamir et Adleman.
<i>UACI</i>	The unified averaged changed intensity.

Liste des figures

Figure 1.1.	Diagramme de bifurcation du système de Rössler pour $a=0,2$ et $b=0,2$.	12
Figure 1.2.	Quelques attracteur étranges.	13
Figure 1.3.	Différents types d'attracteurs réguliers.	14
Figure 1.4.	Projection par l'application de Poincaré du premier retour.	16
Figure 1.5.	Attracteur de Lorenz.	19
Figure 1.6.	Solutions de système de Lorenz.	19
Figure 1.7.	Exposants de Lyapounov de système de Lorenz.	20
Figure 1.8.	Diagramme de bifurcation du système de Lorenz.	21
Figure 1.9.	Section de Poincaré de système de Lorenz	22
Figure 1.10.	Solution du système (1.16) pour $r=4$	23
Figure 1.11.	Diagramme de bifurcation de la fonction logistique	24
Figure 2.1.	Représentation temporelle des signaux (t) , $y(t)$, $z(t)$ et $w(t)$	26
Figure 2.2.	Plant de phase du système de Chen avec $k=0,2$.	29
Figure 2.3.	Plant de phase du système de Chen avec $k=1,2$.	30
Figure 2.4.	Plant de phase du système de Chen avec $k=3,6$.	30
Figure 2.5.	Plant de phase du système de Chen avec $k=3,7$.	31
Figure 2.6.	Plant de phase du système de Chen avec $k=4$.	31
Figure 2.7.	Exposants de Lyapounov de système de Chen avec $k=0,2$.	33
Figure 2.8.	Diagramme de bifurcation du système de Chen.	34
Figure 2.9.	Attracteur chaotique de Chen.	35
Figure 2.10.	Représentation de la section de Poincaré du système de Chen dans (a) le plan de phase et (b) l'attracteur étrange du système de Chen	36
Figure 3.1.	Schéma d'un système de traitement d'images	39
Figure 3.2.	Schéma général de la communication chiffrée entre un émetteur et un récepteur.	40
Figure 3.3.	Images médicales.	46
Figure 3.4.	Représentation matriciel d'une image	46
Figure 3.5.	organigramme de chiffrement par permutation des lignes et des colonnes	47
Figure 3.6.	Chiffrement par ligne appliqué aux images (a, b, c) , (a', b', c') sont les images cryptées correspondante.	49
Figure 3.7.	Chiffrement par lignes (a', b', c') suivi d'un chiffrement par colonnes (a'', b'', c'') des 3 images médicale.	51
Figure 3.8.	Organigramme de chiffrement par diffusion.	52
Figure 3.9.	Chiffrement par permutation suivi d'un chiffrement par diffusion des images (a, b, c) .	56
Figure 3.10.	Principe de décryptage.	58
Figure 3.11	Intégration du crypto-système dans une chaine de tél- radiologie.	59
Figure 4.1.	Résultats d'efficacité de notre algorithme pour les valeurs de NPCR et UACI.	63
Figure 4.2.	Résultat expérimental de chiffrement et de déchiffrement.	66
Figure 4.3.	les images originales(a)L'histogramme des images originales(b) et chiffrées(c).	69

Figure 4.4.	Corrélations des pixels adjacents pour l'image d'IRM. (a) : Horizontalement verticalement et en diagonale pour l'image originale. (b):Horizontalement verticalement et en diagonale pour l'image cryptée	73
Figure 4.5.	Interface générale.	75
Figure 4.6.	Chargement de l'image	76
Figure 4.7.	Choix de l'image	76
Figure 4.8.	Cryptage d'image	77
Figure 4.9.	Sauvegarde de l'image	77

Liste des tableaux

Tableau 1.1.	Application de Poincaré.	17
Tableau 2.1.	Exposants de Lyapunov pour $k=0$ jusqu'à 4.	32
Tableau 3.1.	le lien entre le nombre d'itération et la taille de l'image.	38
Tableau 3.2.	Différentes combinaisons d'états du système hyper-chaotique.	53
Tableau 4.1.	L'espace des clés pour le processus de chiffrement proposé.	65
Tableau 4.2.	Les valeurs d'entropies pour différentes images originales et cryptées.	70
Tableau 4.3.	Les Coefficients de corrélation de deux pixels adjacents dans deux images.	72

Introduction générale

Depuis l'extraordinaire révolution dans les domaines des technologies de communication ces dernières années, la question de la protection des images médicales a suscité de vives préoccupations en raison de la demande croissante de services de télémédecine, en particulier du service de télé-radiologie, c'est-à-dire que les applications médicales traitent souvent avec des données confidentielles des patients, et veillé à ce que les données médicales soient collectées et communiquées de manière sécurisée et accessibles uniquement aux personnes autorisées. Cela est même crucial pour les services de télémédecine / télésanté, car ils impliquent inévitablement la transmission de données médicales, d'imagerie et d'informatique de santé sur des réseaux ouverts tels qu'Internet. De nos jours, la protection de la confidentialité des données médicales est non seulement une exigence éthique, mais également une obligation légale [1].

Pour protéger la liberté et préserver l'intimité de l'information personnelle contre les attaques et pour réduire les vulnérabilités des systèmes, plusieurs solutions ont été proposées, telles que la cryptographie. Cette dernière recouvre l'étude et la conception des procédés de chiffrement des informations ; elle est devenue aujourd'hui un moyen quotidien de protection des données qui doivent être communiquées ou stockées sur une longue période.

Depuis quelques années, la théorie des systèmes non linéaires et surtout chaotiques a été appliquée à la cryptographie afin de proposer d'autres méthodes de chiffrement. En effet, les propriétés des systèmes chaotiques (déterminisme et extrême sensibilité aux conditions initiales) font de ces systèmes de bons outils pour la transmission sécurisée de données. De nombreux schémas sont proposés afin d'appliquer les systèmes chaotiques dans le domaine de la cryptographie.

Pour la cryptographie chaotique, un des concepts les plus importants du déchiffrement, c'est à dire que le récepteur doit reconstruire le même système chaotique avec les mêmes conditions initiales que l'émetteur.

Introduction générale

Dans ce contexte, nous proposons un nouveau crypto-système (algorithme de chiffrement et de déchiffrement) basée sur la permutation et la diffusion en utilisant deux systèmes chaotiques pour le chiffrement d'images médicales.

La permutation des pixels de l'image consiste à les déplacer de manière pseudo aléatoire. En ce sens les pixels sont décalés d'un pas qui dépend des états du système chaotique (fonction Logistique dans le cas de notre projet). Le résultat de ce processus est ce que l'on appelle 'confusion. Pour la diffusion des pixels, c'est-à-dire le changement des valeurs des pixels, le principe est de faire une opération OU EXCLUSIF avec les états du système hyper-chaotique (Système hyper-chaotique de Chen dans le cas de notre projet).

Notre travail de projet de fin d'études a été ainsi structuré en quatre chapitres:

Le premier chapitre présente les principales propriétés des systèmes non linéaires en général et des systèmes chaotiques en particulier. Ces définitions seront utilisées pour la conception du crypto-système chaotique.

Le deuxième chapitre est consacré à l'étude et l'analyse détaillée du système hyper-chaotique de Chen et l'évolution de son comportement en fonction des variations de ses paramètres.

Dans le troisième chapitre, après une présentation générale sur la cryptographie ainsi que son lien avec le chaos, nous proposons un nouveau système de sécurité pour le chiffrement d'images médicales basé sur un système chaotique (fonction logistique) pour le cryptage par confusion et un système hyper-chaotique (système de Chen) pour le cryptage par diffusion.

Le dernier chapitre est consacré à l'analyse des performances de sécurité du chiffrement des images médicales en utilisant les différentes analyses différentielles, statiques, sensibilité et espace de chiffrement de la clé. A cet effet, nous avons effectué une étude comparative des performances de sécurité et la résistance contre les attaques. Ainsi qu'une implémentation graphique du crypto-système.

Introduction générale

Enfin, la conclusion reprend les principaux points abordés dans ce manuscrit et expose certaines perspectives d'approfondissement et d'élargissement pour notre travail.

Chapitre 1 Généralités sur les systèmes chaotiques

1.1. Introduction

En mathématiques, en chimie et en physique théorique, un système dynamique est un ensemble très général de composants en interaction (un système), répartis sur plusieurs états et structurés selon certaines propriétés ; il est le plus souvent régi par un ensemble d'équations différentielles décrivant le mouvement des composants (leur dynamique) où interviennent une classe de paramètres accessibles. Par ailleurs, dans les mathématiques, les systèmes dynamiques chaotiques ont connu une importante généralisation ces dernières décennies touchant ainsi plusieurs applications. Dans cette perspective nous nous intéresserons principalement dans ce chapitre à l'étude des systèmes dynamiques chaotiques.

Après quelques rappels sur les généralités des systèmes dynamiques, les différents types de points fixes selon leur stabilité sont définis. Les méthodes de Lyapunov permettant de tester la stabilité des systèmes dynamiques non linéaires sont démontrées. La notion de chaos est ensuite introduite, ainsi que la description des différents types d'attracteurs et des bifurcations qui peuvent apparaître dans l'évolution de tout système dynamique. Nous terminons ce chapitre par le calcul des exposants de Lyapunov permettant de caractériser le comportement chaotique d'un système et par la présentation de quelques systèmes chaotiques.

1.2. Définition

Un système dynamique non linéaire présente deux aspects, son état et sa dynamique, c'est-à-dire son évolution en fonction du temps ; il est défini par un système d'équation différentielles du premier ordre de la forme :

Chapitre 1 Généralités sur les systèmes chaotiques

Temps continu :

$$\dot{x} = \frac{dx}{dt} = f(x, t, \mu) \quad (1.1)$$

Avec f un champ de vecteurs. $x \in R^n$ le vecteur d'état, $\mu \in R^p$ le vecteur des paramètres et t la variable temporelle.

Lorsque le champ de vecteurs f ne dépend pas explicitement du temps, on dit que le système dynamique est autonome. Dans le cas contraire il est non autonome.

Remarque : Par un changement de variable approprié, on peut toujours transformer un système dynamique non autonome en un système dynamique autonome.

Temps discret :

Un système dynamique dans le cas discret est représenté par une équation aux différences finies sous la forme :

$$x(k+1) = G(x(k), ku) \quad (1.2)$$

$G : R^n \times Z^+ \rightarrow R^n$ Indique la dynamique du système en temps discret.

K nombre d'échantillon, u vecteur de paramètre.

1.2.1. Espaces de phase

Il est possible de suivre l'évolution de l'état d'un système physique dans le temps. Pour cela, on construit d'abord un modèle avec les lois physiques et les paramètres nécessaires et suffisants pour caractériser le système. Ce modèle est bien souvent constitué par des équations différentielles. On définira, à un instant donné, un point dans un « repère ». Ce point caractérisera l'état du système dans l'espace à cet instant. Cet espace est appelé « l'espace des phases ou espaces d'états ». L'espace des phases est une notion purement mathématique qui comporte autant de dimensions qu'il y a de vecteur d'état dans le système dynamique.

Chapitre 1 Généralités sur les systèmes chaotiques

1.2.2. Point fixe ou point d'équilibre

On appelle point d'équilibre (point critique ou point stationnaire) de (1.1), le point \bar{x} de l'espace des phases obtenu en annulant le second membre de (1.1) :

$$f(\bar{x}) = 0 \quad (1.3)$$

Par un changement de variables $\varepsilon = x - \bar{x}$, on peut ramener le point \bar{x} à l'origine.

grâce aux points fixes, on peut caractériser les trajectoires voisines.

1.3. Stabilité du point fixe

On désigne par stable tout système qui reprend son état d'équilibre après une perturbation. La théorie des systèmes dynamiques non linéaire fait intervenir différentes notions de stabilité, il faut rappeler que la stabilité d'un point stationnaire garantit une stabilité locale, c'est une condition nécessaire mais pas suffisante pour avoir une stabilité globale.

Le système dynamique non linéaire est stable si tous ses états stationnaires sont stables. Pour déterminer la stabilité d'un système dynamique non linéaire, on peut utiliser différentes méthodes mathématiques, parmi lesquelles on peut citer : la méthode de Lyapunov et la méthode de l'espace de phase [2]. Elles permettent l'étude de la stabilité autour d'un point d'équilibre.

1.3.1. Stabilité au sens de Lyapunov [3]

Soit le système autonome suivant :

$$\dot{x} = f(x), \text{ ou } f : D \rightarrow \mathbb{R}^n \quad (1.4)$$

On suppose que \bar{x} est un point d'équilibre : $f(\bar{x}) = 0$

Chapitre 1 Généralités sur les systèmes chaotiques

- On dit que \bar{x} est stable si et seulement si :

$$\forall \varepsilon > 0, \exists \alpha > 0 \text{ tel que } : \|x_0 - \bar{x}\| < \alpha \Rightarrow \|x_{(t)} - \bar{x}\| < \varepsilon, \forall t \geq 0 \quad (1.5)$$

C'est-à-dire le point fixe est stable si toutes les solutions issues des points voisins du point d'équilibre restent proches de celui-ci.

- On dit que le point fixe est instable s'il n'est pas stable au sens de Lyapounov.
- On dit que le point fixe est asymptotiquement stable s'il est stable et on peut choisir $\delta > 0$ telque :

$$\|x_0 - \bar{x}\| < \delta \Rightarrow \lim_{t \rightarrow \infty} x_{(t)} = \bar{x} \quad (1.6)$$

La stabilité asymptotique permet de déterminer un voisinage de point fixe tel que toute trajectoire issue d'un point $x(0)$ appartenant à un voisinage de \bar{x} tende vers \bar{x} quand t tend vers l'infini.

L'inconvénient est que les définitions précédentes concernent que les orbites proches de point fixe alors qu'on veut étudier le comportement de tout le système. Pour cela, Lyapounov a donné une méthode permettant de résoudre ce problème.

1.3.2. Stabilité par méthode indirecte de Lyapounov [3]

Supposons que, par un changement de coordonnées, le point fixe est à l'origine: $f(0)=0$, le développement en série de Taylor en $x = 0$ s'écrit :

$$f(x) = Df(0)x - \frac{1}{2!}(D^2f(0)(x,x)) + \frac{1}{3!}(D^3f(0)(x,x,x)) \dots \quad (1.7)$$

Où $Df(0)$ est la matrice jacobienne de $f(x)$ au point d'équilibre $x = 0$.

Chapitre 1 Généralités sur les systèmes chaotiques

La méthode indirecte de Lyapunov, pour étudier la stabilité autour d'un point d'équilibre, consiste à étudier le système linéaire :

$$\dot{x} = A x \quad (1.8)$$

Avec :

$$A = Df(0) = \left(\begin{array}{ccc} \frac{df_1}{dx_1} & \dots & \frac{df_1}{dx_n} \\ \vdots & \ddots & \vdots \\ \frac{df_n}{dx_1} & \dots & \frac{df_n}{dx_n} \end{array} \right)_{x=0} \quad (1.9)$$

A est la matrice jacobienne de $f(x)$ et son déterminant est le Jacobien. Dans le cas où la matrice Jacobienne $Df(0)$ possède n valeurs propres λ_i , $i=1,2,\dots, n$ distinctes, la solution de (1.4) est :

$$x(t) = \sum_{i=1}^n c_i a^{(i)} e^{\lambda_i t} \quad (1.10)$$

Où $a^{(i)}$ est le vecteur propre correspondant à la valeur propre λ et les $c_i, i = 1 \dots n$, sont déterminées par les conditions initiales [4]. On en déduit que :

- Si toutes les valeurs propres λ ont leur partie réelle négative, le point fixe est asymptotiquement stable.
- Si une des valeurs propres a sa partie réelle positive, le point fixe est instable.
- Si une ou plusieurs valeurs propres sont des imaginaires pures, les autres valeurs propres ayant leur partie réelle négative, le point fixe est un centre ou un point elliptique (stable mais pas asymptotiquement stable).
- Si $Df(0)$ n'a pas de valeur propre nulle ou purement imaginaire, le point fixe est un point hyperbolique, dans le cas contraire, c'est un point non-hyperbolique.
- S'il existe i et j tel que $\text{Re}(\lambda_i) < 0$ et $\text{Re}(\lambda_j) > 0$, le point fixe est un point selle.

Chapitre 1 Généralités sur les systèmes chaotiques

- Si toutes les valeurs propres de $Df(0)$ sont réelles et de même signe, le point fixe est un nœud. Un nœud stable est un puit, un nœud instable est une source.

1.4. Chaos

Le chaos dans son ensemble désigne le désordre ou le manque de règle cependant, dans la théorie du chaos, le terme est défini plus rigoureusement. La théorie du chaos est un domaine en mathématiques, avec des applications dans plusieurs disciplines comme la physique, l'ingénierie, la biologie, l'économie, l'informatique, la météorologie, la sociologie et la philosophie. Cette théorie étudie le comportement des systèmes dynamiques qui sont très sensibles aux conditions initiales [5].

De petites différences dans les conditions initiales induisent des changements titanesques sur les résultats des systèmes dynamiques, à long terme grâce à cette sensibilité la prévision devient impossible en général. Cela se produit même si ces systèmes sont déterministes, ce qui signifie que leur comportement futur est entièrement déterminé par leurs conditions initiales, sans éléments aléatoires impliqués.

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 initiales.
- **l'imprévisibilité** : en raison de la sensibilité aux conditions initiales, qui peuvent être connues seulement à un degré fini de précision.

Chapitre 1 Généralités sur les systèmes chaotiques

- **l'irrégularité** : l'ordre caché comprenant un nombre infini de modèles périodiques instables (ou mouvements). Cet ordre caché forme l'infrastructure des systèmes chaotiques.

1.5. Caractéristiques d'un système dynamique chaotique

Pour dire qu'un système dynamique non linéaire est chaotique, il faut qu'il dépende de plusieurs paramètres et que son évolution dans le temps soit très sensible aux conditions initiales, il peut même sembler aléatoire alors qu'il est parfaitement déterministe.

D'un point de vue mathématique, on dit que f montre une dépendance sensible aux conditions initiales lorsque :

$$\exists \delta > 0, \forall \mathbf{x} \in D, \forall \varepsilon > 0, \exists (\mathbf{y}, \mathbf{p}) \in D : \begin{cases} \|\mathbf{x} - \mathbf{y}\| < \varepsilon \\ \|f^p(\mathbf{x}) - f^p(\mathbf{y})\| > \delta \end{cases} \quad (1.11)$$

Les systèmes dynamiques chaotiques sont caractérisés par les propriétés suivantes :

1.5.1 Bifurcation

Un système est dit structurellement stable sur une portion de l'espace des paramètres si une petite perturbation du système étudié ne modifie pas le comportement global de la dynamique sur cette portion. Tant que le système est structurellement stable, les variations de paramètres produisent des changements quantitatifs dans la solution : coordonnées d'un point fixe, amplitude ou fréquence d'une solution périodique par exemple. Cependant, il arrive aussi qu'une infime variation de paramètres produise un changement qualitatif de la solution et un changement de stabilité d'un ensemble limite.

A la valeur particulière du paramètre où la solution change subitement de nature, le

Chapitre 1 Généralités sur les systèmes chaotiques

système est structurellement instable ce qui autorise un brusque changement de type de la solution. Ce phénomène est appelé bifurcation et les points où il se produit sont les points de bifurcation [2][4].

Ce qui nous intéresse, ce sont des bifurcations locale c'est-à-dire ayant lieu au voisinage d'un point d'équilibre, il existe cinq type de bifurcation, bifurcation nœud-col, transcritique, fourche, hop et bifurcation doublement de période [3].

1.5.2 Diagramme de bifurcations

Le diagramme de bifurcation est un tracé très efficace nous informant de la nature des différentes solutions du système en faisons varier l'un des paramètres.

Le tracé est composé d'intervalles sur lesquelles les solutions asymptotiques (ou les ensembles limites qui leur correspondent) évoluent continûment avec le paramètre et les intervalles sont séparés par les points de bifurcation.

Le diagramme de bifurcation est un outil efficace pour évaluer rapidement l'ensemble des solutions possibles d'un système en fonction des variations de l'un de ses paramètres. Il permet de repérer les valeurs particulières du paramètre qui induisent des bifurcations. C'est un diagramme qui porte les valeurs du paramètre en abscisse et des valeurs particulières d'une des variables d'état en ordonnée lorsque le régime asymptotique est atteint.

Soit le système de Rössler suivant :

$$\begin{cases} \dot{x} = -(y + z) \\ \dot{y} = x + ay \\ \dot{z} = b + z(x - c) \end{cases} \quad (1.12)$$

Chapitre 1 Généralités sur les systèmes chaotiques

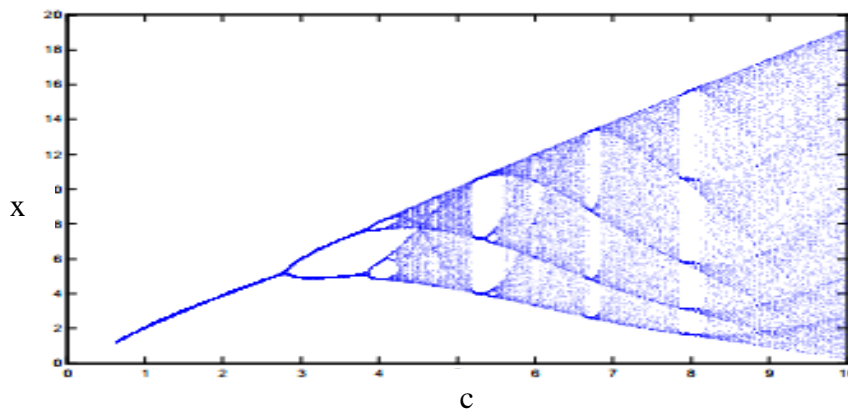


Figure 1.1 Diagramme de bifurcation du système de Rössler pour $a=0.2$ et $b=0.2$

On a alors une évolution vers le chaos c'est-à-dire lorsqu'on varie l'un des paramètres du système, on voit l'apparition du phénomène de doublement de période figure 1.1.

1.5.3. Attracteur étrange (chaotique)

Un attracteur est un objet géométrique vers lequel tendent toutes les trajectoires de l'espace des phases, c'est-à-dire, une situation ou un ensemble de situation vers lesquelles évolue un système, quelles que soient ses conditions initiales.

Dans un espace des phases à deux dimensions, les attracteurs sont soit des points, soit des cycles limites.

Pour tous les attracteurs réguliers, c'est-à-dire pour tous systèmes non chaotiques, des trajectoires qui partent de points proches l'un de l'autre dans l'espace de phase restent indéfiniment voisines. On sait donc prévoir l'évolution de ces systèmes à partir d'une situation connue [4].

L'attracteur étrange dit aussi chaotique ne présente pas de surface lisse, mais une surface repliée plusieurs fois sur elle-même. En effet, les trajectoires des points divergent c'est-à-dire que deux points très proches ne peuvent avoir la même évolution, mais comme l'attracteur a des

Chapitre 1 Généralités sur les systèmes chaotiques

dimensions finies, il doit se replier sur lui-même.

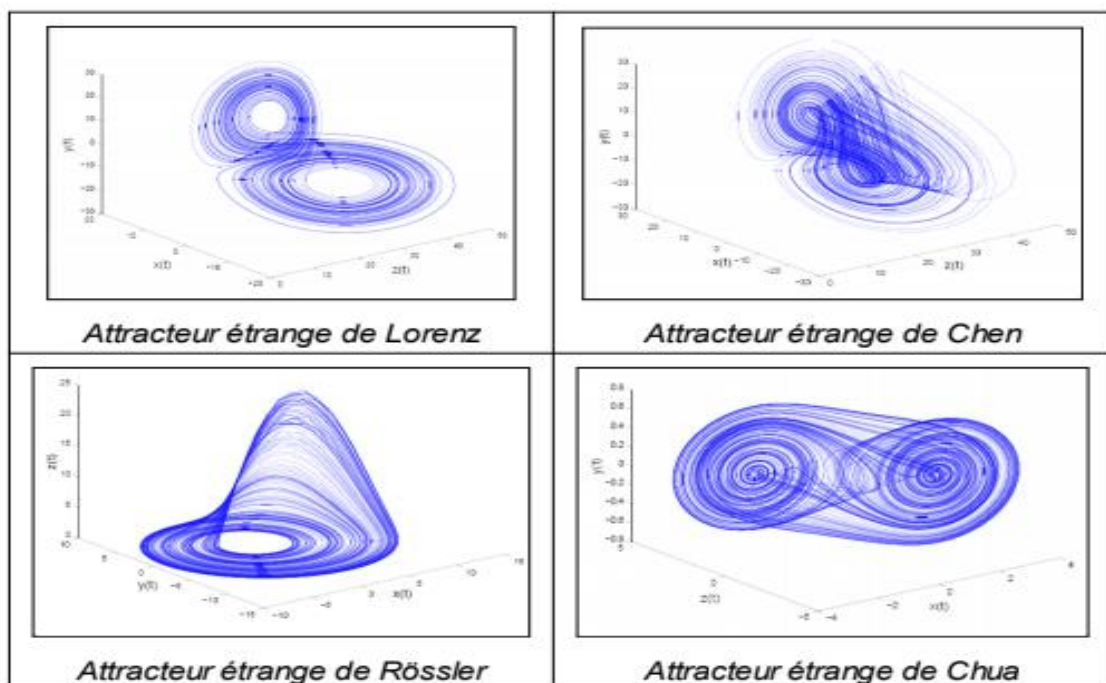


Figure 1.2. Quelques attracteur étranges.

La figure (1.2) montre les objets géométriques de quelques systèmes chaotique : on observe relativement la complexité et la richesse d'information que dégage de ces attracteurs. Un attracteur chaotique possède notamment la propriété remarquable suivante : la trajectoire ne repasse jamais par un même état. Ce qui signifie, entre autres que cette trajectoire passe par une infinité d'états.

Les systèmes non chaotiques sont caractérisés par un autre type d'attracteur qu'on appelle attracteur régulier et peuvent être de trois sortes :

- **Le point fixe** : est le cas le plus simple, dans lequel le système évolue vers un état de repos, ce point s'appelle le puit (Figure (1.3.a)).

Chapitre 1 Généralités sur les systèmes chaotiques

- **Le cycle limite périodique** : quand la trajectoire se referme sur elle-même, le système présentant des oscillations permanentes, alors l'évolution est cyclique (Figure (1.3.b)).
- **Le cycle limite pseudopériodique** : est un cas particulier du type précédent, le système possède deux périodes alors la trajectoire ne se referme pas sur elle-même mais s'enroule sur une variété de dimension 2, elle forme un tore (Figure (1.3.c)).

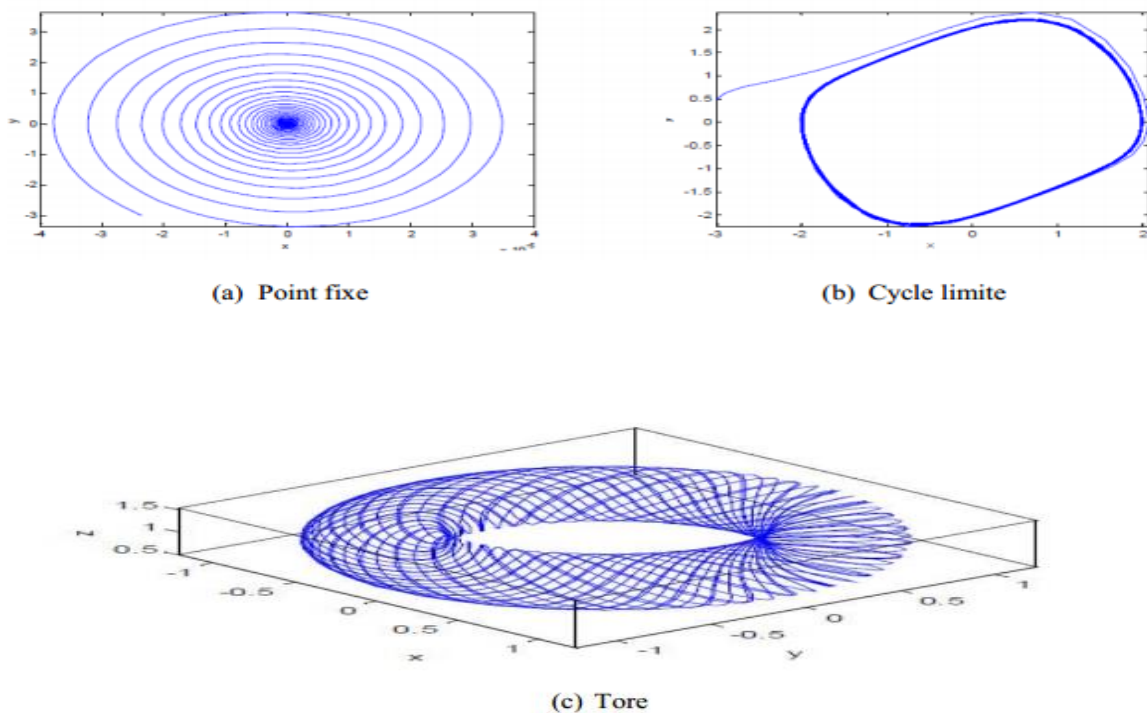


Figure 1.3. Différents types d'attracteurs réguliers [3].

1.5.4. Section de Poincaré

La section de Poincaré est un outil très utilisé pour étudier la stabilité d'un cycle limite

Chapitre 1 Généralités sur les systèmes chaotiques

et aussi les systèmes dynamiques, plus précisément la stabilité des orbites périodique. On lui vaut son nom à Henri Poincaré.

Faire une section de Poincaré veut dire couper la trajectoire chaotique dans un espace d'au moins trois dimensions par un hyperplan d'une dimension inférieure, afin d'étudier les intersections, chaque intersection correspond à une orbite et une seule. Ainsi, on convertit le système continu en un système discret dont le nombre d'interactions remplace le temps, sachant qu'en mathématique, ses propriétés restent toujours conservées, la section de Poincaré est plus détaillée dans [4][6][7].

Considérons le système dynamique autonome suivant :

$$\frac{dx}{dt} = f(x), x \in R^n \quad (1.13)$$

On appelle section de Poincaré, une hyper surface Σ_p de dimension $n - 1$, tel que l'ensemble des points p_0, p_1, p_2, \dots correspond aux intersections successives de la trajectoire (x_0) avec l'hyper surface Σ_p comme illustre la figure suivante :

Chapitre 1 Généralités sur les systèmes chaotiques

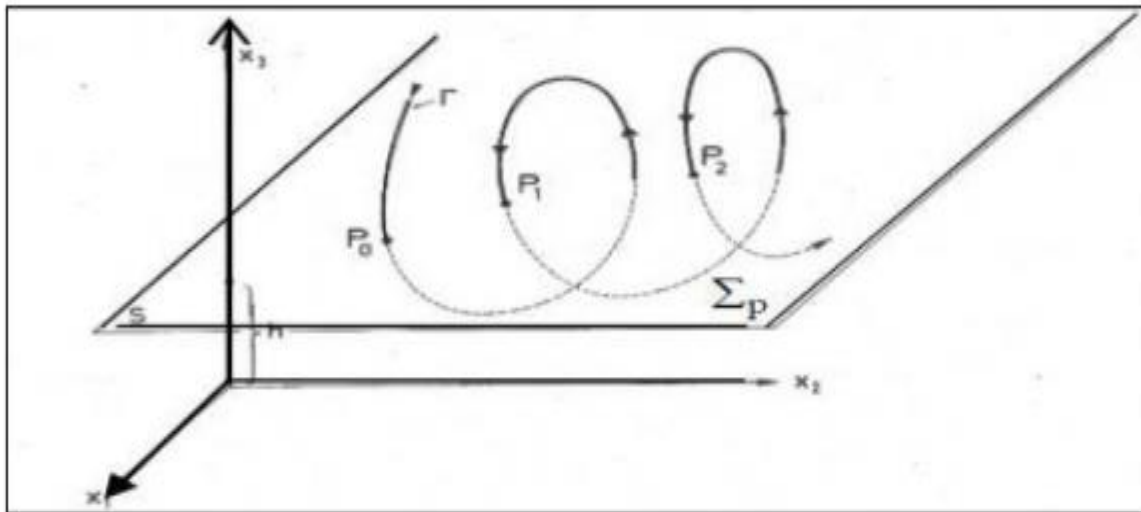


Figure 1.4. Projection par l'application de Poincaré du premier retour [2].

Le système initial de dimension n est transformé en un système de dimension $n-1$ qui est représenté par :

$$p_{k+1} = (Tp_k), \quad k = 0, 1, 2, \dots \dots \dots \quad (1.14)$$

Où : T est l'application du premier retour qui à un point p_i de Σp fait correspondre le prochain point p_{i+1} d'intersection de la trajectoire $\varphi(x_0)$ avec l'hyper surface Σp .

$K = 1, 2, \dots \dots$ caractérise le système dynamique dont les propriétés sont données dans le tableau suivant :

Chapitre 1 Généralités sur les systèmes chaotiques

Attracteur dans l'espace des phases	Application de Poincaré
Cycle limite	1 point
Cycle limite avec p maxima par période	p points
Attracteur quasi-périodique	Courbe fermée
Attracteur étrange	Courbe(s) ouverte(s)

Tableau 1.1. Application de Poincaré.

1.5.5. Les exposants de Lyapounov

Les exposants de Lyapounov, présentés par Oseledec pour la première fois en 1968 [4][6], jouent un rôle important dans l'étude des systèmes non linéaires, notamment les systèmes chaotiques. Ils qualifient le degré de divergence des trajectoires d'un système dynamique non linéaire soumis à des conditions initiales différentes. Cette divergence est exprimée par les exposants de Lyapounov. Les exposants de Lyapounov caractérisent ainsi le comportement du système non linéaire et notamment son caractère chaotique ou hyper-chaotique [8][9]. Par exemple, la positivité du plus grand exposant de Lyapounov d'un système dynamique non linéaire affirme, l'existence d'un régime chaotique.

Grace à l'étude des exposant de Lyapounov on peut détermine qu'un système non linéaire est chaotique ou non en définissant le type d'attracteur (sous l'hypothèse que les trajectoires évoluent dans une région borné) [6] :

- $\lambda_n \leq \dots \leq \lambda_1 < 0$: des exposants de Lyapounov négatifs montrent l'existence d'un point fixe.
- $\lambda_1 = 0, \lambda_n \leq \dots \leq \lambda_2 < 0$: l'attracteur est une orbite fermé,

Chapitre 1 Généralités sur les systèmes chaotiques

- $\lambda_1 = \lambda_2 = 0, \lambda_n \leq \dots \leq \lambda_3 < 0$: l'attracteur est quasi-périodique (fréquences),
- $\lambda_1 = \dots = \lambda_k = 0, \lambda_n \leq \dots \leq \lambda_{k+1} < 0$ l'attracteur est quasi-périodique - (fréquences),
- $\lambda_1 > 0, \sum \lambda_i < 0$: l'attracteur est chaotique,
- $\lambda_1 > \dots > \lambda_k > 0, \sum \lambda_i < 0$: l'attracteur est hyper-chaotique.

1.6. Exemples de systèmes chaotiques

1.6.1. Système à temps continu

Le système de Lorentz est un exemple célèbre de système différentiel au comportement chaotique pour certaines valeurs de paramètres. Ce système est défini par les équations suivantes :

$$\begin{cases} x' = c(y - x) \\ y' = x(a - z) - y \\ z' = xy - bz \end{cases} \quad (1.15)$$

Avec $c = 10$; $a = 8/3$; $b = 28$ on a un système dynamique chaotique, pour la simulation nous avons choisi les conditions initiales suivantes : $x_0 = 8, y_0 = 3, z_0 = 33$, on a obtenu trois points fixes .

La figure (1.5) représente l'attracteur étrange du système de Lorentz :

Chapitre 1 Généralités sur les systèmes chaotiques

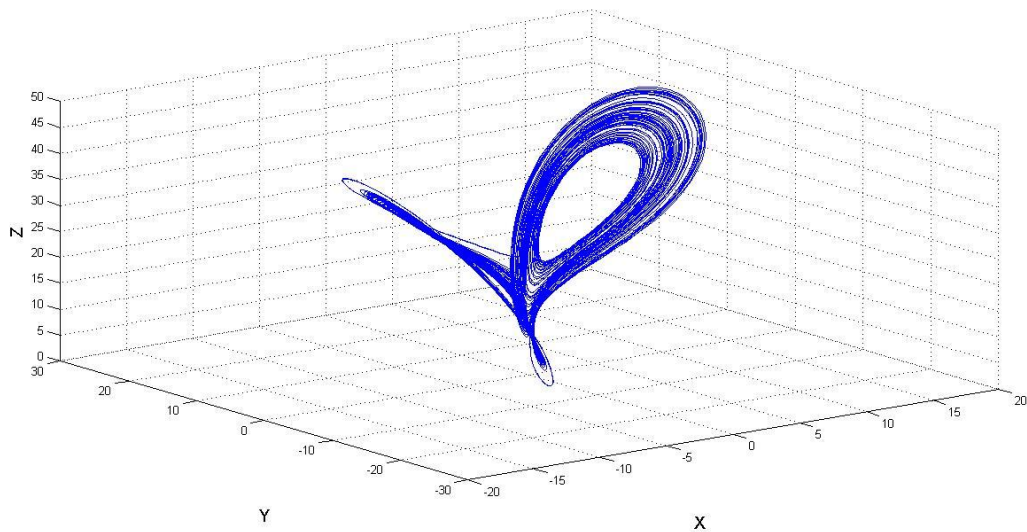


Figure 1.5. Attracteur de Lorenz.

Ainsi que les coordonnées x , y et z en fonction du temps sont données par la simulation du système de Lorenz sous Matlab et représentées sur la figure (1.6):

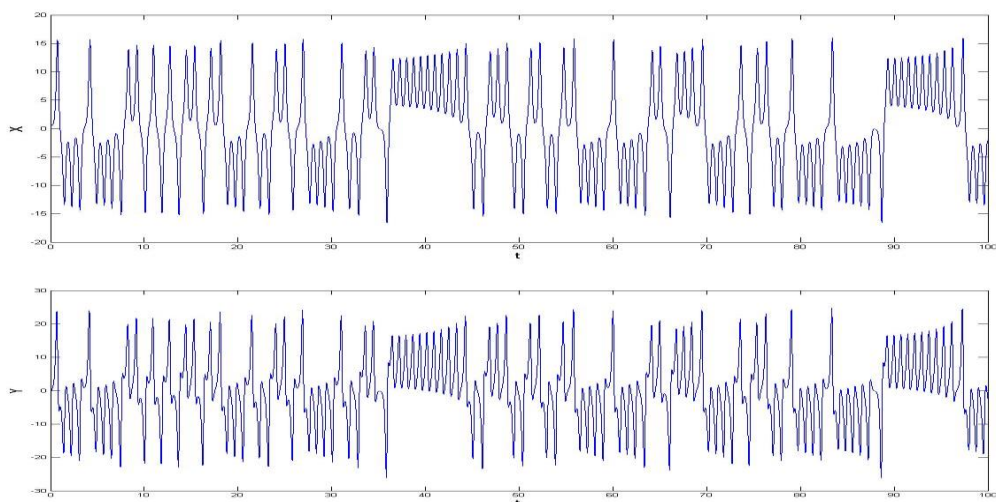


Figure 1.6. Solutions de système de Lorenz.

Chapitre 1 Généralités sur les systèmes chaotiques

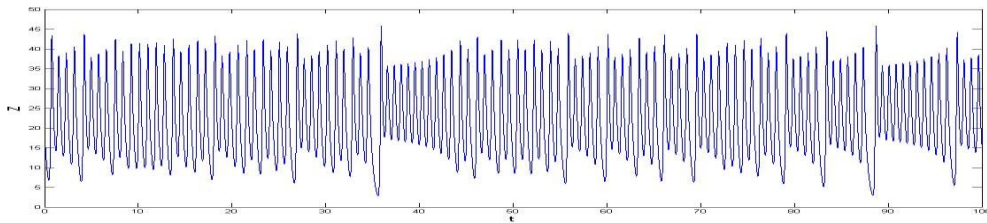


Figure 1.6. (suite) Solutions de système de Lorenz.

Les solutions du système en un aspect aléatoire (bruité) alors qu'ils sont parfaitement déterministes.

Les exposants de Lyapounov sont représentés sur la figure ci-dessous ; il existe un exposant positif et la somme des exposants est négative. Cela signifie que le système chaotique.

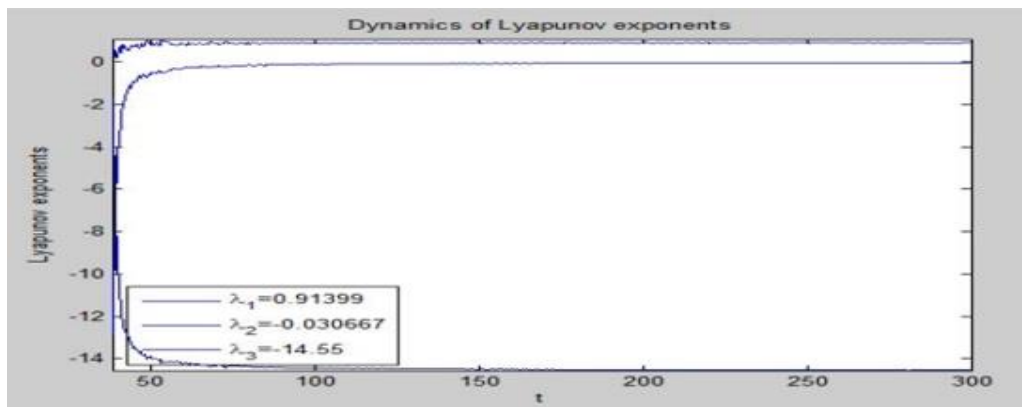


Figure 1.7. Exposants de Lyapounov de système de Lorentz.

Chapitre 1 Généralités sur les systèmes chaotiques

La figure montre le diagramme de bifurcation de système de Lorenz en faisant varier le paramètre **a** :

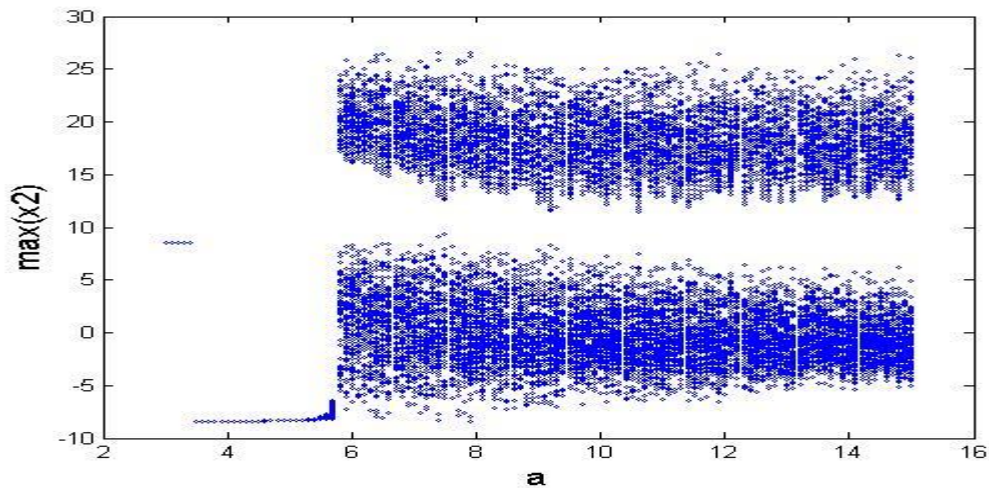


Figure 1.8. Diagramme de bifurcation du système de Lorenz.

Pour $a < 5.7$, le système possède un nombre petit de maximums, cela signifie qu'il a un comportement périodique (non chaotique). Dès que (a) dépasse la valeur 5.8, plusieurs maximums apparaissent (phénomène de doublement de période), ce phénomène nous permet de déduire que le système est chaotique.

Pour la section de Poincaré il suffit de couper le plan de phase pour l'équation $x = 0$, on a obtenu la section de Poincaré représentée par la figure suivante :

Chapitre 1 Généralités sur les systèmes chaotiques

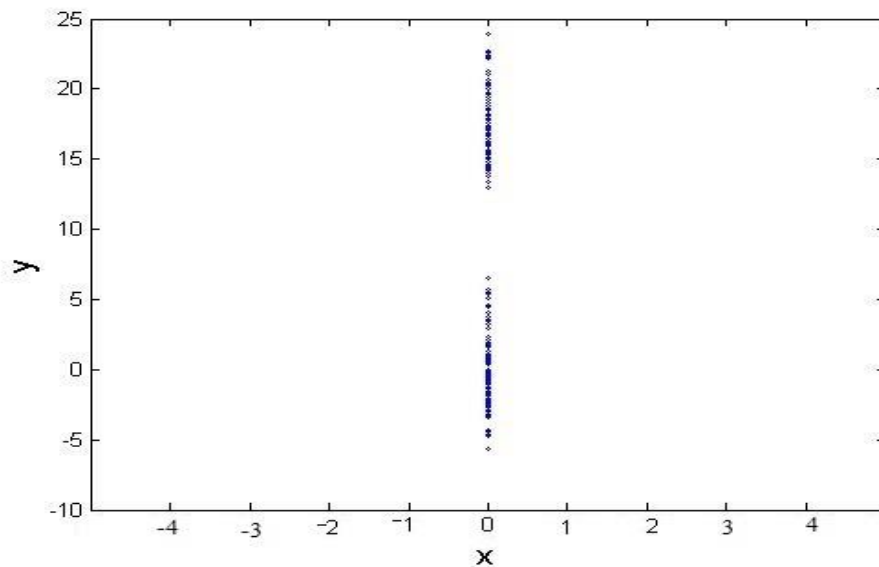


Figure 1.9 Section de Poincaré de système de Lorenz

On remarque qu'il existe une infinité des points d'intersection (courbe ouverte) ce qui caractérise le système chaotique.

1.6.2. Système à temps discret

La fonction logistique très connue dans la théorie des systèmes non linéaires, « qui sera utilisée dans le chapitre 3, comme un générateur de signaux chaotique pour le cryptage », est une application non bijective du domaine $[0, 1]$ dans lui-même qui sert de récurrence à la suite :

$$x_{k+1} = f(x_k) = rx_k(1 - x_k) \quad (1.16)$$

Où $k=0,1,\dots$ dénote le temps discret, x la variable dynamique et r un paramètre réel.

La dynamique de cette application correspond à un comportement différent ; ainsi selon la valeur du paramètre r , une plus grande variété de régimes permanents est représenté parmi lesquelles on trouve, par ordre de complexité :

Chapitre 1 Généralités sur les systèmes chaotiques

- pour $0 < r < 3$, le système possède un point fixe attractif, qui devient instable lorsque $r = 3$.
- pour $3 < r < 3.57\dots$, le système évolue périodiquement de période r^n , avec n un entier qui tend vers l'infini lorsque r tend vers $3.57\dots$
- pour $r = 4$, le système évolue de manière chaotique.

La figure suivante illustre l'aspect aléatoire du système (1.16) pour $r=4$. Il est alors impossible de discerner à l'œil nu cette trajectoire de celle d'une variable aléatoire :

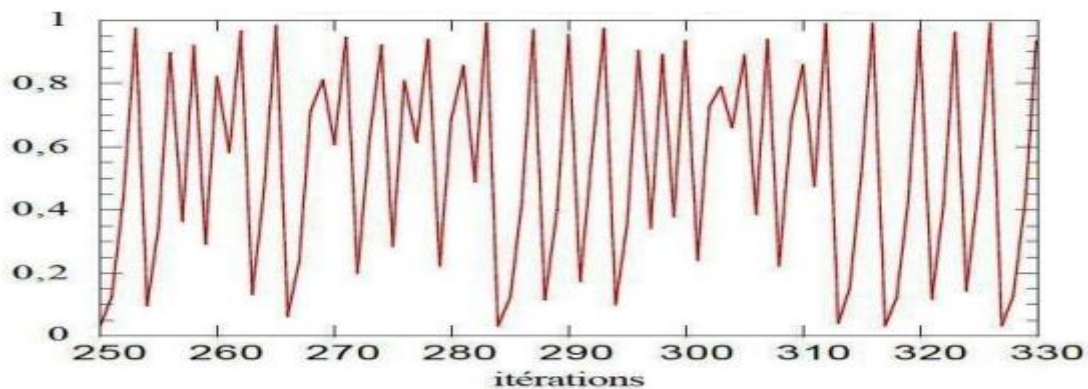


Figure 1.10. Solution du système (1.16) pour $r=4$ [7]

La figure ci-dessous montre le diagramme de bifurcation de la fonction logistique en faisant varier le paramètre r :

Chapitre 1 Généralités sur les systèmes chaotiques

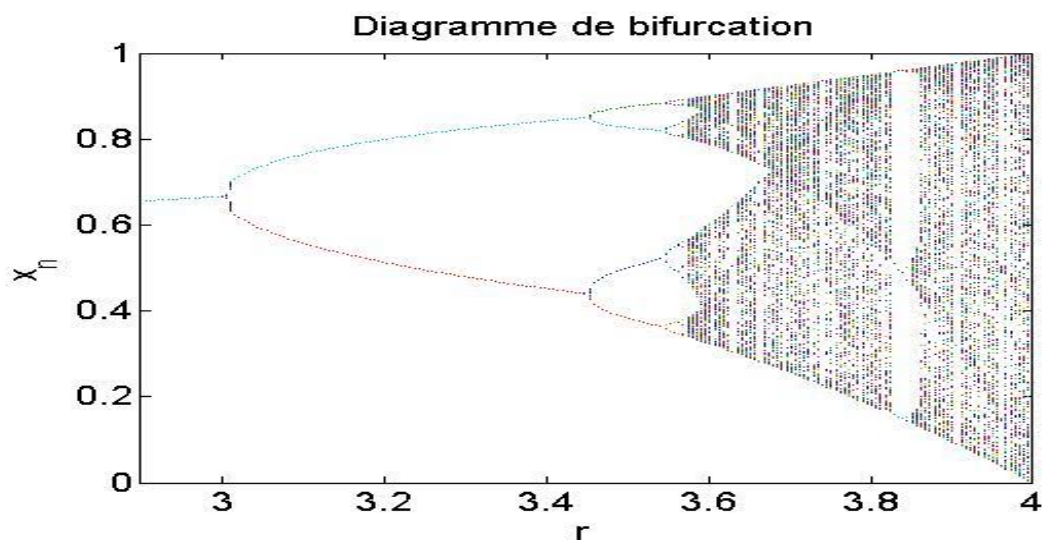


Figure 1.11. Diagramme de bifurcation de la fonction logistique

Pour $r < 3$, le système possède un seul maximum, cela signifie qu'il a un comportement périodique (non chaotique). Dès que r dépasse la valeur 3, plusieurs maximums apparaissent (phénomène de doublement de période), 2 maximums ensuite 4 jusqu'à ce que le phénomène se répète infiniment donnant lieu à une multitude de maximums entre 3.7 et 4 : le système est alors caractérisé de système chaotique.

1.7. Conclusion

Dans le présent chapitre, quelques définitions et notions sur les systèmes dynamiques ont été présentées : point fixe, étude de la stabilité, bifurcation, etc. ainsi que les principales caractéristiques d'un système chaotique ont été décrites en mettant en évidence l'intérêt du calcul des exposants de Lyapounov, de même que différents scénarios possibles de transition vers le chaos.

Ces éléments seront exploités dans les chapitres suivants, lors de l'étude des différents comportements de système de Chen, qui sera utilisé en tant que générateur de signaux chaotique destinée à crypter une image médicale.

Chapitre 2 Etude du système hyper-chaotique de

Chen

2.1. Introduction

Le Système de Chen est un système dynamique non linéaire, il peut être chaotique dans un intervalle bien définie, ce système sera utilisé par la suite dans la partie de cryptage pour cela nous allons étudier ces propriétés.

2.2. Etude du système hyper-chaotique de Chen

Considérons le système hyper-chaotique de Chen :

$$\left\{ \begin{array}{l} \dot{x} = a(y - x) \\ \dot{y} = dx - xz + cy - w \\ \dot{z} = xy - bz \\ \dot{w} = x + k \end{array} \right. \quad (2.1)$$

Ou a, b, c, d et k sont des constantes avec : $a= 36, b= 3, c= 28, d= -16$ et $-0.7 \leq k \leq 0.7$, pour la simulation sous Matlab nous avons choisi les conditions initiales suivantes : $x_0 = 0.01, y_0 = 0.01, z_0=0.01, w_0=0.01$.

A l'œil nu les signaux apparaissent comme un signal bruité alors qu'en réalité, ceux sont des signaux parfaitement déterministes. Nous allons par la suite, déterminer les principales propriétés du système de Chen et montrer son caractère hyper-chaotique.

Les présentations temporelles des signaux $x(t), y(t), z(t)$ et $w(t)$ est donnée par la figure (2.1) :

Chapitre 2 Etude du système hyper-chaotique de

Chen

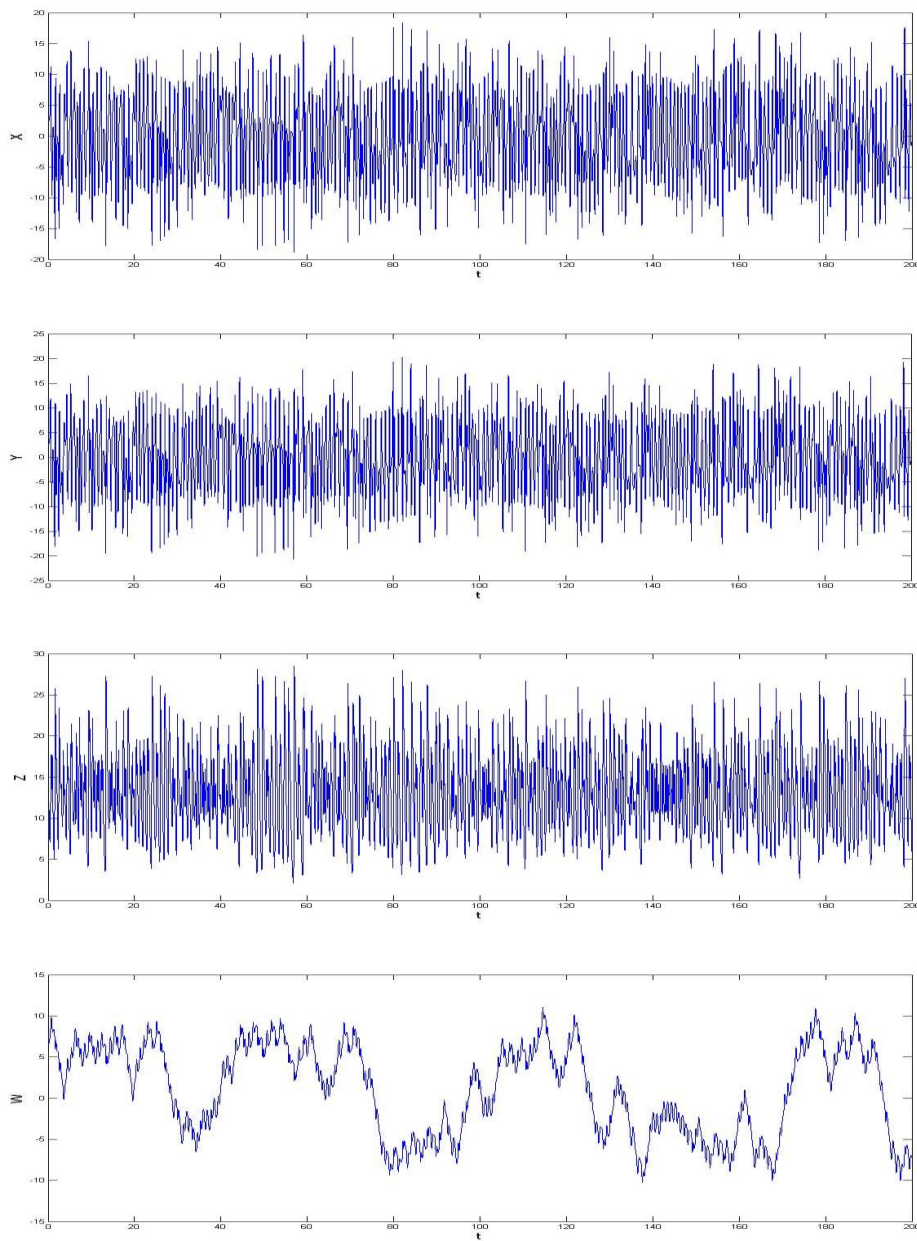


Figure.2.1. Représentation temporelle des signaux $x(t)$, $y(t)$, $z(t)$ et $w(t)$.

Chapitre 2 Etude du système hyper-chaotique de

Chen

2.3. Points d'équilibre

Le système (2.1) admet un seul point d'équilibre E_1 ; il a été obtenu en résolvant le système d'équations suivant:

$$\begin{cases} a(y - x) = 0 \\ dx - xz + cy = 0 \\ xy - bz = 0 \\ x + k = 0 \end{cases} \quad (2.2)$$

$$E_1 = \begin{bmatrix} -0.2 \\ -0.2 \\ 0.0133 \\ -2.402 \end{bmatrix} \quad (2.3)$$

2.3.1. Stabilité des points d'équilibre

L'étude de la stabilité du point fixe déclaré précédemment consiste à analyser les valeurs propres de la matrice Jacobienne du système (2.1) au point d'équilibre E_1 :

$$J = \begin{bmatrix} -36 & 36 & 0 & 0 \\ -16 - z & 28 & -x & 0 \\ y & x & -z & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad (2.4)$$

La matrice Jacobienne au point E_1 :

$$J_1 = J(E_1) = \begin{bmatrix} -36 & 36 & 0 & 0 \\ -16 - 0.0133 & 28 & 0.2 & 0 \\ -0.2 & -0.2 & -0.0133 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad (2.5)$$

Chapitre 2 Etude du système hyper-chaotique de

Chen

Les valeurs propres sont données par les solutions de l'équation :

$$J_1 - \lambda I = 0 \quad (2.6)$$

Où λI est donnée par :

$$\lambda I = \begin{bmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{bmatrix} \quad (2.7)$$

Avec : λ valeur propre de la matrice et I la matrice identité.

L'équation caractéristique est donnée par : $\det(J(E_1) - \lambda I) = 0$,

En utilisant Matlab, nous avons trouvé : $\lambda_1 = 0$, $\lambda_2 = -25.1565$, $\lambda_3 = 17.1498$,
 $\lambda_4 = -0.0066$.

Le point fixe E_1 est un point **selle instable**.

2.4. Plan de phase

L'étude des plans de phase nous permet la compréhension de l'évolution de système chaotique complexe, en visualisant le chemin parcouru par le système par la variation uniquement d'un des paramètres définis précédemment.

A l'aide de Matlab, nous avons pu tracer le plan des phases en faisant varier le paramètre k de -4 à 4, de la manière suivante :

1. Lorsque $k=0.2$, les attracteurs hyper chaotiques sont représentés sur la Figure 2.2(a) et 2.2(b) respectivement.
2. Lorsque $k=1.2$, les attracteurs sont représentés sur la Figure 2.3(a) et 2.3(b) respectivement.

Chapitre 2 Etude du système hyper-chaotique de

Chen

3. Lorsque $k=3.6$, l'attracteur évolue vers un cycle limite à quatre périodes, représentés sur la Figure 2.4(a) et 2.4(b) respectivement.
4. Lorsque $k=3.7$, l'attracteur évolue vers un cycle limite à deux périodes, représentés sur la Figure 2.5(a) et 2.5(b) respectivement.
5. Lorsque $k=4$, l'attracteur évolue vers un cycle limite à une seule période, représentés sur la Figure 2.6(a) et 2.6(b) respectivement.

D'après la relation (2.1), nous notons que ce système est invariant lors de la transformation $(x, y, z, w, k) \rightarrow (-x, -y, z, -w, -k)$. Donc, si (x, y, z, w) est une solution de (2.1) à condition que k soit défini, alors $(-x, -y, z, -w)$ est aussi une solution lorsque k est mis à sa valeur négative.

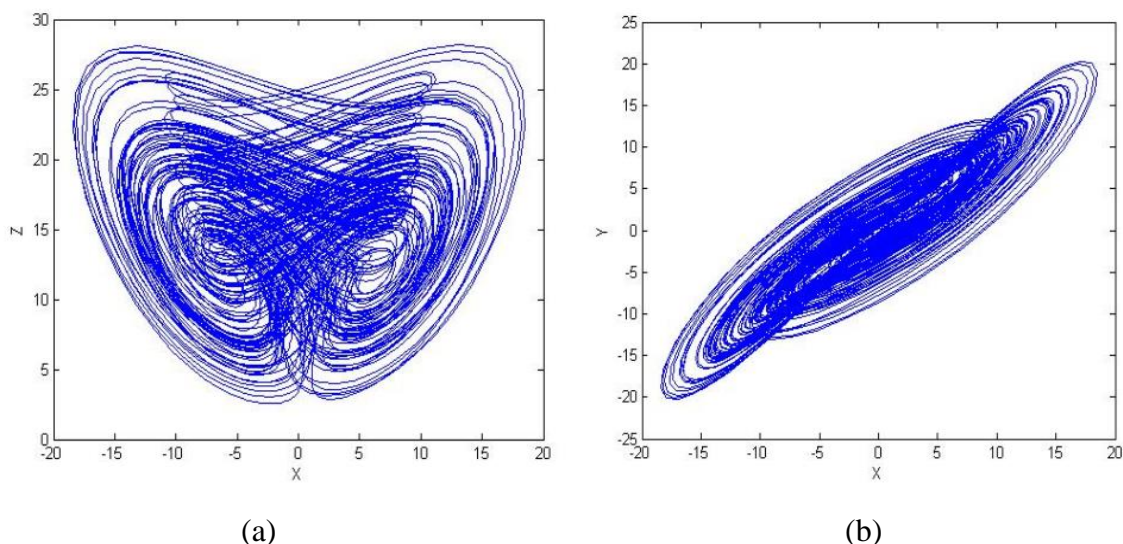


Figure 2.2. Plan de phase du système de Chen avec $k=0.2$.

Chapitre 2 Etude du système hyper-chaotique de

Chen

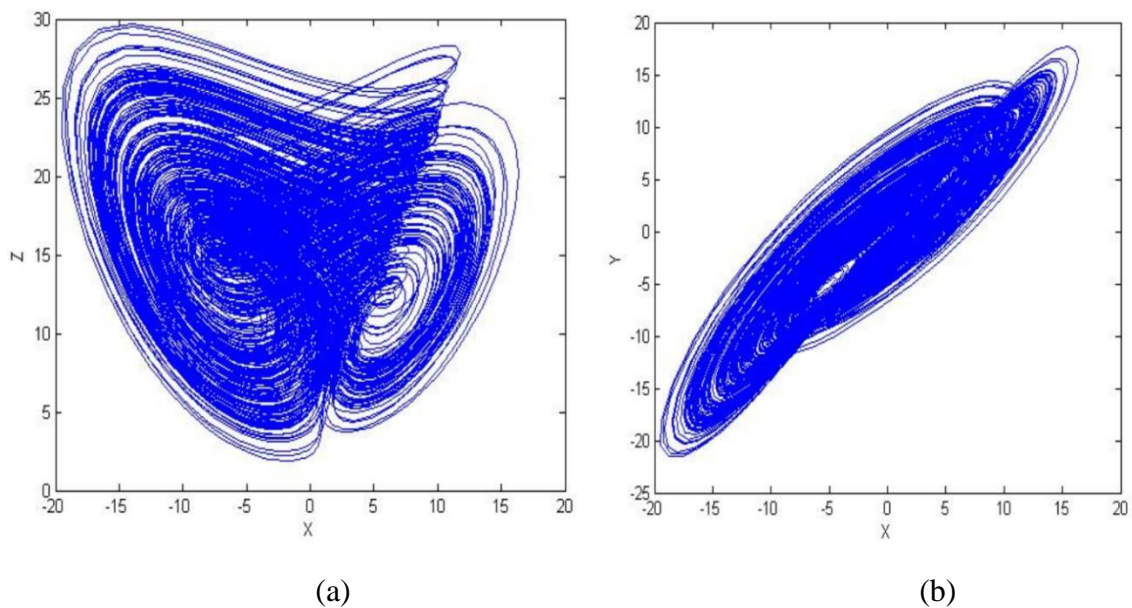


Figure 2.3. Plan de phase du système de Chen avec $k=1.2$.

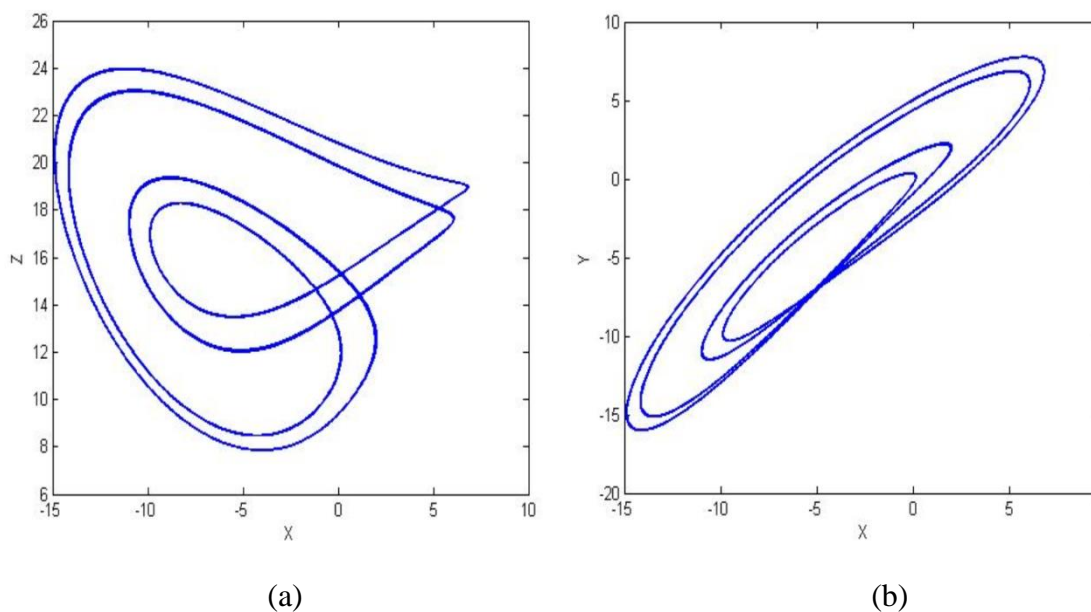
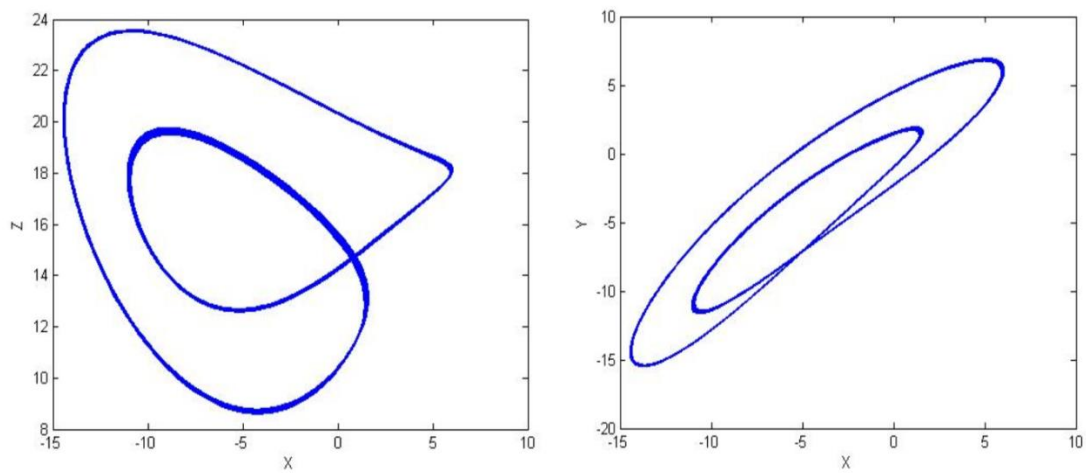


Figure 2.4. Plan de phase du système de Chen avec $k=3.6$.

Chapitre 2 Etude du système hyper-chaotique de

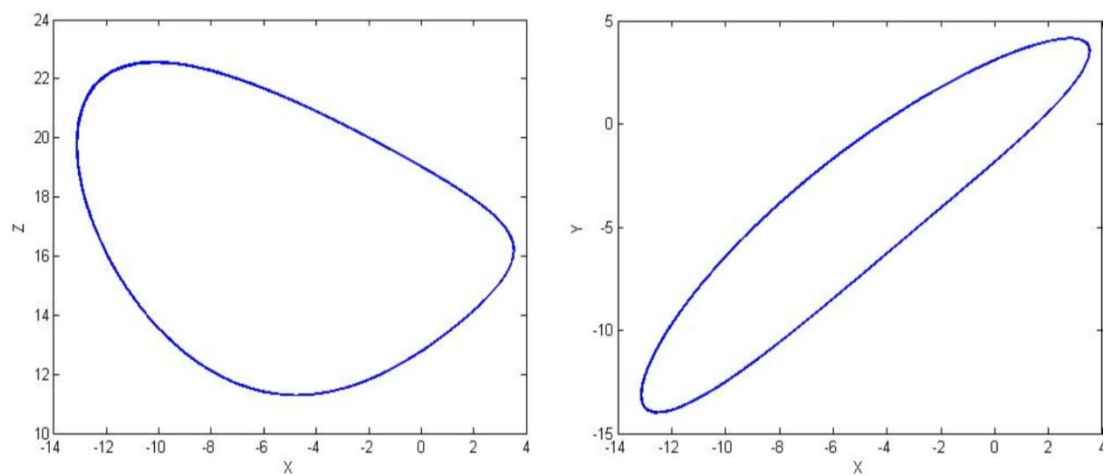
Chen



(a)

(b)

Figure 2.5. Plan de phase du système de Chen avec $k=3.7$.



(a)

(b)

Figure 2.6. Plan de phase du système de Chen avec $k=4$.

Chapitre 2 Etude du système hyper-chaotique de

Chen

2.5. Exposants de LYAPUNOV

Les exposants de Lyapunov vont définir le comportement du système (2.1) Le tableau ci-dessous représente les différentes valeurs de ces exposants après plusieurs simulation en faisant varié le paramètre k :

K	λ_1	λ_2	λ_3	λ_4
0	1.711	0.0264	- 0.044	- 12.691
2	1.356	0	-0.053	-12.291
3	0	0	-0.291	-11.565
4	0	-0.043	-0.817	-10.18

Tableau 2.1. Exposants de Lyapunov pour $k=0$ jusqu'a 4.

- Pour $k=4$, il existe un point fixe.
- Pour $k=3$, l'attracteur est quasi périodique.
- Pour $k=2$, l'attracteur est chaotique.
- Pour $k=0$, l'attracteur est hyper-chaotique.

Après plusieurs simulation sur une plage allons de -0.7 a 0.7, la valeur $k=0.2$ donne au système (2.1) un aspect hyper-chaotique, les exposants de Lyapunov sont représentés sur la figure ci-dessous ; il existe deux exposants positifs et la somme des exposants est négative. Cela signifie que le système est parfaitement hyper-chaotique.

Chapitre 2 Etude du système hyper-chaotique de

Chen

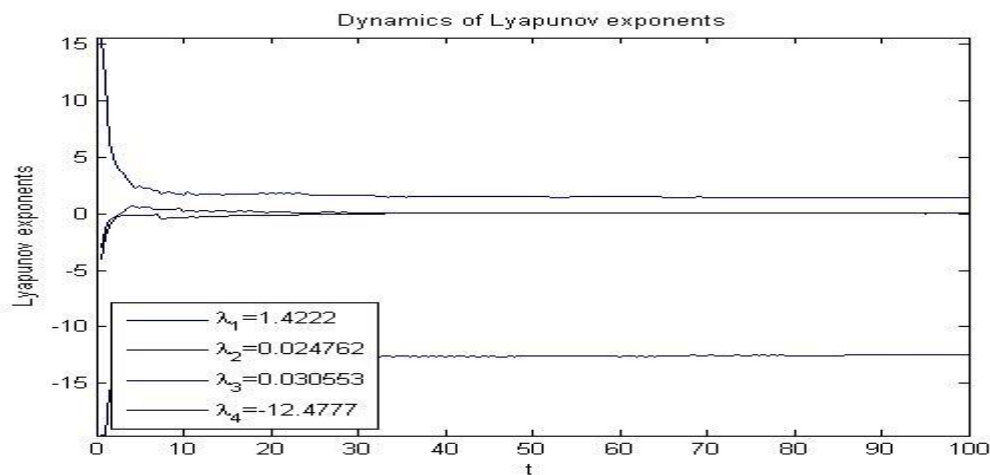


Figure 2.7. Exposants de Lyapounov de système de Chen avec $k=0.2$.

2.6. Bifurcation

Dans le système de Chen, afin de déterminer avec précision les différents comportements possibles de ce système en fonction du paramètre k on construit un diagramme de bifurcation. Après certain nombre d'itération pour certaines valeurs de k c'est-à-dire que l'opération est renouvelée pour plusieurs valeur de k allant de -4 à 4 . On obtient le diagramme de bifurcation, appelé aussi diagramme de Feigenbaum (figure 2.8).

Chapitre 2 Etude du système hyper-chaotique de

Chen

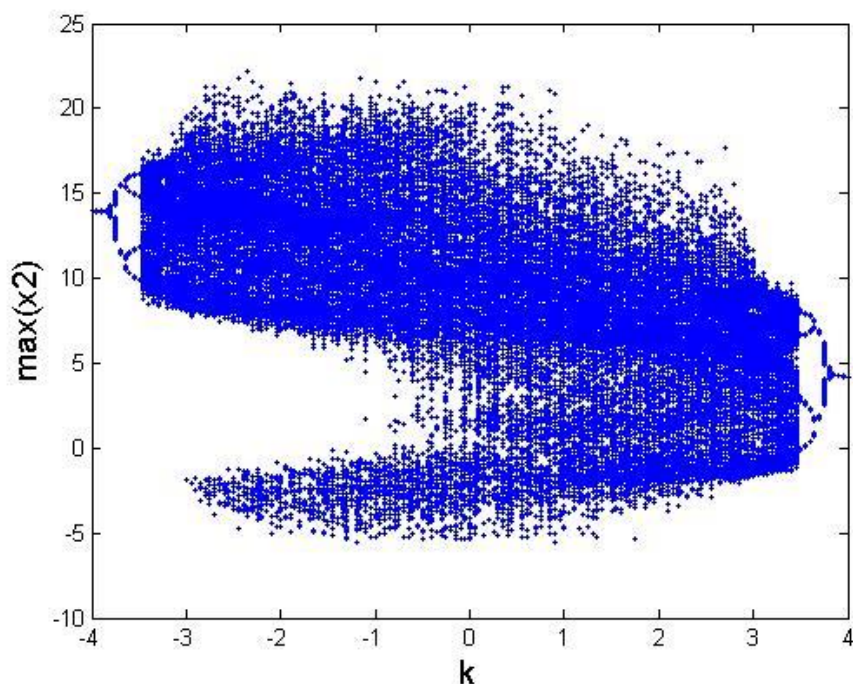


Figure 2.8. Diagramme de bifurcation du système de Chen.

Quand $3.5 \leq k \leq 4$ ou $-4 \leq k \leq -3.5$ le système est soumis à trois types d'orbites périodiques, allant d'un cycle limite d'une seule période suivi par un cycle limite de deux périodes en suite quatre périodes, grâce au phénomène de dédoublements de période.

Quand $0.7 \leq k \leq 3.5$ ou $-3.5 \leq k \leq -0.7$ le système présente un aspect typique d'un phénomène chaotique avec un nombre plus au moins infini de maximums.

Si $-0.7 \leq k \leq 0.7$ le système possède un nombre infiniment grand de maximums cela signifie qu'il y a un comportement hyper-chaotique.

Chapitre 2 Etude du système hyper-chaotique de Chen

2.7. Attracteur

La représentation dans l'espace des phases à trois dimensions pour le système (2.1) donne lieu à la figure.2.9, qui montre l'apparition d'un attracteur chaotique (ou attracteur étrange).

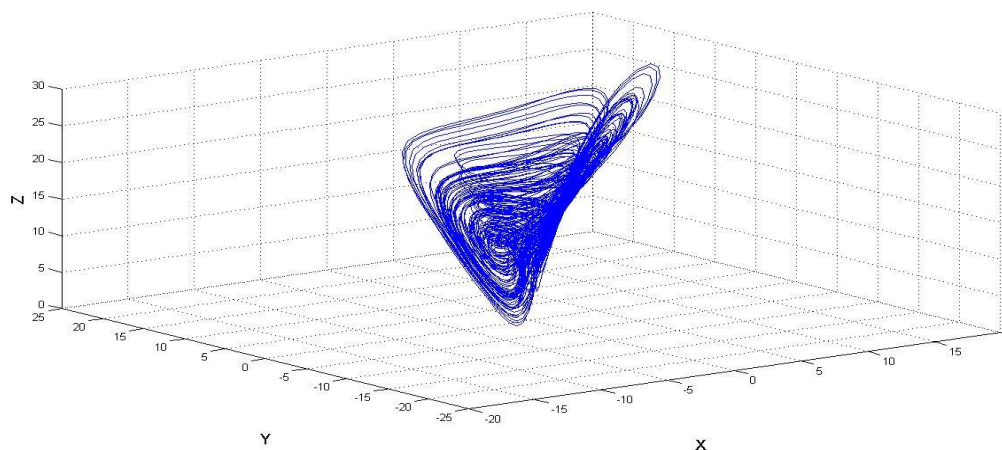


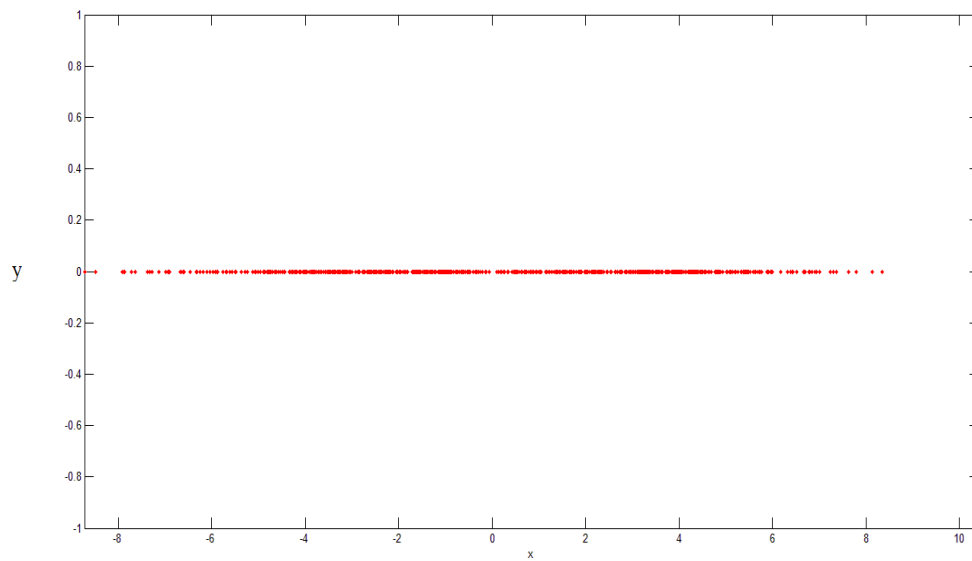
Figure.2.9. Attracteur hyper-chaotique de Chen.

2.8. Section de Poincaré

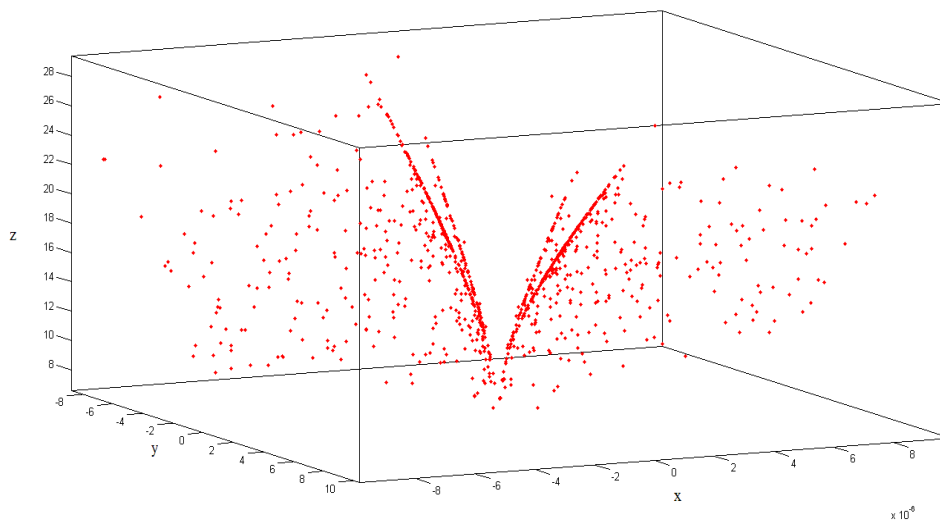
La section de Poincaré revient à couper la trajectoire dans l'espace de phase $y(x)$ Figure 2.2(b). On a obtenu aussi une infinité de points d'intersection, cela montre clairement que le système de Chen est chaotique.

Chapitre 2 Etude du système hyper-chaotique de

Chen



(a)



(b)

Figure.2.10. Représentation de la section de Poincaré du système de Chen , (a) :le plan de phase , (b) : l'attracteur étrange du système de Chen.

Chapitre 2 Etude du système hyper-chaotique de

Chen

2.9. Conclusion

Dans le présent chapitre, les principales propriétés du système de Chen ont été démontrées et les résultats de la simulation ont été donnés. Cela nous a permis de mettre en évidence son caractère hyper-chaotique, offrant ainsi un outil performant au cryptage c'est-à-dire imprédictible.

En effet, la propriété déterministe du chaos associée à l'imprédictibilité permet d'envisager son utilisation dans les crypto-systèmes que nous allons décrire dans le prochain chapitre.

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

3.1. Introduction

Dans le domaine de la télémédecine où les échanges d'informations multimédias se développent rapidement, il est indispensable de pouvoir disposer de systèmes sécurisés et fiables, pour protéger les données confidentielles des patients et veiller à ce que ces données soient collectées et communiquées de manière sécurisée, en tenant compte qu'ils soient accessibles uniquement aux personnes autorisées. Cela est même crucial pour les services de télémédecine, car ils impliquent inévitablement la transmission de données médicales sur des réseaux ouverts tels qu'Internet.

De nos jours, la protection de la confidentialité des données médicales est non seulement une exigence éthique, mais également une obligation légale [1].

Dans ce chapitre, nous proposons un système de sécurité pour le chiffrement d'images médicales basé sur le chaos et l'hyper-chaos utilisant le principe de la permutation et de la diffusion. Ainsi, après une présentation sur les généralités de la cryptographie, nous présentons une vue d'ensemble sur la relation entre le chaos et la cryptographie, suivie d'une description de quelques caractéristiques des images numériques.

Dans la dernière partie de ce chapitre, nous décrivons l'architecture de l'algorithme de chiffrement des images médicales construit autour de deux systèmes chaotiques, la fonction logistique pour la confusion et le système hyper-chaotique de Chen pour la diffusion.

3.2. Système de traitement d'images

Dans une chaîne de traitement d'images, notre travail s'est focalisé sur la partie de transmission sécurisée, en développant un crypto-système pour pouvoir assurer une

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

transmission sans intrus. La figure ci-dessus montre les différents blocs d'un système de traitement d'image.

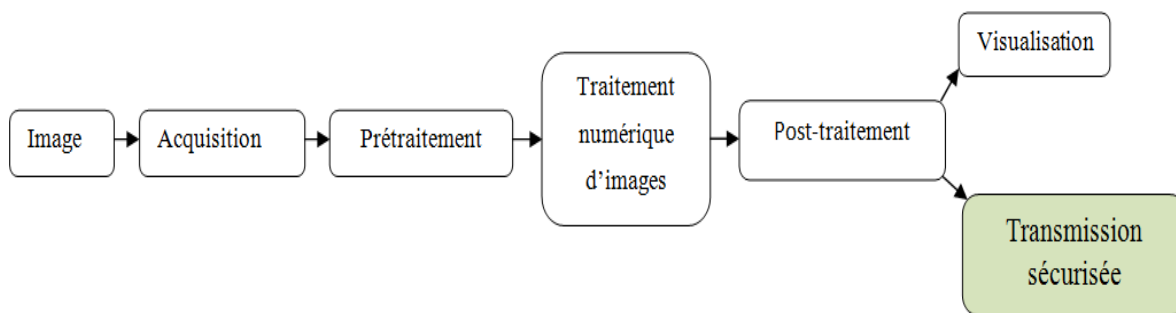


Figure 3.1 : Schéma d'un système de traitement d'images [10].

3.3. La cryptographie

3.3.1. Définition de la cryptographie

La cryptographie désigne un ensemble de méthodes destiné à la sécurité des échanges de données (paroles, images, signes, etc...), c'est-à-dire que ces méthodes vont permettre de chiffrer ses données, et de les rendre inintelligibles. Le fait de coder un message de telle façon à le rendre secret s'appelle chiffrement. La méthode inverse consistant à retrouver le message original, est appelée déchiffrement.

Le chiffrement se fait généralement à l'aide d'une clef de chiffrement, le déchiffrement nécessite quant à lui une clef de déchiffrement.

La cryptographie peut être illustrée par le schéma de principe de la figure (3.2) [10].

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

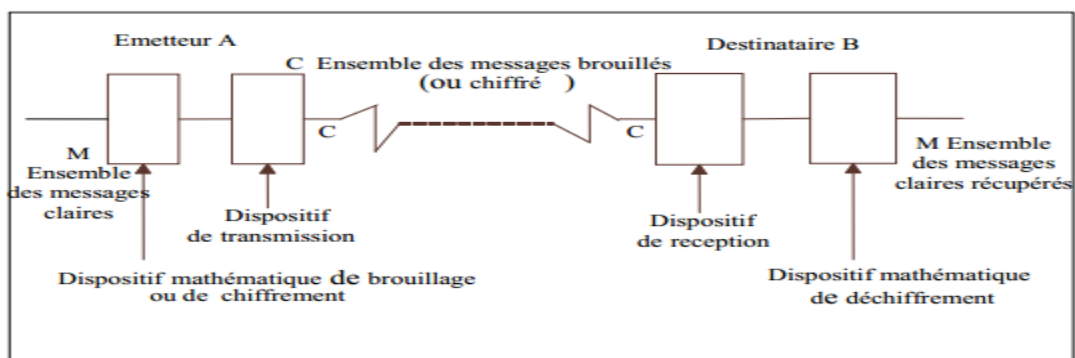


Figure 3.2. Schéma général de la communication chiffrée entre un émetteur et un récepteur.

3.3.2. Historique

- En 487 avant J.C., les grecs employaient un dispositif appelé la "Scytale". C'est un bâton autour duquel une bande longue et mince de cuir était enveloppée et sur laquelle on écrivait le message. Le cuir était ensuite porté comme une ceinture par le messager. Le destinataire avait un bâton identique permettant d'enrouler le cuir afin de déchiffrer le message [12].
- En 50 avant J.C., le premier système de cryptographie à base de mathématiques fut inventé par Jules César. C'est un chiffrement par substitution mono-alphabétique basé sur un décalage des lettres [13].
- En 1970 : Horst Feistel a mené un projet de recherche à IBM Watson Research Lab qui a développé le chiffrement Lucifer, qui inspira plus tard le chiffre DES et d'autres types

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

de chiffrement. Un avantage de ce type d'algorithmes est que chiffrement et déchiffrement sont structurellement identiques [14].

- En 1976 :Whitfield Diffie et Martin Hellman ont publié «New Directions in Cryptography», introduisant l'idée de la cryptographie à clé publique [15] .
- en 1978 :l'algorithme RSA a été publié dans les communications l'Association for Computing Machinery ACM [13].
- 1985 : Victor Miller et Neal Koblitz utilisent les courbes elliptiques pour la cryptographie [14].
- en 1990 :Xuejia Lai et James Massey en Suisse ont publié un algorithme international de cryptage des données (IDEA) qui utilise une clé de 128 bits et utilise des opérations qui sont pratiques pour les ordinateurs à usage général [15].

3.3.3. Terminologies [11] [13]

- **Cryptologie** : Science des messages secrets. Elle englobe la cryptographie et la cryptanalyse.
- **Crypter**: brouiller l'information, la rendre "incompréhensible".
- **Décrypter**: rendre le message compréhensible.
- **Cryptographie** : La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné [6].

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

- **Chiffrement**: transformation à l'aide d'une clé de chiffrement d'un message intelligible appelé texte clair ou libellé en un message incompréhensible ou inintelligible appelé texte chiffré.
- **Clé** : le secret partagé utilisé pour chiffrer le texte clair en texte chiffré et pour déchiffrer le texte chiffré en texte clair.
- **Cryptogramme** : message chiffré. Le destinataire légitime doit pouvoir déchiffrer le cryptogramme et obtenir le texte clair.
- **Un algorithme cryptographique** : c'est une fonction mathématique utilisée dans le processus de chiffrement et de déchiffrement.
- **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.
- **Cryptanalyse** : est la technique qui consiste à déduire un texte en clair d'un texte chiffré sans posséder la clé de chiffrement. Le processus par lequel on tente de comprendre un message en particulier est appelé une **attaque**.

3.3.4. Définition de la clé

La clé est une valeur d'entrée utilisée dans un algorithme de cryptographie. Cette valeur est un nombre complexe dont la taille se mesure en bits. Plus la taille de la clé est grande, plus elle contribue à élever la sécurité. Les clés doivent être stockées de manière sécurisée et de manière à ce que seul leur propriétaire soit en mesure de les atteindre et de les utiliser [16].

- **Les clés symétriques** : il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète.

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

- **Les clés asymétriques** : il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé chiffrement à clé publique). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement.

3.4. Cryptographie et Chaos

De nombreux travaux ont été présentés ces dernières années exploitant les caractéristiques des systèmes chaotiques dans le contexte de la cryptographie, touchant beaucoup plus la transmission sécurisée des données [14][17][18][22][23]. La sécurisation des communications par le chaos est divisée en deux principaux paradigmes distincts.

- Cryptographie chaotique analogique : basée sur les techniques de synchronisation entre l'émetteur et le récepteur [19].
- Cryptographie chaotique numérique : grâce à ses caractéristiques attractives liées aux propriétés requises par le processus de chiffrement. Le chaos a été considéré dans les dernières années comme une solution très prometteuse pour la conception des crypto-systèmes chaotiques numériques [20], dans le cadre de notre travail, on s'intéresse au deuxième paradigme.

Fondamentalement, il existe deux manières générales de concevoir des méthodes de chiffrement chaotiques numériques [18]:

- Utiliser des systèmes chaotiques pour générer un flux de données pseudo-aléatoire, utilisé pour masquer les messages en clair [21].
- Utiliser le texte en clair (image originale) et/ou les clés secrètes comme conditions initiales et/ou paramètres de contrôle, itérer des systèmes chaotiques plusieurs fois pour obtenir un texte chiffré [22].

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

La première correspond au chiffrement de flux. La seconde correspond au chiffrement par bloc qui est basée principalement sur la structure proposée par Fridrich [23] qui utilise l'architecture traditionnelle de confusion diffusion proposée par Shannon [23]. La méthode proposée pour le chiffrement des images médicales est basée sur cette structure (voir chapitre.3 section 3.6).

3.5. Caractéristiques d'une image numérique [24]

Les principales caractéristiques d'une image sont :

- **Pixels** : Ceux sont les plus petits éléments constitutifs d'une image numérique auquel on peut associer une couleur ou un niveau de gris et une intensité.
- **Histogramme** : L'histogramme des niveaux de gris ou des couleurs d'une image est une fonction qui donne la fréquence d'apparition de chaque niveau de gris (couleur) dans l'image. Il permet de donner un grand nombre d'information sur la distribution des niveaux de gris (couleur) et de voir entre quelles bornes est répartie la majorité des niveaux de gris (couleur) dans le cas d'une image trop claire ou d'une image trop foncée.
- **Niveau de gris** : Le niveau de gris est la valeur de l'intensité lumineuse en un point. La couleur du pixel peut prendre des valeurs allant du noir au blanc en passant par un nombre fini de niveaux intermédiaires. Donc pour représenter les images à niveaux de gris, on peut attribuer à chaque pixel de l'image une valeur correspondant à la quantité de lumière renvoyée. Cette valeur peut être comprise par exemple entre 0 et 255 (pour un codage de 8 bit). Chaque pixel n'est donc plus représenté par un bit, mais par un octet.

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

- **Dimension** : C'est la taille de l'image. Cette dernière se présente sous forme de matrice dont les éléments sont des valeurs numériques représentatives des intensités lumineuses (pixels). Le nombre de lignes de cette matrice multiplié par le nombre de colonnes nous donne le nombre total de pixels dans une image.

3.6. Cryptage des images médicales à l'aide des systèmes chaotiques

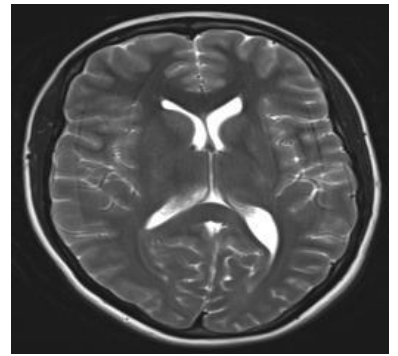
3.6.1. Algorithme de chiffrement

Le schéma de chiffrement basé sur le chaos est composé de deux processus : confusion chaotique des positions de pixels par phénomène de permutation et diffusion des valeurs de niveau de gris des pixels par phénomène de diffusion.

Dans la 1ere phase de l'algorithme, nous allons utiliser une fonction logistique chaotique décrite dans l'équation (1.16) pour la partie de permutation, et dans la 2eme phase nous utiliserons le système hyper-chaotique « 4d » de Chen décrit dans l'équation (2.1) pour la partie de diffusion.

Remarque : Nous allons appliquer le cryptage le cryptage pour les 3 images suivant :

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales



Image(a) : radiographie pulmonaire

Image (b) : CT abdomen

Image (c) : IRM cérébrale

Figure 3.3. Images médicale utiliser .

a. Phase de confusion

Étant donné que les images numériques sont généralement représentées sous forme de matrices bidimensionnelles et sans perte de généralités, nous supposons que la dimension de l'image standard est $N \times M$, $P_{i,j}(I)$ représente la position du pixel ainsi que son intensité (I) avec $i = 0,1, \dots, M - 1$; $j = 0,1, \dots, N - 1$ (figure 3.4).

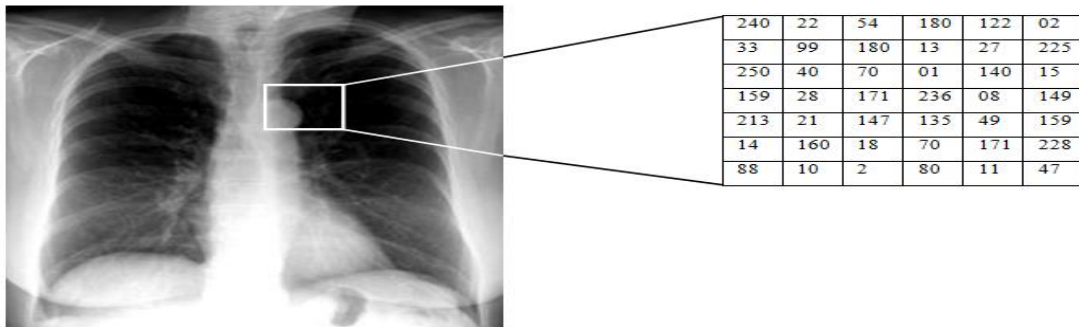


Figure 3.4. Représentation matricielle d'une image.

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

La procédure de réarrangement de la position des pixels est décrite suivant l'organigramme de cryptage de la figure 3.5.

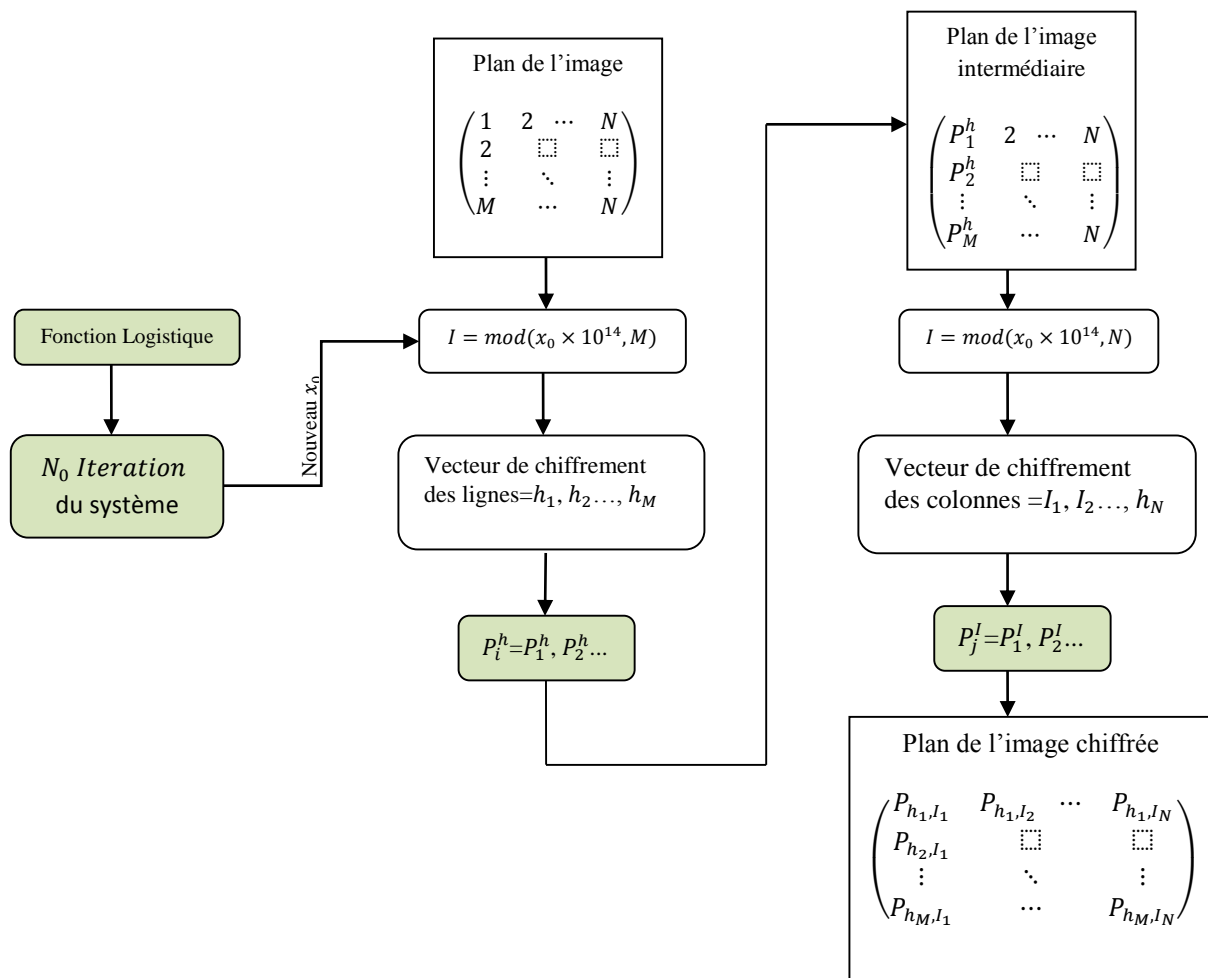


Figure 3.5. Organigramme de chiffrement par permutation des lignes et des colonnes.

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

Etape 1 : La fonction logistique est itérée pendant N_0 fois pour éviter l'effet néfaste de la procédure transitoire, ce qui donnera un nouveau x_0 qui sera utilisé dans l'expression :

$$I = \text{mod}(x_0 \times 10^{14}, M) \quad (3.1)$$

Avec $I \in [0, M - 1]$.

Où I est le reste de la division modulo M

On continue l'itération de la fonction logistique et l'expression (3.1) jusqu'à obtenir M valeurs qui sont toutes comprises entre 0 et $M - 1$ sans répétition. Ces valeurs peuvent être réorganisées sous la forme de $\{h_i, i = 1, 2, \dots, M\}$ ou $h_i \neq h_j$ si $i \neq j$, c'est-à-dire que le réarrangement des lignes de l'image va se faire suivant les valeurs obtenues : ainsi la ligne h_1 va devenir la première ligne et la ligne h_2 va devenir la seconde ligne et ainsi de suite, créant une nouvelle image correspondant à une matrice de position $P_{h_i, j}$ généré sur la base de la transformation de ligne (figure 3.6).

Le nombre d'itération de (3.1) dépend entièrement de la taille de l'image, le tableau ci-dessous résume le lien entre le nombre d'itérations et la taille de l'image :

Taille de l'image	Le nombre moyen d'itérations nécessaires pour accomplir une transformation de ligne
32×32	80
64×64	300
128×128	520
256×256	1600

Tableau 3.1. Le lien entre le nombre d'itération et la taille de l'image.

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

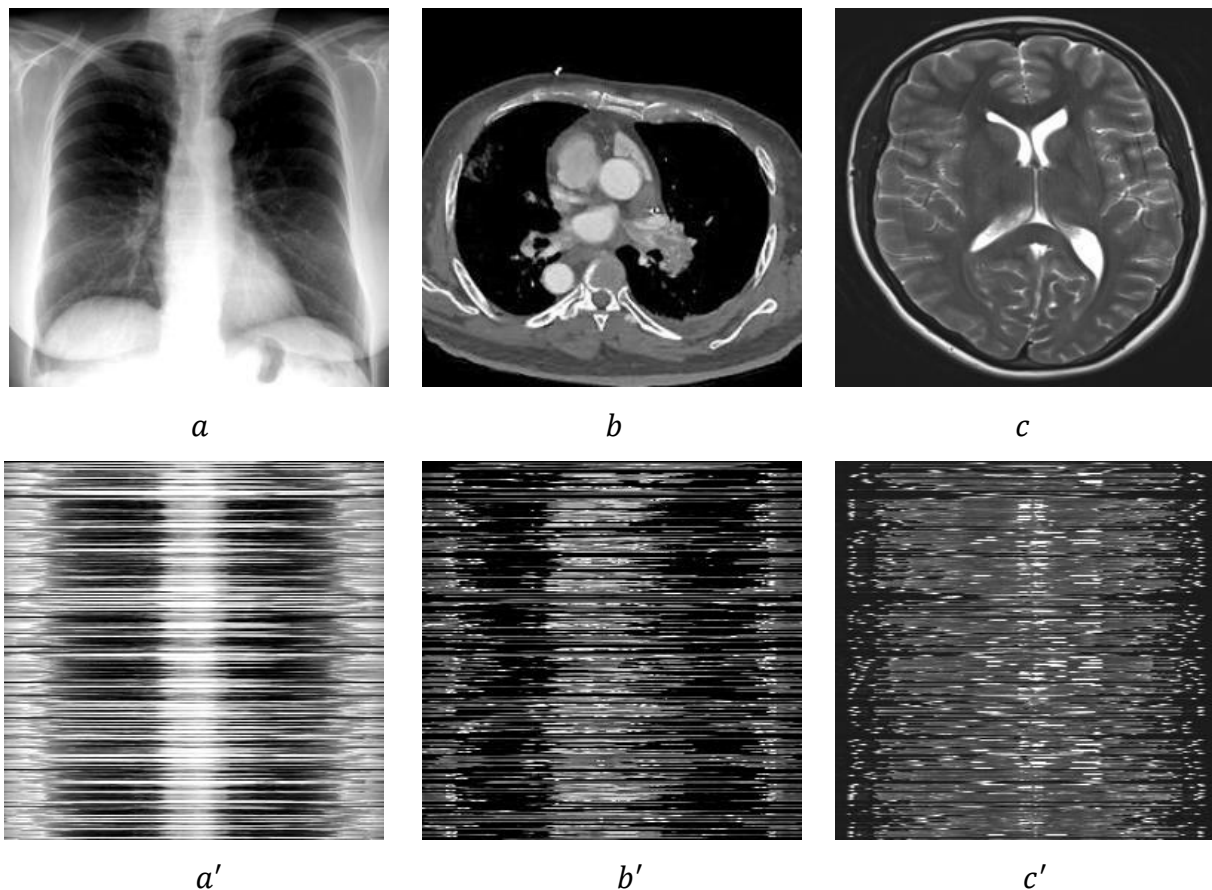


Figure 3.6. Chiffrement par ligne appliqué aux images (a , b , c) , (a' , b' , c') sont les images cryptées correspondante .

Etape 2 : Pour la nouvelle matrice $P_{h,i,j}$ nous allons répéter ce processus pour les colonnes en utilisant le même x_0 pour la fonction logistique :

$$I = \text{mod}(x_0 \times 10^{14}, N) \quad (3.2)$$

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

Avec $I \in [0, N - 1]$.

Où I est le reste de la division modulo N .

En appliquant le même principe que le précédent c'est-à-dire en continuant les itérations sur la fonction logistique et l'expression (3.2) pour obtenir un certain nombre de valeurs du reste de la division, ces valeurs doivent être différentes, comprises entre 0 et $N - 1$, et peuvent être réorganisées sous la forme de $\{I_i, i = 1, 2, \dots, N\}$ ou $I_i \neq I_j$ si $i \neq j$. Les colonnes de $P_{h_i, j}$ vont être réarrangées suivant ces valeurs, ainsi la colonne I_1 va devenir la première colonne et I_2 va devenir la seconde colonne formant ainsi une nouvelle image P_{h_i, I_j} généré sur la base de la transformation de ligne et de colonne (figure 3.7).

Dans cette première partie le processus décrit a permis de permuter tous les pixels de l'image c'est-à-dire le réarrangement des lignes de l'image suivi des colonnes donnant naissance au phénomène de chiffrement par permutation.

La particularité de ce processus est que tous les pixels sont réarrangés de manière pseudo-aléatoire, ce qui conduit à une grande réduction de la corrélation entre les pixels adjacents.

La figure ci dessous représente le chiffrement par colonnes appliqué sur les images chiffrées précédemment par un chiffrage ligne, donc les figures 3.7 (a'' , b'' , c'') représentent un chiffrement complet par permutation des lignes suivie des colonnes.

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

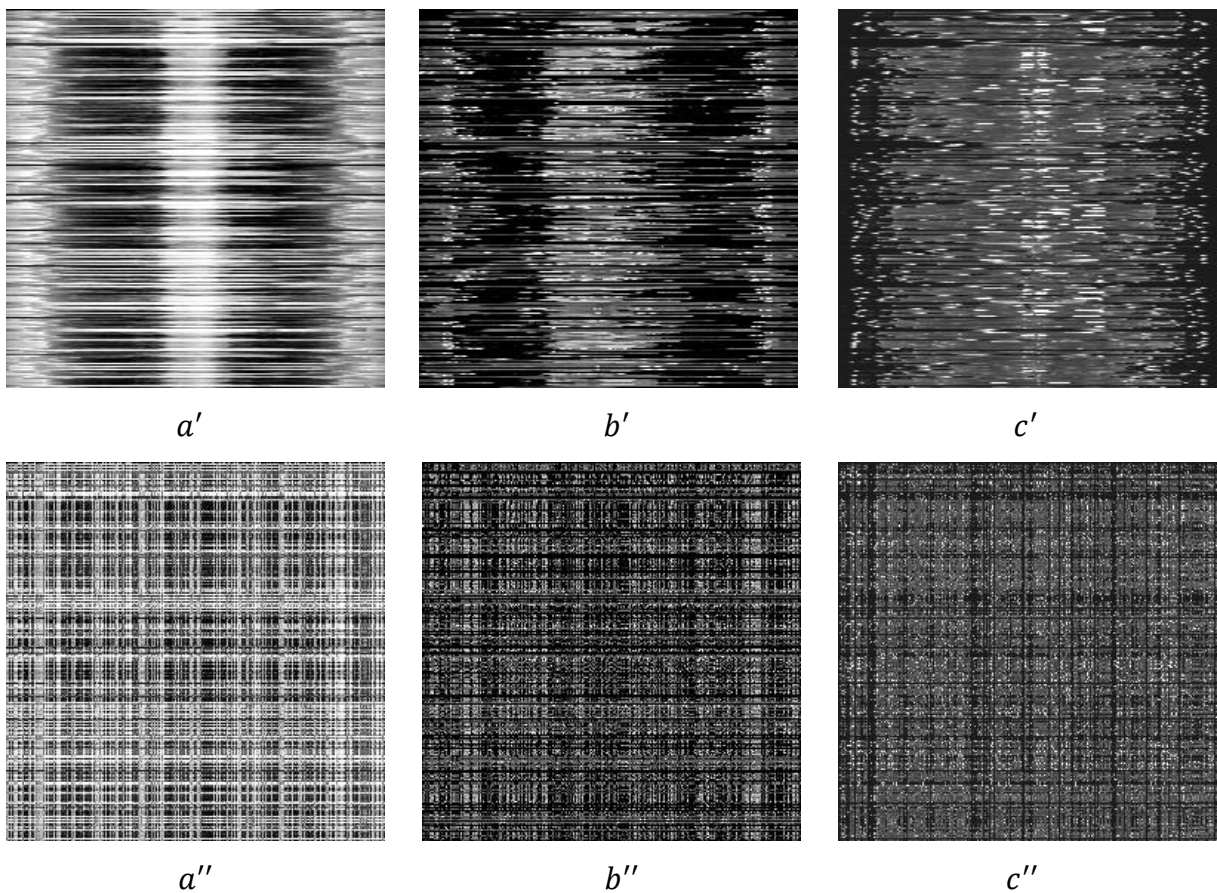


Figure 3.7. Chiffrement par lignes (a' , b' , c') suivi d'un chiffrement par colonnes (a'' , b'' , c'') des 3 images médicale (voir remarque).

b. Phase de diffusion

Après avoir obtenu l'image P_{h_i, l_j} cryptée en utilisant la carte logistique, le système hyper-chaotique de Chen est utilisé pour chiffrer l'image obtenue précédemment par confusion. Le schéma de cryptage (figure 3.8) est basé sur la combinaison des variables d'état du système

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

hyper-chaotique (2.1). Trois des quatre variables sont combinées différemment, de manière à obtenir quatre combinaisons différentes, qui sont données dans le tableau ci-dessous :

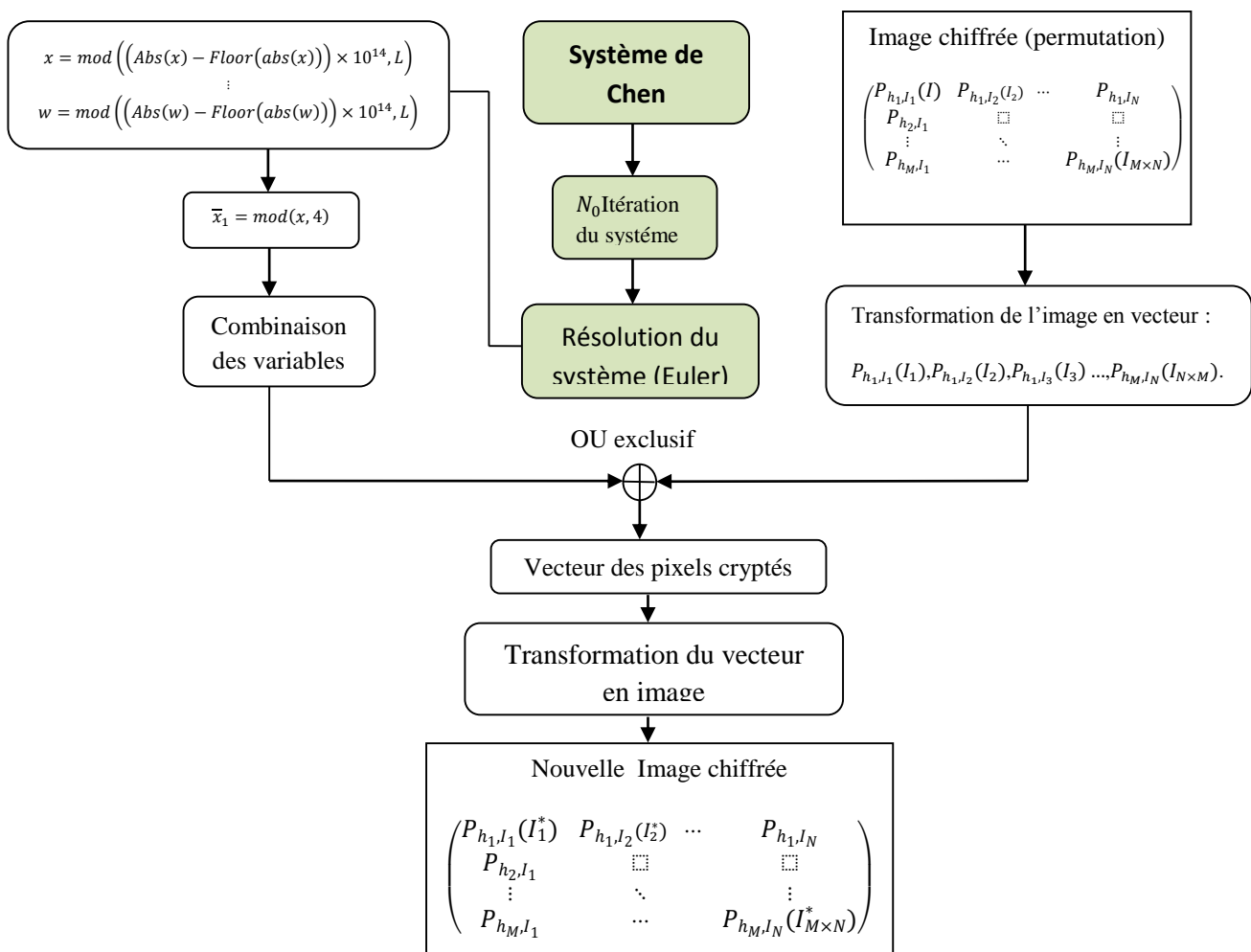


Figure 3.8. Organigramme de chiffrement par diffusion.

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

L'organigramme ci-dessus résume tous les étapes de la diffusion des pixels, en commençant par la génération du système hyper chaotique jusqu'à l'affichage de l'image diffusée.

Etat numéro	Combinaison des états
0	(x, y, z)
1	(x, y, w)
2	(x, z, w)
3	(y, z, w)

Tableau 3.2. Différentes combinaisons d'états du système hyper-chaotique.

Etape 1 : On commence tout d'abord à itérer le système (2.1) pendant N_0 fois pour éviter l'effet néfaste de la procédure transitoire, où N_0 est une constante.

Pour résoudre le système d'équation, on utilise la méthode d'intégration d'Euler, telle que :

$$\begin{cases} x_{n+1} = x_n + f(x) \times h, \\ y_{n+1} = y_n + f(y) \times h, \\ z_{n+1} = z_n + f(z) \times h, \\ w_{n+1} = w_n + f(w) \times h, \end{cases} \quad (3.3)$$

Où :

$$\begin{cases} f(x) = a(y - x) \\ f(y) = -xz + dx + cy - w \\ f(z) = xy - bz \\ f(w) = x + k \end{cases}$$

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

Où h est le pas d'intégration .

Etape 2 : Le système de Chen est itéré en permanence. Pour chaque itération, nous pouvons obtenir quatre valeurs d'état x, y, z, w , ces valeurs sont prétraitées comme suit :

$$\begin{cases} x = \text{mod} \left(\left(\text{Abs}(x) - \text{Floor}(\text{abs}(x)) \right) \times 10^{14}, L \right), \\ y = \text{mod} \left(\left(\text{Abs}(y) - \text{Floor}(\text{abs}(y)) \right) \times 10^{14}, L \right), \\ z = \text{mod} \left(\left(\text{Abs}(z) - \text{Floor}(\text{abs}(z)) \right) \times 10^{14}, L \right), \\ w = \text{mod} \left(\left(\text{Abs}(w) - \text{Floor}(\text{abs}(w)) \right) \times 10^{14}, L \right), \end{cases} \quad (3.4)$$

Où $\text{Abs}(x)$ renvoie la valeur absolue de x . $\text{Floor}(x)$ retourne la valeur de x au nombre entier le plus proche inférieur ou égal à x , $\text{mod}(x, y)$ donne le reste de la division modulo L et L est le niveau de couleur (pour nos images c'est 256 niveaux de gris).

Etape 3 : Elle consiste à générer \bar{x}_1 en utilisant la formule suivante:

$$\bar{x}_1 = \text{mod}(x, 4). \quad (3.5)$$

Avec $\bar{x}_1 \in [0,3]$, est le reste de la division de x modulo 4.

Le résultat de \bar{x}_1 va nous permettre de choisir le groupe de combinaison des états grâce au tableau (3.2), pour effectuer une opération de chiffrement. Par exemple si $\bar{x}_1 = 2$, alors le groupe numéro 2 correspondant à (x, z, w) est utilisé pour le chiffrement.

La procédure de chiffrement consiste à effectuer une opération XOR (OU exclusive),

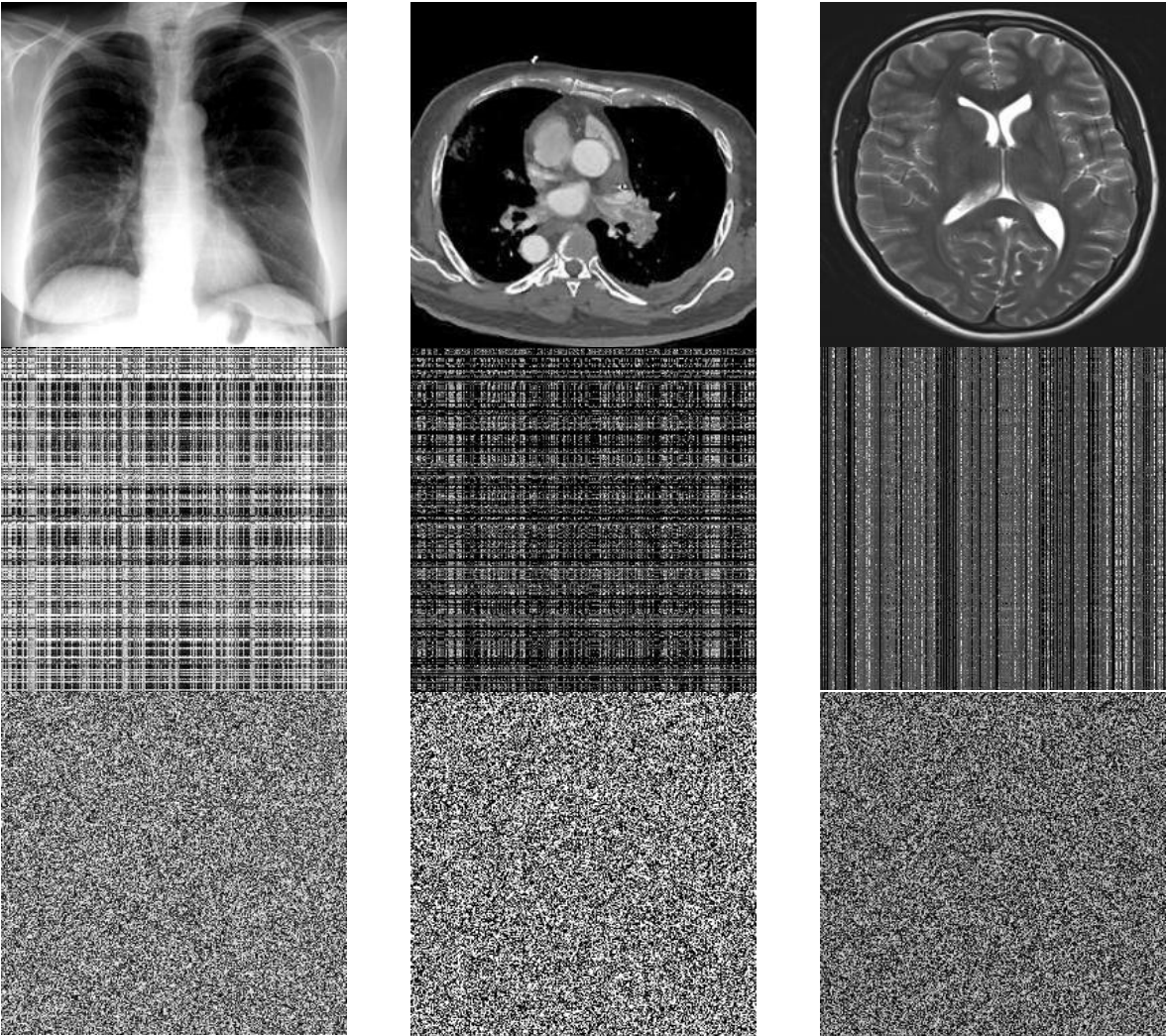
Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

bit-par-bit entre la valeur du pixel de l'image P_{h_i, I_j} et la valeur d'état du système suivant cette formule :

$$\begin{cases} C_{3 \times (i-1) + 1} = P_{3 \times (i-1) + 1} \oplus B_{x_1} \\ C_{3 \times (i-1) + 2} = P_{3 \times (i-1) + 2} \oplus B_{x_2} \\ C_{3 \times (i-1) + 3} = P_{3 \times (i-1) + 3} \oplus B_{x_3} \end{cases} \quad (3.6)$$

Où $i = 1, 2, \dots, N \times M$, représente l'itération du système hyper-chaotique. Le symbole \oplus représente l'opération OU exclusive bit par bit. $P_i, i = 1, 2, \dots, N \times M$, représente les valeurs des intensités des pixels de l'image crypté par confusion P_{h_i, I_j} précédemment par la fonction logistique. B_{x_1}, B_{x_2} et B_{x_3} , représentent les valeurs d'état du groupe correspondant par rapport à la série \bar{x}_1 , c'est-à-dire qu'elles représentent les variables choisies de équation (2.1) après avoir été transformé par équation. (3.4). Le processus ne s'achève pas avant que l'ensemble $P_{h_i, I_j} = \{P_1, P_2, \dots, P_{N \times M}\}$ soit entièrement crypté. Ainsi l'ensemble des pixels cryptés $C = \{C_1, C_2, \dots, C_{N \times M}\}$ est réarrangé dans la nouvelle image P'_{h_i, I_j}

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales



(a)

(b)

(c)

Figure 3.9. Chiffrement par permutation suivi d'un chiffrement par diffusion des images (a, b, c).

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

3.6.2. Algorithme de déchiffrement

En général, la procédure de déchiffrement est similaire à celle du processus de chiffrement, sauf que l'ordre est inversé, c'est-à-dire que pour l'image cryptée, il faut tout d'abord, déchiffrer l'image à l'aide du système hyper-chaotique de Chen avec les mêmes paramètres et valeurs initiales que ceux utilisés pour le cryptage. Ensuite, pour la 2eme partie il faut aussi utiliser la fonction logistique avec les mêmes paramètres et valeurs initiales que ceux utilisés pour le chiffrement, pour obtenir l'image originale.

Le crypto-système proposé étant un chiffrement à clé symétrique, la même clé secrète et les conditions initiales (x_0, \dots) doivent être utilisées pour le déchiffrement. Le processus de déchiffrement peut être décrit comme suit:

Suivre les mêmes étapes que la partie 2 de l'algorithme de chiffrement en allant de l'étape 1 jusqu'à 3, sauf que pour l'équation (3.6), l'ensemble $C = \{C_1, C_2, \dots, C_{N \times M}\}$ désigne le pixel déchiffré. Ainsi en supprimant l'effet de diffusion de l'image chiffrée, on obtient une image intermédiaire (figure 3.10)

Dans la dernière étape, après l'obtention de l'image intermédiaire, on utilise la fonction logistique grâce à la clé secrète et avec les mêmes conditions initiales, pour réarranger les colonnes suivies des lignes et ainsi supprimer l'effet de la permutation pour récupérer l'image originale (figure 3.10).

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

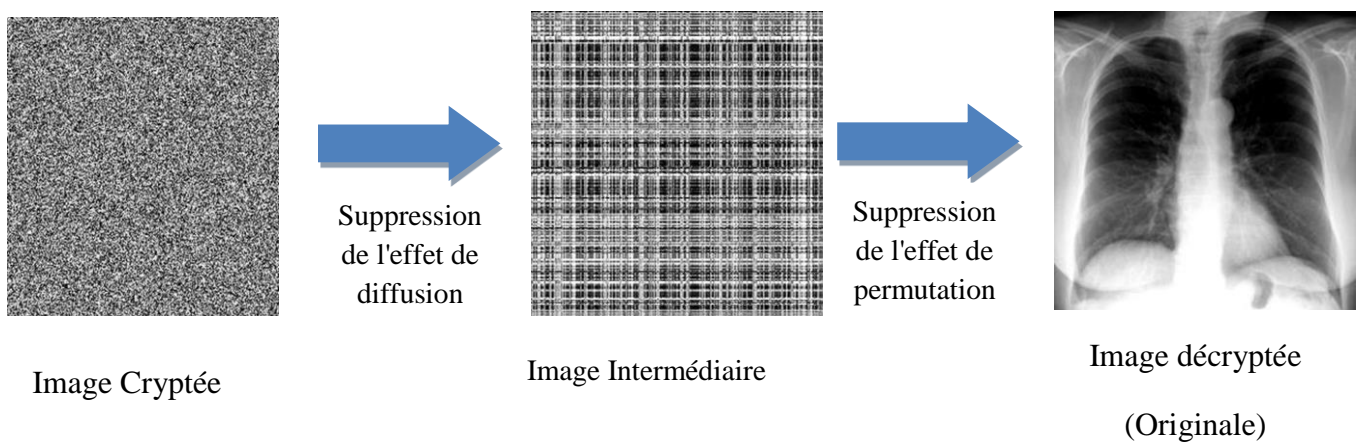


Figure 3.10. Principe du décryptage.

3.7. Intégration du crypto-système proposé

Notre crypto-système proposé peut être facilement intégré dans un système de téléradiologie en tant que module de sécurité indépendant, comme illustré par la figure 3.11

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

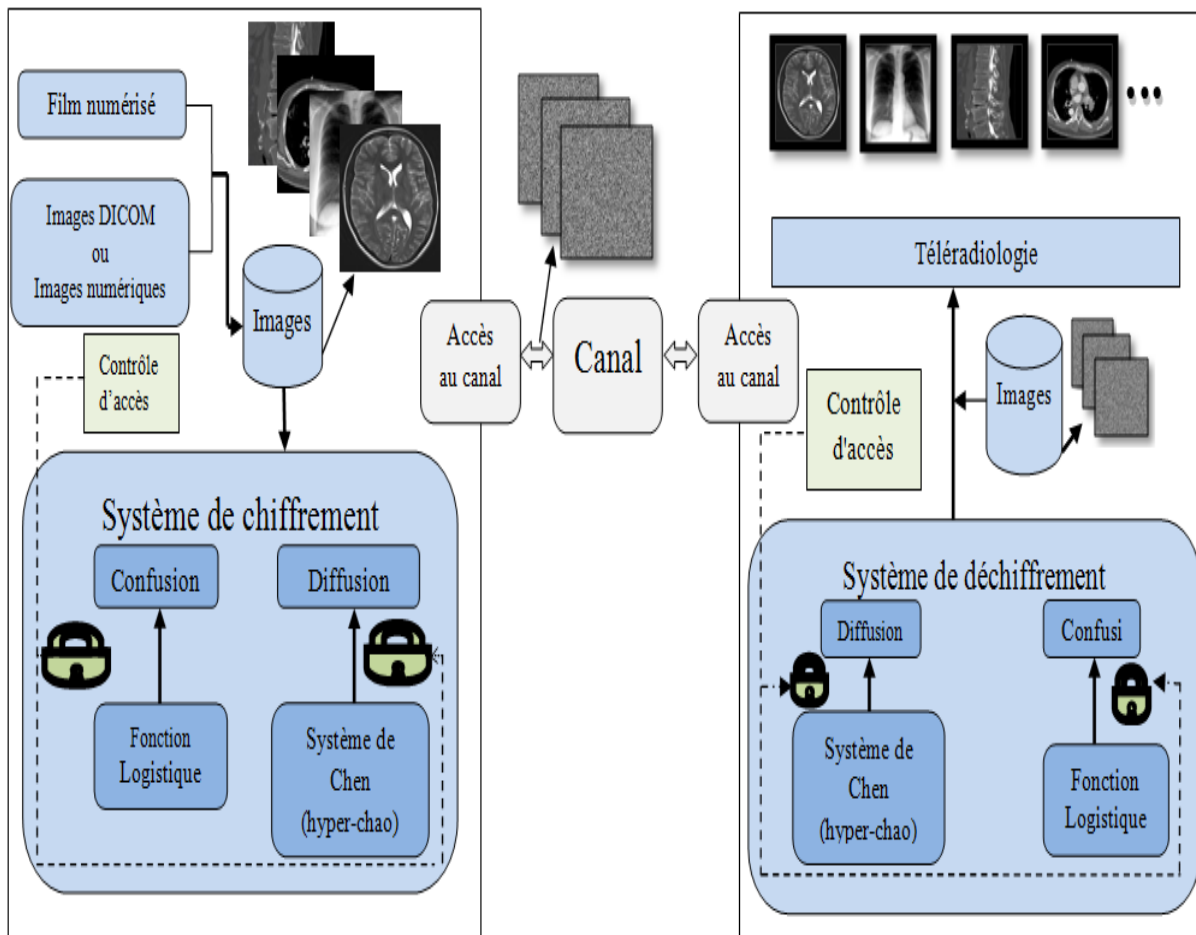


Figure 3.11 : Intégration du crypto-système dans une chaîne de téléradiologie.

Chapitre 3 cryptages hyper-chaotiques appliqués en imagerie médicales

3.8. Conclusion

Nous avons introduit dans ce chapitre les notions de base qui servent de fondement à la compréhension de la cryptographie, ainsi que les différentes caractéristiques d'une image numérique. Nous avons ensuite montré le lien qui unit la cryptographie aux systèmes chaotiques en expliquant l'application du chaos dans le chiffrement d'image.

Par la suite un schéma de cryptage chaotique a été proposé dans ce chapitre. Les systèmes chaotiques utilisés (logistique et Chen) vont servir à générer les clés de chiffrement. Les résultats de l'application de cet algorithme ont été illustrés après chaque étape (confusion et diffusion).

Le prochain chapitre suivant est dédié à l'implémentation et l'analyse de sécurité du crypto-système, basé sur les attaques différentielles et l'étude des analyses statistiques.

Chapitre 4 Implémentation et analyses de sécurités

4.1. Introduction

Le cryptage en imagerie médicale joue un rôle important dans le domaine de la sécurité de l'information médicale, il est donc nécessaire de concevoir un système de chiffrement performant, pour obtenir des images chiffrées de manière aléatoire telles que les attaquants ne peuvent pas comprendre les relations internes entre l'image en clair et l'image chiffrée.

Dans ce chapitre, nous effectuons des tests de sécurité et d'analyse sur l'algorithme de chiffrement médicale ,décrit dans le chapitre précédent tels que l'analyse différentielle, l'analyse de sensibilité de la clé de cryptage , et d'autres analyses appelées analyses statiques, comme l'analyse d'histogramme, l'analyse d'entropie et de corrélation, puis nous effectueront une comparaison des résultats ainsi obtenus avec d'autre méthodes de chiffrements. Puis, une interface graphique a été mise en œuvre sous langage Matlab a l'aide de l'outil Matlab Interface GUI (Graphical User Interface).

4.2. Analyse différentielle

Pour tester l'influence d'un changement d'un pixel sur l'image entière chiffrée par n'importe quel algorithme de cryptage, deux paramètres communs peuvent être utilisé: NPCR et UACI [24] ; ils sont amplement utilisés dans l'analyse de sécurité dans la communauté de cryptage d'image pour les attaques différentielles.

Pour mettre en œuvre une attaque différentielle, un adversaire apporte généralement un léger changement, généralement un pixel, dans l'image simple et chiffre les deux images en utilisant la même clef secrète. Ce genre de cryptanalyse peut devenir inefficace et pratiquement inutile si un changement mineur dans l'image simple peut être efficacement diffusé à l'image entière chiffrée.

Chapitre 4 Implémentation et analyses de sécurités

Les critères de nombre de pixels changeants (NPCR) et d'intensité modifiée unifiée moyenne (UACI) sont généralement utiles pour étudier les performances des attaques différentielles résistantes.

Les formules pour calculer le NPCR et l'UACI sont :

$$\text{NPCR} = \frac{\sum_{i=1}^H \sum_{j=1}^L D(ij)}{H * L} \quad (4.4)$$

La valeur optimale du NPCR est de l'ordre 99.6094 %.

$$\text{UACI} = \frac{1}{H * L} \frac{\sum_{i=1}^H \sum_{j=1}^L |IC1ij - IC2ij|}{Z^{H-1}} * 100 \quad (4.5)$$

La valeur optimale d'UACI est de l'ordre 33.4635 %.

Où H et L représentent la largeur et la hauteur de l'image respectivement. IC1 et IC2 sont les images chiffrées avant et après modification d'un pixel de l'image standard, respectivement.

D (i, j) peut être défini par :

$$D(i, j) = \begin{cases} 1 & \text{si } IC1 \neq IC2 \\ 0 & \text{sinon} \end{cases} \quad (4.6)$$

Le crypto système d'images proposé est exécuté sur les images standards et les images modifiées (modification d'un seul pixel), ensuite on calcule le NPCR et l'UACI. Les résultats sont représentés dans la figure ci dessous :

Chapitre 4 Implémentation et analyses de sécurités



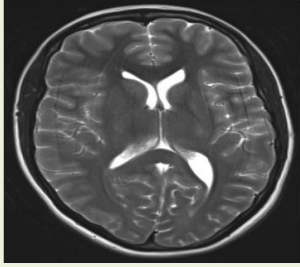





Les images originales	NPCR	UACI	Les images secrètes	NPCR	UACI
 <p>Echo cœur</p>	99.60%	34.74 %	 <p>IRM encéphalique</p>	99.23%	34.65 %
 <p>TDM de Crâne</p>	99.60%	31.88 %	 <p>IRM colon vertébral</p>	98.72 %	33.30%
 <p>Radiographie du pied</p>	98.87%	41.52%	 <p>CT abdomen</p>	99.15%	39.13%
 <p>Radio main droite</p>	99.62%	36.75%	 <p>Radiographie cervicale</p>	99.62%	38.22%

Figure 4.1. Résultats d'efficacité de notre algorithme pour les valeurs de NPCR et UACI.

Chapitre 4 Implémentation et analyses de sécurités

Il est très clair que les valeurs des NPCR et UACI pour tous les cas du test restent dans la gamme des valeurs espérées, c'est-à-dire que l'algorithme proposé montre une extrême sensibilité par rapport à l'image claire. Par conséquent, l'algorithme résiste bien à l'attaque différentielle.

4.3. Analyse de l'espace clef

L'espace des clefs est le nombre total des différentes clefs employées dans la procédure de chiffrement ou de déchiffrement. L'espace clé doit être suffisamment grand pour empêcher les adversaires de deviner la clef en utilisant une attaque par force brute [25], Comme il a été mentionné auparavant, la clef de chiffrement dans la technique proposée est composée de huit parties : un nombre réel et un nombre entier $(X(1), N'_0)$ pour la confusion et quatre nombres réels et deux nombre entier $(x_0, y_0, z_0, w_0, N_0, K)$ pour la diffusion, où K peut prendre n'importe quelle valeur dans l'intervalle $[-0.7, 0.7]$, et N peut avoir n'importe quelle valeur entière. Si on considère une précision de 10^{-14} , le nombre total des valeurs possibles de $(x_0, y_0, z_0, w_0, N_0, K, X(1), N'_0)$ qui peuvent être employées dans la procédure de chiffrement ou de déchiffrement est $(10^{14} \times 8)$ (tableau 4.2).

Dans la technique de chiffrement proposée, la variable K prend n'importe quelle valeur. Par conséquent, il y a un nombre infini des valeurs possibles de K qui peuvent être employées dans la clef secrète. Mais si on se limite à l'intervalle, K également peut avoir un nombre total de 1.4×10^{14} .

Le nombre total des valeurs possibles qui peuvent être employées est effectivement infini. Puisque les valeurs de N_0 et N'_0 affecte directement la vitesse d'exécution des procédures de chiffrement ou de déchiffrement (nombre d'itérations), on préfère garder les valeurs de N_0 et N'_0 autour de 3000. Ce qui rend le nombre total des valeurs possibles prise par N_0 et N'_0 égale

Chapitre 4 Implémentation et analyses de sécurités

à 10^6 . Ainsi, l'espace de la clef pour la technique de chiffrement ou de déchiffrement est $\approx 10^{90}$, ce qui est suffisant pour résister à l'attaque exhaustive.

Clé	Description	Espace clé
x_0, y_0, z_0, w_0	Les conditions initiales du système Chen	10^{56}
N0	Nombre d'itération pour la diffusion	10^3
X(1)	Condition initiale de la fonction Logistique	10^{14}
K	Paramètre de système	10^{14}
N'_0	Nombre d'itération pour la confusion	10^3
Total	Espace des clés total	10^{90}

Tableau 4.1. L'espace des clés pour le processus de chiffrement proposé.

4.4. Test de sensibilité clef

La sensibilité à la clef secrète est une caractéristique essentielle pour un bon crypto-système qui garantit la sécurité de ce dernier contre toute attaque exhaustive. On effectue un test pour observer la sensibilité à la clef secrète de notre algorithme de chiffrement:

- **Test 01** : l'image chiffrée produite par le système cryptographique devrait être très sensible à la clef secrète, c'est-à-dire, si on emploie une clef légèrement différente pour déchiffrer la même image (chiffrées), l'image décryptée ne peut pas être déchiffrée correctement à cause d'une légère différence entre la clef de chiffrement et de déchiffrement.

Les figures ci-dessous représentent les images résultantes du test de déchiffrement avec diverses clés :

Chapitre 4 Implémentation et analyses de sécurités

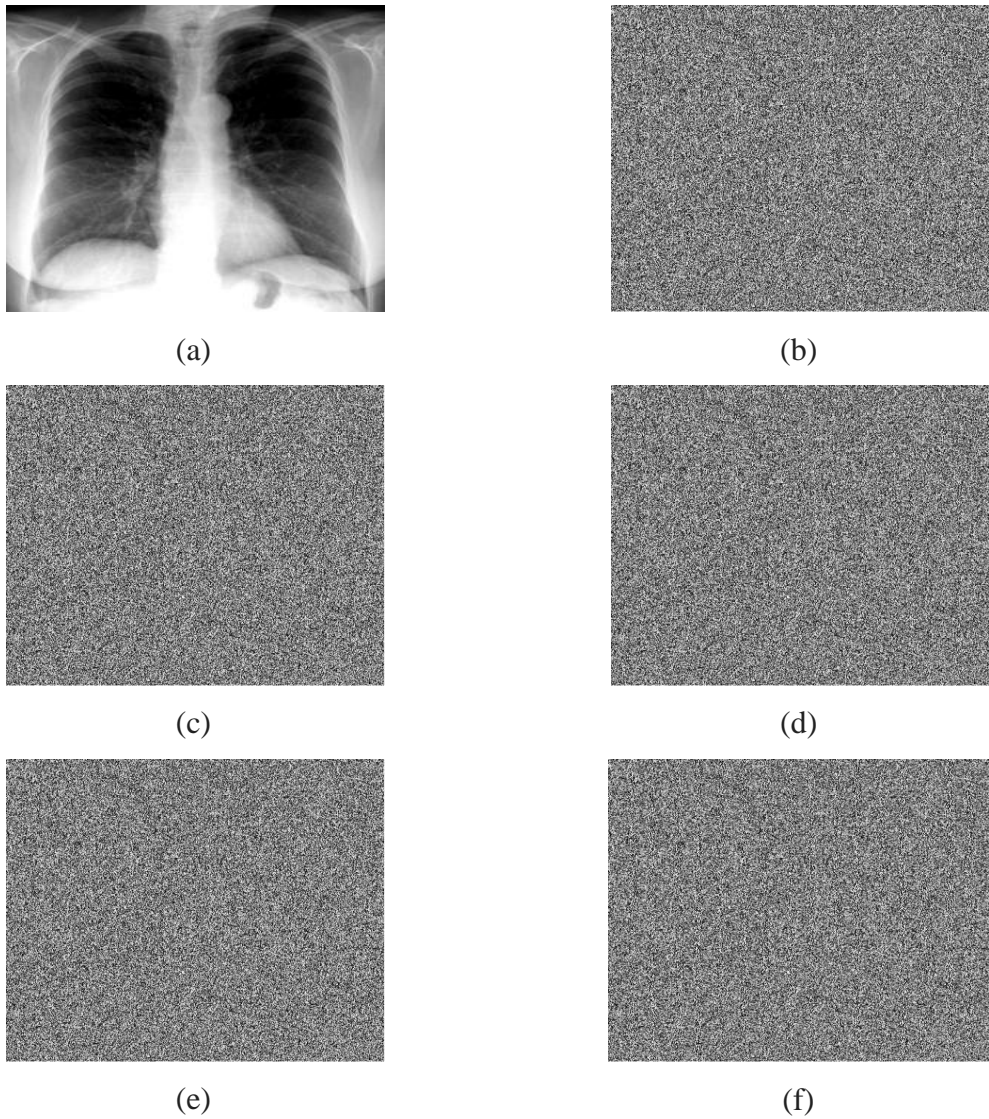


Figure 4.2 Résultats expérimentaux de chiffrement et de déchiffrement.

Chapitre 4 Implémentation et analyses de sécurités

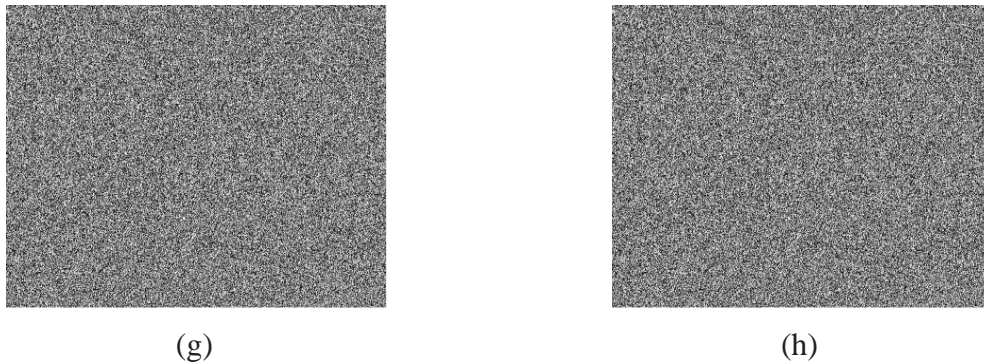


Figure 4.2 (suite) Résultats expérimentaux de chiffrement et de déchiffrement.

- la figure 4.2 : (a) est l'image décryptée avec les mêmes paramètres que ceux utilisés dans les algorithmes de cryptage, c'est-à-dire $x_0 = 0,3$, $y_0 = -0,4$, $z_0 = 1,2$, $w_0 = 1$ et $N_0 = 3\ 000$, $K = 0,2$, $X(1) = 0,87655$.
- la figure 4.2 : (b) est l'image décryptée avec les mêmes paramètres utilisés dans l'algorithme de chiffrement, sauf pour $x_0 = 0,300000000001$.
- les figures 4.2 : (c) est l'image décryptée avec les mêmes paramètres utilisés dans l'algorithme de chiffrement, sauf pour $y_0 = -0,400000000001$.
- les figures 4.2 : (d) est l'image décryptée avec les mêmes paramètres utilisé dans l'algorithme de chiffrement, sauf pour $z_0 = 1,200000000001$.
- les figures 4.2 : (e) est l'image décryptée avec les mêmes paramètres utilisés dans l'algorithme de chiffrement, sauf pour $w_0 = 1,000000000001$.
- la figure 4.2 : (f) est l'image décryptée avec le nombre d'itération initial différent $N_0 = 3001$.
- les figures 4.2 : (g) est l'image décryptée avec les mêmes paramètres utilisés dans l'algorithme de chiffrement, sauf pour $k = 0,200000000001$.

Chapitre 4 Implémentation et analyses de sécurités

- la figure 4.2 : (h) est l'image décryptée avec les mêmes paramètres utilisés dans l'algorithme de chiffrement, sauf pour $X(1) = 0.87656$.

D'après les résultats du test, l'algorithme de cryptage hyper-chaotique est très sensible à la clé, cela étant dû à la sensibilité des systèmes chaotiques aux conditions initiales : un petit changement de la clé générera un résultat de déchiffrement complètement différent.

4.5. Analyses statistiques

Un chiffrement d'image peut être cassé avec succès à l'aide d'attaque statistique [26]. Pour prouver la robustesse de la méthode proposée contre les attaques statistiques, une analyse statistique a été obtenue dans cette section. Ceci a été achevé en utilisant :

- l'analyse des histogrammes.
- entropie.
- l'analyse des coefficients de corrélation.

4.5.1. Analyse des histogrammes

L'histogramme de l'image chiffrée doit avoir deux propriétés [26]:

- Il doit être totalement différent de l'histogramme de l'image originale.
- Il doit avoir une distribution uniforme, ce qui signifie que la probabilité d'occurrence de n'importe quelle valeur est la même.

Une analyse expérimentale (un test visuel) de l'algorithme de chiffrement d'image proposé a été effectuée, sur des images médicales différentes illustrées sur figure 4.3 :

Chapitre 4 Implémentation et analyses de sécurités

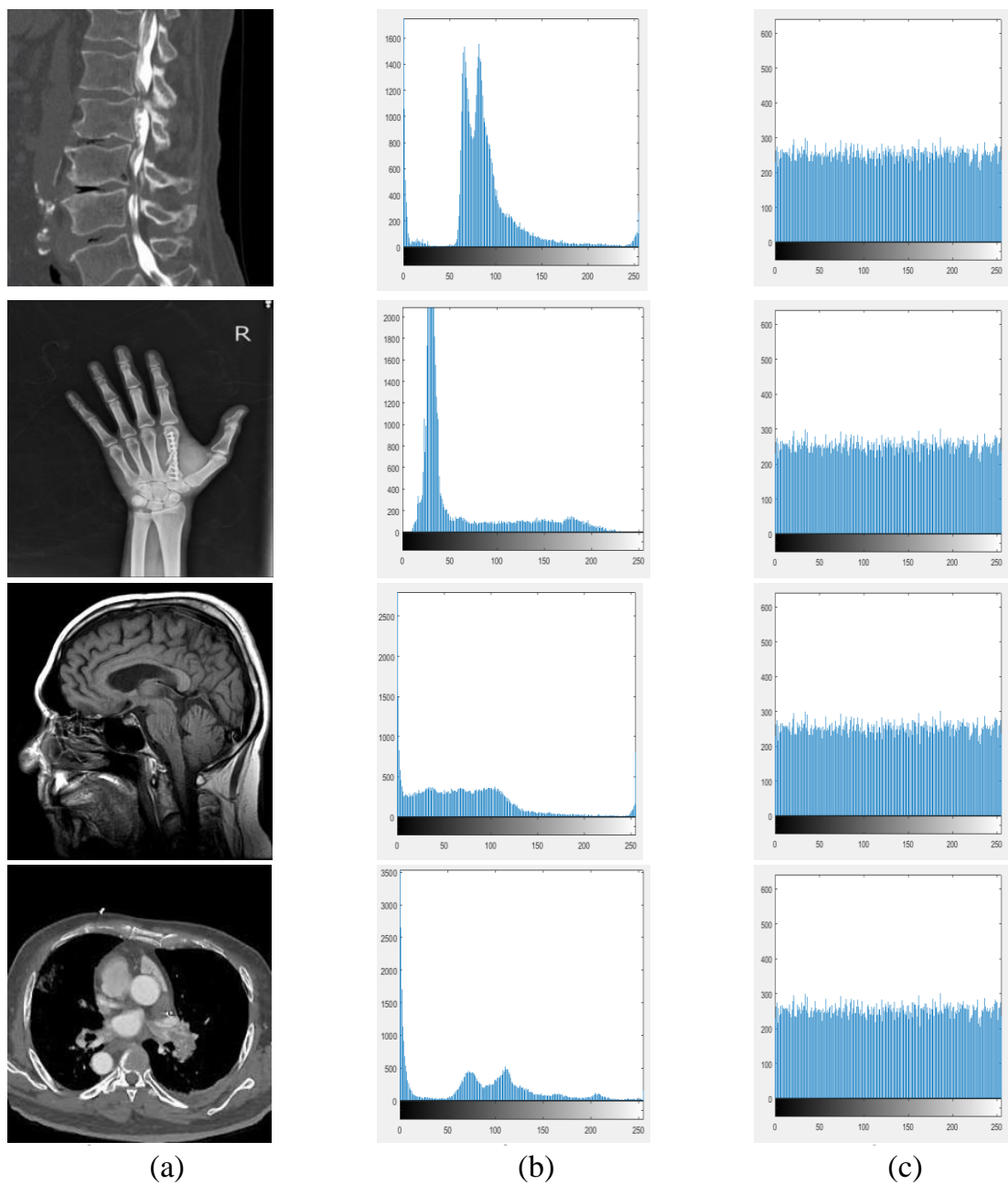


Figure 4.3. (a) Images originales, (b) histogrammes des images originales, (c) histogrammes des images chiffrées.

Chapitre 4 Implémentation et analyses de sécurités

4.5.2. Analyse de l'entropie

L'entropie de Shannon, dû à Claude Shannon, est une fonction mathématique qui correspond intuitivement à la quantité d'information contenue dans une source d'information [27]. Si cette source d'information est une image, l'entropie est utilisée pour caractériser la texture de l'image pour montré le caractère aléatoire des données. La fonction d'entropie est définie comme suit:

$$H(x) = - \sum_{i=1}^n p(i) \log_2 p(i) \quad (4.7)$$

Où :

- $p(i)$ est la probabilité d'apparition d'un niveau d'intensité d'un pixel. $i=0, 1, 2, \dots, N$
- N est le niveau maximum de l'intensité d'un pixel.

Nous avons calculé les entropies des images utilisées pour les tests après le processus de chiffrement (voir Tableau.4.2). On a trouvé que les entropies des images chiffrées sont très proches de la valeur idéale (la valeur idéale est 8).

Test des images	CT rachis lombaire	Radio main droite	Radiographié de pied	radioTélé thorax	IRM encéphalique
Originale	2.6975	5.9224	4.6049	7.7854	6.2746
Crypté	7.9568	7.9584	7.9583	7.9569	7.9564
Test des images	IRM colonne vertébral	CT abdomen	TDM de Crâne	Radiographie cervicale	Echo cœur
Originale	6.2800	5.7055	6.6028	6.8436	4.6036
Crypté	7.9558	7.9560	7.9962	7.9570	7.9563

Tableau 4.2 : les valeurs d'entropies pour différente images originales et cryptées.

Chapitre 4 Implémentation et analyses de sécurités

Remarque : Si l'entropie d'une image chiffrée est significativement moins que la valeur idéale 8, il y'aurait alors une possibilité de prévisibilité qui menace la sécurité de l'image.

Après calculs, les valeurs des entropies obtenues pour les images chiffrées ont une valeur proche de la valeur idéale qui est huit (8), cela implique que la fuite d'informations dans le processus de chiffrement proposé est négligeable et l'algorithme de chiffrement est sécurisé contre les attaques par entropie.

4.5.3. Analyse de la corrélation

Nous savons bien que les pixels adjacents dans une image claire sont fortement corrélés, mais dans une image cryptée par un algorithme de cryptage optimal, ces derniers deviennent faiblement corrélés. Le calcul du coefficient de corrélation entre les pixels adjacents nous donne une idée sur la capacité de notre algorithme de cryptage à résister aux attaques. Les étapes à suivre pour calculer les coefficients de corrélation sont [28] :

- Sélectionner aléatoirement N paires de pixels adjacents (horizontal, vertical ou diagonal), notés (x_i, y_i) , $i = 1, 2, \dots, N$.
- Calculer le coefficient de corrélation de chaque paire en utilisant les formules suivantes :

$$\text{cov}(x, y) = E(x - E(x))(y - E(y)) \quad (4.8)$$

$$r_{xy} = \text{cov}(x, y) / \sqrt{D(x)} \sqrt{D(y)} \quad (4.9)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (4.10)$$

Où : x et y sont les valeurs d'échelle de gris de deux pixels adjacents dans l'image.

Cov (x, y) est la covariance, $E(x)$ est l'espérance mathématique, r_x, y caractérise

l'homogénéité des pixels adjacents et $D(x)$ est la variance.

Chapitre 4 Implémentation et analyses de sécurités

Nous avons sélectionnez au hasard 4096 paires de deux pixels adjacents (horizontal, vertical, diagonal), puis on utilise les formules pour calculer le coefficient de corrélation, pour les comparer avec d'autres méthodes de chiffrement (carte de Cate [24], carte de baker [29], carte standard de Chirikov[30][31]). Les résultats sont présentés dans le tableau 4.3 :

Teste d'image	Direction	Image Originale	Méthode Proposée	carte de cate	Carte de baker	carte standard de Chirikov
TDM de Crâne	Horizontal	0.9430	0.0014	0.0872	0.17115	0.1161
	Vertical	0.9435	0.0010	0.0568	0.1689	0.3717
	Diagonal	0.8958	0.0037	0.07023	0.0036	0.1168
Abdomen CT	Horizontal	0.9691	-0.0023	0.1651	0.2076	0.1304
	Vertical	0.9670	-0.0103	0.1089	0.1413	0.3615
	Diagonal	0.9450	3.7629e-04	-0.1229	0.0534	0.1433
Radio Télé thorax	Horizontal	0.9963	-0.0102	0.273513	0.2310	0.1908
	Vertical	0.9860	-0.0071	0.0925	0.4347	0.5365
	Diagonal	0.9943	0.0040	-0.0652	0.0423	0.1943
IRM colon vertébral	Horizontal	0.9724	-0.0092	0.3207	0.0753	0.0671
	Vertical	0.9859	-0.0065	0.1440	0.4047	0.3144
	Diagonal	0.9630	-0.0024	0.0781	0.0615	0.0716

Tableaux 4.3 Coefficients de corrélation de deux pixels adjacents dans deux images.

Chapitre 4 Implémentation et analyses de sécurités

On peut observer que les images chiffrées obtenues à partir du schéma proposé et les méthodes citées conservent de faibles coefficients (ou pratiquement nulle) de corrélation dans toutes les directions. En comparant les coefficients de corrélation obtenus par la méthode proposée avec ceux calculés avec les autres algorithmes de chiffrements, on peut voir clairement que l'approche proposée surpasse les méthodes évoquées.

Pour plus de détail, les figures ci-dessus représente la corrélation dans toute les directions ; Horizontale, Verticale et Diagonale pour une image en clair et pour une image chiffrée. Il bien remarquable qu'il y a de fortes liaisons entre les pixels adjacents dans l'image en claire et de faibles liaisons dans l'image chiffrée.

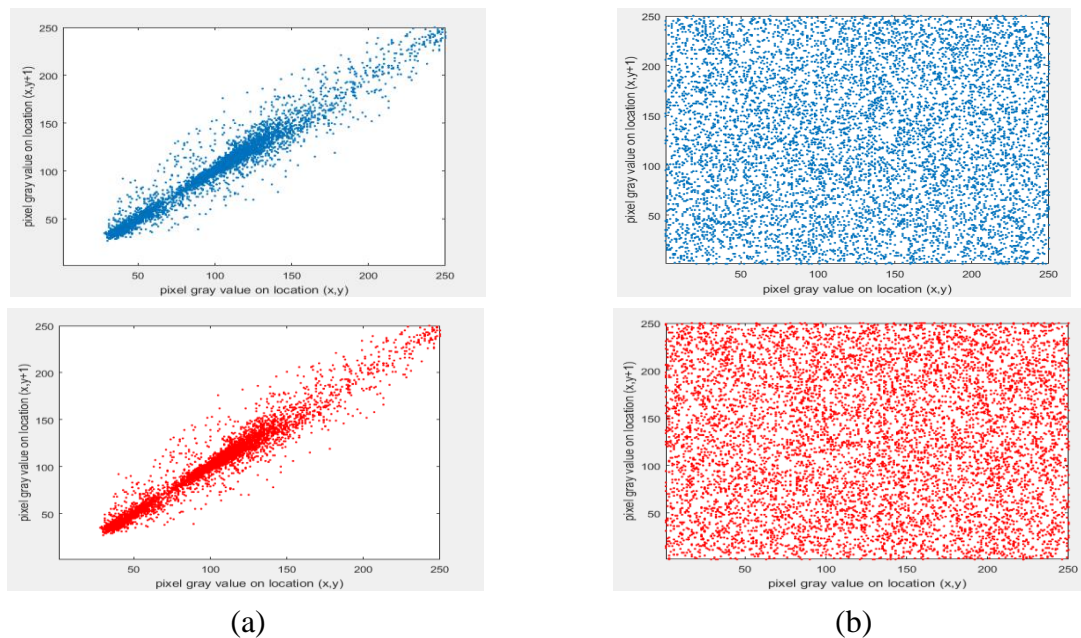


Figure 4.4 Corrélations des pixels adjacents pour l'image d'IRM. (a) : Horizontalement verticalement et en diagonale pour l'image originale. (b) : Horizontalement verticalement et en diagonale pour l'image cryptée.

Chapitre 4 Implémentation et analyses de sécurités

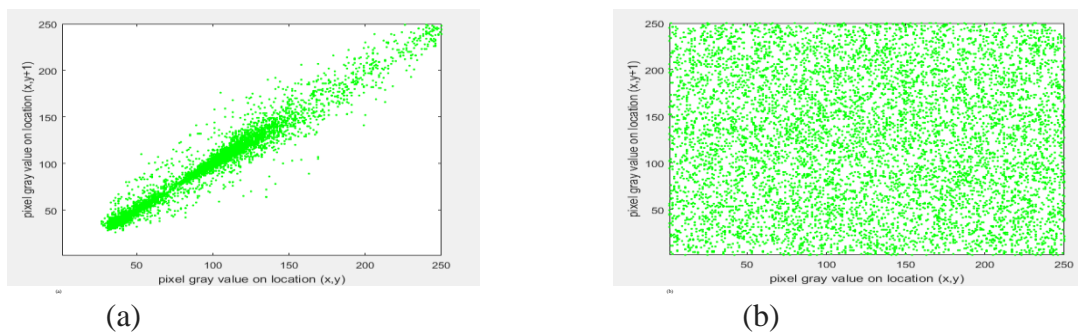


Figure 4.4 (suite) Corrélations des pixels adjacents pour l'image d'IRM. (a) : Horizontalement verticalement et en diagonale pour l'image originale. (b) : Horizontalement verticalement et en diagonale pour l'image cryptée.

4.6. Développement de notre application de cryptage hyper-chaotique

Dans cette section, nous allons présenter une interface graphique de notre cryptosystème.

4.6.1. Langage de développement

Nous avons utilisé Matlab Guide pour l'implémentation de notre application.

Au démarrage, le système affiche l'interface de notre application. Cette interface contient deux panneaux qui sont constitués d'un ensemble de boutons ayant chacun sa fonctionnalité, et deux zone d'affichage (figure 4.5) :

Opération Encrypt : cette fonctionnalité permet aux utilisateurs le cryptage d'images de différents formats JPEG, PNG, TIFF...

Chapitre 4 Implémentation et analyses de sécurités

Opération Decrypt : Cette deuxième fonctionnalité permet aux utilisateurs le décryptage d'images qui sont déjà cryptées avec notre application.

Save : permet de sauvegarder les images.

Quit : permet de sortir de l'application.

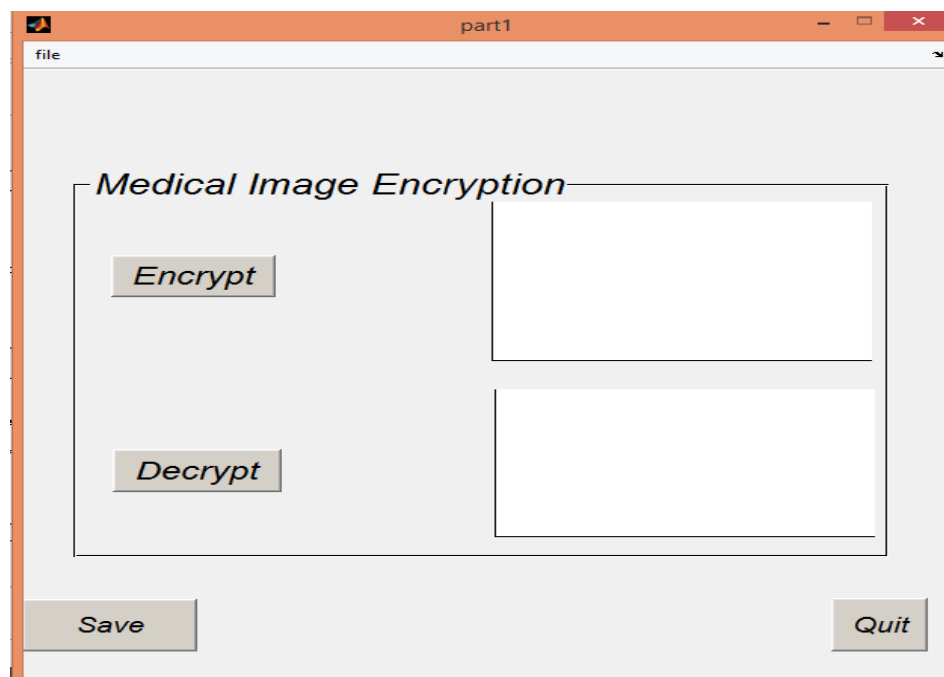


Figure 4.5. Interface générale.

4.6.2. Résultat d'exécution

a. Cryptage/Décryptage des images

Les figures suivantes montrent le résultat d'exécution de notre application :

Chapitre 4 Implémentation et analyses de sécurités

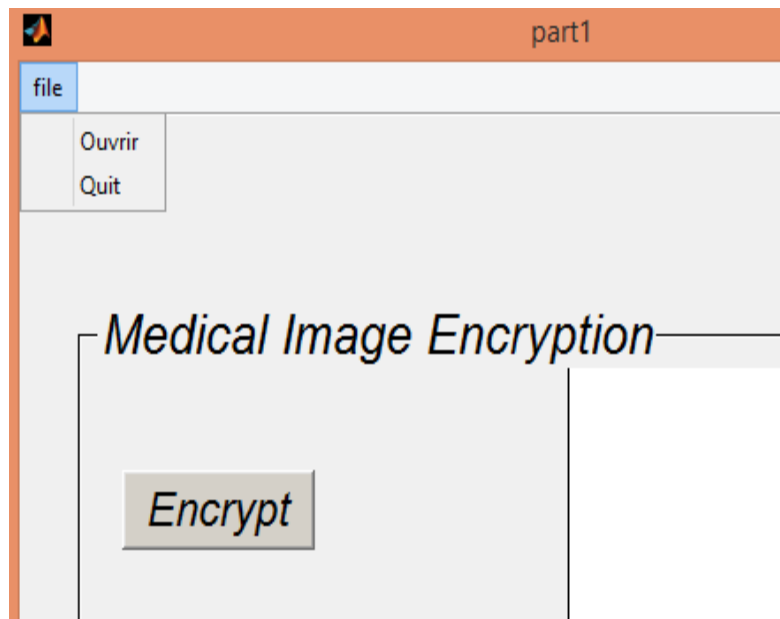


Figure 4.6. Chargement de l'image

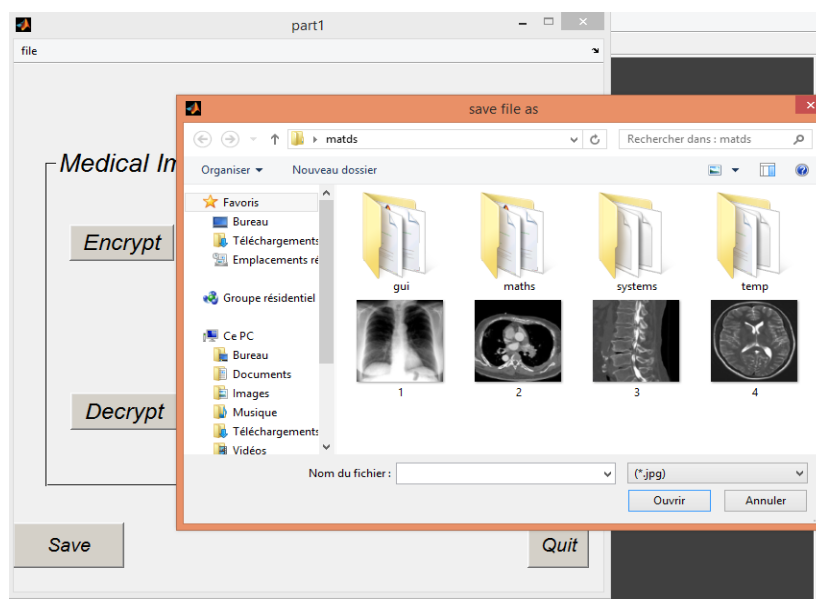


Figure 4.7. Choix de l'image

Chapitre 4 Implémentation et analyses de sécurités

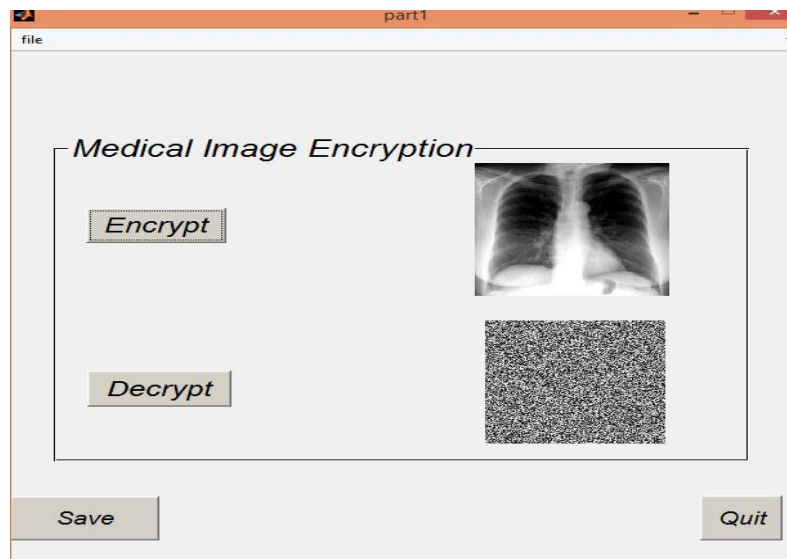


Figure 4.8. Cryptage d'image

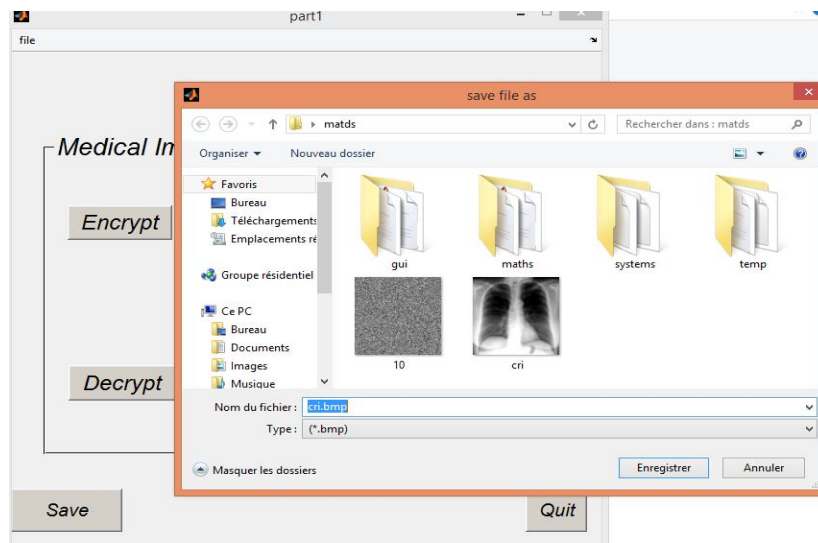


Figure 4.9. Sauvegarde de l'image

Chapitre 4 Implémentation et analyses de sécurités

Le même principe sera utilisé pour le décryptage de l'image en utilisant le bouton decrypt.

4.7. Conclusion

Dans ce chapitre nous avons montré grâce à l'analyse des différents critères de performance que la méthode proposée surpasse les méthodes existantes en ce qui concerne l'efficacité ou l'efficience. Ceci a été obtenu en montrant que les taux du NPCR et UACI sont très proches de l'idéal et que l'espace clé est suffisamment grand, pour rendre une attaque par force brute inefficace. Les analyses statistiques illustrées par l'analyse de l'histogramme, le calcul de l'entropie et des coefficient de corrélation ont montré des performances meilleurs pour le cryptage appliqué en imagerie médicale et en télémédecine. Nous avons par la suite réalisé une interface graphique appliquée à notre crypto-système

Conclusion générale

Dans ce mémoire, nous avons étudié et réalisé un crypto-système à l'aide de systèmes chaotique basé sur le principe de permutation diffusion, pour chiffrer les images médicales.

Le premier chapitre a été consacré à l'étude des systèmes dynamiques chaotiques. Leurs principales caractéristiques ont été décrites en mettant en évidence l'intérêt du calcul des exposants de Lyapunov ainsi que les différents scénarios possibles de transition vers le chaos. Nous avons par la suite décrits quelque exemple de systèmes dynamiques chaotiques discret et continu. Dans le deuxième chapitre, nous avons étudié et analysé les principales caractéristiques (point fixe, exposants de Lyapunov, attracteur, bifurcation,...) du système hyper-chaotique de Chen ainsi que ses différents comportements en fonction de la variation de ses paramètres, grâce aux différentes simulations effectuées. Nous avons ainsi ajusté les paramètres du système de Chen afin d'obtenir un comportement hyper-chaotique.

Dans le troisième chapitre, nous avons proposé et étudié un crypto-système basé sur le chaos (fonction Logistique) et l'hyper-chaos (système de Chen). A ce sujet, nous avons présenté quelques notions et rappels concernant la cryptographie ainsi que la relation qui la relie avec le chaos. Ensuite, nous avons exposé les principales fonctionnalités utilisées dans notre algorithme de chiffrements d'image médicales , à savoir la confusion , la diffusion et la génération des clés de chiffrement , en utilisant la fonction Logistique pour la confusion et le système hyper-chaotique de Chen pour la diffusion ,ainsi que la possibilité d'intégration de notre crypto-système dans un système de télé-radiologie. Dans le dernier chapitre, les résultats expérimentaux, tels que l'analyse différentielle, l'analyse de sensibilité de la clé de chiffrement, l'espace clé de chiffrement, et d'autres analyses appelées analyses statiques, tel que l'analyse d'histogramme, l'analyse d'entropie et de corrélation, nous ont montré que l'algorithme proposé offre une sécurité optimale, ainsi que l'implémentation de notre crypto-système s'intègre parfaitement dans les applications de télémédecine.

Conclusion générale

La contribution principale de ce travail a été le développement d'un algorithme de chiffrement pour une transmission sécurisée des images médicales grâce aux phénomènes de confusion et de diffusion, généré à base de système chaotique et hyper-chaotique.

Le travail réalisé dans ce mémoire ne constitue pas une fin en soi, mais s'ouvre vers des contributions futures. Plusieurs perspectives peuvent être envisagées, à savoir :

- L'emploi d'autres systèmes chaotiques que ceux utilisés dans notre projet à savoir la carte logistique et le système hyper-chaotique de Chen.
- L'intégration d'un système de compression, afin de réduire les coûts de stockage et augmenter la vitesse de transmission, sans altérer la qualité.

- [1] Organisation mondiale de la Santé, 'Règlement sanitaire international', OMS, 2005.
- [2] A .Ikhelif , 'Contrôle,Chaotification et Hyper-chaotification des systèmes dynamique',
Thèse de magister de l'université de Constantine, 2007.
- [3] L.M.Chikhi, 'Application des systèmes dynamiques chaotiques en transmission de données',
Thèse de magister de l'université de Blida 1, 2012.
- [4] V.Huyen et D.Claudine , 'Bifurcation et Chaos : Une introduction à la dynamique
contemporaine', Ellipses, 2000.
- [5] O.Megherbi , 'Etude et réalisation d'un système sécurisé a base de systèmes chaotique',
Thèse de magister de l'université de Mouloud Mammeri Tizi-Ouzou,2013.
- [6] M.Hernault , 'Faisabilité d'un système d'émission-réception analogique pour les
communications sécurisées par le chaos ', Thèse de doctorat de l'université de Paris
6,France, 2007.
- [7] I. Talbi , 'Systèmes dynamique non linaires et phénomène du chaos ',Thèse de magister en
mathématique, Université Mantouri de Constantine, 2010.
- [8] A.Floriane , 'Les systèmes dynamiques chaotiques pour le chiffrement, synthèse et
cryptanalyse.Automatique / Robotique ', Université Henri Poincaré - Nancy I,France, 2006.
- [9] Tanguy .L, ' Grandes déviations d'exposants de Lyapunov dans les systèmes étendus ',
Thèse de doctorat de l'université de Paris 7,France, 2015.
- [10] A.Habri , 'Un Système D'indexation et Recherche D'image Par Le Contenu Basee Sur La
Classification',These de master de l'université de Larbi Ben M'hidi Oum El Bouaghi,2011.
- [11] A.Kihal , 'Systemes chaotique pour la transmission sécurisée de données', Thèse de
magister de l'université de Mohamed Khider Biskra ,2013.
- [12] L.Minh , 'Modélisation et Optimisation non convexe basées sur la programmation DC et
DCA pour la résolution de certaines classes des problèmes en Fouille de Données et
Cryptologie', Thèse de Doctorat de l'université de Paul Verlaine-Metz,France, 2007.
- [13] R. Dumont , 'Cryptographie et Sécurité informatique', Cours de l'université de
Liège,Belgique, 2009 – 2010.

- [14] N.Mahammedi et H.Mahdadi , 'Implémentation de benchmark d'opérations crypto basées ECC pour l'étude et comparaison de courbes elliptiques', mémoire master académique de l'université Kasdi Merbah, Ouargla, 2013.
- [15] D.Muler, 'Petite histoire de la cryptologie'.Disponible sur : <https://www.apprendre-en-ligne.net/crypto/histoire/index.html> (visité le 15/04/2019).
- [16]L.Shalala,'Cryptographie'.29/12/2012.Disponiblesur , <https://sites.google.com/site/steganographie-cryptographie/ii-utilisation-de-la-cryptographie/1-differents-formats-de-cryptages>(visité le 15/042019).
- [17] L.Kocarev et S.Lian , 'Chaos-based cryptography: Theory, algorithms and applications', Springer. Vol. 354,2011.
- [18] L.Shujun ,'Analyses and new designs of digital chaotic ciphers'.Thèse de l'université de Xi'an Jiaotong ,Chine,2003.
- [19] F.Hernandez et B.amalia , 'Cryptanalysis of a Classical chaos-based cryptosystem with some quantum cryptography features ', International Journal of Bifurcation and Chao, World Scientific Publishing Company, Espagne ,2016.
- [20] K.Ahmad , 'Protocoles, gestion et transmission sécurisée par chaos des clés secrètes',these de doctorat ,université de Nante Angers Le Mans ,France,2015.
- [21] Matthews,R. (1984). On the derivation of a "Chaotic" encryption algorithm. Cryptologia, 8(1), 29-41.
- [22] E.Bensikkadour , 'Développement d'un crypto-système basé sur le standard AES et la théorie du chaos pour le chiffrement des images satellitaires à bord d'un satellite d'observation de la terre', Thèse de doctorat de l'université de Sidi Bel Abbes.2018.
- [23] J.Fridrich , 'Symmetric ciphers based on two-dimensional chaotic maps', International Journal of Bifurcation and Chao, World Scientific Publishing Company, Vol 8 ,1259-1284,1998.
- [24] Y.Cherfa , 'Traitement d'image',cours de l'université de Blida 1,2017-2018.
- [25] G. Chen, Y. Mao, & C. Chui , 'A symmetric image encryption scheme based on 3D chaotic cat maps ', ' Chaos,solution & fractals, elsevier, vol 21, 749-761, 2004.

- [26] W.Yue et J.Noonan, 'NPCR and UACI Randomness Tests for Image Encryption ', Journal of selected Areas in Telecommunication , April Edition, 2011.
- [27] D.Goumidi , 'Fonction logistique et standard chaotique pour le chiffrement des images satellitaires',These de magister, Université Mentouri de Constantine,2010.
- [28] C.Merdjal et A.Merakchi ,'Cryptage d'image par un signal unidimensionnel quelconque',These de master, Université Larbi Ben M'hidi Oum El Bouaghi,2018.
- [29] Z. Amrani, S Chitroub et A. Boukhari , ' Cryptage d'Images par Chiffrement de Vigenère Basé sur le Mixage des Cartes Chaotiques, 4th International Conférence on Computer Integrated Manufacturing,Algérie , 2007.
- [30] A.Lini et D.Neenu , 'Secure Image Encryption Algorithms', International journal of scientic & technology research ,issue, Volume 2, avril 2013.
- [31] V.Patidar et N.Pareek , 'A new substitution-diffusion based image cipher using chaotic standard and logistic maps', Commun Nonlinear Sci Numer Simul, 2009.
- [32] Y. Wang, K. Wong , X.Liao, G.Chen et T.Xiang , ' A chaos-based image encryption algorithm with variable control parameters'. Chaos Solitons Fractals,41, 1773–1783.