الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي والبحث العلمي

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED SEDDIK BENYAHIA JIJEL

Faculté des sciences et de la technologie

Département d'Electronique

N° :……/2023

MEMOIRE DE MASTER

DOMAINE: Sciences et Technologies

FILIERE: Télécommunications

SPECIALITE: Systèmes des télécommunications

Thème

Cryptage des images médicales par tatouage

Présenté Par : Boukhari Cherifa **Encadré Par : Dr.Kemih Karim**

Labreche Marwa

Date de soutenance: 25/06/2023

Jury de Soutenance

Président : Dr.Tekkouk Omar	**Univ MSB jijel**
Encadreur : Dr.Kemih Karim	**Univ MSB jijel**
Examinateur : Dr.Messadi Manel	**Univ MSB jijel**

Promotion : 2022 /2023

Remerciements

Au terme de ce travail, nous voudrions d'abord remercier Allah de nous avoir donné la santé et la volonté dans la réalisation de ce projet.

Nous tenons à remercier particulièrement et chaleureusement notre encadrant, **Mr KEMIH Karim**, *pour son encadrement, sa patience, ses conseils très judicieux, ses encouragements et sa disponibilité tout au long de notre projet.*

Nous exprimons toute notre gratitude aux membres du jury pour avoir accepté de juger notre travail, ainsi que tous les enseignants du département d'électronique.

Dédicace

À mes chers parents, mon soutien inconditionnel, ma source d'inspiration,

Papa et Mama, vous êtes les piliers solides qui m'ont guidé tout au long de ce parcours académique. Votre amour, votre encouragement et votre dévouement ont été les fondations sur lesquelles j'ai construit mes réussites. Votre confiance en moi m'a toujours poussé à donner le meilleur de moi-même, et pour cela, je vous suis infiniment reconnaissante.

À mes sœurs : Lwiza, Faiza et Nahla.

À mes frères : Zahre Eddine, Mohamed et le petit Sami.

À mon beau frère Mouataz.

Vous êtes mes compagnons de vie, mes alliés et mes meilleurs amis. Votre présence, votre soutien et votre amour inconditionnel sont une bénédiction que je chéris chaque jour.

À mon binôme Cherifa, partenaire précieuse de cette aventure académique.

À mes amies : Nada et Sana présentes dans les bons moments comme dans les difficultés.

À tous mes camarades de la promo Systèmes des Télécommunications.

Merci du fond du cœur pour tout ce que vous avez fait et continuez de faire. Ce mémoire est dédié à vous, en signe d'amour, de reconnaissance et de gratitude éternelle.

Marwa

Dédicace

À ma chère mère, mon pilier de force, tu as été ma source de réconfort et ma plus grande admiratrice. Tes encouragements sans faille m'ont donné la confiance nécessaire pour persévérer.

À mon cher père, ma source d'inspiration, ton dévouement à l'excellence et ta sagesse m'ont motivé à poursuivre mes aspirations académiques. Tes conseils avisés ont guidé chacune de mes décisions.

À ma sœur Meriem, ma confidente fidèle, tu as toujours été là pour moi, prête à écouter et à m'apporter ton soutien inconditionnel. Ta présence précieuse a été mon ancre dans les moments de doute.

À mon frère Oussama, mon complice de toujours, ton amour, ton soutien indéfectible et ta présence ont été mes moteurs et mes sources de courage.

À mon binôme Marwa, partenaire précieuse de cette aventure académique.

À mes amies : Cheima, Fatiha, Maroua, Hadjer, Amani…, présentes dans les bons moments comme dans les difficultés.

À tous mes camarades de la promo Systèmes des Télécommunications.

Merci du fond du cœur pour tout ce que vous avez fait et continuez de faire. Ce mémoire est dédié à vous, en signe d'amour, de reconnaissance et de gratitude éternelle.

Cherifa

Résumé :

La sécurité des images médicales est une préoccupation essentielle dans le domaine de la santé, en particulier lorsqu'il s'agit de les partager à distance. L'objectif de ce mémoire consiste à proposer un nouvel algorithme de cryptage des images médicale en utilisant le tatouage en ondelette ainsi que le chaos. Les résultats de simulation obtenus montrent l'efficacité et la fiabilité de la technique proposée.

Mots clés : Système chaotique, sécurisation des données, cryptage, chiffrement, tatouage, ondelette.

ملخص :

أمان الصور الطبية هو قلق أساسي في مجال الرعاية الصحية، خاصة عندما يتعلق الأمر بمشاركتها عن بُعد. هدف هذه الأطروحة هو اقتراح خوارزمية جديدة لتشفير الصور الطبية باستخدام تقنية الوترة الموجية والفوضى. أظهرت نتائج المحاكاة فعالية وموثوقية الطريقة المقترحة.

كلمات مفتاحية : نظام فوضوي، تأمين البيانات، تشفير، وشم، أمواج.

Abstract :

The security of medical images is a crucial concern in the healthcare field, especially when it comes to remote sharing. The objective of this dissertation is to propose a new algorithm for encrypting medical images using wavelet-based watermarking and chaos. Simulation results have demonstrated the effectiveness and reliability of the proposed technique.

Keywords: Chaotic system, data security, encryption, watermarking, wavelet.

Sommaire

Chapitre 2 : Etat de l'art sur la sécurisation des données médicales

Chapitre 3 : Tatouage en ondelette

Chapitre 4 : Résultats de simulation

Liste des figures

Chapitre 1 : Etat de l'art du chaos

Chapitre 3 : Tatouage en ondelette

Chapitre 4 : Résultats de simulation

Liste des tableaux

Chapitre 1 : Etat de l'art du chaos

Chapitre 2 : Etat de l'art sur la sécurisation des données médicales

Introduction générale

Introduction générale

Le domaine des images médicales est en constante évolution et joue un rôle essentiel dans le diagnostic, le suivi et le traitement des patients. Cependant, avec la numérisation croissante des images médicales et leur transmission à travers des réseaux informatiques, la sécurité et la confidentialité de ces données sont devenues une préoccupation majeure. Les images médicales, telles que les radiographies, les IRM (Imagerie par Résonance Magnétique), les scanners et autres, contiennent des informations sensibles sur les patients et nécessitent une protection adéquate contre les accès non autorisés.

La théorie du chaos a vu le jour à partir de 1960 grâce aux travaux de nombreux chercheurs, en particulier ceux de Lorenz, et a connu un développement mathématique suivi d'une expansion scientifique significative. Les systèmes chaotiques sont des systèmes déterministes non linéaires qui présentent des caractéristiques importantes telles que l'aspect aléatoire, la sensibilité aux conditions initiales, la sensibilité aux variations des paramètres et un comportement imprévisible dans le temps. Ces propriétés rendent les systèmes chaotiques extrêmement intéressants dans le domaine du cryptage des données.

Le cryptage est une méthode couramment utilisée pour sécuriser les données en les rendant illisibles pour les personnes qui n'ont pas les clés de déchiffrement appropriées [1-8]. Cependant, le cryptage traditionnel des images médicales présente des limitations, notamment en termes de capacité de stockage et de temps de traitement. Ces contraintes peuvent avoir un impact négatif sur l'efficacité et la rapidité des systèmes d'imagerie médicale.

Le tatouage a émergé comme une approche prometteuse pour sécuriser les données sans altérer de manière significative la qualité et la précision des images [11-12].

Le tatouage en ondelette est basé sur l'utilisation de la transformée en ondelettes, une méthode mathématique puissante pour analyser et représenter les images. Cette approche consiste à intégrer des informations de sécurité directement dans les coefficients d'ondelettes de l'image. Les informations de tatouage sont insérées de manière robuste et invisible.

L'objectif de ce mémoire de fin d'étude est d'explorer les techniques de cryptage des images médicales par tatouage en ondelette. Nous nous concentrerons sur l'utilisation de la transformée en ondelettes pour intégrer des informations de sécurité directement dans les coefficients d'ondelettes de l'image. Des expérimentations seront menées sur des ensembles de données d'images médicales réelles afin de démontrer l'efficacité et la fiabilité de ces techniques

de cryptage par tatouage en ondelette. Les résultats de cette recherche contribueront à renforcer la sécurité des images médicales tout en préservant leur qualité et leur précision.

Dans le but de contribuer à la sécurisation des images médicales, nous avons réalisé ce modeste travail qui s'articule sur quatre chapitres :

Le premier chapitre aborde des généralités et notions de base sur les systèmes chaotiques ainsi que leurs caractéristiques.

Le deuxième chapitre souligne les défis, les progrès et les meilleures pratiques liés à la sécurisation des données médicales. En comprenant les problématiques actuelles et en mettant en place des mesures de sécurité appropriées.

Le troisième chapitre fournie une compréhension approfondie du concept de tatouage en ondelette appliqué aux images médicales.

Le quatrième chapitre est consacré aux résultats de simulations réalisées sous MATLAB 2016. Nous explorerons le processus de cryptage/décryptage d'images en utilisant des algorithmes de chiffrement/déchiffrement. Nous discuterons de la technique de tatouage d'images médicales pour marquer et protéger les images numériques. Enfin, nous étudierons la transformée en ondelettes de Haar, une méthode de décomposition des images en différentes échelles de résolution.

Enfin, on termine par une conclusion générale.

Chapitre 1

- Etat de l'art du chaos

1.1 Introduction

Au début du 20ème siècle, l'histoire récente des systèmes dynamiques a été marquée par les travaux d'Henri Poincaré. Il a apporté d'importantes contributions à l'étude qualitative des systèmes dynamiques en proposant une approche basée sur l'analyse des points d'équilibre, des trajectoires périodiques et de leurs bassins d'attraction. Plutôt que de chercher des solutions analytiques exprimées par des formules, il a développé des méthodes qualitatives pour comprendre le comportement de ces systèmes. En effet, pour la plupart des systèmes non linéaires, il est impossible de trouver de telles solutions analytiques.

Par la suite, dans les années 60, Edward Lorenz a présenté le premier exemple d'un système d'équations différentielles simplifiées à seulement trois variables, permettant de décrire l'évolution de masses d'air. La nature des solutions de ce système est complexe, ce qui en fait le premier exemple d'un système chaotique [1].

1.2 Définitions

1.2.1 Système dynamique

Un système dynamique désigne un ensemble mécanique, physique, économique, environnemental ou d'autres domaines dans lequel l'état du système (représenté par un ensemble de grandeurs suffisantes pour le caractériser) évolue au fil du temps [2]. Pour étudier cette évolution d'un système, il est nécessaire de prendre en compte deux éléments :

- Son état initial, c'est-à-dire son état à l'instant t0.
- Sa loi d'évolution, qui décrit comment le système se transforme au cours du temps.

1.2.1.1 Système dynamique à temps continu

Un système dynamique dans un temps continu est représenté par un système d'équations différentielles de la forme :

$$X_t^{\cdot} = f(x,t,p). \tag{1.1}$$

Où $x \in R^n$ *et* $p \in R^r$ où $f : R^n \times R^+ \to R^n$ désigne la dynamique du système [3].

1.2.1.2 Système dynamique à temps discret

Un système dynamique dans le cas discret est représenté par une application (fonction itérative) [3] sous la forme :

$$X_{k+1} = f(x_k, p)\ ,\ \ x_k \in R^n \qquad et \qquad p \in R^r, k = 1,2,3... \qquad (1.2)$$

Où $f : R^n \times Z^+ \to R^n$ indique la dynamique du système en temps discret.

1.2.2 Système autonome ou non autonome

Lorsque le champ de vecteurs f est indépendant du temps, le système (1.1) est considéré comme autonome, et dans ce cas, il peut être écrit comme suit.

$$\dot{X} = f(x, p). \qquad (1.3)$$

Dans le cas contraire on dira qu'il est non autonome. Cependant, en effectuant un changement de variable approprié, il est possible de transformer facilement un système non autonome de dimension n en un système autonome équivalent de dimension n+1 [3].

1.2.3 Système chaotique

La théorie du chaos est une théorie scientifique qui étudie le comportement des systèmes dynamiques sensibles aux conditions initiales. Les systèmes chaotiques sont caractérisés par des trajectoires qui évoluent dans une région bornée et qui présentent un caractère stable sans convergence vers un point fixe ou un cycle limite. Ces trajectoires restent denses dans la région et sont très sensibles aux conditions initiales [4]. Les solutions des équations différentielles non linéaires qui décrivent les systèmes chaotiques ne peuvent généralement pas être calculées de manière analytique, sauf pour certaines classes particulières d'équations [5].

Par conséquent, ces solutions sont souvent déterminées numériquement et le comportement du système est analysé par simulation.

1.3 Propriétés du système chaotique

Il existe plusieurs définitions possibles du chaos. Ces définitions ne sont pas toutes équivalentes, mais elles convergent vers certains points communs caractérisant le chaos [6].

Les caractéristiques des systèmes chaotiques sont [7] :

- Non-linéarité
- Déterminisme
- Aspect aléatoire
- Sensibilité aux conditions initiales
- Notion d'attracteur

- Exposants de Lyapunov
- Diagramme de bifurcation

1.3.1 Non-linéarité

Un système chaotique est un système dynamique non linéaire. Un système linéaire ne peut pas être chaotique.

Pour un système dynamique non linéaire, les propriétés de stabilité deviennent plus complexes par rapport au cas linéaire. La présence de non-linéarités peut entraîner l'émergence de plusieurs caractéristiques, telles que les cycles limites ou le phénomène du chaos. Il est important de noter que la non-linéarité est une condition nécessaire, mais pas suffisante, pour que le chaos se produise.

Donc le comportement chaotique doit venir d'un système non linéaire, mais la non-linéarité n'implique pas nécessairement le chaos [8].

1.3.2 Déterminisme

Un système déterministe est un système qui réagit toujours de la même manière à un événement, ce qui signifie que son évolution sera identique à partir d'un état donné, indépendamment des événements passés. Le système chaotique a des règles fondamentales déterministes et non probabilistes [9].

1.3.3 Aspect aléatoire

L'aspect aléatoire implique que tout système chaotique évolue de manière non périodique et imprévisible [10]. Les Figures 1.1 - 1.3 illustrent l'aspect aléatoire des systèmes de Lorenz, Hénon et Rössler, respectivement.

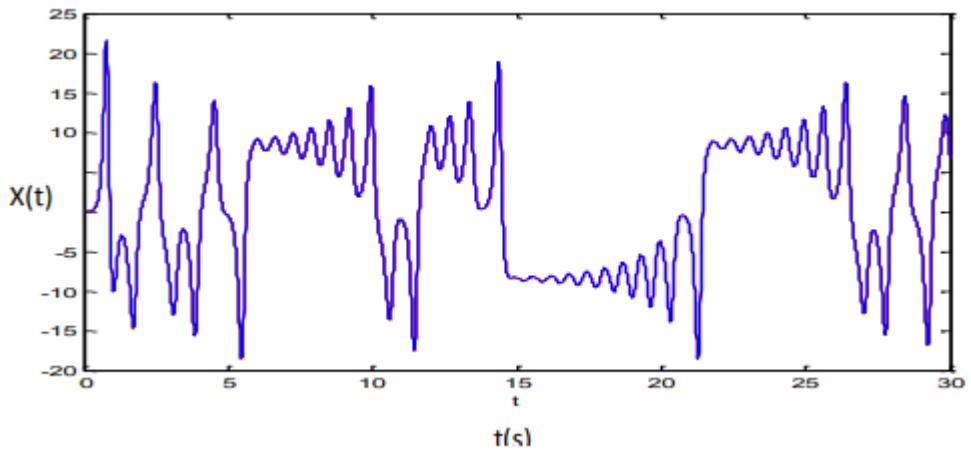


Figure 1.1 : Aspect aléatoire du système de Lorenz.

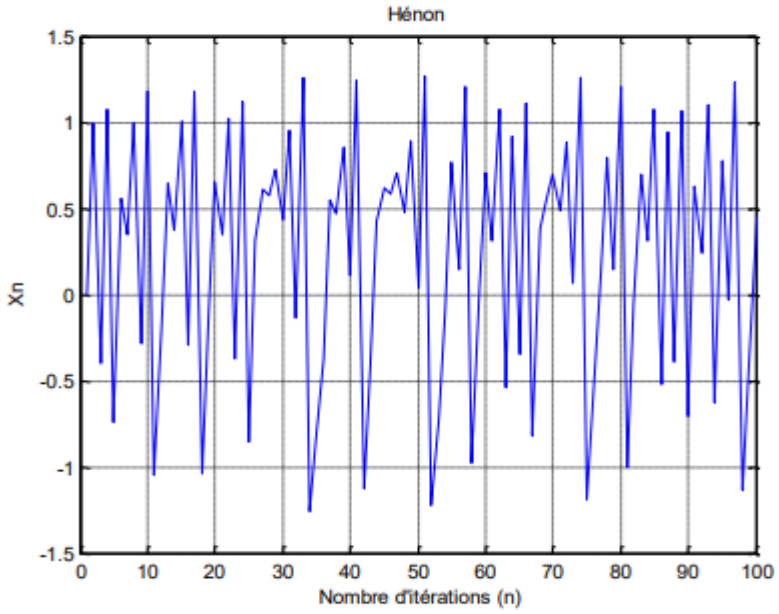


Figure 02 : Aspect aléatoire du système de Hénon.

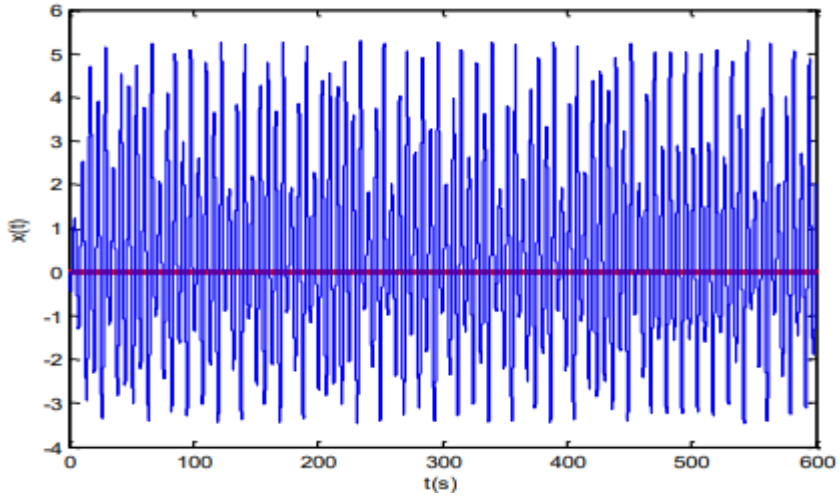


Figure 1.3 : Aspect aléatoire du système de Rössler.

1.3.4 Sensibilité aux conditions initiales

La sensibilité aux perturbations est une caractéristique bien connue des systèmes chaotiques. L'évolution du comportement de ces systèmes est imprévisible en raison de leur grande sensibilité aux conditions initiales. Même une petite erreur dans la connaissance de l'état initial dans l'espace des phases peut entraîner une augmentation significative de cette erreur [11].

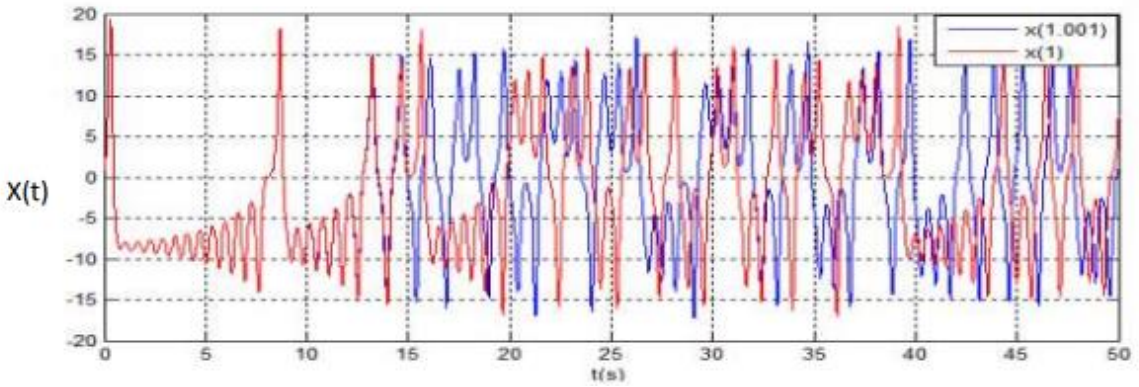


Figure 1.4 : Sensibilité aux conditions initiales du système de Lorenz [10].

1.3.5 Notion d'attracteur

Les systèmes chaotiques possèdent une structure géométrique particulière appelée l'attracteur étrange [12], caractérisé par :

- Un volume
- Une dimension souvent fractale (non entière).
- Une séparation exponentiellement rapide de trajectoires initialement proches.

1.3.6 Exposants de Lyapunov

L'exposant de Lyapunov est utilisé pour évaluer la stabilité d'un système et pour quantifier la sensibilité aux conditions initiales d'un système chaotique. [13].

L'évolution chaotique d'un système est complexe car les trajectoires sur l'attracteur divergent rapidement. Afin de comprendre ce phénomène, il est utile de mesurer ou d'estimer la vitesse de divergence ou de convergence. Cette vitesse est quantifiée par l'exposant de Lyapunov, qui représente le taux de séparation de deux trajectoires initialement très proches dans le plan de phase [14].

Ainsi, si deux trajectoires sont initialement séparées par un certain taux Z1, l'exposant de Lyapunov permet de déterminer comment cette séparation évoluera au fil du temps.

Tableau 1 : Attracteurs et exposants de Lyapunov [13].

Etat	Attracteur	Dimension	Exposants de Lyapunov
Point d'équilibre	Point	0	$\lambda n \leq ... \leq \lambda 1 \leq 0$
Périodique	Cercle	1	$\lambda 1 = 0$; $\lambda n \leq ... \leq \lambda 2 \leq 0$
Périodique d'ordre 2	Tore	2	$\lambda 1 = \lambda 2 = 0$; $\lambda n \leq ... \leq \lambda 3 \leq 0$
Périodique d'ordre K	K-Tore	K	$\lambda 1 = ... = \lambda k = 0$; $\lambda n \leq ... \leq \lambda k+1 \leq 0$
Chaotique		Non entier	$\lambda 1 > 0$; Pn i=1 $\lambda i < 0$
Hyper chaotique		Non entier	$\lambda 1 > 0, \lambda 2 > 0$; Pn i=1 $\lambda i < 0$

Divergent après un temps $\Delta t = t2 - t1$ vers Z2 tel que :

$$|Z2| \approx exp(\lambda.\Delta t)|Z1|. \quad (1.4)$$

Où λ est l'exposant de Lyapunov.

Dans le cas d'un attracteur non chaotique, les exposants de Lyapunov sont tous inférieurs ou égaux à zéro, et leur somme est négative. En revanche, pour un attracteur étrange ou chaotique, il y aura au moins trois exposants de Lyapunov, dont au moins un sera positif. Le tableau suivant permet de classer les attracteurs en fonction de leurs propriétés de stabilité et de sensibilité aux conditions initiales [13].

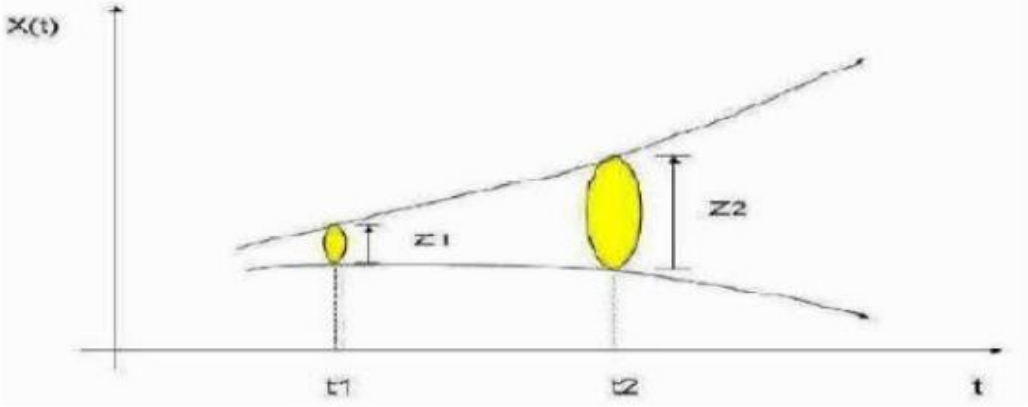


Figure 1.5 : Divergence de deux trajectoires dans le plan de phase [15].

1.3.7 Diagramme de bifurcation

L'évolution du point fixe au chaos n'est pas progressive, mais plutôt caractérisée par des changements marqués. Ces changements sont appelés bifurcations [16].

Une bifurcation représente une transition soudaine du système dynamique vers un autre système possédant des qualités différentes. Le diagramme de bifurcation est un outil graphique qui permet de représenter l'espace des paramètres où les points de bifurcation se situent. Il offre une visualisation plus claire de l'évolution d'un système vers le chaos en fonction de ses paramètres [14].

1.4 Caractéristiques chaotiques de la fonction logistique

La Figure 1.6 illustre la sensibilité d'un système à de très petits changements dans sa condition initiale. On peut clairement observer que les réponses du système sont totalement différentes selon ces changements minimes.

Dans le cas de la Figure 1.7, lorsque les valeurs r = 2.8 et $x0$ = 0.04 sont prises, la suite $\{xn\}$ converge rapidement vers la valeur fixe représentée dans la Figure 1.7(a). La Figure 1.7(b) présente la représentation géométrique de cette suite dans le plan (xn, xn+1) [17].

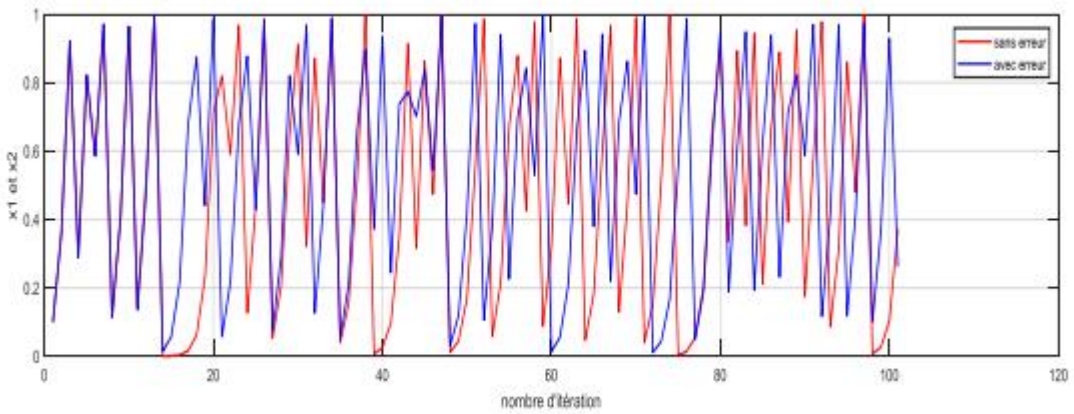


Figure 1.6 : Sensibilité aux conditions initiales d'une carte logistique, erreur 0.0001.

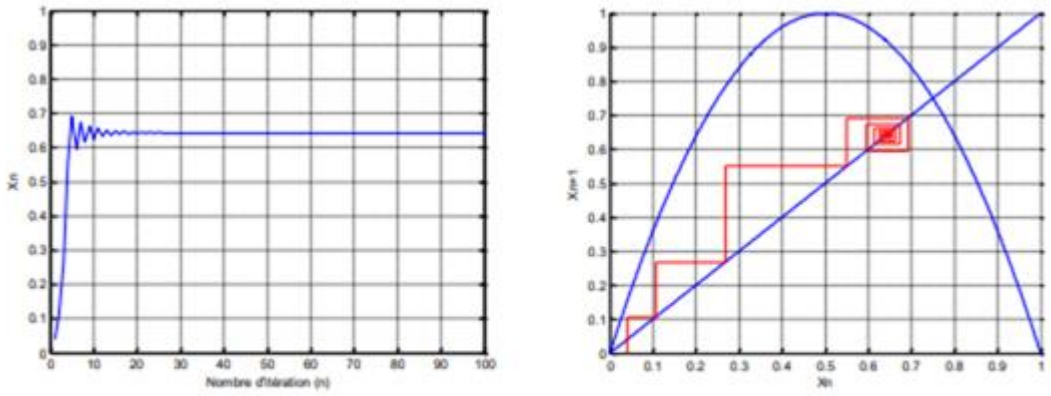


Figure 1.7 : Evolution de la suite {xn} pour r = 2.8 et x0 = 0.04.

La Figure 1.8 présente l'évolution de la suite $\{xn\}$ lorsque r = 3.2. En gardant les mêmes valeurs initiales que dans le cas précédent, la suite converge vers une solution périodique composée de deux points. On peut dire que la trajectoire converge vers un cycle d'ordre 2.

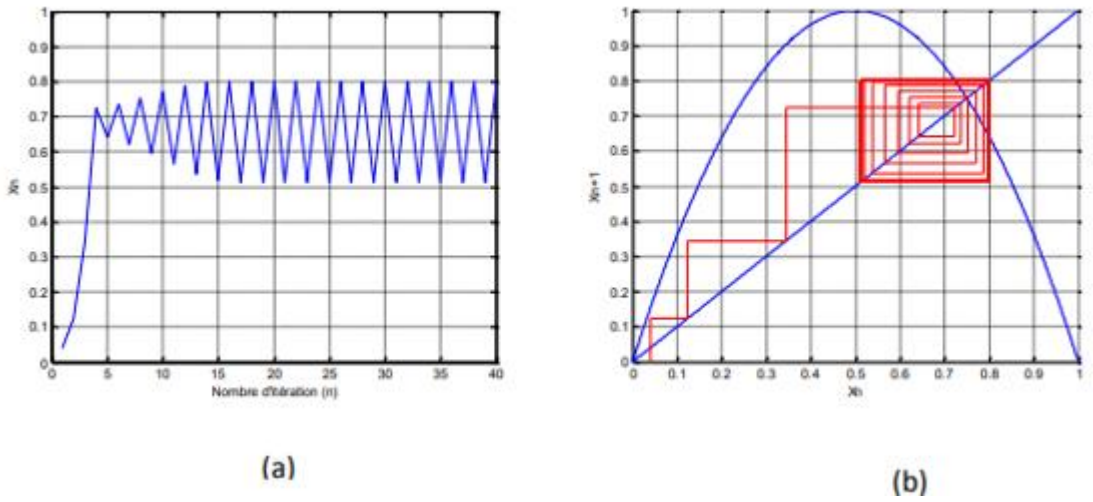


Figure 1.8 : Evolution de la suite {xn} pour r = 3.2 et x0 = 0.04.

Dans la Figure 1.9, on observe l'évolution de la suite dans le cas où r est égal à 4. Contrairement aux exemples précédents, la suite ne converge ni vers un point fixe, ni vers une solution périodique. Au lieu de cela, le système décrit par la transformation logistique se trouve dans un régime chaotique.

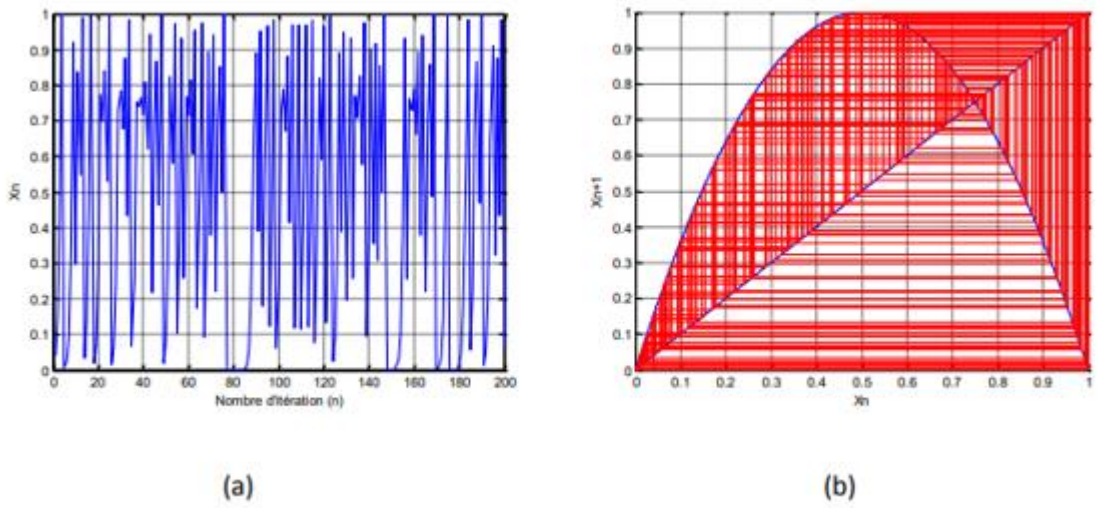


Figure 1.9 : Evolution de la suite {xn} pour r = 4 et x0 = 0.04.

Interprétation

Ce comportement varie considérablement en fonction de la valeur de r et de la valeur initiale $x0$ de la séquence $\{xn\}$. Lorsque la condition initiale $x0$ est modifiée, la séquence converge toujours vers un cycle d'ordre 2, mais la vitesse de convergence diffère.

Il a été montré que pour la valeur critique rc=3.56996, la suite $\{xn\}$ ne présente plus une structure ordonnée : la suite ressemble à une boucle d'ordre infini. De plus, chaque valeur de $x0$, correspond à une séquence différente. Pour la valeur de $r < rc$, la suite converge vers une structure finie quelle que soit la valeur de $x0 \in]0 ; 1[$, Pour $r > rc$ le système devient confus [17].

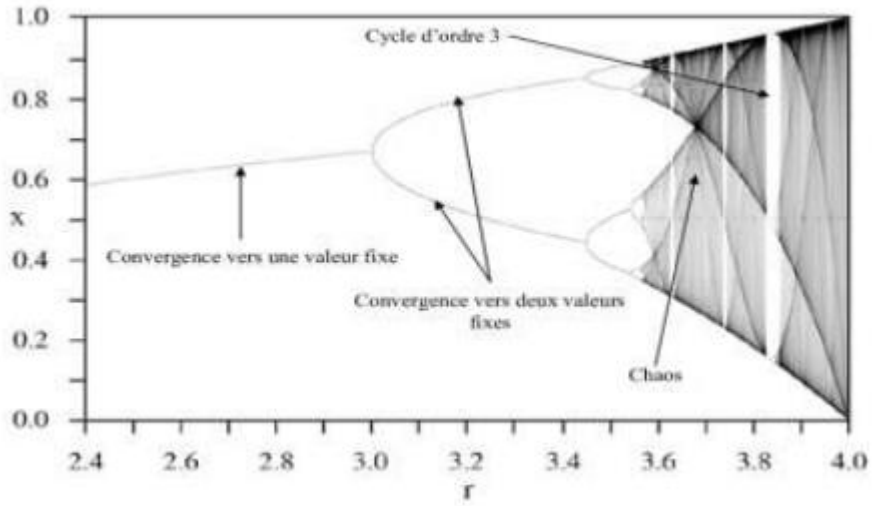


Figure 1.10 : Diagramme de bifurcation de la fonction logistique.

- Pour r ∈ [0 3[, la suite à un comportement simple avec un seul point fixe.
- Pour r ∈ [3 4[, on observe une augmentation des points périodiques. En effectuant une normalisation, plusieurs périodes apparaissent.
- Pour r=3.57, le comportement de la suite devient chaotique.

1.5 Types de systèmes chaotiques

Il existe différentes catégories de systèmes chaotiques utilisés pour générer des signaux chaotiques, notamment les systèmes chaotiques continus et les systèmes chaotiques à temps discret.

1.5.1 Système chaotique continue

En 1963, Lorenz a réalisé une étude numérique d'un système composé de trois équations différentielles qui était supposé représenter de manière approximative la convection thermique dans l'atmosphère. Cet exemple est célèbre car il démontre un comportement chaotique pour certaines valeurs des paramètres. Le système de Lorenz est devenu un modèle emblématique

en théorie du chaos et a contribué à la compréhension et à l'étude des systèmes dynamiques non linéaires.

Il a montré que de petites variations dans les conditions initiales peuvent entraîner des divergences importantes dans les trajectoires du système, ce qui rend la prédiction à long terme très difficile.

Ce système a également été utilisé pour illustrer le concept de sensibilité aux conditions initiales et l'idée du fameux "effet papillon", où de petits changements initiaux peuvent avoir des conséquences drastiques sur le comportement futur du système [18].

Ce système implique 3 équations différentielles :

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - bz \end{cases} \tag{1.5}$$

L'espace des phases est tridimensionnel.

Les figures suivantes représentent le comportement chaotique du système de Lorenz.

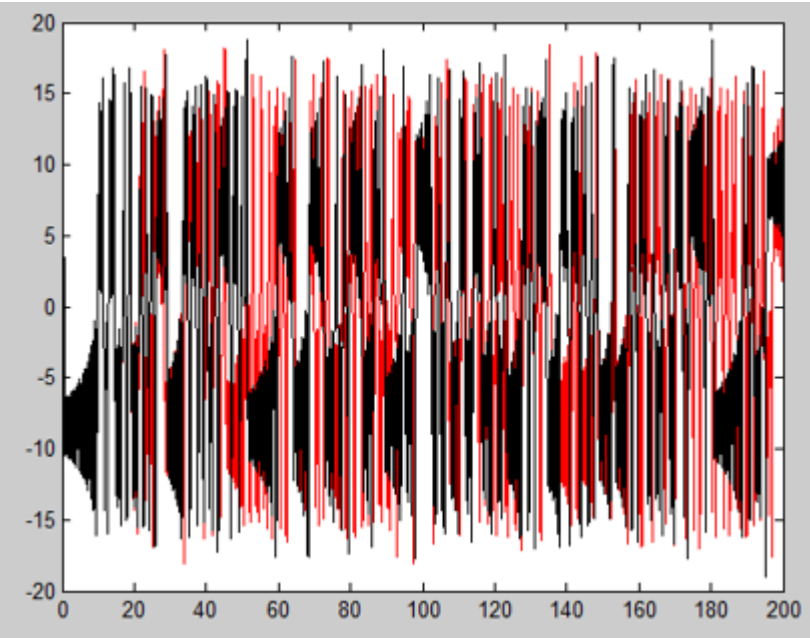


Figure 1.11 : le comportement chaotique du système de Lorenz.

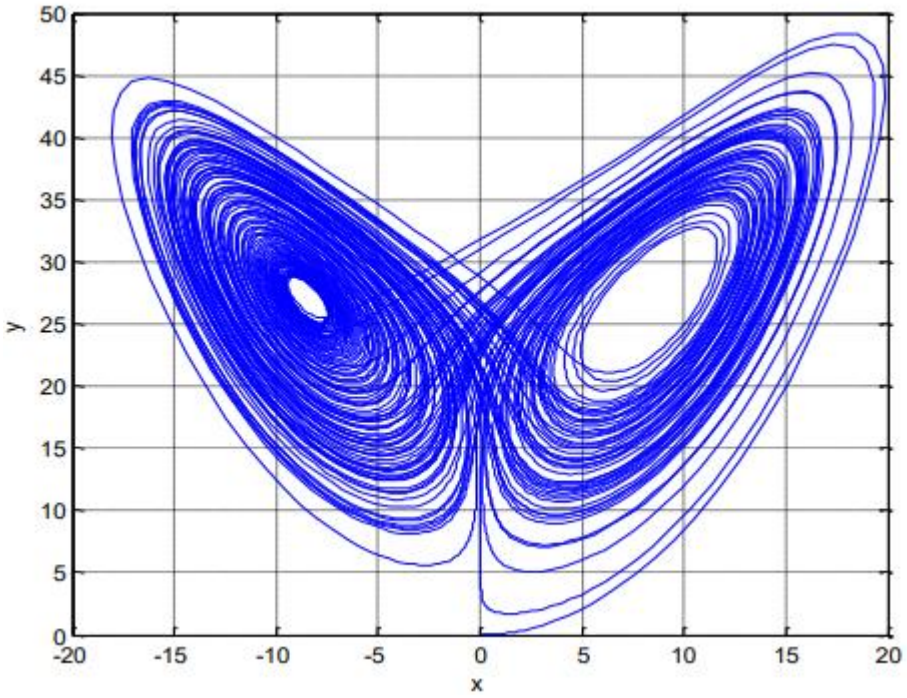


Figure 1.12 : L'attracteur étrange de Lorenz.

L'attracteur étrange de Lorenz représente l'évolution des trois (3) états avec une condition initiale, la structure ressemble à deux (2) ailes de papillon. Dans la littéraire On trouve de nombreux exemples d'autres systèmes chaotiques [19-25].

1.5.2 Système chaotique discret

L'astronome Michel Hénon a développé un système dynamique discret de deux dimensions qui se distingue par sa simplicité et sa réactivité. Contrairement aux systèmes continus où les points évoluent de manière continue, ce système évolue par étapes discrètes dans le temps. Il s'agit donc d'un système à temps discret [26]. Il est défini par la forme suivante :

$$\begin{cases} (n+1) = (y_{(n)}+1) - (a * x_{(n)}) \\ (n+1) = b * x(n) \end{cases} \quad (1.6)$$

a ; b : représentent des paramètres de bifurcation.

La valeur de la constante a control la non linéarité de l'itération, et celle de b traduit le rôle de la dissipation. Les valeurs habituellement utilisées pour a ; b sont : a = 1 ; 4 et b = 0 ; 3.

Avec l'initialisation par : x (1) = y (1) = 0.1. La figure (1.8) présente l'attracteur de système de Hénon.

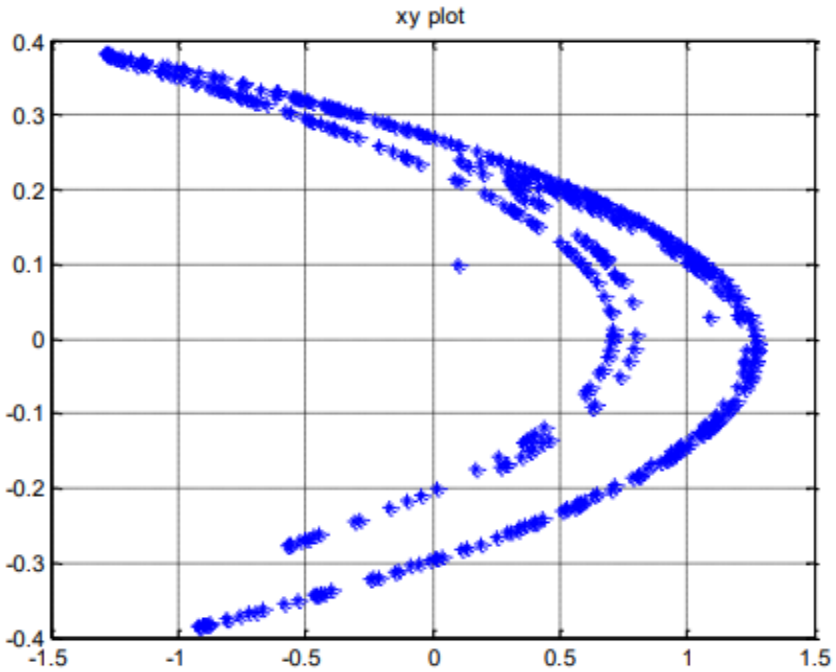


Figure 1.13 : l'attracteur de système de Henon.

Toutes les valeurs qui convergent vers cette structure le font d'une manière différente. L'attracteur de Henon montre une infinité de fines structures à mesure qu'on effectue des grossissements successifs.

1.5.3 Système chaotique à retard

En 1977, une découverte importante a été faite dans le domaine des systèmes chaotiques avec l'introduction du premier système chaotique à retard, connu sous le nom de système Mackey-Glass. Ce système, basé sur un modèle physiologique, a permis de comprendre et d'étudier les propriétés chaotiques dans le contexte des systèmes dynamiques avec rétroaction.

Par la suite, en 1999, Chen et Uta ont fait une autre découverte significative en identifiant un nouvel attracteur chaotique, connu sous le nom de modèle de Chen [27].

Il est défini par le système d'équations à trois (3) dimensions suivantes :

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x + cy - xz \\ \dot{z} = -bz + xy \end{cases} \tag{1.7}$$

Le comportement de ce système est chaotique pour les paramètres a, b et c avec les valeurs suivantes : a = 35, b = 8/3, c = 28, on va ajouter un terme de retard pour le système soit chaotique avec retard. Le modèle de Chen retardé est défini par :

$$\begin{cases} \dot{x} = a(y-x) + a1x(t-\tau 1) + a2x(t-\tau 2) \\ \dot{y} = cy - xz + a3y(t-\tau 1) \\ \dot{z} = -bz + xy + a4z(t-\tau 2) + d \end{cases} \quad (1.8)$$

Les valeurs des paramètres : a = 35, $a1$= 1.4, $a2$= 0.4, $a3$ = $a4$ = 0.5, b = 3, c = 20 et d = -300.
Les retards : $\tau 1$ = 1s, $\tau 2$ = 2s.
La figure qui convient représente le Comportement chaotique du système de Chen retardé pour les paramètres précédents.

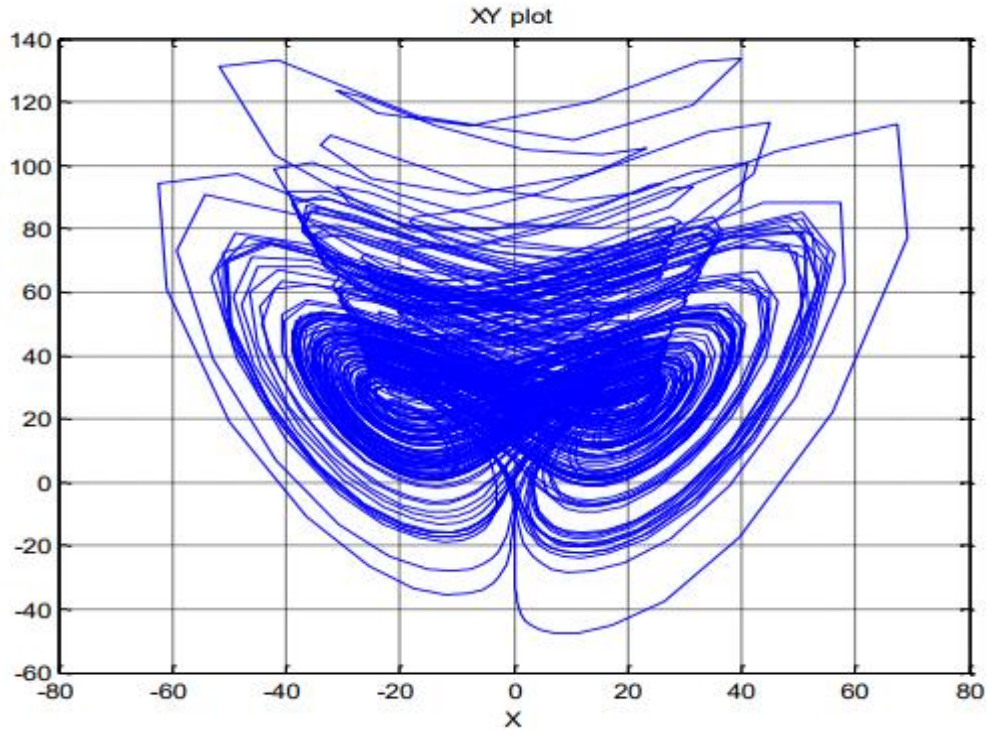


Figure 1.14 : L'attracteur du système de Chen retardé.

,

1.6 Les applications du chaos

1.6.1 En biologie

La théorie du chaos trouve une pertinence particulière en biologie, notamment pour expliquer les variations des populations animales et les oscillations du cerveau. Elle met en évidence que le fonctionnement chaotique du cerveau humain permet de préserver l'unicité de chaque individu, en maintenant un degré d'incertitude propice à l'émergence de possibilités indéterminées.

Ainsi, cette théorie offre une perspective selon laquelle l'homme peut être considéré comme libre et unique.

1.6.2 En économie

La théorie du chaos offre un cadre d'analyse pertinent en économie, en permettant de modéliser les phénomènes complexes tels que les mouvements commerciaux, les marchés financiers et les cycles économiques. Elle met en avant les notions de fractales et de hasard pour expliquer les variations des cours de la Bourse et modéliser des expériences aléatoires complexes. Cette approche permet ainsi de mieux appréhender les dynamiques économiques et de prendre des décisions éclairées dans le domaine de la finance.

1.6.3 En informatique

Les fractales ont apporté des avancées significatives dans le domaine de l'informatique. Elles ont été utilisées pour développer des procédés de compression d'images plus performants, permettant de réduire la taille des fichiers sans compromettre leur qualité. De plus, elles ont contribué à améliorer la génération d'images de synthèse en rendant les objets et les paysages plus réalistes grâce à leur capacité à représenter les formes fractales présentes dans la nature.

Ainsi, les fractales ont ouvert de nouvelles perspectives dans le domaine de l'informatique graphique et ont permis de mieux appréhender et représenter les formes complexes du monde réel.

1.7 Conclusion

Ce chapitre a présenté les notions principales des systèmes chaotiques, en commençant par les définitions des systèmes dynamiques en général, puis en se concentrant sur les systèmes chaotiques en particulier et leurs propriétés et applications. Nous avons également examiné les types de systèmes chaotiques, à savoir à temps continu et discret. Enfin, nous avons vu comment

de petites variations dans les conditions initiales peuvent entraîner des divergences importantes dans les trajectoires du système, ce qui rend la prédiction à long terme très difficile. Ce chapitre a donc permis de mieux comprendre les systèmes chaotiques et leur importance dans différents domaines tels que l'économie, l'informatique et les sciences physiques.

Chapitre 2

- Etat de l’art sur la sécurisation des données médicales.

2.1 Introduction

La sécurisation des données médicales revêt une importance cruciale dans le contexte actuel de la numérisation des informations de santé. Avec l'évolution des technologies de l'information et de la communication, les données médicales sont devenues de plus en plus accessibles et échangées à travers des systèmes informatiques interconnectés. Cependant, cette facilité d'accès et de partage comporte également des risques importants en termes de confidentialité et de protection des données sensibles des patients.

L'objectif de ce chapitre est de mettre en lumière les enjeux, les avancées et les meilleures pratiques liés à la sécurisation des données médicales. En comprenant les défis actuels et en adoptant des mesures de sécurité appropriées, nous pouvons garantir la confidentialité et l'intégrité des données médicales, tout en offrant des soins de qualité aux patients.

Nous explorerons également les réglementations nationales et internationales en matière de protection des données médicales, telles que **RGPD** et **HIPAA.**

2.1.1 Présentation de la norme internationale HIPAA

La norme HIPAA **(Health Insurance Portability and Accountability Act)** est une réglementation américaine adoptée en 1996 pour protéger la confidentialité et la sécurité des informations de santé des individus. Elle établit des normes et des règles pour les entités couvertes, telles que les fournisseurs de soins de santé, les compagnies d'assurance et les prestataires de services de santé, afin de garantir la protection des données médicales.

HIPAA comprend plusieurs règles, notamment la Privacy Rule, qui définit les droits des individus en matière de confidentialité de leurs informations de santé, et la Security Rule, qui exige la mise en place de mesures de sécurité pour protéger les données de santé électroniques.

2.1.2 Présentation de la norme internationale RGPD

La norme RGPD **(Règlement Général sur la Protection des Données**) est une réglementation européenne visant à protéger les données personnelles, donnant plus de contrôle aux individus et imposant des obligations strictes aux organisations qui les traitent. Il vise à assurer la confidentialité et la sécurité des informations personnelles, et prévoit des sanctions en cas de non-conformité.

2.2 Types de données médicales

2.2.1 Données cliniques

Les données cliniques sont des informations sur la santé d'un individu obtenues lors d'une évaluation médicale, d'un diagnostic et d'un traitement. Cela comprend les antécédents médicaux, les symptômes, les résultats des examens physiques, les tests de laboratoire, les procédures médicales, les traitements prescrits et les résultats des procédures[28].

2.2.2 Données d'information

Il s'agit d'informations générales sur la santé, telles que les stratégies de santé publique, les objectifs de dépenses d'assurance maladie, les programmes de santé, la formation médicale, l'offre de soins (établissements et professionnels de santé), etc.

2.2.3 Données de recherche

Les données de recherche médicale sont générées à partir d'études cliniques, de protocoles de recherche et de recherches médicales. Elles peuvent inclure des données sur l'efficacité des traitements, les résultats d'essais cliniques, les données génétiques, les évaluations psychologiques. Ces données sont utilisées pour approfondir les connaissances médicales, améliorer les traitements et contribuer au progrès scientifique.

2.3 Caractéristiques spécifiques des données médicales

2.3.1 Sensibilité

Les données médicales sont considérées comme des données à caractère personnel sensibles. Elles révèlent des informations intimes sur la santé physique ou mentale d'une personne, telles que les antécédents médicaux, les traitements cliniques, les diagnostics, etc. La sensibilité de ces données nécessite une protection renforcée pour préserver la vie privée des individus [28].

2.3.2 Confidentialité

Elle est essentielle pour garantir la vie privée des individus et protéger leurs informations de santé. Les réglementations, telles que le RGPD (règlement européen sur la protection des données), imposent des mesures strictes pour préserver la confidentialité des données médicales et limiter leur accès aux personnes autorisée.

2.3.3 Intégrité

Elle fait référence à la préservation de leur exactitude et de leur fiabilité. Il est crucial de veiller à ce que les données médicales ne soient pas altérées ou modifiées de manière non autorisée, car cela pourrait avoir des conséquences graves sur les décisions médicales prises à leur égard. Des mesures de sécurité, telles que les contrôles d'accès et les mécanismes de protection des données, sont mises en place pour garantir l'intégrité des données médicales [28].

2.3.4 Disponibilité

La disponibilité de ces données se réfère à leur accessibilité pour les professionnels de santé autorisés au moment où ils en ont besoin. Il est essentiel que les données médicales soient accessibles de manière fiable et sécurisée afin de faciliter les soins aux patients, la recherche médicale et les décisions cliniques. Des mesures techniques sont mises en place pour assurer la disponibilité des données médicales tout en respectant les exigences de confidentialité et de sécurité.

2.4 Menaces de données médicales

2.4.1 Présentation des principales menaces

2.4.1.1 Cyber attaques

Les établissements de santé sont devenus des cibles privilégiées pour les cyberattaques. Les attaquants cherchent à accéder aux données médicales sensibles afin de les exploiter à des fins malveillantes, telles que le vol d'identité, le chantage ou la revente sur le marché noir. Ces cyberattaques peuvent prendre la forme de ransomwares, de piratages informatiques ou d'autres méthodes sophistiquées [29].

2.4.1.2 Fuites de données

Les fuites de données médicales se produisent lorsque des informations confidentielles sont accidentellement ou délibérément révélées au public. Ces fuites peuvent être causées par des violations de sécurité, des erreurs humaines ou des actes de cybercriminalité. Une fuite de données expose les informations personnelles et médicales des individus, ce qui peut avoir des conséquences néfastes telles que le vol d'identité ou la discrimination [30].

2.4.1.3 Accès non autorisé

L'accès non autorisé aux données médicales se produit lorsque des personnes non autorisées, qu'il s'agisse de pirates informatiques, d'employés malveillants ou d'autres individus,

obtiennent illégalement l'accès à des informations confidentielles. Cela peut se produire à la suite de failles de sécurité, de vols de mots de passe ou de l'utilisation abusive de privilèges d'accès.

2.4.2 Vulnérabilité spécifiques liées aux données médicales

2.4.2.1 Systèmes obsolètes

Les systèmes obsolètes ou désuets utilisés pour stocker et gérer les données médicales peuvent constituer une vulnérabilité majeure. Ces systèmes peuvent avoir des failles de sécurité connues et ne pas être en mesure de prendre en charge les mesures de sécurité modernes. Cela rend les données médicales plus exposées aux risques de cyberattaques et de violations de la confidentialité [28].

2.4.2.2 Manque de sensibilité

Il est important de reconnaître que les données médicales sont sensibles et confidentielles, et qu'elles nécessitent une protection adéquate pour prévenir tout accès non autorisé ou toute divulgation inappropriée. Le manque de sensibilisation et de prise de conscience quant à la nature sensible de ces données peut entraîner des pratiques inadéquates et augmenter les risques de violations de la vie privée [31].

2.4.2.3 Partage de données

Lorsque les données médicales sont partagées entre différents acteurs, tels que les professionnels de la santé, les établissements de soins et les chercheurs, il est essentiel de garantir que les protocoles de partage sont sécurisés et conformes aux réglementations en matière de protection des données. Un partage de données inapproprié ou non sécurisé peut entraîner des accès non autorisés ou une utilisation abusive des informations médicales [30].

2.5 Techniques de sécurisation des données médicales

2.5.1 Cryptage

Le cryptage est le processus de conversion des données en une forme illisible pour les personnes non autorisées. Il utilise des algorithmes mathématiques pour transformer les informations en un texte codé, appelé texte chiffré. Seules les personnes disposant de la clé de

décryptage peuvent déchiffrer les données et les rendre lisibles à nouveau. L'utilisation du cryptage des données médicales offre plusieurs avantages [17] :

- **Confidentialité** : Le cryptage assure la confidentialité des données médicales en rendant les informations illisibles pour toute personne non autorisée qui tenterait d'y accéder.
- **Intégrité des données** : Le cryptage peut également aider à garantir l'intégrité des données, car toute modification apportée au texte chiffré sera détectée lors du processus de décryptage.
- **Conformité aux réglementations** : Dans de nombreux pays, les lois et les réglementations en matière de confidentialité des données, comme la HIPAA aux États-Unis, exigent que les données médicales soient cryptées pour garantir la confidentialité des patients.

Il existe deux types de cryptages :

Tableau 2.1 : Comparaison entre cryptage symétrique et asymétrique.

Cryptage symétrique	**Cryptage Asymétrique**
- Chiffrement à clé privée - Très facile - Rapide - Les clés de chiffrement symétriques doivent être conservées en lieu sûr -Vous devez vous assurer que toute personne ayant besoin de la clé puisse la retirer sans risque.	- Chiffrement à clé publique - Difficile par rapport au cryptage symétrique - Lent - La clé publique qu'ils utilisent peut-être publiée n'importe où en toute sécurité, car cela peut prendre des centaines d'années de travail pour extraire la clé privée de la clé publique.

2.5.2 Tatouage

Le tatouage des données, également connu sous le nom de tatouage numérique, est une technique qui permet d'incorporer des informations spécifiques dans les données elles-mêmes. Cela peut être fait en ajoutant des balises ou des métadonnées qui identifient l'origine des données ou fournissent d'autres informations pertinentes [32].

L'utilisation du tatouage des données médicales présente plusieurs avantages :

- **Traçabilité :** Le tatouage des données médicales permet de suivre l'origine des informations et de savoir qui les a générées ou modifiées.
- **Authentification :** Les tatouages numériques peuvent servir à vérifier l'authenticité des données médicales, en garantissant qu'elles n'ont pas été altérées ou manipulées.
- **Détection des violations :** En cas de violation de la confidentialité ou d'utilisation abusive des données médicales, le tatouage peut aider à identifier la source de l'incident.

Il est important de noter que le cryptage et le tatouage des données sont souvent utilisés ensemble pour renforcer la sécurité des données médicales. Le cryptage offre une protection globale des données contre les accès non autorisés, tandis que le tatouage permet une traçabilité et une authentification supplémentaires.

2.5.3 Authentification et contrôle d'accès

L'authentification et le contrôle d'accès sont des composantes essentielles de la sécurité des données médicales.

- **Authentification**

Son objectif est de s'assurer que seules les personnes autorisées peuvent accéder aux informations sensibles [33].

Différentes méthodes d'authentification peuvent être utilisées, notamment :

- **Identifiant et mot de passe :** Cette méthode implique l'utilisation d'un identifiant unique (tel qu'un nom d'utilisateur) et d'un mot de passe pour vérifier l'identité de l'utilisateur.
- **Authentification à deux facteurs (2FA)** : En plus de l'identifiant et du mot de passe, cette méthode nécessite une deuxième forme d'authentification, comme un code généré par une application ou envoyé par SMS, pour renforcer la sécurité.
- **Biométrie :** Les caractéristiques physiques uniques d'un individu, telles que les empreintes digitales, la reconnaissance faciale ou l'analyse de la rétine, peuvent être utilisées pour vérifier l'identité d'un utilisateur.
- **Cartes à puce :** Les cartes à puce peuvent contenir des informations d'identification cryptées et sont utilisées avec des lecteurs de cartes pour authentifier les utilisateurs.

- **Contrôle d'accès**

Une fois qu'un utilisateur est authentifié, le contrôle d'accès détermine les ressources, données ou fonctions spécifiques auxquelles un utilisateur est autorisé à accéder. Cela limite les privilèges et les droits d'accès en fonction des rôles, des responsabilités et des niveaux d'autorisation attribués à chaque utilisateur [34].

Quelques éléments clés du contrôle d'accès incluent :

- **Gestion des droits d'accès :** La gestion des droits d'accès consiste à définir et à attribuer des autorisations spécifiques à chaque utilisateur en fonction de son rôle ou de sa fonction au sein de l'organisation.
- **Groupes et niveaux de privilèges :** Les utilisateurs peuvent être regroupés en fonction de leurs autorisations et de leurs responsabilités, ce qui permet une gestion plus efficace des droits d'accès. Les différents niveaux de privilèges garantissent que les utilisateurs ne peuvent accéder qu'aux informations nécessaires à l'exercice de leurs fonctions.
- **Audit et suivi :** Les activités des utilisateurs, y compris les accès, les modifications et les actions effectuées sur les données médicales, doivent être enregistrées et surveillées. Les journaux d'audit permettent de détecter les comportements suspects, les violations potentielles et de mener des investigations en cas d'incident.
- **Révocation des droits d'accès :** Lorsqu'un utilisateur quitte l'organisation ou ne nécessite plus d'accès à certaines ressources, il est essentiel de révoquer rapidement ses droits d'accès pour prévenir les accès non autorisés.

En combinant l'authentification et le contrôle d'accès de manière appropriée, les établissements de santé peuvent garantir que seules les personnes autorisées peuvent accéder aux données médicales, réduisant ainsi les risques de violations de la confidentialité et de l'intégrité des informations sensibles des patients.

2.5.4 Surveillance et détection des intrusions

La surveillance et la détection des intrusions sont des mesures clés pour protéger les systèmes de santé contre les attaques et les accès non autorisés.

- **Surveillance des intrusions**

La surveillance des intrusions consiste à surveiller en temps réel les activités du réseau et des systèmes informatiques afin de détecter les tentatives d'intrusion ou les comportements suspects. Cela peut être réalisé en utilisant des outils de surveillance tels que des systèmes de

détection d'intrusion (IDS) et des systèmes de prévention d'intrusion (IPS). Ces outils analysent le trafic réseau, les journaux d'événements et les comportements des utilisateurs pour identifier les activités potentiellement malveillantes [35].

- **Détection des intrusions**

Elle vise à identifier et à signaler les tentatives d'intrusion réussies ou les violations de la sécurité. Cela peut inclure des techniques de détection basées sur des signatures qui comparent les schémas d'attaques connus avec le trafic réseau, ainsi que des techniques de détection comportementale qui identifient les comportements anormaux ou les modèles d'activité inhabituels. Une fois une intrusion détectée, des mesures de réponse appropriées peuvent être prises pour neutraliser la menace et protéger les données médicales [35].

2.6 Conclusion

En conclusion, la sécurisation des données médicales est d'une importance capitale pour garantir la confidentialité et la protection des informations personnelles des patients. La numérisation croissante des dossiers médicaux et l'utilisation de technologies numériques nécessitent des mesures de sécurité solides afin de prévenir les violations de données et de protéger la vie privée des individus.

Dans le prochain chapitre, nous allons présenter une technique de sécurisation des données qui est le tatouage en ondelette, ainsi ainsi ses propriétés et ses applications.

Chapitre 3

- Tatouage en ondelette.

3.1 Introduction

Le tatouage en ondelette est une technique qui associe les principes du tatouage numérique aux transformations en ondelette, largement utilisées dans le traitement d'images. Cette méthode permet d'incorporer des informations spécifiques dans les coefficients d'ondelette d'une image, créant ainsi un tatouage invisible à l'œil nu [36].

L'objectif de ce chapitre est de fournir une compréhension approfondie du concept de tatouage en ondelette appliqué aux images médicales. Nous aborderons en détail le schéma général du système de tatouage numérique, ainsi que les processus de génération, d'insertion et d'extraction de la marque. Nous explorerons également ses propriétés et ses applications.

En outre, ce chapitre mettra l'accent sur la transformée en ondelettes, une technique d'analyse de signal utilisée dans le cadre du tatouage numérique. Nous examinerons ses principes fondamentaux, ses différentes variantes et son rôle clé dans la réalisation du tatouage en ondelette.

3.2 Définition du tatouage numérique

Le touage numérique est une technique permettant d'insérer une information appelée marque dans un support numérique, de manière visible ou invisible.

La marque peut être une image, une vidéo, un texte, un audio ou bien une autre information numérique [37].

Cette marque est composée d'un ou plusieurs messages secrets et doit être à la fois imperceptible et robuste face aux attaques [36].

Le tatouage numérique consiste à insérer une marque invisible, appelée tatouage, dans une image ou un document numérique dans le but de protéger les informations contre le piratage et de préserver les droits d'auteur.

L'insertion de la marque peut être effectuée dans le domaine spatial ou fréquentiel, en fonction des techniques utilisées.

3.3 Le schéma général du système de tatouage numérique

Le modèle de base du schéma de tatouage numérique est constitué de trois éléments principaux [39] [40] :

Le processus de génération de la marque, le processus d'insertion de la marque et le processus d'extraction de la marque sont décrits dans **les figures 3.1**, **3.2** et **3.3** respectivement.

3.3.1 Le processus de génération de la marque

La génération de la marque n'est pas un processus standard. L'adaptation de la marque aux applications souhaitées est essentielle. Dans les applications simples, les données insérées peuvent être sous forme de texte ou d'image. Dans les applications plus avancées, la marque peut avoir des propriétés particulières en fonction des objectifs visés. Par exemple, dans le domaine médical, la marque peut nécessiter des informations spécifiques du patient ou des caractéristiques extraites de l'image d'origine pour confirmer l'intégrité et l'authenticité des données tatouées. Donc, l'algorithme de génération de la marque dépend du but poursuivi, tout en étant soumis à certaines contraintes.

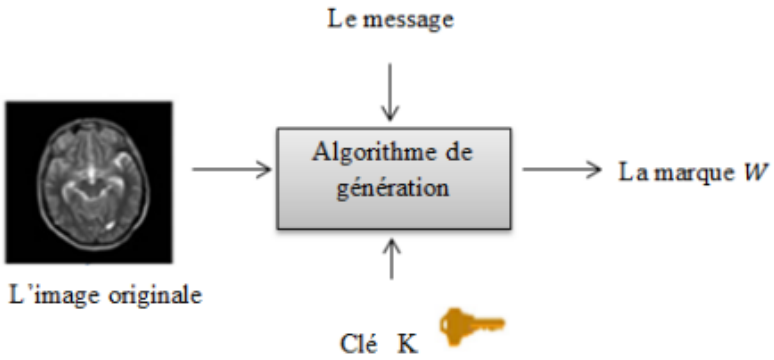


Figure 3.1 : Processus de la génération de la marque.

3.3.2 Le processus d'insertion de la marque

Le processus d'insertion de la marque du côté expéditeur consiste à intégrer la marque aux données originales en utilisant un algorithme de tatouage spécifique et en appliquant une clé secrète k pour générer les données tatouées. Cette étape permet d'incorporer la marque de manière imperceptible dans les données d'origine.

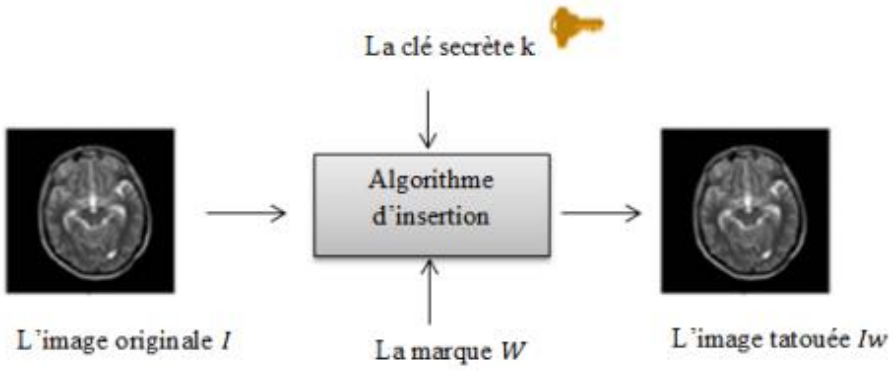


Figure 3.2 : Processus d'insertion de la marque.

3.3.3 Le processus d'extraction de la marque

Pour extraire la marque intégrée, le processus d'extraction implique l'inversion de l'algorithme d'insertion utilisé, en utilisant la clé secrète et/ou les données originales pour détecter et extraire la marque incorporée. Le principe de ce processus est illustré dans la Figure 3.3.

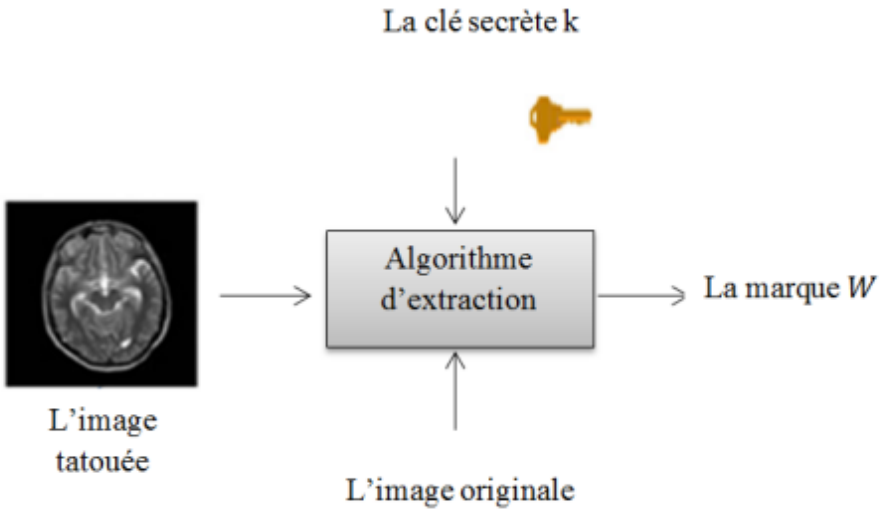


Figure 3.3 : Processus d'extraction de la marque.

3.4 Propriétés du tatouage numérique

Pour la conception d'un algorithme de tatouage performant, il est important de prendre en compte les principales contraintes techniques suivantes [41] :

- **La capacité :** cela fait référence à la quantité d'information que l'on veut insérer dans une image. Cette quantité peut varier en fonction de l'application.
- **La robustesse :** le système de tatouage doit être capable de résister à plusieurs types d'attaques.
- **L'imperceptibilité :** le tatouage numérique va certainement introduire des distorsions. Cette contrainte exige que ces distorsions soient minimales, de sorte que l'image tatouée reste visuellement fidèle à l'image originale.

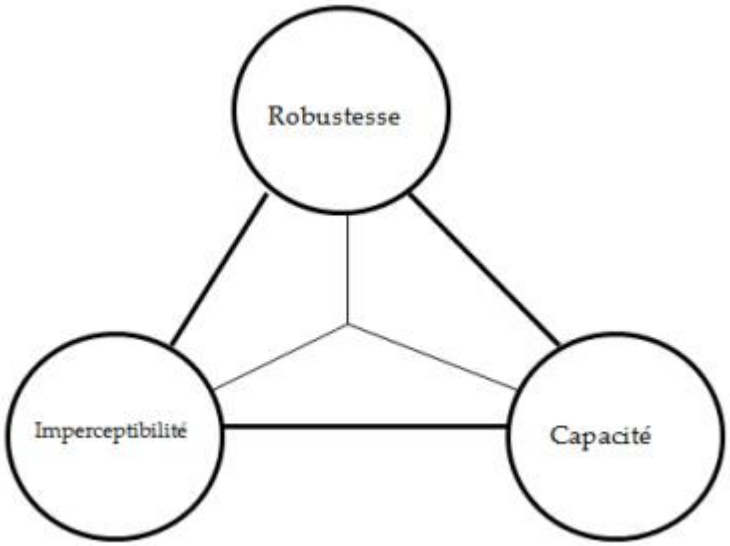


Figure 3.4 : Le triangle de compromis entre les trois propriétés essentielles [42].

3.5 Les applications du tatouage numérique

Il est impossible de créer un algorithme universel qui puisse être adapté à toutes les applications du tatouage numérique. C'est pourquoi il existe de nombreuses applications différentes pour cette technologie [36].

3.5.1 Protection des droits d'auteur

L'application la plus évidente du tatouage numérique est dans le droit d'auteur, où l'objectif est d'insérer une signature permettant d'identifier le propriétaire, de façon très robuste. Les deux principales qualités essentielles à respecter dans ce contexte sont la robustesse et l'invisibilité de la marque [44].

Il est essentiel que la marque soit à la fois invisible et extrêmement résistante, car elle est utilisée pour se prémunir contre le piratage de données. La marque doit être imperceptible

pour ne pas altérer la qualité visuelle de l'objet ou de l'œuvre, tout en étant hautement résistante afin de garantir sa présence et son intégrité même face à des tentatives de contrefaçon ou de falsification [38].

3.5.2 La prévention de la copie illégale ou « fingerprinting »

Fingerprints (Les empreintes digitales) sont les caractéristiques d'un objet qui ont tendance à le distinguer des autres petits objets. Comme dans les applications de protection du droit d'auteur, le filigrane pour l'empreinte digitale est utilisé pour retracer les utilisateurs autorisés qui violent le contrat de licence et distribuer illégalement le matériel protégé par le droit d'auteur. Ainsi, les informations intégrées dans le contenu concernent généralement le client, telles que son numéro d'identification [46].

3.5.3 L'authentification des données

Permet de savoir si l'image a subi des malversations et si tel est le cas, certaines informations pointant la localisation des dégradations peuvent être extraites. Comme son nom l'indique, cette méthode de tatouage ne doit pas être robuste, mais bien au contraire la marque insérée doit être la plus fragile possible pour être effacée dès lors qu'une malversation apparaît [45].

3.5.4 Contrôle d'accès

Un paiement différent permet aux utilisateurs d'avoir différents privilèges (contrôle de lecture / copie) sur l'objet, il est souhaitable dans certains systèmes d'avoir un mécanisme de contrôle de copie et d'utilisation pour empêcher la copie illégale du contenu ou limiter le nombre de copies. Un filigrane robuste peut être utilisé à cette fin [46].

3.6 La transformée en ondelettes (WT)

Une ondelette est une fonction d'onde caractérisée par une durée limitée et une valeur moyenne nulle. En comparant les formes d'onde des ondelettes avec celles des ondes sinusoïdales, on peut intuitivement remarquer que les signaux présentant des changements brusques seraient mieux analysés à l'aide d'une ondelette irrégulière plutôt qu'avec une onde sinusoïdale lisse.

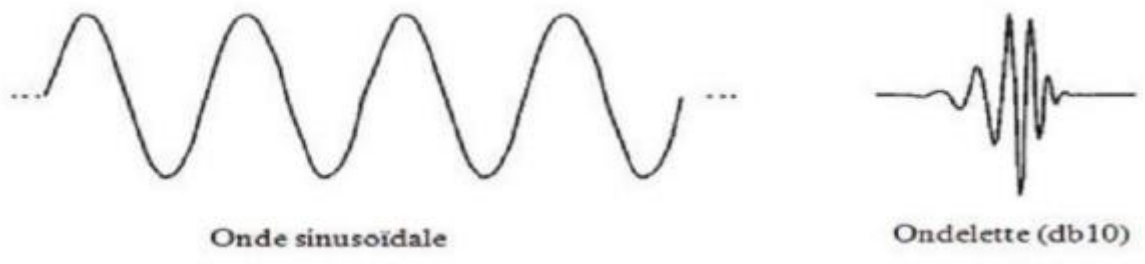


Figure 3.5 : La Différence entre une onde sinusoïdale et une ondelette.

La transformée en ondelettes est une méthode mathématique qui permet de décomposer un signal en différentes composantes fréquentielles tout en préservant sa localisation spatiale. Le signal d'origine est projeté sur un ensemble de fonctions de base qui varient à la fois en fréquence et en position spatiale. Ces fonctions de base s'adaptent aux différentes fréquences présentes dans le signal à analyser. Ainsi, cette transformation offre une localisation précise dans le temps et en fréquence du signal étudié [40].

Figure 3.6 : Le Principe de la Transformée en ondelettes.

L'analyse en ondelettes adopte une fonction de prototype d'ondelettes connue sous le nom de "Ondelettes mère" donné dans l'équation (3.1). Cette Ondelette mère génère une famille d'ondelette constituée de ses délattées et ses translatées [40].

La définition de l'ondelette mère est donnée par la formule suivante :

$$\Psi_{a,b} = \frac{1}{\sqrt{a}} \Psi\left(\frac{t-b}{a}\right) \qquad (3.1)$$

$\frac{1}{\sqrt{a}}$: Facteur de normalisation peut être aussi pris a 1 ou $\frac{1}{a}$.

3.7 Les Propriétés de La Transformée En Ondelette

Bien que les propriétés de la transformée en ondelettes (TO) continue aient été discutées et utilisées tout au long de ce mémoire, il est important de rappeler brièvement les points essentiels de manière concise [1] :

- **Linéarité :**

La linéarité de la TO vient de la linéarité du produit interne.

- **Propriété de translation :**

Si f(x) a pour TO continue alors la fonction translatée **f'(x) = f(x-b)** a pour TO.

- **Propriété d'échelle :**

Si f(x) a pour TO continue alors la fonction **f ' (x) = (1/ s) f (x / s)** a pour TO.

3.8 La transformée en ondelettes continues

La transformée en ondelettes repose sur les translations et les dilatations d'une fonction de base fixe appelée ondelette mère T ∈ L^2 ($\mathbb{R}$). Dans le cas de la transformée continue, les paramètres de translation et de dilatation varient de manière continue. En d'autres termes, la transformée en ondelettes utilise ces fonctions pour analyser le signal [41] :

$$\Psi_{a,b} = \frac{1}{\sqrt{a}}\Psi\left(\frac{t-b}{a}\right) \qquad (3.2)$$

Avec a, b ∈ $\mathbb{R}$, a≠0, ou a sert à dilater (comprimer ou étendre) la fonction Ψ, et b sert à latranslater (la déplacer selon l'axe des temps).

Quand on analyse un signal f(x) avec ces ondelettes, on le transforme en une fonction de deux variables (le temps et l'échelle d'analyse du signal) qu'on peut appeler $\mathcal{W}(a, b)$ [2] [41] :

$\mathcal{W}(a, b) = \langle f, \Psi a, b \rangle$

Que l'on peut également noter :

$$\mathcal{W}\text{ (a, b)} = \int_{-\infty}^{+\infty} f(t)\Psi_{a,b}\ dt \qquad (3.4)$$

Parmi ces ondelettes [42]:

3.8.1 L'ondelette de Morlet

Est également souvent utilisé :

$$\Psi(t) = EXP\left(\frac{t^2}{2}\right) EXP(-i\omega o t)$$

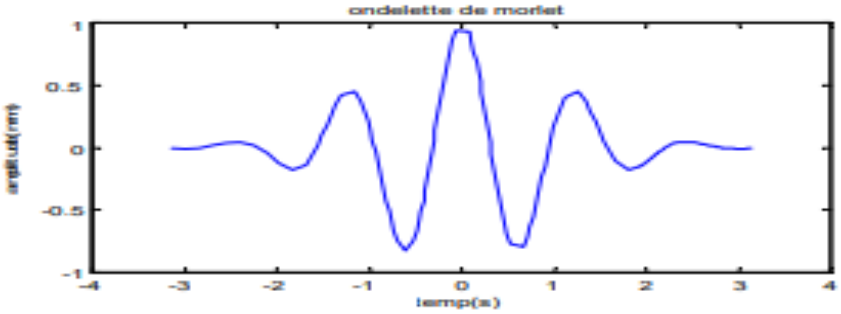


Figure 3.7 : Représentation de l'ondelette de morlet.

3.8.2 L'ondelette de Mexican Hat

$$\Psi(t) = \quad (1 - t^2)e^{-t^2/2}$$

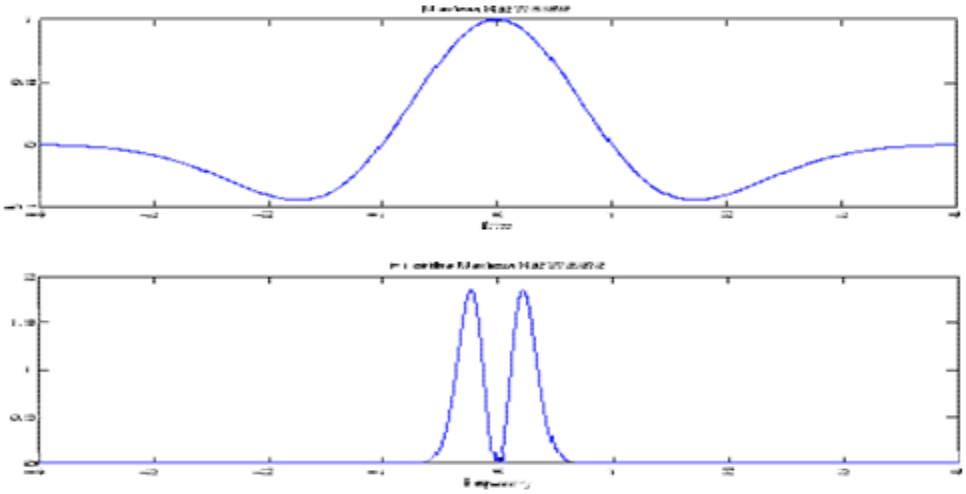


Figure 3.8 : Représentation d'ondelette de chapeau mexicaine dans deux domaines.

En théorie, cette transformation présente une redondance infinie, car l'ondelette est continuellement déplacée. Cependant, il existe des méthodes pour réduire cette redondance, telles que l'utilisation de la transformée en ondelettes discrète [40].

3.9 La transformée en ondelettes discrète

À la différence de la transformée continue qui effectue des dilatations et des translations continues de l'ondelette, la transformée en ondelettes discrète opère des

translations et des dilatations de manière discrète [41].

Les coefficients a et b associés à ces opérations seront discrétisés de la manière suivante :

$$a = a_0^j \text{ et } b = k.b_0.a_0^j$$

Avec : k, j ϵ $\mathbb{Z}^2$, $a_0 > 1$ et $b_0 > 0$.

Les ondelettes sont alors définies de la manière suivante :

$$\Psi_{j,k} = \frac{1}{\sqrt{a_0^j}} \Psi\left(\frac{1}{a_0^m} t - kb_0\right) \quad (3.5)$$

Parmi ces ondelettes [42]:

3.9.1 L'ondelette de Haar

Est assez classique, elle se caractérise par sa fonction d'échelle.

$$\psi(t) = \begin{cases} 1 & \text{pour } 0 \leq t < \frac{1}{2}, \\ -1 & \text{pour } \frac{1}{2} \leq t < 1, \\ 0 & \text{sinon} \end{cases}$$

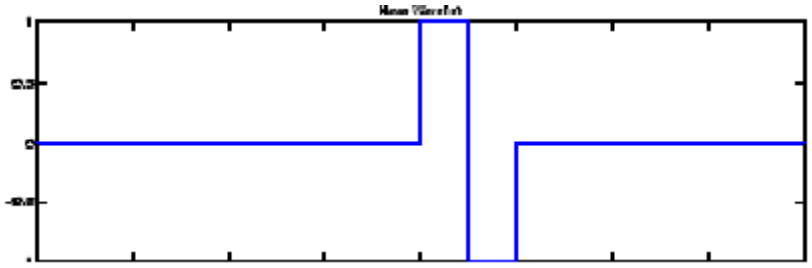


Figure 3.9 : Représentation de l'ondelette de haar.

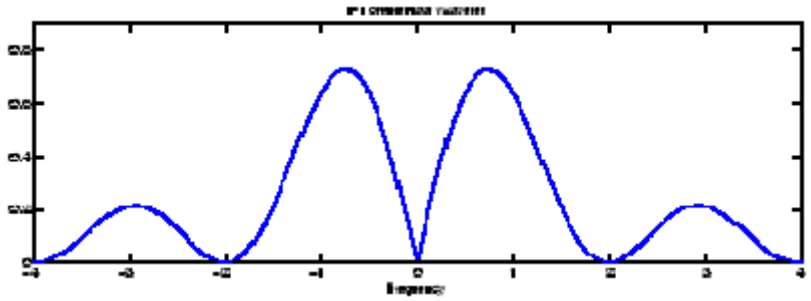


Figure 3.10 : Représentation de l'ondelette de haar dans le domaine fréquentiel.

3.9.2 L'ondelette de Shannon

$$\Psi(t) = \mathrm{sinc}(t/2)\cos(3\Pi t/2)$$

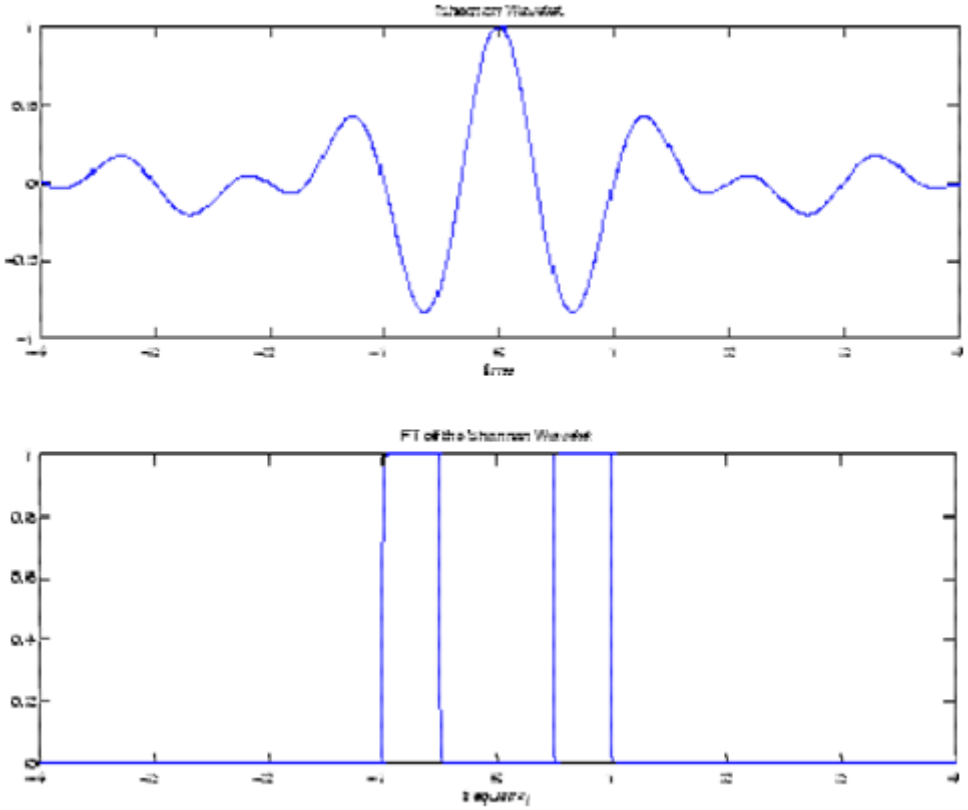


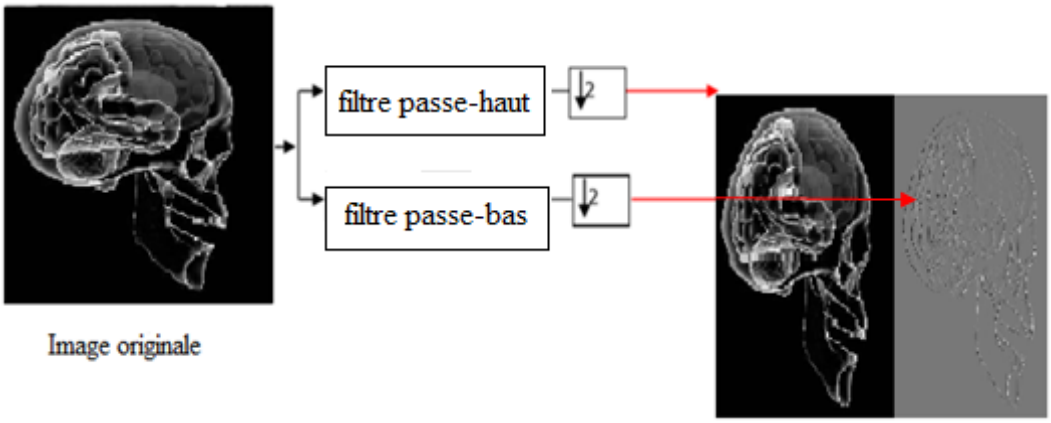
Figure 3.11 : Représentation d'ondelette de Shannon dans deux domaines.

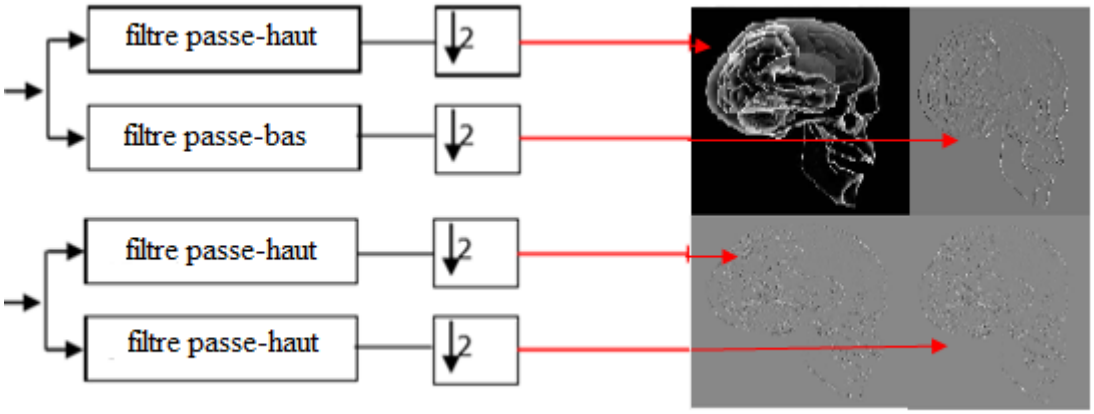
Nous avons constaté que la transformée en ondelettes continue présente une redondance infinie. Pour réduire considérablement cette redondance, sans l'éliminer complètement, nous utilisons la transformée en ondelettes discrète, où les signaux sont représentés par un nombre fini d'échantillons. Lorsque nous souhaitons obtenir une représentation transformée aussi concise que possible, c'est-à-dire avec autant d'échantillons que le signal d'origine, nous utilisons un cas particulier de la transformée en ondelettes discrète : la transformée en ondelettes orthogonale [40].

En résumé, la transformée en ondelettes discrètes permet une décomposition efficace des images en offrant une représentation multi résolution, un dé corrélation des pixels voisins et une adaptabilité aux caractéristiques de l'image.

3.10 Application à la compression d'images

Suite à la transformation d'une image par ondelettes discrètes, il n'y a pas directement de compression de la taille de l'image. En effet, une image de 640*480 pixels sur 8 bits donne, après traitement par la TOD, 640*480 coefficients sur 8 bits, répartis entre les coefficients de détails (CD) et les coefficients d'approximations (CA). Comme dans tout encodage par transformation, le calcul de la transformée du signal à compresser est une des étapes de traitement en vue de la compression. La transformation vise principalement à assurer le dé corrélation des pixels voisins pour permettre une quantification scalaire plus performante [43].





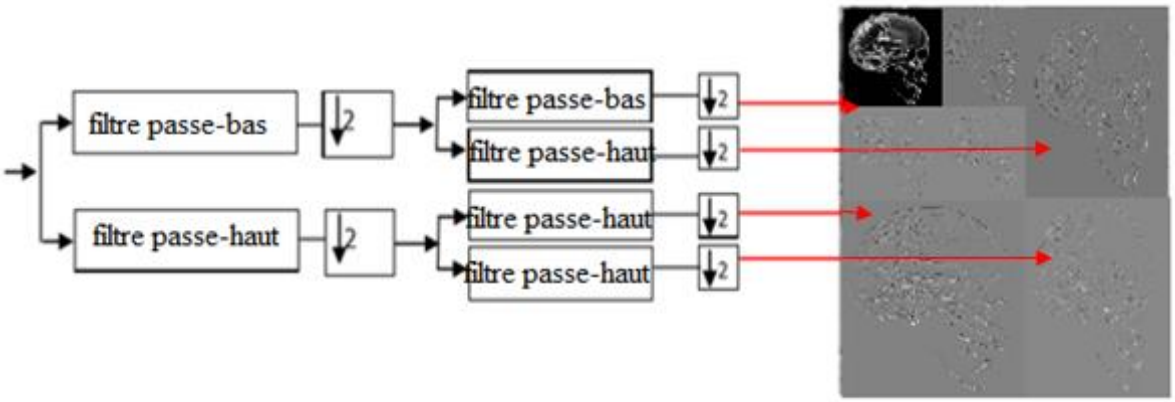


Figure 3.12 : Transforme en ondelette d'une image.

3.11 Conclusion

En combinant la sécurisation des données médicales avec le tatouage par ondelette, il est possible de créer une approche novatrice et efficace pour la protection des informations médicales sensibles. Cela ouvre la voie à de nouvelles perspectives en matière de confidentialité des données et de protection de la vie privée dans le domaine de la santé.

Chapitre 4

- Résultats de simulation.

4.1 Introduction

Dans ce chapitre, on va étaler les différents résultats de simulation sous Matlab 2016.

Nous allons explorer le processus de cryptage d'images à l'aide d'algorithmes de chiffrement. Nous allons également examiner le processus de décryptage, qui permet de récupérer les informations originales contenues dans une image cryptée. Nous allons discuter de l'utilisation de systèmes chaotiques dans le cryptage d'images, ainsi que de la technique de tatouage d'images médicales pour marquer et protéger les images numériques. Enfin, nous allons explorer la transformée en ondelettes de Haar, une technique de décomposition d'images en différentes échelles de résolution.

4.2 Cryptage des images

Le cryptage de l'image est un processus qui consiste à transformer une image en une forme illisible ou difficilement compréhensible, en utilisant des algorithmes de chiffrement.

L'objectif principal du cryptage de l'image est de garantir la confidentialité des informations sensibles contenues dans l'image, en empêchant leur accès par des tiers non autorisés. Cela peut être particulièrement important dans le cas des images médicales, qui contiennent souvent des informations personnelles et confidentielles sur les patients.

4.3 Décryptage des images

Le décryptage des images fait référence au processus de récupération des informations originales contenues dans une image qui a été préalablement cryptée. C'est l'opération inverse du cryptage des images et permet de rendre les données visibles et compréhensibles pour les personnes autorisées.

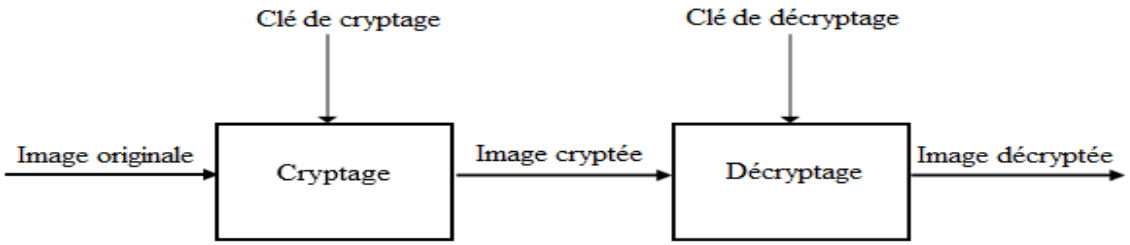


Figure 4.1 : Schéma résumant les différentes étapes du cryptage [17].

4.4 Système chaotique et sa relation avec le cryptage

Dans le contexte du cryptage, un système chaotique est souvent utilisé comme source d'aléa et de complexité pour renforcer la sécurité des algorithmes de chiffrement.

L'utilisation d'un système chaotique dans le cryptage repose sur l'idée que la génération de séquences pseudo-aléatoires à partir de ces systèmes est difficile à prédire, ce qui rend le chiffrement plus robuste contre les attaques cryptanalytiques (il devient extrêmement difficile pour un attaquant de retrouver les valeurs initiales ou les séquences générées sans connaître les conditions initiales exactes et les paramètres du système chaotique). Les valeurs produites par ce système peuvent être utilisées comme clés de chiffrement, comme masques pour le mélange des données, ou comme éléments de substitution dans les opérations de substitution-permutation.

En exécutant les codes de cryptage et de décryptage sur Matlab, on obtient les figures suivantes :

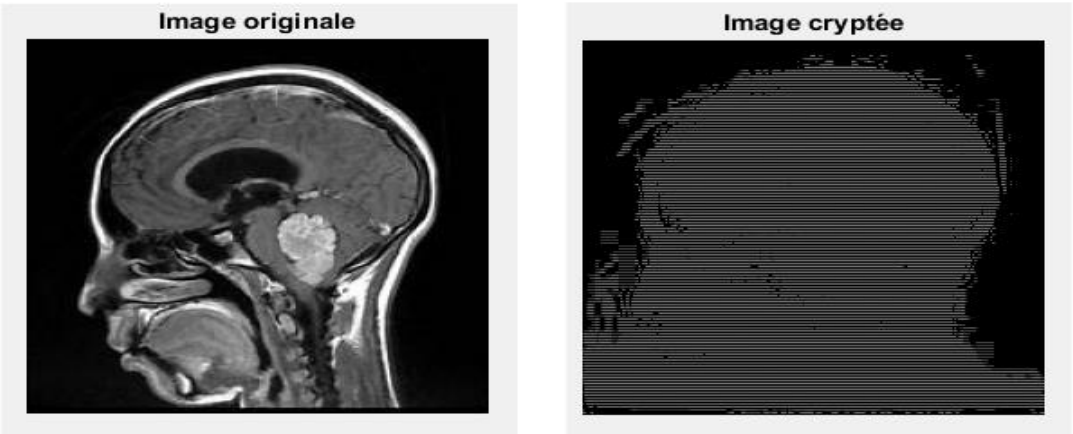


Figure 4.2 : Cryptage d'une image médicale.

Le code Matlab charge une image médicale de 256*256 pixels, la redimensionne en une taille de 512*512, génère une séquence chaotique à l'aide d'une carte logistique, crypte l'image en utilisant cette séquence et affiche l'image cryptée, Chaque pixel du l'image est modifié en fonction de la séquence chaotique, rendant l'image illisible.

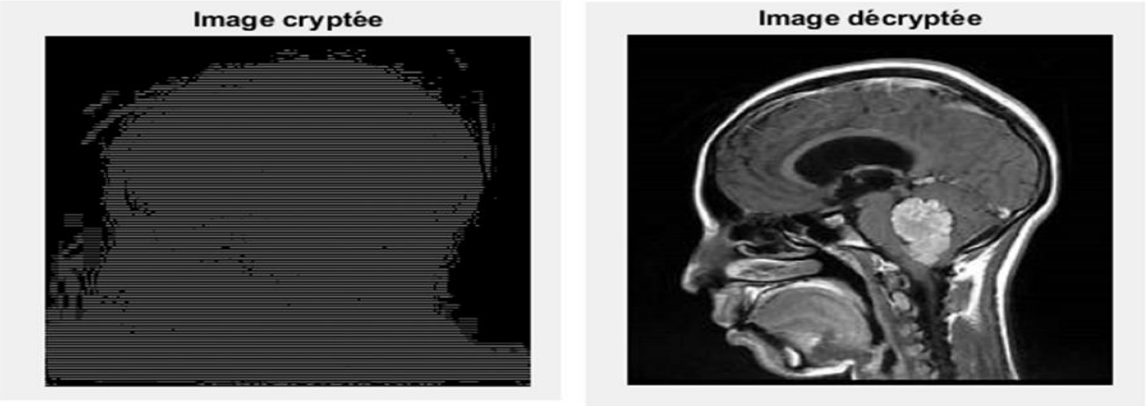


Figure 4.3 : Décryptage d'une image médicale.

Le code Matlab charge une image médicale cryptée de 512*512 pixels, génère une séquence chaotique à l'aide de la carte logistique, décrypte l'image en utilisant cette séquence.

4.5 Tatouage des images médicales

Le tatouage des images médicales, également connu sous le nom de tatouage numérique ou tatouage invisible, est une technique utilisée pour marquer et protéger les images médicales numériques.

Sa mise en œuvre peut varier en fonction des exigences spécifiques de chaque système ou application.

Des techniques de traitement d'image, de codage et de cryptographie sont souvent utilisées pour intégrer et extraire les informations du tatouage.

4.6 L'ondelette de Haar

Elle a été introduite par le mathématicien hongrois Alfréd Haar en 1910, c'est une fonction simple d'ondelette discrète, utilisée dans la transformée en ondelettes de Haar, qui permet de décomposer un signal ou une image en différentes échelles de résolution :

$$\psi(t) = \begin{cases} 1 & \text{pour } 0 \leq t < \frac{1}{2}, \\ -1 & \text{pour } \frac{1}{2} \leq t < 1, \\ 0 & \text{sinon} \end{cases} \tag{4.1}$$

4.7 La Décomposition en ondelette de Haar

C’est une technique utilisée pour décomposer une image en différentes échelles de résolution et en détails en utilisant la transformée en ondelettes de Haar.

L'image est divisée en une approximation de basse résolution (ou sous-bande) et des détails de haute résolution (ou sous-bandes) en utilisant des filtres passe-bas et passe-haut.

Le filtre passe-bas est appliqué horizontalement puis verticalement pour obtenir l'approximation de basse résolution (cA).

Le filtre passe-haut est appliqué de la même manière pour obtenir les détails de haute résolution (cH, cV, cD).

En exécutant le code Matlab de la décomposition d’une image médicale en ondelette jusqu'à trois niveaux on obtient la figure suivante :

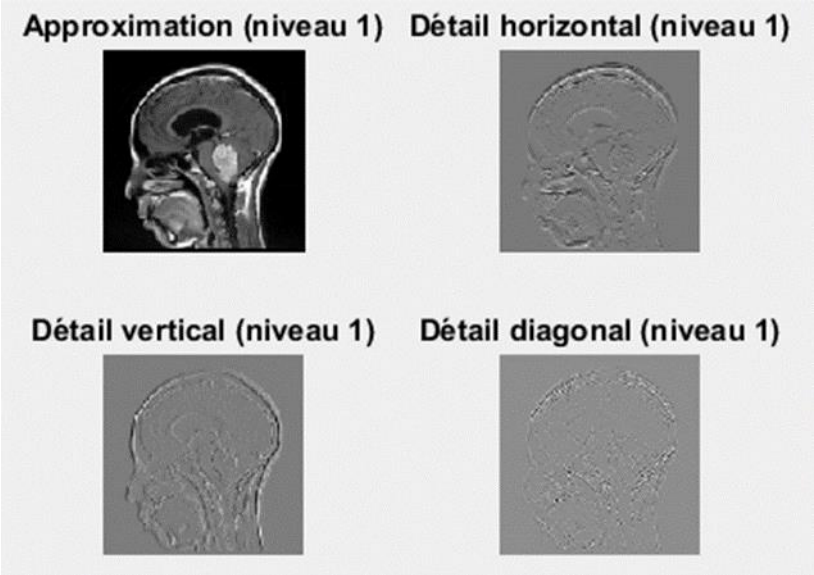


Figure 4.4 : 1er niveau de décomposition d’une image médicale.

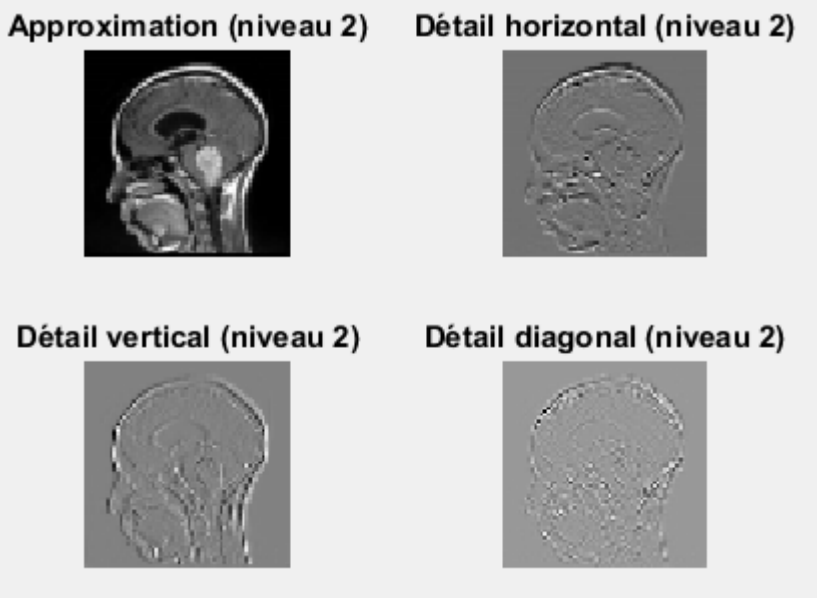


Figure 4.5 : 2ème niveau de décomposition d'une image médicale.

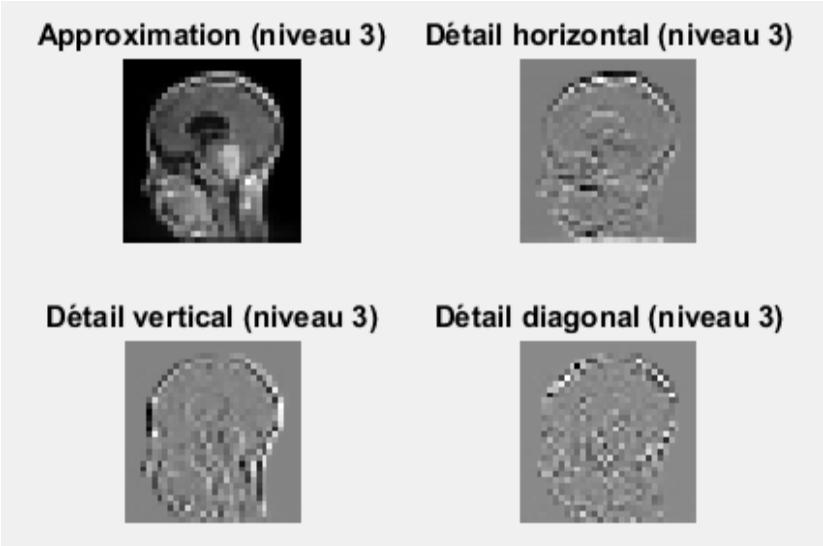


Figure 4.6 : 3ème niveau de la décomposition d'une image médicale.

En effet, une image de 1024*1024 pixels est répartie entre les coefficients de détails (CD) et les coefficients d'approximations (CA), après un traitement par la TOD.

Le code permet ainsi de visualiser les différentes composantes de l'image obtenues grâce à la décomposition en ondelettes de Haar. Cela peut aider à analyser les détails et les structures présents dans l'image à différentes échelles de résolution.

Le premier niveau de la composition en ondelettes est généralement considéré comme le niveau le plus grossier, où l'image ou le signal est décomposé en coefficients d'approximation et de détails. Ensuite, les coefficients d'approximation obtenus à partir du premier niveau sont soumis à une nouvelle décomposition en ondelettes pour obtenir des coefficients d'approximation et de détails de niveau 2. Ce processus est répété pour obtenir les coefficients d'approximation et de détails de niveau 3.

Chaque niveau ajoute des informations supplémentaires et permet une représentation plus détaillée de l'image. En général, plus le nombre de niveaux de composition en ondelettes est élevé, plus la représentation est riche en détails et en informations.

4.8 Reconstruction de l'image

4.8.1 L'ajout de l'image cryptée aux coefficients d'approximation

L'ajout de l'image cryptée aux coefficients d'approximation fait partie d'un processus de cryptage d'image basé sur les ondelettes. Cette technique est utilisée pour sécuriser les données d'image en les combinant avec une séquence chaotique générée à partir d'une carte logistique.

On ajoute une image cryptée de 512*512 pixels aux coefficients d'approximation d'ondelettes de 512*512 pixels, puis on reconstruit l'image en utilisant la décomposition en ondelettes inverse.

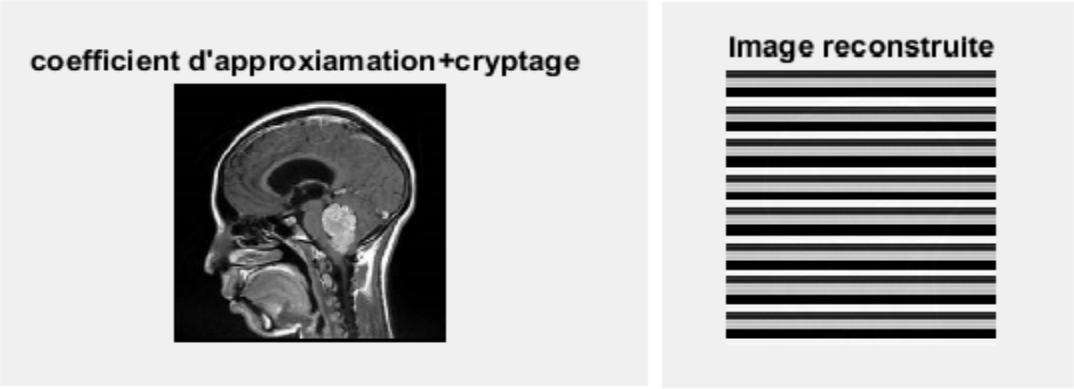


Figure 4.7 : Reconstruction de l'image médicale.

L'ajout de l'image cryptée aux coefficients d'approximation se réfère à l'étape où l'image cryptée est combinée avec les coefficients d'approximation de l'image décomposée en ondelettes. Cela peut être réalisé en additionnant les valeurs des pixels de l'image cryptée à ceux

des coefficients d'approximation. Cette étape permet de mélanger l'information cryptée avec les composantes globales de l'image, ce qui contribue à la sécurisation de l'image.

4.9 Récupération de l'image

Il convient de noter que le processus de cryptage peut être réversible, ce qui signifie qu'il est possible de récupérer l'image originale en effectuant les opérations inverses, telles que la soustraction de l'image cryptée des coefficients d'approximation et la reconstruction de l'image à partir de la décomposition en ondelettes initiale.

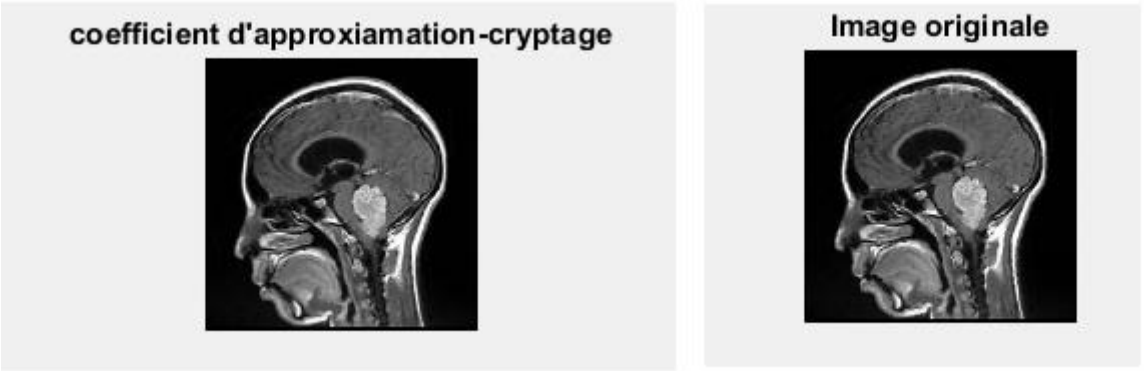


Figure 4.8 : Récupération de l'image médicale.

4.10 Conclusion

La décomposition des images médicales en ondelettes dans le contexte de la sécurité des données offre une approche prometteuse pour la protection et la confidentialité des informations médicales. Les simulations et les résultats obtenus ont confirmé l'efficacité de cette technique pour la dissimulation des données sensibles tout en préservant l'intégrité et la qualité des images médicales. L'utilisation judicieuse de la décomposition en ondelettes et des techniques de codage/cryptage appropriées peut contribuer à renforcer la sécurité des données médicales dans divers scénarios d'application, tels que le partage sécurisé d'images, la transmission confidentielle des données et la protection de la vie privée des patients.

Conclusion générale

Conclusion générale

Avec l’évolution rapide de l'imagerie numérique et des technologies de l'information et de la communication, l'utilisation croissante de la télémédecine est devenue une réalité. Cependant, cette expansion comporte également des risques. Les informations médicales, comprenant des images médicales et des données relatives aux patients, sont extraites et transmises à travers des réseaux non sécurisés. Dans le contexte du diagnostic à distance, du traitement, des téléconférences entre cliniciens, de la consultation médicale à distance, ainsi que de l'enseignement et de la formation à distance, il existe une préoccupation quant à la manipulation non autorisée, tant intentionnelle que non intentionnelle, des images médicales.

Afin de contribuer à cette sécurisation de données médicales, nous avons proposé deux techniques qui sont le cryptage, et le tatouage en ondelette.

Nous avons présenté les concepts généraux liés au chaos, ainsi que les caractéristiques des systèmes chaotiques, tels que leur sensibilité aux conditions initiales, leur nature déterministe et l'aspect aléatoire de leurs trajectoires.

Aussi nous avons également abordé de manière globale les différents types de données médicales, en mettant en évidence leurs caractéristiques spécifiques, les menaces auxquelles elles sont exposées, ainsi que les techniques de sécurisation utilisées pour les protéger.

Ensuite nous avons expliqué les principes fondamentaux de la transformée en ondelettes et son lien avec le tatouage des images médicales. Nous décrirons les différentes étapes du processus de tatouage en ondelette, notamment la décomposition de l'image en coefficients d'ondelettes.

Dans le dernier chapitre on a exposé les résultats de simulation, La réalisation se fait par code MATLAB. Les résultats sont affichés sous forme de sous-figures, montrant l'image originale, les coefficients d'approximation avec et sans cryptage, les coefficients de détails horizontaux, verticaux et diagonaux, l'image reconstruite et l'image originale pour comparaison.

Ce code illustre donc le processus de cryptage et de reconstruction des images médicales en utilisant la transformée en ondelettes et une séquence chaotique pour assurer la sécurité des données médicales.

Comme suite à ce travail, propose l'implémentation de cette approche sur une carte Raspberry Pi 3, pour une application réelle.

Perspectives

1. **Développement de techniques de tatouage en ondelette plus avancées :** De nouvelles recherches peuvent être entreprises pour concevoir des méthodes de tatouage en ondelette plus sophistiquées qui offrent une sécurité encore plus robuste et une meilleure qualité d'image. L'exploration de différentes transformations en ondelette, des modèles de masquage adaptatifs et des techniques de dissimulation des informations de tatouage peut être poursuivie.
2. **Étude de l'impact sur la précision du diagnostic :** Il est essentiel de mener des études approfondies pour évaluer l'impact du tatouage en ondelette sur la précision du diagnostic médical. Cela permettra de s'assurer que les informations médicales cruciales ne sont pas altérées par le processus de cryptage.
3. **Sécurité contre les attaques avancées :** Les attaques visant à contourner les techniques de tatouage en ondelette existantes sont en constante évolution. Des recherches supplémentaires sont nécessaires pour renforcer la sécurité des algorithmes de tatouage en ondelette en développant des défenses robustes contre des attaques telles que le stéganalyse et le traitement malveillant d'images.
4. **Applications dans d'autres domaines de l'imagerie :** Les techniques de tatouage en ondelette peuvent être étendues à d'autres domaines de l'imagerie, tels que la surveillance de sécurité, la gestion des droits numériques et la protection des images dans le domaine artistique. L'exploration de ces applications peut ouvrir de nouvelles perspectives de recherche et d'innovation.

Bibliographie

[1] C.Bouchelaghem, I.Zentout, « Nouveau schéma de communication sécurisée à base du chaos » Mémoire fin d'études, Université de Mila, 2020.

[2] F. P. Yves Benoist, "notes de cours systèmes dynamiques élémentaires", 2003.

[3] W. Laouira, "Contrôle des systèmes dynamiques chaotiques, " Thèse de doctorat, Université Constantine 1, Novembre 2018.

[4] D. Arbane, K. Arab, "Conception de crypto-systèmes à base de systèmes chaotiques d'ordre fractionnaire : Application au cryptage de la parole," Mémoire de Fin d'étude de Master Académique, Université Mouloud Mammeri, Juillet 2018.

[5] Qu'est-ce que la théorie du chaos ? (greelane.com)

[6] S. Chouat, "Synchronisation identique des systèmes chaotiques", Université Mohamed Khider, Biskra, Juin 2019.

[7] E. Goncalvès, « introduction au système dynamiques et Chaos », Cours de l'institut National Polytechnique de Grenoble, 2004.

[8] A. Senouci, "Elaboration de nouvelles approches de transmission sécurisée et cryptage par chaos, " Thèse de doctorat, Université De Jijel, 2014.

[9] A. Bouhous, "Sécurisation de l'information via un canal optique, " Thèse de doctorat, Université De Jijel, Novembre 2018.

[10] F. Zouad, « Élaboration et implémentation de nouvelles approches pour la sécurisation des transmissions à base des systèmes chaotiques d'ordre fractionnaire » Thèse de Doctorat, Université de Jijel, 2019.

[11] H. Hamiche, "Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques. Application à la Transmission Sécurisée de Données," Thèse de doctorat, Université Mouloud Mammeri, Tizi-Ouzou, 2011.

[12] S. Allouache, N. Hamma, “Conception et réalisation d’un système de transmission sécurisé de données à base de systèmes chaotiques sur cartes Arduino,” Mémoire De Fin D’Etude De Master Académique, Université Mouloud Mammeri, Tizi-Ouzou, Juillet 2015.

[13] H. Bouchenine, O. Guermache, “Etude de la dynamique et chaotique du système de Lorenz ”, Mémoire préparé en vue de l’obtention du diplôme de Master, Centre universitaire Abd Elhafid Boussouf -Mila, 2021.

[14] O. Megherbi, “Etude et réalisation d’un système sécurisé à base de systèmes chaotique”, Thèse de magister, Université Mouloud Mammeri Tizi-Ouzou, 2013.

[15] F. Bounar, Z. Zine, “ Application du chaos pour le cryptage des données ”, Mémoire de fin d’études, Université Mouhamed seddik ben Yahia Jijel, 12 Juillet 2022.

[16] H. Zhang. Chaos Synchronization and Its Application to Secure Communication. Thèse de Doctorat, Université de Waterloo, Ontario, Canada, 2010.

[17] C. Hamlil, R. Boucherout, “ Crypto-Systèmes basés sur le Chaos pour la Sécurisation des Données Médicales ”, Mémoire de fin d’études, Université Mouhamed seddik ben Yahia Jijel, 2022.

[18] F. Launay « Cours Commande Robuste Multi-variables Application au Chaos ». Cours De Laboratoire D’Automatique Et D’Informatique Industrielle. Université De Poitiers, 2 Mars 2011.

[**19**] MESSADI, Manal, KEMIH, Karim, MOYSIS, Lazaros, et al. A new 4D Memristor chaotic system: Analysis and implementation. Integration, 2023, vol. 88, p. 91-100.

[**20**] KEMIH, K., HALIMI, M., GHANES, M., et al. Control and synchronization of chaotic attitude control of satellite with backstepping controller. The european physical journal special topics, 2014, vol. 223, no 8, p. 1579-1589.

[**21**] KEMIH, K., GHANES, M., REMMOUCHE, R., et al. A novel 5D-dimentional hyperchaotic system and its circuit simulation by EWB. Mathematical Sciences Letters, 2015, vol. 4, no 1, p. 1-4.

[**22**] MOYSIS, Lazaros, VOLOS, Christos, TAKHI, Hocine, et al. Analysis, synchronization and microcontroller implementation of a generalized hyperjerk system, with application to secure communications using a descriptor observer. In : 2019 Panhellenic Conference on Electronics & Telecommunications (PACET). IEEE, 2019. p. 1-4.

[23] Imène. Ferhat, " Entretien et maintenance d'une installation photovoltaïque", Mémoire de fin d'études, Université Larbi Tebessi – Tébessa, 2022.

[20] A. Hank, R. Younsi, " Systèmes chaotiques pour la transmission sécurisée de données", Mémoire de fin d'études, Université Mouhamed seddik ben Yahia Jijel, 2020.

[25] https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante

[26] https://www.lefigaro.fr/secteur/high-tech/cyberattaques-pourquoi-vos-donnees-de-sante-sont-si-fragile-et-convoitees-20210312

[27] https://www.cdm44.org/le-partage-des-donnees-de-sante-entre-medecins-et-paramedicaux

[28] https://www.cairn.info/concepts-en-sciences-infirmieres-2eme-edition--9782953331134-page-304.htm

[29] M. Arour, N. Kassab, « Le tatouage des images JPEG », Projet fin d'études, Ecole Nationale Polytechnique, Juillet 2010.

[30] R. Chabani, « Implémentation d'un Protocole d'Élection d'un Serveur d'Authentification dans l'Internet des Objets », Mémoire fin d'études, 2021.

[31] J. Paul Khorez EZIKOLA MAZOBA, « L'étude de l'internet des objets et contrôle d'accès aux données », Université Panafricaine, Licence en Génie Informatique, 2015.

[32] D. Hamouda, « Un système de détection d'intrusion pour la cybersécurité », Université de 8 Mai 1945 – Guelma -, Mémoire de Fin d'études Master, Octobre 2020.

[33] K. Lemouchi, « Tatouage d'images par paquet d'ondelettes », Présenté En Vue De L'obtention Du Diplôme De Magister, 2006.

[34] M. Tayachi, « Sécurité des images par tatouage numérique et cryptographie dans les applications médicales » Université de Tunis El Manar, 5 May 2022.

[35] V. Martin1, M. Chabert1, B. Lacaze2, Un algorithme de Tatouage d'images numériques reposant sur les changements d'horloge périodiques, Institut National polytechnique de Toulous 3 Rue Camichel, BP 7122, 31071 Toulous Cedex 7, France

[36] Hussain Nyeem, Wageeh Boles et Colin Boyd, « A review of medical image watermarking requirements for teleradiology », in: Journal of Digital Imaging 26 (2013), p. 326-343.

[37] BOUHOUS, Adil et KEMIH, Karim. Novel encryption method based on optical time-delay chaotic system and a wavelet for data transmission. Optics & Laser Technology, 2018, vol. 108, p. 162-169.

[38] I. Assini, A. Badri, K. Safi, Technique Hybride de Compression pour le Tatouage des images, 2015.

[39] Asaad F Qasim, Farid Meziane et Rob Aspin, « Digital watermarking Applicability for developing trust in medical imaging workflows state of the art review », in: Computer Science Review 27 (2018), p. 45-60.

[40] A. Manoury, Tatouage d''mages numériques par paquets d'ondelettes, 21 Décembre 2001.

[41] I. Assini, A. Badri, K. safi, Technique Hybride de Compression pour le Tatouage des images, 2015.

[42] F. Autrusseau, Tatouage d'images fondé sur la modélisation su système visuel humain et sur la transformation mojette, 7 Novembre 2002.

[43] P. Singh, R.S. Chadha, A survey of digital watermarking technique, Applications and attacks, Issue 9, Mars 2013.

[44] C. Rouife, F. Kissoum, « Watermarking et compression d'images numériques : Applications aux images médicales », Mémoire de fin d'études, 2012

[45] Jean-Paul Guillement," Analyse de Fourier - Ondelettes", cours, Département de Mathématiques, université de Nantes, 2011.

[46] Y.T. Chan. Wavelet basics. Kluwer Academic Publisher, 1995

[47] Y.T. Mohand, "compression d'images hyper spectrales parla transformée en ondelette en 3D", thèse magistère, faculté de génie électrique et informatique, département d'électronique, UMMTO, 2011.