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

Université Mentouri de Constantine
Faculté des Sciences Exactes

Département de Mathématiques

N^0 d'ordre :

Série :

Mémoire
de Magistère en Mathématiques

Thème :

« Systèmes Dynamiques Non Linéaires et Phénomènes de Chaos »

(Application à la Cryptographie)

Option :

Systèmes Dynamiques et Topologie Algébrique

Présenté par **Ibtissem TALBI**

Devant le jury :

F.L. RAHMANI	**M.C.**	**U.M. Constantine**	**Président**
S. BOUGHABA	**M.C.**	**U.M. Constantine**	**Rapporteur**
M. ZITOUNI	**Prof.**	**U.S.T.H.B**	**Examinateur**
M.N. BENKAFADAR	**Prof.**	**U.M. Constantine**	**Examinateur**

Soutenu le : 29 / 06 / 2010

Table des matières

Table des figures

0.1 Introduction générale

Le chaos est toujours associé à une incompréhension des choses, à l'impossibilité de formuler une quelconque loi organisatrice d'un phénomène apparemment inextricable.

Le chaos, partout présent, dont la complexité est issue d'un nombre infini de combinaisons simples, est admirablement pressenti dans la description du chaos marin par **Victor Hugo** [1], texte où l'on retrouve les ingrédients essentiels de ce que regroupe le terme scientifique "chaos" de nos jours. Cependant il faudra attendre l'aube du **XX**e siècle, et les travaux de **Henri Poincaré** sur le mouvement des astres dans l'espace et son fameux problème des trois corps, pour une formulation plus scientifique.

Depuis, de nouveaux concepts sont apparus. Les solutions asymptotiques de certains systèmes dynamiques se nomment attracteurs étranges chaotiques et l'on sait que le complexe peut être engendré par des systèmes d'équations très simples.

Cette nouvelle approche, un peu à l'image de la révolution quantique du début du siècle, envahit peu à peu l'ensemble de la science. Nous savons maintenant que le système solaire est imprédictible au delà de 100 millions d'années [2], que le mouvement complexe du satellite de saturne, Hypérion, est chaotique, et ce, en raison de sa forme oblongue. De même au sein des systèmes physiologiques [3], le chaos procurerait une flexibilité de réponse accrue à différentes situations. Ainsi le rythme cardiaque normal serait chaotique ce qui permettrait au cœur de réagir efficacement à l'effort [4]. Des modèles de réactions chimiques offrent des régimes chaotiques et l'une d'entre elles, la réaction de **Belousov-Zhabotinsky** [5], présente un attracteur étrange compatible avec le modèle théorique de **Rössler** [6]**.**

---

[1] Les travailleurs de la mer, GF-Flammarion, p. 361, 1980.

.. *« Essayer de vous rendre compte de ce chaos. Il est le récipient universel, réservoir pour les fécondations, creuset pour les transformations. Il amasse, puis disperse ; il dévore, puis crée. Il reçoit tous les égouts de la terre, et il les thésaurise. Il est solide dans la banquise, liquide dans le flot, fluide dans l'effluve, Comme matière il est masse, et comme force il est abstraction. Il égalise et manie les phénomènes. Il se simplifie par l'infini dans la combinaison. C'est à force de mélange et de trouble qu'il arrive à la transparence. La diversité soluble se fond dans son unité. Il a tant d'éléments qu'il est l'identité. Une de ses gouttes, c'est tout lui. Parce qu'il est plein de tempêtes, il devient équilibre. »...*

[2] J. Laskar cité dans Chaos et Déterminisme, édité par A.D. Dalmedico, J.L. Chabert, K. Chemla, Points Seuil, Paris, 1992.

[3] R.M. May, Le chaos en biologie, in La science du désordre, La Recherche, 232, p.p. 588 – 598, 1991.

[4] A.L. Golberger, B.J. West, Annals of New York Academy of Sciences, 504, p. 195, 1987.

[5] J.C. Roux, H. Swinney, Topology of chaos in a Chemical reaction, in Nonlinear Phenomena in Chemical Dynamics, eds. C. Vidal, A. Pacault, Spirnger-Verlag, 1981.

[6] An equation for Continuous Chaos, Physics Letters, 57 A (5), p.p. 397 – 398, 1976.

Nous consacrerons la première partie de notre travail à l'introduction des éléments fondamentaux associés aux systèmes dynamiques en général, et aux systèmes chaotiques en particulier. Ainsi les modèles généraux qui définissent les systèmes dynamiques en temps continu et en temps discret sont présentés en même temps avec les notions d'espace des phases et de trajectoire. A partir de ces définitions on présente la classification des comportements dynamiques puis la modélisation mathématique de la dynamique non linéaire et l'apport de la notion de chaos déterministe à la compréhension de l'évolution des systèmes présentant des dynamiques complexes. Nous illustrons toutes ces notions par des exemples majeurs tels que le pendule amorti, l'application logistique et plus particulièrement le modèle de **Lorenz**, en mettant l'accent sur les outils de quantification et de mesure du Chaos (exposants de Lyapounov quantifiant l'imprédictibilité, dimensions fractales rendant compte de la structure des attracteurs étranges dans l'espace des phases, entropie...).

La seconde partie de ce mémoire est consacrée à l'Application de la théorie du Chaos à la Cryptographie. On sait que dans le domaine de la sécurité informatique, le problème de la génération d'une suite suffisamment aléatoire est central. La recherche de suites permettant de bonnes simulations du hasard, tout en restant déterministes, est un domaine de recherche très actif. Les **générateurs pseudo-aléatoires** utilisés habituellement en informatique produisent, à partir d'un germe (i.e. d'une valeur initiale), une suite récurrente, rapide à générer, ayant de bonnes propriétés statistiques de répartition, et pouvant être reproduite à la demande. Ces générateurs conviennent la plupart des utilisations, mais ils ne peuvent pas être utilisés en cryptographie : il leur manque un caractère d'imprévisibilité.

Or, la théorie du chaos traite justement des systèmes dynamiques rigoureusement déterministes, mais qui présentent un phénomène fondamental d'instabilité appelé **sensibilité aux conditions initiales** qui, modulant une propriété supplémentaire de récurrence, les rend non prédictibles en pratique. C'est la raison pour laquelle un nombre sans cesse croissant de publications scientifiques font intervenir le chaos dans un cryptosystème original. D'autant que, si les possibilités de crypter un texte donné sont aujourd'hui satisfaisantes, il n'en est rien concernant les autres médias (sons, images et vidéo) : les méthodes actuelles de cryptage sont inadaptables aux contraintes imposées par ces supports devenus incontournables.

L'introduction des concepts de cryptosystèmes (classification, objectifs, force) est suivie de

la mise en correspondance des deux théories, celle du chaos et celle de la cryptographie. Nous mettrons en exergue toute l'importance de l'utilisation des systèmes dynamiques chaotiques en cryptographie. Plus particulièrement nous développerons les travaux de **L. Kocarev** et **G. Jakimoski** [24], utilisant le modèle de l'application logistique pour la conception d'un algorithme de cryptage par blocs. Nous donnerons quelques applications de la cryptographie chaotique (cryptage d'image, télécommunications,...).

En plus d'une bibliographie d'articles très récents mais qui ne peut être exhaustive, le présent mémoire s'achève sur un panorama des recherches actuelles sur l'application du chaos en cryptographie prouvant que, outre les propriétés qualitative et quantitative des systèmes dynamiques non linéaires chaotiques permettant la sécurisation des communications, la théorie du Chaos peut encore offrir de nombreuses retombées d'un intérêt certain et insoupçonné pour les systèmes de détection et d'interception ainsi que des applications dans l'accès multiple.

Première partie

La théorie du chaos

Chapitre 1

Systèmes dynamiques et chaos

1.1 Introduction

Les systèmes dynamiques désignent couramment la branche de recherche active des mathématiques, à la frontière de la topologie, de l'analyse, de la géométrie, de la théorie de la mesure et des probabilités. Les systèmes dynamiques n'ont été étudiés en tant que tels qu'assez tardivement. Ils sont néanmoins apparus assez tôt dans l'histoire scientifique puisqu'on peut les reconnaitre dans les premiers travaux de la mécanique donnant lieu à des équations différentielles.

Ainsi historiquement, les premières questions relevant des systèmes dynamiques concernaient la mécanique à une époque où elle était incluse dans l'enseignement des mathématiques. Une des questions majeures qui a motivé la recherche mathématique est le problème de la stabilité du système solaire. Les travaux de **Lagrange** sur le sujet consistèrent à interpréter l'influence des corps autres que le Soleil sur une planète comme une succession de chocs infinitésimaux : ces travaux retrouvent des échos dans le théorème KAM **(Kolmogorov-Arnold-Moser)**.

Les systèmes dynamiques se sont développés et spécialisés au cours du **XIXe** siècle.

En effet, vers la fin de ce siècle le mathématicien, physicien et philosophe français **Henri Poincaré** avait déjà mis en évidence le **phénomène de sensibilité aux conditions initiales** lors de l'étude astronomique du problème des trois corps.

Toujours au **XIXe** siècle**,** le mathématicien russe **Alexandre Lyapunov** effectue des recherches sur la stabilité du mouvement. Il introduit l'idée de mesurer l'écart entre deux tra-

jectoires ayant des conditions initiales voisines, lorsque cet écart évolue exponentiellement on parle de **sensibilité aux conditions initiales.**

Ses travaux, seront très précieux pour étudier certains aspects de la théorie du chaos.

En 1963, le météorologue **Edward Lorenz** expérimentait une méthode lui permettant de prévoir les phénomènes météorologiques. C'est par pur hasard qu'il observa qu'une modification minime des données initiales pouvait changer de manière considérable ses résultats. Lorenz venait de mettre en évidence le phénomène de sensibilité aux conditions initiales. Les systèmes répondant à cette propriété seront à partir de 1975 dénommés systèmes chaotiques. C'est donc au cours des années soixante dix que la théorie du chaos a pris son essor.

Evidemment, les travaux des prédécesseurs de Lorenz ont donc été très importants pour la compréhension du chaos déterministe, mais il faut souligner que ce qui va permettre aux scientifiques une compréhension plus accrue des systèmes chaotiques c'est **l'ordinateur**. En effet, les équations différentielles régissant un système chaotique sont nécessairement non linéaires et, sans ordinateur, leur résolution est en général impossible.

1.2 Définitions et notations

En mathématiques, en physique, en ingénierie un système dynamique est un système **"classique"** qui évolue au cours du temps de façon à la fois :

· causale (c.à.d que son avenir ne dépend que des phénomènes du passé ou du présent).

· déterministe (c.à.d qu'à une **"condition initiale"** donnée à l'instant présent va correspondre à chaque instant ultérieur **"un et un seul état futur"** possible).

Les systèmes "bruités" sont exclus car intrinsèquement stochastiques et relevant de la théorie des probabilités.

On définit un système dynamique par un triplet (X, T, f) constitué de l'espace d'états X, du domaine temporel T, et d'une application de transition d'état $f : X \times T \to X$ qui permet de définir à partir d'un vecteur de conditions initiales l'état du système à tout instant.

1.2.1 Représentations mathématiques des systèmes dynamiques

Un Système dynamique décrit par une fonction mathématique présente deux types de variables : dynamiques et statiques, les variables dynamiques sont les quantités fondamentales qui changent avec le temps, les variables statiques, encore appelés paramètres du système, sont fixes.

· Dans le cas où la composante "temps" est continue le système dynamique est présenté par un système d'équations différentielles de la forme :

$$\frac{dx}{dt} = f\left(x, t, p\right) \ \ où\ x \in \mathbb{R}^n\ et\ p \in \mathbb{R}^r \tag{1.1}$$

· Dans le cas où le temps est discret le système dynamique est présenté par une application itérative.

$$x_{k+1} = f\left(x_k, p\right), x_k \in \mathbb{R}^n et\ p \in \mathbb{R}^r, k = 1, 2, 3, ... \tag{1.2}$$

où p un paramètre, et $t \in T$, le domaine temporel.

· Lorsque le temps t ou l'indice k apparaissent explicitement dans les relations (1.1) et (1.2) le système est dit non-autonome. En général, c'est un inconvénient majeur pour la résolution numérique et il est préférable de s'en affranchir.

· Par un changement de variables approprié [17], on peut transformer un système non-autonome avec $X \in \mathbb{R}^n$ en système autonome avec $X \in \mathbb{R}^{n+1}$.

1.2.2 L'espace des phases

Dès que la dimension n du système dépasse l'unité, il devient assez difficile de se représenter "mentalement" comment le système évolue. L'outil de base pour y palier est l'espace de phases. L'espace des phases est fondamental, on le retrouve au coeur de la formulation de la Mécanique Quantique et la Mécanique Statistique.

Cet espace a été introduit, initialement dans des problèmes de Mécanique Céleste, pour décrire de manière unifiée les équations de la Mécanique des points matériels dans un potentiel et les trajectoires des rayons lumineux dans des milieux non homogènes d'indices variables.

Shrodinger en fera l'usage pour construire le Mécanique ondulatoire.

De même, **Poincaré** utlisera cet espace pour introduire des raisonnements géométriques en Mécanique Céleste et pour étudier le problème des trois corps. Ses travaux seront à la base de la Théorie du Chaos.

Ainsi pour décrire l'évolution d'un système dynamique il est souvent commode d'en faire une representation géométrique. A chaque état du système dynamique est associé un vecteur $\overrightarrow{x}$. Suivre la dynamique du système correspond à observer l'évolution du vecteur $\overrightarrow{x}$ dans un espace vectoriel E appelé espace des phases. Cette évolution est décrite par n équations différentielles munies de conditions initiales. L'évolution suivant t du système se traduit alors par un déplacement du point représentatif dans l'espace de phase, traçant ainsi une trajectoire de phase.

1.2.3 Systèmes conservatifs et Systèmes dissipatifs

En physique, un système conservatif est un système qui conserve l'énergie totale, et possède une intégrale première (ou constante) du mouvement, par contre un système dissipatif est un système qui dissipe de l'énergie, et possède au moins un terme dépendant de la vitesse .

Les systèmes considérés sont des systèmes déterministes, et pour préciser cette définition, on dit qu'un système déterministe est conservatif, si et seulement si la dynamique du système associée à chaque condition initiale x_0 a un et un seul état final $x(t)$, il faut pour cela qu'il existe une application bijective ϕ de l'espace des phases.

$$\phi : I \times \mathbb{R} \to I$$
$$(x,t) \to \phi_t(x) = \phi(x,t)$$

qu'on appelle **flot** et qui possède les propriétés suivantes :

$$\phi_t(x_0) = x_0$$
$$\phi_{t+s}(x_0) = \phi_t(\phi_s(x_0)) \text{ pour tous } t, s \in \mathbb{R}$$

Si le système est dissipatif, le flot n'est pas bijectif et il existe en général un (ou plusieurs) attracteurs dans l'espace des phases du système.

Exemple 1.1 : cas continu (L'oscillateur de Duffing)

$$\begin{cases} \frac{dx}{dt} = y \\ \frac{dy}{dt} = x - x^3 - \delta y + \gamma \cos \omega t \end{cases}$$

Où δ, γ, ω sont des paramètres physiques réels (variables statiques)

L'espace des phases est : $\mathbb{R}^2$, l'espace des paramètres est : $\mathbb{R}^3$. Ce système est non linéaire, non autonome, il peut être dissipatif ou conservatif (suivant le mouvement avec ou sans frottement).

Exemple 1.2 : cas discret (l'application de Hénon)

$$\begin{cases} x_{k+1} = y_k + 1 - a x_k^2 \\ y_{k+1} = b x_k \end{cases}$$

Où a, b sont des paramètres réels, l'espace des phases est : $\mathbb{R}^2$, l'espace des paramètres est : $\mathbb{R}^2$.

1.3 Systèmes dynamiques continus

1.3.1 Points fixes

Définition 1.1 :

Un point fixe (ou critique ou singulier, ou point stationnaire) de l'équation $\dot{x} = F(x)$ est un point $\bar{x}$ de l'espace des phases vérifiant $F(\bar{x}) = 0$.

Remarque 1.1 :

Par un changement de variable $z = x - \tilde{x}$ on peut ramener le point à l'origine (0).

1.3.2 Points limites

Définition 1.2 :

Un point $a \in I$ est un point $\omega-$limite d'une trajectoire $x(x_0, t)$ s'il existe une suite $t_n \to +\infty$ tel que :

$$\lim_{n \to \infty} \varphi_{t_n} = a$$

où φ_t est le flot du système $\frac{dx}{dt} = f(x)$, $x \in \mathbb{R}^n$, $f \in C^k(I), I \subseteq \mathbb{R}^n$, et $x(x_0, t)$ est une solution de ce système avec $x(0) = x_0$.

Définition 1.3 :

Un point $b \in I$ est un point $\alpha-$limite d'une trajectoire $x(x_0, t)$ s'il existe une suite $t_n \to -\infty$ tel que :

$$\lim_{n\to\infty} \varphi_{t_n} = b$$

Définition 1.4 :

L'ensemble des points $\alpha-$limites (resp $\omega-$limite) est désigné par $\alpha(x)$ (resp $\omega(x)$), et on definit l'ensemble limite de $x(x_0, t)$ par l'ensemble :

$$\alpha(x) \cup \omega(x)$$

1.3.3 Attracteurs et bassin d'attraction

Ensemble invariant

Définition 1.5 :

Un ensemble $M \subset I$ est dit invariant par un champ de vecteur si toute solution $x(t)$ du système différentiel associe au champ de vecteurs issu de M vérifie $x(t) \subset M$ pour tout t pour lequel cette solution est définie.

Attracteurs

Définition 1.6 :

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

Mathématiquement, l'ensemble A est un attracteur si :

· Pour tout voisinage U de A, il existe un voisinage V de A tel que toute solution $x(x_0, t) = \varphi_t(x_0)$ restera dans U si $x_0 \in V$.

· $\cap\varphi_t(V) = A$, $t \geq 0$

· Il existe une orbite dense dans A.

Définition 1.7 :

Un attracteur possède les propriétés suivantes :

1− Un sous ensemble borné A de l'espace est de volume nul invariant par le flot. Autrement dit, tout point de l'espace d'états qui appartient à un attracteur demeure à l'intérieur de cet attracteur pour tout t.

2− Il existe un ensemble $B \supset A$, tel que pour voisinage de A, la trajectoire qui prend son origine dans B se trouve au bout d'un temps fini dans ce voisinage de A. Cette "zone d'influence" est le basin d'attraction, c'est l'ensemble :

$$W = \cup \varphi_t (V), t < 0$$

3− Un attracteur est indécomposable c'est-à-dire que la réunion de deux attracteurs n'est pas un attracteur.

Les différents types d'attracteurs

Il existe deux type attracteurs : les attracteurs réguliers et les attracteurs étranges ou chaotiques.

1− Attracteurs réguliers

Les attracteurs réguliers caractérisent l'évolution de systèmes non chaotiques, et peuvent être de trois sortes.

· **Le point fixe :** C'est le plus simple attracteur, le système évolue vers un état de repos (point).

· **Le cycle limite périodique :** Il peut arriver que la trajectoire de phase se referme sur elle-même. L'évolution temporelle est alors cyclique, le système présentant des oscillations permanentes. Dans un système physique dissipatif, cela exige la présence d'un terme de forçage dans les équations qui vient compenser en moyenne les pertes par dissipation.

· **Le cycle limite pseudo-périodique :** C'est presque un cas particulier du précédent. La trajectoire de phase ne se referme pas sur elle-même, mais s'enroule sur une variété de dimension 2 (par exemple un tore).

2− Attracteurs étranges

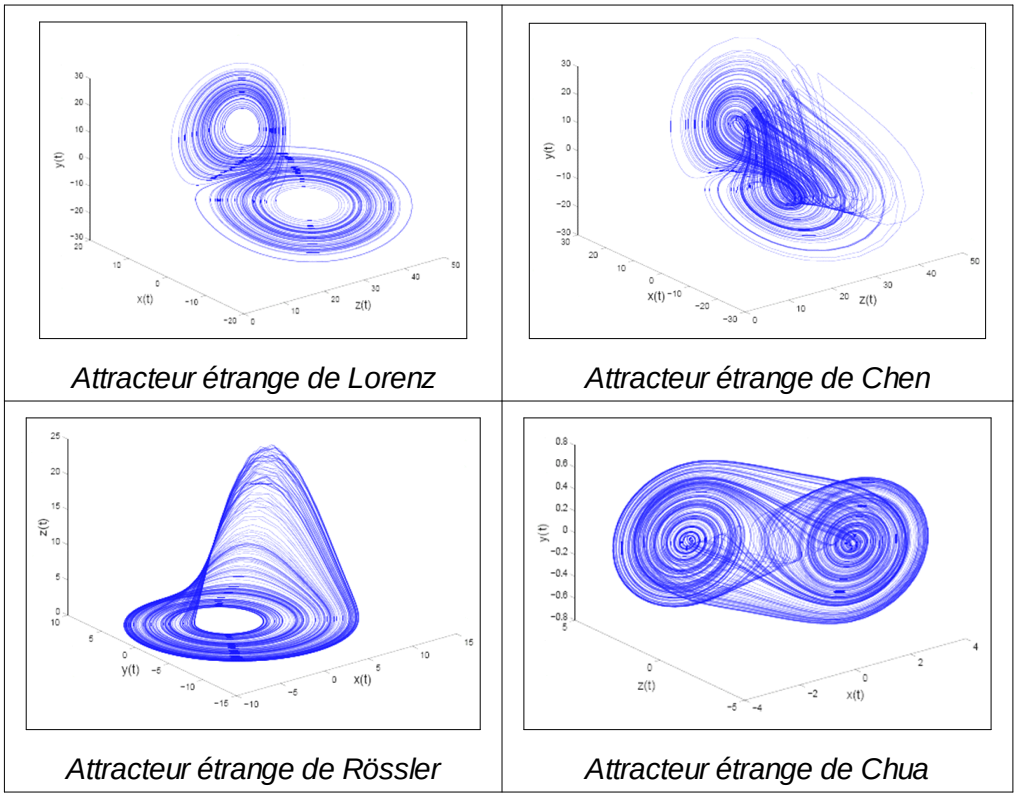


FIG. 1-1 – *Quelques attracteurs étranges*

il s'agit d'ensembles dans l'espace des phases compacts, fermés, dans lesquels on retrouve des trajectoires chaotiques, dont l'une des caractéristiques essentielles est la **SCI**. (les trajectoires issues de conditions initiales proches s'écartent exponentiellement). La coexistence de l'attraction, qui implique le resserrement des trajectoires, avec la **SCI**, qui implique leur écartement, s'explique par le concept d'hyperbolicité de l'attracteur : l'attraction s'opère dans une direction, et la divergence dans une autre. La surface contenant les trajectoires divergentes est appelée **variété instable**, alors que celle contenant les trajectoires convergentes est appelée **variété stable**. Leur dimension est non entière et leur structure est fractale. Par exemple, l'attracteur de Rössler, l'attracteur de Lorenz, l'attracteur de Chen, l'attracteur de Chua, figure (1.1) .

1.3.4 Etude qualitative des systèmes dynamiques

L'étude qualitative d'une équation differentielle permet de s'affranchir de la détermination explicite de la solution et consiste à analyser le comportement des solutions particuliérement au voisinage de points d'équilibre.

Cette approche (locale) est avérée très féconde surtout lorsqu'elle est appliquée à des systèmes d'équations d'ordre élevé et non linéaires. Elle se base sur la linéarisation au voisinage des points d'équilibre.

Au début du siècle, sous l'impulsion d'Henri Poincaré ; cette démarche fut à l'origine du renouveau de l'étude des systèmes dynamiques et a donné naissance à la Théorie du Chaos.

Linéarisation des systèmes dynamiques

Considérons le système dynamique non linéaire défini par :

$$\dot{x} = F(x),\ x = \begin{pmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_n \end{pmatrix},\ F = \begin{pmatrix} f_1 \\ f_2 \\ . \\ . \\ . \\ f_n \end{pmatrix} \tag{1.3}$$

et soit x_0 un point fixe (d'équilibre) de ce système.

Supposons qu'une petite perturbation $\epsilon(t)$ soit appliquée au voisinage du point fixe. La fonction F peut être développée en série de Taylor au voisinage de point x_0 comme suite :

$$\dot{\epsilon}(t) + \dot{x}_0 = F(\dot{x}_0 + \dot{\epsilon}(t)) \simeq F(x_0) + J_F(x_0).\epsilon(t) \tag{1.4}$$

avec $J_F(x_0)$ est la matrice Jacobienne de la fonction F définit par :

$$J_F(x_0) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \ldots & \frac{\partial f_1}{\partial x_n} \\ \ldots & \ldots & \ldots & \ldots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \ldots & \frac{\partial f_n}{\partial x_n} \end{pmatrix}_{x=x_0} \tag{1.5}$$

Comme $F(x_0) = x_0$, alors l'équation (1.4) redevient :

$$\dot{\epsilon}(t) = J_F(x_0).\epsilon(t) \tag{1.6}$$

L'écriture (1.6) veut dire que le système (1.3) est linéarisé.

Théorème de Hatmann-Grobman

Considérons le système dynamique (1.3).

Soit x_0 un point d'équilibre du système (1.3) et soit $J_F(x_0)$ la matrice Jacobienne au point x_0, alors on a le thèorème suivant :

Théorème 1.1 :

Si $J_F(x_0)$ admet des valeurs propres non nulles ou imaginaires pures, alors il existe un homéomorphisme qui transforme les orbites du flot non linéaire vers celles du flot linéaire dans certain voisinage U de x_0.

Ce théorème va nous permettre de lier la dynamique du système non linéaire (1.3) à la dynamique du système linéarisé (1.6).

Classification des points fixes

Il s'agit de distinguer ces points fixes par la nature des valeurs propres de la matrice jacobienne (1.5) du système linéarisé (1.6) associé au système différentiel initial (1.3) en ce point.

Pour cette raison on va supposer que les valeurs propres de la matrice (1.5) sont définies par :

$$\lambda_i = \omega_i + j\sigma_i, i = 1, 2, ...n$$

· Lorsque $\omega_i = 0$ pour $i = 1, 2, ..., n$ le point fixe est dit **hyperbolique**.

La solution $\epsilon(t)$ du système linéairisé s'écrit à partir d'une base des fonctions indépendantes :

$$\epsilon(t) = \sum_{i=1}^{n} C_i e^{\lambda_i t}.V^i$$

Où V^i représente le vecteur propre associé à λ_i et $C_i \in \mathbb{R}$. depend des conditions initiales.

Donc les valeurs propres λ_i définissent l'état de stabilité. Et on va citer les natures de ces points fixes en étudiant la nature des λ_i.

1− Si $\omega_i < 0$ pour $i = 1, 2, ..., n$, le point fixe est asymptotiquement stable : $\lim y(t) = 0, t \to +\infty$. On dit que le point est un **"puits" (foyer)** si $\sigma_i \neq 0$ pour $i = 1, 2, ..., n$ un **"noeud"** si $\sigma_i = 0$ pour $i = 1, 2, ..., n$.

2− Si $\omega_i > 0$ pour $i = 1, 2, ..., n$, le point fixe est instable. On dit que le point est une **"source"** si $\sigma_i \neq 0$ pour $i = 1, 2, ..., n$,et un **"noeud"** si $\sigma_i = 0$ pour $i = 1, 2, ..., n$.

3− Si $\omega_j > 0$ pour $j = 1, 2, ..., p$ avec $p < n$ et $\omega_j < 0$ pour $i \neq j$, la solution est instable et le point est un **"col"**.

· S'il n'y a pas de valeur propre nulle, on a un point **"selle"**, figure (1.2) .

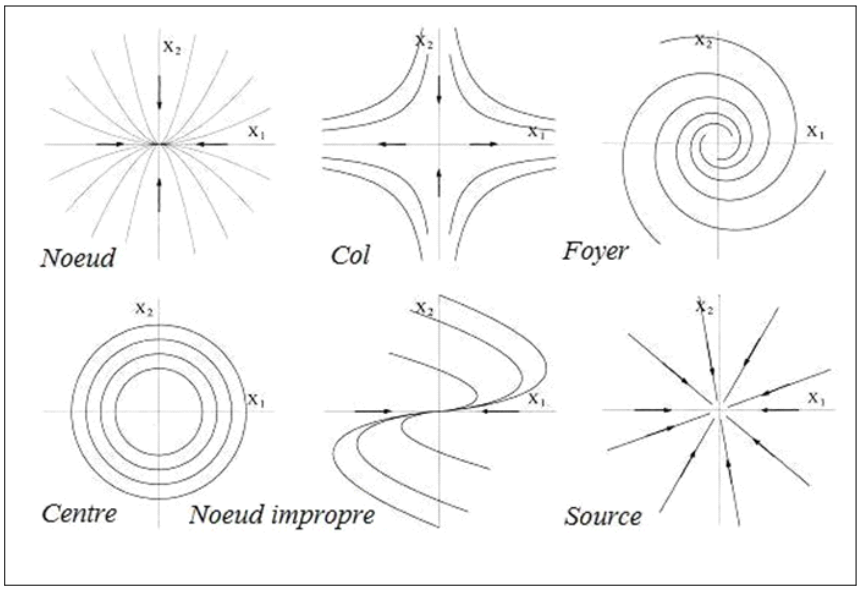


FIG. 1-2 – *Classification des points d'équilibre dans* $\mathbb{R}^2$

1.3.5 Etude de stabilité

Stabilité au sens de Lyapunov

Soit le système dynamique suivant :

$$\frac{dx}{dt} = f(x,t) \tag{1.7}$$

avec f une fonction non linéaire.

Définition 1.8 :

Le point d'équilibre x_0 du système (1.7) est :

· Stable si :

$$\forall \varepsilon > 0, \exists \delta > 0 : \|x(t_0) - x\| < \delta \Longrightarrow \|x(t, x(t_0)) - x_0\| < \varepsilon, \forall t \geq t_0 \tag{1.8}$$

· Asymptotiquement stable si :

$$\forall \delta > 0 : \|x(t_0) - x_0\| < \delta \Longrightarrow \lim_{t \to \infty} \|x(t, x(t_0)) - x_0\| = 0$$

· Exponentiellement stable si :

$$\forall \varepsilon > 0, \exists \delta > 0 : \|x(t_0) - x\| < \delta \Longrightarrow \|x(t, x(t_0)) - x_0\| < a\|x(t_0) - x\| \exp(-bt), \forall t > t_0$$

· Instable si l'équation (1.8) n'est pas satisfaite.

Première méthode de Lyapunov (méthode indirecte)

La première méthode de Lyapunov est basée sur l'examen de la linéarisation autour du point d'équilibre x_0 du système (1.7). Plus précisément, on examine les valeurs propres λ_i de la matrice jacobienne évaluée au point d'équilibre. Selon cette méthode, les propriétés de stabilité de x_0 s'expriment comme suit :

· Si toutes les valeurs propres de la matrice jacobienne ont une partie réelle strictement négative, x_0 est exponentiellement stable.

· Si la matrice jacobienne possède au moins une valeur propre à partie réelle strictement positive, x_0 est instable.

Remarque 1.2 :

Cette méthode ne permet pas de dire si l'équilibre est stable ou instable quand la matrice jacobienne comporte au moins une valeur propre nulle, et aucune valeur propre avec partie réelle strictement positive. Dans ce cas, les trajectoires du système convergent vert un sous-espace (une variété) dont la dimension est le nombre de valeurs propres nulles de la matrice jacobienne, et la stabilité de l'équilibre peut être étudié dans ce sous-espace par la seconde méthode.

Seconde méthode de Lyapunov (méthode directe)

La première méthode de Lyapunov est simple à appliquer mais ne permet d'analyser la stabilité des équilibres que très partiellement. En outre elle ne donne aucune indication sur la taille des bassins d'attraction. La seconde méthode est plus difficile à mettre en œuvre mais, en contrepartie, elle est d'une portée beaucoup plus générale. Elle est basée sur la définition d'une fonction particulière, notée $V(x)$ est appelée fonction de Lyapunov, qui est décroissante le long des trajectoires du système à l'intérieur du bassin d'attraction.

Théorème 1.2 :

Le point d'équilibre x_0 du système (1.7) est stable si il existe une fonction

$V(x) : D \to \mathbb{R}$ continuellement différentiable ayant les propriétés suivantes :

$1-$ D est un ouvert de $\mathbb{R}^n$ et $x_0 \in D$.

$2-$ $V(x) > V(x_0)$ $\forall x \neq x_0$ dans D.

$3 - V(x) \leq 0$ $\forall x \neq x_0$ dans D.

Il n'y a aucune méthode pour trouver une fonction de Lyapunov. Mais en mécanique et pour les systèmes électriques on peut souvent utiliser l'énergie totale comme fonction de Lyapunov.

Théorème de la variété centrale

Soit :

$$\frac{dx}{dt} = f(x, c) \tag{1.9}$$

un systéme dynamique non linéaire, x_0 son point d'équilibre qu'on peut ramener à l'origine par le changement de variable :

$$\xi = x - x_0$$

et soit J la matrice jacobienne d'ordre n associé au système (1.9) après sa linéarisation au

voisinage du point fixe (aprés avoir considéré une petite perturbation ξ au voisinage de point fixe).

$$\frac{d\xi}{dt} = J\xi$$

Soient :

· $\lambda_1, \lambda_2, ..., \lambda_s$ les valeurs propres de la matrice jacobienne J dont la partie réelle est négative.

· $u_1, u_2, ..., u_i$ les valeurs propres de la matrice J dont la partie réelle est positive.

· $s_1, s_2, ..., s_c$ les valeurs propres dont la partie réelle est nulle, avec $s + i + c = n$.

Et soient :

· E^s le sous espace vectoriel de dimension s engendré par $\{\lambda_1, \lambda_2, ..., \lambda_s\}$.

· E^i le sous espace vectoriel de dimension i engendré par $\{u_1, u_2, ..., u_i\}$.

· E^c le sous espace vectoriel de dimension c engendré par $\{s_1, s_2, ..., s_c\}$.

avec

$$E^n = E^s \oplus E^i \oplus E^c$$

On a le théorème suivant :

Théorème 1.3 :

Il existe des variétés de classe C^r : stable W^s, instable W^i, et centrale W^c tangentes respectivement à E^s, E^i et E^c en x_0.Ces variétés sont invariantes, par rapport au flot de système (1.9).

Variété centrale dépendant d'un paramètre

On applique une petite perturbation ε sur le système (1.9), donc le résultat sera un système dynamique dépendant d'un paramètre ε, et supposons que par une certaine transformation on peut ramener le système (1.9) à un système de la forme :

$$\begin{cases} \dot{x} = A_1 x + f(x, y, z, \varepsilon) \\ \dot{y} = A_2 y + g(x, y, z, \varepsilon) \\ \dot{z} = A_3 + m(x, y, z, \varepsilon) \\ \dot{\varepsilon} = 0 \end{cases} \tag{1.10}$$

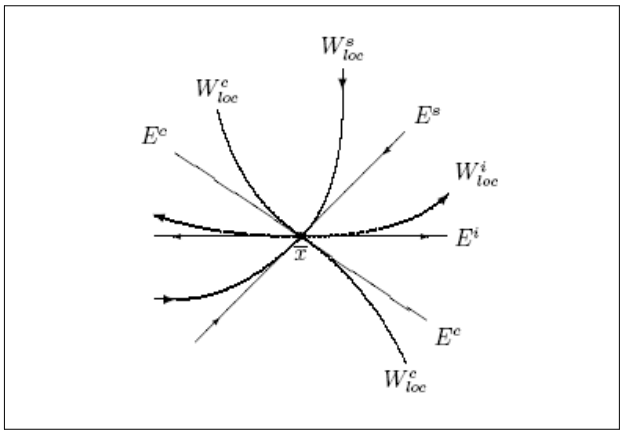


FIG. 1-3 – *Les sous-variétés invariantes autour de point d'équilibre* $\bar{x}, W^s_{loc}$ *et* W^i_{loc} *les sous-variétés stable et instable et* W^c_{loc} *la sous-variété centrale*

La variété centrale au voisinage de $(0,0,0,0)$ est alors donnée par :

$$y = h_1(x,\varepsilon), z = h_2(x,\varepsilon)$$

Après un simple calcul, et après avoir appliqué le développement de Taylor sur $h_1$et h_2, on peut alors écrire le système (1.10) sous la forme :

$$\begin{cases} \dot{x} = A_1 x + f(x, h_1(x,\varepsilon), h_2(x,\varepsilon), \varepsilon) \\ \dot{\varepsilon} = 0 \end{cases} \tag{1.11}$$

Le théorème suivant permet de lier la dynamique du système (1.11) à celle du système (1.10).

Théorème 1.4 :

Si l'origine $x_0 = 0$, du système (1.11) est asymptotiquement stable (resp, instable), alors l'origine du système (1.10) est aussi asymptotiquement stable (resp, instable).

1.3.6 Bifurcations

Les changements qualitatifs du portrait de phases d'un système dynamique dépendant de paramètres sont appelés bifurcations. Pour les systèmes continus dérivant d'un potentiel, le mathématicien **René Thom** emploie, au lieu de bifurcation, le terme catastrophe, terme qui a

connu une fortune médiatique importante. Pour les valeurs des paramètres auxquelles de tels changements qualitatifs apparaissent, valeurs dites de bifurcation, et la construction du portrait de phases nécessite des outils adaptés. L'étude des bifurcations dites locales, c'est à dire relatives à un point d'équilibre d'un système continu ou à un point fixe d'un système discret repose sur la théorie de **Landau** et, en s'appuyant sur le diagramme de bifurcation, sur la méthode de la sous-variété centrale qui permet d'isoler la partie non hyperbolique, dite centrale, du système, et sur la méthode des formes normales de Poincaré où ne subsistent que les vraies non linéarités, c'est à dire celles que l'on ne peut pas faire disparaitre par changement régulier de coordonnées.

Soit le système non linéaire :

$$\frac{dx}{dt} = f(x, t, \mu) \tag{1.12}$$

où $x \in I \subseteq \mathbb{R}^n$, $\mu \in \mathbb{R}^k$, $f \in C^r$.

Définition 1.9 :

Une bifurcation est un changement qualitatif de la solution x_0 du système (1.12) lorsqu'on modifie μ, et d'une manière plus précise la disparition ou le changement de stabilité et l'apparition de nouvelles solutions. La codimension d'une bifurcation est la plus petite dimension de l'espace des paramètres telle que la bifurcation soit persistante.

Les bifurcation de codimension un sont quatre types de bifurcations correspondant tous à des comportements génériques.

Bifurcation nœud-col

Une fonction linéaire ne change pas le nombre de racines. Le polynôme le plus simple qui change de nombre de racines en fonction du paramètre μ est le polynôme quadratique $f(x) = \mu - x^2$, comme celui de la figure suivante :

Considérons le système (1.12). Si on peut réécrire la fonction f sous la forme :

$$f(x) = \mu - x^2 \tag{1.13}$$

Nous appelons la fonction (1.13) la forme normale de la bifurcation nœud-col.

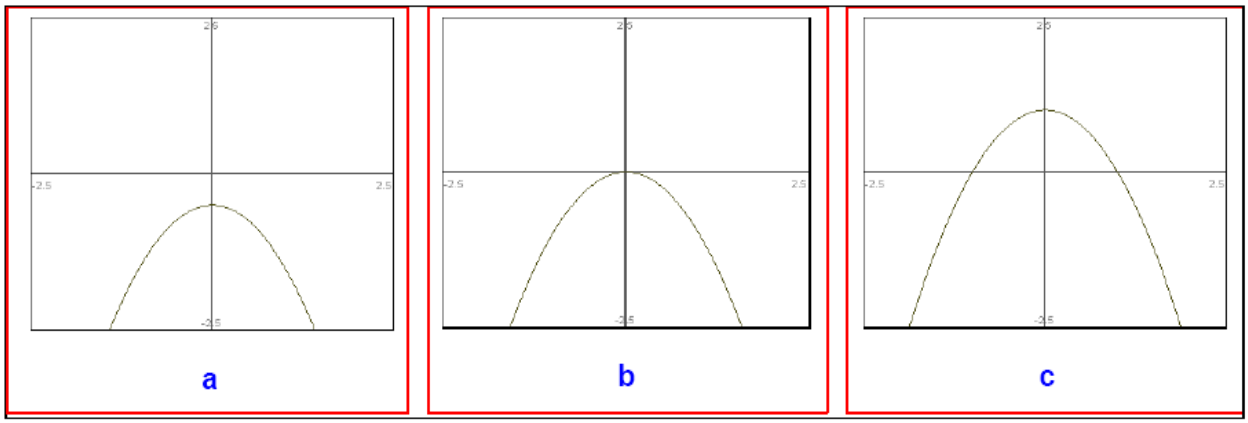


FIG. 1-4 – *Variation des racines de* $f(x,\mu)$ *dans a* $\mu<0$ *dans b* $\mu=0$ *et dans c* $\mu>0$

Etudions le comportement de l'équation (1.13), les points fixes de cette dernière sont :

$$\tilde{x}_{\pm}=\pm\sqrt{\mu}$$

qui existent seulement pour $\mu>0$, leur stabilité est déterminée par :

$$f'(\tilde{x}_{\pm})=-2\tilde{x}_{\pm}=-2(\pm\sqrt{\mu})=\pm\sqrt{\mu}$$

selon les signes de $f'(\tilde{x})$, on voit que $\bar{x}_{+}=\sqrt{\mu}$ est stable, tandis que $\bar{x}_{-}=-\sqrt{\mu}$ est instable.

Remarque 1.3 :

Même étude faite lorsque :

$$f(x,\mu)=-\mu-x^2$$
$$f(x,\mu)=+\mu+x^2$$
$$f(x,\mu)=-\mu+x^2$$

Mais dans tous les cas, il y a une transition à $\mu=0$ entre existence d'aucun point fixe et de deux points fixes dont un est stable et l'autre instable.

La figure (1.5) présente ce que on' appelle le diagramme de bifurcation (la variation du point d'équilibre en fonction de paramètre μ pour le cas $f(x,\mu)=\mu+x^2$).

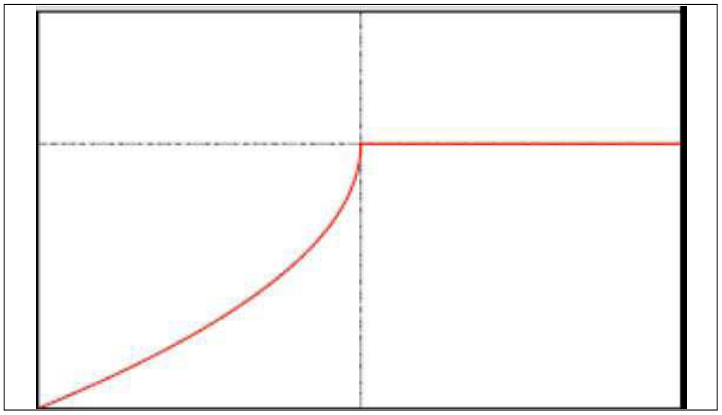


FIG. 1-5 – *Diagramme de Bifurcation nœud-col*

Bifurcation fourche

Si on peut réduire $f(x,\mu)$ à un polynôme cubique a ces quatre cas :

$$f(x,\mu) = \mu x - x^3 \tag{1.14}$$

$$f(x,\mu) = \mu x + x^3$$

$$f(x,\mu) = -\mu x + x^3$$

$$f(x,\mu) = -\mu x - x^3$$

L'´equation (1.14) s'appelle la forme normale d'une bifurcation fourche supercritique.

Ses points fixes :

$$\bar{x}\left(\mu - \bar{x}^2\right) = 0 \Longrightarrow \begin{cases} \bar{x} = 0 \text{ pour tout } \mu \\ \bar{x} = \pm\sqrt{\mu} \text{ pour } \mu > 0 \end{cases}$$

Stabilité de ces points fixes :

$$f'(\bar{x}) = \mu - 3\bar{x}^2 = \begin{cases} \mu \text{ pour } \bar{x} = 0 \\ \mu - 3\mu = -2\mu \text{ pour } \bar{x} = \pm\sqrt{\mu} \end{cases} \tag{1.15}$$

Le point fixe $\bar{x} = 0$ est donc stable pour $\mu < 0$ et devient instable à $\mu = 0$, quand les branches de nouveaux points fixes $\bar{x} = \pm\sqrt{\mu}$ sont créées. Ces nouveaux points fixes sont toujours stables quand ils existent.

Pour (1.15) qui est la forme normale d'une bifurcation fourche souscritique, le même calcul conduit à :

$$\bar{x}\left(\mu - \bar{x}^2\right) = 0 \Longrightarrow \begin{cases} \bar{x} = 0 \text{ pour tout } \mu \\ \bar{x} = \pm\sqrt{-\mu} \text{ pour } \mu < 0 \end{cases}$$

$$f'(\bar{x}) = \mu + 3\bar{x}^2 = \begin{cases} \mu \text{ pour } \bar{x} = 0 \\ \mu + 3(-\mu) = -2\mu \text{ pour } \bar{x} = \pm\sqrt{\mu} \end{cases}$$

Comme pour le cas supercritique, le point fixe $\bar{x} = 0$ est stable pour $\mu < 0$ et devient instable à $\mu = 0$.

Mais contrairement au cas supercritique, les autres points fixes $\pm\sqrt{\mu}$ existent dans la région où $\bar{x} = 0$ est stable, et sont toujours instables.

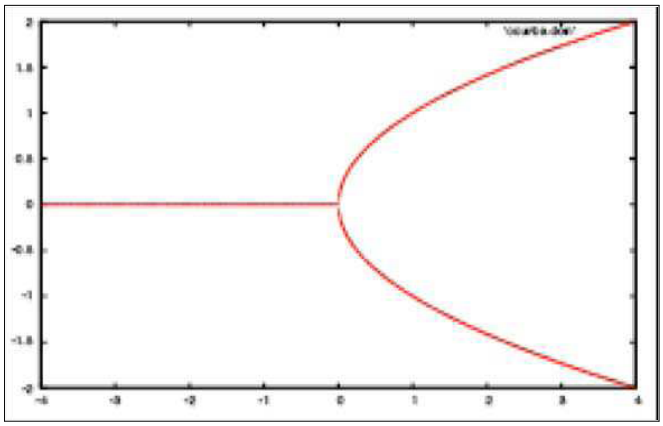


FIG. 1-6 – *Diagramme de bifurcation Fourche*

Bifurcation transcritique

Si f est contrainte à ne pas avoir de terme constant, le développement limité mène à la forme normale d'une bifurcation transcritique.

$$\dot{x} = \mu x - x^2$$

L'analyse usuelle donne :

$$\bar{x}\,(\mu - x) = 0 \Longrightarrow \begin{cases} \bar{x} = 0 \\ \bar{x} = \mu \end{cases}$$

$$f'(\bar{x}) = \mu - 2\bar{x} = \begin{cases} \mu \text{ pour } \bar{x} = 0 \\ -\mu \text{ pour } \bar{x} = \mu \end{cases}$$

Donc $\bar{x} = 0$ est stable pour $\mu < 0$, instable pour $\mu > 0$, tandis que $\bar{x} = \mu$ fait le contraire : ces points fixes échangent simplement leur stabilité.

Bifurcation de Hopf

Contrairement aux bifurcations précédentes qui conduisent à des solutions stationnaires, la bifurcation de Hopf donne naissance à des solutions oscillantes ; l'espace des phases a maintenant deux composantes et s'écrit dans le plan complexe.

Forme normale :

$$\frac{dZ}{dt} = \mu Z - |Z|^2 Z$$

En posant $\mu = \mu_r + i\mu_I$ et $Z = Xe^{i\theta}$, on obtient alors :

$$\begin{cases} \frac{dX}{dt} = \mu_r X - X^3 \\ \frac{dX}{dt} = \mu_I \end{cases}$$

Nous obtenons donc une bifurcation fourche pour l'amplitude tandis que la phase tourne à la vitesse μ_I. La solution est donc périodique et les trajectoires décrivent une spirale attirée vers une courbe asymptotique nommée : cycle limite. Naturellement la bifurcation de Hopf peut être également sous critique si le coefficient du terme $|Z|^2 Z$ est de signe positif, il faut alors un

terme négatif en $|Z|^4 Z$ pour obtenir une saturation non-linéaire.

Selon Landau la bifurcation d'un comportement stationnaire (point fixe) vers un comportement périodique (cycle limite) puis bipériodique (un tore) constitue les premières étapes de la transition vers la turbulence, et le chaos qui est depuis longtemps synonyme de désordre, de confusion et s'oppose à l'ordre. De nombreux chercheurs en sciences se sont intéressés aux mouvements dits chaotiques. Ils ont confirmé que, contrairement à ce que la pensée déterministe, martèle depuis des lustres, il se pourrait qu'il y ait de l'équilibre dans le déséquilibre, de l'organisation dans la désorganisation.

1.4 Systèmes dynamiques discrets

1.4.1 Systèmes dynamiques discrets

Soit $f : D \to D$, $D \subseteq \mathbb{R}^n$ une application continue (ou une transformation), f^k désigne la k ^{ième} itérée de f, c'est-à-dire :

$$f^0(x) = x, f^1(x) = f(x), f^2(x) = f(f(x)), ..., f^k(x) = f\left(f^{k-1}(x)\right)$$

Dans la pratique $x_0, x_1 = f(x_0), x_2 = f^2(x_0), ...$représentent les valeurs d'une certaine quantité au temps $0, 1, 2, ...$

Ainsi la valeur de la quantité au temps $k+1$ est fonction de sa valeur au temps k.

L'application f est appelée un **système dynamique discret**.

1.4.2 Orbites ou trajectoires

L'**orbite positive** de x par le système dynamique f est définie par :

$$O_+^f = \left\{f^k(x), n \in \mathbb{N}\right\}$$

Si f est bijectif, on définit l'**orbite** de x par :

$$O^f = \left\{f^k(x), n \in \mathbb{Z}\right\}$$

Ainsi que l'**orbite négative** :

$$O_{-}^{f} = \left\{ f^{-k}(x), n \in \mathbb{N} \right\}$$

1.4.3 Points fixes

Un point $x \in D$ est un point fixe de f si :

$$f^{k}(x) = x, k = 0, 1, 2, ...$$

Si de plus la matrice jacobienne $Df(x)$ n'a pas de valeurs propres dont le module soit égal à un, x est un point fixe **hyperbolique**. Si tous les modules des valeurs propres de $Df(x)$ sont égaux à un, x est point fixe **elliptique**.

1.4.4 Points périodiques et p-cycles

S'il existe $n \geq 1$, tel que $f^{n}(x) = x$, on dit que x est un point **périodique**. La **période** d'un point périodique x est le plus petit entier $n \geq 1$ tel que :

$$f^{n}(x) = x$$

Un ensemble $\{x_0, x_1, ..., x_{p-1}\}$ forme un **cycle** d'ordre p (ou une **orbite périodique** d'ordre p, ou encore un $p-$**cycle**), si :

$$f(x_i) = x_{i+1}, \text{pour } i = 0, 1, 2, ..., p-1, \text{et } f(x_{p-1}) = x_0$$

Autrement dit, chaque point d'un cycle d'ordre p est un point fixe pour f^{p},où $f^{p}(x_i) = x_i$ pour $i = 0, 1, 2, ..., p-1$, et n'est pas un point fixe pour f^{k} si $k < p$.

1.4.5 Etude de stabilité

L'étude du comportement d'un système dynamique discret, correspond à l'étude de stabilité des points fixes et des points périodiques.

Les deux théorèmes suivants donnent respectivement l'existence et l'unicité des points fixes.

Théorème de Brouwer

Toute application continue $f : \bar{B}^n \to \bar{B}^n$ avec $\bar{B}^n = \{x \in \mathbb{R}^n / \|x\| \leq 1\}$, admet un point fixe c'est-à-dire l'équation $f(x) = x$ admet une solution dans $\bar{B}^n$.

Théorème de contraction de Banach

Soit $f : \bar{B}^2 \to \bar{B}^2$ application continue, où $\bar{B}^2$ est le disque unitaire fermé ; $\bar{B}^2 = \left\{x \in \mathbb{R}^2 / \|x\| \leq 1\right\}$.

Supposons que :

$$|f(x_1) - f(x_2)| < \lambda |x_1 - x_2|$$

pour tout vecteur $x_{i,j} \in \bar{B}^2$ et un certain $0 < \lambda < 1$. Alors il existe un point fixe unique $\bar{x} \in \bar{B}^2$. De plus on a :

$$\lim_{n \to +\infty} f^n(x) = \bar{x} \text{ pour tout } x \in \bar{B}^2$$

Stabilité du point fixe

· Un sous ensemble A de D est invariant par f si $f(A) = A$.

· Un sous ensemble compact fermé A de D est un **attractif** ou est **attracteur** si A est invariant par f, et s'il existe un voisinage V de A tel que pour $x_0 \in V$, l'orbite de x_0 est une suite qui converge vers A. Le voisinage V est appelé le **bassin d'attraction** de A et on a :

$$A = \cap_{k=1}^{\infty} f^k(V)$$

· Le sous ensemble A est **répulsif** ou **instable** s'il existe un voisinage V de A tel que pour tout $x_0 \in V$, l'orbite de x_0 s'éloigne de A (ou de façon équivalente : si A est un attracteur pour f^{-1}).

· Un attracteur A est fractal (ou un attracteur étrange) si l'orbite de x est dense dans A pour tout $x \in A$ et est sensible aux conditions initiales.

L'attracteur le plus simple est le point fixe, il peut être attractif ou répulsif.

Définition 1.10 : stabilité

Un point fixe $\bar{x} \in D$ est stable, si :

$$\forall \varepsilon > 0, \exists \delta > 0 \, |x_0 - \bar{x}| < \delta \Longrightarrow \forall k \geq 0 : |x_k - \bar{x}| < \varepsilon$$

En dimension un, $f : \mathbb{R} \to \mathbb{R}$ est la pente $m = f'(\bar{x})$ de la tangente au point fixe $\bar{x}$ qui détermine le type de point fixe.

Théorème 1.5 :

Pour $f : \mathbb{R} \to \mathbb{R}$ le point fixe est :

1− attractif (ou stable) si $|m| < 1$;

2− répulsif (ou instable) si $|m| > 1$;

3− indifférent si $|m| = 1$;

4− super attractif (ou super stable) si $m = 0$.

m s'appelle le **multiplicateur** de f au point $\bar{x}$.

En dimension n, pour décider si un point fixe $\bar{x}$ est attractif ou non, il faut calculer les valeurs propres de la matrice jacobéenne $Df(x) = J(x)$.

Théorème 1.6 **:**

Si toutes les valeurs propres de $Df(x) = J(x)$ sont à l'intérieur du disque unité, x est stable. Si une de ces valeurs propres a un module plus grand que un, x est instable.

Stabilité des points périodiques

Une orbite périodique est un attracteur si chacun de ses points est un attracteur. Comme les points périodiques d'ordre p sont des points fixes de f^p, alors le théorème suivant est une généralisation du théorème (1.6).

Théorème 1.7 :

Soit x le point périodique d'un cycle d'ordre p. Si le spectre de la matrice $Df^p(x)$ est contenu à l'intérieur du cercle unité, le cycle est stable ; si une des valeurs propres a un module plus grand que un, le cycle est instable.

En dimension un, si $\{x_0, x_1, ..., x_{p-1}\}$ est un cycle d'ordre p, les dérivées $(f^p)'(x_i)$ pour $i = 0, 1, 2, ..., p-1$ sont égales. En effet, la dérivée de f^p au point x_0 s'écrit :

$$(f^p)'(x_0) = f'(f(...f(x_0)))...f'(f(x_0))f'(x_0) = f'(x_{p-1})...f'(x_1)f'(x_0)$$

Mais $x_0 = x_p$. On en déduit que cette valeur $(f^p)'(x_0)$ est la même pour toutes les dérivées

$(f^p)'(x_i), i = 0, 1, 2, ..., p-1$:

$$m_p = (f^p)'(x_0) = ... = (f^p)'(x_{p-1})$$

Cette valeur commune m_p est appelée le **multiplicateur** du cycle $\{x_0, x_1, ..., x_{p-1}\}$, cette dernière détermine le type du cycle.

Théorème 1.8 :

Pour $f : \mathbb{R} \to \mathbb{R}$, le cycle $\{x_0, x_1, ..., x_{p-1}\}$ est :

1− Attractif (ou stable) si $|m_p| < 1$;

2− Répulsif si $|m_p| > 1$;

3− Indifférent si $|m_p| = 1$;

4− Super-attractif (ou super stable) si $m_p = 0$.

1.4.6 Bifurcations

Ce type de système dynamique possède trois types de bifurcations à un paramètre (selon le théoème (1.6)) : doublement de période, nœud-col, et Neimark-Sacker.

1− lorsque une valeur propre réelle de $Df(x)$ quitte (ou rentre dans) le cercle unité à -1, on a alors une bifurcation **fourche** (ou **doublement de période**, ou **flip**).

2− lorsque une valeur propre réelle de $Df(x)$ quitte (ou rentre dans) le cercle unité à $+1$, on a alors une bifurcation **nœud-col (**ou **tangente,** ou **pli).**

3− lorsque deux valeurs propres complexes conjuguées de $Df(x)$ quittent (ou rentrent dans) le cercle unité simultanément à $\lambda_{1,2} = e^{\pm i\theta}$, on a alors une bifurcation de **Neimark-Sacker**.

1.5 La section de Poincaré

La section de Poincaré est un outil très fréquemment utilisé pour étudier les systèmes dynamiques et notamment les trajectoires périodiques.

Considérons le système autonome d'ordre n :

$$\frac{dx}{dt} = f(x), x \in \mathbb{R}^n \tag{1.16}$$

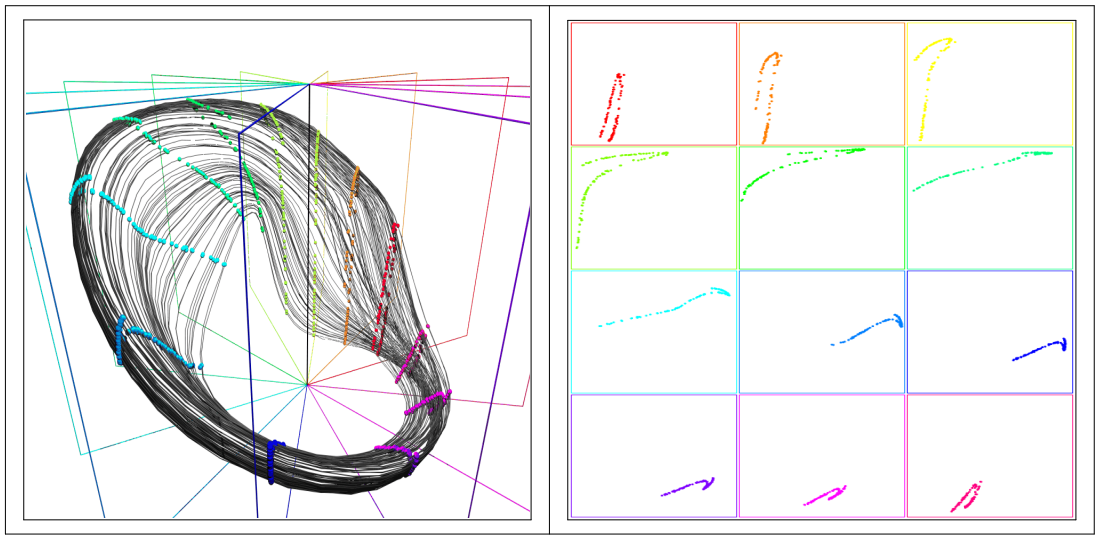


FIG. 1-7 – *Principe de la section de Poincaré*

Soit $\varphi(t, x_0)$ une trajectoire représentant la solution du système (1.16) muni de la solution initiale $x(0) = x_0$.

Le système (1.16) n'ayant généralement pas de solution analytique, on doit étudier chaque solution en considérant sa trajectoire dans l'espace des phases que l'on peut obtenir par une intégration numérique, mais la dimension élevée de l'espace complique, cette étude. C'est pour cela que la section de Poincaré est intéressante. Elle transforme un système continu en un système discret.

Le principe de construction de cette technique est illustré par la figure (1.7), représentant des points d'intersection d'une trajectoire avec un hyperplan.

La méthode de Poincaré permet simultanément de discrétiser le système et de réduire sa dimension en conservant les même propriétés topologiques, plus précisément elle remplace l'analyse des trajectoires d'un système dynamique dont l'espace des phases est de dimension n par celle de la suite des points d'intersections successives : p_0, $p_1, p_2, ...$d'une trajectoire $\varphi(t, x_0)$ avec un hyperplan $\sum_p$ de dimension $(n-1)$, ce dernier peut être quelconque . Mais un bon choix permet d'obtenir les sections aisément exploitables. L'hyperplan $\sum_p$ est appelé la **section de Poincaré**.

On note par π la transformation qui conduit un point au point suivant sur la section, π est

une application continue de $\sum_p$ dans lui-même.

On a pour une trajectoire quelconque, la relation de récurrence suivante :

$$p_k = \pi\left(p_{k-1}\right), k > 0$$

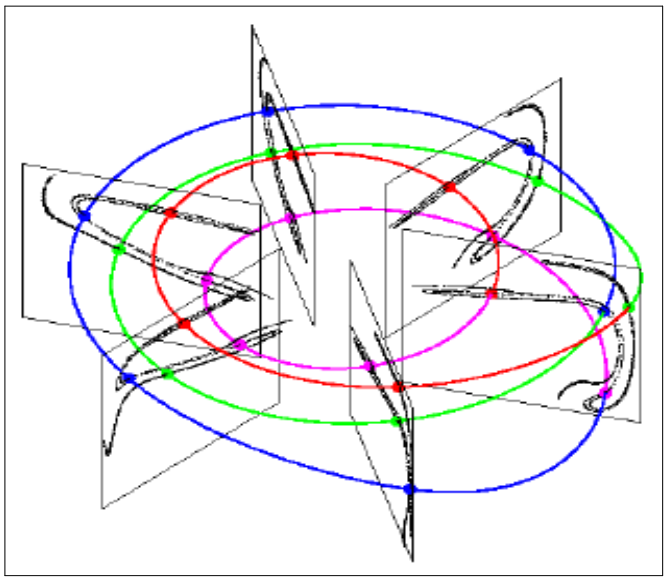


FIG. 1-8 – *Une orbite périodique*

Pour une solution périodique $x\left(t, x_0, t_0\right) = \phi_t\left(x_0\right)$ de période T :

$$\phi_{t+T}\left(x_0\right) = \phi\left(x_0\right)$$

Du système (1.16) la transformation π est équivalente à l'identité puisque la trajectoire se renferme sur elle-même, figure (1.8). p^* est alors un point fixe de l'application π, soit :

$$p_0^* = \pi\left(p_0^*\right) = \pi\left(\pi\left(p_0^*\right)\right) = ...$$

et on peut écrire :

$$\begin{array}{rcl} \pi & : & \sum_p \to \sum_p \\ x & \to & \pi(x) = \phi_T(x) \end{array}$$

où la période T représente le temps nécessaire pour atteindre la section. L'application π est appelée l'**application de Poincaré**.

1.6 Théorie du chaos

1.6.1 Historique sur le chaos

Si l'on demande à une personne au hasard de nous définir ce que représente le chaos pour elle, elle pourrait dire que cela rime avec « absence de règle ».

Vient du mot grec "Khaos" signifiant « abîme ». Le chaos est l'état primordial du monde caractérisé par une confusion de tous les éléments et par l'absence de l'ordre.

Au huitième siècle avant **J.C**, dans la Théogonie du poète grec **Hésiode**, le chaos est la personnification de l'espace vide situé entre le Ciel et la Terre qui se constitua avant toute chose. Après l'apparition de deux autres êtres primordiaux, la Terre (Gaia) Et l'Amour (Eros) ; le chaos engendra les ténèbres des Enfers (Erèbe) et la Nuit (Nyx).

Comme nous pouvons le voir, le chaos est un terme qui a déjà une histoire et un sens. Pourtant, depuis 1975, la dénomination de « chaos », introduite par **Li** et **York**, trouve une nouvelle signification relative à l'instabilité de ses conséquences et qui bouleverse les esprits les plus géniaux depuis déjà plus d'un siècle.

La notion de chaos relevant donc d'un contexte historique, nous devrons, en premier lieu, nous intéresser aux origines du chaos avant de nous focaliser sur un exemple révélateur, puis nous verrons que le chaos se retrouve finalement dans beaucoup de domaines différents.

Les origines de la notion du chaos

Selon **Isaac Newton** ; dans les “philosophiae naturalis principia mathematica” en 1687, le système solaire est un ensemble stable dans lequel la position de chaque planète peut être

prédite à partir de sa position et de sa vitesse à un instant donné.

En d'autres termes, les conditions initiales permettraient de déterminer l'état futur et antécédent du système considéré, la chose ayant été rendue possible grâce à la mise en place d'une nouvelle technique mathématique, le calcul différentiel. C'est la notion du : déterminisme.

Ces révélations sur la dynamique des solides ont influencé un grand nombre d'éminents physiciens et mathématiciens. Si le système de Newton ne considérait que deux corps, dès que l'on envisage un système plus complexe, le système solaire complet par exemple, la difficulté s'en trouve accrue. Ainsi, Lagrange, Laplace, Le verrier font partie de ceux qui vont affiner les connaissances sur le mouvement des planètes.

Un siècle après Isaac Newton, **Pierre Simon de Laplace** $(1749-1827)$, fervent admirateur de ce dernier, écrivait ceci : « nous devons donc envisager l'état présent de l'univers comme l'effet de son état antérieur, et comme la cause de ce qui va suivre » (Essai philosophique sur les probabilités 1795). Comme ses contemporains, il était persuadé du bien-fondé du déterminisme.

Un écossais du nom de **James Clerk Maxwell** $(1831-1879)$ va révolutionner le monde de la physique en général et de l'électromagnétisme en particulier. En 1876, dans son livre intitulé "Matter and Motion", il réfute l'idée laplacienne selon laquelle « les mêmes conditions produisent toujours les mêmes effets ». En effet, cela suppose que des conditions considérées à un moment et en un lieu différents soient exactement les mêmes. Ainsi, ce que Maxwell dit, c'est qu'il faut considérer deux états différents : un état stable et un état instable. Et pourtant, si cela parait être logique aujourd'hui, ce ne fut pas le cas à l'époque. Les mathématiciens et les physiciens faisaient abstraction des considérations d'instabilité car le phénomène tendrait alors vers le désordre, chose que les scientifique ne pouvaient pas concevoir.

Il fallut attendre la fin du 19 siècle avant d'avoir de nouveaux éléments. Le célèbre mathématicien, **Henri Poincaré** $(1854-1912)$ travaille alors sur le problème dit des « trois corps » (« L'analyse et la recherche » (1890)). Il s'agit tout simplement de considérer trois corps comme l'ensemble 'Terre, Lune, Soleil'. Plutôt que d'étudier le mouvement de ces astres, il cherche à déterminer l'ensemble des mouvements susceptibles d'être reproduits par le système. Alors que le système à « deux corps » semble simple et rejoint parfaitement la théorie, le système à « trois corps » révèle certains aspects jusque là non considérés. En effet, Poincaré montre que si l'on étudie le système sur une durée assez longue, alors les trajectoires ne sont plus des touts

comparables aux simples sections coniques comme les paraboles et autres hyperboles. Ainsi, i d'affirmer que sur une durée moindre, les trajectoires sont absolues mais seulement qu'elles sont approximatives. Cela amène à la notion de temps dit temps de **Lyapunov**, qui correspond à la durée à partir de laquelle la prévision se révèle impossible, et la notion de temps caractéristique qui correspond au temps au bout duquel deux mouvements initialement semblables s'écartent sensiblement. De plus, intervient une autre idée, celle de la sensibilité aux conditions initiales. Maxwell affirmait que deux conditions initiales ne peuvent pas être identiques. Poincaré montre que si l'on considère une légère différence (approximation) sur les conditions initiales, cette différence se trouve amplifiée de manière exponentielle après un certain temps à tel point que la trajectoire devient imprévisible. Par exemple, considérons le système solaire. Il est possible de montrer que sur une échelle des temps de l'ordre du millier d'années, nous pouvons considérer que le système solaire est stable. Maintenant, si l'on considère une échelle des temps de l'ordre du million d'années, alors rien ne va plus. Grâce à l'arrivée des ordinateurs et de leur formidable puissance de calcul (mais tout de même limitée par leur mémoire), il a été montré que le système solaire est instable. Pour illustrer la chose, si l'on considère la position de la Terre à 50 mètres près, au bout d'une centaine de millions d'années, cet écart serait de 500 millions de kilomètres. Ainsi, on dira que le système solaire est chaotique à l'échelle de millions d'années.

Après ces quelques éléments d'histoire sur la notion appelée « chaos » au travers de l'histoire des sciences depuis Newton, il est intéressant d'en voir une représentation des plus évocatrices et que l'on connaît sous le nom d'**effet papillon**.

Comme nous venons de le voir, la théorie du chaos a été introduite par Maxwell et appuyée par Poincaré. Pourtant, seul un petit nombre de physiciens et de mathématiciens s'intéressent au problème "d'instabilité" jusqu'à l'intervention d'**Edward Lorenz**.

La météorologie ou la représentation parfaite d'un système chaotique

La prévision météorologique est une des choses les plus complexes qui soit. Comparée au système solaire comportant fondamentalement peu éléments (soleil et planètes) et régi par la loi de gravitation, la météorologie semble dépendre d'une multitude de facteurs. Pour prévoir le temps dans une région donnée, il faut connaître celui qui prévaut dans une autre zone géographique. Il faut tenir compte de la température, de la pression, de l'hydrométrie, du relief et de beaucoup d'autres paramètres. Ces mêmes facteurs sont liés par des relations physiques et

donc par des équations mathématiques très complexes nécessitant une puissance de calcul que les ordinateurs vont permettre d'obtenir dans une certaine mesure.

Dans les années 60, Edward Lorenz, physicien météorologue de son état, travaillait au Massachusetts Instite of Technology (M.I.T). Lors de ses recherches, il est parvenu à simplifier les modèles mathématiques utilisés pour prédire le temps. En effet, de tous les facteurs intervenant sur les conditions météorologiques, il décida de n'en retenir qu'une douzaine, et d'en tirer un système de douze équations différentielles simples, tout aussi instables que le modèle complet.

Lorenz voulut reprendre un calcul qu'il avait déja réalisé. Reprenant des valeurs fournies par l'ordinateur, il s'attendait à juste titre à retrouver les résultats obtenus précédemment. Et pourtant, ce ne fut pas le cas. En effet, le début du calcul fournissait des résultats comparables au premier mais très vite, ces derniers divergeaient totalement.

L'explication vient du fait que l'ordinateur de Lorenz utilisait six chiffres significatifs pour le calcul mais les résultats affichés, étaient tronqués à trois chiffres seulement. Donc, lorsque Lorenz réinjecta ces valeurs, qui n'étaient que des approximations des valeurs réelles.

Lorsqu'en 1963 Lorenz publia un article sur ce qu'il avait mis en évidence, il n'est pas l'attention de la communauté scientifique. Il fallut attendre une dizaine d'années pour que retentisse l'écho de cette découverte. En effet, lors d'une session de l'Association Américaine pour l'Avancement de la Science consacrée au "Programme de Recherche Global sur l'Atmosphère", Lorenz introduit ce qui sera le maître mot de la théorie du chaos : ‹‹ l'effet papillon ›› ou l'idée que le battement d'ailes d'un papillon au Brésil peut provoquer une tornade au Texas. Cela réaffirme la tendance de certains systèmes à l'instabilité et également leur sensibilité aux conditions initiales qu'avait déjà introduites Poincaré plus d'un demi-siècle auparavant.

Lorenz a donc tiré une croix sur l'idée d'un déterminisme absolu et par la même occasion, il a ouvert les yeux à ceux qui ne juraient que par Newton. Cela ne signifie pas pour autant une remise en cause du déterminisme. Seulement, il faut prendre en considération qu'au-delà d'un certain temps, la prévision devient impossible.

Li et **York**, ont traduit cette notion d'instabilité due à la sensibilité aux conditions initiales, par le terme « chaos ». Mais, comme pour « l'effet papillon », ce sont les médias qui ont répandu ce terme que l'on utilise à outrance. La théorie du chaos a ouvert une nouvelle voie de recherche comme l'avait fait la théorie de la relativité ou la mécanique quantique. On en trouve de plus

en plus d'applications et la source est loin de se tarir.

Des systèmes dynamiques non linéaires, ou simplement linéaires par morceau, peuvent faire preuve de comportements complètement imprévisibles, qui peuvent même sembler aléatoires (alors qu'il s'agit de systèmes parfaitement déterministes). Cette imprédictibilité est appelée chaos. La théorie du chaos décrit qualitativement les comportements à long terme des systèmes dynamiques. Dans ce cadre, on ne met pas l'accent sur la recherche de solutions précises aux équations du système dynamique, mais plutôt sur la réponse à des questions comme « Le système convergera-t-il vers un état stationnaire à long terme, et dans ce cas, quels sont les états stationnaires possibles ? » ou « Le comportement à long terme du système dépend-il des conditions initiales ? ».

1.6.2 Caractéristiques du chaos

1– Sensibilité aux conditions initiales

Pour un système chaotique, une très petite erreur sur la connaissance de l'état initial x_0 dans l'espace des phases va se trouver (presque toujours) rapidement amplifiée. D'un point de vue mathématique on dit que $f : I \to I$ montre une dépendance sensible aux conditions initiales lorsque :

$$\exists \delta \succ 0 \ \forall x_0 \in I, \varepsilon \succ 0 \ \exists n \in \mathbb{N}, y_0 \in I : |x_0 - y_0| \prec \delta \Longrightarrow |f^n(x_0) - f^n(y_0)| \succ \delta$$

2– L'attracteur étrange

Un système chaotique dissipatif possède (au moins) un attracteur d'un type particulier appelé attracteur étrange. Géométriquement, un tel attracteur peut être décrit comme le résultat d'opérations d'étirement et de repliement d'un cycle de l'espace des phases, répétée un nombre infini de fois. La "longueur" de l'attracteur est infinie, bien qu'il soit contenu dans un espace fini. Alors on peut donner cette définition

Définition 1.11 :

Un sous-ensemble borné A de l'espace des phases est un attracteur étrange ou chaotique pour une transformation T de l'espace s'il existe un voisinage R de A; c'est à dire que pour tout point de A il existe une boule contenant ce point et contenue dans R vérifiant les propriétés

suivantes :

· Attraction : R est une zone de capture, ce qui signifie que toute orbite par T dont le point initial est dans R, est entièrement contenue dans R. De plus, toute orbite de ce type devient et reste aussi proche de A que l'on veut.

· Il est contenu dans un espace fini. Son volume est nul. Sa dimension est fractale (non entière).

· Presque toute trajectoire sur l'attracteur a la propriété de ne jamais passer deux fois sur le même point : chaque trajectoire est presque sûrement apériodique.

· Deux trajectoires proches à l'instant t voient localement leur distance augmenter à une vitesse exponentielle (sensibilité aux conditions initiales).

3– Spectre de puissance

Une façon simple de caractériser le chaos consiste à calculer le spectre de Fourier de l'évolution temporelle d'une des variables du système. Lorsque le système est intégrable c'est-à-dire qu'il est possible de déterminer complètement les trajectoires d'un système dans son espace de phases, ce système est dit intégrable ; les trajectoires étant la composition de mouvements d'oscillation ayant chacun une pulsation w_i.

Le spectre d'une variable d'un tel système ne contient donc qu'une assemblée de raies fines situées aux pulsations w_i, à leurs harmoniques mw_i avec $m \in \mathbb{N}$, aux combinaisons linéaires de fréquences $mw_i + nw_j$ avec $m, n \in \mathbb{Z}$, les spectres qui sont la combinaison de plusieurs fréquences sans rapport simple sont dit quasipériodiques. L'existence de spectres larges est une caractéristique essentielle des mouvements chaotiques d'un système.

L'évolution temporelle d'un système dynamique est souvent représentée par la valeur d'une de ses variables à intervalle régulier, c'est ce qu'on appelle la série temporelle.

1.6.3 Routes vers le chaos

Un système dynamique possède en général un ou plusieurs paramètres dit "de contrôle", qui agissent sur les caractéristiques de la fonction de transition. Selon la valeur du paramètre de contrôle, les mêmes conditions initiales mènent à des trajectoires correspondant à des régimes dynamiques qualitativement différents. La modification continue du paramètre de contrôle conduit dans bien des cas à une complexification progressive du régime dynamique développé

par le système.

Il existe plusieurs scénarios qui décrivent le passage du point fixe au chaos. On constate dans tous les cas que l'évolution du point fixe vers le chaos n'est pas progressive, mais marquée par des changements discontinus qu'on appelle **"bifurcations"**. Une bifurcation marque le passage soudain d'un régime dynamique à un autre, qualitativement différent. On peut citer trois scénarios de transition vers le chaos :

1− **L'intermittence vers le chaos** : un mouvement périodique stable est entrecoupé par des bouffées de turbulence. Lorsqu'on augmente le paramètre de contrôle, les bouffées de turbulence deviennent de plus en plus fréquentes, et finalement, la turbulence domine.

2− **Le doublement de période** qui est caractérisé par une succession de bifurcations fourches. A mesure que la contrainte augmente, la période d'un système forcé est multipliée par deux, puis par quatre, puis par huit, ..., etc ; ces doublements de période sont de plus en plus rapprochés ; lorsque la période est infinie, le système devient chaotique. La turbulence dans les fluides peut apparaître suivant ce scénario.

3− **La quasi-périodicité** qui intervient quand un deuxième système perturbe un système initialement périodique. Si le rapport des périodes des deux systèmes en présence n'est pas rationnel, alors le système est dit quasipériodique. Ce scénario un peu compliqué est relié à la théorie des nombres, notamment aux travaux de **Jean Christophe Yoccoz**, lauréat de la Médaille Fields en 1994, pour ses travaux sur les systèmes dynamiques.

Chapitre 2

Exemples de systèmes dynamiques chaotiques

2.1 Introduction

Un système chaotique est un système dynamique déterministe non linéaire qui se distingue par son imprévisibilité due à son extrême sensibilité aux conditions initiales. Dans ce chapitre on présente trois exemples de systèmes dynamiques chaotiques qui sont : Le modèle du pendule amorti, le modèle de Lorenz et l'application logistique.

2.2 Le pendule amorti

L'équation du pendule :

Soit une masse m placée dans un champ de gravitation et suspendue en 0 à un fil rigide de longueur l et de masse nulle.

Le pendule oscillant amorti, qui est décrit par une équation différentielle d'ordre 2 :

$$\ddot{\theta} + \lambda\dot{\theta} + \varpi_0^2 \sin\theta = 0 \tag{2.1}$$

où $\lambda = \frac{c}{m}$; $\varpi_0^2 = \frac{g}{l}$ tels que :

$\theta(t)$: angle que fait le fil à l'instant t avec la verticale.

g : accélération de la pesanteur.

$C > 0$: coefficient d'amortissement de l'air.

La force d'amortissement de l'air $C\ \frac{d\theta}{dt}$ s'oppose toujours à la direction du mouvement.

Pour simplifier le problème on suppose que $\varpi_0^2 = 1$ alors (2.1) s'écrit alors :

$$\ddot{\theta} + \lambda\dot{\theta} + \sin\theta = 0$$

On considère ce pendule oscillant dans un plan vertical et **sans frottement,** c'est le cas d'un pendule **conservant l'énergie**.

2.2.1 Le pendule simple

Le mouvement du pendule idéal (simple) est décrit par une équation différentielle d'ordre 2 :

$$\ddot{\theta} + \varpi_0^2 \sin\theta = 0$$

car le coefficient d'amortissement de l'air C est nul.

On définit deux nouvelles variables :

$$\begin{cases} x = \theta \\ y = \dot{x} = \dot{\theta} \end{cases}$$

La variable x n'est autre que l'angle et y est la vitesse angulaire, d'où l'on trouve un système de deux équations différentielles d'ordre 1 :

$$\begin{cases} \dot{x} = y \\ \dot{y} = -\varpi_0^2 \sin x \end{cases}$$

Détermination des points fixes :

Les points fixes sont définis par :

$$\begin{pmatrix} x^* \\ y^* \end{pmatrix} \text{ est un point fixe de } \begin{pmatrix} \dot{x} = f(x,y) \\ \dot{y} = g(x,y) \end{pmatrix} \Leftrightarrow \begin{pmatrix} \dot{x}^* = 0 \\ \dot{y}^* = 0 \end{pmatrix} \text{ implique } \left(x = \theta = k\pi, y = \dot{\theta} = 0\right), k \in \mathbb{Z}.$$

Il s'agit des points où le pendule est **vertical** ou **immobile.**

Certains points sont **stables** (quand le pendule est en bas) et d'autres **instables** (quand le pendule est en haut).

Portrait de phase :

Le passage d'un système à une variable à un système à deux variables pose un problème : L'orbite se situe désormais dans un **espace de phase à** 4 **dimensions** $(x(t), y(t), \dot{x}(t), \dot{y}(t))$.

Or on ne peut pas représenter que deux variables à la fois dans un plan. Une méthode simple permet de dépasser cette difficulté.

On appelle portrait de phase l'ensemble des projections dans le plan de phase des solutions d'un système. C'est une représentation géométrique des orbites qui fournit des informations essentielles sur les propriétés des systèmes autonomes.

Pour θ petit alors $\sin\theta \approx \theta$ l'équation s'écrit sous la forme du système :

$$\begin{cases} \dot{x} = y \\ \dot{y} = -\varpi_0^2 y \end{cases}$$

Le portrait de phase de ce système est le plan dont les axes sont $x(t)$ et $y(t)$. Chaque point de ce plan $x(t)$, $y(t)$ correspond à un état possible de l'oscillateur.

Pour un temps t_0 pour lequel l'orbite passe le point $(x(t=t_0), y(t=t_0))$ au temps $t_0 + \delta t$, le système se trouve au point :

$$\begin{pmatrix} x(t_0+\delta t) \\ y(t_0+\delta t) \end{pmatrix} = \begin{pmatrix} x(t_0) + \delta t \dot{x}(t_0) \\ y(t_0) + \delta t \dot{y}(t_0) \end{pmatrix} = \begin{pmatrix} x(t_0) \\ y(t_0) \end{pmatrix} + \delta t \begin{pmatrix} \dot{x}(t_0) \\ \dot{y}(t_0) \end{pmatrix}$$

pour la condition initiale $(x(t=t_0), y(t=t_0))$ l'orbite s'éloigne dans une direction qui est donnée par la "vitesse" $(\dot{x}(t_0), \dot{y}(t_0))$.

A chaque point du portrait de phase on peut donc associer un vecteur $(\dot{x}, \dot{y})$ sachant que l'orbite est tangente à ce vecteur. Grâce à l'ensemble de ces vecteurs, on peut construire l'orbite de proche en proche.

Les orbites associées à des différentes conditions initiales, pour la condition initiale (x_0, y_0) correspond un vecteur particulier montrant comment l'orbite s'éloigne de ce point.

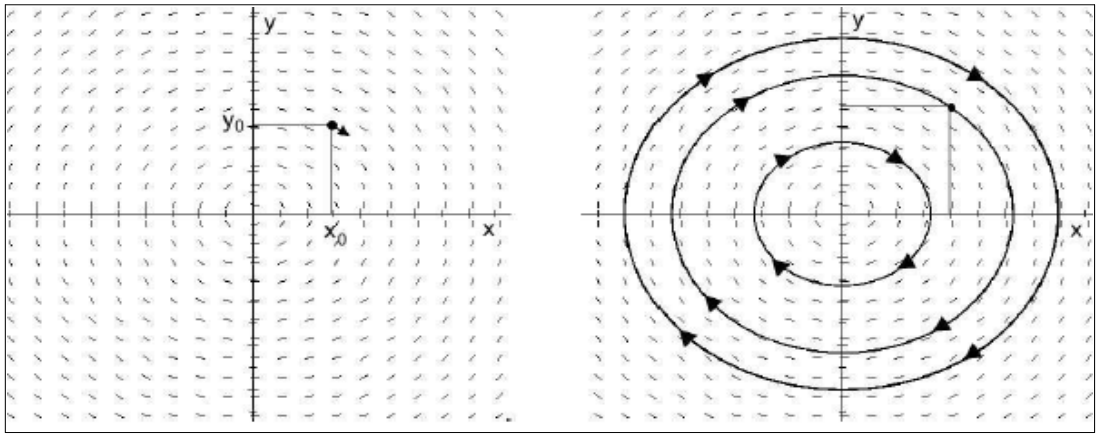


FIG. 2-1 – *Le champ de vecteurs associé à un réseau de points qui couvrent le plan* (x, y)

Remarque 2.1 :

· Il existe une infinité d'orbites dans le portrait de phase mais on ne trace que les plus représentatives.

· L'ensemble de ces orbites définit le flot.

· Toutes les orbites sont fermées cela signifie que le système repasse périodiquement par le même état.

· A une orbite fermée correspond un régime périodique.

· Deux orbites ne peuvent jamais se croiser, sauf en un point fixe (problème de Cauchy).

De l'équation non linéaire on peut déduire une relation entre x et y plus précisément la quantité d'énergie (énergie du pendule) :

$$E(x, y) = \frac{1}{2}y^2 + \omega_0^2 - \omega_0^2 \cos x$$

qui est une constante du mouvement $\left(\frac{dE}{dt} = 0\right)$ i.e. l'énergie est conservée.

Les trajectoires solutions de l'équation sont des courbes d'isoénergie ou courbes de niveau dans le plan des phases.

2.2.2 Le pendule amorti

Supposons maintenant que le pendule oscille dans un plan vertical mais **avec frottement** c'est à dire il y a une **dissipation d'énergie**.

Ce pendule est décrit par l'équation différentielle d'ordre 2 suivante :

$$\ddot{\theta} + \lambda\dot{\theta} + \omega_0^2 \sin\theta = 0$$

Cette équation peut se décomposer en deux équations différentielles du premier ordre, en faisant le changement de variable suivant :

$$\begin{cases} x = \theta \\ y = \dot{x} = \dot{\theta} \end{cases} \text{ d'où l'on déduit } \begin{cases} \dot{x} = y \\ \dot{y} = -\lambda y - \omega_0^2 \sin x \end{cases}$$

la variable x n'est autre que l'angle et y est la vitesse angulaire.

Comme on a deux équations différentielles du 1^{er} ordre à résoudre il faut deux conditions initiales, comme pour l'équation initiale.

Les orbites sont ici ouvertes, cela traduit le mouvement non-périodique avec amortissement progressif et évolution vers le point fixe $(x, y) = (0, 0)$.

2.2.3 Comparaison des portraits de phase du pendule sans et avec amortissement

On observe plusieurs types d'orbites dans la figure ci-dessus :

1− des orbites ouvertes : le pendule tourne toujours dans le même sens sans s'interrompre.

2− des orbites fermées : elles correspondent au mouvement oscillatoire habituel du pendule.

3− une orbite particulière, appelée séparatrice qui marque la frontière entre le mouvement oscillant et le mouvement de rotation.

4− des orbites ouvertes correspondant à une rotation dans le sens négatif.

Les orbites ne se croisent jamais, sauf en un point particulier : les séparatrices se coupent aux point fixe : $(x = \pi + 2k\pi, y = 0), k \in \mathbb{Z}$ ces points correspondent à un pendule dont le balancier se trouve au sommet. Il s'agit donc de points d'équilibre instables contrairement aux points fixes définis par : $(x = 2k\pi, y = 0), k \in \mathbb{Z}$ qui sont stables.

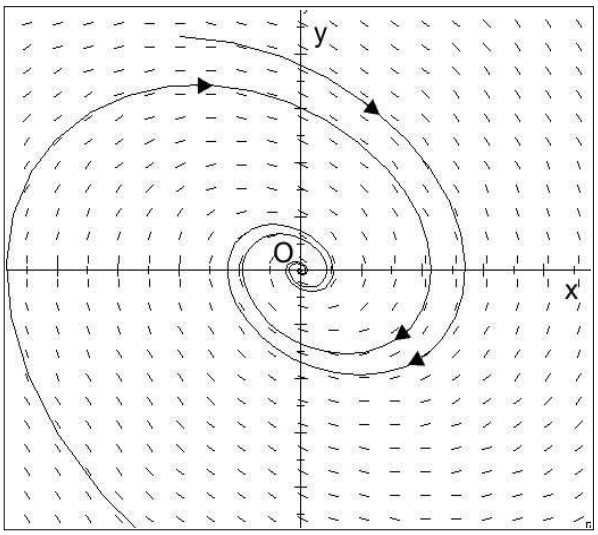


FIG. 2-2 – *Le flot associé à un oscillateur harmonique amorti*

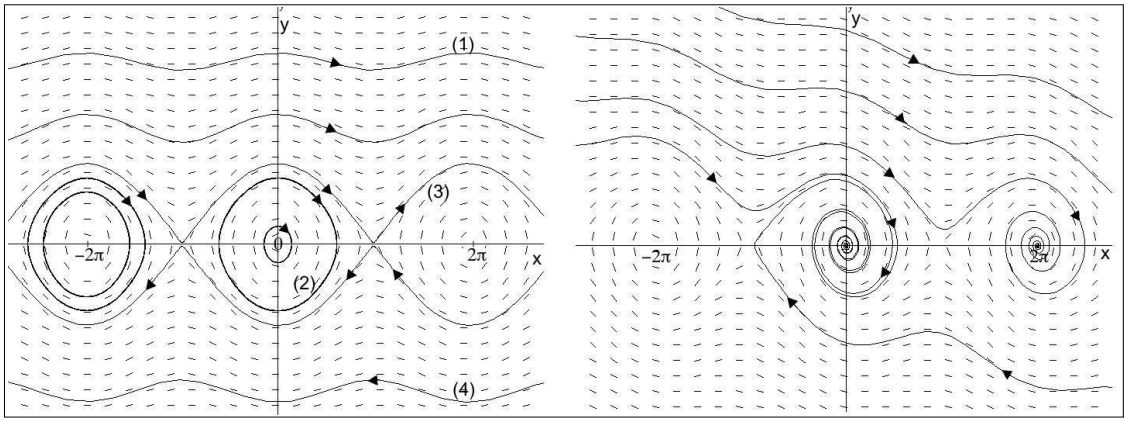


FIG. 2-3 – *Portrait de phase du pendule non-amorti (à gauche) et du pendule faiblement amorti (à droite)*

2.3 Le modèle de Lorenz

En 1963, **Edward Norton Lorenz** a étudié numériquement un système de trois équations différentielles censé représenter grossièrement la convection thermique dans l'atmosphère (obtenu à partir des équations de **Navier-Stokes**).

2.3.1 Les équations du modèle

Le système dynamique s'écrit :

$$\begin{aligned} x^{'} &= \sigma\,(y - x) \\ y^{'} &= rx - y - xz \\ z^{'} &= xy - bz \end{aligned}$$

L'espace des phases est tridimensionnel. Les valeurs de σ et b sont fixées, respectivement à 10 et $\frac{8}{3}$. Le paramètre de contrôle est r qui est positif. Physiquement, r est proportionnel au gradient thermique vertical imposé au fluide, σ au nombre de Prandtl et b à l'élongation de la boite contenant le fluide.

La solution triviale $x = y = z = 0$ du système correspond physiquement à un régime où le fluide est au repos et où la chaleur se transmet uniquement par diffusion moléculaire (état conductif). Pour r grand, cet équilibre est instable et il laisse la place à des régimes où le transfert de chaleur est réalisé par diffusion et par convection.

Les propriétés importantes de ces équations sont :

· Elles sont autonomes.

· Elles associent seulement les dérivées du premier ordre de sorte que l'évolution dépend seulement des valeurs instantanées de (x, y, z).

· Elles sont non-linéaires, ici à travers le térme quadratique xz et xy dans le seconde et la troisième équation.

· Elles sont dissipatives : le terme "diagonal" tel que $\dot{x} = -\sigma x$ correspond à un affaiblissement de mouvement, mais plus systématiquement "les volumes dans l'espace des phases" se réduisent dans cette dynamique.

· Les solutions sont fermées.

2.3.2 L'équilibre du modèle

On cherche les points d'équilibre (x, y, z) vérifiant $\acute{x} = \acute{y} = \acute{z} = 0$.

Pour $r < 1$, il n'y a qu'un seul point d'équilibre, l'origine $(0, 0, 0)$. Et, pour $r > 1$, il y a deux autres points : $(b(r-1), b(r-1), r-1)$.

L'étude de la stabilité des points d'équilibre repose sur le signe de la partie réelle des valeurs propres de la matrice Jacobéenne A obtenu en linéarisant le système autour d'un point d'équilibre.

L'expression de la matrice Jacobéenne A du système est :

$$A = \begin{pmatrix} -\sigma & \sigma & 0 \\ r - z & -1 & -x \\ y & x & -b \end{pmatrix}$$

La stabilité au point $(0, 0, 0)$

Au point $(0, 0, 0)$, les valeurs propres λ de la Jacobéenne A

$$A = \begin{pmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{pmatrix}$$

sont solutions de l'équation suivante :

$$(\lambda + b)\left(\lambda^2 + (1+\sigma)\lambda + \sigma(1-r)\right) = 0$$

· Pour $r < 1$, il y a trois racines réelles négatives, l'équilibre est donc stable.

· Pour $r > 1$, une des valeurs propres est positive : l'équation est donc instable. Il y a une bifurcation quand $r = 1$, l'équilibre est dit **marginal**.

La stabilité pour les deux autres points d'équilibres

Les valeurs propres de la jacobéenne sont solutions de l'équation en λ :

$$\lambda^3 + (\sigma + b + 1)\,\lambda^2 + b\,(\sigma + r)\,\lambda + 2\sigma b\,(r - 1) = 0$$

Selon les valeurs du paramètre r, ce polynôme de degré trois peut avoir trois racines réelles négatives (les équilibres sont donc stables) ou bien une racine réelle et deux racines complexes conjuguées.

On peut chercher s'il existe une valeur critique de r pour laquelle les équations deviennent instables. La déstabilisation de ces équations par changement de signe d'une valeur propre réelle est impossible car si $\lambda = 0$ on a forcément $r = 1$. On peut donc rechercher pour quelles valeurs de r on peut obtenir deux racines $i\omega$ et $-i\omega$ de partie réelle nulle. En reportant la valeur $\lambda = i\omega$ dans l'équation, on obtient les deux conditions :

$$\begin{aligned} -\omega^2\,(\sigma + b + 1) + 2b\,(r - 1)\,\sigma &= 0 \\ -i\omega^3 + i\omega b\,(\sigma + r) &= 0 \end{aligned}$$

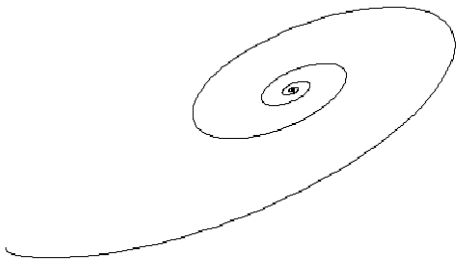
L'élimination de ω^2 entre les deux équations permet d'obtenir la valeur r_C critique :

$$r_C = \frac{\sigma\,(\sigma + b + 3)}{(\sigma - b - 1)}$$

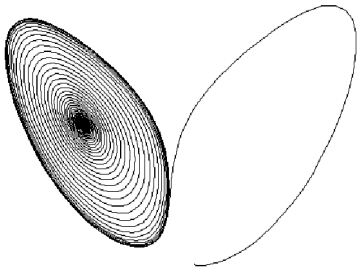
pour les valeurs $\sigma = 10$ et $b = \frac{8}{3}$, la valeur critique est $r_C = \frac{470}{19} \simeq 24.73$.

La déstabilisation des équilibres correspond à une bifurcation de Hopf. Deux valeurs propres complexes conjuguées traversent l'axe des imaginaires lorsque le paramètre r franchit la valeur critique r_C.

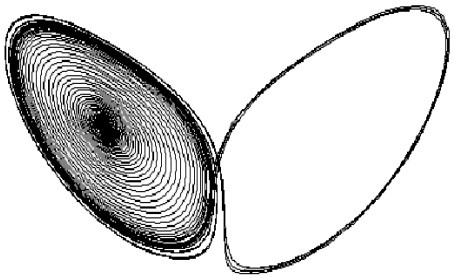
Lorsque $r > r_C$ le système transite vers un régime chaotique. La trajectoire tourne autour l'un des deux équilibres instables comme si elle y convergeait avant de basculer aléatoirement vers l'autre équilibre pour y répéter le même type de comportement. On montre que la distance entre deux conditions très proches s'amplifie très rapidement. Toutes les trajectoires convergent vers l'attracteur étrange.



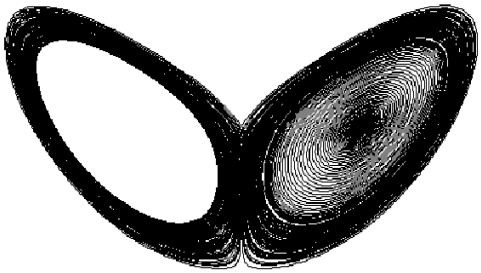
Attracteur de Lorenz pour $r = 5$



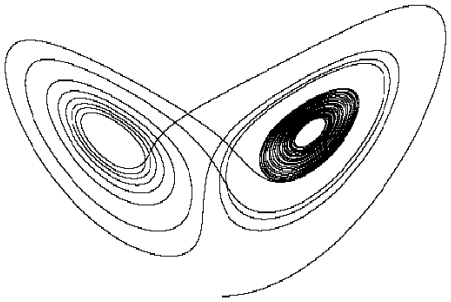
Attracteur de Lorenz pour $r = 10$



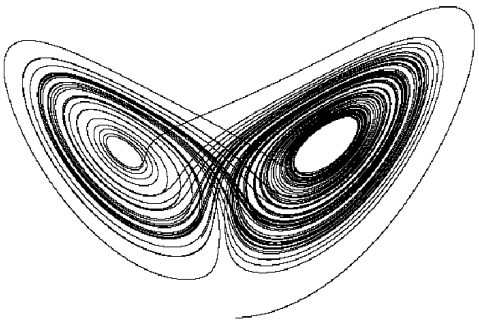
Attracteur de Lorenz pour $r = 15$



Attracteur de Lorenz pour $r = 20$



Attracteur de Lorenz pour $r = 24$



Attracteur de Lorenz pour $r = 28$

La sensibilité aux conditions initiales, ainsi que le chaos déterministe observés avec ce système dynamique, ont servi de base à ce que l'on appelle "l'effet papillon".

2.3.3 Effet papillon

"Le battement d'ailes d'un papillon du Brésil déclenche-t-il une tornade au Texas ?".

Question que Lorenz pose en 1972, lors d'une réunion de l'**American Association for the Advancement of Science**.

Cette formule traduit la ‹‹ sensibilité aux conditions initiales ›› d'un système dynamique, atmosphérique ou autre, c'est à dire qu'elle affirme un principe de non-prédictibilité. Elle est souvent interprétée, à tort, comme une **petite cause** peut avoir de **grands effets**, c'est à dire affirmation d'un principe de causalité. Pour contrer cette mauvaise interprétation, Lorenz ajoute :

"Si le battement d'ailes d'un papillon peut déclencher une tornade, il peut aussi l'empêcher".

2.4 L'application logistique

On présente ici un modèle de classe de systèmes dynamiques non linéaires à temps discret. Ce modèle est appelé **application quadratique** (ou **logistique**).

Afin d'introduire le comportement des cartes itérées, que nous utiliserons par suite, nous allons suivre la démarche de **Feigenbaum**, qui s'est intéressé tout particulièrement à la cascade de doublement de période, dans le cadre des itérations d'une fonction mathématique f à valeurs réelles, vérifiant les hypothèses suivantes :

· f doit être continue et différentiable de $[0,1]$ dans lui-même.

· f a un maximum x_m avec $f\,'(x_m) \neq 0$.

· f est monotone dans $[0, x_m]$ et $[x_m, 1]$.

· f a une dérivée Schwartzienne $S_f\,(x) < 0$ pour tout $x \in [0,1]$, où :

$$S_f\,(x) = \frac{f\,''(x)}{f\,'(x)} - \frac{3}{2}\left(\frac{f\,''(x)}{f\,'(x)}\right)$$

2.4.1 Etude de l'application logistique

Considérons l'application f qui est définie de $[0,1]$ dans lui-même par l'itération suivante :

$$f\,(x_n) = 4\lambda x_n\,(1 - x_n)\,, x_n \in [0,1]$$

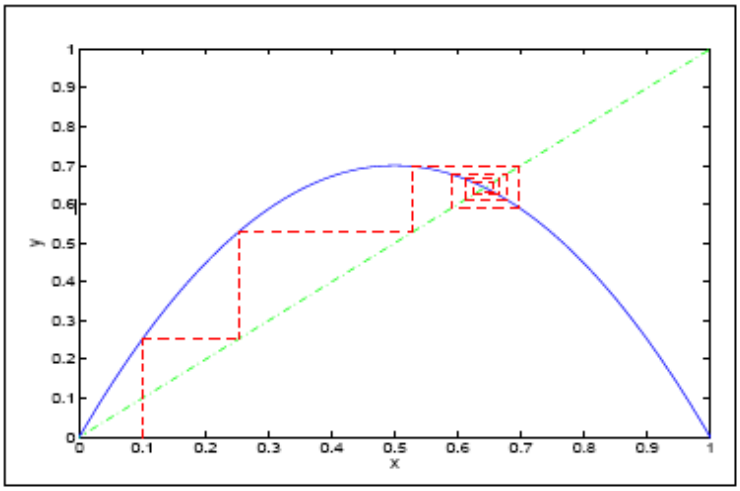


FIG. 2-4 – *Orbite des itérations de la fonction* f, *avec* $\lambda = 0.7$ *et* $x_0 = 0.1$

où $n = 0, 1, 2, ...$dénote le temps discret, x_n l'unique variable dynamique, et $0 \leq \lambda \leq 1$ un paramètre.

f est la fonction logistique, elle s'annule pour $x = 0$ et $x = 1$, et sa dérivée s'annule pour $x = \frac{1}{2}$ donc atteint le maximum à $x = \frac{1}{2}$ et $f\left(\frac{1}{2}\right) = \lambda$.

Les points fixes de f sont les solutions de l'équation :

$$x = 4\lambda x\left(1 - x\right), \lambda > 0 \text{ d'où } x_1 = 0 \text{ et } \ x_2 = 1 - \frac{1}{4\lambda}$$

On voit bien sur la figure (2.4) que les points d'équilibre de la suite considérée correspondent aux intersections de la courbe d'équations $y = f\ (x)$ et $y = x$.

La dynamique de cette application présente un comportement très différent selon la valeur du paramètre λ.

Valeurs de λ comprises entre 0 et 1

Les domaines de stabilité sont alors donnés par :

(x_i est stable si $|f\,'(x_i)| < 1$)

· $0 < \lambda < 0.25$ pour x_1.

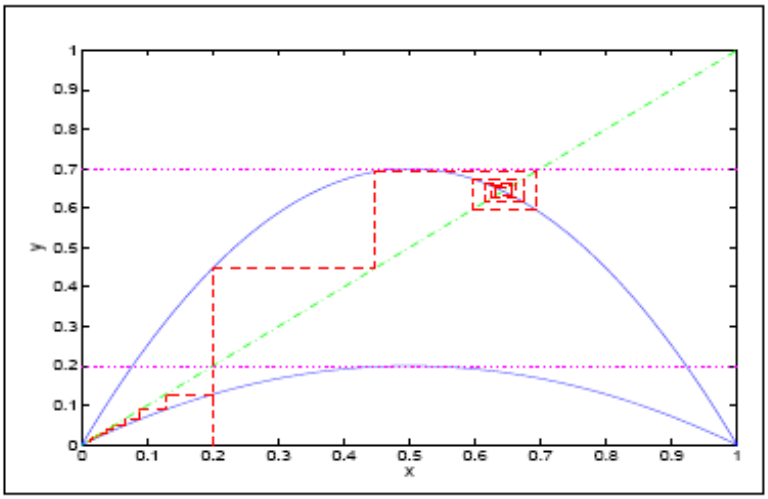


FIG. 2-5 – *Orbite des itérations de la fonction* f *, avec* $\lambda = 0.7$ *et* $x_0 = 0.2$

· $0.25 \leq \lambda \leq \lambda_1$avec $\lambda_1 = 0.75$ pour x_2.

Il existe alors, pour $0 < \lambda \leq \lambda_1$, un unique point fixe stable,

en modifiant la condition initiale x_0, la suite converge toujours mais la vitesse de convergence est différente.

· pour $\lambda_1 = 0.75$: $f\,'(x_2) = -1$ donc $x = \frac{2}{3}$ est un point de bifurcation.

Valeurs de λ comprises entre $\lambda_1$et λ_2

On relève figure (2.6) que pour des valeurs de λ comprises entre $\lambda_1 = 0.75$ et $\lambda_2 = 0.86237$, deux points de convergence x_3 et x_4 prennent naissance autour de x_2; et vérifient :

$$x_3 = f(x_4) \text{ et } x_4 = f(x_3)$$

Ces points ne sont donc pas des points fixes de f mais de $g = f \circ f$, où $\circ$ désigne la composition, ils forment un attracteur d'ordre 2 (cycle).

· pour $\lambda_2 = 0.86237$ le cycle d'ordre 2 perd sa stabilité et donne lieu a un cycle d'ordre 4.

Valeurs de λ comprises entre λ_2 et λ_3

De même, pour des valeurs de λ comprises entre $\lambda_2 = 0.86237$ et $\lambda = 0.87$, la pente de aux points et devient supérieure à 1, et la suite prend alors quatre valeurs différentes, qui

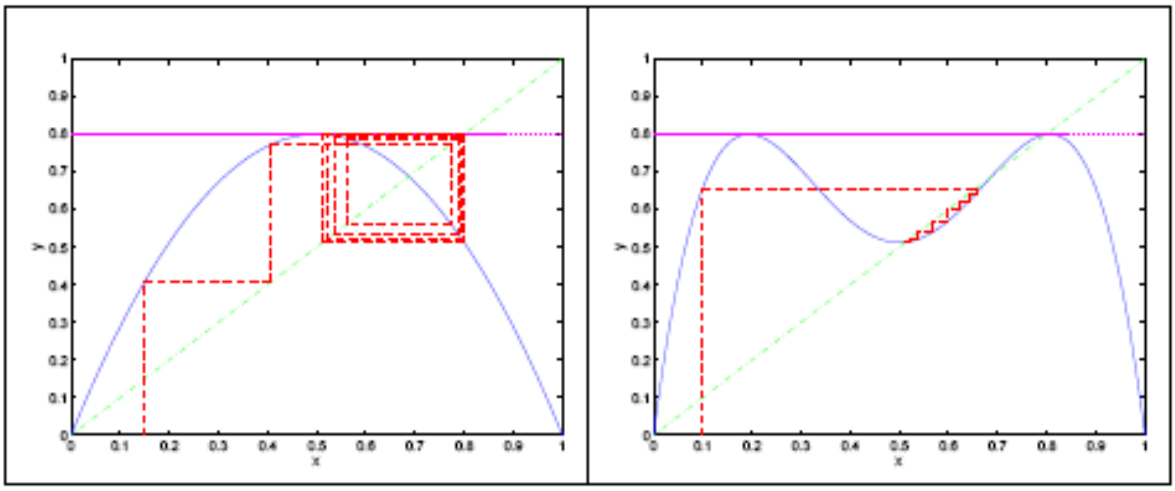


FIG. 2-6 – *Orbite des itérations de la fonction f pour $\lambda = 0.8$ (à gauche); orbite des itérations de la fonction g pour $\lambda = 0.8$ (à droite)*

sont :

$$x_5 = f(x_8), x_6 = f(x_5), x_7 = f(x_6), x_8 = f(x_7)$$

Ces points sont des points de la fonction $h = g \circ g$.

Il y a ainsi **quadruplement de période**.

On assiste ainsi à toute une série de doublement de période, pour des valeurs du paramètre de plus en plus rapprochées, ce qu'on appelle une "**cascade sous-harmonique**".

Cette cascade se produit jusqu'à atteindre une valeur limite du paramètre de bifurcation $\lambda = \lambda_c \simeq 0.892489418$, au-delà de laquelle le comportement devient chaotique.

La longueur des plages de paramètres correspondant à un comportement donné $(\lambda_j - \lambda_{j-1})$ diminue au fur et à mesure des bifurcations de la manière suivante :

$$\lim_{n \longrightarrow +\infty} \frac{\lambda_n - \lambda_{n-1}}{\lambda_{n+1} - \lambda_n} = C_F = 4.6692016609102...$$

où C_F est la **constante de Feigenbaum**.

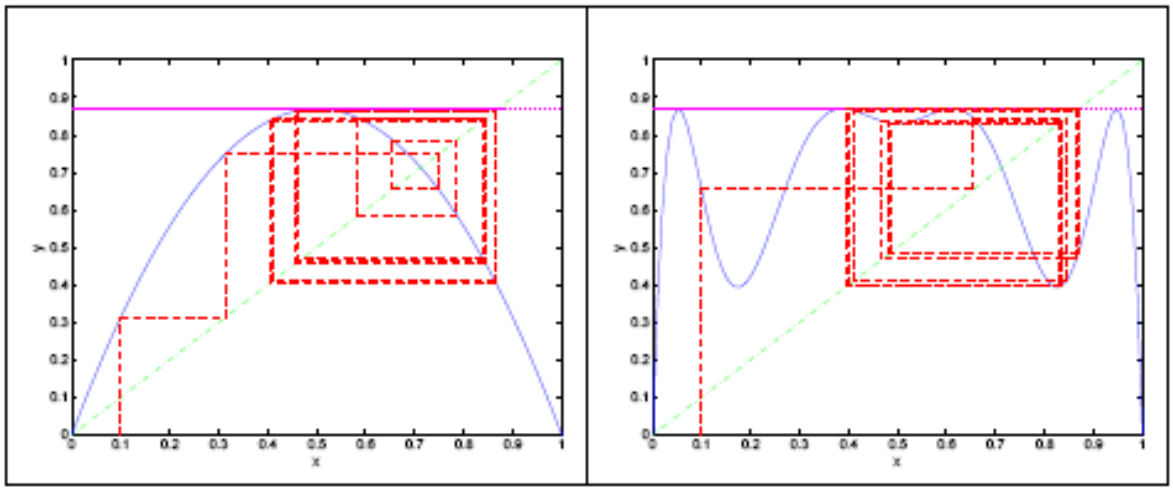


FIG. 2-7 – *Orbite des itérations de la fonction f pour $\lambda = 0.87$ (à gauche) ; orbite des itérations de la fonction h pour $\lambda = 0.87$ (à droite)*

2.4.2 Diagramme de bifurcation

Il est intéressant de visualiser ces différents comportements sur un diagramme de bifurcation. On trace tous les points obtenus en fonction de la valeur du paramètre de bifurcation λ correspondante. Le nombre de points différents représentés sur une même droite verticale donne donc ainsi le facteur par lequel est multipliée la période initiale.

On y retrouve bien les valeurs des seuils de bifurcation λ_i.

2.4.3 La constante de Feigenbaum

La découverte de cette constante est due entièrement au mathématicien Mitchell J. Feigenbaum, qui l'a calculée à l'aide d'une simple calculette vers 1975. Il avait observé que les bifurcations de l'application quadratique convergeaient vers leur limite d'une façon régulière. Il a donc été conduit à étudier la suite $u_k = \lambda_{k+1} - \lambda_k$ et il a remarqué qu'elle se conduisait presque comme une suite géométrique. Presque, car le rapport $\delta_k = \frac{u_k}{u_{k+1}}$ n'est pas contant, mais δ_k tend vers une limite C_F. Avec les valeurs de λ_k que l'on a, cela donne :

$$\delta_1 = 4.7514, \delta_2 = 4.6562, \delta_3 = 4.6682, \delta_4 = 4.6687...$$

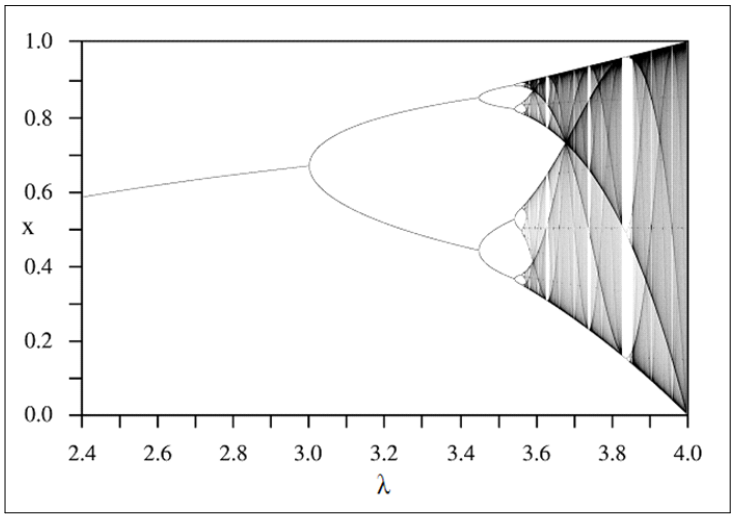


FIG. 2-8 – *Diagramme de bifurcation de la fonction* f *définie par* $f(x) = \lambda x(1-x)$ *pour* $2.4 \leq \lambda \leq 4$

Ce nombre est la constante de Feigenbaum. On le retrouve dans un grand nombre de phénomènes liés aux systèmes dynamiques, dans des domaines aussi variés que l'hydro-dynamique, l'électronique, l'acoustique et le laser.

Chapitre 3

Outils de quantification et de mesure du chaos

3.1 Introduction

On sait que la perte d'information sur les conditions initiales induite par un comportement chaotique, expliquerait en partie la complexité du comportement de certains systèmes réels.

Cependant, ne disposant pas de conditions nécessaires et/ou suffisantes pour caractériser un système chaotique, on cherche des moyens quantitatifs permettant de reconnaître, de distinguer un comportement chaotique d'un comportement aléatoire ou erratique (dû respectivement à un **"bruit"** ou à un nombre très élevé de degré de liberté).

La définition de "**quantificateur du chaos**" permet dans certains cas de décrire la dynamique d'un système et son passage à un régime chaotique en fonction des variations de certains paramètres, dits paramètres de contrôle du système.

3.2 Exposants de Lyapunov

Certains systèmes dynamiques sont très sensibles aux variations de leurs conditions initiales, ces variations peuvent rapidement prendre d'énormes proportions.

Le mathématicien russe **Alexander Markus-Lyapunov** $(1857-1918)$ s'est penché sur ce phénomène et a développé une quantité permettant de mesurer la vitesse à laquelle ces petites

variations peuvent s'amplifier, cette quantité appelée **"exposant de Lyapunov"** mesure en fait le degré de sensibilité d'un système dynamique, autrement dit, le taux de divergence entre l'évolution de trajectoires issues de conditions initiales proches au sein de cet espace borné qu'est l'attracteur étrange.

L'exposant de Lyapunov est une mesure quantitative possible du chaos, et Lyapunov a démontré que le nombre d'exposants de Lyapunov est égale à la dimension de l'espace des phases.

Par ailleurs, parmi les exposants retenus pour un système donné on considère généralement l'exposant le plus élevé.

Considérons la formule suivante :

$$\left|\frac{d_n}{d_0}\right| = \left|\frac{d_n}{d_{n-1}}\right|\left|\frac{d_{n-1}}{d_{n-2}}\right|...\left|\frac{d_1}{d_0}\right| \text{ d'où : } \frac{1}{n}\ln\left|\frac{d_n}{d_0}\right| = \frac{1}{n}\Sigma_{i=1}^{n}\ln\frac{d_i}{d_{1-1}}$$

où $\frac{d_i}{d_{1-1}}$ décrit en fait de quelle façon une petite erreur d_i à la $i^{éme}$ itération, est augmentée ou diminuée dans l'itération suivante. Lyapunov a montré en suite que cette erreur tendait vers une limite "Exposant de Lyapunov".

3.2.1 Cas des systèmes discrets unidimensionnels

Soit une application discrète f de $\mathbb{R}$ dans $\mathbb{R}$ qui applique x_n sur x_{n+1}. on choisit deux conditions initiales très proches, soit x_0 et $x_0^{'}$ séparées d'une distance d_0, et on regarde comment se comportent les trajectoires qui en sont issues. On sait que :

$$d_0 = \left|x_0^{'} - x_0\right|$$

après une itération d_0 devient d_1

$$d_1 = \left|x_1^{'} - x_1\right|$$

après n itérations la distance évolue à d_n

$$d_n = \left|x_n^{'} - x_n\right|$$

$\frac{d_1}{d_0}$: décrit l'évolution de l'erreur $d_1$dans la $1^{ière}$ itération :

$$\frac{d_1}{d_0} = \frac{\left|x_1^{'} - x_1\right|}{\left|x_0^{'} - x_0\right|} = \frac{\left|f\left(x_0^{'}\right) - f\left(x_0\right)\right|}{\left|x_0^{'} - x_0\right|} = \frac{\left|f\left(x_0 + d_0\right) - f\left(x_0\right)\right|}{d_0}$$

pour d_0 infinitésimale

$$\lim_{d_0 \to 0} \frac{d_1}{d_0} = \lim_{d_0 \to 0} \frac{\left|f\left(x_0 + d_0\right) - f\left(x_0\right)\right|}{d_0} = \left|f^{'}\left(x_0\right)\right|$$

On suppose que les deux trajectoires $X\left(x_0, t\right)$ et $X\left(x_0^{'}, t\right)$ s'écartent à un rythme exponentiel à la $1^{ière}$ itération. On pourra alors trouver un réel $\lambda\left(x_1\right)$ tel qu'après 1 itération :

$$\lim_{d_0 \to 0} \frac{d_1}{d_0} = e^{\lambda(x_1)}$$

par comparaison avec la limite précédente

$$e^{\lambda(x_1)} = \left|f^{'}\left(x_0\right)\right|$$

en passant au logarithme, on trouve :

$$\lambda\left(x_1\right) = \log\left|f^{'}\left(x_0\right)\right|$$

$\lambda\left(x_1\right)$ est appelé **exposant de Lyapunov local,** qui mesure la divergence ou la convergence après la $1^{ière}$ itération.

L'évolution de l'erreur après n itérations :

$$\frac{d_n}{d_0} = \frac{\left|x_n^{'} - x_n\right|}{\left|x_0^{'} - x_0\right|} = \frac{\left|f^n\left(x_0^{'}\right) - f^n\left(x_0\right)\right|}{\left|x_0^{'} - x_0\right|} = \frac{\left|f^n\left(x_0 + d_0\right) - f^n\left(x_0\right)\right|}{d_0}$$

pour d_0 infinitésimale

$$\lim_{d_0 \to 0} \frac{d_n}{d_0} = \lim_{d_0 \to 0} \frac{\left|f^n\left(x_0 + d_0\right) - f^n\left(x_0\right)\right|}{d_0} = \left|\frac{df^n}{dx}\left(x_0\right)\right|$$

l'erreur d_n tend vers une limite, un réel λ qui représente l'exposant de Lyapunov.

$$\lim_{d_0 \to 0} \frac{d_n}{d_0} = e^{\lambda n}$$

d'où :

$$e^{\lambda n} \simeq \left| \frac{df^n}{dx}(x_0) \right| \Rightarrow \log e^{\lambda n} \simeq \log \left| \frac{df^n}{dx}(x_0) \right|$$

par conséquent

$$\lambda \simeq \frac{1}{n} \log \left| \frac{df^n}{dx}(x_0) \right|$$

Finalement, en faisant tendre n vers l'infini et en utilisant la règle de dérivation en chaîne, on obtient :

$$\begin{aligned} \lambda &\simeq \frac{1}{n} \log \left| \frac{df\left(f^{n-1}(x_0)\right)}{dx} \right| = ... = \frac{1}{n} \log \left| f'(x_{n-1}) \right| \left| f'(x_{n-2}) \right| ... \left| f'(x_1) \right| \left| f'(x_0) \right| \\ \lambda &\simeq \frac{1}{n} \log \Pi_{i=0}^{i=n} \left| f'(x_i) \right| \end{aligned}$$

on conclut

$$\lambda = \lim_{n \to +\infty} \frac{1}{n} \Sigma_{i=0}^{i=n} \log \left| f'(x_i) \right| \tag{3.1}$$

avec la notation :

$$f'(x_i) = \frac{df}{dx} \mid_{x=x_i}$$

Appliquant la formule précédente pour $x_i = x^*$ tel que x^* est le point d'équilibre, il faut que :

$$\lambda = \log |\gamma| \text{ où } \gamma = f'(x^*)$$

· Si $|\gamma| < 1 \Longrightarrow \lambda < 0$, alors x^* est **asymptotiquement stable** et la trajectoire issue d'une condition initiale x_0 $\left(ie \left\{ x_i \right\}_{i=0}^{i=n} \right)$ est asymptotiquement stable au voisinage de x^*.

· Si $|\gamma| = 1 \Longrightarrow \lambda = 0, x^*$ est **stable** et par conséquent la trajectoire issue de x_0 est périodique donc stable.

· Si $|\gamma| > 1 \Longrightarrow \lambda > 0, x^*$ est **instable** ainsi que la trajectoire issue de x_0 .

En résumé : Soient x_0 est une condition initiale, $B(x^*, \varepsilon)$ est un voisinage du point d'équilibre x^*.

· Si $x_0 \in B(x^*, \varepsilon)$ alors l'exposant de Lyapunov $\lambda = \log|\gamma|$.

· Si $x_0 \notin B(x^*, \varepsilon)$ alors l'exposant de Lyapunov λ est la moyenne de divergence exponentielle donnée par :

$$\lambda = \lim_{n \to +\infty} \frac{1}{n} \Sigma_{i=0}^{i=n} \log \left| f'(x_i) \right|$$

Exemple 3.1 : L'application logistique

$$f(x_i) = 4x_i(1 - x_i); x_i \in [0, 1]$$

En appliquant la formule (3.1) pour calculer l'exposant de Lyapunov de f.

$$\lambda = \lim_{n \to +\infty} \frac{1}{n} \Sigma_{i=0}^{i=n} \log |4(1 - 2x_i)|$$

soit : $\lambda = \log 2 > 0$ d'où le comportement est chaotique.

3.2.2 Cas des systèmes discrets multidimensionnels

Soit f une application discrète de $\mathbb{R}^p$ dans $\mathbb{R}^p$:

$$x_{n+1} = f(x_n)$$

Comme précédemment on s'intéresse à :

$$f^n(x_0 + d_0) - f^n(x) \simeq d_0 e^{n\lambda}$$

Ecrivons un développement en série limitée d'ordre 1 de $f^{\,n}(x_0)$ au voisinage de x_0' :

$$\begin{aligned} x_n - x_n' &\simeq f^n(x_0) - f^n\left(x_0'\right) \\ &\simeq \frac{d\ f^n(x_0)}{dx}(x - x_0) \\ &\simeq J(x_0) J(x_1) ... J(x_n) \left(x_0 - x_0'\right) \\ &\simeq \Pi_{i=0}^{i=n} J(x_i) \left(x_0 - x_0'\right) \end{aligned}$$

On note $\Pi_{i=0}^{i=n} J\left(x_i\right)$ par $J^{\,n}\left(x_0\right)$, ainsi :

$$x_n - x_n^{'} \simeq J^{\,n}\left(x_0\right)\left(x_0 - x_0^{'}\right)$$

où $J^{\,n}\left(x_0\right)$ représente la matrice Jacobéenne de $f^{\,n}\left(.\right)$ au point x_0. Il s'agit d'une matrice carrée $p \times p$. Si elle est diagonalisable, alors il existe une matrice inversible P_p telle que $D_p^n = P_p^{-1} J^{\,n} P_p$ est une matrice diagonale des valeurs propres $q_i\left(f^{\,k}\left(x_0\right)\right)\left(i = 1, ..., p\right)$ de $J^{\,n}$.

On définit alors les p exposants de Lyapunov de la matrice suivante :

$$\lambda_i = \lim_{n \to +\infty} \frac{1}{n} \Sigma_{i=0}^{i=n} \log q_i \left(f^{\,k}\left(x_0\right)\right) \tag{3.2}$$

λ_i représente l'exposant de Lyapunov associé à la trajectoire issue de x_0 dans la $i^{\,éme}$ direction.

Ainsi

$$x_n - x_n^{'} = \left(J\left(x^*\right)\right)^n \left(x_0 - x_0^{'}\right)$$

tel que x^* est un point d'équilibre d'où :

$$\left\|x_{i,n} - x_{i,n'}\right\| = \left[q_i\left(x^*\right)\right]^n \left\|x_{i,0} - x_{i,0'}\right\| \tag{3.3}$$

et puisque :

$$\left\|x_{i,n} - x_{i,n'}\right\| = e^{\lambda i n} \left\|x_{i,0} - x_{i,0'}\right\|$$

par comparaison avec l'égalité (3.3) on obtient :

$$e^{\lambda i n} = \left[q_i\left(x^*\right)\right]^n$$

d'où :

$$\lambda_i = \log q_i\left(x^*\right), i = 1, 2, ..., p$$

Exemple 3.2 : La transformation de boulanger

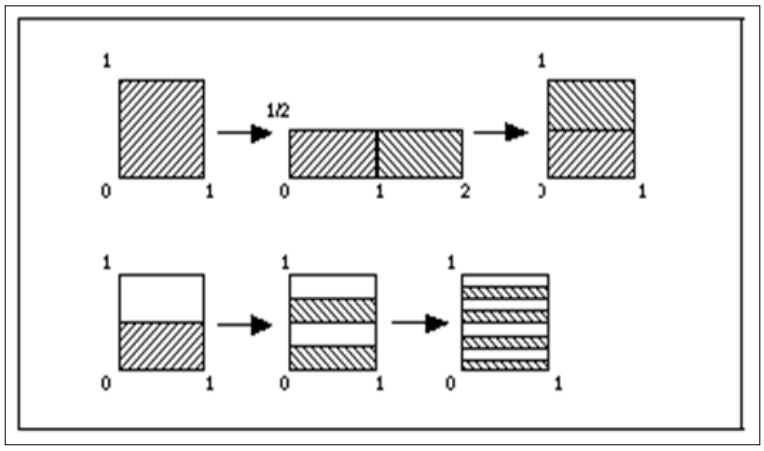


FIG. 3-1 – *La transformation de boulanger*

La transformation de boulanger (figure (3.1)) sur $E = [0,1] \times [0,1]$ définie par :

$$f(x,y) = \begin{cases} x \to 2x \,(\mathrm{mod}\, 1) \;\text{ pour } 0 \leq x < \frac{1}{2} \\ y \to \begin{cases} \frac{1}{2}ay \;\text{ pour } 0 \leq x < \frac{1}{2} \\ \frac{1}{2}(ay \;+1) \;\text{ pour } \frac{1}{2} \leq x < 1 \end{cases} \end{cases} \qquad (0 \leq a \leq 1)$$

$(0,0)$ est le seul point fixe de f dont la jacobéenne J est donnée par :

$$J = \begin{pmatrix} 2 & 0 \\ 0 & \frac{a}{2} \end{pmatrix}$$

Les valeurs propres de J de $f^{\,n}(x_0)$ au point $x_0 = (0,0)$ sont :

$$q_1(f^n(x_0)) = 2 \text{ et } q_2(f^n(x_0)) = \frac{a}{2} \;(\forall n \in \mathbb{N})$$

Appliquant la limite (3.2) dans deux directions ont obtient les exposants de Lyapunov :

$$\lambda_1 = \lim_{n \to +\infty} \frac{1}{n} \Sigma_{i=0}^{i=n} \log 2$$

$$\lambda_2 = \lim_{n\to+\infty} \frac{1}{n} \Sigma_{i=0}^{i=n} \log \frac{a}{2}$$

d'où :

$$\lambda_1 = \log 2 \text{ et } \lambda_2 = \log \frac{a}{2}$$

3.2.3 Cas des systèmes continus multidimensionnels

Pour un système différentiel de dimension n défini par f tel que :

$$\dot{x} = f\left(x\left(t\right)\right) \text{ tel que : } t \in \mathbb{R}, x\left(t\right) \in \mathbb{R}^n$$

l'exposant de Lyapunov dans la direction i est donné par :

$$\lambda_i = \lim_{t\to+\infty} \frac{1}{t} \log \frac{\left\|x_i\left(t\right) - x_i^{'}\left(t\right)\right\|}{\left\|x_i\left(0\right) - x_i^{'}\left(0\right)\right\|}$$

Exemple 3.3 : Le système de Lorenz

$$\begin{cases} \dot{x} = 10\left(y - x\right) \\ \dot{y} = 28x - y - xz \\ \dot{z} = xy - \frac{8}{3}z \end{cases}$$

Les exposants de Lyapunov pour une condition initiale x_0 choisie sont :

$$\lambda_1 \simeq 2.16, \lambda_2 \simeq 0.00, \lambda_3 \simeq -32.40$$

Les exposants de Lyapunov permettent donc de quantifier la sensibilité aux conditions initiales **(SCI)** mais aussi de séparer les comportements instables ou chaotiques des comportements stables et prévisibles. Si un exposant de Lyapunov est strictement positif, alors la **SCI** est très grande et le système peut être considéré comme chaotique. Par contre, s'ils sont tous négatifs ou égaux à zéro, on est en présence d'un phénomène stable ou périodique. Pour une application multidimensionnelle on peut résumer la correspondance entre le type de l'attracteur et le signe des exposants de Lyapunov dans le tableau ci dessous :

Type d'attracteur	*Exposants de Lyapunov*
Point fixe	$0 > \lambda_1 \geq \lambda_2 \cdots \geq \lambda_n$
Cycle	$\lambda_1 = 0,\ \ 0 > \lambda_1 \geq \lambda_2 \cdots \geq \lambda_n$
Tore	$\lambda_1 = \lambda_2 = 0,\ 0 > \lambda_3 \geq \lambda_4 \cdots \geq \lambda_n$
K-tore	$\lambda_1 = \lambda_2 = \cdots = \lambda_K = 0,\ 0 > \lambda_{K+1} \geq \lambda_{K+2} \geq \cdots \geq \lambda_n$
Attracteur étrange	$\lambda_1 > 0,\ \sum \lambda_i < 0$

Il faut surtout retenir que pour un système dissipatif on a : $\sum \lambda_i < 0$, et que l'un des exposants de Lyapunov soit strictement positif pour que le système soit considéré comme chaotique.

Différents algorithmes ont été développés pour calculer les exposants de Lyapunov.

3.2.4 L'algorithme de Wolf

Cet algorithme permet de calculer les exposants de Lyapunov à partir du calcul effectif de la divergence de deux trajectoires après t pas de temps par rapport à la perturbation introduite parallèlement, et ce au sein d'un attracteur, les étapes de l'algorithme sont :

1− changement du paramètre de contrôle.

2− choix aléatoire d'une condition initiale.

3− création d'une nouvelle trajectoire à partir de la trajectoire courante à laquelle on ajoute une petite perturbation.

4− évolution dans l'attracteur de ces deux trajectoires voisines et calcul de la moyenne de la divergence renormalisée entre ces deux trajectoires.

5− réajustement de l'écart, permettant ainsi à chaque pas de temps de l'évolution du point précédent le calcul d'une moyenne de la divergence.

6− retour au point (5) effectué selon un nombre donné.

7− retour au point (1).

8− représentation du plus grand exposant de Lyapunov en fonction du paramètre de contrôle donné.

Exemple 3.4 : exposants de Lyapunov du système de Lorenz par l'algorithme de Wolf

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

pour $\sigma = 16.0$; $r = 45.92$; $b = 4.0$ on a $\lambda_1 = 2.11, \lambda_2 = 0.00, \lambda_3 = -32.40$ avec $\Delta t = 0.01$; le nombre de pas 20000.

3.3 Dimension fractale

Le terme dimension est souvent lié à celui de coordonnée, c'est à dire variable nécessaire pour décrire la position d'un élément, d'un ensemble et cette dimension est par définition un nombre entier.

La dimension de l'attracteur :

· Si l'attracteur est un point sa dimension est 0.

· Si l'attracteur est une ligne ou une courbe fermé sa dimension est 1 et ainsi de suite.

Mais il y a un autre genre d'attracteur qui a une forme inhabituelle, une structure géométrique fractale due à l'étirement dans une direction et au repliement dans une autre direction qui est l'attracteur étrange.

La caractéristique géométrique principale de ce type d'attracteur est leur dimension fractale.

Définition 3.1 :

Selon **Robert Mandelbrot** (1982), un ensemble A est fractal si sa dimension de Hausdorff n'est pas entière. Il existe aussi d'autres dimensions non entières ou fractales comme la dimension de corrélation (ou de **Grassberger** et **Procaccia**), la dimension de Lyapunov. Toutes ces dimensions sont très proches les unes des autres et satisfont les propriétés suivantes :

1− Si $A \subset B$ alors $d(A) \subset d(B)$ ($d(.)$ dimension fractale).

2− Si $A = \varnothing$ alors $d(A) = 0$.

3 − $d(A \times B) = d(A) \times d(B)$.

4− Si f est une application différentiable sur A alors $(f(A)) = d(A)$.

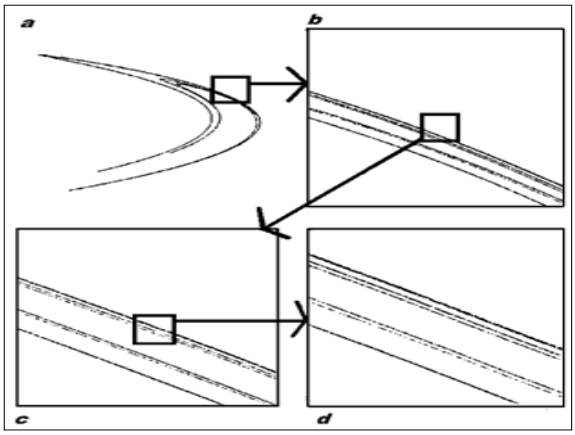


FIG. 3-2 – *L'attracteur de Hénon, agrandissement du carré, si on zoom à n'importe quelle échelle on retrouve toujours la même structure fractale*

3.3.1 Dimension de capacité ou dimension de Kolmogrov

Soit X un ensemble de points de l'attracteur, on recouvre X par un nombre minimal $N(\varepsilon)$ d'hypercubes de coté ε.

– Si X est un carré de coté L il peut être recouvert par $N(\varepsilon) = \left(\frac{L}{\varepsilon}\right)^2$ petits carrés de cotés ε.

– Dans le cas général on a :

$$N(\varepsilon) = \left(\frac{L}{\varepsilon}\right)^d \text{ d'où } d = \frac{\log N(\varepsilon)}{\log L - \log \varepsilon} \text{ quand } \varepsilon \longrightarrow 0 \ \log L << -\log \varepsilon$$

Définition 3.2 :

La dimension de Kolomogrov ou de capacité est définie par :

$$d_c = \lim_{-\varepsilon \to 0} \frac{\log N(\varepsilon)}{\log \varepsilon}$$

Exemple 3.5 :

1– La dimension d'un point est 0, car il sera recouvert par une seule boite (hyper cube), $\forall \varepsilon$.

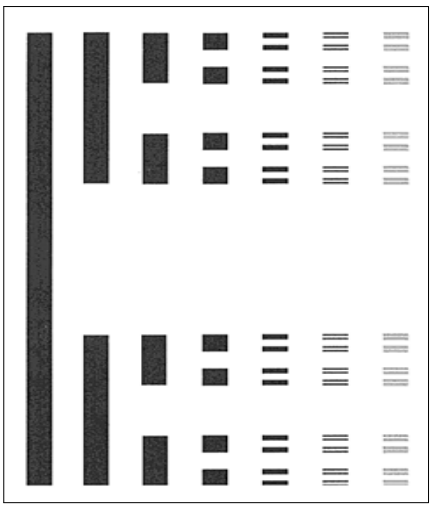


FIG. 3-3 – *L'ensemble de Cantor*

2– La dimension de plusieurs points isolés est aussi 0.

3– La dimension d'un segment est 1 car :

$$d_k = \lim_{-\varepsilon \to 0} \frac{\log n\left(\varepsilon\right)}{\log \varepsilon} = \lim_{-\varepsilon \to 0} \frac{\log l - \log \varepsilon}{\log \varepsilon} = 1$$

Dimension de l'ensemble de Cantor :

Soit un segment de longueur 1, l'ensemble triadique de Cantor est obtenu en enlevant à ce segment son tiers central, puis on répète cette opération sur les deux segments restants, et ainsi de suite (figure (3.3)).

L'ensemble K des points restants s'appelle l'**ensemble triadique de Cantor**.

$$\begin{aligned}
K_0 &= [0,1] \\
K_1 &= \left[0,\frac{1}{3}\right] \cup \left[\frac{2}{3},1\right] \\
K_2 &= \left[0,\frac{1}{9}\right] \cup \left[\frac{2}{9},\frac{1}{3}\right] \cup \left[\frac{2}{3},\frac{7}{9}\right] \cup \left[\frac{8}{9},1\right] \\
&\cdot \\
&\cdot \\
&\cdot \\
K_n &= \left[0,\left(\frac{1}{3}\right)^n\right] \cup \left[2\left(\frac{1}{3}\right)^n,\left(\frac{1}{3}\right)^{n-1}\right] \cup ... \cup \left[1-\left(\frac{1}{3}\right)^n,1\right] \\
... &\subset K_{n+1} \subset K_n \subset ... \subset K_2 \subset K_1 \subset K_0 = [0,1]
\end{aligned}$$

à l'étape n, l'ensemble K_n est constitué de 2^n intervalles de longueur $\left(\frac{1}{3}\right)^n$, la longueur L de l'ensemble triadique est nulle car :

$$\begin{aligned}
L &= 1-\frac{1}{3}-\frac{2}{9}-\frac{4}{27}-... \\
&= 1-\frac{1}{3}\sum_{n=0}^{n=\infty}\left(\frac{2}{3}\right)^n = 1-\frac{1}{3}\frac{1}{1-\frac{2}{3}} = 0
\end{aligned}$$

$$d_k = \lim_{-\varepsilon\to 0}\frac{\log N(\epsilon)}{\log \varepsilon} = -\lim_{n\to+\infty}\frac{\log 2^n}{\log\left(\frac{1}{3}\right)^n} = \frac{\log 2}{\log 3} \simeq 0.6309$$

Dimension de la courbe de Koch :

· on enlève le tiers central du segment de longueur $\frac{1}{3}$ pour former une tente (figure (3.4)).

· pour la seconde on enlève les tiers centraux des petits segments et on les remplace par deux segments de la même longueur.

· à la $n^{ème}$ étape de la construction on aura 4^n segments, la longueur de chacun est $\left(\frac{1}{3}\right)^n$.

Calcul de la dimension d_k de la courbe de koch :

$$\begin{aligned}
d_k &= \lim_{-\varepsilon\to 0}\frac{\log N(\varepsilon)}{\log(\varepsilon)} \\
&= \lim_{-\varepsilon\to 0}\frac{\log 4^n}{\log\left(\frac{1}{3}\right)^n} = \lim_{\varepsilon\to 0}\frac{\log 4}{\log 3} \simeq 1.26
\end{aligned}$$

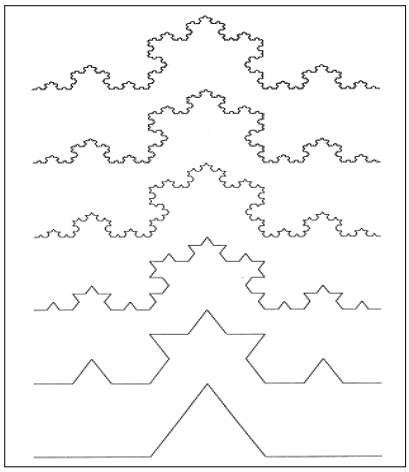


FIG. 3-4 – *Construction de la courbe de Koch qui a une structure fractale*

On remarque que la dimension de la courbe de Koch est supérieure à la dimension d'une courbe $(d = 1)$ mais inférieure à celle d'une surface $(d = 2)$.

3.3.2 Dimension de Hausdorff-Bésikovich

La définition de la dimension de capacité n'est pas facilement applicable, car la limite n'existe pas toujours.

Ce problème de convergence a été résolu par la dimension de **Hausdorff**, ici les hyper cubes ont des cotés de longueur différentes et inférieur ou égales à 1.

Avec ces hyper cubes on recouvre X l'ensemble le plus efficacement possible.

Soit $n(l)$ le nombre minimum des hyper cubes suffisant pour couvrir X.

U est un ensemble de $\mathbb{R}^n$.

$$X \subset \cup_{i=1}^{\infty} U_i, 0 < |U_i| < l$$

$$N(l) = \inf \left\{ \sum_{i=1}^{\infty} |U_i|^d, |U_i| < l \right\} = \mu_d(X, l) \, et \, |U_i| = \sup \{|x - y| : x, y \in U_i\}$$

La mesure de Hausdorff d dimensionnelle est définie par :

$$\mu_d(X) = \lim_{l \to 0} \mu_d(X, l)$$

Hausdorff a montré qu'il existe un réel d_H, unique tel que :

$$\mu_d(X) = \begin{cases} 0, \text{ si } d > d_H \\ \infty, \text{ si } d < d_H \end{cases}$$

d_H est appelé la dimension de Hausdorff de l'ensemble X.

Elle est la préférée des mathématiciens, mais elle reste difficile à calculer. Dans beaucoup de cas la dimension de Hausdorff est égale à la dimension de capacité.

3.3.3 Dimension de corrélation

La dimension de Hausdorff et de capacité sont difficiles à calculer lorsque l'espace de phases est de dimension élevée. Pour calculer plus facilement la dimension de l'attracteur, **Grassberger** et **Procaccia** ont défini une dimension en utilisant la fonction de corrélation, qui est appelée dimension de corrélation d_c.

Sur une trajectoire d'un attracteur qui a suffisamment évolué dans le temps, on prend N points et de ces derniers on choisit ceux qui sont en commun avec la trajectoire et la boule de rayon R et de centre i, un point fixé de la trajectoire.

On définit la fonction de corrélation $C(R)$ en utilisant la fonction Θ de **Heaviside** tel que :

$$\Theta : \begin{cases} \Theta(x) = 0 \text{ si } x < 0 \\ \Theta(x) = 1 \text{ si } x \geq 0 \end{cases}$$

$$C(R) = \frac{1}{N(N-1)} \sum_{i=1}^{N} \sum_{j=1, i \neq j} \Theta(R - |\vec{x}_i - \vec{x}_j|)$$

avec $\vec{x}_i = \left(x_i, x_{i+t_l}, x_{i+2t_l} + ... + x_{i+(d-1)t_l}\right)$ et t_l est le temps retard qui représente l'intervalle de temps entre deux échantillons successifs utilisés pour construire le vecteur $\vec{x}_i$.

La distance euclidienne est usuellement choisie pour calculer la distance entre deux vecteurs.

$$|\vec{x}_i - \vec{x}_j| = \sqrt{\sum_{k=0}^{d-1} (x_{i+kt_l} - x_{j+kt_l})^2}$$

Par commodité de calcul on utilise la distance :

$$|\vec{x}_i - \vec{x}_j| = \max_k |x_{i+kt_l} - x_{j+kt_l}|$$

$$C(R) = \frac{1}{N} \sum_{i=1}^{N} \sum_{j=1, i \neq j} \Theta(R - |\vec{x}_i - \vec{x}_j|)$$

Pour balayer tout l'attracteur on passe à la limite sur $N\,(N \to \infty)$ et la dimension de corrélation est le nombre qui satisfait :

$$C(R) = \lim_{R \to 0} K R^D$$

en utilisant le logarithme on aura :

$$D_C = \lim_{R \to \infty} \frac{\log C(R)}{\log R}$$

3.3.4 Dimension de Lyapunov

Soit A un attracteur représenté dans un espace multidimensionnel de dimension d, **Kaplan** et **York** ont suggéré de calculer la dimension de cette attracteur en utilisant ses exposants de Lyapunov de la manière suivante :

classant les exposants de Lyapunov $\lambda_1.\lambda_2, ..., \lambda_d$ La dimension de Lyapunov D_L est définie par :

$$D_L = j + \frac{\sum_{i=1}^{j} \lambda_i}{\lambda_{j+1}}$$

où j est le plus grand entier qui satisfait :

$$\lambda_1 + \lambda_2 + \lambda_3 + ... + \lambda_j \geq 0$$

Exemple 3.6 :

Les exposants de Lyapunov de la transformation du boulanger sont :

$$\lambda_1 = 2 \text{ et } \lambda_2 = \log \frac{a}{2} \text{ d'où } D_L = 1 + \frac{\log 2}{\log 2 - \log a}$$

3.4 Entropie

L'entropie est une notion qui fut introduite en mécanique statistique, en thermodynamique et dans la théorie de l'information. On définit parfois l'entropie comme la mesure du désordre d'un système ou de sa prédictibilité, l'entropie est considérée comme une fonction d'état d'un système croissante jusqu'à un maximum lorsque le système atteint un état d'équilibre, **Shannon**, **Weiner** et **Von Neumann** ont proposé que l'entropie soit compensée par une croissance en information.

Au milieu des années 50, **Kolmogorov** proposait d'après les travaux de **J. Sinai** et **N.S. Krylov**, une définition de l'entropie appelée (**entropie par unité de temps**) puis rapidement (**entropie de Kolmogorov**). Cette entropie a la propriété d'être positive dans les systèmes dynamiques et permet de mesurer la complexité du comportement d'un tel système. A la fin des années 70, **Robert Shaw** décrit l'entropie comme suit : ‹‹ si l'ensemble des états accessibles au système varie en fonction polynomiale du temps le taux (de la quantité d'information) se rapproche de zéro et l'évolution du système demeure prévisible. Au contraire, lorsque la fonction est exponentielle croissante du temps le système est chaotique ››.

3.4.1 L'entropie d'un système dynamique

L'idée de la définition de l'entropie d'un système dynamique est la suivante : supposons que la condition initiale du système n'est pas connue avec une précision infinie, mais que le comportement que l'on va observer en faisant évoluer le système va nous informer de mieux en mieux sur l'état de départ dans l'espace des phases, alors cette information sur l'ensemble des trajectoires permet de reconstituer le point de départ. La quantité moyenne d'information qu'on gagne en faisant le processus (ou à chaque itération) est l'**entropie du système**. La notion d'information repose sur deux idées.

1− Un événement rare apporte plus d'informations qu'un événement fréquent.

2− Les informations fournies par des événements indépendants s'ajoutent, par exemple : connaître l'état d'un système à un instant t c'est connaître sa position et connaître sa vitesse.

Considérons un système qui peut prendre un état de probabilité p; cela revient à dire qu'il passe une fraction p de temps dans cet état, et le système lui apporte une information égale à :

$$S = \log \frac{1}{p} \tag{3.4}$$

La quantité $\frac{1}{p}$ mesure la rareté d'un évènement. C'est un nombre supérieur ou égal à 1. Un évènement qui n'arrive presque jamais a une rareté grande, donc une infinité d'informations, un évènement qui arrive presque toujours a une rareté de 1,donc l'information est nulle.

L'entropie est l'information reçue par un système en moyenne.

Si on appelle p_i la probabilité pour que le système soit dans l'état i (pour i allant de 1 à n est le nombre d'états possibles) on trouve la célèbre formule :

$$S = -\sum_{i=1}^{i=n} p_i \log p_i \tag{3.5}$$

La formule (3.5) est généralisation de (3.4) si les états ne sont pas équiprobables.

3.4.2 L'entropie et l'espace des phases

La notion fondamentale de l'entropie est basée sur le calcul des états accessibles du système sous certaines considérations et pour cela, Kolmogorov et Sinai ont proposé de quadriller l'espace des phases en des cellules élémentaires de même diamètre. Pour les systèmes dissipatifs divisant seulement la région contenant l'attracteur, on calcule p_i, la possibilité qu'une trajectoire issue d'une cellule C_0 soit dans la $i^{ème}$ cellule C_i tel que : M est le nombre de conditions prises dans C_0, M_i est le nombre de points de trajectoires situées en C_i sachant que la région d'évolution est divisée en m cellules.

L'entropie S_i après n unités de temps est donnée par :

$$S_n = -\sum_{i=1}^{i=n} p_i \log p_i$$

Dans la théorie de l'information la trajectoire est considérée comme un message, les cellules

de la partition sont associées aux lettres de l'alphabet, parfois un texte est une suite finie de lettres 0 et 1. L'entropie d'un texte peut être calculée à partir de la fréquence des 0 et des 1. Elle est maximale lorsque le texte ne contient que des 0 (ou des 1). Le système d'équations différentielles régissant la représentation dans l'espace des phases suppose que le système soit considéré comme réversible dans le sens où aucune information n'est perdue au cours du temps. Dans les systèmes dissipatifs l'information sur les conditions initiales est perdue. Si le système est chaotique, l'information est créée, c'est dans le sens qu'un ensemble d'états initiaux indiscernables (a une certaine précision ε après) sur l'attracteur aboutit de façon non prédictible à une multitude d'états finaux, on a en quelque sorte un enrichissement de l'information. Une variation infinitésimale des conditions initiales provoque un comportement radicalement différent du système donc un changement de l'information que l'on a sur un système. Dans le cas d'un système parfaitement connu et modélisé même une infinité de mesures infiniment rapprochée traitées par une puissance de calcul infinie ne suffiraient pas à empêcher une divergence exponentielle croissante entre la prévision et la création de l'information.

La $K-$entropie K_n après n unités de temps est définie par :

$$K_n = \frac{1}{\tau}\left(S_{n+1} - S_n\right)$$

K_n est le taux de changement de l'entropie allant de $i = n\tau$ à $t = (n+1)\,\tau$ ($\tau :$ unité de temps), la valeur moyenne de la $K-$entropie sur tout l'attracteur (soit une longue durée) divisé en des cellules de diamètre ε est donnée par :

$$\begin{aligned} K_n &= \lim_{N\to+\infty} \frac{1}{N\tau} \sum_{n=0}^{N} \left(S_{n+1} - S_n\right) \\ &= \lim_{N\to+\infty} \frac{1}{N\tau} \left(S_n - S_0\right) \end{aligned}$$

La partition doit être plus fine pour que chaque cellule contienne un seul point. Cela nous permet de suivre la trajectoire point par point et ainsi faire en sorte que la $K-$entropie soit indépendante du choix de la partition, donc on réduit la taille des cellules en prenant $\varepsilon \to 0$. De plus la description de la dynamique devait être la plus précise possible on fait tendre l'unité

de temps vers 0, ce qui conduit à la définition suivante :

$$K = \lim_{\tau \to 0} \lim_{\varepsilon \to 0} \lim_{N \to +\infty} \frac{1}{N\tau} (S_n - S_0)$$

La position de la $K-$entropie renseigne sur l'état chaotique du système donc sur son imprévisibilité à long terme.

Exemple 3.7 : la $K-$entropie de l'application dyadique

$$x_{n+1} = 2x_n \,(\mathrm{mod}\, 1)$$

On doit faire une partition de l'intervalle $[0, 1]$ en M intervalles de longueur $\frac{1}{M}$. Un message à une lettre a pour entropie $S_1 = \log M$. Pour passer d'un ‹‹ message à une lettre ›› aux ‹‹ message à deux lettres ››, l'intervalle de longueur $\frac{1}{M}$ auquel appartenait la condition initiale x_0 se trouve étiré d'un facteur $2\,(x_1 = 2x_{.0})$ et alors :

$$S_2 = -\sum_{i=1}^{2m} p_i \log p_i = -\,(2M)\left(\frac{1}{2M}\right)\log\left(\frac{1}{2M}\right) = \log 2M$$

d'où :

$$S_2 = \log 2 + \log M$$

Les trajectoires, en itérant le système k fois, s'exprime comme des messages à k lettres ($2^k M$ messages de même probabilité), l'écart après k itérations est $\delta_{x_k} = 2^k \delta_{x_0}$.

Alors :

$$S_k = -\sum_{i=1}^{2m} p_i \log p_i = -\left(2^k M\right)\left(\frac{1}{2^k M}\right)\log\left(\frac{1}{2^k M}\right) = \log 2^k M$$

d'où :

$$S_k = k \log 2 + \log M$$

la définition de la $K-$entropie conduit à :

$$K = \lim_{k \to +\infty} \frac{1}{k} (S_k - S_1) \text{ d'où } K = \log 2$$

3.4.3 Le relation entre l'entropie et les exposants de Lyapunov

On recouvre la région de l'attracteur par un nombre fini de cellules, N_0 est le nombre de cellules initiales évoluant après n unités de temps en N_n cellules visitées par les trajectoires, le nombre de cellules augmente exponentiellement avec le temps et on aura :

$$N_n = e^{\lambda_i n\tau} N_0$$

où λ_i exposant de Lyapunov positif dans une direction i, l'entropie est donnée par la formule précédente :

$$S_n = -\sum_{i=1}^{i=m} p_i \log p_i$$

la probabilité p_i est supposée uniforme, m désigne le nombre de cellules de la partition, alors :

$$S_n = \log N_n$$

La $K-$entropie est donnée par :

$$\begin{aligned} K &= \lim_{\tau\to 0}\lim_{\varepsilon\to 0}\lim_{n\to+\infty} \frac{1}{n\tau}\left(S_n - S_0\right) \\ &= \lim_{\tau\to 0}\lim_{\varepsilon\to 0}\lim_{n\to+\infty} \frac{1}{n\tau}\left(\log N_n - \log N_0\right) \\ &= \lim_{\tau\to 0}\lim_{n\to+\infty} \frac{1}{n\tau}\log\left(\frac{N_n}{N_0}\right) \\ &= \lim_{\tau\to 0}\lim_{n\to+\infty} \frac{1}{n\tau} e^{\lambda_i n\tau} \end{aligned}$$

d'où :

$$K = \lambda_i$$

Par conséquent ; si l'étirement se fait dans une seule direction la $K-$entropie est donnée par l'exposant de Lyapunov positif donc :

$$K = \lambda_i$$

et si l'étirement se fait dans plusieurs directions, alors la $K-$entropie est donnée par :

$$K = \sum_{i=1}^{k} \lambda_i$$

où $\lambda_1, \lambda_2, ...\lambda_k$ représentent les exposants de Lyapunov positifs.

3.5 Séries temporelles

Comme cela a été dit précédemment, les séries temporelles et le spectre de puissance sont à la base de méthodes d'analyse destinées à identifier ou caractériser un régime dynamique. L'extraction d'un "sens physique" d'un signal expérimental ou la détermination des propriétés les plus significatives de la structure topologique d'un attracteur dans l'espace des phases est possible grâce à la méthode de "reconstruction" du portrait de phase, ou méthode des retards, à partir d'une variable temporelle.

L'idée de base est que les caractéristiques de la dynamique d'un système transparaissent et se reflètent sur chacune de ses variables dynamiques.

3.5.1 Séries temporelles

Définition 3.3 :

Une série temporelle est une série de mesures (**traitement numérique**) du signal effectué à intervalles de temps réguliers, t_r :

$$\Phi_i^t(X), \Phi_i^{(t+t_r)}(X), \Phi_i^{(t+2t_r)}(X), ...$$

où t_r est le "temps retard" convenablement choisi et $\Phi_i^t(X)$ est la $i^{éme}$ composante de $\Phi^t(X)$.

L'évolution temporelle d'un système dynamique est souvent représentée par la valeur d'une de ses variables à intervalle régulier : c'est ce qu'on appelle sa **série temporelle**.

Exemple 3.8 :

La figure (3.5) donne les séries temporelles de la vitesse angulaire $x(t) = \frac{d\theta}{dt}$ du pendule

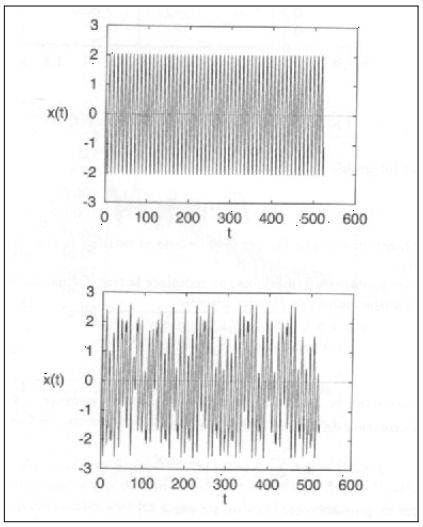


FIG. 3-5 – *Séries temporelles du pendule amorti et entretenu avec* $A = 0.95$ *(en haut) et* $A = 1.5$ *(en bas)*

amorti et entretenu dont le mouvement est régi par l'équation :

$$\frac{d^2\theta}{dt^2} + \alpha\frac{d\theta}{dt} + \sin\theta = A\cos(\omega_D t)$$

où $\alpha = 05$, $\omega_D = \frac{2}{3}$, $A = 0.95$ et $A = 1.5$ respectivement.

Lorsque $A = 0.95$, le mouvement semble être périodique ; $A = 1.5$ conduit à un mouvement que l'on peut, à priori, quantifier de chaotique.

3.5.2 Spectre de Fourier

Soit $x(t) = a(t) + ib(t)$ une fonction à valeurs complexes, de la variables réelle t. La **transformation de Fourier** de $x(t)$ est définie par :

$$X(f) = \int_{-\infty}^{+\infty} x(t)\, e^{-2\pi i f t} dt = R(f) + I(f) \tag{3.6}$$

La quantité : $S(f) = |X(f)|^2 = R^2(f) + I^2(f)$ est appelée le **spectre de Fourier** ou **spectre de puissance** de $x(t)$.

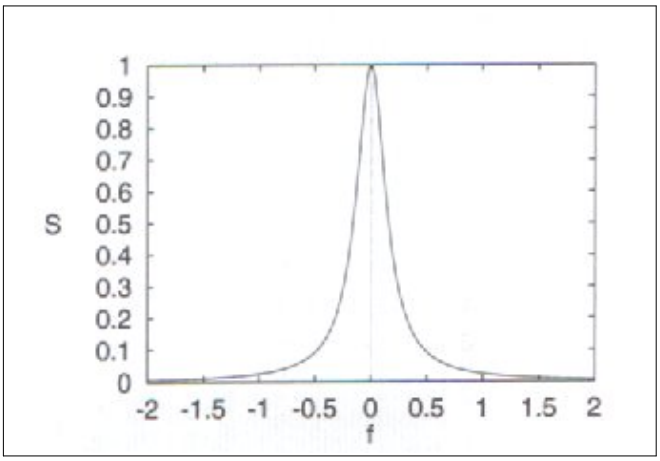


FIG. 3-6 – *Le spectre de puissance de* $x(t) = e^{-t}$

La transformation inverse de (3.6) est :

$$x(t) = \int_{-\infty}^{+\infty} x(f)\, e^{2\pi i f t} df \tag{3.7}$$

Exemple 3.9 :

Calculons le spectre de puissance de :

$$x(t) = e^{-t}; \text{si } t > 0 \text{ et } x(t) = 0 \text{ si } t < 0 \tag{3.8}$$

on a :

$$X(f) = \int_{0}^{+\infty} e^{-(1+2\pi i f)t} dt = \frac{1}{1 + 2\pi i f}$$

on en déduit :

$$S(f) = |X(f)|^2 = \frac{1}{1 + 4\pi^2 i f}$$

Le graphe de $S(f)$ est donné sur la figure (3.6) .

· Si $x(t)$ est intégrable dans le sens :

$$\int_{-\infty}^{+\infty} |x(t)|\, dt < \infty$$

alors sa transformation de Fourier $X(f)$ existe et satisfait la transformation inverse (3.7).

Dans les problèmes numériques, on remplace la transformation de Fourier (3.6) par une transformation de Fourier discrète :

$$X(n\Delta f) = \Delta t \sum_{k=0}^{N-1} x(k\Delta t)\, e^{-2\pi ink/N} \tag{3.9}$$

avec :

$$\Delta f = \frac{1}{N\Delta} \text{ et } n = 0, 1, ..., N-1 \tag{3.10}$$

La transformation de Fourier discrète inverse est :

$$x(k\Delta f) = \Delta f \sum_{n=0}^{N-1} X(n\Delta f)\, e^{2i\pi nk/N}; k = 0, 1, ..., N-1$$

Le spectre de puissance est alors donné par :

$$S(n\Delta f) = |X(n\Delta f)|^2 = |RX(n\Delta f)|^2 + |IX(n\Delta f)|^2; n = 0, 1, ..., N-1$$

Pour réaliser une transformation de Fourier discrète de $x(t)$, on doit donc se donner N et Δt. Pour la fonction (3.8), on peut prendre par exemple $N = 2^{10} = 1024$, $\Delta t = 2^{-7} = \frac{1}{128}$, on aura alors $\Delta f = \frac{1}{8}$.

Dans les exemples précédents $x(t)$ est une variable de l'espace des phases (sa partie imaginaire est donc nulle) et les $x(k\Delta t), k = 0, 1, ..., N-1$ seront calculés par la méthode de **Runge-Kutta**.

Exemple 3.10 :

Le spectre de puissance S de $x(t) = \frac{d\theta}{dt}$ de l'exemple 3.7 par les formules (3.9) et (3.10) en choisissant $N = 2^{12}, \Delta t = 0.1$ (à ne pas confondre avec le pas de temps h de la méthode de Runge-Kutta qui, qui est ici $h = 0.001$. Les constantes sont les mêmes que dans l'exemple 1.Les résultats sont portés sur la figure (3.7). Les 200 premières itérations n'ont pas été pris en compte afin de s'abstraire de tout régime transitoire.

On peut noter le **pic** à la fréquence 0.1 : c'est la fréquence de la **force d'entraînement**. En effet, pour $\omega_D = \frac{2}{3}$ la période de la force d'entraînement est $T_D = \frac{2\pi}{\omega_D} = 3\pi$, d'où $f_D = \frac{1}{T_D} \simeq 0.1$.

Le premier spectre présente un nombre limité de fréquences, la fréquence f_D et une de ses

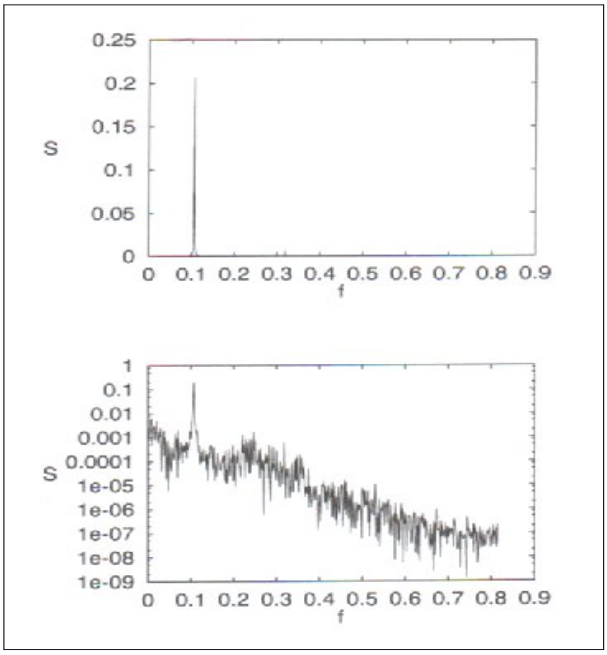


FIG. 3-7 – *Spectre de puissance du pendule amorti et entretenu avec* $A = 0.95$ *(à gauche) et* $A = 1.5$ *(à droite)*

harmoniques : le mouvement est périodique. Le spectre correspondant à l'amplitude $A = 1.5$ est dense : c'est, en général, la signature d'un mouvement chaotique.

Un **signal** peut posséder r fréquences de base et le spectre comporte toutes les fréquences $|n_1 f_1 + n_2 f_2 + ... + n_r f_r|$, les n_i étant des entiers de signe quelconque. La trajectoire dans l'espace des phases s'inscrit sur un tore de dimension r.

Prenons, pour simplifier l'exposé $r = 2$. Deux cas sont à considérer :

· $\frac{f_1}{f_2}$ est un nombre **irrationnel**, $|n_1 f_1 + n_2 f_2|$ forment un ensemble dense sur les réels positifs. Le spectre est donc dense mais non-continu : le mouvement est **quasi-périodique**.

· $\left|\frac{f_1}{f_2}\right|$ est un nombre **rationnel irréductible**, $\left|\frac{n_1}{n_2}\right|$ le spectre présente des raies qui sont les harmoniques de la fréquence $f_0 = \left|\frac{f_1}{n_2}\right| = \left|\frac{f_2}{n_1}\right|$, le mouvement est **périodique**.

Dans le cas général, le mouvement est quasi-périodique si $\sum_1^r n_i f_i \neq 0$ pour $n_i \in \mathbb{Z}$. Lorsqu'un signal n'est ni périodique, ni quasi-périodique, il est dit **apériodique**. Le spectre de Fourier est alors **continu**.

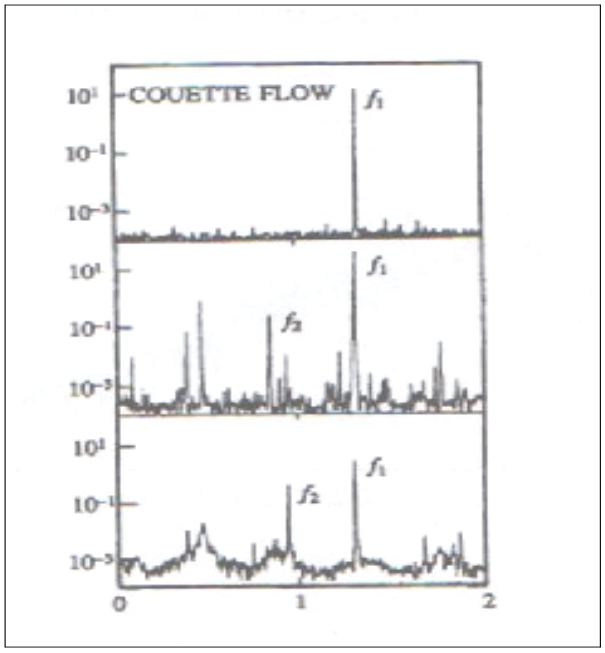


FIG. 3-8 – *Spectre d'un écoulement de Couette : spectre périodique, spectre quasi-périodique et spectre apériodique (de haut en bas) d'après Fenstermacher. Gollub et swinney*

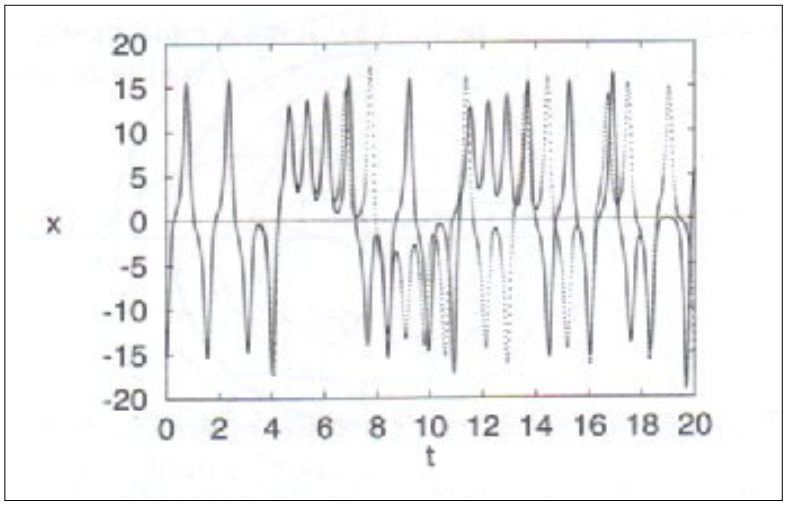


FIG. 3-9 – *Deux séries temporelles du système de Lorenz*

Les spectres de la figure (3.8) ont été mesurés par **R. Fenstermacher**, **H.L. Swinney** et **S.P. Gollub** dans le cas d'un écoulement de **Couette** : il s'agit de l'écoulement d'un fluide entre deux cylindres coaxiaux, le cylindre intérieur tournant à une vitesse constante. Les spectres de la figure (3.8) (de haut en bas) correspondant à des vitesses croissantes du cylindre intérieur et à des écoulements respectivement périodique (1 pic de fréquence), quasi-périodique (plusieurs fréquences indépendantes), et apériodique (l'élargissement des pics et la croissance du niveau du bruit à base fréquence suggèrent l'existence d'un attracteur étrange).

Remarque 3.1 :

En pratique, dans le cas d'un signal quasi-périodique, on n'observe qu'un nombre limité de fréquences dont l'amplitude soit significative car, les fréquences qui correspondent à des valeurs de n, supérieurs à quelques unités, ont une amplitude trop faible pour être détectées.

Remarque 3.2 :

La figure (3.9) donne les résultats de l'intégration du système de Lorenz par la méthode de Runge-Kutta. Partant de deux conditions initiales voisines, l'une $x(0) = -15.00, y(0) = -17.00, z(0) = 35.00$, l'autre, $x(0) = -15.01$ et les mêmes $y(0), z(0)$, on aboutit à deux séries temporelles différentes. C'est l'exemple de la sensibilité aux conditions initiales des attracteurs étranges.

Deuxième partie

Cryptographie et chaos

Chapitre 4

Introduction à la Cryptographie

4.1 Introduction et Historique

Elle vient du mot grec "Kryptos" qui signifie « cacher », et "graphia" qui signifie « par écrit ».

La cryptographie, ou l'art de chiffrer, de coder les messages est une science aussi vieille que l'écriture.

Elle a vécu à partir des années 70 une véritable révolution. Quelques idées brillantes et paradoxales (fonction à sens unique, clés publiques,...) puisant leur inspiration dans la théorie des nombres, ont fait basculer la cryptographie d'une culture séculaire du secret vers une véritable étude scientifique de la confiance. A l'ère de l'Internet et du commerce électronique, elle est devennue une discipline aux facettes multiples. Outre les préocupations traditionnelles de confidentialité des échanges, se sont posées toutes sortes de nouvelles questions : comment s'assurer de l'identité d'un correspondant à travers des réseaux de communication publiques ? Comment authentifier un document numérique à l'aide d'une signature lisible par tous ? Comment réaliser une monnaie numérique parfaitement anonyme ?... Pour répendre à toutes ces questions la cryptographie a développé un arsenal mathématique conséquent, puisant dans l'arithmétique, l'algèbre, la complexité algorithmique, et plus récement la théorie du chaos.

La cryptographie a eu une histoire intéressante, ses racines remontent vers 2000 avant **J.C** en Egypte lorsque les hiéroglyphes furent utilisés pour décorer les tombes afin de raconter l'histoire de la vie du défunt.

Une méthode de cryptographie de l'alphabet Hébreu requis pour être retournée afin que chaque lettre dans l'alphabet d'origine est associée à une lettre différente dans l'alphabet inversé. Cette méthode de cryptage a été appelée méthode d'**Atbash**. Un exemple d'une clé de chiffrement utilisée dans le schéma de chiffrement d'Atbash ci-dessous.

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

Par exemple, le mot "sécurité" est crypté en "hvxfirgv". Il s'agit d'une substitution de chiffrement. Ce type de chiffrement est considéré comme une substitution monoalphabétique, par rapport à d'autres algorithmes de chiffrement qui utilisent des alphabets multiples.

Vers 400 avant **J.C**, les Spartiates utilisaient un système de cryptage des informations en écrivant un message sur une bande de papyrus, ou une lanière de cuir, puis l'enroulaient autour d'une scytale, la scytale lacédémonienne (skutalê) est considérée comme l'ancétre des systèmes de transmissions secrète. C'est le premier instrument employé en cryptographie et le seul système fonctionnant à cette époque selon le principe de transposition. (figure (4.1)). Le message n'était lisible que s'il était entouré sur la bonne scytale.

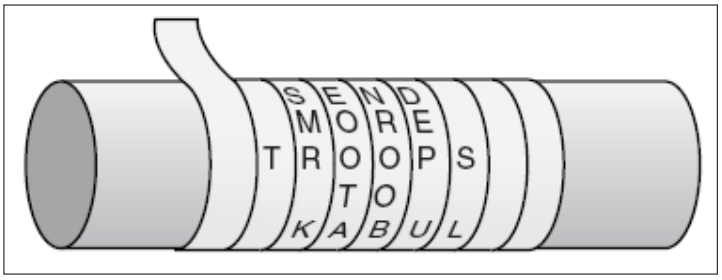


FIG. 4-1 – *La scytale utilsée par les Spartiates pour déchiffrer les messages chiffrés*

Jules César a développé une autre méthode simple de déplacer les lettres de l'alphabet, analogue au système Atbash, cela consiste en un chifrement par un simple décalage. Un nombre convenu détermine la valeur de décalage entre les lettres de l'alphabet chiffré et les lettres

de l'alphabet clair. Ce type de chiffre peut se définir comme une substitution basée sur des décalages cycliques.

Au cours de la Seconde Guerre Mondiale, des dispositifs de cryptage simplistes ont été utilisés pour la communication tactique, qui ont été considérablement amélioré grâce à la technologie mécanique et électromécanique fournissant au monde le télégraphe et la communication radio. L'appareil de chiffrement du rotor, qui est un dispositif de substitution des lettres en utilisant différents rotors dans la machine, a été une avancée considérable dans la cryptographie militaire dont la complexité a été difficile à briser. Ce travail a fait place à la machine de chiffrement la plus célèbre de l'histoire à ce jour : **La machine allemande Enigma.**

FIG. 4-2 – *La machine allemande Enigma*

La machine cryptographique Enigma est une des illustrations du rôle majeur de la science et de la technologie dans les guerres du **XX**e siècle.

Le cryptage réalisé par les Enigma allemandes repose sur les principes suivants :

Enigma a l'apparence d'une machine à écrire : comme cette dernière, elle est munie d'un

clavier dont chaque touche est surmontée d'une lettre. Sur la partie supérieure de l'appareil, on distingue en outre d'autres lettres incluses chacune au sein d'un médaillon. Celui-ci est en réalité un voyant qui peut devenir lumineux. Le fonctionnement de l'Enigma nécessite la présence de deux opérateurs.

Le premier opérateur tape le message à transmettre à l'aide du clavier. A chaque pression sur une touche, plusieurs cylindres situés à l'intérieur de la machine effectuent une rotation à l'issue de laquelle une lettre de substitution apparaît sur le voyant éclairé ; cette lettre de remplacement est prise en note par le deuxième opérateur. La lettre de substitution varie à chaque fois : un "N" devient par exemple un "P" la première fois, un "D" la fois suivante, un "R" au bout de la troisième fois. Pour un mot de trois lettres, des millions de combinaisons sont donc possibles. Transmis en morse, le message reçu est décodé par une deuxième machine Enigma, associant elle aussi deux opérateurs.

Plus précisément cette machine se compose de :

· Un tableau de connexion qui permet d'échanger 6 paires de lettres 2 à 2.

· Trois rotors choisis parmi les 6 rotors existants. Chaque rotor comprend 26 positions différentes. La position du premier rotor avance avec chaque lettre. Au bout de 26 lettres et donc 26 décalages, le premier rotor est revenu à sa position initiale et c'est le second rotor qui avance d'une lettre et ainsi de suite.

· Un réflecteur qui permet de repasser la lettre en cours de chiffrage dans les rotors et dans le tableau de connexion.

Le nombre de clés possibles est le suivant :

· Choix de 6 paires de lettres parmi 26 lettres = 100391791500 possibilités.

· Choix de 3 rotors parmi 6 = 120 possibilités.

· Choix de la position initiale des 3 rotors parmi les 26 positions possibles = $26 * 26 * 26 =$ 17576 possibilités.

· Ce qui fait un nombre total de 211738335288480000 clés différentes.

Le code utilisé par la machine Enigma sera lui aussi cassé durant la seconde guerre mondiale. Les polonais avant et au tout début de la seconde guerre mondiale auront commencé le travail de compréhension de l'algorithme. Les anglais à Bletchley Park avec l'aide d'Alan Turing finiront le travail.

Enigma est la machine à chiffrer et déchiffrer qu'utilisèrent les armées allemandes du début des années trente jusqu'à la fin de Seconde Guerre Mondiale. Elle **automatise le chiffrement par substitution**. Comme on peut le voir ci-contre, cette machine ressemble à une machine à écrire. Quand on presse sur une touche, deux choses se passent. Premièrement, une lettre s'allume sur un panneau lumineux : c'est la lettre chiffrée. Deuxièmement, un mécanisme fait tourner le rotor de droite d'un cran ; toutes les 26 frappes, le deuxième rotor tourne d'un cran, toutes les 676 frappes (26 au carré), c'est le troisième rotor qui tourne d'un cran. Certaines Enigmas avaient 3 rotors, celles de la Kriegsmarine en avaient 4 ou 5 (on peut apercevoir ces 4 cylindres gris sur le dessus de la machine ci-contre). Ces rotors tournants modifient les connexions électriques dans la machine, ce qui fait que la touche "A" allumera peut-être le "B" la première fois, mais le "X" la deuxième, le "E" la troisième, etc. Un **"tableau de connexions"** et un **"réflecteur"** complique encore le système. Le côté génial de cette machine est que même si elle tombe entre les mains ennemies, sa sécurité n'est pas compromise. En effet, c'est le nombre faramineux de réglages de la machine qui fait sa force et les réglages changeaient évidement chaque jour. On peut en effet changer l'ordre de rotors, leur orientation initiale et les branchements du tableau de connexions.

Bien que les mécanismes de l'Enigma aient été compliqués pour l'époque, une équipe de cryptographes polonais a cassé son code et la Grande-Bretagne a eu un aperçu de l'attaque allemande, les plans, et les mouvements militaires. En brisant ce mécanisme de cryptage cela aurait raceourer la Seconde Guerre Mondiale. Après la guerre, des détails sur la machine Enigma ont été publiés, l'un des appareils est exposé à l'institut de Smithsonienne.

L'armée a toujours joué un grand rôle dans l'utilisation de la cryptographie pour le cryptage et le décryptage des informations.

Avec les ordinateurs la cryptographie se développe de manière importante. Le projet le plus connu et couronné de succès est Lucifier, qui a été développé chez **IBM**. Lucifier introduit des équations mathématiques complexes et les fonctions qui furent ensuite adoptées et modifiées par la : "National Security Agency" **(NSA)**, pour le "US Data Encryption Standard" **(DES)**. Le **DES** a été adopté comme standard du gouvernement fédéral américain. Il est utilisé dans le monde entier pour les transactions financières, et est présent dans de nombreuses applications commerciales, depuis plus de 20 ans.

Quelques repères de cryptographie moderne :

· 1975. Conception de **DES,** standart de chiffrement de données, adopté en 1977.

· 1976. Article de Diffie et Hellman introduisant l'idée de système à clé publique.

· 1978. Invention de **RSA,** le premier système concret de cryptographie à clé publique.

· 1985. Invention du système cryptographique **El Garoal**.

· 1991. Adoption du premier standard de signature, **ISO** 9796, basé sur **RSA**.

· 1994. Adoption de **DSS,** standard de signature basé sur **El Garoal**.

La majorité des protocoles (algorithmes) mis au point à l'aube de l'ère de l'informatique ont été améliorés pour inclure la cryptographie. Le cryptage (chiffrement) est utilisé dans des dispositifs matériels et logiciels pour protéger les données, les transactions bancaires, les extranets d'entreprise, courrier électronique, des transactions sur le Web, la communication sans fil, le stockage d'informations confidentielles, les télécopies et appels téléphoniques.

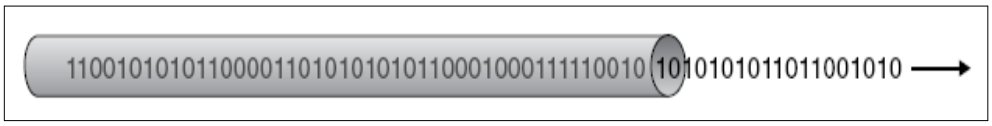


FIG. 4-3 – *Aujourd'hui, les données binaires cryptées passent par les câbles réseau et les ondes*

Les casseurs de code ont fait que, les efforts de cryptanalyse ont été accélérés et accentués.

4.2 Définitions cryptographiques

On présente quelques définitions et concepts basiques en cryptographie :

· **Cryptographie :** science de l'écriture secrète, qui nous permet de stocker et de transmettre les données sous une forme qui est disponible uniquement pour les individus auxquels elles sont destinées.

· **Cryptosystème :** matériel ou logiciel de mise en oeuvre de la cryptographie, qui transforme un texte clair en un texte chiffré et de retour au clair.

· **Algorithme :** ensemble de règles mathématiques utilisées dans le cryptage (chiffrement) et le décryptage (déchiffrement).

· **Plaintext :** le texte clair (texte, audio, image, vidéo,...etc).

· **Cryptage :** processus de masquer un message afin de cacher son contenu.

· **Ciphertext :** le texte crypté (chiffré) ou illisible.

· **Décryptage :** processus de convertir le ciphertext en plaintext.

· **Cryptanalyse :** science consistant à obtenir le texte clair à partir du texte crypté (chiffré) sans avoir la clé, ou briser le ciphertext.

· **Cryptologie :** l'étude de la cryptographie et la cryptanalyse.

· **Alphabet :** ensemble de symboles également appelés caractères.

· **Caractère :** un élément d'un alphabet.

· **String :** séquence finie de caractères dans un alphabet.

· **Clé secrète :** séquence de caractères et d'instructions qui régit l'acte de cryptage et décryptage au regroupement.

· **Clé symétrique :** clé utilisée pour le cryptage et le décryptage.

· **Clé asymétrique :** paire de clés (publique, privée) la clé publique est utilisée pour le cryptage, et la clé privée est utilisée pour le décryptage.

· **Clé clustering :** exemple lorsque deux clés différentes génèrent le même texte crypté (chiffré) de même le texte clair.

· **Espace de clés :** ensemble des valeurs possibles que les clés peuvent prendre.

· **Facteur travail :** estimation du facteur temps de travail, d'efforts et ressources nécessaires pour percer un cryptosystème.

· **Stream cipher :** chiffre qui agit sur le texte clair d'un symbole à la fois.

· **Block cipher :** chiffre qui agit sur le texte clair en blocs de symboles.

· **Substitution cipher :** flux de chiffrement qui agit sur le texte clair en faisant une substitution des caractères avec des caractères d'un nouvel alphabet ou par une permutation des caractères de l'alphabet en clair.

· **Transposition cipher :** bloc de chiffrement qui agit sur le texte clair en permutant les positions des caractères.

4.3 Conception des cryptosystèmes

Cette section, présente la méthode de construction d'un **cryptosystème**, dans deux cas : clé secrète symétrique, et clé secrète asymétrique.

D'une façon formelle un cryptosystème est caractérisé par les éléments (P, C, K, E, D) où :

· P est l'ensemble des textes clairs possibles, C est l'ensemble des textes chiffrés possibles.

· K est l'espace des clés.

· E est l'ensemble des fonctions de chiffrement, D est l'ensemble des fonctions de déchiffrement.

· **La clé symétrique :**

Pour chaque clé $k \in K$, il y a une règle de cryptage $e_k \in E$ et une fonction de décryptage $d_k \in D$ avec $e_k : P \to C$ et $d_k : C \to P$ sont des fonctions telles que :

$$d_k\left(e_k\left(x\right)\right) = x$$

pour tout texte clair $x \in P$.

· **La clé asymétrique :**

Pour chaque paire de clés (k_1, k_2), il y a une règle de cryptage $e_{k_1} \in E$ et une fonction de décryptage $d_{k_2} \in D$ avec $e_{k_1} : P \to C$ et $d_{k_2} : C \to P$ sont des fonctions telles que :

$$d_{k_2}\left(e_{k_1}\left(x\right)\right) = x$$

pour tout texte clair $x \in P$.

La clé k_1 utilisée pour le cryptage est appelée **clé publique**, elle peut être distribuée de manière publique.

La clé k_2 utilisée pour le décryptage est appelée **clé privée**, et elle connue seulement par son propriétaire.

L'invention de la clé asymétrique est une avancée majeure dans la cryptographie, car elle a supprimé le besoin d'utiliser la même clé pour le cryptage et le décryptage.

Le processus de cryptage transforme le texte en clair (plaintext ou cleartext) en texte chiffré (ciphertext ou cryptogramme), et le processus de décryptage transforme le texte chiffré en texte

clair, comme l'illustre la figure (4.4).

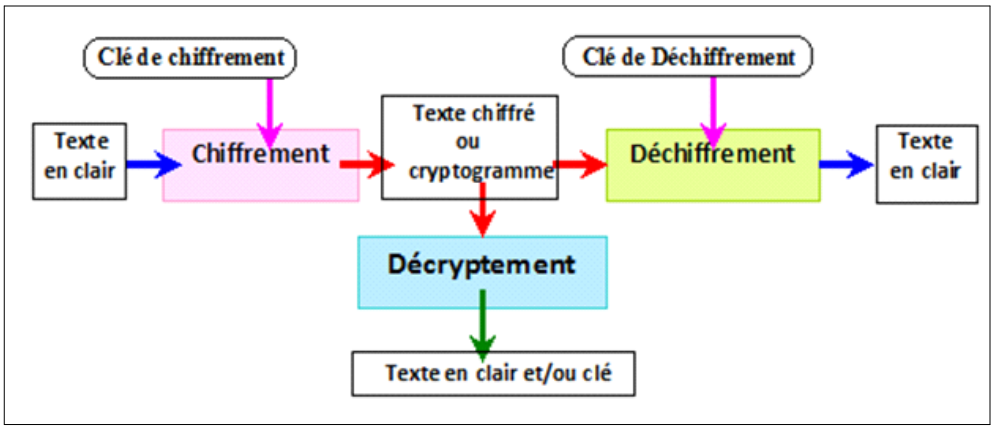


FIG. 4-4 – *Processus de cryptage et décryptage*

De nombreux algorithmes de cryptage sont publiquement connus et bien compris, donc ils ne sont pas la partie secrète du processus de cryptage. La pièce secrète d'un algorithme de chiffrement bien connu est la clé.

Comme le montre la figure (4.5), si une oreille indiscrète capte un message entre deux personnes, il apparait dans sa forme cryptée et il est donc illisible. Même si cet attaquant connait l'algorithme que les deux personnes utilisent pour crypter et décrypter leurs information, sans la clé, ce message reste incompréhensible et indéchiffrable.

La clé peut être n'importe quelle valeur qui est constituée d'une séquence importante de bits aléatoires. Est-ce simplement un nombre de bits aléatoires entassés ? Pas vraiment. Un algorithme contient un espace de clés, qui est une gamme de valeurs qui peuvent être utilisées pour construire une clé. La clé est composée de valeurs aléatoires dans l'espace de clés. Plus l'espace de clés est grand, plus les valeurs disponibles peuvent être utilisées pour représenter les différentes touches, et plus les touches sont aléatoires, plus il est difficile pour les intrus de les comprendre. L'algorithme de cryptage doit utiliser un espace de clés et choisir les valeurs que les clés prennent, de manière très aléatoire. Si un espace de clés plus petit a été utilisé, cela permettrait d'accroitre la chance d'un attaquant de prouver la valeur de la clé, et ainsi de décrypter l'information protégée, (figure (4.6)).

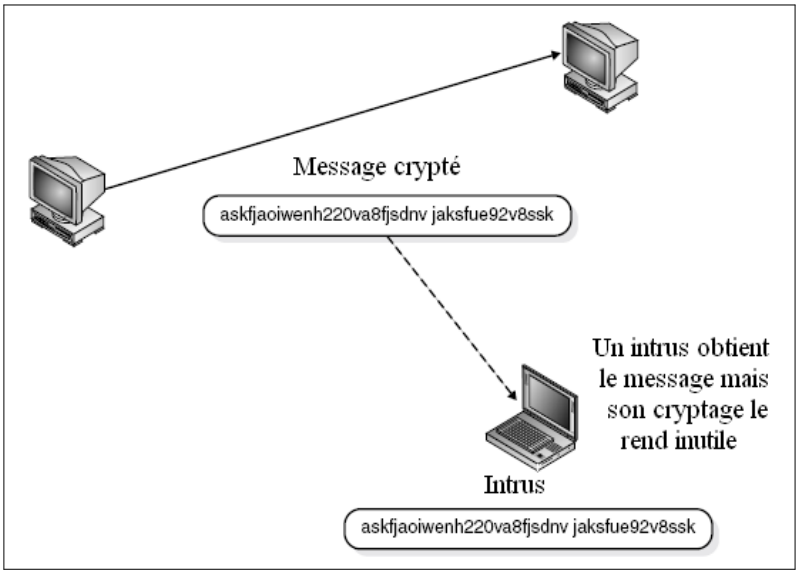


FIG. 4-5 – *Sans la bonne clé, le message capturé est inutile pour un attaquant*

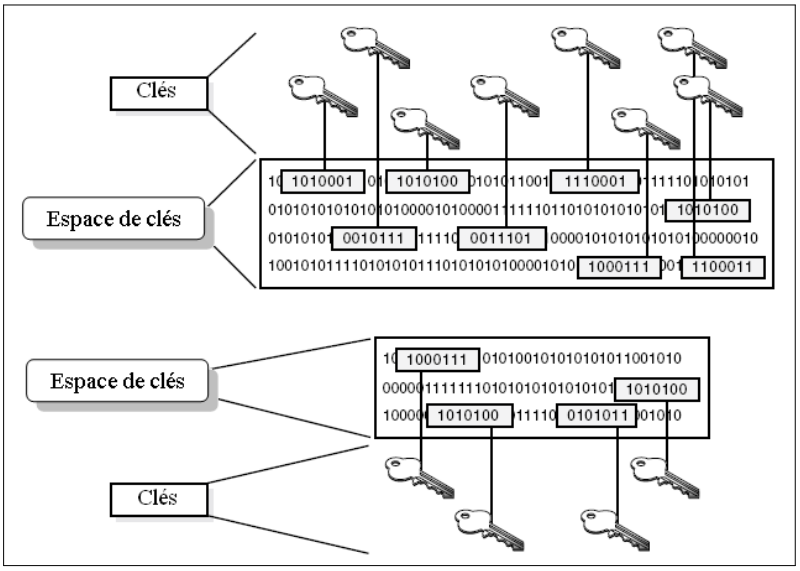


FIG. 4-6 – *Grand espace de clés permet plus de clés possibles*

4.4 Classification des cryptosystèmes

Outre les classifications bien connues telles que :

1− Classification par rapport à la structure de l'algorithme de cryptage : Chiffrement par flot. Chiffrement par blocs.

2− Classification par rapport à la méthode de distribution de la clé secrète (clé symétrique, asymétrique, hybride).

3− Classification par rapport à la méthode de construction de l'algorithme.

on dispose aujourd'hui de méthodes nouvelles basées sur la théorie du chaos qui viennent s'ajouter aux méthodes traditionnelles utilisant : la théorie des nombres, l'algèbre, la géométrie algébrique (courbes elliptiques). Les **méthodes utilisant le chaos** (basées sur des **systèmes dynamiques chaotiques discrets / systèmes dynamiques chaotiques continus)** font l'objet d'une étude particulière dans le présent travail.

4.5 Objectifs des cryptosystèmes

Le cryptosystème assure et garantit : la confidentialité, l'authenticité, l'intégrité et la non-répudiation.

· La confidentialité signifie qu'une personne non autorisée n'ait accès aux information.

· L'authenticité fait référence pour la validation de la source du message pour assurer que l'expéditeur est correctement identifié.

· L'intégrité fournit l'assurance que le message n'a pas été modifié pendant la transmission, accidentellement ou intentionnellement.

· La non-répudiation signifie qu'un expéditeur ne peut pas nier d'avoir envoyé le message et le récepteur ne peut pas nier sa réception.

Remarque 4.1 :

Si une personne envoie un message, puis plus tard, affirme qu'il n'a pas envoyé le message, il s'agit d'un acte de **répudiation**. Quand un mécanisme de cryptage prévoit la **non-répudiation**, cela signifie que l'expéditeur ne peut pas nier d'avoir envoyé le message et le récepteur ne peut pas nier sa réception.

4.6 Force des cryptosystèmes

La force de la méthode de cryptage vient de l'algorithme, le secret de la clé, la longueur de la clé, et des vecteurs d'initialisation. La force est corrélée à la quantité de traitement nécessaire, la puissance et le temps qu'il faut pour casser la clé ou déterminer sa valeur. Casser une clé peut être accompli par une attaque en force brute, qui tente par tous les moyens possibles la valeur de la clé jusqu'à ce que le texte clair qui en résulte soit significative. En fonction de l'algorithme, et de la longueur de la clé, cela peut être une tâche très facile ou une tâche pratiquement impossible. Si une clé peut être rompue avec un processeur **Pentium II** en trois heures, le chiffre n'est pas fort du tout.

Un autre nom pour la force de la cryptographie est le "facteur travail", ce qui est une estimation de l'effort qu'il faudrait un attaquant de pénétrer dans une méthode de cryptage.

La force du mécanisme de protection devrait être utilisée en corrélation avec la sensibilité des données cryptées.

Même si l'algorithme est très complexe et approfondie, il y a d'autres questions relevant du cryptage qui peuvent affaiblir la force des méthodes de cryptage. Parce que la clé est généralement la valeur secrète nécessaire aux messages réellement cryptés et décryptés, la protection abusive de la clé peut affaiblir la puissance de crypatge.

Chapitre 5

Application du chaos en cryptographie

5.1 Introduction

Les 1 ères applications des systèmes chaotiques en cryptographie sont proposées par **Pecora** et **Carroll** [26] comme une possible application de la synchronisation des systèmes dynamiques chaotiques.

Dans le cas de ces systèmes dynamiques continus les méthodes de synchronisation des systèmes chaotiques et de contrôle du chaos s'appliquent essentiellement à la sécurisation des communications. **Kocarev** et **Parlity** [23] mettent en évidence les méthodes de cryptage des messages par la modulation des trajectoires de systèmes dynamiques continus.

Quant aux systèmes dynamiques discrets (avec itérations et itérations inverses d'applications chaotiques) abordés initialement par **Habutsu** et développés par la suite par **Kotulski** et **Szcepanski**, ils sont à la base de la construction de clés [44].

Dans ce chapitre on discute le rapport entre la cryptographie et la théorie du chaos, et les similitudes de leurs concepts cruciaux. Une procédure systématique pour designer un algorithme de cryptage basé sur les applications chaotiques est suggérée et on propose un exemple basé sur l'application logistique.

5.2 Utilisation des systèmes dynamiques chaotiques en cryptographie

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

Tableau 5.1 :

Théorie du chaos	*Cryptographie*
Système chaotique	Système pseudo-chaotique
Transformation non linéaire	Transformation non linéaire
Nombre infini d'états	Nombre fini d'états
Nombre infini d'itérations	Nombre fini d'itérations
État initial	Plaintext
État final	Ciphertext
Condition initiale (s) et / ou paramètre (s)	Clé (s)
Indépendance asymptotique des états initiaux et finaux	Confusion
Sensibilité aux conditions initiale (s) et paramètre (s) i.e. mixage	Diffusion

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

$$x_{k+1} = f(x_k)\,;\ x_0 \in I \tag{5.1}$$

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

On rappelle qu'un système dynamique de la forme (5.1) est dit chaotique si les conditions suivantes sont satisfaites :

1− **Sensibilité aux conditions initiales** :

$$\exists \delta \succ 0\ \forall x_0 \in I, \varepsilon \succ 0\ \exists n \in \mathbb{N}, y_0 \in I : |x_0 - y_0| \prec \delta \Longrightarrow |f^n(x_0) - f^n(y_0)| \succ \delta$$

2− **Transitivité topologique** :

$$\forall I_1, I_2 \subset I \;\; \exists x_0 \in I_1, n \in \mathbb{N} : f^n(x_0) \in I_2$$

3− **Densité du point périodique dans** I :

Soit

$$P = \{p \in I \mid \exists n \in \mathbb{N} : f^n(p) = p\}$$

l'ensemble des points périodiques dans f. P est dense dans I :

$$\overline{P} = I$$

Exemple 5.1 :

1− Les polynomes de Tchebytchev :

T_n des polynomes de degré n définis sur $I = [-1, 1]$ par :

$$T_n = \cos(n \; ar\cos x)$$

soit par la relation recurrente :

$$T_{n+1} = 2xT_n(x) - T_{n-1}(x)$$

sont chaotiques $n \geq 2$.

2− L'application logistique définie par :

$$x_{k+1} = f(x_k) = rx_k(1 - x_k), k \in \mathbb{N}, \text{ où } r \text{ est le paramètre de contrôle}$$

est chaotique pour $3.57 \leq r \leq 4$.

Pour un tel système chaotique sur I (dans le sens où l'ensemble des points périodiques sur I est réduit à un ensemble de mesure nulle sur I) la connaissance de tous les points critiques de f même s'ils sont tous répulsifs (c.à.d. si une trajectoire (x_k) se rapproche d'un cycle périodique pour une certaine valeur k de l'indice k alors elle s'en éloigne pour des valeurs de l'indice supérieures à k) n'est pas suffisante. Il est nécessaire de considérer les exposants de Lyapunov

qui mesurent le degré de sensibilité aux conditions initiales et peuvent être interprétés comme une mesure de la sécurité dans le contexte cryptographique. Dans la pratique ces exposants se sont imposés comme des outils performants, même dans le cas de séries temporelles courtes, avec un coût de calcul relativement réduit par rapport à la dimension de corrélation ou l'entropie de Kolmogorov. Ils semblent constituer la solution la plus pertinente dans le contexte des systèmes à dimension d'état réduite destinés aux communications numériques.

Soit $[X_{\min}, X_{\max}]$ une portion de l'attracteur (il peut être l'attracteur entier). Considèrons les intervalles définis par : $[X_{\min} + (S-1)\ \epsilon, X_{\min} + S\epsilon]$, on choisit $S = 256, \epsilon = (X_{\max} - X_{\min}) \diagup S$. Le nombre d'itérations est lié aux clés secrètes : Les S associations entre $S\epsilon-$intervalles et les $S-$unités de l'alphabet, la première condition initiale X_0, et le paramètre de contrôle r (dans cette présentation on considère $S+2$ clés secrètes), permettent au récepteur de décrypter le ciphertext en itérant l'équation logistique autant de fois qu'indiqué par le ciphertext. La position du point final, par rapport aux $S\epsilon-$intervalles, indique le caractère original au récepteur.

Si on fait référence à X_0 comme étant la première condition initiale, c'est parce qu'à chaque fois qu'on crypte une unité d'un plaintext (par exemple, le mot "hi" est un plaintext avec 2 unités), une nouvelle condition initiale est considérée. Ainsi si $C1$ est le ciphertext de la première unité dans un plaintext, alors pour crypter la seconde unité dans ce plaintext on utilise comme condition initiale $X_0^{'} = F^{C1}(X_0)$, où F^{C1} est la $C1^{ième}$ itération de l'équation logistique. Si $C2$ est le ciphertext de la seconde unité dans ce plaintext alors la condition initiale utilisée pour crypter une troisième unité dans le même plaintext est $X_0^{'} = F^{C2}\left(X_0^{'}\right)$.

Ainsi pour la condition initiale $X_0 = 0.232\ 323\ 000\ 000\ 00$ et pour le paramètre $r = 3.8$. La lettre « h » est associée au site numéro 104 qui représente l'intervalle :

$$[0.44140625000000, 0.44375000000000]$$

et la lettre « i » est associée au site numéro 105 correspondant à l'intervalle :

$$[0.44375000000000, 0.44609375000000000]$$

Pour crypter le plaintext « hi » par le ciphertext ciphertext (1713364) : la 1ére unité du ciphertext 1713 serait obtenue en itérant l'application logistique jusqu'à se situer dans l'intervalle 104. La seconde unité du ciphertext serait obtenue en prenant comme condition initiale $X_0 = X_{1713}$ et en itérant l'application jusqu'à se situer dans le site 105. La méthode de réception est assez simple.

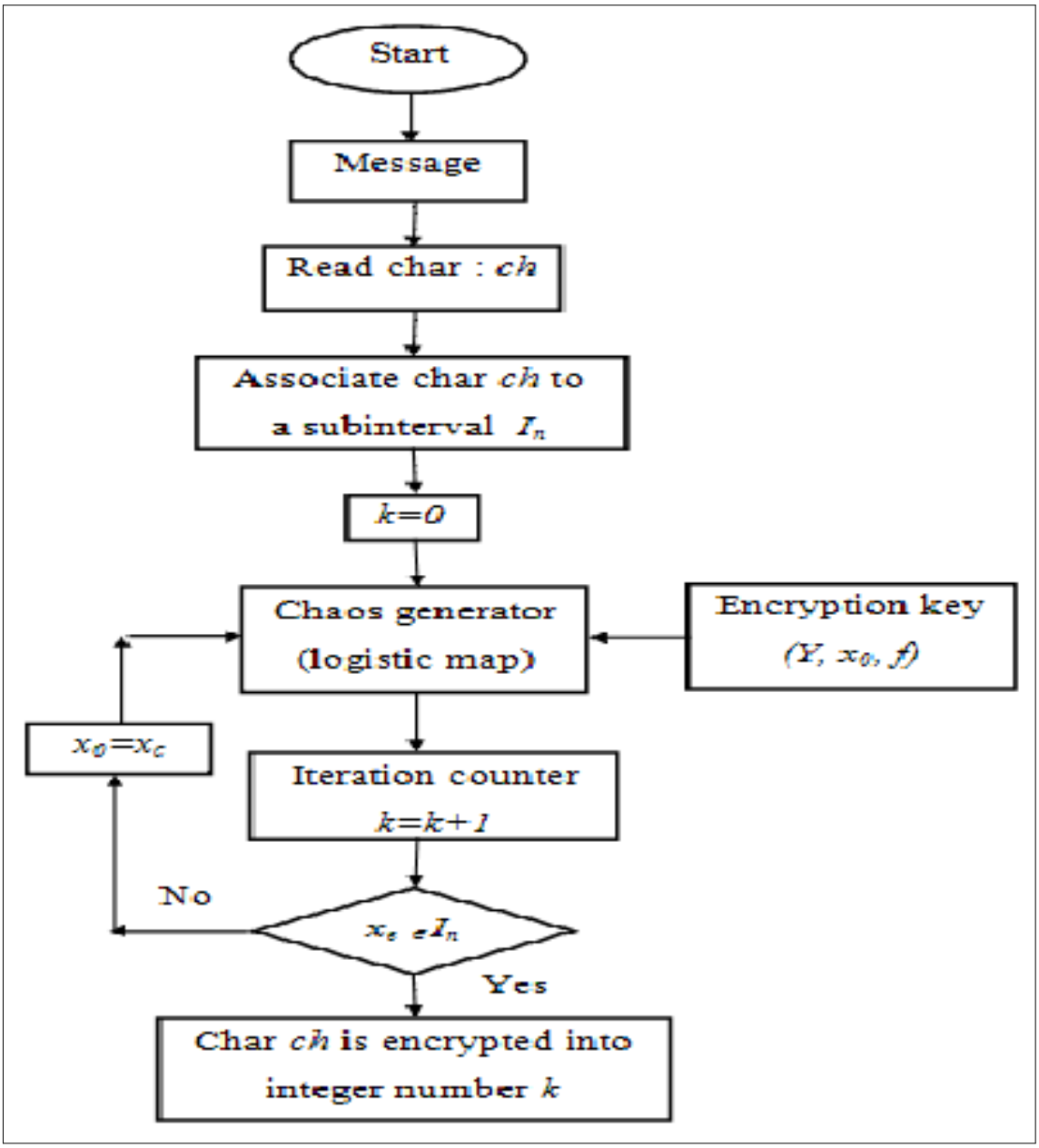


FIG. 5-1 – *Schéma de la méthode de cryptage chaotique*

5.3 L'application logistique comme un algorithme de cryptage par blocs

Dans ce travail l'application logistique est à la base du cryptosystème [24] .

Le caractère hautement imprévisible des signaux chaotiques est la caractéristique la plus attrayante des systèmes déterministes chaotiques qui peuvent conduire à de nouvelles applications. Le Chaos et la cryptographie ont certaines caractéristiques communes, à l'instar de la sensibilité importante à des changements de variables et des paramètres.

Même si au cours de la dernière décennie, l'intérêt pour les deux disciplines scientifiques, qui sont la cryptographie et la théorie du chaos, a permis de mettre une comparaison, ou une mise en parallèle détaillée du chaos et de la cryptographie. Une différence importante entre le chaos et la cryptographie repose sur le fait que les systèmes utilisés dans le chaos ne sont définis que sur des nombres réels, alors que pour les systèmes de cryptographie on se limite à des nombres entiers.

Le chaos a déjà été utilisé pour la conception des systèmes de chiffrement. Ainsi, par exemple, dans une série de documents [24] ([5]), les auteurs proposent un chaos dérivés de nombres générateurs pseudo-aléatoires **(NGPA)**.

Alors que dans des chiffrements cryptographiques conventionnels le nombre d'itérations effectuées par une transformation est généralement moins de 30, dans [29] ce nombre peut être aussi grand que 65536, et il est toujours supérieur à 250.

Un autre algorithme de chiffrement basé sur les systèmes chaotiques synchronisés est proposé dans [24] ([9]). Les auteurs suggèrent que chaque octet (composé de n bits) d'un message correspond à un attracteur chaotique différent.

5.3.1 Les algorithmes de cryptage par blocs

Dans un chiffrement par blocs le message est découpé en blocs réguliers, puis chaque bloc est chiffré de la même façon.

Exemple 5.2 **:**

M (messages) $= C$ (mots chiffrés) $= K$ (clés) ensemble des mots de six chiffres binaires.

Soit le bloc de six lettres :

$$m = (m_1 m_2 ... m_6)$$

on définit :

$$E_k^1 (m) = m \oplus k \text{ avec } k \in K$$
$$E^2 (m) = (m_4 m_5 m_6 m_1 m_2 m_3)$$

la composée $E_k^1 \circ E^2$ forme un tour élémentaire.

Les algorithmes de cryptage sont usuellement écrits sous la forme des transformations :

$$Y = E_Z (X) \tag{5.2}$$

où le plaintext X, le cryptogramme Y et la clé Z sont des séquences de lettres dans des alphabets finis L_X, L_Y, L_Z respectivement, qui ne sont pas nécessairement identiques. L'équation (5.2) souligne que le cryptogramme Y est une fonction E_Z d'un seul plaintext X, la fonction particulière étant déterminée par la valeur de la clé secrète Z, E_Z est appelé un algorithme de cryptage.

Dans la suite on considère un cas spécial des algorithmes de cryptage, appelé : algorithme de cryptage par blocs, pour lequel E_Z est défini comme une fonction F_Z :

$$F_Z : \chi \to \chi, \text{où } \chi = \left\{0, 1, ..., 2^{m-1}\right\}, \text{où } m \geq 64$$

On suppose que F_Z est une correspondance injective, pour plus de simplicité, on écrit F au lieu de F_Z. Chaque élément de l'ensemble χ correspond au bloc de données de m bits. Si F décrit un algorithme de cryptage par blocs la transformation de décryptage est l'application F^{-1} qui permet de retrouver le plaintext X du ciphertext $Y = F(X)$. On peut représenter la situation schématiquement par le diagramme :

$$X \xrightarrow{F} Y \xrightarrow{F^{-1}} X$$

Deux principes généraux qui guident la conception des ciphers pratiques sont la diffusion et la confusion, ces deux propriétés ont été identifiées par **Claude Shannon** dans son document "Communication theory of Securecy Systems" publié en 1949.

D'après la définition de Shannon :

· **la confusion** correspond à une volonté de rendre la relation entre la **clé de chiffrement** et le **texte chiffré** la plus complexe possible.

· **la diffusion** est une propriété où la redondance statistique dans un texte clair est dissipée dans les statistiques du texte chiffré. En d'autres termes les statistiques de la sortie doivent donner le moins possible d'informations sur l'entrée.

Dans un chiffrement avec une bonne diffusion l'inversion d'un seul bit en entrée doit changer chaque bit en sortie avec une probabilité de 0.5.

· **la substitution** (un symbole du texte clair est remplacé par un autre) fut la première approche pour introduire la confusion. Quant à la permutation transposition elle augmente la diffusion.

Remarque 5.1 **:**

Le chaos n'est pas suffisant pour la sécurité. Conformément aux prescriptions de Shannon, chaque algorithme de chiffrement possède des propriétés de confusion, diffusion, de mélange et de sensibilité aux changements du plaintext et de la clé secrète. Ce qui garantit par ailleurs qu'une extension du domaine d'un algorithme de chiffrement à partir d'un réseau à un continuum donnera lieu à une application chaotique.

Ainsi en faisant l'extension du domaine de la fonction itérative de **IDEA** (International Data Encryption Algorithm), il se confirme que la nouvelle application est chaotique. Une interpolation linéaire entre les points du réseau a été utilisée pour étendre définition de la fonction vers le continuum.

A l'inverse, si une application non linéaire chaotique est définie sur un continuum, alors elle présente des propriétés de confusion, de diffusion, de mélange, et de sensibilité aux changements dans les variables. Cependant, un bon algorithme de cryptage doit également être irréductible à toute autre plus simple qui rendrait sa cryptanalyse possible. Un excellent exemple **IDEA** dont le principe de base est l'utilisation de trois groupes algébriques différents.

A l'heure actuelle, la notion de sécurité cryptographique n'a pas d'équivalent dans la théorie du chaos, et la sécurité cryptographique d'un algorithme de cryptage dérivé du chaos ne peuvent être vérifiées que par le biais des outils de cryptographie. Même dans la cryptographie, il n'ya pas de procédure simple pour prouver que l'algorithme de chiffrement est sécurisé.

Remarque 5.2 **:**

La synchronisation est nécessaire que dans certains modes de chiffrement. La façon dont les algorithmes sont utilisés en cryptographie est appelé mode de chiffrement.

Un mode de chiffrement combine l'algorithme et quelques opérations simples. La sécurité de la mode ne dépend que de l'algorithme sous-jacent et non pas des opérations utilisées. De plus le mode de chiffrement ne doit pas compromettre la sécurité de l'algorithme sous-jacent.

Dans la plupart des applications de synchronisation du chaos en cryptographie, en général une nouvelle synchronisation est proposée pour assurer le chiffrement de l'information.

Par conséquent, il est proposé un nouveau schéma pour un mode cryptographique. Dans ce cas la sécurité du schéma depend plutot de l'algorithme sous-jacent, qui est, dans un tel cas, un système dynamique décrit par une application ou par des équations différentielles.

Une hypothèse fondamentale de la cryptanalyse, en premier lieu énoncée par **A. Kerckhoffs** au **XIXe** siècle, est que le secret de l'algorithme doit résider entièrement sur les clés. Ce qui, en termes de systemes dynamiques, signifie que si le cryptanalyste a tous les détails du système dynamique et de sa mise en œuvre alors sa tâche principale est d'estimer, sans la présence de bruit, les paramètres du système connaissant les équations décrivant son évolution dans le temps.

5.3.2 D'une application chaotique à un algorithme de cryptage par blocs

Rappelons d'abord qu'un système dynamique discret est une application G d'un espace de phases $\Omega \subseteq \mathbb{R}^{\infty}$ dans lui même, où $y_{i+1} = G(y_i)$.

Dans la suite on suppose que G est une application chaotique sur Ω avec la propriété de mixage (mélange).

L'analogie entre l'application qui effectue les tours de chiffrement f et l' application chaotique G est évidente. L'itération de f conduit à la diffusion et à la confusion souhaitées, l'itération de la l'application chaotique G applique la région initiale sur l'ensemble de l'espace des phases. Une importante différence entre le chiffrement et l'application chaotique est que le cryptage est défini sur un ensemble fini et dépend de la valeur de la clé Z. Ce n'est pas le cas avec l'application chaotique. Une application définie sur un ensemble fini peut être dérivée d'une application chaotique par discrétisation, dans laquelle on substitue les variables continues et les

opérations définies sur les nombres réels par des variables qui prennent leurs valeurs dans un ensemble fini d'entiers et les opérations appropriées sur les entiers .

Nous suggérons maintenant une procédure systématique de la conception d'un algorithme de chiffrement par blocs basé sur des applications chaotiques. Cette procédure comporte quatre étapes : le choix d'une application chaotique, la discrétisation, programation de clés et la cryptanalyse.

Choix d'une application chaotique

La première étape dans la conception d'un algorithme de chiffrement par bloc est de choisir une application chaotique. Choisir des applications pour les algorithmes de cryptage n'est pas facile, on pourrait considérer seulement les applications ayant les propriétés suivantes : mixage, robustesse du chaos et un ensemble important de paramètres.

La propriété de mixage (mélange) Cette propriété pour les applications chaotiques est étroitement liée à la propriété de diffusion dans les algorithmes de cryptage. Si l'on considère l'ensemble des plaintexts possibles comme une région initiale dans l'espace des phases de l'application en question alors sa propriété de mixage (i.e. sa sensibilité aux conditions initiales) engendre une influence d'un caractère de texte clair sur un plus grand nombre de caractères cryptés.

Robustesse du chaos Un bon algorithme de chiffrement renforce l'influence d'une seule clé sur le texte chiffré. Les clés d'un algorithme de chiffrement représentent ses paramètres. Par conséquent, on considère seulement des transformations dans lesquelles les paramètres et les variables sont liés d'une manière sensible.

Un système dynamique est structurellement stable quand de petites perturbations C^1 conduisent à un système topologiquement équivalent. En d'autres termes, un système structurellement stable ou robuste conserve ses propriétés qualitatives sous de petites perturbations.

Les attracteurs chaotiques robuste ou structurellement stables peuvent éventuellement assurer la propriété de diffusion dans l'espace des clés. Les algorithmes basés sur des systèmes non robustes peuvent avoir des clés faibles. Toutefois, la majorité des attracteurs chaotiques

sont structurellement instables, par conséquent, une grande prudence s'impose dans le choix des applications chaotiques.

Ensemble des paramètres On doit considérer seulement les systèmes qui ont un chaos robuste pour un ensemble important de paramètres (clés). L'entropie d'un cryptosystème est la mesure de la taille de l'espace de clés et elle est usuellement approximée par $\log 2K$, où K est le nombre de clés. Par conséquent, un plus grand espace de paramètres d'un système dynamique implique que sa version discrétisée aura un K plus grand.

On considère des applications chaotiques. On choisit :

$$G(y) = ay(1-y) \tag{5.3}$$

où $y \in [0,1]$ et $a = 4$. C'est l'application logistique présentant un phénomène de chaos pour $a = 4$. L'application logistique n'est pas structurellement stable (dans l'espace du paramètre a) ; par conséquent, on fixe $a = 4$ et on introduit les paramètres en remplaçant y dans (5.3) par $y = \tilde{y} + p \pmod 1$, où $\tilde{y} \in [0,1]$ et p est le paramètre (nombre réel). La raison pour cela est double. Premièrement dans la plus part des algorithmes les clés sont introduites de manière similaire. Deuxièmement, par rapport au paramètre p l'application logistique a un chaos robuste pour tout p. On souligne que cette procédure assure que presque toute application chaotique avec la propriété de mixage peut être utilisée pour la conception d'algorithmes de cryptage.

Discrétisation

La discrétisation est un processus dans lequel l'application

$$G : \Omega \to \Omega$$

est remplacée par l'application

$$F : \chi \to \chi$$

La discrétisation n'est pas le processus unique. Cependant, dans plusieurs cas on peut identifier "un procédé naturel" de le faire. Ainsi, par exemple, si $\beta = \{C_0, ..., C_{2^m-1}\}$ est une portion finie de l'espace de phases Ω, alors $\chi = \{0, ..., 2^m - 1\}$ et F est une restriction de G sur χ.

Ainsi, par exemple, si $\beta = \{C_0, ..., C_{2^m-1}\}$ est un ensemble fini de partitions de l'espace des phases Ω, alors $\chi = \{0, ..., 2^m - 1\}$ et F est la restriction de G sur χ (en supposant que cette restriction existe).

A titre d'exemple, la transformation obtenue à partir de l'application logistique est réalisée en deux étapes : d'abord, l'application logistique est ajustée de sorte que les valeurs d'entrée et de sortie de l'application sont dans l'intervalle $[0, 256]$, d'autre part, l'application logistique réduite est discrétisée.

5.3.3 Un exemple

On considère dans l'algorithme de cryptage par bloc que chaque bloc est constitué de 8 octets. Cela signifie que l'on recherche des systèmes dynamiques de dimension 8. Soit B_0 un bloc de texte en clair d'une longueur de 64−bits.

Soit B_0 un bloc plaintext de longueur 64−bits. On écrit $x_{i,0}, ..., x_{i,7}$ pour les huit bytes du bloc B_i, $B_i = x_{i,0}, ..., x_{i,7}$. Le cipher consiste à r tours des transformations identiques appliquées dans une séquence au bloc plaintext. La transformation de cryptage est donnée par :

$$\begin{aligned} x_{i,2} &= x_{i-1,1} \oplus f_0 \\ x_{i,3} &= x_{i-1,2} \oplus f_1 \\ &\vdots \\ x_{i,0} &= x_{i-1,7} \oplus f_6 \\ x_{i,1} &= x_{i-1,0} \oplus f_7 \end{aligned} \tag{5.4}$$

où $i = 1, ..., r$. Les fonctions $f_1, ..., f_7$ ont la forme suivante :

$$f_i = f\left[x_{i-1,1} \oplus ... \oplus x_{i-1,j} \oplus z_{i-1,j}\right]$$

où $j = 1, ..., 7$ et $f : M \to M$, avec $M = \{0, ..., 255\}$ est une application dérivée par l'application logistique $f_0 = z_{i,0}$ et $z_{i,0}, ..., z_{i,7}$ sont les huit bytes de la sous-clé z_i qui contrôle le $i^{éme}$ tour. Le bloc de sorti $B_i = x_{i,0}, ..., x_{i,7}$ est le bloc ciphertext (information cryptée). La

longueur du bloc ciphertext est 64−bits (8 bytes) et elle égal la longueur du bloc plaintext. Chaque tour i est contrôlé par une sous-clé z_i de 8−bytes. Il y a totalement r sous-clés et elles sont dérivées de la clé par une procédure de génération de tours de sous-clés. Pour le choix d'une application f on a les étapes décrites précédemment et f est obtenue par la discrétisation de l'application logistique. La structure de décryptage défait les transformations de la structure de cryptage : les tours de décryptage r sont appliqués au bloc ciphertext B_r pour produire le bloc plaintext original B_0. Les tours de sous-clés sont appliqués maintenant dans un ordre inverse. Le cycle de la transformation de décryptage est :

$$x_{i-1,k} = x_{i,k+1} \oplus f_{k-1}\left[x_{i,1}, ..., x_{i,k-1}, z_{i,k-1}\right] \tag{5.5}$$

avec $k = 1, ..., 8$; $f_0 = z_0$; $x_8 \equiv x_0$ et $x_9 \equiv x_1$.

Si l'on discrétise l'application logistique, la fonction f est telle qu'il y a des éléments distincts de l'ensemble $\{0, 1, ..., 255\}$ qui sont associésés à la même valeur. Ainsi, le cardinal de l'ensemble des valeurs de sortie possibles est inférieur de 256. Par exemple, le nombre d'éléments qui sont associés à la valeur 255 est 17. Cette propriété implique que, lorsque les valeurs d'entrée sont uniformément distribuées, les valeurs de sortie ne le sont pas uniformément.

En effet, quand toutes les valeurs sont équiprobables, la probabilité d'avoir une valeur de sortie 255 est $\frac{17}{256.}$. Ce chiffre est nettement supérieur à $\frac{1}{256}$.

On applique la procédure suivante :

1− Diviser l'espace des phases en $n+1$ intervalles avec longueur égale. Attribuer les nombres $0, ..., n$ à l'intervalle de sorte qu'un seul nombre est attribué à exactement une région. Si un point est dans la région i on dit que sa magnitude est i.

2− Choisir au hasard, un seul point de départ de chaque intervalle et déterminer son image après N itérations d'une application chaotique.

3− Trouver l'ensemble S des points de départ qui ont une image unique. Choisir un sous-ensemble A qui contient 256 éléments de S et déterminer l'ensemble B des images correspondantes.

4− Affecter des nouvelles magnitudes $0, ..., 255$ aux éléments de A en fonction de leurs anciennes grandeurs. Faire de même avec les éléments de B. Si la nouvelle magnitude d'un

point de départ dans A est i et la nouvelle magnitude de son image est j, alors $f(i) = j$ et f est une application injective.

La fonction finale construite dépond de la manière dont les grandeurs sont attribuées dans la première étape, l'application chaotique qui est itérée, le nombre d'itérations et les points de départ. En changeant n'importe laquelle on peut changer la fonction f. On souligne que, si la cardinalité de l'ensemble S est moins que 256, l'étape 3 est impossible. Le nombre de régions est choisi de sorte que le nombre moyen des points de départ qui ont une image unique est légèrement supérieur à 256, quand l'application chaotique utilisée dans l'étape 2 est l'application logistique.

Il faut maintenant, supposer que l'application chaotique a une mesure ergodique invariante distribuée uniformément et le nombre de régions dans l'étape 1 est $n + 1$. La probabilité que l'image donnée est une image d'exactement un seul point de départ est :

$$\sum_{i=1}^{n} \frac{1}{n} \left[\frac{n}{n+1}\right]^n = \left[\frac{n}{n+1}\right]^n \to \frac{1}{e} \text{ quand } n \to \infty$$

Ainsi pour des valeurs grandes de n la portion des images qui correspondent exactement à un seul point de départ est $\frac{1}{e}$. Si on veut construire une application :

$$f : \{0, ..., k-1\} \to \{0, ..., k-1\}$$

le nombre de régions doit être légèrement supérieur à ke pour des valeurs grandes de k.

Tableau 5.2 : La fonction f obtenue en utilisant l'application logistique [24] .

Le tableau 5.2 montre une fonction construite en utilisant la procédure précédente. Le système de numérotation est hexadécimal. Ainsi, $f(00) = 60$; $f(10) = 92$; $f(20) = b7$ et etc. L'application chaotique, qui a été utilisé dans l'étape 2, est l'application logistique. On choisit $N = 100$ et $n = 767$. La cardinalité de l'ensemble S est 259.

Remarque 5.3 : Les orbites périodiques

Considérons de nouveau l'application $F : \chi \to \chi$ où $\chi = \{0, 1, ..., 2^m - 1\}$, qui décrit un algorithme de cryptage par bloc. Puisque F est une application injective finie, toutes ses trajectoires sont périodiques. Quelle-est la période minimale, typique et maximale de telles orbites ? Bien que cette question, soit en général pertinente en cryptographie, il est toutefois

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	60	c4	56	52	88	17	82	ac	28	96	4f	4a	ff	20	b5	6a
1	92	83	bc	a7	b2	9a	ee	70	35	e1	25	61	9d	a4	9c	47
2	b7	7d	2f	24	c7	7e	c5	c8	77	14	8d	cc	fd	8a	ef	36
3	76	2c	12	11	2a	29	a8	b8	22	84	c3	e9	e6	e2	15	57
4	e0	3c	69	ce	05	d4	cd	fa	30	f8	dd	75	cf	a0	0c	55
5	9f	41	f3	6f	ea	d2	a2	65	23	89	81	39	e4	93	ba	6b
6	a9	b0	1f	f7	34	43	1b	08	04	fc	0b	aa	73	94	eb	8e
7	c2	d6	53	48	18	27	8f	5b	5d	d0	ec	f4	f5	31	4b	ab
8	4e	97	79	bb	13	b6	5e	8b	10	50	49	1d	f6	99	00	68
9	3f	95	ad	e7	e8	87	8c	51	64	1e	d9	e5	5a	da	de	f0
a	0f	46	F1	1c	71	e3	09	a5	dc	9e	bf	40	80	3b	45	02
b	a6	42	d1	ed	d7	fe	16	9b	63	72	c0	78	b4	67	26	03
c	01	54	07	90	38	21	62	3d	d8	ca	7f	b1	0a	d5	44	a1
d	0d	c9	f2	2e	b9	59	6c	66	b3	74	32	bd	df	58	6d	37
e	3a	2d	db	6e	f9	1a	c6	06	5f	a3	2b	19	7c	fb	7b	af
f	be	0e	85	5c	33	7a	c1	4d	cb	86	91	4c	d3	ae	3e	98

hors de propos et inutile pour la théorie des algorithmes de chiffrement par bloc.

Un des buts dans la conception des ciphers bloc est de désigner la transformation qui peut être utilisée pour les deux : cryptage et décryptage. Dans ce cas, $F = F^{-1}$ et évidemment toutes les trajectoires de F sont périodiques de période 2. Un exemple d'un tel cryptage est le **DES** (Data Encryption Standard).

Programmation de clés

C'est le moyen par lequel les bits clé sont transformés en tours de clés de sorte que le cryptage puisse être effectué. L'application fait que chaque tour i dépend de la valeur du tour des sous-clés z_i. On note les bytes des clés K_i par $K_{i,j}$, $j = 0, ..., 15$. La procédure de génération de clés est donnée par :

$$K_{i,k+1} = K_{i-1,k} \oplus f_{k-1}\left[K_{i-1,1}, ..., K_{i-1,k-1}, C_{k-1}\right], \; z_i = RH\left(K_i\right) \tag{5.6}$$

où $i = 1, ..., r$, $k = 1, ..., 16$, $f_0 = c_0$, $K_{i,16} \equiv K_{i,0}$ et $K_{i,17} \equiv K_{i,1}$ et $c_0, ..., c_{15}$ sont les seize bytes de la constante C. La fonction RH attribut le 64−bits demi-droite de la clé K_i au rond de la sous-clé z_i.

La structure de la procédure de généralisation de la clé est similaire à la structure de cryptage (5.5). La seule différence est que la longueur des blocs est 128 bits et les ronds des sous clés sont égaux à la constante C. La valeur de la constante est :

$$C = 45f83fd1e01a638099c1d2f74ae61d04$$

et elle est aléatoirement choisie.

Cryptanalyse

La question centrale de la cryptographie est la sécurité.

La réponse à cette question se fait sur deux plans : le plan théorique et le plan pratique. Au niveau théorique les propriétés fondamentales caractérisant un objet sécurisé sont la « croissance aléatoire » et le « calcul imprédictible » (Voir [24] ([14]) pour de plus amples détails sur ces concepts).

Sur le plan pratique la sécurité d'un algorithme de cryptage par bloc peut être vérifiée en testant sa résistance à différents types d'attaques connues. L'évaluation de la sécurité consiste à :

· prouver la résistance aux attaques différentielles et linéaires.

· tester cette résistance pour les extensions et les généralisations des attaques différentielles et linéaires.

Remarque 5.4 : Les propriétés chaotiques des algorithmes de cryptage

Après avoir discrétiser un système chaotique, il n'est plus chaotique : toutes les trajectoires d'un algorithme de chiffrement sont périodiques. Quelles sont les avantages de l'utilisation des systèmes chaotiques dans la conception des algorithmes de chiffrement ?

Une partie essentielle de chaque algorithme de chiffrement par blocs est un élément non linéaire généralement appelé S-box. Le S-box est une opération de substitution non linéaire. Les S-boxes sont créées de façon aléatoire ou algorithmique.

Kocarev et al. ont proposé une autre méthode de construction des S-boxes : à savoir l'utilisation des applications chaotiques. Ainsi il ressort de ce travail qu'avec des applications chaotiques très simples et des procédures de discrétisation également très simples, il est possible de générer des algorithmes de cryptage sécurisés.

5.3.4 Chaos et cryptographie dans la recherche actuelle

Bien qu'il soit établi qu'il y ait des relations entre le chaos et la Cryptographie, il est certain que certaines propriétés restent encore à découvrir. Ainsi les cryptosystèmes chaotiques étant classés en deux grandes :

Les cryptosystèmes analogiques basés sur le chaos où intervient la technique de synchronisation chaotique, et les cryptosystèmes numériques basés sur le chaos qui font intervenir une ou plusieurs applications chaotiques de telle manière que la clé secrète soit donnée soit par les paramètres de contrôle soit par les conditions initiales.

L'application logistique étant la plus usitée parmi les applications chaotiques, elle fait l'objet d'études particulières et même de controverses quant aux risques de cryptanalyse lorsqu'elle est choisie dans certains cryptosystèmes [7] .

D'autres questions sont encore ouvertes, à savoir : la propriété de diffusion peut-elle s'apparenter aux exposants de Lyapunov qui mesurent la force du chaos dans les systèmes continus ?

Peut-on mesurer la confusion ? Quels sont les propriétés pertinentes des systèmes chaotiques pour la cryptanalyse ?

Le chaos présente-t-il de réels avantages dans la conception de cryptage par blocs ?

5.4 Quelques méthodes de cryptographie basées sur le chaos

5.4.1 Synchronisation du chaos

Utiliser un signal chaotique dans les télécommunications pose le problème de synchronisation du récepteur dans le but de dupliquer le signal chaotique employé à l'émetteur.

Parmi les différents concepts de synchronisation chaotique qui ont ouvert la voie des applications du chaos aux télécommunications on citera celui de **Yamada** et **Fujisaka** [45] qui ont utilisé une approche locale de la synchronisation chaotique, celui d'**Afraimovich** et al qui ont

développé les concepts importants liés à la synchronisation chaotique et évidemment celui de **Pecora** et **Carroll** [26] connu sous le nom de **synchronisation identique**, développée sur la base de circuits chaotiques couplés, avec l'un maître et l'autre esclave .

Une autre solution plus récente est la méthode de **synchronisation généralisée**, de **Rulkov** et al.

La notion de **synchronisation de phase** entre deux circuits chaotiques couplés a fait son apparition en parallèle avec les précédents concepts de synchronisation. Dans ce cas la synchronisation vise à réaliser une cohérence de phase entre les variables d'état des systèmes considérés. Finalement, plus récemment, une nouvelle technique est apparue avec l'emploi des méthodes d'estimation non-linéaire de type filtrage de **Kalman**, vues comme une généralisation du couplage des systèmes chaotiques.

5.4.2 Transmissions à porteuses chaotiques

Les signaux chaotiques peuvent être utilisés pour la transmission de l'information principalement dans deux objectifs.

· Le premier objectif est de **protéger l'information transmise** (on retrouve ainsi le même type d'applications que celles des méthodes de cryptographie classiques).

· Un deuxième objectif est d'**étaler le signal informationnel** (étalement de spectre), et dans ce cas on retrouve aussi des méthodes développées comparables aux systèmes classiques à étalement de spectre.

Du point de vue de la structure d'un tel système de transmission on peut définir deux approches. La première remplace le signal porteur sinusoïdal par un modulateur chaotique contrôlé d'une manière quelconque par le signal informationnel. Cette solution a l'avantage d'être très simple à implémenter mais par contre nécessite un système chaotique avec des contraintes fortes sur les paramètres intrinsèques et en plus celui-ci doit travailler à des hautes fréquences.

En pratique, il est difficile de trouver des circuits permettant un tel fonctionnement et pour le moment cette solution est surtout considérée dans un cadre théorique.

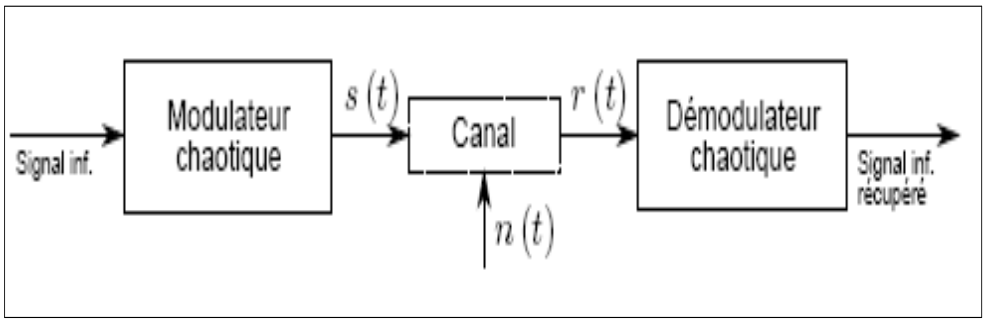


FIG. 5-2 – *Modulation directe du signal informationnel par une porteuse haute fréquence chaotique*

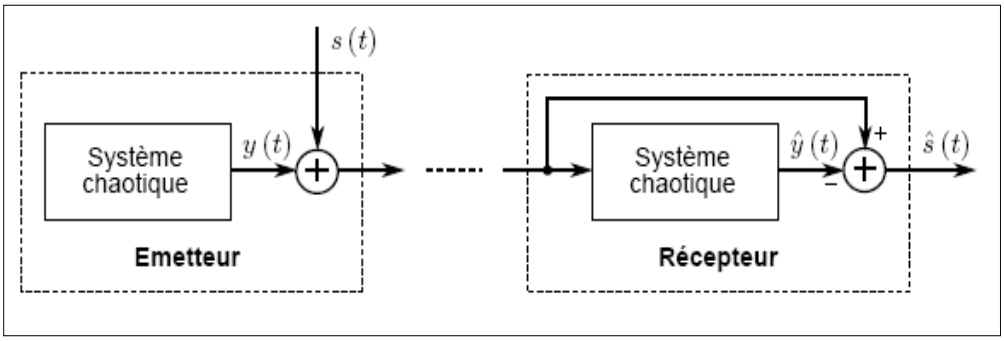


FIG. 5-3 – *Modulation par masquage chaotique*

5.4.3 Masquage chaotique

La méthode de masquage chaotique a été la première solution proposée dans la littérature comme application du chaos aux communications. L'idée est d'additionner directement le signal informationnel $s(t)$ au signal chaotique $y(t)$ et de le récupérer ensuite par synchronisation chaotique. Le même système est utilisé à la fois à l'émetteur et au récepteur, avec la différence que le récepteur est contrôlé par le signal émis pour obtenir la synchronisation.

Grâce à la synchronisation chaotique, il est possible, à la sortie du système dynamique récepteur, que le signal sera plus proche du signal chaotique original $y(t)$ que de la somme $y(t) + s(t)$. Par conséquent une simple différence permet d'obtenir une approximation $\hat{s}(t)$ du

signal informationnel initial. La présence d'un bruit important dans le canal de communication va, de toute évidence, affecter fortement les performances du système. Même si cette méthode n'a pas trouvé d'applications directes sur des canaux radio-fréquence, elle est envisagée comme solution de cryptage dans le cas de la fibre optique.

5.5 Comparaison entre la cryptographie classique et chaotique

Tableau 5.3 :

Cryptographie classique	*Cryptographie chaotique*
Valeurs entières sur un corps fini	**Valeurs continues** en utilisant une représentation en virgule fixe ou flottante
Méthodes algébriques	**Méthodes analytiques**
Réalisation numérique en **arithmétique entière**	Réalisation numérique en **arithmétique non entière**

Chapitre 6

Applications de la cryptographie chaotique

6.1 Introduction

Ces dernières années, en raison de fréquents débit d'images numériques à travers le monde sur les médias de transmission, il est devenu indispensable pour les protéger des fuites. De nombreuses applications comme les bases de données images militaire, de la vidéoconférence confidentielles, systèmes d'imagerie médicale, la télévision par câble, ligne d'albums photos personnels, etc. exigent des systèmes de sécurité robuste, rapide et fiable pour stocker et transmettre des images numériques. Les exigences à remplir les besoins de sécurité des images numériques ont conduit à la mise au point des bonnes techniques de cryptage. Au cours de la dernière décennie, de nombreux algorithmes de chiffrement ont été proposés dans la littérature fondée sur des principes différents. Parmi eux, le chaos des techniques de cryptage basées sur le chaos, afin de fournir une bonne combinaison de vitesse, de haute sécurité, la complexité, les frais généraux raisonnables de calcul et de puissance de calcul, etc. Les images numériques ont certaines caractéristiques telles que : la redondance des données (Data), une forte corrélation entre les pixels adjacents, sont moins sensibles par rapport aux données de texte soit un tout petit changement dans l'attribut d'un pixel de l'image ne dégrade pas considérablement la qualité de l'image et la capacité de données en vrac, etc. En conséquence, les chiffres traditionnels comme **IDEA**, **AES**, **DES**, **RSA**, etc. ne sont pas adaptés pour le cryptage des images en temps réel

que ces chiffres nécessitent un temps de calcul et de grande puissance de calcul élevé. Pour le chiffrement des images en temps réel les chiffres préférables sont seulement ceux qui prennent moins de temps et d'en même temps sans compromettre la sécurité. Un schéma de chiffrement qui tourne très lentement, même peut-être un degré plus haut de fonctionnalités de sécurité serait de peu d'utilité pratique pour les processus en temps réel.

6.2 Le cryptage d'image en utilisant l'application logistique chaotique

Un certain nombre des schémas de chiffrement d'image basés sur le chaos ont été développés ces dernières années que nous discutons en bref dans ce paragraphe. En 1992, **Bourbakis** et **Alexopoulos** ont proposé un schéma de cryptage d'image qui utilise la langue **SCAN** pour crypter et compresser une image en même temps. **Fridrich** ont démontré la construction technique d'un bloc de cryptage symétrique basé sur l'application standard de Baker en deux dimensions. Il ya trois étapes de base dans la méthode de Fridrich :

(a) choisir une application chaotique et la généraliser en introduisant des paramètres.

(b) discrétiser l'application chaotique pour un treillis fini carrés de points qui représentent les pixels.

(c) étendre l'application discrétisée à trois dimensions et en outre il compose avec un simple mécanisme de diffusion.

En outre, **Scharinger** a conçu une technique de cryptage d'image basée sur le chaos de **Kolmogorov**, dans laquelle l'image entière est considérée comme un seul bloc et qui est permutée par le biais d'une clé contrôlée d'un système chaotique. En outre, un registre à décalage générateur pseudo aléatoire est également adopté pour introduire la confusion dans les données. **Yen** et **Guo** ont proposé une méthode de cryptage appelée **BRIE** basée sur l'application logistique chaotique. Le principe de base de la **BRIE** est la recirculation de peu de pixels, ce qui est contrôlé par une séquence chaotique binaire pseudo aléatoire. La clé secrète de la **BRIE** est constituée de deux nombres entiers et une condition initiale de l'application logistique. En outre, Yen et Guo ont également proposé une méthode de cryptage appelée **CKBA** (Chaotic Key Based Algorithm) dans laquelle une séquence binaire comme une clé est générée à l'aide

d'un système chaotique. Les pixels de l'image sont regroupés selon la séquence binaire générée puis **XOR**és et **XNOR**és avec la clé sélectionnée. Plus tard en 2002, **Li** et **Zheng** ont souligné certains défauts dans les systèmes de cryptage présentés dans les références et ont également discuté des améliorations éventuelles à leur sujet. Récemment, Li et al ont proposé une technique de cryptage vidéo basé sur de multiples systèmes numériques chaotique qui est connue comme **CVES** (Chaotic Video Encryption Scheme). Dans ce schéma, 2^n applications chaotiques sont utilisées pour générer des signaux pseudo aléatoires pour masquer la vidéo et effectuer une permutation pseudo aléatoire de la vidéo masqués. En 2004, **Chen** et al ont proposé un chiffrement d'image symétrique dont l'application chaotique en deux dimensions est généralisée à trois dimensions pour la conception en temps réel d'un schéma sécurisé de cryptage d'image. Cette approche utilise l'application tridimensionnelle du chat, pour mélanger les positions des pixels de l'image et utiliser une autre application chaotique pour confondre la relation entre l'image cryptée et son image originale.

Les caractéristiques des applications chaotiques ont attiré l'attention des cryptographes afin de développer de nouveaux algorithmes de cryptage. Etant donné que ces applications chaotiques ont de nombreuses propriétés fondamentales telles que l'érgocité, mixage (mélange) et la sensibilité aux conditions initiales et des paramètres du système / et qui peut être considérée comme analogue à certaines propriétés cryptographiques de cryptage idéal ; comme la confusion, la diffusion, l'équilibre, etc. Dans cette section, un nouveau système de cryptage d'image est proposé sur la base des applications logistiques chaotiques afin de répondre aux exigences de la sécurité de transfert d'image. Dans le schéma de cryptage d'image proposé, une clé secrète externe (tel qu'il est utilisé par Chen et al. Pour le cryptage d'image et par **Pareek** et al pour les ciphers du texte) de $80-$bits et deux applications logistiques chaotiques sont employées. Les conditions initiales pour les applications à la fois logistiques sont calculées en utilisant la clé secrète externe. Dans l'algorithme, la première application logistique est utilisée pour générer des nombres allant de 1 à 24 (nombre peut être répété). La condition initiale de la deuxième application logistique est modifiée par rapport au nombre, généré par la première application logistique. En modifiant l'état initial de la deuxième application logistique de cette manière, sa dynamique devient plus aléatoire. Dans le processus de cryptage proposé, huit différents types d'opérations sont utilisées pour crypter les pixels d'une image et dont le fonctionnement sera

utilisé pour un pixel donné est déterminé par les résultats de la deuxième application. Ainsi, la deuxième application logistique chaotique augmente encore la confusion dans la relation entre l'image cryptée et son image originale. Pour rendre l'algorithme de cryptage plus robuste contre toute attaque, après chaque chiffrement d'un bloc de seize pixels, la clé secrète est modifiée.

6.2.1 La procédure proposée sur le cryptage d'image

Dans cette sous section, nous discutons de la procédure proposée du cryptage d'image étape par étape, ainsi que processus de décryptage en utilisant deux applications logistiques chaotiques.

1− Le processus de cryptage proposé utilise l'image d'une clé secrète externe de 80−bits de longueur. En outre, la clé secrète est divisée en blocs de 8−bits chacun, dénommés **clés de session**.

$$K = k_1 k_2 ... k_{20} \text{ (en hexadécimal)} \tag{6.1}$$

ici, k_i sont les caractères alphanumériques $(0-9$ et A-F) et chaque groupe de deux caractères alphanumériques représente une clé de session. Sinon, la clé secrète peut être représentée en mode **ASCII**.

$$K = K_1 K_2 ... K_{10} \text{ (en } \textbf{ASCII)}$$

ici, chaque K_i représente un bloc de 8−bits de la clé secrète i.e. la clé de session.

2− Dans l'algorithme proposé, deux applications logistiques chaotiques sont utilisées pour atteindre l'objectif de cryptage d'image, qui est comme suit :

$$X_{n+1} = 3.9999 X_n (1 - X_n)$$
$$Y_{n+1} = 3.9999 Y_n (1 - Y_n)$$

Tout au long de l'algorithme, nous gardons la valeur du paramètre du système des applications à la fois chaotiques pour être constant (i.e. 3.9999) ce qui correspond à un cas très chaotique alors que les conditions initiales (X_0 et Y_0) pour ces applications sont calculées en utilisant des manipulations mathématiques sur les clés de session.

3− Pour calculer la condition initiale X_0 pour la première application logistique, on a choisi

trois blocs de clés de session i.e. $K_4K_5K_6$ et les convertir en une chaîne binaire tel que :

$$B_1 = K_{41}K_{42}...K_{48}K_{51}K_{52}...K_{58}K_{61}K_{62}...K_{68}$$

ici, K_{ij} sont les chiffres binaires (0 et 1) du $i^{éme}$ bloc de la clé de session. Ensuite, nous calculons un nombre réel X_{01} en utilisant la représentation binaire ci-dessus tel que :

$$X_{01} = \begin{array}{c}(K_{41} \times 2^0 + K_{42} \times 2^1 + ... + K_{48} \times 2^7 + K_{51} \times 2^8 + K_{52} \times 2^9 + ... + K_{58} \times 2^{15} \\ +K_{61} \times 2^{16} + K_{62} \times 2^{17} + ... + K_{68} \times 2^{23})/2^{24}\end{array}$$

En outre, nous calculons un autre nombre réel X_{02} comme suit :

$$X_{02} = \sum_{i=13}^{18} (k_i)_{10} /96$$

ici les k_i font partie de la clé secrète en mode hexadécimal, comme expliqué dans l'équation (6.1). Maintenant, nous calculons la condition initiale X_0 pour la première application logistique en utilisant X_{01} et X_{02} tel que :

$$X = (X_{01} + X_{02}) \bmod 1$$

4− Nous générons une séquence de 24 nombres réels $f_1, f_2, ..., f_{24}$ par itération de la première application logistique en utilisant la condition initiale obtenue à l'étape 3. Gardons à l'esprit que nous avons considéré que ces valeurs, qui tombent dans l'intervalle $[0.1, 0.9]$, les autres valeurs sont éliminées de la séquence. La séquence de nombres réels est convertie en une séquence d'entiers en utilisant la formule suivante :

$$P_k = int\,(23 \times (f_k - 0.1)\,/0.8) + 1 \text{ où } k = 1, 2, ..., 24$$

5− Pour calculer la condition initiale Y_0 pour la deuxième application logistique, nous avons choisi trois blocs de clés de session i.e. K_1K_2K3, et les convertir en une chaîne binaire tel que :

$$B_2 = K_{11}K_{12}...K_{18}K_{21}K_{22}...K_{28}K_{31}K_{32}...K_{38}$$

ici les K_{ij} sont les chiffres binaires (0 ou 1) du $i^{éme}$ bloc de la clé de session. Nous calculons ensuite un nombre réel Y_{01} en utilisant la représentation binaire comme ci-dessus :

$$Y_{01} = (B_2)_{10} / 2^{24}$$

En outre, nous calculons un autre nombre réel Y_{02} comme suit :

$$Y_{02} = \left(\sum_{k=1}^{24} \underline{B_2 [P_k]} \times 2^{k-1} \right) / 2^{24}$$

ici, $\underline{B_2 [P_k]}$ désigne la valeur du $P_k^{ième}$ bit dans la chaîne binaire B_2 i.e. qu'il est soit 0 ou 1. Maintenant, nous calculons la condition initiale Y_0 pour la deuxième application logistique en utilisant Y_{01} et Y_{02} tel que :

$$Y_0 = (Y_{01} + Y_{02}) \bmod 1$$

6− Les trois octets (bytes) consécutifs à partir du fichier image représentent la valeur des couleurs : rouge, bleu et vert **(RBV)**, respectivement, ensemble forment un seul pixel de l'image.

7− Nous divisons l'intervalle $[0.1, 0.9]$ en 24 intervalles non-cumul et les organiser en huit groupes différents. Ensuite, nous attribuons autre type de fonctionnement correspondant à chacun de ces groupes.

Cette étape est répétée $(K_{10})_{10}$ (i.e. le décimal équivalent de la $10^{éme}$ clé de session) fois. Enfin, les octets cryptés des couleurs rouge, vert et bleu sont écrits dans un fichier i.e. le cryptage des octets est atteint.

Nous répétons les étapes 6 et 7 pour les 15 prochains pixels du fichier image.

8− Après le cryptage d'un bloc de 16 pixels du fichier image, nous modifions les clés de session K_1 par K_9 comme suit :

$$(K_i)_{10} = ((K_i)_{10} + (K_{10})_{10}) \bmod 256, (0 \leq i \leq 9)$$

Après avoir modifié la clé secrète de la manière indiquée ci-dessus, la dernière valeur de X à partir de l'étape 4 comme condition initiale pour la première application logistique (en d'autres termes $X_0 = f_{24}$), nous avons de nouveau générer une séquence de 24 nombres réels, comme

expliqué dans l'étape 4 et puis répétez les étapes $5-7$ jusqu'à ce que le fichier entier de l'image est épuisé.

Le processus de décryptage est tout à fait similaire au processus de cryptage décrit ci-dessus ; seulement une différence dans l'étape 7 i.e. dans le cas des processus de cryptage, on itère la deuxième application logistique $(K_{10})_{10}$ fois et on fait les opérations respectives pour le cryptage (qui dépendra de l'issue de l'application logistique) après chaque itération de l'application. Toutefois, dans le cas de processus de décryptage, nous parcourrions d'abord la deuxième application logistique $(K_{10})_{10}$ fois et nous ferons les opérations respectives pour le décryptage (qui dépend à nouveau des résultats de l'application logistique) dans l'ordre inverse.

6.2.2 Analyse de la sécurité

Un bon procédé de cryptage devrait être robuste contre toutes les formes de cryptanalyse, les statistiques et les attaques par force brute. Dans cette sous section, nous discutons de l'analyse de la sécurité du schéma de cryptage d'image proposé telles que l'analyse statistique, analyse de sensibilité avec respect à la clé et le plaintext, l'analyse de l'espace de clés pour prouver que le cryptosystème proposé est sécurisé contre les attaques les plus communes.

L'analyse statistique

Il est bien connu que de nombreux cryptages ont été analysés avec succès à l'aide de l'analyse statistique et plusieurs attaques statistiques ont été mises au point. Par conséquent, un chiffre idéal devrait être solide contre toute attaque statistique. Pour prouver la robustesse de la procédure du cryptage d'image proposée, nous avons effectué une analyse statistique en calculant les histogrammes, les corrélations de deux pixels adjacents dans les images cryptées et le coefficient de corrélation de plusieurs images et de leurs images cryptées correspondantes, de l'image d'une base de données.

L'analyse d'histogramme Une image-histogramme montre comment les pixels dans une image graphique sont distribués par le nombre de pixels à chaque niveau de l'intensité des couleurs. Nous avons calculé et analysé les histogrammes de plusieurs images cryptées ainsi que plusieurs de leurs images colorées d'origine qui ont un contenu très différent. Un exemple

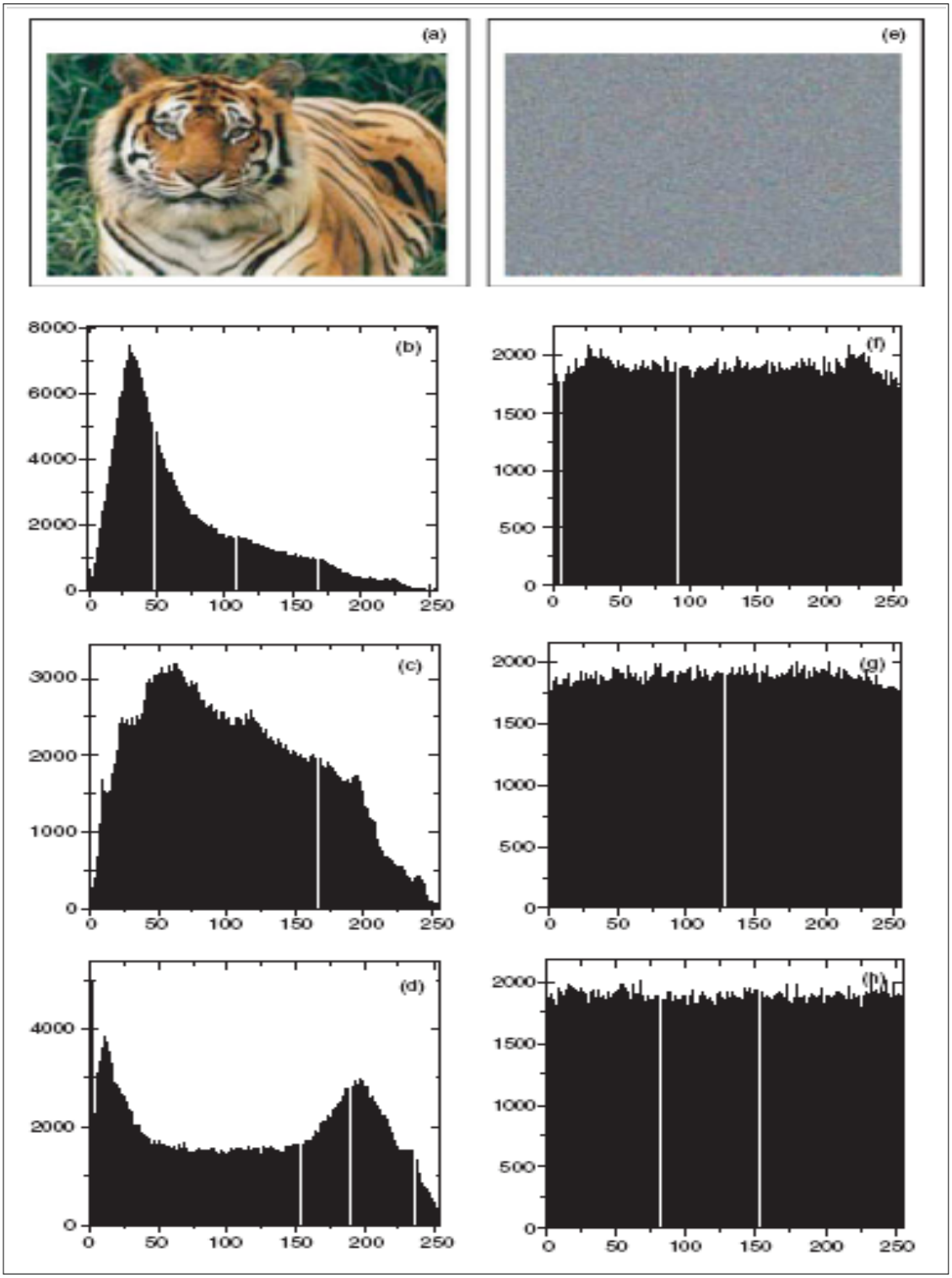


FIG. 6-1 – *Analyse d'histogramme*

d'analyse de l'histogramme est indiqué sur la figure (6.1). Particulièrement dans le cadre (a), nous avons montré l'image d'origine et dans les cadres (b), (c) et (d), respectivement, les histogrammes des canaux rouge, bleu et vert de l'image originale (cadre (a)). Dans le cadre (e), nous avons montré l'image cryptée de l'image originale (cadre (a)) en utilisant la clé secrète '$ABCDEF0123456789FF05$' (en hexadécimal) et dans les cadres (f), (g) et (h), respectivement, les histogrammes des canaux rouge, bleu et vert de l'image cryptée (cadre (e)). Il ressort de la figure (6.1) que les histogrammes de l'image cryptée sont assez homogènes et très différents des histogrammes respectifs de l'image originale et donc ne fournissent aucun élément permettant de concevoir une attaque statistique sur le procédé de cryptage de l'image proposée.

Coefficient de l'analyse de corrélation En plus de l'analyse de l'histogramme, nous avons également analysé la corrélation entre deux pixels adjacents verticalement aussi bien horizontalement dans plusieurs images et leurs images cryptées. Dans la figure (6.2), nous avons montré la distribution de deux pixels adjacents dans les images originales et cryptées montrées dans la figure (6.1) a et (6.1) e. En particulier, dans les cadres (a) et (b), nous avons représenté les distributions de deux pixels adjacents horizontalement dans les images originales et cryptées respectivement. De même, dans les cadres (c) et (d), respectivement, les distributions de deux pixels adjacents verticalement dans les images originales et cryptées ont été représentées.

En outre, nous avons aussi calculé la corrélation entre deux pixels adjacents verticalement aussi bien horizontalement dans les images originales cryptées. Pour ce calcul, nous avons utilisé la formule suivante :

$$C = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{\left(N\sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right) \times \left(N\sum_{j=1}^{N} y_j^2 - \left(\sum_{j=1}^{N} y_j\right)^2\right)}} \tag{6.2}$$

où x et y sont les valeurs de deux pixels adjacents dans l'image et N est le nombre total de pixels de l'image sélectionnée pour le calcul. Dans le tableau 6.1, nous avons donné les coefficients de corrélation pour des images originales et cryptées sur la figure (6.1) a et (6.1) e respectivement. Il ressort de la figure (6.2) et le tableau 6.1, que la corrélation est négligeable

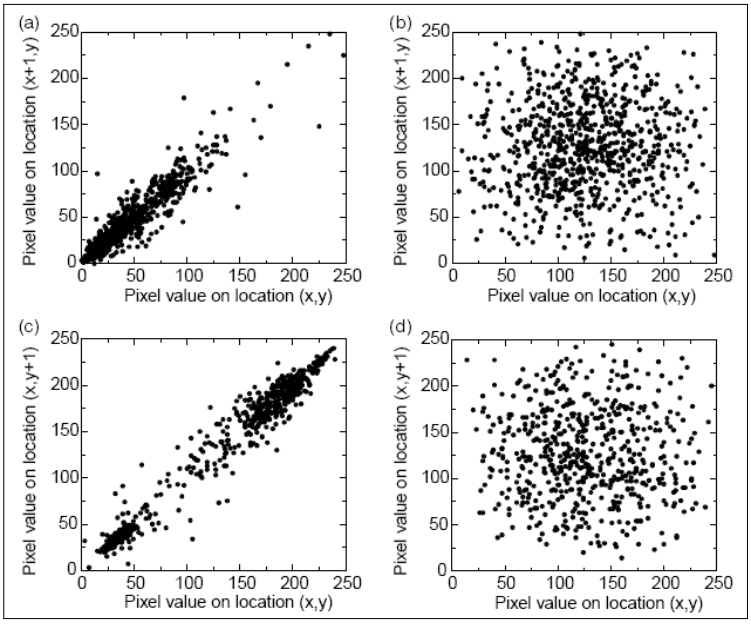


FIG. 6-2 – *Analyse de corrélation*

entre les deux pixels adjacents dans l'image cryptée. Toutefois, les deux pixels adjacents de l'image originale sont fortement corrélés.

Tableau 6.1 :

Sens	*Image originale (figure* (6.1) *a)*	*Image cryptée (figure* (6.1) *e)*
Horizontal	0.8710	0.0041
Vertical	0.4668	−0.0337

L'analyse de sensibilité

Une procédure de cryptage idéal d'image doit être sensible à l'égard de la clé secrète i.e. le changement d'un seul bit de la clé secrète doit produire une image cryptée complètement différente. Pour tester la sensibilité de la clé dans la procédure de cryptage d'image proposée, nous avons fait les étapes suivantes :

(a) L'image originale (figure (6.3) *a*) est cryptée en utilisant la clé secrète '$A148CB3FD50766E47405$' (en hexadécimal) et la même image résultant est référée comme image cryptée A (figure (6.3) *b*).

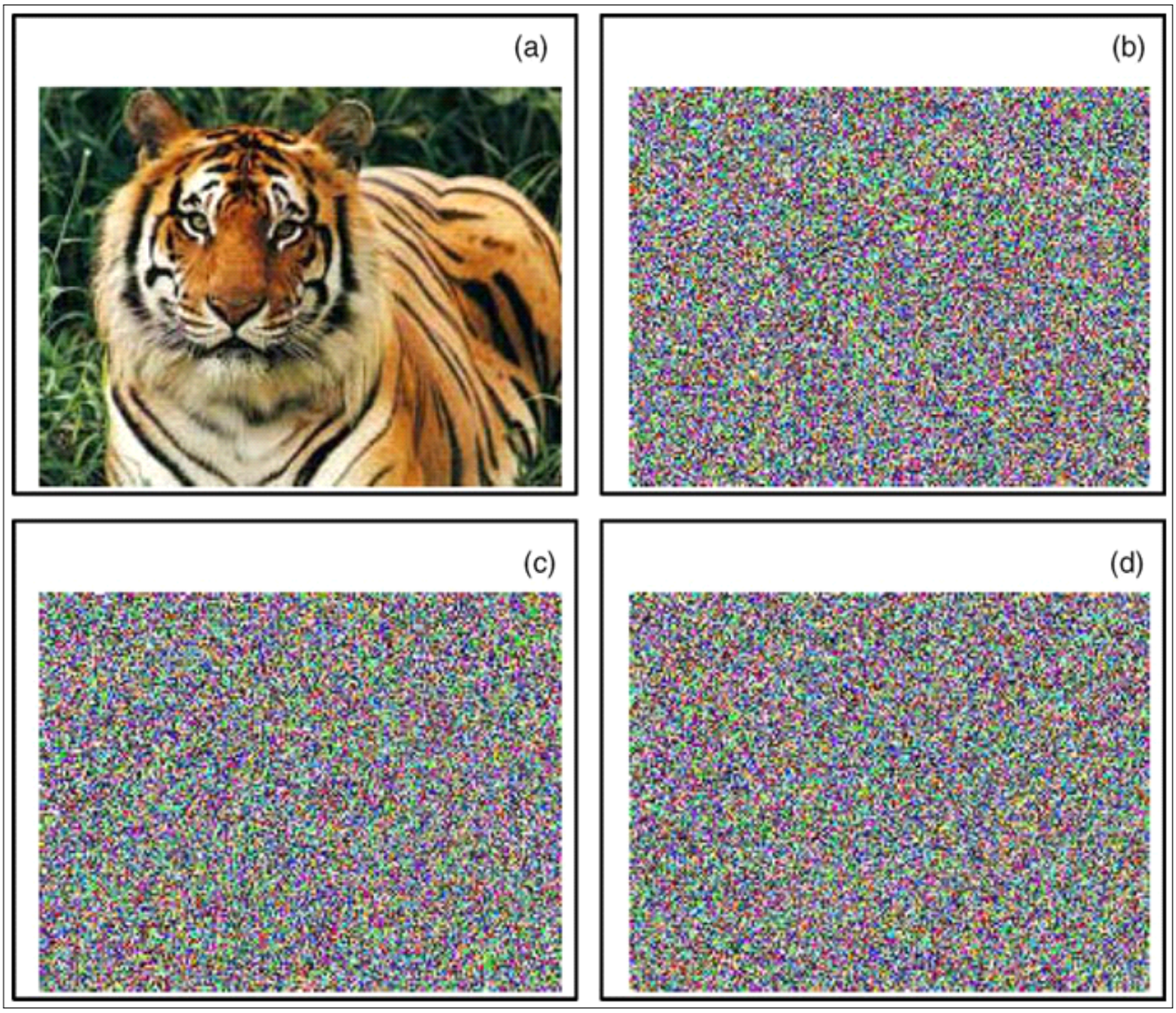


FIG. 6-3 – *Test* 1 *de la sensibilité*

(b) La même image originale est cryptée en faisant une modification légère dans la clé secrète i.e. '$B148CB3FD50766E47405$' (le bit le plus significatif de la clé secrète est modifié) et l'image résultant est référée comme image cryptée B (figure (6.3) c).

(c) De nouveau, la même image originale est cryptée en faisant une modification légère dans la clé secrète i.e. '$A148CB3FD50766E47406$' (le bit le moins significatif de la clé secrète est modifié) et l'image résultant est référée comme image cryptée C (figure (6.3) d).

(d) Finalement, les trois images cryptées A, B et C sont comparées.

Dans la figure (6.3), nous avons montré l'image originale ainsi que les trois images cryptées produites dans les étapes susmentionnées. Il n'est pas facile de comparer les images cryptées par une simple observation. Ainsi, pour faire la comparaison, nous avons calculé la corrélation entre les pixels correspondants des trois images cryptées. Pour ce calcul, nous avons utilisé la même formule donnée dans l'équation (6.2), sauf que dans ce cas, x et y sont les valeurs des pixels correspondants dans les deux images cryptées à être comparées. Dans le tableau 6.2, nous avons donné les résultats des coefficients de corrélation entre les pixels correspondants des trois images cryptées A, B et C. Il est clair d'après le tableau qui n'existe pas de corrélation entre les trois images cryptées, même si celles-ci ont été produites en utilisant des différences légères dans les clés secrètes.

Tableau 6.2 :

Image 1	*Image* 2	*Image* 3
Image cryptée A (figure (6.3) b)	Image cryptée B (figure (6.3) c)	0.00393
Image cryptée B (figure (6.3) c)	Image cryptée C (figure (6.3) d)	-0.00627
Image cryptée C (figure (6.3) d)	Image cryptée A (figure (6.3) b)	0.00289

En outre, dans la figure (6.4), nous avons montré les résultats de quelques tentatives pour décrypter une image cryptée avec une différence légère dans les clés secrètes alors on peut l'utiliser pour le cryptage de l'image originale. En particulier, dans les cadres (a) et (b), respectivement, l'image originale et l'image cryptée produites à l'aide de la clé secrète '$A039FD52FC87CD1E4406$' (en hexadécimal) sont présentées alors que dans les cadres (c) et (d), respectivement, les images après le décryptage de l'image cryptée (montré dans le cadre (b)) avec les clés secrètes '$A139FD52FC87CD1E4406$' (en hexadécimal) et '$A039FD52FD87CD1E4406$'

(en hexadécimal). Il est clair que le décryptage avec une différence légère dans la clé secrète échoue complètement et, partant, la procédure de cryptage d'image proposée est très sensible aux changements des clés secrètes.

FIG. 6-4 – *Test 2 de la sensibilité*

Nous avons aussi mesuré le nombre de taux de change des pixels **(NTCP)** pour voir l'influence de la modification d'un seul pixel dans l'image originale sur l'image cryptée par l'algorithme proposé. Le **NTCP** mesure le pourcentage de différents nombres de pixels entre les deux images. Nous prenons deux images cryptées, C_1 et C_2, dont les images originales correspondantes ont une différence seulement dans un seul pixel. Nous définissons un tableau à deux dimensions D, ayant la même taille que l'image C_1/C_2. Le $D\,(i,j)$ est déterminé à partir de $C_1(i,j)$ et $C_2(i,j)$. Si $C_1(i,j) = C_2(i,j)$ alors $D\,(i,j) = 1$ autrement dit $D\,(i,j) = 0$. Le **NTCP**

est définie par l'équation suivante :

$$NTCP = \frac{\sum_{ij} D(i,j)}{wh} \times 100\%$$

où w et h sont la largeur et la hauteur de l'image cryptée. Nous avons obtenu le **NTCP** pour un grand nombre d'images à l'aide de notre système de cryptage et le trouvé à plus de 99% montrant par là que la méthode de cryptage est très sensible à l'égard de petits changements dans le texte en clair.

Analyse de l'espace de clés

Pour un cipher d'image sécurisé, l'espace de clés doit être assez grand pour faire l'impossible attaque en force brute. Le cipher d'image proposé a 2^{80} $\left(\approx 1.20893 \times 10^{24}\right)$ différentes combinaisons de la clé secrète. Un cipher d'image avec un tel grand espace de clés est suffisant pour une utilisation pratique fiable. Toutefois, on peut avoir plus de clés pour le cryptage / décryptage d'image dans le cipher d'image proposé et il peut facilement être intégré dans l'algorithme en faisant des modifications légères.

Dans le cipher d'image proposé, deux applications chaotiques sont utilisées pour le cryptage / décryptage qui sont sensibles aux conditions initiales. Les conditions initiales pour ces deux applications logistiques sont calculées à partir de la clé secrète avec différentes formules. En raison de la limitation de la précision numérique d'un ordinateur, 24−bit sont utilisés pour assembler un nombre à virgule flottante, c'est à dire l'état initial. En outre, la clé secrète est modifié, après cryptage / décryptage de chaque bloc de 16 pixels, de la part de la clé de session, i.e. K_{10} et de plus, les conditions initiales de ces deux applications logistiques chaotiques sont calculées à partir de la clé secrète modifiée.

Tableau 6.3 :

Taille de l'image (pixels)	*Bits / pixels*	*Durée moyenne (s) cryptage / décryptage*
256×256	24	$0.33 - 0.39$
512×512	24	$0.38 - 0.40$
1024×1024	24	$6.26 - 6.32$
2048×2048	24	$25.15 - 25.32$

L'analyse temporelle

Outre l'examen de la sécurité, la vitesse de course de l'algorithme est également un aspect important pour un bon algorithme de cryptage. Nous avons mesuré les taux de cryptage / décryptage de plusieurs images colorées de différentes tailles en utilisant le système de cryptage d'image proposé. Le temps d'analyse a été fait sur un ordinateur **Pentium** 4 avec 256 Mo de RAM. La durée moyenne de cryptage / décryptage prise par l'algorithme pour différentes images taillées, dans le Tableau 6.3.

Remarque 6.1 **:**

Ce nouveau schéma de cryptage d'images proposé, utilise deux applications logistiques chaotiques et une clé externe de 80 bits. Les conditions initiales pour les deux applications logistiques sont calculées en utilisant la clé secrète externe. Dans le processus de cryptage proposé, huit différents types d'opérations sont utilisés pour crypter les pixels d'une image et dont le fonctionnement sera utilisé pour un pixel donné est déterminé par le résultat de l'application logistique. Pour rendre l'algorithme de cryptage plus robuste contre toute attaque, la clé secrète est modifiée après avoir crypter un bloc de seize pixels de l'image. Nous avons effectué une analyse statistique, analyse de sensibilité des clés et une analyse de l'espace de clés pour prouver la sécurité de la procédure de cryptage de la nouvelle image. Enfin, nous concluons avec la remarque que la méthode proposée devrait être utile pour le cryptage d'images en temps réel et les applications de transmission.

6.3 Dynamiques chaotiques appliquées à la cryptographie pour les télécommunications optiques

La cryptographie par chaos est apparue récemment au début des années 90, comme une application originale des dynamiques non linéaires en régime chaotique. Alors que les premières réalisations ont été mises en œuvre à partir de circuits électroniques, l'optique s'est rapidement intéressée au sujet. Grâce à des propriétés physiques particulières et familières dans le domaine de l'optique, de nombreuses démonstrations originales et variées ont été développées, fonctionnant avec des dynamiques chaotiques aux propriétés attractives, tant en terme de complexité des régimes chaotiques, qu'en terme de bande passante, et donc de vitesse de codage.

Avec l'avènement des réseaux mondiaux et des techniques de communication numérique, la cryptographie a été brutalement transférée à partir d'une zone très limitée i.e. le domaine militaire, la diplomatie, et les affaires d'État, dans une région très vaste, couvrant, dans le même temps, les domaines précédents, mais aussi les entreprises privées, l'information médicale et de la banque, le paiement électronique sur Internet, etc. la sécurité et le secret sont des exigences fondamentales pour chacun, dans la société de la communication aujourd'hui, justifiant ainsi le nombre d'activités de recherche, et à part les techniques de cryptage les plus générales fondées sur des algorithmes Softwere (logiciels), deux méthodes originales de cryptage basées sur des principes physiques sont apparues comme physiquement et technologiquement réalisables au cours des deux dernières décennies : la cryptographie quantique, et la cryptographie basée sur le chaos. La première est principalement dédiée à la sécurité absolue de distribution des clés secrètes, dans laquelle la clé peut ensuite être utilisée pour transmettre des informations en toute sécurité par l'algorithme conventionnel de cryptage. La deuxième méthode est également impliquée au niveau de la couche physique des systèmes de transmission, avec l'avantage de permettre éventuellement un cryptage à très grande vitesse (jusqu'à plusieurs dizaines de Gb / s, à la différence des Softweres de cryptage fondés sur des algorithme qui sont généralement limités à quelques centaines de Mb / s).

La genèse de cryptage par chaos a commencé avec la démonstration de la synchronisation de deux trajectoires chaotiques couplées. La propriété de synchronisation pour ces formes d'ondes a été la première à être réaliste non, en raison de la tendance intrinsèque naturelle de deux quasi-identiques dynamiques chaotiques à s'écarter les unes des autres, en raison de la soi-disant sensibilité aux conditions initiales, populairement appelé « effet papillon ».

En théorie de la communication, la possibilité de synchronisation d'un signal donné, sinusoïdales ou non, signifie généralement que la forme d'onde peut être utilisée comme support d'information dans un système de transmission, la synchronisation est ensuite utilisée dans le récepteur pour récupérer les informations transportées. En outre, lorsque la forme d'onde dispose d'un caractère pseudo-aléatoire, une propriété privée de la communication on peut s'attendre, avec la capacité de support : c'est typiquement le cas pour la technique de transmission numérique bien connue, le **CDMA** (Code Division Multiple Access), utilisé dans le **GPS** (Global Positioning System), et pour la troisième génération de téléphone mobile. En bref, le **CDMA**

implique de longues séquences de bits pseudo-aléatoires comme une forme d'onde porteuse pour chaque canal, dont le transporteur est par conséquent à large bande en raison du caractère pseudo-aléatoire. La séquence agit comme un code, sans laquelle le décodage et l'obtention de l'information codée ne peut pas être effectuée, et la transmission est sécurisée par l'utilisation de ce transporteur pseudo-aléatoire. De même, il a été supposé dans le début des années 1990 que les signaux chaotiques pourrait être utilisés comme signaux porteurs d'informations, et en même temps comme un moyen de protéger l'information transportée en raison de son caractère pseudo-aléatoire et à large bande. Le déterminisme intrinsèque de la dynamique chaotique, est l'étape de la technique de synchronisation.

La première démonstration expérimentale de la transmission des informations en utilisant un transporteur chaotique a été suivie assez rapidement par le principe de synchronisation en 1993. Le générateur de chaos est un circuit électronique générant des oscillations chaotiques de Lorenz incorporé dans un espace de phase $3-$dimensionel. La première cryptanalyse de tels systèmes a souligné que le chaos d'une complexité faible est définitivement une faiblesse du système de cryptage. La dynamique non linéaire de l'optique (la dynamique du laser, le retard de grandes cavités optiques ou optoélectroniques) étaient bien connus pour leur capacité à produire la dynamique de grande complexité. Différents groupes ont été revisités de manière indépendante comme ces différents systèmes optiques pour l'utilisation dans des systèmes de cryptage basés sur le chaos, du point de vue théorique (cavité externe laser semi-conducteur), et du point de vue expérimental (synchronisation des cavités chaotiques externes des lasers semi-conducteurs, le cryptage / décryptage avec des lasers à fibre dopée erbium chaotique, le cryptage / décryptage de longueur d'onde laser chaotique, chaos synchronisé dans les lasers à microprocesseur, la synchronisation entre GHz externes lasers semi-conducteurs à cavité). Tous ces résultats ont été obtenus avec des systèmes optiques, pour les raisons suivantes :

· Ces systèmes sont, bien sûr, intrinsèquement dédiés aux systèmes modernes de communication utilisant des fibres optiques.

· Les processus dynamiques impliqués dans les systèmes optiques peuvent être rapides, ce qui aboutirait à une autre caractéristique intéressante du chaos à base de cryptographie optique, et une vitesse de cryptage potentiellement très élevée.

· Des dynamiques de grande complexité chaotique sont obtenues, que ce soit en raison du

couplage non linéaire complexe des interactions entre la lumière et la matière dans les lasers, ou en raison de la présence d'une cavité commentaires délai permettant une dynamique avec un grand nombre de degrés de liberté.

La cryptanalyse de ces cryptosystèmes optiques basés sur le chaos a été aussi beaucoup plus difficile à coder que celle des premières Setups électroniques. Seules les dynamiques chaotiques des lasers à fibre à l'erbium ont été analysées avec suffisamment de détails, avec l'inconvénient que le chaos ainsi généré peut être brisé et le message facilement récupéré. Le manque de complexité inhérente à la non-linéarité faible attachée à la dynamique du laser à fibre est responsable de la réussite d'attaque. La cryptanalyse des autres systèmes de cryptage basés sur le chaos est toujours en progrès, mais plus orientée vers les techniques habituellement consacrées à l'analyse dynamique non linéaire, les techniques linéaires ne peuvent pas être définitivement suffisantes pour récupérer suffisamment l'information de la série temporelle chaotique masquant le message.

Une telle diversité dans le générateur du chaos optique expérimentale est très positive pour la définition de l'architecture optimale, ainsi que pour la concurrence dans la communauté scientifique impliquée dans les systèmes de cryptage basé sur le chaos.

6.4 Conclusion générale et perspectives

La cryptographie basée sur la théorie du chaos s'est rapidement développée au cours de ces dernières années. Aujourd'hui la plupart des recherches se concentrent sur l'utilisation du chaos dans des cryptosystèmes en vue d'apporter une amélioration (temps de chiffrement, sécurité) par rapport aux méthodes standards de la cryptographie (**DES**, **IDEA**, **AES**), ceci grâce aux caractéristiques des signaux chaotiques tels que : bonnes propriétés cryptographiques, reproductibilité à l'identique (déterministes) et l'hyper sensibilité à la clé secrète.

On cite quelques uns des axes de recherche actuelle portant sur l'étude de nouvelles structures d'algorithmes de chiffrement / déchiffrement basés sur le chaos.

1− Dans une nouvelle approche pour **chiffrer un message en utilisant le chaos**, N. Smaoui et A. Kanso génèrent une orbite chaotique numérique basée sur l'application logistique, ils montrent qu'il existe un nombre fini d'orbites. L'algorithme construit génère un nombre fini

d'applications qui sont utilisées dans l'algorithme de Baptista (*M.S. Baptista,* ***"Cryptography with Chaos",*** 1998), pour chiffrer chaque caractère du message. Il est montré que l'utilisation du chaos et de l'observation dans le processus de chiffrement améliore le niveau de sécurité.

N. Smaoui, A. Kanso, ***"Cryptography with Chaos and Shadowing",*** 2009.

2− **La cryptographie à clé secrète** est au centre de nombreuses recherches dont celles de Wang et Zhao. Il existe quelques algorithmes de chiffrement à clés publiques et des algorithmes cryptographiques basés sur le chaos, importants pour la sécurité des réseaux. Wang et Zhao utilisent l'application chaotique de Chebyshev pour construire un algorithme d'échange de clés. La propriété de semi-groupe des polynômes de Chebytchev permet d'obtenir un algorithme qui pallie aux inconvénients de plusieurs protocoles déjà connus. Pour l'instant les premiers résultats analytiques et expérimentaux montrent qu'il est efficace et sûr.

X. Wang, J. Zhao, ***"An improved key agreement protocol based on chaos"****,* 2010.

3− **Le chiffrement d'image** étant quelque peu différent du cryptage de texte en raison de certaines caractéristiques inhérentes à l'image, telles que la capacité de données et une forte corrélation entre les pixels qui sont généralement difficiles à manipuler par les méthodes conventionnelles, les propriétés cryptographiques souhaitables pour les applications chaotiques comme la sensibilité aux conditions initiales et le comportement aléatoire de type ont attiré l'attention des cryptographes pour développer de nouveaux algorithmes de chiffrement. Par conséquent, les recherches récentes des algorithmes de chiffrement d'image sont de plus en plus basés sur des systèmes chaotiques, mais il y a l'inconvénient d'avoir un espace de clés petit et un niveau faible de sécurité des cryptosystèmes chaotiques unidimensionnels. Mazloom et Eftekhari-Moghadam étudient une technique de cryptographie chaotique à clé de chiffrement symétrique avec un chiffrement par flot. Afin d'accroître la sécurité de l'algorithme proposé, la clé secrète est utilisée pour générer les conditions initiales et les paramètres de l'application chaotique en faisant quelques transformations algébriques à la clé. Pour obtenir plus de sécurité et plus de complexité, le cryptosystème utilise la taille de l'image et des composants des couleurs, augmentant ainsi considérablement la résistance aux attaques connues. Les résultats des analyses expérimentale et statistique ainsi que plusieurs tests de sensibilité des clés montrent que le schéma de cryptage proposé est un moyen efficace et sûr aussi bien pour le chiffrement d'images en temps réel que pour leur transmission.

S. Mazloom, A.M. Eftekhari-Moghadam, ***"Color image encryption based on Coupled Nonlinear Chaotic Map",*** 2009.

4– Les scientifiques de l'université d'Athènes, associés notamment à ceux de l'université de Franche-Comté (dans le cadre du projet **OCCULT**, acronyme de "Optical Chaos Communications Using Laser-diodes Transmitters") sont parvenus à acheminer des données sur une onde porteuse chaotique à travers un réseau commercial à fibre optique, démontrant le potentiel de la communication utilisant le chaos optique dans la transmission protégée de données. Les conclusions de l'expérience ont été publiées dans la revue scientifique Nature (**http ://www.nature.com/)**.

Cette technique d'avant-garde, qui emploie des émetteurs et récepteurs laser synchronisés pour chiffrer l'information au niveau des composants, représente une importante mise à niveau qualitative par rapport aux systèmes de sécurité existants en matière de transmission protégée de données. La communication par cryptage chaotique n'avait jusqu'à présent été expérimentée qu'en laboratoire, mais jamais dans un véritable réseau commercial.

Pour accroître les niveaux de sécurité et de confidentialité, on utilise une onde porteuse de message générée par un laser semi-conducteur opérant en mode chaotique à travers un réseau de 120 km de fibre optique. Grâce à cette méthode, le message est transmis à des vitesses de 1 Go/s, et est récupéré avec un taux d'erreur de transmission inférieur à 1 bit pour 10 millions (**http ://www.femto-st.fr/~jdudley/opto/recherche.htm**).

5– Pour évaluer **la sécurité des systèmes de signature et tatouage numérique** (le tatouage numérique vise à insérer une marque (un filigrane) à un support, et ce de manière robuste), l'université de Franche Comté propose une méthode d'évaluation basée sur la théorie du chaos. Celle-ci vérifiant l'instabilité, et donc la non prédictibilité du processus, cela permet de le rendre plus difficilement piratable. Ce tatouage invisible qui ne dégrade pas le contenu d'une image, permet en revanche de détecter l'éventuelle source d'un vol. Car le tatouage s'apparente à un identifiant pour l'acheteur. Techniquement, le système étudie les propriétés de chaos mathématique de l'algorithme : le degré de mélange des données (soit leur entropie), leur éparpillement, et la sensibilité d'une clé. La théorie du chaos possède bon nombre d'outils qui permettent d'évaluer qualitativement et quantitativement le désordre généré par un système. Plus grand est le nombre de propriétés de chaos satisfaites par le système, meilleure est

l'imprévisibilité, donc la sécurité, de l'algorithme.

D'autres méthodes existent déjà pour évaluer la sécurité de ces solutions de cryptage. Elles sont basées sur les probabilités, c'est-à-dire qu'elles mesurent le niveau de chance qu'un attaquant a de pouvoir trouver le message caché sans connaître la clé secrète. Mais le problème avec cette théorie est qu'elle ne s'avère applicable que dans certains cadres-utilisation d'une même clé secrète et qu'elle suppose des hypothèses fortes rarement satisfaites.

6− **La synchronisation (celle de lasers chaotiques)** à la fois pour coder et décoder l'information, pourrait offrir une alternative fiable pour la sécurisation de réseaux de communications. On citera dans ce cadre les travaux suivants :

· **http ://picasso.di.uoa.gr.** *Photonic Integrated Components Applied to Secure Chaos Encoded Optical Communications Systems. A European Commission project. Accessed* 1 *February* 2010.

· **http ://www.ifisc.uib-csic.es/phocus.** *Towards a Photonic Liquid State Machine Based on Delay-Coupled Systems. A European Commission project. Accessed* 1 *February* 2010.

7− **L'accès sécurisé aux images médicales** conservées sur des supports numériques est de la plus grande importance. Ces images peuvent être de très grande taille et en nombre, et contiennent généralement des données confidentielles. Par conséquent, les deux objectifs principaux sont :

· préserver la confidentialité des données personnelles du patient.

· réduire les coûts de stockage et augmenter la vitesse de transmission, sans altérer la qualité. Aujourd'hui, la pratique des canaux de transmission numériques comme Internet, et les scénarios de stockage numérique, comme les disques durs, **CD** ou **DVD**, sont considérés comme parfaits, sans bruit ou autres interférences. Ainsi, aucun contrôle d'erreur des techniques de codage sont nécessaires.

Les chercheurs Alvarez, Li and Hernandez proposent une nouvelle technique pour transmettre et stocker des images médicales associées à des renseignements confidentiels sur des patients. Dans un premier temps pour garantir la sécurité de l'information des patients, ces données confidentielles sont cryptées en utilisant un algorithme développé par les auteurs. Ensuite, l'information chiffrée est couplée avec les images médicales. Le processus de tatouage consiste à échanger les codes **ASCII** dans le fichier texte crypté avec le bit le moins significatif

(**LSB**) de l'échelle de gris peu à peu. Huit bits du fichier texte (donc un caractère **ASCII**) remplace les **RLSP** de huit consécutifs pixels de l'image. L'image entrelacée est donc transmise sur des canaux bruités et stockées.

G. Alvarez, S. Li, L. Hernandez, ***"Analysis of security problems in a medical image encryption system",*** 2007.

8– Le groupe **SYD** du **LESIA** (Laboratoire d'Etudes Spatiales et d'Instrumentation en Astrophysique) s'intéresse depuis plusieurs années à l'étude théorique de modèles permettant de générer du chaos. Les nombreuses études effectuées ont permis de mettre en évidence différentes classes pour lesquelles le chaos présente des propriétés spécifiques, où intervient une grande sensibilité par rapport au choix des paramètres et des conditions initiales générant le chaos.

Le projet actuel consiste à utiliser des signaux chaotiques pour élaborer le cryptage des messages dans un système de cryptographie à clés publiques reposant sur le principe du « secret partagé ». Dans ce contexte, des signaux chaotiques issus de transformations ponctuelles de dimension deux ou trois sont utilisés. La récurrence est publique, les paramètres de la récurrence et les conditions initiales sont privées.

Afin d'améliorer la robustesse des algorithmes, il est proposé de construire des signaux chaotiques à partir de systèmes de dimension supérieure (supérieure ou égale à trois), de comprendre comment ces signaux chaotiques apparaissent et de les analyser. Des études antérieures ont été menées concernant l'ordre deux.

V. Guglielmi, M. Bonnefont, D. Fournier-Prunaret, P. Pinel, A.K. Taha, ***"Performances d'un Cryptosystème Numérique à base de Chaos",*** 2005.

Les études portent sur la compréhension des mécanismes de bifurcations entraînant l'apparition d'attracteurs chaotiques et leur évolution. De même des études fréquentielles en liaison avec ces bifurcations sont également menées.

V. Guglielmi, P. Pinel, D. Fournier-Prunaret, A.K. Taha, ***"Chaos-based cryptosystem on DSP",*** *accepté pour publication dans Chaos, Solitons and Fractals,* 2010.

La cryptographie est une science en pleine expansion, ainsi l'augmentation considérable des débits des télécommunications réalisée ces dernières années tant dans les transmissions numériques qu'analogiques, a rendu les méthodes usuelles de cryptage vulnérables. En effet, ces dernières reposant sur un algorithme de calcul deviennent de plus en plus fragile face à

la montée en puissance des calculateurs, car, si leur rapidité de calcul est très efficace pour chiffrer ou déchiffrer l'information, elle l'est aussi pour la cryptanalyse. De plus, l'annonce des capacités de calcul très prometteuses (et colossales) de l'ordinateur quantique ainsi que la constante avancée de la théorie des nombres font apercevoir la chute brutale du cryptage algorithmique.

9− **La cryptographie chaotique et la cryptographie quantique** sont deux alternatives très prometteuses qui ont été développées durant la dernière décennie. La cryptographie par chaos, dont on a donné un aperçu dans ce mémoire, a déjà donné la preuve de sa faisabilité et de sa puissance de chiffrage (supérieur à 1 Gbits/s).

Quant à la cryptographie quantique, elle résout de manière radicale le problème de la confidentialité puisque par principe, elle offre une clé incassable (lié au principe d'incertitude d'Heisenberg) mais, son débit est très limité (de l'ordre de quelques dizaines de kbits/s) et son coût de mise en œuvre reste très élevé.

A ce propos une équipe internationale de chercheurs vient de trouver le moyen de réellement randomiser une liste de nombres aléatoires. L'étude vient d'être publiée dans la revue Nature.

Pour créer des listes de nombres aléatoires à des fins de cryptage, les cryptographes utilisent des algorithmes mathématiques appelés "générateurs de nombres pseudo-aléatoires". Cependant, ces derniers ne sont jamais entièrement « aléatoires », car les programmeurs ne peuvent garantir qu'une séquence de nombres ne peut être prévue d'une manière ou d'une autre. Une équipe de physiciens vient d'accomplir un exploit dans la génération de nombres aléatoires en appliquant la mécanique quantique pour produire une série de nombres réellement aléatoires.

Pour de plus amples informations sur cet important résultat, il est possible de consulter l'article paru dans la revue Nature.

S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D.N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T.A. Manning, ***"Random numbers certified by Bell's theorem",*** *Nature* 464, 15 *April* 2010.

Bibliographie

[1] A. Lizée, **"Doublement de Période dans les Instruments a Anche Simple du Type Clarinette ; Approches numérique et expérimentale"**, Université Pierre et Marie Curie, Paris VI, 2004.

[2] A.B. Orue, V. Fernandez, G. Alvarez, G. Pastor, M. Romera, F. Montoya, C. Sanchez-Avila, S. Li, **"Breaking a SC-CNN-based Chaotic Masking Secure Communication System"**, International Journal of Bifurcation and Chaos, Vol. 19, No. 4, p.p. 1329 – 1338, 2009.

[3] B. Gunsel, A.K. Jain, **"Multimedia Content Representation, Classification and Security"**, Springer, 2006.

[4] B. Ycart, **"Systèmes différentiels Systèmes itératifs"**, CPU de l'université Paris V-René Descartes, 2002.

[5] C. Çokal, E. Solak, **"Cryptanalysis of a chaos-based image encryption algorithm"**, Physics Letters A, Vol. 373, Issue 15, p.p. 1357 – 1360, 2009.

[6] C.D. Lee, B.J Choi, K.S. Park, **"Design and evaluation of a block encryption algorithm using dynamic-key mechanism"**, Future Generation Computer Systems, Vol. 20, Issue 2, p.p. 327 – 338, 2004.

[7] D. Arroyo, G. Alvarez, V. Fernandez, **"On the inadequacy of the logistic map for cryptographic applications",** ACTAS DE LA X RECSI, SALAMANCA, p.p. 77 – 82, 2008.

[8] D. Arroyo, R. Rhouma, G. Alvarez, S. Li,V. Fernandez, **"On the security of a new image encryption scheme based on chaotic map lattices"**, International Journal of Modern Physics, 2008.

[9] D. Arroyoar, G. Alvarez, S. Li, C. Li, **"Cryptanalysis of a new chaotic cryptosystem based on ergodicity"**, International Journal of Modern Physics B, Vol. 23, No. 5, p.p. 651 – 659, 2009.

[10] E. Goncalvès, **"Introduction aux systèmes dynamiques et chaos"**, Institut National Polytechnique de Grenoble, 2004.

[11] E.N. Lorenz, **"Deterministic nonperiodic flow"**, J. Atmos. Sci. 20, p.p. 130 – 141, 1963.

[12] F. Sun, Z. Lü, S. Liu, **"A new cryptosystem based on spatial chaotic system"**, Optics Communications, Vol. 283, Issue 10, p.p. 2066 – 2073, 2010.

[13] G. Alvarez, S. Li, **"Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption"**, Communications in Nonlinear Science and Numerical Simulations, Vol. 14, No. 11, p.p. 3743 – 3749, 2009.

[14] G. Alvarez, S. Li, **"Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems"**, International Journal of Bifurcation and Chaos, Vol. 16, No. 8, p.p. 2129 – 2151, 2006.

[15] G. Alvarez, S. Li, L. Hernandez, **"Analysis of security problems in a medical image encryption system"**, Computers in Biology and Medicine, Vol. 37, No. 3, p.p. 224 – 227, 2007.

[16] G. Situ, J. Zhang, **"A lensless optical security system based on computer-generated phase only masks"**, Optics Communications, Vol. 232, Issues 1 – 6, p.p. 115 – 122, 2004.

[17] H. Dang-Vu, C. Delcarte, **"Bifurcations et chaos : Une introduction à la dynamique contemporaine avec des programmes en Pascal, Fortran et Mathématica"**, Ellipses, 2000.

[18] H. Hermassi, R. Rhouma, S. Belghith, **"Joint compression and encryption using chaotically mutated Huffman trees"**, Communications in Nonlinear Science and Numerical Simulation, Vol. 15, Issue 10, p.p. 2987 – 2999, 2010.

[19] H. Liu, X. Wang, **"Color image encryption based on one-time keys and robust chaotic maps"**, Computers and Mathematics with Applications, 2010.

[20] J. Baglio, **"Notes de cours de Physique Non-Linéaire"**, Département de Physique Ecole Normale Supérieure de Cachan, 2007.

[21] J.M. Amigo, L. Kocarev, J. Szczepanski, **"Theory and practice of chaotic cryptography"**, Physics Letters A, Vol. 336, p.p. 211 – 216, 2007.

[22] J.M. Blackledge, **"Multi-algorithmic Cryptography using Deterministic Chaos with Applications to Mobile Communications"**, ISAST Transactions on Electronics and Signal Processing, Vol. 1, No. 2, 2008.

[23] L. Kocarev, **"Chaos-Based Cryptography : A Brief Overview"**, IEEE CAS Newsletter, 2001.

[24] L. Kocarev, G. Jakimoski, **"Logistic map as a block encryption algorithm"**, Physics Letters A, Vol. 289, p.p. 199 – 206, 2001.

[25] L. Larger, J.P. Goedgebuer, **"Encryption using chaotic dynamics for optical telecommunications"**, Comptes Rendus Physique, Vol. 5, p.p. 609 – 611, 2004.

[26] L.M. Pecora, T.L. Carroll, **"Synchronization in Chaotic Systems"**, Physical Review Letters, Vol. 64, No. 8, p.p. 821 – 824, 1990.

[27] M. Amin, O.S. Faragallah, A.A. Abd El-Latif, **"A chaotic block cipher algorithm for image cryptosystems"**, Communications in Nonlinear Science and Numerical Simulation, 2010.

[28] M. Lakshmanan, S. Rajaseker, **"Nonlinear dynamics"**, Springer, 2003.

[29] M.S. Baptista, **"Cryptography with Chaos"**, Physics Letters A, Vol. 240, p.p. 50 – 54, 1998.

[30] N.K. Pareek, V. Patidar, K.K. Sud, **"Image encryption using chaotic logistic map"**, Image and Vision Computing, Vol. 24, p.p. 926 – 934, 2006.

[31] P. Stavroulakis, **"Chaos Applications in telecommunications"**, Taylor and Francis Group, 2006.

[32] Q.V. Lawande, B.R. Ivan, S.D. Dhodapkar, **"Chaos based cryptography : A new approach secure communications"**, BARC Newsletter 258, 2005.

[33] R. Hasimoto-Beltran, **"A generalized chaotic encryption system for multimedia applications"**, Revista Mexicana de Fisica, Vol. 53, No. 5, p.p. 232 – 236, 2007.

[34] R. Rhouma, E. Solak, D. Arroyo, S. Li, G. Alvarez, S. Belghitha, Comment on **"Modified Baptista type chaotic cryptosystem via matrix secret key"**, Physics Letters A, Vol. 373, No. 37, p.p. 3398 – 3400, 2009.

[35] R. Schmitz, **"Use of chaotic dynamical systems in cryptography"**, Journal of the Franklin Institute, Vol. 338, p.p. 429 – 441, 2001.

[36] R.M. May, **"Simple mathematical model with very complicated dynamics"**, Nature, Vol. 261, p. 459, 1976.

[37] S. Behnia, A. Akhshani, A. Akhavan, H. Mahmodi, **"Applications of tripled chaotic maps in cryptography"**, Chaos, Solitons and Fractals, Vol. 40, p.p. 505 – 519, 2009.

[38] S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan, **"A novel algorithm for image encryption based on mixture of chaotic maps"**, Chaos, Solitons and Fractals, Vol. 35, p.p. 408 – 419, 2008.

[39] S. Boughaba,**"Phénoméns de Chaos Deterministe et de Turbulence. L'attracteur étrange de chua : Coexistence D'attracteurs Dynamique Symbolique et Confineurs"**, thèse de doctorat, 2002.

[40] S. Franceschelli, T. Roque, M. Paty, **"Chaos Systèmes Dynamiques : éléments pour une épistémologie"**, Hermann, 2007.

[41] S. Li, **"Encryption-Friendly Multimedia Coding and Communications : Is it Necessary and Possible ?"**, E-Letter of IEEE Communications Society's Technical Committee on Multimedia Communications, Vol. 4, No. 1, p.p. 15 – 18, 2009.

[42] T. Dudok de Wit, **"Fluides et Physique Non-Linéaire"**, UFR Sciences de l'Université d'Orleans, 2006.

[43] T. Gao, Z. Chen, **"A new image encryption algorithm based on hyper-chaos"**, Physics Letters A, Vol. 372, Issue 4, p.p. 394 – 400, 2008.

[44] T. Habutsu, Y. Nishio, I. Sasase, S. Mori, in : "**Advances in Cryptology— EUROCRYPT** '91", Springer, Berlin, p.p. 127 – 140, 1991.

[45] T. Yamada, H. Fujisaka, **"Stability theory of synchronized motion in coupled-oscillator systems"**, Progress of Theoretical Physics, Vol. 69, No. 1, p.p. 32 – 47, 1983.

[46] V.S. Afraimovich, N.N. Verochev, M.I. Rabinovich, **"Stochastic synchronization of oscillations in dissipative systems"**, Radio Phys. and Quantum Electron, 1983.

[47] X.Y. Wang, F. Chen, T. Wang, **"A new compound mode of confusion and diffusion for block encryption of image based on chaos"**, Communications in Nonlinear Science and Numerical Simulation, Vol. 15, Issue 9, p.p. 2479 − 2485, 2010.

[48] Y. Tang, Z. Wang, J.A. Fang, **"Image encryption using chaotic coupled map lattices with time-varying delays"**, Communications in Nonlinear Science and Numerical Simulation, Vol. 15, Issue 9, p.p. 2456 − 2468, 2010.

Réferences des Perspectives

[1] N. Smaoui, A. Kanso, **"Cryptography with Chaos and Shadowing"**, 2009.

[2] X. Wang, J. Zhao, **"An improved key agreement protocol based on chaos"**, 2010.

[3] S. Mazloom, A. M. Eftekhari-Moghadam, **"Color image encryption based on Coupled Nonlinear Chaotic Map"**, Chaos, Solitons and Fractals, Vol. 42, Issue 3, p.p. 1745−1754, 2009.

[4] G. Alvarez, S. Li, L. Hernandez,**"Analysis of security problems in a medical image encryption system"**, Computers in Biology and Medicine, Vol. 37, Issue 3, p.p. 424−427, 2007.

[5] V. Guglielmi, M. Bonnefont, D. Fournier-Prunaret, P. Pinel, A.K. Taha, **"Performances d'un Cryptosystème Numérique à base de Chaos"**, 2005.

[6] V. Guglielmi, P. Pinel, D. Fournier-Prunaret, A.K. Taha, **"Chaos-based cryptosystem on DSP"**, accepté pour publication dans Chaos, Solitons and Fractals, 2010.

[7] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D.N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T.A. Manning, **"Random numbers certified by Bell's theorem"**, Nature international weekly journal of science, Vol. 464, p.p. 1021−1024, 2010.