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

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET D' INFORMATIQUE
DEPARTEMENT D'ÉLECTRONIQUE

Mémoire de Fin d'Etude
de MASTER PROFESSIONNEL

Option : Électronique Industrielle

THÈME:

ÉTUDE ET RÉALISATION D'UN SYSTEME CHAOTIQUE BASÉ SUR LE CIRCUIT DE CHUA

Proposé et diriegé par:
M.HAMICHE, Hamid

Présenté par:
M.AIT HAMMI, Abdelfateh

Année Universitaire **2013-2014**

Sommaire

Introduction générale

Depuis l'antiquité, l'homme n'a pas cessé de chercher les différents moyens pour transmettre un message à son correspondant et pouvoir ainsi communiquer avec lui en toute sécurité. Tout ces efforts ont conduit à l'évolution des modes de communication et à leur développent et continu à la recherche de débits supérieurs, une mobilité améliorée et surtout une confidentialité totale dans la communication.

La cryptographie a été depuis très longtemps un champ de bataille entre deux camps, ceux qui veulent cacher des données contre ceux qui veulent savoir tout ce qui traîne comme données. De ce fait, à chaque fois que le premier trouve un moyen pour dissimuler ses données, aussitôt et dans la limite de ses moyens, le second trouve un moyen lui permettant de récupérer les données cachées.

Ainsi est née la cryptographie chaotique qui consiste à camoufler l'information avec le signal chaotique en vue de les cacher.

Dans ce mémoire, notre travail entre dans cette thématique. Il consiste à la conception et à la réalisation d'un système de transmission sécurisée de données à base d'oscillateur s chaotiques choisies dits de Chua.

Notre travail sera structuré comme suit :

Dans le premier chapitre de ce travail, nous avons défini les systèmes dynamiques de manière générale et les systèmes chaotiques de manière un plus détaillé Le second chapitre sera consacré à la synchronisation des systèmes chaotiques et les différentes méthodes utilisées à cette fin.

Le troisième chapitre est dédié à la simulation d'un système chaotique choisi, le circuit de Chua en l'occurrence ainsi que la méthode choisie pour sa synchronisation.

Le quatrième chapitre consiste à la réalisation pratique d'un système chaotique synchronisable ainsi que son utilisation dans le cryptage d'un signal audio et les possible améliorations à lui apporter.

Ce travail sera finalisé par une conclusion et synthèse des différentes parties de ce mémoire qui permettront d'avoir des perspectives intéressantes sur les possibilités d'améliorations à apporter au système étudié.

CHAPITRE 1

INTRODUCTION AUX SYSTÈMES CHAOTIQUES

1.1 Introduction et historique

CHAOS ?

Il faut admettre que ce terme n'est pas facile à définir. On peut essayer de le définir en se basant sur les références les plus récentes. Le mot lui-même prend origine du terme « χαοσ », utilisé par les Grecs pour décrire l'espace vide infini dont ils ont supposé l'existence avant l'émergence de toutes choses. Les Romains ont repris le terme et interprété l'idée sous-jacente pour concevoir quelque chose d'informe, dans lequel -croient-ils- l'architecte du monde a introduit l'ordre et l'harmonie. De nos jours, dans le langage commun «Chaos» décrit un état de désordre et d'irrégularité [7].

Dans le milieu scientifique, le concept a émergé dans la seconde partie des années 1970 en tant que science des phénomènes non linéaires complexes montrant certaines caractéristiques communes. Le terme a été imposé par les physiciens chez lesquels :

« L'idée dominante a été que le chaos constituait une grande révolution scientifique (la troisième du siècle, disait-on, après la relativité et la mécanique quantique) ou du moins l'avènement d'un paradigme gouvernant un ensemble de disciplines en train de former une nouvelle science ».[10]

Alors que chez les mathématiciens le terme imposé est « systèmes dynamiques » pour souligner l'ancienneté des théories et la continuité des méthodes. Un juste milieu serait de considérer le chaos :

« Un vaste processus de convergence socio-disciplinaire qui s'inscrit sur la longue durée et se cristallise à un moment précis, la décennie 1975-1985 »[11]

Pour mieux comprendre, on doit voir les choses dans un contexte historique. Ce n'est pas injuste de dire que tout a commencé avec le mathématicien Henri Poincaré (1892) qui a démontré que certains systèmes mécaniques, dont l'évolution temporelle est gouvernée par des équations hamiltoniennes, peuvent exhiber un mouvement chaotique.

Malheureusement, ceci fut considéré par beaucoup de physiciens comme simple curiosité.

Il a fallu 70 ans pour que le météorologiste E.N. Lorenz (1963) découvre que

même un simple ensemble de trois équations (non linéaires couplées de premier ordre) peut donner lieu à des trajectoires complètement chaotiques. Ainsi, Lorenz a mis en évidence un des premiers exemples de chaos déterministe dans les systèmes dissipatifs.

Dans les années qui ont suivi, à cause des résultats théoriques, de la puissance incrémentale des ordinateurs, et des techniques expérimentales de plus en plus raffinées, il est devenu vraisemblable que ce phénomène est abondant dans la nature et a beaucoup de conséquences et de ramifications dans de nombreux domaines scientifiques. Pour un historique plus développé, voir [11].

Il faut noter que la non-linéarité est une condition nécessaire, mais pas suffisante pour générer le chaos. Il faut aussi noter que le comportement chaotique observé dans le temps n'est dû, ni à une source extérieure de bruit, ni à un degré infini de liberté, ni à un caractère stochastique, c.-à-d. c'est intrinsèque [7].

Le concept moderne du chaos déterministe est de plus en plus utilisé dans des contextes scientifiques variant des mathématiques et physiques des systèmes dynamiques et jusqu'aux variations temporelles complexes de tous types (ex. dans la chimie, biologie, physiologie, économie, sociologie et même la psychologie) [12].

1890	Le Roi Oscar II de Suède octroie un prix au premier chercheur qui pourrait déterminer et résoudre le problème des n-corps des orbites des corps célestes et ainsi prouver la stabilité du système solaire. Jusqu'à ce jour, le problème n'a pas été résolu.
1890	Henri Poincaré gagne le premier prix du Roi Oscar II. Etant le plus proche à résoudre le problème de n-corps, il a découvert que l'orbite de trois corps célestes agissantes l'une sur l'autre peut engendrer un comportement instable et imprévisible. Ainsi, le chaos est naît (mais pas encore mentionné !).
1963	Edward Lorenz découvre le premier système chaotique dans la météo ou encore appelé attracteur étrange.

1975	Tien-Yien Li et James A. Yorke ont présenté pour la première fois le terme “chaos” dans un article intitulé “Period three implies chaos”.
1978	Mitchell Feigenbaum introduit un nombre universel associé au chaos.
1990	Edward Ott, Celso Grebogi et James A. Yorke. Introduisent la notion de contrôle du chaos.
1990	Lou Pecora. Synchronisation des systèmes chaotiques.

Tab-1 Historique du chaos

Contrôle	Première application du chaos est le contrôle du comportement irrégulier dans les circuits et les systèmes. Liste des divers applications est inclue dans le tableau 3.
Synchronisation	Communication sécurisée, cryptage, radio.
Traitement d’information	Codage, décodage et stockage d’information dans des systèmes chaotiques, tel que les éléments de mémoires et les circuits. Reconnaissance de forme.
Prédiction à court terme	Les maladies contagieuses, température, économie.

Tab-2 Application du chaos

Engineering	Contrôle de vibration, stabilisation des circuits, réactions chimiques, turbines, étages de puissance, lasers, combustion, et beaucoup plus.
Ordinateurs	Commutation des paquets dans des réseaux informatiques. Cryptage. Contrôle du chaos dans les systèmes robotiques.
Communications	Compression et stockage d’image. Conception et management des réseaux d’ordinateurs.
Médecine et biologie	Cardiologie, analyse du rythme du cœur (EEG), prédiction et contrôle d’activité irrégulière du cœur.
Management et finance	Prévisions économiques, analyse financière, et prévision du marché.

Tab-3 Domaine d’application du chaos

1.2 Définitions

1.2.1 Système dynamique non linéaire

Un système dynamique en temps continu est décrit par un système d'équations différentielles, alors qu'en temps discret, on parle d'un système d'équations aux différences finies.

temps continu

$$\dot{x}=f(t,x,u)\ y=h(t,x,u) \tag{1}$$

avec $x\in U\subseteq\mathbb{R}^n$ vecteur de dimension n

$f:\mathbb{R}^n\to\mathbb{R}^n$ fonction non linéaire désignant le champs de vecteurs

$h:\mathbb{R}^n\to\mathbb{R}^n$ fonction éventuellement non linéaire qui désigne le vecteur de sortie

et $u\in V\subseteq\mathbb{R}^p$ représente l'entrée du système

si le système (1) ne depend pas de l'entrée, on aura dans ce cas

$$\dot{x}=f(t,x) \tag{2}$$

le système (2) est considéré dynamique pour la simple raison qu'a partir de n'importe quelle condition initialle x_0, on peut deduire l'état futur x(t) pour t>0.

temps discret

Comme mentionné ci-dessus, un système dynamique en temps discret est representé par des équations aux differences finies ayant comme modèl général

$$x(k+1)G(k,x(k),u(k))\ y(k)=h(k,x(k),u(k)) \tag{3}$$

avec

$G:\mathbb{R}^n\to\mathbb{R}^n\times\mathbb{Z}^+\to\mathbb{R}^n$ signifie la dynamique du système en temps discret

En temps discret, on définit aussi le système autonome comme une dynamique qui ne dépend pas de l'instant k :

(4) $$x(k+1)=G(x(k),u(k))\ y(k)=h(x(k),u(k))$$

1.2.2 Système autonome

Un système autonome est tout système dynamique non linéaire qui ne dépend pas explicitement du temps. Il est donné comme suit:

$$\begin{cases} \dot{x} = f(x, y) \\ \dot{y} = g(x, y) \end{cases} \quad (5)$$

Un système autonome est indépendant du temps initial, alors qu'un système non autonome ne l'est pas. Dans un système autonome, tout instant peut être considéré comme instant initial, et tout état x(t) du système peut être considéré comme un état initial.

1.2.3 Comportement chaotique

Un système non linéaire peut avoir un comportement en régime permanent plus complexe que les comportements habituels: oscillations périodiques, quasi-périodiques, etc. Dans ce cas, la sortie du système est très sensible aux conditions initiales, d'où la "non prévisibilité" de la sortie à long terme. On dit alors que le système a un comportement chaotique.
Le modèle chaotique, ci-dessous, donné par Otto de Rössler illustre le caractère chaotique de tels systèmes:

$$\begin{cases} \dot{x}_1 = -x_2 - x_3 \\ \dot{x}_2 = x_1 + a x_2 + 0.01\, x_1 \ln(x_3) \\ \dot{y} = c + x_3 (x_1 - b) \end{cases} \quad (6)$$

avec (x1, x2, x3) le vecteur d'état et a, b et c les paramètres du système.
Le système de Rössler montre un comportement chaotique pour a = 0.2, b = 5.7, c = 0.2 avec les conditions initiales x1(0) = 0.01, x2(0) = 0.01 et x3 (0) = 0.01.

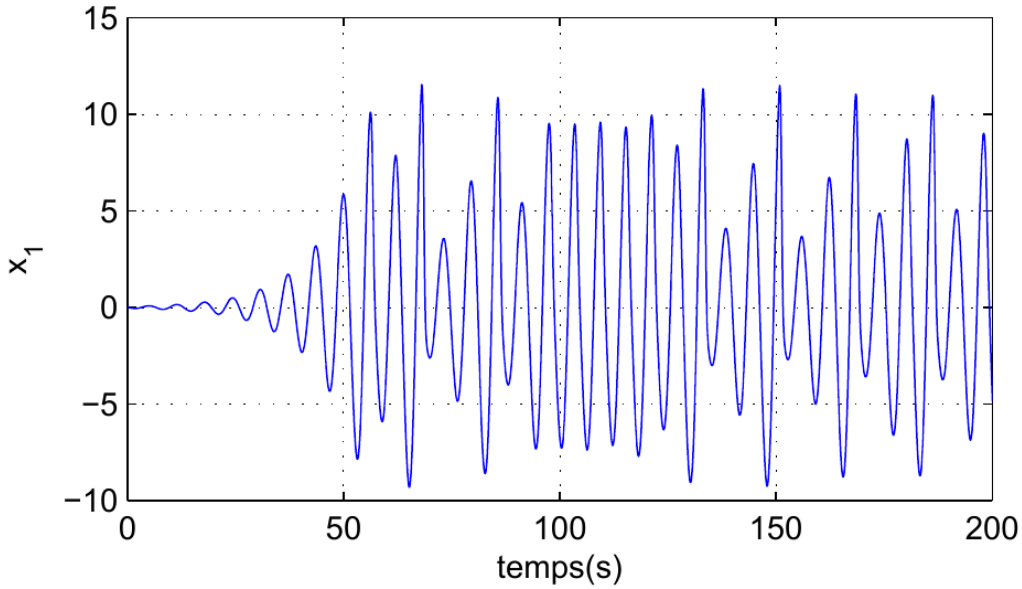


Fig-1 Etat chaotique x1 du système de Rössler

1.3 Le chaos

Le chaos tel que le scientifique le comprend ne signifie pas l'absence d'ordre, il se rattache plutôt à une notion d'imprévisibilité, d'impossibilité de prévoir une évolution à long terme du fait que l'état final dépend de manière si sensible de l'état initial.

On appelle donc un système dynamique chaotique, un système qui dépend de plusieurs paramètres et caractérisés par une extrême sensibilité aux conditions initiales. Ils ne sont pas déterminés ou modélisés par des systèmes d'équations linéaires ni par les lois de la mécanique classique , pourtant, ils ne sont pas nécessairement aléatoires, relevant du seul calcul des probabilités.

Pour une meilleur comprénhension des systèmes chaotiques, on se sert de ces quelques définitions et proprietés.

a) Non-linéarité

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

b) Déterminisme

Un système déterministe est un système dont l'état présent est complètement déterminé par les conditions initiales, en contradiction avec un système stochastique pour lequel l'état présent reflète les conditions initiales avec en plus d'une réalisation particulière d'un paramètre aléatoire (bruit ou variable interne).

c) Aspect aléatoire

Tous les états d'un système chaotique présentent des aspects aléatoires comme illustré dans la figure 1.

d) Sensibilité aux conditions initiales

Sensibilité aux conditions initiales signifie que chaque point dans un système chaotique est arbitrairement près approchée par d'autres des points avec sensiblement différentes voies d'avenir, ou trajectoires. Ainsi, un petit changement arbitraire, ou perturbation, de la trajectoire actuelle peut conduire à un comportement futur significativement différente.

La sensibilité aux conditions initiales est populairement connu comme « l'effet papillon », ainsi appelé parce que le titre d'un document donné par Edward Lorenz en 1972 à l'Association américaine pour l'avancement des sciences à Washington, DC, intitulé Prévisibilité: Est-ce que le battement d'ailes d'un papillon dans Brésil déclencher une tornade au Texas?. [1] Le battement des ailes représente un petit changement dans l'état initial du système, ce qui provoque une chaîne d'événements conduisant à des phénomènes à grande échelle. Avait pas le papillon battit des ailes, la trajectoire du système aurait pu être très différent.

Une conséquence de sensibilité aux conditions initiales, c'est que si nous commençons avec seulement une quantité limitée d'informations sur le système (comme c'est généralement le cas dans pratique), puis au-delà d'un certain

temps, le système ne sera plus prévisible. C'est le plus connu dans le cas de la météo, qui est généralement prévisible seulement une semaine à l'avance [2] Bien sûr, cela ne signifie pas que nous ne pouvons rien dire sur les événements dans un avenir lointain.; il ya des restrictions sur le système. Avec le temps, nous savons que la température ne sera jamais atteindre 100 degrés Celsius ou tomber à -130 degrés Celsius sur la terre, mais nous ne sommes pas en mesure de dire quel jour exactement nous aurons la température la plus chaude de l'année.

En termes plus mathématiques , l'exposant de Lyapunov mesure la sensibilité aux conditions initiales. Compte tenu de deux trajectoires de départ dans l'espace des phases qui sont infiniment proches, avec une séparation initiale δZ qui finissent divergentes à un taux donné par

$$|\delta Z| \approx e^{\lambda t} |\delta Z_0| \tag{7}$$

où t est le temps et λ est l'exposant de Lyapunov. Le taux de séparation dépend de l'orientation du vecteur de séparation initiale, donc il ya tout un spectre d'exposants de Lyapunov. Le nombre d'exposants de Lyapunov est égal au nombre de dimensions de l'espace de phase, mais il est courant de se référer simplement à la plus grande. Par exemple, l'exposant de Lyapunov maximal (MLE) est le plus souvent utilisé car il détermine la prévisibilité global du système. Un MLE positif est généralement considéré comme une indication que le système est chaotique.

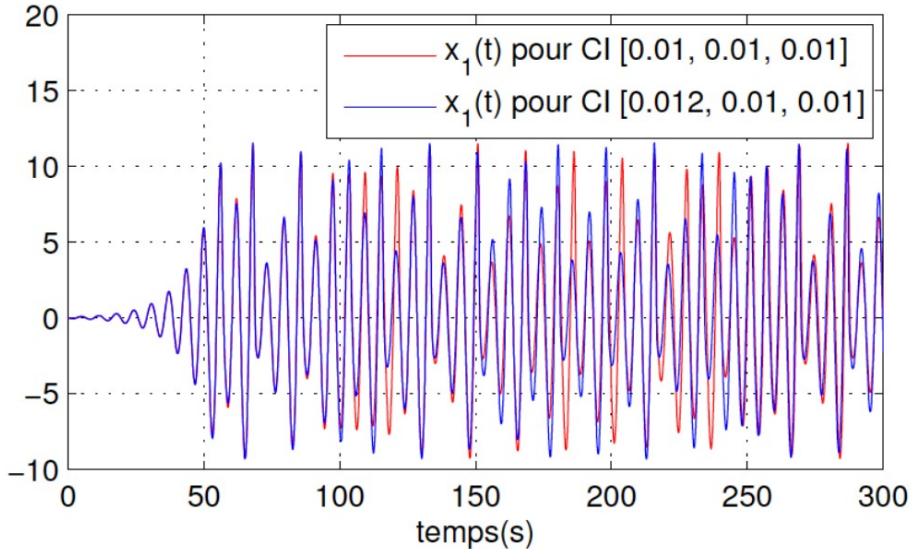


Fig-2 Illustration de la propriété de sensibilité aux conditions initiales sur l'état x1

Il existe également d'autres propriétés liées à la sensibilité des conditions initiales, comme mesure théorique mélange (tel que discuté dans la théorie ergodique) et les propriétés d'un système K . [3]

1.3.1 Exposants de Lyapunov

L'évolution chaotique est difficile à appréhender car la divergence des trajectoires sur l'attracteur est rapide. Pour cette raison on essaie si c'est possible de mesurer sinon d'estimer la vitesse de divergence ou de convergence. Cette vitesse est donnée par l'exposant de Lyapunov qui caractérise le taux de séparation de deux trajectoires très proches [4] [5].

Soit $f:\mathbb{R}\to\mathbb{R}$ une fonction de classe C^1. Pour chaque point x_0 on définit un exposant de Lyapunov $\lambda(x_0)$ comme suit :

$$\lambda(x_0)=\lim_{n\to\infty}\sup\frac{1}{n}\log\left(\left|f(n)'(x_0)\right|\right)=\lim_{n\to\infty}\sup\frac{1}{n}\sum_{j=0}^{n-1}\log\left(\left|f'(x_j)\right|\right) \qquad (8)$$

Avec x j = f j (x0)

Donc deux trajectoires dans le plan de phase initialement séparées par un taux Z_1 divergent après un temps $\Delta t = t_2 - t_1$ vers Z_2 tel que :

$$\left|Z_2\right|\approx e^{\lambda\Delta t}\left|Z_1\right| \qquad (9)$$

Où λ est l'exposant de Lyapunov

Les exposants de Lyapunov sont une généralisation des valeurs propres pour le pointfixe et des multiplieurs caractéristiques pour les solutions périodiques.
Pour un attracteur non chaotique, les exposants de Lyapunov sont tous inférieurs ou égaux à zéro et leur somme est négative. Un attracteur étrange possèdera toujours au moins trois exposants de Lyapunov, dont un au moins doit être positif (voir le tableau ci-dessous).

ETAT STABLE	Flot	Dimension de Lyapunov	Exposants de Lyapunov
Point d'équilibre	point	0	$\Lambda n \leq \ldots \leq \lambda 1 \leq 0$
Périodique	cercle	1	$\lambda 1 = 0$ $\lambda n \leq \ldots \leq \lambda 2 \leq 0$
Période d'ordre 2	tore	2	$\lambda 1 = \lambda 2 = 0$ $\lambda n \leq \ldots \leq \lambda 3 \leq 0$
Période d'ordre K	K-tores	k	$\Lambda 1 = \ldots = \lambda K = 0$ $\lambda n \leq \ldots \leq \lambda K+1 \leq 0$
Chaotique		Non entier	$\lambda_1 > 0$ $\sum_{i=1}^{n} \lambda_i < 0$
Hyperchaotique		Non entier	$\lambda_1 > 0,\ \lambda_2 > 0$ $\sum_{i=1}^{n} \lambda_i < 0$

Tab-4 Classification des régimes permanents selon les exposants de Lyapunov

1.3.2 Section de Poincaré

En mathématiques, dans la théorie des systèmes dynamiques, la section de Poincaré est l'intersection d'une trajectoire (périodique, quasi-périodique ou chaotique) dans l'espace d'au moins trois dimension, avec un hyperplan d'une dimension inférieure. Ainsi, nous observons le retour de la trajectoire vers l'hyperplan qui commence à un certain point de celle-ci l'ensemble des points marqués par la trajectoire sur l'hyperplan est appelé plan de Poincaré [6].

Considérons $x(x_0 , t_0 , t \mapsto \varphi_t (x_0)$ une solution d'un système autonome $\dot{x}=f(x)$

On définit localement un hyperplan $\Sigma \subset \mathbb{R}^n$ de dimension n − 1, transversal au champs de vecteurs f en x_0.

On suppose maintenant un point x au voisinage $V \subseteq \Sigma$ de x_0.

L'application de Poincaré $P: V \to \Sigma$ est alors définie par

$$x_1 = P(x) = \varphi_\tau(x) \tag{10}$$

où $\tau = \tau(x)$ est le temps après lequel la trajectoire retourne et intersecte Σ pour la première fois.

L'hyperplan Σ s'appelle alors "section de Poincaré". La section de Poincaré remplace le système dynamique en temps continu par un système en temps discret. C'est une visualisation par échantillonnage du système avec une paramétrisation qui doit être choisie convenablement pour accéder au maximum d'informations.

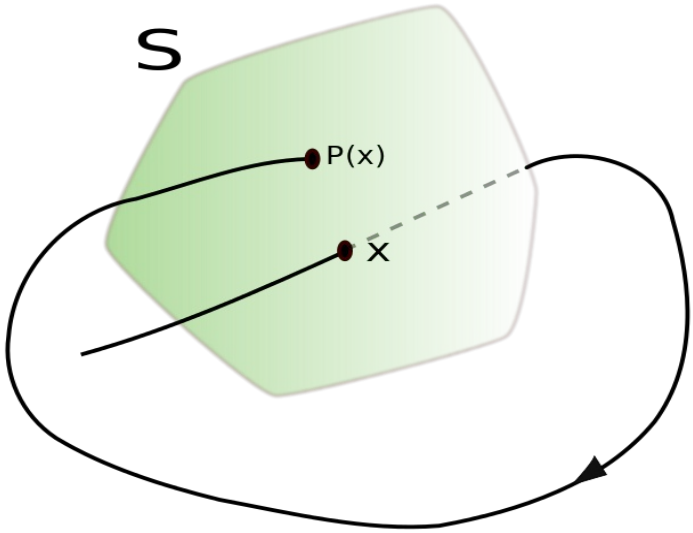


Fig-3 Projection par l'aplication de Poincaré du point x sur P(x) dans la section de Poincaré S

1.3.3 Notion d'attracteur

Dans l'étude des systèmes dynamiques, un attracteur (ou ensemble-limite) est un ensemble ou un espace vers lequel un système évolue de façon irréversible en l'absence de perturbations. Constituants de base de la théorie du chaos, cinq types d'attracteurs sont définis : ponctuel, ponctuel périodique, périodique, étrange, spatial.

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

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

Les systèmes à deux variables ne peuvent pas conduire à des mouvements chaotiques :

il suffit de rajouter une troisième variable pour que de tels systèmes, dans certaines conditions, deviennent instables. Sous-adjacent dans le chaos déterministe, cet objet particulier possède une structure fractale.

La figure 4 illustre l'attracteur chaotique du système de Rössler.

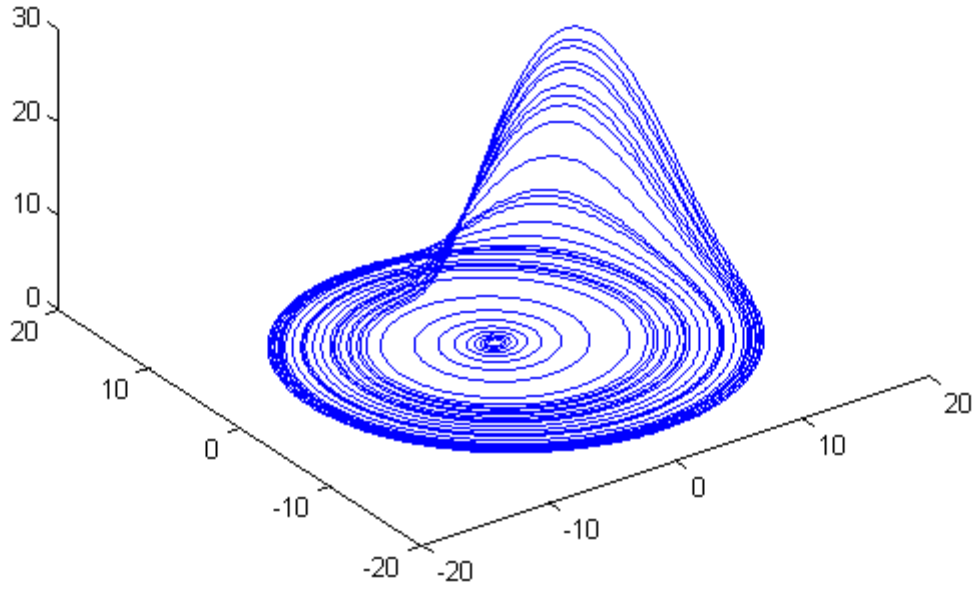


Fig-4 L'attracteur de Rössler

L'attracteur chaotique dit aussi étrange n'est pas une surface lisse, mais une surface repliée plusieurs fois sur elle-même. En effet, les trajectoires des points divergent (puisque, par définition deux point ne peuvent avoir la même évolution), mais comme l'attracteur a des dimensions finies, il doit se replier sur lui-même.

Le bassin d'attraction d'un attracteur est l'ensemble des points de l'espace des phases qui donnent une trajectoire évoluant vers l'attracteur considéré. On peut donc avoir plusieurs attracteurs dans un même espace des phases. Il existe deux types d'attracteurs: les attracteurs réguliers et les attracteurs étranges ou chaotiques.

L'objet géométrique observé dans la figure 4 est relativement complexe et dégage la richesse d'informations que contient le système. Un attracteur chaotique possède notamment la propriété remarquable suivante : la trajectoire ne repasse jamais par un même état. Ce qui signifie, entre autres, que cette trajectoire passe par une infinité d'états.

Il est à noter que pour observer les trajectoires d'un attracteur, il est parfois intéressant de réduire la dimension d de l'espace de phases.

La section de Poincaré est un hyperplan Σ de dimension d-1 qui transforme la trajectoire continue en une succession de points de passages discontinus à travers la section (figure 5).

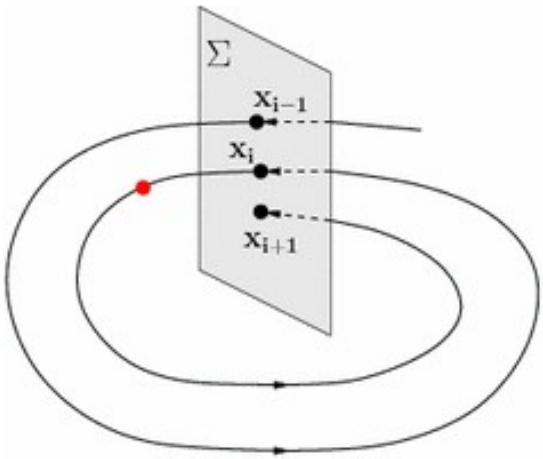


Fig-5 Section de Poincaré

a) Attracteur étrange

Un attracteur est dit étrange si il a une structure fractale. C'est souvent le cas lorsque la dynamique sur ce dernier est chaotique, mais aussi des attracteurs non chaotiques étranges existent. Le terme a été inventé par David Ruelle et Floris Takens pour décrire l'attracteur qui résulte d'une série de bifurcations d'un système décrivant l'écoulement dun fluide. Les attracteurs étranges sont souvent dérivables dans quelques directions, mais certains sont comme la poussière de Cantor, et donc pas dérivables. Les attracteurs étranges peuvent également être trouvés en présence du bruit, où ils peuvent être présentés à l'appui des mesures de probabilité aléatoire invariants de type de Sinaï-Ruelle-Bowen; voir Chekroun et al. (2011).
Exemples d'attracteurs étranges comprennent l'attracteur Double-scroll, Hénon attracteur, Rössler attracteur, Tamari attracteur, et l'attracteur de Lorenz.

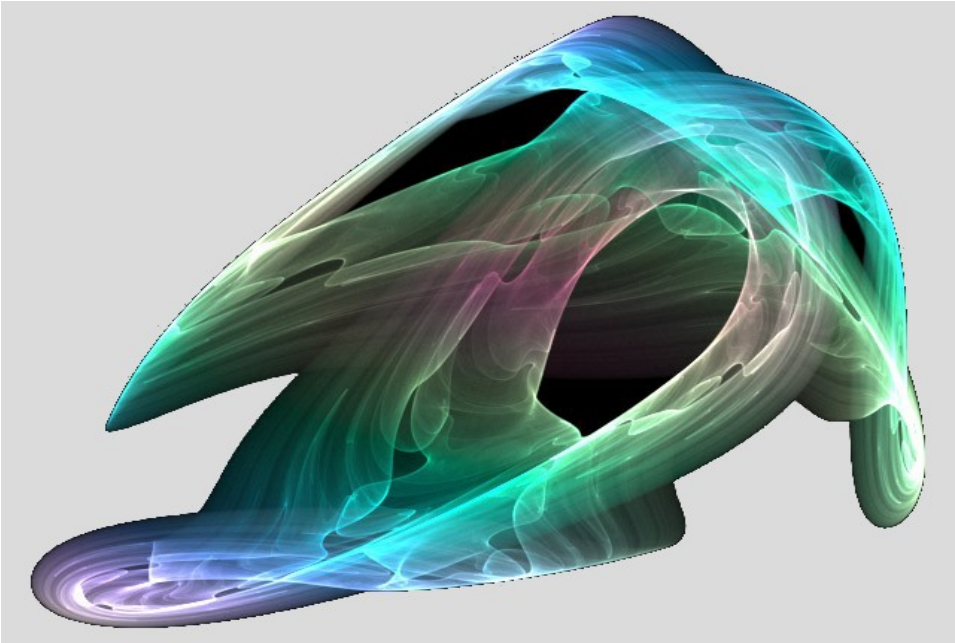


Fig-6 Représentation visuelle d'un attracteur étrange

b) Attracteur de Lorenz

En 1963, le météorologue Edward Lorenz est le premier à mettre en évidence le caractère vraisemblablement chaotique de la météorologie.
Le modèle de Lorenz, appelé aussi système dynamique de Lorenz ou oscillateur de Lorenz, est une modélisation simplifiée de phénomènes météorologiques basée sur la mécanique des fluides. L'oscillateur de Lorenz est un système dynamique tridimensionnel qui engendre un comportement chaotique dans certaines conditions.
Il s'agit d'un système dynamique non linéaire en temps continu de dimension 3, obtenu des équations de transfert de la chaleur dans un liquide. Le système de Lorenz est défini par :

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = x(b - z) - y \\ \dot{z} = xy - cz \end{cases} \tag{11}$$

avec (x, y, z) le vecteur d'état et a, b et c les paramètres du système.

L'attracteur de Lorenz est une structure fractale correspondant au comportement à long terme de l'oscillateur de Lorenz. L'attracteur montre comment les différentes variables du système dynamique évoluent dans le temps en une trajectoire non périodique.

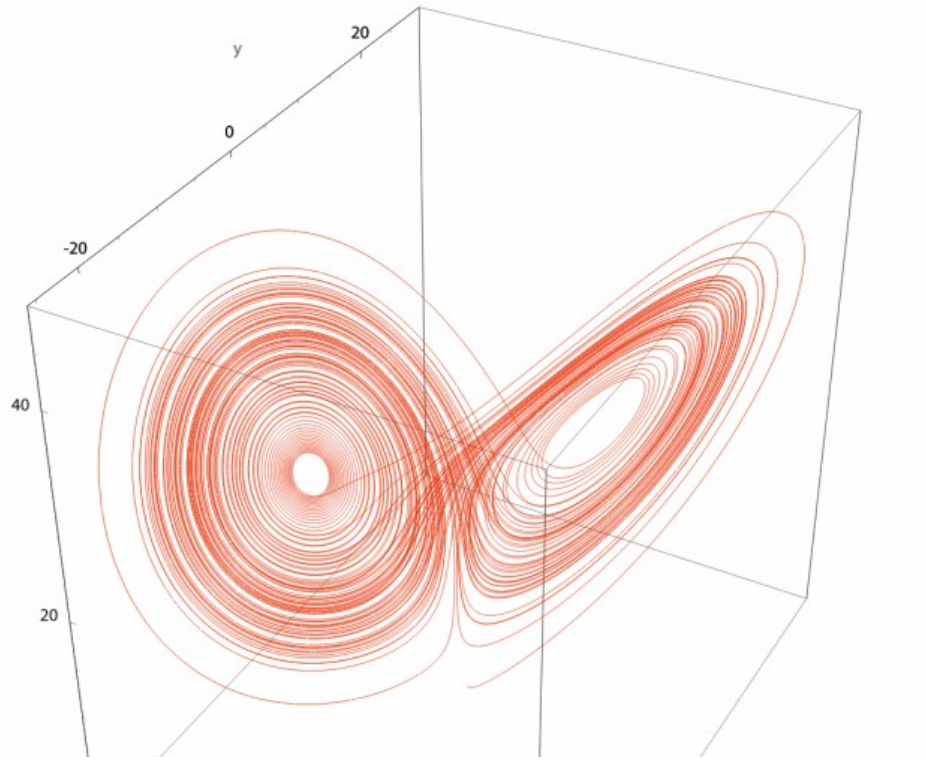


Fig-7 Attracteur de Lorenz

c) Attracteur de Hénon

L'attracteur de Hénon est un système dynamique à temps discret. C'est l'un des systèmes dynamiques ayant un comportement chaotique les plus étudiés.
L'attracteur de Hénon prend tout point du plan (x, y) et lui associe le nouveau point :

$$\begin{cases} x_{n+1} = y_n + 1 - a x_n^2 \\ y_{n+1} = b x_n \end{cases} \tag{12}$$

avec (x, y) le vecteur d'état et a, b les paramètres du système.
Le système de Hénon montre un comportement chaotique et génère un attracteur étrange pour a = 1.4, b = 0.3 avec x(0) = 0 et y(0) = 0 les conditions initiales du système.

Fig-8 Attracteur de Hénon

d) Attracteur de Rössler

Otto Rössler conçut son attracteur en 1976 dans un but purement théorique, mais ces équations s'avérèrent utiles dans la modélisation de l'équilibre dans les réactions chimiques.

L'attracteur de Rössler est l'attracteur associé au système dynamique de Rössler, un système de 3 équations différentielles non-linéaires.

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = x + ay \\ \dot{z} = b + z(x - c) \end{cases} \tag{13}$$

Avec: *a,b* et *c* étant 3 constantes positives.

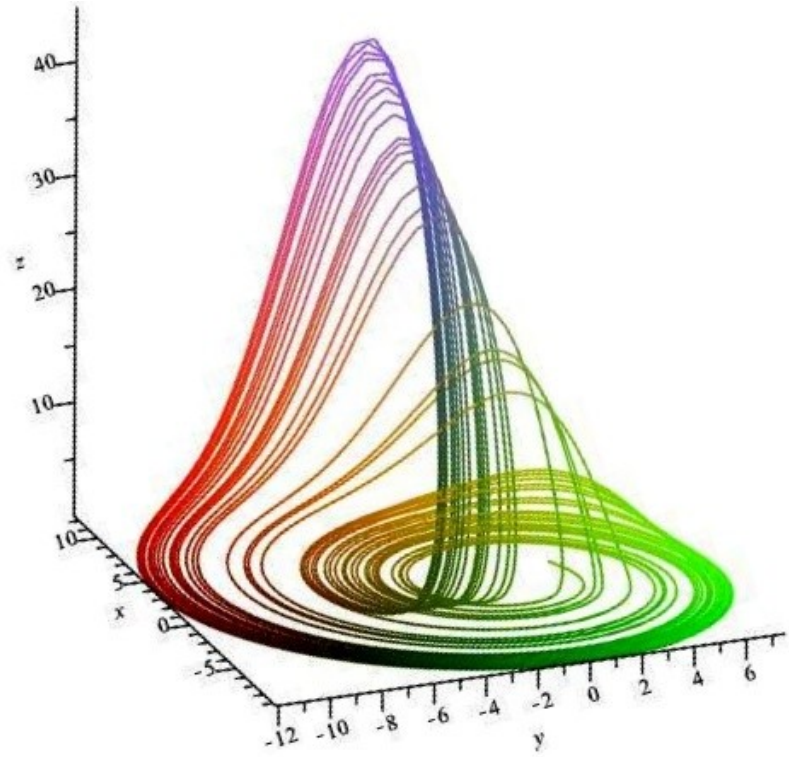


Fig-9 Attracteur de Rössler

1.4 Bifurcation ou la Route vers le chaos

A ce jour, on a distingué au moins trois routes ou transitions dans lesquelles un système non linéaire peut devenir chaotique si un paramètre de contrôle externe est varié. Toutes ces routes peuvent être vérifiées expérimentalement et montrent un comportement universel fascinant.

La route vers le chaos la plus récente a été trouvée par Grosmann et Thomae (1977), Feigenbaum (1978) et Coullett et Tresser (1978). Ils ont considéré une simple équation de différence utilisée par les biologistes pour décrire la dynamique d'une population dont le nombre varie avec le temps. Ils ont trouvé que, en variant un paramètre externe, l'état du système oscille entre des valeurs stables (points fixes) dont le nombre augmente pour certaines valeurs distinctes du paramètre externe. Ceci continue jusqu'au moment où le nombre de points fixes devient infini à une valeur finie et précise du paramètre externe, c'est à ce moment-là que le système devient chaotique.

Feigenbaum a montré dans un travail remarquable que ces résultats ne sont pas restreints à ce modèle spécial, mais sont universels, et peuvent être vérifiés pour une grande variété de systèmes biologiques, chimiques ou physiques.

Une deuxième transition vers le chaos, appelé la route d'intermittence, a été trouvée par Manneville et Pomeau (1979). Intermittence veut dire qu'un signal qui a un comportement régulier (laminaire) est interrompu par des périodes de comportement irrégulier statistiquement distribué (des éclats intermittents). Le nombre moyen de ces éclats augmentent en variant un paramètre de contrôle externe jusqu'à ce que le système devienne complètement chaotique.

La troisième possibilité a été trouvée par Ruelle et Takens (1971) et Newhouse (1978).

Ils ont trouvé une transition vers la turbulence qui est différente de celle proposée par Landau (1944, 1959), qui a considéré les turbulences dans le temps comme la limite d'une séquence infinie d'instabilité (Bifurcation de Hopf), chacune créant une nouvelle fréquence de base.

Cependant, Ruelle, Takens, et Newhouse ont montré qu'après deux instabilités seulement, la trajectoire rejoint au niveau de la troisième étape un attracteur chaotique et ainsi le système devient turbulent [7].

Comme exemple de la bifurcation, on prend l'équation de récurrence du premier ordre :

$$x_n = f_a(x_{n-1}) = x_{n-1}^2 + a \qquad (14)$$

Cette famille de fonctions est appelée les fonctions quadratiques. Le paramètre externe à varier est le constant a. L'équation admet un simple point d'équilibre à x=0 quand a=0. Pour a>0 cette équation n'admet aucun point d'équilibre, car fa(x)>0 quelque soit x, cependant pour a<0 cette équation admet deux états d'équilibres. Ainsi, une bifurcation a lieu quand le paramètre a varié en passant par la valeur 0. La figure I-3 montre clairement ce phénomène, cette figure a été réalisée sous Scilab où les 5000 itérations sur la trajectoire de la fonction fa ont été calculées en partant du point initial x0=0. Le même calcul est répété pour plusieurs valeurs de a dans l'intervalle [0,-2], on remarque les différents points de bifurcation et finalement la transition vers le chaos [8].

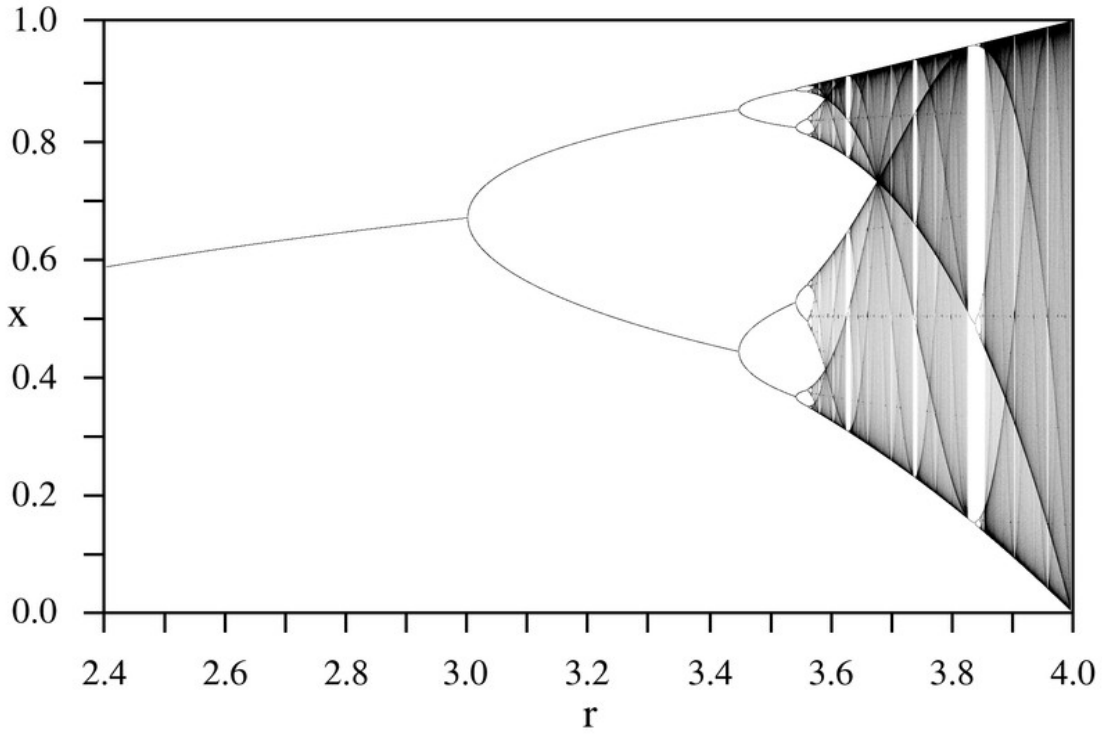


Fig-10 Bifurcation vers le chaos par doublement de période

1.5 Où est le chaos ?

Après Lorenz, beaucoup d'études ont démontré l'existence de diverses sources de chaos.

Un très grand nombre de recherches actuelles sur le chaos, essaient soit d'exploiter les sources déjà trouvées, soit explorent d'autres sources pas encore maîtrisées.

1.5.1 Le chaos dans les systèmes inertes

Observons une cascade qui plonge des hauteurs d'une falaise pour former un torrent en contre-bas. Près des berges couvertes de mousses, au détour d'un méandre on observe un courant régulier, traversé ci et là par de petites ondes ou des structures imbriquées plus complexes. Près des rochers on observe des turbulences, un exemple particulier de phénomène où règne un régime chaotique. On observe ainsi que le même système physique peut présenter à la fois un comportement simple et complexe.

1.5.2 Les systèmes vivants

Les méthodes récentes de la dynamique non linéaire ont permis de mieux comprendre le comportement de nos organes, en particulier du coeur et du cerveau.

a) Le Coeur

On a découvert que l'activité cardiaque n'est pas régulière et présente un comportement chaotique. En effet son rythme est sensible aux conditions initiales et à la dimension fractale de son attracteur qui est basé sur la dynamique cardiaque. On a découvert que plus le coeur bat régulièrement par exemple moins il est capable de s'adapter. C'est dans ces conditions que survient la crise cardiaque.
Le chaos cardiaque présente une dimension fractale élevée, de l'ordre de 3.25, ce qui signifie que nous avons besoin d'au moins 4 variables pour décrire ce système. L'étude de la dimension fractale des cas pathologiques permet donc aux spécialistes de savoir si la personne a déjà eu un infarctus. Mais en présence de certaines pathologies cardiaques, la dimension fractale peut également diminuer et le rythme peut se régulariser, d'où l'intérêt de comparer la dimension fractale du système au rythme cardiaque.

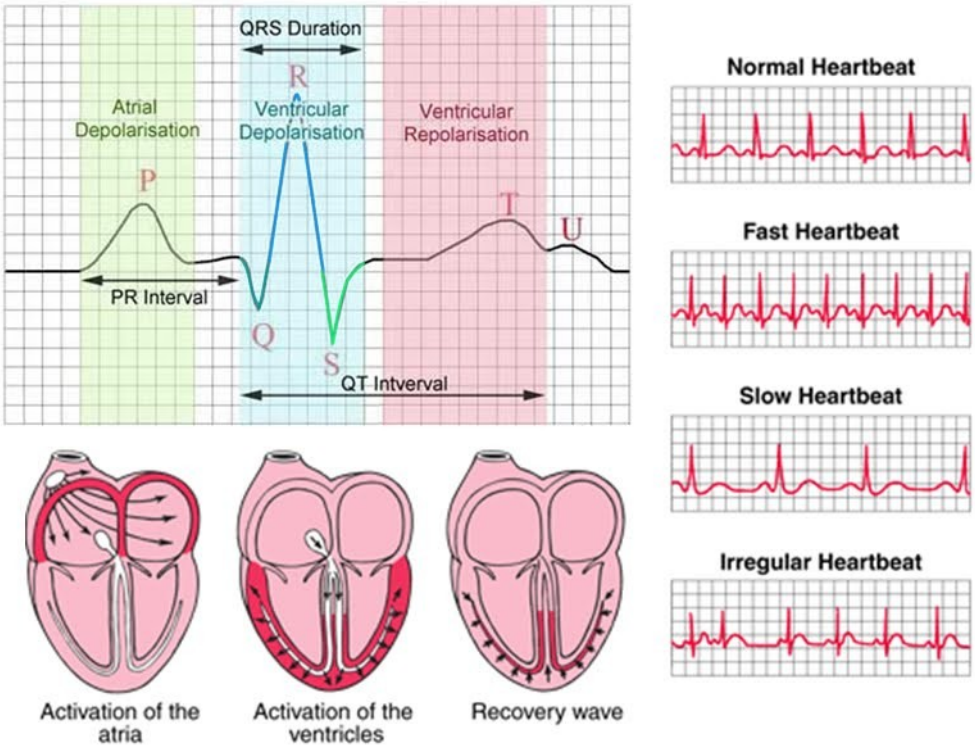


Fig-13 Le signal ECG

b) Le Cerveau

L'activité neuronale du cortex semble également relever du chaos. Cela ne signifie pas que le cerveau est le siège d'un désordre total, mais bien au contraire qu'il dépend d'un système d'organisation très complexe sensible aux conditions initiales.

Ceci explique pourquoi le cerveau comme le coeur sont capables de s'adapter très rapidement aux circonstances ou de changer rapidement d'état. Les modèles dynamiques du cerveau, ce que l'on appelle les systèmes informatiques neuronaux sont aujourd'hui étudiés avec la plus grande attention et ce n'est que tout récemment que les chercheurs ont démontré que le chaos joue un rôle dans l'organisation du cerveau.

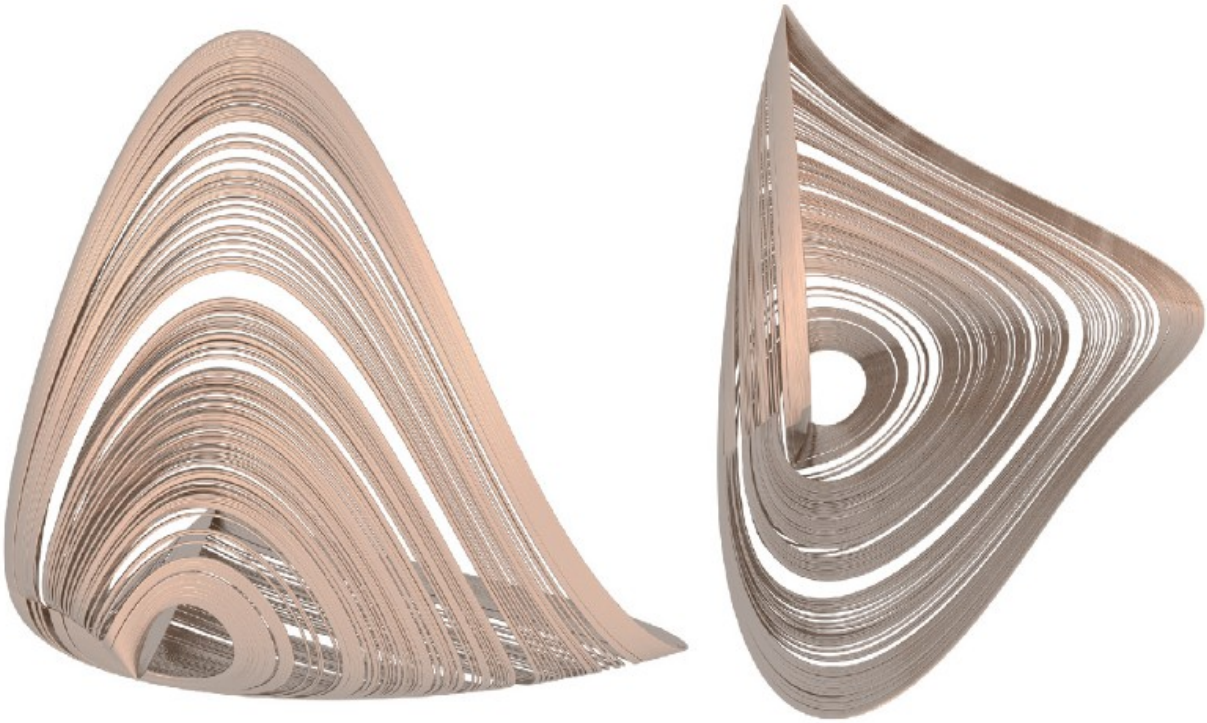


Fig-14 Attracteur d-un model de cerveau (activité électrique)

1.5.3 Le chaos dans la communication sécurisée

Ces deux dernières décennies ont été marquées par une tendance partagée à l'exploration des possibilités du cryptage des transmissions par le chaos. Ces possibilités ont été la suite logique de la découverte de la synchronisation des systèmes chaotiques en 1989 [9].

En effet, Pecora a trouvé qu'un système chaotique peut être construit d'une certaine façon pour que ces parties évoluent harmonieusement dans le temps. Cependant, on sait que deux systèmes chaotiques complètement isolés ne peuvent pas se synchroniser, à cause de leurs sensibilités aux erreurs, même insignifiantes. Alors, un genre de couplage doit être introduit entre les systèmes à synchroniser.

Pecora a proposé un exemple illustré par la figure 11, où un système chaotique et un duplicata d'une partie du système sont synchronisés.

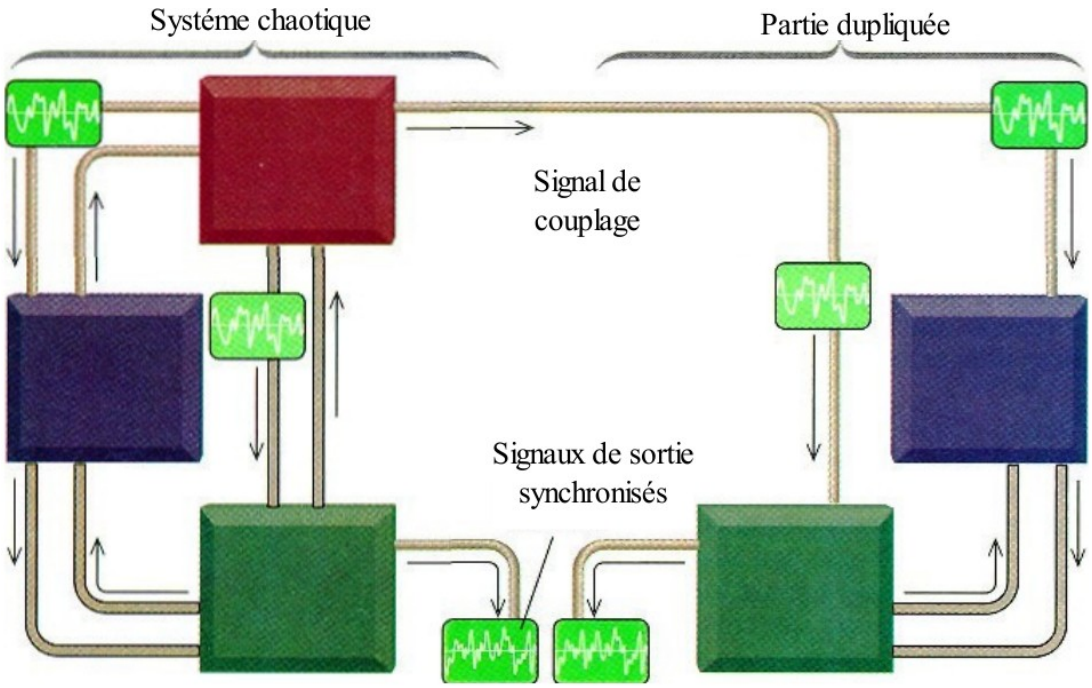


Fig-11 Synchronisation dans le système de Pecora [9]

Le concept important dans cet exemple est le fait que la partie dupliquée (carrés vert et bleu) est stable lorsqu'elle est pilotée par la partie non dupliquée (carré rouge). Ainsi, des variations dans les conditions initiales de la partie dupliquée n'auront pas de conséquences vis-à-vis du signal de sortie. Alors, le système global est chaotique et les deux sorties sont synchrones.

Dans ce cas, le couplage est effectué par la liaison entre le carré rouge et la partie dupliquée à droite.

Pour simuler cette idée, Pecora a choisi le système de Lorenz (11), où l'une des trois variables d'états a été utilisée comme signal de couplage, et la dynamique des deux restantes comme la partie dupliquée.

Ainsi, malgré que les deux parties aient été initialisées différemment, elles ont fini par se rattraper en harmonie totale. Ce type de synchronisation est dite unidirectionnelle, car le système est considéré comme la source et la partie dupliquée est considérée comme la destination. Par la suite Carroll a proposé un système de communication crypté basé sur l'exemple de Pecora et illustré par la figure 12.

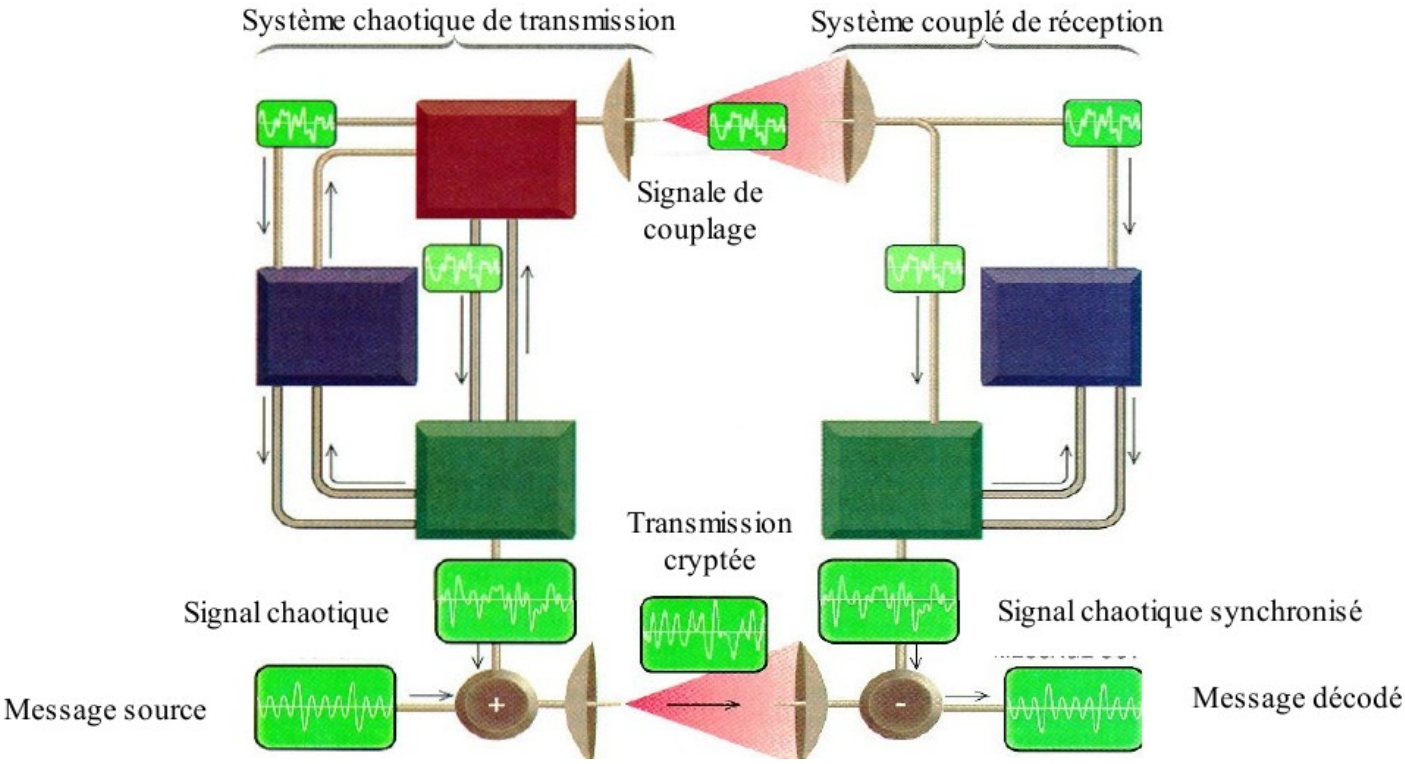


Fig-12 Communicationchaotique par le systèmede Pecora et Carroll [9]

Le transmetteur ajoute un signal chaotique au message à transmettre et envoie le résultat en plus du signal de couplage au récepteur. Ce dernier est composé d'une partie dupliquée du système de transmission, alors le signal chaotique est régénéré et retranché du signal reçu pour avoir le message original.
Depuis, Pecora et Carroll ont introduit d'autres exemples basés sur des principes différents. Les axes de ces recherches sont principalement la synchronisation, le cryptage et la cryptanalyse.

1.6 Conclusion

Dans ce présent chapitre, nous avons vus quelques définitions, notions et quelques caracteristiques sur les systèmes chaotiques parmi lesquelles:

• Le chaos est le résultat d'un processus déterministe.

• Il apparaît dans les systèmes non linéaires.

• La trajectoire ou la forme observée apparaît principalement désordonnée et aléatoire.

• Le chaos apparaît dans les systèmes bouclés; où les évènements passés

influencent sensiblement les évènements présents.

• Pour certaines conditions ou paramètres fixes, le chaos est auto- générateur, dans le sens où des variations de variables externes (ex. un bruit) ne sont pas nécessaires.

• Le chaos n'est pas le résultat d'incertitude, telles les erreurs de mesure ou d'échantillonnage.

• Les variables du système sont bornées. Ces bornes sont illustrées dans l'espace de phase par l'attracteur borné.

• Le comportement d'un système chaotique est hypersensible aux changements des conditions initiales.

• Les prédictions de long terme sont inutiles; par contre, les prédictions de court terme peuvent être relativement précises.

• Le spectre de Fournier des signaux chaotiques est dispersé (principalement un bruit non corrélé) mais avec des pics (périodicités) qui se manifestent de temps à autre.

• La trajectoire dans l'espace de phase peut avoir des propriétés fractales.

Le prochain chapitre se portera sur la synchronisation et le cryptage ainsi que leurs differentes méthodes.

CHAPITRE 2

SYNCHRONISATION DES SYSTÈMES CHAOTIQUES

2.1 Introduction

Á ce jour, différentes formes de synchronisation ont été explorées. Parmi ces formes on trouve les méthodes à synchronisation complète, les méthodes à synchronisation généralisée et les méthodes à synchronisation de phase.

Dans la synchronisation complète, nous avons une coïncidence complète entre les variables d'états des deux systèmes synchronisés. Les méthodes à synchronisation complète sont typiquement associées avec la synchronisation des systèmes identiques, dont nous avons déjà illustré un exemple (système de Pecora et Carroll). D'autres exemples de synchronisation complète utilisent un schéma à rétroaction et sont décrits comme étant bidirectionnels, car les deux systèmes sont à la fois source et destination.

Les méthodes à synchronisation généralisée se manifestent par une relation fonctionnelle entre deux systèmes chaotiques couplés. Ces méthodes sont considérées comme une généralisation des méthodes à synchronisation complète pour synchroniser des systèmes chaotiques typiquement différents [20].

Dans la synchronisation de phase, la phase entre deux oscillateurs chaotiques est verrouillée, ou, plus généralement, une définition particulière adéquate d'une représentation de la phase de deux systèmes chaotiques est verrouillée. Ces méthodes peuvent être utilisées avec des systèmes identiques ou pas [19].

Dans tous les cas de figure, une attention particulière doit être donnée au choix de couplage [20].

Une classification moins récente, mais plus détaillée peut être trouvée dans [21], où parmi les méthodes énumérées, on trouve la synchronisation hyper – chaotique, qui décrit les méthodes utilisées pour synchroniser deux systèmes caractérisés par plus d'un exposant de Lyapunov positif (ex. la concaténation de plusieurs systèmes chaotiques).

On y retrouve [21] également les méthodes de synchronisation élaborées comme solution à un problème de synthèse d'observateur. Ce type de problème est classique dans le domaine de l'automatique, et utilise beaucoup des résultats relatifs au contrôle du chaos.

Récemment, des méthodes novatrices de cette classe ont exploré les systèmes discrets et hybrides, soit comme systèmes à synchroniser [18] soit comme partie de la méthode de synchronisation [22]. Finalement, on trouve dans [23] une proposition d'une méthode efficace pour la quantification de la synchronisation, en d'autres termes c'est une méthode d'évaluation de la qualité et la sensibilité des méthodes de synchronisation.

2.2 Concept Et Methodes De Synchronisation

La synchronisation repose sur le fait qu'un système chaotique est déterministe et possède un ou plusieurs exposants de Lyapunov positifs et qu'il est instable. Il est donc possible de construire une réplique identique à ce système et d'essayer de synchroniser de façon que les deux signaux chaotiques issus des deux exemplaires soient identiques.
Deux classes de synchronisation exsistent, suivant la manière avec laquelle les deux systèmes chaotiques sont couplés, on a la synchronisation unidirectionnelle et la synchronisation bidirectionnelle.

2.2.1 Synchronisation Unidirectionnelle

Dans le cas d'une synchronisation unidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément fonctionnant dans un seul sens, par exemple l'utilisation d'un circuit électrique suiveur [13].

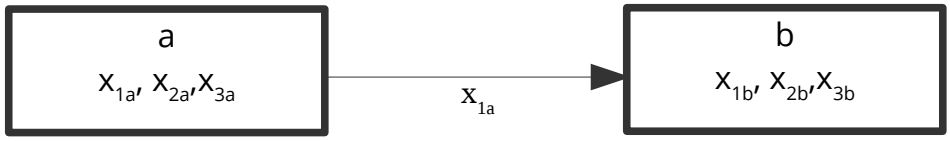


Fig-13 Couplage unidirenctionnel

2.2.2 Synchronisation Bidirectionnelle

Dans le cas d'une synchronisation bidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément permettant l'échange d'énergie dans les deux sens, par exemple l'utilisation d'une simple résistance [13].

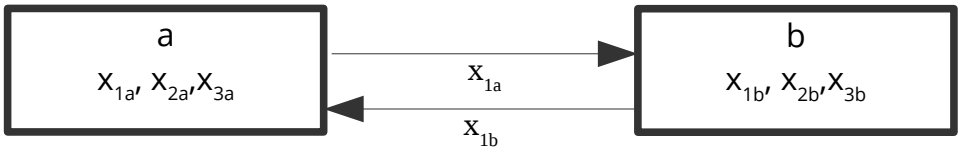


Fig-14 Couplage bidirenctionnel

2.3 Methodes De Synchronisation

2.3.1 Synchronisation Par Décomposition Du Systeme (caroll)

Certains sous-systèmes non-linéaires chaotiques peuvent être synchronisés en les reliant entre eux avec des signaux communs [14], donc on peut les décomposer en deux sous-systèmes maître et esclave. En 1990, Pecora et Carroll ont proposés un système chaotique

$$\dot{x}=f(x) \tag{15}$$

avec une sortie $y=h(x)$ est décomposé en deux sous-systèmes dont les états sont x_1 et x_2 respectivement

$$\dot{x}_1=f_1(x_1,x_2) \tag{16}$$

$$\dot{x}_2=f_2(x_2,y) \tag{17}$$

avec

$$x=\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

Le système est partitionné de façon à ce que les Exposants de Lyapunov Conditionnels [14] du sous-système (17) soient negatifs.

Les Exposants de Lyapunov Conditionnels caractérisent la stabilité de (17). Si tous les exosants sont négatifs, la trajectoire $x_2(t)$ est asymptotiquement stable [14]. Ce qui signifie que les états de plusieurs copies du sous-système (17) se synchroniseront à l'aide du même signal y(t).

On considère le système suivant

$$\dot{\hat{x}}_2 = f_2(\hat{x}_2, y) \tag{18}$$

Si les exposants conditionnels de ce système sont tous négatifs et $\dot{\hat{x}}_2(0)$ est suffisamment proche de $x_2(0)$, alors l'état $\hat{x}_2$ converge asymptotiquement vers x_2, *i.e :*

$$\lim_{t\to\infty} \|x_2 - \hat{x}_2\| = 0$$

la figure suivante résume le principe de Pecora et Carroll

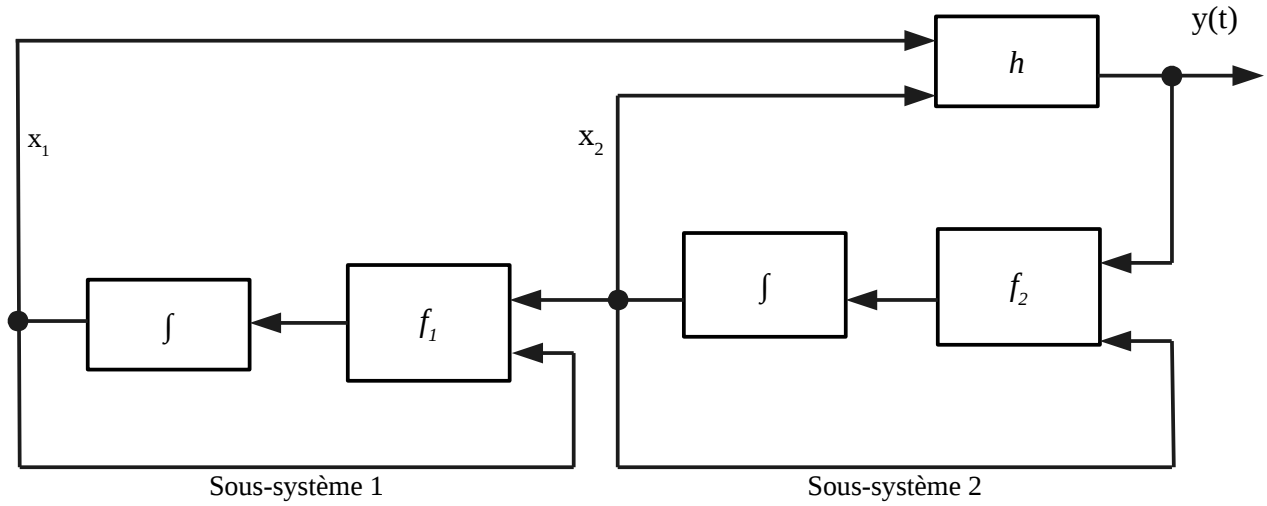


Fig-15 Synchronisation maître-esclave (Pecora et Carroll)

2.3.2 Synchronisation identique

Connue aussi sous le nom de synchronisation complète (Boccaletti et al. 2002), c'est la forme la plus simple de synchronisation [15].
Plusieurs procédés permettant la synchronisation existent, en contraste avec le couplage utilisé, ces procédés peuvent etre différent [15].
D'où il faut distinguer entre le coulage unidirectionnel et biderectionnel. L'étude de la synchronisation du chaos est souvent faite pour des systèmes sous la forme

$$\frac{dX}{dt} = F(X) + kN(X - Y) \qquad (19)$$
$$\frac{dY}{dt} = G(y) + kM(X - Y)$$

avec

$F \, et \, G \in \mathbb{R}^n, X \, et \, Y \in (\mathbb{R}^n)^2$, M et N matrices de couplage dans $\mathbb{R}^{n \, x n}$

si F=G, alors le deux sous-systèmes X et Y sont identiques.
Si les deux matrices differe de zero, le couplage est bidirectionnel, si une des deux matrices est égale a zéro alors le couplage est unidirectionnel.

2.3.3 Synchronisation par Boucle Fermée

La synchronisation des systèmes chaotiques par les méthodes en boucle ouverte implique une sensibilité aux variations paramétriques. Pour y remédier, de nouvelles techniques basées sur un bouclage par contre-réaction ont été proposées. L'idée est d'appliquer une correction au système en fonction de l'erreur entre le signal transmis par le premier système et le signal régénéré par l'autre. Cette erreur est ainsi injectée en contre-réaction d'où l'appellation de l'approche.
Cette technique permet également la synchronisation entre des paires différentes de systèmes chaotiques. [16]

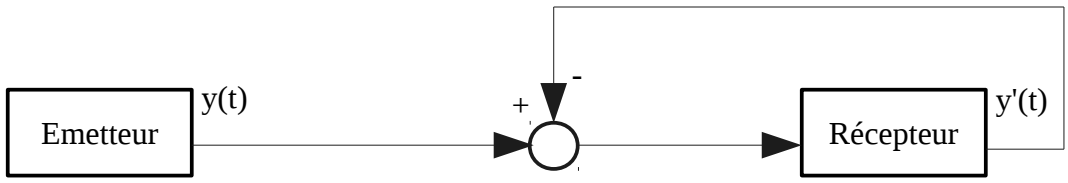


Fig-16 Synchronisation par boucle fermée

2.3.4 Synchronisation de Phases

La synchronisation de phase se produit lorsque les oscillateurs chaotiques couplés conservent leur différence de phase, tandis que leurs amplitudes délimitée restent non corrélés. Ce phénomène se produit même si les oscillateurs ne sont pas identiques. L'observation de la synchronisation de phase nécessite une définition précédente de la phase d'un oscillateur chaotique. Dans de nombreux cas pratiques, il est possible de trouver un plan dans l'espace de phase dans lequel la projection de la trajectoire de l'oscillateur suit une rotation autour d'un centre bien défini. Si tel est le cas, la phase est définie par l'angle, φ(t), décrit par le segment reliant le centre de rotation et la projection du point de trajectoire sur le plan. Dans d'autres cas, il est toujours possible de définir une phase à l'aide de techniques fournies par la théorie du traitement du signal, telles que la transformée de Hilbert. Dans tous les cas, si $\varphi_1(t)$ et $\varphi_2(t)$ désignent les phases des deux oscillateurs couplés, la synchronisation de phase est donnée par la relation $n\varphi_1(t)=n\varphi_2(t)$ avec m et n des nombres entiers.

2.3.5 Synchronisation retardée

La synchronisation de phase se produit lorsque des oscillateurs chaotiques non identiques sont faiblement couplés: les phases sont verrouillés, tandis que les amplitudes restent non corrélées. [15]

Lorsque la force du couplage devient plus importante, certains rapports entre les amplitudes peuvent être établies. En effet, il a été montré (Rosenblum et al.1997), dans les oscillateurs non identiques de façon symétrique et couplés dans les systèmes temporisés, qu'il existe un régime de synchronisation retardée. Ce processus apparaît comme une coïncidence des états décalés dans le temps de deux systèmes:

$$\lim_{t \to +\infty} \left\| Y(t) - X(t-\tau) \right\| \tag{20}$$

où X(t) est l'état du système emetteur et Y(t) est l'état du système recepteur et τ un retard positif.

2.3.6 Synchronisation projective

Dans cette méthode, l'état du système récepteur se synchronise avec un multiple de l'état du système émetteur. Soit a et τ tels que :

$$\lim_{t \to +\infty} \left\| X'(t) - aX(t-\tau) \right\| \tag{21}$$

où a est le facteur d'échelle, X(t) est l'état du système émetteur, X'(t) est l'état du système récepteur et τ est un retard positif.
Cette approche est utilisée pour des systèmes partiellement linéaires et permet de synchroniser à un facteur près les états qui ne peuvent être synchronisés [16].

2.3.7 Synchronisation Impulsive

Les équations differentielles impulsives [Samoilenko & Perestyuk,1995] décrivent le procédé d'évolution qui, à certains moments, changent leurs états par des sauts. Ce type de comportement peut etre trouvé dans plusieurs

domaines tels que la chemie, la biologie, l'économie...etc [17]

Considerons le système suivante

$$\dot{x}=f(t,x) \tag{22}$$

avec

$f:\mathbb{R}_+\times\mathbb{R}^n\to\mathbb{R}^n$ continue, $x\in\mathbb{R}^n$ variable détat

considerons une suite de temps discret {τ} avec

$0 < \tau_1 < \tau_2 < .. < \tau_i < \tau_{i+1} < ..$

avec $\tau\to\infty$ et $i\to\infty$

Soit

$$U(i,x)=\Delta x\big|_{t=\tau_i}=x(\tau^+_i)-x(\tau_i) \tag{23}$$

le saut de la variable d'état à l'instant τ_i, alors, le système impulsif est défini par

$$\begin{cases}\dot{x}=f(t,x) & t\neq\tau_i\\ \Delta x=U(i,x) & t=\tau_i\\ x(t_0)=x_0, t_0\geq 0, i=1,2,..\end{cases} \tag{24}$$

cete dernière est appelée équation differetielle impulsive [Lakshmikantham et al.,1989].

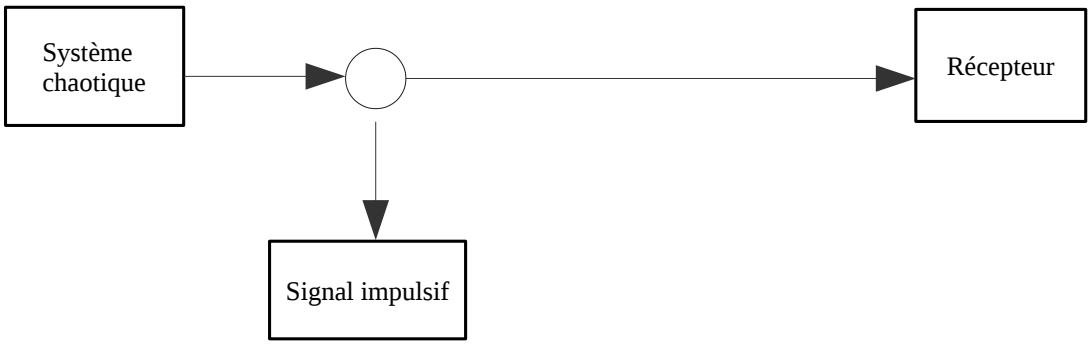


Fig-17 Synchronisation Impulsive

2.4 Transmission basée sur la synchronisation de systèmes chaotiques

En transmission sécurisée d'information binaire, le message appelé "texte" est transformé de manière à le rendre incompréhensible. Ce processus est appelé "chiffrement" ou "cryptage". Par ailleurs, le destinataire doit engager un processus, appelé "déchiffrement" ou "décryptage", pour reconstruire le message à partir du texte chiffré. Pour cela, des algorithmes sont utilisées, qui sont en effet des fonctions mathématiques destinées au chiffrement et déchiffrement du message. Afin de transmettre le message d'une manière sûre, un élément appelé "clé" de cryptage est introduit, qui est utilisé par l'expéditeur et le destinataire. Cette clé peut prendre des valeurs parmi un grand nombre de valeurs possibles. Certains algorithmes utilisent des clés différentes pour le chiffrement et le déchiffrement. Avec ces algorithmes, toute la sécurité réside dans la (les) clé(s) et non pas dans l'algorithme. Alors un espion, même s'il connaît l'algorithme, ne peut pas détecter le message s'il ne connaît pas la clé.

On distingue deux types de clés : clé "secrète" et clé "publique". Dans un algorithme à clé secrète, la clé de chiffrement est calculée à partir de la clé de déchiffrement et vice-versa. Dans la plupart des cas, les deux clés sont identiques, l'expéditeur et le destinataire se mettent d'accord sur une clé avant d'échanger des messages. Ainsi, si cette clé secrète est dévoilée, n'importe qui peut lire le message.

Un algorithme à clé publique utilise des clés différentes au niveau du chiffrement et du déchiffrement. De plus, ces clés ne peuvent pas être calculées l'une à partir de l'autre.

Ainsi, la clé de chiffrement peut être rendue publique, mais seul celui qui possède la clé de déchiffrement peut lire le message. La clé de déchiffrement est alors appelée clé "privée".

Des recherches ont été effectuées afin de pouvoir appliquer les méthodes de cryptographie aux informations continues. Grâce aux résultats obtenus en synchronisation des systèmes chaotiques, il a été possible d'employer des signaux chaotiques continus comme porteur d'informations.

Dans ce cas, le message est codé par l'émetteur et il est décodé et extrait du signal chaotique par le récepteur. Parmi les méthodes de transmission chaotiques, on peut citer le cryptage par addition, le cryptage par commutation, le cryptage par modulation, le cryptage par inclusion.[13]

2.5 Techniques De Cryptage Par Le Chaos

Le cryptage proprement dit, ou comment mélanger et séparer les données et le signal chaotique, est l'étape finale pour construire le système de communication chaotique. Un signal chaotique porteur d'information représente une généralisation des systèmes conventionnels de modulation. Ainsi, un message source à faible amplitude est masqué par un signal chaotique plus large.
Cependant, contrairement aux porteuses sinusoïdales conventionnelles, et à cause de l'absence de notions précises d'amplitude, de phase et de fréquence; le signal chaotique est mélangé avec le message source de différentes façons. Principalement deux classes de méthodes existent: le cryptage additif et le cryptage par inclusion.

2.5.1 Cryptage par addition (additive chaos masking scheme)

La première et la plus simple des méthodes de cryptage, illustrée dans la figure 18, developpé en 1993 [24]. Elle consiste en deux systèmes chaotiques identiques, l'émetteur et le récepteur.Le signal chaotique c(t) est l'une des variables d'état du système dans l'émetteur. Le message d'information (le signal utile qui doit être crypté) m(t), qui est typiquement très faible devant c(t), est ajouté au signal c(t) et donne le signal transmis s(t). Comme c(t) est très complexe et m(t) est beaucoup plus petit que c(t), alors il est difficile de séparer m(t) du signal s(t) sans connaître c(t).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. Au niveau du récepteur, après synchronisation grâce au signal reçu, on récupère le message original par une simple soustraction.

Par conséquent, un intrus ne soupçonnera pas qu'un message est transmis, même s'il intercepte le signal y(t) (porteuse chaotique plus le message), donc il ne cherchera pas à appliquer des techniques de décryptage

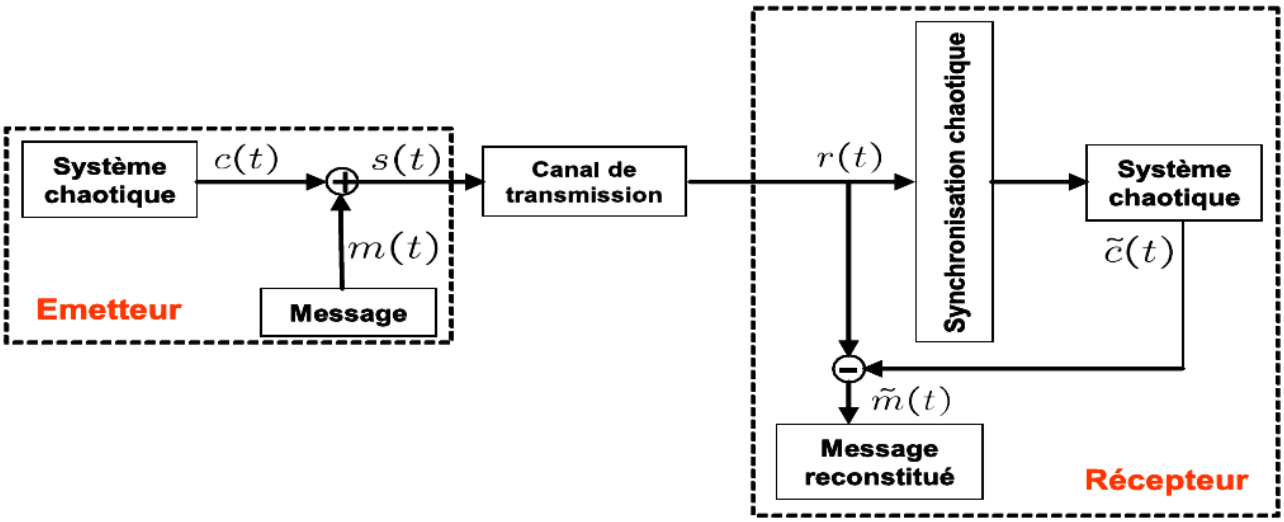


Fig-18 Cryptage par addition

2.5.2 Cryptage par commutation (Chaotic Shift Keying, CSK)

Appelé aussi cryptage par décalage, est une technique réservée aux message numériques. Dans le schéma de communication, illustré dans la figure 19, le message d'information est utilisé pour commuter le signal transmis entre deux attracteurs chaotiques statistiquement similaires, qui sont utilisés respectivement pour coder le bit 0 et le bit 1 du message d'information numérique.

Ces deux attracteurs sont générés par deux systèmes chaotiques de même structure et de paramètres différents. A la réception, le signal reçu est utilisé pour produire un système chaotique identique à ceux de l'émetteur. Le message d'information est restitué par application d'un filtre passe-bas et ensuite un

seuillage de l'erreur de synchronisation e(t). [24]

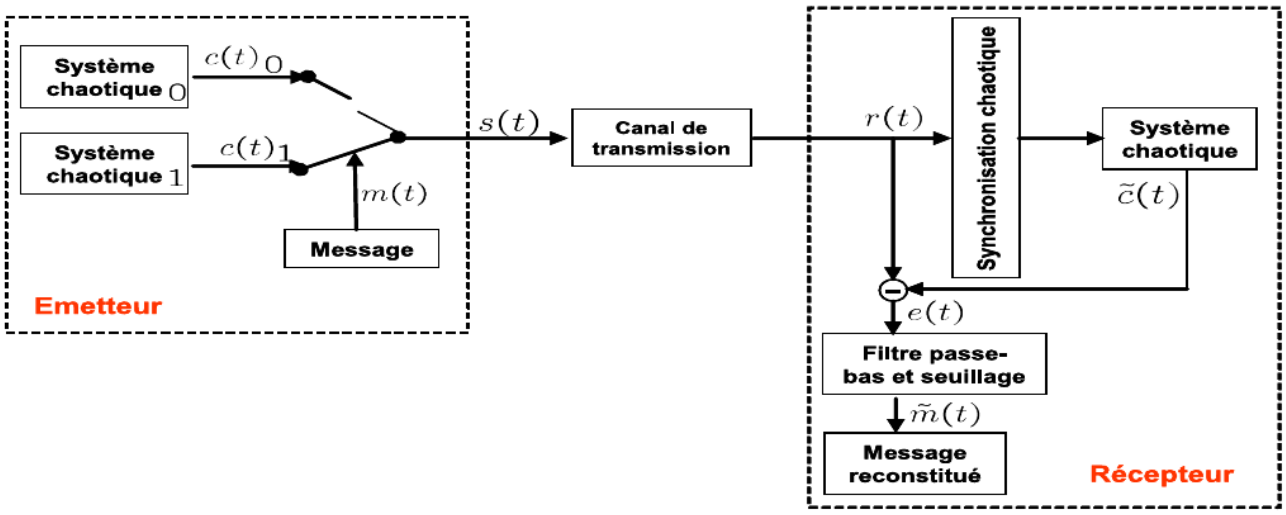


Fig-19 Cryptage CSK

2.5.3 Cryptage Par Modulation

Différent au cryptage par addition et commutation, dans un schéma de modulation chaotique le message m (t) est injecté dans le système émetteur de telle sorte que sa dynamique est modifiée par le message en continu.

Dans ce cas, généralement un contrôleur adaptatif (qui peut aussi être considéré comme un système dynamique supplémentaire bidirectionnelle couplée avec le système de l'emetteur) est ajouté au système esclave selon une règle telle que sa sortie m'(t) converge asymptotiquement à m (t). Pour suivre la dynamique du système maître, la sortie du contrôleur (c-à-d. m (t)) doit être injecté dans le système l'esclave de la même manière que dans le système maître. La figure 20 illustre la structure de base d'un système de modulation chaotique typique. À noter que dans certains systèmes de modulation chaotique il peut n'y avoir aucun retour de s (t) dans le système maître. [25]

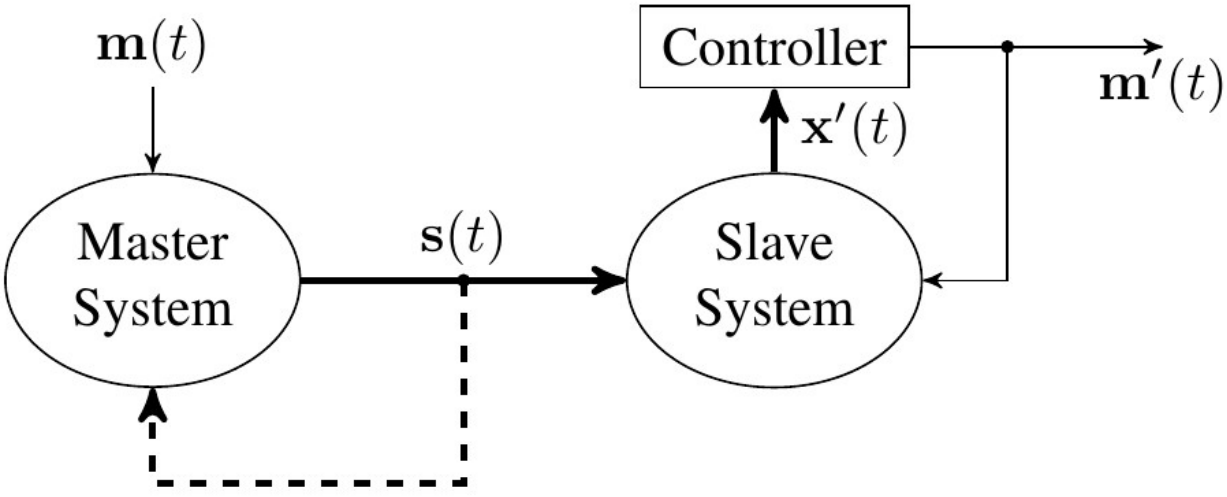


Fig-20 Cryptage par modulation

Il éxiste deux types de cryptage par modulation :

- Modulation de paramètre, où le signal m(t) module la valeur de un ou plusieurs paramètres de contrôl

-Modulation directe, où le signal m(t) est injecté dans une ou plusieurs variables du système maître sans changer aucune valeur des paramètre de contrôl.

Comparé au cryptage par addition, la modulation du chaos peut récuper de manière très fidèle le message trasmis si certaines conditions sont satisfaites. Comme étant le cryptage CSK est utilisé seulement pour les signaux numériques, la modulation a une meilleur performance que le CSK. Le cryptage par modulation peut transmettre, si bien conçu, plusieurs messages. Il faut moduler *n* parametres de contrôl du système maître avec *n* signaux de message. Un serieux desavantage du cryptage par modulation est que le contrôleur depend de la structure des systèmes maître et esclave, ce qui signifie qu'il faut concevoir different contrôleurs pour differents systèmes maître, et aussi, il se peut qu'il n'existe pas de contrôleurs certains systèmes à cause de défauts dans les systèmes maître/esclave. [25]

2.5.4 Cryptage Par Inclusion

Dans le cryptage par inclusion, le message source est inclus dans la structure du système chaotique du côté de l'émission. Dans ce cas, un observateur doit être utilisé à la réception pour récupérer le message original. Cette classe de méthodes nécessite un seul canal de transmission. [26]

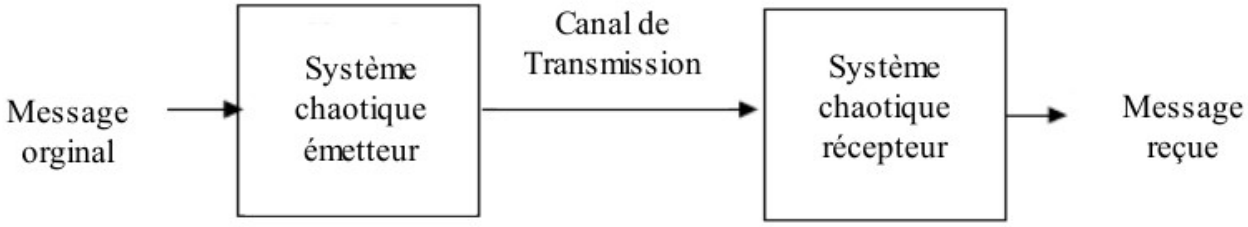


Fig-21 Cryptage par inclusion

Un exemple intéressant sur la méthode d'inclusion serait le CSK (Chaos Shift Keying) représenté par la figure 19 où les symboles du message binaire à transmettre sont utilisés pour la commutation entre deux systèmes chaotiques différents. À la réception le démodulateur qui est en fait un observateur d'états discrets (observateur hybride) est utilisé pour reconstruire le message original. Un tel observateur peut être représenté par la figure 22

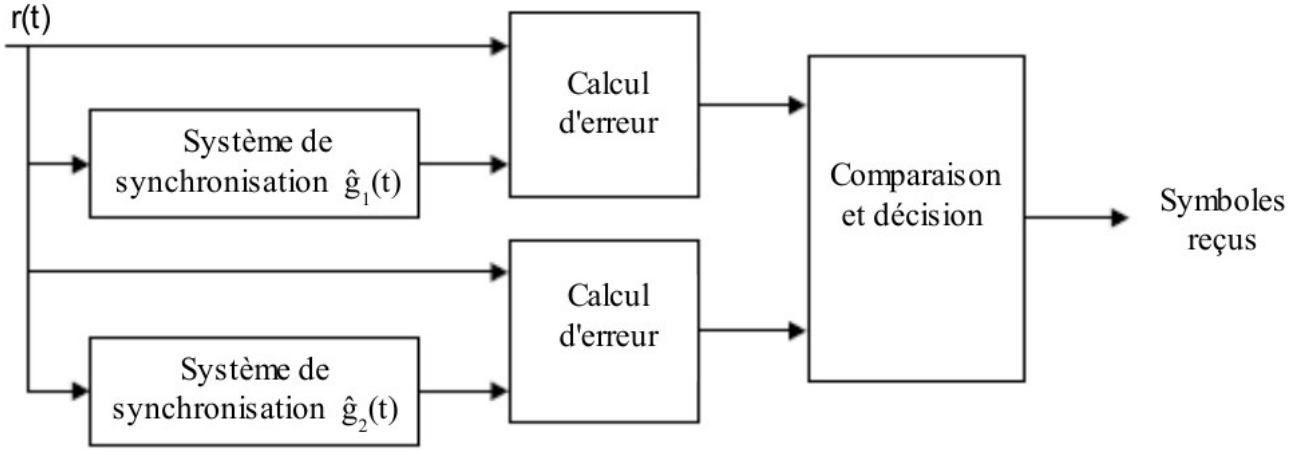


Fig-22 Bloc de démodulation dans la méthode CSK

2.5.5 Cryptage Mixte

Afin de faire face aux problèmes de sécurité des méthodes précédentes, une nouvelle technique combinant les principes de la cryptographie standard et la synchronisation chaotique a été proposée. Le message u(t) contenant l'information est crypté grâce à une clé, c(t), générée par l'émetteur chaotique.
Le message crypté est alors injecté dans la dynamique du système chaotique, pour la rendre plus complexe. Ensuite, un signal y(t) fonction des variables d'état de l'émetteur est transmis au récepteur, qui établit une synchronisation avec l'émetteur. La clé est alors reconstruite par le récepteur, qui peut finalement décoder le message. Le principe général de cette méthode est illustré par la figure 23. [16]

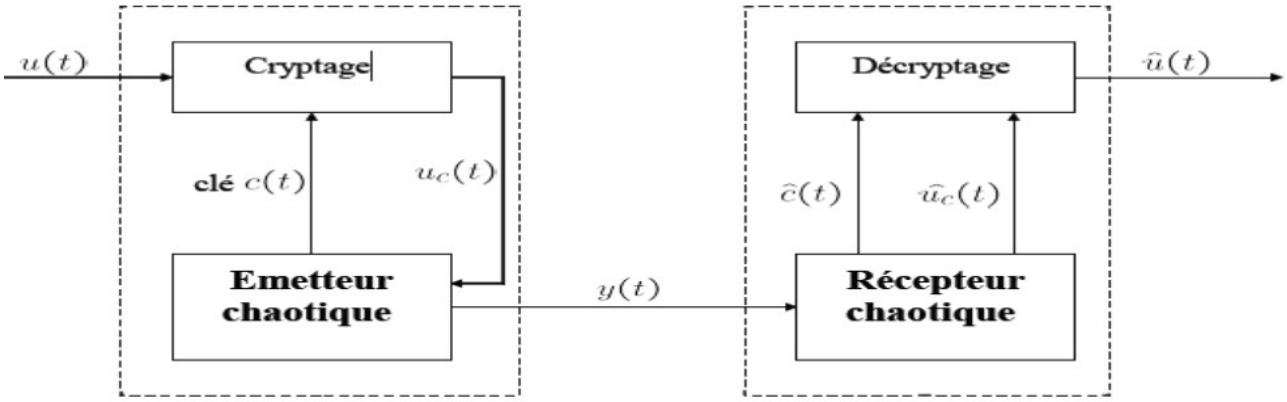


Fig-23 Cryptage mixte

2.6 Transmission Par Deux Voies

Pour cette technique, les deux étapes, synchronisation et cryptage, sont indépendantes. En effet, deux lignes de transmission sont utilisées. La première sert à synchroniser l'émetteur et le récepteur, tandis que la deuxième est utilisée pour le cryptage.
En gros, ce nouveau schéma de communication est composé de trois étapes :

1- cryptage

2- synchronisation

3- décryptage

Dans la première étape, une fonction fortement non linéaire Φ est utilisée pour crypter simultanément le message confidentiel s(t) et l'état chaotique x(t).
Le signal crypté s c(t) est ensuite envoyé à travers un canal de transmission vers le récepteur.
Dans la deuxième étape, un signal chaotique y = h(x) est transmis via un deuxième canal de transmission séparé du premier. Ce signal y est utilisé seulement pour la synchronisation, et ne contient aucune information du message s(t). Dans la troisième et la dernière étape, l'estimé z(t) de l'état x(t), généré par le récepteur chaotique (construit par le processus de la synchronisation) et la fonction de décryptage Ψ sont utilisés pour reproduire l'estimé approximatif sd(t) du message confidentiel s(t). Une description systématique de cette procédure est illustrée par la figure 24. Pour un exemple de fonctions Φ et Ψ. [24]

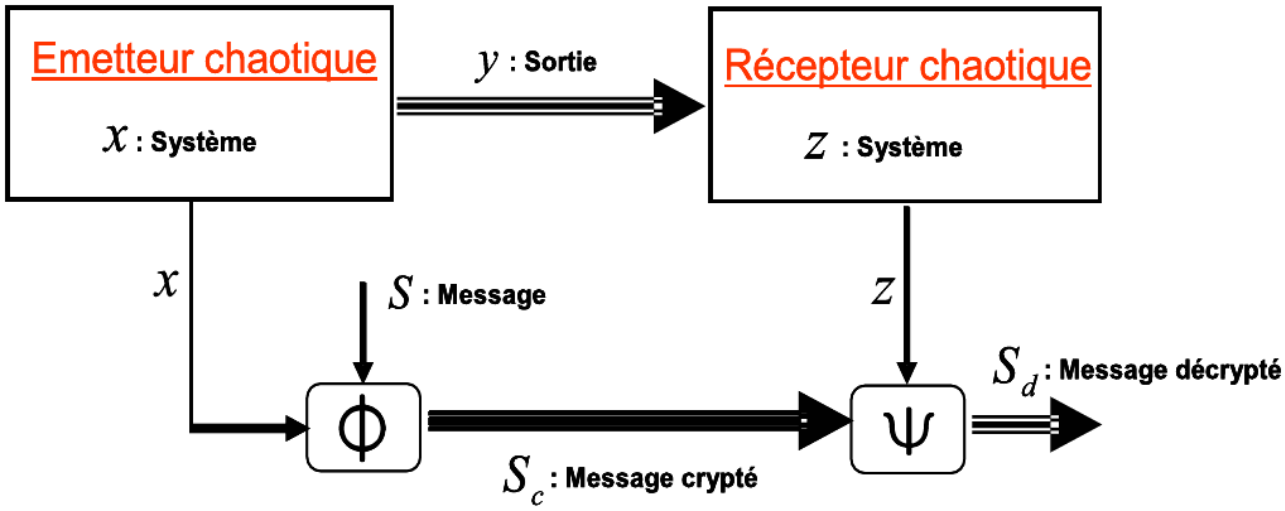


Fig-24 Communication à deux lignes de transmission

2.7 La cryptanalyse

La cryptanalyse ou l'attaque du système de cryptage est une étape importante, mai parfois délaissée, elle permet d'évaluer le niveau de sécurité apporté par la méthode proposée.

Par conséquent, après l'élaboration d'une méthode de synchronisation et de cryptage chaotique, toutes les méthodes d'attaque applicables doivent être explorées suivant différents scénarios. Car généralement, on ne s'aperçoit d'une brèche de sécurité qu'après la catastrophe. Ainsi, ironiquement le constructeur (ou l'utilisateur) d'un système de cryptage doit être le premier à le casser.

Pratiquement, casser un cryptage revient à l'extraction du message source sans avoir une connaissance préalable sur le schéma du récepteur, ou au moins avec une connaissance partielle de ce dernier. Généralement, l'intrus doit disposer d'au moins deux versions (crypté et en clair) d'un message pour pouvoir commencer l'attaque. Également, des statistiques linguistiques sont généralement utilisées pour associer les symboles en clair avec leurs versions cryptées. C'est ce point qui a sollicité l'intérêt des systèmes chaotiques dans le cryptage. En effet, le signal chaotique crypté associé à un symbole en clair à un instant donné coïncidera rarement avec le même symbole en d'autres instants.

Là aussi, un potentiel majeur existe pour les méthodes de reconnaissance de chaos. Car le fait même de pouvoir détecter (ou distinguer) qu'une transmission cryptée par le chaos est établie constitue une base importante de critique et de comparaison, entre les différentes méthodes de cryptages.

2.8 Conclusion

Dans ce chapitre, nous venons de voir le principe de synchronisation des systèmes chaotiques ainsi que les differentes méthodes utilisées pour la sysnchronisation.

Ce travail est très important pour le troisième et quatrième chapitre où il sera procédé à la simulation sur ordinateur puis la réalisation pratique d'une

comminication basée sur le chaos.

La cryptographie permet d'avoir une « couche » supplementaire de sécurité (mis à part qu'un système chaotique est plus ou moins difficile à déchiffrer) pour prevenir le signal transmis détre lus et decrypté par une personne/organisme autre que celui auquel le message crypté est destiné.

CHAPITRE 3

SIMULATION D'UN SYSTÈME CHAOTIQUE

3.1 Introduction

Suite aux progrès considérables ralisés dans les dernières décennies, la sécurité dans l'échange de l'information est devenu plus qu'une nécessité. Dans ce context, la cryptographie joue un rôle majeur car l'information est généralement transportée dans des canaux publiques.

L'objectif d'utiliser la cryptographie est de « cacher » l'information transmise à travers des canaux non sécurisés, en d'autres termes, assurer une confidentialité et une protection des données transmises. Malgré la diversité des techniques de cryptage, on trouve deux classes distinguées : La cryptographie symétrique et la cryptographie asymétrique, ou cryptographie à clé publique.

Le chaos est l'une des dynamiques les plus complexes pouvant présenter les systèmes non-linéaires. Les signaux générés par les systèmes chaotiques ont des propriétés statistiques similaires à l'aléatoire en dépit d'être déterministe. De ce fait, les systèmes chaotiques ont été utilisés pour une communication sécurisée et plusieurs systèmes de cryptages basés sur le chaos ont été proposés à fin de cacher l'information parmis lesquels : le masquage par addition, CSK, cryptage par inclusion...etc. [27]

La plupart des schémas de communication se composent de deux parties : un générateur de chaos, appelé émetteur, et un système de réponse, appelé récepteur.

Dans le crypytage symmetrique, le décryptage de l'information necessite une synchronisation entre l'émetteur et le récepteur. Pour parvenir à la synchronisation, la sortie de l'emetteur doit être envoyée au récepteur.

L'utilisation d'oscillateurs est requise pour générer un signal chaotique. Plusieurs types d'oscillateurs éxistent. Ces derniers diffèrent par leur structures, la technologie impliquée ainsi que les composants utilisés dans leurs création. Les oscillateurs les plus répandus sont le circuit de chua (choisi pour la suite de ce chapitre) et le Colpitts, ce dernier se caracterisant par la simplicité de sa structure, comportant une non-linéarité intrinsèque liée à la caractéristique exponentielle du transistor. [16]

3.2 Le circuit de Chua

3.2.1 Présentation du circuit de Chua

Un circuit électronique doit respecter certaines conditions pour montrer un comportement chaotique, appelés critères chaotiques. Il doit contenir :

- Un élément non linéaire ou plus.
- Une résistance localement active ou plus.
- Trois éléments de stockage d'énergie ou plus.

En 1983, l'ingénieur Leon Ong Chua a mis au point le plus simple circuit électronique respectant ces critères. Il comporte deux condensateurs, une bobine, une résistance active et une diode de Chua.

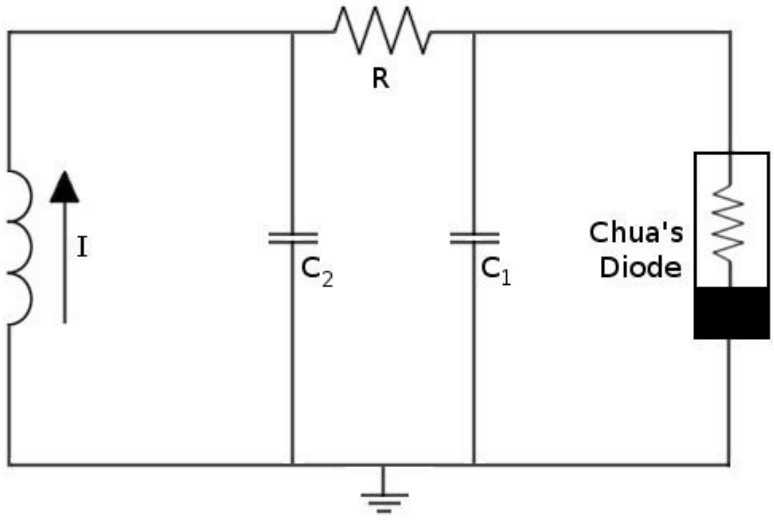


Fig-26 Circuit de Chua

La presence d'un attracteur chaotique dans ce circuit de 3ème ordre, a été présenté pour la premiere fois par T. Matsumoto [29] en utilisant des simulation par ordinateur.

La dynamique du circuit est définie par les équations suivantes :

$$\begin{cases} C_1\dot{V}_1 = \dfrac{V_2 - V_1}{R} - f(V_1) \\ C_2\dot{V}_2 = \dfrac{V_1 - V_2}{R} + i \\ L\dot{i} = -V_2 \end{cases} \quad (25)$$

avec V_1,V_2:la tension aux bornes des capacités C_1 et C_2 respectivement, i le courant travesant l'inductance et f : la réponse en courant de la diode de chua

3.2.2 La Diode De Chua

La diode de Chua représente l'élément non linéaire du circuit. C'est une résistance active non-linéaire qui peut être décrite par des équation linéaires, c'est la partie la plus essentielle du circuit de Chua et un circuit oscillateur très simple qui exhibe des oscillations chaotiques et est ainsi vastement utilisé comme un exmple de systèmes chaotiques.

La diode de Chua n'est pas comercialisée et est géneralement construite en utilisant des composants électroniques standards tels que: diodes, capacités, résistances et amplificateurs opérationnels. [30]
La diode de Chua (résistance non-linéaire) possède une caractéristique voltage/courant non-linéaire [31] régie par la fonction f(V_1) de l'équation (25)

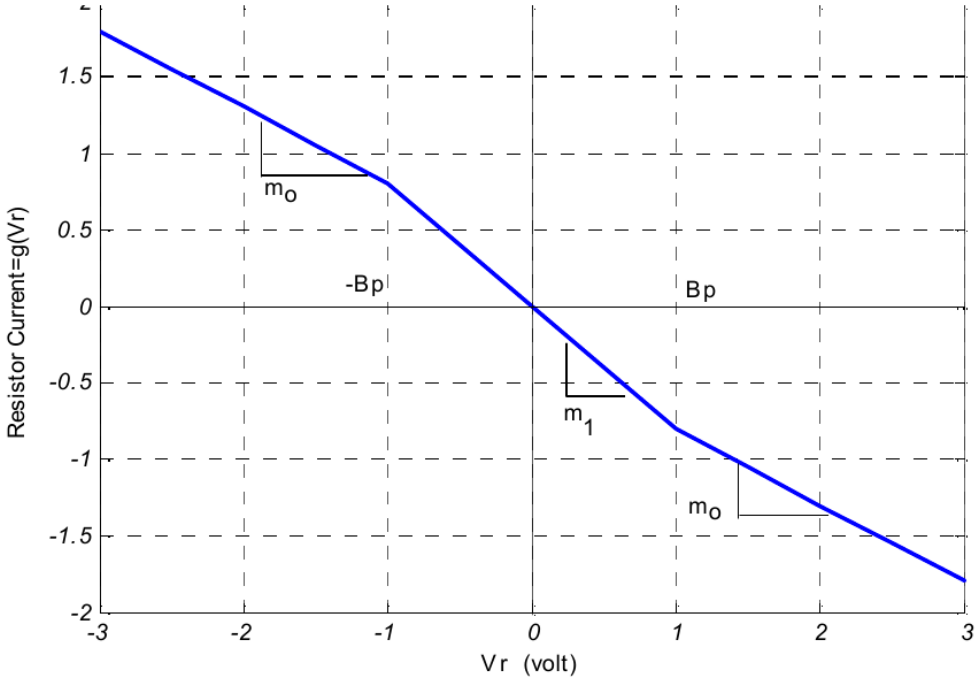


Fig-27 Caractéristique de la résistance non-linéaire de Chua

L'équation f(V_1) est définie par :

$$f(V_1)=m_0V_1+\frac{1}{2}(m_1-m_0)|V_1+B_p|+\frac{1}{2}(m_0-m_1)|V_1-B_p| \quad (26)$$

avec :

m_0,m_1: tangentes interieur et exterieure respectivement

$\pm B_p$ points de ruputre

3.2.3 Etude de la bifurcation

En appliquant les lois de Kirchhoff dans le circuit de Chua que nous avons réalisé, nous obtenons le système d'équations (25). Mais ces équation sont difficile à maipuler pour une analyse théorique ou numérique, alors il est procédé à la normalisation de ces dernières et les écrire sous une forme sans dimension.

D'où les changement de variables à effectuer sont :

$x=\frac{V_1}{B_p}$, $y=\frac{V_2}{B_p}$ et $z=\frac{iR}{B_p}$

Le système devient alors :

$$\begin{cases} \frac{dx}{d\tau}=\alpha(y-x-f_n(x)) \\ \frac{dy}{d\tau}=x-y+z \\ \frac{dz}{d\tau}=-\beta y \end{cases} \quad (27)$$

avec $f_n(x)=bx+\frac{1}{2}[(a+b)(|x+1|-|x-1|)]$ et $\tau=\frac{t}{RC_2}$

où $\begin{cases} \alpha=\frac{C_2}{C_1} \\ \beta=\frac{R^2C^2}{L} \end{cases}$ et $\begin{cases} a=Rm_1 \\ b=Rm_0 \end{cases}$

La fonction $f_n(x)$ est decrite par les parametres a et b qui allouent ses tangentes et le point de rupture normalisé B_p=1 lié à l'amplitude du signal et est arbitrairement choisie pour agrandir/rétrécir l'attracteur. [32]

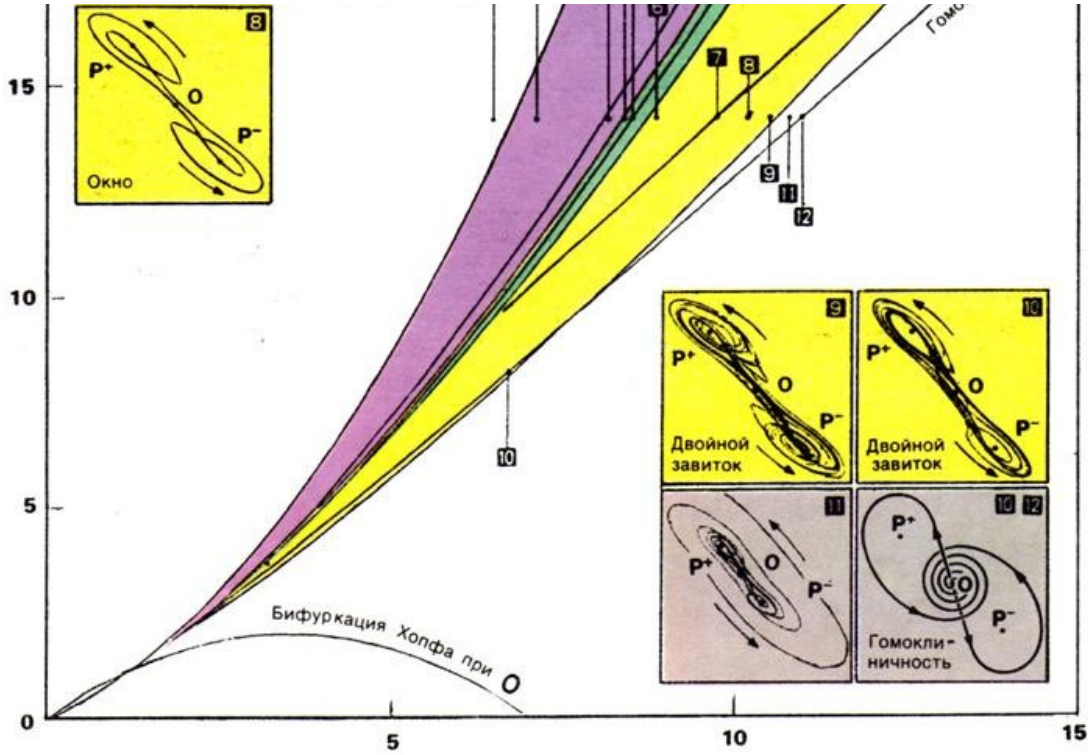


Fig-28 Diagramme de bifurcation1 du système d'équation normalisé du circuit de Chua [33]

La figure 28 nous montre le comportement du système en fonction des paramètres α et β. Ces deux paramètres sont dépendants des valeurs des composants du système. Si nous choisissons α et β dans la zone superieur gauche, le système va converger vers un point. Dans la zone violette, le système sera périodique autour d'un point. Dans la zone verte on a un attracteur chaotique similaire à celui de Rössler. La zone jaune nous amène à un système qui oscille autour de deux points et finalement, la zone inferieur droite est un cycle limite stable. Nous souhaitons nous trouver dans la zone rose foncé, qui nous permettra d'avoir un système qui oscille entre deux points. En effet, il s'agit du comportement typique d'un circuit de Chua. On choisissons donc le couple

$$\begin{cases}\alpha=10\\ \beta=14\end{cases}$$ [34]

D'après ce diagramme il est possible de déduire les valeurs des composants C_1, C_2, R et L

$$\begin{cases} \alpha = \dfrac{C_2}{C_1} = 10 \\ \beta = \dfrac{R^2 C_2}{L} = 14 \end{cases} \Rightarrow \begin{cases} C_2 = 10\,C_1 \\ R^2 C_2 = 14\,L \end{cases}$$

Si on prend $a = Rm_1 \approx 1.27\, et\, Rm_0 \approx 0.68$ qui sont souvent utilisés pour modéliser l'élément non linéaire, alors on trouve que C_1=10nF, C_2=100nF, R=1.6kΩ et L=18.2mH satisfairont approximativement la condition necessaire pour avoir un double attracteur.

3.3 Simulation sous Matlab/Simulink

Pour simuler le comportement du circuit de Chua, on utilise un logiciel d'analyse numérique tel que : Scilab, GNU Ocatve, Matlab...

Ayant aquis quelque notions de base sur Matlab, on va essayer de simuler le comportement du circuit Chua en utilisant Simulink de Matlab, pour cela on va utiliser les équations (27) et non pas

(26) pour les raisons sus-cités et on aura le système illustré dans la figure 29

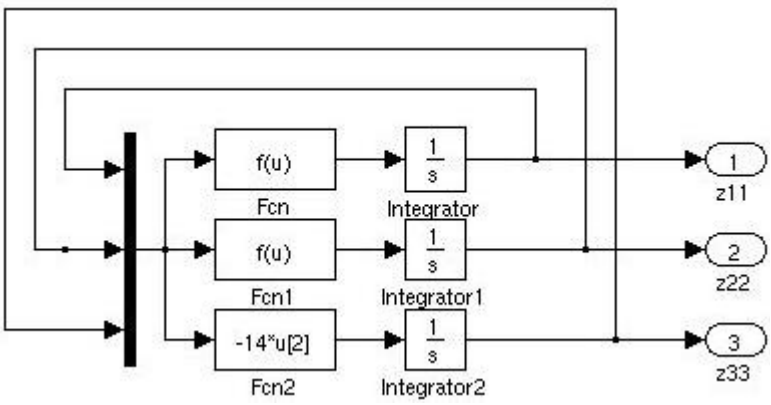


Fig-29 Représentation des équations de Chua dans Simulink

Après avoir introduit les équations dans les block adequats dans le sous-sytème illustré dans l'image ci-dessus, on obtient la representation du circuit de chua dans le sytème illustré dans la figure 30 ci-dessous.

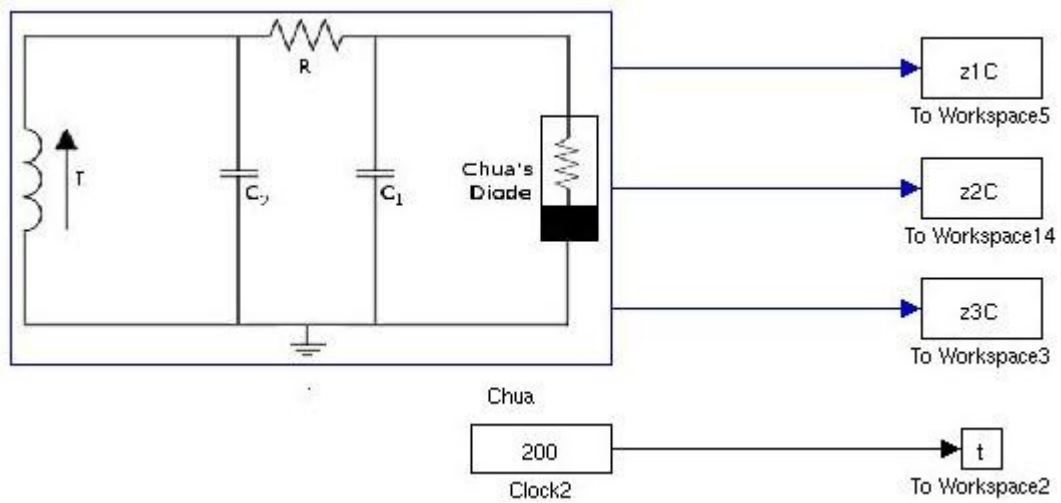


Fig-30 Modèlisation du circuit de chua dans Simulink

Le système ci-dessus est configuré pour être simuler pendant une periode de 200 secondes (voir illustration) et cela afin de voir si on parviens à avoir le fameux double attracteur qui caractérise le circuit de chua.

La figure 31 nous montre bel et bien un double attracteur, ce qui signifie que les équations (27) representent un circuit de chua et qu'il presente un aspect chaotique.

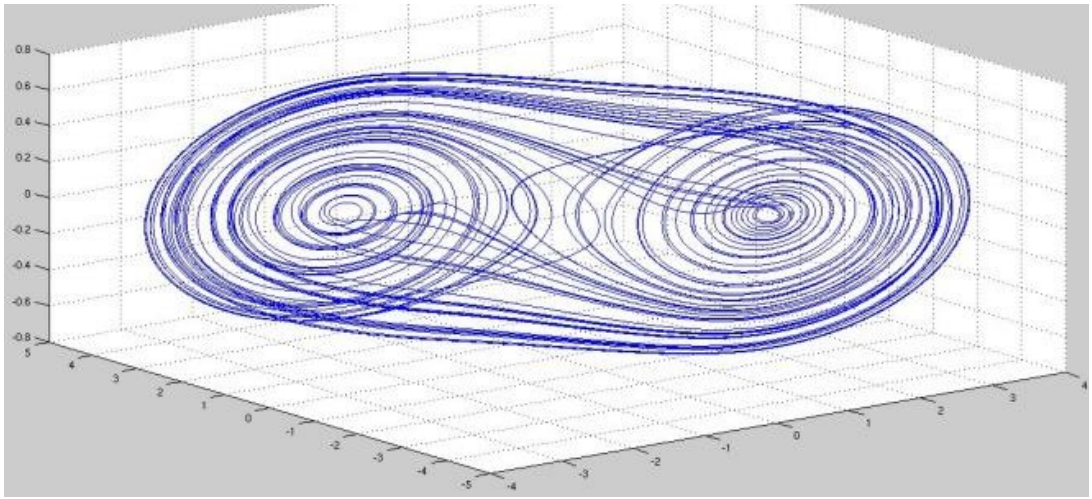


Fig-31 Double attracteur obtenu par la simulation

3.4 Simulation avec MULTISIM

3.4.1 Multisim

NI Multisim (anciennement MultiSIM) est un programme de capture et de simulation de schéma électronique qui fait partie d'une série de programmes de conception de circuits, avec NI Ultiboard. Multisim est l'un des rares programmes de conception de circuit à employer la simulation d'origine logicielle basée sur Berkeley SPICE. Multisim a été créé à l'origine par une société nommée Electronics Workbench, qui est maintenant une division de National Instruments. Multisim inclut la simulation de microcontrôleur (anciennement connu sous le nom MultiMCU), ainsi que l'importation et l'exportation fonctionnalités intégrées dans le logiciel de mise en page de circuits imprimés dans la suite NI Ultiboard.

3.4.2 Simulation du circuit de Chua sous Multisim

Nous avons vu que les équations (26) representent mathématiquement le comportement d'un circuit de chua, alors maintenant nous allons essayer de simuler un circuit de Chua (sous Multisim), et plus tard, voir comment synchroniser deux circuits et les utiliser pour le cryptage de données.

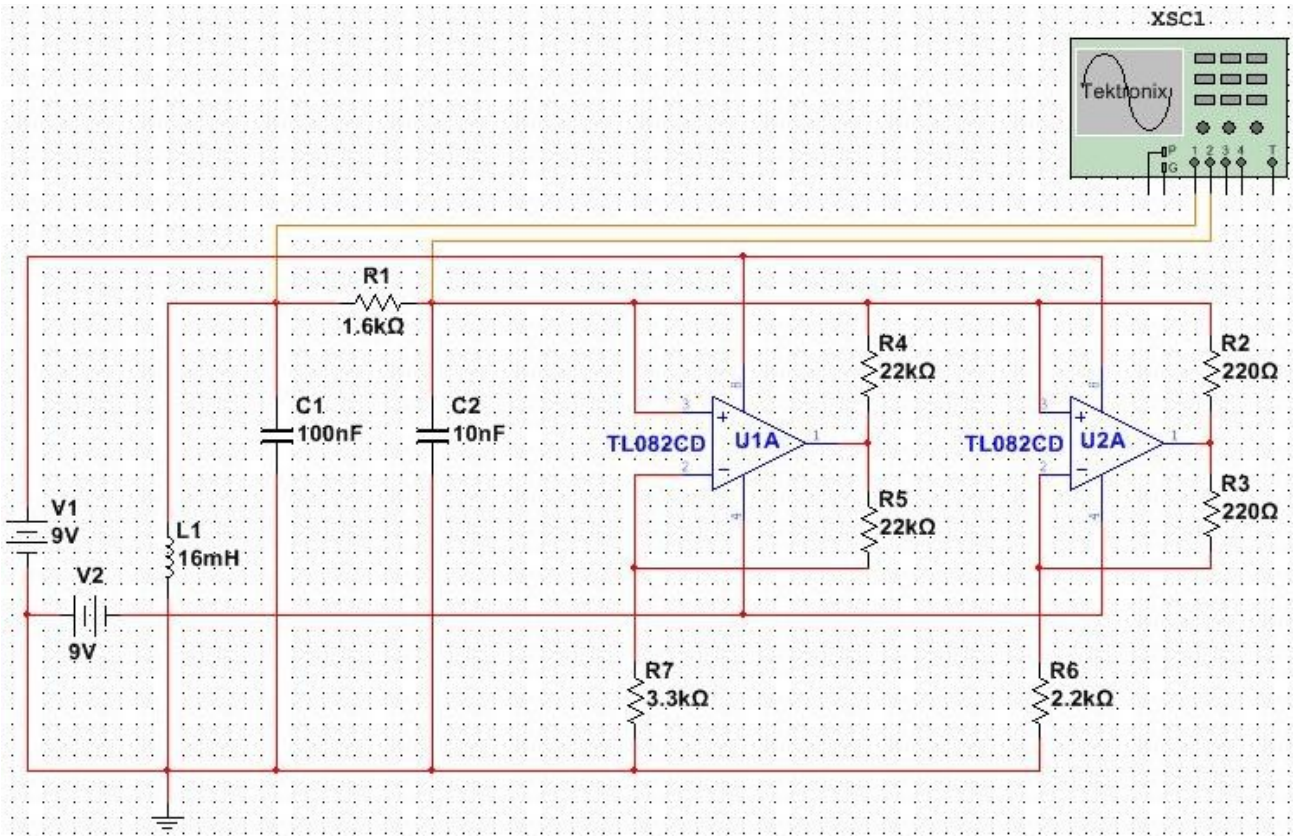


Fig-32 Schéma du circuit de Chua sous Multisim

L'image ci-dessus nous montre une réalisation simple d'un circuit de Chua à l'aide d'ampli opérationnels pour simuler la diode de Chua.[31]

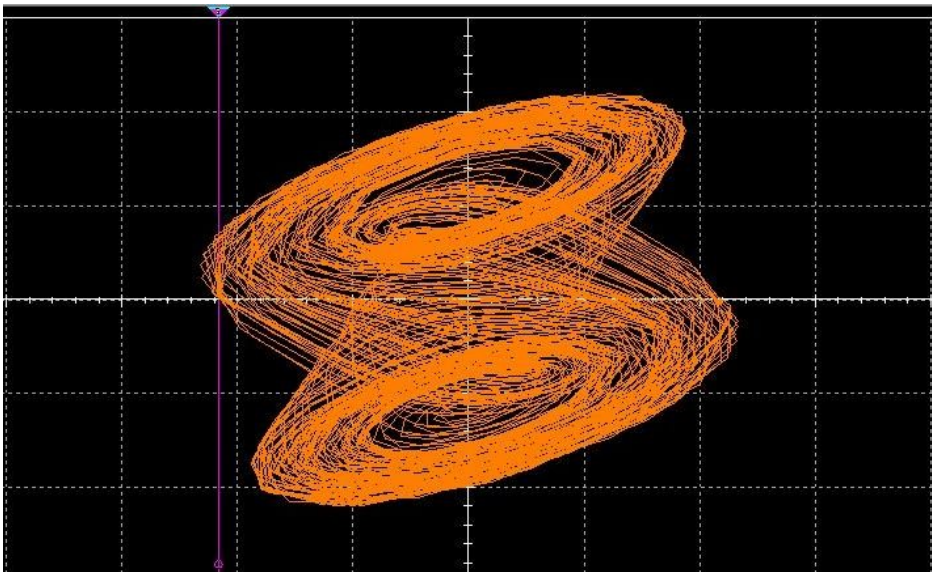


Fig-33 Double attracteur résultant de la simulation précedente

Comme il est visible sur la figure ci-dessus, on a bel et bien un circuit de Chua qui présent un aspet aléatoire.

3.5 Synchronisation de circuits de Chua

A présent, nous savons qu'un circuit chaotique a trois états (trois signaux). Un des avantages d'un circuit chaotique est que, s'il est laissé seul, deux circuits n'auront jamais les trois signaux identiques en tout point dans le temps (en raison de la propriété de «sensibilité aux conditions initiales»). En d'autres termes, deux circuits ne seront jamais naturellement en harmonie. Mais, avec un peu plus de circuits, nous pouvons synchroniser les deux circuits chaotiques et les signaux ségaleront.

Les circuits chaotiques synchronisés sont fréquemment utilisés dans des applications réelles. Pour réaliser la synchronisation de base de deux circuits, nous devons mettre en place nos deux circuits avec un circuit de couplage intermédiaire, comme dans les figures 34 et 35. Il ya plusieurs façons de coupler un système de synchronisation, les deux plus populaires sont bidirectionnel, et l'unidirectionnel (Maître / Esclave).

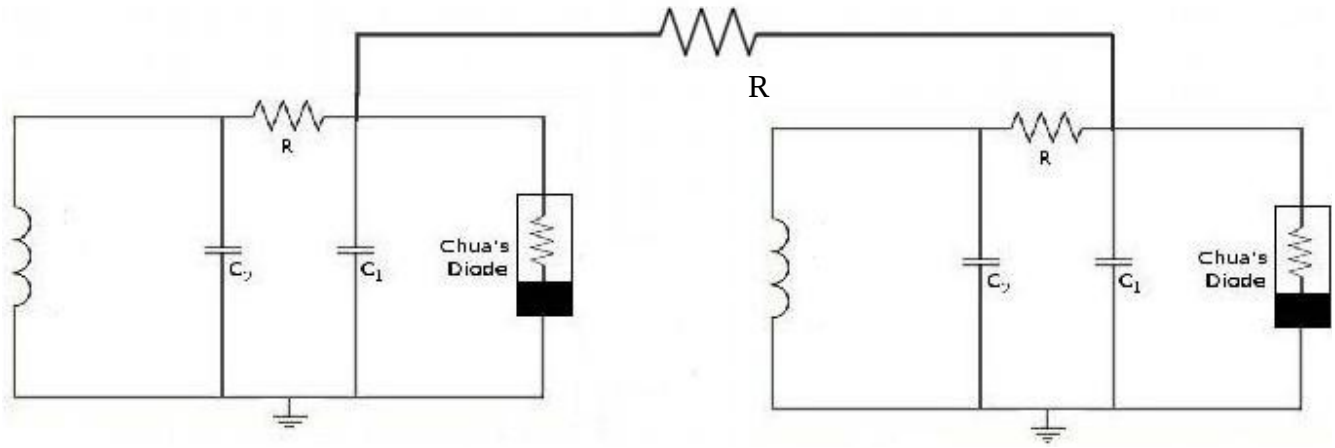


Fig-34 Couplage bidirectionnel de circuits de Chua

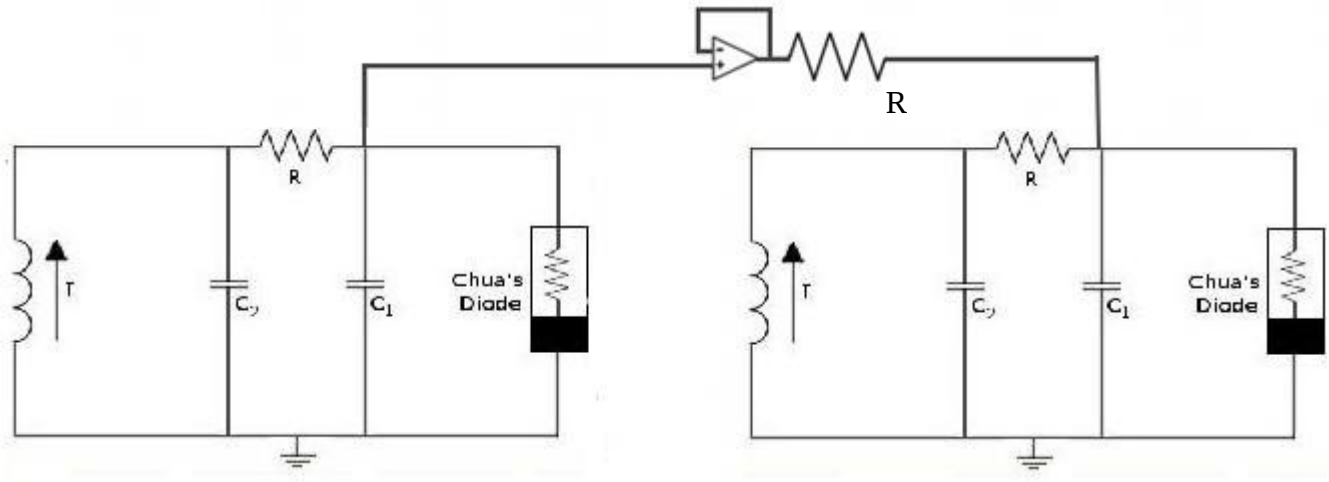


Fig-35 Couplage unidirectionnel de circuits de Chua

On a choisi l'approche Maître/esclave. Dans cette approche il n'y a qu'un seul circuit de Chua Maître et le reste sont des esclaves. Le circuit maître n'est pas affectée par les circuits esclave ou le couplage et agit de façon autonome. Les circuits esclave utilisent le circuit de couplage pour se synchroniser avec le signal du maître. En résumé, les esclaves se synchronisent (mais n'affectent pas) au circuit maître.

3.6 Réalisation sous Multisim

Maintenant que nous avons vu et choisi la méthode à utiliser pour la synchronisation, on passe directement au logiciel Multisim pour réaliser et voir de façon réaliste la synchronisation entre deux circuit de Chua.

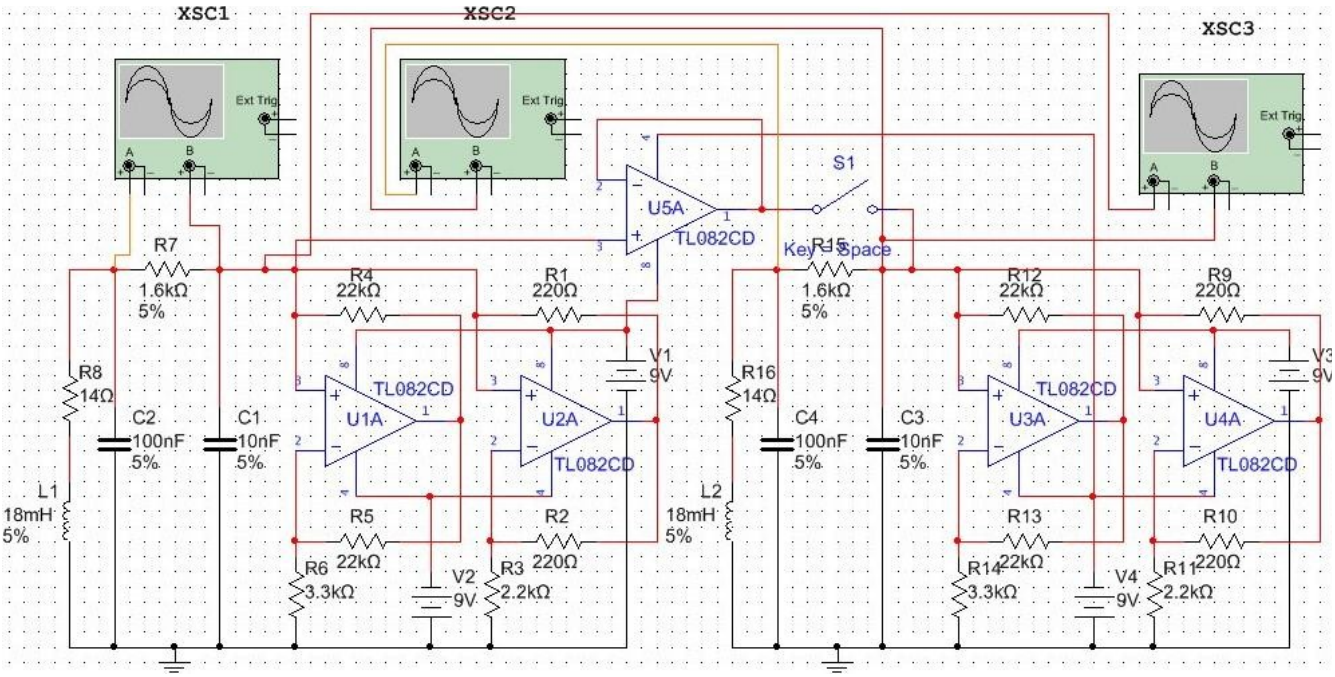
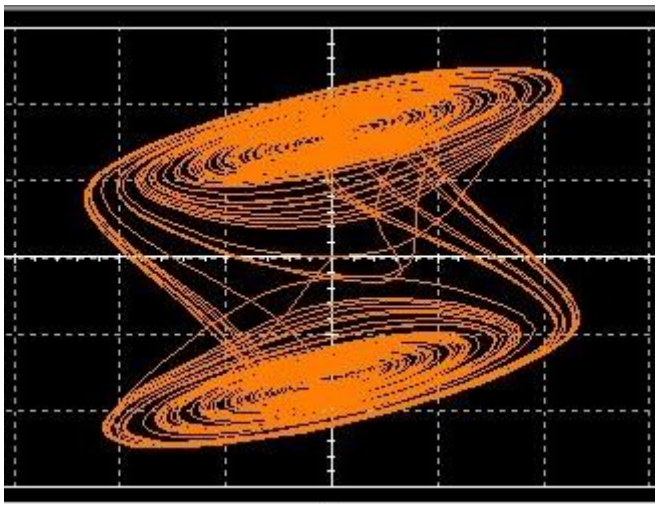
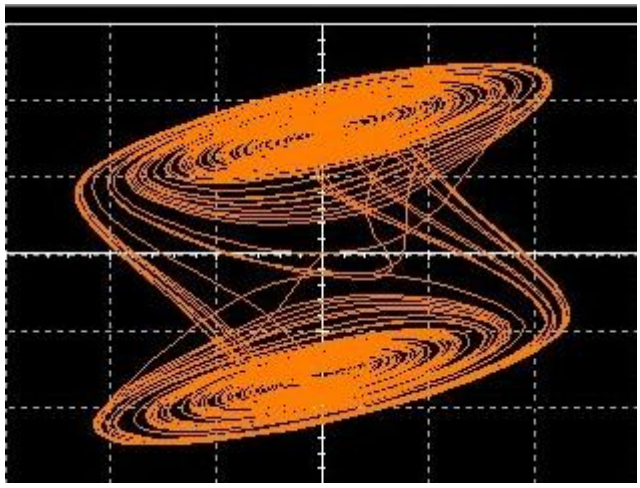


Fig-36 Schéma du couplage sous Multisim

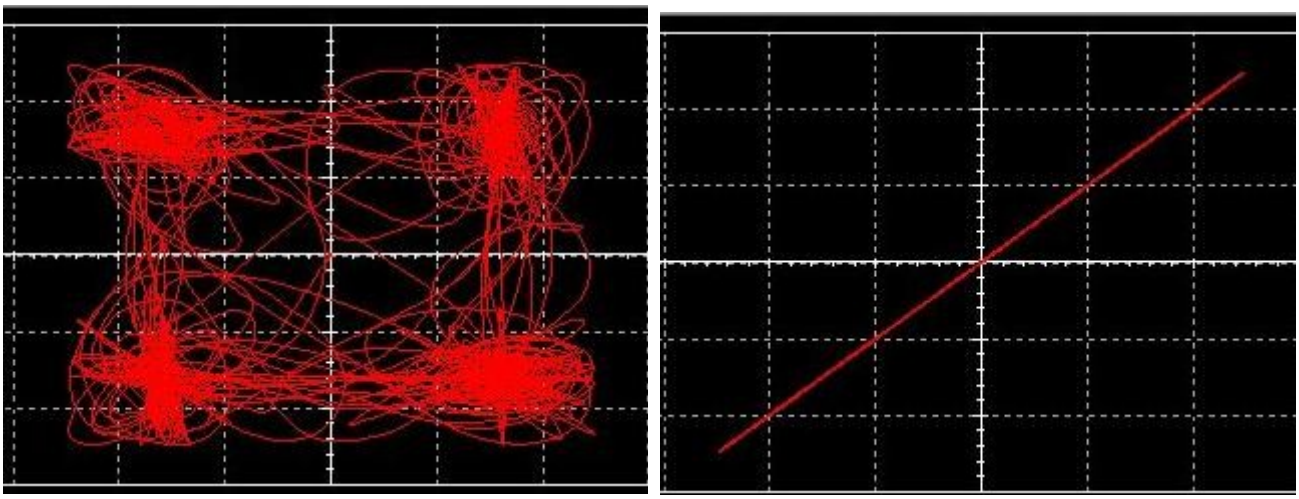
La figure ci-dessus nous montre le schéma du couplage unidirectionnel auquel on a ajouté un switch pour jouer sur la synchronisation des deux circuits.
En appuyant sur le bouton "Run" pour demarrer la simulation et en laissant le switch ouvert puis fermé, on obtient la figure suivante



(a)



(b)



(c) (d)

Fig-37 Résultat de la simulation:

(*a) Double attracteur du circuit mître, (b) double attracteur deucircuit esclave*

(c) Pas de synchronisation entre maître et esclave, (d) Synchronisation entre mître et esclaves

En demarrant la simultion, et en laissant le switch ouvert, on obtient sur les oscilloscopes 1 et 2 (XSC1 et XSC2 de la figure 36 les double attracteurs des circuits maître et esclave respectivement (imagee (a) et image (b) de la figure 37. Les images (c) et (d) nous montrent l'abscence et la presence de synchronisation lors de l'ouverture et la fermeture du switch respectivement et cela en reliant l'oscilloscope 3 (XSC3 de la figure 36 au bornes de la capacité C_1 du circuit maître et la capcité C_3 du circuit esclave.

3.7 Conclusion

Dans ce chapitre, nous venons de voir ce qu'est un circuit de Chua et de quoi il se compose ainsi que la méthode utilisée pour synchroniser deux ou plus circuits. Ceci nous ouvre la voie au prochain chapitre dans lequel nous allons essayer de beneficier de l'aspet chaotique du circuit de Chua et mettre en action cette particularité afin de crypter et proteger un signal (audio dans notre cas).

CHAPITRE 4

RÉALISATION D'UN SYSTÈME CHAOTIQUE

4.1 Introduction

Nous avons vu dans le chapitre précedent ce qu'est un circuit de Chua ainsi que ses prorietés et son fonctionnement théorique et simulé. Ayant acquis les notions nécessaires, nous allons, dans ce chapitre, appliquer ces connaissances afin de réaliser sur maquette deux circuits de Chua et les synchroniser et de voir en pratique son fonctionnement et ses possibles applications.

4.2 Cryptage d'un signal (audio) avec le circuit de chua

A présent que nous savons comment construire un circuit de Chua et comment le mettre en oeuvre, nous allons voir comment utiliser ce circuit pour crypter (masquer) un signal (audio dans ce cas) et ensuite le decrypter pour récuperer le signal original.

4.2.1 Masquage basique avec le chaos

Dans sa configuration la plus basique, le masquage par chaos necessite: un signal d'entrée (audio), un générateur de chaos (circuit maître), un ampli pour l'addition, un générateur de chaos esclave et un ampli de soustraction.

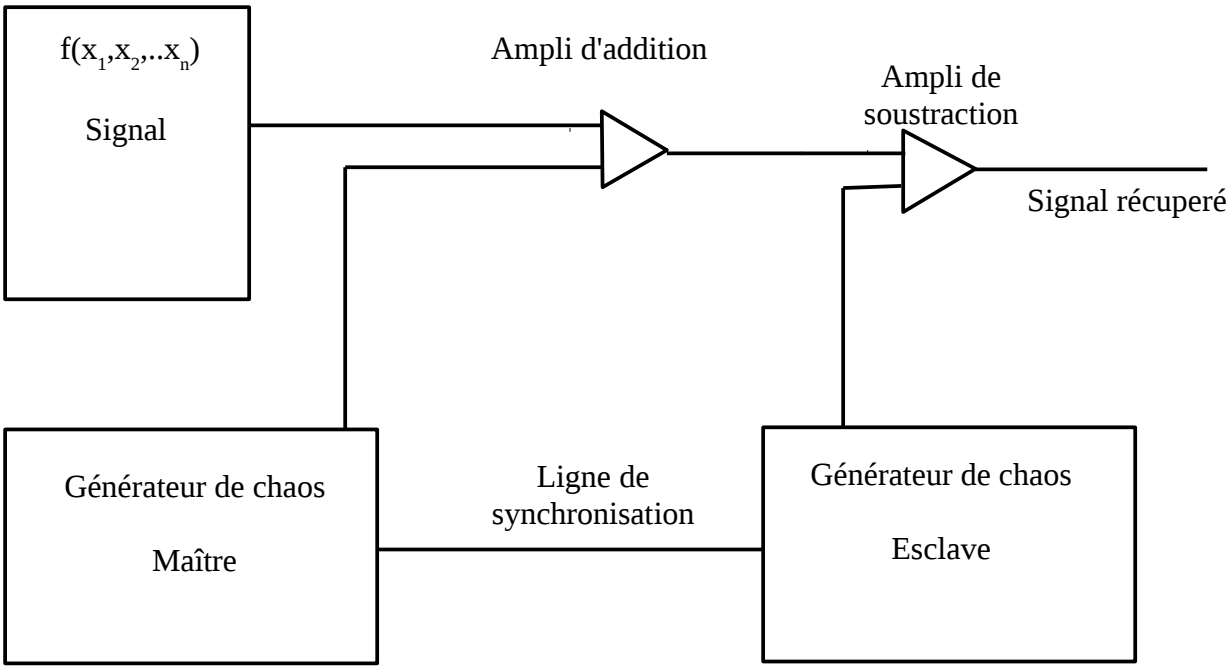


Fig-38 Diagramme du masquage basique d'un signal analogique

4.2.2 Principe de fonctionnement

Le générateur de chaos maître produit une tension qui, visualisée sur l'oscilloscope, ressemble à du buit. Lorsque on additionne ce "bruit" avec notre signal original, on devra avoir un message non reconnaissable. Pour récuperer le massage d'origine, on doit avoir un signal identique au signal généré par le circuit maître, autrement le signal reçu apparaîtra comme du simple bruit. La synchronisation entre le circuit maître et l'esclave, conçus avec les mêmes compposants rendra les dynamiques des deux systèmes identiques, ce qui rend possible la replication du signal chaotique maître utilisé pour le masquage et ceci en temps réel.
En soustryant le signal esclave avec le signal maître additionné avec le signal original, on devra en théorie avoir une copie exacte du signal original.

4.3 Le générateur de chaos

On reprend le schéma de la figure 32, on modifie legèrement les valeurs de C_1 et C_2 pour maximiser les performance du circuit. [35]

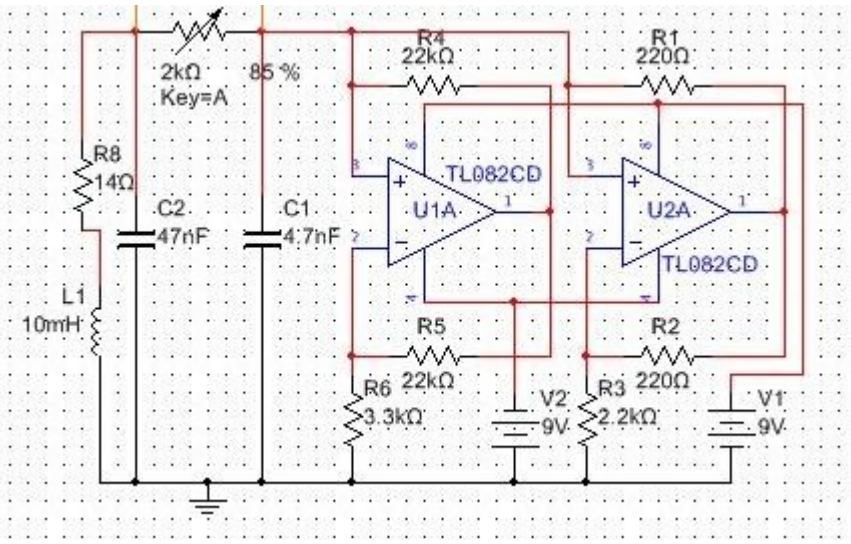


Fig-39 Circuit de chua avec C_1=4.7nF,C_2=47nF et L=10mH

Les deux circuit de Chua seront réalisés à l'aide d'un seul ampli op de type TL082, qui se compose à l'interieur de deux ompli op distincts.

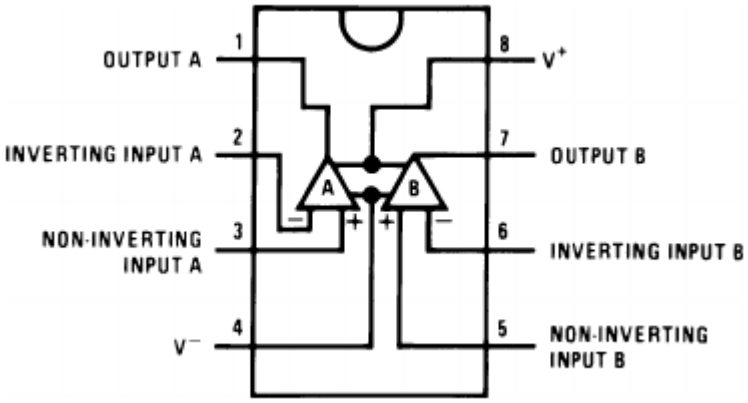


Fig-40 Diagramme de connexion d'un TL082

Pour réaliser ce circuit, on utilise le logiciel DesignSpark qui permet de créer des circuit PCB avec une grande facilité, et on obtient le schéma PCB suivant:

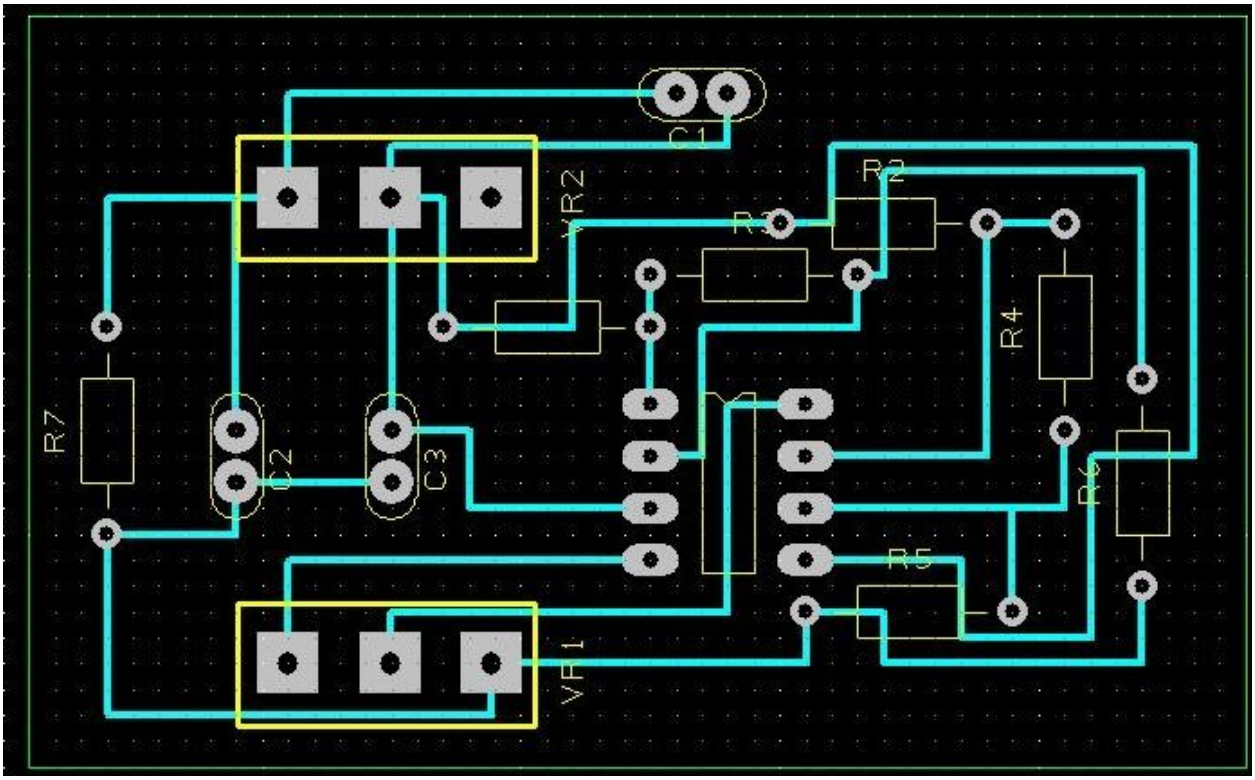


Fig-41 Schéma PCB sous DesignSpark

et pour plus de réalisme ,DesignSpark génére une image tridimentionnelle pour une meilleur visualisation du circuit afin d'avoir un avant gout sur le produit final, comme illustré ci-dessous

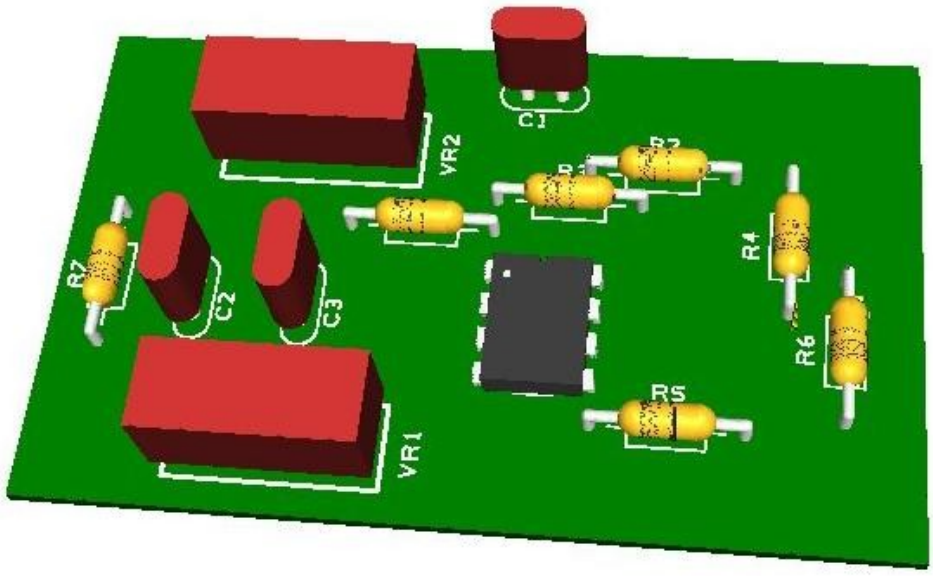


Fig-42 Rendu 3D du circuit de Chua sous DesignSpark

La synchronisation des deux circuits de Chua étant unidirectionelle, on peut la réaliser avec un ampli op tel que le TL082

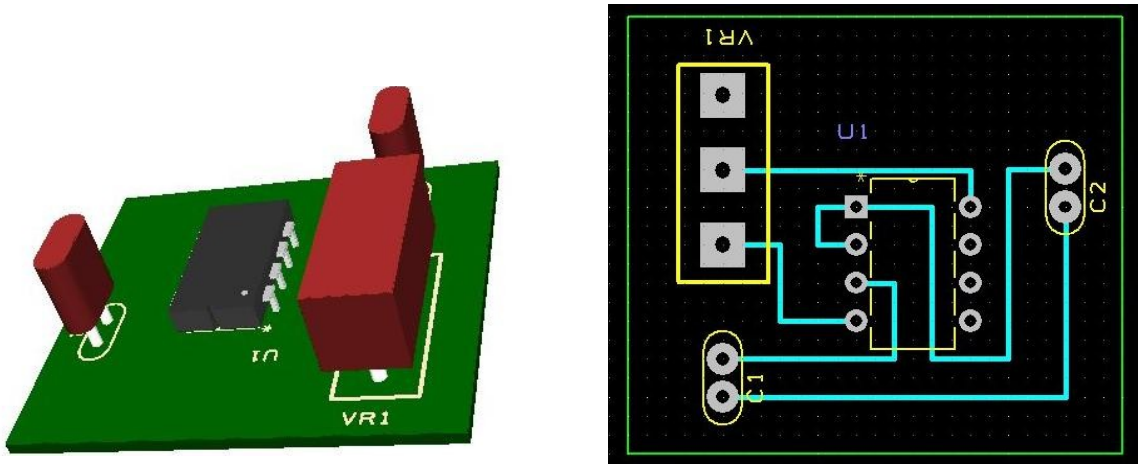


Fig-43 Rendu 3D et schéma PCB du circuit de couplage

4.4 Le circuit de masquage

Ce circuit se compose de l'additionneur, du soustracteur et d'un inverseur, les valeurs des résistances de l'additionneur et du soustracteur ont été choisies de manière à limiter le gain, tandis que les valeurs de R21 et R17 ont des valeurs très grandes afin de limiter le feedback du courant dans les générateurs de chaos, qui s'avère déteriorer le signal chaotique.

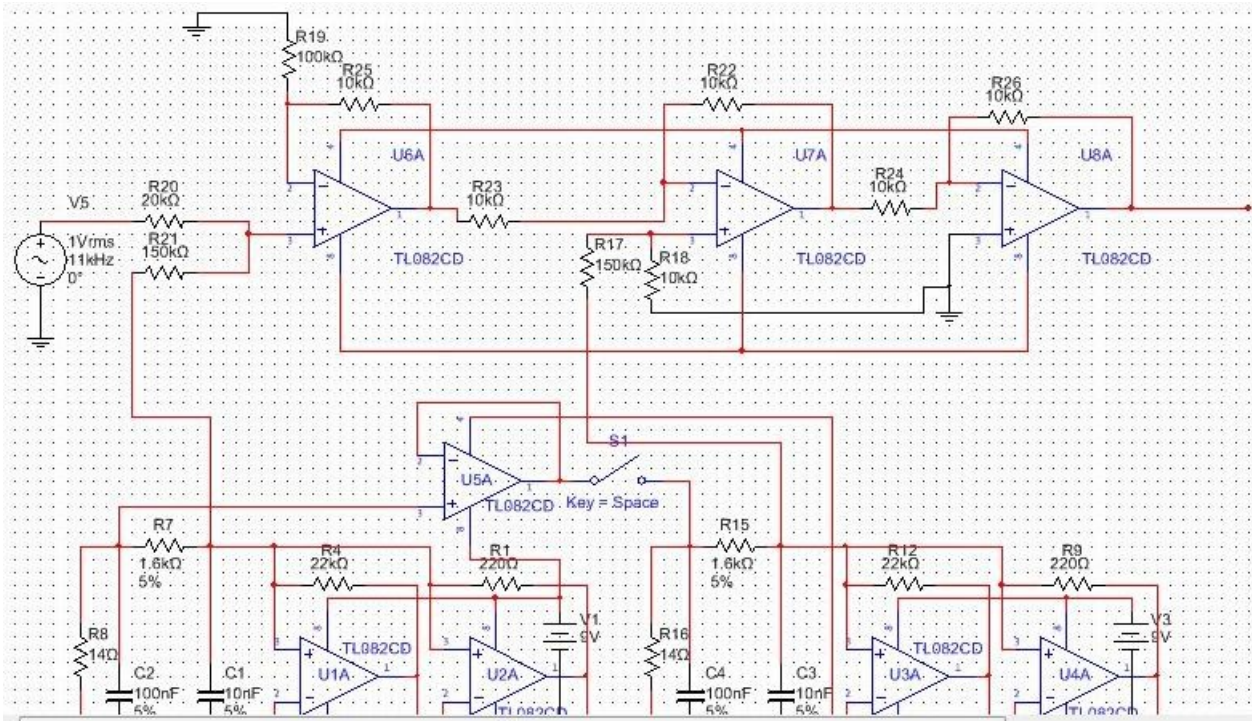


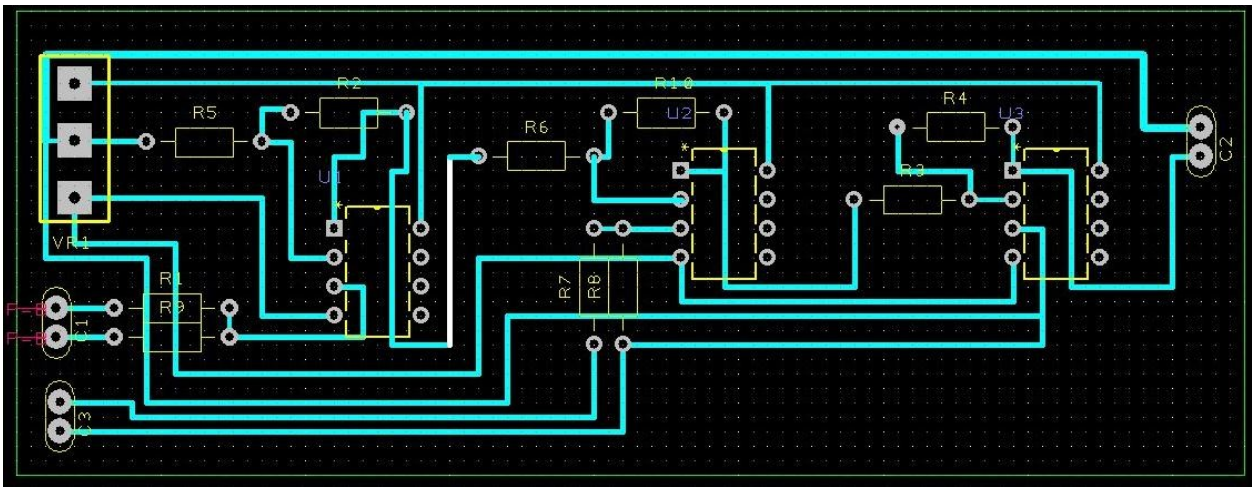
Fig-44 Simulation du masquage par le chaos

La tension de sortie de l'ampli op de l'additionneur est

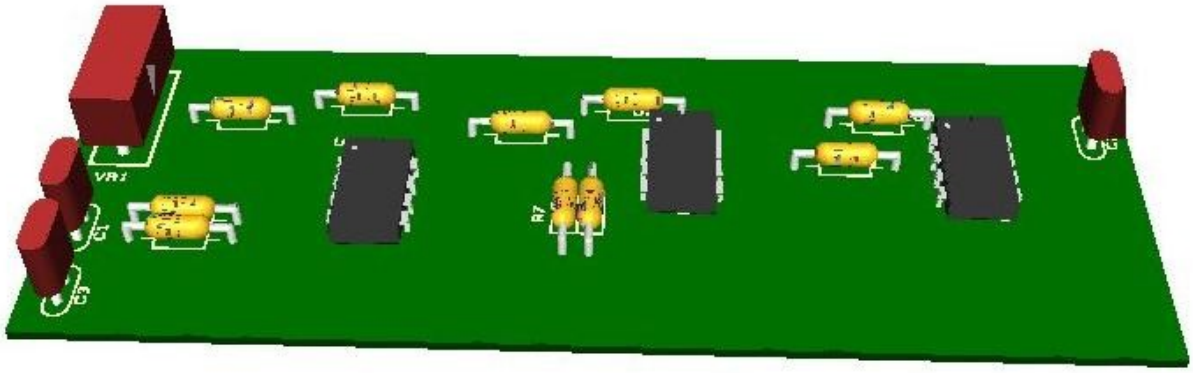
$$V_{out(U6A)}=\left(V_5\frac{R_{21}}{R_{20}+R_{21}}+V_{C1}\frac{R_{20}}{R_{20}+R_{21}}\right)\left(1+\frac{R_{25}}{R_{19}}\right) \qquad (28)$$

Pour la tension de sortie du soustracteur, elle est sous la forme

$$V_{out}=\left(\frac{R_{23}+R_{22}}{R_{17}+R_{18}}\right)\frac{R_{18}}{R_{23}}V_{out(R_{23})}-\frac{R_{22}}{R_{23}}V_{out(U6A)} \qquad (29)$$



(a)



(b)

Fig-45 Schéma PCB et rendu 3D de l'additionneur/soustracteur

4.5 Réalisation pratique

Après avoir réalisé les schémas des circuits récedents, nous obtenons les differentes maquettes illustées ci-desous

Fig-46 Les deux circuits, maître et esclave

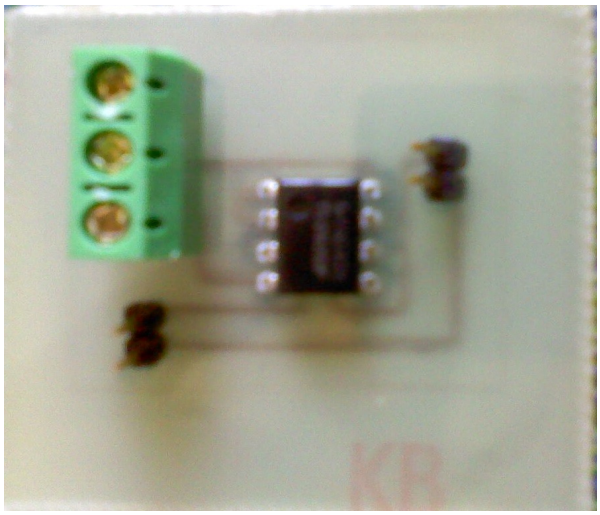


Fig-47 Le circuit de couplage

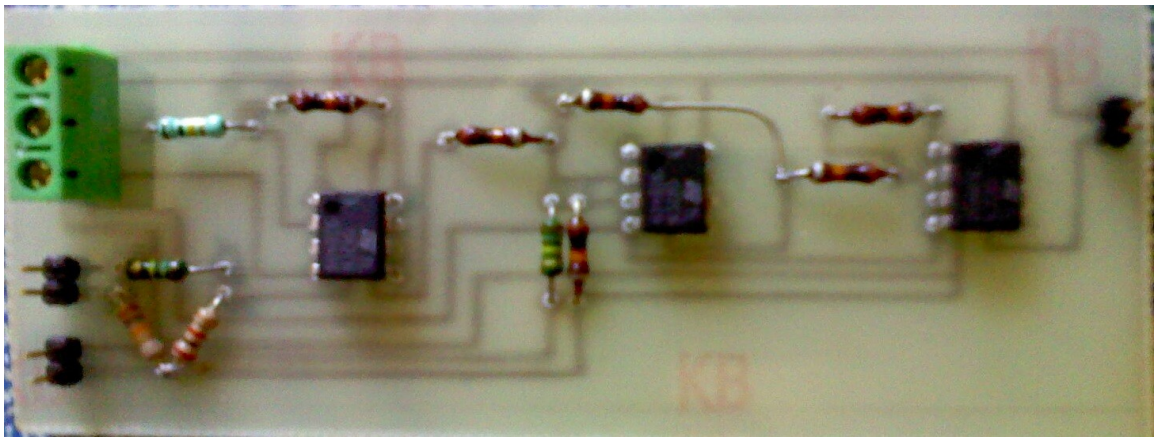


Fig-48 Le circuit additionneur/soustracteur

4.5.1 La mise en marche

Une fois tout le necessaire réuni (circuits maître et esclave, additionneur/soustracteur, circuit de couplage et biensur 2 atteries de 9 V ainsi que les fils pour relier les differents composants), on procède aux tests en utilisant un oscilloscope.

4.5.2 L'oscilloscope des pauvres (Soundcard Oscilloscope)

L'utilisation d'un vrai oscilloscope n'etant pas strictement necessaire dans ce test , on peut utiliser la carte son d'un PC en tant qu'oscilloscope à l'aide du logiciel gratuit Soundcard Oscilloscope qui permet de « transformer » la carte son en oscilloscope simple mais parfaitement adequat pour notre cas.
Lors de l'utilisation de la carte son en tant qu'oscilloscope, il faut prendre certaines précautions, tels que la fréquence des signaux à mesurer qui doivent être inférieur à celle des cartes son (les cartes récentes peuvent aller jusqu'à 512kb de fréquence d'échantillonage) et la tension d'entrée qui ne doit pas dépasser les 5 V au risque de griller la carte son, pour celà l'utilisation d'un diviseur de tension peut s'averer très utile pour préserver le matériel utilisé.

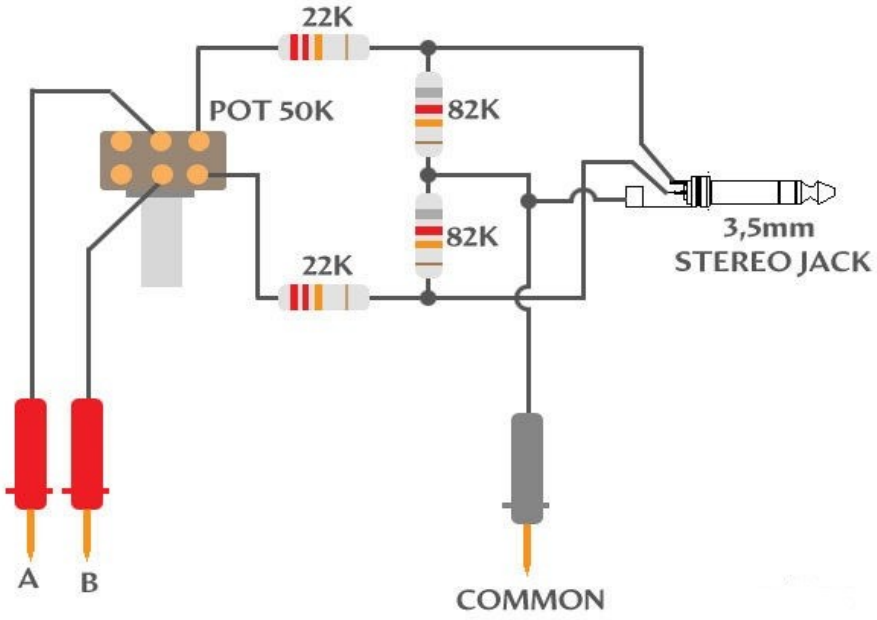


Fig-49 Exemple d'un diviseur de tension de protection

Ayant pris toutes les précautions nécessaires, on relie les différents composants, on alimente et on observe

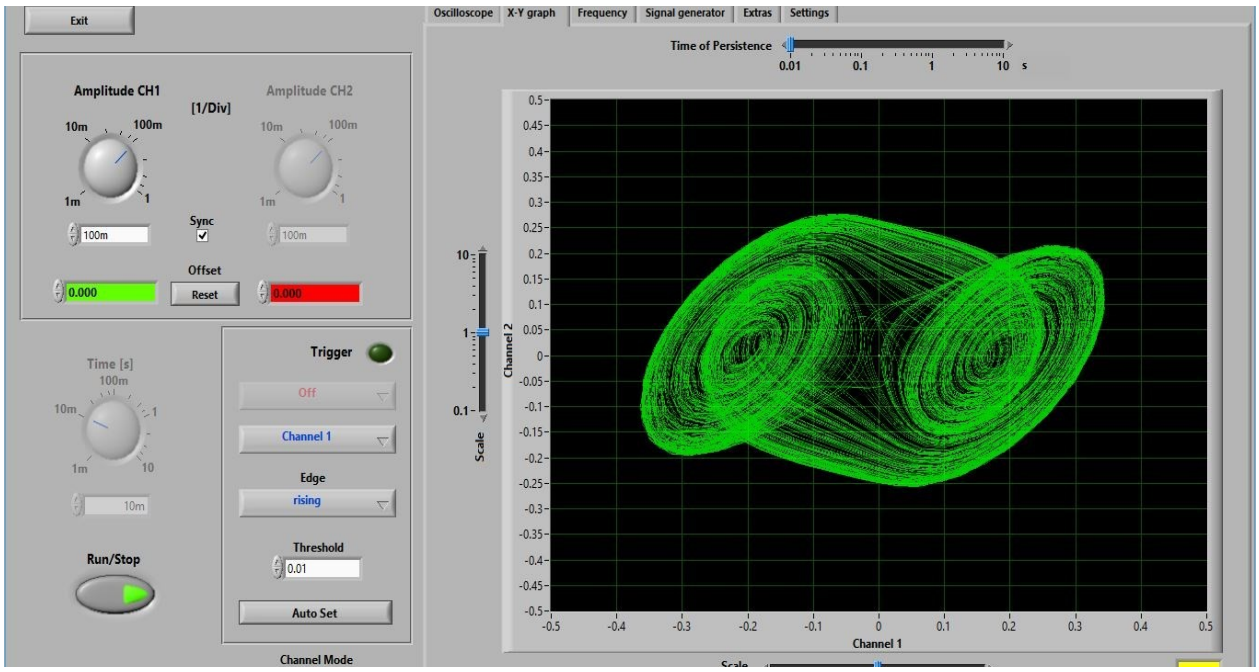


Fig-50 Double attracteur dans le circuit maitre

L'illustration ci-dessus nous montre la présence d'un double atracteur dans le premier circuit (maître), ce qui signifie qu'il génere bel et bien un

signal chaotique. Un double attracteur similaire est aussi présent dans le deuxieme circuit, impliquant la présence d'un signal chaotique.
Une fois que nous avons vu le bon fonctionnement des deux circuits, on procède à l'étape suivante qui est le cryptage d'un son audible (extrait de musique) d'une fréquence de 8 Khz, le choix d'une tel fréquence s'est fait à cause de la fréquence de fonctionnement du circuit de chua choisi qui de l'ordrre de 6 à 8 Khz.
A la sortie de l'additionneur nous obtenons un son qu'on peut considerer comme un « bruit », ce qui veut dire que le circuit à bien crypté l'extrait de musique. Maintenant en passe à la sortie du soustracteur et retrouve le même son (extrait de musique) mais avec une légère perte de qualité qui est du à plusieurs aspects du circuit et des composants et l'architecture même du circuit de chua.

4.6 Améliorations possibles

La plupart des limites de ce système chaotique proviennent de l'utilisation de la technique de masquage notamment ceux liées à la bande passante faible du signal chaotique généré par le système de Chua.
Une solution possible serait de carrément changer le système chaotique utilisé, par exemple un système de Lorenz peut assurer une bande passante un peu plus large jusqu'à environs 16KHz mais cela ne résous pas le problème totalement. Mais il existe une solution bien meilleure: Utiliser un circuit de Chua utilisant un CFOA (Current Feedback Operational Amplifiers) [38] tel que sa fréquence d'oscillations est de l'orde de 50MHz

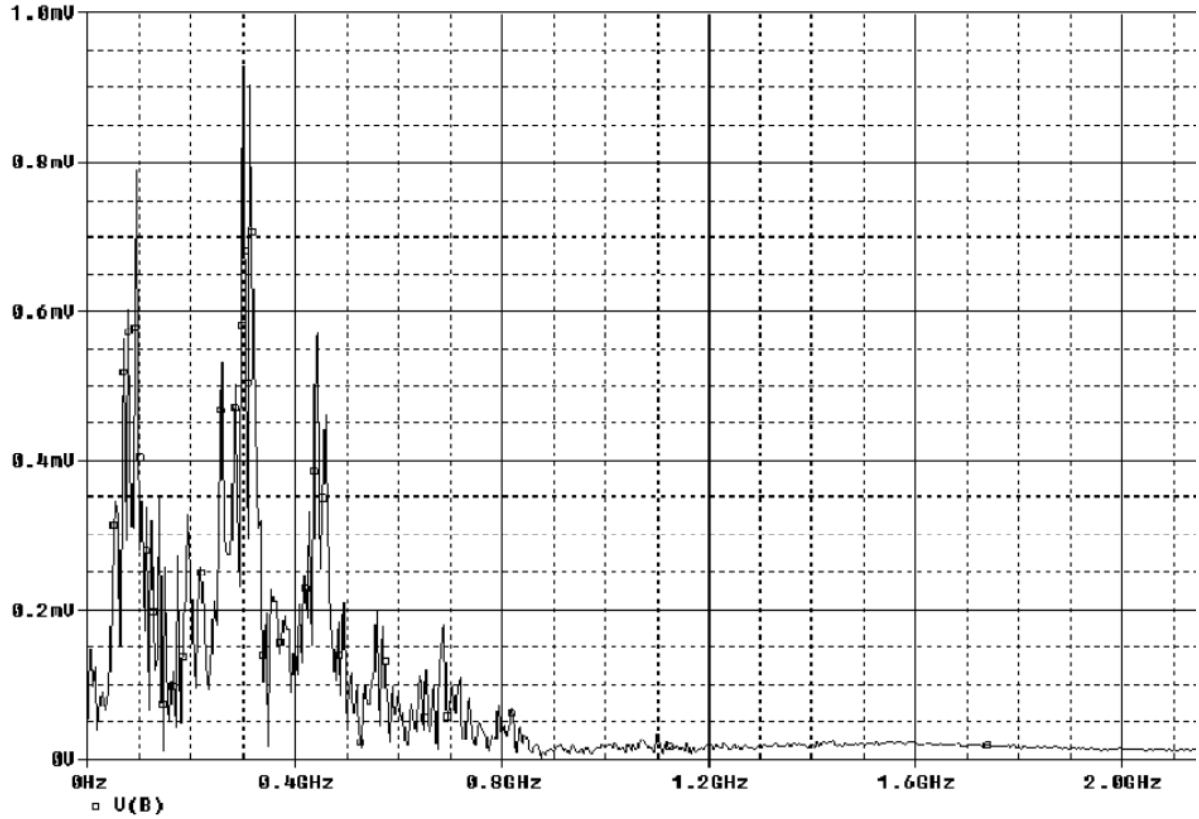


Fig-46 FFT du circuit de chua (CFAO)

4.7 Conclusion

Dans ce chapitre nous venons de voir une implémentation simple du circuit de Chua ainsi que ses différentes caractéristiques et les possibles améliorations pouvant être apportées à ce circuit pour booster ses performances pour une utilisation où la fréquence d'oscillation requise est grande

Conclusion générale

Au cours de ce projet, nous avons effectué des recherches sur plusieurs axes de la cryptographie chaotique. Nous avons étudié ses origines avec la découverte de la synchronisation et son apogée avec les techniques de « sécurisation » et leurs intérêt dans une utilisation quotidienne et dans plusieurs domaines.

Le premier chapitre porte sur quelques notions concernant les systèmes dynamiques puis nous nous sommes raprochés des systèmes chaotique qui présentent plusieurs caractéristiques très intéressantes notamment pour la transmission de données mais aussi présente un intérêt dans le domaine médicale, où plusieurs études ont été conduites, et continues d'être d'actualité.
parmi ces caractéristiques ont peut citer la sensibilité aux conditions initiales, ce qui signifie que la moindre difference dans les conditions initiales engendre une évolution qui différe a chaque fois. Une autre caractéristique serait le déterminisme, ce qui veut dire qu'il est possible de reproduire le comportement chaotique.
Au deuxième chapitre nous avons vu un schéma simple illustrant une transmission sécurisée de données basée sur le chaos, son principe est de "cacher" les données dans un signal chaotique et les transmetre sur un canal ouvert vers le recepteur qui decryptera les données.
Pour parvenir à une récuperation des données, l'emetteur et le récepteur doit pocéder le signal chaotique, d'où la synchronisation des deux systèmes, puis nous avons vu les différentes méthodes et techniques de synchronisations pouvant être mise en oeuvre pour synchroniser les deux systèmes.
Le troisième chapitre à porté sur une simulation sur ordinateur d'un système chaotique, un circuit de chua dans notre cas, et nous avons procédé à la synchronisation de circuits en utilisant la méthode unidirectionnelle.

Ce travail a été finalisé dans le quatrième chapitre avec la réalisation d'un circuit de chua et le masquage de données (signal audio) et ensuite leur récuperation par le récepteur.

Ce travail nous a permis de nous familiariser avec un domaine quelque peu sensible qu'est la sécurisation de données et aussi nous a permis de faire connaissance avec une méthode, parmi tant d'autre, de cryptage. Le système présent dans ce travail est loin d'être parfait, mais peut être amélioré en étudiant la robustesse du circuit de Chua dans un but majeur d'augmenter sa fréquence d'oscillation nécessaire pour pouvoir crypter non-seulement un signal audio mais aussi un signal video.

Bibliographie

[1] Wikiversity (28 July 2011). "1972/Lorenz". Wikipedia. Retrieved 8 April 2014

[2] Watts, Robert G. (2007). Global Warming and the Future of the Earth. Morgan & Claypool. p.17.

[3] Werndl, Charlotte (2009). "What are the New Implications of Chaos for Unpredictability?". The British Journal for the Philosophy of Science 60 (1): 195–220. doi:10.1093/bjps/axn053

[4] A.J. Michaels. "Digital Chaotic Communications." Thèse de Doctorat, Georgia Institute of Technology, 2009.

[5] T. Yang. «Impulsive Control theory.» Springer Verlag, Lecture Notes in Control and Information sciences, 2001.

[6] K. T. Alligood, T. D. Sauer and A. J. Yorke, Chaos : An introduction to dynamical systems, Springer-verlag, New York, 1996.

[7] H. Schuster Georg. ''Deterministic Chaos - an Introduction''. 4 e edition , Wiley, (2005), 288 pp.

[8] Hirsch M., Smale S., Devaney R. ''Differential equations, dynamical systems and an introduction to chaos''. 2 e Edition, USA, Elsevier Academic Press (2004), 432 pp.

[9] W. L. Ditto, L. M. Pecora, "Mastering Chaos" Scientific American, (Aout 1993) pp. 77-84.

[10] David Aubin, Amy Dahan. ''Systèmes dynamiques et Chaos : Convergences et recompositions, un aperçu historique''. Apparu dans Chaos & Systèmes dynamiques: éléments pour un épistémologie, dir. Sara Franceschelli, Tatiana Roque & Michel Paty. Paris: Hermann, (11 décembre 2007), pp. 327-356.

[11] D. Aubin et A. Dahan Dalmedico. ''Writing the History of Dynamical Systems and Chaos: Longue Durée and Revolution, Disciplines and Cultures''. Historia Mathematica (2002), vol. 29, pp. 273-339.

[12] THEODOR LEIBER. ''On the Impact of Deterministic Chaos on Modern Science and Philosophy of Science: Implications for the Philosophy of Technology?''. ADVANCES IN THE PHILOSOPHY OF TECHNOLOGY: PROCEEDINGS OF A MEETING OF THE INTERNATIONAL ACADEMY OF THE PHILOSOPHY OF SCIENCE, KARLSRUHE, GERMANY, (MAY 1997), N2 , pp. 23-50.

[13] H. Hamiche,Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques, Applications à la Transmission Sécurisée de Données. Thèse de Doctorat, Universite Mouloud Mammeri de Tizi-Ouzou, (2011).

[14] L.M. Pecora and T.L. Carroll, Synchronization in Chaotic Systems, Physicals Review and Letters, Volume 64,Number 8, (1990).

[15] Aziz-Alaoui, M.A., Synchronization of Chaos, Encyclopedia of Mathematical Physics, Elsevier, Vol. 5, pp : 213-226, (2006).

[16] Melle Megherbi Ouerdia. Etude et réalisation d'un système sécurisé à base de systèmes chaotiques, Memoire de Magister, Universite Mouloud Mammeri de Tizi Ouzou, (2013).

[17] Tao Yang and Leon O.Chua,Impulsive Control and Synchronisation of Nonlinear Dynamical Systems and Application to Secure Communication, Internationa Journal of Bifurcation and Chaos, Vol. 7, No. 3 (1997) 645-664.

[18] I.Belmouhoub et M. Djemaï. ''Synchronization of Discrete-Time Chaotic Systems for Secured Data Transmission''. Chaos in Automatic Control : From Theory Towards Engineering Application (2005), Edited by W. Perruquetti and J.P. Barbot, CRC Press Book, pp. 527-551.

[19] S. Guan, C.-H. Lai, and G. W. ''Phase synchronization between two essentially different chaotic systems'' Wei, Phys. Rev. Vol. 72, Iss. 1, (2005) pp. 016205 –016212.

[20] Guan, Shuguang; Li, Kun; Lai, C.-H., ''Chaotic synchronization through coupling strategies''. Chaos, Volume 16, Issue 2, (2006) pp. 023107-023109

[21] Louis M. Pecora, Thomas L. Carroll, Gregg A. Johnson, et Douglas J. Mar. ''Fundamentals of synchronization in chaotic systems, concepts, and applications'' Chaos 74, (1997); pp. 520-543.

[22] Jun Guo Lu; Hill, D.J. ''Impulsive Synchronization of Chaotic Lurapos;e Systems by Linear Static Measurement Feedback: An LMI Approach''. IEEE Transactions on Circuits and Systems II: Express Briefs, Volume 54, Issue 8, (Aug. 2007) pp. 710-714.

[23] Bindu M. Krishna, P. Indic , Usha Nair , R. Pratap. ''Quantifying chaotic synchronization using error evolution''. Commun Nonlinear Sci. Numer. Simulat. Vol. 14 (2009) pp. 3682–3692.

[24] Ali Zemouche, Sur l'observation de l'état des systèmes dynamiques non linéaire, Thèse de Doctorat, Université Louis Pasteur Strasbourg I, (2007).

[25] Shujun Li , Gonzalo Alvarez, Zhong Li and Wolfgang A. Halang, Analog Chaos-based Secure Communications and Cryptanalysis: A Brief Survey, 3rd International IEEE Scientific Conference on Physics and Control (PhysCon 2007), (2007).

[26] ABDUL RAHUMAN Ahmed, Analyse des Systèmes Non-linéaires à Dynamiques Complexes, Thèse de Magister, L'UNIVERSITÉ ABOU BEKR BELKAÏD, 2009

[27] M. Halimi , K. Kemih and M. Ghanes, Circuit Simulation of an Analog Secure Communication based on Synchronized Chaotic Chua's System, Applied Mathematics & Information Sciences 8, No. 4, 1509-1516, (2014)

[28] Colpitts Oscillator, fichier example NI Multisim v13.0

[29] T. Matsumoto, Transactionson Circuitsand Systems,Vol. Cas-31,No.12, December1984

[30] http://en.wikipedia.org/wiki/Chua's_diode

[31] Michael Peter Kennedy, Robust OP AMP Realisation of Chua's Circuit, University College Dublin, 1992

[32] R. Trejo-Guerra, E. Tlelo-Cuautle, CHAOTIC COMMUNICATION SYSTEM USING CHUA'S OSCILLATORS REALIZED WITH CCII+s,International Journal of Bifurcation and Chaos, Vol.19, No. 12 (2009) 4217–4226

[33] IEEE Trans. Circuits and Systems-I, Volume 33, Issue 11, 1986

[34] HOET Thomas, LORENZI Baptiste, SAHIN Serdar, La cryptographie chaotique, Soutenance à l'Institut national des sciences appliquées de Toulouse, 2012

[35] Karan Khatter, Simulation of Small Chaos Generator to Study Chaotic Dynamics and Mathematical Network, International Journal of Engineering Research and Reviews (IJERR), InternationVol. 1, Issue 1, pp: (37-43), 2013

[36] Christopher R. Comfort, Simple Analog Signal Chaotic Masking and Recovery, University of California, San Diego,2012