République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur

Et de la Recherche Scientifique

Université Mohamed Saddik BENYAHIA de Jijel

Faculté des Sciences Exactes et Informatique

Département d'Informatique

Mémoire de fin d'études pour l'obtention du diplôme

de Master en Informatique

Option : ILM

Thème

Réalisation d'un système chaotique pour la sécurisation des images numériques

Encadré par :

M^me^.Louzzani Noura

Réalisé par :

BOUTASSETA Selma
MEHIZ Radja

Promotion : 2018

Remerciements

Nous remercions en premier lieu Dieu le tout puissant qui nous a éclairé la vie par le savoir et nous a accordé à réaliser ce travail de fin d'étude.

Un sincère et honnête merci à nos parents et nos frères et sœurs pour leur soutien indéfectible qu'ils savent nous l'apporter tout au long de nos études et en particulier pendant cette mémoire.
Ce travail est réalisé pour obtenir le diplôme de master , spécialité Informatique légale multimédia au département de l'informatique, université de Jijel.

Nous avons témoigné ici notre respectueuse reconnaissance et remerciement très sincèrement à Mme N.louazzani enseignante au département de l'informatique à l'Université de Jijel pour l'intérêt qu'elle a apporté à notre travail, et pour les conseils qu'elle nous a donné et pour sa patience au cours d'encadrement.

Nous remercions vivement les membres de jury.

Nous remercions également tous les enseignants du département de l'informatique et spécialement les enseignants qui apportent cette spécialité à l'Université de Jijel.

Nous remercions tous nos collègues et amis qui ont partagés deux années agréable, avec une ambiance éducative inoubliable.

Nous remercions tous les membres de département de l'informatique qui font pendent cinq années nous informer et guider concernant nos intérêts préoccupations et administrative.

Enfin, nous remercions tous ceux qui ont participé dans la réalisation de ce travail de près ou de loin.

Merci pour tous ...

Dédicaces

A chaque fois qu'on achève une étape importante dans notre vie, on fait une pose pour regarder en arrière et se rappeler toutes ces personnes qui ont partagé avec nous tous les bons moments de notre existence, mais surtout les mauvais.

Ces personnes qui nous ont aidés sans le leur dire, soutenus sans réserve, aimé sans compter, ces personnes à qui notre bonheur devient directement le leur, se transforme en pleur.

Je remercie Dieu qui a toujours était à mais côtes.

Je dédie ce modeste travail

Aux fleurs de ma vie, Ma mère Farida et ma tante zoubida, ma raison d'être, ma raison de vivre, La lanterne qui éclaire mon chemin Et m'illumine de douceur et d'amour

Mon père hassene, en signe d'amour, de reconnaissance et de gratitude pour tous Les soutiens et les sacrifices dont il a fait preuve à mon égard

Sans oublier de dédier ce mémoire

A mes chers frères Mohamed Amine, Abdellah,et soeurs hossena, Hadil, et takoua.

À mon binôme Radja, A tous ma familles , mes ancles et surtout kamel houcine et mes amies .

En témoignage de l'amitié sincère qui nous à liée Et des bons moments passés ensemble A tous les gens qui ont cru en moi et qui me donnent l'envie D'aller avant

Je veux remercier tous, votre soutien et vos encouragements me donnent La force de continuer.

« Selma »

Dédicaces

A chaque fois qu'on achève une étape importante dans notre vie, on fait une pose pour regarder en arrière et se rappeler toutes ces personnes qui ont partagé avec nous tous les bons moments de notre existence, mais surtout les mauvais.

Ces personnes qui nous ont aidés sans le leur dire, soutenus sans réserve, aimé sans compter, ces personnes à qui notre bonheur devient directement le leur, se transforme en pleur.

Je remercie Dieu qui a toujours était à mais côtes.

Je dédie ce modeste travail

Aux fleurs de ma vie, Ma mère Zakia, ma raison d'être, ma raison de vivre, La lanterne qui éclaire mon chemin

Et m'illumine de douceur et d'amour

Mon père nouraddine, en signe d'amour, de reconnaissance et de gratitude pour tous Les soutiens et les sacrifices dont il a fait preuve à mon égard

Sans oublier de dédier ce mémoire

Et mes chéres sœurs houda, chahra, ibtissame, sakina, et youssra .

À mon binôme Selma, et tous mes amies surtout Selma et Ahlem .

En témoignage de l'amitié sincère qui nous à liée Et des bons moments passés ensemble A tous les gens qui ont cru en moi et qui me donnent l'envie D'aller avant

Je veux remercier tous, votre soutien et vos encouragements me donnent La force de continuer.

« Radja»

Table des matières

Liste des tableaux

Table des figures

Résumé :

Pendant longtemps, le chaos a été considéré comme un phénomène indésirable par la communauté scientifique. Cependant, dans les années 90, des scientifiques ont réalisé que le chaos pouvait être contrôlé et ont commencé à chercher ses applications possibles. Les signaux issus des systèmes chaotiques sont imprédictibles à long terme, et présentent des propriétés proches de l'aléatoire.

Notre travail dans ce mémoire porte sur le cryptage des images par l'utilisation des propriétés remarquables du chaos. Pour ce faire, nous étudions une méthode décryptage basée sur la fonction logistique et circle map. Nous testons l'efficacité de cette méthode en appliquant le principe de l'algorithme pour différentes itérations du système de cryptage afin de mieux sécuriser l'image envoyé.

L'opération de décryptage est ensuite exécutée pour récupérer le message d'origine à partir du message chiffré. Une clé particulière est choisie pour assurer la confidentialité des informations contre tous ceux qui ne sont pas autorisés à recevoir le message d'origine.

Mots clés: Chaos, Cryptage, Décryptage, Fonction logistique, Cercle map.

Abstract :

For a long time, chaos has been regarded as an undesirable phenomenon by the scientific community. However, in the 1990s, scientists realized that chaos could be controlled and began to search for its possible applications.

The signals from the chaotic systems are unpredictable long-term, and have properties close to the random.

Our work in this paper deals with the encryption of images by using the remarkable properties of chaos. To do this we study a decryption method based on the logistic function. We test the efficiency of this method by applying the principle of the algorithm for different itération of the encryption system in order to better secure the image sent.

The decryption operation is then executed to retrieve the original image from the encrypted image. A particular key is chosen to ensure the confidentiality of the information against all those who are not allowed to receive the original message.

Keywords: Chaos, Encryption, Decryption, Logistic function, Cercle map.

Introduction générale

De puis le début des civilisations, l'homme n'a cessé de développer et de diffuser les moyens de communication pour transmettre des informations et des données personnelles ou confidentielles (images, signes, signal etc..), il cherchait à les protéger contre toutes les attaques et les violations.

Aujourd'hui,avec le développement technologique rapide, les méthodes de protection sont devenues plus fortes et plus sûrs, mais elles ont également généré des moyens très avancés d'espionnage, de falsification et de piratage.

À cet égard, plusieurs solutions ont été proposées, telles que : la cryptographie.

La cryptographie est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger une information ,on lui applique une transformation qui le rend incompréhensible ; c'est ce qu'on appelle le chiffrement, qu'à partir d'une information originale , donne une autre chiffré ou cryptogramme. Inversement, le déchiffrement est l'action qui permet de reconstruire l'information originale à partir de l'information chiffré.

La cryptographie englobe plusieurs techniques et méthodes telles que la cryptographie à clé publique, la cryptographie à clé privée, la cryptographie hybride, la cryptographie quantique et la cryptographie basée sur chaos.

L'idée de base de la cryptographie chaotique est de brouiller un message adéquatement avec le chaos au niveau de l'émetteur, afin de le dissimuler des intrus, avant de le transmettre à sa destination qui sera la seule capable de le déchiffrer.

Les algorithmes basés sur le chaos ont montré leurs performances supérieures, Ils sont un phénomène d'apparence aléatoire mais qui est déterministe à l'origine pour le masquage d'information.

Le travail présenté dans ce mémoire se situe dans le cadre des approches qui proposent l'usage du chaos pour sécuriser les données. Il consiste à définir un nouveau système

chaotique par la fusion des deux systèmes chaotiques basé sur la fonction logistique et circle map.

Notre objectif est d'implémenter cette méthode pour le chiffrement et le déchiffrement des images.

Organisation du mémoire

Le travail de ce mémoire est organisé de la façon suivante :

Dans le premier chapitre on va citer les propriétés des systèmes dynamiques en général, et les systèmes chaotiques en particulier. On va parler des notions de stabilité, de bifurcation. Ainsi, on va présenter les systèmes dissipatifs en passant par l'étude du voisinage du point d'équilibre, les systèmes entretenus et la section de Poincaré. Ensuite, des exemples les plus trouvés dans la littérature, vont être évoqué.

Le deuxième chapitre sera consacré à la cryptographie chaotique. Il aborde la notion de la cryptographie et son objectif, le principal schéma de chiffrement et de déchiffrement en cryptographie usuelle, la cryptographie classique, le chiffrement à clé publique et le chiffrement symétrique par blocs ou par flot sont décrit, puis on illustre, le chiffrement asymétrique, hybride, et le chiffrement quantique,ensuite la communication sécurisé par le chaos et ses propriétés, aussi on va parcourir les différents méthodes de la synchronisation des systèmes chaotiques, De plus le principe du crypto-système basées sur le chaos est décrit. Plusieurs modes de chiffrement d'information incluant une dynamique chaotique proposés dans la littérature sont présentés : le chiffrement par addition, par commutation, la modulation paramétrique, et le chiffrement par inclusion et mixte.

Le troisième chapitre sera consacré pour présenter un état de l'art sur les différentes techniques de cryptage utilisant le chaos proposé par les chercheurs du domaine de cryptage d'image.

le dernier chapitre est dédié à l'étude détaillée de notre système de chiffrement chaotique basé sur la fusion de la fonction logistique et circle map , nous présentons le processus de chiffrement/déchiffrement utilisant le modèle, et les résultats obtenus en simulant ce dernier et des analyses des performances.

Nous clôturons ce manuscrit par une conclusion générale qui présente le bilan du travail réalisé.

Chapitre 1

Système dynamique et théorie du chaos

Introduction

La notion du temps dans l'étude des modèles physiques et mathématiques remonte à Galilée, qui est le premier à introduire cette notion dans l'étude de la chute des corps et le mouvement de la terre autour du soleil, cette introduction du temps dans les équations est ce qui s'appellera l'étude des système dynamique. au XVIII siècle, Isaac Newton a défini l'équivalence masse-énergie et trouve de manière explicite la cause de certains mouvements apparemment désordonnés. Il parle de déterminisme.

Selon cette vision, tout semblait aussi être parfaitement prédictible et causal. Le futur devenait prévisible : il suffisait de traduire le mouvement en équations différentielles et de les résoudre [1].

En général, un système dynamique décrit des phénomènes qui évoluent au cours du temps. Le terme « système » fait référence à un ensemble de variables d'état (dont la valeur évolue au cours du temps) et aux interactions entre ces variables.

1.1 Un peu d'histoire

La science du 20ème siècle a été marqué par trois découvertes majeures : La relativité, La mécanique quantique et le chaos.

Selon le philosophe Daniel Parrochia [2], la théorie du chaos constitue une des trois grandes révolutions scientifiques du dix-neuvième siècle et correspond à un changement de paradigme comparable à ceux qu'entrainèrent la théorie de la relativité et la mécanique quantique. Ce siècle a vu s'écrouler l'un après l'autre les murs de certitudes qui entouraient la forteresse de la physique newtonienne. Einstein avec sa théorie de la relativité a éliminé en 1905 l'illusion newtonienne d'un espace et d'un temps absolus. dans les années 1920 à 1930, la mécanique quantique a détruit la certitude de tout pouvoir mesurer aussi précisément que possible.

A la fin du dix-neuvième siècle, Henri Poincaré réussit à mettre en évidence la possibilité de comportements irréguliers dans les systèmes déterministes. C'est Edward Lorenz, un météorologue américain qui fut le premier à comprendre et à déterminer un modèle mathématique du chaos, mais comme conclusion de l'histoire de naissance de la théorie du chaos, elle est le résultat d'une confrontation entre l'histoire de longue durée, qui trouve ses racines au dix-neuvième siècle dans les travaux d'Henri Poincaré, et une période de reconfiguration, constituée par les travaux séminaires d'Edward Lorenz, Stephen Smale, David Ruelle et Floris Talkens.

Le chaos est un phénomène qui se produit largement dans les systèmes dynamiques, de point de vue pédagogique ce phénomène a été considéré complexe et n'a jamais été donné de l'importance, parce qu'il n'y avait aucune analyse simple disponible qui pourrait aider les étudiants et les chercheurs à immerger dans ce phénomène intéressant et obtenir des outils et des expériences.

Depuis la présence de chaos s'est répandu dans beaucoup de champs, c'est bon d'avoir quelque perspicacité dans ce droit du phénomène du niveau haut [3].

1.2 Systèmes dynamiques

Un système dynamique peut être représenté par un ensemble de variables. Ces variables peuvent être destinées pour l'étude des fluctuations d'état d'un phénomène ou d'un objet quelconque, qui évoluent au cours du temps de façon à la fois :

- **Causale**, c'est-à-dire son avenir ne dépend que de phénomènes du passé ou du présent.
- **Déterministe**, c'est-à-dire qu'à partir d'une condition initiale donnée à l'instant présent va correspondre à chaque instant ultérieur un et un seul état futur possible.

L'évolution déterministe du système dynamique peut alors se modéliser de deux façons :

-une évolution **continue** dans le temps, représentée par une équation différentielle.

-une évolution **discrète** dans le temps, ce second cas est souvent le plus simple à décrire mathématiquement, l'étude théorique de ces modèles discrets est fondamentale, car elle permet de mettre en évidence des résultats importants, qui se généralisent souvent aux évolutions dynamiques continues. Elle est représentée par le modèle général des équations aux différences finies.

1.2.1 Temps discret

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

$$x(k+1) = G(x(k), k) \tag{1.1}$$

$G : \mathbb{R}^n.\mathbb{Z}^+ \to \mathbb{R}^n$, indique la dynamique du système en temps discret.
On peut également identifier pour chaque couple (x_0, k_0) une solution unique :

$$\varphi_G = (x_0, k_0)\mathbb{Z}^+ \to \mathbb{R}^n$$

tel que :

$$Q_G(K_0; x_0, k) = X_0 et Q_G(K+1; x_0, k_0) = G(Q_G(K; x_0, k_0), K) \tag{1.2}$$

En temps discret, on définit aussi le système autonome comme une dynamique qui ne dépend pas de l'instant k [1].

$$x(k+1) = G(x(k)), \tag{1.3}$$

1.2.2 Temps continu

Dans ce cas, le système dynamique peut-être modélisée mathématiquement par un système d'équations différentielles ordinaires :

$$X(t) = F(x(t), t), \tag{1.4}$$

où, $F = \mathbb{R}^n.\mathbb{R}^+ \to \mathbb{R}^n$indique la dynamique du système.
Si on associe à cette dynamique un état initial $X_0 = X(t_0)$ Pour chaque couple choisi (X_0, t_0),on peut identifier une solution unique :

$$\varphi(K_0; x_0, t_0) : \mathbb{R}^+ \to \mathbb{R}^n,$$

tel que :

$$\varphi_f(t_0; x_0, t_0) = X_0 et \varphi_f(t; x_0, t_0) = F(\varphi_f(t; x_0, t_0)), t), \tag{1.5}$$

Cette solution unique déterminée à l'aide des équations **(1.5)** appelée souvent trajectoire, qui fournit l'ensemble d'états successifs occupés par les systèmes à chaque instant t [4].

On considère l'exemple du célèbre système différentiel de Lorenz (cf :section 1.13.2) donné par les équations suivantes :

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y - x), \\ \frac{dy}{dt} &= x(\rho - z) - y, \\ \frac{dz}{dt} &= xy - \beta z. \end{aligned} \tag{1.6}$$

Les paramètres pour l'exemple de trajectoire donné dans l'équation **(1.4)** ont été choisis de la manière suivante : $\sigma = 10$, $\rho = 28$, $\beta = 8/3$ avec la condition initiale $(x_0, y_0, z_0) = (2, 5, 20)$.

- ce système présente un superbe attracteur étrange en forme d'ailes de **papillon**.

- on observe que la dynamique du système de Lorenz donnée par les équations **(1.6)**est indépendante de l'instant **t** considérée.

- généralement ce type de système est qualifié d'autonome[1].

La dynamique, dans ce cas particuliers, a la forme suivante :

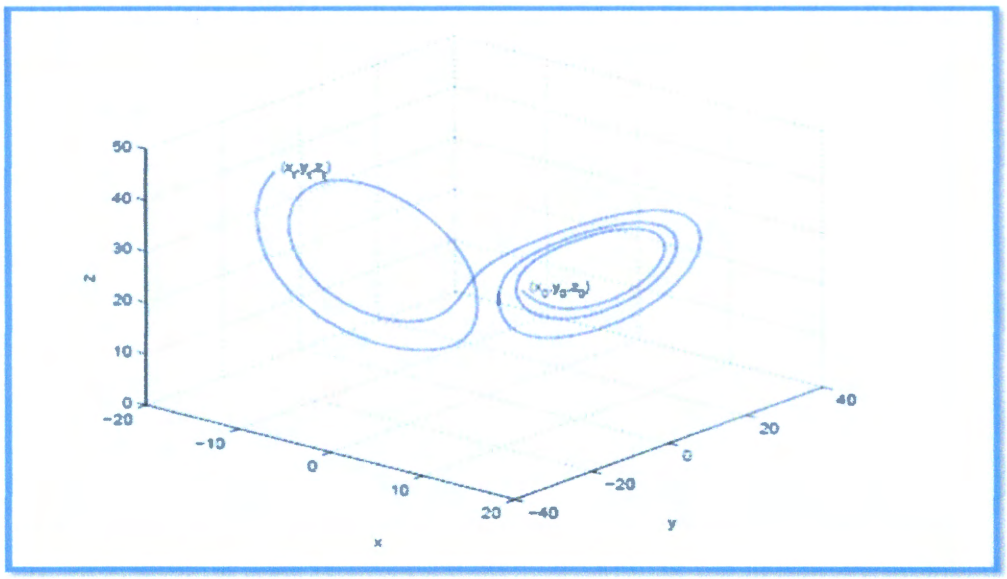

FIGURE 1.1 – Exemple de trajectoire du le système Lorenz [3].

1.3 Comportement des systèmes dynamiques

1.3.1 Point d'équilibre

Dans ce cas, la solution asymptotique est représentée par un point, sa valeur étant déterminée en fonction de la condition initiale choisie. Ainsi, pour des conditions initiales différentes on peut retrouver plusieurs points d'équilibres. De même ces points peuvent être stables ou instables suivant que les trajectoires voisines convergent ou divergent entre elles.

Dans le cas de la dynamique logistique **(cf.section 1.12.2)**, on observe que pour toute valeur $\mathbf{r} \in [1, 3]$,le régime permanent est formé par un point limite stable, sa valeur étant dépendante du choix de paramètre **r**.

la **figure 1.2** nous donne un aperçu d'une telle trajectoire pour $\mathbf{r = 2}$. Ainsi on observe qu'après une période de transition relativement courte, la séquence se stabilise autour du point fixe qui cette fois est $\mathbf{x = 0.5}$.

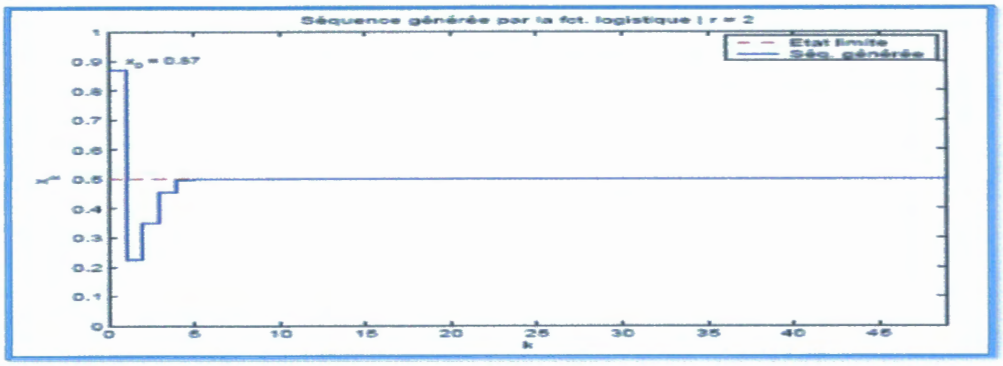

FIGURE 1.2 – Les états limites et séquence générée pour r = 2.

1.3.2 Régime périodique

Le régime périodique correspond à une trajectoire dont les répliques d'une portion élémentaire sont séparées à des intervalles **nT**, $n \in \mathbb{N}+$,**T** désigne la période.

FIGURE 1.3 – Les états limites et séquence générée pour r = 3.2.

1.3.3 Régime quasi-périodique

Un régime quasi-périodique peut être représenté dans l'espace d'état par un tore. Il correspond à une somme de résultats périodiques, dont le rapport des périodes est un nombre irrationnel.

1.3.4 Régime chaotique

Par définition, le régime chaotique est tout régime permanent qui n'appartient à aucune des classes montrées antérieurement.

Une telle solution a une trajectoire asymptotique bornée avec une extrême sensibilité aux conditions initiales, cette sensibilité par rapport aux conditions initiales traduit aussi le comportement, en apparence stochastique, des générateurs chaotiques, de telle sorte qu'une prévision à long terme du comportement du système est impossible.

La **figure 1.4** illustre pour deux conditions initiales séparées par une valeur de 10^4. On remarque que juste après quelques itérations, les deux trajectoires divergent et deviennent non corrélées.

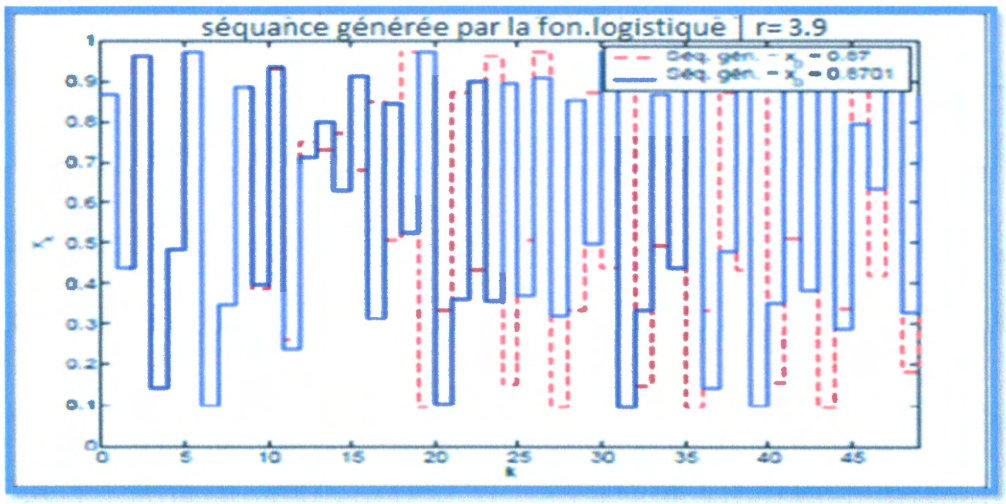

FIGURE 1.4 – Sensibilité aux conditions initiales pour r = 3.9.

1.4 Définition du chaos

Le chaos est défini généralement comme un comportement particulier d'un système dynamique déterministe non-linéaire. Il présente un aspect fondamental d'instabilité appelé sensibilité aux conditions initiales, ce qui le rend imprédictible en pratique à long terme. Une autre caractéristique du système chaotique est son évolution qui semble aléatoire.

1.5 Différence entre le chaos et l'aléatoire

La différence entre le chaos et l'aléatoire nous a paru le point le plus important de la compréhension du chaos. En effet, on a toujours tendance à considérer qu'un phénomène tire son imprédictibilité du nombre trop important de paramètres en jeu dans sa description. Ce qui nous pousse à en donner une approche probabiliste qui peut être parfaitement satisfaisante, garde par définition une certaine marge d'aléatoire.

En ce qui concerne le chaos, il n'en est rien, les systèmes chaotiques se comportent, en effet, d'une manière qui peut sembler aléatoire, mais ce comportement est en fait décrit de manière déterministe par des équations non linéaires parfaitement déterministes, c'est-à-dire en particulier avec des outils mathématiques permettant une approche précise et certaine [6].

1.6 L'évolution vers le chaos

Il y a plusieurs types d'évolution possibles d'un système dynamique régulier vers le chaos, nous allons en exposer brièvement deux, ces évolutions surviennent par augmentation des contraintes appliquées au système comme les vitesses angulaires dans le cadre des pendules.

a) Par intermittences :

Le système conserve pendant un certain laps de temps un régime périodique, c'est à dire une certaine "régularité", et il se déstabilise, brutalement, pour donner lieu à une sorte d'explosion chaotique. Il se stabilise de nouveau ensuite,pour donner lieu à une nouvelle "bouffée" plus tard.

On a constaté que la fréquence et la durée des phases chaotiques avaient tendance à s'accroître plus on s'éloignait de la valeur critique de la contrainte ayant conduit à leur apparition [6].

b) Par doublement de la période :

Par augmentation du paramètre de contrôle de l'expérience, la fréquence du régime périodique double, puis est multipliée par 4,par 8,par 16...etc.

Les doublements étant de plus en plus rapprochés, on tend vers un point d'accumulation auquel on obtiendrait hypothétiquement une fréquence infinie. C'est à ce moment que le système devient chaotique [6].

1.7 Avantages du chaos

- Les systèmes chaotiques possèdent une infinité de trajectoires non périodiques denses.

- Les systèmes chaotiques très sensible aux conditions initiales.

- Les propriétés des systèmes chaotiques nous permettent de générer un nombre infini de signaux chaotique non corrélé d'un même système en utilisant différentes valeurs initiales, ceci peut être employé pour générer des séries de nombres pseudo-aléatoires.

- Les série est très utile dans certains cryptosystèmes traditionnels ou dans le protocole de Tcp/Ip.

- Les systèmes chaotiques employés pour crypter les messages [2].

1.8 Systèmes Dynamiques chaotiques

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. Les systèmes chaotiques ont un comportement infiniment complexe.

On appelle donc un système dynamique chaotique, un système qui dépend de plusieurs paramètres et qui est caractérisé par une extrême sensibilité aux conditions initiales et une forte récurrence [3].

Il n'est pas déterminé ou modélisé 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 [7].

1.9 Caractéristiques des systèmes chaotiques

On va présenter quelques caractéristiques qui permettent de comprendre qualitativement les points marquants d'un système chaotique [8].

a) Non-linéarité :

Un système chaotique est un système dynamique non linéaire.

un système linéaire ne peut pas être chaotique. On parle de non linéarité lorsque l'entrée d'un système n'est pas proportionnelle à sa sortie, ou lorsqu'un événement a des imprévisibles à long terme [8]. La notion de système dynamique chaotique est relative à tous les systèmes dont l'évolution dépend du temps. l'évolution irrégulière du comportement d'un système chaotique est due aux non linéarités.

b) Déterminisme :

Un système chaotique a des règles fondamentales déterministes et non probabilistes. La notion de déterminisme signifie la capacité de " prédire " le future d'un phénomène à partir d'un évènement passé ou présent.

c) Sensibilité aux conditions initiales :

Certains phénomènes dynamiques non linéaires sont sensibles aux conditions initiales que, même s'ils sont régis par des lois rigoureuses et parfaitement déterministes, les prédictions exactes sont impossibles.

Une autre propriété des phénomènes chaotiques est qu'ils sont très sensibles aux perturbations. L'un des premiers chercheurs à s'en être aperçu fut Edward Lorenz qui s'intéressait à la météorologie et par conséquent aux mouvements turbulents d'un fluide comme l'atmosphère [12].

Lorenz venait de découvrir que dans des systèmes non linéaires, d'infimes différences dans les conditions initiales engendraient à la longue des trajectoires totalement différentes. Il a illustré ce fait par l'effet papillon.

Il est clair que la moindre erreur ou imprécision sur la condition initiale interdit de décider à tout temps quelle sera la trajectoire effectivement suivie et, en conséquence, de faire une prédiction sur l'évolution à long terme du système.

Une des propriétés essentielles du chaos est donc bien cette sensibilité aux conditions initiales que l'on peut caractériser en mesurant des taux de divergence des trajectoires.

d) Imprévisibilité :

En raison de la sensibilité aux conditions initiales, qui peuvent être connues seulement à un degré fini de précision. Le chaos ne signifie pas l'absence d'ordre, il se rattache plutôt à une notion d'impossibilité de prévoir une évolution à long terme du fait que l'état final dépend de manière si sensible de l'état initial.

e) Aspect aléatoire

Une autre caractéristique des systèmes chaotiques peut être observée sur les courbes de la **Figure 1.5**. En effet, un système chaotique évolue d'une manière qui semble être aléatoire. La **Figure 1.5** permet de comparer l'évolution périodique est donc prédictible d'un système classique avec l'évolution plus complexe, non périodique et non prédictible du système chaotique de Lorenz.

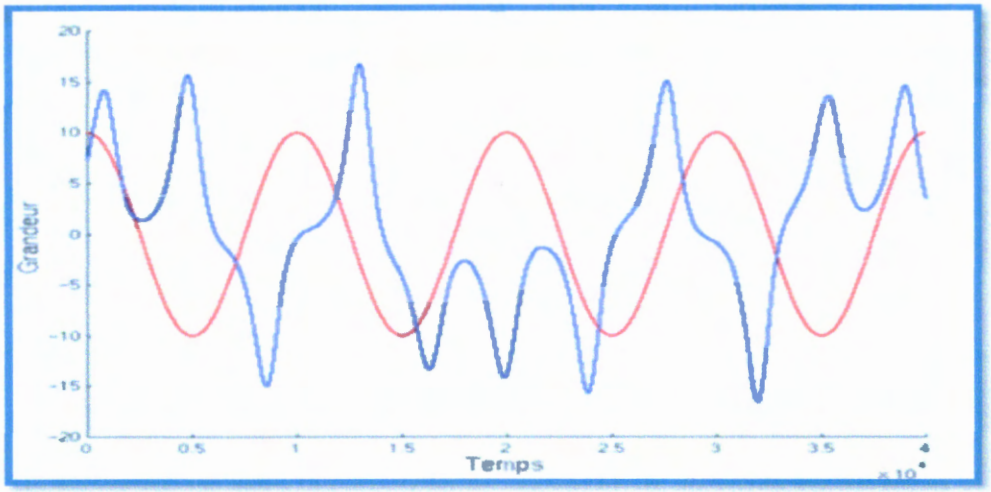

FIGURE 1.5 – Evolution dans le temps d'un système chaotique,comparé à une sinusoïde.

f) Attracteur étrange

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

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.

❖ Attracteurs réguliers

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

a) un point fixe :

La trajectoire du pendule dissipatif simple (dans l'espace des phases représentant son altitude et sa vitesse), par exemple, tend vers l'origine du repère, quelles que soient la position et la vitesse initiales. C'est-à-dire pour un point fixe stable, un écartement de sa position initiale dû à une quelconque perturbation n'aura aucune influence (**Figure 1.6 (a)**). Le mouvement perturbé s'atténuera pour faire revenir l'état du système à sa position initiale.

b) un cycle limite :

La trajectoire du pendule idéal dans ce même espace des phases, par exemple pour tous les attracteurs réguliers, c'est à dire 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[6].

Il sera caractéristique d'un mouvement périodique entretenu (apport d'énergie extérieure pour composer la dissipation). Le système ne revient pas à une position initiale mais y repassera après avoir parcouru le cycle.Sa représentation graphique dans l'espace des phases (**Figure 1.6 (b)**) est une courbe fermée.

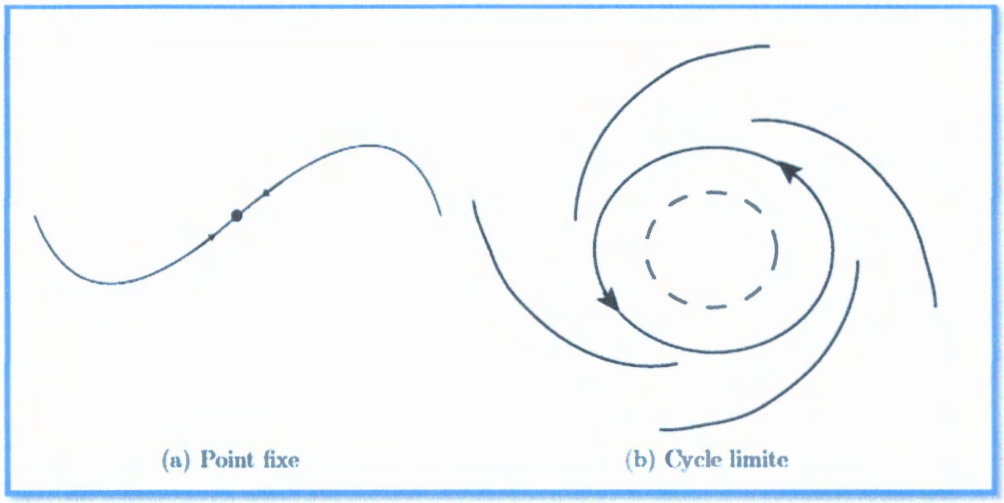

FIGURE 1.6 – Deux exemples d'attracteurs réguliers dans un espace de phase 2D.

✥ Attracteurs étranges

Les attracteurs étranges sont caractéristiques de l'évolution des systèmes chaotiques : au bout d'un certain temps, tous les points de l'espace des phases (et appartenant au bassin d'attraction de l'attracteur) donnent des trajectoires qui tendent à former l'attracteur étrange.

A grande échelle, un attracteur 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, l'attracteur doit se replier sur lui-même.

Le processus d'étirement-repliement se répète à l'infini et fait apparaître un nombre infini de "plis" imbriqués les uns dans les autres qui ne se recoupent jamais. Ainsi, deux points très proches au départ (conditions initiales) peuvent se retrouver à deux extrémités opposées de l'attracteur (conditions finales). Cela traduit le comportement divergent des phénomènes chaotiques. On obtient ainsi des attracteurs différents (en fonction des systèmes étudiés), qui présentent des formes diverses et surprenantes[6].

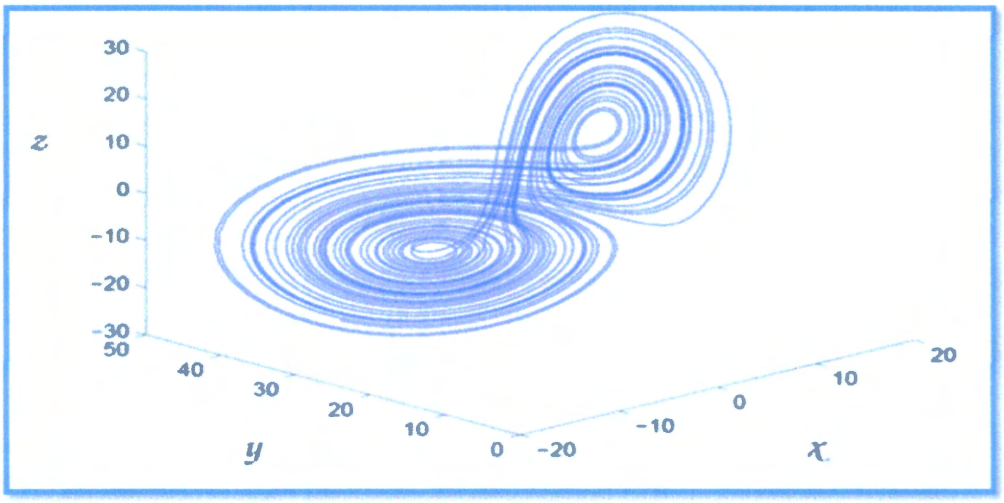

FIGURE 1.7 – Attracteurs étranges.

1.10 Outils d'étude des systèmes chaotiques

a) Espace de phase

L'espace des phases est une structure correspondant à un certain nombre de variables d'état qui ont la propriété de définir complètement l'état du système à un instant donné.

L'évolution de chacune de ces variables d'état est responsable du comportement dynamique du système.

Cet espace est appelé l'espace de phase où chaque point définit un état,et le point agrégé a cet état décrit une trajectoire.

b) Fractale

Un objet fractal est doté d'une propriété dite d'auto-similitude. Ce phénomène est observé dans les systèmes chaotiques,c'est-à-dire qu'on y observe une invariance par changement d'échelle.

Si l'on zoome d'un facteur suffisant sur une partie de la courbe, on retrouve la structure et la topologie de celle-ci à sa taille initiale.Un zoom plus grossissant encore reproduit le phénomène, aussi loin qu'on puisse aller.

c) Exposants de Lyapunov

L'évolution chaotique et difficile à appréhender car la divergence des trajectoires sur l'attracteur est rapide.

Pour cette raison on essaye 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.

d) Section de Poincaré

Dans l'espace de phase, la direction tangentielle à la trajectoire d'un système autonome peut changer si on change les paramètres du temps, et par conséquent ne traduit pas la géométrie de l'attracteur. Ainsi, la composante tangentielle des points x_k peut être négligée, réduisant ainsi la dimension de l'espace de phase par 1, et transformant la trajectoire continue en une trajectoire discrète.

Cette méthode s'appelle la section de Poincaré, et se résume à choisir une surface Σ dans l'espace de phase et de construire une application inversible P sur cette surface traduisant la relation entre les points d'intersections successives entre la trajectoire et la surface [4].
La **Figure 1.8** illustre le principe :

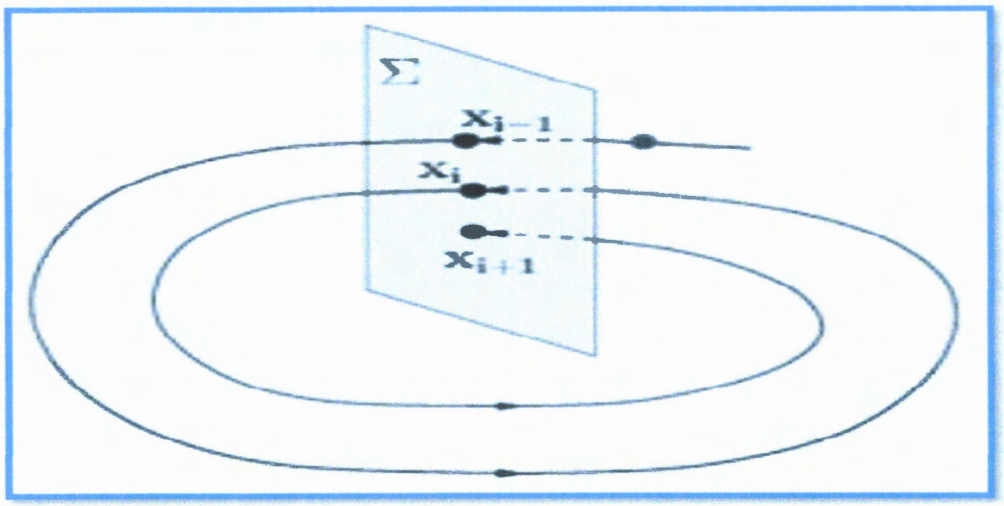

FIGURE 1.8 – Construction de la section de Poincaré.

Le temps discret résultant de l'intersection est variable,et pas nécessairement proportionnel au temps d'intégration Δt. Le nombre de points d'intersection obtenu dépend sensiblement de la surface choisie. Un choix standard de la surface est la section à phase constante où la durée écoulée entre deux intersections est constante.

e) Dimension de l'attracteur

Les attracteurs des systèmes chaotiques dissipatifs,où les trajectoires éloignées rétrécissent vers l'intérieur d'un méta-cube, ont généralement une géométrie très complexe, d'où l'appellation d'attracteurs étranges comme mentionné précédemment.

f) Notion de Bifurcation

Le terme bifurcation veut dire division d'une branche principale en au moins deux branches. Le comportement d'un système dynamique non-linéaire peut changer quand un paramètre du système change. Ce changement de comportement correspond à un phénomène de bifurcation, il est accompagné d'un changement de type de stabilité.

Le terme de bifurcation est utilisé pour désigner dans un sens large, toute modification qualitative du comportement d'un système dynamique, suite à la variation de l'un des paramètres dont dépend le système étudié.
Il existe plusieurs types de bifurcations, parmi lesquelles on peut citer : bifurcation stationnaire, bifurcation col noeud... [9].

•Bifurcation stationnaire

Dans une bifurcation stationnaire, une seule valeur propre réelle quitte la zone de stabilité. Elle survient dans les systèmes dynamiques continus, quand la valeur propre traverse l'axe imaginaire, et dans les systèmes dynamiques discrets quand une valeur propre quitte le cercle unitaire auteur de l'origine.

•Bifurcation col noeud

La bifurcation col-noeud est le cas le plus simple de bifurcation. Elle peut survenir dans un système qui n'a pas de points fixes.
Au point de bifurcation deux points fixes vont apparaître, l'un stable est l'autre instable [10]. Par exemple, pour le système à une dimension :

$$\dot{x} = f(x;r) = r - x^2 \tag{1.7}$$

Où, 'r' représente le paramètre de contrôle, ce système possède un point fixe,

$$x_{f,1} = 0, \ \grave{a} \quad r_0 = 0, \tag{1.8}$$

et une courbe d'équilibre,

$$(x_f)^2 = r, \ r \geq 0 \tag{1.9}$$

où $xf_{,2} = \sqrt{r}$ est stable et $x_{f,3} = -\sqrt{r}$ est instable pour,$r \geqslant 0$,

•Bifurcation par doublement de période

Un autre type de bifurcation aussi important, est la bifurcation par doublement de période. Pour ce type de bifurcation, une valeur propre réelle franchit la zone de stabilité à la valeur d'un (système discret). En un point de bifurcation, un cycle limite de période 2^k bifurque et donne naissance à un cycle limite de période2^{k+1} et ainsi de suite jusqu'à aboutir à un comportement chaotique.

•Bifurcation de pitchfork

Les bifurcations de pitchfork sont possibles dans les systèmes dynamiques avec inversion ou symétrie. Ce type de système a un point fixe ou un cycle limite symétrique. Au point de bifurcation, la stabilité de la solution change et une nouvelle paire d'état d'équilibre se crée. La bifurcation de pitchfork peut être stable (supercritique) ou instable (subcritique) comme le montre la **Figure 1.9**.

Soit le système à une dimension :

$$x = f(x;r) = r - x \tag{1.10}$$

il possède un point d'équilibre,

$$x_{f,1} = 0, \grave{a} r_0 = 0 \tag{1.11}$$

et une courbe d'équilibre,

$$(xf)^2 = r, r \geqslant 0, \tag{1.12}$$

la jacobéenne est :

$$j = r - 3(xf)^2 \tag{1.13}$$

Donc : $x_{f,1} = 0$ est instable pour $r > r_0 = 0$, et stable pour $r < r_0 = 0$.

De plus, la courbe d'équilibre est donnée par : $x_{f,2} = r$ est stable pour tous $r > 0$ pour lesquels la jacobéenne est j= $-2r$.

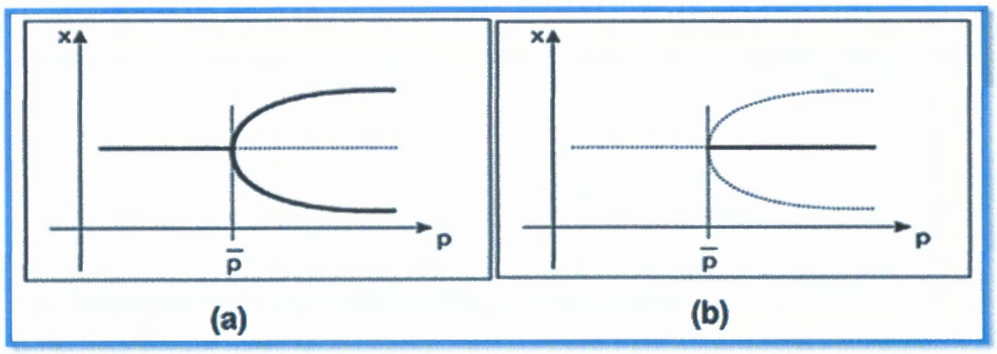

FIGURE 1.9 – (a) Bifurcation supercritique, (b) Bifurcation subcritique.

•Diagramme de bifurcation :

Dans ce cas, prenant l'exemple de la fonction logistique (cf.la section suivante) on peut s'intéresser à la construction d'un diagramme représentant l'évolution de population x_n en fonction du paramètre **r**. Les différents calculs pour voire l'évolution du système en fonction de la valeur de r, montrent qu'il existe un « trajet » qui mène d'un état l'ordre à un autre état le chaos pour des valeurs de r variant de 1 à 4 avec un pas de 0.001, et 50 itérations sur **xn** on obtient le diagramme de la **Figure 1.10**.

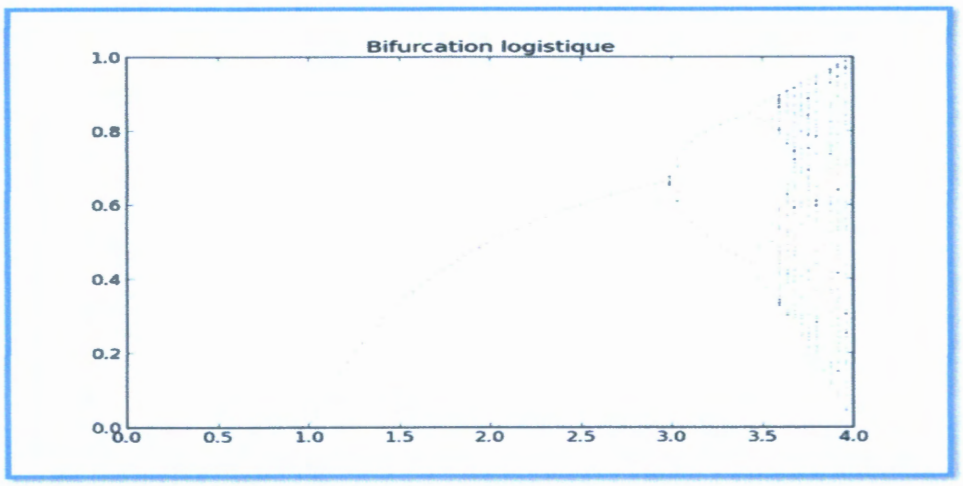

FIGURE 1.10 – Diagramme de bifurcation de la fonction logistique.

1.11 Cartes chaotiques

Parmi les nombreuses cartes chaotiques de la littérature, nous présentons très brièvement ci-dessous seulement les équations de trois cartes chaotiques très utilisées en pratique qui sont : la carte logistique, la carte PWLCM (Piece Wise Linear Chaotic Map) et la carte Skewtent, Ces cartes possèdent plusieurs bonnes propriétés : réalisation simple, et généralement assez bonne propriété cryptographique [15].

a) La carte d'ARNOLD

La carte chaotique appelée la carte d'Arnold en reconnaissance de mathématicien russe Vladimir I. Arnold, qui l'a découverte en utilisant une image d'un chat. C'est une démonstration et une illustration simple et élégante de certains des principes de chaos, une évolution apparemment aléatoire d'un système.

Si nous considérons $X = \begin{pmatrix} x \\ y \end{pmatrix}$, une matrice de taille n x n, la transformation d'Arnold T est :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ x+2y \end{pmatrix} mod\ n \tag{1.14}$$

b) Logistique map

Une suite logistique est une suite simple, dont la récurrence n'est pas linéaire et donnée par la relation suivante.

$$x(n+1) = rx(n)(1 - x(n)) \tag{1.15}$$

x est la variable dynamique prenant des valeurs entre **0** et **1** non inclus et **r** est le paramètre

du système. Selon la valeur de **r**,la suite peut être un point fixe, une suite périodique de période 2, 4, 8,..., et 64, pour **r = 3,569692**,ou une suite chaotique pour **r** compris entre **3,56996** et **4**.

c) Carte PWLCM (Piece Wise Linear Chaotic Map)

La carte chaotique Piece Wise Linear Chaotic Map (PWLCM)[14] est composée de plusieurs segments linéaires par morceaux dont l'équation est donnée par :

$$x(n) = \begin{cases} x(n-1) \times \frac{1}{p} & si\ 0 \leq x(n-1) < p \\ [x(n-1) - p] \times \frac{1}{0.5-p} & si\ p \leq x(n-1) < 0.5 \\ F[1 - x(n-1)] & si\ 0.5 \leq x(n-1) < 1 \end{cases} \quad (1.16)$$

p ∈[0, 0.5] est le paramètre de contrôle et x (0) ∈[0, 1[est la valeur initiale.

La **Figure 1.11 (a)** ci-dessous représente la forme temporelle de la fonction PWLCM pour 300 itérations, utilisant une valeur initiale **x(0)** égale à **0.6**, et une valeur de paramètre p égale à **0.3**.

La **Figure 1.11 (b)**, représente l'attracteur,courbe [**X(n), X(n+1)**] de la carte PWLCM (tracé pour 1000 itérations).

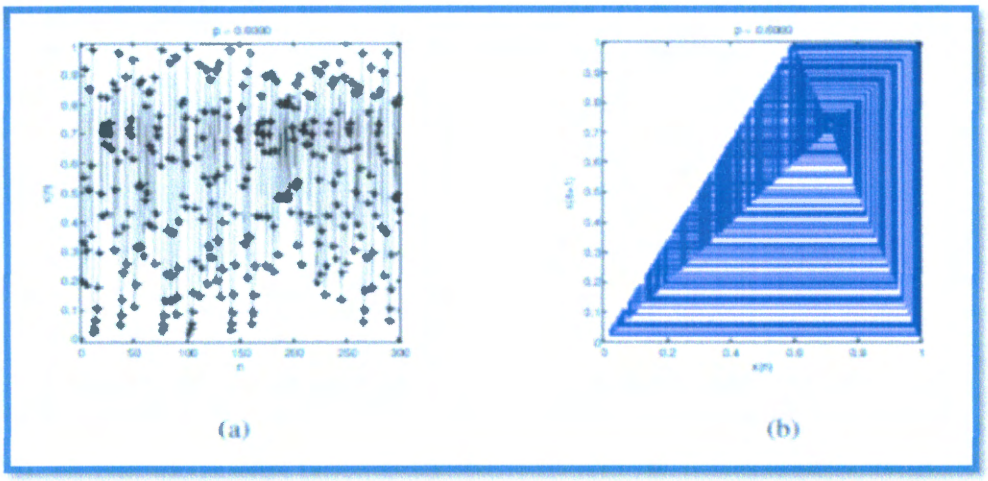

FIGURE 1.11 – carte PWLCM : (a)séquence x(n),(b) attracteur.

1.12 Exemples des systèmes chaotiques

Dans ce qui suit, nous présentons quelques exemples de systèmes chaotiques les plus célèbre.

1.12.1 Systèmes à temps discret

•Système de Hénon

La récurrence de Hénon est un modèle proposé en 1976 par le mathématicien Michel Hénon [11], le modèle d'état associé est :

$$\begin{cases} x_{n+1} = y_n + 1 - ax_n^2, \\ y_{n+1} = bx_n \end{cases} \tag{1.17}$$

tel que $(x_n, y_n) \in \mathbb{R}^2$, a et b représentent des paramètres.

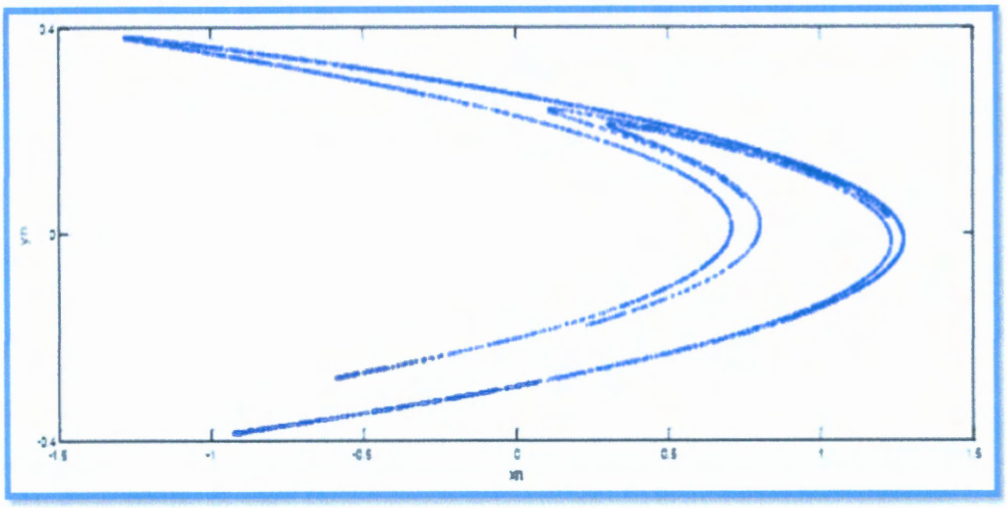

FIGURE 1.12 – Attracteur chaotique de Hénon.

•Système de Lozi

La récurrence de Lozi est obtenue en remplaçant $(x_k)^2$ dans la Système de Hénon par $|(x_k)|$ et en modifiant la valeur des paramètres. Ce système est donnée par la représentation d'état suivante[12] :

$$\begin{cases} x_{n+1} = y_n + 1 - a|x_n|, \\ y_{n+1} = bx_n \end{cases} \tag{1.18}$$

tel que$(x_n, y_n) \in \mathbb{R}^2$,a et b représentent des paramètres. L'attracteur chaotique de Lozi est représenté sur **la Figure 1.13** pour les valeurs numériques a = 1,7 et b = 0,5.

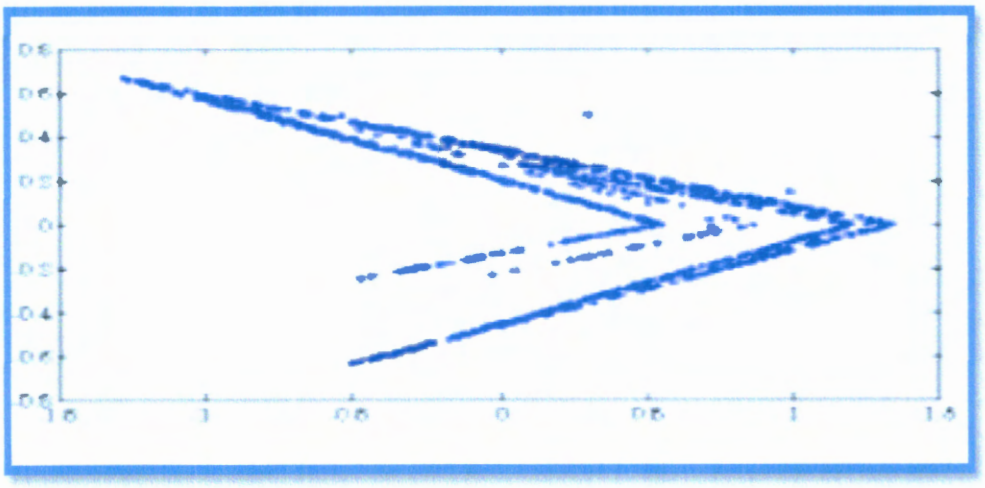

FIGURE 1.13 – Attracteur chaotique de Lozi.

1.12.2 Systèmes à temps continu

•Système de Lorenz

Le système de Lorenz est un système dynamique chaotique qui fut utilisée à l'origine pour simuler le mouvement d'une particule dans des courants de convection et des systèmes météorologiques simplifiés.

De petites différences dans les conditions initiales conduisent rapidement à des valeurs divergentes. C'est ce qu'on appelle parfois l'effet papillon.

Ce système est l'un des éléments fondât du développement de la théorie du chaos[12]. Il est utile comme source audio chaotique ou comme source de modulation basse fréquence[8].
Ce système est défini par le système d'équations différentielles couplées suivant :

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x), \\ \frac{dy}{dt} = x(\rho - z) - y, \\ \frac{dz}{dt} = xy - \beta z \end{cases} \tag{1.19}$$

σ : dépend des propriétés du fluide et caractérise la viscosité et la conductivité thermique du fluide.
ρ : en fonction du gradient de température dans la cellule.
β : varie avec la géométrie de la cellule de convection.
L'évolution dans le temps de coordonnée (x) dans l'espace de phase des valeurs numériques $\sigma = 10$, $\rho = 28$, $\beta = 8/3$ qui implique un comportement chaotique.

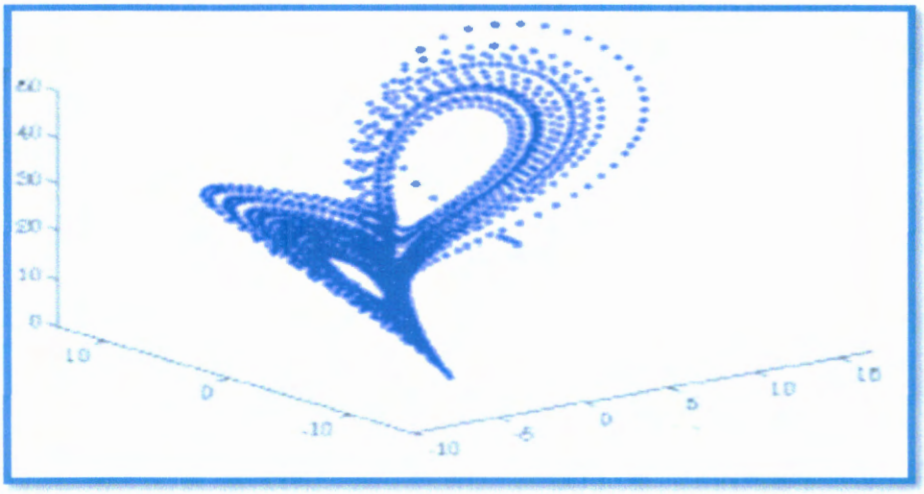

FIGURE 1.14 – Attracteur chaotique de Lorenz.

•Système de Rossler

Le système de Rossler,proposé par l'Allemand Otto Rössler est lié à l'étude de l'écoulement des fluides. Il découle des équations de Navier-Stokes. Les équations de ce système ont été découvertes à la suite de travaux en cinétique chimique. Ce système est défini par les équations suivantes [12] :

$$\begin{cases} \frac{dx}{dt} = -y - z, \\ \frac{dy}{dt} = x + ay, \\ \frac{dz}{dt} = b + z(x - c) \end{cases} \tag{1.20}$$

a , b, c représentent les paramètres du système .

L'attracteur chaotique de Rossler est donné sur la Figure 1.15 pour les valeurs numériques $a = 0{,}398, b = 2$ et $c = 4$.

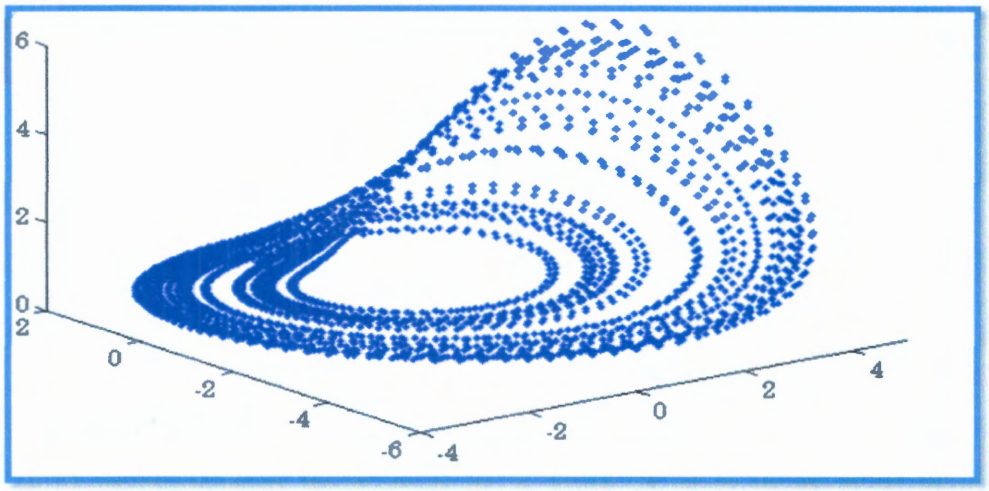

FIGURE 1.15 – Attracteur chaotique de Rossler.

conclusion

Ce chapitre avait comme objectif l'introduction de quelques notions élémentaires des systèmes dynamiques chaotiques. Dans la première section les définitions des systèmes dynamiques non-linéaires en temps continu et discret, ainsi que leurs particularisations pour le cas de systèmes chaotiques ont été données. Ensuite nous avons présenté quelques définitions et propriétés des systèmes chaotiques tel que : la non-linéarité, le déterministe, la sensibilité aux conditions initiales. Et à la fin nous avons détaillé quelques exemples des systèmes chaotiques en temps continu et discret tel que : système de Lorenz.

Chapitre 2

Cryptographie chaotique

Introduction

Dans le domaine des télécommunications, où les échanges d'informations multimédias se développent rapidement, il est indispensable de pouvoir disposer de systèmes sécurisés pour protéger les données à caractère personnel ou confidentiel et assurer la sécurité des transferts de données.

Il est donc nécessaire de développer un outil efficace de protection des données transférées et des communications contre les intrusions arbitraires. Le cryptage des données est très souvent le seul moyen efficace pour répondre à ces exigences [12].

2.1 Définition

Le terme cryptographie vient en effet des deux mots grecs : Kruptus qu'on peut traduire comme secret (caché) et Graphein pour écriture [13].

La cryptographie est une science en évolution continue, et beaucoup d'études dans ce domaine sont faites dans les laboratoires du monde entier [14].

Le but de ces recherches est de rendre les méthodes de chiffrement de plus en plus sûres (incassables même avec l'évolution technologique).

La cryptographie garantit entre autre l'intégrité, la non répudiation et l'authentification des données en plus de la confidentialité :

- **Confidentialité** : la confidentialité ou masquage des données,le contenu des données va être sauvé de toutes les personnes, machines et systèmes à l'exception de ceux qui ont le droit d'accès.

- **Authentification** : permet à l'émetteur de signer son message, ainsi, le récepteur n'aura pas de doute sur l'identité du premier.

- ✧ **Intégrité** : les données vont être protégées du changement (suppression, ajout, mise à jour) de la personne non autorisé.

- ✧ **Non-répudiation** : est la garantie qu'aucun des deux individus ayant effectué une transaction ne pourra nier avoir reçu ou envoyé les messages[13].

2.2 Processus de chiffrement et de déchiffrement

Chiffrement :
Le chiffrement est l'opération qui consiste à transformer une donnée (texte, message,...) à l'aide d'une clé, afin de la rendre incompréhensible par tous ceux qui ne sont pas autorisés à le connaître par une personne autre que celui qui a créé le message et celui qui en est le destinataire.

Déchiffrement :
Le déchiffrement est l'opération inverse du chiffrement permettant de retrouver un texte clair à partir du texte chiffré dont on possède la clé de déchiffrement.

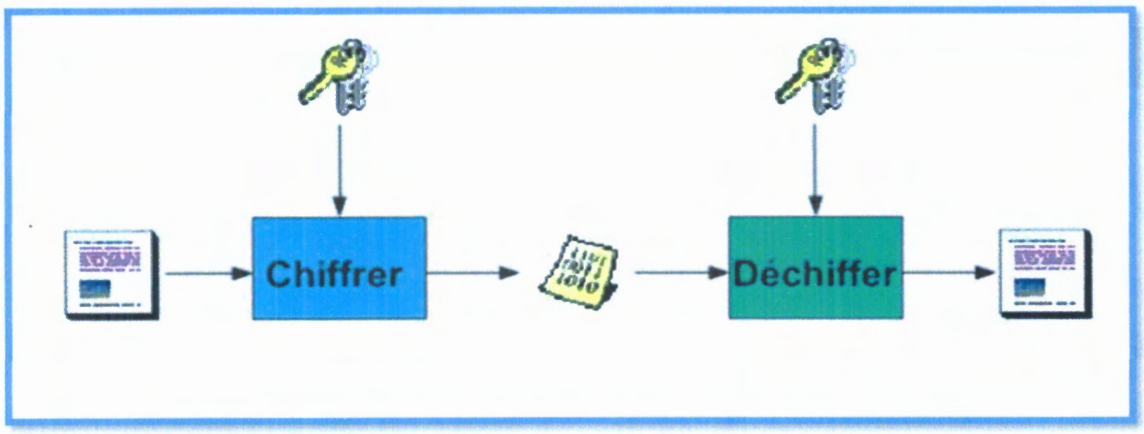

FIGURE 2.1 – Chiffrement et déchiffrement.

2.3 Aspect technique du chiffrement

Les méthodes cryptographiques peuvent être classées en trois catégories, la premiere catégorie c'est la cryptographie classique qui contient le chiffrement par substitutions et par transpositions, la deuxiéme c'est la cryptographie moderne qu'elle est aussi constituee d'un chiffrement à clé publique et d'un chiffrement à clé privée la derniere categorie c'est la

cryptographie future comme le chiffrement quantique.comme il est montré dans le schéma de la **figure 2.2** ci-dessous [14] :

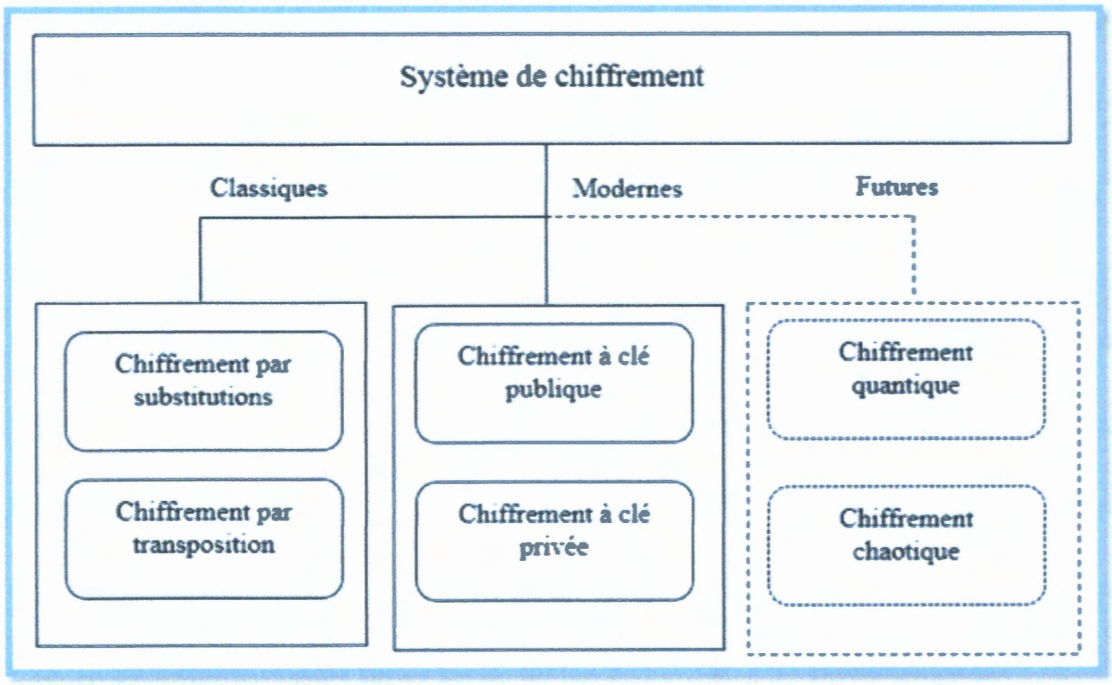

FIGURE 2.2 – Principales catégories en cryptographie [14].

2.3.1 Chiffrement classique

La cryptographie classique est la plus ancienne classe d'algorithmes de chiffrement. Elle traite des systèmes basés sur les lettres et les caractères d'une langue. On appelle cette classe de méthodes : le chiffrement à usage **restreint**.

Généralement les méthodes de chiffrement classiques reposent sur deux principes fondamentaux : la substitution et la transposition.

- ✓ **La substitution :** signifie qu'on remplace des lettres par d'autres ou par des symboles dans le but de créer de la confusion.
- ✓ **La transposition :** consiste à permuter les lettres du message afin de le rendre inintelligible [14].

2.3.2 Chiffrement moderne

De nos jours pratiquement, la cryptographie est englobée par deux grands algorithmes de chiffrement :

- les algorithmes de **chiffrement symétrique** (à clé privé) .
- les algorithmes de **chiffrement asymétrique** (à clé publique).

2.3.2.1 Chiffrement symétrique

Les algorithmes symétriques,aussi appelé chiffrement à clef secrète ou chiffrement à clef privée, utilisent la même clef pour le chiffrement et le déchirement [16].

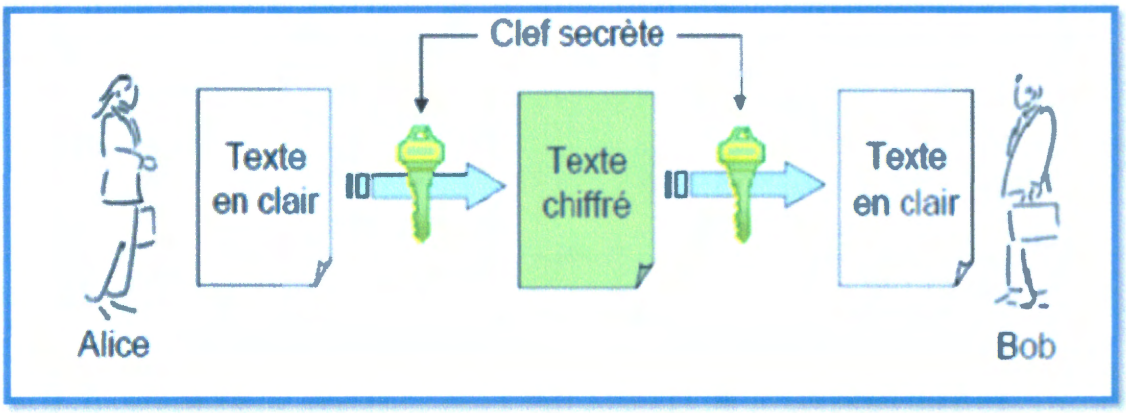

FIGURE 2.3 – Principe de chiffrement symétrique.

L'exemple historique de l'utilisation du cryptage symétrique est le fameux téléphone rouge qui reliait le Kremlin à la Maison Blanche. La clé privée était alors transmise dans une valise diplomatique. Pour une meilleure sécurité, elle était détruite et réinitialisée après chaque conversation.

Un algorithme de chiffrement symétrique est un couple de fonctions : une fonction de chiffrement **E** et une fonction de déchiffrement **D**[17].

La fonction **E** prend en entrée un message clair **m** représenté sous la forme d'une suite d'éléments d'un alphabet fini, le plus souvent égal à **0,1** et à l'aide de la clé **K** sélectionnée dans un ensemble **K**, le transforme en un message chiffré $\mathbf{c = E\ (m,\ K)}$. La fonction de déchiffrement réalise l'opération inverse $\mathbf{m = D(c,\ K)}$.

En effet, le temps de chiffrement augmente avec la taille de la clef (les processeurs actuels permettent toutefois de traiter rapidement des quantités de données importantes).

Il y a deux catégories de systèmes à clef privée : les chiffrements par **bloc** et les chiffrements par **flot**.

a. chiffrement par bloc

Les chiffrements par blocs sont des primitives cryptographiques largement répandues [18].

Un chiffrement est dit par blocs s'il divise le texte en clair en blocs de taille donnée fixe (généralement 64 ou 128 bits) puis chiffre chacun de ces blocs séparément l'un après l'autre. Les différents blocs sont combinés entre eux via un mode opératoire.

Par exemple,le mode ECB(Electronique Code Book)chiffre simplement successivement en parallèle chacun des blocs de clair. Chaque bloc de clair est combiné via un Xor avec le chiffré du bloc précédent Quel que soit le mode utilisé [19]. le chiffrement par blocs est itératif applique itérativement une fonction de tour qui constituée de combinaisons complexes de substitutions et/ou de transpositions.

Une itération est appelée un **tour** ou une **ronde**. Chaque ronde prend en entrée la sortie de la ronde précédente et à l'aide de la fonction de ronde et d'une sous-clé de ronde générée à partir de la clé secrète K fait le chiffrement de cette entrée.

La fonction de chiffrement est constituée par l'ensemble de toutes les rondes alors elle est n'est pas la fonction de ronde.

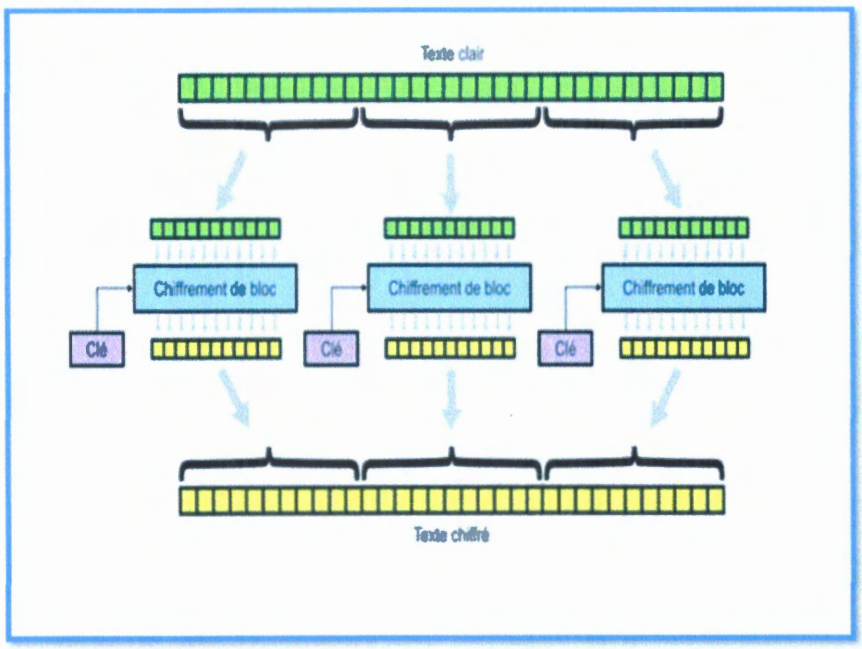

FIGURE 2.4 – Chiffrement par bloc [20].

Il existe plusieurs algorithmes de chiffrement par bloc [19], citons quelques algorithmes :

- **DES** (Data Encryption Standard).
- **3-DES** (ou triple DES).
- **IDEA** (International Data Encryption Algorithm).
- **AES** (Advanced Encryption Standard).

b. chiffrement par flot

Le chiffrement par flot et appelé aussi chiffrement en continu, ils traitent l'information bit à bit, et il sont très rapides.

Ils sont parfaitement adaptés à des moyens de calcul et de mémoire (cryptographie en temps réel), leur principe est d'effectuer un chiffrement de Vernam en utilisant une clé pseudo-aléatoire, c'est à dire une clé qui ne soit pas choisie aléatoirement parmi tous les mots binaires de longueur n.

Cette clé (qu'on appellera suite pseudo-aléatoire) est générée par différents procédés à partir d'une clé secrète d'une longueur juste suffisante pour résister aux attaques exhaustives [23], **RC4**[21] est l'exemple le plus connu de ce type de chiffrement.

2.3.3 Chiffrement Asymétrique

Le principe du chiffrement à clé publique (appelé aussi chiffrement asymétrique) est apparu en 1976.

c'est une méthode de chiffrement qui s'oppose au chiffrement symétrique. Elle repose sur l'utilisation d'une b_i clé, constitué d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de coder le message et l'autre de le décoder[25].

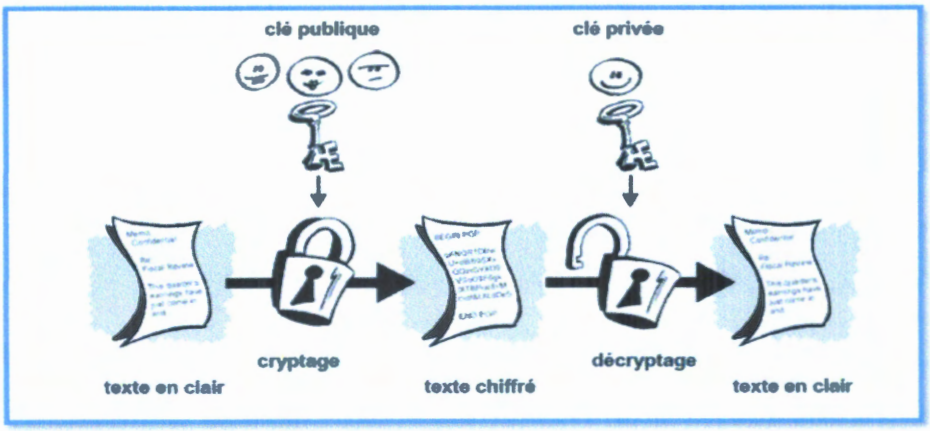

FIGURE 2.5 – Chiffrement asymétrique[26].

2.3.4 Chiffrement hybride

Le concept de chiffrement hybride fait appel aux deux techniques, symétrique et asymétrique, il a été mis en oeuvre par zimmermann pour le **PGP**(pretty good privacy) en 1991.

l'idée d'un système hybride est d'utiliser la rapidité de l'algorithme symétrique et la sécurité de l'asymétrique.

- Une clef secrète K de 128 bits est générée automatiquement pour la session.

- le message m est chiffré avec cette clef K en utilisant un chiffreur symétrique, $m' = e_k(m)$.

- la clef K est alors chiffrée avec un chiffreur asymétrique en utilisant la clef publique du destinataire B, k' = e k_B^{pub} (k) .

- Ensuite, le message entier $M = m' + k'$ (message chiffré symétriquement et clef symétriquement) est envoyé au destinataire.

- De l'autre côté, B utilise sa clef privée K_B^{pri} pour décrypter la clef K' et ensuite déchiffrer le message. un exemple d'un système hybride est le protocole SSL (secure socket layer) développé par les sociétés Netscape et RSA Security, cette dernière est responsable de l'algorithme RSA [27].

2.3.5 Chiffrement quantique

La cryptographie quantique est née au début des années 70. Elle repose sur le principe d'incertitude d'Heisenberg, selon lequel la mesure d'un système quantique perturbe ce système.

Dans tous les cas étudié auparavant, il a été considéré que le canal de communication peut être espionné. Un système de cryptographie parfait devrait donc utiliser un canal de communication sure.

Pour cela la cryptographie quantique propose une solution : Si une personne tente d'intercepter les communications alors le message est modifié ou détruit. Pour cela, la cryptographie quantique utilise des photons polarisés à des angles de 0 degré, 45 degré, 90 degré et 135 degré [28].

L'espion ne peut obtenir des informations, même partielles, sur le message sans altérer celui-ci de manière imprévisible et incontrôlable.

Le principe de base est que chaque bit est codé avec un seul photon, si celui-ci est capté alors le récepteur ne le reçoit pas ou alors de manière modifié et est ainsi mis au courant de l'écoute.

De plus, ce système résout le problème de la distribution des clefs. Deux utilisateurs peuvent donc s'échanger des clefs et ce de manière complètement sûre [29].

2.4 Communications Sécurisées par chaos

Avec le développement des réseaux de communication, il faut protéger les informations sensibles de l'interception indésirable a toujours attiré l'attention.

Nouvellement, plusieurs méthodes de cryptage ont été introduits, tels que la communication par chaos.

Les signaux chaotiques servent soit à véhiculer l'information soit à réaliser le cryptage de données.

Nous intéressons au cryptage de données à transmettre et plus particulièrement dans un contexte de transmission sécurisée. Dans certain cas, la cryptanalyse peut se baser sur la respectabilité du signal transmis car les algorithmes de cryptage sont des suites de nombres pseudo aléatoires.

Il est alors possible de reconstruire la clé à partir du signal crypté. Pour éviter ce type de faille, il faut donc que la clé ait une dimension suffisamment complexe pour que même à long terme, on ne puisse pas remonter au code. Le principe serait alors de se servir d'un bruit aléatoire évoluant dans le temps dont on connaît les caractéristiques en guise de clé.

2.5 Propriétés des système de communication a base du chaos

Les Propriétés des systèmes de communication chaotiques seront étudiées et comparées aux propriétés des systèmes classiques.

a. Spectre à large bande :

les systèmes chaotiques ont spécifiquement un spectre à large bande. Cette Propriété est bénéfique pour les applications qui nécessitent une importante robustesse face aux interférences et une faible probabilité de détection [30].

Ces problème ont été pris en compte par les premiers systèmes de transmission en utilisant des spectres larges et des modulations par saut de fréquences. Cependant malgré le recours à ces moyens, la synchronisation entre l'émetteur et le récepteur reste une tâche qui n'est pas toujours triviale. En effet les schéma de transmission qui utilisent un saut de fréquence requièrent une nouvelle synchronisation à chaque changement de fréquence de la porteuse. Donc l'utilisation des systèmes chaotiques permet la transmission des signaux à large bandes, ainsi la synchronisation entre l'émetteur et le récepteur est plus simple.

b. Signal non périodique :

la périodicité, dans la communication sécurisée engendre des pics spectraux indésirables, par contre, un signal chaotique est non périodique et son évolution ne peut être prédite sur un long intervalle de temps.

Par conséquent, il y a absence des pics spectraux. De plus il est plus difficile de développer un modèle de prévisions pour les dynamiques non périodiques[18].

c. Implémentation analogique simple :

les systèmes de communication à base du chaos peuvent être implémentés en utilisant des dispositifs électroniques ou optiques. Dans les schémas traditionnels par exemple, la

transmission par saut de fréquences nécessite la numérisation des données, ceci impliques des circuits indépendants plus complexe[30].

2.6 Concept et méthode de synchronisation

Le concept de synchronisation repose sur le constat 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 identique. Il existe deux classes de synchronisation suivant la manière avec laquelle les deux système chaotique sont couplés, on distingue la synchronisation unidirectionnelle et la synchronisation bidirectionnelle [31].

* **Synchronisation unidirectionnelle :** Le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément fonctionnant dans un seul sens.

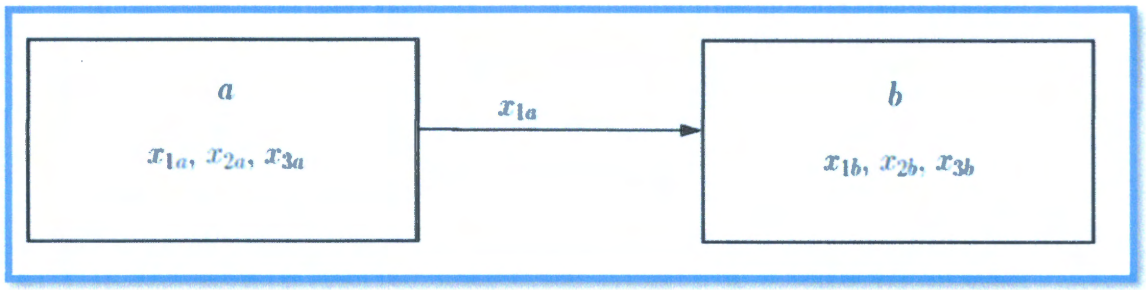

FIGURE 2.6 – Couplage unidirectionnelle.

* **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.

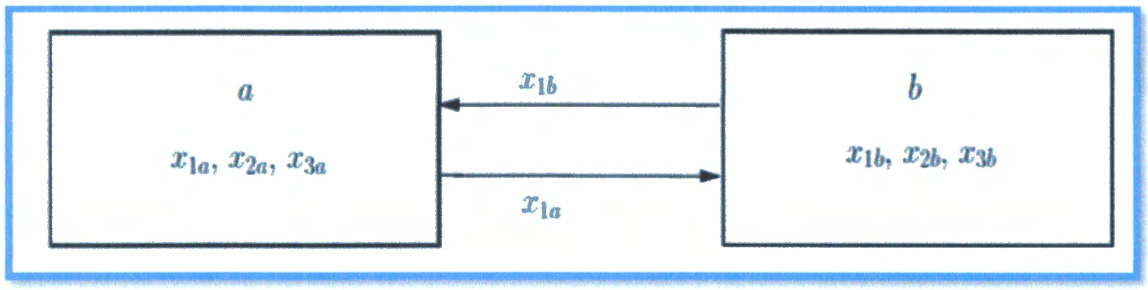

FIGURE 2.7 – Couplage bidirectionnelle.

2.7 Principe du crypto-système basée chaos

Les techniques de chiffrage basées sur le chaos, fournissent une bonne combinaison de vitesse, de haute sécurité,de complexité, de frais généraux raisonnables de calcul et de puissance de calcul,...etc. Les algorithmes de chiffrement chaotique utilisent des nombres pseudo-aléatoires générés par les fonctions (ou générateurs) chaotiques. Une fonction est dite chaotique, si elle est non linéaire et surtout si elle est sensible aux modifications, même extrêmement faibles de la valeur de la clé secrète qui est formée des conditions initiales et des paramètres du système. La séquence de nombre pseudo-aléatoire générée est utilisée par l'algorithme chaotique pour chiffrer le message en clair comme montre la figure suivante [34] :

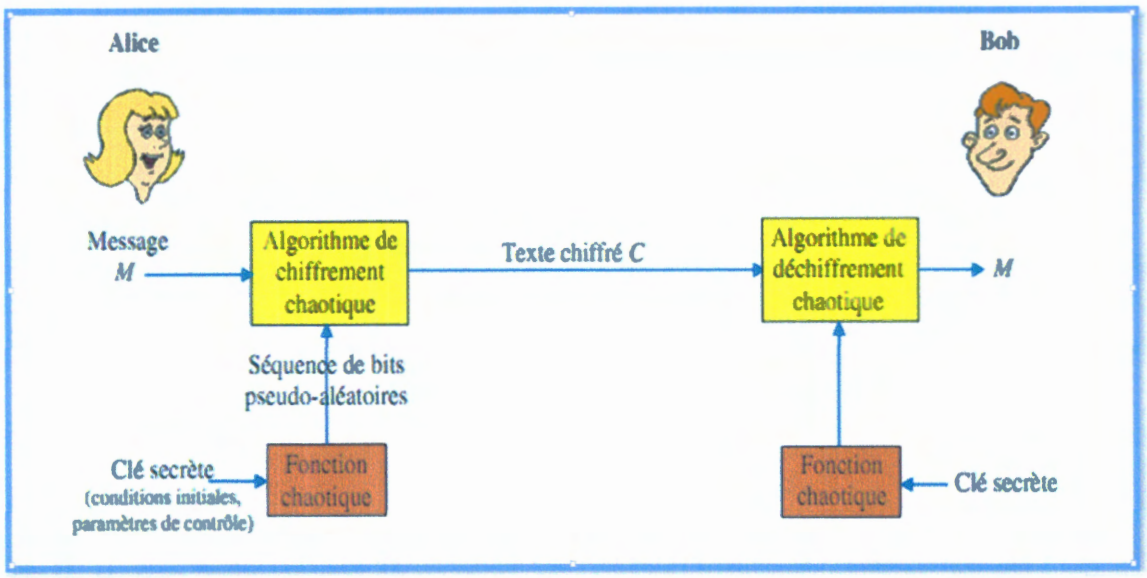

FIGURE 2.8 – Schéma de principe d'un crypto-système basé chaos[34].

Le chiffrement d'un message par le chaos s'effectue donc en superposant à l'information initiale un signal chaotique.

Alice envoyé le message noyé dans le chaos à un récepteur qui lui connaît les caractéristiques du générateur de chaos (clé secrète et séquence de nombre pseudo-aléatoires).

À la réception, Bob soustraire le chaos de son message pour retrouver l'information numérique (une image, une texte ...etc).

le chiffrement chaotique consiste à mélanger l'information m_k avec une séquence chaotique issue d'un émetteur, décrit généralement par une représentation d'état avec le vecteur d'état X_k. Seule la sortie Y_k de l'émetteur est transmise au récepteur.

Le récepteur a pour rôle d'extraire l'information originale du signal reçu Y_k. La récupération de l'information est généralement basée sur la synchronisation des états X_k de l'émetteur et des états du récepteur [31], c'est-à-dire :

$$\lim_{k\to\infty} \|X_k - X'_k\| = 0 \tag{2.1}$$

où

$$\exists\, k_f, \|X_k - X'_k\| = 0 \ \forall\, k < k_f \tag{2.2}$$

2.8 Techniques de chiffrement par chaos

Il existe plusieurs techniques qui peuvent servir comme moyen de masquage de l'information dans le chaos, nous décrivons ici quelques-uns :

2.8.1 Chiffrement par addition

Cette méthode appelée aussi « **masquage chaotique** » a été la première solution proposée dans la littérature comme application du chaos aux communications.
l'émetteur est un système chaotique autonome dont le signal de sortie **y(t)** est ajouté au signal du message **m(t)** .

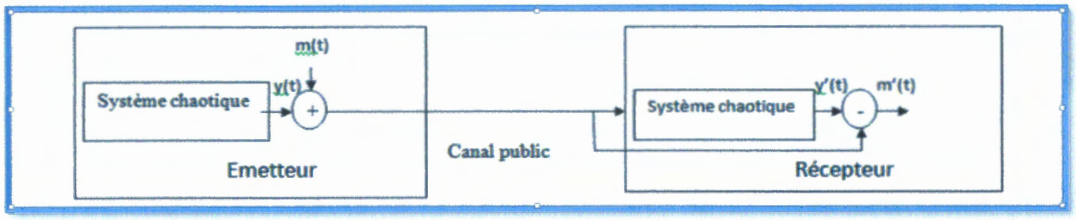

FIGURE 2.9 – Principe du chiffrement chaotique par addition.

La Figure 2.9 illustre parfaitement le principe du chiffrement chaotique par addition, l'idée est d'additionner directement les deux signaux de les transmettre au récepteur à travers le canal de transmission,qui est un canal public.

Le récepteur est constitué d'un système chaotique identique à l'émetteur et un simple soustracteur. Après la synchronisation des deux systèmes chaotique (émetteur et récepteur),le message est extrait a l'aide d'une opération de soustraction[35].

Si cette méthode n'a pas trouvé d'applications directes sur des canaux radiofréquence, elle est envisagée comme solution de cryptage sur des canaux à fort SNR, comme c'est le cas dans la fibre optique[32] .

Avantages	Inconvénients
La simplicité du cryptage.	Le message inférieure à la sortie de l'émetteur.
appliquée à des message continus.	la présence de bruit du canal, il devient difficile de détecter l'information.
appliquée à des message discrets.	sensible aux attaques extérieures.
/	l'usage du canal de transmission est inefficace(point de vue de l'énergie transmise par rapport à la qualité d'information fournie).

TABLE 2.1 – Avantages et Inconvénients de cryptage par addition

2.8.2 Chiffrement par commutation

Cette méthode, est aussi connue sous le nom « Chaos Shift Keying, **CSK** en anglais», est réservée aux messages prenant un nombre fini de valeurs. Pour plus de simplicité, nous traitons le cas des messages binaires : m(t)∈ 0, 1.

L'émetteur est constitué de deux systèmes chaotiques : ces deux systèmes peuvent avoir le même modèle dynamique, avec des paramètres différents, ou avoir deux modèles dynamiques totalement différents. L'un des systèmes envoi sa sortie sur la ligne de transmission. Ainsi, le signal transmis commune entre deux attracteurs étrange. Le récepteur est constitué de deux systèmes chaotiques identiques à ceux de l'émetteur et un bloc de comparaison permet de relever la valeur du message noté **m'(t)**.

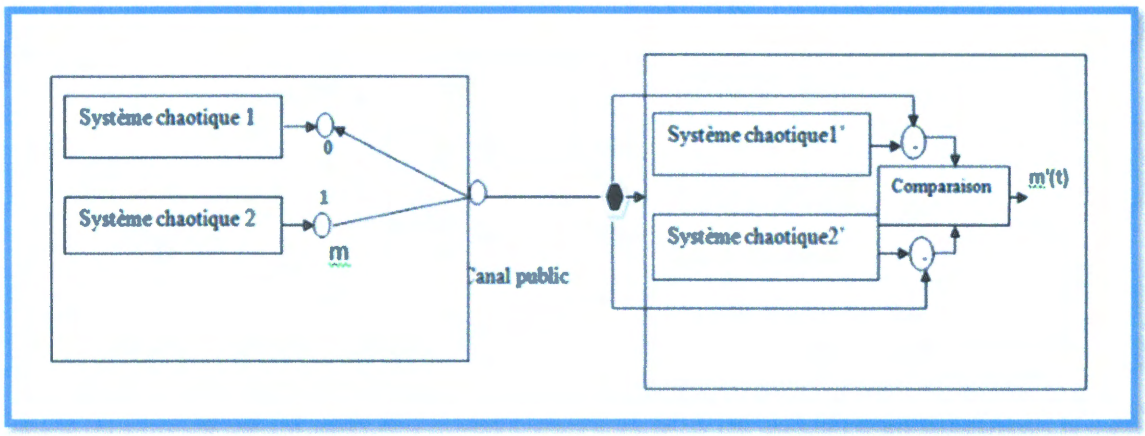

FIGURE 2.10 – Principe du chiffrement chaotique par commutation[35].

2.8.3 Chiffrement par modulation paramétrique

L'approche par modulation paramétrique utilise le message contenant l'information pour moduler un ou plusieurs paramètres θ de l'émetteur chaotique.

Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du continu d'attracteur, et de ce fait, le signal transmis est plus complexe qu'un signal chaotique « normal » .

Cependant, la façon d'injecter le message et donc la fonction démodulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur.

Cette technique exploite pleinement les qualités et propriétés des systèmes chaotiques.

Elle n'a pas d'équivalent parmi les systèmes de communication « classiques ».

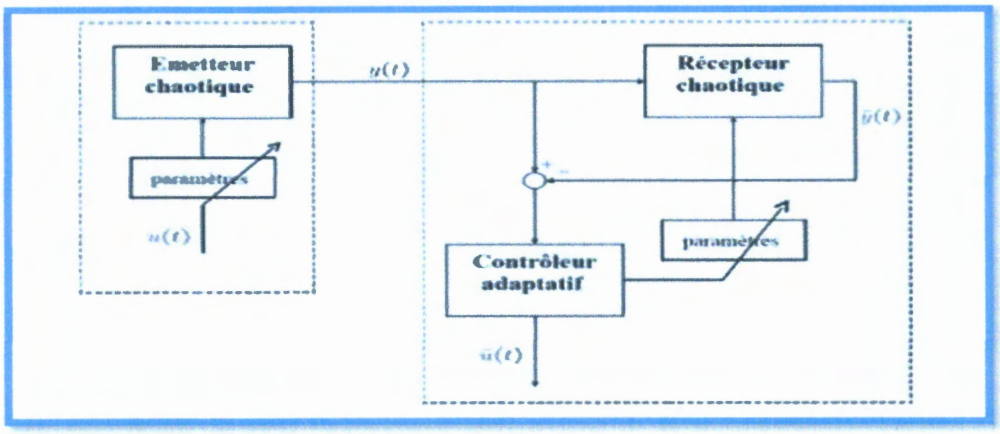

FIGURE 2.11 – Principe du chiffrement chaotique par modulation[35].

2.8.4 Chiffrement par inclusion

Cette technique de cryptage consiste à injecter le message dans la dynamique de l'émetteur. La restauration de l'information se fait principalement par deux techniques, reposant soit sur les observateurs à entrées inconnues, soit sur l'inversion du système émetteur. Cette méthode présente beaucoup d'avantages et reste très utilisée en pratique [36].

a. Observateurs à entrées inconnues

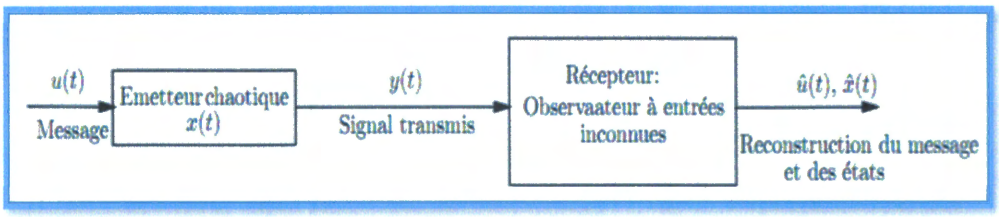

FIGURE 2.12 – Observateurs à entrées inconnues.

Le schéma de **la figure 2.15** illustre un problème classique d'estimation d'état non linéaire à entrées inconnues.
Il y a différentes techniques d'observateurs à entrée inconnues utilisées dans la littérature, et peuvent être utilisées à des fins de décryptage.

b. Décryptage par inversion

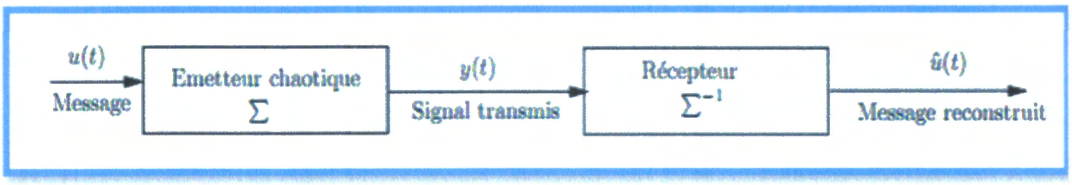

FIGURE 2.13 – Principe du cryptage par inversion

2.8.5 Chiffrement 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 peut finalement décoder le message. Le principe général de cette méthode est illustré par la figure suivante :

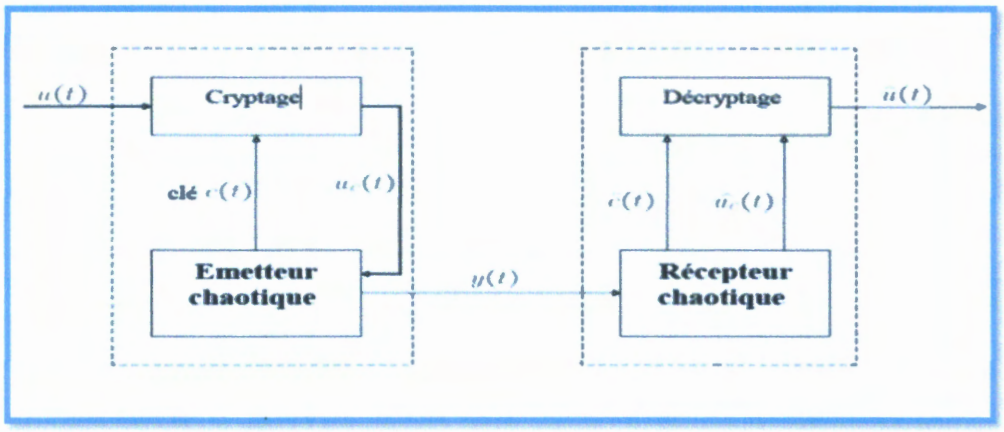

FIGURE 2.14 – Principe de Mixte

2.8.6 Transmission à deux voies

Dans ce schéma de communication, l'émetteur envoie deux signaux au récepteur :
- Le premier signal **y**, est une fonction à valeurs réelles de l'état **x** du système chaotique émetteur, dont l'unique but est de permettre la synchronisation du récepteur.
- Le second signal y_2 , envoyé sur un autre canal, est un signal chaotique contenant l'information à transmettre.

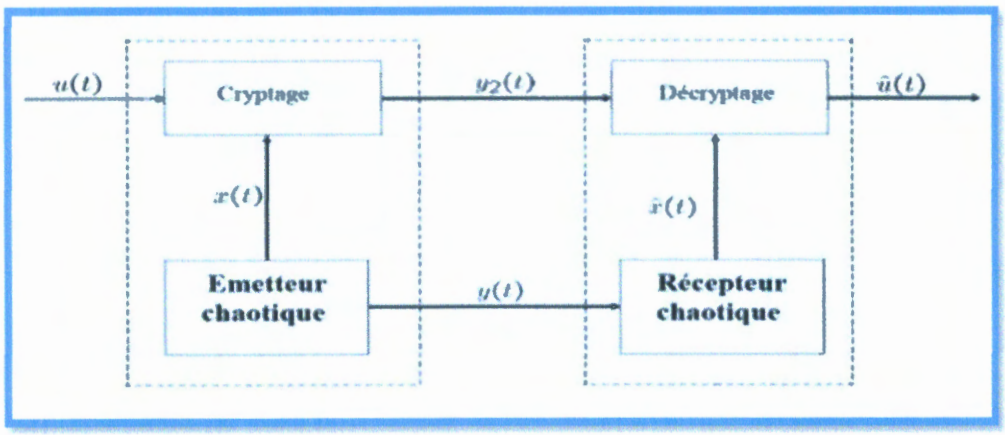

FIGURE 2.15 – Transmission à deux voies.

Cette méthode présente plusieurs avantages : le signal **y** ne contient aucune information, par conséquent la synchronisation peut s'établir de façon optimale.

Le second signal y_2 contient l'information qui peut être soit cryptée par une fonction non linéaire de l'état **x**, soit simplement masquée par un signal chaotique généré par l'émetteur, qui sert de porteuse.

Les deux étapes de synchronisation de cryptage étant totalement indépendantes, le décryptage n'est pas nécessairement effectuer, au niveau du récepteur, en même temps que

la synchronisation.

2.9 Comparaison entre chaos et cryptographie

Depuis les années 90, plusieurs chercheurs ont noté qu'il existe un rapport intéressant entre le chaos et la cryptographie. En effet, plusieurs propriétés des systèmes chaotiques présentent des correspondances similaires ou presque, avec des systèmes cryptographiques traditionnels. Le tableau suivant illustre parfaitement cette correspondance[36].

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

TABLE 2.2 – Correspondance entre la théorie du chaos et la cryptographie.

On considère les systèmes de cryptographie reposant sur la prise en compte des signaux chaotiques issus de rècurrences discrètes non linèaires, des systèmes discrets modèlisès par une èquation de la forme :

$$x_{k+1} = f(x_k) : x_0 \in I \tag{2.3}$$

Où I est l'intervalle unité ou le carré unité, et $f : I \longrightarrow I$, le but étant de mettre en évidence .
les propriétés mathématiques de ces systèmes chaotiques capables d'accroître la sécurité des cryptosystèmes construits à partir de ces systèmes dynamiques[37].

Propriété du chaos	Propriété de la cryptographie	Description
Ergodicité	Confusion	Le rendement a la même distribution pour n'importe quelle entrée (chaque trajectoire tend à une distribution invariable qui est indépendante des conditions initiales).
Sensibilité aux conditions initiales et aux paramètres du système.	Diffusion avec un petit changement du plaintext/ de la clé secrète.	Une petite déviation en entrée peut causer un grand changement au rendement.
Dynamique déterministe	Aspect déterministe pseudo-aléatoire.	Un processus déterministe peut causer un comportement pseudo-aléatoire.
Complexité de structure	Complexité d'algorithme	Un processus simple d'une complexité très élevée.

TABLE 2.3 – Comparaison entre le chaos et la cryptographie

Conclusion

En cryptographie usuelle, et parmi une grande variété de mécanismes de chiffrement, on distingue le chiffrement à clé publique et le chiffrement a clé secrète.

Dans ce chapitre une vue sur la cryptographie est donnée. Ensuite, les deux principaux algorithmes de la cryptographie standard (chiffrement a clé publique et chiffrement a clé secrète) sont présentés. Après nous avons cités les différents schémas de chiffrement par le chaos rencontrés dans la littérature.

Nous avons conclu le chapitre par l'étude de correspondance entre le chaos et la cryptographie.

Chapitre 3

Les systèmes de cryptage chaotique des images : Etat de l'art

Introduction

Les recherches récentes des systèmes dynamiques non linéaires ont été de plus en plus basées sur le Chaos.Les schémas de cryptage d'image ont été de plus en plus étudiés pour répondre à la demande de transmission d'images sécurisées en temps réel sur des réseaux privés ou publics.L'algorithme conventionnel de chiffrement d'image tel que le standard de chiffrement de données (DES) ne convient pas au chiffrement d'image en raison des caractéristiques de stockage particulières d'une image [2] et de la faiblesse de l'efficacité de bas niveau [3].

Au cours des dernières années, les chercheurs proposaient de nouvelles techniques de cryptage de l'image fondée sur de nouveaux systèmes chaotiques. Le principal avantage de ces techniques est de traiter les défaits du cryptage d'image pour plus de robustesse, d'obscurité et de rapidité. Dans ce chapitre on va présenter quelque développement effectué dans la cryptographie chaotique.

3.1 Le concept de confusion et diffusion

Les propriétés fondamentales de confusion et diffusion, doit posséder tout crypto système fiable, qu'ont été identifiées par Shannon en 1949.

- Le but de la confusion est de cacher toute relation existante entre l'image claire, l'image chiffrée et la clé.

- Le but de la diffusion est l'étalement des informations locales sur l'image entière. Ces deux principes rendent la cryptanalyse très difficile. Plus précisément, un système de communication qui possède une bonne confusion et une bonne diffusion résiste aux attaques.

3.2 Classification des techniques :

a. *En temps discret :*

• un nouvel algorithme proposé pour le cryptage d'image en utilisant plusieurs cartes circulaires basées sur le chaos.

- Générer une paire de sous-clés en utilisant des cartes logistiques chaotiques.

- Les images sont cryptées à l'aide d'une sous-clé de la carte logistique et dans sa transformation conduit à un processus de diffusion.

- Les sous-clés sont générées par quatre cartes chaotiques différentes tel que logistic map, tent map, quadratic map, Bernoulli map cité respectivement :

$$x(n+1) = \mu * x(n) * (1 - x(n)) \tag{3.1}$$

$$X_{n+1} = \begin{cases} \mu x_n & pour\ x_n < 1/2 \\ \mu(1 - x_n) & pour\ 1/2 < x_n \end{cases} \tag{3.2}$$

$$X_{n+1} = f_c = x_n^2 + c \tag{3.3}$$

$$f(x) = \begin{cases} 2x, & 0 \leqslant x < 0.5 \\ 2x - 1, & 0.5 \leqslant x < 1 \end{cases} \tag{3.4}$$

Selon les conditions initiales, chaque carte peut produire divers nombres aléatoires à partir de divers orbites des cartes [39].

• en utilisant "circel map" (est une carte chaotique dynamique discret) avec 3 paramètres, où différentes images ont été utilisées pour tester la validité de l'algorithme.[40]
Pour le chiffrement : l'équation mathématique suivante est utilisée :

$$x_{n+1} = mod((\sqrt{k_1} + k_2 x_n + sin(2.\pi.k_3.x_n)), 1) \tag{3.5}$$

• Un autre système chaotique simple et efficace présenté dans [41], propose d'utiliser une combinaison de deux cartes chaotiques unidimensionnelles (1D) telles que LTS, LSS, TSS et cela pour améliorer les performances des cartes chaotiques (la carte logistique, la carte de tente, la carte des sinus), l'équation LTS qui permet d'implémenter l'algorithme de la Figure(3.1) est défini comme suit :

$$x_{n+1} = A_{L\tau}(r, x_n) + \tau((4-r), x_n))mod\,1$$

$$= \begin{cases} rX_n\ (1-X_n\ ) + (4-r)\,X_n\ /2)\ mod\ 1 & X_i\ < 0.5 \\ rX_n\ (1-X_n\ ) + (4-r)\,(1-X_n\ )/2)\ mod\ 1 & X_i\ \geq 0.5 \end{cases} \quad (3.6)$$

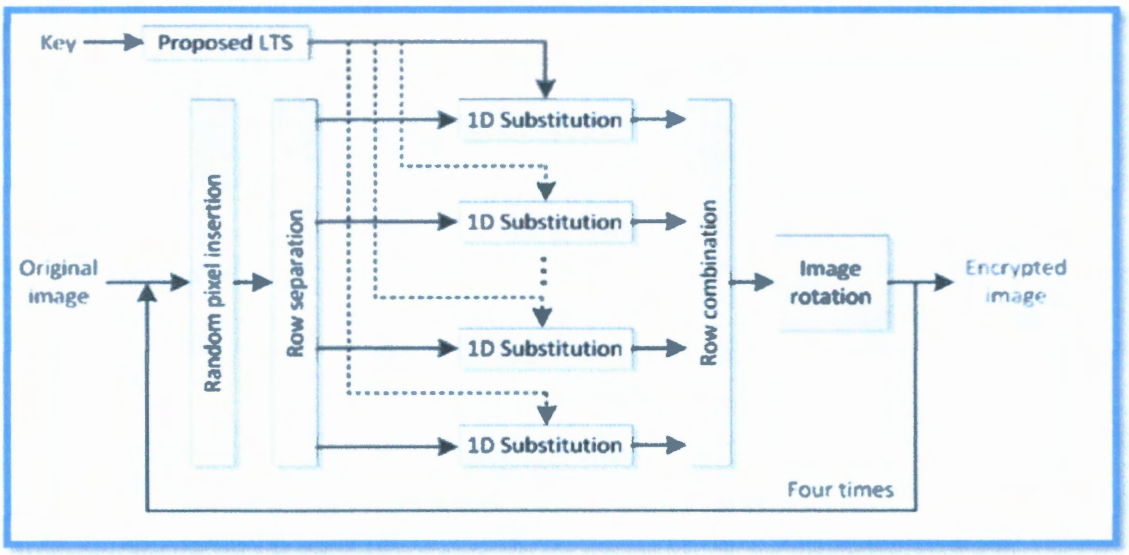

FIGURE 3.1 – Nouvel algorithme de chiffrement d'image [41].

Étape 1 : Insérer un pixel aléatoire au début de chaque ligne de l'image d'origine.

Étape2 : Séparer chaque ligne en une matrice de données 1D.

Étape3 : Appliquer un processus de substitution pour modifier les valeurs des données dans chaque matrice 1D.

Étape4 : Combiner toutes les matrices 1D dans une matrice de données 2D en fonction de leurs positions de ligne dans l'image originale et supprime le premier pixel de chaque ligne.

Étape5 : Faire pivoter la matrice 2D de 90 degrés dans le sens antihoraire.

La répétition de ces processus quatre fois obtient l'image cryptée finale.

L'algorithme proposé est capable de transformer des images originales de manière aléatoire en différentes images cryptées de type bruit avec d'excellentes propriétés de

confusion et de diffusion.

• Dans [42], Er Ankita Gaur et Er Maneesha Gupta proposent une variété d'algorithmes basés sur un système chaotique pour protéger l'image comme la carte de chat d'Arnold, la carte de sinus, la carte de tente et la carte logistique.
Les équations mathématiques des cartes précédentes sont définies de la manière :

$$\Gamma : \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} 1 & p \\ q & 1+q \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\, n \tag{3.7}$$

L'équation de logistique map et tent map sont déjà cité au paravant.

$$x_{n+1} = ax_n^2 sin(\pi x_n) \tag{3.8}$$

• les chercheurs dans [43] parlent sur la méthodologie pour concevoir un système cryptographique sécurisé libre. En général, pour générer un chiffrement d'image, on peut utiliser une clé de cryptage et une condition initiale. Le processus de génération de clé se compose de deux étapes :

- Obtenir des valeurs initiales à l'aide d'une fonction fractale supérieure.

- Générer une séquence de clés chaotique à l'aide de 2D-STCM (2D-Sine Tent composite map).

L'étape suivante consiste à crypter l'image à l'aide des séquences de clé générées à l'étape précédente :

- Mélanger les pixels de l'image ordinaire par CCPS (chaotic circular pixel shuffling).

- Effectuer l'opération XOR complexes à l'image mélangée on utilisant la séquence de clé chaotique.

Pour renforcer le système, le processus entier est répété trois fois différentes.

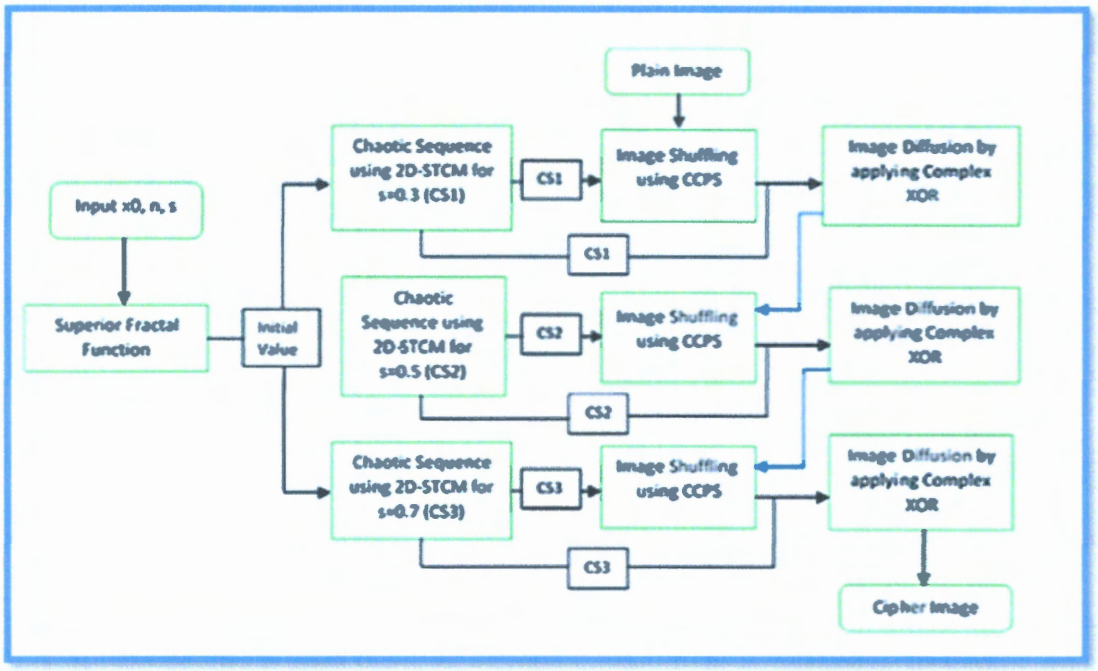

FIGURE 3.2 – Diagramme de processus de chiffrement proposé dans[43].

• Parmi les technologies de cryptage de l'image, les algorithmes de cryptage d'image à base chaotique montrent d'excellents résultats. les chercheurs dans [44] propose un nouveau algorithme de cryptage d'image appelé CMT-AIE basé sur le CMT (chaotic magic transform) et une séquences pseudo-aléatoires est générée pour modifier les positions des pixels d'image en utilisant la 2D-SLMM (2D Sine Logistic modulation map) dérivé de la modulation entre logistique et Sine map , et la substitution des pixels pour modifier les valeurs des pixels de l'image. La 2D-SLMM est définie par l'équation suivante :

$$x_{n+1} = \alpha(sin(\pi y_n) + \beta)x_i(1 - x_i) \tag{3.9}$$

$$y_{n+1} = \alpha(sin(\pi x_n) + \beta)y_i(1 - y_i) \tag{3.10}$$

La CMT-AIE utilise deux itérations d'opérations de substitution et de CMT.
Pour le processus de décryptage on inverse les opérations de chiffrement de CMT-AIE.

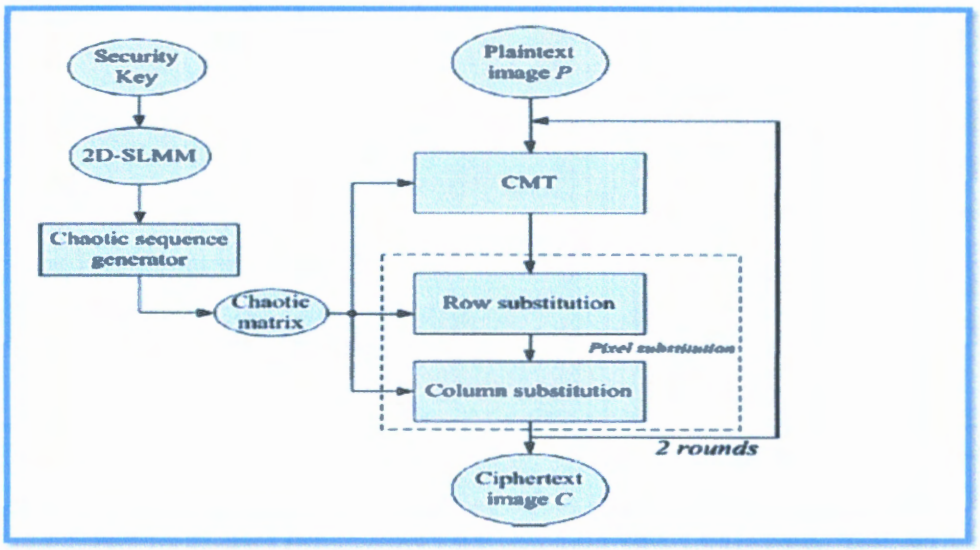

FIGURE 3.3 – Diagramme de cryptage d'image utilisant CMT-AIE .

• Dans [45], Fridrich a suggéré qu'une technique de chiffrement basée-chaos devrait comporter des itérations de deux processus : la confusion et la diffusion, dans son algorithme, la confusion est réalisée en permutant tous les pixels à l'aide d'une carte chaotique 2D Baker, et la diffusion est faite en altérant les valeurs des pixels séquentiellement et la modification apportée à un pixel particulier dépend de l'effet accumulé de toutes les valeurs des pixels précédents. Cette architecture de confusion-diffusion a formé plus tard, la structure de base pour plusieurs techniques de chiffrement d'images basées- chaos.
La carte Baker, B est décrite par les formules suivantes :

$$B(x,y) = (2x, y/2) \ \text{où} \ 0 \leqslant x < 1/2 \tag{3.11}$$

$$B(x,y) = (2x-1, y/2+1/2) \ \text{où} \ 1/2 \leqslant x < 1 \tag{3.12}$$

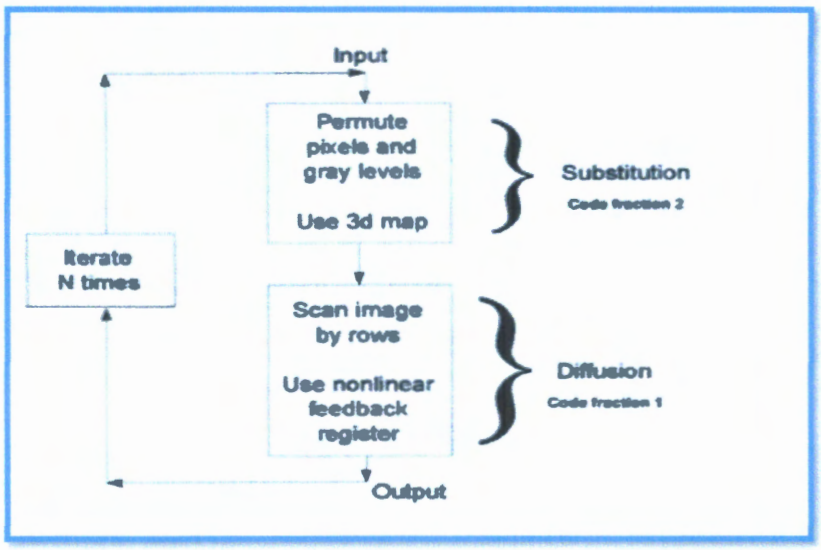

FIGURE 3.4 – Diagramme de chiffrement produit d'une itération composée d'une étape de permutation et d'une étape de diffusion.

• Dans [46], Chen et al ont employé une version 3D de la carte ALD Cat pour la substitution, la carte logistique pour la diffusion et le système chaotique de Chen comme un générateur des clefs, L'algorithme de chiffrement est illustré dans la figure suivante :

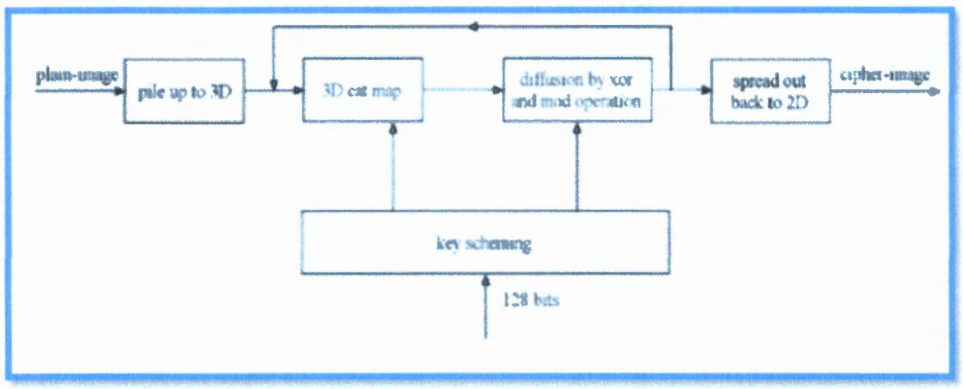

FIGURE 3.5 – Diagramme de cryptage d'image utilisant 3D cat map.

Étape 1 : Générer les clés : Sélectionner une séquence de 128 bits et la diviser en huit groupes, qui sont également affectés à plusieurs paramètres pour la carte de chat 3D et la carte logistique.
Étape 2 : Empilez l'image de deux dimensions en trois dimensions, ensuite empiler tous les pixels de l'image, pour former plusieurs cubes.
Étape 3 : Implémenter la Cat map en 3D.
Étape 4 : Appliquer les opérations XOR et MOD entre la valeur de chaque pixel et la

valeur de la carte map 3D, cette étape est répétée deux fois.

Étape 5 : Transformer les cubes 3D en une image en deux dimensions.

Les opérations sont effectuées aux étapes 3 et 4 sont répétées plusieurs fois selon les exigences de sécurité.

Après la conversion de l'image originale en 3D, la carte 3D Arnolad's Cat définie comme suit :

$$\begin{bmatrix} X_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = A \begin{bmatrix} X_n \\ y_n \\ z_n \end{bmatrix} modN \tag{3.13}$$

est employée pour créer la confusion. Ensuite, la formule ci-après est utilisée pour Créer la diffusion.

$$c(k) = \Phi(k) \bigoplus [i(k) + \Phi(k)] \, modN \bigoplus c(k-1) \tag{3.14}$$

où, $\Phi(k)$ est généré en utilisant la carte logistique, $i(K)$ représente la valeur du pixel en cours et $c(K)$ est la nouvelle valeur du pixel en cours.

• Dans [47] la même idée précédente est utilisée par Mao et al sauf qu'ils ont employé la carte3D Baker à l'étape de substitution au lieu de la carte 3D Cat. qui est définie par l'équation suivante :

$$B(x,y,z) = \begin{cases} (2x, 2y, z/4) & 0 \leqslant x < 1/2, \quad 0 \leqslant y < 1/2 \\ (2x, 2y-1, z/4+1/2) & 0 \leqslant x < 1/2, \quad 1/2 \leqslant y < 1 \\ (2x-1, 2y, z/4+1/4) & 1/2 \leqslant x < 1, \quad 1/2 \leqslant y < 1 \\ (2x-1, 2y-1, z/4+3/4) & 1/2 \leqslant x < 1, \quad 1/2 \leqslant y < 1 \end{cases} \tag{3.15}$$

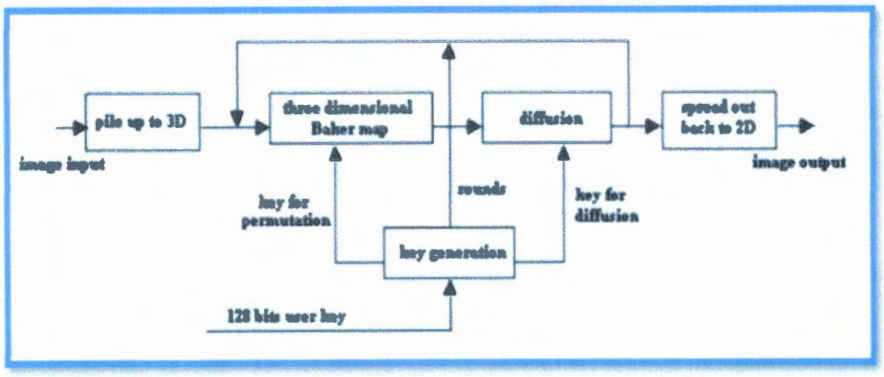

FIGURE 3.6 – Diagramme de cryptage d'image utilisant 3D baker map[47].

• V. Patidar et al [48] ont proposé un nouvel algorithme de chiffrement en utilisant la carte chaotique standard et la carte logistique (3.1) avec une clef secrète de 157 bits pour chiffrer des images couleurs.

la carte standard, se définie par :

$$\begin{cases} a_{i+1} = (a_i + b_i) mod\ 2\pi, \\ b_{i+1} = (b_i + ksin(a_i + b_i)) mod\ 2\pi, \end{cases} \tag{3.16}$$

La condition initiale, le paramètre système de la carte standard et le nombre d'itération constituent ensemble la clef secrète. Ensuite, dans les deux rondes de diffusion les propriétés des pixels horizontalement et verticalement adjacents sont mélangées respectivement. Dans la quatrième ronde une confusion robuste et efficace est réalisée à l'aide de la carte standard et logistique.

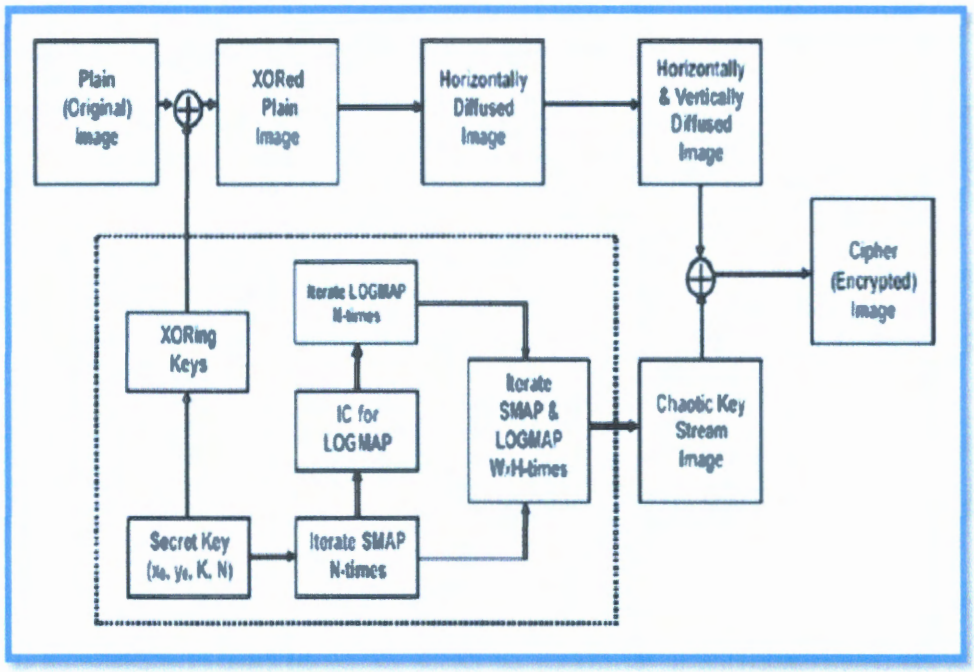

FIGURE 3.7 – Diagramme de chiffrement utilisant la carte standard et logistique.[48]

• Lian et al [49] ont prouvé qu'il existe quelques clefs faibles (problème de sécurité) dans les techniques de chiffrement qui utilisent les cartes chaotiques Baker et Cat (3.13 et 3.15), et que l'espace de clef de la carte chaotique standard est assez grand que ces deux dernières cartes Ils ont utilisé la carte standard(3.16) pour la substitution (Figure 3.8).

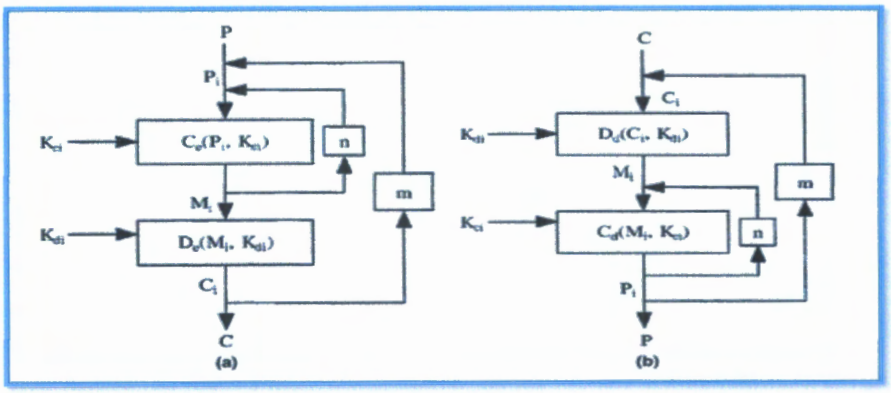

FIGURE 3.8 – Processus de chiffrement et déchiffrement : (a) Processus de chiffrement, (b) Processus de déchiffrement.

3.3 Analyse de sécurité :

Le tableau suivant présente les résultats obtenus des différents travaux présentés.

Réf	Les Auteurs	Espace couleur	CoefH Img orig/img chiff	CoefV Img orig/img chiff	CoefD Img orig/img chiff	NPCR	UACI	Entropie Img orig/img chiff
[39]	Sriraam et al	NDG	0.9670/ -0.0025	0.9870/-0.0218	0.9692/ 0.0167	98.4754	32.2128	/
[52]	Mandal et al	NDG	0.9712/ 0.0012	0.9698/ 0.0032	0.9861/ 0.0058	/	/	7.4312/ 7.9878
[41]	Long et al	NDG	0.8652/ 0.0053	0.8593/-0.2088	0.7957/ 0.0036	/	/	5.19634/ 7.99763
[43]	S.Agarwal	RGB	0.9698/ -0.0029	0.9799/ 0.0052	0.9627/ -0.0054	99.5580	33.0396	7.4140/ 7.9942
[44]	parmi	NDG	0.965935/ 0.002383	0.936620/-0.008576	0.915342/ 0.040242	99.5693	33.7016	/
[46]	Chen et al	NDG	0.91765 / 0.01183	0.95415 / 0.00016	0.90205 / 0.01480	/	/	/
[47]	Mao et al	NDG	0.97653/ 0.04454	0.97961 / 0.02843	0.95025 / 0.02066	/	/	/

TABLE 3.1 – comparaison entre les résultats des méthodes en temps discret.

b. *En temps continu :*

• Vishnu G.kamat et madhu sharma[38] proposent un nouvel algorithme pour diviser la clé sur 3 dimensions. Il utilise le système de rossler pour la génération de clé chaotique.
Le système de Rossler est un système d'équations différentielles non linéaires qui a des propriétés chaotiques, Comme indiqué ci-dessous :

$$\dot{x}(t) = -y_n - zn \tag{3.17}$$

$$\dot{y}(t) = x_n + \alpha y_n \tag{3.18}$$

$$\dot{z}(t) = \beta + z_n(x_n - \gamma) \tag{3.19}$$

Il est également conçus pour fonctionner avec des images couleur (RVB), la diffusion horizontale dans l'algorithme est utilisé séparément sur chaque canal (effectuée sur les 3 canaux de l'image) après le cryptage de la chaîne. La diffusion verticale est effectuée avant et après le cryptage complet [38].

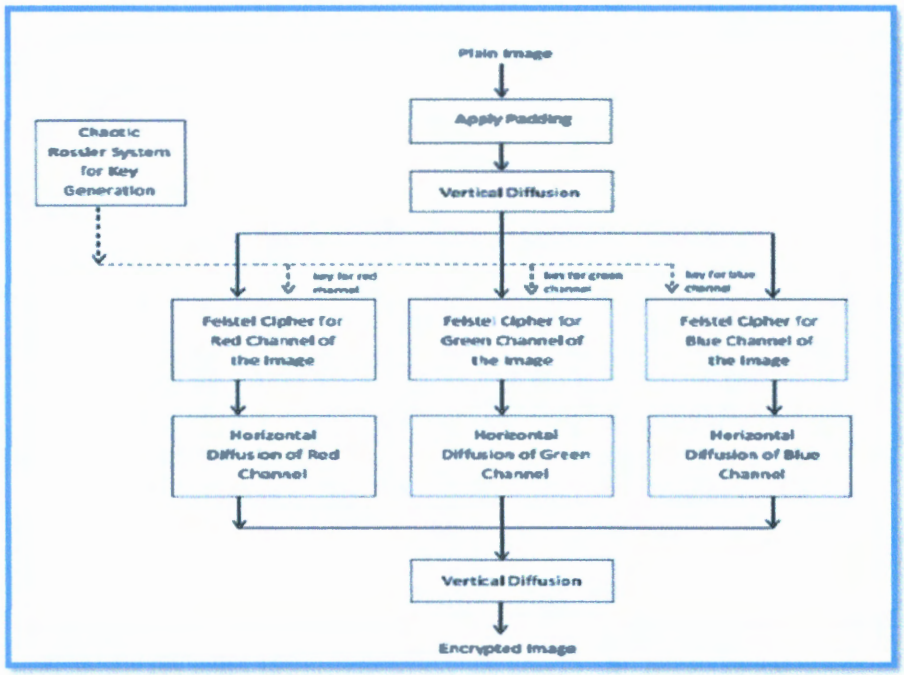

FIGURE 3.9 – Schéma de chiffrement / déchiffrement[38].

On peut résumer les étapes de chiffrement comme suit :
Rembourrage : le remplissage est ajouté pour faire la taille du bloc d'entrée 32 octets, lorsque la taille de l'image n'est pas en double octet, elle est ajoutée (1-31 octets) à la fin de chaque ligne.

Génération de clé : la séquence aléatoire générée par chaque équation de la carte est utilisée comme une clé séparément pendant le processus de cryptage.
Diffusion verticale et horizontale : La diffusion horizontale est utilisée séparément sur chaque canal après le cryptage du canal, mais en diffusion verticale, les canaux sont traités collectivement.
Chiffrement : le cryptage est effectué sur 256 bits (32 octets) de données à la fois en utilisant huit registres 32 bits. Quatre octets de la clé sont ajoutés à d'autres enregistrements. Ensuite, les calculs sont effectués sur les données d'image.

• L'algorithme proposé par les chercheurs dans [50] pour le cryptage d'images est basé sur l'idée de Shanon de confusion et de diffusion, c'est-à-dire, combinant le réseau de substitution et de permutation (S- P), les bruits aléatoires sont les suivants a également été ajouté pour modifier les pixels de l'image brute. donc, il y a trois modules de la technique anticipée, ajout de bruit, permutation et substitution. La figure suivante résume les étapes de cet algorithme :

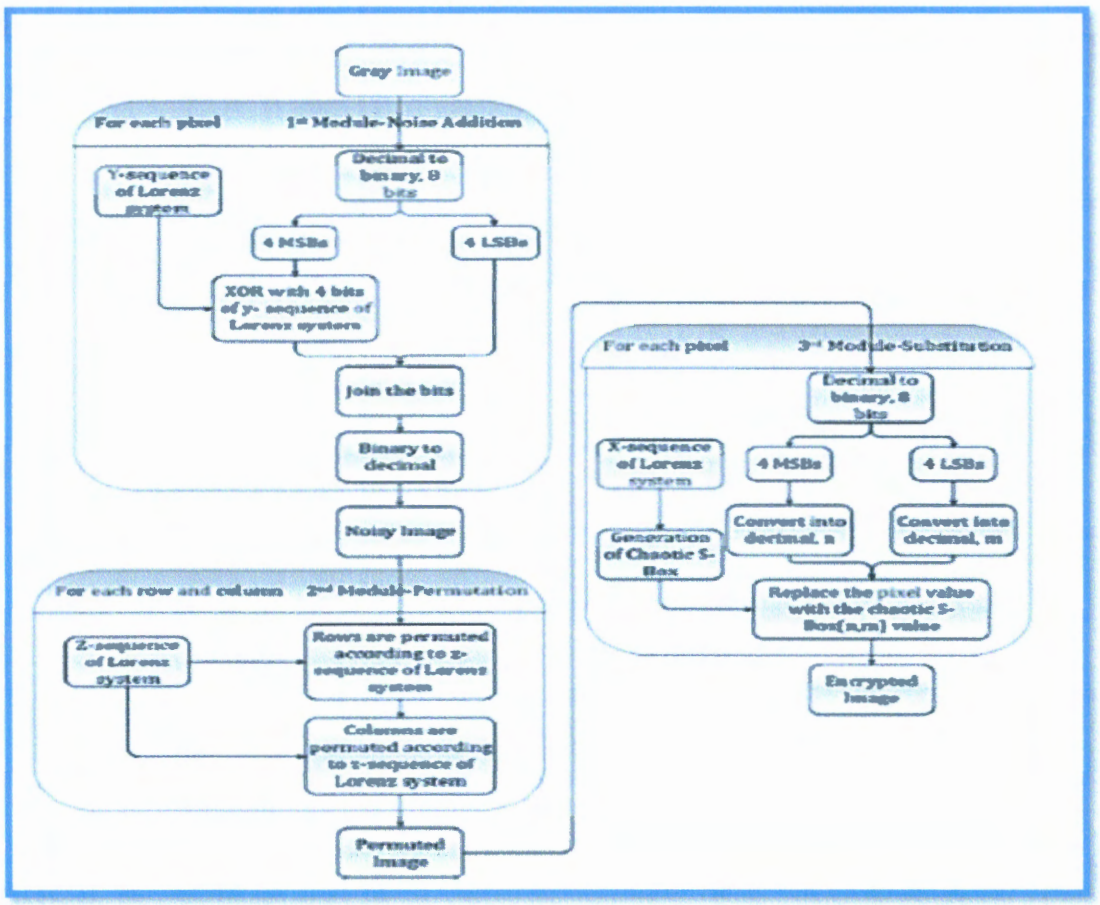

FIGURE 3.10 – Diagramme de cryptage d'image utilisant les trois modules.

L'ajout de bruit :

Pour la dé-corrélation des pixels d'image, le bruit aléatoire est générée par le y-séquence de système de Lorenz avec les conditions initiales :x, y, z.

Les valeurs obtenues sont ensuite changé entre [0...15] à l'aide d'un seuil et la fonction MOD. La valeur décimale d'image est converti en binaire de 8 bits puis l'opération XOR est appliquée bit à bit avec MSBs et LSBs de l'image.

La valeur de chaque bruit est ajouté à quatre bits les plus significatifs (MSBs) de chaque pixel de l'image. Cependant, ce bruit n'est pas directement ajouté à l'image. La raison pour laquelle accomplir l'opération XOR est les échelles de gris Image se situe entre [0,255], de sorte que toute l'opération arithmétique linéaire effectuée sur l'image donne la valeur maximale de 255.

On fait une opération de XOR entre les quatre bits de bruit et les quatre bits LSB.

La valeur binaire de bruit est convertie en décimale de 4 bits et puis ces bits sont XOR bit à bit pour obtenir l'image bruité.

La permutation :

Dans ce module la permutation est faite en fonction de séquence chaotique du système de Lorenz. Les lignes d'image sont permutées les uns avec les autres et les colonnes sont permuté de la même manière que les lignes pour former une image permutée.

La substitution :

Après la permutation, une substitution des pixels de l'image, est faite à l'aide de la boîte de substitution (S-Box). Tout d'abord la valeur décimale d'image est converti en binaire de 8 bits puis on fait un XOR entre ces bits et MSBs et LSB de l'image ensuite on va converti une autre fois en décimale MSBs et LSB pour générer le Box et faire la substitution à l'aide du système de Lorenz.

• Le processus de chiffrement proposé dans [51] peut être décrit par les étapes suivantes :

Etape 1 : générer des valeurs initiales $(x0, y0, z0)$

Etape 2 : générer la séquence chaotique qui utilise le système de Rossler avec les conditions initiales$(x0, y0, z0)$.

Etape 3 : : convertir les séquences chaotiques xi, yi, zi en des tableaux de deux dimensions $x(i,j)$, $y(i,j)$, $z(i,j)$, respectivement .

Etape 4 : limiter la valeur de la séquence chaotique entre 0 et 255 (échelle de gris 8 bits) par l'opération mod :$x(i,j) = mod((x(i,j)10000), 256)$.

Etape 5 : exécuter le remplacement de pixel de l'image de l'original par bit XOR entre l'image originale et la séquence chaotique.

Etape 6 : générer une nouvelle séquence chaotique yz qui est définie par :

$$yz(i,j) = y(i,j) \oplus z(i,j). \tag{3.20}$$

Maintenant, l'opération du mélange des pixels est réalisée à l'aide de la séquence yz pour obtenir l'image chiffrée.

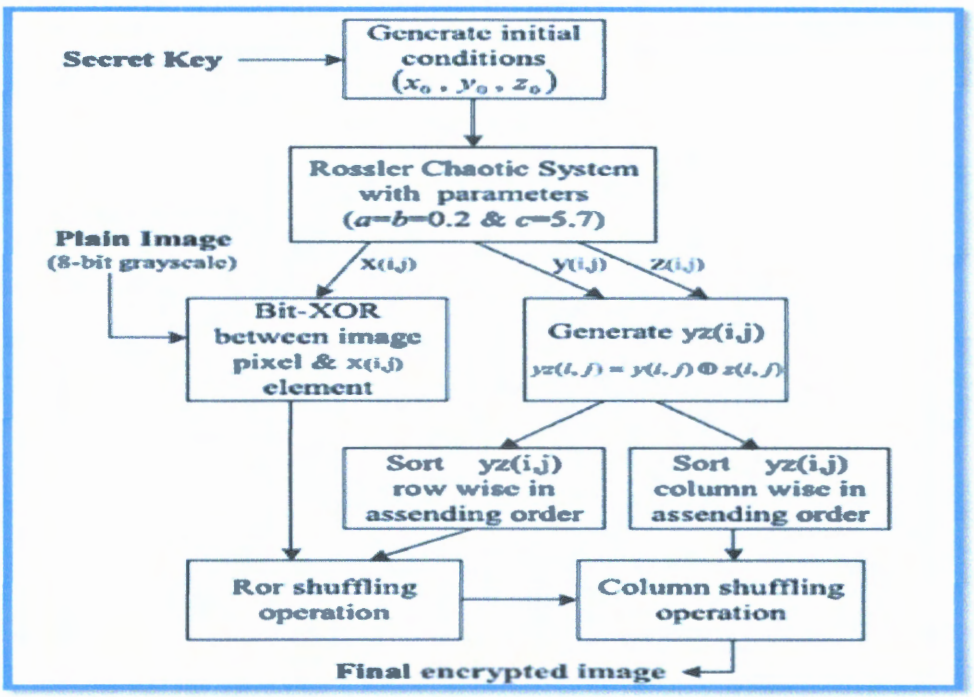

FIGURE 3.11 – Diagramme de cryptage d'image selon[51]

• la méthode dans [52] propose une nouvelle technique de cryptage d'image fondée sur de nouveaux systèmes chaotiques en ajoutant deux systèmes chaotiques : le système chaotique de Lorenz et le système chaotique Rossler. sa valeur initiale et les paramètres structurels sont utilisés comme clé de cryptage. L'avantage principal de cette technique est le grand espace de clé et le renforcement de la sécurité, le haut niveau d'obscure et une grande vitesse. Cette méthode a les étapes suivantes :

Etape 1 : configurer les paramètres (les conditions initiales et les paramètres$(\delta, \beta, r, a, b, c, y_0, x_0, z_0)$ dans l'intervalle acceptable.

Etape 2 : générer le premier masque avec la même taille d'image.

Etape 3 : effectuer le XOR entre le masque d'image et l'image originale.

Etape 4 : si l'image n'est pas cryptée, générer le deuxième masque avec la même taille d'image.

Etape 5 : effectuer l'opération XOR entre le masque chaotique et l'image à l'étape 3.

Etape 6 : si l'image n'est pas cryptée, générer le troisième masque avec la même taille d'image.

Etape 7 : effectuer le XOR entre le masque chaotique et l'image à l'étape 5.

Etape 8 : l'image chiffrée.

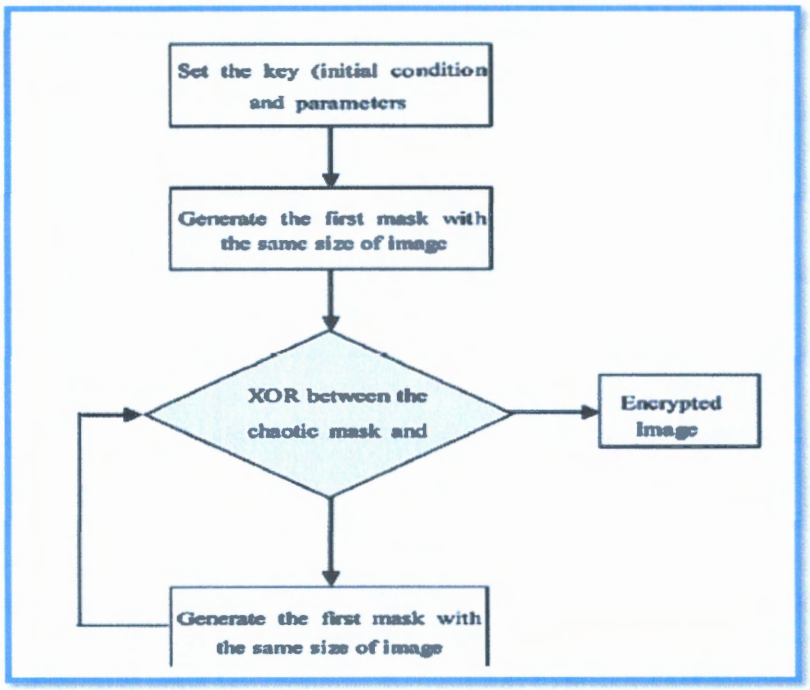

FIGURE 3.12 – Diagramme de cryptage d'image selon[52]

• Dans [53], M. Manikandan et all ont proposé un algorithme de cryptage pour les images en couleur RGB qui combine le système de Lorenz avec le système de Rossler et le système Chen avec le concept multi-clé. Le processus de cryptage est effectué avec un système chaotique à une ou plusieurs clés(multi-clé), où les valeurs de pixels de l'image sont modifiées de façon aléatoire en utilisant la confusion et la diffusion. La Figure 3.13 illustre le processus de cryptage/décryptage de l'algorithme proposé par les chercheurs :

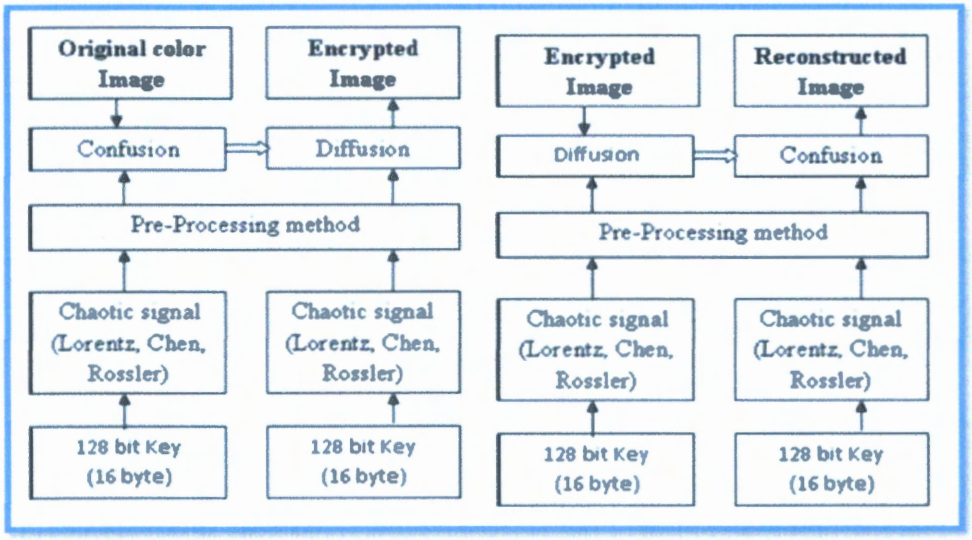

FIGURE 3.13 – Schéma de chiffrement / déchiffrement.

Etape 1 : la clé secrète de l'image est générée de manière chaotique. La figure 1, la condition initiale et le paramètre de contrôle pour générer une clé secrète pour la séquence chaotique.

Etape 2 : La valeur générée est ajoutée à l'un des paramètres de Lorenz, Rossler ou chen sur les variables et sur les valeurs des paramètres.

Etape 3 : le processus de confusion et de diffusion est fait pour augmenter le niveau de sécurité. (Chen système chaotique).

Finalement, il faut signaler que pour les déchiffrement, le processus inverser et appliquer.

Synthèse sur l'analyse des résultats :
Dans le tableau suivant nous avons regroupés les résultats obtenus des méthodes présentées précédemment :

Réf	Les Auteurs	Espace couleur	CoefH Img orig/img chiff	CoefV Img orig/img chiff	CoefD Img orig/img chiff	NPCR	UACI	Entropie Img orig/img chiff
[38]	Vishnu Et al	rouge	0.9558/ -0.0014	0.9781/ -0.012	0.9336/ 0.0004	99.6333	33.4706	/
		vert	0.9401/ 0.0004	0.9695/ 0.0067	0.9180/- 0.0026			
		bleu	0.9189/ -0.0049	0.9495/ 0.0014	0.8948/- 0.0005			
[50]	A.aness	NDG	/	/	/	92.23	33.31	7.4889/ 7.8124
[51]	K. Mandal et all	NDG	0.936393/ 0.040309	0.973760/- 0.008468	0.908536/ 0.005196	99.60020	28.451221	7.415264/ 7.997045
[52]	h.Qais et all	NDG	0.9681/ 0.0483	0.9434/ 0.1078	0.9238/- 0.0283	/	/	/

TABLE 3.2 – Comparaison entre les résultats des méthodes en temps contenu.

Conclusion

Ce chapitre présente des nouvelles techniques qui offrent la possibilité d'utiliser des systèmes chaotiques dans le domaine de la cryptographie. Le haut niveau de sécurité qu'offre ce type de systèmes ainsi que la rapidité de calcul due à leur structure dynamique permet d'envisager l'utilisation du chaos pour réaliser la fonction de chiffrement et de déchiffrement des documents de grand taille tel que les images .

Après cette synthèse des différentes contributions théoriques, nous proposons dans le chapitre suivant, de décrire notre contribution au niveau empirique, en présentant la fonction proposée, ainsi que le système de cryptage des images pour lequel nous avons opté.

Chapitre 4

Réalisation d'un système de cryptage chaotique des images

Introduction

Comme nous avons constaté dans les chapitres précédents, les systèmes chaotiques ont un certain nombre de propriétés intéressantes. Ces propriétés rendent les systèmes chaotiques pour la construction des systèmes de cryptage.
Dans ce chapitre, nous allons tout d'abord présenter la méthode de cryptage chaotique des images en se basant sur la définition d'une nouvelle fonction chaotique. Ensuite, nous allons présenter notre application qu'on a développée sous Python pour le chiffrement et le déchiffrement des images. Des résultats expérimentaux sont donnés pour démontrer l'efficacité du système implémenté.

4.1 Fonctions chaotiques

4.1.1 Fonction logistique :

comme c'est déjà mentionné (cf chapitre I) une fonction logistique est définie par

$$x_{n+1} = rx_n(1 - x_n) \tag{4.1}$$

Pour que le processus du système dynamique discret fonctionne, il faut choisir une valeur de paramètre pour laquelle cette fonction est chaotique. La première valeur de paramètre qui conduit au chaos est d'environ $r = 3,57$. Les orbites chaotiques peuvent être trouvées d'environ $r = 3,57$ à $r = 4$. Les valeurs des paramètres $r < 3.57$,$r > 4$ et les fenêtres périodiques internes sont rejetées car celles-ci ne créent pas de comportement chaotique.
Dans notre application, nous pouvons choisir n'importe qu'elle valeur dans l'intervalle $[3.57, 4]$ pour le paramètre r.

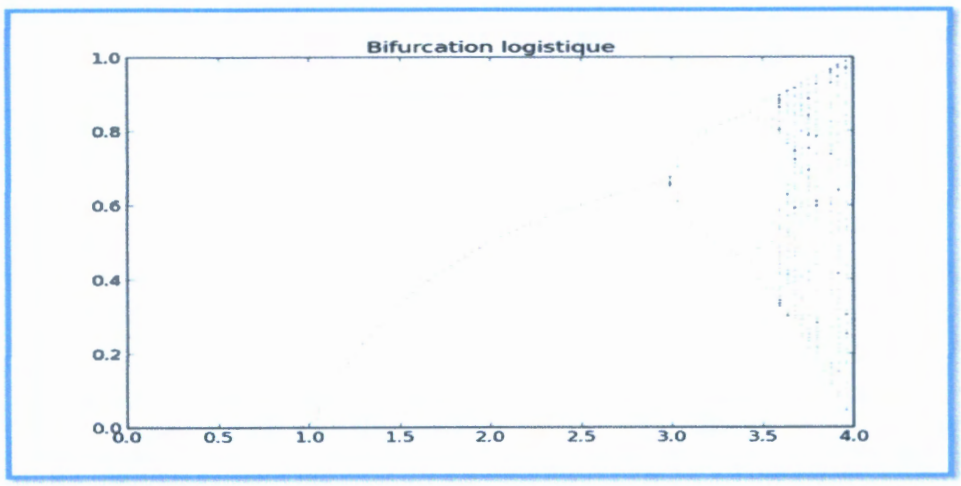

FIGURE 4.1 – Diagramme de bifurcation de la suite logistique

4.1.2 Circle Map :

comme c'est déjà décrit (cf chapitre III) une fonction circle map est définie par :

$$x_{n+1} = mod[\sqrt{k_1} + k_2 x_n + sin(2.\pi.k_3.x_n), 1] \tag{4.2}$$

Nous avons étudié son fonctionnement chaotique par l'implémentation de son diagramme de bifurcation.

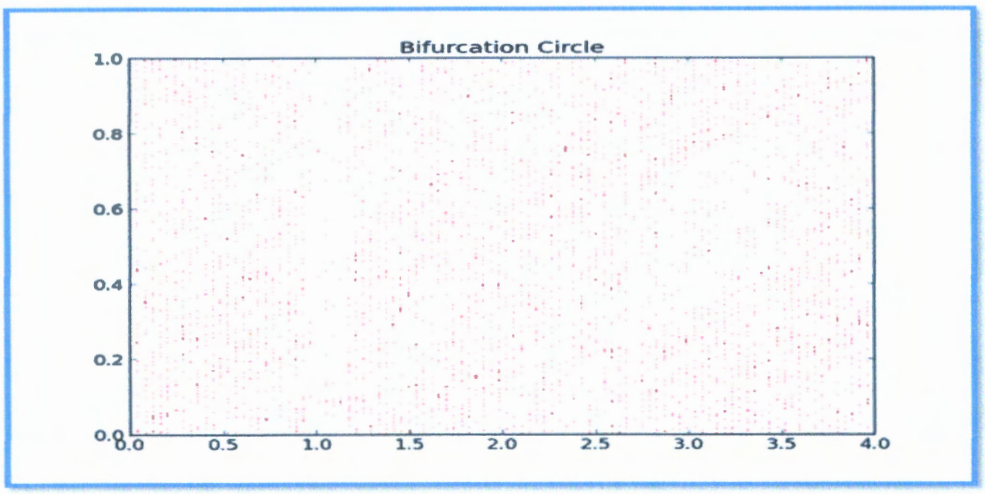

FIGURE 4.2 – Diagramme de bifurcation de la fonction circle map

Le diagramme de bifurcation de la fonction circle map dans la figure montre que le comportement chaotique est au long d'intervalle [1 ; 4].

4.1.3 Définition d'une nouvelle fonction chaotique CircLog

Nous avons défini une nouvelle fonction chaotique par l'application de l'opérateur XOR entre la fonction logistique (4.1) et circle map(4.2).
Cette nouvelle fonction se définie par :

$$x_{n+1} = ((k_1 x_n(1 - x_n))XOR\ (mod(\sqrt{k_1} + k_2 x_n + sin(2.\pi.k_3.x_n), 1])) \tag{4.3}$$

il faut signaler que dans cette nouvelle fonction, nous avons remplacer le paramètre r de la fonction logistique par le paramètre k_1.
Le comportement chaotique de notre fonction (CircLog) est montré par le diagramme de bifurcation suivant :

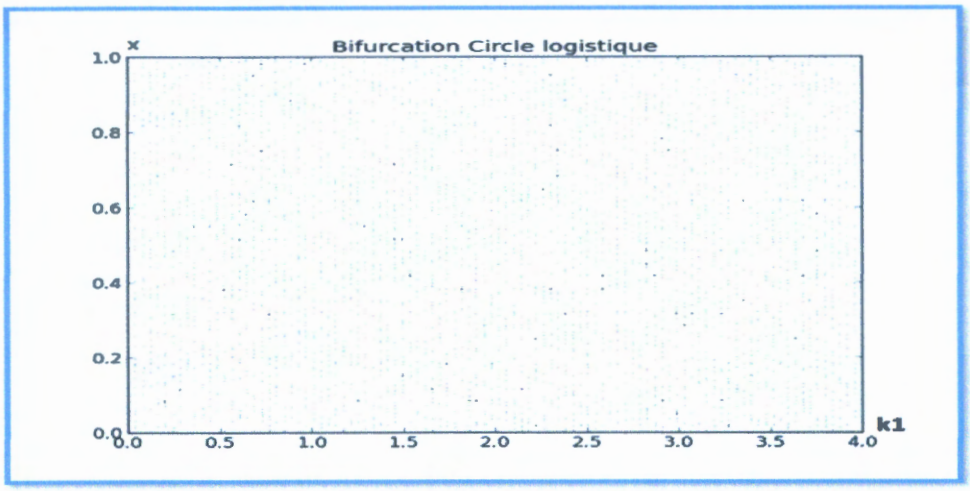

FIGURE 4.3 – Diagramme de bifurcation de la fonction CircLog.

4.2 Processus général de notre système de chiffrement /déchiffrement chaotique des images.

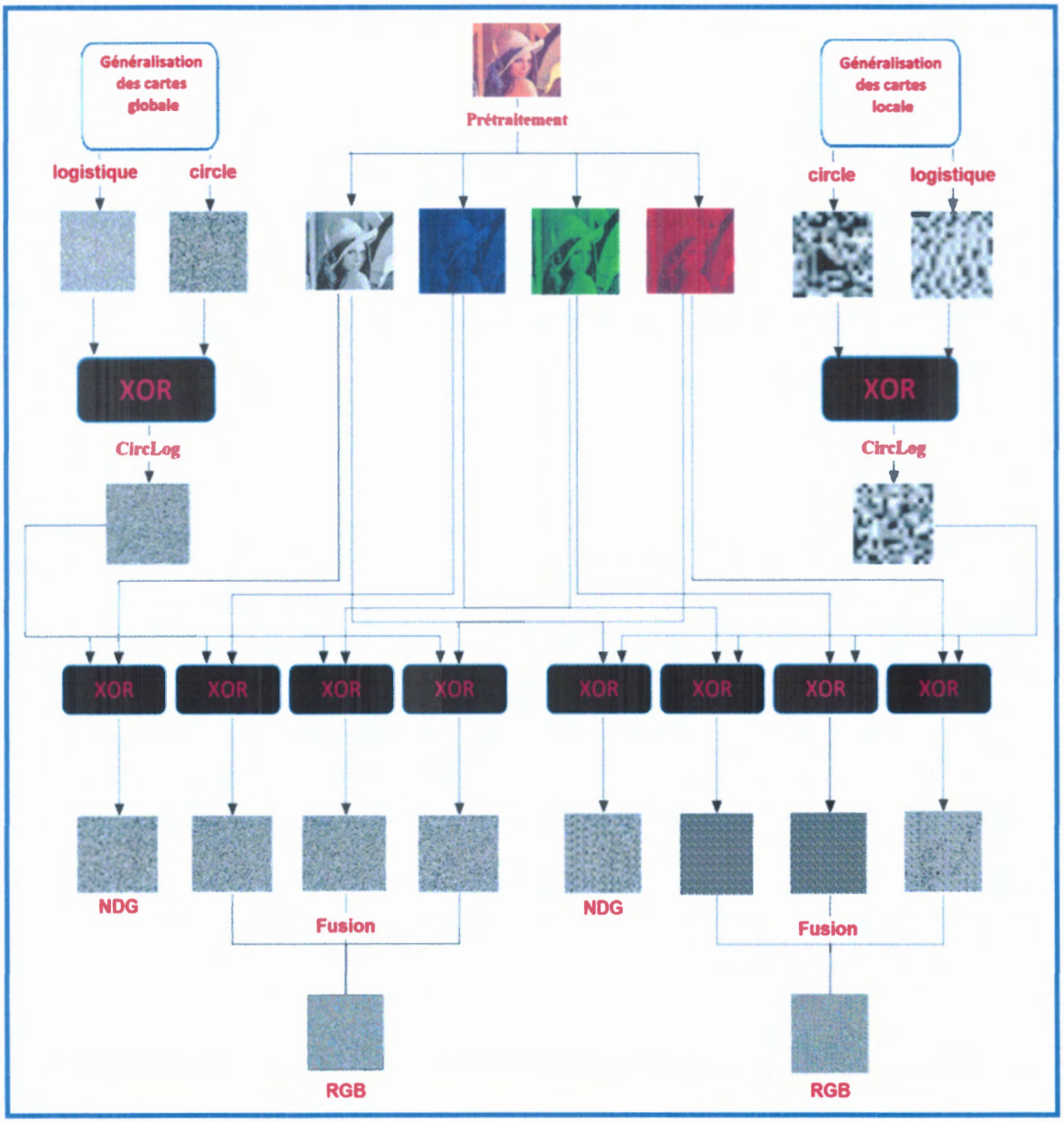

FIGURE 4.4 – Schéma illustratif de notre système de chiffrement /déchiffrement chaotique des images.

4.2.1 pré-traitement

Une image est définie comme une suite de pixels (des points lumineux). Chaque pixel possède une couleur : celle-ci est définie par un nombre entier, converti par la suite en binaire.

Dans notre travail, nous avons utilisé des images en niveau de gris et des images couleurs.

a)Conversion vers niveau de gris

Une image en niveaux de gris a des couleurs qui sont des nuances de gris. La raison pour différencier ces images de toute autre sorte d'image couleur est que moins d'informations doivent être fournies pour chaque pixel. En fait, une couleur grise est celle dans laquelle les composantes rouge, vert et bleu ont tous une intensité égale dans l'espace RVB, et il est donc seulement nécessaire de spécifier une seule valeur d'intensité pour chaque pixel, par opposition, trois intensités sont nécessaires pour spécifier chaque pixel dans une image couleur.Souvent, l'intensité au niveau de gris est stockée comme un entier de 8 bits produisant 256 nuances de gris du noir au blanc.

FIGURE 4.5 – conversion d'image vers niveau de gris

b) Diffusion vers R, G, B

Le rouge, vert et bleu (RGB en anglais) est un espace de couleur largement utilisé pour l'infographie. Le rouge, le vert et le bleu sont les trois couleurs primaires additives (composants individuels additionnés pour former une couleur souhaitée) et sont représentés par un cube tridimensionnel tel que le rouge, vert et bleu se situent dans les coins de chaque axe, le noir à l'origine et le blanc à l'opposé. L'échelle du niveau de gris suit la ligne du noir au blanc, dans un système graphique de 24 bits avec 8 bits pour chaque canal, le rouge est (255, 0, 0) tandis que dans le cube de couleur.

FIGURE 4.6 – Diffusion vers R, G, B

4.2.2 Chiffrement

Le principe de chiffrement est simple, il s'agit "d'effectuer le (ou exclusif)" entre deux matrices, la matrice clé et la matrice qui correspond à l'image qu'on veut crypter, grâce à l'opérateur XOR. Les éléments de la matrice clé sont générés par une des fonctions chaotiques décrites dans la section précédente.
Pour le mode de chiffrement, nous avons utilisé dans notre application, deux modes différents :

a.Chiffrement globale : dans ce mode, l'image entière constitue l'entrée de l'algorithme de chiffrement. Trois images clés sont générées qui correspond aux trois fonctions décrites précédemment.

b.Chiffrement par bloc : l'image est divisée à un ensemble de blocs, chaque bloc est de taille 16×16 pixels. Pour chaque nouveau bloc à chiffrer, les paramètres de chiffrements sont initialisés et une nouvelle image clé est définie.

4.2.3 Application du XOR

le schéma suivant illustre l'application du XOR entre un pixel en clair défini en mode RGB et les valeurs générées par une des fonctions décrites précédemment.

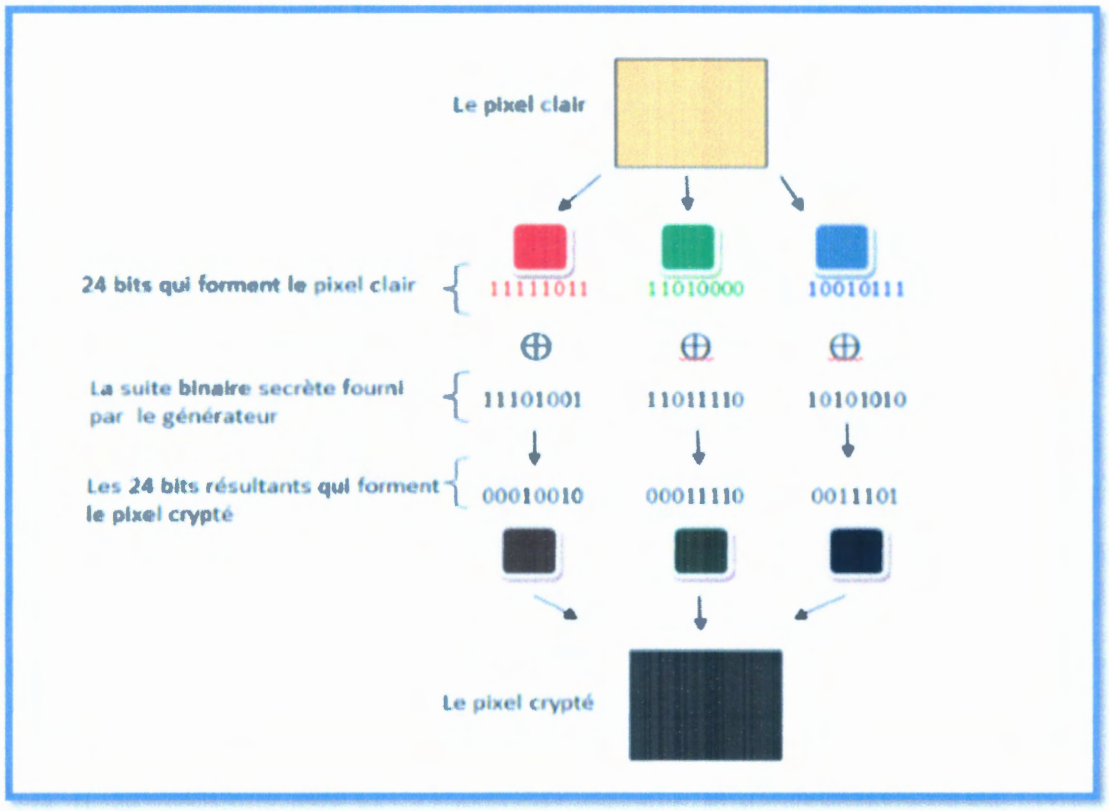

FIGURE 4.7 – Exemple de chiffrement d'un pixel.

4.2.4 Algorithme de chiffrement/déchiffrement chaotique

Dans cette section, nous discutons, étape par étape, l'algorithme proposé pour les processus de chiffrement globale.

Entrée : img : une image de taille M × N.

Etape 1 : définir la matice Mat.

-pour une image au niveau de gris :$Mat_{NG}(i,j)$: désigne le niveau de gris dans l'intervalle de 0 à 255 du pixel qui possède la position (i,j), où 1 ≤ i ≤ M et 1 ≤ j ≤ N.

-pour une image couleur : trois matrice sont définies ;
$Mat_R(i,j)$: désigne la valeur de la couleur Rouge à la position du pixel (i, j). $Mat_G(i,j)$: désigne la valeur de la couleur verte à la position du pixel (i, j). $Mat_B(i,j)$: désigne la valeur de la couleur bleu à la position du pixel (i, j), où $1 \leq i \leq Met1 \leq j \leq N$.

Etape 2 : Générer une matrice Mchao de taille M × N, qui représente les valeurs de séquence chaotique dans l'intervalle de 0 à 1 en utilisant le principe des fonctions (4.1), (4.2) et (4.3). Les différentes valeurs des conditions initiales et des paramètres de chaque fonction sont données dans le tableau 4.1.

Étape 3 : Générer C' = Mat XOR Mchao.

Sortie : image cryptée.

-Pour les images couleurs, les trois matrices Mat_R, Mat_B,Mat_G sont chiffrées séparément (cf **Figure4.7**).

-Pour le processus de chiffrement par bloc, le principe reste le même, la différence est que dans l'étape 3 de l'algorithme précédent plusieurs matrices chaotiques sont générées, le nombre de ces matrices égale aux nombres de blocs de limage originale.

-Pour récupérer l'image originale, on applique l'algorithme inverse.

-afin de renforcer notre système de cryptage nous exécutons 4 itérations de cet algorithme.

Le tableau suivant, présente les valeurs des conditions initiales et des paramètres de chaque fonction utilisée dans notre application.

	Fonction Logistique	Fonction Circle Map	Fonction CircLog
Condition initiale x_0	0.001	0.5	0.5
r	3.99	/	/
K_1	/	1.001	1.001
K_2	/	2.002	2.002
K_3	/	3.003	3.003

TABLE 4.1 – les valeurs des conditions initiales et des paramètres de chaque fonction utilisée dans notre application.

4.3 Développement de notre application de cryptage chaotique

4.3.1 Langage de développement :

Afin de développer notre application on a utilisé le langage python version 2.7 comme un moyen de simulation pour implémenter un algorithme de sécurisation d'images numériques. Python est un langage de programmation orienté objet interprété, sa syntaxe est simple et claire, elle respecte les standards du domaine.

4.3.2 Les images utilisées

4.4 Analyse de sécurité :

Un algorithme de chiffrement idéal est l'algorithme qui résiste à toutes sortes d'attaques. Nous discutons dans cette section, les résultats de la sécurité et l'analyse des performances effectués sur l'algorithme proposé de chiffrement d'images.

4.4.1 Analyse d'histogramme :

Dans un contexte de traitement d'image, l'histogramme d'une image désigne un histogramme des valeurs d'intensité des pixels. Cet histogramme est un graphique illustrant le nombre de pixels dans une image à chaque valeur d'intensité trouvée dans cette image. Pour une image grise il y a 256 intensités différentes possibles, ainsi, l'histogramme s'affiche graphiquement en utilisant 256 chiffres indiquant la distribution des pixels entre ces valeurs de niveaux de gris **[40]**.

FIGURE 4.8 – Exemple d'histogramme niveau de gris

Les histogrammes peuvent également être pris d'images en couleur ; soit des histogrammes individuels des canaux rouge, vert et bleu, ou un seul histogramme 3-D avec les trois axes représentant les trois plans, et la luminosité dans chaque point représente le nombre de pixels. En conséquence, l'histogramme d'une image ne représente pas la répartition spatiale ; ainsi, deux images différentes peuvent disposer le même histogramme [41].

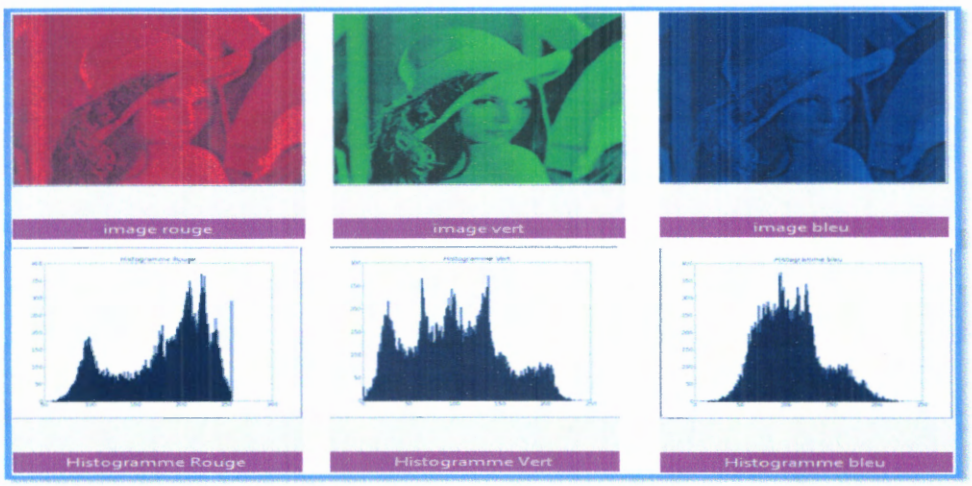

FIGURE 4.9 – Exemple d'histogramme R,G,B

Dans un contexte de chiffrement d'image, l'histogramme de l'image chiffrée doit être uniforme pour qu'un adversaire ne puisse extraire aucune information à partir de cet histogramme.

On peut bien voir que les histogrammes des images chiffrées sont très différents de celui de l'image originale. L'algorithme de chiffrement utilisé fait en sorte que la dépendance des propriétés statistiques de l'image chiffrée et de l'image originale soit quasi aléatoire. Ceci rend la cryptanalyse de plus en plus difficile.

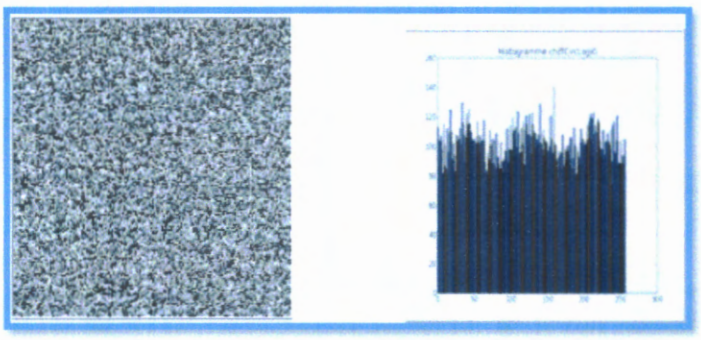

FIGURE 4.10 – Histogramme de chiffrement locale de l'image originale.

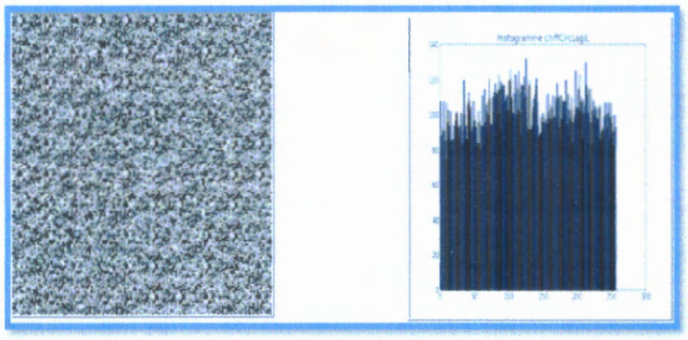

FIGURE 4.11 – Histogramme de chiffrement globale de l'image originale.

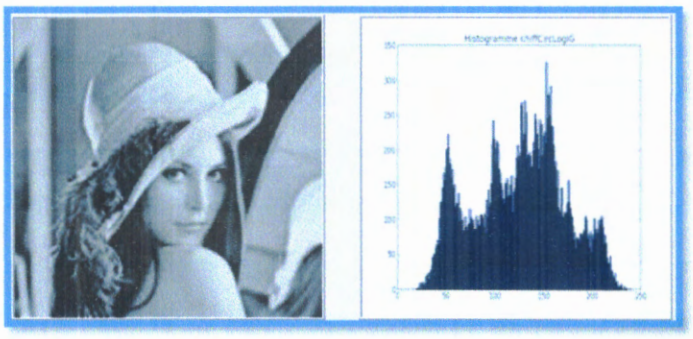

FIGURE 4.12 – Histogramme de l'image décryptée selon le mode de chiffrement globale.

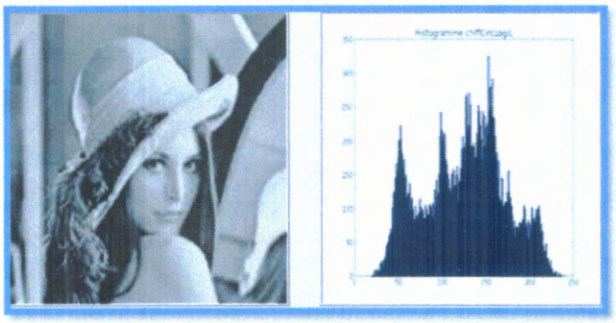

FIGURE 4.13 – Histogramme de l'image décryptée selon le mode de chiffrement local.

4.4.2 Analyse de Coefficient de Corrélation :

La corrélation est une technique qui permet de comparer deux images pour estimer les déplacements des pixels d'une image par rapport à une autre image de référence.
Les pixels adjacents d'une image standard ont une forte corrélation. Un bon schéma de cryptage d'image doit supprimer une telle corrélation afin d'assurer la sécurité contre l'analyse statistique.
Afin de tester la corrélation entre deux images on choisit au hasard des paires de deux pixels adjacents dans les trois directions ; horizontal, vertical et diagonal à partir des composants R, G, B de l'image claire et son image chiffrée et les coefficients de corrélation de chaque paire ont été calculées en utilisant les formules suivantes :

$$r = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{4.4}$$

où

$$cov(x,y) = 1/N \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{4.5}$$

$$E(x) = 1/N \sum_{i=1}^{N} x_i, D(x) = \sum_{i=1}^{N} (x_i - E(x))^2 \tag{4.6}$$

Les tableaux 4.2, 4.3 , 4.4 et 4.5 liste les coefficients de corrélation des images claires et leurs chiffrées en utilisant le schéma proposé. Les coefficients de corrélations mesurées des images claires sont près de 1 tandis que ceux des images chiffrées sont proches de 0. Basant sur les résultats obtenus, nous pouvons affirmer que l'algorithme proposé a supprimé avec succès la corrélation des pixels adjacents.

★ **Pour le chiffrement des images niveau de gris**

a) Pour l'image originale :

mode de chiffrement	Nom d'image	Image Originale		
		Horizontale	Verticale	Diagonale
Chiffrement Locale	lena	0.9108442	0.9581544	0.8759888
	babon	0.7163711	0.6035276	0.6107996
	barbara	0.8745833	0.9136446	0.8409144
Chiffrement Globale	lena	0.9108442	0.9581544	0.8759888
	babon	0.7163711	0.6035276	0.6107996
	barbara	0.8745833	0.9136446	0.8409144

TABLE 4.2 – Coefficients de corrélation horizontale, verticale, diagonale de l'image originale.

b)Pour l'image cryptée :

Mode de Chiffrement	Nom d'image	Image Cryptée			
		Fonction de Cryptage	Horizontale	Verticale	Diagonale
Chiffrement Locale	lena	Fonction Logistique	0.0002680	0.0426909	-0.1114371
		Fonction Circle map	-0.1030496	-0.0394419	0.0435764
		Fonction CircLog	-0.0609522	-0.0493396	-0.0273738
	babon	Fonction Logistique	-0.0451638	-0.0639043	-0.0316764
		Fonction Circle map	-0.0754467	-0.0299956	0.0214047
		Fonction CircLog	-0.0193711	0.0398797	-0.0408011
	barbara	Fonction Logistique	-0.0459532	-0.1083657	-0.0332223
		Fonction Circle map	-0.1014723	-0.0339550	-0.027999
		Fonction CircLog	-0.0366406	-0.0402389	-0.0328352
Chiffrement Globale	lena	Fonction Logistique	-0.0457293	0.0250099	0.0253157
		Fonction Circle map	-0.9731612	-0.0145812	0.0035511
		Fonction CircLog	0.01891914	0.0102490	-0.0079168
	babon	Fonction Logistique	-0.0245975	0.0110723	0.0033138
		Fonction Circle map	-0.0640476	0.0012155	0.0004028
		Fonction CircLog	0.00904963	0.0029419	-0.0041271
	barbara	Fonction Logistique	-0.0288291	0.0120493	0.0008277
		Fonction Circle map	-0.0823822	-0.0031317	0.0028553
		Fonction CircLog	0.01498664	0.0016634	-0.0090008

TABLE 4.3 – Coefficients de corrélation de deux pixels adjacents pour le chiffrement locale /globale.

-Si le coefficient est 1 donc les deux images sont égaux (l'image n'est pas chiffrée). Sinon, Si la valeur obtenue est 0 ou proche de 0 alors les deux images sont différentes (l'image est bien chiffrée).

★ **pour le chiffrement des images RGB**

a) pour l'image originale :

mode de chiffrement	Nom d'image	Image Originale		
		Horizontale	Verticale	Diagonale
Chiffrement Locale	lena	0.92020734	0.96295377	0.88791146
	babon	0.86805914	0.80050198	0.80626670
	barbara	0.89433254	0.92470394	0.86314349
Chiffrement Globale	lena	0.92020734	0.96295377	0.88791146
	babon	0.86805914	0.80050198	0.80626670
	barbara	0.89433254	0.92470394	0.86314349

TABLE 4.4 – Coefficients de corrélation horizontale, verticale, diagonale de l'image originale.

b) Pour l'image cryptée :

Mode de Chiffrement	Nom d'image	Image Cryptée			
		Fonction de Cryptage	Horizontale	Verticale	Diagonale
Chiffrement Locale	lena	Fonction Logistique	0.06915466	-0.10120541	-0.08306132
		Fonction Circle map	-0.10178507	0.09050030	-0.09019337
		Fonction CircLog	0.03494163	-0.02589445	-0.09019337
	babon	Fonction Logistique	-0.01974442	-0.00795809	-0.03142644
		Fonction Circle map	-0.07084881	0.04361579	-0.04546306
		Fonction CircLog	0.0017785	-0.01571399	0.02324536
	barbara	Fonction Logistique	-0.0323736	0.0453141	-0.0263547
		Fonction Circle map	-0.00808041	0.00167680	0.00092000
		Fonction CircLog	0.01841189	-0.01644045	-0.04261184
Chiffrement Globale	lena	Fonction Logistique	0.00067636	-0.00637151	0.00862705
		Fonction Circle map	-0.00851572	0.00243694	-0.00243044
		Fonction CircLog	0.03494163	-0.02589445	-0.09019337
	babon	Fonction Logistique	-0.00771234	0.00447767	0.00760571
		Fonction Circle map	0.00031444	0.00228156	-0.00638581
		Fonction CircLog	0.0017785	-0.01571399	0.02324536
	barbara	Fonction Logistique	-0.00398445	0.00074690	-0.00710086
		Fonction Circle map	-0.08608327	0.06289617	-0.04607027
		Fonction CircLog	0.00761346	-0.00771150	-0.00414996

TABLE 4.5 – Coefficients de corrélation horizontale, verticale, diagonale de l'image cryptée.

D'après ces résultats des coefficients de corrélation, l'algorithme utilisé présente des bonnes aptitudes pour la confusion et la diffusion, et peut résister aux attaques statistiques.

La figure suivante montre les corrélations de deux pixels adjacents verticalement horizontalement et diagonalement dans l'image claire et son chiffrée. Il est clair que les pixels adjacents après le cryptage n'ont pas de corrélation.

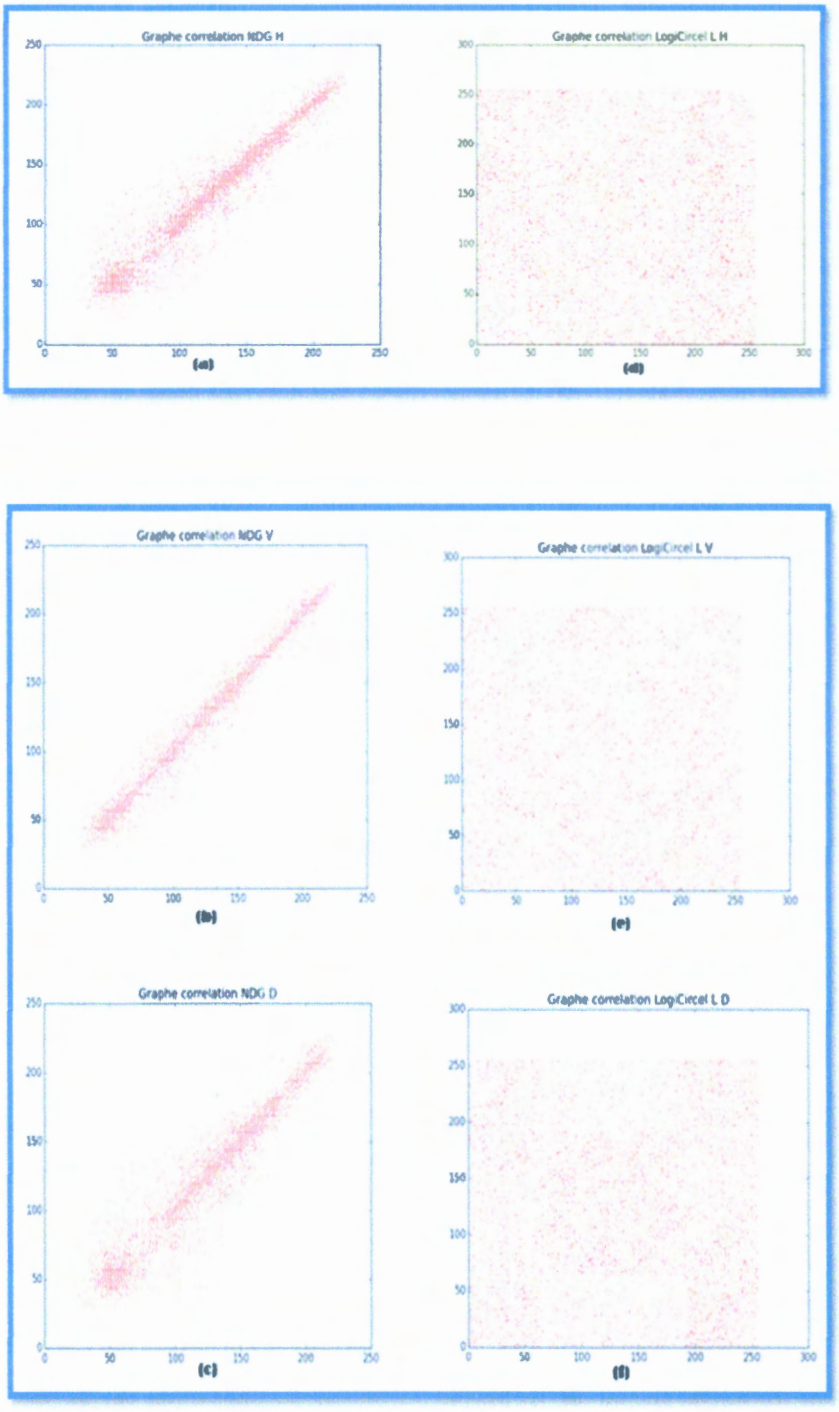

FIGURE 4.14 – Corrélation de deux pixels adjacents horizontalement, diagonalement et verticalement dans l'image originale et l'image chiffrée : (a), (b) et (c) sont pour l'image originale ; (d), (e) et (f) sont pour l'image cryptée.

On remarque dans les graphes des coefficients de corrélation du pixel adjacent horizontal, vertical et diagonal une bonne diffusion des pixels après le chiffrement.

4.4.3 Entropie :

L'entropie est une mesure statistique du hasard dans la théorie de l'information. La performance des algorithmes de cryptage est mesurée en calculant l'entropie de l'image originale et l'image cryptée, puis les comparer. L'entropie E de l'image est calculé en utilisant l'équation :

$$E = \sum_{i=0}^{255} [\ p(i) * log_2(1/p(i))] \tag{4.7}$$

Où p_i représente la probabilité du symbole i et l'entropie est exprimée en bits. Supposons que la source émet 28 symboles avec une probabilité égale, i.e., 0 à 255, $m = m_0, m_1, ..., m_{255}$ après évaluation de l'équation ci-dessus, on obtient son entropie $E = 8$, correspondant à une source véritablement aléatoire.
En fait, étant donné qu'une source d'information pratique génère rarement des messages aléatoires,en général,sa valeur d'entropie est plus petite que celle idéale.
Cependant,lorsque les messages sont chiffrés, leur entropie devrait idéalement être 8. Si la sortie d'un tel chiffre émet des symboles avec une entropie inférieure à 8,il existe un certain degré de prévisibilité qui menace sa sécurité.

★ **Pour le chiffrement des images niveau de gris**

Image Originale		Image Cryptée					
		Chiffrement Globale			Chiffrement Locale		
		Logistique	Circle map	Circlog	Logistique	Circle map	Circlog
lena	7.432656	7.988270	7.9898127	7.993223	7.987772	7.990958	7.991521
babon	7.389656	7.968060	7.9961464	7.997097	7.964966	7.996797	7.993542
barbara	7.434561	7.978269	7.995827	7.997027	7.975671	7.996144	7.996398

TABLE 4.6 – Entropie des images cryptée (niveau de gris).

★ **Pour le chiffrement des images RGB**

Entropie des images couleurs cryptée.

Image Originale		Image Cryptée					
		Chiffrement Globale			Chiffrement Locale		
		Logistique	Circle map	Circlog	Logistique	Circle map	Circlog
lena	7.452201	7.994099	7.993127	7.991647	7.991043	7.991261	7.991299
babon	7.389656	7.997324	7.997456	7.996816	7.995919	7.996470	7.995962
barbara	7.4345	7.9973	7.9971	7.9972	7.9969	7.996209	7.9964

Les tableaux 4.6 et 4.7 illustre les valeurs d'entropie obtenues pour des images claires et chiffrées différentes. La plus grande valeur d'entropie dans ce cas est proche de 8 donc on peut confirmer que l'algorithme proposé fournit les meilleures propriétés d'aléatoire.

4.4.4 Analyse de sensibilité :

Afin de détecter la relation entre l'image originale et l'image cryptée, un adversaire fait un petit changement sur l'image claire,ensuite utilise l'algorithme de cryptage pour crypter l'image avant et après le changement,dans le but de tester comment une petite modification dans l'image originale affecte l'image cryptée.Ce genre d'attaque est appelé attaque différentiel.

Pour assurer la sécurité d'un schéma de cryptage d'image contre l'analyse différentielle, deux mesures quantitatives sont utilisés : le **NPCR** (Number of Pixels Change Rate) et **l'UACI** (Unified Average Changing Intensity).

Le **NPCR** représente le taux de pixels différents entre les deux images chiffrées, tandis que **l'UACI** représente la différence de l'intensité moyenne. La formule utilisée pour calculer ces deux pourcentages est définie comme suit :

$$NPCR = \frac{\sum_{i,j} f(i,j)}{W * H} * 100\% \tag{4.8}$$

$$UACI = \frac{1}{H * W}[\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255}] * 100\% \tag{4.9}$$

Où W et H représentent la largeur et la hauteur de l'image respectivement.

$C_1(i,j)$ est l'image cryptée et $C_2(i,j)$ est l'image cryptée après avoir changé un pixel de l'image clair.

Pour les pixels à la position (i,j), si $C_1(i,j) \neq C2(i,j)$, alors $f(i,j) = 1$; sinon $f(i,j) = 0$.

Un **NPCR** $> 99,6094\%$ et un **UACI** $> 33,4635\%$ assure qu'un schéma de chiffrement d'image est sécurisé contre une attaque.

Le tableau suivant résume les valeurs des différentes mesures obtenues après les tests qui ont été effectués sur une image originale (lena, image de taille $256 * 256$ en niveau de gris), par un chiffrement chaotique.

★ **pour le chiffrement des images niveau de gris**

a) Pour l'image originale :

Nom d'image	NPCR	UACI
lena	0	0
babon	0	0
barbara	0	0

TABLE 4.7 – Les Valeurs de NPCR et UACI des images originale (niveau de gris).

b) Pour l'image cryptée :

Mode de Chiffrement	Nom d'image	Image Cryptée		
		Fonction de Cryptage	NPCR	UACI
Chiffrement Locale	lena	Fonction Logistique	99.609375	30.489797
		Fonction Circle map	99.609375	27.465747
		Fonction Circlog	99.21875	29.408639
	babon	Fonction Logistique	100	25.795228
		Fonction Circle map	99.609375	26.829247
		Fonction Circlog	99.21875	27.281266
	barbara	Fonction Logistique	100	26.663279
		Fonction Circle map	99.609375	27.506462
		Fonction Circlog	99.21875	26.978212
Chiffrement Globale	lena	Fonction Logistique	99.996093	30.352205
		Fonction Circle map	99.585937	28.413970
		Fonction Circlog	99.5625	28.431648
	babon	Fonction Logistique	100	26.663279
		Fonction Circle map	99.624633	27.765096
		Fonction Circlog	99.635314	27.916164
	barbara	Fonction Logistique	100	27.8964771
		Fonction Circle map	99.624633	28.628456
		Fonction Circlog	99.560546	28.774216

TABLE 4.8 – Les Valeurs de NPCR et UACI des images cryptée (niveau de gris).

★ **Pour le chiffrement des images RGB**

a) Pour l'image cryptée :

Mode de Chiffrement	Nom d'image	Image Cryptée		
		Fonction de Cryptage	NPCR	UACI
Chiffrement Locale	lena	Fonction Logistique	99.55078125	28.61363357
		Fonction Circle map	99.5	29.16920955
		Fonction Circlog	99.53515625	28.32438725
	babon	Fonction Logistique	99.52850341	27.40503049
		Fonction Circle map	99.65057373	28.16049014
		Fonction Circlog	99.56512451	26.32939955
	barbara	Fonction Logistique	99.59411621	28.40216543
		Fonction Circle map	99.61090087	28.89239741
		Fonction Circlog	99.56207275	27.97452440
Chiffrement Globale	lena	Fonction Logistique	99.60546875	28.45954350
		Fonction Circle map	99.60546875	28.58691789
		Fonction Circlog	99.61328125	28.37201286
	babon	Fonction Logistique	99.62005615	27.95239018
		Fonction Circle map	99.59869384	27.97296262
		Fonction Circlog	99.59411621	27.82320508
	barbara	Fonction Logistique	99.61853027	28.59679577
		Fonction Circle map	99.62158203	28.65023743
		Fonction Circlog	99.61242675	28.77766328

TABLE 4.9 – Les Valeurs de NPCR et UACI des images crypté (RGB).

Conclusion

Dans ce chapitre, nous avons présenté dans un premier lieu notre approche de cryptage et décryptage chaotique qui se base sur la définition d'une nouvelle fonction chaotique CircLog, Ensuite en deuxième lieu, nous avons présenté notre application qui permet de crypter et décrypter des images en se basant toujours sur la fonction CicLog. Les résultats obtenus nous permet de prouver sa grand niveau de sécurité.

Conclusion générale

Le développement rapide des réseaux de communication a provoqué de nouveaux problèmes de la sécurité des données.

La sécurisation des données stockées ou transmises est généralement effectuée par des techniques de cryptage dont leur développement est devenu un grand challenge dans ces dernières années.

Après une étude bibliographique des techniques de cryptage basées sur la cryptographie standard (DES, AES, RSA), nous avons constaté qu'elles ne sont pas très robustes aux attaques récentes, car elle est fondée sur les calculs algébriques. C'est l'une des raisons qui ont déclenché, la nécessité de chercher d'alternatif, dont l'usage du chaos sujet de notre travail, est l'une des solutions proposées.

Dans ce manuscrit, nous nous somme basé sur la cryptographie chaotique. Nous avons commencé notre mémoire par une synthèse sur la théorie du chaos, où nous avons apporté quelques notions de base, tel que l'illustration des caractéristiques des systèmes chaotiques, et la présentation de quelques systèmes chaotique les plus célèbres.Ensuite nous avons abordé la cryptographie, où nous avons introduit les objectifs de la cryptographie.

Nous avons abordé, par la suite, les différentes catégories de la cryptographie depuis sa première apparition jusqu'à nos jours. le chiffrement classique, les deux principales familles de cryptosystèmes en énumérant par la suite les algorithmes de chiffrement symétrique et les différents modes du chiffrement symétrique, après nous avons terminé par une description du chiffrement quantique.

Ensuite nous sommes intéressées à la cryptographie chaotique. A cet effet, nous avons présenté plusieurs modes de chiffrement de l'information incluant une dynamique chaotique.

Enfin, Nous intéressons par le chiffrement/déchiffrement d'image à base du chaos, en utilisant la fonction logistique et la carte du cercle. Les résultats expérimentaux montrent que cette fusion présente un grand niveau de sécurité.

En perspectives de ce travail :

- Appliquer les systèmes chaotiques sur d'autre types des données, à savoir le signal de la parole et la vidéo .

- les ressources informatiques restent des fois limitées face à une quantité énorme d'informations à stocker ou à transférer. Dans l'objectif d'optimisation du temps de transmission de chaque image ainsi que de son espace de stockage, une approche de compression d'image doit être combinée avec les schémas de cryptages proposés.

~~1.~~

Bibliographie

[1] Yahia Moussa. Elaboration d'algorithmes de masquage pour les systèmes de communication chaotique. thèse de doctorat en electronique. université mentouri constantine.19 avril 2012.

[2] Hamid Hamiche. Invrsion à gauche des système dynamiques hybrides chaotiques .mémoire de magister en : Automatique. université mouloud mammeri de tizi-ouzou. 2011.

[3] N.Kouadri Moustefai. Test de validation pour les crypto-systèmes chaotiques .mémoire de magister .l'université de sciences et technologies mohamed boudief oran.juin 2014.

[4] Abdul Rahuman Ahmed. Analyse des systèmes non-linéaires à dynamiques complexes. mémoire de magister. université abou bekr belkaid faculté des sciences de l'ingénieur département d'électroniques.2009.

[5] Mihai Bogdan Luca. Apports du chaos et des estimateurs d'états pour la transmission sécurisée de l'information.thèse doctorat.2006.

[6] `http://www.juliensalort.org.2016`.

[7] Hassan Noura. Conception et simulation des generateurs, crypto-systemes et fonctions dehachage bases chaos performants. thèse doctorat en electronique. université de nantes.juin 2012.

[8] Kihal Ahmed Ridha. Système chaotiques pour la transmission sécurisée de donnée. mémoire de magister en electronique. université mohamed khider - biskra.2013.

[9] Tayeb Hamaizia. Systèmes dynamiques et chaos. thèse de doctorat en mathématique. l'université de constantine 1.avril 2013.

[10] Soula Yamina. Bifurcation et symétrie dans les systèmes dynamiques discrets couples. thèse de doctorat en sciences en mathématiques. université de constantine 1 juin 2014.

[11] Meriem Halimi. Observation et détection de modes pour la synchronisation des systèmes chaotiques : une approche unifiée. thèse de doctorat. université de lorraine.décembre 2013.

[12] M. Baudet. Sécurité des protocoles cryptographiques : aspects logiques et calculatoires. thèse de doctorat en informatique. l'école normale supérieure de cachan.16 janvier.

[13] N. Sad Houari. Cryptographie et sécurité informatique. thèse de doctorat en mathémtique et informatique. université d'oran ahmed ben bella.2017.

[14] Z. Kaddouri. Mise en oeuvre de nouvelles techniques pour la sécurité informatique basees sur les algorithmes evolutionnistes et les fonctions de hachage. thèse de doctorat en informatique. faculté des sciences de rabat, maroc.4 décembre 2014.

[15] N.Medjahdi. Cryptage chaotique basé sur l'attracteur clifford. mémoire de master en informatique. université abou bakr belkaid .2016-2017.

[16] A. Wurcker. étude de la sécuritv d'algorithmes de cryptographie embarquée vis-à-vis des attaques par analyse de la consommation de courant. thèse de doctorat en informatique. université de limoges.23 octobre 2015.

[17] Come Berbain. Analyse et conception d'algorithme de chiffrement flot. thèse de doctorat, université paris (paris 7).octobre 2007.

[18] M.Videau. Critères de sécurité des algorithmes de chiffrement clé secrète. thèse de doctorat . université paris 6 novembre 2005.

[19] G.Thomas. Design et analyse de sécurité pour les constructions en cryptographie symétrique. thèse de doctorat . université de limoges.2 juin 2015.

[20] J. Buchmann. Introduction à la cryptographie . dunod. paris.2006.

[21] R. Dumont. Cryptographie et sécurité informatique.notes de cours provisoires. université de liége .2009 - 2010.

[22] S. Jacob. Protection cryptographique des bases de données :conception et cryptanalyse. thèse de doctorat en informatique. université pierre et marie curie.08-03-2012.

[23] Goumidi Djamal Eddine. Fonction logistique et standard chaotique pour le chiffrement des images satellitaires mémoire de magister. école doctorale en electronique. spécialité télécommunications spatiales. 2010.

[24] Houda Ferradi. Introduction à la cryptographie :chiffrement par bloc (des) . université paris 13 villetaneuse. spécialité télécommunications spatiales. 01-02-2016.

[25] Idiri Fahima. Algorithmes de chiffrement asymétrique à base de factorisation :mise en oeuvre de rsa. rabin et paillier .mémoire de master. université a/mira de béjaia. 2015.

[26] P. Barthélemy et all. Cryptographie.herme-science . paris.2005.

[27] Boukhatem mohammed belkaid. Application des techniques de cryptage pour la transmission sécurisée d'image msg. mémoire de magister en electronique. université mouloud mammeri tizi-ouazou.11-03-2015.

[28] C.E. Shannon. Communication theory of secrecy systems.bell systemtechnical journal. vol 28 n10 pp. 656-715.october.1949.

[29] G.Ribordy et all. Un saut quantique en crypto 92 proceedings. p. 487-496.springer-verlag.

[30] R.Tenny. Symmetric and asymmetric secure communication schemes. thèse de doctorat. university of califorania san diego.2003.

[31] Floriane Anstett. Les systèmes dynamiques chaotiques pour le chiffrement : synthèse et crypt-analyse .centre de recherche en automatique de nancy (cran) . thèse de doctorat.2005.

[32] D.Benzemam. Systèmes chaotiques et hyperchaotiques pour la transmission sécurisée de données . mémoire de magister en télécommunications. laboratoire de telecommunication de telemcen .thése de doctorat en electronique. école doctorale sciences et technologie.2009-2010.

[33] O.Megherabi. étude et réalisation d'un systémes sécurisé à base de systèmes chaotiques .mémoire de magister.université mouloud mammeri tizi- ouzou. 10-10-2013.

[34] Kassem Ahmad. Protocoles, gestion et transmission sécurisée par chaos des clès secrètes. applications aux standards : Tcp/ip via dvb-s, umts, eps . hèse de doctorat en electronique. école doctorale sciences et technologie. 16 juillet 2013.

[35] C .Benhabib. Etude d'un système chaotique pour la sécuritsation des communications optiques . mémoire de master en télécommunications. université de tlemcen . thèse de doctorat.2014.

[36] H.Hamiche. Inversion à gauche des systèmes dynamiques hybrides chaotiques.application à la transmission sécurisé de données . thèse de doctorat. université mouloud mammeri tizi-ouzou.2011.

[37] I.Talbi. Systèmes dynamiques non linèaires et phénoménes de chaos . mémoire de magister en mathématiques.université mentouri de constantine. p. 487-496.springer-verlag.29 -06-2010.

[38] V. Kamat.Symmetric Image Encryption Algorithm Using 3D Rossler System. University Dehradun.2014.

[39] S.Agarwal.Secure Image Transmission Using Fractal and 2D-Chaotic Map. University of Macau system.2017.

[40] D. Chattopadhyay .Symmetric key chaotic image encryption using circle map. National Institute of Technology. Durgapur . 2011.

[41] Y.Zhoul et all . A new1Dchaoticsystemforimageencryption.University of Macau system.2014.

[42] Er. Ankita Gaurlet all. Review : Image Encryption Using Chaos Based algorithms. Electronics and communication Engineering department.2014.

[43] S.Agarwal. Secure image transmission using fractal and 2d-chaotic map, university of macau system.2017.

[44] et al Z. Hua. 2d sine logistic modulation map for image encryption, university of macau system.2014.

[45] J. Fridrich. Symmetric ciphers based on two-dimensional chaotic maps , int jbifurc chaos. 1998.

[46] G.Chen et al. A symmetric image encryption based on 3d chaotic cat maps . chaos solitons and fractals .2004.

[47] Yaobin Mao et al .A novel fast image encryption scheme based on 3D chaotic Baker maps . Int J Bifurc Chaos.2004.

[48] S. Lian et al .A block cipher based on a suitable use of chaotic standard map . Chaos Solitons and Fractals.2005.

[49] https ://www.researchgate.net/publication/. A new substitution diffusion based image cipher using chaotic standard V. Patidar et al and logistic maps .2009.

[50] A. Anees. An image encryption scheme based on lorenz system for low profile applications .kwangwoon university and springer-verlag berlin heidelberg.2015.

[51] K. Mandal et al. Symmetric key image encryption using chaotic rossler. institute of technology system.2013.

[52] H.Qais et al. Symmetric key image encryption using chaotic rossler. institute of technology system.2013.

[53] M. Manikandan. An efficient and optimized color image encryption technique using lorentz.rossler and chen attractor.department of electronics et communication engineering.2015.