REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIUER ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED El-BACHIR El-IBRAHIMI

BORDJ BOU-ARRERIDJ

FACULTE DES SCIENCES ET TECHNOLOGIES

DEPARTEMENT D'ELECTRONIQUE

MEMOIRE DE FIN D'ETUDES

Réalisé en vue de l'obtention du diplôme de MASTER

Option Electronique des systèmes embarqués

Thème

Développement de nouvelles suites chaotiques et leur application dans le cryptage d'images numériques.

Présenté par :

-Bendjoual NADJET

Encadré par :

- Dr Bekkouche TEWFIK

Soutenu publiquement le 07 / 09/ 2019 devant le jury composé de :

Pr.Z.Messali	Univ.B.Ibrahimi BBA	Président
Mme.N.DIFFELAH	Univ.B.Ibrahimi BBA	Examinateur

Année universitaire : 2018-2019

Remerciements

Avant tout on tient notre remerciement à notre dieu tout puissant de nous avoir donné la foi, la force et le courage.

Je remercie mon encadreur Dr Bekkouche TOUFIK, de sa Disponibilité, sa générosité professionnelle et ses précieux conseils.

Je remercie les membres du jury qui m'ont honoré de leur présence et d'avoir accepté de juger mon travail.

Merci à tous.

Bendjoual NADJET

Dédicaces

Je dédie ce travail à mes très chers parents, pour leur soutien et tous les efforts Qu'on m'a donnée le long de mon parcours et je leurs souhaite bonne santé et longue vie.

Je dédie ce travail aussi à mes frères et toutes mes sœurs.

A toute ma famille, tous mes amis

Et tous ceux que j'aime et qui m'aiment

A tous mes enseignants qui ont fait leurs possibles pour nous Donner le maximum d'informations concernant notre étude

Merci infiniment.

Bendjoual NADJET

Liste des figures

Liste des Tableaux :

Introduction générale

Introduction générale

Le chaos est un phénomène fascinant qui a été observé dans la nature (météo et climat, dynamique des satellites dans le système solaire, évolution dans le temps du système magnétique des corps célestes et croissance démographique en écologie) et en laboratoire (électricité circuits, lasers, réactions chimiques, dynamique des fluides, systèmes mécaniques et dispositifs magnéto-mécaniques). Le comportement chaotique a également trouvé de nombreuses applications en génie électrique et communication, information et communication technologies, biologie et médecine. Cela était principalement dû au caractère large bande des signaux chaotiques, contrôle expérimental facile du chaos et tout ce qui est réalisé avec une réalisation en laboratoire peu coûteuse des circuits électriques ou des algorithmes correspondants si seules les séries de nombres étaient au point. Communication et traitement du signal

Les applications du chaos, en tant que zones d'intérêt permanent, ont été grossièrement établies depuis 1990, après que les théories de la synchronisation du chaos et du contrôle du chaos ont été élaborées dans plus de détails. Aujourd'hui, des applications d'ingénierie sonore à séquence quasi aléatoire génération, modélisation des canaux de communication à l'aide du chaos, cryptographie chaotique, Encodage numérique d'images et phénomènes de transport chaotiques dans des réseaux complexes tous représentent des domaines de recherche permanente avec des solutions d'ingénierie commercialement fiables.

Durant les dernières décennies, les systèmes de communication ont complètement changés grâce aux technologies et aux nouveaux réseaux de communication, aussi bien dans les transmissions numériques qu'analogiques. En effet, de nos jours, des millions de kilo-octets d'informations confidentielles sont transmises à travers des canaux de communication non sécurisés, la révolution d'internet a permis que les échanges d'informations soient grandement facilités. Reste qu'avec ce flux permanent, nous peinons à trouver un espace de confidentialité. L'information peut, à tout moment être interceptée par des personnes non autorisées. La cryptographie, science déjà très ancienne, a assuré une certaine sécurité à l'aide d'algorithmes de cryptage traditionnels tel que AES, DES, RSA, etc, devenus aujourd'hui insuffisants.

En effet, la sécurité préoccupe de plus en plus d'utilisateurs dans des domaines variés (paiements sécurisés, courrier électronique confidentiel, signature électronique…).

La cryptologie est à la fois une science, un art et un champ d'innovation et de recherche. Pour cela, deux alternatives ont été développées durant cette dernière décennie :

- La cryptographie quantique, dérivée des prédicats de la mécanique quantique.
- La cryptographie chaotique, basée sur l'utilisation de systèmes chaotiques.

L'utilisation du chaos pour sécuriser les données est un sujet d'étude depuis plusieurs années. Le chaos trouve ses fondements dans l'article de Lorenz, où il a connu un développement mathématique dans les années 70 suivi d'un véritable essor scientifique. Le chaos est obtenu à partir de systèmes non linéaires. Il correspond à un comportement borné de ces systèmes ayant l'apparence d'un bruit pseudo aléatoire. Il peut donc être utilisé pour masquer ou mélanger les informations dans une transmission sécurisée.

L'une des propriétés des systèmes chaotiques est qu'ils présentent une sensibilité aux conditions initiales (SCI); Cela signifie que si l'on modifie légèrement un paramètre d'une équation ou d'un système, un comportement différent peut se produire et c'est ce qui fait leurs forces.

Notre travail dans ce mémoire est composé de trois chapitres. Le premier est consacré à des rappels sur la théorie du chaos et les suites chaotiques ont été effectués définition et propriétés du signal chaotique génération du chaos systèmes chaotiques continus suites chaotiques à temps discret. Le deuxième chapitre est dédié aux concepts fondamentaux de la cryptographie et le système de combinaison chaotique de R. Parvaz , M. Zarebnia.

Dans le troisième chapitre, nous avons proposé une suite chaotique modifiée appliquée au cryptage d'images. Cette suite s'inspire de la suite sinus de base appelée dans ce manuscrit suite sinus modifiée.

Ce manuscrit est clos par une conclusion relatant les principales remarques entourant l'élaboration de ce mémoire et des perspectives.

Chapitre 1

Chapitre 1 : Généralités sur la théorie du chaos et les suites chaotiques.

1.1 Introduction

La théorie du chaos fait partie des sciences les plus récentes et est devenue l'un des domaines les plus avancés dans la recherche contemporaine. Les origines de cette nouvelle théorie s'étendent aux mathématiques et physiques des débuts du 20ème siècle, mais elle a émergé dans les années 1960-1970. Durant des années, le chaos était considéré comme incontrôlable et même inutilisable, malgré la mise en équation de certains phénomènes et la démonstration du déterminisme dans des aspects d'apparence aléatoire.

La théorie du chaos est définie comme une étude des systèmes dynamiques non-linéaires complexes ou les systèmes complexes qui sont exprimés par des récurrences et des algorithmes mathématiques et qui sont dynamiques non constants et non périodiques. Elle inclut l'étude qualitative et quantitative d'un comportement instable non périodique et aléatoire des systèmes dynamiques non linéaires déterministes. Le chaos peut être vu aussi comme un système avec des propriétés stochastiques. Dans toutes les définitions qui peuvent exister pour le chaos, un phénomène fondamental est indispensable : la sensibilité aux conditions initiales.

En effet, en programmant son ordinateur et en changeant par 10^{-4} et les conditions initiales des prévisions météo, Edward Lorenz a découvert que pour certaine équation ou système d'équations non linéaires, les résultats montrent une grande sensibilité aux conditions initiales.

On peut dire que cet acte est la base du chaos déterministe.

La théorie du chaos influence l'explication de plusieurs phénomènes et trouve son application dans plusieurs domaines tels que :

- Economie : Prévision des cycles économiques, des mouvements commerciaux et des marchés financiers.
- Météo : Prévisions météorologiques.
- Santé : Prévision des crises d'épilepsie.
- Sciences sociales : Comportement des systèmes sociaux.
- Cryptage de l'information.

1.2 Définition et propriétés du signal chaotique

Plusieurs définitions peuvent être données pour le chaos. Le chaos dans son sens linguistique est la confusion générale des éléments, de la matière, avant la création du monde.

C'est le désordre. Une autre définition considère le chaos comme l'un des dispositifs intriguant de la dynamique non linéaire déterministe. Les systèmes dynamiques sont toute chose qui varie dans le temps. Les exemples sont diversifiés comme le pendule ou le système solaire. Il existe un espace d'état ou un espace de phase qui contient tout état possible du système et sa loi d'évolution qui décrit le futur lorsque le présent est donné. Une définition proposée par Devaney pour les systèmes à temps discret est la suivante :

Soit (χ, δ) un espace métrique compact et f : $\chi \to \chi$, une fonction.

Le système dynamique à temps discret $x_{n+1} = f(x_n)$ est dit chaotique si les conditions suivantes sont vérifiées :

- Sensibilité aux conditions initiales.
- Transitivité topologique.
- Densité des orbites périodiques.
- Ergodicité

1.2.1 Sensibilité aux conditions initiales

En faisant la troncature de quelques chiffres de conditions initiales de son système de prévision météorologique, Lorenz a mis en relief le caractère le plus important des systèmes chaotiques qui est la sensibilité aux conditions initiales. Mais en fait c'est avant cette anecdote, que ce phénomène a été découvert. Vers la fin du 19ème siècle, Poincaré montrait que les trois orbites de 3 corps en mouvement sous une force centrale due à la gravité changent radicalement avec une petite modification des conditions initiales.

Pour un système chaotique, une très petite erreur sur la connaissance de l'état initial x_0 dans l'espace des phases va se trouver (presque toujours) rapidement amplifiée.

Il existe un nombre réel $\beta > 0$, tel que pour tout $x_0 \in \chi$ et pour tout $\varepsilon > 0$, il existe un point $y_0 \in \chi$ et un entier $n > 0$ vérifiant :

$\delta(x_0, y_0) < \varepsilon \rightarrow \delta(x_n, y_n) > \beta$

1.2.2 Transitivité topologique

La fonction f est dite topologiquement transitive :

S'il existe $x \in \chi$ tel que l'orbite $\{f^n(x) / k \in \mathbb{N}\}$est dense dans χ. f^nreprésente la Nième composition de la fonction f.

1.2.3 Densité des orbites périodiques

Soit F et X deux ensembles. F est dense dans X ; si F est inclus dans X et si pour tout point $x \in X$, chaque voisinage de x contient au moins un point de F.

L'ensemble des orbites périodiques $\{x_0 \in \chi; \exists\, n > 0, x_n = x_0\}$ et est dense dans χ.

1.2.4 Ergodicité

L'ergodicité est la propriété dans laquelle les trajectoires suivies par les points appartenant à l'espace des phases se déplacent à travers l'espace avec une distribution uniforme. La trajectoire d'un système chaotique satisfait cette propriété. On peut dire autrement que l'ergodicité d'un système signifie qu'il parcourt tous les états possibles avec des probabilités égales.

1.2.5 Espace des phases

Les trajectoires dynamiques des systèmes chaotiques sont fréquemment situées dans un espace appelé espace de phase. Les régions de l'espace sans l'existence permanente des dynamiques chaotiques seront inutiles puisque les points dans ces zones tendent vers l'infini et ne contribuent pas à la continuité du processus chaotique. Les variables qui construisent cet espace doivent contenir toute information sur la dynamique du système. On forme alors des équations chaotiques fonctionnant avec ces coordonnées dans l'espace et chaque itération de ces équations signifie l'incrémentation au temps suivant.

1.2.6 Les attracteurs

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.

1.2.6 .1 Attracteurs réguliers

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

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.

Un cycle limite : la trajectoire du pendule idéal dans ce même espace des phases.

Un tore : qui correspond à l'attracteur obtenu par les mouvements résultant de deux oscillations indépendantes, par exemple : les oscillateurs électriques.

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 des phases restent

indéfiniment voisines. On sait donc prévoir l'évolution à long terme de ces systèmes, à partir d'une situation connue.

1.2.6 .2 Attracteurs étranges

On peut définir un attracteur en étant une limite asymptotique des solutions de toute condition initiale localisée dans un domaine de volume non nul ou bassin d'attraction.

Les trajectoires complexes dans l'espace de phase qui attirent les solutions du système chaotique sont alors des attracteurs. L'ensemble de points attirés vers l'attracteur constitue le bassin d'attraction. Autrement, l'attracteur est une figure géométrique de l'espace de phase indiquant le comportement d'un système chaotique. L'attracteur peut être étrange avec structure fractale ou bien point fixe ou bien cercle limite. Parmi les premiers exemples des attracteurs étranges mentionnés dans l'histoire du chaos, on cite l'attracteur de Lorenz. On donnera par la suite plusieurs exemples d'attracteurs étranges.

1.3. La 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 qui permettant une approche précise et certaine. Pour paraphraser une publicité célèbre, on pourrait écrire : "Ça ressemble à du hasard, ça a le goût du hasard,...mais ce n'est pas du hasard !".[1]

1.4 Génération du chaos

Il existe plusieurs systèmes chaotiques qui sont utilisés pour générer les signaux chaotiques.

Dans ce paragraphe, nous présenterons deux classes : les systèmes chaotiques continus et les systèmes chaotiques à temps discret.

1.4.1 Systèmes chaotiques continus

- **Attracteur de Lorenz**

Cet exemple a été publié en 1963 dans un journal météorologique. L'attracteur de Lorenz est généré par le système d'équations suivant :

$$\begin{cases} \dot{x} = -\sigma x + \sigma y \\ \dot{y} = \rho x - y - xz \\ \dot{z} = -\beta z + xy \end{cases} \quad (1.1)$$

Les paramètres σ, β et ρ sont des réels strictement positifs.

Le chaos est obtenu pour les valeurs suivantes : σ > β+1 ; ρ > 0 et ρ $> \frac{\sigma(\sigma+\beta+3)}{\sigma-\beta-1}$

La figure 1.1 illustre l'attracteur de Lorenz en 3 dimensions x(t), y(t) et z(t) tel que σ = 10, β = 8/3 et ρ = 28.

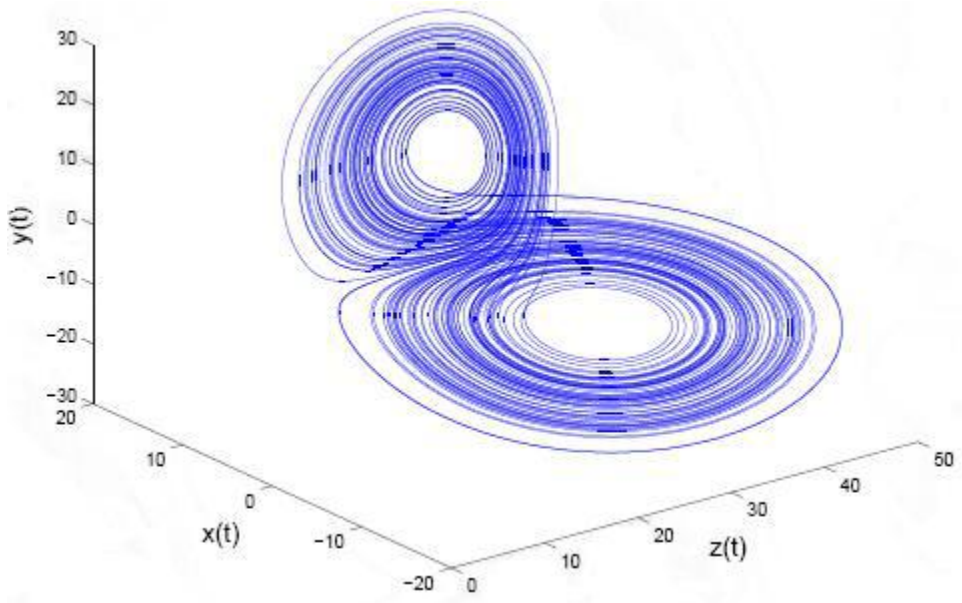


Figure 1.1. Attracteur de Lorenz.

- **Système de Chen**

Il est donné par le système d'équations suivant :

$$\begin{aligned} \dot{x} &= a(y - x) \\ \dot{y} &= (c - a)x - xz + cy \\ \dot{z} &= xy - bz \end{aligned} \quad (1.2)$$

La figure 1.2 montre l'attracteur de Chen en 3 dimensions x(t), y(t) et z(t) avec a=35, b=3 et c=28.

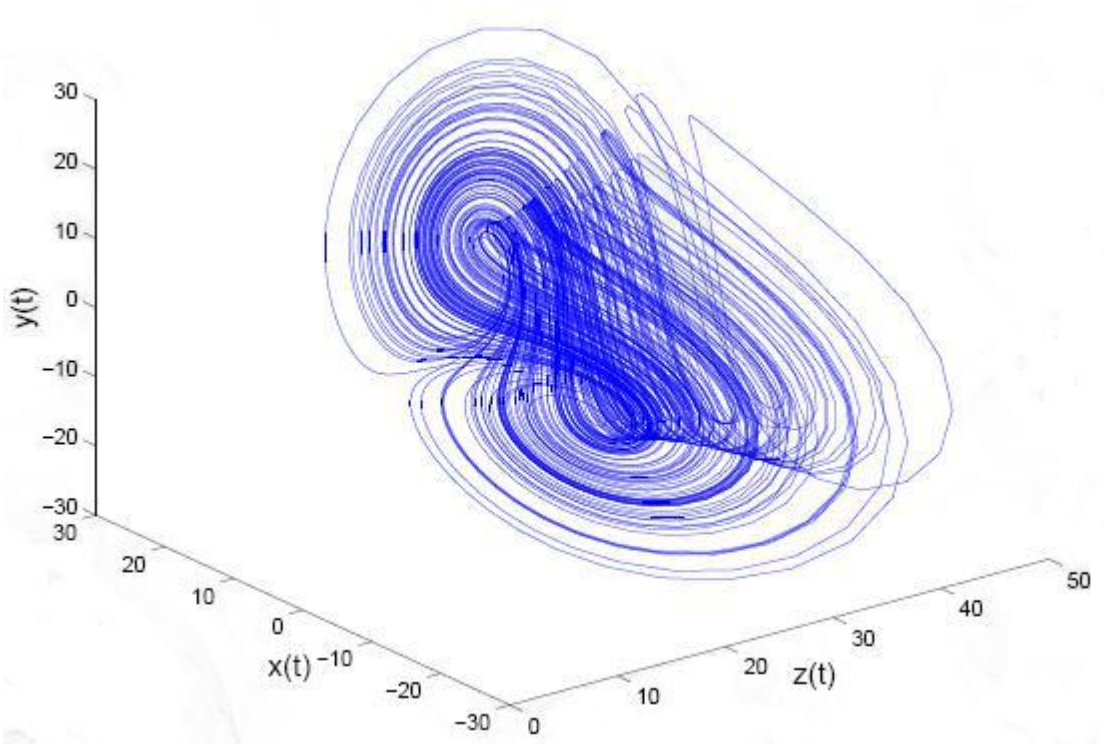


Figure 2.2. Attracteur de Chen.

- **Système de Rössler**

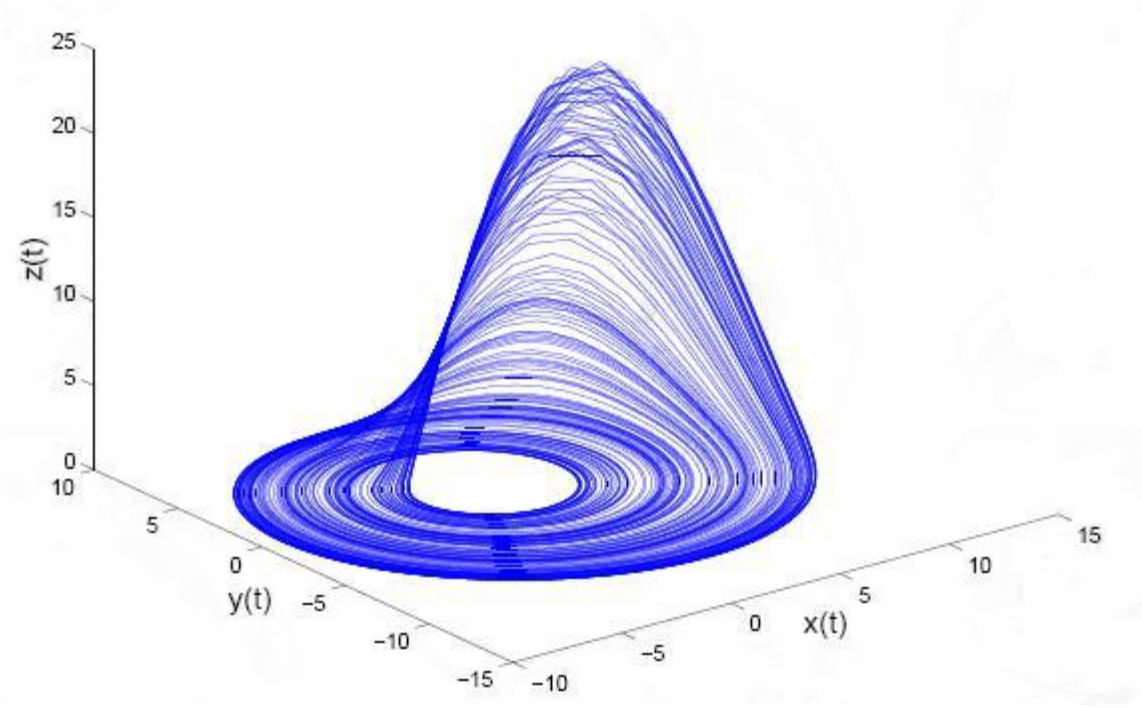


Figure 3.3. Attracteur de Rössler

Il a été inventé par Otto Rössler en 1976. Ce simple système chaotique est présenté comme suit:

$$\begin{aligned} \dot{x} &= -(y - z) \\ \dot{y} &= x + ay \\ \dot{z} &= (x - c)z + b \end{aligned} \tag{1.3}$$

Avec a = 0.2, b = 0.2 et c = 5.7

La figure 1.3 montre l'attracteur de Rössler en 3 dimensions x(t), y(t) et z(t).

1 .4.2 Suites chaotiques à temps discret

- **Suite logistique (Logistic Map)**

Cette fonction chaotique 1D non linéaire est donnée par l'équation suivante :

$$X_{n+1} = rX_n(1 - X_n) \tag{1.4}$$

où $r \in [0,4]$ est le paramètre de contrôle. Elle est générée itérativement en partant de $x_0 \in [0,1]$ appelée condition initiale. La suite logistique est vraiment chaotique si $r \in [3.75,4]$et purement chaotique si $r \cong 4$ La suite montre un bon comportement et elle est fréquemment utilisée dans de nombreuses applications est le paramètre de contrôle

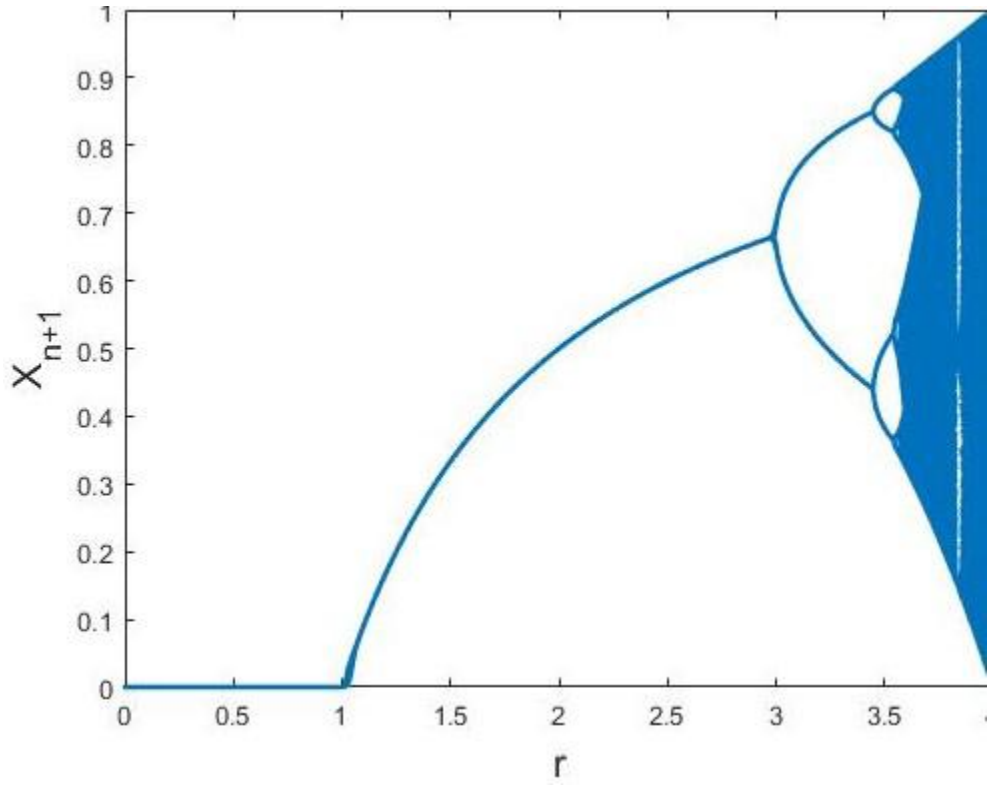


Figure 4.4. Diagramme de bifurcation de la suite logistic map.

- **Les suites chaotiques linéaires par morceaux (PLCM)**

La Suite chaotique du système PLCM a gagné récemment une attention particulière de plusieurs chercheurs en théorie du chaos en raison de sa simplicité dans la représentation, son efficacité en implémentation, et son bon comportement dynamique. La suite chaotique PLCM peut être décrite dans l'équation par :

$$z_{n+1} = F(z_n, \lambda) = \begin{cases} \frac{z_n}{\lambda}, & 0 \le z_n < \lambda \\ \frac{(z_n - \lambda)}{0.5 - \lambda}, & \lambda \le z_n < 0.5 \\ F(1 - z_n, \lambda), & 0.5 \le z_n < 1 \end{cases} \quad (1.5)$$

où $z_k \in [0,1]$ avec $n \in \mathbb{N}$ et z_0 comme condition initiale. $\lambda \in [0,0.5]$ est considéré comme étant le paramètre de contrôle. Le système PLCM a une distribution uniforme invariante, une bonne ergodicité et une bonne confusion, de sorte qu'il peut fournir une excellente séquence aléatoire, qui convient aux systèmes cryptographiques. La distribution de z avec différents du système PLCM est représentée sur la **figure 1.5**, où les valeurs de z sont uniformément réparties [2].

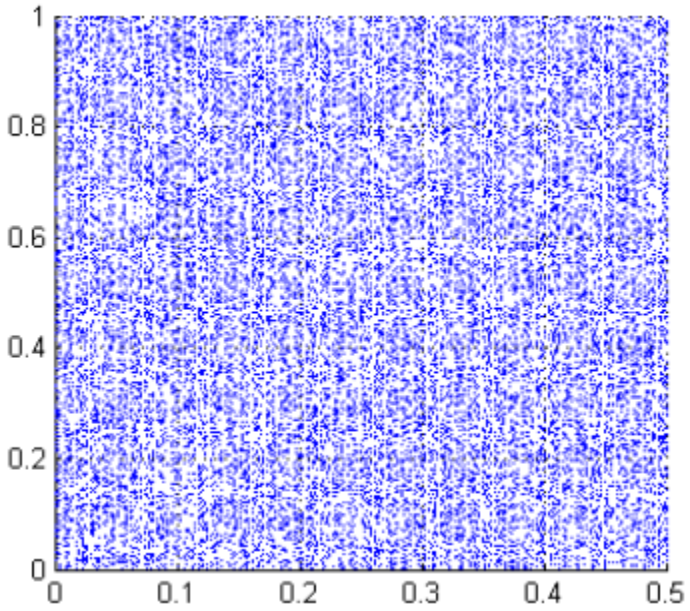


Figure 5.5. Diagramme de bifurcation de la suite PLCM.

- **Suites chaotiques linéaires par morceaux (Tent Map)**

Il existe plusieurs récurrences chaotiques linéaires par morceaux, nous citons la « *Tent Map* »

$$x_{n+1} = T(x_n, r) = \begin{cases} r\frac{x_n}{2}, & x_n < 0.5 \\ r\frac{1 - x_n}{2}, & x_n \ge 0.5 \end{cases} \quad (1.6)$$

Son nom est du au fait que le graphe de a la forme d'une tente pour les valeurs du paramètre **r** compris entre 0 et 1.

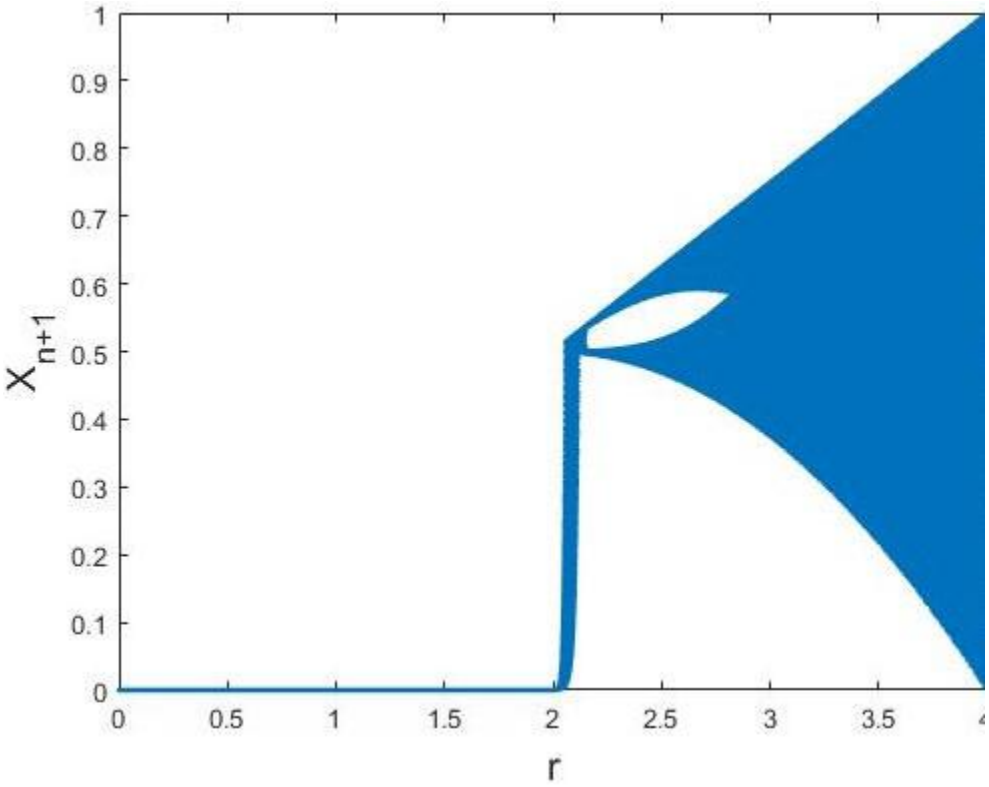


Figure 6.6. Diagramme de bifurcation de la suite tent map

- **La récurrence de Hénon**

Elle constitue un système dynamique à temps discret introduit par l'astronome Michel Hénon en 1976. Il est présenté par l'équation suivante :

$$x_{n+1} = y_n + 1 - a{x_n}^2 \quad (1.7)$$

$$y_{n+1} = bx_n \quad (1.8)$$

Tel que $(\mathrm{x_n}, \mathrm{y_n}) \in \mathbb{R}^2$

- **sine map**

Il est présenté par l'équation suivante :

$$x_{n+1} = F_s(r, x_n) = r \times \sin(\pi \times x_n) \quad (1.9)$$

La suite sine map est vraiment chaotique si $r \in [0,1]$

Nous observons à partir de la figure 1.7 que la suite sine map a une propriété similaire à la suite logistic map.

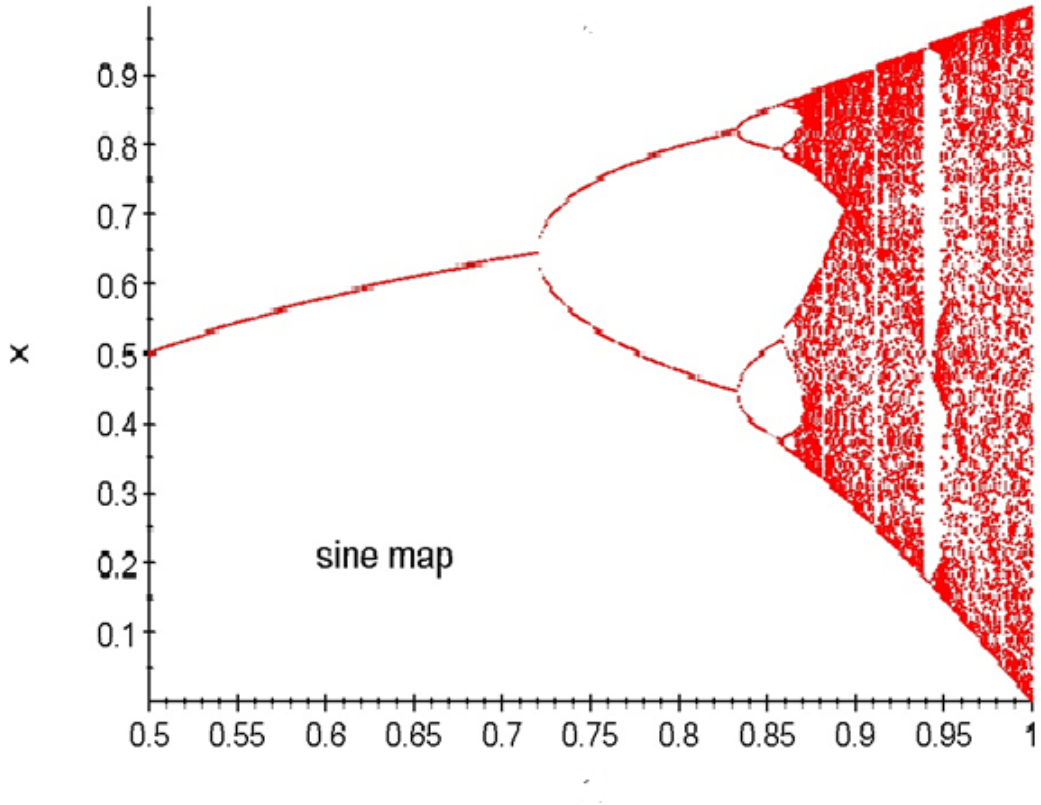


Figure7.7.Diagramme de bifurcation de la suite sine map

- **Chebyshev map**

Cette fonction chaotique 1D non linéaire est donnée par l'équation suivante :

$$x_{n+1} = F_c(a, x_n) = cos(a \times arccos x_n) \quad (1.9)$$

1 .5 Conclusion

Dans le présent chapitre, quelques rappels sur la théorie du chaos et les suites chaotiques ont été effectués. Nous allons montrer leur utilisation à des fins de chiffrement de données. Les suites chaotiques comme logistic map , sine map et tent map sont utilisées dans de cryptage d'image parce qu'elles ont une grande sensibilité à leurs valeurs initiales et paramètres de contrôle. logistic, sine et tent maps ont quelques inconvénients. Ces suites pour certaines valeurs de r ont chaotique comportement. De plus, ces suites ont une distribution non uniforme sur la sortie. Donc nombreuses méthodes ont été proposées pour résoudre ces problèmes et nous allons voir l'exemple dans le prochain chapitre qui introduit la notion de la cryptographie et présente des différents développements requis dans la construction de nouvelles suites chaotiques basés sur des systèmes dynamiques chaotiques et leur application dans le cryptage d'images.

Chapitre 2

Chapitre 2 : Les développements requis dans la construction de nouvelles suites chaotiques et leur application en cryptage d'image numérique

2.1 Introduction

Le cryptage d'image basé sur le chaos est devenu l'un des plus efficaces. Et d'excellentes méthodes de cryptage. C'est parce que les systèmes est chaotique et les cartes ont une sensibilité élevée à leurs valeurs initiales paramètres de contrôle, propriété chaotique, non-convergence et Ergodicité des états. Les cartes logistiques, sinus et tente ont quelques inconvénients. Ces cartes pour certaines valeurs de r ont chaotique comportement. De plus, ces cartes ont une distribution non uniforme sur la sortie. De nombreuses méthodes ont été proposées pour résoudre ces problèmes, en utilisant différentes fonctions comme sin; cos; . . ., les développeurs combinent la logistic map sine map et tent map puis en utilisant cette combinaison pour trouver des différents systèmes chaotiques.

Dans ce chapitre, nous allons parler sur le cryptage d'image les notions de base de la cryptographie et les systèmes de combinaison chaotique ou les développements basés sur les suites chaotiques.

2.1 Les concepts fondamentaux de la cryptographie:

2.1.1- Historiques: Ceux-ci sont les périodes les plus importantes :

• Age artisanal: (→ 1900)

• César : chaque lettre est remplacée par celle située trois positions plus loin dans l'alphabet

• Systèmes de substitutions et de permutations basiques

• Age technique: (1900 → 1970)

• Substitutions et permutations utilisant des machines mécaniques ou électro-mécaniques: Hagelin, Enigma (2ème guerre mondiale) –

• Age paradoxal (depuis 30 ans): Nouveaux mécanismes répondant à des questions à priori hors d'atteinte

• Comment assurer un service de confidentialité sans avoir établi une convention secrète commune sur un canal qui peut être écouté par un attaquant ?

• Comment assurer un service d'authenticité – basé sur la possession d'un secret – sans révéler la moindre information sur le secret ?.

2.2.2- Définition de la cryptologie:

La cryptologie, dérivée de « la science du secret », ne peut être vraiment considérée comme une science que depuis peu de temps. Cette science englobe la cryptographie (qui signifie l'écriture secrète) et la cryptanalyse (l'analyse de cette dernière).

Cryptologie = Cryptographie + Cryptanalyse

2.2.3- Définition de la cryptographie:

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Le verbe crypter est parfois utilisé mais on lui préfèrera le verbe chiffrer. Le fait de coder un message de telle façon à le rendre secret s'appelle chiffrement. La méthode inverse, consistant à retrouver le message original, est appelée déchiffrement.

2.2.4- Vocabulaire de base :

Chiffrement : transformation à l'aide d'une clé de chiffrement d'un message intelligible appelé texte clair ou libellé en un message incompréhensible ou inintelligible appelé texte chiffré ou cryptogramme si on ne dispose pas d'une clé de déchiffrement (en anglais encryption) ; En cryptographie, le chiffrement, parfois appelé à tort cryptage.

Déchiffrement: c'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair.

Chiffre : utilisation de la substitution au niveau des lettres ; anciennement code secret, par extension l'algorithme utilisé pour le chiffrement ;

Code : utilisation de la substitution au niveau des mots ou phrases pour coder ;

Coder : utilisation d'un code sur un texte ;

Cryptogramme : message chiffré ; Le destinataire légitime doit pouvoir déchiffrer le cryptogramme et obtenir le texte clair.

Crypto système : un ensemble composé d'algorithmes cryptographiques et de tous les textes en clairs, textes chiffrés et clés possibles.

Décrypter : retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement (terme que ne possèdent pas les anglophones, qui eux « cassent » des codes secrets), ceci est effectué par un espion (cryptanaliseur, décrypteur ou oreille indiscrète).

Cryptographie : étymologiquement « écriture secrète », devenue par extension l'étude de cet art (donc aujourd'hui la science visant à créer des cryptogrammes, c'est-à-dire à chiffrer).

Cryptanalyse : science analysant les cryptogrammes en vue de les décrypter.

Cryptologie : c'est une science mathématique qui comporte deux branches la cryptographie et la cryptanalyse. Le fait de coder un message de telle façon à le rendre secret s'appelle chiffrement. La méthode inverse, consistant à retrouver le message original, est appelée déchiffrement.

Clé : Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement. Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux opérations [1].

2.2.5- L'usage de la cryptographie:

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité [3].

La confidentialité : consiste à rendre l'information l'intelligible à d'autres personnes que les acteurs de la transaction c.-à-d c'est un concept permettant de garantir que seul le destinataire ou le détenant de la clé puisse découvrir le message en clair.

L'intégrité :

vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication.

L'authentification :

consiste à assurer l'identité d'un utilisateur, c.-à-d. de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

La non répudiation

La non-répudiation signifie la possibilité de vérifier que l'envoyeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues.

2. 2.6- Les clés en cryptographie:

Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement.

Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux opérations [2].

A- Les clés symétriques (ou clé secrète)

Il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète.

On peut citer l'algorithme Data Encryption System (DES) et L'International Data Encryption Algorithm (IDEA).

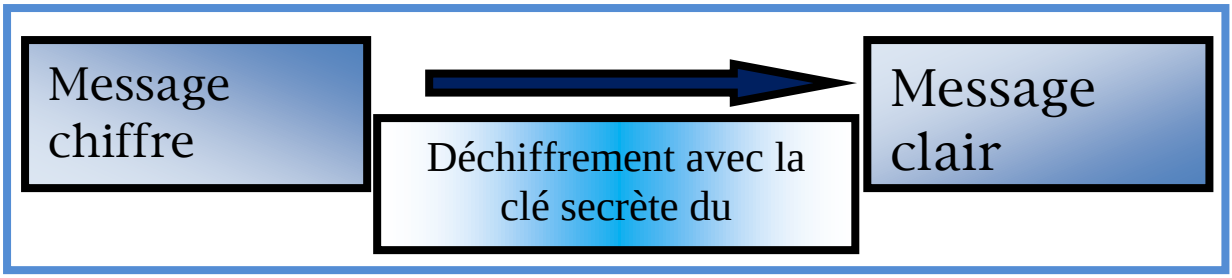


Figure 2.1: Principe de cryptage symétrique.

B- Les clés asymétriques (ou clé publique)

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

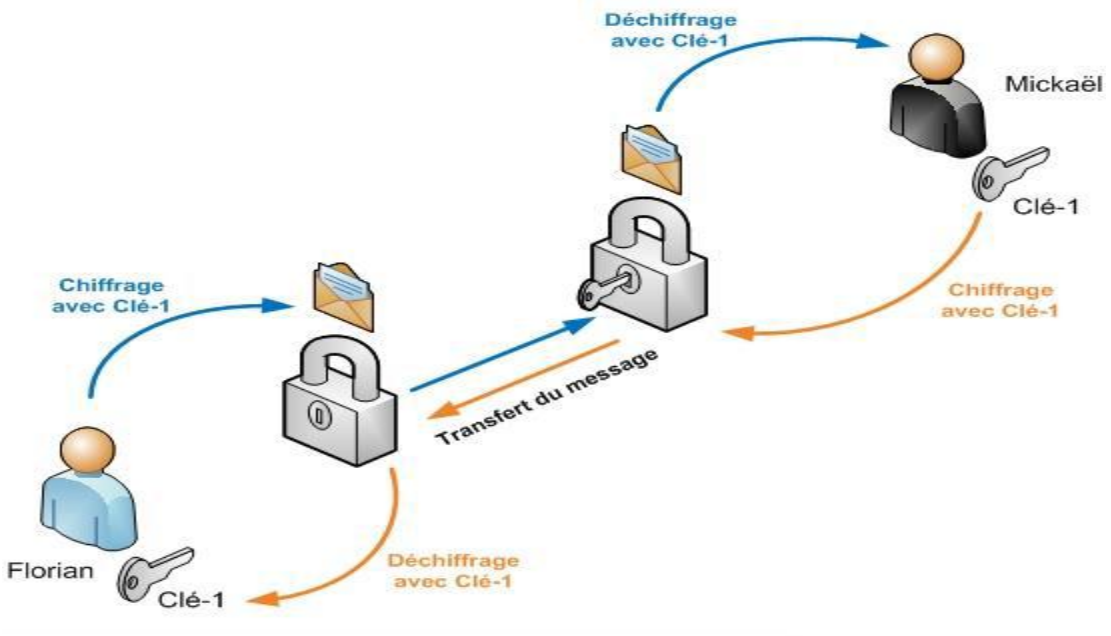


Figure 2.2: Principe de cryptage asymétrique.

On peut citer le RSA (**R**ivest, **S**hamir, **A**delman, les 3 inventeurs) comme le plus connu de ces algorithmes.

Type de cryptosystème	Avantages	Inconvénients
Clé secrète	-Rapide -Peut être facilement réalisée sur une puce	- Difficulté de distribuer les clés -Ne permet pas de signature électronique
Clé publique	- Utilise deux clés différentes - Fournit des garanties d'intégrité et de non répudiation par signature électronique	-Lent et demandant beaucoup de calculs

Tableau 2.1: Avantages et inconvénients 2 méthodes de cryptographie.

2. 2.7.Les différents types de cryptographie

On peut regrouper les systèmes de chiffrement en deux catégories:

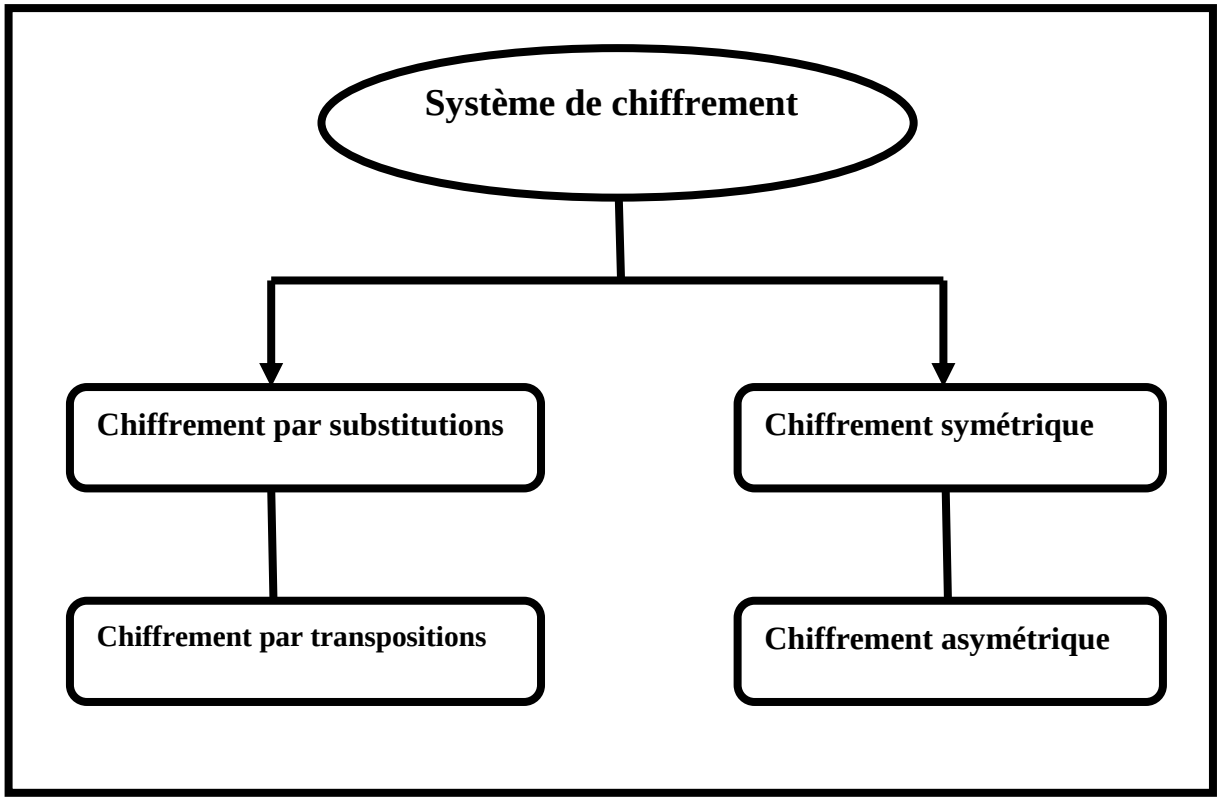


Figure 2.3: principe de systèmes de chiffrement.

2. 2.7.1La cryptographie classique

Dans le schéma ci-dessous figurent les différentes branches de la cryptographie classique.

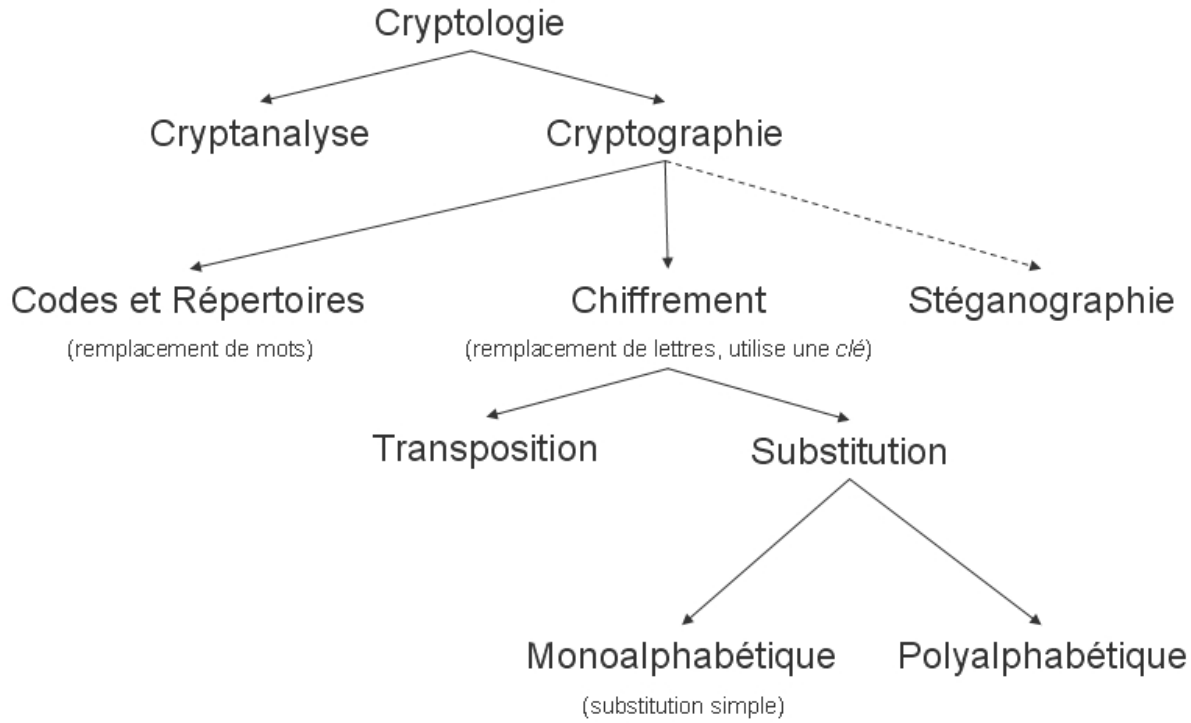


Figure 2.4: Domaines inclus dans la cryptologie.

A- Chiffrement par substitution

Le chiffrement par substitution consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou plusieurs autres entités [4].

On distingue généralement plusieurs types de cryptosystèmes par substitution :

- Substitution mono-alphabétique

Consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet.

Exemple : Le chiffre de César On décale les lettres de 3 positions.

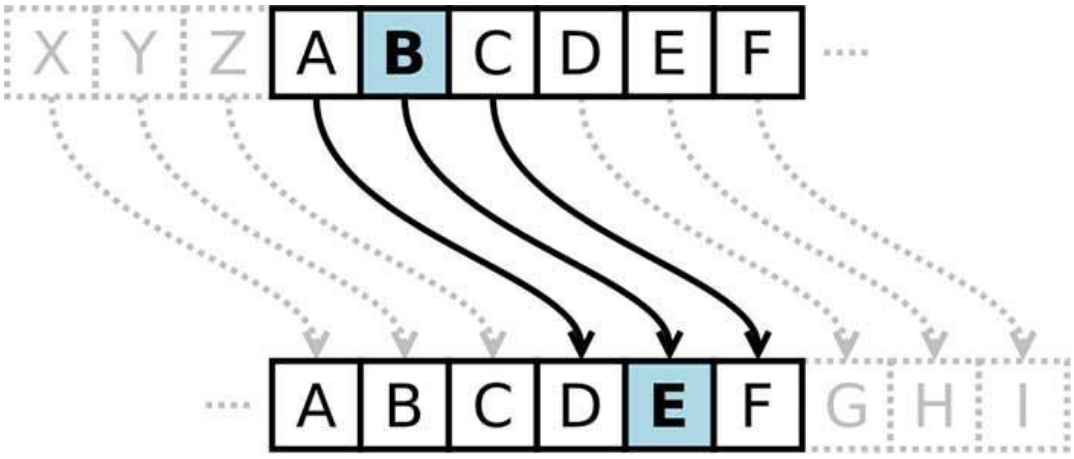


Figure 2.5:exemple du chiffre de césar.

- Substitutions polyalphabétiques

Consiste à utiliser une suite de chiffres monoalphabétique réutilisée périodiquement.

Exemple : le chiffre de Vigenere Cela signifie qu'il permet de remplacer une lettre par une autre qui n'est pas toujours la même.

Lettre claire	L	E	A	I	R	E	S	S	O	N	T
Clef	E	T	P	E	T	P	E	T	P	E	T
Décalage	5	20	16	5	20	16	5	20	16	5	20
Lettre chiffrée	X	P	M	K	T	W	L	D	R	M	R

Figure 2.6:exemple du chiffre de Vigenere.

-La substitution homophonique

Permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères.

-La substitution de polygrammes

Elle consiste à substituer un groupe de caractères (polygramme) dans le message par un autre groupe de caractères.

B-Chiffrement par Transpositions

Les méthodes de chiffrement par transposition consistent à réarranger les données à chiffrer de façon à les rendre incompréhensibles. Il s'agit par exemple de réordonner géométriquement les données pour les rendre visuellement inexploitables [5].

Exemple: Le plus souvent on utilise deux visions géométriquement différentes du texte.

-On enroule une bande de papyrus sur un cylindre appelé **scytale** ;

Figure 2.7: Scytale.

- Ecrire le texte longitudinalement sur la bandelette ainsi enroulée.
- Pour décrypter le message il faut un cylindre du bon diamètre.

2.2.7.2- La cryptographie Moderne

La cryptographie moderne est distinguée en deux types et se situe entre les chiffrements de type symétrique et ceux de type asymétrique [6].

A- Cryptographie symétrique (à clefs privés)

La cryptographie à clefs privées est aussi appelée cryptographie symétrique. Les principaux types de cryptographie symétrique à clefs privés utilisés aujourd'hui se répartissent en deux grandes catégories de chiffrements modernes : Chiffre par bloc et chiffre de flux. Le chiffrement symétrique (aussi appelé chiffrement à clé privée ou à clé secrète) consiste à utiliser la même clé pour le chiffrement et le déchiffrement. Le chiffrement consiste alors à effectuer une opération entre la clé privée et les données à chiffrer afin de rendre ces dernières inintelligibles. Le déchiffrement consiste à réaliser l'opération inverse c'est-à-dire récupérer le message d'origine à partir du message chiffré en utilisant la clé secrète.

- Chiffrement par blocs:

C'est une des deux grandes catégories de chiffrements modernes en cryptographie symétrique. Il consiste à un découpage des données en blocs de taille généralement fixe (souvent une puissance de deux comprise entre 32 et 512 bits). Les blocs sont ensuite chiffrés les uns après les autres. Il est possible de transformer un chiffrement de bloc en un chiffrement par flot en utilisant un mode d'opération comme ECB (Electronic Code Book) (chaque bloc chiffré indépendammentdes autres) ou CFB (Cipher Feedback)(on chaîne le chiffrement en effectuant un XOR entre les résultats successifs).

- Chiffrement par flux:

Dans un crypto-système par flots, le cryptage des messages se fait caractère par caractère ou bit à bit, au moyen de substitutions de type César générées aléatoirement: la taille de la clef est donc égale à la taille du message.

B- Cryptographie asymétrique (à clefs publiques)

La cryptographie asymétrique se base sur des problèmes mathématiques complexes (factorisation de grands nombres entiers ou équation de logarithme discrète). La cryptographie asymétrique se base sur le principe de deux clés: clé publique, clé privée. La clé publique est mise à la disposition de quiconque désirant chiffrer un message (cette clé peut être connue par tout le monde). Ce dernier ne pourra être déchiffré qu'avec la clé privée, qui doit être confidentielle et connue seulement par son propriétaire.

2.3- La cryptographie visuelle:

La cryptographie visuelle est un domaine de la cryptographie dans lequel on utilise ou l'on transmet une image, dont le but est de pouvoir crypter une image en images cryptées n'ayant chacune aucune ressemblance ou corrélation avec l'originale.

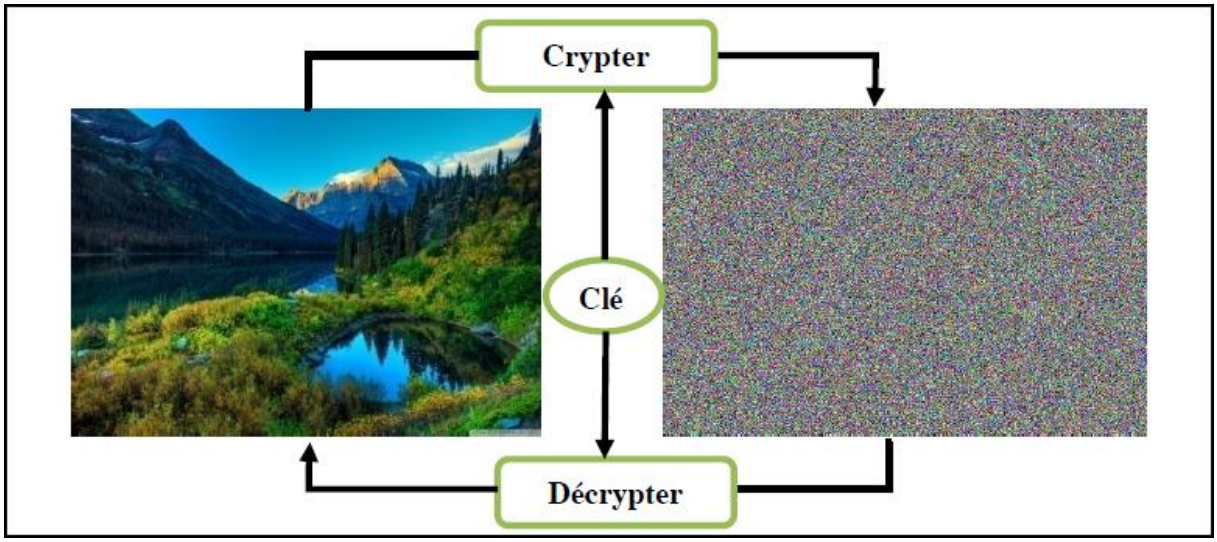


Figure 2.8: Cryptage d'image.

2.3.1 Définition d'image numérique

L'image numérique est la transformation d'un signal continu en signal discret. On définit aussi une image numérique comme étant une suite de valeurs restituées en une grille bidimensionnelle ou chaque élément est appelé pixel [9].

L'image numérique est caractérisée par les paramètres suivants:

- Pixels

Le pixel représente ainsi le plus petit élément constitutif d'une image numérique l'ensemble de ces pixels est contenu dans un tableau à de dimension constituant l'image finalement obtenu [12].

-Définition (dimension de l'image) :

On appelle définition le nombre de points (pixels) constituant une image: c'est le nombre de colonnes de l'image que multiplie son nombre de lignes.

-Poids d'une image:

Le poids se mesure en octets (et ses multiples : ko, Mo, Go). Un octet est une unité de mesure informatique. Pour simplifier, il vous indique la place que va prendre une image sur un ordinateur.

L'image aura un poids différent en fonction du format (.jpeg, .png, .bmp…), de sa définition, du nombre de couches et de niveaux de couleur possibles, de la méthode de compression, du taux de compression et aussi du sujet de l'image (une image très colorée et avec beaucoup de détails sera plus lourde qu'une image avec très peu de nuances et dans les mêmes teintes) [7].

2.3.2 Types d'image numérique

Il existe deux types d'images numériques, le premier est basé sur les pixels et l'autre sur des formules mathématiques:

2.3.2.1 Les images matricielles

Une image matricielle (ou bitmap) est une image constituée d'un ensemble de points : les pixels. Chaque point porte des informations de position et de couleur.

Format d'images bitmap : BMP, PCX, GIF, JPEG, TIFF. Les photos numériques et les images scannées sont de ce type.

2.3.2.2 Les images vectorielles

Les images vectorielles sont composées de formes géométriques qui vont pouvoir être décrites d'un point de vue mathématique. Par exemple, une droite sera définie par 2 points, un cercle par un centre et un rayon. Le processeur est chargé de "traduire" ces formes en informations interprétables par la carte graphique (images

Word, Publisher, CorelDraw - format WMF, CGM, etc.)

Les avantages d'une image vectorielle : les fichiers qui la composent sont petits, les redimensionnements sont faciles sans perte de qualité. Les inconvénients : une image vectorielle ne permet de représenter que des formes simples. Elle n'est pas donc utilisable pour la photographie notamment pour obtenir des photos réalistes [8].

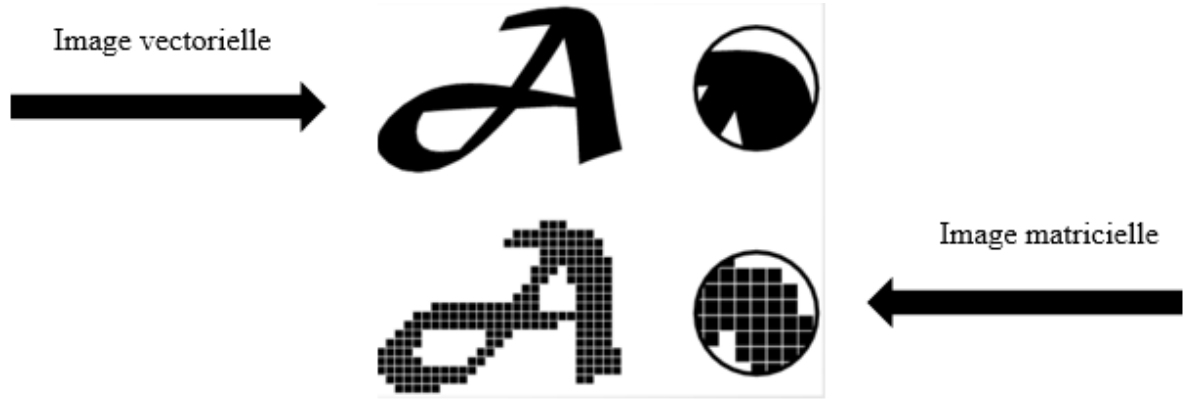


Figure 2.9 : Différence entre image vectorielle et image matricielle.

2.3.3- Cryptage d'image

Pour crypter une image, il faut avoir une fois de plus recours aux bits. Chaque pixel possède une couleur : celle-ci est définie par un nombre entier, converti par la suite en binaire. Le principe de cryptage est simple : par exemple, il s'agit d' "additionner" deux images, une image-clé et l'image qu'on veut crypter, grâce à l'opérateur bit à bit XOR [10].

Exemple :

(1) 1er pixel de l'image à crypter	**01110011**
(2)1er pixel de l'image clé	10100101
(1) XOR (2) -->1er pixel de l'image cryptée	11010110

avec/sans perte. D'autre part, les algorithmes de chiffrement des images peuvent être classés selon le domaine d'application : les méthodes du domaine spatial ou bien celle du domaine fréquentiel.

2.3.3.1- Méthodes dans le domaine spatial

Dans le domaine spatial, on applique le schéma de cryptage sur le plan d'image lui-même, et les approches de cette catégorie sont basées sur une manipulation directe des pixels d'une image. Dans ces algorithmes, le chiffrement détruit la corrélation entre les pixels et rend les images cryptées incompressibles. Les pixels de l'image peuvent être reconstruits (récupérés) complètement par un processus inverse sans aucune perte d'information.

Les algorithmes de cryptage d'image dans le domaine spatial existants peuvent être classés en deux catégories.

- Dans la première catégorie, un pixel est considéré comme le plus petit élément, et une image numérique est considérée comme un ensemble de pixels.
- Toutefois, dans la deuxième classe, un pixel peut être en outre divisé en bits, sur lesquels des opérations au niveau de bits sont effectuées. Par exemple, un pixel dans une image en niveaux de gris est généralement constitué de 8 bits.

2.3.3.2- Méthode dans le domaine fréquentiel

Les schémas de cryptage dans le domaine fréquentiel sont basés sur la modification de la fréquence de l'image en utilisant une transformation, ainsi, la reconstruction des pixels de l'image originale dans le processus de décryptage cause généralement une perte d'information [11].

2.4. Les outils élémentaires d'analyse d'un algorithme de cryptage d'image

2.4. 1. Espace de clés

La taille de l'espace de clé est nécessaire pour assurer la sécurité contre l'attaque par force brute. Par exemple, si la taille de clé est 512 bit, alors l'espace de clé fournit c'est 2^{512} ($\cong 10^{154}$ Clé combinaisons possibles). Ainsi, si un ordinateur fait 10^{10} calculs par seconde, il faudra environ de 10^{136} d'ans pour trouver la clé.

2.4..2. L'histogramme

L'histogramme est une représentation graphique qui permet de connaître la répartition des intensités lumineuses des pixels

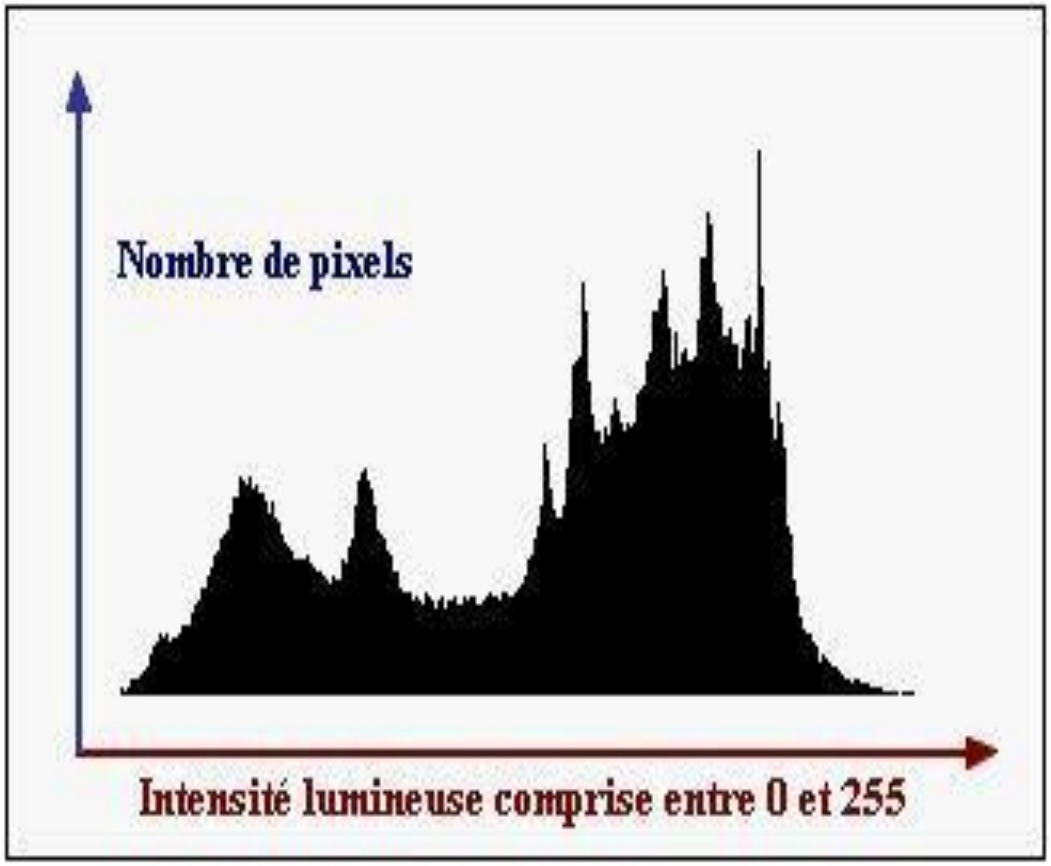


Figure 2.10 : **Histogramme d'une image niveau de gris**

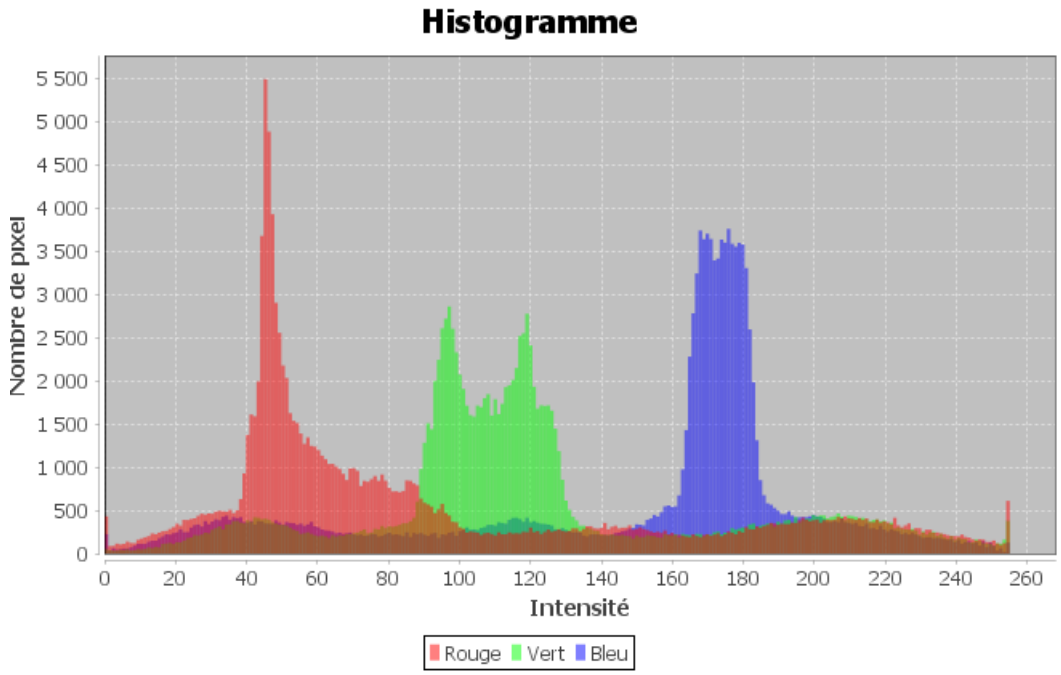


Figure 2.11 : Histogramme d'une image couleur

Dans un contexte de chiffrement d'image, l'histogramme de l'image chiffrée doit être uniforme pour assurer la sécurité contre l'attaque de texte en clair connue, autrement dit l'attaquant ne peut pas extraire information à partir de cet histogramme. Par exemple, La Figure 2.12 est l'histogramme de l'image originale et la Figure 2.13 est l'histogramme de l'image cryptée. La Figure 2.12 montre que l'histogramme plus uniforme qui est hautement souhaitable.

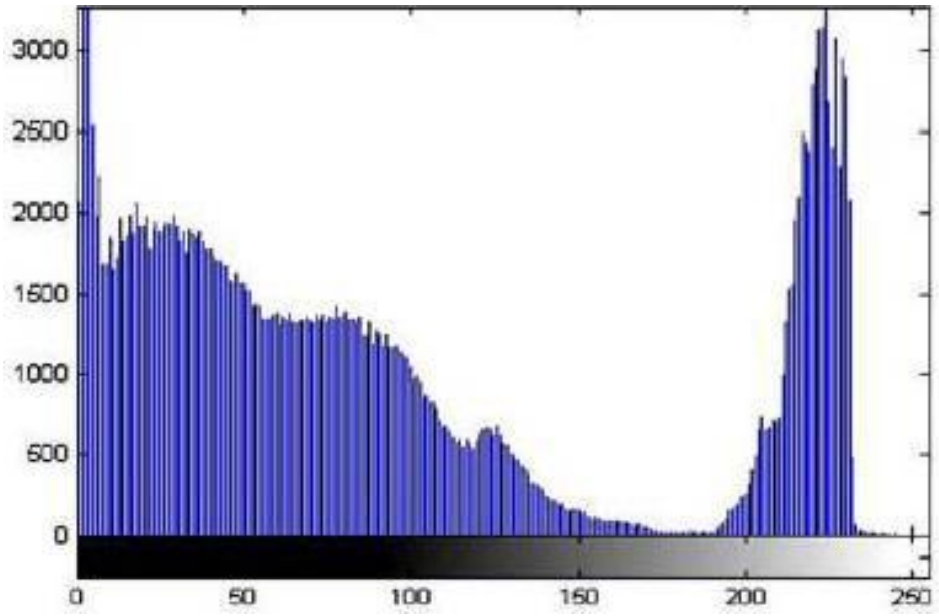


Figure 2.12 : Histogramme d'une image originale.

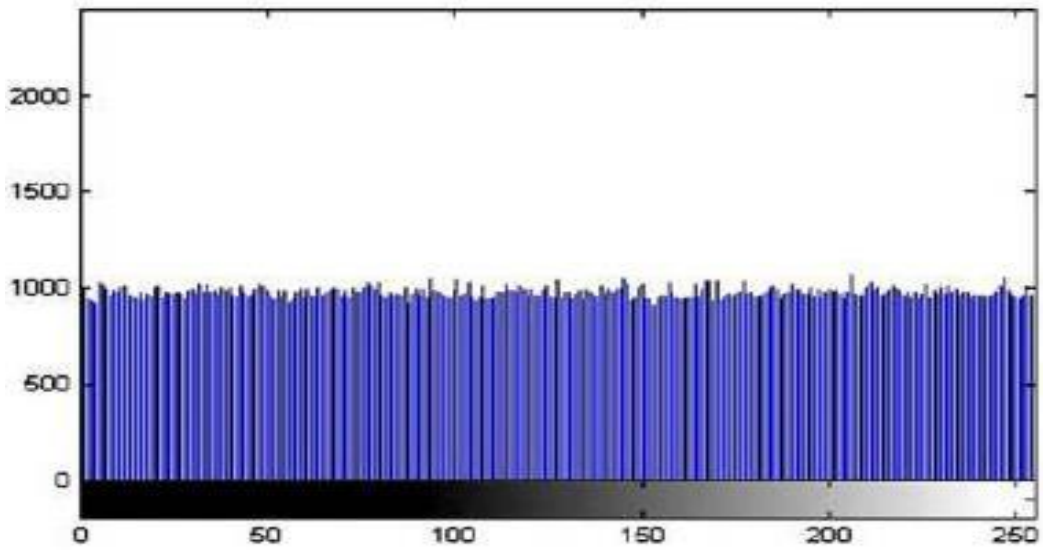


Figure 2.13 : Histogramme d'une image cryptée.

2.4..3. La corrélation entre les pixels adjacents

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.

$$r = \frac{\mathrm{cov(x;y)}}{\sqrt{\mathrm{D(x)}}\ \sqrt{\mathrm{D(y)}}} \qquad (2.1)$$

Ou :

$$\mathrm{cov(x,y)} = \frac{1}{\mathrm{N}} \sum_{i=1}^{N} (x_i - \mathrm{E(x)})(\mathrm{y_i} - \mathrm{E(y)}) \qquad (2.2)$$

$$\mathrm{E(x)} = \frac{1}{\mathrm{N}} \sum_{i=1}^{N} x_i D(x) = \sum_{i=1}^{N} (x_i - \mathrm{E(x)})^2 \qquad (2.3)$$

Si corrélation ≈ 1, cela signifie que l'Image-clair et de Image-Chiffrée sont très dépendantes.

Si corrélation ≈ 0 – +

, cela signifie que l'Image-Chiffrée et l'Image-clair ne sont pas corrélés.

Ainsi, plus faible est la valeur de corrélation, la qualité de cryptage est meilleure.

2.4..4. L'entropie

L'entropie de Shannon, est une fonction mathématique qui permit de mesures de l'aléatoire de l'information. Pour tout message codé sur *M* bits, la limite supérieure de l'entropie est *M*.

La formule :

$$H(\mathrm{M}) = -\sum_{i=1}^{n} p_i \mathrm{x} \log_2 p_i \quad (2.4)$$

Où p_i définit la probabilité d'un pixel et N est le nombre de bits dans chaque pixel.

Donc pour un chiffrement d'images au niveau de gris, La valeur de l'entropie doit être très proche de 8, Parce que si l'entropie est inférieure à 8, il existe des degrés de prévisibilité, donc on ne peut pas assurer la sécurité contre l'analyse statistique. De sorte que l'entropie devrait idéalement être 8[14].

2.5. Les système de combinaison chaotique

2.5. 1 Le système de combinaison R. Parvaz , M. Zarebnia

Dans cette section, nous décrivons la combinaison de systèmes chaotiques. Logistic map, sine map et tent map sont définies comme suit[13]

$$x_{n+1} = L(r, x_n) = r \times x_n(1 - x_n) \quad (2.5)$$

$$x_{n+1} = S(r, x_n) = r \times \sin(\pi \times x_n)/4 \quad (2.6)$$

$$\mathrm{x_{n+1}} = \mathrm{T}(x_n, r) = \begin{cases} r \times \frac{x_n}{2}, & x_n < 0.5 \\ r \times \frac{1-x_n}{2}, & x_n \geq 0.5 \end{cases} \quad (2.7)$$

Où le paramètre $r \in [0,4]$ On sait que le système logistique (Sinus ou Système de tent) pour certaines valeurs de $r \in [2,4]$ qu'elles sont chaotique.

Figure 2.15 (a) et 4 (a) montrent que le système logistique pour $r = 2$ n'a pas été chaotique]. L'histogramme du système de tente logistique est illustré à la **Figure. 2.16**(a). Gamme chaotique n'est pas limitée au système de tente logistique, mais à partir de la **Figure. 2.16**(a), nous pouvons voir que l'histogramme du système de tente logistique n'est pas assez plat. Non uniforme la distribution par rapport à la série de production conduit à une faiblesse attaque statistique. Pour résoudre ce problème, nous ajoutons des poids et des fonctions dans le système de tente logistique ou le système de tente sinus comme suit (voir **Figure. 2.14**)

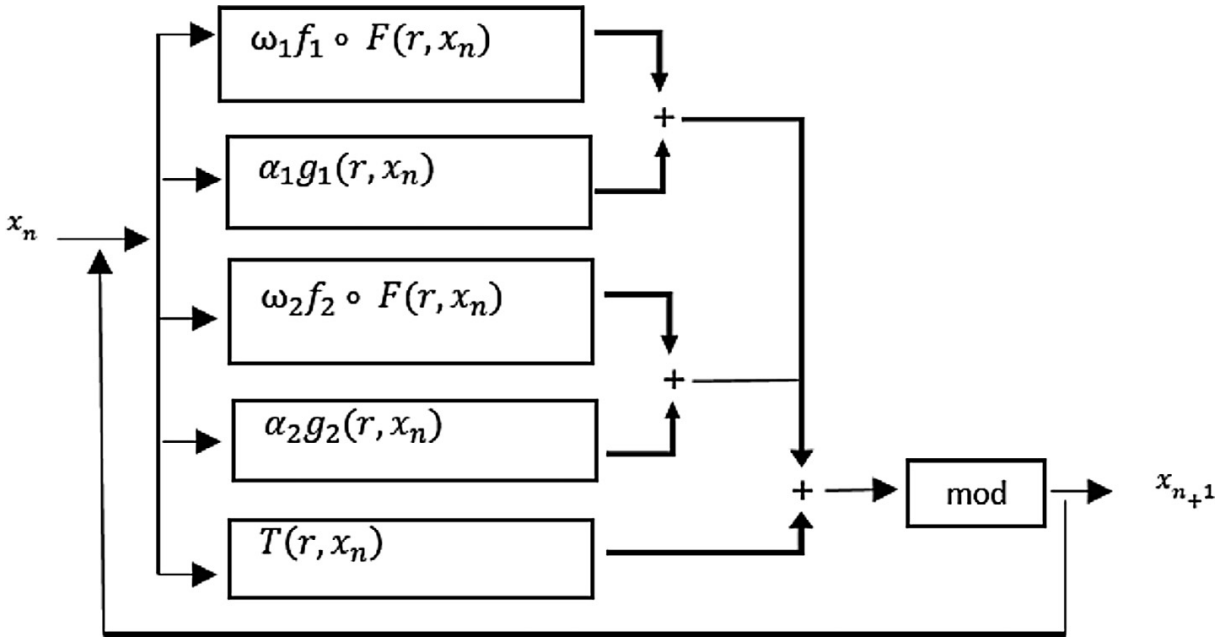


Figure. 2.14 La combination de système chaotique.

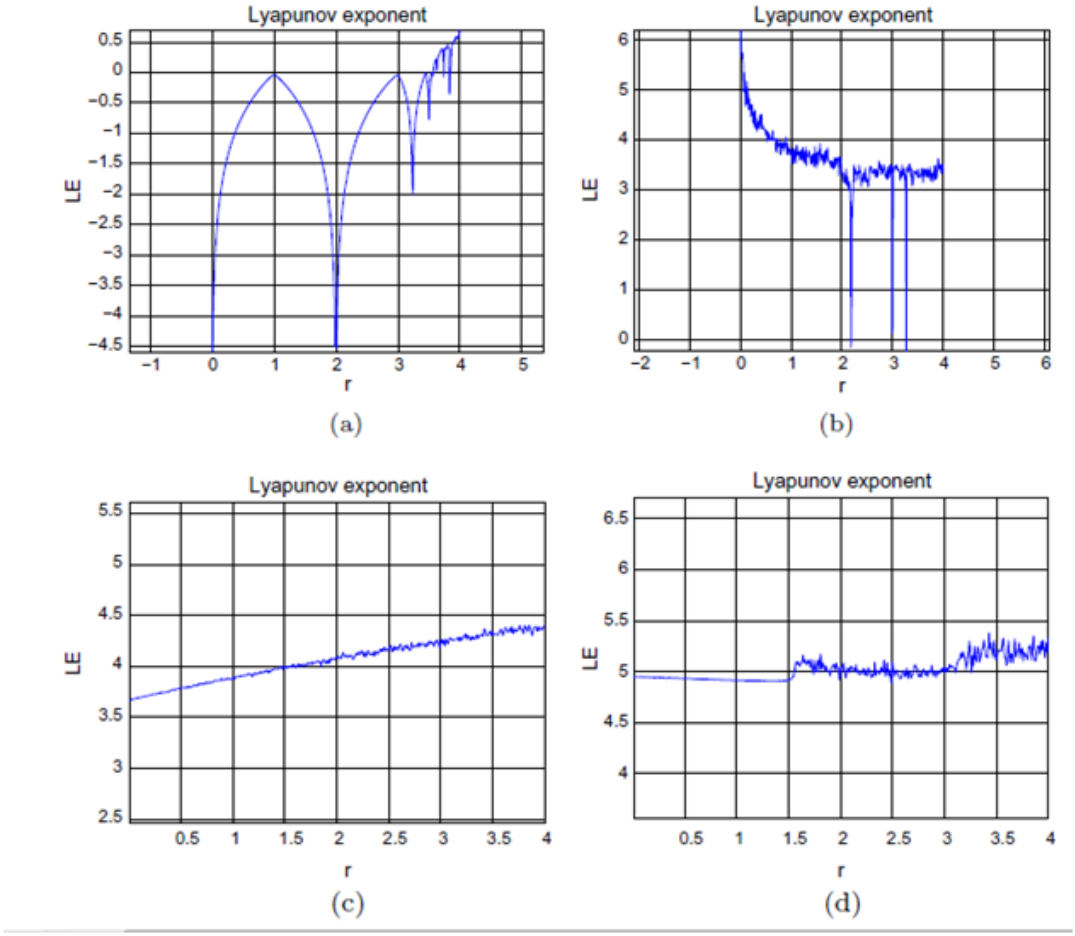


Figure 2.15 Diagramme de Lyapunov (a) Logistic map, (b) Cas (i), (c) Cas (ii), (d) Cas (iii).

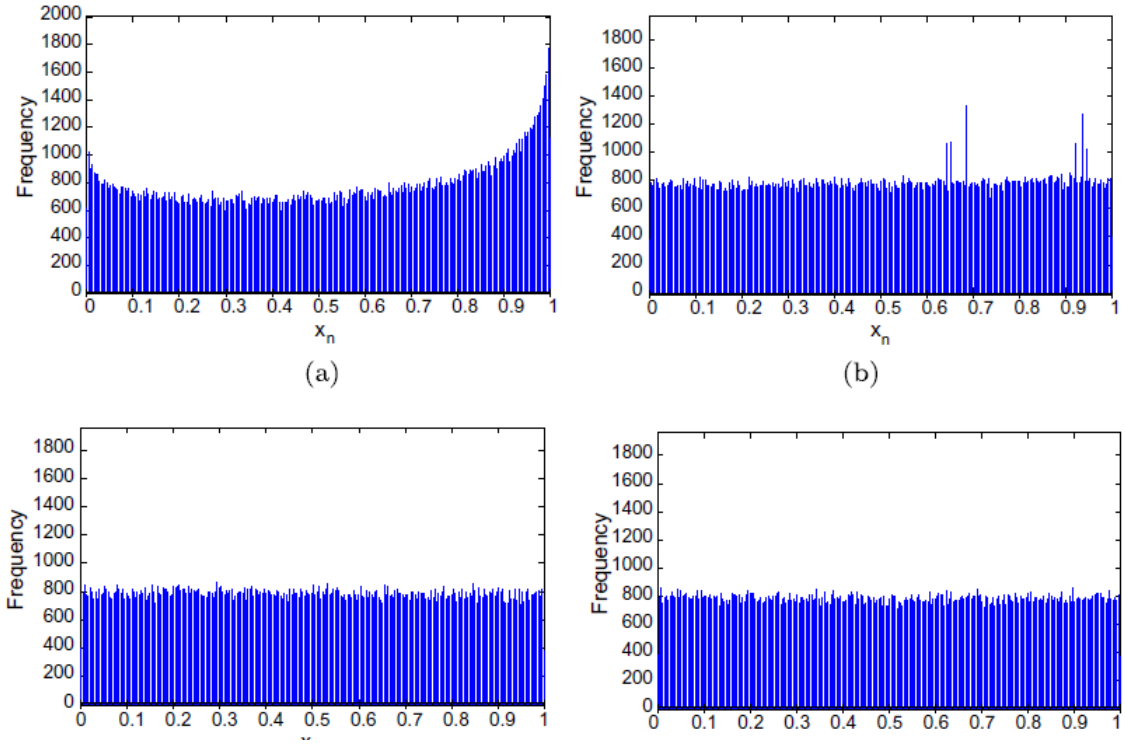


Figure. 2.16 Histogramme (a) Logistic map, (b) Cas (i), (c) Cas (ii), (d) Cas (iii).

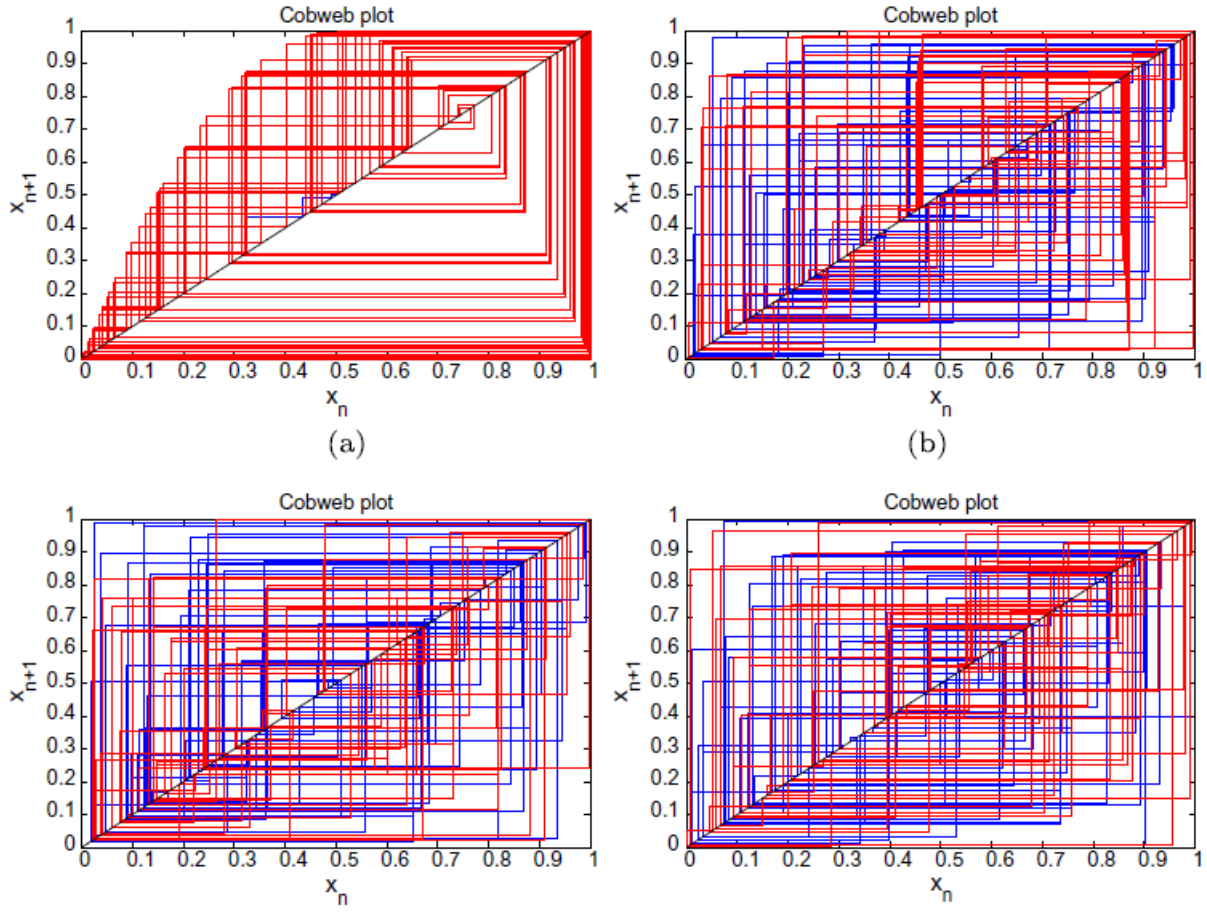


Figure. 2.17 Cobweb (a) Logistic map, (b) Cas (i), (c) Cas (ii), (d) Cas (iii).

$$\mathrm{x_{n+1}} = \mathrm{G}(x_n) = \begin{cases} \omega_1 f_1 F(r, x_n) + \alpha_1\, g_1(r \times x_n) + \xi_1 \times \frac{(c-r)x_n}{2} mod 1, \\ x_n < 0.5 \\ \omega_2 f_2 F(r, x_n) + \alpha_2\, g_2(r \times x_n) + \xi_2 \times \frac{(\beta_2 - r)(1-x_n)}{2} mod 1, \\ x_n \geq 0.5 \end{cases} \quad (2.8)$$

Ou $F(r, x_n)$ est logistic map ou sine map (2.) $f_i(x)$ et $g_i(x)$ $(i = 1,2)$

peut être considéré comme ax , $sin(ax), cos(ax)$, $tan(ax)$, $cot(ax)$, $exp(ax), exp(ax)$, $log(ax)$ (a est une constante) et toute autre fonction appropriée.

Également dans la formule ci-dessus $\omega_i, \alpha_i, \xi_i$ et $\beta_i (i = 1,2)$ sont des nombres réels et le paramètre $r \in [0,4]$ Dans la prochaine étape pour enquêter sur la

propriétés du nouveau système, nous considérons les cas suivants

- i : $2\omega_1 = \omega_2 = 20$, $-\alpha_1 = \alpha_2 = -2$, $2\xi_1 = \xi_2 = 4$, $\beta_1 = 4$, $\beta_2 = -20$

$f_1(x) = sin(x)$, $f_2(x) = exp(x)$, $g_1(x) = cot(x)$, $g_2(x) = cos(\pi x)$, $F(r, x_n) = L(r, x_n)$

- ii: - i : $\omega_1 = \omega_2 = 20$, $-\alpha_1 = \alpha_2 = 0$, $2\xi_1 = \xi_2 = 1$, $\beta_1 = \beta_2 = 80$

$f_1(x) = sin(x)$, $f_2(x) = exp(x)$, $F(r, x_n) = L(r, x_n)$.

- iii: $\omega_1 = \omega_2 = 1$, $\alpha_1 = \alpha_2 = 1$, $\xi_1 = 7$, $\xi_2 = 15$, $\beta_1 = 2\beta_2 = 40$ $f_1(x) = cos(x)$, $f_2(x) = tan(x)$, $g_1(x) = tan(x)$, $g_2(x) = x$, $F(r, x_n) = S(r, x_n)$

2.6 Conclusion

Dans ce chapitre, nous avons présenté des généralités sur la cryptographie et historiques. En premier lieu, nous avons commencé par donner quel est l'usage de la cryptographie et les clés en cryptographie. Puis nous avons cité les différents types de cryptage et les outils élémentaires d'analyse d'un algorithme de cryptage d'image comme l'espace de clés et l'histogramme, la corrélation entre les pixels adjacents, et le dernier c'est l'entropie.

Dans le chapitre suivant, nous allons proposer de nouvelle suite chaotique et son application dans le cryptage d'image numérique

.

Chapitre 3

Chapitre 3 : Proposition d'une suite chaotique modifiée appliquée au cryptage d'images.

3.1 Introduction

Dans ce chapitre, nous proposons une nouvelle suite chaotique unidimensionnelle basée sur la suite chaotique sinus, c'est l'idée de l'article intitulé : Digital image scrambling based on a new one-dimensional coupled Sine map, apparu au journal de Nonlinear Dyn en 2019 [1]. Le but de la conception de cette suite sinus modifiée est d'accroître la sécurité de l'espace clé par rapport aux suites chaotiques de base, telles que la suite logistique et la suite Sinus. Nous allons prouver à travers l'utilisation du diagramme de bifurcation et l'analyse des exposants de Lyapunov que cette suite est quasiment chaotique et peut être utilisée de manière sécurisée comme étant un générateur de nombres pseudo-aléatoires dans les systèmes de chiffrement d'images numériques. En outre, pour voir l'utilité et l'efficacité de la suite proposée, nous allons présenter un algorithme de cryptage d'images à base de cette suite, en le comparant aussi avec d'autres algorithmes similaires. Les résultats de la simulation de cet algorithme sont évalués en fonction de la sécurité et les critères d'analyse de performance. Ces résultats ont montré que la technique suggérée a de meilleures performances en termes de sécurité et mesures de qualités visuelles.

3.2 Définition de la suite sinus de base

La suite Sinus de base est une suite unidimensionnelle qui génère des séquences chaotiques dans l'intervalle[0 1]. Elle est définie par l'équation suivante [2,3]:

$$x_{n+1} = \mu \sin(\pi x_n) \tag{3.1}$$

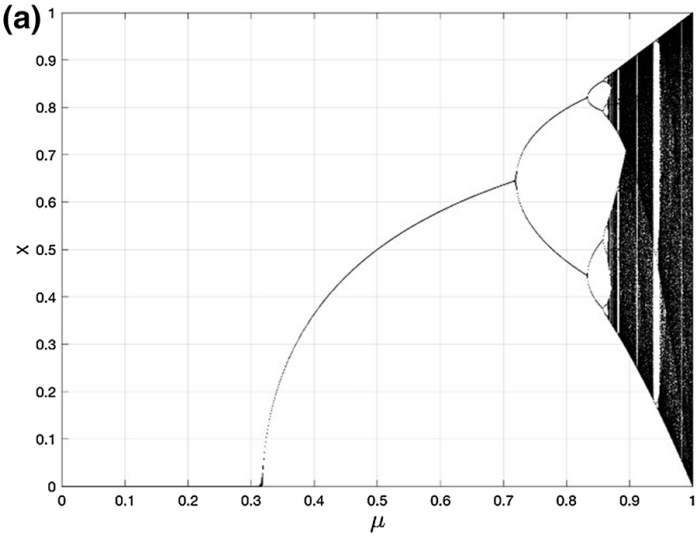
Ou μ est le paramètre de contrôle prenant ces valeurs dans l'intervalle[0 1].

3.2.1 Diagramme de bifurcation

Dans les systèmes dynamiques non linéaires, et dans certains cas, une petite variation de certains paramètres dits paramètres de contrôle, peut dans des conditions bien définies, au voisinage d'une valeur critique, provoquer un changement complet de comportement à l'équilibre du système. C'est ce qu'on appelle une bifurcation. Ce sont les scénarios de transition des systèmes dynamiques vers les états chaotiques (appelés aussi bifurcations). La bifurcation est une théorie qui s'intéresse à l'étude mathématique des changements qualitatifs (changement qualitatif des propriétés d'un système telles que la stabilité, le nombre de points

d'équilibre ou la nature des régimes permanents) ou topologiques de la structure d'un système dynamique. Un digramme de bifurcation représente la variation de l'état d'équilibre d'une variable en fonction de la valeur du paramètre de contrôle.

La figure 3.1 illustre le diagramme de bifurcation de la suite sinus de base, elle montre bien que la suite est chaotique pour $\mu \in [0.85\ 1]$.



. Figure 3.1 : Diagramme de bifurcation de la suite sinus de base.

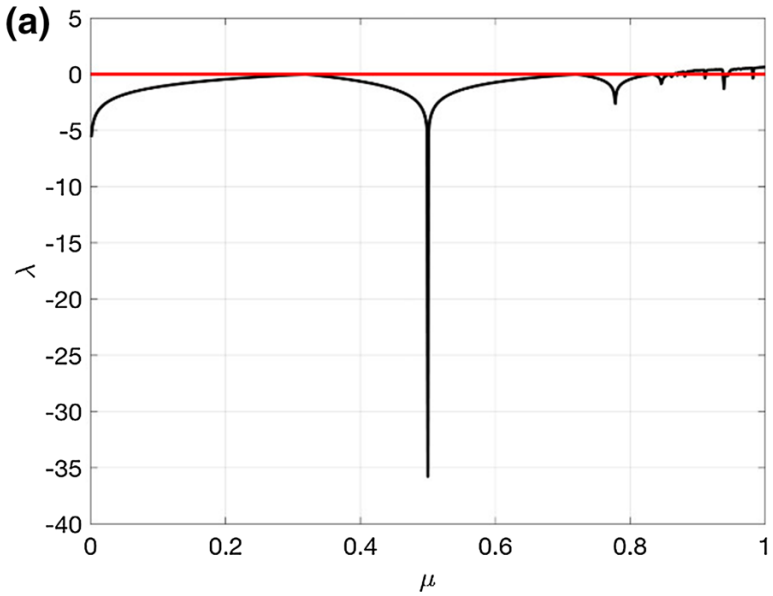


Figure 3.2 : Analyse de l'exposant de Lyapunov de la suite sinus de base.

3.2.2 L'exposant de Lyapunov

L'un des paramètres les plus importants pour le test du comportement chaotique des systèmes dynamiques est l'exposant de Lyapunov. En effet la sensibilité aux conditions

initiales de telle suite peut être étudiée à l'aide de l'exposant de Lyapunov. L'exposant de Lyapunov pour une carte unidimensionnelle peut être exprimé selon l'équation d'état :

$x_{n+1} = f(x_n, \alpha, \beta, \gamma)$, qui est définie comme suit [4–5]:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln|f'(x_i)| \tag{3.2}$$

Un exposant positif indique que le système est instable et vraiment chaotique. La figure 3.2 illustre l'analyse de l'exposant de Lyapunov de la suite sinus de base , elle confirme que la suite est chaotique pour $\mu \in [0.85\ 1]$.

3.3 Définition de la suite sine modifiée

Nous considérons les deux fonctions sinus suivantes :

$$f_1(x) = \mu \sin(\pi x) \tag{3.3}$$

$$f_2(x) = \mu \sin(\pi x(1-x)) \tag{3.4}$$

Puis les deux paramètres de contrôle β et γ sont incorporés au sein des deux équations (3.3) et (3.4) respectivement de la manière suivante :

$$f_1(x, \beta) = \mu \sin(\beta^3 \pi x) \tag{3.5}$$

$$f_2(x, \gamma) = \mu \sin(\gamma^3 \pi x(1-x)) \tag{3.6}$$

Pour utiliser la nouvelle carte Sine des fonctions f_1 et f_1, le modèle fonctionnel de la suite couplée basé sur le paramètre α est comme suit :

$$\Phi(x, \alpha, \beta, \gamma) = \alpha . f_1(x, \beta) + (1-\alpha).\big(1 - f_2(x, \gamma)\big) \tag{3.7}$$

Du moment que les générateurs de nombres pseudo-aléatoires sont souvent dans l'intervalle [0,1], pour éviter de générer des valeurs négatives, la fonction absolue est ajoutée à Eq. (3.7).

$$\Phi(x, \alpha, \beta, \gamma) = \alpha . |f_1(x, \beta)| + (1-\alpha).(1 - |f_2(x, \gamma)|) \tag{3.8}$$

Finalement, la suite chaotique sinus modifiée est donnée par l'équation suivante :

$$\boldsymbol{x_{n+1} = \alpha . \left|\sin(\beta^3 \pi x_n)\right| + (1-\alpha).\left(1 - \left|\sin(\pi \gamma^3 x_n (1-x_n))\right|\right)} \tag{3.9}$$

où $x_0 \in [0,\ 1]$ est la condition initiale, $\alpha \in [0, 1]$ et $\beta,\ \gamma \in [8,\ 10]$ sont des paramètres de contrôle.

La figure 3.3 et la figure 3.4 illustrent le diagramme de bifurcation et l'analyse de l'exposant de Lyapunov de la suite sinus modifiée et la suite sinus de base conjointement.

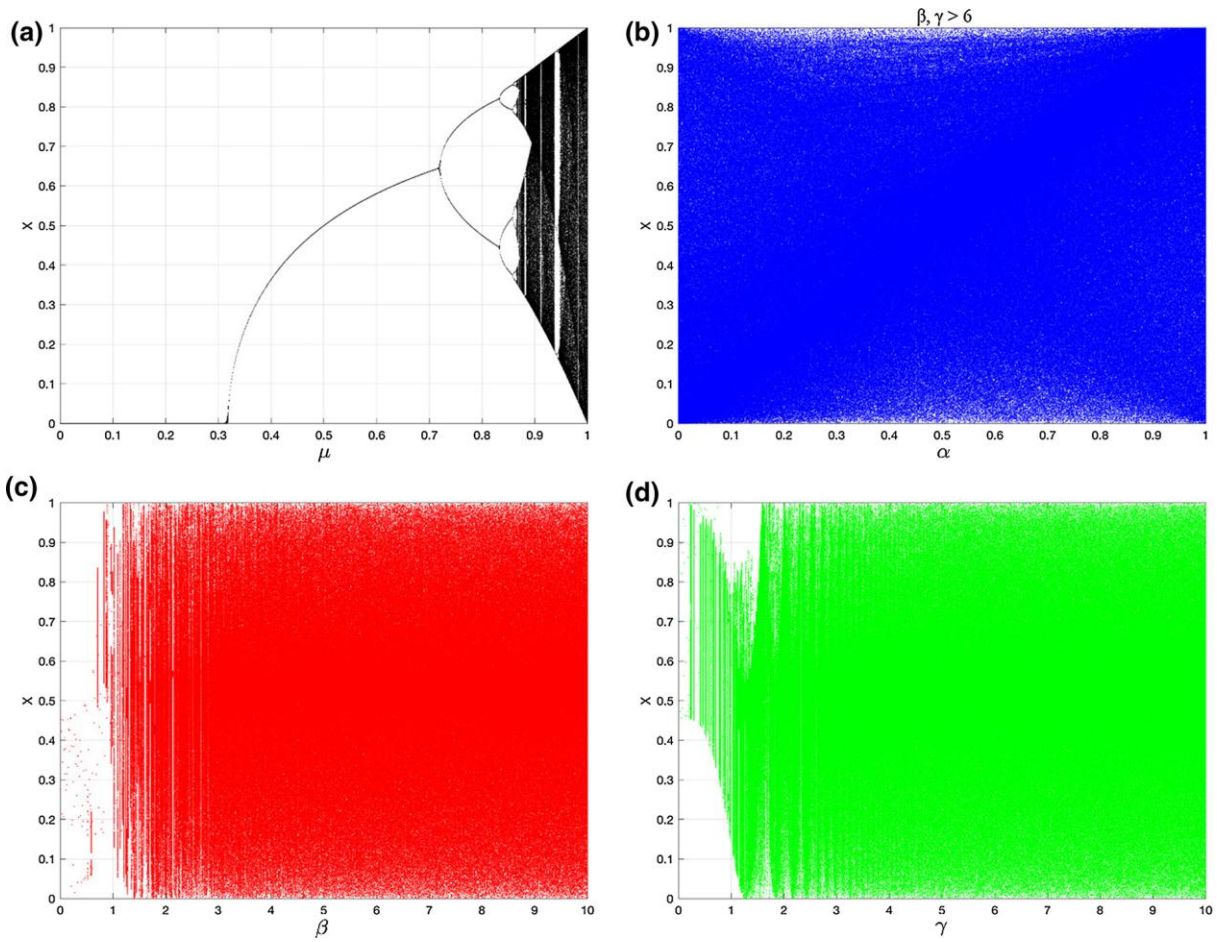


Figure 3.3 : Diagramme de bifurcation (a) de la suite sinus de base ; (b), (c) et d de la suite sinus modifiée.

Il est bien clair qu'avec le suite modifiée, nous avions eu des plages chaotiques plus étendues [0.10] par rapport a la carte chaotique initiale [0.1], cela d'une part, d'autre part l'intervalle ou le système est vraiment chaotique passe de l'intervalle $\mu \in [0.85\ 1]$ à l'intervalle $\mu \in [0.85\ 10]$..

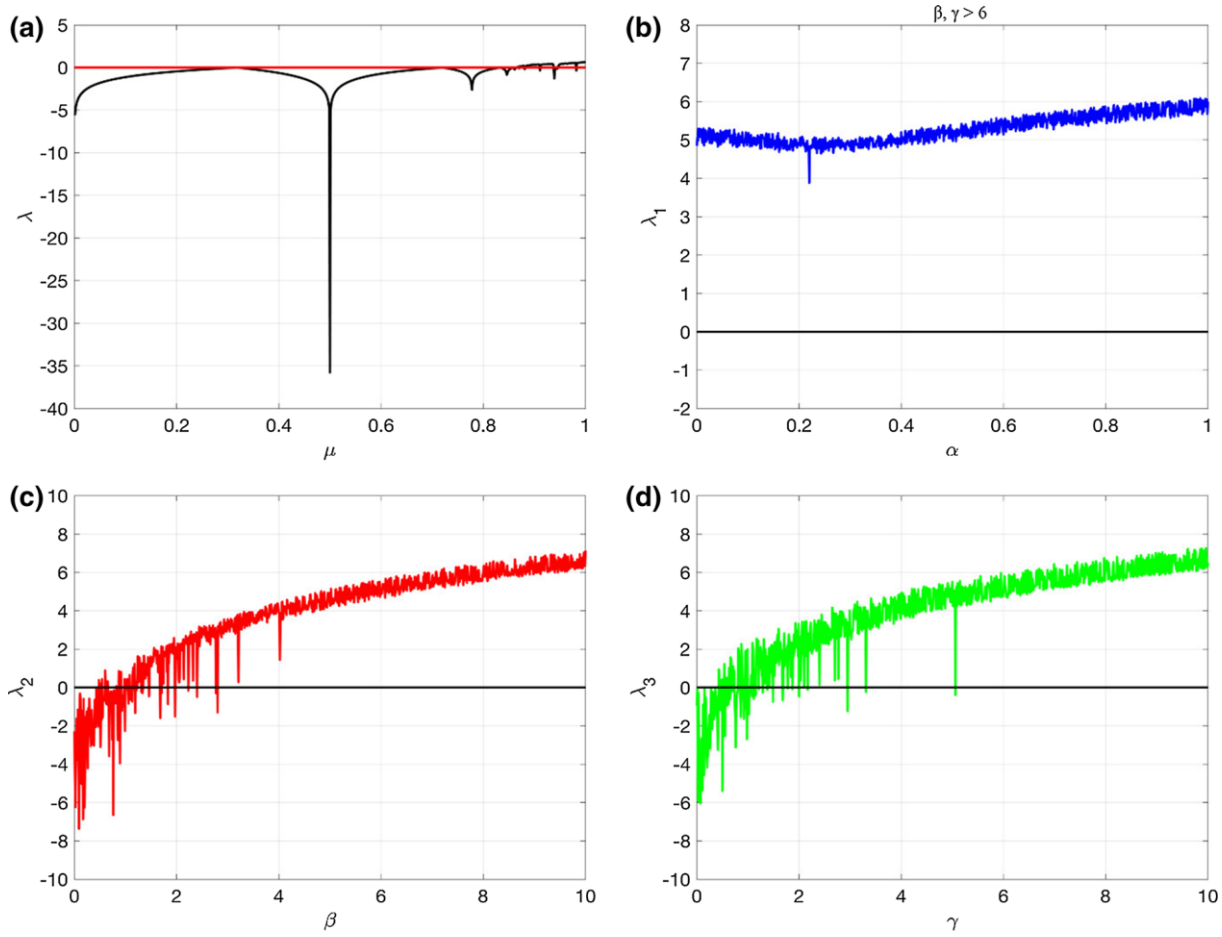


Figure 3.4 : Analyse de l'exposant de Lyapunov (a) de la suite sinus de base ; (b), (c) et d de la suite sinus modifiée.

3.4 Algorithme de cryptage d'images proposé

Le schéma de cryptage proposé est détaillé comme suit :

1- Soit I l'image originale à crypter de taille (m, n) .

2- Remodeler la matrice image à crypter en un vecteur v de taille $(1, m \times n)$.

Phase de substitution :

3- Le vecteur v est embrouillé (changement de position des pixels) selon un ordre imposé par une suite chaotique sinus modifiée de paramètres $\{x_1, \alpha_1\}$, pour donner un autre vecteur vv de taille $(1, m \times n)$.

4- Générer un autre vecteur de taille$(1, m \times n)$, en utilisant une autre suite chaotique sinus modifiée de paramètres $\{x_2, \alpha_2\}$, afin d'être adapter au niveau du gris ce vecteur est multiplié par 255 puis arrondi pour donner naissance à un autre vecteur appelé vvv.

Phase de diffusion :

5- La phase de diffusion (changement des valeurs des pixels) est assurée par application de l'opération XOR entre le vecteur vv et le vecteur vvv pour donner naissance à un vecteur résultant c selon la formule suivante :

$$\mathbf{c(1)} = \boldsymbol{vv}\mathbf{(1)} \oplus \boldsymbol{vvv}\mathbf{(1)} \quad \mathbf{pour\ i = 1}$$

$$\mathbf{c(i)} = \mathbf{c(i-1)} \oplus \boldsymbol{vv}\mathbf{(i)} \oplus \boldsymbol{vvv}\mathbf{(i)} \mathbf{pour\ i\ allant\ de 1\ à\ m \times n} \qquad (3.10)$$

Où $\oplus$ désigne l'opérateur ou exclusif

6- Le vecteur c ainsi trouvé est converti en une image I_{cry}de taille$(m \times n)$.qui est l'image cryptée

NB/ Le processus de décryptage prendra exactement le chemin inverse de celui de cryptage

3.5 Résultats de simulation et tests

Les tests de simulations sont faits sous environnement matlab 2014 moyennant un labtop personnel ayant les caractéristiques suivantes : Intel (R) core (TM) i3-4005U CPU@ 1.70 GHZ avec mémoire (RAM) de 4GHZ. Les images tests utilisées sont celles de Lena et Barbara de taille (256×256) et Living-room et Clown de taille (512×512), les paramètres de la suite sinus modifiée utilisée sont : la valeur initiale $x_1 = 0.43$ avec $x_1 \in [0\ 1]$, $\alpha = 0.67$ avec $\alpha \in [0\ 1]$, $\beta = 6.94$ avec $\beta > 6$, $\gamma = 7.84$ avec $\gamma > 6$.

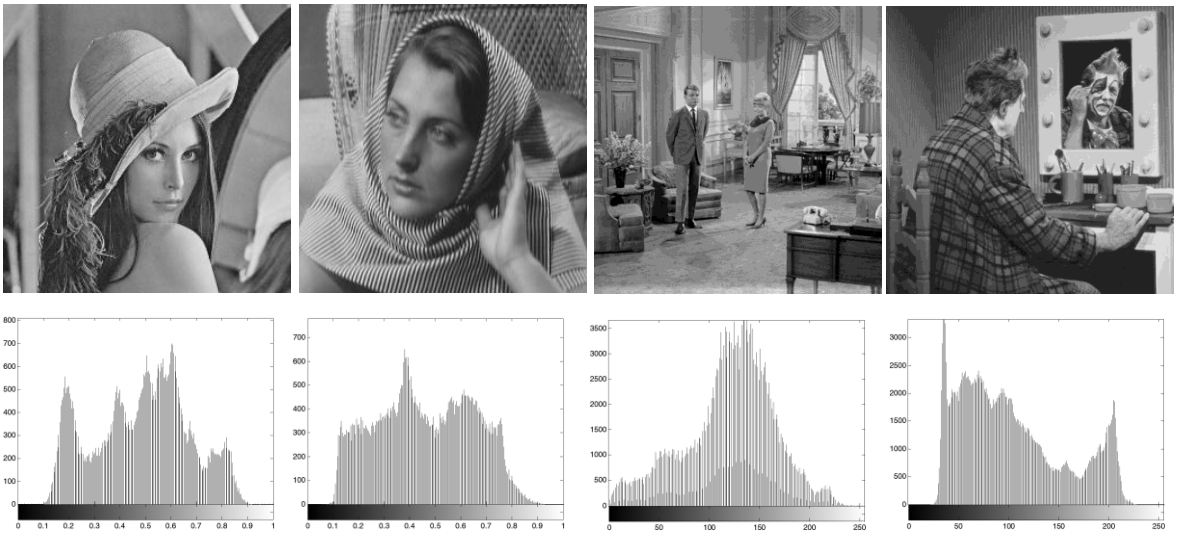


Figure 3.5 : Images de test de Lena, Barbara, Living-room et Clown et leurs histogrammes.

3.5.1 Analyse des histogrammes

Nous partons de quatres images standards de test de Lena, Barbara, Living-room et Clown ayant des histogrammes différents comme illustrer dans la figure 3.5. Nous

remarquons que leurs images cryptées (figure 3.6) ayant des histogrammes identiques, ce qui est difficile pour un éventuel attaquant d'en tirer une information qui peut révéler l'image originale, par conséquent, nous concluons que l'algorithme proposé est robuste vis-à-vis de l'analyse par histogrammes.

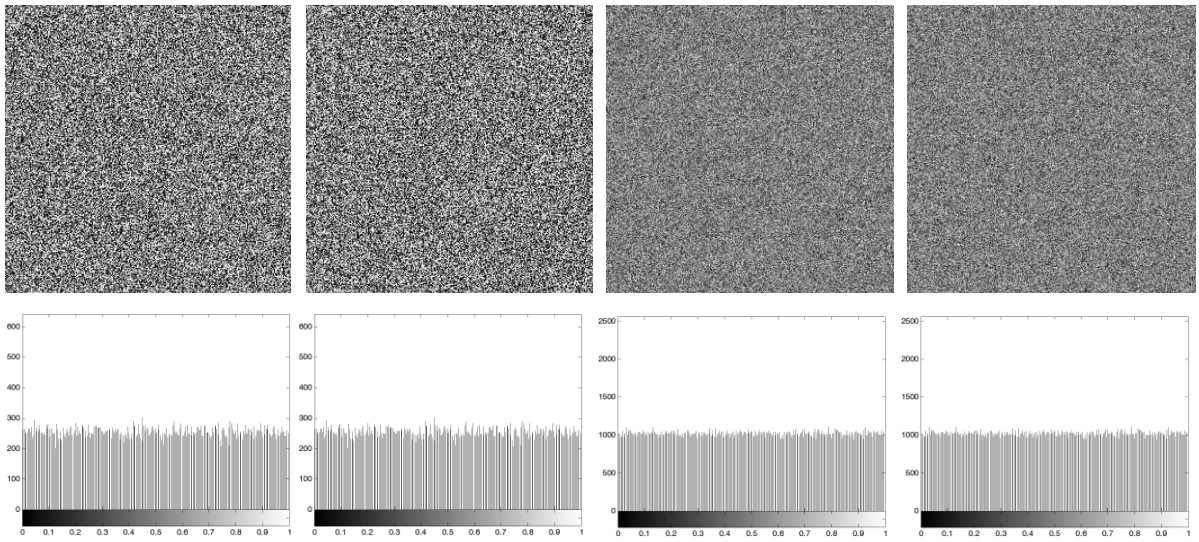
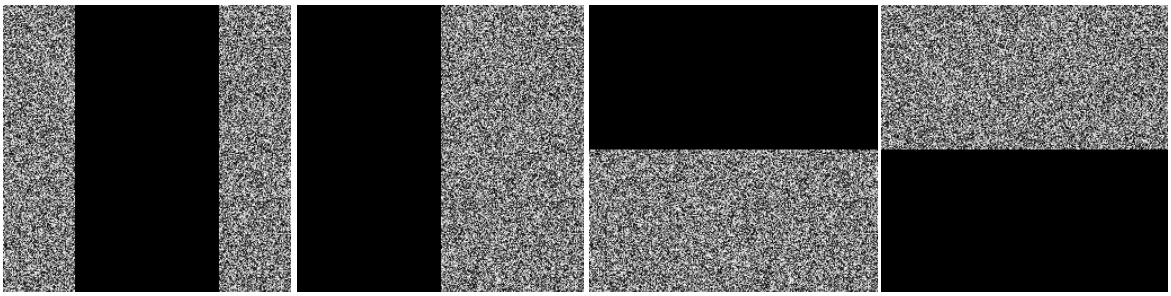
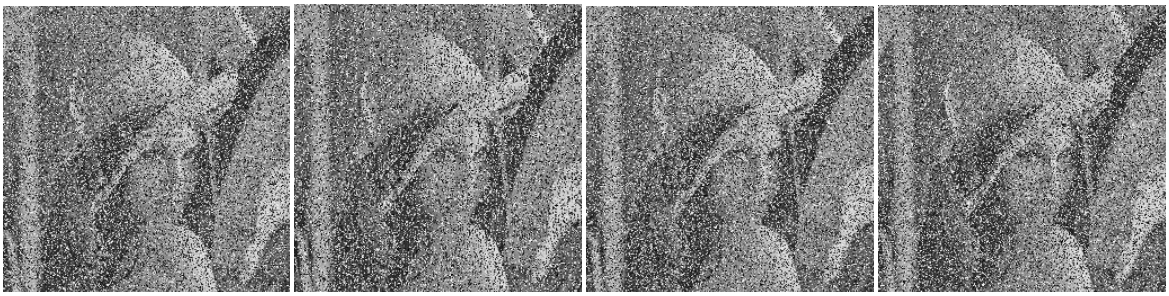


Figure 3.6 : Images cryptées de Lena, Barbara, Living-room et Clown et leurs histogrammes.

3.5.2 Test de l'algorithme vis-à-vis des pertes de données



(a)



(b)

Figure 3.7 : Test de pertes de données: (a) **Image cryptée de Lena avec pertes de 50%** (b) **Son image décryptée correspondante.**

Pour tester la robustesse de l'algorithme vis-à-vis des pertes de données, nous supposons que l'image cryptée subit une déperdition de données d'un taux de 50% , ce qui est exprimé par simulation par remplacement de la moitié des données des pixels en niveau du gris par des zéros à l'émission comme indiquer sur la figure 3.7 et voir sa répercussion sur l'image décryptée au niveau de la réception. Nous remarquons que malgré un taux de pertes de 50%, l'image décryptée est déchiffrable voire identifiable à l'œil nu, ce qui vérifie la robustesse de l'algorithme proposé.

3.5.3 Analyse de corrélation des pixels adjacents

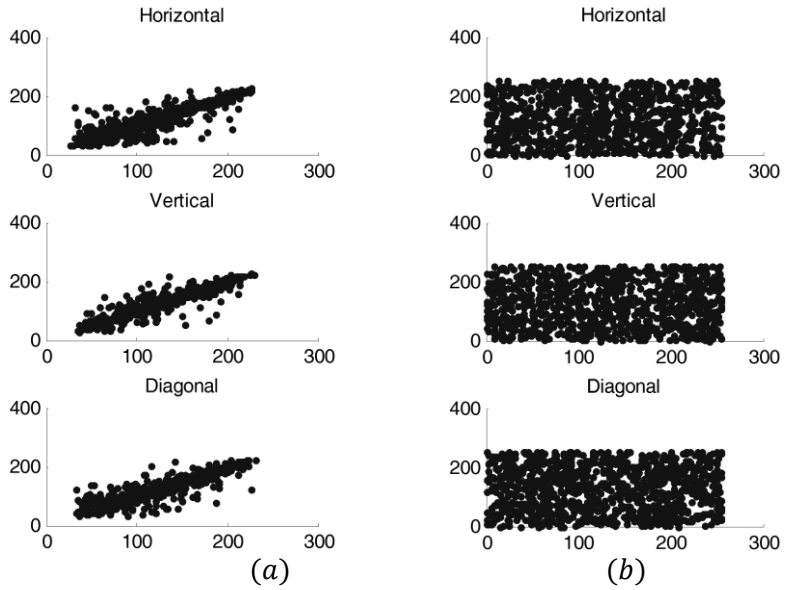


Figure 3.8 : Distribution de la corrélation des pixels adjacents dans les trois directions horizontale, verticale et diagonale de: (a) **Image originale** (b) **Image cryptée.**

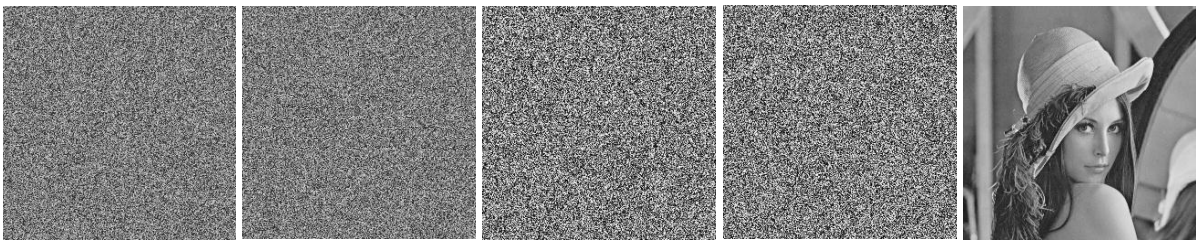
Le test de corrélation entre pixels adjacents s'agit de sélectionner de façon aléatoire 1000 paires de pixels adjacents de l'image originale et 1000 paires de l'image cryptée et analyser les corrélations aux directions horizontale, verticale et diagonale des deux images originale et cryptée. Les diagrammes de corrélation entre les pixels adjacents aux directions horizontale, verticale et diagonale de l'image de Lena originale et de son image cryptée sont représentés sur la figure 3.8 et les coefficients de corrélation de l'image originale dans les trois directions se rapprochent de 1, tandis que ceux de son image cryptée se rapprochent de 0 TABLE 1. Dans ce cas, nous disons que le chiffrement a atténué considérablement la corrélation entre pixels de l'image cryptée, nous remarquons aussi sur la figure 3.8 (a) que la distribution des intensités des pixels de l'image originale se concentre sur la diagonale,

les pixels sont alors fortement corrélés, tandis que ceux de l'image cryptée figure 3.8 (b) sont non-corrélés et ont une distribution uniforme [6].

TABLEAU 3.1 ANALYSE DE CORRELATION DES PIXELS ADJACENTS

Coefficient de corrélation Image Originale / Image cryptée			
Direction	*méthode proposée*	[4]	[5]
Horizontale	0.9258/0.0013	0.9258/-0.0105	0.9258/0.0027
Verticale	0.9593/-0.0069	0.9593/-0.0009	0.9593/0.0026
Diagonale (lower left to top right)	0.9258/0.0014	0.9258/0.0029	0.9258/0.0004
Diagonale (lower right to top left)	0.9037/0.0036	0.9037/0.0079	0.9037/0.0024

3.5.4 Sensibilité de la clé de cryptage



(a) (b) (c) (d) (e)

Figure 3.9 : Test de sensibilité: image de Lena décryptée avec (a) $\boldsymbol{\alpha_1' = \alpha_1 + 10^{-16}}$ $\boldsymbol{(b) x_1' = x_1 + 10^{-16}}$ $\boldsymbol{(c) \alpha_2' = \alpha_2 + 10^{-16}}$ $\boldsymbol{(d) x_2' = x_2 + 10^{-16}}$ $\boldsymbol{(e)}$ **Clé correcte**.

la clé de cryptage est composée des parametres de la suite chaotique sinus modifiée $\{\boldsymbol{x_1},\ \boldsymbol{\alpha_1}\}$ et $\{\boldsymbol{x_2},\ \boldsymbol{\alpha_2}\}$ utilisés. Pour vérifier la sensibilité de l'algorithme proposé , nous opérons une erreur dans l'un des élements des composante de cette clé de cryptage designée par $\boldsymbol{k}\{\boldsymbol{x_1},\ \boldsymbol{\alpha_1}, \boldsymbol{x_2}, \boldsymbol{\alpha_2}\}$ toute en gardant les autres. La figure 3.9 illustre les cinq cas possibles $\{\boldsymbol{x_1' = x_1' + 10^{-16}}, \boldsymbol{\alpha_1}, \boldsymbol{x_2}, \boldsymbol{\alpha_2}\}$, $\{\boldsymbol{x_1' = x_1'}, \boldsymbol{\alpha_1 + 10^{-16}}, \boldsymbol{x_2}, \boldsymbol{\alpha_2}\}$, $\{\boldsymbol{x_1' = x_1'}, \boldsymbol{\alpha_1}, \boldsymbol{x_2 + 10^{-16}}, \boldsymbol{\alpha_2}\}$, $\{\boldsymbol{x_1},\ \boldsymbol{\alpha_1}, \boldsymbol{x_2}, \boldsymbol{\alpha_2 + 10^{-16}}\}$ et clé correcte. les quatres premiers cas montrent clairement que l'image décryptée est totalement brouillée , ce qui prouve la sensibilité du cryptage à la clé $\boldsymbol{k}\{\boldsymbol{x_1},\ \boldsymbol{\alpha_1}, \boldsymbol{x_2}, \boldsymbol{\alpha_2}\}$.

3.5.5 Clé de cryptage

La clé de cryptage $\{x_1,\ \alpha_1, x_2, \alpha_2\}$ comme indiqué au paragraphe précédent est composée des parametres de la suite chaotique sinus modifiée $\{x_1,\ \alpha_1\}$ et $\{x_2,\ \alpha_2\}$ ayant chacune une sensibilité de 10^{-16} donc une précision de 10^{+16}, donc la clé de cryptage en entier vaut : $10^{+4\times16} = 10^{64} \cong 2^{192}$ qui est largement suffisante devant la valeur exigé en cryptographie.

3 .6 Conclusion

Dans le présent chapitre, nous avons évoqué le problème de limitation de l'intervalle chaotique des suites chaotiques de bases telles que la suite Logistique map, sinus map etc, et par conséquent la limitation de l'espace clé des algorithmes de cryptage associés.

Nous avons démontré à travers les résultats de simulation qu'il est possible d'améliorer les performances de ces suites de base par des modifications opérées au sein de ces suites. L'exemple expérimental est porté sur la suite sinus de base et la suite modifiée est appelée suite sinus modifiée, les outils de vérification comme le diagramme de bifurcation et l'exposant de Lyapunov ont prouvé l'efficacité de ces modifications et les résultats d'expérimentation lorsque elle est utilisée en cryptage d'images ont consolidé les améliorations escomptées.

Conclusion générale

Conclusion générale

Le Chaos est une sorte des caractéristiques des systèmes non linéaires, qui est un comportement dynamique instable borné que "les expositions" sensibles ont une dépendance aux conditions initiales et comprend une infinité de mouvements périodiques instables. Bien qu'il semble être aléatoire, il se produit dans un système déterministe non-linéaire dans des conditions déterministes.

En l'occurrence, le chaos est une alternative pour remplacer ou améliorer les techniques de chiffrement classiques déjà existantes.

Le travail réalisé dans ce mémoire consiste à développer et implémenter une nouvelle suite unidimensionnelle est appelée suite sinus modifiée basée sur la suite chaotique sinus et cette nouvelle suite a été développée dans un algorithme de cryptage d'image ayant pour but l'amélioration de la sécurité de l'espace clé par rapport aux suites chaotiques de base telles que la suite logistique et la suite Sinus.

Et à travers le diagramme de bifurcation et l'analyse des exposants de Lyapunov obtenus qu'on a prouvé les performances de la suite et qui peut être utilisée de manière sécurisée comme étant un générateur de nombres pseudo-aléatoires dans les systèmes de cryptage pour les images numériques.

L'algorithme de cryptage d'images à base de cette suite est basé sur la structure de confusion-diffusion et qui exploite le principe de récursivité et la dépendance des paramètres de cette suite à l'image à crypter.

Nous concluons que l'algorithme proposé est robuste à travers les tests cryptographiques appliqués comme l'analyse par histogrammes et l'attaque par pertes de données, en effet la clé de cryptage est très suffisante 2^{192} devant la valeur exigé en cryptographie .

En confirmant avec les résultats obtenus expérimentalement que la technique suggérée a de meilleures performances en termes de sécurité et mesures de qualités visuelles.

Bibliographie

Chapitre 1

[1] Broer Vakgroep, The how and what of chaos, NAW 5/1 nr.1 maart 2000, pp 34-43,2000.

[2] Bekkouche. T, « Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes » Thèse Doctorat. Soutenue le 14/10/2018.

Chapitre 2

[1] http://dspace.univ-tlemcen.dz/bitstream/112/1046/8/Chapitre2.pdf.

[2] http://dit-archives.epfl.ch/FI00/fi-sp-00/sp-00-page5.html, 25-Avr-2018.

[3] AHMED BELHADJ, souhila, "Etude comparative entre la cryptographie àclé secrète et à clé publique appliquée aux textes arabes", 19-nov-2014.

[4] https://www.commentcamarche.com/contents/213-chiffrement-parsubstitution;11-05-2018.

[5] https://www.commentcamarche.com/contents/216-cryptage-par-transposition

[6] http://dspace.univ-tlemcen.dz/bitstream/112/1046/9/Chapitre3.pdf

[7] https://www.tezabo.com/blog/definition-resolution-poids-taille-ppi-dpidimension-image;12-05-2018

[8] http://serge.wacker.free.fr/technoprimaire/c2i/revisions/formats_image.pdf

[9] http://www.mycube.fr/quest-ce-quune-image-numerique/index.html.

[10] http://www.cryptage.org/images-cryptees.html.

[11] Contribution à l'étude des mécanismes cryptographiques, Thèse deDoctorat en Informatique, Présentée Par Beloucif Assia, Université de Batna 2**,**Soutenue le: 22 / 09 / 2016.

[12] https://www.sites.univ-rennes2.fr/artspectacle/ cian/image_numFlash/pdf/chap3_tout.pdf.

[13] Parvaz, R., Zarebnia, M.: A combination chaotic system and application in color image encryption. Opt. Laser Technol. **101** (2018)

[14] Aimeur Akram. :Conception et implémentation d'un système hybride pour la sécurité de données : application aux images numériques, 26-30 2017

Chapitre 3

[1] Irani ,B. Y. et al.: Digital image scrambling based on a new one-dimensional coupled Sine map. Nonlinear Dyn, doi.org/10.1007/s11071-019-05157-5.

[2] Hilborn, R.C.: Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers. Oxford University Press on Demand, Oxford (2000).

[3] Robert, L.D.: An Introduction to Chaotic Dynamical Systems. Addison-Wesley, Boston (1989)

[4] Hanis, S., Amutha, R.: A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterfly-like structure. Nonlinear Dyn. **95**(1), 421–432 (2019)

[5] Parvaz, R., Zarebnia, M.: A combination chaotic system and application in color image encryption. Opt. Laser Technol. **101**, 30–41 (2018)

[6] Bekkouche. T, « Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes » Thèse Doctorat. Soutenue le 14/10/2018.

Abstract

Chaos, a phenomenon typical of nonlinear systems, is today very widely studied, within reason of its properties and the many potential applications. Indeed, we can observe chaos in many physical phenomenons, electronic, chemical, meteorological, demographic or economic phenomena and its characteristics "make it possible to consider using it for application purposes." In this thesis, we proposed a new modified chaotic map that is called a modified sine map we have also discussed the problem of limiting the chaotic interval of basic chaotic sequences such as the map, sinus map, by the proposition of this modified sequence which is beneficially applied in image encryption.

Keywords: chaotic suite, sinus map, image encryption

.*Résumé*

Le chaos, phénomène typique des systèmes non linéaires, est aujourd'hui très largement étudié, en raison de ses propriétés et des nombreuses applications potentielles. En effet, on peut observer du chaos dans de nombreux phénomènes physiques, électronique, chimiques, météorologiques, démographiques ou économiques et ses caractéristiques "font qu'on peut envisager de l'utiliser à des fins applicatives. Dans ce mémoire, nous avons proposé une nouvelle suite chaotique modifiée qui est appelée suite sinus modifiée. Nous avons évoqué également le problème de limitation de l'intervalle chaotique des suites chaotiques de bases telles que la suite Logistique map, sinus map par la proposition de cette suite modifiée qui est bénéfiquement appliquée au cryptage d'images.

Mots clés : suite chaotique, sinus map, cryptage d'image

ملخص

الفوضى هي ظاهرة نموذجية للأنظمة غير الخطية، تدرس اليوم على نطاق واسع ، بسبب خصائصها والعديد من التطبيقات المحتملة. في الواقع ، يمكننا ملاحظة الفوضى في العديد من الظواهر الفيزيائية أو الإلكترونية أو الكيميائية أو الأرصاد الجوية أو الديموغرافية أو الاقتصادية وخصائصها "تجعل من الممكن النظر في استخدامها لأغراض التطبيق." في هذه الأطروحة ، اقترحنا خريطة فوضوية معدلة جديدة تسمى مجموعة الجيب المعدلة لقد ناقشنا أيضًا مشكلة الحد من الفاصل الزمني الفوضوي للخرائط الفوضوية الأساسية مثل الخريطة اللوجستية ، خريطة الجيب ، من خلال اقتراح هذا الخريطة المعدلة الذي يتم تطبيقها بشكل مفيد في تشفير الصور.

.**الكلمات المفتاحية**: خريطة فوضى ، خريطة الجيوب الأنفية ، تشفير الصور