République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur Et de la Recherche Scientifique
Université Mohamed Sadik 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
Spécialité : Réseau et Sécurité
Thème

Réalisation d'un **S**ystème de **C**ryptage des **I**mages **N**umérique basé sur le **C**haos

Dirigée par:
M^me^ . Noura Louzzani

Réalisé par :
Aissam Djemaa
Aissa Boubednikh

2021

Résumé

Aujourd’hui, il est important de protéger les informations sensibles afin qu'elles ne deviennent pas vulnérables à un accès non autorisé. Le cryptage est utilisé pour assurer une sécurité élevée pour les images. Chaos a été largement utilisé pour le cryptage d'images pour ses différentes fonctionnalités.

Notre travail dans ce mémoire porte sur le cryptage des images numériques par l’utilisation des propriétés remarquables du chaos. Pour ce faire, nous présentons un nouveau système de cryptage des images numériques basé sur une combinaison de la fonction Logistique et la fonction Sine Map.

Les résultats obtenus sont encourageants et nous permettent de prouver son grand niveau de sécurité.

Mots clés

Cryptage, Chaos, Images Numériques, Fonction Logistique, Sine Map.

Abstract

Today, it is important to keep sensitive information secure from becoming vulnerable to unauthorized access. Encryption is used to ensure high security for Images. Chaos has been widely used for image encryption for its different features.

In this thesis, we focuse on the encryption of digital images by using the remarkable properties of chaos.to make this happened, we present a new digital image encryption system based on a combination of the logistics function and the sine function.

Our results are reliable and it allows us to prove the high level of security of our system.

Keywords

Encryption, Chaos, Digital Images, Logistic Function, Seine Map.

REMERCiMENT

Grand merci à Allah, Miséricordieux, le tout puissant qui nous 'a donné la force, la persévérance et la patience d'accomplir notre travail.

*Notre gratitude, Nos vifs remerciements et nos respects à notre encadrante M^me^* ***Louzzani Nora****, pour tous ses judicieux conseils, son temps qu'elle nous 'a consacré et pour ses orientations.*

Nous remercions l'ensemble des membres du jury qui nous 'ont fait l'immense plaisir d'avoir accepté d'examiner et d'évaluer mon travail.

Un grand merci à tous ***les enseignants*** *du* ***département d'Informatique*** *qui ont été impliqués d'une manière ou d'une autre dans la formation en master et en licence.*

J'exprime également mes remerciements à nos familles, nos amis et tous ceux qui ont contribué de près ou de loin à la cristallisation de ces souvenirs, ainsi qu'à la réussite de cette merveilleuse année universitaire…

Table des matières

Chapitre II : Etat de l'Art sur les Systèmes de Cryptage Chaotique des Images

Chapitre III : Réalisation d'un système de cryptage chaotique des images

Liste des Figures

Liste des Tableaux

Liste des Abréviations

- **WEP** : Wired Equivalent Privacy

-**DES**: Data Encryption Standard

- **SSL** : Secure Sockets Layer

-**CFB** : Cipher Feedback

-**OFB** : Output Feedback

-**CBC** : Cipher Block Chaining

-**ECB** : Electronic Code Book

-**PCX** : PiCtureeXchange

-**GIF** : GraphicInterchange Format

-**BMP** : Windows Bitmap

- **TIFF** : Tag Image File Format

-**JPEG**: Joint Photographic Experts Group

-**PSNR** : Peak Signal to Noise Ratio

-**MSE** : Means Square Error

-**ET** : Encryption Throughput

-**NCPB** : Number of Cycles Per Byte

-**UACI** : Unified Average Changing Intensity.

-**1D** :1 Dimensional

-**2D**: 2 Dimensional

-**3D** :3 Dimensional

-**LTS** : Logistic Tent System

-**PWLCM** : Piece-Wise LinearChaoticMap

-**RGB**: Red Green Blue.

-**AES**: Advanced Encryption Standard.

- **ADN** : acide désoxyribo nucléique.

Introduction Générale

Introduction générale

Depuis l'Antiquité, l'homme s'est intéressé aux moyens de communication et n'a cessé de les développer pour transférer des informations et des données personnelles ou confidentielles (images, signes, signal etc...), il essaie à les protéger contre toutes les attaques et les violations.

A l'heure actuelle, avec le développement technologique rapide, il y a un développement des méthodes de protection en termes de sécurité, qui s'est accompagné du développement des moyens d'espionnage et de piratage. A cet égard, plusieurs solutions ont été proposées, telles que : la cryptographie.

La cryptographie est l'étude des méthodes qui permettent de transmettre des données de manière confidentielle. Afin de protéger une information, on lui applique une transformation qui la rend incompréhensible ; c'est ce qu'on appelle le chiffrement/cryptage, qu'à partir d'une information originale, il donne une autre information chiffrée. Inversement, le déchiffrement/décryptage est l'action qui permet de reconstruire l'information originale à partir de l'information chiffrée/cryptée.

Récemment, nous pouvons remarquer une augmentation significative de l'utilisation de photos et de vidéos dans les réseaux sociaux tels que Facebook et Instagram, dans les moteurs de recherche visuels tels que Google images et la recherche d'images Yahoo, les services de stockage en cloud tels que Google Drive. Cette croissance rapide de l'utilisation du contenu visuel devrait augmenter dans l'avenir proche en raison des technologies à venir telles que la réalité virtuelle et la 5G. Afin de transférer ce contenu de manière sécurisée, certains mécanismes et applications peuvent être utilisés, dont la plupart peuvent dépendre de la cryptographie.

Dans le monde réel, une variété des algorithmes de cryptage efficaces sont disponibles, tels que AES (Advanced Encryption Scheme), RSA (Rivest-Shamir-Adelman) et ElGamel. Ces algorithmes sont conçus pour crypter des informations textuelles, et malheureusement, ils ne fonctionnent pas avec la même efficacité avec des données fortement

corrélées comme les images ou les vidéos, ce qui fait de la sécurisation de ce type de données un problème croissant, et l'une des solutions non traditionnelles à ce problème est ce que l'on appelle les "algorithmes de cryptage d'images basés sur le chaos", comme son nom l'indique : ce sont des algorithmes cryptographiques qui exploitent les phénomènes de chaos et ses caractéristiques telles que la sensibilité aux conditions initiales pour crypter les images.

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

Dans ce travail, nous allons donner une proposition pour répondre au problème précédemment énoncé : un algorithme de cryptage d'images qui utilise des systèmes chaotiques, qui est essentiellement une combinaison de la fonction logistique bien connue et la fonction sine map.

Organisation du mémoire

Ce mémoire est organisé comme suit :

Le **premier chapitre** présente un aperçu des trois sujets liés à notre sujet principal : « cryptage d'images basé sur le chaos », qui sont : la cryptographie, le chaos et les images numériques.
Dans le *premier sujet*, nous présentons les bases de la cryptographie moderne et ses deux principaux types : les chiffrements symétriques, les chiffrements asymétriques.
Dans le *second*, nous présentons une brève introduction aux systèmes dynamiques, chaos et aux quelques concepts de base tels que la bifurcation.
Alors que dans le *dernier sujet*, nous présentons les concepts liés à l'image numérique, les types d'images existants et les formats de fichiers d'images largement utilisés.

Dans **le deuxième chapitre**, nous ferons un état de l'art des systèmes de cryptage d'images basés sur le chaos que nous pouvons les appelé les systèmes de la cryptographie chaotique des images, dans ce chapitre, nous présenterons d'abord les métriques utilisées pour

évaluer la sécurité et les performances des schémas de cryptage d'images, ensuite, nous classons les systèmes de cryptage d'images basés sur le chaos en deux classes, la première classe contient des systèmes qui n'utilisent que des systèmes chaotiques dans le processus de cryptage/décryptage. Alors que la seconde contient des chiffrements basés sur un mélange de systèmes chaotiques et non chaotiques.

Le **dernier chapitre** est dédié à l'étude détaillée de notre système de cryptage chaotique basé sur une nouvelle fonction chaotique définit par une combinaison des deux fonctions : la fonction logistique et la fonction sine map.

A la fin de ce mémoire, nous donnerons une conclusion générale, qui contiendra un résumé de ce travail, et les différentes perspectives.

Chapitre I

Généralités sur la cryptographie, le chaos et l'image numérique

I.1. Introduction

Quand on parle de la cryptographie plusieurs interprétations se réveille. En général, la cryptographie a été dans la plupart des cas perçue comme une chimie noire qui est seulement utilisée par les états et les gouvernements reflétant la complexité et la difficulté et parfois l'impossibilité de la décrypter que par des mathématiciens brouillons.

Dans ce chapitre nous présentons un aperçu sur les trois éléments clés qui sont directement liés à notre travail : la cryptographie, le chaos et les images, tout en donnant les concepts de base les plus importantes nécessaires à la compréhension de notre travail.

I.2 Cryptographie

I.2.1 Définition de la cryptographie

Le mot cryptographie vient des deux mots grecs kryptós "secret" et gráphein "écrire", c'est-à-dire écrire secrètement. Ce terme générique désigne l'ensemble des méthodes utilisées pour cacher l'information, c'est-à-dire la rendre incompréhensible sans aucun secret.

Donc la cryptographie est l'art de cacher une information pour la rendre inintelligible [1][2] à toute personne ne connaissant pas un certain secret. Autrement dit, c'est l'ensemble des processus de verrouillage visant à protéger l'accès à certaines données afin de les rendre incompréhensible aux personnes non autorisées [3].

La figure suivante illustre le schéma du principe général de la cryptographie.

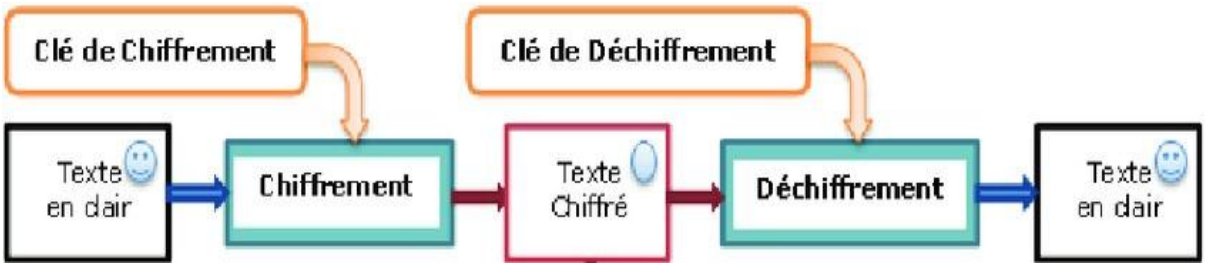


Figure I.1 Schéma général de la cryptographie.

- **Texte en clair :** est le message à protéger (à chiffrer).
- **Texte chiffré :** est le résultat du chiffrement du texte en clair.

- **Chiffrement :** est la méthode ou l'algorithme utilisé pour transformer un texte en clair en texte chiffré.
- **Déchiffrement :** est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair.
- **Clé :** est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré (clé de chiffrement) et pour déchiffrer le texte chiffré en texte en clair (clé de déchiffrement). On peut parfaitement concevoir un algorithme qui n'utilise pas de clé, dans ce cas c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé.

I.2.2 Objectifs de la cryptographie

Il existe quatre grands objectifs :

- **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[1] de signer son message, ainsi, le récepteur[2] n'aura pas de doute sur l'identité du premier.
- **Intégrité** : les données vont être protégées du changement de la personne non autorisé comme la suppression, l'ajout, et la mise à jour.
- **Non-répudiation** : est la garantie qu'aucun des deux individus ayant effectué une transaction ne pourra nier avoir reçu ou envoyé les messages.

I.2.3 Méthodes de la cryptographie

On distingue les méthodes de la cryptographie classiques et les méthodes de la cryptographie modernes.

I.2.3.1 Méthodes de la cryptographie Classiques

a. Cryptographie par substitution : Les substitutions consistent à remplacer des symboles ou des groupes de symboles par d'autres symboles ou groupes de symboles dans le but de créer de la confusion.

On distingue deux méthodes de substitution, la substitution mono-alphabétique et la substitution poly-alphabétique [4].

1 :C'est la personne qui possède la clé de chiffrement pour chiffrer un message et l'envoie au récepteur.
2 : C'est la personne qui possède la clé de déchiffrement pour déchiffrer un message reçu de l'émetteur.

- Substitution mono-alphabétique : Remplace chaque lettre du message par une autre lettre de l'alphabet. La méthode de remplacement est sur le tableau (I.1).

Texte clair	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Texte chiffré	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tableau I.1 substitution mono-alphabétique

-Exemple : on a le texte clair « la cryptographie » donc le texte crypté sera « odfubswrjudsklh ».

- Substitution poly-alphabétique : Utilise une suite de chiffres monoalphabétiques "la clé" réutilisée périodiquement.

b. Cryptographie par transposition : Les transpositions consistent à mélanger les symboles ou les groupes de symboles d'un message clair suivant des règles prédéfinies pour créer de la diffusion. Ces règles sont déterminées par la clé de chiffrement. Une suite de transpositions forme une permutation.

c. Cryptographie par produit : C'est la combinaison de chiffrement par substitution et chiffrement par transposition. La plupart des algorithmes à clés symétriques (voir la section 4.2.1) utilisent le chiffrement par produit. On dit qu'un « round » est complété lorsque les deux transformations ont été faites une fois substitution et transposition. Ces successions des rondes portent également le nom de réseaux S-P de Shannon.

I.2.3.2 Méthodes de la cryptographie Modernes

On distingue deux méthodes majeures de la cryptographie modernes : les méthodes à clef secrète c'est la cryptographie symétrique et les méthodes à clef publique/clef privée c'est la cryptographie asymétrique.

a. Cryptographie symétrique

Le chiffrement symétrique aussi appelé chiffrement à clé privée ou à clé secrète se base sur l'utilisation de la même clé pour crypter et décrypter les messages. La sécurité de cette solution repose sur le fait que la clé est connue uniquement par l'émetteur et le récepteur du message. La figure (I.2) illustre son principe.

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.

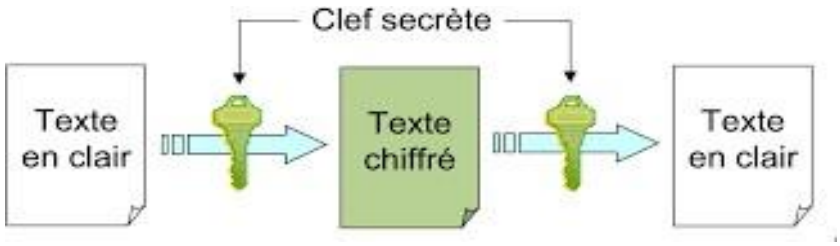


Figure I.2 Principe de cryptographie symétrique

Le cryptage symétrique fonctionne selon deux procédés différents : le cryptage par bloc s'effectue sur des blocs de bits, et le cryptage par flot s'effectue en continu, bit par bit.

a.1 Cryptage par bloc (Block Cipher)

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. Le chiffrement par bloc utilise quatre modes opératoires : Electronic Code Book(ECB), Cipher Block Chaining (CBC), Output Feedback (OFB) et Cipher Feedback(CFB) [5].

- Electronic Code Book(ECB)

Un message réel en général composé de nombreux blocs. La façon la plus immédiate pour chiffrer un tel message est de chiffrer successivement chaque bloc, avec la même clé. Toutefois cette méthode, dite ECB (Electronic Code-Book), présente des inconvénients. En particulier, lorsque deux blocs du message ou de deux messages clair sont identiques, cela se voit sur le chiffré. De plus un attaquant actif peut permuter des blocs chiffrés/ou en supprimer de telle façon que le clair modifié ait encore un sens, différent du sens initial. La méthode ECB à toute fois l'avantage d'être parallélisable, de laisser la liberté de chiffrer/déchiffrer les blocs dans n'importe quel ordre et, en cas de perte d'un bloc chiffré, de ne pas bloquer le déchiffrement des blocs restants. Ce mode est présenté sur la figure (I.3)

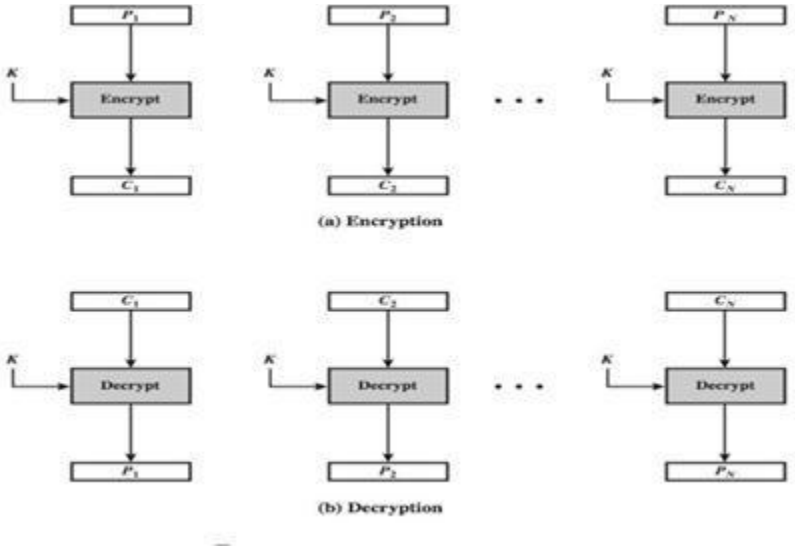


Figure I.3 ECB.

- **Cipher Block Chaining (CBC)**

Pour pallier aux inconvénients d'ECB, on utilise souvent des modes opératoires permettant de chaîner les blocs. Ainsi le mode CBC consiste, avant le chiffrement d'un bloc, à le masquer par le résultat du chiffrement du bloc précédent au moyen de l'opération XOR. Le premier bloc clair est lui aussi masqué, par une valeur habituellement notée VI (Valeur Initiale) et de préférence variable. La date et l'heure peuvent faire une bonne VI pour que les chiffrements successifs du même message soient différents. Le principe d'CBC est illustré dans la figure (I.4).

La valeur initiale VI n'a pas besoin d'être secrète, et elle est en général transmise en clair avant le message chiffré. Noter que si le destinataire reçoit un bloc chiffré avec des bits erronés, cela affecte le déchiffrement de ce bloc et du suivant mais pas des autres.

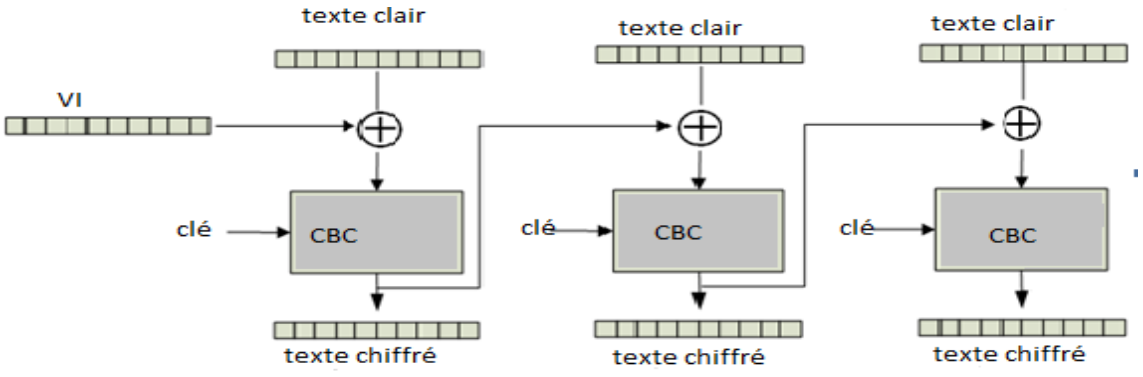


Figure I.4 CBC.

- Output Feedback (OFB)

Pour déchiffrer un message en mode ECB ou CBC, il faut avoir reçu chaque bloc chiffré complet avant de pouvoir obtenir n'importe quel bit du bloc clair correspondant. Cependant, certains applications nécessitent de pouvoir déchiffrer le flux des données au fur et à mesure de leur arrivée, même si la transmission se fait par petits morceaux. Cela est possible en utilisant le mode OFB. Celui-ci consiste à itérer la fonction de chiffrement sur une valeur initiale VI et à utiliser le flot de bits pseudo-aléatoires obtenus pour masquer les bits clairs à l'aide de l'opération XOR. Il est cette fois ci très important que la valeur initiale IV soit différente pour chaque nouveau message. A noter que l'opération de déchiffrement est identique à celle de chiffrement, et utilise la fonction de chiffrement de bloc et non celle de déchiffrement. Remarquons un inconvénient de cette méthode : un attaquant actif peut modifier des bits du message clair en modifiant les bits correspondants du chiffré, cela peut être aussi un avantage, si un bit du message chiffré est modifié par erreur au cours de la transmission, seul le bit correspondant du message clair sera affecté.

- Cipher Feedback (CFB)

Enfin, le mode CFB est proche du mode OFB mais le flot de bits pseudo-aléatoires dépend cette fois des blocs chiffrés. Un attaquant peut encore modifier un bit du clair en modifiant le bit correspondant du chiffré, mais alors le bloc suivant une fois déchiffré sera complètement différent du bloc original.

Pour cette catégorie, deux algorithmes très connus DES et AES sont distingués :

- DES est le système de chiffrement à clé secrète le plus célèbre et le plus utilisé, il a été adopté comme standard pour les communications commerciales. Le DES opère sur des blocs de 64 bits et utilise une clé secrète de 56 bits.
- AES est le nouveau standard de chiffrement à clef secrète. Il a été choisi parmi les 15 systèmes proposés en réponse à l'appel d'offre lancé par le NIST National Institute of Standards and Technology. Cet algorithme, initialement appelé RIJNDAEL. Il opère sur des blocs de message de 128 bits et est disponible pour trois tailles de clé différentes: 128, 192 et 256 bits [6].

a.2 Cryptage par flot (Stream Cipher)

Les algorithmes de chiffrement de flux peuvent être définis comme étant des algorithmes de chiffrement par blocs, où le bloc a une dimension unitaire 1 bit, 1 octet, etc. ou relativement petite. Leurs avantages principaux viennent du fait que la transformation peut être changée à chaque symbole du texte clair et du fait qu'ils soient extrêmement rapides. De plus, ils sont utiles dans un environnement où les erreurs sont fréquentes car ils ont l'avantage de ne pas propager les erreurs. Ils sont aussi utilisés lorsque l'information ne peut être traitée qu'avec de petites quantités de symboles à la fois [7]. Les algorithmes de cryptographie symétrique par flot:

A5: utilisé dans les téléphones mobiles de type GSM pour chiffrer la communication par radio entre le mobile et l'antenne-relais la plus proche.

RC4 : le plus répandu, conçu par Ronald Rivest, utilisé notamment par le protocole WEP Wired Equivalent Privacy, un algorithme récent de Eli Biham – E0 utilisé par le protocole Bluetooth.

- Caractéristiques du cryptage symétrique

- La rapidité d'exécution.
- La simplicité d'implémentation.
- La sécurisation de la chaîne de transmission de la clé.
- La complexité de fonctionnement : une obligation d'avoir le nombre de clés privées égal au nombre de destinataires.

b. Cryptographie asymétrique

Le cryptage asymétrique, contrairement au symétrique, se base sur l'utilisation des 2 clés : clé publique pour crypter, elle est accessible publiquement, et clé privée pour décrypter le message, elle est gardée secrète. Ce type de cryptage élimine la problématique de la transmission de la clé. Ce mode de cryptage est également nommé le cryptage à clé publique. Il est essentiel que l'on ne puisse pas déduire la clé privée de la clé publique [8]. La figure (I.5) présent son principe général.

L'exemple d'échange d'une lettre entre un émetteur et un destinataire permet d'illustrer bien ce principe : L'émetteur possède deux clés : privé et publique. Il envoie sa lettre contenant la clé publique au destinataire. Le destinataire utilise la clé publique pour crypter son message; il envoie tout à l'émetteur initial. L'émetteur utilise sa clé privée pour décrypter le message.

Un exemple d'utilisation du cryptage asymétrique est la transmission d'une clé secrète dans SSL Secure Sockets Layer. Dans la première phase de l'échange, le serveur envoie sa clé publique au client, ensuite le client valide sa fiabilité. Si la validation est correcte, il génère une pré clé principale avec l'utilisation de la clé publique du serveur. Le résultat de cette génération est ensuite envoyé au serveur.

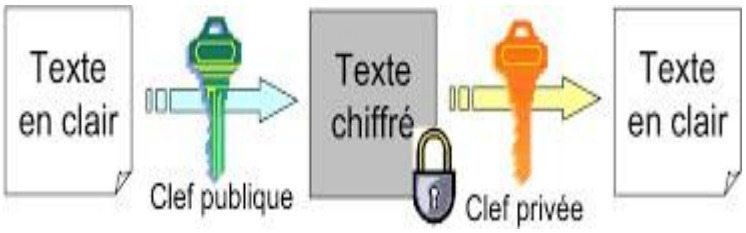


Figure I.5 Principe de cryptographie asymétrique

- **Caractéristiques du cryptage asymétrique**

- L'élimination de la problématique de la transmission de la clé.
- La possibilité d'utiliser la signature électronique.
- L'impossibilité de décrypter le message dans le cas de son interception par une personne non autorisé.
- Une paire de clés (publique/secrète) peut être utilisée plus longtemps qu'une clé symétrique.
- Le temps d'exécution : plus lent que le cryptage symétrique.
- Le danger des attaques par substitution des clés d'où la nécessité de valider les émetteurs des clés.
- Taille des clés, plus grande que celle des systèmes symétriques.

I.3 Système Dynamique

Un système dynamique est un système physique qui évolue. Il peut évoluer dans le temps ou par rapport à une autre variable suivant l'espace de phase considéré. La trajectoire d'un objet en mouvement dans le temps est donc un système dynamique, ainsi que le nombre d'individu d'une population quelconque dans le temps, encore les valeurs d'une fonction par rapport à une variable x [9] . On distinguée deux types des systèmes dynamiques (discret ou continu).

a. Systèmes dynamiques linéaires

Un système physique est dit linéaire si la relation entre les grandeurs d'entrée et de sortie peut être définie par des équations différentielles linéaires (à coefficients constants).Ces deniers vérifient alors les principes de proportionnalité des effets aux causes, et de superposition [10].

b. Système dynamique non linéaire

Un système non linéaire est un système qui n'est pas linéaire, c'est-à-dire (au sens physique) qui ne peut pas être décrit par des équations différentielles linéaires à coefficients constants. Cette définition, ou plutôt cette non-définition explique la complexité et la diversité des systèmes non linéaires et des méthodes qui ne sont pas une théorie générale pour ces systèmes, mais plusieurs méthodes adaptées à certaines classes de systèmes non linéaires [10].

I.3.1 Chaos

Il n'existe pas une définition du chaos adoptée de façon universelle dans la littérature, on pourrait dire que c'est un phénomène qui peut apparaitre dans les systèmes dynamiques déterministes non linéaires caractérisés par une évolution qui semble aléatoire et un aspect fondamental d'instabilité appelé sensibilité aux conditions initiales, ce qui le rend imprédictible en pratique à long terme.

I.3.2 Propriétés de système chaotiques

Bien qu'il n'y ait pas de définition mathématique du chaos universellement acceptée, une définition couramment utilisée stipule que pour qu'un système dynamique soit classifié entant que chaotique, il doit comporter les propriétés suivantes :

- Aspect aléatoire
- Sensibilité aux conditions initiales
- Imprévisibilité
- Notion d'attracteur

I.3.2.1 Aspect aléatoire

Les systèmes chaotiques se comportent, en effet d'une manière qui peut sembler aléatoire. Cet aspect aléatoire du chaos vient du fait que l'on est incapable de donner une description mathématique du mouvement, mais ce comportement est en fait décrit par des équations non linéaires parfaitement déterministes, comme par exemple les équations de Newton régissant l'évolution d'au moins trois corps en interaction. Les figures ci-dessus illustrent les aspects aléatoires du système chaotique continu et discrets.

I.3.2.2 Sensibilité aux conditions initiales

En faisant la troncature de quelques chiffres sur les 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 à la condition initiale. Mais en fait c'est avant cette anecdote, que ce phénomène a été découvert. Vers la fin du $19^{éme}$ 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, dans l'espace des phases va se trouver (presque toujours) rapidement amplifiée .

I.3.2.3 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 maniéré si sensible de l'état initial.

I.3.2.4 Notion d'attracteur

Avant d'expliquer la notion d'attracteur, il faudrait d'abord définir ce qu'est l'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 peut maintenant définir un attracteur comme étant une limite asymptotique des solutions de toute condition initiale localisée dans un domaine de volume non nul ou bassin d'attraction [12]. 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 dit, l'attracteur est une géométrique de l'espace de phase (formant une structure feuilletée) indiquant le comportement d'un système chaotique. L'attracteur peut être étrange avec structure fractale (une courbe ou surface de forme irrégulière ou morcelée qui se crée en suivant des règles déterministes ou stochastiques impliquant une transformation ponctuelle de type homothétie interne) ou point fixe ou encore cycle limite. Parmi les premiers exemples des attracteurs étranges mentionnés dans l'histoire du chaos, on cite l'attracteur de Lorenz, illustré par la figure (I.8).

I.3.3 Etude de comportement chaotique (l'espace de phase)

Un système dynamique est caractérisé par un certain nombre de variables d'état, qui ont la propriété de définir complètement l'état du système à un instant donné. Le comportement dynamique du système est ainsi relié à l'évolution de chacune de ces variables d'état. Cet espace est appelé l'espace de phase ou chaque point définit un état et le point associé à cet état décrit une trajectoire, appelé également une orbite.

I.3.3.1 Exposants de Lyapunov

L'évolution chaotique est difficile à appréhender car la divergence des trajectoires sur l'attracteur est rapide. Pour cette raison on 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.

L'exposant de Lyapunov se définit par :

$$\lambda(x_0) = \lim_{n\to\infty} \sup \frac{1}{n} \log(|f(n)'(x_0)|) = \lim_{n\to\infty} \sup \frac{1}{n} \sum_{j=0}^{n-1} \log(|f'(x_j)|) \quad \ldots\ldots\ldots (I.1)$$

avec $x_j = f_j(x_0)$.

où λ est l'exposant de Lyapunov.

I.3.3.2 Bifurcation

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques

de la structure d'un système dynamique. Une bifurcation survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif des propriétés d'un système telles que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents. Les valeurs des paramètres au moment du changement sont appelées valeurs de bifurcation.

Dans les systèmes dynamiques, un diagramme de bifurcation montre les comportements possibles d'un système, à long terme, en fonction des paramètres de bifurcation.

I.3.4 Classe des systèmes chaotiques

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.

I.3.4.1 systèmes chaotiques continus

Un système chaotique à temps continu est décrit par un système d'équation différentielle de forme [10] :

$$x=\boldsymbol{f}\ (t,,), \quad y=h(t,x,u), \qquad \text{(I.2)}$$

où : $\boldsymbol{f}$ est le vecteur d'état de dimension n, f: $IR^n \square IR^n$ est une fonction non linéaire qui désigne le champ de vecteur, $h:R^n \square R$ une fonction éventuellement non linéaire qui désigne le vecteur de sortie et $u \in V \subseteq \Re^p$ représente l'entrée du système. Si ce système ne dépend pas de l'entrée, on aura alors.

$$x=f(t,x) \qquad \text{(I-3)}$$

Il existe plusieurs systèmes chaotiques continus. Parmi eux, on peut citer les systèmes de Lorenz, Rössler, Bogdanov, le circuit de Chua, etc.

a. Système de Lorenz

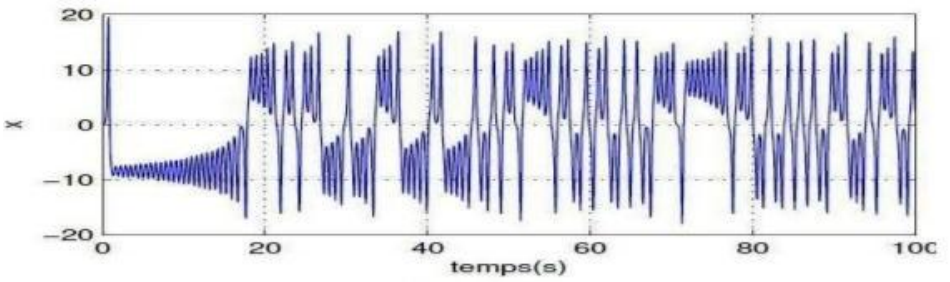
Le système de Lorenz est généré par le système d'équations suivant : [11]

$$\begin{aligned} \dot{x} &= a(y-x) \\ \dot{y} &= x(b-z)-y \\ \dot{z} &= xy-cz \end{aligned} \qquad \text{(I-4)}$$

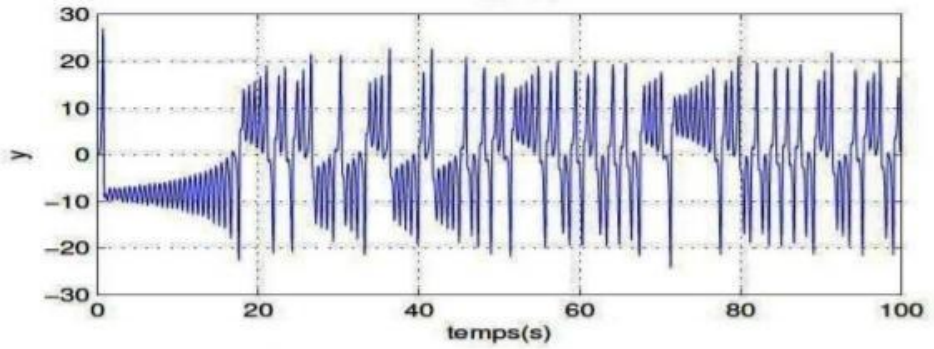
Les variables *x*, *y* et *z* représentent les états du système à chaque instant. *a*, *b*, *c* sont les paramètres du systèmes. Le système présente un comportement chaotique pour a=12, b=26, c=9 et présente un attracteur étrange en forme d'ailes de papillon.

a1. Aspect aléatoire du système de Lorenz :

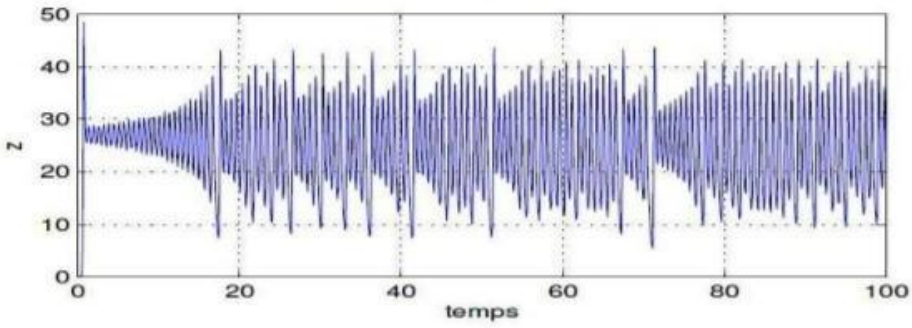
La figure (figure I.6) illustre l'aspect aléatoire des états du système (I.4)



(a) : état *x* du système de Lorenz



(b) : état *y* du système de Lorenz



(c) : état *z* du système de Lorenz

Figure I.6 Aspect aléatoire du système Lorenz.

a2.Sensibilité aux conditions initiales du système de Lorenz :

On a le cas initial:

$$\begin{cases} x_1(0)=0.100 \\ x_2(0)=0.101 \end{cases}$$

En prenant $x_1(0)$ $x_2(0)$ pour conditions initiales très proches, les évolutions des signaux x_1 et x_2 ont un comportement différent au fur et à mesure que le temps augmente, la figure (I.7), illustre les résultats obtenus.

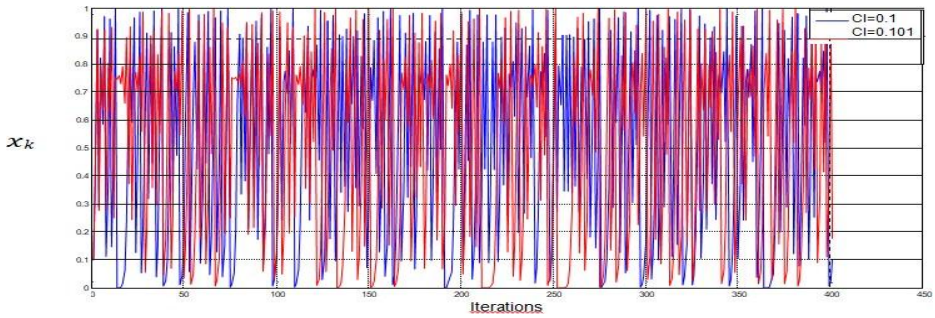


Figure I.7 Sensibilité aux conditions initiales pour le Système de Lorenz

a.3. Attracteur de Lorenz

Le système chaotique (I.4) présente une superbe attracteur étrange en forme d'ailes de papillon, représenté sur la figure (I.8). La trajectoire commençant par s'enrouler sur une aile, puis sautant pour commencer à s'enrouler sur l'autre aile, et ainsi de suite. On observe que la dynamique du système de Lorenz donné par le système (I.4) est indépendante du temps t, par conséquent ce type de système est qualifié d'être autonome.

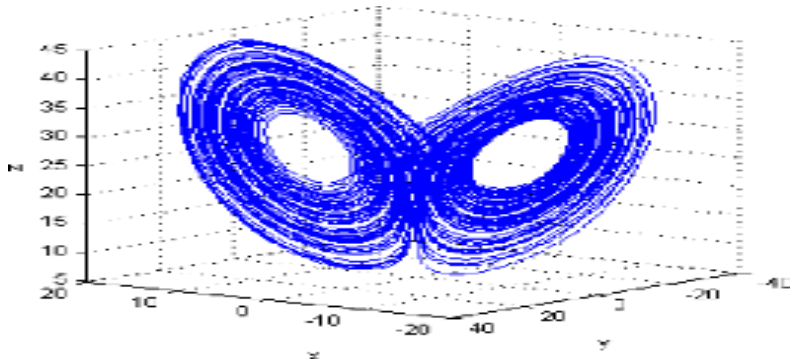


Figure I.8 Attracteur de Lorenz

I.3.4.2 Systèmes chaotiques discrets

Un système chaotique à temps discret est décrit par un système d'équations aux différences finies, dont le modèle général est le suivant :

$$x(n+1)=(x(n),u(n)), \qquad y(n)=(x(n),u(n)) . \qquad \text{(I.5)}$$

Il existe plusieurs systèmes chaotiques discret-s. Parmi eux, on peut citer les systèmes de Hénon, Lozi, la fonction logistique, etc…

a. Fonction logistique

La fonction logistique très connue dans la théorie des systèmes non linéaires, est une application non bijective du domaine [0, 1] dans lui-même qui sert de récurrence à la suite :

$$x_{n+1} = r*x_n *(1 - x_n). \qquad \text{(I.6)}$$

Où, n= 0,1,……. dénote le temps discret, x la variable dynamique et r un paramètre réel. La dynamique de cette application correspond à un comportement très différent ; ainsi selon la valeur du paramètre r, une plus grande variété de régimes permanents se présente, parmi lesquelles on trouve, par ordre de complexité :

- Pour $0 < r < 3$, le système possède un point fixe attractif, qui devient instable lorsque r = 3.
- Pour $3 < r < 3.57\ldots$, le système évolue périodiquement de période r^n, avec n un entier qui tend vers l'infini lorsque r tend vers 3.57…
- Pour r =4, le système évolue de manière chaotique.

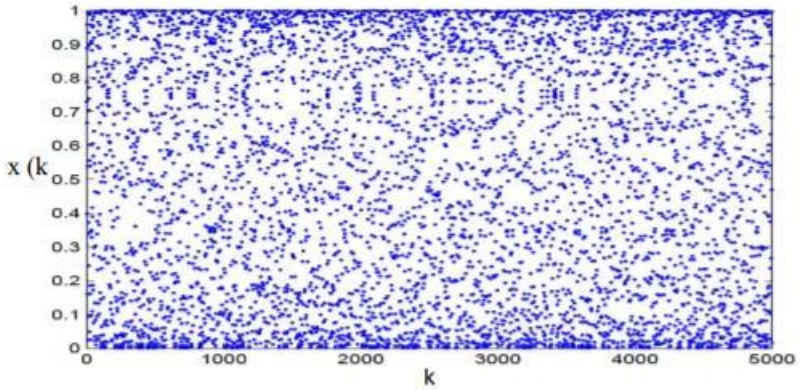


Figure I.9 Trajectoire de la fonction logistique

a.1 Aspect aléatoire de la fonction logistique

La figure suivante illustre l'aspect aléatoire du système (I.6) pour $r = 4$. Il est alors impossible de discerner à l'œil nu cette trajectoire de celle d'une variable aléatoire.

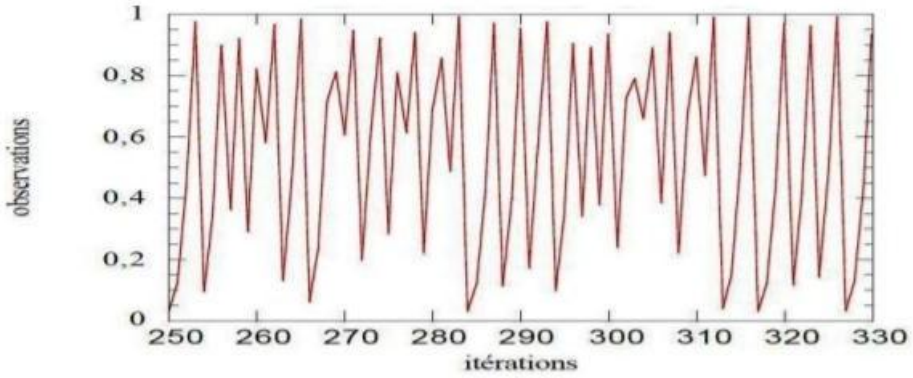


Figure I.10 application logistique pour r=4

a.2. sensibilité aux conditions initiales de la fonction logistique

On a le cas initial:

$$\begin{cases} x_1(0) = 0.8 \\ x_2(0) = 0.\ 0.8000001 \end{cases}$$

En prenant $x_1(0)$ $x_2(0)$ pour conditions initiales très proches, les évolutions des signaux x_1 et x_2 possèdent un comportement différent au fur et à mesure que le temps augmente, on a obtenu les résultats suivants, figure I.12.

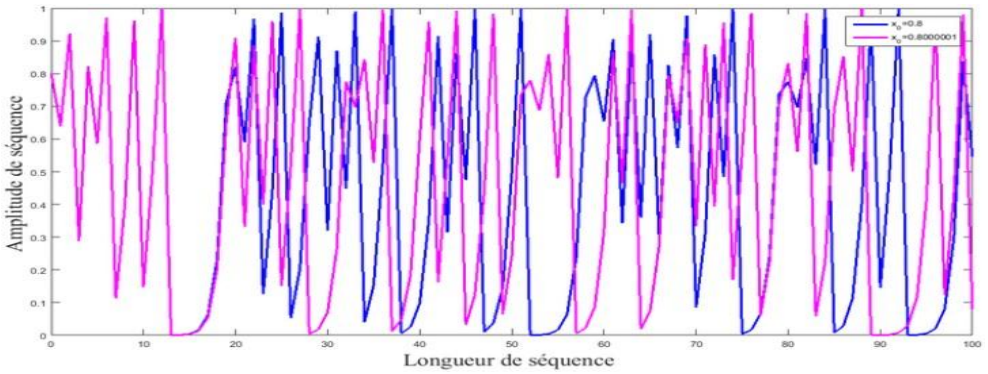


Figure I.11 Sensibilité aux conditions initiales de la fonction logistique

a.3 Exposant de Lyapunov de la fonction logistique

Après calcul de l'exposant de Lyapunov de fonction logistique :

$$\lambda = \lim_{k\to} \quad \frac{1}{k} \sum_{i=0}^{k-1} \ln|(r - \quad r\ x_i)| \qquad (I.7)$$

λ est appelé exposant de Lyapunov , il représente le taux de divergence .

-Pour $\lambda \leq 0$: la trajectoire de l'évolution du système peut tendre vers un point fixe, avoir un comportement périodique ou quasi-périodique.

-Pour $\lambda > 0$: le système est chaotique.

a.4 Diagramme de bifurcation pour la fonction logistique :

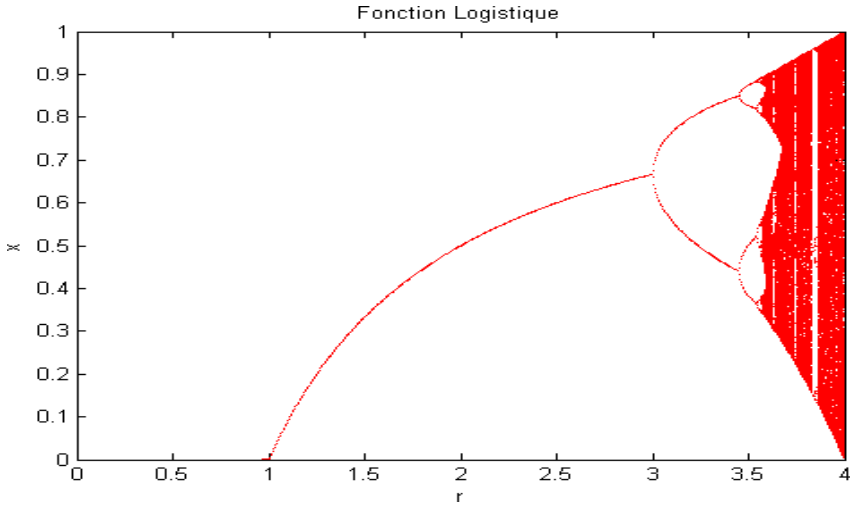
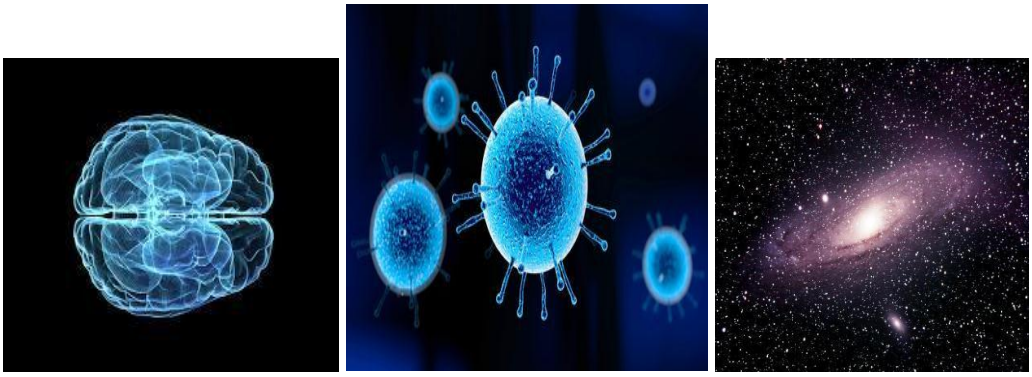


Figure I.12 Diagramme de bifurcation de la fonction logistique

I.4 Image numérique

Une image est une représentation planaire d'une scène ou d'un objet. Elle est issue du contact des rayons lumineux provenant des objets formants la scène avec un capteur (caméra, scanner, rayons X, …). L'image est considérée comme un ensemble de points auxquels sont affectés des grandeurs physiques (luminance, couleur).



(a) (b)

Figure I.13. (a) image médicale,(b) image biologique ,(c) image astronomique

*

I.4.1 Définitions et termes

I.4.1.1 Image Numérique

Une image numérique est une image (dessin, icône, photographie...) créée, traitée, stockée sous forme binaire (suite de 0 et de 1)[12].

I.4.1.2 Édition d'images numériques

L'édition d'images numériques est la manipulation d'images numériques à l'aide d'un logiciel existant, tel que " Adobe Photoshop " ou " Corel Paint ".

I.4.1.3 Traitement d'images numériques

Le traitement d'images est une discipline de l'informatique et des mathématiques appliquées qui étudie les images numériques et leurs transformations, dans le but d'améliorer leur qualité ou d'en extraire de l'information.

I.4.1.4 Pixel

Le pixel représente le plus petit élément constitutif d'une image numérique [13].
Une image numérique est constituée d'un **ensemble de points** appelés **pixels** (abréviation de **PIC**ture **El**ement) pour former une image. L'ensemble de ces pixels est contenu dans un tableau à deux dimensions constituant l'image :

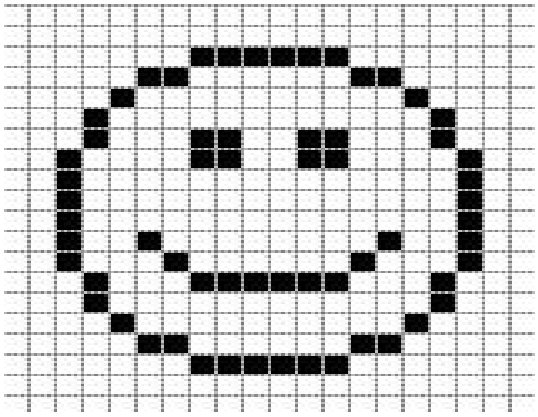


Figure I.14 tableau à deux dimensions de l'image

I.4.1.5 Définition

On appelle **définition** d'une image **le nombre de pixels composant une image**: c'est le nombre de colonnes de l'image que multiplie son nombre de lignes [12]. par exemple : Une image possédant 10 colonnes et 11 lignes aura une définition de 10 x 11 c'est à dire 110 pixels.

I.4.1.6 Résolution d'une image

La résolution d'affichage d'une image numérique est le nombre de pixels affichés par unité de longueur : elle est couramment exprimée en pixels par pouce[2] (en français ppp, en anglais : dpi pour Dots Per Inch).

Résolution (en ppp) = nombre de pixels (en pixels) / dimension (en pouces)

I.4.2 Types des images

II existe différentes types d'image selon le nombre de bit sur lequel est codée la valeur de chaque pixel [14].

I.4.2.1 Image monochrome (binaire)

C'est le plus simple type d'image où chaque pixel peut prendre uniquement la valeur noire ou blanche (chaque pixel est codé sur un seul bit) . C'est typiquement le type d'image que l'on utilise pour scanner du texte quand celui-ci est composé d'une seule couleur.

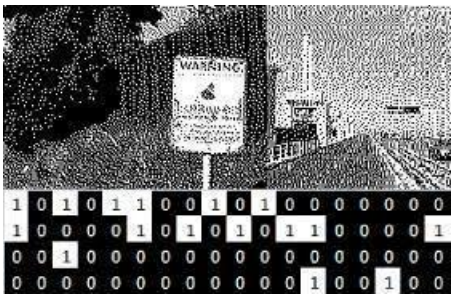


Figure I.15 Image Monochrome

I.4.2.2 Image en niveaux de gris

Le niveau de gris est la valeur de l'intensité lumineuse à un point. La couleur du pixel peut prendre des valeurs allant du noir au blanc en passant par un nombre fini de niveaux intermédiaires. Donc pour représenter les images à niveaux de gris (figure I.17), on peut attribuer à chaque pixel de l'image une valeur correspondante à la quantité de lumière renvoyée. Cette valeur peut être comprise par exemple entre 0 et 255. Chaque pixel n'est donc plus représenté par un bit, mais par un octet.

[2] 1pouce=2.54cm

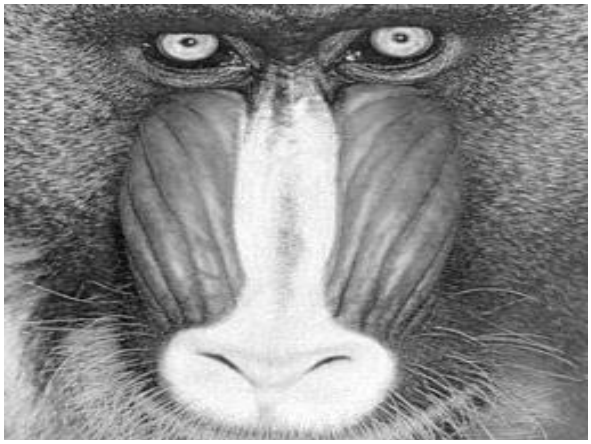


Figure I.16 Image en niveau de gris

I.4.2.3 Image en couleurs

Même s'il est parfois utile de pouvoir représenter des images en noir et blanc ou en niveau de gris, les applications multimédias utilisent le plus souvent des images en couleurs (figure I.18). La représentation des couleurs s'effectue de la même manière que les images en niveaux de gris avec cependant quelques particularités. En effet, il faut tout d'abord choisir un modèle de représentation.

Figure I.17 Image en couleur

- Modèle de couleur RVB

Le modèle RVB est un modèle de couleur additif qui utilise les couleurs primaires de la lumière : rouge, vert, et le bleu, de sorte que toute couleur peut être obtenue en combinant différentes quantités de ces trois couleurs primaires.

Une couleur dans l'espace couleur RVB est définie par trois valeurs numériques (un tuple) qui spécifient la quantité de rouge, de vert et de bleu qui composent la couleur spécifiée.

L'origine se trouve à <0, 0, 0> correspond à la couleur noir tandis que le coin opposé se trouve à <1, 1, 1> et correspond à la couleur blanche.

La ligne reliant le noir pur et le blanc pur dans l'espace couleur RVB est appelée échelle de gris car tout point situé sur cette ligne est une nuance de gris.

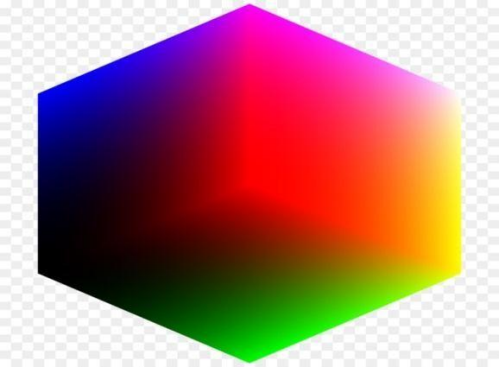


Figure I.18 L'espace de couleurs RVB

I.4.2.4 Images indexées

Les images couleurs indexées stockent pour chaque pixel un numéro de couleur (son index), qui fait référence à une couleur stockée séparément dans une palette.

L'intérêt de ces images est de réduire l'espace de stockage nécessaire, au prix d'une perte de qualité par rapport aux images en vraies couleurs. Par exemple, une image en 256 couleurs indexées occupera sensiblement la même place qu'une image en 256 niveaux de gris (la place occupée par la palette est négligeable par rapport à la taille de l'image).

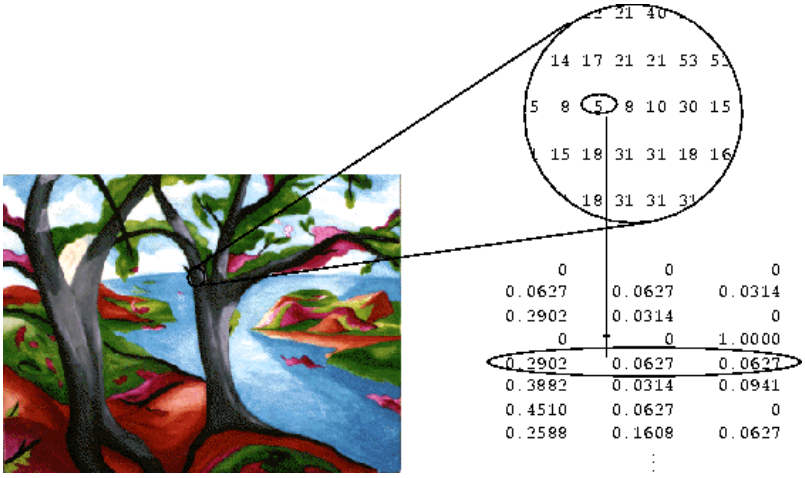


Figure I.19 Image Indexée

I.4.3 Formats standards d'image

Plusieurs formats d'image existent, nous présentons ci-dessus les plus utilisés [15].

I.4.3.1 BMP (Windows Bitmap)

C'est le format actuel utilisé par Windows. Il produit des images de bonne qualité et est reconnu par de nombreuses applications. C'est le format le plus utilisé, par contre, il est extrêmement volumineux lorsqu' il utilise le codage en « true colors ».

I.4.3.2 PCX (PiCture eXchange)

Le format défini par Paintbrush. Il accepte les modes de couleur, indexés, niveaux de gris et le noir et blanc.

I.4.3.3 GIF(Graphic Interchange Format)

Créé par Compuserve, utilise aussi le codage RGB, mais le format GIF n'utilise pas toutes les 16 millions de couleurs. Il prend les 256 couleurs les plus courantes pour réaliser l'image au format GIF. Cela permet une bonne compression et un affichage rapide de l'image [15].

I.4.3.4 JPG ou JPEG (Joint Photographique Experts Group)

Créé par un consortium industriel, ce format très utilisé sur Internet, permet d'afficher les images en mode 16 millions de couleurs. Il est conçu pour réduire le plus possible la taille des fichiers graphiques en acceptant éventuellement de légères pertes de qualité. Il est destiné à la transmission rapide d'information. Ces résultats de compression sont extraordinaires.

I.4.3.5 TIFF (Tag Image File Format)

C'est un format d'excellente qualité, mais qui présente des problèmes de compatibilité du fait d'une multiplicité de version. Il existe aussi une version compressée qui fournit des fichiers très compacts sans perte notoire de qualité. Ce format est compatible avec d'autres plates-formes (macintosh). Il est utilisé par les professionnels.

I.5 Conclusion

Ce chapitre avait comme objectif l'introduction de quelques notions élémentaires des trois sujets sur lesquels porte notre travail: la cryptographie, le chaos et l'image.

Dans la section I.2 une vue sur la cryptographie est donnée. Nous avons commencé par donner quelques terminologies nécessaires à la compréhension du sujet. Puis nous avons cité les deux modes de chiffrements en présentant quelques algorithmes.

La section I.3 avait comme objectif d'éclairer quelques notions de bases liées aux systèmes dynamiques chaotiques. Nous avons commencé par définir les systèmes dynamiques, ensuite nous avons présenté quelques définitions et propriétés des systèmes chaotiques tel que : la non-linéarité, le déterministe, la sensibilité aux conditions initiales. Et finalement nous avons détaillé quelques exemples des systèmes chaotiques en temps continu et discret tel que : système de Lorenz.

Dans la section I.4, nous avons présenté les types d'images existants, ainsi que les formats les plus utilisés.

Le chapitre suivant présente un état de l'art des systèmes chaotique de cryptage d'images, pour ce faire nous essayons de les classer en fonction du type de système chaotique utilisé.

Chapitre II

Etat de l’art sur les systèmes de cryptage chaotique

II.1 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.

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

Dans ce chapitre, nous allons tourner autour de ces méthodes. Tout d'abord, nous présenterons la structure générale d'un système de cryptage chaotique d'images qui se base sur le principe de confusion et diffusion, nous présentons ensuite les principales métriques utilisées pour évaluer les performances et la sécurité de ces cryptages. La section II.6 a l'objectif de présenter notre classification des systèmes de cryptage chaotique selon le type des systèmes chaotiques utilisé dans le cryptage, tout en présentant quelques travaux associés à chaque classe. Nous terminons le chapitre un tableau qui illustre leurs résultats de quelques paramètres d'analyse de sécurité obtenus.

II.2 Concept de confusion et diffusion

En cryptographie, la confusion et la diffusion sont deux propriétés fondamentales d'un chiffrement sécurisé.

- La **confusion** signifie que chaque bit du texte crypté doit dépendre de plusieurs parties de la clé, tout en cachant les relations entre les deux. Alors, Le but de la confusion est de masquer toute liaisons existante entre le texte en claire, le texte crypté et la clé.
- La **diffusion** est une propriété où la redondance statistique dans un texte en clair est dissipée dans les statistiques de texte crypté.

Ces deux propriétées rendent la cryptanalyse trés difficile. Plus précisément, un cryptosystème qui possède une bonne confusion et une bonne diffusion résiste aux différentes attaques.

II.3 Cryptage Chaotique des images

Les schémas de cryptage d'images proposés sont basés sur deux principes cités dans la section précédente : la confusion et la diffusion, où la confusion est simplement un réarrangement des pixels, en d'autres termes, elle est basée sur le principe du changement de

position des pixels, alors que le principe de diffusion change la valeur des pixels. La structure générale du schéma de cryptage d'image est illustrée à la Figure II.1.

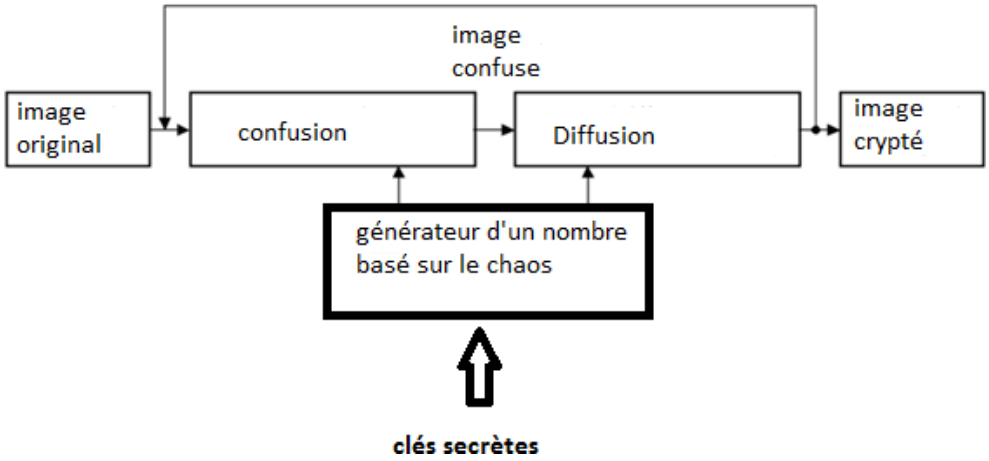


Figure II.1 Structure générale d'un schéma de cryptage d'image chaotique

II.4 Analyse de la sécurité et des performances

II.4.1 Analyse clé

II.4.1.1 Analyse de l'espace clé

Le nombre total de clés possibles qu'un attaquant doit essayer de casser pour un système de cryptage est appelé **espace clé** et il doit être suffisamment grand pour empêcher les attaques par force brute. Pour qu'un algorithme soit résistant aux attaques par force brute, l'espace de clé doit être supérieur à 2^{100} [16].Cet espace est calculé en multipliant simplement l'espace total de chaque clé individuelle comme indiqué dans la formule suivante [17].

$$S \quad \prod_{i=1}^{K} Sk_i \qquad (II.1)$$

Où,**S** est l'espace de clé total et $\mathbf{Sk_i}$ est l'espace de l'^{ième} clé.

Il convient de noter que l'espace clé de chaque clé individuelle dépend principalement de la précision de la clé. Un nombre en double précision est représenté sur 48 bits (6 octets), ce qui signifie que l'espace total est de 2^{48}, ce qui est approximativement égal à 10^{14}.

A titre d'exemple, un système qui contient 2 clés différentes, k1 tombant dans la plage [0,5] et l'autre tombant dans la plage [0,1], l'espace clé total du système est :

$$S= 5*2^{48}*1*2^{48} =2^{2.32}*2^{96} =2^{98.32}$$

II.4.1.2 Sensibilité des clés

Un schéma de chiffrement efficace est très sensible aux modifications des clés de chiffrement et de déchiffrement. En appliquant une modification mineure à la clé de cryptage, la deuxième image cryptée devrait être assez différente de la première image cryptée. De même, s'il existe une petite différence entre les clés de chiffrement et de déchiffrement, l'image cryptée ne peut pas être décryptée correctement**.**

Généralement, une métrique nommée Cipher-text Difference Rate (CDR) est utilisée afin d'étudier la sensibilité aux clés secrètes. Le CDR est calculé à l'aide de la formule suivante [17]:

$$CDR = \frac{Diff(y,y1)+Diff(y,y2)}{2*W*H}*100\%.$$

$$Diff(A,B)=\sum_{i=0}^{W-1} Diff(A(i,j), B(i,j)$$

$$Diff(A(i,j), B(i,j) = \begin{cases} 1, & Si\ A(i,j) \neq B(i,j) \\ 0, & Sinon \end{cases} \qquad (II.2)$$

Tel que : Y= C(l,K), Y1 = C(I, K + ΔK) , Y2 = C (I, K - ΔK)

Où,

- C représente la fonction de cryptage, Y est une image cryptée de l'image en clair I utilisant une clé K.
- Y1 et Y2 sont deux images cryptées de la même image I avec un petit changement de clé (respectivement +ΔK et -ΔK).
- Diff (A, B) est la somme des différents pixels de deux images données A et B.

II.4.2 Analyses statistiques

II.4.2.1 Analyse de l'entropie de l'information

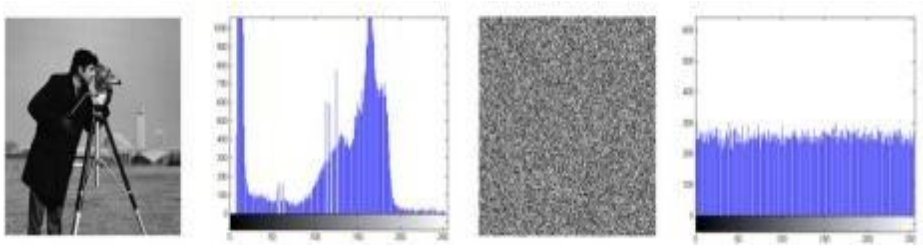
L'entropie d'un système est interprétée comme un indicateur pour mesurer et caractériser la quantité de désordre dans le système. Ce dernier peut mesurer la distribution des valeurs des pixels dans l'image. Une bonne image cryptée a une entropie très proche de 8. En d'autres termes, il représente les informations nécessaires pour définir les états du système. L'entropie est définie comme :

$$H(M) = \sum_{i=0}^{2n-1} (mi)g2 \qquad \frac{1}{(mi)} \qquad (II.3)$$

II.4.2.2 Analyse d'histogramme (attaque statistique)

Un histogramme d'image représente le transport des pixels de l'image en traçant le nombre de pixels à chaque niveau d'échelle de gris. La redondance du texte en clair doit être cachée dans la distribution du texte chiffré et cette distribution doit logiquement être uniforme [19].

Donc l'analyse d'histogramme est le moyen le plus populaire et le plus efficace pour tester l'uniformité des valeurs (invulnérabilité aux attaques statistiques). Ainsi, pour une image cryptée, il est nécessaire qu'une image cryptée ait une répartition uniforme des valeurs de pixels sur les deux axes [19], autrement dit un bon chiffrement doit produire des images cryptées ayant un histogramme uniforme autant que possible, voir figure II.2.



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

Figure II. 2(a) image en clair, (b) histogramme d'image en clair, (c) images cryptées, (d) histogramme d'image cryptée.

II.4.2.3 Analyse de corrélation

Une forte corrélation existe entre les pixels adjacents dans chaque image en clair. Un algorithme de chiffrement sécurisé devrait produire des images cryptées dont la corrélation des pixels adjacents est très faible. Habituellement, 1 000 ou 2 000 pixels sont sélectionnés pour l'analyse de corrélation et la corrélation est calculée dans les directions horizontale, verticale et diagonale. Le coefficient de corrélation est calculé à l'aide de la formule suivante :

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}} \qquad \text{(II. 4)}$$

tel que :

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=0}^{N}(x_i - E(x))(y_i - E(y))$$

$$D(x) = \frac{1}{N}\sum_{i=0}^{N}(x_i - E(x))^2,\ E(x) = \frac{1}{N}\sum_{i=0}^{N} x_i$$

Où, x et y représentent les valeurs d'intensité de deux pixels adjacents. N est le nombre de pixels dans l'échantillon d'analyse actuel. D(x) et E(x) représentent la variance et l'espérance de l'échantillon actuel.

La valeur de corrélation se situe dans la plage [-1,1] : 0 représente aucune corrélation et 1 représente une corrélation complète (les images sont identiques), généralement, une corrélation jusqu'à 0,8 représente une forte corrélation.

De manière générale, plus la valeur de corrélation entre les pixels adjacents sont petites, meilleures sont les performances de l'algorithme de cryptage [21].

II.4.2.4 Analyse de robustesse

Les images sont inévitablement contaminées par le bruit ou subissent des pertes de données lors du stockage et de la transmission sur les réseaux, en particulier lors de l'utilisation de protocoles peu fiables (tels que UDP).

Les images cryptées doivent avoir la capacité de résister aux attaques qui causent de perte de données, et afin de tester cette capacité, la capacité de restaurer l'image après avoir appliqué différents niveaux de bruit ou de perte de données, la métrique du rapport signal sur bruit (PSNR) est généralement utilisé, cette métrique est calculée par la formule suivante :

$$PSNR = 10.log\frac{255^2}{MSE}\ (dB) \quad \text{(II. 5)}$$

L'erreur quadratique moyenne (MSE) est utilisée pour analyser l'effet d'avalanche. L'effet d'avalanche indique que le changement de l'image en clair ou de la clé provoque un changement considérable dans l'image cryptée correspondante. La MSE est calculée pour deux images numériques et correspond à l'erreur quadratique cumulée entre elles. Mathématiquement, il peut être calculé comme :

$$\text{MSE} = \frac{1}{W*H}\sum_{i=0}^{W-1}\sum_{j=0}^{H-1}(Ip(i,j) - Id(i,j))^2$$

Où, Ip et Id sont respectivement l'image en clair et l'image décryptée.
Plus la valeur PSNR est élevée, plus la capacité de restauration de l'image décryptée est élevée. En général, il est très difficile de différencier l'image d'origine réelle et l'image décryptée lorsque le PSNR est supérieur à 35 dB.

II.4.2.5 Analyse de vitesse

Le temps d'exécution d'un algorithme de chiffrement est aussi important que son niveau de sécurité, en particulier pour les applications en temps réel. Donc un algorithme de chiffrement est efficace lorsqu'il utilise moins de ressources et a un temps de calcul minimal.
Deux métriques sont couramment utilisées pour tester les performances de vitesse d'un chiffrement, le débit de chiffrement (ET) et le nombre de cycles par octet (NCPB), les deux sont exprimés dans la formule suivante [19] :

$$\text{ET} = \frac{\text{taille de l'image (octet)}}{\text{temps de cryptage (s)}} \quad \text{(II.6)}$$

$$\text{NCPB} = \frac{vitesse\ CPU}{ET} \quad \text{(II.7)}$$

II.4.2.6 Résistance aux attaques différentielles

Dans un algorithme de cryptage d'image sécurisé, un seul changement de pixel dans l'image en clair devrait entraîner un changement significatif dans l'image cryptée correspondante.

Lorsqu'une image cryptée est modifiée de manière significative, cela montre que le schéma proposé est résistant aux attaques différentielles. Pour étudier l'effet du changement d'un pixel sur une image cryptée, les paramètres couramment utilisés sont : (i) le nombre de taux de changement de pixels (NPRC) et (ii) l'intensité de changement moyenne unifiée (UACI) [22], [21]. L'expression mathématique du NCPR est :

$$\text{NPRC} = \frac{\sum_{i,j} D(i,j)}{M*N} * 100\% \qquad \text{(II.8)}$$

Et l'expression mathématique pour UACI est :

$$\text{UACI} = \frac{1}{M*N} \left[\sum_{i,j} \frac{|E1(i,j) - E2(i,j)|}{255} \right] * 100\% \qquad \text{(II.9)}$$

Où :M et N représentent la largeur et la hauteur de l'image respectivement.
E1, E2 sont deux images cryptées différentes de la même image en clair.

Pour un pixel à la position (i; j), **si** E1(i; j) GE2(i; j) **alors** D(i; j) = 1 ;
sinon D(i; j) = 0.

II.5 Classification des systèmes de cryptage d'images basés sur le chaos

Nous pouvons classer les systèmes chaotiques existants en fonction du type de systèmes chaotiques utilisés pour le chiffrement en deux classes comme suit :

- Le cryptage basé sur des **"systèmes chaotiques purs",** c'est-à-dire que le système se base uniquement sur les systèmes chaotiques dans le processus de chiffrement/déchiffrement. Selon la façon d'utilisation de ces systèmes chaotiques, nous pouvons distinguer : systèmes chaotiques homogènes, systèmes chaotiques améliorés, systèmes chaotiques en cascade, et systèmes chaotiques hétérogènes.

- Le cryptage basé sur des **"systèmes hybrides"**, autrement dit : ce sont les systèmes qui combinent les systèmes chaotiques avec les systèmes non chaotiques.

II.5.1 Systèmes chaotiques purs

II.5.1.1 Systèmes chaotiques homogènes

Les systèmes chaotiques homogènes sont des systèmes qui exploitent un ou plusieurs systèmes chaotiques du même type. Le chiffrement qui exploite la carte logistique 1-D ou deux cartes sinusoïdales distinctes (dans ce cas, une carte est utilisée en utilisant des clés différentes.) sont des exemples de systèmes chaotiques homogènes.

Les auteurs dans [23], ont proposé un nouvel algorithme de cryptage d'image à base de la carte logistique tridimensionnelle, définit par les équations suivantes :

$$x_{i+1} = \alpha x_i (1-x_i) + \beta y_i^2 x_i + \gamma z_i^3 \qquad \text{(II.10)}$$

$$y_{i+1} = \alpha y_i (1-y_i) + \beta z_i^2 y_i + \gamma x_i^3 \qquad \text{(II.11)}$$

$$z_{i+1} = \alpha z_i (1-z_i) + \beta x_i^2 z_i + \gamma y_i^3 \qquad \text{(II.12)}$$

Le schéma général du processus de chiffrement est illustré par la figure II.3, dont les étapes principales sont :

E1. Lire une image en clair ($P_{a \times b \times c}$), obtenir la taille de P. Soit N = a*b,

- Extraire : image_clair_Rouge $PR_{a\times b\times 1}$, enregistrer dans $PR_{(N)}$
  image_clair_Vert$PG_{a\times b\times 2}$, enregistrer dans $PG_{(N)}$,
  image_clair_bleu$PB_{a\times b\times 3}$, enregistrer dans $PB_{(N),P}$
- Initialiser les valeurs : x(0) = 0,100001, y(0) = 0,100001 et z(0) = 0,100001 ;

E2.Définir les valeurs α,β,γ dans les équations(10), (11) et (12) et itérer N pour obtenir les différents tableaux $X_{(N)}$, $Y_{(N)}$ et $Z_{(N)}$;

E3.Etape de diffusion : $CDR_{(N)} = X_{(N)} * PR_{(N)}$, $CDG_{(N)} = Y_{(N)} * PG_{(N)}$, $CDB_{(N)} = Z_{(N)} * PB_{(N)}$;

E4.Etape de confusion : Changer $X_{(N)}$, $Y_{(N)}$ et $Z_{(N)}$ en [0,255], obtenir $SX_{(N)}$,$SY_{(N)}$ et $SZ_{(N)}$, nous pouvons obtenir $CCR_{(N)} = SX_{(N)} \oplus CDR_{(N)}$, $CCG_{(N)} = SY_{(N)} \oplus CDG_{(N)}$, $CCB_{(N)} = SZ_{(N)}\ CDB_{(N)}$;

E5. Changer $CCR_{(N)}$, $CCG_{(N)}$ et $CCB_{(N)}$ en $C_{a\times b\times c}$, qui crypte chaque élément de la matrice ($P_{a\times b\times c}$) en utilisant le tableau de clés $X_{(N)}$, $Y_{(N)}$ et $Z_{(N)}$, en mélangeant le résultat de la confusion de l'image originale ($P_{a\times b\times c}$) ($X_{(N)}$, $Y_{(N)}$ et $Z_{(N)}$) avec le résultat de la diffusion de l'image originale ($P_{a\times b\times c}$) ($X_{(N)}$, $Y_{(N)}$ et $Z_{(N)}$), l'image résultante est l'image cryptée $C_{a\times b\times c}$.

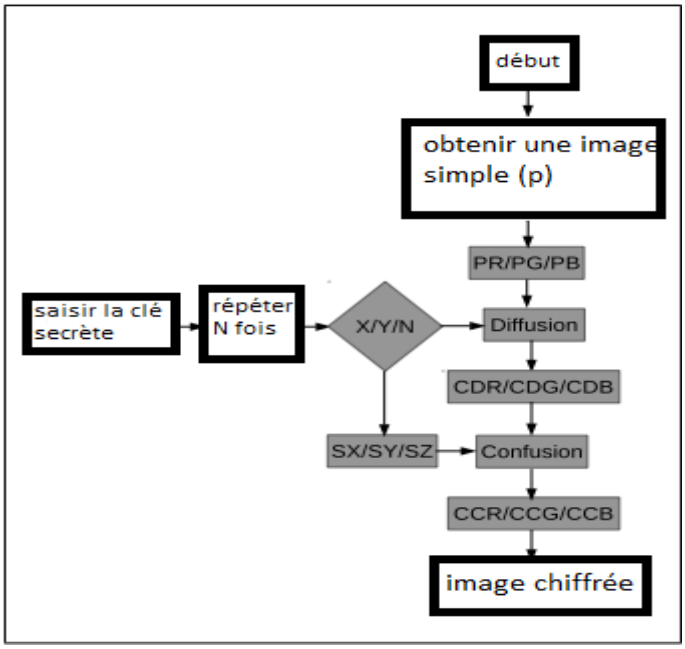


Figure II.3 Principe du cryptage de [23].

Le système de cryptage d'image introduit dans[24], est basé sur des cartes chaotiques de type 2D-3D,Soit la carte Cat 2D avec deux paramètres de contrôle positifs et les coordonnées des positions des pixels dans l'image en clair. Soit q = {(x1, y1) | x1, y1 = 1, 2, 3, . . ., P}, tel que :

$$X1' = (x1+my1) \bmod (p)$$

$$Y1' = (nx1+ (mb+1)\ y1\ ) \bmod(p)$$

Où,

(x1 , y1) représentent la position des pixels dans l'image en clair.

(x1', y1') représentent la nouvelle position des pixels lors de l'application de la carte Cat 2D.

m, n sont des nombres positifsqui représente le paramètre de contrôle,

P représente la largeur ou la hauteur de l'image en clair.

Comme la carte logistique est considérée comme la fonction chaotique la plus simple, elle est donc définie par l'équation (II. 13):

$$x_{n+1} = rx_n\,(1-x_n) \qquad \text{(II.13)}$$

L'équation montre un comportement chaotique lorsque $0<x_n<1$ et $\lambda=4$. Une carte logistique en 3 dimensions est utilisée. Les équations sont les suivantes :

$$x_{i+1} = \lambda\, x_i\,(1-x_i) + \beta y_i^2\, x_i + \alpha z_i^3$$

$$y_{i+1} = \lambda\, y_i\,(1-y_i) + \beta z_i^2\, y_i + \alpha x_i^3$$

$$z_{i+1} = \lambda\, z_i\,(1-z_i) + \beta x_i^2\, z_i + \alpha y_i^3$$

Les équations exposées ci-dessus ont de bonnes caractéristiques chaotiques lorsque $3{,}53<\lambda<3{,}81$, $0<\beta<0{,}022$, $0<\alpha<0{,}015$ et x,y,z prennent les valeurs entre [0, 1].

Les principales étapes ci-dessous illustrent l'algorithme de cryptage d'image, illustré par la figure II.4 :

- Lire l'image couleur (M) .
- Diviser l'image (M) en composants essentiels R ,V, B.
- Convertisser la valeur de couleur pour chaque composant en tableau 1D (MR, MG, MB).
- Générer 3 clés (KR, KG, KB) en utilisant des cartes logistiques 3D.
- Crypter (MR , MG, MB) avec la clé respective (KR, KG, KB) .
- Convertir le résultat de l'étape précédente pour chaque composant en tableau 2D.
- Le résultat de cette étape est une image cryptée (IE).

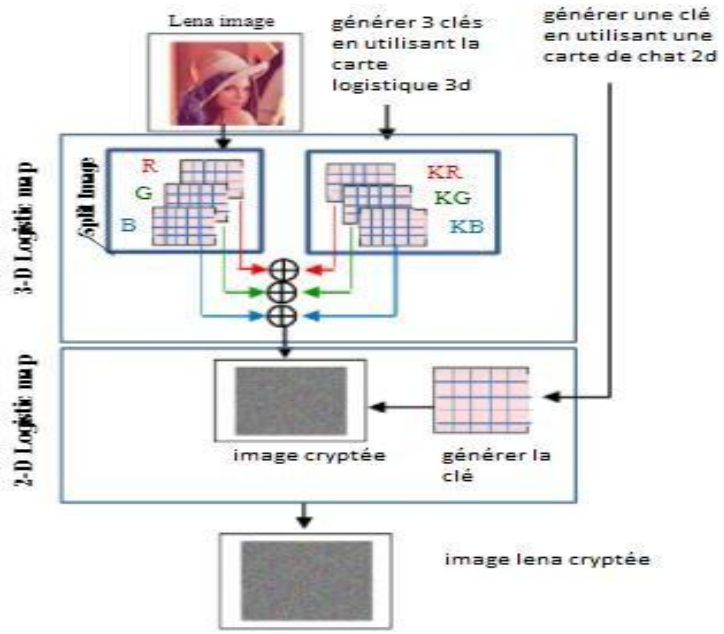


Figure II.4 Principe de cryptage définit dans [24]

II.5.1.2 Systèmes chaotiques améliorés

Dans cette classe, un nouveau système chaotique est définit en améliorant l'intervalle des valeurs chaotiques (Figure II.5). Un exemple illustratif de cette classe, est le travail de [25]. Les

auteurs ont proposé un nouvel algorithme de cryptage d'image, en utilisant une nouvelle fonction chaotique LTS Logistic Tent System définit par :

$$X_{n+1} = \mathcal{A}_{\mathcal{LT}}(r, X_n) = (\mathcal{L}(r, X_n) + \mathcal{T}((4-r), X_n)) mod\ 1$$
$$= \begin{cases} (rX_n(1-X_n) + (4-r)X_n/2) mod\ 1 & X_i < 0.5 \\ (rX_n(1-X_n) + (4-r)(1-X_n)/2) mod\ 1 & X_i \geq 0.5 \end{cases}$$

Son diagramme de bifurcation est le suivant :

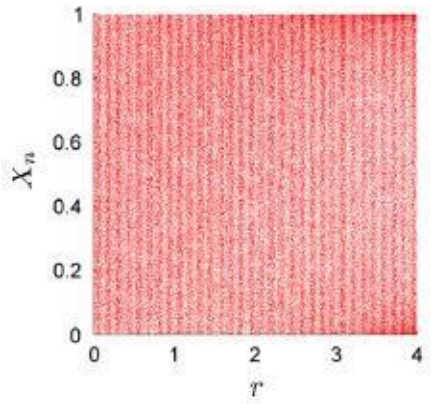


Figure II.5 Diagramme de bifurcation de la fonction LTS.

L'algorithme proposé est illustré à la figure (6), il se Chaque cycle de déroule en 4 cycles. Le cryptage comprend cinq étapes : l'insertion aléatoire de pixels, la séparation des lignes, la substitution 1D, la combinaison des lignes et la rotation de l'image. L'algorithme insère d'abord un pixel aléatoire au début de chaque ligne de l'image d'origine, sépare chaque ligne en une matrice de données 1D, applique un processus de substitution pour modifier les valeurs de données dans chaque matrice 1D, combine toutes les matrices 1D dans une matrice de données 2D en fonction de leurs positions de ligne dans l'image en clair, puis fait pivoter la matrice 2D de 90 degrés dans le sens inverse des aiguilles d'une montre. La répétition de ce processus quatre fois permet d'obtenir l'image cryptée finale.

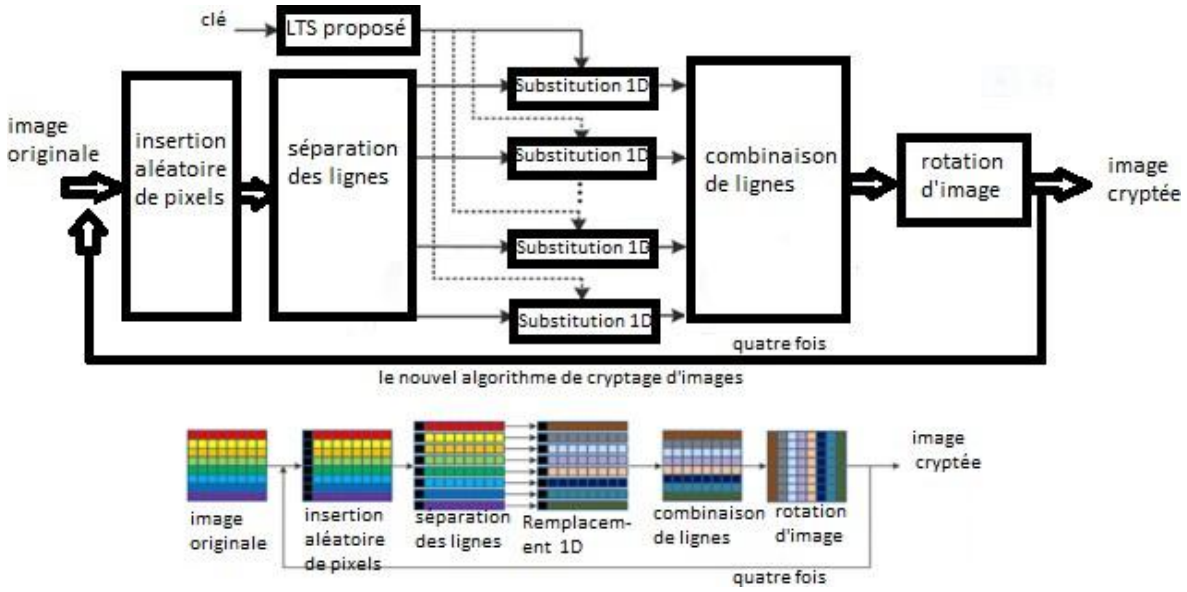


Figure II.6 Structure général du principe proposé dans [25]

Un autre travail qui se base sur le même principe est celui illustré dans [26]. Dans ce travail, une nouvelle carte chaotique qui peut être considérée comme une croissance 2D de la carte logistique traditionnelle. Cette carte est définit par l'équationII.14, la position d'origine (x_n, y_n) peut être mappée sur une nouvelle position (x_{1+n}, y_{1+n}) comme suit :

$$Y_{1+n} = b^2 x_n \,, \qquad \text{II.14}$$

$$X_{1+n} = (x_n)^2 + (y_n)^2 - a.r \,,$$

Où, les variables d'état x et y sont les séries temporelles simulées. a, b et r représentent les paramètres externes de contrôle, et n est un nombre d'itérations utilisant cette carte.

Son graphe de bifurcation est présenté sur la figure II.7(a). ce graphe a trois zones différentes : (i) la zone d'assemblage est à r ϵ [0, 0,55], (ii) la zone de bifurcation est à rϵ [0,55, 1,0] et rϵ[1.0, 1.4]est la zone de confusion. La figure II.7(b) montre le type de Lyapunov de la carte chaotique

principale proposée. Il est clairement évident que lorsque r∈ [0, 0.55] tous les valeurs de l'exposants de Lyapunov sont inférieurs ou équivalents à zéro. Lorsque r∈ [0, 0,55], les exposants de Lyapunov sont positifs.

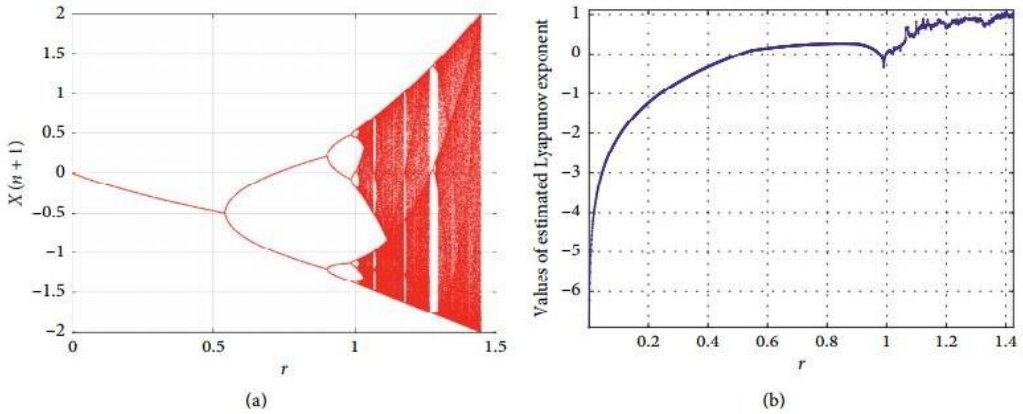


Figure -7 le diagramme de bifurcation (a) et l'exposant de Lyapunov (b) pour la carte proposée à x(0) = 0.02, y(0) = 0.02, a = 1.4, et b = 0.3.

La comparaison des propriétés de pseudo-aléatoire des deux cartes en termes de densité de distribution, d'exposant de Lyapunov et de bifurcation, démontre la supériorité du système proposée par rapport à la carte traditionnel, et par conséquent, la carte modifiée est capable de générer un meilleur flux chaotique.

II.5.1.3 Systèmes chaotiques en cascade

Un système chaotique en cascade est le résultat de la mise en cascade de deux ou plusieurs systèmes chaotiques, en d'autres termes : est le résultat de la combinaison de deux systèmes chaotiques supplémentaires dans lesquels la sortie du premier système chaotique devient l'entrée du second, et ainsi de suite. La sortie du nouveau système est ensuite utilisée pour crypter/décrypter les images.

Les auteurs de [27] ont proposé un schéma de cryptage d'image en cascade basé sur le fonctionnement du 'bit-plane operation' en utilisant PWLCM (Piece-Wise LinearChaoticMap) (II.15) et un système appelé Logistic-Adjusted-Sine map(II.16). Ensuite, ils appliquent la fonction de hachage SHA256, voir la figure II.8.

$$X_{n+1} = \begin{cases} \frac{Xn}{u} & \text{if } 0 < X_n < u \\ \frac{Xn-u}{0.5-u} & \text{if } u \leq X_n < 0.5 \\ 1\text{-}x_n & \text{if } 0.5 \leq X_n < 1 \end{cases} \qquad \text{(II.15)}$$

$$\begin{cases} x_{n+1} = \sin(\pi * r * (y_n + 3) * x_n * (1\text{-}x_n)) \\ y_{n+1} = \sin(\pi * r * (x_{n+1} + 3) * y_n * (1\text{-}y_n)) \end{cases} \qquad \text{(II.16)}$$

L'algorithme proposé consiste d'abord à appliquer le 'bit-plane operation'en utilisant le système PWLCM, cette opération non seulement confond les pixels mais les diffuse également simultanément, puis une étape de confusion en effectuant un mélange de lignes et de colonnes à l'aide de la carte 2D Logistic-Adjusted-Sine. La fonction de hachage est utilisée pour mettre à jour les clés secrètes afin de rendre le système résistant aux attaques de texte en clair connues et aux attaques de texte en clair choisi, car une petite différence dans l'image en clair modifie sa valeur de hachage et, par conséquent, modifie la clé de cryptage, cela rend le chiffrement très sensible à l'image en clair.

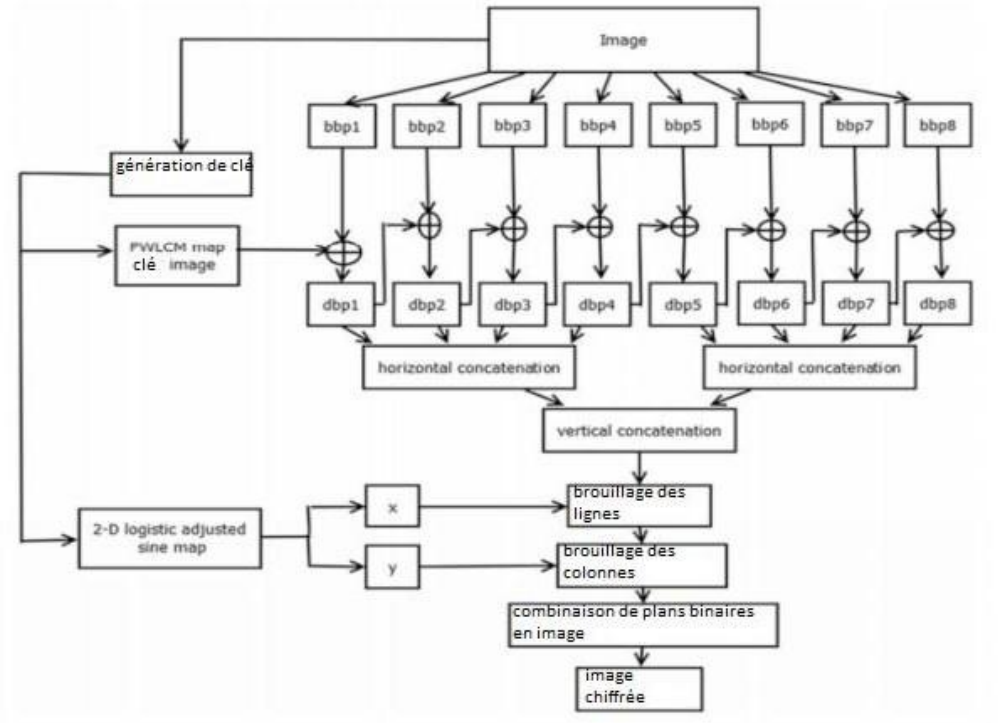


Figure II. 8. Schéma de cryptage proposé dans [27].

II.5.1.4 Systèmes chaotiques hétérogènes

Sont des Systèmes qui utilisent la sortie de différentes cartes chaotiques dans le système afin de crypter/décrypter l'image, par exemple un cryptaget qui utilise la sortie d'un système chaotique dans la phase de confusion et la sortie d'un autre système chaotique dans la phase de diffusion, etc.

Les auteurs de [28] ont proposé un nouveau système chaotique basé sur une méthode hybride du mouvement brownien des particules et certaines cartes chaotiques dynamiques discrètes pour obtenir une séquence aléatoire maximale. Ils ont supposés et défini un certain nombre de particules par rapport au temps avant d'utiliser certaines cartes chaotiques. La figure II.9, résume les principales étapes :

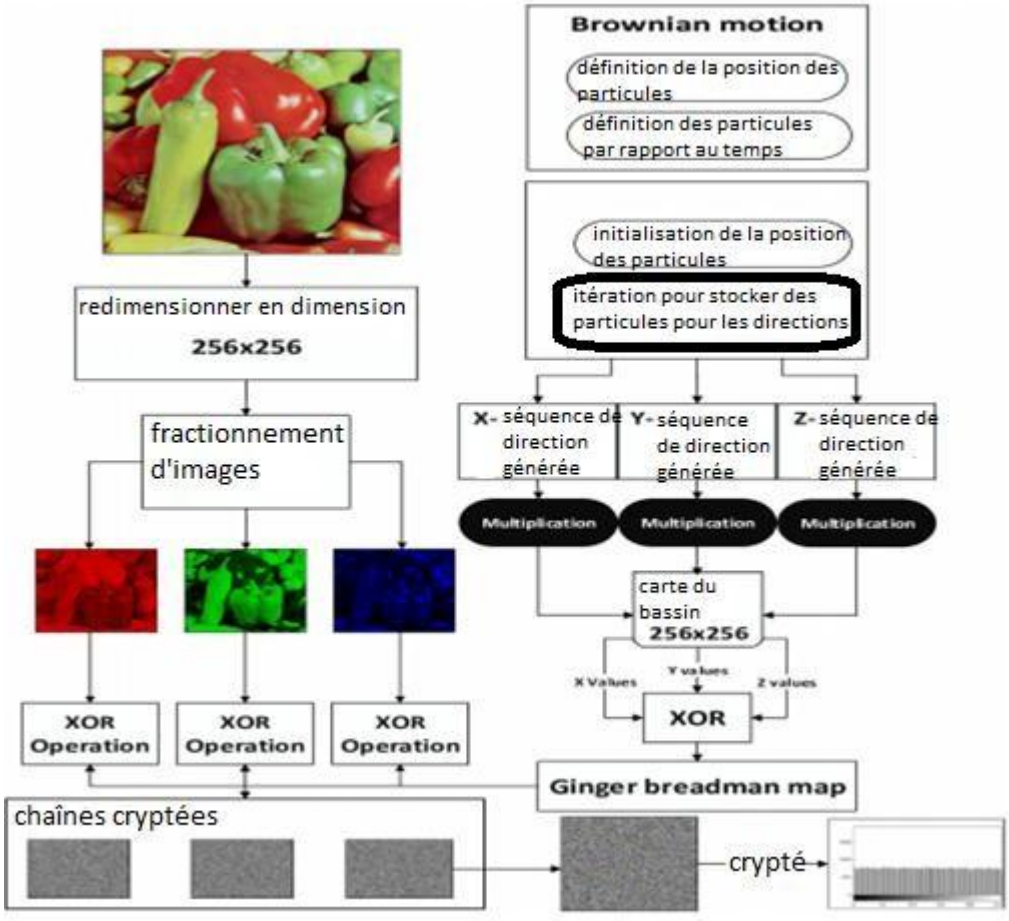


Figure II.9. Schéma du principe général [28]

E1.Lire une image de taille 512×512×3 au format jpg.

E2. Redimensionnement de l'image de 512×512×3 à 256×256×3 dans la même extension.

E3. Division de l'image en trois couches de rouge (couche R), vert (couche V) et bleu (couche B).

E4. Génération du mouvement brownien avec initialisation de la position des particules par rapport à temps en secondes, nombre de particules supposées et nombre d'impulsions par changement de piste.

E5. Itération du stockage de la position des particules pour trois positions différentes le long de X, Y et Z axe

E6. Génération d'une carte chaotique basin_2D ayant la même longueur de 256 × 256.

E7. Multiplication de la carte chaotique basin_2D généré avec trois positions différentes des particules généré à l'étape E.5.

E8. Génération d'une carte chaotique gingerbread man_2D ayant la même longueur de 256×256.

E9. Application du XOR entre la position générée à l'étape E.5 et la séquence de cartes chaotiques générée par gingerbread man_2D d'une longueur de 256×256.

E10. Application du XOR entre la sortie de l'étape 9 et les couches générées de rouge, vert, bleu à l'étape E.3.

E11. Combinaison d'une couche d'images en 256 × 256 × 3 pour obtenir une image cryptée.

II.5.2 Système hybride

II.5.2.1 Combinaison de systèmes chaotiques et de codage ADN

Cette classe de systèmes utilise un codage d'ADN avec des systèmes chaotiques de chiffrement pour crypter les images.

L'utilisation de la technologie de codage ADN pour coder les images n'est pas suffisamment sécurisée et peut être combinée avec d'autres technologies telles que Chaos [29].

Avant de présenter un travail basé sur le codage de l'ADN et les systèmes chaotiques, nous présentons quelques bases du codage de l'ADN et comment il peut être utilisé pour coder une séquence de bits.

Il existe quatre acides nucléiques différents dans une séquence d'ADN qui sont nommés A (adénine), T (thymine), C (cytosine) et G (guanine). Les règles d'appariement des bases sont, (A) s'apparie toujours avec (T) et (C) s'apparie toujours avec (G). On peut conclure que (A) et (T)

sont complémentaires, (G) et (C) sont également complémentaires. Ces relations sont souvent appelées les règles de l'appariement de bases Watson-Crick.

De même, dans le système binaire, (0,1) sont complémentaires, ce qui signifie que (00,11) et (10,01) sont également complémentaires. Donc, si nous utilisons les quatre désoxynucléotides "A", "T", "G" et "C" pour représenter les nombres binaires "00", "11", "01" et "10", respectivement, alors chaque pixel peut être codé dans une chaîne de nucléotides, par exemple, $(11000101)_2$ est le format binaire qui pourrait être codé en utilisant la règle 3 comme (ATGG).

Il existe 24 types de combinaisons pour les quatre nucléotides. Cependant, seules huit combinaisons de codage sont adaptées au principe de complémentarité. Ces règles sont résumées dans le tableau II.1.

	A	T	C	G
règle 1	00	11	10	01
règle 2	00	11	01	10
règle 3	11	00	10	01
règle 4	11	00	01	10
règle 5	10	01	00	11
règle 6	01	10	00	11
règle 7	10	01	11	00
règle 8	01	10	11	00

TableauII. 1. Règles de carte d'encodage et de décodage de la séquence d'ADN de [30]

Les auteures de [31] ont proposé un processus de cryptage comprend la diffusion par une approche ADN et la permutation par une séquence générée. La carte Hénon-Sine 2D (2D-HSM) permet de contrôler les règles ADN, le fonctionnement de l'ADN et la séquence de permutation. L'organigramme du processus de chiffrement est illustré par la figure II.10.Les étapes détaillées de l'algorithme de chiffrement sont présentées ci-dessous.

E1. Choisir les clés secrètes $\{a_1,b_1,x^0_1,y^0_1,a_2,b_2,x^0_2,y^0_2\}$, qui sont les paramètres et les valeurs initiales de 2D-HSM.

E2. Obtenir les flux de clés chaotiques x_1,y_1et x_2,y_2 en utilisant l'équation II.17 avec les paramètres de contrôle et les valeurs initiales a_1,b_1,x^0_1,y^0_1et a_2,b_2,x^0_2,y^0_2, respectivement.

$$x_{n+1} = (1- a \sin^2 (x_n) + y_n) \bmod 1 \qquad (II.17)$$
$$y_{n+1} = bx_n \bmod 1.$$

E3.Lire une image$I_{m\times n}$et enregistrer les valeurs de I dans un tableau unidimensionnel P de taille m*n.

E 4.Suivre les étapes de diffusion décrites dans l'algorithme 1 pour obtenir une séquence New_P.

Algorithm 1 The proposed diffusion algorithm

Input: Pixel value P^i (the ith pixel value of P), $i = 1, 2, \cdots, mn$, and key-streams x_1, y_1, x_2, y_2.
Output: The diffused pixel value New_P^i.
1: $temp = \sum_i(P^i) \bmod 256$.
2: $R_x \leftarrow \text{Round}(x_1^i \times 10^{10}) \bmod 8 + 1$;
$R_y \leftarrow \text{Round}(y_1^i \times 10^{10}) \bmod 8 + 1$;
$R_z \leftarrow \text{Round}(x_2^i \times 10^{10}) \bmod 8 + 1$.
3: $R \leftarrow \text{Round}(y_2^i \times 10^{10}) \bmod 256$.
4: $DNA_R \leftarrow$ Encode R with rule R_z.
5: $DNA\_P^i \leftarrow$ Encode P^i with rule R_y.
6: $New\_P^i \leftarrow DNA\_P^i \oplus DNA_R$.
7: $New\_P^i \leftarrow$ Decode New_P^i with rule R_x.
8: $New\_P^i \leftarrow New\_P^i \oplus temp$.
9: $temp \leftarrow New\_P^i$.

E5. Permuter les valeurs de New P avec l'algorithme 2 pour obtenir la séquence cryptée finale C.

Algorithm 2 The proposed permutation algorithm

Input: Pixel value P^i and the diffused pixel value New_P^i.
Output: A permutated sequence C.
1: $S = \text{Round}(x_1 \times 10^{10}) \bmod mn + 1$.
2: Remove the redundant elements in sequence S to obtain Loc which is not repeated and contains all of the data from 1 to mn.
3: Move the ith element of P to $Loc(i)$th as follows:
4: **FOR** $i = 1 : mn$
5: $C(Loc(i)) = P(i)$.
6: **END FOR**

E 6. Construire I_c de taille m×n à partir du tableau C, I_c est l'image cryptée.

Le schéma ci-dessus est conçu principalement pour crypter une image en niveau de gris. Pour une image couleur RVB, le schéma la divise d'abord en composants R, V et B, puis chiffre chaque composant de l'image et intègre les trois composants pour former l'image cryptée finale.

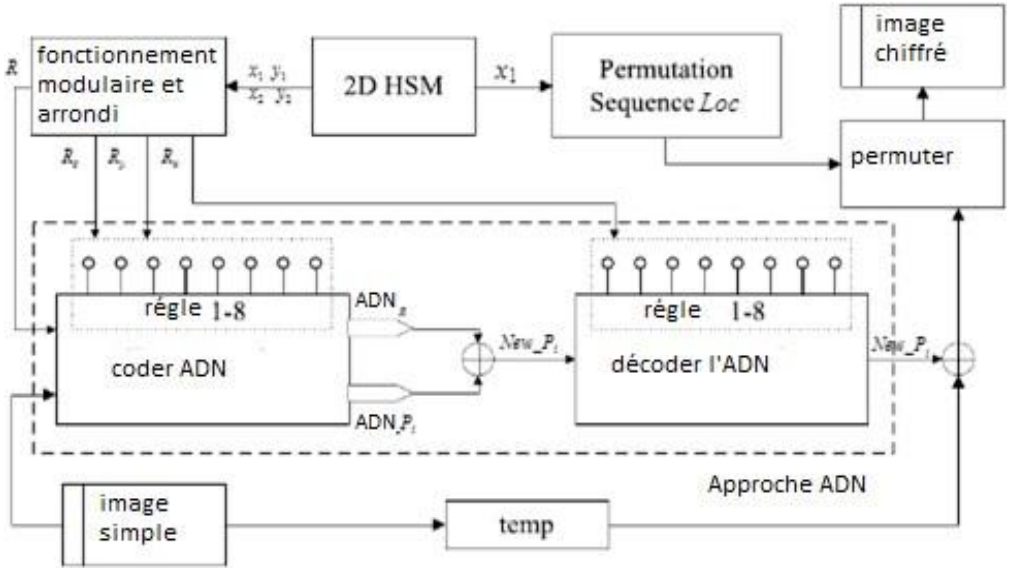


Figure II.10. Processus de cryptage d'image proposé [32].

II.5.2.2 Combinaison de cryptosystèmes chaotiques et non chaotiques

Cette classe de chiffrements utilise une combinaison des Algorithmes de chiffrements non chaotiques traditionnels (AES, ElGamel, etc.) et des systèmes chaotiques dans le chiffrement.

Un nouveau schéma de cryptage des images en couleur était proposé dans [32], les auteurs ont utilisé une combinaison du chiffrement symétrique standard bien connu AES et deux cartes chaotiques efficaces : la carte de Renom et la carte logistique. La figure II.11 résume le principe.

Le principe est de décomposer d'abord l'image I de taille M*N en trois matrices R,V, B de taille M*N, puis permuter les valeurs d'intensité des pixels en utilisant la carte chaotique de Renon 2D, ensuite en utilisant la carte logistique chaotique lD. Finalement les valeurs des trois matrices sont modifiées en utilisant AES pour construire l'image cryptée. Le processus de déchiffrement est le processus inverse du chiffrement.

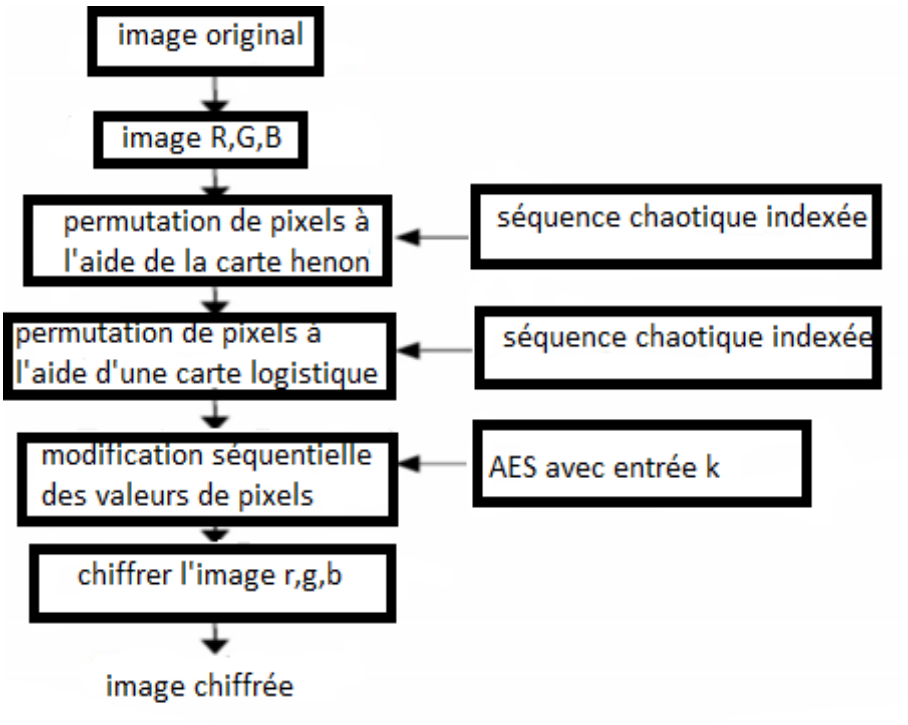


Figure II.11. Schéma de cryptage proposé dans [33]

II.6 Analyse de sécurité des différents systèmes de cryptage chaotique étudiés

Le tableau II.2 résume les résultats obtenus de quelques paramètres d'analyse de sécurité présentés dans la section II.4 des différents travaux étudiés dans la section II.5.

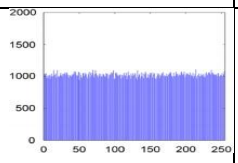
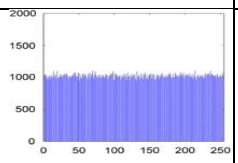
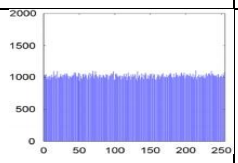
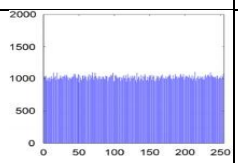
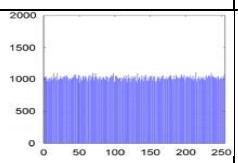
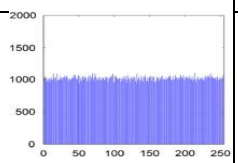
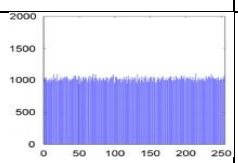
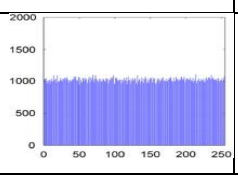
Travaux	Entropie	Histogramme	NPRC	UACI	Corrélation			Espace de clés
					H	V	D	
[23]	7.9981632		99.615	33.36	0.0036	0.0073	0.0059	10^{95}
[24]	7.998		99.64	30.66	0.00027	0.00067	0.00049	2^{136}
[25]	7,9989		99,6108	33,4635	0.000009750	0.0000057066	0.00072484	10^{84}
[26]	7,999		100	33,5515	0.00047	0.03911	0.00305	2^{128}
[27]	7,9973		99	33.47	0.000975	0. 00057	0.00048	$1.11038*2^{377}$
[28]	7,997		99.64	33.51	0.0014	0.0032	0.0043	2^{192}
[31]	7.9976		99.6200	33.4169	0.0006	0.0038	0.0010	10^{112}
[32]	7.9974		99,6	33,3	0.0039	0.0076	0.0063	$3.4*10^{122}$

Tableau II.2 Résultats obtenus des différents travaux étudiés

D'après le tableau, nous pouvons conclure que :

- les histogrammes des images cryptées des différents travaux sont uniformes présentant une similarité statistique.

- les valeurs d'entropies des images cryptées sont très proches de la valeur idéale (la valeur idéale = 8).
- les travaux conservent de faibles coefficients de corrélation dans toutes les directions.
- les valeurs de test (NPCR et UACI) sont assez proches de leurs valeurs théoriques correspondantes, indiquant que tout petit changement dans l'image en clair rend les images cryptées correspondantes complètement différentes.
- l'espace de clés des travaux proposés est supérieur à 2^{100} ce qui maintient le crypto-système en haute sécurité contre les attaques par force brute.

II.7 Conclusion

Dans ce chapitre nous avons présenté le principe de confusion et de diffusion, puis nous avons donné quelques mesures d'analyse et d'évaluation de performances des systèmes de cryptage chaotique. Ensuite, nous avons étudié quelques travaux de cryptage chaotiques des images rencontrés dans la littérature.

Après une synthèse de ces différents travaux, nous proposons dans le chapitre suivant, de décrire notre proposition au niveau empirique, en présentant la fonction proposée, ainsi que notre système de cryptage des images.

Chapitre III

Réalisation d'un système de cryptage chaotique des images

III.1 Introduction

Dans ce chapitre, nous allons tout d'abord présenter les deux fonctions chaotiques que nous avons utilisées dans notre travail : La fonction logistique et la fonction sine map, ces deux fonctions ont beaucoup d'applications en raison de leurs structures simples. Ensuite nous décrivons en détail notre système de cryptage chaotique des images numériques proposé, qui se base essentiellement sur une nouvelle fonction chaotique SinLog défini à partir des deux fonctions chaotiques mentionnées précédemment.

III.2 Fonctions chaotiques

III.2.1 Fonction Logistique

La fonction logistique est une des célèbres fonctions chaotiques 1Dimension. Rappelons tout d'abord sa définition mathématique et son diagramme de bifurcation décrits déjà dans le chapitre I, section I.3.4.2:

$$x_{n+1}=r*x_n*(1-x_n) \qquad \textbf{(III.1)}$$

Dans l'équation (III.1) ci-dessus, r est le paramètre de contrôle qui peut avoir des valeurs dans l'intervalle $0 < r < 4$ et $x_n \in [0, 1]$.

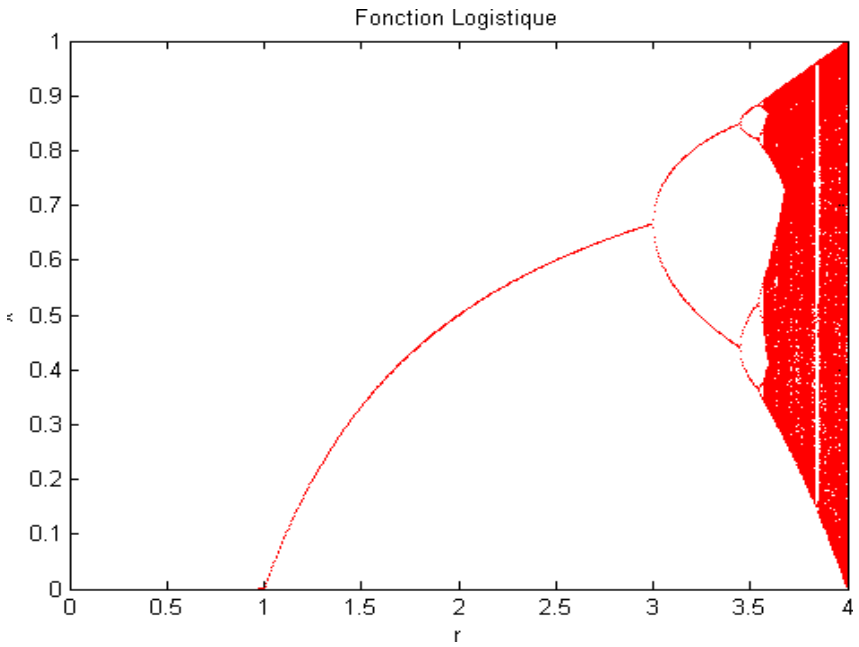


Figure III.1 : Diagramme de bifurcation pour la fonction logistique.

Selon ce diagramme de bifurcation, la fonction ci-dessus a un comportement chaotique pour r > 3,568945672.

III.2.2 Fonction Sine map

Une autre fonction chaotique très utilisée dans la littérature est la fonction Sine map défini par l'équation suivante :

$$x_{n+1} = a * \sin(\pi * x_n)/4 \qquad \text{(III.2)}$$

Où le paramètre **a** ∈ [0, 4] et x_n ∈ [0, 1].

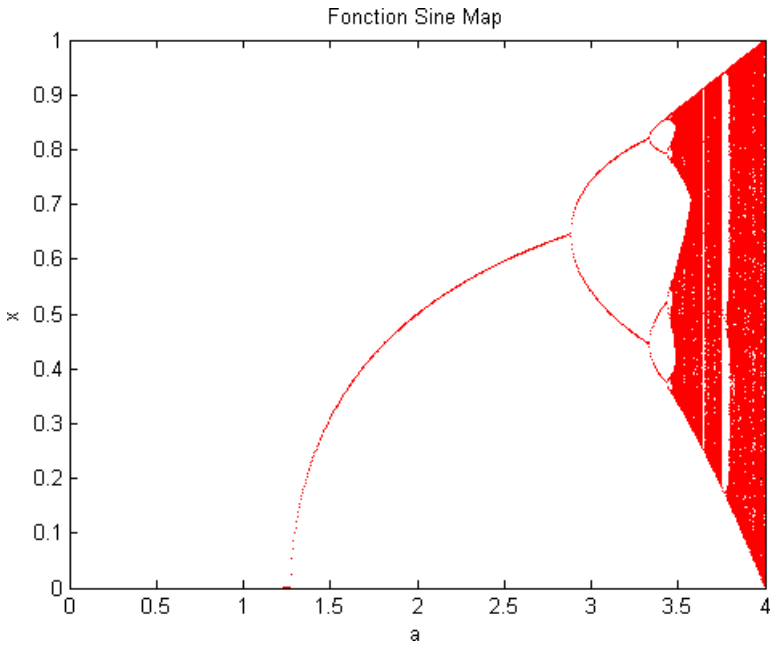


Figure III.2 : Diagramme de bifurcation pour la fonction Sine Map.

Comme le montre la figure III.2, le comportement chaotique de cette fonction est similaire à celui de la fonction logistique.

III.2.3 Nouvelle Fonction chaotique SinLog

La nouvelle fonction SinLog que nous proposons est défini à partir de deux fonctions chaotique décrites précédemment par les équations III.1 et III.2. Nous définissons cette nouvelle fonction par l'équation suivante :

La figure suivante illustre son comportement chaotique.

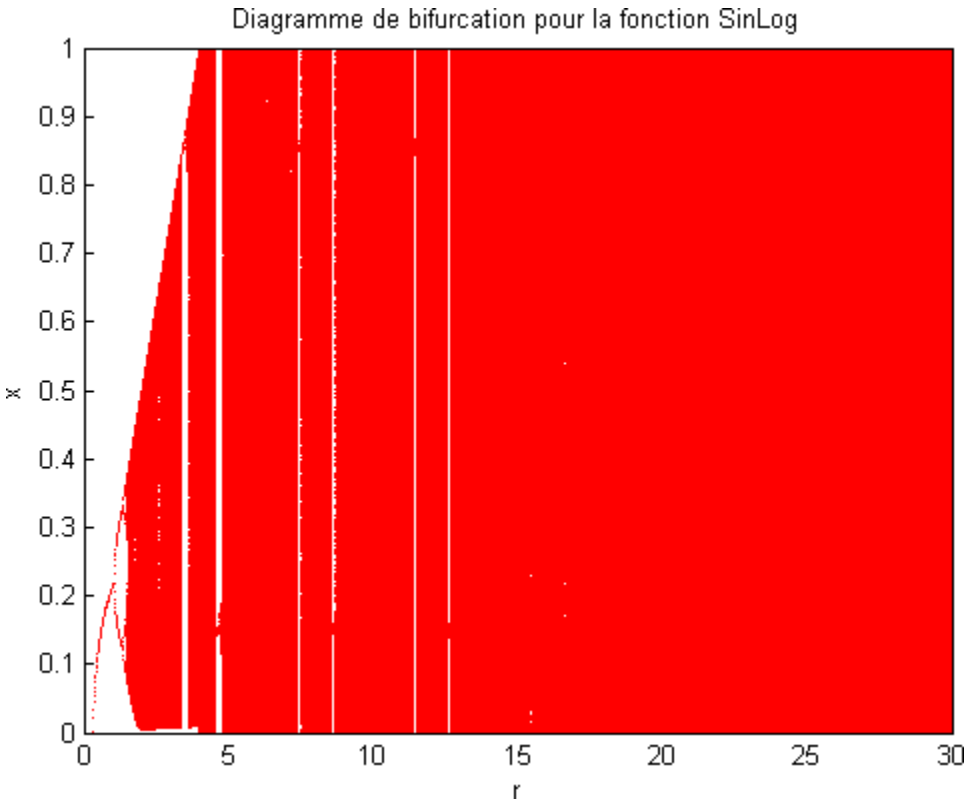


Figure III.3 : Diagramme de Bifurcation de la fonction SinLog.

Il est clair que cette nouvelle fonction SinLog possède un comportement différent de celui des deux fonctions décrites précédemment. SinLog présente un large intervalle correspond à la zone chaotique, ce qui très important pour un système de cryptage chaotique.

Pour bien illustrer les valeurs possibles du paramètre a, nous présentons dans la figure suivante, le diagramme de l'exposant de Lyapunov associé.

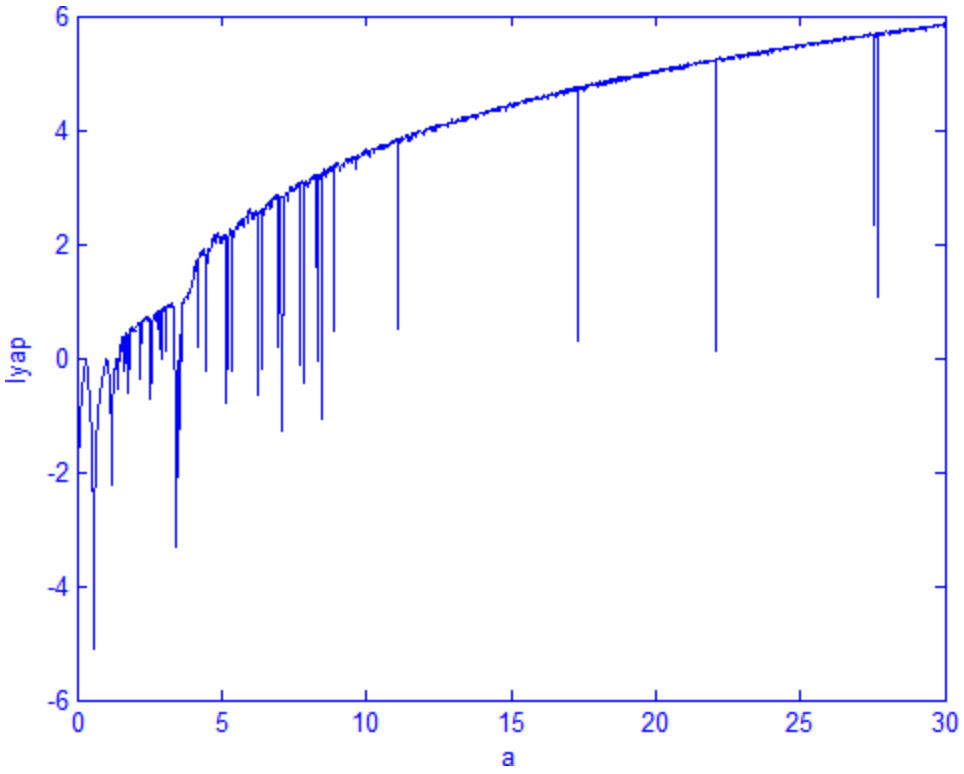


Figure III.4 : Diagramme de lyapunov de la fonction SinLog

La section suivante a comme objectif de présenter notre système du cryptage chaotique des images, basé sur notre nouvelle fonction chaotique SinLog. Les valeurs positives sont des valeurs que peut prendre SinLog afin d'avoir un comportement chaotique.

III.3. Présentation de notre système de cryptage chaotique des images numérique

Le système proposé est basé sur les principes de confusion/diffusion décrites dans le chapitre précédent (section II.2).

La confusion est juste un réarrangement des pixels de l'image sans modification des valeurs des pixels, l'objectif principal de cette phase est de briser la forte corrélation entre les pixels, tandis que la phase de diffusion consiste à masquer les pixels ordinaires par des nouvelles valeurs chaotiques secrètes.

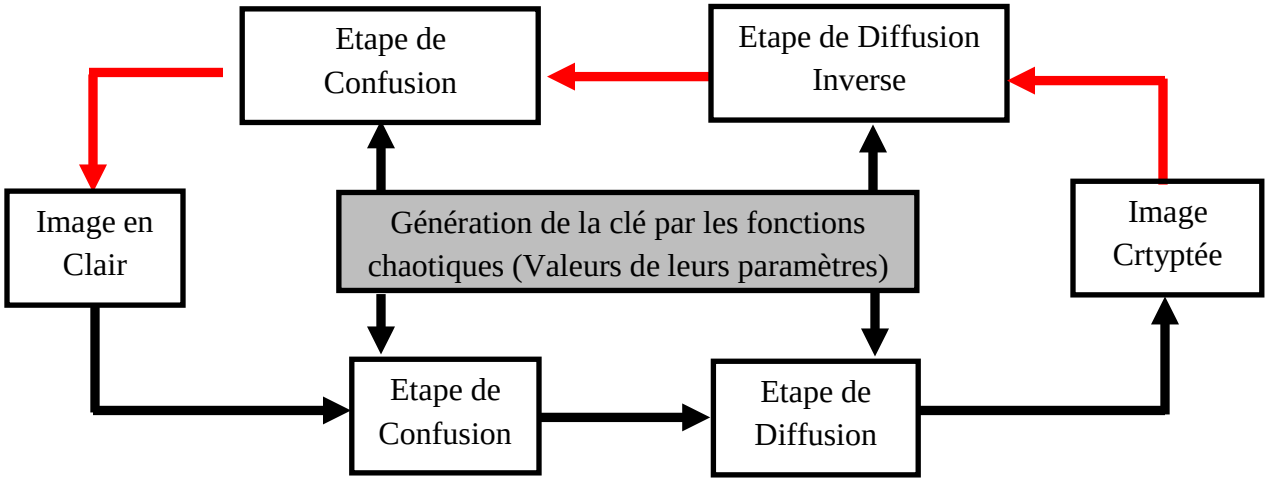


Figure III.5 : Schéma général de notre système chaotique.

III.3.1 Processus de Cryptage

III.3.1.1 Etape de Confusion

Confusion

Entrée : Image en clair de taille M*N
Sortie : Image après confusion
Choisir les valeurs initiales des paramètres de la fonction SinLog : r, x_0 et a[1].

1. Décaler_Ligne :
Pour chaque ligne
Générer un entier compris entre 0 et M.
Décaler les pixels de la ligne selon la valeur obtenue.

2. Décaler_Colonne:
Pour chaque colonne
Générer un entier compris entre 0 et N.
Décaler les pixels de la colonne selon la valeur obtenue.

[1] Les valeurs de paramètres de la fonction chaotique représentent une clé dans notre système de cryptage.

III.3.1.2 Etape de Diffusion

Les étapes E1, E2, E4 et E5 de l'algorithme ci-dessus sont similaires à celles décrites dans [33]. Cet algorithme sera exécuté pourchaque pixel de l'image à cryptée.

Diffusion

- VP est la valeur du pixel.
- Définir les valeurs initiales des paramètres de la fonction SinLog a, r, x0 : a $\in$[2,30], x0 $\in$[0,1] et r $\in$ [3.57, 4].

Pour chaque pixel P en clair, P est le numéro de pixel en clair.

E1 : Générer 08 valeurs entières ordonnées

- Calculer 8 valeurs différentes de la séquence chaotique: S_j / j = 1.. 8.

Il faut noter que la dernière valeur trouvée (S_8) sera mise comme valeur initiale lorsqu'on exécute cet algorithme pour le prochain pixel.

- Multiplier les valeurs S_j par un scalaire $K=10^8$ et assurer que ces différentes valeurs sont comprises entre 0 et 255 :

$$V_j = (S_j * \text{scalaire}) \bmod 256.$$

- Ordonner ces valeurs V_j par ordre croissant,

E2 : Calculer les suites ; SC(P,j) et SCT(P,j), j=1..8.

- Initialisation : $SC(P,0)= V_1$, $SCT(P,0)=0$,

$SC(P,j)= SCT(P,j-1) +V_j$

$SCT(P,j)= SCT(P,j-1)+ SC(P,j)$.

E3 : Générer une valeur XP aléatoire pour chaque pixel P.

- Choisir les valeurs initiales des paramètres de la fonction SinLog r , x_0 et a.
- Calculer un entier En compris entre 0 et 256.

$$XP=(En* 10^6) \bmod 256.$$

E4 : Définir SY(P).

- Convertir la valeur de XP obtenu dans (E3) en binaire.
- Calculer la somme S

$$SY(P) = \sum_{j=1}^{8} SC(P,j) * XP_{9-j}$$

E05 : Calculer la nouvelle valeur Pn de pixel P par :

$$Pn = fl((C(p) * 10^6)\ mod\ 256) \text{ Tel que}$$

$$C(p) = (p)/SCT(p,8)$$

E06 : Définir la valeur du pixel crypté Pc.

- Px = Pn Xor VP.
- Convertir Px en binaire.
- Définir sa valeur miroir.
- Pc est la valeur décimale correspondante à la valeur miroir précédente.

Le processus de décryptage prendra exactement le chemin inverse de celui de cryptage.

III.3.2 Application Numérique

Nous montrons un exemple d'application de l'étape de diffusion. Nous prenons comme valeur de Pixel VP = 53 (après l'étape de confusion).

Les valeurs des paramètres de notre fonction SinLog sont a= 9.99 / r= 3.99 / X_0= 0.01 (la clé).

E1 : La séquence chaotique de huit valeurs obtenue par l'équation III.3 est :

- S_j = [0.3089791091625665, 1.1235028714993331, -2.4624966218965083, -0.023806705097591193, -0.7508525868682806, 1.725169595722108, -0.08533989228622493, -2.2901482795946144].

- **Les valeurs entières ordonnées par ordre croissant sont :**
  V_j = [17, 17, 99, 138, 170, 171, 207, 227]

E2 : Calcul des suites ; SC(P,j) et SCT(P,j), j=1..8.

Sc =[17, 34, 133, 322, 676, 1353, 2742, 5504]

SCT = [17, 51, 184, 506, 1182, 2535, 5277, 10781]

E3 : Génération une valeur XP aléatoire pour chaque pixel P.

La valeur de XP est 243 : (0.308979*10^6) mod 256=243 tel que En=0.308979

E4: Définition de SY(P).

La valeur binaire de 243 est égale à '11110011'

SY(P) = (17***1** + 34***1** + 133***0** + 322***0** + 676***1** + 1353***1** + 2742***1** + 5504***1**)= 10326

E5 : Calcul de la nouvelle valeur Pn de pixel

C(p)= (10326 / 10781) = 0.957796122280

Pn= (0.957796122280 * 10^6) mod 256 = 100

E6 : Définition de la valeur Pc

Px= Pn XOR VP = 100 XOR 53 = 81

Px en Binaire = '01010001'

La valeur Miroir de '01010001' est : '10001010'

La valeur du pixel cryptée est:

Pc= 138.

III.4. Implémentation de notre Système de cryptage chaotique des images numériques.

III.4.1. Langage de programmation

Les diagrammes de bifurcation présentés dans ce mémoire sont générés par Matlab R2013a. Tandis que pour notre application nous avons utilisé le langage python 3.9. Python est un langage de programmation orienté objet interprété, sa syntaxe est simple et claire, elle respecte les standards du domaine.

III.4.2. Images numériques

Dans notre application, Nous nous sommes basées sur des images numériques standards de test comme "Lena.jpg", "Barbara.jpg", "Fleur.jpg" et "camearmen.jpg"

III.4.3 Résultats Expérimentaux

Un système de cryptage est un système qui résiste à tous types d'attaques. Nous discutons dans cette section les résultats de la sécurité et l'analyse des performances de notre système décrit précédemment.

Les paramètres de notre système de cryptage chaotique des images selon la fonction chaotique utilisée :

Paramètres / Fonction Chaotique	x_0	r	a
Sin_Log	0.01	3.99	9,99
Logistique	0.01	3.99	-

Tableau III.1 : Paramètres des deux fonctions chaotiques.

Nous présentons dans ce qui suit, les résultats obtenus de notre système de cryptage chaotique des images basé sur la fonction SinLog. Une étude comparative du même système avec la fonction logistique est l'objet de la section III.5

III.4.3.1 Analyse de l'espace de clé

L'espace de clé de notre système possède 3 clés : $x \in [0,1]$, $r \in [3.57, 4]$ et $a \in [2,30]$, ce qui signifie que son espace clé selon la formule (II.1) est égal à :

Nous avons:

$$K1=2^{48}, \quad K2=0.43*2^{48}, \quad K3=28*2^{48}.$$

Alors:

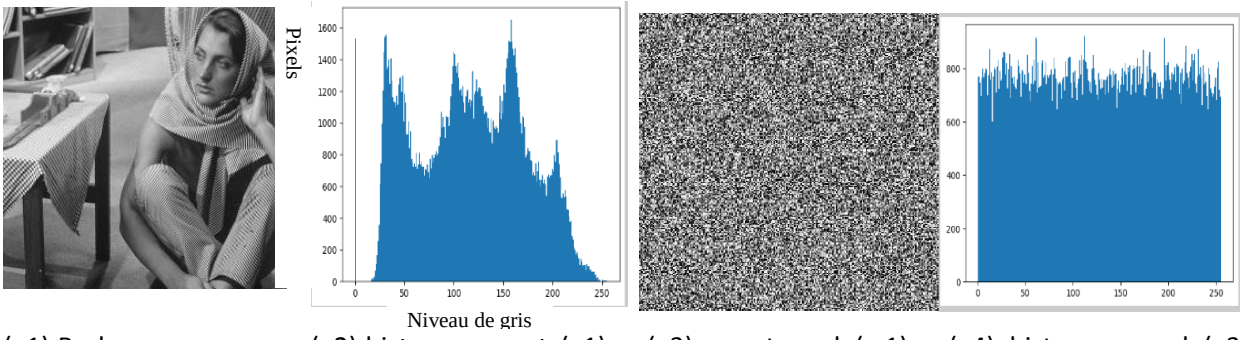
$$S=Sk1*SK2*SK3=2^{48}*0.43*2^{48}*28*2^{48} = 2^{149}$$

Cette valeur est plus grande que 2^{100}, cela prouve que notre système proposé est résistant aux attaques forces brutes.

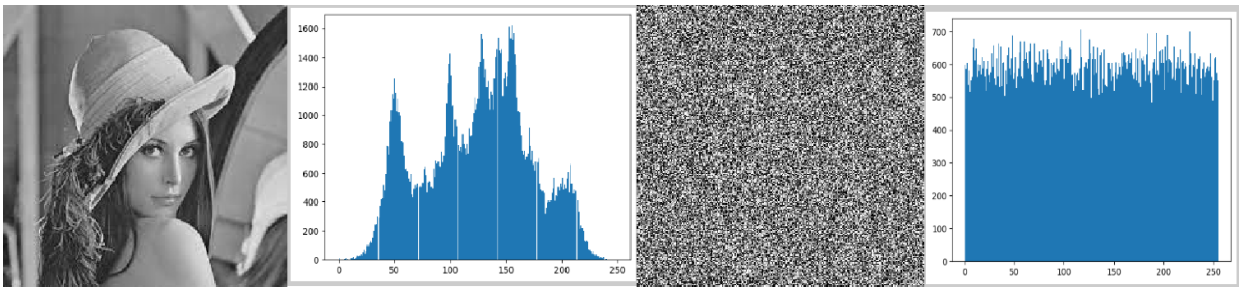
III.4.3.2 Analyse d'histogramme

Rappelons qu'un histogramme est un graphe qui illustre le nombre de pixels dans une image à chaque valeur d'intensité trouvée dans cette image. Pour une image en niveau de gris, il y en 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.

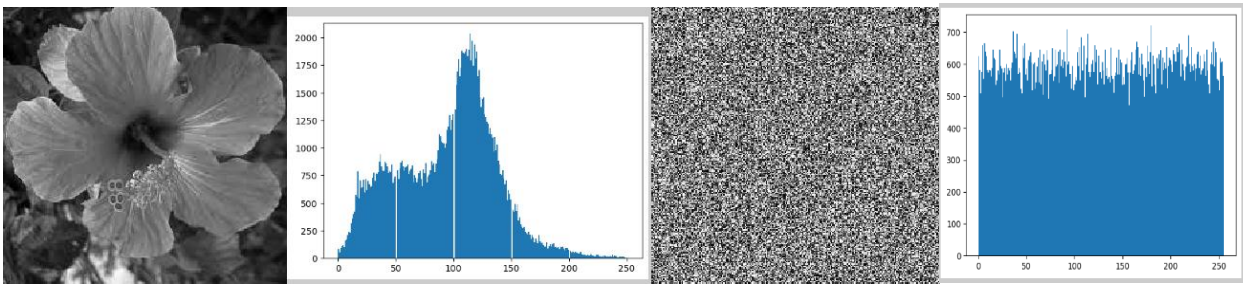
Les images testées sont de taille 256x256 correspondantes aux figures : a1, b1, c1, d1 de la figure III.6 Alors que les figures a2, b2, c2, d2 de la figure III.6 représentent leurs histogrammes correspondant. Les images cryptées associés aux différentes images précédentes ainsi que leurs histogrammes sont illustrés en a3, b3, c3, d3 de la même figure et a4, b4, c4, d4 respectivement.



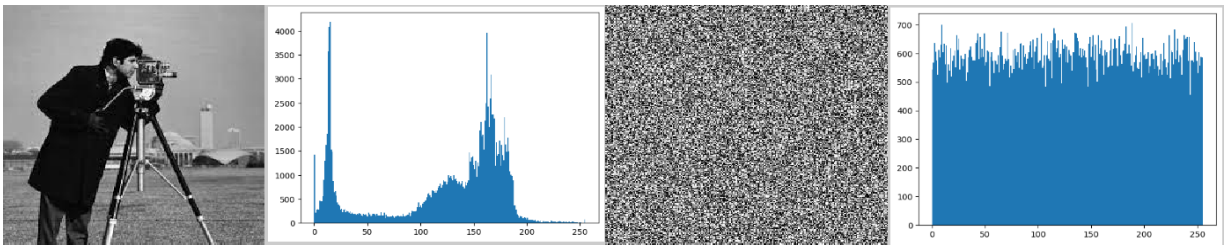
(a1):Barbara (a2):histogramme de(a1) (a3): cryptage de(a1) (a4): histogramme de(a3)



(b1):Lena (b2):histogramme de (b1) (b3): cryptage de(b1) (b4): histogramme de(b3)



(c1):Fleur (c2):histogramme de (c1) (c3): cryptage de (c1) (c4): histogramme de (c3)



(d1):Cameraman (d2):histogramme de(d1) (d3): cryptage de(d1) (d4): histogramme de(d3)

figure III.6 Résultats d'analyse d'histogrammes

Nous pouvons clairement remarquer que l'histogramme des images cryptées a une distribution uniforme des valeurs de pixels (tous les pixels ont la même chance d'apparition), ceci est prouvé que le système chaotique n'est pas vulnérable à l'attaque d'histogramme.

III.4.3.3 Analyse de Coefficient de Corrélation :

Les pixels adjacents d'une image en clair ont une forte corrélation. Un bon système de cryptage d'image doit supprimer une telle corrélation afin d'assurer la sécurité contre l'analyse statistique.

Afin de tester la performance de notre système, nous avons choisi au hasard 2000 pixels de l'image en clair et leurs correspondants dans l'image cryptée puis calculé les différents coefficients de corrélations en niveau horizontal, vertical et diagonal.

Direction	**Horizontal**		**Vertical**		**Diagonal**	
Images	**Image en clair**	**Image cryptée**	**Image en clair**	**Image cryptée**	**Image en clair**	**Image cryptée**
Lena	0.9209	-0.0070	0.9556	-0.0011	0.8898	0.0042
Barbara	0.8926	0.0047	0.9229	-0.0013	0.8777	-0.0002
Fleur	0.9589	0.0092	0.9621	-0.0100	0.9353	-0.0008
Cameraman	0.9384	0.0090	0.9598	0.0051	0.9106	-0.0059

Tableau III.2 : Coefficients de Corrélation des images en clair et cryptée.

Nous pouvons clairement remarquer que les valeurs des coefficients de corrélation sont proches de 1, cela signifie que les images en clair sont fortement corrélées. Cependant les valeurs des coefficients de corrélation des images cryptées sont proches de 0, cela signifie qu'il n'existe aucune corrélation entre les pixels.

Graphiquement, la corrélation dans différentes directions de l'image lena.jpg en clair et sa correspondante cryptée est illustrée par la figure suivante.

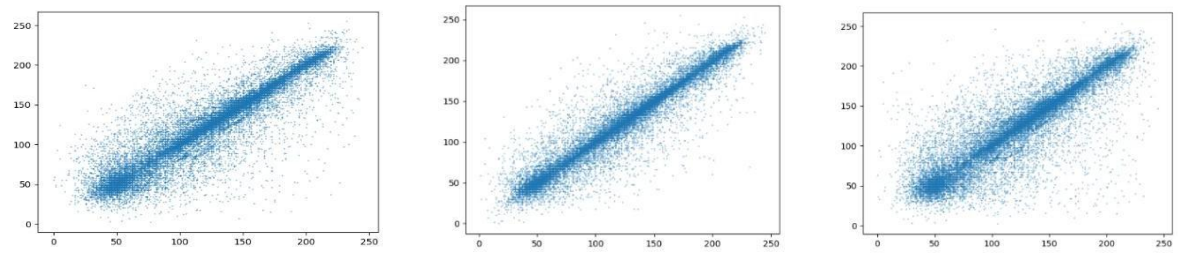


Figure III.7 : Corrélation des pixels de l'image en clair dans les directions horizontale verticale et diagonale

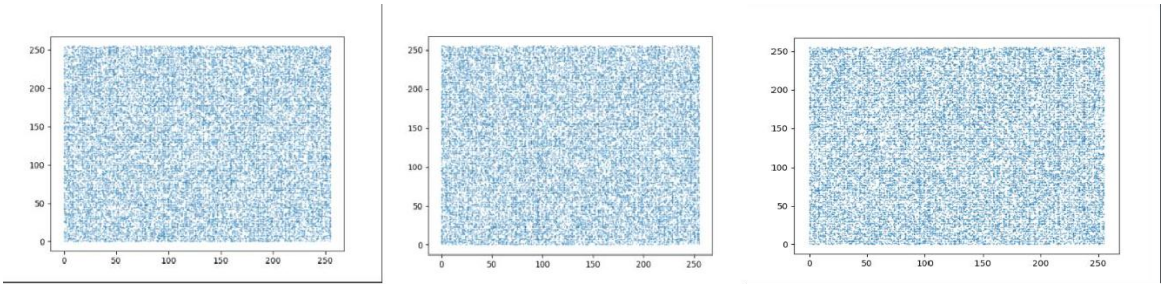


Figure III.8 : Corrélation des pixels de l'image en cryptée dans les directions horizontale verticale et diagonale

La faible corrélation entre les pixels adjacents prouve que le système proposé peut casser la corrélation entre les différents pixels de l'image.

III.4.3.4 Entropie

L'entropie est une mesure statistique du hasard dans la théorie de l'information. La performance d'un système de cryptage est mesurée en obtenant une valeur de l'entropie proche de la valeur 8.

La valeur entropie de différentes images selon notre système est décrite dans le tableau suivant:

Images de test	Entropie	
	Image en clair	Image Cryptée
Lena	7.5011	7.9964
Barbara	7.6435	7.9958
Fleur	7.358	7.9961
Cameraman	7.1307	7.9961

Tableau III.3 : Entropie Des images Originales et Cryptées

Il est clair que toute la valeur d'entropie de toutes les images cryptées est proche de la valeur idéale.

II.4.3.5 Analyse de sensibilités

Le nombre de taux de pixels changeants (NPCR) et l'intensité modifiée moyenne unifiée (UACI) sont deux tests standardisés utilisés pour examiner la sensibilité d'une image simple contre une attaque différentielle.

Images	NPCR	UACI
Lena	99.6258	33.6935
Barbara	99.5847	33.5644
Fleur	99.6239	33.6179
Cameraman	99.6180	33.6579

Tableau III.4 : les valeurs de NPCR et UACI

Un bon système de cryptage doit avoir une valeur de NPCR > 99; 6094% et un UACI > 33;4635%, ce qui est assuré par notre système (Tableau III.4).

II.4.3.6 PSNR

La valeur de PSNR doit être inférieure à 35entre l'image en clair et image, ce qui est prouvée par le tableau suivant :

Images	PSNR
Lena	**26.1609**
Barbara	**27.9408**
Fleur	**29.9668**
Cameraman	**26.7131**

Tableau III.5 : Valeurs de PSNR

III.5 Etude Comparative

Dans cette section, nous allons effectuer une étude comparative entre les deux fonctions chaotiques : la fonction logistique et la fonction SinLog, autrement dit, nous garderons le même système de cryptage, et nous changerons seulement la fonction. Les résultats des différentes métriques sont donnés dans le tableau suivant :

Image de test	Métriques	Notre système chaotique à base de la fonction	
		Logistique	**SinLog**
	Espace de clé	2^{97}	2^{149}
Lena.jpg	**Entropie**	**7.9956**	**7.9964**
	NPRC	**99.6180**	**99.6258**
	UACI	**33.7885**	**33.6935**
	PSNR	**26.1609**	**26.1609**
Barbara.jpg	**Espace de clé**	2^{97}	2^{149}
	Entropie	**7.9959**	**7.9958**
	NPRC	**99.6434**	**99.5847**
	UACI	**33.6534**	**33.5644**
	PSNR	**27.9408**	**27.9408**

Fleur.jpg	**Espace de clé**	2^{97}	2^{149}
	Entropie	**7.9954**	**7.9961**
	NPRC	**99.5866**	**99.6239**
	UACI	**33.6033**	**33.6179**
	PSNR	**29.9668**	**29.9668**
Cameraman.jpg	**Espace de clé**	2^{97}	2^{149}
	Entropie	**7.9957**	**7.9961**
	NPRC	**99.6082**	**99.6180**
	UACI	**33.6457**	**33.6579**
	PSNR	**26.7131**	**26.7131**

Tableau III.6 Etude Comparative des deux fonctions étudiées :Logistique et SinLog

On voit clairement dans le tableau précédent que les résultats des analyses de performances et de sécurité des deux fonctions chaotiques sont encourageants pour l'entropie, NPRC et UACI, PSNR et l'analyse de corrélation. Cependant, le système de cryptage basé sur SinLog a une valeur d'espace de clé supérieure à celle du même système basé sur la fonction logistique, ce qui prouve qu'il est mieux résistant aux attaques de force brute.

III.6 Conclusion

Dans ce chapitre, nous avons présenté notre nouvelle fonction chaotique SinLog qui se base sur la fonction logistique et la fonction Sine map. Ensuite, nous avons décrit notre système de cryptage chaotique des images numériques en se basant toujours sur la fonction SineLog. Finalement, nous avons prouvé la haute performance et la haute sécurité de notre proposition.

Conclusion Générale

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.

Il existe une variété des algorithmes de cryptage, qui ont prouvé leur performances et leurs efficacité pour les des informations textuelles comme AES, RSA, mais le problème qui se pose et que ces dernier sont inadéquats pour le chiffrement des données fortement corrélées. Une des solutions prometteuses de ce problème est d'utiliser le phénomène de chaos dans le cryptage en raison de caractéristiques particulières comme la sensibilité aux conditions initiales.

Rappelons que notre objectif dans ce mémoire consiste à concevoir et implémenter un système de cryptage chaotique des images. Pour atteindre cet objectif, nous avons d'abord présenté des généralités sur les trois domaines qui englobent notre travail : cryptographie, chaos et images, Ensuite nous avons présenté un état de l'art sur la cryptographie chaotique des images.

Sur le plan empirique, nous avons prouvé le comportement chaotique d'une nouvelle fonction chaotique définit à partir d'une combinaison des deux fonctions : la fonction logistique et la fonction sine map, puis nous avons implémenté un système de cryptage d'image basé sur cette nouvelle fonction proposée.

Les résultats expérimentaux ont montré que l'algorithme proposé présente un niveau élevé de sécurité et de performance.

En perspectives de ce travail :

- Faire des comparaisons des résultats du système proposé avec d'autres travaux récents et en utilisant d'autres images de tests.

- Adapter notre système chaotique aux images couleurs : car le système réalisé est conçu principalement pour les images en niveau de gris.

- Appliquer notre système chaotique sur d'autres types des données à savoir, la vidéo.

Bibliographie

Bibliographie

[1] B. Schneier. Cryptographie appliquée. *International Thomson Publishing France, Paris*, janvier 2001.

[2] S. Douglas. Cryptographie :Théorie et pratique. *Vuibert Informatique*, *Paris*, 2001.

[3] A. Ali pacha, N. Hadj said . La Cryptographie et ses principaux systèmes de références, *RIST Vol*, *12 n'01*, 2002.

[4] R. Stinson. Cryptography theory and practice, discrete mathematics and its applications. *chapman & hall/crcpress*, *New York*, November 2005.

[5] M.A. FILALI. Etude et implémentation pipeline sur FPGA de l'algorithme de chiffrement AES, *Mémoire de Magister*, Université de Mohamed Boudiaf, *Oran*, 2014-2015.

[6] A. Wurcker. Etude de la sécurité 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, France, 2015.

[7] J. Emonet. Algorithmes de chiffrement. *Documentation* :version 1.0, 22 juin 2005.

[8] M.B. M.Belkaid. Application des techniques de cryptage pour la transmission sécurisé d'image MSG, *Mémoire de Magister en électronique*, Mouloud Mammeri, TiziOuzou, 2015-2016.

[9] M.B.Luca. Apports du chaos et des estimateurs d'états pour la transmission sécurisée de l'information. *Thèse de doctorat en électronique*, université de Bretagne Occidentale, 2006.

[10] G. Kaddoum. Contributions à l'amélioration des systèmes de communication multiutilisateurs par Chaos: synchronisation et analyse des performances, *Thèse de Doctorat de l'Université de Toulouse*, 2008.

[11] G. Zaibi. Sécurisation par dynamiques des réseaux locaux sans fil au niveau de la couche MAC, *Thèse de Doctorat de l'université de Toulouse*, 2012.

[12] "Digital_image.".Disponible:https://en.wikipedia.org/wiki/Digital_image.

[13] M. Lossendière. Caractéristiques d'une image numérique, Août 2016 https://www.lossendiere.com/2016/08/31/caracteristiques-dune-image-numerique/.

[14] L. Bouanzi. Les formats de numération des images fixes, DES en informatique documentaire rapport de stage, *Ecole Nationale Supérieure des Sciences de l'Information et des Bibliothèques (ENSSIB*), *Université Claude Bernard Lyon1*, 1999.

[15] "Image-Numerique„".Disponible:https://www6.inrae.fr/pfl-cepia/Axe-images/Tutoriel/L-image-numerique

[16] G. Alvarez and S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, *Int.J.Bifurcation Chaos*, vol.16, no.8,pp .2129–2151, Aug.2006.

[17] E. Yavuz. A novel chaotic image encryption algorithm based on content sensitive dynamic functions witching scheme, *Optics and Laser Technology*, 2019.

[18] M.A. Mohamed, A.S. Samrah, A.M. AbuTaleb, & M.G. Abdel-Fattah, Development of hybrid encryption watermarking techniques of multimedia," *Master thesis, Faculty of Engineering, Mansoura University*, Egypt, 2015.

[19] M.Asgari-Chenaghlu, M.-A.Balafarand & M.-R.Feizi-Derakhshi, A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation, *Signal Processing,* 2018.

[20] Z.Tang,Y, Yang,S.XuandX.Z, ChunqiangYu, Image encryption with double spiral scans and chaotic maps,*Security andCommunicationNetworks,*2019.

[21] M. Alawida, A. Samsudin, J.S. Teh & R.S. Alkhawaldeh, A new hybrid digital chaotic system with applications in image encryption, *SignalProcess.*,vol.160,pp.45–58,Jul.2019.

[22] J.S.Teh,M. Alawida, & Y.C.Sii, Implementation and practical problems of chaos-based cryptography revisited, *J.Inf.Secur.Appl.*,vol.50,Feb.2020,Art.no.102421.

[23] C.Li, G.Luo, & C.Li, An Image Encryption Scheme Based on The Three-dimensional chaotic logistic map, *International Journal of Network Security*, Vol.21,No.1,PP.22-29, Jan. 2019.

[24] SalahT. Allawi, MayM.Abbas, A New method for image encryption based on 2D-3D chaotic maps, *International Journal of Computer Science and Information Security (IJCSIS)*,Vol.18, No. 11, November 2020.

[25] Y. Zhou, L. Bao, C.L.Philip Chen, "A new 1D chaotic system for image encryption, *Signal Processing,* 2014.

[26] I. Yasser, F. Khalifa, M.A. Mohamed, & A Samrah, A New image encryption scheme based on hybrid chaotic maps , *Hindawi Complexity*, Volume 2020,Article ID 9597619, 23 pages.

[27] D. Sravanthi, K. K. Patro, B. Acharya & S. Majumder, A secure chaotic image encryption based on Bit Plane operation*, Advances in Intelligent Systems and Computing*, 2018.

[28] M. Khan, F.Masood, A.Alghafis, M. Amin, & S. I.B.Naqvi, A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion, *PLoS ONE 14(12): e022503*, 2019.

[29] J. Zhang, D. Fang & H. Ren, Image encryption algorithm based on DNA encoding and chaotic maps, *Mathematical Problems in Engineering*, 2014.

[30] Z. Hua, B. Zhou & Y. Zhou, Image content-based encryption algorithm using high-dimensional chaotic system, *International Symposiumon Nonlinear Theory and its Applications*, 2015.

[31] J.Wu, X. fengLiao, Image encryption using 2D Hénon Sine Map and DNA approach, *Signal Processing*, 2018.

[32] P. Nayak, S. K. Nayak and S. Das. A secure and efficient color image encryption scheme based on two chaotic systems and advanced encryption atandard, *International Conference on Advances in Computing, Communications and Informatics (ICACCI),* 2018.

[33] Merzoug Assia. Neuronal cryptosystème basé sur un attracteur chaotique, *Doctorat en Informatique*, *Université de Batna2*, 2019.