REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de **T**echnologie

Département **I**ngénierie des **S**ystèmes **E**lectriques

Mémoire de Master

Présenté par

M[lle] BAOUALIFeriel

M[lle] BOUTIH Hamida

Filière : Télécommunications

Spécialité : Réseaux et **T**élécommunications

Cryptage d'images par les systèmes hyper chaotiques

Soutenu le ..../…./2022 devant le jury composé de:

HOCINE	Faiza	MCB	Université de Boumerdès	Président
BELKACEM	Samia	MCA	Université de Boumerdès	Encadreur
MESSAOUDI	Noureddine	MCA	Université de Boumerdès	Examinateur

2021/2022

Remerciements

On remercie tout d'abord ALLAH le tout puissant de nous avoir donné le courage, la force et la patience d'achever ce modeste travail.

Nos remerciements chaleureux à notre promotrice Madame MESSAOUDI Samia née BELKACEM, pour son soutien, et avant tout pour nous avoir proposé un sujet très intéressant.

On aimera également remercier les membres de jury qui nous feront l'honneur d'évaluer notre travail.

Dédicace

Louange à Dieu tout puissant, qui m'a permis de voir ce jour tant attendu

Je dédie ce travail :

A mon chère papa « Ibrahim » que dieu lui fasse miséricorde.

A ma chère maman « Malika » qui a été à mes côtés durant mon parcours scolaire et surtout au cour de réalisation de mémoire, elle m'a trop encouragé tu as toujours été pour moi un exemple de la mère parfaire,tu été aussi mon père après son décès je tiens à honorer la femme que tu es. Je voudrais te remercier pour ton amour, ta gentillesse, ta générosité, ta compréhension... Ton soutien fut une lumière dans tout mon parcours. Aucune dédicace ne saurait exprimer l'amour l'estime et le respect que j'ai toujours eu pour toi.
Ce modeste travail est le fruit de tous les sacrifices que tu as déployés pour mon éducation et ma formation. Je t'aime maman et j'implore le tout-puissant pour qu'il t'accorde une bonne santé et une vie longue et heureuse.

A mes frères Amer, Mouloud et Malek je les remercie pour leur amour, leur confiance, leurs conseils ainsi que leur soutien inconditionnel qui m'a permis de réaliser les études pour lesquelles je me destine et par conséquent ce mémoire.

A ma chère cousine BAOUALI Ratiba Maitre Conférencesdans l'université de Bab-Ezzouar qui m'a aidé lors de la réalisation de ce mémoire.

A Oussama Laouadi qui m'a aidé à réaliser la partie de pratique de ce mémoire.

A mes amies : Rania, Fatima,Feriel,et Safa je voudrais exprimer ma reconnaissance envers eux carelles m'ont apporté leur soutien moral et intellectuel tout au long de ma démarche.

Feriel

Dédicace

Je dédie ce travail :

A mes plus chers : la personne qui m'aimait et m'encourageait à étudier et voulait que je sois toujours au top, mon très cher père.

A la personne qui a travaillé dur avec moi et qui a terminé mon parcours académique avec moi ma chère mère.

A tous mes frères et mes sœurs.

A mon futur mari, et bien sûrà toute la famille BOUTIH et ma belle-famille GHOUMRASSI.

Hamida

Liste des abréviations

AES : Advanced Encryption Standard.

DES : Data Encryption Standard.

FFT : Fast Fourier Transform.

HTTP :hyperText Transfer Protocol.

IDEA :IDE (Integrated Development Environment) for Java.

IRM : Imagerie Par Résonance.

MPEG : Moving Picture Experts Group.

NIST : NationalInstitue of Standards and Technology.

NPCR : Number of Pixels Change Rate.

NSA : National Security Agency.

PGP : Pretty Good Privacy.

RGB : Red, Green, Blue**.**

RSA : Rivest–Shamir–Adleman.

RVB : Rouge, Vert, Bleu.

S/MIME : Secure/Multipurpose Internet Mail Extensions.

SSH : Secure Shell.

SSL : Secure Sockets Layer.

SIM : Subscriber Identity Module.

TLS : Transport Layer Security.

UACI : Unified Average Changing Intensity.

ملخص

مع التطور السريع لاستخدام الصور الرقمية في العديد من المجالات، أصبح من الضروري حماية بيانات الصور السرية من الوصول غير المصرح به. في هذا العمل، استخدمنا خوارزمية تشفيرآر إس إيه يمكن تطبيقها على الصور، وهي مبنية على نظام وخوارزمية لورينز الفائقة الفوضى. وتجري عمليات محاكاة رقميةفي ماطلاب لتوضيح أدائها من حيث الجودة والسلامة والحساسية.

الكلمات المفتاحية :صور رقمية، تشفير، أنظمة فوضوية، نظام فرط الفوضى، تقييم الأداء.

Abstract

With the rapid development of the use of digital images in many areas, it has become imperative to protect confidential image data from unauthorized access. In this work, we used an encryption algorithm that can be applied to images, it is based on Lorenz's hyperchaotic system and the RSA algorithm. Numerical simulations in MATLAB are performed to clarify its performance in terms of quality, safety and sensitivity.

Keywords: Digital images, encryption, chaotic systems, hyperchaotic system, performances evaluation.

Résumé

Avec le développement rapide de l'utilisation des images numériques dans de nombreux domaines, il est devenu impératif de protéger les données d'image confidentielles contre tout accès non autorisé. Dans ce travail, nous avons utilisé un algorithme de cryptage qui peut être appliqué aux images, il est basé sur le système hyperchaotique de Lorenz et l'algorithme RSA. Des simulations numériques en MATLAB sont effectuées pour clarifier ses performances en termes de qualité, sécurité et sensibilité.

Mots clés : Images numérique, cryptage, systèmes chaotique, système hyperchaotique, Evaluation de performances.

Table des matières

Liste des figures

Liste des tableaux

Introduction générale

Grace à l'évolution rapide d'Internet et de technologie informatique, des informations comme les images, sont transmises et stockées via Internet. Pour cela une attention croissante est accordée à la sécurité des images.

Le cryptage est la principale application de la cryptographie, est une méthode efficace pour sécuriser les images. Il effectue cette sécurité par des algorithmes et des valeurs secrètes appelées clé. **(Ferik,2020)**

Ces années, le cryptage a pris une place importante dans l'actualité à cause de propagation d'éventuelles cyberattaques visant à causer un dommage aux informations, ce qui permet de soulever les questions suivantes qui définissent la problématique de notre mémoire :

- Et ce que le cryptage est en mesure pour nous assurer la sécurité des images ?
- Quel est l'intérêt de système hyperchaotique dans le cryptage d'image ?

Afin de bien conduire notre travail, on tente de répondre à la problématique en définissant des hypothèses qui sont :

- Notre algorithme de cryptage d'image proposé est efficace et offre des performances.
- Les systèmeshyper chaotiques sont en mesure d'assurer un cryptage optimal pour les différentes attaques contre les images.

Notre mémoire consiste à mettre en œuvre un algorithme de cryptage d'image adéquat et robuste, basé sur le système hyper chaotique de Lorenz et l'algorithme Rivest–Shamir–Adleman (RSA), implémenté sous le logiciel MATLAB pour faire face aux menaces.

Le choix du thème de ce mémoire est dû à un thème d'actualité. Lecryptage a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité.

Ce mémoire est organisé comme suit :

Le premier chapitre présente un aperçu de deux sujets liés à notre sujet principal, dans le premier sujet nous présentons les concepts liés à l'image numérique, les types d'images existants et leur traitement. Alors que dans ledeuxième sujet nous présentons les bases de la cryptographie moderne et ses deux principaux types : les chiffrements symétriquesetasymétriques.

Le deuxième chapitre est consacré aux deux sujets, dont le premier sujet met le point sur les notions de base de systèmes chaotique, ses propriétés, ses différentes classes ainsi que ses cartes. Pour le deuxième sujet on donne une brève présentation sur les systèmes hyper chaotiques.

Le troisième chapitre commence par une description sur l'algorithme utilisé et un aperçu sur le logiciel utilisé « Matlab ». Puis nous présentons les résultats expérimentaux de cryptage sur différents types d'images. Enfin, nous terminons par un ensemble de tests faits dans le cadre de l'utilisation méthode de cryptage basée sur les systèmes hyperchaotique afin de faire ressortir son efficacité dans le cryptage d'images.

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

Chapitre 1 Généralités sur le cryptage d'images

1 Introduction

Ce chapitre se concentre sur le cryptage d'images, premièrement on va donner des généralités de traitement d'images. Dans la deuxième partie, nous abordons la thématique du cryptage, et puis on donne un aperçu sur les cryptosystèmes tout en définissant les méthodes de chiffrement les plus connus.

2 Généralités sur le traitement d'images

Dans cette section nous donnons quelques notions liées au domaine de traitement d'images.

2.1 Introduction au traitement d'image

Le traitement d'image est né de l'idée de la nécessité de remplacer l'observateur humain par la machine. L'image ou les signaux provenant des capteurs ont alors été numérisés pour pouvoir être traités par ordinateur.

Le traitement d'image étant une méthode qui permet d'effectuer certaines opérations sur une image, soit il transforme l'image (pour améliorer l'apparence, ou de la coder de manière plus compacte en vue d'une transmission) ou bien il extrait l'information (reconnaissance automatique de l'écriture manuscrite). [**1]**

2.2 L'évolution historique de traitement d'image

Sur la figure (1.1) nous donnons l'évolution historique de traitement d'images.

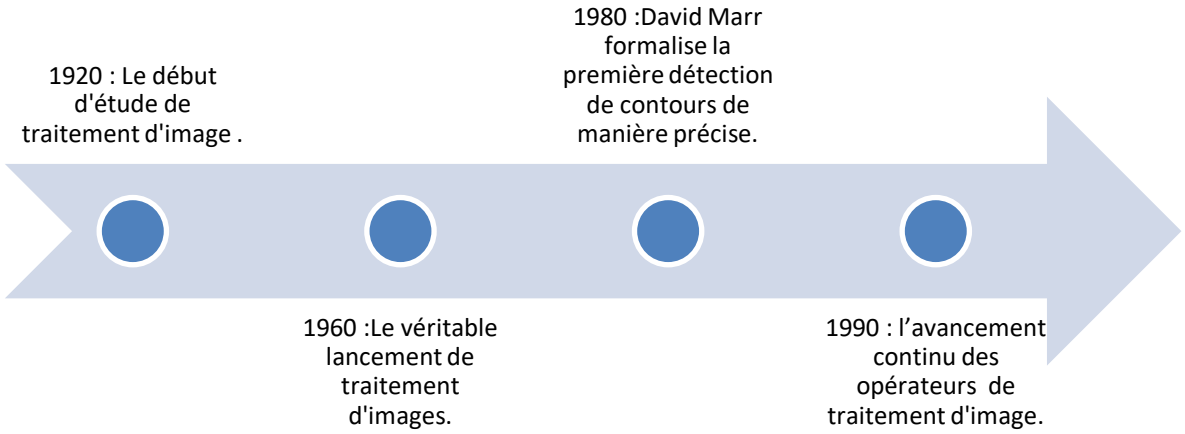


Figure 1. 1 : Chronologie de traitement d'image.

Le traitement d'images commence à être étudié dans les années 1920 pour la transmission d'images par le câble sous-marin allant de New York à Londres. Harry G. Bartholomew et Maynard D. McFarlane réalisent la première numérisation d'image avec compression de données pour envoyer des fax de Londres à New York.

Dans les années 1960 c'était le véritable lancement de traitement d'images, lorsque les ordinateurs commencent à être suffisamment puissants pour travailler sur des images. Peu après, la redécouverte de la transformée de Fourier rapide (FFT) révolutionne le domaine, en rendant envisageable les manipulations du contenu fréquentiel des signaux sur ordinateur. Cependant, la majeure partie des recherches porte toujours, à cette époque, sur le perfectionnement des images et leur compression.

En 1980, David Marr formalise la première détection de contours de manière précise. Au cours des années 1980, un véritable engouement se fait jour pour le traitement de l'image et en particulier pour la compréhension de l'image par des systèmes experts. Les ambitions étaient énormément trop grandes, l'échec fut d'autant plus cuisant.

Les années 1990 ont vu l'avancement continu des opérateurs. La recherche médicale devient un très gros demandeur en traitement d'images pour perfectionner les diagnostics faits à partir des nombreuses techniques d'imagerie médicale, la technique reine étant l'IRM. Les publicitaires, puis le grand public se familiarisent avec la retouche d'image grâce au logiciel

Photoshop, et le traitement d'images dans un objectif esthétique se répand avec la naissance d'autres logiciels dédiés. Enfin, la décennie se termine par une passion pour les ondelettes et les images multimodales.**[2]**

2.3 Qu'est-ce qu'une image ?

Plusieurs points de vue sont résumés ci-dessous **[3]**:

2.3.1 D'un point de vue humain

Une représentation d'une réalité portant plusieurs informations sémantiques.

2.3.2 D'un point de vue mathématique

Une image est une matrice de nombre représentant un signal.

2.3.3 D'un point de vue physique

Une image est définie comme une fonction bidimensionnelle, F(x,y) , où x et y sont des coordonnées spatiales, et l'amplitude de F à n'importe quelle paire de coordonnées (x,y) est appelée l' intensité de cette image. Lorsque x, y et les valeurs d'amplitude de F sont finies, nous l'appelons une image numérique.

Une image peut également être représentée en 3D dont les coordonnées sont x, y et z. Les pixels sont alors disposés sous la forme d'une matrice. C'est ce qu'on appelle une image RVB (ou RGB en anglais). Si l'image est en niveaux de gris, il n'y a qu'un seul canal : z = 1.**[4]**

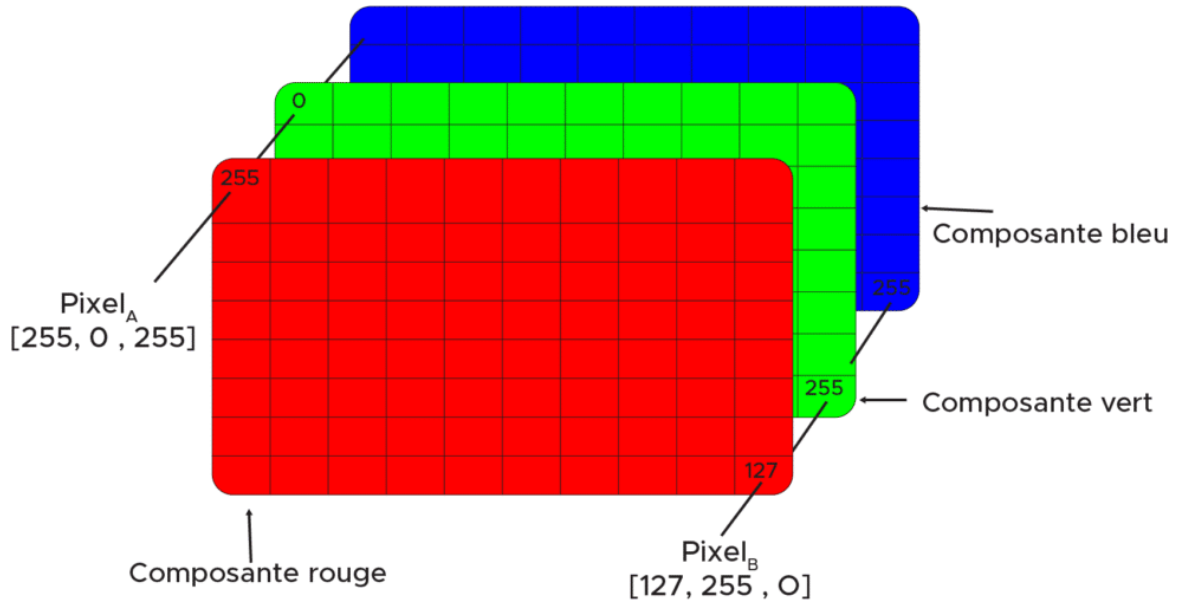


Figure 1. 2 : Illustration d'une image RVB.[4]

2.4 Les types d'image

Dans cette section on donne les types d'images **[5]** :

2.4.1 Image binaire (image noir et blanc)

L'image binaire, comme son nom l'indique, ne contient que deux éléments de pixel, c'est-à-dire 0 et 1, où 0 fait référence au noir et 1 au blanc. Cette image est également connue sous le nom de Monochrome.

2.4.2 Image couleur

Pour les images couleur il existe deux format dont :

- **Format couleur 8 bits**

C'est le format d'image le plus célèbre. Il contient 256 nuances de couleurs différentes et est communément appelé image en niveaux de gris. Dans ce format, 0 correspond au noir, 255 au blanc et 127 au gris.

- **Format couleur 16 bits**

Il s'agit d'un format d'image couleur. Il contient 65 536 couleurs différentes. Il est également connu sous le nom de High Color Format. Dans ce format, la répartition des couleurs n'est pas la même que celle de l'image en niveaux de gris.

Un format 16 bits est en fait divisé en trois autres formats qui sont le rouge, le vert et le bleu. Ce fameux format RVB.

2.5 Image numérique

L'image numérique est l'image dont la surface est divisée en éléments de tailles fixes appelés cellules ou pixels, ayant chacune comme caractéristique un niveau de gris ou de couleur prélevée à l'emplacement correspondant dans l'image réelle, ou calculé à partir d'une description interne de la scène à représenter. **(Saad, 2012)**

2.5.1 Caractéristique d'une image numérique

Le plus petit élément comportant une image appelé Pixel. Alors, une image est représentée sous forme d'un tableau qui contient un ensemble de pixels. L'image est unensemble structuré d'information caractérisée par plusieurs paramètres :**(Saad, 2012)**

2.5.2 Dimension

La représentation de l'image est une matrice dont les éléments sont des valeursnumériques, donc la multiplication du nombre de ligne par le nombre de colonnes nousdonnera la taille de l'image en pixels.

2.5.3 Résolution

La résolution est exprimée en nombre de pixels par unité de mesure (pouce ou Centimètre) On utilise aussi le mot résolution pour désigner le nombre total de pixels estaffichable horizontalement ou verticalement sur un moniteur. Plus le nombre de pixels estgrand plus la résolution est meilleure.

- 1 pouce = 2.54 centimètre.

- Une faible résolution indique une mauvaise qualité de l'image, par contre si on augmente le nombre de pixel dans chaque unité de mesure la clarté de l'image est améliorée.

2.5.4 Luminance

Lequotient de l'intensité d'une surface par l'aire apparente de cette surface, pour un observateurlointain, le mot luminance est substitué au mot brillance, qui correspond à l'éclat

d'un objet.La luminance (brillance) d'une image numérique en niveau de gris est définie comme la moyenne des pixels de l'image :

$$L(I) = \frac{1}{M*N} \sum_{x=o}^{M-1} . \sum_{y=0}^{N-1} f(x,y) \quad (1.1)$$

Avec **:** M : nombre de colonnes.

N : nombre de lignes.

f(x, y) : la valeur de niveau de gris du point(x, y).

2.5.5 Contraste

Le contraste est défini en fonction des luminances entre deux zones d'image, plusprécisément entre les régions sombre et les régions claires de cette image. Si L1 et L2 sont lesdegrés de luminosité respectivement de deux zones voisines A1 et A2 d'une image, lecontraste C est défini par le rapport :

$$C = \frac{L1-L2}{L1+L2} \quad (1.2)$$

2.5.6 Contour

Les contours présentent les frontières entre les objets de l'image ou la limite entre deuxpixels dont le niveau de gris représente une différence significative.

2.6 Notion d'histogramme

Il y a plusieurs notions sur l'histogramme notamment :

2.6.1 Définition

L'histogramme est une représentation visuelle des zones de lumière d'une image.**[6]**

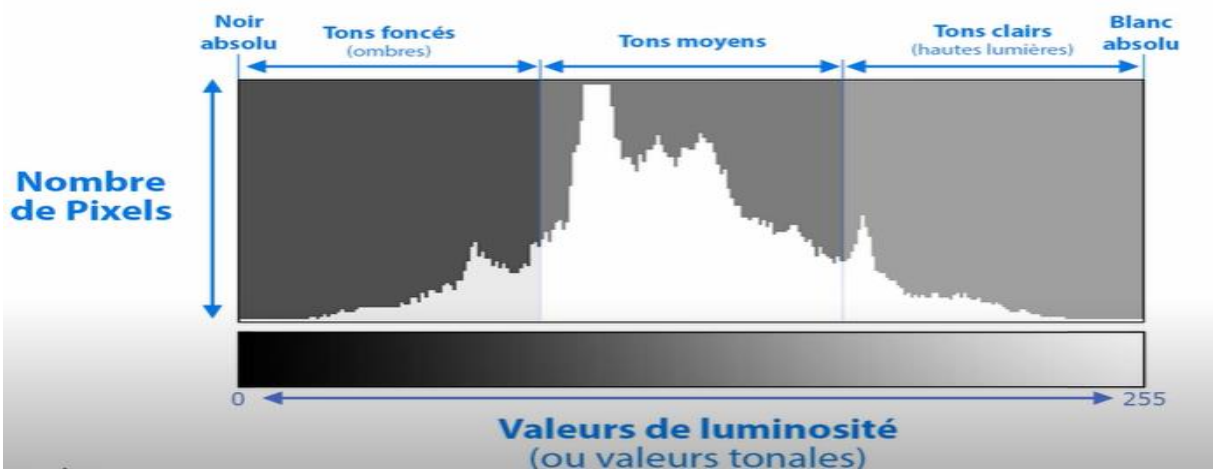


Figure 1. 3 : L'histogramme. [6]

2.6.2 Histogramme des images

Si l'image est sous exposée au très sombre, on va avoir un histogramme concentré sur la gauche c'est-à-dire au niveau des tons foncés comme le montre la figure ci-dessous.

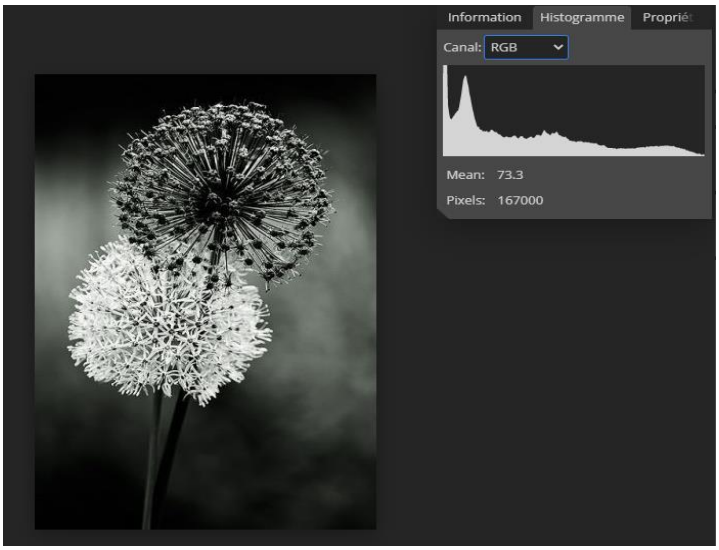


Figure 1. 4 : histogramme d'une image sombre.

Si l'image est sous exposée au très lumineuse, on va avoir un histogramme concentré sur la droite c'est-à-dire au niveau des tons clairs comme le montre la figure (1.5) :

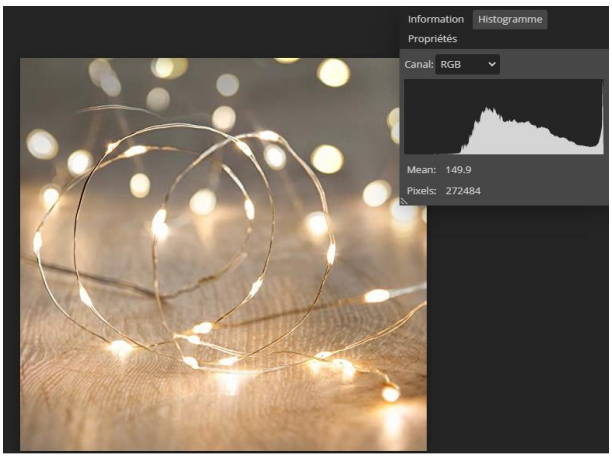


Figure 1. 5 : histogramme d'une photo lumineuse.

Si l'image est encouleur on va avoir un histogramme qui affiche la moyenne de luminosité combinée des couches RGB comme le montre la figure ci-dessous :

Figure 1. 6 : Histogramme d'une image en couleur.

Si l'image est chiffrée on va avoir un histogramme assez uniforme ce qui rend difficile d'extraire les pixels nature statistique de l'image en claire comme le montre la figure ci-dessous :

(a)Image en claire

(b) Image cryptée

(c) Histogramme de l'image clair

(d) Histogramme de l'image cryptée

Figure 1. 7 Histogramme de l'image cryptée.

Se référant aux résultats obtenus, nous pouvons clairement voir que l'image en claire diffère largement de celui correspondant cryptée.

2.6.3 Types d'histogrammed'image

Les types d'histogramme peuvent être variés selon le nombre de pic : **(Saad,2012)**

2.6.3.1 Histogramme uni-modal

Ce type d'histogramme n'a qu'un seul pic, il présente soit un objet soit un fond.

2.6.3.2 Histogramme bi-modal

Il est formé de deux modes bien séparés (deux pic séparés par une vallée) et l'on déduit ainsi qu'il existe un objet sur un fond.

2.6.3.3 Histogramme multi-modal

Il est formé de plusieurs modes séparés (plusieurs pics séparés par plusieurs vallées) qui nous renseigne sur la présence de plusieurs objets.

2.7 Phases de traitement d'image

Le traitement d'image passe par plusieurs phases dont:**[5]**

2.7.1 Acquisition

Consiste au passage de la scène de la forme physique à la forme numérique.

2.7.2 Amélioration d'image

C'est la modification de l'image dans le but de la rendre plus agréable à l'œil

2.7.3 Restauration d'image

Correction des défauts dus à une source de dégradation.

2.7.4 Traitement d'image couleur

Il traite des pseudo-couleurs et des modèles de couleur de traitement d'image en couleur applicables au traitement d'image numérique.

2.8 Domaines applicatifs

Les exemples et domaines d'applications du traitement d'image sont très nombreux. Les deux principaux domaines qui ont permis au traitement d'image de se développer sont :**[7]**

2.8.1 Le domaine militaire

- Dispositif de reconnaissance automatique de la cible.
- Missiles en tous genres
- Le renseignement (télédétection à partir d'images satellite dont la précision peut aller aujourd'hui jusqu'à quelques centimètres, ou aériennes, la photo-interprétation),
- Les simulateurs « réels » (de vol avion, de char, etc.),

2.8.2 Le domaine médical

- Angiographie, radiographie, échographie, scanner, IRM, etc.

Mais, une multitude d'applications apparaissent dans des domaines divers comme :

2.8.3 Le domaine industriel

- Le contrôle de la qualité des produits en bout de chaîne (état de surface, dimensionnement, forme, couleur, présence des comprimés par exemple dans l'industrie pharmaceutique),
- Le contrôle non destructif.
- Les manipulations automatiques par des robots (« pick and place » : récupération sur un tapis roulant pour mise en sachet ou dans un conteneur) y compris dans l'industrie alimentaire en plus du contrôle de la composition, de la fraîcheur, etc.

2.8.4 Le domaine du multimédia

- La compression dont Elle connaît une grande expansion avec le développement d'Internet et de la télévision numérique, aussi la décompression pour la transmission d'images ou le stockage.

- La TV haute définition (Standard MPEG4), le coloriage des dessins animés, des vieux films N&B.

- Le remplacement des panneaux publicitaires dans des retransmissions sportives.

En passant par de nombreux domaines dont :

2.8.5 L'imagerie civile satellitaire et aérienne

- La météorologie : les prévisions à partir des images du satellite Météosat en estimant les déplacements futurs des fronts nuageux, la cartographie, etc.

2.8.6 La reconnaissance de caractères, de documents

- Le photocopieur intelligent, capable d'analyser le document et de séparer zones de texte, de dessins et graphiques, d'images et de les traiter différemment, de déterminer les directions principales et ainsi de pouvoir redresser la copie d'un original posé de travers.

- L'archivage de documents renseignés tels que les documents à remplir de la Sécurité Sociale ou des Caisses d'Allocations Familiales : comprend le contenu, et met à jour le dossier dans la base de données.

- Traitement automatique du courrier : reconnaissance automatique de l'adresse (Code postal).

3 Concepts de base sur le cryptage

Dans cette section on va donner quelques concepts de base concernant la cryptographie :

3.1 Généralités sur le cryptage

La cryptographie est l'étude de techniques mathématiques liées à la sécurité d'information afin de pouvoir garantir leur confidentialité, leur intégrité, leur authenticité et leur non répudiation. Lacryptographie consiste notamment en l'élaboration de schémas de chiffrement/déchiffrement oucryptosystème pratiquée par des cryptographes.

En cryptographie, l'information à masquer est également appelée message ou texte en clair (en anglais plaintext). Le résultat du chiffrement d'un texte en clair est appelé texte chiffré (en anglais ciphertext) ; le texte chiffré est le résultat d'une transformation dépendant du message et d'une clé. Grâce à la cryptographie, tout type d'information numérique (texte, données, parole ou images) peut être chiffré de sorte que seules les personnes détenant la bonne clé puissent le déchiffrer. **(Rimani,2021)**

Les différents processus de la cryptographie sont illustrés par la figure suivante :

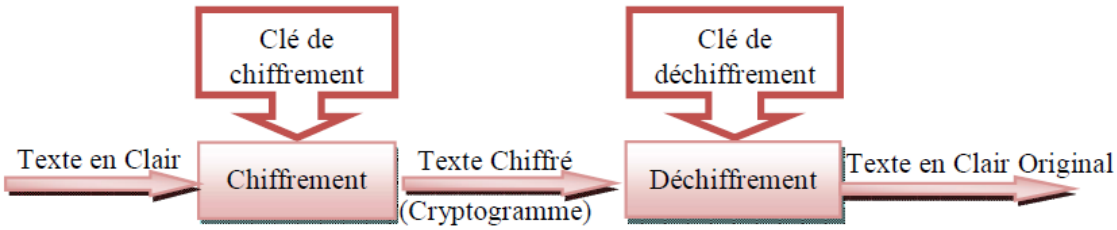


Figure 1. 8: Processus de Chiffrement et Déchiffrement. (Rimani,2021)

3.2 Définitions

Il y a plusieurs terminologies sur le cryptage notamment **[8]**:

3.2.1 Cryptologie

Etude à la protection de l'information sous forme numérique contre des accès ou manipulations non-autorisés. La cryptologie c'est de la cryptographie plus la cryptanalyse.

3.2.2 Cryptographie

La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.

3.2.3 Cryptanalyse

Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.

3.2.4 Le cryptage

Le cryptage est une forme de sécurité des données dans laquelle les informations sont converties en texte chiffré. Seules les personnes autorisées qui possèdent la clé peuvent déchiffrer le code et accéder aux informations originales en clair.

3.2.5 Clé de cryptage

On appelle clé une valeur utilisée dans un algorithme de cryptographie, afin de chiffrer une donnée. Il s´agit en fait d´un nombre complexe dont la taille se mesure en bits. On peut imaginer que la valeur numérique correspondant à 1024 bits est absolument grande. Aussi c'est une suite de caractères aléatoires, qui peut être divisée en plusieurs parties ou sections. D'une manière générale, plus la clé de cryptage est longue plus il est difficile de décoder un message.**[9]**

La clé de cryptage doit être strictement protégée, et c'est l'objectif le plus important de tous les protocoles de cryptage. **[10]**

3.2.6 Coder/ décoder

C'est une méthode ou un algorithme permettant de modifier la mise en forme d'un message sans introduire d'élément secret.

3.3 Le fonctionnement de cryptage

Pour pouvoir déchiffrer des données cryptées, un utilisateur doit disposer d'une clé. Avec la bonne clé, on ouvre la bonne serrure, et le déchiffrement s'opère. A l'inverse, si une personne tente de déchiffrer des données avec une mauvaise clé, elle ne pourra pas lire les données.**[11]**

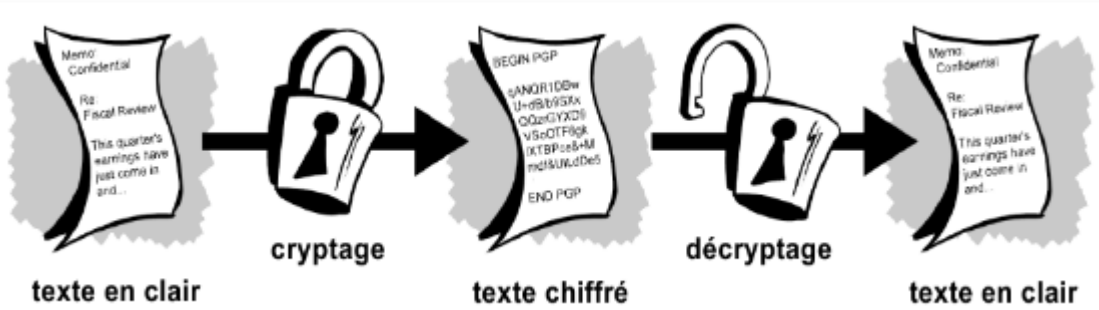


Figure 1. 9 : Cryptage et décryptage. [8]

3.4 Les avantages du cryptage

Le chiffrement est devenu un atout énorme pour les organisations, leur permettant d'offrir en toute confiance une expérience plus sécurisée pour les employés, les clients et les autres parties prenantes, on peut citer comme avantage : **[11]**

3.4.1 Confidentialité et sécurité

Le cryptage peut empêcher les violations de données. Même si un attaquant accède de manière malveillante à un réseau, si un appareil est crypté, l'appareil sera toujours sécurisé, rendant les tentatives de l'attaquant de consommer les données inutiles. Le cryptage garantit que personne ne peut lire les communications ou les données, à l'exception du destinataire prévu ou du propriétaire des données. Cela empêche les attaquants d'intercepter et d'accéder aux données sensibles.

3.4.2 Règlements

Le cryptage des données permet aux organisations de protéger les données et de maintenir la confidentialité conformément aux réglementations de l'industrie et à la politique gouvernementale. De nombreux secteurs, en particulier ceux des services financiers et de la santé, ont des règles explicites sur la protection des données. Par exemple, la loi Gramm-Leach-Bliley oblige les institutions financières à faire savoir aux clients comment leurs données sont partagées et comment leurs données restent protégées. Le cryptage aide les institutions financières à se conformer à cette loi.

3.4.3 Navigation Internet sécurisée

Le cryptage protège également les utilisateurs lorsqu'ils naviguent sur Internet. Plus tôt dans l'histoire d'Internet, les attaquants ont trouvé des moyens de voler des informations non chiffrées envoyées entre les utilisateurs et les services Web via le protocole de transfert hypertexte (HTTP). La norme pour chiffrer le contenu Web en exécutant HTTP sur le protocole Secure Socket Layer est apparue, bientôt remplacée par le protocole Transport Layer Security, permettant aux entreprises, aux éditeurs et aux fournisseurs de commerce électronique d'offrir une expérience sécurisée aux utilisateurs.

Avec le cryptage, les utilisateurs se sentent plus en sécurité en saisissant des informations personnelles sur des pages Web et en effectuant des transactions financières ou de commerce électronique.

3.4.4 Protection des données sensibles

Le cryptage continuera d'être une fonctionnalité de sécurité essentielle dans tout, des chats vidéo au commerce électronique en passant par les médias sociaux. Fondamentalement,

s'il peut être partagé ou stocké, il sera crypté. Les organisations et les utilisateurs individuels gagneraient à se tenir au courant des normes de cryptage pour s'assurer que leurs données personnelles et professionnelles sont à l'abri d'une utilisation abusive ou d'une compromission.

3.5 Les inconvénients de cryptage

Bien que le chiffrement soit conçu pour empêcher les entités non autorisées de comprendre les données qu'elles ont acquises, dans certaines situations, le chiffrement peut empêcher le propriétaire des données d'accéder également aux données.

La gestion des clés est l'undes plus grands défis de l'élaboration d'une stratégie de chiffrement d'entreprise, car les clés permettant de déchiffrer le texte chiffré doivent se trouver quelque part dans l'environnement, et les attaquants ont souvent une assez bonne idée de l'endroit où chercher.

Il existe de nombreuses bonnes pratiques pour la gestion des clés de chiffrement. C'est juste que la gestion des clés ajoute des couches supplémentaires de complexité au processus de sauvegarde et de restauration. Si un sinistre majeur devait survenir, le processus de récupération des clés et de leur ajout à un nouveau serveur de sauvegarde pourrait augmenter le temps nécessaire pour démarrer l'opération de récupération.

La mise en place d'un système de gestion des clés ne suffit pas. Les administrateurs doivent proposer un plan complet pour protéger le système de gestion des clés. En règle générale, cela signifie le sauvegarder séparément de tout le reste et stocker ces sauvegardes de manière à faciliter la récupération des clés en cas de sinistre à grande échelle. **[12]**

4 Généralités sur le cryptosystème

Dans cette section nous donnons des généralités sur les systèmes de cryptage.

4.1 Introduction au cryptosystème

Un cryptosystème est un concept essentiel pour la sécurité des informations vitales sur Internet. Toute information personnelle urgente est transmise via un serveur sécurisé, puis cryptée ou codée. La personne qui reçoit les informations doit disposer du système approprié pour décoder ou déchiffrer les informations. Les informations telles que les noms, adresses,

numéros de cartes de crédit et de sécurité sociale sont souvent protégées en utilisant au moins une forme de cryptosystème. Le mot cryptosystème est utilisé comme abréviation pour les termes système cryptographique.

Les cryptosystèmes sont généralement considérés comme le meilleur choix pour assurer la sécurité des informations vitales sur Internet. Les protocoles de sécurité tels que SSL, TLS et SSH reposent tous sur des cryptosystèmes et des primitives cryptographiques pour former la base de leur codage. La sécurité liée à l'utilisation de systèmes cryptographiques n'est pas totalement infaillible, car il existe des facteurs variables, notamment l'utilisateur, l'ordinateur, le réseau sur lequel les informations sont stockées et le serveur sur lequel elles sont partagées.

Avant l'avènement des ordinateurs et d'Internet, le mot cryptosystème était utilisé dans un contexte différent. Un cryptographe, ou quelqu'un qui utilise des codes secrets pour masquer des informations, créerait un ensemble de trois algorithmes mathématiques. Un ensemble générerait les informations, un autre les chiffrerait et le troisième les déchiffrerait. Essentiellement, les informations utilisées en cryptographie seraient «brouillées» deux fois et non brouillées une fois.

Parmi Les techniques cryptographiques les plus sûres sont les algorithmes. Ces algorithmes de bas niveau sont construits et recréés pour établir un code qui ne peut être cassé que d'un certain nombre de façons. Plus le nombre de manières de résoudre un cryptosystème est faible, plus la cryptographie est considérée comme étant sûre.

Comme ce terme est utilisé parmi les agents de sécurité informatique et les cryptographes, une publication populaire des professionnels de la sécurité Internet, Internet Security Glossary, suggère que le terme cryptosystème ne doit pas être utilisé avec la sécurité Internet pour éviter toute confusion. Plutôt que d'utiliser ce terme, le glossaire de la sécurité Internet suggère d'utiliser les termes cryptographie ou cryptographie. Malgré les recommandations de la publication, de nombreuses personnes continuent à utiliser le mot cryptosystème pour désigner à la fois des codes informatisés et des codes non informatisés. **[13]**

4.2 Définition d'un cryptosystème

Un cryptosystème est une suite d'algorithmes cryptographiques nécessaires pour mettre en œuvre un service de sécurité particulier, tel que le cryptage. Le terme est une combinaison de système cryptographique, ce qui signifie un système informatique qui utilise la cryptographie, qui est une méthode de protection des informations et de la communication par code afin que seul l'utilisateur auquel les informations sont destinées puisse les lire. **[14]**

4.3 Les composants de base d'un cryptosystème

Les composants de base d'un cryptosystème comprennent: **[14]**

4.3.1 Texte clair

Les données à protéger lors de la transmission (le message à protéger).

4.3.2 Texte chiffré

Version brouillée du texte en clair produit par l'algorithme de chiffrement à l'aide d'une clé de chiffrement spécifique(c'est le résultat du chiffrement du texte en clair.).

4.3.3 Chiffrement

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

4.3.4 Algorithme de chiffrement

Processus mathématique qui utilise un algorithme pour transformer des informations en texte chiffré sans signification et nécessite l'utilisation d'une clé pour transformer les données dans leur forme d'origine.

4.3.5 Clé de chiffrement

Valeur connue de l'expéditeur. L'expéditeur entre la clé de chiffrement dans l'algorithme de chiffrement avec le texte en clair pour calculer le texte chiffré.

4.3.6 Déchiffrement

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

4.3.7 Algorithme de déchiffrement

Processus mathématique qui produit du texte en clair pour tout texte chiffré et clé de déchiffrement donnés. Le texte chiffré et une clé de déchiffrement sont l'entrée, le texte brut est la sortie.

4.3.8 Clé de déchiffrement

Valeur connue du destinataire. Il est lié à la clé de chiffrement, mais pas toujours identique à celle-ci. Le récepteur entre la clé de déchiffrement dans l'algorithme de déchiffrement avec le texte chiffré pour calculer le texte en clair.

4.4 Les différents types de cryptosystème

On peut regrouper les systèmes de chiffrement en deux catégories comme la figure ci-dessous indique :**(Belkadi,2018)**

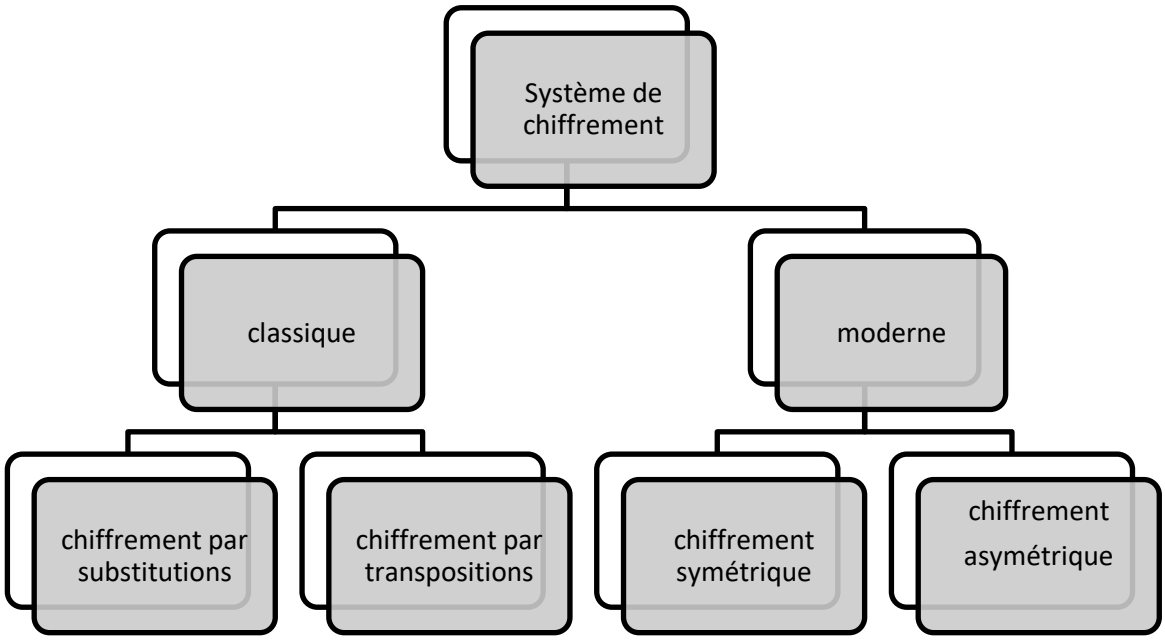


Figure 1. 10 : Principe de systèmes de chiffrement.

4.4.1 Description de systèmes cryptographiques classiques

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

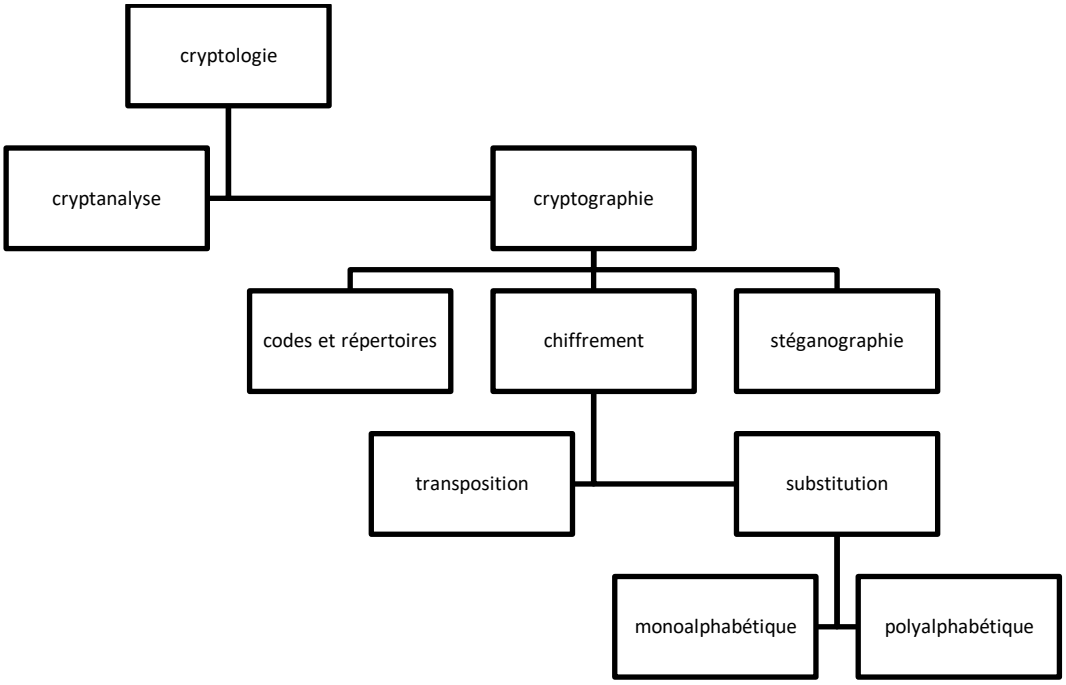


Figure 1. 11 : Domaines inclus dans la cryptologie.

4.4.1.1 Algorithme de substitution

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

On distingue généralement plusieurs types de cryptosystèmes par substitution :

a. Substitution mono-alphabétiques

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

b. Substitution poly-alphabétique

Consiste à utiliser une suite de chiffres mono alphabétiques réutilisée périodiquement.

4.4.1.2 Algorithme de transposition

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

Dans ces méthodes de chiffrement, le plus souvent est d'utiliser deux visions géométriquement différentes du texte :

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

- On écrit le texte longitudinalement sur la bandelette ainsi enroulée.

Figure 1. 12 : Scytale. (Belkadi, 2018)

✓ Pour décrypter le message il faut un cylindre du bon diamètre.

4.4.2 Système cryptographiques modernes

La cryptographie moderne est distinguée en deux types et se situe entre les chiffrements de type symétrique et ceux de type asymétrique :

4.4.2.1 Chiffrement à clé symétrique

Un système de cryptage dans lequel l'expéditeur et le destinataire d'un message partagent une seule clé commune qui est utilisée pour crypter et décrypter le message.**[15]**

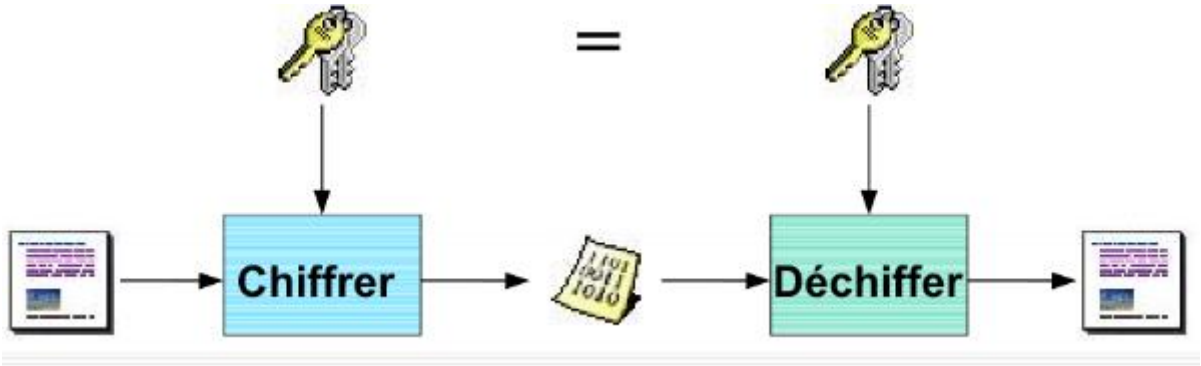


Figure 1. 13 : Chiffrement à clé symétrique.[9]

- **Types de chiffrement à clé symétrique**

Quelques algorithmes de chiffrement symétrique très utilisés :**[12]**

Chiffrement DES

Est une méthode de cryptage de données à clé symétrique obsolète. DES fonctionne en utilisant la même clé pour chiffrer et déchiffrer un message, de sorte que l'expéditeur et le destinataire doivent connaître et utiliser la même clé privée. DES a été remplacé par l'algorithme AES plus sécurisé.

Chiffrement AES

Est un chiffrement par bloc symétrique choisi par le gouvernement américain pour protéger les informations classifiées ; il est implémenté dans des logiciels et du matériel dans le monde entier pour chiffrer les données sensibles. Le NIST a commencé le développement d'AES en 1997 lorsqu'il a annoncé la nécessité d'un algorithme successeur pour le Data Encryption Standard (DES), qui commençait à devenir vulnérable aux attaques par force brute .

4.4.2.2 Chiffrement de clé asymétrique

Un système de cryptage dans lequel différentes clés sont utilisées pour le cryptage et le décryptage, les clés étant mathématiquement liées. Chaque partie a sa propre paire de clés échangées lors de la transmission. **[14]**

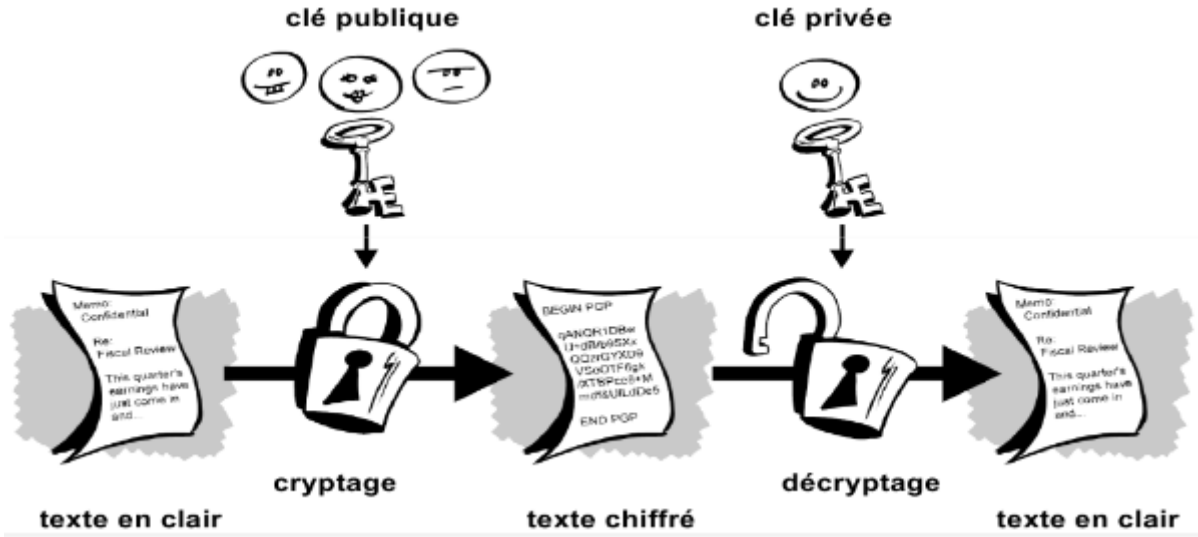


Figure 1. 14 : Chiffrement de clé asymétrique. [8]

- **Types de chiffrement à clé asymétrique**

Quelques algorithmes de chiffrement asymétrique très utilisés :**[12]**

Chiffrement RSA

Le chiffrement RSA (nommé par les initiales de ses trois inventeurs) est un algorithme de cryptographie asymétrique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. De nombreux protocoles, comme Secure Shell (SSH), OpenPGP, Secure/Multipurpose Internet Mail Extensions (S/MIME) et Secure Sockets Layer (SSL /TLS), s'appuient sur RSA pour les fonctions de cryptage et de signature numérique .

Diffie-Hellman (l'échange de clés)

Egalement appelé échange de clés exponentiel, est une méthode de chiffrement numérique qui utilise des nombres élevés à des puissances spécifiques pour produire des clés de déchiffrement sur la base de composants qui ne sont jamais directement transmis, ce qui rend la tâche d'un briseur de code potentiel mathématiquement écrasante.

5 Types d'attaques

Les attaquants continueront d'attaquer même s'ils savent que les données ou les appareils sont cryptés. Ils pensent qu'avec un peu d'effort, ils pourraient passer. Pendant de nombreuses années, les mots de passe faibles ont incité les attaquants à continuer d'essayer, car certains logiciels sophistiqués pourraient tôt ou tard découvrir les mots de passe. **[11]**

On distingue, les différents types d'attaques en fonction des données supposés connues par les attaquants **(Rimani,2021)** :

5.1 Attaque à texte chiffré seulement (Ciphertextonlyattack)

Consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés. L'attaquant ou (l'adversaire) a connaissance du texte chiffré de plusieurs messages ;alors iltente de déduire la clé secrète ou le texte clair en observant seulement le texte chiffré.

5.2 Attaque à texte en clair connu (knownplaintextattack)

Consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, connaissant le texte en clair correspondant. Le cryptanalyste a non seulement accès aux textes chiffrés de plusieurs messages mais aussi aux textes en clairs correspondants. La tâche est de

retrouver la ou les clé(s) utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer n'importe quel nouveau message chiffré avec la même clé.

5.3 Attaque à texte en clair choisi (chosenplaintextattack)

Consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, l'attaquant ayant la possibilité de les générer à partir de textes en clair. Non seulement le cryptanalyste a accès aux textes chiffrés et aux textes en clair mais de plus il peut choisir les textes en clair à chiffrer. Cette attaque est plus efficace que l'attaque à texte en clair connu car le cryptanalyste peut choisir des textes en clair spécifiques qui donneront plus d'informations sur la clé.

5.4 Attaque adaptative à texte en clair choisi (adaptive chosenplaintextattack)

C'est un cas particulier de l'attaque à texte en clair choisi. Non seulement le cryptanalyste peut choisir les textes en clair mais il peut également adapter ses choix en fonction des textes chiffrés précédents. Dans une attaque à texte en clair choisi, le cryptanalyste est juste autorisé à choisir un grand bloc de texte en clair au départ tandis que dans une attaque à texte en clair adaptative, il choisit un bloc initial plus petit et ensuite il peut choisir un autre bloc en fonction du résultat pour le premier et ainsi de suite (le choix du texte clair peut dépendre du texte chiffré reçu précédemment).

5.5 Attaque à texte chiffré choisi (chosenciphertextattack)

Consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, l'attaquant ayant la possibilité de les générer à partir de textes en clair. Lecryptanalyste peut choisir différents textes chiffrés à déchiffrer. Les textes déchiffrés lui sont alors fournis. Par exemple, le cryptanalyste a un dispositif qui ne peut être désassemblé et qui fait du déchiffrement automatique, sa tâche est de retrouver la clé.

5.6 Attaque adaptative à texte chiffré choisi (adaptive chosenciphertextattack)

Cette attaque est une attaque à texte chiffré choisi où le choix du texte chiffré peut dépendre du texte en clair reçu précédemment.

5.6 Attaque exhaustive ou attaque par force brute (brute force attack)

L'attaquant essaie toutes les combinaisons possibles des clés jusqu'à l'obtention d'un texte clair. Cette attaque est la plus coûteuse en temps de calcul et en mémoire à cause de la recherche exhaustive. Une attaque par force brute va essayer toutes les clés possibles de clé afin de trouver la bonne. Un peu comme quelqu'un qui tenterait d'ouvrir un cadenas en essayant toutes les combinaisons. Cette action peut être empêchée par l'utilisation de chiffrement plus complexe, comme l'AES-256. Avec ce cryptage utilisant une clé de 256 bits, il faudrait des années à une attaque de force brute pour décrypter les données. La plupart des VPN utilisent l'AES-256 comme norme de cryptage, pour une sécurité optimale.

5.7 Attaques physiques

Le principe de ces attaques est d'essayer de reconstituer la clef secrète par exemple en écouter la transmission entre le clavier de l'ordinateur et l'unité centrale ou en mesurant la consommation électrique du microprocesseur qui effectue le décodage du message ou encore en mesurant son échauffement.

6 Application du cryptage

La cryptographie est utilisée aujourd'hui dans de nombreuses applications : **[15]**

6.1 Signatures numériques

L'authentification est tout processus par lequel on prouve et vérifie certaines informations. Parfois, on peut vouloir vérifier l'origine d'un document, l'identité de l'expéditeur, l'heure et la date à laquelle un document a été envoyé et/ou signé, l'identité d'un ordinateur ou d'un utilisateur, etc. Une signature numérique est un moyen cryptographique par lequel bon nombre d'entre eux peuvent être vérifiés. La signature numérique d'un document est une information basée à la fois sur le document et sur la clé privée du signataire. Il est généralement créé à l'aide d'une fonction de hachage et d'une fonction de signature privée (algorithmes qui créent des caractères encryptés contenant des informations spécifiques sur un document et ses clés privées).

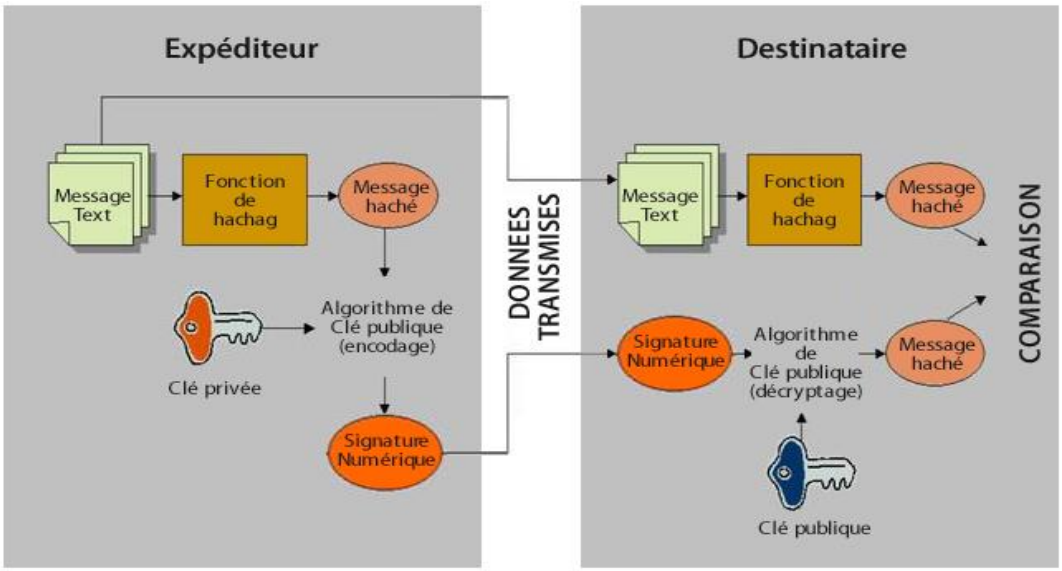


Figure 1. 15 : Fonctions hachage et signature privée. [16]

6.2 Horodatage

L'horodatage est une technique qui peut certifier qu'un certain document ou une communication électronique a existé ou a été livré à un certain moment. L'horodatage utilise un modèle de cryptage appelé schéma de signature aveugle. Les schémas de signature aveugle permettent à l'expéditeur d'obtenir un message reçu par une autre partie sans révéler aucune information sur le message à l'autre partie.

L'horodatage est très similaire à l'envoi d'une lettre recommandée par la poste américaine, mais fournit un niveau de preuve supplémentaire. Il peut prouver qu'un destinataire a reçu un document spécifique. Les applications possibles incluent les demandes de brevets, les archives de droits d'auteur et les contrats. L'horodatage est une application essentielle qui contribuera à rendre possible la transition vers les documents juridiques électroniques.

6.3 Monnaie électronique

La définition de la monnaie électronique (également appelée monnaie électronique ou monnaie numérique) est un terme qui évolue encore. Les principales crypto-monnaies telles que Bitcoin, Ethereum et Rippl. Il comprend les transactions effectuées par voie électronique avec un transfert net de fonds d'une partie à l'autre, qui peuvent être soit à débit, soit à crédit et peuvent être soit anonymes, soit identifiées. Il existe des implémentations matérielles et logicielles.

Les applications anonymes ne révèlent pas l'identité du client et sont basées sur des schémas de signature aveugle. Les schémas de dépenses identifiés révèlent l'identité du client et s'appuient sur des formes plus générales de schémas de signature. Les stratagèmes anonymes sont l'analogue électronique de l'argent liquide, tandis que les stratagèmes identifiés sont l'analogue électronique d'une carte de débit ou de crédit. Il existe également des approches hybrides où les paiements peuvent être anonymes vis-à-vis du commerçant mais pas de la banque ; ou anonymes pour tous, mais traçables (une séquence d'achats peut être liée, mais pas directement liée à l'identité du dépensier).

Le cryptage est utilisé dans les systèmes de monnaie électronique pour protéger les données de transaction conventionnelles telles que les numéros de compte et les montants des transactions, les signatures numériques peuvent remplacer les signatures manuscrites ou les autorisations de carte de crédit, et le cryptage à clé publique peut assurer la confidentialité. Il existe plusieurs systèmes qui couvrent cette gamme d'applications, des transactions imitant les transactions papier conventionnelles avec des valeurs de plusieurs dollars et plus, à divers systèmes de micropaiement qui regroupent des transactions à très faible coût en montants qui supporteront les frais généraux de cryptage et de compensation de la banque.

6.4 Cryptage/Décryptage dans les e-mails

Le cryptage des e-mails est une méthode de sécurisation du contenu des e-mails de toute personne extérieure à la conversation par e-mail cherchant à obtenir les informations d'un participant. Sous sa forme cryptée, un e-mail n'est plus lisible par un humain. Ce n'est qu'avec votre clé de messagerie privée que vos e-mails peuvent être déverrouillés et décryptés dans le message d'origine.

Le cryptage des e-mails fonctionne en utilisant ce qu'on appelle la cryptographie à clé publique. Chaque personne possédant une adresse e-mail possède une paire de clés associées à cette adresse e-mail, et ces clés sont nécessaires pour chiffrer ou déchiffrer un e-mail. L'une des clés est connue sous le nom de «clé publique» et est stockée sur un serveur de clés où elle est liée à votre nom et à votre adresse e-mail et accessible à tous. L'autre clé est votre clé privée, qui n'est partagée publiquement avec personne.

Lorsqu'un e-mail est envoyé, il est crypté par un ordinateur à l'aide de la clé publique et le contenu de l'e-mail est transformé en un brouillage complexe et indéchiffrable très

difficile à déchiffrer. Cette clé publique ne peut pas être utilisée pour déchiffrer le message envoyé, uniquement pour le chiffrer. Seule la personne disposant de la clé privée correspondante appropriée a la capacité de déchiffrer l'e-mail et de lire son contenu.

6.5 Cryptage dans WhatsApp

WhatsApp utilise le protocole "signal" pour le cryptage, qui utilise une combinaison d'algorithmes cryptographiques à clé asymétrique et symétrique. Les algorithmes à clé symétrique garantissent la confidentialité et l'intégrité tandis que les algorithmes cryptographiques à clé asymétrique aident à atteindre les autres objectifs de sécurité, à savoir l'authentification et la non-répudiation.

Whatsapp utilise l'algorithme basé sur Curve25519. L'histoire de Curve25519 mérite d'être notée car elle a été introduite après les inquiétudes concernant les allégations selon lesquelles certains paramètres des normes NIST P-256 précédemment répandues ont été manipulés par la NSA pour faciliter l'espionnage. L'algorithme EllipticCurveDiffieHellman est un algorithme mathématique qui aide deux entités communicantes à s'entendre sur un secret partagé sans s'envoyer les clés réelles.

6.6 Cryptage dans Instagram

L'interaction avec Instagram est probablement une communication cryptée. Lorsque votre téléphone demande des données avec instagram, il utilise SSL/TLS sur le port 443 pour crypter les demandes des serveurs Instagram et vous enverra des données sur le même flux de données cryptées. Cela empêche les parties malveillantes d'écouter la conversation entre vous et Instagram.

6.7 Authentification de la carte SIM

Authentification : Pour décider si la carte SIM peut ou non accéder au réseau, la carte SIM doit être authentifiée. Un nombre aléatoire est généré par l'opérateur et est envoyé à l'appareil mobile. Avec la clé secrète Ki, ce nombre aléatoire parcourt l'algorithme A3 (c'est ce Ki qui a récemment été compromis). La sortie de ce calcul est renvoyée à l'opérateur, où la sortie est comparée au calcul que l'opérateur a lui-même exécuté (l'opérateur possède les clés secrètes de toutes les cartes SIM distribuées par l'opérateur).

Cryptage : Cette partie est la partie qui a été fissurée. En bref, l'opérateur génère un nombre aléatoire (encore) et l'envoie au téléphone mobile. Avec la clé secrète Ki, ce nombre aléatoire parcourt l'algorithme A8 et génère une clé de session KC. Ce KC est utilisé, en combinaison avec l'algorithme A5 pour chiffrer/déchiffrer les données.

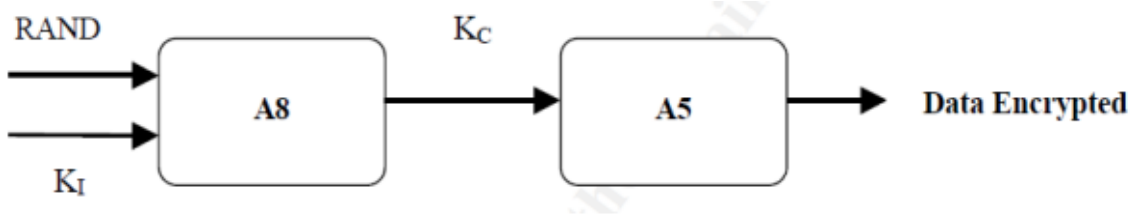


Figure 1. 16: Authentification de la carte SIM . [15]

6.8 Les opérations militaires

Les applications de la cryptographie dans l'armée sont bien connues. Les opérations militaires ont également largement utilisé la cryptographie pendant longtemps. Utilisés pour crypter les canaux de communication militaires, les dispositifs de cryptage militaires convertissent les vrais caractères de communication afin que les ennemis ne puissent pas connaître leurs plans à venir.

En termes simples, la cryptographie transmet en toute sécurité des messages d'un bout à l'autre sans laisser les forces ennemies intercepter le véritable sens. Il s'agit d'une application très importante de la cryptologie car elle peut être à la fois publique et privée.

À grande échelle, il peut être largement utilisé pour déclarer des guerres et envoyer des messages cruciaux sans l'intervention d'un messager. Contrairement aux temps traditionnels, cette technologie peut être utilisée avec précision pour renforcer la force militaire d'une nation.**[16]**

6.9 Les téléphones portables

Dans le cas des téléphones mobiles, la cryptographie est utilisée pour assurer la confidentialité des communications. En effet, la loi sur les télécommunications oblige les opérateurs à garantir la sécurité des communications des utilisateurs. En particulier dans le cas des téléphones mobiles, les communications entre le téléphone et la station hertzienne sont chiffrées. On utilise uniquement la cryptographie à clé secrète et l'algorithme de chiffrement est un algorithme par flot appelé A5. **[17]**

6.10 La télévisions à péage

La cryptographie est aussi utilisée dans le cas des télévisions à péage pour que seuls les usagers autorisés puissent avoir accès aux programmes. Ainsi, les programmes sont chiffrés et seuls les abonnés connaissent la clé de déchiffrement. De plus, la cryptographie permet aujourd'hui par exemple de détecter les décodeurs pirates mais, pour des raisons économiques, ces systèmes sont peu employés. **[17]**

6.11 Internet

La cryptographie permet de garantir la confidentialité de certaines communications comme la transmission du code d'une carte bleue (protocole SSL) ou d'assurer la confidentialité, l'intégrité et l'authentification de l'émetteur dans les messageries électroniques (protocole S/MIME) **[17]**

6.12 Cryptage de disque

Les programmes de chiffrement de disque chiffrent l'intégralité de votre disque dur afin que vous n'ayez pas à vous soucier de laisser des traces des données non chiffrées sur votre disque.PGP peut également être utilisé pour chiffrer des fichiers. Dans ce cas, PGP utilise la clé privée de l'utilisateur avec un mot de passe fourni par l'utilisateur pour chiffrer le fichier à l'aide d'IDEA. Le même mot de passe et la même clé sont utilisés pour déverrouiller le fichier. **[18]**

6.13 Les opérations bancaires

Les cartes bancaires possèdent trois niveaux de sécurité : **[19]**

Le code confidentiel : c'est la suite de chiffres à mémoriser et à saisir à l'abri des regards indiscrets.

La signature RSA : permet de vérifier l'identité de la carte sans avoir besoin de secrets; en d'autres termes, cette vérification peut se faire sans connexion à un centre distant.

L'authentification DES : apporte une preuve de légitimité de la carte, et se fait par connexion à un centre distant.

6.14 Communications réseau sécurisées (pour les navigateurs)

Les navigateurs ou broswers, tels que Mozilla Firefox ou Internet Explorer, utilisent le protocole de sécurité SSL (Secure Sockets Layers), qui repose sur un procédé de cryptographie par clé publique : le RSA.**[19]**

7 Conclusion

Dans ce chapitre nous avons évoqué le traitement d'image d'un côté, et d'un autre coté le cryptage d'image d'une façon générale. La première partie de ce chapitre est consacrée aux généralités de traitement d'image dont nous avons présenté des informations qui servent de fondement à la compréhension de cette partie. La deuxième partie de ce chapitre comportent des renseignements de façon particulière sur le cryptage, tel que les concepts de bases, les algorithmes de chiffrements et déchiffrements les plus utilisés.

Dans le chapitre suivant, nous allons présenter les systèmes chaotiques et hyper chaotiques.

Chapitre 2 Les systèmes chaotiques et hyper chaotiques

1 Introduction

Les systèmes dynamiques chaotiques sont inclus dans des applications effectives depuis la dernière décade malgré qu'elles soient connues depuis longtemps dans le domaine mathématique. **(Benayache,2020)**

Pour le comportement hyper chaotique il a été étudié dans différentes applications telles que : l'oscillateur de Colpitts, les circuits non-linéaires, les systèmes de communications et la synchronisation. Pour cela, la génération de ce comportement dynamique complexe devient un sujet de recherche très important. **(Rezzag, 2016)**

L'objectif de ce chapitre porte principalement sur deux volets majeurs. Dans le premier volet, les systèmes chaotiques sont étudiés. Dans l'autre volet, les systèmes hyper chaotiques sont considérés.

2 Les systèmes chaotiques

La théorie du chaos est un domaine des études en mathématiques, avec des applications dans plusieurs disciplines comme la physique, l'ingénierie, la biologie, l'économie, etc. La théorie du chaos étudie le comportement des systèmes dynamiques qui sont très sensibles aux conditions initiales. **(Bessam,2020)**

2.1 Historique

L'histoire récente des systèmes dynamiques commence vers le début du 20ème siècle par les travaux d'Henri Poincaré dans lesquels il propose des études qualitatives basées sur l'étude des points d'équilibre et des trajectoires périodiques, puis de leurs bassins d'attraction au lieu de chercher des solutions analytiques donnés par des formules (car pour la plupart des systèmes non-linéaires il est impossible de trouver de tel formules). Dans ses travaux H. Poincaré avais présenté la nature complexe (sensibilité aux conditions initiales) de certains systèmes dynamiques qui semblent être simples dans leurs formes. Par la suite, dans les

années 60 Edward Lorenz a établi le premier exemple de système d'équations différentielles simplifiées de trois variables seulement qui permettaient de déterminer l'évolution de masses d'air et dont la nature des solutions est complexe (premier système chaotique). **[20]**

2.2 Définitions

On présente quelques définitions concernant les systèmes chaotiques : **(Hannoun,2014)**

2.2.1 Systèmes dynamiques

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, ou encore les valeurs d'une fonction par rapport à la valeur de x.

2.2.2 Système dynamique (discret ou continu)

Décrit par une fonction mathématique présente deux types de variables : dynamiques et statiques. Les variables dynamiques sont les quantités fondamentales qui changent avec le temps. Les variables statiques, encore appelées paramètres du système, sont fixes.

2.2.3 Système dynamique linéaire

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 dernières vérifient alors les principes de proportionnalité des effets aux causes, et de superposition.

2.2.4 Système dynamique non linéaire

Un système non linéaire est un système 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 'y appliquent. Il n'y pas une théorie générale pour ces systèmes, mais plusieurs méthodes adaptées à certaines classes de systèmes non linéaires.

2.2.5 Systèmes chaotiques

On appelle un système dynamique chaotique, un système qui dépend de plusieurs paramètres et qui est caractérisé par une extrême sensibilité aux conditions initiales. Il n'est pas déterminé ou modélisé par des systèmes d'équations linéaires ni par les lois de la mécanique classique**. (Lakhdari,2020)**

C'est un système déterministe qui se distingue par son imprévisibilité. Un système linéaire ne peut pas être chaotique.

2.2.6 L'attracteur

Dans l'étude des systèmes dynamiques, un attracteur est un ensemble d'états vers lequel un système évolue de façon irréversible en l'absence de perturbations. Constituants de base de la théorie du chaos, au moins cinq types sont définis : ponctuel, quasi périodique, périodique, étrange et spatial. **[21]**

2.3 Propriétés

Il existe un ensemble de propriétés qui résument les caractéristiques observées dans les systèmes chaotiques tel que :

2.3.1 Non-linéarité

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

2.3.2 Non périodicité

Un système présentant un comportement chaotique évolue dans une orbite qui ne se répète jamais sur elle-même. C'est à dire, les orbites ne sont jamais périodiques. (Bessam,2020)

2.3.3 Le déterminisme et l'imprévisibilité

Dans le cas des systèmes déterministes, théoriquement la connaissance de l'état initial de l'entrée, et du modèle permet de prédire l'état futur du système. Cependant il est difficile de calculer la solution analytique théorique de certains systèmes non linéaires, qui est le cas pour les systèmes chaotiques déterministes, car ils sont caractérisés par une sensibilité aux conditions initiales, dont une simple erreur de mesure ou un simple arrondi conduit à des

solutions différentes, ce qui les rendent imprévisibles, en conséquence la prévisibilité n'est plus liée au déterminisme. **(Arab,2018)**

2.3.4 Sensibilité aux conditions initiales

La sensibilité aux conditions initiales est populairement connue sous l'effet papillon.

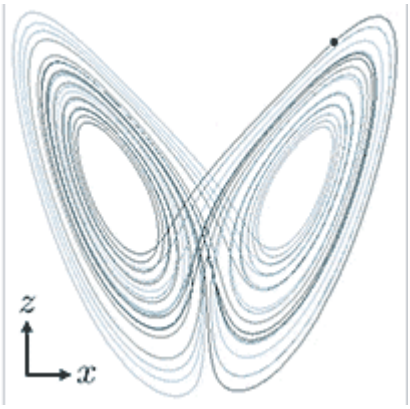


Figure 2. 1 : Effet papillon. [22]

La sensibilité explique le fait que, pour un système chaotique, une modification infime des conditions initiales peut entrainer des résultats imprévisibles sur long terme. Le degré de sensibilité aux conditions initiales quantifie le caractère chaotique du système. **(Bessam,2020)**

On confirme la déclaration précédente par la figure ci-dessous (figure 2.2), dont les deux conditions initiales sont très proches tel que :

$(x_{01}, y_{01} z_{01})$ = (0.1, 0.1, 0.1)

$(x_{02} y_{02} z_{02})$= (0.1001, 0.1001, 0.1001)

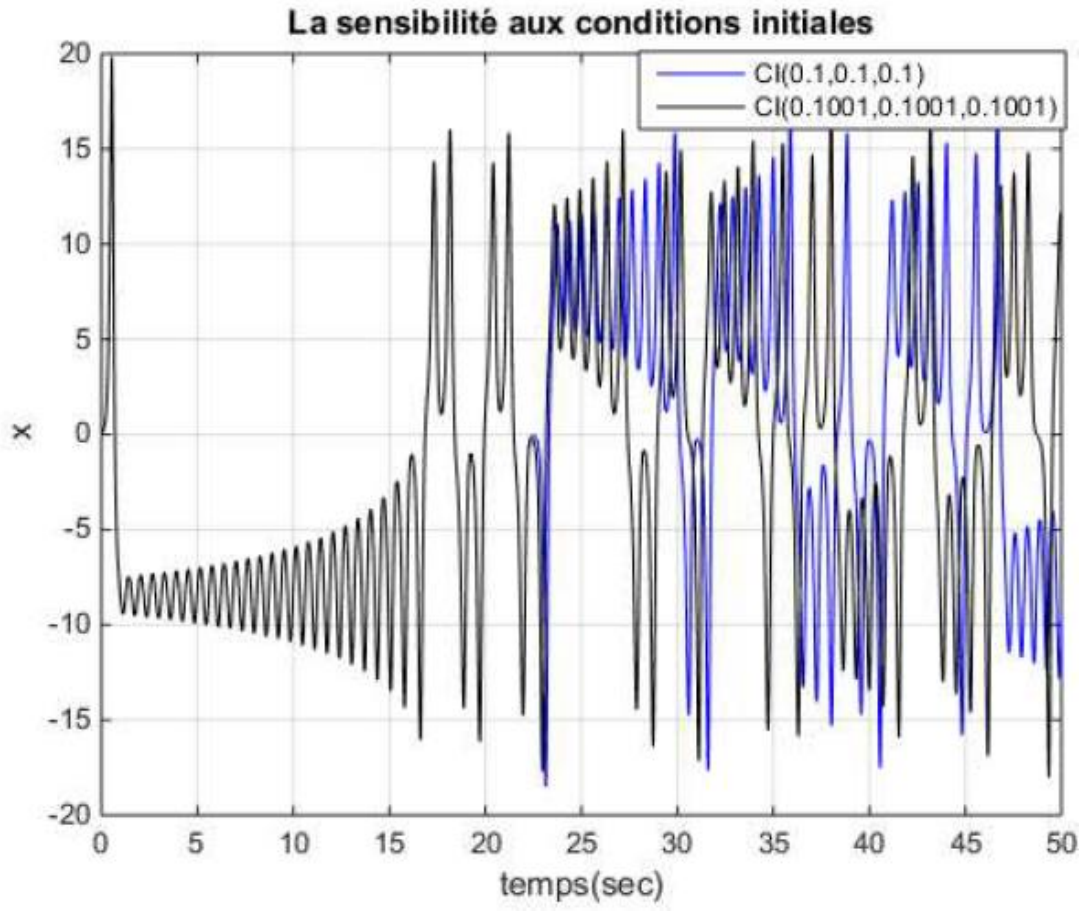


Figure 2. 2 : Évolution dans le temps pour deux conditions initiales très proches. (Arab ,2018)

2.3.5 L'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. (Berkan,2016)

La figure ci-dessous illustre un aspect aléatoire :

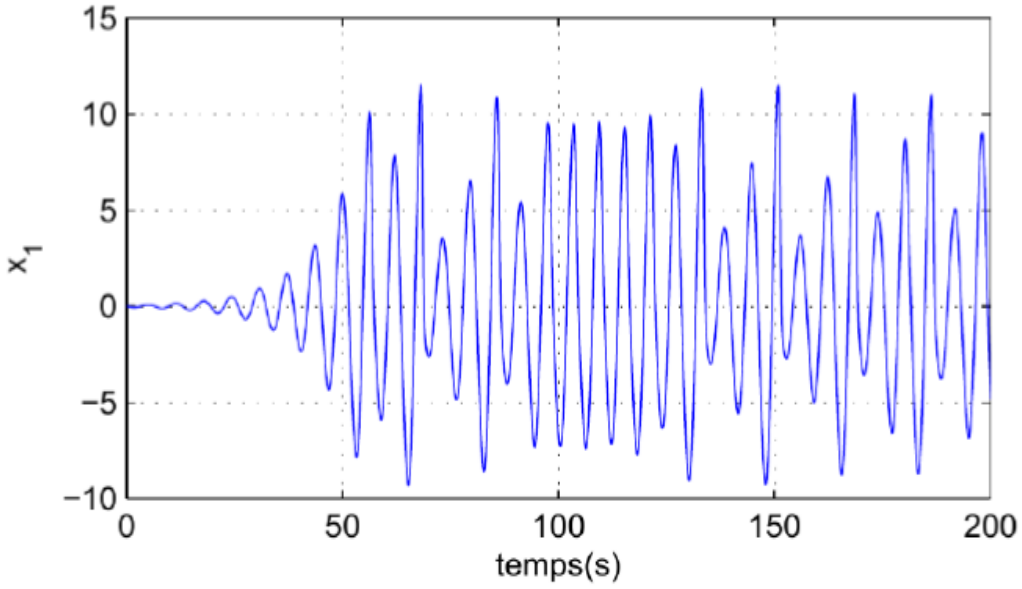


Figure 2. 3: Aspect aléatoire du système de Rössler. (Benayache,2020)

2.3.6 Attracteur étrange

Les attracteurs étranges sont caractéristiques de l'évolution des systèmes chaotiques : au bout d'un certain temps, tous les points de l'espace des phases (et appartenant au bassin d'attraction de l'attracteur) donnent des trajectoires qui tendent à former l'attracteur étrange.A grande échelle, un attracteur étrange n'est pas une surface lisse, mais une surface repliée plusieurs fois sur elle-même. En effet, les trajectoires des points divergent (puisque, par définition deux point ne peuvent avoir la même évolution), mais comme l'attracteur a des dimensions finies, l'attracteur doit se replier sur lui-même.

Le processus d'étirement-repliement se répète à l'infini et fait apparaître un nombre infini de "plis" imbriqués les uns dans les autres qui ne se recoupent jamais. Ainsi, deux points très proches au départ (conditions initiales) peuvent se retrouver à deux extrémités opposées de l'attracteur (conditions finales). Cela traduit le comportement divergent des phénomènes chaotiques. **(Goumidi,2010)**

2.4 Classes des systèmes chaotiques

Nous présenterons deux classes de système chaotique : Les systèmes chaotiques continus et les systèmes chaotiques à temps discret.

2.4.1 Systèmes chaotiques continus

On appelle système en temps continu, tous systèmes d'équation différentielle du premier ordre, le système chaotique à temps continu est décrit par un système d'équation différentielle de forme :

$$\dot{x} = f(t, x, u), y = h(t, x, u) \quad \textbf{(2.1)}$$

Où :

x : le vecteur d'état de dimension n

f : $R^n \rightarrow$**R :** fonction non linéaire qui désigne le champ de vecteur

h : $R^n \rightarrow$**R :** fonction éventuellement non linéaire qui désigne vecteur de sortie

u : l'entrée du système

Il existe plusieurs systèmes chaotiques continus. Parmi eux, on peut citer ces systèmes :

2.4.1.1 Système de Lorenz

Le système de Lorenz est généré par le système d'équations suivant : **(Souleres, 2022)**

$$\begin{cases} \frac{dx}{dt} = Pr(y - x) \\ \frac{dy}{dt} = -xz + rx - y \\ \frac{dz}{dx} = xy - bz \end{cases} \quad \textbf{(2.2)}$$

Pr :le nombre de Prandtl du fluide.

R :le nombre de Rayleigh réduit du fluide.

(x;y;z) :le vecteur d'état.

(a;b;c) :les paramètres du système de «Lorenz».

2.4.1.2 Système de Rössler

Le système de Rössler est donné par les équations suivantes : **[22]**

$$\begin{cases} \dfrac{dx}{dt} = -y - z \\ \dfrac{dy}{dt} = x + ay \\ \dfrac{dz}{dx} = b + z(x - c) \end{cases} \quad (2.3)$$

Où :

x, y, et z : variables d'états du système.

a, b, c : paramètres réels.

Rossier étudia l'attracteur pour a=0,2 b=0,2 et c= 5,7, mais les propriétés de a=0,1 b=0,1 et c=14 sont aujourd'hui les plus étudiées.

2.4.2 Système chaotique à temps discret

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

$$x(K+1) = G\big(x(k), u(k)\big), y(k) = h\big(x(k), u(k)\big) \quad \textbf{(2.4)}$$

Parmi les systèmes chaotiques discrets, on peut citer ces systèmes dont :

a. Système de Hénon

Introduit par l'astronome Michel Hénon en 1976, il est présenté par les équations suivantes : **(Berkan, 2016)**

$$\begin{cases} x(k+1) = y(k) + 1 - a * x(k)^2 \\ y(k+1) = b * x(k) \end{cases} \quad \textbf{(2.5)}$$

Tel que :

(x(k),y(k)) ϵ $\mathbf{R}_2$ **:** représente le vecteur d'état.

- ✓ Pour les valeurs a=1.4 et b=0.3 le système présente un comportement chaotique
- ✓ Les conditions initiales prises sont x_0=0.1, y_0=0.
- ✓ Pour d'autres valeurs de a et b, il peut être chaotique, intermittent ou converger vers une orbite périodique.

b. Système Hénon-Heiles ou Hénon modifié

Il est donné par les équations suivantes :

$$\begin{cases} x(k+1) = a - y^2(k) - bz(k) \\ Y(k+1) = x(k) \\ Z(k+1) = y(k) \end{cases} \quad (2.3)$$

Pour avoir un comportement chaotique, les paramètres du système sont donnés comme suit :

a=1.76 et b=0.1

Et les conditions initiales du système :

x_0= 0.1, y_0= 0.1, z_0 =0.1

2.5 Identification du chaos

Dans cette section, nous présentons quelques outils qui permettent d'identifier le comportement chaotique d'un système dynamique.

2.5.1 Exposant de Lyapunov

Certains systèmes dynamiques (systèmes qui décrivent dans l'espace un état qui évolue dans le temps) sont très sensibles aux petites variations de leur condition initiale. Ces variations peuvent rapidement prendre d'énormes proportions. Le mathématicien russe Alexander Lyapunov s'est penché sur ce phénomène et a développé une quantité permettant de mesurer la vitesse à laquelle ces petites variations peuvent s'amplifier. Cette quantité appelée « **exposant de Lyapunov** » mesure en fait le degré de sensibilité d'un système dynamique. En fait l'exposant de Lyapunov est synonyme d'instabilité et de chaos.

$$\lambda(P_0) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \ln |f'(P_{i-1})| \quad (2.7)$$

Cette quantité sert à mesurer le degré de sensibilité d'un système comme celui du haut, suite à une variation infinitésimale de sa condition initiale Po. Un système sensible à de très petites variations de la condition initiale Po (une des caractéristiques des systèmes chaotiques), donc que le système est classique et obéit aux lois de la dynamique (réversibilité, etc.), alors il aura une quantité λ positive. A l'inverse, la quantité λ sera négative si de petites variations de Po n'ont aucun effet à long terme sur le système. **[24]**

Les figures ci-dessous présentent des exposants de Lyapunov en différents systèmes :

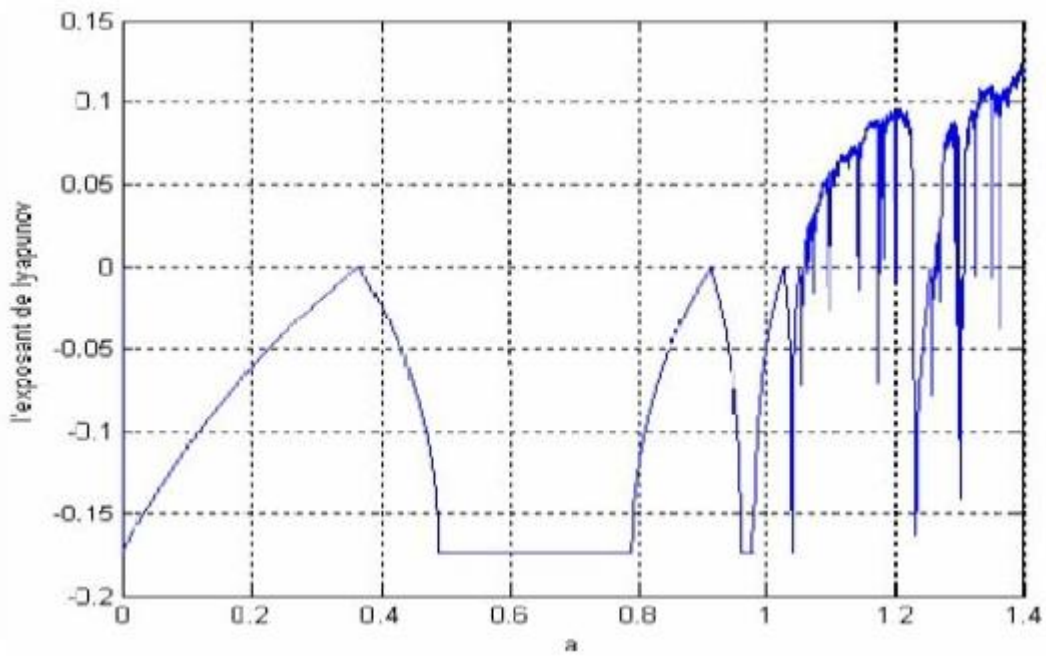


Figure 2. 4: Exposant de Lyapunov du système Discret de Hénon . (Badaoui ,2021)

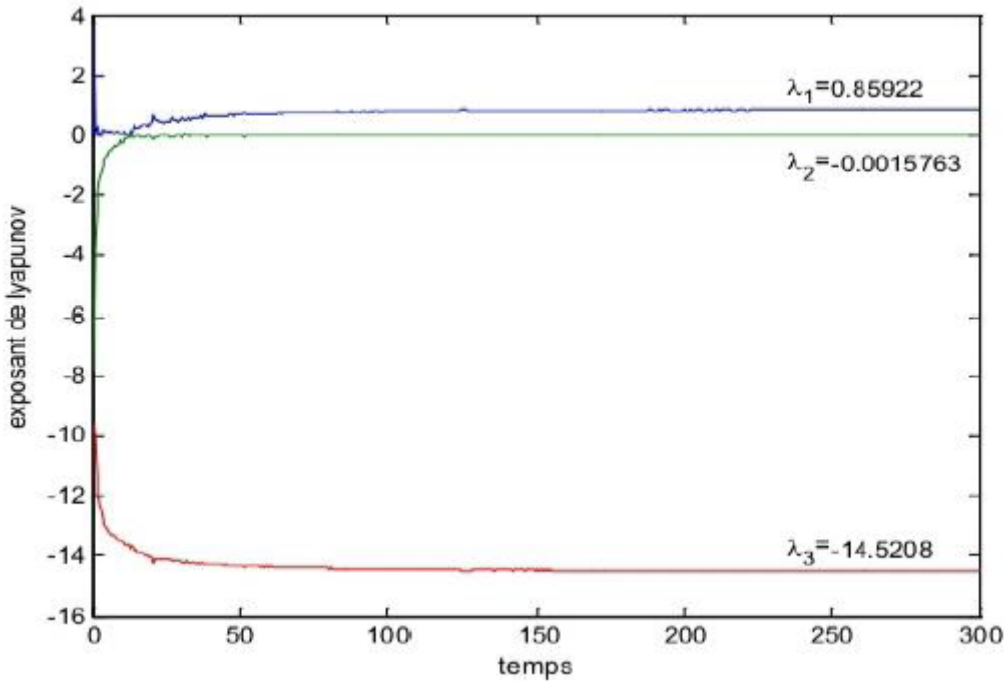


Figure 2. 5 : Exposant de Lyapunov du système continu de Lorenz. (Badaoui ,2021)

2.5.1.1 Méthodes de Calcul des exposants de Lyapunov

Le calcul des exposants de Lyapunov est un outil efficace pour décrire le comportement d'un système dynamique discret ou continu, il définit la divergence entre deux trajectoires initialement voisines. **(Filali, 2020)**

La figure ci-dessous illustre la divergence entre deux trajectoires :

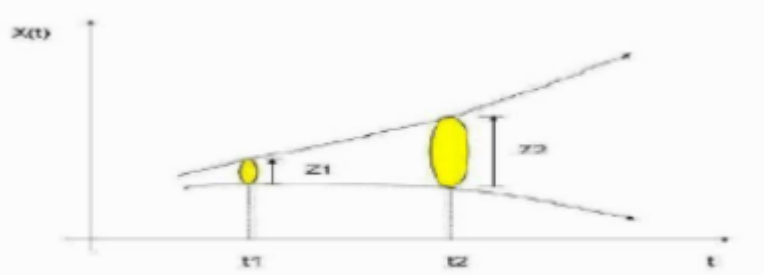


Figure 2. 6 : Divergence de deux trajectoires dans le plan de phase . (Bouchakour ,2018)

Pour un système différentiel de dimension n défini par f dont :

$$\dot{x} = f(x(t)) \qquad \textbf{(2.8)}$$

Où : t ε R et

x(t) εR^n

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

$$\lambda_i = \lim_{t\to+\infty} \frac{1}{t} \ln \frac{||x_i(t) - x'_i(t)||}{||x_i(0) - x'_i(0)||} \qquad \textbf{(2.9)}$$

- ✓ Exposants de Lyapunovdans l'état chaotique et hyper chaotique sont illustrés dans le tableau ci-dessous :

Tableau 2. 1 : Classification des régimes permanents selon les exposants de Lyapunov.

Etat stable	Dimension de Lyapunov	Exposant de Lyapunov
Chaotique	Non entier	$\boldsymbol{\lambda_1} > 0$ $\sum_{i=1}^{n} \lambda_i < 0$
Hyper chaotique	Non entier	Au moins deux exposants positifs : $\boldsymbol{\lambda_1} > 0$, $\boldsymbol{\lambda_2} > 0$ $\sum_{i=1}^{n} \lambda_i < 0$

- ✓ Il existe plusieurs méthodes de calcul des exposants de Lyapunov tels que la méthode (QR), (HQR) et (HQRB). L'une des méthodes les plus utilisées est l'algorithme de Wolf :

- **L'algorithme de Wolf**

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

1. Changement du paramètre de contrôle.

2. Choix aléatoire d'une condition initiale.

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

4. Evolution dans l'attracteur de ces deux trajectoires voisines et calcul de la moyenne

de la divergence renormalisée entre ces deux trajectoires.

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

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

7. Retour au point (1).

8. Représentation du plus grand exposant de Lyapunov en fonction du paramètre de contrôle donné. **(Bouchakour ,2018)**

2.5.2 Fonction d'auto-corrélation

La fonction d'auto corrélation nommée C(α) permet d'estimer le degré de ressemblance entre la variable x à l'instant t et sa valeur à l'instant t+α, et elle est obtenue en faisant la moyenne arithmétique d'un grand nombre de x(t) et x(t+α), sachant que le spectre de puissance correspond à la transformation de Fourier de la fonction d'auto corrélation.

Sa relation est citée ci-dessous :

$$\mathbf{C(\alpha) = \frac{1}{t_2} - t_1\{x(t)x(t+\alpha)dt[t_2, t_1]} \qquad \mathbf{(2.10)}$$

En faisant varier progressivement l'intervalle α on obtient la fonction d'auto-corrélation, et donc si x(t) est constant (périodique ou quasi-périodique), C(α) reste non nulle quand (t→∞), car le spectre de puissance est formé de raies distinctes, et pour des oscillations périodiques C(α) oscille entre−1 et1.Cependant dans le cas des oscillations chaotiques ou le spectre présente une partie continu, C(α) tend exponentiellement vers0 quand α varie.

Cette propriété assure que les solutions divergentes les unes des autres. Si la fonction de corrélation est nulle pour des horizons non nuls, alors c'est un processus non corrélé, et on parle de «bruit blanc déterministe». **(Badaoui,2021)**

2.6 Les cartes chaotiques

En mathématiques, une carte chaotique est une carte qui présente une sorte de comportement chaotique.Les cartes peuvent être paramétrées par un paramètre de temps discret ou un paramètre de temps continu. **[25]**

Nous présentons quelques cartes chaotiques dont :

2.6.1 La carte chaotique logistique (la récurrence logistique)

C'est une cartographie polynomiale de deuxième degré qui présente un comportement chaotique. **(Zhang, 2014)**

L'équation de la carte logistique est donnée par :

$$\boldsymbol{x_{n+1} = \mu x_n(1 - x_n)} \qquad \mathbf{(2.11)}$$

avec : $0 < x_n < 1$.

Où :

x_n **:** le rapport entre la population existante et la population maximale.

2.6.2 La carte chaotique sine (la récurrence sine)

La récurrence sine d'une (01) dimension a pour représentation d'état :

$$X_{n+1} = \lambda \sin(\pi X_n) \qquad (2.12)$$

Avec : $\lambda = 1$

Le comportement chaotique est généré par une manière très similaire à la fonction logistique. Comme la récurrence logistique, la carte sine est quadratique au voisinage de $x = 0{,}5$. Elles ont une distribution probabiliste et une évolution vers le chaos par doublement de période presque identique. Les fenêtres se produisent périodiquement dans le même ordre. Elle a le même nombre de Feigenbaum que la carte logistique. Malgré les similitudes, il existe quelques différences, l'exposant de Lyapounov[2] est d'environ cinquante pour cent plus petit.

Les bifurcations par doublement de période survenir plus tôt, et les fenêtres périodiques sont plus larges par rapport à la carte logistique. **(Goumidi, 2010)**

2.6.3 La carte chaotique standard (la récurrence standard)

La récurrence standard de deux (02) dimensions a pour représentation d'état :

$$\begin{cases} X_{n+1} = X_n + K \sin Y_n \\ Y_{n+1} = Y_n + X_{n+1} \end{cases} \qquad (2.13)$$

Où :

X_n, Y_n **:** sont prises modulo 2π.

Pour K = 0, la carte n'est pas linéaire et seules les orbites périodiques et quasipériodiques existent. Lorsqu'elles sont tracées dans l'espace des phases, les orbites périodiques apparaissent comme des courbes fermées, et les orbites quasi-périodiques comme des petites courbes fermées dont leurs centres se situent dans une autre courbe fermée plus grande. Ces types d'orbites sont observés suivant les conditions initiales utilisées. La non-linéarité de la carte est augmentée lorsque k augmente. **(Goumidi,2010)**

2.6.4 La carte chaotique d'Arnold

La carte chaotique d'Arnold est une carte chaotique générée mathématiquement à partir d'une surface tournante, découverte par Vladimir Arnold. Cette surface (ou tore) est créée en faisant tourner un cercle dans l'espace 3D. **(Ferdush, 2021)**

Cette carte chaotique est la transformation :

$$\gamma : T^2 \to T \qquad \textbf{(2.14)}$$

Où : T^2 **:** le tore.

En notation matricielle, cela peut être écrit par l'équation suivante :

$$\gamma\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod 1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod 1 \qquad \textbf{(2.15)}$$

Où :

x**, y :** respectivement la ligne et les colonnes de la matrice.

2.6.5 Carte chaotique SkewTent

La carte Skewtent est une carte linéaire par morceaux. **(Kouadri,2014) .**

Elle est décrite en réel par l'équation suivante :

$$\textbf{X(n) = f(x(n-1),p)} = \begin{cases} \frac{x(n-1)}{p}, Si\ 0 \leqslant x(n-1) \leqslant p \\ \frac{1-x(n-1)}{1-p}, si\ p < x(n-1) \leqslant 1 \end{cases} \qquad \textbf{(2.16)}$$

Avec f :S→ S ,S= [0 ,1],x(n) εS

Où :

P : le paramètre de contrôle qui varie dans : 0 <p<1

2.7.6 Carte Chaotique Linéaire par MorceauxPWLCM

Une carte chaotique linéaire par morceaux PWLCM (où PWLCM :PiecewiseLinearChaoticMap) est une carte chaotique 1D composée de plusieurs segments linéaires. Cette carte a des propriétés dynamiques et statistiques que les cartes chaotiques à segment unique. Une telle carte a été utilisée par certains chercheurs pour concevoir des chiffrements chaotiques et des PRNG-chaotiques, nous l'appelons PLCM **(Krim, 2019)**

Le PWLCM est définie par les définitions suivantes :

$$X(n) = f(x(n-1),p) = \begin{cases} \frac{x(n-1)}{p} & si\ 0\ x(n-1)p \\ \frac{[x(n-1)-p]}{0,5-p} & si\ p\ x(n-1)0,5 \\ f(1-x(n-1,p) & ailleurs \end{cases} \quad (2.17)$$

avec : $X(n) \in [0,1]$

Où :

P : Paramètre de contrôle 0< p <0,5

2.7 Application du chaos

Le chaos peut s'appliquer dans des diverses applications, on peut mentionner les applications suivantes. Parmi les nombreux domaines d'application du chaos, on cite les suivants [Benayache, 2020] :

- **Engineering:** contrôle de vibration, stabilisation des circuits, réactions chimiques, turbines, étages de puissance, lasers…
- **Ordinateurs:** communications des paquets dans des réseaux informatiques. Cryptage, contrôle du chaos dans les systèmes robotique.
- **Communications:** compression et stockage d'image, conception et management des réseaux d'ordinateurs.
- **Médecine et biologie:** cardiologie, analyse et rythme du cœur (EEG), prédiction et contrôle d'activité irrégulière du cœur.
- **Management et finance:** prévision économiques, analyses financières, et prévision des marché.

3 Le passage de chaotique vers hyper chaotique

Durant les dernières années, les systèmes chaotiques ont été utilisés dans des domaines aussi différents que le cryptage, la synchronisation, le contrôle, les réseaux de neurones, la communication sécurisée, … etc. Dans la communication chaotique sécurisée, le signal chaotique est utilisé pour masquer les messages à transmettre. Perez et Cerderia ont prouvés

que le masquage des messages par un système chaotique normal (possédant un seul exposant de Lyapunov positif) n'est pas toujours efficace. Puis Peroca a montré qu'on peut résoudre ce problème en utilisant un système hyperchaotique de dimension élevée (système avec plusieurs exposants de Lyapunov positifs).

Le comportement dynamique des systèmes hyperchaotiques va donc être très compliqué, c'est pour cela que ces systèmes offrent plus de sécurité dans la communication chaotique.**(Ikhlef, 2007)**

4 Les systèmes hyper chaotiques

Le comportement hyperchaotique a été découvert pour la première fois par Rössler en 1979 par une boucle de retour appliquée sur son système original. Cette découverte a ouvert un autre horizon de recherche dans la théorie du chaos. **(Rezzag,2016)**

4.1 La différence entre système chaotique et hyper chaotique

Le système hyper chaotique est déterminé comme étant un comportement d'un système chaotique qui possède au moins deux exposants de Lyapunov positifs.

4.2 Définition

Un attracteur hyper chaotique est généralement défini, comme étant un comportement chaotique avec au moins deux exposants de Lyapunov positifs, combiné avec un exposant nul le long de l'écoulement et un exposant négatif pour garantir la reliée de la solution. **(Benzmam, 2010)**

4.3 Le premier système hyper chaotique

Le premier système hyperchaotique à 4 dimensions a été proposé en 1979 par Rössler.

Ce système est défini par les équations suivantes :

$$\begin{cases} \boldsymbol{x = -y - z} \\ \boldsymbol{\dot{y} = x + ay + w} \\ \boldsymbol{\dot{z} = b + xz} \\ \boldsymbol{\dot{w} = -cz + dw} \end{cases} \qquad \textbf{(2.18)}$$

Ce système a un comportement hyperchaotique comme la figure ci-dessous indique quand les paramètres a,b,c et d prennent les valeurs suivantes : a=0,25 ,b=3 , c=0,5 et d=0,05

Les conditions initiales peuvent être : $x_0 = -10\,; y_0 = -6\,;\ z_0 = 0; w_0 = 10{,}0$

Les quatre exposants de Lyapunov correspondants sont :

$$\lambda_1 = 0{,}112\,; \lambda_2 = 0{,}019; \lambda_3 = 0\ et\ \lambda_4 = -25{,}188$$

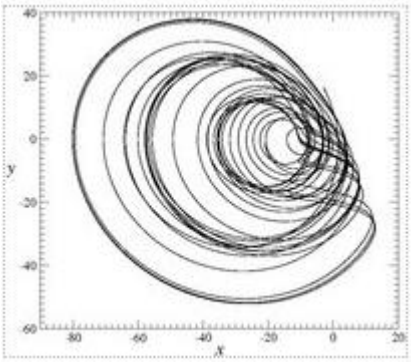


Figure 2. 7 : Projection plane de la solution de l'attracteur hyperchaotique au système Rössler 4D. (Letellier, 2007)

Le caractère hyperchaotique de ce comportement n'est pas si évident à partir de cette projection plane qui ressemble un peu à un attracteur chaotique "bruité".**(Letellier, 2007)**

4.4 Modèle 9D pour une transition chaos-hyperchaos

Un modèle de 9 dimensions, pour une convection Rayleigh-Bénard dans une cellule carrée a été proposé par Reiterer en 1998 [Rezzag,-].Il est défini ainsi comme l'équation ci-dessous :

$$\begin{cases} \dot{C}1 = -\sigma b1C1 - C2C4 + b4C4^2 + b3C3C5 - \sigma b2C7 \\ \dot{C}2 = -\sigma C2 + C1C4 - C2C5 + C4C5 - \sigma C9/2 \\ \dot{C}3 = -\sigma b1C3 + C2C4 - b4C2^2 - b3C1C5 + \sigma b2C8 \\ \dot{C}4 = -\sigma C4 - C2C3 - C2C5 + C4C5 + \sigma C9/2 \\ \dot{C}5 = -\sigma b5C5 + C2^2/2 - C4^2/2 \\ \dot{C}6 = -b6C6 + C2C9 - C4C9 \\ \dot{C}7 = -b1C7 - RC1 + 2C5C8 - C4C9 \\ \dot{C}8 = -b1C8 + RC3 - 2C5C7 + C2C9 \\ \dot{C}9 = -C9 - RC2 + RC4 - 2C2C6 + 2C4C6 + C4C7 - C2C8 \end{cases} \quad \textbf{(2.19)}$$

Où :

-R=43,3

-Les paramètres constants bi sont une mesure de la géométrie de la cellule carrée, définie par :

$$\begin{cases} b_1 = 4\frac{1+a^2}{1+2a^2} \\ b_2 = 4\frac{1+2a^2}{2(1+a^2)} \\ b_3 = 2\frac{1-a^2}{1+a^2} \\ b_4 = \frac{a^2}{1+a^2} \\ b_5 = \frac{8a^2}{1+2a^2} \\ b_6 = \frac{4}{1+2a^2} \end{cases} \quad \textbf{(2.20)}$$

4 Conclusion

Dans ce chapitre nous avons évoqué deux systèmes dynamiques dont le système chaotique et hyper chaotique.Nous avons présenté dans la première partie quelques types de cartes chaotiques. Cependant, dans la deuxième partie, nous avons donnéles principales définitions relatives aux systèmes dynamiques chaotiques. Ce dernier peut être conçu sous deux classes : système dynamique discrets et système dynamique continu. Ainsi nous avons présenté deux identification de chaos tel que l'exposant Lyapunov et la fonction d'autocorrélation.

Le prochain chapitre nous basons sur la partie pratique de thème tel que l'implémentation et tests sous MATLAB.

Chapitre 3
Implémentation et tests

1 Introduction

Dans ce chapitre, nous utilisons un nouvel algorithme de cryptage d'image basé sur le système hyper chaotique de Lorenz et l'algorithme Rivest–Shamir–Adleman (RSA). Tout d'abord, nous présenterons la structure générale de l'algorithme utilisé qui repose sur le principe de confusion et diffusion, ensuite nous parlerons sur les résultats expérimentaux, dont on décrit les tests utilisés pour évaluer ce dernier.

2 Méthode utilisée

L'algorithme de cryptage d'image utilisé est basé sur deux fonctions, une fonction pour le chiffrement et l'autre pour le déchiffrement. **(Lin, 2021)**

2.1 Fonction de chiffrement d'image

Le processus de cryptage est décrit comme suit :

- **Etape 1 :** Sélectionner les nombres premiers p et q, puis calculer n= p*q et la fonction d'Euler

$\varphi(n) = (p-1)\,(q-1)$.

- **Etape 2 :** Générer la clé publique *(e,* n) et la clé privée *(d,* n) en utilisant l'algorithme RSA.

- **Etape 3 :** Choisir quatre grands nombres entiers positifs (m1, m2, m3, m4) au hasard comme informations confidentielles ; ensuite utiliser la clé publique (e, n) pour calculer $c_i = m_i^e$ mode (n), i = 1, 2, 3, 4, qui est envoyé au destinataire.

- **Etape 4 :** Calculer les paramètres x0, y0, z0, w0 de système hyper chaotique de Lorenz par les équations suivantes :

$$\begin{cases} x_0 = sqrt\,(\log(c_1 + m_1)) \\ y_0 = sqrt\,(\log(c_2 + m_2)) \\ z_0 = sqrt\,(\log(c_3 + m_3)) \\ \omega_0 = sqrt\,(\log(c_4 + m_4)) \end{cases} \quad \textbf{(3.1)}$$

- **Etape 5 :**Générer la séquence pseudo-aléatoire S, X et R et convertir les valeurs générées dans la plage de 0 à 255 :

$$\begin{cases} S = mod(floor\left((S + 100) * 10^{10}\right), 256) \\ X = mod\,(floor((S + 100) * 10^{14}), 256) \\ R = mod(floor((S + 100) * 2^{16}), 256) \end{cases} \quad \textbf{(3.2)}$$

- **Etape 6 :** Enregistrer l'image simple en tant que P et effectuer la suite à une opération de diffusion en mode additif deux fois avec le flux de clé S généré pour obtenir l'image A :

$$\begin{cases} A_i = (A_{i-1} + S_i + P_i) mod 256 \\ A_i = (A_{i+1} + S_i + P_i) mod 256 \end{cases} \quad \textbf{(3.3)}$$

Où :

A_i, S_i et P_i : les éléments de A,S et P.

- **Etape 7 :**Utiliser le flux de clé X et procéder de manière non répétitive permutation de l'image A pour obtenir l'image B. Effectuer permutation associée au texte en clair.

- **Etape 8 :**Utiliser la touche flux R et effectuer une diffusion en champ fini de l'image B pour obtenir l'image C :

$$\begin{cases} C_i = C_{i-1} + R_i + B_i \\ C_{i+} = C_{i+1} + R_i + B_i \end{cases} \quad \textbf{(3.4)}$$

- **Etape 9 :** Enfin, transformer C pour obtenir une image cryptée noté par la matrice matrice E.

2.2 Fonction de déchiffrement d'image

Le déchiffrement d'image est le processus inverse du cryptage d'image, il s'est effectué comme suit :

- **Etape 1 :**Le récepteur déchiffre l'image originale par la clé privée (d, n) basée sur l'information de texte chiffré reçu C_i, i=1 ,2 ,3 ,4 ,puis il calcule $m_i = C_i^d$ mode

(n).Calculer les paramètres x_0,y_0,z_0,w_0 de système hyper chaotique de Lorenz par l'équation **(3.1)** .

- **Etape 2 :**Générer une séquence pseudo-aléatoire S ,X' et R' ,et convertir les valeurs générées en plage de 0 à 255 :

$$\begin{cases} S' = \boldsymbol{mod}(\boldsymbol{floor}\left((s' + \mathbf{100}) * \mathbf{10^{10}}\right), \mathbf{256}) \\ X' = \boldsymbol{mod}\ (\boldsymbol{floor}((s' + \mathbf{100}) * \mathbf{10^{14}}), \mathbf{256}) \\ R' = \boldsymbol{mod}(\boldsymbol{floor}((s' + \mathbf{100}) * \mathbf{2^{16}}), \mathbf{256}) \end{cases} \quad \textbf{(3.5)}$$

- **Etape 3 :**Utiliser la touche R' et effectuer la diffusion en champ fini de l'image E pour obtenir l'image C' :

$$\begin{cases} \boldsymbol{C'_i = E_i \div E_{i-1} \div R'_i} \\ \boldsymbol{C'_i = E_i \div E_{i+1} \div R'_i} \end{cases} \textbf{(3.6)}$$

Où :

C_i',E_i' et R_i': éléments de C',E' et R'.

- **Etape 4 :**Utiliser le flux de clés X' et effectuer des permutations de l'image C' pour obtenir l'image B'. Effectuer la permutation associée au texte en clair.

- **Etape 5 :**Exécuter deux fois le mode de diffusion additive suivant sur B' par le flux de clé générée S pour obtenir l'image A' :

$$\begin{cases} \boldsymbol{A'_i = (2 * 256 + B'_i - B'_{i-1} - S'_i) mod 256} \\ \boldsymbol{A'_i = (2 * 256 + B'_i - B'_{i+1} - S'_i) mod 256} \end{cases} \quad \textbf{(3.6)}$$

Où :

A' $_i$, B' $_i$ et S'$_i$: les éléments de A', B' et C'.

Etape 6 : Transformer Ai' pour obtenir la matrice image originale Pi'.

3 Résultat expérimentaux

Cette partie est consacrée pour clarifier si la méthode utilisée de chiffrement et déchiffrement est efficace ou non. Les résultats de simulation ont été implémentés sous MATLAB (les tests).

3.1 La procédure expérimentale

La procédure expérimentale est effectuée à l'aide d'un code sur MATLAB. La clé privée consistait en grands nombres premier p= 3259 et q= 3821 c'est d=3385223, pour la multiplication de q et p est n= 12452639, et la fonction d'Euler φ(n) est φ(n) = 12445560.

Quatre entiers positifs ont été sélectionnés séparément m1= 178333, m2= 38628, m3=92873897 et m4=829809, et la clé publique consistait en e = 1288367, C_1 =174038 C_2=1799483, C_3=12452638 et C_4=4198591.

Les résultats obtenus sont affichés sur la fenêtre de commande de MATLAB, les valeurs affichées de paramètre de système hyper chaotique de Lorenz sont les suivantes :

x_0= 3.5739, y_0= 3.7979, z_0= 4.2980, et w_0= 3.9282.

3.2 Les données de test utilisées

Les données utilisées dans notre mémoire, est une base de données d'images de test au niveau couleur et au niveau de gris :

3.2.1 Les images originales

Sur la figure ci-dessous nous donnons les images utilisées pour le test.

Figure 3. 1: Les images originales de test.

3.2.2 Les images en gris

La figure ci-dessous montre quelques images de test au niveau de gris :

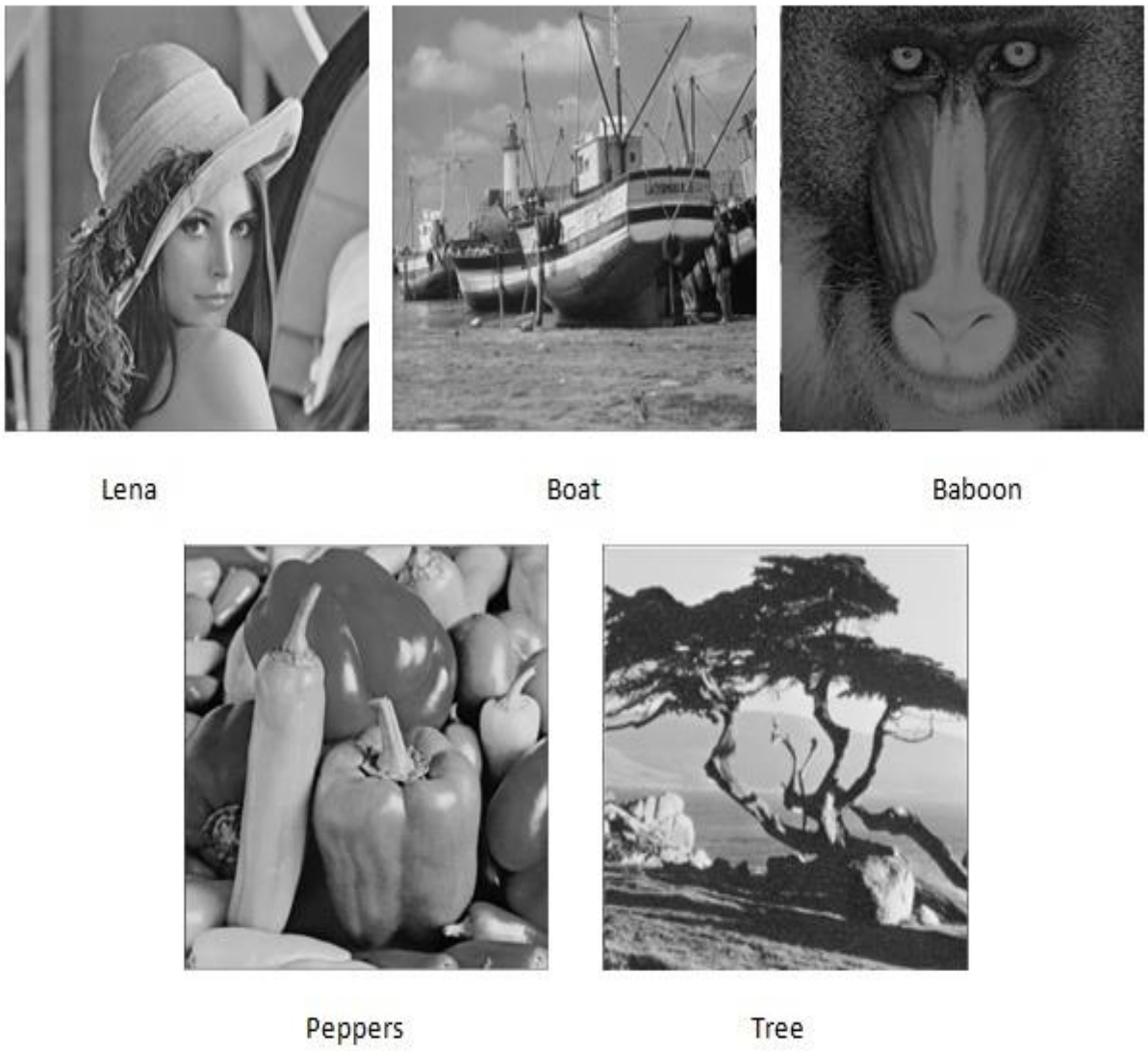


Figure 3. 2 : Les images de test au niveau de gris.

3.2.3 Les images chiffrées

Les résultats du cryptage pour l'image de test sont illustrés sur la figure ci-dessous :

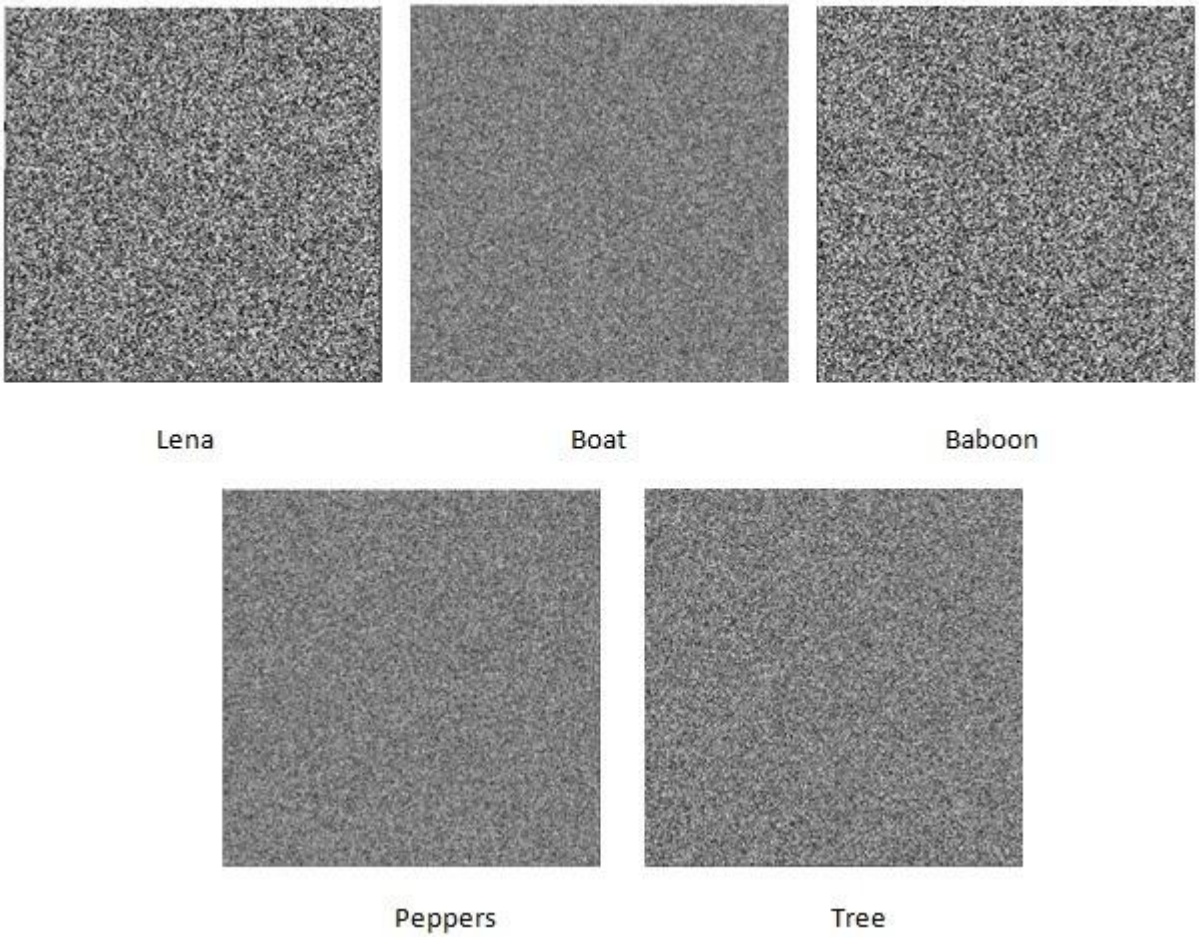


Figure 3. 3 : Images de test chiffrées.

Les images cryptées dans la figure ci-dessus révèlent qu'aucune information n'a pu en être tirée.

3.2.4 Les images déchiffrées

Les résultats du décryptage pour l'image de test sont illustrés sur la figure ci-dessous :

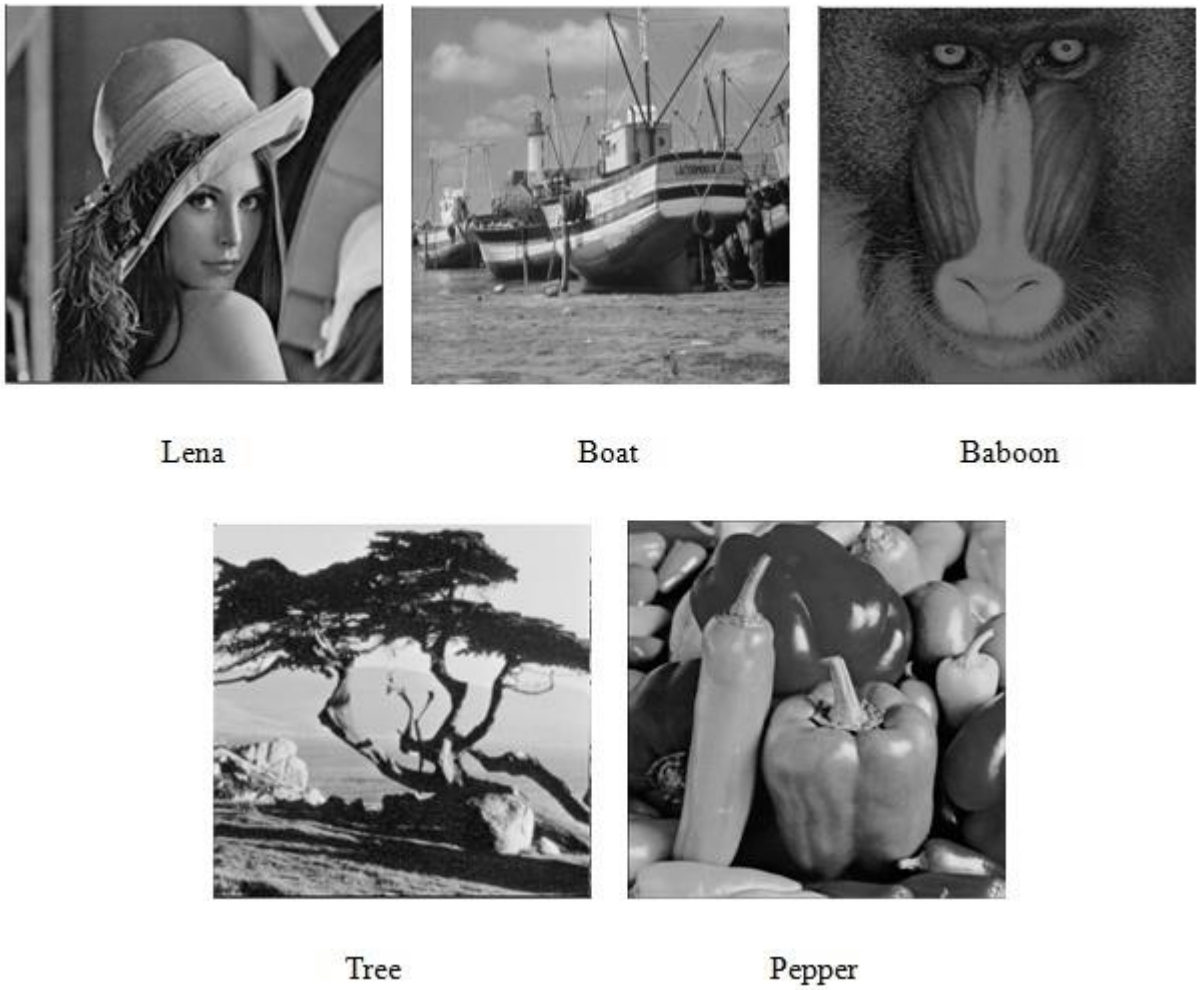


Figure 3. 4 : images de test déchiffrées.

Les images décryptées dans la figure ci-dessus montrent que les informations d'image simple peuvent être correctement restaurées

D'après les résultats obtenus sur les figures ci-dessus qui comportent les images cryptées et décryptées, la méthode utilisée de chiffrement et déchiffrement est efficace.

3.3 Le temps de chiffrement et déchiffrement

Le temps de chiffrement et déchiffrement veut dire le temps d'exécution, est aussi une norme importante pour savoir si la méthode proposée est efficace, car plus le processus de cryptage est rapide, plus sa révélation en cryptanalyse est difficile.

Le tableau (3.1) montre le temps du chiffrement et déchiffrement par la méthode utilisée en seconde (s):

Tableau 3. 1 : Le temps du chiffrement et de déchiffrement.

Image	Lena	Baboon	Boat	Peppers	Tree
Temps de chiffrement (s)	0.410336	0.429091	0.551365	0.520102	0.232474
Temps de déchiffrement (s)	0.469415	0.485496	0.561332	0.674208	0.301007

D'après le tableau on peut voir que le temps de cryptage et décryptage de schéma utilisé est court, par conséquent, le schéma utilisé est efficace.

4 Critères d'évaluation

Un bon système de cryptage doit être protégé contre toutes les attaques possibles, pour cela on applique des simulations numériques en utilisant un ensemble de mesures d'évaluation pour montrer la sécurité et l'efficacité de l'algorithme proposé. Dans notre projet on va présenter comme mesure des tests statique tel que (l'histogramme, la corrélation, l'entropie), les tests différentielle tel que (UACI, NPCR), l'espace de clés et la sensibilité de la clé.

4.1 Les tests statiques

En utilisant différents tests pour l'image en claire et crypté tell que : l'histogramme, la corrélation, et l'entropie.

4.1.1 L'histogramme

Un histogramme est une courbe statistique indiquant la répartition des pixels selon leur valeur. L'histogramme est très utile pour contrôler l'exposition d'une image. **(Hamada, 2020)**

Cinq images de tests ont été utilisées dans l'analyse, leurs traçages d'histogramme se trouvent sur la figure ci-dessous :

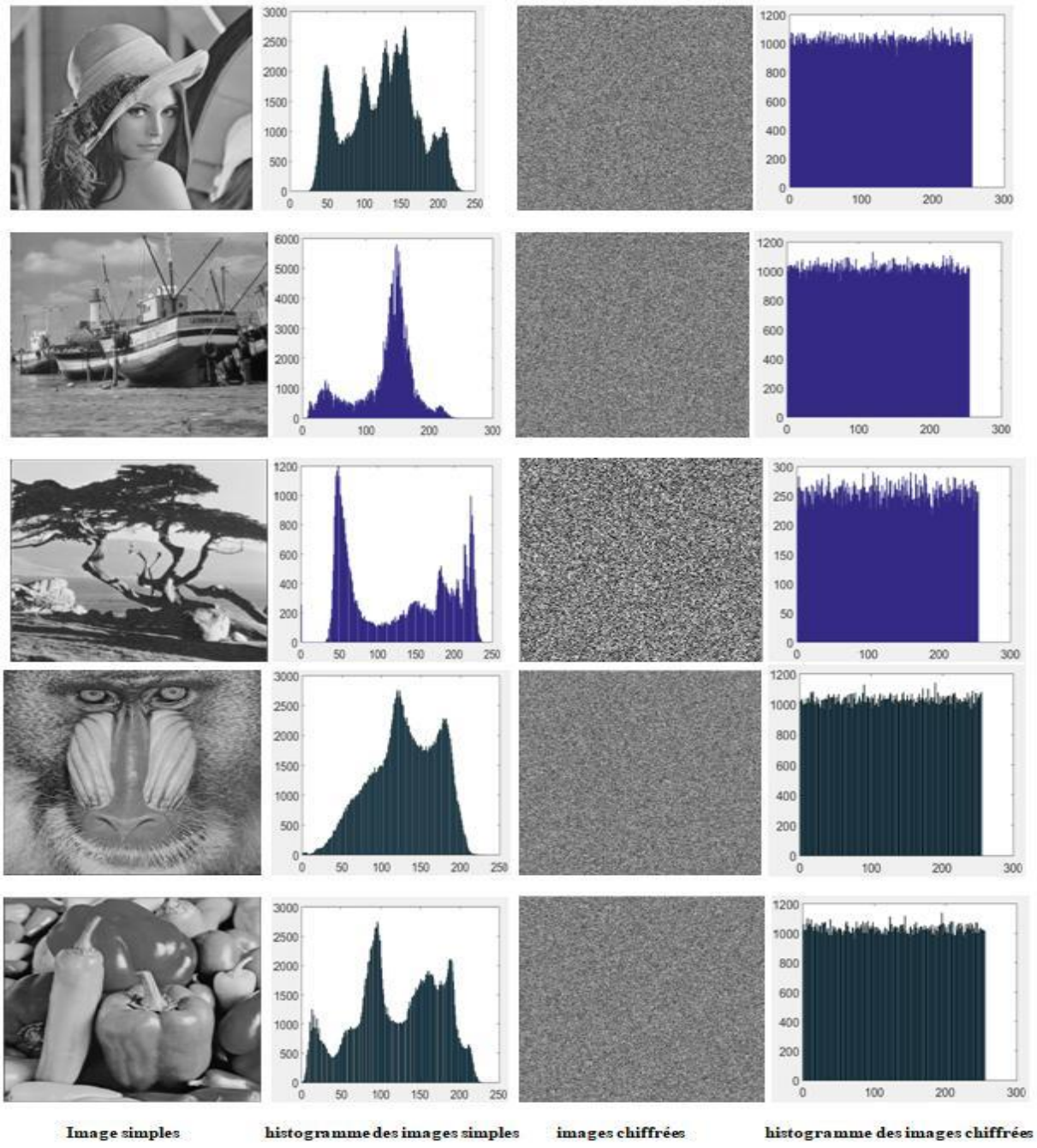


Figure 3. 5: Histogramme des images en claire et cryptées.

Les résultats montrent que les histogrammes des images cryptées sont uniformes, ils ne fournissent aucune information utile à l'attaquant. Par contre les histogrammes des images claires (originales) ils sont non uniformes.

4.1.2 La corrélation

Coefficient de corrélation des pixels adjacents, est une mesure courante utilisée dans l'évaluation de niveau de sécurité pour les algorithmes de cryptage d'images nouvellement

conçus est basé sur le fait bien connu que, généralement en images simples, tout pixel choisi arbitrairement est fortement corrélé avec ses pixels adjacents (soit ils sont orientés en diagonale, verticalement ou horizontalement). Par conséquent, dans le cas d'une image haute performance algorithmes de chiffrement, les scores de corrélation des pixels adjacents devraient être proches de zéro. **(Diaconu, 2017)**

L'expression de calcul de coefficient de corrélation est donnée par**(Khouildat, 2019)**:

$$\mathbf{R}= \frac{cov\,(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad \textbf{(3.7)}$$

Où

$$\mathbf{cov(x,y)} = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))\ (y_i - E(y)) \qquad \textbf{(3.8)}$$

$$\mathbf{E(x)} = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad \textbf{(3.9)}$$

$$\mathbf{D(x)} = \frac{1}{N}\sum_{i=1}^{N} x_i - E(x))^{2} \qquad \textbf{(3.10)}$$

Tel que :

r : la corrélation.

cov: la covariance.

E : l'espérance mathématique.

D : la variance.

x ,y : les valeurs des pixels des images.

Pour étudier la corrélation, on utilise l'algorithme de cryptage proposé pour crypter l'image de boat, donc le coefficient de corrélation va être calculé entre l'image originale (boat) et l'image cryptée comme l'illustre la figure ci-dessous :

Figure 3. 6 : Image originale de boat et l'image cryptée.

Ensuit on calcule les coefficients de corrélation dans les trois directions (verticale, horizontale et diagonale), les deux figures ci-dessous montrent les courbes des corrélations entre les deux images, image claire et cryptée.

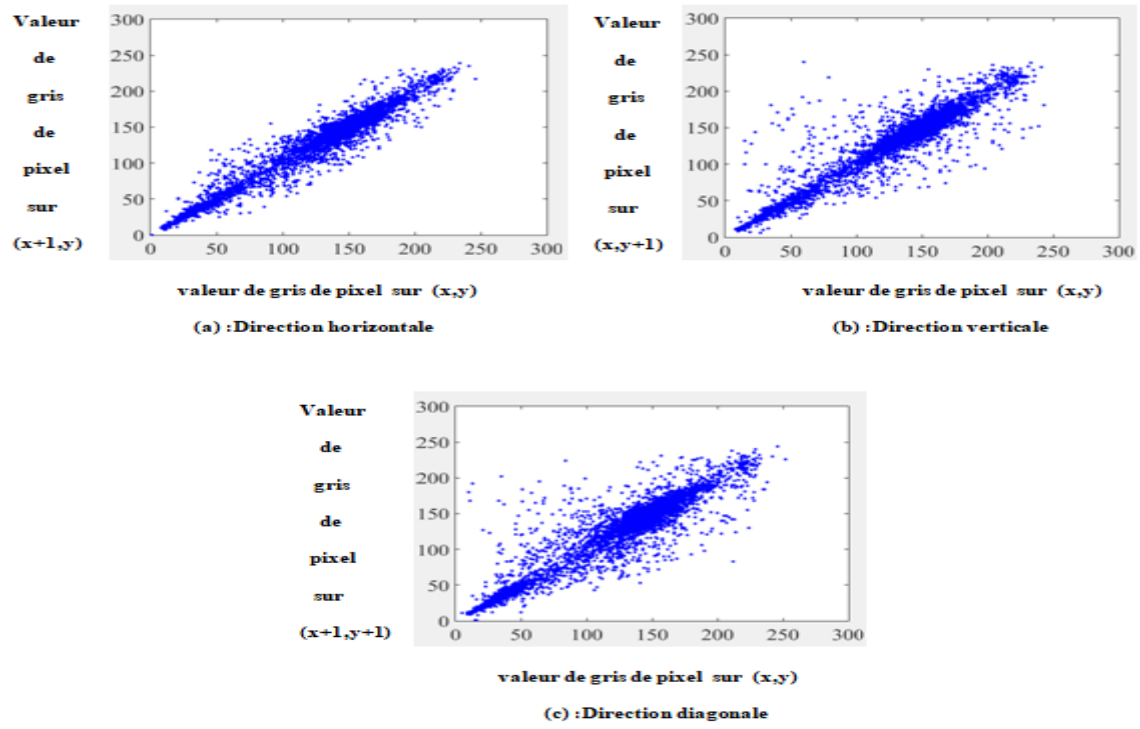


Figure 3. 7 : Les corrélations horizontale, verticale et diagonale des pixels de l'image claire.

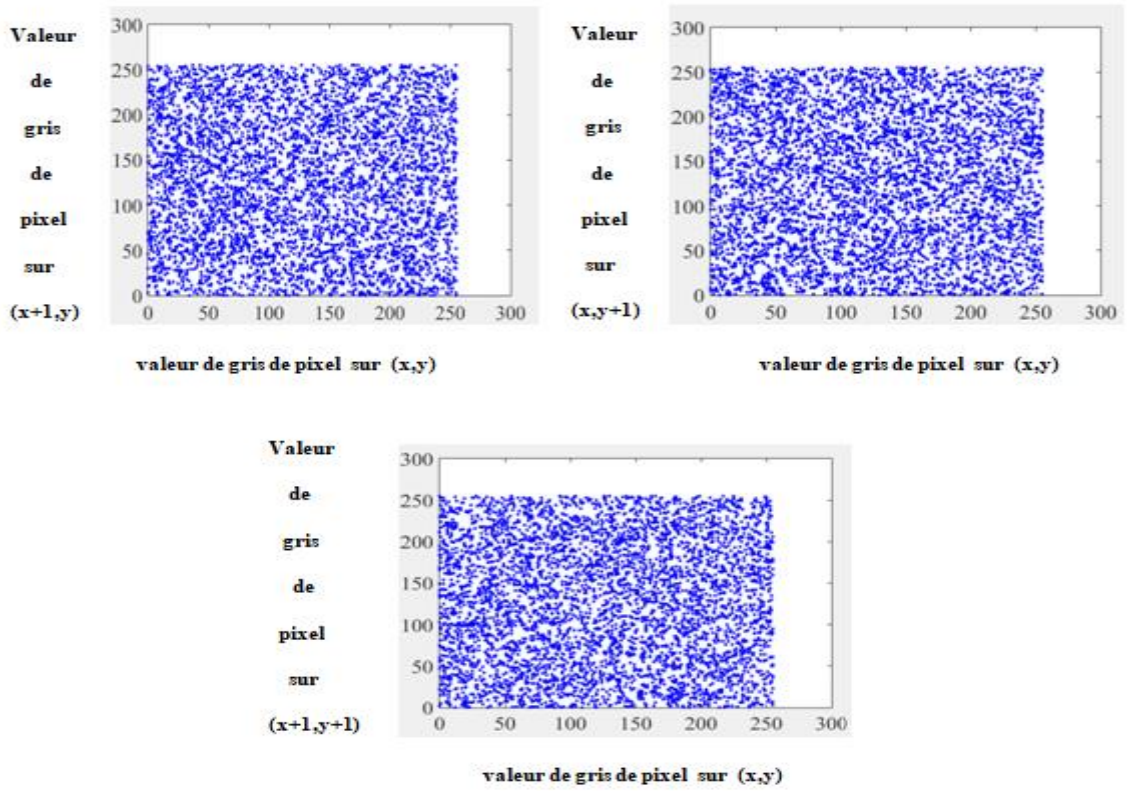


Figure 3. 8 : Les corrélations horizontale, vertical et diagonal des pixels de l'image cryptée.

Il ressort de ces figures que dans le cas des images originales, les pixels adjacents ont de fortes corrélations et s'alignent sur la première bissectrice. Par contre, dans le cas des images chiffrées, les pixels adjacents sont dispersés presque de manière aléatoire.

D'une manière générale, l'observation des pixels hautement diffusés se réfèrent à un algorithme robuste à toute attaque statistique.

Le tableau ci-dessous répertorie les corrélations des images claires et leurs images chiffrées en utilisant l'algorithme proposé.

Tableau 3. 2 : Coefficients de corrélation entre l'image originale et l'image chiffrée de boat.

Corrélation	Image claire	Image chiffrée
Horizontale	0,9697	-0,0042
Verticale	0,9341	0,0377
Diagonale	0,9246	0,0013

Les résultats de tableau montrent que la corrélation de l'image chiffrée est très faible dans les trois niveaux (diagonal, horizontal, vertical) par rapport la corrélation de l'image claire.

Plus la valeur de corrélation est faible plus la qualité de cryptage est meilleure.

4.1.3 L'entropie

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. **(Djemaa, 2021)**

L'entropie H (x) de toute donnée peut être calculée comme :

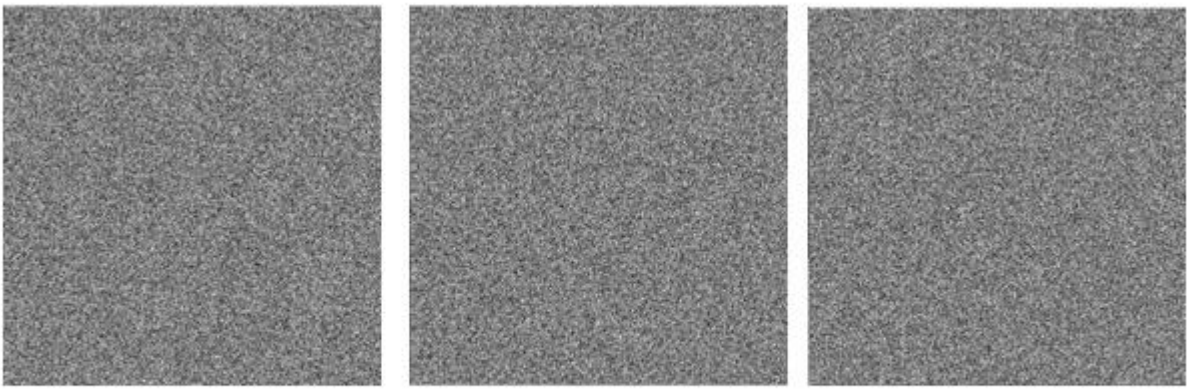
$$\mathbf{H(m)} = \sum_{i=0}^{2^{n-1}} \boldsymbol{P(m)_i log_2 \frac{1}{P(m_i)}} \textbf{(3.11)}$$

Si l'image est bien cryptée La valeur de l'entropie est très proche de 8, Parce que si l'entropie est inférieure à 8, il existe des degrés de prévisibilité, Pour l'image cryptée avec 256 symboles, donc on ne peut pas assurer la sécurité contre l'attaque par entropie.

Pour l'entropie on adopte trois images de « peppers », qui se diffèrent selon les valeurs de ses couches de couleur, la figure ci-dessous montre ces images utilisées :

Figure 3. 9: Différentes images de peppers en claire.

Les images « peppers» cryptées sont illustrées respectivement sur la figure ci-dessous :



a' b' c'

Figure 3. 10: Les différentes images de peppers cryptées.

Le tableau ci-dessous présente les valeurs de l'entropie des images claires et chiffrées :

Tableau 3. 3 : Comparaison des Entropie entre les images en claire et chiffrée.

Nom de l'image	Entropie de l'image en claire	Entropie de l'image chiffrée
a	7,3388	7,9994
b	7,4963	7,9993
c	7,0583	7,9994
Moyenne d'entropie	7,2978	7,9994

A près la simulation des trois images, les résultats de tableau montrent que les valeurs de l'entropie des images chiffrée sont plus proche à la valeur 8. Cela montre qu'il est difficile ou dire qu'il est impossible d'avoir la prévisibilité d'information.

4.2 Les tests différentiels

NPCR et UACI sont les deux plus importantes quantités qui quantifient la force d'algorithmes de cryptage.

4.2.1 NPCR

NPCR (taux de changement de nombre de pixels), mesure le pourcentage du nombre de pixels différents entre deux images par rapport au nombre total de pixels. **(Bekkouche, 2018)**

Il est défini comme suit :

$$\mathbf{NPCR} = \sum_{ij} \frac{D(i,j)}{m*n} * 100\ \% \qquad \mathbf{(3.12)}$$

4.2.2 UACI

UACI (intensité unifiée moyenne évolutive) représente la différence de l'intensité moyenne. Il est défini comme suit :

$$\mathbf{UACI} = \frac{1}{M \times N}\left[\sum_{i,j}\frac{c1(i,j)-c2(i,j)}{255}\right] \mathbf{x\ 100\%} \qquad \mathbf{(3.13)}$$

Le tableau ci-dessous montre la liste des valeurs de NPCR et UACI entre images.

Tableau 3. 4 : Les valeurs d'UACI et NPCR.

Nom d'image	Taille de l'image	Valeur UACI	Valeur de NPCR
Lena 512	512 x 512	33.4824	99.5819
Baboon	512 x 512	33.4675	99.6075
peppers	512 x 512	33.5190	99.621

Un score NPCR/UACI élevé est généralement interprété comme une résistance élevée aux attaques différentielles. Autrement dit si un changement mineur dans l'image en clair peut provoquer un changement significatif dans l'image cryptée, alors l'attaque différentielle devient inutile et l'attaquant ne trouve aucune relation significative entre l'image claire et celle cryptée.

Les résultats de tableau montrent des valeurs NPCR/UACI élevées donc on peut dire que la résistance aux attaques est élevée.

4.3 Analyse de sensibilité clé

Consiste à analyser la différence entre deux images chiffrées obtenues en chiffrant la même image simple lorsque la clé change légèrement.

On a travaillé par deux ensembles de clé dont clés 1 et clés 2, qui diffèrent légèrement afin de pouvoir réaliser l'analyse de sensibilité clé, le résultat de notre travail est interprété sur la figure ci-dessous :

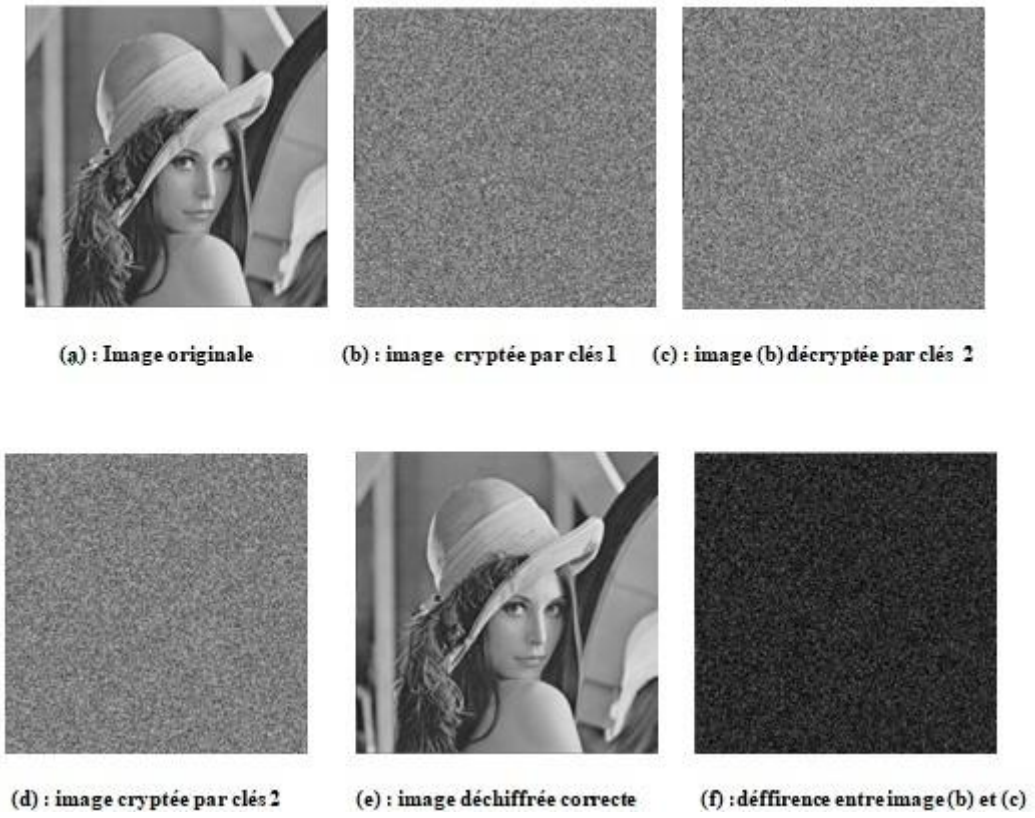


Figure 3. 11 : Analyse de sensibilité clé.

On remarque qu'il y a des différences significatives entre les deux images chiffrées comme la figure (f) indique, donc la sensibilité de la clé du système de chiffrement d'image est forte. On peut dire qu'un bon système de cryptage d'image doit avoir une forte sensibilité des clés.

4.4 Espace de clés

Pour rendre les attaques impossibles l'espace clé doit être suffisamment grand. Un espace clé est une collection de tous clés valides. Pour le crypto-système d'images numériques proposé, les clés K $=\{x0, y0, z0, w0\}$ sont la valeur initiale du système hyper chaotique de Lorenz, où x0 ε (-40, 40), y0 ε (-40, 40), z0 ε (1, 81),et ω0 ε(-250, 250).Tous les pas de x_0, y_0 et z_0 sont 10^{-13}, et les pas de ω_0 sont 10^{-12}.

Par conséquent, la taille de l'espace de la clé est d'environ $S=2{,}56 * 10^{59}$ qui est égal à la longueur de la clé $L= \log_2 S = 197$ bit.

Donc dans notre algorithme, l'espace clé est suffisamment grand alors si l'espion utilise une recherche exhaustive de la clé pour casser le cryptage ou le décryptage du

cryptosystème, il n'a besoin que de tenter la moitié des clés dans l'espace de clé. Les méthodes de chiffrement et de déchiffrement étant réciproques, il suffit d'évoquer le cas du chiffrement.

Le temps nécessaire pour déchiffrer par une recherche exhaustive de la clé peut être approximé par le produit du nombre de clés dans la moitié de l'espace de clé et le temps d'un chiffrement unique, qui est d'environ 4,4607 × 1051 ans, c'est à dire que l'espace clé du système chaotique de Lorenz est suffisamment grand.

5 Conclusion

Dans ce chapitre, nous avons utilisé un schéma de chiffrement d'image basé sur système hyper chaotique de Lorenz et l'algorithme Rivest–Shamir–Adleman (RSA). Les résultats obtenus ont montré que le système de cryptage d'image implémenté possède un grand espace de clés et une sécurité de haut niveau. Ainsi l'analyse prouve la sécurité, l'efficacité et la sensibilité.

Conclusion générale

Rappelons que notre objectif dans ce mémoire consiste à implémenter un système de cryptage hyperchaotique des images.Pour atteindre cet objectif, nous avons d'abord donné des généralités sur les trois domaines qui englobent notre travail dont le traitement d'images, les systèmes de cryptage, et les systèmes chaotique et hyperchaotique.

Dans cette étude on a utilisé un nouveau schéma de cryptage d'image basésur le système hyperchaotique de Lorenz et de l'algorithme Rivest-Shamir-Adle man (RSA). Puis nous avons l'implémenté sous logiciel « MATLAB ».

Pour analyser la méthode précédente nous avons effectué un ensemble de tests quimontrent la bonne robustesse de notre algorithme. Les résultats expérimentaux ont prouvé que le schéma de cryptage d'image proposé est efficace et a une forte anti -attaque et présenteune sensibilité à la clé,donc il présente un niveau élevé de sécurité et de performance.

Comme perspective à ce travail, nous allons étudier comment améliorer l'efficacité du schéma pour les images en couleur. Nous souhaitons continuer en utilisant de nouvelles idées dans notre méthode de chiffrement et proposer un algorithme de sélection de pixels spécifique pour les chiffrer

Bibliographie

(Arab,2018) :K.Arab,D Arbane, Conception de crypto-systèmes à base de systèmes chaotiques d'ordre fractionnaire : Application au cryptage de la parole,Mémoire Master, Université Mouloud MammeriTizi-Ouzou,2018.

(Badaoui,2021) :A.Badaoui,A.Guendouz,S.Khemidja, Etude des suites chaotiques et leurs applications en cryptage d'images, Mémoire Licence,Université de Mohamed El-Bachir El-Ibrahimi - Bordj Bou Arreridj,2021.

(Bekkouche, 2018) : T.Bekkouche, Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes, Thèse de doctorat, Université FERHAT ABBAS SETIF-1,2018.

(Belkadi,2018) : I.Belkad, N.Amiar, Cryptage d'image par considération desplans de bits des pixels séparément parordre de leurs poids avec une clé publiquede taille libre,Mémoire de Master,Université LARBI BEN M'HIDIOUM EL BOUAGHIFACULTE, 2018.

(Benayache,2020) :H.Benayache,O.ROUIKHA,Compression de l'information à l'aide de systèmes chaotiques,Mémoire Master, Université Mohamed SeddikBenYahia Jijel,2020.

(Benzmam,2010) :D.Benzmam, Systèmes chaotiques et hyperchaotiquespour la transmission sécurisée de données,Thèse de Doctorat ,Université Abou BkerBelkaid Tlemcen,2010.

(Berkan,2016) :A.Berkane,Transmission sécurisée à base de la synchronisation impulsive de deux systèmes chaotiques discrets, Mémoire Master, Université Mouloud Mammeri Tizi-Ouzou,2016.

(Bessam,2020) :A.Bessam, Etude d'un système dynamique chaotique, Mémoire Master, Université Mohamed Khider, Biskra,2020.

(Bouchakour,2018) :F.Bouchakour, La stabilité du système hyperchaotique le plus général de dimension quatre, Mémoire Master,Université Larbi Ben M'hidi – OUM EL BOUAGHI,2018.

(DIACONU, 2017) : Adrian-ViorelDiaconu, Ana Cristina Dascalescu, Correlation distribution of adjacent pixels randomess test for image encryption, Proceedings of the Romanian academy, Series A, Volume 18, Special Issue 2017, pp. 351-360, 2017.

(Djemaa, 2021) : A.Djemaa, A.Boubednikh, Réalisation d'un Système de Cryptage des Images Numérique basé sur le Chaos, Mémoire Master, Université Mohamed Sadik BENYAHIA de Jijel, 2021.

(Ferdush, 2021):JannatulFerdush, MahbubaBegum, and Mohammad Shorif Uddin, Chaotic Lightweight Cryptosystem for Image Encryption, Hindawi Advances in Multimedia Volume 2021.

(Ferik,2020) : B.Ferik, **T**echnique d'encryption efficace dédiée pour une donnée volumineuse, mémoire master, UNIVERSITE ECHAHID HAMMA LAKHDAR - EL OUED, 2020.

(Filali,2020) :H.Filal, K.Chouchane, Un algorithme pour le calcul desexposants de Lyapunov d'un système dynamique, Mémoire Master, Centre UniversitaireAbdElhafidBoussouf – Mila,2020.

(Goumidi,2010) :D.Goumidi, Fonction logistique et standard chaotique pour le chiffrement des images satellitaires, Mémoire Master, Université Mentouri de Constantine,2010.

(Hamada,2020) : A. Hamada, Y.Bousnoubra, La cryptographie des images numériques par la carte logistique chaotique, Mémoire Master, Université 8Mai 1945 –Guelma,2020.

(Hannoun,2014) :K.Hannoun , Etude Simulation et implémentation d'un émetteur hyper chaotique sur carte ArduinoUno, Mémoire Master, Université Mouloud Mammeri Tizi-Ouzou,2014.

(Ikhlef,2007) :A.Ikhlef, Contrôle, chaotification et hyperchaotification des systèmes dynamiques, Thèsede Doctorat,Université de Mentouri Constantine, 2007.

(Khouildat, 2019) : H.Khouildat, Méthode de cryptage d'image basée sur la permutation et la matrice de Householder, Mémoire MASTER, Université KASDI-MERBAH Ouargla, 2019.

(Kouadri,2014) :M.Kouadri, Tests de validation pour les crypto-systèmes Chaotiques,Mémoire Master, Université de Sciences et de la Technologie d'Oran Mohamed Boudiaf,2014.

(Krim,2019) :M.Krim, Implémentation des séquences chaotiques sur les systèmes de communication moderne :Etalement de spectre à séquence directe DS-SS,Thèse de Doctorat, Université de Sciences et de la Technologie d'Oran Mohamed Boudiaf,2019.

(Lakhdari,2020) :K.Lakhdari,Analyse et contrôle de systèmes dynamiquesChaotiques,MémoireMaster,Université Mohamed Khider, Biskra,2020.

(Letellier, 2007) : Christophe Letellier, Otto E. Rossler, 2007, Hyperchaos, disponible sur : http://www.scholarpedia.org/article/Hyperchaos#The_first_hyperchaotic_system consulté le 06/02/2021.

(Lin, 2021): R. Lin and Sheng Li, An Image Encryption Scheme Based on Lorenz HyperchaoticSystem and RSA Algorithm, Hindawi, Security and Communication Networks, Volume 2021, Article ID 5586959, 2021.

(Rezzag,2016) :S.Rezzag, Etude et estimation des bornes de systèmes dynamiques chaotiques et hyper chaotiques, Thèse de doctorat, Université Larbi Ben M'hidi, 2016.

(Rimani,2021) :R.Rimani,Sécurisation des images par une combinaisondes techniques de chiffrement et de recalage d'image, Thèse de Doctorat, UNIVERSITE MOHAMED BOUDIAF ORAN,2021.

(Saad, 2012) : N. Saad, L'apport des bandelettes par rapport aux ondelettes dans les applications de traitement d'images, Mémoire Master, UNIVERSITE TIZI OUZOU, 2012.

(Souleres, 2022) : Thierry Souleres, Le systeme de Lorenz. Disponible sur : https://hmf.enseeiht.fr/travaux/CD9598/travaux/optmfn/IH/98PA/lorenz/lorenz.html#:~:text=Le%20systeme%20de%20Lorenz%20est,alors%20decrit%20que%20quelques%20boucles. Consulté le :02/02/2022

(Zhang, 2014) : Xianhan Zhang and Yang Cao, A Novel Chaotic Map and an Improved Chaos-Based Image Encryption Scheme, Hindawile Scientific World Journal Volume 2014.

Webographie

[1] :https://www.youtube.com/watch?v=vIaCEVtoxm4&list=PLYufX86sb3TvcuepC7o0XWgBuQaXPtvV

[2] :http://www.traitement-signal.com/traitement_d_images.php

[3] :https://www.youtube.com/watch?v=gOzaoP89xag&list=PLYufX86sb3TvcuepC7o0XWgBuQaXPtvV&index=2

[4] :https://datascientest.com/image-processing-tout-savoir

[5] :https://www.geeksforgeeks.org/digital-image-processing-basics/?ref=lbp

[6] :https://www.youtube.com/watch?v=H48_fxbx24k&t=75s

[7] :https://patrick-bonnin.developpez.com/cours/vision/Bases-du-Traitement-Image/Chap1/#LV-A

[8] :https://docplayer.fr/82396638-Chapitre-2-concepts-de-cryptographie-et-de-cryptanalyse.html

[9] :https://www.itpro.fr/qu-est-ce-que-cryptage-donnees/

[10] :https://www.emajit.com/conseils-informatique-cybersecurite/quest-ce-que-cryptage-chiffrement/

[11] :https://www.fortinet.com/resources/cyberglossary/encryption

[12] :https://www.techtarget.com/searchsecurity/definition/encryption

[13] :https://www.netinbag.com/fr/internet/what-is-a-cryptosystem.html

[14] :https://commentouvrir.com/blog/cryptosysteme/

[15] :https://medium.com/@prashanthreddyt1234/real-life-applications-of-cryptography-162ddf2e917d

[16] :https://www.analyticssteps.com/blogs/characteristics-types-and-applications-cryptography

[17] :https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/cryptographie-authentification-protocoles-de-securite-vpn-42314210/cryptographie-appliquee-h5210/applications-de-la-cryptographie-protocoles-de-communication-h5210niv10004.html

[18] :https://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/life.html#:~:text=Encryption%20is%20used%20in%20electronic,key%20encryption%20can%20provide%20confidentiality

[19]: http://www.cryptage.org/applications-cryptographie.html

[20]: http://elearning.centre-univ-mila.dz/pluginfile.php/13220/mod_resource/content/0/SYSTEMES%20CHAOTIQUES.pdf

[21]: https://www.techno-science.net/definition/1291.html

https://hmf.enseeiht.fr/travaux/CD9598/travaux/optmfn/IH/98PA/lorenz/lorenz.html

[22]: https://fr.wikipedia.org/wiki/Effet_papillon

[23]: https://fr-academic.com/dic.nsf/frwiki/152736

[24]: https://complexe.jimdofree.com/la-th%C3%A9orie-du-chaos/les-suites-logistiques/l-exposant-de-lyapunov/

[25]
https://en.wikipedia.org/wiki/List_of_chaotic_maps#:~:text=In%20mathematics%2C%20a%20chaotic%20map,the%20study%20of%20dynamical%20systems