*République Algérienne Démocratique et Populaire*
*Ministère de l'Enseignement Supérieur Et de La Recherche Scientifique*

*Université de Ghardaïa*

N° d'ordre :
N° de série :

Faculté des Sciences et Technologies
Département d'automatique et électromécanique

**Mémoire présenté en vue de l'obtention du diplôme de**

# MASTER

**Domaine :** *Sciences et Technologies*
**Filière :** *Automatique*
**Spécialité :** *Automatique et Système*

**Par** : ***Hamel Mohamed Mokhtar et Anteur Tarek***

# Thème

***Utilisation croisé d'hyperchaotiques et des séquences d'ADN pour cryptage d'image***

**Soutenu publiquement le 21/10/2020**

**Devant le jury :**

| | | | |
|---|---|---|---|
| **Hadj Yahia Seba** | Grade | Université | **Président** |
| **Bokhari Hamed** | Grade | Université | **Examinateur** |
| **Ladjel Boumediene** | Grade | Université | **Examinateur** |
| **Arif Mohamed** | Grade | Université | **Encadreur** |

**Année universitaire 2019/2020**

# *Dédicace*

***Avec l'expression de ma reconnaissance, je dédie ce modeste travail à ceux qui, quels que soient les termes embrassés, je n'arriverais jamais à leur exprimer mon amour sincère***
***A l'homme, mon précieux offre du dieu, qui doit ma vie, ma réussite et tout mon respect : mon cher père.***

***A la femme qui a souffert sans me laisser souffrir, qui n'a jamais dit non âmes exigences et qui n'a épargné aucun effort pour me rendre heureuse: mon adorable mère.***

***Et aux honorables professeurs***

***Vous avez tous les éloges et l'appréciation de notre part, pour le nombre de gouttes de pluie, les couleurs des dés et l'arôme du parfum, pour vos efforts précieux et précieux pour l'avancement du chemin de notre université.***

***Anteur Tarek***

# *Dédicace*

*Je dédie ce mémoire à mes chers parents qui m'ont toujours poussé et motivé dans mes études .sans eux, je n'aurais certainement pas fait d'études longues. Ce mémoire fin d'étude représente donc l'aboutissement du soutien et des encouragements qu'ils m'ont prodigués tout au long de ma scolarité. Qu'ils en soient remerciés par cette trop modeste dédicace.*

*c'est un moment de plaisir de dédier cet travail à ma femme et mes seurs en signe d'amoure de reconnaissance et de gratitude pour le dévouement et les sacrifices dont vous avez fait toujours preuve à mon égard.*

*et finalement à mes amies et tout les membres mnea qui n'ont jamais cessé de me soutenir.*

*Hamel Med Mokhtar*

# *Remerciements*

*Tout d'abord, nous remercions Dieu notre Créateur de nous avoir donné la force et la volonté pour terminer ce travail. Nous remercions M. Arif Mohammed pour sa suggestion et sa gestion de ce travail et nous sommes reconnaissants de sa présence, de son attention, de ses encouragements, de ses observations et de ses conseils qui ont contribué au développement de ce travail. Nous tenons à remercier nos familles pour leur soutien et leur aide à tous égards. Nous remercions enfin tous les enseignants du département Automatique, tous les amis Et tous ceux qui nous ont aidés dans ce travail de près ou de loin.*

## Résumé

Nous avons proposé un algorithme de chiffrement nouveau et efficace basé sur le chaos et les règles d'encodage de l'ADN. Piecewise Linear Chaotic Map (PWLCM) et Logistic Map sont appliqués pour générer tous les paramètres dont l'algorithme présenté a besoin et les fonctions de la technologie d'encodage de l'ADN en tant qu'outil auxiliaire. L'algorithme proposé se compose de ces parties: premièrement, utiliser PWLCM pour produire une image clé, dont les pixels sont générés par chaos ; Deuxièmement, encodez l'image simple et l'image clé avec des règles d'ADN par lignes respectivement et différentes lignes sont codées selon les différentes règles décidées par carte logistique; Après cela, utilisez l'image clé codée pour effectuer des opérations d'ADN avec l'image simple codée ligne par ligne pour obtenir une image intermédiaire et l'opération spécifique exécutée chaque ligne est choisie par carte logistique; Ensuite, décoder l'image intermédiaire comme l'image simple de l'étape suivante. Enfin, répétez les étapes ci-dessus par les colonnes à nouveau pour obtenir l'image de chiffrement ultime. Les résultats et l'analyse de l'expérience indiquent que l'algorithme proposé est capable de résister aux attaques typiques et a un bon caractère de sécurité.


**Mots-clés :** Chiffrement d'image. Chaos. Codage d'ADN. Carte chaotique linéaire par morceaux. Carte logistique


## Abstract

We proposed a novel and effective image encryption algorithm based on Chaos and DNA encoding rules. Piecewise Linear Chaotic Map (PWLCM) and Logistic Map are applied to generate all parameters the presented algorithm needs and DNA encoding technology functions as an auxiliary tool. The proposed algorithm consists of these parts: firstly, use PWLCM to produce a key image, whose pixels are generated by Chaos ; Secondly, encode the plain image and the key image with DNA rules by rows respectively and different rows are encoded according to various rules decided by logistic map; After that, employ encoded key image to conduct DNA operations with the encoded plain image row by row to obtain an intermediate image and the specific operation executed every row is chosen by logistic map; Then, decode the intermediate image as the plain image of next step. Finally, repeat steps above by columns again to get the ultimate cipher image .The experiment results and analysis indicate that the proposed algorithm is capable of withstanding typical attacks and has good character of security.

**Keywords :** Image encryption . Chaos. DNA encoding. Piecewise linear chaotic map. Logistic map.

**ملخص**

اقترحنا خوارزمية تشفير جديدة وفعالة تستند إلى قواعد الفوضى وترميز الحمض النووي. يتم تطبيق خريطة الفوضى الخطية (PWLCM) و "خريطة لوجستية" لتوليد جميع المعلمات احتياجات الخوارزمية المقدمة ووظائف تكنولوجيا ترميز الحمض النووي كأداة مساعدة. وتتألف الخوارزمية المقترحة من هذه الأجزاء: أولا، استخدام PWLCM لإنتاج صورة رئيسية، التي يتم إنشاؤها بكسل من الفوضى; ثانيا ، ترميز الصورة العادية والصورة الرئيسية مع قواعد الحمض النووي من قبل الصفوف على التوالي ، ويتم ترميز الصفوف المختلفة وفقا لقواعد مختلفة تقررها خريطة اللوجستية ؛ بعد ذلك، استخدم صورة مفتاح مشفرة لإجراء عمليات الحمض النووي مع ترميز صورة عادية صف للحصول على صورة وسيطة ويتم اختيار عملية محددة تنفيذ كل صف من قبل خريطة لوجستية؛ ثم فك ترميز الصورة المتوسطة كصورة عادية للخطوة التالية. وأخيرا ، كرر الخطوات أعلاه بواسطة الأعمدة مرة أخرى للحصول على صورة التشفير في نهاية المطاف. تشير نتائج التجربة وتحليلها إلى أن الخوارزمية المقترحة قادرة على تحمل الهجمات النموذجية ولها شخصية جيدة من الأمان.

**الكلمات المفتاحية**: تشفير الصور . الفوضى. ترميز الحمض النووي. خريطة فوضوية خطية. خريطة لوجستية

# *Liste des figures*

# *Liste des tableaux*

# *Sommaire*



## Chapitre I : Généralités sur le traitement d'images.

## Chapitre II : Généralités sur la Cryptographie, Méthodes et Algorithmes

## Chapitre III: Nouvelle méthodes (ADN)

## Introduction Générale :

Le développement des réseaux informatiques, l'utilisation accrue d'Internet à l'heure actuelle et l'augmentation significative de l'échange de messages multimédias et d'images numériques ont conduit à la dépendance à l'égard de ces technologies dans diverses questions de vie.

La fourniture d'informations de sécurité mutuelle est une exigence nécessaire pour toutes les utilisations, que ce soit à des fins politiques, médicales, économiques et même personnelles. Au fur et à mesure que les images numériques pénètrent dans tous ces domaines, un large éventail de recherches et d'algorithmes de cryptage d'images numériques ont été fournis. En raison des caractéristiques des informations d'image numérique sur les informations textuelles telles que la quantité des données élevées et l'interconnexion étroite entre les informations d'image et d'autres caractéristiques propres aux images numériques des données textuelles, en plus du besoin d'applications photo dans certains cas à d'autres exigences telles que le traitement en temps réel et la précision et le maintien de la coordination d'image, ce qui rend les méthodes de cryptage traditionnelles difficiles à appliquer et le traitement lent pour les images et la difficulté d'atteindre ces exigences avec une haute sécurité et de haute qualité, algorithmes de cryptage traditionnels ne sont pas adaptés au cryptage Photos numérique , La tendance était donc à d'autres théories et algorithmes pour fournir des spécifications de cryptage et de sécurité élevées pour l'image numérique. Au cours des dernières années, la théorie du chaos dans le domaine du cryptage a été utilisée pour les avantages de cette théorie et de sa relation étroite avec la science de la cécité, où elle se caractérise par sa grande sensibilité au changement des valeurs primaires et la facilité de générer leurs valeurs et d'obtenir des valeurs aléatoires similaires au bruit d'eux.

Depuis que la scientifique Jessica Frederick a proposé un système de cryptage photo utilisant la théorie anarchiste en 1997, la recherche a été en cours dans le domaine du cryptage d'image en utilisant la théorie du chaos.

Il y a quelques années, cette théorie a été combinée à l'utilisation du cryptage basé sur l'ADN basé sur l'informatique d'ADN (DNA Computing) pour obtenir des systèmes de cryptage et des algorithmes efficaces. Le début de la science de l'informatique de l'ADN avec la recherche du scientifique Leonard Edelman en 1994, dans lequel il a été en mesure d'utiliser des bandes d'ADN et des processus biologiques moléculaires pour résoudre le

problème de l'homme voyageant entre sept villes et, ce faisant, a ouvert de nouveaux horizons pour la science de l'informatique ultra-rapide et énorme parallèle et un niveau très élevé de complexité en raison des propriétés possédées par l'analyse de l'ADN des chaînes d'ADN a été utilisé dans de nombreux domaines, y compris les questions difficiles qui ne peuvent pas être résolus en raison de ressources limitées en raison du temps limité ou de la durée limitée. En 1995, les chercheurs ont fourni un moyen de briser l'algorithme d'ADN (DES) connu sous le nom de calcul de l'ADN, et en 2000 les processus biologiques ont été utilisés pour chiffrer les images à l'aide du cryptage de l'ADN et deux façons de chiffrer l'image ont été proposées ainsi qu'un moyen de cacher des informations dans les bandes d'ADN. Les chercheurs ont introduit des algorithmes pour chiffrer l'image en combinant la théorie anarchiste avec le codage à l'aide de l'ADN, en utilisant différentes cartes anarchistes et différentes propriétés et processus de l'ADN, tels que l'utilisation de la méthode de collecte et de soustraire les bases d'azote, ou en utilisant une fonction exclusive (fonction XOR) entre ces règles, ou en utilisant d'autres propriétés basées sur la base de processus biologiques, puis analysé les propriétés des algorithmes proposés et leur immunité à plusieurs types d'attaques et d'analyses. [0]

Le but de notre travail consiste à développer l'utilisation croisé d'hyperchaoliques et de séquences d'ADN pour cryptage d'image.

Ce mémoire s'organise autour de trois chapitres :

- Le premier chapitre est consacré à une étude bibliographique qui retrace les notions de base sur le traitement d'image.
- Le deuxième chapitre concerne une généralité sur la cryptographie et l'historique de développement des algorithmes de cryptage.
- Dans le troisième chapitre on développe la modélisation mathématique de ce travail et présentons et discutons les résultats obtenus par ce modèle développé.

Nous finalisons ce mémoire par une conclusion générale qui est le fruit de ce travail, elle résume les résultats obtenus dans ce travail et donne des perspectives pour les prochains travaux de recherche.

# 1. Introduction :

Les images constituent l'un des solutions les plus importants qu'utilise l'homme pour transmettre et livrer le savoir et l'information depuis l'aube de l'humanité, dans la mesure où une image à elle seule peut réunir une quantité énorme d'informations. Un système de traitement d'images se compose principalement des fonctions suivantes : acquisition d'images, un prétraitement pour la diminution du bruit, analyser l'image pour arriver à une description synthétique de l'information brute incluse dans l'image. Dans ce chapitre nous allons introduire quelques notions générales dans le domaine de traitement d'image.

# 2. Définition générale :

## 2.1 L'image :

L'image définie une reproduction ou une représentation analogique exacte d'une scène réelle, elle aussi désignée comme une scène tridimensionnelle sur un support en deux dimensions. L'image contient en chaque point, une intensité lumineuse, celle-ci peut être représentée sous forme d'une fonction f avec deux variables x et y qui présentent les coordonnées linéaires d'un point de l'image, la fonction f présente l'intensité lumineuse définie sur un domaine bien défini. Dans le cas où une image est inexploitable par l'ordinateur, elle nécessite sa numérisation à l'aide de diverses méthodes.[a]

## 2.2 L'image numérique :

Une image numérique désigne toute image tel que le dessin, l'icône…, converti de son état analogique d'origine par des convertisseurs numériques. L'image numérique peut être aussi crée directement à l'aide des programme informatiques comme la modélisation en trois dimensions.[a]

## 2.3 Différents types d'image numérique :

Il existe différents types d'image numérique :

### 2.3.1 Image vectorielle :

Une image vectorielle appelée aussi une image en mode trait, est une image numérique composée par des formules géométriques individuelles, des primitives géométriques (cercle, courbe de Bézier, droite) définie pour différentes caractéristiques comme leur forme, position,

couleurs, etc… Ces modifications peuvent conduire à l'obtention de différentes transformations telles que l'écrasement de l'mage, inclinaison, agrandissement, sans perdre la qualité initiale de cette image.[a]

### 2.3.2 Images matricielles :

Une image matricielle nommée aussi carte de point (bitmap), est une image constituée d'une matrice ou d'un tableau sous forme de grille) ou chaque case possède une couleur (point coloré) qui lui est propre. Il s'agit donc d'une juxtaposition de point de couleur formant dans leur ensemble, une image, ces points de couleurs appelés dans le domaine d'image numérique « pixel ». Les avantages de ce mode sont :

- Simplicité de stockage en mémoire, puisqu'il suffit de coder la succession des valeurs de la matrice.
- Grande facilité de traitement par des algorithmes primitifs au niveau du pixel.
- Les inconvénients de ce type de représentation sont de deux ordres :
- Espace mémoire important pour gérer des grandes images ou des images de bonne qualité.
- Algorithme de tracé plus complexe (défaut de reproduction dû au mode d'affichage des lignes en marche d'escalier).[a]

## 2.4 Caractéristiques d'une image numérique :

### 2.4.1 Pixel :[a]

Le pixel est l'unité de base permettant de mesurer la définition d'une image numérique matricielle. Le pixel (extrait des mots anglais "Picture element") est le plus petit élément de l'image. Il possède une valeur I (i, j) qui représente son niveau de gris (I étant la matrice représentant l'image). les coordonnées i, j donnent sa position dans l'image I. Il peut être représenté en mémoire sur :

- Un bit (0 ou 1) pour les images monochromes : 0 pour le noir et 1 pour le blanc.
- Un octet, soit 256 niveaux de gris pour une image à niveaux de gris : 0 noir et 255 blancs.

La couleur du pixel est la combinaison des trois nuances de chaque couleur. Trois octets pour une image couleur (RVB) :

- 1 octet pour la couleur rouge (256 nuances de rouge).
- 1 octet pour la couleur verte (256 nuances de vert).
- 1 octet pour la couleur bleue (256 nuances de bleu).

### 2.4.2 Résolution : [b]

La résolution est déterminée par le nombre de points par unité de surface. Généralement exprimée par pouce (un pouce représentant 2,54 cm).

246 x 273 (pixels) 64×64 25×25

Figure 1.1 : Résolution d'une image.

### 2.4.3 Luminance : [b]

La luminance est le degré de luminosité de chaque point de l'image. Elle est définit comme étant le quotient de l'intensité lumineuse d'une surface.

### 2.4.4 Contraste : [b]

Si L1 et L2 sont les degrés de luminosité respectivement de deux zones voisines A1 et A2 d'une image, le contraste C est défini par le rapport :

$$c = \frac{L1-L2}{L1+L2} \qquad (1.1)$$

### 2.4.5 Histogramme d'une image :

Un histogramme est une représentation statistique indiquant la répartition des pixels, selon leur valeur, d'une image. Elle dénombre chaque niveau de gris et le représente en fonction de sa valeur.

### 2.4.6 Bruit :

C'est un signal, qui lors de l'acquisition vient s'ajouter à l'image, Il se matérialise par la présence dans une région homogène des valeurs plus ou moins éloignées de l'intensité de la région. Le bruit est le résultat de certains défauts électroniques du capteur et de la qualité de numérisation. Il existe plusieurs types de bruits : Gaussien, Salt and Pepper, Poisson …etc.

## 2.5 Traitement d'images : [b]

Le traitement d'images est défini comme l'ensemble des techniques qui permettent de calculer à partir d'une image d'entrée une nouvelle image de sortie. Pour faire le traitement, il faut analyser l'image (classification, description des différentes régions qu'elle contient, mesure des paramètres … etc) ainsi que son interprétation (relation entre les régions et l'objet de façon à donner un sens).

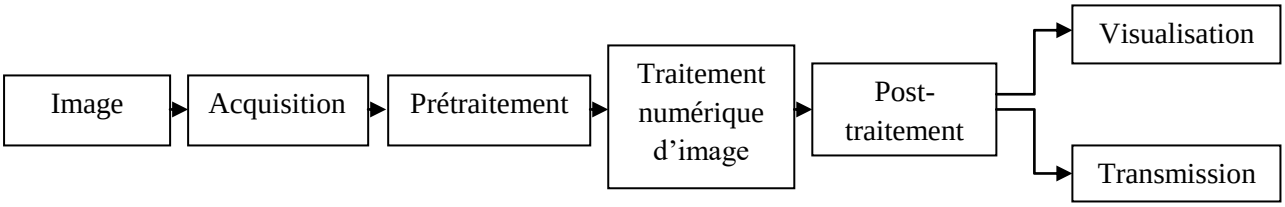



Figure 1.2 Etapes de traitement d'images.

Le traitement d'images regroupe plusieurs disciplines que l'on classe en deux catégories :

- Les processus de bas-niveaux, qui nécessitent très peu d'informations sur le contenu de l'image. Il s'agit ici de : filtrage, amélioration et restauration d'images.
- Les processus de haut-niveaux, qui nécessitent des informations sur le contenu des images. Il s'agit de : reconnaissance de formes, Segmentation.

### 2.5.1 Acquisition d'une image :

L'acquisition d'images est une mesure spatiale d'une interaction entre une onde et de la matière. L'onde est émise par une source et reçue par un capteur. Par exemple dans le cas de l'échographie, l'ultrason, une onde acoustique, est émise et reçue par la sonde. L'interaction est la réflexion de l'ultrason sur la structure du corps.

Dans le cas d'onde électromagnétique, la photographie utilise le spectre visible c'est-à-dire qui est visible pour l'œil humain. Il y a des applications sur l'ensemble du spectre électromagnétique, des rayons gamma jusqu'aux ondes radio. Ainsi, les images acquises

par rayons X ou par rayons gamma sont surtout utilisées en imagerie médicale et en astronomie. En médecine, on utilise des imageurs IRM, TEP, scanner X, échographie Doppler, échographie, scintigraphie, tomographie.

Les deux caractéristiques importantes de la mesure spatiale est la taille du plus petit élément (pixel), mais aussi l'intercorrélation de deux éléments voisins : plus cette intercorrélation est faible, meilleure est l'image.

### 2.5.2 Prétraitement : [b]

#### 2.5.2.1 Filtrage :

Le but du filtrage est de diminuer l'amplitude des perturbations liées au bruit. On peut définir le filtrage comme le remplacement d'un pixel par une valeur qui est fonction des données de proximité du pixel. On distingue plusieurs types de filtres : moyenner, médian, …..etc.

**(A)** **(B)**

Figure 1. 3 : (A) Image bruitée, (B) Application d'un filtre médian.

#### 2.5.2.2 Amélioration d'images :

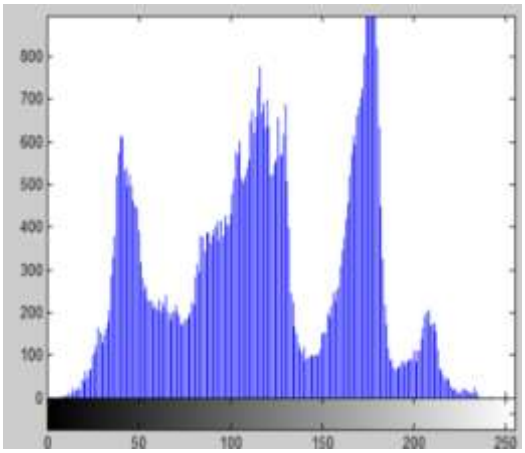
L'amélioration d'images consiste à modifier les caractéristiques visuelles de l'image de manière à en faciliter son interprétation par l'œil humain. Il peut s'agir de rehausser les contrastes, d'accentuer certaines intensités pour mettre en valeur une région, ... Les histogrammes sont fréquemment utilisés pour effectuer ce type d'opérations.

### 2.5.2.3 Égalisation d'histogramme :

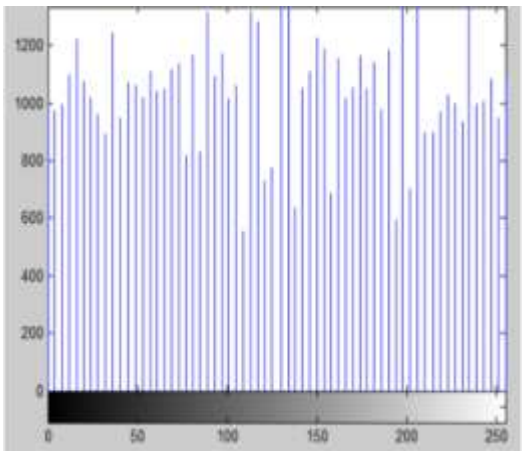
L'égalisation d'histogramme est une méthode d'ajustement du contraste d'une image numérique qui utilise l'histogramme. Il permet alors de renforcer le contraste sur des détails, qui sont masqués par des variations d'intensité de plus grande amplitude.

(A)

(B)




(C)




(D)

Figure1.4 : (A) Image originale, (B) Image améliorée, (C) histogramme de l'image A,

(D) histogramme égalisée.

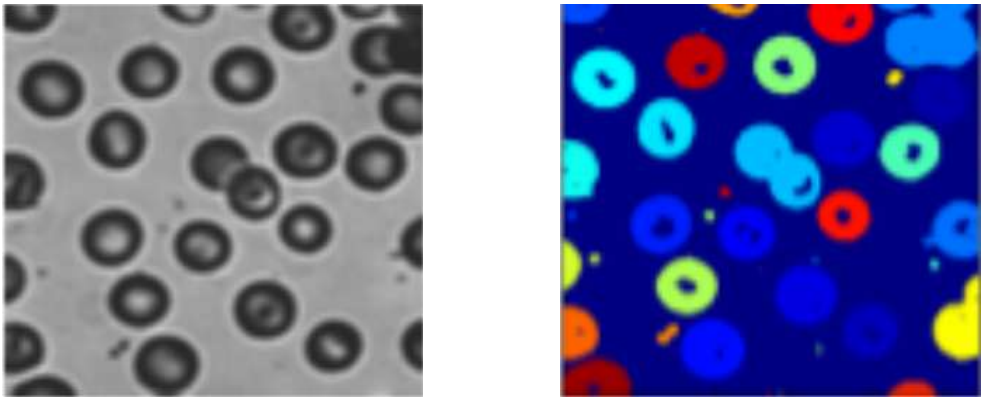
### 2.5.3 Segmentation d'images :

La segmentation consiste à découper une image en régions connexes de niveaux de gris, présentant une homogénéité selon un certain critère. Une multitude de méthodes de

segmentation sont proposées dans la littérature, elles se répartissent en trois grandes familles : la segmentation par approche contour, région et classification.

### 2.5.3.1 Approche région :

Une région est un ensemble de pixels ayant des caractéristiques communes (intensité, texture … etc.), qui les différencient des pixels des régions voisines. L'approche région a pour objectif de décomposer l'image en un ensemble de régions connexes les plus homogènes possible, et les plus différentes pour celles qui se côtoient.

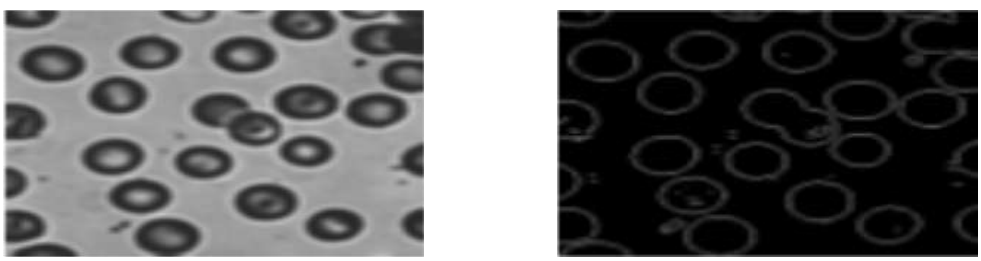


(A) (B)

Figure1.5 : (A) Image originale, (B) Image Segmentée par région.

### 2.5.3.2 Approche contour :

Un contour est un ensemble de pixels formant une frontière entre deux ou plusieurs régions voisines, où la limite ente deux pixels dont le niveau de gris représente une différence significative. L'approche contour consiste à identifier les discontinuités qui séparent les différentes régions de l'image, cette approche cherche les di similarités.



(A) (B)

Figure 1.6 : (A) Image originale, (B) Image Segmentée par Contour.

## 3. Conclusion :

Nous avons présentés dans ce chapitre, une introduction générale et quelques notions sur le traitement d'image utilisés dans le domaine informatique.

Le traitement d'images est l'ensemble des techniques permettant de modifier une image dans le but de l'améliorer ou d'en extraire des informations. Ce traitement, souvent appelé prétraitement, il regroupe toutes les techniques visant à améliorer la qualité d'une image.

Tous ces travaux ont pour préparer une image presque parfait pour la phase de cryptage, dans le chapitre qui suit, nous expliquons les termes cryptage, encryptage et décryptage, et donnons une idée générales sur quelques algorithmes de cryptage, et expliquons notre modèle utilisée dans cette thèse.

# 1 .Introduction

Le nombre des besoins pour sécuriser la vie quotidienne restent toujours en croissance. Pour cette raison, plusieurs systèmes cryptographiques ont été développés pour satisfaire ces besoins. La cryptologie est la « science du secret »,et regroupe deux branches : la cryptographie, et la cryptanalyse. En particulier, le cryptage des images et des vidéos a beaucoup d'applications dans divers domaines, tel que la communication mobile, Internet, l'imagerie médicale, la télémédecine et les communications militaires. La cryptographie est utilisée pour atteindre la flexibilité, la conformité et l'intimité des données qui sont des exigences dans les systèmes d'aujourd'hui. Dans ce chapitre nous présentons les notions de base liés à la cryptographie.

# 2. Cryptage et décryptage

Les données lisibles et compréhensibles sans intervention spécifique sont considérées comme du texte en clair. La méthode permettant de dissimuler du texte en clair en masquant son contenu est appelée le cryptage. Le cryptage consiste à transformer un texte normal en charabia inintelligible appelé texte chiffré. Cette opération permet de s'assurer que seules les personnes auxquelles les informations sont destinées pourront y accéder. Le processus inverse de transformation du texte chiffré vers le texte d'origine est appelé le décryptage. [c]

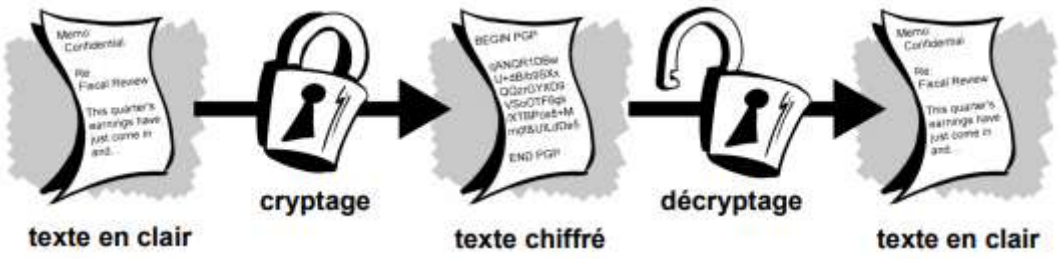



Figure 2.1 Cryptage et décryptage. [1]

# 3. Vocabulaire de base : [d]

- **Texte en clair** : c'est le message à protéger.
- **Texte chiffré** : c'est le résultat du chiffrement du texte en clair.
- **Chiffrement** : c'est la méthode ou l'algorithme utilisé pour transformer un texte en clair texte chiffré.

- **Déchiffrement :** c'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair.
- **Clé** : c'est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré et pour déchiffrer le texte chiffré en texte en clair. On peut parfaitement concevoir un algorithme qui n'utilise pas de clé, dans ce cas c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé.
- **Cryptographie** : cette branche regroupe l'ensemble des méthodes qui permettent de chiffrer et de déchiffrer un texte en clair afin de le rendre incompréhensible pour quiconque n'est pas en possession de la clé à utiliser pour le déchiffrer.
- **Cryptanalyse** : c'est l'art de révéler les textes en clair qui ont fait l'objet d'un chiffrement sans connaître la clé utilisée pour chiffrer le texte en clair.
- **Cryptologie :** il s'agit de la science qui étudie les communications secrètes. Elle est composée de deux domaines d'étude complémentaires : la cryptographie et la cryptanalyse.
- **Décrypter** : c'est l'action de retrouver le texte en clair correspondant à un texte chiffré sans posséder la clé qui a servit au chiffrement. Ce mot ne devrait donc être employé que dans le contexte de la cryptanalyse**.** [d]

## 3.1 Définition Cryptographie

La cryptographie est la science qui utilise les mathématiques pour le cryptage et le décryptage de données. Elle vous permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (tels que l'Internet), afin qu'aucune personne autre que le destinataire ne puisse les lire. Alors que la cryptographie consiste à sécuriser les données, la cryptanalyse est l'étude des informations cryptées, afin d'en découvrir le secret. La cryptanalyse classique implique une combinaison intéressante de raisonnement analytique, d'application d'outils mathématiques, de recherche de modèle, de patience, de détermination et de chance. Ces cryptanalyses sont également appelés des pirates. La cryptologie englobe la cryptographie et la cryptanalyse. [c]

Le chiffrement se fait généralement à l'aide d'une clef de chiffrement, le déchiffrement nécessite quant à lui une clef de déchiffrement. On distingue généralement deux types de clefs:

- Les clés symétriques: il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète.

- Les clés asymétriques: il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé chiffrement à clé publique). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement**. [e]**

## 4. L'usage de la cryptographie

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

**La confidentialité** : consiste à rendre l'information l'intelligible à d'autres personnes que les acteurs de la transaction.

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

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

**La non répudiation :** de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.

## 5. Mécanismes de la cryptographie

Un algorithme de cryptographie ou un chiffrement est une fonction mathématique utilisée lors du processus de cryptage et de décryptage. Cet algorithme est associé à une clé (un mot, un nombre ou une phrase), afin de crypter le texte en clair. Avec des clés différentes, le résultat du cryptage variera également. La sécurité des données cryptées repose entièrement sur deux éléments : l'invulnérabilité de l'algorithme de cryptographie et la confidentialité de la clé. Un système de cryptographie est constitué d'un algorithme de cryptographie, ainsi que de toutes les clés et tous les protocoles nécessaires à son fonctionnement. [c]

## 6. Les clés en cryptographie

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

### 6.1 Les clés symétriques (ou clé secrète)

Autrement appelée cryptage à clé privée, ce type se base sur l'utilisation d'une clé pour crypter et décrypter les messages. La sécurité de cette solution repose sur le fait que la clé est connue uniquement par l'émetteur et le récepteur du message.


Figure 2.2 Principe de cryptage symétrique.

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

Le cryptage symétrique fonctionne selon deux procédés différents :

- le cryptage par flot : le cryptage s'effectue en continu, bit par bit
- le cryptage par bloc : le cryptage s'effectue sur les blocs de bits

On peut citer l'algorithme Data Encryption System (DES) et L'International Data Encryption Algorithm (IDEA) comme le plus connu de ces algorithmes.

#### 6.1.1 Les avantages

- ❖ la rapidité d'exécution (une seule clé utilisée).
- ❖ la simplicité d'implémentation (gestion d'une seule clé).

### 6.1.2 Les inconvénients

- ❖ la complexité de fonctionnement : une obligation d'avoir le nombre de clés privées égal au nombre de destinataires.
- ❖ la sécurisation de la chaîne de transmission de la clé.

## 6.2 Les clés asymétriques (ou clé publique)

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

Pour bien comprendre le principe, on peut l'illustrer avec l'échange d'une lettre entre un émetteur et un destinataire :

- l'émetteur possède deux clés : privé et publique. Il envoie sa lettre contenant la clé publique au destinataire.
- le destinataire utilise la clé publique pour crypter son message; il envoie tout à l'émetteur initial
- l'émetteur utilise sa clé privée pour décrypter le message.

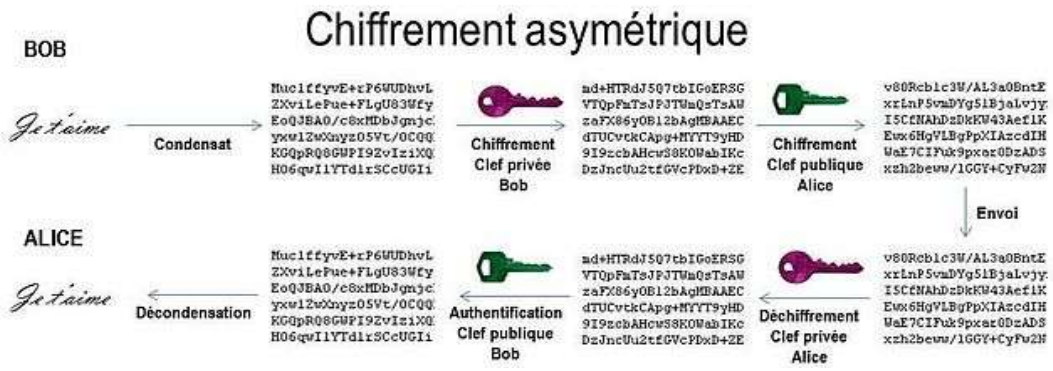



Figure 2.3 : Principe de cryptage asymétrique. [1]

On peut citer le RSA (Rivest, Shamir, Adelman, les 3 inventeurs) comme le plus connu de ces algorithmes.

### 6.2.1 Les avantages

- ❖ l'élimination de la problématique de la transmission de clé.
- ❖ la possibilité d'utiliser la signature électronique.
- ❖ l'impossibilité de décrypter le message dans le cas de son interception par une personne non autorisée.

### 6.2.2 Les inconvénients

- ❖ le temps d'exécution : plus lent que le cryptage symétrique.
- ❖ le danger des attaques par substitution des clés (d'où la nécessité de valider les émetteurs des clés).

## 7. Les différents types de cryptographie

Les systèmes de cryptage peuvent être divisés en deux groupe :

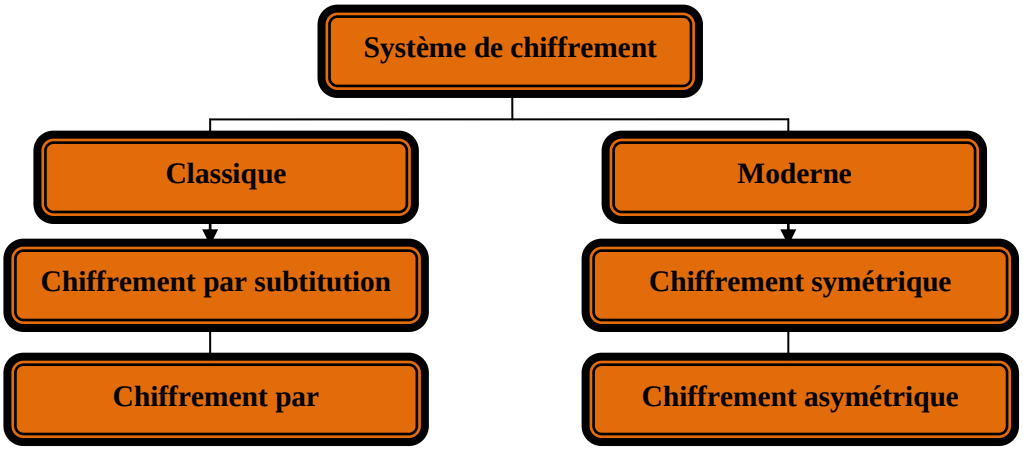



Figure 2.4: principe des systèmes de cryptage.

### 7.1 La cryptographie classique

Dans le schéma ci-dessous toutes les branches de la cryptographie classique ont été résumées :

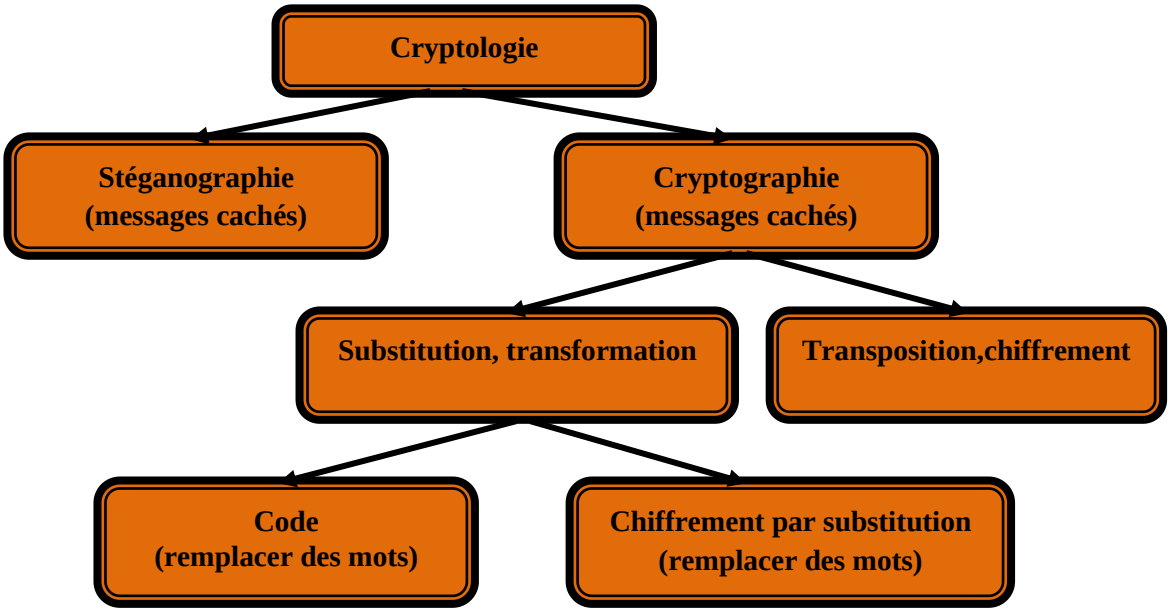



Figure 2.5 : Domaines inclus dans la cryptologie.

### 7.1.1 Chiffrement par substitution

Le chiffrement par substitution consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou plusieurs autres entités. On distingue généralement plusieurs types de cryptosystèmes par substitution :

- **La substitution monoalphabétique**

Consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet. Comme le chiffre de césar est un chiffrement par décalage les lettres de 3 positions.

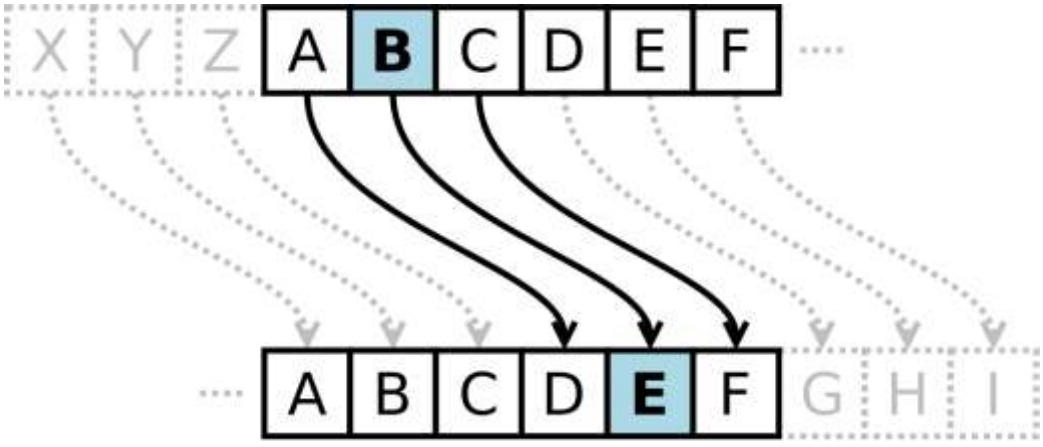



Figure 2.6: chiffre de césar (chiffrement par décalage).[3]

### ❖ Substitutions polyalphabétiques

Consiste à utiliser une suite de chiffres monoalphabétique réutilisée périodiquement. Comme le chiffre de Vigenere Cela signifie qu'il permet de remplacer une lettre par une autre qui n'est pas toujours la même.

| Letter Claire | C | A | C | H | E | S | D | E | R | R | I |
|---|---|---|---|---|---|---|---|---|---|---|---|
| clef | P | E | T | P | E | T | P | E | T | P | E |
| Décalage | 16 | 5 | 20 | 16 | 5 | 20 | 16 | 5 | 20 | 16 | 5 |
| Letter chiffré | R | E | V | W | I | L | S | I | K | G | M |

Figure 2.7 : chiffre de Vigenere.

### ❖ La substitution homophonique

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

### ❖ La substitution de polygrammes

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

## 7.1.2 Chiffrement par Transpositions

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

Comme la méthode de scytale, Pour déchiffrer le texte chiffré, il suffisait d'utiliser un bâton possédant exactement le même diamètre que le précédent, d'y enrouler la lanière de cuir et le texte en clair pouvait alors être relu. [c]

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

Figure 2.8 : Scytale.[4]

## 7.2 La cryptographie Moderne

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

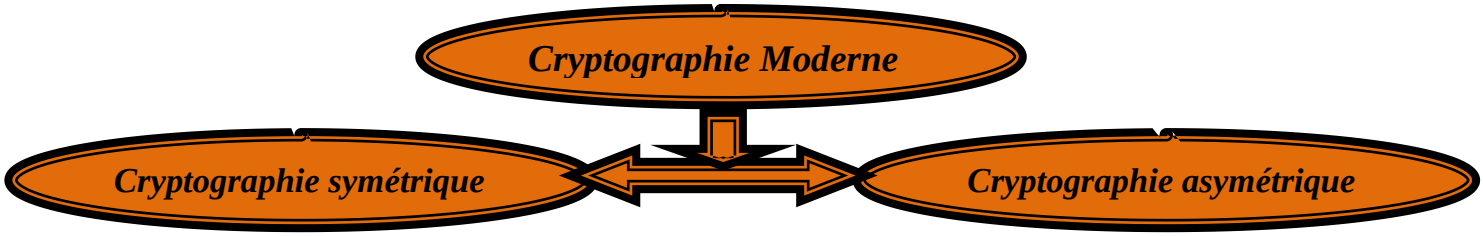



Figure 2.9 : Principe de la cryptographie moderne.

### 7.2.1 Cryptographie symétrique( à clefs privés)

Les algorithmes de chiffrement symétrique se fondent sur une même clé pour chiffrer et déchiffrer un message. **L'un des problèmes de cette technique est que la clé, qui doit rester totalement confidentielle, doit être transmise au correspondant de façon sûre.** La mise en œuvre peut s'avérer difficile, surtout avec un grand nombre de correspondants car il faut autant de clés que de correspondants. [h]

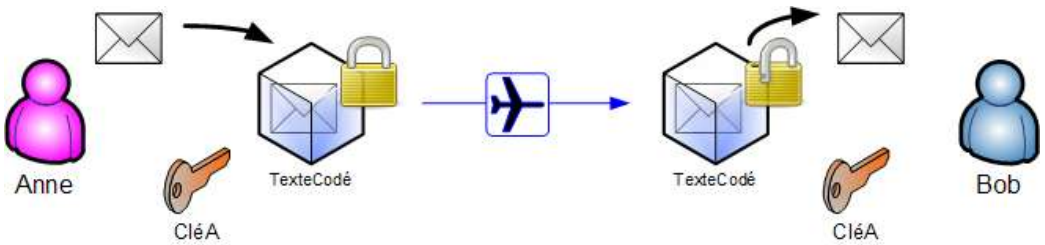



Figure 2.10 : Cryptographie symétrique.[5]

Quelques algorithmes de chiffrement symétrique très utilisés :

- Chiffre de Vernam (le seul offrant une sécurité théorique absolue, à condition que la clé ait au moins la même longueur que le message, qu'elle ne soit utilisée qu'une seule fois à chiffrer et qu'elle soit totalement aléatoire)
- DES(Norme de chiffrement des données)
- 3DES(Triple DES est enchaînant 3 applications successives de l'algorithme DES sur le même bloc de données de 64 bits, avec 2 ou 3 clés DES différentes)
- AES (Norme de chiffrement avancée)
- RC4(Rivest Cipher 4)
- RC5(Rivest's Cipher 5 est fonctionnant grâce à une clé, dont la longueur varie de 40 à 2 040 bits)
- MISTY1(Mitsubishi Improved Security Technology)

On distingue deux catégories de chiffrement symétrique :

- **Le chiffrement par bloc** (en anglais block cipher) est une des deux grandes catégories de chiffrements modernes en cryptographie symétrique, l'autre étant le chiffrement par flot. La principale différence vient du découpage des données en blocs de taille généralement fixe. La taille de bloc est comprise entre 32 et 512 bits, dans le milieu des années 1990 le standard était de 64 bits mais depuis 2000 et le concours AES le standard est de 128 bits.

- **Le chiffrement de flux ou chiffrement par flot** (en anglais stream cipher). Un chiffrement par flot arrive à traiter les données de longueur quelconque et n'a pas besoin de les découper. Un chiffrement par flot se présente souvent sous la forme d'un générateur de nombres pseudo-aléatoires avec lequel on opère un XOR entre un bit à la sortie du générateur et un bit provenant des données.

### 7.2.2 Cryptographie asymétrique (à clefs publiques)

Les problèmes de distribution des clés sont résolus par la cryptographie de clé publique. Ce concept a été introduit par Whitfield Diffie et Martin Hellman en 1975. (Il est maintenant prouvé que les services secrets britanniques avaient fait cette même découverte plusieurs années avant Diffie et Hellman et avaient protégé ce secret militaire (sans en faire aucune utilisation). [c]

La cryptographie de clé publique est un procédé asymétrique utilisant une paire de clés pour le cryptage : une clé publique qui crypte des données et une clé privée ou secrète correspondante pour le décryptage. Vous pouvez ainsi publier votre clé publique tout en conservant votre clé privée secrète. Tout utilisateur possédant une copie de votre clé publique peut ensuite crypter des informations que vous êtes le seul à pourvoir lire. Même les personnes que vous ne connaissez pas personnellement peuvent utiliser votre clé publique.

D'un point de vue informatique, il est impossible de deviner la clé privée à partir de la clé publique. Tout utilisateur possédant une clé publique peut crypter des informations, mais est dans l'impossibilité de les décrypter. Seule la personne disposant de la clé privée correspondante peut les décrypter.

La cryptographie asymétrique se base sur des problèmes mathématiques complexes (factorisation de grands nombres entiers ou équation de logarithme discrète).

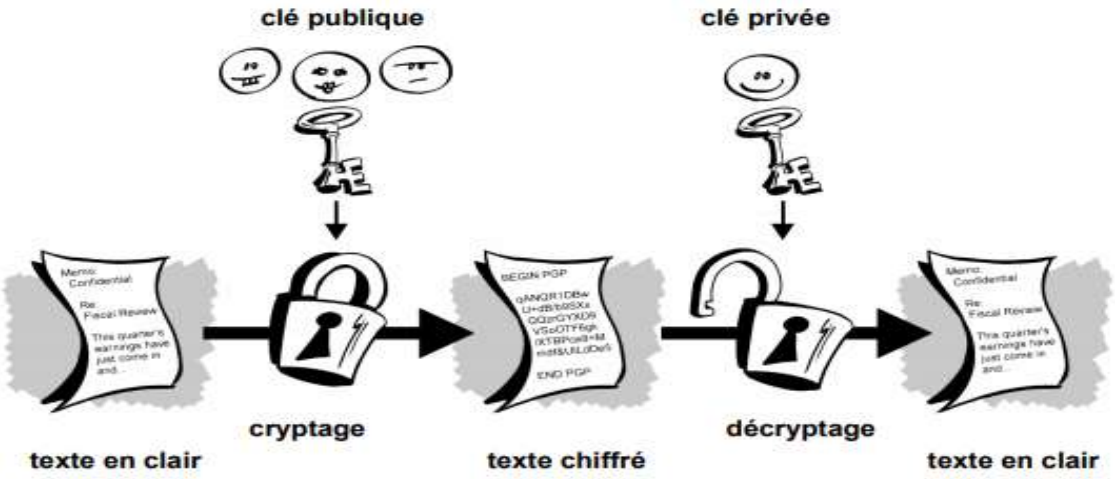



Figure 2.11 Cryptographie asymétrique.[6]

## 8. L'ADN

L'information est très importante et riche dans le temps présent où il est devenu inspirant les scientifiques où il est devenu dans le besoin de protection et afin de protéger ces informations de nombreux chercheurs ont utilisé l'écriture secrète ancienne et présente et les techniques les plus importantes qui sont utilisés et se propagent est le cryptage et la

stéganographie où ces dernières manipule l'information et les induire en erreur et de les cacher afin de les protéger et de cacher son existence.

Le cryptage de l'ADN est l'un des nouveaux domaines de la science aveugle qui a émergé avec le début de l'informatique de l'ADN et lorsque le chiffrement de l'ADN est utilisé par des méthodes biologiques, les bandes d'ADN sont utilisées comme porteurs d'informations modernes et de techniques biologiques comme outils de mise en œuvre. La recherche sur l'utilisation de l'ADN est devenue à l'avant-garde de la recherche mondiale dans la science de la cécité dans divers domaines, comme son utilisation dans le domaine de la dissimulation de l'information (stéganographie), Chiffrement des données texte et image, gestion et génération de clés. Ces méthodes sont basées sur des problèmes et des processus biologiques. L'ordinateur ADN n'est pas similaire à l'ordinateur ordinaire en termes de capacités informatiques, car il possède des capacités et des capacités qu'il ne possède pas.

## 8.1 Que signifie ADN ?

L'acide désoxyribonucléique ou ADN **est** une macromolécule biologique présente dans toutes les cellules ainsi que chez de nombreux virus. L'ADN contient toute l'information génétique, appelée génome, permettant le développement, le fonctionnement et la reproduction des êtres vivants. [i]

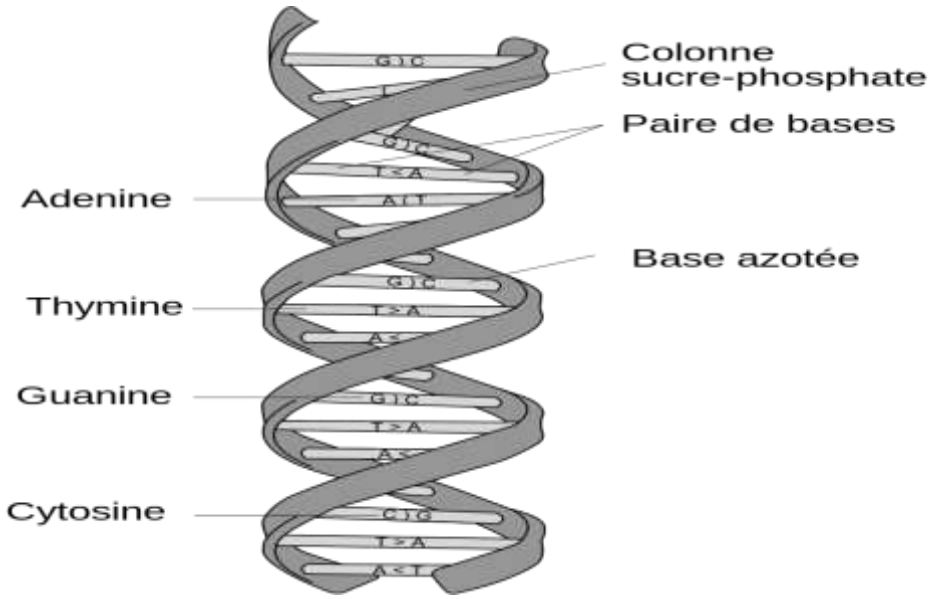



Figure 2.12 : L'ADN.[7]

## 8.2 Structure et principe

La molécule ADN est constituée d'un grand nombre de nucléotides (environ 3,3 milliards de paires de nucléotides) qui vont permettre la création d'acides aminés, composants des protéines. On compte 4 sortes de nucléotides (appelés aussi bases) symbolisés par les lettres A, C, G et T respectivement nommés Adénine, Cytosine, Guanine et Thymine. Un nucléotide est une structure chimique composée d'une base azotée, d'un phosphate et d'un sucre. [j]

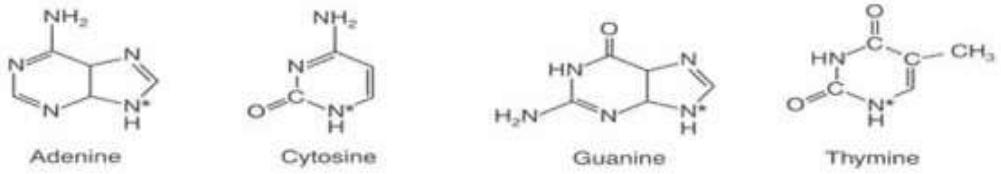



Figure 2.13 Les 4 nucléotides composant l'hélice d'ADN.[8]

Ces quatre nucléotides suffisent pour coder la fabrication de 20 acides aminés présents dans notre corps. Des chaines de 100 à 1000 acides aminés vont constituer les protéines qui sont les "hommes à tout faire" de notre corps. Les protéines vont en effet permettre le bon fonctionnement de nos organes, de nos yeux, nos muscles et de toutes les fonctions vitales de notre organisme. Les milliers de protéines présentes dans notre corps gèrent toute notre activité biologique en passant par la création de molécules ou par la transmission d'informations. Les protéines qui ont une activité de catalyseur sont appelées des enzymes. Ainsi la protéine qui permet de copier une molécule ADN en deux molécules ADN identiques est une enzyme appelée ADN polymérase.

## 8.3 Définition de quelles que notions

### 8.3.1 Chromosome

Un chromosome est une structure cellulaire microscopique représentant le support physique des gènes et de l'information génétique, toujours constituée d'ADN, et souvent de protéines. Les chromosomes existent dans les cellules de tous les êtres vivants, en nombre variable, spécifique à chaque espèce.

### 8.3.2 le rôle

Les chromosomes sont constitués d'ADN, qui est la molécule qui contient le code génétique, c'est à dire le code qui permettra la synthèse de toutes les protéines de notre organisme. Une cellule normale humaine contient 23 paires de chromosomes: 22 paires d'autosomes numérotés de 1 à 22 et une paire de chromosomes sexuels, XX si on est une fille, XY si on est un garçon. Une anomalie chromosomique est une anomalie soit du nombre de chromosomes (la trisomie 21 est la plus connue de ces anomalies) soit une anomalie de structure de ces chromosomes (chromosomes cassés, chromosomes réarrangés entre eux).

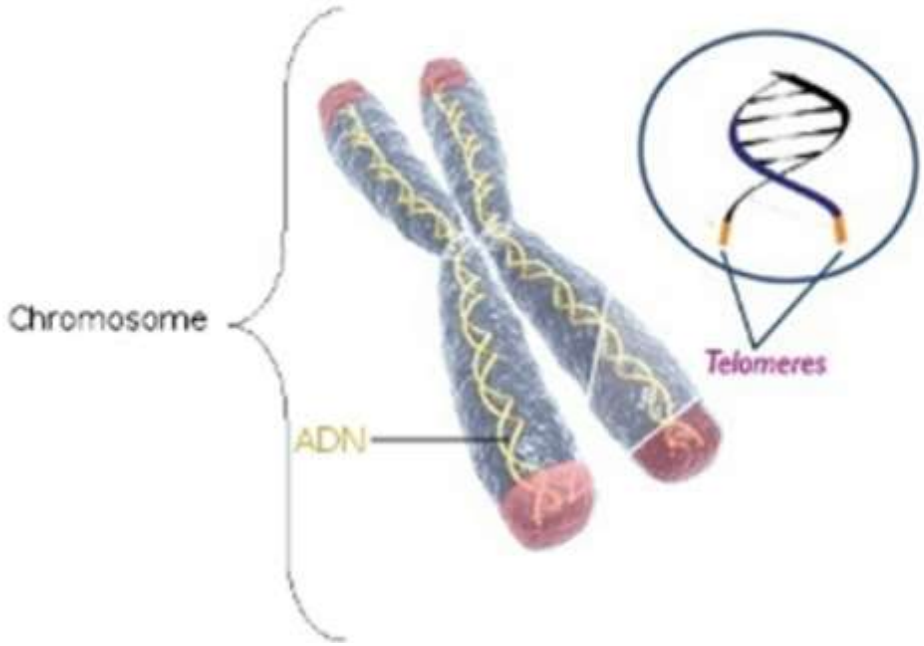



Figure 2.14 Structure d‘un chromosome.

### 8.3.3 Le nucléotide

Un nucléotide est une molécule organique qui est l'élément de base d'un acide nucléique tel que l'ADN ou l'ARN. Il est composé d'une base nucléique (ou base azotée), d'un ose à cinq atomes de carbone, dit pentose, dont l'association forme un nucléoside, et enfin de un à trois groupes phosphate. [k]

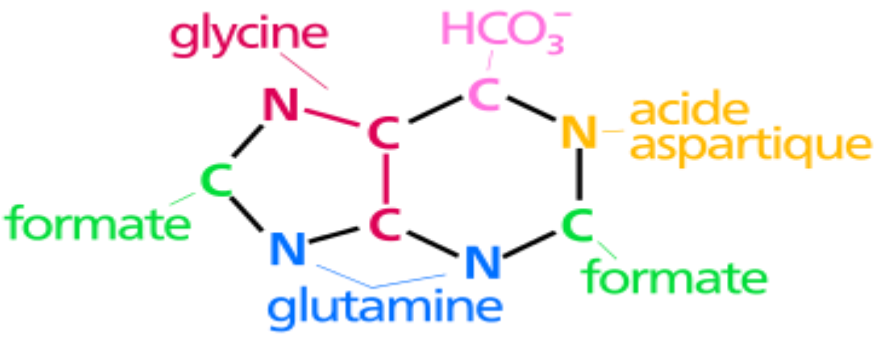



Figure 2.15 : Structure de Nucléotide.

### 8.3.4 Le nucléoside

Un nucléoside identifie un composé formé d'une base, une base azotée, et d'un pentose: le ribose (ribonucléoside) ou le désoxyribose (désoxyribonucléoside). Dans une cellule, différents nucléosides apparaissent, qui diffèrent par la teneur en nucléobase ou en pentose (sucre). Contrairement aux nucléotides qui constituent les acides nucléiques (ADN ou ARN), ils ne contiennent pas de radicaux phosphate.[l]

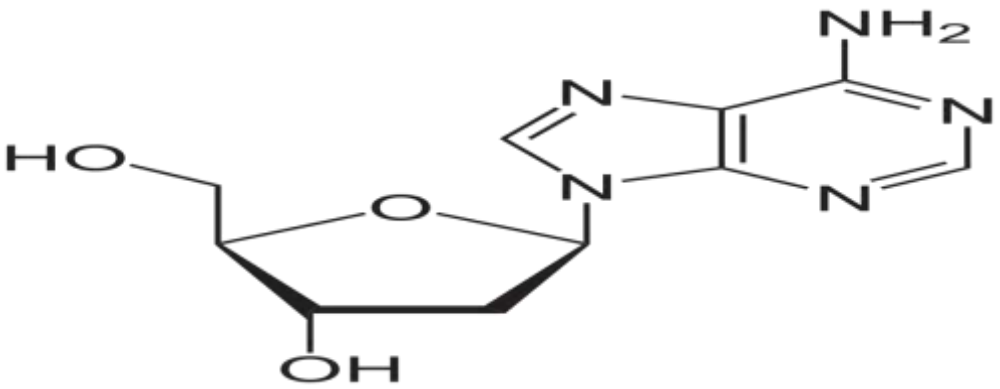



Figure 2.16 Structure de nucléoside.

## 9. Travaux connexes [m]

### 9.1 Carte chaotique linéaire piecewise et carte logistique

Dans cet algorithme proposé, nous utilisons Carte chaotique linéaire piecewise (PWLCM) et carte logistique pour générer tous les paramètres dont l'algorithme nécessite. PWLCM a beaucoup de bons caractères pour nous aider à construire l'image clé tandis que la

carte logistique prend quelques travaux auxiliaires tels que le choix de type particulier d'opérations ou de règles d'ADN.

PWLCM décrite par l'équation suivante :

$$x_{n+1} = F_p(x_n) = \begin{cases} \frac{x_n}{p}, 0 < x_n < p \\ \frac{(x_n - p)}{0.5 - p}, p \leq x_n \\ F_p(1 - x_n), 0.5 \leq x_n < 1 \end{cases} \quad (1)$$

$x_n \in (0,1)$ et p le paramètre de contrôle est tel que : p∈(0,0.5) , dans notre expérience, appliquer p=0. 25678900.

Carte logistique décrite par l'équation suivante :

$$x_{n+1} = \mu x_n (1 - x_n) \quad (2)$$

$x_n \in (0,1)$ et μ∈(0,4] ,À partir du diagramme de bifurcation de la carte logistique, nous pouvons comprendre que lorsque $\mu \in (3.9,4]$, la séquence pseudo aléatoire est en 0 et 1 . Dans l'algorithme proposé, nous attribuons μ = 3.99999999.

## 9.2 Séquence d'acide de désoxyribonucléique

L'acide désoxyribonucléique est une sorte de molécules qui sont composées de quatre types de nucléotides, L'adénine (A), thymine (T), cytosine (C) et Guanine (G) et d'autres éléments essentiels sont des composants principaux des nucléotides. Selon les règles de l'ADN, A et T, C et G sont des paires complémentaires. Il y a 8 combinaisons juridiques selon les règles complémentaires de l'ADN. Ce genre de règles complémentaires ont quelque chose en commun avec le système binaire . Par exemple, '0' et '1' sont complémentaires ainsi que '00' et '11', '01' et '10' dans le système binaire. Parce que chaque pixel de l'image à l'échelle grise a 8 bits, pour la simplicité, nous appliquons '00', '01', '10' et '11' comme métadonnées. Nous pouvons utiliser 4 types de nucléobases en vertu de 8 règles pour encoder l'image simple. Par exemple, un pixel est 201 en décimale, sa valeur binaire correspondante est '11001001'. Encodez-le par des règles ADN, nous pouvons obtenir 8 types de combinaisons : 'TACG', 'TAGC', 'ATCG', 'ATGC', 'CGTA', 'CGAT', 'GCTA' et 'GCAT'. En outre, utilisez différentes opérations de séquence d'ADN pour chiffrer l'image. Les règles et les opérations de correspondance d'ADN sont énumérées dans les tableaux suivants, tableau 2.1 au tableau 3.2 :

| Règle | Règle1 | Règle2 | Règle3 | Règle4 | Règle5 | Règle6 | Règle7 | Règle8 |
|---|---|---|---|---|---|---|---|---|
| 00 | A | A | T | T | C | C | G | G |
| 01 | C | G | C | G | A | T | A | T |
| 10 | G | C | G | C | T | A | T | A |
| 11 | T | T | A | A | G | G | C | C |

Tableau 2. 1 Règles d'encodage et de décodage.

| XOR | A | C | T | G |
|---|---|---|---|---|
| A | A | C | T | G |
| T | T | G | A | C |
| C | C | A | T | T |
| G | G | T | C | A |

Tableau 2. 2 Opération exclusive OR (XOR).

## 9.3 Message Digest Algorithme 5 :

Message Digest Algorithme 5 (MD5) est une fonction de hachage cryptographique largement utilisée, qui génère 128 bits de valeur de hachage généralement présenté comme un nombre hexadécimal à 32 chiffres littéralement. en raison de sa bonne caractéristique de la sécurité, même un changement d'un bit peut conduire à une différence significative entre deux images. Les valeurs initiales des cartes de chaos sont générées par la valeur de hachage MD5.

Message Digest Algorithme 5 décrite par l'équation suivante :

$$x_0 = \mathrm{mod}(d_1 \oplus d_2 \oplus d_3 \oplus d_4, 256)/255 \qquad (3)$$

où $x_o$ est la valeur initiale de la carte du chaos, la valeur de $x_o$ peut être de 0 ou 1 avec une certaine possibilité, si cela s'est produit, sauter cette valeur, utiliser équation (1.1) pour en obtenir un autre.

$d_1,d_2,d_3,d_4$ sont extraits de la valeur de hachage MD5 de l'image ordinaire. La valeur de hachage MD5 de l'image ordinaire se compose de 128 bits, nous utilisons les 32 premiers bits pour générer $d_1,d_2,d_3,d_4$ chacun d'entre eux est un seul byte .

## 10. Conclusion :

Dans ce chapitre, nous avons présenté des généralités sur la cryptographie et les méthodes, algorithmes de cryptage proposé.

Nous avons commencé par des vocabulaires de base, l'usage de la cryptographie et mécanisme de la cryptographie et développement des clés en cryptographie. Puis nous avons cité les différents types de cryptage. Enfin, nous avons présenté les Travaux connexes.

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

Dans le chapitre suivant, nous allons présenter l'algorithme de cryptage d'image proposé en utilisant un modèle basé sur la complexité de la structure de L'ADN.

# 1. Introduction

Avec le développement rapide de la technologie et de l'industrie, un nombre croissant de nouveaux appareils intelligents sortent. Les images numériques prises d'eux ont une haute résolution et occupent un plus grand espace de stockage. En raison de la capacité de données encombrante, de la redondance élevée et des corrélations fortes entre les pixels adjacents, les algorithmes typiques de cryptage d'images tels que Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA) ne sont pas compétents pour chiffrer ces images numériques La dépendance sensible aux conditions initiales, la pseudo-randomité, l'ergodicité et la reproduction sont les principales caractéristiques du système de chaos, qui répond aux exigences du cryptage. De nombreux algorithmes de cryptage d'image basés sur le chaos ont été mis en avant ces dernières années.

Les algorithmes de cryptage d'image basés sur l'encodage de l'ADN et le Chaos émergent mais matures des algorithmes normaux de cryptage d'image basés sur le chaos se composent de deux étapes, le mélange et la diffusion, qui sont exécutés à tour de rôle ou simultanément. Alors que les algorithmes utilisant la technologie d'encodage de l'ADN sont également composés de deux étapes, la phase de codage et la phase de décodage. Dans la première phase, les images simples sont codées par les règles de l'ADN, en attendant, une image clé a été générée et codée. Ensuite, certaines opérations d'ADN sont effectuées sur l'image clé codée et l'image simple codée. Enfin, en décodant l'image intermédiaire, nous pouvons obtenir l'image de chiffrement. Sur l'ensemble du processus, toutes les œuvres sur le hasard sont terminées par le chaos. Les algorithmes de cryptage basés sur les images de processus de chaos dans un degré mathématique, tandis que les algorithmes utilisant la technologie de codage d'ADN sont dans un degré biologique.

Enayatifar et al ont proposé un algorithme de cryptage d'image basé sur la séquence GA et ADN. Dans cette recherche, des règles de map logistique et d'encodage de l'ADN sont adoptées pour créer des masques d'ADN initiaux, l'algorithme choisit le meilleur masque pour le cryptage par algorithme GA. Liu et al ont proposé un algorithme basé sur le Chaos et l'ADN règle complémentaire. Dans la recherche, chaque pixel est codé et transformé en paire de base après avoir été permuté les lignes et les colonnes respectivement par les tableaux générés par la carte chaotique linéaire. Wang et al ont mettre en place avec un nouveau système de cryptage d'image basé sur des séquences d'ADN et une carte chaotique. Dans

cette recherche, une sorte de système de chaos spatio-temporelle, tel que le treillis de carte couplé est appliqué pour confondre l'image simple. Après avoir codé l'image confuse, permutez ses lignes et ses colonnes pour obtenir l'image de chiffrement codée. Huang et al ont a proposé un nouvel algorithme de cryptage d'image faisant l'utilisation de l'hyper-chaos et de la séquence d'ADN. Dans cette recherche, la séquence pseudo-aléatoire, obtenue par un système bidimensionnel hyper-chaos, est transformée en séquence d'ADN pour diffuser l'image ordinaire. Après plusieurs séries de permutation, le chiffrement peut être obtenu.

Dans l'algorithme proposé, des règles ou des opérations spécifiques d'ADN sont décidées au hasard par le chaos, ce qui est assez stochastique. Tout d'abord, utilisez PWLCM pour générer l'image clé; Deuxièmement, codez l'image simple et l'image clé respectivement par des rangées avec des règles d'ADN qui sont sélectionnées parmi huit types ; Après cela, traiter deux images codées ligne par ligne pour gagner l'image intermédiaire. L'opération particulière est décidée par carte logistique ; Ensuite, décoder l'image intermédiaire comme l'image simple de l'étape suivante; Enfin, suivez à nouveau les étapes ci-dessus par des colonnes pour obtenir l'image de chiffrement ultime.

## 2. Algorithmes de cryptage et de décryptage :[m] [n]

### 2.1 Algorithme de cryptage

Flux de l'algorithme de cryptage est présenté dans Figure 3.1, les détails comme suite :

**Étape 1** : Utilisez Equation (1) et Equation (4) pour générer l'image clé.

$$\mathbf{Pixel=[x\times 256]} \qquad \mathbf{(4)}$$

le pixel est la valeur pixel de l'image clé. x(0,1), c'est-à-dire la valeur d'itération de PWLCM. Itérer Equation (1) et Equation (4) pour obtenir une image clé. La valeur initiale de l'Equation (1) est calculée par Equation (3). Les pixels adjacents de l'image clé sont censés être faiblement corrélés les uns avec les autres. Pour répondre à cette exigence, les pixels obtenus par carte du chaos sont un bon choix. La valeur du pixel suivant généré n'a rien à voir avec l'actuel.

| + | A | T | C | G |
|---|---|---|---|---|
| A | C | A | G | T |
| T | G | T | C | A |
| C | A | C | T | G |
| G | T | G | A | C |

Tableau 3.1 Opération d'addition.

| - | A | C | T | G |
|---|---|---|---|---|
| A | C | G | A | T |
| T | G | T | C | A |
| C | A | T | C | G |
| G | T | A | G | C |

Tableau 3.2 Opération de soustraction.

**Étape 2** : Encoder l'image simple et l'image clé respectivement par des rangées avec des règles d'ADN qui sont décidées par Equation ( 2) et Equation (5).

$$\textbf{Règle} = [x \times 8] + 1 \qquad \textbf{(5)}$$

La règle est la règle spécifique, qui domine le progrès de codage. La valeur initiale de l' Equation (2) est fournie par Equation (3). Les détails sur les règles d'ADN sont indiqués dans le tableau 2.1. Chaque pixel d'une ligne est codé par la règle d'ADN spécifiée, différentes lignes ont des règles différentes, jusqu'à ce que tous les pixels d'image soient codés. Chaque pixel d'image ordinaire à l'échelle grise se compose de 8 bits, selon les règles d'encodage de l'ADN, ces 8 bits peuvent être divisés et codés en 4 sortes de nucléobases. Supposons que la taille de l'image ordinaire originale est M×N, M est la largeur, N est hauteur. Après avoir encodé ligne par ligne, une image de taille 4×M×N est formée.

**Étape 3** : Effectuer des opérations d'ADN entre l'image simple codée et l'image clé codée ligne par ligne. Le type spécifié d'opérations d'ADN est déterminé par Equation (2) et Equation (6). Les détails sur les opérations génétiques sont présentés au tableau2.2 tableau 3.2.

$$\textbf{Opération} = [x \times 3] + 1 \qquad \textbf{(6)}$$

l'opération est le type choisi d'opération d'ADN. Effectuer l'opération vérifiée ligne par ligne jusqu'à ce que l'image intermédiaire codée est générée, pendant ce temps, trois types

d'opérations d'ADN (XOR, +, -) sont effectuées alternativement. La taille de l'image intermédiaire codée est de 4×M×N.

**Étape 4** : Décoder l'image intermédiaire codée pour obtenir une image intermédiaire décodée. La règle de décodage est selon Equation (5). Grâce à cette étape, nous pouvons obtenir un chiffre primaire image. Le décodage et l'encodage aléatoires améliorent les performances de diffusion de l'algorithme proposé. L'image principale de chiffrement est avec la taille M×N.

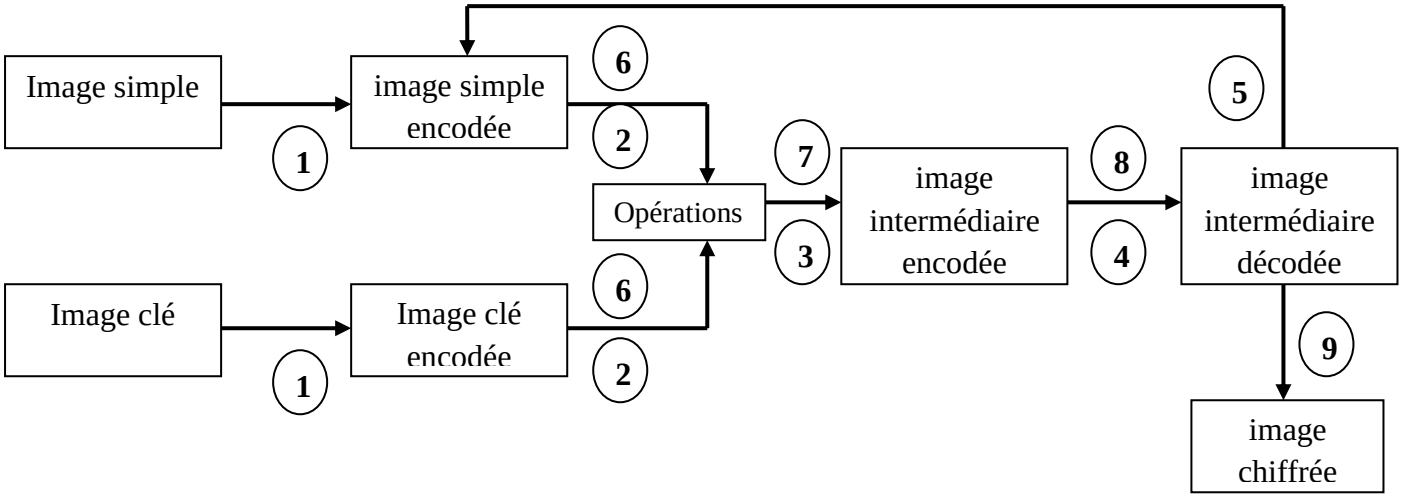



Figure 3.1 Diagramme de bloc de l'algorithme de cryptage.

**Étape 5** : Faites pivoter l'image de chiffrement primaire de 90 degrés dans le sens des aiguilles d'une montre pour obtenir une nouvelle image ordinaire utilisée à l'étape suivante. Grâce à cette opération, nous simplifions l'algorithme proposé pour gérer les images par lignes d'abord, puis par colonnes.

**Étape 6** : Faire étape 1 à l'étape 4 à nouveau pour obtenir l'image de chiffre final.

## 2.2 Algorithme de décryptage

L'algorithme de décryptage est le processus inverse de l'algorithme de cryptage. Mais plusieurs détails sont censés être concentrés en particulier comment inverser le fonctionnement de l'ADN de la soustraction. Avant que les récepteurs ne décodent les images de chiffrement, ils auraient déjà dû posséder les clés utilisées pour chiffrer les images simples, qui sont transmises plus tôt que les images de chiffrement. Ensuite, nous pouvons décoder les images de chiffrement en suivant les étapes suivantes :

**Étape 1** : Encoder l'image de chiffrement selon le processus inverse exact qui se réfère aux règles décrites dans l'étape 4 de la section '' Algorithme de cryptage''.

**Étape 2** : Générer l'image clé et coder l'image clé. Les détails se réfèrent à l'étape 1 à l'étape 2 de l'algorithme de cryptage.

**Étape 3** : Utilisez l'image clé codée et l'image de chiffrement codée pour générer l'image codée intermédiaire. L'opération spécifique est décrite dans l'étape 3 de l'algorithme de cryptage. Nous devrions accorder plus d'attention ici, il y a trois types d'opérations, ADN XOR, ADN Addition, soustraction de l'ADN. Du tableau 2.2 au tableau 3.2, les matrices de ces opérations sont symétriques, à l'exception de la soustraction de l'ADN. C'est-à-dire que les opérations de l'ADN XOR et de l'ajout d'ADN peuvent être utilisées intactement dans l'algorithme de décryptage, mais le fonctionnement de la soustraction de l'ADN devrait être affiné pour répondre aux règles de l'ADN. C'est le point clé de l'algorithme de décryptage. Par exemple, selon les règles du tableau 3.2, A-A=C, A-C=G, A-T=A, A-G=T. Lors du processus inverse, C-A=A, G-C=A, A-T=A, T-G=A, mais A-C=G, C-G=G, T-A=G, G-T=G, qui est causée par l'asymétrie de la soustraction d'opération. Ainsi, lors de la conception de l'algorithme de décryptage, plus de détails sur la soustraction de fonctionnement devraient être concentrés.

**Étape 4** : Décoder l'image codée intermédiaire générée à partir de l'étape 3 pour obtenir une image décodée.

**Étape 5** : Tournez l'image décodée de l'étape 4 par 90º dans le sens des aiguilles d'une montre. Jusqu'à présent, nous avons atteint l'image de chiffrement de l'image ordinaire qui est cryptée un tour par rangées.

**Étape 6** : Faire étape 1 à l'étape 4 à nouveau pour obtenir l'image simple.

Les résultats du cryptage et du décryptage sont présentés dans Figure 3.2.

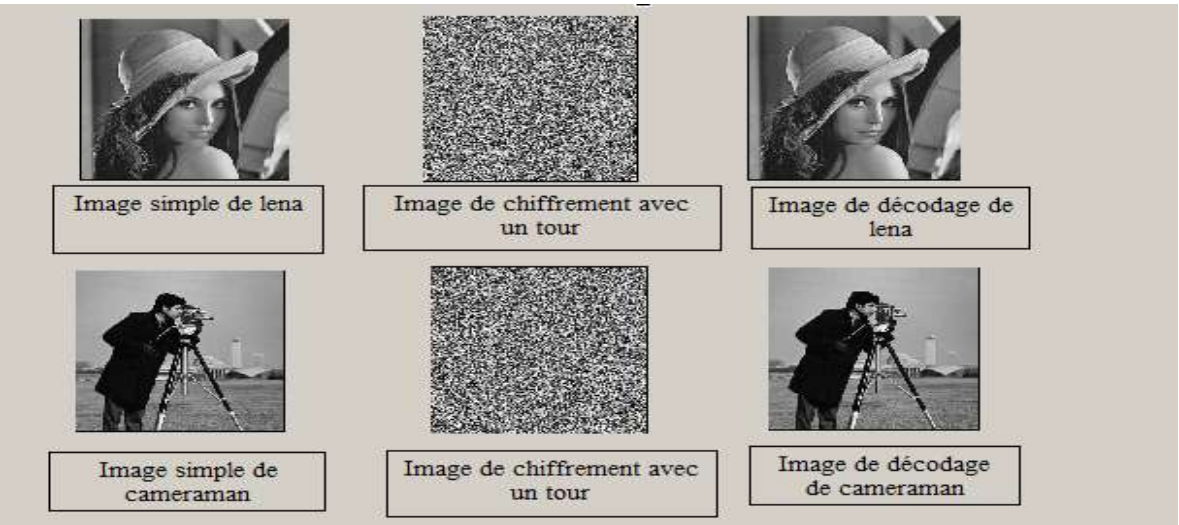



Figure 3.2 Résultats du cryptage et du décryptage.

## 3. Analyse de sécurité et analyse de la complexité du temps :[m][n]

### 3.1 Analyse statistique

L'analyse des histogrammes et de l'analyse de corrélation de deux pixels adjacents sur les images de chiffrement peut nous aider à mesurer les performances de l'algorithme proposé contre les attaques statistiques. En théorie, un bon algorithme de cryptage d'image devrait être capable de résister à toutes sortes d'attaques statistiques.

Histogramme reflète le nombre de pixels sur ses niveaux gris. Plus l'histogramme d'images de chiffrement est plat, mieux l'algorithme proposé fonctionne. Les histogrammes de Lena et ses images de chiffrement correspondantes sont montrés dans Figure 3.3.

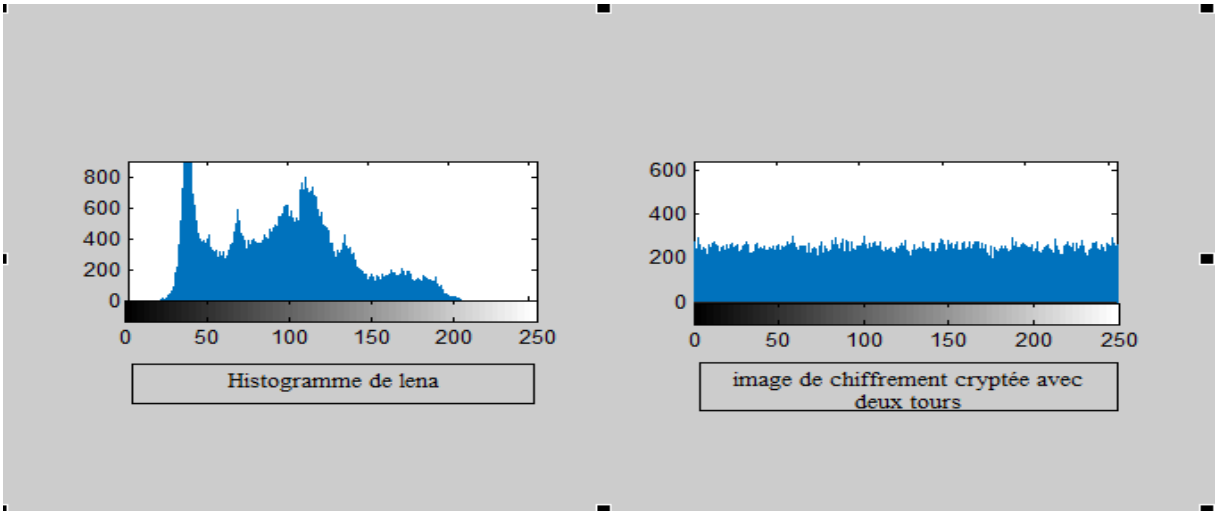



Figure 3.3 Histogrammes d'images simples et de chiffrement.

Dans les images simples, deux pixels adjacents sont fortement corrélatifs. Un bon algorithme de cryptage d'image devrait rompre ce type de relation entre les pixels.1000 paires de pixels adjacents sont choisis au hasard dans l'image ordinaire de Lena et son image chiffrée cryptée avec un tour dans le sens horizontal, vertical et diagonal, pour avoir une analyse plus approfondie sur leurs corrélations, les détails sont présentés sur la Figure 3.4.

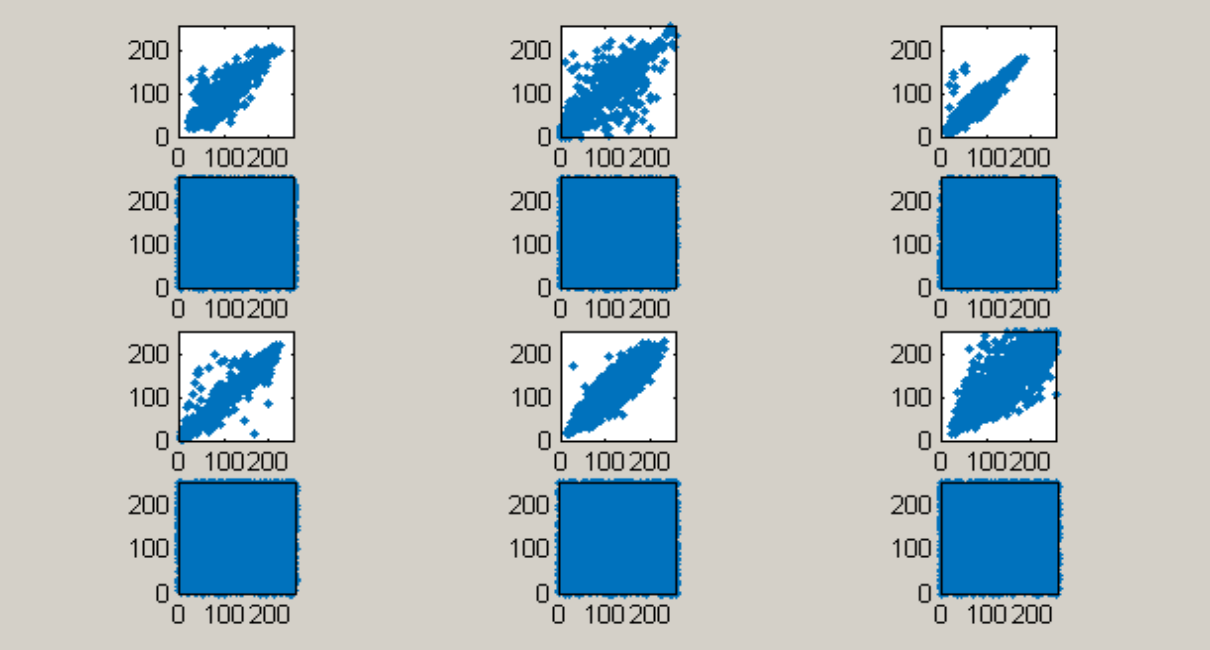



Figure 3.4 Corrélations de deux pixels adjacents.

Les coefficients de corrélation $r_{x,y}$ sont calculés pour quantifier les corrélations entre pixels en utilisant Equation (7) et Equation (8).

Covariance: $$cov(x,y) = E\{(x - E(x))(y - E(y))\} \quad (7)$$

Corrélation : $$r_{x,y} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (8)$$

où x et y sont des valeurs de deux pixels adjacents dans l'image ordinaire ou l'image chiffrée,

Espérance mathématique : $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \, , D(x) = \frac{1}{N}\sum_{i=1}^{N} x_i - E(x))^2$ (9)

Les tests sont effectués 10 fois, les détails sont comme le tableau 3.3.

| Image | Image simple | | | Image de chiffrement | | |
|---|---|---|---|---|---|---|
| | Horizontale | Diagonale | Verticale | Horizontale | Diagonale | Verticale |
| Bird | 0.9756 | 0.9749 | 0.9921 | −0.0061 | 0.0042 | 0.0089 |
| Boat | 0.9282 | 0.8824 | 0.9319 | 0.0043 | 0.0077 | −0.0064 |
| Brain | 0.9573 | 0.9369 | 0.9685 | −0.0266 | −0.0046 | 0.0091 |
| Finger | 0.9201 | 0.8362 | 0.9464 | −0.0017 | −0.0041 | −0.0082 |
| House | 0.9835 | 0.9352 | 0.9722 | 0.0024 | 0.0092 | 0.0011 |
| Lena | 0.9260 | 0.9172 | 0.9698 | −0.0033 | −0.0072 | 0.0079 |
| Moon | 0.9080 | 0.8873 | 0.9321 | 0.0064 | 0.0074 | −0.0112 |
| Peppers | 0.9471 | 0.9254 | 0.9609 | 0.0171 | 0.0072 | −0.0019 |
| Plane | 0.9098 | 0.9098 | 0.9243 | −0.0085 | −0.0082 | −0.0096 |

Tableau 3.3 Coefficients de corrélation de deux pixels adjacents dans l'image ordinaire et l'image chiffrée.

## 3.2 Test du $x^2$

Nous pouvons utiliser Test du $x^2$ pour analyser plus en détail la distribution des valeurs de pixels des images chiffrées. La valeur de Test du $x^2$ peut être calculée par Equation (10).

$$x^2 = \sum_{i=1}^{255} \frac{(v_i - v_o)}{v_o} \qquad (10)$$

Où $v_i$ est la fréquence observée d'une valeur de pixel i ($0 \leq i \leq 255$) et $v_o$ est la fréquence attendue d'une valeur de pixel i, tableau 3.4. Du tableau 3.4, nous pouvons déduire que la distribution des pixels est uniforme dans les images chiffrées, ce qui signifie que le schéma proposé est capable de résister à certaines attaques statistiques.

| Image de test | Test du $x^2$ | |
|---|---|---|
| | Image simple | Image de chiffrement |
| Bird | 131009.42 | 254.36 |
| Boat | 98745.42 | 304.42 |
| Brain | 5183442.38 | 226.61 |
| Finger | 93005.64 | 264.54 |

| | | |
|---|---|---|
| House | 368979.38 | 225.45 |
| Lena | 47828.65 | 231.57 |
| Moon | 135537.51 | 232.60 |
| Peppers | 34677.46 | 235.01 |

Tableau 3.4 Résultats de Test du $x^2$ sur des images de test standard.

## 3.3 Analyse de l'espace clé

### 3.3.1 Espace clé

Un algorithme de chiffrement d'image éligible doit être sensible à ses clés et avoir un grand espace de clé de la Figure 3.5, nous pouvons voir que $x_o$,$x_o'$,$x_o''$, μ et p sont des clés secrètes, $x_0$ est la valeur initiale de l'équation (2), μ est le paramètre de l'équation (2). $x_o'$ est la valeur initiale de l'équation (1) et p est le paramètre de l'équation (1). $x_o''$ est la valeur initiale utilisée pour conduire le système de chaos lors de l'encodage des images. L'espace clé de cet algorithme proposé est :

$$10^{16}\times 10^{16}\times 10^{16}\times 10^{16}\times 10^{15}\text{-}10^{79}\approx 2^{263}$$

### 3.3.2 Sensibilité à la clé secrète

Dans cet algorithme proposé, la valeur initiale $x_o$ et le paramètre μ de l'équation (2), la valeur initiale $x_o'$ , et le paramètre p de l'équation (1) et la valeur initiale $x_o''$ utilisée pour activer le chaos lors du codage des images sont des clés secrètes. Selon les résultats expérimentaux sur clé sensibilité, on peut apprendre que $x_o$, $x_o'$, $x_o''$, p a la précision de $10^{-16}$ pour un tour le chiffrement, tandis que μ a la précision de $10^{-15}$. Dans notre expérience, μ = 3,99999999 et p = 0,25678900. Les résultats sont présentés sur la figure 3.5.

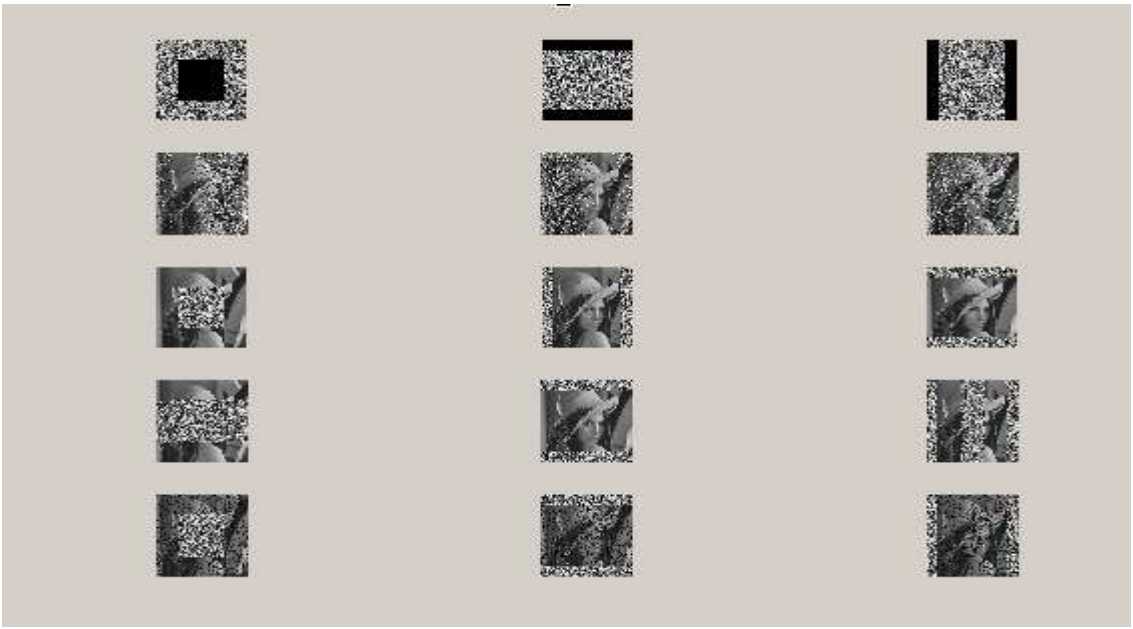


Figure 3.5 Sensibilité des clés secrètes.

## 3.4 Entropie de l'information

L'entropie de l'information est utilisée pour mesurer la complexité d'un système. Les chercheurs utilisent ce concept pour évaluer les performances de l'algorithme de chiffrement. Il peut être calculé par l'équation (11).

$$H(x) = -\sum_{i=1}^{n} p(x_i) log p(x_i) \qquad (11)$$

où x est un ensemble de symboles; n est le nombre total de symboles, $x_i \in x$; p ($x_i$) est la probabilité de $x_i$ dans x. Théoriquement, plus la valeur de H (x) est élevée, meilleur est l'algorithme de chiffrement. Par exemple, nous utilisons 256 images en niveaux de gris pour mener l'expérience. En théorie, l'entropie de l'information de l'image de chiffrement devrait être 8. Le tableau 3.5 montre les résultats de l'évaluation des images chiffrées qui sont chiffrées par l'algorithme proposé. Le tableau 3.5 montre que les entropies d'informations réelles de différentes images de chiffrement sont proches de 8, ce qui indique que nous avons obtenu de bonnes performances de chiffrement. En outre, il est également montré la comparaison entre les images chiffrées et les images simples.

| Nom | Bird | Boat | Brain | Finger | House | Lena | Moon |
|---|---|---|---|---|---|---|---|
| Image de chiffrement | 7.9972 | 7.9976 | 7.9971 | 7.9971 | 7.9975 | 7.9975 | 7.9974 |
| Image simple | 6.7744 | 7.1226 | 4.1514 | 5.1963 | 6.3323 | 7.3785 | 6.7093 |

Tableau 3.5 Entropies d'informations des images en clair et des images chiffrées.

## 3.5 Entropie locale de Shannon

Nous pouvons utiliser l'entropie de Shannon locale pour mesurer le caractère aléatoire des images chiffrées. L'entropie locale de Shannon (k, $T_\beta$) est définie comme suit:

$$\overline{H_{(k,T_\beta)}(S)} = \sum_{i=1}^{k} \frac{H(S_i)}{k} \quad (12)$$

Où $S_1$, $S_2$, $S_3$,…, $S_k$ sont des blocs sans chevauchement avec des pixels TB d'image chiffrée, qui sont sélectionnés au hasard. H ($S_i$) (i = 1,2,3,…, k) sont calculés par l'entropie de Shannon Eq . (dix). Dans le test, nous attribuons k = 30, $T_\beta$ = 1936, ce qui signifie que 30 blocs d'image chiffrée avec 1936 pixels respectivement sont sélectionnés au hasard. nous pouvons penser que l'intervalle (30, 1936) d'entropie locale de Shannon devrait être compris entre [7.901901305, 7.903037329], par rapport à un niveau de confiance α- de 0,05. Le tableau 4.3 présente les résultats de l'entropie locale de Shannon sur les images de test, à partir desquelles nous pouvons voir que le degré de caractère aléatoire des images chiffrées est idéal.

| Test d'images | Entropie locale de Shannon des images de chiffrement | Résultat |
|---|---|---|
| Bird | 7.902826 | SUCCESS |
| Boat | 7.902972 | SUCCESS |
| Brain | 7.902053 | SUCCESS |
| Finger | 7.902153 | SUCCESS |
| House | 7.902812 | SUCCESS |
| Lena | 7.902813 | SUCCESS |
| Moon | 7.902899 | SUCCESS |
| Peppers | 7.902904 | SUCCESS |

Tableau 3.6 Test d'entropie local de Shannon pour les images chiffrées k = 30, TB = 1936, α = 0,05)

## 3.6 Analyse de l'attaque différentielle résistante

Afin de résister aux attaques différentielles, les images chiffrées sont censées être pertinentes pour leurs images simples correspondantes, ce qui signifie qu'un changement minime dans les images simples peut entraîner une altération significative des images chiffrées. Dans l'algorithme proposé, nous utilisons une valeur de somme de contrôle qui est calculée par la valeur de hachage MD5 de l'image simple comme valeur initiale de la carte

logistique et de la carte chaotique de revêtement par morceaux pour générer tous les paramètres dont l'algorithme présenté a besoin. Nous construisons donc la relation entre les images simples et les images chiffrées. Certains tests de référence tels que le taux de changement du nombre de pixels (NPCR) et l'intensité de changement moyenne unifiée (UACI) sont utilisés pour mesurer l'influence d'un petit changement sur l'image chiffrée entière. Désigner l'image ordinaire et son image chiffrée correspondante comme $P_1$ et $C_1$. Ne modifiez qu'un pixel de l'image ordinaire en ajoutant 1 à un pixel sélectionné au hasard. L'image ordinaire modifiée et son image chiffrée sont notées $P_2$ et $C_2$ Une matrice auxiliaire D est créée, où lorsque $C_1$ (i, j) = $C_2$ (i, j), alors D (i, j) = 0; Sinon, D (i, j) = 1. NPCR et UACI sont définis comme:

$$NPCR = \frac{\sum_{(i,j)} D(i,j)}{M \times N} \times 100\% \quad (13)$$

$$UACI = \frac{1}{M \times N}\left(\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right) \times 100\% \quad (14)$$

où M × N est la taille de l'image.

Un pixel est choisi au hasard dans l'image ordinaire et a changé sa valeur par l'ajout1. NPCR fait référence aux nombres de pixels modifiés dans l'image chiffrée qu'un seul pixel est modifié dans l'image ordinaire. UACI indique la valeur moyenne de la différence entre deux images chiffrées. Les valeurs théoriques maximales sont de 99,609375% pour le NPCR et de 33,463541% pour l'UACI. En raison de divers développements de l'environnement, les valeurs réelles peuvent flotter près des valeurs standard. Les résultats sont présentés dans le tableau 4.4, qui sont basés sur la valeur moyenne de l'expérience. Du tableau 4.4, nous pouvons déduire que l'algorithme proposé a de bonnes caractéristiques pour résister aux attaques différentielles.

| Nom | | Bird | Boat | Finger | House | Lena | Moon | Plane |
|---|---|---|---|---|---|---|---|---|
| NPCR | 1 tour | 0.9961 | 0.9958 | 0.9964 | 0.9961 | 0.9960 | 0.9959 | 0.9965 |
| | 2 tour | 0.9962 | 0.9962 | 0.9962 | 0.9962 | 0.9960 | 0.9958 | 0.9959 |
| UACI | 1 tour | 0.3330 | 0.3332 | 0.3362 | 0.3350 | 0.3345 | 0.3332 | 0.3347 |
| | 2 tour | 0.3335 | 0.3360 | 0.3351 | 0.3339 | 0.3338 | 0.3333 | 0.3358 |

Tableau 3.5 NPCR et UACI.

## 3.7 Analyse de la résistance au texte en clair connu et attaques en texte clair choisi

Nous utilisons une carte logistique et une carte chaotique linéaire par morceaux pour générer tous les paramètres dont l'algorithme proposé a besoin. De plus, les valeurs initiales des cartes du chaos, $x_o$,$x_o$',$x_o$" sont générées en utilisant la somme de contrôle de hachage MD5 de l'image ordinaire. Les clés secrètes utilisées pour chiffrer les images en clair sont différenciées par $x_o$,$x_o$',$x_o$". Selon la sensibilité des clés secrètes, même de minuscules changements aux clés secrètes, il y aura une énorme différence entre les images chiffrées et les images simples, donc cet algorithme proposé est capable de résister aux attaques en texte clair connu et en texte clair choisi.

Deux types spéciaux d'images simples sont utilisés pour tester si l'algorithme proposé est suffisamment robuste pour résister à l'attaque en texte clair choisi. L'une est l'image noire, l'autre est l'image blanche. La figure 4.4 présente les résultats du chiffrement, où nous pouvons comprendre qu'aucune information utile ne peut être directement extraite des images de chiffrement afin que l'algorithme proposé soit qualifié pour résister à l'attaque en texte clair choisi.

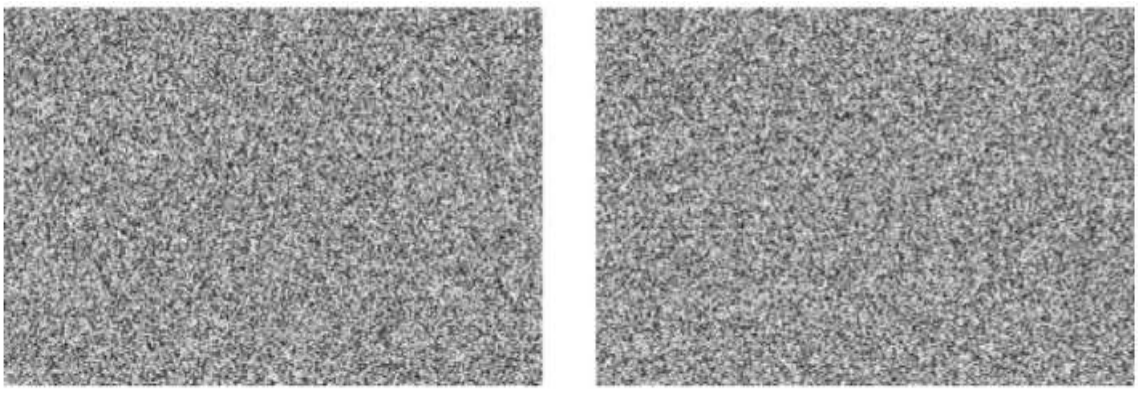



Figure 3.6 Chiffrer les images de l'image noire et de l'image blanche.

## 3.8 Analyse de la complexité temporelle, comparaisons avec d'autres recherches et travaux ultérieurs

### 3.8.1 Analyse de la complexité temporelle

Les instructions les plus fréquemment exécutées et les plus longues sont les opérations de codage et de décodage de l'ADN. Supposons que la taille de l'image ordinaire soit M × N, ce qui signifie qu'il y a M × N pixels dans une image ordinaire. Bien que l'algorithme analyse l'image ordinaire ligne par ligne, en fait, chaque pixel de l'image ordinaire est codé ou décodé. La complexité de base du temps est donc O (M × N).

De plus, lorsque vous utilisez une image ordinaire codée et une image clé codée ligne par ligne, la complexité temporelle est O (4 × M × N). Pour les images en niveaux de gris, chaque pixel a au moins 8 bits, et l'algorithme proposé mappe un octet unique à 4 nucléobases d'ADN, les opérations sont basées sur chaque paire de nucléobases d'ADN. Les éléments impliqués sont donc 4 fois l'image simple et la complexité temporelle de cet algorithme proposé est O (4 × M × N), sous condition d'exécution en série.

## 4. Conclusions

Dans ce mémoire, nous avons proposé un algorithme de cryptage d'image nouveau et efficace qui est basé sur le chaos et les règles de codage de l'ADN. Le codage de l'ADN est une technologie nouvelle mais mature, qui est naturellement bien adaptée au stockage d'informations biologiques. En raison de son bon caractère de traitement des informations, il est largement utilisé dans le domaine du cryptage d'images. Nous considérons l'image ordinaire comme une unité composée de plusieurs lignes. L'algorithme proposé balaye l'image ordinaire de la première ligne à la dernière. Lorsqu'une ligne spécifique est rencontrée, utilisez l'un des huit types de règles de codage d'ADN pour la coder. Le type particulier de règle d'ADN est décidé au hasard par la carte du chaos. Pendant ce temps, une image clé codée est générée. Une fois que l'image entière est complètement codée, faites fonctionner une ligne d'image ordinaire codée et une autre d'image clé codée pour générer une ligne de données codées d'image chiffrée. Décodez l'image chiffrée codée pour obtenir l'image chiffrée intermédiaire que nous utiliserons comme nouvelle image ordinaire pour refaire des opérations similaires afin d'obtenir l'image chiffrée ultime. Soit dit en passant, les opérations menées au cours de ce processus sont choisies au hasard. Les résultats des expériences montrent que l'algorithme proposé a la capacité de crypter en toute sécurité les images.

## Conclusion Générale :

Dans ce mémoire, nous avons proposé un algorithme de chiffrement d'image nouveau et efficace qui est basé sur le chaos et les règles d'encodage de l'ADN. L'encodage de l'ADN est une technologie nouvelle mais mature, qui convient naturellement bien au stockage biologique de l'information. En raison de son bon caractère de traiter avec l'information, il est largement utilisé dans la zone de chiffrement d'image.

Nous considérons l'image simple comme une unité composée de plusieurs lignes. L'algorithme proposé analyse l'image simple de la première ligne à la dernière. Lorsqu'une ligne spécifique est remplie, utilisez l'un des huit types de règles d'encodage d'ADN pour l'encoder.

Le type particulier de règle d'ADN est aléatoirement décidé par la carte de chaos. Pendant ce temps, une image de clé codée est générée. Une fois que l'image ordinaire entière est entièrement codée, actionnez une ligne d'image simple codée et une autre d'image de clé codée pour générer une ligne de données codées de l'image de chiffrement. Décoder l'image de chiffrement codée pour obtenir l'image de chiffrement intermédiaire que nous utiliserons comme nouvelle image simple pour effectuer des opérations similaires à nouveau pour atteindre l'image de chiffrement ultime. Soit dit en passant, les opérations menées au cours de ce processus sont choisis au hasard.

Un algorithme de chiffrement d'image simple et efficace basé sur l'ADN HC (Hyperchaos) a été proposé. Un système hyperchaotique 4-D (en quatre dimensions) a été employé pour générer la séquence de pseudorandom. Pixel brouillage et de substitution ont été réalisés simultanément par GBS (Global Bit Scrambling). Pour augmenter l'efficacité de l'algorithme et l'imprévisibilité du chiffrement, l'opération d'ajout d'ADN a été adoptée au lieu de l'opération binaire. L'espace clé est assez grand pour résister aux différentes attaques. Les résultats montrent que l'ADN HC (Hyperchaos) est assez robuste contre les attaques différentielles. En outre, en raison du GBS et de la non-linéarité de l'opération algébrique de l'ADN, l'ADN HC (Hyperchaos) peut résister efficacement aux attaques linéaires courantes, au bruit et à l'attaque de recadrage.

Les résultats des expériences montrent que l'algorithme proposé a la capacité de chiffrer en toute sécurité les images.

# Bibliographie

[0] : Fakhrulddin H. Ali, Maha Basher Hussein"Algorithme pour chiffrer l'image couleur à l'aide de l'encodage de l'ADN et de la théorie du chaos" 19-21/11/2013.

[a] : BENDAOUD Mohammed Habib"Développement de méthodes d'extraction de contours sur des images à niveaux de gris", 27/02/2017.

[b] :Brahim / Belmesmar Djamila"Traitement d'image et morphologie mathématique"1 / 06 /2016.

[c] : Copyright © 1990- 1998 Network Associates, Inc"Introduction à la cryptographie".

[d] : https://ram-0000.developpez.com/tutoriels/cryptographie/#LI.

[e] : A. Menezes, P. VanOorschot, S. Vanstone,Handbook of applied cryptography, 1997 by CRC Press.

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

[g] : http://www.bart-konieczny.com/fr/blog/securite-des-applications-web/cryptage-symetrique-et-asymetrique

[k] : https://linux.goffinet.org/administration/confidentialite/chiffrement-symetrique#1-algorithmes-de-cryptographie-sym%C3%A9trique-%C3%A0-cl%C3%A9-secr%C3%A8te

[i] : https://fr.wikipedia.org/wiki/Acide_d%C3%A9soxyribonucl%C3%A9ique

[j] : https://www.police-scientifique.com/adn/structure-et-principe-de-base

[k] : https://fr.wikipedia.org/wiki/Nucl%C3%A9otide

[l] : https://www.aquaportail.com/definition-8498-nucleoside.html

[m] : Xingyuan Wang, Chuanming Liu"A novel and effective image encryption algorithm based on chaos and DNA encoding"26 January 2016.

[n]: Kun Zhan, Dong Wei, Jinhui Shi, Jun Yu"Cross-utilizing hyperchaotic and DNA sequences for image encryption" Feb,23, 2017.

## Reference de les figure:

[1]: http://laurent.flaum.free.fr/pgpintrofr.htm

[2]: https://fr.wikipedia.org/wiki/Cryptographie_asym%C3%A9trique

[3]: https://fr.wikipedia.org/wiki/Chiffrement_par_d%C3%A9calage

[4]: https://fr.wikipedia.org/wiki/Scytale

[5]: https://linux.goffinet.org/administration/confidentialite/chiffrement-symetrique

[6]: http://david.carella.free.fr/fr/cryptographie/principes-de-base.html

[7]: https://fr.wikipedia.org/wiki/Acide_d%C3%A9soxyribonucl%C3%A9ique

[8]: https://www.police-scientifique.com/adn/structure-et-principe-de-base