Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE ABOU BEKR BELKAID TLEMCEN

FACULTE DE TECHNOLOGIE

DEPARTEMENT DE Télécommunication

MÉMOIRE

Pour l'obtention du diplôme de

Master en Télécommunications

Option : Réseau et télécommunication

THEME

Chiffrement des images médicales par un crypto système basé sur la théorie du chaos.

REALISES PAR :

- **ZENASNI Houssem Abderrahim**
- **SAIM Younes**

- **Soutenu en 06 juillet 2021 devant le Jury:**

M. ABDELMALAK ABDELHAFID	MCB	Univ. Tlemcen	Président
M. BOUKLI HACENE ISMAIL	MCA	Univ. Tlemcen	Directeur de mémoire
Mlle. ABDI HADJER	Doctorante	Univ. Tlemcen	Co-Directeur de mémoire
M. BOUABDELLAH REDA	MAA	Univ. Tlemcen	Examinateur

Année universitaire : 2020-2021

Remerciement

Tout d'abord, Merci au bon Dieu de nous avoir guidé vers le bon chemin, celui de la science, de nous avoir donné la santé, la volonté et la motivation, pour bien mener ce travail.

Nous tenons à remercier vivement le Docteur BOUKLI HACENE Ismail, qui a su encadrer avec rigueur ce travail de fin d'études. Qu'il trouve ici l'assurance de notre sincère reconnaissance et de notre profonde admiration pour son dévouement au travail, sa disponibilité et sa patience, qualités qui nous ont profondément marqué.

Nos remerciements et notre profonde gratitude s'adressent au doctorante ABDI Hadjer, notre co-encadrant, pour ses multiples conseils, sa disponibilité, son soutien permanent et son encouragement.

Nos remerciements vont également à tous les membres du jury qui ont bien voulu consacrer leur temps précieux pour l'examination de ce mémoire

Nous exprimons notre profonde gratitude au professeur …de nous avoir fait l'honneur de présider le jury.
Nous tenons à remercier chaleureusement le docteur ….d'avoir accepté d'examiner notre travail.

Nos remerciements vont aussi à toute personne ou organisme, qui d'une manière ou d'une autre, a contribué à la réalisation de ce travail.
Veuillez trouver ici l'expression de notre profonde et sincère gratitude.

Dédicace

Durant toutes ces années d'étude, Vous avez cru en moi
Si je suis arrivé ici ce n'est que grâce à vos encouragements et prières.
Le mot MERCI ne suffirait pas et je ne saurais jamais vous récompenser assez.
Je vous dédie avec profonde gratitude ce modeste travail :
Mes très chers parents ; pour votre amour, confiance, compréhension et patience envers moi. Je ne pourrai jamais assez vous remercier
Mes sœurs : Ikram & Myriam
Mes frères : Aymen & Hadi
Merci pour votre soutien permanent, vous avez toujours été là pour moi…

Chère Mima, mes oncles, mes tantes, mes cousins et mes cousines

A la mémoire de ma chère et tendre JEDDATI, aucune dédicace ne suffit pour exprimer l'immense amour que je te porte, tu as été notre petit rayon de bonheur, que dieu te garde dans son vaste paradis, et j'espère que ta bénédiction m'accompagnera toujours

A mes amis : BENSMOSTEFA Hibellah ,groupe technique sur fb « 1001 tech » et mes amies de 44

HOUSSEM

Dédicace

Arrivé au terme du parcours universitaire, J'exprime toute ma gratitude, ma reconnaissance et ma tendresse à mes parents, qui m'ont accompagné tout au long de mon cursus, qui ont su me supporter et me soutenir dans toute circonstance,

Je dédie ce mémoire à ma mère & mon père,
Mon frère : Mohamed
Mes sœurs : Wafaà & Souad

Mes oncles surtout :abdelhafid , mes tantes, mes cousins et mes cousines
Mes chers amis : Houssem Z,Mohamed Amine R,Fekhrredin B, Bilal Z, Amine CH,Amine S,Sofiane S,Reda M, Loqman T et Walid T.

YOUNES

ملخص :

يشهد العالم اليوم تطوراً تقنياً خصوصاً في مجال الاتصالات السلكية واللاسلكية ، والعمل البحثي لهذه الأطروحة هو جزء من تشفير الصور الطبية بواسطة نظام التشفير القائم على نظرية الفوضى ، ونقدم أولاً وقبل كل شيء عمومية على نظام التشفير مع تقنيات التشفير التقليدية مثل: AES و DES و RSA ، مع نظرة عامة على نظرية الفوضى ، تتمثل أصالة هذه الأطروحة في اقتراح خوارزمية تشفير جديدة يمكن تطبيقها على الصور الرمادية العادية والطبية من العمل على بعض الفوضى صورة وخريطة ، مع مقارنة مجموعة من النتائج مما يدل على أننا قمنا بعمل رائع.

الكلمات المفتاحية: التشفير، الصور الطبية، نظام التشفير ،نظرية الفوضى، تقنيات التشفير، الصور العادية ، الخرائط الفوضوية.

Résumé :

Aujourd'hui, le monde assiste à un développement technologique, notamment dans le domaine des télécommunications, Les travaux de recherche de ce mémoire s'inscrivent dans le cadre de chiffrement des images médicales par crypto-système basé sur la théorie de chaos. Nous présentons en premier lieu les généralités sur le système de cryptage traditionnelles tel que : AES, DES et RSA. L'originalité de ce mémoire consiste à proposer un nouvel algorithme de cryptage qui peut être appliqué aux images normales et médicales en niveaux de gris basé sur les cartes chaotiques. Nous avons obtenus de bons résultats comparés avec d'autres algorithmes trouvés dans la littérature.

Mots clés : chiffrement, images médicales, crypto-système, théorie de chaos, techniques de cryptage, images normales, carte chaotique.

Abstract : Today , the world is witnessing a technological development, especially in the field of telecommunications. The research work of this thesis is part of the framework of encryption of medical images by crypto-system based on chaos theory. We first present the generalities on the traditional encryption system such as: AES, DES and RSA. The originality of this thesis is to propose a new encryption algorithm that can be applied to normal and medical grayscale images based on chaotic maps. We have obtained good results compared with other algorithms found in the literature.

Key Word: encryptions, medical image, crypto-system, chaos theory, encryptionstechniques,normalimages, chaotic Mapp.

LISTE DES FIGURES

Figure I.1: Principe générale d'un algorithme de chiffrement.

Figure I.2: les méthodes de la cryptographie moderne.

Figure I.3: La cryptographie symétrique.

Figure I.4 : Schémas générale du DES.

Figure I.5: Schéma chiffrement et déchiffrement de l'AES.

Figure I.6 : La cryptographie Asymétrique.

Figure I.7 :Principe du chiffrement/déchiffrement asymétrique.

Figure I.8: Les différents standards de fonctions de hachage.

Figure II.1 : Image numérique.

Figure II.2 : Distribution des pixels par lignes et colonnes .

Figure II.3 : Les mesures en pouce.

Figure II.4 : Différence entre image vectorielle et image matricielle.

Figure II.5 : Codage binaire (0,1) .

Figure II.6 : Image Noir et blanc .

Figure II.7: image de niveau de gris.

Figure II.8 : Image niveau de gris .

Figure II.9: les couleur de image RVB.

Figure II.10 : Image RVB.

Figure II.11 : Image médicale **.**

Figure II.12 : Scanner D'IRM.

Figure II.13: Un échantillon d'images radiographiques.

Figure II.14: Le Rayon X dans Image médicale.

Figure II.15: Image L'échographie.

Figure II.16 : Séquences générées par la fonction logistique pour X_0= 0.1 pour :a) r = 2 ;b) r = 3.2 ; c) r = 3.55 ; d) r = 3.9.

Figure II.17 : Attracteur de l'équation logistique.

Figure II.18 : L'espace de phase de la carte standard / K = 0.5, 1.0, 1.5, 2.5, 6.0 et 18.9 .

Figure II.19 : Algorithme de chiffrement image .

Figure II.20 : Histogramme d'une image de niveau de gris .

Figure II.21 : Histogramme d'une image Crypté .

Figure III.1 : Création de clé.

Figure III.2 : Fonction de cryptage par la carte chaotique logistique

Figure III.3 : Fonction de déchiffrement par la carte chaotique logistique

Figure III.4 : les images originales.

Figure III.5: les images crypté par la carte chaotique.

Figure III.6 : les images décryptées par la carte chaotique

Figure III.7 : Histogramme des images original.

Figure III.8 : Histogramme des images crypté par la carte chaotique logistique.

Figure III.9 : Histogramme des images crypté par la carte Arnold.

Figure III.10 : résultats des corrélation.

LISTE DES TABLEAUX

Tableau I.1: La comparaison entre la cryptographie symétrique et asymétrique .

Tableau II.1 : : Les formats vectoriels .

Tableau III.1 : cryptage image de Cerveau .

Tableau III.2: résultats des entropie

Tableau III.3 : résultats des corrélation

Tableau III.4: résultats des NPCR et UACI

Tableau III.5: résultats des entropie .

Tableau III.6 : résultats des corrélation

Tableau III.7: résultats des NPCR et UACI.

t**ableau III.8**: comparaison entre carte logistique et carte Arnold.

LES ABREVIATIONS

AES : Advanced encryption standard.

BMP: BitMaP.

CCITT : Comité consultatif international téléphonique et télégraphique.

CLM : Chaotique logistique Mapp.

CNRS: Centre national de la recherche scientifique.

DES : data encryptions standard.

DEXA : Dual Energy X-Ray Absorptiometry.

dpi : dots per inch.

FIPS : Federal Information Processing Standard.

GIF: *Graphics Interchange Format.*

IBM: International Business Machine .

IRM : Imagerie Par Résonance Magnétique**.**

ISO : Organisation internationale de normalisation.

JFIF : *JPEG File Interchange Format.*

JPEG: Joint Photographic Experts Group.

LZ: algorithm Lempel-Ziv.

LZW: Lempel-Ziv -Welch .

NIST: National Institute of Standards and Technologies.

NPCR: Number of *Pixels* Change Rate.

PCX: *PiCture eXchange.*

PNG : Portable Network Graphics .

PRGA :*Princeton Reconfigurable Gate Array*.

RC4 : Rivest Cipher 4.

***RLE* :** algorithm Run Length Encoding.

RSA : Rivest, Shamir and Adleman.

RVB : Rouge, Vert et Bleu.

SSI: *système de sécurité incendie.*

TIFF: Tagged Image File Format.

UACI : Unified average changing intensity**.**

TABLE DES MATIERES

1 INTRODUCTION GENERALE 1

CHAPITRE I: GENERALITE SUR LA CRYPTOGRAPHIE

1 INTRODUCTION. 2

1 INTRODUCTION SUR LA SECURITE INFORMATIQUE : 2

1.1 SECURITE D'INFORMATIQUE : 2
1.2 LA VULNERABILITE : 2
1.3 MENACE : 2
1.4 RISQUE : 2
1.5 ATTAQUE : 2

2 NOTION DE BASE SUR LA CRYPTOGRAPHIE : 3

2.1 CRYPTOLOGIE : 3
2.2 CRYPTOGRAPHIE : 3
2.3 CRYPTANALYSE : 3
2.4 CRYPTO-SYSTEME : 3
2.5 LES CLEFS : 3
2.6 CHIFFREMENT : 4
2.7 TEXTE CHIFFRE : 4
2.8 LE DECHIFFREMENT : 4

3 PROPRIETE DE CRYPTOGRAPHIE : 4

3.1 LA CONFIDENTIALITE : 4
3.2 L'INTEGRITE : 4
3.3 L'AUTHENTIFICATION : 4
3.4 LA NON-REPUDIATION : 4

4 CLASSIFICATION DES SYSTEMES CRYPTOGRAPHIE : 5

4.1 CRYPTO-SYSTEME SYMETRIQUE 5
4.1.1 Chiffrement par blocs : 5
4.1.2 Chiffrement par flots : 10

4.2 CRYPTO-SYSTEME ASYMETRIQUE : 10
4.2.1 Principe de fonctionnement du chiffrement asymétrique 11
4.2.2 Fonction à sens unique : Fonction de Hachage 13
4.2.3 Applications des fonctions de hachage 14
4.2.4 Signature électronique 14
4.2.5 Signature RSA 16
4.3 COMPARAISON ENTRE LA CRYPTOGRAPHIE SYMETRIQUE ET ASYMETRIQUE : 17
5 CONCLUSION : 17
CHAPITRE II: Introduction au système chaotique
1 INTRODUCTION : 19
2 NOTION DE BASE : 19
2.1 DEFINITION D'UNE IMAGE : 19
2.2 IMAGE NUMERIQUE 19
2.3 PIXEL : 19
2.4 LA DEFINITION 20
2.5 LA TAILLE 20
2.6 LA RESOLUTION 20
3 LES DIFFERENTS TYPES D'IMAGE : 21
3.1 IMAGE MATRICIELLE (BITMAP) 21
3.2 IMAGE VECTORIELLE 21
4 LES DIFFERENTS FORMATS D'IMAGES : 22
4.1 LES FORMATS D'IMAGE MATRICIELS 22
4.1.1 JPEG : 22
4.1.2 TIFF 22
4.1.3 GIF 22
4.1.4 PNG 23
4.2 LES FORMATS VECTORIELS 23
5 LES DIFFERENTS MODES DE COULEURS DES IMAGES 24
5.1 MODE BINAIRE (NOIR ET BLANC) : 24
5.2 MODE NIVEAU DE GRIS : 24
5.3 MODE COULEUR (RVB) : 25

6 IMAGERIE MEDICALE : 26

6.1 DEFINITION 26

6.2 TYPES D'IMAGERIE MEDICALE 26

6.2.1 Les champs magnétiques 26

6.2.2 La radioactivité 27

6.2.3 Les rayons X 27

6.2.4 L'échographie 28

7 CHIFFREMENT DU CHAOS ET CHIFFREMENT DES IMAGES: 29

7.1 DEFINITION : 29

7.2 LES CONDITIONS D'UN SYSTEME CHAOTIQUE: 29

7.2.1 La carte chaotique logistique simple : 30

7.2.2 La carte chaotique sine : 31

7.2.3 la carte chaotique standard : 31

7.2.4 La carte d'Arnold 32

7.2.5 Tchebychev 32

7.3 RELATION ENTRE LE CHAOS ET LES CRYPTO-SYSTEMES : 32

8 CRITERE D'EVALUATION 33

8.1 L'HISTOGRAMME : 33

8.2 LA CORRELATION : 34

8.3 L'ENTROPIE : 34

8.4 LES TESTS DIFFERENTIELS : 35

Le NPCR 35

l'UACI 35

8.5 ESPACE DE CLES: 35

8.6 SENSIBILITE DE LA CLE : 35

9 ETAT DE ART : 36

10 CONCLUSION : 36

CHAPITRE III: RESULTATS EXPEMENTAUX

1 INTRODUCTION 38

2 LES METHODES UTILISEES 38

2.1 GENERATEUR DE CLE : 39

2.2 CHIFFRE IMAGE 40

2.2.1Etape de confusion 40
2.2.2Etape de diffusion 40
2.3 DECHIFFREMENT IMAGE 41
3 RESULTATS EXPERIMENTAUX 41
3.1 LES DONNEES UTILISEES 41
3.2 ENVIRONNEMENT DE DEVELOPPEMENT 41
3.3 LANGAGE DE PROGRAMMATION 42
3.4 IMAGE NIVEAU DE GRIS ET IMAGES MEDICALES 42
4 CRITERES D'EVALUATION 44
4.1 L'ESPACE DE CLE 44
4.2 LA CARTE CHAOTIQUE LOGISTIQUE 44
4.2.1 Histogramme des image original : 44
4.2.2 Histogramme des images crypté : 47
4.2.3 L'entropie 51
4.2.4 La corrélation entre les pixels adjacents 52
UACI et NPCR 53
4.3 LA CARTE ARNOLD MAPP 54
4.3.1 Histogramme des image crypté : 54
4.3.2 Entropie 56
4.3.3 Corrélation 58
UACI et NPCR 59
COMPARAISON ENTRE CARTE LOGISTIQUE ET CARTE ARNOLD 60
5 CONCLUSION 62
1 CONCLUSION GENERAL 64
BIBLIOGRAPHIE 65

Introduction générale

1 Introduction générale :

Depuis longtemps, l'homme avait besoin de moyens secrets pour transmettre des messages. Actuellement, avec la grande accélération dans le développement des technologies d'Internet et de la communication, la communication des images en général et les images médicales en particulier qui jouent un rôle très important dans la transmission de l'information.

La problématique dans notre projet de fin d'étude entre dans le cadre de la protection des images médicales à travers des canaux de communication non sécurisé ? Donc, il est primordial de chiffrer les images avant leur transmission sur le réseau. Il n'est pas évident d'utiliser des méthodes de chiffrement classiques standard comme RSA, DES, AES, pour le chiffrement d'image médicales, car ils ne sont pas atteindre fin requis pour ce type de données et l'accélération en multimédias. Ainsi les images médicales sont caractérisées par la redondance élevée, la forte corrélation et par leurs tailles volumineuse. Notre 2eme contribution s'intègres dans la construction d'un système fiable de cryptage dont le but d'assurer la sécurité de ce type de données ? Dans ce mémoire nous allons répondu à cette problématique, on va développer et implémenter un système chaotique qui gère à la fois des images médicales et les images normales.

Organisation du mémoire :

Nous avons structuré notre mémoire en trois chapitres. Dans Le premier chapitre, nous donnons une brève présentation sur les techniques de cryptographie et ses classifications.

Le deuxième chapitre, nous allons introduire au début le concept de base de l'imagerie numérique. Ensuite, nous allons exposer la théorie sur les systèmes chaotique, ainsi que les différents types tel que : logistique simple, sine et standards. Un état de l'état sur les différents travaux existants sur les systèmes chaotique dans la littérature a été présenté.

Dans le troisième chapitre, des résultats expérimentaux ont été présenté en détail pour le chiffrement des images naturelles et d'images médicales en particulier par les systèmes chaotique dont nous allons utiliser deux types tel que : la carte logistique simple et la carte Arnold.

Puis on va terminer par une conclusion générale et quelques perspectives pouvant aider la communauté scientifique dans l'amélioration de notre système dans le futur.

CHAPITRE I

GENERALITES SUR LA CRYPTOGRAPHIE

1 Introduction :

La sécurité informatique s'agit d'un domaine très large, couvrant tous les aspects de la protection des informations ou des données. Et à cette fin la plupart des développeurs se concentrent sur les techniques de cryptage pour fournir de bons résultats de protection de ces données numérique.

Dans ce chapitre, nous expliquons les terminologies de base de la cryptographie, ainsi que leurs propriétés et nous terminons par les classifications des algorithmes de cryptage symétrique et asymétrique en détails.

1 Introduction sur la sécurité informatique :

1.1 Sécurité d'informatique :

La sécurité informatique (SSI) est une discipline qui se veut de protéger l'intégrité et la confidentialité des informations stockées dans un système informatique et pour réduire la vulnérabilité d'un système informatique système contre les menaces accidentelles.

1.2 La vulnérabilité :

Faiblesse au niveau d'un bien (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien). [2]

1.3 Menace :

Cause potentielle d'un incident, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.[2]

1.4 Risque :

$$\textbf{Risque} = \frac{\boldsymbol{Menace} \times \boldsymbol{Vunlérabilité}}{\boldsymbol{Contre-mesure}} \quad \textbf{.....(I.1)}$$

La probabilité qu'une menace exploitera une vulnérabilité du système. Couple (menace, vulnérabilité) [3]

1.5 Attaque :

Action malveillante destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la concrétisation d'une menace, et nécessite l'exploitation d'une vulnérabilité. [2]

2 Notion de Base sur la Cryptographie :

2.1 Cryptologie :

Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse.[4]

Cryptologie = Cryptographie + Cryptanalyse ……..……(I.2)

2.2 Cryptographie :

Le mot « Cryptographie » est composé des mots grecques : CRYPTO = caché / GRAPHY = écrire. C'est donc l'art de l'écriture secrète. C'est une science permettant de préserver la confidentialité des échanges.[5]

2.3 Cryptanalyse :

Est l'art de déchiffrer des messages chiffrés sans besoin de savoir la clé de déchiffrement à fin de trouver les attaques qui peuvent casser un crypto-système. [5]

2.4 Crypto-système :

Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné. [6]

2.5 les clefs :

Il s'agit d'un paramètre important utilisé comme entrée pour les opérations de chiffrement et déchiffrement.

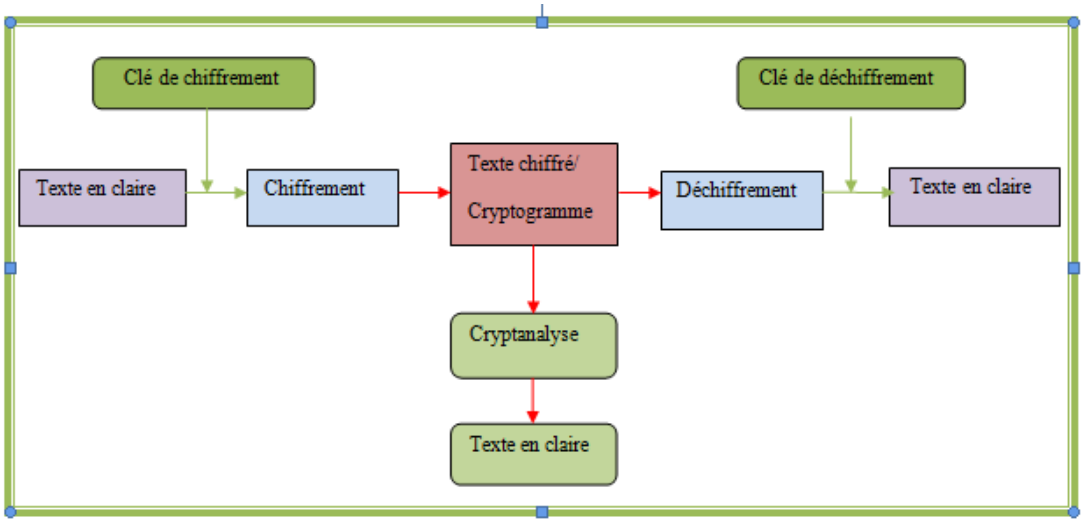


Figure 1.1: Principe générale d'un algorithme de chiffrement.

2.6 Chiffrement :

Le chiffrement est une transformation cryptographique qui transforme un message clair en un message inintelligible (dit message chiffré), afin de cacher la signification du message original aux tierces entités non autorisées à l'utiliser ou le lire.[5]

2.7 Texte chiffré :

Appelé également cryptogramme, Données ou messages incompréhensibles causés par le cryptage.

2.8 Le Déchiffrement :

Le déchiffrement est l'opération qui permet de restaurer le message original à partir du message chiffré.

3 Propriété de cryptographie :

3.1 La confidentialité :

Consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.

3.2 L'intégrité :

Permet de vérifier qu'une donnée reçue par le récepteur n'a pas été modifiée par une entité tierce (accidentellement ou intentionnellement).

3.3 L'authentification :

Permet de vérifier l'identité revendiquée par une entité, ou l'origine d'un message, ou d'une donnée.

3.4 La non-répudiation :

Permettant de garantir qu'une transaction ne peut être niée. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues [7].

4 Classification des systèmes cryptographie :

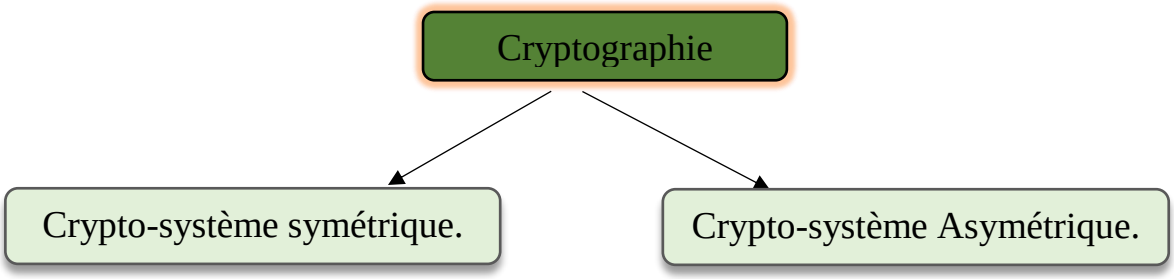


Figure 1.2: les méthodes de la cryptographie moderne.

4.1 Crypto-système symétrique :

Dans le chiffrement symétrique, une même clé est partagée entre l'émetteur et le récepteur. Cette clé dite symétrique est utilisée par l'émetteur pour chiffrer le message et par le récepteur pour le déchiffrer en utilisant un algorithme de chiffrement symétrique. Ce type de chiffrement permet de :

- Garantir la confidentialité du message chiffré
- Utiliser une paire de clés publique/privée
- Assurer la non-répudiation

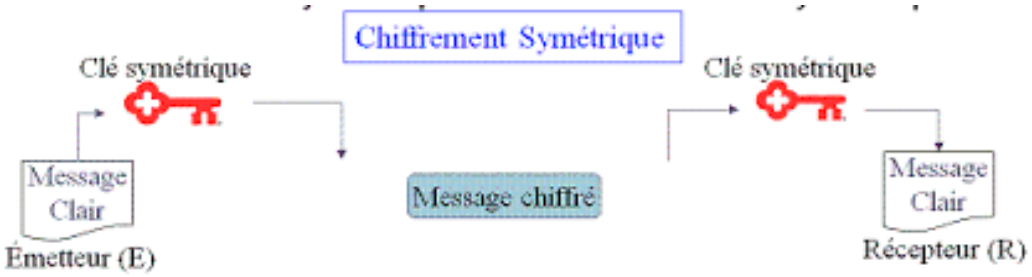


Figure 1.3: La cryptographie symétrique.[5]

Il existe deux types d'algorithmes de chiffrement symétrique :

4.1.1 Chiffrement par blocs :

Le principe des algorithmes de chiffrement par bloc est de diviser un texte clair en blocs de la taille fixe, puis chaque bloc est chiffré avec une clé de la même taille.

Parmi les algorithmes les plus utilisés :

a) **DES (data encryptions standard)** :

DES est l'un des algorithmes pionnier de chiffrement symétrique. Il est basé sur un ensemble de permutations et substitutions comme présenté ci-dessous. C'est un algorithme qui opère sur des blocs de 64 bits, et utilise une clé de 56 bits qui était suffisante à l'époque. .[5].

Le cahier des charges était le suivant :

- L'algorithme repose sur une clé relativement petite, qui sert à la fois au chiffrement et au déchiffrement.
- L'algorithme doit être facile à implémenter, logiciellement et matériellement, et doit être très rapide.
- Le chiffrement doit avoir un haut niveau de sûreté, uniquement lié à la clé, et non à la confidentialité de l'algorithme.

Principe du DES :

DES n'est qu'un code produit Shannon : il combine à la fois diffusion et confusion, et ces technologies elles-mêmes ne sont pas très sécurisées. Cependant, leur combinaison permet de s'appuyer sur un niveau de sécurité assez élevé. Personne ne peut prouver l'intégrité de ce produit, mais les bits de cryptage aléatoires dans le produit rendent toute cryptanalyse très difficile. La Permutation utilise ici la permutation, le but est de casser le fichier redondant crypté dans le fichier Clair.

La confusion qui a pour but de compliquer la liaison entre le fichier crypté et les clés secrètes, utilise ici des substitutions, non linéaires, de façon à produire un système cryptographique qui résiste à toute cryptanalyse mathématique.

En effet, la sécurité des données cryptées repose sur une clé secrète de 64 bits (succession de 0 et de 1), Mais en réalité, seuls 56 bits sont utilisés pour déterminer la clé. Les bits 8, 16, 24, 32,40, 48, 56, 64 sont des bits de parité (bits de détection d'erreur). Le 8éme bit est fait en sorte que sur les 8 premiers bits, il y ait un nombre impair de 1. Par exemple, si les 7 premiers bits sont 0110101, le 8éme bits est 0. Ceci permet d'éviter les erreurs de transmission.

Les étapes de l'algorithme sont les suivantes :

- 1er préparation- diversification de la clé :

Le texte est divisé en blocs de 64 bits. Nous avons également diversifié la clé K, c'est-à-dire que nous avons fabriquons K en 16 sous-clés K1,..., K16 en 48 bits. Ki est composé de 48 K bits dans un ordre spécifique.

- 2eme permutation initiale :

Pour chaque bloc de 64 bits x du texte, on calcule une permutation finie y=P(x). Y est exprimé sous la forme $y = G_0D_0$, où G_0 correspond aux 32 bits du côté gauche de y et D_0 aux 32 bits du côté droit.

- 3eme Itération :

On applique 16 rondes d'une même fonction. A partir de $G_{i-1}Di_{-1}$ (pour i de 1 à 16), on calcule G_iD_i en posant :

- $G_i=D_{i-1}$
- $D \otimes G_{i-1}$ $f(D_{i-1},K_i)$

Et pour le déchiffrement

- $C \otimes = D_i$ $f(G_i,K_i)$
- $D_{i-1}= G_i$

XOR est le ou exclusif bit à bit « 0 XOR 0 =0 , 0 XOR 1=1 » et f est une fonction de confusion, suite de substitution et de permutations.

- 4eme permutation finale :

On applique à $G_{16}D_{16}$ la permutation initiale dans le sens inverse. $Z=P^{-1}(G_{16}D_{16})$ est le bloc de 64 bits chiffré à partir de x.

Description du DES :

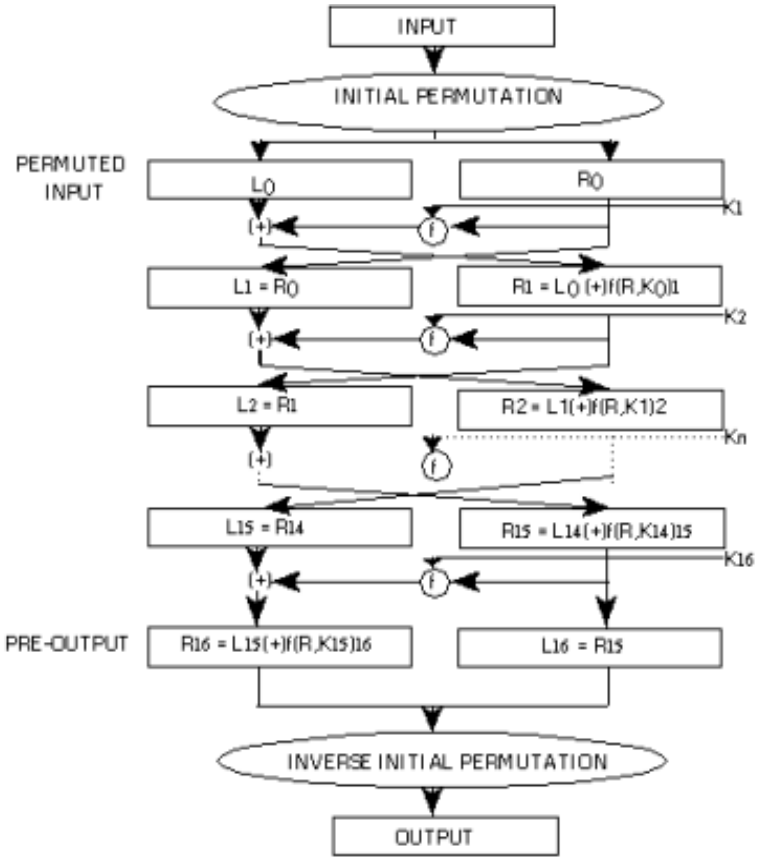


Figure 1.4 : Schémas générale du DES [5]

Les avantages

Ce cryptage présente de grands avantages :

- sa rapidité, il est particulièrement adapté à la transmission de grandes quantités de données .

Les inconvénients

- nombres de clés.
- Taille des clés .
- Distribution de clés.
- Connaissance de clé par l'émetteur et récepteur.

AES(Advanced encryptions standard) :

La progression de la puissance des ordinateurs a causé la mort du DES. En janvier 1997, le NIST (National Institute of Standards and Technologies) des Etats-Unis lance un appel d'offres pour élaborer l'AES, Advanced encryptions System. Le cahier des charges comportait les points suivants :

- évidemment, une grande sécurité.
- une large portabilité: l'algorithme devant remplacer le DES, il est destiné à servir aussi bien dans les cartes à puces, aux processeurs 8 bits peu puissants, que dans des processeurs spécialisés pour chiffrer des milliers de télécommunications à la volée.
- la rapidité.
- une lecture facile de l'algorithme, puisqu'il est destiné à être rendu public.
- techniquement, le chiffrement doit se faire par blocs de 128 bits, les clés comportant 128,192 ou 256 bits.

Au 15 juin 1998, date de la fin des candidatures, 21 projets ont été déposés. Certains sont l'œuvre d'entreprises (IBM,...), d'autres regroupent des universitaires (CNRS,...), les derniers sont écrits par à peine quelques personnes. Pendant deux ans, les algorithmes ont été évalués par des experts, avec forum de discussion sur Internet, et organisation de conférences. Le 2 octobre 2000, le NIST donne sa réponse : c'est le Rijndael qui est choisi, un algorithme mis au point par 2 belges, Joan Daemen et Vincent Rijmen. Depuis, le Rijndael, devenu AES, a été

largement déployé et a remplacé progressivement le DES.

- **Les propriétés d'AES :**

- Plusieurs longueurs de clef et de bloc sont possibles : 128, 192, ou 256 bits
- Le nombre de cycles (ou "rondes") varie en fonction de la longueur des blocs et des clés (de 10 à14)
- La structure générale ne comprend qu'une série de transformations/permutations/sélections
- Il est beaucoup plus performant que le DES

- Il est facilement adaptable à des processeurs de 8 ou de 64 bits
- Le parallélisme peut être implémenté .

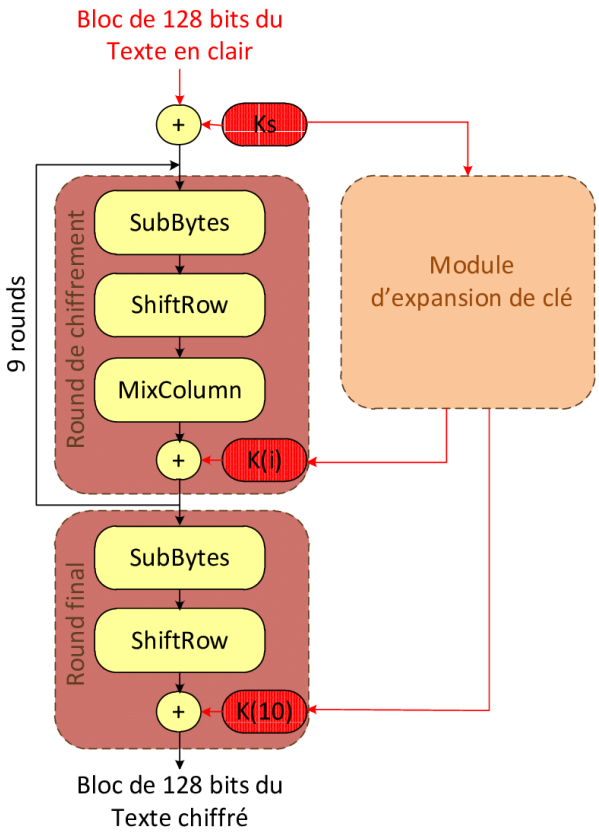


Figure 1.5: Schéma chiffrement et déchiffrement de l'AES.[6]

4.1.2 Chiffrement par flots :

le bloc a une dimension unitaire (1 bit, 1 octet, ...).[5]

par exemple :

RC4 : chiffrement octet par octet .

4.2 Crypto-système Asymétrique :

La cryptographie symétrique consiste à chiffrer puis déchiffrer un message en utilisant la même clé et le même algorithme.

La distribution des clés a été le point faible des systèmes de cryptographie symétrique, d'où la proposition des algorithmes à clés publiques (algorithmes asymétriques)

La cryptographie asymétrique (à clés publiques) exige que chacun des correspondants possède une clé publiée dans un annuaire utilisée par tout le monde pour chiffrer des messages destinés à un individu particulier, et l'autre privée que cet individu est seul à détenir et qui lui permet de déchiffrer les messages qu'il reçoit.

Figure 1.6 : La cryptographie Asymétrique.[5]

- Une clé publique pour le chiffrement.
- Une clé secrète pour le déchiffrement

Etant donné les avantages potentiels de la cryptographie à clé publique les chercheurs se sont attelés à la tache et quelques algorithmes ont été publiés.

4.2.1 Principe de fonctionnement du chiffrement asymétrique :

- Afin de permettre à ses correspondants de lui envoyer des messages cryptés, Ali doitpréparer sa clé publique qu'il diffusera à tous le monde dans un annuaire, il prépare également sa clé privée qu'il sera seul à connaitre.
- Pour chiffrer un message destiné à Ali, Omar doit récupérer la clé d'Ali publiée dans l'annuaire.
- Grace à sa clé privée, Ali peut déchiffrer et lire le message que Bob a envoyé.

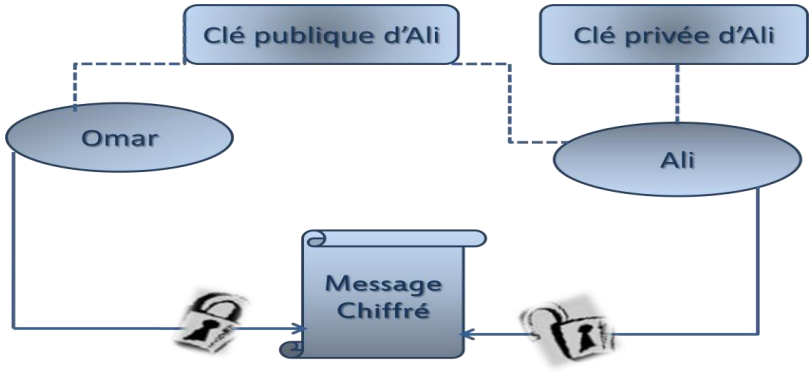


Figure 1.7 :Principe du chiffrement/déchiffrement asymétrique.

Omar chiffre avec la clé publique d'Ali . Ali le déchiffre avec sa clé privée

Algorithmes de chiffrement asymétrique :

RSA :

L'algorithme RSA est sans doute le plus utilisé des systèmes à clé publique actuellement ;il a été présenté en 1977 par Ron Rivest, Adi Shamir, et Len Adlmen. Il nécessite des clés d'au moins 1024 bits pour obtenir une sécurisation satisfaisante.

- Principe de fonctionnement du RSA :

Etape 1: Création des clés :

Ali choisit au hasard deux nombres premiers p et q et calcule $n = pq$ Il choisit au hasard e tel que :

$$\begin{cases} 1 < e < \phi(n) = (p-1)(q-1) \\ p\gcd(e, \phi(n)) = 1 \end{cases}$$

f(n): le nombre d'entiers inférieurs à n, premiers avec n

Ali calcule l'entier d pour inverser la fonction de chiffrement tel que :

$$\begin{cases} 1 < d < \phi(n) \\ ed = 1 \, mod \, \phi(n) \end{cases}$$

La clé publique d'Alice est (n,e) et sa clé secrète est (n,d)

Etape 2: Chiffrement du message :

Omar récupère la clé publique (n,e) d'Ali et souhaite lui envoyer la version cryptée d'un texte enclair, représenté par la donnée d'un entier m tel que :

$$0 \leq m < n.$$

calcule : $c = m^e \ mod \ m$……(I.3)

Etape 3: Déchiffrement du message :

Lorsque Ali reçoit c, il calcule c^d, et récupère ainsi le message m puisque :

$$m = c^d \ mod \ n \text{……(I.4)}$$

Ce qu'est en rouge sont des nombres privée d'Ali.

4.2.2 Fonction à sens unique : Fonction de Hachage :

Les fonctions de hachages sont des fonctions à sens uniques « sans collision », générant une sortie de taille fixe (appelée condensat ou empreinte), caractéristique des données fournies en entrée.

Ces fonctions sont dites à sens unique car il est impossible de retrouver les données initiales à partir del'empreinte.

Une fonction est dite « sans collision » ou « injective » lorsqu'il est réputé très difficile de trouver deux sources différentes conduisant à un même résultat.

Les fonctions de hachage permettent entre-autres, grâce au calcul du condensat d'un document et lacomparaison de celui-ci avec sa valeur initiale, de :

- contrôler l'intégrité d'un document.
- comparer un mot de passe entré par un utilisateur à un mot de passe stocké dans une base de données
- publier l'empreinte d'un logiciel : pour comparer l'empreinte fournie par l'éditeur et l'empreinte qu'il obtient sur le fichier téléchargé
- vérifier l'intégrité d'un message de son point d'envoi jusqu'au destinataire.

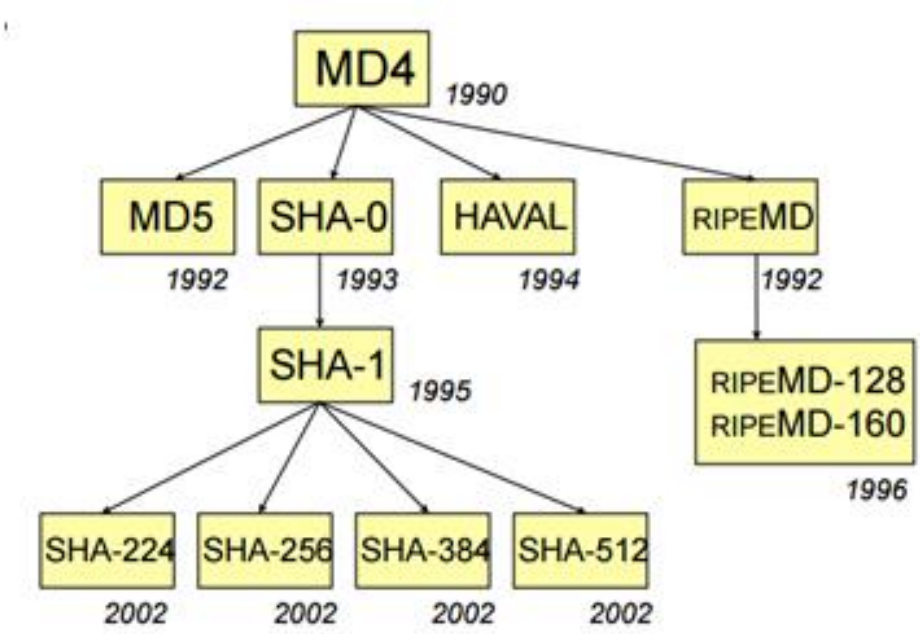


Figure 1.8:Les différents standards de fonctions de hachage

4.2.3 Applications des fonctions de hachage :

- Calcul d'empreinte
- Vérification d'intégrité
- Vérification d'authenticité
- Dérivation de clés :
  - Utilisation avec des clés secrètes
  - Hiérarchie de clés
- Générateur pseudo-aléatoire

4.2.4 Signature électronique :

La cryptographie à clé publique existe depuis un certain temps déjà. L'essor Internet dans le monde, modifie de manière fondamentale les modes de communication. Ainsi, de plus en plus de documents qui étaient auparavant transmis sur papier sont maintenant échangés électroniquement. Cela présente de nombreux avantages : les communications entre une entreprise et ses clients sont beaucoup plus rapides, et la réduction de la quantité de papier nécessaire à ces communications ne peut être que bénéfique pour l'environnement.

La cryptographie à clé publique est extrêmement attrayante et riche en perspectives, intégrant à la fois le chiffrement et la signature numérique. Elle constitue une véritable percée par rapport aux systèmes cryptographiques à clé symétrique.

Une signature électronique est un ensemble de données informatiques générées à partir d'un document électronique qui permet d'authentifier ce document. Elle peut être intégrée au document ou séparée de celui-ci.

Une signature électronique doit garantir deux propriétés : elle doit identifier le signataire du document, et garantir que le document n'a pas été altéré depuis l'apposition de la signature.

La signature électronique repose sur deux familles d'algorithmes, qui seront utilisés de manière complémentaire :

Les algorithmes de chiffrement asymétriques et les fonctions de hachages:

Principe de signature et vérification :

Voici comment se déroule la signature d'un document, et la vérification de cette signature :

Signature :

Le signataire calcule le condensat du document à signer, puis il chiffre ce condensat à l'aide de sa clé privée.

Il crée ensuite la signature, qui peut être intégrée au document original ou enregistrée dans un fichier séparé. Cette signature est composée de l'empreinte signée (le condensat chiffré) et de son certificat.

Vérification :

Le destinataire calcule le condensat du document reçu (en omettant la signature, si celle-ci est intégrée au document), et déchiffre l'empreinte signée, à l'aide de la clé publique contenue dans le certificat du signataire.

La sécurité de la plupart des schémas de signature est basée sur l'intractabilité d'un des problèmes suivants :

- le problème du logarithme discret dans un groupe multiplicatif (DLP),

- le problème du logarithme discret sur les courbes elliptiques (Elliptic Curve Discrète Logarithme Problème, ECDLP)
- le problème de factorisation en nombres premiers (FP).

4.2.5 Signature RSA :

A partir du fait que la transformation de chiffrement RSA est une bijection, les signatures numériques peuvent être créées en inversant les rôles de cryptage et de décryptage.

- Algorithme de génération de clés pour le schéma de signature RSA Chaque entité crée une clé publique RSA et une clé privée correspondante. Chaque entité A doit faire ce qui suit:

1. Générer deux grands nombres premiers distincts p et q au hasard, ayant les deux la même taille.
2. Calculer n = pq et j(n) = (p - 1) (q - 1).
3. Sélectionnez un e entier aléatoire, 1 <e<j(n), tels que pgcd (e; j(n)) = 1.
4. Utiliser l'algorithme d'Euclide étendu pour calculer l'unique entier d, 1 < d < j(n),tel que ed º 1 (modj(n)).
5. La clé publique est (n; e); la clé privée est d.

- Algorithme de génération et de vérification de signature RSA

Une entité A signe un message m. Toute entité B peut vérifier la signature A et récupérer le message m à partir de la signature.

1. **Génération de signature :** L'entité A doit faire ce qui suit

- Calculer m˜ = H (m), à l'aide d'une fonction de hachage
- Calculer s = m˜d mod n.
- La signature de m pour A est s.

2. **Vérification :** Pour vérifier la signature de A et de récupérer le message m, B doit:

- obtenir la clé publique authentique de A : (n, e).
- Calculer m˜ = se mod n.
- Vérifiez que m˜ = H (m), sinon, rejeter la signature.

4.3 Comparaison entre la cryptographie symétrique et asymétrique :

La figure ce dessus montre le tableau de comparaison entre la cryptographie symétrique et asymétrique :

Le type de crypto système	Les avantages	Les inconvénients
Symétrique (clé secrete)	• Clés relativement courtes (128 ou 256 bits) • Rapide • Facile	• Gestion des clés difficiles (nombreuses clés) • Difficulté de distribuer la clé secrète • Ne permet pas de signature électronique
Asymétrique (clé public)	• Utilise deux clés différentes • Fournit des garanties d'intégrité et de non répudiation par signature électronique • Très utile pour échanger les clés	• Des clés plus longues (1024 à 4096 bits) • Lenteur de calcul • Difficile

Tableau 1.1: La comparaison entre la cryptographie symétrique et asymétrique [8].

5 Conclusion :

Dans ce chapitre, nous avons expliqué les terminologies de base de la cryptographie, puis nous avons parlé sur leurs propriétés et ces différents types. Enfin, en termine par les classifications des algorithmes de cryptage avec une comparaison. Dans le chapitre qui suit nous parlerons en détails sur cryptage des images médicales basé sur la théorie de chaos.

CHAPITRE II

Introduction au système chaotique

1 Introduction :

En raison de l'importance des images numériques et de la valeur des informations qu'elles contiennent, Dans ce chapitre, nous allons comprendre les concepts de base de l'imagerie à travers les types des images numériques, les formats connues les plus célèbres et leurs caractéristiques. Dans la deuxième partie, nous allons décrit les techniques de cryptage d'image avec la théorie de chaos et état de l'art.

2 Notion de base :

2.1 Définition d'une image :

La définition est le nombre de points (ou pixel) que comporte une image numérique en largeur et en hauteur (le nombre de colonnes et nombre de ligne).

2.2 Image numérique

Les images numériques sont des images (Dessins, icônes, photos ...) créées, traitées, stockées sous forme binaire (ordre de 0 et 1).

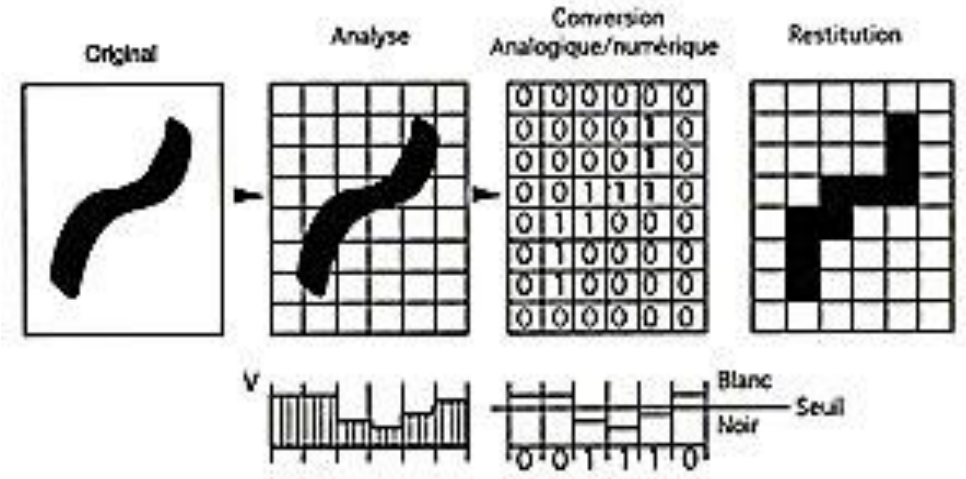


Figure 2.1 : Image numérique .

2.3 Pixel :

Le pixel (abréviation venant de l'anglais « **Pic**ture **él**iment ». Le point de base de la numérisation d'images. Un pixel peut être représenté par un seul bit (noir ou blanc), ou plus souvent par 8, 16, voire 32 bits qui contient des informations telles que la couleur, la texture, la transparence, etc.

Par conséquent, un pixel correspond à un point de chromaticité, et lorsqu'il est combiné avec de nombreux autres points, une image dite matricielle est formée.

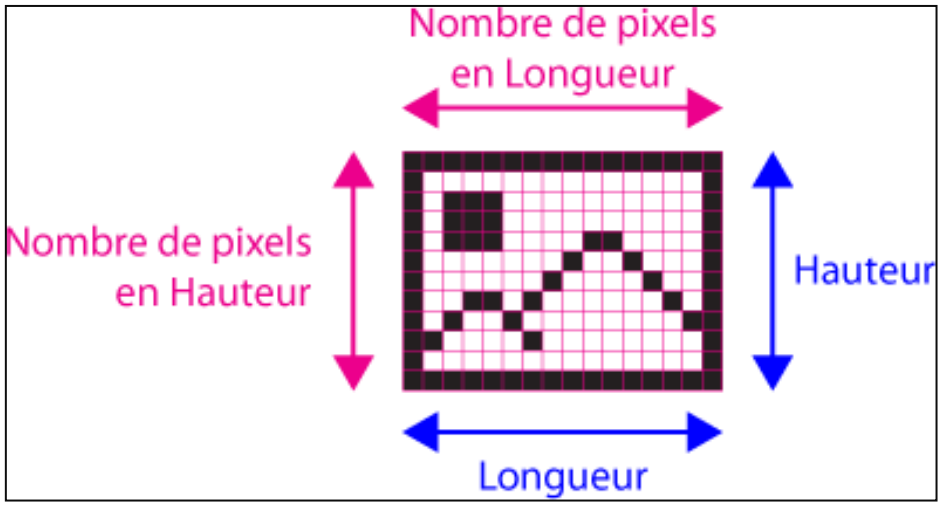


Figure 2.2 : Distribution des pixels par lignes et colonnes .

2.4 La définition

La définition est le nombre de pixels qui composent l'image.

Définition = (Nombre de pixel en Longueur) x (Nombre de pixel en (II.1)

2.5 La taille

La taille correspond à la largeur et à la hauteur de l'image lors de l'impression. Par conséquent, il est exprimé en centimètres ou en pouces. [12]

Taille de l'image = (Définition sur la Longueur / Résolution) x (Définition sur la Hauteur / Résolution) .....(II.2)

2.6 La résolution

La résolution est ce qui lie la définition à la taille. C'est le nombre de pixels sur une zone donnée. Par convention, cette valeur est exprimée en dpi (dots per inch ou pixels) et traduite en anglais par dpi (dots per inch) [12]

Résolution=définition /longueur. .....(II.3)

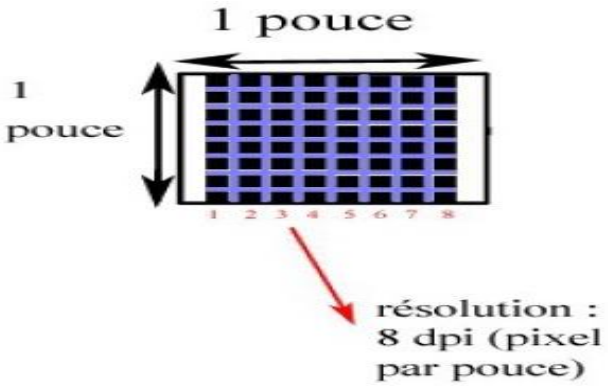


figure 2.3 : Les mesures en pouce.[13]

1 pouce = 2.54 centimètres.

3 Les différents types d'image :

3.1 Image Matricielle (bitmap) :

Une image Matricielle ou image bitmap (en anglais) est une image numérique dans un format de données, composée d'un ensemble de pixels ou de points colorés, généralement rectangulaires, et pouvant être affichée sur un écran d'ordinateur ou autre périphérique d'affichage RVB. Les principaux formats matriciels sont : TIFF, BMP, GIF, PCX, JPEG. [11]

3.2 Image Vectorielle :

Une image vectorielle est une image numérique composée de plusieurs objets géométriques distincts (lignes, polygones, arcs), créée sur la base d'équations mathématiques. Chaque forme dépend de plusieurs paramètres (hauteur, largeur, rayon) affectés au vecteur.

Les images vectorielles sont généralement à l'opposé des images matricielles ou "bitmap", qui sont des ensembles de points numériques, généralement appelés pixels rectangulaires.[11]

Figure 2.4 : Différence entre image vectorielle et image matricielle[11]

4 Les différents formats d'images :

Il existe deux principaux formats d'images numériques qui sont les images vectorielles et les images matricielles ou dite images Bitmap.

4.1 Les formats d'image matriciels

4.1.1 JPEG :

Le terme JPEG est un acronyme utilisé pour le Joint Photographie Experts Group. Il représente un enregistrement numérique et un format de compression. Ce format est utilisé pour les images réelles complexes (domaine spatial et temporel) ISO, CCITT, JFIF, et caractériser par :

- Des tons continus.
- Une profondeur variée.
- Pas de transparence.
- Un espace colorimétrique libre : RGB, YUV, YCrCb.
- Un facteur de qualité : 10% < FQ < 100%.
- Une technique de compression destructive (avec pertes) : quantification scalaire dans le domaine -spectral.
- La souplesse. [14]

4.1.2 TIFF :

Le format **TIFF** est un format de fichier matriciel. Similaire au JPeg, ce fichier permet de stocker des images de tailles plus importantes sans perte de qualité. Il est optimal pour l'imprimé (publication, dépliant, grand format, etc.), mais pas pour le Web à cause de son poids élevé.[14]

4.1.3 GIF :

Le Graphics interchange Format, est un format d'image numérique couramment utilisé sur la Toile.

Le format GIF est une image matricielle. Ce format est limité à 256 couleurs et est surtout utilisé pour la diffusion d'images sur le Web. Il est optimisé pour du texte et des images graphiques. Contrairement au format JPeg, le GIF réduit considérablement le poids du fichier sans perte de qualité de l'image. Il est considéré comme un format universel.[14]

4.1.4 PNG :

Le format PNG (Portable Network Graphics ou format Ping) est un format de fichier graphique bitmap (raster) permet de stocker des images en noir et blanc.

-libre de droit, Basé sur l'algorithme LZ77.

- codage format brut possible.

- couleurs réelles ou indexées, transparence -> 32 bits.

- mode de transmission : entrelacé.

- codage prédictif. possible .[14]

4.2 Les formats vectoriels :

Nom du format	Avantages	inconvénients	Cas d'utilisation
AI	Générés par tous les logiciels de design vectoriel le plus populaire à ce jour , Adobe illustrateur	Format propriétaire.	Utilisé pour création design et pour une impression de haut qualité , de logo….
PS/EPS (**P**ost**s**cript / **E**ncapsulated **P**ost**s**cript)	Prédécesseur de PDF . très utilisé dans le milieu professionnel . ce forma conserver les attributs vectoriel d'un fichier .	N'a d'intérêt que dans le cadre d'une impression. Fichier très lourd.	A moins d'avoir des habitudes spécifique avec son imprimeur. EPS n'utilise pas.
SVG (**S**calable **V**ector **G**raphics)	Il peur étre édite par un éditeur de texte basique car c'est un XML . Il peur stylé grace à CSS.	Encore très peu reconnu, car peu d'outils disponibles et manque d'implémentation au sein de navigateurs (besoin d'un plugin).	Le SVG est utilisé pour créer des icone pour les site web.
PDF (**P**ortable **D**ocument **F**ormat)	Affiche les documents	-Possible de modifier les fichier PDF gratuitement. -facile de modifier les fichier dans des formats autre que le PDF .	Le plus couramment utilisé par les imprimeurs, et pour les outils de communication visuelle .
PICT (**Pict**ure)	Format par défaut de Mac OS, donc encore utilisé.	Disponible uniquement sur la plateforme d'Apple	N'a plus grand intérêt face aux autres formats existants.

Tableau 1.1 : Les formats vectoriels[15]

5 Les différents modes de couleurs des images

5.1 Mode binaire (noir et blanc) :

Le mode binaire (mode Bitmap) utilise une des deux valeurs chromatiques (noir ou blanc) pour représenter les pixels dans une image. Chaque pixel de l'image peut contenir une valeur égale à 0 (noir) ou à 1 (blanc)

Codage en 1 bit par pixel : $\Longrightarrow 21 = 2$ possibilités : (0,1)

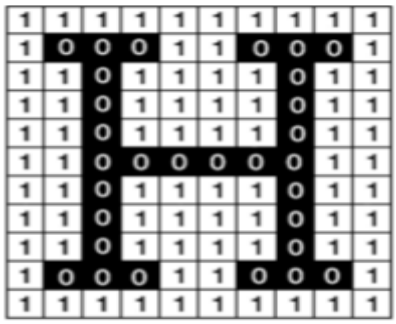


Figure 2.5 : Codage binaire (0,1)

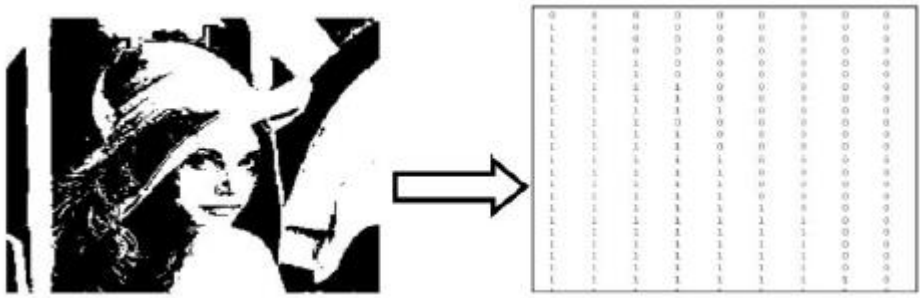


Figure 2.6 : Image Noir et blanc

5.2 Mode niveau de gris :

Le codage dit en niveaux de gris permet d'obtenir plus de nuances que le simple noir et blanc. Une image en niveaux de gris nécessite pour son codage 8 bits (correspondant à 1 octet), les valeurs de niveau de gris étant comprises entre 0 (pour le noir) et 255 (Pour le blanc). [21]

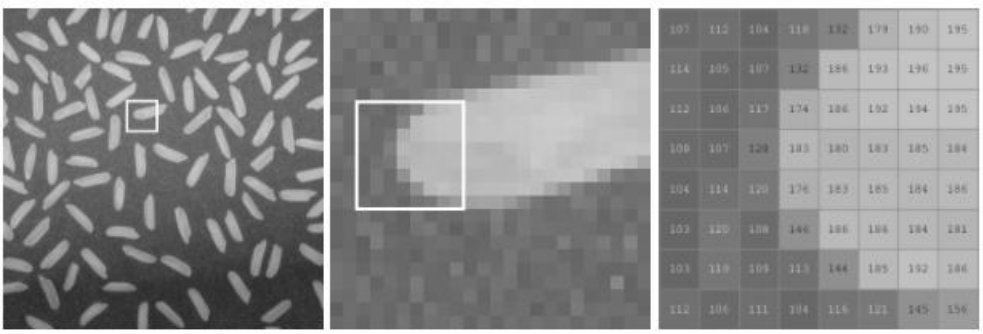


Figure 2.7: image de niveau de gris

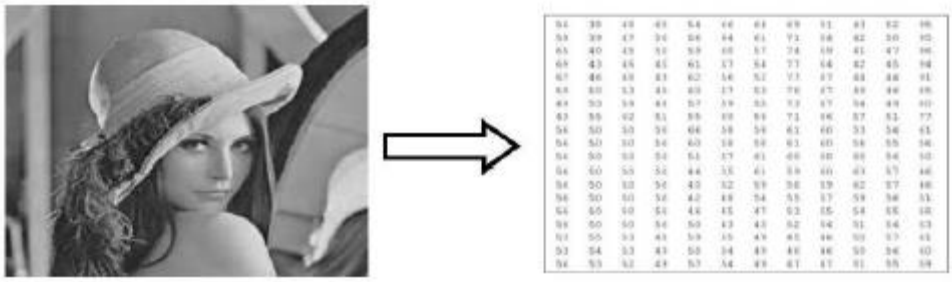


Figure 2.8 : Image niveau de gris

5.3 Mode couleur (RVB) :

Ce mode est basé sur un mélange additif (combinaison de rayons lumineux) de trois couleurs primaires (Rouge, Vert, Bleu). Avec un codage en RVB 8 bits par couche :

Chaque couche utilise 8bits (1 octet), soit 256 nuances possibles : 8 bits pour le Rouge, 8 bit pour le Vert et 8 bits pour le Bleu.

Donc utilisation de 3 x 8 bits = 24 bits utilisées au total.

=> 256 x 256 x 256 = 224 = 16,7milions possibles !

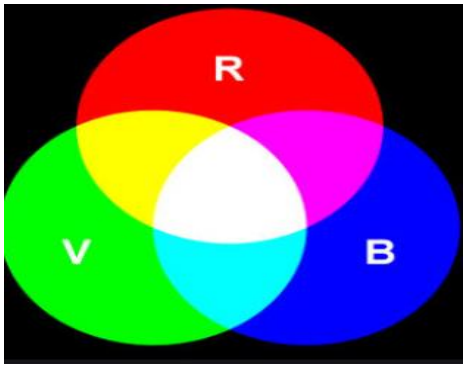


Figure 2.9: les couleur de image RVB

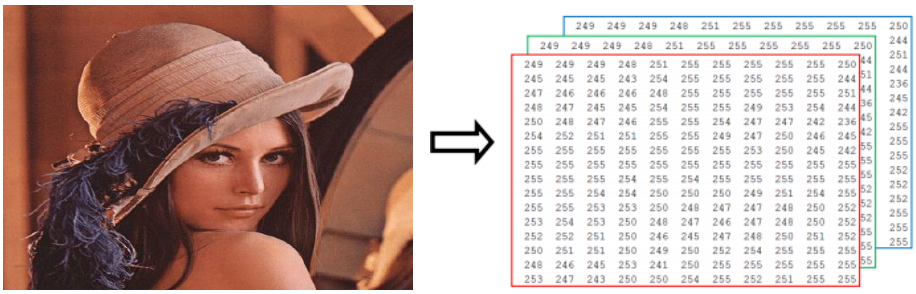


Figure 2.10 : Image RVB

6 Imagerie médicale :

6.1 Définition :

L'imagerie médicale regroupe l'ensemble des moyens physiques ou des techniques utilises par la médecine pour le diagnostic mais aussi pour le traitement d'un grand nombre de pathologies pour visualiser les cellules d'un organisme (corps humain)[16]

6.2 Types d'imagerie médicale :

Parmi les méthodes d'imagerie médicales les plus couramment employées en médecine, on peut citer d'une part les méthodes tomographiques basées soit sur les rayons X (radiologie conventionnelle, tomodensitomètre ou CT-scan, angiographie,...) soit sur la résonance magnétique (IRM), les méthodes échographiques utilisant les ultra-sons, et enfin les méthodes optiques utilisant les rayons lumineux [17]

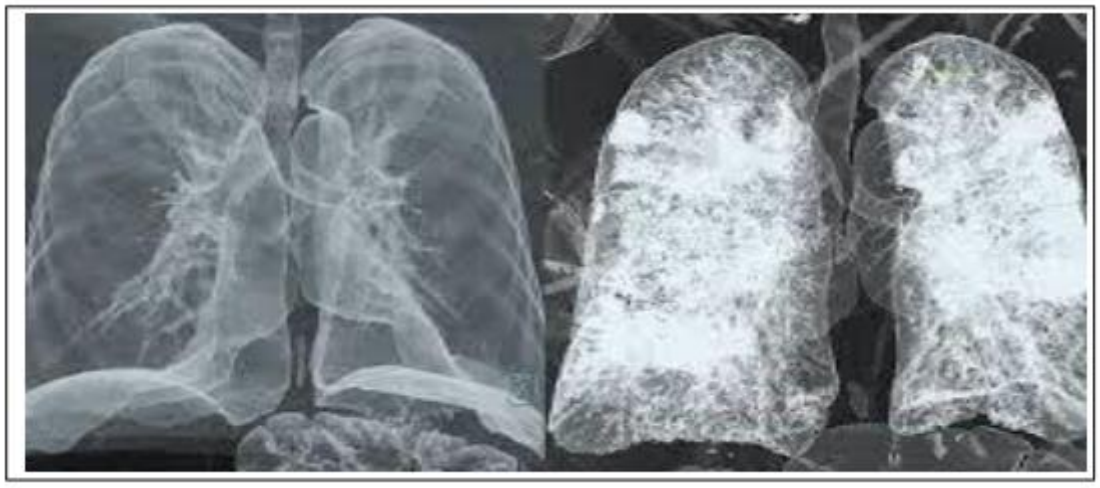


Figure 2.11 : Image médicale

6.2.1 Les champs magnétiques :

L'imagerie par résonance magnétique (IRM) permet de visualiser la structure anatomique de tout volume du corps, en particulier des tissus mous tels que le cerveau, la moelle épinière, les viscères, les muscles ou les tendons. L'IRM permet aussi de suivre l'activité d'un organe tel le cerveau, à travers l'afflux de sang l'oxygène dans certaines de ses zones (IRM fonctionnelle**).** [16]

Figure 2.12 : Scanner D'IRM

6.2.2 La radioactivité :

La radioactivité utilise les rayons X. Passant à travers une certaine partie du corps, ils impressionnent un film radiographique, plus ou moins noirci en fonction de l'organe traversé. La radio ressemble ainsi à une ombre chinoise, ou les os apparaissent en blanc et les structures moins denses (comme les poumons) en noir [18].

Figure 2.13: Un échantillon d'images radiographiques

6.2.3 Les rayons X :

Les rayons X (RX) sont des ondes électromagnétiques de même nature que les ondes de lumière mais plus énergétiques. Ils ont la propriété d'être atténués par toutes sortes de

substances y compris les liquides et les gaz. Ils peuvent préter le corps humain, ou seront plus ou moins atténués suivant la densité des structures traversées .[16]

Différents types d'examens utilisent les rayons X :

- Radiographie.
- Scanner X .
- Scanner DEXA

Figure 2.14: Le Rayon X dans Image médicale

6.2.4 L'échographie :

L'échographie est une technique d'exploration de l'intérieur du corps basée sur les ultra- sons. Une sonde envoie un faisceau d'ultrasons dans la zone du corps à explorer. Selon la nature des tissus, ces ondes sonores sont réfléchies avec plus ou moins de puissance. Le traitement de ces échos permet une visualisation des organes observés [18].

Figure 2.15: Image L'échographie.

7 Chiffrement du chaos et chiffrement des images:

7.1 Définition :

Il n'y a pas de définition précise du chaos, Il faut reconnaître la notion de "phénomènes imprévisibles et instables". Ces systèmes sont donc déterministes bien qu'imprévisibles. La théorie du chaos a été vue par Jacques Hadamard et Henri Poincaré au début du XXe siècle, a été définie à partir des années1960 par de nombreux scientifiques.

Nous appelons cela un phénomène chaotique complexe, qui dépend de plusieurs paramètres et se caractérise par une extrême sensibilité aux conditions initiales.

7.2 Les conditions d'un système chaotique:

La trajectoire d'un système dynamique à partir d'un vecteur de conditions initiales X_0 et en passant par un régime transitoire, arrive à une région permanente de l'espace des phases. Ce comportement asymptotique obtenu pour t (en continu) ou k (discret) qui tendent vers l'infini est une des caractéristiques essentielles à étudier pour tout système dynamique.

- Pour les systèmes linéaires la solution asymptotique est unique et ne dépend pas des conditions initiales.

- La non linéarité engendre une plus grande variété de régimes permanents, parmi lesquels on trouve, par ordre de complexité : points d'équilibre, solutions périodiques, solutions quasi-périodiques et chaos, respectivement . Ces comportements peuvent être illustrés dans un exemple de systèmes dynamiques unidimensionnels discrets, connu dans la théorie des systèmes non linéaires sous le nom de la carte logistique, qui est une fonction itérative définie par la fonction :

$$Xn + 1 = rXn(1 - Xn)$$

Le paramètre r défini dans [0,4] , est responsable du type de comportement de cette dynamique.

La figure 2.16 représente le comportement du système en fonction du paramètre r .

- . Ainsi on trouve pour r = 2, la tendance de la suite logistique vers un point d'équilibre .
- r = 3.2 la suite logistique oscille entre deux valeurs
- r = 3.5 la suite logistique oscille entre plus de deux valeurs
- r = 3.9 la suite logistique a un comportement qui semble aléatoire: c'est le comportement chaotique.

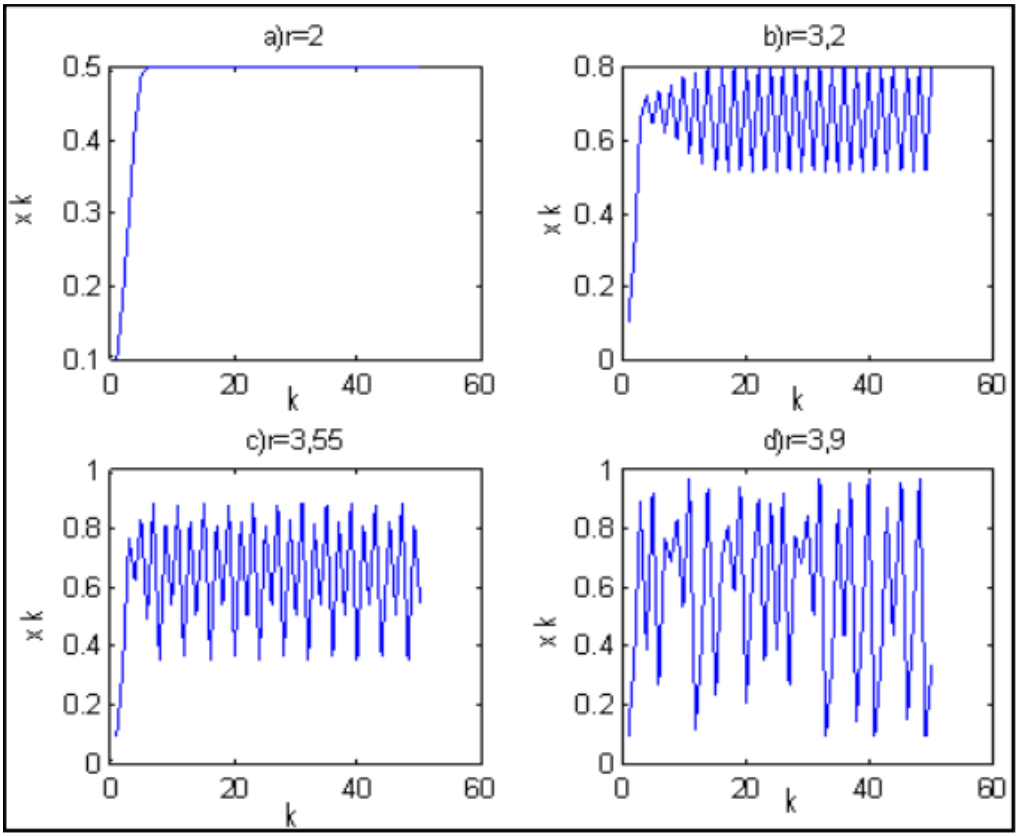


Figure 2.16 : Séquences générées par la fonction logistique pour X_0= 0.1 pour : a) r = 2 ;b) r = 3.2 ; c) r = 3.55 ; d) r = 3.9

7.2.1 La carte chaotique logistique simple :

La carte chaotique est une carte polynôme de l'ordre 2, souvent cité comme un exemple de la façon dont un comportement chaotique il peut résulter d'une simple équation dynamique non-linéaire .La carte a été rendu populaire en 1972 de biologiste Robert May

$$n + 1 = r\,xn(1 - xn) \quad avec\ xn\ £\ [0,1] \qquad \text{.....(II.4)}$$

La figure suivante présente l'attracteur de l'équation logistique qui justifie le choix du paramètre μ = 3.9999 [29].

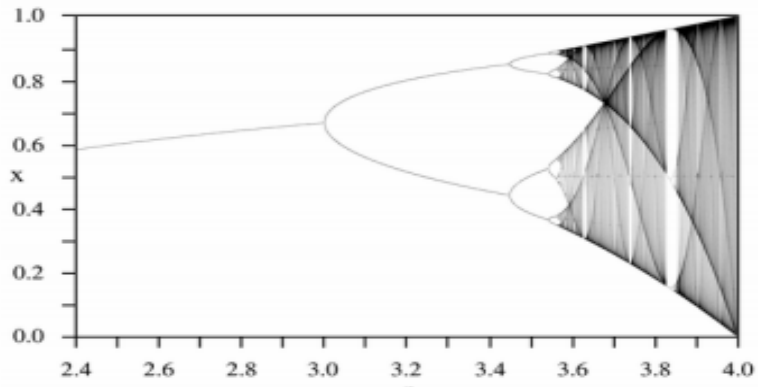


Figure 2.17 : Attracteur de l'équation logistique.

La figure 2.17 représente un diagramme dit de bifurcation de Feigenbaum qui décrit la transition de la suite logistique vers le chaos.

La représentation on a choisi le temps discret k = 0,1,2...100 et le nombre de valeurs de r égal à 500 définies dans l'intervalle [0,4] . le diagramme de bifurcation de Feigenbaum que :

- 1< r < 3, le système possède un point fixe attractif qui devient instable. lorsque r = 3 comme il est représenté sur la figure (2.17) .
- 3 ≤ r < 3.37 3 le système se comporte périodiquement, de période m 2 où m est un entier qui tend vers l'infini lorsque r tend vers 3.57, comme il est représenté sur la figure (2.17).
- 3.57 ≤ r < 4 le système présente une succession de bifurcations (doublement de période), alors on aura un comportement chaotique, comme il est représenté sur la figure (2.17) .

un système dynamique chaotique est caractérisé par un sensible aux conditions initiales et un aspect semblable à l'aléatoire. [25]

7.2.2 La carte chaotique sine :

Il existe quelques différences dans la deuxième carte (expression (2)), l'exposant de Lyapounov2 est d'environ 50% plus petit. Les bifurcations par doublement de période survenues plus tôt, et les fenêtres périodiques sont plus larges par rapport à la carte logistique.

7.2.3 la carte chaotique standard :

(expression (3)) est connue sous le nom de carte standard (également connue sous le nom de carte de Chirikov-Taylor ou carte standard de Chirikov), d'où la constante K mesure l'intensité des coups. et pour K = 18.9, le

chaos s'installe d'où elle conduit a une suite chaotique .[28]

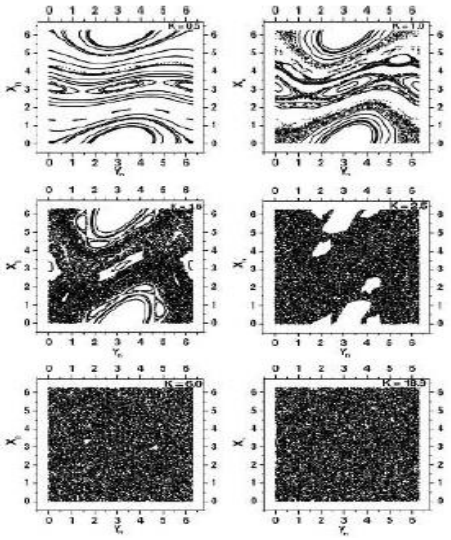


Figure 2.18 : L'espace de phase de la carte standard / K = 0.5, 1.0, 1.5, 2.5, 6.0 et 18.9 [11]

7.2.4 La carte d'Arnold :

La carte Arnold découverte par mathématicien russe Vladimir I. c'est une démonstration et une illustration simple est élégante de certain des principe de la théorie de chaos , une évolution apparemment aléatoire d'un système

7.2.5 Tchebychev :

En mathématiques, un polynôme de Tchebychev est un terme de l'une des deux suites de polynômes orthogonaux particulières reliées à la formule de Moivre. Les polynômes de Tchebychev sont nommés ainsi en l'honneur du mathématicien russe Pafnouti Lvovitch Tchebychev.

Il existe deux suites de polynômes de Tchebychev, l'une nommée polynômes de Tchebychev de première espèce et notée Tn et l'autre nommée polynômes de Tchebychev de seconde espèce et notée Un

Ces deux suites peuvent être définies par la relation de récurrence :

$\forall n \in N \quad Pn + 2 = 2X\ Pn + 1 - Pn$

Et les deux premiers termes :

$$T0 = 1\ , T1 = X \quad Pour\ la\ suite\ T$$

$$U0 = 1\ , U1 = 2X\ pour\ la\ suite\ U$$

7.3 Relation entre le chaos et les crypto-systèmes :

Tout d'abord, notez qu'il y a une forte ressemblance entre les crypto-systèmes symétriques à chiffrement par bloc et les systèmes chaotiques. En ce qui concerne Sur les propriétés des systèmes chaotiques. Veuillez noter que le système chaotique se compose de quelques fonctions de base f, qui sont itérées à l'ensemble X. Le fonctionnement de ce système comprend le respect des conditions suivantes :

- Soit un mélangeur Cela signifie que l'ensemble X doit être mélangé au hasard par la répétition de l'action de f.
- soit sensible à l'état initial de telle sorte qu'une légère modification dans les états initiaux engendra des états complètement différents.
- soit sensible aux certains paramètres de contrôle et un léger changement dans ces paramètres causera un changement dans les propriétés de la carte chaotique.

En comparant entres les particularités d'un crypto-système et les caractéristiques d'un système chaotique, De toute évidence, le cryptage a une ressemblance frappante avec le

théorème chaos. Si nous considérons que les données nettes correspondent à un état initial, la clef correspond à l'ensemble des paramètres, et la fonction de cryptage correspond à la fonction de base f.[30]

8 Critère d'évaluation

8.1 L'histogramme :

L'histogramme est la représentation graphique des pixels qui composent une image. Ces pixels sont répartis en fonction de leur luminosité. Dans un contexte de chiffrement d'image, l'histogramme de l'image chiffrée doit être uniforme pour qu'un adversaire ne puisse extraire aucune information à partir de cet histogramme.

Les figures (2.16) et (2.17) présentent l'histogramme d'une image en clair et l'histogramme d'une image après le chiffrement.

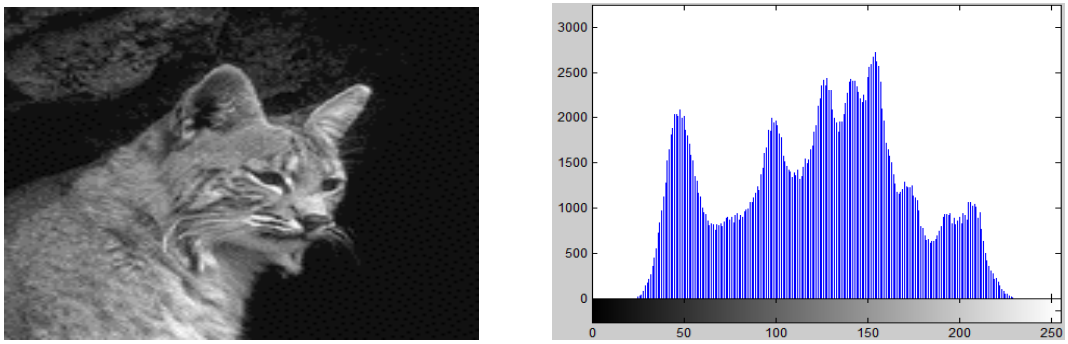


Figure 2.20 : Histogramme d'une image de niveau de gris

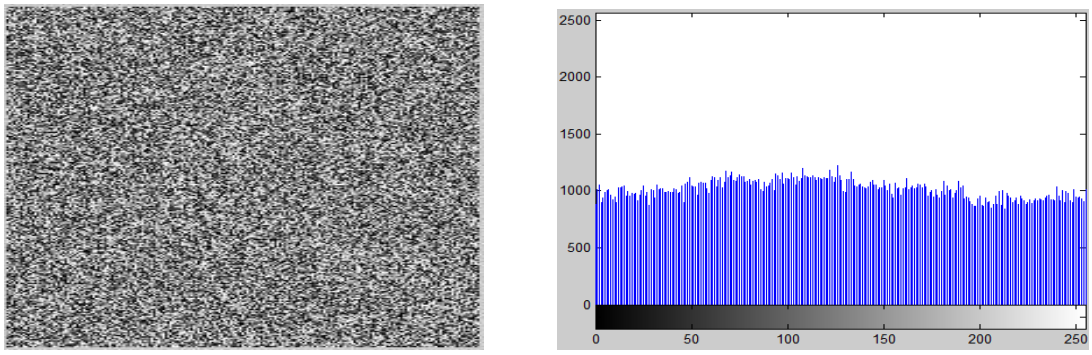


Figure 2.21 : Histogramme d'une image Crypté

8.2 La corrélation :

La corrélation d'images est une technique expérimentale permettant de comparer deux images pour estimer les déplacements des pixels d'une image par rapport à une autre image de référence. Les pixels adjacents d'une image standard ont une forte corrélation. Un bon schéma de cryptage d'image doit supprimer une telle corrélation afin d'assurer la sécurité contre l'analyse statistique [23],

Les coefficients de corrélation de chaque paire ont été calculées en utilisant les formules suivantes :

$$r = \frac{\mathrm{cov(x,y)}}{\sqrt{\mathrm{D(x)}\sqrt{D(y)}}} \quad \textbf{.....(II.5)}$$

Ou :

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

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} Xi \; D(x) = \sum_{i=1}^{N} \big(Xi - E(x)\big)^2$$

Tel que :

r : la corrélation.

cov : la covariance.

E : l'espérance mathématique.

D : la variance.

x, y : les valeurs des pixels des images.

8.3 L'entropie :

Quantité d'information moyenne apportée par chaque symbole de la source. L'entropie H (m) de toute donnée peut être calculée comme :

$$\mathbf{H(m) = -\sum_{i=0}^{2n-1} \mathcal{P}i \; \log_2(\mathcal{P}i)} \quad \textbf{.....(II.6)}$$

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

8.4 Les tests différentiels :

Le NPCR : mesure le pourcentage du nombre de pixels différents par rapport au nombre total de pixels entre deux images.

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{i=0}^{N-1} D(i,j)}{M \times N} \times 100 \quad \textbf{.....(II.7)}$$

l'UACI : mesure la moyenne de différence d'intensité entre les deux images.

$$UACI = \frac{1}{M \times N}\sum_{i=0}^{M-1}\sum_{i=0}^{N-1}\frac{\mathrm{I1(i,j)} - I2(i,j)}{255} \times 100 \quad \textbf{.....(II.8)}$$

Où M et N représentent respectivement la largeur et la hauteur d'une image.
I1(i,j) et I2(i,j) sont les valeurs des pixels à la position (i,j) des deux images cryptées dont les images originales ne diffèrent que d'un seul pixel. I1 et I2 sont parfois utilisées comme l'image originale et l'image cryptée.
D(i,j) est une matrice de la même taille que I1 et I2 tel que :

$$D(i,j) = f(x) = \begin{cases} 1, & sI\ I1(i,j) \neq I2(i,j) \\ 0, & sinon \end{cases}$$

Un score NPCR/UACI élevé se traduit, généralement, par une forte résistance aux attaques différentielles.

8.5 espace de clés:

La taille de l'espace de clé est le nombre de paires de clés de cryptage/décryptage qui sont disponibles dans le système de chiffrement. [24] elle est nécessaire pour assurer la sécurité contre l'attaque par force brute.

8.6 Sensibilité de la clé :

La sensibilité à la clé est caractérisée par un petit changement dans la clé qui donne une naissance à des nouvelles données chiffrées complètement différentes.

9 Etat de Art :

- Tiegang Gao et al [31], ont suggérés un nouveau schéma de cryptage d'image. Le cryptage proposé ici se compose de deux processus, premièrement, ils permutent les positions de pixels de l'image d'une façon aléatoire en fonction d'une matrice globale générée en utilisant la carte logistique, puis ils cryptent l'image associée en utilisant l'hyper-chaos [11].
- Safwan El Assad et al [32], proposent une nouvelle méthode de crypto-système simple et robuste basée sur le chaos. Le crypto-système utilise une couche de diffusion suivie d'une couche de permutation de bits, au lieu de permutation d'octets, pour changer les positions des pixels de l'image .La méthode montrant un bon exemple de cadre pour l'analyse de la sécurité des crypto systèmes chaotiques au niveau d'octet.
- Methaq Talib Gaata et al [33] proposent une nouvelle méthode de chiffrement basée sur la carte logistique CLM et l'algorithme de cryptage RC4 (Rivest Cipher 4). Tous d'abord, une clé secrète et un algorithme CLM ont été utilisé pour produire un tableau unidimensionnel. Ensuite, l'algorithme RC4 est utiliser (en s'appuyant sur le contenu du tableau crée par CLM) pour changer la valeur de chaque pixel et créer une image chiffrée diffèrent de l'image original. Cette méthode proposée devrait être utile en temps réel applications de cryptage et de transmission d'images [33]

10 Conclusion :

Dans la première partie de ce chapitre, nous avons introduire les concepts de base de l'imagerie numériques (types, formats) ; ainsi que les différentes modalités de l'imagerie médicales. Dans la deuxième partie, nous avons décrit les techniques de cryptage basé sur les systèmes chaotique, dont nous allons par la suite dans le dernier chapitre présenté notre méthode et résultats.

CHAPITRE 3

Résultats expérimentaux

1 Introduction

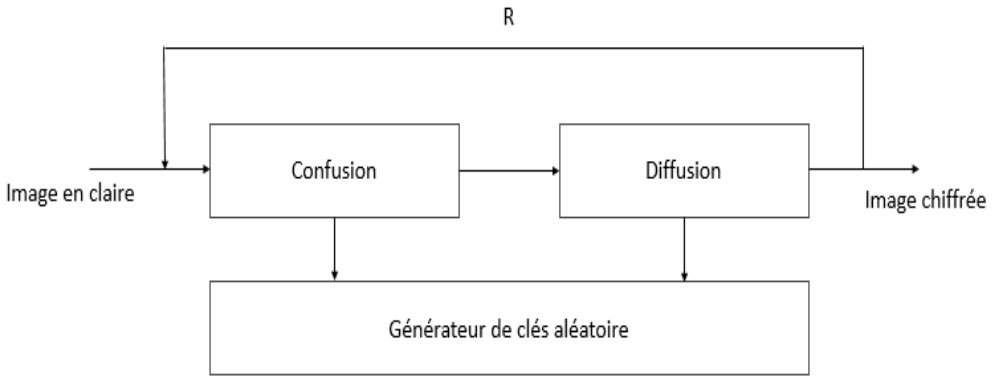
Les chercheurs de cryptographie ont été proposés plusieurs techniques de chiffrement d'images médicales . Parmi eux il y a des algorithmes qui basées sur les théories comme la théorie de chaos, la permutation .

Dans ce chapitre nous allons présenter notre algorithme de cryptage que nous avons développé. Cet algorithme de chiffrement proposé est basé sur la théorie de Chaos et en basé sur techniques de cryptage la carte chaotique logistique . Les résultats de la simulation montrent l'efficacité et la sécurité de notre système proposé.

2 Les Méthodes utilisées

Le schéma proposé est basé sur l'algorithme Fridrich qui présente la structure de base de la plus par des schémas de chiffrement des images qui se base sur la théorie du chaos. Cette structure est composée de deux couches (confusion et diffusion).

La confusion cherche à établir une permutation aléatoire des positions des pixels en utilisant une carte chaotique. La couche de diffusion pour changer entièrement les valeurs des pixels en utilisant un générateur de clé pseudo aléatoire. Le processus peut être répété plusieurs fois.



Notre crypto-système est composé d'un générateur de clé pseudo-aléatoire et un algorithme de chiffrement à l'aide de la clé générée.

2.1 Générateur de clé :

- Définir les paramètres initiaux de la suite de Tchebychev (P, k) ou

$$k_{(i+1)} = \cos(P * \arccos(k_i)) \text{.....(III.1)}$$

- Convertir k en entier ou (k_1=k*255)
- Convertir k_1 en format binaire puis faire une permutation pour obtenir k_2

Combiner k_1 et k_2 par une relation OU-exclusive (XOR) bit par bit pour obtenir la clé de chiffrement $clé = k_1 \oplus k_2$

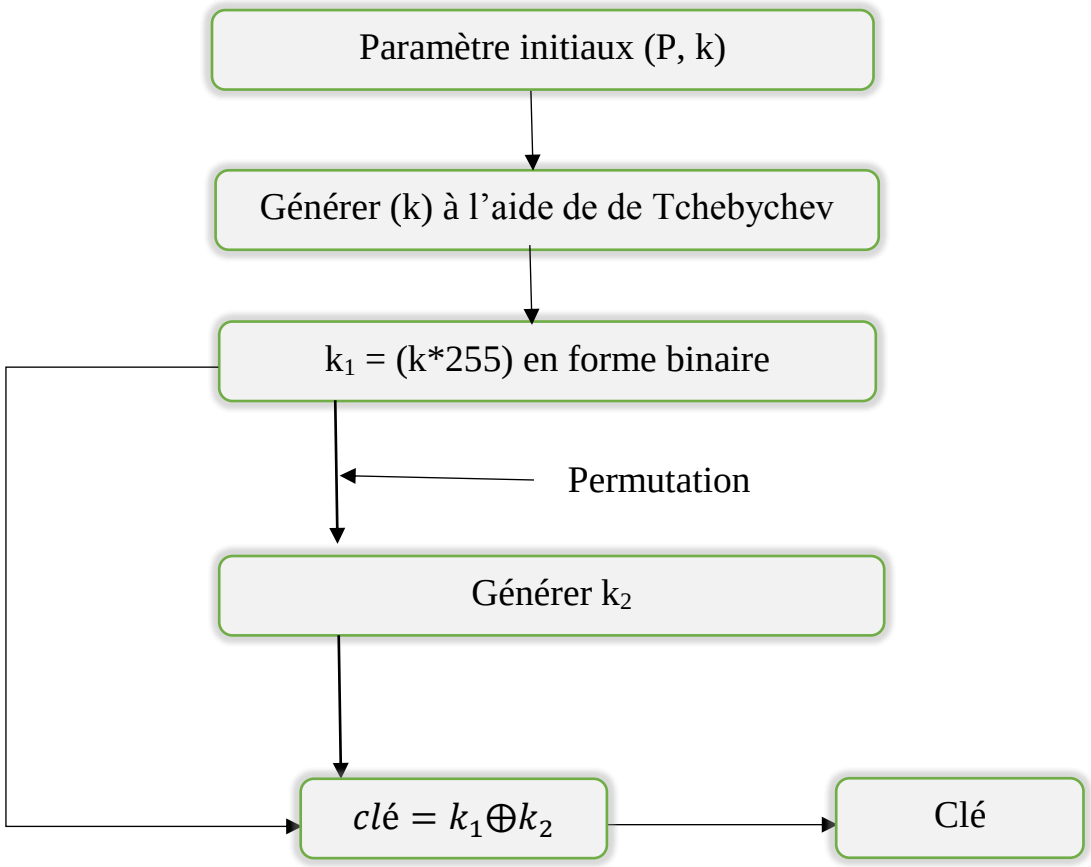


Figure 3.1 : Générateur de clé.

2.2 Chiffre image

2.2.1Etape de confusion :

Dans cette partie nous avons utilisé un générateur pseudo aléatoire basé sur la carte logistique Chaotique qui utilise la formule mathématique suivante :

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

Cette étape permet de changer des positions de l'image claire d'une façon aléatoire.

- Définir les paramètres initiaux de la carte logistique (r, X_0)

  Les paramètres initiaux utilisées dans notre travaille sont :

  r = 3.66 ;

  $0 < X_0 = 0.7 < 1$;

- Générer un flux pseudo aléatoire X utilisant la carte logistique avec la même taille que l'image M.
- Faire une permutation des positions des pixels à l'aide du flux pseudo aléatoire X.

2.2.2Etape de diffusion :

Le but de cette étape est de changé les valeurs des pixels en utilisant la clé générée précédemment en combinant bit par bit l'image claire et la clé avec l'operateur OU-exclusive XOR.

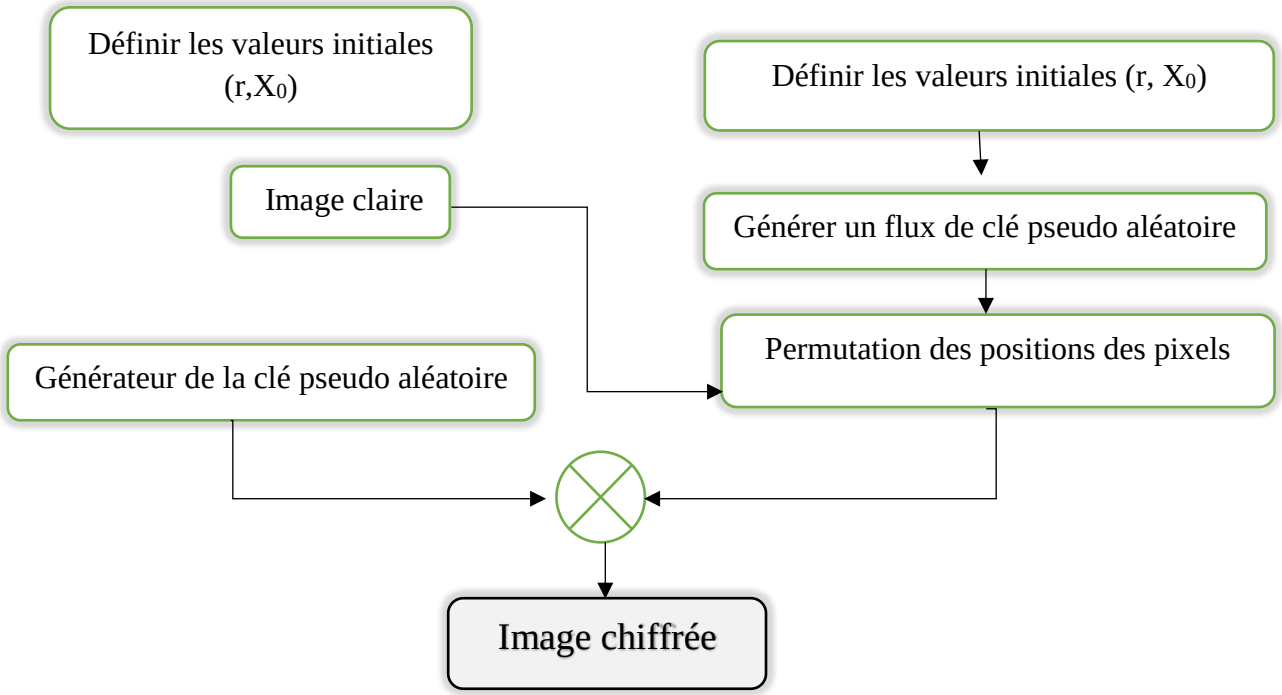


Figure 3.2 : Fonction de cryptage par la carte chaotique logistique

2.3 Déchiffrement image :

Le déchiffrement se compose également des mêmes étapes que le chiffrement mais dans l'ordre inverse.

- Générer la clé pseudo aléatoire avec les mêmes paramètres initiaux (P, k)
- faire une diffusion inverse avec l'operateur XOR

faire une confusion inverse avec le même paramètre initial de la carte logistique

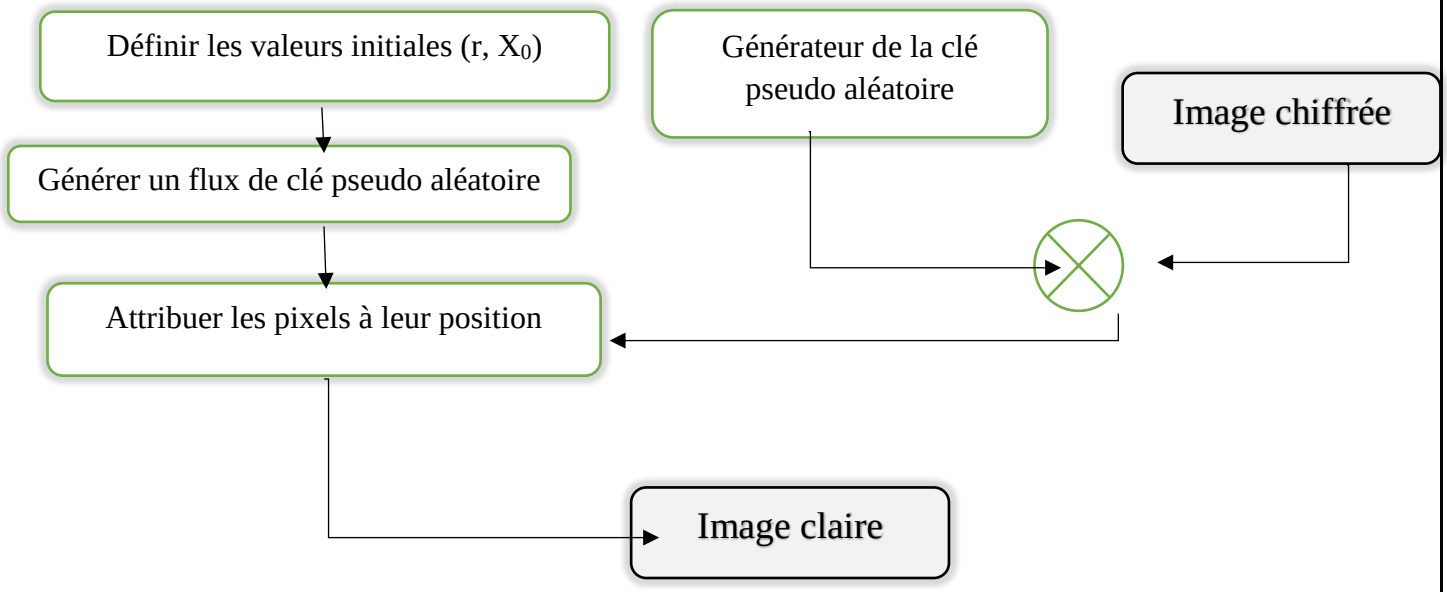


Figure 3.3 : Fonction de déchiffrement par la carte chaotique logistique

3 Résultats expérimentaux

3.1 Les données utilisées :

Les données utilisées dans notre mémoire, est une base de données d'images, Ils sont disponibles gratuitement sur les sites Web suivantes : Les images médicales sont prises à partir d'un site Web Medpic [35], et des images standard en Pinterest de format « BMP , JPG »

3.2 Environnement de développement :

L'application a été créa depuis un PC ACER :

- Mémoire : 4 Go RAM.
- Processeur : Intel ® CoreTM i3-3210M CPU @ 2.50 GHZ (4 CPUs)
- Système d'exploitation : Windows 7 professionnel 32 bits.
- Carte Graphique : Intel® HD Graphique 2Go.

3.3 Langage de programmation :

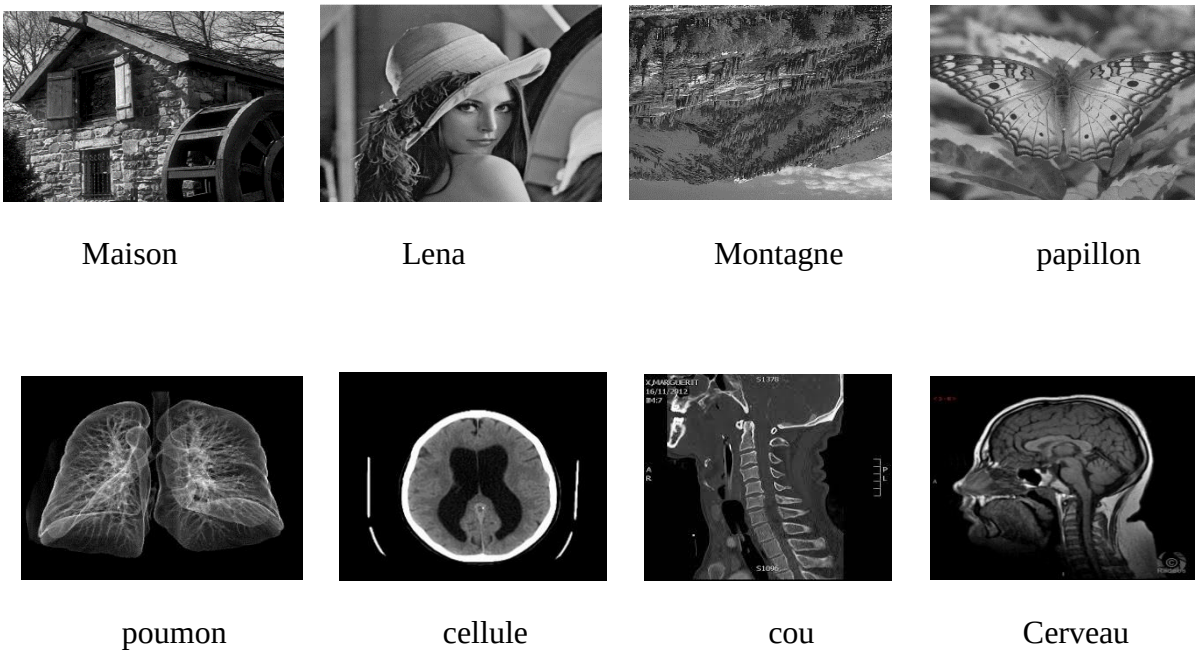
Nous choisissons le langage MATLAB pour développer notre système. Ce choix de langage est motivé par les raisons suivantes :

- MATLAB est organisée, il contient des classes bien conçu et bien reparties .
- MATLAB est connu et donc plus de chance de trouver des développeurs MATLAB.
- MATLAB comprend de nombreuses fonctions, de calcul ou de traitement de données, d'affichage de tracé des courbes.
- Le meilleur pour traite une image

3.4 Image niveau de gris et images médicales :

Des simulations numériques ont été faites pour confirmer les bonnes performances de notre schéma. Les figures au-dessous montrent plusieurs images au niveau de gris de différentes tailles sont cryptées en utilisant la carte chaotique logistique.

Les images originales :

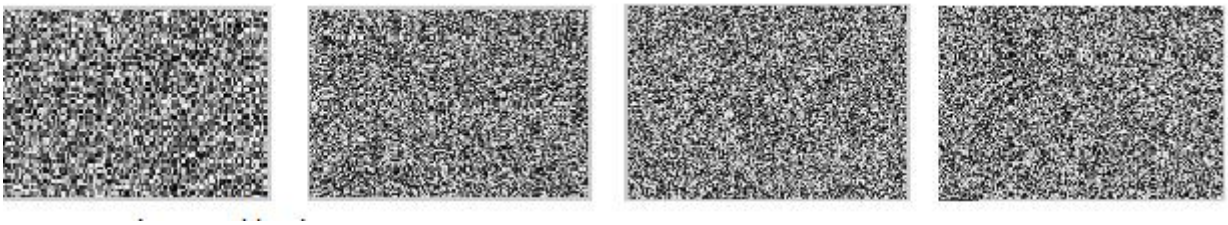


Maison Lena Montagne papillon

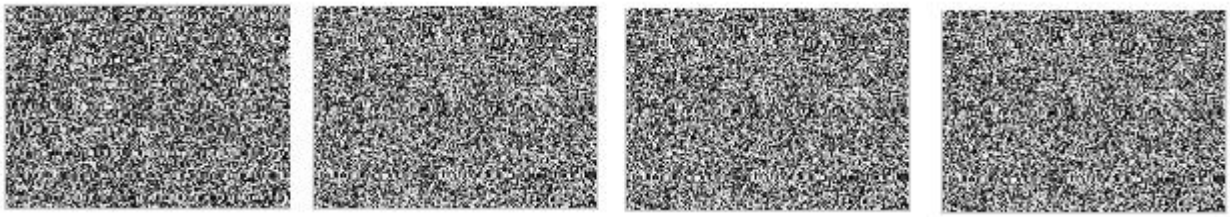
poumon cellule cou Cerveau

Figure 3.4 : les images originales.

Les images cryptés :



Maison Lena Montagne papillon

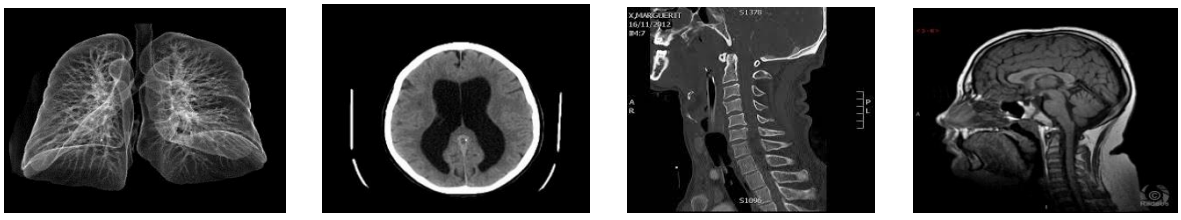


poumon cellule cou Cerveau

Figure 3.5: les images crypté par la carte chaotique.

Les images décryptées :

Maison Lena Montagne papillon



poumon cellule cou Cerveau

Figure 3.6 : les images décryptées par la carte chaotique

4 Critères d'évaluation :

Un bon système de cryptage doit être protégé de toutes les attaques possibles, des simulations numériques avec différents mesures ont donc été effectuées pour montrer la sécurité et l'efficacité des algorithmes utilisés. Plus important encore, tels que : espace clé, histogramme, entropie, corrélation entre pixels adjacents.

4.1 L'espace de clé :

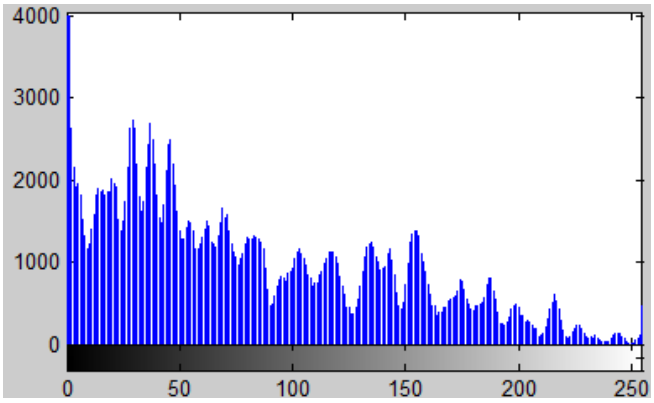
Un bon algorithme de chiffrement doit être sensible aux clés de chiffrement et l'espaceclé doit être suffisamment grand et plus longue que la taille de l'image pour empêcher les attaques .Dans notre travail , la taille de clé utilisé est $n \times m$ (la même taille d'image originale) et comme chaque élément les nombres aléatoires codé sur 8bits donc l'espace de la clé est :

$$2^{8\times n \times m}.$$

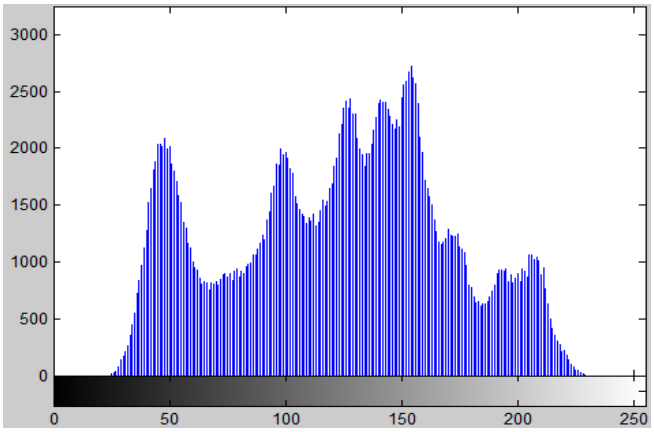
4.2 la carte chaotique logistique

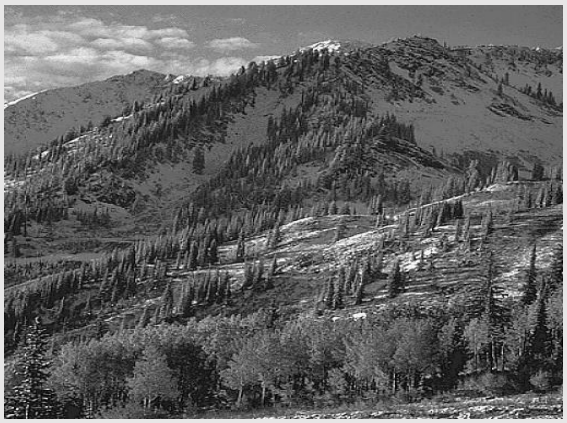
Huit images de teste ont été utilisées pour l'analyse : «Maison ,Lena ,Montagne,Pappilon ,Poumon,Cellule , Cou, Cerveau ».

4.2.1 Histogramme des image original :

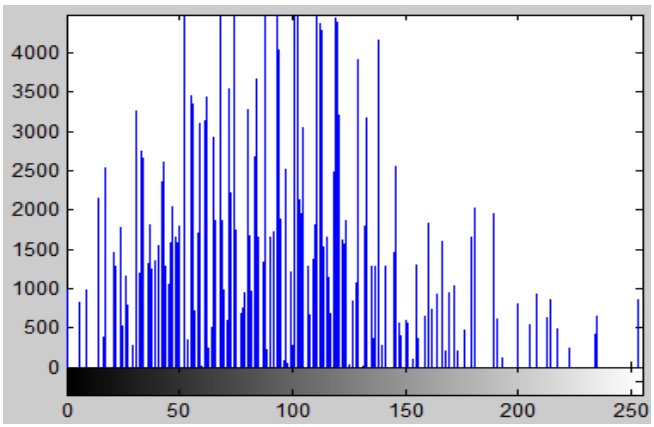
Image Original	Histogramme
 Maison	

Lena

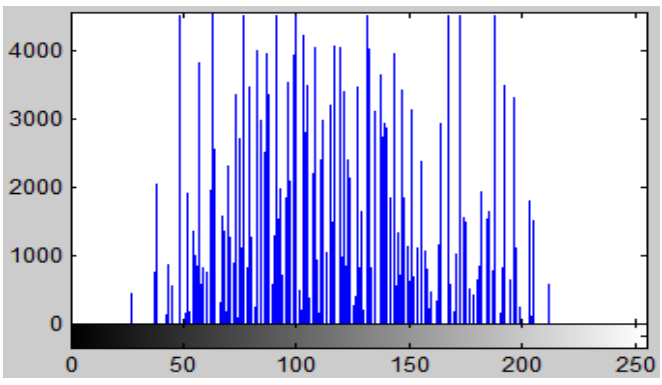




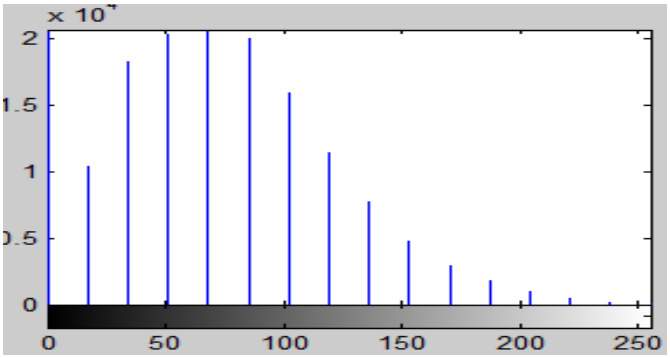
Montagne



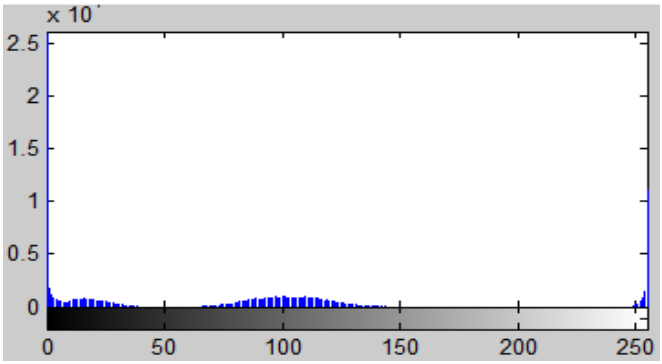
Papillon



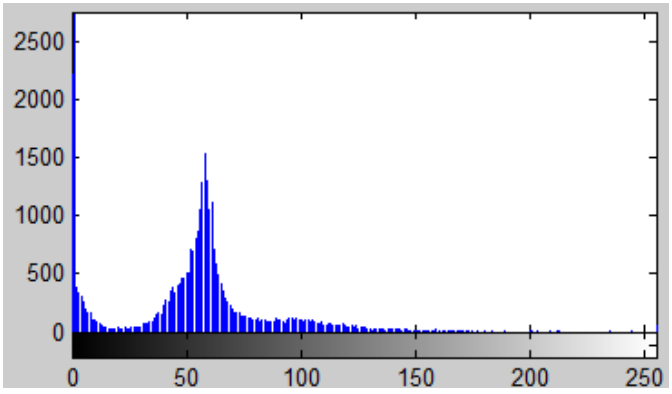
poumon



cellule



Cou



Cerveau

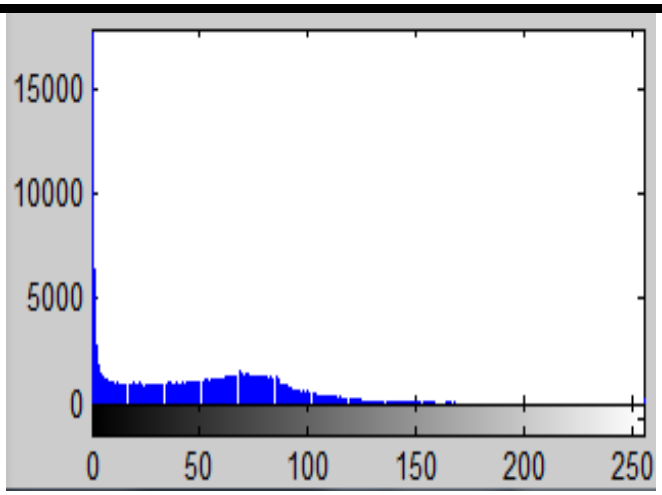
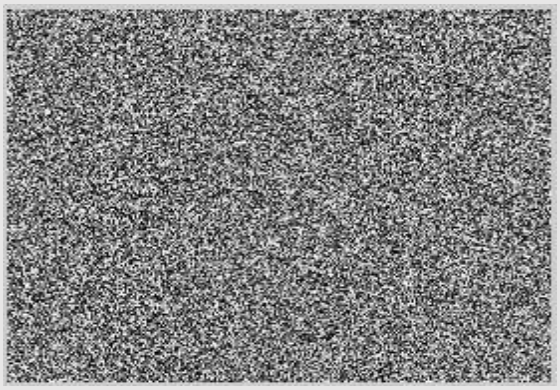
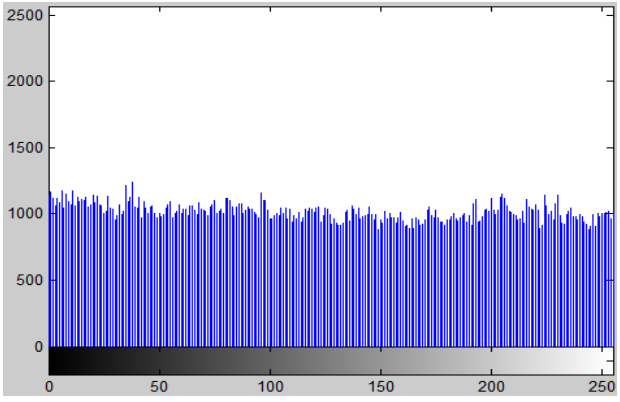
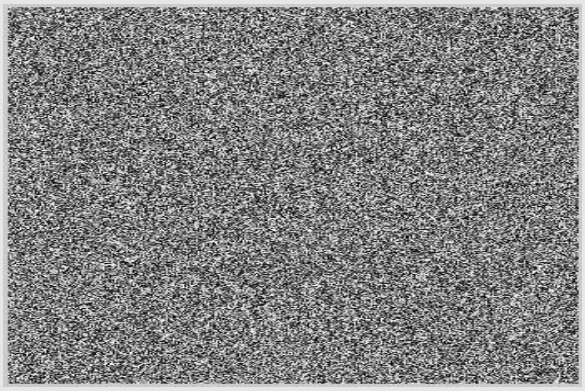
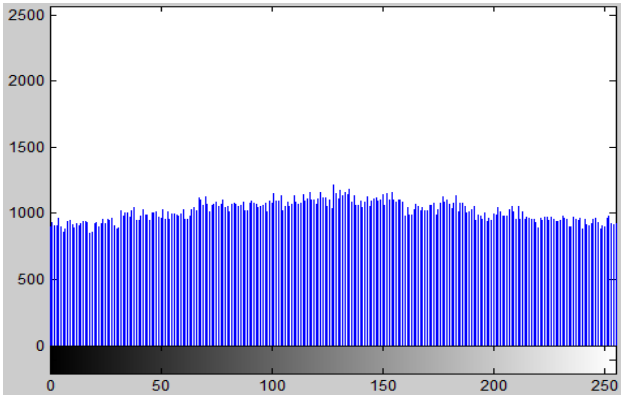
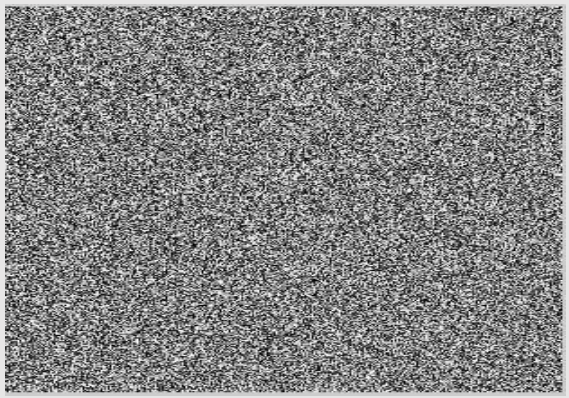
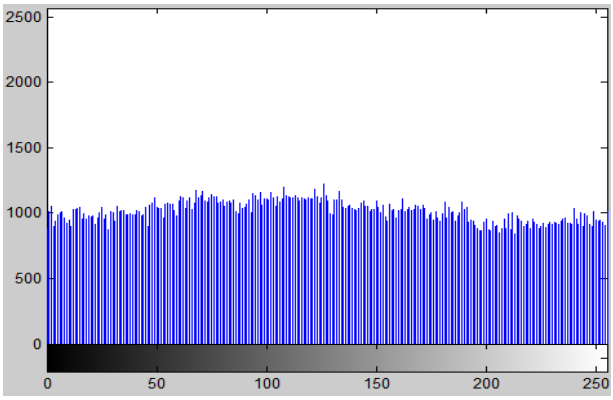
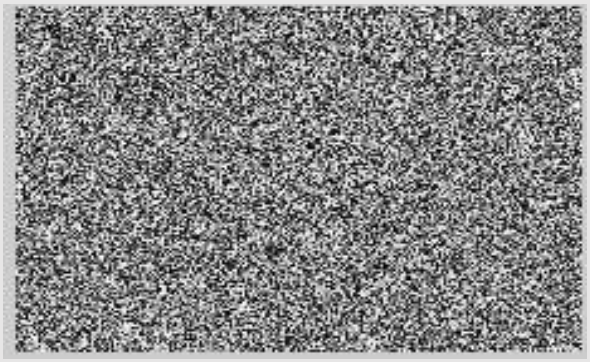
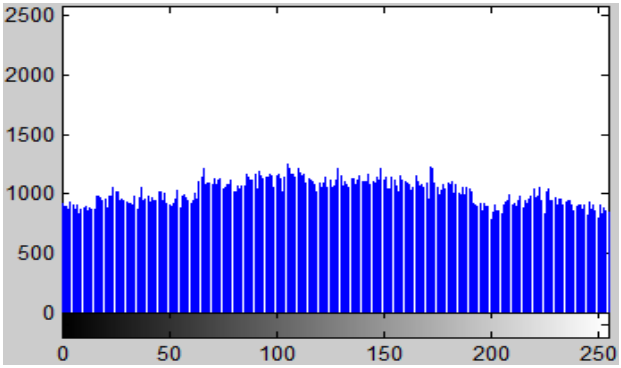
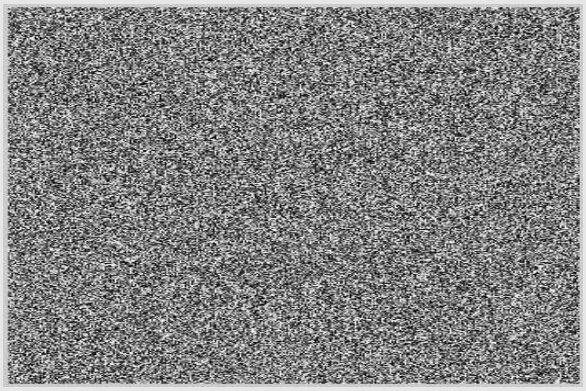


Figure 3.7 : Histogramme des images original.

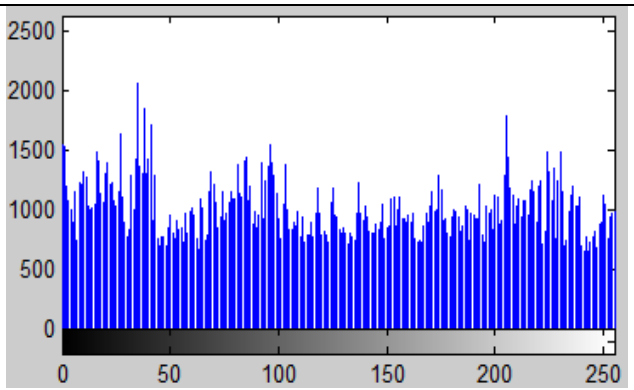
4.2.2 Histogramme des images crypté :

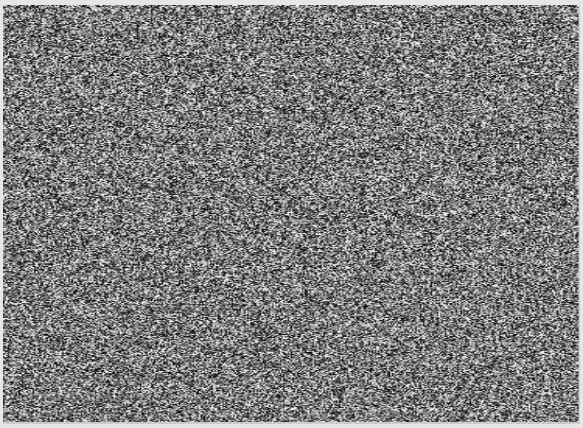
Image crypté	Histogramme crypté
 Maison	

 lena	
 Montagne	
 Papillon	

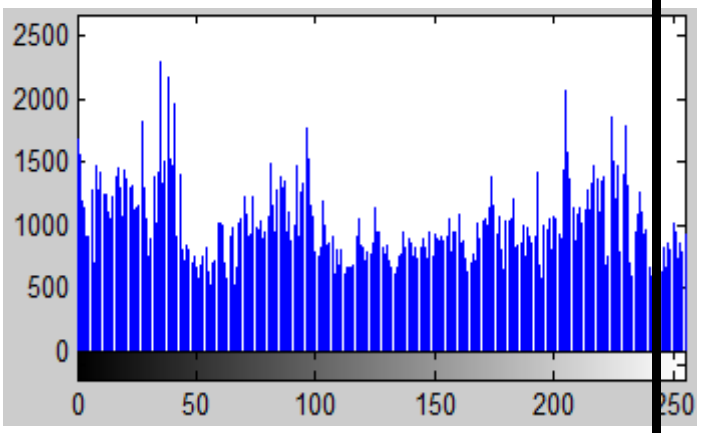


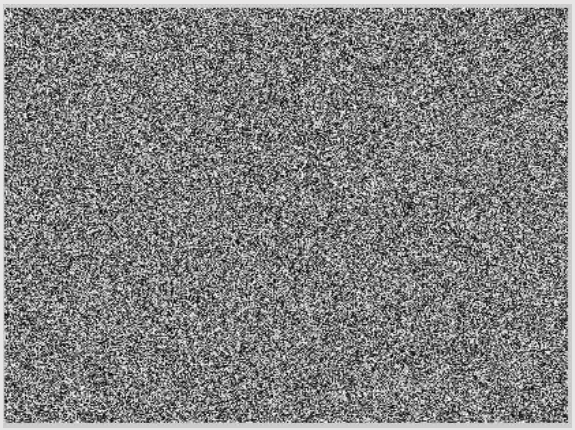
Poumon



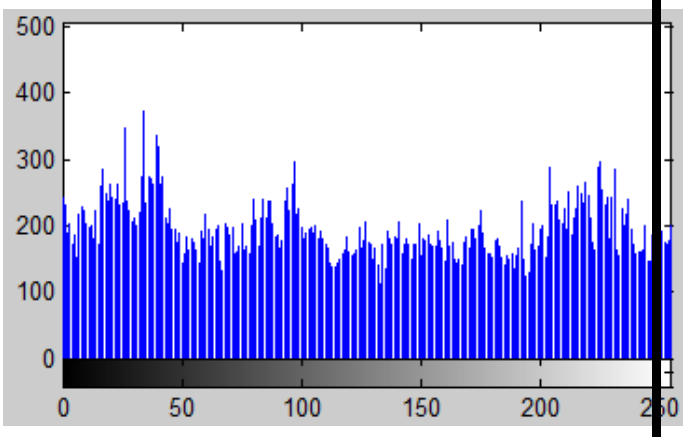


Cellule





Cou



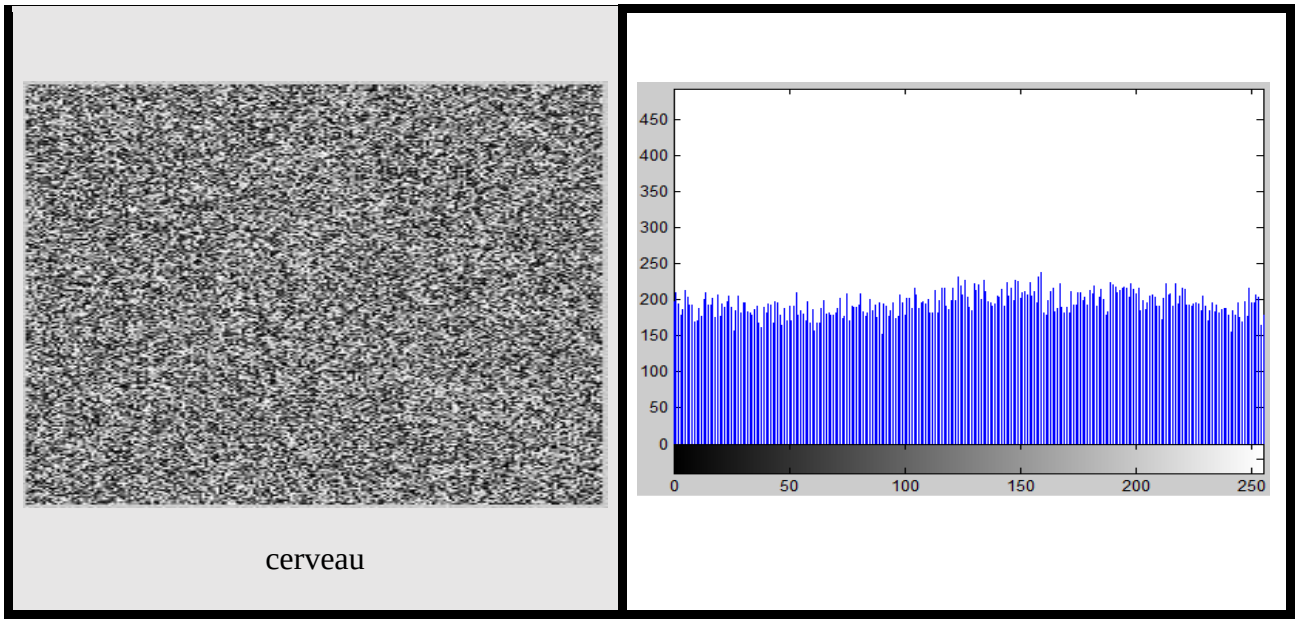


Figure 3.8 : Histogramme des images Crypté par carte logistique choatique.

Les résultats montrent que les histogrammes des images chiffrée utilisant la carte chaotique logistique sont homogène après le cryptage donc l'attaquant ne peut pas extraire aucune information à partir de l'histogramme de l'image cryptée .

Le tableau suivant correspond a cryptage image de cerveau et afficher tous les résultats de critère d'évaluation :

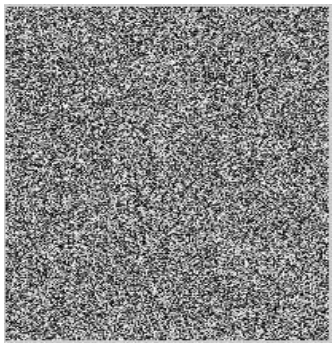
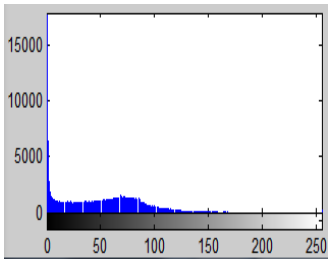
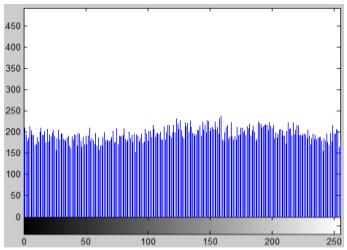
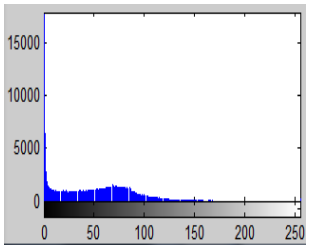
	Original	*Crypté*	*Décrypté*
Image			
Histogramme			
Entropie	7.4517	7.9675	7.4517
Corrélation	0.9549	0.0078	0.9549

Tableau 3.1 : cryptage image de Cerveau .

4.2.3 L'entropie

Le tableau 3.3 montrant les valeurs de l'entropie des images claires et chiffrées en utilisant la carte logistique chaotique .

Nom de l'image	*Taille*	*type*	*Entropie*	
			Image Chiffrée	*Image claire*
Maison	512×512	Niveau de gris	7.9975	7.8427
Lena	512×512	Niveau de gris	7.9961	7.5888
Montagne	512×512	Niveau de gris	7.9957	7.8363
Papillon	512×512	Niveau de gris	7.9927	7.8446
Poumon	512×512	Niveau de gris	7.9647	7.4527
Cellule	512×512	Niveau de gris	7.9398	7.5317
Cou	512×512	Niveau de gris	7.9704	7.4399
Cerveau	512×512	Niveau de gris	7.9675	7.4517
Valeur Moyenne			7.9780	7.6480

Tableau 3.2: résultats des entropie

Après la simulation de 8 images, la valeur moyenne de l'entropie des images chiffrées 7.9780 pour la clé générée par la carte logistique chaotique, et la moyenne de l'entropie de image clair est 7.6480 donc nous observons que la valeur moyenne de l'entropie est proche en 8 donc attaquant ne peux pas obtenir des informations sur le contenu des images.

4.2.4 La corrélation entre les pixels adjacents :

Le tableau 3.4 montrant les corrélations des images claires et leurs chiffrées en utilisant clé généré par la carte chaotique logistique.

Si la valeur de corrélation est proche de 1, cela signifie que les images claires et les images cryptées sont fortement dépendantes. Lorsque la valeur de corrélation est proche de 0, cela indique que la dépendance entre images cryptées et images cryptées est très élevée.

Remarque : Si une valeur de corrélation plus faible signifie une meilleure qualité de cryptage.

Nom de l'image	*Taille*	*type*	*Corrélation*	
			Image Claire	*Image chiffre*
Maison	512×512	Niveau de gris	0.8741	-0.0019
Lena	512×512	Niveau de gris	0.9588	-0.0010
Montagne	512×512	Niveau de gris	0.6974	0.0013
Papillon	512×512	Niveau de gris	0.9289	-0.0018
Poumon	512×512	Niveau de gris	0.9201	-0.0028
Cellule	512×512	Niveau de gris	0.9514	-0.0015
Cou	512×512	Niveau de gris	0.8023	-0.0054
Cerveau	512×512	Niveau de gris	0.9538	-0.0021
Valeur Moyenne			0.8858	-0.0152

Tableau 3.3 : résultats des corrélation

UACI et NPCR

Nom de l'image	*Taille*	*type*	*NPCR*	*UACI*
Maison	512×512	Niveau de gris	0.9960	0.1730
Lena	512×512	Niveau de gris	0.9975	0.1394
Montagne	512×512	Niveau de gris	0.9959	0.1453
Papillon	512×512	Niveau de gris	0.9961	0.1350
Poumon	512×512	Niveau de gris	0.9949	0.1957
Cellule	512×512	Niveau de gris	0.9944	0.2181
Cou	512×512	Niveau de gris	0.9957	0.4402
Cerveau	512×512	Niveau de gris	0.9952	0.2017

Tableau 3.4: résultats des NPCR et UACI

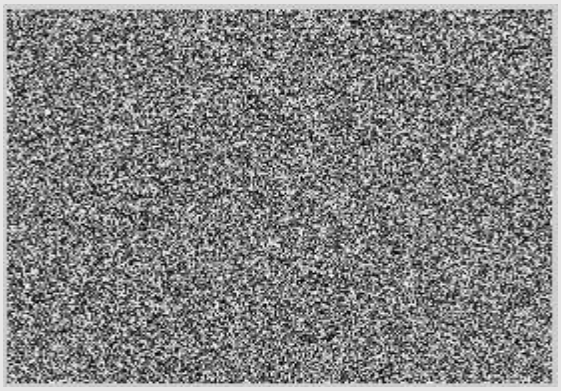
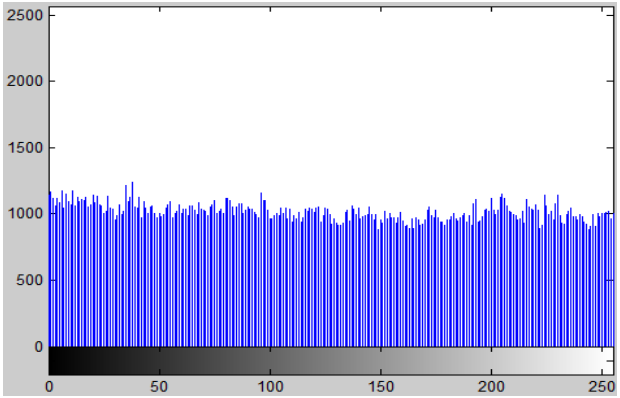
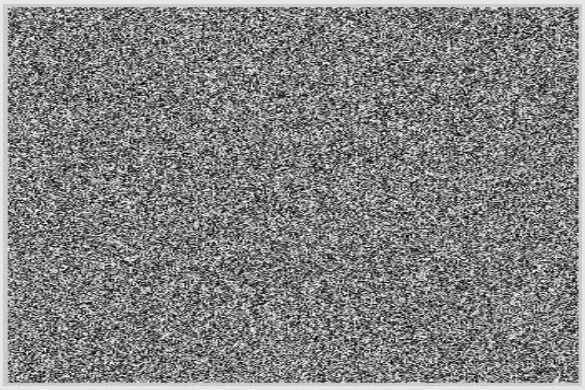
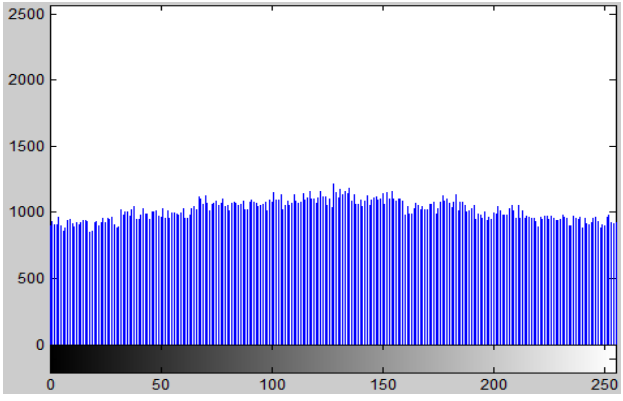
Après la simulation de 8 images, la valeur moyenne des corrélations des images chiffrées est -0.0152 pour la clé générée par la carte chaotique logistique , Donc les valeurs sont plus proches de 0.

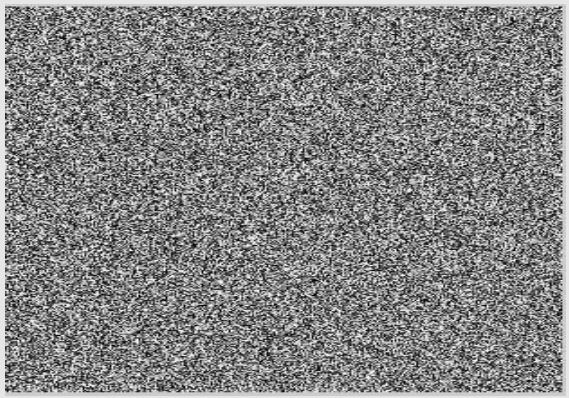
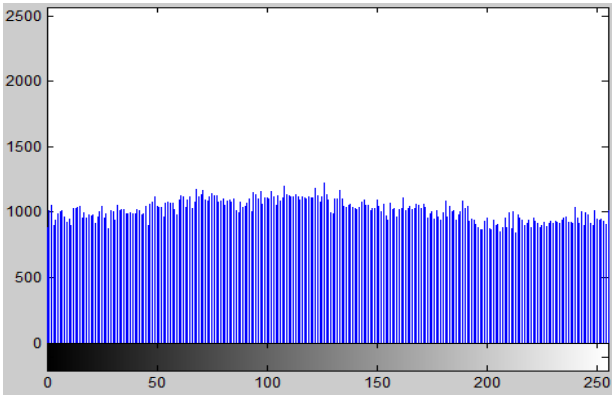
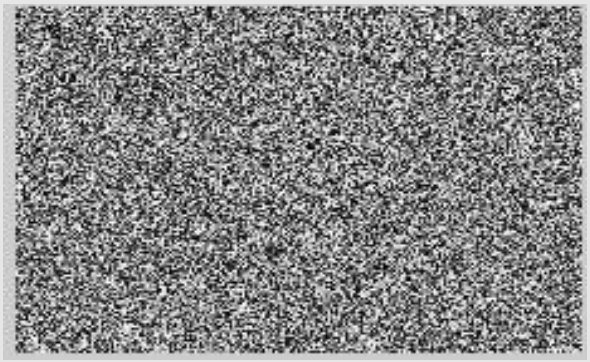
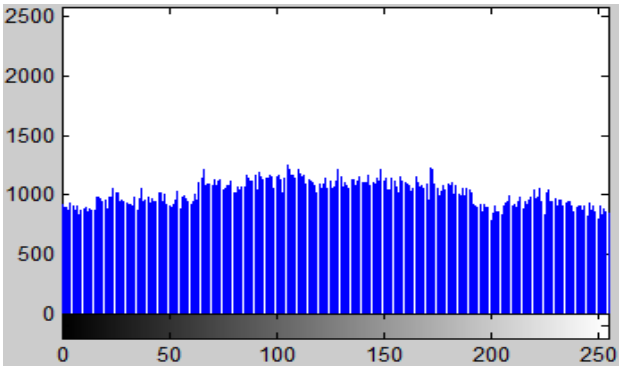
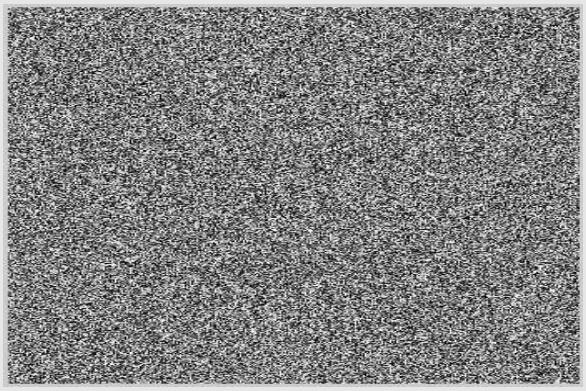
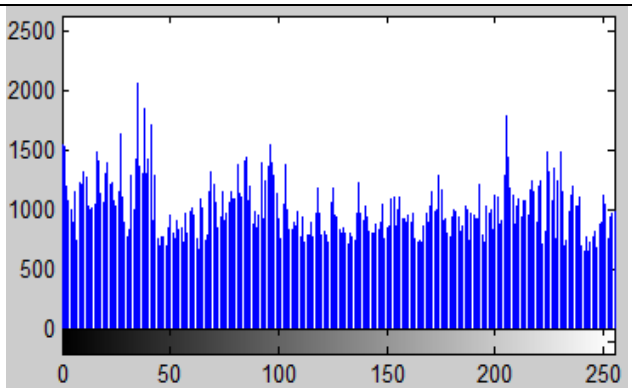
cela signifié que la qualité de cryptage est meilleure.

4.3 la carte Arnold Mapp :

en utilise les même photos

4.3.1 Histogramme des image crypté :

Image crypté	Histogramme crypté
 Maison	
 lena	

 Montagne	
 Papillon	
 Poumon	

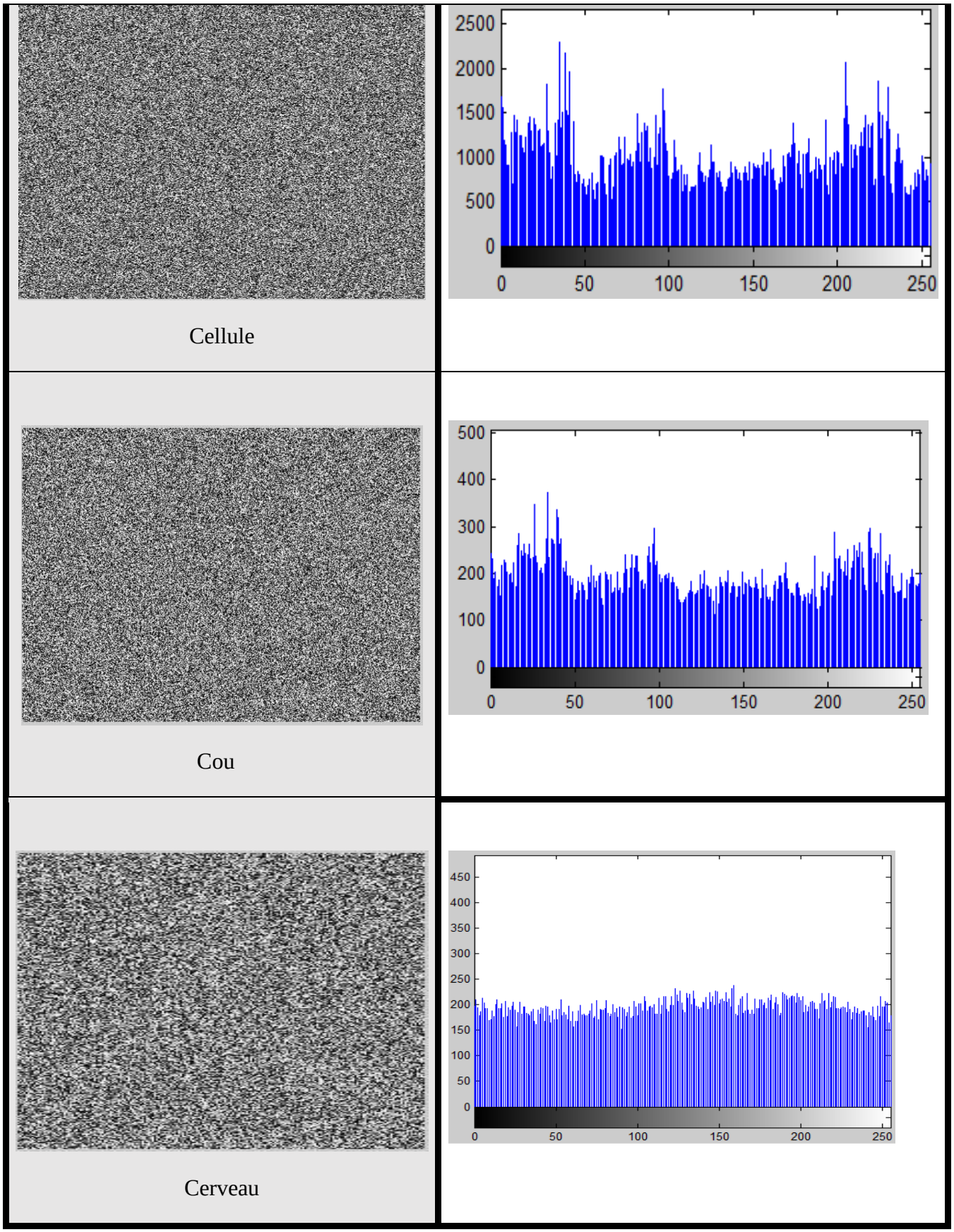


Figure 3.9 : Histogramme des images Crypté par carte Arnold .

4.3.2 Entropie :

Le tableau 3.7 montrant les valeurs de l'entropie des images claires et chiffrées en utilisant la carte Arnold Mapp.

Nom de l'image	*Taille*	*type*	*Entropie*	
			Image Chiffrée	*Image Claire*
Maison	512×512	Niveau de gris	7.9974	7.7684
Lena	512×512	Niveau de gris	7.9956	7.9269
Montagne	512×512	Niveau de gris	7.9959	7.8365
Papillon	512×512	Niveau de gris	7.9930	7.8469
Poumon	512×512	Niveau de gris	7.9652	7.4532
Cellule	512×512	Niveau de gris	7.9399	7.5318
Cou	512×512	Niveau de gris	7.9781	7.4474
Cerveau	512×512	Niveau de gris	7.9672	7.4514
Valeur Moyenne			7.9789	7.6611

Tableau 3.5: résultats des entropie .

Après la simulation de 8 images, la valeur moyenne de l'entropie des images chiffrées par carte Arnold Mapp 7.9789, et la moyenne de l'entropie de image clair est 7.6611 donc nous observons que la valeur moyenne de l'entropie est proche en 8 donc attaquant ne peux pas obtenir des informations sur le contenu des images.

4.3.3 Corrélation :

Nom de l'image	*Taille*	*type*	*Corrélation*	
			Image Claire	*Image chiffre*
Maison	512×512	Niveau de gris	0.8741	-0.0024
Lena	512×512	Niveau de gris	0.9588	-0.0068
Montagne	512×512	Niveau de gris	0.6976	0.0016
Papillon	512×512	Niveau de gris	0.9289	0.1446
Poumon	512×512	Niveau de gris	0.9201	-0.0012
Cellule	512×512	Niveau de gris	0.9514	-0.0018
Cou	512×512	Niveau de gris	0.916	-0.0010
Cerveau	512×512	Niveau de gris	0.9538	-0.0013
Valeur Moyenne			0.9070	0.0165

Tableau 3.6 : résultats des corrélation

Les résultats proche au 0 signifié que la qualité de cryptage est meilleure

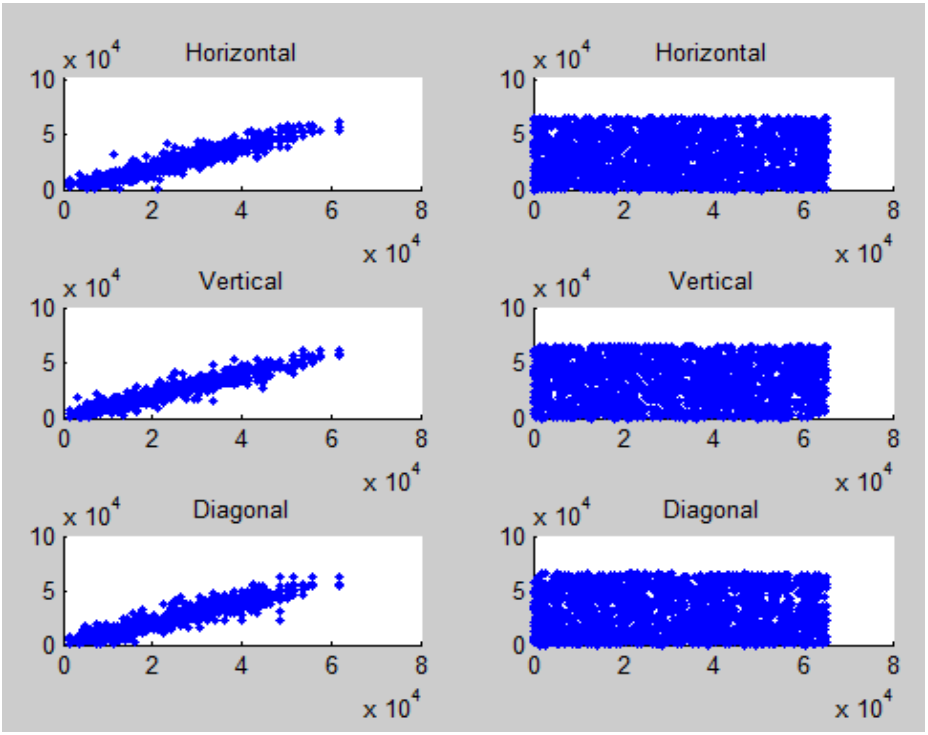


Figure 3.10 : résultats des corrélation.

UACI et NPCR

Nom de l'image	*Taille*	*type*	*NPCR*	*UACI*
Maison	512×512	Niveau de gris	0.9959	0.3330
Lena	512×512	Niveau de gris	0.9958	0.3226
Montagne	512×512	Niveau de gris	0.9959	0.3253
Papillon	512×512	Niveau de gris	0.9959	0.3208
Poumon	512×512	Niveau de gris	0.9949	0.3357
Cellule	512×512	Niveau de gris	0.9944	0.3417
Cou	512×512	Niveau de gris	0.9954	0.3401
Cerveau	512×512	Niveau de gris	0.9952	0.3317

Tableau 3.7: résultats des NPCR et UACI.

Comparaison entre carte logistique et carte Arnold :

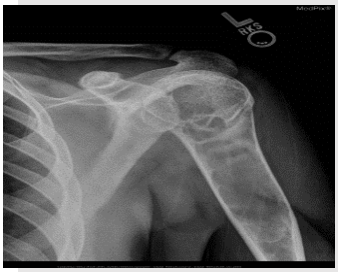
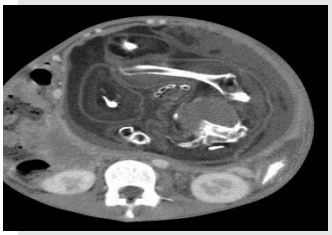
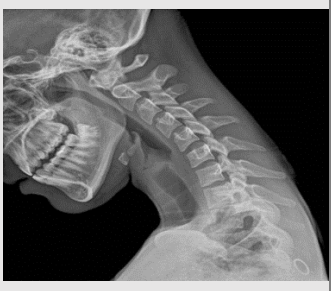
image	*Logistique*		*Arnold*	
	Entropie	**Corrélation**	**Entropie**	**Corrélation**
	7.9701	0.0045	7.9808	-0.0028
	7.9928	-0.0031	7.9932	-0.0029
	7.9855	0.0029	7.9857	0.0088
	7.9826	-0.0017	7.9909	-0.0022
	7.9905	-0.0025	7.9649	-0.0012
	7.9644	-0.0021	7.9649	-0.0012
La valeur moyenne	**7.9699**	**-0.0020**	**7.9830**	**0.0002**

tableau 3.8: comparaison entre carte logistique et carte Arnold.

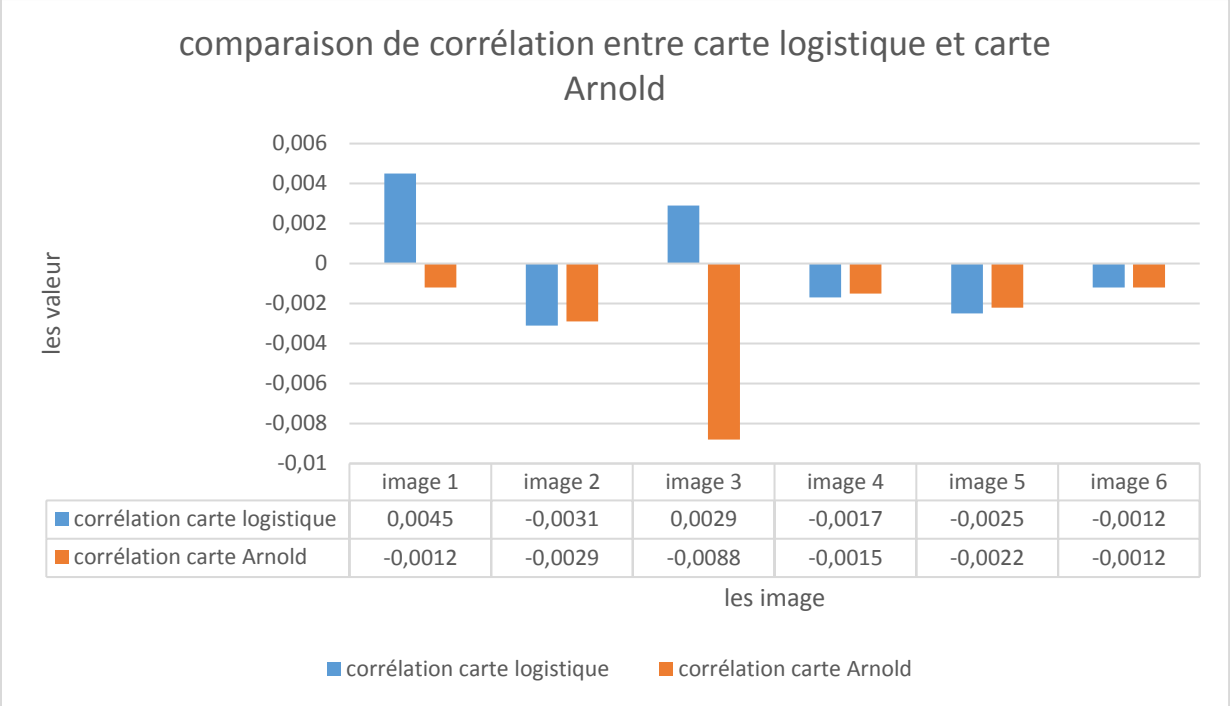


	image 1	image 2	image 3	image 4	image 5	image 6
corrélation carte logistique	0,0045	-0,0031	0,0029	-0,0017	-0,0025	-0,0012
corrélation carte Arnold	-0,0012	-0,0029	-0,0088	-0,0015	-0,0022	-0,0012

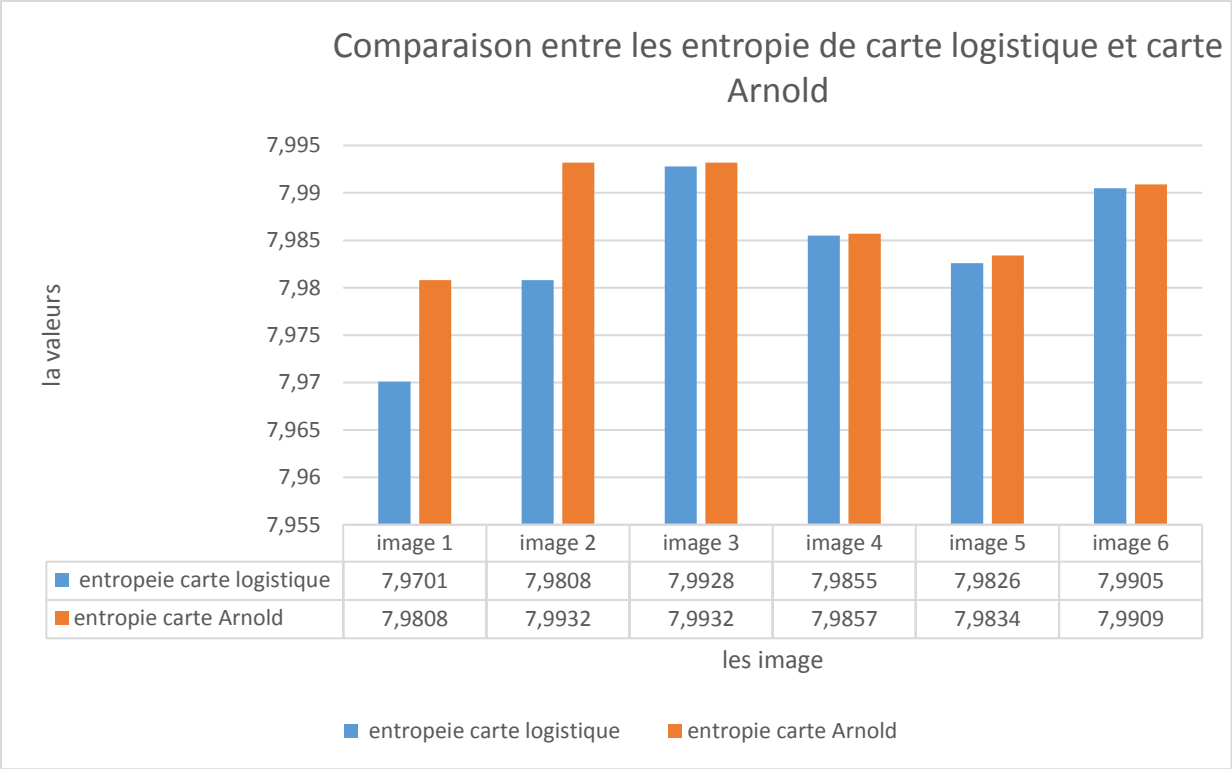


	image 1	image 2	image 3	image 4	image 5	image 6
entropeie carte logistique	7,9701	7,9808	7,9928	7,9855	7,9826	7,9905
entropie carte Arnold	7,9808	7,9932	7,9932	7,9857	7,9834	7,9909

5 Conclusion :

Dans ce chapitre, nous avons utilisé algorithme de cryptage basé sur la carte chaotique logistique. Les résultats expérimentaux ont montré que le système de cryptage par la carte chaotique logistique possède un grand espace de clés et une sécurité de haut niveau , ainsi que l'analyse et la comparaison de l'entropie et la corrélation des images chiffrées que l' algorithme assure une efficacité , une haute protection et sécurité contre les attaques brute.

Conclusion général

1 Conclusion général :

Les images médicales sont les plus utilisées dans la vie quotidienne et avec l'accélération et le développement que le monde connaît dans le domaine technologique.

Au début de cette mémoire, nous avons discuté des bases et des types de cryptage, puis nous avons mentionné les types d'images numériques en plus d'un aperçu de la théorie du chaos avec des critères d'évaluation.

Au cours de ce mémoire, nous avons proposé d'utiliser deux algorithmes de chiffrement d'image le premier algorithme est basé sur la suite de Tchebychev pour générer la clé et le deuxième c'est l'algorithme de Friedrich est basé sur la carte logistique chaotique et aussi la carte Arnold pour faire la comparaison, Le but principal de ce chiffrement est de savoir qui assure la sécurité parmi les deux.

En comparant les résultats des images précédentes avec les résultats obtenus à partir de deux l'algorithme proposé, nous montrons que La méthode que nous avons proposée il permet également une efficacité et d'une grande précision et qualité qui nous permet de faciliter et de simplifier les choses pour les utilisateurs d'images médicales.

Bibliographie

[1] https://lesdefinitions.fr/securite-informatique , consulté le 5 févr. 2013 .

[2] Sensibilisation et initiation à la cybersécurite ANSSI , https://www.ssi.gouv.fr/uploads/2016/05/cyberedu_module_1_notions_de_base_02_2017.pdf

[3] Mme L. SAOUDI, initiation à la cryptographie, support de cours du module Sécurité informatique, Département d'informatique, université de Msila, Année 2015/2016.

[4] R. Dumont, Cryptographie et Sécurité informatique, Notes de cours provisoires, Université de Liège, 2009 – 2010.

[5] BETTAHAR, Hatem et CHALLAL, Yacine. Introduction à la sécurité informatique. *Supports de cours, Systèmes Intelligents pour le Transport, Université de Technologie de Compiègne, France*, 2008, vol. 15.

[6] Mr.BOUCLI HACENE Ismail 'Polycopie de cours et TD INFORMTIQUE MEDICALE' .filiére génie biomedical université abou bakr belkaid tlemcen .années 2021-2021

[7] Non-répudiation. Wikipedia, https://fr.wikipedia.org/wiki/Non-répudiation/.

[8] MERDJAL, Choumaissa, MERAKCHI, Ahlam, et NINI, Ibrahim. Cryptage d'image par un signal unidimensionnel quelconque », Mémoire de Master informatique vision artificielle, Université LARBI BEN M'HIDI, OUM EL BOUAGHI, Année 2018.

[**9]** Le standard de chiffrement AES. La bibliothèque des Mathématiques. http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/aes/
[**10]** site web https://www.futura-sciences.com/tech/definitions/informatique-pixel-591

[12] https://www.imedias.pro/cours-en-ligne/graphisme-design/definition-resolution-taille-image/relations-definition-resolution-taille-image/

[13] HTTPS://WWW.LOSSENDIERE.COM/CATEGORY/STN/

[11] HADJI, Faiçal. *Conception et réalisation d'un système de cryptage pour les images médicales*. Thèse de doctorat. FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE. Filière: Informatique. UNIVERSITE MOHAMED BOUDIAF-M'SILA .2018

[14] William Puech , Crypto-Compression System for Secure Tranfer of Medical Images, CNRS/ University of Montpellier, FRANCE 23 Oct 2006

[15] https://www.printmytransfer.fr/132-47-117-format-des-fichiers-psd-pdf-eps-quel-format-pour-vos-impressions-ligne.html

[16] Bekkouche Souad « Tatouage appliqué à l'Imagerie Médicale » diplôme de magistère en Informatique.UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE d'ORAN Mohamed Boudiaf .Année universitaire: 2011/2012

[17] https ://fr.wikipedia.org/wiki/Imagerie

[18] https://www.doctissimo.fr/html/sante/imagerie/imagerie sommaire.htm.

[19] Léon Robichaud, L'image numérique Pixels et couleurs, support de cours, Département d'histoire, Université de Sherbrooke. 2020.

[20] Belkadi Imane, Amiar Narimen : « Cryptage d'image par considération des plans de bits des pixels séparément par ordre de leurs poids avec une clé publique de taille libre », Mémoire de Master en informatique vision artificielle, Université LARBI BEN M'HIDI, OUM EL BOUAGHI, Année 2017-2018.

[21] Yaovi, G. (2007). Cours de Traitement d'Image .. Licence de Physique S6 Annee Academique .Universite de Picardie Jules Verne. 2007-2008.

[22] jean De Dieu Nkapkop « Evaluation d'un algorithme de cryptage chaotique des images basé sur le modèle du perceptron » diplôme de Master en Informatique Université de Ngaoundéré - Master II 2012

[23] A. Beloucif, « Contribution à l'étude des mécanismes cryptographiques », thése En vue de l'obtention du diplôme de Doctorat en Informatique, Université de Batna2, 2016.

[24] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. Handbook Of Applied Cryptography 17 April 2013

[25] MADANI, M. et BENTOUTOU, Y. Cryptage d'images médicales à la base des cartes chaotiques. International Conference Colloque Tassili SCCIBOV. Université Djillali Liabes de Sidi Bel Abbes 2015.

[26] J.Zou, C.Z. Xiong, D. Qi, and R. K.Ward, "The application of chaotic maps in image encryption," IEEE International Symposium on Circuits and Systems, 2005.PP+DOI/……

[27] J.Peng, X.Liao, and Z.Wu, "Digital image secure communication using Chebyshev map chaotic sequences," IEEE secure communication, pp. 492-496, 2002.

[28] V. Patidar, N. K. Preek, K.K., "Sud a new substitution-diffusion based image cipher using chaotic standard and logistic maps". 3 mars 2014

[29] A. Hillion, "Les théories mathématiques des populations," Universitaires de France - PUF, P.U.F, 1986, coll.

[30] MANA, Boumedyen « Cryptage chaotique des images et de texte ». diplôme de Master en Informatique Université Abou Bakr Belkaid– Tlemcen. Année universitaire :2015-2016

[31] Tiegang Gao, Zengqiang Chen, A new image encryption algorithm based on hyper-chaos, Physics Letters A, 372(4):394–400, 2008.

[32] S. El Assad, M. Farajallah / Signal Processing: Image Communication 41 (2016) 144–157

[33] Dr. Methaq Talib Gaata[1] , Fadya Fouad Hantoosh[2]/ International Journal of Modern Trends in Engineering and Research (IJMTER) Volume 03, Issue 09, [September– 2016] .

[35] https://medpix.nlm.nih.gov/home