REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université 8Mai 1945 – Guelma
Faculté des sciences et de la Technologie
Département d'Electronique et Télécommunications

Mémoire de fin d'étude

pour l'obtention du diplôme de Master Académique

Domaine : **Sciences et Technologie**
Filière : **Electronique**
Spécialité : **Instrumentation**

La cryptographie des images numériques par la carte logistique chaotique

Présenté par :

- Bousnoubra Yasser

- Hamada Aymen

Sous la direction de :

-Pr .Boudjehem Djalil

Septembre 2020

بسم الله الرحمان الرحيم

Dédicace

Nous dédions ce modeste travail :

À tous les membres de notre famille pour leur soutien continu et Nous leur souhaitons bonne santé et long vie.

À tous nos amis et à tous ceux que nous aimons et à ceux qui nous aiment.

À tous nos professeurs qui ont fait de leur mieux pour nous Donner le plus d'informations possible sur notre étude.

***Merci infiniment**.*

/

Remerciement

Au terme de ce travail, on tient notre remerciement à notre dieu de nous avoir donné la chance de suivre le Chemin de la science.

Mes vifs remerciements sont aussi adressés à notre encadreur Pr. Boudjehem Djalil de sa Disponibilité, sa générosité professionnelle et ses précieux conseils.

Nous remercions les membres du jury Nous feront l'honneur d'apprécier ce modeste travail.

Enfin, nous tenons à remercier toutes les personnes qui nous ont aidés directement ou indirectement avec ce travail.

Merci à tous .

Résumé

Avec le développement rapide de l'utilisation des images numériques dans de nombreux domaines, il est devenu impératif de protéger les données d'image confidentielles contre tout accès non autorisé .Dans ce mémoire de fin d'étude, nous avons utilisé deux types d'algorithme de cryptage qui peut être appliqué aux images en niveaux de gris, le premier basé sur un clé aléatoire et le second basé sur chaotique carte logistique. Après avoir étudié ces deux algorithmes et mené quelques expériences, nous avons conclu qu'ils offrent de bonnes performances en termes de qualité et sécurité.

Mots Clés:

Cryptographie, Image numérique, Carte logistique chaotique.

الملخص

مع التطور السريع لاستخدام الصور الرقمية في العديد من المجالات ، أصبح من الضروري حماية بيانات الصور السرية من الوصول غير المصرح به. في هذه الأطروحة الأخيرة ، اقترحنا نوعين من خوارزمية التشفير التي يمكن تطبيقها على الصور الرمادية ، الأول يعتمد على مفتاح عشوائي والثاني يعتمد على خريطة لوجستية فوضوية. بعد دراسة هاتين الخوارزميتين وإجراء بعض التجارب توصلنا إلى أنهما تقدمان أداءً جيدًا من حيث الجودة والسلامة.

الكلمات المفتاحية

التشفير ، الصورة الرقمية ، الخريطة اللوجستية الفوضوية

Abstract

With the rapid development of the use of digital images in many fields, it has become imperative to protect confidential image data from unauthorized access. In this graduation thesis, we used two types of encryption algorithm that can be applied to grayscale images, the first based on a random key and the second based on a chaotic logistic map. After studying these two algorithms and carrying out some experiments, we concluded that they offer a good performance in terms of quality and safety.

Key words:

Cryptography, Digital Image, Chaotic Logistic Map

Table des matières

Chapitre 2 : Les images numériques

Liste des figures

Liste des tableaux

Liste d'abréviations

AES: Advanced Encryption Standard

DES: Data Encryption Standard

EPS: Encapsulated PostScript

Jpeg: Joint Photographic Experts Group

GEDEFU 18: GEheimschrift DEr FUnker 18

GIF: Graphics Interchange Format

NSA: National Security Agency

PDF: Portable Document Format

Png: Portable Network Graphics

RC4: Rivest Cipher 4

RSA: nommé par les initiales de ses trois inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman

RVB: rouge, vert et bleu

SSL: Secure Sockets Layer

SVG: Scalable Vector Graphics

TLS: Transport Layer Security

WEP: Wired Equivalent Privacy

Introduction générale

Depuis longtemps, l'homme avait besoin de moyens secrets pour transmettre des messages, c'est pourquoi il a utilisé de nombreuses techniques et méthodes pour atteindre cet objectif. Ce sont des méthodes qui transforment le message en une forme incompréhensible, ou le cache à l'aide d'une image, d'un texte ou d'autres choses afin d'empêcher une personne étrangère de l'identifier. Ces méthodes appelées des méthodes de cryptographie.

Les méthodes de cryptographie se basent en général sur certaines notions. Actuellement, la cryptographie moderne se base en partie sur certaines notions difficiles.

L'utilisation des notions difficiles ou contraire à l'ordinaire pour établir des algorithmes de cryptographie était une tradition chez les cryptographes arabes. Ils avaient utilisé, entre autres, la poésie comme moyen de transmission et ont utilisé, par exemple, la difficulté d'écrire des vers de poésie (ou des morceaux de vers) suivant un modèle donné ou des vers qu'on peut lire de droite à gauche et en même temps de gauche à droite comme base d'algorithmes de cryptographie.

Ainsi, la poésie Arabe était un moyen de transmission, d'information, de publicité et de cryptographie.

Les Arabes ont utilisé la cryptographie même avant l'Islam ; mais les piliers de la cryptographie Arabe étaient bâtis par EL Khalil (718-786) et EL Kindi (801-873). Al Khalil avait :

- Modélise la poésie Arabe en 16 modèles.
- Elaboré un dictionnaire qui ne donne pas seulement la définition d'un mot donné mais donne aussi les définitions de tous les mots obtenus par permutation des lettres du mot initial. Ceci permettra de décrypter tout mot crypté par permutation de lettres. Ainsi, c'est de plus un dictionnaire de cryptanalyse.
- Ecrit un livre de cryptographie qui n'a jamais été retrouvé.
- Introduit les statistiques linguistiques et l'analyse combinatoire

El Kindi, le plus connu des savants Arabe en cryptographie, avait laissé un grand nombre de livres dans plusieurs domaines (philosophie, logique, mathématique, chimie, astronomie, poésie, médecine, musique, politique…), en particulier en cryptographie. Il avait montré que tout message crypté à l'aide des méthodes de substitution peut être décrypté. Il avait utilisé, en

particulier, l'analyse des fréquences de lettres, pour la cryptanalyse de plusieurs méthodes de cryptographie. El Kindi est donc le premier cryptanalyste Arabe.

Organisation du mémoire

Nous avons structuré notre mémoire en trois chapitres. Dans Le premier chapitre on donne une brève présentation sur les techniques de cryptographie et ses classifications. Le deuxième chapitre met le point sur les notions de base d'image numérique, ses types, les différents modes de couleur des images ainsi que leurs formats. Le troisième chapitre consiste à présenter la réalisation de la cryptographie des images utilisant la carte logistique chaotique. Puis on va terminer par une conclusion générale.

Chapitre 1
Généralité sur la cryptographie

1. Introduction

La cryptographie se concentre sur la protection des messages contre l'identification par d'autres personnes (en garantissant la confidentialité, l'authenticité et l'intégrité) en utilisant souvent des secrets ou des clés. Contrairement à la stéganographie qui dissimule un message dans un autre message, la cryptographie rend un message totalement inintelligible. Il est utilisé depuis longtemps, mais certaines de ses méthodes les plus importantes, comme la cryptographie asymétrique, datent de la fin du XXe siècle [1].

2. Notions de base sur la cryptographie

2.1 Cryptographie

Le cryptage est un processus qui cherche à préserver la confidentialité des informations, images, textes, etc., grâce à des programmes qui convertissent ces informations en un mélange de symboles, de chiffres ou de lettres qui ne sont pas compris. Le processus de cryptage et de décryptage est effectué par une clé, Il existe deux types de cryptage symétrique et asymétrique, que nous expliquerons chacun d'eux dans ce chapitre

La cryptographie n'est pas le seul moyen d'assurer la sécurité des informations, mais plutôt un ensemble de techniques [2].

2.2 La Cryptologie

La cryptologie, étymologiquement la science du secret, ne peut être vraiment considérée comme une science que depuis peu de temps. Cette science englobe la cryptographie, l'écriture secrète, la cryptanalyse et l'analyse de cette dernière-.

La cryptologie est un art ancien et une science nouvelle : un art ancien car les Spartiates l'utilisaient déjà (la scytale) ; une science nouvelle parce que ce n'est un thème de recherche scientifique académique, c'est-à-dire universitaire, que depuis les années 1970. Cette discipline est liée à beaucoup d'autres, par exemple l'arithmétique modulaire, l'algèbre, la théorie de la complexité, la théorie de l'information, ou encore les codes correcteurs d'erreurs [3].

2.3 La Cryptanalyse

C'est la science qui déchiffre les algorithmes et convertit le texte crypté en texte non crypté. Le processus par lequel on tente de comprendre un message en particulier est appelé une attaque [4].

2.4 Le Chiffrement

Le chiffrement consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le

destinataire. La fonction permettant de retrouver le texte clair à partir du texte chiffré porte le nom de déchiffrement [5].

2.5 Texte chiffré

Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair [5].

2.6 Clef

Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement. Dans le cas d'un algorithme symétrique, la clef est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux opérations [5].

2.7 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 [5].

2.8 Déchiffrement

C'est le processus de conversion du message chiffré à son état normal, c'est-à-dire le décodage.

2.9 Diffusion

La diffusion est une propriété où la redondance statistique dans un texte en clair est dissipée dans les statistiques du texte chiffré. En d'autres termes, un biais en entrée ne doit pas se retrouver en sortie et les statistiques de la sortie doivent donner le moins possible d'informations sur l'entrée [6].

2.10 Confusion

La confusion correspond à une volonté de rendre la relation entre la clé de chiffrement et le texte chiffré la plus complexe possible [6].

2.11 Permutation (transposition)

Chiffrement par permutation (Un chiffrement par transposition) est un chiffrement qui consiste à changer l'ordre des lettres, le chiffrement par transposition demande de découper le texte clair en blocs de taille identique. La même permutation est alors utilisée sur chacun des blocs [6].

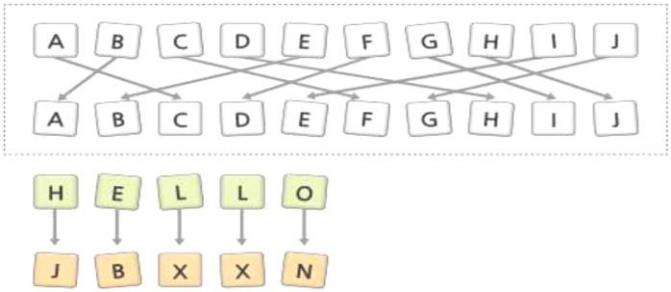


Figure 1.1 : chiffrement par permutation

2.12 Texte en clair : C'est le résultat du processus de décryptage. En cryptographie le texte en clair c'est une information non chiffrée [7].

2.13 Substitution : Le chiffrement par substitution consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou plusieurs autres entités [8].

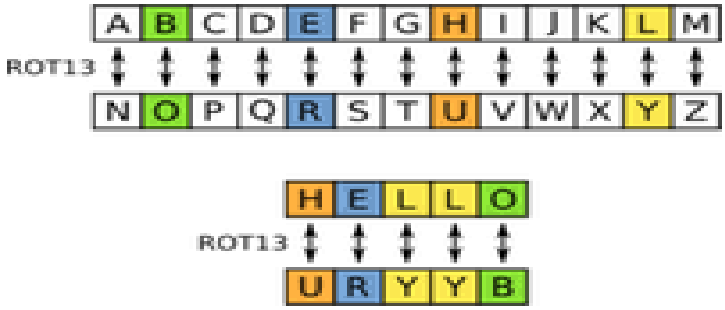


Figure 1.2 : chiffrement par substitution**.**

3. Objectif de la cryptographie

La cryptographie garantit entre autres l'intégrité, le non reniement et l'authenticité des données en plus de leurs confidentialités.

3.1 Confidentialité des Données

C'est-à-dire préserver le contenu de l'information contre le risque d'être accédé par des personnes indésirables, sauf ceux autorisé à l'avoir [2].

3.2 Authentification

L'authentification est un service lié à l'identification. Cette fonction s'applique aux deux entités et l'information elle-même. Deux parties concluant une communication devraient identifier l'une et l'autre. Les informations fournies sur un canal doivent être authentifiées quant à leur origine, date d'origine, contenu des données, heure d'envoi, etc. Pour ces raisons, cet aspect de cryptographie est généralement subdivisé en deux classes principales : l'authentification d'entité et les données, et l'authentification d'origine. L'authentification de l'origine des données fournit implicitement l'intégrité des données (car si un message est modifié, la source a changé) [2].

3.3 Non répudiation

La non-répudiation est un service qui empêche une entité de renier ses engagements antérieurs ou des actions. Lorsque des litiges surviennent du fait qu'une entité nie que certaines actions ont été prises, un moyen de résoudre la situation est nécessaire. Par exemple, une entité peut autoriser l'achat d'un bien par une autre entité et refuser ultérieurement cette autorisation a été

accordée. Une procédure impliquant un tiers de confiance est nécessaire pour résoudre la dispute , La non répudiation se décompose en trois :

a. Non-répudiation d'origine l'émetteur ne peut nier avoir ´écrit le message et il peut prouver qu'il ne l'a pas fait si c'est effectivement le cas.

b. Non-répudiation de réception le receveur ne peut nier avoir reçu le message et il peut prouver qu'il ne l'a pas reçu si c'est effectivement le cas.

c. Non-répudiation de transmission l'émetteur du message ne peut nier avoir envoyé le message et il peut prouver qu'il ne l'a pas fait si c'est effectivement le cas [2].

3.4 Intégrité des données

L'intégrité des données est un service qui traite de la modification non autorisée des données. À assurer l'intégrité des données, il faut avoir la capacité de détecter la manipulation des données par des personnes non autorisées des soirées. La manipulation des données comprend des éléments tels que l'insertion, la suppression et substitution.

Un objectif fondamental de la cryptographie est de répondre adéquatement à ces quatre domaines à la fois Théorie et pratique. La cryptographie concerne la prévention et la détection de la tricherie et autres activités malveillantes [2] .

4. Evolution du cryptage d'image dans le temps (Historique)

4.1 Cryptographie classique

Pour des raisons différentes, les humains ont été intéressés à protéger leurs messages, les Assyriens étaient intéressés à protéger leur commerce secret de fabrication de la poterie. Les Chinois étaient intéressés à protéger leur secret commercial de fabrication de la soie. Les Allemands étaient intéressés à protéger leurs secrets militaires en utilisant leur fameuse machine Enigma.

On peut signaler ainsi le chiffrement de César, le Système de Vigenère et le Système ADFG(V)X qui date du XVIe siècle av. J.-C.

4.1.1 Chiffrement de César

Cette méthode nécessite de changer chaque lettre du texte a chiffré par la lettre qui se trouve ***n*** places plus loin dans l'alphabet qui se suivent. Par exemple si n=3, on remplacera A par D, B par E, C par F etc [9].

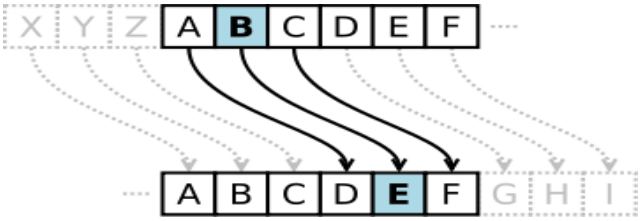


Figure 1.3 : Exemple de chiffrement par code de César (n=3)

Tableau 1.1 : Chiffre de César appliqué à un message (pour n=7)

Message clair :	B	E	L	L	U	M	—	C	A	L	E	N	D	A	E
Place dans l'alphabet :	2	5	12	12	21	13	—	3	1	12	5	14	4	1	5
Clef de chiffrement :	$lettre \rightarrow lettre + 7$														
Résultat de l'opération :	9	12	19	19	2 [3]	20	—	10	8	19	12	21	11	8	12
Message chiffré :	I	L	S	S	B	T	—	J	H	S	L	U	K	H	L

4.1.2 Le système de Vigenère

Au XVIe siècle Blaise de Vigenère (1523-1596) expose le maniement du chiffre carré dans son écrit " Traité des chiffres, ou secrètes manières d'écrire ; Paris 1596 ". Quant à son système (système de Vigenère), il résista aux décrypteurs jusqu'en 1863.

Pour crypter, on choisit une clef (mot ou phrase). A chaque lettre du texte clair on fait correspondre une lettre de la clef (la clef étant répétée autant de fois que nécessaire). La lettre du texte chiffré sera prise dans la colonne correspondante à la lettre du texte clair, et dans la ligne correspondante à la lettre de la clef [10].

Le chiffre de Vigenère est une amélioration décisive du chiffre de César. Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message. On peut résumer ces décalages avec un carré de Vigenère. Ce chiffre utilise une clef qui définit le décalage pour chaque lettre du message (A: décalage de 0 cran, B: 1 cran, C: 2 crans, ..., Z: 25 crans).

***Exemple* :** chiffrons le texte "CHIFFRE DE VIGENERE" avec la clef "BACHELIER" (cette clef est éventuellement répétée plusieurs fois pour être aussi longue que le texte clair).

Tableau 1.2: Application du carré de Vigenère

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

4.1.3 Le système ADFG(V) X

En 1918 Les armées allemandes et françaises sont exsangues. L'état-major français, dirigé par le maréchal Foch, redoute l'imminence d'une offensive massive de l'ennemi, qui enfoncerait les lignes de défense jusque Paris. Cinq points d'offensive sont possibles, mais les forces françaises de réserve ne permettent de se concentrer que sur un seul. Il est vital, pour l'issue de la guerre, de ne pas se tromper.

Depuis mars 1918, l'armée allemande utilise un nouveau code pour communiquer, le chiffre ADFGVX, ou GEDEFU 18 (GEheimschrift DEr FUnker 18, chiffre des télégraphistes 18). Ce chiffre est constitué d'une substitution de type carré de Polybe, suivie d'une transposition.

Pour réaliser la substitution, les 26 lettres de l'alphabet et les 10 chiffres sont rangés dans un tableau 6×6, aux extrémités desquelles on a ajouté les lettres ADFGVX. Elles ont été choisies pour ce code car l'essentiel des télécommunications est transmis par radio, et les lettres ADFGVX ont des codes morses très différents.

Exemple :

Tableau 1.3 : exemple de système ADFG(V) X

	A	D	F	G	V	X
A	Q	Y	A	L	S	E
D	Z	C	R	X	H	0
F	F	O	4	M	8	7
G	3	I	T	G	U	K
V	P	D	6	2	N	V
X	1	5	J	9	W	B

Chaque lettre est codée par le couple de lettres qui correspond à sa ligne et à sa colonne. Ainsi, « R » est codé « DF », et le message « RENFORT COMPIEGNE 16H10 » devient : « DFAXV VFAFD DFGFD DFDFG VAGDA XGGVV AXXAV FDVXA DX ».

4.2 Cryptographie moderne

4.2.1 Cryptographie symétrique (à clé secrète)

La cryptographie à algorithmes symétriques utilise la même clé pour les processus de codage et de décodage ; cette clé est le plus souvent appelée « secrète ». Le chiffrement consiste à appliquer une opération (algorithme) sur les données à chiffrer à l'aide de la clé privée, afin de les rendre inintelligibles. Ainsi, le moindre algorithme peut rendre le système quasiment inviolable (la sécurité absolue n'existant pas) [11].

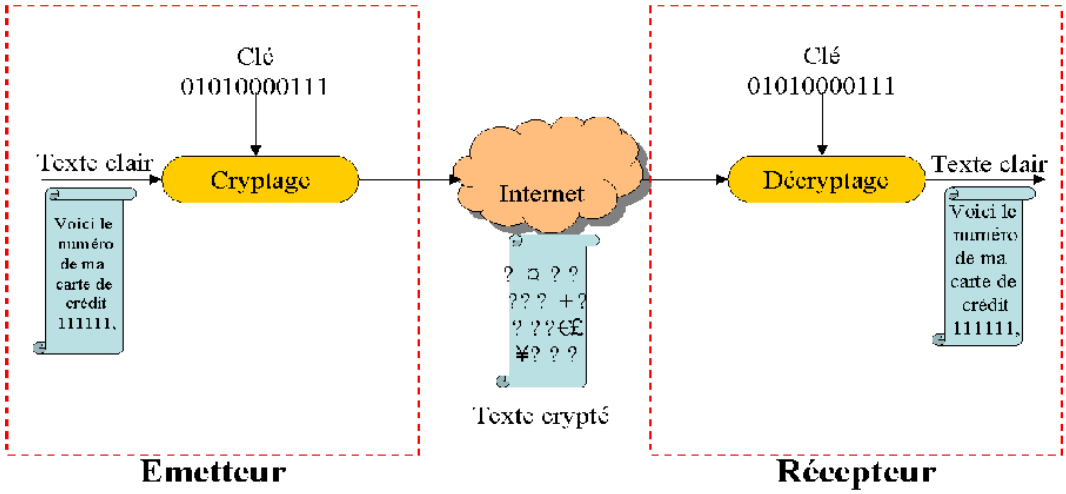


Figure 1.4 : cryptographie symétrique [11].

4.2.1.1 Chiffrement par flot : les chiffrements par flots fonctionnent généralement sur de petites unités de texte en clair, généralement des bits. Ainsi, les chiffrements par flots sont beaucoup plus rapides qu'un chiffrement par blocs typique. Généralement, un chiffrement par flots génère une séquence de bits en tant que clé (appelée flux de clé) en utilisant un générateur de nombres pseudo-aléatoires (PRNG) qui étend une courte clé secrète (par exemple 128 bits) en une longue chaîne de bits (flux de clé). Le chiffrement est effectué en combinant le flux de clé avec le texte en clair. Habituellement, l'opération XOR bit à bit est choisie essentiellement pour sa simplicité à effectuer ce chiffrement [12].

Parmi les algorithmes qui utilisent chiffrement par flot : RC4, A5/1, E0 …. etc. On parlera de RC4 car c'est le plus répandu.

a) Algorithme RC4

(Rivest Cipher 4) est un algorithme de chiffrement conçu en 1987 par Ronald Rivest. Il est supporté par différentes normes, par exemple dans Transport Layer Security (TLS), anciennement nommé Secure Sockets Layer (SSL), et il est exploité encore par des protocoles courants tels que WEP, pour la protection des réseaux WiFi [13].

b) Principe du RC4

RC4 fonctionne de la façon suivante : la clef RC4 permet d'initialiser un tableau de 256 octets en répétant la clef autant de fois que nécessaire pour remplir le tableau. Par la suite, des opérations très simples sont effectuées : les octets sont déplacés dans le tableau, des additions

sont effectuées, etc. Le but est de mélanger autant que possible le tableau. Finalement on obtient une suite de bits pseudo-aléatoires qui peuvent être utilisés pour crypté les données via un XOR.

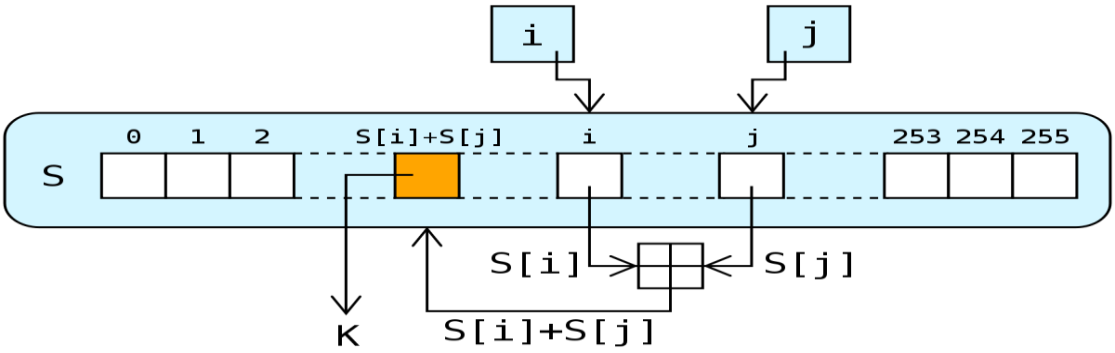


Figure 1.5 : Principe de RC4

4.2.1.2 Chiffrement par bloc

Un chiffrement par blocs est un type d'algorithme de chiffrement à clé symétrique qui transforme un bloc de données de texte en clair de longueur fixe en un bloc de données de texte chiffré de même longueur. La longueur fixe est appelée la taille du bloc. Pour plusieurs chiffrements par blocs, la taille du bloc est de 64 ou 128 bits. Plus la taille du bloc est grande, plus le chiffrement est efficace, mais plus les algorithmes et les dispositifs de chiffrement et de décryptage sont complexes. Un exemple de cryptage par blocs est le schéma (DES) [12].
Parmi les algorithmes qui utilisent chiffrement par bloc : DES , AES , Blowfish…. Etc

a) Algorithme DES

Le Data Encryption Standard (DES, prononcer /dɛs/) est un algorithme de chiffrement symétrique (chiffrement par bloc) utilisant des clés de 56 bits. Son emploi n'est plus recommandé aujourd'hui, du fait de sa lenteur à l'exécution et de son espace de clés trop petit permettant une attaque systématique en un temps raisonnable. Quand il est encore utilisé c'est généralement en Triple DES, ce qui ne fait rien pour améliorer ses performances. DES a notamment été utilisé dans le système de mots de passe UNIX.
Le premier standard DES est publié par FIPS le 15 janvier 1977 sous le nom FIPS PUB 46. La dernière version avant l'obsolescence date du 25 octobre 1999 [14].

b) Principe du DES

L'algorithme DES transforme un bloc de 64 bits en un autre bloc de 64 bits. Il manipule des clés individuelles de 56 bits, représentées par 64 bits (avec un bit de chaque octet servant pour le contrôle de parité). Ce système de chiffrement symétrique fait partie de la famille des chiffrements itératifs par blocs, plus particulièrement il s'agit d'un schéma de Feistel (du nom de Horst Feistel à l'origine du chiffrement Lucifer).

c) Algorithme AES

Advanced Encryption Standard ou AES , aussi connu sous le nom de Rijndael, est un algorithme de chiffrement symétrique. Il remporta en octobre 2000 le concours AES, lancé en 1997 par le NIST et devint le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis. Il a été approuvé par la NSA (National Security Agency) dans sa suite B des algorithmes cryptographiques. Il est actuellement le plus utilisé [15].

d) Principe de AES

L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(28) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.

Finalement, un OU exclusif XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours.

4.2.2 La cryptographie asymétrique (à clé publique)

La cryptographie asymétrique à clé publique est apparue pour la première fois en 1976 avec la publication d'un ouvrage sur la cryptographie par Whitfield Diffie et Martin Hellman, c'est méthode de chiffrement qui s'oppose à la cryptographie symétrique.

Dans un tel crypto système, les clés existent en paires d'où l'appellation bi-clés :

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

L'utilisateur d'un crypto système asymétrique, choisit une clé aléatoire (la clé privé), à partir de cette clé et en appliquant la fonction à sens unique il calcule la clé publique qu'il diffuse au travers d'un canal non sécurisé.

Lorsqu'une personne désire envoyer un message il suffit de chiffrer ce dernier à l'aide de la clé publique.

Le destinataire sera en mesure de déchiffrer le message à l'aide de sa clé privé. Ce système est basé sur une fonction facile à calculer dans un sens (appelé fonction à trappe à sens unique) et mathématiquement très difficile à inverser sans la clé privée appelé trappe

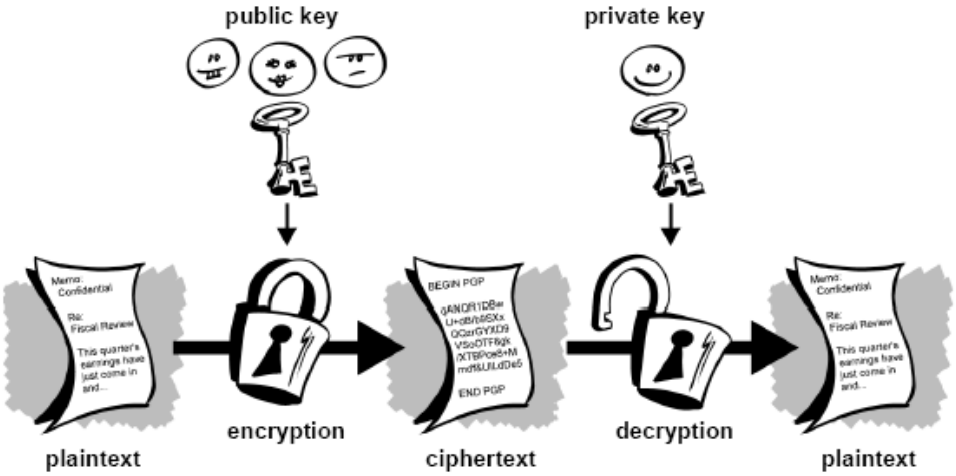


Figure 1.6 : la cryptographie asymétrique

Plaintext : le texte non chiffré.

Encryption : Le processus de cryptage avec une clé publique.

Ciphertext : Le texte crypté.

Decryption : Décryptage par clé privée.

Plaintext : Le message d'origine après décryptage.

Les principaux algorithmes asymétriques à clé publiques sont : RSA, DSA, Diffie-Hellman

a) Algorithme RSA

Le chiffrement RSA (nommé par les initiales de ses trois inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman) créé en 1977, est un algorithme de cryptographie asymétrique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet [16].

b) Principe de RSA

Tous les calculs se font modulo un nombre entier n qui est le produit de deux nombres premiers. Le petit théorème de Fermat joue un rôle important dans la conception du chiffrement.

Les messages clairs et chiffrés sont des entiers inférieurs à l'entier n. Les opérations de chiffrement et de déchiffrement consistent à élever le message à une certaine puissance modulo *n* (c'est l'opération d'exponentiation modulaire).

La seule description des principes mathématiques sur lesquels repose l'algorithme RSA n'est pas suffisante. Sa mise en œuvre concrète demande de tenir compte d'autres questions qui sont

essentielles pour la sécurité. Par exemple le couple (clé privée, clé publique) doit être engendré par un procédé vraiment aléatoire qui, même s'il est connu, ne permet pas de reconstituer la clé privée. Les données chiffrées ne doivent pas être trop courtes, pour que le déchiffrement demande vraiment un calcul modulaire, et complétées de façon convenable (par exemple par l'Optimal Asymmetric Encryption Padding).

c) Création des clés

1. Choisir p et q, deux nombres premiers distincts ;
2. Calculer leur produit n = pq, appelé module de chiffrement ;
3. Calculer $\varphi(n) = (p-1)(q-1)$ (c'est la valeur de l'indicatrice d'Euler en n) ;
4. Choisir un entier naturel e premier avec $\varphi(n)$ et strictement inférieur à $\varphi(n)$, appelé exposant de chiffrement ;
5. Calculer l'entier naturel d, inverse de e modulo $\varphi(n)$, et strictement inférieur à φ(n), appelé exposant de déchiffrement ; d peut se calculer efficacement par l'algorithme d'Euclide étendu.

Comme e est premier avec $\varphi(n)$, d'après le théorème de Bachet-Bézout il existe deux entiers d et k tels que $ed = 1 + k\varphi(n)$, c'est-à-dire que $ed \equiv 1 \ (mod\ \varphi(n))$: e est bien inversible modulo $\varphi(n)$.

Le couple (n, e) ou (e, n) est la clé publique du chiffrement, alors que sa clé privée est le nombre d, sachant que l'opération de déchiffrement ne demande que la clef privée d et l'entier n, connu par la clé publique (la clé privée est parfois aussi définie comme le couple (d, n) ou le triplet (p, q, d).

d) Chiffrement du message

Si M est un entier naturel strictement inférieur à n représentant un message, alors le message chiffré sera représenté par :

$$C \equiv M^e \ (mod\ n)$$

C est un entier naturel strictement inférieur à n.

e) Déchiffrement du message

Pour déchiffrer C, on utilise d, l'inverse de e modulo $(p-1)(q-1)$, et l'on retrouve le message clair M par :

$$M \equiv C^d \ (mod\ n)$$

5. Conclusion

Dans ce chapitre, nous avons présenté quelques notions fondamentales sur la cryptographie et son objectif, et les différentes techniques qu'il existe. Nous avons aussi mentionné la cryptographie classique et moderne ainsi que la description des algorithmes les plus utilisés.

Chapitre 2
Les images numériques

1. Introduction

Les premiers types d'images numériques sont apparus lorsque les appareils de numérisation ont été développés au milieu du XXe siècle, et grâce à ces scanners, il est devenu possible de numériser des images ordinaires et de les convertir en images numériques. Les images ne sont entrées dans le monde des ordinateurs que lorsque les ordinateurs ont été développés qui contiennent un dispositif d'affichage (écran), où il est devenu possible de revoir la plupart des images numériques.

2. Notions de base

2.1 Définition d'une image

L'image est définie comme étant une fonction f (x, y) à deux dimensions, où x et y sont les coordonnées spatiales, et l'amplitude à tous points (x, y) correspondant à l'intensité ou au niveau de gris. lorsque x, y et les valeurs d'intensité de f sont toutes des quantités finies et discrètes, nous appelons l'image une image numérique [17].

2.2 Image numérique

Une image numérique est un tableau de pixels, chaque pixel est codé par un nombre binaire pour un niveau de gris, ou par trois nombres binaires qui correspond à une nuance de rouge, de vert et de bleu (codage RVB) [18].

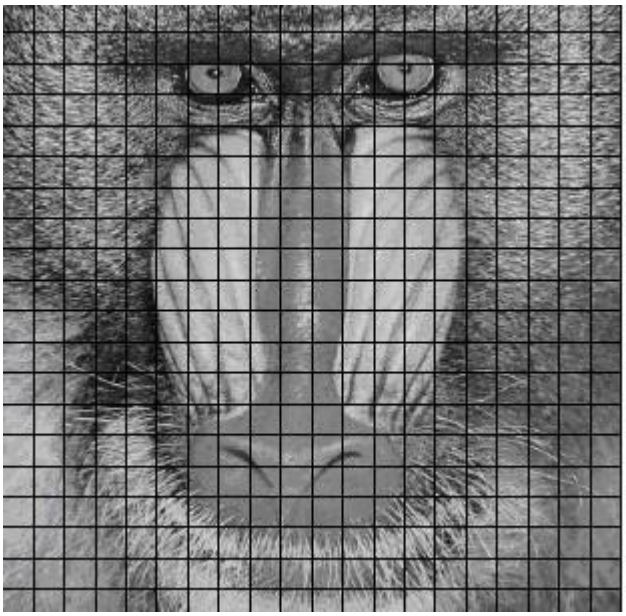


Figure 2.1: image numérique

2.3 Pixel

Une image numérique est constituée d'un ensemble de points appelés pixels (abréviation de Picture Elément) pour former une image. Le pixel représente ainsi le plus petit élément constitutif d'une image numérique. L'ensemble de ces pixels est contenu dans un tableau à deux dimensions constituant l'image [19].

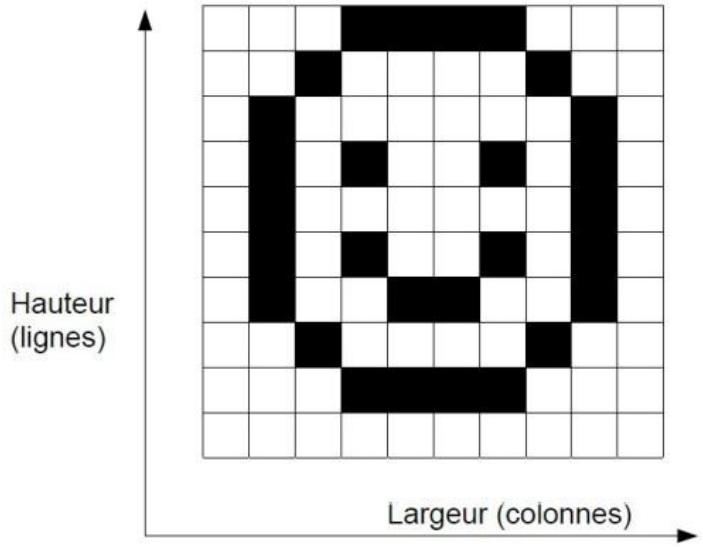


Figure 2.2 : Distribution des pixels

2.4 La définition

On appelle *définition* le nombre de points (pixels) constituant une image : c'est le nombre de colonnes de l'image que multiplie son nombre de lignes. Une image possédant 10 colonnes et 11 lignes auront une définition de 10x11 [19].

$$Définition = Résolution\ x\ Taille\ réelle\ d'impression$$

2.5 La taille :

La taille de l'image est la place qu'elle occupe dans le codage binaire, son unité est l'octet.

$$Taille = nombre\ d'octets\ par\ pixel \times définition$$

Exemple :

Une image, en niveaux de gris de définition 640×480 est codée en 24bits/pixel= 3 octets/pixel (car 1 octet = 8bits) sa taille sera : taille = nombre d'octets par pixel × définition = 3 × 640 × 480 = 9,22.105 octets [20].

2.6 La résolution

La résolution d'une image est définie par le nombre de pixels par unité de longueur (dpi (dot per inch = point d'encre par pouce) pour une imprimante ou ppp = pixels par pouce pour un fichier image). Cette résolution dépendra de la qualité de la numérisation.

$Résolution = définition / longueur$ [20].

Un pouce = 2.54 cm.

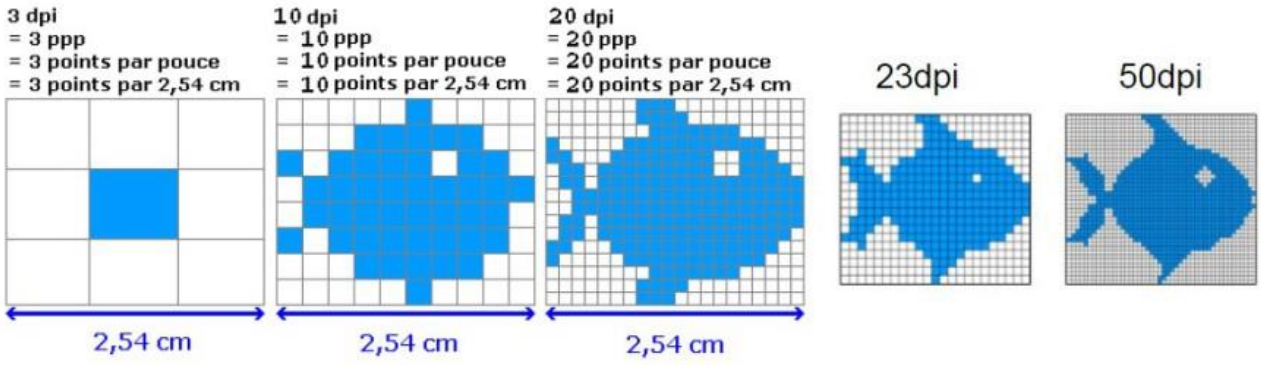


Figure 2.3 : Schéma explicatif de résolution d'une image

3. Les différents types d'images

3.1 Les images matricielles

Les images matricielles (ou image en mode point, en anglais « bitmap » ou « raster») sont celles que nous utilisons généralement pour restituer des photos numériques.

Elles reposent sur une grille de plusieurs pixels formant une image avec une définition bien précise. Lorsqu'on les agrandi trop, on perd de la qualité (« pixelisation ») [19].

3.2 Les images vectorielles

Ce sont des images dont la particularité est que chaque forme qui la compose est décrite mathématiquement à partir de points et de tangentes. Elles ne peuvent pas décrire une image trop complexe comme une photographie, mais sont tout à fait adaptées au rendu typographique, aux logos et autres formes composées de tracés simples [19].

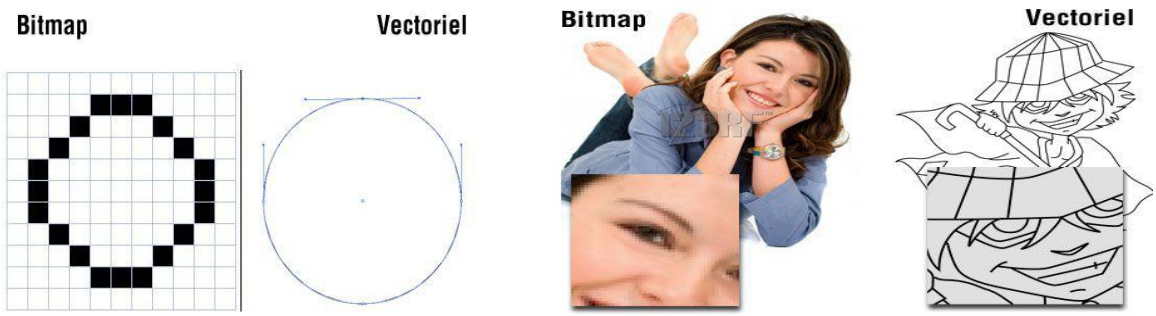


Figure 2.4 : Différence entre image matricielle(bitmap)et image vectorielle

4. Les différents modes de couleur des images

4.1 Mode bitmap (noir et blanc)

Avec ce mode, il est possible d'afficher uniquement des images en deux couleurs : noir et blanc. Il utilise une seule couche.

Codage en 1 bit par pixel (bpp) : => 2 possibilités : [0, 1]

Chaque pixel peut donc avoir 2 couleurs possibles : soit noir ou soit blanc [19].

1	1	1	1	1	1	1	1	1	1
1	1	1	0	0	0	0	1	1	1
1	1	0	1	1	1	1	0	1	1
1	0	1	1	1	1	1	1	0	1
1	0	1	0	1	1	0	1	0	1
1	0	1	1	1	1	1	1	0	1
1	0	1	0	1	1	0	1	0	1
1	0	1	1	0	0	1	1	0	1
1	1	0	1	1	1	1	0	1	1
1	1	1	0	0	0	0	1	1	1
1	1	1	1	1	1	1	1	1	1

Figure 2.5 : Codage binaire

4.2 Mode niveau de gris

A chaque pixel est affecté un nombre binaire variant de « 0 » (pour le noir) à «$2n - 1$ » (pour le blanc), avec n le nombre de bits pour chaque pixel. Il y aura alors « $2n$ » niveaux de gris [20].

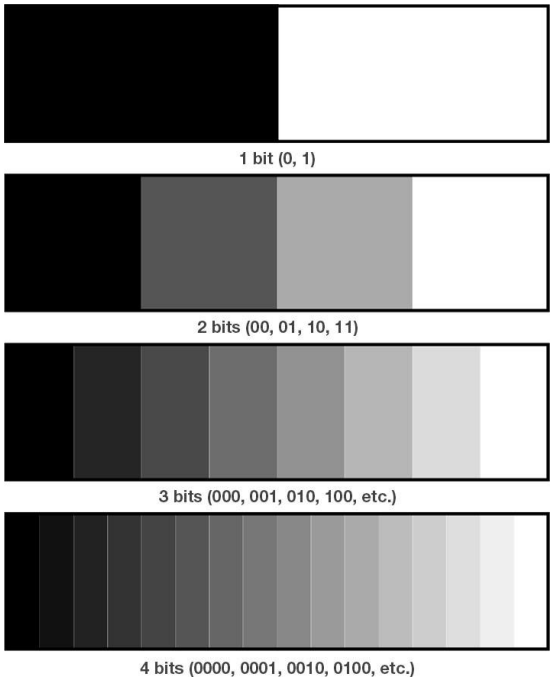


Figure 2.6 : Différentes nuances avec différent nombres de bits

Figure 2.7 : Image au niveau de gris

4.3 Le mode RVB

Le principe consiste à mélanger les 3 couleurs : rouge, vert et bleu (noté RVB ou RGB en anglais). A l'aide de ces 3 couleurs, on obtient toute une palette de nuances allant du noir au blanc. A chaque couleur est associé un octet (donc 256 niveaux de luminosité) de chacune des couleurs fondamentales [21].

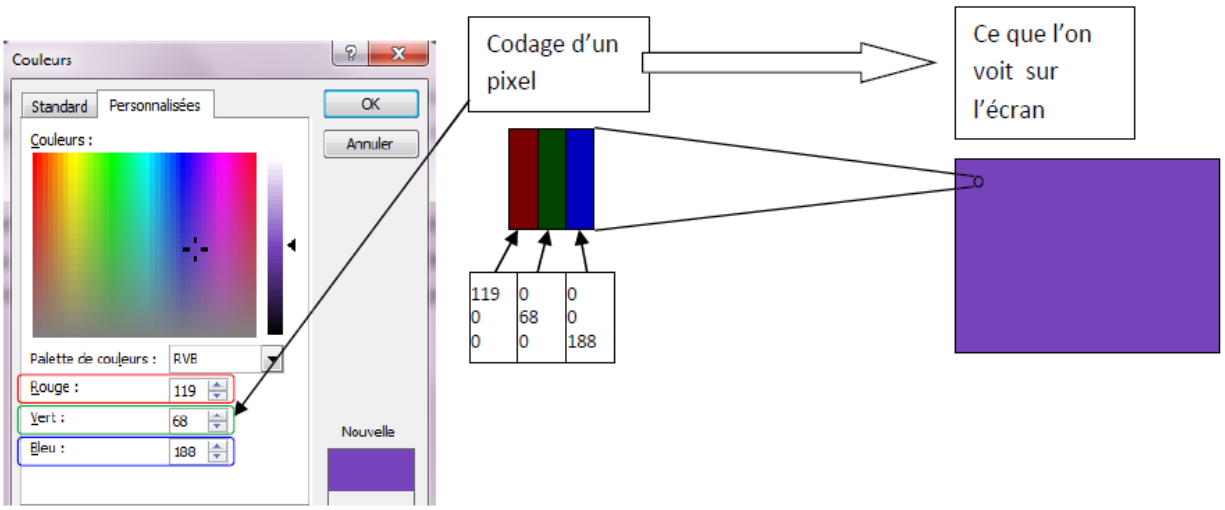


Figure 2.8 : Principe de codage RVB

Un pixel 'couleur' est alors codé avec 3 octets et on a alors la possibilité d'obtenir 224 possibilités de couleurs soit de l'ordre de 16 millions de couleurs différentes. On dit que les images obtenues sont en couleurs « vraies ». La qualité colorimétrique obtenue est celle d'une photographie argentique couleur.

La synthèse additive : c'est le phénomène qui se passe lorsqu'un un écran affiche une image par la lumière. On part du noir (lumière éteinte) et on va vert le blanc. L'addition du rouge, du vert et du bleu donne le blanc [20].

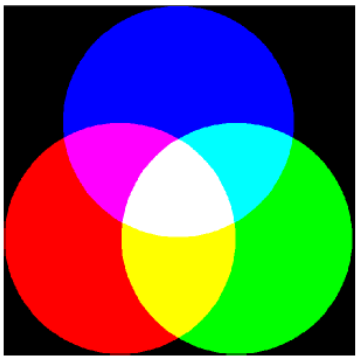


Figure 2.9 : le mode RVB

4.4 Le mode CMJN

Comme les écrans d'ordinateur ne peuvent afficher que du RGB, Photoshop sépare les images CMJN en 4 couches (Cyan, Magenta, Jaune et Noir ou chaque couleur est exprimée en

pourcentage) et converti le tout en RGB pour être affiché sur l'écran. Cependant pour L'utilisateur, le fichier possède bien 4 couches distinctes sur lesquels il est possible de travailler [20].

La synthèse soustractive : c'est le phénomène qui se passe lorsqu'on mélange des pigments colorés en peinture. On part du blanc (support papier) pour aller vers le noir. L'addition du Cyan, du Magenta et du Jaune donne le Noir.

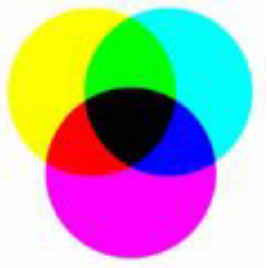


Figure 2.10 : Le mode CMJN

4.5 mode couleurs indexées

Ce mode permet d'obtenir jusque 256 couleurs fixes, définies à l'avance dans une palette. Il utilise qu'une seule couche.

Figure 2.11 : Image codée en couleurs indexée

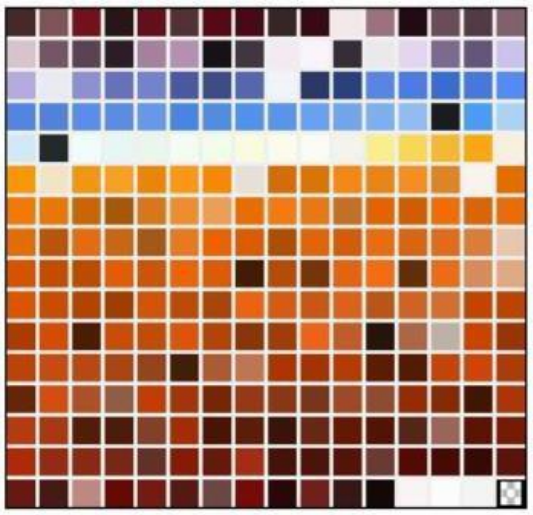


Figure 2.12 : Palette de 256 couleurs utilisées

5. Les formats d'images

5.1 Les formats matriciels [22]

a) **Bitmap (bmp)** : est un format d'image matricielle développe par Microsoft et IBM. C'est un format simple, ouvert et facilement utilisable par les logiciels mais il est peu utilisé sur le web à cause de la taille volumineuse de ses fichiers, la couleur de chaque pixel étant codée sans effort de compression.

b) **Joint Photographic Experts Group (jpeg ou JPG)** : est un format d'image ouvert compresse pour des images de type photographie (16 millions de couleurs). Le principe de compression JPEG est de coder la couleur de rectangles dont les pixels ont la même couleur (compression sans perte) ou des couleurs très proches (compression avec perte, taux de qualité paramétrable).

c) **Graphics Interchange Format (GIF)** : est un format d'image ouvert compresse pour des images de type dessin. Il permet de définir une couleur de fond transparente, de proposer un mode d'affichage entrelace (aperçu de l'image qui se précise en cours de téléchargement) et de créer des images animées. Les couleurs d'une image sont définies sur une palette de 256 couleurs choisies parmi 16 millions de couleurs possibles : c'est le principe de base de la compression GIF, dite en couleurs indexées

d) **Portable Network Graphics (png)** : est un format d'image ouvert compresse. Il effectue une compression en couleurs indexées, mais la palette n'est pas limitée à 256 couleurs.

5.2 Les formats vectoriels :

a) **EPS :** Le format **Encapsulated PostScript** (**EPS**) est un format ouvert créé par le système Adobe en langage PostScript qui permet de décrire des images qui peuvent être constituées d'objets vectoriels ou bitmap [23].

b) **SVG** : signifie **Scalable Vector Graphics**, en clair c'est un format de données utilisé pour définir des graphiques vectoriels. Il est inspiré des formats VML (soutenu entre autres par Microsoft) et PGML (soutenu par Adobe et Sun). Contrairement aux deux précédents, SVG est recommandé par la W3C. Ce format est basé sur du XML et permet de définir des éléments graphiques pour le web. Il est surtout utilisé pour l'affichage de graphiques mais également pour les applications mobiles [24].

c) **FLA** : Les fichiers FLA sont des fichiers de projet créés dans Adobe Flash ou Adobe Flash Professional. L'ouverture du fichier dans le programme correspondant permet à l'utilisateur d'apporter des modifications à l'animation Flash à l'intérieur du fichier de projet ou de l'enregistrer dans un format adapté au web [25].

d) **PDF** : Le Portable Document Format, communément abrégé en PDF, est un langage de description de page présenté par la société Adobe Systems en 1992 et qui est devenu une norme ISO en 2008.

La spécificité du PDF est de préserver la mise en page d'un document polices de caractère, images, objets graphiques, etc. telle qu'elle a été définie par son auteur, et cela quels que soient le logiciel, le système d'exploitation et l'ordinateur utilisés pour l'imprimer ou le visualiser [26].

e) **PICT** : est un format de fichier graphique créé par Apple comme métafichier standard pour ses premiers Macintosh. Il peut contenir des informations graphiques bitmap ou vectorielles, ainsi que quelques champs de texte. C'est également le format natif de QuickDraw Manager [27].

6. Méthodes de cryptage d'images

dans la plupart des cas ne sont pas applicables au codage d'images, et cela est dû à la différence de taille car la quantité d'informations dans l'image est beaucoup plus grande que celle des données de texte en plus de la différence de perte de données lors de l'application de la technologie de compression, contrairement à l'image, l'utilisation d'une méthode de compression avec perte est présente Lors de l'encodage de texte, c'est ce qui a poussé les chercheurs à étudier plusieurs méthodes d'encodage des images .En revanche, les algorithmes d'encodage d'images peuvent être classés selon le domaine d'application: méthodes de champ mécanique ou de domaine fréquentiel .Méthodes de cryptage d'images [28].

6.1 Méthode dans le domaine spatial

Le schéma de cryptage s'applique au niveau de l'image lui-même dans le domaine spatial et les méthodes de cette classe sont basées sur un traitement des pixels directement dans l'image. Le codage dans ces algorithmes détruit la corrélation entre les pixels et rend l'image chiffrée incompressible. Les pixels de l'image peuvent être récupérés par le processus inverse sans perdre aucune information.

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

- Dans la première catégorie, un pixel est considéré comme le plus petit élément, et une image numérique est considérée comme un ensemble de pixels.

- Dans la deuxième classe, un pixel peut être en outre divisé en bits, sur lesquels des opérations au niveau de bits sont effectuées. Par exemple, un pixel dans une image en niveaux de gris est généralement constitué de 8 bits [28].

6.2 Méthode dans le domaine fréquentiel

Dans le domaine fréquentiel, les schémas de cryptage dépendent de la modification de la fréquence de l'image à l'aide de la conversion, de sorte qu'une perte d'informations se produit lors de la reconstruction des pixels de l'image d'origine par le processus de décryptage [28].

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

7.1 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. Une condition nécessaire, mais pas suffisante à un schéma de cryptage pour qu'il soit sûr est que l'espace clés soit suffisamment grand pour assurer la sécurité contre l'attaque par force brute [28].

7.2 L'histogramme

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

- A l'acquisition, il permet de contrôler et affiner les réglages de prise de vue.
- Pour le traitement, il permet de corriger ou modifier l'exposition de l'image, ainsi que l'échelle des couleurs.

Par exemple : améliorer le contraste, corriger une image sous-exposée, renforcer la composante rouge, corriger la non-linéarité du capteur....

- En utilisant judicieusement l'histogramme, on peut faire apparaître les détails et les nuances acquises par le capteur et présentes dans le fichier, mais nos visibles à l'œil [29].

7.2.1 Histogramme des images en niveau de gris

Il indique pour chaque valeur entre le noir (0) et le blanc (255), combien il y a de pixels de cette valeur dans l'image ; en abscisse (axe x) : le niveau de gris (de 0 à 255); en cordonnée (axe y) : le nombre de pixels.

Les pixels sombres apparaissent à gauche de l'histogramme, les pixels clairs à droite de l'histogramme et les pixels gris au centre de l'histogramme [29].

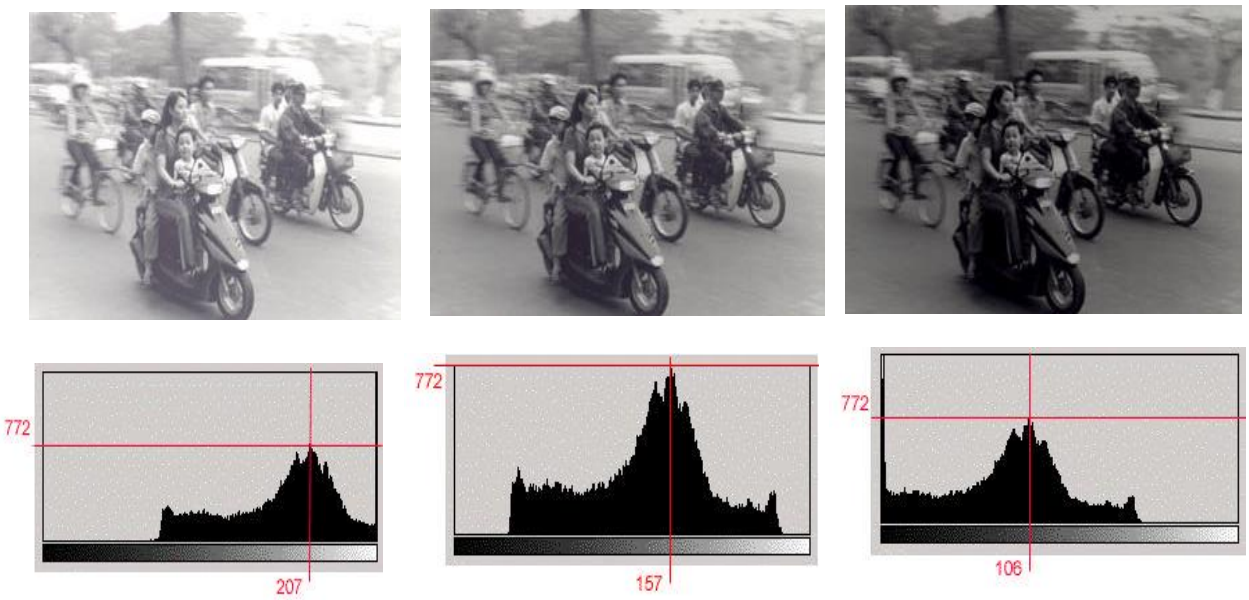


Figure 2.13 : exemple d'histogrammes pour une même image "plus ou moins bien exposée" [29].

7.2.2 Histogramme des image couleurs

Pour les images couleurs, plusieurs histogrammes sont utilisés :

- L'histogramme des luminances
- Les 3 histogrammes de chacune des composantes R.V,B [29].

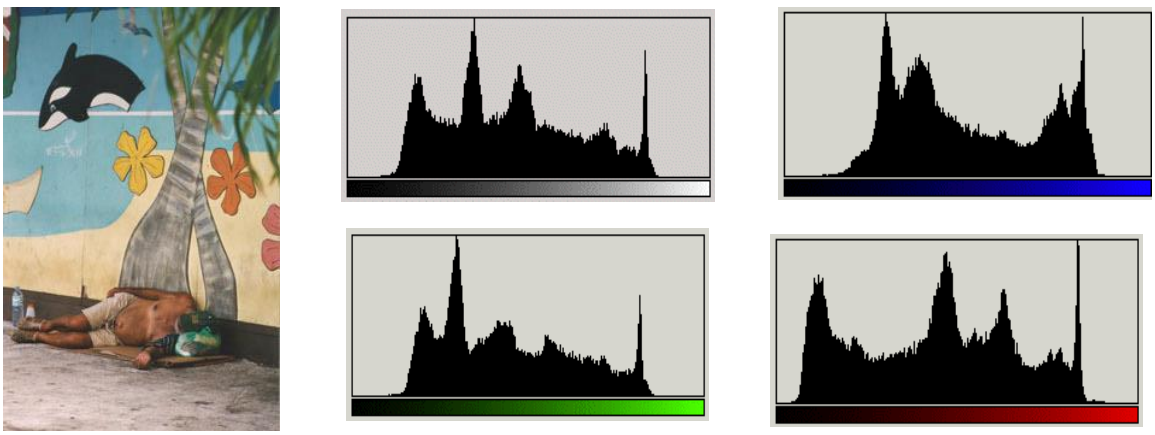


Figure 2.14 : Image colorée correspondant à des histogrammes différents pour chaque composante [29].

Dans un contexte de chiffrement d'image, l'histogramme de l'image chiffrée doit être uniforme pour assurer la sécurité contre l'attaque de texte en clair connue, autrement dit l'attaquant ne peut pas extraire information à partir de cet histogramme

Par exemple, La Figure 2.15 est l'histogramme de l'image originale et la Figure 2.16 est l'histogramme de l'image cryptée. La Figure 2.16 montre que l'histogramme plus uniforme qui est hautement souhaitable.

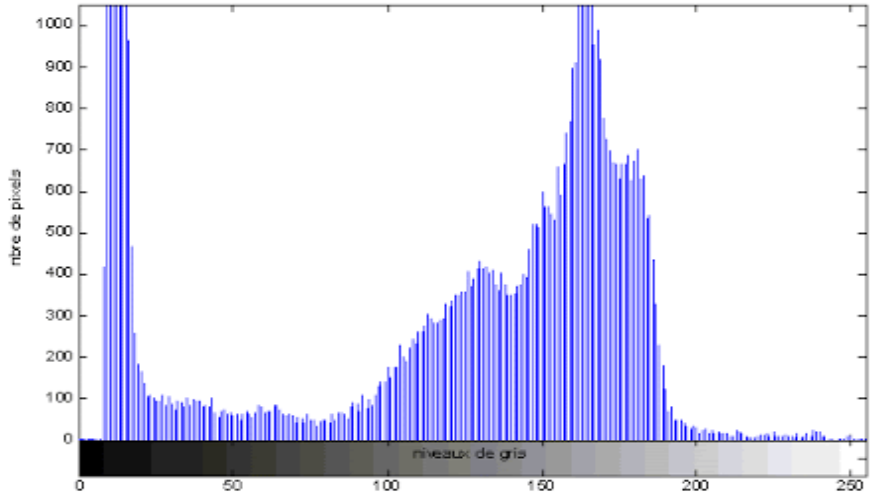


Figure 2.15 : Histogramme d'une image originale

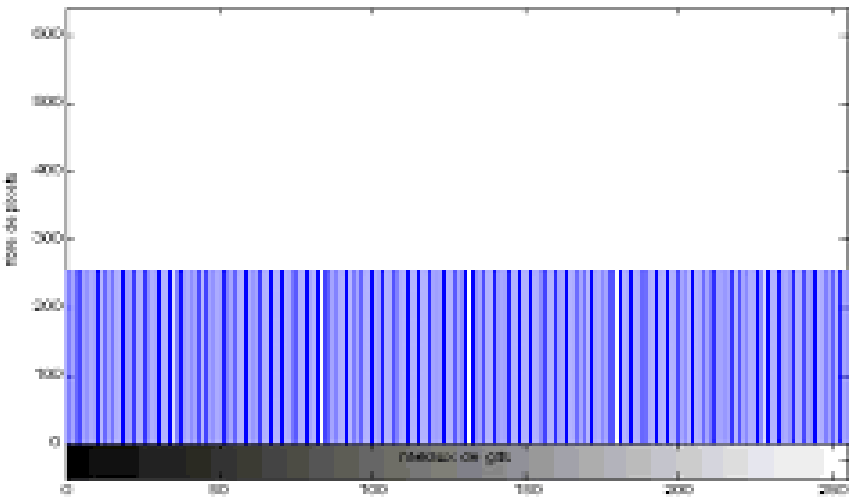


Figure 2.16 : Histogramme d'une image cryptée

7.3 La corrélation entre les pixels adjacents

La corrélation est une technique qui permet de comparer deux images pour estimer les déplacements des pixels d'une image par rapport à une autre image de référence. Les pixels

adjacents d'une image standard ont une forte corrélation. Un bon schéma de cryptage d'image doit supprimer une telle corrélation afin d'assurer la sécurité contre l'analyse statistique. Afin de tester la corrélation entre deux images ont choisi au hasard 10 000 paires de deux pixels adjacents dans les trois directions ; horizontal, vertical et diagonal à partir des composants R, G, B de l'image claire et son image chiffrée et les coefficients de corrélation de chaque paire ont été calculées en utilisant les formules suivantes [28] :

$$r = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

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

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

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

Tel que :

r : la corrélation.

cov : la covariance.

E : l'espérance mathématique.

D : la variance.

x, y : les valeurs des pixels des images.

7.4 L'entropie

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

L'entropie est donnée par la formule suivante :

$$H(m) = -\sum_{i=0}^{2^n-1} p_i \log_2(p_i)$$

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

Donc pour un chiffrement d'images au niveau de gris, La valeur de l'entropie doit être très proche de 8, Parce que si l'entropie est inférieure à 8, il existe des degrés de prévisibilité, donc

on ne peut pas assurer la sécurité contre l'analyse statistique. De sorte que l'entropie devrait idéalement être 8 [31].

8. La cryptographie basée sur la théorie du Chaos

8.1 Les systèmes chaotiques

Chaos est un nom dérivé du mot grec « Xaos », qui signifie un état sans ordre ni prévisibilité. Le système chaotique est un système simple, non linéaire, déterministe et dynamique qui affiche un caractère aléatoire et explique un comportement complètement inattendu. Il est utilisé en cryptographie en raison de la nature de ses caractéristiques aléatoires et la grande sensibilité aux conditions initiales. Il a également été utilisé pour générer des nombres aléatoires, ou un petit changement de sa valeur initiale, provoque l'obtention d'une séquence complètement différente.

On peut faire plusieurs conclusions sur la base des caractéristiques d'un système à comportement chaotique :

1. Le système est non linéaire, ce qui signifie que la sortie n'est pas directement proportionnelle à l'entrée, et parce que le système non linéaire et dynamique, il est sensible aux conditions initiales.
2. Le système peut changer à des moments discrets ; il a des règles sous-jacentes déterministes (plutôt que probabilistes). Donc, les états du système doivent suivre ces règles il n'y a donc pas de composant aléatoire dans le système [34].

8.2 La carte chaotique logistique

De nombreuses méthodes ont été développées pour concevoir des algorithmes de cryptage de l'image en utilisant des cartes chaotiques « Chaotic Maps en English ». La carte logistique est une cartographie polynomiale, ou le comportement de cette carte est basé sur une très simple équations non linéaires dynamiques.

L'équation de la carte chaotique logistique est donnée par [31] :

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

Où X variable dans l'intervalle [0, 1] et n est le nombre d'itérations, et r est un nombre définit dans l'intervalle [0,4].

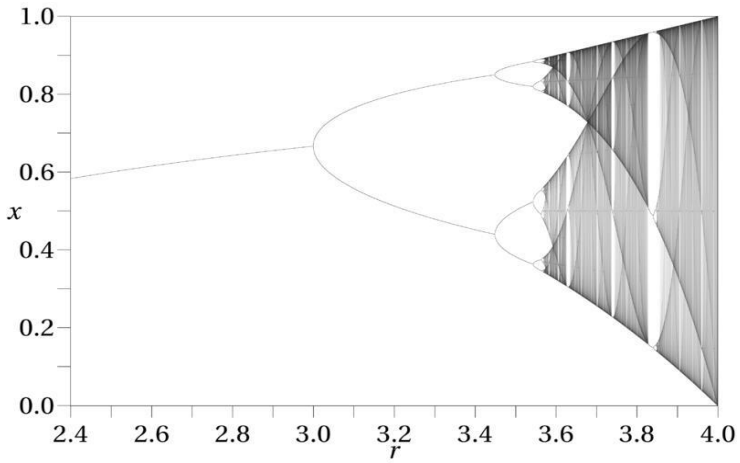


Figure 2.17 : Le diagramme de la bifurcation de la carte logistique [31].

9. Conclusion

Dans la première partie de ce chapitre, nous avons présenté quelques notions de base sur les images numérique, ses types, les différents modes de couleur des images ainsi que leurs formats. Dans la deuxième partie, nous avons décrit les techniques de cryptage d'image suivi par les outils élémentaires d'analyse d'un algorithme de cryptage d'image. A la fin nous avant présenté l'utilisation des cartes logistique chaotique dans la cryptographie des images.

Chapitre 03

La cryptographie par la carte chaotique logistique

1. Introduction

Les chercheurs de cryptographie ont été proposés plusieurs techniques de chiffrement d'images numériques. Parmi eux il y a des algorithmes qui basés sur des théories comme la théorie de chaos et Fibonacci, et aussi des algorithmes qui basés sur différentes technologies comme : le séquençage de l'ADN, l'optique, l'automate cellulaire et la transformation de Fourier, et beaucoup d'autres techniques.

Dans notre mémoire nous avons proposé d'utiliser deux algorithmes de cryptographie ; dans le premier algorithme nous avons utilisé une clé aléatoire pour le cryptage, alors que le deuxième algorithme est basé sur la carte logistique chaotique pour générer une clé pseudo aléatoire. A la fin nous avons présenté une comparaison entre ces deux algorithmes de cryptographie pour découvrir ce qui assure la protection maximale.

2. Les Méthodes utilisées

Dans le schéma proposé, nous avons utilisé deux algorithmes, dans le premier algorithme nous avons généré un flux de clés aléatoire avec la même taille de l'image originale, puis appliquer l'opération XOR élément par élément entre l'image en clair et le flux de clés aléatoire généré, afin d'obtenir une image cryptée.

Dans le deuxième algorithme on a utilisé la formule mathématique de carte logistique Chaotique pour générer un flux de clé pseudo aléatoire sous forme d'une matrice de la même taille de l'image originale, puis faire l'opération XOR élément par élément entre l'image en clair et la matrice clé.

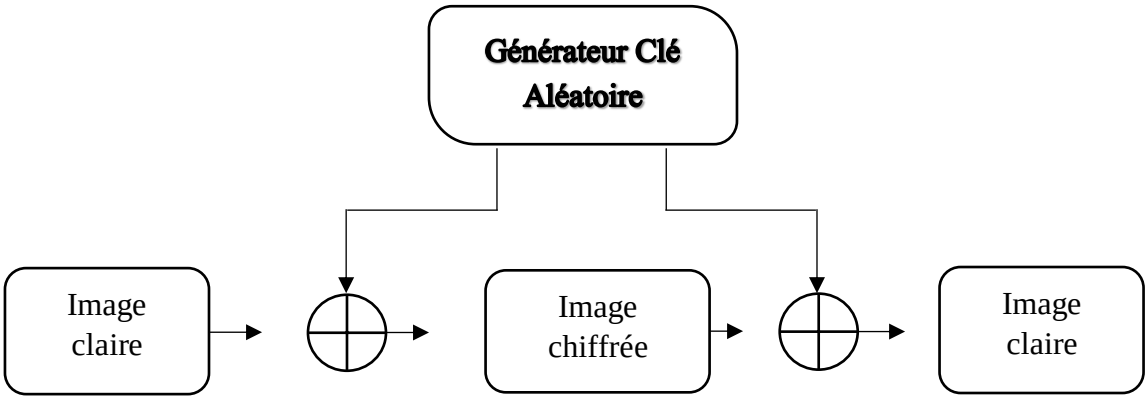


Figure 3.1 : Schéma de chiffrement utilisé

2.1 Générateur un flux de clés aléatoire

Pour le premier algorithme on a générer la clé aléatoire par la commande rand sous Matlab

Le deuxième générateur pseudo aléatoire est basé sur la carte logistique Chaotique qui utilise la formule mathématique suivante :

$$X_{n+1} = rX_n(1 - X_n) \qquad 2.1$$

Comme nous le savons, la séquence chaotique basée sur la carte logistique donne des valeurs réelles qui doivent être binarisées. Cela peut être fait de l'une des deux manières suivantes:

$$f(x) = \begin{cases} 1 & X \geq 0{,}5 \\ 0 & X < 0{,}5 \end{cases}$$

$$f(x) = \begin{cases} 1 & X \geq \tau \\ 0 & X < \tau \end{cases} \quad avec\ \tau = moy(f(x))$$

Les paramètres initiaux utilisées dans notre travaille sont :

r = 3.9999998 et $0 < X \leq 1$.

2.2 Fonction de chiffrement

1) La cryptographie par la clé aléatoire

Pour le premier algorithme nous avons suivi les étapes suivantes :

1- Générer un flux de clé aléatoire, mais à condition que le flux généré doive être même taille d'image en clair n x m.
   a. Arrondi toutes les valeurs de la clé à valeur entier.
   b. Convertir la clé sur 8bits.
2- Convertir l'image en claire sur 8 bits.
3- Faire l'opération XOR entre l'image en claire et le flux de clé aléatoire Pour obtenir un flux de données chiffrés (image chiffrée).

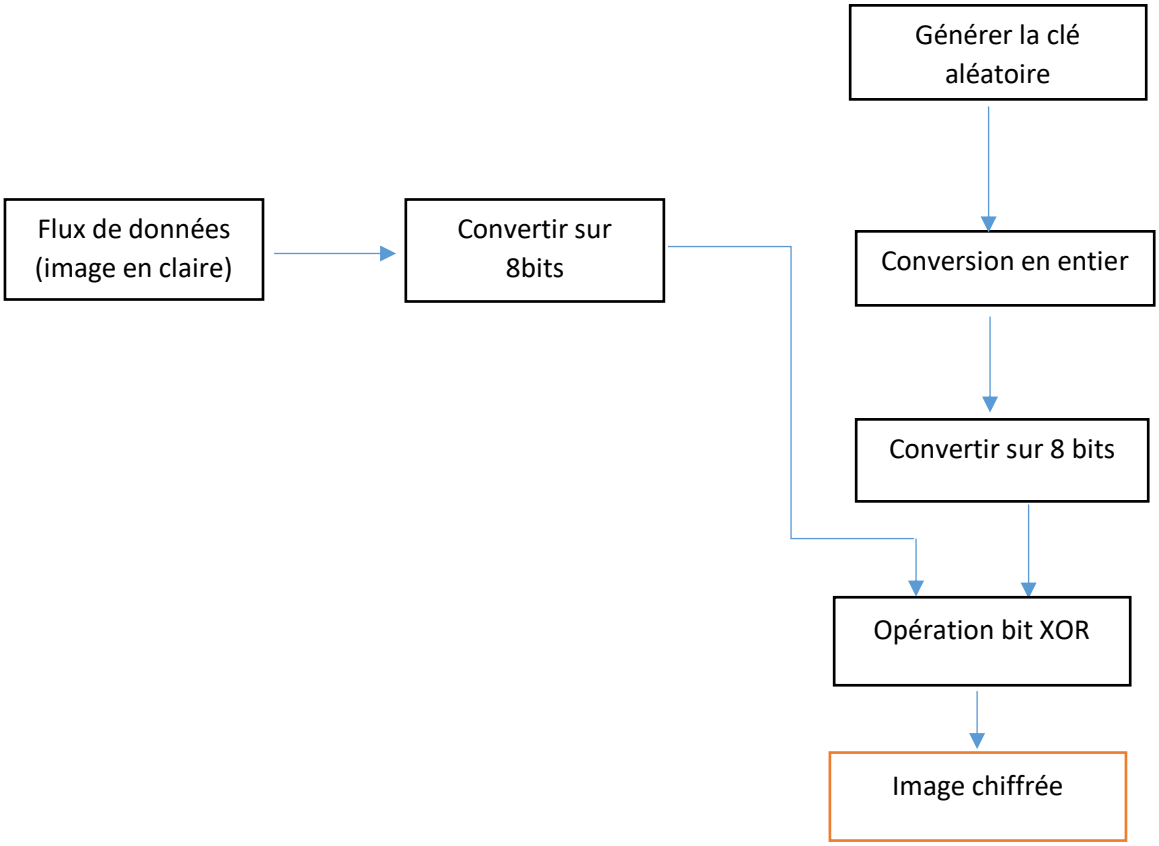


Figure 3.2 : Fonction de cryptage par la clé aléatoire

2) La Cryptographie par la carte chaotique logistique

Pour le premier algorithme nous avons suivi les étapes suivantes :

1- Générer un flux de clé pseudo aléatoire utilisant la carte chaotique logistique
   a. Définissez les valeurs initiales et les paramètre pour la Carte Logistique Chaotique (r, X).
   b. Générer un flux de nombre binaire à partir de la formule mathématique de la carte logistique chaotique de taille $n \times m \times 8$.
   c. Crée une séquence des nombres binaire de 8 bits.
   d. Crée une matrice clé de la même taille de l'image claire.
   e. Convertir le flux générer sur 8bits.
2- Convertir l'image en clair à un flux de données sur 8bits.
3- Faire l'opération XOR entre l'image en claire et le flux de clé pseudo aléatoire généré.

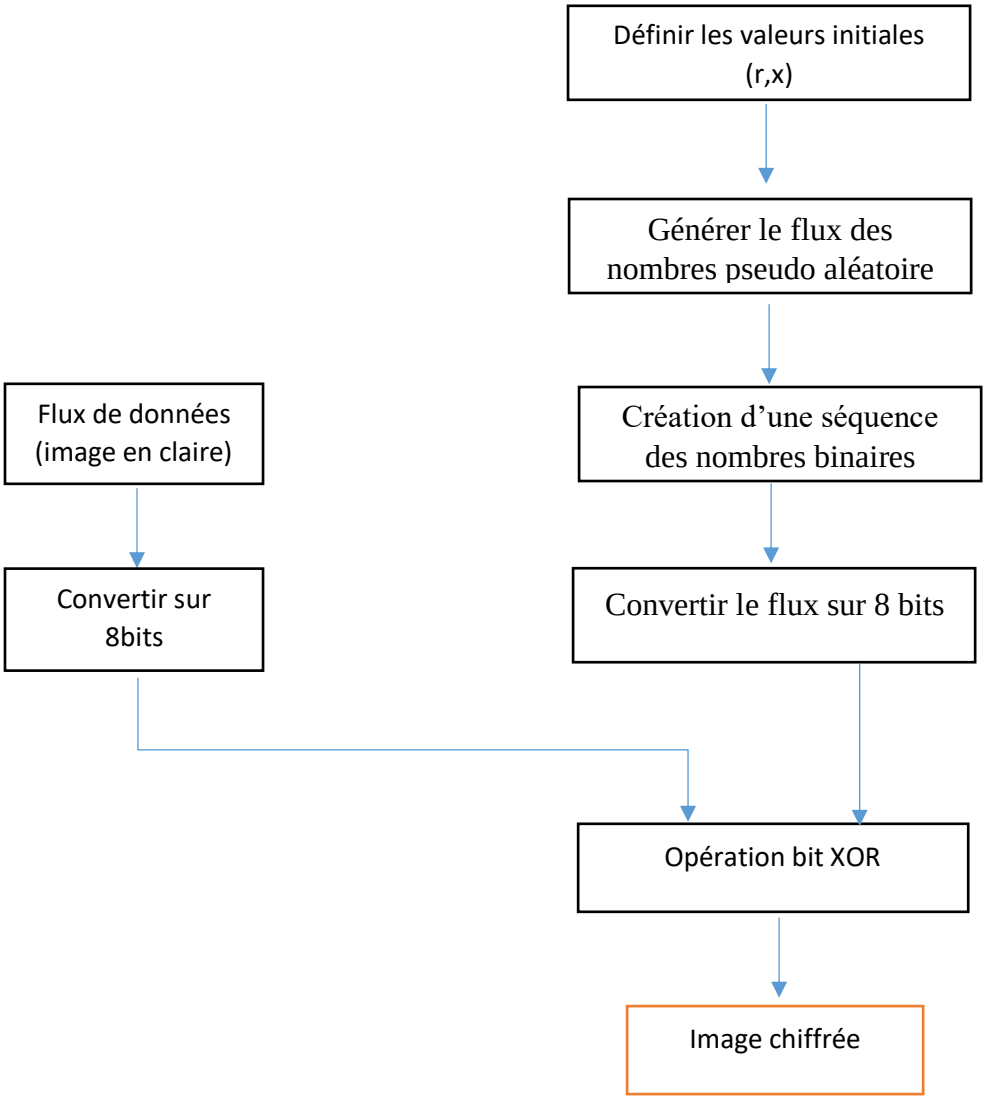


Figure 3.3 : Fonction de cryptage par la carte chaotique logistique

2.3 Fonction déchiffrement

1) Le décryptage par la clé aléatoire

Pour le déchiffrement, la clé doit être remise au destinataire, par exemple si on veut crypter une image d'une taille 256X256, il faut utiliser une clé de la même taille de l'image c.-à-d. la taille de la clé soit 256×256 ; c'est trop pour envoyer une clé d'une taille 256×256 au destinataire, cette difficulté considéré parmi les inconvénients de cet algorithme.

2) Le décryptage par la carte chaotique logistique

1- Définissez les valeurs initiales et les paramètres pour la Carte Logistique Chaotique (r, X).

a. Générer un flux de nombre binaire à partir de la formule mathématique de la carte logistique chaotique de taille n×m×8.

b. Crée une séquence des nombres binaire de 8 bits.

c. Crée une matrice clé de la même taille de l'image claire.

d. Convertir le flux générer sur 8bits.

e. Convertir l'image en clair à un flux de données sur 8bits.

2- Faire l'opération XOR entre l'image chiffrée et le flux de clé pseudo aléatoire généré.

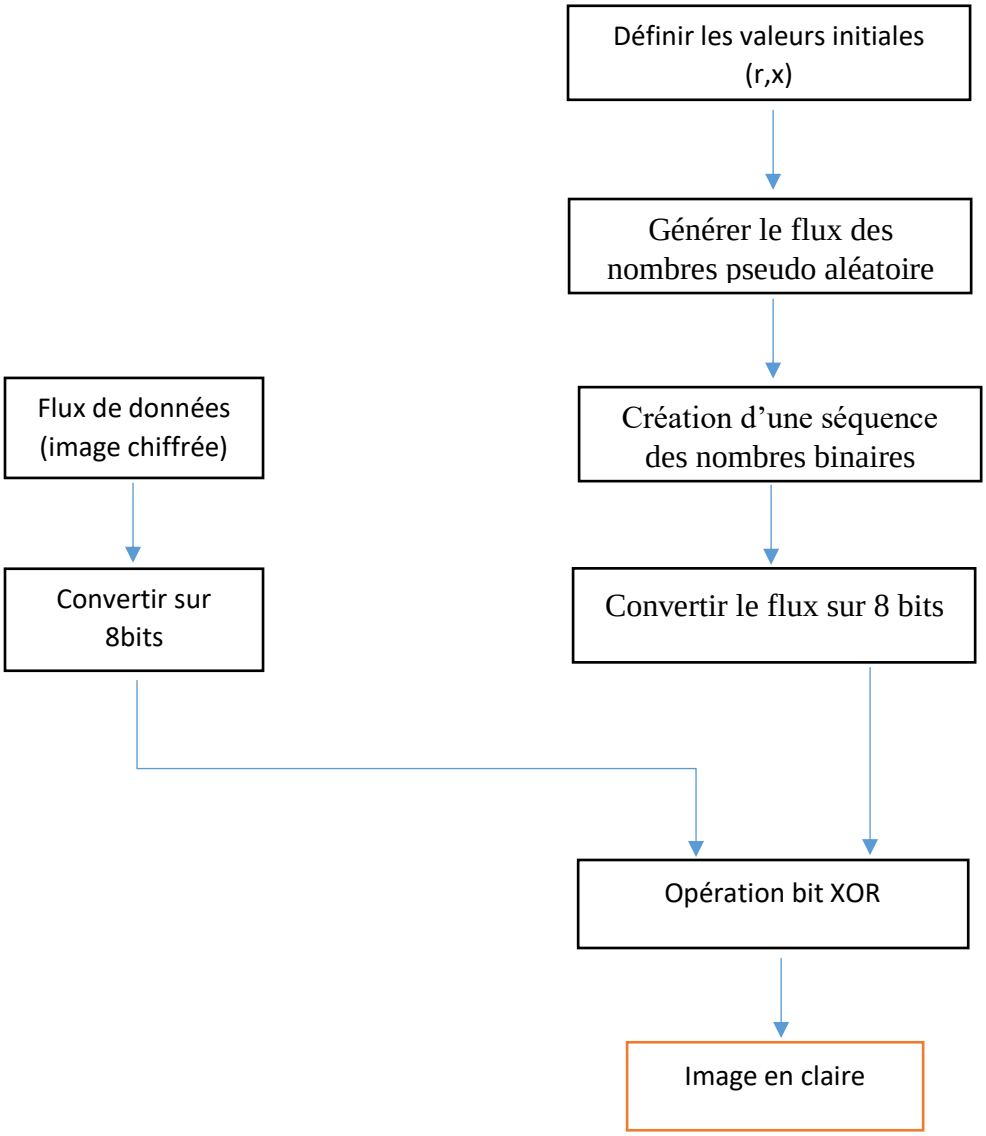


Figure 3.4 : Fonction de décryptage par la carte chaotique logistique

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 : University of Waterloo [36] Et University of Wisconsin-Madison [37]. Les images médicales sont prises à partir d'un site Web [38].

3.2 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 les deux algorithmes utilisés.

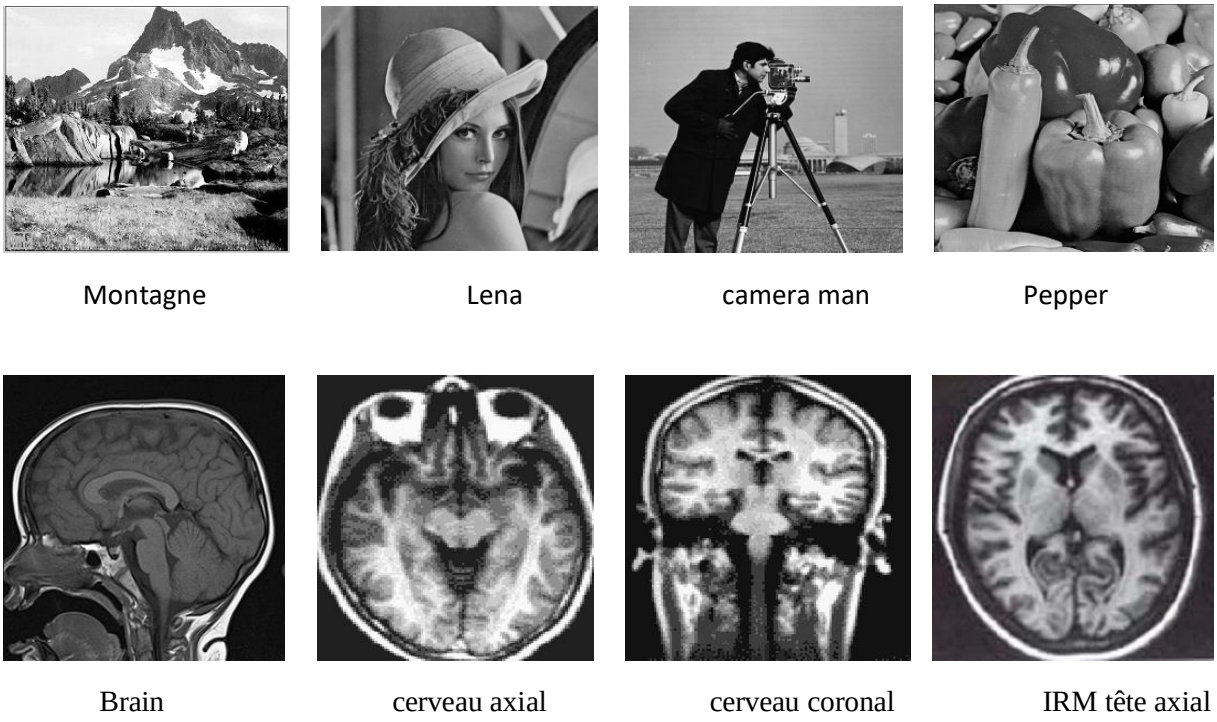


Figure 3.5 : les images originales

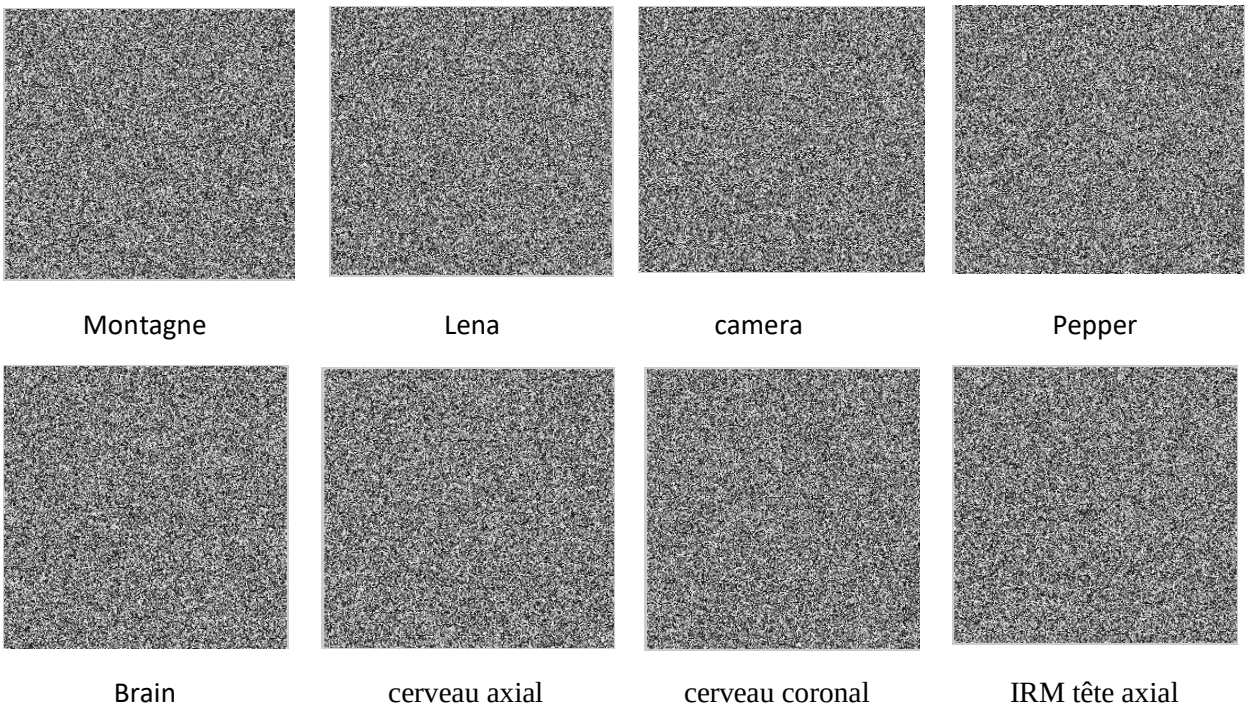


Figure 3.6 : les images cryptées par la clé aléatoire

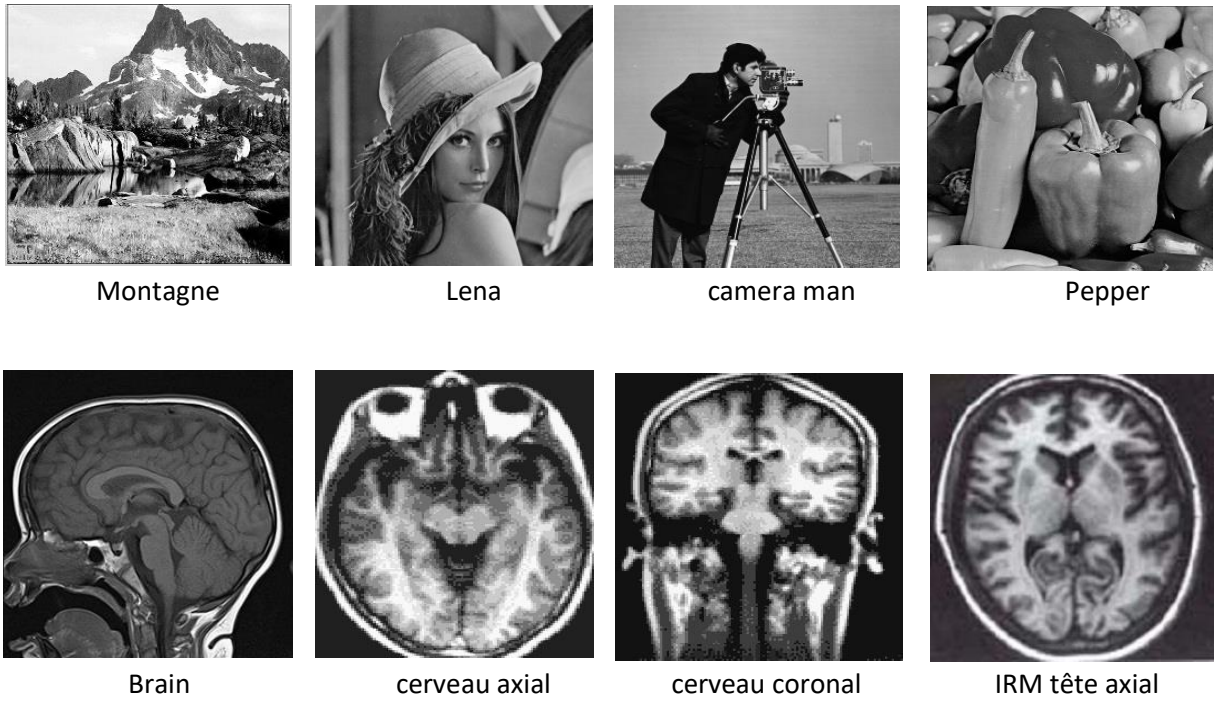


Figure 3.7 : les images décryptées par la clé aléatoire

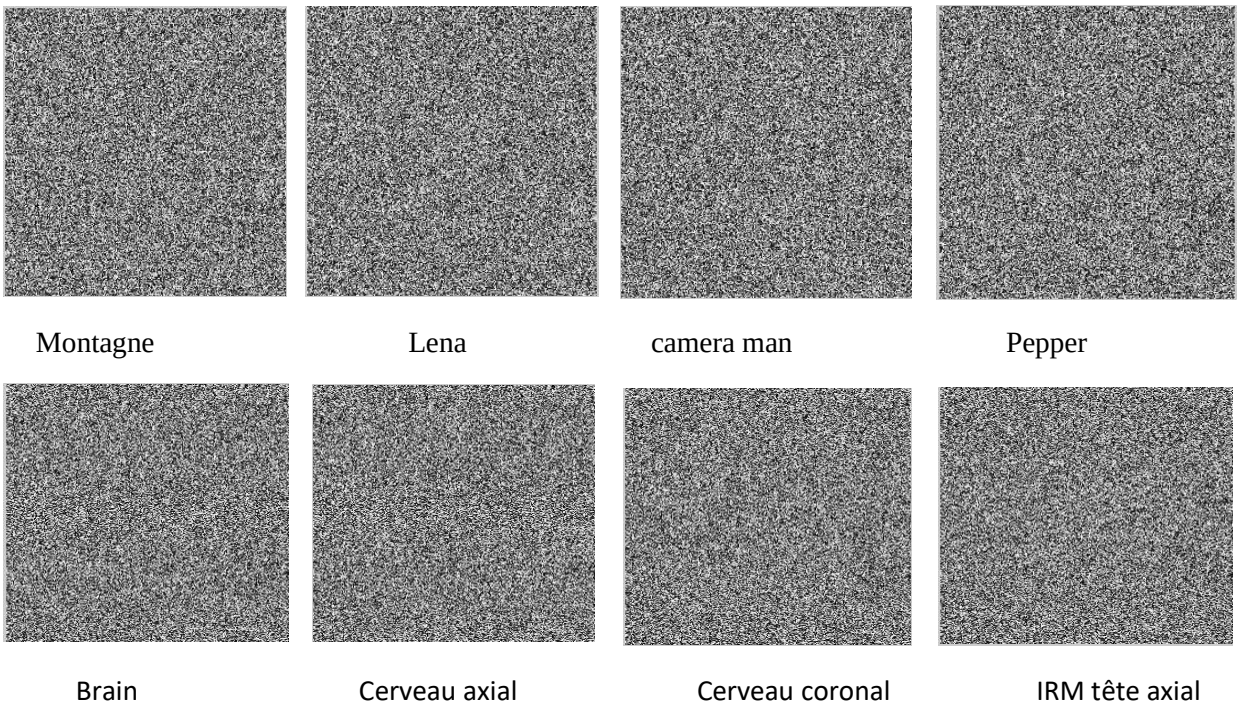
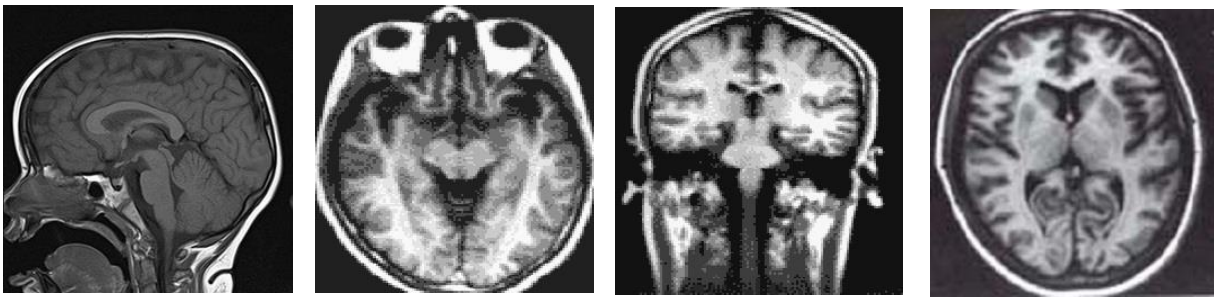


Figure 3.8 : les images cryptées par la carte chaotique logistique

montagne Lena camera man Pepper



Brain cerveau axial cerveau coronal IRM tête axial

Figure 3.9 : les images décryptées par la carte chaotique logistique

4. Critères d'évaluation

Un bon système de cryptage doit être protégé contre toutes les attaques possibles, donc il y a des simulations numériques qui ont été effectuées en utilisant différentes mesures d'évaluation pour montrer la sécurité et l'efficacité de l'algorithme utilisé. Nous allons présenter les plus important comme : l'espace de clés, L'histogramme, L'entropie, La corrélation entre les pixels adjacents.

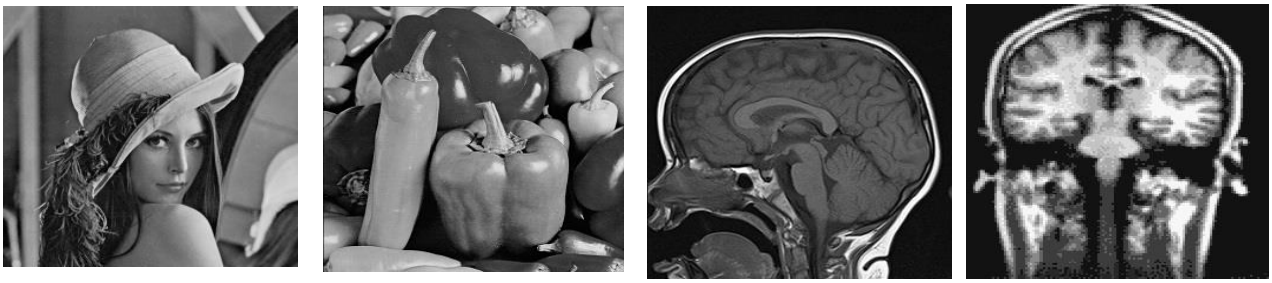
4.1 L'espace de clé

Un bon algorithme de chiffrement doit être sensible aux clés de chiffrement et l'espace clé doit être suffisamment grand et plus longue que la taille de l'image pour rendre les attaques impossibles. Dans notre travaille, les clés utilisées pour les deux algorithmes se sont des nombres aléatoires, la taille des clés utilisés 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 :

$$2^{8\times256\times256}.$$

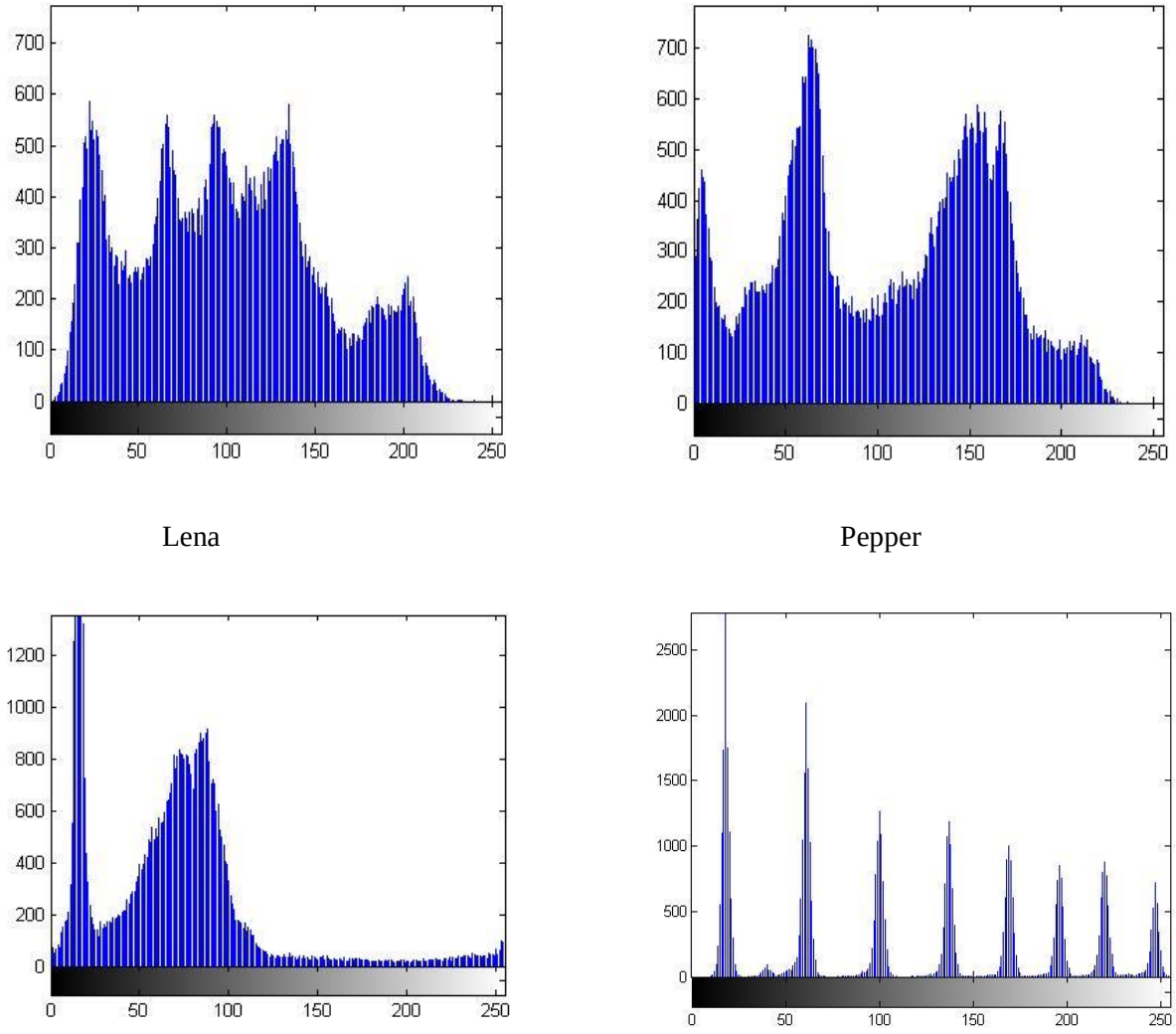
4.2 L'histogramme

Quatre images de teste ont été utilisées pour l'analyse : Lena, Pepper et deux images médicales : Brain, cerveau coronal. Les tracés des histogrammes des images et les images chiffrées sont montrés dans les figures ci- dessous :



Lena Pepper Brain cerveau coronal

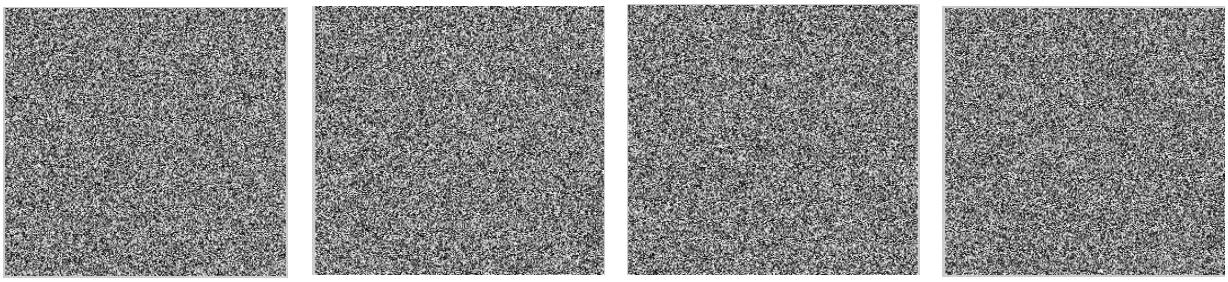
Figure 3.10 : les images originales



Lena Pepper

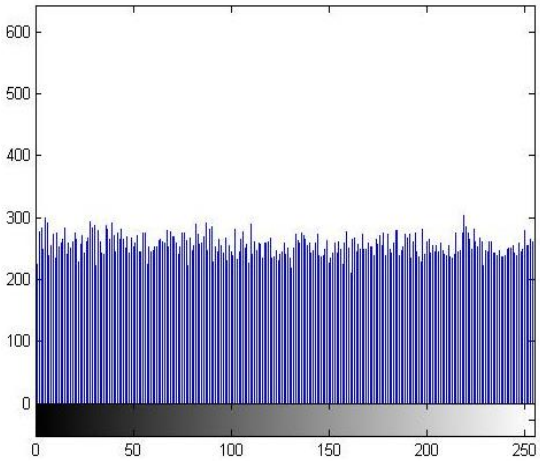
Brain Cerveau coronal

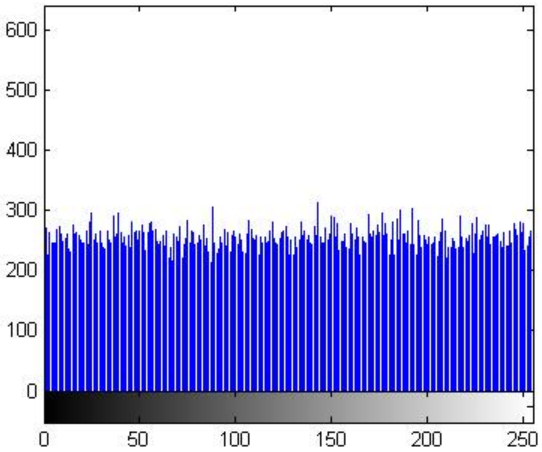
Figure 3.11 : l'histogramme des images originales



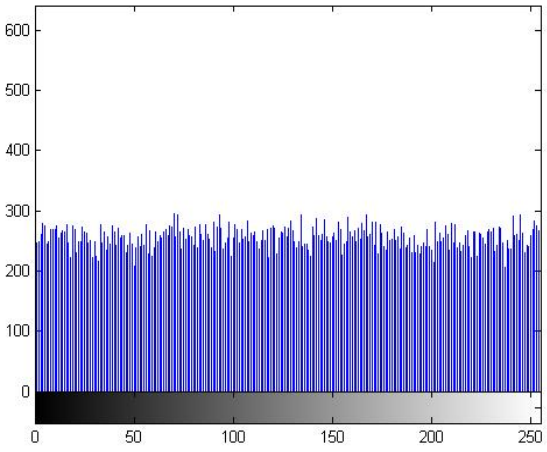
Lena Pepper Brain cerveau coronal

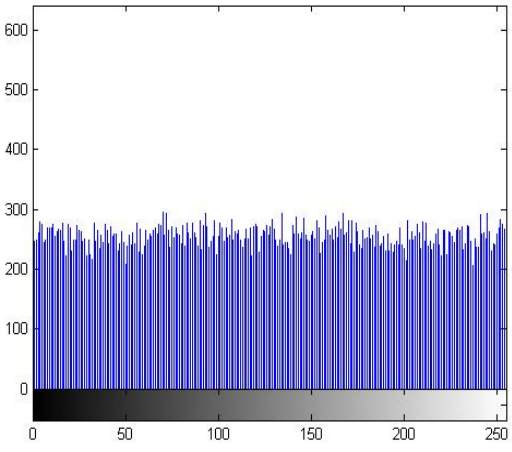
Figure 3.12 : les images cryptées par la clé aléatoire





Lena Pepper

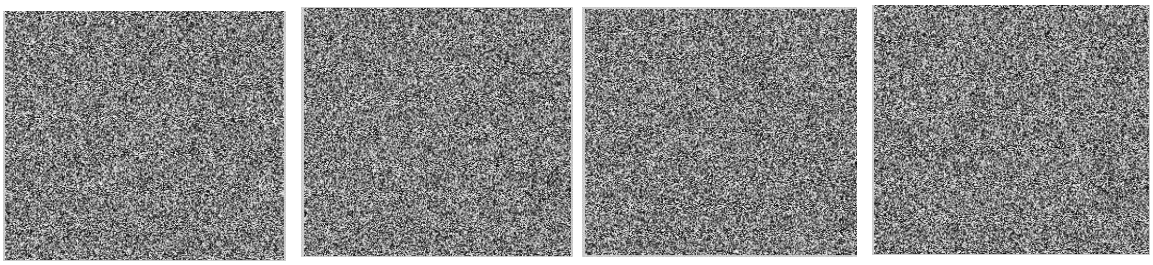




Brain Cerveau coronal

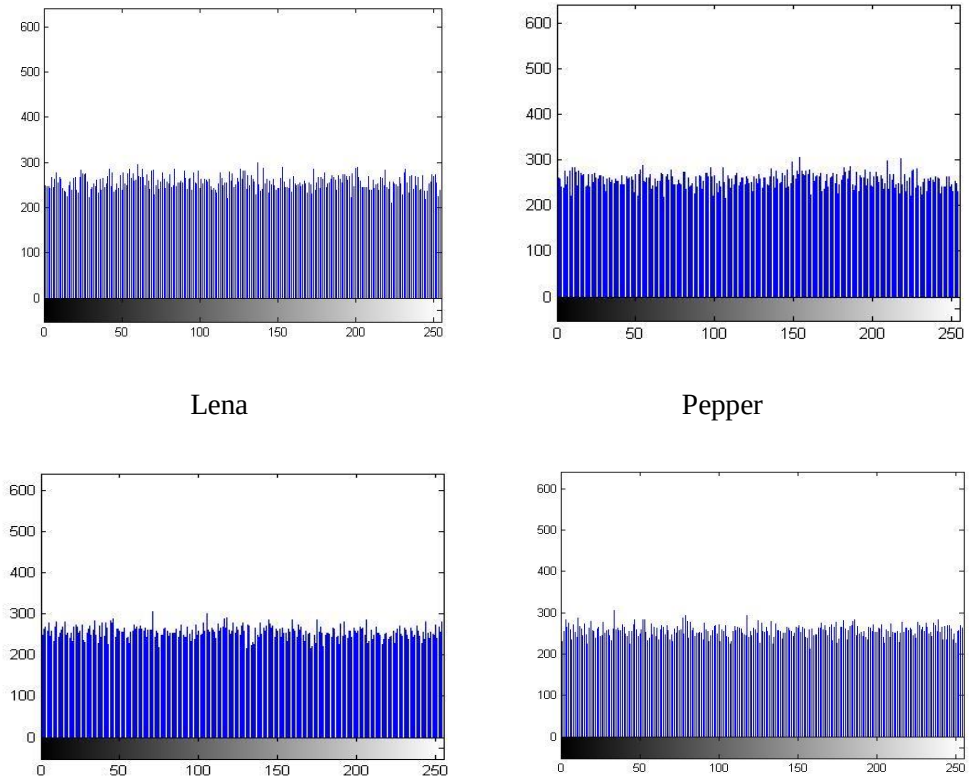
Figure 3.13 : l'histogramme des images cryptées par la clé aléatoire

Les résultats montrent que les histogrammes des images chiffrées par clé aléatoire sont uniformes après le cryptage. Par conséquent l'attaquant ne peut pas extraire l'information à partir de l'histogramme de l'image cryptée.



Lena Pepper Brain cerveau coronal

Figure 3.14 : les images cryptées par la carte chaotique logistique



Lena Pepper

Brain Cerveau coronal

Figure 3.15 : l'histogramme des images cryptées par la carte chaotique logistique

Les résultats montrent que les histogrammes des images chiffrées par la carte chaotique logistique sont uniformes après le cryptage. Par conséquent l'attaquant ne peut pas extraire information à partir de l'histogramme de l'image cryptée

4.3 **L'entropie**

Le tableau 3.1 montrant les valeurs de l'entropie des images claires et chiffrées en utilisant la clé aléatoire et la carte logistique chaotique

La valeur de l'entropie doit être très proche de 8, Parce que si l'entropie est inférieure à 8, il existe des degrés de prévisibilité, donc on ne peut pas assurer la sécurité contre l'analyse statistique.

Tableau 3.1 : Comparaison des Entropie entre les images en claire et chiffrée.

Nom de l'image	**Taille**	**Type**	**L'entropie de l'image**		
			Image claire	**Image chiffrée**	
				Clé aléatoire	**Clé chaotique**
Lena	256×256	Niveau de gris	7.5736	7.9970	7.9972
Pepper	256×256	Niveau de gris	7.5933	7.9973	7.9972
Brain	256×256	Niveau de gris	6.6771	7.9969	7.9975
Camera man	256×256	Niveau de gris	7.0097	7.9972	7.9970
Cerveau axial	256×256	Niveau de gris	5.6336	7.9967	7.9976
Cerveau coronal	256×256	Niveau de gris	5.4884	7.9973	7.9976
Mounain	256×256	Niveau de gris	7.7813	7.9971	7.9973
IRM tête axial	256×256	Niveau de gris	7.4622	7.9966	7.9972
Valeur moyenne			**6.9024**	**7.9970**	**7.9973**

Après la simulation de 8 images, la valeur moyenne de l'entropie des images chiffrées est 7.9970 pour la clé aléatoire ; et 7.9973 pour la clé générée par la carte logistique chaotique, donc nous observons que la valeur moyenne proche de 8 cela signifié la difficulté d'avoir la prévisibilité.

4.4 **La corrélation entre les pixels adjacents**

Le tableau 3.2 montrant les corrélations des images claires et leurs chiffrées en utilisant la clé aléatoire et la clé généré par la carte chaotique logistique.

Si la valeur de corrélation est proche de la valeur 1, cela signifie que l'image claire et l'image chiffrée sont très dépendantes. Et si la valeur de corrélation proche de la valeur 0, cela signifie que l'image chiffrée et l'image clair ne sont pas corrélés. Ainsi, si est la valeur de corrélation plus faible, implique une meilleure qualité de cryptage.

Tableau 3.2 : Comparaison des Entropie entre les images en claire et chiffrée.

Nom de l'image	Taille	Type	La corrélation des images		
			Corrélation d'Image claire	Corrélation d'image chiffrée	
				Clé aléatoire	Clé chaotique
Lena	256×256	Niveau de gris	0.9380	0.0290	0.0036
Pepper	256×256	Niveau de gris	0.9481	0.0160	0.0252
Brain	256×256	Niveau de gris	0.9299	0.0077	0.0050
Camera man	256×256	Niveau de gris	0.9201	0.0383	0.0167
Cerveau axial	256×256	Niveau de gris	0.9563	0.0171	0.0206
Cerveau coronal	256×256	Niveau de gris	0.9458	0.0280	0.0112
Mounain	256×256	Niveau de gris	0.8348	0.0099	0.0289
IRM tête axial	256×256	Niveau de gris	0.9739	0.0276	0.0163
Valeur moyenne			**0.9308**	**0.0217**	**0.0159375**

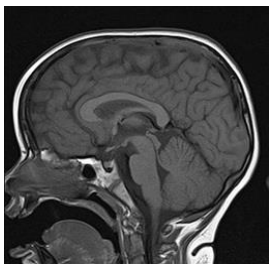
Après la simulation de 8 images, la valeur moyenne des corrélations des images chiffrées est 0.0217 pour la clé aléatoire ; et 0.0159375 pour la clé générée par la carte chaotique logistique Donc les valeurs sont plus proches de 0, cela signifié que la qualité de cryptage est meilleure

4.5 La présence du bruit dans les images cryptées

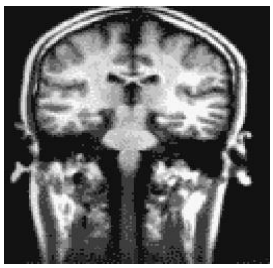
Pour le test de bruit nous avons ajouté un bruit blanc additif gaussienne de moyenne nulle. Et à l'image crypté avons de passer à la phase de la décryptographie. Figure 3.16 montre les images originales, les images cryptées bruitées ainsi que les images décryptées**.**

Lena

Pepper

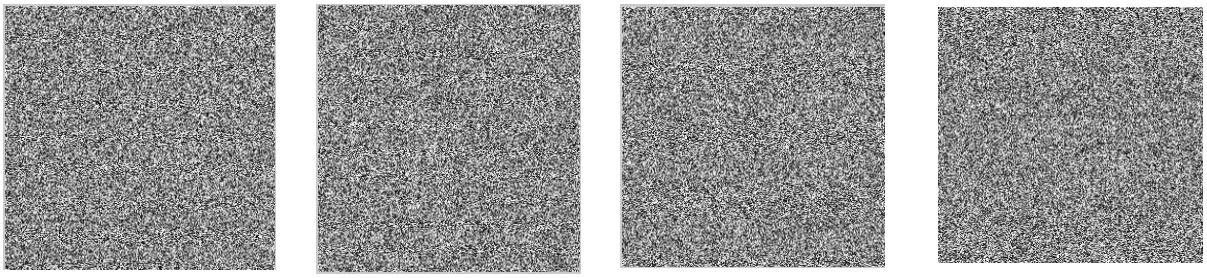


Brain

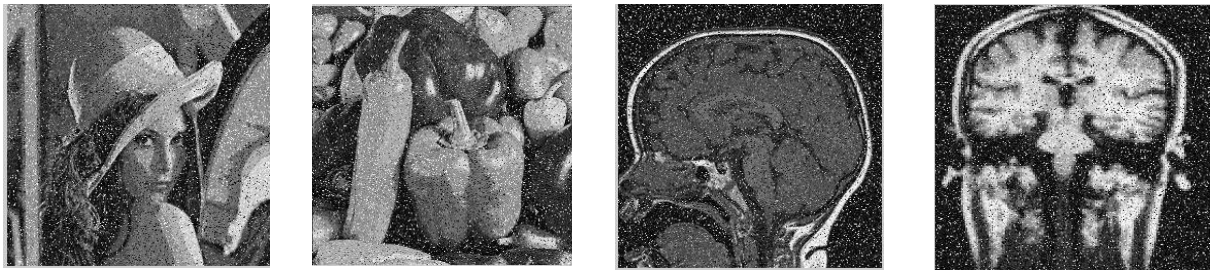


cerveau coronal

(a)



(b)



Lena **Pepper** **Brain** **cerveau coronal**

(c)

Figure 3.16 (a) les images originales, (b) les images cryptées bruitées (c) les images décryptées

5. Conclusion

Dans ce chapitre, nous avons utilisé deux algorithme de cryptage, le premier algorithme est basé sur la clé aléatoire et la deuxième algorithme 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 entre les deux algorithmes montre que le deuxième algorithme assure une efficacité , une haute protection et sécurité contre les attaques brute .

Conclusion générale

Au cours de ce mémoire, nous avons proposé d'utiliser deux algorithmes de chiffrement d'image le premier algorithme est basé sur une clé aléatoire et le deuxième algorithme est basé sur la carte logistique chaotique, Le but principal de ce chiffrement est de savoir qui assure la sécurité parmi les deux.

Les résultats expérimentaux montrent clairement, que l'algorithme basé sur la carte logistique chaotique dispose un niveau élevé de confusion. Et ainsi l'espace clé est suffisamment grand, ce qui rend une attaque force brute infaisable. Par conséquent l'histogramme d'image chiffrée est très uniforme après le cryptage, voire, l'attaquant il ne peut pas extraire l'information à partir de l'histogramme de l'image cryptée. Également l'algorithme utilisé présente les meilleurs résultats que ce soit sur l'entropie ou la corrélation entre les pixels adjacents. Il montre aussi une grande efficacité et une forte sécurité.

Bibliographie

[1] Gilles Zémor, Cours de cryptographie, Paris, Cassini, 15 décembre 2000 .

[2] A. Menezes, P. van Oorschot, and S. Vanstone , Handbook of Applied Cryptography , CRC Press, 1996 .

[3] http://michel.arboi.free.fr/cryptFAQ/ , consulté le 07/05/2020

[4] Daniel J. Bernstein, « Grover vs. McElice », *Springer*, 2010

[5] KHALDI Amine, support de cours du module Sécurité informatique, Département d'informatique, université d'Ouargla, année 2017/2018

[6] HADJI Faiçal, Conception et réalisation d'un système de cryptage pour les images médicales, Mémoire présenté pour l'obtention Du diplôme de Master Académique, université Mohamed boudiaf – M'sila, année 2017/2018

[7 http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8354294 , consulté le 20/05/2020

[8] https://web.maths.unsw.edu.au/~lafaye/CCM/crypto/simple.htm , consulté le 11/06/2020

[9] http://www.primenumbers.net/Renaud/fr/crypto/Cesar.htm, consulté le 11/06/2020

[10] http://www.primenumbers.net/Renaud/fr/crypto/Vigenere.htm, consulté le 11/06/2020

[11] M. Riguidel, Quelque rappels sur les techniques cryptographiques, 2002

[12] Bekkouche Toufik, Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes, thèse de doctorat, université Ferhat Abbas Sétif.

[13] https://web.archive.org/web/20060508042238/http://citeseer.ist.psu.edu/mantin01practical.html consulté le 17/06/2020

[14] Data Encryption Standard (Des)- Federal Information Processing Standards Publication - Reaffirmed 1999 October 25

[15] Niles Ferguson, Richard Schroeppel et Doug Whiting (2001) « A Simple Algebraic Representation of Rijndael » *Selected Areas in Cryptography*: 103–111 p., Springer Berlin Heidelberg.

[16] Pascal Boyer, *Petit compagnon des nombres et de leurs applications*, Calvage et Mounet, 2019, 648 p

[17] Rafael C Gonzalez and Richard E Woods. Digital image processing 3rd edition 2007.

[18] site web, https://www.schoolmouv.fr/definitions/image-numerique/definition , consulté le 05/07/2020

[19] Raphaël Isdant, traitement d'image numérique, 2009

[20] http://numeriksciences.fr/_media/image-numerique.pdf, consulté le 20/07/2020

[21] C. alleau. Images numériques. Physique - Chimie - Académie de Poitiers. http://ww2.ac-poitiers.fr/sc_phys/sites/sc_phys/IMG/pdf/Images_numeriques.pdf, consulté le 23/07/2

[22] Nathalie DENOS, Karine SILINI .travailler dans environnement numérique évolutif – C2i, version 1.0,

[23] https://fr.wikipedia.org/wiki/Encapsulated_PostScript , consulté le 24/07/2020

[24] https://www.synbioz.com/blog/tech/le-svg-pour-quoi-faire , consulté le 24/07/2020

[25] https://www.online-convert.com/fr/format-fichier/fla , consulté le 26/07/2020

[26] https://fr.wikipedia.org/wiki/Portable_Document_Format , consulté le 26/07/2020

[27] https://fr.wikipedia.org/wiki/PICT , consulté le 02/08/2020

[28] 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,

[29]https://www.sites.univ-rennes2.fr/artsspectacle/cian/image_numFlash/pdf/chap5_tout52.pdf, consulté le 05/08/2020

[30] Claude Elwood Shannon. A mathematical theory of communication. ACM SIG-MOBILEMobile Computing and Communications Review, 5(1) :3–55, 2001

[31] Aimeur Akram, Conception et implémentation d'un système hybride pour la sécurité de données : application aux images numériques, Mémoire présenté pour l'obtention Du diplôme de Master Académique, UNIVERSITE MOHAMED BOUDIAF - M'SILA, année 2016/2017

[32] Wikipédia, https://fr.wikipedia.org/wiki/Leonardo_Fibonacci, consulté le 09/08/2020

[33] suite de Fibonacci- maths-et-tiques, https://www.maths-et-tiques.fr/index.php/histoire-des-maths/mathematiciens-celebres/fibonacci consulté le 23/08/2020

[34] International Journal of Computer Applications (0975 – 8887) Volume 151 – No.3, October 2016,(Multi-Levels Image Encryption Technique based on Multiple Chaotic Maps and Dynamic Matrix), Mustafa Dhiaa AL-Hassani, PhD Computer Science, Dept. / Mustansiriyah-University-Baghdad-Iraq,- https://www.ijcaonline.org/archives/volume151/number3/alsaraji-2016-ijca-911693.pdf, consulté le 23/08/2020

[35] Avi Dixit, Pratik Dhruve and Dahale Bhagwan ,(IMAGE ENCRYPTION USING PERMUTATION AND ROTATIONAL XOR TECHNIQUE) - Department of Electronics and Telecommunication, Thakur College of Engineering and Technology, Mumbai University, Mumbai,India http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.1463&rep=rep1&type=pdf, consulté le 25/08/2020

[36] University of Waterloo, Base de données d'images

http://links.uwaterloo.ca/Repository.html, consulté le 27/08/2020

[37] University of Wisconsin-Madison, Base de données d'images https://homepages.cae.wisc.edu/~ece533/images/., consulté le 10/09/2020

[38] https://info-radiologie.ch/resonance_magnetique.php, consulté le 10/09/2020