REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED BOUDIAF - M'SILA

FACULTE : MATHEMATIQUES ET DE L'INFORMATIQUE

DEPARTEMENT : D'INFORMATIQUE

N° : ……..

DOMAINE : Mathématiques et Informatique

FILIERE : Informatique

OPTION : Réseaux

Mémoire présenté pour l'obtention
Du diplôme de Master Académique

Par: Aimeur Akram

Intitulé

Conception et implémentation d'un système hybride pour la sécurité de données : application aux images numériques

Soutenu devant le jury composé de :

Mr : BENOUIS Mohamed	Université de M'sila	Président
Dr : LAMICHE Chaabane	Université de M'sila	Rapporteur
Mr : GUEMOUGUI Abdessatar	Université de M'sila	Examinateur

Année universitaire : 2016 /2017

﴿قَالُوا سُبْحَانَكَ لاَ عِلْمَ لَنَا
إِلاَّ مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ
العَلِيمُ الحَكِيمُ﴾

سورة البقرة، الآية ٣٢.

Dédicaces

Je dédie ce travail à mes très chers parents, pour leur soutien et tous les efforts Qu'on m'a donnée le long de mon parcours et je leurs souhaite bonne santé et longue vie.

Je dédie ce travail aussi à mon très cher frère Ilays et toutes mes sœurs.

A toute ma famille, tous mes amis

Et tous ceux que j'aime et qui m'aiment

A tous mes enseignants qui ont fait leurs possibles pour nous

Donner le maximum d'informations concernant notre étude

Merci infiniment.

Aimeur Akram

Remerciements

Avant tout on tient notre remerciement à notre dieu tout puissant de nous avoir donné la foi, la force et le courage.

Je remercie mon encadreur Dr Lamiche Chaabane, de sa

Disponibilité, sa générosité professionnelle et ses précieux conseils.

Je remercie les membres du jury qui m'ont honoré de leur présence et d'avoir accepté de juger mon travail.

Merci à tous.

Aimeur Akram

Table des matières

CHAPITRE 3: MÉTHODE PROPOSÉE

Liste des figures

Liste des tableaux

Introduction générale

Aujourd'hui, avec l'avancement rapide de la technologie des réseaux notamment Internet, les images numériques ont un énorme type d'information impliquées dans les communications modernes. Et qui sont largement utilisées dans plusieurs domaines sensibles tels que le commerce électronique, les affaires militaires et les dossiers médicaux. …etc. Par conséquent, la sécurité des images numériques devient un enjeu essentiel que ce soit pour le stockage ou pour la transmission. La cryptographie est parmi les méthodes les plus éfficace pour établir la confidentialité et l'intégrité de ce type d'information.

Problématique et objectif

Actuellement, Il est devenu clair que nous ne pouvons pas utiliser les méthodes de chiffrement classiques standard comme RSA, DES, AES, pour le chiffrement d'image numériques, par ce que ils sont conçues pour les données textuelles. Ainsi les images numériques sont caractérisées par *la redondance élevée*, *la forte corrélation* et *la taille volumineuse*. Le problème posé est comment peut-on concevoir un système de cryptage pour assurer la sécurité de ce type de données ?, Dans ce mémoire et afin de répondre à cette problématique, on va développer et implémenter un système hybride pour le cryptage des images numérique. Ce système est basé sur la Suite de Fibonacci modifiée et Chaotique carte logistique en exploitant les avantages apportés par chacune d'elles.

Organisation du mémoire

Nous avons structuré notre mémoire en trois chapitres. Le premier chapitre donnera une brève présentation sur les techniques de cryptographie et ses classification, particulièrement revue sur la cryptographie symétrique. Dans le deuxième chapitre met le point sur les notions de base d'image numérique et les techniques de cryptage d'image. En troisième chapitre consiste à présenter notre méthode proposée. Puis on va terminer par une conclusion générale et quelques perspectives pouvant aider dans l'amélioration du système dans le futur.

CHAPITRE 1

REVUE SUR LA CRYPTOGRAPHIE SYMETRIQUE

1. Introduction

La sécurité de l'information est un domaine très vaste qui regroupe tous les aspects de la sauvegarde ou la protection de l'information ou des données, donc pour garantir la sécurité de l'information c'est la cryptographie qui s'en charge. La cryptographie est historiquement l'une des premières applications de l'informatique. Ce domaine, qui était il y a encore quelques années, réservé aux militaires et aux grandes entreprises, concerne aujourd'hui tous ceux qui souhaitent transmettre des données protégées, qu'ils soient professionnels ou particuliers. Pour cela, il existe de nombreuses méthodes de cryptographie.

Donc dans ce chapitre, nous allons expliquer les terminologies de base de la cryptographie, on décrit brièvement les objectifs de la cryptographie ensuite, la classification de système cryptographique et on termine par les algorithmes de chiffrement symétrique.

2. Introduction à la sécurité informatique

2.1. Sécurité Informatique

Est un ensemble de moyens techniques pour réduire la vulnérabilité d'un système informatique système contre les menaces accidentels.

2.2. La vulnérabilité

En sécurité informatique, une vulnérabilité ou faille est une faiblesse dans la protection du système informatique, permettant à un attaquant de porter atteinte à la confidentialité, l'intégrité et la disponibilité des données ou ressources informatiques.

2.3. Les menaces

Le fait qu'une personne ou quelque chose qui peut exploiter une vulnérabilité pour obtenir, modifier ou empêcher l'accès au système.

2.4. Attaque

Une attaque peut être définit comme toute action ou ensemble d'actions malveillante qui tente d'exploiter une faiblesse dans le système.

3. La terminologie de la cryptographie

3.1. La cryptologie

La cryptologie est une science fondée sur les mathématiques qui comporte en deux branches: la cryptographie et la cryptanalyse.

3.2. La cryptographie

Discipline incluant les principes, les moyens et les méthodes de transformation des données, dans le but de masquer leur contenu, d'empêcher leur modification ou leur utilisation illégale [1].

3.3. La cryptanalyse

La cryptanalyse à l'inverse, est l'étude des procédés cryptographiques dans le but de trouver des faiblesses et, en particulier, de pouvoir décrypter des textes chiffrés. Le décryptement est l'action consistant à retrouver le texte en clair sans connaitre la clef de déchiffrement [2].

3.4. Texte en clair (Plaintext)

Texte en clair c'est les données ou message lisible avant chiffrement.

3.5. Le chiffrement (Encryption)

Est un moyen qui permet de transformer un message (Texte en clair) afin qu'il ne soit lisible qu'à l'aide d'une clé de chiffrement afin de protéger l'information contre l'accès non autorisé.

3.6. Clef

Est un paramètre important qui utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement, scellement, signature numérique, vérification de signature).

3.7. Texte chiffré (Ciphertext)

Données ou message inintelligible résultant du chiffrement.

3.8. Le déchiffrement (Decryption)

Est un moyen qui permet à retrouver le message original (Texte en clair) à partir du message chiffré en utilisant la clé de déchiffrement.

4. Propriétés de cryptographie

4.1. La confidentialité

La confidentialité consiste à rendre l'information inintelligible à tous ceux qui pourraient intercepter les données ou message. La confidentialité peut être aussi vue comme la protection des données contre une divulgation non autorisée.

4.2. L'intégrité

L'intégrité est un mécanisme permet d'assurer que les données reçues par récepteur n'ont pas été modifiés, altérés durant la transmission.

4.3. L'authentification

L'authentification est un mécanisme permettant d'identifier des personnes ou des entités et de certifier leur identité.

4.4. La non répudiation

La non-répudiation signifie la possibilité de vérifier que l'envoyeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message. 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 [3].

5. Classification des systèmes cryptographiques

5.1. La cryptographie symétriques (clé secrète)

La cryptographie symétrique, également dite à clé secrète (par opposition à la cryptographie asymétrique), est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé [4].

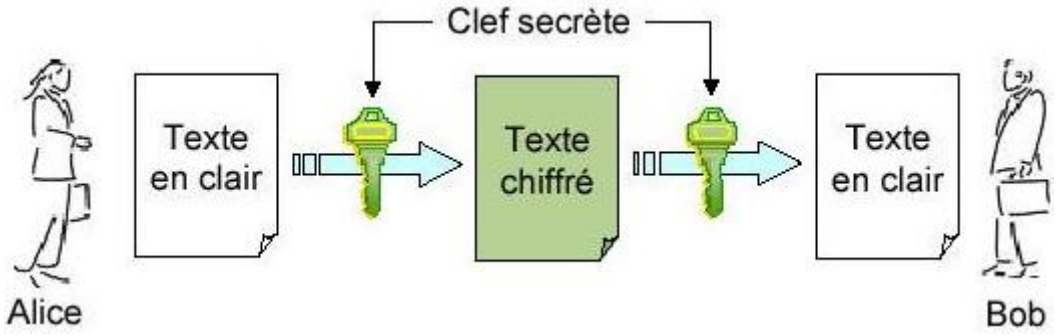

Figure 1.1 : La cryptographie symétrique [5].

Les Caractéristiques :

- Les clés sont identiques : $K_E = K_D = K$
- La clé doit rester secrète.
- Les algorithmes les plus répandus sont le *DES*, *AES*, *3DES*, ... etc.
- Au niveau de la génération des clés, elle est choisie aléatoirement dans l'espace des clés.
- Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé
- La taille des clés est souvent de l'ordre de 128 bits. Le *DES* en utilise 56, mais l'*AES* peut aller jusque 256 [6].

5.2. La cryptographie asymétriques (clé publique)

Le principe de chiffrement asymétrique (appelé aussi chiffrement à clés publiques) est apparu en 1976, avec la publication d'un ouvrage sur la cryptographie par Whitfield Diffie et Martin Hellman. Dans un cryptosystème asymétrique (ou cryptosystème à clés publiques), les clés existent par paires :

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

Il lui suffit de chiffrer le message à envoyer au moyen de la clé publique du destinataire (qu'il trouvera par exemple dans un serveur de clés). Ce dernier sera en mesure de déchiffrer le message à l'aide de sa clé privée (qu'il est seul à connaître) [7].

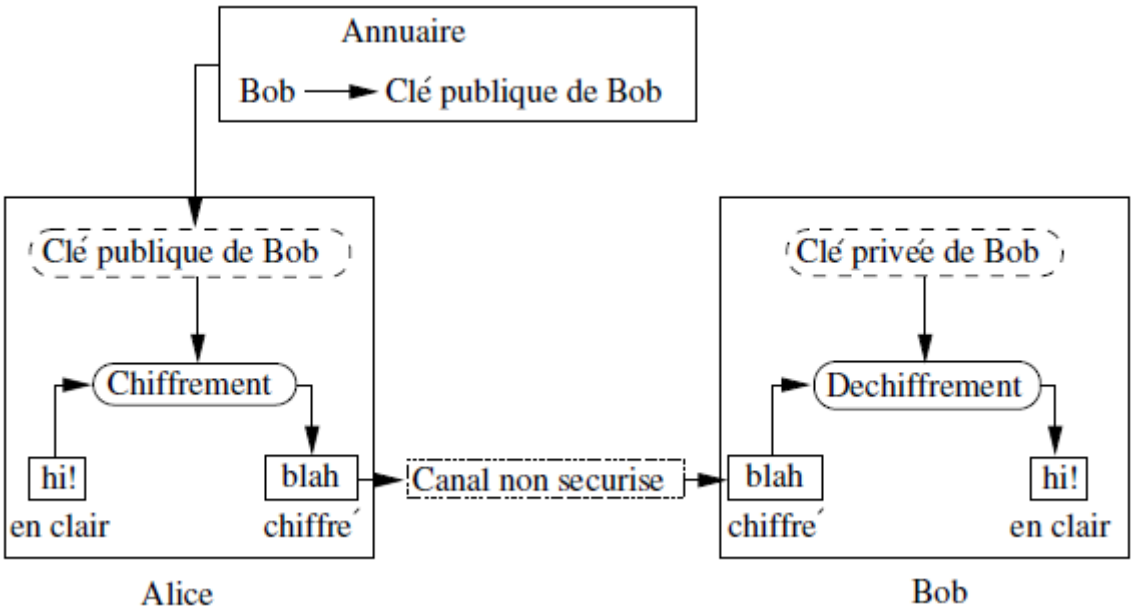

Figure 1.2 : La cryptographie Asymétriques [8].

Les Caractéristiques :

- Une clé publique P_K (symbolisée par la clé verticale)
- Une clé privée secrète S_K (symbolisée par la clé horizontale)
- Propriété : La connaissance de P_K ne permet pas de déduire S_K
- $D_{S_K}\left(E_{P_K}(M)\right) = M$
- L'algorithme de cryptographie asymétrique le plus connu est le *RSA,*
- Le principe de ce genre d'algorithme est qu'il s'agit d'une fonction unidirectionnelle à trappe. Une telle fonction à la particularité d'être facile à calculer dans un sens, mais difficile voire impossible dans le sens inverse. La seule manière de pouvoir réaliser le calcul inverse est de connaître une trappe. Une trappe peut par exemple être une faille dans le générateur de clés. Cette faille peut être soit accidentelle ou intentionnelle de la part du concepteur.
- Les algorithmes se basent sur des concepts mathématiques tels que l'exponentiation de grands nombres premiers (*RSA*), le problème des logarithmes discrets (ElGamal), ou encore le problème du sac à dos (Merkle-Hellman).
- La taille des clés s'étend de 512 bits à 2048 bits en standard. Dans le cas du *RSA,* une clé de 512 bits n'est plus sûre au sens "militaire" du terme, mais est toujours utilisable de particulier à particulier [6].

6. Cryptographie à clé secrète (symétrique)

6.1. Chiffrement par blocs

On désigne par chiffrement par blocs (block-chiper en anglais), tout système de chiffrement (symétrique) dans lequel le message clair est découpé en blocs d'une taille fixée, et chacun de ces blocs est chiffré [9].

Les plus célèbres algorithmes de chiffrement par blocs sont le *DES* et l'*AES*.

L'idée générale du chiffrement par blocs est la suivante :

1. Remplacer les caractères par un code binaire
2. Découper cette chaîne en blocs de longueur donnée
3. Chiffrer un bloc en l'"additionnant" bit par bit à une clef.
4. Déplacer certains bits du bloc.
5. Recommencer éventuellement un certain nombre de fois l'opération 3.
6. Passer au bloc suivant et retourner au point 3 jusqu'à ce que tout le message soit chiffré.

Les catégories de chiffrement par bloc :

- *Chiffrement par substitution*

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

- *Chiffrement par transposition*

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

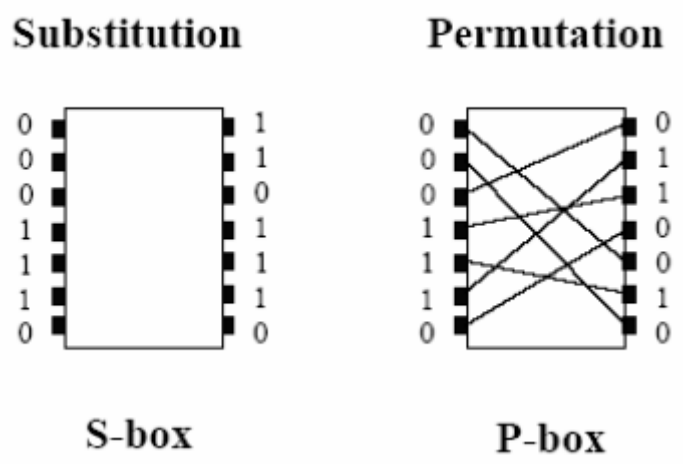

Figure 1.3 : Substitution et permutation [6].

- *Chiffrement par produit*

C'est la combinaison des deux. Le chiffrement par substitution ou par transposition ne fournit pas un haut niveau de sécurité, mais en combinant ces deux transformations, on peut obtenir un chiffrement plus robuste. La plupart des algorithmes à clés symétriques utilisent le chiffrement par produit. On dit qu'un « round » est complété lorsque les deux transformations ont été faites une fois (substitution et transposition).

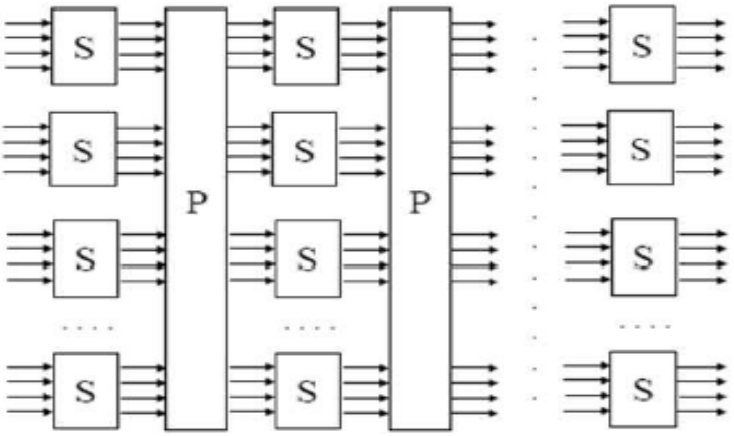

Figure 1.4 : Chiffrement par produit [6].

6.1.1. Algorithme DES

- Introduction

Le D.E.S. (Data Encryption Standard, c'est-à-dire Standard de Chiffrement de Données) est un standard mondial depuis la fin des années 1970. Bien qu'il soit un peu vieillissant, il résiste toujours très bien à la cryptanalyse et reste un algorithme très sûr.

Au début des années 70, le développement des communications entre ordinateurs a nécessité la mise en place d'un standard de chiffrement de données pour limiter la prolifération d'algorithmes différents ne pouvant pas communiquer entre eux. Pour résoudre ce problème, L'Agence Nationale de Sécurité américaine (N.S.A.) a lancé des appels d'offres. La société I.B.M. a développé alors un algorithme nommé Lucifer, relativement complexe et sophistiqué. Après quelques années de discussions et de modifications, cet algorithme, devenu alors D.E.S., fut adopté au niveau fédéral le 23 novembre 1976 [10].

- Algorithme principal du DES

Les grandes lignes de l'algorithme sont les suivantes :

1. Diversification de la clé (64bit): fabrication de 16 sous-clés
2. Permutation initiale
3. Calcul médian (16 fois) : application d'un algorithme complexe appliqué en fonction de la clé
4. Permutation finale

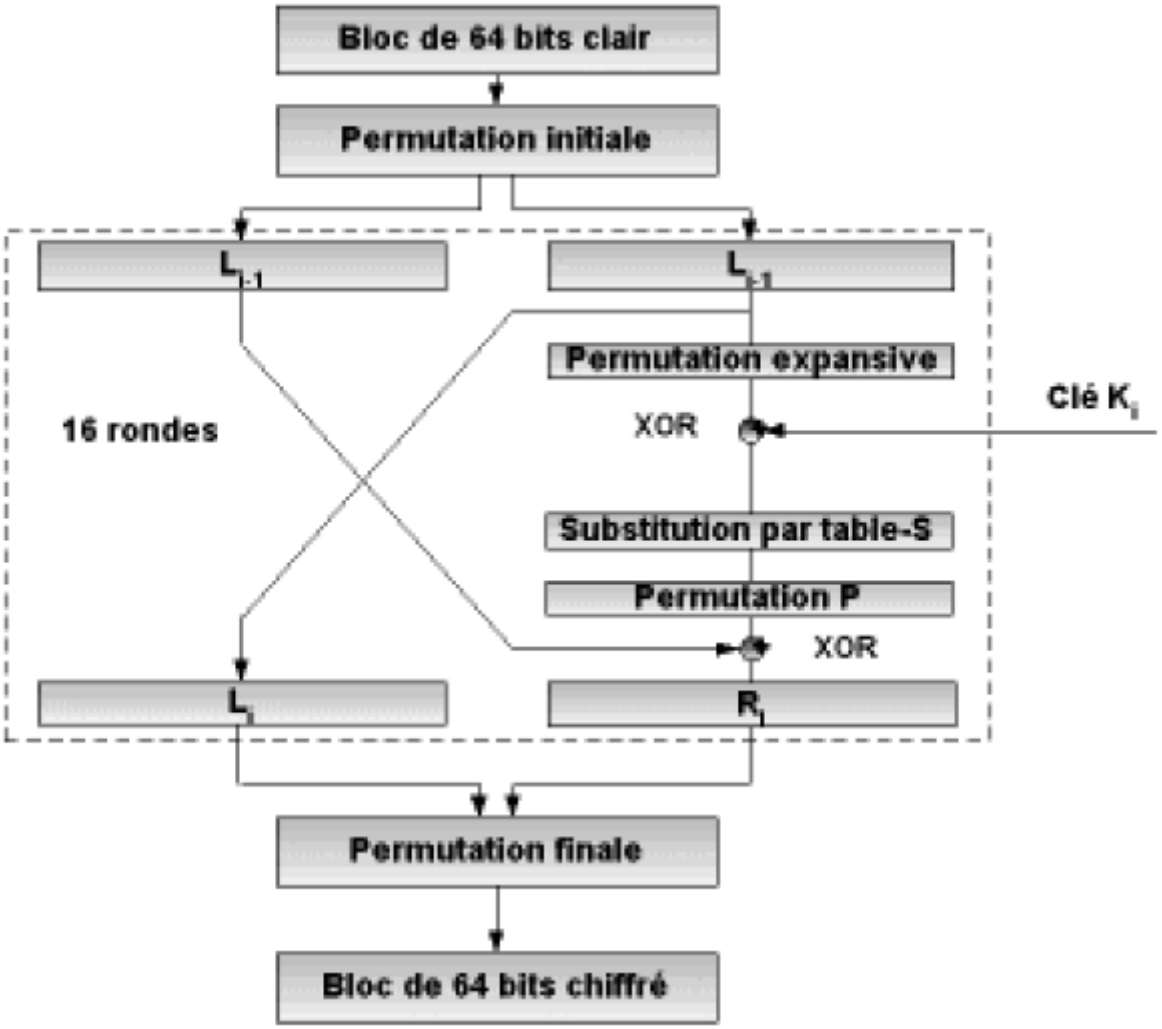

Figure 1.5 : Algorithme principal du DES [6].

6.1.2. Algorithme AES

- Introduction

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 Encryption System. Le cahier des charges comportait les points suivants :

a. évidemment, une grande sécurité.
b. 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.

c. la rapidité.
d. une lecture facile de l'algorithme, puisqu'il est destiné à être rendu public.
e. 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'oeuvre 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 [11].

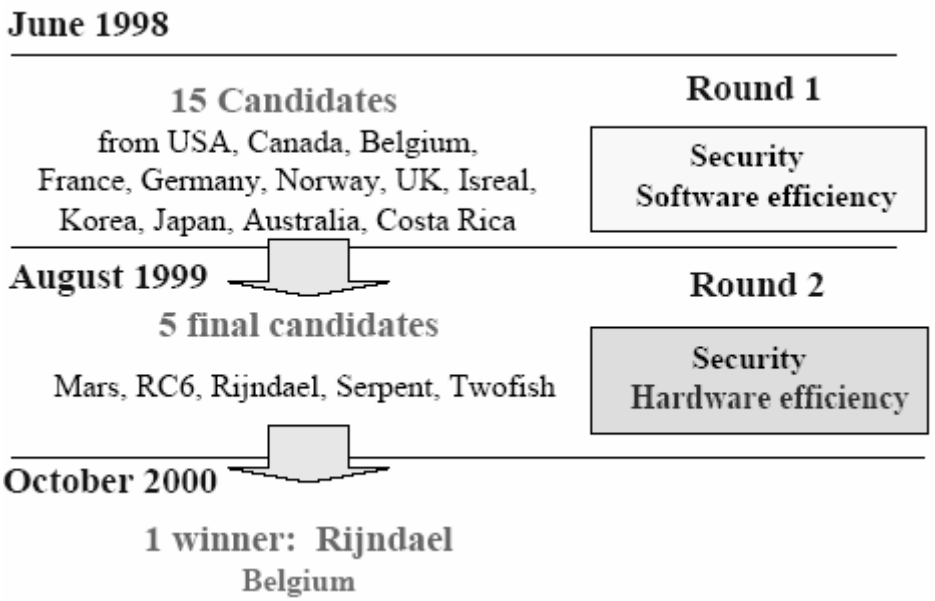

Figure 1.6 : Différents participants au concours AES [6].

- 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

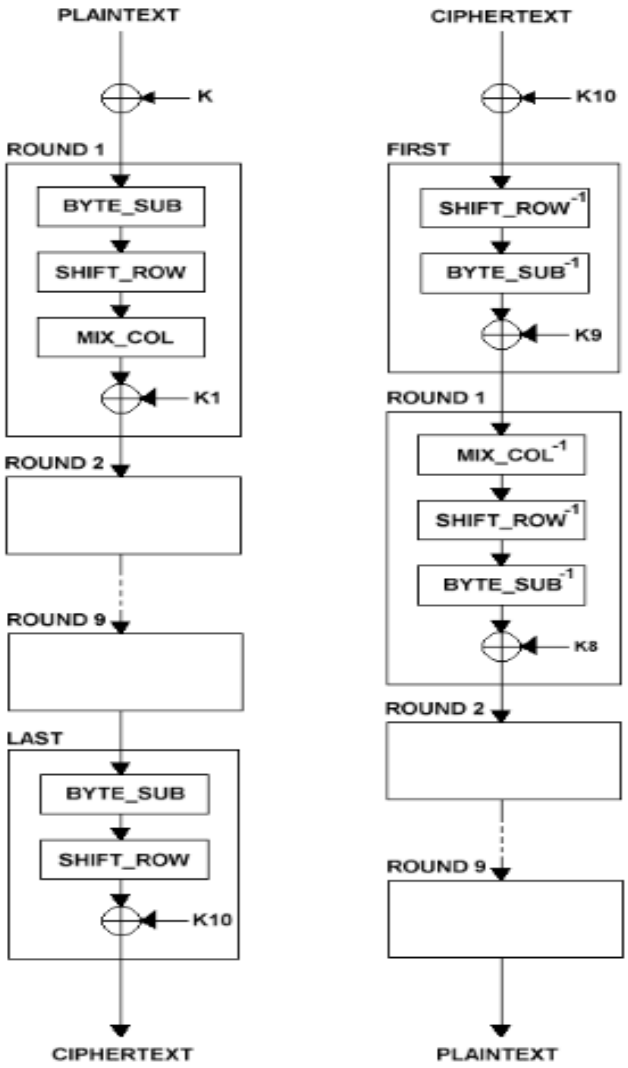

Figure 1.7 : Schéma chiffrement et déchiffrement de l'AES [12].

6.2. Chiffrement par flots

Le principe du chiffrement par flot est de chiffrer une suite de caractères (ou octets ou mots-machine) Un à la fois, à l'aide d'une transformation qui varie au fur et à mesure du texte. Au

contraire, le chiffrement par bloc utilise une transformation fixe, sur des blocs plus gros, typiquement 64 ou 128 bits [13].

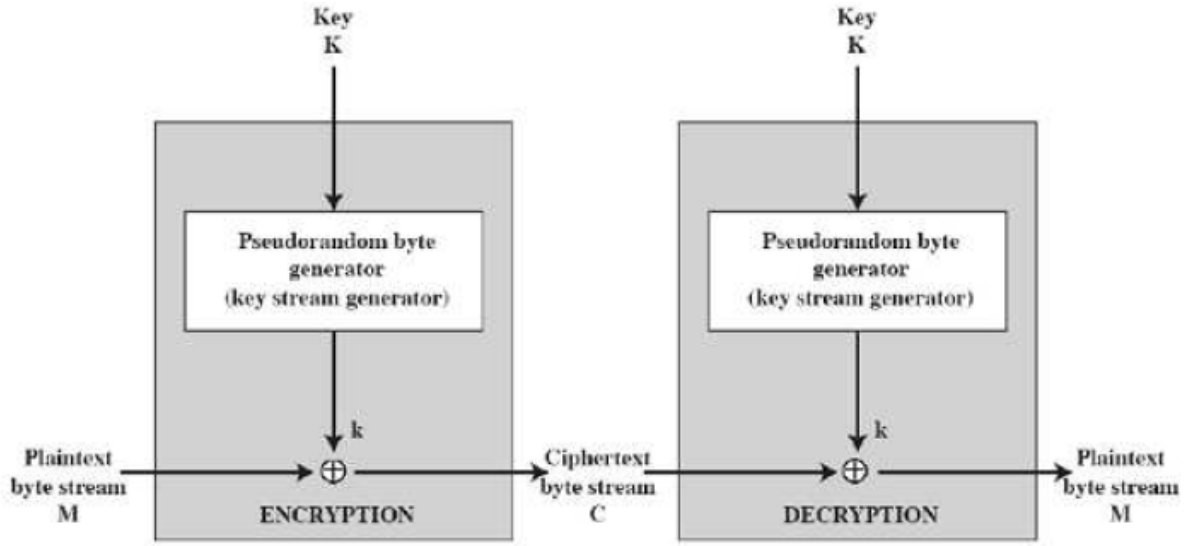

Figure 1.8 : Schéma de chiffrement pat flot [14].

Parmi les algorithmes qui utilisent chiffrement par flots c'est : *RC4, A5/1, E0,*...etc.

6.2.1. Algorithme RC4

- Introduction :

RC4 (Rivest Cipher 4) est un algorithme de chiffrement à flot conçu en 1987 par Ronald Rivest, l'un des inventeurs du RSA, pour les Laboratoires RSA. Il est supporté par différentes normes, par exemple dans TLS (anciennement SSL) ou encore WEP [15].

- Principe général 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 chiffrer les données via un XOR.

- Description détaillée

RC4 est un générateur de bits pseudo-aléatoires dont le résultat est combiné avec le texte en clair via une opération XOR, le déchiffrement se fait de la même manière.

Pour générer le flot de bits, l'algorithme dispose d'un état interne, tenu secret, qui comprend deux parties :

– une permutation S de tous les 256 octets possibles

– deux pointeurs i et j de 8 bits qui servent d'index dans un tableau

La permutation est initialisée grâce à la clé de taille variable, typiquement entre 40 et 256 bits, grâce au key Schedule de RC4.

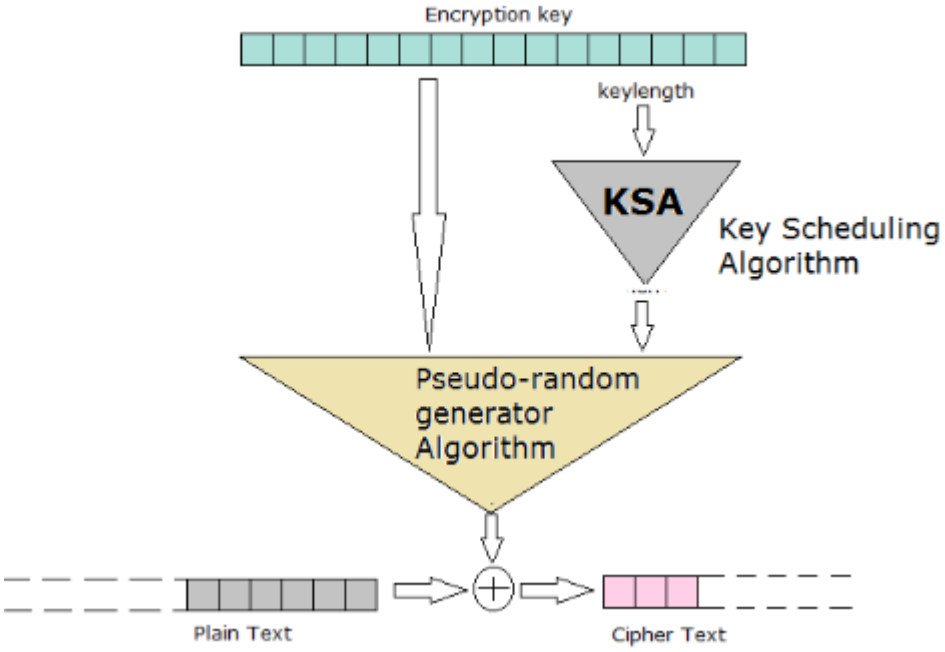

Figure 1.9 : Schéma de représentation RC4 [16].

7. Conclusion

Dans ce chapitre, nous avons fourni une brève aperçue sur les des différentes techniques de la cryptographie. Nous avons concentré également sur la classification des systèmes cryptographiques concerne les algorithmes de chiffrement symétrique.

Dans le prochain chapitre, nous allons voir les notions de base sur les images numériques.

CHAPITRE 2

IMAGE NUMERIQUE

1. Introduction

Donc dans ce chapitre, nous allons expliquer les notions de base sur l'imagerie, on décrit les différents types d'images, ensuite nous passons aux codages des couleurs et les différents formats d'image numérique. Puis on va décrit aussi les outils élémentaires d'analyse d'un algorithme de cryptage d'image comme espace de clés et l'histogramme, la corrélation entre les pixels adjacents, et le dernier c'est l'entropie. Enfin on va terminer par état de l'art sur les techniques de cryptage d'image.

2. Notions de base

2.1. Définition d'une image

Une image peut être définie comme une fonction bidimensionnelle, $f(x, y)$, où x et y sont des coordonnées spatiales (plan), et l'amplitude de f à n'importe quelle paire de coordonnées (x, y) s'appelle l'intensité ou le niveau de gris de l'image à ce point [17].

2.2. L'image numérique

Une image numérique est composée de cases appelées « pixels ». Ces pixels seront affectés de nombres binaires permettant de définir des teintes de gris ou des couleurs [18].

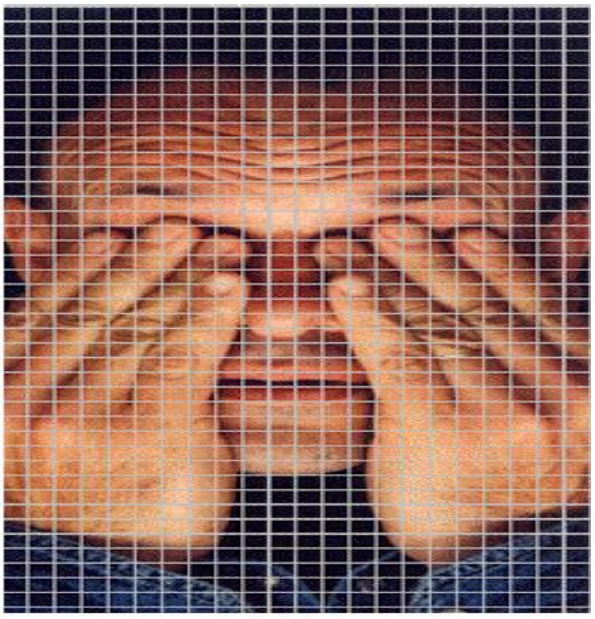

Figure 2.1 : Image numérique [19].

2.3. Pixel

Le pixel contraction des mots anglais ***PIC****ture* ***EL****ement*, c'est à dire élément d'image. Le pixel c'est la plus petite entité d'une image. Le nombre de pixels par ligne et le nombre de colonnes par image déterminent la définition de l'image.

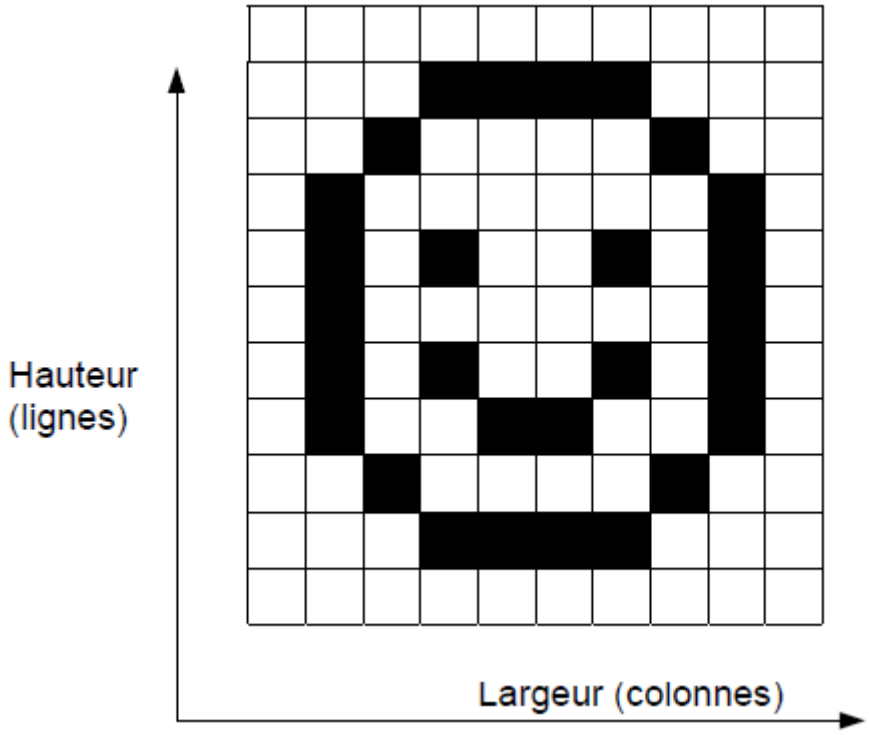

Figure 2.2 : Pixels par ligne et colonnes [20].

Exemple :

Si l'image a une définition de 640×480, cela signifie que l'image a une largeur de 640 pixels et une hauteur de 480 pixels d'où un nombre de pixels (définition): $640 \times 480 = 3{,}07 \times 10^5$ pixels.

Ainsi à chaque pixel est associée une couleur ou une teinte de gris.

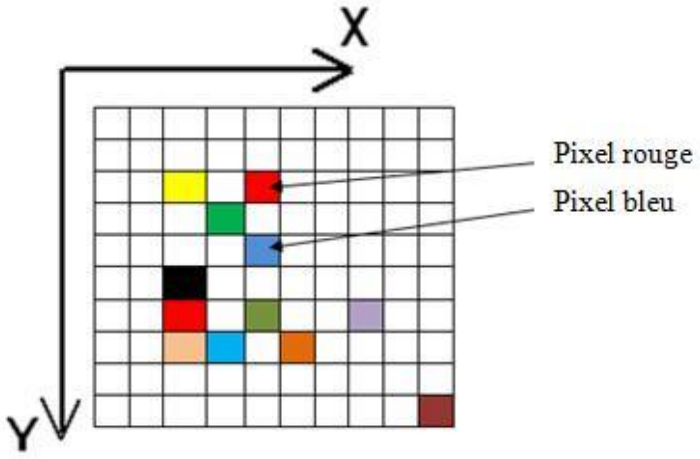

Figure 2.3 : Les couleurs de pixel [21].

2.4. 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 × 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 = 921600 octets.

2.5. Résolution

En général la résolution indique le niveau de qualité de l'image. Plus la résolution est élevée, meilleure est la qualité de l'image.

Donc, on peut définie la résolution d'une image c'est le nombre de pixels par unité de longueur. Usuellement, on compte le nombre de pixels par pouce (1 pouce = 2,54 cm, noté ppp ou dpi) ou par centimètre.

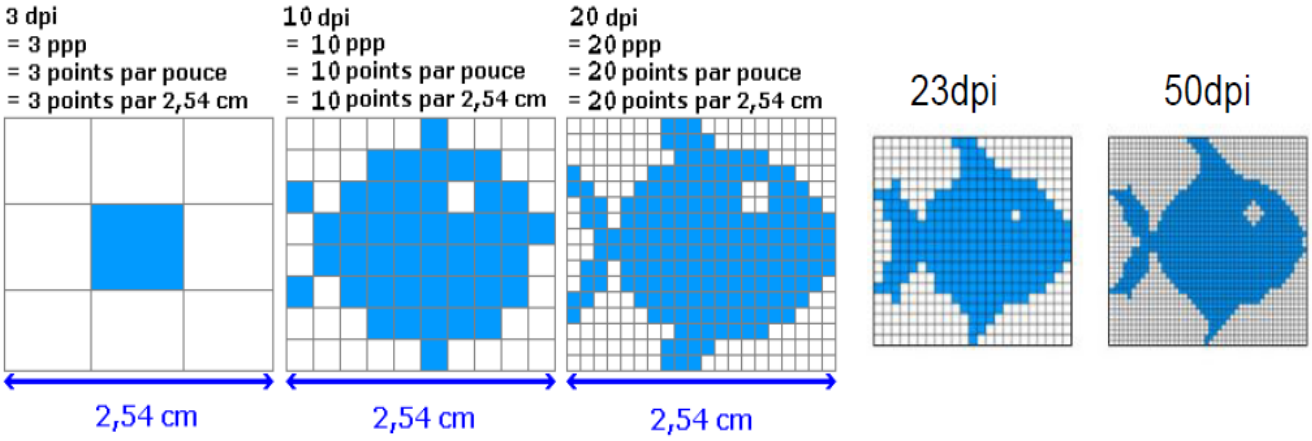

Figure 2.4 : Schéma explicatif de résolution d'une image [20].

3. Les différents types d'images

3.1. Images matricielles (Bitmap)

Image matricielle (ou bitmap) elle est formée d'une grille de points ou pixels. Chacun pouvant avoir une couleur différente. Une image matricielle est caractérisée notamment par :

- Sa dimension en pixels
- Sa résolution
- Son mode colorimétrique

Les images vues sur un écran de télévision ou une photographie sont des images matricielles. On obtient également des images matricielles à l'aide d'un appareil photo numérique, d'une caméra vidéo numérique ou d'un scanner [18].

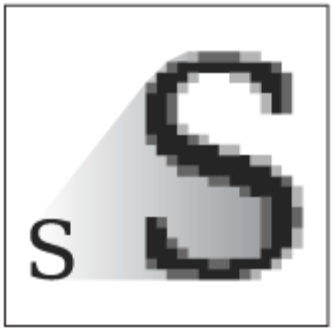

Figure 2.5 : Images matricielles [22].

3.2. Images vectorielles

L'image vectorielle utilise également la technique du Pixel, mais cette fois, leur position et leur couleur ne sont pas figées puisqu'elles sont calculées dynamiquement par le logiciel.

Autrement dit, pour afficher une ligne par exemple, le logiciel détermine le point de départ, le point d'arrivée puis la trajectoire à suivre. Ensuite, il calcule et positionne l'ensemble des pixels nécessaires pour afficher cette ligne. Il en va de même pour des formes et des couleurs plus complexes.

Cette technique est souvent utilisée lors du travail avec les palettes graphiques, la création de logos ou de bandes dessinées [23].

Figure 2.6 : Images vectorielle [22].

4. Codages des couleurs

4.1. Images binaires

Une image binaire est une image pour laquelle chaque pixel peut avoir seulement deux valeurs d'intensité. Ils sont affichés en noir et blanc. Numériquement, les deux valeurs sont souvent 0 pour le noir, et 1 pour le blanc.

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

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 2.7 : Codage binaire (0,1) [20].

Exemple sur images binaires :

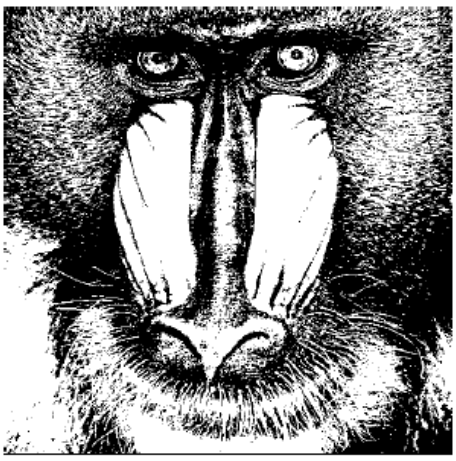

Figure 2.8 : Image codée en binaire.

4.2. Images au niveau de gris

Le codage dit en niveaux de gris permet d'obtenir plus de nuances que le simple noir et blanc. Il offre des possibilités supplémentaires pour coder le niveau de l'intensité lumineuse.

La couleur est codée souvent sur un octet soit 8 bits ce qui offre la possibilité d'obtenir 256 niveau de gris (0 pour le noir et 255 pour le blanc). On peut aussi le faire avec 16 niveaux de gris (4 bits).

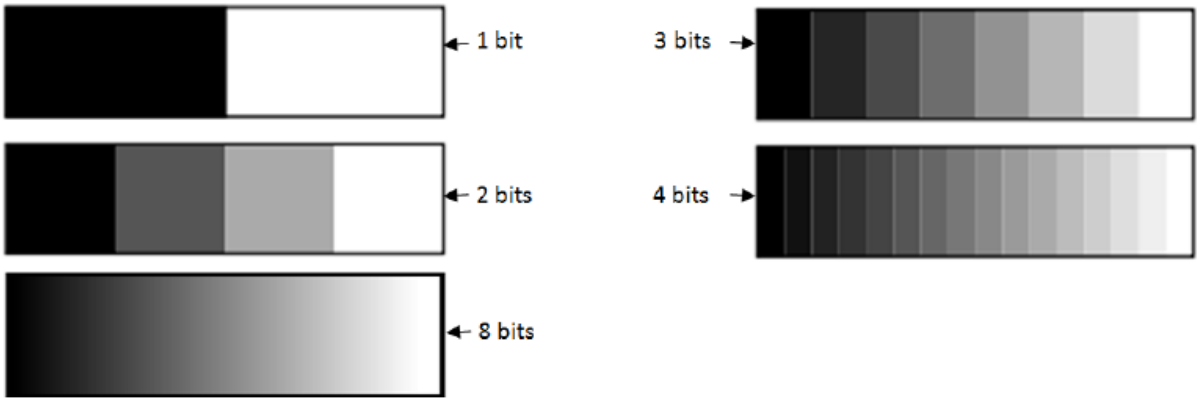

Figure 2.9 : Différent nuances avec différent nombres de bits [18].

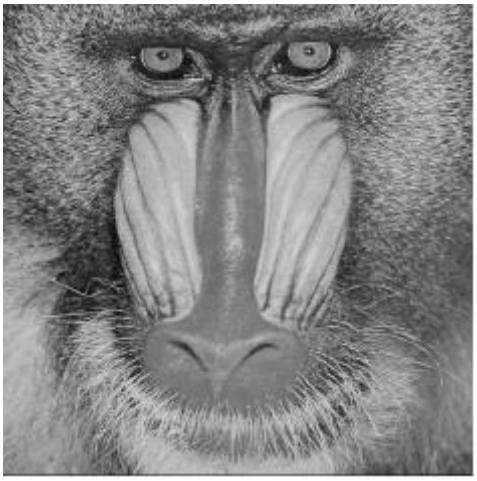

Figure 2.10 : Image au niveau de gris.

4.3. Images couleurs

4.3.1. Principe

La couleur d'un pixel est obtenue, comme le ferait un peintre, par le mélange de couleurs fondamentales. Il ne s'agit pas ici de décrire toutes les techniques utilisées. Nous allons décrire un des principes les plus couramment utilisé qui est celui de la synthèse additive.

La synthèse additive c'est la construction des couleurs par addition de 3 couleurs primaires,

Les 3 couleurs primaires sont le rouge (R), le vert (V) et le bleu (B). On parle de « Codage RVB ».

4.3.2. Codage RVB

Le principe consiste à mélanger les 3 couches de couleur : rouge, vert et bleu (noté RVB ou RGB en anglais). A l'aide de ces 3 couches de couleur, 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.

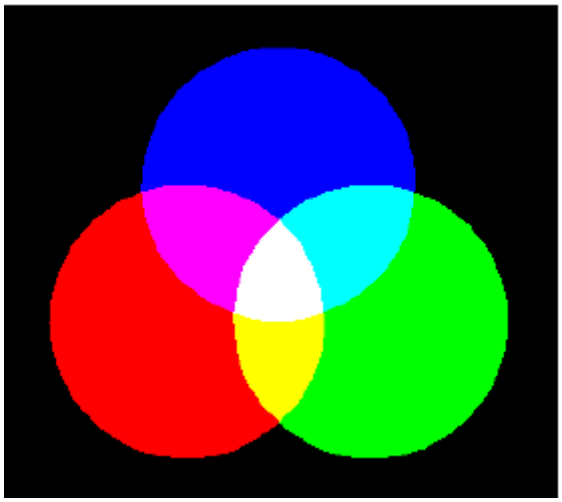

Figure 2.11 : Codage RVB [19].

Rouge	Vert	Bleu	Couleur
0	0	0	Noir
0	0	1	Nuance de noir
255	0	0	Rouge
0	255	0	Vert
0	0	255	Bleu
128	128	128	Gris
255	255	255	Blanc

Table 2.1 : Principe codage de la couleur [24].

- *Avec un codage en RVB 8 bits PAR COUCHE :*

Chaque couche utilise 8bit (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 = **16,7** millions, *Chaque pixel peut prendre 16,7 Millions de couleurs possibles!*

- *Avec un codage en RVB 16 bits PAR COUCHE*:

Chaque couche utilise le double, soit **16 bits!** (65535 nuances). **3 x 16 = 48 bits** utilisées au total.

=> 65535 x 65535 x 65535 = 248= **4** milliards, *4 milliards de nuances de couleurs sont possibles!*

Figure 2.12 : Image codée en couleurs 24 bits.

5. Les différents formats d'images

5.1. JPEG

JPEG (Joint Photographic Experts Group) est une méthode de compression avec perte, Les images JPEG compressées sont généralement stockées dans le format de fichier JFIF (JPEG Interchange File Format). Il est le format de fichier d'image le plus utilisé. Les appareils photo numériques et les pages Web utilisent des fichiers JPG. Cependant JPEG utilise la compression avec perte, qui peut conduire à une réduction significative de la taille du fichier.

L'extension du fichier JPEG / JFIF est JPG ou JPEG. Presque chaque appareil photo numérique peut enregistrer des images au format JPEG / JFIF, qui code sur 8 bits des images au niveau de gris et sur 24 bits les images couleurs [25].

5.2. TIFF

Le format TIFF (Tagged Image File Format), Il permet de stocker des images de haute qualité en noir et blanc, couleurs RVB jusqu'à 32 bits par pixels. Il supporte aussi les images indexées faisant usage d'une palette de couleurs, les calques et les couches alpha (transparence) [20,25].

5.3. GIF

GIF (Graphics Interchange Format), C'est un format léger qui peut également contenir des animations. Une image GIF ne peut contenir que 2, 4, 8, 16, 32, 64, 128 ou 256 couleurs parmi 16.8 millions dans sa palette en mode RVB. GIF Limité à une palette 8-bit, ou 256 couleurs [20,25].

5.4. PNG

Le format de fichier PNG (Portable Network Graphics), Il permet de stocker des images en noir et blanc (jusqu'à 16 bits par pixels), en couleurs réelles (True color, jusqu'à 48 bits par pixels) ainsi que des images indexées, faisant usage d'une palette de 256 couleurs. Il offre enfin une couche alpha de 256 niveaux pour la transparence [20,25].

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

6.1. Espace de clés

La taille de l'espace de clé est nécessaire pour assurer la sécurité contre l'attaque par force brute. Par exemple, si la taille de clé est 512 bit, alors l'espace de clé fournit c'est 2^{512} ($\cong 10^{154}$ Clé combinaisons possibles). Ainsi, si un ordinateur fait 10^{10} calculs par seconde, il faudra environ de 10^{136} d'ans pour trouver la clé.

6.2. L'histogramme

L'histogramme est une représentation graphique qui permet de connaître la répartition des intensités lumineuses des pixels [26].

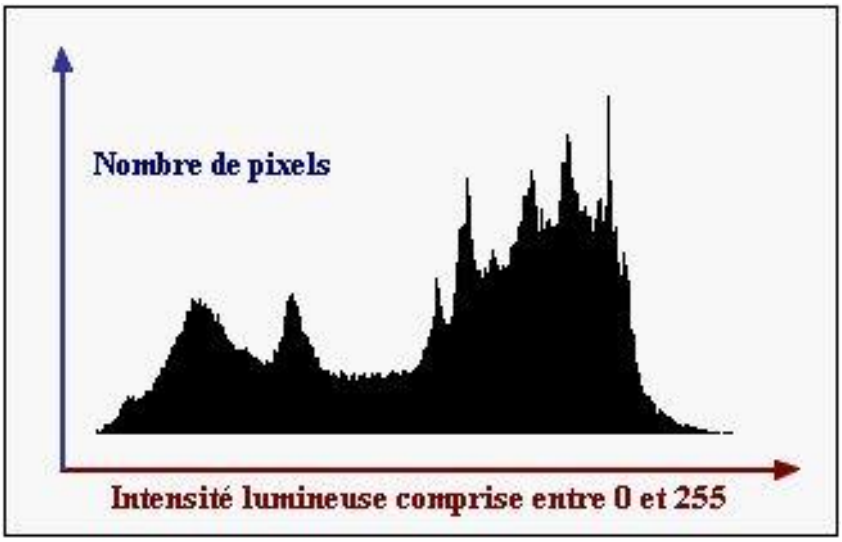

Figure 2.13 : Histogramme d'une image niveau de gris [26].

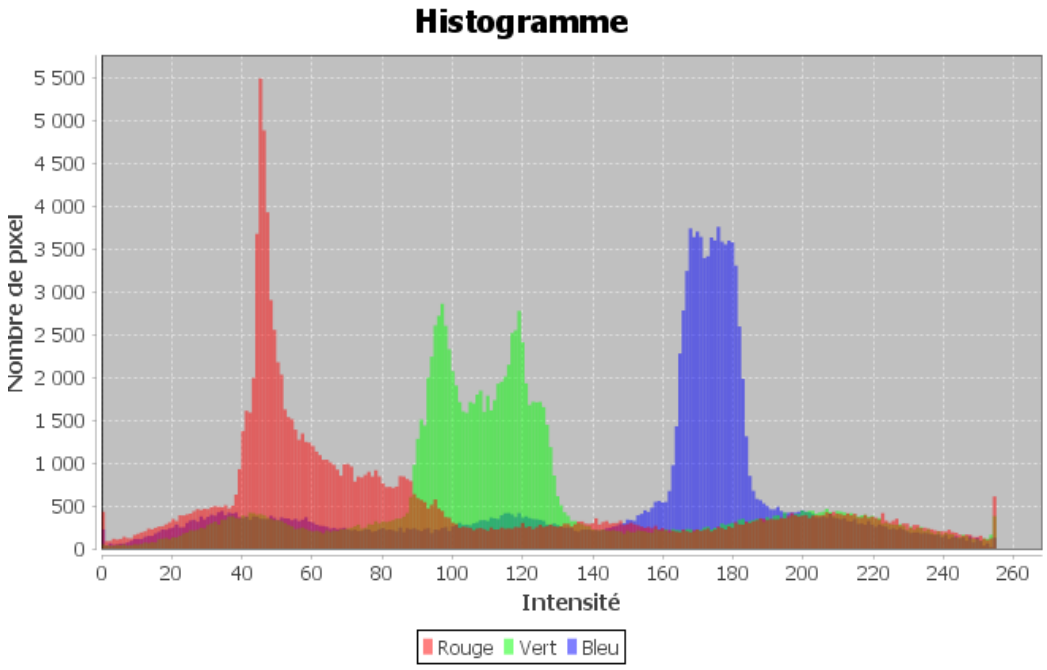

Figure 2.14 : Histogramme d'une image couleur.

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.

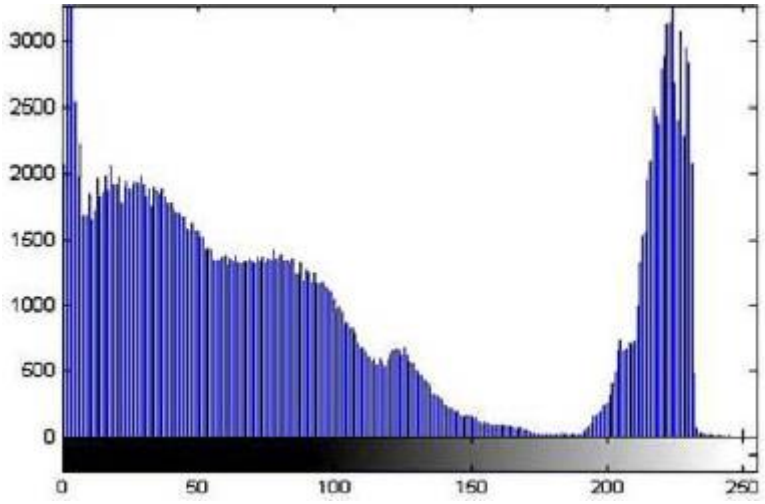

Figure 2.15 : Histogramme d'une image originale.

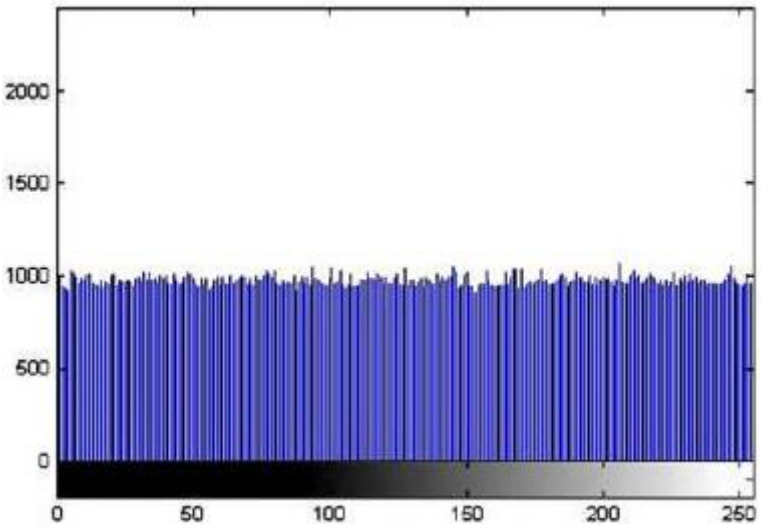

Figure 2.16 : Histogramme d'une image cryptée.

6.3. 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.

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

Où :

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

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

Si corrélation ≈ 1, cela signifie que l'Image-clair et de Image-Chiffrée sont très dépendantes. Si corrélation ≈ ± 0, cela signifie que le Image-Chiffrée et l'Image-clair ne sont pas corrélés. Ainsi, plus faible est la valeur de corrélation, la qualité de cryptage est meilleure.

6.4. 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*. La formule :

$$H(M) = -\sum_{i=1}^{n} p_i \text{ x } log_2\ p_i$$

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.

7. État de l'art sur les techniques de cryptage d'image

Comme nous avons dit, il y a plusieurs algorithmes de chiffrement d'images numériques qui ont été proposés par les chercheurs de cryptographie.

Dans notre travail, nous allons décrit prélèvement les algorithmes de chiffrement d'images numériques qui sont basé sur la théorie du fibonacci, et la théorie chaos. Par ce que on va faire hybridation entre eux dans la méthode proposée.

7.1. Méthode basé sur la théorie du Fibonacci

7.1.1. Introduction :

Leonardo Fibonacci (Pise, vers 1170 - vers 1250) est un mathématicien italien. Fibonacci (de son nom moderne), connu à l'époque sous le nom de Leonardo Pisano (Léonard de Pise), mais aussi de Leonardo Bigollo (bigollo signifiant voyageur), s'appelait en réalité Leonardo Guilielmi [27].

7.1.2. La suite de fibonacci :

Dans son Liber abaci, datant de 1202, il décrit un problème exprimant la reproduction des lapins et menant à la suite dite de Fibonacci

« Combien de couples de lapins obtiendrons-nous à la fin de l'année si, commençant avec un couple, chacun des couples produisait chaque mois un nouveau couple lequel deviendrait productif au second mois de son existence ? » [28].

En janvier : 1 couple
En février : 1 couple
En mars : 1 + 1 = 2 couples
En avril : 1 + 2 = 3 couples
En mai : 2 + 3 = 5 couples
En juin : 3 + 5 = 8 couples
En juillet : 5 + 8 = 13 couples
Donc la suite de fibonacci vérifie la relation de récurrence suivante :

$$U_{n+1} = U_n + U_{n-1} \qquad (1)$$

7.1.3. Les travaux basés sur la théorie du Fibonacci :

- Adda ALI-PACHA, Naima HADJ SAID [29], ont suggéré un nouveau schéma pour le chiffrement d'image basé sur la suite de fibonacci modifiée. Leur réalisation de cette méthode permet la génération des nombres pseudo aléatoires à l'aide de fibonacci modifiée qui basée sur la somme de deux graines modulo la valeur maximal désirée, puis faire l'addition entre les nombres pseudo aléatoires et les données de l'image en clair pour obtenir des données cryptée c'est-à-dire image cryptée.
- Yicong Zhou, Karen Panetta, Sos Agaian, C.L. Philip Chen [30], ont conçus un nouvel algorithme de cryptage d'image, qui basé sur le code P de Fibonacci pour la décomposition du plan bit-image et la transformée 2D P-Fibonacci pour cryptage d'image car ils dépendent des paramètres.
- Weijia Cao, Yicong Zhou, C.L. Philip Chen [31], ont proposé une nouvelle approche pour le chiffrement d'image, qui utilisé Truncated P-Fibonacci et Bit-planes.

7.2. Méthode basé sur la théorie du Chaos

7.2.1. Introduction :

Le chaos est dérivé du mot grec 'Χαos', Qui signifie un état sans prévisibilité ou sans ordre. Un système chaotique est un système non-linéaire, simple, déterministe, et dynamique, Qui illustre un comportement totalement inattendu et montre le hasard. Il est utilisé en cryptographie pour la nature des caractéristiques est très sensible aux conditions initiales du système, Aléatoire et apériodique comme l'évolution à long terme qui résulte des systèmes non linéaires déterministes, En raison de ces propriétés, il a été utilisé pour créer des nombres aléatoires. Avec un très petit changement dans leurs valeurs initiales, les séries générées sont complètement différentes [32,33].

7.2.2. La carte 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 », pour ce là, discute à la carte logistique «Logistic Maps en English ».

La carte logistique est une cartographie polynomiale, un système chaotique complexe, Le comportement de la carte logistique est très simple équations non linéaires dynamiques.

L'équation de la carte logistique est [34,35]:

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

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

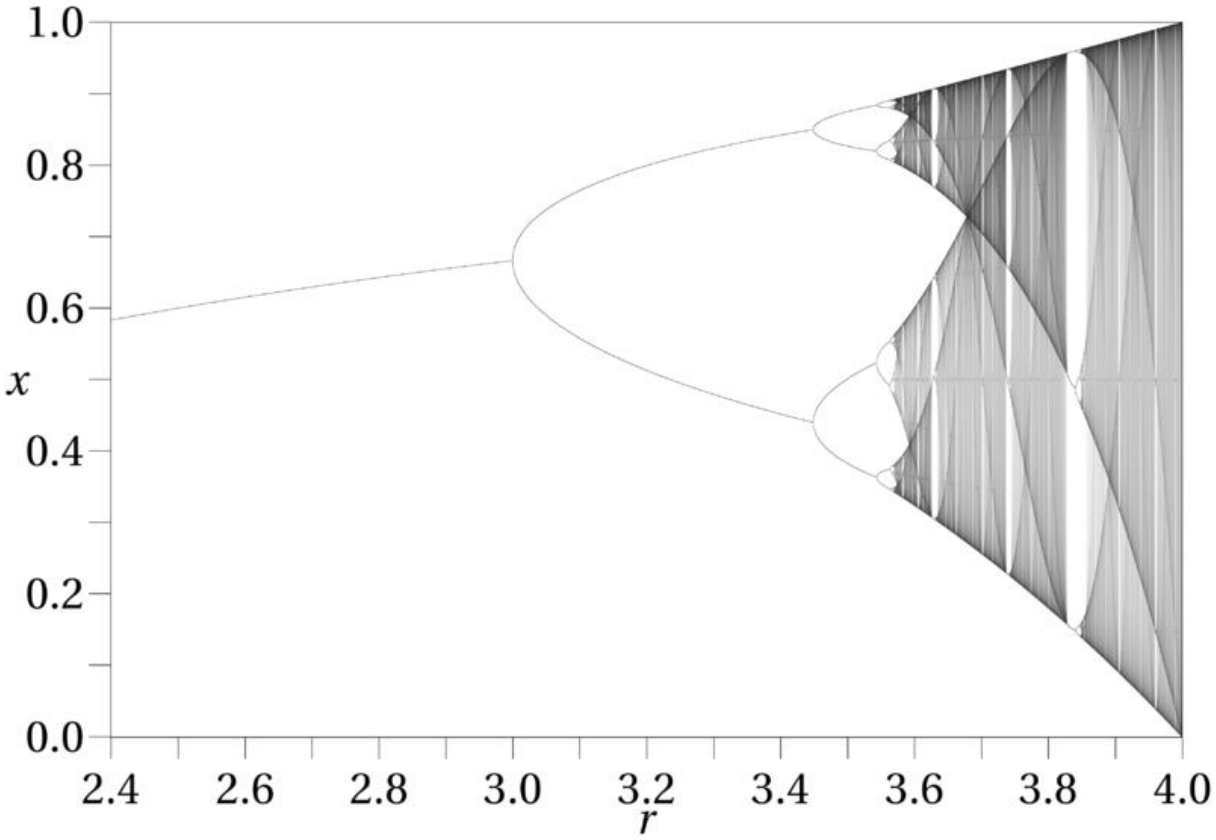

Figure 2.17 : Le diagramme de la bifurcation de la carte logistique.

7.2.3. Les travaux basés sur la théorie du chaos :

- Tiegang Gao et Zengqiang Chen [36] ont suggéré un nouveau schéma de cryptage d'image. Le cryptage proposé ici se compose de deux processus, premièrement, ils mélangent l'image en fonction d'une matrice globale de brassage généré en utilisant la carte logistique, puis ils cryptent l'image mélangée en utilisant l'hyper-chaos.
- Baydda Flaeh AL-Saraji et Mustafa Dhiaa AL-Hassani [37] ont conçus un nouvel algorithme de cryptage d'image, Leurs recherche visent à améliorer le niveau de sécurité et le secret fourni par le chiffrement qui basé sur carte chaotique. Un générateur de flux de clés N-array est proposé dans ce travail, qui est basé sur des cartes de logistique multiple pour générer les clés de chiffrement et la matrice dynamique en utilisant LFSR pour augmenter le caractère aléatoire de l'image.

- G.A.Sathishkumar et Dr.K.Bhoopathy bagan et Dr.N.Sriraam [38] ont proposé une nouvelle approche pour le chiffrement d'image. Leur algorithme proposé décrit comme les suivants : Tout d'abord, une paire de sous-clés est donnée en utilisant des cartes logistiques chaotiques. Deuxièmement, l'image est cryptée à l'aide de la carte logistique sous-clé et dans sa transformation conduit à un processus de diffusion. Troisièmement, les clés secondaires sont générées par quatre différentes cartes chaotiques et les images sont traitées comme un tableau 1D en effectuant un balayage Raster et un balayage en Zigzag. Les tableaux numérisés sont divisés en divers sous-blocs. Ensuite, pour chaque sous-bloc, la permutation de position et la transformation de valeur sont effectuées pour produire l'image cryptée.

7.3. Autres Méthodes

Beaucoup d'algorithmes de chiffrement d'image existant ont été proposées en fonction de différentes technologies, tel que : l'optique [39, 40, 41, 42, 43, 44, 45], le séquençage de l'ADN [46, 47, 48, 49, 50], l'automate cellulaire [51, 42, 53, 54], la transformation de Fourier [55, 56, 57] et beaucoup d'autres techniques.

8. Conclusion

Dans ce chapitre, nous avons essayé de fourni une brève aperçue sur les notions de base de l'imagerie. On décrit brièvement les définitions, les types d'images, les codages des couleurs, et puis nous avons décrit les outils élémentaires d'analyse d'un algorithme de cryptage d'image comme espace de clés et l'histogramme, la corrélation entre les pixels adjacents, et le dernier c'est l'entropie. Enfin nous avons terminé par état de l'art sur les techniques de cryptage d'image.

Dans le prochain chapitre, nous allons expliquer la méthode que nous avons développée pour le cryptage d'image numérique.

CHAPITRE 3

MÉTHODE PROPOSÉE

1. Introduction

Il est devenu clair que nous ne pouvons pas utiliser les méthodes de chiffrement classiques standard comme RSA, DES, AES, pour le chiffrement d'image numériques, par ce que ils sont conçues pour les données textuelles. Ainsi les images numériques sont caractérisées par la redondance élevée, la forte corrélation et la taille volumineuse.

Alors les chercheurs de cryptographie ont été proposés plusieurs techniques de chiffrement d'images numériques. Parmi eux il y a des algorithmes qui basés sur les 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 ce chapitre nous allons présenter notre algorithme de cryptage que nous avons développé. Cet algorithme de chiffrement proposé est basé sur l'hybridation entre deux techniques de cryptage, autrement dit c'est la combinant les propriétés et les avantages entre deux algorithmes, le premier algorithme basé sur Chaotique carte logistique, et le deuxième algorithme basé sur Suite de Fibonacci Modifiée. Afin d'améliorer ses performances en terme de espaces de clés et empêche l'analyse par force brute. Les résultats de la simulation montrent l'efficacité et la sécurité de notre système proposé.

2. Méthode proposée

Dans le schéma proposé, nous avons utilisé deux algorithmes qui utilisent les formules mathématiques du Chaotique carte logistique et Suite de Fibonacci Modifiée pour générer un flux de clés pseudo aléatoire avec même taille d'image, puis faire l'opération XOR élément par élément entre image en clair et le flux de clés pseudo aléatoire généré, afin d'obtenir une image cryptée.

Le but principal de ce chiffrement c'est, masquer les bits d'image en clair avec les bits des clés pseudo aléatoire généré à travers l'opération OU-exclusif (ou XOR).

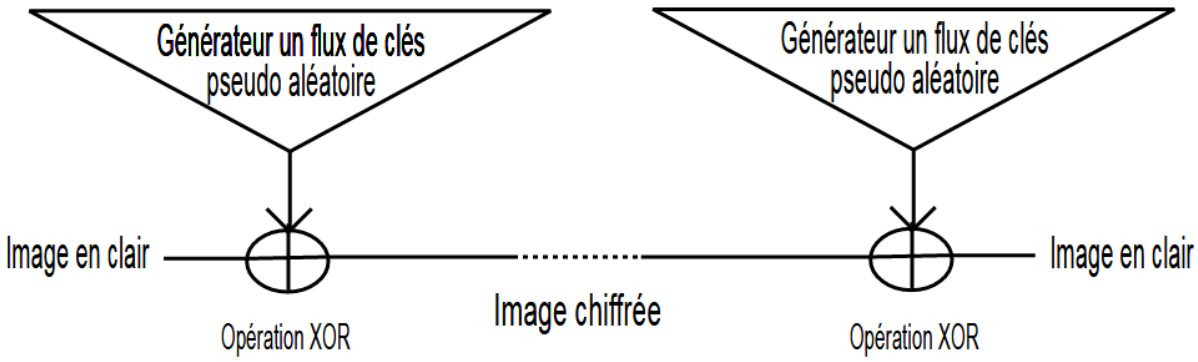

Figure 3.1 : Schéma de chiffrement proposé.

2.1. Générateur un flux de clés pseudo aléatoire

Dans notre cas, le générateur de clés pseudo aléatoire est réaliser par la combinaison OU-exclusif (ou XOR) entre deux générateurs de nombres pseudo aléatoires qui utilisent des formules mathématiques sont les suivants :

1) Le premier générateur pseudo aléatoire appelé : *Suite de fibonacci modifiée*

Formule mathématique : $X_n = (X_{n-1} + X_{n-2}) \, Mod \, M$

Les paramètres initiaux sont : (L, K), Où (X_0= L), (X_1= K). Et M = 255, (L, K) ∈ ℕ

2) Le deuxième générateur pseudo aléatoire appelé : *Chaotique carte logistique*

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

Les paramètres initiaux sont : (r, X), Où $0 < r \leq 4$ et $0 < X \leq 1$

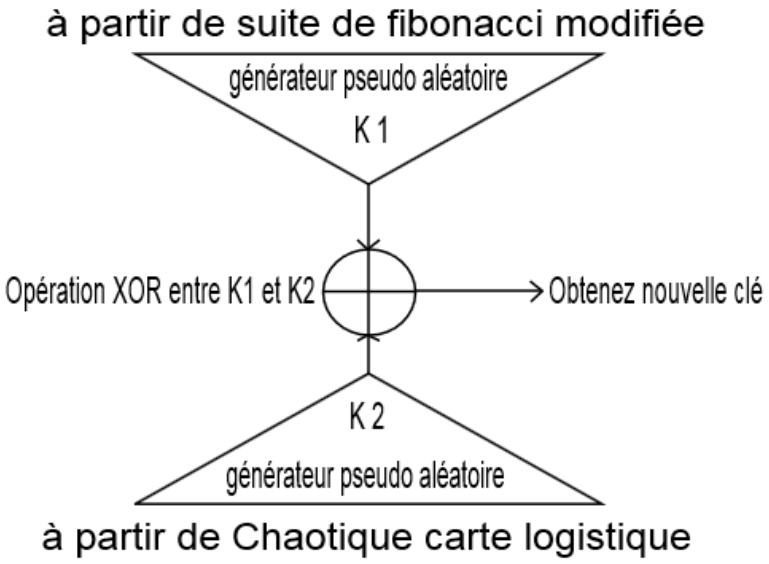

Figure 3.2 : Générateur un flux de clés pseudo aléatoire proposé.

2.2. Fonction de chiffrement

1) Générer un flux de clés pseudo aléatoire
    A. Définissez les valeurs initiales et le paramètre pour la Suite de Fibonacci Modifiée (*L*, *K*) et Chaotique Carte Logistique (*r*, *X*).
    B. Générer deux flux de nombre pseudo aléatoire à travers les formules mathématiques de Suite de Fibonacci Modifiée (K_1) et de Chaotique Carte Logistique (K_2), mais à condition que chaque flux généré doive être même taille d'image en clair *n* x *n*.
    C. Convertir chaque valeur de K_2 à valeur entier par $K_2 * 255$
    D. Convertir les deux flux généré (K_1), (K_2) sous forme des bits.
    E. Faire la combinaison OU-exclusif (ou XOR) bit par bit entre ces flux généré. Pour obtenir un flux de clés pseudo aléatoire (Clé).
    Clé = $K_1 \oplus K_2$
2) Convertir l'image en clair à un flux de données sous forme des bits m_i
3) Faire la combinaison OU-exclusif (ou XOR) bit par bit entre le flux de données (l'image en clair) et flux de clés pseudo aléatoire. Pour obtenir un flux de données chiffrés (image chiffrée C_i) $C_i = m_i \oplus$ Clé.

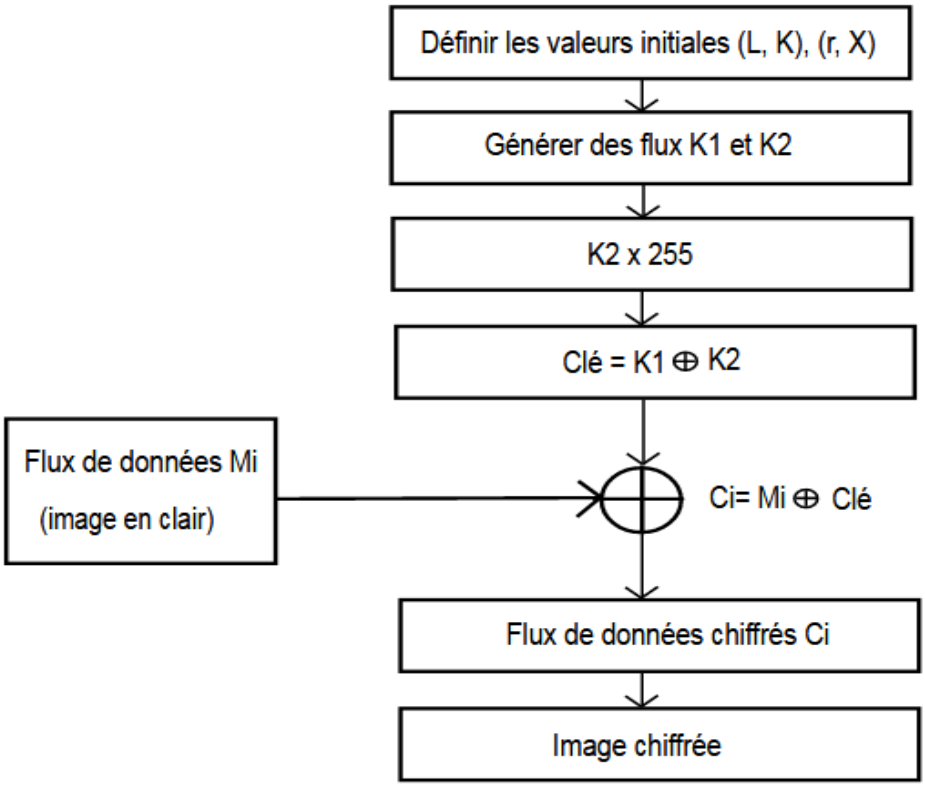

Figure 3.3 : Fonction de chiffrement.

2.3. Fonction de déchiffrement

1) Générer un flux de clés pseudo aléatoire
    A. Définir le même paramètre qui vous utilisé dans la fonction de chiffrement pour la Suite de Fibonacci Modifiée (*L*, *K*) et Chaotique Carte Logistique (*r*, *X*).
    B. Générer deux flux de nombre pseudo aléatoire à travers les formules mathématiques de Suite de Fibonacci Modifiée (K_1) et de Chaotique carte logistique (K_2), mais à condition que chaque flux généré doive être même taille d'image en clair *n* x *n*.
    C. Convertir chaque valeur de K_2 à valeur entier par $K_2 * 255$
    D. Convertir les deux flux généré (K_1), (K_2) sous forme des bits.
    E. Faire la combinaison OU-exclusif (ou XOR) bit par bit entre ces flux généré. Pour obtenir un flux de clés pseudo aléatoire (Clé) Clé = $K_1 \oplus K_2$.
2) Convertir l'image chiffrée à un flux de données sous forme des bits C_i
3) Faire la combinaison OU-exclusif (ou XOR) bit par bit entre le flux de données (l'image chiffrée) et flux de clés pseudo aléatoire. Pour obtenir un flux de données (image en clair m_i) m_i = $C_i \oplus$ Clé.

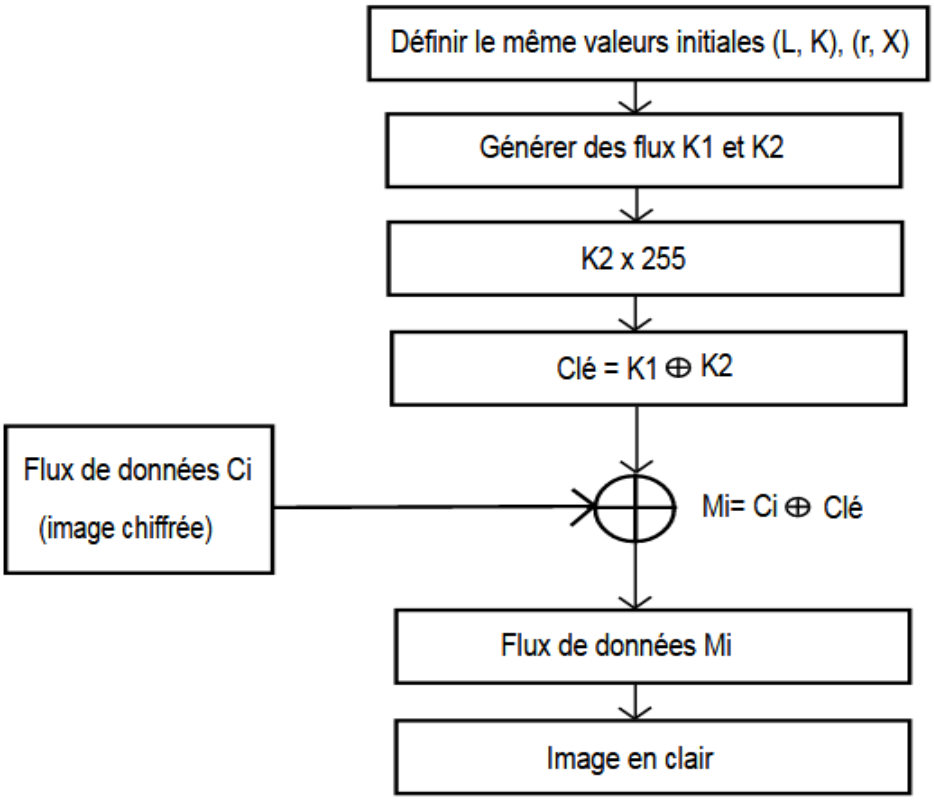

Figure 3.4 : Fonction déchiffrement.

3. Résultats expérimentaux

3.1. Environnement de développement

L'application a été créa depuis un PC Dell Inspiron N5010 :

- Mémoire : 6000 MB RAM
- Processeur : Intel ® Core™ i5 CPU M 480 @ 2.67 GHZ (4 CPUs)
- Système d'exploitation : Windows 7 Ultimate 64 bits
- Carte Graphique : ATI Mobility Radeon HD 6370

3.2. Langage de programmation

Nous avons choisi le langage ***JAVA*** pour développer notre système. Ce choix de langage est motivé par les raisons suivantes :

- Java est organisée, il contient des classes bien conçu et bien reparties.
- Java est connu et donc plus de chance de trouver des développeurs java, pour concevoir ou amélioré une application.

- Java est portable (donc exécutable sur n'importe quel système, à condition d'avoir installé une JVM).
- Java est gratuite.

Nous avons exploité l'environnement de programmation ***Netbeans*** IDE. Et utilisé l'environnement ***SWING*** pour la réalisation de l'interface graphique.

Les bibliothèques utilisées :

- jfreechart-1.0.19.
- jai_imageio-1.1.

3.3. L'architecture de l'application

Dans notre application nous avons utilisé motif *Modèle-Vue-Contrôleur* (abr. MVC), ce motif est composé de trois types de modules ayant trois responsabilités différentes: les modèles, les vues et les contrôleurs.

- Un modèle contient les données à afficher.
- Une vue contient la présentation de l'interface graphique.
- Un contrôleur contient la logique concernant les actions effectuées par l'utilisateur.

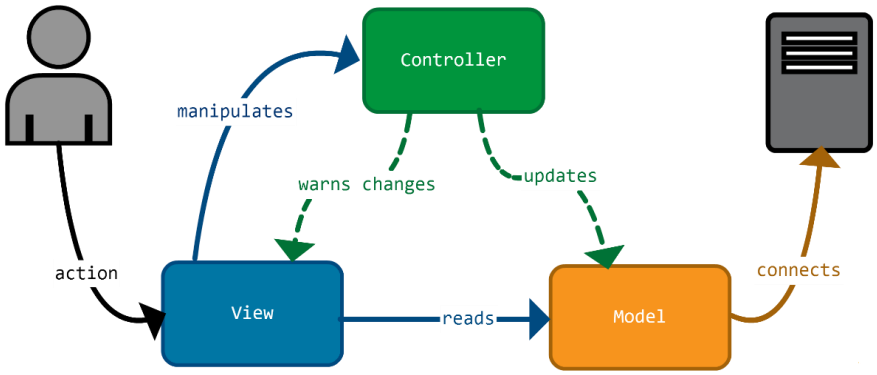

Figure 3.5 : Motif MVC.

Ce choix d'architecture logicielle motivé par les raisons suivantes :

- Une conception ***claire*** et ***efficace*** grâce à la séparation des données de la vue et du contrôleur.
- Une plus ***grande souplesse*** pour organiser et développer du logicielle.
- Un ***gain de temps*** de maintenance et d'évolution du logicielle.

3.4. Les interfaces du logiciel développé

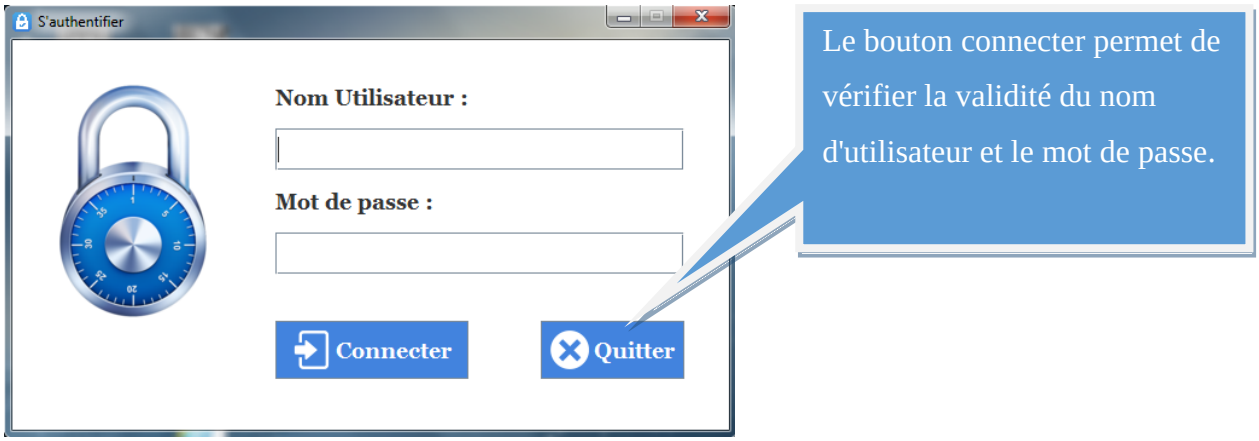

Figure 3.6 : Forme d'authentification.

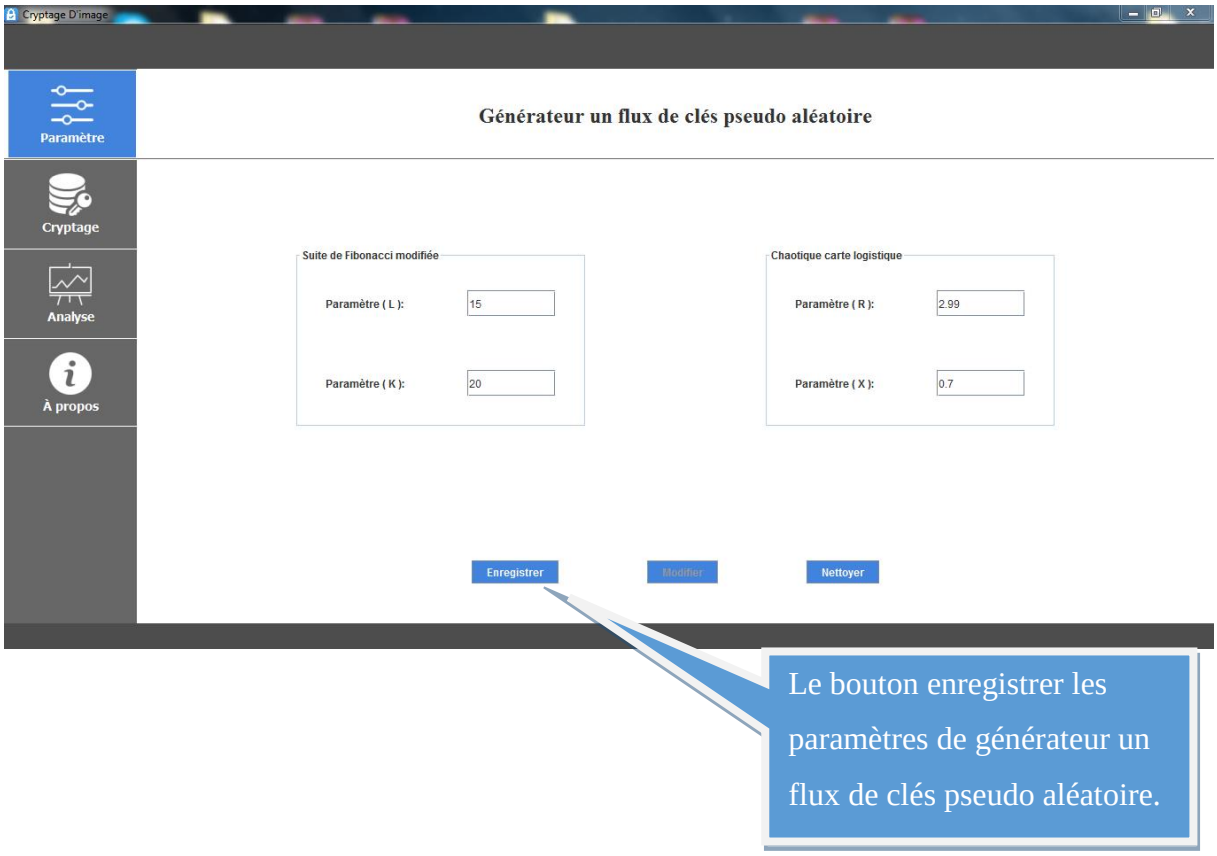

Figure 3.7: Forme de paramètres.

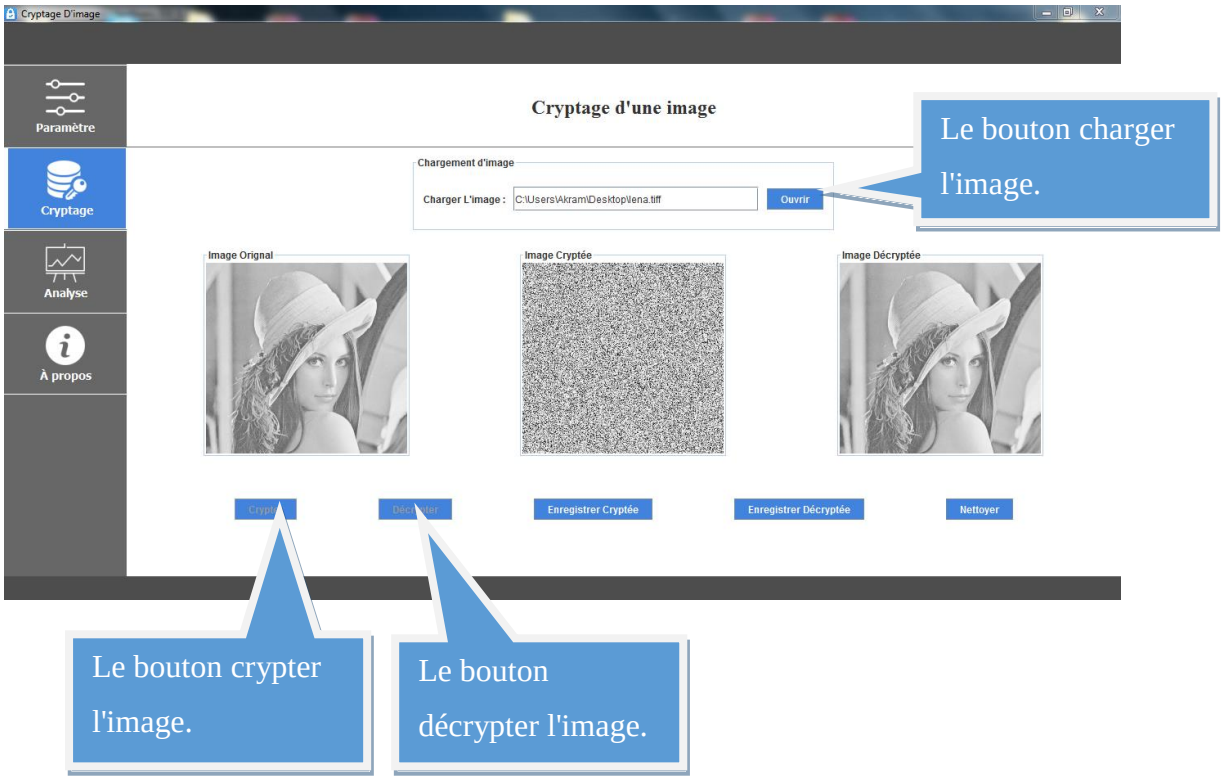

Figure 3.8 : Forme de cryptage.

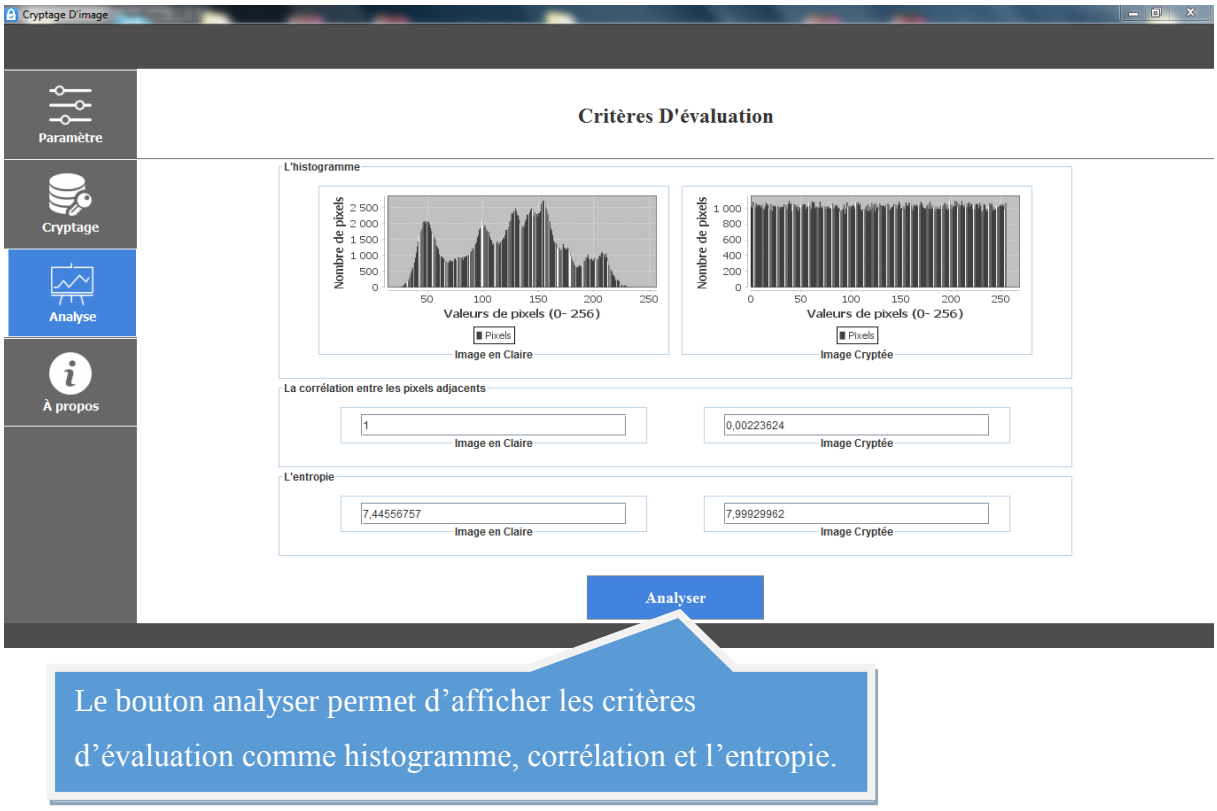

Figure 3.9 : Forme d'évaluation.

3.5. 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 Southern California [58], Et University of Waterloo [59], Et le dernier University of Wisconsin-Madison [60].

Ces images sont conçues pour le traitement et d'analyse d'un cryptage d'images numériques.

3.6. Images niveau de gris

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 l'algorithme proposé.

Figure 3.10 : Les images claires.

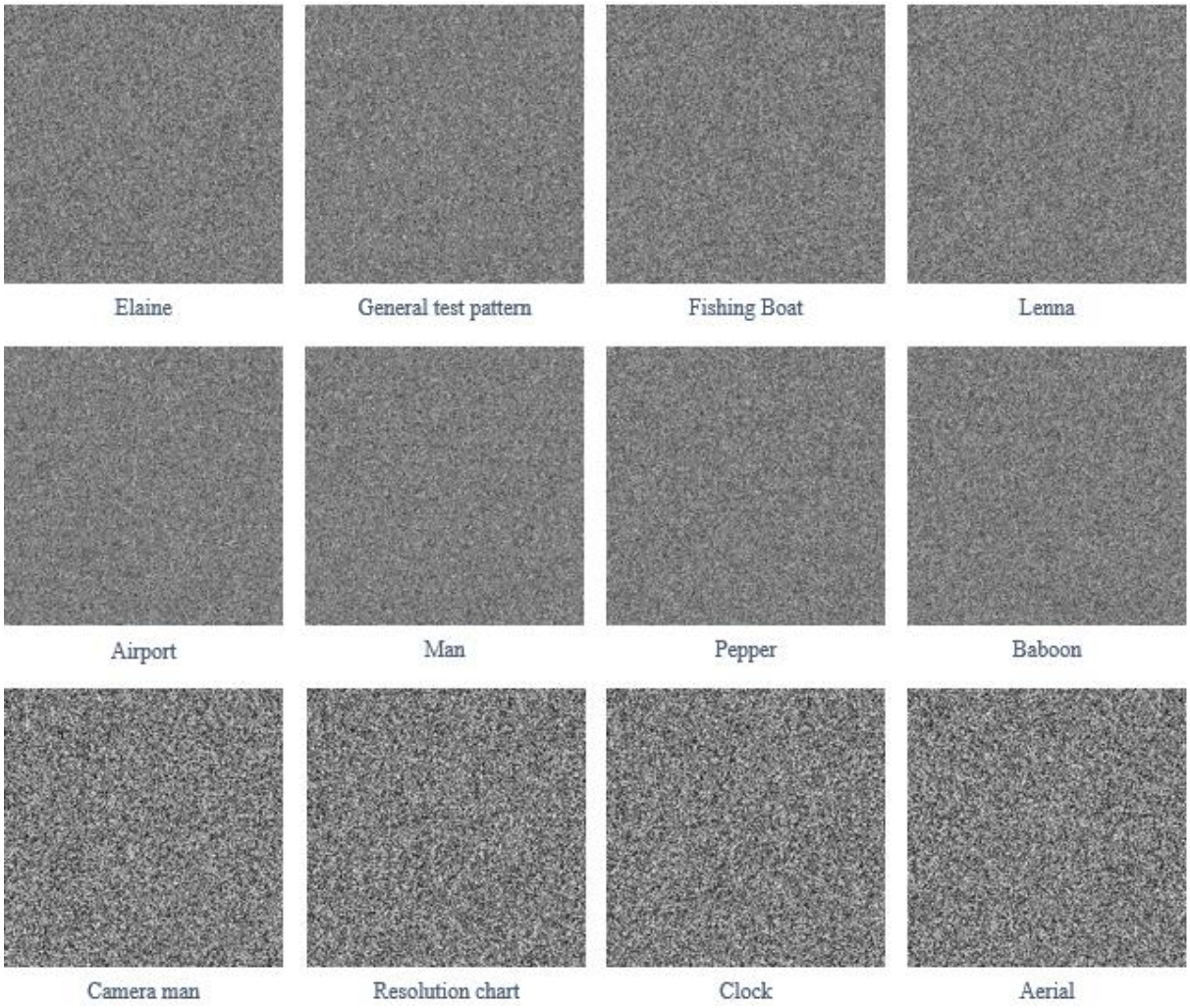

Figure 3.11 : Les images cryptées.

Figure 3.12 : Les images décryptées.

3.7. Images médicales

Récemment, les dossiers médicaux électroniques ont été envoyés largement sur les réseaux et l'Internet afin d'améliorer les services [61, 62, 63]. Alors les images médicales doivent être cryptées avant d'être envoyées sur les réseaux. Donc Les Figures au-dessous montre plusieurs images médicales sont cryptées en utilisant l'algorithme proposé.

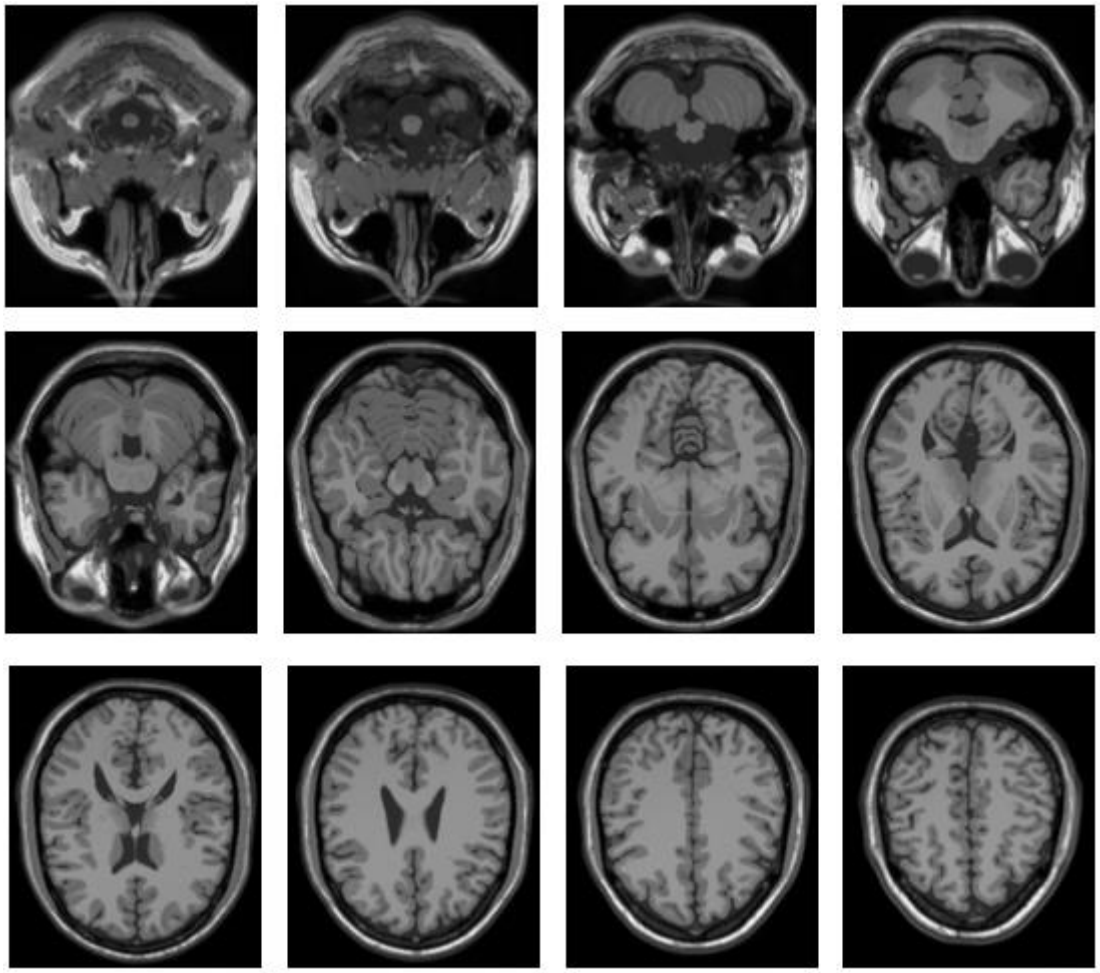

Figure 3.13 : Les images médicales claires.

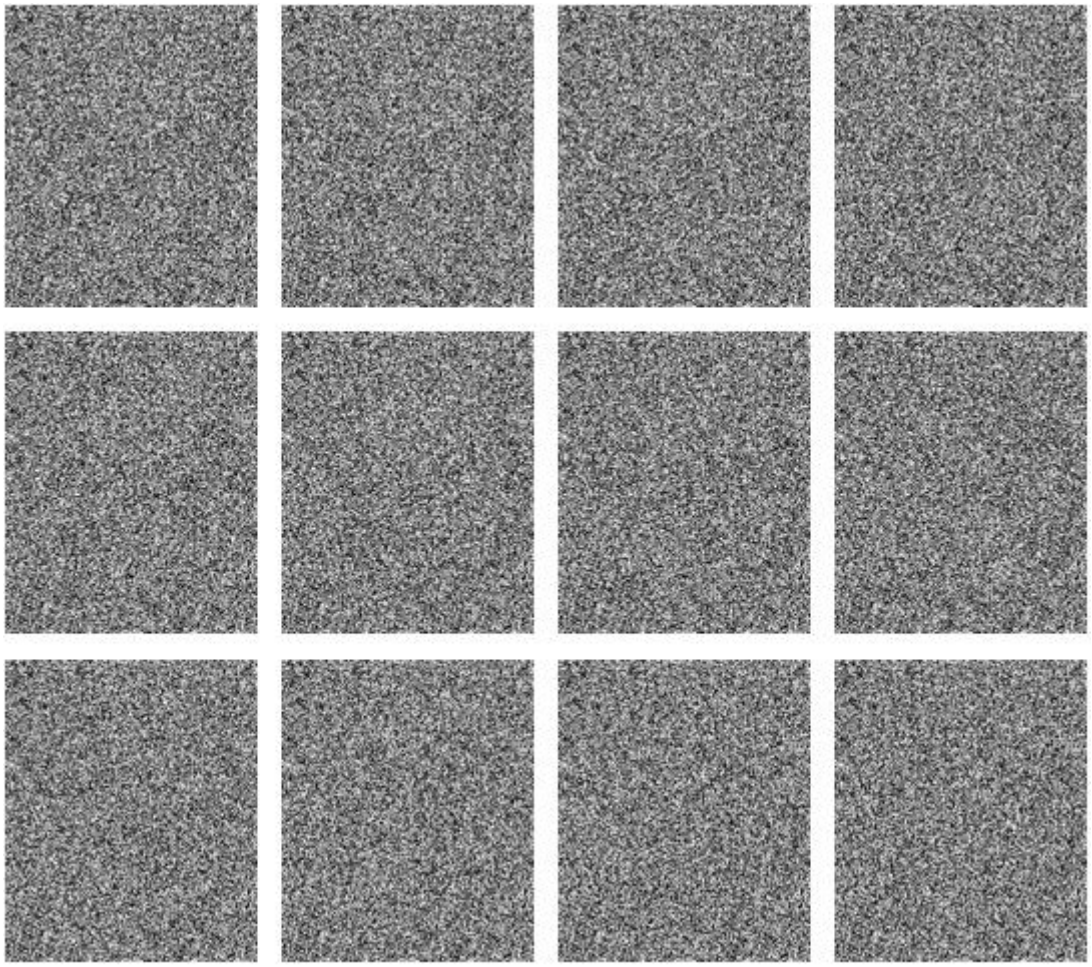

Figure 3.14 : Les images médicales cryptées.

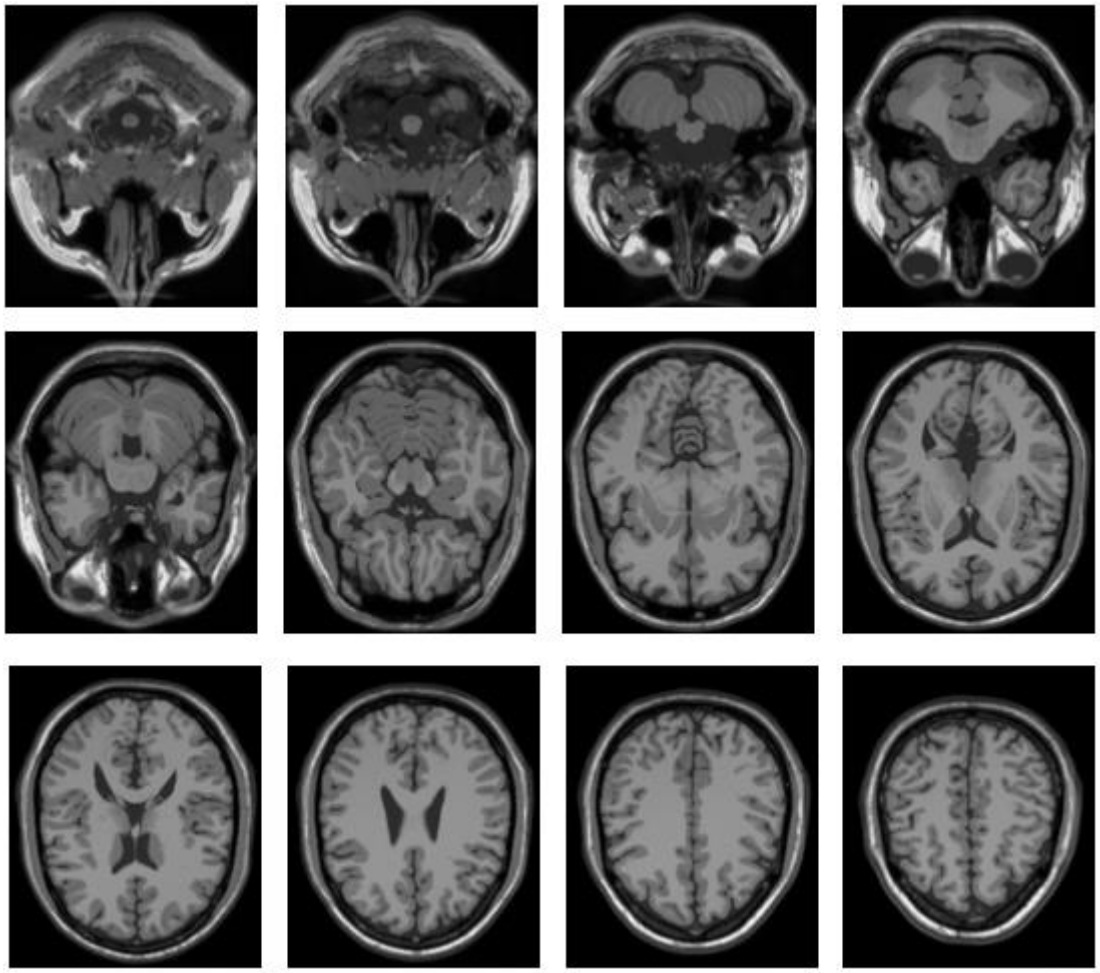

Figure 3.15 : Les images médicales décryptées.

4. Critères d'évaluation

Un bon système de cryptage devrait résister à toutes sortes d'attaques connues, 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 proposé. Nous allons présenter les plus important comme : l'espace de clés, L'histogramme, L'entropie, La corrélation entre les pixels adjacents.

4.1. Espace de clés

Un bon algorithme de chiffrement doit être sensible aux clés de chiffrement et l'espace clé doit être suffisamment grand pour rendre les attaques de force brute impossibles. La clé utilisée dans notre schéma est des nombres pseudo aléatoires qui été généré par les paramètres (L, K, r, X), La taille de la clé secrète est *n* x *n* c'est la taille de l'image originale, alors chaque élément

dans les nombres pseudo aléatoires est codé sur 8 bits. Donc l'espace de clés c'est2^{8*n*n}. Par exemple pour une image de taille 256 x 256 l'espace de clés c'est $2^{8*256*256}$.

4.2. L'histogramme

Trois images de tests ont été utilisées dans l'analyse : Lena, Peppers et Baboon. Les tracés des histogrammes des images et les images chiffrées sont montrés dans les figures ci-dessous

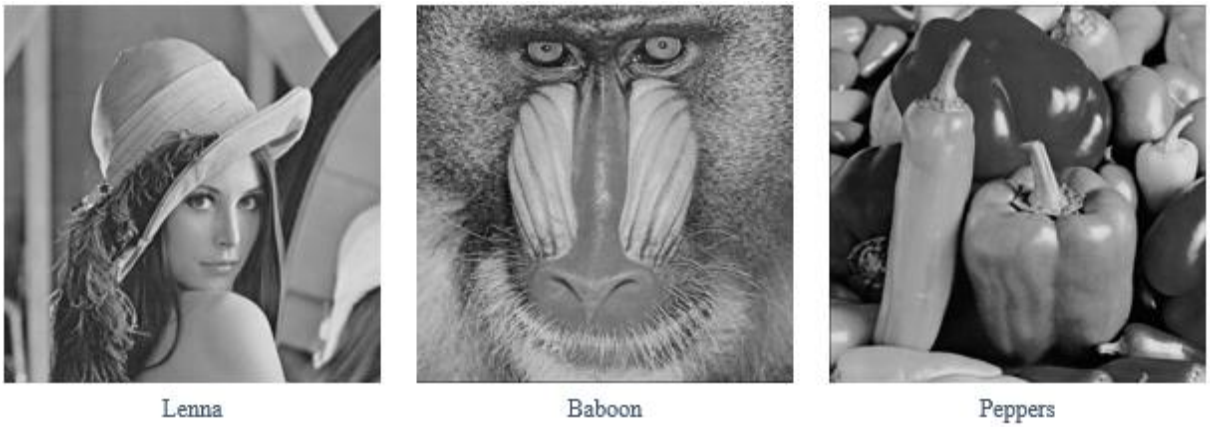

Figure 3.16 : Les images claires.

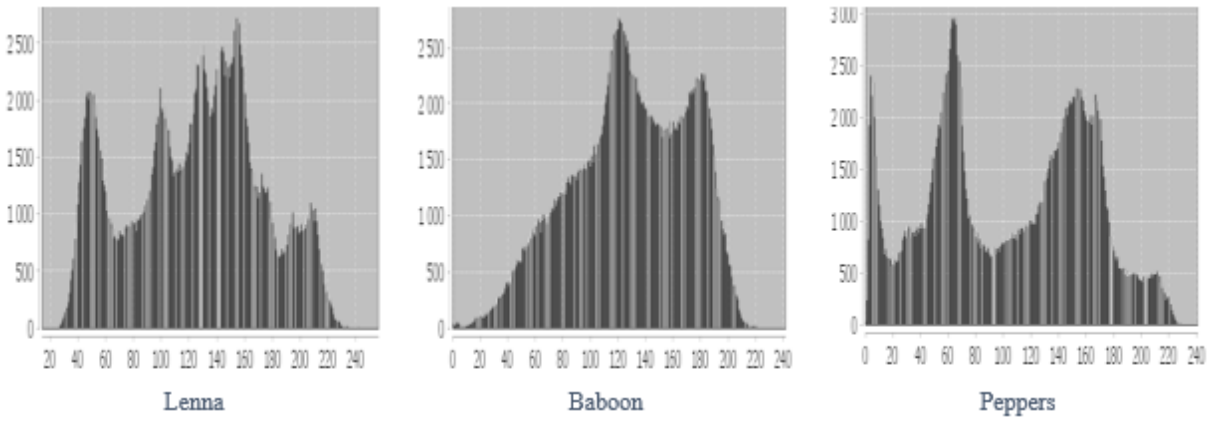

Figure 3.17 : Histogrammes sur les images en claires.

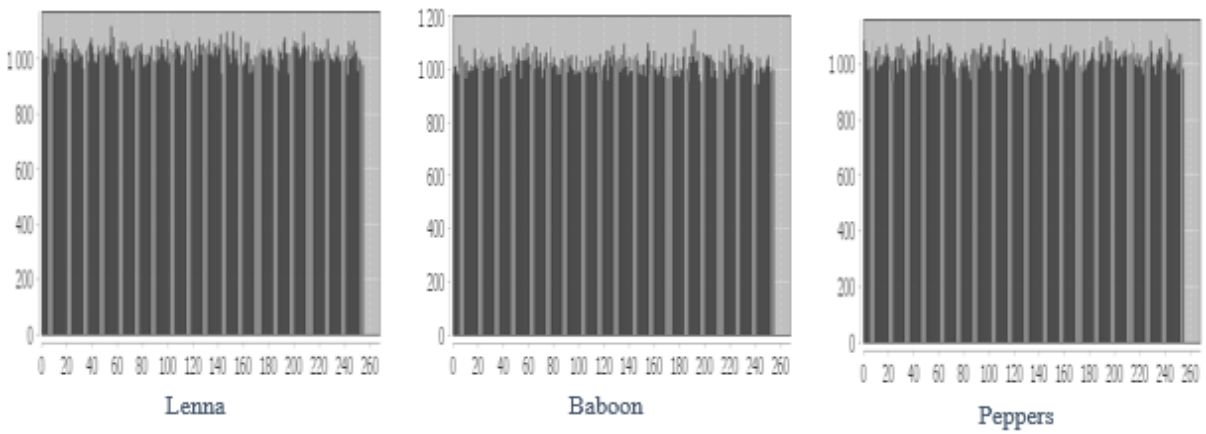

Figure 3.18 : Histogrammes sur les images cryptées.

Le résultat montre que les histogrammes des images chiffrées 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 ci-dessous liste les valeurs de l'entropie des images claires et leurs chiffrées en utilisant le schéma proposé.

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.

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

Nom de l'image	Description de l'image	Taille	Type	Entropie de l'image en claire	Entropie de l'image chiffrée
5.1.09.tiff	Moon surface	256×256	Niveau de gris	6,7093	7,9976
5.1.10.tiff	Aerial	256×256	Niveau de gris	7,3118	7,9969
5.1.11.tiff	Airplane	256×256	Niveau de gris	6,4522	7,9973
5.1.12.tiff	Clock	256×256	Niveau de gris	6,7056	7,9970
5.1.13.tiff	Resolution chart	256×256	Niveau de gris	6,5483	7,9966
5.1.14.tiff	Chemical plant	256×256	Niveau de gris	7,3424	7,9971
5.2.08.tiff	Couple	512×512	Niveau de gris	7,2010	7,9992
5.2.09.tiff	Aerial	512×512	Niveau de gris	6,9939	7,9993
5.2.10.tiff	Stream and bridge	512×512	Niveau de gris	5,7055	7,9993
5.3.01.tiff	Man	1024×1024	Niveau de gris	7,5237	7,9997
5.3.02.tiff	Airport	1024×1024	Niveau de gris	6,8303	7,9998
7.1.01.tiff	Truck	256×256	Niveau de gris	6,0274	7,9993

7.1.02.tiff	Airplane	1024×1024	Niveau de gris	4,0044	7,9992
7.1.03.tiff	Tank	512×512	Niveau de gris	5,4957	7,9993
7.1.04.tiff	Car and APCs	512×512	Niveau de gris	6,1074	7,9993
7.1.05.tiff	Truck and APCs	512×512	Niveau de gris	6,5631	7,9993
7.1.06.tiff	Truck and APCs	512×512	Niveau de gris	6,6952	7,9993
7.1.07.tiff	Tank	512×512	Niveau de gris	5,9915	7,9992
7.1.08.tiff	APC	512×512	Niveau de gris	5,0534	7,9992
7.1.09.tiff	Tank	512×512	Niveau de gris	6,1898	7,9992
7.1.10.tiff	Car and APCs	512×512	Niveau de gris	5,9087	7,9991
7.2.01.tiff	Airplane (U-2)	1024×1024	Niveau de gris	5,6414	7,9997
boat.512.tiff	Fishing Boat	512×512	Niveau de gris	7,1913	7,9992
elaine.512.tiff	Girl (Elaine)	512×512	Niveau de gris	7,5059	7,9993
gray21.512.tiff	21 level step wedge	512×512	Niveau de gris	4,3922	7,9992
numbers.512.tiff	256 level test pattern	512×512	Niveau de gris	7,7292	7,9993
ruler.512.tiff	Pixel ruler	512×512	Niveau de gris	7,5000	7,9984
testpat.1k.tiff	General test pattern	1024×1024	Niveau de gris	4,4077	7,9996
camera_man.tiff	Camera man	256×256	Niveau de gris	7,0097	7,9972
lena.tiff	Girl (lena)	512×512	Niveau de gris	7,4455	7,9992
peppers.tiff	Peppers	512×512	Niveau de gris	7,5714	7,9992
Baboon.tiff	Baboon	512×512	Niveau de gris	7,3579	7,9992
Moyenne				**6,0973**	**7,9988**

Le résultat montre qu'après simuler de 32 images, la valeur moyenne de l'entropie des images chiffrées est **7,9988**, c'est-à-dire il est plus proche à la valeur 8. Cela montre qu'il est difficile d'avoir la prévisibilité.

4.4. La corrélation entre les pixels adjacents

Le tableau ci-dessous liste les corrélations des images claires et leurs chiffrées en utilisant le schéma proposé.

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

Table 3.2 : Comparaison de corrélations entre les images en claire et chiffrée.

Nom de l'image	Description de l'image	Taille	Type	Corrélation de l'image en claire	Corrélation de l'image chiffrée
5.1.09.tiff	Moon surface	256×256	Niveau de gris	1,0	0,0007
5.1.10.tiff	Aerial	256×256	Niveau de gris	1,0	0,0017
5.1.11.tiff	Airplane	256×256	Niveau de gris	1,0	0,0033
5.1.12.tiff	Clock	256×256	Niveau de gris	1,0	0,0033
5.1.13.tiff	Resolution chart	256×256	Niveau de gris	0,99	0,0003
5.1.14.tiff	Chemical plant	256×256	Niveau de gris	1,0	-0,0014
5.2.08.tiff	Couple	512×512	Niveau de gris	0,99	-0,0004
5.2.09.tiff	Aerial	512×512	Niveau de gris	0,99	-0,0016
5.2.10.tiff	Stream and bridge	512×512	Niveau de gris	1,0	0,0014
5.3.01.tiff	Man	1024×1024	Niveau de gris	0,9	-0,0001
5.3.02.tiff	Airport	1024×1024	Niveau de gris	0,9	-0,0009
7.1.01.tiff	Truck	256×256	Niveau de gris	1,0	-0,0009
7.1.02.tiff	Airplane	1024×1024	Niveau de gris	1,0	0,0024
7.1.03.tiff	Tank	512×512	Niveau de gris	1,0	-0,0006
7.1.04.tiff	Car and APCs	512×512	Niveau de gris	1,0	-0,0002
7.1.05.tiff	Truck and APCs	512×512	Niveau de gris	0,99	-0,0015
7.1.06.tiff	Truck and APCs	512×512	Niveau de gris	1,0	-0,0005
7.1.07.tiff	Tank	512×512	Niveau de gris	1,0	-0,0003
7.1.08.tiff	APC	512×512	Niveau de gris	1,0	0,0005
7.1.09.tiff	Tank	512×512	Niveau de gris	0,99	-0,0021
7.1.10.tiff	Car and APCs	512×512	Niveau de gris	0,99	0,0009
7.2.01.tiff	Airplane (U-2)	1024×1024	Niveau de gris	1,0	-0,0006
boat.512.tiff	Fishing Boat	512×512	Niveau de gris	1,0	0,0003
elaine.512.tiff	Girl (Elaine)	512×512	Niveau de gris	1,0	0,0004
gray21.512.tiff	21 level step wedge	512×512	Niveau de gris	0,99	0,0007
numbers.512.tiff	256 level test pattern	512×512	Niveau de gris	1,0	-0,0018
ruler.512.tiff	Pixel ruler	512×512	Niveau de gris	1,0	0,0007
testpat.1k.tiff	General test pattern	1024×1024	Niveau de gris	0,9	-0,0021
camera_man.tiff	Camera man	256×256	Niveau de gris	1,0	-0,0012
lena.tiff	Girl (lena)	512×512	Niveau de gris	0,99	0,0002
peppers.tiff	Peppers	512×512	Niveau de gris	0,99	-0,0001
Baboon.tiff	Baboon	512×512	Niveau de gris	1,0	0,0022
Moyenne				**1,0**	**0,0011**

Le résultat montre qu'après simuler de 32 images, la valeur moyenne des corrélations dès l'image chiffrée est **0,0011**, c'est-à-dire il est plus proche à la valeur 0. Cela montre que les pixels adjacents après le cryptage n'ont pas de corrélation.

5. Étude comparative

Dans cette étude, nous avons comparé notre algorithme proposé avec les autres techniques de cryptage d'image, qui été proposé par les chercheurs de cryptographie.

On commence par la première comparaison, c'est l'algorithme proposé avec d'autres cinq algorithmes de cryptage d'image.

Le tableau ci-dessous liste : la comparaison entre l'algorithme proposé et les cinq autres algorithmes de cryptage, Et aussi la corrélation a été utilisée pour cette comparaison

Les valeurs initiales et le paramètre utilisé dans notre algorithme proposé pour cette comparaison sont : L=5, K=7, R=3.99, X=0.9.

Table 3.3 : Résultats de première comparaison.

Nom de l'image	**Description de l'image**	**Taille**	**Algorithme Proposé**	**Algo-1** [64]	**Algo-2** [64]	**Algo-3** [64]	**Algo-4** [65]	**Algo-5** [66]
5.1.09.tiff	Moon surface	256×256	0,0007	0,0054	0,0043	0,0866	-0,0322	-0,0101
5.1.10.tiff	Aerial	256×256	0,0017	0,0017	0,0057	0,1304	0,0065	0,0008
5.1.11.tiff	Airplane	256×256	0,0033	0,0035	0,0049	0,0965	-0,0189	-0,0077
5.1.12.tiff	Clock	256×256	0,0033	0,0037	0,0053	0,1552	-0,0424	-0,0041
5.1.13.tiff	Resolution chart	256×256	0,0003	-0,0043	-0,0061	0,1738	0,0083	-0,0118
5.1.14.tiff	Chemical plant	256×256	-0,0014	-0,0022	-0,0022	0,1215	0,0046	-0,0179
5.2.08.tiff	Couple	512×512	-0,0004	0,0008	0,0028	0,1166	-0,0056	-0,0090
5.2.09.tiff	Aerial	512×512	-0,0016	-0,0052	0,0015	0,1086	0,0108	-0,0062
5.2.10.tiff	Stream and bridge	512×512	0,0014	0,0000	0,0009	0,1510	-0,0135	-0,0060
5.3.01.tiff	Man	1024×1024	-0,0001	0,0003	0,0055	0,1555	0,0125	-0,0015
5.3.02.tiff	Airport	1024×1024	-0,0009	0,0009	0,0003	0,0986	-0,0145	-0,0003
7.1.01.tiff	Truck	256×256	-0,0009	-0,0019	-0,0022	0,0776	-0,0230	-0,0019
7.1.02.tiff	Airplane	1024×1024	0,0024	-0,0019	0,0014	0,0602	-0,0177	-0,0069
7.1.03.tiff	Tank	512×512	-0,0006	-0,0000	0,0003	0,0781	-0,0076	-0,0066
7.1.04.tiff	Car and APCs	512×512	-0,0002	-0,0007	0,0006	0,0998	-0,0020	-0,0112
7.1.05.tiff	Truck and APCs	512×512	-0,0015	0,0007	-0,0013	0,0995	0,0086	-0,0021
7.1.06.tiff	Truck and APCs	512×512	-0,0005	-0,0042	-0,0065	0,0923	-0,0180	-0,0066

7.1.07.tiff	Tank	512×512	-0,0003	-0,0001	-0,0016	0,0730	-0,0017	0,0013
7.1.08.tiff	APC	512×512	0,0005	0,0032	0,0017	0,0757	-0,0024	-0,0030
7.1.09.tiff	Tank	512×512	-0,0021	-0,0010	0,0012	0,1050	-0,0442	0,0063
7.1.10.tiff	Car and APCs	512×512	0,0009	-0,0003	-0,0008	0,0784	-0,0174	-0,0100
7.2.01.tiff	Airplane (U-2)	1024×1024	-0,0006	0,0001	-0,0094	0,0643	0,0038	-0,0063
boat.512.tiff	Fishing Boat	512×512	0,0003	0,0009	-0,025	0,1314	-0,0214	-0,0043
elaine.512.tiff	Girl (Elaine)	512×512	0,0004	-0,0027	0,0006	0,1304	-0,0032	-0,0098
gray21.512.tiffX	21 level step wedge	512×512	0,0007	-0,0026	0,0030	0,2009	-0,0115	-0,0078
numbers.512.tiff	256 level test pattern	512×512	-0,0018	-0,0005	-0,0026	0,1689	0,0040	-0,0111
ruler.512.tiff	Pixel ruler	512×512	0,0007	0,0030	0,0006	0,1836	0,0007	0,0031
testpat.1k.tiff	General test pattern	1024×1024	-0,0021	0,0005	0,0009	0,1952	-0,0149	-0,0007
Moyenne			**0,0011**	**0,0018**	**0,0027**	**0,1181**	**0,0132**	**0,0062**

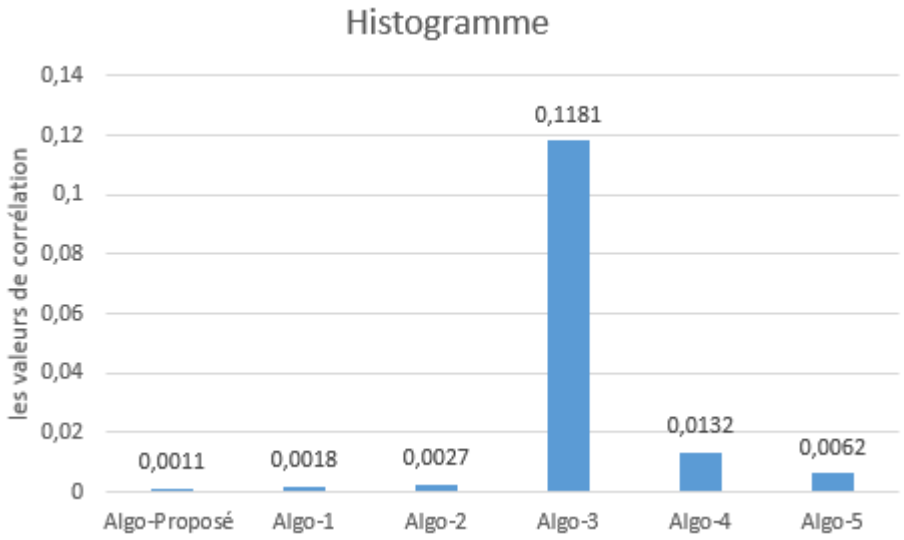

Figure 3.19 : Histogramme comparatif.

Le résultat après le calcul de la valeur moyenne de corrélation de chaque algorithme, montre d'une part que la valeur moyenne obtenue par notre algorithme proposé est inférieure aux celles obtenues par les différents cinq algorithmes cités. D'autres parts, cette valeur est plus proche à la valeur 0 ce qui signifié que les données sont sécurisées efficacement par notre système proposé.

Pour mieux évaluer notre méthode de cryptage, une deuxième comparaison a été établie avec un autre travail proposé dans [29]. Ce dernier est basé sur l'utilisation de la Suite de Fibonacci modifiée pour le cryptage d'image. Les résultats obtenus en utilisant l'entropie et la corrélation comme critères d'évaluation sont présentés dans le tableau 3.4 ci-dessous :

Table 3.4 : Résultats de deuxième comparaison.
(L=5, K=7, R=3.99, X=0.9)

Nom de l'image	**Description de l'image**	**Algorithme proposé**		**Algorithme dans [29]**	
		Entropie de l'image chiffrée	**Corrélation de l'image chiffrée**	**Entropie de l'image chiffrée**	**Corrélation de l'image chiffrée**
Lena.png	Girl (Lena)	7,9974	0,0022	7,9551	0,0014
Cameraman.tif	Camera man	7,9972	-0,0012	7,9415	-0,0075
Peppers.png	Peppers	7,9992	-0,0001	7,9465	-0,0042
Mandrill.jpg	Mandrill	7,9993	0,0018	7,9506	0,0052
Clown.bmp	Clown	7,9994	0,0001	7,9542	0,0006
Barbara.png	Barbara	7,9993	-0,0015	7,9547	-0,0017
Boat.png	Fishing Boat	7,9992	-0,0012	7,9541	-0,0040
Moyenne		**7,9987**	**0,0011**	**7.9509**	**0.0035**

A partir du tableau 3.4, on peut remarquer que la valeur moyenne de l'entropie de notre algorithme est supérieure de celle proposé [29]. De plus, cette valeur est plus proche à la valeur 8 par rapport ce qui indique son efficacité. La valeur moyenne de corrélation de notre algorithme proposé est inférieure de l'algorithme présenté dans [29]. Aussi, elle est plus proche à la valeur 0 ce qui confirme la qualité de la sécurité des images utilisées.

6. Conclusion

Dans ce chapitre, nous avons proposé un schéma de chiffrement d'image qui basé sur l'hybridation entre deux algorithmes, le premier algorithme basé sur Chaotique carte logistique, et le deuxième algorithme basé sur Suite de Fibonacci modifiée. Les résultats expérimentaux ont montré que le système de cryptage d'image proposé possède un grand espace de clés et une sécurité de haut niveau. Ainsi l'analyse prouve la sécurité, et l'efficacité. De plus, les comparaisons avec les schémas de chiffrement d'image existants qui ont été réalisées, montrent que l'algorithme proposé offre des performances très favorables.

Conclusion générale

De nos jours, de plus en plus les images numériques sont transférées ou stockées sur les réseaux informatiques. Avec le temps, la confidentialité d'image numérique est devenue indispensable. Au cours de ce mémoire, nous avons proposé un schéma de chiffrement d'image basé sur l'hybridation entre deux algorithmes, le premier algorithme basé sur Chaotique Carte Logistique, et le deuxième algorithme basé sur Suite de Fibonacci Modifiée. Le but principal de ce chiffrement est la combinant les propriétés et les avantages entre eux.

Les résultats expérimentaux montrent clairement, que l'algorithme proposé 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 proposé a été atteintes beaucoup amélioré sur l'entropie et la corrélation entre les pixels adjacents. De ce fait l'algorithme proposé montre l'efficacité et la sécurité de notre système proposé.

Finalement les comparaisons avec les schémas de chiffrement d'image existants qui ont été réalisées, montrent que l'algorithme proposé offre des performances très favorables.

Comme perspective à ce travail, nous allons améliorer notre approche sur les images couleur, et de même utiliser d'autres bases d'images. Et de plus faire de comparaisons sur d'autres travaux récents.

Bibliographie

[1] A. bayad. Introduction à la cryptographie. Université d'evry val d'essonne, 2008. Https://www.maths.univ-evry.fr/.

[2] G. Labouret. Introduction à la cryptographie. HSC - Herve Schauer Consultants - Cabinet de consultants en sécurité informatique 2001, Http://www.hsc.fr/.

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

[4] Cryptographie symétrique. Wikipedia, https://fr.wikipedia.org/wiki/Cryptographie_symétrique/.

[5] Public Key Infrastructure (PKI). Institut d'électronique et d'informatique Gaspard-Monge, http://igm.univ-mlv.fr/~dr/XPOSE2007/vma_PKI/concepts_de_base.html/.

[6] R. Dumont. Cryptographie et Sécurité informatique, Université de liége faculté des sciences appliquées 2007, https://www.ulg.ac.be.

[7] Les systèmes à clé publiques. CCM - Comment ça marche - Communauté informatique, http://www.commentcamarche.net/contents/201-les-systemes-a-cle-publiques/.

[8] A. Dragut. RSA, Cours de cryptographie Chapitre III. Université Aix-Marseille, 2012

[9] Pierre-Louis Cayrel. Chiffrement par blocs. Université de Limoges, 2015. https://www.cayrel.net/.

[10] Algorithmes de cryptage : «D.E.S.». Algorithmique / Programmation. http://lwh.free.fr/pages/algo/crypto/des.htm/.

[11] Le standard de chiffrement AES. La bibliothèque des Mathématiques. http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/aes/.

[12] L'AES : Advanced Encryption Standard. La sécurité informatique - La sécurité des informations. https://www.securiteinfo.com/cryptographie/aes.shtml/.

[13] P. Zimmermann, L. Fousse. Chiffrement symétrique : Chiffrement par bloc, par flot. Loria, http://www.loria.fr/.

[14] R. Dumont. Le chiffrement par blocs. Montefiore Institute ULg. http://www.montefiore.ulg.ac.be/.

[15] RC4. Wikipedia, https://fr.wikipedia.org/wiki/RC4/.

[16] JP BUNTINX. The attack on cryptographic cipher rc4, 2015. http://bitcoinist.com/httpstls-rc4-vulnerability-serious-threat-bitcoin-platforms/.

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

[18] Image numérique. Numeriksciences. Http://numeriksciences.fr,

[19] Qu'est-ce qu'une image numérique. Université Rennes 2. https://www.sites.univ-rennes2.fr/.

[20] R. Isdant. Traitement numérique de l'image.2009

[21] Traitement d'images en Java. Http://slim-boukettaya.developpez.com/tutoriels/traitement-images-java/.

[22] Les images vectorielles et matricielles. http://www.imedias.pro/cours-en-ligne/graphisme-design/definition-resolution-taille-image/les-images-vectorielles-matricielles/.

[23] O. Poutarédy. Différences entre image Bitmap et image vectorielle. Site des enseignants en Arts Appliqués de l'académie d'Orléans-Tours, 2015

[24] C. alleau. Images numériques. Physique - Chimie - Académie de Poitiers. Http://ww2.ac-poitiers.fr/.

[25] Image file formats. Wikipedia, Https://en.wikipedia.org/wiki/Image_file_formats.

[26] Utiliser l'histogramme. PhotoFiltre Studio, http://www.photofiltre-studio.com/doc/histogramme.htm

[27] Suite de fibonacci. Collège Le Castillon - académie de Caen. Http://le-castillon.etab.ac-caen.fr/

[28] Yvan MONKA - Académie de Strasbourg. La suite de fibonacci. Maths et tiques http://www.maths-et-tiques.fr/

[29] Adda ALI-PACHA, Naima HADJ SAID, Suite de Fibonacci Généralisée appliquée à la confidentialité des Données. Actes de la Conférence Internationale sur le Traitement de l'Information Multimédia CITIM, 2015.

[30] Yicong Zhou, Karen Panetta, Sos Agaian, and CL Philip Chen. Image encryption using p-fibonacci transform and decomposition. Optics Communications, 285(5): 594–608, 2012.

[31] Weijia Cao, Yicong Zhou, C.L. Philip Chen. A New Image Encryption Algorithm Using Truncated P-Fibonacci Bit-planes. IEEE International Conference on Systems, Man, and Cybernetics, 2012.

[32] Zhang, H. and J.-x. Dong. "Chaos theory and its application in modern cryptography in Computer Application and System Modeling (ICCASM)", International Conference on, 2010.

[33] Amit P, Goseph Z., "A Chaotic Encryption Scheme for Real-time Embedded Systems: Design and Implementation, Department of Electrical and Computer Engineering, Iowa State University, Ames, USA, Springer, 2011.

[34] Wang Feng-ying, Cui Guo-wei, "A New Image Encryption Algorithm Based on the Logistic Chaotic System", Department of Information Engineer, Inner Mongolia University of Science & Technology, China, © IEEE, 2010.

[35] H. Hermassi, R. Rhouma, S. Belghith, "Improvement of an Image Encryption Algorithm Based on Hyper-chaos", National School of Engineers ENIT, Springer, 2011.

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

[37] Baydda Flaeh AL-Saraji, Mustafa Dhiaa AL-Hassani. Multi-Levels Image Encryption Technique based on Multiple Chaotic Maps and Dynamic Matrix, International Journal of Computer Applications: (0975 – 8887) Volume 151, 2016.

[38] G.A.Sathishkumar, Dr.K.Bhoopathy bagan, Dr.N.Sriraam. Image encryption based on diffusion and multiple chaotic maps. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, 2011.

[39] IshaMehra, Naveen K Nishchal. Optical asymmetric image encryption using gyrator wavelet transform. Optics Communications, 354:344–352, 2015.

[40] Wen Chen, Xudong Chen. Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain. Optics Communications, 284(16):3913–3917, 2011.

[41] Shutian Liu, Quanlin Mi, and Banghe Zhu. Optical image encryption with multistage and multichannel fractional fourier-domain filtering. Optics Letters, 26(16):1242–1244, 2001.

[42] G Unnikrishnan, J Joseph, and Kehar Singh. Optical encryption by double random phase encoding in the fractional Fourier domain. Optics Letters, 25(12):887–889, 2000.

[43] Pramod Kumar, Joby Joseph, and Kehar Singh. Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator. Applied optics, 50(13):1805–1811, 2011.

[44] Xiaopeng Deng. Optical image encryption based on real-valued coding and subtracting with the help of QR code. Optics Communications, 349:48–53, 2015.

[45] Xiangling Ding and Guangyi Chen. Optical color image encryption using position multiplexing technique based on phase truncation operation. Optics & Laser Technology, 57:110–118, 2014.

[46] Rasul Enayatifar, Abdul Hanan Abdullah, and Ismail Fauzi Isnin. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Optics and Lasers in Engineering, 56:83–93, 2014.

[46] Qiang Zhang, Ling Guo, and Xiaopeng Wei. A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik-International Journal for Light and Electron Optics, 124(18):3596–3600, 2013.

[48] Qiang Zhang and Xiaopeng Wei. A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system. Optik-International Journal for Light and Electron Optics, 124(23):6276–6281, 2013.

[49] Noorul Hussain UbaidurRahman, Chithralekha Balamurugan, Rajapandian Mariappan. A novel DNA computing based encryption and decryption algorithm. Procedia Computer Science, 46:463–475, 2015.

[50] Qiang Zhang, Ling Guo, Xiaopeng Wei. Image encryption using DNA addition combining with chaotic maps. Mathematical and Computer Modelling, 52(11):2028–2035, 2010.

[51] Olu Lafe. Data compression and encryption using cellular automata transforms. In Intelligence and Systems, IEEE International Joint Symposia on, pages 234–241. IEEE, 1996.

[52] Rong-Jian Chen and Jui-Lin Lai. Image security system using recursive cellular automata substitution. Pattern Recognition, 40(5):1621–1631, 2007.

[53] Xiao Wei Li, Sung Jin Cho, and Seok Tae Kim. A 3d image encryption technique using computer-generated integral imaging and cellular automata transform. Optik-International Journal for Light and Electron Optics, 125(13):2983–2990, 2014.

[54] Faraoun Kamel Mohamed. A parallel block-based encryption schema for digital images using reversible cellular automata. Engineering Science and Technology, an International Journal, 17(2):85–94, 2014.

[55] Narendra Singh, Aloka Sinha. Optical image encryption using fractional Fourier transform and chaos. Optics and Lasers in Engineering, 46(2):117–123, 2008.

[56] Dezhao Kong, Xueju Shen. Multiple-image encryption based on optical wavelet transform and multichannel fractional Fourier transform. Optics & Laser Technology, 57:343–349, 2014.

[57] Liansheng Sui, Kuaikuai Duan, Junli Liang, Zhiqiang Zhang, Haining Meng. Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain. Optics and Lasers in Engineering, 62:139–152, 2014.

[58] University of Southern California, Base de données d'images http://sipi.usc.edu/database/database.php?volume=misc.

[59] University of Waterloo, Base de données d'images http://links.uwaterloo.ca/Repository.html

[60] University of Wisconsin-Madison, Base de données d'images https://homepages.cae.wisc.edu/~ece533/images/.

[61] A Kanso and M Ghebleh. An efficient and robust image encryption scheme for medical applications. Communications in Nonlinear Science and Numerical Simulation, 2015.

[62] JB Lima, F Madeiro, and FJR Sales. Encryption of medical images based on the cosine number transform. Signal Processing: Image Communication, 35:1–8, 2015.

[63] Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic, and Ch Roux. An a priori and a posteriori protection by means of data hiding of encrypted images: application to ultrasound images. In The International Conference on Health Informatics, pages 220–223. Springer, 2014.

[64] F. K. Tabash, M.Q. Rafiq, M. Izharrudin. Image Encryption Algorithm based on Chaotic Map. International Journal of Computer Applications (0975 – 8887): Volume 64– No.13, 2013.

[65] Gao, Zhang, Liang, Li. A new chaotic algorithm for image encryption. Chaos Solitons Fractals, 29, pp.393–399, 2005.

[66] Pareek, Patidar, Sud. Image encryption using chaotic logistic map. Image and Vision Computing, 24, pp.926–934. 2006.

Global Research & Development Services

ACCEPTANCE/ INVITATION LETTER
(To Whom It May Concern)

22-May- 2017

Paper Title: A New Encryption System Applied to Digital Grayscale image
Paper ID: GICICHLSR1708094

Conference Name: 19th International Conference on Healthcare & Life-Science Research (ICHLSR)
Conference Dates: 28-Jul- 2017 to 29-Jul- 2017
Conference Venue: Universitat de Barcelona - Edifici Histic, Barcelona, Spain
Organizing Association: INTERNATIONAL ASSOCIATION FOR PROMOTION OF HEALTHCARE AND LIFE-SCIENCE RESEARCH (IAPHLSR)
Professional Conference Organizer: Global Research & Development Services

Name of Person Attending: Akram Aimeur
Affiliation: Department Of Computer Science,University of algeria,Msila, Algeria
Participation Category: Absentia
Author/ s : Aimeur Akram, Lamiche Chaabane

This International Conference aims to bring together industry, academia and professionals to exchange and share their scholarly ideas, research findings or experiences.
Herewith, the Conference Committee is pleased to inform you that the above mentioned delegate is cordially invited to participate in the aforesaid conference.

- *The conference committee highly appreciates the researcher's work, and we request all concerned authorities to cooperate in the funding/ leaves/ visa process.*
- *The original articles accepted for the conference will be double-blind peer reviewed and published in conference journals without any additional publication fee if the registered author fulfills reviewer/ editor guidelines within stipulated time.*
- *The co-authors (if any) are also cordially invited for the conference. They need to kindly apply and register separately.*
- *This invitation is conditional on fulfillment of required registration formalities.*
- *This letter also certifies that the delegate is also, free life-time member of the scholarly association organizing this conference.*

We would greatly appreciate if you could facilitate granting the conference delegate the necessary visa/ leaves/ grants.

Dr. D Lazarus
Conference Secretariat,
www.grdsweb.com
Email: info@grdsweb.com

الملخص

مع التقدم السريع في استخدام الصور الرقمية في العديد من التطبيقات، من المهم حماية بيانات الصورة السرية من الوصول غير المصرح به. في هذا العمل المخصص لمذكرة نهاية الدراسة، فقد اقترحنا خوارزمية تشفير جديدة والتي يمكن تطبيقها على الصور الرمادية، والتي تعتمد إلى التهجين بين خوارزميتين ، الخوارزمية الاولى تعتمد على خريطة لوجستية فوضوية، و الخوارزمية الثانية تعتمد على نظرية فيبوناكسي المعدلة. مقارنة أجريت مع خوارزميات حديثة لتشفير الصور تبين أن الخوارزمية المقترحة توفر أداءا تنافسيا للغاية.

الكلمات المفتاحية : الصور الرقمية ، الصورة السرية ، تشفير، خريطة لوجستية فوضوية ، فيبوناكسي المعدلة.

Abstract

With the fast progression of using digital images in many applications, it is important to protect the confidential image data from unauthorized access. In the end of this memory, we have proposed a new encryption algorithm, which can be applied to grayscale images, based on the hybridization between two algorithms, the first algorithm based on chaotic logistic map, and the second algorithm based on modified Fibonacci sequence. Comparisons with recent algorithms of images encryption were performed showing that the proposed algorithm provide highly favorable performances.

Key words: digital images, confidential image, encryption, chaotic logistic map, modified Fibonacci sequence.

Résumé

Avec la progression rapide de l'utilisation d'images numérique dans de nombreuses applications, Il est important de protéger les données d'image confidentielles contre les accès non autorisés. Dans ce mémoire de fin d'étude, Nous avons proposé un nouvel algorithme de chiffrement, qui peut être appliqué aux images en niveaux de gris, qui basé sur l'hybridation entre deux algorithmes, le première algorithme basé sur Chaotique carte logistique, et le deuxième algorithme basé sur suite de fibonacci modifiée. Des comparaisons avec des schémas de chiffrement d'images récemment proposés ont été réalisées montrant que l'algorithme proposé offre des performances très favorables.

Mots clés : Images numériques, images confidentielles, chiffrement, Chaotique carte logistique, suite fibonacci modifiée.