République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mohammed Seddik Ben Yahia - Jijel

Faculté des Sciences Exactes et Informatique
Département d'Informatique

Mémoire de fin d'études pour l'obtention du diplôme de

Master en Informatique

Option : Informatique Légale et Multimédia

Thème

Cryptage des images médicales à la base des cartes chaotiques

Présenté par :

- Frikha Houria
- Tellouche Ines

Encadré par :

Dr.Hemioud Mourad

Année Universitaire : 2021 - 2022

Dédicace

Je me dois d'avouer pleinement ma reconnaissance à toutes les personnes qui m'ont soutenue durant mon parcours, qui ont su me hisser vers le haut pour finaliser ce travail. C'est avec amour, respect et gratitude que,

Je dédie ce travail à :

mon père, qui veillait sur notre confort et notre éducation, j'espère qu'Allah prolonge sa vie afin de qu'il se réjouisse avec plus de succès.

celle qui m'a transmis la vie, l'amour, le courage, à toi **chère mère** toutes mes joies, mon amour et ma reconnaissance.

mes chère frères : Hocine et Hamza et rabeh.

toute ma famille.

ines et mes collègues de promotion.

des personnes spéciales dans ma vie, qu'ils étaient avec moi tout le temps.

tous ceux ou celles qui me sont chèrs.

tous mes enseignants tout au long de mes études.

tous ceux qui ont participé à la réalisation de ce travail.

Houria

Dédicace

C'est avec une grande émotion et un immense plaisir que je dédie, ce travail fabuleux à mes chers parents.

Mon père dont les qualités supérieures avec ses précieux conseils, son encouragement infini.

Ma mère bien aimée, adorable, compréhensive et chaleureuse.

Ces deux personnes mon soutenu durant cette période cruciale Sans se lasser, afin d'obtenir le résultat de longues années d'études.

J'exprime ma gratitude à ma sœur spirituelle **Sarah**, mon frère **mohamed Islam** qui m'a guidé.

J'adresse également mes remercîments à mes proches, mes amies, ma binôme **houria** , mes collègues de promotion et spécialement mes professeurs **jury**, mon encadreur.

Mes salutations les plus distinguées

Ines

Remerciements

Avant toute chose, nous rendons grâce à ***Allah*** *le tout puissant qui nous a fait ouvrir les portes du savoir, qui nous a donné le courage, la volonté, la force nécessaire durant tout notre cursus pédagogiques.*

Notre profonde gratitude à nos ***parents*** *pour leur soutien moral indéfectible.*

Nous tenons à remercie notre encadreur ***Dr Hemioud Mourad****, pour son aide, ses conseils, et ses orientations pour l'accomplissement de ce mémoire.*

Nous remercions également ***les membres du jury*** *qui nous ont honorés en acceptant l'invitation d'évaluer ce modeste travail.*

Enfin, nous tenons à exprimer notre reconnaissance à tous nos ***amis*** *et* ***collègues*** *pour le soutien moral et matériel.*

RÉSUMÉ

Dans ce mémoire,nous introduisons une nouvelle Génération d'une séquence pseudo-aléatoire définit à partir d'une fonction de comparaison entre deux cartes chaotiques la carte Pwlcm et la carte logistique. Pour évaluer le caractère aléatoire et la sensibilité aux conditions initiales ainsi que l'indépendance des séquences , générée par le générateur, des tests statistiques bien connus ont été effectués et les résultats ont confirmé que les séquences générées étaient statistiquement adaptées aux applications cryptographiques.

Dans ce travail nous avons proposé également un mécanisme de cryptage d'image pour sécuriser les données d'images médicales des utilisateurs non autorisés. Le crypto-système d'image basé sur le chaos est composé d'étapes alternatives de confusion et de diffusion.La carte Arnold généralisé est utilisée dans l'étape de confusion pour la permutation des pixels de l'image, tandis que notre Séquence proposée est utilisée à des fins de diffusion.Enfin, nous avons amélioré notre crypto-système proposé en ajoutant la méthode Salsa20.

Plusieurs simulations ont été effectuées pour prouver l'efficacité de Système proposé.
Les résultats obtenus par les simulations ont démontré la haute sécurité de Crypto-système, donc notre Système peut sécuriser efficacement plusieurs formats d'images médicales et est également résistant à diverses attaques de sécurité telles que la force brute, l'homme du milieu, etc...

Mots clés : Séquence pseudo-aléatoire, Caractère aléatoire, Tests statistiques, Cartes chaotiques, Les applications cryptographiques, Crypto-système, Confusion, Diffusion, Salsa 20, Images médicales.

ABSTRACT

In this thesis, we introduce a new Generation of a pseudo-random sequence defined from a comparison function between two chaotic maps the Pwlcm map and the logistic map. To evaluate the randomness and sensitivity to initial conditions as well as the independence of the sequences, generated by the generator, some well-known statistical tests were performed and the results confirmed that the generated sequences are statistically appropriate in cryptographic applications.

In this work we also proposed an image encryption mechanism to secure medical image data from unauthorized users.The chaos-based image crypto-system is composed of alternate stages of confusion and diffusion. The generalized Arnold map is used in the confusion stage for image pixel permutation, while our Proposed Sequence is used for diffusion purposes. At the end we improved our proposed crypto-system by adding the salsa20 method.

Several simulations have been performed to prove the effectiveness of proposed System. The results obtained by the simulations have demonstrated the high security of Crypto-system, therefore our System can effectively secure multiple formats of medical images and is also resistant to various attacks from security such as brute force, man in the middle, etc...

Keywords :Pseudo-random sequence, Randomness, Statistical tests, Chaotic maps, Cryptographic applications, Crypto-system, Confusion, Diffusion, Salsa 20, Medical images.

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

LISTES DES ACRONYMES

DES	*Norme de cryptage des données(Data Encryption Standard).*
AES	*Norme de cryptage des données(Advanced Encryption Standard).*
RC4	*Norme de cryptage des données(ivest Cipher* 4*).*
RSA	*Norme de cryptage des données(Rivest Shamir Adleman).*
DH	*Norme de cryptage des données(diffie − Hellman).*
BMB	*Windows bitmap.*
PCX	*PiCture eXchange.*
GPEG	*signifie Joint Photographic Experts Group.*
TIFF	*Tagged ImageFile Format.*
RGB	*red green blue.*
TDM	*déroulement d'une tomodensitométrie.*
IRM	*L'imagerie par résonance magnétique.*
CT	*Computed Tomography*
SPECT	*single photon emission computed tomography.*
PET	*Positron Emission Tomography.*
SIC	2*la sensibilité aux conditions initiales.*
PWLCM	*Carte chaotique linéaire par morceaux (piecewise linear chaotic map).*
NPCR	*Taux de changement du nombre de pixels (Number of Pixels Change Rate).*
UACI	*Moyenne unifiée du changement d'intensité (Unified Average Changing Intensit*
SSIM	*Standard Schedule Information Manual.*
PSNR	*Peak signal to noise ratio.*
MSE	*Means Square Error.*
NIST	*National Institute of Standards and Technology.*

INTRODUCTION GÉNÉRALE

En raison du développement rapide des technologies de l'information ,les documents multimédias sont devenus les éléments essentiels de divers domaines d'application. en fait ,ce sont des outils de travail essentiels en biomédecine, en imagerie satellitaire et astronomique, en production cinématographique ou encore en informatique industrielle. Bien que les mécanismes de sécurité cryptographique protègent les données multimédias lors de leur transmission, les risques de fraude, de manipulation et de piratage sont des menaces. En fait, ces données peuvent être facilement craquées, modifiées et redistribuées sans Il n n'y a pas de perte de qualité significative. La protection des données multimédias est indispensable si l'on veut garantir la qualité des prestations fournies. Cela à stimulé l'intérêt pour le développement des algorithmes et de techniques plus robustes, Vérifier confidentialité, l'authenticité et l'intégrité des données multimédias échangées.

Le domaine de cryptage d'image spécifiquement imagerie médicale (avec des démonstrations d'hôpitaux offrant des soins aux patients dans des régions éloignées, l'utilisation de la télé-médecine s'est rapidement répandue et s'intègre maintenant dans les opérations courantes des hôpitaux, des services spécialisés, des agences de santé à domicile ainsi que des cabinets de médecins privés) connaît un extraordinaire développement et plusieurs techniques ont vu le jour,mais chacune ne peut pas garantir de ne pas avoir de faiblesses ou qu'elle est insensible aux méthodes d'attaque. C'est pourquoi les chercheurs ne cessent de développer des nouveaux systèmes de cryptographie pour minimiser ces problèmes tel que "les systèmes chaotiques".

La science a été dominée par le déterminisme et la prévisibilité. L'apparition de la théorie du chaos, qui a vu le jour dans les travaux d'Henri Poincaré, a poussé l'horizon des recherches

scientifiques plus loin. Le chaos a fait l'objet de beaucoup d'études approfondies qui ont permis de l'introduire dans divers domaines. N'ayant pas de définition au sens universel, le chaos est décrit comme étant un cas particulier d'un système non linéaire déterministe, caractérisé par son comportement très sensible aux conditions initiales et bien qu'il soit déterministe, il est imprédictible à long terme et présente un aspect aléatoire sans pour autant faire partie des phénomènes aléatoires.

Ces dernières années, de nombreux travaux sur les crypto systèmes basés sur le chaos ont été publié. La plupart des schémas de chiffrement/déchiffrement décrits sont des chiffrements basés sur le concept de "substitution-permutation". Dans un algorithme de chiffrement basé sur le chaos, les opérations de substitution et de permutation sont effectuées conformément avec des séquences chaotiques pour atteindre la diffusion requise et l' effet de confusion.

Organisation du document

Le travail présenté dans ce mémoire se situe dans le cadre des approches qui proposent l'usage du chaos pour sécuriser la transmission des images Médicale . Afin d'aborder ce travail, nous avons divisé ce mémoire en quatre chapitres dont :

Le premier chapitre est consacré à la cryptographie et à l'imagerie nous présentons des notions de cryptographie et des services qu'elle offre puis nous exposons la notion des images numériques et ses différents types et caractéristiques , dans le dernier sujet, nous présentons les concepts liés à l'imagerie médicale, les types d'imagerie existants .

Le second chapitre nous présentons une brève introduction aux systèmes dynamiques, chaos et aux quelques concepts de base tels que la bifurcation , ensuite nous présenterons les métriques utilisées pour évaluer la sécurité et les performances des schémas de cryptage des images enfin l'étude de différents algorithmes à base de récurrences chaotiques pour le chiffrement d'images médicales.

Le troisième chapitre introduire une nouvelle Génération d'une séquence pseudo-aléatoires , puis on discutons de l'uniformité , sensibilité aux valeurs initiales et du caractère aléatoire de séquence proposée.

Le dernier présente en détaille notre Crypto-système proposé pour le cryptage des images médicales basé la Séquence proposée ,sachant que les résultats expérimentaux et les analyses de sécurité de l'algorithme cryptographique proposé sont aussi rapportés et abordées dans le chapitre4.

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

CHAPITRE 1

GÉNÉRALITÉS SUR LA CRYPTOGRAPHIE ET L'IMAGERIE MÉDICALE

1.1 introduction

Dans le Domaine des télécommunications, les données, y compris les images médicales sont exposées à plusieurs menaces qui peuvent causer des dommages sous formes de destruction et modification défavorable, il est nécessaire de pouvoir disposer des systèmes sécurisés pour protéger les informations à caractère personnel ou confidentiel.
Les techniques cryptographiques apportent plusieurs fonctionnalités (chiffrement, intégrité et authentification) permettant de palier plusieurs types de menaces.

Dans ce chapitre nous commence par expliquer Les concepts fondamentaux de la cryptographie, ainsi que ses type... Ensuite, on va expliquer l'image numérique en général et l'image médicale en particulier ainsi que ses diffèrent technique.

1.2 Principes généraux de la cryptographie

La cryptographie compte parmi les différents systèmes d'écriture permettant de modifier de façon volontaire les caractères d'un message. Donc, ce procédé protège une communication qui devient lisible uniquement par l'expéditeur et par le destinataire auquel le message est adresse.

1.2.1 Terminologie de cryptographie

Cryptologie : Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse. [1]

Cryptologie = la cryptographie + cryptanalyse.

Cryptographie : La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné. [1]

Cryptanalyse : Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés. [1]

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. [1]

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 . [1]

1.2.2 Fonction de la cryptographie

Un algorithme de chiffrement est une fonction mathématique utilisée lors du processus cryptage et de décryptage.
Cet algorithme est associé à une clé (un mot, un nombre ou une phrase), afin de crypté le texte en clair ,avec des clés différentes, le résultat du cryptage variera également [1],comme il est illustré dans la Figure 1.1.

1. **Chiffrement :** Transformation d'un message pour en cacher le sens.

   - L'émetteur doit transmettre un message M (en clair) M ∈ Messages à envoyer.

   -Il construit un texte chiffré C au moyen d'une fonction E qui dépend clé k . [2]

$$C = Ek\,(M)$$

2. **Déchiffrement :** Opération inverse du chiffrement Récupération d'un message en clair La fonction de déchiffrement Dk'(C).

$$\mathrm{M} = \mathrm{Dk'(C)}$$

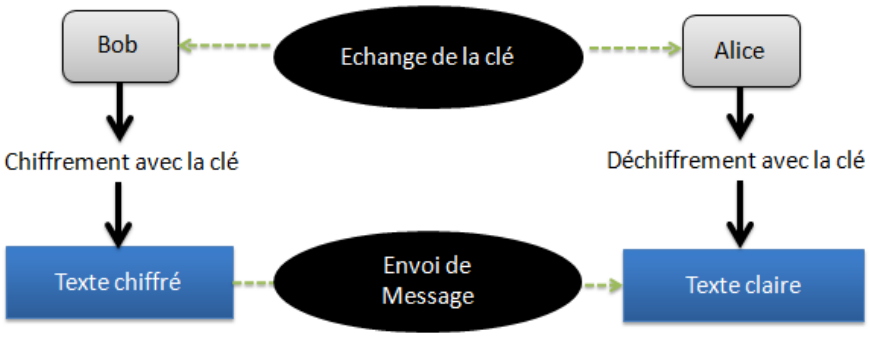


FIGURE 1.1 – Fonction de la cryptographie . [1]

1.2.3 Objectif de cryptographie

Les principaux objectifs à garantir par l'application de la cryptographie sont [4] :

Confidentialité : un mécanisme pour transmettre des données de telle sorte que seul le destinataire autorisé puisse les lire.

Intégrité des données : un mécanisme pour s'assurer que les données reçues n'ont pas été modifiées durant la transmission, frauduleusement ou accidentellement.

Authentification :un mécanisme pour permettre d'authentifier les utilisateurs de façon à limiter l'accès aux données, serveurs et ressources aux seules personnes autorisées (un mot de passe par un nom de login ou un certificat numérique).

Non-répudiation : un mécanisme pour enregistrer un acte ou un engagement d'une personne ou d'une entité de telle sorte que celle-ci ne puisse pas nier avoir accompli cet acte ou pris cet engagement. Ce mécanisme se décompose :

- non-répudiation d'origine l'émetteur ne peut nier avoir écrit le message.
- non-répudiation de réception le receveur ne peut nier avoir reçu le message.
- non-répudiation de transmission l'émetteur du message ne peut nier avoir envoyé le message.

1.2.4 Différents types de cryptographie

Nous avons regrouper les systèmes de chiffrement en deux catégories :
La crypto graphique classique et moderne. Figure 1.2 illustre différente type de crypto graphique.

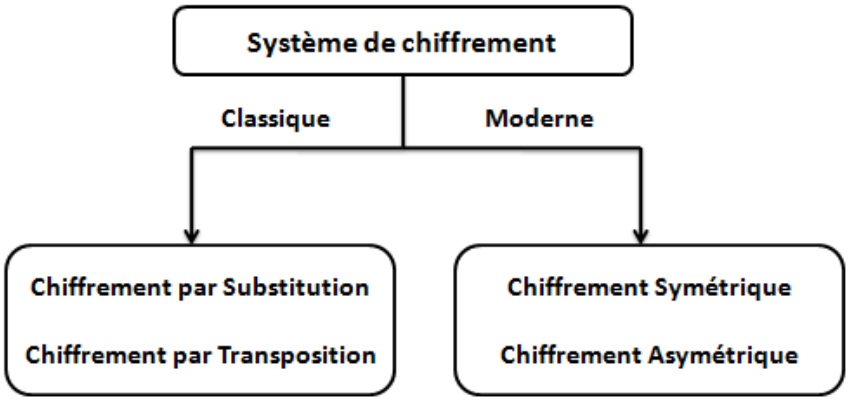


FIGURE 1.2 – principe de systèmes de chiffrement [6]

1.2.4.1 Cryptographie classique :

Dans la cryptographie classique, la méthode et la clé de chiffrement ainsi que celle de déchiffrement sont connues par l'émetteur et le destinataire.
La plupart des méthodes déchiffrement classique reposent sur deux principes essentiels : la substitution et la transposition.

1.2.4.1.1 Chiffrement par substitution : Le chiffrement par substitution consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou plusieurs autres entités. [7]
On distingue généralement plusieurs types de crypto systèmes par substitution :

1.2.4.1.2 Substitution mono-alphabétique : consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet. L'algorithme de substitution mono-alphabétique le plus connu est Le chiffre de César.La Figure 1.3 illustre Le chiffre de César [7].

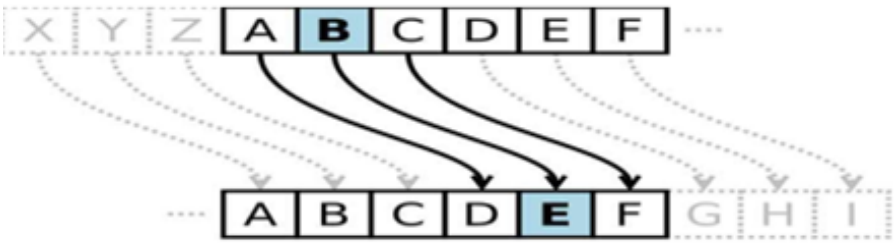


FIGURE 1.3 – principe de systèmes de chiffrement . [5]

1.2.4.1.3 substitution poly alphabétique : Elle consiste à utiliser plusieurs alphabets décalés pour crypter un message. L'algorithme de substitution poly alphabétique le plus connu est le chiffre de Vigenèr .La figure 1.4 illustre Le chiffre de Vigenèr [1]

Lettre claire	L	E	A	I	R	E	S	S	O	N	T
Clef	E	T	P	E	T	P	E	T	P	E	T
Décalage	5	20	16	5	20	16	5	20	16	5	20
Lettre chiffrée	X	P	M	K	T	W	L	D	R	M	R

FIGURE 1.4 – le principe de chiffrement de chiffre de Vigenèr [5]

1.2.4.1.4 Chiffrement par transposition : Le chiffrement par transposition (ou le chiffrement par permutation) consiste à faire un réarrangement de l'ordre des lettres qui cache le sens initial. Cette méthode demande de dé couper le texte clair en blocs de taille identique, et applique la même permutation sur chacun des bloc. [5]

1.2.4.2 cryptographie moderne

La cryptographie moderne se compose de deux grandes familles selon le principe de fonctionnement :

- Méthode à clé secrète : la cryptographie symétrique.
- Méthode à clé public : la cryptographie asymétrique

1.2.4.2.1 Cryptographie symétrique(à clefs privés) : le chiffrement symétrique (aussi appelé chiffrement à clé privée ou à clé secrète) consiste à utiliser la même clé pour le chiffrement et le déchiffrement. c'est-à-dire que l'émetteur et le récepteur doivent avoir la même clef

— Le chiffrement :consiste alors à effectuer une opération entre la clé privée et les données à chiffrer afin de rendre ces dernières inintelligibles.

— Le déchiffrement :consiste à réaliser l'opération inverse c'est-à-dire récupérer le message d'origine à partir du message chiffré en utilisant la clé secrète [7].

Les techniques symétriques peuvent être divisées en deux catégories : le chiffrement par bloc et le chiffrement par flux.

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 chiffre.
   Les méthodes les plus connues dans cette famille sont : DES et AES [9]
2. **Chiffrement par flot :** flot Dans un crypto-système par flots, le cryptage des message fait caractère par caractère ou bit à bit, au moyen de substitutions de type César aléatoirement : la taille de la clef est donc égale à la taille du message.
   Par exemple RC4 est un : chiffrement octet par octet.

1.2.4.2.2 Cryptographie asymétrique (à clefs publiques) : Dans la cryptographie à clé asymétrique, différentes clés sont utilisées pour le chiffrement et le déchiffrement .
La clé publique est annoncée au public , tandis que le la clé privée est conservée par le destinataire
. L'expéditeur utilise la clé publique du destinataire pour le cryptage et le destinataire utilise sa clé privée pour le déchiffrement.
Ici, le nombre de clés nécessaires est faible mais il n'est pas efficace pour les longs messages .
Dans chiffrement à clé asymétrique l'algorithme RSA et l'algorithme Diffie-Hellman différents facteurs sont analysés. [10]

1.3 Notions de base sur l'imagerie

Le traitement d'images représente l'ensemble des techniques permettant de modifier une image numérique afin de l'améliorer ou d'extraire les informations qu'elle contient.

1.3.1 Définition d'image

On peut définir une image comme un tableau bidimensionnel dont chaque élément (pixel) représente une surface élémentaire de l'image. La disposition de ces pixels est généralement en ligne et colonne [12].

L'image est définie Mathématiquement 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 [13].

Lorsque les points (x,y) et l'amplitude sont discrétisés, on parle d'image numérique ou digitale. Dans ce dernier cas la fonction f est remplacée par la lettre I et le couple (x,y) par le couple (i,j), la Figure 1.5 représente les différents caractéristiques d'une image.

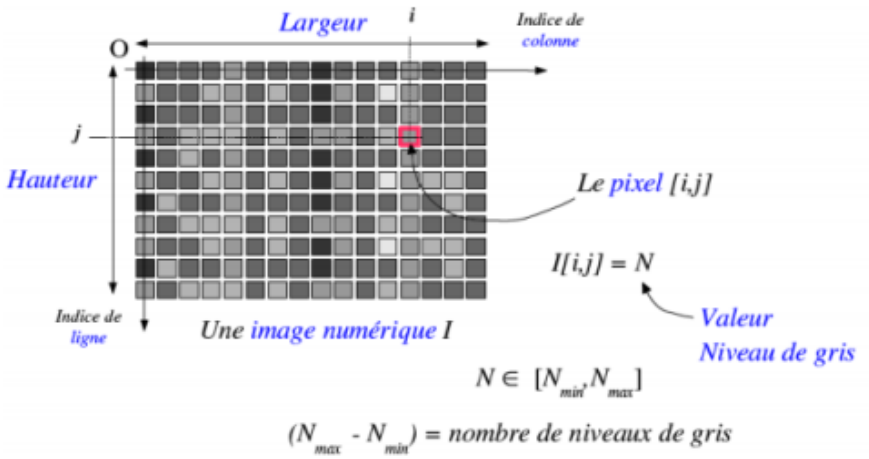


FIGURE 1.5 – représentation des notion d'image e pixel [12] .

1.3.2 Les formats d'images

1. **Image matricielle (bitmap) :** Elle est composée de petits points appelés « pixels » que l'on ne voit pas à l'œil nu. Lors de l'agrandissement d'une image matricielle, cette dernière devient floue car les pixels ressortent, ce sont les carrés qui apparaissent sur l'écran [14]. Les formats d'images bitmap : BMP, PCX, GIF, JPEG, TIFF. Les photos numériques et les images scannées sont de ce type [15].

2. **Image vectorielle :** Les images vectorielles sont composées de formes géométriques qui vont pouvoir être décrites d'un point de vue mathématique. Par exemple une droite sera définie par 2 points, un cercle par un centre et un rayon. [13]

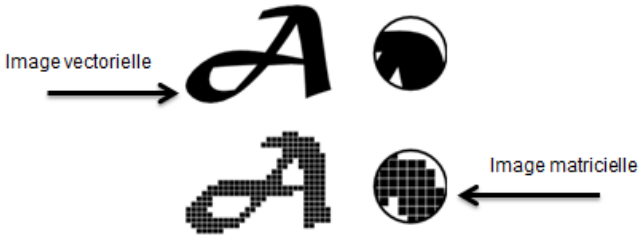


FIGURE 1.6 – Différence entre image vectorielle et image matricielle [14]

1.3.3 représentation des couleur

Il existe plusieurs modes de codage informatique des couleurs, les plus utilisés sont :

Image binaire : Une image en noir et blanc, un pixel sera représenté par 1 bit, on aura deux valeur possible (0 = noir, 1 = blanc),comme il est illustré dans la Figure 1.7 [17]

FIGURE 1.7 – Exemple d'une image binaire [16]

Image niveau de gris : Une image en niveaux de gris est codée avec 8 bits = 1 octet=2^8= 256 valeurs de dégradations de couleur du noir au blanc . [12]

Image couleur : Dans une image en couleurs, codée dans l'espace RGB (256 teintes de rouge, 256 teintes de vert, 256 teintes de bleu), chaque pixel est représenté par 3 octets =3 x 8 bits permettant de représenter $(2^8)^3 = 16,8$ millions de Couleurs.

1.3.4 Les caractéristiques d'une image

L'image est un ensemble structuré d'information caractérisé par les paramètres suivants :

Pixel : image numérique est constituée d'un ensemble de points appelés pixels (Pix abbreviation of pictures + element) pour former une image. Par conséquent, un pixel représente le plus petit élément constitutif Image digitale.
Tous ces pixels sont contenus dans un tableau à deux dimensions constituant une image. [16]
La figure 1.8 ci-dessous montre la distribution des pixels.

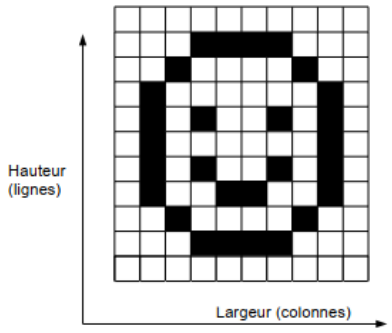


FIGURE 1.8 – Distribution des pixels par lignes et colonnes [16]

Dimension : le nombre de points (ou pixels) que comporte une image numérique en largeur et en hauteur. On l'exprime en donnant le nombre de pixels en hauteur et en largeur (exemple : 1600×1200). [17]

Résolution : La résolution d'une image est le nombre de pixels contenus dans l'image par unité de longueur, elle s'exprime le plus souvent en PPP (Point Par Pouce) ou en DPI (Dot Per Inch), parfois en point 3 par cm, La résolution définit la qualité d'une image, plus la résolution est grande plus l'image est précise dans les détails. La résolution d'une image est montre dans la figure 1.9 [12]

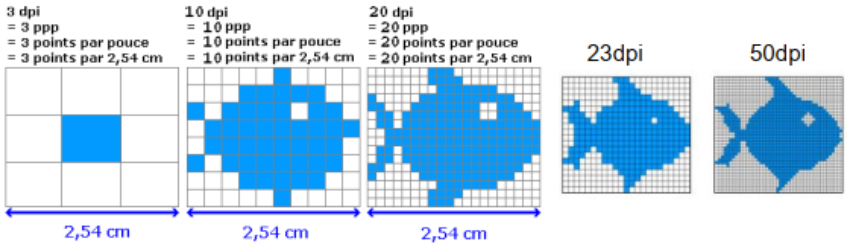


FIGURE 1.9 – Explication de résolution d'une image [16]

Bruit : Le bruit est un phénomène parasite aléatoire (suivant une distribution de probabilité connue ou non), il correspond à des perturbations soit du dispositif d'acquisition, soit de la scène observée elle-même. [1] Les sources de bruit d'une image sont nombreuses et diverses :

— Bruits liés aux conditions de prise de vue (bougé, éclairage de la scène)

— Bruits liés à l'échantillonnage.

— Bruits liés à la nature de la scène (poussières, rayures)

Voisinage : Le plan de l'image est divisé en termes de formes rectangulaires ou hexagonales permettant ainsi l'exploitation de la notion de voisinage . Le voisinage d'un pixel est formé par l'ensemble des pixels qui se situent autour de ce même pixel. On définit aussi l'assiette comme étant l'ensemble de pixels définissant le voisinage pris en compte autour d'un pixel [13] . On distingue deux types de voisinage :
Voisinage à 4 : On ne prend en considération que les pixels qui ont un coté commun avec le pixel considéré.
Voisinage à 8 : On prend en compte tous les pixels qui ont au moins un point en liaison avec le pixel considéré.

Contraste : C'est l'opposition marquée entre deux régions d'une image. Une image contrastée présente une bonne dynamique de la distribution des valeurs de gris sur tout l'intervalle des valeurs possibles, avec des blancs bien clairs et des noirs profonds. Au contraire une image peu contrastée a une faible dynamique, la plupart des pixels ayant des valeurs de gris très prochesi [17].
Si L1 et L2 sont les degrés de luminosité respectivement de deux zones voisines A1 et A2 d'une image, le contraste est défini par le rapport :

$$\frac{l_1 - l_2}{l_1 + l_2} \tag{1.1}$$

Luminance : C'est le degré de luminosité des points de l'image. Elle est définie aussi comme étant le quotient de l'intensité lumineuse d'une surface par l'aire apparente de cette surface, pour un observateur lointain, le mot luminance est substitué au mot brillance, qui correspond à l'éclat d'un objet. Une bonne luminance se caractérise par [17] : Des images lumineuses (brillantes).
Un bon contraste : il faut éviter les images où la gamme de contraste tend vers le blanc ou le noir, ces images entraînent des pertes de détails dans les zones sombres ou lumineuses.
L'absence de parasites.

Contour : Une limite entre deux (ou un groupe de) pixels dont la différence de niveau de gris (couleur) est significative. Un contour correspond à une variation d'intensité ou à une discontinuité entre les propriétés de deux ensembles de points.

1.4 Imagerie médicale

L'imagerie médicale fait référence à plusieurs technologies différentes qui sont utilisées pour visualiser le corps humain afin de diagnostiquer, surveiller ou traiter des conditions médicales . Toutes les modalités d'imagerie ont en commun que la condition médicale devient visible par une certaine forme de contraste, ce qui signifie que la caractéristique d'intérêt (telle qu'une tumeur) peut être reconnue dans l'image et examinée par un radiologue qualifié. [18]

1.4.1 Imagerie analogique et imagerie numérique

Il existe deux façon de représenter les information [19] :

1.4.2 L'imagerie analogique

la façon analogique qui La façon analogique qui représente l'information comme une quantité physique continue ,il faut savoir que les phénomènes qui nous entourent sont quasiment tous continuent et l'lorsqu'un support peut prendre des valeurs continuent comme par exemple une cassette vidéo audio.

1.4.3 L'imagerie numérique : numérisation

On peut numériser les images (digitalisation en anglais), c'est à dire transformer l'information initiale en une matrice de nombre. On peut donc passer d'une image analogique à une image numérique par la numérisation.
Dans la numérisation, il y a deux étapes :

1. **Un codage spatial (échantillonnage spatial) :** L'image va d'abord être divisée en pixels (Picture elements) qui sont des petites surfaces élémentaires de l'image. Lorsque l'on est en présence d'une image de coté N et M, on aura une image divisée en NxM pixels.
2. **Un codage en intensité (quantification) :** Dans chaque pixel on va pouvoir mettre un nombre qui correspond a la valeur moyenne de l'intensité en ce point

On se retrouve alors avec une matrice de nombre qui comprend la totalité des renseignements nécessaires. On enregistre donc ces nombres à l'aide d'ordinateurs (Ainsi l'imagerie médicale c'est beaucoup développée parallèlement au développement des ordinateurs), on est alors capable de retranscrire cette matrice de nombre en une image visuelle. Pour ce faire, on associe chaque nombre enregistré à un niveau de gris.

On a donc une intensité qui varie par palier, les images numériques contiennent donc une information discrète et non continue.

1.4.4 Différents type d'imagerie médical

Un service d'imagerie de nos jours est constitué d'une multitude de modalités que nous citerons ci-dessous .

Tomodensitométrie (TDM) : Cette procédure d'imagerie utilise est une modalité d'imagerie volumétrique basée sur l'absorption des rayons X.
la TDM permet la reconstruction d'une carte d'absorbeur en deux ou trois dimensions.
La tomodensitométrie dépasse largement l'imagerie par rayons X par projection dans le contraste des tissus mous, mais la résolution spatiale d'un tomodensitogramme (scanner) clinique du corps entier est nettement inférieure à celle de l'imagerie par rayons X simple. Néanmoins, la tomodensitométrie peut révéler de petites tumeurs, des détails structures dans l'os trabéculaire ou le tissu alvéolaire des poumons. [18]

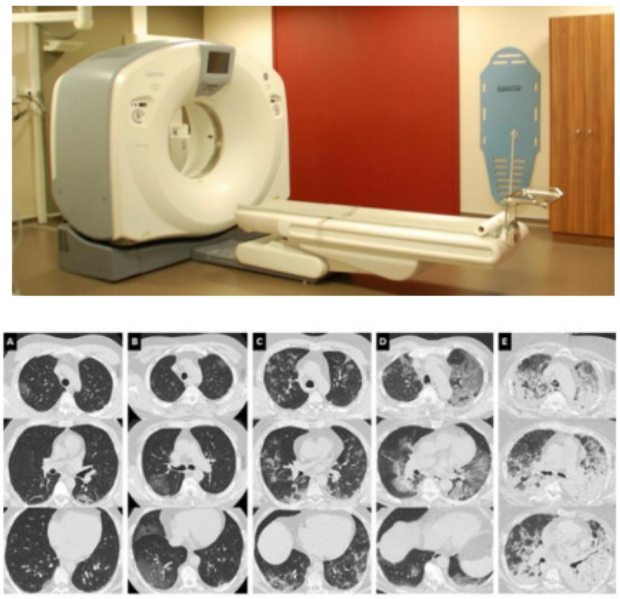


FIGURE 1.10 – Schéma d'un scanner (en haut) et un échantillon d'images (en bas). [23]

Radiographie : est la plus ancienne modalité d'imagerie médicale, qui a trouvé sa place dans la pratique médicale peu de temps après la découverte des rayons X en 1895. Les rayons X sont des photons de haute énergie, et l'interaction atomique avec les électrons de la couche interne est fondamentale à la fois pour la production de rayons X et la génération de contraste de rayons X.

Le contraste des tissus mous est relativement faible, mais l'os et l'air offrent un excellent contraste. Les images aux rayons X peuvent révéler des caractéristiques très subtiles, mais ont des effets très nocifs sur la santé pour des durées d'exposition longues ou répétées et/ou pour de fortes intensités.

L'imagerie par rayons X est utilisée pour diagnostiquer les fractures osseuses, les maladies pulmonaires, Etc. [21]

FIGURE 1.11 – Schéma d'un système de radiographie (à gauche) [22]et un échantillon d'images radio-graphiques (à droite). [23]

L'imagerie par résonance magnétique (IRM) : Est une modalité d'imagerie volumétrique parallèle, dans une certaine mesure, à la tomodensitométrie. Cependant, les principes physiques sous-jacents sont fondamentalement différents de la TDM. La où la tomodensitométrie utilise des photons de haute énergie et l'interaction des photons avec les électrons de la couche atomique pour la génération de contraste, l'IRM est basée sur l'orientation des protons à l'intérieur d'un champ magnétique puissant. Cette orientation peut être manipulée avec des ondes radio fréquences résonantes, et le retour des protons à leur état d'équilibre peut être mesuré. Les constantes de temps de relaxation dépendent fortement des tissus et l'IRM présente un contraste supérieur des tissus mous, dépassant de loin celui du TDM. [18]

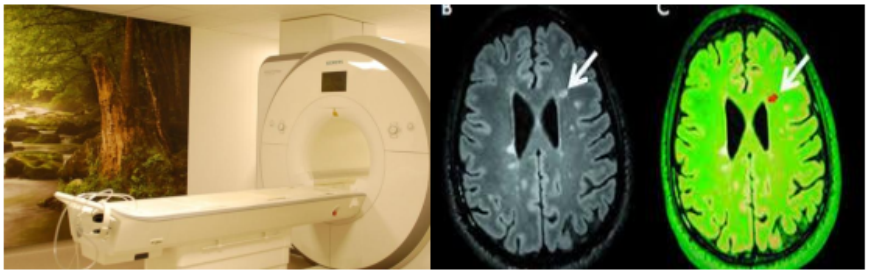


FIGURE 1.12 – Schéma d'un système d'IRM [23] (à gauche) et un échantillon d'image (à droite) indiquant les formes progressives de sclérose en plaques (SEP) . [25]

Imagerie par ultrasons : L'imagerie par ultrasons utilise les propriétés des ondes sonores dans les tissus.

Les ondes de pression dans la gamme des mégahertz inférieurs traversent les tissus à la vitesse du son, étant réfractées et partiellement réfléchies aux interfaces. Le contraste échographique est donc lié à des inhomogénéités échogènes dans les tissus.

Les images échographiques montrent un bon contraste des tissus mous, mais échouent en présence d'os et d'air. Bien que les images ultrasonores puissent être générées avec des circuits purement analogiques, les appareils à ultrasons modernes utilisent un traitement d'image informatisé pour la formation, l'amélioration et la visualisation des images. L'imagerie par ultrasons est très populaire en raison de son instrumentation peu coûteuse et de sa facilité d'application. Cependant, un examen échographique nécessite la présence d'un opérateur expérimenté pour ajuster divers paramètres pour un contraste optimal, et les images écho-graphiques nécessitent généralement un radiologue expérimenté pour interpréter l'image. [18]

Nuclear Imaging : L'imagerie nucléaire est liée à l'imagerie par rayons X et CT en ce sens qu'elle utilise des rayonnements. Cependant, contrairement aux modalités d'imagerie basées sur les rayons X, les composés radioactifs sont incorporés dans le corps en tant que sources de rayonnement. Ces composés radioactifs sont généralement liés à des substances pharmacologiquement actives (« radiopharmaceutiques ») qui s'accumulent à des sites spécifiques du corps, par exemple dans une tumeur.

Avec des techniques de projection ou une reconstruction d'image informatisée volumétrique, la distribution spatiale du produit radiopharmaceutique peut être déterminée. De cette façon, les processus métaboliques peuvent être imagés et utilisés pour un diagnostic. Les reconstructions tridimensionnelles sont obtenues d'une manière similaire à la tomodensitométrie, conduisant à une modalité appelée tomographie par émission monophotonique (SPECT). Une technologie

parallèle, la tomographie par émission de positons (TEP), utilise des émetteurs de positons qui provoquent des paires coïncidentes de photons gamma à émettre. Sa sensibilité de détection et son rapport signal sur bruit sont meilleurs que le SPECT. Le SPECT et le PET ont tous deux une résolution nettement inférieure à celle du CT avec des tailles de voxel pas beaucoup plus petites que 1 cm. Souvent, les images SPECT ou PET sont superposées aux images CT ou MR pour fournir une référence spatiale. Une limitation facteur de l'utilisation généralisée des modalités d'imagerie nucléaire est le coût. De plus, les marqueurs radioactifs ont une durée de vie très courte avec des demi-vies de quelques heures seulement, et la plupart des radiopharmaceutiques doivent être produits sur place. Cela nécessite que les centres d'imagerie nucléaire disposent d'une certaine forme de réacteur pour la génération d'isotopes. [18]

1.4.5 Spécificité des images médicales

Des pixels aux voxel : Par rapport à l'image numérique bidimensionnelle dont le processus d'échantillonnage est basé sur les composants de base, les « pixels d'échantillonnage de volume » ajoutent une troisième dimension de « voxels ». Les mécanismes d'imagerie médicale sont reconstitués en termes de $[1 \dots X] \times [1 \dots Y] \times [1 \dots Z]$ Une image volumétrique modélisée comme une fonction discrète, où chaque emplacement est associé à des informations. [26]

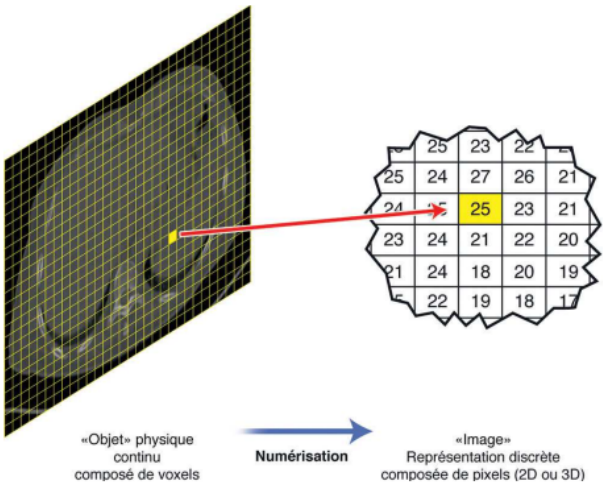


FIGURE 1.13 – Numérisation d'un objet en image médical [26].

Taille des images : La taille d'une image médicale dépend du capteur responsable de l'acquisition de la région anatomique à imager. Généralement en tomodensitométrie (technique d'analyse par coupe), les images font du $512 \times 512 \times 12$ bits. En IRM, les formats d'images

varient plus que n'importe quelle autre modalité avec des formats matriciels carrés et non carrés (par exemple 64 x 64, 64 x 128, 128 x 128, 128 x 192, 256 x 512, 512 x 512, 512 x 1024, ...).

Résolution spatiale et temporelle : Chaque modalité a différentes capacités pour résoudre les détails fins dans le corps d'un patient. Généralement deux définitions sont données à la résolution spatiale.

— Dans [27] : la résolution réfère a la capacité de voir de petits détails.

— Dans [28] : elle représente la capacité d'un système d'imagerie à représenter distinctement deux objets de plus en plus petits et rapprochés.
D'après ces définitions, un système d'imagerie a une plus grande résolutions spatiale s'il peut démontrer la présence d'objets de plus en plus petits dans l'image. Suivant chaque modalité, un ou plusieurs facteurs peuvent causer une limitation de la résolutions spatiale.

Bruit : Dans le domaine du traitement du signal et de l'image, le bruit correspond à un phénomène aléatoire qui se surajoute à l'image idéale.
Probablement la meilleure approche pour comprendre le bruit est de réaliser que si l'on acquiert plusieurs fois l'image d'un même objet, immobile et inchangé , on n'observera pas exactement le même résultat : la différence est liée au bruit. De la même manière, en lançant plusieurs fois un dé, on n'obtient pas le même résultat, c'est aléatoire. [26]

Contraste : Le contraste dans une image représente la différence entre les niveaux de gris de l'image. Une image uniformément grise n'a pas de contraste, alors qu'une image avec des transitions vives entre un gris obscure et un gris clair démontre un contraste élevé [29].

1.5 conclusion

Ce chapitre a été consacré d'une part aux concepts de la cryptographie qui permettent d'assurer la confidentialité des données, qu'elles soient stockées localement sur une machine ou transmises sur un réseau non sécurisé. Nous avons présenté les différentes méthodes de la cryptographie, ceci nous a permis de constater que la sécurité offerte par les algorithmes de chiffrement traditionnel risquait d'être réduite considérablement avec l'augmentation de la puissance des ordinateurs. Ensuite, nous avons parlé de l'importance des images numériques et de ses types,les méthodes de codage des pixels des images numériques, les formats connus les plus célèbres et leurs caractéristiques, avec un accent sur les images médicales pour la sensibilité des informations contenues.

CHAPITRE 2

CRYPTOGRAPHIE À BASE DES SYSTÈMES CHAOTIQUES

2.1 introduction

La technologie multimédia, en particulier la technologie de l'image, connaît actuellement une évolution et une croissance rapides en raison de l'adoption accrue des communications Internet [30]. Les techniques de cryptage actuelles, telles que AES, DES et RSA, ne conviennent pas au cryptage des données d'image et ne peuvent pas garantir la confidentialité et la sécurité des données [31]raison de la taille et de la redondance des images [32] [33].

Au cours des deux dernières décennies, de nombreuses techniques ont été proposées pour crypter les données d'image, dont le cryptage basé sur le Chaos s'est avéré être le plus efficace [34]. La théorie du chaos a été proposée pour la première fois dans les années 1970 pour être utilisée en physique, en mathématiques, en biologie et en ingénierie. Ce n'est que dans les années 1980 que la théorie du chaos s'est avérée avoir des applications cryptographiques . Les méthodes de chiffrement basées sur le chaos sont populaires en raison de leur caractère aléatoire, leur imprévisibilité, leur sensibilité et leur transitivité topologique.

2.2 définition

le terme “chaos” définit un état particulier d’un système dont le comportement ne se répète jamais, est très sensible aux conditions initiales, est imprédictible à longterme.

Les systèmes chaotiques sont des systèmes dont les trajectoires évoluent dans une région bornée présentant un caractère stable mais sans toute fois converger vers un point fixe ou un cycle limite.Les solutions des équations différentielles non linéaires ne peuvent pas être calculées avec exactitude analytiquement car il n’existe pas de méthode de résolution analytique pour ces équations, sauf pour certaines classes particulières.
Elles sont alors déterminées numériquement et le comportement du système est analysé par simulation [35].

2.3 Système dynamique

C’est une structure qui change au cours du temps. Mathématiquement, un système dynamique est défini à partir d’un ensemble de variables qui forment le vecteur d’état Xn où n représente la dimension du vecteur, et qui caractérisent l’état instantané du système dynamique. L’ensemble de tous les états possibles est appelé espace d’état ou espace de phase. En plus de l’espace d’état, un système dynamique est défini par une loi d’évolution, généralement désignée par dynamique, qui caractérise l’évolution de l’état du système au cours du temps.
Les systèmes dynamiques sont classés en deux catégories [36] :

2.3.1 Discrets

Un système dynamique discret est représenté comme suit :

- La condition initiale est : x_0
- Le premier état est :$x_1 = f(x_0)$
- Le deuxième état, qui suit immédiatement le premier, est : $x_2 = f(x_1) = f(f(x_0)) = f^2(x_0)$
- Le nième état est donné par : $x_n = f(x_{n-1}) = ... = f^n(x_0)$

2.3.2 Continus

Un système dynamique continu est décrit par un système d'équations différentielles de la forme :

$$\frac{\mathrm{d}x(t)}{\mathrm{d}t} = f(x(t), t) \tag{2.1}$$

2.4 Différence entre le chaos et l'aléatoire

La différence entre le chaos et l'aléatoire nous a paru le point le plus important de la compréhension du chaos. En effet, on a toujours tendance à considérer qu'un phénomène tire son imprédictibilité du nombre trop important de paramètres en jeu dans sa description. Ce qui nous pousse à en donner une approche probabiliste qui peut être parfaitement satisfaisante, garde par définition une certaine marge d'aléatoire.
En ce qui concerne le chaos, il n'en est rien, les systèmes chaotiques se comportent, en effet, d'une manière qui peut sembler aléatoire. Mais ce comportement est en fait décrit de manière déterministe par des équations non linéaires parfaitement déterministes, c'est-à-dire en particulier avec des outils mathématiques qui permettant une approche précise et certaine. [34]

2.5 Système chaotique

Le chaos tel que le scientifique le comprend ne signifie pas l'absence d'ordre [37] ; il se rattache plutôt à une notion d'imprévisibilité, d'impossibilité de prévoir une évolution à long terme du fait que l'état final dépend de manière si sensible de l'état initial .

2.6 Propriété de système chaotique

Il existe plusieurs définitions possibles du chaos, Ces définitions ne sont pas toutes équivalentes, mais elles convergent vers certains points communs caractérisant ainsi le chaos.
Ci-dessous, nous présentons quelques caractéristiques qui permettent de comprendre qualitativement les points marquants d'un système chaotique [39] .

2.6.1 Non-linéarité

Un système chaotique est un système dynamique non linéaire. Un système linéaire ne peut pas être chaotique [40], le dernier est défini sous la forme :

$$y = ax + b \tag{2.2}$$

Le comportement chaotique d'un système dynamique non linéaire ,est défini sous la forme [41] :

$$y = mx \tag{2.3}$$

Soit y une fonction non linéaire de x, si x multiplié par une autre variable, ou multiplié par lui-même.
En général, pour prévoir des phénomènes générés par les systèmes dynamiques, la démarche consiste à construire un modèle mathématique qui établit une relation entre un ensemble de causes et un ensemble d'effets. Si cette relation est une opération de proportionnalité, le phénomène est linéaire. Dans le cas d'un phénomène non linéaire, l'effet n'est pas proportionnel à la cause. [40]

2.6.2 Déterminisme

La Déterminisme veut dire qu'à partir d'un événement d'un phénomène (passé où présent) on peut prédire le futur de ce phénomène. Un système chaotique généralement régi par des équations différentielles non linéaires qui décrivent son comportement dynamique, et qui nous permet de prédire son évolution au cours du temps. [42]

2.6.3 Sensibilité aux conditions initiales (S.C.I)

Est une propriété observée par le père de l'effet papillon Edward Lorenz [13] lors de ses travaux en météorologie est connu sous le nom d'effet papillon, « un battement d'ailes de papillon à un endroit du monde peut provoquer une tempête à un autre endroit ».

Donc on peut dire qu'une infime modification des conditions initiales peut entrainer des résultats imprévisibles sur le long terme, ça veut dire que l'existence d'une moindre erreur sur la condition initiale conduit à une divergence rapide des trajectoires au cours du temps. Ceci est illustré par la Figure 2.1 [43]

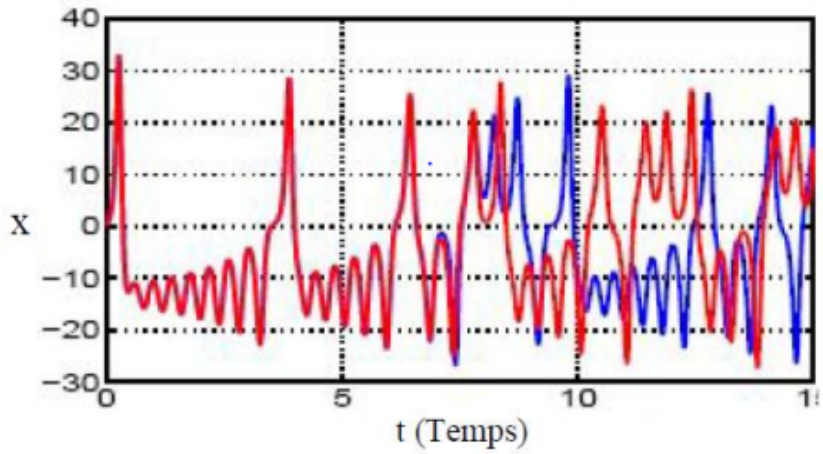


FIGURE 2.1 – Évolution dans le temps pour deux conditions initiales très proches [43]

2.6.4 Espace de phase

Un système dynamique est caractérisé par un certain nombre de variables d'états, qui ont la propriété de définir l'état du système à un instant donné. Le comportement dynamique du système est ainsi relié à l'évolution de chacune de ces variables d'état. Cet espace est appelé l'espace de phase ou chaque point définit un état et le point associé à cet état décrit une trajectoire appelé également une or bit . [12]

2.6.5 Attracteurs

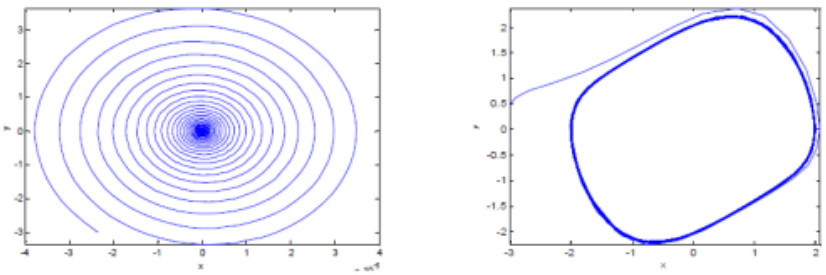
Un attracteur est un objet géométrique vers lequel tendent toutes les trajectoires des points de l'espace des phases, c'est à dire une situation ou un ensemble de situations vers lesquelles évoluent un système, quelles que soient ses conditions initiales. Le bassin d'attraction d'un attracteur est l'ensemble des points de l'espace des phases qui donnent une trajectoire évoluant vers l'attracteur considéré. On peut donc avoir plusieurs attracteurs dans un même espace des phases. Il existe deux types d'attracteurs : les attracteurs réguliers et les attracteurs étranges ou chaotiques. [45].

2.6.5.1 Attracteurs réguliers

un point fixe : est un point de l'espace de phase vers lequel tendent les trajectoires, c'est donc une solution stationnaire constante.

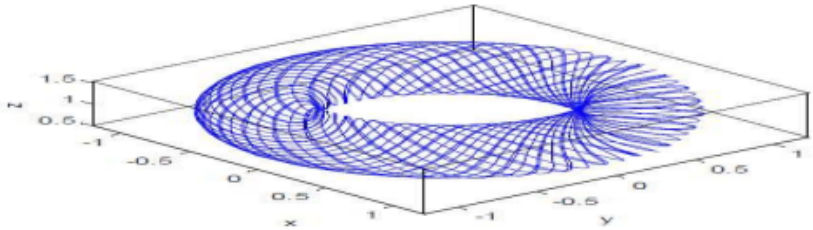
un cycle limite : L'attracteur "cycle limite" est une trajectoire fermée dans l'espace des phases vers laquelle tendent les trajectoires. C'est donc une solution périodique du système.

L'attracteur "tore" : :représente les mouvements résultant de deux ou plusieurs oscillations indépendantes que l'on appelle parfois "mouvements quasi périodiques". [45]



(a)point fixe (b) cycle limite

FIGURE 2.2 – Attracteurs réguliers [45]



c) Tore

FIGURE 2.3 – Attracteurs réguliers [45]

2.6.5.2 Attracteurs étranges

Les attracteurs étranges sont caractéristiques de l'évolution des systèmes chaotiques : au bout d'un certain temps, tous les points de l'espace des phases (et appartenant au bassin d'attraction de l'attracteur) donnent des trajectoires qui tendent à former l'attracteur étrange

grande échelle, un attracteur étrange n'est pas une surface lisse, mais une surface repliée plusieurs fois sur elle-même. En effet, les trajectoires des points divergent (puisque, par définition deux point ne peuvent avoir la même évolution), mais comme l'attracteur a des dimensions finies, l'attracteur doit se replier sur lui même. Le processus d'étirement-repliement se répète à l'infini et fait apparaître un nombre infini de "plis" imbriqués les uns dans les autres qui ne se recoupent jamais.

Ainsi, deux points très proches au départ (conditions initiales) peuvent se retrouver à deux extrémités opposées de l'attracteur (conditions finales). Cela traduit le comportement divergent des phénomènes chaotiques.

On obtient ainsi des attracteurs différents (en fonction des systèmes étudiés), qui présentent des formes diverses et surprenantes. [45]

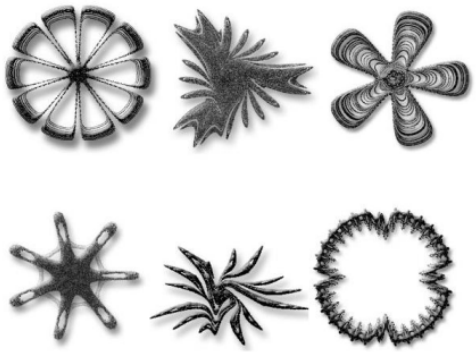


FIGURE 2.4 – Les attracteurs étranges [45]

2.7 Bifurcation et L'évolution vers le chaos

2.7.1 Bifurcation

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique [46]. Une bifurcation survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif des propriétés d'un système telles que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents. Les valeurs des paramètres au moment du changement sont appelées valeurs de bifurcation.

2.7.2 L'évolution vers le chaos

Il existe plusieurs types d'évolution possibles d'un système dynamique régulier vers le chaos [31]. Nous allons en exposer brièvement deux. Ces évolutions surviennent par augmentation des contraintes appliquées au système (par exemple, les vitesses angulaires dans le cadre des pendules).

Par intermittences : le système conserve pendant un certain laps de temps un régime périodique ou pratiquement périodique, c'est à dire une certaine "régularité", et il se déstabilise, brutalement, pour donner lieu à une sorte d'explosion chaotique. Il se stabilise de nouveau ensuite, pour donner lieu à une nouvelle "bouffée" plus tard. On a constaté que la fréquence et la durée des phases chaotiques avaient tendance à s'accroître plus on s'éloignait de la valeur critique de la contrainte ayant conduit à leur apparition [59] .

Par doublement de la période : par augmentation du paramètre de contrôle de l'expérience, la fréquence du régime périodique double, puis est multipliée par 4, par 8, par 16 < etc. Les doublements étant de plus en plus rapprochés, on tend vers un point d'accumulation auquel on obtiendrait hypothétiquement une fréquence infinie. C'est à ce moment que le système devient chaotique.

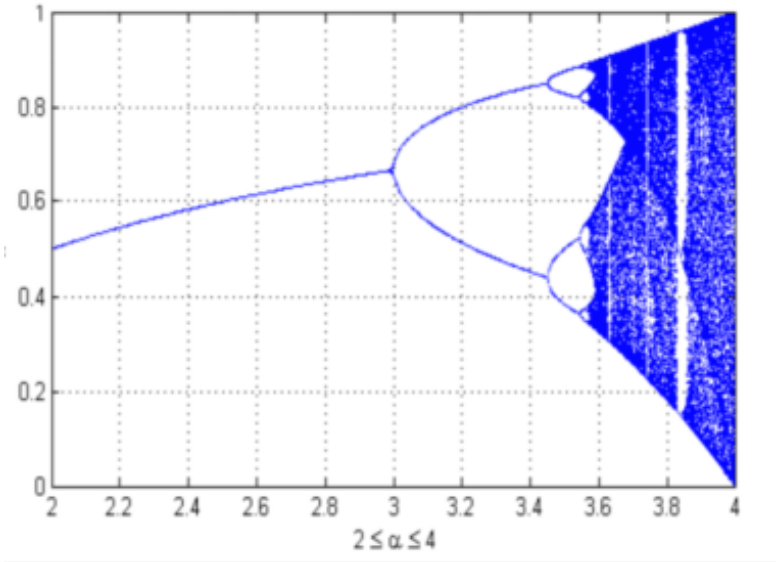


FIGURE 2.5 – Diagramme de bifurcation de la fonction logistique. [45]

2.8 Les cartes chaotiques

Parmi les nombreuses cartes chaotiques de la littérature, nous présentons très brièvement ci-dessous seulement les équations de quatre cartes chaotiques très utilisées en pratique qui sont [18] : la carte Logistique, la carte PWLCM (Piece Wise Linear Chaotic Map), La carte d'ARNOLD et la carte Sine . Ces cartes possèdent plusieurs bonnes propriétés : réalisation simple, et généralement assez bonne propriété cryptographique.

2.8.1 La carte Logistique

Une suite logistique est une suite simple, dont la carte n'est pas linéaire et donnée par la relation suivante [18] :

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

x est la variable dynamique prenant des valeurs entre 0 et 1 non inclus et r est le paramètre du système. Selon la valeur de r, la suite peut être un point fixe, une suite périodique de période 2, 4, 8, : : : , et 64 pour r = 3,569692, ou une suite chaotique pour r compris entre 3,56996 et 4.

2.8.2 La carte PWLCM (Piece Wise Linear Chaotic Map)

La carte chaotique Piece Wise Linear Chaotic Map (PWLCM) est composée de plusieurs segments linéaires par morceaux dont l'équation est donnée par [48] :
$x(n) = F\left[x\left(n-1\right), p\right]$

$$x\left\{n\right\} = \begin{cases} x\left(n-1\right) \times \frac{1}{p} & : \ 0 \leq x\left(n-1\right) < p \\ \left(x\left(n-1\right) - p\right) \times \frac{1}{0.5-p} & : \ p \leq x\left(n-1\right) < 0.5 \\ F\left[1 - x\left(n-1\right)\right] & : \ 0.5 \leq x\left(n-1\right) < 1 \end{cases} \tag{2.4}$$

$p \in [0, 0:5]$ est le paramètre de contrôle et $x(0) \in [0, 0:5[$ est la valeur initiale.
La figure 2.6 (a) ci-dessous représente la forme temporelle de la fonction PWLCM pour 300 itérations, utilisant une valeur initiale x(0) égale à 0.6, et une valeur de paramètre p égale à 0.3.
La figure 2.6 (b), représente l'attracteur, courbe $\left[x\left(n\right), x\left(n+1\right)\right]$ de la carte PWLCM (tracé pour 1000 itérations).

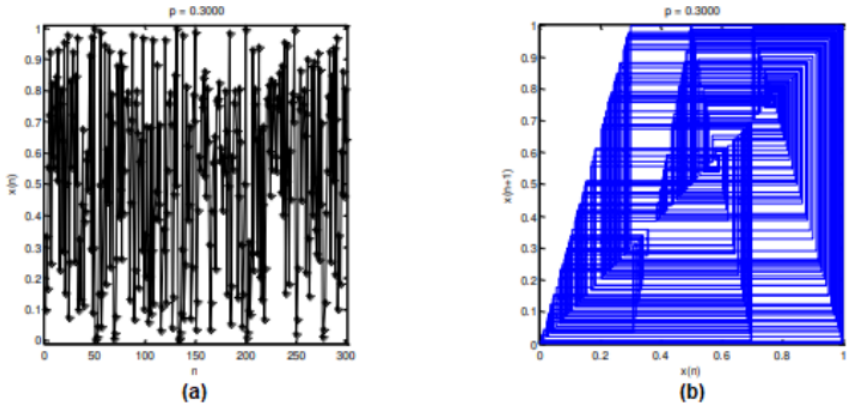


FIGURE 2.6 – Carte PWLCM : (a) Séquence x(n) ; (b) Attracteur. [48]

La carte PWLCM est caractérisée par :

1. Une densité invariante et uniforme .
2. Une réalisation simple du point de vue matériel et logiciel .

2.8.3 La carte d'ARNOLD

La carte chaotique appelée la carte d'Arnold en reconnaissance de mathématicien russe Vladimir I. Arnold, qui l'a découverte en utilisant une image d'un chat. C'est une démonstration et une illustration simple et élégante de certains des principes de chaos, une évolution apparemment aléatoire d'un système. [48]

La carte de chat d'Arnold est une carte chaotique typique, son expression est comme dans :

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \times \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod n \tag{2.5}$$

x_{n+1} et y_{n+1}'est nouvelle position du pixel, et x,y est la position originale de ce pixel,a, b sont les paramètres qui sont des entiers positifs.

2.9 schéma de cryptage d'image basé sur le chaos

Avec le développement rapide de la transmission d'images à travers les réseaux informatiques, en particulier Internet, la sécurité des images numériques est devenue une préoccupation majeure. Le cryptage d'image diffère du cryptage de texte en raison de certaines caractéristiques

intrinsèques des images, notamment les capacités de données en masse, une redondance élevée, de fortes corrélations entre les pixels, etc. [49] Ces caractéristiques rendent les systèmes de chiffrement conventionnels tels que DES, AES et RSA inadaptés au chiffrement d'image pratique. Afin de pallier les problèmes de chiffrement d'images, ces dernières années, de nombreux scientifiques et ingénieurs ont conçu des algorithmes de chiffrement d'images basés sur une ou plusieurs cartes chaotiques [50] [51].En raison des propriétés souhaitables des systèmes dynamiques non linéaires telles qu'une forte dépendance sensible aux conditions initiales et au paramètre de contrôle, l'imprévisibilité, et un grand espace de clé ,etc..., qui sont analogues aux propriétés de confusion et de diffusion de Shannon [52].le cryptage basé sur le chaos a suggéré une nouvelle façon efficace de traiter le problème insoluble de l'image rapide et hautement sécurisée.
Fridrich [53] a suggéré qu'un algorithme de cryptage d'image basé sur le chaos approprié devrait être composé de deux phases : une phase consiste à permuter l'ordre des pixels de l'image à l'aide de cartes chaotiques tandis que l'autre phase consiste à modifier les valeurs numériques représentant le couleur de chaque pixel, toujours en utilisant des cartes chaotiques. Ces deux phases sont appelées la phase de confusion (permutation) et la phase de diffusion.

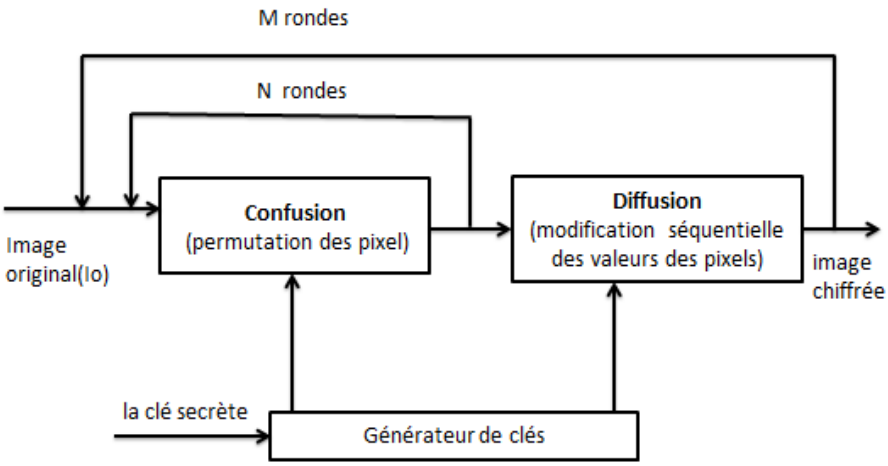


FIGURE 2.7 – Algorithme de chiffrement d'image basé sur le chaos [54].

2.9.1 Permutation

Dans l'étape de permutation, tous les pixels de l'image sont permutés selon certaines transformations, sans changer leurs valeurs . Les pixels adjacents dans une image naturelle ont généralement une corrélation élevée car leurs valeurs sont proches les unes des autres. Pour dé corréler leur relation, il faut les déplacer dans des lieux différents, avec l'existence des tours de

permutation (m) où ($m \geq 1$) A la fin de cette étape, chaque pixel est remplacé par un autre dans la même image.

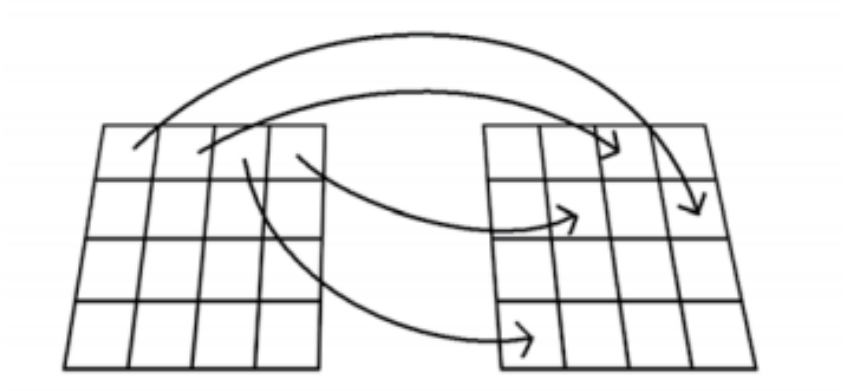


FIGURE 2.8 – permutation des pixels . [54]

2.9.2 Diffusion

Dans l'étape de diffusion, les valeurs des pixels sont modifiées séquentiellement pour confondre la relation entre l'image chiffrée et l'image simple afin d'augmenter l'entropie de l'image simple en uniformisant son histogramme [55].

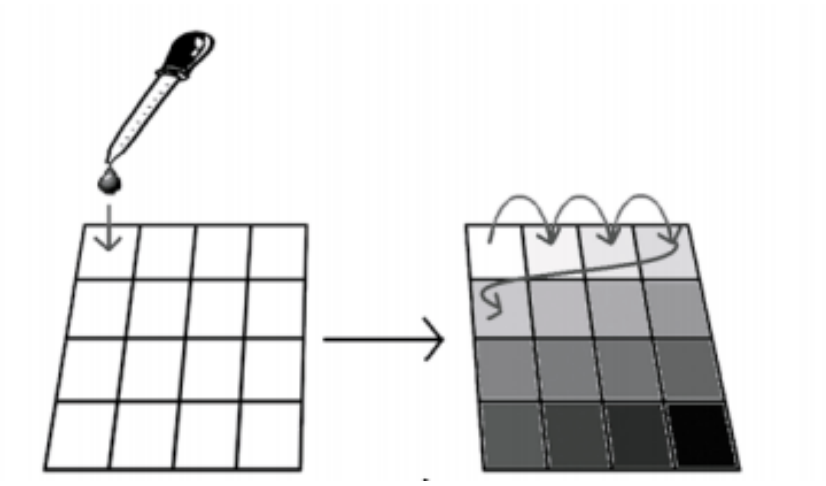


FIGURE 2.9 – diffusion des pixels. [54]

2.10 Analyse des performances et de la sécurité :

La sécurité d'un crypto système d'image est déterminée par ses capacités de confusion et de diffusion. Elle est généralement évaluée par les mesures quantitatives suivantes [56].

2.10.1 Analyse clé

L'analyse de la clé comprend l'espace de clé, la sensibilité de la clé pour évaluer la force du crypto système contre la force brute et les pirates différentiels. [57]

2.10.1.1 Espace de clé

La clé des crypto systèmes d'images basés sur le chaos de type substitution-diffusion est une combinaison de la clé de substitution et de la clé de diffusion. La clé de substitution est généralement composée des paramètres de la carte chaotique sélectionnée tandis que la clé de diffusion est constituée de la valeur initiale et des paramètres de la fonction de diffusion.
Pour un crypto système d'image efficace et sécurisé, un espace de clés de 2^{128}bits ou plus est nécessaire pour résister aux attaques de recherche par force brute. [54]
Cet espace est calculé en multipliant simplement l'espace total de chaque clé individuelle comme indiqué dans la formule suivante [58] :

$$S = \prod_{i=1}^{k} Sk_i \tag{2.6}$$

Où , S est l'espace de clé total et Sk_i est l'espace de l'ième clé.
Il convient de noter que l'espace clé de chaque clé individuelle dépend principalement de la précision de la clé. Un nombre en double précision est représenté sur 64 bits (8 octets), ce qui signifie que l'espace total est de 2^{64}.

2.10.1.2 Sensibilité de la clé :

Un algorithme idéal de chiffrement d'image doit être sensible à la clé. C'est-à-dire le Changement d'un seul bit dans la clé secrète devrait produire une image cryptée complètement Différente. [59]

2.10.2 Analyses statistiques

L'analyse statistique permet de déchiffrer les algorithmes de cryptage comme était Mentionné sur [60].
Durant cette partie, nous allons étudier les histogrammes des images cryptées ainsi que la corrélation de pixels adjacents.

2.10.2.1 Histogramme :

L'histogramme de l'image est une courbe statistique bidimensionnelle montrant la répartition des valeurs d'intensité lumineuses des pixels. [57]

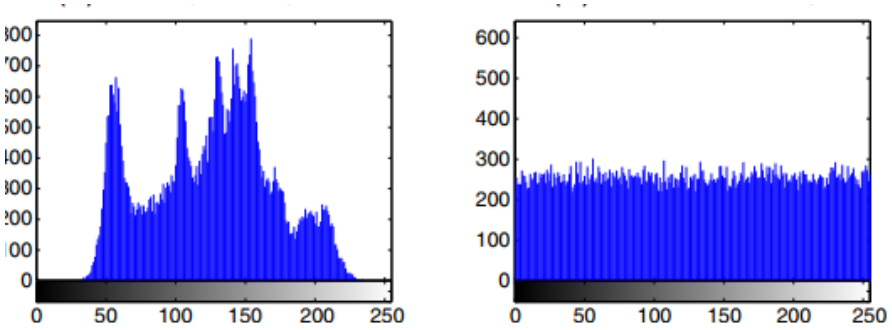


FIGURE 2.10 – Histogramme de l'image originale et de l'image cryptée [57]

2.10.2.2 Corrélation des 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, et les coefficients de corrélation de chaque paire ont été calculées en utilisant les formules suivantes : [57]

$$r = \frac{Cov\left(x,y\right)}{\sqrt{D\left(x\right)}\sqrt{D\left(y\right)}} \tag{2.7}$$

2.10.2.3 L'entropie

L'entropie d'une image est un indicateur de sa complexité. Si l'image est uniforme et ne possède qu'une couleur, son entropie est nulle. Plus l'entropie est élevée, plus l'image est "aléatoire" [57].

$$H\left(m\right) = -\sum_{i=0}^{2^n-1} p_i \log_2\left(p_i\right) \tag{2.8}$$

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.

2.10.3 Attaques différentielles :

Afin de résister à une attaque différentielle, une petite altération de l'image simple devrait provoquer un changement substantiel de l'image cryptée. Les deux images cryptées sont ensuite comparées quantitativement à l'aide des mesures suivantes [44] [45] :

2.10.3.1 Taux de changement du nombre de pixels(NPCR) :

Le nombre de pixels changeants dans deux images de texte chiffré peut être calculé via le test NPCR lorsqu'il y a une différence infime d'un pixel entre leurs images en clair. La formule mathématique du NPCR est [72] :

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{2.9}$$

Si les deux images chiffrées ont la même valeur alors$D\left(i,j\right) = 0$ alors que dans le cas contraire, $D\left(i,j\right) = 1$. La limite supérieure du NCPR est de 100% mais pour un bon système de chiffrement, la valeur du NCPR doit être supérieure à $99,5\%$.

2.10.3.2 Intensité variable moyenne unifiée(UACI)

Le degré d'intensité modifiée moyenne entre deux images de texte chiffré peut être calculé à l'aide du test UACI lorsqu'il existe une différence d'un pixel entre leurs images de texte en clair correspondantes. L'expression mathématique pour UACI est [72] :

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{2.10}$$

$c_1\left(i,j\right)$ et $c_2\left(i,j\right)$ signifient les images cryptées dont les images en clair correspondantes sont différentes les unes des autres d'un seul pixel.

2.10.4 PSNR et SSIM

pour évaluer le changement de valeurs de pixel et la fiabilité de l'image décryptée à partir de l'image simple, deux outils importants sont couramment utilisés ,à savoir la valeur de similarité structurelle (SSIM), le rapport signal sur bruit de crête (PSNR) . [61]

1. **PSNR**

   Le PSNR est évalué comme suit :

$$PSNR = 10 \times \log_{10} \frac{2^8 - 1}{MSE} \tag{2.11}$$

   où

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{ij} - Y_{ij})^2 \tag{2.12}$$

   X représente image claire, Y est l'image cryptée et M × N représente la longueur et largeur de l'image simple, la valeur de PSNR doit être le plus bas possible .

2. **SSIM**

   L'indice SSIM est utilisé pour mesurer la similarité de structure entre deux images. L'indice SSIM est calculé sur diverses fenêtres d'une image donnée. Le SSIM entre deux fenêtres X et Y est donné par l'équation suivante :

$$SSIM(X,\ Y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{2.13}$$

   où μ_x et μ_y représentent respectivement les moyennes de X et Y. σ_x et σ_y représentent les écarts types de X et Y . σ_{xy} est la covariance de X et Y , c_1 et c_2 sont deux constantes ajoutées pour éviter les zéros dominants. Les valeurs SSIM sont comprises entre 0 et 1 ,0 signifie une différence majeure entre l'image cryptée et l'original.

2.11 Travaux connexes

2.11.1 Chong Fu ,Yu-fu,2018

Dans le présent article Chong Fu ,Yu-fu Shan ,ont proposé un nouvel algorithme cryptographique basé sur le chaos pour la protection des images médicales. Dans l'étape de permutation, nous introduisons une méthode de brouillage d'images basée sur l'échange de pixels avec une séquence de flux de clés générée à partir de la carte logistique. Dans l'étape de substitution, trois cartes chaotiques 1-D composées, sont utilisées pour générer les séquences de flux clés pour mélanger les valeurs de pixel.
propriétés tout en restant simplicité. Pour assurer la robustesse de l'algorithme proposé contre l'attaque du texte en clair choisi et augmenter l'intensité de diffusion, nous introduisons un mécanisme pour associer la séquence de flux de clés de substitution à l'image en clair. [62]

2.11.2 B aoru Han, Yuanyuan Jia,2020

B aoru Han, Yuanyuan Jia et al ont proposé un algorithme de cryptage des images médicales basé sur le réseau neuronal chaotique Hermite , Premièrement, l'algorithme de cryptage des images médicales utilise des séquences chaotiques générées par la carte logistique. Deuxièmement, cette séquence chaotique est utilisée pour former un réseau neuronal chaotique Hermite et adopte mn , Les indicateurs de formation du réseau neuronal chaotique Hermite sont déterminés en fonction de la situation réelle. Et l'algorithme de formation BP est utilisé afin d'accélérer la vitesse d'apprentissage ,ensuite Deux ensembles de séquences chaotiques sont générés par le Réseau neuronal chaotique Hermite et deux valeurs initiales. Leur nombre est déterminé par l'image médicale initiale à chiffrer. Ces deux ensembles de séquences chaotiques sont chacun multipliés par les coefficients correspondants. Les deux coefficients correspondants sont 0,35 et 0,65,et Les deux ensembles de séquences chaotiques traités sont additionnés. Deux ensembles de séquences chaotiques deviennent une séquence chaotique en fin L'image médicale d'origine est multipliée par un coefficient.tour ($somme \times 256$) est multiplié par un autre coefficient. La somme de ces deux coefficients vaut 1. Effectuez ensuite l'opération d'addition pour obtenir l'image médicale crypté. l'algorithme de déchiffrement est l'inverse du processus chiffrement. [64]
L'analyse de sécurité montre que l'algorithme de cryptage peut résister efficacement à l'analyse statistique, a une forte sensibilité aux clés, un grand espace de clés et améliore considérablement la sécurité des images médicales.

2.11.3 Seyed Shahabeddin Moafimadani ,2019

Seyed Shahabeddin Moafimadani et.al ont proposé un nouvel algorithme basé sur des systèmes chaotiques et des systèmes SHA-256 pour protéger les images contre les attaque , Le système est divisé en deux parties, la première partie est le processus de permutation à grande vitesse où l'image simple est prise en entrée. Les vecteurs dans le processus de diffusion adaptative sont obtenus en itérant à travers le système chaotique en utilisant les paramètres de départ et les valeurs de l'image d'entrée, puis la règle de décalage binaire est appliquée pour les quantifier en tant que clé. À l'aide de la clé générée, le cryptage et le décryptage sont effectués. Le texte brut sélectionné est testé à l'aide d'images spéciales comme toutes les images noires ou toutes les images blanches. Les résultats de la méthode proposée qui sont obtenus à partir de l'analyse des attaques de bruit et d'occlusion montrent qu'elle peut résister aux attaques. Les images résultantes sont de qualité satisfaisante et l'algorithme présente également une entropie élevée par rapport aux autres méthodes. L'algorithme de chiffrement est illustré dans la figure2.11 [63]

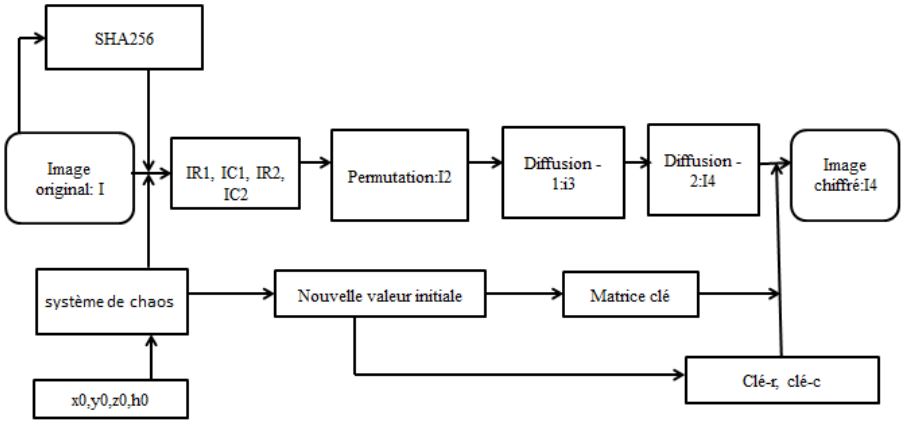


FIGURE 2.11 – Schéma de l'algorithme de chiffrement proposé [63]

2.11.4 M Harshitha, C Rupa,2021

Dans ce travail M Harshitha, C Rupa et al ont proposé, Sécuriser les données médicales à l'aide d'un mappage logistique chaotique basé sur un chiffrement symétriques ,ils génèrent d'abord la matrice clé en utilisant la carte logistique chaotique et le registre à décalage droit. Une séquence de sous-clés, c'est-à-dire k1, est générée à l'aide de la carte logistique * et une autre séquence de sous-clés est générée, c'est-à-dire k2, en utilisant un registre à décalage linéaire à droite qui fonctionne avec une valeur de départ initiale. Ensuite, les deux séquences

k1 et k2 sont XOR pour former la matrice clé finale. Ensuite, la matrice de clé générée est XOR avec le pixel d'image médicale simple de 8 bits pour obtenir une matrice de chiffrement. La matrice de pixels d'image médicale simple est ensuite remplacée par cette matrice de chiffrement pour obtenir le chiffrement image médicale. Nous pouvons stocker cette image chiffrée ou la transmettre. Cela augmente la résistance du système aux attaques de sécurité telles que les attaques cryptanalytiques par force brute, etc. Lors des tests, le système a pu sécuriser efficacement divers formats d'images de différentes tailles et a également réussi à sécuriser les images RVB et en niveaux de gris. Ces fonctionnalités rendent le système robuste et encore plus sécurisé. De plus, le mécanisme proposé fonctionne avec un faible temps de calcul. Ainsi, le système peut être utilisé dans des scénarios en temps réel pour sécuriser efficacement les données d'images médicales dans un court laps de temps. [65]

2.11.5 X Chen ,CJ Hu,2017

Cet article propose un algorithme de cryptage adaptatif d'images médicales basé sur une cartographie chaotique améliorée afin de surmonter les défauts de l'algorithme de cryptage d'images chaotique existant. Tout d'abord, l'algorithme a utilisé la cartographie du chaos Logistique sine pour brouiller l'image simple. Ensuite, l'image brouillée a été divisée en 2-par-2sous-blocs. En utilisant le système hyper-chaotique (expresion 2.14), les sous-blocs ont été cryptés de manière adaptative jusqu'à ce que tout le cryptage des sous-blocs soit terminé. En analysant l'espace clé, l'entropie de l'information, le coefficient de corrélation et la sensibilité du texte en clair de l'algorithme, les résultats expérimentaux montrent que l'algorithme proposé surmonte le défaut de manque de diffusion dans le chiffrement à sens unique. Il pourrait résister efficacement à toutes sortes d'attaques et a une meilleure sécurité et robustesse. [66]

Système hyper-chaotique : L'équation du système hyper-chaotique est décrite comme :

$$\begin{cases} x_1 = a\left(x_2 - x_1\right) x_2 x_3 x_4 \\ x_2 = b\left(x_1 + x_2\right) x_1 x_3 x_4 \\ x_3 = -c x_3 + x_1 x_2 x_4 \\ x_4 = -d x_4 + x_1 x_2 x_3 \end{cases} \tag{2.14}$$

a, b, c et d sont les paramètres de contrôle du système.
Dans le cas où a = 35, b = 10, c = 1 et d = 10, un algorithme de Runge-Kutta du quatrième ordre est utilisé pour résoudre l'équation ,avec un pas de h = 0,001. Pendant ce temps, x1 est défini comme une petite valeur initiale produite à partir du flux de clé, tandis que les autres paramètres sont inchangés. Les quatre groupes de séquences chaotiques discrètes produites par itération sont X1, X2, X3 et X4.

2.11.6 Akram Belazi,Akram Belazi,2019

Dans cet article, Akram Belazi, Muhammad et al ,ont proposé un nouveau schéma de cryptage basé sur le chaos pour les images médicales. Il est basé sur une combinaison de chaos et de calcul ADN sous le scénario de deux cycles de chiffrement, précédés d'une couche de génération de clé, et suit la structure de permutation-substitution-diffusion. [67]
La fonction de hachage SHA-256 aux côtés des clés secrètes initiales est utilisée pour produire les clés secrètes des systèmes chaotiques. Chaque cycle de l'algorithme proposé comprend six étapes, à savoir la permutation basée sur les blocs, la substitution basée sur les pixels, le codage de l'ADN, la substitution au niveau du bit (c'est-à-dire la complémentation de l'ADN), le décodage de l'ADN et la diffusion au niveau du bit. . Les flux de clé dans la substitution au niveau du bit sont basés sur la carte logistique de Chebyshev, tandis que la carte sinusoïdale de Chebyshev permet de produire les flux de clé dans la diffusion au niveau du bit. L'image cryptée finale est obtenue en répétant une fois les étapes précédentes à l'aide de nouvelles clés secrètes. Les analyses de sécurité et les simulations informatiques confirment toutes deux que le schéma proposé est suffisamment robuste contre tous sortes d'attaques. Sa faible complexité indique son fort potentiel pour les applications d'images en temps réel et sécurisées.
Une séquence d'ADN comprend quatre bases d'acide nucléique, c'est-à-dire A (adénine), G (guanine), C (cytosine) et T (thymine). Ces bases d'ADN suivent le principe de Watson-Crick Autrement dit, A et T sont complémentaires, et C et G sont complémentaires. Habituellement, les quatre bases d'ADN A, C, G et T sont codés par deux bits, c'est-à-dire 00, 01, 10 et 11.En codage binaire, 0 et 1 sont complémentaires, donc 00 et 11 sont complémentaires, tout comme 01 et 10En utilisant quatre bases A, C, G et T pour coder 00, 01, 10 et 11, il y a 24 règles de codage, parmi lesquelles il n'y a que huit règles (voir tableau 2.1) vérifiant les relations complémentaires entre xel est de 100, sa valeur binaire correspondante est "10011101", qui peut être codée comme la séquence d'ADN "GCAC" en utilisant la règle de codage de l'ADN 7.

base	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	00	11	10	10	01	01	00	00
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01

TABLE 2.1 – les Règles de codage de l'ADN

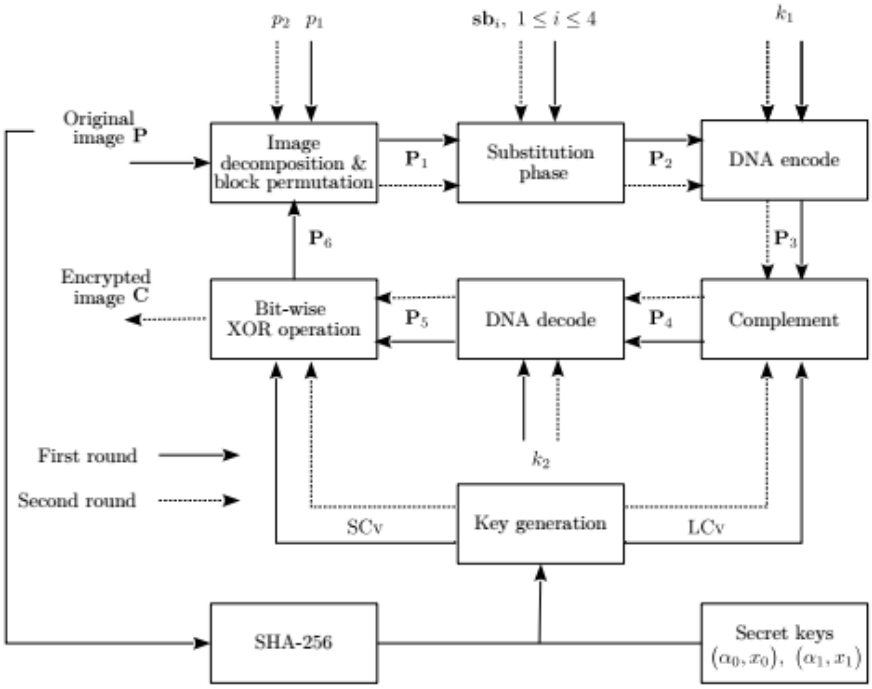


FIGURE 2.12 – Organigramme de l'approche de chiffrement proposé

2.11.7 M Madani and Y Bentoutou,2015

Cet article [68] a proposé un nouveau système de chiffrement pour les images médicales en s'appuyant sur un générateur des clés basé sur le mixage des cartes chaotiques et une technique de confusion-diffusion des données. En pratique, l'algorithme est implémenté avec trois cartes chaotiques, Logistique (expression 2.15), Chebyshev (expression 2.17)et la carte standard(expression 2.17).

Pour ce schéma, trois cartes chaotiques sont utilisées, la carte logistique la carte sine et la récurrence standard .

$$x_{n+1} = r x_n \left(1 - x_n\right) avec\ x_n \subset [0, 1] \tag{2.15}$$

$$x_{n+1} = \lambda \sin\left(\prod x_n\right) \tag{2.16}$$

$$x_{n+1} = x_n + K \sin(y_n)\, x_{n+1} = y_n + (x_{n+1}) \tag{2.17}$$

Au début il faut augmenter les nombres de bits par pixels de 16 à 32 selon la taille de l'image, puis mettre l'image sous forme d'un vecteur et on applique le chiffrement chaotique. Ce choix a été effectué afin d'avoir une qualité plus élevée demandée par les images médicales, et aussi pour appliquer une méthode qui nous permet d'effectuer une diminution de la taille de la matrice image sans perdre aucune information. les étapes pratiques de l'algorithme de chiffrement peuvent être exprimées comme suit :

— Une diffusion, pseudo confusion et compression, Ici l'étape consiste à modifier les propriétés de l'image afin de lui donner une taille variable et plus petite que l'originale selon les valeurs trouvées dans la matrice. Au lieu de garder toute l'information on conserve juste le 1er pixel parmi les autres pixels adjacents et de même niveau de couleur, plus grouper ses positions en séparant chaque niveau différent par 0.

— Un Générateur chaotique de l'expression 2.17utilisé pour le choix entre deux autres systèmes aléatoires (2.16) permettant d'appliquer une confusion de l'image compressée avec une clé générée à partir de l'une des cartes choisies (expression 2.15 ou 2.16).

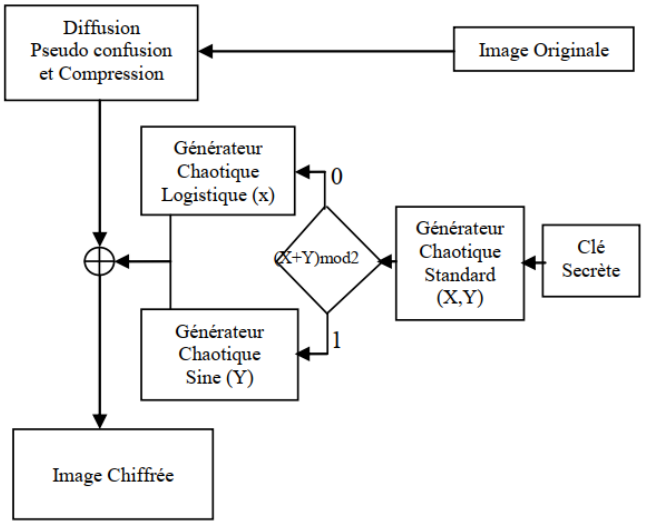


FIGURE 2.13 – Algorithme de chiffrement [68]

2.11.8 Junjie Zhang, Jun Tan,2017

cet article ont proposé Algorithme de chiffrement d'images médicales basé sur une fonction chaotique.les étapes pratiques de l'algorithme de chiffrement peuvent être exprimées comme suit : [69]

— Sélectionnez les valeurs initiales appropriées et itérez selon la fonction traditionnelle de Chebyshev , les temps d'itération sont déterminés en fonction du nombre de pixels N= M*N. Obtenir un vecteur à N- dimensions $\{x_0, x_1, x_2, ...x_{n-1}\}$.

— Trier le vecteur N-dimensionnel obtenu par itération en obtenir une nouvelle suite $\{x'_0, x'_1, x'_2, x'_3\}$.

— Selon le vecteur aléatoire qui est généré par la fonction itérée du chaos, un indice de brouillage chiffré par un nombre naturel $\{h_1, h_2, h_3...\}$qui contient 1... N.

— Numérotez chaque pixel, réorganisez-le en fonction du hasard, nombre de vecteurs naturels $\{h_1, h_2, h_3...\}$ et IIème position correspondante du pixel dans le vecteur à N dimensions, pixels sont brouillés.

— Envoyer les images cryptées et l'adresse IP de la partie cryptée côté stockage.

2.11.9 HS Jeong, KC Park,2018

Dans cet article, ont proposé une nouvelle méthode de cryptage d'images médicales en couleur utilisant une carte chaotique bidimensionnelle et C-MLCA. La carte chaotique bidimensionnelle est une structure aux propriétés d'auto-préservation, qui déplace la position du pixel et crypte l'image.
[70] C-MLCA utilise une séquence PN de longueur maximale basée sur les propriétés de CA. Les séquences avec des règles complexes imprévisibles créent une image de base et l'image de base est calculée par OU exclusif avec l'image originale. C'est-à-dire que C-MLCA crypte l'image en modifiant les valeurs propres des pixels via le processus de calcul. En utilisant ces deux fonctionnalités, ils introduisent une méthode de cryptage efficace pour surmonter les limites des méthodes de cryptage existantes. En comparant et en analysant l'image cryptée avec l'image originale, ils ont pu confirmer que la méthode de cryptage proposée a un haut niveau de stabilité et de sécurité.

2.11.9.0.1 C-MLCA : Cellular Automata (CA) est un système dynamique à temps discret qui peut implémenter une fonction de transition déterminant l'état suivant par sa propre cellule et les deux cellules voisines. Il est défini par :

$$s_i^{t+1} = f(s_{i-1}^t, s_t^i, s_{i+1}^t) \tag{2.18}$$

s^t signifie que l'état de la i^{th} au temps t et f est une fonction due à l'interaction locale. Puisque la fonction f est une fonction booléenne à trois variables, les fonctions de transition d'état suivantes existent dans les cas 2^{2^3}. Wolfram a proposé le système et il est exprimé sous forme de règles utilisant chacun des 256 cas Dans cet article, nous utilisons la règle 90 et la règle 150, qui conviennent pour générer des modèles qui ont des caractéristiques linéaires et sont difficiles à prévoir.

2.11.10 Yasser, Ibrahim ,2021

Yasser, Ibrahim dans [71] ont recommandé un nouveau schéma hybride de cryptage/décryptage qui peut être appliqué dans les soins de santé en ligne, ou IoHS (Internet des systèmes de santé), pour la protection des images médicales. Le système proposé explore des algorithmes de perturbation innovants qui utilisent de nouvelles cartes chaotiques. Ils ont aussi proposé deux nouvelles cartes chaotiques 2D pour un pipeline robuste d'images médicales et/ou de cryptage de données. Le cadre proposé est une approche non linéaire en temps discret avec un comportement chaotique dynamique unique.
l'un est utilisé pour modifier les positions des pixels tandis que l'autre est utilisé pour modifier les valeurs de densité de pixels. De plus, l'évaluation à l'aide de diverses images de test a indiqué que le crypto système proposé est rapide, a une efficacité élevée, a montré une robustesse et une protection élevées des images médicales, et a documenté la bonne capacité à résister à une variété de cyber attaques.

2.12 Conclusion

Ce chapitre avait comme objectif d'introduction de quelques notions élémentaires concernant les systèmes dynamiques ainsi que l'étude théorique du phénomène chaotique qui a uncomportement sensible aux conditions initiales et un aspect semblable à l'aléatoire, par la suite nous avons présenté la route vers le chaos et nous avons défini quelques types de cartes chaotique. En plus de présenter quelques célèbres algorithmes de cryptage d'images basés sur le chaos où nous essayons d'analyser quelque-uns et aussi extraire les différents mesures de performance de chaque recherche ainsi nous comprenons les différents utilisations des cartes chaotiques pour le cryptage des images ou on a fait une analyse expérimentale détaillée de chaque article au but de connaitre les mesures adapter pour chaque carte.

Le chapitre suivant, sera consacré à l'explication des différents étapes suivis pour la réalisation de notre méthode proposée, ainsi tous les métriques sur lesquelles nous nous sommes appuyés pour arriver à une explication précise et détaillée de chiffrement propos.

CHAPITRE 3

NOUVELLE GÉNÉRATION D'UNE SÉQUENCE PSEUDO-ALÉATOIRE

3.1 Introduction

Un générateur de nombres aléatoires est un composant essentiel des systèmes cryptographiques modernes, des systèmes de communication, des systèmes de simulation statistique [74] et bien d'autres. L'une des applications les plus importantes des générateurs de nombres aléatoires est en cryptographie pour générer des clés cryptographiques, et également plus utilisée dans les fonctions de diffusion du cryptage d'image pour les pixels diffusés d'une image simple.

Les générateurs de nombres aléatoires peuvent être classés en trois classes ; vrais générateurs de nombres aléatoires, générateurs de nombres pseudo-aléatoires et générateurs de nombres aléatoires hybrides. Les générateurs de nombres pseudo-aléatoires sont des processus déterministes qui génèrent une série de sorties à partir d'un état de départ initial [75].

Dans ce chapitre nous allons présenter notre proposition. Cette proposition c'est la génération d'une séquence pseudo aléatoire basé sue les deux cartes chaotiques (la carte Pwlcm et la carte logistique). Les séquences de bits aléatoires produites par ce générateur sont évaluées à l'aide des 15 tests statistiques recommandés par le NIST et autre mesures de Séquence pour être prouver qu'elle est aléatoire , déterministe est sensible aux conditions initiales.

Ensuite on va Crypté différentes images numérique en basant sur la génération de séquence proposé, une série des mesures statistiques de sécurité et d'outils d'évolution doit être effectuée sur ce cryptage pour prouver que la Séquence proposée peut être appliqué dans la cryptographie.

3.2 Génération d'une séquence pseudo aléatoire

Dans cette section, nous introduisons une nouvelle proposition pour générer une séquence pseudo-aléatoire qui peut être utilisé de nombreuses fins, y compris les applications de cryptographie, cette génération est basés sur les deux cartes chaotiques carte logistique et carte pwlcm qui ont été mentionnées sur le chapitre2 (section2.8),la figure 3.1illustre le principe de cette proposition.

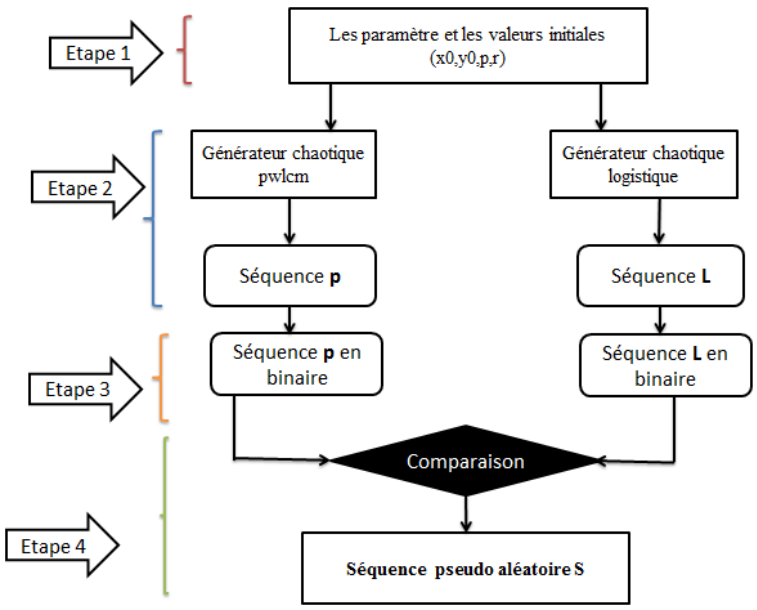


FIGURE 3.1 – schéma général de séquence proposée.

3.2.0.1 Processus de séquence proposée.

Voici le processus de génération de séquence préposée :

Etape 1 : définir les valeurs initiales et les contrôles de paramètres de la fonction pwlcm (x_0= 0.2159 , p= 0.3) et de fonction logistique (y_0=0.5842,r=3.999) .

Etape 2 : Nous allons générer deux séquences aléatoires en itérant la carte PWLCM et la carte logistique pour N itérations,Ensuite, nous convertissons les nombres réels de chaque séquence en un entier, ainsi nous obtenons deux séquences entières P et L.

Exemple :

Avec les valeurs initiales et les contrôle de paramètres écrite dans l'étape 1 , on va itérer les deux cartes pwlcm et logistique pour n=8 itérations,on obtient les séquences réels suivantes :

P = [0.7196666666666667 , 0.9344444444444444 , 0.21851851851851864 , 0.7283950617283955, 0.9053497942386817 , 0.3155006858710611 , 0.07750342935530563 , 0.25834476451768545] .

L = [0.97139852964 , 0.1111059215867311 , 0.394946821704602 , 0.9556163550904113 , 0.16961253415953878 , 0.5632356455396568 , 0.9837590112795984 , 0. 0638928988041357].

On convertit les deux séquences réels aux deux séquences entières P et L :

P = [170, 28, 75, 167, 124, 98, 234, 184].

L = [160, 209, 92, 49, 17, 237, 23, 93].

Etape 3 : La troisième étape consiste à convertir P et L sous forme des bits

P = [10101010000111000100101110100111011111000110001011101010101110000]

L = [10100000110100010101110000110001000100011110110100010111010111101]

Etape 4 : Faire la comparaison bit par bit entre la séquence L et la séquence P , Pour obtenir la séquence pseudo aléatoire S, on appliquent le principe du comparaison comme suite :

Algorithm 1 Comparaison

Séquence S, P, L
while $i < Taille(P)$ **do**
  if *P[i]=L[i]* **then**
    S(i)=0
  else
    S(i)=1
  end
end

3.3 Analyse de séquence

Dans cette partie, nous discutons l'analyse de sécurité pour prouvez que la Séquence proposée est aléatoire, déterministe et sensible à la condition initial. Ces tests de sécurité peuvent être utiles comme première étape pour déterminer si la génération de Séquence proposée est adapté pour l'utilisation en cryptographie, Ces tests comprennent : le test du NIST, l'histogramme, corrélation, ainsi que Sensibilité au condition initiale.

3.3.1 Analyse NIST

Les séquences sont évaluées par la suite de tests statistiques NIST. La suite contient un ensemble statistique contenant 15 tests pour quantifier et évaluer le caractère aléatoire des séquences [73]. Comme le montre le tableau3.1

Nist test	$P - value$	Résultat
Frequency Test	0.610051	Succès
Run Test	0.232579	Succès
Serial test (1)	0.400405	Succès
Serial test (2)	0.336543	Succès
Approximate Entropy Test	0.431500	Succès
Cummulative Sums Test	0.750519	Succès
Frequency Test within a block	0.083373	Succès
Binary Matrix Rank Test	0.865127	Succès
Discrete Fourier Transform Test	0.818545	Succès
Random Excursions Variant Test	0.638947	Succès
Random Excursions Test	0.516560	Succès
Overlapping Template Matching Test	0.577900	Succès
Non-overlapping Template Matching Test	0.643592	Succès
Linear Complexity Test	0.159128	Succès
Universal Statistica	0.359392	Succès

TABLE 3.1 – NIST(National Institute of Standards and Technology) résultats de test.

Les résultats de détection montrent que les fréquences ($p - valeur$) est $\geq$a= 0,01 signifierait que la séquence serait aléatoire avec une confiance de (1 - a) = 99%.

3.3.2 Sensibilité au condition initiale

Une séquence pseudo aléatoire parfait doit être sensibles aux conditions initiales, c'est a dire que un très léger changement de la valeur initiale peut conduire à deux séquences complètement

différentes, la figure 4.31 montre que la sensibilité de la méthode proposée à les valeurs initiales est très notable .

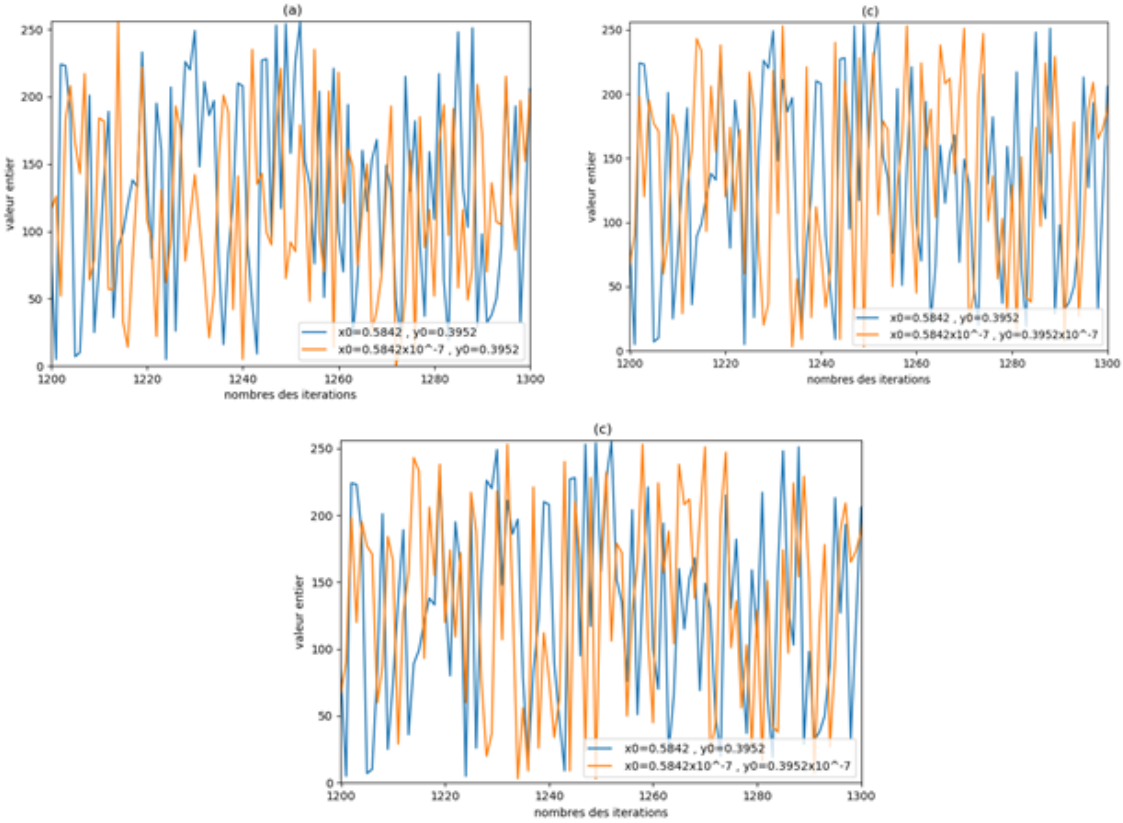


FIGURE 3.2 – la sensibilité de séquence : (a) : $x_0 = 0.5842 + 10^{-12}, y_0 = 0.2159, (b) : x_0 = 0.5842, y_0 = 0.2159 + 10^{-12}, (c) : x0 = 0.5842 + 10^{-12}, y0 = 0.2159 + 10^{-12}$

3.3.3 Analyse de corrélation

Nous générons 3 séquences avec des modifications dans les conditions initiales puis le test de corrélation est appliqué pour ces séquences. La table 3.2 montre que les séquences générés sont approximativement indépendants au sens où ils doivent être appliqués en cryptographie.

Y_0	Y_0	PXY
$0.7516 + 10^{-12}$	0.3952	0.0009716
0.7516	$0.3952 + 10^{-12}$	-0.0057663
$0.7516 + 10^{-12}$	$0.3952 + 10^{-12}$	0.0002779

TABLE 3.2 – Coefficients de corrélation entre x_0 et y_0 .

3.3.4 Histogrammes

Affichage des histogrammes de la séquence pour les controles des paramètres (p=0.3138 et r=3.999) avec 50.000 itérations.

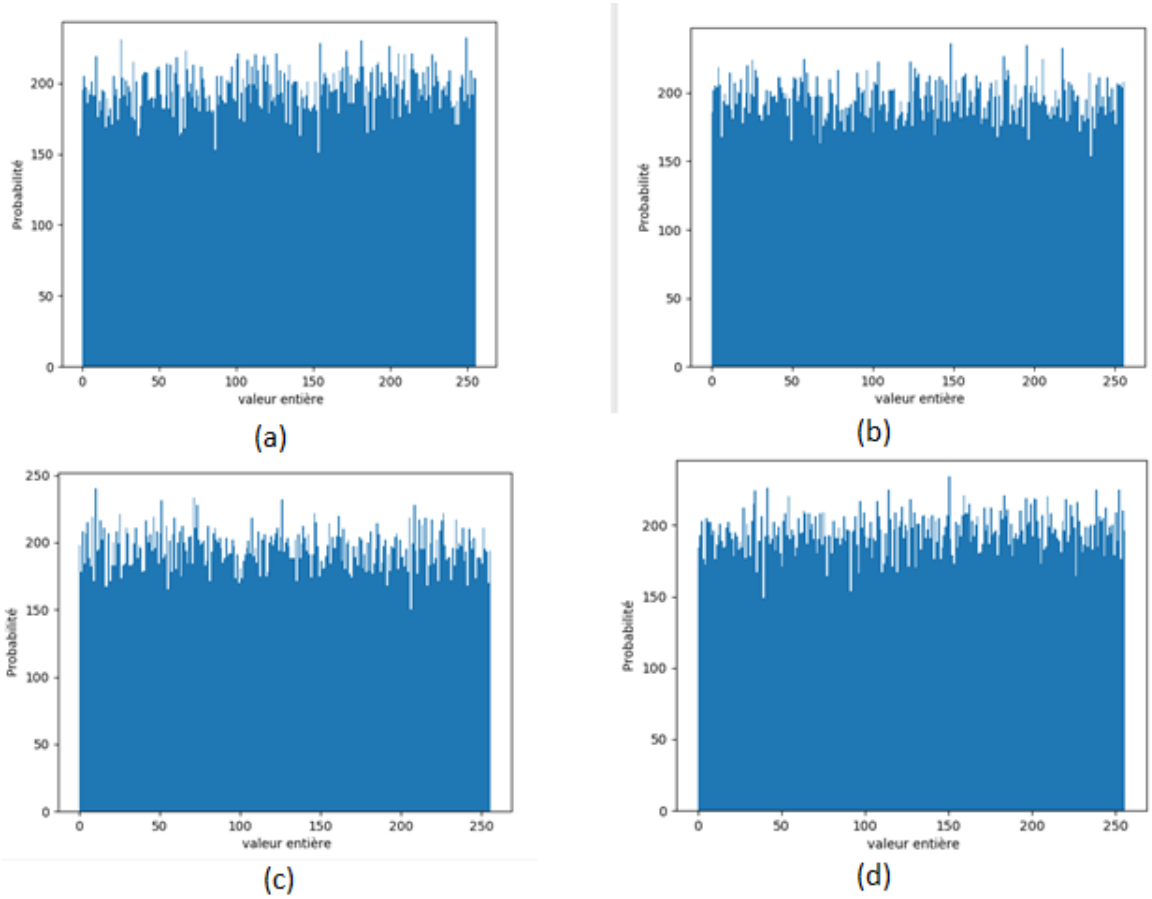


FIGURE 3.3 – Histogramme de la séquence : (a) x0= 0.5842,y0=0.2159 ; (b) x0= 0.7956,y0=0.4952 ; (c) x0= 0.7956 y0=0.3952 ; (d) x0= 0.6956,y0=0.4952

3.4 Cryptage d'image en utilisant la séquence générée

Dans cette section on va crypter des images en utilisant le générateur3.1proposée, d'abord une séquence pseudo aléatoire est générée en appliquons le générateur ensuite une opération XOR est effectuée entre la séquence générée et l'image claire , Une représentation schématique de la fonctionnalité de ce cryptage est illustrée dans la figure3.4Ci-dessous .

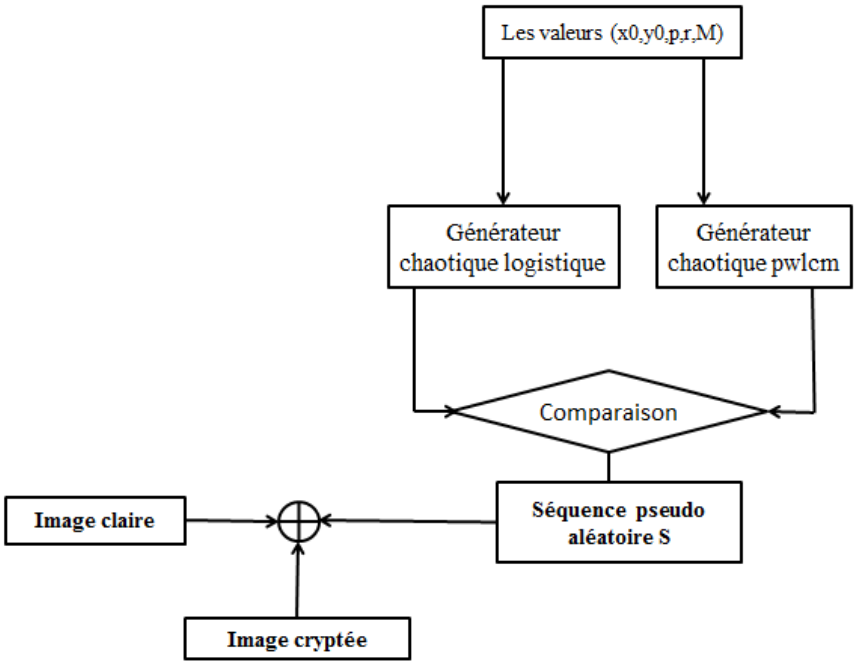


FIGURE 3.4 – cryptage d'image à laide de Générateur pseudo aléatoire proposé.

3.4.1 Résultats expérimentaux

Nous allons présenter les outils utilisés pour l'implémentation : le matériel et le langage.

3.4.1.1 Environnement de développement

Dans cette partie nous allons citer l'environnement matériel (Hardware) et logiciel (Software) utilisés.

1. **Environnement matérielle**
   - L'application a été créé depuis un HP Pavilion 15 Notebook PC tactile .
   - Processeur : Intel(R) Core(TM) i3-40300 CPU@ 1.90GHz .
   - Mémoire installé(RAM) : 4,00 Go .
   - Carte graphique : Intel(R) HD Graphics Family, NVIDIA GeForce 830M.
2. **Environnement logiciel**

   Nous avons choisi le langage Python (Version 3.8) pour développer notre système. Ce choix de langage est motivé par les raisons suivantes :
   - Python prend en charge à la fois le langage de programmation orienté objet et procédural.
   - sa syntaxe est simple et claire.

— respecte les standards du domaine .

— Disponibilité des packages de tous les domaines.

IDLE est l'environnement de développement et d'apprentissage intégré de Python(Integrated Development and Learning Environment).

Les bibliothèques utilisées : **tkinter**,**PIL**,**numpy**,**matplotlib**.

3.4.2 Les données utilisées

Des simulations numériques ont été faites pour confirmer les bonnes performances de notre schéma de cryptage. le tablaux 3.3 au-dessous montrent plusieurs images au niveau de gris de différentes tailles sont cryptées en utilisant le schéma 3.1 .

nous définissons les valeurs initiales et les contrôles de paramètres comme suite : $x_0 = 0.5842$, y_0 =0.2159 ,r=3.999, p=0.3.

Image	taille
Clock	256 × 256
Moon surface	256 × 256
Cameraman	256 × 256
Airplain	256 × 256
Baboon	512 × 512
Lenna	512 × 512
Peppers	512 × 512
Couple	512 × 512
Fishing Boat	512 × 512
Male	1024 × 1024
airport	1024 × 1024

TABLE 3.3 – Différentes images à utiliser

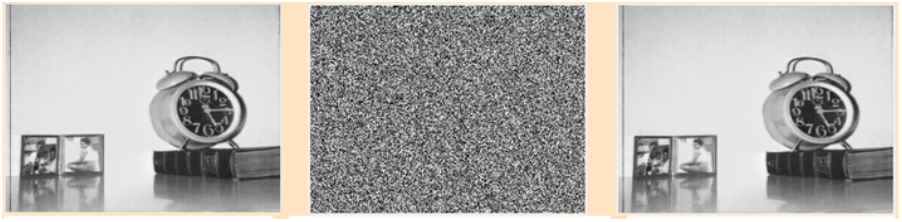


FIGURE 3.5 – Cryptage et décryptage d'image clock

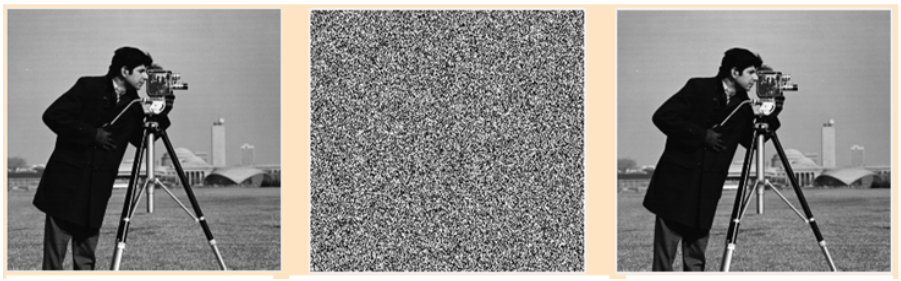


FIGURE 3.6 – Cryptage et décryptage d'image camera

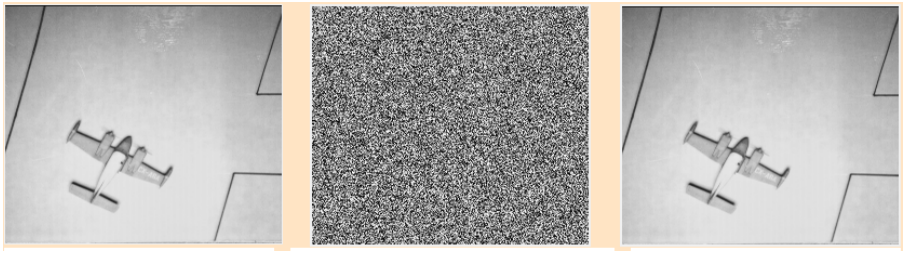


FIGURE 3.7 – Cryptage et décryptage d'image airplain

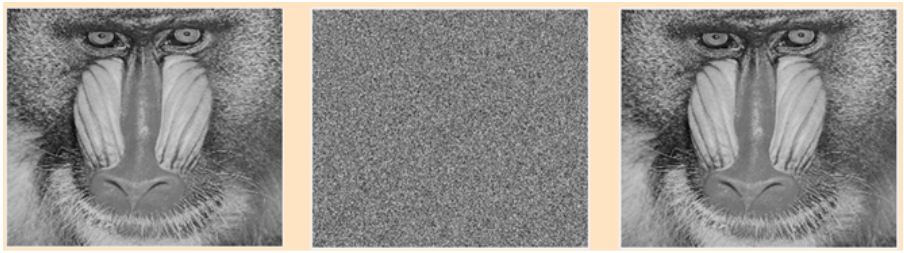


FIGURE 3.8 – Cryptage et décryptage d'image baboon

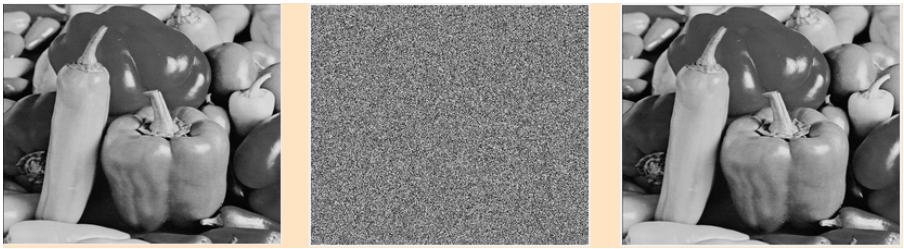


FIGURE 3.9 – Cryptage et décryptage d'image peppers

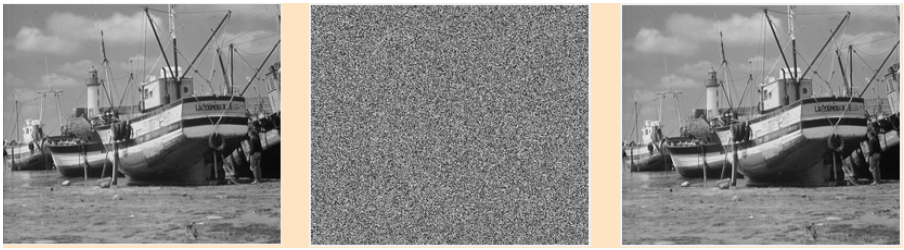


FIGURE 3.10 – Cryptage et décryptage d'image phishing boat

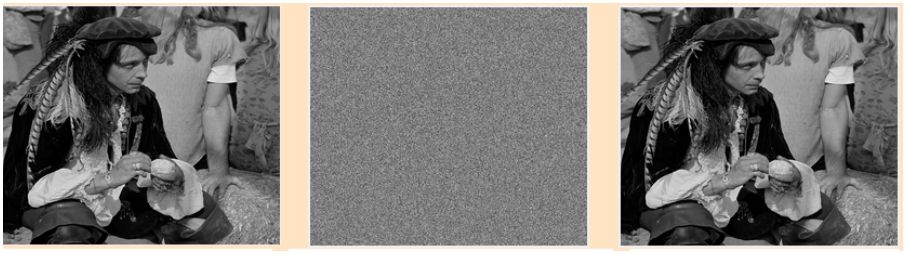


FIGURE 3.11 – Cryptage et décryptage d'image Male

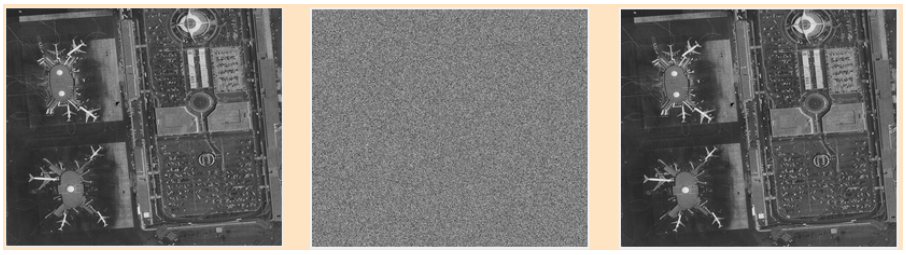


FIGURE 3.12 – Cryptage et décryptage d'image airoport

3.4.3 Mesure d'évaluation

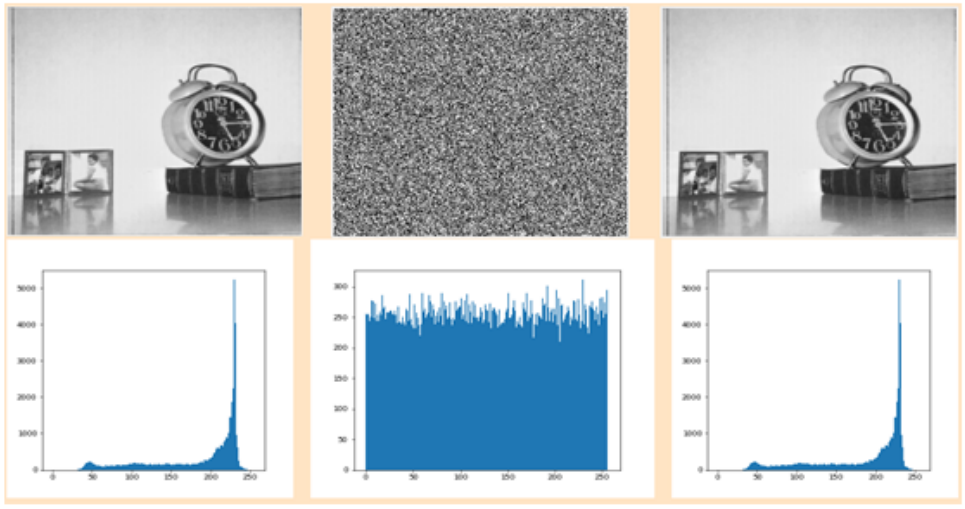
Pour assurer que l'image cryptée de ce schéma est suffisamment sécurisée contre diverses attaques cryptographiques, Certaines analyses ont été effectuées, comme démontré dans ce qui suit :

3.4.3.1 Analyse de l'espace de clé

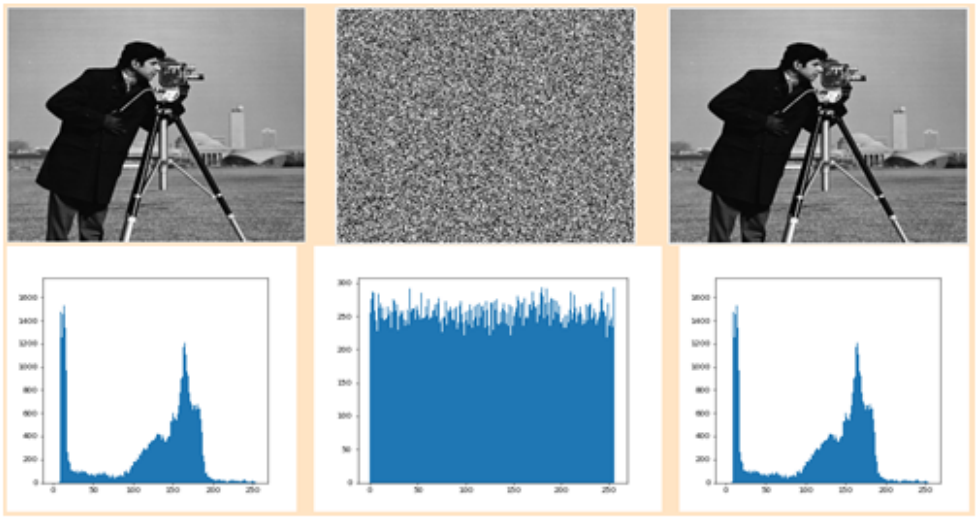
La taille de l'espace clé indique le nombre des clés différentes pouvant être utilisées pour le générateur de séquence (x_0, y_0, r, p),et selon la formule2.6 :
Donc la taille de l'espace clé est : $(1 \times 2^{64}) \times (1 \times 2^{64}) \times (0.5 \times 2^{64}) \times (0.432 \times 2^{64}) = 2^{253.8}$.
Cette valeur est plus grande que 2^{128}, cela prouve que notre système est résistant aux attaques forces brutes.

3.4.3.2 Histogramme

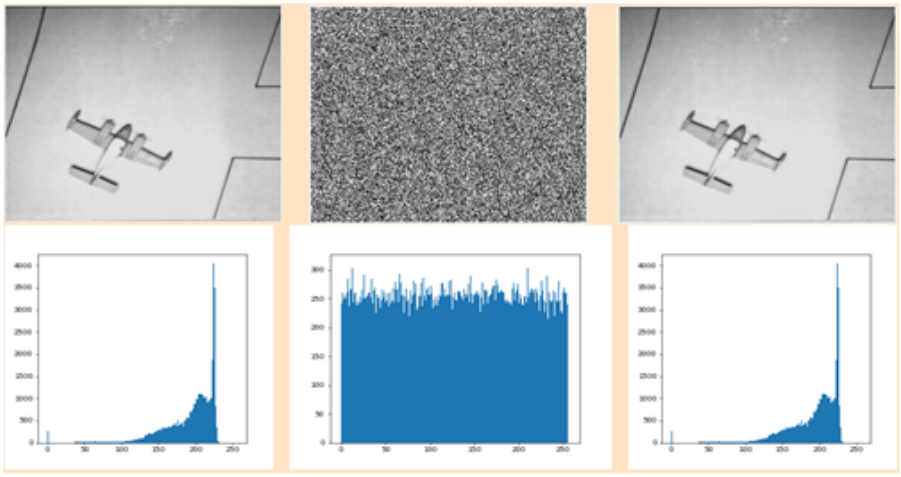
Toutes les images de tests du tableau 3.3 ont été utilisées dans cette analyse.
Les traces des histogrammes des images claires (a), images cryptées (b) et images décryptées (c) sont montrés dans la figure 3.13 ci-dessous.



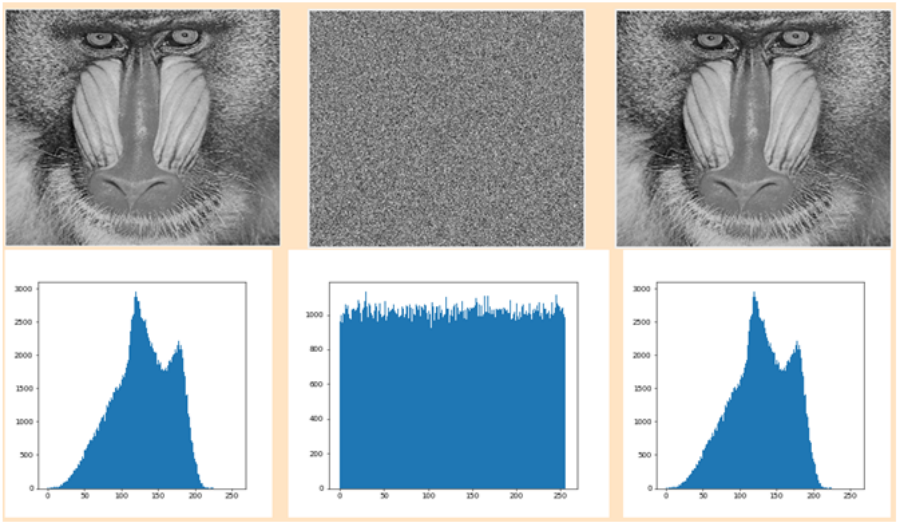
a1 **b1** **c1**



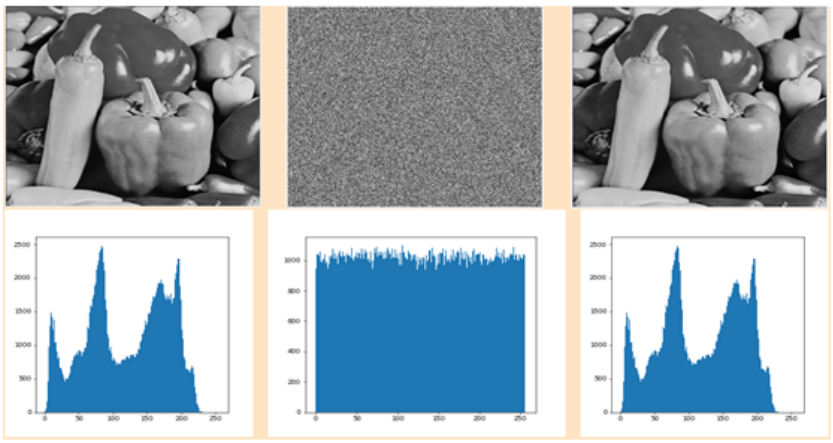
a2 **b2** **c2**



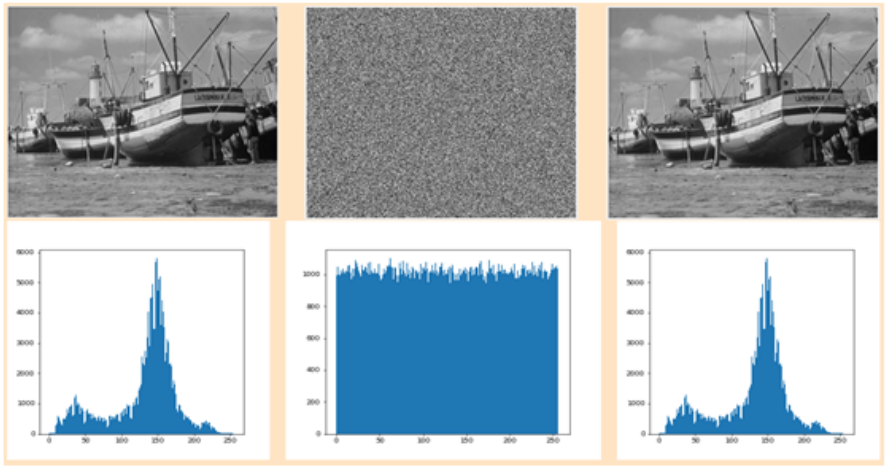
a3 **b3** **c3**



a4 **b4** **c4**



a5 **b5** **c5**



a6 **b6** **c6**

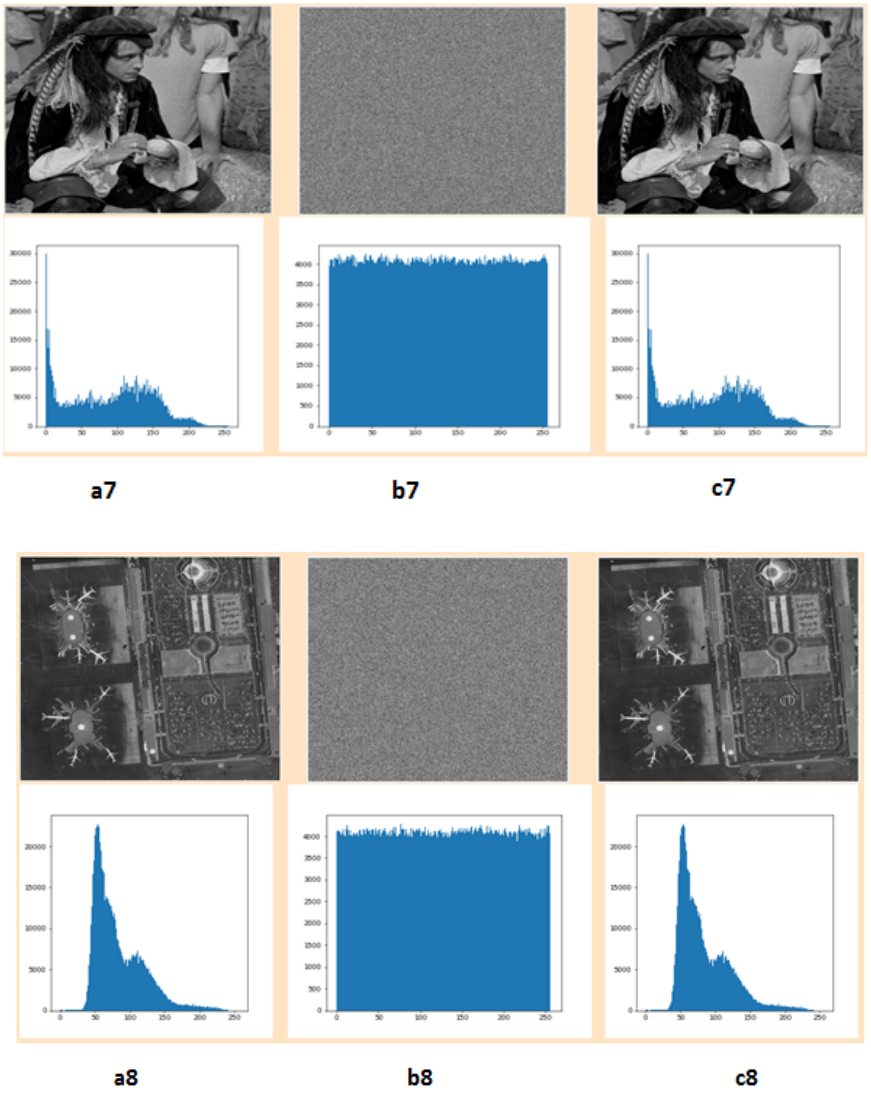


FIGURE 3.13 – Résultats d'analyse d'histogrammes : (a) image original ,(b)Image cryptée , (c) image décryptée .

Nous pouvons clairement remarquer que l'histogramme des images cryptées a une distribution uniforme des valeurs de pixels (tous les pixels ont la même chance d'apparition), ceci prouve que le cyrptage n'est pas vulnérable à l'attaque d'histogramme.

3.4.3.3 Corrélation

Pour tester la corrélation2.7 , nous avons sélectionné au hasard 10000 pair de deux pixels adjacents horizontalement , verticalement et diagonalement d'une image simple et cryptée , Le tableau 3.4 montrant les corrélations des images claires et leurs chiffrées en utilisant le schéma de cryptage .

Direction	Horizontal		Vertical		Diagonal	
Image	claire	cryptée	claire	cryptée	claire	cryptée
Lenna	0.9698	-0.0067	0.9852	-0.0059	0.95708	0.0139
Clock	0.9537	0.00103	0.97432	0.01292	0.93689	0.0023
Cameraman	0.9332	0.00083	0.9563	-0.0015	0.90516	0.0068
baboon	0.9305	-0.0099	0.9001	0.0002	0.8672	0.00705
Peppers	0.9605	-0.0074	0.9666	0.0026	0.9379	0.01317
Fishing Boat	0.9365	-0.015	0.9719	-0.0129	0.9271	0.0039
Male	0.9762	0.00409	0.9815	-0.01432	0.9669	0.0079

TABLE 3.4 – Coefficients de Corrélation des images en clair et cryptée

Nous pouvons clairement remarquer que les valeurs des coefficients de corrélation sont proches de 1, cela signifie que les images en clair sont fortement corrélées. Cependant les valeurs des coefficients de corrélation des images cryptées sont proches de 0, cela signifie qu'il n'existe aucune corrélation entre les pixels.

Graphiquement, la corrélation dans différentes directions de l'image "Fishing Boat" en clair et sa correspondante cryptée sont illustrées dans la figure 3.14 suivante :

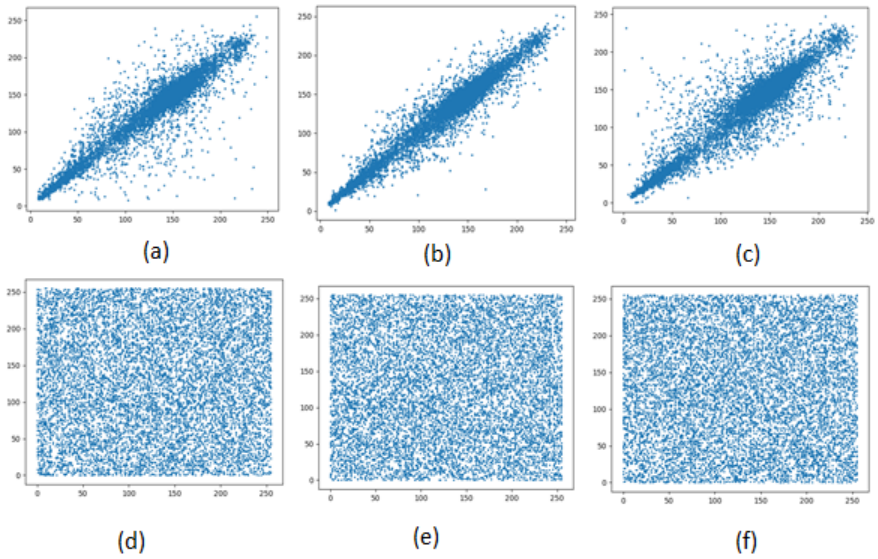


FIGURE 3.14 – (a) Direction horizontale de l'image simple (b) Direction verticale de l'image simple (c) Direction diagonale de l'image simple (d) Direction horizontale de l'image cryptée (e) Direction verticale de l'image crypté (f) Sens diagonal de l'image crypté.

Les résultats indiquent que ce schéma de cryptage peut éliminer efficacement la corrélation entre les pixels voisins dans une image d'entrée.

3.4.3.4 Entropie :

Comme on peut le voir sur le tableau 3.5, les entropies de toutes les images cryptées de sortie sont pratiquement égales à la valeur théorique de 8. Les résultats ci-dessous démontrent que le schéma est sécurisé contre l'analyse statistique.

Image	Entropy	
	Image original	Image cryptée
Clock	6.7056	7.9971
Cameraman	7.0097	7.9973
Airplane	6.4522	7.9973
Moon surface	6.7093	7.9974
Baboon	7.2925	7.9992
Peppers	7.6387	7.9992
Fishing Boat	7.1913	7.9993
couple	7.2010	7.9994
Male	7.5237	7.9998
airport	6.8303	7.9998

TABLE 3.5 – Entropie Des images Originales et Cryptées

3.4.3.5 Sensitivité de la clé

Pour évaluer la propriété de sensibilité clé de schéma , plusieurs image claires ont été d'abord cryptée à l'aide de clé secrète , puis on crypte les mêmes images claires en utilisant les clés (a) et (b), Les résultats sont récapitulés dans le tableau3.6 .

Les paramètres initiaux sont :$x_0 = 0.5842$,$y_0 = 0.2159$, p = 0.3 , r =3.999.

les changements sont comme suit :

(a) : $x_0 = 0.58420001$, $y_0 = 0.2159$.

(b) : $x_0 = 0.5842$,$y_0 = 0.21590001$.

Image	(a)		(b)	
	NPCR	UACI	NPCR	UACI
Clock	99.59	33.58	99.56	33.52
Airplane	99.59	33.40	99.56	33.49
Peppers	99.60	33.43	99.59	33.44
Male	99.61	33.48	99.60	33.47

TABLE 3.6 – les valeurs de NPCR et UACI.

En suite les image cryptées avec la clé secrète original ont été décryptées à l'aide des clés (a),(b) figure3.15 et 3.16 illustre le résultat de ce test sur les deux images 'Clock' et 'Peppers'.

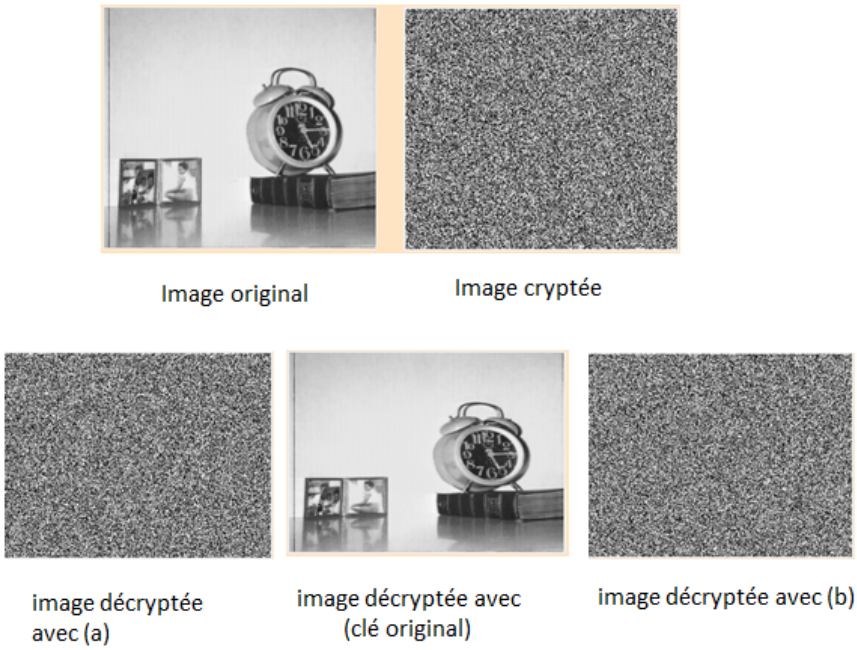


FIGURE 3.15 – Sensibilité de la clé en utilisant les différents paramètres en décryptage pour image 'Clock' .

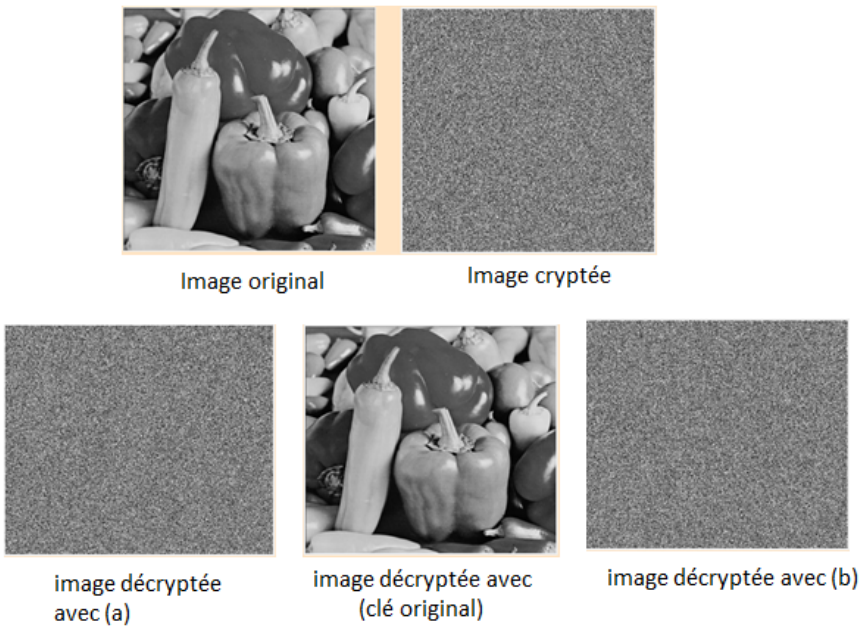


FIGURE 3.16 – Sensibilité de la clé en utilisant les différents paramètres en décryptage pour image 'Peppers' .

à partir de laquelle nous pouvons voir qu'un espion ne peut obtenir aucune information sur l'image en clair, même en utilisant une clé de déchiffrement presque parfaitement devinée, On peut donc conclure que cet schéma satisfait pleinement à l'exigence de sensibilité de la clé.

3.4.3.6 Analyse du temps

Pour tester la vitesse d'exécution de notre schéma de cryptage, on va calculer le temps de cryptage de plusieurs images de tailles différente (cameraman (256×256) ,lenna (512×512) , male (1024x1024) ,le schéma est effectué sur ces images. Spécifications de l'ordinateur portable utilisé pour effectuer cette expérience sont décrites on sous-section (3.4.1). Les résultats de cette l'analyse (en second) sont présentés dans le tableau 3.7 :

Taille des images	Cryptage (s)	Décryptage (s)
256 ×256	0.258402	0.384202
512 × 512	0.84942	0.71950
1024 × 1024	3.92548	4.058421

TABLE 3.7 – Analyse du temps de chaque taille.

Le résultat montre que l'augmentation de la taille de l'image signifie que le temps de calcul augmente également.

3.5 Étude comparative

Dans cette étude, Nous comparons notre schéma de cryptage avec les autres techniques de cryptage , qui ont été proposé par d'autres chercheurs dans le domaine de cryptage des images [77] [78] [79] [80] [81].

3.5.1 Comparaison espace de clé

le Tableau 3.8 récapitule l'espace clé de notre schéma de cryptage proposé et les quatre autres algorithmes de cryptage.

Référence	Notre schéma	[77]	[81]	[78]
Espace de clé	2^{253}	2^{128}	2^{144}	2^{504}

TABLE 3.8 – Comparaison d'espace de clé de différents algorithmes de chiffrement

Bien que notre schéma ne consiste pas en une étape de confusion, il est clairement comparable aux méthodes proposées dans [77] [81] [78]

3.5.2 Comparaison de corrélation

Le tableau 3.9 montrant la comparaison entre le schéma de cryptage proposé et les deux autres algorithmes de cryptage, utilisée dans cette comparaison c'est la corrélation(horizontal, vertical et diagonal) .

I :image, P :pepper, B :baboon, L :lenna, FB :fishing boat, M :moyen

	Notre schéma			[77]			[78]		
I	H	V	D	H	V	D	H	V	D
P	-0.0074	0.0026	0.0131	9.4483	0.0014	0.0020	0.0015	0.0007	0.0002
B	-0.0099	0.0002	0.00705	0.0027	0.0013	-5.4562	-	-	-
L	-0.0067	-0.0059	0.0139	7.4248	-7.5330	9.1292	0.0009	0.0027	-0.0005
FB	-0.0151	-0.0129	0.0039	-	-	-	0.0077	0.0008	0.0008
M	-0.0080	-0.0010	0.011349	0.000649	0.0006489	0.000789	-	-	-
	0.0098	-0.0055	0.0103	-	-	-	0.0033	0.001453	0.00015

TABLE 3.9 – Comparaison de corrélation de différents algorithmes de chiffrement

nous remarquons que la valeur de corrélation des méthodes [77] [78] est inférieure à notre du fait de la non existence d'étape de confusion dans notre schéma de cryptage.

3.5.3 Comparaison d'entropie

le tableau3.10 montrant la comparaison entre notre schéma de cryptage et les deux autres algorithmes de cryptage, utilisée dans cette comparaison c'est l'entropie .

Image	Notre schéma	[79]	[80]
Moon surface	7.9974	7.9974	7.9975
Airplain	7.9973	7.9974	7.9972
Couple	7.9994	7.9993	7.9993
Fishing Boat	7.9993	7.9993	7.9993
Male	7.9998	7.9998	7.9998
Airport	7.9998	7.9998	7.9998
Moyen	7.99883	7.99883	7.99881

TABLE 3.10 – Comparaison d'entropie de différents algorithmes de chiffrement

À partir les résultats de tableau 3.10 on remarque que de la valeur moyenne d'entropie de notre schéma est supérieure de celle proposé dans [80] , et on égalité avec un travail récent [79].

3.6 conclusion

Dans ce chapitre, nous avons présenté notre nouvelle Génération d'une séquence pseudo aléatoire qui se base sur la fonction logistique et la fonction pwlcm , Ensuite pour prouver la haute sécurité de notre proposition certaines analyses sur la séquence ont été effectués : les résultats de tableau NIST signifie que la séquence obtenue est aléatoire , aussi on a montré que la sensibilité de la Séquence proposée aux valeurs initiales est très notable,finalement notre Séquence est déterministe car on a utilisé des cartes chaotiques. On conclue que notre Séquence est déterministe , aléatoire et sensible aux conditions initiales qui démontre que la séquence proposée est adapté pour l'utilisation en cryptographie,

À la fin , nous avons Crypté des images numériques en se basant toujours sur la séquence proposée. Les résultats expérimentaux ont montré que le chiffrement possède un grand espace de clés et une sécurité de haut niveau. De plus, les comparaisons avec les schémas de chiffrement d'image existants qui ont été réalisées, montrent que la séquence proposé offre des performances très favorables.

Le chapitre suivant, sera consacré à l'explication des différents étapes suivis pour la réalisation de notre crypto-système proposé, ainsi tous les métriques sur lesquelles nous nous sommes appuyés pour arriver à une explication précise et détaillée de cryptage proposé.

CHAPITRE 4

CRYPTO-SYSTÈME PROPOSÉ

4.1 introduction

En général, les données côté utilisateur contiennent à la fois des informations personnelles et des données confidentielles, en particulier des images. Il est donc essentiel de garantir la sécurité des images pour protéger les données des utilisateurs contre différentes attaques malveillantes, ainsi que pour garantir l'intégrité des données des utilisateurs et éviter la perte d'informations. Un moyen direct et évident de protéger les données médicales consiste à utiliser un algorithme de cryptage.

Dans ce chapitre nous allons d'expliquer notre algorithme de cryptage que nous avons proposé. Ce dernier est basé sur le concept de permutation et de diffusion pour le cryptage des images médicales.Pour implémenter notre Crypto-système proposé nous avons utilisé la carte chaotique Arnold et la séquence déjà présenté dans le chapitre précédent.

Enfin, on a fait une amélioration sur le crypto-système proposé, ce dernier est basée sur le concept de chiffrement salsa20 avec la Séquence proposée qui sont combinés avec d'autres cartes chaotiques.

Nous évaluons l'efficacité de notre système à travers divers tests qui sont effectué tel que (l'histogramme, la corrélation, l'entropie) et les tests différentiels tel que (UACI ,PNCR), l'espace de clés et la sensibilité de la clé .

4.2 Crypto système proposé

Dans cette section, nous proposons un nouveau crypto système pour la sécurisation des images médicales qui sont considérées comme des données particulières en raison de leurs qualités d'information. Le système de cryptage proposé est basé sur les principes de confusion/diffusion décrites dans le chapitre 2 (section 2.9).

Le processus de confusion est de réarranger les pixels de l'image sans faire des modifications de leurs valeurs, l'objectif principal de cette phase est de briser la forte corrélation entre les pixels, Dans notre système afin de perturber cette corrélation, nous adoptons la carte Arnold généralisé qui été mentionnée dans le chapitre 2 (sous-section 2.8.2) pour mélanger les positions des pixels de l'image Claire(P).

L'étape de diffusion consiste à masquer les pixels ordinaires par des nouvelles valeurs secrètes, Ce faisant, l'histogramme est rendu uniforme et significativement différent de celui de l'image simple, dans notre crypto système afin de dissimuler les valeurs original, nous utilisons la génération de séquence proposée dans chapitre3 (section 3.2).

4.3 Processus de cryptage

Le cryptage des données d'image médicale simples est effectué à l'aide de processus de Cryptage proposé ci-dessous :

— Charger une image médicale niveau de gris de taille (M x N).

— définir les contrôles des paramètres et nombre d'itérations pour la carte d'Arnold généralisée (a, b, R).

— Définir les valeurs des conditions initiales x0, y0 et contrôles de paramètres p, r de Séquence Proposée.

— On mélange les positions des pixels d'image d'entrée en appliquent la carte d'Arnold généraliser pour R itération afin d'obtenir Image brouillé (A).

— Générer une séquence pseudo aléatoire (S) à travers la génération de Séquence proposée, la longueur de séquence (S) égal à nombre des pixels d'image médical charger.

— Réarranger la séquence générer (S) en une matrice 2D (M).

— appliquer l'opération xor entre la matrice générer (M) et les pixels d'image médicale brouillé(A) pour obtenir une Image médicale Cryptée C.

Le mécanisme de Cryptage du Crypto système proposée est illustré comme suit dans la figure 4.1 :

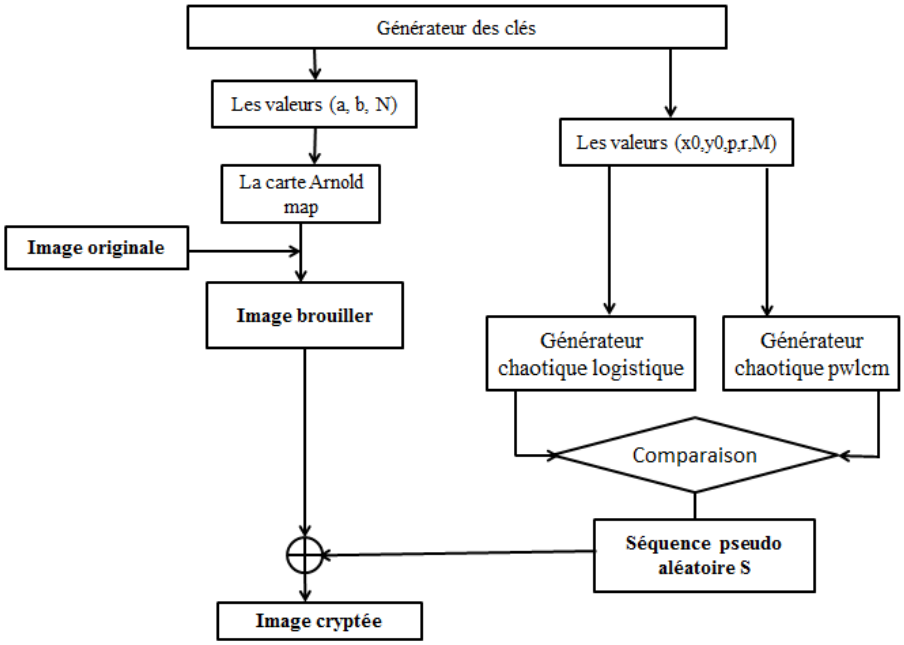


FIGURE 4.1 – Schéma de cryptage proposé .

4.4 Processus de décryptage :

Le processus de décryptage est similaire à Le processus de cryptage mais avec le fonctionnement inverse, et aussi la génération des clés doit être le même lorsque utilisé dans Le processus de cryptage, Les étapes de cet processus sont décrites ci-dessous :

— charger l'image C (image Cryptée) .

— Génération d'une séquence pseudo-aléatoire comme le cas de cryptage.

— Réarranger la séquence générer (S) en une matrice 2D (M).

— appliquer l'opération logique xor entre la matrice générer (M) et les pixels image Cryptée C pour obtenir Image brouillé(A) .

— Appliquer la fonction inverse de la carte d'Arnold généralisé sur l'image brouillé (A), pour d'obtenir une image en clair avec le nombre d'itération T .

La figure 4.2 ci-dessous montre le processus de décryptage.

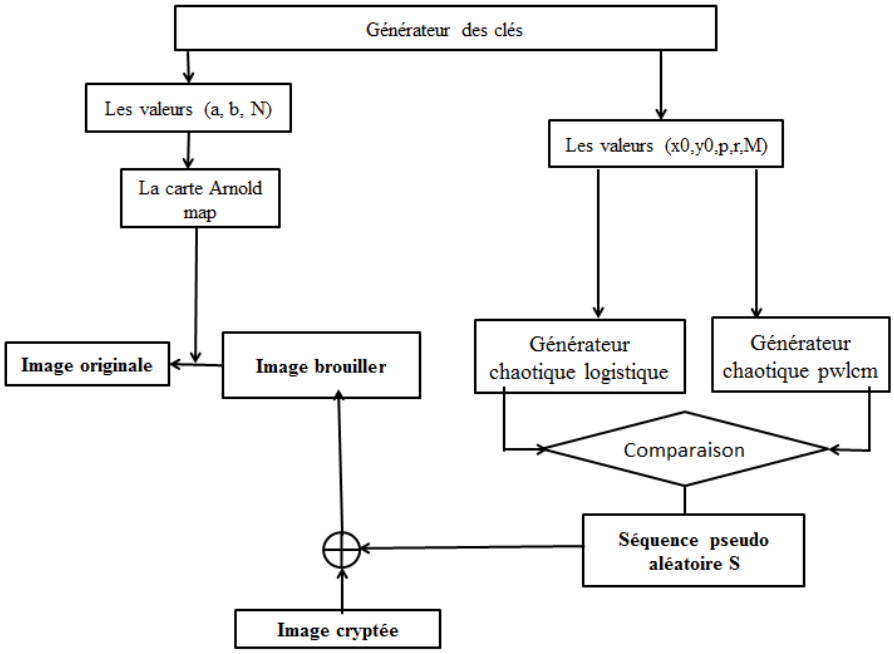


FIGURE 4.2 – schéma de décryptage proposé.

4.5 Implémentation de notre Système de cryptage chaotique des images médicales

nous avons appliqué notre algorithme sur les images médicales que sont notre objectif principal. Récemment, les images médicales ont été envoyées largement sur les réseaux et l'Internet et pour cela nous avons développé notre système essentiellement orienté vers les images médicales enregistrées en tant qu'images normales.

4.5.1 Langage de programmation

Pour le développement d'application de notre Crypto système proposé nous avons utilisé aussi le langage Python 3.8, les motivations sont mentionnées dans le chapitre 3 (sous-section3.4.1.1).

Les bibliothèques utilisées :(tkinter, PIL, numpy, matplotlib).

4.5.2 Résultats Expérimentaux

Un système de cryptage est un système qui résiste à tous types d'attaques. Nous discutons dans cette section les résultats de la sécurité et l'analyse des performances de notre système décrit précédemment.

Nous fixons les valeurs initiales et les paramètres de contrôle comme suit :

paramètres	a	b	x0	y0	r	p
Carte Arnold généralise	20	25	-	-	-	-
Séquence Proposée	-	-	0.5842	0.2159	3.999	0.3

TABLE 4.1 – Paramètres des fonctions chaotiques.

Nous présentons dans ce qui suit, les résultats obtenus de notre système de cryptage chaotique des images médicales basés sur la séquence proposée.

FIGURE 4.3 – Cryptage et décryptage d'image ct-kedney

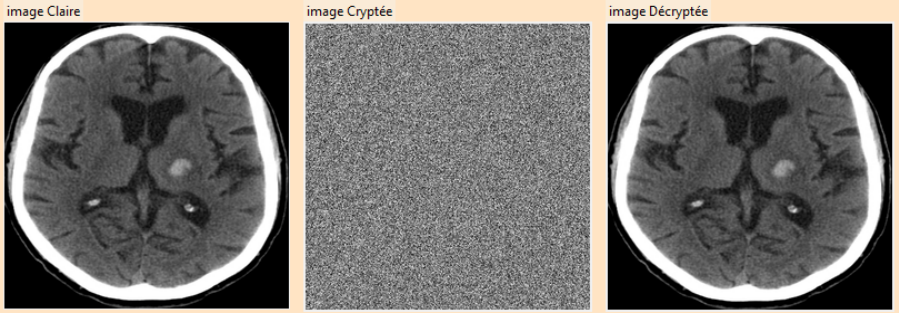


FIGURE 4.4 – Cryptage et décryptage d'image $head - ct$

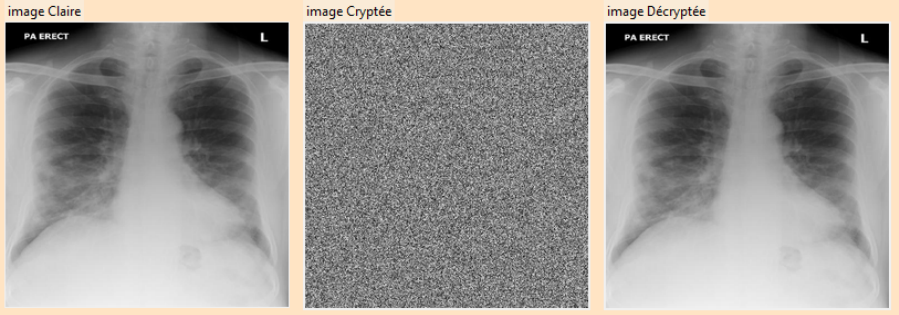


FIGURE 4.5 – Cryptage et décryptage d'image $chest - xray$

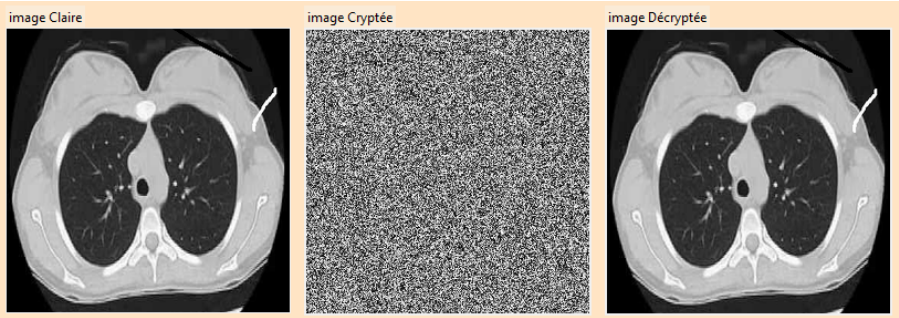


FIGURE 4.6 – Cryptage et décryptage d'image $ct - lung$

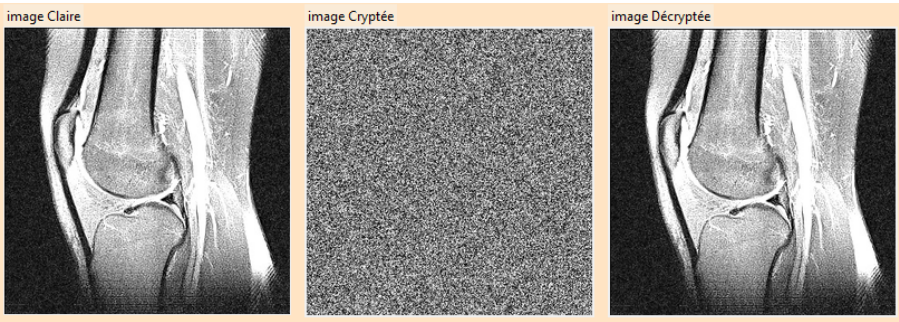


FIGURE 4.7 – Cryptage et décryptage d'image $knee - mri$

L'inspection visuelle des Figures 4.3 , 4.4 , 4.5 , 4.6 et 4.7 montres la possibilité d'appliquer avec succès le principe de diffusion de confusion proposée pour le cryptage d'image basé sur le chaos à la fois dans le cryptage et le décryptage. De plus, il révèle son efficacité à cacher les informations qu'ils contiennent.

4.6 Mesure d'évaluation

Un bon système de cryptage doit être protégé contre toutes les attaques possibles de n'importe quelle sorte, il y a donc un ensemble de mesures qui servent cet objectif. Nous allons présenter les plus important comme : l'espace de clés, l'histogramme, sensitivité de la clé, etc....

4.6.1 Analyse de l'espace de clé

Dans notre crypto système proposé les paramètres de la carte Arnold généralisé sont utilisés comme clé de permutation et les conditions initiales et les paramètres de la carte pwlcm et la carte logistique sont utilisés comme clé de substitution, et selon la formule 2.6 :

Permutation :les clés sont (a, b, N) donc : $k_1 = (2^8)^3 = 2^{24}$

Diffusion :les clés sont (x_0, p, y_0, r) donc : $K_2 = (1 \times 2^{64}) \times (1 \times 2^{64}) \times (0.5 \times 2^{64}) \times (0.432 \times 2^{64}) = 2^{253.8}$.

Alors : espace de clé = $k_1 \times K_2 = (2^{277.8})$

Cette valeur est plus grande que 2^{128}, cela prouve que notre système proposé est résistant aux attaques forces brutes.

4.6.2 Histogramme

L'analyse de l'histogramme est effectuée sur plusieurs images médicales est illustrée dans les figures ci-dessous :

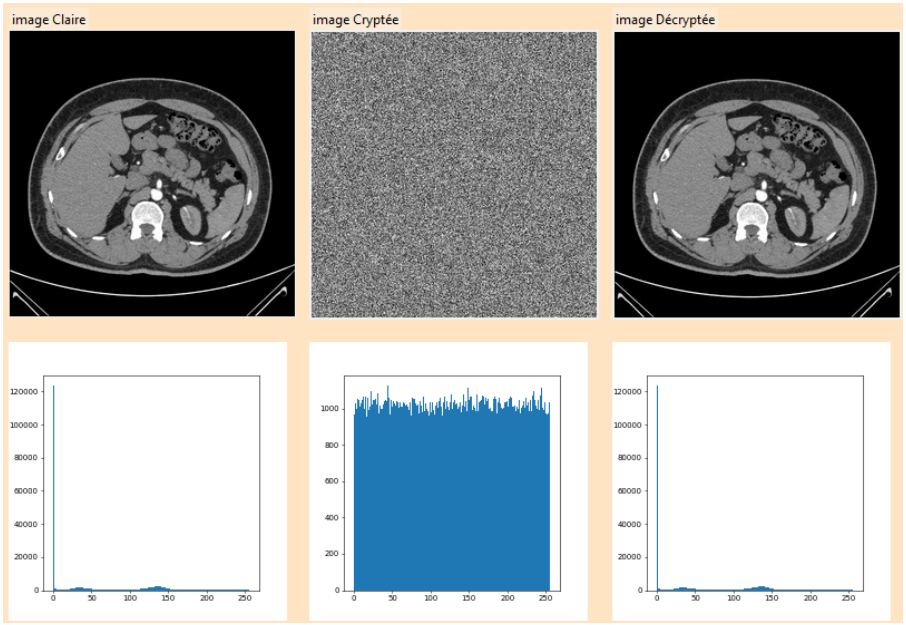


FIGURE 4.8 – Résultats d'analyse d'histogrammes d'image $ct - kedney$

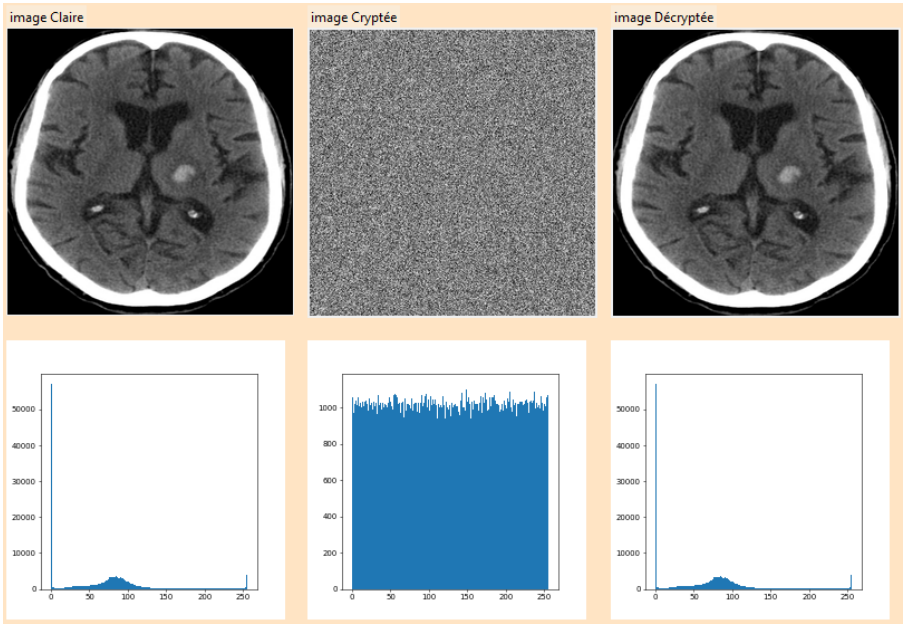


FIGURE 4.9 – Résultats d'analyse d'histogrammes d'image $head - ct$

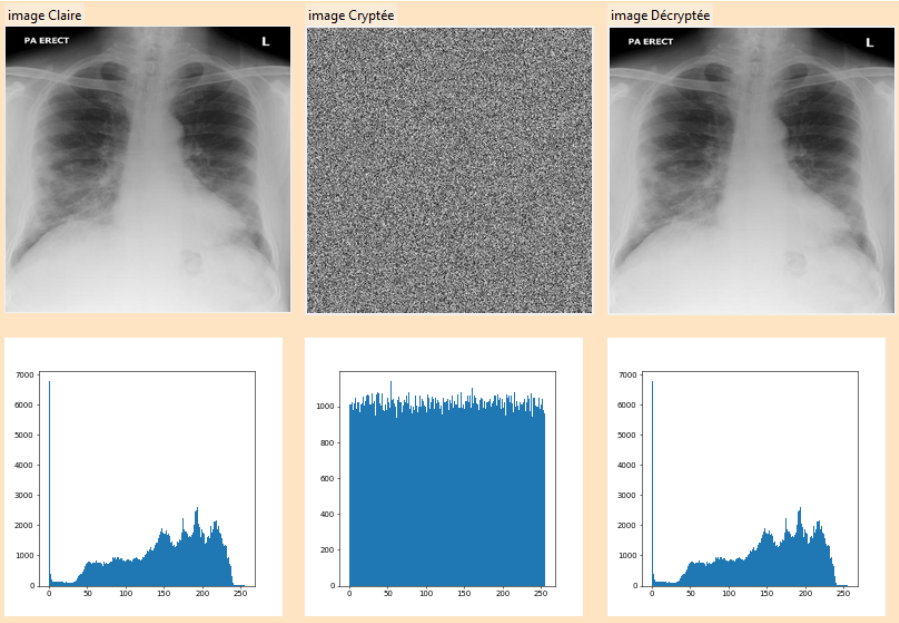


FIGURE 4.10 – Résultats d'analyse d'histogrammes d'image *chest – xray*

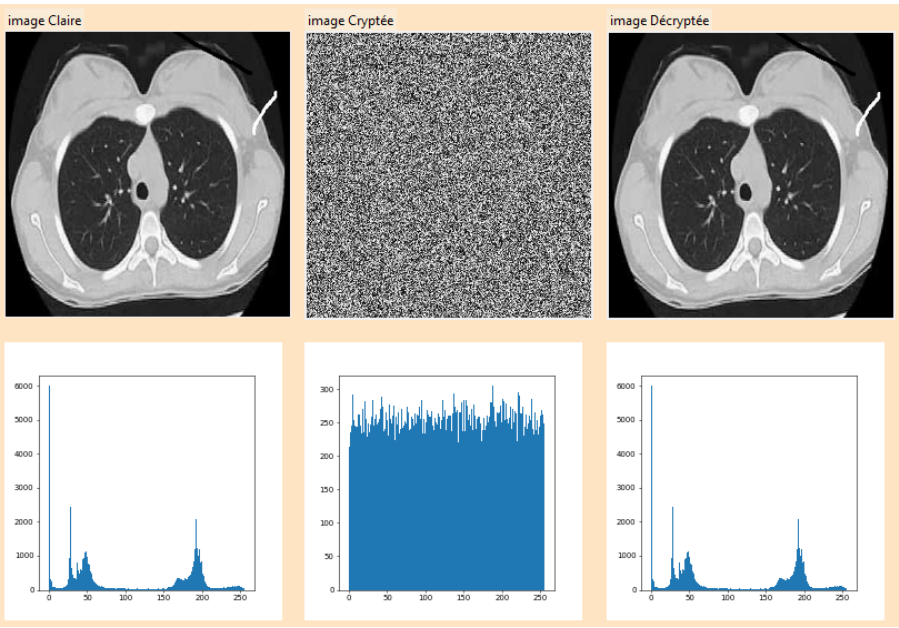


FIGURE 4.11 – Résultats d'analyse d'histogrammes d'image *ct – lung*

Les histogrammes des images cryptées illustrées sur les figures 4.8 , 4.9 , 4.10 , 4.11 et 4.12 Sont presque uniformes, ce qui suggère que le système proposé a pu sécuriser les données médicales sans divulguer aucune information sur les données sources, ce qui rend difficile pour les pirates de se procurer les données médicales sensibles.

De plus, les histogrammes des images décryptées présentées sont presque similaires aux histogrammes d'image d'origine, ce qui montre que le mécanisme proposé a pu récupérer les données médicales d'origine sans aucune modification significative ne soit apportée à l'image d'origine.

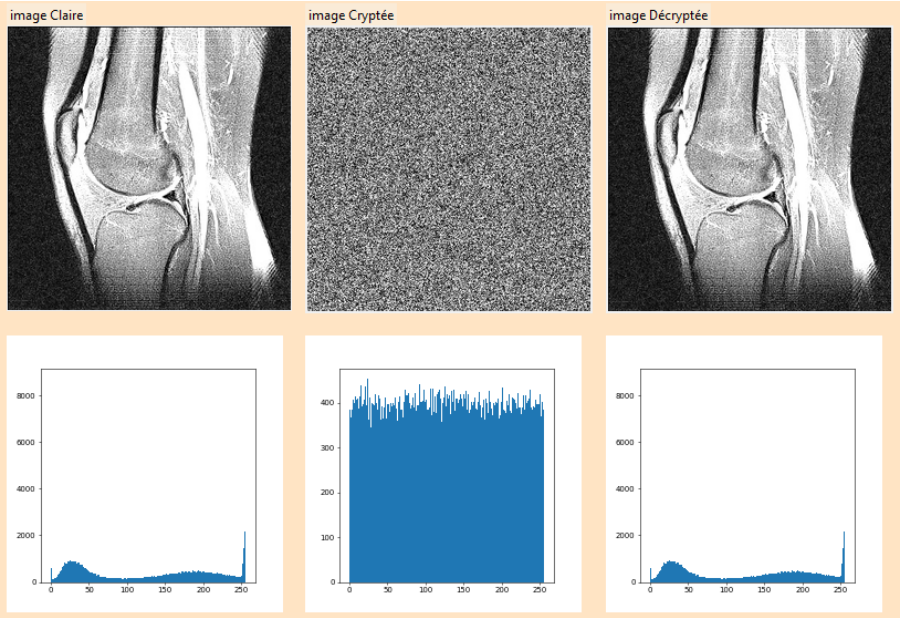


FIGURE 4.12 – Résultats d'analyse d'histogrammes d'image $knee - mri$

4.6.3 Corrélation

Cette analyse effectuée en suivant les procédures, Au hasard 10000 paires sont sélectionnées et elles sont sélectionnées comme adjacentes horizontalement, verticalement et en diagonale.La corrélation est calculée par le équation 2.7,Comme le montre le tableau 4.2 suivant :

Direction	Horizontal		Vertical		Diagonal	
Image	**claire**	**cryptée**	**claire**	**cryptée**	**claire**	**cryptée**
$C - kedney$	0.9773	0.00875	0.9538	0.0035	0.9426	- 0.0140
$Ct - head$	0.9914	-0.0046	0.9888	0.0024	0.9832	0.0022
$Chest - xray$	0.9961	0.0033	0.9846	-0.0063	0.9941	0.0078
$Mri - knee$	0.9049	-0.0021	0.9260	0.0088	0.8817	0.0107

TABLE 4.2 – Coefficients de Corrélation des images en clair et cryptée

Le tableau4.2 montre que Les valeurs de l'image simple sont presque égales à 1 car le la corrélation entre les pixels adjacents est élevée. Les valeurs d'image cryptées sont d'environ 0. La corrélation horizontale, verticale et diagonale des pixels dans l'image 'ct head' d'origine et la corrélation des pixels dans l'image 'head ct' cryptée sont illustrées à la figure4.13

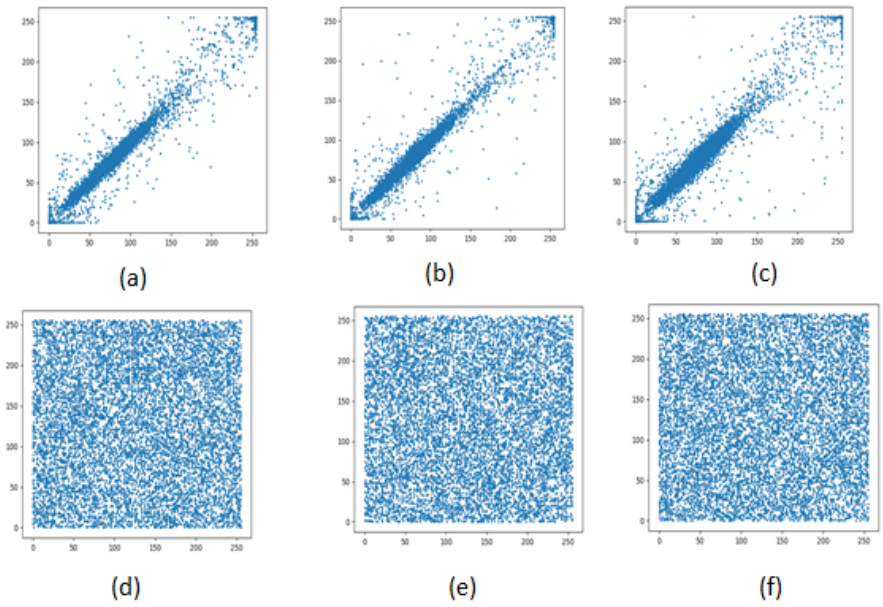


FIGURE 4.13 – (a) Direction horizontale de l'image simple (b) Direction verticale de l'image simple (c) Direction diagonale de l'image simple (d) Direction horizontale de l'image cryptée (e) Direction verticale de l'image cryptée (f) Sens diagonal de l'image cryptée pour l'image de test' head ct'

Les pixels de l'image Cryptée comme le montre la figure 4.13 (d) et (f) sont distribués et la corrélation entre eux est presque égale à zéro, ce qui suggère que le Crypto système proposé a réussi à rompre efficacement la corrélation entre les pixels de l'image originale (a)et (c) et à les disperser en sécurisant les données d'image médicale contre tout accès non autorisé.

4.6.4 Entropie

La valeur entropie de différentes images médicales selon notre crypto-système est décrite dans le tableau4.3 suivant :

Image	Taille	Entropie	
		Image original	Image cryptée
$Ct - kedney$	512× 512	4.8191	7.9992
$Ct - head$	512×512	6.0223	7.9993
$Chest - xray$	512×512	7.6166	7.9992
$Ct - lung$	256×256	6.7448	7.9972
$Mri - knee$	320×320	7.5121	7.9981

TABLE 4.3 – Entropie Des images Originales et Cryptées

Il est clair que toute les valeurs d'entropie de toutes les images cryptées sont proche de la valeur ideale 8.

4.6.5 Sensitivité de la clé

Pour évaluer la propriété de sensibilité clé de la proposition cryptages, plusieurs images médicales originals claires ont été d'abord crypté à l'aide de clé secrète (a=10,b=8,R=100,X_0 = 0.5842 , y_0 =0.2159 , p = 0.3 , r =3.999), puis on crypte les mêmes images claires en utilisant les clés (a) , (b) et (c), Les résultats sont récapitulés dans le tableau 4.4.

Les changements sont comme suit :

(a) : (a= 10, b=8, R=100, X_0 = 0.58420001 , y_0 =0.2159 , p = 0.3, r =3.999).

(b) : (a= 10,b=8, R=100, X_0 = 0.5842 , y_0=0.21590001 , p = 0.3 , r =3.999).

(c) : (a= 10, b=8, R=101, X_0 = 0.5842 , y_0 =0.2159 , p = 0.3, r =3.999).

Image	Taille	(a)		(b)		(c)	
		NPCR	UACI	NPCR	UACI	NPCR	UACI
$Ct - kedney$	512×512	99.60	33.45	99.59	33.49	77.75	23,13
$Ct - head$	512×512	99.60	33.49	99.59	33.53	94.12	24.97
$Chest - xray$	512×512	99.60	33.49	99.59	33.48	99.44	31.02

TABLE 4.4 – les valeurs de NPCR et UACI

En suite les image médicales cryptées avec la clé secrète original ont été décryptées à l'aide des clés de décryptage suivantes (a1),(b1) et(c1) :

(a1) : (a= 10, b=8, T=156, X_0= 0.58420001 , y_0 =0.2159 , p = 0.3, r =3.999).

(b1) : (a= 10,b=8, T=156 X_0 = 0.5842 ,y_0=0.21590001 , p = 0.3 , r =3.999).

(c1) : (a= 10, b=8, T=155,X_0 = 0.5842 , y_0 =0.2159 , p = 0.3, r =3.999).

les figures 4.14 et 4.15 illustres les résultats de ce test sur les deux images 'ct kedney' et'chest xray'.

Les exemples ci-dessous montrent que de légères modifications des clés de cryptage de notre schéma (ou leurs ordres à n'importe quelle position) produisent une sortie semblable à du bruit et protègent ainsi les images originales de la récupération par des utilisateurs autorisés. Cela met en évidence l'efficacité de notre crypto système et sa haute sensibilité.

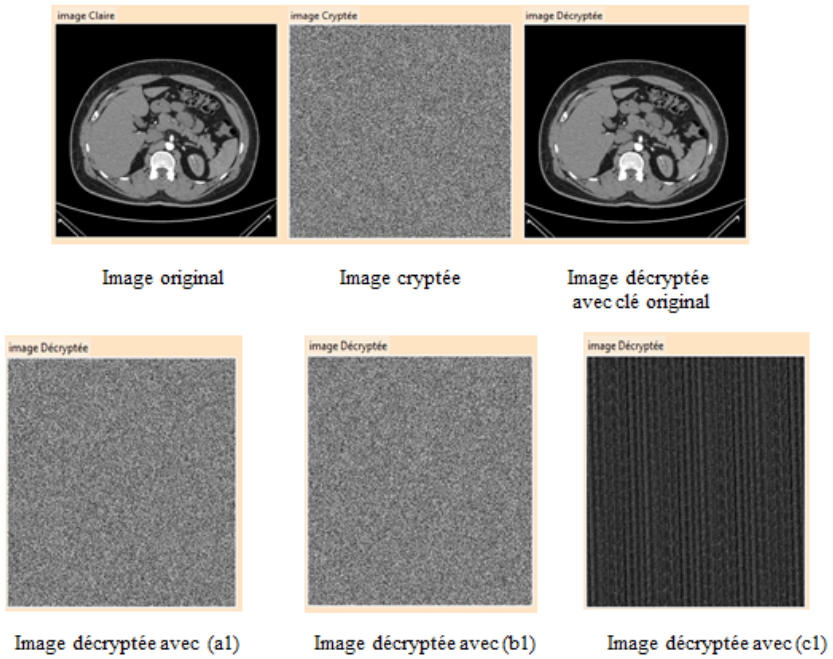


FIGURE 4.14 – Sensibilité de la clé en utilisant les différents paramètres en décryptage pour image 'ct-kedney'

.

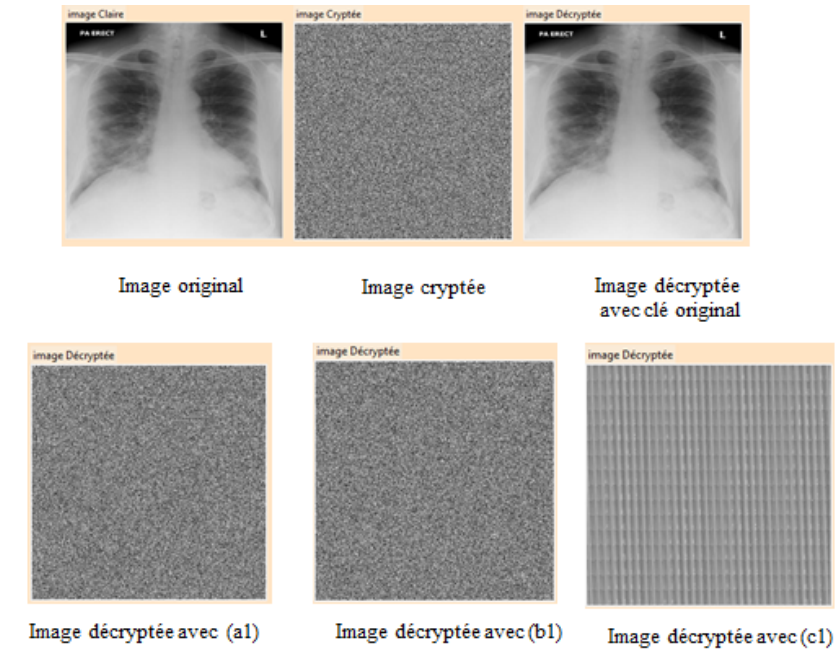


FIGURE 4.15 – Sensibilité de la clé en utilisant les différents paramètres en décryptage pour image 'chest-xray'

.

4.6.6 Ssim et Psnr

Le tableau affiche les valeurs SSIM et PSNR pour l'image en échelle médicale cryptée par rapport à l'image originale d'origine :

Images	Ct kedney	Chest xray	Head ct	Mri knee	Ct lung
Ssim	0.0044	0.009	0.0069	0.0046	0.0067
Psnr	6.27	8.32	6.98	6.98	7.159

TABLE 4.5 – les valeurs de Ssim et Psnr

Selon les résultats du tableau 4.5 , on peut remarquer que les valeurs ssim obtenues à partir de la technique proposée sont presque égales à zéro , et valeurs psnr sont faibles, Ce qui indique que l'image originale et cryptée ne sont pas similaires.

4.6.7 Attaques de bruit

Dans les applications du monde réel, les images numériques sont transmises via un canal de communication qui est généralement soumis à un bruit de canal. Pour Analyser l'immunité au bruit de système proposé basé sur séquence proposée Le bruit de gaussien a été utilisé pour attaquer les images cryptées avec une variance de 0,01 et 0,1.
Le tableau4.6 montre les valeurs de MSE et du PSNR entre image décryptée sans attaque de bruit et les images décryptées sous attaques de bruit de gaussien avec les deux valeurs de variance .

Bruit gaussien	Psnr/Mse	kedney	Mri knee	Ct head
variance = 0,01 moyenne = 0	Psnr	26.02	27.715	27.63
	Mse	162.20	110.04	112.114
variance = 0,1 moyenne = 0	Psnr	26.02	27.81	27.58
	Mse	162.557	108.08	113.311

TABLE 4.6 – les valeurs psnr et mse

La figure 4.16 illustre l'effet de décryptage du l'image de ct kedney après avoir été soumise à l'attaque de bruit de gaussien.

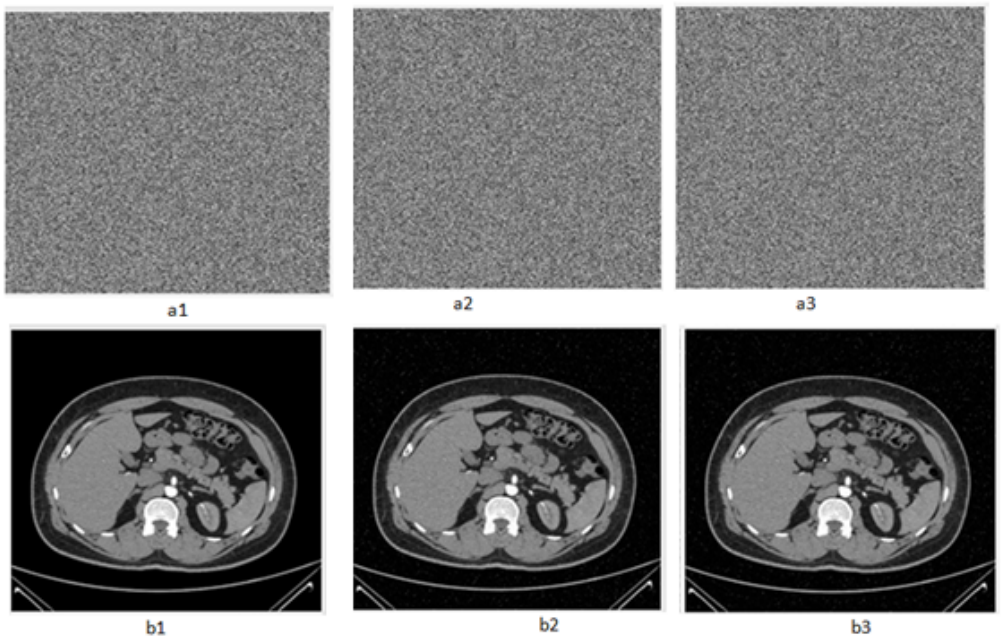


FIGURE 4.16 –) (a1) est image cryptée original et (b1)image décryptée sans les attaques de bruit, (a1) image cryptée sous attaques avec variance de 0.01 et (b2)image décryptée avec variance de 0.01 ,(a3) image cryptée sous attaques avec variance de 0.1 et (b3)image décryptée avec variance de 0.1.

Comme on peut le voir sur la figure 4.16 (b2) et (b3), les images décryptées sous attaque gaussienne sont visibles ce qui démontre que l'algorithme proposé est résistant aux attaques de bruit

4.6.8 Analyse de temps

La consommation de temps de système proposé est principalement généré par la carte Arnold, et à mesure que la taille de l'image devient plus grande, le temps pour la carte Arnold est également plus long ,Spécifications de l'ordinateur portable utilisé pour effectuer cette expérience sont décrites on (sous-section3.4.1.1), Les tests de temps sont effectués sur chaque image de taille différente (head ct (512×512),knee mri(320 ×320) et ct lung (256×256)),Les résultats du test de temps sont présentés dans le tableau 4.7 suivant :

Image	Cryptage(s)	Décryptage(s)
256×256	7.33326	5.09709
320×320	11.3326	12.0723
512×512	37.1670	57.033

TABLE 4.7 – Analyse du temps

Mais d'après les résultats de test Le temps de calcul est acceptable sur le déroulement de l'algorithme de cryptage/ décryptage. Donc on a des possibilités de résister à des tentatives d'attaques.

4.7 Une amélioration dans le crypto-système proposé en utilisant la méthode salsa20

D'autre part, en plus du système proposé que nous avons déjà implémenté, nous proposons un nouveau schéma de chiffrement chaotique qui inclut des améliorations au cryptosystème proposé. Le but de cette amélioration est de supprimer la faiblesse de l'algorithme Salsa20, car il contient des entrées à poids fixe, utilisant ainsi la séquence chaotique proposée comme clé pour générer un flux de clés suffisamment fort et suffisamment aléatoire pour être imprévisible par un attaquant.
Pour cela, Dans cette section, nous allons besoin d'examiner la fonction de cryptage Salsa20.

4.7.1 Fonction de cryptage Salsa20

Salsa 20 est un chiffrement de flux proposé par Bernstein. Ce chiffrement est conçu sur la base d'une addition 32 bits (XOR), et d'opérations de rotation. L'algorithme a une clé (séquence proposé) de 256 bits, un nonce de 64 bits, une position de flux de 64 bits et quatre constantes d'une sortie de 32 à 512 bits (flux de clé). [82]

constantes 1	clé 1	clé 2	clé 3
clé 4	constantes 2	nonce 1	nonce 2
position 1	position 2	constantes 3	clé 5
clé 6	clé 7	clé 8	constantes 4

TABLE 4.8 – l'état initial de la méthode salsa 20

Une fonction de hachage d'une entrée de 64 octets et d'une sortie de 64 octets est au cœur de Salsa20, qui est un chiffrement de flux qui fonctionne en mode compteur. Un flux de clé de 64 octets est produit en hachant la clé, le nonce et le compteur de blocs et le résultat est l'opération XOR avec un texte en clair de 64 octets.
La fonction de hachage Salsa20 invoque ce qu'on appelle une fonction quart.

La figure 4.17 montre le quart de fonction Salsa20.

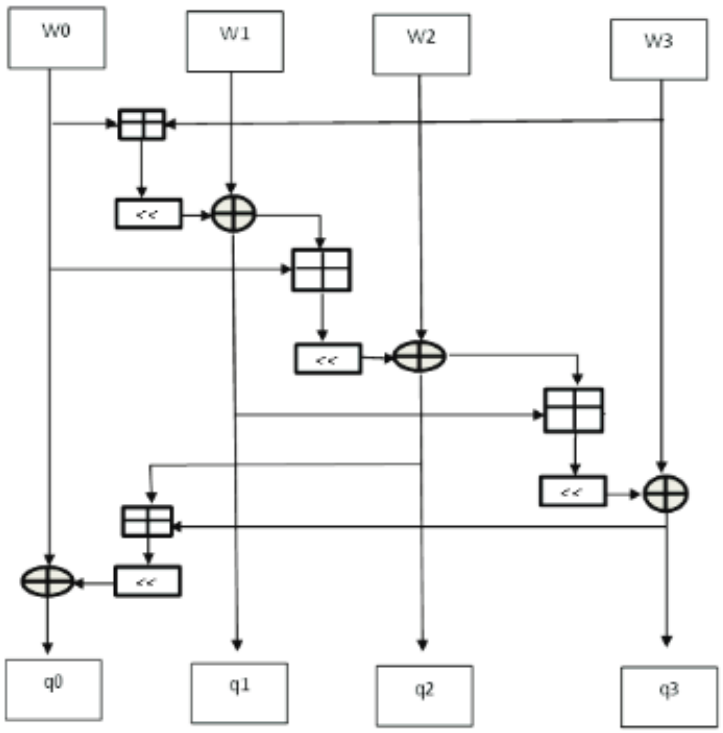


FIGURE 4.17 – Diagramme en quart de rond [82]

La fonction quart de rond peut être représentée mathématiquement par les équations suivantes :

$$q_0 = w_1 \oplus ((w_0 + w_3) \ll 7) \tag{4.1}$$

$$q_1 = w_2 \oplus ((w_1 + w_0) \ll 9) \tag{4.2}$$

$$q_2 = w_3 \oplus ((w_2 + w_1) \ll 13) \tag{4.3}$$

$$q_3 = w_0 \oplus ((w_3 + w_3) \ll 18) \tag{4.4}$$

4.7.2 Cryptage salsa 20

— Charger une image médicale niveau de gris de taille (M x N).

— définir les contrôles des paramètres et nombre d'itérations pour la carte d'Arnold généralisée (a, b, r).

— Définir les valeurs des conditions initiales x0, y0 et contrôles de paramètres p, r de Séquence Proposée.

— On mélange les positions des pixels d'image d'entrée en appliquent la carte d'Arnold généraliser pour R itération afin d'obtenir Image brouillé (A).

— Faire Une séquence d'opérations mathématiques est mise en œuvre pour générer un séquence chaotique décrites dans le chapitre précédent (section 1).

— Appliquer le principe l'algorithme Salsa20 pour générer un ensemble de flux pseudo-aléatoires de 64 octets appelés flux de clés, de longueur égale à la taille de la matrice d'image.

— Appliquer l'opérateur logique XOR entre chaque bloc de 64 octets de flux pseudo-aléatoires et chaque bloc de 64 octets de l'image brouillé (A).

4.7.3 Décryptage salsa 20

L'algorithme est symétrique, donc les mêmes étapes doivent être utilisées à l'envers pour les étapes de décryptage .La sortie de l'algorithme salsa 20 Xored avec des blocs de l'image cryptée pour produire les 64 octets de l'image en claire.

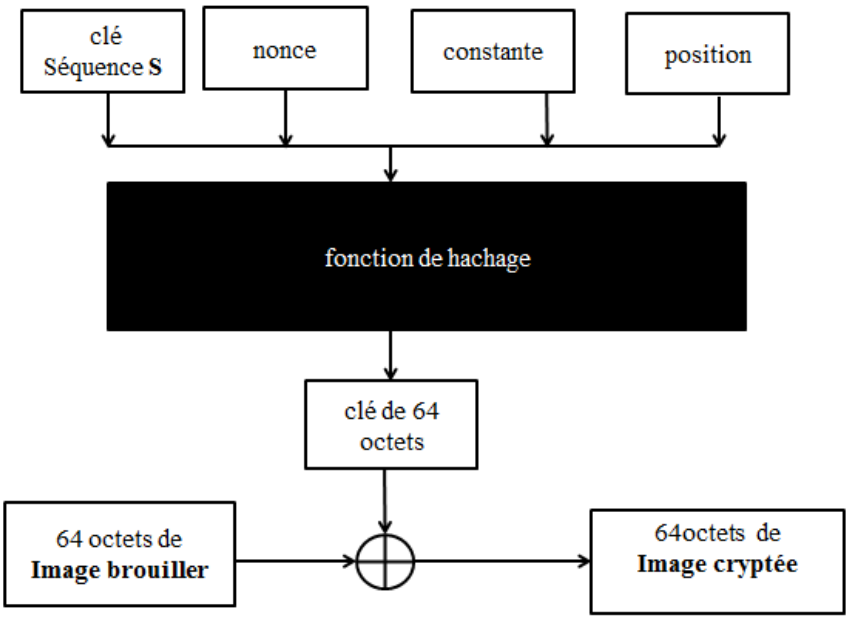


FIGURE 4.18 – Principe générale de l'algorithme de chiffrement salsa 20.

Le principe de confusion-diffusion est : (la carte sélectionnée pour la confusion) et (salsa 20 pour la diffusion) est illustré dans la Figure 4.19 suivante :

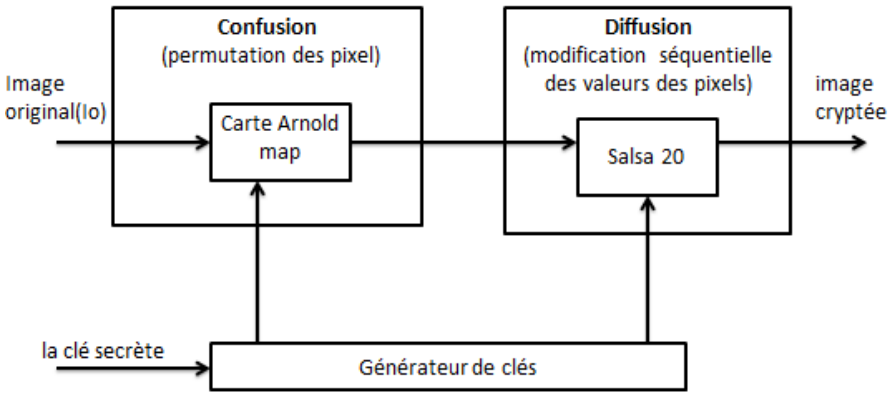


FIGURE 4.19 – Le processus de cryptage.

4.8 Analyse de crypto système chaotique (cartes chaotiques arnold map /chiffrement de salsa 20)

Pour l'efficacité de cet amélioration, e cryptage l'image ne doit pas montrer d'informations visuelles. les figures 4.20 , 4.21 , 4.22 , 4.23 et 4.24 répertorie les résultats de l'application des méthodes proposées de tests d'images médical en niveau de gris, qui ont différentes taille, Les images extraites sont également expliquées visuellement par rapport à l'image d'origine.

Nous fixons les valeurs initiales et les paramètres de contrôle comme suit :

Carte Arnold généralise

a=10,b=8 ,N=116 pour les images de taille (512×512)

a=10,b=8 ,N=75 pour les images de taille (256×256) et (320×320) .

Génération de Séquence Proposée X_0 = 0.6141, p=0.31, y_0=0.5487, r=3.999.

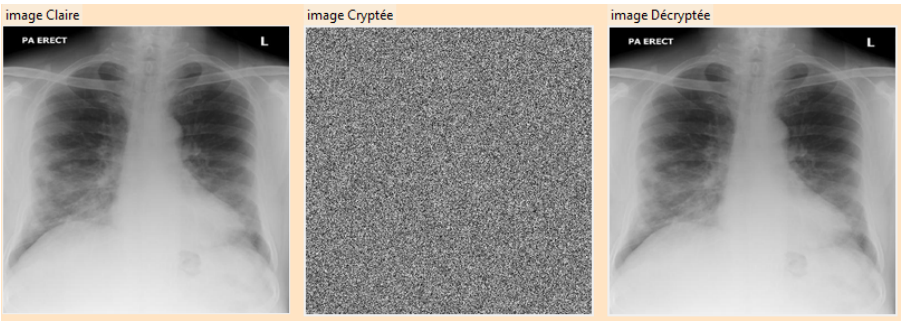


FIGURE 4.20 – Cryptage et décryptage d'image $chest - xray$ par salsa 20

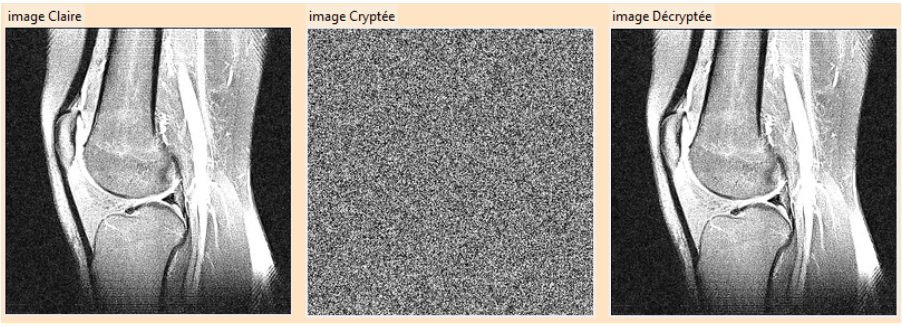


FIGURE 4.21 – Cryptage et décryptage d'image $knee - mri$ par salsa 20

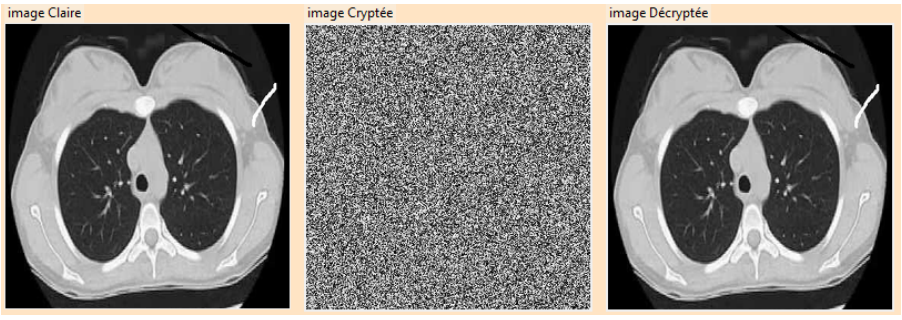


FIGURE 4.22 – Cryptage et décryptage d'image par $ct - lung$ salsa 20

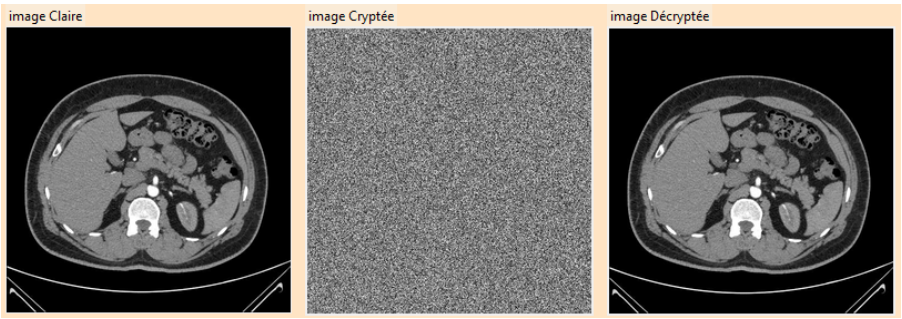


FIGURE 4.23 – Cryptage et décryptage d'image $ct - kedney$ par salsa 20

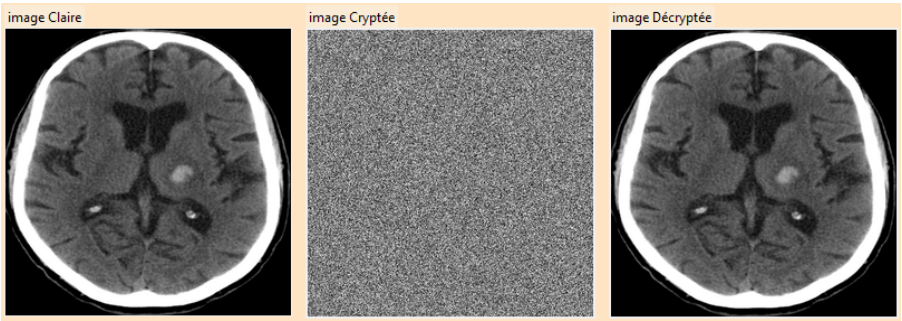


FIGURE 4.24 – Cryptage et décryptage d'image $head - ct$par salsa 20

4.8.1 Analyse de l'espace de clé

Dans notre système basé sur salsa20 les paramètres de la carte Arnold généralisé sont utilisés comme clé de permutation et dans l'étape de substitution la méthode Salsa20 utilise la fonction

de hachage en mode compteur. Il a un état de 512 bits et est initialisé en y copiant une clé de 256 bits, dans notre cas les conditions initiales et les paramètres de la carte pwlcm et la carte logistique sont utilisés comme la clé. Un nonce et un compteur de 64 bits et une constante de 128 bits.

Permutation :les clés sont (a, b, N) donc : $k_1 = (2^8)^3 = 2^{24}$

Diffusion :les clés sont (clé, compteur) donc : $K_2 = (2^{256}) \times (2^{64}) = 2^{320}$.

Alors : espace de clé = $k_1 \times K_2 = (2^{344})$

Apparemment, l'espace clé est assez grand pour résister à tous types d'attaques par force brute.

4.8.2 Histogramme :

plusieurs images médicales de tests ont été utilisé dans l'analyse . Les tracés des histogrammes des images claires et les images cryptée sont montrés dans les figures ci dessous :

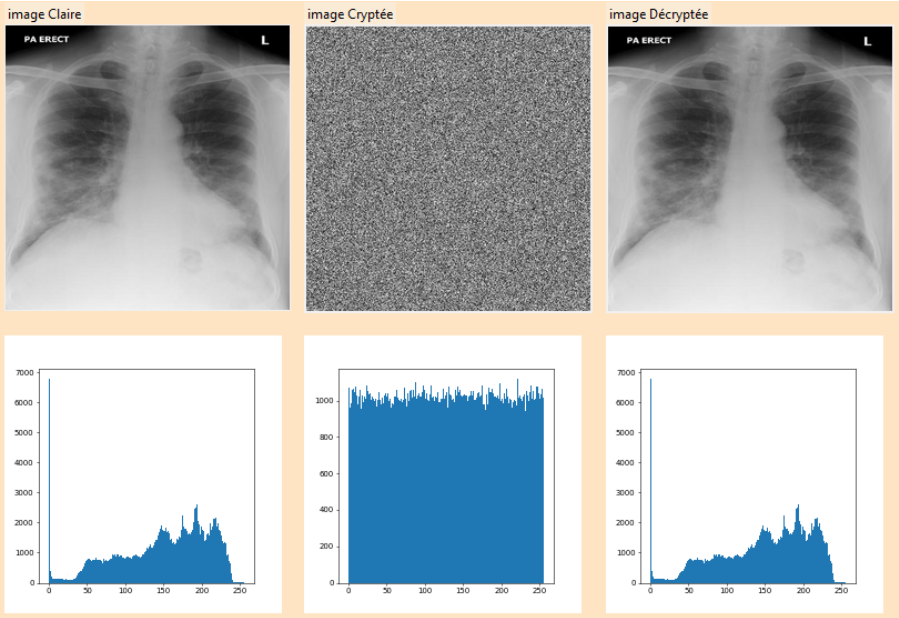


FIGURE 4.25 – Résultats d'analyse d'histogrammes d'image *chest − xray*

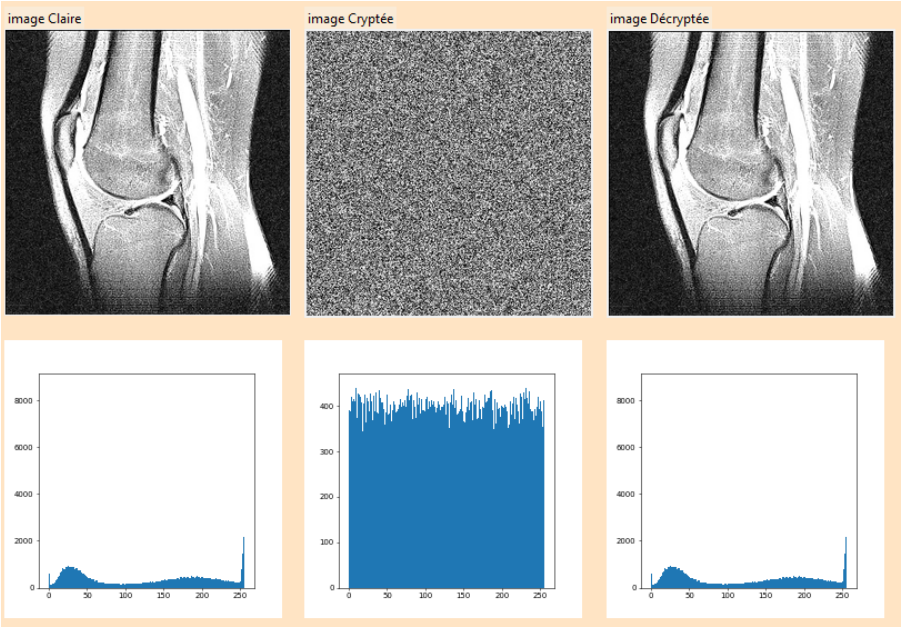


FIGURE 4.26 – Résultats d'analyse d'histogrammes d'image *knee – mri*

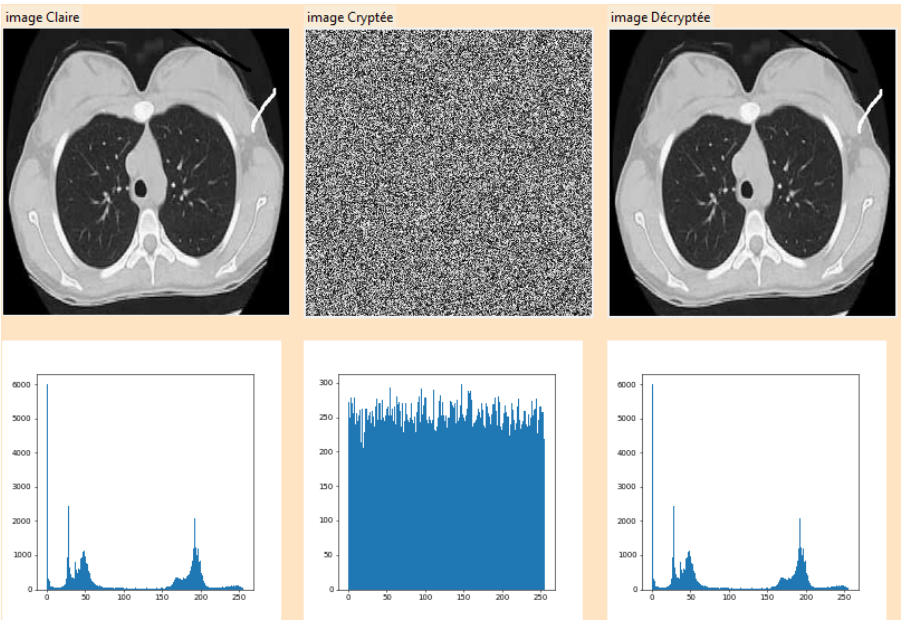


FIGURE 4.27 – Résultats d'analyse d'histogrammes d'image *ct – lung*

Les histogrammes des images cryptées illustrées dans les figures 4.25 , 4.26 , 4.27 , 4.28 et 4.29 ont une distribution uniforme qui diffère complètement de l'image originale correspondante. Par conséquent, il est difficile pour les attaquants d'effectuer l'analyse statistique de l'histogramme car les images cryptées ne contiennent aucune information utile pouvant être exposée.

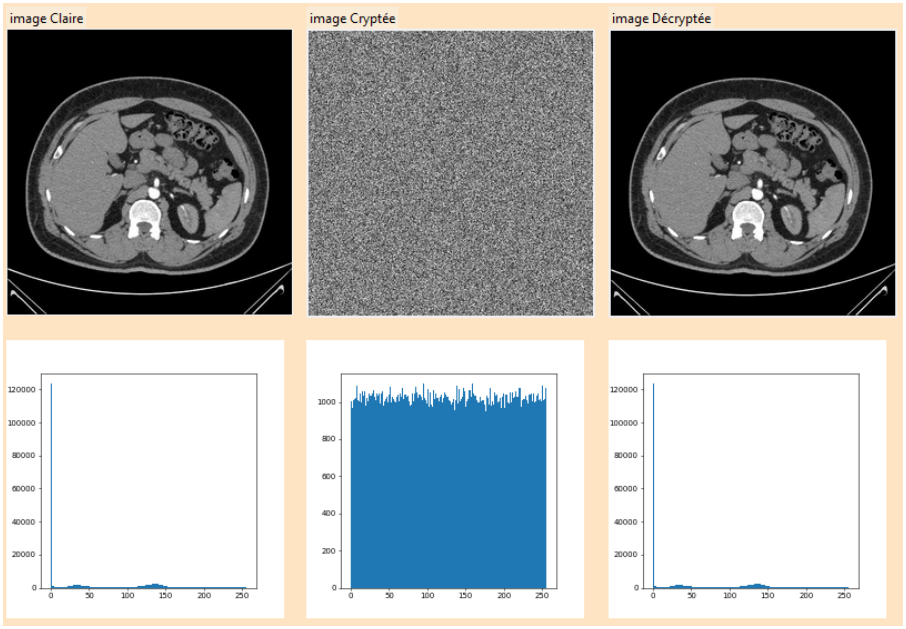


FIGURE 4.28 – Résultats d'analyse d'histogrammes d'image $ct - kedney$

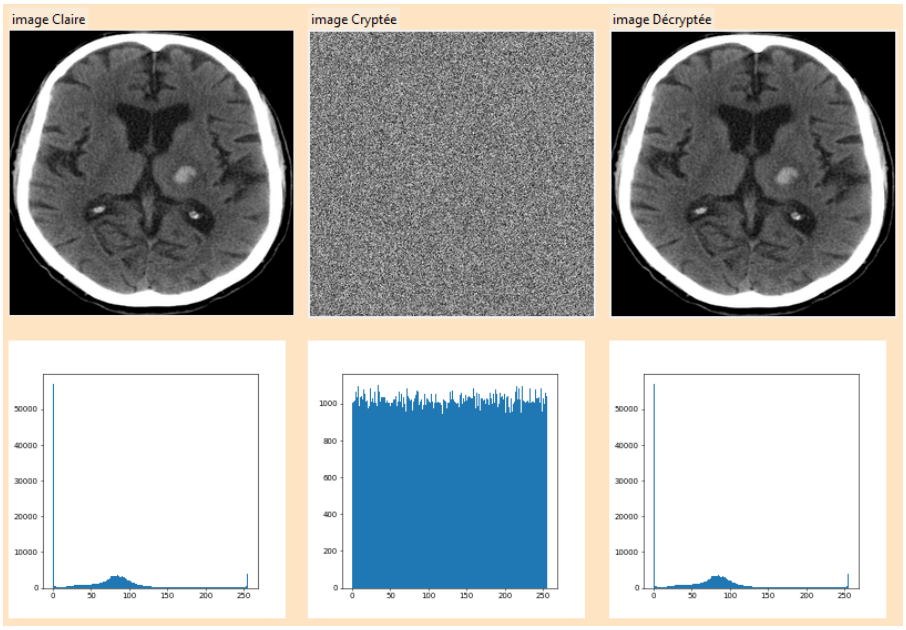


FIGURE 4.29 – Résultats d'analyse d'histogrammes d'image$head - ct$

4.8.3 Corrélation

Cette analyse effectuée en suivant les procédures,Au hasard 10000 paires sont sélectionnées et elles sont sélectionnées comme adjacentes horizontalement, verticalement et en diagonale. La corrélation est calculée par l' équation 2.7,Comme le montre le tableau 4.9 suivant :

Image	Horizontal		Vertical		Diagonal	
$Ct - kedney$	0.9773	-0.01717	0.9538	-0.0024	0.9426	-0.0029
$Ct - head$	0.9914	0.00007	0.9888	0.0048	0.9832	0.0042
$Chest - xray$	0.9961	-0.0026	0.9846	-0.0039	0.9941	-0.0055
$Ct - lung$	0.9616	0.0785	0.9847	0.0064	0.9746	0.0093
$mri - knee$	0.9069	0.0039	0.9239	-0.0138	0.8784	-0.0155

TABLE 4.9 – Coefficients de Corrélation des images en clair et cryptée

les résultats du calcul la corrélation des images originales et des images cryptées dans trois directions pour la méthode proposée qui se rapproche à zéro. Cela signifie que le système proposé a une bon Sécurité.

La corrélation horizontale, verticale et diagonale des pixels dans l'image $knee - mri$ d'origine et la corrélation des pixels dans l'image $knee - mri$ cryptée sont illustrées à la figure4.30.

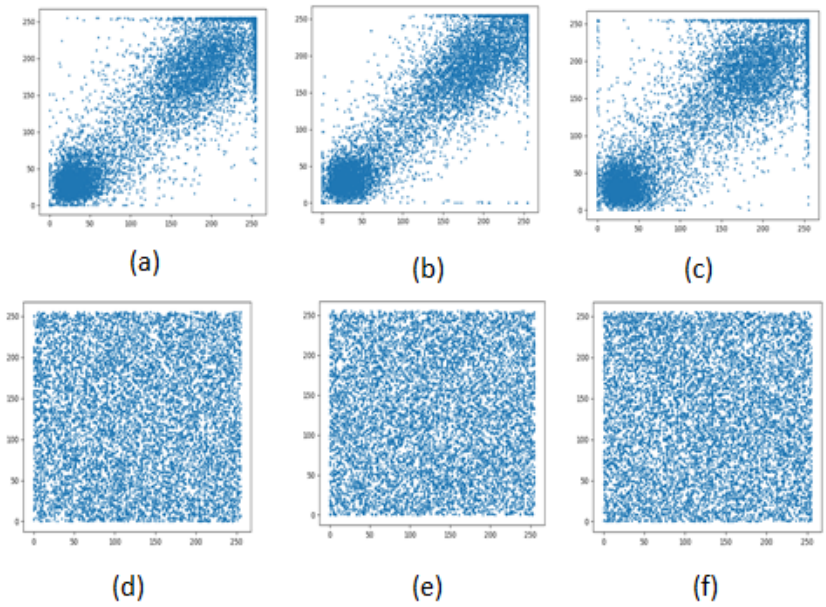


FIGURE 4.30 – 8 (a) Direction horizontale de l'image simple ,(b) Direction verticale de l'image simple ,(c) Direction diagonale de l'image simple ,(d) Direction horizontale de l'image cryptée (e) Direction verticale de l'image cryptée, (f) Sens diagonal de l'image cryptée pour l'image de test $knee - mri$

La faible corrélation entre les pixels adjacents dans 4.30 prouve que le système basé sur la méthode de salsa peut casser la corrélation entre les différents pixels de l'image.

4.8.4 Entropie

Nous calculons les entropies d'information de différent images de test et leurs images Cryptée correspondantes.

Image	Taille	Entropie	
		Image original	Image cryptée
$Ct - kedney$	512x512	4.8191	7.9993
$Ct - head$	512x512	6.0223	7.9993
$Chest - xray$	512x512	7.6166	7.9993
$Ct - lung$	256x256	6.7448	7.9971
$Knee - mri$	320x320	7.5121	7.9983

TABLE 4.10 – Entropie Des images Originales et Cryptées

Comme on peut le voir sur le tableau4.10, les entropies de toutes les images cryptée sont proche de la valeur idéale 8, Les résultats ci-dessus démontrent que l'amélioration proposé est sécurisé contre l'attaque statistique.

4.8.5 Sensitivité de la clé

Pour évaluer la propriété de sensibilité clé de la proposition cryptage, plusieurs image médicales original claires de taille (512×512) ont été d'abord cryptées à l'aide de clé secrète (a=10,b=8, R=116,X_0 = 0. 6141 , y_0=0. 5487 , p = 0.31 , r =3.999), puis on crypte les mêmes images claires en utilisant les clés (a) , (b) et (c), Les résultats sont récapitulés dans le tableau 4.11 :

Les changements sont comme suit :

(a) :(a=10,b=8,N=116,X_0 = 0. 61410001 , y_0 =0.5487 , p = 0.31 , r =3.999) .

(b) :(a=10,b=8,N=116, X_0 = 0. 6141 ,y_0 =0. 54870001 , p = 0.31 , r =3.999).

(c) :(a=10,b=8,N=114, X_0 = 0. 6141 , y_0 =0. 5487 , p = 0.31 , r =3.999).

Image	Taille	(a)		(b)		(c)	
		NPCR	UACI	NPCR	UACI	NPCR	UACI
$Ct - kedney$	512x512	99.60	33.43	99.62	33.44	77.53	23.06
$Ct - head$	512x512	99.60	33.43	99.62	33.45	93.92	24.96
$Chest - xray$	512x512	99.60	33.46	99.62	33.40	99.38	30.96

TABLE 4.11 – Sensibilité de la clé en utilisant les différents paramètres

En suite les image médicales cryptées avec la clé secrète original ont été décryptées à l'aide des clés de décryptage suivantes (a1),(b1) et(c1) :

(a1) : (a=10,b=8,N=140, ,X_0= 0. 61410001 „y_0 =0.5487 , p = 0.31 , r =3.999) .

(b1) : (a=10,b=8,N=140, ,X_0 = 0. 6141 , ,y_0 =0. 54870001 , p = 0.31 , r =3.999).

(c1) : (a=10,b=8,N=138, ,X_0 = 0. 6141 , ,y_0 =0. 5487 , p = 0.31 , r =3.999).

la figure4.19 illustre les résultats de ce test sur l'image $head - ct$

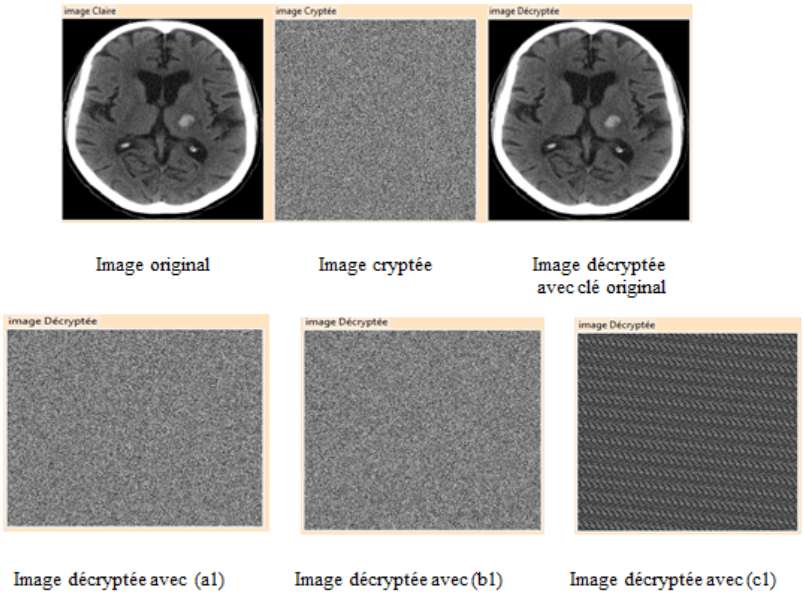


FIGURE 4.31 – Résultats d'analyse d'histogrammes d'image $head - ct$

la Figure4.31 démontre que les résultats décryptés avec une mauvaise clé sont toujours des images bruitées. Cela indique que notre algorithme est sensible à la clé.

4.8.6 Ssim et Psnr

Le tableau affiche les valeurs SSIM et psnr pour l'image en échelle médicale cryptée par rapport à l'image originale d'origine .

images	Ct kedney	Chest xray	Head ct	Mri knee	Ct lung
ssim	0.0042	0.0095	0.0067	0.0081	0.0063
psnr	6.27	8.346	6.974	6.975	7.15

TABLE 4.12 – les valeurs de Ssim et Psnr

Selon les résultats du tableau4.12,on peut remarquer que les valeurs ssim obtenues à partir de la technique basé sur salsa 20 sont presque égales à zéro , et les valeurs psnr sont faibles, Ce qui indique que l'image originale et image cryptée ne sont pas similaires.

4.8.7 Attaques de bruit

Dans les applications du monde réel, les images numériques sont transmises via un canal de communication qui est généralement soumis à un bruit de canal. Pour Analyser l'immunité au bruit de système améliorer Le bruit de gaussien a été utilisé pour attaquer les images cryptées avec une variance de 0,01 et 0,1.

Bruit gaussien	Psnr/Mse	Ct kedney	Head ct	Mri knee
variance = 0,01 moyenne = 0	Psnr	26.02	27.22	27.85
	Mse	162.20	123.28	106.45
variance = 0,1 moyenne = 0	Psnr	26.02	27.22	27.85
	Mse	162.557	123.28	106.45

TABLE 4.13 – les valeurs de Mse et Psnr

Le tableau 4.13 montre les valeurs de MSE et du PSNR entre image décryptée sans attaque de bruit et les images décryptées sous attaques de bruit de gaussien avec les deux valeurs de variance.

La figure 4.32 illustre l'effet de décryptage du l'image de ct kedney après avoir été soumise à l'attaque de bruit de gaussien.

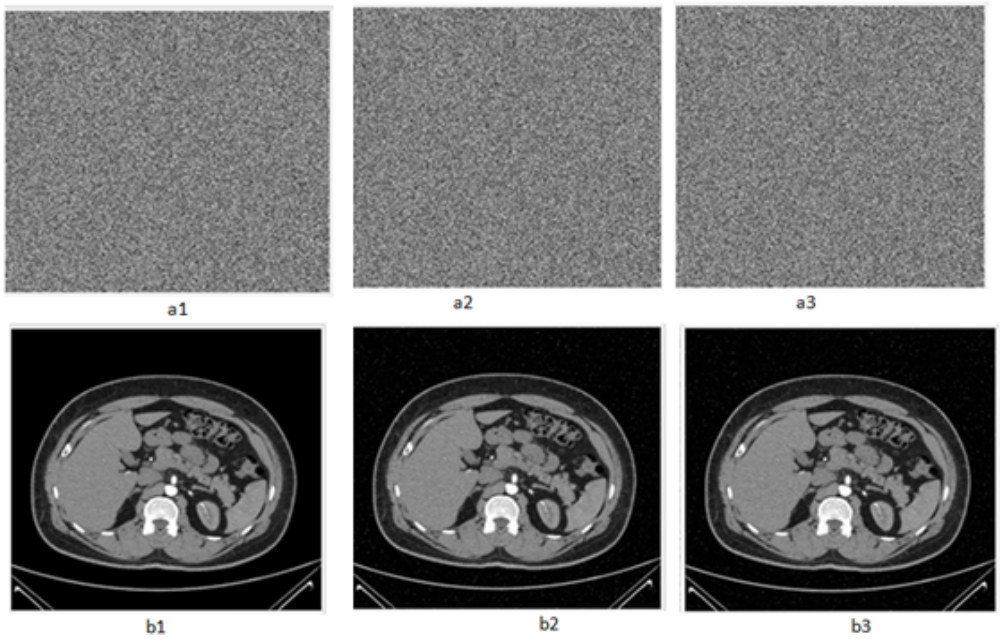


FIGURE 4.32 – (a1) est image cryptée original et (b1)image décryptée sans les attaques de bruit, (a1) image cryptée sous attaques avec variance de 0.01 et (b2)image décryptée avec variance de 0.01 ,(a3) image cryptée sous attaques avec variance de 0.1 et (b3)image décryptée avec variance de 0.1.

Comme on peut le voir sur les figures 4.32 (b2) et (b3), les images décryptées sous attaque gaussienne sont visibles ce qui démontre que l'algorithme proposé basé sur salsa20 est résistant aux attaques de bruit.

4.8.8 Analyse de temps

La consommation de temps de système proposée2 (base sur chiffremet salsa 20) est principalement généré par la carte Arnold, et à mesure que la taille de l'image devient plus grande, le temps pour la carte Arnold est également plus long ,Spécifications de l'ordinateur portable utilisé pour effectuer cette expérience sont décrites on sous-section(4.5.1), Les tests de temps sont effectués sur chaque image de taille différente (head ct (512×512),knee mri(320 ×320) et ct lung (256256)),Les résultats du test de temps sont présentés dans le tableau 4.14 ci-dessous. Mais d'âpres les résultats de test Le temps de calcul est acceptable sur le déroulement de

Image	Cryptage(s)	Décryptage(s)
256×256	7.33326	5.09709
320×320	11.3326	12.0723
512×512	37.1670	57.033

TABLE 4.14 – Analyse du temps

l'algorithme de cryptage/ décryptage. Donc on a des possibilités de résister à des tentatives d'attaques.

4.9 Etude comparative

Pour évaluer davantage la précision et la robustesse de notre deux systèmes proposée, nous l'avons testé sur des images de référence et comparé ses performances à d'autres algorithmes proposés. Nous avons utilisé les images «chest xray» et « ct kedney » à des fins de comparaison. Les résultats de simulation de système proposée sont analysés statistiquement à l'aide de différentes mesures (l'entropie, espace de clé,Corrélation,Analyse de temps) en comparaison avec d'autres schémas [62] [67] [68] [69] [71] :

4.9.1 Entropie

La moyenne et les valeurs d'entropie des différentes méthodes proposées sont données dans le tableau4.15 :

Image	proposée 1	proposée 2	[62]	[71]
Ct kedney	7.9992	7.9993	7.9992	7.9980
Chest xray	7.9992	7.9993	7.9994	7.9990
moyen	7.9992	7.9993	7.9993	7.9985

TABLE 4.15 – comparaison entropie de différentes méthodes proposée

.

À partir de tableau 4.15on remarque que moyenne d l'entropie pouvant être atteinte par les deux systèmes proposées est très proche de [71], l'entropie de première proposition supérieure de celle proposée à [71], et légèrement inférieur à celles de [62],ainsi que l'entropie de méthode basé sur salsa supérieure de celle proposée à [71], et on égalité à celle de [62]. Nous déduisons que les schémas de cryptage proposés offre un meilleur caractère aléatoire que [62] [71] [68]

4.9.2 Espace de clé

Le tableau 4.16 montre que l'espace clé de notre deux crypto système proposée est largement plus grand que l'espace clé dans [62] [71] [68] :

référence	proposée 1	proposée 2	[62]	[71]	[68]
Espace de clé	$2^{277.7}$	2^{344}	2^{159}	($\geq$ 1014 $\times$1014 $\times$1014 $\times$1014 $\times$255)	2^{148}

TABLE 4.16 – comparaison d'espace de clé de différentes méthodes proposée

4.9.3 Corrélation

Le tableau 4.17 montre la moyen des coefficients de corrélation des images cryptées de notre deux crypto-système proposés et les algorithmes de [62] [67] [69] dans les directions horizontale, verticale et diagonale

	Corrélation			Coefficient total
	H	V	D	
[62]	0.0104	0.0150	-0.0046	0.0208
[67]	0.0025	0.0029	0.0027	0.0081
[69]	0.2491	0.2783	0.2582	0.0081
Proposé 1	0.0013	0.0062	-0.0022	0.0052
Proposé 2	0.0125	- 0.0021	-0.0024	0.0080

TABLE 4.17 – comparaison de corrélation de différentes méthodes proposée

Les résultats après calcul du coefficient de corrélation total de chaque algorithme montrent, d'une part, que la valeur obtenue par notre système proposé1 est inférieure à celles obtenues par les différents quatre algorithmes mentionnés, y compris un autre système proposé basé sur la salsa. Ensuite, nous remarquons également que la valeur de corrélation totale de la méthode proposée2 est inférieure à celles obtenues par le reste des algorithmes cités. En revanche, ces valeurs sont plus proches de zéro ce qui signifie que les données sont effectivement mieux sécurisées par nos deux systèmes de chiffrement que [62], [67], [69].

4.9.4 Analyse de temps

Analyse de temps dépend de nombreux facteurs, notamment le nombre d'itérations, le type de calculs effectués et l'efficacité de la machine utilisée. Il est donc difficile de comparer les performances de vitesse en fonction des résultats publiés, car ils utilisent des systèmes différents et emploient différents approches techniques de programmation, Cependant, le temps d'exécution de sortie des documents de référence est indiquée dans tableau 54, pour la comparaison nous avons utilisé image médical (ct lung) de taille (256 $\times$256).

référence	P1	P2(salsa)	[68]
le temps	7.0556(s)	7.33326(s)	23.97(s)

TABLE 4.18 – Analyse de temps

Nos deux systèmes de cryptage proposés, comme le montre le tableau 4.18, sont plus rapides que la méthode de [68], mais malheureusement, [62]et [71] n'ont pas publié leurs résultats pour montrer que nos deux méthodes sont mieux adaptées aux applications réelles.

4.10 Conclusion

Nous avons consacré notre chapitre à l'implémentation et l'évaluation des performances de notre crypto système proposé ainsi que l'interprétation des résultats obtenus.
Grâce aux comparaisons entre multiples critères d'analyse différentielle aussi que statistique entre les étapes de processus de la méthode proposé, nous avons conclu que les conditions initiales des systèmes chaotiques ont un impact significatif sur les résultats de cryptage / décryptage car un léger changement dans les conditions initiales de chiffrement appliquées provoquent un changement notable dans les images cryptée par différents algorithmes proposés.
La méthode proposée démonte le haut niveau de sécurité des systèmes chaotique développés ainsi elle confirme sa robustesse face à différentes attaques.

CONCLUSION GÉNÉRALE

Rappelons que notre objectif dans ce mémoire consiste à concevoir et implémenter un système de cryptage chaotique des images médicales. Pour atteindre cet objectif, nous avons d'abord présenté des généralités sur les trois domaines qui englobent notre travail : cryptographie,imagerie et chaos .

Sur le plan empirique, nous avons prouvé que la Génération de séquence proposée qui définit à partir d'une comparaison des deux cartes chaotique : la carte logistique , la carte PWLCM est aléatoire , déterministe et sensible aux condition initiales c'est qui démontre que la séquence proposée peut être appliqués en cryptographie .

Nous avons implémenté un système de cryptage d'image basé sur cette nouvelle séquence proposée avec une architecture de confusion-diffusion bien étudiée. Pour démontrer l'efficacité et la robustesse de notre séquence proposé nous avons améliorer notre Crypto-système chaotique par combinées la séquence proposée avec le chiffrement salsa 20.

Certaines analyses de sécurité sont effectuées tel que l'analyse d'histogramme, de corrélation, d'entropie, d'espace de clé pour démontrer la haute sécurité de cryptage proposé .
le système proposé dispose un niveau élevé de confusion ,nous apercevons clairement que l'analyse d'histogramme des images cryptées sont uniformément distribuées, Par conséquent, l'attaquant il ne peut pas extraire l'information à partir de l'histogramme de l'image cryptée de manière facile. La corrélation entre les images chiffrés et ses images originales ne donne aucune information cela signifie la robustesse de l'algorithme.

Aussi ,les différentes combinaison qui comporte la clé secrète montre que la taille de L'espace de clé est suffisamment grand pour rendre l'attaque par force brute infaisable, Un chiffrement d'image avec un espace de clé long est suffisant pour une utilisation pratique fiable. Les deux mesures ont été utilisées : NPCR et UACI pour montrer un changement entre l'image crypté

et l'image d'origine .De ce fait l'algorithme proposé montre l'efficacité et la sécurité de notre système proposé.

Enfin, les comparaisons avec les schémas de chiffrement d'image existants qui ont été réalisées et avec les algorithmes de base de notre méthode montrent que l'algorithme proposé offre des performances très favorables.

BIBLIOGRAPHIE

[1] Renaud Dumont,Cryptographie et informatique, support de cours, Université De Liège, (2009, 2010).

[2] G Florin and S Natkin, Les techniques de cryptographie, (2002).

[3] Bayad A. *Introduction à la cryptographie. Université d'Evry val d'Essonne*, (2008).

[4] ahmed ammar et bouzgag mabrouk , *Conception d'un application de tatouage numériqu"Water mark" robuste aux imagesJPEG* ,Université Kasdi Mer bah Ouaregla,(2018).

[5] http ://dit-archives.epfl.ch/FI00/fi-sp-00/sp-00-page5.html, (2018).consulté le 12-5-2022

[6] Rezkallah, Louiza. De la cryptographie classique à la cryptographie moderne théorie et application. Diss. Alger, 2007.

[7] jean-François Pillou, *Chiffrement par substitution* (2008).

[8] Pierre-Louis Cayrel, *Chiffrement par blocs* ,Université de Limoges,(2015).

[9] Nivedita Bisht1et Sapna Singh2,*A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms* ,(2015).

[10] Numeriksciences, https ://numeriksciences.fr/ , consulté le consulté le 12-5-2022.

[11] Rafael C Gonzalez and Richard E Woods, Digital image processing reading, (1992)

[12] H Naciri and N Chaoui,Conception et réalisation d'un système automatique d'identification des empreintes digitales. Mémoire de PFE, Université de Tlemcen, (2003).

[13] https :www.researchgate.net/profile/David Ameisen/publication/259326499 Qu'estce-qu'une image numerique/links/0c96052b02619cf84d000000/Quest ce quune image numerique.pdf*. consulté le 12-5-2022

[14] Léon Robichaud, L'image numérique pixels et couleurs, https ://mtlnumerique.uqam.ca/upload/files/presentation1 LeonRobinchaud theorie.pdf, (2021).consulté le 12-5-2022

[15] Serge WACKE,Les formats d'images numeriques, http ://serge.wacker.free.fr/ technoprimaire/c2i/revisions/formatsimage.pdf.consulté le 12-5-2022

[16] Isdant, Raphaël. "Traitement numérique de l'image." (2009).

[17] http ://serge.wacker.free.fr/ chnoprimaire/c2i/revisions/format simage.pdf. consulté le 12-5-2022

[18] Haidekker, Mark A. "Medical imaging technology." (2013).

[19] Salomé Le Gall,Bases physiques de l'imagerie médicale : imagerie analogique / imagerie numérique, Cours 3 UE2, (2016).

[20] YAGOUB Imad Eddine, *Systèmes dynamiques discrets et chaos*, université du havre,(2010/2011).

[21] Estelle Cherrier,*Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires*.PhD thesis,(2006).

[22] COLARD, J DELPUECH, Les rayons X une révolution dans l'avancé du diagnostic médical(2020).

[23] <http ://www.radiologieperpignan.fr/wpcontent/ uploads/photogallery/Photos,(2020).consulté le 12-5-2022.

[24] Kevin M Cuomo and Alan V Oppenheim, *Circuit implementation of synchronized chaos with applications to communications*,Physical review letters,(1993).

[25] HODEL, J, Formes progressives de sclérose en plaques : place actuelle de l'IRM pour le diagnostic positif et différentiel,(2018).

[26] DURAND, E BLONDIAUX, E , In imagerie médicale, Elsevier Masson SAS,12p,(2017).

[27] A Naiit Ali et Christine Cavaro-menard, Compression des images et des signaux médicaux,(2007).

[28] Jerrold T Bushberg,J Anthony Seibert, Edwin M Leidholdt Jr, John M Boone, and Edward J Goldschmidt Jr,The essential physics of medical imaging,Medical Physics,(2003).

[29] Jerrold T Bushberg, J Anthony Seibert, Edwin M Leidholdt Jr, John M Boone, and Edward J Goldschmidt Jr, The essential physics of medical imaging, Medical Physics,(2003).

[30] Sankpal, Priya R, PA Vijaya. Image Encryption Using Chaotic Maps : A Survey. Signal and Image Processing (ICSIP),(2014).

[31] Jolfaei Alireza, AbdolrasoulMirghadri. An image encryption approach using chaos and stream cipher. Journal of Theoretical and Applied Information Technology, (2010).

[32] Wang, Xingyuan, Lin Teng, Xue Qin. A novel colour image encryption algorithm based on chaos. Signal Processing, (2012).

[33] Coppersmith Don. The Data Encryption Standard (DES) and its strength against attacks. IBM Journal of Research and Development,1994.

[34] Julien salort. https ://www.maths.univ-evry.fr/, (2021).consulté le 12-5-2022

[35] Melle Megherbi Ourdia. *« Etude et réalisation d'un système sécurisé a base de Systèmes chaotiques »*, Mémoire de Magister, Université Mouloud Mammeri de Tizi-Ouzou, (2013).

[36] IKHLEF Ameur, *synchronisaon, Chaoficaon et Hyperchaoficaon des Systèmes Nonlinéaires : Méthodes et Applicaons*, thèse de doctorat à l'Université Mentouri de Constanne, Algérie,(2011).

[37] T Hamaizia. *systèmes dynamiques et chaos : Application à l'optimisation à l'aide d'algorithme chaotique*,PhD thesis, Thèse de Doctorat, Université Mentouri de Constantine,(2013).

[38] Samia BELKACEM. *Chaos based image watermarking*. PhD thesis, Université de Batna 2, (2015).

[39] YAGOUB Imad Eddine, *Systèmes dynamiques discrets et chaos*, université du havre,(2010/2011).

[40] Chouaib BENHABIB. *étude d'un système chaotique pour la sécurisation des communications optiques*,PhD thesis, (2014).

[41] M. P. Kennedy, *Basic concepts of nonlinear dynamics and chaos,*, (1994).

[42] Ouerdia Megherbi. *Etude et réalisation d'un système sécurisé à base de systèmes chaotiques.*PhD thesis, Université Mouloud Mammeri, tizi-ouzou, (2013).

[43] BENIANI Rabab,*Sécurité des images Numériques compressées JPEG* ,Université Djilali Liebes,thesis ,(2019).

[44] Chen, G., Mao, Y., Chui, C.K. : Chaos, Solitons and Fractals 21,749–761 (2004).

[45] 7. Mao, Y., Chen, G., Lian, S. : Int. J. Bifurcat Chaos 14, 3613–3624 (2004).

[46] .Ben Ammar Asma, Haddouche khalissa, *Amélioration de la génération des sous clés de l'algorithme cryptographique DES*, UNIVERSITE Akli Mohand Oulhadj —Bouira,(2017).

[47] 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).

[48] Dalia Battikh. *Sécurité de l'information par stéganographie basée sur les séquences chaotiques* ,PhD thesis, Rennes, INSA, (2015).

[49] Jastrzebski K., and Kotulski Z, "On improved image encryption scheme based on chaotic map lattices, (2009)

[50] Faraoun K., "A chaos-based key stream generator based on multiple maps combinations and its application to images ,(2010).

[51] Mohammad S., and Mirzakuchaki S., "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," Signal processing, (2012).

[52] Shannon C., "Communication theory of secrecy systems, 1949

[53] Fridrich J., "Symmetric ciphers based on two dimensional chaotic maps," International Journal of Bifurcation and Chaos,2018.

[54] Wong, KwokWo. *Image encryption using chaotic maps.* Intelligent Computing Based on Chaos. Springer, Berlin, Heidelberg,(2009).

[55] Jean De Dieu Nkapkop ,Chaotic Encryption Scheme Based on A Fast Permutation and Diffusion Structure, Department of Physics, October 7, (2015).

[56] . Mao, Y., Chen, G. : *Chaos-based image encryption.* In :Bayro-Corrochano, E. (ed.) Handbook of computational geometry for pattern recognition, computer vision, neural computing and robotics,(2003).

[57] Assia Beloucif. Contribution à l'étude des mécanismes cryptographiques. PhD thesis, Université de Batna 2,(2016).

[58] E. Yavuz. A novel chaotic image encryption algorithm based on content sensitive dynamic functions witching scheme, Optics and Laser Technology, 2019.

[59] 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).

[60] Claude E Shannon. *Communication theory of secrecy systems. The Bell system technical journal, 28(4) :656–715, 1949.*

[61] Benssalah, Mustapha, and Yasser Rhaskali. "A secure DICOM image encryption scheme based on ECC, linear cryptography and chaos." , (2020).

[62] C. Fu, Y. -F. Shan, M. -Y. He, Z. -Y. Yu and H. -L. Wu, "A New Medical Image Encryption Algorithm Using Multiple 1-D Chaotic Maps," 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC),(2018).

[63] Moafimadani SS, Chen Y, Tang C. A New Algorithm for Medical Color Images Encryption Using Chaotic Systems. Entropy (Basel). (2019)

[64] HAN, Baoru, JIA, Yuanyuan, HUANG, Guo, et al. A Medical Image Encryption Algorithm Based on Hermite Chaotic Neural Network. (2020) .

[65] HARSHITHA, M., RUPA, Ch, SAI, K. Pujitha, et al. Secure Medical Data Using Symmetric Cipher Based Chaotic Logistic Mapping. In : (2021).

[66] CHEN, Xiao et HU, Chun-Jie. Adaptive medical image encryption algorithm based on multiple chaotic mapping. Saudi journal of biological sciences,(2017).

[67] A. Belazi, M. Talha, S. Kharbech and W. Xiang, "Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding,(2019).

[68] M Madani and Y Bentoutou. Cryptage d'images médicales à la base des cartes chaotiques. In International Conference Colloque Tassili SCCIBOV, (2015).

[69] Zhang, Junjie, Jun Tan, and Yun Cheng. "Medical Image Encryption Algorithm Based on Chaotic Function." 2017.

[70] Jeong, Hyun-Soo, et al. "Color medical image encryption using two-dimensional chaotic map and C-MLCA." 2018 ,(2018).

[71] Yasser, Ibrahim, et al. "A Robust Chaos-Based Technique for Medical Image Encryption." IEEE Access 10 (2021) : 244-257.

[72] KOUADRI Moustefai. Tests de validation pour les crypto-systèmes chaotiques. PhD thesis, Universite mohamed boudiaf'des sciences et de la technologie d'oran, 2014.

[73] Rukhin, Andrew, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Booz-allen and hamilton inc mclean va, 2001.

[74] H. Bauke, S. Mertens, Random numbers for large-scale distributed Monte Carlo simulations, Phys. Rev. E 75 (2007) 066701–14

[75] J.F. Fernandez, C. Criado, Algorithm for normal random numbers, Phys. Rev. E 60 (1999) 3361–3365.

[76] Dalia Battikh. Sécurité de l'information par stéganographie basée sur les séquences chaotiques. PhD thesis, Rennes, INSA, (2015).

[77] Mishra, Kapil, and Ravi Saharan, "A fast image encryption technique using Henon chaotic map." Progress in advanced computing and intelligent engineering, (2019).

[78] technology. IEEE, 2014. [7] Wang, Xingyuan, and Pengbo Liu. "A new image encryption scheme based on a novel one-dimensional chaotic system." (2020).

[79] Balakrishnan, Binu, and D. Muhammad Noorul Mubarak. "An Improved Image Encryption using 2D Logistic Adjusted Sine Chaotic Map with Shuffled Index Matrix.", (2021).

[80] Rim Zahmoul, Ridha Ejbali and Mourad Zaied, Image encryption based on new Beta chaotic maps, Optics and Lasers in Engineering, (2017).

[81] Gopalakrishnan, T., Shankar Ramakrishnan, and M. Balakumar. "An image encryption using chaotic permutation and diffusion." 2014 International conference on recent trends in information technology. IEEE, (2014).

[82] Almazrooie,Samsudin, . Improving the diffusion of the stream cipher salsa20 by employing a chaotic logistic map. Journal of Information Processing Systems, 11(2), 310-32,(2015)