République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Akli Mohand Oulhadj de Bouira

Faculté des Sciences et des Sciences Appliquées

Département d'Informatique

Mémoire de Master

en Informatique

Spécialité : *Génie des systèmes informatique*

&

Ingénierie des Systémes d'informations et Logicielles

Thème

Conception et implémentation d'un algorithme de cryptage d'images basé sur des cartes chaotiques 1D.

Encadré par

- MR BENAISSI SELLAMI

Réalisé par

- KOULOUGHLI SONIA
- LAKROUM KENZA

2023/2024

Remerciements

Nous remercions Dieu le tout puissant de nous avoir donné la santé et la volonté d'entamer et de terminer ce travail.

En premier lieu,nous souhaitons exprimer notre gratitude envers nos parents pour tous leurs efforts, ainsi que envers tous les membres de notre famille et nos amis.

Nos sincères remerciements vont également à notre directeur de mémoire, benaissi sellami, pour sa guidance précieuse, ses conseils avisés et son soutien constant tout au long de ce travail. Sa patience, son expertise et sa disponibilité ont été d'une importance capitale pour la réussite de ce projet.

Enfin, nous tenons à remercier toutes les personnes qui, de près ou de loin, ont contribué à ce travail, ainsi que toutes celles qui ont cru en nous et nous ont soutenus tout au long de ce parcours académique.

Dédicaces

Je dédie ce modeste travail avec toute ma gratitude et mon affection :

À mes chers parents, pour leur amour inconditionnel, leur soutien et leurs encouragements constants.

À mes frères et sœurs, pour leur compréhension, leur patience et leur inspiration.

À ma binôme kenza et mes amies (djamila,nserine,houda, hafsa) pour leur amitié sincère, leur aide précieuse et leur encouragement continu.

Je tiens à exprimer ma reconnaissance envers mes professeurs à l'université, qui ont partagé leur savoir et leur expertise, et m'ont guidé tout au long de mes études. Leur passion pour l'enseignement a été une source d'inspiration pour moi.

Un mot spécial à mon encadrant, suite à son accompagnement, ses conseils précieux et son soutien constant, pour la réalisation de ce mémoire.

À toute personne qui m'a soutenu de près ou de loin durant ce travail.

Sonia

Dédicaces

Je dédie ce travail à ceux qui ont été ma source d'inspiration et de force tout au long de ce voyage académique.

À mes parents, pour leur amour et leur soutien inébranlable, qui ont été le socle de ma vie.

À mes frères et ma sœur, pour leur complicité et leurs encouragements, qui ont été une source de motivation constante.

À mes amis et ma binôme, merci pour votre présence, votre amitié sincère, les souvenirs précieux, et pour avoir été mon réseau de soutien.

À mes professeurs, pour leur dévouement et leur patience, qui ont façonné mon parcours éducatif.

Et à tous ceux qui ont touché ma vie, de manière visible ou invisible, et qui ont contribué à façonner la personne que je suis aujourd'hui.

Kenza

ملخص

مع زيادة استخدام شبكات الاتصالات، يتم نقل العديد من المعلومات عبر هذه الشبكات. من الضروري ضمان حماية هذه البيانات لتجنب أي وصول غير مصرح به ولمنع أي تسريب، خاصة بالنسبة للمعلومات الحساسة وبشكل خاص الصور. لذلك، تعتبر أنظمة التشفير الحل الأكثر فعالية لحل هذه المشكلة.

الطرق التقليدية للتشفير مثل

(DES) ,(IDEA),(RSA)

ليست مناسبة لتشفير الصور لأسباب متعددة؛ حيث أنها ضعيفة وغير فعالة. لهذا السبب، استخدمنا في هذه الأطروحة الخرائط الفوضوية لتشفير الصور بالألوان والصور بمستويات رمادية، وكان هدفنا إنشاء تسلسلات فوضوية من أجل استخدامها لتشفير وفك تشفير البيانات وبعد دراسة هذا الخوارزمية، لاحظنا أنها تقدم أداءًا جيدًا من حيث الجودة والأمان.

الكلمات الرئيسية : صورة رقمية، التشفير، الخريطة لفوضوية، الخريطة اللوجستية المحسّنة، الخريطة السينوسية المحسّنة.

Résumé

Avec l'augmentation de l'utilisation des réseaux de communication, de nombreuses informations sont transmises sur ces réseaux. Il est essentiel de garantir la protection de ces données afin d'éviter tout accès non autorisé et de prévenir toute fuite des informations sensibles, en particulier pour les images. Ainsi, la solution la plus efficace pour résoudre ce problème consiste à utiliser un système de cryptage.
Les méthodes traditionnelles de chiffrement telles que le DES, IDEA et RSA ne sont pas adaptées pour le chiffrement d'images pour différentes raisons : elles sont faibles et peu efficaces. C'est pourquoi, dans ce mémoire, nous avons utilisé la carte chaotique pour chiffrer les images en couleur et en niveaux de gris. Notre objectif était de créer des séquences chaotiques afin de les utiliser pour chiffrer et déchiffrer les données. Après avoir étudié cet algorithme, nous avons constaté qu'il offre une performance de qualité et de sécurité satisfaisante.

Mots clés : Image numérique, Cryptographie, carte chaotique, Carte logistique améliorée ILM, Carte sinusoïdale améliorée ISM.

Abstract

With the increasing use of communication networks, a lot of information is transmitted through these networks. It is essential to guarantee the protection of such data in order to prevent unauthorized access and to prevent leakage of sensitive information, in particular images. Thus, the most effective solution to solve this problem is to use an encryption system.

Traditional encryption methods such as DES, IDEA, and RSA are not suitable for encrypting images for various reasons,They are weak and ineffective. And Therefore, in this memory, we used the chaotic maps for encrypting images in both grayscale and color. Our aim was to generate chaotic sequences to utilize for encrypting and decrypting data. After studying this algorithm, we found that it offers satisfactory quality performance and security.

Key words : Digital Image, Cryptography, Chaotic Map, Improved Logistic Map ILM, Improved Sinusoidal Map ISM.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

- **PPP** : Pixels Per Pouces
- **BPP** : Bits Par Pixel
- **RGB** : Rouge, Vert, Bleu
- **BMP** : BitMaP
- **GIF** : Graphics Interchange Format
- **JPEG** : Joint Photographic Expert Group
- **ASCII** : American Standard Code for Information Interchange
- **IFF** : Interchange File Format
- **PCX** : Personal Computer eXchange
- **PNG** : Portable Network Graphics
- **TGA** : TARGA (format de fichier d'image)
- **DPI** : Dots Per Inch
- **N/B** : Noir et Blanc
- **TCP/IP** : Transmission Control Protocol/Internet Protocol
- **DES** : Data Encryption Standard
- **FPE** : Format Preserving Encryption

- **IDEA** : International Data Encryption Algorithm
- **ECC** : Elliptic Curve Cryptography
- **AES** : Advanced Encryption Standard
- **RSA** : Rivest-Shamir-Adleman (un algorithme de cryptographie asymétrique)
- **SSL** : Secure Sockets Layer
- **TLS** : Transport Layer Security
- **LE** : Exposant de Lyapunov
- **PWLCM** : Piecewise Linear Chaotic Map
- **1D** : Unidimensionnel
- **MD** : multidimensionnelles
- **ADN** : Acide désoxyribonucléique
- **SCAN** : Signatures numériques et compression d'image sans perte
- **QKD** : Quantum Key Distribution (Distribution de clés quantiques)
- **ILM** : Carte logistique améliorée
- **ISM** : Carte sinusoïdale améliorée
- **UACI** : Uniform Average Change Intensity (Changement Intensité Moyen Uniforme)
- **NPCR** : Number of Pixel Change Rate (Taux de Changement du Nombre de Pixels)

Introduction générale

La sécurisation des données est devenue une préoccupation majeure à l'ère numérique, où la transmission et le stockage d'informations sensibles sont omniprésents. Parmi ces données, les images numériques occupent une place prépondérante, que ce soit pour des applications personnelles, commerciales, médicales ou de surveillance. La protection de ces images contre les accès non autorisés et les manipulations malveillantes est essentielle pour préserver la confidentialité, l'intégrité et l'authenticité des informations qu'elles contiennent.

La cryptographie, en tant que science et art de protéger les informations par le biais de techniques de codage, joue un rôle crucial dans la sécurisation des images numériques. Elle permet de transformer les images en formes illisibles pour toute personne non autorisée, assurant ainsi leur protection contre les intrusions. Cependant, le cryptage des images présente des défis uniques en raison de leurs caractéristiques spécifiques, telles que les redondances spatiales et les corrélations élevées entre les pixels adjacents.

Dans ce contexte, l'application des systèmes chaotiques à la cryptographie d'images a émergé comme une solution prometteuse. Les systèmes chaotiques, caractérisés par leur sensibilité aux conditions initiales et leur comportement imprévisible mais déterministe, offrent des propriétés intéressantes pour le cryptage, telles que la complexité et la diffusion élevées. L'utilisation de cartes chaotiques multidimensionnelles permet de renforcer la sécurité des algorithmes de cryptage en introduisant des niveaux supplémentaires de complexité et de confusion.

Dans ce mémoire on a propose une nouvelle méthode hybride de chiffrement des images numériques, basée sur les cartes chaotiques 1D et le XOR. L'objectif est de développer un algorithme de cryptage qui assure un haut niveau de sécurité tout en optimisant les coûts de calcul et la vitesse de traitement. Les résultats obtenus montrent que les systèmes chaotiques peuvent efficacement renforcer la robustesse des algorithmes de cryptage, offrant ainsi de nouvelles perspectives pour le développement de solutions cryptographiques avancées adaptées aux exigences croissantes des applications modernes.

Le premier chapitre introduit les notions de base relatives aux images numériques, incluant leurs caractéristiques, types, et formats, ainsi qu'une introduction à la cryptographie, ses objectifs et ses différentes méthodes. Le deuxième chapitre est dédié à la théorie du chaos et aux systèmes dynamiques chaotiques, en détaillant leurs caractéristiques et en expliquant comment ils peuvent être utilisés dans le cryptage des images.

Le troisième chapitre examine en profondeur les techniques de cryptage des images, en décrivant les algorithmes de confusion et de diffusion, ainsi que diverses méthodes de substitution et de permutation. Une attention particulière est accordée aux méthodes de cryptographie chaotique, en analysant leurs avantages en termes de sécurité et de performance. Le quatrième chapitre présente l'implémentation pratique de l'application de cryptage d'image proposée, détaillant les algorithmes utilisés, l'environnement de travail, l'interface graphique développée, et les résultats expérimentaux obtenus. Une évaluation de la performance et une comparaison avec des méthodes existantes sont également incluses pour démontrer l'efficacité de l'approche proposée.

En conclusion, ce mémoire souligne l'importance cruciale de sécuriser les images numériques dans un environnement numérique en constante évolution. Il démontre également l'efficacité des systèmes chaotiques pour renforcer la robustesse des algorithmes de cryptage.

Chapitre 1

Généralité sur les images et la cryptographyie

1.1 Introduction

Les images numériques et la cryptographie sont deux domaines fondamentaux de l'informatique qui jouent des rôles cruciaux dans notre vie quotidienne. Les images numériques, représentations visuelles d'objets et de scènes dans un espace bidimensionnel, sont omniprésentes dans les médias, les communications et les applications informatiques. D'autre part, la cryptographie, l'art de sécuriser les communications en les rendant inintelligibles pour les personnes non autorisées, est essentielle pour garantir la protection et la sécurité des informations dans le domaine numérique.

1.2 les images

1.2.1 Définition de l'image numérique

Une image numérique est représentée comme un Une image numérique est représentée comme un ensemble de points connus sous le nom de *pixels*. Le terme *pixel* vient de l'anglais *Picture Element*, signifiant élément d'image. Chaque pixel est défini par une valeur numérique qui représente sa couleur et son intensité. La taille d'une image est de $K \times L$ pixels, où L représente le nombre de lignes et K le nombre de colonnes [21].
Comme l'exmple dans la Figure 1.1.

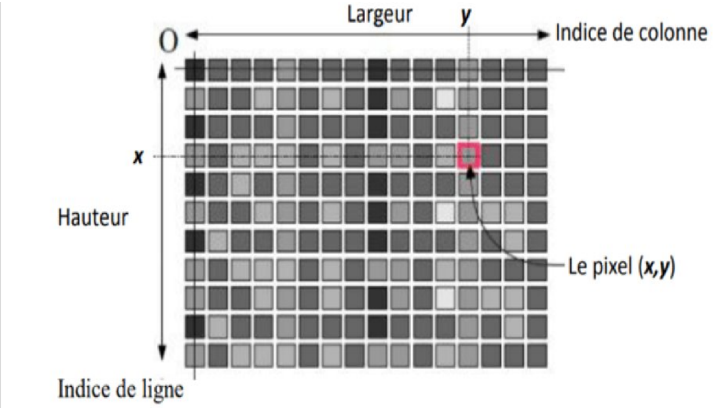


FIGURE 1.1 – Concept d'image représenté en pixels [1].

1.2.2 Caractéristique d'une image numérique

- **Pixels :**

  Il s'agit de la partie la plus petite d'une image numérique. Chaque pixel peut contenir des informations sur la couleur [22].

- **Dimensions :**

  les dimensions font référence à la taille de l'image en termes de largeur L et de hauteur H. Par la multiplication (L*H).

- **BPP :**

  L'unité bpp (bits par pixel, en anglais : bits per pixel) désigne le nombre de couleurs par pixel et indique le nombre de couleurs ou de niveaux de gris possibles dans le traitement d'images. Les valeurs courantes sont : * 1 bit : 2 couleurs, noir et blanc (monochrome). * 4 bits : 16 couleurs. * 8 bits : 256 couleurs. * 16 bits : 65 536 couleurs. * 24 bits : 16 777 216 couleurs, en règle générale 8 bits respectivement pour le rouge, le vert et le bleu, où chaque composante chromatique doit être précisée sur une échelle de 0 à 255 [23].

- **Résolution :**

  La résolution d'une image est définie par le nombre de pixels par unité de longueur (dpi (dot per inch = point d'encre par pouce) pour une imprimante ou ppp = pixels par pouce pour un fichier image). Cette résolution dépendra de la qualité de la numérisation [24].

$$\text{Résolution} = \frac{\text{définition}}{\text{longueur}}.$$

Comme l'exemple illustré dans la Figure 1.2.

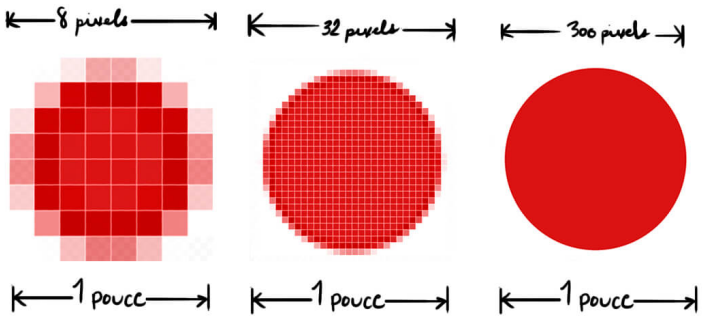


FIGURE 1.2 – explication de résolution d'une image [2].

1.2.3 Types d'images

Les images appartiennent à deux grandes familles : matricielle(BitMap) et vectorielle.

- **Image matricielle(BitMap) :**

  une image Bitmap est une images numérique peut être représentée par une matrice ou un tableau de valeurs, utilise des coordonnées (x, y) pour définir la position des pixels [25].

  Chaque pixel est représenté par une valeur binaire (suite de 0 et de 1) [26] et contribue à la composition générale de l'image. La dimension de l'image est définie par le nombre de lignes (L) et de colonnes (K) de pixels. On dit alors que l'image possède une dimension de K*L pixels, formant ainsi une matrice de pixels.

  En raison de sa nature basée sur des pixels, une image bitmap est généralement très manipulable et traitable. Les logiciels de traitement d'images, tels que les éditeurs graphiques, peuvent effectuer diverses opérations sur une image bitmap. Ces opérations incluent le redimensionnement, la rotation, l'ajustement des couleurs, le flou, la netteté, et bien d'autres encore. Mais le redimensionnement réduit sa qualité [27].

- **Image vectorielle :**

  Une image vectorielle est une image constituée de différents objets géomé- triques individuels (droites, polygones, arcs de cercle). La création de l'image vectorielle repose sur des équations mathématiques. Plusieurs paramètres (hauteur, largeur, rayon) sont donnés à des vecteurs pour chaque forme [28].

L'image vectorielle peut être facilement modifiée spatialement (réduction, agrandissement, translation, rotation, etc.) sans perte d'information [27] et il est difficile de réaliser certaines manipulations comme les changements de couleurs sur une zone d'un objet, sur un objet simple ou sur un groupe d'objets [27].

La Figure 1.3 représente un exemple d'image matricielle et l'image vectorielle.

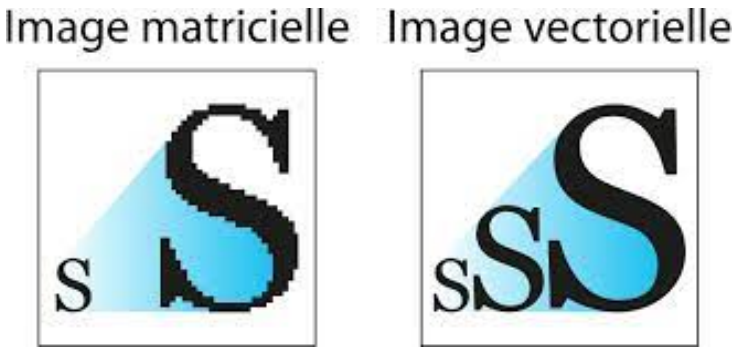


FIGURE 1.3 – image matricielle et image vectorielle [3].

1.2.4 Représentation des couleur

- **Image noir et blanc (binaire) :**

  Une image binaire, également appelée d'image en noir et blanc, est une image où chaque pixel ne peut détenir que deux valeurs (0 ou 1), pour représente deux couleurs : noir ou blanc.

  Comme illustré sur la Figure 1.4.

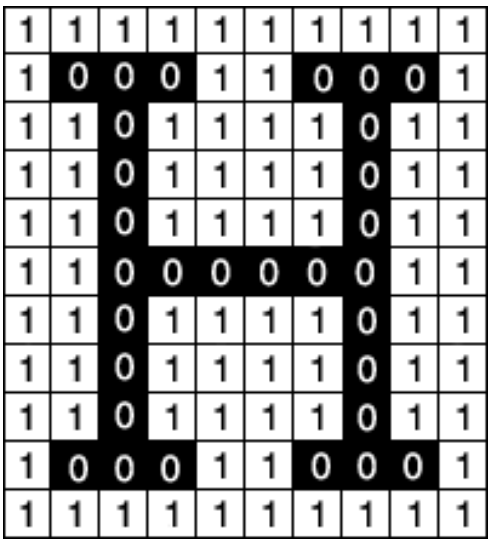


FIGURE 1.4 – La codification des couleur dans une image binaire [4].

- **Niveaux de gris :**

  Une image en niveaux de gris est une représentation numérique qui utilise différentes nuances de gris pour exprimer la variation de luminosité. Les images en niveaux de gris sont monochromes, chaque pixel est caractérisé par son niveau de luminosité ou de gris. Par exemple la gamme de valeurs va de 0 à 255, où 0 correspond au noir absolu et 255 au blanc absolu [13].

  Comme illustré sur la Figure 1.5.

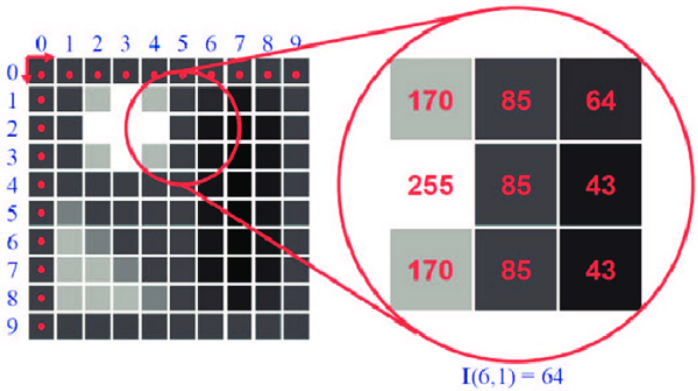


FIGURE 1.5 – Une image qui illustre la forme des pixels dans une image en couleur.

- **Image en couleur(RGB) :**

  Un pixel dans une image couleur est composé de trois parties représentant les couleurs rouge, verte et bleue, selon le modèle RGB. Chaque canal (rouge, vert, bleu) peut avoir une intensité lumineuse allant de 0 à 255, offrant ainsi une gamme de 256 valeurs possibles. Comme illustré sur la Figure 1.6.

FIGURE 1.6 – Une image qui illustre la forme des pixels dans une image en couleur [5].

1.2.5 Formats d'Images

Le format désigne la manière dont une image est représentée. Il y a différents formats d'images :

- **BMP (BitMaP) :** Le BMP est un format développé par Microsoft et IBM. Il a été conçu pour être utilisé sur des ordinateurs personnels (PC) et sous Windows et OS/2.

- **GIF (Graphics Interchange Format) :** GIF est un format créé par Compuserve, qui présente deux principaux avantages :
  Sa portabilité et son autonomie par rapport au système d'exploitation, ainsi que sa facilité et sa rapidité de lecture.

- **JPEG :** Le JPEJ, créé par le Joint Photographic Expert Group, présente les mêmes bénéfices que le GIF. Mais il est plus adapté aux images en couleur [29]. Le tableau 1.1 expose les formats les plus le plus utilisés.

Format	**Tailles maximales**	**Le maximum de couleurs**
BMP	65536 × 65536	16777216
GIF	65536 × 65536	256
IFF	65536 × 65536	Supérieur à 16777216
JPEG	65536 × 65536	Supérieur à 16777216
PCX	65536 × 65536	16777216
PNG	65536 × 65536	Supérieur à 16777216
TGA	65536 × 65536	Supérieur à 16777216
TGA	2^{32}-1	Supérieur à 16777216

TABLE 1.1 – Format d'image [17].

1.2.6 Le poids d'une Image

Afin d'obtenir le poids d'une image (exprimé en octe). Il est nécessaire de faire des calculer le nombre de pixels présents dans l'image, ce qui correspond au calcul de dimension de l'image. Le poids d'une image est évalué en multipliant sa dimension par le poids

de chaque pixel.

Les calculs suivants concernent une image de 512x512 en trois couleurs :

- La dimension : 512 x 512 = 262 144, en utilisant 3 octets par pixel.
- En conséquence, le poids de l'image est de 262144 x 3 = 786432 octets = 768 Ko [18].

Les exemples de poids d'image sont présentés dans le tableau 1.2.

Dimensions d'image	Image en noir et blanc	Image niveaux de gris (8 bits)	Image (16 bits)	Trois couleurs (24 bits)
128x128	2 ko	16 ko	32 ko	48 ko
2048x1152	288 ko	2,25 Mo	4,25 Mo	6,75 Mo
1024x1024	128 ko	1 Mo	2 Mo	3 Mo
3264x1836	731,53 ko	5,71 Mo	11,43 Mo	17,14 Mo
4128x3096	1,52 Mo	12,19 Mo	24,37 Mo	36,56 Mo

TABLE 1.2 – Quelques exemples de poids d'image [18].

1.3 la cryptographie

1.3.1 Définition 1

Cryptographie est un mot grec ancien qui dérive des mots « Kruptos » qui signifie « cacher » et « graphein » qui signifie « écrire ». Ainsi, il peut être interprété littéralement comme « cacher l'écriture ».

Le Petit Larousse définit la cryptographie comme un ensemble de méthodes de cryptage qui assurent la sécurité des textes et, en informatique, des données [30].

1.3.2 Définition 2

La cryptographie est une branche spécialisée de la cryptologie qui englobe l'ensemble des méthodes et des techniques permettant de chiffrer et de déchiffrer un texte en clair. Son objectif principal est de rendre ce texte incompréhensible pour toute personne n'ayant

pas accès à la clé nécessaire pour effectuer le déchiffrement.

En d'autres termes, la cryptographie vise à assurer la confidentialité des informations en les transformant de manière sécurisée, offrant ainsi une protection contre les accès non autorisés. (voir figure 1.7).

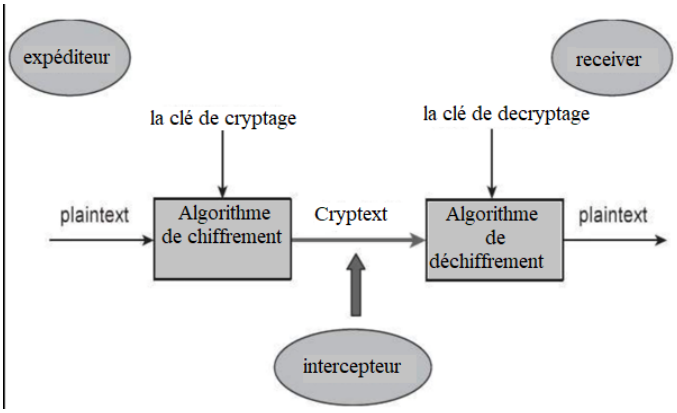


FIGURE 1.7 – Schéma général de la cryptographie [6].

1.3.3 Vocabulaire de cryptographie fondamental

- **Cryptanalyse :**

  Son objectif est d'analyser les lacunes des informations sécurisées en utilisant un modèle de recherche, une analyse et d'outils mathématiques, afin d'améliorer la méthode de chiffrement et la protection contre le piratage informatique [31].

- **Cryptologie :**

  la cryptologie représente la théorie du cryptage.

  Les deux branches principales de la cryptologie sont la cryptographie et la cryptanalyse [6].

$$Cryptologie = Cryptographie + Cryptanalyse.$$

- **Crypto-système :**

  Le matériel ou le logiciel utilisé pour mettre en place la cryptographie permet de convertir un texte clair en un texte chiffré et de le réécrire [31].

- **Plaintext :**

  Le texte clair (texte, audio, image, vidéo, ... etc.) [31].

- **Cryptext :**

  Le texte chiffré ou illisible [31].

- **Attaque :**

  Action malveillante visant à exploiter une faiblesse du système et à violer un ou plusieurs critères de sécurité [31].

- **Clé secrète :**

  Un ensemble de caractères et d'instructions qui régissent les opérations de cryptage et de décryptage [31].

- **Clé symétrique :**

  Clé employée pour la cryptage et la décryptage [31].

- **Clé asymétrique :**

  Un ensemble de clés (public et privé) La clé public sert au chiffrement, tandis que la clé privée sert au déchiffrement [31].

- **Espace de cles :**

  Les différentes valeurs possibles que les clés peuvent adopter [31].

- **le chiffrement et le déchiffrement :**

  Le processus de chiffrement transforme le texte en clair (plaintext ou cleartext) en texte chiffré, et le processus de déchiffrement transforme le texte chiffré en texte clair, comme l'illustre la figure 1.8.

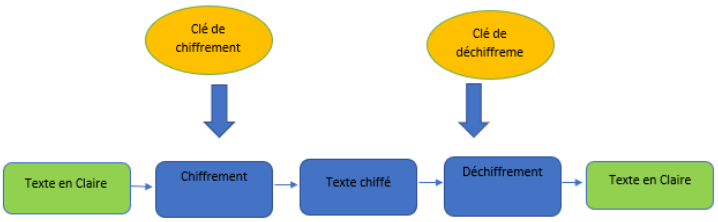


FIGURE 1.8 – Processus de chiffrement et déchiffrement [7].

- **Confusion :**

  La confusion est le désir de rendre la relation entre la clé de chiffrement et le texte chiffré autant que possible complexe [7].

- **diffusion :**

  La diffusion est une caractéristique qui permet de dissiper la redondance statistique dans un texte en clair en utilisant les statistiques du texte chiffré [7].

- **Substitution :**

  Les substitutions sont des substitutions de symboles ou de groupes de symboles qui sont utilisés pour créer de la confusion [7].

- **Permutation (transposition) :**

  Le chiffrement par permutation, également connu sous le nom de chiffrement par transposition, implique de modifier l'ordre des lettres.

  Le chiffrement par transposition implique de diviser le texte clair en blocs de taille identique. On utilise alors la même permutation pour chacun des blocs [7].

1.3.4 Objectifs de la cryptographie

La cryptographie consiste à examiner les méthodes mathématiques utilisées pour garantir la sécurité de l'information. Dans cette situation, la protection des données comprend des éléments tels que la confidentialité des informations, l'intégrité, l'authentification, la transmission des informations, la non-répudiation des données et la disponibilité des informations.

- **Confidentialité des informations :**

  assure que les informations transmises à un destinataire ne seraient déchiffrées que par celui-ci, et par aucun autre. Il est essentiel d'identifier de manière précise le destinataire et d'adopter une méthodologie qui rend l'information illisible pour tout autre destinataire que celui-ci [32].

- **Intégrité :**

  représente la méthode qui garantit que l'information n'a pas subi d'altération lors de son passage ou de son stockage sur le réseau [32].

- **L'authentification :**

  assure la vérification d'où provient un message et de qui est le destinataire. Ainsi, grâce aux dispositifs d'authentification d'un protocole, il est essentiel de pouvoir assurer l'identité des deux parties impliquées dans une communication [32].

- **La non-répudiation :**

  Il s'agit d'une propriété acquise grâce à des techniques cryptographiques qui empêchent une personne de nier avoir commis une action spécifique liée aux données [32].

- **La disponibilité :**

  L'objectif est de garantir l'accessibilité et la pérennité d'un système ou d'une donnée pendant la durée d'utilisation prévue [32].

1.3.5 Les différents types de cryptographie

- **Cryptographie classique :** La cryptographie traditionnelle relate une époque antérieure aux ordinateurs, où les principaux moyens employés étaient de substituer des caractères par d'autres et de les transposer dans des séquences différentes tout en préservant les instructions de cryptage ou de décryptage.
  En l'absence de cela, le système est totalement inefficace car tout le monde peut déchiffrer le message crypté.
  Ce type de cryptographie regroupe deux types de méthodes : la substitution et la transposition [8].

  – **Chiffrement par substitution :** Le chiffrement par substitution consiste à remplacer une ou plusieurs entités (habituellement des lettres) dans un message par une ou plusieurs autres entités.
    En général, on distingue plusieurs types de cryptosystèmes en fonction de leur substitution :

    * **Substitution mono-alphabétique :**

      Il s'agit de substituer chaque lettre du message par une lettre de l'alphabet différente [8].

      Exemple : le chiffre de césar on décale les lettres de 3 positions.

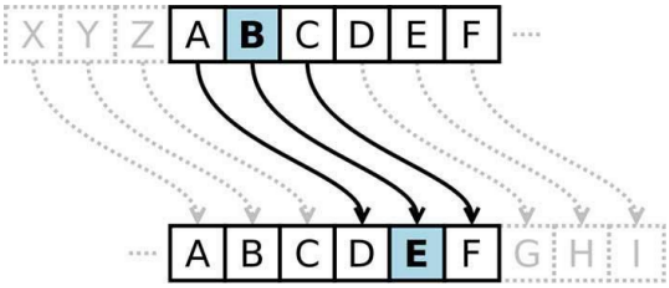


FIGURE 1.9 – exemple du chiffre de césar [8].

∗ **La substitution homophonique :**

Comme pour le précédent principe, à la différence près qu'à un caractère du texte en clair, on obtient plusieurs caractères dans le texte chiffré.

Par exemple, « A » peut être 5, 13, 25 ou 56 ; « B », peut être 7, 19, 31, ou 42 ; etc. Ce système est plus sûr, mais il est aussi vulnérable aux attaques des cryptanalystes ou des espions expérimentés [8].

∗ **Substitutions polyalphabétiques :**

Toutes les lettres du message en clair sont remplacés par une lettre nouvelle choisie dans un ou plusieurs alphabets aléatoires [8].

Exemple : le chiffre de Vigenere Il permet de substituer une lettre par une autre qui n'est pas toujours la même. Figure 1.10 represente un example.

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 1.10 – exemple du chiffre de Vigenere [8].

∗ **La substitution de polygrammes :**

les caractères du texte en clair sont chiffrés par blocs. Par exemple,on peut chiffrer "ABA" par "RTQ" tandis que "ABB" est chiffré par "SLL" [8].

– **Chiffrement par Transpositions :**

Dans le domaine du chiffrement par transpositions, les lettres d'un message sont réarrangées selon un ordre différent, en utilisant le principe mathématique des

permutations. Ce procédé offre diverses techniques, dont l'une des plus connues utilise deux perspectives géométriques distinctes [8].

Une méthode courante consiste à utiliser une bande de papyrus enroulée autour d'un cylindre appelé scytale :

* Écriture du texte longitudinalement : Le texte est soigneusement inscrit le long de la bandelette de papyrus une fois celle-ci enroulée autour du cylindre.
* Décryptage : Pour déchiffrer le message, il est impératif de disposer d'un cylindre ayant le bon diamètre, permettant ainsi de lire le texte dans son ordre original.

- **La cryptographie Moderne :**

  La cryptographie moderne se divise en deux catégories : les chiffrements symétriques et les chiffrements asymétriques.

  – **Cryptographie symétrique (à clés privés) :**

  On appelle également cryptographie symétrique la cryptographie à clés privées. Les informations sont chiffrées et déchiffrées à l'aide d'une seule clé de chiffrement, ce qui est appelé cryptage symétrique. Il est donc nécessaire que la clé soit partagée à la fois avec l'envoyeur et avec le destinataire [9]. La Figure 1.11 represente le chiffrement symétrique.

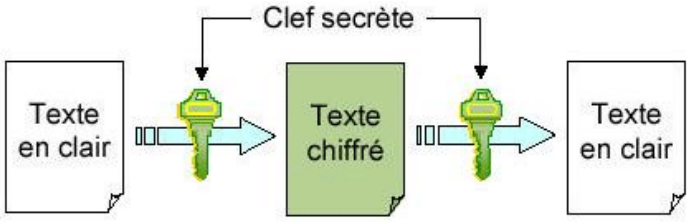


FIGURE 1.11 – Chiffrement symétrique [9]

Les principaux types de cryptographie symétrique actuellement employés se divisent en deux catégories principales : le chiffrement par bloc et le chiffrement de flux. Le tableau 1.3 ci-dessous présente la différence entre la Chiffrement en flux et chiffrement par bloc.

Chiffrement de flux	Chiffre de bloc
Chiffrer les données en blocs de longueur fixe.	Pendant que les données sont chiffrées, le système les conserve en mémoire, en attendant que des blocs complets soient prêts à être envoyés.
Chiffre les données un bit ou octet à la fois.	Chiffrer les données dans des blocs de longueur fixe.
utiliser 8 bits de la clé.	Utilise soit 64 bits ou plus de 64 bits de la clé.
Plus complexe que le chiffrement par blocs.	Plus simple que le chiffrement par flux.
Chiffrer les données en blocs de longueur fixe.	Lent et adapté aux applications hors ligne.

TABLE 1.3 – Chiffrement en flux vs chiffrement par bloc [19].

– **Cryptographie asymétrique (à clés publiques) :** Contrairement au cryptage symétrique, le cryptage asymétrique utilise une seule clé pour crypter les données et une autre pour les décrypter.

Le chiffrement asymétrique est aussi appelé chiffrement à clé publique, car la clé de chiffrement des informations est accessible à tous et peut être utilisée par de nombreuses personnes.

De son côté, la personne qui reçoit le message possède une clé privée correspondante, qui permet de décrypter le message [9]. Regarder la figure 4.2.

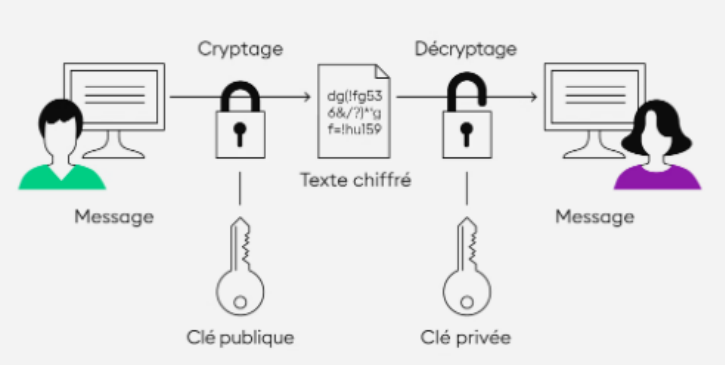


FIGURE 1.12 – Chiffrement asymétrique [9].

1.3.6 les méthodes de cryptage

- **AES (Advanced Encryption Standard) :** C'est un algorithme de chiffrement symétrique qui permet de chiffrer en même temps des blocs de données de 128 bits avec des clés de 128, 192 ou 256 bits. La clé de 256 bits traite les données en 14 tours, la clé de 192 bits en 12 tours et la clé de 128 bits en 10 tours.
  Toutes les tours sont composées de différentes étapes de substitution, de transposition, de mélange de texte clair, etc.
  Mettez en œuvre l'AES afin de garantir la sécurité du Wi-Fi, de chiffrer les applications mobiles,...etc [33].

- **RSA (Le chiffrement Rivest-Shamir-Adleman) :** L'algorithme de chiffrement asymétrique utilise la factorisation du produit de deux grands nombres premiers. Seule une personne qui connaît les nombres choisis peut saisir le message.
  Ce chiffrement est souvent employé pour assurer la confidentialité de la transmission des données entre deux points de communication [33].

- **DES (Data Encryption Standard) :** Cela représente une méthode de chiffrement symétrique et une version plus avancée de la technique DES qui permet de chiffrer des blocs de données avec une clé de 56 bits. Chaque bloc de données est chiffré trois fois selon la norme de triple chiffrement des données.
  Utilisez cette convention pour sécuriser les codes aux guichets automatiques des banques ainsi que les mots de passe UNIX [33].

- **Le chiffrement Blowfish :** Le chiffrement symétrique Blowfish consiste à séparer les messages en segments de 64 bits et à les chiffrer un par un. Blowfish est connu

pour sa vitesse, sa souplesse et sa résistance. Il fait partie du domaine public et est donc accessible à tous.

Pour protéger vos transactions sur les plateformes de commerce électronique, vous pouvez utiliser Blowfish [33].

- **Le chiffrement préservant le format (FPE) :** Le chiffrement de vos données est assuré par un algorithme symétrique qui maintient le format et la longueur de vos données.

  Par exemple, si le numéro de téléphone du client est le 08 13 20 49 01, FPE le modifie en le transformant en 08 38 61 92 40. Il n'y a donc pas de changement dans le format et la longueur, mais les données ont été protégées par des chiffres [33].

- **IDEA (International Data Encryption Algorithm) :** C'est un algorithme de chiffrement par blocs symétrique, similaire au DES. L'algorithme de chiffrement et de déchiffrement est le même. Il est compatible avec des fichiers de texte en clair de 64 bits et une clé de 128 bits [33].

- **ECC (Elliptic Curve Cryptography) :** C'est une méthode de cryptographie à clé publique récente, plus performante que le chiffrement RSA.

  La vitesse est accrue grâce à l'emploi de clés plus courtes. L'utilisation de ce chiffrement asymétrique permet de renforcer la sécurité de vos communications en ligne en utilisant les protocoles SSL/TLS.

  Utilisez le chiffrement unidirectionnel d'e-mails et les signatures électroniques pour les crypto-monnaies en utilisant ECC [33].

1.3.7 L'attaque

Au fil des années, de nombreuses attaques potentielles contre les crypto-systèmes ont été identifiées, ce qui rend difficile la constitution d'une liste exhaustive.

Deux catégories principales d'attaques se distinguent en revanche : les attaques actives et les attaques passives.

- **Attaques actives :** En ce qui concerne les attaques actives, l'ennemi cible directement les informations pour compromettre l'intégrité des données, l'authentification et la confidentialité. Ces attaques peuvent prendre diverses formes,

notamment en altérant la transmission du message sur le canal.

Par exemple, l'attaquant a la possibilité de modifier le contenu du message en suppression, en ajout ou en modifiant des séquences spécifiques. En outre, il a la capacité de perturber la transmission en retardant ou en empêchant l'envoi du message. Dans certaines situations, l'ennemi peut aussi essayer de mettre en péril la sécurité en répétant délibérément l'envoi du message [34].

- **Attaque passives :** Dans le contexte des attaques passives, l'ennemi utilise une méthode plus discrète en observant les données qui circulent sur le canal, sans les modifier.

  Ces attaques visent principalement à obtenir des données sur le cryptosystème sans perturber son fonctionnement. Cela englobe la collecte de données confidentielles comme le contenu du message ou la clé secrète utilisée lors du processus de cryptage [34].

1.4 Conclusion

Dans ce chapitre, nous avons présenté un aperçu général des images et du chiffrement, ainsi que des concepts fondamentaux. Tout d'abord, nous avons donné une définition des images numériques. Les caractéristiques telles que les pixels, les dimensions, le BPP et la résolution sont expliquées en détail. De plus, les types d'images (matricielles et vectorielles) ainsi que les représentations de couleur (noir et blanc, niveaux de gris, couleur RGB) sont également abordés.

La section sur la cryptographie présente des définitions claires, détaillant la cryptographie, la cryptanalyse, le cryptosystème et divers termes associés. Les objectifs de la cryptographie, tels que la confidentialité, l'intégrité, l'authentification, le non-répudiation et la disponibilité, sont soulignés. Le chapitre explore également les différents types de cryptographie, notamment la cryptographie classique et moderne, en mettant en lumière des méthodes telles que le chiffrement par substitution et transposition. Les algorithmes importants, tels que DES, AES, RSA, DSA et IDEA, sont discutés. Enfin, nous avons parlé de deux catégories d'attaques : les attaques actives et les attaques passives.

Chapitre 2

Les systèmes chaotiques.

2.1 Introduction

La théorie du chaos, initiée par le mathématicien Henri Poincaré, est un outil puissant pour comprendre de nombreux systèmes complexes. Henri Poincaré en a posé les bases théoriques.

Plus tard, dans les années 1960, Edward Lorenz, un météorologue américain, a relancé l'intérêt pour la théorie du chaos. Ses travaux, entrepris en 1961, ont joué un rôle fondamental dans le développement de cette théorie.

La théorie du chaos est une branche des mathématiques qui se concentre sur le comportement des systèmes dynamiques. Elle trouve de nombreuses applications dans divers domaines tels que la météorologie, la physique, l'informatique, l'ingénierie, la politique, les affaires, les sciences sociales, l'économie, la philosophie et la biologie.

2.2 Théorie chaotique

Rappel Historique :

Les fonctions chaotiques ont vu le jour au début du XXe siècle avec les travaux d'Henri Poincaré sur la physique des corps célestes.

C'est toutefois dans les années 1960, avec l'apparition des ordinateurs, que cette théorie a été approfondie. La nécessité de réaliser de nombreuses opérations de calcul a été comblée par la puissance de calcul informatique disponible à cette époque, ce qui n'était pas réalisable auparavant.
En 1963, le météorologue Edward Lorenz a démontré le caractère chaotique des conditions météorologiques. Il a mis en évidence que de légères variations dans l'état initial pouvaient entraîner des évolutions totalement différentes, conceptualisant ainsi le fameux postulat du battement d'aile de papillon.
L'intérêt pour les travaux de Poincaré a été renforcé par cette découverte, et en 1975, le mathématicien James Yorke a parlé pour la première fois du chaos.
Depuis lors, la théorie du chaos s'est répandue dans divers domaines d'application, tels que la psychologie, l'économie, la sociologie, la physique, la biologie et la sécurité de l'information, ...etc [35].

2.2.1 Définition du chaos

Le concept de chaos, selon les scientifiques, ne signifie pas un désordre, mais plutôt une idée d'imprévisibilité. Il s'agit de l'incapacité de prédire une évolution à long terme en raison de la sensibilité extrême de l'état final aux conditions initiales.
Ainsi, on qualifie un système dynamique de chaotique lorsqu'il dépend de multiples paramètres et présente une sensibilité remarquable aux conditions initiales. Ces systèmes ne sont pas gouvernés ou modélisés par des équations linéaires. Pourtant, ils ne sont pas nécessairement aléatoires [36].

2.2.2 Les systèmes dynamiques chaotiques

Un système dynamique chaotique est déterministe, mais il présente un comportement en apparence aléatoire en raison de sa dépendance et de sa sensibilité extrême à ses conditions initiales. Étant donné qu'il est impossible en pratique de spécifier les conditions initiales avec une précision infinie, le comportement d'un système chaotique devient imprévisible, ressemblant ainsi à du bruit.
L'application de cette théorie dans divers domaines de recherche permet d'obtenir une compréhension fondamentale des systèmes dynamiques non linéaires.
Trois types de systèmes dynamiques sont pris en compte dans la théorie chaotique[37] :

- **Systèmes dynamiques autonomes.**
- **Les systèmes dynamiques non autonomes :**Les systèmes non autonomes dynamiques se distinguent des systèmes autonomes. Étant donné que le champ de vecteur est une fonction de x et de t, il est impossible de placer l'état initial de manière arbitraire à zéro.
- **Des systèmes dynamiques de temps discret :** sont caractérisés par l'équation d'état, $X_{k+1} = g\left(X_k\right), K = 0, 1, 2, \ldots\ldots$, où $X_k \in R_n$ est connu sous le nom d'état, et g trace l'état X_k au prochain état X_{K+1}.en commençant par un état initial X_0les applications répétées de la carte créent une séquence de points $\{X_K : K+ = 0, 1, 2, \ldots\}$ connue sous le nom d'orbite du système à temps discret. La théorie chaotique repose sur le troisième type de système dynamique lorsqu'il opère dans un état chaotique [38].

2.3 Caractéristiques du chaos

2.3.1 Non linéarité

Le comportement instable d'un système chaotique est causé par les non-linéarités qui y sont présentes. On peut définir un système chaotique comme un système dynamique non linéaire. Il est important de noter qu'un système linéaire ne peut pas exhiber de comportement chaotique [39].

2.3.2 L'irrégularité

L'irrégularité résulte de l'organisation formée d'un nombre infini de modèles périodiques instables (mouvement).
Cet ordre dissimulé constitue l'infrastructure des systèmes chaotiques [40].

2.3.3 Déterminisme

Le déterminisme signifie que le système ne dépend pas du hasard et ne contient aucun paramètre ou entrée stochastique. Tous les systèmes dont l'évolution est déterminée par un ensemble d'équations différentielles non linéaires possèdent cette caractéristique. À la différence des phénomènes aléatoires où la trajectoire d'une particule quelconque est impossible à prédire, les systèmes dynamiques chaotiques, même s'ils semblent au départ aléatoires, sont régis par des équations particulières qui rendent compte du phénomène [38].

2.3.4 Sensibilité aux conditions initiales

La dépendance sensible aux conditions initiales signifie que de petites variations dans les valeurs initiales des variables se développent avec le temps, produisant des différences imprévisibles à mesure que nous calculons l'orbite ou le trajectoire [10].
Ceci est illustré par l'exemple dans la figure 2.1 :

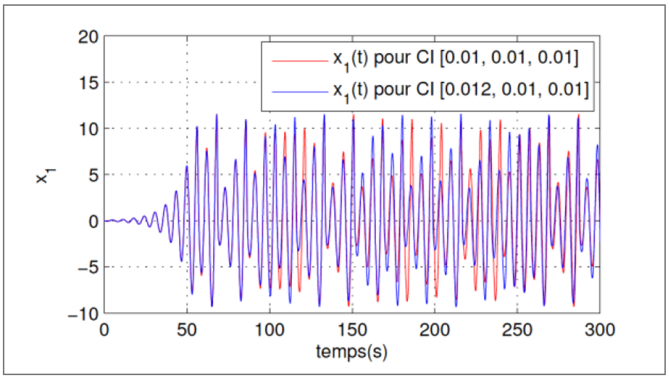


FIGURE 2.1 – La propriété de sensibilité aux conditions initiales est illustrée sur l'état x1 [10].

2.3.5 Sensibilité aux paramètres

Un changement mineur des paramètres de contrôle donne lieu à deux trajectoires chaotiques très différentes, même si elles partent de la même condition initiale. Les paramètres exercent un impact significatif sur le comportement dynamique du système chaotique, influençant notamment sa stabilité. Ainsi, le système peut se retrouver dans un état différent dès que les paramètres sont modifiés [10]. Comme le montre l'exemple dans la figure 2.2.

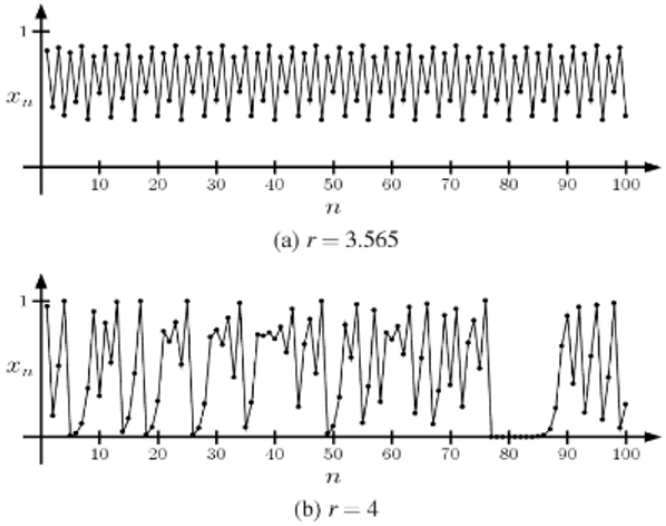


FIGURE 2.2 – Exemple pour r=3.565 et r=4 [10].

2.3.6 l'imprévisibilité

L'imprévisibilité résulte de la sensibilité aux conditions initiales, qui ne peuvent être connues qu'à un degré de précision déterminé [41].

2.3.7 le chaos et l'aléatoire

Le point le plus important de la compréhension du chaos est la distinction entre le chaos et l'aléatoire. Souvent, on tend à attribuer l'imprédictibilité d'un phénomène à la multitude de paramètres impliqués dans sa description. Cela conduit à adopter une approche probabiliste qui, même si elle est satisfaisante, conserve par définition une certaine marge d'aléatoire.

Cependant, en ce qui concerne le chaos, la situation diffère. Les systèmes chaotiques peuvent adopter un comportement qui semble aléatoire, mais ce comportement est en réalité déterministe et est décrit de manière précise par des équations non linéaires purement déterministes. En d'autres termes, il est possible de comprendre ces systèmes chaotiques en utilisant des outils mathématiques qui offrent une approche précise et certaine [31].

2.3.8 Diagramme de Bifurcation

Un graphique appelé tracé de bifurcation vous permet d'évaluer rapidement toutes les solutions du système et sa stabilité en fonction des variations dans l'un de ses paramètres. Il peut aussi identifier des valeurs spécifiques de paramètres qui induisent des bifurcations. Il expose des intervalles où les solutions asymptotiques évoluent continuellement avec le paramètre, et il classe les valeurs du paramètre sur l'axe des abscisses et les valeurs d'une des variables d'état sur l'axe des ordonnées [42].

2.3.9 Exposants de Lyapunov

L'exposant de Lyapunov (LE) est un outil permettant de mesurer la sensibilité de la carte chaotique aux légère changements dans les conditions initiales et les paramètres de contrôle.
La carte chaotique avec un LE positif démontre un bon comportement chaotique. Plus la valeur LE est élevée indique une meilleure sensibilité de la carte à sa valeur initiale [43]. L'exposant de Lyapunov d'un système non linéaire différentiable $x_{i+1} = f(x_i)$ peut être calculé comme suit :

$$\lambda = \lim_{n\to\infty} -\frac{1}{n}\sum_{i=0}^{n-1} \ln|f'(x_i)|$$

Où λ est l'exposant de Lyapunov, et n est le nombre d'itérations.

2.4 Définition mathématique de Carte chaotique

La carte chaotique fait partie des systèmes dynamiques où le temps est discret plutôt que continu.

On appelle ces systèmes des relations de récurrence, des fonctions itérées ou simplement des cartes (Map en anglais) [44].

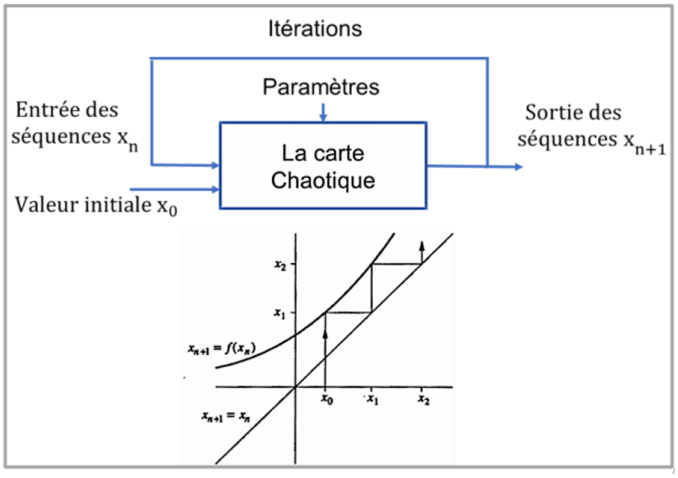


FIGURE 2.3 – .Création d'une carte par itération [11].

Par exemple, la fonction itérée d'un intervalle I = [a, b] est :

$$X\mathrm{n}+1 = f\left(Xn, a_i\right).$$

La séquence $x0, x1, x3, \ldots$ est appelée l'orbite de f. $x0$, est appelée la valeur initiale de l'orbite, ai sont les paramètres de trajectoire de x est la séquence :

$$x0 = x, x1 = f(x), \ldots, xn = fn(x), \ldots$$

Où n est le nombre d'itérations.

$$x1 = f(x0), x2 = f(x1) = f(f(x0)) \ldots, xn = fn(x0), \ldots$$

Si $f(p) = p$, p est un point fixe p. Si $f^n(p) = p$ p est un point fixe périodique de période n .

f' est considérée comme une carte chaotique lorsque :

1. La densité des points périodiques est élevée dans I.
2. Transitivité : Une fois que deux sous-intervalles ouverts $U1$ et $U2$ sont présents dans I, il y a un point $x_0 \in U1$ et un $n > 0$ tel que $f^n(x_0) \in U2$.
3. Dépendance sensible aux conditions initiales : Il y a une constante de sensibilité, que nous représenterons par $\beta > 0$, telle que pour tout $x_0 \in I$ et tout intervalle ouvert U autour de x_0, il existe $y_0 \in U$ et $n > 0$ tels que $f^n(x_0) - f^n(y_0) > \beta$ [11].

   La figure 2.3 décrit la méthode d'itération graphique utilisée pour représenter les orbites.

   En cas de condition initiale x_0 est une condition initiale, nous partons d'abord du point (x_0, x_0) sur la ligne $x = y$ et nous nous déplaçons verticalement jusqu'à l'intersection f au point (x_0, x_1). Par la suite, nous nous déplaçons horizontalement jusqu'à (x_1, x_1).

   En continuant de cette manière, nous pouvons trouver l'orbite entière [44].

   x_0 est un point fixe stable si $|f'(x_0)| < 1$, où $|f'(x_0)|$ est appelé le coefficient de stabilité de x_0. x_0 est un point fixe instable si $|f'(x_0)| > 1$.[6]

2.4.1 L'utilisation du chaos

Dans différents domaines, on a pu constater le chaos, pour ne citer que quelques exemples :

- dans la nature,
- dans la météo et le climat,
- dans la croissance des populations,en écologie et en économie.

Il a aussi fait l'objet d'observations en laboratoire dans divers systèmes comme :

- les circuits électriques,
- les lasers,
- les réactions chimiques,
- la dynamique des fluides,
- les systèmes mécaniques et les dispositifs magnéto-mécaniques [16].

2.5 Certaines catégories de cartes chaotiques

Les cartes chaotiques sont des systèmes dynamiques qui sont caractérisés par des relations de récurrence. En général, elles sont utilisées pour représenter des phénomènes complexes et non linéaires, s'appliquant ainsi à divers domaines. Nous fournirons quelques exemples de cartes chaotiques :

2.5.1 La carte logistique

La carte logistique est une cartographie polynomiale qui fonctionne à l'aide d'équations dynamiques non linéaires et très simples.
La carte chaotique logistique est représentée par l'équation suivante :

$$x_{n+1} = r \cdot x_n \cdot (1 - x_n) \tag{2.1}$$

Dans l'intervalle [0, 1], x est une variable et n est le nombre d'itérations, tandis que r est un nombre défini dans l'intervalle [0, 4].
La carte logistique peut être utilisée pour représenter des phénomènes complexes dans différents domaines tels que la physique, la biologie et l'ingénierie [12].

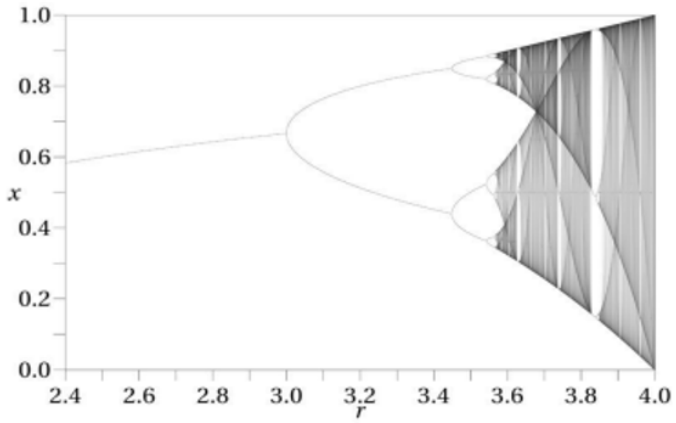


FIGURE 2.4 – Le diagramme de la bifurcation de la carte logistique [12].

2.5.2 La carte Skew tent

la carte Skew tent est une carte non linéaire en morceaux, telle que décrite par l'équation ci-dessous :

$$x(n) = f(x(n-1), p) = \begin{cases} \frac{x(n-1)}{p} & \text{si } 0 \leq x(n-1) \leq p \\ \frac{1-x(n-1)}{1-p} & \text{si } p < x(n-1) \leq 1 \end{cases} \tag{2.2}$$

Le paramètre de contrôle, p, varie dans l'intervalle suivant : $p \in [0, 1]$.

2.5.3 La carte de PWLCM (Piecewise Linear Chaotic Maps)

PWLCM (Piecewise Linear Chaotic Map) est considéré comme particulièrement approprié dans la conception de cryptosystèmes basés sur le chaos [45].
L'équation suivante donne la représentation du système PWLCM.

$$x(i+1) = F_p(x_i) = \begin{cases} \frac{x_i}{p}, & \text{si } 0 \leq x_i \leq p \\ \frac{x_i - p}{0.5 - p}, & \text{si } p < x_i \leq 0.5 \\ F_p(1 - x_i), & \text{si } 0.5 < x_i \leq 1 \end{cases} \tag{2.3}$$

2.5.4 La carte Sine map

La fonction *Sine map* est une autre fonction chaotique fréquemment employée dans la littérature, définie par l'équation suivante :

$$x_{n+1} = a \cdot \frac{\sin(\pi \cdot x_n)}{4} \tag{2.4}$$

Où le paramètre $a \in [0, 4]$ et $x_n \in [0, 1]$.

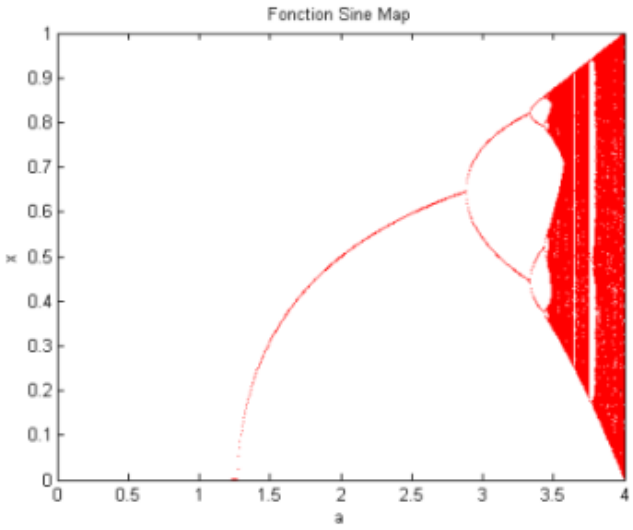


FIGURE 2.5 – Diagramme de bifurcation pour la fonction Sine Map [13].

Selon la figure 2.5, cette fonction présente un comportement chaotique similaire à celui de la fonction logistique [13].

2.5.5 Combinaison de Cartes Chaotiques (Les fonction hybride)

Une fonction hybride dans le contexte des cartes chaotiques est une fonction qui combine deux ou plusieurs cartes chaotiques différentes pour produire un nouveau comportement chaotique. Cette combinaison peut augmenter la complexité du système et améliorer la sécurité dans les applications de chiffrement. Voici comment elle pourrait être employée :

La fonction chaotique SinLog :

Cette fonction SinLog est basée sur deux fonctions chaotique décrites précédemment par les équations 2.1 et 2.4. Cette nouvelle fonction est définie par l'équation suivante :

$$x_{n+1} = r \cdot \sin\left(\pi \cdot x_n \cdot (1 - x_n)\right) \tag{2.5}$$

La figure 2.6 ci-dessous met en évidence son comportement désordonné.

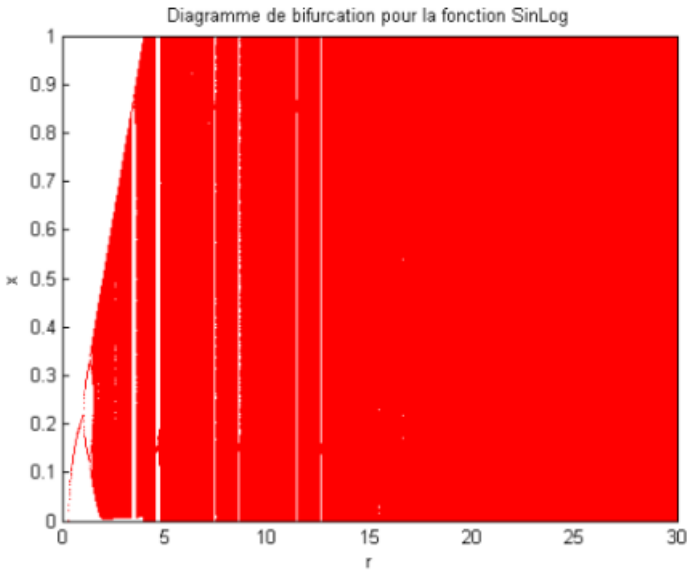


FIGURE 2.6 – Diagramme de Bifurcation de la fonction SinLog [13].

Il est évident que la fonction SinLog a un comportement différent de celui des deux fonctions mentionnées ci-dessus. La zone chaotique de SinLog est largement correspondante, ce qui revêt une grande importance pour un système de cryptage chaotique [13]. Afin de mieux illustrer les différentes valeurs du paramètre a, nous exposons dans la figure 2.7 ci-dessous le schéma de l'exposant de Lyapunov correspondant.

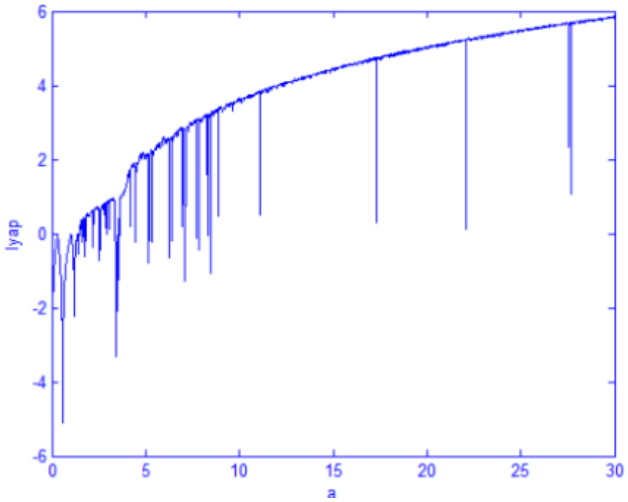


FIGURE 2.7 – Diagramme de lyapunov de la fonction SinLog [13].

2.6 Les cartes chaotiques multidimensionnelles

Les cartes chaotiques multidimensionnelles sont des systèmes dynamiques définis par des relations de récurrence.
Les paramètres du système et les conditions initiales agissent comme une clé privée dans un cryptosystème chaotique.
Il existe une variété importante de cartes chaotiques, dont certaines présentent des ordres fractionnaires dans des espaces de dimensions différentes, tels que 1D, 2D et 3D :

- Les cartes chaotiques unidimensionnelles (1D) discrètes telles que Logistic, Skew tent...
- Les cartes chaotiques bidimensionnelles (2D) comme Cat, Hénon et Baker...
- Les cartes chaotiques tridimensionnelles continues (3D) telles que Lorenz, Chua et Rössler [44].

2.6.1 Les cartes chaotiques unidimensionnelles (1D)

Une carte chaotique 1D est une fonction mathématique qui décrit l'évolution d'un système dynamique à une seule variable. Elle prend une valeur d'entrée (x) et produit une valeur de sortie (f(x)) qui représente l'état du système à l'étape suivante.

Les avantages :

- **Simplicité :** Les cartes 1D sont relativement faciles à comprendre et à analyser. Elles offrent une représentation visuelle intuitive du comportement du système.
- **Calculs plus rapides :** Les calculs impliquant les cartes 1D sont généralement plus rapides que ceux impliquant des cartes multidimensionnelles.
- **Coût de calcul faible :** Les cartes 1D nécessitent moins de ressources informatiques pour être calculées, ce qui les rend plus efficaces pour des applications en temps réel.
- **Compréhension de base :** Elles permettent d'acquérir une compréhension de base des systèmes chaotiques et de leurs propriétés.

Les inconvénients :

- **Limites de modélisation :** Les cartes 1D ne peuvent pas modéliser des systèmes complexes avec plusieurs variables. Elles ne peuvent représenter que des systèmes avec une seule variable dynamique.
- **Manque de complexité :** Les cartes 1D ne peuvent pas générer des séquences aussi complexes que les cartes multidimensionnelles.
- **Manque de réalisme :** Elles ne peuvent pas capturer la complexité des systèmes réels qui impliquent souvent plusieurs variables interagissant entre elles.
- **Prédictions limitées :** Les prédictions basées sur des cartes 1D peuvent être moins précises et moins fiables que celles basées sur des cartes multidimensionnelles.

2.6.2 Les cartes chaotiques multidimensionnelle (MD)

Une carte chaotique multidimensionnelle est une fonction mathématique qui décrit l'évolution d'un système dynamique à plusieurs variables. Elle prend un vecteur d'entrée (x1, x2, ..., xn) et produit un vecteur de sortie (f1(x1, x2, ..., xn), f2(x1, x2, ..., xn), ..., fn(x1, x2, ..., xn)) qui représente l'état du système à l'étape suivante.

Les avantages :

- **Modélisation plus réaliste :** Les cartes multidimensionnelles peuvent modéliser des systèmes complexes avec plusieurs variables interagissant entre elles. Elles offrent une représentation plus réaliste des systèmes réels.
- **Prédictions plus précises :** Les prédictions basées sur des cartes multidimensionnelles peuvent être plus précises et plus fiables que celles basées sur des cartes 1D.
- **Capacité à capturer des comportements complexes :** Elles peuvent capturer des comportements complexes et imprévisibles qui ne peuvent pas être modélisés par des cartes 1D.

Les inconvénients :

- **Complexité :** Les cartes multidimensionnelles sont plus complexes à comprendre et à analyser que les cartes 1D.
- **Calculs plus longs :** Les calculs impliquant les cartes multidimensionnelles sont généralement plus longs et plus complexes que ceux impliquant des cartes 1D.
- **Difficulté d'interprétation :** L'interprétation des résultats obtenus avec des cartes multidimensionnelles peut être difficile en raison de la complexité des systèmes qu'elles modélisent.
- **Exigences en ressources informatiques plus élevées :** Les cartes MD nécessitent davantage de ressources système (mémoire, puissance de calcul) pour leur implémentation, ce qui peut être un défi pour les systèmes embarqués ou les dispositifs à faibles ressources.

2.7 Conclusion

Dans ce chapitre, nous avons exploré Le système chaotique. Nous avons commencé par retracer l'historique de la théorie chaotique, depuis les travaux pionniers d'Henri Poincaré jusqu'aux contributions modernes dans divers domaines scientifiques. Ensuite, nous avons défini le chaos comme un comportement imprévisible mais déterministe, caractérisé par une sensibilité extrême aux conditions initiales. Nous avons également examiné les caractéristiques du chaos, telles que la non-linéarité, l'irrégularité, le déterminisme, la sensibilité aux conditions initiales et aux paramètres, ainsi que l'imprévisibilité. Nous avons ensuite abordé différents types de systèmes dynamiques chaotiques, notamment les systèmes autonomes et non autonomes, ainsi que les systèmes à temps discret. Nous avons discuté de l'utilisation de diagrammes de bifurcation et d'exposants de Lyapunov pour étudier le comportement chaotique des systèmes. Ensuite, nous avons examiné la définition et l'utilisation des cartes chaotiques, en mettant en évidence des exemples populaires tels que la carte logistique, la carte Skew tent, la carte PWLCM, ainsi que les cartes chaotiques multidimensionnelles. Nous avons souligné les avantages et les inconvénients de chaque type de

carte chaotique. En conclusion, le système chaotique offre un cadre puissant pour comprendre et modéliser une grande variété de phénomènes dynamiques. Son caractère imprévisible mais déterministe en fait un outil précieux dans de nombreux domaines scientifiques et technologiques.

Chapitre 3

Cryptage des image

Le cryptage d'images est une technique essentielle pour sécuriser les données visuelles en les rendant illisibles aux personnes non autorisées. Tout comme la cryptographie traditionnelle protège les données textuelles, le cryptage d'images vise à sécuriser les images numériques contre les accès non autorisés. Cette discipline de la sécurité informatique utilise diverses techniques et méthodes pour transformer une image en une forme chiffrée, tout en préservant sa structure et ses caractéristiques visuelles. Le but principal du cryptage d'images est de garantir la confidentialité des données visuelles, qu'il s'agisse de photographies, d'illustrations, de captures d'écran ou d'autres types d'images. Il est largement utilisé dans des domaines sensibles comme la sécurité nationale, la médecine, le commerce électronique et la protection des données personnelles.

3.1 Chiffrement d'images

Le but du cryptage d'images est d'assurer la sécurité visuelle du contenu d'imagerie. Lorsque l'intégralité du contenu original est cryptée, on parle de cryptage « total ». L'image est protégée après l'opération de cryptage. Dans ce cas, les informations liées à l'image en clair ne peuvent pas être extraites de l'image cryptée. Lorsqu'il n'y a que des données partielles à choisir, on utilise le cryptage « sélectif ». Enfin, lorsque seule une zone spécifique d'une image est chiffrée et que les pixels en dehors de cette zone restent clairs, on parle de cryptage « partiel ».

La figure 3.1 illustre les différences entre ces trois types de chiffrement.

FIGURE 3.1 – a) Image originale, b) Chiffrement total, c) Chiffrement sélectif, d) Chiffrement partiel [14].

De plus, les méthodes de chiffrement d'images doivent vérifier deux propriétés :

- Le format : le format de l'image cryptée doit être le même que le format de l'image originale.
- La taille : Il est essentiel que la taille de l'image chiffrée soit la même que celle de l'image originale.

La première propriété indique que les données doivent être structurées de la même manière avant et après le chiffrement. Par conséquent, les méthodes de chiffrement traditionnelles ne peuvent pas être appliquées directement aux images sans tenir compte des particularités du format de l'image. Concernant la deuxième propriété, nous observons qu'une augmentation limitée de la taille des données après chiffrement peut être tolérée dans certaines applications [14].

3.2 Domaines de cryptographie d'images

Le cryptage des images peut être divisé en deux domaines : le domaine spatial et le domaine fréquentiel.

3.2.1 domaine spatial

Dans le domaine spatial, le chiffrement est appliqué directement aux images. Les techniques utilisées impliquent une manipulation directe des pixels qui composent l'image. Ces algorithmes de chiffrement altèrent la relation entre les pixels, rendant les images cryptées complètement inintelligibles. Cependant, il est possible de récupérer intégralement les pixels d'origine par un processus inverse, sans perte d'information. Les méthodes actuelles de chiffrement d'images peuvent être classées en deux catégories principales en fonction de leur approche du traitement des pixels de l'image :

- **Première catégorie :** Chaque pixel est perçu comme l'unité de base de l'image. Chaque pixel est l'unité fondamentale de l'image et l'image est vue comme une grille de pixels.
- **Deuxième catégorie :** Chaque pixel est subdivisé en bits, et les opérations de cryptage sont effectuées sur ces bits. Prenons l'exemple d'une image en niveaux de gris où chaque pixel est habituellement représenté par 8 bits [46].

3.2.2 domaine fréquentiel

Dans le domaine du cryptage d'images basé sur la fréquence, les schémas de cryptage utilisent habituellement une transformation pour modifier la fréquence de l'image. Par conséquent, la reconstruction des pixels de l'image originale lors du décryptage entraîne généralement une perte d'information [46].

3.3 la confusion et la diffusion dans le cryptage des images

3.3.1 Algorithme basé sur la transposition (Confusion)

La transposition, également appelée confusion, consiste à réarranger les éléments de l'image en clair. Ce réarrangement est généralement effectué par permutation [16].

3.3.2 Algorithme basé sur la transformation des valeurs(Diffusion)

L'algorithme basé sur la transformation des valeurs, appelé diffusion, modifie la valeur de chaque pixel de l'image. La nouvelle valeur est calculée en appliquant un algorithme spécifique à chaque pixel. En essence, l'algorithme est une opération mathématique qui prend en entrée la valeur d'un pixel, la traite avec des formules spécifiques et produit une nouvelle valeur pour ce pixel [16].

3.4 Substitution

La substitution est l'une des principales techniques utilisées dans le chiffrement d'images, en complément de la diffusion.

Dans le chiffrement d'images, la substitution consiste à remplacer chaque pixel de l'image par une nouvelle valeur. Voici les principes de base de cette méthode :

3.4.1 Substitution Mono-alphabétique

Chaque pixel ou groupe de pixels est remplacé par un autre selon une table de correspondance unique. Par exemple, si nous avons une image en niveaux de gris, chaque valeur de pixel (disons de 0 à 255) pourrait être remplacée par une autre valeur selon une table de substitution prédéfinie.

3.4.2 Substitution Poly-alphabétique

Contrairement à la substitution mono-alphabétique, la substitution poly-alphabétique utilise plusieurs tables de correspondance. Cela signifie que la même valeur de pixel pourrait être chiffrée différemment en fonction de sa position dans l'image ou d'autres critères [47].

3.4.3 Substitution Homophonique

Pour les pixels ou valeurs qui apparaissent fréquemment, plusieurs valeurs de substitution peuvent être utilisées. Cela rend l'analyse de fréquence plus difficile pour

un attaquant, car il ne peut pas se baser sur la fréquence d'apparition d'une valeur pour déchiffrer l'image [47].

3.4.4 Substitution par Permutation

Cette méthode diffère de la substitution pure en ce qu'elle implique une permutation des pixels ou des blocs de pixels dans l'image. Cela peut être combiné avec la substitution pour augmenter la complexité du chiffrement [47].

3.5 Permutation

La permutation d'une image consiste à déplacer une partie de l'image. Il existe trois méthodes principales pour réaliser ce processus :

3.5.1 Permutation binaire (permutation des bits)

Une image est représentée par un tableau de pixels, où chaque pixel en 8 bits correspond à 256 niveaux de gris. Dans cette méthode de permutation, les bits de chaque pixel de l'image sont échangés selon une clé sélectionnée à partir d'un ensemble de clés, en utilisant un générateur d'index pseudo-aléatoire [48].

3.5.2 Permutation par pixel

Dans ce schéma (voir figure 3.2), des groupes de pixels sont extraits de l'image. Chaque groupe de pixels est ensuite permuté en utilisant une clé choisie parmi un ensemble de clés disponibles. Le processus de chiffrement et de déchiffrement est similaire à celui de la permutation de bits, où la longueur du groupe de pixels correspond à celle de la clé utilisée [48].

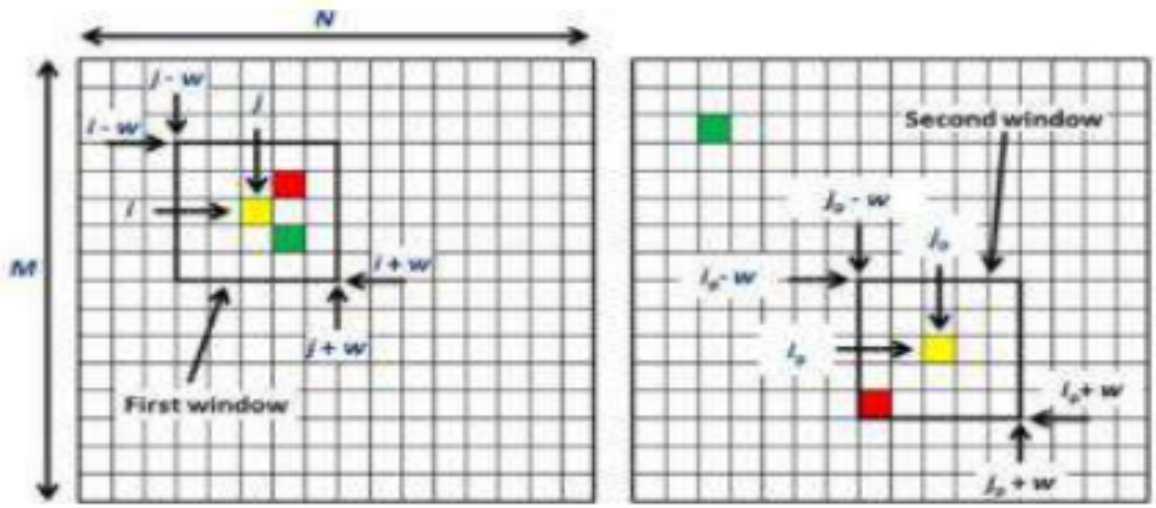


FIGURE 3.2 – Exemple sur la permutation pixel [15].

3.5.3 Permutation par bloc

En utilisant cette méthode, l'image est divisée en blocs. Un groupe de ces blocs est extrait de l'image, puis permuté de manière similaire aux permutations de bits et de pixels. Pour assurer un cryptage efficace, la taille du bloc doit être relativement petite, car si le bloc est trop petit, l'objet et ses bords ne seront pas visibles [48].

3.6 Les méthodes de chiffrement

Les méthodes de chiffrement classiques peuvent ne pas être les candidats les plus souhaitables pour le chiffrement d'images, en particulier pour les applications de communication rapide et en temps réel, pour deux raisons principales :

- la forte corrélation entre les pixels d'images .
- et l'énorme volume de données .

Pour cette raison, de nombreuses méthodes de cryptage d'images ont été proposées en utilisant différentes technologies telles que :

3.6.1 Encodage ADN et règle de complémentarité

Le séquençage de l'ADN est le processus utilisé pour cartographier la séquence nucléotidique formant un brin d'ADN.

Quatre bases, adénine (A), thymine (T), guanine (G) et cytosine (C), forment les éléments constitutifs du code génétique. "A" est lié à "T" et "G" est lié à "C".

Nous savons que chaque pixel d'une image numérique peut être exprimé par des nombres binaires sur 8 bits.

Comme les nombres binaires "0" et "1" sont complémentaires, "00" et "11" ainsi que "01" et "10" sont également complémentaires.

Si nous utilisons les quatre désoxyribonucléotides "A", "T", "G" et "C" pour représenter les nombres binaires "00", "11", "01" et "10", respectivement, alors chaque pixel peut être encodé dans une chaîne de nucléotides.

Par exemple, la valeur de gris d'un pixel d'une image numérique est 228, et le binaire correspondant à cette valeur est "11100100". Selon les règles ci-dessus, la chaîne de nucléotides qui correspond à ce binaire est "TCGA".

Il existe 24 types de combinaisons pour les quatre nucléotides. Cependant, seules huit combinaisons de codage conviennent au principe de complémentarité [20]

Le tableau ci-dessous résume ces règles.

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

TABLE 3.1 – Les règles de l'encodage de l'ADN [20].

Nous supposons que la taille de l'image en niveaux de gris originale I est $M \times N$, transformons I en une matrice binaire I', puis sélectionnons de manière aléatoire l'une des huit combinaisons de codage d'ADN pour coder I'.

La matrice codée est appelée I''.

Enfin, I'' est convertie en une séquence unidimensionnelle X, qui peut être exprimée comme suit :

$$X = \{x_1, x_2, x_3, ..., x_{4MN}\}, \quad x_i \in \{A, T, G, C\} \tag{3.1}$$

Selon le principe de la base complémentaire, nous définissons la chaîne nucléotidique x_i des nucléotides de codage comme suit :

$$\begin{aligned} &x_i \neq P(x_i) \neq P(P(x_i)) \neq P(P(P(x_i))), \\ &x_i = P(P(P(\neg(x_i)))) \end{aligned} \tag{3.2}$$

où $P(x_i)$ et x_i sont complémentaires ; en d'autres termes, $P(x_i)$ et x_i forment une paire de paires de bases.

Ces paires de bases doivent satisfaire aux conditions de la correspondance injective. Selon (2), il existe six types de combinaisons complémentaires rationnelles de paires de bases :

$$(AT)(TC)(CG)(GA),$$
$$(AT)(TG)(GC)(CA),$$
$$(AC)(CT)(TG)(GA),$$
$$(AC)(CG)(GT)(TA),$$
$$(AG)(GT)(TC)(CA),$$
$$(AG)(GC)(CT)(TA).$$

Pendant la diffusion des pixels, les nucléotides seront substitués en utilisant la règle de complémentarité de l'ADN.

Nous sélectionnons de manière aléatoire une règle parmi les six disponibles pour réaliser une substitution complémentaire.Ainsi, nous pouvons atteindre notre objectif de diffusion des pixels [20].

3.6.2 La cryptographie quantique

La cryptographie quantique (ou chiffrement quantique) désigne différentes techniques employées dans le domaine de la cybersécurité afin de protéger et de transmettre des données sécurisées en respectant les lois de la nature immuable de la mécanique quantique.
Même si le chiffrement quantique n'est encore qu'à ses débuts, il a le potentiel de devenir un mécanisme beaucoup plus sûr que les autres types d'algorithmes cryptographiques qui l'ont précédé.Et en théorie, le piratage est même impossible.
La cryptographie quantique, à la différence de la cryptographie traditionnelle, s'appuie sur les lois de la physique [49].
Plus spécifiquement, elle s'appuie sur les principes spécifiques de la mécanique quantique :

- **Les particules sont intrinsèquement incertaines :** à un niveau quantique, il est possible que les particules existent simultanément à plusieurs endroits ou dans plusieurs états, et il est impossible de prédire leur état quantique précis.
- **Il est possible de mesurer les photons de manière aléatoire dans des positions binaires :** les photons, qui sont les plus petites particules de lumière, peuvent être définis selon une polarité spécifique, ou un spin, qui peut être utilisé comme une contrepartie binaire aux uns et aux zéros des systèmes de calcul traditionnels.
- **Il est impossible de mesurer un système quantique sans qu'il soit modifié** : d'après les lois de la physique quantique, seule la mesure ou même l'observation d'un système quantique aura toujours un effet mesurable sur ce système.
- **Il est possible que les particules soient partiellement clonées, mais pas entièrement :** même si certaines propriétés peuvent être clonées, il est a priori impossible d'obtenir un clone 100 % fidèle [49].

La distribution de clefs grâce aux photons polarisés :

avec les principes de mécanique quantique générale, un photon est une boîte à deux compartiments dont l'un d'eux est inévitablement détruit à chaque fois qu'on ouvre à un autre pour en voir le contenu (on ne peut donc connaître que le contenu de l'un des deux compartiments).
L'envoyeur utilise cette propriété pour envoyer une clef secrète à son partenaire.
Détaillons-la :
L'envoyeur place des bits (des 0 et des 1) dans des "compartiments" tirés au hasard, qui déterminent la clef qu'il souhaite partager avec le récepteur. Il émet ainsi le flux de photons créé. Chaque photon reçu est ouvert au hasard par son partenaire. Par un canal quelconque, l'émetteur signale au récepteur dans quels compartiments des photons les bits secrets étaient placés. À peu près un photon sur deux, ouvert correctement par le récepteur, fournit un bit commun aux deux partenaires.
Tous ces bits servent donc de clef secrète pour la communication [44].

Distribution quantique de clé (QKD) :

La distribution quantique de clé (QKD), théorisée en 1984 par Charles H. Bennett et Gilles Brassard, est un système de cryptographie quantique couramment utilisé. Les systèmes QKD ne chiffrent pas les données elles-mêmes, mais permettent un échange de clés sécurisé entre deux parties pour créer une clé privée partagée.
Dans les systèmes QKD, des photons individuels sont envoyés à travers des câbles de fibres optiques. Chaque photon représente un seul bit de données, avec des filtres polarisés modifiant leur orientation physique. Le récepteur décode les positions des photons pour former la clé partagée. Cette méthode assure la sécurité car il est impossible d'observer un état quantique sans l'affecter, permettant ainsi de détecter toute tentative d'espionnage.
Bien que la QKD offre des avantages prouvés en laboratoire et sur le terrain, des défis pratiques persistent, notamment la dégradation des photons sur de longues distances. Cependant, des avancées récentes ont étendu la portée de certains systèmes QKD à l'échelle continentale grâce à l'utilisation de nœuds sécurisés et de répéteurs de photons [49].

Les types de cryptographie quantique :

D'autres domaines de cryptologie quantique sont encore étudiés par les chercheurs, tels que le chiffrement direct, les signatures numériques, l'intrication quantique et d'autres formes de communications quantiques [49].
D'autres formes de cryptage quantique sont :

- Cryptographie basée sur la localisation quantique.
- Cryptage quantique autonome de l'appareil.
- Protocole Kek.
- Protocole Y-00.

3.6.3 Détection de Compression (Compressive Sensing)

La Détection de Compression, ou Compressive Sensing (CS) en anglais, est une technique qui permet de reconstruire un signal de grande dimension à partir d'un nombre réduit de mesures. Cette technique repose sur le principe que de nombreux signaux sont naturellement parcimonieux, c'est-à-dire qu'ils peuvent être représentés avec un nombre limité de coefficients non nuls dans une certaine base [50].

Principe de la CS :

1. **Représentation parcimonieuse :** Le signal x de longueur N est supposé être K-parcimonieux, c'est-à-dire qu'il peut être exprimé comme une combinaison linéaire de K vecteurs de base, avec $K \ll N$. On peut écrire :

$$x = \Psi s$$

   où s est un vecteur de coefficients de transformation contenant au plus K entrées non nulles, et Ψ est une matrice de transformation orthogonale (matrice de base éparse).

2. **Mesure de compression :** Une matrice de mesure Φ de taille $M \times N$ ($M < N$), indépendante de Ψ, est utilisée pour projeter le signal x dans un espace de dimension réduite. On obtient ainsi M observations linéaires y :

$$y = \Phi x = \Phi \Psi s$$

3. **Reconstruction du signal :** Le signal original x peut être reconstruit à partir des observations y en résolvant le problème d'optimisation suivant :

$$\min_s ||s||_1 \quad \text{subject to} \quad y = \Phi \Psi s$$

Ce problème vise à trouver le vecteur s le plus parcimonieux qui satisfait la contrainte $y = \Phi \Psi s$. L'algorithme SL0 est utilisé pour résoudre ce problème d'optimisation [50].

Conditions de reconstruction :

Il est possible de reconstruire le signal original avec une grande probabilité si le nombre de mesures M est supérieur à un certain seuil, donné par :

$$M \geq K \log_2 \left(\frac{N}{K} \right)$$

Avantages de la CS :

- **Réduction de la quantité de données :** La CS permet de réduire considérablement la quantité de données à acquérir et à transmettre.
- **Réduction du temps de mesure :** La CS permet de réduire le temps nécessaire pour acquérir les données.
- **Réduction du coût :** La CS permet de réduire le coût des systèmes d'acquisition et de traitement des données [50].

Matrices de mesure :

Plusieurs types de matrices de mesure peuvent être utilisés en CS, notamment :

- Matrices aléatoires gaussiennes
- Matrices partielles orthogonales

- Matrices de Hadamard
- Matrices circulaires

Génération de la matrice de mesure :

La première ligne de la matrice circulaire est un vecteur U généré par une carte chaotique memristive. Les lignes suivantes sont générées en décalant la précédente vers la droite et en multipliant le premier élément par λ [50] :

$$\begin{cases} \Phi(j,1) & = \lambda \cdot \Phi(j-1,N) \\ \Phi(j,2:N) & = \Phi(j-1,:N-1) \end{cases} \tag{3.3}$$

Applications de la CS :

- **Imagerie médicale :** La CS peut être utilisée pour réduire le temps d'acquisition des images IRM et des scanners CT.
- **Traitement du signal :** La CS peut être utilisée pour compresser et reconstruire des signaux audio et vidéo.
- **Réseaux sans fil :** La CS peut être utilisée pour améliorer la fiabilité des communications sans fil [50].

3.6.4 La cryptographie chaotique

La cryptographie chaotique utilise les propriétés des systèmes chaotiques pour concevoir des algorithmes de chiffrement robustes. Les systèmes chaotiques sont caractérisés par leur sensibilité aux conditions initiales et leur comportement imprévisible. Ces propriétés les rendent particulièrement adaptés à la cryptographie, car elles permettent de créer des clés de chiffrement complexes et difficiles à prédire.

L'architecture d'un cryptosystème d'images basé sur le chaos se compose généralement de deux étapes principales :

- **L'étape de confusion**
- **L'étape de diffusion**

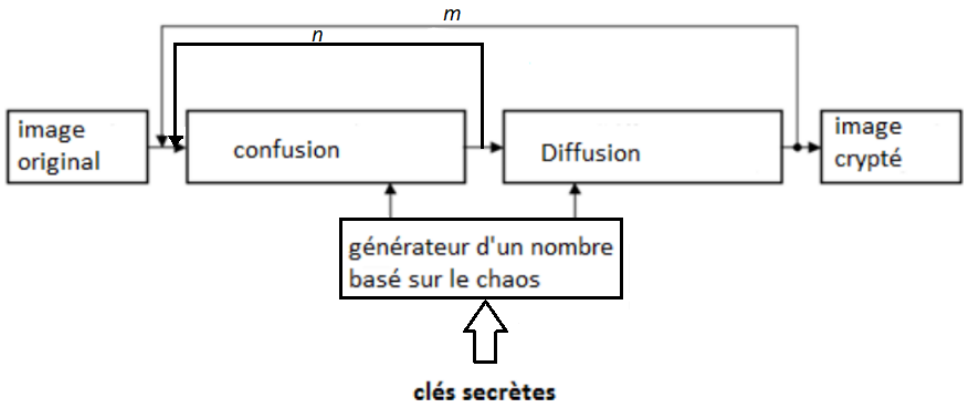


FIGURE 3.3 – Structure générale d'un schéma de cryptage d'image chaotique [16].

La phase de confusion :

Cette phase vise à brouiller la structure de l'image en permutant les positions des pixels selon une séquence déterminée par une clé secrète. Les valeurs des pixels ne sont pas modifiées, mais leur ordre est remanié de manière complexe, rendant l'image méconnaissable. Cette permutation est généralement effectuée plusieurs fois, en utilisant des fonctions chaotiques, pour renforcer la sécurité [16].

La phase de diffusion :

Cette phase vise à diffuser l'information dans l'image en modifiant les valeurs des pixels. La modification d'un pixel affecte les pixels voisins, créant une dépendance complexe entre les pixels. Cette phase utilise des systèmes chaotiques pour générer des séquences qui modifient les valeurs des pixels de manière à ce qu'une petite modification d'un pixel se propage à plusieurs autres pixels [16].

Combinaison des phases de confusion et de diffusion :

Pour renforcer la sécurité du cryptage, les phases de confusion et de diffusion sont généralement combinées et répétées plusieurs fois. La confusion est effectuée n fois, avec n généralement supérieur à 1, suivie d'une phase de diffusion. L'ensemble du processus de confusion-diffusion est ensuite répété m fois, avec m généralement supérieur à 1, pour atteindre un niveau de sécurité satisfaisant.

Cryptosystèmes d'images :

L'architecture typique des systèmes de cryptage d'images basés sur le chaos se compose donc de ces deux étapes principales : la confusion et la diffusion. La phase de confusion rend l'image méconnaissable en permutant les pixels, tandis que la phase de diffusion rend l'image résistante aux attaques en modifiant les valeurs des pixels de manière complexe. La répétition de ces deux étapes permet d'atteindre un niveau de sécurité élevé [16].

3.7 Analyse de sécurité et performance

L'espace de clés représente l'ensemble de toutes les clés possibles qui peuvent être utilisées pour chiffrer et déchiffrer une image. En d'autres termes, il s'agit de la taille de l'ensemble des combinaisons possibles de clés de cryptage/décryptage disponibles dans le système de chiffrement [51].
La taille de l'espace de clés est un facteur crucial car elle détermine la complexité d'une attaque. Lorsque l'espace de clés est grand, cela signifie qu'il existe de nombreuses combinaisons possibles de clés différentes que l'attaquant devrait explorer afin de trouver la clé correcte [52].

3.7.1 Analyse statistique

– **L'histogramme :** est un outil largement utilisé en traitement d'images pour analyser la répartition des valeurs d'intensité des pixels dans une image. Il se présente sous la forme d'un graphique qui montre le nombre de pixels ayant

une intensité spécifique, souvent sur une échelle de 0 (noir) à 255 (blanc) pour les images en niveaux de gris, ou sur plusieurs canaux de couleur comme le rouge, le vert et le bleu pour les images en couleur [53].

Il est important d'avoir une uniformité dans l'histogramme de l'image chiffrée afin d'éviter qu'un adversaire ne puisse extraire des informations de cet histogramme.

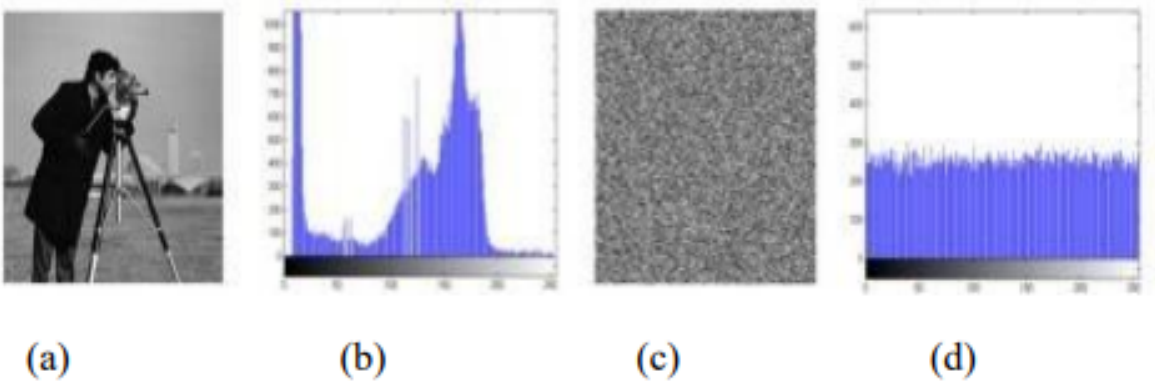


FIGURE 3.4 – (a) image en clair, , (b) histogramme d'image en clair, (c) images cryptées, (d) histogramme d'image cryptée.

– **La corrélation entre les pixels adjacents :**La corrélation évalue le degré d'association entre deux pixels voisins dans une image cryptee et dans une image clair, les pixels adjacents sont souvent fortement corrélés dans différentes directions, notamment horizontale, verticale et diagonale. Un bon algorithme de chiffrement d'images doit réduire la corrélation entre les pixels adjacents afin d'assurer la sécurité contre l'analyse statistique [54]. et les formules de calcul des coefficients de corrélation de chaque paire comme suit :

$$r = \frac{\mathrm{cov}(x, y)}{\sqrt{\mathrm{Var}(x)}\sqrt{\mathrm{Var}(y)}} \tag{3.4}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{3.5}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{3.6}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{3.7}$$

Tel que :

r : la corrélation.

cov : la covariance.

E : l'espérance mathématique.

D : la variance.

x, y : les valeurs des pixels des images.

– **L'entropie :** Selon la théorie de Shannon [55], l'entropie d'une source d'information évalue la quantité d'information englobée ou libérée qui lui est associée. Plus la source est redondante, moins elle renferme d'informations.
L'entropie d'une image est en effet un indicateur important de sa complexité. Lorsque l'entropie d'une image est nulle, cela signifie que l'image est uniforme et ne présente qu'une seule couleur, Une entropie plus élevée correspond à une image plus "aléatoire" [54]. et tout message codé sur M bits a une limite d'entropie supérieure de M. La formule pour déterminer l'entropie d'une source m est la suivante :

$$H(m) = -\sum_{i=0}^{n-1} p_i \log_2(p_i) \tag{3.8}$$

p_i : la probabilité d'un pixel.

n : le nombre de bits dans chaque pixel.

3.7.2 Analyse de sensitivité

– **Résistance aux attaques différentielles :** Dans un algorithme de chiffrement d'image sécurisé, chaque pixel de l'image en clair est traité de manière significative pour assurer la sécurité du processus de chiffrement. L'objectif est que toute modification d'un seul pixel dans l'image en clair entraîne un

changement notable dans l'image chiffrée correspondante. Cela garantit que l'algorithme de chiffrement est robuste contre les attaques différentielles [56].

Des mesures quantitatives telles que le NPCR (Nombre de Pixels Change Rate) et l'UACI (Unified Average Changing Intensity) sont utilisées pour évaluer la résistance d'un schéma de chiffrement d'image à l'analyse différentielle. Le NPCR représente le pourcentage de pixels différents entre deux images chiffrées et se calcule comme suit :

$$\text{NPCR} = \frac{\sum_{i,j} f(i,j)}{W \times H} \times 100\% \tag{3.9}$$

L'UACI mesure l'intensité moyenne de changement et est calculé selon la formule :

$$\text{UACI} = \frac{1}{W \times H} \left[\frac{\sum_{i,j} |C1(i,j) - C2(i,j)|}{255} \right] \times 100\% \tag{3.10}$$

Où W et H représentent respectivement la largeur et la hauteur de l'image. $C1(i,j)$ et $C2(i,j)$ désignent les valeurs des pixels dans les images chiffrées avant et après la modification d'un pixel dans l'image claire. Pour un pixel à la position (i,j), si $C1(i,j) \neq C2(i,j)$, alors $f(i,j) = 1$; sinon $f(i,j) = 0$.

Un NPCR d'environ 99,6094% et un UACI d'environ 33,4635% sont des valeurs typiques indiquant la sécurité d'un schéma de chiffrement d'image contre les attaques différentielles [56].

– **Sensibilité de la clé :** Un algorithme de chiffrement efficace devrait être sensible à la clé, de sorte que même en appliquant une modification mineure a la clé secrète entraîne une transformation complète de l'image chiffrée. Pour évaluer la sensibilité de la clé de chiffrement dans un algorithme donné, nous avons suivi les étapes suivantes [54] :

  * Chiffrement de l'image originale avec la clé secrète.
  * Chiffrement de la même image avec une clé légèrement modifiée.
  * Les deux images chiffrées résultantes sont comparées en utilisant les mesures NPCR et UACI.

3.8 Conclusion

Le cryptage d'images est un domaine crucial de la cryptographie moderne, offrant une variété de méthodes et de techniques pour protéger la confidentialité et l'intégrité des données visuelles. Ce chapitre a exploré divers aspects du cryptage d'images, notamment les techniques de chiffrement dans les domaines spatial et fréquentiel, ainsi que les concepts de confusion et de diffusion. Nous avons également examiné les différentes méthodes de substitution et de permutation utilisées dans le cryptage, ainsi que des approches innovantes telles que l'encodage ADN et la cryptographie quantique . Enfin, nous avons souligné l'importance de l'analyse de sécurité et de performance pour évaluer l'efficacité des algorithmes de cryptage d'images. En combinant ces connaissances, il est possible de développer des systèmes de cryptage robustes et efficaces pour protéger les images contre les menaces potentielles.

Chapitre 4

Notre proposition :

4.1 Introduction

Plusieurs techniques de cryptage d'images numériques ont été proposées par les chercheurs en cryptographie. Il existe différents types d'algorithmes, basés sur des théories du chaos, la substitution, la permutation, ainsi que des algorithmes qui utilisent des technologies telles que le séquençage de l'ADN, et de nombreuses autres techniques.

Ce chapitre de notre étude se concentre sur l'implémentation pratique de notre schéma de cryptage d'images, basé sur l'utilisation de deux cartes chaotiques unidimensionnelles améliorées et modifiées : la carte logistique améliorée (ILM) et la carte sinusoïdale améliorée (ISM). Ces deux cartes offrent des performances robustes, ce qui en fait un choix idéal pour renforcer la sécurité des systèmes de cryptage.

4.2 Les cartes utilisées

Les cartes unidimensionnelles se caractérisent par une vitesse d'exécution élevée et une facilité de mise en œuvre, tandis que les cartes multidimensionnelles sont caractérisées par un grand espace clé et plus de complexité.

Cependant, les systèmes chaotiques présentent des limites en termes de performances chaotiques. Les cartes unidimensionnelles souffrent de petits espaces clés, d'une complexité insuffisante et d'une faible sécurité, tandis que les cartes multidimensionnelles

présentent un coût de calcul élevé et une implémentation difficile [57]. Ces limitations entraînent certaines lacunes dans les algorithmes de cryptage. Pour éviter ces inconvénients, de nombreux chercheurs ont recours à l'amélioration des cartes existantes ou à des méthodes hybrides utilisant plusieurs cartes [58]. Nous suggérons que le travail repose sur l'utilisation de deux cartes 1D améliorées et modifiées : la carte logistique améliorée (ILM) et la carte sinusoïdale améliorée (ISM).

4.3 Algorithme de cryptage d'image

– Dans cette section, nous détaillons notre l'algorithme proposé pour le chiffrement d'images :

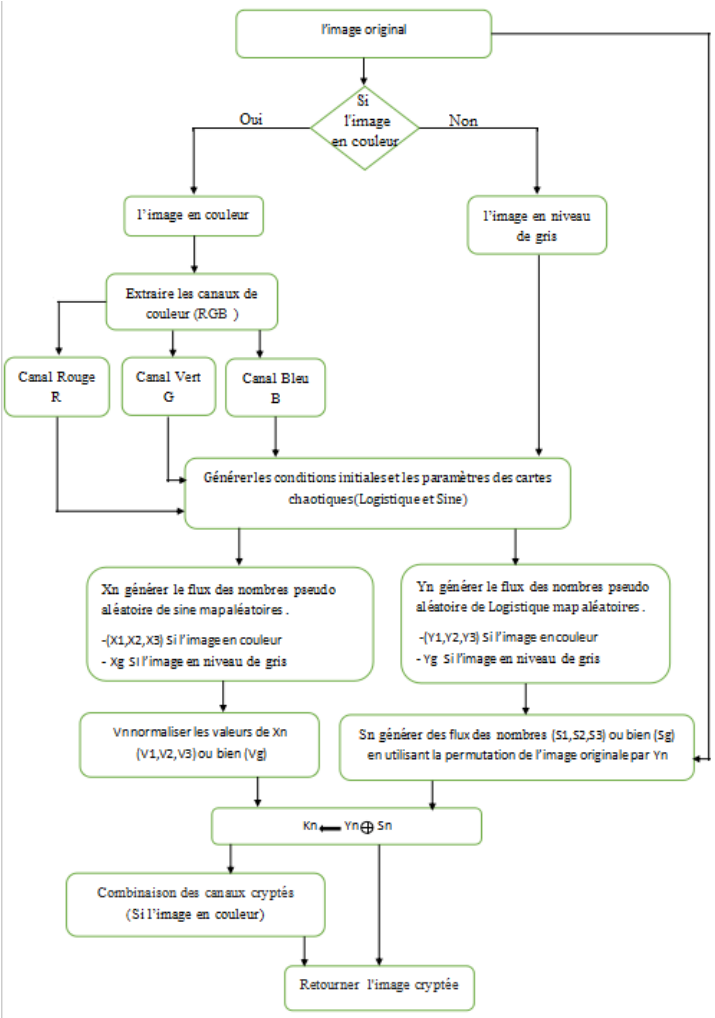


FIGURE 4.1 – Les étapes de chiffrement.

4.3.1 Utilisation de plusieurs cartes chaotiques 1D

En raison de la puissance et de la rapidité des cartes chaotiques dans la génération de séquences de nombres aléatoires, et pour éviter les limitations des cartes unidimensionnelles et multidimensionnelles, nous avons sélectionné deux cartes 1D modifiées et améliorées (la carte logistique améliorée ILM et la carte sinusoïdale améliorée ISM). Ces cartes ont été choisies en raison de leurs performances robustes, où un petit changement dans les conditions initiales entraîne une grande différence dans les résultats. Ces performances sont confirmées par les analyses de Lyapunov et le grand domaine obtenu par le diagramme de bifurcation présenté au Chapitre 2.

4.3.2 Extraction des conditions initiales et les paramètres à partir de l'image

Une fonction permet de gérer automatiquement les conditions initiales et les paramètres, qui sont influencés par l'image. Ils diffèrent donc d'une image à l'autre.

Pour générer les valeurs initiales contenant les conditions et les paramètres, nous appliquons l'algorithme suivant :

Algorithme extract_chaotic_params (channel) ;

Entrée : channel ;

Sortie : paramLogMap, paramSineMap ;

1 : paramLogMap.r = mean2(channel) / 255 ;

2 : paramLogMap.x0 = std2(channel) / 255 ;

3 : paramSineMap.a = mean2(channel) / 255 ;

4 : paramSineMap.x0 = std2(channel) / 255 ;

5 : paramLogMap.r = 0.9 + (paramLogMap.r * (4 - 0.9)) ;

6 : paramSineMap.a = 0.00009 + (paramSineMap.a * (4-0.9)) ;

Cet algorithme, appelé `extract_chaotic_params`, prend en entrée un canal (*channel*) et produit deux sorties, *paramLogMap* et *paramSineMap*.

Nous calculons plusieurs paramètres à partir des données du canal et les normalisons en les divisant par 255 .

* Nous calculonsla moyenne des valeurs du canal et la divise par 255, assignant le résultat à *paramLogMap.r*.
* Nous calculons l'écart type des valeurs du canal et le divise par 255, assignant le résultat à *paramLogMap.x0*.
* Nous calculons à nouveau la moyenne des valeurs du canal et la divise par 255, assignant le résultat à *paramSineMap.a*.
* Nous calculons à nouveau l'écart type des valeurs du canal et le divise par 255, assignant le résultat à *paramSineMap.x0*.
* Nous ajustons *paramSineMap.a* et *paramLogMap.r* dans l'intervalle [0, 4] en effectuant une opération de mise à l'échelle.

– Nous effectuons le chiffrement sur l'image en utilisant l'algorithme suivant :

Algorithme encrypt_image(img) ;

Entrée : img ;
Sortie : encryptedImg, permIndex ;

1 : Si (l'image img en niveaux de gris) Alors
2 :[paramLogMap,paramSineMap]←extract$_c haotic_p arams(img)$;
3 :[encryptedImg, permIndex] ← encrypt$_c hannel(img, paramLogMap, paramSineMap)$;
4 :Sinon
5 :[paramLogMapR, paramSineMapR] ← extract$_c haotic_p arams(img[:, : 1])$;
6 : [paramLogMapG, paramSineMapG] ← extract$_c haotic_p arams(img[:, :, 2])$;
7 :[paramLogMapB, paramSineMapB] ← extract$_c haotic_p arams(img[:, :, 3])$;
8 :[encryptedR, permIndexR] ← encrypt$_c hannel(img(:, :, 1), paramLogMapR, paramSineMapR)$;
9 :[encryptedG, permIndexG] ← encrypt$_c hannel(img(:, :, 2), paramLogMapG, paramSineMapG)$;
10 :[encryptedB, permIndexB] ← encrypt$_c hannel(img(:, :, 3), paramLogMapB, paramSineMapB)$;
11 :encryptedImg ← concaténer les canaux cryptés (encryptedR, encryptedG, encryptedB) ;
12 :permIndex ← permIndexR, permIndexG, permIndexB ;
13 :Fin Si

* Nous effectuons la vérification de l'image en niveaux de gris :
  - Si l'image est en niveaux de gris, elle a une seule matrice. Cela signifie que l'image est représentée en deux dimensions (largeur, hauteur).
  - Nous extrayons les paramètres et les conditions initiales chaotiques nécessaires en appelant la fonction `extract_chaotic_params` avec l'image en niveaux de gris comme argument.
  - Nous chiffrons l'image en appelant la fonction `encrypt_channel` avec l'image et les paramètres chaotiques extraits. Cette fonction retourne l'image chiffrée (*encryptedImg*) et les indices de permutation (*permIndex*), Comme suit :

Algorithme encrypt_channel (paramLogMap, paramSineMap)

Entrée : channel, paramLogMap, paramSineMap ;
Sortie : permutedChannel, permIndex ;

1 : [M, N] ← dimensions(channel) ;
2 :(X2, _) ← Logistic_Map_M(paramLogMap.r, paramLogMap.x0, M * N) ;
3 :(permutedChannel, permIndex) ← permute_pixels_using_X2(X2, channel) ;
4 :(X3, _) ← Sine_Map_ISM(paramSineMap.a, paramSineMap.x0, M * N) ;
5 :cx ← reshape (X3, [M, N]) ;
6 :cx ← uint8(mod (cx * 255, 256)) ;
7 : encryptedChannel ← bitxor(uint8(permutedChannel), cx) ;
8 : Retourner encryptedChannel, permIndex ;

L'algorithme débute en obtenant les dimensions du canal d'image, ce qui révèle le nombre de lignes (hauteur) et de colonnes (largeur) de l'image. Ensuite, il utilise le Map Logistique pour générer une séquence chaotique X2 adaptée à la taille de l'image. Cette séquence est essentielle pour permuter les pixels de l'image.

L'algorithme utilise la séquence chaotique X2 pour permuter les pixels de l'image en appelant la fonction `permute_pixels_using_X2`. Cette fonction retourne le canal d'image permuté (*permutedChannel*) ainsi que les indices de permutation (*permIndex*). Comme suit :

Algorithme permute_pixels_using_X2(X2 channel)

Entrée : X2, channel ;

Sortie : permutedChannel, permIndex ;

1 : [M, N] ← size(channel) ;
2 : X2 ← reshape (X2, [M*N, 1]) ;
3 : [sortedX2, perm$_i ndices$] ¸$sort(X2)$;
4 : permIndex ← perm$_i ndices$;
5 : permutedChannel ← channel(perm$_i ndices$);
6 : permutedChannel ← reshape (permutedChannel, [M, N]) ;
7 : Return permutedChannel, permIndex ;

Les étapes dans cet algorithme sont les suivantes :

- Obtient les dimensions M et N de la matrice.
- Redimensionne le vecteur X2 en une colonne unique de taille M*N.
- Trie le vecteur X2 et récupère les indices de permutation.
- Enregistre les indices de permutation dans *permIndex*.
- Réorganise les pixels du canal selon les indices de permutation.
- Rétablit la forme originale de la matrice.
- Renvoie le canal réorganisé et les indices de permutation.

∗ Ensuite, nous effectuons une opération de Diffusion en utilisant Map Sinusoidal.

∗ Finalement, l'algorithme retourne l'image chiffré ainsi que les indices de permutation.

∗ Le chiffrement de l'image en couleur est effectué de la même manière que pour les images en niveaux de gris, mais pour chaque canal individuellement, puis à la fin ils sont réunis.

4.4 Implémentation

4.4.1 Environnement de travail

Les éléments matériels (Hardware) et logiciels (Software) utilises :

– **Environnement matérielle :**

Notre algorithme a été développée sur un système équipé des spécifications suivantes :

* Processeur : Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz (jusqu'à 1.90 GHz).
* Système d'exploitation : Windows 10 Pro 64 bits.
* Mémoire vive (RAM) : 8 Go.

– **Environnement logiciel :** Le langage de programmation Matlab a été utilisé pour mettre en place notre application, avec la version Matlab R2017a.

– **MATLAB :**

Est un langage de programmation et un environnement de développement pour le calcul numérique et l'analyse de données. Développé par MathWorks, il est particulièrement utilisé par les ingénieurs et les scientifiques pour la manipulation de matrices, la visualisation de données, l'implémentation d'algorithmes, et la création de modèles.

Le nom MATLAB vient de "matrix laboratory" (laboratoire matriciel), reflétant son orientation vers les applications mathématiques et techniques.

MATLAB est également connu pour ses boîtes à outils spécialisées, qui étendent ses capacités à des domaines spécifiques tels que le traitement du signal, le contrôle de systèmes, le deep learning, et bien d'autres [59].

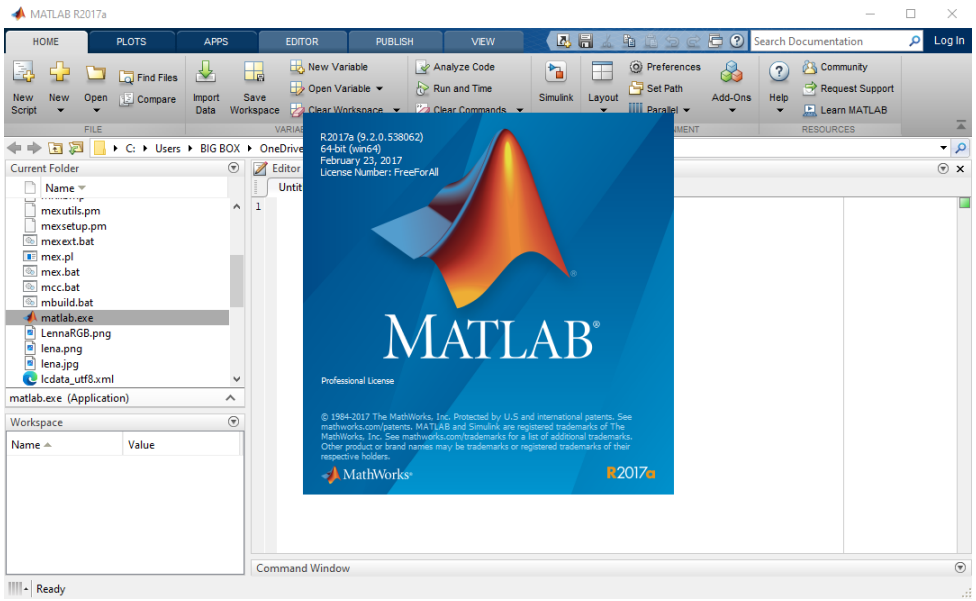


FIGURE 4.2 – environnement de Matlab.

4.4.2 Interface graphique

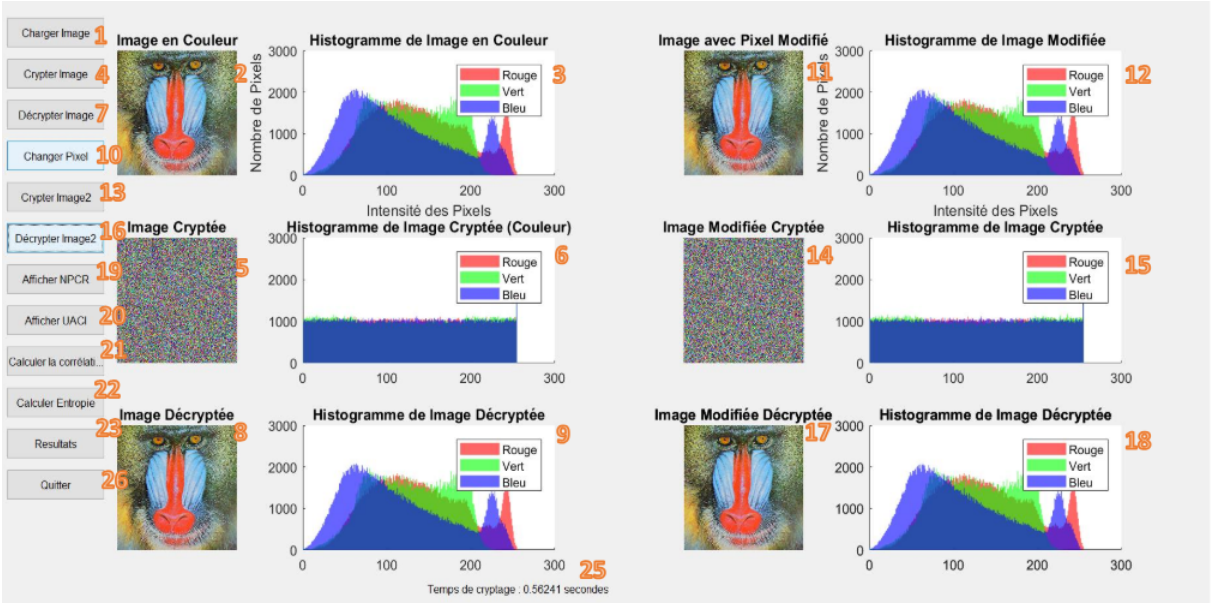


FIGURE 4.3 – Interface graphique.

L'explication :

1-bouton pour charger une image.

2-l'image orignale.

3-l'histogramme de l'image orignale.

4- bouton pour crypter l'image.

5- l'image cryptée.

6- l'histogramme de l'image cryptée.

7- bouton pour décrypter l'image.

8- l'image décryptée.

9- l'histogramme de l'image décryptée.

10- bouton pour changer un pixel dans l'image.

11- l'image avec pixel modifié.

12- l'histogramme de l'image avec pixel modifié.

13- bouton pour crypter l'image modifiée.

14- l'image modifié cryptée.

15- l'histogramme de l'image modifié cryptée.

16- bouton pour décrypter l'image modifiée.

17- l'image modifié décryptée.

18- l'histogramme de l'image modifié décryptée.

19- bouton pour calculer NPCR.

20- bouton pour calculer UACI.

21- bouton pour calculer la corrélation entre les pixels adjacents .

22- bouton pour calculer L'entropie.

23- bouton pour afficher les résultats.

24- Interface pour afficher les résultats (voir la figure 4.4).

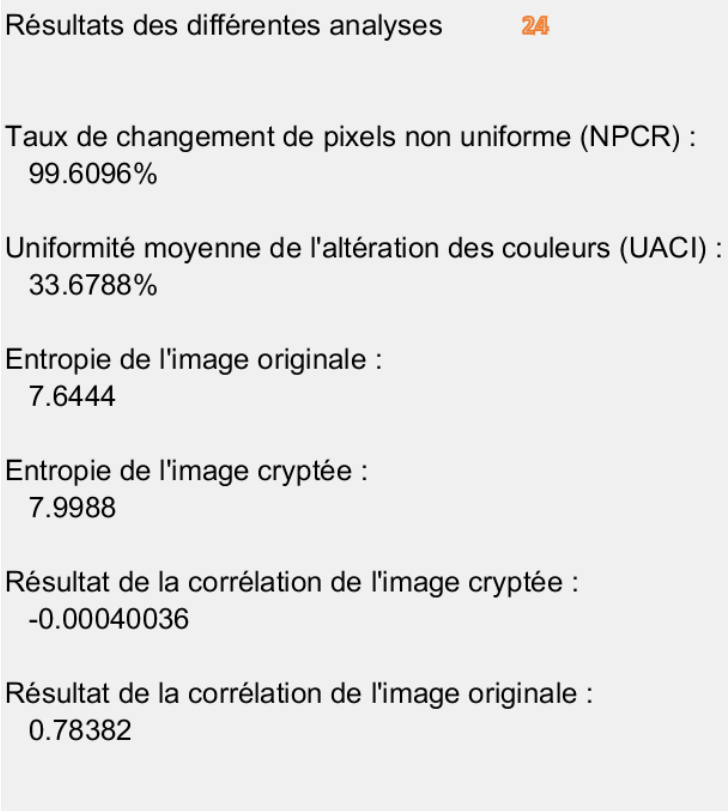


FIGURE 4.4 – affichage de toutes les valeurs calculéer.

25-temps de crypter de l'image.

36- bouton pour quitter l'interface.

4.4.3 Résultats expérimentaux

Les données utilisées dans notre étude sont des images qui ont été évaluées pour confirmer l'efficacité de notre méthode de chiffrement. Quatre images en couleur de différentes tailles sont cryptées dans les figures 4.5 ci-dessous.

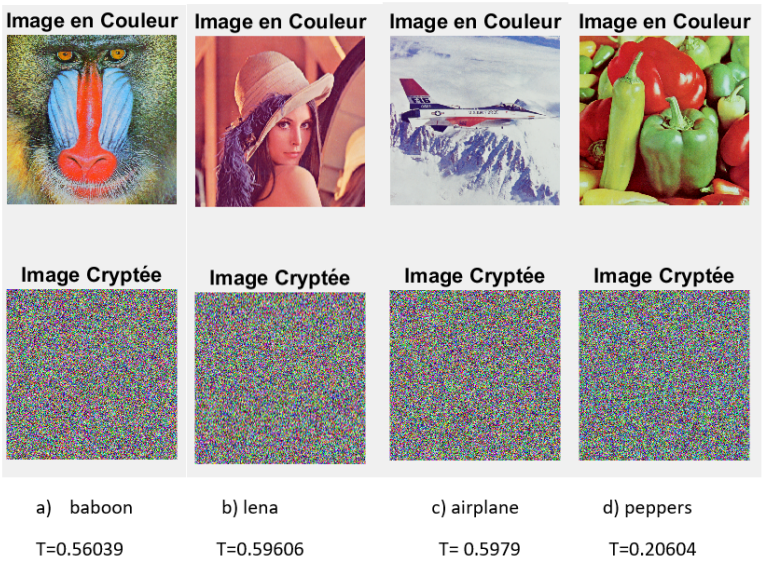


FIGURE 4.5 – Quatre images cryptées (en couleur) .

La figure au-dessous 4.6 montrent deux images cryptées en niveau de gris .

FIGURE 4.6 – Deux images cryptées (en niveau de gris) .

T : temps de cryptage.

4.4.4 Évaluation de performance

– **Espace des clés :**

L'espace de clé doit être suffisamment grand pour garantir la sécurité. Dans notre travail :

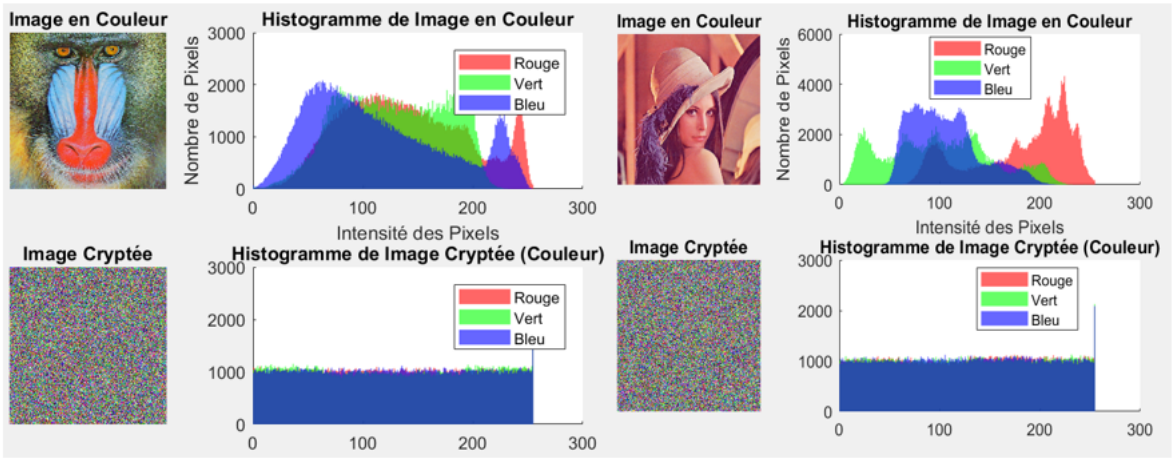
Pour une image en niveaux de gris, le code utilise deux cartes chaotiques, chacune avec deux paramètres (r et x0). Le nombre total de paramètres est de 2x2 = 4.

Étant donné que chaque paramètre est un nombre réel prenant 15 bits, la taille de l'espace de clés pour une image en niveaux de gris est $(10^{15})^4 = 10^{60}$.

Pour une image en couleur, le code utilise deux cartes chaotiques pour chaque canal de couleur (rouge, vert et bleu). Chaque carte chaotique a deux paramètres (r et x0). Le nombre total de paramètres est de 2x6 = 12. La taille de l'espacede clés pour une image en couleur donc est de $(10^{15})^{12} = 10^{180}$.

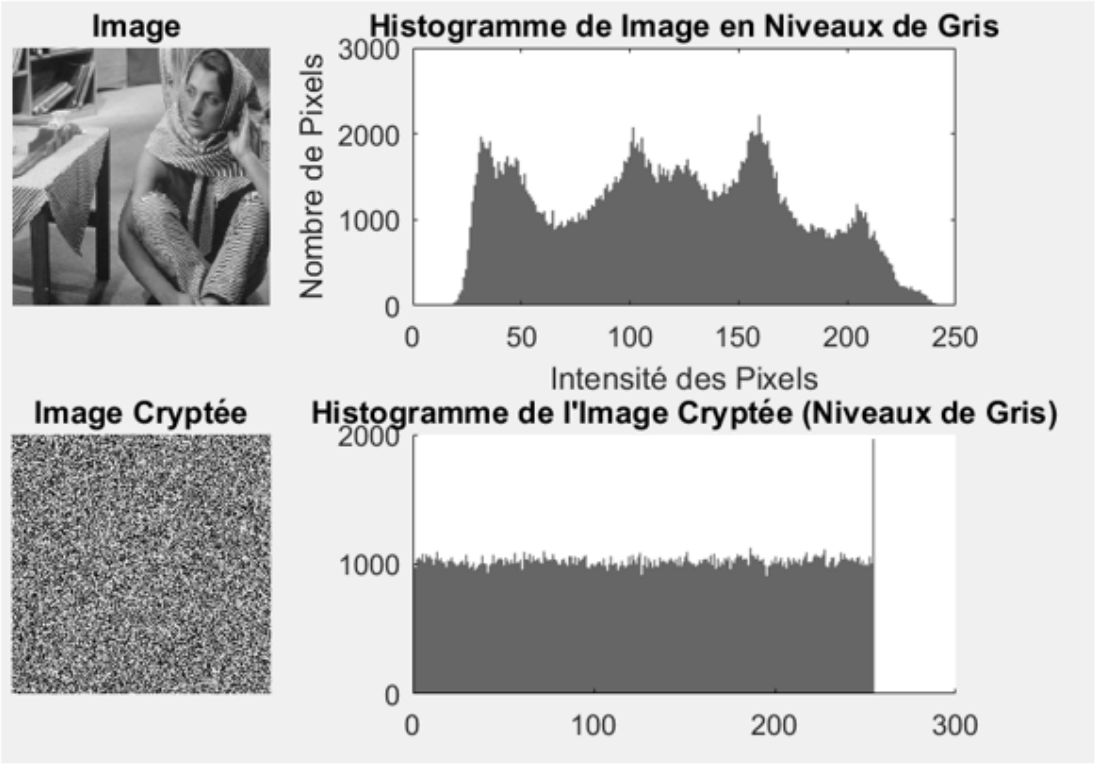
– **L'histogramme :**

Les figures 4.7 et 4.8 présentent les tracés des histogrammes des images originales et des images cryptées.



a) baboon b) lena

FIGURE 4.7 – des histogrammes des images originales et des images cryptées (en couleur).



b) Barbara

FIGURE 4.8 – des histogrammes des images originales et des images cryptées (en niveau de gris) .

Selon nos résultats, les histogrammes des images chiffrées sont uniformes après leur cryptage, ce qui rend extrêmement difficile pour un attaquant d'extraire des informations à partir de l'histogramme de l'image cryptée.

– **Sensibilité de la clé :**

Dans le test de sensibilité de la clé de l'algorithme proposé, deux clés sont utilisées :

la première est extraite de l'image originale, tandis que la deuxième est extraite d'une image après la modification d'un seul pixel. Ensuite, ces deux différentes clés sont utilisées pour chiffrer l'image. Les résultats de ce test sont résumés dans le tableau 4.1.

Image	**UACI**	**NPCR**
Lena	33.5236%	99.6053%
Baboon	33.4747%	99.6043%
Airplane	33.4275%	99.6162%
Barbara	33.4013%	99.6082%
Peppers	33.4955%	99.6095%
Cameraman	33.539%	99.6078%

TABLE 4.1 – Comparaison de l'UACI et du NPCR pour différentes images

– **L'entropie :**

Le tableau 4.2 montre les valeurs d'entropie des images claires ainsi que de leurs versions chiffrées. Il est crucial que l'entropie soit proche de 8, car une valeur inférieure indiquerait une prévisibilité accrue, compromettant ainsi la sécurité contre l'analyse statistique.

Image	**Entropie des images claires**	**Entropie des images chiffrées**
Lena	7.2891	7.997
Baboon	7.6444	7.9993
Airplane	6.5768	7.9991
Barbara	7.6321	7.9993
Peppers	7.2978	7.9992
Cameraman	7.1048	7.9972
Moyenne	**7.3227**	**7.9990**

TABLE 4.2 – Comparaison de l'entropie des images claires et chiffrées

Selon les résultats, après avoir simulé 5 images, la valeur moyenne de l'entropie des images chiffrées est de 7.9990, ce qui est très proche de 8. Cela démontre que la prévisibilité est difficile à obtenir.

– **La corrélation entre les pixels adjacents :**

Le tableau 4.3 présente les corrélations entre les images claires et leurs versions chiffrées. Une corrélation proche de 1 indique une forte dépendance entre l'image claire et l'image chiffrée, tandis qu'une corrélation proche de 0 indique une absence de lien entre les deux. De cette manière, plus la valeur de corrélation est faible, plus la qualité du chiffrement est élevée.

Image	**Corrélation des images claires**	**Corrélation des images chiffrées**
Lena	0.94441	-0.0011069
Baboon	0.78382	0.0000451
Airplane	0.95582	-0.0005612
Barbara	0.91243	0.0000451
Peppers	0.97331	0.00043391
Cameraman	0.9333	0.0020524
Moyenne	**0.9218**	**0.00046**

TABLE 4.3 – Comparaison des corrélations des images claires et chiffrées

Selon les résultats après avoir essayé 5 images, on observe une valeur moyenne de 0.00046 pour les corrélations des images chiffrées, ce qui est très proche de 0. Cela démontre que les pixels adjacents après le cryptage ne sont pas corrélés.

4.4.5 Comparaison externe

Le tableau 4.4 montrant la Comparaison des valeurs de NPCR et UACI entre notre approche proposée et les autres méthodes :

Scheme	Images Valeur idéale	NPRC (%) ≈ 99.6094	UACI (%) ≈ 33.4635
Notre scheme	Lena	99.6053	33.5236
	Baboon	99.6043	33.4747
	Barbara	99.6082	33.4013
	Cameraman	99.6078	33.539
	Pepper	99.6095	33.4955
Ref [60]	Lena	99.6032	33.5986
	Barbara	99.6118	33.4142
	Cameraman	99.6112	33.5076
	Pepper	99.6561	33.4312
Ref [61]	Lena	99.6641	33.6124
	Baboon	99.6438	33.6430
	Cameraman	99.6523	33.6425
	Pepper	99.6287	33.6012
Ref [62]	Lena	99.6002	33.5079
	Baboon	99.5903	33.5281
	Cameraman	99.6082	33.5574
	Pepper	99.6112	33.5265
Ref [63]	Lena	99.61	33.46
	Baboon	99.61	33.48
	Barbara	99.60	33.43

TABLE 4.4 – Comparaison externe : NPCR et UACI.

Le tableau ci-dessous 4.5 présente une comparaison des valeurs d'entropie obtenues à partir de notre approche proposée et d'autres méthodes existantes :

L'entropie					
Images	Lena	Baboon	Barbara	Cameraman	Pepper
Notre scheme	7.9970	7.9993	7.9993	7.9972	7.9992
Ref [64]	7.9980	7.9973	-	7.9974	7.9976
Ref [65]	7.9972	-	-	7.9970	7.9972
Ref [66]	7.9980	7.9973	-	7.9974	7.9976
Ref [7]	7.9992	7.9992	7.9993	7.9974	7.9992

TABLE 4.5 – Comparaison externe : L'entropie.

Le tableau ci-dessous 4.6 résente les coefficients de corrélation pour différentes images (Lena, Baboon, Barbara, Cameraman, et Pepper) obtenus par notre approche proposée ainsi que par plusieurs autres méthodes référencées :

Coefficient de corrélation de l'image					
Images	Lena	Baboon	Barbara	Cameraman	Pepper
Notre scheme	-0.0011	0.00004	0.00004	0.0020	0.0004
Ref [7]	-0.0021	0.0008	0.0009	-0.0013	0.0016
Ref [67]	0.0018	-0.0009	0.0007	-	-0.0014
Ref [65]	0.0036	-	-	0.0167	0.0252
Ref [66]	0.0033	0.0007	-	0.0014	0.0023

TABLE 4.6 – Comparaison externe : La corrélation.

4.5 Conclusion

Ce chapitre a présenté en détail notre algorithme de cryptage d'image proposé, en mettant en lumière ses principaux éléments et leur fonctionnement. Nous avons no-

tamment mis en avant l'utilisation de plusieurs cartes chaotiques unidimensionnelles pour générer des séquences de nombres aléatoires, renforçant ainsi la complexité du processus de cryptage. L'implémentation de notre algorithme a été réalisée dans l'environnement MATLAB. Nous avons également détaillé les caractéristiques matérielles et logicielles de notre environnement de travail.

De plus, nous avons présenté l'interface graphique développée pour faciliter l'utilisation de notre algorithme de cryptage, en mettant en avant ses différentes fonctionnalités. Les résultats expérimentaux de notre schéma de cryptage d'images démontrent que notre système proposé est à la fois efficace et sécurisé.

Enfin, les comparaisons externes avec d'autres schémas de chiffrement d'image existants montrent que l'algorithme proposé présente des performances très avantageuses.

Conclusion générale

Aujourd'hui, l'utilisation croissante des images entraîne une transmission importante de ce type de données entre les réseaux en général et l'Internet en particulier. Cela rend indispensable la confidentialité de ces données.

Dans ce mémoire, nous nous intéressons à la cryptographie des images dans le but de sécuriser les images numériques par une approche chaotique utilisant les cartes chaotiques. Pour ce faire, nous avons proposé l'utilisation de deux cartes chaotiques améliorées unidimensionnelles (1D) : la carte logistique améliorée (ILM) et la carte sinusoïdale améliorée (ISM).

Les résultats expérimentaux démontrent que l'algorithme suggéré présente un niveau élevé de confusion. Cela indique que l'espace clé est adéquat, ce qui rend infaisable une attaque à la force brute. De plus, après le cryptage, l'histogramme de l'image chiffrée est très uniforme. Ainsi, l'attaquant ne peut pas extraire d'information de l'histogramme de l'image chiffrée.

Pour évaluer précisément la robustesse de la sensibilité de la clé et les changements entre l'image cryptée et l'image d'origine, nous avons utilisé deux mesures importantes : le NPCR (Number of Pixels Change Rate) et l'UACI (Unified Average Changing Intensity). Nous avons obtenu des valeurs très satisfaisantes. L'algorithme suggéré a également été considérablement amélioré en ce qui concerne l'entropie et la corrélation entre les pixels adjacents. Ainsi, l'algorithme suggéré met en évidence l'efficacité et la sécurité de notre système.

Enfin, les comparaisons des résultats d'autres schémas de chiffrement d'image existants démontrent que l'algorithme proposé présente des performances très avanta-

geuses.

Bibliographie

[1] L. Hachemi Guerrout. Home, ecole nationale supérieure d'informatique, laboratory lmc, 2024. Accessed : 2024-07-01.

[2] Joannie Therrien. Tout sur la résolution, 2024. Consulté le 1er juillet 2024.

[3] iMedias. Différence entre une image matricielle et une image vectorielle, 2024. Consulté le 1er juillet 2024.

[4] Aimeur Akram. Conception et implémentation d'un système hybride pour la sécurité de données : application aux images numériques, 2017. Année universitaire 2016/2017.

[5] Pixees. Les images numériques, 2024. Consulté le 1er juillet 2024.

[6] Renaud Dumont. Cryptographie et sécurité informatique. *Faculté des Sciences Appliquées*, 2010.

[7] F Hadji. Conception et réalisation d'un système de cryptage pour les images médicales. *UNIVERSITE MOHAMED BOUDIAF-M'SILA FACULTE DES MATHEMATIQUES ET DE L*, 2018.

[8] family=Delestan given i=LL/S, given=Lionel Lejeune / Serge. Chiffrement cryptographie - aspect technique. Dernier accée le 21/04/2024.

[9] Kinsta. Qu'est-ce que le cryptage de données ? définition, types et meilleures pratiques - kinsta®. Dernier accée le 21/04/2024.

[10] Ljupco Kocarev and Shiguo Lian. *Chaos-based cryptography : Theory, algorithms and applications*, volume 354. Springer, 2011.

[11] J. M. T. Thompson, H. B. Stewart, and R. Turner. Nonlinear dynamics and chaos. *Computers in Physics*, 4 :562–563, 1990.

[12] Akram Aimeur. Conception et implémentation d'un système hybride pour la sécurité de données : application aux images numériques. Master's thesis, Université Mohamed Boudiaf - M'Sila, 2017. Mémoire présenté pour l'obtention du diplôme de Master Académique.

[13] Aissam Djemaa, Aissa Boubednikh, and Noura Encadreur Louzzani. *Réalisation d'un Système de Cryptage des Images Numérique basé sur le Chaos*. PhD thesis, université de jijel, 2021.

[14] Pauline Puteaux. *Analyse et traitement des images dans le domaine chiffré*. PhD thesis, Université Montpellier, 2020.

[15] Salwa K Abd-El-Hafiz, Sherif H AbdElHaleem, and Ahmed G Radwan. Novel permutation measures for image encryption algorithms. *Optics and Lasers in Engineering*, 85 :72–83, 2016.

[16] BENAISSI Sellami. *Cryptography and image encryption*. PhD thesis, Mohamed Boudiaf University of M'Sila, 2020.

[17] M. Benabdellah. *Outils de compression et de cryptocompression : Applications aux images fixes et vidéo*. PhD thesis, Université Mohammed V-Agdal, Rabat, Maroc, 2007.

[18] Ammar BOUCHEMEL. *Contribution à la transmission des images compressées : Application aux systèmes de télécommunications*. ThÈse, 2018.

[19] Sanket Sarwade. Comprendreanding Types de cryptographie : symétrique, asymétrique, hachage et plus encore. . ., 10 2023.

[20] Jian Zhang, Dongxin Fang, and Hongxiang Ren. Image Encryption Algorithm Based on DNA Encoding and Chaotic Maps. *Mathematical problems in engineering*, 2014 :1–10, 1 2014. Dernier accée le 24/04/2024.

[21] Saad Nora. *L'apport des bandelettes par rapport aux ondelettes dans les applications de traitement d'image*. PhD thesis, Université Mouloud Mammeri, 2012.

[22] . Ouali Assia Boukabene Randa. *Segmentation des IRM-3D en utilisant les champs aléatoires de Markov cachés et cuckoo search technique.* PhD thesis, Ecole nationale supérieure d'informatique, 2020.

[23] Compart. Bpp - bits per pixel, 2024. Accessed : 2024-07-01.

[24] HADJI Faiçal. Conception et réalisation d'un système de cryptage pour les images médicales. Mémoire de master académique, Université Mohamed Boudiaf - M'Sila, 2018.

[25] David Ameisen. Qu 'est-ce qu 'une image numérique. In *Conference Paper*, volume 57, pages 169–172, 2013.

[26] louis jérome. Résolution, définition d'une image. https ://edu1d.ac-toulouse.fr/politique-educative-31/site-ressources31/files/04-photofiltre7-resolution-definition-simplifie.pdf, Février 2021. Dernier accée le 20/04/2024.

[27] Youcef Boucetta and Mohammed Haddouche. Détection, poursuite et comptage d'objets par la vision artificielle. Mémoire de projet de fin d'études, Université SAAD DAHLAB de BLIDA, 2017.

[28] BLOG MACAP. Qu'est-ce qu'une image vectorielle ? https ://www.macapflag.com/blog/image-vectorielle/, Février 2020. Dernier accée le 18/03/2024.

[29] Richard Chbeir. *Modélisation de la description d'images : Application au domaine médical.* PhD thesis, Institut National des Sciences Appliquées de Layon, France, Décembre 2001.

[30] Nirina R. Tout savoir sur la cryptographie : définition, principes et utilisation. 8 2022. Dernier accée le 21/04/2024.

[31] Yamina ZERAGUI and Sabah MAAROUF. *Cryptage d'images numériques à la base de carte chaotique.* PhD thesis, Université Ibn Khaldoun-Tiaret-, 2020.

[32] Mohammed Kaddouri, Samira Encadreur Dib, and Mourad Grimes. *Conception et réalisation d'un crypto-système pour la sécurisation des données médicales.* PhD thesis, Université de Jijel, 2021.

[33] Bhavya Aggarwal Sabrina Khoulalène. Les 7 meilleures méthodes de chiffrement des données en 2024. Dernier accée le 24/04/2024.

[34] Sung-Ming Yen and Kuo-Hong Liao. Shared authentication token secure against replay and weak key attacks. *Information processing letters*, 62(2) :77–80, 4 1997. Dernier accée le 24/04/2024.

[35] Fatma Zahra Abdellaoui and Zineb Zerfaoui. *Synchronisation du chaos dans les systèmes dynamiques discrets non linéaires*. PhD thesis, Université Larbi Tébessi-Tébessa, 2022.

[36] Ouerdia Megherbi. *Etude et réalisation d'un système sécurisé à base de systèmes chaotiques*. PhD thesis, Université Mouloud Mammeri, 2013.

[37] Toufik Bekkouche. *Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes*. PhD thesis, Nom de l'Université, octobre 2018. Thèse de doctorat en sciences.

[38] Samia Belkacem. *Chaos based image watermarking*. PhD thesis, Université Hadj Lakhdar Batna, Année de soutenance. Thèse de doctorat en sciences en électronique.

[39] Amina Bessam. Etude d'un système dynamique chaotique. Master's thesis, Université Mohamed Khider, Biskra, juin 2020. Mémoire présenté en vue de l'obtention du diplôme de Master en Mathématiques, Option : Analyse.

[40] Hana Elhachi. Sécurisation de la couche physique ofdm dans un réseau de capteurs : Application sur les images médicales. Master's thesis, Université de Guelma, Année de soutenance. Mémoire de Fin d'Etude pour l'Obtention du Diplôme de Master Académique.

[41] Tifouti Miloud Agaguena Houdjatoulah. Etude et simulation d'un système de cryptage d'images à base de chaos. 2023.

[42] Fatma Zohra Terchoune and Hanaa Lina Mehdad. La cryptographie des images numériques par des cartes chaotiques unidimensionnelles (1d). Master's thesis, Université de Djelfa, Année de soutenance. Mémoire préparé en vue de l'obtention du diplôme de Master.

[43] BENAISSI Sellami. *image encryption based on chaotic maps*. PhD thesis, Mohamed Boudiaf University of M'Sila, 10 2021.

[44] Karima Amara Korba. *La Sécurité des Réseaux de Capteurs sans fil Multimédia par des Systèmes Chaotiques*. PhD thesis, Université 08 mai 45 Guelma (Algérie), 2022.

[45] Hassan Noura. *Conception et simulation des générateurs, crypto-systèmes et fonctions de hachage basés chaos performants*. PhD thesis, université de Nantes, 2012.

[46] CHOUAICHIA Safa MOUSSAOUI Lina. Etude et simulation d'un crypto-système basé sur l'algorithme aes-gcm. 2023.

[47] dCode. Chiffre par substitution. Dernier accée le 13/05/2024.

[48] Avi Dixit, Dahale Bhagwan, and Pratik Dhruve. Image encryption using permutation and rotational xor technique. *Proceedings of SIPM, FCST, ITCA, WSE, ACSIT, CS & IT*, 06 :01–09, 2012.

[49] Qu'est-ce que la cryptographie quantique ? | ibm. Dernier accée le 24/04/2024.

[50] Ye Guodong, Liu Min, and Wu Mingfa. Double image encryption algorithm based on compressive sensing and elliptic curve [j]. *Alexandria Engineering Journal*, 61(9) :6785–6795, 2022.

[51] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of Applied Cryptography*. CRC press, 1996.

[52] Gonzalo Alvarez and Shujun Li. Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, 16(8) :2129–2151, 2006.

[53] A. Walker, E. Wolfart, R. Fisher, and S. Perkins. Image processing learning resources explore with java. Dernier accée le 10/03/2024.

[54] A. Beloucif. *Contribution à l'étude des mécanismes cryptographiques*. PhD thesis, Université de Batna2, 2016. Thèse en vue de l'obtention du diplôme de Doctorat en Informatique.

[55] Claude E. Shannon. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1) :3–55, 2001.

[56] J. S. Teh, M. Alawida, and Y. C. Sii. Implementation and practical problems of chaos-based cryptography revisited. *Journal of Information Security and Applications*, 50(Art. no. 102421), February 2020.

[57] R. Lan, J. He, S. Wang, T. Gu, and X. Luo. Integrated chaotic systems for image encryption. *Signal Processing*, 147 :133–145, 2018.

[58] A.P. Kari, A.H. Navin, A.M. Bidgoli, and M. Mirnia. A new image encryption scheme based on hybrid chaotic maps. *Multimedia Tools and Applications*, 80(2) :2753–2772, 2021.

[59] Matlab - le langage du calcul technique. Dernier accée le 13/05/2024.

[60] Farhan Musanna and Sanjeev Kumar. Image encryption using quantum 3-d baker map and generalized gray code coupled with fractional chen's chaotic system. *Quantum Information Processing*, 19, 08 2020.

[61] Ibrahim Yasser, Fahmi Khalifa, Mohamed A Mohamed, Ahmed S Samrah, et al. A new image encryption scheme based on hybrid chaotic maps. *Complexity*, 2020, 2020.

[62] Jiahui Wu, Xiaofeng Liao, and Bo Yang. Image encryption using 2d hénon-sine map and dna approach. *Signal processing*, 153 :11–23, 2018.

[63] Erivelton G Nepomuceno, Lucas G Nardo, Janier Arias-Garcia, Denis N Butusov, and Aleksandra Tutueva. Image encryption based on the pseudo-orbits from 1d chaotic map. *Chaos : An Interdisciplinary Journal of Nonlinear Science*, 29(6), 2019.

[64] Shubo Liu, Jing Sun, and Zhengquan Xu. An improved image encryption algorithm based on chaotic system. *J. Comput.*, 4(11) :1091–1100, 2009.

[65] Hamada Aymen Bousnoubra Yasser. La cryptographie des images numériques par la carte logistique chaotique. 2020.

[66] Benyamin Norouzi, Sattar Mirzakuchaki, Seyed Mohammad Seyedzadeh, and Mohammad Reza Mosavi. A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. *Multimedia tools and applications*, 71 :1469–1497, 2014.

[67] FK Tabash, MQ Rafiq, and M Izharrudin. Image encryption algorithm based on chaotic map. *International Journal of Computer Applications*, 64(13), 2013.

[68] COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES. Photographie numérique caractéristiques des images. http ://hazmat.free.fr/7-photo/photo-images.html, Février 2019. Dernier accée le 18/03/2024.

[69] family=Ionos given i=LÉ, given=L'équipe Éditoriale. Aperçu des procédures de chiffrement. Dernier accée le 21/04/2024.

[70] Cherifa Boukhari, Marwa Labreche, and Karim Encadreur Kemih. *Cryptage des images médicales par tatouage*. PhD thesis, Université de Jijel, 2023.

[71] HADJ-SAID Naima and ALI PACHA Adda. Sécurité analogique de l'information :(sécurité du futur). 2011.