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 : *GSI*

Thème

Conception et implémentation d'un algorithme de cryptage d'images basé sur des cartes chaotiques multidimensionnel

---

Encadré par

— BENAISSI Sellami

Réalisé par

— Laiche Newel

— Laifaoui Rima

2023/2024

Remerciements

Avant de présenter ce travail, nous tenons à remercier Dieu tout puissant, de nous avoir d'arriver à ce niveau d' etude, et aussi pour nous avoir donné beaucoup de patience et de courage sans oublier nos parents qui n'ont lésiné sur aucun problème c'est normal de nous donner tout pour nous apporter toute l'aide nécessaire pour atteindre ce niveau qui nous permettra d'assurer notre avenir.

A travers cette modeste thèse nous tenons à présenter nos sincères remerciements et notre profonde reconnaissance à notre aimable encadreur S.BENAISSI qui nous a donné son temps et son aide. Nous tenons à vous dire que vos conseils et vos recommandations ont largement contribuées à ce succès dont nous vous seront loyalement redevable.

Nous adressons aussi notre sincère reconnaissance à tous les enseignants au département informatique de l'université Akli Mohand Oulhadj de Bouira pour leurs aides, soutiens et leurs conseils.

Enfin , nos remerciements vont egalement aux membres de juré d'avoir accepter de juger notre travail.

Dédicaces

Je dédie ce modeste travail en signe de respect, reconnaissance et de remerciement
À mes chers parents :
Ma maman : qui a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie.
Mon père : qui peut être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie.

Je dédie ma graduation à mon cher frère Hamza, que Dieu ait pitié de lui, qui nous a quittés il y a peu de temps. J'aurais souhaité qu'il soit avec moi en ce jour. "J'ai accompli ce que vous m'avez demandé malgré les circonstances difficiles que j'ai traversées."

Je dédie également ma graduation à mon petit frère Khaled, qui m'a soutenu dans mes moments difficiles.

LAICHE Nawel

Dédicaces

Je dédie ma graduation à mon cher père, que Dieu ait pitié de lui, et à ma chère mère, qui a été mon soutien dans ma carrière universitaire et qui s'est tenue à mes côtés dans les crises de ma vie et dédie ma graduation , à mes frères et sœurs , à mes beaux-frères , à mes belles sœurs ,à mes neveux et niéces, je dédie ce travail dont le grand plaisir leurs revient en premier lieu pour leur conseils, aides et encouragements.

A toutes mes amies : Sakina ,Rachda ,Ibtissam et Khadidja qui m'ont accompagné durant ces années d' etude et m'ont apporté la joie et le bonheur dans ma vie.

LAIFAOUI Rima

Abstract

Image encryption has emerged as a pivotal technique in secure communication, garnering significant attention in recent times. This method is widely acclaimed for its efficacy in safeguarding sensitive data by harnessing maximum quality from noisy images. Chaotic map-based encryption methods, such as the modified Chirikov map and non-linear 3D logistic map, exhibit robustness and randomization, thus fortifying security measures and enhancing the randomness of the ciphered images.

Keywords : Image Encryption, Chirikov Map, 3D Logistic Map, Chaotic Maps.

Résumé

Le cryptage d'images a récemment attiré beaucoup d'attention en tant que méthode de communication sécurisée. Cette technique est largement reconnue pour son efficacité dans la protection des données sensibles en exploitant au maximum la qualité des images bruitées. Les méthodes de cryptage d'images basées sur des cartes chaotiques, telles que la carte Chirikov modifiée et la carte logistique 3D non linéaire, offrent une robustesse et une randomisation, renforçant ainsi les mesures de sécurité et améliorant la randomisation des images chiffrées.

Mots-clés : Cryptage d'Image, Carte Chirikov, Carte Logistique 3D, Cartes Chaotiques.

ملخص

تشفير الصور جذب مؤخرا الكثير من الاهتمام كوسيلة للتواصل الآمن. تعرف هذه التقنية بكفاءتها في حماية البيانات الحساسة من خلال استغلال جوده الصور المشوشة الى اقصى حد. توفر طرق تشفير الصور القائمة على الخرائط الفوضوية, مثل خريطة شيريكوف و الخريطة اللوجيستية ثلاثية الابعاد غير خطية, متانة و عشوائية, مما يعزز إجراءات الأمان ويحسن من عشوائية الصور المشفرة.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

DPI	Dot Per Inch
PPP	Pixels Par Pouce
RVB	Rouge-vert-bleu
CMJN	Cyan-Magenta-Yellow-Key
DES	Data Encryption Standard
RSA	le Rivest Shamir Adelman (nommé par les initiales de ses trois inventeurs.)
IDEA	International Data Encryption Algorithm
LE	Exposant de Liapounov
AES	Advanced Encryption Standard
LSE	L'entropie locale de Shannon
PSNR	Rapport signal sur bruit maximal
MSE	Erreur quadratique moyenne
NPCR	numéro de pixel change rate
UACI	Unified Average Change Intensity

Introduction générale

Dans notre ère numérique actuelle, les images jouent un rôle indispensable dans notre vie quotidienne, que ce soit à des fins personnelles ou commerciales. Elles constituent une forme significative de mémoire, de créativité et de transmission d'informations. Avec l'importance croissante des images, nécessité de les protéger et de les sécuriser contre. Toute utilisation non autorisée ou intrusion est devenue primordiale.

Le chiffrement des images consiste à transformer les données numériques qui représentent une image, de manière à les rendre illisibles ou inutilisables sans la clé de déchiffrement appropriée. Parmi les méthodes efficaces pour accomplir cela, l'usage de cartes chaotiques multidimensionnelles semble être une méthode prometteuse pour crypter les images.

L'idée de chiffrer les images en utilisant des cartes chaotiques repose sur l'exploitation du chaos pour générer des clés de chiffrement robustes et complexes. Les cartes chaotiques multidimensionnelles sont particulièrement reconnues pour leur capacité à produire des séquences de nombres aléatoires et imprévisibles. En utilisant ces séquences comme clés de chiffrement, il devient extrêmement difficile pour une personne non autorisée de déchiffrer et de récupérer les informations d'origine.

Dans ce contexte, cette étude se propose de développer un algorithme performant pour le chiffrement des images en utilisant des cartes chaotiques multidimensionnelles. Nous évaluerons les performances de cet algorithme et le comparerons avec d'autres méthodes traditionnelles de chiffrement d'images, dans le but de proposer une solution offrant un haut niveau de sécurité et d'efficacité pour la protection des images numériques.

Est-ce que cet algorithme peut garantir une sécurité et une flexibilité élevées dans les opérations de chiffrement et de déchiffrement ?

Chapitre 1

Généralités sur l'image

1.1 Introduction

Étant donné l'importance des images numériques et la valeur des données qu'elles renferment, ce chapitre examinera les concepts fondamentaux de l'image à travers les diverses catégories d'images numériques. Nous étudierons ensuite les techniques de cryptage des images. Nous allons ensuite étudier les formats les plus importants et les plus connus.

1.2 Définition d'image

L'image numérique est une représentation visuelle de données ou d'informations à l'aide de chiffres et de formes numériques. La photographie numérique est composée d'un ensemble de pixels (petits éléments colorés) qui forment une scène ou une image complète. Ces pixels sont enregistrés numériquement dans des fichiers d'image, et chaque pixel contient des informations sur la couleur, la luminosité et le contraste pour représenter l'image dans son ensemble. Dans notre société contemporaine, l'image numérique est l'une des formes de données numériques les plus courantes et les plus utilisées. Elle est utilisée dans différents domaines tels que la photographie, l'art numérique, la médecine, le marketing, les communications, l'éducation, la sécurité, et bien d'autres encore.[**33**]

1.3 Image numérique

Une image numérique est une notion abstraite (des données numériques) qui prend une signification pour nos yeux avant sa visualisation, c'est-à-dire la manipulation du logiciel adéquat. Elle est composée d'éléments essentiels (appelés pixel) qui représentent chacun une partie de l'image.

Ainsi, une image est définie comme suit :

— La largeur et la hauteur des pixel qui la composent peuvent varier à peu près à l'infini.

— La diversité des couleurs grises ou des couleurs que chaque pixel peut avoir (on parle de la dynamique de l'image).

L'ensemble de ces données présentes dans l'image est structuré de façon précise afin de faciliter leur stockage. On définit ainsi des formats d'images qui correspondent à cette structure particulière.[**33**]

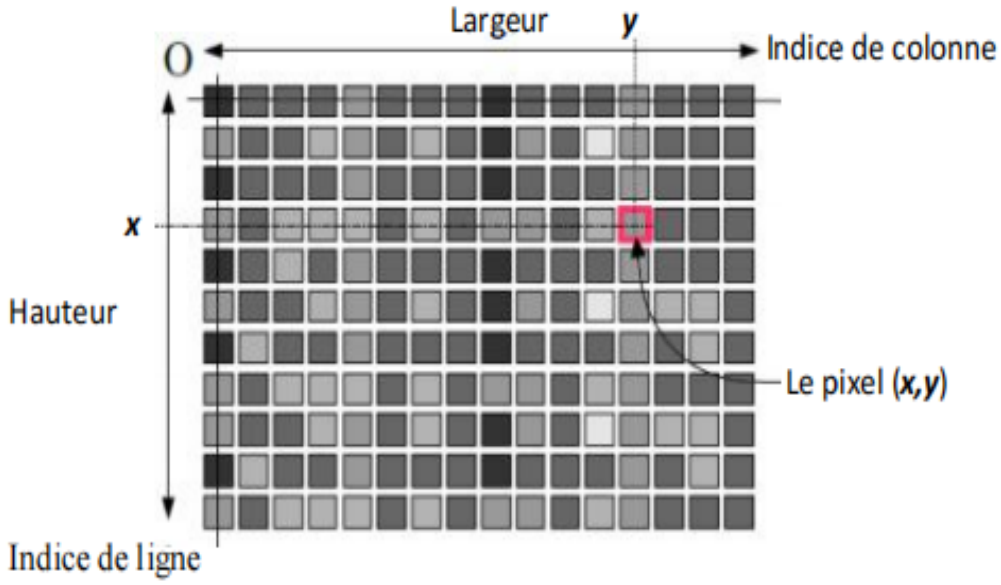

FIGURE 1.1 – Représentation d'image numérique.[43]

1.4 Caractéristiques d'une image numérique

1.4.1 Pixel

L'élément essentiel d'une image ou d'un écran est le pixel (littéralement « picture element » en anglais), c'est-à-dire un point. Tous ces pixels sont regroupés dans un tableau à deux dimensions (largeur et hauteur) pour former l'image.[**1**]

Les points (ou pixels) d'une image numérique en largeur et en hauteur (le nombre de colonnes et de lignes).

1.4.2 La taille

L'image est mesurée en fonction de sa position dans le codage binaire. L'octet est son unité.[**2**]

Un exemple similaire peut être utilisé pour une image de 512 × 512 en gris :

Nombre de pixels :

$$512 \times 512 = 262{,}144 \text{ pixels}$$

Taille de chaque pixel :

$$8 \text{ bits}/8 = 1 \text{ octet}$$

Le poids de l'image est ainsi égal à :

$$262{,}144 \times 1 = 262{,}144 \text{ octets}$$

Taille = nombre d'octets pour chaque pixel × Taille de chaque pixel .

Donc, pour cette image, la taille totale serait de 262,144 octets.

Taille = nombre d'octets pour chaque pixel × Taille de chaque pixel .

1.4.3 Résolution

La résolution d'une image est déterminée en utilisant 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. La résolution sera impactée par la qualité de la numérisation.

$$\text{Précision} = \frac{\text{Taille de chaque pixel}}{\text{Longueur}}$$ [3]

Le niveau de détail représenté sur une image est déterminé par la résolution d'une image. Les deux équations suivantes doivent être prises en compte pour la numérisation :

$$\text{Largeur en pixels : } X \times \text{résolution} = x \text{ pixels}, \tag{1.1}$$

$$\text{Hauteur en pixels : } Y \times \text{résolution} = y \text{ pixels}. \tag{1.2}$$

Telle que :

— Les variables X et Y représentent les dimensions de la structure à numériser, exprimées en pouces ou centimètres (1 pouce = 2,54 centimètres).

— La résolution de numérisation est indiquée par l'item résolution.

— La taille (en pixels) de l'image est indiquée par x et y.[4]

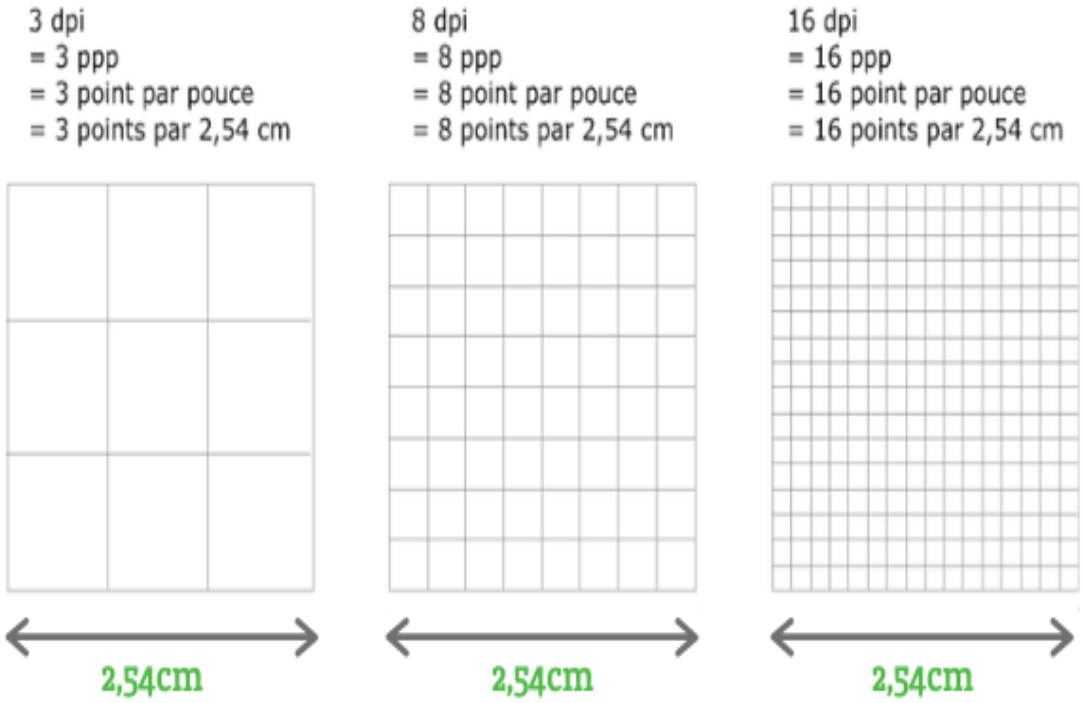

FIGURE 1.2 – Explication de résolution d'une image. [36]

1.5 Les différents types d'image

Trois types d'images sont couramment distingués :

— Image binaire : utilise deux couleurs (arrière-plan et avant-plan).

— Image monochrome : composée de différentes nuances d'une seule couleur.

— Image polychrome : utilise une gamme étendue de couleurs.

1.5.1 Images binaires (en noir et blanc)

Un graphique binaire correspond à un graphique où chaque pixel peut être représenté par 0 ou 1. Il existe une grande quantité d'outils spécialisés et de théories mathématiques pour manipuler de telles images, pour différentes raisons.

— Pendant les premiers temps du traitement des images numériques, il était difficile de traiter les images complexes en raison de problèmes de temps de calcul, de manque d'espace mémoire et de la qualité des périphériques de sortie. Par ailleurs, les premières applications (enregistrement de caractères, analyse des traces laissées dans les chambres à bulles par des particules) à partir de 1950 étaient parfaitement adaptées à ce genre d'images.

— Les images binaires offrent la possibilité de résoudre mathématiquement des problèmes en utilisant des outils comme la topologie.

L'image binaire est souvent suivie de la phase de segmentation, qui est souvent perçue comme un élément essentiel dans le domaine de la vision industrielle (détection de défauts, contrôle qualité, mesure,...).

Il est donc indispensable d'avoir deux catégories d'outils pour assurer un codage efficace (et éventuellement la compression) et pour le traitement (analyse et description des formes).[**5**]

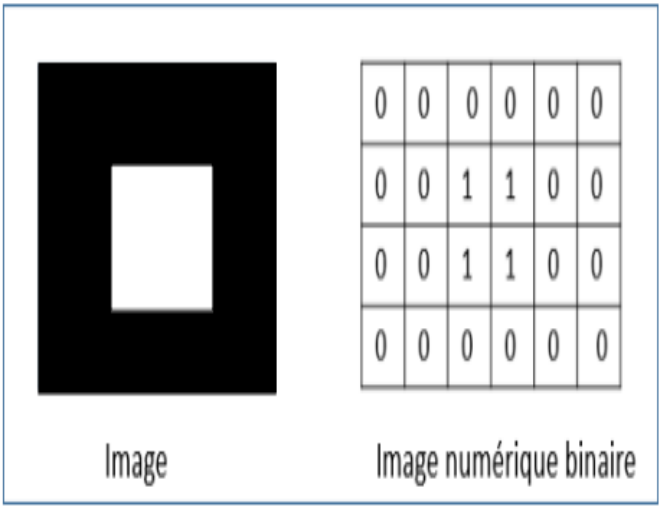

FIGURE 1.3 – Image binaire.[**37**]

1.5.2 Images à niveaux de gris (Monochromes)

Le niveau gris correspond à l'intensité lumineuse d'un point spécifique. Le pixel est capable de changer de couleur du noir au blanc à travers un nombre limité de niveaux intermédiaires. Ainsi, dans le cas des images en gris, on peut attribuer une valeur à chaque pixel de l'image qui correspond à la quantité de lumière renvoyée. À titre d'exemple, ce nombre peut varier de 0 à 255. Ainsi, chaque pixel ne représente plus 1 bit, mais 1 octet. Ainsi, le dispositif utilisé pour l'affichage de l'image doit être capable de générer les divers niveaux de gris qui y sont liés.

Le niveau de gris varie en fonction du nombre de bits employés pour représenter la « couleur » de chaque pixel de l'image. Plus ce chiffre est important, plus il y a d'opportunités.[**6**]

1.5.3 Images en couleurs (Polychromes)

Image en couleurs (RVB) :

Dans une représentation en couleurs, chaque pixel est défini par une combinaison de trois composantes : rouge (R), vert (V), et bleu (B), chacune pouvant varier dans l'intervalle de 0 à 255. En mélangeant ces trois couleurs de base, on crée ainsi une gamme étendue de teintes pour former une couleur spécifique pour chaque pixel.

En informatique, le modèle RVB (rouge, vert, bleu) est largement employé pour décrire les couleurs.

Par exemple, les valeurs {255, 255, 255} correspondent au blanc pur, {255, 0, 0} représentent le rouge pur, et {100, 100, 100} indiquent un ton de gris.

Chaque composante de couleur est représentée par un nombre dans le triplet, respectivement rouge, vert, et bleu. Ainsi, avec 3 octets par composante, l'ensemble de la représentation nécessite 24 bits au total.

En utilisant un format RVB de 16 bits par composante : Chaque composante utilise désormais 16 bits (permettant 65535 nuances chacune), ce qui fait un total de 48 bits pour l'ensemble. Cela signifie que $65535 \times 65535 \times 65535$ offre plus de 4 milliards de possibilités de couleurs différentes. [**6**]

Mode couleur CMJN (support papier) :

Dans le contexte des images destinées à l'impression, le mode couleur CMJN (cyan, magenta, jaune et noir) est primordial. Contrairement aux écrans d'ordinateur, qui utilisent le mode RVB, les logiciels comme Photoshop fragmentent les images CMJN en quatre couches distinctes, chacune représentant une couleur avec une valeur en pourcentage. Ces images sont ensuite converties en RVB pour être visualisées sur l'écran, mais pour l'utilisateur, les couches CMJN demeurent une catégorie de travail distincte.[**7**]

En employant une résolution de 8 bits par couche CMJN, chaque couleur (cyan, magenta, jaune, noir) dispose de 256 nuances possibles, totalisant ainsi 32 bits utilisés pour l'ensemble de l'image. Cela offre un potentiel de $256 \times 256 \times 256 \times 256 = 2^{32} = 4$ milliards de combinaisons.

Opter pour une résolution de 16 bits par couche CMJN double la précision, avec chaque couleur bénéficiant de 65535 nuances. Cette configuration requiert 64 bits pour représenter toutes les couches CMJN, offrant ainsi un nombre impressionnant de $65535 \times 65535 \times 65535 \times 65535 = 2^{64} = 264$ possibilités de couleurs.[**7**]

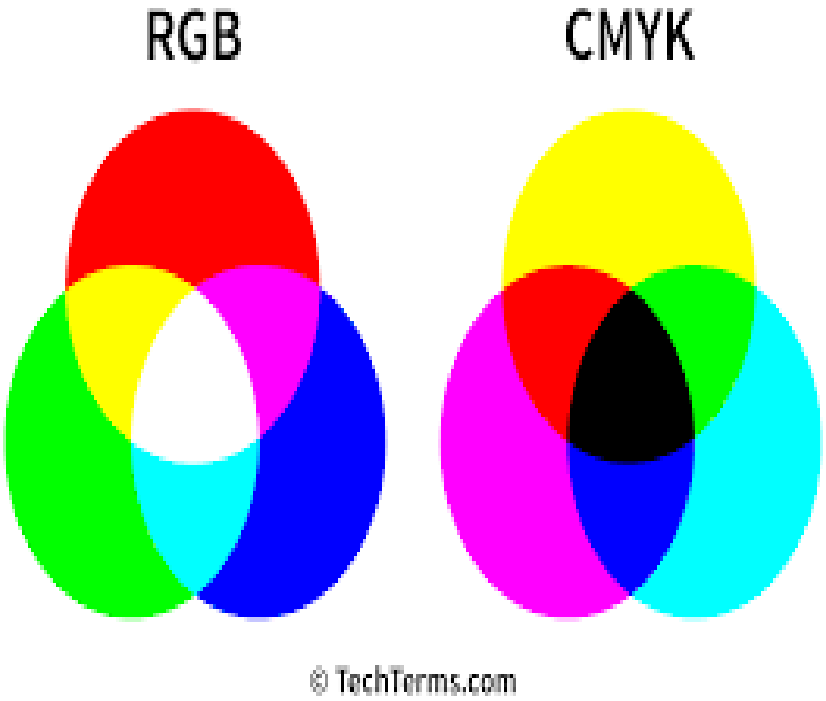

FIGURE 1.4 – couleurs .[**38**]

L'utilisation de 24 bits pour chaque point de l'image permet de visualiser en couleurs

authentiques. Le composant rouge (R) est décrié en 8 bits, le vert (V) en 8 bits et le bleu (B) en 8 bits. On peut donc représenter simultanément environ 16,7 millions de couleurs différentes. Cependant, cette théorie demeure valable, car aucun écran ne peut représenter 16 millions de points. Seulement 1 920 000 points sont affichés sur l'écran dans la résolution la plus élevée (1600 x 1200). En outre, l'œil humain ne peut pas voir autant de couleurs.

FIGURE 1.5 – Types d'images.[44]

1.6 Images Bitmap et Images Vectorielles

— **Image Bitmap (Matricielle) :** L'image bitmap, aussi connue sous le nom d'image matricielle, est constituée de pixels individuels qui symbolisent les différentes teintes.

Les images bitmap sont aujourd'hui les plus courantes et de nombreux logiciels sont spécialement conçus pour les traiter (Adobe Photoshop par exemple). En outre, l'emploi des pixels est parfait pour les images qui requièrent des effets, des ombres et des dégradés, ce qui est beaucoup plus compliqué à accomplir avec des vecteurs. Toutefois, cela comporte quelques désavantages. En premier lieu, on crée une image bitmap pour une taille précise qui est généralement constante. Autrement dit, elle est constituée de pixels fixes, ce qui signifie que toute agrandissement ou impression de l'image occasionne une diminution de qualité visible sous forme de pixels visibles.

Pour remédier à ce problème, il est possible d'améliorer la qualité de l'image ou de lui attribuer une résolution élevée dès le départ. Cependant, cela augmente considérablement la taille du fichier, ce qui peut entraîner des problèmes tels que des ralentissements sur les sites web.[**8**]

— **Image Vectorielle :** À première vue, une image vectorielle est constituée de vecteurs. Un vecteur est essentiellement un ensemble de points géométriques qui définissent des trajectoires entre ces points.

L'image vectorielle présente des avantages et des inconvénients similaires à ceux des images bitmap ! En d'autres termes, l'utilisation de l'imagerie vectorielle n'est pas particulièrement adaptée à la création d'images complexes, mais plutôt à des formes généralement simples. Cependant, lorsqu'il est agrandi, une image vectorielle ne perd pas en qualité car il n'y a pas de résolution spécifique ; les proportions entre les formes sont conservées. Une remarque cruciale : les images vectorielles sont extrêmement légères ! [**8**]

1.7 Formats de fichiers et logiciels graphiques

La création et le traitement d'images Bitmap sont réalisés avec de nombreux logiciels graphiques compatibles avec différents formats de fichiers. Le tableau ci-dessous présente les formats de fichiers les plus fréquemment utilisés ainsi que les logiciels graphiques adaptés aux formats d'images matricielles et vectorielles.

Image	Format de fichiers	Logiciels graphique
Images matricielles	TIF, JPG, BMP, PNG, GIF	Adobe Photoshop GIMP Corel PaintShop Pro
Images vectorielles	SVG, EPS, AI, CDR, WMF	Adobe Illustrator Corel Draw Inkscape

TABLE 1.1 – Formats de fichiers et logiciels graphique

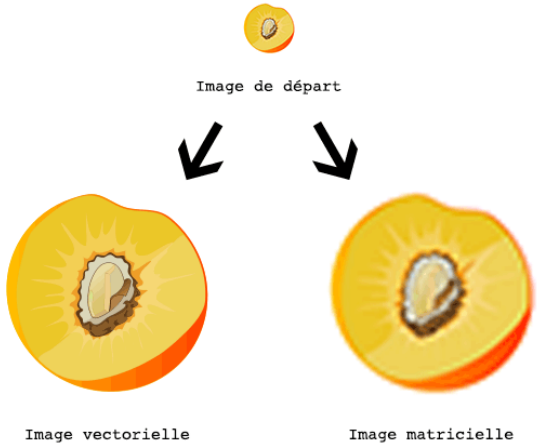

FIGURE 1.6 – Difference entre l'image vectorielle et l'image matricielle.[**39**]

1.7.1 Avantages et Inconvénients

L'Image Matricielle

— **Avantages :** Les images matricielles permettent de rendre avec précision les détails des couleurs, de créer des dégradés et des ombres sophistiquées. En augmentant la taille d'une image matricielle, il est possible d'effectuer des ajustements pixel par pixel, ce qui permet d'ajouter des effets de texture au design.

— **Inconvénients :** Généralement, les fichiers matriciels sont plus volumineux que les fichiers vectoriels. De plus, agrandir indéfiniment une image matricielle peut entraîner un flou. Ce format ne permet pas de modifier l'échelle de votre création graphique sans compromettre sa qualité. [**9**]

L'Image Vectorielle

— **Avantages :** Les images vectorielles peuvent être ajustées à tout moment sans subir de changement. Les vecteurs sont utilisés pour générer des lignes et des courbes parfaitement nettes, ce qui est parfait pour un design épuré et symétrique. Par ailleurs, les fichiers vectoriels ont souvent une taille inférieure à celle des fichiers matriciels.

— **Inconvénients :** Les vecteurs ne peuvent pas reproduire les nuances subtiles de couleur ni les effets d'ombres complexes, donnant ainsi un aspect plus plat aux images vectorielles par rapport aux images matricielles. [**9**]

1.8 Conclusion

Dans ce chapitre, nous avons exploré en profondeur le domaine des images,le chapitre sur les images et leurs caractéristiques a mis en lumière l'importance de comprendre les différentes composantes des images numériques. Nous avons exploré les concepts fondamentaux tels que les pixels et la résolution, qui sont essentiels pour comprendre la qualité et la netteté d'une image. De plus, nous avons examiné les différents types d'images, y compris les images binaires, en niveaux de gris et en couleur, chacun ayant ses propres applications et avantages.

En outre, nous avons étudié les images matricielles et vectorielles. Les images matricielles sont caractérisées par leur composition en pixels, offrant une haute définition des couleurs et de la luminosité, mais pouvant entraîner une perte de qualité lorsqu'elles sont étirées ou compressées. D'autre part, les images vectorielles sont définies par des formules mathématiques, ce qui leur permet de conserver leur netteté et leur qualité indépendamment de leur taille, mais elles peuvent être plus difficiles à éditer et à manipulers.

Chapitre 2

Généralité sur la cryptographie

2.1 Introduction

La cryptographie, qui peut être considérée comme l'art de communiquer de manière sécurisée et secrète, remonte à des millénaires. Son histoire est riche en évolutions techniques et en intrigues, souvent tissées dans les coulisses des grandes civilisations et des conflits historiques.

Les origines de la cryptographie remontent à l'Antiquité, où des civilisations telles que les Égyptiens et les Babyloniens utilisaient des méthodes basiques pour chiffrer leurs messages. Cependant, c'est avec l'essor de l'Empire romain que la cryptographie a pris une place significative dans les affaires militaires et diplomatiques. Les Césars utilisaient des techniques de substitution et de transposition pour protéger leurs communications contre les espions ennemis.

Une autre grande avancée a eu lieu pendant la Renaissance avec l'apparition de méthodes plus sophistiquées telles que la substitution polyalphabétique, popularisée par le polymathe italien Leon Battista Alberti au 15ème siècle. Plus tard, au 16ème siècle, le mathématicien allemand Johannes Trithemius a écrit sur la stéganographie, l'art de cacher des messages à l'intérieur d'autres messages.

Le 20ème siècle a été témoin de progrès révolutionnaires dans le domaine de la cryptographie, en particulier pendant les deux guerres mondiales. La Première Guerre mondiale a vu l'utilisation extensive du chiffre allemand Enigma, une machine de cryptage mécanique réputée inviolable à l'époque. Cependant, grâce aux efforts des cryptanalystes, notamment ceux de l'équipe de Bletchley Park dirigée par Alan Turing pendant la Seconde Guerre

mondiale, Enigma a été déchiffrée, jouant un rôle crucial dans la victoire des Alliés.

Après la guerre, la cryptographie s'est rapidement développée avec l'avènement de l'informatique et de la théorie mathématique moderne. Claude Shannon, parmi d'autres chercheurs, a établi les bases théoriques de la sécurité informatique, tandis que l'évolution de l'informatique quantique a révélé de nouvelles opportunités en cryptanalyse et en cryptographie quantique.

De nos jours, la cryptographie est présente partout dans notre vie quotidienne, jouant un rôle crucial dans la protection des communications en ligne, des opérations financières et des informations sensibles. Les données sensibles sont protégées contre les regards indiscrets grâce à l'utilisation d'algorithmes sophistiqués et de protocoles de cryptographie sécurisés, garantissant ainsi la confidentialité et l'intégrité numériques. Le chaos est un élément essentiel dans de nombreux algorithmes de cryptage.

Dans ce chapitre, nous étudierons le concept de chiffrement et mettrons en lumière sa relation avec le chaos.

2.2 La cryptographie

L'art et la science de la cryptographie (du grec ancien *kryptos*, qui signifie « cacher » et *graphein*, qui signifie « écrire ») consistent à préserver l'information en la transformant de manière à ce qu'elle soit invisible pour toute personne qui n'a pas les clés pour la lire.

Dans notre époque numérique, où les données sont échangeées à une vitesse effrénée à travers les réseaux informatiques, le rôle crucial de la cryptographie informatique est de garantir la confidentialité, l'intégrité et l'authenticité des informations.

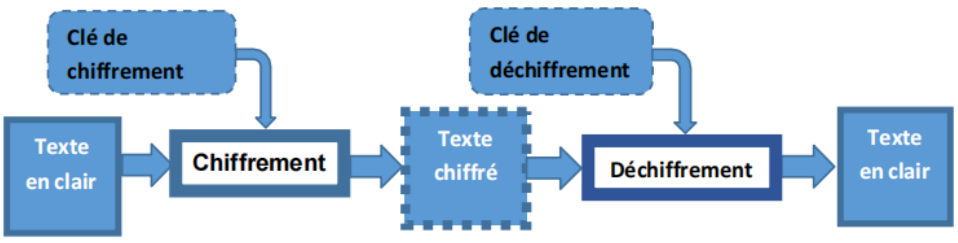

FIGURE 2.1 – Schéma général de la cryptographie.[45]

2.2.1 Vocabulaire de base de la cryptographie

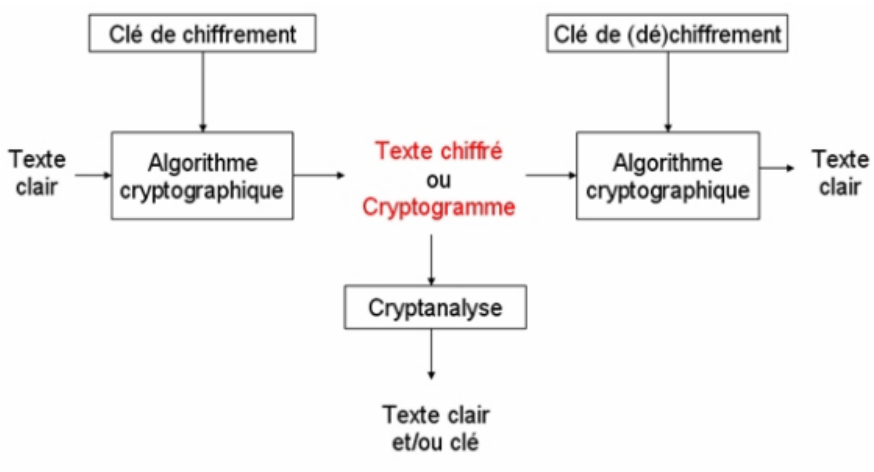

FIGURE 2.2 – Protocole de cryptage.[46]

Quelques définitions et concepts fondamentaux en cryptographie sont exposés :
Présenter Brièvement la méthode de conception choisie.

— **Cryptologie :** Il s'agit d'une science mathématique structurée en deux domaines : la cryptographie et la cryptoanalyse.

— **Cryptographie :** La cryptographie est l'étude des méthodes qui permettent d'envoyer des données de manière confidentielle sur un support donné.

— **Chiffrement :** Le chiffrement consiste à modifier une information (texte, message,...) de façon à la rendre inaccessible à une autre personne que celle qui a élaboré le message et celle qui en est le destinataire.

La technique de déchiffrement consiste à extraire le texte clair du texte chiffré.

— **Texte chiffré :**Le cryptogramme, également appelé texte chiffré, correspond à un texte obtenu en utilisant un chiffrement sur un texte clair.

— **Clef :**Ce paramètre permet de réaliser des opérations de chiffrement et/ou de déchiffrement.

Dans le cas d'un algorithme symétrique, la clé est identique pour les deux opérations. Quant aux algorithmes asymétriques, cela diffère pour les deux opérations.[**10**]

Il est essentiel de conserver les clés de manière sécurisée et de les protéger afin que seul leur propriétaire puisse les accéder et les utiliser.

Il existe en général deux catégories de clés :

- **Les clés symétriques :** Ces clés servent à chiffrer et déchiffrer des données. Il s'agit alors de cryptage symétrique ou de cryptage à clé confidentielle.
- **Les clés asymétriques :** Ces clés sont utilisées dans le domaine du cryptage asymétrique (également appelé cryptage à clé publique). Dans ce cas, le chiffrement et le déchiffrement sont effectués avec une clé différente.

— **Cryptanalyse :** Contrairement à la cryptographie, il vise à générer un texte clair à partir de textes chiffrés en identifiant les lacunes des algorithmes employés.

— **Décrypter :** Il est impossible de décrypter un cryptogramme pour retrouver le message en clair sans disposer de la clé de déchiffrement (« casser » le code secret).

— **Cryptosystème :** Il s'agit de toutes les clés disponibles (espace de clés), des textes clairs et chiffrés qui peuvent être associés à un algorithme spécifique.[**11**]

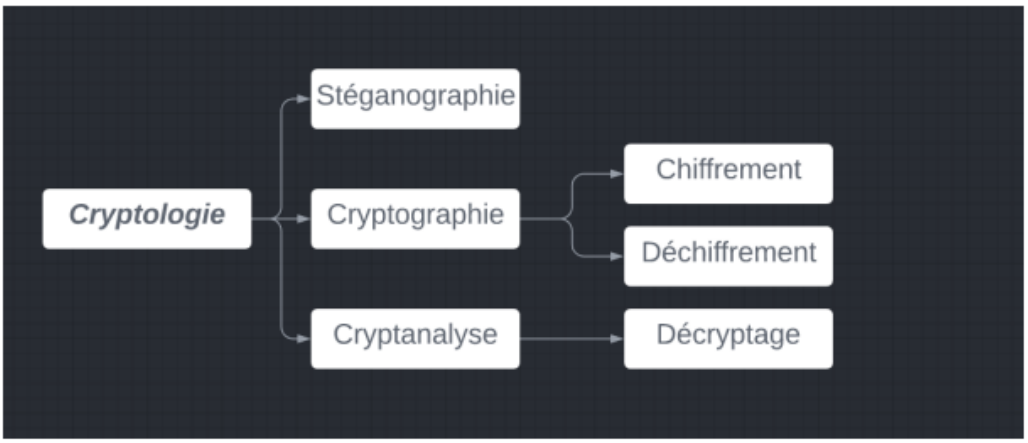

FIGURE 2.3 – Structure de la cryptologie.

2.2.2 Objectifs de la cryptographie

Pour garantir la sécurité des informations transmises, les objectifs de la cryptographie sont fondamentaux. L'objectif principal de la cryptographie est de :

1. Confidentialité : La cryptographie garantit que seuls des utilisateurs autorisés peuvent consulter les données.
2. Intégrité : Elle garantit que les données n'ont pas été altérées.
3. Authentification :La cryptographie permet de vérifier l'authenticité des données ou l'identité d'un utilisateur.

4. Non-répudiation :Elle a pour but d'empêcher un utilisateur de nier des engagements ou des actions antérieures. [**12**]

2.2.3 Classes de la cryptographie :

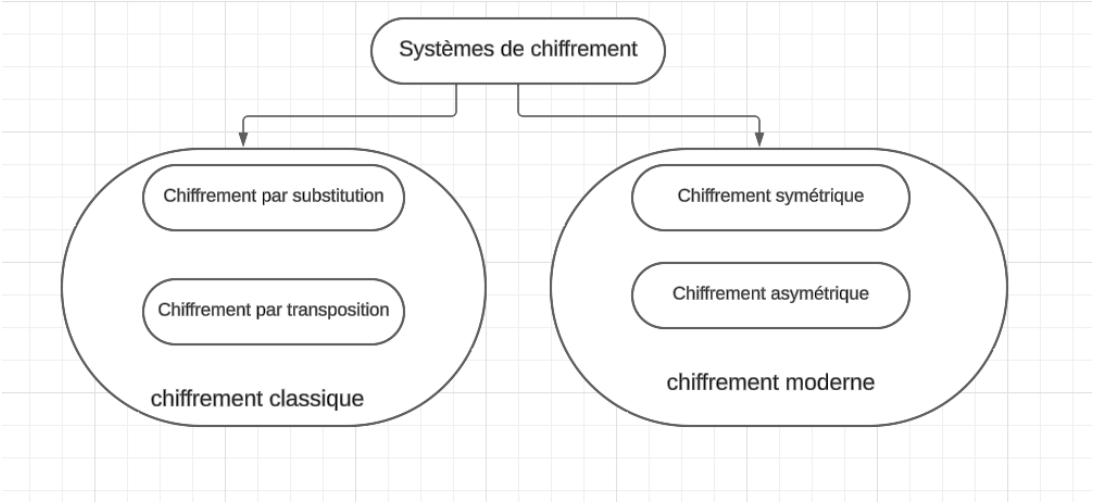

FIGURE 2.4 – Principale méthode de cryptographie.

2.2.4 La Cryptographie Classique

La cryptographie traditionnelle correspond à la période précédant les ordinateurs. Elle aborde les systèmes de lettres et de caractères d'une langue particulière.

Les principales opérations qui fondent la cryptographie traditionnelle incluent :

— Chiffrement par substitution.

— Chiffrement par transposition. [**13**]

Chiffrement par substitution :

Le chiffrement par substitution est un algorithme qui consiste à substituer chaque caractère du message clair (écrit dans un alphabet spécifique) par un autre caractère dans le message chiffré (qui peut être écrit dans un alphabet différent de celui du message clair) selon une règle convenue.

En cryptographie traditionnelle, on distingue trois catégories de chiffrement par substitution :[**13**]

a. **Substitution mono-alphabétique :**Un seul caractère du message chiffré est utilisé pour remplacer le message clair. [**14**]

— **Le code de César :** La plus ancienne technique de cryptographie employée par l'armée romaine est le code de César (1er siècle avant JC). Son principe est une substitution mono-alphabétique, où la substitution se caractérise par un décalage de lettres.

Par exemple : En utilisant un décalage de 3 positions, on substitue A par D, on substitue B par E, C par F, D par G, etc...

Son concept très simple à mettre en pratique simplifie sa cryptanalyse car le nombre de méthodes de chiffrement d'un message reste très limité, Étant donné qu'il est équivalent au nombre de lettres de l'alphabet, il n'existe que 26 méthodes. Il a néanmoins été réutilisé par les officiers sudistes pendant la guerre de Sécession, à cause de sa simplicité.

Il en fut de même en 1915 pour l'armée russe.La cryptanalyse fréquentielle est une autre méthode d'attaque de ce système, qui repose sur le fait que les lettres les plus courantes dans le texte en clair sont les plus courantes dans le texte chiffré. Ainsi, ce système ne peut pas être exempt des variations fréquentes des caractères, ce qui constitue une faiblesse majeure qui permet aux techniques statistiques d'associer une lettre probable aux lettres les plus courantes. De plus, à travers une méthode sémantique récursive, les algorithmes basés sur des substitutions mono-alphabétiques sont facilement dépassés par les experts. [**14**] [**13**]

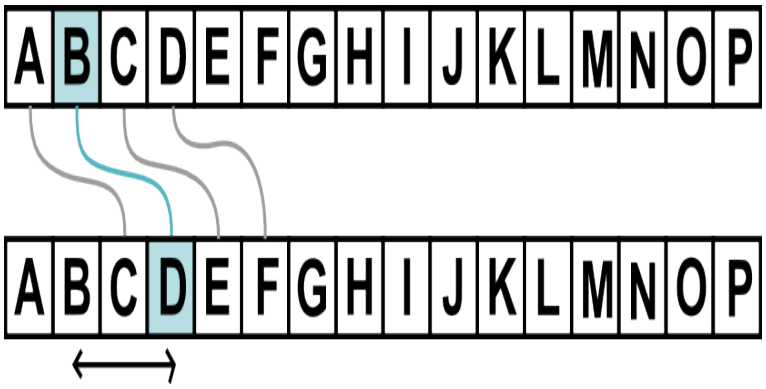

FIGURE 2.5 – Exemple sur le code de César .[**40**]

b. **Substitution poly-alphabétique :** Un caractère clair du message correspond à plusieurs caractères du message chiffré. Le principe consiste à associer une liste de lettres à chaque caractère de l'alphabet des messages clairs, tandis que l'ensemble de ces listes forment une partition de l'alphabet des messages chiffrés.[**14**]

— **Chiffre de Vigenère :**Ce nombre a été introduit par le diplomate français Blaise de Vigenère en 1586 dans son Traité des chiffres ou Secrets manières d'écrire.

Vigenère suggère d'employer un nombre de César, mais avec un décalage qui varie de lettre en lettre. Ainsi, une table de 26 alphabets, écrits dans l'ordre, mais décalés d'une ligne à l'autre d'un caractère, est utilisée. En haut de la clé, un alphabet complet est encore écrit, tandis qu'à gauche, verticalement, un dernier alphabet est écrit pour le texte à coder.

[**14**]

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

FIGURE 2.6 – Le carré de Vigenère.[**41**]

— **Application :**Le texte "CRYPTOGRAPHIE DE VIGENERE" doit être codé avec la clé "MATHWEB". Tout d'abord, nous écrivons la clé sous le texte à coder :

Message	C	R	Y	P	T	O	G	R	A	P	H	I	E		D	E		V	I	G	E	N	E	R	E
Clé	M	A	T	H	W	E	B	M	A	T	H	W	E		B	M		A	T	H	W	E	B	M	A

FIGURE 2.7 – CRYPTOGRAPHIE DE VIGENERE.

Maintenant, nous pouvons procéder à l'encodage caractère par caractère en

utilisant le tableau de Vigenère. Voici comment cela se ferait :

1. Convertir chaque lettre en nombre (A=0, B=1, ..., Z=25).
2. Additionner les nombres correspondants du texte à coder et de la clé (modulo 26).
3. Convertir les résultats en lettres selon la correspondance (0=A, 1=B, ..., 25=Z).

Pour coder "CRYPTOGRAPHIE DE VIGENERE" avec la clé "MATHWEB" en utilisant la méthode de Vigenère, nous allons suivre les étapes décrites précédemment. Voici le détail du processus :

Conversion des lettres en nombres

$$C = 2, \quad R = 17, \quad Y = 24, \quad P = 15, \quad T = 19, \quad O = 14, \quad G = 6, \quad R = 17, \quad A = 0,$$
$$P = 15, \quad H = 7, \quad I = 8, \quad E = 4, \quad D = 3, \quad E = 4, \quad V = 21, \quad I = 8, \quad G = 6,$$
$$E = 4, \quad N = 13, \quad E = 4, \quad R = 17, \quad E = 4$$

Conversion de la clé en nombres (répétée pour correspondre à la longueur du texte)

$$M = 12, \quad A = 0, \quad T = 19, \quad H = 7, \quad W = 22, \quad E = 4, \quad B = 1, \quad M = 12, \quad A = 0,$$
$$T = 19, \quad H = 7, \quad W = 22, \quad E = 4, \quad B = 1, \quad M = 12, \quad A = 0, \quad T = 19,$$
$$H = 7, \quad W = 22, \quad E = 4, \quad B = 1, \quad M = 12, \quad A = 0, \quad T = 19$$

Addition des nombres correspondants (modulo 26)

$C + M = 2 + 12 = 14\,(O)$ $R + A = 17 + 0 = 17\,(R)$

$Y + T = 24 + 19 = 43\,\%\,26 = 17\,(R)$ $P + H = 15 + 7 = 22\,(W)$

$T + W = 19 + 22 = 41\,\%\,26 = 15\,(P)$ $O + E = 14 + 4 = 18\,(S)$

$G + B = 6 + 1 = 7\,(H)$ $R + M = 17 + 12 = 29\,\%\,26 = 3\,(D)$

$A + A = 0 + 0 = 0\,(A)$ $P + T = 15 + 19 = 34\,\%\,26 = 8\,(I)$

$H + H = 7 + 7 = 14\,(O)$ $I + W = 8 + 22 = 30\,\%\,26 = 4\,(E)$

$E + E = 4 + 4 = 8\,(I)$ $D + B = 3 + 1 = 4\,(E)$

$E + M = 4 + 12 = 16\,(Q)$ $V + A = 21 + 0 = 21\,(V)$

$I + T = 8 + 19 = 27\,\%\,26 = 1\,(B)$ $G + H = 6 + 7 = 13\,(N)$

$E + W = 4 + 22 = 26\,\%\,26 = 0\,(A)$ $N + E = 13 + 4 = 17\,(R)$

$E + B = 4 + 1 = 5\,(F)$ $R + M = 17 + 12 = 29\,\%\,26 = 3\,(D)$

$E + A = 4 + 0 = 4\,(E)$

Texte chiffré : ORRWSHD AIOIEQV BNARFDE

Déchiffrement :

Pour déchiffrer le message codé, on suit le même processus en sens inverse, en utilisant la clé pour ramener chaque lettre à sa position d'origine.

c. **Substitution poly-gramique :** Le concept consiste à remplacer un seul caractère par des blocs de caractères (deux ou trois générales). Par exemple, dans une substitution bigrammique, deux lettres du texte clair sont transformées en deux lettres du cryptogramme. [**13**]

— **Chiffrement de Playfair :** L'alphabet comprend 25 lettres (à l'exception du W). Le W est conservé dans la version anglaise et le I et le J sont combinés dans une grille de 5x5, ce qui donne la clé. En utilisant un mot clé secret pour créer un alphabet désordonné, les grilles de chiffrement sont remplies ligne par ligne. Les autres lettres de l'alphabet sont ajoutées dans l'ordre de la grille pour la compléter. [**15**]

— **Chiffrement de Hill :** consiste à :

1. Changer chaque lettre en fonction de son ordre dans l'alphabet.

   où $A = 0$, $B = 1$, ..., $Z = 25$.

2. Collecter les nombres obtenus en blocs de m.
3. Pour chaque bloc de nombres m, il est nécessaire de réaliser des combinaisons linéaires avec une clé K en utilisant une matrice carrée ordinaire m.
4. On peut procéder au déchiffrement en utilisant la matrice inverse K^{-1} dans Z_{26}.[**16**]

Cryptographie par transposition :

Le but est de modifier l'ordre des éléments d'une information (caractères d'une phrase, pixels d'une image...) afin de mieux dissimuler le message.

Il existe différents types de transposition : [**14**]

a. **Transposition simple par colonnes :** Le message est représenté de manière horizontale dans une matrice préétablie, tandis que pour retrouver le texte chiffré, on lit la grille au vertical. Le déchiffrement correspond au processus inverse. [**14**]

La figure 2.1 résume ce principe.

Exemple : Texte à chiffer : I LOVE MY ENGLISH TEACHER, utilise une matrice [6 ;4].

$$\begin{bmatrix} I & L & O & V \\ E & M & Y & E \\ N & G & L & I \\ S & H & T & E \\ A & C & H & E \\ R & & & \end{bmatrix}$$

TABLE 2.1 – Transposition simple par colonnes.[47]

Texte chiffré :"IENSA RLMGH COYLT HVEIE E"

b. **Transposition complexe par colonnes :** L'ordre d'apparition dans l'alphabet des lettres qui constituent ce mot est le résultat d'un mot clé secret composé uniquement de caractères différents. Le cryptage consiste en l'écriture du mes-

sage en lignes dans un rectangle, comme illustré dans la figure 2.8, puis en la lecture du texte en colonnes dans l'ordre donné par la séquence.

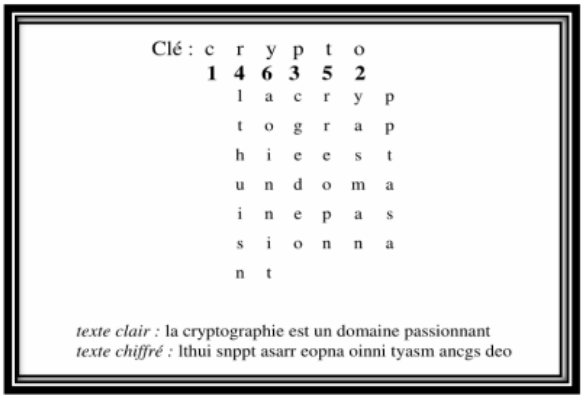

FIGURE 2.8 – Transposition complexe par colonnes.[14]

Une fois ces deux techniques de cryptage (substitution et transposition) décrites, il est clair que les transpositions sont un peu plus sûres que les substitutions, mais qu'elles ne peuvent être utilisées que sur des messages à chiffrer de longueur limitée et qu'elles sont plus consommatrices de mémoire, ce qui limite leur utilisation dans les algorithmes.[**14**]

2.2.5 Cryptographie moderne :

La cryptographie moderne occupe une place essentielle dans la sécurité informatique et les communications, en exploitant des concepts mathématiques tels que la théorie des nombres, la théorie de la complexité computationnelle et la théorie des probabilités par exemple. La cryptographie moderne se démarque de la cryptographie traditionnelle par trois traits clés : elle fonctionne sur des séquences binaires, utilise des algorithmes mathématiques connues publiquement pour coder l'information et repose sur des clés secrètes pour garantir la confidentialité des communications. Contrairement à la cryptographie traditionnelle qui était basée sur la sécurité par la sécurité obscure, la cryptographie moderne garantit la confidentialité grâce à des clés secrètes et à la complexité des algorithmes, rendant pratiquement impossible aux attaquants de récupérer l'information originale. [**16**]

La cryptographie contemporaine se compose de deux sections clairement distinctes :

- La **cryptographie à clé secrète**, aussi appelée **cryptographie symétrique**.
- La **cryptographie à clé publique**, dites aussi **asymétrique**.

Cryptographie symétrique :

Les méthodes de cryptage symétrique (ou à clé privée) sont celles où l'émetteur et le destinataire partagent une clé commune. Cela implique que la clé de chiffrement est également utilisée comme clé de déchiffrement. Ainsi, lors d'une communication, l'utilisation de ce type d'algorithme nécessite que les deux parties échangent préalablement la clé de manière sécurisée, par exemple via un canal sécurisé ou en utilisant d'autres techniques cryptographiques.

Le principal atout de ce mode de chiffrement réside dans sa vitesse. Toutefois, la taille de la clé joue un rôle crucial dans la sécurité d'un système à clé privée. En effet, la clé est possible d'obtenir par une méthode dite d'attaque exhaustive. L'objectif de cette méthode est de lister toutes les clés potentielles du système et de chercher à les utiliser pour déchiffrer un message chiffré. La clé mesure k bits, soit 2 k de tentatives d'attaque complètes pour déchiffrer le message chiffré.

Ainsi, afin de sanctionner une telle attaque, il est nécessaire que la clé soit assez grande.

D'autres types d'attaques peuvent concerner les systèmes de chiffrement à clé privée, généralement en exploitant certaines structures spécifiques de l'algorithme ou certaines caractéristiques statistiques dans la répartition des couples de textes clairs-chiffrés. Les plus connues sont la cryptanalyse différentielle, développée par Biham et Shamir en 1991, et la cryptanalyse linéaire, développée par le Japonais Matsui en 1993.[**17**]

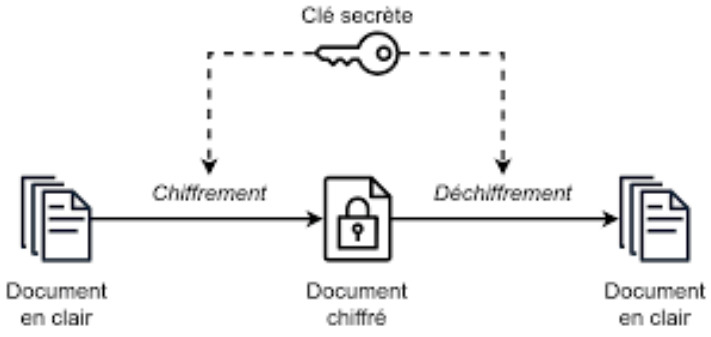

FIGURE 2.9 – Chiffrement à clé privée.[**42**]

Le cryptage à clé privée peut être divisé en deux catégories principales :

— **Cryptosystèmes par flots :** sont une catégorie de chiffrement qui agissent directement sur chaque bit du texte en produisant une clé arbitrairement longue à partir d'une clé courte fixée, imitant ainsi le chiffre de Vernam. À la différence des cryptosystèmes par blocs qui divisent chaque texte clair en blocs de même longueur et les chiffrent bloc par bloc, les cryptosystèmes par flots ne possèdent pas de taille de bloc fixe et peuvent chiffrer des textes de taille variable. Les systèmes utilisés sont rapides et les clés sont généralement de 128 à 256 bits, et sont fréquemment employées pour chiffrer les communications téléphoniques. Il est recommandé d'utiliser des algorithmes de chiffrement par flot qui ont été largement expérimentés dans le domaine académique afin de garantir leur sécurité.[**18**]

— **Cryptosystèmes par blocs :** Les cryptosystèmes par blocs sont une catégorie de chiffrement qui fragmente le texte initial en blocs de taille fixe. En général, il est de 64 bits et chaque bloc est chiffré individuellement afin de générer un message chiffré. Lorsqu'on procède au déchiffrement, on inverse le processus en utilisant l'algorithme de déchiffrement pour retrouver le texte clair d'origine. Les systèmes de cryptographie par blocs sont couramment employés afin de garantir la sécurité des données et sont liés à des algorithmes renommés tels que le DES (Standard d'Encryption des Données) et l'AES (Standard d'Encryption avancé). Plusieurs méthodes ont été standardisées afin de décrire l'application des chiffrements individuels, en prenant en compte l'algorithme sélectionné et la clé initiale. Le mode ECB (Electronic CodeBook), le mode CBC (Cipher Block Chaining), le mode CFB (Cipher FeedBack) et le mode OFB (Output FeedBack) sont parmi les modes de chiffrement par blocs les plus couramment utilisés.[**19**]

Le cryptage est effectué sur des blocs de texte explicites. L'idée générale d'un chiffrement par bloc est la suivante :

- Utilisation d'un code binaire pour modifier les caractères.
- Création de blocs de même longueur à partir de la chaîne.
- Chiffrement d'un bloc en ajoutant progressivement des bits à une clé.
- Possibilité de répéter cette opération plusieurs fois si nécessaire.

- Répéter les étapes 3 et 4 jusqu'à ce que tout le message soit crypté.

Avantages et inconvénients du chiffrement symétrique :

Considérons les avantages et les inconvénients du chiffrement symétrique :

— **Avantages :**
  - Facile à appliquer et à utiliser.
  - Le chiffrement asymétrique est plus rapide.
  - Plus limité en termes de ressources.
  - Utile pour traiter et transférer de grandes quantités de données.

— **Inconvénients :**
  - La disparition d'une clé implique que les informations chiffrées avec cette clé sont en danger.
  - Il est important de partager la clé en toute sécurité avec l'autre personne.[**20**]

Chiffrement asymétrique :

La technique de cryptage asymétrique, également connue sous le nom de cryptage à clé publique, consiste à utiliser une paire de clés distinctes afin de protéger et déchiffrer les données. Dans ce système, une clé est publique et peut être partagée avec tout le monde, tandis que l'autre clé est privée et doit être gardée secrète. Lorsqu'un message est chiffré avec la clé publique, seule la clé privée correspondante peut le déchiffrer, assurant ainsi la confidentialité des communications. Le chiffrement asymétrique est largement utilisé pour sécuriser les échanges de données sur Internet, notamment dans les protocoles de communication sécurisée tels que SSL/TLS et SSH. Il offre une réponse efficace à la question de la sécurité de la distribution des clés dans les communications cryptographiques.[**21**]

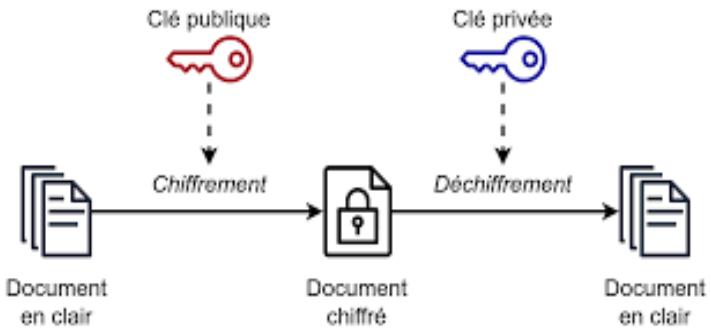

FIGURE 2.10 – Chiffrement à clé privée,clé publique.[**42**]

Avantages et inconvénients du chiffrement asymétrique

Le chiffrement asymétrique présente à la fois des avantages et des inconvénients. Examinons les aspects suivants :

— **Avantages :**

- Il est impossible de déchiffrer les données sans utiliser la clé privée du propriétaire.
- Si la clé publique est perdue ou volée, les données ne sont pas en danger.
- En plus de garantir la confidentialité, le chiffrement asymétrique permet également l'authentification et la non-répudiation. [**20**]

— **Inconvénients :**

- Il a une vitesse inférieure à celle de cryptage symétrique.
- Optimisez l'utilisation de ressources.
- Si la clé privée est perdue, aucun moyen de la récupérer n'est possible.[**20**]

La différence entre Chiffrement symétrique et chiffrement asymétrique :

Chiffrement symétrique	**Chiffrement asymétrique**
Décrypte et décrypte les données en utilisant une seule clé.	Utilisez une clé publique pour sécuriser les données et une clé privée pour les déchiffrer.
Processus de cryptage plus rapide	Le processus de cryptage est plus lent.
Exemples de tailles de clés de 128 ou 256 bits.	Exemples de tailles de clés de 2048 bits ou plus.
Utilisez peu de ressources.	Utilise plus de ressources
Le texte chiffré est de taille inférieure ou égale à celle du texte clair original.	La taille du texte chiffré est supérieure ou égale à celle du texte clair original.
Les algorithmes symétriques permettent l'authentification, mais seule la non-répudiation peut être obtenue en utilisant un algorithme asymétrique.	Les algorithmes symétriques et asymétriques permettent tous deux l'authentification. Seule la non-répudiation peut être obtenue en utilisant un algorithme asymétrique.
Exemples d'algorithmes : AES, DES, 3DES, IDEA et Blowfish	Exemples d'algorithmes : RSA, ECC, DSA et El Gamal
Meilleur traitement et transfert de grandes quantités de données	Meilleur traitement et transfert de petites quantités de données
Si la clé n'est pas correctement gérée, il y a un risque de vol.	Il existe un risque de perdre la clé privée (la paire de clés est inextinguible).

TABLE 2.2 – La différence entre Chiffrement symétrique et chiffrement asymétrique.[**20**]

2.3 Conclusion :

En conclusion, la cryptographie est un domaine essentiel de la sécurité informatique. Elle vise à protéger les informations sensibles en transformant les messages de manière à ce qu'ils ne puissent être compris que par les parties autorisées.

La cryptographie garantit la confidentialité des données et la sécurité des communications à l'ère numérique en utilisant des algorithmes et des clés. Que ce soit dans le domaine militaire, financier ou même dans nos échanges quotidiens, la cryptographie joue un rôle essentiel dans la préservation de la confidentialité, de l'intégrité et de l'authenticité des informations transmises. En résumé, elle joue un rôle essentiel dans la confiance numérique et la préservation des données.

Chapitre 3

La carte chaotique

3.1 Introduction :

De nombreux types de connectivité et de communications (appareils portatifs, réseaux sociaux, etc.) ont été rapidement et largement utilisés pour faciliter l'échange d'informations en ligne. À ce sujet, les images numériques sont actuellement l'une des données les plus importantes partagées sur Internet, notamment sur les réseaux sociaux. Cela est causé par la diffusion massive et le développement rapide des caméras portables, que nous retrouvons dans toutes les tailles, dans les téléphones, à la maison, aux hôpitaux, sur les satellites militaires et autres. De plus, la représentation visuelle des informations revêt une grande importance et une grande utilité, ce qui peut constituer une catégorie d'affaires privées .

De nombreuses applications très importantes sont également offertes par les images numériques, telles que dans le domaine de la médecine, de la banque en ligne, des achats en ligne, des télécommunications, des images à thème militaire, etc... Dès lors, il est primordial et indispensable de garantir la sécurité de ces images, car elles sont diffusées via le réseau ouvert. Si l'on néglige ou omet dans ce domaine, cela met en péril la sécurité des informations confidentielles. Ainsi, la sécurité de ces images revêt une grande importance et est indispensable, car elles sont diffusées via le réseau ouvert. Et toute négligence ou absence dans ce domaine risque de compromettre la sécurité des informations confidentielles.

Le mécanisme le plus crucial pour garantir la protection des données est le chiffrement . C'est pourquoi les chercheurs se sont penchés sur ce point et ont

suggéré de nombreuses techniques pour crypter les images . Cependant, certains traits différencient l'information présente dans les images numériques des données textuelles. Les facteurs clés sont la corrélation très forte entre les pixels d'image, le volume d'information considérable, la fréquence et la redondance élevées des pixels, et bien d'autres. [**22**]

Certains algorithmes de chiffrement classiques (DES, RSA et IDEA) ont été utilisés avec succès dans le chiffrement de texte.Toutefois, ces algorithmes traditionnels ne peuvent pas être utilisés pour crypter l'image car les images ont des caractéristiques intrinsèques comme la répétition d'informations essentielles et la corrélation entre les pixels. Les désavantages de l'utilisation d'algorithmes classiques comprennent la faible performance du cryptage. Il est donc nécessaire de trouver des techniques de chiffrement d'image qui prennent en considération les caractéristiques de l'image. Ces dernières années, de plus en plus de cryptosystèmes d'images ont été exploités à travers différentes techniques, comme la conversion de fréquence, la détection compressée et la théorie du chaos. [**23**]

3.2 Conception et méthodologie :

Cette recherche présente un algorithme de cryptage d'image qui se compose de deux parties principales. Dans la première partie, on utilise une carte chaotiques MD, à savoir la carte logistique afin de produire une séquence unique de nombres entiers allant de 0 à 255 pour chaque élément des quatre matrices. Les quatre canaux d'une image couleur 32 bits, rouge, vert, bleu et alpha, sont représentés par ces matrices, placées dans un carré de 16 × 16, comme le montre la Figure 3.1.

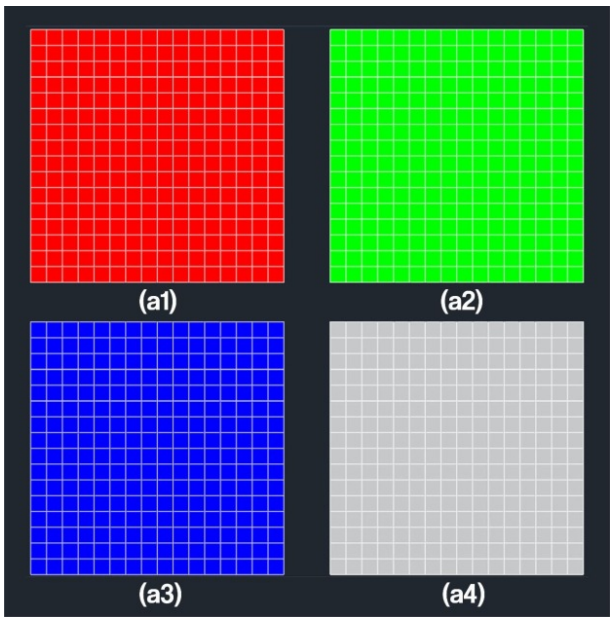

FIGURE 3.1 – Les quatre matrices de notre système de chiffrement sont composées d'entiers uniques générés par quatre cartes chaos. [**24**]

3.2.1 La carte chaotique :

Les cartes chaotiques se réfèrent à des formules mathématiques qui permettent de produire des séquences aléatoires qui sont fortement influencées par leurs conditions initiales et leurs paramètres limitants. Les cartes chaotiques sont divisées en deux types : les cartes unidimensionnelles (1D) et les cartes multidimensionnelles, ou MD. On considère ici les cartes chaotiques bidimensionnelles (2D) comme un type de cartes MD.

Nous étudierons dans cette partie les équations mathématiques et le fonctionnement de diverses cartes chaotiques qui ont récemment été employées dans la

recherche de cryptage d'images.

La carte logistique 1D :

La carte logistique est considérée comme la première carte chaotique, car elle représente une équation de différence 1D non linéaire. Elle est couramment utilisée comme un exemple pratique de la manière dont un comportement complexe et chaotique peut résulter d'un système simple.[**24**]

$$x_{n+1} = L(\alpha, x_n) = \alpha \times x_n \times (1 - x_n) \tag{3.1}$$

La valeur du système au moment n est x_n, tandis que α est un paramètre qui gère le comportement du système. Quand α se situe entre 3.57 et 4, la carte logistique montre un comportement chaotique.

Les diagrammes d'exposant et de bifurcation de Lyapunov illustrés dans la figure 3.2 confirment que l'intervalle chaotique se trouve entre 3.57 et 4. En ce qui concerne les valeurs α inférieures à 3.57, nous avons constaté que ces valeurs se situent dans l'intervalle $[0, 1]$. On a rempli le carré rouge de notre système de chiffrement $(a1)$ en utilisant l'équation suivante :

$$L'(\alpha, x_n) = E(255 \times L(\alpha, x_n)) \tag{3.2}$$

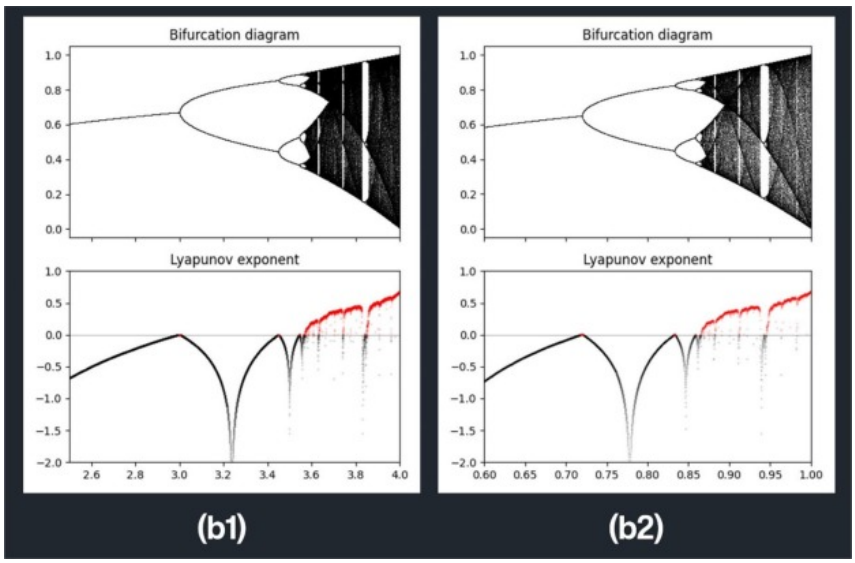

FIGURE 3.2 – Étude du comportement chaotique des cartes Logistique (b1) et Sine (b2) en se basant sur la bifurcation et les diagrammes exponentiels de Lyapunov. [**24**]

La carte sinueuse est la deuxième carte chaotique, une autre carte en 1D non linéaire qui présente un comportement chaotique. On le définit à travers l'équation :

$$y_{n+1} = S(\beta, y_n) = \beta \times \sin(\pi \times y_n) \tag{3.3}$$

où y représente la valeur du système à un moment donné, et β est un paramètre qui régule le comportement du système. Quand β se situe entre 0.87 et 1, la carte sine présente un comportement chaotique élevé.

Les graphiques illustrés dans la figure 3.2 montrent que la carte Sine présente un comportement chaotique similaire à celui de la carte logistique. Plus spécifiquement, il présente un comportement instable dans la plage de valeurs β allant de 0.87 à 1. On a rempli le carré gris ($a4$) de notre système de chiffrement en utilisant l'équation suivante :

$$S'(\beta, y_n) = E(255 \times S(\beta, y_n)) \tag{3.4}$$

La carte Chebyshev est la troisième carte chaotique, qui est une carte unidimensionnelle et non linéaire fréquemment employée dans la cryptographie et d'autres domaines qui requièrent la génération de nombres aléatoires. On le définit à travers les équations :

$$z_{n+1} = C(\gamma, z_n) = \cos(\gamma \times \arccos(z_n)) \tag{3.5}$$

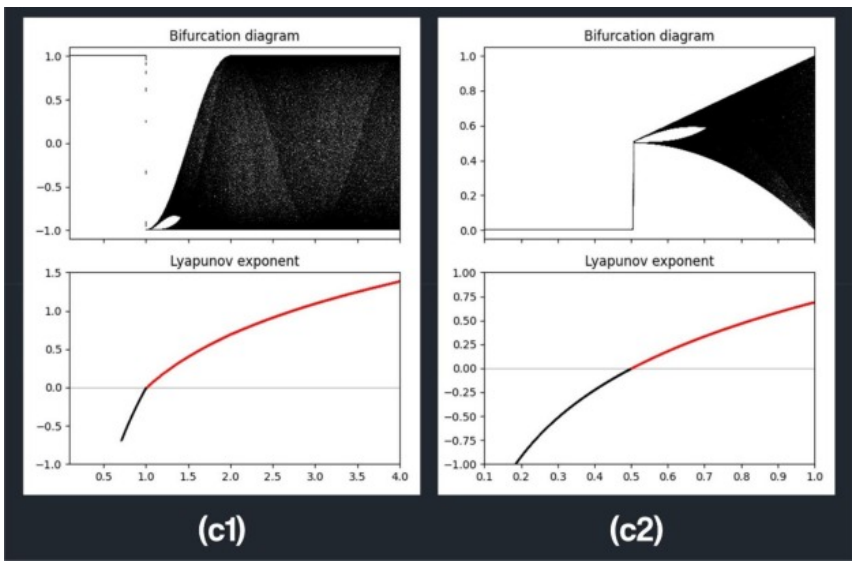

FIGURE 3.3 – Analyse du comportement chaotique des cartes Chebyshev (c1) et Tent (c2) en utilisant la bifurcation et les diagrammes exponentiels Lyapunov.[**24**]

Avec $\gamma \in N$.

La figure 3.3 illustre le comportement chaotique de la carte Chebyshev. Le diagramme de bifurcation révèle que la carte Chebyshev présente un comportement chaotique lorsque le paramètre γ dépasse 1 et dans la plage de $[-1, 1]$.

On a rempli la matrice bleue de notre système de chiffrement ($a3$) en utilisant l'équation mentionnée précédemment.

$$C'(\gamma, z_n) = E(255 \times |C(\gamma, z_n)|) \tag{3.6}$$

La quatrième carte chaotique que nous avons utilisée pour remplir tous les cas du carré gris (a4) est une fonction en morceaux qui modifie ou plie les valeurs d'entrée en fonction de leur spectre. Il est possible de définir mathématiquement sa forme généralisée comme suit.

$$T(\epsilon, t_n) = \begin{cases} 2 \times \epsilon \times t_n, & \text{si } t_n < 0.5 \\ 2 \times \epsilon \times (1 - t_n), & \text{si } t_n \geq 0.5 \end{cases} \tag{3.7}$$

Avec le paramètre ϵ compris entre 0 et 1.

Le comportement chaotique de la carte en T' est illustré dans la figure 3.3. Le diagramme de bifurcation indique que l'intervalle se situe entre 0.5 et 1, comme le montre le diagramme de bifurcation, et cela est confirmé par le diagramme de l'exposant de Lyapunov. Lorsque ϵ est inférieur à 0.5, ce diagramme accepte des valeurs inférieures à zéro, et d'autres supérieures à zéro lorsque p est supérieur à 0.5. Et nous pouvons voir que les valeurs se situent dans l'intervalle $[0, 1]$. Nous avons utilisé l'équation suivante pour remplir la matrice verte ($a2$) de notre système de chiffrement.

$$T'(\epsilon, t_n) = E(255 \times |T(\epsilon, t_n)|) \tag{3.8}$$

[**24**]

La carte logistique 3D chaotique :

$$\begin{aligned} A_{n+1} &= \alpha \cdot A_n \cdot (1 - A_n) + \beta \cdot B_n^2 \cdot A_n + \gamma \cdot C_n^3 \\ B_{n+1} &= \alpha \cdot B_n \cdot (1 - B_n) + \beta \cdot C_n^2 \cdot B_n + \gamma \cdot A_n^3 \\ C_{n+1} &= \alpha \cdot C_n \cdot (1 - C_n) + \beta \cdot A_n^2 \cdot C_n + \gamma \cdot B_n^3 \end{aligned} \tag{3.9}$$

L'ensemble d'équations non linéaires ci-dessus montre un comportement chaotique lorsque les valeurs des paramètres de contrôle sont :

$3.53 < \alpha < 3.81$, $0 < \beta < 0.022$ et $0 < \gamma < 0.015$ et les valeurs initiales $(A_0, B_0, C_0) \in (0, 1)$.

Le couplage quadratique et cubique avec 3 paramètres de contrôle dans la carte logistique 3D le rend encore plus complexe, chaotique et sécurisé.

Les paramètres (α, β, γ) et (A_0, B_0, C_0) agissent comme des clés dans le schéma de cryptage proposé.

La Fig. 3.4 montre le graphique 3D chaotique de l'Éq. 3.9, avec les paramètres constants $\alpha = 3.7700$, $\beta = 0.0157$ et $\gamma = 0.0125$, et les valeurs initiales $A_0 = 0.859375$, $B_0 = 0.156250$ et $C_0 = 0.921875$.

De plus, la Fig 3.5 montre le comportement aléatoire des trois composantes (A_n, B_n, C_n) de la carte logistique 3D séparément dans une vue superposée. [**25**]

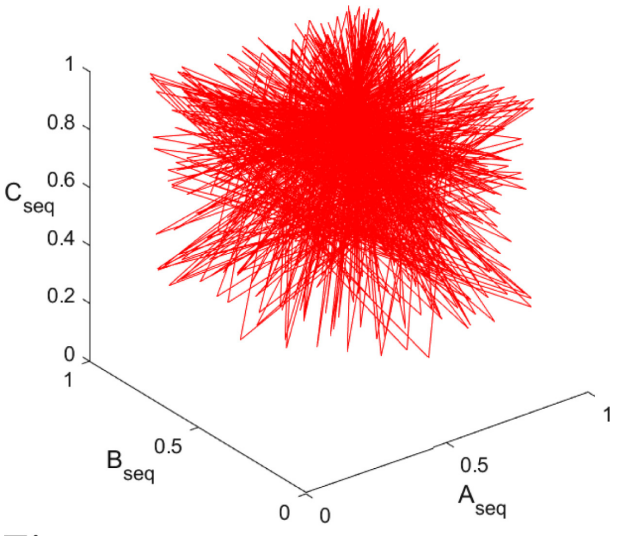

FIGURE 3.4 – Plan caractéristique de la carte logistique 3D.[**25**]

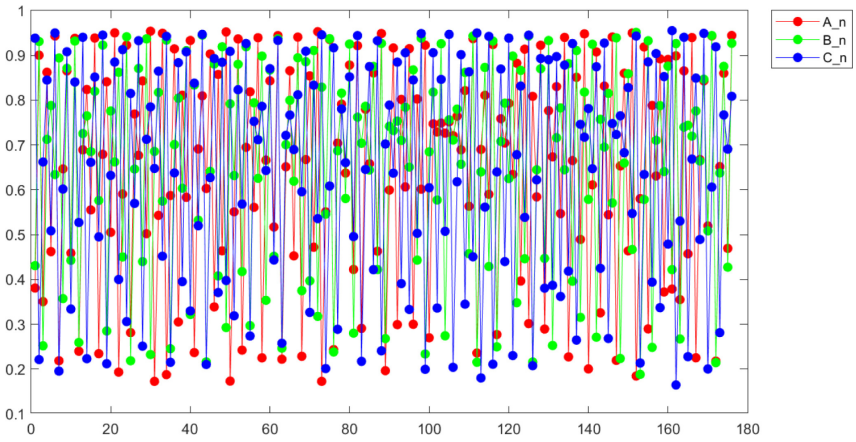

FIGURE 3.5 – Plots séparés des composantes An, Bn et Cn de la carte logistique en 3D dans une vue superposée. [**25**]

3.2.2 La nouvelle carte chaotique mémorable :

Carte sinus classique :

La carte sine est une carte chaotique en une seule dimension (1D), et elle est définie comme :

$$x_{n+1} = a \sin(\pi x_n) \tag{3.10}$$

Le paramètre de contrôle a est une valeur réelle.

Selon l'équation (3.10), la figure 3.6 montre la bifurcation de l'exposant de Lyapunov (LE) de la carte sinusoïdale pour des valeurs de a allant de -20 à 20. On constate que l'exposant de Lyapunov prend $a = 0$ comme point de référence et augmente lorsque a s'éloigne de zéro. Toutefois, la carte sinus classique présente un inconvénient : le système présente une fenêtre périodique très visible lorsque a change, et cet état se manifeste régulièrement.[**26**]

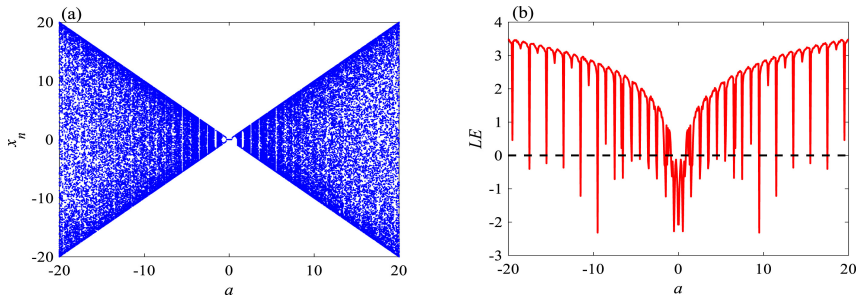

FIGURE 3.6 – La bifurcation vs. LE de la carte sine avec un $\epsilon \in [-20, 20]$, (a) la bifurcation, (b) le LE.[**26**]

Modulateur de memristeur discret sinusoïdal :

Prenons l'exemple d'un mémorisateur parfait à charge contrôlée dans le domaine du temps continu.

$$\begin{aligned} v(t) &= M(q) \cdot i(t) \\ \frac{dq(t)}{dt} &= i(t) \end{aligned} \tag{3.11}$$

où v et i représentent respectivement la tension et le courant.

M(q) correspond à la mémoire, et q est la variable de charge.

Par la suite, on peut simplifier le modèle de mémoire en introduisant la théorie de la différence, tel que

$$\begin{aligned} v_n &= M(q_n) \cdot i_n, \\ q_{n+1} &= (q_n + i_n) \mod k'. \end{aligned} \tag{3.12}$$

Dans cette expression, k, v_n, i_n, q_n et $M(q_n)$ sont les valeurs d'échantillonnage des paramètres de contrôle, tandis que *mod* est l'opération modulaire. D'après certains memristors continus déjà existants, on propose un modèle de memristor discrète appelé *modular-sinusoidal-discrete-memristor* (MSDM) dont la méductance est de :

$$M(q_n) = k \sin(\pi q_n) \tag{3.13}$$

Quand un courant discret $I_n = A \sin(\omega n)$ est ajouté au mémristor discret, l'hystérèse piquée se produit avec $A = 0.01$ et $k = 2$, et la fréquence variable ω de MSDM est illustrée dans la Figure 3.7. Il met en évidence que l'évolution de ces boucles hystériques avec ω est en accord avec la définition de mémoire généralisée. [**26**]

Modèle de Sine-MSDM :

Une nouvelle carte chaotique mémorable nommée Sine-MSDM est développée, qui est construite à partir de la carte sine classique et MSDM. Tout d'abord, prenez la sortie de MSDM comme l'entrée de la carte sinus pour obtenir x_{n+1}. Ensuite, obtenez le résultat y_{n+1} en pliant x_n et y_n à une plage fixe en utilisant des opérations modulaires. Enfin, la dimension de la carte sine est étendue de 1D à 2D, et une nouvelle carte chaotique, Sine-MSDM, est obtenue. L'équation mathématique est écrite comme :

$$\begin{aligned} x_{n+1} &= a \sin(\pi k x_n \sin(\pi y_n)) \\ y_{n+1} &= (x_n + y_n) \mod k' \end{aligned} \tag{3.14}$$

où les paramètres a et k sont hérités de la carte sine et MSDM, respectivement. [**26**]

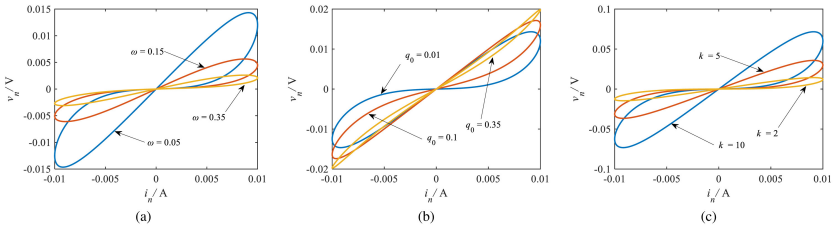

FIGURE 3.7 – Boucles d'hystérèse serrées avec amplitude A = 0,01 pour MSDM : (a) fréquence variable et (k, q0) = (2, 0,01), (b) valeur initiale variable q0 et (K,) = (2, 0,05), (c) paramètre variable k et (, q0) = (0.05, 0.01).[**26**]

3.3 Mettre en place une carte 3D :

Une image rectangulaire est composée de pixels de dimensions N × M et de niveaux de bits de K. A(i, j) peut être représenté de la manière suivante :

$$A(i,j) = \sum_{n=0}^{\log_2 K-1} 2^n \cdot A_n(i,j) \tag{3.15}$$

comme K=256,puis $\log_2 K - 1 = 7, donc,$

$$\begin{aligned} A(i,j) = & A_0(i,j) \times 1 + A_1(i,j) \times 2 \\ & + A_2(i,j) \times 4 + A_3(i,j) \times 8 \\ & + A_4(i,j) \times 16 + A_5(i,j) \times 32 \\ & + A_6(i,j) \times 64 + A_7(i,j) \times 128. \end{aligned} \tag{3.16}$$

La figure 3.8 montre que l'image ordinaire est constituée de 8 couches : $A_0(i,j)$, $A_1(i,j)$, $A_2(i,j)$, $A_3(i,j)$, $A_4(i,j)$, $A_5(i,j)$, et $A_6(i,j)$ en fonction des niveaux de bits de K. Chaque couche pourrait être considérée tel un dessin. Il pourrait ensuite placer les images et les connecter successivement. Ainsi, les 8 images ont été incluses dans une image de taille $(2N \times 4M)$. [**27**]

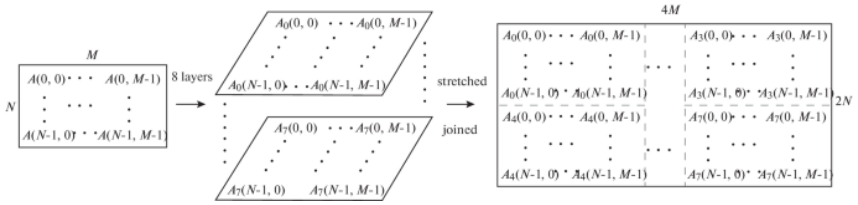

FIGURE 3.8 – Extension d'une nouvelle image plus grande. [**27**]

3.4 La mise à jour des cartes chaotiques améliorées :

La première proposition de la carte remonte à et ne pouvait traiter que des images carrées. Cet algorithme a été amélioré. Une image rectangulaire était composée de pixels $N \times M$ $(M > N)$ et de K bits. La création de la carte a été effectuée en organisant les pixels d'image. Dans un premier temps, chaque pixel de chaque colonne de l'image rectangulaire se trouvait entre deux pixels adjacents de la ligne correspondante. En cas de $M > N$, les autres pixels $M - N$ ont été rangés dans l'ordre initial. Ensuite, on a procédé à la mise en place d'un pixel de la colonne suivante entre deux pixels adjacents de la ligne suivante correspondante. Les pixels de l'image rectangulaire ont été organisés en une ligne de pixels après n fois de traitement. Finalement, Nous avons réorganisé les pixels dans une nouvelle image rectangulaire de taille $N \times M$ $(M > N)$. En utilisant

cette méthode, il a modifié les positions des pixels de l'image. Il est illustré dans la figure 3.9. Il y avait deux cartes pour les différentes directions diagonales ici.[**27**]

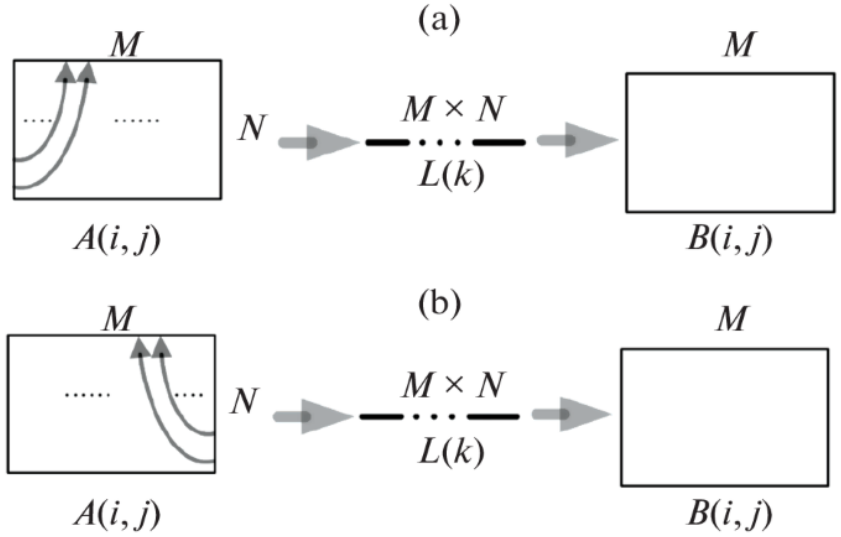

FIGURE 3.9 – Diagramme schématique : (a) carte gauche ; (b) carte droite.[**27**]

Afin d'expliquer davantage, voici deux exemples. Les caractéristiques d'une carte sont illustrées dans la figure 3.10a . La photo mesurait 4×5 pixels. D'après le schéma de la carte (a), il était possible d'insérer le pixel $(1, 0)$ dans la première colonne entre les pixels $(0, 0)$ et $(0, 1)$ du premier rang. Il serait possible d'insérer les pixels $(2, 0)$ dans la première colonne entre les pixels $(0, 1)$ et $(0, 2)$ dans le premier rang, et ainsi de suite. Dans le cas où $M > N$, les pixels restants $(0, 4)$ étaient dans l'ordre initial. Continuer le traitement de toutes les images en associant les pixels de l'image simple à une série de pixels : $(0, 0)$, $(1, 0)$, $(0, 1)$, $(2, 0)$, $(0, 2)$, $(3, 0)$, $(0, 3)$, $(0, 4)$, $(1, 1)$ et les autres. Finalement, il s'agissait de pixels représentant une image rectangulaire indéterminée. Ces cartes étaient symétriques à droite et à gauche (Fig. 3.10b). [**27**]

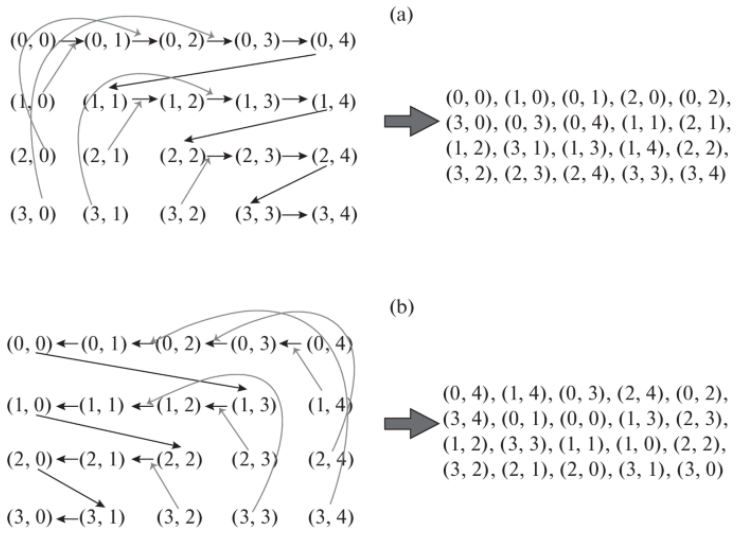

FIGURE 3.10 – (a) An example of left-map ; (b) an example of right-map.[**27**]

Il pourrait tirer la formule du processus mentionné précédemment. Il s'agissait de $N \times M$, avec N, M entiers, $M > N$. $A(i, j)$ représentait une matrice dont chaque élément correspondait à une valeur du pixel (i, j), tandis que $L(k)$ représentait une ligne de pixels.

La figure 3.9a était la carte de gauche. L'algorithme a été décrit comme suit (ici, $i = 0, \ldots, N-1$, $j = 0, \ldots, M-1$, $p = M + N$) :

$$L[(p-j-2)j + 2i - 1] = A(i, j), \quad \text{while} \quad i > j \tag{3.17}$$

$$L[(p-i-2)i + j + N - 1] = A(i, j), \quad \text{while} \quad i \leq j, \tag{3.18}$$

$$L[(p-i-2)i + 2j)] = A(i, j), \quad \text{while} \quad i \leq j. \tag{3.19}$$

La figure 3.9b est la carte à droite. L'algorithme était (ici, $i = 0, \ldots, N-1$, $j = 0, \ldots, M-1$, $p = M + N$) :

$$L[(p-j-2)j + 2i - 1] = A(i, M-1-j), \quad \text{while} \quad i > j, \tag{3.20}$$

$$L[(p-i-2)i + j + N - 1] = A(i, M-1-j), \quad \text{while} \quad i \leq j, \tag{3.21}$$

$$L[(p-i-2)i + 2j)] = A(i, M-1-j), \quad \text{while} \quad i \leq j. \tag{3.22}$$

On a réorganisé la L en B :

$$B(i, j) = L(j + iM).[\mathbf{27}] \tag{3.23}$$

3.5 Algorithme d'encryption d'images :

Une méthode de cryptage d'image rectangulaire tridimensionnelle a été conçue, comme le montre la figure 3.11.

L'ensemble du processus comprenait trois étapes suivantes :

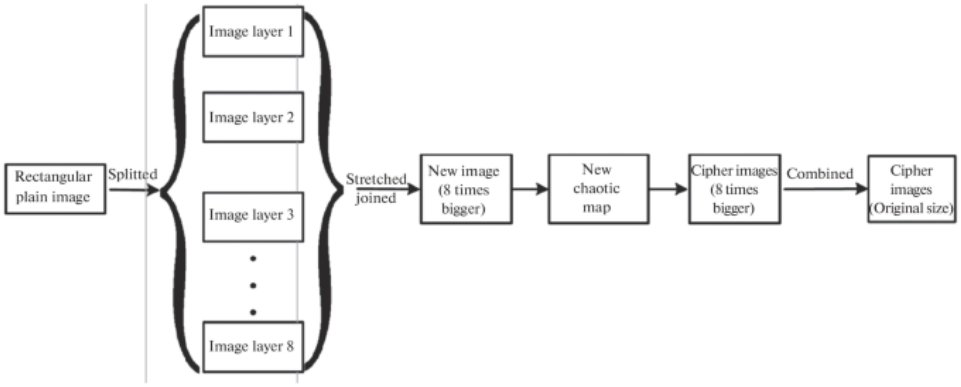

FIGURE 3.11 – Un chiffrement au niveau des bits.[**27**]

3.6 l'algorithme de cryptage et de décryptage proposé

Le domaine du chiffrement d'images a vu émerger diverses approches innovantes visant à renforcer la sécurité et la robustesse des méthodes de protection des données numériques. Parmi ces avancées, l'intégration de deux cartes chaotiques distinctes représente une proposition prometteuse. j'ai proposé de combiner deux cartes chaotiques, la carte logistique 3D et la carte de chirikov. Cette stratégie vise à optimiser le processus de chiffrement en exploitant les propriétés uniques de chaque carte pour assurer une diffusion et une confusion efficaces des données de l'image.

3.6.1 Utilisation des cartes logistique 3D et chirikov pour le chiffrement d'images

Dans le domaine du chiffrement d'images, l'utilisation de cartes dynamiques comme la carte logistique 3D et la carte chirikov offre une approche innovante. La carte logistique 3D est utilisée pour la phase de confusion, tandis que la carte chirikov est employée pour la phase de diffusion.

Phase de confusion avec la carte logistique 3D

La carte logistique 3D génère des valeurs chaotiques qui sont appliquées pour modifier les valeurs de pixels dans l'image, assurant ainsi une distribution aléatoire et complexe des couleurs et des niveaux d'éclairage.

Phase de diffusion avec la carte chirikov

La carte chirikov est utilisée pour réorganiser les positions des pixels dans l'image, provoquant un échange intensif de pixels et augmentant la complexité de la structure finale de l'image chiffrée.

Avantages de la méthode

Cette approche présente plusieurs avantages :

— Sécurité élevée grâce à la nature chaotique des cartes utilisées, rendant la récupération de l'image originale extrêmement difficile sans les équations chaotiques et les paramètres initiaux corrects.

— Efficacité computationnelle, facile à implémenter sur les dispositifs modernes.

— Complexité accrue : l'utilisation de deux cartes différentes augmente la complexité du chiffrement, rendant le processus de déchiffrement sans les clés appropriées encore plus ardu.

L'utilisation conjointe de la carte logistique 3D pour la confusion et de la carte chirikov pour la diffusion représente une approche prometteuse dans le domaine de la protection des données numériques, offrant un haut niveau de sécurité tout en conservant l'efficacité et la rapidité dans le processus de chiffrement et de déchiffrement.

3.6.2 Organigramme de système crypté et décrypté d'image

La figure 3.12 représente le processus de chiffrement d'image par carte chaotique

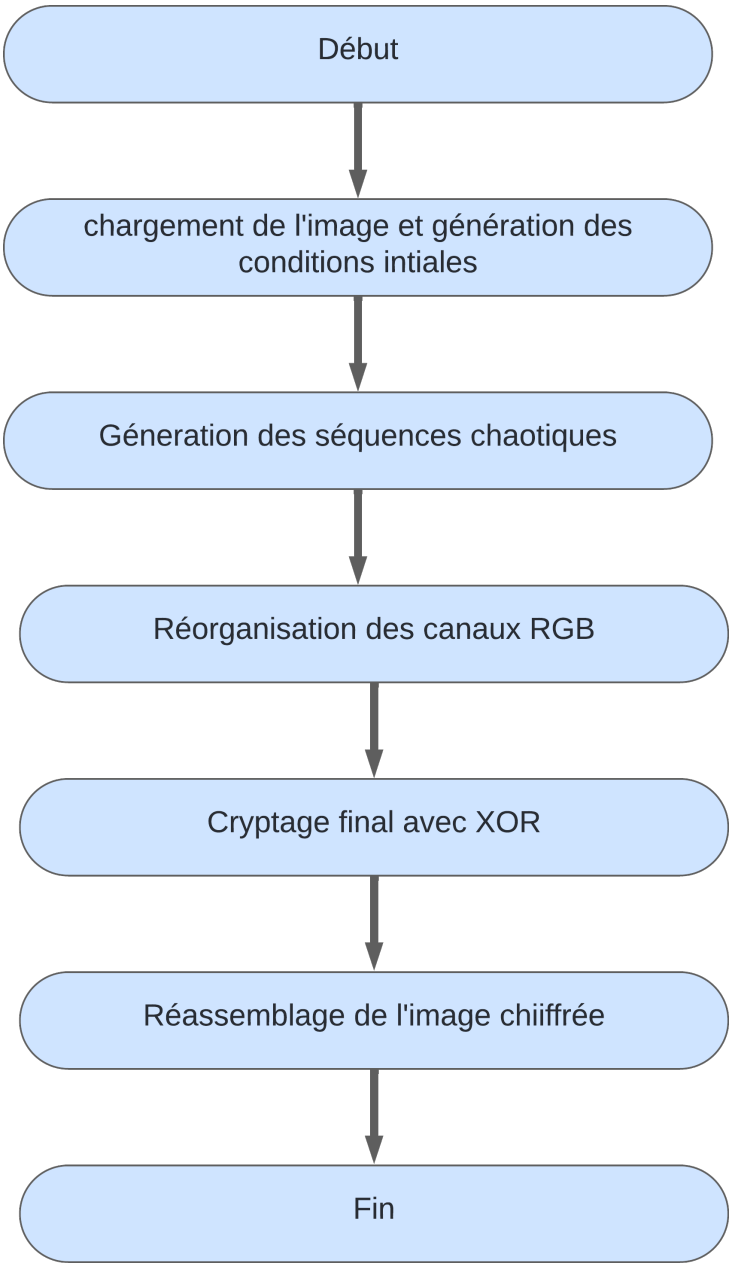

FIGURE 3.12 – Organigramme de système crypté et décrypté d'imag.

Explication des étapes :

- **Étape 1 : Chargement de l'Image et Génération des Conditions Initiales :**
  - Charger l'image à partir d'un fichier.
  - En utilisant la fonction `info_image`, on extrait des données de l'image telles que la taille, la valeur max/min de l'histogramme, la moyenne, le coefficient de corrélation, le MSE, le PSNR, etc.
  - a, b, l : Génèrent des paramètres chaotiques aléatoires dans des intervalles

donnés. $3.53 < l < 3.81$, $0 < b < 0.022$, $0 < a < 0.015$.

— $x(1)$, $y(1)$, $z(1)$: Génèrent des conditions initiales pour les séquences chaotiques basées sur les caractéristiques de l'image.

— **Étape 2 : Génération des Séquences Chaotiques :**

— Les séquences x, y et z sont générées en utilisant des équations chaotiques itératives =

$$x_{i+1} = l \cdot x_i \cdot (1 - x_i) + b \cdot y_i^2 \cdot x_i + a \cdot z_i^3$$
$$y_{i+1} = l \cdot y_i \cdot (1 - y_i) + b \cdot z_i^2 \cdot y_i + a \cdot x_i^3$$
$$z_{i+1} = l \cdot z_i \cdot (1 - z_i) + b \cdot x_i^2 \cdot z_i + a \cdot y_i^3$$

— Normaliser et transformer les séquences chaotiques en valeurs comprises entre 0 et 255 : (S_x, S_y, S_z).

— **Étape 3 : Réorganisation des Canaux RGB :**

— Convertir les canaux de couleur de l'image en vecteurs pour simplifier le chiffrement de l'image.

— Les canaux rouge, vert et bleu de l'image sont convertis en vecteurs linéaires PR, PG, PB.

— **Étape 4 : Cryptage Final avec XOR :**

— Les valeurs pré-cryptées CCR, CCG, CCB sont ensuite passées par une opération XOR avec les séquences chaotiques scalées et modulées S_x, S_y, S_z respectivement. Cette opération de chiffrement bitwise XOR ajoute une couche de sécurité.

— **Étape 5 : Réassemblage de l'Image Chiffrée :**

— **Réassemblage des Canaux :** Les vecteurs cryptés CCR, CCG, CCB sont reformés en matrices 2D correspondant aux dimensions originales des canaux de l'image.

— **Concaténation des Canaux :** Les matrices 2D cryptées $CCRN$, $CCGN$, $CCBN$ sont combinées pour reformer l'image cryptée complète ci.

Toutes ces étapes précédentes sont la phase de confusion.

— **Étape 6 :Déclaration de la fonction et génération de la clé :**

— Commencez par définir la fonction encrypt qui prend une image et une clé en entrée.

— Si aucune clé n'est fournie, une clé de quatre éléments est générée basées sur les caractéristiques de l'image.

- **Étape 7 : Initialisation et calcul des paramètres de la carte de Chirikov :**
  - Les valeurs x, y, k, et h sont extraites de la clé.
  - Les paramètres Kk, hh, xx, et yy sont calculés pour la carte de Chirikov en utilisant des expressions trigonométriques et exponentielles.
- **Étape 8 : Conversion de l'image en tableau de bits :**
  - L'image est convertie en un tableau binaire de 8 bits.Ce tableau est aplati en une seule dimension.
- **Étape 9 :Génération des positions mélangées :**
  - **Initialisation des positions pour le mélange :**Deux tableaux de positions (posX et posY) sont initialisés avec les valeurs xx et yy.
  - Un ensemble de positions mélangées est généré en utilisant la carte de Chirikov. Les positions sont normalisées et arrondies.
- **Étape 10 : Mélange des bits de l'image :** Les bits de l'image sont mélangés selon les positions générées.
- **Étape 11 : Restauration de l'image chiffrée :**
  - Le tableau binaire est restructuré en groupes de 8 bits.
  - Ces groupes sont convertis en valeurs réel.
  - L'image chiffrée est reconstruite à partir de ces valeurs entières et reshaped aux dimensions originales.

Toutes ces étapes précédentes sont la phase de diffusion.

3.6.3 Organigramme de chiffrement image 3D

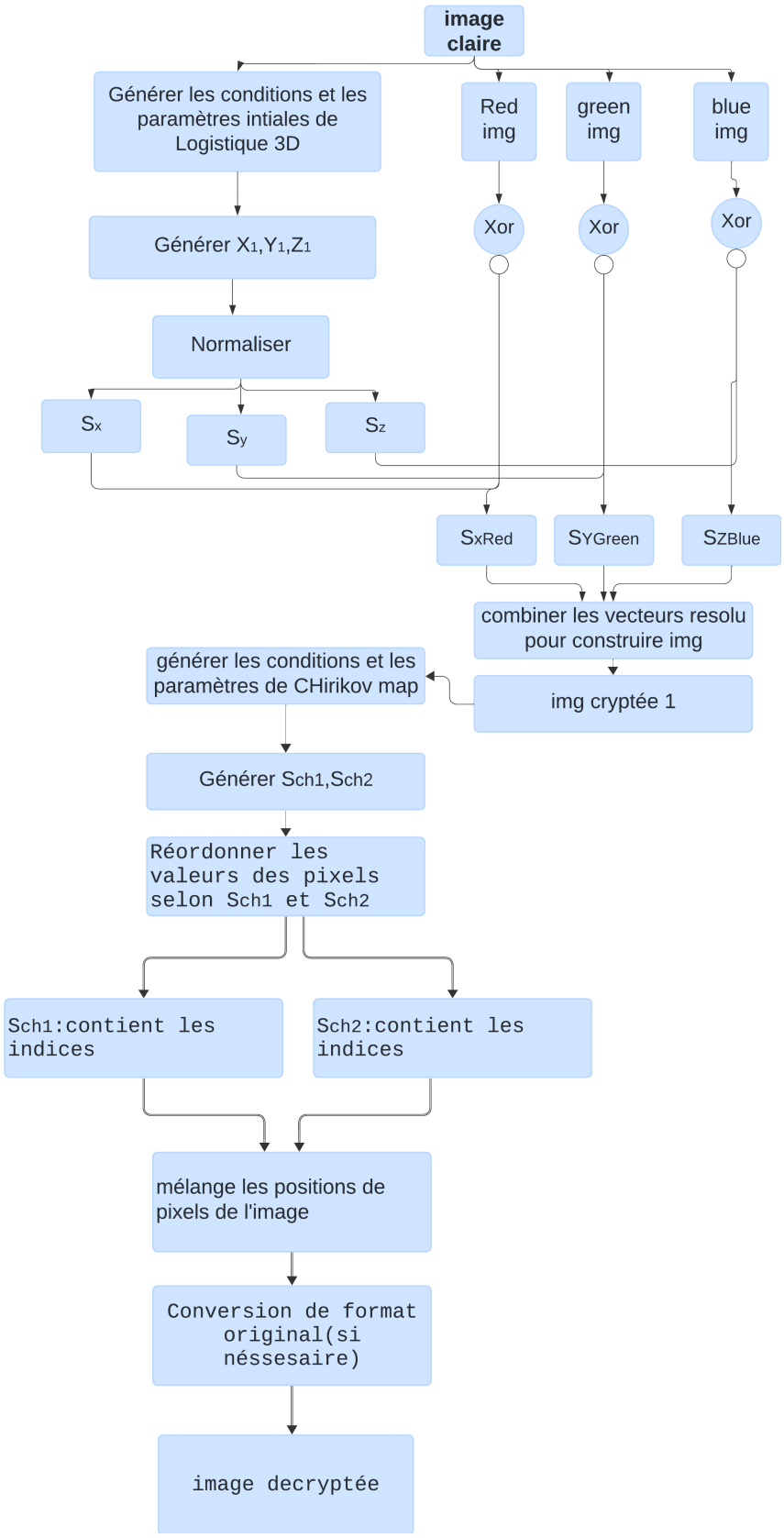

FIGURE 3.13 – Diagramme de block de l'algorithme de cryptage.

3.7 conclusion

Dans ce chapitre, nous avons proposé une procédure pour la conception d'algorithmes fondés sur le chaos ; cette méthode consiste à générer des nombres pseudo-random et à effectuer un chiffrement multimédia. Par exemple, nous avons présenté un algorithme de chiffrement basé sur la carte logistique.

Chapitre 4

Résultats

4.1 Introduction :

Les données multimédias se composent de texte, d'audio, de vidéo, de graphiques et d'images, ainsi que de photos. En raison de l'utilisation croissante des donnes multimédias sur Internet, il est primordial de les préserver. Le cryptage des images est différent du cryptage d'autres 'el'ements multim'edias en raison de certaines caract'eristiques intrins'eques, comme la capacit'e de donn'ees volumineuses et la corr'elation 'etroite entre les pixels.

Puisque les pixels sont étroitement liés, les techniques de chiffrement pr'ec'edentes comme les techniques de chiffrement AES, DES, etc. ne conviennent pas aux applications courantes. La sécurité des données repose sur l'alliance entre la cryptographie et la théorie chaotique. Un aspect essentiel de la protection des données. En ce qui concerne le cryptage d'images, la tendance récente repose sur le chaos en raison de paramètres de contrôle, de sensibilité aux circonstances initiales, de non-périodicité et de non-convergence.

Le chaos est utilisé par divers algorithmes de cryptage d'images. Dans ce chapitre, nous avons exposé une approche cryptique simple basée sur le chaos à trois dimensions (3D) non linéaire, en utilisant pour la première fois la carte logistique à trois dimensions (3D) pour la permutation de position. L'utilisation du chaos à trois dimensions (3D) a été utilisée pour la première fois dans la carte logistique afin de changer de position et de transformer une méthode de transformation des valeurs.

4.2 Pourquoi des cartes chaotiques pour le cryptage d'image ?

Concevoir une méthode de cryptage utilisant à la fois les principes de la confusion et de la diffusion.

La confusion implique une modification radicale des données de l'entrée à la sortie, par exemple, en traduisant les données à travers une table non linéaire générée à partir de la clé. Il existe de nombreux outils de calcul linéaires inverses, ce qui signifie que plus il est non linéaire, plus il gêne les outils d'analyse.

La diffusion signifie qu'un seul caractère de l'entrée changera de nombreux caractères de la sortie. Bien fait, chaque partie de l'entrée affecte chaque partie de la sortie, rendant l'analyse beaucoup plus difficile. Aucun processus de diffusion n'est parfait : il laisse toujours passer certains schémas. Une bonne diffusion disperse largement ces schémas dans la sortie, et s'il y a plusieurs schémas qui passent, ils se brouillent mutuellement. Cela rend les schémas beaucoup plus difficiles à repérer et augmente considérablement la quantité de données à analyser pour casser le chiffre.

Le comportement à long terme d'une carte chaotique change radicalement avec de petits changements dans la valeur initiale, ce qui nous donne notre "première clé". Commençons à modifier l'alignement des pixels, ou les intensités de pixels, en réalisant des opérations arithmétiques sur eux, qui sont à leur tour des fonctions de X_n, où n est la clé de notre algorithme.

Nous pouvons utiliser des cartes chaotiques multidimensionnelles et effectuer une variété d'opérations, ce qui nous permet de crypter notre image avec de nombreuses clés à chaque étape. Ainsi, cela rend le déchiffrement de l'image presque impossible si les valeurs de clé initiales sont inconnues.[**28**]

4.2.1 Expérimentations et résultats

Nous avons implémenté l'algorithme en langage MATLAB , pour tester ses performances. Cette section présente et discute les résultats obtenus.

4.2.2 Environnement de travail

Nous avons implémenté l'algorithme sur un pc Hp I5 , ram 8G , sous le système d'exploitation Windows 10.

4.2.3 Langage de programmation

MATLAB représente une méthode de programmation avancée qui propose des caractéristiques mathématiques qui permettent de résoudre des problèmes scientifiques et d'ingénierie. Grâce à son mode interactif, vous pouvez obtenir des résultats immédiats en exécutant successivement les commandes, ce qui vous permet d'explorer rapidement différentes options et d'atteindre une solution optimale. De plus, MATLAB propose aussi les caractéristiques des langages de programmation classiques, comme le contrôle de flux, la gestion d'exceptions et la programmation orientée objet.[**29**]

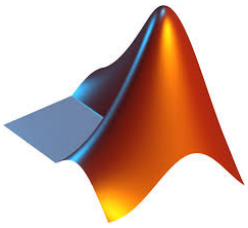

FIGURE 4.1 – logo de MATLAB.[**29**]

4.3 Cryptage d'image par la technique du chiffrement continu à base de l'algorithme Chaotique

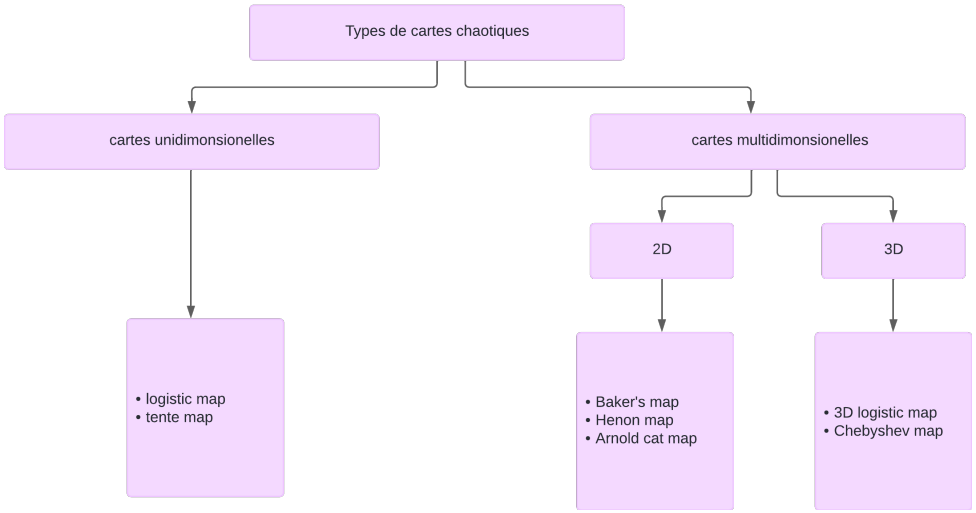

FIGURE 4.2 – Types de cartes chaotique.

La technique du chiffrement est fréquemment utilisée dans le domaine de l'imagerie numérique afin de garantir la sécurité de l'image. Ce procédé vise à transformer l'image originale en une autre image qui ne peut être interprétée. En d'autres termes, elle assure que personne ne peut saisir le contenu sans une clé pour le déchiffrer. Au cours de ce chapitre, nous allons concevoir un générateur pseudo aléatoire en utilisant une carte logistique 3D et la carte chirikov pour réaliser un chiffrement en continu en utilisant des systèmes chaotiques. Le but principal du générateur pseudo aléatoire est d'être idéal pour le chiffrement, en espérant produire une suite de symboles potentiellement illimitée qui a l'apparence d'une suite aléatoire.[**30**]

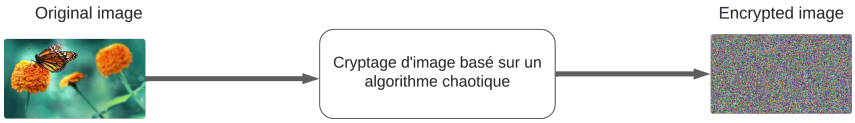

FIGURE 4.3 – cryptage d'image par la technique Du chiffrement continu à base de l'algorithme Chaotique.

4.3.1 Principe de l'algorithme de cryptage et de décryptage proposé :

Dans cet algorithme, vous choisissez deux types des cartes chaotiques, ils sont :

— **Carte logistique en 3D :** La carte logistique en 3D est une extension de la carte logistique classique à trois dimensions. Elle est définie par l'équation

$$\begin{aligned} x_{i+1} &= l \cdot x_i \cdot (1 - x_i) + b \cdot y_i^2 \cdot x_i + a \cdot z_i^3 \\ y_{i+1} &= l \cdot y_i \cdot (1 - y_i) + b \cdot z_i^2 \cdot y_i + a \cdot x_i^3 \\ z_{i+1} &= l \cdot z_i \cdot (1 - z_i) + b \cdot x_i^2 \cdot z_i + a \cdot y_i^3 \end{aligned} \tag{4.1}$$

$$\begin{aligned} x_{i+1} &= l \cdot x_i \cdot (1 - x_i) + b \cdot y_i^2 \cdot x_i + a \cdot z_i^3 \\ y_{i+1} &= l \cdot y_i \cdot (1 - y_i) + b \cdot z_i^2 \cdot y_i + a \cdot x_i^3 \\ z_{i+1} &= l \cdot z_i \cdot (1 - z_i) + b \cdot x_i^2 \cdot z_i + a \cdot y_i^3 \end{aligned}$$

Les constantes l, b et a sont des constantes, tandis que les séquences x, y et z sont définies par les équations précédentes.

où a, b, l : Génèrent des paramètres chaotiques aléatoires dans des intervalles donnés : $3.53 < l < 3.81$, $0 < b < 0.022$, $0 < a < 0.015$. Cette carte présente un comportement chaotique dans l'espace tridimensionnel.

- **Carte standard (Chirikov) :** est une carte de conservation de la zone pour deux variables dynamiques canoniques, c'est-à-dire, momentum et coordonnées (p,x). Il est décrit par les équations :[**33**]

$$x_{n+1} = x_n + y_n - \frac{K}{2\pi}\sin(2\pi x_n)$$
$$y_{n+1} = y_n - \frac{K}{2\pi}\sin(2\pi x_n)$$

4.3.2 Discussion des résultats

Analyse de la sécurité

Un bon algorithme de chiffrement devrait être capable de faire face aux attaques qui lui sont adressées. Cette partie examine la sécurité de la proposition de schéma de cryptage d'image. Différentes techniques d'analyse statistique, telles que l'histogramme, l'analyse de corrélation entre deux pixels voisins, l'analyse de sensibilité à la clé et l'analyse différentielle, sont utilisées pour montrer que l'algorithme proposé offre une grande sécurité contre les attaques majeures.

Les expérimentations sont faites avec les paramètres suivant :
x(1)=0.2350 ; y(1)=0.3500 ; z(1)=0.7350 ; a(1)=0.0125 ; b(1)=0.0157 ; l(1)=3.7700 ;

— Cryptage puis décryptage de l'image avec l'algorithme proposé :

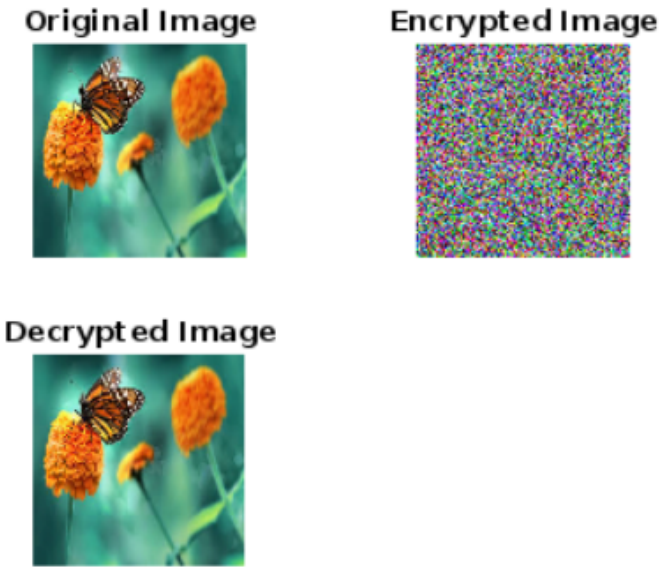

FIGURE 4.4 – (image originale, image cryptée, image décryptée.

L'histogramme

L'histogramme d'une image est un graphique qui illustre les valeurs d'intensité des pixels. Cette représentation graphique illustre le nombre de pixels dans une image à chaque valeur d'intensité de cette image. La valeur d'intensité d'une image grise est de 256, ce qui permet de représenter graphiquement l'histogramme en utilisant 256 chiffres qui indiquent la répartition des pixels entre ces différentes valeurs de niveaux de gris.[**28**]

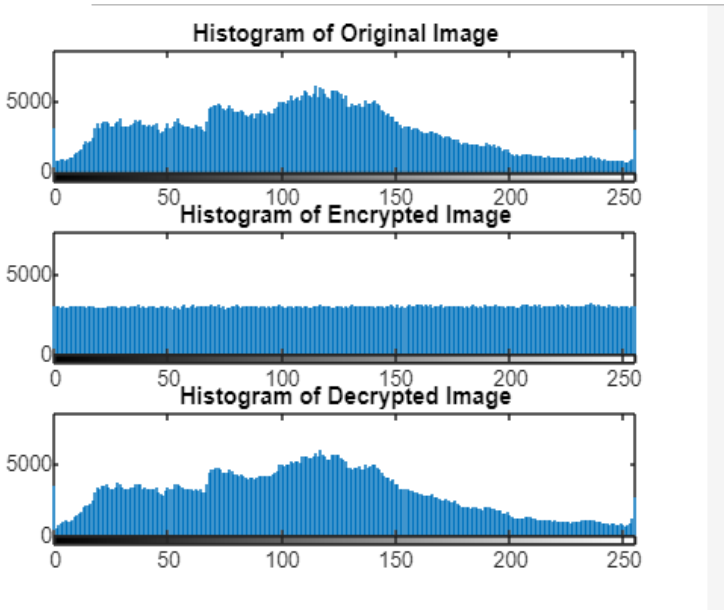

FIGURE 4.5 – (histogrammes :(a)image original,(b) image crypté,(c) image décryptée avec algorithme proposé.

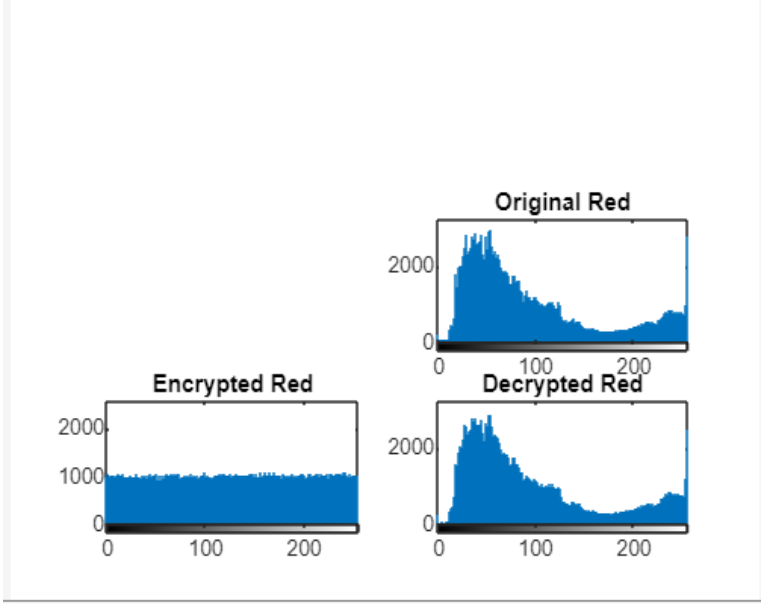

FIGURE 4.6 – (histogrammes :image (en coleur rouge).

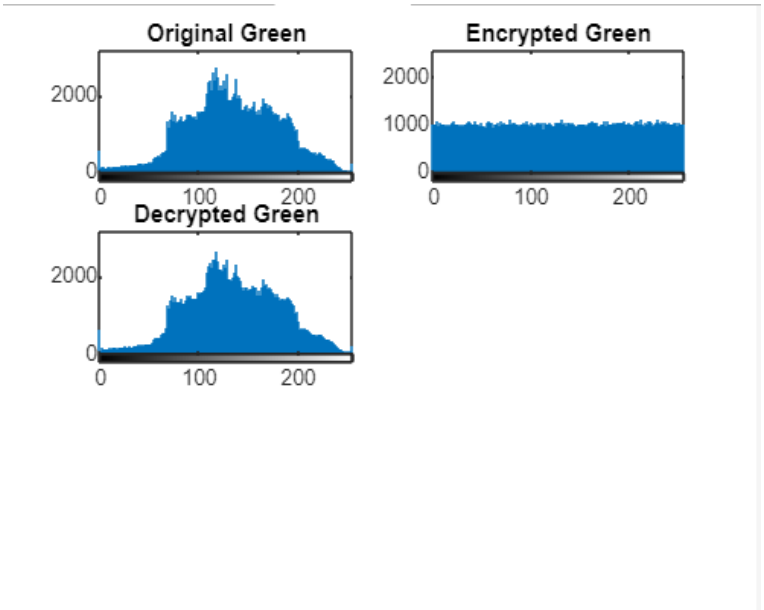

FIGURE 4.7 – (histogrammes :image (en coleur vert).

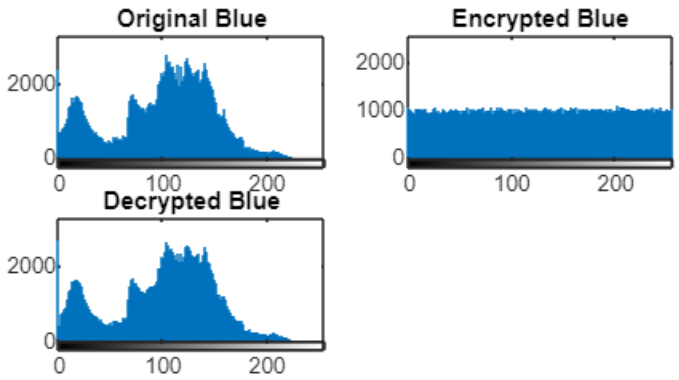

FIGURE 4.8 – (histogrammes :image (en coleur blue).

L'analyse de corrélations

L'analyse des corrélations entre les pixels adjacents est une étape de test qui permet d'évaluer la robustesse de l'algorithme de chiffrement. Dans le cadre des images originales et cryptées, les relations entre les pixels adjacents horizontaux, verticaux et diagonaux voisins ont été analysées. Les figures a et b présentent les distributions de deux pixels adjacents horizontaux pour l'image originale et chiffrée de Lena, respectivement.[**30**]

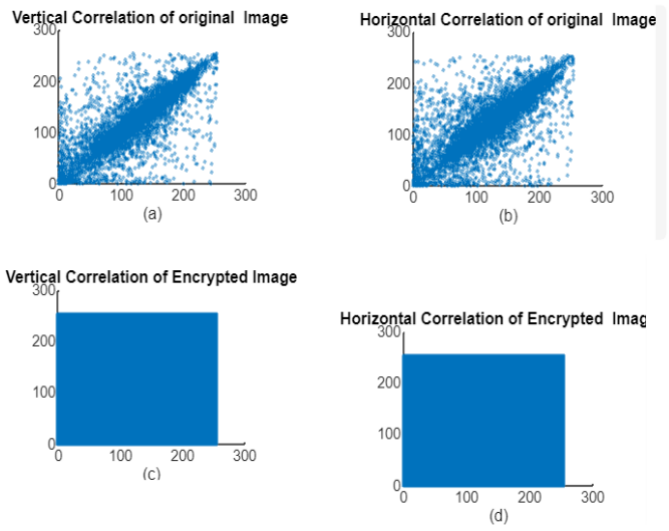

FIGURE 4.9 – Corrélation vertical et horizontal

On a également élaboré le coefficient de corrélation entre deux pixels adjacents verticaux et horizontaux, tant de l'image originale que chiffrée.

Sens	Originale	Chiffrée
Horizontal	0.98677	0.0013576
vertical	0.99308	0.002226

TABLE 4.1 – Coefficients de corrélation entre l'image originale et l'image chiffrée.

Les coefficients de corrélation observés pour l'image originale sont proches de 1, ce qui suggère une corrélation élevée entre les pixels, tandis que pour l'image chiffrée, ils sont proches de 0, ce qui souligne l'absence de corrélation entre les images originales et chiffrées. La version chiffrée de l'image diffère donc totalement de l'originale.

Analyse de l'information et de l'entropie

La mesure statistique de l'incertitude, nommée entropie, joue un rôle fondamental dans la théorie de l'information. L'efficacité d'un système de cryptage est souvent évaluée en visant une valeur d'entropie proche de 8.

Voici les valeurs d'entropie de différentes images telles qu'elles ont été mesurées dans notre système.[**30**]

Originale	Chiffrée	déchiffrée
7.813	7.9997	7.8132

TABLE 4.2 – Entropie Des images originale, l'image chiffrée et l'image déchiffrée.

4.3.3 Mesures de Performance du Chiffrement d'Image :

Entropie :

L'entropie locale de Shannon (LSE) est une mesure importante par laquelle la randomisation de l'image peut être évaluée. LSE est calculé par

$$H = -\sum_{i=0}^{255} p(i) \log_2 p(i) \tag{4.2}$$

Où $p(i)$ est la probabilité d'apparition de la valeur de pixel i.

Coefficient de corrélation :

Dans l'image originale, les pixels adjacents sont fortement corrélés dans les directions verticale, horizontale et diagonale. L'image chiffrée doit avoir une corrélation faible entre les pixels adjacents dans trois directions.

Le coefficient de corrélation est calculé par

$$r_{XY} = \frac{\operatorname{cov}(X,Y)}{\sqrt{\operatorname{var}(X) \cdot \operatorname{var}(Y)}}$$

$$\operatorname{cov}(X,Y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(X))\,(y_i - E(Y))$$

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

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

où x, y sont deux pixels adjacents. N est le nombre total de pixels sélectionnés à partir de l'image pour calculer la corrélation. Dans les expériences menées, 10 000 paires de pixels adjacents sont sélectionnés au hasard.

Signal de pointe au rapport sonore (PSNR) et MSE :

PSNR utilisé pour mesurer l'efficacité des techniques de décryptage. Le PSNR est mesuré par :

$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right)$$

$$\mathrm{MSE} = \frac{1}{W \times H}\sum_{i=0}^{H-1}\sum_{j=0}^{W-1}|O(i,j) - D(i,j)|^2$$

où O est l'image originale et D est l'image déchiffrée. Une valeur de PSNR plus grande indique une meilleure qualité d'image.

Sensibilité de clé :

Les algorithmes de chiffrement de l'image doivent être très sensibles à la clé. Tout changement dans les conditions initiales qui génèrent la clé secrète originale produira une image chiffrée différente. NPCR (numéro de pixel change rate) et UACI (Unified Average Change Intensity) sont utilisés pour mesurer la sensibilité de la clé.

$$\text{NPCR} = \frac{1}{W \times H} \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} D(i,j) \times 100\%$$

où $D(i,j)$ est défini comme :

$$D(i,j) = \begin{cases} 0 & \text{si } c1(i,j) = c2(i,j) \\ 1 & \text{si } c1(i,j) \neq c2(i,j) \end{cases}$$

$$\text{UACI} = \frac{1}{W \times H} \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} \frac{|c1(i,j) - c2(i,j)|}{255} \times 100\%$$

où $c1$ est l'image cryptée avec la clé secrète originale et $c2$ est l'image cryptée avec une clé incorrecte. La valeur idéale du NPCR est de 99,6094, tandis que son UACI est d'environ 33,4635.

Selon la norme IEEE de point flottant, la précision de calcul du nombre 64 bits avec une double précision est d'environ 10^{15}.

$(10^{15})^{10} = 10^{150}$

Résultats expérimentaux

Nous avons utilisé des images numériques standards dans notre application.

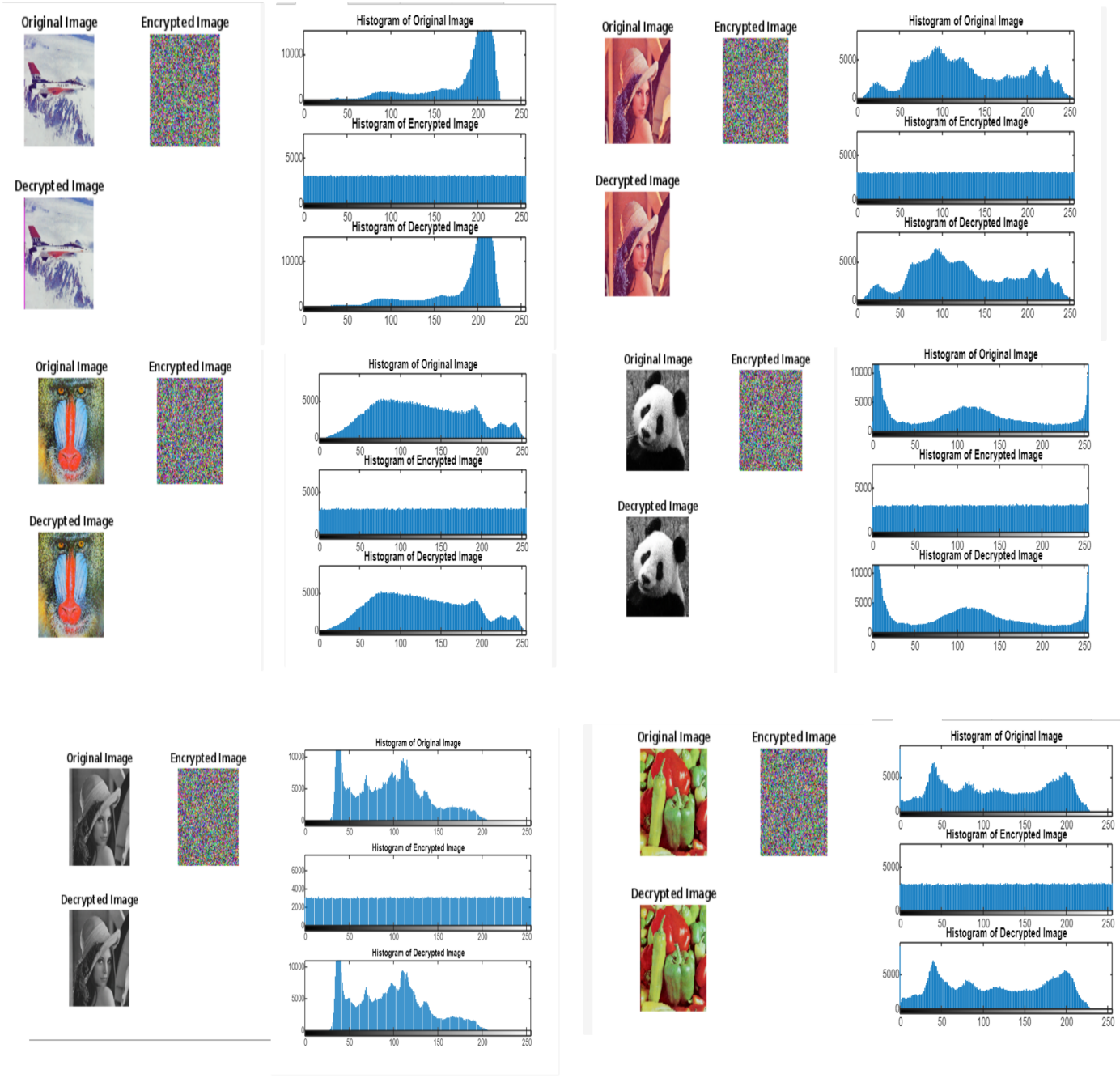

FIGURE 4.10 – Résultats d'analyse d'histogrammes

Il est évident que l'histogramme des images cryptées présente une répartition homogène des valeurs de pixels (tous les pixels ont la même probabilité d'apparition), ce qui démontre que le système chaotique n'est pas susceptible d'être atteint par une attaque d'histogramme.

Les 3 tableaux suivants 4.3 , 4.4 et 4.5 représentent les différents résultats obtenus.

Image	Dimensions	Originale	Chiffrée	Déchiffrée
lena	512x512	7.7502	7.9994	7.7502
panda256	256x256	7.497	7.999	7.497
pappers	512x512	7.6698	7.9998	7.6698
lena (180x180)	180x180	7.1791	7.998	7.1791
baboon	512x512	7.7624	7.9998	7.7624
airplane	512x512	6.6639	7.9998	6.6639
cameraman	225x225	7.0853	7.9989	7.0853
cameraman	160x160	7.0392	7.9975	7.0392
onion	135x198	7.6197	7.9976	7.6197

TABLE 4.3 – Entropie des images originale, chiffrée et déchiffrée.

Le tableau 4.3 présente les valeurs d'entropie des différentes images expérimentales ainsi que leurs images principales . On constate que l'entropie de toutes les images chiffrées dépasse 7,99. Dès lors, il est possible de conclure que ces valeurs sont très proches de la valeur optimale (8), ce qui rend impossible l'attaque d'entropie.

Image	NPCR	UACI	MSE	PSNR	CC
lena	99.6143	30.5318	8980.9931	8.5976	-0.0054977
panda256	99.5972	33.9074	12511.7034	7.1576	-0.0029003
peppers	99.6197	32.2126	10108.5329	8.0839	0.0014436
lena (180x180)	99.6204	29.3972	8275.4417	8.9529	-0.0014932
baboon	99.5927	29.9953	8648.6205	8.7613	-0.0027336
airplane	99.6056	32.6187	10372.109	7.9721	7.0544e-05
cameraman	99.63	31.1286	9390.4839	8.4039	-0.00054697
cameraman(160)	99.6003	30.9468	9256.7216	8.4662	-0.0025554
onion	99.5835	34.0884	11347.7953	7.5817	-0.0069016

TABLE 4.4 – Mesures NPCR, UACI, MSE, PSNR et CC des différentes images de test.

Les mesures PSNR et MSE des différentes images de test sont présentées dans le tableau 4.4. Les résultats obtenus montrent une MSE élevée et des mesures PSNR

faibles (< 10), ce qui prouve que l'algorithme proposé est très efficace pour repérer les variations ou les modifications dans les images de test.

Image	Dimensions	Corrélation			
		originale		cryptée	
		horizontal	vertical	horizontal	vertical
lena	512x512	0.9774	0.9880	0.0026	-0.00039
panda256	256x256	0.98466	0.98166	0.0033171	0.0015736
peppers	512x512	0.96177	0.96397	-0.00091225	0.00054093
lena (180x180)	180x180	0.94395	0.96547	0.0019166	-0.0045507
baboon	512x512	0.92178	0.86241	6.072e-05	-2.8973e-06
airplane	512x512	0.9726	0.95069	-0.0040927	0.0014896
cameraman	225x225	0.93634	0.95915	-0.0042623	-0.0065271
cameraman	160x160	0.93363	0.95686	-0.0060649	-0.001334
onion	135x198	0.98585	0.96676	-0.0099237	0.0040469

TABLE 4.5 – Corrélation entre l'image originale et l'image cryptée.

Les tableaux suivants 4.6 et 4.7 représentent les différents résultats obtenus à partir des recherches :

Image	Entropie	NPCR	UACI	MSE	PSNR	CC
lena	7.9994	99.6143	30.5318	8980.9931	8.5976	-0.0054977
lena [**22**]	7.9993	99.6223	33.3823	31078.8827	9.2257	-0.0020
lena [**35**]	7.9973	99.6323	33.4286	7773.3	9.2248	-0.0007
baboon	7.9998	99.5927	29.9953	8648.6205	8.7613	-0.0027336
baboon [**22**]	7.99976	99.5667	33.5354	6920.1784	9.7296	-0.0001
baboon [**35**]	7.9974	99.6017	33.4191	6960.4	9.7045	0.0017
peppers	7.9998	99.6197	32.2126	10108.5329	8.0839	0.0014436
peppers [**22**]	7.9992	99.6403	33.5468	33667.8582	8.8792	0.0009
peppers [**35**]	7.9970	99.5865	33.5052	8433.8	8.8706	-0.0027

TABLE 4.6 – Comparaison des mesures d'entropie, NPCR, UACI, MSE, PSNR et CC pour différentes images de test.

Image	Corrélation			
	Originale		Cryptée	
	Horizontal	Vertical	Horizontal	Vertical
lena	0.9774	0.9880	0.0026	-0.00039
lena [**22**]	0.9691	0.9841	0.00305	1.1×10^{-6}
lena [**35**]	0.9456	0.0006	0.9727	-0.0035
peppers	0.96177	0.96397	-0.00091225	0.00054093
peppers [**22**]	0.9733	0.9763	-0.0006	0.00208
peppers [**35**]	0.9635	0.0026	0.9705	-0.0004
baboon	0.92178	0.86241	6.072×10^{-5}	-2.8973×10^{-6}
baboon [**22**]	0.8677	0.8198	-0.005	-0.0014
baboon [**35**]	0.8737	-0.0024	0.8261	0.0053

TABLE 4.7 – Comparaison de la corrélation entre l'image originale et l'image cryptée .

4.4 Conclusion

Les cartes chaotiques multidimensionnelles sont largement utilisées dans le domaine de la sécurité en raison de leur comportement extrêmement complexe et chaotique, qui les rend bien plus imprévisibles et difficiles à analyser que leurs équivalents unidimensionnels.

Parmi ces cartes, la carte tridimensionnelle logistique et la carte de Chirikov sont particulièrement réputées. L'utilisation de la carte logistique tridimensionnelle offre une variété de comportements chaotiques complexes, ce qui augmente la complexité et l'efficacité des systèmes de code.

D'autre part, la carte de Chirikov se démarque par sa capacité à produire des comportements non réguliers et divers, ce qui renforce la solidité du cryptage et rend difficile sa casse. Ces propriétés renforcent la sécurité des applications de cryptage, car ces cartes proposent un large espace de clés et des comportements inattendus, ce qui rend le décryptage extrêmement complexe même avec des techniques d'attaque classiques ou brutales.

Conclusion générale

Cette étude propose un nouveau schéma de cryptage d'image utilisant une carte logistique 3D et une carte de Chirikov améliorée. Les méthodes de cryptage et de décryptage sont clairement expliquées, et une analyse de sécurité approfondie montre que l'algorithme résiste aux attaques statistiques, à la force brute, au bruit et aux attaques différentielles.

L'algorithme est très sensible aux variations des valeurs initiales et des paramètres clés, ce qui le rend difficile à déchiffrer sans ces informations. Comparé aux méthodes existantes, ce système est plus sécurisé et rapide. Il peut également être étendu à des cartes chaotiques multidimensionnelles et inclure d'autres méthodes de compression.

Bibliographie

a. Bibliographie : Ouvrages et articles consultés lors de l'élaboration du rapport :

[1] https://edu1d.ac-toulouse.fr/politique-educative-31/site-ressources31/files/04-photofiltre7-resolution-definition-simplifie.pdf

[2] Numeriksciences, http://numeriksciences.fr, consulté le 14/04/2023.

[3] @articleagaguena2023etude, title=Etude et simulation d'un système de cryptage d'images à base de chaos, author=Agaguena Houdjatoulah, Tifouti Miloud, year=2023, publisher=Université 08 Mai 1945 de Guelma

[4] https://www.univ-constantine2.dz/files/Theses/Informatique/Magistere/Mohamed-Sandeli.pdf

[5] http://bnazarian.free.fr/MyUploads/INGBM06BINAIRES.PDF

[6] https://iast.univsetif.dz/documents/Cours/CoursInformatiqueL1GAT21.pdf

[7] R. Isdant, Traitement numérique de l'image, 2009, http://raphael.isdant.free.fr/traitement_numerique/2-traitementnumeriquedel%27image.pdf, consulté le 17/03/2024.

[8] https://www.tezabo.com/blog/image-bitmap-vectorielle-quelles-differences-n57, consulté le 02/03/2024.

[9] https://graphiste.com/blog/images-matricielles-vectorielles-qui-utiliser/, consulté le 21/02/2024.

[10] https://elearning.centre-univ-mila.dz/a-2023/pluginfile.php/91644/mod_resource/content/1/Chapitre%202%20%20.pdf, consulté le 25/03/2024.

[11] https://people.montefiore.uliege.be/dumont/pdf/crypto09-10.pdf

[12] https://aws.amazon.com/fr/what-is/cryptography/, consulté le 21/03/2024.

[13] https://www.scribd.com/document/647540652/Chapitre-2-Cryptographie-Classique

consulté le 25/03/2024.

[14] @articleboussayoudcryptage, title=Cryptage/Chiffrement & Tatouage des données numériques, author=BOUSSAYOUD, Ryma Dr and CHIOUKH, Labiba and AFER, Doha and BOUCHAIR, Djihan and TITI, Nesrine , consulté le 28/04/2024.

[15] `https://dspace.ummto.dz/server/api/core/bitstreams/70807841-743d-4b7b-92bd-9` `content`

[16] `https://www.tutorialspoint.com/cryptography/modern_cryptography.` `htm`

[17] D'après un cours de Daniel Barsky Ghislain Dartois, Cryptographie, Paris 13 le 1 octobre 2010 `https://www.math.univ-paris13.fr/`

[18] `https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-mecanismes_` `crypto-2.04.pdf`

[19] `https://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne%` `2Fblocs`

[20] `https://blog.mailfence.com/fr/difference-chiffrement-symetrique-asymetrique/`

[21] `https://members.loria.fr/PZimmermann/cours/id12-2005-3.pdf`, consulté le 17/03/2024.

[22] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," 2022.

[23] M. Es-sabry, N. El Akkad, L. Khrissi, K. Satori, W. El-Shafai, T. Altameem, and R. S. Rathore, "An encryption technique using multiple chaotic maps and advanced ciphers," 2024.

[24] Zhang, Hangming, and Hanping Hu. "An image encryption algorithm based on a compound-coupled chaotic system," 29 December 2023.

[25] Manzoor Ahmad Lone and Shaima Qureshi. (2022). *RGB image encryption based on symmetric keys using Arnold transform, 3D chaotic map and affine hill cipher*

[26] Peng, Yuexi, et al. "A simple color image encryption algorithm based on a discrete memristive hyperchaotic map and time-controllable operation," 13 May 2023.

[27] Zhenhui Li, He, Z., Huang, F. et al. *A Bit-Level Three-Dimensional Rectangular Image Encryption Algorithm Using New Chaotic Maps*. Aut. Control Comp. Sci. (2023).

[28] https://butec.univ-saida.dz/admin/opac_css/doc_num.php?explnum_id=1358, consulté le 02/05/2024.

[29] https://fr.mathworks.com/videos/advanced-programming-with-matlab-87540.html, consulté le 11/05/2024.

[30] https://di.univ-blida.dz, consulté le 06/05/2024.

[33] @articleBADETZ200437, title = La face cachée des images numériques en anatomie et cytologie pathologiques (1) : les contraintes de l'image numérique, journal = Revue Française des Laboratoires, volume = 2004, number = 367, pages = 37-40, year = 2004, issn = 0338-9898, doi = https ://doi.org/10.1016/S0338-9898(04)80285-3, url = https ://www.sciencedirect.com/science/article/pii/S0338989804802853, author = Lionel Badetz and Françoise Cornélis and Jacqueline Ferrand

[34] Cong Xu, Jingru Sun, Chunhua Wang. "An Image Encryption Algorithm Based on Random Walk and Hyperchaotic Systems." *J*uly 5, 2019.

[35] Mohammed Jabbar Obaid, Najlae Falah Hameed Al Saffar. "Asymmetric Image Encryption Based on Singular Cubic Curve with Chaotic Map " *May 30,2024*

[36] https://blog.veoprint.com/quelle-resolution-dimage-adopter-en-fonction-du-su

[37] https://iast.univ-setif.dz/documents/Cours/CoursInformatiqueL1GAT21.pdf

[38]https://www.auxartsgraphiques.fr/pages/rvb_cmjn.php

[39]https://www.baches-publicitaires.com/blog/actualites/vectorisation-cest/

[40]http://cryptographie.over-blog.com/2018/04/le-chiffre-de-cesar.html

[41]https://www.bibmath.net/crypto/index.php?action=affiche&quoi=poly/vigprobable

[42]https://fr.wikipedia.org/wiki/Cryptographie_asym%C3%A9trique

[43] https://www.researchgate.net/figure/Representation-dune-image-numerique23_fig1_344266838

[44] https://constantine.mta.gov.dz/

[45] https://www.researchgate.net/figure/Chiffrement-et-dechiffrement_fig1_237608366

[46] https://tpetransmissioncryptographie.wordpress.com/tpe-cryptographie-introdu

[47] http://nopb.chez.com/crypto2.html