الجمهوريـــة الجزائريـة الديمقراطيـة الشعبيـة
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

وزارة التعليم العالي والبحث العلمي

Université 20 août 1955 – Skikda-

جامعة 20 أوت 1955 سكيكدة

Ref:D012123030D

FACULTE DE TECHNOLOGIE

THESE

Présentée Pour l'obtention du

Diplôme de

DOCTORAT

Filière : Electronique

Option : Signaux et Images

Par

HADDAD Ismail

THEME

Techniques de cryptage des Images Couleurs en utilisant les Signaux Chaotiques d'ordre fractionnaires.

Soutenue le 20/12/2023 devant le Jury:

DJEMILI Rafik	**Professeur**	**Université 20 août 1955 Skikda**	**Président**
BELMEGUENAI Aissa	**Professeur**	**Université 20 août 1955 Skikda**	**Rapporteur**
BOUMERDASSI Selma	**Professeur**	**CNAM,Paris-France**	**Co-rapporteur**
MAAZOUZI Ismail	**Professeur**	**Université 20 août 1955 Skikda**	**Examinateur**
FERDI Youcef	**Professeur**	**ENS.Biotechnologie Constantine**	**Examinateur**
BELATTAR Mounir	**MCA**	**Université 20 août 1955 Skikda**	**Examinateur**

العنوان: تقنيات تشفير الصور الملونة باستخدام إشارات الفوضى ذات الترتيب الجزئي

ملخص

في عالم اليوم الرقمي، يعد نقل المعلومات الآمن أمرًا بالغ الأهمية، خاصة عندما يتعلق الأمر بالصور الرقمية. لم تعد أساليب التشفير التقليدية كافية لتأمين أمان جميع أنواع الصور الرقمية، مما أدى إلى ظهور تشفير الصور كمسألة حرجة. قام العديد من الخبراء بالتحقيق في منهجيات مختلفة لهذه المشكلة، بما في ذلك ترميز الحمض النووي ونظرية الكم ونظرية الفوضى. على الرغم من هذه الجهود، فإن غالبية مخططات تشفير الصور المقترحة بها العديد من نقاط الضعف الأمنية التي يجب حلها. توفر تقنيات التشفير التي تستخدم أنظمة فوضوية صحيحة الأمان والأداء غير المسبوقين. لسوء الحظ، تعاني هذه الأنظمة من أوجه قصور كبيرة، مثل المجالات الفوضوية المحصورة والتوزيع غير المتكافئ للتسلسلات العشوائية. نتيجة لذلك، فإن أنظمة التشفير القائمة على هذه الأنظمة معرضة للهجوم. يهدف هذا البحث إلى معالجة التحديات الأمنية الناشئة عن نقاط ضعف النظام الفوضوي في الترتيب الصحيح من خلال تقديم طرق تشفير جديدة تتناسب مع أهداف حماية الصورة. تعتمد هذه الأساليب على أنظمة فوضوية جزئية أكثر تعقيدًا وأقل قابلية للتنبؤ بها ولها مجال فوضوي أكبر من نظيراتها الصحيحة. لمعالجة قيود الأنظمة الفوضوية للأنظمة الصحيحة، يتم تقديم نظام فوضوي معزز للترتيب الجزئي لزيادة أداء وأمن نظام التشفير.

الكلمات المفتاحية النظام الفوضوي الجزئي ، ترميز الحمض النووي ، نظرية الكم ، تشفير الصور.

Titre : Techniques de Cryptage des Images Couleurs en utilisant les Signaux Chaotiques d'ordre Fractionnaires.

Résumé :

Dans le monde numérique d'aujourd'hui, le transport sécuritaire de l'information est essentiel, surtout en ce qui concerne les images numériques. Les approches cryptographiques classiques ne suffisent plus à assurer la sécurité de toutes sortes des images numériques, ce qui fait de la cryptographie des images un enjeu crucial. Plusieurs experts ont étudié diverses méthodologies à ce sujet, y compris la théorie quantique, le codage de l'ADN et la théorie du chaos. Malgré ces efforts, la majorité des schémas de cryptage des images proposés présentent de nombreuses faiblesses de sécurité qui doivent être résolues. Les techniques de cryptage qui utilisent des systèmes chaotiques d'ordre entier fournissent une sécurité et des performances inégalées. Malheureusement, ces systèmes ont des lacunes, comme les champs chaotiques confinés et la distribution inégale des séquences aléatoires. En conséquence, les crypto-systèmes basés sur ces systèmes sont vulnérables aux attaques. Notre recherche vise à relever les défis de sécurité émergeant des faiblesses des systèmes chaotiques d'ordre entier en offrant des nouvelles méthodes de chiffrement qui correspondent aux objectifs de protection des images. Ces méthodes dépendent des systèmes chaotiques d'ordre fractionnaire, qui sont plus complexes, moins prévisibles, et ont un champ chaotique plus grand que leurs homologues d'ordre entier. Pour répondre aux contraintes des systèmes chaotiques d'ordre entier, nous avons présenté un système chaotique d'ordre fractionnaire amélioré en augmentant la performance et la sécurité du système de cryptage.

Mots clés :Système chaotique d'ordre fractionnaire, codage de l'ADN, théorie quantique, chiffrement d'image.

Title : Techniques de Cryptage des Images Couleurs en utilisant les Signaux Chaotiques d'ordre Fractionnaires.

Abstract :

In today's digital age, the assurance of secure information transmission is critical, especially in the context of digital images. Traditional cryptographic methods are proving insufficient in safeguarding the security of diverse digital images, prompting the urgent need for advancements in image cryptography. Experts have explored various methodologies, such as DNA coding, quantum theory, and chaos theory, to address this challenge. Despite these efforts, many proposed image encryption schemes still exhibit significant security vulnerabilities that require resolution.

One specific area of concern is the use of encryption techniques involving integer-order chaotic systems. While these methods offer unparalleled security and performance, they suffer from notable drawbacks, including confined chaotic fields and uneven distribution of random sequences. These limitations make them susceptible to various attacks. This research aims to overcome the security challenges posed by the weaknesses of integer-order chaotic systems by introducing novel encryption methods aligned with the objectives of image protection.

The proposed methods rely on fractional-order chaotic systems, which are characterized by greater complexity, unpredictability, and a larger chaotic field compared to their integer-order counterparts. To address the constraints associated with integer-order chaotic systems, an enhanced fractional-order chaotic system is introduced. This enhancement is designed to improve the performance and security of the encryption system, offering a more robust solution to the challenges posed by securing digital images in today's dynamic digital landscape.

Keywords : : Fractional order chaotic system, DNA coding, quantum theory, image encryption

Liste des publications

- ✓ **Colour image encryption based on an improved fractional order logistic** **Ismail Haddad** ,Djamel Herbadji, Aissa Belmeguenai,Selma Boumerdassi. Date de publication 2022/12/15 Revue International Journal of Electronic Security and Digital Forensics Volume 15 Numéro 1 Pages 66-87
  https ://www.inderscience.com/info/inarticle.php ?artid=127747
- ✓ **A Robust Color Image Encryption based on new Zigzag Technique and 3D Fractional-Order Chaotic system** **Ismail Haddad** ,Djamel Herbadji, Aissa Belmeguenai,Selma Boumerdassi. Revue Optik (Article en soumission)

Liste des communications

- ✓ **Color image encryption based on fractional order logistic map** **Ismail Haddad**, Aissa Belmeguenai, Djamel Herbadji,Selma Boumerdassi. 7th International conference on image and signal processing and thier applications (ISPA),2022 in Mostaganem.
  https ://ieeexplore.ieee.org/document/9786281
- ✓ **A New Encryption Approach For Color Image Using 3D Fractional Order Chaotic System**
  Ismail Haddad, Aissa Belmeguenai, Djamel Herbadji,Selma Boumerdassi. IEEE 21st international Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA),2022 in Sousse,Tunisia.
  https ://ieeexplore.ieee.org/document/10019142
- ✓ **Novel Image Encryption Using Fractional Order Chaotic System** **Ismail Haddad**, Djamel Herbadji, Aissa Belmeguenai,Selma Boumerdassi. 1st International Conference on Scientific and Academic Research (ICSAR),2022 in Konya,Turkey

- ✓ **Fractional Order Chaotic System and Its Application in color image encryption** **Ismail Haddad**, Djamel Herbadji, Aissa Belmeguenai,Selma Boumerdassi. National Conference on Telecommunications and its Applications (CNTA'22),2022 in Ain-Témouchent, Algeria.

- ✓ **New Approach For Color Image Encryption Using Two 1-D chaos systems** Djamel Herbadji, Abderhmane Herbadji,**Ismail Haddad**, Aissa Belmeguenai,Nadir Derouiche. National Conference on Telecommunications and its Applications (CNTA'22),2022 in Ain-Témouchent, Algeria

- ✓ **A New Medical Image Encryption Using Enhanced Chaotic system** Djamel Herbadji,**Ismail Haddad**, Abderhmane Herbadji, Aissa Belmeguenai. The 1st National Workshop on Wireless Network,Cloud Computing and Cryptography.2023 in boumerdes,Algeria.
- ✓ **Fast and accurate diagnosing of COVID-19 cases using Convolutional neural network** Djamel Herbadji, Abderhmane Herbadji ,**Ismail Haddad**,Hichem kahia , Aissa Belmeguenai. The 1st National Workshop on Wireless Network,Cloud Computing and Cryptography.2023 in boumerdes,Algeria

Remerciement

Nous tenons avant tout à remercier dieu qui nous a aidé et donné la volonté et la résistance pour réaliser ce travail de thèse.

Ce travail a été réalisé au laboratoire de recherche en électronique, sous la direction de Aissa Belmeguenai professeur à l'université 20 août 1955 -Skikda, dans le cadre de la préparation de thèse de doctorat en électronique au département gêné-électrique de l'université 20 août 1955 Skikda.

Je remercie tous les membres du laboratoire et tous les membres du doctorat " signaux et images" sous la direction de Monsieur Djemili Rafik Professeur à l'Université 20 août 1955 de Skikda.

Je remercie vivement mon directeur et mon co-directeur de thèse, Messieurs BELMEGUENAI Aissa Professeur à l'université 20 août 1955 -Skikda et BOUMERDASSI Selma Professeur chez CNAM,Paris-France qui ont accepté d'assurer l'encadrement de ce travail. leurs suivi permanant, leurs orientations efficaces, leurs conseils précieux et leurs qualités humaines m'ont permis de réaliser convenablement les différentes étapes de ce travail de thèse.

Je suis très honoré de remercier pour leur présence à mon jury de thèse : Messieurs DJEMILI Rafik Professeur à l'université 20 août 1955 Skikda , MAAZOUZI Ismail Professeur à l'université 20 août 1955 Skikda, FERDI Youcef Professeur à ENS. Biotechnologie Constantine et BELATTAR Mounir Maître de conférences (MCA) à l'Université 20 août 1955 de Skikda pour le temps consacré à la lecture de cette thèse, et pour les suggestions et les remarques judicieuses qu'ils ne manquerons pas de m'indiquer.

Je voudrais aussi adresser toute ma reconnaissance à mes professeurs des universités de Guelma et de Skikda, qui m'ont fourni les outils nécessaires à la réussite de mes études universitaires.

A titre plus personnel, j'aimerais exprimer ma gratitude à mes parents, mon frère et ma soeur pour leur grande patience, leurs encouragements et leur amour, ainsi que pour leur soutien qui m'a été bien utile durant ma thèse.

En fin, à tous mes amis en particulier Djamel Herbadji qui m'ont apporté leur soutien moral et intellectuel tout au long de ma démarche.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

✓ **AES** : Advanced Encryption Standard

✓ **COA** : Attaque sur texte chiffré seul

✓ **CPA** : Attaque texte clair choisi

✓ **DES** : Data Encryption Standard

✓ **NIST** : National Institute of Standards Technologie

✓ **NPCR** : Number of Pixels Change Rate

✓ **PRNG** : Pseudo Random Number Generator

✓ **RGB** : Red Green Blue

✓ **RSA** : Ronald Rivest, Adi Shamir et Leonard Adleman

✓ **RVB** : Rouge Vert Bleu

✓ **UACI** : Unified Average Changing Intensity

✓ **XOR** : OU exclusif

Introduction Générale

Actuellement, avec l'avancement des techniques de communication telles que l'internet, les satellites et les communications sans fil, ainsi que l'expansion continue des tactiques et des approches de pénétration, il est de plus en plus nécessaire de prioriser la protection et la confidentialité des données échangées entre les réseaux et les ordinateurs. Cette exigence a toutefois créé de nouveaux défis, non seulement pour fournir des solutions efficaces en matière de sécurité de l'information, mais aussi pour leur développement. Selon ce contexte, la cryptographie a acquis un rôle essentiel dans la préservation de l'information sensible dans le monde technologique, faisant de l'utilisation des techniques de chiffrement une exigence inévitable. De nombreux algorithmes ont été développés et déployés pour protéger et crypter les données, y compris les méthodes de cryptage traditionnelles telles que DES (Data Encryption Standard) et RSA (Rivest Shamir Adleman). Ces algorithmes sont très efficaces pour coder des données binaires ou textuelles. Cependant, ces algorithmes peuvent ne pas convenir aux fichiers multimédias sophistiqués, tels que les images, en raison que ces types des données a du grand volume, ainsi que du haut degré d'interconnexion entre les pixels [1, 2]. Selon la recherche, de nombreux algorithmes réussis sont construits avec des systèmes chaotiques entiers. Les systèmes chaotiques d'ordre entier ont plusieurs avantages, y compris une grande sensibilité aux conditions initiales et à la capacité de créer des valeurs pseudo-aléatoires de manière sonore [3–5] . Nous pouvons généralement générer une nouvelle séquence aléatoire différente en modifiant les valeurs initiales ou les paramètres de contrôle. Grâce à ces qualités, les algorithmes de cryptage basés sur le système chaotique d'ordre entier sont très efficaces en termes de sécurité et de vitesse. Malgré le succès des systèmes chaotiques entiers, ils font face à certaines limitations telles qu'un champ chaotique restreint et une distribution inégale des séquences aléatoires. Ces faiblesses rendent les systèmes cryptographiques basés sur eux vulnérables aux attaques. Une des solutions pour résoudre ce problème est d'utiliser des systèmes chaotiques d'ordre fractionnaire pour crypter les images couleurs parce qu'elles sont plus complexes et moins prévisibles que leurs homologues d'ordre entier. Cela pourrait être une réponse à des techniques de cryptage plus fortes et plus sécurisées. De ce point de vue, la motivation de ce travail est d'analyser les systèmes chaotiques avec un ordre fractionnaire comme générateur des nombres aléatoires tout en trouvant des nouvelles façons de chiffrer les images couleurs. Ainsi, dans le but d'améliorer les exigences de protection des images couleurs, trois algorithmes de cryptage efficaces basés sur des systèmes chaotiques d'ordre fractionnaire ont été proposés.

La thèse est structurée en cinq chapitres, qui sont organisés comme suit :

- ✓ Le premier chapitre de cette thèse est consacré à l'étude des systèmes chaotiques d'ordre fractionnaire. Il commence par un examen des définitions et des propriétés importantes des systèmes chaotiques, puis passe à une discussion des concepts de base et des définitions de calcul fractionnaire. Ces concepts sont essentiels pour modéliser et étudier les systèmes

chaotiques fractionnaires.

✓ Le deuxième chapitre offre une approfondie dans les bases fondamentales de la cryptographie, tout en exposant en détail la classification des diverses techniques de chiffrement. De manière significative, une attention particulière est accordée aux outils spécifiques utilisés pour une évaluation précise de l'efficacité du chiffrement appliqué aux images. Cette section vise à fournir une compréhension exhaustive des principes sous-jacents de la cryptographie, tout en mettant en lumière les moyens concrets par lesquels les praticiens peuvent mesurer et analyser la robustesse des méthodes de chiffrement visant à sécuriser des données graphiques.

✓ Au sein du troisième chapitre de notre étude, nous approfondissons la présentation d'un système novateur de cryptage des images couleurs fondé sur une carte chaotique d'ordre fractionnaire. Notre analyse approfondie met en lumière les caractéristiques singulières de cette approche, ouvrant ainsi une perspective nouvelle et prometteuse dans le domaine de la sécurité des données visuelles. Le choix d'adopter la carte chaotique d'ordre fractionnaire repose sur son efficacité remarquable et ses caractéristiques distinctes par rapport à la carte chaotique d'ordre entier. Cette distinction confère à la carte chaotique d'ordre fractionnaire des avantages significatifs en termes de complexité, de sensibilité aux conditions initiales et de capacité de diffusion. De manière notable, l'utilisation du paramètre d'ordre fractionnaire supplémentaire fourni par la carte logistique d'ordre fractionnaire élargit considérablement l'espace clé du cryptosystème. Cette fonctionnalité renforce ainsi l'importance et l'utilité du procédé dans le contexte du cryptage des images.

✓ Le quatrième chapitre constitue une avancée significative dans le domaine de la sécurité des images grâce à la présentation d'un algorithme de cryptage novateur basé sur une carte logistique chaotique d'ordre fractionnaire améliorée, cet algorithme offre une contribution majeure à la préservation de la sécurité des données visuelles. La contribution essentielle de ce chapitre réside dans la proposition d'une amélioration spécifique de la carte logistique fractionnaire, conçue pour être intégrée dans une nouvelle approche de chiffrement. Cette amélioration surmonte des défis inhérents tels que la distribution non uniforme des séquences chaotiques et la limitation de la gamme des comportements chaotiques, lesquels ont été résolus grâce à une optimisation de la carte d'ordre fractionnaire. Ainsi, dans le contexte des algorithmes de chiffrement, cette optimisation renforce considérablement la sécurité et accroît la fiabilité de l'algorithme.

✓ Le cinquième chapitre de cette étude représente une avancée majeure dans la résolution

des problèmes inhérents aux méthodes en zigzag utilisées dans les systèmes de cryptographie existants. Ces méthodes classiques traitent les pixels de manière continue, les considérant comme une séquence linéaire se déplaçant uniformément dans une direction fixe, avec des valeurs de décalage constantes. Bien que cette approche soit souvent perçue comme une limitation difficile à surmonter, notre objectif est de dépasser ces contraintes en améliorant de manière significative la méthode en zigzag existante. Pour atteindre cet objectif, nous avons introduit une approche novatrice en utilisant une technique unique de zigzag et un système chaotique tridimensionnel avec un ordre fractionnaire. Cette approche vise à rendre le processus de cryptage plus distinct et capable de suivre divers emplacements des pixels, contribuant ainsi à renforcer la sécurité globale du système. Notre recherche repose sur l'utilisation simultanée de plusieurs variantes de zigzag, générant des modèles imprévisibles régis par un système chaotique d'ordre fractionnaire tridimensionnel. L'intégration de cette méthode vise à accroître considérablement la complexité de l'algorithme, renforçant ainsi sa résilience contre différentes attaques et établissant les bases de systèmes de cryptage plus robustes.

Dans la dernière partie, nous présentons une conclusion exhaustive qui résume la recherche effectuée et les résultats obtenus.

Chapitre 1

Généralité sur les signaux chaotiques d'ordre Fractionnaire

Sommaire

1.1 Introduction

La théorie du chaos est une nouvelle discipline de la physique et des mathématiques qui aide à la compréhension de divers systèmes et processus physiques [6] . Edward Lorenz l'a publié pour la première fois dans la deuxième partie du XXe siècle [7]. En conséquence, sa popularité a augmenté, et il a réussi à attirer des intérêts de recherche, ouvrant la voie à des nombreuses études axées sur le comportement des systèmes dynamiques non linéaires. Les premières recherches sur le chaos ont révélé qu'il possède plusieurs caractéristiques particulières, telles que la sensibilité aux conditions initiales, complexité, ergodicité, transitivité et déterminisme [8], qui ont été utilisées dans des domaines critiques comme les télécommunications [9–11], la robotique [12, 13], et la médecine [14, 15].

Le calcul fractionnaire est un concept mathématique qui a apparu pour la première fois en 1695, mais ses applications à la physique et l'ingénierie ont seulement récemment attiré l'attention des chercheurs [16]. Il a été découvert que de nombreux systèmes dans diverses disciplines sont caractérisés par une équation différentielle fractionnaire par exemple, la polarisation électrolytique [17], la modélisation de la viscoélasticité [18] et la propagation des ondes [19] .

Le but de ce chapitre est d'étudier théoriquement les systèmes chaotiques d'ordre fractionnaire, nous commencerons par quelques définitions liées au calcul fractionnaire et aux opérateurs d'ordre fractionnaire et quelques propriétés principales, puis nous introduirons quelques notions de base sur le chaos. Nous terminons ce chapitre en présentant une classification des systèmes chaotiques d'ordre fractionnaire.

1.2 Le calcul fractionnaire

Le calcul fractionnaire est un domaine des mathématiques analytiques qui explore les nombreuses façons de déterminer les ordres en nombres réels ou complexes de l'opérateur de différenciation et d'intégration. Dans ce qui suit, nous présenterons quelques bases mathématiques du calcul fractionnaire.

1.2.1 Outils mathématiques de base

Dans cette partie, nous aborderons les fonctions mathématiques clés qui nous permettent de fournir des réponses aux problèmes de calcul fractionnaire : la fonction Gamma d'Euler, la fonction bêta, La fonction hypergéométrique et la fonction Mittag-Leffler.

1.2.1.1 La fonction Gamma

La fonction Gamma d'Euler est l'une des fonctions fondamentales du calcul fractionnaire. La limite d'Euler fournit une formulation de la fonction gamma comme suit [20] :

$$\Gamma(x) = \lim_{N \to +\infty} \left(\frac{N! N^x}{x[x+1][x+2] \ldots\ldots\ldots\ldots [x+N]} \right) \tag{1.1}$$

La définition intégrale (1.1) est fréquemment utilisée même si elle est limitée aux valeurs positives de x [20] :

$$\Gamma(x) = \int_0^{+\infty} y^{x-1} e^{-y} dy, x > 0 \tag{1.2}$$

Nous pouvons déduire de (1.2) que :

$$\Gamma(1) = \int_0^{+\infty} e^{-t} dt = 1 \tag{1.3}$$

En effectuant une intégration par partie de l'expression(1.2), on aboutit à la propriété fondamentale de la fonction gamma, illustrée par la relation suivante :

$$\Gamma(\alpha + 1) = \alpha \Gamma(\alpha) \tag{1.4}$$

Aussi, pour tout entier positif x, nous avons :

$$\Gamma(x + 1) = x! \tag{1.5}$$

1.2.1.2 La fonction Bêta

La fonction Bêta est une intégrale d'Euler spécifiée pour des nombres complexes z et w selon [21] :

$$B(z, w) = \int_0^1 t^{z-1} (1-t)^{w-1} dt, Re(z) > 0, Re(W) > 0 \tag{1.6}$$

La relation entre les fonctions Beta et Gamma est la suivante :

$$B(z, w) = \frac{\Gamma(z)\Gamma(w)}{\Gamma(z+w)}, Re(z) > 0, Re(W) > 0 \tag{1.7}$$

D'après (1.7), il est évident que :

$$B(z, w) = B(w, z), Re(z) > 0, Re(W) > 0 \tag{1.8}$$

1.2.1.3 La fonction hypergéométrique

La fonction hypergéométrique de gauss est définie comme la somme des séries hypergéométriques dans le disque unitaire :

$$F_1(a,b,c,z) = \sum_{k=0}^{\infty} \frac{(a)_k (b)_k}{(c)_k} \frac{z^k}{k!} \tag{1.9}$$

où $(a)_k, (b)_k$ et $(c)_k$ sont des symboles de Pochhammer, qui sont des généralisations des factorielles. La fonction hypergéométrique peut être donnée par la représentation de l'intégrale d'Euler :

$$F_1(a,b,c,z) = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \int_0^1 t^{b-1}(1-t)^{c-b-1}(1-zt)^{-a} dt \tag{1.10}$$

Lorsque $Re(b) > 0, Re(c) > 0$ et$|arg(1-z)| < \pi$ la fonction hypergéométrique est définie comme suit :

$$F_1(a,c,z) = \sum_{k=0}^{\infty} \frac{(a)_k}{(c)_k} \frac{z^k}{k!} \tag{1.11}$$

1.2.1.4 La fonction Mittag-Leffler

La fonction exponentielle est particulièrement importante dans l'étude des équations différentielles d'ordre entier. G.M. Mittag-Leffler a présenté la généralisation de la fonction exponentielle à un seul paramètre, qui est indiqué par la fonction suivante [22] :

$$E_\alpha(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(\alpha k + 1)} \tag{1.12}$$

La fonction Mittag-Leffler à deux paramètres est également cruciale dans la théorie du calcul fractionnaire. Elle est caractérisée par le développement en série suivant [22] :

$$E_{\alpha,\beta}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(\alpha k + \beta)}, (\alpha, \beta > 0) \tag{1.13}$$

A partir de la relation (1.13) on montre que :

$$E_{1,1}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(k+1)} = \sum_{k=0}^{\infty} \frac{z^k}{k!} = e^z \tag{1.14}$$

La fonction Mittag-Leffler a le même but que la fonction exponentielle dans les équations différentielles d'ordre fractionnaire.

1.2.2 Définitions des dérivées et des intégrales d'ordre fractionnaire

Au cours du développement de la théorie du calcul fractionnaire, une variété de définitions d'intégration et des dérivations d'ordre fractionnaire ont été proposées. Les définitions les plus couramment utilisées par la communauté scientifique sont présentées dans les sections qui suivent :

1.2.2.1 Intégrales d'ordre fractionnaire

Soit f(t) une fonction réelle de la variable réelle t qui est continue et intégrable sur [0, +∞ [, la formule suivante représente son intégration répétée j fois [23] :

$$I^j f(t) = \frac{1}{(j-1)!} \int_{t_0}^{t} (t-\tau)^{j-1} f(\tau) d\tau \tag{1.15}$$

La fonction Gamma a été introduite par Riemann pour remplacer la fonction factorielle. La fonction d'intégration fractionnaire est ainsi obtenue [23] :

$$I^\alpha f(t) = \frac{1}{\Gamma(\alpha)} \int_{t_0}^{t} (t-\tau)^{\alpha-1} f(\tau) d\tau \tag{1.16}$$

$\Gamma(.)$ est la fonction de Gamma, donnée par :

$$\Gamma(x) = \int_0^{+\infty} t^{x-1} e^{-t} dt. \forall x \in \Re^* \tag{1.17}$$

En substituant la borne inférieure d'intégration de l'intégrale d'ordre réel (1.15) par -∞, on aboutit à la formulation connue sous le nom de définition de Riemann-Liouville.

1.2.2.2 Dérivées fractionnaires

Il existe différentes définitions de dérivés fractionnaires. Dans cette section, nous proposons les définitions les plus utilisées telles que Riemann-Liouville, Caputo et Grunwald-letnikov.

Définition de Riemann-Liouville : La définition de Riemann-Liouville est essentielle au développement de la théorie des dérivés fractionnaires. La dérivé d'ordre fractionnaire d'une fonction f (t) selon Riemann-Liouville est donné par l'équation suivante [24] :

$$D_{t_0}^\alpha f(t) = \frac{1}{\Gamma(n-\alpha)} \frac{d^n}{d\tau^n} \int_{t_0}^{t} (t-\tau)^{n-\alpha-1} f(\tau) d\tau \tag{1.18}$$

Où n est un nombre entier, sous la condition $(n-1 < \alpha < n)$. La transformation de Laplace de Riemann-Liouville est la suivante :

$$L[D^{\alpha}_{t_0} f(t)] = \begin{cases} P^{\alpha} F(P) & \alpha < 0 \\ \sum_0^{n-1} P^k (D_t^{\alpha-k-1} f(0)) & \alpha > 0 \end{cases} \tag{1.19}$$

Avec $n-1 < \alpha < n$ et $n \in \mathbb{N}$.

Définition de caputo : Plusieurs chercheurs, y compris Caputo, ont reconnu que la notion de dérivation fractionnaire dans le sens de Riemann-Liouville doit être mis à jour en raison des problèmes rencontrés dans la viscoélasticité, la mécanique du solide et la rhéologie. Caputo a développé un autre concept de dérivation fractionnaire dans le cadre de son travail à la fin des années 1960. Cette définition est exprimée mathématiquement comme suit [23] :

$$D^{\alpha}_{t_0} f(t) = \frac{1}{\Gamma(n-\alpha)} \int_{t_0}^{t} (t-\tau)^{n-\alpha-1} f^n(\tau) d\tau \tag{1.20}$$

avec $f^{(n)}(\tau)$ est la dérivée d'ordre entier de la fonction $f(\tau)$ et n entier positif vérifiant $n-1 < \alpha < n$. La dérivé d'ordre fractionnaire de Caputo peut être défini en utilisant la formulation de Riemann-Liouville comme suit.

$${}^{RL}_{0}D^{\alpha} f(t) = {}^{C}_{0} D^{\alpha} f(t) + \sum_{k=0}^{n-1} \frac{t^{k-a}}{\Gamma(k-\alpha+1)} f^{(k)}(0^+) \tag{1.21}$$

Selon la définition de Caputo, la transformation de Laplace de la dérivée d'ordre fractionnaire de la fonction f(t) est donnée par :

$$L[{}^{C}_{0}D^{\alpha} f(t)] = P^{\alpha} F(P) - \sum_{i=0}^{n-1} P^{\alpha-i-1} D^i f(\tau) \mid_{t=0} \tag{1.22}$$

Définition de Grünwald-Letnikov : Le but de cette technique est d'étendre la définition conventionnelle du dérivé d'ordre entier d'une fonction à des ordres dérivés arbitraires. La formulation de Grünwald convient mieux aux calculs de dérivation fractionnée numérique. En effet, en commençant par la première dérivée et un intervalle d'échantillon de h :

$$D^1 f(t) = \lim_{h \to 0} \frac{f(t) - f(t-h)}{h} \tag{1.23}$$

La dérivé seconde est :

$$D^2 f(t) = \lim_{h \to 0} \frac{f(t) - 2f(t-h) + f(t-2h)}{h^2} \tag{1.24}$$

Ce qui suit donne le premier niveau de généralisation à un ordre entier n :

$$D^n f(t) = \lim_{h\to 0} \frac{1}{h^n} \sum_{j=0}^{n} (-1)^j \binom{n}{j} f(t - jh) \tag{1.25}$$

La notation $\binom{n}{j}$ désigne la combinaison des éléments j entre n, où n est un entier. Pour les valeurs fractionnaires α, L'équation (1.25) s'écrit comme suit, qui est la définition de Grünwald [22] :

$$D_t^\alpha f(t) = \lim_{h\to 0} \frac{1}{h^\alpha} \sum_{j=0}^{\frac{t-t_0}{h}} (-1)^j \binom{\alpha}{j} f(t - jh) \tag{1.26}$$

Le symbole $\binom{\alpha}{j}$ dénote le binôme de Newton étendu aux ordres réels :

$$\binom{\alpha}{j} = \frac{\Gamma(\alpha + 1)}{j!\Gamma(\alpha - j + 1)} \tag{1.27}$$

1.2.3 Quelques propriétés de l'intégration et de la dérivation d'ordre fractionnaire :

Les principaux attributs des opérateurs fractionnaires sont les suivants :

— Si f(t) est une fonction de t, alors $D^\alpha f(t)$, qui est son dérivé d'ordre fractionnaire, est une fonction analytique de t et α .

— L'opération$D^\alpha f(t)$ donne le même résultat que la différenciation d'ordre entier standard n pour $\alpha = n$.

— L'opération $D^\alpha f(t)$ est l'opération d'identité pour $\alpha = 0$, c'est-à-dire Df(t)=f (t).

— La différenciation et l'intégration des ordres fractionnaires sont des processus linéaires : $D^\alpha(a_1 f_1(t) + a_2 f_2(t)) = D^\alpha a_1 f_1(t) + D^\alpha a_2 f_2(t)$

— La loi additive d'index $D^\alpha D^\beta f(t) = D^\beta D^\alpha f(t) = D^{\alpha+\beta} f(t)$

— La dérivée d'ordre fractionnaire commute avec la dérivée d'ordre entier : $\frac{d^n}{dt^n}(D_t^\alpha f(t)) = D_t^\alpha(\frac{d^n}{dt^n} f(t)) = D_t^{\alpha+n} f(t)$ Avec la condition $f^k(\alpha) = 0$.

1.3 Généralités sur les systèmes chaotiques

Les travaux d'Henri Poincaré, à la fin du XIXe siècle, sont à l'origine de l'idée des systèmes chaotiques [25]. Poincaré faisait des recherches sur le problème des trois corps, un système physique simple qui comprend le mouvement de trois corps célestes interagissant entre eux par gravité. Poincaré a découvert que le comportement de ce système était extrêmement dépendant des conditions initiales et ne se prêtait pas à la prédiction à long terme . Le mathématicien et

météorologue Edward Lorenz a développé l'idée des systèmes chaotiques au 20ème siècle tout en recherchant le comportement des modèles météorologiques [7]. Lorenz a constaté que de modestes variations dans les conditions initiales d'un modèle météorologique pourraient avoir une incidence importante sur la capacité du modèle à prévoir les tendances météorologiques futures. Grâce à ses recherches, la théorie de « l'effet papillon », qui renvoie à la notion que des changements modestes dans les conditions initiales peuvent avoir des conséquences importantes et imprévues sur le comportement d'un système chaotique, a été développée. Depuis lors, l'étude des systèmes chaotiques est devenue un domaine de recherche majeur dans un large éventail de domaines, y compris les mathématiques, la physique, l'économie et la biologie. L'étude des systèmes chaotiques a également conduit au développement des nouvelles techniques pour comprendre et prédire le comportement des systèmes complexes.

Donc, Un système chaotique est un système qui présente un comportement apparemment aléatoire et imprévisible qui est sensible aux conditions initiales. Cela signifie que de petites différences dans les conditions initiales du système peuvent conduire à des résultats très différents au fil du temps. Nous développerons plus en détail une classification et quelques propriétés de base des systèmes chaotiques afin de mieux comprendre leur comportement chaotique et les motivations de leur utilisation dans notre thèse.

1.3.1 Caractérisation du comportement chaotique

En général, les systèmes non linéaires peuvent être caractérisés à partir d'observations effectuées à l'aide des techniques du domaine de la dynamique non linéaire, comme : le diagramme de bifurcation, l'espace de phases et outils mathématiques comme les exposants de Lyapunov.

1.3.1.1 Le diagramme de bifurcation

Un diagramme de bifurcation est une représentation graphique du comportement d'un système en fonction d'un paramètre de contrôle changeant. Généralement, le graphique montre comment le système change lorsque le paramètre de contrôle est modifié, y compris les bifurcations ou autres changements qualitatifs qui se produisent. Les bifurcations sont des points auxquels le comportement du système change de manière significative, tels que l'apparition de nouveaux points fixes ou la perte de stabilité des points fixes existants. Le diagramme de bifurcation peut aider à comprendre le comportement général du système et identifier les régions de l'espace de paramètre où diverses formes de comportement se produisent. La figure 1.1 est un exemple de diagramme de bifurcation de la carte logistique. il se présente mathématiquement comme suit [26] :

$$x_{n+1} = \rho x_n(1 - x_n) \tag{1.28}$$

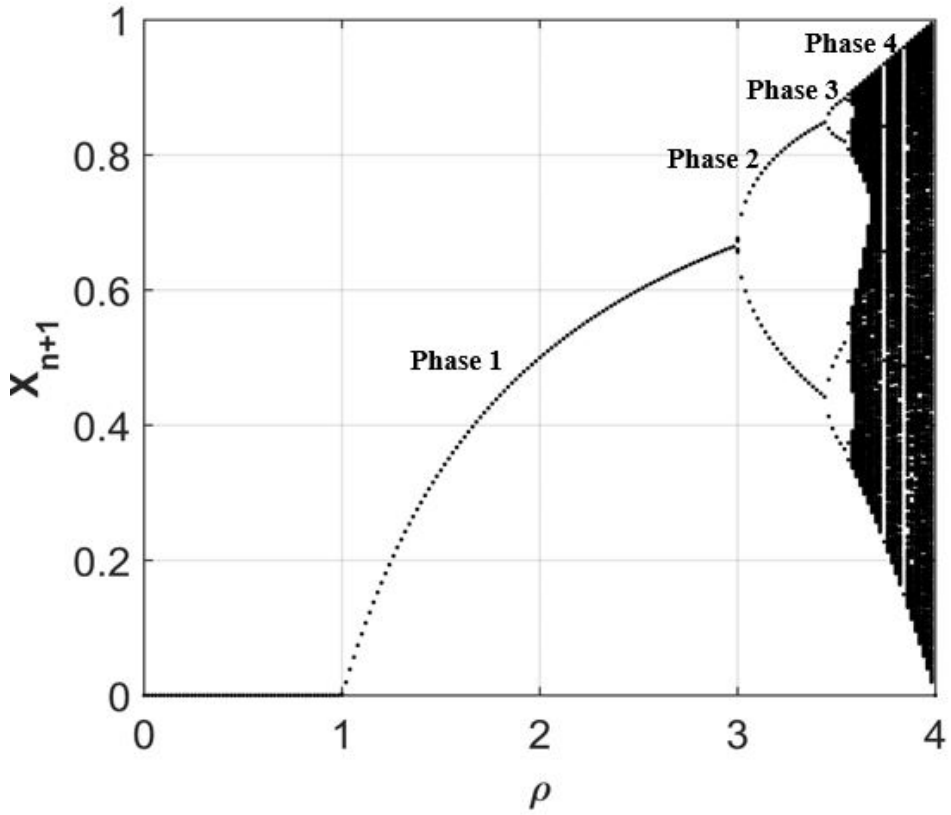


FIG. 1.1 *Diagramme de bifurcation de la carte logistique*

Ou ρ représente le paramètre de contrôle . Le comportement dynamique de la carte logistique peut être divisé en 4 phases :

— La phase 1 représente un état stable.

— La phase 2 représente l'état périodique.

— La phase 3 représente un doublement de période.

— La phase 4 représente l'état chaotique

1.3.1.2 L'espace de phase

L'espace de phase est un concept mathématique utilisé en physique et dans d'autres sciences pour décrire les états possibles d'un système. C'est un espace mathématique qui combine toutes les variables de position et d'impulsion d'un système en un seul point, appelé point de phase. Ce point représente l'état complet du système à un moment donné, et il peut être utilisé pour étudier la dynamique et le comportement du système au fil du temps. L'ensemble de tous les points de phase possibles est connu comme l'espace de phase du système.

Dans l'espace de phase d'un système chaotique, les états possibles du système sont représentés sous forme de points, appelés points de phase. Ces points peuvent être tracés dans l'espace de phase pour former une trajectoire, qui représente le chemin que le système prend à travers ses

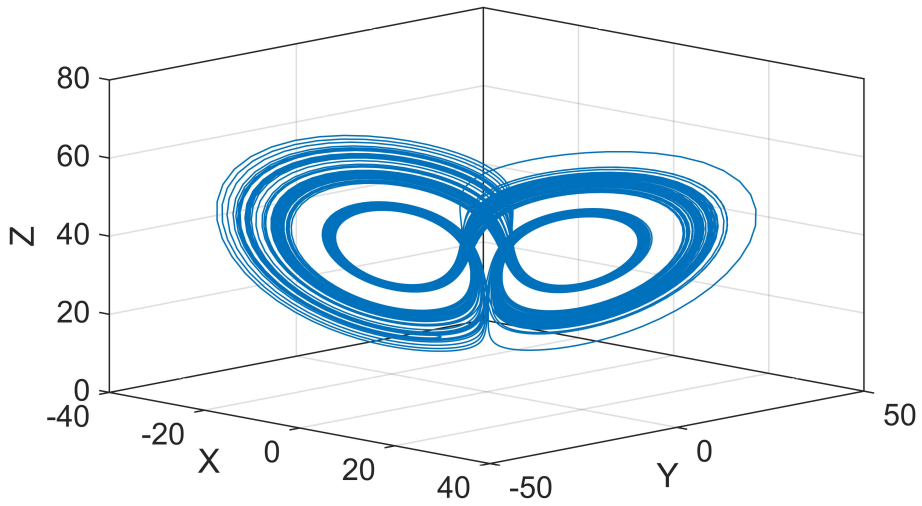


FIG. 1.2 *Plan de phase (x,y,z) du système de chen d'ordre fractionnaire*

états possibles. La trajectoire d'un système chaotique est généralement très complexe et difficile à prévoir, avec de petites différences dans les conditions initiales conduisant à des résultats très différents au fil du temps. La présence d'attracteurs étranges est une propriété importante de l'espace de phase d'un système chaotique. Un attracteur étrange est une structure géométrique générée par la trajectoire des points de phase à travers le temps qui dépeint le comportement à long terme du système. La forme de l'attracteur étrange peut être utilisé pour catégoriser le genre de chaos dans le système ainsi que pour déterminer la stabilité du système. Un exemple d'espace de phase du système de Chen d'ordre fractionnaire est illustré à la figure 1.2.

1.3.1.3 Les exposants de Lyapunov

Dans un système dynamique, l'exposant de Lyapunov mesure la vitesse à laquelle les trajectoires voisines dans l'espace de phase divergent les uns des autres. En d'autres termes, il mesure la sensibilité d'un système à des modifications modestes des conditions initiales. C'est une mesure importante de la stabilité et de la prévisibilité d'un système.

Un ou plusieurs des exposants de Lyapunov pour un système chaotique sont positifs, indiquant que les trajectoires proches divergent exponentiellement les uns des autres. Cela signifie que de petites différences dans les conditions initiales conduiront rapidement à des résultats très différents à long terme, rendant le système imprévisible. En revanche, pour un système stable, tous les exposants de Lyapunov sont négatifs, indiquant que les trajectoires proches convergent l'une vers l'autre.

En pratique, les exposants de Lyapunov sont généralement calculés numériquement en dérivent les équations du système et en surveillant la séparation entre deux trajectoires proches dans le temps. Les exposants de Lyapunov peuvent être calculés pour différentes conditions

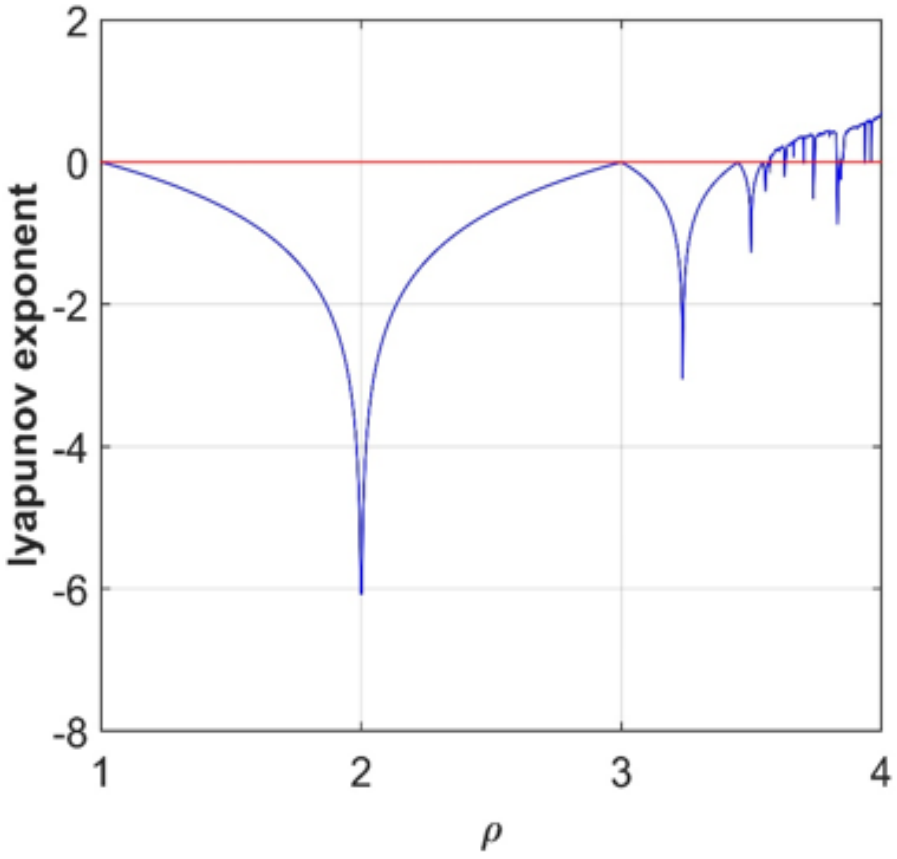


FIG. 1.3 *l'exposant de Lyapunov de la carte logistique*

initiales et différentes directions dans l'espace de phase. Le plus grand exposant de Lyapunov est particulièrement pertinent car il donne la mesure globale de la chaoticité du système. Le calcul de limite suivant donne l'exposant Lyapunov[26] :

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} log(\left|f(x_i)'\right|) \tag{1.29}$$

Ou λ représente l'exposant de Lyapanov. La valeur de l'exposant de Lyapunov montre le degré de chaos du système comme suit :

— $\lambda = 0$ indique une orbite stable.

— $\lambda < 0$ désigne une orbite périodique ou un point fixe

— $\lambda > 0$ désigne une orbite chaotique.

Un exemple de l'exposant de Lyapunov de la carte logistique est illustré à la figure 1.3. Comme le montre la figure 1.3, la simulation donne un exposant positif pour les valeurs du paramètre de contrôle ρ entre 3.5 et 4. Cela implique que la carte logistique montre un comportement chaotique.

1.3.2 Propriétés des systèmes chaotiques

Les systèmes chaotiques sont caractérisés par plusieurs propriétés. Les plus connues sont [27] :

Sensibilité aux condition initial : C'est l'attribut le plus important. Des petites différences dans les conditions initiales peuvent conduire à des résultats très différents dans un système chaotique. Ceci est souvent appelé l'effet papillon, où un petit changement dans les conditions initiales peut conduire à des changements à grande échelle dans le comportement du système.

Non périodicité : Les systèmes chaotiques ne présentent pas de comportement régulier et périodique, et leur comportement à long terme est généralement imprévisible. Cela signifie que les orbites du système sont non répétitives et imprévisibles. Par exemple, un pendule chaotique peut ne pas revenir à un point de départ précis, et son mouvement peut être très irrégulier.

Non-linéarité : De nombreux systèmes chaotiques sont non-linéaires, ce qui signifie que la sortie n'est pas directement proportionnelle à l'entrée. Cette non-linéarité est ce qui rend ces systèmes complexes et difficiles à prévoir.

Ergodique : Les systèmes chaotiques sont typiquement ergodiques, ce qui signifie que le système explore tout son espace de phase au fil du temps. Il est donc difficile de prédire un comportement à long terme, car le système peut passer beaucoup de temps dans une région de l'espace de phase avant de passer à une autre.

Caractère aléatoire : Le comportement des systèmes chaotiques peut sembler aléatoire, même s'il est généré par des équations déterministes. Cela est dû à la sensibilité aux conditions initiales et à la complexité du comportement du système.

Mélange topologique : Les systèmes chaotiques présentent un type de mélange connu sous le nom de mélange topologique, ce qui signifie que les trajectoires dans l'espace de phase deviennent arbitrairement proches les unes des autres, ce qui rend difficile de prédire leur comportement à long terme.

1.3.3 Classification des systèmes chaotiques

Les systèmes chaotiques peuvent être classés selon plusieurs facteurs clés telle que la forme, dimension et l'ordre.

Forme (Discret ou continu) : Les systèmes chaotiques peuvent être discrets ou continus, selon qu'ils sont modélisés à l'aide de pas de temps discrets ou de temps continu les systèmes discrets peuvent présenter un comportement complexe, mais ils pourraient ne pas être en mesure de représenter efficacement certains phénomènes qui sont mieux caractérisés en utilisant le temps continu.

Dimension : Les systèmes chaotiques peuvent également être classés en fonction du nombre de dimensions qu'ils ont :

— système chaotique unidimensionnel :qui peut être décrit par une seule variable ou equation. ils ont moins de paramètres et une structure simple, son temps d'exécution est rapide et le coût de mise en oeuvre est faible.

— Système chaotique multidimensionnel : qui peut être décrit par des multiples variables ou équations et présente un comportement chaotique. En raison de la dimension supplémentaire et de la complexité de la dynamique, ces systèmes sont généralement plus difficiles à analyser et à visualiser que les systèmes unidimensionnels.

Ordre : Les systèmes chaotiques peuvent être classés selon l'ordre de leurs équations. Les systèmes chaotiques d'ordre entier sont régis par des équations différentielles avec des dérivés entiers, tandis que les systèmes chaotiques d'ordre fractionnaires sont régis par des équations différentielles avec des dérivés fractionnaires. Les systèmes chaotiques d'ordres fractionnaires peuvent présenter des comportements plus complexes et riches que les systèmes d'ordres entiers.

1.4 Les systèmes chaotiques d'ordre fractionnaire

Dans ces parties nous présentons des exemples des systèmes chaotiques d'ordre fractionnaires. Il s'agit des systèmes unidimensional et multidimensionnel d'ordre fractionnaire :

1.4.1 Système unidimensional :

1.4.1.1 La carte logistique d'ordre fractionniare :

La carte logistique est la carte la plus connue qui représente un comportement chaotique, et elle est décrite comme suit :

$$x_{n+1} = \rho x_n(1 - x_n) \tag{1.30}$$

Avec ρ représente le paramètre de contrôle. À partir des équations 1.30 et 1.26, nous obtenons la carte logistique d'ordre fractionnaire :

$$x_{n+1} = x_n + \frac{r^{\alpha}}{\Gamma(1+\alpha)}\rho x_n(1 - x_n) \tag{1.31}$$

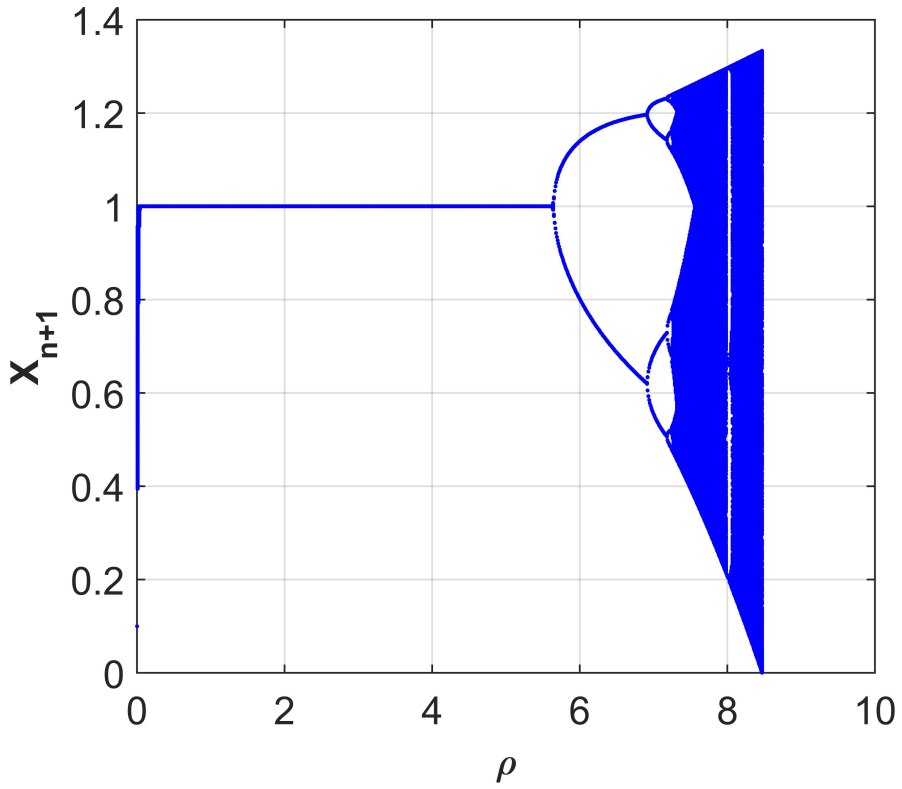


FIG. 1.4 *Diagramme de bifurcation de la carte logistique d'ordre fractionnaire*

Où r est une constante, ρ est le paramètre de contrôle et α est le paramètre d'ordre fractionnaire. Soit ρ compris entre 0 et 9, r et α étant constants à 0,25 et 0,8. l'état initial du système est $x_0 = 0,1$, le diagramme de bifurcation est illustré à la figure 1.4. La zone pointillée indique un comportement chaotique, tandis que la zone vide indique un comportement non chaotique. Comme indiqué, la carte logistique d'ordre fractionnaire se comporte de manière chaotique lorsque $\rho \in [7.3, 8.47]$. Nous utilisons un examen de la composante Lyapunov pour vérifier ces résultats. Le système est chaotique lorsque la composante Lyapunov est positive. Selon l'illustration, la carte logistique d'ordre fractionnaire est chaotique dans $\rho \in [7.3, 8.47]$.

1.4.1.2 Système d'ordre fractionnaire de Puu

Le système de revenu dynamique discret d'ordre entier avec non linéarité cubique d'ordre entier a été créé par Puu et Sushko et il est représenté par l'equation suivant [28] :

$$x_{n+1} = ax_n - (a+1)x^3(n) \tag{1.32}$$

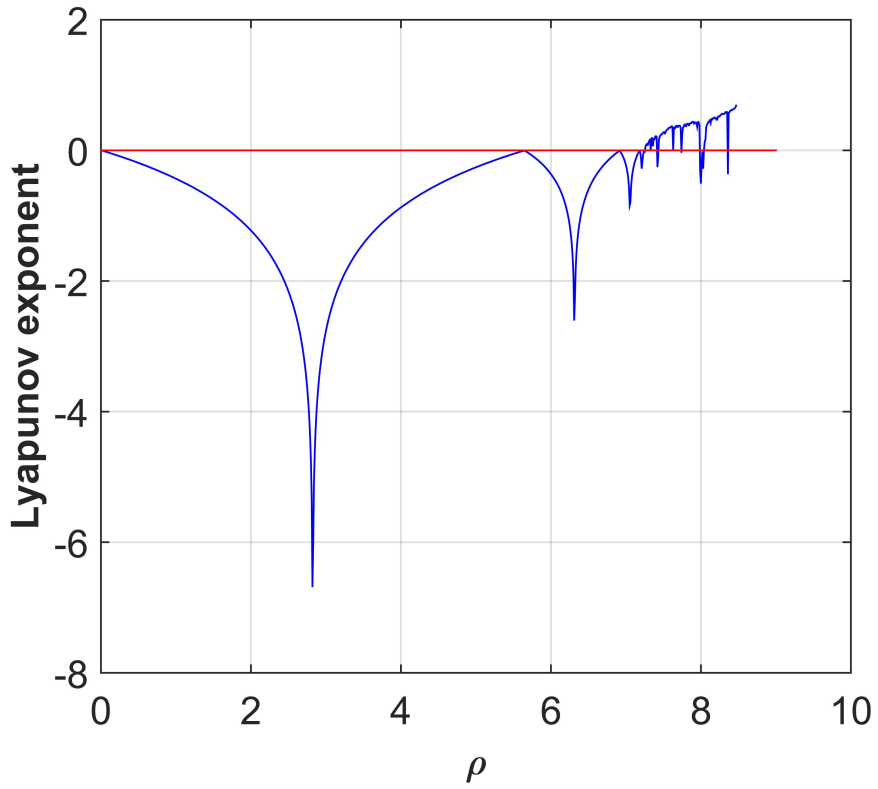


FIG. 1.5 *L'exposant de Lyapunov de la carte logistique d'ordre fractionnaire.*

Ou a est un paramètre réel. Le système Puu de type Caputo d'ordre fractionnaire peut être modélisé par l'équation suivante [28] :

$$\Delta^q x(t) = f(x(k+q-1)) = ax(k+q-1) - (a+1)x^3(k+q-1).k \in \mathbb{N}_{q-1} \tag{1.33}$$

où Δ^q est la différence d'ordre fractionnaire de type Caputo. En résolvant numériquement 1.33 on obtient :

$$x(n) = x(0) + \frac{1}{\Gamma(q)} \sum_{i=1}^{n} \frac{\Gamma(n-i+q)}{\Gamma(n-i+1)} [ax(i-1) - (a+1)x^3(i-1)] \tag{1.34}$$

Soit $q = 0,7$, a varié de 0,6 à 1,4. L'état initial du système puu d'ordre fractionnaire est supposé être 0,1. les résultats de simulation du diagramme de bifurcation et du composant de laypunov sont présentés à la figure 1.6. Le diagramme de bifurcation est représentée par la couleur bleue, tandis que l'exposant de lyapunov est représentée par la couleur rouge. Il démontre que le système puu d'ordre fractionnaire présente un comportement chaotique lorsque $a \in [1.2, 1.4]$.

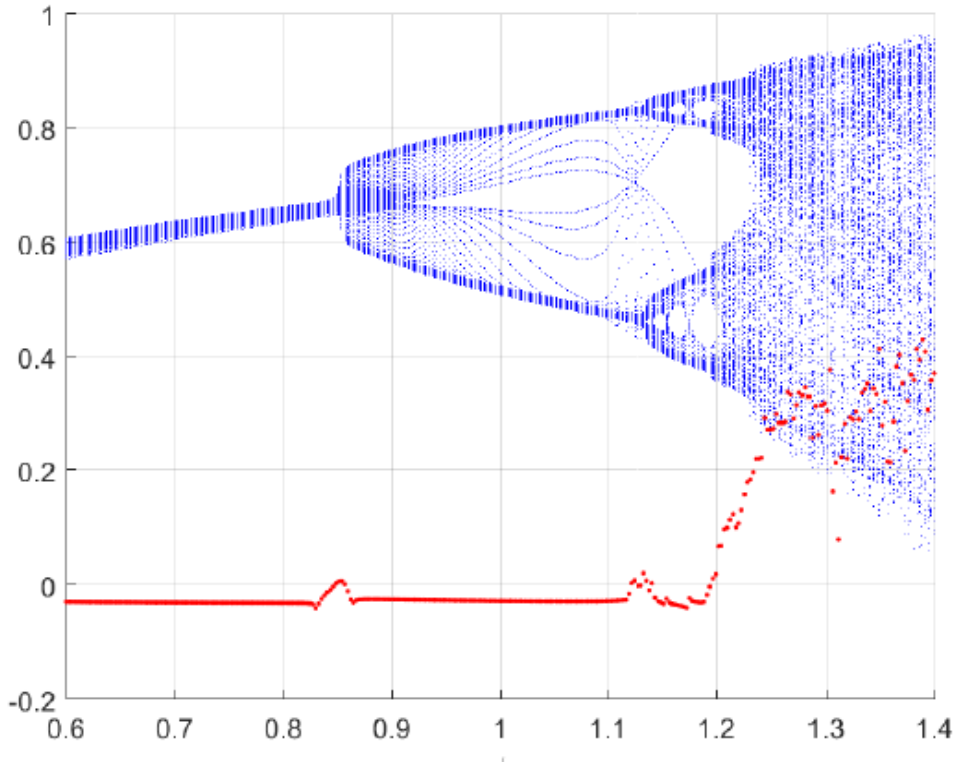


FIG. 1.6 *Diagramme de bifurcation et l'exposant de laypunov du système de puu d'ordre fractionnaire[28]*

1.4.2 Système chaotique multidimensionnel :

1.4.2.1 Carte de Henon d'ordre fractionnaire

La carte du henon est la carte bidimensionnelle la plus connue qui fournit un comportement chaotique. Elle est donnée par l' équation suivante [29] :

$$\begin{cases} x_{n+1} = y_n + 1 - \alpha x_n \\ y_{n+1} = \beta x_n \end{cases} \tag{1.35}$$

où α et β sont des paramètres de contrôle . Nous transformons la carte conventionnelle en une carte fractionnaire en utilisant un calcul fractionnaire discret :

$$\begin{cases} \Delta_{\alpha}^{\mu} x(t) = y(t+\mu-1) + 1 - \alpha x(t+\mu-1)^2 - x(t+\mu-1) \\ \Delta_{\alpha}^{\mu} y(t) = \beta x(t+\mu-1) - y(t+\mu-1) \end{cases} \tag{1.36}$$

La carte de hénon d'ordre fractionnaire est écrite directement en résolvant l'équation1.36

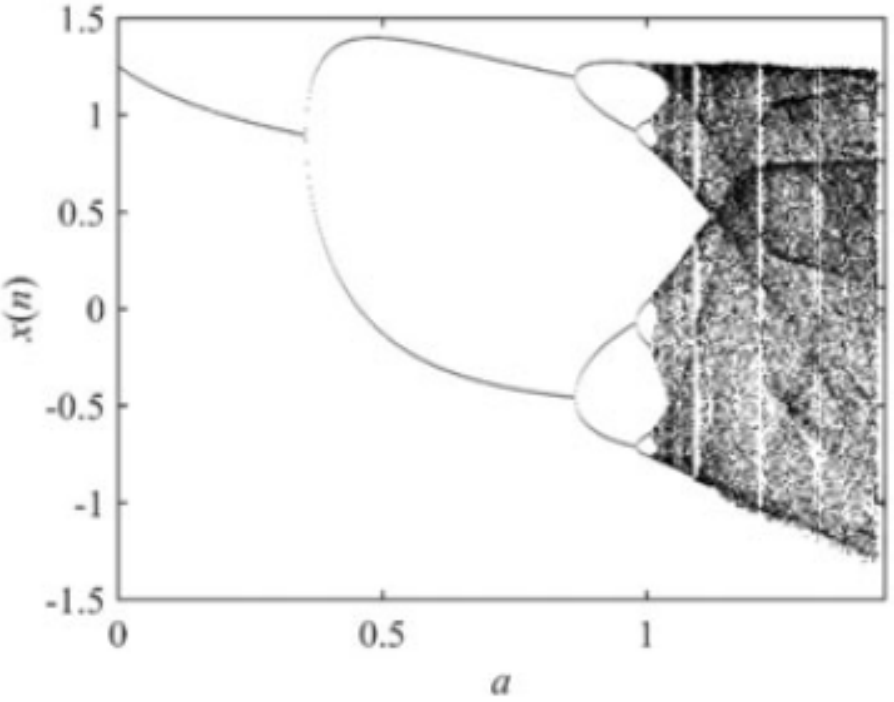


FIG. 1.7 *diagramme de bifurcation de la carte henon fractionnaire[29]*

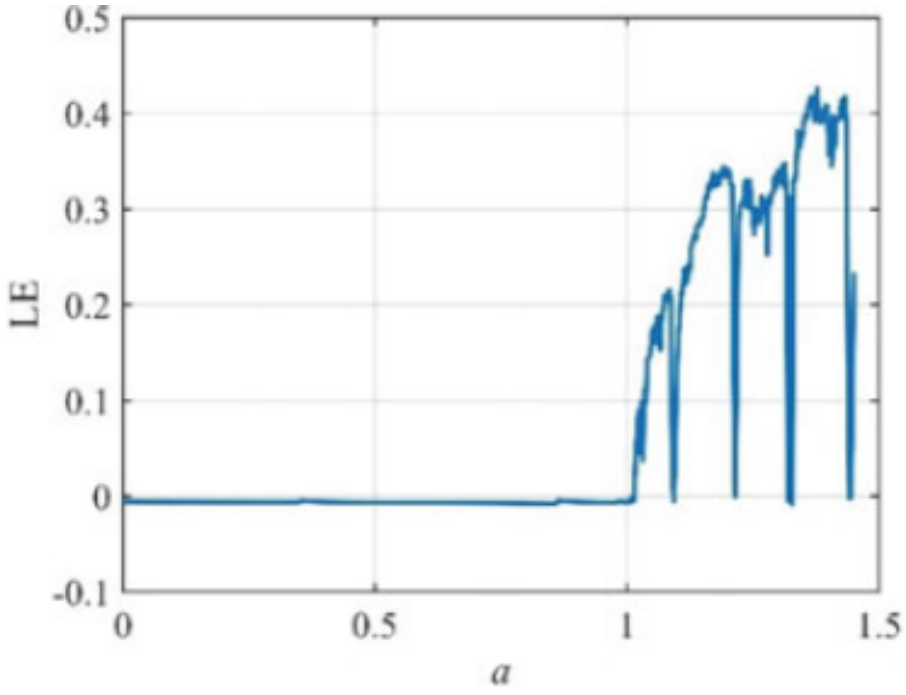


FIG. 1.8 *l'exposant lyapunov de la carte henon fractionnaire [29].*

comme suit [29] :

$$\begin{cases} x_{n+1} = x(\alpha) + \frac{1}{\Gamma(\mu)} \sum_{j-1}^{n} \frac{\Gamma(n-j+\mu)}{\Gamma(n-i+1)} [y_n + 1 - \alpha x_n^2 - x_n] \\ y_{n+1} = y(\alpha) + \frac{1}{\Gamma(\mu)} \sum_{j-1}^{n} \frac{\Gamma(n-j+\mu)}{\Gamma(n-i+1)} [\beta x_n - y_n] \end{cases} \tag{1.37}$$

Le diagramme de bifurcation et le composant Lyapunov de la carte henon d'ordre fractionnaire sont représentés dans les figures 1.7 et 1.8, respectivement. Les conditions initiales de $x(0)$ et $y(0)$ sont égales à -0,3 et 0,2 respectivement, le paramètre d'ordre fractionnaire $\mu = 0.9$, le paramètre de contrôle β =0.2 et α varié de 0 à 1,5. La carte henon d'ordre fractionnare agit de façon chaotique lorsque α est entre 1 et 1.5.

1.4.2.2 Système Chen d'ordre fractionnaire

Le système de chen est un système dynamique tridimensionnel continu non linéaire et autonome. Il est modélisé par la dérivé fractionnaire de Caputo, comme suit [8] :

$$\begin{cases} D^{\alpha} x = a(y - x) \\ D^{\beta} y = (c - a)x - xz + cy \\ D^{\gamma} z = xy - bz \end{cases} \tag{1.38}$$

Où $D^{(\alpha,\beta,\gamma)}$ est l'opérateur d'ordre différentiel du Caputo. a, b et c sont les paramètres du système . L'exposant de lyapunov positif est une propriété cruciale pour démontrer le comportement chaotique du système. Par conséquent, l'exposant de lyapunov et le diagramme de bifurcation du système de chen d'ordre fractionnaire sont montrés dans les figures 1.9 et 1.10. Comme nous pouvons le voir sur les figures 1.9 et 1.10 et lorsque nous fixons $\alpha = \beta = 1, \gamma = 0.9$, b=3 et c=28, et varions a, nous pouvons constater que le système peut présenter des comportements chaotiques lorsqu'un $a \in [34.1, 43]$.

1.4.2.3 Système de Lorenz d'ordre fractionnaire

Un autre exemple des systèmes chaotiques tridimensionnels est le système de Lorenz d'ordre fractionnaire, il est présenté par l'equation suivante [30] :

$$\begin{cases} D^{q} x_1 = a(x_2 - x_1) \\ D^{q} x_2 = c x_1 - x_1 x_3 + d x_3 \\ D^{q} x_3 = x_1 x_2 - b x_3 \end{cases} \tag{1.39}$$

où q est l'ordre dérivé fractionnaire et a, b, c et d sont les paramètres du système. Les figures 1.11 et 1.12 montrent le diagramme de bifurcation et l'exposant de Lyapunov du système de

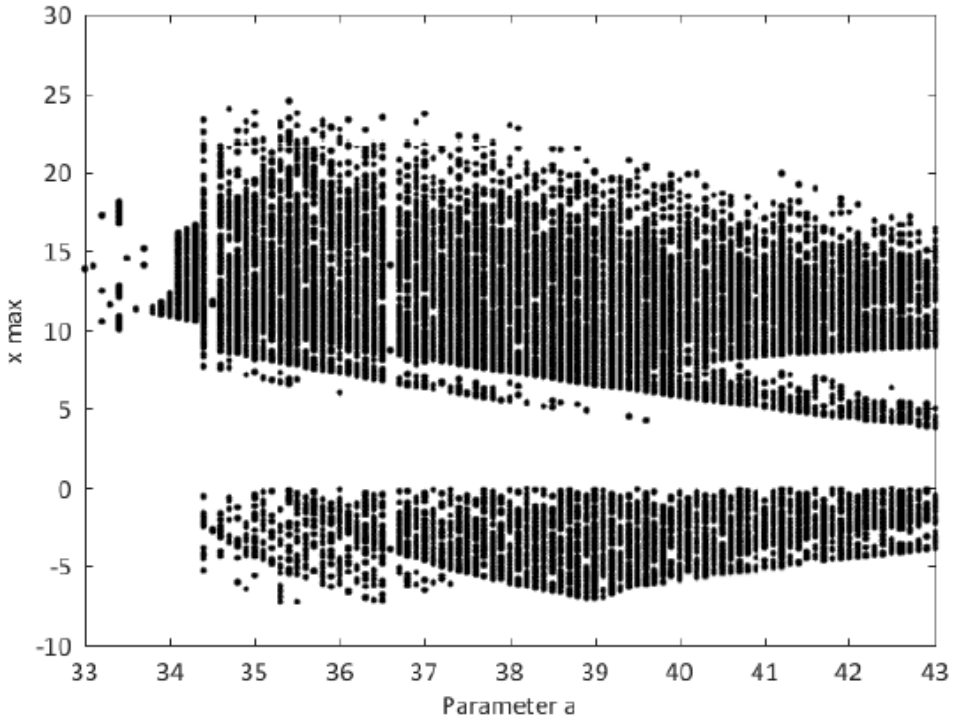


FIG. 1.9 *Diagramme de bifurcation de système de chen d'ordre fractionnaire [8]*

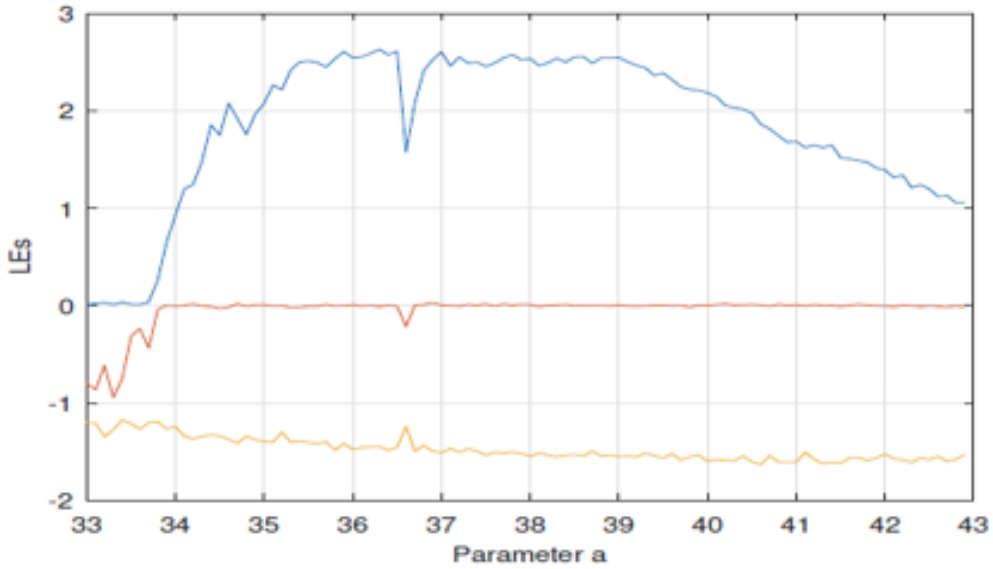


FIG. 1.10 *l'exposant de lyapunov de système de chen d'ordre fractionnaire[8]*

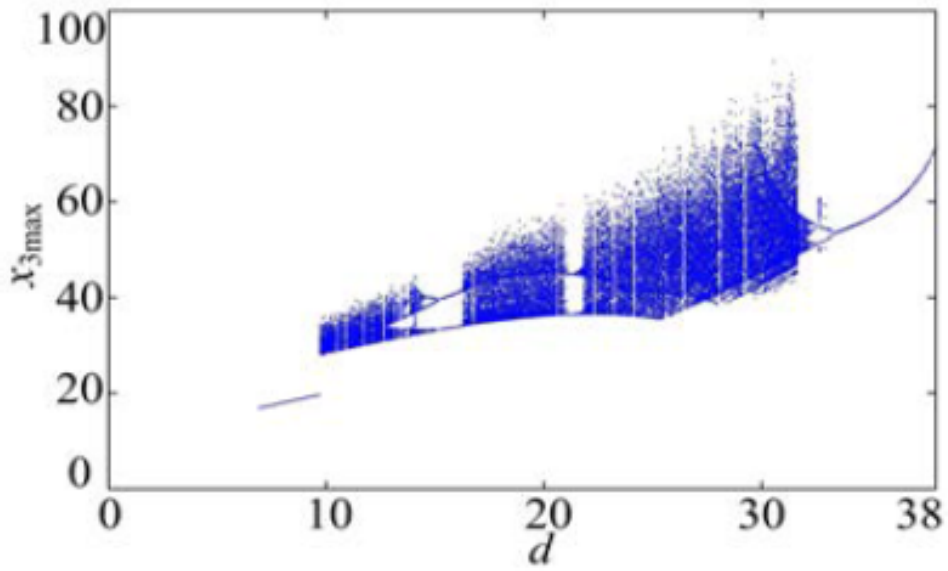


FIG. 1.11 *Diagramme de bifurcation du système de lorenz fractionniare[30]*

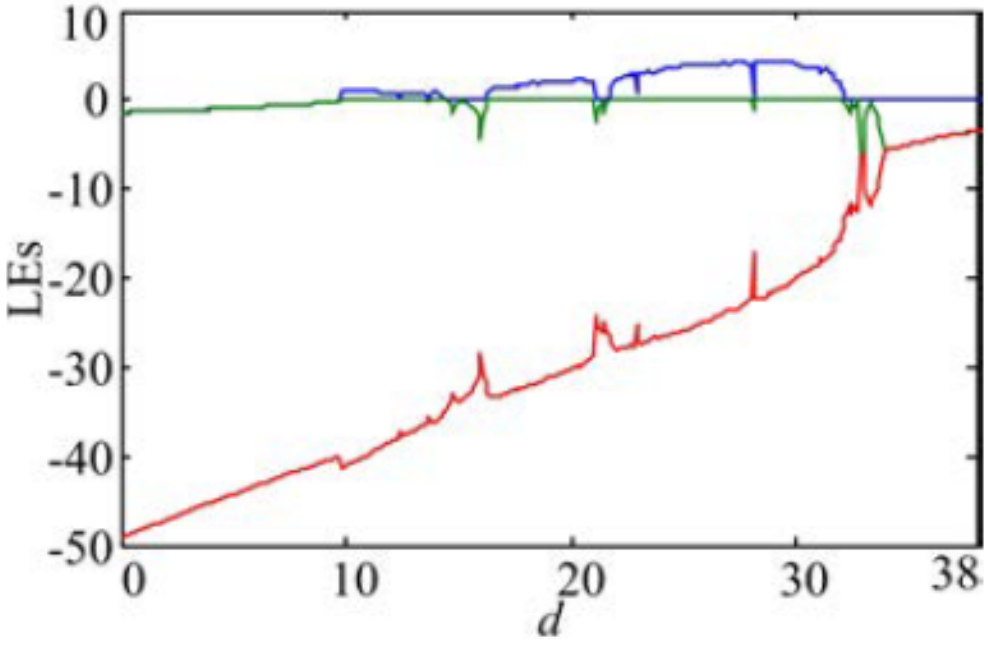


FIG. 1.12 *l'exposant de lyapunov du système de lorenz fractionnaire[30]*

Lorenz fractionnaire. Lorsque en choisissant les paramètres de contrôle a=40, b=3, c=10 , le paramètre d'ordre fractionnaire q= 0,98 et en faisant varier d. le système de lorenz fractionnaire se comporte de manière chaotique lorsque $d \in [9.8, 32.1]$.

1.5 Conclusion

Dans ce chapitre, nous avons couvert les fondamentaux ainsi que les outils mathématiques nécessaires pour étudier les systèmes chaotiques d'ordre fractionnaire. Nous avons couvert plusieurs concepts fondamentaux dans le calcul fractionnaire, tels que les fonctions Gamma Euler et Mittag-Leffler. Juste après, un état de l'art sur la théorie du chaos et les caractéristiques fondamentales des systèmes chaotiques a été introduite. Nous avons conclu ce chapitre avec quelques exemples des systèmes chaotiques d'ordre fractionnaire.

Chapitre 2

Les notions fondamentales de la cryptographie

Sommaire

2.1 Introduction

La transmission de l'information par les médias au moyen des divers réseaux de communication est un processus essentiel pour les entreprises, les organisations et les particuliers. Il communique avec les clients, les employés, les partenaires et les membres de la famille. Toutefois, la sécurité des données transmises est essentielle, car elles peuvent être interceptées et modifiées par des personnes malveillantes. Par conséquent, il est essentiel de mettre en oeuvre des mesures de sécurité pour protéger les données lorsqu'elles sont transmises par les médias sur divers réseaux de communication. La pratique de la communication sécurisée, y compris les techniques et les principes utilisés pour sécuriser les données et l'information, est connue sous le nom de cryptographie. Il comprend des méthodes comme le cryptage, les signatures numériques et l'échange sécurisé de clés pour protéger la confidentialité, l'intégrité et l'authenticité des données. Ce chapitre fournira un aperçu de la cryptographie et de cryptage des images, y compris les concepts de base utilisés dans ce domaine, ainsi que les principes de la cryptanalyse, les techniques utilisées, la génération et la gestion des clés. Nous discutons également des techniques utilisées pour analyser et évaluer les algorithmes de cryptage.

2.2 Concepts de base

La cryptographie est utilisée pour sécuriser les images. En fait, certains concepts cryptographiques fondamentaux sont utilisés comme blocs de construction pour les applications de sécurité des images [31]. Pour une meilleure compréhension des problèmes de sécurité des images, un aperçu de la cryptographie est présenté.

2.2.1 Cryptologie

La cryptologie est une combinaison des mots grecs cryptos (secret) et logy (science). En fait, il est la science du secret et ne peut être considéré comme tel pour une courte période de temps. Il comprend la cryptographie et la cryptanalyse [32].

2.2.1.1 Cryptographie

La cryptographie est la science de l'écriture secrète où il inclut des mécanismes pour cacher le contenu des données. Elle convertit des données telles que des messages, des images numériques et des fichiers audio en données obscures et incompréhensibles appelées données cryptées. Personne ne peut la comprendre, sauf l'expéditeur et le destinataire. Le processus de conversion du texte brut en texte chiffré est connu sous le nom de cryptage, tandis que l'opération inverse, convertir le texte chiffré en texte brut, est connu sous le nom de déchiffrement. La cryptographie est donc l'ensemble des techniques et des méthodes utilisées pour assurer

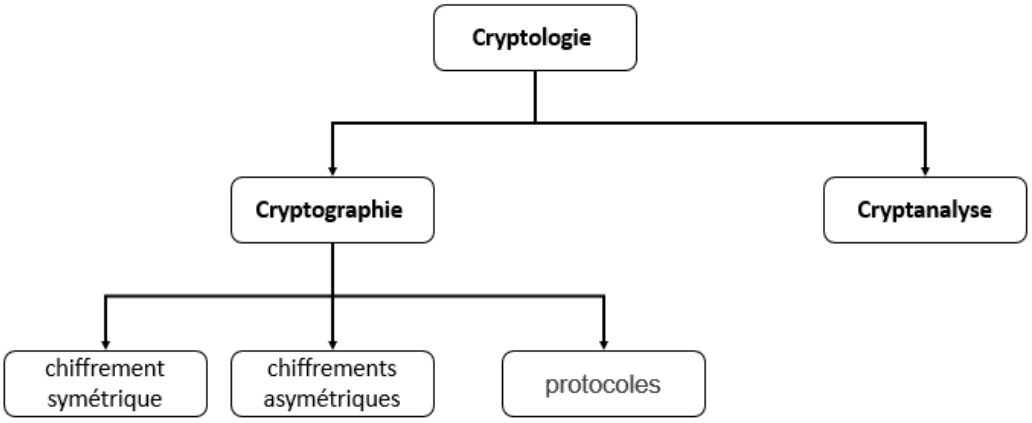


FIG. 2.1 *Aperçu du domaine de la cryptologie*

l'intégrité, la confidentialité et l'authenticité des données transmises. Il crypte les données à l'aide des algorithmes mathématiques, le rendant illisible à quiconque n'a pas la clé de déchiffrement.

2.2.1.2 Cryptanalyse

La cryptanalyse est l'étude des moyens d'obtenir les faiblesses des systèmes de cryptage et d'obtenir le contenu des messages cryptés sans accès à la clé secrète. C'est le processus de briser le système de cryptage pour obtenir le message original sans avoir besoin de la clé de cryptage. Le processus consistant à tenter de comprendre un message crypté est appelé une attaque. La sécurité d'un cryptosystème doit être continuellement évaluée et mise à jour pour assurer sa résistance contre toute attaque cryptanalytique connue, à mesure que la technologie et les méthodes de cryptage progressent avec les méthodes de cryptanalyse.

Il existe diverses formes principales d'attacks cryptanalytiques. Nous mentionnons certaines les plus importantes :

Attaque sur texte chiffré seul : Une attaque par chiffrement seulement est une sorte de cryptanalyse dans laquelle l'attaquant n'a pas des informations supplémentaires que le message crypté (chiffrement). L'objectif de l'attaquant est de déduire le message en clair ou la clé utilisée pour le chiffrement. Parce que le message crypté ne contient aucune information directe sur le message original ou la clé, ce genre d'attaque est difficile. Certaines failles dans la méthode de cryptage ou d'implémentation, cependant, peuvent être exploitées pour identifier la clé ou le message original. Une attaque par force brute est une forme d'attaque par texte chiffré seul. Il est basé sur une recherche de clé exhaustive, et il devrait être informatiquement irréalisable pour les cryptosystèmes bien conçus. La figure 2.2 illustre cette attaque.

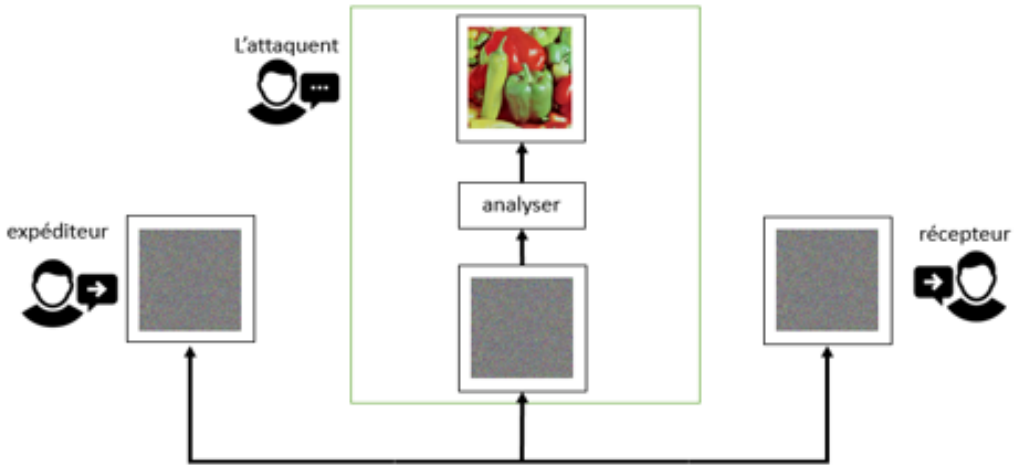


FIG. 2.2 *Attaque sur texte chiffré seul*

Attaque à texte clair connu : C'est une forme d'attaque d'analyse cryptographique dans laquelle l'attaquant possède des échantillons de messages en clair et chiffrées[33] Cette attaque est considérée comme un danger majeur en raison de la capacité de l'attaquant d'identifier des informations secrètes telles que la clé de chiffrement et de récupérer des communications chiffrées à l'aide de cette clé[33]. Ce type d'attaque est illustré à la figure 2.2.

Attaque texte clair choisi (CPA) : Un adversaire peut essentiellement alimenter le texte en clair sélectionné dans la boîte noire, qui comprend la technique de chiffrement et la clé de chiffrement. Le texte chiffré correspondant est fourni par la boîte noire, et l'adversaire peut utiliser les informations recueillies sur les paires text en claire -text chiffré pour découvrir des termes inconnus tel que la clé secrete[34].

Attaque texte chiffré choisi : Est une forme d'attaque dans laquelle l'attaquant a la capacité de déchiffrer des textes chiffrés sélectionnés, cela peut fournir des informations sur la clé secrète utilisée dans le processus de chiffrement, permettant à l'attaquant de déchiffrer entièrement le texte chiffré. Dans ce cas, l'attaquant examine les paires de texte chiffré et de texte en clair collectées [34] . Elle est montrée dans la figure 2.5

2.2.2 Le but de la cryptographie

La cryptographie est l'étude des techniques mathématiques utilisées pour atteindre des objectifs tels que la confidentialité, l'authentification, la non-répudiation et l'intégrité des données afin d'assurer la sécurité des communications [35] :

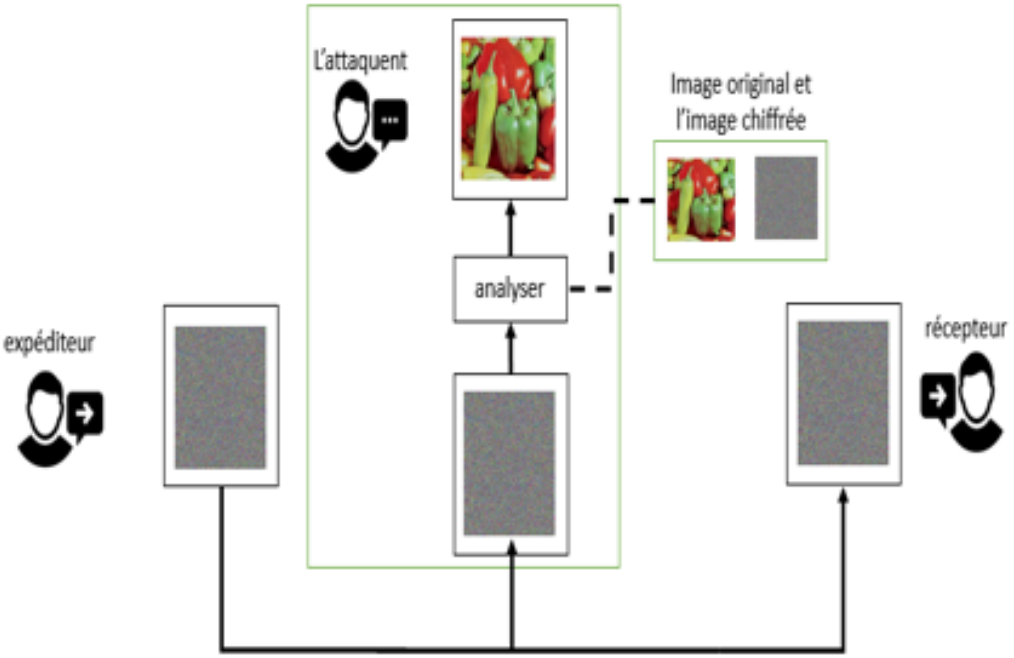


FIG. 2.3 *Diagramme d'attaque connu en clair*

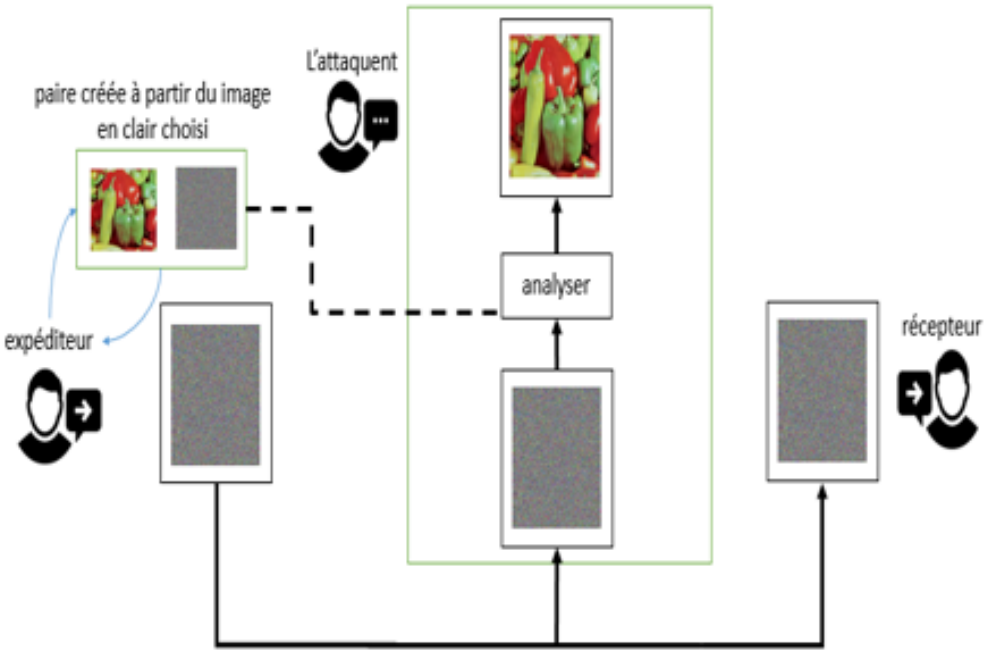


FIG. 2.4 *Diagramme d'attaque texte clair choisi*

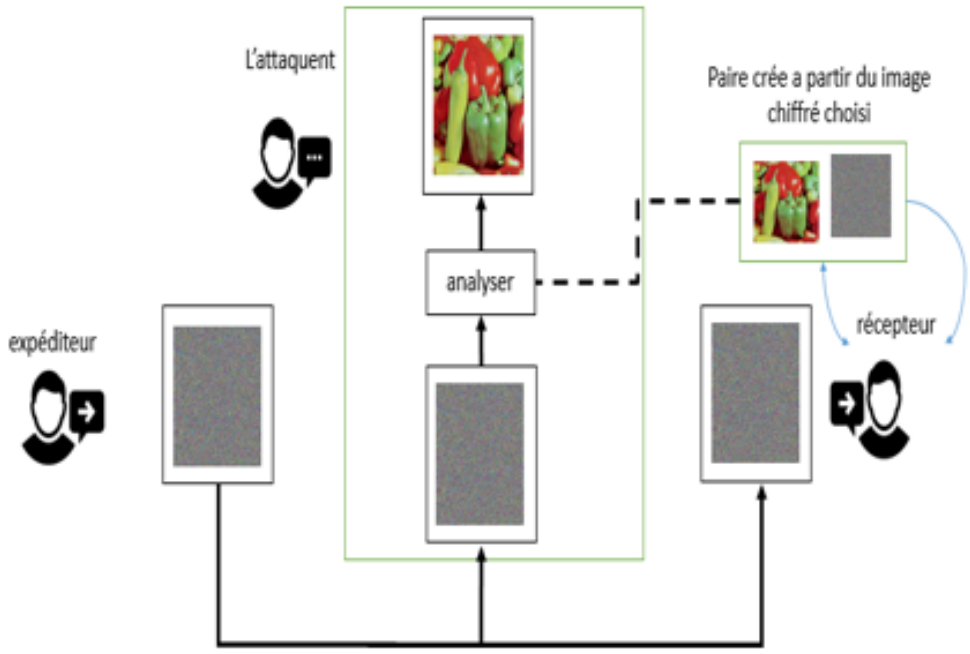


FIG. 2.5 *Diagramme d'attaque texte clair choisi*

2.2.2.1 Confidentialité

C'est un objectif fondamental de la cryptographie qui a toujours été abordé et appliqué tout au long de l'histoire de l'activité cryptographique. Il désigne la protection de l'information contre tout accès non autorisé. Un interlocuteur indésirable, appelé opposant, ne doit pas avoir accès au contenu de la communication.

2.2.2.2 L'authentification

L'authentification est la vérification de l'identité de l'utilisateur pour s'assurer qu'il n'y a pas de vol d'identité. L'authentification des entités et l'authentification des messages sont les deux types de mécanismes d'authentification. L'authentification de l'entité est la procédure par laquelle une partie est informée de l'identification d'une seconde partie s'engageant dans un protocole et que la seconde a réellement participé juste avant l'acquisition des preuves. L'authentification des messages est synonyme d'authentification de l'origine des données. Il assure l'intégrité des données et la vérification de l'origine des données en ce qui concerne la source du message original, mais pas l'unicité ou l'actualité

2.2.2.3 La non-répudiation

La non-répudiation est une technique pour prouver qu'une communication a été transmise par l'expéditeur et reçue par le destinataire. Par conséquent, l'expéditeur ne peut pas prétendre

qu'il n'a pas envoyé le message ou signé certains renseignements numériques, et le destinataire ne peut pas refuser de le recevoir.

2.2.2.4 L'intégrité

Le destinataire doit être en mesure de confirmer que le message n'a pas été altéré lors de la transmission. Un troisième utilisateurs doit être incapable de remplacer un message authentique par un message frauduleux. Il garantit que l'information n'a pas été modifiée de façon illégale. Si l'information est modifiée, le destinataire et l'éxpiditeur remarquent ce changement.

2.3 Principes fondamentaux des systèmes de chiffrement

Le concept fondamental du chiffrement consiste à modifier les données, y compris les messages, les images et le son, de manière à ce que seuls les destinataires autorisés puissent reconstruire le contenu des données.

La figure 2.6 représente un exemple de chiffrement et de déchiffrement d'une image couleur. D'après ce qui est représenté, l'image plaintext notée P est transformée par une fonction de chiffrement notée E_{cc} en une image ciphertext notée C. L'image plaintext P est convertie en image ciphertext C en utilisant la fonction E_{cc} comme suit :

$$C = E_{cc}(p) \tag{2.1}$$

Où cc est la clé de chiffrement, et E est la fonction de chiffrement. De même, la procédure de déchiffrement est définie comme

$$p = D_{cd}(C) \tag{2.2}$$

cd désigne la clé de déchiffrement, tandis que D désigne la fonction de déchiffrement. La sécurité d'un chiffrement devrait uniquement être basée sur la clé de déchiffrement cd, car un adversaire avec cd peut récupérer l'image plaintext du l'image ciphertext observé.

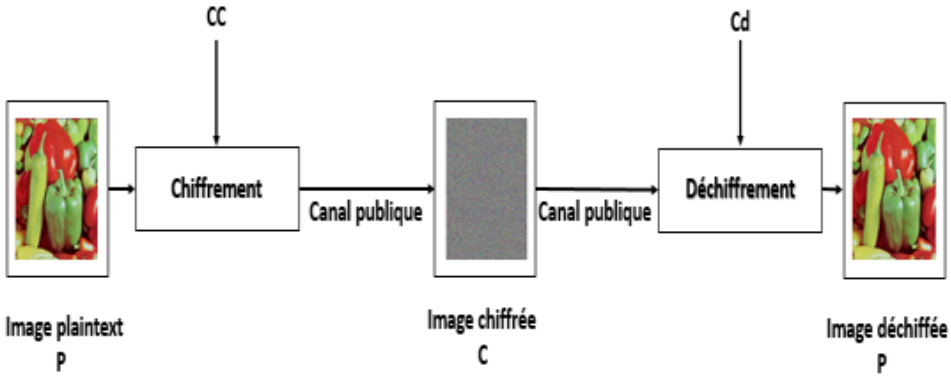


FIG. 2.6 *Chiffrement et déchiffrement d'une image*

2.4 Hypothèse de Kerckhoffs

Le principe de Kerckhoff est un principe cryptographique qui affirme qu'un système cryptographique devrait être sécurisé même si tout ce qui concerne le système est de notoriété publique, sauf la clé. Auguste Kerckhoffs a initialement établi cette notion au XIXe siècle, et elle a depuis été universellement reconnue comme une prémisse fondamentale de la cryptographie moderne [36]. Il publie une liste de six critères comme suit :

— Il doit être pratiquement et mathématiquement impossible de casser le système

— Le système ne devrait pas avoir besoin d'être secret et devrait pouvoir être repris par un adversaire sans inconvénient.

— La clé doit pouvoir être comprise et conservée sans avoir besoin de notes écrites, et elle doit être suffisamment souple pour que les correspondants puissent la mettre à jour ou la modifier au besoin.

— Il doit être propre à la correspondance télégraphique

— La sécurité du système ne doit dépendre que du secret de la clé

— Étant donné les conditions qui exigent son application, il est essentiel que le système soit simple à utiliser, ce qui ne nécessite ni effort mental ni connaissance d'une vaste ensemble de règlements.

2.5 Classification des algorithmes de chiffrement

Les algorithmes de chiffrement peuvent être classés de différentes façons en fonction de divers facteurs : selon les clés, selon la structure du cryptage ou selon le domaine de travail [32]

2.5.1 Classification selon la clé

Selon le type de clé utilisée, les techniques de chiffrement peuvent être classées comme symétriques ou asymétriques

2.5.1.1 Chiffrement symétrique

Pour le chiffrement et le déchiffrement, les techniques de chiffrement symétrique utilisent la même clé (cc=cd) [37]. Cela implique que la clé secrète doit rester privée et accessible à la fois à l'expéditeur et au destinataire [37]. Les techniques de chiffrement symétrique sont rapides et efficaces, mais leur principal inconvénient est l'obligation de partager en toute sécurité la clé secrète. Advanced Encryption Standard (AES), Data Encryption Standard (DES) et Blowfish sont quelques exemples de méthodes de chiffrement symétriques. Un exemple de cryptosystème symétrique est présenté à la figure 2.7.

2.5.1.2 Chiffrement asymétrique

Une paire de clés ($cc \neq cd$) est utilisée pour le chiffrement asymétrique, une pour le chiffrement et une pour le déchiffrement [38]. La clé de déchiffrement est gardée secrète, tandis que la clé de chiffrement est divulguée. Cela permet de communiquer en toute sécurité sans échanger de clés secrètes au préalable [38]. Les techniques cryptographiques asymétriques sont plus lentes et moins efficaces que les algorithmes symétriques, mais elles comprennent des caractéristiques de sécurité supplémentaires comme les signatures numériques et l'échange de clés. RSA, Elliptic Curve Cryptography (ECC) et Diffie-Hellman sont des exemples de méthodes de chiffrement asymétrique. Un exemple de cryptosystème asymétrique est présenté à la figure 2.8. Le tableau 2.1 présente les exigences en matière de chiffrement symétrique et de chiffrement asymétrique.

2.5.2 Classification selon la structure de chiffrement

Les techniques de chiffrement sont catégorisées en chiffrements par blocs et en flux en fonction de leur structure de chiffrement.

2.5.2.1 Chiffrements par blocs

Un chiffrement par bloc est une sorte de méthode de chiffrement à clé symétrique, qui convertit un bloc de données en clair-texte de longueur fixe en bloc de données en texte chiffré de longueur fixe. Pour les chiffrements de blocs courants, la longueur fixe, aussi appelée taille de bloc, est généralement de 64 ou 128 bits. Plus la taille du bloc est grande, plus le chiffrement est sécurisé, mais plus les algorithmes et les dispositifs de chiffrement et de déchiffrement sont compliqués . Les caractéristiques suivantes distinguent les chiffrements de blocs modernes :

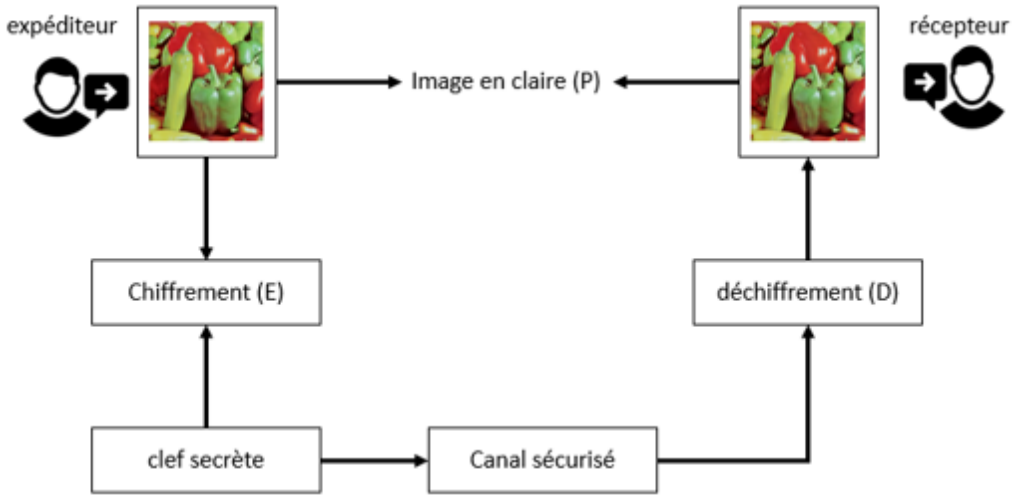


FIG. 2.7 *Chiffrement symétriques*

TABLE 2.1 *Les exigences en matière de chiffrement symétrique et de chiffrement asymétrique*

Chiffrement Symétrique	**Chiffrement Asymétrique**
Le même algorithme et la même clé peuvent être utilisés pour le chiffrement et le déchiffrement.	Avec une paire de clés, un est utilisé pour le chiffrement et un pour le déchiffrement.
L'algorithme et la clé doivent être partagés entre l'expéditeur et le destinataire.	L'expéditeur et le destinataire doivent avoir chacun une des clés appariées.
La clé doit rester cachée.	La clé de déchiffrement doit rester confidentielle.
Si aucune autre information n'est fournie, il doit être difficile ou impossible de déchiffrer un message.	Si aucune autre information n'est fournie, il doit être difficile ou impossible de déchiffrer un message.
La connaissance de la méthode et des échantillons chiffrés doit être insuffisante pour découvrir la clé.	La connaissance de la méthode et des échantillons chiffrés doit être insuffisante pour découvrir la clé.

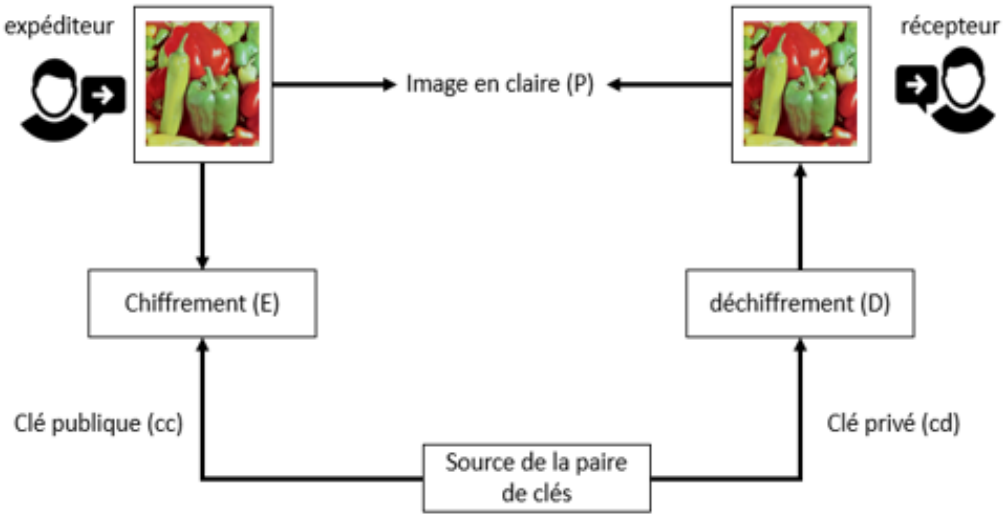


FIG. 2.8 *Chiffrement asymétriques*

— Ils traitent les données dans des blocs de taille fixe de 128 bits ou moins.

— Pour convertir le texte en clair en texte chiffré, ils effectuent une séquence d'opérations mathématiques sur chaque bloc de texte en clair.

— Ils sont idéaux pour crypter d'énormes volumes de données et peuvent crypter de nombreux blocs simultanément.

— L'expéditeur et le destinataire doivent partager la même clé en toute sécurité.

2.5.2.2 Chiffrements par flot

Les chiffrements de flux diffèrent des chiffrements par blocs en ce sens qu'ils chiffrent des unités des données plus petites, parfois juste un bit ou un octet à la fois. En conséquence, ils sont censés être extrêmement rapides, beaucoup plus rapides qu'un chiffrement de bloc normal. En général, un chiffrement de flux crée une série de bits comme une clé avec la même taille que le texte en clair en utilisant un générateur de nombres pseudoaléatoires, et le chiffrement est effectué en combinant le flux de clé avec le texte en clair . Typiquement, la technique XOR bitwise est utilisée pour effectuer le chiffrement, en raison de sa simplicité. Les caractéristiques suivantes distinguent les chiffrements de flux :

— La sécurité du système est déterminée par les caractéristiques du générateur de nombres pseudoaléatoires (PRNG).

— Le PRNG doit être inattendu : étant donné une série de bits de sortie, le bit suivant doit être difficile à anticiper

— Facilité de mise en oeuvre : Comme les chiffrements de flux sont faciles à mettre en oeuvre dans les logiciels ou le matériel, ils constituent un choix populaire pour les applications spécialisées.

— Rapide : Comme les chiffrements de flux peuvent être conçus pour être rapides et efficaces, ils sont idéaux pour chiffrer les flux de données en temps réel.

— Résistant aux attaques : Les chiffrements de flux peuvent être construits pour résister à des agressions spécifiques, telles que les attaques par chiffrement seulement ou les attaques en clair connues.

— Les chiffrements de flux utilisent souvent des clés plus courtes que les chiffrements de bloc, ce qui simplifie la mise en oeuvre et réduit les coûts de traitement.

2.6 Mesures d'évaluation du chiffrement des images

Cette section décrit en detail les mesures de sécurité statistique bien connues et les outils d'évaluation des algorithmes de chiffrement des images.

Les mesures de sécurité statistique bien connues et les outils d'évaluation des algorithmes de chiffrement des images sont décrite en detail par cette section .

2.6.1 Analyse de l'espace de la clé de chiffrement

L'espace clé d'un algorithme de chiffrement/déchiffrement est la somme des nombreuses clés qui peuvent être utilisées dans l'opération de chiffrement/déchiffrement. Lorsque l'espace de clé principal est vaste, cela signifie qu'il existe de nombreuses possibilités pour la clé . Il est donc difficile pour l'attaquant de découvrir la bonne clé. Par conséquent, la taille de l'espace de clé est un facteur important dans l'évaluation de la durabilité et de la sécurité du système de chiffrement contre diverses attaques telles que la force brute, l'attaque en text clair connue ou l'attaque en text choisi. Selon la littérature, la taille de la clé doit être supérieure à 2^{100} pour offrir un bon niveau de sécurité [1].

2.6.2 Sensibilité à la clé de chiffrement

La sensibilité élevée de la clé de chiffrement est un aspect important d'un système de chiffrement solide et contribue à assurer la sécurité des données chiffrées. L'analyse de sensibilité de la clé est une procédure qui évalue la force d'un système de chiffrement en apportant des petites modifications à l'un des éléments constituants la clé de chiffrement et en évaluant l'impact sur le processus de déchiffrement. Si un petit changement dans la clé fait échouer complètement le déchiffrement, cela est considéré comme un signe positif, ce qui rend le schéma de chiffrement sécurisé. Nous améliorons la précision de cette modification à chaque fois jusqu'à ce que l'image déchiffré apparaisse clairement. Cette limite permettra d'assurer l'exactitude de l'élément qui compose cette clé. L'espace clé de la technique de chiffrement proposé sera déterminé par la précision de tous les facteurs composants de la clé de chiffrement.

2.6.3 L'entropie

La théorie de Shannon définit l'entropie de l'information comme la quantité d'information absorbée ou émise par une source d'information. En cryptographie, il est fréquemment utilisé pour évaluer la sécurité d'un algorithme de chiffrement. L'entropie d'une image chiffrée est déterminée en examinant la distribution de fréquence des pixels de l'image. Une forte technique de chiffrement vise à s'assurer que la probabilité de chaque pixel apparaît presque la même. L'entropie du message chiffré se présente comme suit [39] :

$$H(C) = \sum_{i=0}^{255} pro(C_i) log_2 \frac{1}{pro(C_i)} \tag{2.3}$$

$pro(c_i)$ est le nombre de fois que chaque niveau se produit, et $H(C)$ est l'entropie de l'image cryptée C. Pour une image 8 bits, la valeur d'entropie peut varier de 0 à 8, 0 indiquant une prévisibilité totale et 8 indiquant un caractère aléatoire maximal. D'une manière générale, une plus grande valeur d'entropie dénote un chiffrement plus sécurisé et de meilleurs niveaux de protection pour l'image chiffré. L'analyse d'entropie peut aider à estimer la force d'un système de chiffrement et à découvrir les trous que les attaquants peuvent exploiter.

2.6.4 Le coefficient de corrélation

Le coefficient de corrélation est une mesure statistique utilisée pour montrer la relation linéaire entre deux variables. Dans le chiffrement des images, cette mesure est nécessaire pour évaluer le caractère aléatoire et la sécurité de l'image chiffrée en mesurant la corrélation entre les pixels adjacents. Le faible coefficient de corrélation indique que l'image chiffrée a un degré élevé d'aléatoire et elle est difficile à prédire. Cela signifie que le système de chiffrement est solide et capable de détruire la forte interconnexion des pixels adjacents qui caractérisent les images ordinaires. Cette mesure peut être calculée comme suit[39] :

$$\begin{cases} r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \\ E(x) = \frac{1}{N}\sum_1^N x_i \\ D(x) = \frac{1}{N}\sum_1^N [x_i - E(x)]^2 \\ cov(x,y) = E([x - E(x)][y - E(y))]) \end{cases} \tag{2.4}$$

Où $E(x)$ est l'espérance de x, D (x) est la variance, et N est le nombre total des échantillons, x et y sont les valeurs d'échelle de gris des deux pixels voisins de l'image. La figure 2.9 montre la distribution des pixels voisins dans diverses directions de l'image originale et de l'image chiffrée. Nous voyons que la distribution de l'intensité des pixels de l'image originale est centrée sur la diagonale et elle est fortement corrélée, mais les pixels de l'image chiffrée sont non corrélés et

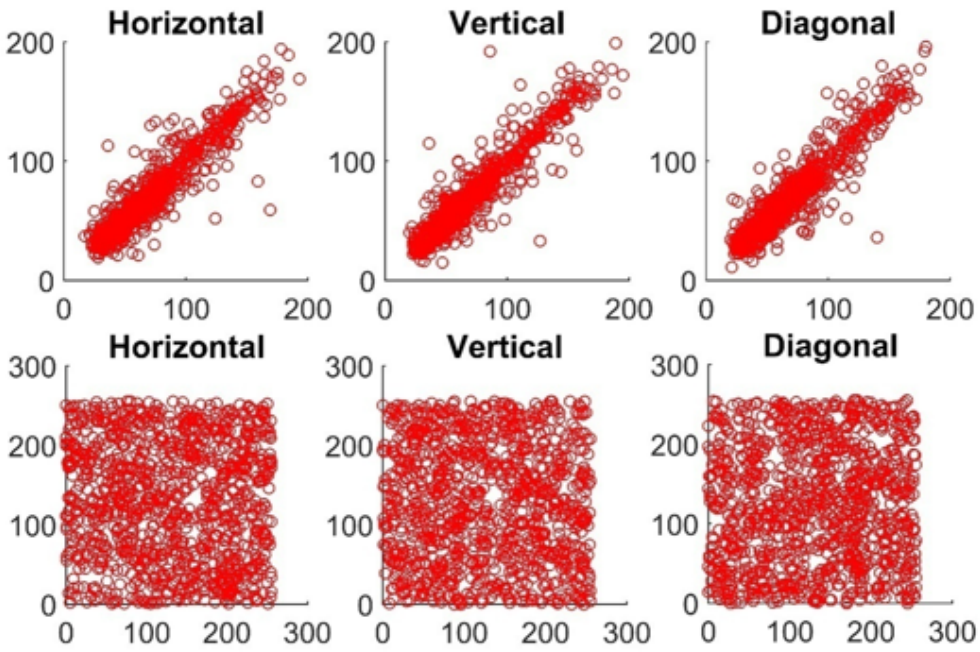


FIG. 2.9 *Distribution des pixels voisins dans différentes directions. La première ligne montre l'image originale ; la deuxième ligne montre l'image chiffrée.*

ils ont une distribution uniforme.

2.6.5 L'histogramme

Un histogramme décrit l'occurrence de chaque niveau de gris dans l'image à l'aide d'un graphique à barres. La valeur du niveau de gris est représentée par l'axe horizontal. Il commence à zéro et remonte jusqu'au nombre de niveaux de gris (255)[32]. Chaque barre verticale reflète le nombre de fois que le niveau de gris correspondant apparaît dans l'image.

L'analyse d'histogramme est une technique souvent utilisée dans le chiffrement des images pour évaluer la sécurité d'une image cryptée en évaluant la distribution des intensités de pixels. L'histogramme de l'image chiffrée devrait avoir deux qualités pour les algorithmes de chiffrement d'image :

— Elle doit être complètement différente de l'histogramme de l'image originale et ne pas révéler d'informations sur l'image originale (histogramme plat).

— Elle doit avoir une distribution uniforme, ce qui implique que chaque valeur d'échelle de gris a la même chance de se produire.

Cependant, si l'histogramme de l'image chiffrée n'est pas plat, il peut exposer des informations sur l'image originale, ce qui rend l'algorithme de chiffrement ouvert à l'attaque. Par exemple, des pics ou des groupes des intensités dans l'histogramme d'une image chiffrée, peuvent démontrer que la stratégie de chiffrement a conservé une partie de la structure de l'image originale, cela

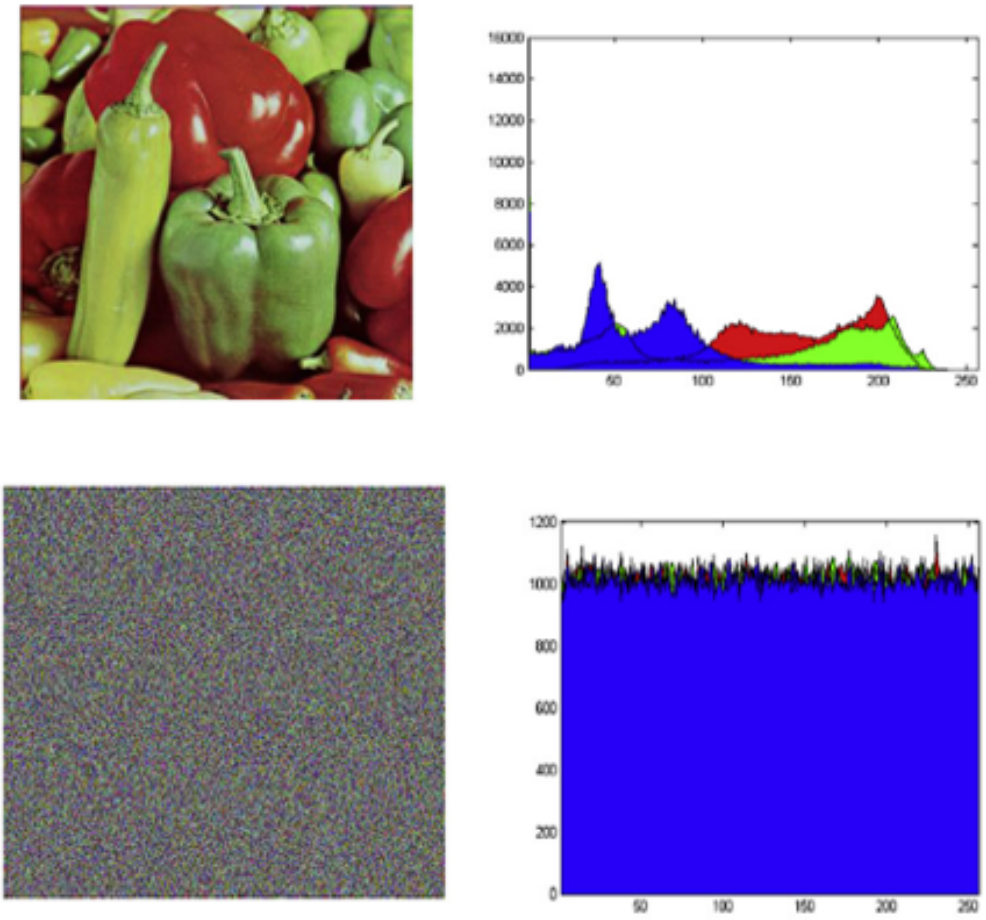


FIG. 2.10 *L'histogramme de l'image originale et de l'image chifrée.*

peut être exploité pour briser l'algorithme de chiffrement. La figure 2.10 illustre l'histogramme de l'image originale et chiffrée. Les résultats montrent clairement que l'histogramme de l'image chiffrée est assez uniforme et significativement différente de l'histogramme de l'image de base, rendant les attaques statistiques impossibles.

2.6.6 Attaque différentielle

Une attaque différentielle est un type d'attaque qui vise à modifier une image standard afin d'obtenir une version chiffrée modifiée. Puis, l'image originale est chiffrée en utilisant le même système de chiffrement. Un attaquant, peut comparer l'image chiffrée et l'image chiffrée modifiée pour voir s'il y a des tendances perceptibles dans les écarts entre les deux. Si la technique de chiffrement est soumise à des attaques différentielles, l'attaquant peut être en mesure de rétroconcevoir la clé de chiffrement et d'acquérir l'accès à l'image originale en utilisant cette connaissance. Le NPCR et l'UACI sont des mesures qui peuvent être utilisées pour évaluer la résilience d'un algorithme de chiffrement aux attaques différentielles [40].

NPCR est une mesure de la quantité de pixels qui changent entre deux images cryptées,

représentée en pourcentage du nombre total de pixels dans l'image. En revanche, l'UACI est une mesure de l'uniformité des changements d'intensité des pixels entre les deux images chiffrées. Elle est déterminée comme la différence absolue moyenne d'intensité entre les pixels correspondants des deux images chiffrées. Ils sont définis comme suit :

$$\begin{cases} NPCR = \frac{1}{n \times m} \sum D(i,j) \times 100\% \\ UACI = \frac{1}{n \times m} \sum \frac{c_1(i,j) - c_2(i,j)}{255} \times 100\% \end{cases} \tag{2.5}$$

Où $c_1(i,j) et c_2(i,j)$ représentent les deux images chiffrées dont le changement de bit correspond à la même image, m et n sont la hauteur et la largeur des images. D(i,j) est déterminé à partir de $c_1(i,j) et c_2(i,j)$ comme suit :

$$D(i,j) = \begin{cases} 0 & c_1(i,j) = c_2(i,j) \\ 1 & c_1(i,j) \neq c_2(i,j) \end{cases} \tag{2.6}$$

Lorsque la valeur de NPCR et UACI est égale à la valeur optimale spécifiée dans la littérature par 96.6% et 33.46% respectivement. Cela signifie que l'algorithme de chiffrement disperse efficacement les changements sur l'image. Ce qui le rend difficile pour l'attaquant d'utiliser des techniques d'attaque différentielle.

2.6.7 Resistance au bruit et aux pertes de données

L'évaluation de la résilience d'un algorithme de chiffrement d'image au bruit et à la perte des données est un élément clé pour établir sa sécurité globale et son applicabilité à un certain cas d'utilisation. Le bruit est défini comme toute modification aléatoire ou indésirable des données qui pourrait survenir au cours du processus de chiffrement ou de transmission, tandis que la perte des données est définie comme la perte d'information dans l'image cryptée en raison de causes telles que la compression des données ou les défaillances de transmission. Une technique de chiffrement d'image devrait être en mesure de résister à ces éléments inhabituels. La figure 2.11 représente la capacité de l'algorithme de chiffrement à résister à la perte des données et la figure 2.12 représente également la capacité de résister au bruit. Si l'image dechiffrée contient la plupart des informations visuelles originales, nous disons que la technologie de chiffrement est puissante et capable de resister à la perte des données et au bruit.

2.6.8 Temps d'exécution

Le coût de la technique de chiffrement d'image suggérée est fortement influencé par la vitesse d'un cryptosystème. Le temps nécessaire pour chiffrer et déchiffer une image est appelé le temps de l'exécution. Plus le temps de l'exécution est court, le cryptage est plus efficace.

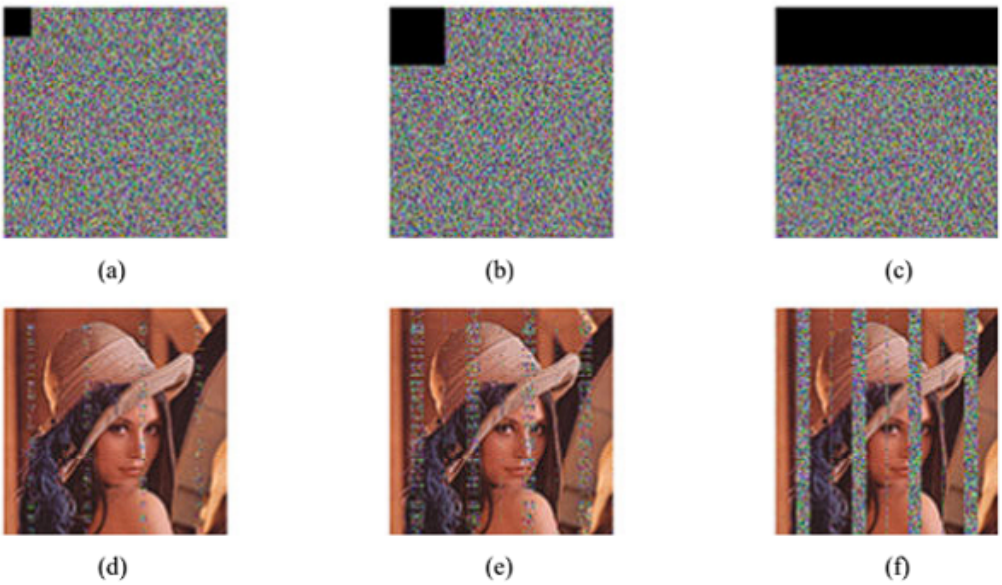


FIG. 2.11 *La capacité de l'algorithme de chiffrement à résister à la perte des données : :(a)* 64×64 *perte des données (b)*128×128*perte des données.(c)* 128×513 *perte des données.(d-f) l'image déchffrée.*

FIG. 2.12 *Processus de décryptage avec nez sel et poivree.*

Le temps d'exécution d'une technique de chiffrement d'image dépend d'un certain nombre de facteurs, y compris la taille de l'image, la complexité de l'algorithme, la capacité de traitement de l'ordinateur ou du dispositif exécutant l'algorithme, et les ressources accessibles au programme.

2.6.9 Test statistique de NIST

Le NIST test est un groupe d'essai statistique pour les générateurs de nombres aléatoires produit par le National Institute of Standards and Technology (NIST) aux États-Unis. La suite comprend une variété de tests statistiques visant à évaluer le caractère aléatoire de l'image chiffrée ou l'imprévisibilité et la qualité des générateurs de nombres aléatoires utilisés pour chiffrer les images. Nous avons utilisé NIST SP800-22, qui composé de 15 tests statistiques[41]. La réussite de chaque test est déterminée en calculant la valeur de P_{value} et en la comparant à un nombre prédéfini appelé α(α égale 0,01). Si les résultats de chaque test répondent à

l'hypothèse$P_{value} > \alpha$, les séquences sont considérées aléatoires. Si P_{value} est égal à 1 pour chaque test, la séquence testée est entièrement aléatoire, mais un P_{value} = 0 indique un caractère non aléatoire. Ensuite, les 15 tests NIST sont fournis[42] :

2.6.9.1 Test de fréquence

Ce test examine la distribution des 1 et des 0 dans la séquence binaire. Ceci est accompli en comptant le nombre de 1 et de 0 et en les comparant à la distribution prédite pour une séquence véritablement aléatoire. Le test détermine si le pourcentage de 1 est proche du 1/2. Voici les étapes du test :

— les 0 et 1 de la séquence sont transformés en 1 et - 1, respectivement.

— faire la somme bit à bit de la sequence.

— Si le total est trop grand (trop 1) ou trop peu (trop 0), la séquence est donc non aléatoire.

2.6.9.2 Test de fréquence par bloc

Ce test utilise le même principe que le test de fréquence, en examinant la proportion des "uns" et des "zéros" dans les sous-séquences de bits de la suite binaire à tester. Dans cet aspect, la séquence binaire sera séparée en blocs de M bits, et nous chercherons à voir si la fréquence de certains est proche de 1/2 dans chaque bloc. Pour un bloc de taille M = 1.

2.6.9.3 Test de somme cumulative

Le but de ce test est d'établir si le total cumulé des bits successifs de la séquence étudiée ajusté à (-1, +1) est extrêmement grand ou très petit, afin de détecter l'existence de quantités substantielles des zéros ou des uns. Ce test peut être appliqué de deux façons. Le premier mode 0 consiste à exécuter la séquence en commençant par le premier bit. Le deuxième mode 1 consiste à exécuter la séquence en commençant à partir du dernier bit.

2.6.9.4 Test de série

Ce test compte le nombre runs dans la séquence binaire, où une runs est définie comme une série de bits identiqués qui est répétée dans une rangée. Ceci est accompli en comptant le nombre de séries de longueurs variables et en les comparant à la distribution prévue pour une séquence véritablement aléatoire. Ce test détecte spécifiquement si l'oscillation entre les zéros et les uns est trop rapide ou trop lente.

2.6.9.5 Test de longues séries de 1

Ce test détermine la longueur de la plus longue série des uns dans un nombre donné de blocs de M bits. Ceci est accompli en comptant le nombre de blocs avec une certaine plus longue série des uns et en les comparant à la distribution prévue pour une séquence véritablement aléatoire.

2.6.9.6 Test de rang de la matrice binaire

Le rang de la matrice binaire produite à partir de la séquence binaire est évalué dans cet test. Ceci est accompli en créant une matrice à partir de la séquence binaire, en déterminant son rang, et en la comparant à la distribution prédite pour une séquence vraiment aléatoire.

2.6.9.7 Test sur la transformée de Fourier discrete

Pour détecter la périodicité, ce test prend en compte les hauteurs de pics de la transformée de Fourier de la séquence. L'objectif est de déterminer si le nombre de pics qui dépassent le seuil de 95% est significativement différent de 5%.

2.6.9.8 Recherche d'un motif apériodique

l'objet de cet test ce fait en comptant le nombre d'occurrences de chaque sou suite donnée dans la séquence binaire. Le but de ce test est de rejeter les séquences avec un nombre excessif des cas de motif apériodique. La recherche est effectuée en déplaçant une fenêtre m-bit à travers la séquence dans la découverte d'un motif. Lorsque ce motif est identifié, la fenêtre de recherche est remplacée sur le premier bit suivant le modèle découvert.

2.6.9.9 Recherche d'un motif périodique

La prémisse de ce test est la même que celle du test de recherche d'un motif apériodique : compter le nombre d'instances d'un certain motif dans la séquence considérée. Lorsque ce motif est identifié dans la suite, la fenêtre de recherche n'est pas déplacée à la fin de celle-ci ; au lieu de cela, elle continue à traverser la suite bit à bit.

2.6.9.10 Test universel de Maurer

L'objectif de ce test est de découvrir si oui ou non la séquence peut être compressée sans perte d'information. Les séquences non aléatoires sont celles qui sont évidemment compressibles.

2.6.9.11 Test de la complexité linéaire

Ce test évalue la complexité linéaire des sous-séquences de longueur croissante pour déterminer la difficulté de la séquence binaire. Il spécifie la longueur d'un décalage de register.

La séquence n'est pas aléatoire si le registre est trop court.

2.6.9.12 Test de l'entropie approximative

Ce test porte sur La fréquence de récurrence de toutes les sous-séquences réalisables de longueur définie m. Il compare les fréquences obtenues avec les longueurs m et m+1. Ce test mesure l'entropie des sous-séquences de longueur croissant pour évaluer la prévisibilité de la séquence binaire.

2.6.9.13 Test d'excursions aléatoires

Lors d'une marche au hasard, ce test compte le nombre de cycles visités avec précision K fois. La somme des séquences de (0, 1) donne la marche aléatoire. L'objectif de ce test est de voir si le nombre des visites à un état pendant un balayage aléatoire est supérieur à la quantité prévue pour une séquence aléatoire.

2.6.9.14 Variante du test d'excursions aléatoires

L'objectif de ce test est de calculer le nombre de fois qu'un certain état est visité et de découvrir des écarts par rapport au nombre prévu des visites à des états de marche aléatoires distincts.

2.6.9.15 Test série

Ce test concerne la fréquence de récurrence de chaque sous-séquence M-bit sur toute la séquence. L'objectif de ce test est d'évaluer si toutes les séquences M-bit qui composent la séquence à tester ont la même chance d'apparaître, comme c'est le cas pour une séquence vraiment aléatoire.

En résumé, la séquence qui réussit le test doit être uniforme, avec des comptes d'occurrence égales pour tous les modèles M-bit. Par conséquent, pour M=1, le test série est égaux au test de fréquence.

2.7 Conclusion

Dans ce chapitre, nous avons exploré les notions fondamentales de la cryptologie. De plus, nous avons discuté de la classification des méthodes de chiffrement des images, ainsi que des méthodologies d'évaluation des algorithmes de chiffrement, comme l'anlyse d'espace clé, l'anlyse de l'histograme, l'analyse de l'entropie, l'anlyse des coffiecients de correlation et la norme d'évaluation du NIST et ses différents tests.

Chapitre 3

Un algorithme de chiffrement des images couleurs basées sur une carte chaotique logistique d'ordre fractionnaire

Sommaire

3.1 Introduction

Avec l'évolution de la vitesse des ordinateurs et le nombre d'outils de piratage, il est désormais important de protéger les données telles que les images lorsqu'elles sont transférées sur internet [43]. Comme on le sait, plusieurs méthodes de chiffrement traditionnelles, comme la norme de cryptage des données (DES), la norme de cryptage avancée (AES) et RivestShamir-Adleman (RSA) sont maintenant lent et donc inefficace pour le cryptage de l'image [44]. Les chercheurs sont invités à utiliser des algorithmes de cryptage basés sur des systèmes chaotiques [45–47]qui se caractérisent par des propriétés aléatoires importantes, ainsi qu'une sensibilité aux paramètres et aux conditions initiales.

Les systèmes chaotiques d'ordre fractionnaire ont également suscité un intérêt considérable de la part des chercheurs pour leurs diverses applications, comme le contrôle [48]et l'électrotechni -que [49]. Ces systèmes ont également été utilisés comme générateurs des séquences pseudo-aléatoires dans de nombreux schémas de chiffrement. Il dispose d'une gamme plus chaotique ainsi que plus de paramètres, ce qui permet un processus de cryptage plus sécurisé. Zhang et al. [50] ont proposé le schéma d'encodage des images qui dépend des S-Boxes et d'un système chaotique fractionnaire ,confirmant qu'il a une plage plus large et un comportement plus chaotique que le système classique. Huang et al [51] ont utilisé un nouveau cryptage de l'image dépendant d'un système hyperchaotique d'ordre fractionnaire, où ils ont démontré que le système peut être utilisé pour crypter les images. Paral et al [52] ont suggéré une nouvelle méthode de cryptage où ils ont utilisé plusieurs systèmes chaotiques fractionnaires pour créer la clé de chiffrement. Aydin et ozkaynuk [53] ont utilisé deux systèmes d'ordre fractionnaire à savoir Chen et Chua pour crypter les images.

ce chapitre vise à introduire une nouvelle méthode de cryptage de l'image dépendant de la création de la clé de cryptage à travers la carte logistique d'ordre fractionnaire. Diverses analyses ont été discutées confirme la qualité de l'algorithme proposé et sa capacité pour répondre à diverses attaques.

3.2 Analyse de la carte logistique fractionnaire

Le calcul d'ordre fractionnaire est l'extension du calcul d'ordre entier. L'équation (1.26) présente la définition de Grundwald-Letnikov (G-L). Nous appliquons cette définition à la carte logistique traditionnelle, aboutissant à la carte d'ordre fractionnaire représentée par l'équation (1.31) [54].

Les figures 1.1 et 1.3 montrent le diagramme de bifurcation et l'exposant de Lyapunov de la carte logistique et les figures 1.4 et 1.5 montrent le diagramme de bifurcation et l'exposant de Lyapunov de la carte logistique d'ordre fractionnaire. Comme le montre la figure 1.1 et 1.4, à travers le diagramme de bifurcation, la zone vide représente le comportement non chaotique et la

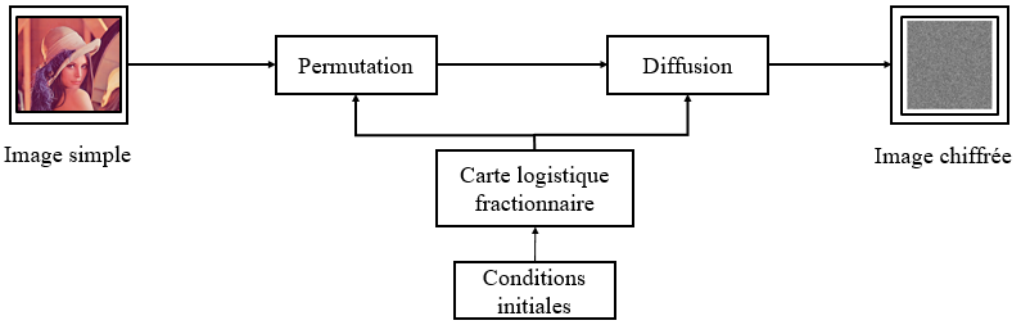


FIG. 3.1 *Le schéma fonctionnel des processus de chiffrement proposés.*

zone pointillée représente le comportement chaotique. La carte logistique d'ordre fractionnaire est chaotique quand $\rho \in [7.30, 8.47]$, alors que la carte logistique classique est chaotique quand $\rho \in [3.57, 4]$. D'après les figures 1.3 et 1.5, le comportement chaotique apparaît lorsque $Ly > 0$, donc la plage chaotique de la carte classique et de la carte d'ordre fractionnaire est $\rho \in [3.57, 4]$ et $\rho \in [7.30, 8.47]$ respectivement. Ainsi, la carte logistique d'ordre fractionnaire a une plage plus chaotique que la carte classique.

3.3 Schéma de cryptage de l'image couleur proposée

Dans cette section, nous introduisons une technique de cryptage dépendant du processus de permutation et de diffusion pour éliminer la corrélation élevée des pixels de l'image. Nous changeons l'emplacement des pixels en décalant les rangées de l'image d'origine, puis nous utilisons deux vecteurs d'index pour permuter la position des lignes et des colonnes. L'algorithme suggéré est illustré à la figure 3.1 . Les détails de l'algorithme sont expliqués comme suit :

— **Étape 1 :** Diviser l'image originale I de taille $M \times N \times 3$ en Canaux $R, GetB$.

— **Étape 2 :** Nous créons deux vecteurs d'indice I, J de taille M, N respectivement en arrangeant deux séquences aléatoires X, Y, où X et Y ont été créés par l'équation (1.31) avec les valeurs initiales $(x_{0.1}, \rho_{0.1})$, $(x_{0.2}, \rho_{0.2})$, respectivement.

— **Étape 3 :** Nous créons une matrice aléatoire V de taille $M \times 2$ en utilisant la formule (1.31) avec des valeurs initiales $(x_{0.3}, \rho_{0.3})$.

— **Étape 4 :** On crée deux séquences aléatoires X1, Y1 de taille M, N respectivement, en utilisant l'équation (1.31) avec les valeurs initiales $(x_{0.4}, \rho_{0.4})$, $(x_{0.5}, \rho_{0.5})$. Ensuite, ils sont convertis en nombre entier par l'équation suivante :

$$\begin{cases} SR = mod(floor([|X1_i| \times 10^{15}], \frac{M}{2}) \\ SL = mod(floor([|Y1_i| \times 10^{15}], \frac{N}{2}) \end{cases} \tag{3.1}$$

— **Étape 5 :** Nous décalons les rangées des canaux R, G et B à l'aide de la règle suivante :

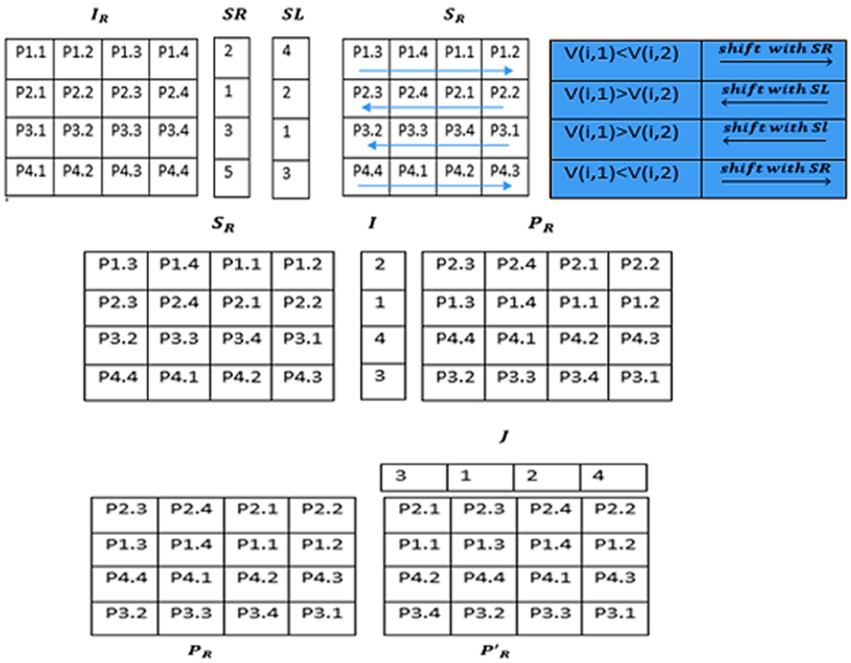


FIG. 3.2 *un exemple de processus de permutation des pixels.*

Si $V(i,1) < V(i,2)$, décaler la ligne i des canaux R, G et B vers la droite avec le numéro de pas SR. Sinon, décaler la ligne i des canaux R, G et B vers la gauche avec le numéro de pas SL.

— **Étape 6 :**Les canaux (R, G et B) permutés sont obtenus en utilisant les canaux décalés ($S_R, S_G et S_B$) et les deux indices I et J en utilisant les équations suivantes :

$$\begin{cases} p_R(i,j) = S_R(I(i),j)) \\ p_G(i,j) = S_G(I(i),j) \\ p_B(i,j) = S_B(I(i),j) \end{cases} \tag{3.2}$$

$$\begin{cases} p'_R(i,j) = p_R(i,J(j)) \\ p'_G(i,j) = p_G(i,J(j)) \\ p'_B(i,j) = p_B(i,J(j)) \end{cases} \tag{3.3}$$

Où (p'_R, p'_G et p'_B) sont les canaux (R, G et B) permutés avec l'indice J, (p_R, p_G et p_B) sont les canaux (R, G et B) permutés avec indice I et (S_R, S_G et S_B) sont les canaux (R, G et B) décalés. Pour comprendre le processus de permutation, nous fournirons un exemple avec une image de taille 4×4 . L'exemple numérique est illustré à la figure 3.2.

— **Étape 7 :** On génère une séquence chaotique aléatoire k1 de taille $m \times n$ en utilisant l'équation (1.31) avec les valeurs initiales $(x_{0.6}, \rho_{0.6})$. Puis k1 converti en entier comme

suit :

$$cle_1 = mod(floor([|k1_i| \times 10^{15}], 256) \tag{3.4}$$

— **Étape 8 :** Les canaux (p'_R, p'_G et p'_B) permutés sont convertis en vecteur 1D.

— **Étape 9 :** Obtenir les canaux cryptés (R, G et B) en utilisant les canaux permutés à une dimension (p'_R, p'_G et p'_B) et la cle_1 en utilisant les équations suivantes :

$$\begin{cases} C_{1D,R}(1) = p'_{1D,R}(1) \oplus cle_1(1) \\ C_{1D,G}(1) = p'_{1D,G}(1) \oplus cle_1(1) \\ C_{1D,B}(1) = p'_{1D,B}(1) \oplus cle_1(1) \end{cases} \tag{3.5}$$

$$\begin{cases} C_{1D,R}(i) = p'_{1D,R}(i) \oplus cle_1(i) \oplus p'_{1D,R}(i-1) \\ C_{1D,G}(i) = p'_{1D,G}(i) \oplus cle_1(i) \oplus p'_{1D,G}(i-1) \\ C_{1D,B}(i) = p'_{1D,B}(i) \oplus cle_1(i) \oplus p'_{1D,B}(i-1) \end{cases} \tag{3.6}$$

Où ($c_{1D,R}$, $c_{1D,G}$ et $c_{1D,B}$) sont les canaux chiffréeS unidemesionalS et $\oplus$ est une opération XOR au niveau du bit. Nous convertissons les canaux chiffrées ($c_{1D,R}, c_{1D,G} et c_{1D,B}$) aux matrices, et nous composons l'image couleur cryptée finale à l'aide de ces matrices.

3.4 Résultat de la simulation

Dans cette partie, nous allons tester notre algorithme sur trois images de taille $512 \times 512 \times 3$ pour déterminer la qualité et l'efficacité de l'algorithme de cryptage des images. Tous les tests ont été effectués sur i7 7500u, Ram 8 Go et logiciel Matlab 2021a. Les résultats de cryptage de notre algorithme sont présentés dans la figure 3.3.

3.4.1 Analyse de l'espace clé

Chaque algorithme doit avoir un espace de clé de chiffrement large afin de rendre une attaque par force brute inefficace. Il a été estimé dans la littérature par plus de 2^{100} [50, 55, 56]. Notre clé est composée de 13 éléments représentés par 6 initiales valeurs ($x_{0.1}, x_{0.2}, x_{0.3}, x_{0.4}, x_{0.5}, x_{0.6}$), 6 paramètres de contrôle ($\rho_{0.1}, \rho_{0.2}, \rho_{0.3}, \rho_{0.4}, \rho_{0.5}, \rho_{0.6}$) et le paramètre fractionnaire α. La précision de chaque élément clé peut aller jusqu'à 10^{-15}. Par conséquent, notre taille de clé est $10^{15\times13=195}$. Ainsi que notre algorithme est capable de vaincre les attaques par force brute.

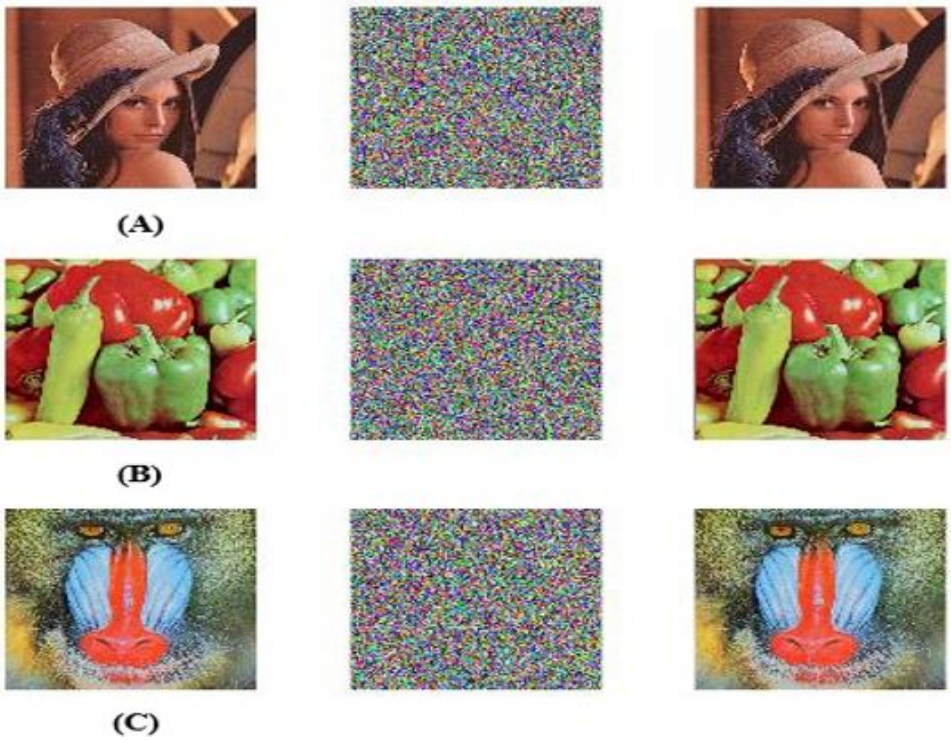


FIG. 3.3 *Résultats de chiffrement et de déchiffrement. La deuxième et la troisième colonne montrent les images chiffrées et déchiffrées. (A) Poivrons, (B) Babouin et (C) Lena.*

3.4.2 Analyse de la sensibilité clé

L'extrême sensibilité de la clé de chiffrement est l'une des bases qui déterminent la qualité d'un système de cryptage. Lorsqu'un petit ajustement de 10^{-15} est appliqué à l'un des éléments clés, cela provoque un défaut majeur dans le processus de décryptage et d'obtenir une image complètement différente de l'image déchiffrée avec une clé correcte. Nous avons déchiffré l'image de Lena en utilisant une clé différente, où l'un des éléments clés a été modifié de 10^{-15} pour confirmer la sensibilité de notre clé. La figure 3.4 illustre les résultats. Comme montré, nous avons un échec de décryptage majeur, ce qui signifie que la clé de notre algorithme est très sensible et excessive.

3.4.3 Analyse d'histogramme

L'histogramme est une technique d'affichage de la distribution des niveaux des pixels dans une image. [4]. Là où il est considéré comme un test important de la capacité de l'algorithme à repousser les attaques statistiques utilisées par les pirates pour extraire des données par histogramme. Donc, l'histogramme de l'image chiffrée doit être uniforme pour masquer tous statistiques renseignements. La figure 3.5 montre l'histogramme de l'image de Lena et son image chiffrée. A travers la même figure , l'histogramme de l'image chiffrée est de nature uniforme. Donc, notre algorithme est capable de contrecarrer toute attaque statistique.

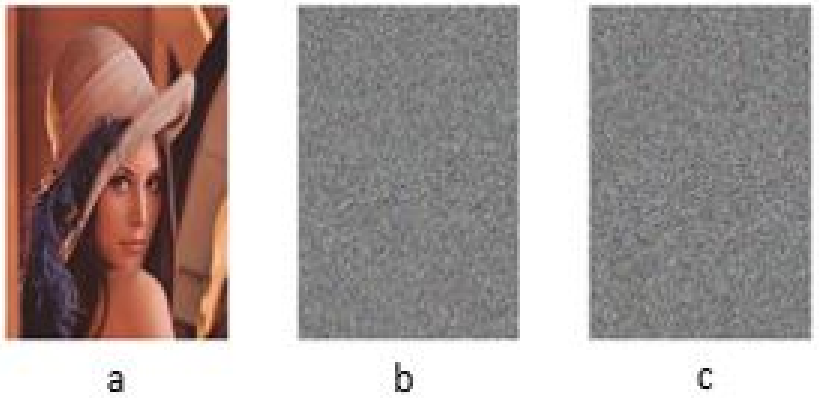


FIG. 3.4 *Le test de sensibilité à la clé de l'image déchiffrée : (a) avec la clé correcte, (b) avec mauvaise $x_{0.1}$ (c) avec mauvaise $x_{0.1}$.*

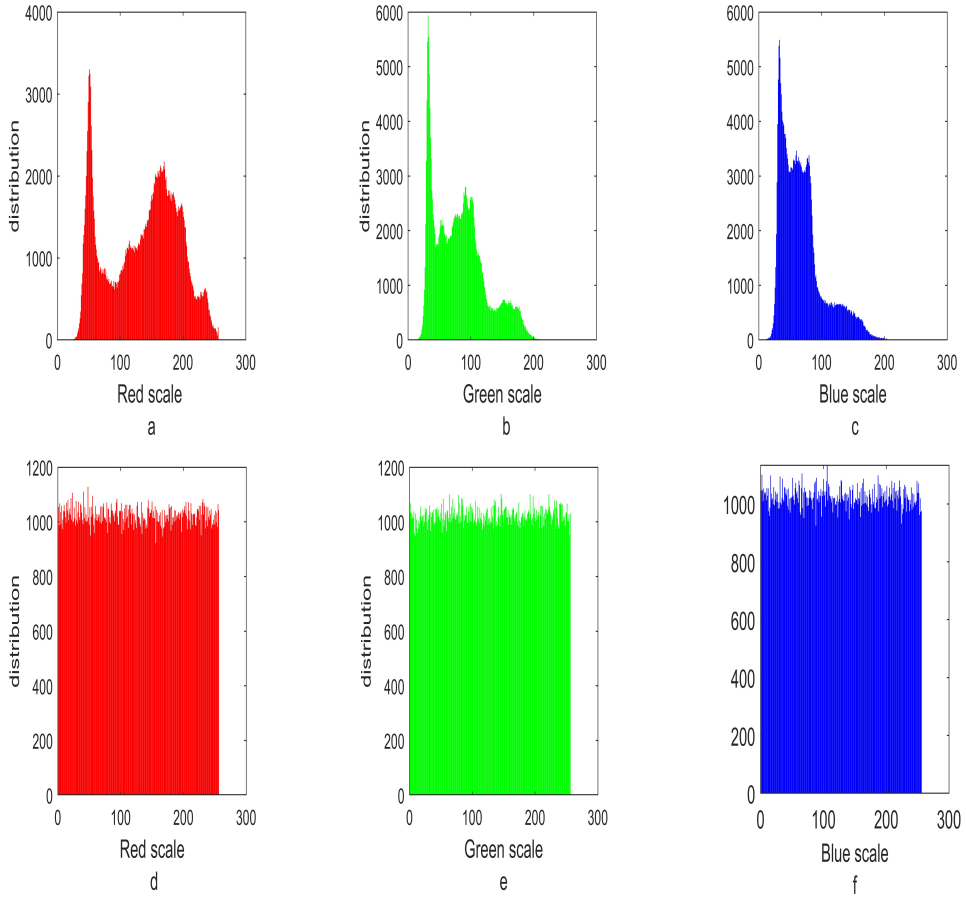


FIG. 3.5 *Histogramme de l'image de Lena et de son image chiffrée. (a)-(c) Histogramme de Composantes R,G,B de l'image originale, (d)-(f) histogramme des composantes R,G,B de l'image chiffrée.*

TABLE 3.1 *Entropie de l'image simple et de l'image chiffrée.*

Image	Images clair	Notre méthode	Ref[46]	Ref [57]
Lena	7,7647	**7.9997**	7.9994	7.9968
Peppers	7.6698	**7.9998**	7.9993	7.9963
Baboon	7.7624	**7.9997**	7.9992	7.9965

3.4.4 Analyse de l'entropie de l'information

L'entropie de l'information est un indice très important pour déterminer le caractère aléatoire [57], il est défini par l'équation 2.3.

L'entropie optimale que chaque système de chiffrement doit offrir est 8. Nos résultats d'entropie, comparés à certains de la littérature, sont montrés dans le tableau 3.1. Comme il est vu, les résultats de notre algorithme sont plus proches de la valeur 8 par rapport aux autres dans les références[46] et [57]. En conséquence, notre schéma est le moins susceptible à l'attaque d'entropie .

TABLE 3.2 *coefficient de corrélation dans l'image originale et l'image cryptée ..*

Canal	Directions	Image originale	Notre Algorithme	Ref [58]	Ref [59]
Canal R	Horizontal	0.9556	-0.0023	-0.0091	0.0001
	Vertical	0.9780	-0.0041	0.0013	0.0091
	Diagonal	0.9434	-0.0004	0.0026	-0.0023
Canal G	Horizontal	0.9443	0.0002	-0.0032	-0.0025
	Vertical	0.9711	-0.0016	-0.0032	-0.0061
	Diagonal	0.9301	0.0011	-0.0039	0.0058
Canal B	Horizontal	0.9280	-0.0011	0.0010	-0.0074
	Vertical	0.9575	0.0001	-0.0018	-0.0059
	Diagonal	0.9030	-0.0004	0.0012	0.0015

3.4.5 Coefficient de corrélation

L'une des caractéristiques évidentes que chaque système de cryptage doit fournir est la capacité de briser la forte corrélation entre les pixels voisins de l'image d'origine au niveau de toutes les directions. La formule mathématique est définie par l'équation (2.4)

Le schéma de chiffrement doit fournir une valeur de corrélation pour les pixels voisins proches de zéro dans toutes les directions. Les résultats du coefficient de corrélation de l'image originale et de l'image chiffrée par notre algorithme par rapport à la littérature sont présentés dans le tableau 3.2. Grâce aux résultats, notre algorithme fournit un coefficient de corrélation

plus proche de zéro par rapport à la littérature [58] et [59], ce qui signifie que notre schéma peut repousser toute attaque statistique.

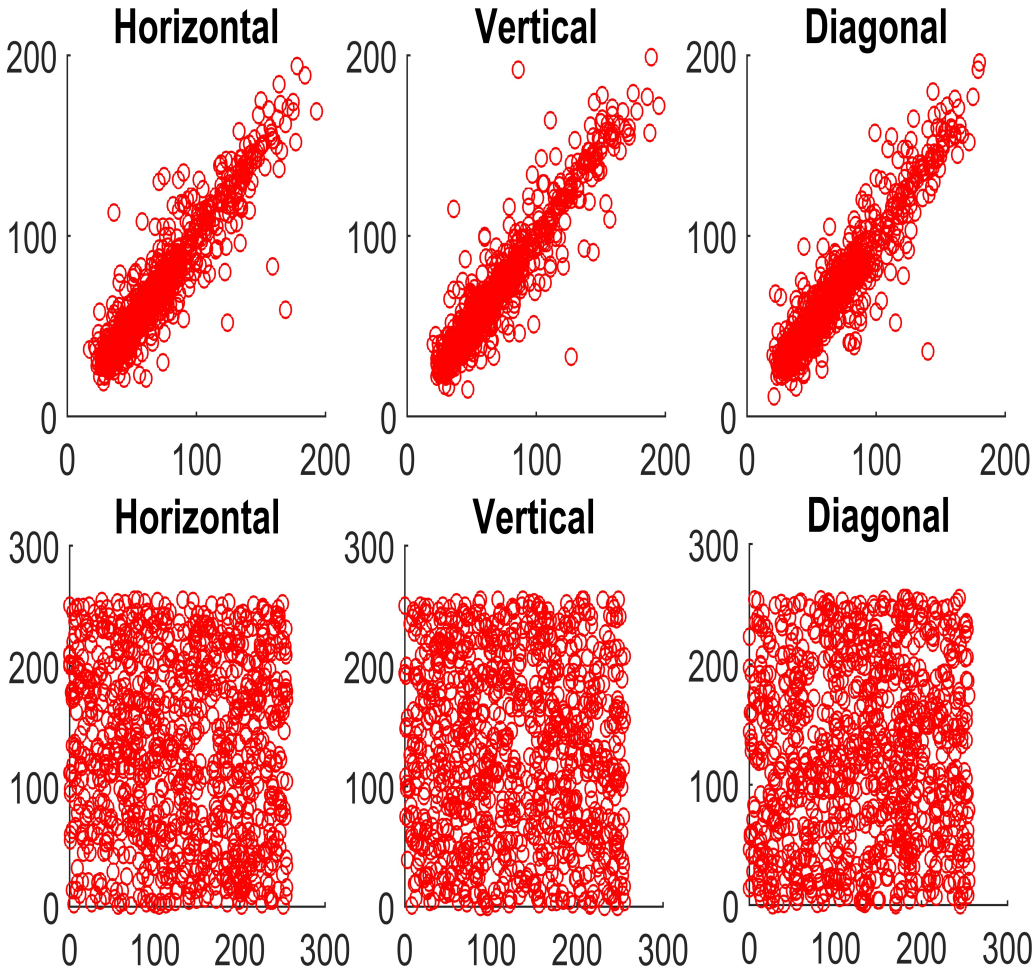


FIG. 3.6 *Distribution des pixels voisins dans différentes directions de Lena. La première ligne montre l'image originale ; la deuxième ligne montre l'image chiffrée.*

3.4.6 Test de caractère aléatoire de l'image chiffrée

Le test Nist est un important ensemble des tests développé par l'institut national des normes et de la technologie (NIST) pour l'examen des propriétés aléatoires [60–63]. Pour déterminer le caractère aléatoire des pixels, nous avons utilisé le test NIST800-22 sur l'image chiffrée. Si les valeurs p dépassent 0.01, le test est considéré comme réussi. Le tableau 3.3 affiche les résultats du test Nist, où nous pouvons voir le succès de tous les tests. Comme un résultat, notre méthode produit d'excellents résultats aléatoires.

TABLE 3.3 *Test NIST 800-22 sur l' image cryptée*

NIST tests	P value	Results
Frequency	0,219446967977955	Passed
Block Frequency	0,725204711762814	Passed
The Run Test	0,936628486043261	Passed
Longest Run of Ones in a block	0,608608963098052	Passed
Binary Matrix Rank	0,494406445242031	Passed
DFT Spectral	0,926883724880223	Passed
Non-Overlapping Template Matching	0,0930461681480921	Passed
Overlapping Template Matching	0,498641147392577	Passed
Maurer's Universal Statistical Test	0,718146098591997	Passed
Linear Complexity	0,680964202303460	Passed
Serial Test	0,198617192160687	Passed
Approximate Entropy	0,940610547173222	Passed
Cumulative Sums	0,205778652812043	Passed
Random Excursions	0,0495559887958185	Passed
Random Excursions Variant	0,679750584710869	Passed

3.5 Conclusion

Dans ce chapitre, nous nous sommes concentrés sur l'application d'une nouvelle technique de cryptage des images à travers la carte logistique d'ordre fractionnaire. Où cette carte est utilisée pour produire la séquence pseudoaléatoire qui est utilisée tout au long des processus de la permutation et de la diffusion. Les résultats de l'analyse ont démontré que le schéma proposé présente un faible coefficient de corrélation et une grande sensibilité à la clé de chiffrement, tout en ayant la capacité de contrer différentes attaques, telles que l'attaque statistique et l'attaque d'entropie.

Chapitre 4

Cryptage des images couleurs basées sur une carte logistique d'ordre fractionnaire améliorée

Sommaire

4.1 Introduction

De nos jours, avec la popularité grandissante d'internet et l'évolution des technologies de réseau, les images numériques sont devenues très essentielles et jouent un rôle important, il est donc devenu nécessaire de sécuriser ces images sur le réseau [64]. En raison de certaines caractéristiques intrinsèques qui caractérisent les images, telles que un grand espace des données, une corrélation entre pixels voisins et un haut niveau de redondance. L'utilisation de certains algorithmes de chiffrement traditionnels est devenue inefficace tels que la norme de cryptage des données (DES) , la norme de cryptage avancée (AES) et Rivest Shamir-Afleman (RSA)[65–67]. En outre, afin de répondre à l'exigence d'une transmission sûre des images numériques. L'algorithme de chiffrement utilisant des systèmes chaotiques a suscité un intérêt considérable de la part des chercheurs en raison des caractéristiques importantes que ces systèmes offrent, telles que la sensible, la dépendance aux conditions initiales et aux paramètres de contrôle, l'imprévisibilité, la pseudo- aléatoire, l'ergodicité et la caractéristique dynamique complexe [61, 68]. Par conséquent, les systèmes chaotiques peuvent être utilisés pour crypter les images.

Les équations différentielles fractionnaires ont récemment suscité un intérêt considérable de la part de chercheurs [69, 70] , en raison de leur application dans divers domaines, par exemple le contrôle [48], l'électromagnétisme et l'ingénierie électrique analogique [71]. Les systèmes dynamiques d'ordre fractionnaire affichent des comportements différents et des nouveaux bifurcations dans les attracteurs. Il montre également des comportements chaotiques différents par rapport à l'équation d'ordre entier [50], les algorithmes de chiffrement utilisant des systèmes chaotiques fractionnaires ont également une plus grande caractéristique de sécurité en raison du paramètre d'ordre fractionnaire, qui offre plus de plage et de liberté en tant que générateurs de nombres pseudo-aléatoires (PRNG). Malgré le fait que les systèmes chaotiques d'ordre fractionnaire, tels que la carte logistique d'ordre fractionnaire, sont préféré aux systèmes chaotiques d'ordre entier. Cependant, ils souffrent encore de quelques problèmes tels que la distribution inégale des données et un comportement chaotique limité. Beaucoup des chercheurs se sont récemment intéressés au cryptage des images basé sur le chaos d'ordre fractionnaire, où plusieurs méthodes de cryptage ont été suggérées. Zhao et al [72] ont proposé un système chaotique d'ordre fractionnaire inapproprié pour le cryptage d'image, ce schéma repose sur la division de l'image originale en quatre parties pour mettre en oeuvre la diffusion et le processus de substitution.Wu et al [73] ont introduit un nouveau modèle de chiffrement, qui comprend le processus de la permutation et de la diffusion. Ils ont utilisé des réseaux à cartes couplées (CML) et un système chaotique d'ordre fractionnaire pour crypter les composantes rouge, verte et bleue de l'image couleur.Yang et al [74] ont proposé une nouvelle technique de cryptage d'image basée sur le système hyper-chaotique d'ordre fractionnaire, où ils confirment que la séquence hyper-chaotique peut être utilisée dans le cryptage des images car elle est plus imprévisible. Mani et al [75] ont présenté un algorithme de cryptage de l'image dans lequel des réseaux de neurones

cellulaires flous chaotiques d'ordre fractionnaire (FOFCNN) ont été utilisés pour produire des séquences pseudo-aléatoires afin de mettre en oeuvre le processus de la diffusion. Li et al [68] ont proposé une nouvelle technique combinant le système hyper-chaotique d'ordre fractionnaire avec la séquence d'ADN pour augmenter le niveau de sécurité du cryptage des images. Lui et al [65] ont suggéré un modèle de schéma de cryptage de l'image chaotique rapide dépendant de la permutation et de la diffusion en même temps, ce qui offre plus de protection contre les attaques séparées. Zhang et al [50] ont suggéré un modèle de chiffrement de l'image utilisant S-Boxes et un système chaotique d'ordre fractionnaire, où il était confirmé que le système offre une meilleure protection contre les attaques des cryptanalystes en raison de sa gamme plus large et son comportement chaotique plus élevé que le système classique. Xu et al [76] ont conçu une nouvelle méthode de chiffrement des images où ils ont utilisé une combinaison du système chaotique fractionnaire et de son système de synchronisation pour chiffrer et déchiffrer l'image.

Ce chapitre vise à améliorer la carte logistique d'ordre fractionnaire afin de surmonter ses problèmes à utiliser dans le cryptage des images. Par conséquent, une nouvelle approche de cryptage de l'image utilisant une carte logistique d'ordre fractionnaire améliorée a proposé. Plusieurs analyses ont été discutées pour assurer l'efficacité de l'algorithme proposé dans la protection des exigences pour le transfert des images numériques, telles que les coefficients de corrélation, l'analyse de la sensibilité clé, l'histogramme, l'attaques différentielles, ainsi que d'autres mesures analytiques.

4.2 Analyse de la carte logistique d'ordre fractionnaire et de la carte améliorée :

Le calcul d'ordre fractionnaire est la généralisation du calcul d'ordre entier classique. La carte logistique d'ordre fractionnaire est calculée à l'aide de la dérivé d'ordre fractionnaire de Caputo. La définition de caputo est présentée comme suit :

$$D^{\alpha}_{t_0} f(t) = \frac{1}{\Gamma(m-\alpha)} \int_{t_0}^{t} f^{m}(u)(t-u)^{m-\alpha-1} du \tag{4.1}$$

Où α est l'ordre fractionnaire, m est un entier donc $(m-1) < \alpha < m$ et $\Gamma(.)$ est la fonction gamma. Considérons les équations différentielles fractionnaires données par [77] :

$$D^{\alpha} x(t) = \rho x(t)(1-x(t)), t > 0 \tag{4.2}$$

Avec $x(0) = x_0$ est la condition initiale, α est le paramètre d'ordre fractionnaire et ρ est le taux de croissance. Dans la section suivante, nous présentons le processus de discrétisation pour

discréditer la contrepartie d'Eq4.2 avec des arguments constants par morceaux

$$D^{\alpha}x(t) = \rho x([\frac{t}{r}r])(1 - x([\frac{t}{r}]r) \tag{4.3}$$

Avec $x(0) = x_0$ est la condition initiale, r est une constante. Soit $t \in [0, r]$, puis $\frac{t}{r} \in [0, r]$. Donc, on obtient :

$$D^{\alpha}x(t) = \rho x_0(t)(1 - x_0), t \in [0, r] \tag{4.4}$$

La solution de l'équation 4.3 est donnée par :

$$\begin{aligned} x_1(t) &= x_0 + I^a \rho x_0 \,(1 - x_0) \\ &= x_0 + \rho x_0 \,(1 - x_0) \int_0^t \frac{(t-s)^{\alpha-1}}{\Gamma(\alpha)} ds \\ &= x_0 + \rho x_0 \,(1 - x_0) \,\frac{t^{\alpha}}{\Gamma(1+\alpha)} \end{aligned} \tag{4.5}$$

Soit $t \in [r, 2r]$, puis $\frac{t}{r} \in [1, 2]$. donc, on obtient :

$$D^{\alpha}x(t) = \rho x_1(t)(1 - x_1), t \in [t, 2r] \tag{4.6}$$

Ce qui suit est la solution de l'équation 4.6 :

$$\begin{aligned} x_2(t) &= x_1(r) + I_t^{\alpha} \rho x_1 \,(1 - x_1) \\ &= x_1(r) + \rho x_1 \,(1 - x_1) \int_{\tau}^t \frac{(t-s)^{\alpha-1}}{\Gamma(\alpha)} ds \\ &= x_1(r) + \rho x_1(r) \,(1 - x_1(r)) \,\frac{(t-r)^{\alpha}}{\Gamma(1+\alpha)} \end{aligned} \tag{4.7}$$

Nous pouvons facilement trouver la solution de l'équation 4.3 en répétant le processus. Cette solution est donnée comme suit :

$$x_{n+1}(t) = x_n(nr) + \frac{(t-nr)^a}{\Gamma(1+\alpha)} \rho x_n(nr) \,(1 - x_n(nr)) \,, t \in \lceil nr, (n+1)r \rceil \tag{4.8}$$

Soit $t \longrightarrow (n+1)r$ la discrétisation est obtenue :

$$x_{n+1}((n+1)r) = x_n(nr) + \frac{r^a}{\Gamma(1+\alpha)} \rho x_n(nr) \,(1 - x_n(nr)) \tag{4.9}$$

Par conséquent, la carte logistique d'ordre fractionnaire est obtenue :

$$x_{n+1} = x_n + \frac{r^a}{\Gamma(1+\alpha)} \rho x_n(1 - x_n) \tag{4.10}$$

Où r est une constante, α est le paramètre d'ordre fractionnaire, ρ est le taux de croissance et x_n est la population actuelle. Pour surmonter les problèmes de la carte logistique d'ordre fractionnaire, nous suggérons de l'améliorer en appliquant des opérations mathématiques de base et en utilisant l'arithmétique modulaire (mod1). L'équation mathématique de la carte améliorée se présente comme suit :

$$x_{n+1} = 2^k \times x_n + \frac{r^\alpha}{\Gamma(1+\alpha)} \rho \times 2^k \times x_n \left(1 - 2^k \times x_n\right) \bmod 1 \tag{4.11}$$

Où k est une constante, x_n dans l'équation (4.10) est remplacé par le terme $(2^k \times x_n)$.

4.2.1 Diagramme de bifurcation

Le diagramme de bifurcation est l'étude du comportement dynamique d'un système en termes de valeurs de paramètres de contrôle [78]. La figure 4.1 présente le schéma de la bifurcation de la carte améliorée et de la carte logistique d'ordre fractionnaire. La zone pointillée indique que le système est chaotique, et la zone vide prouve que le comportement du système n'est pas chaotique. Comme le montre la figure 4.1, la carte améliorée présente des caractéristiques chaotiques sur l'ensemble de champ de paramètre $\rho \in [0, 9]$. Alors que la gamme du comportement chaotique de la carte logistique d'ordre fractionnaire est $\rho \in [7.30, 8.47]$. Ce qui signifie que la carte améliorée offre une meilleure performance chaotique que la carte logistique d'ordre fractionnaire.

4.2.2 Exposant de Lyapunov

L'exposant de Lyapunov est une mesure importante pour évaluer le comportement dynamique et identifiant le degré chaotique du système [79]. L'équation de L'exposant de Lyapunov est donnée comme suit.

$$ly = \lim_{n \to +\infty} \frac{1}{n} \sum_{i=0}^{N} ln \left| f(x_i)' \right| \tag{4.12}$$

Où f' est la fonction de dérivation du système chaotique f. Lorsque l'exposant de Lyapunov dépasse zéro $ly > 0$, cela indique que le comportement du système est chaotique. L' exposants Lyapunov de La carte améliorée et de la carte logistique d'ordre fractionnaire sont présentés dans la figure 4.2. Comme le montre la figure 4.2, la plage des valeurs positives de Lyapunov pour la carte améliorée est supérieure à la carte logistique d'ordre fractionnaire.

4.2.3 Test de NIST

NIST est une collection de 15 tests critiques pour mesurer la qualité d'une séquence binaire aléatoire [61]. Pour chaque test, la valeur P doit être supérieure à 0,01 pour confirmer le succès de la séquence binaire dans le test[61]. Afin de s'assurer que le système chaotique d'ordre

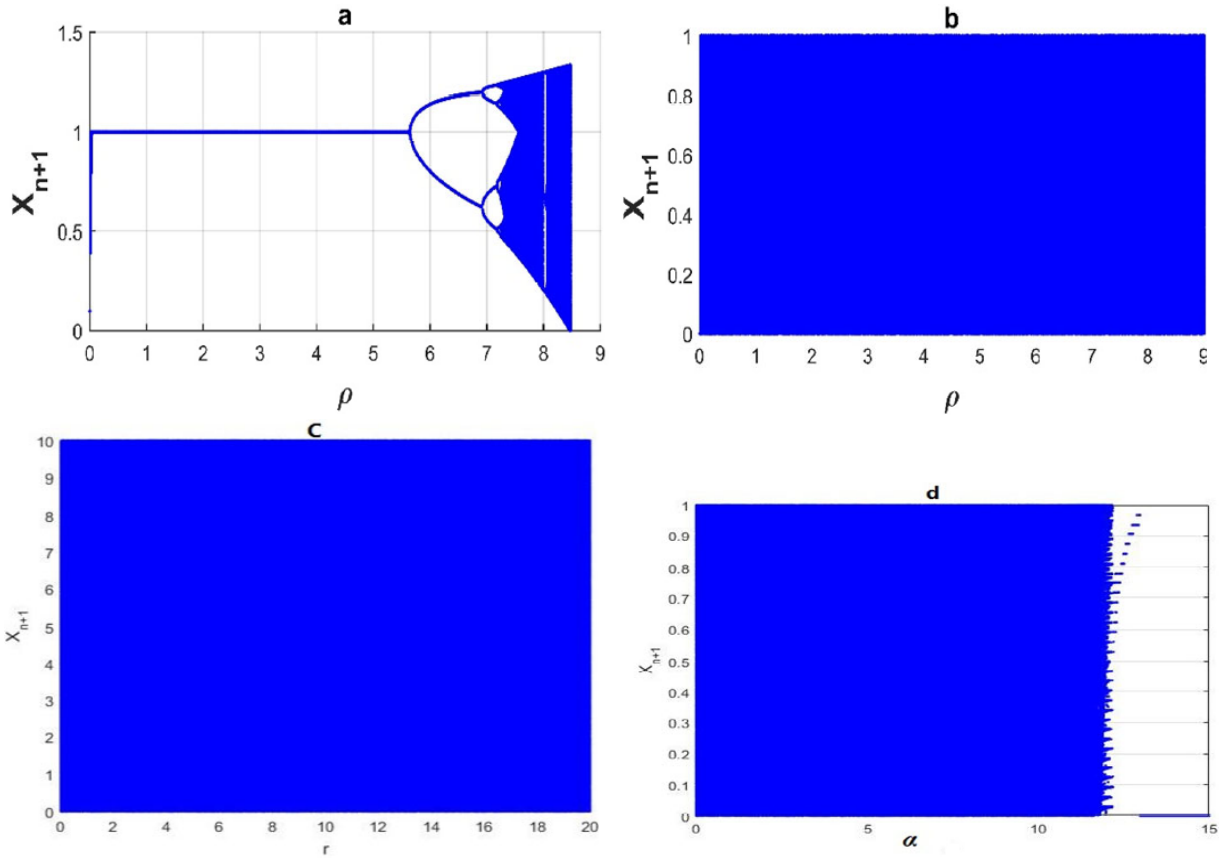


FIG. 4.1 *les diagrammes de bifurcation de la Carte logistique d'ordre fractionnaire (a) et la carte améliorée (b - d).*

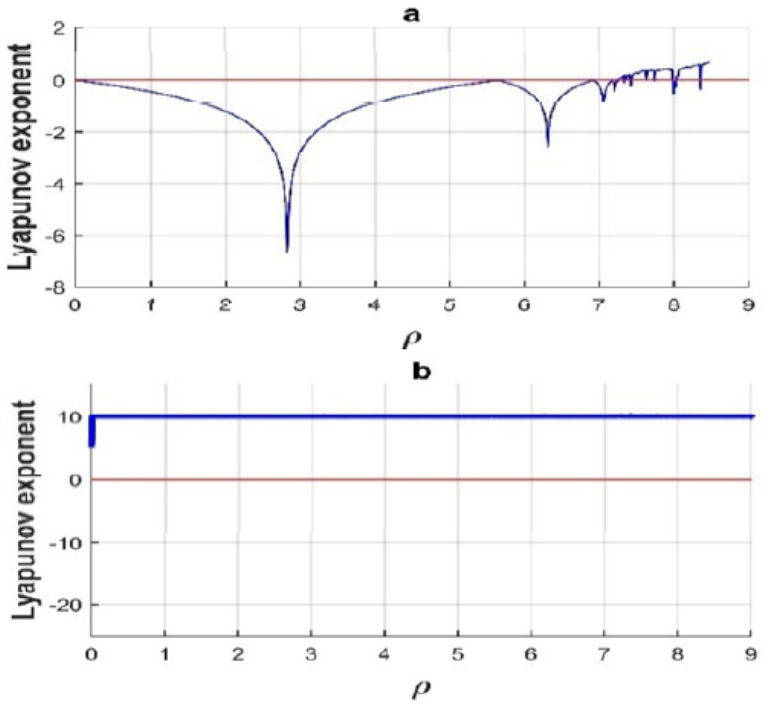


FIG. 4.2 *(a) Lyapunov exposant de la carte logistique d'ordre fractionnaire et (b) la carte améliorée*

TABLE 4.1 *Résultats des tests NIST-800-22 de la carte logistique d'ordre fractionaire améliorée*

NIST tests	P value	Results
Frequency	0.638355017565112	Passed
Block Frequency	0.388233403726571	Passed
The Run Test	0.958352670669443	Passed
Longest Run of Ones in a block	0.201377525588149	Passed
Binary Matrix Rank	0.421450616751419	Passed
DFT Spectral	0.594556664151719	Passed
Non-Overlapping Template Matching	0.0712333835934371	Passed
Overlapping Template Matching	0.324397624273318	Passed
Maurer's Universal Statistical Test	0.645937742145016	Passed
Linear Complexity	0.3988135818906010	Passed
Serial Test	0.899825376592255	Passed
Approximate Entropy	0.89331304289261	Passed
Cumulative Sums	0.627394094334661	Passed
Random Excursions	0.988758946011156	Passed
Random Excursions Variant	0.990123446161416	Passed

fractionnaire amélioré peut être utilisé pour l'encodage des images, nous avons effectué un test NIST-800-22 sur les séquences générées par ce système. Les résultats des tests NIST présentés dans le tableau 4.1, où nous pouvons voir que la carte améliorée passe avec succès tous les 15 tests. En conséquence, les séquences créées par ce système contiennent un degré élevé d'aléatoire et convient au cryptage des images.

4.3 Algorithme de cryptage de l'image couleur proposé

Dans cette partie, nous proposons un nouvel algorithme pour le chiffrement des images en utilisant une carte logistique d'ordre fractionnaire améliorée. Ce dernier a plus de paramètres et une clé plus large que la carte classique. La clé de l'algorithme proposé est constituée de 18 paramètres présentés comme suit :
$x_{0.1}, \rho_{0.1}, \alpha_{0.1}, x_{0.2}, \rho_{0.2}, \alpha_{0.2}, x_{0.3}, \rho_{0.3}, \alpha_{0.3}, x_{0.4}, \rho_{0.4}, \alpha_{0.4}, x_{0.5}, \rho_{0.5}, \alpha_{0.5}, x_{0.6}, \rho_{0.6}, \alpha_{0.6}$. L'algorithme suggéré est illustré à la figure 4.3. L'algorithme proposé utilise une structure de cryptage à deux tours. L'insertion aléatoire des pixels, la permutation et le processus de la diffusion sont tous utilisés dans chaque cycle de chiffrement. Les détails du schéma de chiffrement sont indiqués dans les étapes suivantes :

— **Étape 1 :** Lire l'image couleur $O_{n\times m\times 3}$, au début de chaque ligne de l'image originale, nous ajoutons un pixel avec une valeur aléatoire. Pour faire l'entrée aléatoire des pixels, nous

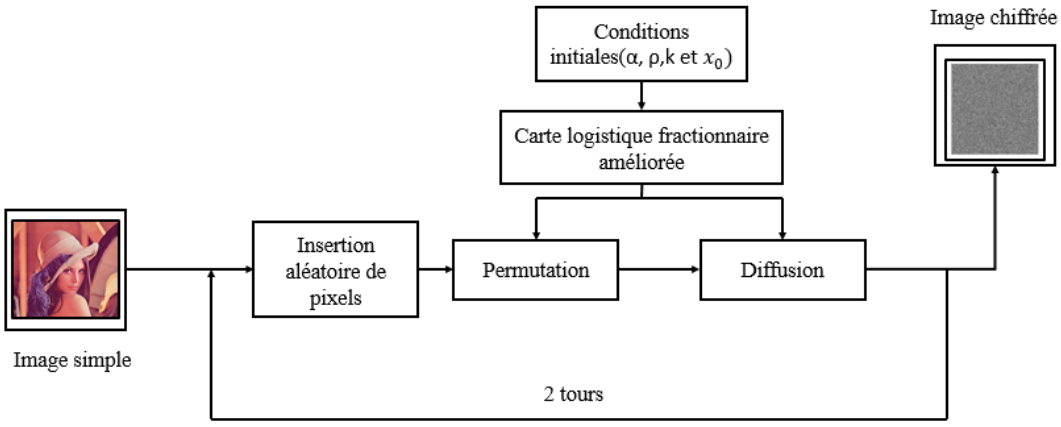


FIG. 4.3 *Schéma fonctionnel de l'algorithme de chiffrement proposé.*

utilisons la fonction Rand qui produit des nombres aléatoires. Le but de l'insertion d'un pixel aléatoire est d'obtenir une image aléatoire, différente pour chaque tour de cryptage.

— **Étape 2 :** Dans cette partie, nous introduisons un algorithme de permutation pour casser la corrélation entre les pixels. Cet algorithme modifie simultanément la ligne et la colonne de l'image. Dans ce qui suit, nous montrerons les détails de l'algorithme de la permutation suggéré :

  — Soient X, Y deux suites aléatoires,$X = X_1, X_2.....X_M$ de longueur M et, $Y = Y_1, Y_2.....Y_N$ de longueur $(N + 1)$ généré par le l'équation (4.11) avec les valeurs initiales $(x_{0.1}, \rho_{0.1}, \alpha_{0.1})$, $(x_{0.2}, \rho_{0.2}, \alpha_{0.2})$.

  — On obtient deux séquences d'index I, J en triant les séquences chaotiques X et Y.

  — Nous générons deux matrices aléatoires V de longueur $M \times 2$ et G de longueur $(N + 1) \times 2$ en utilisant l'équation (4.11) avec les valeurs initiales $(x_{0.3}, \rho_{0.3}, \alpha_{0.3})$, $(x_{0.4}, \rho_{0.4}, \alpha_{0.4})$ respectivement.

  — Le but de ces deux matrices est de déterminer le balayage et la direction de la permutation. Lorsque $V(I(i), 1) > V(I(i), 2)$ la ligne $I(i)$ de l'image O est retournée de gauche à droite. Sinon, la ligne $I(i)$ de l'image O est retournée de droite à gauche enfin on obtient l'image permutée P.

— **Étape 3 :** Nous générons deux séquences chaotiques différentes $S = S_1, S_2.....S_{SW}$, $Z = Z_1, Z_2.....Z_{zh}$ de taille$M \times N \times 3$ en utilisant l'équation (4.11) avec des valeurs initiales $(x_{0.5}, \rho_{0.5}, \alpha_{0.5})$, $(x_{0.6}, \rho_{0.6}, \alpha_{0.6})$ respectivement. Alors S et Z sont transformés en entier en utilisant la fonction suivante :

$$\begin{cases} key_1(i) = floor(S(i) \times 10^{15}) mod 256 \\ key_2(i) = floor(Z(i) \times 10^{15}) mod 256 \end{cases} \tag{4.13}$$

où la fonction "floor" rapproche la valeur de X à des entiers.

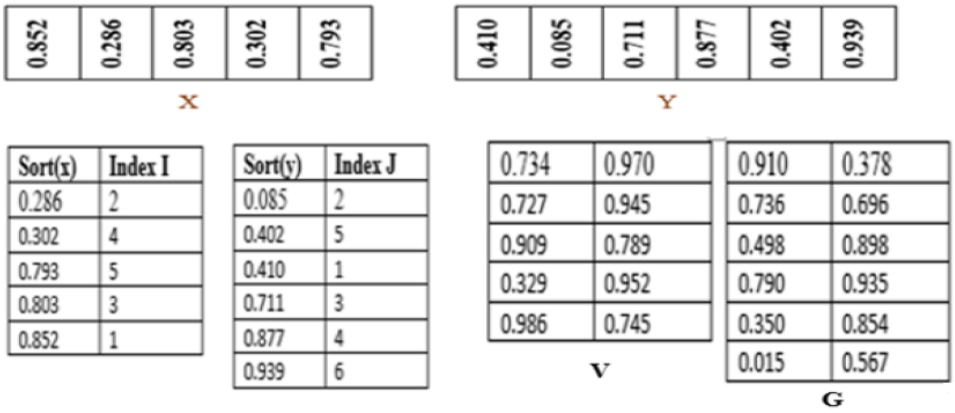


FIG. 4.4 *Exemple de création des séquences chaotiques (a) créant deux index J et I (b) créant deux matrices V et G.*

— **Étape 4 :** L'image de chiffrement C est obtenue à partir de l'image brouillée P et de la clé (key1) à l'aide des équations suivantes :

$$\begin{cases} c(i,j) = p(i,j) \oplus key_1(i) & si(i=1, j=1) \\ c(i,j) = (p(i,j) \oplus key_1(i)) \oplus c(i-1,j) & si(i \neq 1, j=1) \\ c(i,j) = (p(i,j) \oplus key_1(i)) \oplus c(i,j-1) & sinon \end{cases} \tag{4.14}$$

où $\oplus$ est l'opérateur XOR.

L'algorithme 2 décrit le processus de la diffusion du schéma proposé. Nous utilisons la clé (key_2) dans le deuxième tour. Nous allons présenter un exemple avec une image de taille 5×5 pour comprendre comment la proposition de l'algorithme fonctionne. L'exemple numérique est illustré par la figure 4.4 et la figure 4.5 :

— Deux séquences aléatoires X et Y de taille M,$N+1$ respectivement ont été générées.

— On arrange les séquences ascendantes pour obtenir deux indices J et I.

— On génère deux matrices aléatoires V et G de taille $M \times 2$ et $(N+1) \times 2$ respectivement, où V et I sont utilisés en permutation au premier tour et G, J sont utilisés pour le second tour.

— Nous insérons des pixels aléatoires ($pr1, pr2, pr3, pr4, pr5$) au début de chaque ligne de l'image originale O.

— Nous utilisons I et V pour permuter l'image où nous changeons les lignes en fonction de I. Par exemple, la 1^{er} ligne de l'image P est remplacée par la deuxième ligne de l'image originale O'. Si $V(I(i),1) > V(I(i),2)$ la ligne est commutée de gauche à droite. Sinon, la ligne est retournée de droite à gauche et ainsi de suite.

— On utilise l'algorithme 2 pour obtenir l'image chiffrée p pour le premier tour.

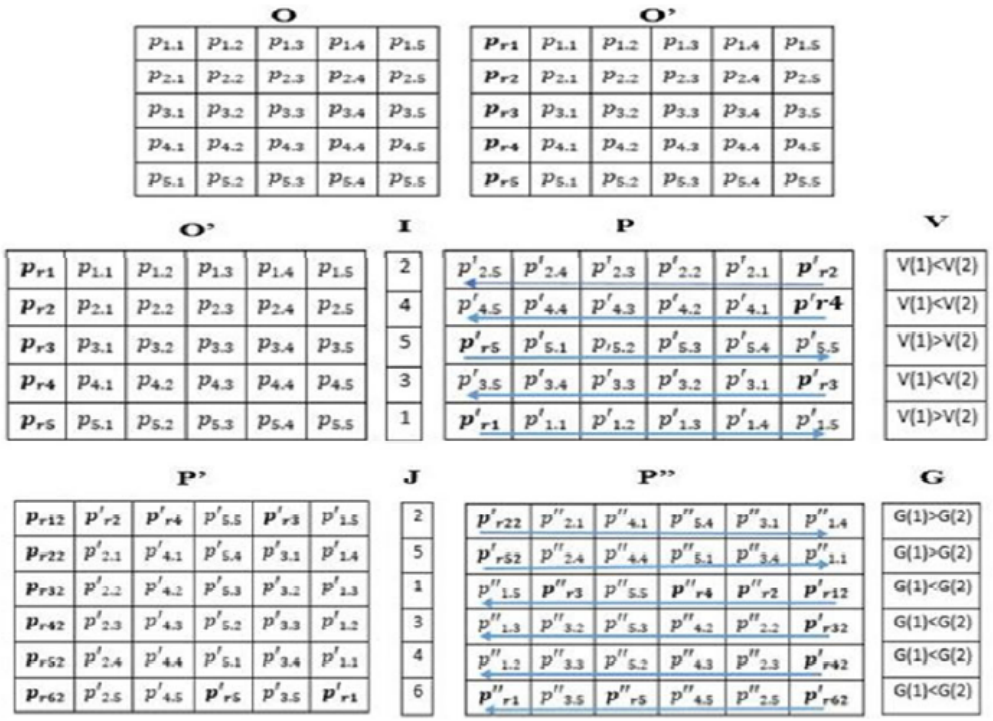


FIG. 4.5 *Processus de la permutation et de la diffusion (a) insertion des pixels aléatoires dans chaque ligne de l'image O (b) permutation et diffusion vers P en utilisant I (c) rotation de l'image de 90 degrés dans le sens antihoraire avec insertion de pixels aléatoires (p') pour commencer le deuxième tour de chiffrement (d) permutation et diffusion vers P" en utilisant J.*

— Au second tour, on fait pivoter l'image p de 90 degrés, et on insère des pixels (pr12, pr22, pr32, pr42, pr52, pr52) au début de chaque ligne. On obtient l'image P'.

— On utilise J et G pour permuter l'image P' et l'algorithme 2 pour obtenir l'image cryptée p".

— La taille de l'image chiffrée est $(M+1)\times(N+1)$ en raison de l'entrée des pixels au début de chaque ligne de l'image originale.

Le décryptage se fait en inversant les étapes de cryptage en utilisant la même clé de chiffrement.

4.4 Résultats des simulations

Dans cette section, trois données des images de taille $512\times512\times3$ seront utilisées comme entrée pour évaluer les performances de l'algorithme proposé. De plus, il sera comparé à d'autres algorithmes dans la littérature pour clarifier l'efficacité de cet algorithme. La figure 4.6 illustre le résultat du processus de chiffrement et de déchiffrement de l'image.

Algorithme 1 Permutation

Entrée :V, G, I, J, O'
Sortie : : image permutée p"
$k \leftarrow M$
pour $l = 1 : 3$ **faire**
  pour $i = 1 : M$ **faire**
    si $V(I(i), 1) \geq V(I(i), 2)$ **alors**
      pour $j = 1 : N$ **faire**
        déplacez la ligne I(i) de gauche à droite en utilisant ce qui suit :
        $p(I(i), j) \leftarrow O'(i, j, l)$
      fin pour
    sinon
      pour $j = 1 : N$ **faire**
        déplacez la ligne I(i) de droite à gauche en utilisant ce qui suit :
        $p(I(i), K) \leftarrow O'(i, j, l)$
        $k \leftarrow k - 1$;
      fin pour
    fin si
  fin pour
  $k \leftarrow M$
fin pour
La deuxième série de permutations
$p' \leftarrow rot90(p)$
Ajoutez un pixel aléatoire au début de chaque ligne de l'image p'
$k \leftarrow N$
pour $l = 1 : 3$ **faire**
  pour $i = 1 : M$ **faire**
    si $G(J(i), 1) \geq G(J(i), 2)$ **alors**
      pour $j = 1 : N$ **faire**
        Inverser la rangée J(i) de gauche à droite en utilisant ce qui suit :
        $p''(J(i), j) \leftarrow p'(i, j, l)$
      fin pour
    sinon
      pour $j = 1 : N$ **faire**
        Inverser la rangée J(i) de droite à gauche en utilisant ce qui suit :
        $p''(J(i), j) \leftarrow p'(i, j, l)$
        $k \leftarrow k - 1$;
      fin pour
    fin si
  fin pour
  $k \leftarrow N$
fin pour

Algorithme 2 Diffusion

Entrée :image permutée p" ; Clés secrètes :($x_{0.5}, \rho_{0.5}, \alpha_{0.5}, x_{0.6}, \rho_{0.6}, \alpha_{0.6}$)
Sortie : :Image chiffrée C
Utilisez les clés secrètes pour obtenir ls séquences chaotiques S et Z de taille $M \times N \times 3$, puis S et Z sont transformés en entiers en utilisant la fonction suivante :
$key1(i) = floor(S(i) \times 10^{15}) mod 256$, $key2(i) = floor(Z(i) \times 10^{15}) mod 256$
Lire l'image permutée p"
pour $l = 1 : 3$ **faire**
  pour $i = 1 : M$ **faire**
    pour $j = 1 : N$ **faire**
      si (i = 1 and j = 1) **alors**
        $c(i, j, l) = p''(i, j, l) \oplus key1$
      sinon si $(i \neq 1 and j = 1)$ **alors**
        $c(i, j, l) = (p''(i, j, l) \oplus key1) \oplus c(i - 1, n, l)$
      sinon
        $c(i, j, l) = (p''(i, j, l) \oplus key1) \oplus c(i, j - 1, l)$
      fin si
    fin pour
  fin pour
fin pour

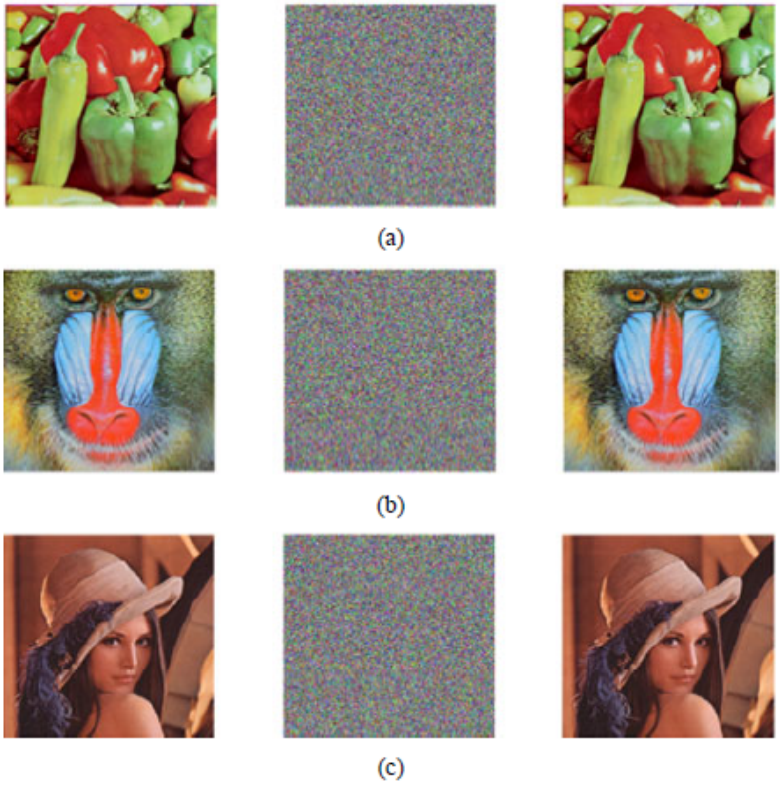


Fig. 4.6 *Résultats du chiffrement et du déchiffrement (a) peppers (b) baboon (c) Lena.*

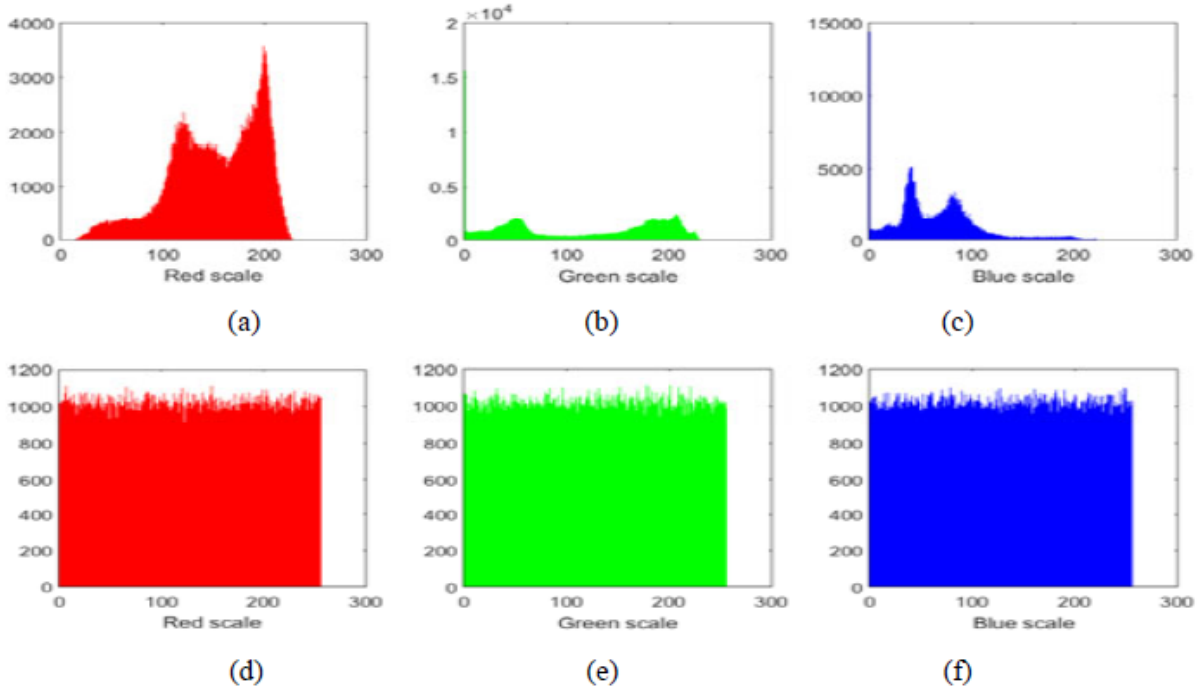


FIG. 4.7 *Histogramme de l'image de "pepper" et de l'image chiffrée (a)-(c) histogramme de R, G, B composants de l'image originale (d)-(f) histogramme de R, G, B composants de l'image chiffrée.*

4.4.1 Analyse de l'espace clé

Un bon algorithme cryptographique doit disposer d'une large espace des clés afin d'améliorer leur résistance aux attaques par force brute. Comme on le sait, l'espace clé doit être supérieur à 2^{100}[59, 80]. Comme nous l'avons mentionné précédemment, les clés de sécurité de notre algorithme comprennent 18 paramètres, tels que 6 paramètres de contrôle $\rho_{0.1}, \rho_{0.2}, \rho_{0.3}, \rho_{0.4}, \rho_{0.5}, \rho_{0.6}$, 6 paramètres d'ordre fractionnaire $\alpha_{0.1}, \alpha_{0.1}, \alpha_{0.2}, \alpha_{0.3}, \alpha_{0.4}, \alpha_{0.5}$ et 6 valeurs initiales $x_{0.1}, x_{0.2}, x_{0.3}, x_{0.4}, x_{0.5}, x_{0.6}$. La précision de chaque valeur initiale est 10^{14}, donc la taille de l'espace clé de notre algorithme est de $10^{18\times14=252} = 2^{837}$. En conséquence, notre espace de clé d'algorithme est suffisamment large pour résister aux attaques par force brute.

4.4.2 Analyse d'histogramme

Pour étudier l'efficacité des algorithmes de chiffrement contre les attaques statistiques, nous utilisons l'histogramme qui représente la distribution de la valeur des pixels de l'image. Dans lequel l'image chiffrée doit avoir un histogramme plat[81]. La figure 4.7 montre les histogrammes du "pepper" image et son image chiffrée. À partir de la figure4.7, on peut voir que l'histogramme de l'image chiffrée semble uniforme et complètement différent de l'image originale. Cela signifie que notre système empêche l'attaquant de collecter des données statistiques et l'empêche ainsi de mener des attaques statistiques.

TABLE 4.2 *Analyse d'entropie des "peppers, baboon et Lena".*

Image	Images clair	Notre méthode	Ref[65]	Ref [68]	Ref [80]
Peppers	7.6698	**7.9998**	7.9971	7.9994	7.9984
Baboon	7.7624	**7.9997**	7.9967	/	7.9989
Lena	7,7647	**7.9998**	7.9972	7.9971	7.9997

4.4.3 Analyse de l'entropie de l'information

L'entropie de l'information est un indicateur important pour mesurer l'aléatoire et l'imprévisibilité . L'entropie de l'information est présentée par l'équation 2.3 .

la valeur d'entropie idéale est proche de 8. Le tableau 4.2 montre les valeurs d'entropie des différentes images chiffrées. Grâce aux résultats du tableau, les valeurs d'entropie des différentes images chiffrées par nos algorithmes sont proches de huit. Notre algorithme fournit également de meilleurs résultats que ceux obtenus dans les références [65, 68, 80].

4.4.4 Coefficient de corrélation

L'analyse de corrélation est un indice important pour évaluer la qualité des algorithmes de chiffrement des images. Il est bien connu que les pixels de l'image sont caractérisés par leur forte corrélation les uns avec les autres sur les niveaux horizontal, vertical et diagonal. Par conséquent, un bon algorithme de cryptage est nécessaire pour rompre ce lien entre les pixels. Le coefficient de corrélation est donné par l'équation (2.4) .

Le tableau 4.3 présente les résultats du coefficient de corrélation de l'image chiffrée de Lena de notre algorithme par rapport aux autres algorithmes trouvés dans la littérature. Comme le montre le tableau 4.3, les valeurs de corrélation pour l'image originale sont proches de 1 dans toutes les directions tandis que la corrélation dans l'image chiffrée est presque nulle. Les résultats obtenus grâce à nos algorithmes sont bien meilleurs que ceux mentionnés dans les référence [59, 81]. Ainsi, notre algorithme est capable de casser la corrélation entre les pixels, ce qui est montré dans la figure4.8. Par conséquent, notre schéma est capable de bloquer les attaques statistiques.

4.4.5 Analyse d'attaque différentielle

En cryptographie, deux pourcentages, le nombre de taux de changement de pixel(NPCR) et l'intensité de changement moyenne unifiée(UACI) sont généralement utilisés pour mesurer la sensibilité du léger changement dans l'image d'origine et ce qui en résulte lorsqu'il est crypté. Par conséquent, ces deux pourcentages sont d'une grande importance pour déterminer l'efficacité du schéma proposé face aux attaques différentielles. Les formules suivantes sont utilisées pour

Table 4.3 *Coefficient de corrélation de l'image originale et de l'image chiffrée et comparaison avec différents algorithmes.*

Canal	Directions	Image originale	Notre Algorithme	Ref [81]	Ref [59]
Canal R	Horizontal	0.9556	0.0026	-0.0025	0.0001
	Vertical	0.9780	-0.0002	0.0913	0.0091
	Diagonal	0.9434	-0.0005	0.0011	-0.0023
Canal G	Horizontal	0.9443	-0.0023	0.0058	-0.0025
	Vertical	0.9711	0.0008	-0.0372	-0.0061
	Diagonal	0.9301	-0.0016	-0.0014	0.0058
Canal B	Horizontal	0.9280	0.0007	-0.0058	-0.0074
	Vertical	0.9575	-0.0017	0.0036	-0.0059
	Diagonal	0.9030	0.0003	2.11e-4	0.0015

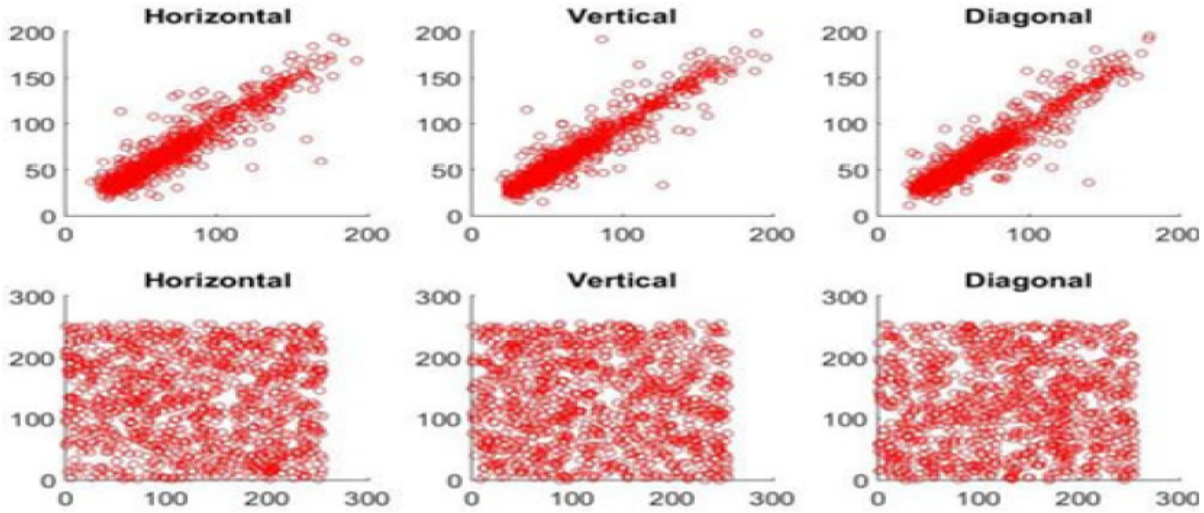


Fig. 4.8 *Distribution des pixels voisins dans différentes directions de Lena.*

mesurer le NPCR et l'UACI :

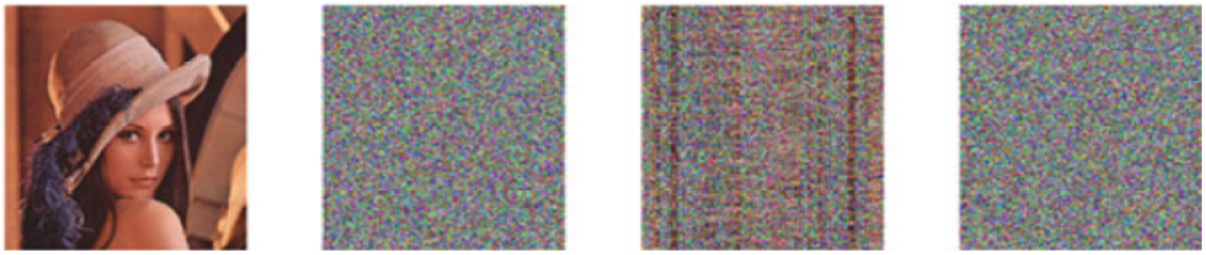
$$\begin{cases} NPCR = \frac{1}{L}\sum D(i,j) \times 100\% \\ UACI = \frac{1}{L}\sum \frac{c_1(i,j)-c_2(i,j)}{255} \times 100\% \end{cases} \tag{4.15}$$

Où L est le nombre total des pixels, C1 et C2 sont la valeur du pixel avant et après la même modification, respectivement. Les règles pour déterminer D (i, j) sont les suivantes :

$$D(i,j) = \begin{cases} 0 & c_1(i,j) = c_2(i,j) \\ 1 & c_1(i,j) \neq c_2(i,j) \end{cases} \tag{4.16}$$

TABLE 4.4 *NPCR et UACI de diverses images cryptées.*

	NPCR(%)			UACI(%)		
Image	Peppers	Baboon	Lena	Peppers	Baboon	Lena
notre méthode	99.60	99.61	99.61	33.46	33.47	33.49
Ref[65]	/	99.636	99.6216	/	33.4702	33.4994
Ref[68]	99.5845	/	99.5723	33.2703	/	33.3159
Ref[80]	99.61	99.62	99.61	31.03	33.46	32.23



(a) (b) (c) (d)

FIG. 4.9 *Le test de sensibilité de la clé de l'image déchiffrée (a) avec la clé correcte (b) avec incorrect* $\alpha_{0.1} + 10^{-14}$ *(c) avec incorrect* $x0.1 + 10^{-14}$ *(d) avec incorrect* $\alpha_{0.6} + 10^{-14}$

Les valeurs optimales mentionnées dans la littérature pour le NPCR et l'UACI sont de $99,6094\%$ et $33,4635\%$ respectivement . Nous avons changé un seul pixel des images originales pour obtenir les valeurs NPCR et UACI. Les résultats obtenus sont présentés dans tableau 4.4.5. Les valeurs NPCR et UACI de notre algorithme sont très proches des valeurs idéales par rapport aux méthodes mentionnées dans les références[65, 68, 80]. Ainsi, l'algorithme proposé est très efficace contre les attaques différentielles.

4.4.6 Analyse de la sensibilité clé

Une sensibilité extrême des clés est nécessaire pour tout algorithme de cryptage, car une fois que la clé est changée par une très petite quantité, cela entraînera une défaillance massive de déchiffrer et d'obtenir une image de chiffrement entièrement différente. Cela signifie que si la clé secrète est modifiée, le résultat du déchiffrement sera entièrement différent. Pour voir l'impact de notre sensibilité clé, nous avons changé la valeur de chaque clé de 10^{-14}, les résultats obtenus sont montrés dans la Figure 4.9. Comme nous pouvons le voir, une fois que la clé change d'un petit pourcentage de 10^{-14}, nous obtenons une image différente de celle qui est décryptée avec la bonne clé.

FIG. 4.10 *Processus de décryptage avec nez sel et poivre.*

FIG. 4.11 *Résultats de l'analyse de l'attaque par perte des données (a)* 64×64 *perte des données (b)* 128×128*perte des données (c)* 128×513 *perte des données ,(d) l'image déchiffrée de (a) ,(e) l'image déchiffrée de (b) ,(f) l'image déchiffrée de (c).*

4.4.7 Perte des données et des attaques par bruit

Lors de la transmission de l'image chiffrée sur le réseau, elle peut être dispersée par des phénomènes tels que la perte des données et le bruit. A cet effet, l'attaque par le bruit et la perte des données sont utilisés pour déterminer la qualité de l'algorithme de chiffrement dans la prévention de ces attaques. Nous avons ajouté un bruit sel et poivre de niveau $1\%, 5\% et 10\%$ à l'image cryptée de Lena pour effectuer un test anti-bruit. Les résultats obtenus sont présentés à la figure 4.10, nous avons également recadré l'image chiffrée en différentes tailles, comme le montre la figure 4.11. A travers les figures 4.10 et 4.11, et malgré le bruit et la perte des données, L'image déchiffrée contient la majorité de l'information de l'image originale, ce qui montre que notre algorithme est efficace contre les attaques de bruit et la perte des données.

TABLE 4.5 *Analyse de la vitesse.*

Image	Schéma proposé	Ref[82]	Ref[83]
Lena 512×512	2.32	3.5145	3.76

4.4.8 Analyse de la vitesse

En termes de cryptographie, un bon schéma de chiffrement doit être caractérisé par une haute vitesse de fonctionnement. Nous avons utilisé l'environnement Matlab R2015a avec un processeur Intel I7-7500U avec @ 2,7 GHz et 8 Go de RAM sur Windows 10 pour exécuter notre algorithme. Le tableau 4.5 montre les résultats du test de la vitesse de cryptage. Comme on peut le voir, notre schéma est plus rapide que d'autres algorithmes dans les références [82, 83].il est donc fiable pour les applications réelles.

4.5 Conclusion

Dans ce chapitre, nous avons proposé un nouveau algorithme de chiffrement des images utilisant une carte logistique d'ordre fractionnaire améliorée, où cette carte a de meilleures caractéristiques que la carte logistique fractionnaire classique, y compris un espace clé plus grand, une plus grande portée, une distribution des données uniformes et plus de paramètres. Ce qui est confirmé par l'analyse du diagramme de bifurcation et de l'exposant de Lyapunov.

Les résultats des simulations et des analyses de performances ont prouvé que notre algorithme possède d'excellentes propriétés, y compris un grand espace clé en plus de la sensibilité à des petits changements de clé et une faible corrélation par rapport aux algorithmes précédents. Ça aussi offre une meilleure protection contre les attaques des pirates telles que les attaques statistiques et les attaques différentielles.

Chapitre 5

Chiffrement robuste des images couleurs basées sur la nouvelle technique en zigzag et le système chaotique tridimensionnel d'ordre fractionnaire.

Sommaire

5.1 Introduction

Avec l'échange croissant des données multimédias sur les réseaux de communication, il est devenu vital d'enquêter sur des nouvelles méthodes pour éviter la fuite de leur vie privée et les manipulations illicites, d'autant plus que les applications de piratage prolifèrent à notre époque moderne [62]. Les techniques traditionnelles de chiffrement telles que DES, RSA et AES ne satisfont plus les critères de cryptage des données multimédias telles que les images et le son. Cela prend beaucoup de temps et une forte consommation d'ordinateur ressource en raison des caractéristiques distinctives de ces médias par rapport aux textes [61]. En conséquence, il est devenu indispensable d'explorer d'autres techniques de chiffrement, ce qui a conduit à l'apparition de nombreuses approches basées sur des concepts variés, y compris l'ADN [84], la théorie quantique [85] et le chaos le plus populaire [86–91] où cette technique offre une vitesse et une sécurité accrues, ce qui le rend utile dans le domaine des applications de chiffrement.

Les systèmes chaotiques ont démontré des résultats impressionnants dans les applications de chiffrement telles que la sécurité de communication et cryptage des images. Ce qui est dû à ses qualités distinctes telles que la sensibilité aux valeurs initiales, la pseudo hasard et imprévisibilité. Il peut également résister à une détérioration dynamique . Ces systèmes peuvent être examinés à partir de deux perspectives distinctes, qui sont les systèmes d'ordre entier et les systèmes d'ordre fractionnaire. Les systèmes chaotiques avec un ordre entier ont des paramètres inférieurs et une structure de base, ce qui les rend facilement fissurés. De l'autre coté, les systèmes chaotiques fractionnaires ont des propriétés dynamiques plus complexes ainsi que plus de paramètres qui peuvent être utilisés comme clé dans le schéma de cryptage, ce qui augmente l'espace clé et la complexité, ce qui rend le cryptage plus sécurisé.

Plusieurs techniques de chiffrement des images utilisant le chaos ont été proposées dans la littérature. Li et al [68] créent une approche de chiffrement d'image utilisant un hyper-chaos avec l'ordre fractionnaire et le calcul d'ADN , où ils ont intégré la carte du chaos avec la base d'ADN complémentaire pour obtenir l'image chiffrée. Kaur et al [92] ont développé une nouvelle approche qui utilise le chaos et une transformation Hartley fractionnaire qui est contrôlée par une autre carte chaotique pour donner une excellente sécurité du système de cryptage. Lai et al [93] ont développé la technique "pixel-split" pour le chiffrement des images. Cette approche utilise un mécanisme d'échange des pixels qui peut modifier à la fois l'emplacement et la valeur des pixels. Chai et al [94] ont proposé un schéma amélioré qui applique d'abord un traitement parcimonieux à l'image simple, suivi de brouillage en zigzag. Ensuite, la technique de détection compressée (CS) est utilisée pour compresser et chiffrer simultanément l'image brouillée. Dans leur approche du chiffrement des images, Yousif et al [95] ont utilisé diverses cartes chaotiques dans le but d'améliorer la sécurité tout en veillant à ce que les performances de traitement restent à un niveau élevé. Muhammad et al [96] offraient une technique améliorée qui utilisait l'algorithme DES et huit structures S-box pour augmenter leur complexité. Lorsqu'elle est combinée avec Zigzag,

cette approche offre une sécurité particulièrement forte pour le cryptage des images. Wang et al [97] ont utilisé la transformation 3D Zigzag pour permuter l'image simple et ont comparé son efficacité avec d'autres transformations, y compris Arnold, décalage circulaire et Zigzag standard. La comparaison a montré que la transformation en zigzag 3D produit un meilleur effet de permutation. Cependant, certains schémas de cryptage des images basés sur le chaos ont des inconvénients notables, tels qu'une sensibilité limitée à l'image simple, ce qui implique qu'ils sont vulnérables à certains agressions, telles que les attaques de texte en clair choisi et de texte en clair connu. Dou et al [98] déterminent que le schéma de chiffrement décrit dans [99] est vulnérable à une attaque de texte en clair choisie car il n'est pas lié à l'image en clair. Selon [100], l'approche de chiffrement décrite dans [101] a été fissurée par une attaque en clair choisi. De même, le schéma [102] était vulnérable à une attaque en clair choisie [103] puisque la clé de chiffrement n'était pas liée à l'image en clair.

Ce chapitre présente un nouveau système de cryptage qui combine une nouvelle technique de zigzag et un système chaotique tridimensionnel avec un ordre fractionnaire. Contrairement aux schémas de cryptographie existants dans la littérature qui s'appuient sur un seul type de zigzag, notre méthode introduit une approche unique d'appliquer plusieurs types de zigzag simultanément. Ce type de zigzag est hautement imprévisible puisqu'il est contrôlé par un système chaotique 3D à ordre fractionnaire. L'incorporation de ce système a pour but d'augmenter la complexité de l'algorithme de chiffrement, ce qui à son tour améliore la sécurité du système et le rend plus résistant aux attaques. La valeur de hachage SHA-512 de l'image simple est utilisée pour établir les valeurs initiales du système chaotique d'ordre fractionnaire afin d'éviter les attaques en clair choisies.

5.2 Analyses du système chaotique d'ordre fractionnaire

Il existe différentes définitions de la dérivée fractionnaire d'ordre $q > 0$, mais la formulation de Caputo est la plus largement utilisée dans la modélisation des systèmes d'ordre fractionnaire. Le problème de la valeur initiale (IVP) d'un système d'ordre fractionnaire est défini à l'aide de la dérivée de Caputo comme suit [8] :

$$D^q x(t) = f(x(t)), x(0) = x_0. \tag{5.1}$$

Où x_0 est la condition initiale, f est une fonction non linéaire continue de Lipschitz et D^qest l'opérateur d'ordre différentielle de Caputo $0 < q < 1$. Ensuite, le système (5.1) est décrit comme ayant un ordre proportionnel ; sinon, il est décrit comme ayant un ordre non proportionnel. D^q est donné par :

$$D^q x(t) = \frac{1}{\Gamma(m-q)} \int_0^t \frac{x^m(\tau)}{(t-\tau)^{q+1-m}} d\tau, m-1 < q < m \tag{5.2}$$

Où m est le plus petit entier supérieur à q, $x(m)$ est la dérivée normale d'ordre m et Γ est la fonction Gamma d'Euler. Pour évaluer l'équation différentielle fractionnaire (5.1), des méthodes d'approximation numérique telles que Grünwald-Letnikov, Riemmann-Liouville et le prédicateur-correcteur Adams-Bashforth-Moulton (ABM) peuvent être utilisés.

Afin d'augmenter la complexité du système de cryptage, nous avons utilisé le système de Chen d'ordre fractionnaire comme générateur des nombres aléatoires. Il est caractérisé par une dynamique plus complexe et riche par rapport à son ordre entier contrepartie. Il est décrit par [8] :

$$\begin{cases} D^{q1}x(t) = a(y-x) \\ D^{q2}y(t) = (c-a)x - xz + cy \\ D^{q3}z(t) = xy + bz \end{cases} \tag{5.3}$$

où D^{q1} désigne l'opérateur différentiel de Caputo , x, y et z désignent les variables dépendantes du système , et a, b et c désignent les paramètres du système.

5.2.1 Diagramme de bifurcation

Le diagramme de bifurcation est un outil utile pour évaluer visuellement le comportement qualitatif des systèmes chaotiques. Il démontre comment un paramètre de contrôle qualitatif affecte le comportement du système. Le diagramme de bifurcation du système Chen avec ordre fractionnaire est illustré à la figures 5.1(a-c). La région pointillée dans le diagramme signifie que le système est dans un état de chaos, tandis que la zone vide démontre que le comportement du système n'est pas chaotique. En fixant $q1 = q2 = 1, q3 = 0,8$, $b = 3$ et $c = 28$, puis en faisant varier la valeur de a, le diagramme de bifurcation du système est illustré à la figure 5.1 (a).comme le montre le diagramme, on peut voir que le comportement chaotique peut se produire dans le système lorsqu'un $a \in [36, 47]$. En choisissant $q1 = q2 = 1, q3 = 0,8, a = 40$ et $c = 28$, puis en ajustant b, le diagramme de bifurcation s'affiche à la figure5.1 (b). L'examen de cette figure révèle que le système peut se comporter de façon chaotique lorsque $b \in [0, 8, 5]$. En définissant $q1 = q2 = 1, q3 = 0.8, b = 3, eta = 40$, puis en changeant la valeur de c, le diagramme de bifurcation du système est présenté à la figure 5.1 (c). de la figure précédente , on peut déduire que lorsque $c \in [23, 32]$, le comportement chaotique peut se manifester dans le système.

5.2.2 L'exposant de Lyapunov

L'exposant de Lyapunov est un instrument crucial pour comprendre les subtilités du chaos. Il donne un aperçu dans le niveau du chaos dans les systèmes dynamiques. Les valeurs positives de l'exposant de Lyapunov signifient le chaos dans le système, ce qui finira par conduire à une

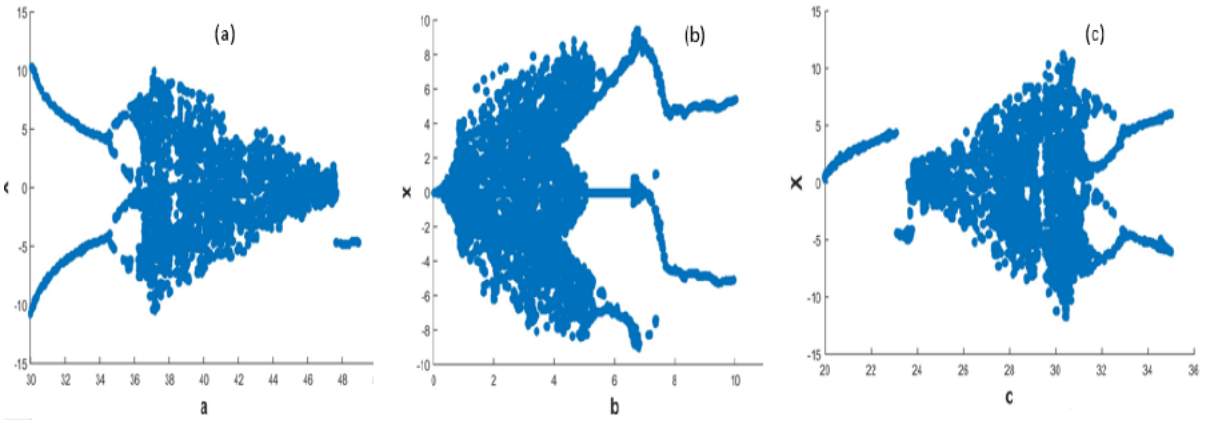


FIG. 5.1 *le diagramme de bifurcation du système Chen fractionnaire.*

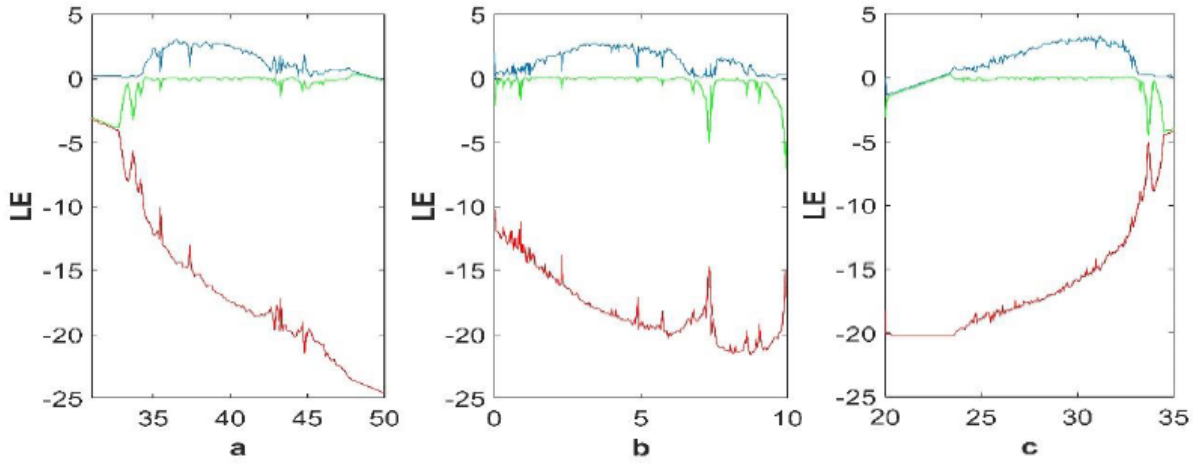


FIG. 5.2 *L'exposant Lyapunov du système Chen fractionnaire.*

imprévisibilité totale. La formule de l'exposant de Lyapunov se présente comme suit :

$$ly = \lim_{n \to +\infty} \frac{1}{n} \sum_{i=1}^{N} ln \left| f(x_i') \right| \tag{5.4}$$

Où $f(xi)'$ représente la fonction dérivée du système chaotique. L'exposant Lyapunov du système Chen avec ordre fractionnaire est représenté sur la figure 5.2 (a-c). Les spectres des exposants de Lyapunov sont en bon accord avec les diagrammes de bifurcation. Sur la base de l'analyse ci-dessus, on peut conclure que le système Chen d'ordre fractionnaire présente un comportement chaotique souhaitable.

5.3 Cryptosystème proposé

Dans cette section, nous présentons notre nouveau système de cryptage qui intègre un système chaotique d'ordre fractionnaire tridimensionnel et une nouvelle méthode de zigzag.

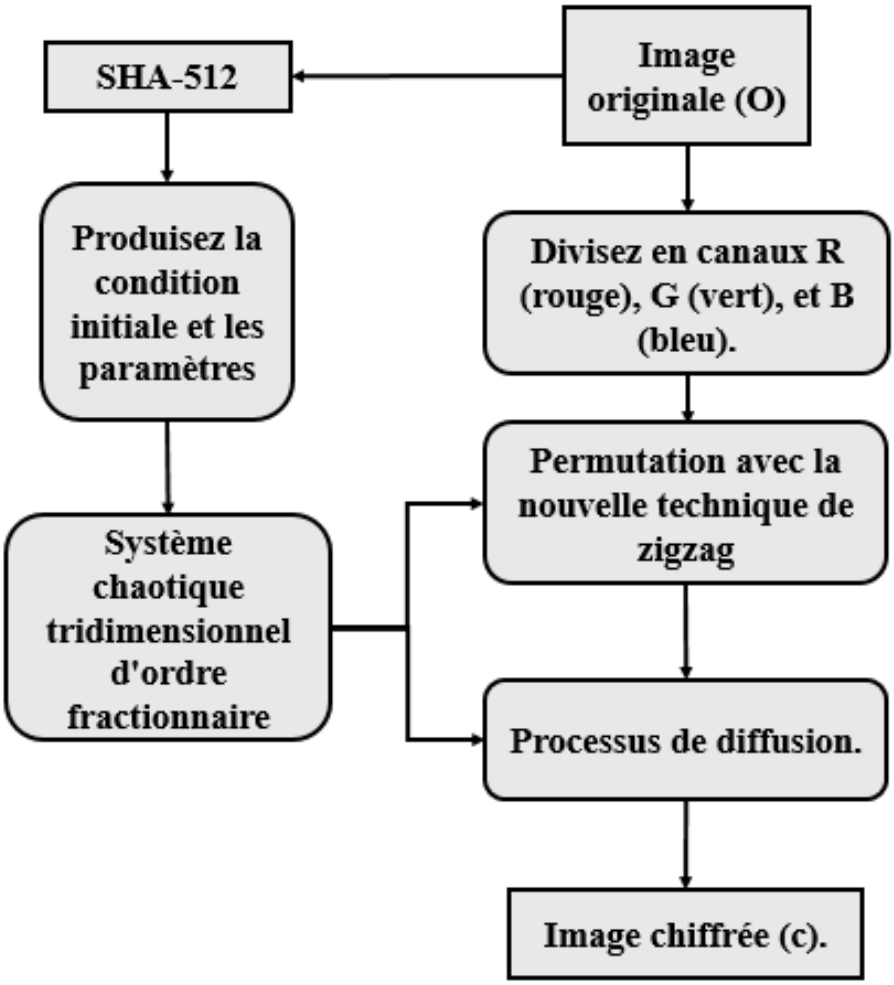


FIG. 5.3 *L'organigramme du système de cryptage proposé.*

Notre approche génère plusieurs groupes des motifs en zigzag en utilisant le système chaotique d'ordre fractionnaire pour modifier les emplacements des pixels de l'image. L'une des forces de notre algorithme est sa capacité à utiliser simultanément divers motifs en zigzag, ainsi que le caractère aléatoire de leur création, ce qui le rend très imprévisible. Cette fonctionnalité améliore la sécurité du système de cryptage et le rend plus résilient contre diverses attaques. La valeur d'hachage SHA-512 de l'image simple est utilisée pour calculer les valeurs initiales du système chaotique d'ordre fractionnaire. La figure 5.3 illustre l'algorithme proposé. Les étapes suivantes décrivent les spécificités du schéma de chiffrement :

— **Étape 1 :** L'image simple O de taille $m \times n \times 3$ est lue, puis elle est partitionnée en trois parties constitutives(R, G et B).

— **Étape 2 :** Nous appliquons l'équation 5.3 en utilisant les paramètres a, b, c, les conditions initiales x_0, y_0 et z_0, ainsi que les paramètres d'ordre fractionnaire q_1, q_2 et q_3 pour générer trois séquences des valeurs aléatoires dénotées par x, y et z de taille $m \times n$. Les conditions initiales sont créées par le hash SHA-512.

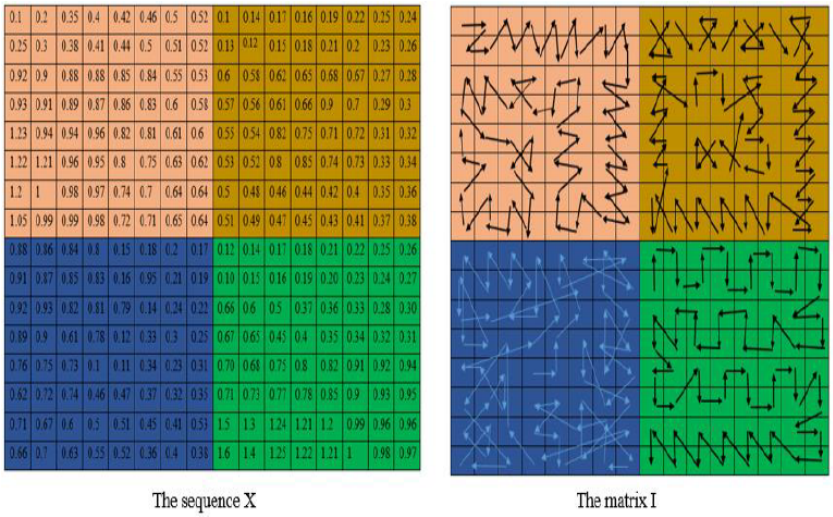


FIG. 5.4 *Création de divers motifs en zigzag : un exemple numérique.*

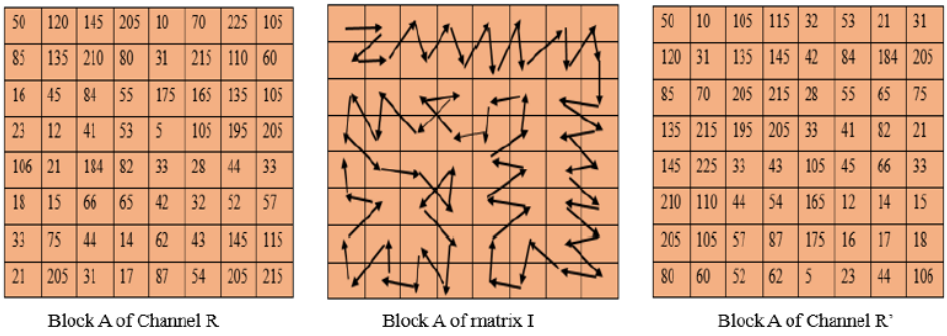


FIG. 5.5 *processus de permutation utilisant divers motifs en zigzag.*

— **Étape 3 :** Nous transformons la séquence aléatoire x en matrice I, qui est ensuite divisée en blocs 8×8. Nous avons ensuite triez les éléments de chaque bloc par ordre croissant pour créer une variété des motifs en zigzag. La figure 5.4 illustre un exemple de ce processus.

— **Étape4 :** On utilise les séquences Y et Z pour créer une nouvelle séquence de taille égale au nombre de blocs dans la matrice I. Ensuite, nous transformons cette séquence en une matrice J et organisons ses éléments par ordre croissant pour former un nouveau zigzag.

— **Étape5 :** On partitionne les canaux (R, G et B) de l'image originale O en blocs de taille $8x8$.

— **Étape6 :** En utilisant les différents motifs en zigzag générés à partir de la matrice I, nous modifions les emplacements des pixels dans chaque bloc des canaux R, G et B. Ce processus consiste à appliquer les motifs en zigzag à chaque canal pour modifier le placement des pixels individuels. Cette procédure est présentée dans la figure 5.5.

— **Étape7 :** Nous utilisons les motifs en zigzag créés à partir de la matrice J pour modifier le placement des blocs dans chacun des canaux R', G' et B'. Les canaux R, G et B modifiés qui en résultent sont appelés canaux brouillés $(R_s, G_s et B_s)$. Cette procédure est présentée

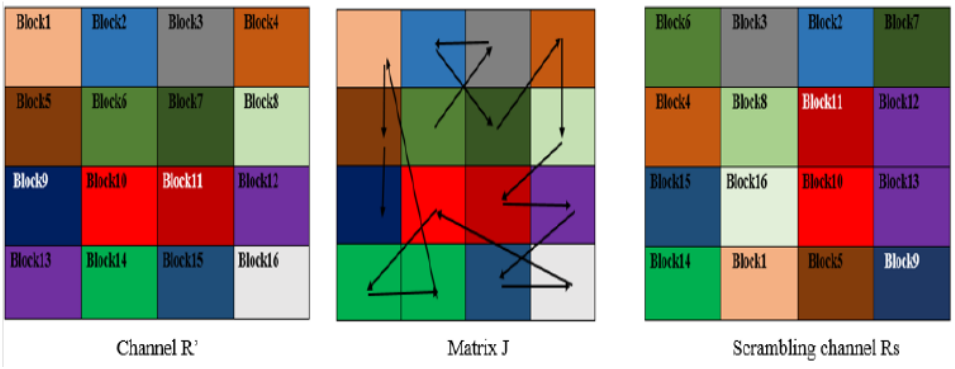


FIG. 5.6 *Processus de permutation des blocs.*

dans la figure 5.6.

— **Étape8 :** Nous obtenons trois clés en appliquant l'équation 5.3 avec les valeurs initiales de (a, b, c), $q'_1, q'_2 et q'_3$ et ($x_1, y_1 et z_1$). Une fois ces clés obtenues, nous les transformons en nombres entiers.

$$\begin{cases} key1 = floor(x(i) \times 10^{15}) mod 256. \\ key2 = floor(y(i) \times 10^{15}) mod 256 \\ key3 = floor(z(i) \times 10^{15}) mod 256 \end{cases} \tag{5.5}$$

— **Étape9 :** Nous convertissons les canaux brouillés $(R_s, G_s et B_s)$ en vecteurs et effectuons ensuite une opération XOR entre les clés et les vecteurs brouillés pour obtenir des vecteurs chiffrés comme suit :

$$\begin{cases} R_e(i) = R_{s1d}(i) \oplus key_1(i) \oplus R_{s1d}(i-1). \\ G_e(i) = G_{s1d}(i) \oplus key_2(i) \oplus G_{s1d}(i-1) \\ B_e(i) = B_{s1d}(i) \oplus key_3(i) \oplus B_{s1d}(i-1) \end{cases} \tag{5.6}$$

Où $R_e, G_e et B_e$ sont les vecteurs chiffrés.

— **Étape10 :** Une fois que nous avons obtenu les vecteurs chiffrés $R_e, G_e et B_e$, nous les reconvertissons en matrices. On peut alors utiliser ces matrices pour construire l'image cryptée.

5.4 Résultats de la simulation

Notre configuration de test comprenait une machine avec 8 Go de mémoire et un processeur Intel (R) Core (TM) i7-7500u fonctionnant à 2,90 GHz. Le logiciel utilisé était MATLAB R2021a. Nous avons testé les performances de notre méthode suggérée sur 4 ensembles des

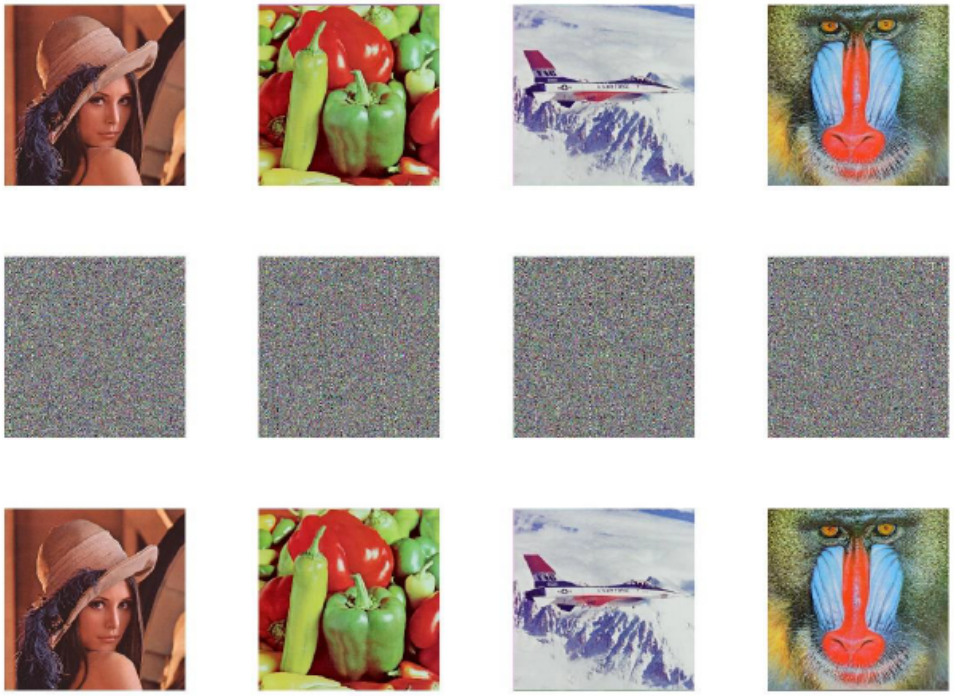


FIG. 5.7 *Résultats de chiffrement et de déchiffrement (Lena, poivrons, avion, babouin).*

données des images ayant 512×512×3 dimensions. Pour démontrer l'efficacité de notre méthode, nous avons comparé nos résultats avec ceux d'autres schémas de chiffrement de la littérature. La figure 5.7 illustre les résultats du cryptage d'image et la procédure de déchiffrement.

5.4.1 Analyse de l'espace clé

La taille de l'espace clé est une mesure de la capacité d'un algorithme de chiffrement à résister aux attaques violentes. Généralement, une méthode de chiffrement efficace doit avoir un espace clé d'au moins 2^{100} [61]. La clé de notre schéma de cryptage est construite sur des sous-clés dans sa structure principale, qui sont basées sur des conditions initiales, des paramètres de contrôle et des paramètres d'ordre fractionnaire du système chaotique. Différent valeurs sous-clé ont été mis en oeuvre dans les deux processus de la permutation et de la diffusion. Donc, la clé de notre schème comprend un total de18 éléments, comme suit :

— Les conditions initiales $(x_0, y_0 etz_0)$ et $(x_1, y_1 etz_1)$.

— Les paramètres de contrôle $(a_0, b_0 etc_0)$ et $(a_1, b_1 etc_1)$.

— Les paramètres d'ordre fractionnaire $(q_1, q_1 etq_1)$ et $(q'_1, q'_1 etq'_1)$.

Sur la base de nos résultats expérimentaux, chaque élément dans l'espace clé a une taille d'environ 10^{15}. Ainsi, l'espace de clé de l'algorithme de cryptage suggéré est de $10^{15\times18=270}$. Notre système de cryptage dispose d'un espace clé suffisamment grand, rendant extrêmement difficile pour les pirates de lancer des attaques violentes et de compromettre la sécurité du

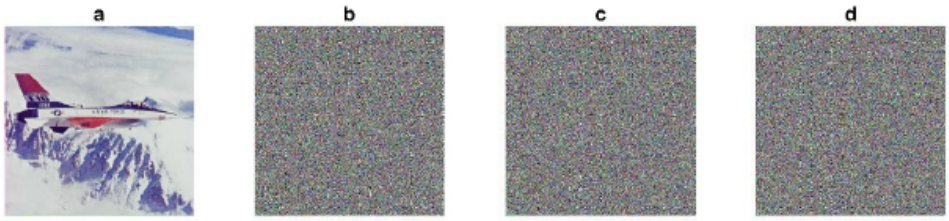


FIG. 5.8 *Le test de sensibilité de clé de l'image déchiffrée (a) clé correcte (b) mauvaise q_1 (c) mauvaise b (d) mauvaise x_0.*

système.

5.4.2 Analyse de la sensibilité clé

Pour assurer le chiffrement et le décryptage sécurisés, chaque méthode de chiffrement doit être très sensible à la clé de chiffrement. Même une modification mineure dans l'un des composants clés peut rendre l'image déchiffrée complètement invisible, ce qui entraîne un échec de déchiffrement. Nous avons évalué la sensibilité de notre clé en modifiant la valeur d'un élément clé par un petit pourcentage de10^{-15}. Les résultats obtenus sont illustrés à la figure 5.8. Comme en témoigne clairement l'image décryptée, elle ne fournit aucune information utile sur l'image originale, démontrant la grande sensibilité de la technique suggérée à la clé de cryptage. Il est donc très difficile pour les attaquants de déchiffrer l'image originale, car même le moindre écart par rapport à la clé correcte entraînera une image déchiffrée complètement différente et rendant leurs efforts inutiles.

5.4.3 Analyse d'histogramme

Un histogramme fournit une représentation visuelle de la distribution des pixels dans une image. Lorsque l'histogramme d'une image chiffrée n'est pas uniforme, elle peut exposer des modèles aux attaquants, rendant l'image vulnérable aux attaques statistiques. Par conséquent, avoir un histogramme plat (uniforme) est essentiel pour un système de cryptage sécurisé. Pour assurer la sécurité des images, nous avons effectué une analyse approfondie des histogrammes des images originales et cryptées. La figure 5.9 montre les histogrammes de l'image du poivre et de son image chiffrée.La figure5.9 illustre clairement que l'histogramme de l'image chiffrée est uniformément distribuée et remarquablement distincte de celle de l'image originale. Cela indique que notre approche proposée empêche efficacement les attaquants d'obtenir toute information statistique qui pourrait être utilisée pour lancer des attaques statistiques et rend impossible de déterminer la connexion entre la distribution de pixels de l'image originale et l'image cryptée.

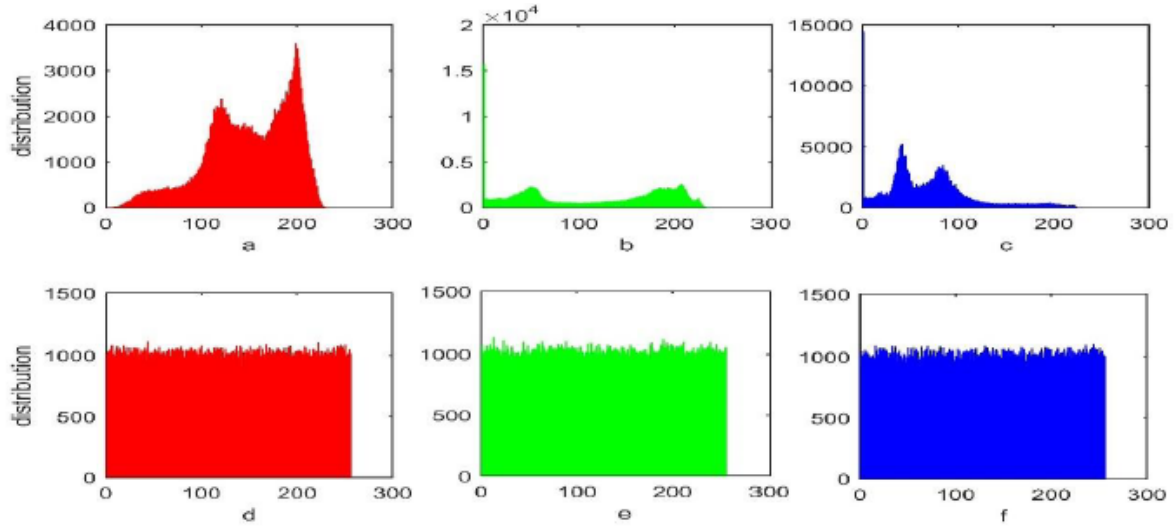


FIG. 5.9 *Histogramme de l'image des poivrons et de l'image chiffrée (a)-(c) histogramme des canaux R, G, B de l'image simple (d)-(f) histogramme de Canaux R, G, B de l'image chiffrée .*

TABLE 5.1 *Résultats d'entropie".*

Image	Images clair	Notre méthode	Ref[87]	Ref [89]	Ref [91]
Lena	7,4767	**7.9998**	7.9996	7.9992	7.99746
Peppers	7.6698	**7.9997**	7.9995	7.9912	7.99423
plane	6.7174	**7.9998**	7.9998	7.9996	7.99664
Baboon	7.7624	**7.9997**	7.9997	7.9974	7.99494

5.4.4 Analyse d'entropie

L'entropie de l'information est une mesure essentielle pour évaluer la sécurité d'une méthode de chiffrement, car elle quantifie le contenu informatif moyen d'une image numérique. De plus, il donne un aperçu du caractère aléatoire et imprévisible de l'image cryptée[61]. La formule (2.3) est utilisée pour déterminer l'entropie de l'image. La valeur d'entropie de l'information acquise par l'approche de chiffrement doit être aussi proche que possible de huit. Plus la valeur obtenue est proche de huit, plus le système de cryptage est sécurisé. Le tableau 5.1 présente les résultats d'entropie de notre méthode et montre clairement que l'entropie de l'information pour toutes les images cryptées est remarquablement élevée, avec des valeurs proches du maximum théorique huit. De plus, nous avons comparé l'entropie d'information de notre algorithme proposé avec plusieurs autres algorithmes. Notre approche proposée présentait une valeur d'entropie de l'information plus élevée, indiquant une performance supérieure et un niveau de sécurité plus élevé.

Table 5.2 *Résultats des coefficients de corrélation.*

Images		Canal R			Canal G			Canal B		
		H	V	D	H	V	D	H	V	D
notre méthode	Lena	0.0009	-0.0007	-0.0015	-0.0019	0.0012	0.0021	0.0001	-0.0002	-0.0017
	Pepper	-0.0027	0.0041	-0.0004	0.0022	-0.0005	-0.0001	0.0021	-0.0009	-0.0001
	Plane	0.0037	0.0012	0.0002	-0.0030	0.0014	-0.0007	0.0026	0.0012	-0.0010
	Baboon	-0.0022	-0.0018	0.0048	0.0042	0.0018	-0.0004	0.0012	-0.0012	0.0019
Ref [[84]]	Lena	-0.0002	-0.0023	-0.0021	-0.00029	-0.0043	0.007	0.0074	-0.0010	-0.0007
	Pepper	-0.0008	-0.0067	-0.0069	0.0007	0.0072	-0.0048	0.0006	-0.0043	-0.0007
	Plane	-0.0032	-0.0053	0.0047	-0.0008	-0.0021	-0.0002	0.0030	-0.0006	0.0015
	Baboon	-0.0045	-0.0002	0.0014	0.005	0.0029	0.0005	0.0006	0.0001	0.0022
Ref [[86]]	Lena	-0.0022	0.0009	0.0013	0.0057	-0.0041	0.0017	0.0007	0.0004	0.0104
	Pepper	-0.0038	-0.0026	-0.0187	0.0014	0.0038	0.0058	-0.0094	0.0035	0.0035
	Plane	0.0006	0.0013	0.0023	0.0023	0.0010	-0.0057	0.0009	-0.0017	0.0083
	Baboon	0.0049	0.0006	0.0021	-0.0026	-0.010	0.0147	0.0068	0.0038	-0.0040

5.4.5 Coefficient de corrélation

L'analyse de corrélation est une métrique cruciale utilisée pour évaluer les performances des méthodes de chiffrement des images. C'est largement reconnu que les pixels d'une image sont fortement corrélés horizontalement, verticalement et en diagonale les uns avec les autres. Par conséquent, des algorithmes de cryptage puissants sont nécessaires pour rompre cette association entre les pixels. Le coefficient de corrélation peut être définie par l'équation (2.4).

Le tableau 5.2 compare les résultats du coefficient de corrélation acquis à partir de notre algorithme à ceux obtenus à partir d'autres méthodes de chiffrement examinées dans la littérature et montre que l'image cryptée a des valeurs de corrélation beaucoup plus faibles dans toutes les directions. De plus, en termes de valeurs de coefficient de corrélation, notre technique de chiffrement proposée surpasse les méthodes de référence. Ce qui implique que notre méthode est plus robuste pour prévenir les attaques statistiques.

5.4.6 Résistance à l'attaque différentielle

L'attaque différentielle est largement reconnue comme une stratégie très réussie parmi les différents types d'attaques. Les attaquants utilisent souvent cette méthode pour discerner la relation entre une image originale et chiffrée en évaluant le taux de changement de chaque pixel dans une image chiffrée. Pour prévenir de telles agressions, un système de cryptage d'image doit être capable de résister aux attaques différentielles. Pour évaluer la robustesse des méthodes de chiffrement des attaques différentielles, le taux de changement du nombre de pixels (NPCR) et l'intensité de changement moyenne uniforme (UACI) sont largement appliqués. Lorsqu'on compare deux images cryptées avec des entrées légèrement variables, NPCR révèle la proportion des pixels qui changent, tandis que UACI mesure la différence moyenne des valeurs des pixel. Les formules utilisées pour calculer le NPCR et l'UACI sont les suivantes :

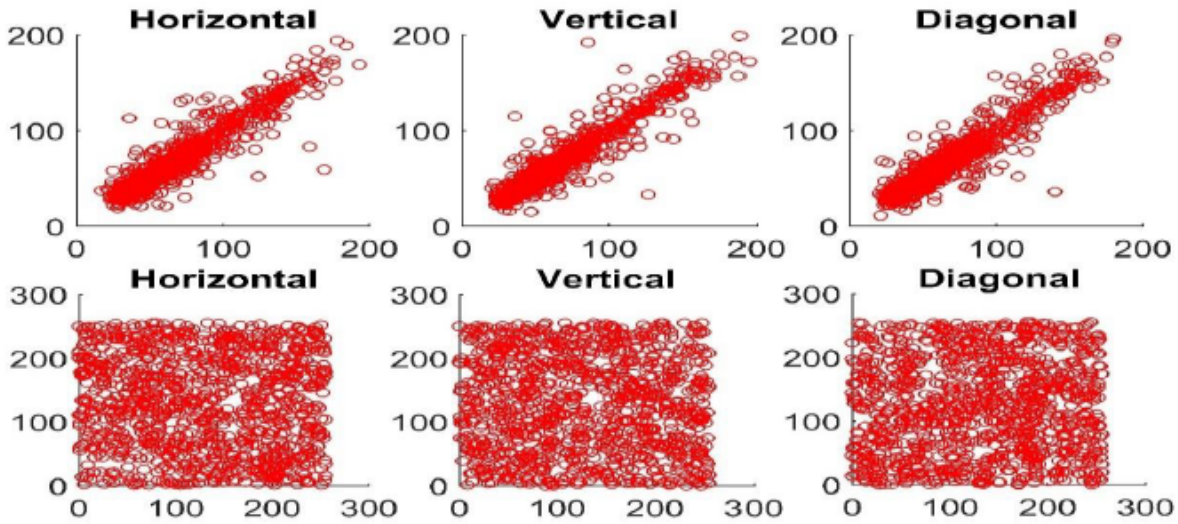


FIG. 5.10 *Distribution des pixels voisins des poivrons dans différentes directions .*

$$\begin{cases} NPCR = \frac{1}{L}\sum D(i,j) \times 100\% \\ UACI = \frac{1}{L}\sum \frac{c_1(i,j)-c_2(i,j)}{255} \times 100\% \end{cases} \tag{5.7}$$

Où L représente le nombre total des pixels. C1 et C2 sont les valeurs des pixels initiales et modifiées, respectivement. Les règles suivantes doivent être suivies pour déterminer D (i, j) :

$$D(i,j) = \begin{cases} 0 & c_1(i,j) = c_2(i,j) \\ 1 & c_1(i,j) \neq c_2(i,j) \end{cases} \tag{5.8}$$

La littérature indique que les valeurs les plus souhaitables pour le NPCR et l'UACI sont 99,6094 et 33,4635, respectivement. Pour évaluer l'efficacité de notre méthode contre les attaques différentielles, nous avons apporté une petite modification à l'image originale en modifiant un seul pixel. Ensuite on calcule les valeurs NPCR et UACI ultérieures. Le tableau 5.3 affiche les résultats du test. Les résultats de notre schéma démontrent que le schéma de chiffrement proposé fonctionne nettement mieux que les autres algorithmes de la littérature. Sur la base de l'analyse des résultats du NPCR et de l'UACI, notre méthode a montré un niveau de performance beaucoup plus proche des valeurs recommandées, ce qui signifie que le système est capable de résister aux attaques différentielles.

5.4.7 Perte des données et des attaques par bruit

Inévitablement, lors de la transmission d'une image à travers un canal, elle peut rencontrer des interférences sonores ou perte des données. Pour tester la capacité de l'algorithme de chiffrement proposé à résister à de telles perturbations. Nous avons introduit le sel et le bruit de poivre à

TABLE 5.3 *NPCR et UACI de diverses images cryptées.*

	NPCR(%)				UACI(%)			
Images	Lena	Pepper	Plane	Baboon	Lena	Pepper	Plane	Baboon
Notre méthode	**99.60**	**99.60**	**99.61**	**9.60**	**33.44**	**33.46**	**33.48**	**33.44**
Ref[91]	99.645	99.61	99.583	99.627	33.56	33.58	33.61	33.547
Ref [86]	99.615	99.61	99.61	99.61	33.43	33.43	33.48	33.44

FIG. 5.11 *Processus de déchiffrement utilisant différents niveaux de nez poivre et sel.*

différents niveaux de 1%, 5% et 10% sur les images cryptées. Nous avons ensuite examiné la qualité des images décryptées et montré nos résultats à la figure 5.11. De plus, nous avons effectué un test où l'image cryptée a été coupés à différentes tailles et déchiffrés à l'aide de la bonne clé. La figure 5.12 illustre les résultats de ce test. Ces expériences nous ont aidés à déterminer la capacité des algorithmes de chiffrement à gérer la corruption d'image causée par le bruit et la perte des données. Nos résultats indiquent que même si une quantité importante de bruit est injectée dans l'image cryptée ou certaines données sont perdues pendant la transmission, notre système peut récupérer efficacement les informations essentielles de l'image originale à partir de l'image déchiffrée. Les résultats montrent que nos techniques sont extrêmement adaptables à une variété de situations réelles dans lesquelles les données peuvent être sensibles à diverses sortes d'interférences. En fait, notre algorithme est résistant aux attaques de bruit et à la perte des données, ce qui le rend idéaux pour les applications nécessitant la sécurité et l'intégrité des données.

5.5 Conclusion

Dans ce chapitre, nous proposons une stratégie de cryptage d'image qui utilise des systèmes chaotiques d'ordre fractionnaire en combinaison avec une nouvelle technique en zigzag. Notre technique utilise plusieurs types de zigzag pendant le processus de permutation, chaque zigzag étant contrôlé par un système chaotique d'ordre fractionnaire pour améliorer la sécurité du schéma en le rendant plus imprévisible. La clé de cryptage est déterminée par l'ordre fractionnaire et la valeur initiale du système chaotique, augmentant la complexité et l'espace clé du schéma. Nos simulations de performances démontrent que notre méthode présente des caractéristiques

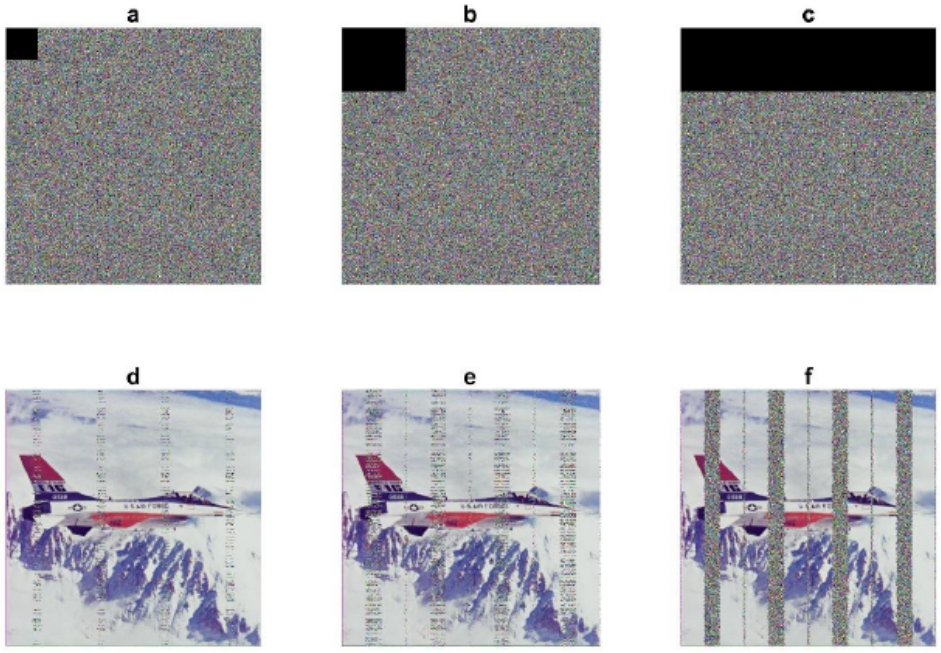


FIG. 5.12 *Analyse des attaques par perte des données (a)* 64×64 *, perte des données (b)* 128×128 *et perte des données (c)* 128×512 .

supérieures, notamment un large espace de clé, une sensibilité aux changements de clé mineurs et une faible corrélation par rapport aux algorithmes précédents. En outre, il offre une protection renforcée contre les attaques des pirates telles que les attaques statistiques et différentielles.

Chapitre 6

Conclusion générale

Conclusion générale

De nos jours, les chercheurs accordent une grande importance à l'amélioration et à la validation des algorithmes de chiffrement des images. Cela est dû aux caractéristiques uniques des images, qui diffèrent grandement des autres formes des données, telles que le texte. Les images sont généralement de grande taille et présentent une forte corrélation entre les pixels voisins, ce qui rend inadéquate l'utilisation des algorithmes de chiffrement traditionnels tels que Rivest-Shamir-Adleman (RSA), la norme de chiffrement des données (DES) et la norme de chiffrement avancée (AES). En conséquence, il y a eu un intérêt croissant pour l'application des systèmes chaotiques entiers pour crypter les images. Bien que les systèmes chaotiques possèdent des caractéristiques distinctes, ils présentent encore certaines vulnérabilités en termes de protection adéquate.

Cette thèse présente une étude et une analyse approfondie des problèmes de protection des données, notamment liés aux images, et propose des solutions viables utilisant des systèmes chaotiques à ordre fractionnaire. Ces systèmes offrent un champ chaotique plus grand et un nombre accru des paramètres, ce qui les rend plus complexes que les systèmes avec un ordre entier, offrant ainsi une meilleure protection des systèmes de chiffrement. Grâce à cette recherche, nous visons à répondre aux limites des algorithmes de chiffrement traditionnels et à mettre en évidence le potentiel des systèmes chaotiques d'ordre fractionnaire pour offrir des solutions de chiffrement plus robustes et efficaces pour la transmission sécurisée des données.

Nous avons présenté des approches standardisées pour mesurer les performances des générateurs aléatoires, nous permettons d'analyser les propriétés des séquences chaotiques générées par le chaos d'ordre fractionnaire avant de les utiliser pour l'encodage des images.

Nous avons développé ensuite un système avancé de cryptage d'image qui utilise la carte logistique d'ordre fractionnaire. Cette carte offre des performances supérieures par rapport à son homologue traditionnel d'ordre entier. Nos résultats ont été rigoureusement validés par le diagramme de bifurcation et l'exposants de lyapunov, qui ont confirmé l'efficacité de la carte logistique d'ordre fractionnaire. De plus, nous avons utilisé le paramètre d'ordre fractionnaire comme un des éléments clés de chiffrement, améliorant ainsi les mesures de sécurité de notre approche. Le schéma proposé a fait l'objet d'une évaluation approfondie de la sécurité, qui impliquait de le comparer avec des ouvrages connexes. Nos résultats démontrent que notre système surpasse ces travaux en offrant une grande sécurité contre diverses attaques.

Nous avons introduit une carte logistique d'ordre fractionnaire améliorée dans une nouvelle technique de chiffrement des images couleurs. Notre enquête expérimentale sur la conduite chaotique et la portée chaotique a révélé que la carte modifiée surpasse la carte logistique d'ordre fractionnaire traditionnelle dans plusieurs mesures, y compris les tests NIST, l'exposant

de Lyapunov et l'analyse de bifurcation. Ces résultats indiquent que notre carte logistique modifiée avec ordre fractionnaire représente une approche prometteuse pour améliorer la qualité des systèmes de cryptage et pour protéger les données numériques.

Nous avons enfin créé un nouveau système de cryptage des images utilisant une nouvelle approche de zigzag, qui est contrôlée par un système chaotique tridimensionnel avec un ordre fractionnaire. L'objectif principal de cette stratégie est d'augmenter la complexité du schéma de cryptage en utilisant les propriétés uniques d'un système chaotique fractionnaire tridimensionnel, augmentant ainsi l'efficacité et la sécurité de notre schéma contre un large éventail d'agressions possibles. Pour évaluer l'efficacité et la précision de notre schéma suggéré, nous avons effectué une étude approfondie et une comparaison avec des nombreuses recherches antérieures. Nos résultats de tests éprouvés ont démontré que nos méthodes proposées surpassent de nombreuses études antérieures dans ce domaine en termes de performances et de qualité.

Nous nous engageons à faire progresser ce domaine d'étude en poursuivant plusieurs pistes de travail prometteuses :

- ✓ Nous projetons d'améliorer le système chaotique d'ordre fractionnaire tridimensionnel en terme de comportement chaotique.

- ✓ Nous visons à valider l'aspect pratique de notre approche en la mettant en oeuvre dans des systèmes réels tels que les systèmes embarqués basés sur FPGA.

Bibliographie

[1] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve elgamal scheme," *Signal Processing*, vol. 141, pp. 109–124, 12 2017.

[2] A. Jolfaei, X. W. Wu, and V. Muthukkumarasamy, "On the security of permutation-only image encryption schemes," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 235–246, 2 2016.

[3] N. A. Hikal and M. M. Eid, "A new approach for palmprint image encryption based on hybrid chaotic maps," *Journal of King Saud University - Computer and Information Sciences*, vol. 32, pp. 870–882, 9 2020.

[4] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Processing*, vol. 148, pp. 124–144, 2018.

[5] X. Wang, C. Liu, D. Xu, and C. Liu, "Image encryption scheme using chaos and simulated annealing algorithm," *Nonlinear Dynamics*, vol. 84, pp. 1417–1429, 5 2016.

[6] O. MEGHERBI, *Synchronisation des systèmes chaotiques discrets d'ordre fractionnaire pour la sûreté de communication à base d'observateurs impulsifs*. PhD thesis, Université Mouloud Mammeri de Tizi Ouzou,Algerie, 2018.

[7] E. N. Lorenz, "Deterministic Nonperiodic Flow.," *Journal of the Atmospheric Sciences*, vol. 20, pp. 130–148, Mar. 1963.

[8] J.-C. Nunez-Perez, V.-A. Adeyemi, Y. Sandoval-Ibarra, F.-J. Perez-Pinal, and E. Tlelo-Cuautle, "Maximizing the chaotic behavior of fractional order chen system by evolutionary algorithms," *mathematics*, vol. 9, p. 1194., 2021.

[9] R. Sujarani, D. Manivannan, R. Manikandan, and B. Vidhyacharan, "Lightweight bio-chaos crypt to enhance the security of biometric images in internet of things applications," *Wireless Personal Communications*, vol. 119, pp. 2517–2537, 8 2021.

[10] H.-J. Chen, Q.-X. Ji, H. Wang, Q.-F. Yang, Q.-T. Cao, Q. Gong, X. Yi, and Y.-F. Xiao, "Chaos-assisted two-octave-spanning microcombs," *Nat Commun*, vol. 11, p. 2336, 2020.

[11] Z. W. Peng, W. X. Yu, J. N. Wang, J. Wang, Y. Chen, X. K. He, and D. Jiang, "Dynamic analysis of seven-dimensional fractional-order chaotic system and its application in encrypted communication," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 5399–5417, 11 2020.

[12] J. Lian, W. Yu, K. Xiao, and W. Liu, "Cubic spline interpolation-based robot path planning using a chaotic adaptive particle swarm optimization algorithm," *Mathematical Problems in Engineering*, vol. 2020, 2020.

[13] V. L. Freitas, S. Yanchuk, M. Zaks, and E. E. Macau, "Synchronization-based symmetric circular formations of mobile agents and the generation of chaotic trajectories," *Communications in Nonlinear Science and Numerical Simulation*, vol. 94, 3 2021.

[14] L. Liu, Q. Zhang, D. Wei, G. Li, H. Wu, Z. Wang, B. Guo, and J. Zhang, "Chaotic ensemble of online recurrent extreme learning machine for temperature prediction of control moment gyroscopes," *Sensors*, vol. 20, no. 17, 2020.

[15] Z. Shirzhiyan, A. Keihani, M. Farahi, E. Shamsi, M. GolMohammadi, A. Mahnam, M. R. Haidari, and A. H. Jafari, "Introducing chaotic codes for the modulation of code modulated visual evoked potentials (c-vep) in normal adults for visual fatigue reduction," *PLoS ONE*, vol. 14, 3 2019.

[16] M. S. Tavazoei and M. Haeri, "Chaos control via a simple fractional-order controller," *Physics Letters, Section A : General, Atomic and Solid State Physics*, vol. 372, pp. 798–807, 2 2008.

[17] P. Zaccagnini, L. Baudino, A. Lamberti, A. L. Alexe-Ionescu, G. Barbero, L. R. Evangelista, and C. F. Pirri, "Electrode polarization in the presence of a first order ionic trapping reaction," *Journal of Electroanalytical Chemistry*, vol. 918, 8 2022.

[18] D. Craiem and R. Magin, "Fractional order models of viscoelasticity as an alternative in the analysis of red blood cell (rbc) membrane mechanics," *Physical biology*, vol. 7, p. 13001, 03 2010.

[19] S. Patnaik, J. P. Hollkamp, S. Sidhardh, and F. Semperlotti, "Fractional order models for the homogenization and wave propagation analysis in periodic elastic beams," *Meccanica*, vol. 57, pp. 757–773, 4 2022.

[20] B. Hanane, *contribution a la commande adaptative et robuste d'ordre fractionnaire des processus industriels*. PhD thesis, Université Larbi Ben Mhidi de Oum ElBouaghi,Algerie, 2021.

[21] A. khalouta, *Résolution Des équations Aux Dérivées Partielles Linéaires Et Non-linéaires Moyennant Des Approches Analytiques : Extension Aux Cas D'edp D'ordre Fractionnaire*. PhD thesis, Université Ferhat Abbas Setif 1,Algerie, 2019.

[22] H. Tarek, *Analyse du Chaos dans un Système d'équations Différentielles Fractionnaires*. PhD thesis, Université constantine 1,Algerie, 2014.

[23] K. RABAH, *Contribution à la Modélisation et la Commande des Systèmes Chaotiques d'ordre Fractionnaire*. PhD thesis, Université du 20 aout 1955 skikda,Algerie, 2018.

[24] C. Li, D. Qian, and Y. Chen, "On riemann-liouville and caputo derivatives," *Discrete Dynamics in Nature and Society*, vol. 2011, 2011.

[25] H. Poincare, "Sur le probleme des trois corps et les equations de la dynamique," *Acta mathematica*, 1890.

[26] S. Zhu, X. Deng, W. Zhang, and C. Zhu, "A new one-dimensional compound chaotic system and its application in high-speed image encryption," *Applied Sciences (Switzerland)*, vol. 11, 12 2021.

[27] F. Kais, *Analyse spectrale des signaux chaotiques.* PhD thesis, Institut National des Sciences Appliquees de Toulouse,France, 2014.

[28] M. F. Danca, "Puu system of fractional order and its chaos suppression," *Symmetry*, vol. 12, 3 2020.

[29] K. Sun, S. He, and H. Wang, "Solution and characteristic analysis of fractional-order discrete chaotic system," 2022.

[30] S. He, K. Sun, and H. Wang, "Dynamics of the fractional-order lorenz system based on adomian decomposition method and its dsp implementation," *IEEE/CAA Journal of Automatica Sinica*, 11 2016.

[31] F. E. A. El-Samie, H. Eldin, H. Ahmed, I. F. Elashry, M. H. Shahieen, O. S. F. U. El-Sayed, M. El-Rabaie, and S. A. Alshebeili, *Image encryption : a communication perspective*. Taylor and Francis Group, LLC, 2014.

[32] B. TOUFIK, *Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes*. PhD thesis, Université FERHAT Abbas SETIF,Algerie, 2018.

[33] C. Li and K. T. Lo, "Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Processing*, vol. 91, pp. 949–954, 2011.

[34] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using rt-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 3 2018.

[35] R. T. Mohammed Abutaha, Mousa Farajallah and M. Odeh, "Survey paper : Cryptography is the science of information security," *International Journal of Computer Science and Security (IJCSS)*, p. 298, 2011.

[36] P. Guillot, "Auguste kerckhoffs et la cryptographie militaire," *Journal des sciences militaires*, 5 2013.

[37] B. Rabab, *Sécurité des images Numériques compressées JPEG*. PhD thesis, Université Djilal Liebes Sidi Bel Abbes,Algerie, 2019.

[38] H. Djamel, *Transmission sécurisée des images par cryptage basé sur les systèmes chaotiques 1D, dans les systèmes de communication.* PhD thesis, Université 20 aout 1955 Skikda,Algerie, 2020.

[39] M. FARAJALLAH, *Chaos-based crypto and joint crypto-compression systems for images and videos*. PhD thesis, Université de Nantes, 2015.

[40] X. Lv, X. Liao, and B. Yang, "Bit-level plane image encryption based on coupled map lattice with time-varying delay," *Modern Physics Letters B*, vol. 32, 4 2018.

[41] X. Wang, S. Wang, Y. Zhang, and K. Guo, "A novel image encryption algorithm based on chaotic shuffling method," *Information Security Journal*, vol. 26, pp. 7–16, 1 2017.

[42] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD*, 2010.

[43] Y. Zhou, L. Bao, and C. L. Chen, "A new 1d chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, 2014.

[44] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on dna sequences and multiple improved 1d chaotic maps," *Applied Soft Computing Journal*, vol. 37, pp. 24–39, 2015.

[45] M. Ghebleh, A. Kanso, and D. Stevanovi, "A novel image encryption algorithm based on piecewise linear chaotic maps and least squares approximation," *Multimedia Tools and Applications*, vol. 77, 2017.

[46] J. Wu, X. Liao, and B. Yang, "Image encryption using 2d henon-sine map and dna approach," *Signal Processing*, vol. 153, pp. 11–23, 2018.

[47] Z. Hua and Y. Zhou, "Image encryption using 2d logistic-adjusted-sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.

[48] A. Dumlu and K. Erenturk, "Trajectory tracking control for a 3-dof parallel manipulator using fractional-order piÎ»dÎ¼ control," *IEEE Transactions on Industrial Electronics*, vol. 61, pp. 3417–3426, 2014.

[49] L. A. Said, A. G. Radwan, A. H. Madian, and A. M. Soliman, "Three fractional-order-capacitors-based oscillators with controllable phase and frequency," *Journal of Circuits, Systems and Computers*, vol. 26, 2017.

[50] Y. Q. Zhang, J. L. Hao, and X. Y. Wang, "An efficient image encryption scheme based on s-boxes and fractional-order differential logistic map," *IEEE*, vol. 8, 2020.

[51] X. Huang, T. Sun, Y. Li, and J. Liang, "A color image encryption algorithm based on a fractional-order hyperchaotic system," *Entropy*, vol. 17, pp. 28–38, 2015.

[52] P. Paral, T. Dasgupta, and S. Bhattacharya, "Colour image encryption based on cross-coupled chaotic map and fractional order chaotic systems," *International Conference on Communication and Signal Processing, ICCSP 2014 - Proceedings*, pp. 1947–1952, 2014.

[53] Y. Aydin and F. Ozkaynak, "A provable secure image encryption schema based on fractional order chaotic systems," *Proceedings of the 23rd International Conference Electronics 2019, ELECTRONICS 2019*, pp. 0–4, 2019.

[54] O. A. Aboulseoud and S. M. Ismail, "Fpga floating point fractional-order chaotic map image encryption," *Proceedings of the International Conference on Microelectronics, ICM*, vol. 2019-Decem, pp. 134–137, 2019.

[55] D. Herbadji, A. Belmeguenai, N. Derouiche, Y. Zennir, and S. Ouchtati1, "A novel color image encryption scheme using logistic map and quadratic map systems," in *Mobile, Secure, and Programmable Networking*, 2019.

[56] D. Herbadji, N. Derouiche, A. Belmeguenai, T. Bekkouche, A. Labiad, M. Lashab, and A. Herbadji, "A new image encryption scheme using an enhanced logistic map," in *2018 International Conference on Applied Smart Systems (ICASS)*, pp. 1–6, 2018.

[57] Y. G. Yang, B. W. Guan, J. Li, D. Li, Y. H. Zhou, and W. M. Shi, "Image compression-encryption scheme based on fractional order hyper-chaotic systems combined with 2d compressed sensing and dna encoding," *Optics and Laser Technology*, vol. 119, p. 105661, 2019.

[58] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic dna encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.

[59] L. ping Chen, H. Yin, L. guo Yuan, A. M. Lopes, J. A. Machado, and R. chao Wu, "A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and dna sequence operations," *Frontiers of Information Technology and Electronic Engineering*, vol. 21, pp. 866–879, 6 2020.

[60] X. Zhang, L. Wang, Y. Wang, Y. Niu, and Y. Li, "An image encryption algorithm based on hyperchaotic system and variable-step josephus problem," *International Journal of Optics*, vol. 2020, 2020.

[61] D. Herbadji, A. Belmeguenai, N. Derouiche, and H. Liu, "Colour image encryption scheme based on enhanced quadratic chaotic map," *IET Image Processing*, vol. 14, pp. 40–52, 1 2020.

[62] D. Herbadji, N. Derouiche, A. Belmeguenai, N. Tahat, and S. Boumerdassi, "A new colour image encryption approach using a combination of two 1d chaotic map," *International Journal of Electronic Security and Digital Forensics*, vol. 12, no. 04, 2020.

[63] D. Herbadji, N. Derouiche, A. Belmeguenai, A. Herbadji, and S. Boumerdassi, "A tweakable image encryption algorithm using an improved logistic chaotic map," *Traitement du Signal*, vol. 36, pp. 407–417, 2019.

[64] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," *Optics and Lasers in Engineering*, vol. 90, pp. 146–154, 3 2017.

[65] L. Liu, Y. Lei, and D. Wang, "A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation," *IEEE*, vol. 8, 2020.

[66] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a dna sequence," *Optics and Lasers in Engineering*, vol. 56, pp. 83–93, 5 2014.

[67] L. ping Chen, H. Yin, L. guo Yuan, A. M. Lopes, J. A. Machado, and R. chao Wu, "A novel color image encryption algorithm based on a fractional-order discrete chaotic

neural network and dna sequence operations," *Frontiers of Information Technology and Electronic Engineering*, vol. 21, pp. 866–879, 2020.

[68] T. Li, M. Yang, J. Wu, and X. Jing, "A novel image encryption algorithm based on a fractional-order hyperchaotic system and dna computing," *Complexity*, vol. 2017, 2017.

[69] J. Singh, D. Kumar, and J. J. Nieto, "Analysis of an el nino-southern oscillation model with a new fractional derivative," *Chaos, Solitons and Fractals*, vol. 99, pp. 109–115, 6 2017.

[70] H. M. Srivastava, D. Kumar, and J. Singh, "An efficient analytical technique for fractional model of vibration equation," *Applied Mathematical Modelling*, vol. 45, pp. 192–204, 5 2017.

[71] A. G. Radwan, A. M. Soliman, and A. S. Elwakil, "Design equations for fractional-order sinusoidal oscillators : Four practical circuit examples," *International Journal of Circuit Theory and Applications*, vol. 36, pp. 473–492, 6 2008.

[72] J. Zhao, S. Wang, Y. Chang, and X. Li, "A novel image encryption scheme based on an improper fractional-order chaotic system," *Nonlinear Dynamics*, vol. 80, pp. 1721–1729, 6 2015.

[73] X. Wu, Y. Li, and J. Kurths, "A new color image encryption scheme using cml and a fractional-order chaotic system," *PLoS ONE*, vol. 10, no. 3, 2015.

[74] F. Yang, J. Mou, J. Liu, C. Ma, and H. Yan, "Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application," *Signal Processing*, vol. 169, 4 2020.

[75] P. Mani, R. Rajan, L. Shanmugam, and Y. H. Joo, "Adaptive control for fractional order induced chaotic fuzzy cellular neural networks and its application to image encryption," *Information Sciences*, vol. 491, pp. 74–89, 7 2019.

[76] Y. Xu, H. Wang, Y. Li, and B. Pei, "Image encryption based on synchronization of fractional chaotic systems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, pp. 3735–3744, 2014.

[77] A. A. Akbergenov and H. P. Pelyukh, "Continuous solutions of systems of nonlinear difference equations," *Journal of Mathematical Sciences (United States)*, vol. 215, pp. 267–273, 4 2016.

[78] N. Ramadan, H. Eldin, H. Ahmed, S. E. Elkhamy, and F. E. A. El-Samie, "Chaos-based image encryption using an improved quadratic chaotic map," *American Journal of Signal Processing*, vol. 6, pp. 1–13, 2016.

[79] K. Nosrati and M. Shafiee, "Fractional-order singular logistic map : Stability, bifurcation and chaos analysis," *Chaos, Solitons and Fractals*, vol. 115, pp. 224–238, 10 2018.

[80] B. Yang and X. Liao, "A new color image encryption scheme based on logistic map over the finite field zn," *Multimedia Tools and Applications*, vol. 77, pp. 21803–21821, 8 2018.

[81] P. Li, J. Xu, J. Mou, and F. Yang, "Fractional-order 4d hyperchaotic memristive system and application in color image encryption," *Eurasip Journal on Image and Video Processing*, vol. 2019, 12 2019.

[82] L. Huang, S. Cai, X. Xiong, and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," *Optics and Lasers in Engineering*, vol. 115, pp. 7–20, 4 2019.

[83] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.

[84] Q. Zhang and J. Han, "A novel color image encryption algorithm based on image hashing, 6d hyperchaotic and dna coding," *Multimedia Tools and Applications*, vol. 80, pp. 13841–13864, 4 2021.

[85] Y. Su and X. Wang, "A robust visual image encryption scheme based on controlled quantum walks," *Physica A : Statistical Mechanics and its Applications*, vol. 587, 2 2022.

[86] Z. Li, C. Peng, W. Tan, and L. Li, "A novel chaos-based color image encryption scheme using bit-level permutation," *Symmetry*, vol. 12, 9 2020.

[87] A. Alghafis, N. Munir, and M. Khan, "An encryption scheme based on chaotic rabinovich-fabrikant system and s8 confusion component," *Multimedia Tools and Applications*, vol. 80, pp. 7967–7985, 2 2021.

[88] E. Yavuz, "A new parallel processing architecture for accelerating image encryption based on chaos," *Journal of Information Security and Applications*, vol. 63, 12 2021.

[89] H. R. Shakir, "Implementing digital image security framework with hybrid approach of chaotic map and singular-value decomposition," *Chaos, Solitonsa nd Fractals*, vol. 8, p. 100075, 2022.

[90] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," *Entropy*, vol. 23, 3 2021.

[91] M. Ahmad, M. N. Doja, and M. M. S. Beg, "Security analysis and enhancements of an image cryptosystem based on hyperchaotic system," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, pp. 77–85, 1 2021.

[92] G. Kaur, R. Agarwal, and V. Patidar, "Color image encryption system using combination of robust chaos and chaotic order fractional hartley transformation," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, pp. 5883–5897, 9 2022.

[93] Q. Lai, G. Hu, U. Erkan, and A. Toktas, "A novel pixel-split image encryption scheme based on 2d salomon map," *Expert Systems with Applications*, vol. 213, 3 2023.

[94] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Processing*, vol. 134, pp. 35–51, 5 2017.

[95] B. Yousif, F. Khalifa, A. Makram, and A. Takieldeen, "A novel image encryption/decryption scheme based on integrating multiple chaotic maps," *AIP Advances*, vol. 10, 7 2020.

[96] Z. M. Z. Muhammad and F. Ozkaynak, "An image encryption algorithm based on chaotic selection of robust cryptographic primitives," *IEEE Access*, vol. 8, pp. 56581–56589, 2020.

[97] X. Wang, C. Liu, and D. Jiang, "A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3d dct," *Information Sciences*, vol. 574, pp. 505–527, 10 2021.

[98] Y. Dou, X. Liu, H. Fan, and M. Li, "Cryptanalysis of a dna and chaos based image encryption algorithm," *Optik*, vol. 145, pp. 456–464, 9 2017.

[99] A. Jain and N. Rajpal, "A robust image encryption algorithm resistant to attacks using dna and chaotic logistic maps," *Multimedia Tools and Applications*, vol. 75, pp. 5455–5472, 5 2016.

[100] R. Bechikh, H. Hermassi, A. A. A. El-Latif, R. Rhouma, and S. Belghith, "Breaking an image encryption scheme based on a spatiotemporal chaotic system," *Signal Processing : Image Communication*, vol. 39, pp. 151–158, 11 2015.

[101] C. Y. Song, Y. L. Qiao, and X. Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos," *Optik*, vol. 124, pp. 3329–3334, 9 2013.

[102] Q. Zhang, L. Guo, and X. Wei, "A novel image fusion encryption algorithm based on dna sequence operation and hyper-chaotic system," *Optik*, vol. 124, pp. 3596–3600, 9 2013.

[103] Y. Zhang, "Cryptanalysis of a novel image fusion encryption algorithm based on dna sequence operation and hyper-chaotic system," *Optik*, vol. 126, pp. 223–229, 2015.