Ministère de l'enseignement Supérieur et de la recherche Scientifique
وزارة التعليم العالي والبحث العلمي

Badji Mokhtar Annaba University
Université Badji Mokhtar – Annaba
Faculté de Technologie
Département d'informatique

جامعة باجي مختار – عنابـــــــــة
كليةالتــكنولـــوجـــيا
قســـــــم الإعلام الآلي

Thèse

Présentée pour obtenir le diplôme de

Doctorat En-Sciences

Spécialité :Informatique

Par :
LOUZZANI Noura

Thème :

Contribution à l'amélioration de la transmission sécurisée des images à base du chaos

Thèse soutenue le **13 -07-2022**, devant le jury composé de :

N°	Nom et prénom	Grade	Etablissement	Qualité
01	MOHAMED BENALI Yamina	Pr.	Université Badji Mokhtar - Annaba	Président
02	BOUKABOU Abdelkrim	Pr.	Université de Jijel	Rapporteur
03	BAHI Halima	Pr.	Université Badji Mokhtar –Annaba	Co-rapporteur
04	BOUDEN Toufik	Pr.	Université de Jijel	Examinateur
05	SARI Toufik	Pr.	Université BadjiMokhtar- Annaba	Examinateur
06	SOUICI Ismahane	MCA.	Université de Jijel	Examinateur

المساهمة في تحسين النقل الآمن للصورالقائمةعلى الفوضى

الملخص:
في هذه الأطروحة،نقترح الدالة المولدة لكثيرات الحدود لتشيبتشاف مع فترة نموذجية تتضاعف في حالة التشويش (الفوضى). فيهذاالسياق،أثبت المنحنى البياني للتشعب والأس الخاص بمعامل ليابونوف أن الدالة المولدة المقترحة هي نظام حتمي يُظهر سلوكًا فوضويًا لقيم محددة لمعلمات التحكم. كتطبيق،يتم استخدام الدالة المولدة المقترحة هذه كنظام تشفير قائم على الفوضى لتشفير الصور المختلفة. أظهرتحليلا لأمان أن وظيفة التوليد المقترحة لكثيرات الحدود لتشيبتشاف تظهر أداءً ممتازًا في تشفيرا لصور ضد الهجمات المختلفة .

كلمات مفتاحية:الدالة المولدة ، كثيرات الحدود لتشيبتشاف من النوع الثاني، الفوضى، أس ليابونوف المنحنى البياني للتشعب، أنظمة التشفير,

Contribution à l'amélioration de la transmission sécurisée des images à base du chaos

Résumé :

Dans cette thèse, nous proposons une fonction génératrice pour les polynômes de Chebyshev avec un doublement de période typique au chaos. Dans ce contexte, le diagramme de bifurcation et l'exposant de Lyapunov ont prouvé que la fonction génératrice proposée est un système déterministe qui présente un comportement chaotique pour des valeurs spécifiques des paramètres de contrôle. En tant qu'application, cette fonction génératrice proposée est utilisée comme un crypto système basé sur le chaos pour crypter différentes images. L'analyse de sécurité a démontré que la fonction de génération proposée des polynômes de Chebyshev présente d'excellentes performances en cryptage d'images contre diverses attaques.

Mots clés : Fonction génératrice, Polynômes de Chebyshevde seconde espèce, Chaos, Exposant de Lyapunov, Diagramme de bifurcation, Crypto système.

Contribution to improving the secure transmission of chaos-based images

Abstract :

In this thesis, we propose a generating function for Chebyshev polynomials with typical period-doubling to chaos. In this context, the bifurcation diagram and Lyapunov exponent proved that the proposed generating function is a deterministic system that exhibits chaotic behavior for specific values of the control parameters. As an application, this proposed generating function is used as a chaos-based cryptosystem to encrypt different images. Security analysis demonstrated that the proposed generating function of the Chebyshev polynomials presents an excellent performance in image encryption against various attacks.

Key words Generating function, Chebyshev polynomials of the second kind, Chaos, Lyapunov exponent , Bifurcation diagram, Cryptosystem.

REMERCIEMENTS

الحمد لله الذي بنعمته تتم الصالحات

Je souhaite tout d'abord exprimer ma sincère gratitude à mon Directeur de thèse, **Pr. BOUKABOU Abdelkrim**, pour ses conseils, son soutien, sa patience et la confiance qu'il a bien voulu m'accorder. Je lui suis également très reconnaissante pour le temps conséquent qu'il m'a accordé par ses qualités pédagogiques et scientifiques.

Mes sincères remerciements vont également à mon Co-Directeur de thèse, **Pr. BAHI HALIMA** pour son soutien, sa patience et ses conseils avisés qui ont été prépondérants pour la bonne réussite de cette thèse.

Mes chers encadrants, Merci, vous m'avez appris, vous m'avez encouragé et vous m'avez orienté.

Je remercie vivement **Pr. MOHAMED BENALI Yamina, Pr. BOUDEN Toufik**, **Pr. SARI Toufik** et **Dr SOUICI Ismahane** pour l'intérêt qu'ils ont porté à mon travail et pour l'honneur qu'ils m'ont fait d'avoir acceptés d'examiner mon travail.

Je remercie vivement **Madame MELIT Leila**, **Monsieur LOUZZANI Yassine** et **Monsieur BOUSSAYOUD Ali** qui ont relu la thèse et m'ont fait bénéficier de leurs critiques et remarques très instructives.

Mes remerciements affectueux et chaleureux s'adressent à toute ma famille, à mes amies et à mes collègues pour leurs prières et leurs encouragements.

Productions scientifiques

Publications internationales:

N. Louzzani, A. Boukabou, H. Bahi, A. Boussayoud, A novel chaos based generating function of the Chebyshev polynomials and its applications in image encryption, , Chaos, Solotons and Fractals. 151 (111315), 1-10 , **2021. IF: 5.944.**

Communications internationales :

[1] **N. Louzzani**, A. Boukabou, H. Bahi, Image Encryption Algorithm Using Chaos and Generating Functions, 4th International E-Conference on Mathematical Advances and Applications, May 26-29, **2021**, Istanbul, Turkey.

[2] **N. Louzzani**, A. Boukabou, H. Bahi, Chaotic Behavior In The Product Of Generating Functions, 1st International Conference on Pure and Applied Mathematics, IC-PAM'21 May 26-27, **2021**, Ouargla, Algeria.

[3] **N. Louzzani**, A. Boukabou, H. Bahi, Nouvelle Fonction Chaotique pour le Chiffrement Symétrique des Images Numériques, *Séminaire International sur les Mathématiques et l'informatique, Algerian Journal of Engineering, Architecture and Urbanism, 05 -06 Février* ***2021,*** *Oran, Algerie.*

Liste des Figures

Liste des Tableaux

Table des matières

Introduction Générale

Dans le domaine des télécommunications et avec l'évolution de l'internet, où les échanges d'informations (paroles, images, signes, signaux etc.) se développent rapidement, il est indispensable de pouvoir disposer de systèmes sécurisés pour protéger les données à caractère personnel ou confidentiel et assurer la sécurité des transferts de données. Il est donc nécessaire de développer un outil de protection efficace des données transférées et des communications contre les intrusions arbitraires. Le cryptage des données est très souvent le seul moyen efficace pour répondre à ces exigences.

La cryptographie a depuis des siècles été une histoire de conflit qui oppose deux camps, un qui cherche à cacher une information et un autre qui essaie de trouver ce qu'on lui cache. Ainsi, à chaque fois que le premier trouve un moyen de chiffrer ses messages, le second mobilise tous les moyens dont il dispose afin de trouver la méthode ou l'astuce pour les décrypter. La cryptographie est une discipline qui a pour objet l'étude des méthodes qui permettent de transmettre des données de manière confidentielle. Afin de protéger une information, on lui applique une transformation qui la rend incompréhensible aux non-destinataires ; c'est ce qu'on appelle le chiffrement/cryptage. Donner une information chiffrée à partir d'une information originale. Inversement, le déchiffrement/décryptage est l'action qui permet de reconstruire l'information

originale à partir de l'information chiffrée/cryptée. De ce fait, la cryptographie est l'art de transmettre l'information de manière sécurisée.

Au cours des deux dernières décennies, nous pouvons remarquer une augmentation significative de l'utilisation de photos et de vidéos dans les réseaux sociaux tels que Facebook et Instagram, dans les moteurs de recherche visuels tels que Google images et la recherche d'images Yahoo, les services de stockage en cloud tels que Google Drive. Cette croissance rapide de l'utilisation du contenu visuel sera augmenter dans l'avenir proche en raison des technologies émergentes telles que la réalité virtuelle et la 5G. Afin de transférer ce contenu de manière sécurisée, certains mécanismes et applications peuvent être utilisés, dont la plupart dépendent de la cryptographie.

Il existe dans le monde réel, de nombreux algorithmes de cryptage efficaces, tels que AES (Advanced-Encryption- Scheme), RSA (Rivest-Shamir-Adelman) et El Gamel. Ces algorithmes sont conçus pour crypter des informations textuelles. Ils sont néanmoins moins efficaces lorsqu'il s'agit de traiter des données fortement corrélées comme les images ou les vidéos. Cela a conduit au développement d'algorithmes de cryptage d'images « basés sur le chaos ». Rappelons que le chaos est un phénomène naturel découvert par Edward Lorenz en 1963 tout en étudiant l'effet papillon dans les systèmes dynamiques. En effet, en programmant son ordinateur et en changeant par 10^{-14} les conditions initiales des prévisions météo, il a découvert que pour certaine équation ou système d'équations non linéaires, les résultats montrent une grande sensibilité aux conditions initiales. Ces algorithmes cryptographiques qui exploitent le chaos et ses caractéristiques, telles que la sensibilité aux conditions initiales, pour crypter les images rend la sécurisation de ce type de données une des problématiques qui prend de l'ampleur ces dernières années [1] .

L'idée de base de la cryptographie chaotique est de brouiller un message de manière adéquate avec le chaos au niveau de l'émetteur, afin de le dissimuler des intrus, avant de le transmettre à sa destination qui sera la seule capable de le décrypter.

Ces algorithmes, reconnus par leur performance supérieure, décrivent un phénomène d'apparence aléatoire mais, qui est à l'origine, déterministe pour le masquage d'information.

Les fonctions chaotiques, comme par exemple la fonction logistique qui se définit par $f(x) = r * x * (1 - x)$, sont des fonctions de récurrence. Les suites définies par une relation de récurrence sont utilisées dans des domaines et disciplines très différents. On trouve ce type de fonctions, par

exemple, en analyse combinatoire dans les problèmes de dénombrement, en biologie dans le cadre de la dynamique des populations, en informatique dans le cadre de l'analyse des algorithmes, et même dans des disciplines des sciences humaines et sociales, telle que la macroéconomie. Les plus célèbres nombres, utilisés dans le chiffrement, existent depuis très longtemps et sont récurrents d'ordre deux (à trois termes), à savoir les nombres de Fibonacci F_n ; Lucas L_n ; Pell P_n ; etc. Ces différents nombres possèdent des polynômes notés par : $F_n(x)$, $L_n(x)$, $P_n(x)$, tels que pour chaque nombre et polynôme, nous pouvons définir la fonction génératrice associée.

Les applications des fonctions génératrices sont également nombreuses et variées. Abondamment utilisées en théorie des probabilités, elles forment un lien entre l'analyse mathématique des fonctions à valeurs réelles et les problèmes portant sur les séquences, et fournissent par ailleurs une expression explicite de certaines suites définies par une relation de récurrence.

Notre travail dans cette thèse est de proposer un nouvel ensemble de fonctions génératrices, aux propriétés chaotiques liées à un polynôme de Chebyshev de second espèce [2]. Le comportement chaotique correspondant a été étudié par analyse du diagramme de bifurcation et par quantification de l'exposant de Lyapunov pour différentes valeurs des paramètres du système. Nous étudions ensuite la performance de cette nouvelle fonction chaotique et sa robustesse sur un système de cryptage des images numériques.

La thèse s'articule en quatre chapitres :

Le premier chapitre présente le contexte théorique du travail réalisé en s'appuyant sur deux sujets fondamentaux, la cryptographie et l'image numérique. Ainsi, on présente en premier lieu les bases de la cryptographie moderne et ses deux principaux types, de chiffrement symétrique et asymétrique. Puis, on aborde les concepts liés à l'image numérique à travers les types d'images existants et les formats de fichiers d'images largement utilisés.

Le deuxième chapitre est consacré au contexte mathématique du sujet abordé : le chaos dans les fonctions génératrices. Dans ce chapitre, on présente une brève introduction aux systèmes dynamiques, des généralités sur la théorie du chaos, et plus particulièrement les concepts de base tels que la bifurcation et l'exposant de Lyapunov. Pour ce qui est des fonctions génératrices, nous les définissons et présentons quelques rappels sur les relations des récurrences et des polynômes.

Le troisième chapitre présente un état de l'art des systèmes de cryptage d'images basés sur le

chaos, que nous pouvons qualifier de systèmes de cryptographie chaotique des images. Dans ce chapitre, nous présentons aussi les métriques utilisées pour évaluer la sécurité et les performances des schémas de cryptage d'images.

Le dernier chapitre est dédié à l'étude détaillée d'un système de cryptage chaotique basé sur la nouvelle fonction chaotique : la fonction génératrice ordinaire de polynôme de Chebychev de deuxième espèce.

Chapitre 1

Généralités sur la cryptographie et les images numériques

1.1 Introduction

Les données numériques, présentées sous forme de fichiers audio, de vidéos ou encore des images numériques, jouent un rôle de plus en plus important dans notre vie quotidienne. Le secrétaire général de l'OCDE a déclaré au sommet de Paris portant sur la transformation numérique, en mars 2019, que cette transformation « n'épargne aucun aspect de nos vies. Elle redessine les interactions économiques et sociales, et suscite des inquiétudes quant aux emplois, aux compétences, au respect de la vie privée et à la sécurité. Elle met également à l'épreuve nos cadres d'action, tandis que nous nous efforçons de trouver un juste équilibre entre les innovations porteuses d'amélioration du bien-être et les préoccupations en matière, notamment, de protection de la vie privée, de sécurité, de concurrence ou d'égalité». Les états, les scientifiques et les acteurs socio-économiques se mobilisent pour mieux protéger les données numériques et mieux sécuriser les usagers. Pouvoir disposer de systèmes sécurisés et protéger ces différentes données devient un des enjeux majeurs dans une société où le numérique impacte tous les domaines de l'activité humaine. C'est dans ce contexte que l'émergence de la cryptographie, en tant qu'art et science qui concerne principalement la protection de ses données contre les interceptions non autorisées, prend toute son importance.

Dans ce chapitre, nous présentons deux éléments clés qui sont au cœur de notre sujet : la cryptographie et les images numériques. Aussi nous introduisons les terminologies de base de la cryptographie tout en décrivant brièvement les objectifs de la cryptographie (section 1.2). Nous présentons ensuite les deux grandes familles d'algorithmes de chiffrement, à savoir : le chiffrement symétrique et le chiffrement asymétrique. Nous terminons cette section par la présentation du principe de la cryptanalyse. La Section 1.3 présente les concepts essentiels liés à l'image numérique à savoir sa définition, ses différents types, ainsi que les différents formats d'enregistrement.

Le cryptage des images numériques est aussi abordé à la fin de ce chapitre, à travers ses deux modes de cryptage qui sont le mode spatial et le mode fréquentiel.

1.2 Cryptographie

A l'origine, le mot cryptographie vient des deux mots grecs kryptós qui signifie "secret" et gráphein qui graphique signifie "écrire". Le sens général est d'écrire secrètement afin d'assurer la confidentialité des informations. Actuellement, la cryptographie est la science qui vise à cacher l'information contre tous types d'accès ou d'utilisation non autorisés. Autrement dit, elle désigne l'ensemble des méthodes utilisées pour atteindre les trois principaux objectifs de la sécurité, que résument les trois mots clés suivants : Confidentialité -Intégrité -Authentification [1, 3].

- **Confidentialité :** désigne le masquage des données de toutes les personnes, machines et systèmes à l'exception de ceux qui ont le droit d'accès.

- **Intégrité :** les données sont protégées de tous types de changements effectués par une personne non autorisée et par conséquent éviter l'altération des données par les personnes non autorisées.

- **Authentification :** permet à l'utilisateur d'apporter la preuve de son identité. Il s'agit de garantir à chacun des correspondants de s'assurer que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées. La figure suivante illustre le schéma du principe général de la cryptographie (Figure 1.1).

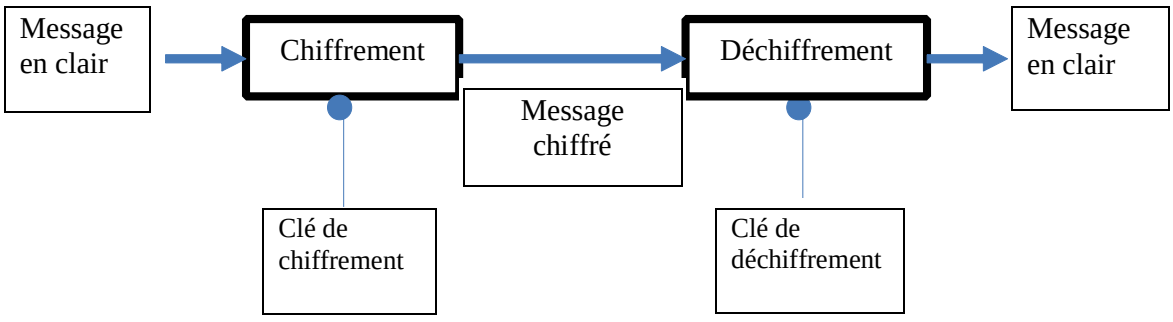


Figure 1.1. Schéma de principe général de la cryptographie.

Par ailleurs, ce domaine repose sur un vocabulaire particulier qu'il est important de rappeler dans ce qui suit.

1.2.1 Concepts cryptographiques

La cryptologie est la science des messages secrets. Elle a comme objectif principal la transmission d'informations entre deux interlocuteurs A et B, de manière sûre. La cryptologie englobe principalement deux disciplines "duales" : la cryptographie, qui s'intéresse à la sécurisation de l'information, et la cryptanalyse, qui cherche à l'attaquer.

Bien que cette thèse traite principalement de cryptographie, il est indispensable de connaître certains aspects de la cryptanalyse afin de s'assurer de la robustesse de notre cryptosystème (le système de chiffrement).

En termes cryptographiques, le message en clair est le message original qui peut être lu et compris par les humains et le message chiffré est le message original après le processus de chiffrement ; le message chiffré est apparemment aléatoire et ambigu pour les humains. L'idée de base du chiffrement est de brouiller les informations secrètes de manière à ce qu'elles ne puissent pas être comprises par des personnes non autorisées. Le chiffrement est le processus, la méthode ou l'algorithme utilisé pour transformer un message en clair en un message chiffré. Tandis que le déchiffrement est le processus, la méthode ou l'algorithme inverse du chiffrement, qui transforme le message chiffré en message clair. Ce dernier s'effectue uniquement en possession de la clé de déchiffrement. *La Clé :* est la valeur secrète utilisée pour chiffrer un message en clair en un message chiffré (clé de chiffrement) et pour déchiffrer un message chiffré en un message en clair (clé de déchiffrement). On peut parfaitement concevoir un algorithme qui n'utilise pas de clé. Dans ce cas, c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé.

Les cryptographes sont des personnes qui travaillent à développer des cryptosystèmes pour fournir des services de sécurité, tandis que les cryptanalystes sont des personnes qui travaillent à développer et à trouver des méthodologies pour casser les cryptosystèmes.

1.2.2 Classification des systèmes cryptographiques

Les algorithmes de chiffrement sont classés en deux types : symétrique et asymétrique.

1.2.2.1 Cryptographie symétrique et ses caractéristiques

La première classe est celle de chiffrement symétrique, illustrée à la figure 1.2, aussi appelée chiffrement à clé privée ou à clé secrète ; c'était le seul type de chiffrement utilisé avant le développement du chiffrement à clé publique dans les années 1970. Dans ce système, les deux entités (l'émetteur et le récepteur) utilisent la même clé dans le processus de chiffrement/déchiffrement.

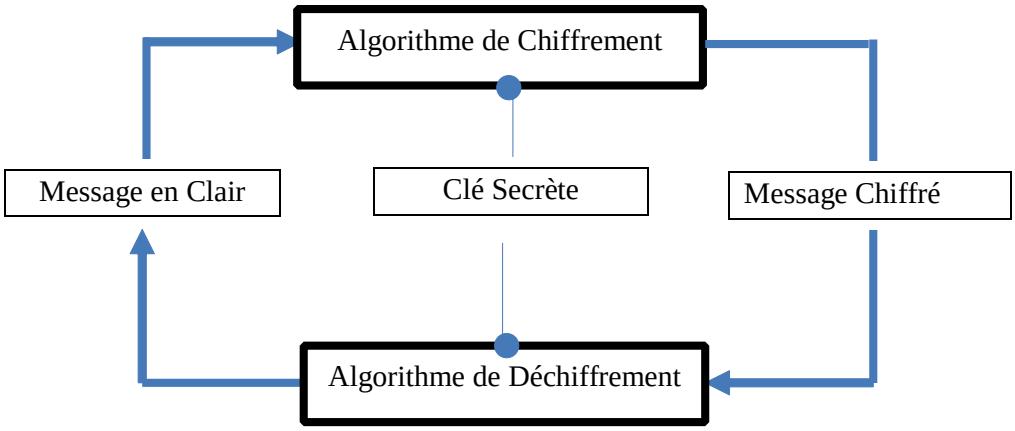


Figure 1.2. Principe de la cryptographie symétrique.

Formellement, le chiffrement et le déchiffrement d'un message M en utilisant la clé secrète K avec un algorithme symétrique sont désignés par les équations suivantes :

$$\begin{cases} E_K(M) = C, \\ D_K(C) = M. \end{cases}$$

Au sein des cryptosystèmes symétriques, on distingue principalement deux catégories :

- **les chiffrements par blocs :** chaque message à chiffrer est décomposé en blocs de taille fixe (quitte à compléter les blancs), et le chiffrement agit sur l'ensemble du bloc à l'aide de permutations (transpositions) et de substitutions.

- **les chiffrements à flots de données :** ces chiffrements sont généralement les plus rapides, et plus appropriés lorsque le débit de caractères à chiffrer n'est pas constant. Ces chiffrements agissent généralement bit par bit ou octet par octet [3, 4].

Notons qu'il existe plusieurs systèmes cryptographiques symétriques largement utilisés ces dernières années : tels que le DES Standardisé, et son alternative AES.

a. Chiffrements classiques

Les chiffrements classiques sont des chiffrements antérieurs aux ordinateurs et fonctionnent donc avec des lettres et non pas avec des bits) [4] Il existe plusieurs types de ce chiffrement.

a.1. Chiffrement de César

C'est l'un des chiffrements les plus anciens et les plus simples. Le chiffrement de César se résume en un chiffrement de substitution simple : où chaque lettre du texte en clair est décalée d'un nombre secret fixe X pour obtenir le texte chiffré.

Dans l'exemple suivant, nous allons chiffrer un message en décalant chaque lettre de 1 pour que le A devienne B et B devienne C et ainsi de suite :

Texte brut : « CRYPTAGECHAOTIQUEDESIMAGES »

Texte chiffré : "DSZQUBHFDIBPUJRVFEFTJNBHFT"

a.2. Chiffrement de Vernam

Publié par Gilbert Vernam en 1926 ; sa sécurité a été formellement prouvée par Shannon quelques années plus tard. Ce dernier a utilisé la notion de secret parfait. Ce chiffrement est également connu sous le nom d'OTP « one-time pad » dans la mesure où la clé est destinée à être utilisée pour un seul texte en clair. Aussi, le chiffrement de Vernam est défini par :

le texte en clair qui est une chaîne de bits : un élément de $\{0,1\}^n$

la clé secrète est un élément uniformément distribué de $\{0,1\}^n$

le texte chiffré est $CK(X) = X \oplus K$ où $\oplus$ est le XOR au niveau du bit.

Les principaux inconvénients de ce type de chiffrement sont :

- la clé doit être au moins aussi longue que le message.
- le chiffrement devient peu sûr si une clé est utilisée deux fois.
- le résultat de sécurité n'a de sens que lorsque la clé est vraiment aléatoire.

b. Chiffrements modernes

Les chiffrements modernes sont ceux qui utilisent le processeur de l'ordinateur pour effectuer les processus de chiffrement et de déchiffrement. Il existe plusieurs chiffrements modernes standardisés. Nous allons nous intéresser ici à la Data Encryption Standard (DES) et à l'Advanced Encryption Standard (AES).

b.1. DES

Jusqu'à l'introduction de l'Advanced Encryption Standard (AES) en 2001, le Data Encryption Standard (DES) était le schéma de cryptage le plus utilisé. DES a été publié en 1977 par le National Bureau of Standards NDS, appelé aujourd'hui National Institute of Standards and Technology (NIST). Pour DES, les données sont chiffrées en blocs de 64 bits à l'aide d'une clé de 56 bits (en fait, la clé est représentée en 8 octets (64 bits) et le bit le plus significatif MSB est utilisé pour le contrôle de parité).

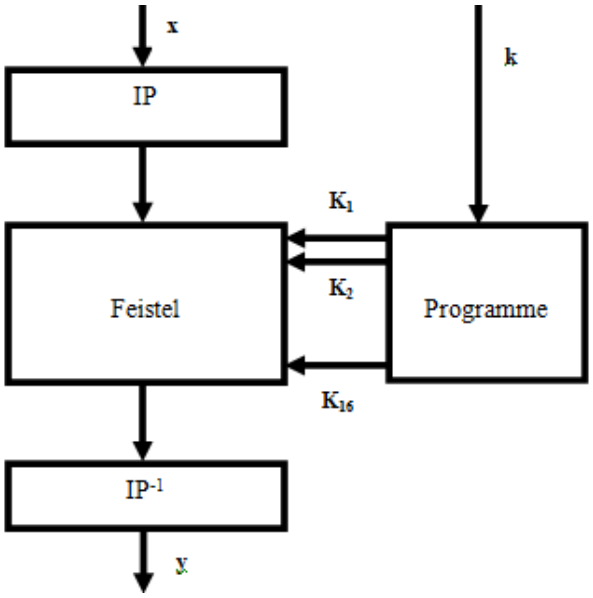


Figure 1.3. Schéma de cryptage DES.

Comme illustré dans la Figure 1.3, DES commence par une permutation de bits initiale (IP) en utilisant la matrice de permutation et exécute le chiffrement de Feistel (cf. la Figure 1.4) en faisant des permutations et des substitutions répétées 16 fois (appelées rondes) ; en utilisant des sous-clés générées par un programme de clé. Enfin, il exécute la permutation initiale inverse en utilisant la matrice de permutation.

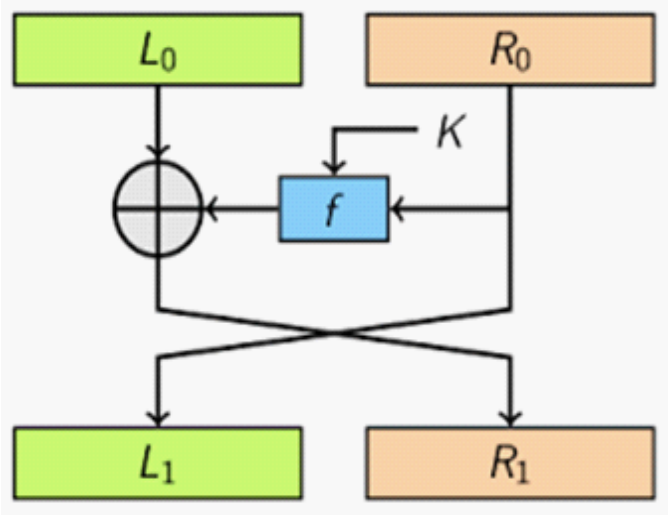


Figure 1.4. Schéma de Feistel.

b.2. AES

AES est aujourd'hui le standard du chiffrement symétrique par bloc. Ce chiffrement symétrique est normalisé par le NIST en 2000. AES repose sur la combinaison entre la permutation et la substitution ; plus communément appelés réseaux de substitution-permutation (SPN). Chaque tour dans l'AES contient des opérations : substitution (octet substitutif), permutation (décaler la ligne et mélanger les colonnes) et une application du XOR entre la clé et le résultat de l'opération de la substitution-permutation de bloc précédent [4, 5].

L'AES reste le standard aujourd'hui, intégré dans différents processeurs modernes tels que les processeurs Intel, processeurs AMD, les cartes bancaires, et même certains téléphones, avec des clés de 128 à 256 bits [4].

Après l'énumération de ces différents types de chiffrement symétrique on peut désormais présenter ses principales caractéristiques.

Caractéristiques du cryptage symétrique

- Les clés dans les cryptosystèmes symétriques sont relativement de petite taille.

- Les algorithmes de chiffrement à clé symétrique peuvent être utilisés comme des primitives pour construire divers mécanismes cryptographiques, y compris les générateurs de nombres pseudo-aléatoires, les fonctions de hachage et des schémas de signature numérique.

- Les chiffres à clé symétrique peuvent être composés pour produire des chiffres plus forts. Ils sont basés sur des transformations simples qui sont faciles à analyser. Mais en s'appuyant sur leur propre faiblesse, ils peuvent être utilisés pour construire des chiffres forts.

- Dans une communication entre deux entités, la clé doit rester secrète aux deux extrémités.

- Dans un grand réseau, il y a beaucoup de paires de clés à gérer. Par conséquent, une gestion efficace des clés nécessite l'utilisation d'une autorité de confiance.

- Dans une communication à deux parties entre deux entités A et B, la pratique cryptographique impose que la clé doit être changée fréquemment, et peut-être même pour chaque session de communication.

1.2.2.2 Cryptographie asymétrique et ses caractéristiques

Le chiffrement asymétrique, nommé également le cryptage à clé publique, se base sur l'utilisation des deux clés. Une clé publique pour chiffrer, elle est accessible publiquement, et une clé privée, qui est gardée secrète, pour déchiffrer le message (Figure 1.5). Ce type de chiffrement élimine la problématique de la transmission de la clé. L'invention de la cryptographie à clé publique est souvent attribuée à Whit field Diffie et Martin Hellman dans un article célèbre publié en 1976, qui décrit les exigences de cette nouvelle approche. Depuis, de nombreux algorithmes ont été proposés. Ils n'ont pas tous été à la hauteur des défis que rencontre la cryptographie, néanmoins l'algorithme RSA [1, 3] a donné une certaine satisfaction aux usagers.

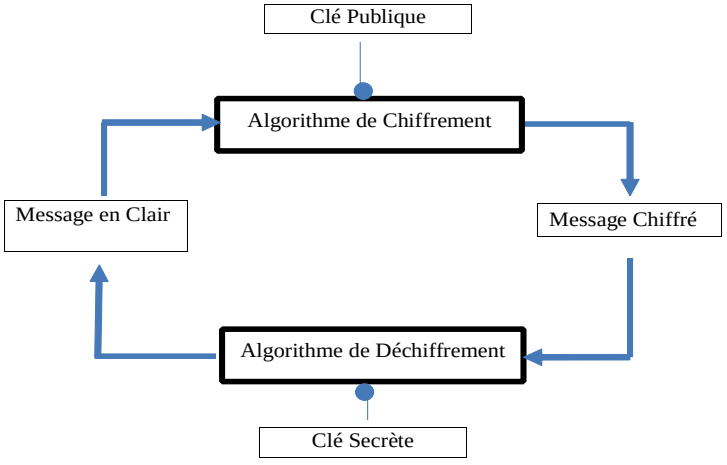


Figure 1.5. Principe de cryptographie asymétrique.

Il convient de souligner qu'un schéma de chiffrement asymétrique Π, peut être décrit par l'un des trois algorithmes (GenClé, Chiff, Dechiff) suivants :

1. Un algorithme de génération de clef **GenClé**. C'est un algorithme probabiliste qui retourne un couple (p_k, s_k).

2. Un algorithme de chiffrement **Chiff**. C'est un algorithme qui retourne un message chiffré C, généré à partir d'une clef publique p_k et d'un message clair, m.

3. Un algorithme déchiffrement **Dechiff**. C'est un algorithme qui prend en entrée une clef secrète s_k et un chiffré C et qui retourne un message clair m.

Algorithme RSA :

Cet algorithme tire son nom de ses inventeurs : R. Rivest, A. Shamir et L. Adleman. Il constitue la première application des concepts Deffi-Hellman de cryptographie à clé publique. En d'autres termes, c'est le premier chiffrement asymétrique inventé en 197l. Son principe de chiffrement et de déchiffrement se base sur les deux fonctions suivantes :

$$\begin{cases} C = M^e \bmod n, \\ M = C^d \bmod n. \end{cases}$$

Alors que l'algorithme de génération de clé **KeyGen** de RSA se résume comme suit :

1- Sélectionner deux grands nombres premiers p et q.

2- Calculer $n = p * q$.

3- Calculer $\phi(n) = (p-1)(q-1)$.

4- Choisir e tel que e soit relativement premier à $\phi(n)$.

5- Déterminer l'entier d tel que $d * e = 1 \bmod \phi(n)$ et $de < \phi(n)$.

Sachant que les clés privées sont (d, n) tandis que les clés publiques sont (e, n).

Caractéristiques principales du cryptage asymétrique

Le cryptage asymétrique nous permet l'élimination de la problématique de la transmission de la clé. Il nous donne la possibilité d'utiliser la signature électronique.

On peut également souligner l'impossibilité de décrypter le message dans le cas d'une interception par une personne non autorisé.

Une paire de clés (publique/secrète) peut être utilisée plus longtemps qu'une clé symétrique et le temps d'exécution est plus lent que le cryptage symétrique.

En revanche, il existe un danger des attaques par substitution des clés d'où la nécessité de valider les émetteurs des clés. Enfin la taille des clés est plus grande que celle des systèmes symétriques.

1.2.3 Cryptanalyse

La cryptanalyse, à la différence de la cryptographie, est l'étude des procédés cryptographiques dans le but de trouver des faiblesses afin de pouvoir décrypter des messages chiffrés. Le décryptement est l'action qui consiste à trouver le message en clair sans connaitre la clef de déchiffrement.

La cryptanalyse des schémas de cryptage peut être effectuée sous un certain nombre d'hypothèses. Une hypothèse fondamentale, connue sous le nom de :

1.2.3.1 Principe de Kerchoff

Selon cette hypothèse, l'adversaire connait complètement l'algorithme de cryptage, à l'exception de la clé secrète qui est inconnue. Cela signifie que la sécurité du cryptosystème repose entièrement sur la clé secrète, et non pas sur la confidentialité du schéma. Le but de l'attaquant est alors de retrouver le texte clair ou n'importe qu'elle information sur le texte clair ; ce qui, dans la plupart des cas, nécessite la connaissance de la clé secrète. D'autres hypothèses peuvent alors être formulées. Pour plus de détails, le lecteur peut se référer aux travaux de [6].

1.2.3.2 Types d'attaques classiques

En plus de l'analyse mathématique des algorithmes cryptographiques, la cryptanalyse comprend l'étude des attaques par canal secondaire qui ne ciblent pas les faiblesses des algorithmes cryptographiques eux-mêmes, mais exploitent plutôt les faiblesses de leur mise en œuvre. Même si l'objectif a été le même, les méthodes et techniques de cryptanalyse ont radicalement changé à travers l'histoire de la cryptographie, s'adaptant à une complexité cryptographique croissante. Les méthodes pour briser les cryptosystèmes modernes impliquent souvent de résoudre des problèmes soigneusement construits en mathématiques pures, la plus connue étant la factorisation

d'entiers.

Le processus par lequel on tente de comprendre un message en particulier est appelé une attaque. Les attaques peuvent être classées en fonction du type d'informations dont l'attaquant dispose. Nous énumérons ci-dessous les quatre types d'attaques classiques les plus couramment utilisées aujourd'hui contre les applications cryptographiques [7] :

- Attaque par texte chiffré : le cryptanalyste n'a accès qu'à une collection de textes chiffrés.

- Attaque par texte en clair connu : le cryptanalyste détient une chaîne de caractères du texte en clair et du texte chiffré correspondant.

- Attaque par texte en clair choisi : le cryptanalyste a profité de l'accès à la machine de cryptage comme une boîte noire et peut obtenir les textes chiffrés pour des textes en clair arbitraires.

- Attaque par texte chiffré choisi : le cryptanalyste a profité de l'accès à la machine de décryptage comme une boîte noire et peut construire les textes en clair pour des textes chiffrés arbitraires.

Notons que l'attaque par texte clair choisi est le modèle d'attaque le plus courant en cryptanalyse. Par conséquent, l'algorithme n'est considéré comme efficace que s'il peut résister à ce type d'attaque.

1.3 Image

Une image est une représentation concrète ou abstraite d'un objet. Elle est issue du contact des rayons lumineux provenant des objets formants la scène avec un capteur (caméra, scanner, rayons X, ...). L'image est considérée comme un ensemble de points auxquels sont affectés des grandeurs physiques (luminance, couleur). On distingue dans la littérature plusieurs types d'image.

Figure 1.6.(a) image astronomique, (b)image médicale, (c)image biologique.

1.3.1 Image numérique

On qualifie une information visuelle qui est représentée sous forme binaire (suite de 0 et de 1) d'image numérique. Mathématiquement, elle peut être définie par :

$I : [0, L-1] \times [0, C-1] \rightarrow [0, M]^p$

M définit une image de L lignes et C colonnes dont l'information portée est définie dans un espace à p dimensions.

- Si I est une image binaire, alors $(p, M) = (1, 1)$.

- Si I est une image en niveaux de gris, alors $p = 1$et le plus souvent $M = 255$.

- Si I est une image couleur, alors $p = 3$ et le plus souvent $M = 255$.

Avant d'évoquer ces différents types d'images, nous allons nous interroger sur ce que signifie une définition de l'image numérique et sa résolution.

1.3.1.1 Définition de l'image numérique

La définition d'une image est le nombre total de pixels qui constitue l'image calculé en multipliant le nombre de pixels de la colonne par le nombre de pixels de la ligne [8].

Par exemple ; la définition d'une image avec 800 pixels de largeur et 600 est 480000.

Cela nous conduit à clarifier la notion de pixel. Le mot Pixel est l'abréviation de « PICtureELement » et représente la plus petite unité d'une image numérique. L'ensemble de ces pixels est contenu dans un tableau à deux dimensions constituant l'image. Les valeurs d'un pixel sont

toujours des mots binaires de longueur k afin qu'il puisse représenter 2^k valeurs différentes. La valeur de k est souvent appelée « profondeur de l'image ». Pour une image couleur typique avec trois composantes RVB, le pixel entier est codé en 24 bits, en conséquence, cette image peut représenter 2^{24} couleurs différentes, ce qui équivaut à 16777216 couleurs différentes [8, 9].

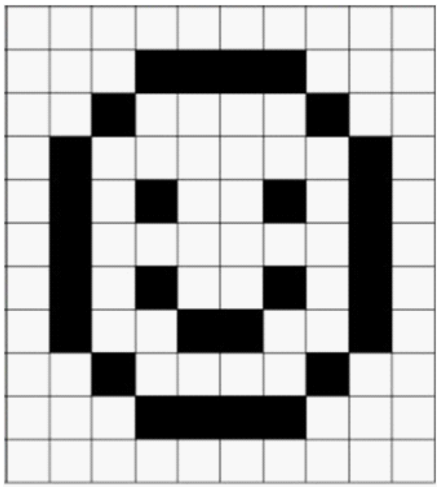


Figure 1.7. Tableau à deux dimensions de l'image.

1.3.1.2 Résolution d'une image

La résolution d'affichage d'une image numérique est le nombre de pixels affichés par unité de surface : elle est couramment exprimée en pixels par pouce (PPP, en anglais : DPI pour Dots PerInch).

Résolution(en ppp)= nombre de pixels (en pixels) / dimension (en pouces)

D'autres mesures existent, comme par exemple lignes par pouce (lpi) pour une production imprimée, ou en pixels par kilomètre pour les images satellite.

Notons que plus la résolution est élevée (plus le pas de discrétisation est faible), mieux les détails de l'image seront représentés.

1.3.2 Types des images

II existe différentes types des images selon le nombre de bits sur lequel est codée la valeur de chaque pixel [10].

1.3.2.1 Image binaire

Les images binaires sont un type spécial d'image où les pixels ne peuvent prendre qu'une des deux valeurs, noir ou blanc. Généralement codé en utilisant un seul bit (0/1) par pixel. C'est typiquement le type d'image que l'on utilise pour scanner du texte quand celui-ci est composé d'une seule couleur.

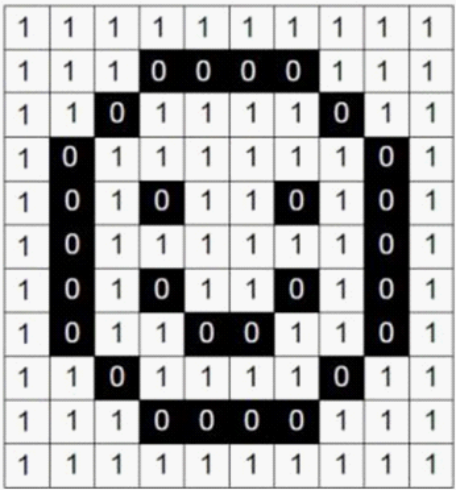


Figure 1.8. Image binaire.

1.3.2.2 Image en niveaux de gris

Une image en niveaux de gris a des couleurs qui sont des nuances de gris (Figure 1.9.b). Le niveau de gris est la valeur de l'intensité lumineuse à un point. La couleur du pixel peut prendre des valeurs allant du noir au blanc en passant par un nombre fini de niveaux intermédiaires.

Une image typique en niveaux de gris utilise $k = 8$ bits par pixel, chaque pixel n'est donc plus représenté par un bit, mais par un octet. La valeur de l'intensité lumineuse correspondante est comprise entre 0 et $2^8 - 1$. Où 0 représente la luminosité minimale (noir) et 255 représente la luminosité maximale (blanc). Dans certains domaines tels que la photographie professionnelle, la médecine et l'astronomie, 8 bits par pixel ne sont pas suffisants, des profondeurs d'image de $12, 14$ et même 16 bits sont souvent utilisées.

1.3.2.3 Image en couleurs

Même s'il est parfois utile de pouvoir présenter des images en noir et blanc ou en niveau de gris, les applications multimédias utilisent le plus souvent des images en couleurs (Figure 1.9.c). La plupart des images en couleur sont basées sur les couleurs primaires rouge, vert et bleu (RVB), lesquels utilisent généralement 8 bits pour chaque composante de couleur. Cela signifie que chaque pixel nécessite $3 \times 8 = 24$ bits pour coder les trois composantes, et l'intervalle de chaque composante de couleur individuelle est de $[0, 255]$. Alors que les images couleurs avec 30, 36 et 42 bits par pixel sont couramment utilisées dans les applications professionnelles.

Les images couleurs indexées, dont une classe très spéciale d'image couleur, qui stockent pour chaque pixel un numéro de couleur (son index), le quel fait référence à une couleur stockée séparément dans une palette.

L'intérêt de ces images est de réduire l'espace de stockage nécessaire, au prix d'une perte de qualité par rapport aux images en vraies couleurs. Par exemple, une image en 256 couleurs indexées occupera sensiblement la même place qu'une image en 256 niveaux de gris (la place occupée par la palette est négligeable par rapport à la taille de l'image).

Figure 1.9. (a) Image binaire, (b) Image en niveau de gris, (c) Image couleur.

1.3.3 Modèles de couleurs

Un modèle de couleur est un système mathématique abstrait pour représenter les couleurs. Comme la couleur est une entité tridimensionnelle, un espace de couleur définit trois couleurs primaires qui correspondent à ces trois dimensions ou axes. A partir de ces trois couleurs primaires

toutes les couleurs possibles sont dérivées en mélangeant diverses quantités de ces primaires. La gamme de couleurs couverte par un modèle de couleurs est appelée soit la gamme, soit l'espace colorimétrique.

Plusieurs modèles de couleurs peuvent être présentés en deux catégories.

1.3.3.1 Modèles de couleurs additifs

Lorsque la lumière est utilisée pour générer des couleurs pour l'affichage, la couleur noire représente une absence totale des couleurs primaires tandis que la couleur blanche correspond à des quantités maximales et égales de chacune des couleurs primaires. On qualifie ce type de modèles de couleurs d'additifs, lesquels sont couramment utilisés par les écrans d'ordinateur et les projecteurs LCD, appareils photo, scanners, etc.

- Modèle de couleur RVB

Le modèle RVB est un modèle de couleur additif qui utilise les couleurs primaires de la lumière : rouge, vert, et le bleu, de sorte que toute couleur peut être obtenue en combinant différentes quantités de ces trois couleurs primaires. Une couleur dans l'espace couleur RVB est définie par trois valeurs numériques (un tuple) qui spécifient la quantité de rouge, de vert et de bleu qui composent la couleur spécifiée. L'origine se trouve à $< 0, 0, 0 >$ qui correspond à la couleur noire tandis que le coin opposé se trouve à $< 1, 1, 1 >$ qui correspond à la couleur blanche. La ligne qui relie l'espace couleur RVB est appelée échelle de gris car tout point situé sur cette ligne est une nuance de gris [10].

1.3.3.2 Modèles de couleurs sous tractifs

Lorsqu'un pigment est utilisé pour créer des couleurs telles qu'une absence totale de tout pigment correspond à la couleur blanche, alors que la combinaison des trois primaires en quantités maximales et égales donne la couleur noire. Les modèles de couleurs soustractives supposent que lorsque la lumière blanche est projeté sur un pigment, le pigment absorbe la puissance de certaines longueurs d'onde et réfléchit la puissance à d'autres longueurs d'onde. Cette absorption est décrite comme une soustraction. En termes de systèmes électroniques, les images rendues avec des imprimantes à encre sont décrites le plus naturellement à l'aide d'un modèle de couleur

soustractif [10].

Modèle de couleur CMJ

Le modèle CMJ est un modèle de couleur soustractif qui utilise les trois couleurs du pigment : Cyan, Magenta et Jaune comme des couleurs primaires. L'espace colorimétrique CMJ peut, comme celui du RVB, être considéré comme un cube où une couleur CMJ est désignée par un tuple de valeurs normalisé.

Le modèle de couleur CMJ est inversement lié au modèle de couleur RVB.

$$\begin{cases} C = 1 - R \\ M = 1 - V \\ J = 1 - B \end{cases} .$$

1.3.4 Types de formats standards d'image

Il existe un grand nombre de formats standards d'enregistrement d'images. Nous présentons ci-après les formats de fichiers les plus utilisés.

1.3.4.1 GIF (Graphic Interchange Format)

Le format GIF (Graphics Interchange Format) a été conçu à l'origine par CompuServe en 1986. Il est depuis devenu l'un des formats les plus largement utilisés pour représenter des images sur le Web. Cette popularité est en grande partie due à sa prise en charge des couleurs indexées à plusieurs profondeurs de bits, à la compression LZW et à la capacité d'encoder des animations simples. GIF est essentiellement un format de fichier image indexé conçu pour les images en couleur et en niveaux de gris avec une profondeur maximale de 8 bits. Par conséquent, les images obtenues par ce format ont une taille généralement très faible. Ce format offre un support efficace pour l'encodage de palettes contenant de 2 à 256 couleurs, dont une peut être marquée pour la transparence [11].

1.3.4.2 TIFF (Tag Image File Format)

Le format TIFF (Tagged Image File Format) est un format de fichier largement utilisé et flexible, conçu pour répondre aux besoins professionnels de divers domaines tels que l'archivage de documents, les applications scientifiques, la photographie numérique. Il a été conçu à l'origine par Aldus, étendu ensuite par Microsoft et développé actuellement par Adobe.

Un fichier TIFF prend en charge les images en niveaux de gris ainsi que les images couleur de différents espaces colorimétriques.

La spécification TIFF fournit une gamme de différentes méthodes de compression (LZW, ZIP, CCITT et JPEG) et d'espaces de couleurs, de sorte qu'il est possible, par exemple, de stocker un certain nombre de variations d'une image de différentes tailles et de les représenter ensemble dans un fichier TIFF unique [11].

1.3.4.3 Graphiques réseau portables (PNG)

PNG (Portable Network Graphics) a été initialement développé pour remplacer le format de fichier GIF lorsque des problèmes de licence sont survenus en raison de son utilisation de la compression LZW. Il a été conçu comme un format d'image universel plus particulièrement pour une utilisation sur Internet. En tant que tel, PNG prend en charge trois types d'images différents :

- Images en vraies couleurs (jusqu'à 3×16 bits/pixel) ;
- Images en niveaux de gris (jusqu'à 16 bits/pixel) ;
- Images couleurs indexées (jusqu'à 256 couleurs).

Le format ne prend en charge qu'une seule image par fichier. La compression sans perte au moyen d'une variante de PKZIP (Phil Katz's ZIP) est utilisée pour ce format. Aucune compression avec perte n'est disponible. Il faut signaler que le format PNG atteint ou dépasse les capacités du format GIF à tous égards, excepté la capacité du GIF à inclure plusieurs images dans un seul fichier pour créer des animations simples.

1.3.4.4 JPEG

Ce format fut développé par le Joint Photographic Experts Group (JPEG) [11]. Malgré son usage courant, le JPEG n'est pas un format de fichier, il ne s'agit en réalité que d'une méthode avec perte de compression des données d'image, notamment pour les images produites par des appareils photo numériques. Ce standard définit une méthode de compression pour les images en niveaux de gris et en couleur.

Il existe de nombreuses spécifications qui précisent le format de fichier.

- JFIF : fichier « JPEG File Interchange Format » (JFIF) : spécifie un format de fichier basé sur la norme JPEG en définissant les éléments nécessaires restants d'un format de fichier, en prenant en charge les images jusqu'à $65535 * 65535$ pixels.

- JPEG-2000 :Ce format est spécifié par une norme ISO-ITU pour surmonter certaines des faiblesses les plus connues du codec JPEG traditionnel. Les améliorations apportées à ce dernier lui permettent d'atteindre des taux de compression nettement plus élevés (jusqu'à $0,25$ bits par pixel sur les images couleur RVB). Malgré ces avantages, JPEG-2000 n'est pris en charge que par quelques applications de traitement d'images et navigateurs Web [11].

1.3.4.5 Windows Bitmap (BMP)

Le format Windows Bitmap (BMP) est un format de fichier simple et largement utilisé sous Windows, prenant en charge les images en niveaux de gris, indexées et en couleurs vraies. Il prend également en charge les images binaires, mais de manière peu efficace, car chaque pixel est stocké en utilisant un octet entier. De plus, le format prend en charge une compression simple sans perte basée sur la longueur d'exécution.

1.4 Cryptage des images numériques

Le but du chiffrement d'images est de garantir la sécurité visuelle du contenu en clair d'une image.

Les images sont différentes du texte. Bien que nous puissions théoriquement utiliser les méthodes de cryptage traditionnelles (présentées dans la section 1.2.2) pour chiffrer directement les

images numériques, ce n'est pas pour autant très recommandé pour deux raisons principales. La première est que la taille de l'image est généralement beaucoup plus grande que celle du texte. Par conséquent, les méthodes traditionnelles ont besoin de beaucoup de temps pour chiffrer directement les données d'image. La seconde est liée au texte décrypté qui doit être égal au texte original. Notons par ailleurs que cette dernière exigence n'est pas nécessaire pour les images numériques. En effet, le niveau d'exigence de la perception humaine des images décryptée est plus faible et de ce fait une image décryptée contenant une faible distorsion est généralement acceptable.

Afin de transmettre des images de manière confidentielle, une variété de schémas de cryptage a été proposée. Ces schémas peuvent être répartis en deux grandes catégories : les schémas du domaine spatial et ceux du domaine fréquentiel.

1.4.1 Schémas du domaine spatial

Le terme domaine spatial fait référence au plan de l'image lui-même, et les approches de cette catégorie sont basées sur la manipulation directe des pixels d'une image. Dans ces algorithmes, le cryptage général détruit généralement la corrélation entre les pixels et rend ainsi les images cryptées incompressibles.

1.4.2 Schémas du domaine fréquentiel

Pour ce type de schémas, il est toujours nécessaire de convertir les valeurs de pixels de l'image en clair en certaines composantes de fréquence avant un traitement ultérieur. Plusieurs méthodes de transformation des fréquences existent. Nous pouvons en citer les plus utilisées dans la littérature telles que : TFD, TWD et TCD.

1.5 Conclusion

Pendant des décennies, des efforts importants ont été consacrés à la conception et au développement des moyens efficaces, qui permettent d'assurer la sécurité des images numériques.

Comme nous l'avons précisé ci-dessus la cryptographie est un outil important pour la protection du contenu de ces images. Ces dernières sont chiffrées avant d'être transmises.

Lors du développement d'un système de cryptage d'images, nous devons tenir compte de certaines caractéristiques des images comme une plus grande taille, une redondance plus élevée et une forte corrélation de pixels adjacents. Pour ces raisons, les algorithmes symétriques et asymétriques traditionnels ne conviennent pas au chiffrement d'images. En 1963, Edward Lorenz a introduit le concept de théorie du chaos. Les systèmes basés sur le chaos conviennent au chiffrement d'images, en raison de leurs propriétés telles que la sensibilité aux conditions initiales, l'imprévisibilité et l'ergodicité. Récemment, le développement des cryptosystèmes chaotiques est devenu un domaine de recherche largement acceptable pour le cryptage d'images. Un état de l'art sur ce domaine s'impose et constitue donc l'objet du troisième chapitre.

A ce stade, il convient de souligner que les apports mathématiques relèvent une importance majeure dans notre thèse. Nous lui consacrons le chapitre suivant, en montrant comment nous avons mobilisé la théorie du chaos mais aussi les fonctions génératrices.

Chapitre 2

Introduction à la théorie du chaos et aux fonctions génératrices

---

2.1 Introduction

La notion du temps dans l'étude des modèles physiques et mathématiques remonte à Galilée, qui est le premier à introduire cette notion dans l'étude de la chute des corps et le mouvement de la terre autour du soleil. Cette introduction du temps dans les équations sera qualifiée ensuite d'étude des systèmes dynamiques. Au XVIII siècle, Isaac Newton définit l'équivalence masse-énergie et trouve de manière explicite la cause de certains mouvements apparemment désordonnés. Il parle de déterminisme. Selon cette vision, tout semble être parfaitement prédictible et causal. Le futur devient prévisible : il suffit de traduire le mouvement en équations différentielles et de les résoudre [11].

En général, un système dynamique décrit des phénomènes qui évoluent au cours du temps. Le terme « système » dans les modèles mathématques et physiques fait référence à un ensemble de variables d'état, dont la valeur évolue au cours du temps, et aux interactions entre ces variables.

Le chaos est un phénomène qui se produit largement dans les systèmes dynamiques. Du point de vue pédagogique le phénomène a été considéré comme complexe. Il a été soigneusement mis de coté en raison de la difficulté de proposer une analyse simplifié qui pourrait aider les étudiants et les chercheurs à immerger dans ce phénomène complexe mais trés intéressant et obtenir des outils et des expériences exploitables. Depuis la présence de chaos s'est répandu dans beaucoup de champs disciplinaires.

2.2 Systèmes dynamiques

Un système dynamique est défini à partir d'un ensemble de variables qui forment le vecteur d'état où n représente la dimension du vecteur. Un système dynamique en temps continu est décrit par un système d'équations différentielles, alors qu'en temps discret on parle d'un système d'équations aux différences finies.

Les systèmes dynamiques sont classés en deux catégories :

1. Systèmes dynamiques discrets (à temps discret),
2. Systèmes dynamiques continus (à temps continu).

a. Systèmes dynamiques à temps continu

Dans ce cas, le système dynamique peut-être modélisé mathématiquement par un système d'équations différentielles ordinaires

$$\dot{x}(t) = F(x(t), t), \tag{2.1}$$

où $F : \mathbb{R}^n \times \mathbb{R}_+ \to \mathbb{R}^n$, indique la dynamique du système.

Si la dynamique du système donnée par l'équation (2.1) est indépendante de l'instant t considéré, ce type de système est qualifié d'autonome. La dynamique dans ce cas particulier a la forme suivante :

$$\dot{x}(t) = F(x(t)). \tag{2.2}$$

On considère l'exemple du célèbre système différentiel de Lorenz donné par les équations suivantes :

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = x(p - z) \\ \frac{dz}{dt} = xy - bz \end{cases} . \tag{2.3}$$

Les paramètres pour l'exemple de trajectoire donné dans l'équation (2.3) ont été choisis de la manière suivante :

$$\sigma = 10, p = 28, b = 8/3,$$

avec la condition initiale

$$(x_0, y_0, z_0) = (2, 5, 20).$$

Ce système présente une superbe attractrice étrange en forme d'ailes de **papillon**. On observe que la dynamique du système de Lorenz donnée par les équations (2.3) est indépendante de l'instant t considérée. Généralement ce type de système est qualifié d'autonome [13].

La dynamique du système, dans ce cas particuliers, est donnée par la forme suivante [14] :

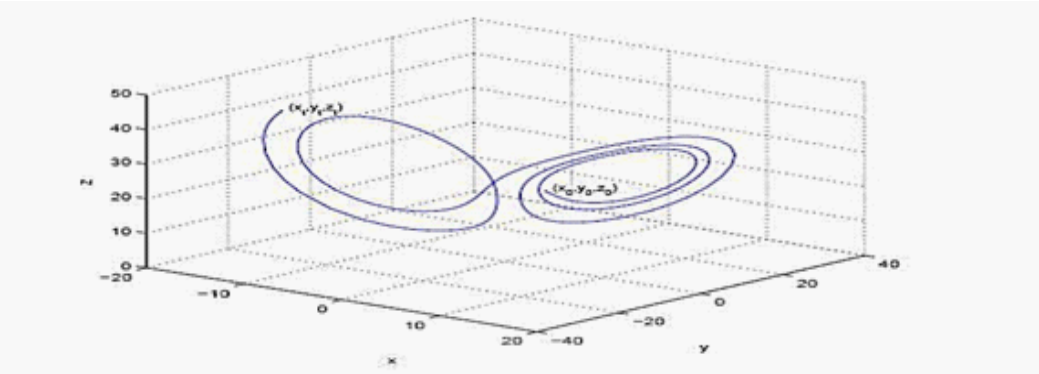


Figure 2.1. Exemple de trajectoire du le système Lorenz.

b. Systèmes dynamiques à temps discret

Un système dynamique dans le cas discret est représenté par une équation aux différences finies sous la forme :

$$x(k+1) = G(x(k), k). \tag{2.4}$$

G :$F : \mathbb{R}^n \times \mathbb{Z}_+ \to \mathbb{R}^n$ Indique la dynamique du système en temps discret.

L'évolution d'un système dynamique unidimensionnel peut être décrite par une fonction itérative appelée en anglais « *Map* ».

En temps discret on définit aussi le système autonome comme une dynamique qui ne dépend pas de l'instant k [13].

$$x(k+1) = G(x(k)). \tag{2.5}$$

2.2.1 Définition du chaos

Le mot CHAOS prend origine du terme « $\chi\alpha o\sigma$ » , utilisé par les Grecs pour décrire l'espace vide infini dont ils ont supposé l'existence avant l'émergence de toutes choses. Le chaos ne signifie pas absence d'ordre ; c'est l'imbrication d'ordre et de désordre, que l'on appelle chaos déterministe.

2.2.2 Systèmes dynamiques chaotiques

Le chaos tel que le scientifique le comprend ne signifie pas l'absence d'ordre, il se rattache plutôt à une notion d'imprévisibilité, d'impossibilité de prévoir une évolution à long terme du fait que l'état final dépend de manière sensible de l'état initial. Les systèmes chaotiques ont un comportement infiniment complexe.

On appelle donc un système dynamique chaotique, un système qui dépend de plusieurs paramètres et qui est caractérisé par une extrême sensibilité aux conditions initiales et une forte récurrence [12].

Il n'est pas déterminé ou modélisé par des systèmes d'équations linéaires ni par les lois de la mécanique classique, pourtant ils ne sont pas nécessairement aléatoires, relevant du seul calcul des probabilités [12].

2.2.3 Caractéristiques des systèmes chaotiques

On va présenter quelques caractéristiques qui permettent de comprendre qualitativement les points marquants d'un système chaotique [13].

a) Non-linéarité :

Un système chaotique est un système dynamique non linéaire. Un système linéaire ne peut Pas être chaotique. On parle de non linéarité lorsque l'entrée d'un système n'est pas proportionnelle à sa sortie, ou lorsqu'un événement a des imprévisibles à long terme [17]. La notion de système dynamique chaotique est relative à tous les systèmes dont l'évolution dépend du temps. L'évolution irrégulière du comportement d'un système chaotique est due aux non linéarités.

b) Déterminisme :

Un système chaotique a des règles fondamentales déterministes et non probabilistes.

La notion de déterminisme signifie la capacité de " prédire " le future d'un phénomène à partir d'un évènement passé ou présent.

c) Sensibilité aux conditions initiales :

Certains phénomènes dynamiques non linéaires sont si sensibles aux conditions initiales que, même s'ils sont régis par des lois rigoureuses et parfaitement déterministes, les prédictions exactes

sont impossibles.

Une autre propriété des phénomènes chaotiques est qu'ils sont très sensibles aux perturbations. L'un des premiers chercheurs à s'en être aperçu fut Edward Lorenz qui s'intéressait à la météorologie et par conséquent aux mouvements turbulents d'un fluide comme l'atmosphère. Lorenz venait de découvrir que dans des systèmes non linéaires, d'infimes différences dans les conditions initiales engendraient à la longue des trajectoires totalement différentes. Il a illustré ce fait par l'effet papillon. Le battement d'ailes d'un papillon aujourd'hui à Tlemcen engendrerait une tempête le mois prochain au Québec.

Il est clair que la moindre erreur ou imprécision sur la condition initiale interdit de décider à tout temps quelle sera la trajectoire effectivement suivie et, en conséquence, de faire une prédiction sur l'évolution à long terme du système. Une des propriétés essentielles du chaos est donc bien cette sensibilité aux conditions initiales que l'on peut caractériser en mesurant des taux de divergence des trajectoires.

d) Imprévisibilité :

En raison de la sensibilité aux conditions initiales qui peuvent être connues seulement à un degré fini de précision le chaos ne signifie pas l'absence d'ordre, il se rattache plutôt à une notion d'impossibilité de prévoir une évolution à long terme du fait que l'état final dépend de manière si sensible de l'état initial.

e) Aspect aléatoire :

Une autre caractéristique des systèmes chaotiques peut être observée sur les courbes de la Figure 2.2. En effet, un système chaotique évolue d'une manière qui semble être aléatoire. La Figure 2.2 permet de comparer l'évolution périodique est donc prédictible d'un système classique avec l'évolution plus complexe, non périodique et non prédictible du système chaotique de Lorenz.

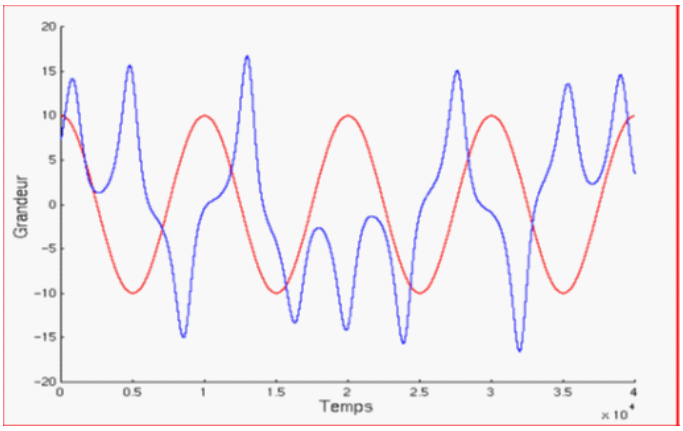


Figure 2.2. Evolution dans le temps d'un système chaotique, comparé à une sinusoïde.

f) Attracteur étrange :

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

Il existe deux types d'attracteurs : **les attracteurs réguliers** et l**es attracteurs étranges ou chaotiques.**

– **Attracteurs réguliers**

Les attracteurs réguliers caractérisent l'évolution de systèmes non chaotiques, et peuvent être de deux sortes :

1- Un point fixe :

La trajectoire du pendule dissipatif simple (dans l'espace des phases représentant son altitude et sa vitesse), par exemple, tend vers l'origine du repère, quelles que soient la position et la vitesse initiales.

C'est-à-dire pour un point fixe stable, un écartement de sa position initiale dû à une quelconque perturbation n'aura aucune influence (figure 2.3 (a)). Le mouvement perturbé s'atténuera pour faire revenir l'état du système à sa position initiale.

2- Un cycle limite :

La trajectoire du pendule idéal dans ce même espace des phases, par exemple.

Pour tous les attracteurs réguliers, c'est à dire pour tous les systèmes non-chaotiques, des trajectoires qui partent de "points" proches l'un de l'autre dans L'espace de phase restent indéfiniment voisines. On sait donc prévoir l'évolution de ces systèmes, à partir d'une situation connue [13].

Il sera caractéristique d'un mouvement périodique entretenu (apport d'énergie extérieure pour composer la dissipation). Le système ne revient pas à une position initiale mais y repassera après avoir parcouru le cycle. Sa représentation graphique dans l'espace des phases (figure 2.3 (b)) est une courbe fermée.

(a) Point fixe (b) Cycle limite

Figure 2.3. Deux exemples d'attracteurs réguliers dans un espace de phase 2D.

– **Les attracteurs étranges**

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

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

jamais. Ainsi, deux points très proches au départ (conditions initiales) peuvent se retrouver à deux extrémités opposées de l'attracteur (conditions finales). Cela traduit le comportement divergent des phénomènes chaotiques. On obtient ainsi des attracteurs différents (en fonction des systèmes étudiés), qui présentent des formes diverses et surprenantes [14].

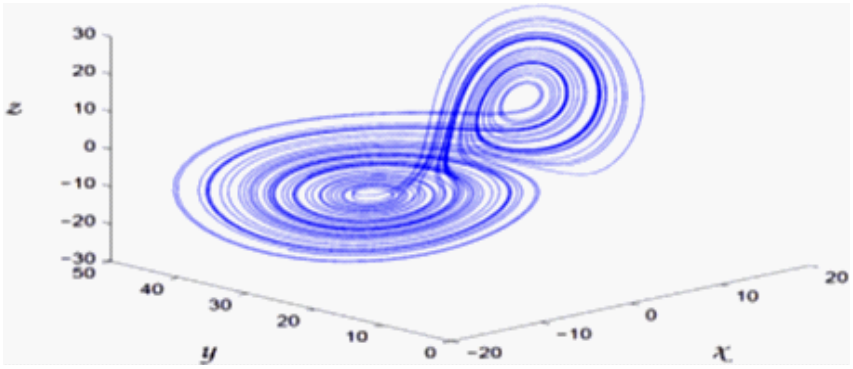


Figure 2.4. Attracteurs étranges.

2.2.4 Outils d'étude des systèmes chaotiques

a. Espace de phase

L'espace des phases est une structure correspondant à un certain nombre de variables d'état qui ont la propriété de définir complètement l'état du système à un instant donné.

L'évolution de chacune de ces variables d'état est responsable du comportement dynamique du système. Cet espace est appelé l'espace de phase où chaque point définit un état, et le point associé à cet état décrit une trajectoire.

b. Fractale

Un objet fractal est doté d'une propriété dite d'auto-similitude. Ce phénomène est observé dans les systèmes chaotiques, c'est-à-dire qu'on y observe une invariance par changement d'échelle. Si l'on zoome d'un facteur suffisant sur une partie de la courbe, on retrouve la structure et la topologie de celle-ci à sa taille initiale. Un zoom plus grossissant encore reproduit le phénomène, aussi loin qu'on puisse aller.

c. Exposants de Lyapunov

L'évolution chaotique et difficile à appréhender car la divergence des trajectoires sur l'at-

tracteur est rapide. Pour cette raison on essaye, si c'est possible, de mesurer sinon d'estimer la vitesse de divergence ou de convergence. Cette vitesse est donnée par l'exposant de Lyapunov qui caractérise le taux de séparation de deux trajectoires très proches.

d. Section de Poincaré

Dans l'espace de phase, la direction tangentielle à la trajectoire d'un système autonome peut changer si on change les paramètres du temps, et par conséquent ne traduit pas la géométrie de l'attracteur. Ainsi, la composante tangentielle des points xk peut être négligée, réduisant ainsi la dimension de l'espace de phase par 1, et transformant la trajectoire continue en une trajectoire discrète.

Cette méthode s'appelle la section de Poincaré, et se résume à choisir une surface $\sum$ dans l'espace de phase et de construire une application inversible P sur cette surface traduisant la relation entre les points d'intersections successives entre la trajectoire et la surface [9]. La Figure 2.5 illustre le principe.

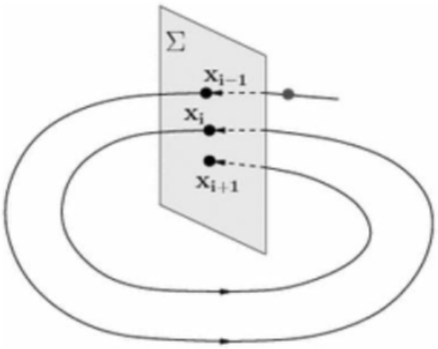


Figure 2.5. Construction de la section de Poincaré.

Le temps discret résultant de l'intersection est variable, et pas nécessairement proportionnel au temps d'intégration Δt. Le nombre de points d'intersection obtenu dépend sensiblement de la surface choisie. Un choix standard de la surface est la section à phase constante où la durée écoulée entre deux intersections est constante.

e. Dimension de l'attracteur

Les attracteurs des systèmes chaotiques dissipatifs, où les trajectoires éloignées rétrécissent vers l'intérieur d'un méta-cube, ont généralement une géométrie très complexe, d'où l'appellation

d'attracteurs étranges comme mentionné précédemment.

f. Notion de bifurcation

Le terme bifurcation veut dire division d'une branche principale en au moins deux branches. Le comportement d'un système dynamique non-linéaire peut changer quand un paramètre du système change. Ce changement de comportement correspond à un phénomène de bifurcation ; il est accompagné d'un changement de type de stabilité. Le terme de bifurcation est utilisé pour désigner dans un sens large, toute modification qualitative du comportement d'un système dynamique, suite à la variation de l'un des paramètres dont dépend le système étudié. Il existe plusieurs types de bifurcations, parmi lesquelles on peut citer : bifurcation stationnaire, bifurcation col nœud [14].

– **Diagramme de bifurcation**

Dans ce cas, on peut s'intéresser à la construction d'un diagramme représentant l'évolution de population x_n en fonction du paramètre p. Les différents calculs pour voire l'évolution du système en fonction de la valeur de p, montrent qu'il existe un « trajet » qui mène d'un état l'ordre à un autre état le chaos pour des valeurs de p variant de 1 à 4 avec un pas de 0.001 et 50 itérations sur x_n on obtient le diagramme de la Figure 2.6.

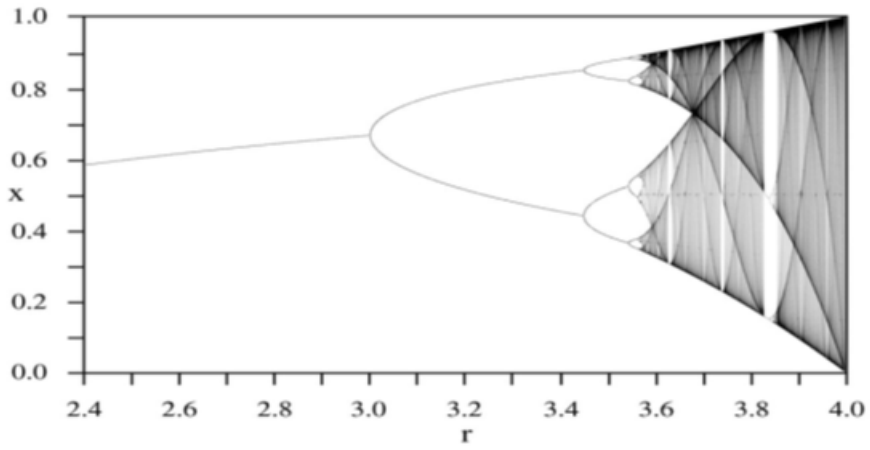


Figure 2.6. Diagramme de bifurcation de la fonction Logistique.

2.2.5 Exemples des systèmes chaotiques

Dans ce qui suit, nous présentons quelques exemples de systèmes chaotiques les plus célèbre.

a. Systèmes à temps continu

On rappelle les deux systèmes ci-dessous car ils ont une importance historique dans l'histoire du chaos :

Système de Lorenz

Le système de Lorenz est un système dynamique chaotique qui fut utilisée à l'origine pour simuler le mouvement d'une particule dans des courants de convection et des systèmes météorologiques simplifiés. De petites différences dans les conditions initiales conduisent rapidement à des valeurs divergentes. C'est ce qu'on appelle parfois l'effet papillon. Ce système est l'un des éléments fondât du développement de la théorie du chaos. Il est utile comme source audio chaotique ou comme source de modulation basse fréquence.

Ce système est défini par le système d'équations différentielles couplées suivant :

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = x(p - z) - y \\ \frac{dz}{dt} = xy - \beta z \end{cases}, \tag{2.7}$$

σ : dépend des propriétés du fluide et caractérise la viscosité et la conductivité thermique du fluide

p : varie en fonction du gradient de température dans la cellule.

β : varie avec la géométrie de la cellule de convection.

L'évolution dans le temps de coordonnée (x) dans l'espace de phase des valeurs numériques $\sigma = 10$, $p = 28$, $\beta = 8/3$ qui implique un comportement chaotique.

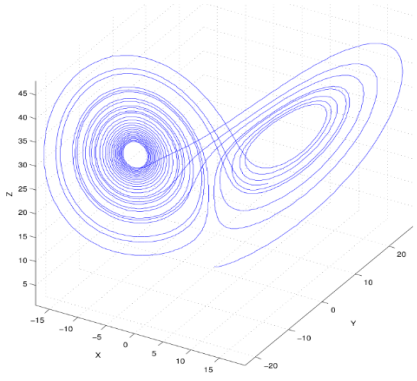


Figure 2.7. Attracteur chaotique de Lorenz.

b. Systèmes à temps discret

Système de Hénon

La récurrence de Hénon est un modèle proposé en 1976 par le mathématicien Michel Hénon [15], le modèle d'état associé est :

$$\begin{cases} x_{n+1} = y_n + 1 - ax_n^2 \\ y_{n+1} = bx_n \end{cases}, \tag{2.8}$$

tel que $(x_n, y_n) \in \mathbb{R}^2$, a et b représentent des paramètres.

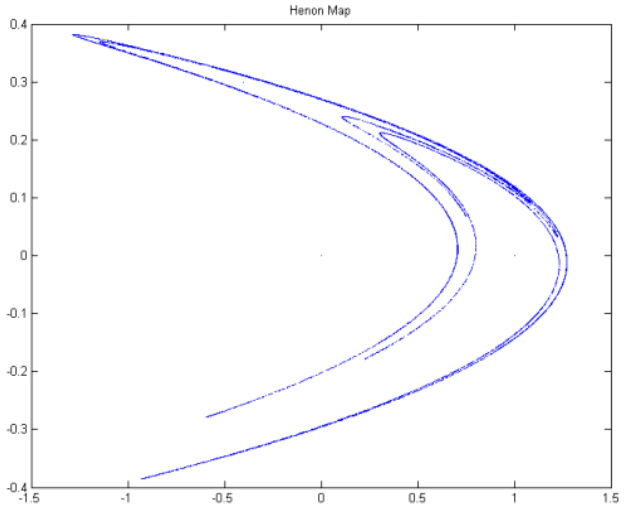


Figure 2.8. Attracteur chaotique de Hénon.

2.3 Les tests du NIST

Les tests du NIST (National Institute of Standards and Technology) forment un paquetage statistique de tests conçus pour détecter l'aspect aléatoire des séquences binaires à la sortie des générateurs de nombres aléatoires ou pseudo-aléatoires utilisés dans des applications nécessitant de la cryptographie.

La sortie des générateurs de nombre pseudo-aléatoires doit être imprévisible en ignorant l'entrée.

Les tests du NIST se concentrent sur différents types d'aspects non-aléatoires que l'on peut trouver dans une séquence et les comparer avec une séquence aléatoire. Certains tests sont décomposables en un ensemble de sous-tests.

Il est important que l'ordre d'application des tests soit arbitraire. Cependant, le test de fréquence doit être appliqué en premier lieu, dans la mesure où il fournit la preuve la plus évidente de l'aspect non aléatoire, qui est la non uniformité. En conséquence, si le test ne réussit pas, la probabilité d'échec des tests suivants est élevée.

Le résultat de chaque test est donné par une P-Value qui représente la probabilité qu'un générateur de nombre aléatoire parfait produise une séquence moins aléatoire que la séquence déjà testée. Cette variable a une distribution uniforme sur l'intervalle $[0, 1]$.

P-Value $= 1$: aspect aléatoire parfait.

P-Value $= 0$: aspect non aléatoire.

Une constante α est fixée dans l'intervalle $[0.001 - 0.01]$. Elle est appelée "niveau de signification". Si les P-Value sont supérieures ou égales à α, alors la séquence réussit le test sinon elle échoue.

Nous présentons dans ce qui suit les 15 tests du NIST.

T1. Test de fréquence

Le but de ce test est de déterminer si les nombres de 0 et de 1 dans une séquence sont approximativement les mêmes comme il est prévu pour une séquence réellement aléatoire. Le test vérifie si la fraction de 1 est proche de $1/2$.

T2. Test de fréquence dans un bloc

Le but de ce test est de déterminer si la fréquence des 1 dans un bloc de M bits est approximativement $1/2$. Pour un bloc de taille $M = 1$, on revient au test de fréquence.

T3. Test d'exécution

Le « Runs Test » permet de déceler des oscillations entre les 0 et les 1 trop rapides ou trop lentes.

T4. Test de la plus longue série des uns dans un bloc

Ce test consiste à déterminer si la distribution de longues séries de 1 est conforme avec les probabilités théoriques.

T5. Test du rang

Le focus du test est le rang de sous-matrices disjointes de la séquence entière. Le but de ce test est de vérifier la dépendance linéaire entre les chaînes de longueur fixe de la séquence originale.

T6. Test de la transformée de Fourier discrète

Ce Test vérifie la hauteur des pics dans la transformée de Fourier discrète de la séquence. Son but est de détecter les caractéristiques périodiques dans la séquence éprouvée qui indiquerait un écart par rapport à l'hypothèse du hasard. Le but est de détecter si le nombre de pics qui dépassent le seuil de 95% est significativement différent de 5%.

T7. Test de correspondance des modèles sans chevauchement

Ce test met le focus sur le nombre d'occurrences d'une chaîne pré-spécifiée. Son but est de détecter les générateurs qui produisent trop d'occurrences d'un modèle non périodique donné.

T 8. Test de correspondance des modèles de chevauchement

Le but de ce test est identique à celui du $7^{ème}$ test qui consiste à calculer le nombre d'occurrences de B dans chacun des N blocs. On crée une fenêtre de m bits qui traverse la séquence en comparant les bits de la fenêtre avec B. Un compteur s'incrémente quand il y a une égalité. Après chaque test, la fenêtre est décalée de 1 bit.

T9. Test statistique universel de Maurer

Le but de ce test est de déterminer si la séquence est compressible ou non sans perte d'information. Sachant qu'une séquence nettement compressible est considérée comme non aléatoire.

T10. Test d'entropie approximative

Le but de ce test est la fréquence de tous les m-bits modèles de chevauchement possibles dans toute la séquence. Plus précisément, il s'agit de comparer la fréquence des blocs de chevauchement de deux longueurs consécutives/adjacentes (M et $M + 1$) avec le résultat attendu pour une séquence aléatoire.

T11. Test de complexité linéaire

Ce test est basé sur la longueur d'un registre à décalage à rétroaction linéaire. Son but est de déterminer si la séquence est assez complexe pour être considérée comme aléatoire.

Les séquences aléatoires sont caractérisées par de long LFSR. Bien évidemment, un LFSR trop court implique l'aspect non aléatoire.

T12. Test en série

Ce test est basé sur la fréquence de tous les m-bits de chevauchement tout au long de la séquence. Son but est de déterminer si le nombre d'occurrences des $2m$ des modèles de chevauchement des m bits est identique à celui d'une séquence aléatoire (m est le nombre de bits dans chaque bloc).

Une séquence est aléatoire telle que chaque modèle de m-bits a la même chance d'apparence que d'autre m-bits. Pour $m = 1$, le test de série est équivalent au test de fréquence.

T13. Test des sommes cumulées

Le but de ce test est de déterminer si la somme cumulative dans une séquence est trop grande ou trop petite (somme de 1 et -1). Ceci indique la présence de nombre important de 0 ou de 1.

La somme cumulative peut être considérée comme une marche au hasard (random walk) qui est un modèle mathématique d'un système possédant une dynamique discrète composée d'une succession de pas aléatoires, ou effectuée « au hasard ». Il convient de noter que pour une séquence aléatoire, les excursions du "random walk" doivent être proches de 0.

T14. Test des excursions aléatoires

Un cycle d'une marche aléatoire (excursion) est une séquence de pas aléatoires qui commence et finit à son origine.

On a recours à déterminer si le nombre de visites à un état particulier d'un cycle dévie de ce qui est attendu.

Ce test est une série de 8 tests et conclusions. Un test est une conclusion pour chaque état : $-4, -3, -2, -1$ et $+1, +2, +3, +4$;

T15. Test des variantes d'excursions aléatoires

Le but de ce test est de calculer le nombre de fois où un état particulier est visité, et de détecter la déviation par rapport au nombre de visites attendu à différents états de la marche aléatoire. Ce test est en réalité une série de dix-huit tests (et conclusions), tout en admettant qu'un test est une conclusion pour chacun des Etats :$-9, -8, ..., -1$ et $+1, +2, ..., +9$.

2.4 Domaines d'application du chaos

Historiquement, le chaos est utilisé en mathématiques et en physique dans le démarrage. Elle s'est prolongée dans l'ingénierie et, plus récemment, dans les sciences de l'information et les sciences sociales. Il y a quelques années, il y a eu un intérêt croissant pour les applications commerciales et industrielles des systèmes chaotiques. Il existe plusieurs types d'applications commerciales et industrielles latentes basées sur différents aspects du système basé sur le chaos qui sont présentés dans le tableau 2.

Catégorie	**Applications**
Contrôler	Contrôle des comportements irréguliers dans les appareils et les systèmes.
Synthèse	Contrôle potentiel de l'épilepsie, amélioration des systèmes hésitants, tels que les gyroscopes laser en anneau. Commutation de paquets dans les réseaux informatiques
Synchronisation	Communications sécurisées, radio large bande chaotique et cryptage.
Traitement d'informations	Codage, décodage et stockage d'informations dans des systèmes chaotiques, tels que des éléments de mémoire et des circuits. Meilleure performance des réseaux de neurones. La reconnaissance de formes.

Prévision à court terme	Maladies contagieuses, météo, économie.
Ingénierie	Contrôle des vibrations, stabilisation des circuits, réactions chimiques, turbines, réseaux électriques, asers, lits fluidisés, combustion, et bien d'autres.
Ordinateurs	Commutation de paquets dans les réseaux informatiques. Chiffrement. Contrôle du chaos dans les systèmes robotiques.
Communications	Compression et stockage des informations Réseau informatique conception et gestion.
Médecine et Biologie	Cardiologie, analyse du rythme cardiaque (EEG), Prédiction et contrôle de l'activité cardiaquei régulière (défibrillateur sensible au chaos).

Tableau 2.1. Applications basées sur le chaos.

2.5 Relations de Récurrences

Soit IK un corps commutatif ($IK = \mathbb{R}$ ou $\mathbb{C}$), pour plus de détails, vous pouvez consulter la référence [16].

2.5.1 Relation de récurrence linéaire homogène

Définition 2.1 *Une relation de récurrence est dite linéaire homogène d'ordre k à coefficients constant, si elle est de la forme :*

$$u_n + d_1 u_{n-1} + d_2 u_{n-2} + ... + d_k u_{n-k} = 0, \tag{2.9}$$

où $d_1, d_2, ..., d_k \in \mathbb{R}, d_k \neq 0$.

Remarque 2.1 *Si $u_n = 0$ est une solution de l'équation* (2.9)*, elle s'appelle solution triviale .*

Remarque 2.2 *Si $u_n = x^n$ est solution de l'équation* (2.9) *avec $u_n \neq 0$, vérifie*

$$x^n + d_1x^{n-1} + d_2x^{n-2} + ... + d_kx^{n-k} = 0 \Leftrightarrow x^k + d_1x^{k-1} + d_2x^{k-2} + ... + d_k = 0.$$

Cette dernière équation est l'équation caractéristique de la relation de récurrence.

2.5.2 Polynôme caractéristique

Définition 2.2 *Soit $u_n + d_1u_{n-1} + d_2u_{n-2} + ... + d_ku_{n-k} = 0$, le polynôme caractéristique qui lui correspond est :*

$$P(x) = x^k + d_1x^{k-1} + d_2x^{k-2} + ... + d_k.$$

Remarque 2.3 *L'équation caractéristique associée à la relation de récurrence est obtenue en annulant le polynôme caractéristique de cette dernière. Les racines du polynôme caractéristique sont appelées les racines caractéristiques.*

Théorème 2.1 *Soient $d_1, d_2, ..., d_k$ des nombres réels tels que d_k est non nul. Supposons que le polynôme caractéristique $P(x)$ admette k racines distinctes $x_1, x_2, ..., x_k$, alors u_n est une solution générale de la relation de récurrence si et seulement si*

$$u_n = c_1x_1^n + c_2x_2^n + ... + c_kx_k^n,$$

avec $c_1, c_2, ..., c_k$ des constantes réelles.

Exemple 2.1 *Soit la récurrence de la suite de Fibonacci :*

$$\begin{cases} F_n = F_{n-1} + F_{n-2} \quad \text{pour } n \geq 2 \\ F_0 = F_1 = 1 \end{cases}.$$

Son équation caractéristique est donnée par :

$$x^2 - x - 1 = 0,$$

qui a pour racines simples les valeurs suivantes :

$$x_1 = \frac{1+\sqrt{5}}{2} \text{ ou } x_2 = \frac{1-\sqrt{5}}{2}.$$

La solution générale est donnée par :

$$F_n = c_1 x_1^n + c_2 x_2^n,$$

chercher c_1, c_2 sur la base de la relation suivante :

$$\begin{cases} c_1 + c_2 = 1 \text{ si } n = 0 \\ c_1 x_1 + c_2 x_2 = 1 \text{ si } n = 1 \end{cases}.$$

Par suite :

$$\begin{cases} c_1 = \frac{1+\sqrt{5}}{2\sqrt{5}} \\ c_2 = \frac{-1+\sqrt{5}}{2\sqrt{5}} \end{cases},$$

alors :

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right].$$

2.5.3 Polynômes de Chebyshev de 1^{er} et $2^{ème}$ espèce

Définition 2.3 *On définit la fonction T_n par*:

$$T_n(\cos\theta) = \cos(n\theta), \ \theta \in [0, \pi],$$

si $x \in [-1, 1]$ alors on a :

$$T_n(x) = \cos(n(\arccos x)).$$

Proposition 2.1 *Les polynômes de Chebyshev de 1^{er} espèce sont définies par la relation de*

récurrence suivante :

$$\begin{cases} T_0(x) = 1 \\ T_1(x) = x \\ T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x), n \geq 2 \end{cases}$$

Preuve: Il suffit de prouver que :

$$T_n(x) + T_{n+2}(x) = 2xT_{n+1}(x).$$

Pour $\theta \in [0, \pi]$, $n \in \mathbb{N}$, on a :

$$\begin{aligned} \cos(n\theta) + \cos((n+2)\theta) &= \cos((n+1)\theta)\cos\theta + \sin((n+1)\theta)\sin\theta \\ &\quad + \cos((n+1)\theta)\cos\theta - \sin((n+1)\theta)\sin\theta \\ &= 2\cos\theta\cos((n+1)\theta), \end{aligned}$$

ce qui fournit encore

$$\forall\theta \in [0, \pi] : T_n(\cos\theta) + T_{n+2}(\cos\theta) = 2\cos\theta T_{n+1}(\cos\theta),$$

donc :

$$\forall x \in [-1, 1] : T_n(x) + T_{n+2}(x) = 2xT_{n+1}(x).$$

■

Définition 2.4 *On définit la fonction U_n par :*

$$\sin\theta U_n(\cos\theta) = \sin(n\theta),\ \theta \in [0, \pi],$$

si $x \in]-1, 1[$ alors on a :

$$U_n(x) = \frac{\sin(n(\arccos x))}{\sqrt{(1-x^2)}}.$$

Proposition 2.2 *Les polynômes de Chebyshev de $2^{ème}$ espèce sont définies par la relation récur-*

rence suivante :

$$\begin{cases} U_0(x) = 1 \\ U_1(x) = 2x \\ U_n(x) = 2xU_{n-1}(x) - U_{n-2}(x), n \geq 2 \end{cases}.$$

Preuve: Il suffit de prouver que :

$$U_n(x) + U_{n+2}(x) = 2xU_{n+1}(x).$$

Pour $\theta \in [0, \pi]$, $n \in \mathbb{N}$, on a :

$$\begin{aligned} \sin(n\theta) + \sin((n+2)\theta) &= \sin((n+1)\theta)\cos\theta - \cos((n+1)\theta)\sin\theta \\ &\quad + \sin((n+1)\theta)\cos\theta + \cos((n+1)\theta)\sin\theta \\ &= 2\cos\theta\cos((n+1)\theta), \end{aligned}$$

ce qui fournit encore

$$\forall\theta \in [0, \pi] : \sin\theta U_n(\cos\theta) + \sin\theta U_{n+2}(\cos\theta) = 2\cos\theta\sin\theta U_{n+1}(\cos\theta)$$

donc :

$$\forall x \in]-1, 1[: U_n(x) + U_{n+2}(x) = 2xU_{n+1}(x).$$

■

2.6 Séries formelles

Soit K un corps commutaif $(K = \mathbb{R} \vee \mathbb{C})$.

Définition 2.5 *Les éléments de l'ensemble* $K[[X]] = \left\{ \sum_{n=0}^{\infty} a_n x^n, a_n \in A \right\}$ *s'appellent les séries formelles à coefficients dans* K. *Pour* $n \in \mathbb{N}$, x^n *s'appelle le monôme de degré* n *et* a_n *est son coefficient.*

Définition 2.6 *Soient* $u(z) = \sum_{n=0}^{\infty} a_n x^n$ *et* $v(z) = \sum_{n=0}^{\infty} b_n x^n$ *deux séries formelles. On peut définir les opérations comme suite*

1. La somme

$$u + v = \sum_{n=0}^{\infty} (a_n + b_n) x^n.$$

2. Le produit

$$u \times v = \sum_{n=0}^{\infty} (\sum_{k=0}^{n} a_k b_{n-k}) x^n.$$

3. Multiplication par un scalaire

$$\lambda u = \sum_{n=0}^{\infty} \lambda a_n x^n.$$

4. Dérivation

$$u' = \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n.$$

2.6.1 Inverse d'une série formelle

Définition 2.7 *On dit que la série* $\sum_{n=0}^{\infty} b_n z^n$ *est l'inverse de de la série* $\sum_{n=0}^{\infty} a_n z^n$ *si*

$$\left(\sum_{n=0}^{\infty} a_n z^n \right) \left(\sum_{n=0}^{\infty} b_n z^n \right) = 1.$$

Proposition 2.3 *Une série formelle* $\sum_{n=0}^{\infty} a_n z^n$ *est inversible si et seulement si* $a_0 \neq 0$.

Preuve: Soit $\sum_{n=0}^{\infty} b_n z^n$ est l'inverse de la série $\sum_{n=0}^{\infty} a_n z^n$ telle que

$$\begin{aligned} \left(\sum_{n=0}^{\infty} a_n z^n \right) \left(\sum_{n=0}^{\infty} b_n z^n \right) &= 1 \\ \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n &= 1 \\ a_0 b_0 + \sum_{n=1}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n &= 1, \end{aligned}$$

par identification ; on trouve

$$a_0 b_0 = 1,$$

et

$$\sum_{n=1}^{\infty}\left(\sum_{k=0}^{n}a_k b_{n-k}\right)x^n=0,$$

ce qui donne le coefficient a_0 non nul.

Réciproquement, supposons que $a_0\neq 0$, alors le système triangulaire d'équations

$$\begin{cases} a_0b_0=1 \\ a_1b_0+a_0b_1=0 \\ . \\ . \\ a_0b_0+a_{n-1}b_1+...+a_0b_n=0 \end{cases}$$

a une solution unique. ■

Exemple 2.2

1. La série $\sum_{n=0}^{\infty}z^n$ *est inversible et d'inverse* $1-z$.

2. La série $\sum_{n=0}^{\infty}(-1)^n z^n$ *est inversible et d'inverse* $1+z$.

3. La série $\sum_{k=0}^{n}\frac{z^n}{n}$ *est inversible et son inverse* $\sum_{n=0}^{\infty}(-1)^n\frac{z^n}{n}$.

2.7 Fonctions génératrices ordinaire

Définition 2.8 *Soit* $(u_n)_{n\geq 0}$ *une suite de nombre, on associe à cette suite la série génératrice ordinaire (SGO) suivante :*

$$g(x)=\sum_{n=0}^{\infty}u_n x^n, \tag{2.10}$$

la fonction définie par cette série est appelée fonction génératrice ordinaire associée à $(u_n)_{n\geq 0}$

Théorème 2.2 *Soient* $g(x)$ *une fonction génératrice de la suite* (a_n), *et* $h(x)$ *une fonction génératrice de la suit* (b_n) *donc :*

1. $g(x)h(x)$ *: fonction génératrice de la suite* $(b_0a_n+b_1a_{n-1}+...+a_1b_{n-1}+b_na_0)$.
2. $c_1g(x)+c_2h(x)$ *: fonction génératrice de la suite* $(c_1a_n+c_2b_n)$.
3. $g(x)(1-x)$ *: fonction génératrice de* (a_n-a_{n-1}).

4. $xg\prime(x)$ *: fonction génératrice de la suite* (na_n) *.*

5. $g(x)/(1-x\ )$ *: fonction génératrice de la suite* $(a_0+a_1+...+a_n)$*.*

2.7.1 Fonctions génératrices associées à la suite Fibonacci

Considérons la suite de Fibonacci définie par :

$$\begin{cases} F_0 = F_1 = 1 \\ F_n = F_{n-1} + F_{n-2},\ n \geq 2. \end{cases}$$

Posons

$$g(x) = \sum_{i=0}^{\infty} F_n x^n,$$

$$\begin{aligned} g(x) &= F_0 + F_1 x + \sum_{i=2}^{\infty} (F_{n-1} + F_{n-2})\, x^n \\ &= 1 + x + x\left(\sum_{i=0}^{\infty} F_n x^n - F_0\right) + x^2 \sum_{i=2}^{\infty} F_{n-2} x^{n-2} \\ &= 1 + xg(x) + x^2 g(x). \end{aligned}$$

Donc :

$$g(x) = \frac{1}{1-x-x^2}.$$

2.7.2 Fonctions génératrices associées aux polynômes de Chebyshev

1) Considérons la relation de récurrence de polynôme de Chebyshev de 1$^{\text{er}}$espèce définie par :

$$\begin{cases} T_0(x) = 1 \\ T_1(x) = x \\ T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x), n \geq 2 \end{cases}.$$

Posons

$$g(z) = \sum_{n=0}^{\infty} T_n z^n,$$

$$\begin{aligned} g(z) &= T_0 + T_1 z + \sum_{n=2}^{\infty} \left(2xT_{n-1} - T_{n-2}\right) z^n \\ &= 1 + xz + 2xz\left(\sum_{n=0}^{\infty} T_n z^n - T_0\right) - z^2 \sum_{n=2}^{\infty} T_{n-2} z^{n-2} \\ &= 1 - xz + 2xzg(z) - z^2 g(z). \end{aligned}$$

Donc :

$$g(z) = \frac{1 - xz}{1 - 2xz + z^2}.$$

2) Considérons la relation de récurrence de polynôme de Chebyshev de 2$^{\text{ème}}$espèce définie par :

$$\begin{cases} U_0(x) = 1 \\ U_1(x) = 2x \\ U_n(x) = 2xU_{n-1}(x) - U_{n-2}(x), n \geq 2 \end{cases}.$$

Soit

$$g(z) = \sum_{n=0}^{\infty} U_n z^n,$$

$$\begin{aligned} g(z) &= U_0 + U_1 z + \sum_{n=2}^{\infty} \left(2xU_{n-1} - U_{n-2}\right) z^n \\ &= 1 + 2xz + 2xz\left(\sum_{n=0}^{\infty} U_n z^n - U_0\right) - z^2 \sum_{n=2}^{\infty} U_{n-2} z^{n-2} \\ &= 1 + 2xzg(z) - z^2 g(z). \end{aligned}$$

On obtient :

$$g(z) = \frac{1}{1 - 2xz + z^2}.$$

2.8 Conclusion

Ce chapitre avait comme objectif d'introduire quelques notions élémentaires des systèmes dynamiques chaotiques et des fonctions génératrices. Dans la section 2.2, Nous avons abordé les systèmes dynamiques non-linéaires en temps continu et discret, tout en mettant en avant le cas de systèmes chaotiques. Ensuite nous avons présenté quelques définitions et propriétés des systèmes chaotiques tels que : la non-linéarité, le déterministe, la sensibilité aux conditions initiales. Plus loin nous avons rappelé quelques définitions sur les relations des récurrences, les polynômes orthogonaux et les fonctions génératrices ordinaires.

Chapitre 3

Etat de l'art sur les systèmes de cryptage chaotiques des images numériques

---

3.1 Introduction

Dans le domaine des télécommunications, où les échanges d'informations multimédias se développent rapidement, il est indispensable de pouvoir disposer de systèmes sécurisés pour protéger les données à caractère personnel ou confidentiel, ainsi que de s'assurer de la sécurité de transferts de données.

La cryptographie chaotique décrit l'utilisation de la théorie du chaos pour effectuer différentes tâches cryptographiques dans un système cryptographique.

Ce chapitre est consacré à un état de l'art sur le thème du cryptage des images à base du chaos. Pour cela, une vue d'ensemble de l'impact potentiel du cryptage sur les applications en science et technologie, ainsi que les progrès récents des méthodes de cryptage des images à base du chaos y seront présentées. Les développements proposés dans ce chapitre permettront de comprendre entre autres la diversité des cartes chaotiques. Ces dernières se caractérisent par leur sensibilité aux conditions initiales, et en plus d'un aspect aléatoire...

3.2 Structure générale d'un schéma de cryptage des images à base du chaos

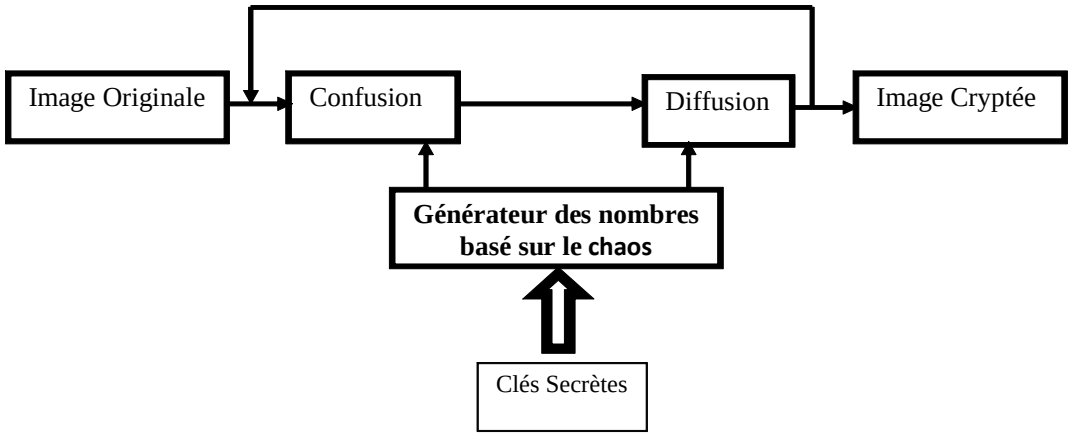


Figure 3.1. Structure générale d'un schéma de cryptage d'image à base du chaos.

D'après la figure 3.1 qui illustre la structure générale d'un schéma de cryptage d'image à base du chaos, un schéma de cryptage des images se base sur deux principes la confusion et la diffusion (Shanon 49). La confusion est simplement un réarrangement des pixels de l'image, ce qui permet de diminuer la redondance en répartissant les pixels sur toute l'image cryptée. Alors que, la diffusion permet de modifier la valeur de chaque pixel.

Avant de présenter quelques travaux portant sur ce domaine scientifique, nous proposons tout d'abord, de clarifier le lien qui existe entre le chaos et la cryptographie (présentés dans les chapitres précédents).

3.3 Liaison entre la cryptographie et le chaos

Depuis les années 90, plusieurs chercheurs ont noté qu'il existe un rapport intéressant entre le chaos et la cryptographie. En effet, plusieurs propriétés des systèmes chaotiques présentent des correspondances similaires ou presque, avec des systèmes cryptographiques traditionnels.

En se référant aux propriétés des systèmes chaotiques discutées dans le chapitre précédent, il est clair d'une part que les propriétés d'ergodicité, d'auto similitude, de mélange topologique sont directement liées à la confusion. La dynamique dans l'attracteur chaotique est donnée par des orbites apériodiques qui génèrent des modèles statistiques similaires. Ces modèles peuvent être utilisés pour masquer des messages clairs au moyen de techniques de type substitution.

D'autre part, la diffusion est étroitement liée à la sensibilité que les systèmes chaotiques présentent aux conditions initiales et aux paramètres de contrôle. La diffusion produit l'effet d'avalanche où une différence minimale dans l'entrée du cryptosystème donne une sortie complètement différente. Un système chaotique produit ce comportement lorsqu'un petit changement est appliqué à ses conditions initiales ou à ses paramètres de contrôle. L'utilisation de ces variables comme entrée dans l'algorithme du cryptosystème peut produire le même effet d'avalanche.

Propriété du chaos	**Propriété de la cryptographie**	**Description**
Ergodicité	Confusion	Le rendement a la même distribution pour n'importe quelle entrée (chaque trajectoire tend à une distribution invariable qui est indépendante des conditions initiales)
Sensibilité aux conditions initiales et aux paramètres du système	Diffusion avec un petit changement du texte/de la clés secrète	Une petite déviation en entrée peut causer un grand changement au rendement
Dynamique déterministe	Aspect déterministe pseudo-aléatoire	Un processus déterministe peut causer un comportement pseudo-aléatoire
Complexité de structure	Complexité d'algorithme	Un processus simple d'une complexité très élevée

Tableau 3.1. Résumé des liens entre le chaos et la cryptographie [18].

À l'heure actuelle, l'histoire de la cryptographie basée sur le chaos remonte à plus de deux décennies. D'abord, certains travaux apparaissent dans les années 80 (Wolfram, 1985 ; Guan, 1987), mais c'est dans les années 90 que la cryptographie chaotique prend son envol. Deux articles marquent ce début [19] et (Pecora, 1989). Le premier propose un chiffrement de flux numérique où un signal généré à partir d'un système chaotique est utilisé pour masquer le message clair. Le deuxième propose une synchronisation par chaos pour masquer le message clair par un signal chaotique au niveau physique du canal de communication et pour utiliser des techniques de synchronisation au niveau du récepteur pour filtrer le signal chaotique.

Depuis lors, un grand nombre de méthodes de cryptage basées sur le chaos ont été proposées. Il existe deux principales idées de conception récentes en vue des schémas de chiffrement basés sur un système chaotique, l'une consiste à améliorer la sécurité du flux de clés en utilisant de nouveaux types de systèmes chaotiques, l'autre idée est de concevoir des algorithmes plus complexes par de nouvelles technologies, comme la permutation au niveau du bit, l'encodage

ADN, compressive (compression) sensing, les automates cellulaires.

3.4 Etat de l'art sur les systèmes de cryptage des images à base du Chaos

Dans cette section, nous présentons un aperçu sur certains systèmes de cryptage des images à base du Chaos. Il faut signaler que plusieurs classifications sont proposées selon l'objectif ciblé.

Dans [21], et dans son introduction, une classification des techniques de cryptage d'image existantes en trois classes est proposées : celles qui se basent sur la permutation de position de pixel, celles qui sont fondées sur la transformation des valeurs de pixels et la dernière classe contient des techniques hybrides.

Dans [22], les auteurs présentent une revue des techniques de cryptage d'image basées sur des systèmes chaotiques, en essayant de les regrouper dans trois catégories selon leurs domaines : spatial, fréquentiel et hybride.

Selon les auteurs dans [23], les algorithmes de cryptage d'images basés sur le chaos peuvent être classés en quatre grandes catégories : (1) algorithmes de faible dimension (2) multidimensionnels (3) hyper-chaotiques et (4) algorithmes chaotiques composés.

Comme notre travail porte sur la définition d'une nouvelle fonction chaotique, qui a comme objectif principal de générer des séquences aléatoires. Ces dernières servent à définir la valeur de la clé secrète. Nous présentons dans cette section un état de l'art des travaux selon trois classes. La première, qualifiée de la sécurité en termes de flux de clés ; elle est basée sur la présentation de quelques travaux qui s'intéressent à la définition des nouvelles fonctions chaotiques. La seconde porte sur la structure complexe des systèmes de cryptage chaotique ; elle est nommée structure complexe de l'algorithme de cryptage. La dernière classe présente quelques travaux qui exploitent la notion de parallélisme, implémentation physique des générateurs, matrice de tri fractale, etc.

3.4.1 Travaux qualifiés de la sécurité en termes de flux de clés

Avant de présenter quelques travaux de cette classe, il est nécessaire de définir le chaos dans les systèmes dynamiques.

3.4.1.1 Définition du chaos dans les systèmes dynamiques

Ces dernières années, la recherche sur la bifurcation et le comportement chaotique dans les systèmes dynamiques non linéaires est devenue très importante. La bifurcation et le chaos ont été identifiés dans un grand nombre d'expériences, et plusieurs auteurs ont avancé l'idée que les simulations informatiques jouent un rôle important dans la recherche de nouveaux attracteurs chaotiques [24, 25]. Le chaos est généralement caractérisé par la dépendance sensible aux conditions initiales de la dynamique. Il existe de nombreuses méthodes pour identifier et quantifier le chaos dans la dynamique. Il peut être identifié en recherchant le dédoublement de période ou en observant le comportement des séries temporelles et il peut être quantifié en calculant les exposants de Lyapunov [26]. En particulier, une cascade typique de doublement de période vers le chaos a été étudiée dans des cartes discrètes telles que la carte logistique, la carte de cat, la carte de tente, la carte de Henon, etc. La cascade de doublement de période vers le chaos a également été explorée dans certaines séquences bien connues et polynômes. Dans [27], les auteurs ont montré que le rapport des nombres de Fibonacci successifs converge vers la moyenne d'or à chaque période de doublement, et donc la convergence vers le nombre le plus irrationnel se produit de concert avec l'apparition du chaos déterministe. Dans [28, 29, 30], les auteurs ont développé plusieurs types de cartes chaotiques. La dynamique réelle de certaines cartes logistiques généralisées a été étudiée en détail dans [31]. La bifurcation des fonctions génératrices de Fibonacci associées à la moyenne d'or a été étudiée dans [32]. De la même manière, la bifurcation et le comportement chaotique dans la dynamique des familles unidimensionnelles des applications correspondant aux fonctions génératrices de Fibonacci associées aux moyens argent et bronze ont été abordés dans [33]. Dans [34, 35], les auteurs ont analysé la bifurcation et le chaos dans la dynamique réelle des familles à un paramètre des fonctions transcendantales. La dynamique réelle de la famille de fonctions à un paramètre $\frac{bx-1}{x}$ a été explorée dans [36].

De nombreux travaux ont été réalisés dans l'étude de la bifurcation et du chaos dans certaines fonctions génératrices bien connues ; cependant, la bifurcation et le comportement chaotique des fonctions génératrices associées aux polynômes de Chebyshev n'ont pas été étudiés en profondeur. En fait, il existe de nombreuses familles distinctes de polynômes connus sous le nom de polynômes de Chebyshev qui peuvent être appliqués dans la théorie de l'approximation, les règles

de quadrature, etc. [37, 38, 39]. La représentation complexe de ces polynômes permet la dérivation de nombreuses identités impliquant des fonctions génératrices spéciales de type exponentiel, bilinéaire et mixte [40, 41].

Il convient de noter que la plupart des fonctions chaotiques développées ont été appliquées pour générer des générateurs de bruit pseudo-aléatoire (PRNG). En conséquence, des cartes de chaos ont été mises en œuvre à l'aide d'électronique numérique et analogique. Les implémentations numériques consistent à approximer la réponse chaotique d'un système en résolvant des équations différentielles ordinaires. La mise en œuvre numérique en temps réel a été réalisée sur des réseaux prédiffusés programmables sur le terrain (FPGA) via un langage de description de matériel (HDL), généralement VHDL [41] ou Verilog-A [42]. La réalisation matérielle utilise différentes approches pour implémenter des générateurs de chaos. Dans ce contexte, Fraga et al. [43] ont montré l'avantage des diagrammes de bifurcation pour implémenter un PRNG basé sur quatre cartes chaotiques, à savoir la carte de décalage de Bernoulli, les cartes de tente, de zigzag et de Borujeni. Les séquences binaires générées à partir de ces cartes sont implémentées dans un logiciel utilisant des architectures de microprocesseur 32 et 64 bits et avec une arithmétique de calcul à virgule flottante et à virgule fixe. L'implémentation matérielle a également été réalisée à l'aide d'une architecture FPGA. Le caractère aléatoire des séquences binaires générées a été validé avec la suite de tests NIST 800-22-a en arithmétique à virgule flottante et à virgule fixe. Senouci et al. [44] a introduit une méthode de modélisation rapide, indépendante de l'appareil et largement accessible pour étudier, simuler et exécuter le PRNG chaotique dans un environnement unique. La méthode est basée sur MATLAB HDL Coder et la boîte à outils Fixed Point pour obtenir une description synthétisable des modèles chaotiques créés dans le framework Simulink. Le prototypage rapide a été validé à l'aide de la carte d'évaluation ML507. L'implémentation matérielle a également été étudiée à l'aide d'une architecture FPGA avec différents systèmes chaotiques bien connus tels que les générateurs chaotiques Lorenz, Rossler, Chua, Chen, Linz-Sprott et Sprott de type B, E et H. Par ailleurs, la mise en œuvre analogique consiste à convertir l'ensemble des équations différentielles ordinaires représentant le générateur chaotique en une description de circuit électronique. Valtierra et al. [45] ont fourni un véritable schéma de générateur de nombres aléatoires (TRNG) basé sur un oscillateur chaotique à carte oblique

et sur le principe du circuit à condensateur commuté. Ce schéma proposé appliquait un bloc de post-traitement simple de sorte que le circuit à condensateur commuté à carte oblique présente une plus grande linéarité, un effet pseudo-parasite inférieur et une interface plus simple car il ne nécessite pas de transformation tension-courant-tension par rapport au circuit d'homologues à courant commuté.

3.4.1.2 Système chaotiques de cryptage des images à base des systèmes 1D

De nombreux travaux de cryptages chaotiques des images existent dans la littérature. Les auteurs de [116] ont proposé une nouvelle carte chaotique $1D$ simple. Les caractéristiques chaotiques ont été montrées en utilisant l'analyse de bifurcation et l'analyse des exposants de Lyapunov. De plus, un nouvel algorithme de cryptage d'image basé sur cette nouvelle carte chaotique est proposé. Les deux étapes de confusion et de diffusion sont liées à cette nouvelle carte.

De nombreux tests statistiques et analyses de sécurité indiquent que cet algorithme a d'excellentes performances de sécurité et peut être compétitif avec certains autres algorithmes de chiffrement d'images récemment proposés. Cette nouvelle fonction a été exploitée par Prasetyo dans son algorithme de cryptage [46].

Liu & Miao [116] introduisent un nouveau système chaotique polynomial unidimensionnel de cosinus (1-DCP). Ce système constitue la base de leur schéma de chiffrement d'image. Contrairement à la plupart des schémas de chiffrement existants, ils combinent les étapes de confusion et de diffusion pour augmenter considérablement la vitesse de chiffrement en réduisant le nombre de boucles sur les pixels. Le processus de chiffrement d'une image en clair P est divisé en deux modules : une phase ligne suivie d'une phase colonne.

- **Phase ligne :** les valeurs de chaque ligne Pi et une autre ligne PEP (i) définie par une clé EP sont masquées en utilisant les valeurs de la ligne prédécesseur, une séquence de nombres pseudo-aléatoires générée à partir de la carte chaotique 1-DCP, et l'opérateur modulo. Enfin, l'opération shift est appliquée.
- **Phase colonne :** les mêmes étapes décrites ci-dessus sont appliquées, pour chaque colonne de la matrice transposée associées à la matrice résultant de la phase précédente.

Dans [116], trois systèmes chaotiques $1D$ améliorés, à savoir le système Logistic-Tent (LTS),

le système Logistic-Sine (LSS) et le système Tent-Sine, ont été plus récemment suggérés dans la littérature scientifique afin de corriger les inconvénients des cartes chaotiques d'entrée en améliorant ses performances en termes de plage chaotique, de structure des paramètres de contrôle et de sensibilité. Chaque système chaotique est le résultat de calcul de deux cartes chaotiques $1D$ différentes , à savoir la carte logistique, la carte de tente et la carte sinus.

Ces différentes fonctions constituent la base d'un nouvel algorithme de cryptage d'image, qui comprend cinq étapes : l'insertion aléatoire de pixels, la séparation des lignes, la substitution $1D$, la combinaison des lignes et la rotation de l'image.

Dans le même contexte, les auteurs de [47] ont proposé un nouveau schéma de cryptage chaotique pour les images couleur basé sur un nouveau système chaotique. Ce dernier est une combinaison de trois cartes chaotiques $1D$ bien connues : carte sinus, carte logistique et la carte Chebyshev ; les combinaisons sont Sine-Sine map (SSM), Logistic-LogisticMap (LLP) et Chebyshev-Chebyshev Map (CCM). Les auteurs montrent que leur système est un système chaotique efficace avec de meilleures performances chaotiques et une plus grande plage chaotique $[0, 4]$. Les résultats des expériences ont également montré que le schéma de cryptage proposé a d'excellentes performances en cryptage d'image.

Hua et al. [48] proposent la carte logistique-sinusmap, la carte gaussienne-logistique et la carte gaussienne-sinusmap. Ils ont prouvé que ces nouvelles cartes chaotiques ont une meilleure performance de chaos que leurs cartes classiques correspondantes. Wang et al. [49] ont proposé une carte Logistique-Logistique, une carte Logistique-Cubique, une carte Logistique-Tente, et les résultats montrent que leurs plages des valeurs chaotiques sont considérablement élargis.

3.4.1.3 Systèmes chaotiques de cryptage des images à base des systèmes multidimensionnels

Les systèmes chaotique $1D$ ont généralement une structure simple et ne contient qu'une seule variable et relativement peu de paramètres système, de sorte que les orbites chaotiques, les conditions initiales et les paramètres système sont facilement estimés [50]. En revanche, avec plus de variables et plus de paramètres, une carte chaotique multidimensionnelle a un espace clé plus grand et une structure relativement compliquée. Les orbites sont assez difficiles à estimer et ses

paramètres sont beaucoup plus difficiles à prédire, c'est pourquoi plusieurs travaux s'orientent vers ce type de systèmes chaotiques

Chen al utilise la carte de cat $3D$ [51] et une carte de boulanger $3D$ [52] dans l'étape de confusion. Guan et al. ont utilisé une carte de cat $2D$ pour l'étape de confusion et le système chaotique discrétisé de Chen pour l'étape de diffusion [53]. Lian et al. [54] utilisent une carte standard $2D$ dans l'étape de confusion et une carte logistique quantifiée dans l'étape de diffusion. Les paramètres et la condition initiale de ces deux cartes chaotiques sont déterminés par un flux de clés généré à chaque tour.

Le schéma proposé par K.S. Sankaran et B.S. Krishna [55] se base sue l'un des trois systèmes chaotiques $3D$: le système de Lorenz, le système de Chen et le système de Lu dans chaque étape de processus de cryptage. Pour l'étape de confusion, la permutation de la position des pixels est effectuée à l'aide de l'un quelconque des systèmes chaotiques $3D$ précédents. Ceci est suivi par l'étape de diffusion dans laquelle la diffusion de valeur de pixel est effectuée à nouveau avec l'un quelconque des systèmes chaotiques. Le choix d'un système chaotique est effectué par une clé séparée externe afin d'améliorer la sécurité de l'algorithme. Ce même principe du choix entre un ensemble des fonctions chaotiques est utilisé dans [56]. Les systèmes utilisés dans les phases de processus de cryptage sont le système de Lorenz est celui du Baker.

3.4.1.4 Systèmes chaotiques de cryptage des images à base des systèmes Hyper-chaotiques

Les systèmes hyper-chaotiques ont deux exposants de Lyapunov positifs ou plus, et leur comportement dynamique est plus complexe. Par conséquent, les systèmes hyper-chaotiques peuvent générer des séquences chaotiques plus aléatoires, donc et un système de cryptage à base d'un système hyperchaotique présente une sécurité plus. Dans la littérature plusieurs travaux existent, citons à titre d'exemple le travail de Peng et al. [57] qui ont proposé un algorithme de cryptage d'image basé sur un nouvel attracteur hyperchaotique $4D$. Le système a deux exposants de Lyapunov supérieurs à zéro, qui peuvent générer des attracteurs hyperchaotiques sous différents paramètres. Dans [58], les auteurs proposent une nouvelle carte hyperchaotique dérivée des équations paramétriques de la courbe serpentine. Cette nouvelle carte est utilisée pour générer

des séquences aléatoires dans l'étape de confusion et l'étape de diffusion. Les résultats obtenus montrent que le schéma de cryptage d'image proposé fournit un moyen efficace et sécurisé pour le cryptage d'image.

Dans [59] et dans [60] de nouveaux schémas de cryptage d'image basés sur des séquences hyperchaotiques améliorés ont été proposés, où une séquence de nombres pseudo-aléatoires générée par une carte hyperchaotique $4D$ a été utilisée pour modifier les valeurs des pixels avec un schéma XOR.

3.4.2 Travaux portant sur une structure complexe de l'algorithme de cryptage

3.4.2.1 Systèmes chaotiques de cryptage des images en niveau de bit

En raison des avantages des permutations au niveau du bit, qui peuvent modifier simultanément la position et la valeur d'un pixel, plusieurs chercheurs ont introduit des schémas de cryptage au niveau du bit [61, 62, 63]. Généralement, la permutation au niveau des bits peut surmonter les inconvénients du brouillage typique au niveau des pixels, et elle est plus efficace pour le cryptage des images.

Wang et al. [61] ont proposé un schéma de chiffrement au niveau du bit en utilisant un modèle perceptron. Dans [62], les auteurs présentent un nouvel algorithme de cryptage d'images au niveau du bit basé sur des cartes chaotiques (PWLCM). Tout d'abord, l'image simple est transformée en deux séquences binaires de même taille. Ensuite, une nouvelle stratégie de diffusion est introduite pour diffuser mutuellement les deux séquences. Ensuite, nous échangeons les éléments binaires dans les deux séquences par le contrôle d'une carte chaotique, ce qui peut permuter les bits d'un bitplane dans n'importe quel autre bitplane. Les résultats de la simulation et l'analyse des performances montrent que l'algorithme proposé est à la fois sûr et fiable pour le chiffrement d'images avec un seul tour. Récemment, des algorithmes de cryptage d'image basés sur la permutation des plans de bits ont été proposés, où l'image originale est décomposée en huit images binaires, puis combinée en une grande image binaire [64, 65, 66]. La position de la grande image binaire est confondue par la séquence chaotique, puis l'image binaire est réassemblée pour obtenir

l'image chiffrée. Dans [67], un algorithme de cryptage d'image avec générateur de séquences de bits aléatoires a été proposés, l'image est partitionnée en huit plans de bits, puis les bits sont permutés et substitués selon une séquence chaotique. Enfin, les plans de bits embrouillés sont combinés en images chiffrées. Dans le but d'optimiser le système de cryptage, les auteurs dans [68, 69] ont proposé de diviser les bits de l'images en des plans de bits supérieurs et des plans de bits inférieurs, puis différents plans de bits sont attribués avec différentes méthodes de cryptage.

3.4.2.2 Cryptage à base de combinaison de systèmes chaotiques et de codage ADN

L'utilisation de la technologie de codage ADN pour coder les images n'est pas suffisamment sécurisée et peut être combinée avec d'autres technologies [70].

Avant de présenter quelques travaux basés sur le codage de l'ADN et les systèmes chaotiques, nous proposons quelques bases du codage de l'ADN et montrons comment il peut être utilisé pour coder une séquence de bits.

Il existe quatre acides nucléiques différents dans une séquence d'ADN qui sont nommés A (adénine), T (thymine), C (cytosine) et G (guanine). Les règles d'appariement des bases sont, (A) s'apparie toujours avec (T) et (C) s'apparie toujours avec (G). On peut conclure que (A) et (T) sont complémentaires, (G) et (C) sont également complémentaires. Ces relations sont souvent appelées les règles de l'appariement de bases Watson-Crick.

De même, dans le système binaire, $(0, 1)$ sont complémentaires, ce qui signifie que $(00, 11)$ et $(10, 01)$ sont également complémentaires. Donc, si nous utilisons les quatre désoxynucléotides "A","T","G" et "C" pour représenter les nombres binaires"00", "11", "01" et "10", respectivement, alors chaque pixel peut être codé dans une chaîne de nucléotides, par exemple, $(11000101)_2$ est le format binaire qui pourrait être codé en utilisant la règle 3 comme (ATGG).

Il existe 24 types de combinaisons pour les quatre nucléotides. Cependant, seules huit combinaisons de codage sont adaptées au principe de complémentarité. Ces règles sont résumées dans le tableau 3.2.

	A	**T**	**C**	**G**
régle1	00	11	10	01
régle2	00	11	01	10
régle3	11	00	10	01
régle4	11	00	01	10
régle5	10	01	00	11
régle6	01	10	00	11
régle7	10	01	11	00
régle8	01	10	11	00

Tableau 3.2 Règles de carte d'encodage et de décodage de la séquence d'ADN**[70].**

Liu et al.[71], ont proposé un nouvel algorithme de cryptage qui combine le codage de l'ADN et les cartes chaotiques. Ils ont utilisé le schéma de codage de l'ADN pour coder chaque pixel de l'image originale en quatre nucléotides et ont appliqué la règle complémentaire pour transformer chaque nucléotide en leur paire de bases à différents moments générés par la carte chaotique de Chebyshev.

Un schéma d'imagerie médicale proposé par Akrambelazi et al [72] utilise une permutation basée sur des blocs et une substitution basée sur les valeurs des pixels. Le schéma aboutit à une image cryptée forte en raison de cette confusion et de cette diffusion. Les mérites distincts incluent la substitution en cascade basée sur les pixels et la substitution au niveau des bits.

Huilui, et al. proposent dans [73] un schéma de cryptage basé sur la cryptographie ADN et la carte logistique bidimensionnelle ($2D$). Le système fonctionne selon le principe de l'ADN et de la sécurité des nombres pseudo-aléatoires. Les nombres pseudo-aléatoires (PRN) sont générés par la carte logistique $2D$ qui possède de bonnes caractéristiques. L'algorithme de cryptage d'image utilise le codage de l'ADN, deux cycles pour la génération de PRN, l'ajout d'ADN, le calcul de probabilité des bases d'ADN, les réarrangements au niveau des pixels et des bases d'ADN et le décodage de l'ADN. Il fournit une distribution assez uniforme, une entropie d'information élevée et une réduction du coefficient de corrélation élevé. Ce système se caractérise par sa haute sécurité, sa vitesse d'exécution du processus de cryptage et le fonctionnement en parallèle [73].

Les auteurs dans [74] ont proposé de convertir l'image simple en une matrice d'ADN, et la carte chaotique est utilisée pour générer une matrice clé qui est utilisée pour fusionner la matrice d'ADN confuse. Puis les valeurs initiales et les paramètres du système chaotique sont mis à jour par la distance de Hamming de l'image simple. Enfin la matrice d'ADN diffusée est décodée, afin d'obtenir l'image chiffrée.

D'autres travaux récents existent, à titre d'exemple, le travail dans [75] qui propose un système de cryptage, basé sur l'ADN et la carte logistique. Le travail de Xing, et al. [76] qui présente un système de cryptage qui se base sur le principe d'ADN et la carte coupled map latice. Taiyong, et al. [77] intègre dans son système de cryptage le calcul ADN, le filtrage et les cubes latins.

3.4.2.3 Cryptage à base de combinaison de systèmes chaotiques et les automates cellulaires

Martin del Rey et al.[78] ont présenté un nouvel algorithme de chiffrement des images numériques. La proposition est basée sur la carte cat map les automates cellulaires réversibles (RCA) unidimensionnels ($1D$). Dans l'étape de la confusion, les pixels de l'image simple sont permutés à l'aide des valeurs générée par la carte cat map qui présente de bonnes caractéristiques cryptographiques. A l'étape de diffusion, les valeurs du pixel de l'image confuse (permutée/ mélangée) sont modifiées séquentiellement à l'aide de RCA, qui vise à diffuser l'effet d'un pixel sur les autres pixels de l'image. Enfin l'image chiffrée est le résultat final de ce processus.

Les mêmes auteurs proposent une extension de ce travail dans [79] dans laquelle la phase de confusion reste la même alors que dans la phase de diffusion les RACs sont remplacées par les automates cellulaires à mémoire réversible (MRAC) bidimensionnels (2D), avec le voisinage de Moore. D'après les résultats de sécurité donnés, les deux travaux [78, 79] présentent un niveau de sécurité acceptable. Alors que le temps d'exécution de [79] est vraiment lent, et cela dû nombre de fois élevé d'exécution de l'étape de diffusion pour obtenir l'mage chiffrée.

Wang et al. [80] dans leur article proposent de combiner les automates cellulaires de la fourmi de Langton et du chaos. Tout d'abord, l'image originale est convertie en un tableau 1D de pixels, puis, la fourmi cellulaire de Langton est adoptée pour brouiller ces pixels, sous le contrôle des séquences chaotiques générées à l'aide d'une carte logistique entrelacée pour la phase de confusion.

Dans la phase de diffusion, chaque pixel confus est diffusé en adoptant un mode séquentiel, sous le contrôle des séquences chaotiques générées par la PWLCM. Le résultat est l'image cryptée.

La proposition de [81] est basée sur la combinaison du chaos et des automates cellulaires (CA) dans les scénarios d'une architecture de chiffrement/déchiffrement et de permutation-diffusion. Tous les flux de clés générés dans les cryptosystèmes proposés sont basés sur l'utilisation d'un système chaotique unidimensionnel ($1D$) amélioré [c'est-à-dire un système logistique-tente] avec d'excellentes propriétés chaotiques.

Ces flux de clés sont liés à la fois à la clé secrète et aux caractéristiques de l'image simple. Avant d'appliquer le processus de cryptage, un pixel de l'image simple à une position aléatoire est écrasé en insérant la valeur d'histogramme pondérée comme nouvelle mesure pour représenter le les fonctionnalités de l'image simple. Ce pixel retient la routine de cryptage et sera en outre utilisé pour garantir la résistance aux attaques d'image simple connues/choisies (CPA sécurisé). Dans la phase de confusion, une permutation au niveau du bit est adoptée avec les flux de clés uniques générés en utilisant un système chaotique LTS proposé dans [**?**]. La phase de diffusion est divisée en deux sous-phases : dans la première, la valeur de chaque pixel est modifiée séquentiellement au moyen du système LTS. Pour la deuxième sous-phase, des automates cellulaires à mémoire réversible $2D$ sont associés à la stratégie de décomposition quad tree et appliqués à la sortie de la première sous-phase, pour améliorer la sécurité.

Dans le même contexte, [82] propose un schéma de cryptage basé sur le chaos et les automates cellulaires like_life, la permutation et la substitution. Dans la permutation, la carte 2D-LASM (two-dimensional Logistic adjusted-Sine map) pour changer les positions des pixels. Dans la diffusion, un AC réaliste de second ordre avec une règle équilibrée est utilisé. Les résultats expérimentaux montrent que le schéma proposé a des performances cryptographiques importantes et peut résister efficacement aux attaques courantes, ce qui est très approprié pour le cryptage d'images.

3.4.3 Autres systèmes chaotiques de cryptage des images

Garcia-Guerrero et al. [83] ont développé un cryptosystème compatible avec les nouveaux protocoles de télécommunication via les canaux Zigbee. Ce cryptosystème a introduit un processus

pour améliorer le caractère aléatoire de cinq cartes chaotiques implémentées sur un microcontrôleur PIC avec une consommation d'énergie efficace. Tlelo-Cuautle et al. [84] ont implémenté un schéma de cryptage d'image chaotique sur FPGA pour les images couleur en utilisant les neurones de Hopfield et Hindmarsh-Rose. La principale contribution s'est concentrée sur l'obtention de valeurs de paramètres appropriées pour les neurones afin de générer des séquences binaires aléatoires robustes à appliquer dans le codage d'images. La performance de ce schéma proposé a été confirmée en présentant les résultats des tests de corrélation, d'histogramme, de variance, d'entropie et du taux de changement du nombre de pixels (NPCR).

Les progrès récents du cryptage continuent de promouvoir l'application en temps réel des communications informatisées. Wang et al. [85] ont proposé un algorithme de cryptage d'image rapide basé sur un système de calcul parallèle pour garantir le parallélisme de diffusion au plus haut degré et atteindre une amélioration qualitative de l'efficacité par rapport aux méthodes de diffusion conventionnelles. Wang et Gao [86, 87] ont récemment conçu des algorithmes intuitifs de chiffrement d'images chaotiques basés sur la théorie du produit matriciel semi-tenseur où la clé secrète est générée dans un réseau booléen. La structure complexe d'un tel réseau rend sa cryptanalyse difficile. D'autres améliorations sur ce problème ont été apportées récemment par Wang et Yang [88] en utilisant la matrice de tri fractal, et par Xian et Wang [89] en utilisant le chaos spatio-temporel. Ces méthodes proposées ont montré la capacité de résister à différentes formes d'attaques statistiques, et que les attaques de bruit ont été améliorées dans une certaine mesure.

Basé sur l'idéologie des fonctions génératrices, nous proposons un nouvel ensemble de fonctions génératrices aux propriétés chaotiques liées aux polynômes de Chebyshev de seconde espèce [2]. Le comportement chaotique est observé en analysant le diagramme de bifurcation et en quantifiant l'exposant de Lyapunov de la nouvelle classe de fonction génératrice proposée par Boussayoud et al. [90, 91, 92] pour différentes valeurs des paramètres système. Les fonctions génératrices chaotiques proposées ont montré une distribution de type aléatoire et peuvent présenter une cascade typique de doublement de période vers le chaos. Plus important encore, ces fonctions génératrices peuvent être générées de manière itérative, ce qui a amélioré l'efficacité temporelle du processus informatique innovant. L'application de la fonction de génération basée sur le chaos

développée au cryptage d'image peut améliorer l'efficacité et la sécurité de l'algorithme de cryptage proposé par Himeur et Boukabou [93]. Les simulations et l'analyse de sécurité ont montré que la fonction génératrice proposée des polynômes de Chebyshev généralisés avec un comportement chaotique offre d'excellentes performances et pourrait être utilisée comme PRNG dans de nombreuses applications d'ingénierie basées sur le chaos. En fait, ces fonctions de génération proposées peuvent être bien employées dans le processus de brouillage pour obtenir des résultats de brouillage plus efficaces et plus rapides que les méthodes de balayage traditionnelles. Les résultats de la simulation ont montré que la corrélation des images était considérablement réduite et que la capacité à résister aux attaques statistiques et sonores était grandement améliorée. En outre, une comparaison a été effectuée avec les normes de cryptage avancées en fournissant les résultats des tests statistiques NIST, les histogrammes, l'entropie, la corrélation des pixels adjacents, les attaques différentielles et en utilisant des images numériques de différentes tailles.

3.5 Analyse de la sécurité et des performances

3.5.1 Analyse de la clé

3.5.1.1 Analyse de l'espace clé

L'espace clé désigne le nombre total de clés possibles qu'un attaquant doit essayer de casser, ce qui oblige que ce nombre doit être suffisamment grand, pour empêcher tous type d'attaque par force brute. Une valeur d'espace de clé supérieur à 2^{100} garantit que l'algorithme de cryptage résiste aux attaques par force brute. Cet espace est calculé par la multiplication de l'espace total de chaque clé individuelle [94], défini par l'équation suivante :

$$S = \prod_{i=1}^{k} Sk_i. \tag{3.1}$$

Où, S est l'espace de clé total et Sk_i est l'espace de l^{ième} clé.

Il convient de noter que l'espace clé de chaque clé individuelle dépend principalement de la précision de la clé. Un nombre en double précision est représenté sur 48 bits (6 octets), ce qui

signifie que l'espace total est de 2^{48}, ce qui est approximativement égal à 10^{14}.

3.5.1.2 Sensibilité des clés

Un schéma de chiffrement efficace est très sensible aux modifications des clés de chiffrement et de déchiffrement. En appliquant une modification mineure à la clé de cryptage, la deuxième image cryptée devrait être assez différente de la première image cryptée. De même, s'il existe une petite différence entre les clés de chiffrement et de déchiffrement, l'image cryptée ne peut pas être décryptée correctement.

Généralement, une métrique nommée Cipher-text Difference Rate (CDR) est utilisée afin d'étudier la sensibilité aux clés secrètes. Le CDR est calculé à l'aide de la formule suivante [17] :

$$CDR = \frac{Diff(y, y_1) + Diff(y, y_2)}{2 * W * H} \times 100\%,$$

$$Diff(A, B) = \sum_{i=0}^{w-1} Diff(A(i,j)B(i,j)).$$

$$Diff(A(i,j)B(i,j)) \begin{cases} 1, \text{ si } A(i,j) \neq B(i,j) \\ 0, \qquad\qquad \text{Sinon} \end{cases}, \tag{3.2}$$

tel que : $y = C(I, K),\ y_1 = C(I, K + \Delta K),\ y_2 = C(I, K - \Delta K)$.

Où,

- C représente la fonction de cryptage, Y est une image cryptée de l'image en clair I utilisant une clé K.

- y_1 et y_2 sont deux images cryptées de la même image I avec un petit changement de clé (respectivement $+\Delta K$ et $-\Delta K$).

- $Diff(A, B)$ est la somme des différents pixels de deux images données A et B.

3.5.2 Analyses statistiques

3.5.2.1 Analyse de l'entropie de l'information

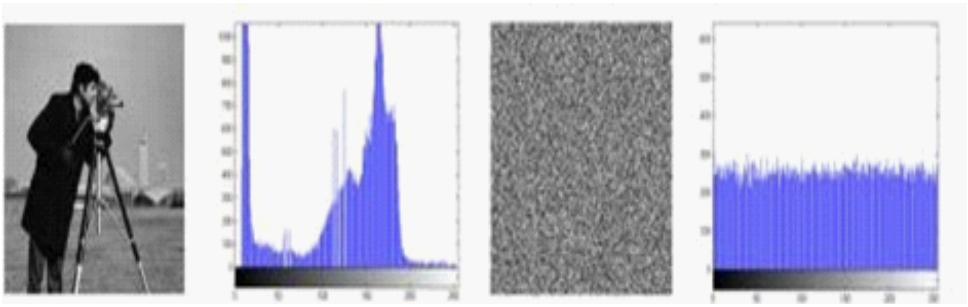
L'entropie d'un système est interprétée comme un indicateur pour mesurer et caractériser la quantité de désordre dans le système. Ce dernier peut mesurer la distribution des valeurs des pixels dans l'image. Une bonne image cryptée a une entropie très proche de 8. En d'autres termes, il représente les informations nécessaires pour définir les états du système. L'entropie est définie comme :

$$H(M) = \sum_{i=1}^{2n-1} p(m_i) \log_2 \left(\frac{1}{p(m_i)} \right), \tag{3.3}$$

où $p(m_i)$ est la probabilité du symbole mi, et N est le nombre de niveaux d'intensité.

3.5.2.2 Analyse d'histogramme (attaque statistique)

Dans un contexte de traitement d'image, l'histogramme d'une image désigne un graphique qui illustre le nombre de pixels associé à chaque valeur d'intensité trouvée dans cette image. Pour une image en niveau de gris, il existe 256 intensités différentes possibles, ainsi, l'histogramme s'affiche graphiquement en utilisant 256 chiffres indiquant la distribution des pixels entre ces valeurs de niveaux de gris [95]. Donc l'analyse d'histogramme est un moyen efficace qui permet de tester l'uniformité des valeurs (invulnérabilité aux attaques statistiques). Ainsi, pour une image cryptée, il est nécessaire qu'une image cryptée ait une répartition uniforme des valeurs de pixels sur les deux axes [95]. Autrement dit un bon chiffrement doit produire des images cryptées ayant un histogramme uniforme autant que possible, voir Figure 3.2.



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

Figure 3. 2. (a) image en clair, (b) histogramme d'image en clair, (c) image cryptée, (d) histogramme d'image cryptée.

3.5.2.3 Analyse de corrélation

Une image en clair présente une forte corrélation entre les pixels adjacents. Un algorithme de chiffrement sécurisé devrait produire des images cryptées dont la corrélation des pixels adjacents est très faible. Habituellement, 1000 ou 2000 pixels sont sélectionnés pour l'analyse de corrélation et la corrélation est calculée dans les directions horizontale, verticale et diagonale à l'aide de la formule suivante :

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}}, \tag{3.4}$$

tel que : $cov(x,y) = \frac{1}{N}\sum_{i=0}^{N}(x_i - E(x))(y_i - E(y)),\ D(x) = \frac{1}{N}\sum_{i=0}^{N}(x_i - E(x))^2,\ E(x) = \frac{1}{N}\sum_{i=0}^{N}x_i.$

Où, x et y représentent les valeurs d'intensité de deux pixels adjacents. N est le nombre de pixels dans l'échantillon d'analyse actuel. $D(x)$ et $E(x)$ représentent la variance et l'espérance de l'échantillon actuel.

La valeur de corrélation se situe dans la plage $[-1,1]$: 0 représente aucune corrélation et 1 représente une corrélation complète (les images sont identiques), généralement, une corrélation supérieur à $0,8$ représente une forte corrélation.

De manière générale, plus les valeurs de corrélation entre les pixels adjacents sont petites,

meilleures sont les performances de l'algorithme de cryptage [96].

3.5.3 Analyse de robustesse

Les images sont inévitablement contaminées par le bruit ou subissent des pertes de données lors du stockage et de la transmission sur les réseaux, en particulier lors de l'utilisation de protocoles peu fiables (tels que UDP).

Les images cryptées doivent avoir la capacité de résister aux attaques qui causent de perte de données, et afin de tester cette capacité, la capacité de restaurer l'image après avoir appliqué différents niveaux de bruit ou de perte de données, la métrique du rapport signal sur bruit (PSNR) est généralement utilisé, cette métrique est calculée par la formule suivante :

$$PSNR = 10 \log \frac{255^2}{MSE} dB \tag{3.5}$$

L'erreur quadratique moyenne (MSE) est utilisée pour analyser l'effet d'avalanche. L'effet d'avalanche indique que le changement de l'image en clair ou de la clé provoque un changement considérable dans l'image cryptée correspondante. La MSE est calculée pour deux images numériques et correspond à l'erreur quadratique cumulée entre elles. Mathématiquement, il peut être calculé comme :

$$MSE = \frac{1}{M * N} \sum_{i=0}^{W-1} \sum_{j=0}^{H-1} Ip(i,j) Id(i,j). \tag{3.6}$$

Où, Ip et Id sont respectivement l'image en clair et l'image décryptée.

Plus la valeur PSNR est élevée, plus la capacité de restauration de l'image décryptée est élevée. En général, il est très difficile de différencier l'image d'origine réelle et l'image décryptée lorsque le PSNR est supérieur à 35 dB.

3.5.4 Résistance aux attaques différentielles

Dans un algorithme de cryptage d'image sécurisé, un seul changement de pixel dans l'image en clair devrait entraîner un changement significatif dans l'image cryptée correspondante.

Lorsqu'une image cryptée est modifiée de manière significative, cela montre que le schéma

proposé est résistant aux attaques différentielles. Pour étudier l'effet du changement d'un pixel sur une image cryptée, les paramètres couramment utilisés sont : (i) le nombre de taux de changement de pixels (NPRC) et (ii) l'intensité de changement moyenne unifiée (UACI) [96]. L'expression mathématique du NCPR est :

$$NCPR = \frac{\sum_{i,j} D(i,j)}{M * N} * 100\%. \tag{3.7}$$

Et l'expression mathématique pour UACI est :

$$UACI = \frac{1}{M * N} \left[\sum_{i,j} \frac{|E1(i,j) - E2(i,j)|}{255} \right] * 100\%. \tag{3.8}$$

Où : M et N représentent la largeur et la hauteur de l'image respectivement. $E1$, $E2$ sont deux images cryptées différentes de la même image en clair.

3.6 Conclusion

Les cartes chaotiques ont été utilisées dans la conception de cryptosystèmes car elles décrivent des caractéristiques souhaitables telles que le pseudo-aléatoire, la complexité et la sensibilité aux changements de paramètres. Bien que ces caractéristiques soient analogues aux exigences cryptographiques, les cryptosystèmes basés sur le chaos qui en résultent sont généralement difficiles à analyser, inefficaces et présentent des problèmes de reproductibilité.

Aujourd'hui, la cryptographie à base du chaos reste un domaine très actif, avec de nombreuses publications scientifiques. Ainsi, le nombre de cryptosystèmes chaotiques qui ont été proposés est trop important pour être couvert dans ce chapitre.

Chapitre 4

Développement d'un système de cryptage à base de la fonction génératrice chaotique proposée

---

4.1 Introduction

Dans ce chapitre nous proposons une fonction génératrice pour les polynômes de Chebyshev avec un doublement de période typique au chaos. En tant qu'application, cette fonction génératrice proposée est utilisée comme un crypto-système basé sur le chaos pour crypter différentes images. L'analyse de sécurité a montré que la fonction génératrice proposée des polynômes de Chebyshev présente d'excellentes performances dans le cryptage d'images contre diverses attaques.

4.2 Fonction génératrice

Il convient en premier lieu de rappeler la définition et quelques propriétés des polynômes de Chebyshev univariés de second espèce.

Définition 4.1 *Les polynômes de Chebyshev de second espèce d'ordre n sont définis comme suit :*

$$U_n(r) = \frac{\sin\left[(n+1)\arccos(r)\right]}{\sqrt{1-r^2}}, \tag{4.1}$$

avec $r \in [0,\ 1],\ n = 0, 1, 2, \ldots$

En changeant d'échelle avec $r = \cos\theta$, Eq. (4.1) peut être réécrit comme

$$U_n(r) = \frac{\sin[(n+1)\theta]}{\sin\theta}.$$

De plus, il peut être représenté en termes de séries hypergéométriques gaussiennes comme suit [109] :

$$U_n(r) = (n+1)\,{}_2F_1\left(\begin{matrix}-n; n+2, & \frac{1-r}{2} \\ & \frac{3}{2}\end{matrix}\right).$$

Les polynômes de Chebyshev de seconde espèce $U_n(r)$ de degré n sont des polynômes orthogonaux, à l'exception d'un facteur constant par rapport à la fonction de poids $W(r) = \sqrt{1-r^2}$. Par ailleurs, les polynômes de Chebyshev de deuxième type satisfont la relation d'orthogonalité

suivante [109] :

$$\int_0^1 \sqrt{r}\sqrt{(1-r)}U_n(r)U_m(r)dr = \begin{cases} 0 & if \quad m \neq n, \\ \frac{\pi}{8} & if \quad m = n. \end{cases}$$

Les polynômes orthogonaux classiques univariés sont définis traditionnellement sur $[-1,\ 1]$; cependant, il est plus pratique d'utiliser $[0,\ 1]$.

4.2.1 Fonction génératrice proposée

Les termes des polynômes satisfont la relation de récurrence suivante

$$\begin{cases} U_n(r) = 2rU_{n-1}(r) - U_{n-2}(r),\ n \geq 2, \\ U_0(r) = 1,\ U_1(r) = 2r. \end{cases} \tag{4.2}$$

Considérant le fait que

$$\sum_{n=0}^{\infty} U_n(r)x^n = \frac{1}{1-2rx+x^2},$$

alors la fonction génératrice des polynômes de Chebyshev généralisés de seconde espèce est donnée par

$$f(x) = \frac{1}{1-2xr+r^2}.$$

La théorie bien connue de la formule de Binet sur les nombres de Fibonacci [110, 111] permet d'exprimer les polynômes de Chebyshev généralisés de seconde type en fonction des racines α_1 et α_2 de l'équation caractéristique associée à la relation de récurrence (4.2) :

$$\alpha^2 = 2r\alpha - 1. \tag{4.3}$$

Proposition 4.1 *(Formule de Binet) Les polynômes de Chebychev de seconde espèce sont donnés par*

$$U_n(r) = \frac{\alpha_1^{n+1} - \alpha_2^{n+1}}{\alpha_1 - \alpha_2},$$

Où $\alpha_1,\ \alpha_2$ sont les racines de l'équation caractéristique (4.3) *; alors que $\alpha_1 > \alpha_2$.*

Preuve: . Les racines de l'équation caractéristique (4.3) sont $\alpha_1 = \frac{r+\sqrt{r^2-1}}{2}$ et $\alpha_2 = \frac{r-\sqrt{r^2-1}}{2}$.

Puisque $r > 0$, le

$\alpha_2 < 0 < \alpha_1$ et $|\alpha_2| < |\alpha_1|$,

$\alpha_1 + \alpha_2 = 2r$ et $\alpha_1.\alpha_2 = 1$. ■

Les polynômes de Chebyshev définis ci-dessus peuvent être généralisés en considérant la relation de récurrence suivante

$$\begin{cases} P_n(r) = 2prP_{n-1}(r) + qP_{n-2}(r),\ n \geq 2 \\ P_0(r) = a,\ P_1(r) = br \end{cases} \tag{4.4}$$

Où a, $b \in \mathbb{Z}$, et p, q sont des nombres réels.

De plus, en considérant $a = 1$ et $b = 1$, on obtient les polynômes de Chebyshev de second espèce pour $p = -q = 1$.

Proposition 4.2 *Soit $p, q \in \mathbb{R}$. Une fonction génératrice des polynômes de Chebyshev généralisés de second espèce est dérivée comme suit :*

$$g_{p;q}(x) = \frac{1}{1 - 2prx + qx^2}.$$

Preuve: Le polynôme de Chebyshev généralisé de seconde espèce est donné par

$$\begin{cases} U_n(r) = 2prU_{n-1}(r) - qU_{n-2}(r),\ n \geq 2 \\ U_0(r) = 1,\ U_1(r) = 2pr \end{cases}.$$

En conséquence, la fonction génératrice ordinaire associée est définie par :

$$g_{p;q}(x) = \sum_{n=0}^{+\infty} U_n(r)x^n = U_0(r) + U_1(r)x + \sum_{n=2}^{+\infty} U_n(r)x^n.$$

En utilisant les conditions initiales, nous avons :

$$\begin{aligned} g_{p;q}(x) &= \sum_{n=0}^{+\infty} U_n(r)x^n = U_0(r) + U_1(r)x + \sum_{n=2}^{+\infty} U_n(r)x^n \\ &= 1 + 2pxr + \sum_{n=2}^{+\infty} \left[2prU_{n-1}(r) - qU_{n-2}(r)\right] x^n. \end{aligned} \tag{4.5}$$

Considérant le fait que $j = n - 2$ et $p = n - 1$, l' Eq. (4.5) est réécrite comme suit

$$\begin{aligned} g_{p;q}(t) &= 1 + 2pxr + 2pxr \sum_{p=0}^{+\infty} \left[U_p(r) - 1\right] x^p - qx^2 \sum_{j=0}^{+\infty} U_j(r) x^j \\ &= 1 + 2pxr + 2pxr \sum_{p=0}^{+\infty} U_p(r) x^j - 2pxr - qx^2 \sum_{j=0}^{+\infty} U_j(r) x^j, \end{aligned}$$

ce qui est équivalent à

$$\left(1 - 2pxr + qx^2\right) g_{p;q}(x) = 1,$$

Par conséquent,

$$g_{p;q}(x) = \frac{1}{1 - 2pxr + qx^2}.$$

Ceci complète la preuve. ■

4.2.2 Quantification du comportement chaotique dans la fonction génératrice proposée

Dans cette section, le comportement dynamique de la fonction génératrice proposée est étudié à l'aide de simulations numériques. Pour cela, la fonction génératrice proposée est réécrite sous la forme de récurrence suivante :

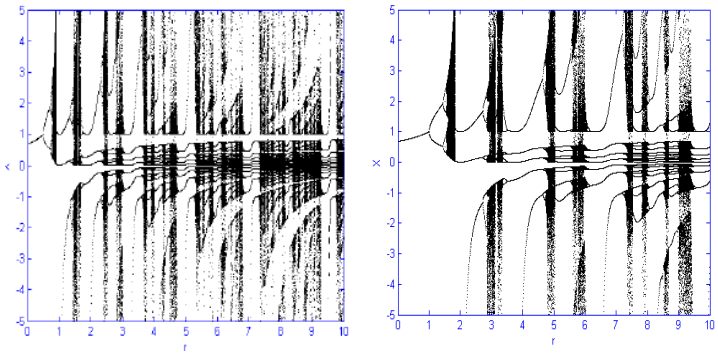
$$x_{p,q}(n) = \frac{1}{1 - 2prx(n-1) + qx^2(n-1)}, \tag{4.6}$$

Où $p,\ q$ sont les paramètres du système.

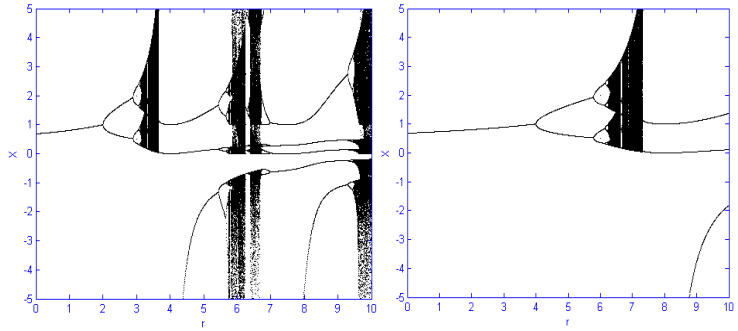
4.2.2.1 Diagramme de bifurcation

Rappelons que le diagramme de bifurcation est un outil de base important pour indiquer le comportement des systèmes chaotiques. Dans le cas de la fonction génératrice proposée, le comportement dynamique de $x(n)$ est exploré pour différentes valeurs de paramètre r dans la plage [0, 10] avec $q = 1$. En utilisant une simulation graphique. Le résultat correspondant est montré sur la Figure 4.1 (a) pour $p = 1$,la Figure 4.1 (b) pour $p = 1/2$,la Figure 4.1 (c) pour

$p = 1/4$ et la Figure 4.1 (d) pour $p = 1/8$. . Il est clair que, les diagrammes de bifurcations montrent une région de cycles limites stables cède ensuite la place à une région étendue de comportements complexes avec des valeurs croissantes du paramètre r. Les régions sombres sont communément appelées comportement chaotique.



(a) $p = 1$ (b) $p = \frac{1}{2}$



(c) $p = \frac{1}{4}$ (d) $p = \frac{1}{8}$

Figure 4.1. Diagramme de bifurcation de la forme de récurrence (4.6).

4.2.2.2 Exposant de Lyapunov

L'existence du chaos dans la fonction génératrice proposée est confirmée par l'analyse de l'exposant de Lyapunov. Par conséquent, pour quantifier le chaos dans le système donné, l'exposant

de Lyapunov est calculé de la manière suivante

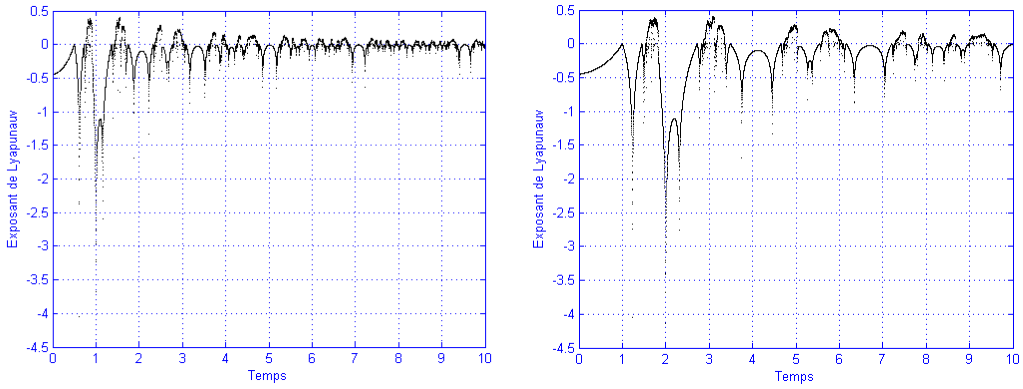
$$\alpha = \lim_{n\to\infty} \frac{1}{N} \sum_{n=1}^{N} \ln\left(\left|\frac{dx_{n+1}}{dx_n}\right|\right), \tag{4.7}$$

d'où, à partir de (4.6) on obtient

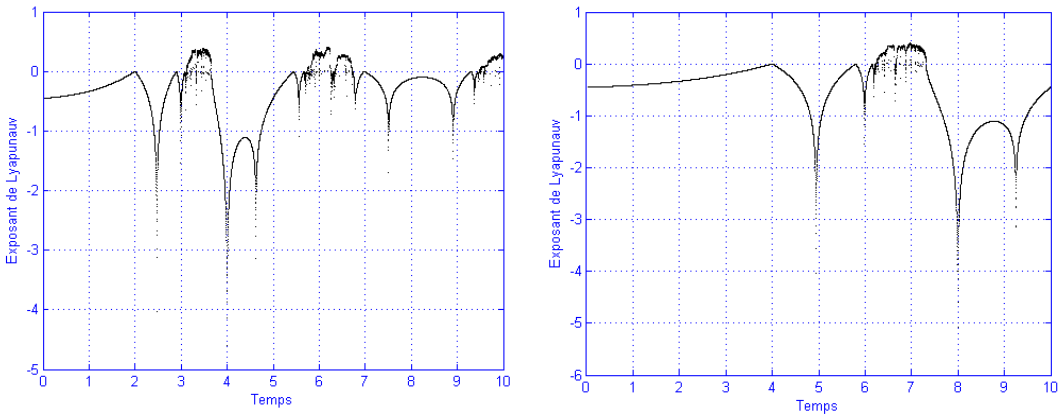
$$\alpha = \lim_{n\to\infty} \frac{1}{N} \sum_{n=1}^{N} \ln\left(\left|\frac{2pr - 2qx_n}{(1 - 2prx_n + qx_n)^2}\right|\right). \tag{4.8}$$

Les valeurs calculées de l'exposant de Lyapunov sont données par la Figure 4. 2.(a) pour $p = 1$, la Figure 4. 2.(b) pour $p = 1/2$, la Figure 4. 2.(c) pour $p = 1/4$, et par la Figure 4. 2.(d) pour $p = 1/8$.

Il est clair que l'exposant de Lyapunov est positif dans les régions sombres du diagramme de bifurcation pour la même plage de paramètres r, ce qui montre la présence de chaos dans la fonction génératrice proposée des polynômes de Chebyshev généralisés de seconde espèce. Notons que, pour certaines plages de paramètres r, le diagramme de bifurcation contient des régions blanches et l'exposant de Lyapunov est négatif ; cela indique que les régions chaotiques se séparent temporairement en région non chaotiques, puis retournent à l'état chaotique.



(a) $p = 1$ (b) $p = \frac{1}{2}$



(c) $p = \frac{1}{4}$ (d) $p = \frac{1}{8}$

Figure 4. 2. Exposant de Lyapunov.

4.2.2.3 Test NIST

La suite de tests statistiques du NIST est un système expérimental. En particulier, NIST SP 800 est une série de directives de sécurité de l'information publiée par le National Institute of Standards and Technology (NIST) qui est devenue une norme et un guide faisant autorité largement reconnu par les chercheurs dans le domaine de la sécurité de l'information. Les tests statistiques sont réalisés à l'aide de la combinaison NIST SP $800-22$ qui se compose de 15 sous-tests pour évaluer le caractère aléatoire des séquences chaotiques générées. Les paramètres du système sont d'abord considérés comme $p = 0.24517, q = 1, r = 2.9493$ et génèrent 100 séquences de longueur de $flux = 1000000$ bit. Les résultats des tests montrent principalement les avantages et les inconvénients de la séquence pseudo-aléatoire en analysant l'uniformité et le taux de réussite du séquençage, où la valeur de probabilité $(P-Value)$ représente l'uniformité de la séquence, et la proportion représente le taux de réussite de la séquence [50]. Dans ce contexte, chaque test donne un niveau de significativité de $\alpha = 0.01$. Par conséquent, la séquence est considérée comme aléatoire uniquement dans le cas où $P - Value \geq \alpha$. Les résultats des tests du NIST sont donnés dans le tableau 1. Evidemment, la plupart des valeurs P sont supérieures à $0,01$ et les proportions sont toutes supérieures à 98%, sauf pour les tests de chevauchement de modèles et de variantes d'excursions aléatoires. Les résultats des tests statistiques attestent du

bon caractère aléatoire des séquences chaotiques générées par la fonction génératrice proposée.

Nom du test	**Valeur p**	**Proportion %**	**Statut**
Test de fréquence	0.6351	99	Passe
Test de fréquence dans un bloc ($m = 128$)	0.7991	100	Passe
La plus longue série de uns dans un test en bloc	0.2884	98	Passe
La plus longue série de uns dans un test en bloc	0.2474	100	Passe
Test du rang	0.0698	99	Passe
Test de la transformée de Fourier discrète	0.0954	99	Passe
Test de correspondance des modèles sans chevauchement	0.9623	100	Passe
Test de correspondance des modèles de chevauchement	0.8811	95	Passe
Test statistique universel de Maurer	0.4475	98	Passe
Test d'entropie approximative	0.4801	100	Passe
Test de complexité linéaire	0.5710	100	Passe
Test en série	0.9612	100	Passe
Test des sommes cumulées ($x = +1$)	0.5294	99	Passe
Test des excursions aléatoires ($x = -1$)	0.7001	100	Passe
Test des variantes d'excursions aléatoires	0.4549	96	Passe

Tableau 4.1. Résultats des tests de la norme NIST 800-22 pour le PRNG chaotique proposé.

4.3 Application de la nouvelle fonction chaotique au cryptage des images numériques

Le système proposé est basé sur le principe de confusion/diffusion décrit dans le chapitre précédent. La confusion n'est qu'un réarrangement des pixels de l'image sans modification des valeurs des pixels avec un objectif primordial qui est celui de briser la forte corrélation entre les pixels. En revanche, la phase de diffusion consiste à masquer les pixels ordinaires par de nouvelles

valeurs chaotiques secrètes. Le schéma général du cryptage est illustré dans la Figure 4.3.

ProcessusdeDéchiffrement

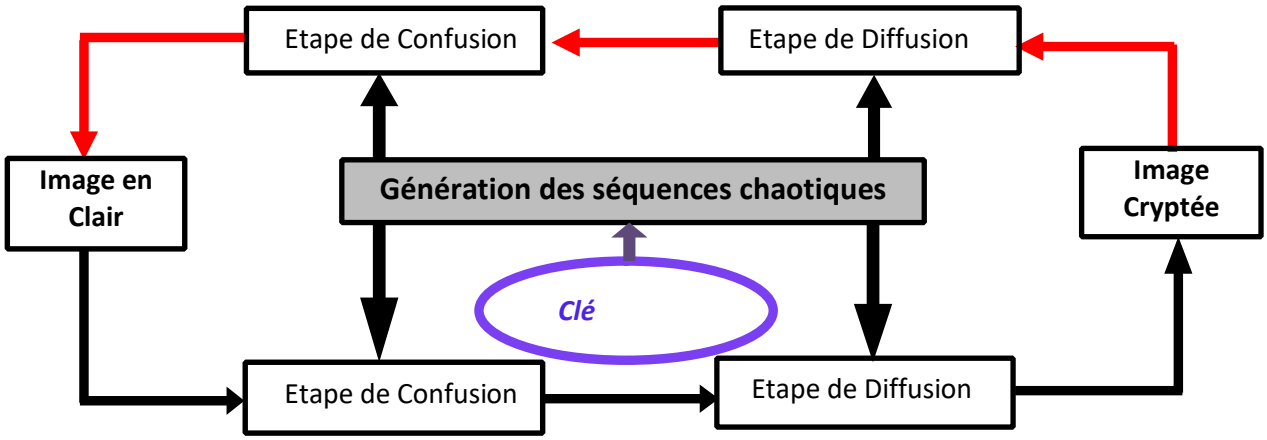


Figure 4.3. Schéma générale du système de cryptage chaotique.

4.3.1 Algorithme de cryptage

Une nouvelle méthode de cryptage d'images a été proposée récemment par Himeur et Boukabou [109], qui utilise un schéma cryptographique basé sur le chaos et utilisant la fonction logistique bidimensionnelle (2-D). Ce crypto-système a prouvé sa robustesse contre de multiples attaques de cryptanalyses. Par conséquent, une mise en œuvre simple de cet algorithme permet d'atteindre un taux de cryptage élevé sur des ordinateurs à usage général et convient donc parfaitement à certaines applications multimédias telles que les systèmes de communication mobiles. Dans notre travail, nous introduisons quelques modifications au schéma de cryptage d'image [93] en utilisant la fonction génératrice chaotique proposée de sorte que la valeur initiale ainsi que les paramètres du système constituent la clé de cryptage. Ce schéma représente l'élément crucial de l'étape de confusion dans notre système de cryptage. Pour ce qui est de l'étape de diffusion, nous nous sommes appuyés sur l'opérateur XOR afin de réaliser le "masquage". L'algorithme suivant illustre les différentes étapes.

1. Choisir une image en clair.

2. Définir également la clé secrète K_s en fonction des conditions initiales et des paramètres du système exprimés par $K_s = [x(0), r_1, r_2, r_3, r_4, r_5]$.

3. Générer une séquence chaotique en utilisant la fonction génératrice proposée des polynômes de Chebyshev de seconde espèce donnée par l'équation (4.6).

4. Construire une séquence binaire $C = [c_0; c_1; ...; c_{N-1}]$ comme suit :

$$c_k = \begin{cases} 1 & \text{si } x(n) > T \\ 0 & \text{sinon} \end{cases},$$

où N est la longueur de la séquence binaire C et T est la valeur du seuil. Un vecteur V_{in} d'indices linéaires correspondant à C sera attribué.

5. Diviser les bits du vecteur d'entrée $V_{in} = [v_0, v_2, \ldots, v_{N-1}]$ en deux groupes $B_1 = [b_0^1, b_1^1, ..., b_{\frac{N}{2}-1}^1]$ et $B_2 = [b_0^2, b_1^2, ..., b_{\frac{N}{2}-1}^2]$ en fonction des bits de la séquence C. Pour chaque bit c_k de C, le bit correspondant de V_{in} est vérifié. Si le bit est à 1, le bit correspondant dans V_{in} est placé dans B_2. Sinon, ce bit sera placé dans B_1.

6. Mettre $V_{out} = C$, puis répéter les étapes 1 à 4 Nc fois. Enfin, la valeur de résultat dans V_{out} est obtenue en concaténant B_1 et B_2.

7. Générer deux séquences chaotiques «Seq1» et «Seq2» , à l'aide de la fonction génératrice proposée des polynômes de Chebyshev de seconde espèce donnée par l'équation (4.6).

8. Calculer les valeurs de la séquence « Mask1 » et « Mask2» par la multiplication des valeurs de des séquences «Seq1» et «Seq2» par un scalaire K=10^{10}. Ces différentes valeurs doivent être comprises entre 0 et 255.

9.Calculer l'image cryptée par l'application de l'opération XOR entre la valeur de chaque pixel et la valeur correspondante de Seq1 et Seq2.

Le processus de déchiffrement constitue le processus inverse du processus de cryptage. Il faut noter qu'une très légère variation de l'un de ces paramètres rend le processus de décryptage impossible.

4.3.2 Analyse des performances

Un bon schéma de cryptage doit résister à tous les types d'attaques connus, tels que les attaques exhaustives, les attaques statistiques, les attaques différentielles, etc. Dans cette section, l'analyse de sécurité du schéma de cryptage proposé est discutée en détail. En général, quatre aspects sont souvent utilisés comme mesures de performance dans les systèmes basés sur le cryptage d'images, à savoir l'analyse des histogrammes, l'analyse des corrélations entre pixels, l'analyse de l'entropie des informations et la capacité à résister à tous les types d'attaques connus.

4.3.2.1 Analyse de clé (attaque exhaustive)

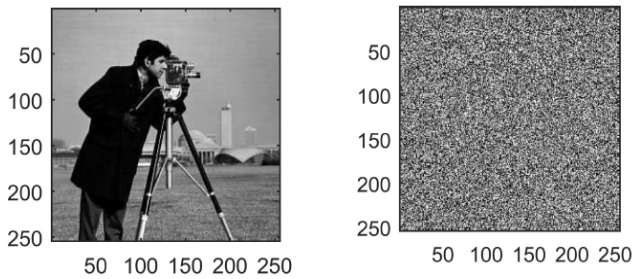
4.3.2.1.1 Analyse de l'espace clé Dans le système de cryptage proposé, l'espace des clés est le nombre total de clés différentes utilisées dans la procédure, qui se compose de six parties (x_0, r_1, r_2, r_3, r_4, r_5) et d'un nombre flottant à double précision d'une longueur de 52 bits, conformément à la norme IEEE 754. Notons que plus l'espace des clés est grand plus le crypto-système est efficace. Supposons que toutes les valeurs initiales x_0 du système chaotique soient des nombres positifs inférieurs à 1 et que les plages de paramètres r_1, r_2, r_3, r_4, r_5 sont données sans le Tableau 4.2. Ainsi, l'espace de clé est $10^{14}\times(2.83\times10^{14})^2\times(2.35\times10^{14})\times(1.68\times10^{14})\times(0.97\times10^{14})$ $= 30.6705\times10^{84} = 2^{4.93}\times2^{288} = 2^{292.93} > 2^{100}$ qui est suffisamment grand, et peut donc résister aux attaques par force brute.

Paramètre p	**Fonction génératrice appliquée**	**Range**
$p = 1$	$\frac{1}{1-2r_1x+x^2}$	2.837
$p = \frac{1}{2}$	$\frac{1}{1-r_3x+x^2}$	2.354
$p = \frac{1}{4}$	$\frac{1}{1-\frac{1}{2}r_4x+x^2}$	1.689
$p = \frac{1}{8}$	$\frac{1}{1-\frac{1}{4}r_5x+x^2}$	0.973

Tableau 4.2. Plage de valeurs pour chaque variable de la clé de sécurité.

4.3.2.1.2 Analyse de la sensibilité des clés Cette sensibilité est un critère important pour évaluer un bon système de cryptage d'images. A cette fin, plusieurs tests ont été effectués en utilisant l'image en clair 'cameraman' comme indiqué ci-dessous :

Dans le processus de chiffrement, l'image en clair est chiffrée en utilisant la clé secrète K_1 : (0.6, 2.94, 2.9493, 0.111, 3.225, 7.225). Ensuite, on essaie de déchiffrer l'image chiffrée obtenue en utilisant la clé K_2 en modifiant très légèrement la clé originale K_1, c'est-à-dire K_2 : (0.6, 2.94, 2.9493, $0.111 + 10^{-14}$, 3.225, 7.225). Les images décryptées obtenues sont présentées à la figure 4.4. Un changement minime de la clé de sécurité entraîne un changement important de l'image chiffrée.



(a) (b)

Figure 4.4. Décryptage de l'image cryptée obtenue à l'aide de la clé secrète : $(a)K_1$ et (b) K_2.

En outre, des analyses quantitatives sont effectuées pour chaque clé en utilisant l'information mutuelle. Cette métrique est généralement appliquée pour évaluer la sensibilité aux clés de deux images cryptées par des clés secrètes différentes sur la même image en clair.

L'information mutuelle est présentée comme suit :

$$I(E1; E2) = H(E1) - H(E1|E2). \tag{4.9}$$

Par conséquent, plus la valeur de l'information mutuelle de deux images cryptées $E1$ et $E2$ est faible, plus la sensibilité des clés secrètes est élevée. Ainsi, si les deux images cryptées $E1$ et $E2$ ne sont pas identiques, alors la connaissance de $E1$ ne donne pas nécessairement d'information sur $E2$ et vice versa. En fait, il n'y a pas d'échange d'informations entre les deux images cryptées, et la sensibilité de la clé, dans ce cas, est très élevée. Par contre, si E1 et E2 sont identiques, dans ce cas, toutes les informations transmises par $E1$ seront partagées avec $E2$ et il n'y a pas de sensibilité de la clé.

Pour les expériences de simulation, la sensibilité des clés a été comparée entre toutes les

clés secrètes. En conséquence, la sensibilité a été calculée en utilisant (4.7) pour chaque clé par rapport aux autres clés non modifiées. Les images en clair ont été testées pour le cryptage à un tour dans les expériences. Les sensibilités de chaque clé et la performance moyenne sont indiquées dans le tableau 4. 3. D'après les résultats obtenus, on remarque que la sensibilité d'une clé est élevée car l'information partagée entre $E1$ et $E2$ est proche de zéro. Par conséquent, on peut affirmer que l'adversaire ne sera pas en mesure de distinguer les différents paramètres des clés secrètes.

Image	x_0	r_1	r_2	r_3	r_4	r_5
Cameraman	01899	0.1918	0.1914	0.1895	0.1904	0.1906
Bateau	0.1908	0.1920	0.1900	0.1912	0.1902	0.1894
Babouin	0.1893	0.1919	0.1912	0.1883	0.1921	0.1887
Moyenne	0.1900	0.1919	0.1908	0.1897	0.1909	0.1895

Tableau 4.3. Information mutuelle de l'algorithme proposé comparée entre toutes les clés secrètes.

4.3.2.2 Analyse statistiques

4.3.2.2.1 Analyse de l'entropie de l'information Les valeurs d'entropie des images cryptées sont données dans le tableau 4.6. Comme on peut le constater, les valeurs d'entropie obtenues sont très proches des valeurs théoriques. Cela signifie que la fuite d'information dans le processus de cryptage d'image est négligeable.

Image testée	**Taille**	**Image en clair**	**Image cryptée**
Bbaboon	256×256	7.3461	7.9993
Boat	512×512	7.4842	7.9995
Cameraman	256×256	7.0097	7.9982
Mountain	512×512	7.1914	7.9994

Tableau 4.4. Valeurs d'entropie des images cryptées.

4.3.2.3 Analyse des histogrammes

L'analyse de l'histogramme est très importante car elle décrit la distribution des pixels dans une image en traçant le nombre de pixels à chaque niveau d'intensité. Dans un contexte de cryptage d'image, l'histogramme de l'image cryptée doit être uniforme pour garantir la sécurité contre l'attaque du texte en clair connu, c'est-à-dire qu'un attaquant ne peut pas extraire d'informations de l'image cryptée. La figure 4.5 montre les résultats de simulation obtenus pour le processus de cryptage.

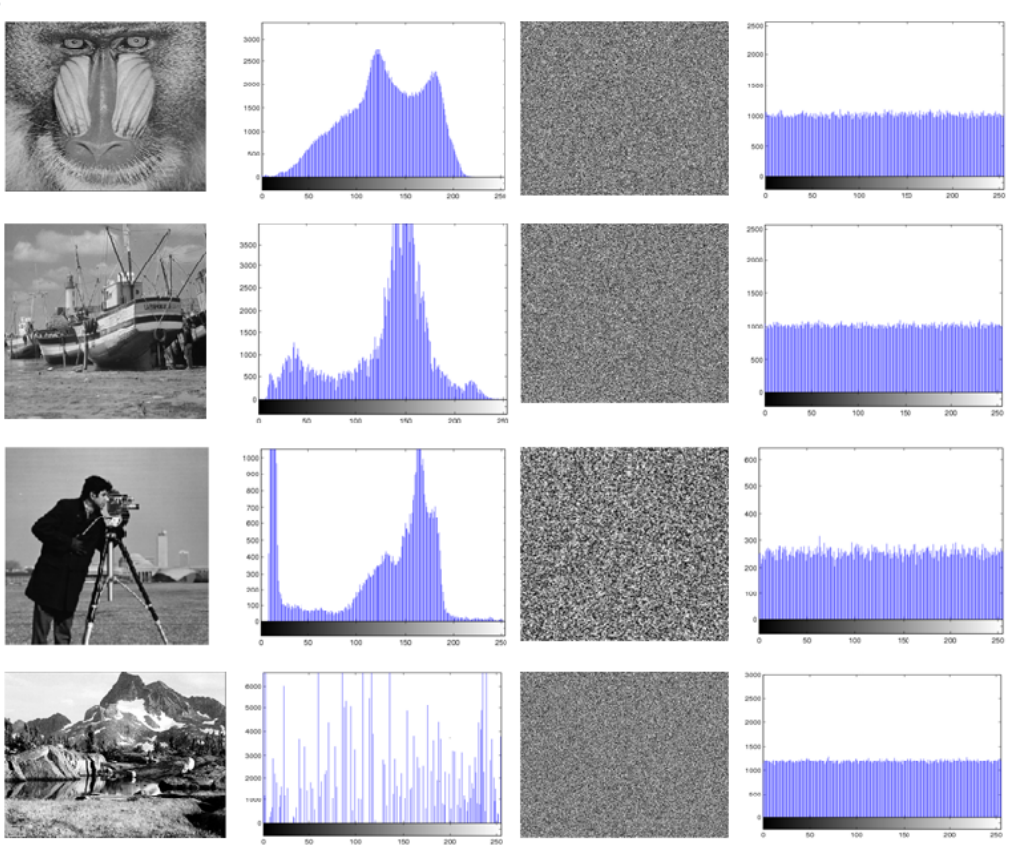


Figure 4.5. Résultats des simulations. (a) Images originales. (b) Histogrammes des images originales. (c) Images cryptées. (d) Histogrammes des images cryptées.

A partir de la figure 4.4, on peut voir que l'histogramme des images cryptées est uniformément distribué par rapport à l'histogramme des images en clair (à gauche), et ne fournit donc aucune information utile pour effectuer une attaque sur l'image cryptée.

Alors que l'histogramme est une estimation de la distribution de probabilité réelle des valeurs d'intensité pour les images cryptées obtenues, la variance d'un histogramme est très utile pour comparer les variances entre les images cryptées lorsque les clés secrètes changent [114]. Une valeur plus faible des variances indique une plus grande uniformité des images cryptées.

La variance de l'histogramme d'une image en niveaux de gris est définie par :

$$var(Y) = \frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{1}{2} (y_i - y_j)^2, \tag{4.10}$$

Où $Y = \{y_1, y_2, ..., y_{256}\}$ est le vecteur des valeurs de l'histogramme, tandis que y_i et y_j sont les nombres de pixels tels que i et j sont les valeurs de gris correspondantes, respectivement.

Le tableau 4.5 montre les valeurs de variance de l'histogramme et les valeurs PSNR pour les images en clair et les images cryptées correspondantes. Evidemment, les valeurs de variance des images en clair sont beaucoup plus importantes que celles des images cryptées. Les résultats obtenus prouvent que le schéma de cryptage proposé a distribué uniformément les histogrammes des images cryptées. En outre, les valeurs de variance d'histogramme obtenues sont plus petites par rapport à celles obtenues par Chai et al [114]. Ensuite, nous procédons à l'analyse des résultats PSNR obtenus. Ces résultats indiquent que le PSNR est inférieur à 5 dB (< 5 dB) pour toutes les images cryptées.

Image	**Originale**	**Cryptée**	**PSNR**
Caméraman	11097.33	258.62	4.374
Bateau	96083.68	253.70	4.321
Babouin	65912.54	269.24	4.485

Tableau 4. 5. Variations des histogrammes et PSNR pour les images en clair et leurs images cryptées correspondantes.

4.3.2.4 Analyse des corrélations de pixels

Les pixels adjacents d'une image standard présentent une forte corrélation. Un bon schéma de cryptage d'image doit supprimer cette corrélation pour garantir la sécurité contre l'analyse

statistique. Dans cette section, les corrélations des pixels adjacents de l'image originale et de l'image cryptée sont analysées et comparées en choisissant 10000 paires de pixels adjacents dans les directions horizontales, verticales et diagonales de l'image en clair et de son image cryptée. Le coefficient de corrélation est calculé pour les paires sélectionnées en utilisant l'équation suivante [115] :

$$R_{xy} = \frac{Conv(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{4.11}$$

Tandis que ;

$$\begin{aligned} Conv(x,y) &= \frac{1}{N}\sum_{n=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right). \\ D(x) &= \frac{1}{N}\sum_{n=1}^{N}\left[x_i - E(x)\right]^2,\ E(x) = \frac{1}{N}\sum_{n=1}^{N} x_i, \end{aligned}$$

Où x et y sont les valeurs en niveaux de gris de deux pixels adjacents de l'image, respectivement, et N est le nombre total de pixels. Si le coefficient de corrélation est égal à 1, cela signifie que l'image originale et son image cryptée sont fortement dépendantes. En revanche, si ce coefficient est égal à 0, alors l'image cryptée et l'image en clair ne sont pas corrélées. Les résultats obtenus sont indiqués dans le tableau 4.6.

Directions des pixels	Horizontale		verticale		Diagonale	
Image	Originale	Cryptée	Originale	Cryptée	Originale	Cryptée
Caméraman	0.9335	-0.0034	0.9592	0.0044	0.9087	0.0046
Bateau	0.9381	-0.0002	0.7587	-0.0016	0.7262	-0.0040
Montagne	0.8632	0.0017	0.8580	0.0016	0.38266	0.0023
Babouin	0.8665	0.0015	0.9713	0.0012	0.7262	0.0009

Tableau 4. 6. Coefficients de corrélation entre les pixels adjacents de l'image en clair et de l'image cryptée.

Selon la relation spatiale d'un pixel et de son pixel adjacent, la distribution de corrélation des contrôles de deux pixels adjacents peut être appliquée aux trois directions (c'est-à-dire hori-

zontale, verticale et diagonale). Les figures 4.6 (a) - (d) montrent la distribution de corrélation des pixels adjacents dans différentes directions pour 1024 paires de pixels adjacents sélectionnés au hasard pour l'image en clairet l'image cryptée. Dans chaque figure, l'axe des x représente l'intensité d'un pixel sélectionné au hasard et l'axe des y représente l'intensité du pixel adjacent correspondant. Il est clair que la corrélation fortement dépendante entre les pixels adjacents est complètement brisée dans toutes les directions après l'application du processus de cryptage.

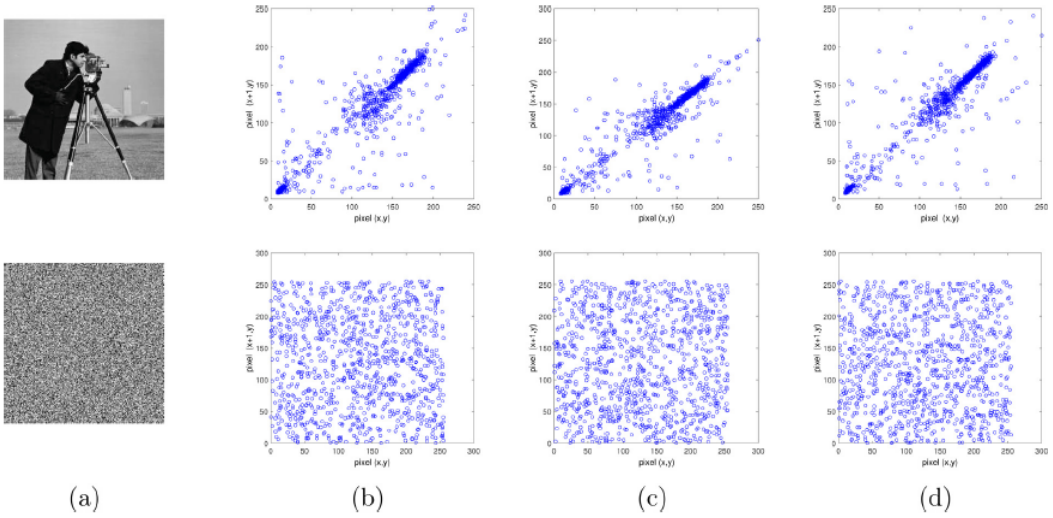


Figure 4.6. Distribution de la corrélation des pixels adjacents dans différentes directions. (a) Images originales et cryptées. (b) Direction diagonale. (c) Direction verticale. (d) Direction horizontale.

4.3.2.5 Capacité de résistance à l'analyse différentielle

Une propriété souhaitable des systèmes de cryptage est leur grande sensibilité aux petites modifications de l'image en clair. Pour calculer l'effet de la modification d'un seul pixel sur l'image cryptée, deux quantités courantes peuvent être utilisées : le taux de changement du nombre de pixels (NPCR) et la moyenne unifiée du changement d'intensité (UACI). Le NPCR mesure le pourcentage du nombre de pixels différents par rapport au nombre total de pixels entre deux images tandis que l'UACI mesure la différence moyenne d'intensité entre les deux images.

Ces deux quantités sont définies par les formules (3.6) et (3.7) comme suit :

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100, \tag{4.12}$$

$$UACI = \frac{1}{M \times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{|I_1(i,j) - I_2(i,j)|}{255} \times 100. \tag{4.13}$$

Où M et N représentent respectivement la largeur et la hauteur d'une image. $I_1(i,j)$ et $I_2(i,j)$ sont les valeurs des pixels à la position (i,j) des deux images cryptées dont les images en clairs ne diffèrent que d'un pixel. La matrice $D(i,j)$ est de même taille que I_1 et I_2 telle que :

$$D(i,j) = \begin{cases} 1, & \text{si } I_1(i,j) \neq I_2(i,j) \\ 0, & \text{sinon} \end{cases}.$$

Le tableau 4.7 montre la robustesse de l'algorithme appliqué utilisant la fonction de génération proposée en termes de métriques NPCR et UACI. Les résultats obtenus montrent que les caractéristiques de la fonction de génération chaotique proposée ont une performance similaire à la fonction logistique 2-D standard utilisant l'algorithme proposé dans [93].

Image	**NPRC(%)**	**UACI(%)**
Caméraman	99.6109	33.0123
Bateau	99.6902	32.6151
Montagne	99.6191	33.4928
Babouin	99.8142	33.6863

Tableau 4.7. Robustesse de l'algorithme appliqué en utilisant la fonction de génération proposée en termes de scores NPCR et UACI.

4.3.2.6 Test d'aléatoire de l'image cryptée

Le test NIST a été appliqué pour vérifier les caractères aléatoires des images cryptées obtenues en utilisant la séquence chaotique formée par la fonction génératrice proposée. Les résultats du

test sont présentés dans le tableau 4.8. Evidemment, le cryptage proposé présente de bonnes performances aléatoires puisque tous les résultats de test obtenus sont supérieurs à $0,01$.

Nom du test	**Image cryptée du caméraman**	**Statut**
Test de fréquence	0.3055	Passe
Test de fréquence dans un bloc	0.5479	Passe
Test d'exécution	0.4834	Passe
La plus longue série de uns dans un test en bloc	0.1468	Passe
Test du rang	0.0423	Passe
Test de la transformée de Fourier discrète	0.9200	Passe
Test de correspondance des modèles sans chevauchement	0.3875	Passe
Test de correspondance des modèles de chevauchement	0.8350	Passe
Test statistique universel de Maurer	0.6878	Passe
Test d'entropie approximative	0.4701	Passe
Test de complexité linéaire	0.5610	Passe
Test en série	0.9522	Passe
Test des sommes cumulées	0.5194	Passe
Test des excursions aléatoires	0.3901	Passe
Test des variantes d'excursions aléatoires	0.9451	Passe

Tableau 4.8. Résultats du test NIST pour l'image cryptée.

L'algorithme proposé est sensible à la condition initiale x_0 et aux cinq paramètres du système r_1, r_2, r_3, r_4, r_5. Comme indiqué précédemment dans la sous-section consacrée à l'analyse de la sensibilité de la clé, une très légère modification de la clé originale ne permet pas de décrypter l'image originale et la valeur du résultat V_{out} dans l'algorithme de cryptage sera totalement différente. De plus, étant donné que le vecteur d'entrée V_{in} dépend des deux groupes B_1 et B_2 dans l'étape de diffusion combinée, une image chiffrée différente a une valeur en clair pré-modifiée et une valeur chiffrée pré-modifiée totalement différentes de l'image en clair originale.

Par conséquent, l'algorithme proposé peut résister à l'attaque par texte en clair/texte chiffré sélectionné.

4.4 Conclusion

Une fonction génératrice des polynômes de Chebyshev de deuxième espèce a été proposée. Cette fonction génératrice a montré un comportement chaotique pour certaines plages de paramètres du système, en particulier, une cascade typique de doublement de période vers le chaos. Ce phénomène a été prouvé par l'analyse du diagramme de bifurcation et de l'exposant de Lyapunov et quantifié à l'aide de la combinaison de test NIST. En tant qu'application, la fonction génératrice proposée a été insérée dans un algorithme de crypto-système récent à la place de la fonction logistique 2-D. Le principal avantage de cet algorithme consiste dans le fait de distribuer les erreurs de rafale causées par les différentes attaques à travers différentes positions. Les résultats numériques obtenus et exprimés par les différentes figures et les différents tableaux montrent que l'algorithme de cryptage proposé peut rendre les pixels de l'image originale presque indépendants les uns des autres. Par conséquent, des résultats très prometteurs ont été obtenus en termes d'analyse de sécurité, de robustesse aux attaques exhaustives, aux attaques statistiques et aux attaques différentielles.

Conclusion Générale

Actuellement, les chercheurs accordent beaucoup d'attention à la proposition de nouvelles fonctions chaotiques afin de les appliquer dans le domaine de la cryptographie pour protéger les données numériques, et en particulier les images numériques. En effet, ces dernières présentent plusieurs propriétés intrinsèques telles que la redondance en hauteur des données, la grande taille et la forte corrélation entre pixels adjacents, qui les rendent différentes des données textuelles. De plus, des caractéristiques temporelles sont nécessaires à la transmission d'images numériques en temps réel. Par conséquent, il devient indispensable de disposer d'un système de cryptage à haut débit et de haute sécurité.

Il existe une variété des algorithmes de cryptage, qui ont prouvé leur performance et leur efficacité pour des informations textuelles, comme AES, RSA. Cependant, ils sont loin d'être adéquats pour le chiffrement des données fortement corrélées. Une des solutions prometteuses pour le chiffrement de ce type de données est celle que nous avons explorée dans cette thèse. Nous nous sommes appuyées sur la théorie du chaos dans le cryptage en raison de ses caractéristiques particulières et notamment sa sensibilité aux conditions initiales.

Notre objectif dans cette thèse fût donc de concevoir et mettre en œuvre un système de cryptage chaotique pour les images numériques. Pour ce faire, nous avons commencé par rappeler des généralités instructives concernant les quatre domaines de notre travail : la cryptographie, l'image numérique, le chaos et les fonctions génératrices. Ensuite nous avons présenté un état de l'art en matière de la cryptographie chaotique des images, ce qui nous a permis de bien

positionner notre travail.

Nous avons montrer par recourir au diagramme de bifurcation et de l'analyse des exposants de Lyapunov le comportement chaotique de la fonction génératrice ordinaire des polynômes de Chebychev de deuxième espèce. Cette nouvelle fonction chaotique peut être utilisée de manière sécurisée comme étant un générateur de nombres pseudo-aléatoires pour le système de cryptage chaotique des images numériques.

Les résultats de la simulation ont montré que la corrélation de l'image est considérablement réduite et que la capacité à résister aux attaques statistiques et au bruit est considérablement améliorée.

Notre thèse ouvre la voie à de nombreuses pistes de recherche que nous considérons comme prometteuses. A titre d'exemple nous envisageons à court terme, l'étude du comportement dynamique de la famille unidimensionnelle de la fonction $g_{p;q}(x) = \frac{1}{1-2pxr+qx^2}$, pour les différentes valeurs des paramètres de contrôle p et q. Les diagrammes de bifurcation et les exposants de Lyapunov nous permettront de montrer qu'un petit changement pour les valeurs de p ou de q conduit à un comportement chaotique totalement différent. A plus long terme, l'étude d'une fonction de chebychev de second ordre à deux (2D) (voire à plusieurs) dimensions serait à envisager. Quant au système de cryptage, l'exploitation du principe d'ADN dans l'algorithme de cryptage pourrait le rendre encore plus performant.

Enfin rappelons que notre système est davantage conçu pour les images en niveau de gris. D'autres types de données peuvent être traités, nous pensons notamment à celles des vidéos.

Bibliographie

[1] B. Schneier, Cryptographie appliquée. International Thomson Publishing France, Paris, (2001).

[2] N. Louzzani, A. Boukabou, H. Bahi, A. Boussayoud, A novel chaos based generating function of the Chebyshev polynomials and its applications in image encryption, , Chaos, Solotons and Fractals. 151 (111315), 1-10 , 2021.

[3] S. Douglas, Cryptographie :Théorie et pratique. Vuibert Informatique, Paris, (2001).

[4] A. Ali pacha, N. Hadj said, La Cryptographie et ses principaux systèmes de références, RIST 12 (1), 173-193, 2002.

[5] R. Stinson, Cryptography theory and practice, discrete mathematics and its applications. chapman & hall/crcpress, New York, (2005).

[6] M.A. Filali, Etude et Implémentation Pipeline sur FPGA de l'algorithme de chiffrement AES, mémoire de magister, Université de Mohamed Boudiaf, Oran, (2015).

[7] X. Wang, L. Teng, X. Qin. A novel colour image encryption algorithm based on chaos, Signal Process. 92(4), 1101–1108, 2012.

[8] A. Wurcker. Etude de la sécurité d'algorithmes de cryptographie embarquée vis-à-vis des attaques par analyse de la consommation de courant, Thèse de Doctorat en Informatique, Université de Limoges, France, (2015).

[9] B. Gérard, Cryptanalyses statistiques des algorithmes de chiffrement à clef secréte, Thèse de Doctorat en Informatique, Université de Paris 6, France, (2015).

[10] M.B.Luca, Apports du chaos et des estimateurs d'états pour la transmission sécurisée de l'information. Thèse de doctorat en électronique, université de Bretagne Occidentale, (2006).

[11] G. Zaibi, Sécurisation par dynamiques des réseaux locaux sans fil au niveau de la couche MAC, Thèse de Doctorat de l'université de Toulouse, (2012).

[12] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, Int.J. Bifurcation Chaos, 16(8), 2129–2151, 2006.

[13] E. Yavuz, A novel chaotic image encryption algorithm based on content sensitive dynamic functions witching scheme, Optics and Laser Technology, Optics & Laser Technology, 114, 224-239, 2019.

[14] M. Asgari-Chenaghlu, M.A. Balafarand, M.-R.Feizi-Derakhshi, A novel image encryption algorithm based on polynomial combination of chaoticmaps and dynamic function generation, Signal Processing, 157, 1-13, 2019.

[15] Z.Tang,Y, Yang, S. XuandX.Z, C.Yu, Image Encryption with Double Spiral Scans and Chaotic Maps,Security and Communication Networks, 19 Article ID 8694678, 15 pages, 2019.

[16] A. Boussayoud, L'action de l'opérateur $\delta^k_{e_1e_2}$ sur la série $\sum_{n=0}^{\infty\infty} S_n(A)e_1^n z^n$, Thèse de doctorat en Mathématiques, Université de Jijel, (2017).

[17] M. Alawida, A. Samsudin, J.S. Teh, R.S. Alkhawaldeh, A new hybrid digital chaotic system with applications in image encryption, Signal Process, 160, 45–58, 2019.

[18] G. Alvarez , S. Li, Some basic cryptographicrequirements for chaos-basedcryptosystems, Int. J. Bifurcation Chaos. 16(8), 2129–2151, 2006.

[19] R. Matthews, On the derivation of a chaoticencryptionalgorithm. Cryptologia. 13(1), 29–42, 1989.

[20] L. M. Pecora, T. L. Carroll, Synchronization in chaotic systems, Physical review letters.64(8), 821-825, (1990).

[21] K. U. Shahna, A. Mohamed, A novel image encryptions chemeusing both pixel level and bit level permutation with chao ticmap, Appl. Soft Comput. 90, 106-162, 2020.

[22] M. Sharma, Mk. Kowar, Image encryption techniques usingchaoticschemes, International Journal of Engineering Science and Technology, 2(6), 2359-2363, 2010.

[23] S. Shaukat, A.L. Arshid,A. Eleyan, S.A. Shah, J. Ahmad, Chaos theory and its application : An essential framework for image encryption, Chaos Theory. Appl. 2(1), 15–20, 2020.

[24] G. Chen, T. Ueta, Yet another chaotic attractor. Int J Bifurcation Chaos, 9(07), 1465–1476, 1999.

[25] G. Layek, An introduction to dynamical systems and chaos, Springer, (2015).

[26] R. Kautz, Chaos : the science of predictable random motion, Oxford University Press, (2011).

[27] G. Linage, F. Montoya, A. Sarmiento, Showalter K , Parmananda P . Fibonacci order in the period-doubling cascade to chaos, Phys Lett A, 359(6), 638–649, 2006.

[28] JC.Sprott, Chaos and time-series analysis, Oxford University Press, (2003).

[29] W.M. Ahmad , JC. Sprott, Chaos in fractional-order autonomous nonlinear systems. Chaos Solitons Fractals ,16(2), 339–351, 2003.

[30] K. Kiers, T. Klein ,J. Kolb, S. Price, JC. Sprott, Chaos in a nonlinear analog com- puter. Int J Bifurcation Chaos, 14(08), 2867–2873, 2004.

[31] A. Radwan, On some generalized logistic maps with arbitrary power. J Adv Res.4, 163–71, 2013.

[32] M. Özer, A. Cenys, Y. Polatoglu, G. Hacibekiroglu, E. Akat, A. Valaristos, Bifurcations of fibonacci generating functions. Chaos Solitons Fractals.33(4), 1240–1247, 2007.

[33] P. Kumar, B.N. Miller, Chaotic dynamics of one-dimensional systems with peri- odic boundary conditions. Phys Rev E, 90(6) ID062918, 2016.

[34] R.E. Carvalho, E.D. Leonel, Squared sine logistic map, Physica A.463, 37–44, 2016.

[35] M. Sajid, AS. Alsuwaiyan, Chaotic behavior in the real dynamics of a one parameter family of functions, Int J.Appl. Sci.Eng. 12(4) :289–301,2014.

[36] M. Sajid, Real fixed points and dynamics of one parameter family of function. J Assoc Arab Univ.Basic Appl Sci. 21(1) :92–105, 2016.

[37] L.C. Andrews, Special functions for engineers and applied mathematicians, Macmillan, (1985).

[38] PJ. Davis, Interpolation & approximation. New York : Dover Publication Inc, (1975).

[39] G. Dattoli, D. Sacchetti, C. Cesarano, A note on Chebyshev polynomials. Annali dell'Universitádi Ferrara, 47(1), 107–15, 2001.

[40] HS-H. Manocha, H. Srivastava, A treatise on generating functions. Mathematics and its applications. Ellis Horwood Series ; (1984).

[41] C. Cesarano, Identities and generating functions on Chebyshev polynomials. Georgian Math J. 19(3) :427–440, 2012.

[42] JL. Vega, E. Tlelo-Cuautle, Simulation of piecewise-linear one-dimensional chaotic maps by Verilog-A. IETE Tech Rev. 32(4) :304–310, 2003.

[43] LG. Fraga, E. Torres-Pérez, E. Tlelo-Cuautle, C. Mancillas-López, Hardware implementation of pseudo-random number generators based on chaotic maps. Nonlinear Dyn.90(3), 1661–1670, 2017.

[44] A. Senouci, H. Bouhedjeur, K. Tourche, A. Boukabou, FPGA based hardware and device-independent implementation of chaotic generators, AEU-Int J Electron- Commun. 82, 211–220, 2017.

[45] JL.Valtierra, E. Tlelo-Cuautle, Á. Rodríguez-Vázquez, A switched-capacitor skew–tent map implementation for random number generation. Int J Circuit Theo- ryAppl, 45(2), 305–315, 2017.

[46] H Prasetyo, A New Image Encryption Technique Using Simple ChaoticMaps 2018 International Symposium on Electronics and Smart Devices (ISESD), 2018, pp. 1-4, doi : 10.1109/ISESD.2018.8605462.

[47] C. Pak, L. Huang, A new color image encryption using combination of the 1D chaotic map, Signal Processing, 2017.

[48] Z. Hua, Y. Zhou, C. Chen, Digital Signal Processing and Signal Processing Education Meeting (IEEE, 2013) pp. 118–123.

[49] Wang, G.Y., Yuan, F. : Cascade chaos and its dynamic characteristics. Acta Phys. Sin 62(2), 020506, 2013.

[50] L. Liu, H. Song, Electron. Design Eng. 13, 123, 2014.

[51] G. Chen, Y. Mao and C. K. Chui, A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps, Chaos Solitons & Fractals. 21(3), 749–761, 2004.

[52] Y. Mao, G. Chen, S. Lian, A Novel Fast Image Encryption Scheme Based On 3D Chaotic Baker Maps International Journal of Bifurcation and Chaos.14,(10), 3613-3624, 2004.

[53] Z.H. Guan, F.J. Huang, W.J. Guan, Chaos-based image encryption algorithm. Phys. Lett. A 346, 153–157, 2005.

[54] S. Lian , J. Shun, Z. Wang, A block cipher based on a suitable use of the chaotic standard map. Chaos, Solitons & Fractals
26(1), 117–29, 2005.

[55] K.Sakthidasan Sankaran, B.V.Santhosh Krishna, A New ChaoticAlgorithm for Image Encryption and Decryption of Digital Color Images, International Journal of information and Education Technology, 1(2), 137-141, 2011.

[56] A. Anto Steffi, D. Sharma, Modified Algorithm of Encryption and Decryption of Images using Chaotic Mapping , International Journal of Science and Research 2(2), 77-81, 2013.

[57] Z. Peng, C. Wang, Y. Lin, X. Luo, A novel four-dimensional multi-wing hyperchaotic attractor and its application in image encryption, Acta Phys. Sin. 63 (24), 97–106, 2014.

[58] R. Boriga, A.C. Dăscălescu, I. Priescu, A new hyperchaotic map and its application in an image encryption scheme, Signal Process – Image. 29 (8) 887-901, 2014.

[59] T. Gao, Z. Chen, A new image encryption algorithm based on hyperchaos, Phys. Lett. A. 372 (4), 394–400, 2008.

[60] S. Cang, G. Qi, Z. Chen, A four-wing hyper-chaotic attractor and transient chaos generatedfrom a new 4-D quadraticautonomous system, Nonlinear Dyn.59 (3), 515–527, 2012.

[61] X. Wang, L. Yang, R. Liu, R, A chaotic image encryption algorithm based on perceptron model, Nonlin. Dyn. 62, 615–621, 2010.

[62] L. Xu , Z. Li , J. Li , A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng.78, 17–25, 2016.

[63] XL. Chai , An image encryption algorithm based on bit level Brownian motion and new chaotic systems, Multimed Tools Appl 76(1), 1159–1175, 2017.

[64] SL. Sun, A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling, IEEE Photonics Journal 10(2), 1–14, 2018.

[65] Z. Tang, J. Song, X. Zhang, Multiple-image encryptionwith bit-plane decomposition and chaoticmaps, Opt Lasers Eng. 80, 1–11, 2016.

[66] L. Teng, X. Wang, J. Meng, A chaotic color image encryption using integrated bit-level permutation, Multimed Tools Appl 77(16), 6883–6896, 2018.

[67] H. Khanzadi, M. Eshghi, S.E. Borujeni, Image Encryption Using Random Bit Sequence Based on Chaotic Maps, Arab J Sci Eng 39(2), 1039–1047, 2014.

[68] J. Liu, D. Yang, H. Zhou, A digital image encryption algorithm based on bit-planes and an improved logistic map, Multimed Tools Appl.77(8), 10217–10233, 2018.

[69] LY. Xiang , XB. Shen, JH. Qin , W. Hao, Discrete multi-graph hashing for large-scalevisualsearch, Neural ProcessLett 49(3), 1055–1069, 2019.

[70] J. Zhang, D. Fang , H. Ren, Image Encryption Algorithm Based on DNA Encoding and Chaotic Maps, Mathematical Problems in Engineering, ID 917147, 10 pages, 2014.

[71] H. Liu , X. Wang, Image encryptionusing DNA complementaryrule and chaoticmaps, Applied Soft Computing.12, 1457–1466, 2012.

[72] A. Belazi, M.Talha, S. Kharbech,W. Xiang, NovelMedical Image EncryptionSchemeBased on Chaos and DNA Encoding, IEEE Access, 7, 36667–36681, 2019.

[73] H. Liu, B. Zhao,L. Huang, A RemoteSensing Image Encryption Scheme Using DNA Bases Probability and Two-Dimensional Logistic Map, IEEE Access, 7, 65450–65459, 2019.

[74] X. Chai, Y. Chen Y, L. Broyde, A novel chaos-based image encryptionalgorithm using dnas equence operations. Opt Lasers Eng. 88, 197–213, 2017.

[75] T. Zhang, S. Yan, C. Yan Gu, K. Liao, Research on Image EncryptionBased on DNA Sequence and Chaos Theory, Physics : Conf. Series,1004, 1–6, 2018.

[76] X. Quan Fu, B. Liu, Yi. Xie, W. Li, Y Liu, Image Encryption-Then-Transmission Using DNA EncryptionAlgorithm and The Double Chaos, IEEE Photonics, 10(3), 1-16, 2018.

[77] T. Li, J. Shi, X. Li, J. Wu, F. Pan, Image EncryptionBased on Pixel-Level Diffusion with DynamicFiltering and DNA-Level Permutation with 3D Latin Cubes, Entropy,21(3), 1-21, 2019.

[78] A. Rey, G. Anchez, A. de la Villa Cuenca, A Protocol to Cipher Digital Images Based on Cat Maps and Cellular Automata , Third Iberian Conference, IbPRIA 2007, Girona, Spain, June 6-8, 2007, Proceedings, Part I.

[79] Á. Martín del Rey, G. Rodríguez Sánchez, A. de la Villa Cuenca, Encrypting Digital Images Using Cellular Automata, Lecture Notes in Computer Science, ID 7209 :78-88, 2012.

[80] X.Wang, D Xu, A novel image encryptions chemeusing chaos and langtonsant cellular automaton, Nonlinear Dynamics, 79(4), 2449-2456, 2015.

[81] A. Souyah, A. Faraoun, An image encryption scheme combining chaos-memory cellular automata and weightedhistogram, Nonlinear Dyn, 86, 639–653, 2016.

[82] P. Ping, J. Wu, Y. Mao, F. Xu , J. Fan, Design of image cipherusing life-likecellu- larautomata and chaoticmap, Signal Process.150, 233–47, 2018.

[83] E. García-Guerrero E, E. Inzunza-González, O. López-Bonilla, J. Cárdenas-Valdez, E.Tlelo-Cuautle, Randomness improvement of chaotic maps for image encryp- tion in a wireless communication scheme using PIC-microcontroller via Zigbee channels, Chaos Solitons Fractals, 133, ID109646, 2020.

[84] E. Tlelo-Cuautle, JD. Díaz-Muñoz, AM. González-Zapata, R. Li, W.D. León-Salas, FV. Fernández, Chaotic image encryption using hopfield and Hind- marsh–Rose neurons implemented on FPGA. Sensors. 20(5), ID1326, 2020.

[85] X. Wang, L. Feng, H. Zhao, Fast image encryption algorithm based on parallel computing system. Inf Sci. 486, 340–358, 2019.

[86] X. Wang, S. Gao, Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a boolean network. Inf Sci. 539, 195–214, 2020.

[87] X. Wang, S. Gao, Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensor product theory. Inf Sci. 507 :16–36, 2020.

[88] X. Wang , J. Yang, A privacy image encryption algorithm based on piece- wise coupled map lattice with multi dynamic coupling coefficient. Inf Sci. 569, 217–40, 2021.

[89] Y. Xian, X. Wang, Fractal sorting matrix and its application on chaotic image encryption. Inf Sci. 547, 1154–1169, 2021.

[90] A. Boussayoud, A. Abderrezzak, S. Araci, A new symmetric endomorphism op- erator for some generalizations of certain generating functions. Notes Number Theory Discrete Math.24, 45–58, 2018.

[91] A. Boussayoud , M. Kerada, A. Abderrezzak, A generalization of some orthogonal polynomials. Springer Proc Math Stat. 41, 229–235, 2013.

[92] N. Saba, A. Boussayoud, On the bivariate Mersenne Lucas polynomials and their properties. Chaos Solitons Fractals. 146, ID110899, 2021.

[93] Y. Himeur, A. Boukabou, A robust and secure key-frames based video watermarking system using chaotic encryption. Multimedia Tools Appl. 77(7), 8603–8627, 2018.

[94] E. Yavuz, A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme, Optics and Laser Technology, 114, 224-239, 2019.

[95] M. Asgari-Chenaghlu, M.-A. Balafar and M.-R. Feizi-Derakhshi, A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation, Signal Processing, 157, 1-13, 2019.

[96] Z. Tang, Y. Yang, S. Xu and X. Z, ChunqiangYu, Image Encryptionwith Double Spiral Scans and ChaoticMaps, Security and Communication Networks, 19, ID 8694678, 15 pages, 2019.

[97] H. Liu, X. Wang, Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl. 59(10) :3320–3327, 2010.

[98] H. Liu, X. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun, 284(16–17) :3895–3903, 2011.

[99] H. Liu, X. Wang, Image encryption using dna complementary rule and chaotic maps. Appl Soft Comput. 12(5) :1457–1466, 2012.

[100] X. Wang, Y. Zhang ,X. Bao, A novel chaotic image encryption scheme using DNA sequence operations. Opt Lasers Eng. 73 :53–61, 2015.

[101] X. Wang, L. Yang, R. Liu, A. Kadir, A chaotic image encryption algorithm based on perceptron model, Nonlinear Dyn. 62(3), 615–621, 2010.

[102] X. Wang, L. Liu, Y. Zhang, A novel chaotic block image encryption algorithm based on dynamic random growth technique, Opt Lasers Eng . 66, 10–18, 2015.

[103] Y. Mao, G. Chen, S. Lian, A novel fast image encryption scheme based on 3D chaotic baker maps. Int J Bifurcation Chaos. 14(10), 3613–3624, 2004.

[104] X. Ge, B. Lu, F. Liu, D. Gong, An image encryption algorithm based on informa- tion hiding. Int J Bifurcation Chaos. 26(11),165-192, 2016.

[105] G. Ye, C. Pan, X. Huang, Z. Zhao, J. He, A chaotic image encryption algorithm based on information entropy. Int J Bifurcation Chaos. 28(01), 185–210, 2018.

[106] C. Gangadhar, K. Deergha Rao, Hyperchaos based image encryption. Int J Bifur- cation Chaos.19(11), 3833–3839, 2009.

[107] Y. Li, C. Wang, H. Chen, A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation, Opt Lasers Eng.90, 238–246, 2017.

[108] F. Djimasra, JD. Nkapkop, N.Tsafack, J. Kengne, JY. Effa, A. Boukabou, Robust cryptosystem using a new hyperchaotic oscillator with stricking dynamic properties, Multimedia Tools Appl. 80(11), 1–17, 2021.

[109] GB. Djordjevic . Some properties of partial derivatives of generalized fibonacci and Lucas polynomials. Fibonacci Quart. 39, 138–141, 2001.

[110] S. Falcon, A. Plaza, On k-fibonacci sequences and polynomials and their deriva- tives. Chaos Solitons Fractals. 39(3) :10 05–1019, 2009.

[111] H. VE, Fibonacci and Lucas numbers. Palo Alto, (1969).

[112] A. Rukhin , J. Soto, J. Nechvatal, M. Smid, E. Barker, A statistical test suite for random and pseudorandom number generators for cryptographic applications. Tech. Rep.. Booz-Allen and Hamilton Inc McLean VA, (2001).

[113] Y-Q. Zhang, X-Y, Wang, A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Inf Sci. 273, 329–51, 2014.

[114] X. Chai, Z. Gan, K.Yuan, Y. Chen, X. Liu, A novel image encryption scheme based on dna sequence operations and chaotic systems. Neural Comput Appl.31(1), 219–237, 2019.

[115] L. Kocarev, S. Lian, Chaos-based cryptography : theory, algorithms and applica- tions,354, Springer Science & Business Media, (2011).

[116] L. Liu, S. Miao, A new simple one-dimensional chaotic map and its application for image encryption, Multimed. Tools Appl. 77(16), 21445–21462, 2018.