جامعة سيدي محمد بن عبد الله بفاس
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH DE FES

كلية العلوم والتقنيات فاس
FACULTÉ DES SCIENCES ET TECHNIQUES DE FÈS

N° d'ordre : 47/2023

Centre des Etudes Doctorales : Sciences et Techniques et Sciences Médicales
Formation Doctorale : SISPMI (Sciences de l'Ingénieur, Sciences Physiques, Mathématiques et Informatique)
Spécialité* : Informatique
Laboratoire : Systèmes Intelligents et Applications (SIA)

Thèse pour l'obtention de DOCTORAT

Contribution au chiffrement des images niveaux de gris en utilisant la théorie du Chaos et les moments orthogonaux discrets

Préparée par : Mr Abdelhalim Kamrani

Soutenue le 08 Juillet 2023 **devant le jury :**

Nom et Prénom	Grade	Etablissement	Qualité
Rachid BEN ABBOU	PES	Faculté des Sciences et Techniques de Fès	Président
My Driss EL OUADGHIRI	PES	Faculté des Sciences de Meknès	Rapporteur
Mohamed EL ANSARI	PES	Faculté des Sciences de Meknès	Rapporteur
Abdelali BOUSHABA	PH	Faculté des Sciences et Techniques de Fès	Rapporteur
Hakim EL FADILI	PES	Ecole Nationale des Sciences Appliquées de Fès	Examinateur
Khalid ZENKOUAR Said NAJAH	PES PES	Faculté des Sciences et Techniques de Fès Faculté des Sciences et Techniques de Fès	Directeurs de thèse

جامعة سيدي محمد بن عبد الله بفاس
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH DE FES
كلية العلوم والتقنيات فاس
FACULTÉ DES SCIENCES ET TECHNIQUES DE FÈS

Résumé de la thèse

Dans ce travail nous proposons un ensemble d'algorithmes de chiffrement basés sur la théorie du chaos et les moments discrets orthogonaux. Dans une première contribution nous introduisons un nouveau schéma de chiffrement basé sur la théorie de moment. En effet, Les coefficients des moments de l'image sont d'abord estimés, ensuite on applique les opérations de chiffrement chaotique sur cet espace moment. Ainsi, nous avons développé cinq algorithmes de chiffrement basés sur les moments de Tchebichef, Krawtchouk, Hahn, Dual-Hahn et Racah. Une étude comparative entre ces algorithmes et un algorithme de chiffrement basé sur la DCT montre la supériorité des algorithmes proposés. Outre, une étude comparative est menée entre nos algorithmes et ceux de l'état de l'art. Nous avons conclu que les algorithmes proposés sont assez sécurisés pour résister à tout type d'attaques connues.

Le deuxième d'axe de recherche consiste à optimiser le temps du calcul des algorithmes proposés. Pour cela, nous avons proposé un nouveau schéma de chiffrement basé sur les moments de Tchebichef et la théorie du chaos. Ce chiffrement dit sélectif, chiffre un sous ensemble de coefficients de Tchebichef, le résultat est un algorithme plus rapide avec un temps de calcul largement réduit. En plus, les expérimentations menées ont montré que cet algorithme est sécurisé entre toutes les attaques classiques. Toujours dans cette perspective d'améliorer le temps de calcul des algorithmes de chiffrement, nous proposons un ensemble d'algorithmes de chiffrement chaotiques basés sur un schéma de calcul parallèle et qui utilise les moments séparables discrets. Ce schéma de calcul parallèle réalise les étapes nécessaires au chiffrement sur des « Thread » séparés, ce qui permet l'exécution de plusieurs processus en même temps. Ainsi, nous avons présenté trois algorithmes de chiffrement basés sur les moments séparables de Tchebichef-Krawtchouk (TKM), Tchebichef-Hahn (THM) et Krawtchouk-Hahn (KHM) et utilisant un schéma de chiffrement chaotique parallèle. Les résultats des expérimentations réalisés montrent bien une amélioration considérable de temps de calcul ainsi qu'une résistance à toutes les attaques connues.

Mots clés : Chiffrement d'image, théorie du chaos, les moments discrets orthogonaux, les moments séparables, chiffrement sélectif.

Abstract

In this work we propose a set of encryption algorithms based on chaos theory and orthogonal discrete moments. In a first contribution we introduce a new encryption scheme, the coefficients of the moments of the image are first computed and the chaotic encryption operations are applied to them. Thus we develop five encryption algorithms based on the moments of Tchebichef, Krawtchouk, Hahn, Dual-Hahn and Racah. A comparative study between these algorithms and an encryption algorithm based on DCT shows the superiority of the proposed algorithms. In addition, a comparative study is conducted between our algorithms and those of the state of the art. We concluded that the proposed algorithms are secure enough to resist all types of known attacks.

The second axis of research consists in optimizing the computation time of the proposed algorithms. For this purpose, we have proposed a new encryption scheme based on Tchebichef moments and chaos theory. This so-called selective encryption, encrypts a subset of Tchebichef coefficients, the result is a faster algorithm with a greatly reduced computation time. In addition, experiments have shown that this algorithm is secure against all classical attacks. Still in this perspective of improving the computation time of encryption algorithms, we propose a set of chaotic encryption algorithms based on a parallel computation scheme and which makes use of separable moments. This scheme realizes the necessary steps for encryption on separate threads, which allows the execution of several processes at the same time. Thus, we have presented three encryption algorithms based on the separable moments of Tchebichef-Krawtchouk (TKM), Tchebichef-Hahn (THM) and Krawtchouk-Hahn (KHM) using a parallel chaotic encryption scheme. The results of the experiments show a considerable improvement in computation time and resistance to all known attacks.

Keywords : Image encryption, chaos theory, discrete orthogonal moments, separable moments, selective encryption.

Remerciements

Je tiens à exprimer ma profonde gratitude envers toutes les personnes que je souhaite remercier dans ces lignes, non pas par simple tradition, mais parce qu'elles ont joué un rôle crucial dans la réalisation de ce travail.

Tout d'abord, mes remerciements les plus sincères vont à mes encadrants, **M. ZENKOUAR Khalid** et **M. NAJAH Said**, chercheurs à la Faculté des Sciences et Techniques de Fès, ainsi que membres du Laboratoire Systèmes Intelligents et Applications. Leur expertise, leurs conseils éclairés, leur soutien continu et leur disponibilité ont été des éléments essentiels dans le développement de cette thèse. Je suis profondément reconnaissant envers vous pour votre précieuse contribution.

Je souhaite également exprimer ma gratitude envers mes amis et collègues du Laboratoire Systèmes Intelligents et Applications. Votre amitié, vos discussions enrichissantes et votre soutien infaillible ont contribué à rendre ce parcours plus agréable et stimulant. Je vous suis reconnaissant pour votre présence.

Un remerciement tout particulier est également adressé aux membres du jury : **M. BEN ABBOU Rachid**, Professeur à la Faculté des Sciences et Techniques de Fès ; **M. EL OUADGHIRI My Driss**, Professeur à la Faculté des Sciences de Meknès ; **M. EL ANSARI Mohamed**, Professeur à la Faculté des Sciences de Meknès ; **M. BOUSHABA Abdelali**, Professeur à la Faculté des Sciences et Techniques de Fès ; et **M. EL FADILI Hakim**, Professeur à l'Ecole Nationale des Sciences Appliquées de Fès. Votre temps, votre expertise et votre intérêt pour ma thèse ont été des facteurs déterminants dans la réussite de ce travail. Je vous suis extrêmement reconnaissant.

Enfin, je souhaite exprimer ma reconnaissance envers ma famille et toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce projet. Vos encouragements, votre soutien et vos sacrifices ont été essentiels dans la concrétisation de cette thèse.

Merci à tous pour votre précieuse collaboration et votre impact significatif sur ce travail. Votre contribution restera gravée dans ma mémoire.

Productions scientifiques

Articles

Abdelhalim Kamrani, Khalid Zenkouar, and Said Najah. "A new set of image encryption algorithms based on discrete orthogonal moments and Chaos theory." Multimedia Tools and Applications 79.27 (2020): 20263-20279.

Abdelhalim Kamrani, Khalid Zenkouar, and Said Najah. "Fast chaotic encryption scheme based on separable moments and parallel computing" (En cours de révision dans le journal Multimedia Tools and Applications, Springer).

Abdelhalim Kamrani, Khalid Zenkouar, and Said Najah. "Fast selective encryption algorithms based on moments and chaos theory" (En cours de révision dans le journal EAI Endorsed Transactions)

Conférences

Abdelhalim Kamrani, Khalid Zenkouar, and Said Najah "A Framework For Privacy Preserving Medical Content Based Image Retrieval" (Acceptée et publication en cours chez The International Conference on Advances in Communication Technology and Computer Engineering (ICACTCE) - AIP(2022)- Meknes, Morocco.)

Abdelhalim Kamrani, Khalid Zenkouar, and Said Najah "Efficient Selective Image Encryption Based on Chaos and Tchebichef Moments" (Acceptée et publication en cours chez The International Conference on Advances in Communication Technology and Computer Engineering (ICACTCE) - AIP(2022)- Meknes, Morocco.)

Abdelhalim Kamrani, Khalid Zenkouar, and Said Najah "Selective encryption for textured images based on Tchebichef moments" (Acceptée et publication en cours chez The 5th International Conference of Computer Science and Renewable Energies- Agadir, Morocco, July 22-24, 2022)

Table des matières

1 Chiffrement des images et théorie du Chaos **5**
1.1 Introduction . . . 5
1.2 Chiffrement des images . . . 5
1.2.1 Généralités sur le chiffrement . . . 5
Chiffrement par flux ou chiffrement par bloc . . . 6
Cryptanalyses . . . 6
1.2.2 Particularités du chiffrement d'image . . . 7
1.3 Théorie du chaos . . . 9
1.3.1 Définition . . . 9
1.3.2 Découverte du chaos . . . 10
1.3.3 Systèmes chaotiques . . . 10
1.3.4 Les caractéristiques de base du chaos . . . 11
Définition du chaos discret . . . 11
Relations entre le chaos et la cryptographie . . . 12
Le chaos pour la cryptographie . . . 13
1.4 Conclusion . . . 14

2 Théorie des moments **15**
2.1 Généralités sur les moments . . . 15
2.1.1 Représentation des caractéristiques . . . 15
2.1.2 Apperçu mathématique des moments . . . 17
2.1.3 Applications des moments . . . 19
2.2 Orientations de recherche et avancées récentes . . . 20
2.2.1 Calculs précis . . . 22
Erreur géométrique . . . 22
Erreur d'intégration numérique . . . 23
Erreur de représentation . . . 25
Progression récente du calcul précis . . . 26
2.2.2 Calcul rapide . . . 27
Calcul global . . . 27
Calcul local . . . 28
Progrès récents du calcul rapide . . . 30
2.2.3 Robustesse/Invariance Optimisation . . . 31
Transformation affine . . . 32
Bruit . . . 33
Brouillage . . . 34
Progrès récents dans le domaine de l'optimisation de la robustesse/Invariance . . . 35
2.3 Conclusion . . . 36

3 Un nouvel ensemble d'algorithmes de chiffrement d'images basé sur les moments orthogonaux discrets et la théorie du chaos 37
3.1 Introduction . . . 37
3.2 Contexte théorique . . . 39
3.2.1 Fonctions de moment . . . 39
3.2.2 Moments orthogonaux discrets . . . 39
3.2.3 La théorie du chaos pour la cryptographie . . . 41
3.3 Approche proposée . . . 41
3.3.1 Chiffrement . . . 42
3.3.2 Déchiffrement . . . 43
3.4 Résultats expérimentaux . . . 43
3.4.1 Attaques différentielles NPCR et UACI . . . 44
3.4.2 Analyse du coefficient de corrélation . . . 46
3.4.3 Analyse des espaces clés . . . 47
3.4.4 Analyse d'entropie . . . 47
3.4.5 Chiffrement sélectif des images basé sur le chaos et les moments de Tchebichef . . . 49
Chiffrement . . . 50
Déchiffrement . . . 50
3.4.6 Étude expérimentale . . . 50
Analyse des espaces clés . . . 50
Similitude d'image . . . 50
Coefficient de corrélation . . . 51
Analyse différentielle : NPCR et UACI . . . 51
Entropie . . . 51
Analyse de la vitesse . . . 52
3.5 Conclusion . . . 52

4 Schéma de chiffrement chaotique rapide basé sur les moments séparables et le calcul parallèle 55
4.1 Introduction . . . 55
4.2 Connaissances pertinentes . . . 57
4.2.1 Moments séparables . . . 57
4.2.2 Carte logistique . . . 58
4.3 Les algorithmes de chiffrement proposés . . . 58
4.3.1 Chiffrement . . . 61
4.3.2 Déchiffrement . . . 62
4.4 Étude expérimentale . . . 63
4.4.1 Analyse des espaces clés . . . 63
4.4.2 Attaques différentielles . . . 63
4.4.3 Analyse statistique . . . 66
Analyse d'histogramme . . . 66
Corrélation des pixels adjacents . . . 66
4.4.4 Analyse de l'entropie de l'information . . . 66
4.4.5 Analyse de la vitesse . . . 68
4.5 Conclusion . . . 68

Bibliographie 75

Table des figures

2.1 Une classification des moments de l'image 18
2.2 Les directions de recherche des moments d'image 21
2.3 La mise en correspondance des coordonnées entre la région carrée de l'image numérique et le disque unitaire. 23
2.4 Le mappage des coordonnées dans le schéma de pavage en pixels polaires 25
2.5 Illustrations de points symétriques dans le disque unitaire 29

3.1 Architecture d'un système de chiffrement basé sur le chaos 41
3.2 Architecture des algorithmes proposés 42
3.3 Images de tests 46

4.1 Schéma général pour le chiffrement basé sur le chaos 58
4.2 Diagramme de bifurcation pour la carte logistique 60
4.3 Exposant de Lyapunov avec $\mu = 3.999$ 60
4.4 Le schéma de chiffrement proposé 61
4.5 Le schéma de déchiffrement 63
4.6 Images utilisées pour les expériences 66
4.7 Analyse d'histogramme pour les algorithmes de chiffrement proposés 68

Liste des tableaux

1.1 Similitudes et différences entre le chaos et la cryptographie 13

2.1 Coordonnées cartésiennes et coordonnées polaires des points symétriques 29

3.1 Principales caractéristiques des moments orthogonaux discrets 40
3.2 Résultats comparatifs en termes de valeurs NPCR des images de test. . 45
3.3 Résultats comparatifs en termes de valeurs UACI des images de test. . 47
3.4 Résultats comparatifs en termes de coefficient de corrélation des images de test. 48
3.5 Résultats comparatifs en termes d'entropie des images de test. 49
3.6 Résultats MSE 51
3.7 Résultats du coefficient de corrélation 51
3.8 Résultats NPCR 52
3.9 Résultats UACI 52
3.10 Résultats de l'entropie 52
3.11 Résultats pour le temps de calcul 53

4.1 proprietés des moments séparables utilisés 59
4.2 Résultats NPCR pour les algorithmes proposés par rapport aux algorithmes de l'état de l'art 64
4.3 Résultats UACI pour les algorithmes proposés par rapport aux algorithmes de l'état de l'art 65
4.4 Coefficient de corrélation pour les algorithmes de chiffrement proposés par rapport aux algorithmes de l'état de l'art. 67
4.5 Résultats de l'entropie pour les algorithmes proposés par rapport aux algorithmes de l'état de l'art 69
4.6 Analyse de la vitesse des algorithmes proposés par rapport aux algorithmes de l'état de l'art 70

Introduction générale

Ces dernières années, parallèlement à la promotion et à la popularisation rapides de la technologie des réseaux et de la technologie de communication numérique dans le monde, les images numériques et les images numériques basées sur la vidéo sont devenues un support important pour le stockage et la transmission d'informations dans le réseau informatique dans les domaines civil et militaire. Cependant, les problèmes de sécurité des réseaux ont longtemps été un facteur important qui a entravé et limité le développement de la technologie des réseaux. En particulier dans le contexte des ressources d'information du public et des départements gouvernementaux, comment réaliser la protection de la sécurité des données dans le réseau informatique est le contenu important et la direction de la recherche dans le domaine de la sécurité des réseaux et de l'information. Parmi ces données, l'image numérique et la vidéo numérique sont devenues le contenu important de la transmission de données dans le réseau en raison de leur caractère intuitif et pratique. Par conséquent, la protection de la sécurité des images numériques a reçu une grande attention de toutes les parties. Compte tenu de la situation de plus en plus grave en matière de sécurité des réseaux ces dernières années, la transmission et le partage d'informations basées sur des images numériques sont souvent confrontés à des problèmes de vol, de falsification, de suppression et d'attaque des données, qui ont causé de grandes pertes aux propriétaires ou aux éditeurs d'images numériques.

Dans le système de sécurité des informations numériques, la technologie de chiffrement est une technique très courante. Si la sécurité et la fiabilité de la méthode de chiffrement sont suffisamment élevées, la confidentialité des informations numériques peut être protégée [76, 269, 40]. Par conséquent, la recherche sur la technologie et la méthode de chiffrement des images numériques est une direction importante pour la protection de la sécurité des images numériques. Cependant, la technologie de chiffrement ou le système de chiffrement est principalement basé sur les exigences du chiffrement de texte. Actuellement, le système de chiffrement le plus courant ne peut pas obtenir de meilleurs résultats en matière de compatibilité et de qualité de chiffrement des images numériques. Bien que les images numériques puissent être traitées comme un ensemble de données bidimensionnelles, les systèmes cryptographiques qui utilisent directement des techniques de chiffrement de texte sont souvent confrontés à des problèmes d'inefficacité du chiffrement et du déchiffrement, de faible praticabilité et de faible sécurité [27, 22, 202, 118]. La recherche d'un système cryptographique ou d'une méthode de chiffrement adaptée au chiffrement des images numériques est le seul moyen de protéger la confidentialité des images numériques dans l'environnement réseau. Dans le domaine du chiffrement sécurisé des images numériques, deux types de moyens techniques sont généralement utilisés :

1) Technologie de filigrane numérique, cette technologie adopte le traitement de la signature des images numériques et ajoute des informations de filigrane personnalisées aux images numériques originales afin de protéger le droit d'auteur des images numériques. C'est l'un des moyens techniques importants pour la protection de la sécurité des images sur Internet. Cependant, l'inconvénient de la technologie du

filigrane numérique est que la visibilité des images numériques ne peut être évitée. En général, seul le droit d'auteur de l'image n'est pas violé, et lorsque le contenu de l'image numérique doit être protégé, il n'y a rien à faire.

2) La méthode de protection de l'image numérique est la technologie de chiffrement d'image [225, 223, 264, 3], et son principe de base est de chiffrer les informations numériques contenues dans l'image numérique, et d'obtenir des images chiffrées complètement différentes de l'apparence et de l'image numérique originale, de sorte que le contenu de l'image numérique ne peut pas être visualisé directement. Lorsque l'image numérique est nécessaire pour être visualisée ou utilisée, l'algorithme de déchiffrement correspondant est utilisé pour calculer et déchiffrer l'image chiffrée afin de restaurer le contenu original de l'image numérique, ce qui est un moyen important pour la protection du contenu de l'image numérique dans un environnement distribué avec des exigences de sécurité élevées.

Avec la demande croissante de chiffrement d'images, de nombreux chercheurs ont proposé de nombreuses techniques et méthodes de chiffrement différentes dans le domaine du chiffrement d'images numériques. Les algorithmes ou techniques typiques d'usage courant comprennent principalement le chiffrement d'images numériques basé sur la transformation des pixels, le chiffrement d'images numériques basé sur la séquence aléatoire, le chiffrement d'images numériques basé sur le codage de compression d'images et le chiffrement d'images numériques basé sur la clé d'image. La technologie du chaos est difficile à craquer et aléatoire, ce qui fait que la technologie de chiffrement d'image numérique basée sur la technologie du chaos devient une technologie de chiffrement d'image numérique plus fiable. De nombreux chercheurs ont introduit le concept de chaos; dans les années 1980 [146], le mathématicien britannique Matthews a proposé pour la première fois une méthode de chiffrement basée sur un système chaotique logistique. Dans la méthode de chiffrement de Matthews, le type de technologie de chiffrement est la technologie de chiffrement de flux, qui combine spécifiquement la puissance chaotique et la cryptographie. Bien que la technologie et la méthode de chiffrement ne puissent pas répondre aux exigences commerciales en termes de précision de chiffrement, de capacité de sécurité de chiffrement et d'efficacité réelle de chiffrement, elles jouent un rôle essentiel dans le développement et l'application de la technologie de chiffrement chaotique. Ensuite, Toshiki Habutsu [75], un universitaire japonais, a publié la méthode de chiffrement itérative du chiffrement chaotique dans la conférence européenne de cryptographie, ce qui constitue une avancée majeure pour la technologie de chiffrement chaotique. Par la suite, les recherches de la communauté cryptographique sur la technologie de chiffrement chaotique se sont rapidement développées. Le chercheur américain Fridrich [70] a proposé une technologie et une méthode de chiffrement chaotique basées sur la cartographie bidimensionnelle de Baker et l'a appliquée au chiffrement et à la protection des images numériques. Il s'agit de la première application et pratique du chiffrement chaotique dans le domaine du chiffrement des images numériques [96, 53, 218]. Afin d'améliorer la sécurité et la fiabilité de la technologie de chiffrement chaotique, certains chercheurs ont étendu la méthode de chiffrement chaotique bidimensionnelle pour réaliser des méthodes de chiffrement chaotique dans un espace tridimensionnel et multidimensionnel [256, 135, 28]. Cependant, dans le processus de chiffrement chaotique tridimensionnel, les étapes de traitement de l'opération de brouillage et de l'opération d'obfuscation sont toujours traitées de manière isolée, et des paramètres de contrôle fixes sont adoptés dans le traitement, de sorte que l'algorithme et la méthode de chiffrement chaotique semblent toujours être brisés.

D'après la situation générale, les résultats de la recherche dans le domaine du

chiffrement chaotique d'images numériques sont relativement riches, et ils ont également grandement favorisé le développement et l'application rapides de la technologie de chiffrement d'images numériques. Cependant, la technologie actuelle de chiffrement chaotique des images ne parvient toujours pas à franchir la catégorie des systèmes chaotiques bidimensionnels d'ordre entier, et les caractéristiques dynamiques et le caractère pseudo-aléatoire peuvent encore être améliorés. La technologie de chiffrement chaotique basée sur l'espace de haute dimension proposée par certains chercheurs présente les problèmes de la faible uniformité des pixels dans le processus de chiffrement, de la difficulté du traitement de la confusion et de la faible efficacité du processus de chiffrement et de déchiffrement.

Cependant, Les moments ont été largement utilisés dans le traitement des images, la reconnaissance des formes et la vision par ordinateur [47, 153, 277]. Teague a proposé des polynômes orthogonaux continus comme fonctions de base pour calculer les moments continus [203]. Ces polynômes orthogonaux comprennent les polynômes de Zernike, les polynômes de Legendre, les pseudo-Zernike et les polynomes de Tchebichef. Parmi les différents types de moments, les moments géométriques cartésiens sont les plus utilisés. Il a été démontré [159] que les moments orthogonaux discrets sont plus performants que les moments orthogonaux continus classiques en termes de capacité de représentation des images. Depuis que Hu a introduit les invariants de moments, les moments et les fonctions de moments, en raison de leur capacité à représenter les caractéristiques globales d'une image, ont trouvé de nombreuses applications dans les domaines du traitement des images et de la reconnaissance des formes [254, 155], de l'indexation des images [143], de l'ajustement robuste des lignes [106] et de la reconnaissance des images [38]. Toutefois, l'application de la théorie des moments dans le domaine de la sécurité d'information n'a pas encore suscité suffisamment d'intérêt. [101].

Notre travail de thèse s'inscrit dans cette dynamique de recherche et se propose d'enrichir la littérature par de nouvelles contributions liés au chiffrement des images utilisant la théorie des chaos. Dans un premier travail nous proposons un ensemble d'algorithmes de chiffrement basé sur le chaos et les moments discrets orthogonaux, Ainsi nous avons introduit cinq algorithmes de chiffrements basé sur la théorie du chaos et opérants dans le domaine transformé de Tchebichef, Krawtchouk, Hahn, Dual Hahn et Racah respectivement. Plusieurs expérimentations ont été menées afin de prouver l'efficacité de ces algorithmes et une comparaison avec un schéma similaire utilisant la transformation DCT a prouvé la supériorité des nouveaux algorithmes proposés.

Le deuxième axe majeur de cette thèse consiste à améliorer le temps du calcul des algorithmes proposés. Dans un premier travail nous proposons un nouveau schéma de chiffrement partiel basé sur les moments de Tchebichef et la théorie du chaos. Ce schéma a démontré une amélioration importante de temps de calcul sans impacter la sécurité. Dans la même perspective d'améliorer le temps de calcul, nous avons proposé un ensemble d'algorithmes basés sur les moments séparables et le calcul parallèle utilisant le chaos, Le schéma proposé permet d'exécuter plusieurs étapes nécessaires au chiffrement au même temps, le résultat est un temps de calcul largement diminué et une sécurité supérieure.

Le présent mémoire s'étale sur six chapitres. Le deuxième chapitre expose la théorie du chaos et son application au chiffrement des images, dans un troisième chapitre nous présentons la théorie des moments vu qu'elle fait une partie intégrante de nos travaux. Dans le quatrième chapitre, une première partie, sera dédiée à la présentation d'un ensemble de nouveaux algorithmes de chiffrement basés sur la théorie du chaos et les moments orthogonaux. La deuxième partie du chapitre

trois présente notre travail intitulé chiffrement sélectif efficace des images basé sur le chaos et les moments de Tchebichef. Le cinquième chapitre sert à présenter un schéma de chiffrement chaotique rapide basé sur les moments séparables et le calcul parallèle. Finalement, on termine notre mémoire par une conclusion générale accompagnée des perspectives envisagées pour la continuité de nos travaux.

Chapitre 1

Chiffrement des images et théorie du Chaos

1.1 Introduction

Avec la prolifération d'Internet et la maturation de la technologie de traitement des signaux numériques, les applications de l'imagerie numérique sont répandues et continuent de se développer rapidement et en permanence aujourd'hui. Pourtant, le principal obstacle au déploiement généralisé des services d'image numérique a été de faire respecter la sécurité et de garantir un accès autorisé aux données sensibles. À cet égard, une solution directe consiste à utiliser un algorithme de chiffrement pour masquer les flux de données d'image, ce qui a conduit aux célèbres algorithmes de chiffrement basés sur la théorie des nombres, tels que le Data Encryption Standard (DES), l'International Data Encryption Algorithm (IDEA) et l'algorithme développé par Rivest, Shamir et Adleman (RSA) [127, 112, 199]. Cependant, ces schémas de chiffrement ne semblent pas être idéaux pour les applications d'image, en raison de certaines caractéristiques intrinsèques des images, telles que la capacité de données volumineuses et la redondance élevée, qui sont problématiques pour le chiffrement traditionnel. En outre, ces systèmes de chiffrement nécessitent des opérations supplémentaires sur les données d'image compressées, ce qui exige un temps de calcul long et une puissance de calcul élevée. Dans les communications en temps réel, en raison de leur faible vitesse de chiffrement et de déchiffrement, ils peuvent introduire une latence importante. Dans ce chapitre nous allons enumérer les particularités du chiffrement d'image par rapport au chiffrement du texte, puis nous allons présenter l'aspect théorique du chaos avant de montrer son application au chiffrement des images

1.2 Chiffrement des images

Par rapport au chiffrement de texte, que visent la plupart des normes de chiffrement existantes, le chiffrement d'images (ou plus généralement le chiffrement multimédia) possède ses propres caractéristiques et particularités, avec de nombreuses spécifications uniques. Afin de développer des techniques de chiffrement d'image efficaces, il faut les comprendre parfaitement. La section suivante présente quelques concepts de base en cryptographie concernant le chiffrement d'images.

1.2.1 Généralités sur le chiffrement

L'idée de base du chiffrement est de modifier le message de manière à ce que son contenu ne puisse être reconstruit que par un destinataire légal. Un cryptosystème

à valeurs discrètes peut être caractérisé par [183] :

- un ensemble de messages en clair possibles, P
- un ensemble de cryptogrammes possibles, C
- un ensemble de clés de chiffrement possibles, K
- ensemble de transformations de chiffrement et de déchiffrement possibles, E et D

Pour chaque clé, $k \in K$, il existe une fonction de chiffrement $e(k,.) \in E$ et une fonction de déchiffrement correspondante $d(k,.) \in D$, telles que pour chaque texte en clair $p \in P$, la condition de décodage unique, $d(k, e(k, p)) = p$ est satisfaite.
La sécurité d'un cryptosystème repose généralement sur la clé uniquement. En d'autres termes, on suppose que l'adversaire connaît la structure du système de chiffrement, possède l'algorithme de chiffrement et a accès au canal de transmission pour obtenir un segment arbitraire du texte chiffré c. Un bon cryptosystème permet toujours que cette situation se produise, et cette condition ou exigence est appelée principe de Kerckhoff [199].

Chiffrement par flux ou chiffrement par bloc

Les algorithmes de chiffrement, également appelés ciphers, peuvent être classés en fonction de leur structure. Il existe deux types de chiffrement : le chiffrement par flux et le chiffrement par blocs. Un algorithme de chiffrement par blocs est un type d'algorithme de chiffrement à clé symétrique qui transforme un bloc de données de texte en clair de longueur fixe en un bloc de données de texte chiffré de même longueur. La longueur fixe est appelée la taille du bloc. Pour de nombreux algorithmes de chiffrement par blocs, la taille du bloc est de 64 ou 128 bits. Plus la taille du bloc est grande, plus le chiffrement est sûr, mais plus les algorithmes et les dispositifs de chiffrement et de déchiffrement sont complexes. Les chiffrements par blocs typiques comprennent DES, Triple DES, Blowfish, IDEA et AES ; certains d'entre eux sont devenus récemment des normes de chiffrement.

Contrairement aux chiffrements par blocs, qui fonctionnent sur de grands blocs de données, les chiffrements par flux fonctionnent généralement sur de plus petites unités de texte en clair, généralement des bits. Ainsi, les chiffrement par flux peuvent être conçus pour être exceptionnellement rapides, beaucoup plus rapides qu'un chiffrement par bloc typique. En général, un chiffrement par flux génère une séquence de bits comme clé (appelée flux de clés), et le chiffrement est accompli en combinant le flux de clés avec le texte en clair. Habituellement, l'opération OU exclusif (XOR) par bit [149] est choisie pour effectuer le chiffrement, essentiellement pour sa simplicité. À l'heure actuelle, aucun chiffrement de flux n'est devenu une norme. Le chiffrement de flux le plus largement utilisé est RC4, tandis que RC5 a été incorporé dans certains produits majeurs tels que BSAFE, JSAFE et S/MAIL de RSA Data Security, Inc. [112]

Cryptanalyses

Un bon chiffrement doit avoir une forte capacité à résister à toutes sortes de cryptanalyse et d'attaques qui tentent de casser le système. Dans une certaine mesure, la résistance aux attaques est une bonne mesure de la performance d'un cryptosystème; elle est donc souvent utilisée pour évaluer les cryptosystèmes.

Selon la méthode d'accès de l'adversaire à des informations supplémentaires, les attaques contre un cryptosystème peuvent être classées en quatre catégories :

- *Attaque en texte chiffré uniquement* : L'adversaire a accès au canal de communication et peut écouter certaines parties du texte chiffré par une certaine clé. La tâche de l'adversaire est de révéler autant de texte en clair que possible, voire de pouvoir déduire la clé de chiffrement.
- *Attaque par connaissance du texte en clair* : En plus des segments de texte chiffré obtenus, l'adversaire connaît également un morceau de texte en clair associé. La tâche de l'adversaire est alors de déduire la clé de chiffrement.
- *Attaque par le texte en clair choisi* : L'adversaire n'a pas seulement accès à certains segments du texte chiffré et du texte en clair, mais il peut également choisir le texte en clair à chiffrer et obtenir ainsi un texte chiffré correspondant qu'il souhaite comparer. Ce type d'attaque est plus intensif que l'attaque par texte en clair connu.
- *Attaque par choix de texte chiffré* : L'adversaire peut choisir différents segments du texte chiffré et obtenir ainsi le texte en clair correspondant.

Outre les attaques typiques susmentionnées, il existe un type d'attaque appelé recherche exhaustive de la clé, qui essaie toutes les possibilités de la clé dans l'espace des clés pour déchiffrer complètement le message en clair. Si l'espace de clés d'un chiffrement est relativement petit, cette recherche exhaustive fonctionne assez bien, étant donné la disponibilité de la puissance de calcul actuelle.
Il convient de souligner que tout algorithme de chiffrement, qu'il soit traditionnel ou basé sur le chaos, doit obéir aux principes cryptographiques de base afin de pouvoir résister à des attaques sérieuses.

1.2.2 Particularités du chiffrement d'image

Contrairement aux messages textuels, les données d'image présentent des caractéristiques particulières telles qu'une capacité de masse, une redondance élevée et une forte corrélation entre les pixels, sans oublier qu'elles sont généralement de taille énorme, ce qui rend les méthodes de chiffrement traditionnelles difficiles à appliquer et lentes à traiter. Parfois, les applications d'image ont aussi leurs propres exigences, comme le traitement en temps réel, la réservation de la fidélité, la cohérence du format de l'image et la compression des données pour la transmission. La satisfaction simultanée de ces exigences, ainsi que les demandes de haute sécurité et de haute qualité, ont représenté de grands défis pour la pratique de l'imagerie en temps réel. Un exemple est le cas où l'on doit gérer à la fois le chiffrement et la compression. Ainsi, si une image doit être chiffrée après la conversion de son format, par exemple d'un fichier TIFF à un fichier GIF, le chiffrement doit être mis en œuvre avant la compression. Cependant, une image chiffrée classique est très peu compressible. D'autre part, la compression rendra impossible un déchiffrage correct et sans perte, en particulier lorsqu'un schéma de chiffrement d'image hautement sécurisé est utilisé. Ce conflit entre la compressibilité et la sécurité est très difficile, voire impossible, à résoudre complètement.

Les particularités du chiffrement des images peuvent être résumées comme suit :

1. Une redondance élevée et une grande capacité rendent généralement les données d'image chiffrées vulnérables aux attaques par cryptanalyse. Grâce à la

capacité de masse, l'adversaire peut obtenir suffisamment d'échantillons de texte chiffré (même à partir d'une seule image) pour effectuer une analyse statistique. En même temps, comme les données des images sont très redondantes, les pixels adjacents ont probablement des valeurs de niveaux de gris similaires, ou les blocs d'image ont des motifs similaires, qui intègrent généralement l'image avec certains motifs qui entraînent une fuite du secret.

2. Les données d'image ont de fortes corrélations entre les pixels adjacents, ce qui rend le brassage rapide des données assez difficile. L'analyse statistique d'un grand nombre d'images montre que 8 à 16 pixels adjacents sont en moyenne corrélés dans les directions horizontale, verticale et diagonale, tant pour les images naturelles que pour les images graphiques. Selon la théorie de l'information de Shannon [187], un cryptosystème sûr doit remplir une condition sur l'entropie de l'information, $E(P|C) = E(P)$, où P représente le message en clair et C le message chiffré ; c'est-à-dire que l'image chiffrée ne doit fournir aucune information sur l'image en clair. Pour satisfaire à cette exigence, l'image chiffrée doit donc être présentée de manière aussi aléatoire que possible. Étant donné qu'une source de message uniformément distribuée a une incertitude maximale [188], une image chiffrée idéale doit avoir un histogramme équilibré et deux pixels adjacents ne doivent pas être corrélés statistiquement. Cet objectif n'est pas facile à atteindre avec seulement quelques tours de permutation et de diffusion.

3. La capacité volumineuse des données d'image rend également difficile le chiffrement en temps réel. Par rapport aux textes, la capacité des données d'image est terriblement grande. Par exemple, une image courante en couleurs vraies de 24 bits, d'une hauteur de 512 pixels et d'une largeur de 512 pixels, occupe un espace de $512 \times 512 \times 24/8 = 768$ Ko. Ainsi, une image animée d'une seconde atteindra environ 19 Mo. Des contraintes de traitement en temps réel sont souvent requises pour les applications d'imagerie, telles que la vidéoconférence, la surveillance d'images, etc. Les grandes quantités de données d'image font peser une lourde charge sur les processus de codage et de décodage. Le chiffrement pendant ou après la phase de codage, et le déchiffrement pendant ou après la phase de décodage, aggraveront le problème. Si un algorithme de chiffrement s'exécute très lentement, même avec une sécurité élevée, il aurait peu d'intérêt pratique pour les applications d'imagerie en temps réel. C'est la raison pour laquelle les méthodes de chiffrement actuelles telles que DES, IDEA et RSA ne sont pas les meilleurs candidats pour cette considération.

4. Le chiffrement des images doit souvent être effectué en combinaison avec la compression des données. Dans presque tous les cas, les données sont compressées avant d'être stockées ou transmises en raison de l'énorme quantité de données d'image et de leur très forte redondance. Ainsi, l'intégration directe des exigences de sécurité dans le système de compression des données est une approche très intéressante. Le principal défi consiste à garantir une sécurité raisonnable tout en réduisant le coût de calcul sans dégrader les performances de compression sans dégrader les performances de compression.

5. Dans l'utilisation des images, la conversion des formats de fichiers est une opération fréquente. Il est souhaitable que le chiffrement des images n'affecte pas une telle opération. Ainsi, le fait de traiter directement les données d'image comme des données ordinaires pour le chiffrement rendra la conversion de

format de fichier impossible. Dans ce scénario, le chiffrement du contenu, où seules les données de l'image sont chiffrées, laissant l'en-tête du fichier et les informations de contrôle non chiffrées, est préférable.

6. La vision humaine présente une grande robustesse à la dégradation de l'image et au bruit. Seul le chiffrement des bits de données liés à l'intelligibilité peut permettre de protéger efficacement les images [227]. Cependant, la cryptographie conventionnelle traite tous les bits de données de l'image avec la même importance, et nécessite donc une puissance de calcul considérable pour les chiffrer tous, ce qui s'est souvent avéré inutile.

7. En termes de sécurité, les données d'image ne sont pas aussi sensibles que les informations textuelles. La sécurité des images est largement déterminée par la situation réelle d'une application. En général, la valeur des informations de l'image est relativement faible, sauf dans certaines situations spécifiques comme les applications militaires et d'espionnage ou la vidéoconférence dans les entreprises. Une attaque très coûteuse des données médianes es ne vaut généralement pas la peine. En pratique, de nombreuses applications d'image n'ont pas d'exigences très strictes en matière de sécurité. Dans certaines circonstances, la protection de la fidélité d'un objet image est plus importante que son caractère secret. Les signatures électroniques en sont un exemple. Autre exemple, dans les applications de bases de données d'images, seuls les utilisateurs qui ont payé pour ce service peuvent avoir accès à des images de grande taille et de haute résolution. Les adversaires peuvent être en mesure d'obtenir certaines images de petite taille et de faible résolution par des attaques basées sur la cryptanalyse, mais ces images ont peu de valeur commerciale et sont peut-être beaucoup moins chères que le coût de la préparation et de l'exécution des attaques. Dans le pire des cas, une éventuelle fuite partielle de certains secrets dans les médias, dans certaines limites, est toujours autorisée, tandis que pour les informations textuelles, ce scénario est largement interdit car il est alors assez facile de prédire le message entier sur la base des informations obtenues à partir d'une fuite partielle.

Aujourd'hui, il ne semble pas exister d'algorithme de chiffrement d'images capable de répondre à toutes les spécifications et exigences susmentionnées.

1.3 Théorie du chaos

1.3.1 Définition

Le mot Chaos vient du mot grec "Khaos", qui signifie "vide béant". Les mathématiciens disent qu'il est difficile de définir le chaos, mais qu'il est facile de le "reconnaître quand on le voit". En d'autres termes, le chaos désigne un état de confusion totale ou de prévisibilité dans le comportement d'un système naturel complexe. La théorie du chaos [51] est le concept selon lequel un petit changement aujourd'hui peut entraîner un très grand changement plus tard. Il s'agit d'un champ d'étude en mathématiques, avec des applications dans plusieurs disciplines, notamment la physique, l'ingénierie, l'économie, la biologie [152] et la philosophie, qui affirme principalement que de petites différences dans les conditions initiales (telles que celles dues à des erreurs d'arrondi dans le calcul numérique) peuvent produire des résultats très divergents pour les systèmes chaotiques, rendant la prédiction à long terme impossible en général.

La théorie du chaos est l'une des théories fondamentales de notre vie. Il s'agit de l'étude des systèmes dynamiques complexes et non linéaires. C'est une branche des mathématiques qui traite des systèmes qui semblent être ordonnés (déterministes) mais qui, en fait, ont des comportements chaotiques. Elle traite également des systèmes qui semblent être chaotiques, mais qui, en fait, ont un ordre sous-jacent. En d'autres termes, la nature déterministe [148] de ces systèmes ne les rend pas prévisibles. Ce comportement est connu sous le nom de chaos déterministe, ou simplement de chaos. La nature est extrêmement complexe, et la seule prédiction que l'on puisse faire est qu'elle est imprévisible. La théorie du chaos a réussi à capturer la beauté de l'imprévisible et à l'afficher dans les modèles les plus impressionnants. La nature, lorsqu'on la regarde avec les bons yeux, se présente comme l'une des œuvres d'art les plus fabuleuses qui soient. La théorie du chaos [138] repose sur l'axiome selon lequel la réalité elle-même subsiste dans un état d'anarchie ontologique.

1.3.2 Découverte du chaos

Le phénomène de la théorie du chaos a été introduit dans le monde moderne par Edward Lorenz en 1972 avec la conceptualisation de "l'effet papillon". Comprendre cette théorie permet de rendre un système complexe plus prévisible. Ainsi, lorsque vous travaillez avec un système, vous devez être conscient de toutes les entrées et les garder sous contrôle. La théorie du chaos ayant été élaborée grâce aux contributions de divers mathématiciens et scientifiques, ses applications se retrouvent dans un grand nombre de domaines scientifiques. Lorenz était un météorologue qui a développé un modèle mathématique utilisé pour modéliser la façon dont l'air se déplace dans l'atmosphère. Il a provoqué de grandes différences dans les résultats du modèle. Il a ainsi découvert le principe de la dépendance sensible aux conditions initiales (SDIC), qui est aujourd'hui considéré comme un élément clé de tout système chaotique. L'intérêt multidisciplinaire pour le chaos, la complexité et les systèmes auto-organisés a commencé dans les années 1970 avec l'invention des ordinateurs. Benoît Mandlebrot a trouvé la pièce du puzzle du chaos qui rassemble toutes les choses. Mandelbrot a publié un livre, The Fractal Geometry of Nature [51], qui examine la base mathématique de la formation de motifs dans la nature, un peu comme les travaux antérieurs de Turing. Ses fractales (la géométrie des dimensions fractionnaires) ont permis de décrire ou d'imaginer les actions du chaos, plutôt que de les expliquer. Le chaos et ses mécanismes peuvent désormais être visualisés en couleur sur un ordinateur.

Au début des années 1970, May travaillait sur un modèle qui traitait de la variation la natalité des insectes en fonction de l'approvisionnement en nourriture. Il a constaté qu'à certaines valeurs critiques, son équation nécessitait deux fois plus de temps pour revenir à son état initial - la période ayant doublé en valeur. Après plusieurs cycles de doublement de la période, son modèle est devenu imprévisible, un peu comme les populations réelles d'insectes ont tendance à être imprévisibles. Depuis la découverte de May sur les insectes, les mathématiciens ont découvert que ce doublement de la période est une voie naturelle vers le chaos pour de nombreux systèmes différents.

1.3.3 Systèmes chaotiques

Les systèmes chaotiques sont instables car ils ont tendance à ne pas résister aux perturbations extérieures mais à réagir de manière significative. En d'autres termes, ils

n'échappent pas aux influences extérieures mais sont en partie pilotés par elles. Ces systèmes sont déterministes car ils sont constitués d'un petit nombre d'équations différentielles simples et ne font aucune référence à des mécanismes aléatoires implicites. Un système déterministe est un système dans lequel aucun aléa n'intervient dans l'évolution des états futurs du système. Il est dit chaotique lorsque son évolution dépend des conditions initiales. Cette propriété implique que deux trajectoires émergeant de deux conditions initiales différentes proches. Cependant, ce n'est que dans les trente dernières années du vingtième siècle que des observations expérimentales l'ont mis en évidence. En fait, les systèmes chaotiques sont courants dans la nature. De nombreux phénomènes naturels peuvent également être caractérisés comme étant chaotiques. On les retrouve dans la météorologie, le système solaire, le cœur et le cerveau des organismes vivants, etc.
Les caractéristiques d'un système chaotique sont résumés comme suite :

i. Pas de comportement périodique.

ii. Sensibilité aux conditions initiales.

iii. Le mouvement chaotique est difficile ou impossible à prévoir.

iv. Le mouvement semble aléatoire.

v. Non linéaire.

En raison des différents facteurs impliqués dans les systèmes chaotiques, il est difficile de les prévoir. Ils nécessitent beaucoup de calculs compliqués et d'équations mathématiques. Les solutions des systèmes chaotiques peuvent être complexes et ne peuvent généralement pas être facilement extrapolées à partir des tendances actuelles. Le jeu de la roulette est un exemple intéressant qui pourrait illustrer la distinction entre les systèmes aléatoires et chaotiques. Si l'on étudie les statistiques des résultats de parties répétées, on constate que la séquence des chiffres est totalement aléatoire. Enfin, les systèmes chaotiques sont très sensibles à la condition initiale, ce qui signifie qu'un léger changement du point de départ peut entraîner des résultats extrêmement différents. Cela rend le système assez imprévisible.

1.3.4 Les caractéristiques de base du chaos

Le chaos est un phénomène omniprésent dans les systèmes déterministes non linéaires qui présentent une sensibilité extrême aux conditions initiales et des comportements de type aléatoire. Depuis sa découverte par Edward N. Lorenz en 1963 [139], la théorie du chaos est devenue une branche des études scientifiques actuelles [37]. Puisque les systèmes dynamiques chaotiques discrets (c'est-à-dire les cartes) sont utilisés en cryptographie, cette notion est brièvement présentée.

Définition du chaos discret

Il existe plusieurs définitions du chaos, qui se ressemblent mais ne sont en fait pas équivalentes [36]. Pour des raisons de brièveté, seule une définition simple est présentée ici.
Pour des raisons de simplicité, nous parlerons de cartes unidimensionnelles. Considérons un système dynamique discret sous la forme générale de

$$x_{k+1} = f(x_k), f : I \to I, x_0 \in I, \tag{1.1}$$

où f est une carte continue sur l'intervalle $I = [0, 1]$. Ce système est dit chaotique si les conditions suivantes sont satisfaites [50] :

i. Sensible aux conditions initiales :

$$\exists \delta > 0 \forall x_0 \in I, \epsilon > 0 \exists n \in N, y_0 \in I : |x_0 - y_0| < \epsilon \Rightarrow |f^n(x_0) - f^n(y_0)| > \delta \tag{1.2}$$

ii. Transitivité topologique :

$$\forall I_1, I_2 \subset I \exists x_0 \in I_1, n \in N : f^n(x_0) \in I_2 \tag{1.3}$$

iii. Densité des points périodiques dans I : Soit $P = p \in I | \exists n \in N : f^n(p) = p$ l'ensemble des points périodiques de f.
Alors P est dense dans $I : \bar{P} = I$.

Cette définition comporte quelques redondances, qui ne sont pas abordées ici.

La sensibilité du chaos aux conditions initiales est souvent illustrée par l'effet papillon, qui trouve son origine dans la formulation originale de Lorenz : "Le battement d'ailes d'un papillon au Brésil déclenche-t-il une tornade au Texas ?". Cette propriété de sensibilité est couramment utilisée pour les clés des cryptosystèmes.
La propriété de transitivité topologique assure l'ergodicité d'une carte chaotique, ce qui signifie que si nous divisons l'espace d'état en un nombre fini de régions, quel qu'en soit le nombre, toute orbite de la carte passera par toutes ces régions. Cette propriété est liée à la caractéristique de diffusion des cryptosystèmes.
En cryptologie chaotique, les deux propriétés ci-dessus sont souvent utilisées pour construire des chiffrages à flux et des chiffrages par blocs. Une comparaison plus approfondie est donnée dans la section suivante.

Relations entre le chaos et la cryptographie

Les relations entre les systèmes chaotiques et les cryptosystèmes ont fait l'objet de nombreuses discussions dans la littérature [46, 107, 107, 111, 182]. Comme mentionné ci-dessus, la principale différence entre la théorie du chaos et la cryptographie est que les cryptosystèmes fonctionnent sur un champ fini, alors que le chaos n'a de sens que sur un continuum. Néanmoins, ces deux notions scientifiques sont très étroitement liées. De nombreux concepts fondamentaux de la théorie du chaos, tels que le mélange et la sensibilité aux conditions initiales et aux paramètres, coïncident en fait avec ceux de la cryptographie.
L'extrait suivant du chef d'oeuvre de Shannon [187] démontre que les algorithmes cryptographiques ont inconsciemment utilisé la propriété de mélange du chaos, même avant l'aube de la recherche sur le chaos [69, 70, 107] :
Les bonnes transformations de mélange sont souvent formées par les produits répétés de deux opérations simples non commutatives. Hopf a montré, par exemple, que la pâte à pâtisserie peut être mélangée par une telle séquence d'opérations. La pâte est d'abord étalée en une fine plaque, puis repliée, puis étalée, puis repliée, etc.... Dans une bonne transformation de mélange . . . les fonctions sont compliquées, impliquant toutes les variables de manière sensible. Une petite variation de n'importe quelle (variable) change (la sortie) considérablement.
Les similitudes et les différences entre ces deux sujets peuvent être énumérées [107], comme le montre le tableau 1.1. Les cartes chaotiques et les algorithmes cryptographiques ont des propriétés similaires : tous deux sont sensibles à d'infimes changements dans

TABLE 1.1: Similitudes et différences entre le chaos et la cryptographie

Systèmes chaotiques	Algorithmes cryptographiques
Espace de phase : ensemble des nombres réels	Espace de phase : ensemble fini d'entiers
Itérations	Rounds
Paramètres	Clé
Sensibilité aux conditions initiales et aux paramètres	Diffusion

les conditions initiales et les paramètres ; tous deux ont des comportements semblables à ceux du hasard ; et les algorithmes cryptographiques brassent et diffusent les données par des cycles de chiffrement, alors que les cartes chaotiques diffusent une petite région de données sur l'ensemble de l'espace de phase par des itérations. La seule différence, à cet égard, est que les opérations de chiffrement sont définies sur des d'entiers finis, tandis que le chaos est défini sur des nombres réels.

Le chaos pour la cryptographie

Il est naturel d'appliquer la théorie du chaos discret à la cryptographie pour les raisons suivantes [111] :

- La propriété de dépendance sensible des orbites aux conditions initiales rend la nature du chiffrement très compliquée. Supposons que l'on ait le schéma de chiffrement suivant basé sur le chaos : Pour un texte en clair P dans (0, 1), certains paramètres d'une carte chaotique sont utilisés comme clé pour le chiffrement. Choisissez un système dynamique chaotique unidimensionnel (I, ϕ) pour effectuer le chiffrement. Ensuite, la procédure de chiffrement est l'itération n fois de la carte ϕ avec la valeur initiale P, et le texte chiffré C est le résultat du chiffrement : $C = \phi^n(P) = (\phi(\phi(...\phi(P))))$ Puisque la carte est chaotique, elle a un exposant de Lyapunov positif, c'est-à-dire qu'à un certain point $x \in I, \lambda_x > 0$; donc,

$$\begin{aligned} \forall \epsilon > 0 \exists n_1, n_2 \exists U_{n_1,n_2} \ni x, \forall n_1 \leq n \leq n_2, \forall z_1, z_2 \in U_{n_1,n_2} e^{(\lambda_x - \epsilon)n} |z_1 - z_2| \\ < |\phi^n(z_1) - \phi^n(z_2)| < e^{(\lambda_x + \epsilon)n} |z_1 - z_2| \end{aligned} \tag{1.4}$$

  où $U_{n1,n2}$ est un voisinage de x dans I. L'expression ci-dessus implique que, après n itérations, la distance initiale $|z_1 - z_2|$ entre deux points arbitrairement proches mais distincts z1 et z2 augmentera exponentiellement comme $e^{\lambda_x n}|z_1 - z_2|$. Cela signifie que si l'on utilise k1 comme clé de chiffrement mais que l'adversaire utilise k2 pour déchiffrer le message, alors même avec $|k1 - k2| < \epsilon$, la différence | z1 - z2 | sera significativement énorme. Cela empêche le système de toute attaque par force brute.

- Une mesure de Lebesgue μ est dite invariante si et seulement si elle satisfait à la condition suivante

$$\forall A \in \sigma(X), \mu(A) = \mu(\phi(A)) \tag{1.5}$$

  où $\sigma(X)$ est la σ-algèbre de tous les sous-ensembles mesurables dans X. Ici, (X, ϕ) est appelé ergodique si et seulement s'il n'a que des ensembles invariants triviaux, c'est-à-dire que $\phi(B) \subseteq B$ implique soit $\mu(B) = 0$ soit $\mu(B) =$

$\mu(X)$. L'ergodicité implique que l'espace d'état ne peut pas être divisé de manière non triviale en plusieurs sous-espaces. Ainsi, si une orbite part d'un point arbitraire x, elle ne sera jamais limitée à une petite région. Cette propriété indique que si une carte chaotique est utilisée pour composer le chiffrement, l'espace du texte en clair ne sera pas restreint à un petit sous-espace. Ainsi, pour un texte chiffré C, pour rechercher le texte en clair P correspondant, il faut passer par la carte chaotique. correspondant P, il faut parcourir tout l'espace d'état X.

- Le système susmentionné est mixte si la condition suivante est satisfaite (on suppose que $\mu(X) = 1$) :

$$\lim_{n\to\infty} \frac{\mu(\phi^n(B) \bigcap A)}{\mu(A)} = \frac{\mu(B)}{\mu(X)} \tag{1.6}$$

  Cette propriété implique qu'après n itérations, une partie de B sera contenue dans A, et le pourcentage de B qui est contenu dans A est asymptotiquement proportionnel au pourcentage de B dans X par rapport à la mesure μ. Ainsi, le texte en clair P est complètement contenu dans son texte chiffré C si une carte chaotique est utilisée pour le chiffrement.

Les propriétés du chaos décrites ci-dessus sont les fondements de la cryptographie chaotique. Pour concevoir des algorithmes cryptographiques sûrs, tant pour les blocs, toutes ces propriétés doivent être bien utilisées.

1.4 Conclusion

Dans ce chapitre nous avons présenté une brève introduction au chiffrement généralement et au chiffrement des images plus particulièrement, nous avons cité quelques particularités des images qui incitent les chercheurs à trouver des nouvelles pistes de développement des algorithmes de chiffrement pour les images. Ensuite nous avons discuté la théorie du chaos et son application au chiffrement des images.

Chapitre 2

Théorie des moments

2.1 Généralités sur les moments

Au milieu du XXe siècle, le mathématicien américain Claude Elwood Shannon a publié son article intitulé A mathematical theory of communication [186], qui a marqué la création de la théorie de l'information. Contribution historique, la théorie de l'information est le fondement théorique du stockage, du traitement et de la transmission de l'information dans les systèmes informatiques modernes. D'autre part, elle impose également que le signal brut (c'est-à-dire les données numériques) du multimédia (par exemple, l'image) n'est pas sémantique par nature. Par conséquent, l'une des principales exigences dans de nombreuses applications de vision par ordinateur et de reconnaissance des formes est d'avoir une "représentation significative" dans laquelle les caractéristiques sémantiques de l'image numérique sont facilement apparentes. Ce processus est souvent appelé représentation d'image. Par exemple, pour la reconnaissance, la représentation doit mettre en évidence les éléments sémantiques les plus saillants ; pour le débruitage, elle doit distinguer efficacement le signal (sémantiquement pertinent) du bruit (sémantiquement non pertinent) ; et pour la compression, elle doit capturer le plus d'informations sémantiques en utilisant le moins de coefficients possible.

2.1.1 Représentation des caractéristiques

D'un point de vue mathématique, l'idée de base de la représentation d'images consiste à projeter la fonction de l'image originale sur un espace formé par un ensemble de fonctions de base spécialement conçues et à obtenir le vecteur caractéristique correspondant. Depuis de nombreuses années, la conception de dictionnaires (c'est-à-dire l'ensemble des fonctions de base) a été étudiée par de nombreux chercheurs selon deux voies différentes : l'apprentissage manuel et l'apprentissage profond [268].

Récemment, les techniques d'apprentissage profond, représentées par les réseaux de neurones convolutifs (CNN), ont permis d'obtenir de très bonnes performances sur une variété de problèmes de vision par ordinateur et de reconnaissance des formes. Les représentations d'images basées sur l'apprentissage profond sont formées par la composition de multiples transformations non linéaires, qui transforment directement les données d'image brutes en représentations sémantiques abstraites sans intervention manuelle (c'est-à-dire le paradigme de bout en bout). Pour ces méthodes d'apprentissage de représentation, le dictionnaire peut être considéré comme une fonction composite et est formé/appris par erreur de rétro-propagation. Les représentations d'images basées sur l'apprentissage profond offrent une grande flexibilité et la capacité de s'adapter à des données de signal spécifiques. En raison de leur nature axée sur les données, ces approches sont fortement influencées par les

dernières avancées en matière d'algorithmes d'optimisation, de matériel informatique et de données d'apprentissage. Par conséquent, les approches d'apprentissage profond présentent des limites dans les trois aspects suivants [73] :

i. La qualité de la représentation dépend fortement de l'exhaustivité des données d'entraînement, c'est-à-dire qu'un ensemble d'entraînement important et diversifié est nécessaire.

ii. Le coût temps/espace de ces approches est souvent très élevé, ce qui les empêche d'être utilisées dans des applications où le temps est critique.

iii. La robustesse à la transformation géométrique est limitée, ce qui nécessite l'augmentation des données pour améliorer l'invariance géométrique, mais au prix d'une complexité temps/espace.

En revanche, les représentations d'images créées à la main sont encore compétitives dans les trois aspects ci-dessus. Il convient également de mentionner que les expériences réussies derrière les caractéristiques créées à la main sont instructives pour la conception de méthodes d'apprentissage profond telles que le réseau d'analyse en composantes principales (PCANet) [30] et la mise en commun de pyramides spatiales (SPP) [79].

Avant l'ère des réseaux neuronaux, les représentations artisanales et l'ingénierie des caractéristiques ont apporté d'importantes contributions au développement de la vision par ordinateur et de la reconnaissance des formes. À l'heure actuelle, les caractéristiques créées à la main ne peuvent toujours pas être complètement remplacées, étant donné que certaines limitations du deep learning ne sont que les caractéristiques des représentations créées à la main [9]. Les méthodes existantes de représentation d'images créées à la main peuvent être divisées en quatre catégories [151] :

- *Transformations de fréquence* - telles que la transformation de Fourier, la transformation de Walsh-Hadamard et la transformation en ondelettes ;

- *Texture* - comme la transformation de caractéristiques invariantes à l'échelle (SIFT), l'histogramme de localisation et d'orientation du gradient (GLOH) et les motifs binaires locaux (LBP). (GLOH) et les motifs binaires locaux (LBP) ;

- *Réduction de la dimensionnalité* - comme l'analyse en composantes principales (ACP), la décomposition en valeurs singulières (DVS) et l'incorporation localement linéaire (LLE) ;

- *Moments et invariants de moment* - tels que les moments de Zernike (ZM), les moments de Legendre et les transformations harmoniques polaires (PHT).

En partant de la nature sémantique de la tâche de représentation, il est clair que la représentation des images doit satisfaire les conditions de base suivantes [66] :

– Discriminabilité - la représentation reflète les variations entre les classes, c'est-à-dire que deux objets de deux classes différentes ont des caractéristiques différentes.

– Robustesse - la représentation n'est pas influencée par les variations intra-classes, c'est-à-dire que deux objets d'une même classe ont les mêmes caractéristiques.

Les représentations artisanales basées sur la transformation de fréquence, la texture et la réduction de la dimensionnalité ont été largement utilisées dans les applications du monde réel. Cependant, en raison de l'écart sémantique inhérent entre

les descripteurs de bas niveau et les concepts visuels de haut niveau, ces méthodes présentent des défauts au niveau de la robustesse et de la discrimination, voire des deux. Par exemple, les caractéristiques SIFT présentent de la synonymie et de la polysémie [257], ce qui entraîne une discrimination et une robustesse médiocres. En revanche, les moments et les invariants de moment permettent de mieux combler le fossé sémantique grâce à leurs propriétés mathématiques avantageuses :

– Indépendance - l'orthogonalité des fonctions de base garantit l'absence de redondance de l'information dans l'ensemble des moments, ce qui permet une meilleure discrimination dans la représentation des images.

– Invariance géométrique - les invariants par rapport aux transformations géométriques (rotation, mise à l'échelle, translation et retournement) peuvent être dérivés de l'ensemble des moments, ce qui signifie une meilleure robustesse dans la représentation des images.

2.1.2 Apperçu mathématique des moments

Mathématiquement, le moment de l'image est généralement défini comme le produit interne $< f, V_{nm} >$ de la fonction image f et de la fonction de base V_{nm} d'ordre $(n+m)$ sur le domaine D [66] :

$$< f, V_{nm} >= \iint_V V^*_{nm}(x,y) f(x,y) dxdy \tag{2.1}$$

où l'astérisque * désigne le conjugué complexe. L'interprétation géométrique directe de l'ensemble des moments de l'image $< f, V_{nm} >$ est qu'il s'agit de la projection de f sur un sous-espace formé par un ensemble de fonctions de base $V_{nm} : (n, m \in \mathbb{Z}^2)$ [80]. Comme il existe un nombre infini d'ensembles de fonctions de base, il est souvent nécessaire de concevoir manuellement un ensemble de fonctions de base spéciales V_{nm}ayant des propriétés bénéfiques en $< f, V_{nm} >$qui répondent aux exigences sémantiques. Selon les propriétés mathématiques des fonctions de base, la famille des moments d'image peut être divisée en différentes catégories, comme le montre la figure 2.1.

Tout d'abord, selon que les fonctions de base satisfont ou non à l'orthogonalité, les moments de l'image peuvent être classés en moments orthogonaux et moments non orthogonaux. L'orthogonalité signifie que deux fonctions de base différentes V_{nm} et $V_{n'm'}$de l'ensemble des fonctions de base ne sont pas corrélées ou sont "perpendiculaires" en termes géométriques, ce qui entraîne l'absence de redondance dans l'ensemble des moments. Mathématiquement, V_{nm} et $V_{n'm'}$ sont orthogonales lorsque la condition suivante est satisfaite.

$$< V_{nm}, V_{n'm'} >= \iint_D V_{nm}(x,y) V^*_{n'm'}(x,y) dxdy = \delta_{nn'}\delta_{mm'} \tag{2.2}$$

où δ_{ij}est la fonction delta de Kronecker définie comme suit :

$$\delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases} \tag{2.3}$$

Les moments non orthogonaux les plus populaires sont les moments géométriques [66], les moments de rotation [205], les moments complexes [1] et le descripteur de Fourier générique [258]. En raison de la non-orthogonalité des fonctions de

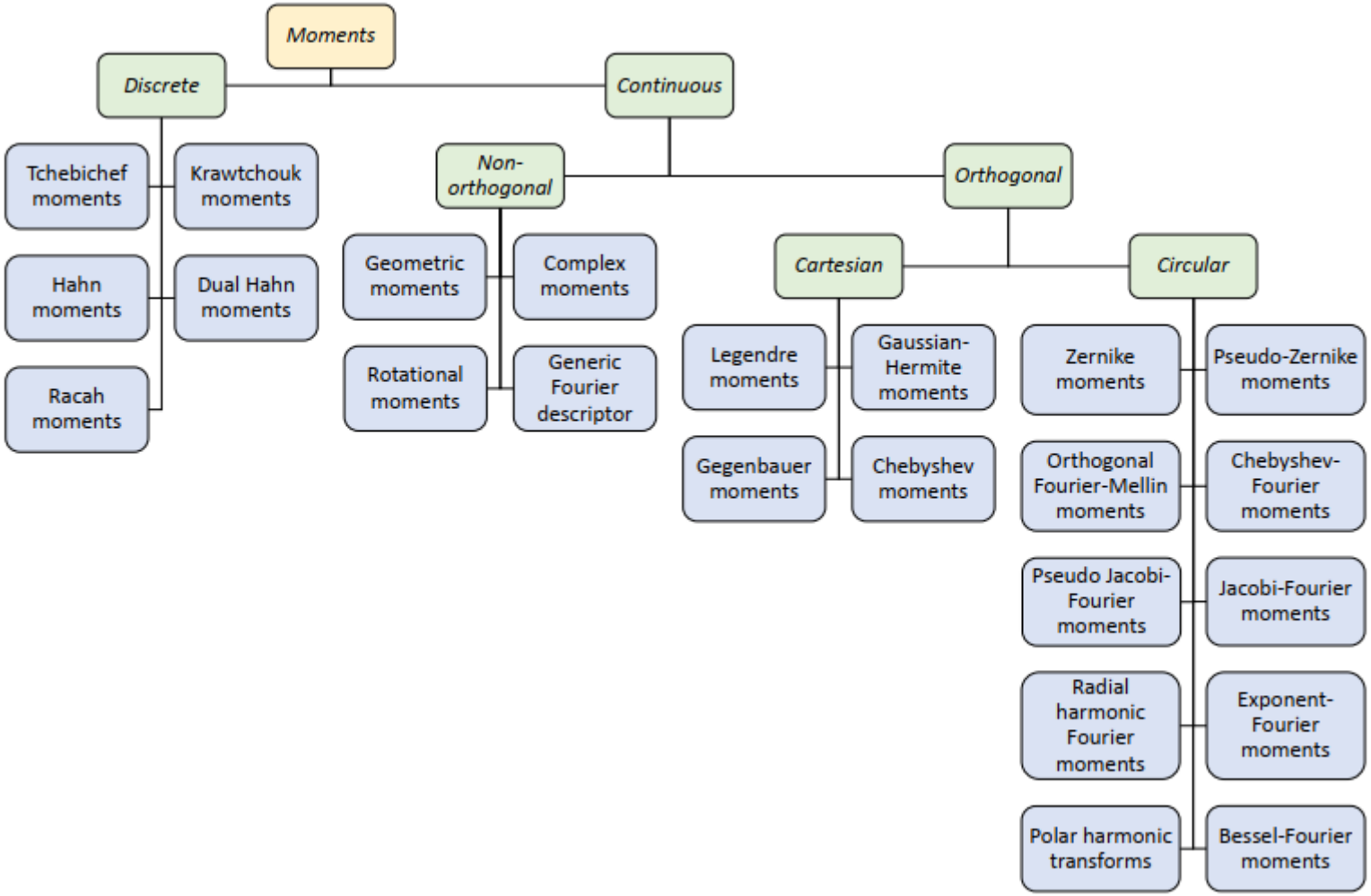


FIGURE 2.1: Une classification des moments de l'image

base, il existe une forte redondance de l'information dans ces moments. Cela entraîne des difficultés dans la reconstruction de l'image et une mauvaise discrimination/robustesse dans la représentation de l'image. Par conséquent, il est naturel de satisfaire à l'orthogonalité lors de la conception des fonctions de base.

Deuxièmement, selon que la fonction de base est continue ou non, les moments de l'image peuvent être divisés en moments continus et moments discrets. Dans le cas d'images bidimensionnelles $(2D)$, les fonctions de base des moments continus et discrets sont généralement définies dans l'espace à valeurs réelles $2D$ et l'espace d'image numérique $2D$, c'est-à-dire les domaines $D \in \mathbb{R}^2$ et $D \in \mathbb{Z}^2$, respectivement. Lorsqu'il est nécessaire de calculer les moments continus d'une image numérique, une approximation de discrétisation appropriée de l'intégrale continue est souvent introduite avec les erreurs de calcul correspondantes. Au contraire, les moments discrets, tels que les moments de Tchebichef [155], les moments de Krawtchouk [250], les moments de Hahn [251], les moments de Hahn doubles [272] et les moments de Racah [272], ne comportent aucune erreur d'approximation. Ils sont donc plus adaptés aux tâches de traitement d'images de haute précision, par exemple, la reconstruction, la compression et le débruitage d'images.

Enfin, en fonction du système de coordonnées qui définit les fonctions de base, les moments de l'image peuvent être regroupés en moments cartésiens et moments circulaires. Dans le cas des moments continus, les fonctions de base des moments cartésiens sont définies dans $D = (x, y) : x \in (-\infty, +\infty), y \in (-\infty, +\infty)$ou $D = (x, y) : x \in [-1, 1], y \in [-1, 1]$tandis que le domaine pour les moments circulaires est $D = (r, \theta) : r \in [0, +\infty), \theta \in [0, 2\pi)$ ou $D = (r, \theta) : r \in [0, 1], \theta \in [0, 2\pi)$ (i. e., le disque unitaire). Selon la preuve de Bhatia et al. [18], la fonction de base V_{nm} sera invariante en forme par rapport aux rotations d'axes autour de l'origine $(x, y) = (0, 0)$ si et seulement si, exprimée en coordonnées polaires (r, θ), elle est de la forme

$$V_{nm}(rcos\theta, rsin\theta) \equiv V_{nm}(r, \theta) = R_n(r)A_m(\theta), \tag{2.4}$$

avec une fonction de base angulaire $A_m(\theta) = exp(jm\theta)(j = \sqrt{-1})$ et la fonction de base radiale $R_n(r)$ pourrait être de forme quelconque [80]. Soit f^{rot}la version tournée de l'image originale f. Lorsque V_{nm}est conforme à la forme de l'équation (4), il doit exister une fonction I telle que

$$I(< f, V_{nm} >) \equiv I(< f^{rot}, V_{nm} >) \tag{2.5}$$

C'est-à-dire satisfaisant l'invariance de rotation. Par conséquent, les moments cartésiens, tels que les moments de Legendre [203], les moments de Gaussian-Hermite [191], les moments de Gegenbauer [84], les moments de Chebyshev [271], et les moments discrets énumérés ci-dessus, ont des difficultés à obtenir l'invariance de rotation. Comme pour le calcul des moments circulaires, une transformation de coordonnées appropriée est souvent introduite puisque les images numériques sont généralement définies dans un système de coordonnées cartésiennes avec les erreurs de calcul correspondantes.

2.1.3 Applications des moments

Outre les travaux théoriques décrits ci-dessus, la recherche sur les applications des moments orthogonaux est également active. Ces applications couvrent de nombreux problèmes familiers du traitement d'images, de la vision par ordinateur et de la sécurité de l'information, ainsi que certaines frontières interdisciplinaires. Dans cette section, compte tenu de l'objectif de cette étude, nous visons à donner une intuition

de haut niveau des applications des moments d'image sans entrer dans les détails techniques:

– Traitement d'images - Pour les tâches de vision de bas niveau, les moments d'image sont des choix populaires. L'application implique différents contenus du traitement de l'image : détection et représentation des caractéristiques de bas niveau (par exemple, détection des bords [255] et des points clés [95], représentation de la région d'intérêt [39], de la texture [52] et du flux optique [181]), restauration et représentation des images dégradées (par exemple, débruitage [114], désembrouillage [113] et superrésolution [71]), enregistrement des images [249], compression, codage et communication des images [236] et évaluation de la qualité des images [126]. De même, les moments ont également été utilisés pour les tâches de vision de bas niveau dans l'analyse vidéo [132] et l'infographie [20].

– Compréhension visuelle - Pour les tâches de vision de haut niveau, les moments de l'image ont été explorés dans différentes applications de la vision par ordinateur. On trouve des travaux connexes dans la classification d'images [156], la recherche d'instances [168], la détection d'objets [266] et la segmentation sémantique [215]. Une autre catégorie importante d'applications est la reconnaissance de formes, y compris la reconnaissance de comportements [94], la reconnaissance de textes [210], la reconnaissance biométrique [136] et la reconnaissance de sentiments [116].

– Sécurité de l'information - Les moments et les invariants de moment ont montré un impact significatif sur la recherche de la sécurité de l'information, en particulier pour les médias visuels. Cette popularité doit être attribuée à la robustesse de la représentation basée sur les moments, ce qui est cohérent avec la nature à deux acteurs de la recherche sur la sécurité. Les applications réussies comprennent principalement le filigrane numérique [207], la stéganographie [265], le hachage perceptuel [267] et la criminalistique passive des médias (par exemple, la détection des mouvements de copie [45] et des collages [34]).

– Interdisciplinaire - Le traitement et la compréhension de l'information visuelle étant des tâches communes à de nombreuses disciplines, la représentation basée sur les moments peut naturellement être étendue à ces domaines. Les applications interdisciplinaires typiques couvrent la médecine (par exemple, l'imagerie médicale [47]), la géographie (par exemple, la télédétection [48]), la robotique (par exemple, l'asservissement visuel [31]), la physique (par exemple, l'optique [26] et la mécanique des fluides [108]), la chimie (par exemple, la chimie analytique [26]), la biologie (par exemple, la représentation de la structure des protéines [197]) et la science des matériaux (par exemple, la représentation de l'environnement atomique [208]).

2.2 Orientations de recherche et avancées récentes

Outre la définition de nouveaux moments d'image, les travaux existants se concentrent principalement sur l'optimisation des moments classiques énumérés précédemment. Comme le montre la figure 2.2, les directions de recherche actuelles comprennent généralement : le calcul précis, le calcul rapide, l'optimisation de la robustesse/invariance. Cette section présente les directions ci-dessus ainsi que les avancées récentes.

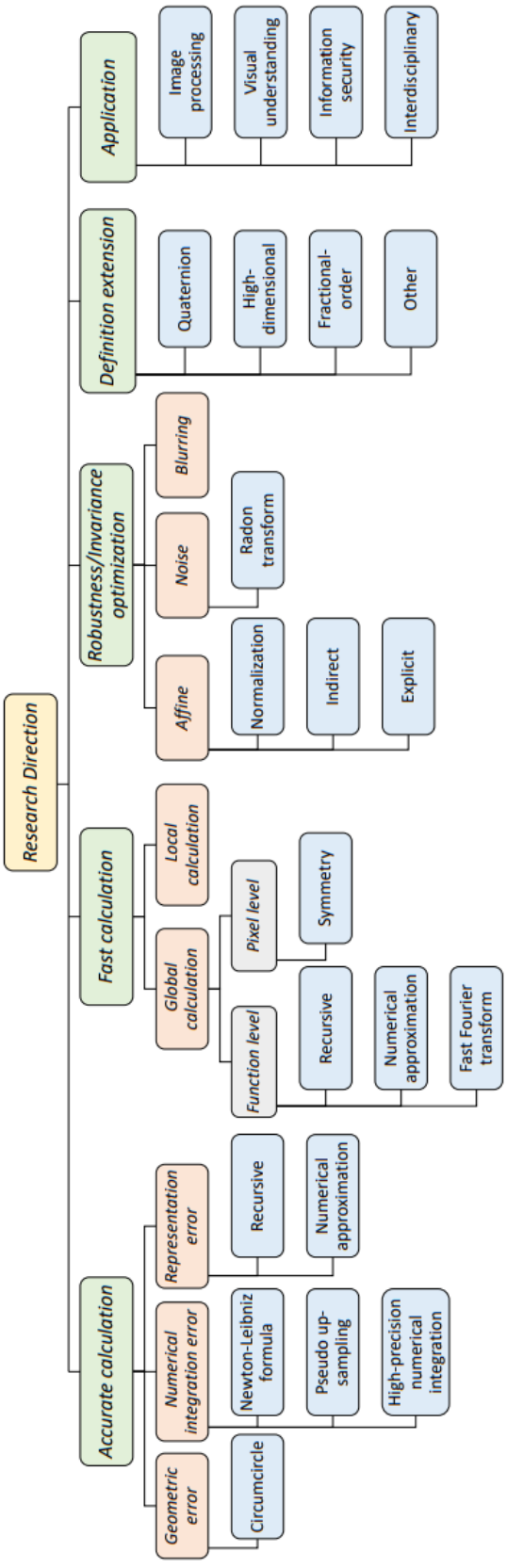


FIGURE 2.2: Les directions de recherche des moments d'image

2.2.1 Calculs précis

La procédure générale de calcul des moments de l'image est d'abord présentée comme le contexte mathématique des sections 2.2.1 et 2.2.2. moments de l'image est d'abord donnée.
En revenant à l'équation 2.1, pour calculer les moments de l'image $< f, V_{nm} >$ d'une image numérique définie dans la grille cartésienne discrète $\{f(i,j) : (i,j) \in [1,2,...,N]^2\}$, il est d'abord nécessaire d'unifier les domaines de $f(i,j)$et $V_{nm}(x,y)$, c'est-à-dire, pour concevoir une correspondance entre les deux :

$$(i,j) \rightarrow (x_i, y_j) \tag{2.6}$$

où une région de pixels $[i - \frac{\Delta i}{2}, i + \frac{\Delta i}{2}] \times [j - \frac{\Delta i}{2}, j + \frac{\Delta j}{2}]$ centré sur (i,j) est représenté dans une région $[x_i - \frac{\Delta x_i}{2}, x_i + \frac{\Delta x_i}{2}] \times [y_j - \frac{\Delta y_j}{2}, y_j + \frac{\Delta y_j}{2}]$ centrée sur (x_i, y_j). Par la correspondance des coordonnées $(i,j) \rightarrow (x_i, y_j)$, L'équation 2.1 peut être écrite sous forme discrète comme suit :

$$< f, V_{nm} >= \sum_{(x_i,y_j) \in D} h_{nm}(x_i, y_j) f(i,j) \tag{2.7}$$

où $h_{nm}(x_i, y_j)$ est la valeur intégrale de la fonction de base V_{nm}sur la région de pixels cartographiée $[x_i - \frac{\Delta x_i}{2}, x_i + \frac{\Delta x_i}{2}] \times [y_j - \frac{\Delta y_j}{2}, y_j + \frac{\Delta y_j}{2}]$, définie comme suit :

$$h_{nm}(x_i, y_j) = \int_{x_i - \frac{\Delta x_i}{2}}^{x_i + \frac{\Delta x_i}{2}} \int_{[y_j - \frac{\Delta y_j}{2}}^{y_j + \frac{\Delta y_j}{2}} V_{nm} * (x,y) dx dy \tag{2.8}$$

En général, le calcul des moments orthogonaux souffre d'une erreur géométrique, d'une erreur d'intégration numérique et d'une erreur de représentation (principalement une instabilité numérique). Ces erreurs limitent fortement la qualité de la représentation de l'image, en particulier lorsque des moments d'ordre supérieur sont nécessaires pour mieux décrire l'image. Par conséquent, les stratégies de calcul précis des moments sont vitales pour l'applicabilité.

Erreur géométrique

Une erreur géométrique peut se produire lors du mappage du domaine de l'image dans le domaine de la fonction de base, c'est-à-dire l'équation 2.6. Ces erreurs sont courantes dans le calcul des moments orthogonaux basés sur le disque unitaire, car les images numériques sont généralement définies sur une région carrée dans le système de coordonnées cartésiennes, plutôt que sur le disque unitaire.

Quant au mappage entre la région carrée et le disque unitaire, il existe naturellement, comme le montre la figure 2.3, le mappage incirculaire [133] :

$$\begin{cases} i \rightarrow x_i = \frac{2i-N}{N} = i\Delta x_i - 1 \\ j \rightarrow y_j = \frac{2j-N}{N} = j\Delta y_j - 1 \end{cases} \tag{2.9}$$

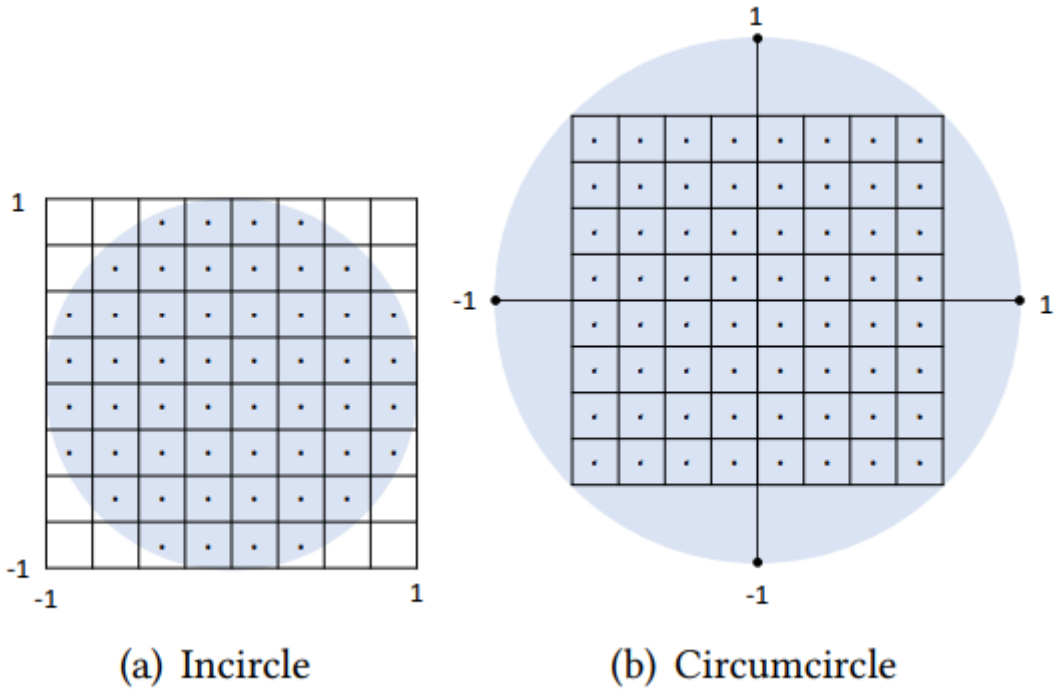


FIGURE 2.3: La mise en correspondance des coordonnées entre la région carrée de l'image numérique et le disque unitaire.

et la cartographie de la circonférence [41] :

$$\begin{cases} i \to x_i = \frac{2i-N}{\sqrt{2}N} = i\Delta x_i - \frac{\sqrt{2}}{2} \\ j \to y_j = \frac{2j-N}{\sqrt{2}N} = j\Delta y_j - \frac{\sqrt{2}}{2} \end{cases} \tag{2.10}$$

Lorsque la cartographie incirculaire est utilisée, il existe (i, j)tel que $(x_i, y_j) \notin D$, c'est-à-dire, les pixels cartographiés à l'extérieur du disque unitaire ne sont pas comptés, et il existe (i, j) tel que $[x_i - \frac{\Delta x_i}{2}, x_i + \frac{\Delta x_i}{2}] \times [y_j - \frac{\Delta y_j}{2}, y_j + \frac{\Delta y_j}{2}] - D \neq 0$, c'est-à-dire, certaines régions de pixels cartographiées coupent partiellement le disque unitaire. Dans les deux cas, des erreurs géométriques se produisent.
Quant à la cartographie du cercle circonscrit, elle est capable d'éviter complètement ces deux cas, de sorte qu'il n'y aura pas d'erreurs géométriques. Cependant, cela se fait au détriment de la capacité de représentation [209], car les régions cartographiées contenant des informations sur l'image n'occupent que $\frac{2}{\pi}$ du disque unitaire entier.

Erreur d'intégration numérique

Une erreur d'intégration numérique peut se produire lors du calcul de l'intégrale intégrale des fonctions de base continues, c'est-à-dire l'équation 2.8. Ici, pour les moments discrets, les fonctions de base V_{nm} sont généralement constantes sur l'intervalle $[x_i - \frac{\Delta x_i}{2}, x_i + \frac{\Delta x_i}{2}] \times [y_j - \frac{\Delta y_j}{2}, y_j + \frac{\Delta y_j}{2}]$. Ainsi , il est facile de vérifier que $h_{nm}(x_i, y_j) = V_{nm} * (x_i, y_j)\Delta x_i \Delta y_j$ ce qui signifie que les moments discrets n'impliquent pas d'erreurs d'intégration numérique [155]. Quant aux moments continus, puisque les fonctions

de base V_{nm} sont continues sur l'intervalle $[x_i - \frac{\Delta x_i}{2}, x_i + \frac{\Delta x_i}{2}] \times [y_j - \frac{\Delta y_j}{2}, y_j + \frac{\Delta y_j}{2}]$, la résolution de $h_{nm}(x_i, y_j)$ nécessite quelques astuces d'intégration.
Dans le cas le plus simple, il existe une solution analytique de $h_{nm}(x_i, y_j)$, c'est-à-dire que l'équation 2.8 peut être résolue directement par la formule de Newton-Leibniz [224, 196]. De tels calculs n'impliquent pas non plus d'erreurs d'intégration numérique.
Dans le cas plus général, compte tenu de la complication de la définition de nombreuses fonctions de base V_{nm}, il est souvent difficile de déterminer la solution analytique et certains algorithmes d'approximation sont nécessaires pour obtenir la solution numérique de $h_{nm}(x_i, y_j)$. L'algorithme d'approximation le plus couramment utilisé est l'approximation d'ordre zéro (ZOA) [133], qui imite le calcul des moments discrets, comme suit:

$$h_{nm}(x_i, y_j) \approx V_{nm} * (x_i, y_j)\Delta x_i \Delta y_j \tag{2.11}$$

En général, la précision de la méthode d'intégration numérique est inversement proportionnelle à la surface de l'intervalle $\Delta x_i \Delta y_j$. Par conséquent, en divisant davantage une région à pixel unique en plusieurs intervalles d'intégration plus petits (par exemple, des sous-intervalles 3×3), une précision plus élevée peut être facilement obtenue. Cette stratégie est souvent appelée pseudo-échantillonnage ascendant [217, 160]. Lorsque la ZOA est utilisée dans ces sous-intervalles, l'intégrale peut être exprimée comme suit

$$h_{nm}(x_i, y_j) \approx \sum_{(a,b)} V_{nm} * (u_a, v_b)\Delta u_a \Delta v_b \tag{2.12}$$

où (u_a, v_b)est le point d'échantillonnage avec $u_a \in [x_i - \frac{\Delta x_i}{2}, x_i + \frac{\Delta x_i}{2}]$et $v_b \in [y_j - \frac{\Delta y_j}{2}, y_j + \frac{\Delta y_j}{2}]$. Sur cette approche simple, d'autres stratégies d'intégration numérique de haute précision plus complexes [173, 194, 195], telles que la règle de quadrature gaussienne et la règle de Simpson, peuvent également être utilisées dans le calcul de l'équation 2.8. Leur définition générale est la suivante

$$h_{nm}(x_i, y_j) \approx \sum_{(a,b)} w_{ab} V_{nm} * (u_a, v_b)\Delta x_i \Delta y_j \tag{2.13}$$

où w_{ab} est le poids correspondant au point d'échantillonnage u_a, v_b
Il convient de noter que toutes les discussions ci-dessus reposent sur le système de coordonnées cartésiennes, que nous appelons méthode de calcul basée sur le système cartésien. En conséquence, il existe également une méthode de calcul basée sur le système de coordonnées polaires pour les moments orthogonaux basés sur le disque unitaire, souvent appelée "pavage de pixels polaires" [239, 86].

Il rééchantillonne d'abord l'image numérique $f(i, j)$en une grille polaire discrète (r_u, θ_{uv}), comme le montre la figure 2.4, puis effectue le calcul d'une manière similaire à l'équation 2.7 et à l'équation 2.8 :

$$< f, V_{nm} >= \sum_{r_u, \theta_{uv} \in D} h_{nm}(r_u, \theta_{uv}) f(r_u, \theta_{uv}), \tag{2.14}$$

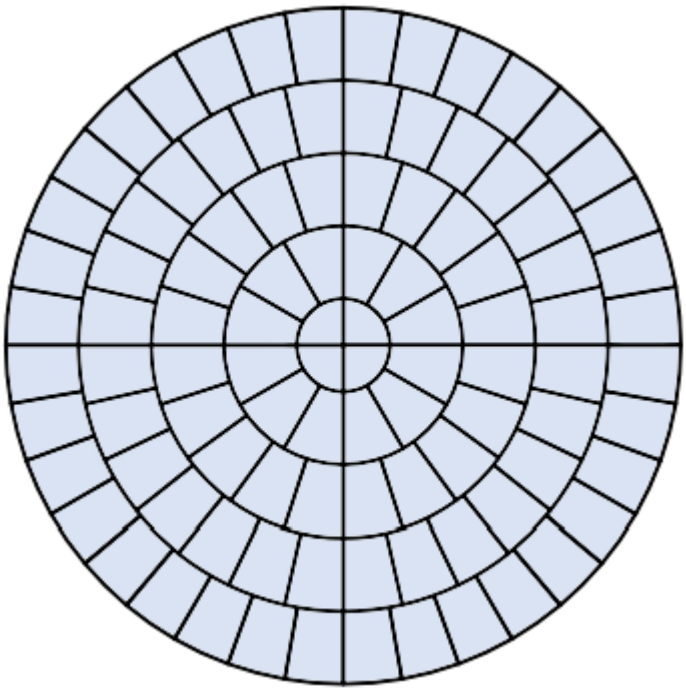


FIGURE 2.4: Le mappage des coordonnées dans le schéma de pavage en pixels polaires

avec

$$h_n m(r_u, \theta_{uv}) = \int_{r_u}^{r_{u+1}} \int_{\theta_{uv}}^{\theta_{u(v+1)}} V_{nm} * (r, \theta) r dr r d\theta = \int_{r_u}^{r_{u+1}} R_n(r) r dr \int_{\theta_{uv}}^{\theta_{u(v+1)}} exp(-jm\theta) d\theta \tag{2.15}$$

Notez que l'équation 2.15 présente un avantage distinct, à savoir que le calcul de $h_{nm}(r_u, \theta_{uv})$ peut être séparé en deux parties indépendantes [23] : 1)$\int_{r_u}^{r_{u+1}} R_n(r) r dr$ peut être intégré approximativement par pseudo-échantillonnage ascendant et règle de quadrature gaussienne ; 2) $\int_{\theta_{uv}}^{\theta_{u(v+1)}} exp(_j m\theta) d\theta$ peut être intégré exactement par la formule de Newton-Leibniz, comme suit :

$$\int_{\theta_{uv}}^{\theta_{u(v+1)}} exp(-jm\theta) d\theta = \begin{cases} \frac{j[exp(-jm\theta_{u(v+1)}) - exp(-jm\theta_{uv})]}{m} & m \neq 0 \\ \theta_{u(v+1)} - \theta_{uv} & m = 0 \end{cases} \tag{2.16}$$

En plus de l'avantage ci-dessus, le pavage de pixels polaires a des propriétés similaires à la méthode de calcul cartésienne en termes d'erreur géométrique et d'erreur d'intégration numérique, et ne sera pas répété ici.

Erreur de représentation

L'erreur de représentation est causée par la précision finie des systèmes de calcul numérique, qui se produit dans tous les processus de calcul, c'est-à-dire l'équation 2.6, l'équation 2.7 et l'équation 2.8. L'erreur de représentation peut être subdivisée en erreur de débordement, erreur de sous-débordement et erreur d'arrondi [209]. L'instabilité numérique courante est principalement attribuable à l'erreur d'arrondi et à l'erreur de débordement.
Les fonctions de base basées sur les polynômes de Jacobi contiennent des termes

factoriels/gamma. Lorsque l'ordre est grand, les valeurs réelles de ces coefficients peuvent dépasser la plage de représentation du système de calcul numérique, ce qui entraîne une erreur d'arrondi ou même une erreur de dépassement. Pour éviter le calcul direct des termes factoriels/gamma, des stratégies récursives [154, 52, 209] et des algorithmes d'approximation numérique [165, 166] sont souvent utilisés. La méthode récursive s'appuie sur la relation récursive des fonctions de base dérivées de $a! = a.(a-1)!$ et $\Gamma(a) = a.\Gamma(a-1)$, en utilisant plusieurs fonctions de base d'ordre inférieur pour dériver directement les fonctions d'ordre supérieur. Ce processus ne fait pas intervenir la factorielle/gamma du grand nombre. Dans une autre voie, la méthode d'approximation numérique permet d'obtenir des calculs sans factorielle en recourant à une approximation appropriée pour les factorielles, telle que la formule de Stirling
En plus des termes factoriels/gamma, les fonctions de base de certains moments orthogonaux ont des valeurs absolues très élevées (ou même infinies) en certains points, qui peuvent également dépasser la plage de représentation du système de calcul numérique. Par exemple, bien que les définitions de RHFM et EFM n'impliquent aucun terme factoriel/gamma, leurs fonctions de base sont infinies à l'origine, ce qui entraînera une erreur d'arrondi ou même une erreur de dépassement.

Progression récente du calcul précis

Dans le domaine du calcul précis des moments orthogonaux basés sur les disques unitaires, le pavage de pixels polaires de Xin et al [239] est peut-être le travail le plus influent et le plus représentatif. Les articles récents combinent généralement le pavage de pixels polaires avec d'autres techniques, notamment la cartographie par cercles circulaires, le pseudo-échantillonnage ascendant, l'intégration numérique de haute précision, la formule de Newton-Leibniz et la stratégie récursive, afin de fournir des performances de pointe.

De cette façon, Sáez-Landete [178] a intégré les travaux de Camacho-Bello et al. [23] et Upneja et al. [209], donnant un algorithme de calcul précis pour le JFM. Par conséquent, il s'applique également à d'autres moments basés sur des polynômes de Jacobi tels que l'OFMM et le CHFM. En raison du pavage polaire des pixels, les parties radiales compliquées peuvent être évaluées à l'aide d'une quadrature gaussienne, d'un pseudo-échantillonnage ascendant et d'une relation récursive, tandis que les parties angulaires peuvent être évaluées exactement par la formule de Newton-Leibniz. Une méthode quelque peu similaire a été proposée par Hosny et al. [85] pour la PHT basée sur la fonction harmonique. La principale différence est que, en raison de la définition simple de la fonction de base radiale, les parties radiales peuvent également être intégrées exactement par la formule de Newton-Leibniz, tout comme les parties angulaires.

Ces deux travaux récents fournissent une précision quasi parfaite pour le calcul des moments basés sur le polynôme de Jacobi et des moments basés sur la fonction harmonique, respectivement. Pour être critique, le seul défaut peut être l'erreur introduite dans le processus de rééchantillonnage de l'image sur une grille polaire discrète [239]. Si les méthodes d'interpolation non linéaires sont utilisées, comme la méthode bicubique, l'erreur d'interpolation est négligeable pour les tâches de représentation d'images. Par contre, si une tâche donnée est sensible à de telles

erreurs, d'autres outils mathématiques plus complexes, comme la méthode pseudo-polaire [7], sont instructifs pour la conception de calculs précis [247].

2.2.2 Calcul rapide

Dans la mise en œuvre des moments orthogonaux, la complexité globale peut devenir excessivement élevée lorsque 1) un grand nombre de moments est nécessaire, 2) l'image a une haute résolution, 3) de nombreuses images doivent être traitées, ou 4) un calcul de haute précision est requis. Comme ces exigences sont courantes dans les applications pratiques, le calcul rapide des moments orthogonaux est fortement demandé. En fonction du scénario d'application, les efforts d'optimisation de la vitesse de calcul peuvent être divisés en deux catégories : le calcul global et le calcul local.

Calcul global

Le calcul global consiste à calculer les moments de l'image pour l'ensemble de l'image. Dans ce scénario, le nombre de moments et la résolution de l'image sont les principaux facteurs qui affectent la complexité temporelle. En prenant comme exemple le calcul direct le plus simple basé sur la ZOA, le coût en temps d'un moment d'image d'ordre n provient de :

- Pour l'équation 2.8, il est nécessaire d'évaluer les valeurs de la fonction de base V_{nm} points d'échantillonnage $N \times N$, c'est-à-dire $\{V_{nm} * (x_i, y_j) : (i, j) \in [1, 2, ..., N]^2\}$ La complexité temporelle est liée à la définition des fonctions de base. Par exemple, les fonctions de base utilisant des polynômes de Jacobi nécessitent $O(nN^2)$ additions pour la sommation. En revanche, les fonctions de base utilisant des fonctions harmoniques ne nécessitent pas de telles additions.

- Pour l'équation 2.7, il est nécessaire de calculer le produit interne de la fonction de base V_{nm} et de l'image numérique $f$aux $N \times N$points d'échantillonnage, c'est-à-dire $< f(i, j), V_{nm} * (x_i, y_j)\theta x_i, \theta y_j >$. La complexité temporelle est de $O(N^2)$multiplications et $O(N^2)$additions.

Notez que les calculs énumérés ci-dessus ne sont nécessaires que pour un seul moment. Soit K une certaine constante entière, si tous les moments des ordres dans l'ensemble $\{(n, m) : |n|, |m| \leq K\}$ sont calculés, la complexité totale augmentera d'un facteur $O(K^2)$. De plus, le coût de calcul de l'équation 2.8 peut augmenter fortement si la stratégie d'intégration numérique de haute précision, telle que la quadrature gaussienne, est adoptée. Pour réduire la complexité des équations 2.7 et 2.8, les méthodes existantes sont conçues au niveau de la fonction et du pixel.

- Niveau de fonction : Pour les moments orthogonaux basés sur des polynômes de Jacobi, si la méthode récursive et l'approximation numérique sont utilisées pour évaluer les fonctions de base, le nombre d'additions (provenant de la sommation) et de multiplications (provenant de la factorielle) dans le calcul de l'équation 2.8 peut être réduit [23, 52, 209, 165, 166]. Par exemple, le calcul récursif du polynôme $R_n(\sqrt{x_i^2 + y_j^2})$nécessite $O(N^2)$additions, moins que les $O(nN^2)$ du calcul direct. Si K polynômes $R_n(\sqrt{x_i^2 + y_j^2})$ d'ordres $0, 1, ..., K$ sont nécessaires, la méthode directe implique $O(K^2N^2)$additions, tandis que

le schéma récursif ne nécessite que $O(KN^2)$ additions. Pour les moments orthogonaux basés sur les fonctions harmoniques, outre l'adoption de la forme récursive similaire [82, 193, 81], une stratégie plus efficace consiste à utiliser sa relation inhérente avec la transformée de Fourier [246, 44, 216]. Une fois que la relation explicite entre les deux est déterminée, l'algorithme de la transformée de Fourier rapide (FFT) peut être utilisé pour calculer les moments. Notez que la FFT permet de réduire le nombre de multiplications les plus longues de l'équation 2.7 de $O(N^2)$ à $O(NlogN)$.

- Niveau de pixel : La stratégie la plus courante dans cette voie consiste à simplifier le calcul en explorant la symétrie et l'antisymétrie des fonctions de base dans le domaine [93, 5]. Plus précisément, les valeurs des fonctions de base de tous les points d'échantillonnage $N \times N$peuvent être entièrement dérivées des valeurs des fonctions de base de quelques points d'échantillonnage spéciaux, ce qui réduit la complexité des équations 2.8 et 2.7. Dans la figure 2.5, nous donnons une illustration de points symétriques dans le disque unitaire. Pour un point P_1, il existe sept points symétriques $\{P_2, P_3, P_4, P_5, P_6, P_7, P_8\}$ par rapport aux axes de coordonnées, à l'origine et à $y = x$. Leurs coordonnées cartésiennes et leurs coordonnées polaires sont indiquées dans le tableau 2.1. On peut constater que tous ces points ont la même coordonnée radiale et la même coordonnée angulaire associée. Sur la base des propriétés mathématiques de la fonction exponentielle complexe, c'est-à-dire les identités trigonométriques, une telle corrélation des coordonnées sera directement convertie en corrélation des valeurs de la fonction de base. Cette observation peut donc conduire à une réduction de la complexité de calcul de l'équation 2.8 et de l'équation 2.7 d'environ 1/8. Si l'on considère que tous les moments orthogonaux basés sur le disque unitaire sont basés sur des fonctions de base angulaires utilisant des fonctions exponentielles complexes, les propriétés de symétrie et d'antisymétrie ci-dessus sont maintenues dans toutes ces méthodes. Par conséquent, cette stratégie de calcul rapide est générique et facile à utiliser en combinaison avec d'autres algorithmes rapides.

Calcul local

Le calcul local consiste à calculer les moments de l'image pour une partie de l'image, comme les blocs d'image denses ou les régions d'intérêt des points clés. l'image, comme les blocs d'image denses ou les régions d'intérêt des points clés. Dans ce scénario d'application, les résolutions de ces parcelles d'image sont généralement faibles et peuvent être décrites à l'aide de quelques moments. La principale raison de l'augmentation de la complexité temporelle est que le nombre de ces parcelles est généralement très élevé, par exemple, ce nombre pour les blocs denses peut être de l'ordre de 10^5 ou même 10^6 . Par conséquent, les méthodes d'optimisation de la vitesse pour le calcul global ne résolvent souvent pas bien le problème du calcul local. À l'heure actuelle, le problème du calcul des moments locaux de l'image n'a pas fait l'objet d'une discussion approfondie. La voie la plus prometteuse consiste à trouver et à comprimer les opérations redondantes dans le traitement en boucle de patchs d'images. À cet égard, des propriétés utiles des fonctions de base (comme les propriétés de décalage dans [33, 145]) et des structures de données spéciales (comme les images intégrales à valeurs complexes dans [17]) ont été explorées pour améliorer l'efficacité.

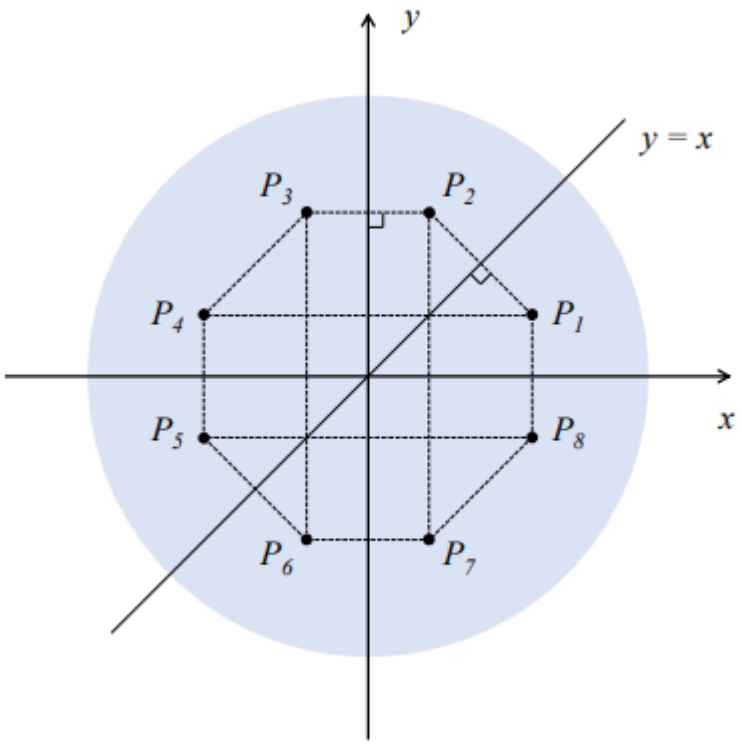


FIGURE 2.5: Illustrations de points symétriques dans le disque unitaire

TABLE 2.1: Coordonnées cartésiennes et coordonnées polaires des points symétriques

Point de symétrie	Axe de symétrie	Coordonnées cartésiennes	Coordonnées polaires
P1		(x, y)	(r, θ)
P2	$y = x$	(y, x)	$r, \frac{\pi}{2} - \theta$
P3	$y = x, y - axis$	$(-y, x)$	$r, \frac{\pi}{2} + \theta$
P4	$y - axis$	$(-x, y)$	$(r, \pi - \theta)$
P5	$origin$	$(-x, -y)$	$(r, \pi + \theta)$
P6	$origin, y = x$	$(-y, -x)$	$r, \frac{3\pi}{2} - \theta$
P7	$y = x, x - axis$	$(y, -x)$	$r, \frac{3\pi}{2} + \theta$
P8	$x - axis$	$(x, -y)$	$(r, 2\pi - \theta)$

Progrès récents du calcul rapide

Pour le calcul global rapide des moments orthogonaux basés sur le polynôme de Jacobi, les méthodes de pointe utilisent généralement la récursion et la symétrie en combinaison. les méthodes les plus récentes utilisent généralement la récursion et la symétrie en combinaison. Un travail récent de cette manière a été proposé par Upneja et al [209] pour JFM (voir aussi [23, 178]), il nécessite $O(\frac{1}{8}(KN^2 + K^2N^2))$ additions et $O(\frac{1}{8}K^2N^2)$ multiplications pour tous les moments d'ordres dans l'ensemble $\{(n,m) : |n|,|m| \leq K\}$. Considérant que la multiplication est généralement beaucoup plus coûteuse que l'addition dans les systèmes informatiques modernes, donc le temps total écoulé est principalement déterminé par les $O(\frac{1}{8}K^2N^2) = O(K^2N^2)$ multiplications. Dans ce cas, il est clair que lorsqu'une résolution d'image plus élevée (c'est-à-dire que N augmente) ou un plus grand nombre de moments (c'est-à-dire que K augmente) sont nécessaires, le coût de calcul augmente toujours de manière quadratique. Ceci est principalement dû à la complexité des polynômes de Jacobi, en d'autres termes, ce qui conduit à l'absence d'implémentation rapide avec une complexité inférieure au temps quadratique.

Pour le calcul global rapide des moments orthogonaux basés sur la fonction harmonique, les performances de l'état de l'art offertes par la mise en œuvre rapide basée sur la FFT. L'idée la plus ancienne en la matière remonte à 2014, lorsque Ping et al. [172] ont introduit la FFT par la relation entre l'EFM et la transformée de Fourier. Par la suite, des idées similaires ont été utilisées pour la RHFM [44] et la PCET [216]. Un travail important a été récemment proposé par Yang et al. [246], qui ont généralisé ces techniques basées sur la FFT à une version générique des moments orthogonaux basés sur la fonction harmonique. Cette implémentation rapide générique, similaire à ses formes spéciales précédentes, présente une complexité multiplicative de $O(M^2logM) = O(N^2logN)$, où M est un paramètre d'échantillonnage et $M\infty N$ Notez que, de manière surprenante, K ne joue aucun rôle dans la complexité multiplicative. Cette propriété signifie que lorsque K est légèrement plus élevé, de sorte que K^2 est supérieur à $logN$, le temps écoulé de cette méthode générique sera nettement inférieur à la stratégie basée sur la récursion et la symétrie telle que [246]. En plus du gain d'efficacité, il a également été prouvé (à la fois analytiquement et expérimentalement) que cette méthode évite l'instabilité numérique, tout en offrant une précision de calcul assez élevée lorsque M est grand.

Pour le calcul local rapide, les travaux récents de Bera et al. [17] apportent une contribution cruciale. Ils ont réduit le calcul ZM de blocs d'images denses à un temps constant, c'est-à-dire $O(1)$, en introduisant une structure de données élégante : l'image intégrale à valeurs complexes. D'autres améliorations de la vitesse peuvent être obtenues à l'aide d'une autre structure : la table de consultation. Bien que l'utilisation d'une image intégrale dans une mise en œuvre rapide ne soit pas rare (par exemple, SURF l'utilise pour accélérer SIFT [13]), c'est la toute première fois que de telles techniques sont utilisées pour des moments orthogonaux. Grâce à cette dérivation complexe, nous avons découvert que deux outils mathématiques jouaient un rôle important dans la réécriture de la définition de ZM vers les images intégrales, à savoir la représentation dans le plan complexe des coordonnées radiales et angulaires et l'expansion binomiale. Les structures et outils susmentionnés introduits par Bera et al. peuvent fournir des informations importantes aux chercheurs dans ce domaine. Malheureusement, comme l'expliquent les auteurs, cet algorithme rapide semble n'être applicable qu'au ZM et non à d'autres moments ayant un meilleur

pouvoir de représentation (c'est-à-dire sans suppression d'information), comme le OFMM. Si une mise en œuvre similaire en temps constant pouvait être développée pour tous les moments orthogonaux basés sur le disque unitaire, cela favoriserait grandement leur application dans les tâches en temps réel.

2.2.3 Robustesse/Invariance Optimisation

Comme un contexte mathématique de cette section, les définitions générales de l'invariance, de la robustesse et de la discriminabilité dans la représentation des images sont d'abord données.
S'il existe une fonction R telle que l'image originale f et sa version dégradée $D(f)$, où D est l'opérateur de dégradation, satisfassent:

$$R(f) \equiv R(D(f)), \tag{2.17}$$

pour tout f , la représentation R est dite invariante à la dégradation D.
Nous considérons la fonction $L : X \times X \to [0, +\infty)$ comme une mesure de distance sur un ensemble X, où pour tout $x, y, z \in X$ les trois axiomes suivants sont satisfaits :

- identité des indiscernables - $L(x, y) = 0 x = y$
- symétrie - $L(x, y) = L(y, x)$
- subadditivité ou inégalité triangulaire - $L(x, y) \leftrightarrow L(x, z) + L(z, y)$

Étant donné une fonction de distance L, la robustesse exige que la distance intra-classe de la représentation R :

$$L(R(f), R(D(f))), \tag{2.18}$$

devrait être suffisamment petit. Inversement, en supposant que l'image g est sémantiquement différente de l'image f , la discriminabilité exige que la distance interclasse de la représentation R :

$$L(R(f), R(g)), \tag{2.19}$$

doit être suffisamment grande. On peut voir que l'invariance implique la robustesse parfaite, c'est-à-dire que $L(R(f), R(D(f))) = 0$ tient si et seulement si l'équation 2.17 tient en raison du premier axiome de L. Ici, la représentation d'image basée sur le moment I est une forme spéciale de la représentation générique R, qui dépend de la fonction de base donnée V_{nm} et peut être écrite comme suit

$$R(f) = I(< f, V_{nm} >) \tag{2.20}$$

Il est presque impossible de concevoir une représentation qui conserve bien l'invariance ou la robustesse à tous les types de dégradations. Plus précisément, la seule possibilité correspond à une représentation sans aucune discriminabilité [66]. Ainsi, en pratique, la conception d'une représentation R repose généralement sur certaines hypothèses concernant la dégradation D. En général, les méthodes d'optimisation de l'invariance/robustesse sont proposées contre trois types d'attaques : la transformation affine, le bruit et le flou.

Transformation affine

Il s'agit d'une transformation des coordonnées de l'espace image, c'est-à-dire que l'opérateur de dégradation D est une mise en correspondance des coordonnées des pixels (x, y) avec les nouvelles coordonnées x', y', $D : (x, y) \rightarrow (x', y')$, est défini comme suit :

$$\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} & t_x \\ a_{10} & a_{11} & t_y \\ 0 & 0 & 1 \end{pmatrix} . \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \tag{2.21}$$

où les paramètres affines $(a_{00}, a_{01}, a_{10}, a_{11}, t_x, t_y)$ peuvent coder la rotation, la mise à l'échelle, la translation, le cisaillement, le retournement et toutes les combinaisons linéaires des transformations ci-dessus. Dans la représentation d'image basée sur les moments, il existe trois méthodes pour obtenir l'invariance à la transformation affine D : la normalisation, les méthodes indirectes et explicites [66, 64, 16].

- Méthode de normalisation [170, 190] : Dans cette approche, l'image d'entrée dégradée $D(f)$ est convertie en une certaine forme de référence f^{ref}, de sorte que la représentation de cette image normalisée, $R(f^{ref})$, sera invariante à la transformation affine D. Évidemment, l'invariance de cette approche provient de la technique de correction indépendante. Plus précisément, la normalisation peut être considérée comme une fonction N, qui doit tenir $N(D(f)) = N(f) = f^{ref}$ pour toute image f et toute transformation affine admissible D. Notez que la transformation géométrique n'a pas besoin d'être réellement mise en œuvre sur l'image numérique, ce processus de normalisation est conceptuel [66]. Comme on peut le voir, les résultats de la normalisation affecteront fondamentalement l'invariance de la représentation. Au fil des ans, de nombreux chercheurs se sont penchés sur la conception d'une telle approche de normalisation dans le cadre de différentes tâches telles que la correction géométrique [192, 214] et le recalage d'images [21, 276]. L'une des méthodes les plus simples repose sur les moments géométriques, qui permettent d'obtenir l'invariance en translation, en échelle et en rotation en évaluant/éliminant le centroïde, le facteur d'échelle et l'axe principal de l'image, tous basés sur des moments géométriques d'ordre inférieur. Pour plus de détails à ce sujet, nous encourageons vivement les lecteurs à consulter les ouvrages de Flusser et al [66, 64], qui fournissent une analyse et une définition complètes. Pour d'autres types de méthodes de normalisation, les lecteurs peuvent se référer à l'article de Zitova et al [276].

- Méthode indirecte [43, 102] : Il est bien connu que les moments géométriques sont faciles à dériver des invariants explicites pour une transformation affine D, comme le montrent [61, 66, 64]. Par conséquent, cette approche exprime les invariants des moments orthogonaux comme une combinaison linéaire des invariants des moments géométriques, basée sur la relation algébrique entre les moments orthogonaux et les moments géométriques. Évidemment, l'invariance de cette approche provient des invariants de moments géométriques. Ici, la relation de conversion est universelle, puisque les polynômes sont formés directement à partir de combinaisons linéaires de séquences $\{x^0, x^1, ..., x^n\}$, et que les fonctions harmoniques peuvent être écrites sous une forme similaire via les séries de Taylor. Notez que la normalisation d'image à l'aide de moments géométriques suivis d'une description basée sur les moments orthogonaux et les invariants de moments orthogonaux dérivés d'une combinaison linéaire d'invariants de moments géométriques jouent un rôle très similaire en

théorie ; en pratique, les différentes méthodes présentent différents problèmes de stabilité numérique et de complexité de calcul [66].

- Méthode explicite [42, 14, 274] : Cette approche cherche à dériver les invariants directement à partir des moments orthogonaux. Mathématiquement, elle essaie de satisfaire l'identité $I(< f, V_{nm} >) = I(< D(f), V_{nm} >)$ en concevant V_{nm} et I. L'invariance de cette approche provient directement des moments donnés. Une méthode très courante dans cette approche consiste à construire explicitement les invariants de rotation des moments circulaires. Duo à la fonction de base angulaire $A_m(\theta) = exp(jm\theta)$ et au théorème du décalage de Fourier, les moments circulaires définis dans l'équation (1) et l'équation (4) de l'image tournée $f^{rot}(r, \theta) = f(r, \theta + \phi)$ sont $M'_{nm} = exp(jm\phi)M_{nm}$. Par conséquent, l'opération de rotation de l'image n'affecte que la phase des moments circulaires. La méthode traditionnelle pour réaliser l'annulation de phase est basée sur la magnitude, c'est-à-dire, $|M'_{nm} = |exp(jm\theta)M_{nm}| = |M_{nm}|$. Cependant,ces méthodes simples écartent trop d'informations sur l'image : elles ne laissent que la magnitude, et la phase, plus importante, est ignorée [161, 177]. Pour cela, Flusser [60] a proposé les invariants de rotation à valeurs complexes contenant l'information de phase. Soit $L \geq 1$ et $n_i \in N, m_i, k_i \in Z, i = 1, ..., L$ tels que $\sum_{i=1}^{L} m_i k_i = 0$. Alors, les invariants de rotation à valeurs complexes des moments circulaires peuvent être définis comme $inv = \prod_{i=1}^{L} [M_{ni,mi}]^{k_i}$ [60]. En fait, la méthode de normalisation peut être peu pratique pour de nombreuses applications, par exemple la représentation de blocs d'images denses. De plus, les moments calculés par le schéma de normalisation peuvent différer des moments réels de l'image standard, en raison d'erreurs dans l'évaluation des paramètres de normalisation. En ce qui concerne la méthode indirecte, un long temps est alloué au calcul des coefficients polynomiaux, nécessitant ainsi le calcul récursif de ces coefficients. En revanche, en raison de sa structure directe, la méthode explicite est plus applicable dans une variété de scénarios et peut généralement atteindre une plus grande précision et efficacité [247].

Bruit

Différente de la transformation affine, l'attaque par le bruit agit sur le domaine de l'intensité, c'est-à-dire que l'opération de dégradation D est une mise en correspondance de la fonction d'intensité originale $f(x, y)$ avec la nouvelle fonction d'intensité $f'(x, y), D : f(x, y) \rightarrow f'(x, y)$. Mathématiquement, sur la base d'une fonction de bruit spécifique $\eta(x, y)$, le bruit additif commun est défini comme suit :

$$f'(x, y) = f(x, y) + \eta(x, y) \tag{2.22}$$

et le bruit multiplicatif est défini comme :

$$f'(x, y) = f(x, y) \times \eta(x, y) \tag{2.23}$$

Pour améliorer la robustesse au bruit, il est difficile d'adopter une normalisation similaire à celle de la représentation affine invariante, car les problèmes inverses sont souvent mal conditionnés ou mal posés [189, 263]. Actuellement, une stratégie courante dans la représentation d'images basée sur les moments consiste à convertir l'image dans un nouvel espace avec un rapport signal/bruit (SNR) plus élevé via une transformation spécifique T, par exemple l'espace de Radon [237, 83, 150]. Sur la base de ce nouvel espace, V_{nm} et I sont conçus pour obtenir une représentation

robuste R :

$$I(< T(f), V_{nm} >) \approx I(< T(D(f)), V_{nm} >) \tag{2.24}$$

La représentation d'images basée sur la transformée de Radon présente l'avantage d'être robuste au bruit additif [97]. La transformée de Radon d'une fonction image $f(x, y)$ est définie comme :

$$Rad_f(\rho, \alpha) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} f(x, y)\delta_{\rho, xcos\alpha + ysin\alpha} dxdy \tag{2.25}$$

où δ_{ij}est la fonction delta de Kronecker définie dans l'équation 2.1, $\rho = xcos\alpha + ysin\alpha$ est une ligne droite avec l'angle α (par rapport à l'axe y) et la distance ρ (par rapport à l'origine). La transformée de Radon de l'image bruyante définie dans l'équation 2.22 peut être écrite comme suit :

$$Rad_{f'}(\rho, \alpha) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} [f(x, y) + \eta(x, y)]\delta_{\rho, xcos\alpha + ysin\alpha} dxdy = Rad_f(\rho, \alpha) + Rad_\delta(\rho, \alpha) \tag{2.26}$$

Dans le domaine continu, la transformée de Radon du bruit $Rad_\delta(\rho, \alpha)$est égale à la valeur moyenne du bruit, que l'on suppose nulle. Ainsi, on a

$$Rad_{f'}(\rho, \alpha) = Rad_f(\rho, \alpha) = \tag{2.27}$$

Cela signifie que le bruit additif de moyenne nulle n'a aucun effet sur la transformée de Radon de l'image. Quant au bruit multiplicatif tel que l'équation 2.23, une stratégie potentielle consiste à utiliser la transformation logarithmique comme prétraitement pour séparer l'image et le bruit en deux parties additives, c'est-à-dire, $log[f(x, y) \times \eta(x, y)] = log[f(x, y) + log[\eta(x, y)]]$. En pratique, cependant, l'identité parfaite de l'équation 2.27 ne tient pas car l'image et le bruit sont échantillonnés et quantifiés. Pour le cas discret, le RSB de l'image dans l'espace de Radon est toujours significativement plus élevé que celui de l'image originale, ce qui signifie une meilleure robustesse. Le lecteur est invité à consulter les articles de Hoang et al. [83] et de Jafari-Khouzani et al. [97] pour une analyse théorique et des expériences détaillées.

Brouillage

De manière similaire à l'attaque par le bruit, le flou agit également sur le domaine de l'intensité, c'est-à-dire $D : f(x, y) \rightarrow f'(x, y)$. Mathématiquement, sur la base d'une fonction d'étalement du point (PSF) spécifique $\mu(x, y)$, l'image floue observée peut être décrite comme une convolution :

$$f'(x, y) = f(x, y) \otimes \mu(x, y) \tag{2.28}$$

Par conséquent, l'invariance du flou peut également être appelée invariance de la convolution. Pour le flou des images, la "normalisation" signifie en fait la déconvolution aveugle, qui est un problème fortement mal conditionné ou mal posé [115, 24]. À l'heure actuelle, la représentation invariante des images floues repose généralement sur une transformation spécifique de l'espace image, comme une opération de projection similaire à la transformée de Radon. L'idée principale peut également être exprimée par l'équation 2.24. À cet égard, les travaux de Flusser et al. [110, 67, 68, 169] sont remarquables.

Progrès récents dans le domaine de l'optimisation de la robustesse/Invariance

Les invariants de moment affine d'une image 2D et 3D sont des outils bien établis [201, 142]. Dans les livres de Flusser et al [66, 64], les invariants affines explicites et la stratégie de normalisation utilisant les moments géométriques/complexes sont dérivés en détail. De plus, ces invariants peuvent facilement être étendus aux moments orthogonaux grâce à la relation de conversion inhérente. Par conséquent, le travail de Flusser et al. sur les invariants affines est très générique et reste l'un des efforts les plus marquants dans ce domaine. Plus récemment, l'extension des invariants a suscité un vif intérêt scientifique [241]. 1) Extension à d'autres groupes de transformations, comme les invariants sous réflexion [123], projectifs [124], de Möbius [260] et chiraux [261], le flou arbitraire à symétrie . 2) Extension à d'autres dimensions ou formats de données : tels que les invariants d'une image couleur [78], d'une courbe [240], d'une surface [240], d'un champ vectoriel [108, 109] et d'un champ tensoriel [117, 174]. 3) Extension à d'autres moments, tels que les invariants des OFMM [262], des JFM [233], de la transformée de Fourier-Mellin [248], des moments radiaux de Tchebichef [232], des moments radiaux de Legendre [234] et des moments de Gaussian-Hermite [244, 245]. Dans un travail remarquable, Li et al [125] ont exploré en profondeur la structure des invariants. Ils ont proposé deux fonctions génératrices (GF) fondamentales, qui peuvent coder les invariants des moments géométriques et construire ensuite des descripteurs de forme, tout comme l'ADN code les protéines. Ils ont également découvert que les sept invariants de Hu peuvent être décomposés en un ensemble plus simple d'invariants primitifs (IP), ce qui peut signifier une nouvelle perspective pour l'étude des invariants [122].

Il est bien connu que les problèmes inverses du bruit et du flou des images sont généralement plus difficiles à résoudre que les problèmes inverses des transformations affines. Cela signifie que les méthodes de normalisation, c'est-à-dire le débruitage et le désembrouillage, sont des tâches très difficiles. Une telle approche est généralement lente et instable en raison des artefacts de restauration [110]. Pour la voie de la force brute telle que le CNN, le manque d'invariance inhérente les rend très sensibles au bruit et aux opérations de flou non vues lors de la formation. Un travail récent [171] a confirmé cette conclusion par des expériences approfondies. La stratégie la plus courante pour pallier ce problème est l'augmentation des données. Cependant, elle est très consommatrice de temps et de mémoire, et se résume à un "apprentissage par cœur". En raison de ces faits, la représentation invariante des images bruyantes ou floues basée sur le moment est cruciale pour de nombreuses applications pratiques. Dans cette voie, un objectif principal poursuivi par les chercheurs est de simplifier les hypothèses sur la dégradation, qui sont la base de la conception des invariants. Par exemple, grâce à des contraintes supplémentaires sur le PSF, ils ont dérivé des invariants pour le flou de mouvement [63], le flou à symétrie axiale dans le cas de deux axes [62], le flou à symétrie circulaire [65, 32], le flou arbitraire à symétrie N-fois [67], le flou gaussien à symétrie circulaire [68] et le flou gaussien général (anisotrope) [110]. Récemment, une représentation invariante prometteuse du flou a été proposée par Kostková et al [110]. La principale contribution est la conception d'invariants pour le flou gaussien général, où le PSF est une fonction gaussienne avec des paramètres inconnus, c'est-à-dire que le noyau du flou peut être arbitrairement orienté, mis à l'échelle et allongé.

2.3 Conclusion

Dans ce chapitre nous avons présenter une étude théorique concernant les moments d'image. Après avoir démontré l'utilité de la représentation manuelle des carctéristiques de l'image nous avons attaqué la théorie mathématique derrière les moments, ensuite nous avons fait le tour des application des moments dans le monde réel. Finalement nous avons exposer les différentes approches pour l'implémentation des moments et les voix d'optimisations de leurs algorithmes. A savoir que ce chapitre sert comme une introduction générale à la théorie des moments. Dans le reste de ce manuscrit nous allons présenter au fur et à mesure les moments nécessaires pour l'implémentation de chaque algorithme proposé.

Chapitre 3

Un nouvel ensemble d'algorithmes de chiffrement d'images basé sur les moments orthogonaux discrets et la théorie du chaos

3.1 Introduction

Le chiffrement est le processus qui consiste à transformer des données "significatives" en une forme inintelligible. Son objectif est d'assurer la sécurité du stockage et la transmission sécurisée du contenu sur le réseau [162]. Le chiffrement d'images pose des défis différents de ceux du chiffrement de texte. En effet, les images numériques présentent certaines caractéristiques telles que : la redondance des données, la forte corrélation entre les pixels adjacents et la taille importante des données. Ainsi, les chiffrements traditionnels tels que IDEA, AES, DES, RSA, etc. ne sont pas adaptés au chiffrement d'images en temps réel, car ils nécessitent un temps de calcul important et des ressources informatiques élevées [129, 259]. Différents algorithmes ont été spécifiquement conçus pour le chiffrement d'images : Chaos[70, 242, 121, 252, 253], SCAN [35], S-Box [92], algorithmes de permutation uniquement [128]. Parmi les algorithmes proposés, le chaos a été le plus étudié et a donné des résultats encourageants [59, 221], en raison de ses caractéristiques spécifiques telles que : pseudo-aléatoire, ergodicité, haute sensibilité aux conditions initiales et aux paramètres [111].

Au cours de la dernière décennie, un certain nombre de méthodes de chiffrement d'images ont été proposées dans la littérature. En général, les méthodes de chiffrement d'images peuvent être classées en deux catégories : les algorithmes de chiffrement utilisant le domaine spatial et les autres algorithmes utilisant le domaine de transformation. La première catégorie tend à être une approche directe puisque les pixels de l'image sont manipulés directement ; cependant, elle entraîne une non-corrélation entre les pixels, ce qui rend l'image chiffrée incompressible [99]. A l'inverse, les méthodes de chiffrement basées sur les domaines de transformation utilisent, au lieu des pixels de l'image, les coefficients obtenus via le domaine de transformation. Ces algorithmes semblent avoir une plus grande efficacité, sont plus robustes face à certaines opérations de traitement d'image et peuvent permettre une récupération sans perte de l'image originale [119, 120, 137, 204]. Dans la littérature, différents domaines de transformation ont été utilisés : J. Wu et al. [229] ont proposé un algorithme de chiffrement d'image basé sur une transformée en cosinus discrète fractionnelle préservant la réalité et une séquence génératrice basée sur le chaos, qui hérite de la réalité ainsi que de la non-périodicité de la matrice de la transformée en

cosinus discrète (TCD) ; en outre, la séquence génératrice (SG), qui résulte de la multiplicité de la racine de la matrice TCDFr, est présentée comme une clé de chiffrement supplémentaire. Y. Luo et al. [141] ont introduit un schéma de chiffrement d'image symétrique dans le domaine des ondelettes et du temps en utilisant la transformation en ondelettes entières (IWT) ; les coefficients d'approximation sont diffusés par des clés secrètes générées à partir d'un système chaotique spatio-temporel suivi d'une IWT inverse pour construire l'image diffusée. Un algorithme de chiffrement d'image basé sur le chaos spatio-temporel dans le domaine DCT a été étudié par G. Xin et al. [238] où chaque bloc est d'abord permuté en plaçant la valeur sur la même position d'un bloc choisi en utilisant une carte logistique, puis les signes des blocs permutés sont extraits et chiffrés par le chaos spatio-temporel.

Notez que la plupart de ces méthodes de chiffrement utilisent les domaines de fréquence comme domaine de transformation. Cependant, les moments d'image s'imposent comme l'une des transformations les plus attrayantes en traitement d'image, ils sont meilleurs en termes de description d'image et plus robustes au bruit [11, 15]. Ces dernière années, différents polynômes orthogonaux ont été étudiés. Les moments orthogonaux continus ont été établis pour la première fois [203], ils sont formés à partir des fonctions de base des polynômes orthogonaux continus et ont démontré une capacité remarquable dans la représentation des caractéristiques [104, 213]. Cependant, lors de la mise en œuvre de ces moments, plusieurs problèmes sont rencontrés tels que : l'approximation numérique des intégrales continues, la grande variation dans la gamme dynamique des valeurs et la transformation de l'espace des coordonnées [155, 250]. Ces problèmes ont incité les chercheurs à rechercher des moments orthogonaux discrets comme ensemble de base, ce qui permet d'éviter toute approximation numérique et d'obtenir une reconstruction d'image supérieure. Depuis lors, des études approfondies ont été menées sur ces moments, et ils ont été appliqués dans de nombreux domaines tels que : l'analyse d'images [12, 155, 250, 270, 273, 272], le tatouage d'images [49, 206], la reconnaissance de formes [61, 200], la détection de bords [87, 72] et la compression de données [87]. Néanmoins, à notre connaissance, les transformations de moments d'images n'ont pas encore été explorées dans le domaine du chiffrement d'images.

En observant les excellentes capacités de représentation d'images des moments discrets, nous sommes motivés pour explorer les capacités des moments pour le chiffrement d'images. Pour cela, dans ce manuscrit, nous introduisons un nouvel ensemble d'algorithmes de chiffrement basés sur le chaos et opérant dans le domaine de transformation des moments. Nous nous concentrerons particulièrement sur l'utilisation des moments orthogonaux discrets classiques tels que Tchebichef [155], Krawtchouk [250], Hahn [270], Dual-Hahn [272] et Racah [273]. Nous utilisons deux cartes chaotiques logistiques pour le chiffrement, une clé externe de 128 bits est divisée en deux segments de taille égale : K1 et K2, chaque 64 bits sert de condition initiale pour la carte logistique correspondante. Après avoir calculé les coefficients des moments, une opération de confusion/diffusion est effectuée pour obtenir l'image chiffrée. Le déchiffrement est le processus inverse qui permet de récupérer l'image originale à partir de la forme chiffrée. Un ensemble d'expériences et de tests sont menés : l'entropie, l'analyse de l'espace des clés, les attaques statistiques et différentielles sont utilisées afin d'évaluer les performances des algorithmes proposés, puis nous les comparons avec le chiffrement dans le domaine fréquentiel en utilisant la DCT et les algorithmes de l'état de l'art présentés dans [29, 141].
Le reste de ce chapitre est organisé comme suit. La section 2 sert d'étude de base pour les moments orthogonaux et le chiffrement du chaos. La section 3 présente les schémas proposés. Les résultats expérimentaux sont illustrés dans la section 4. Dans

la section 5 nous introduisons une dérivée des algorithmes proposés qui est basée sur le chiffrement sélectif. Finalement une conclusion est tirée dans la section 6.

3.2 Contexte théorique

3.2.1 Fonctions de moment

Introduits pour la première fois par Hu [89] en 1961, les invariants des moments ont trouvé plusieurs applications [25, 54, 144] dans le traitement des images en raison de leurs capacités à représenter des caractéristiques globales. Cependant, la reconstruction de l'image est une tâche difficile car ces moments ne sont pas orthogonaux. En 1980, Teague [203] a proposé des moments avec des fonctions de base orthogonales telles que Legendre et Zernike. Ces moments sont capables de stocker des informations avec une redondance minimale et ont été largement utilisés dans un passé récent [8, 105, 72]. L'approximation numérique des intégrales continues, la grande variation de la gamme dynamique des valeurs et la transformation de l'espace des coordonnées sont quelques problèmes communs rencontrés lors de la mise en œuvre de ces moments. Ces problèmes ont incité les chercheurs à envisager l'utilisation de polynômes orthogonaux discrets comme ensemble de base, car la mise en œuvre des moments orthogonaux discrets n'implique aucune approximation numérique, les fonctions de base satisfont à la propriété d'orthogonalité et permettent donc une représentation supérieure de l'image [155].

3.2.2 Moments orthogonaux discrets

Pour une image $N \times M$ avec une fonction d'intensité $f(x, y)$, la formule générale d'un moment d'ordre $(n + m)$, peut être exprimée comme suit

$$M_{nm} = NF \times \sum_{i=1}^{N} \sum_{j=1}^{M} kernel_{nm}(x_i, y_i) f(x_i, y_i) \tag{3.1}$$

Où NF est le facteur de normalisation, $kernel_{nm}()$ est le noyau des moments qui constitue la base orthogonale d'un polynôme spécifique d'ordre n et m. En changeant le polynôme du noyau, on obtient différentes familles de moments. Le tableau 3.1 résume les principales caractéristiques des moments utilisés dans ce manuscrit.
La fonction de transformation inverse pour reconstruire l'image originale est :

$$\tilde{f}(x, y) = \sum_{n=0}^{\eta_{max}} \sum_{m=0}^{\eta} kernel_{nm}(x, y) M_{nm} \tag{3.2}$$

D'un point de vue théorique, si tous les moments de l'image sont calculés, on peut récupérer une image reconstruite qui sera identique à l'image originale avec une erreur de reconstruction minimale [164].

Afin de faciliter les calculs de ces moments, les auteurs de [158, 163, 184] ont étudié leurs aspects computationnels : la propriété de symétrie et la formule récursive sont deux aspects qui diminuent le coût de calcul. Le lecteur est invité à consulter ces articles pour plus de détails sur les aspects informatiques des moments.

TABLE 3.1: Principales caractéristiques des moments orthogonaux discrets

Famille de moments	$Kernel_{nm}(x,y)$	Forme polynomiale	Facteur de normalisation
Tchebichef [155]	$t_n(x) \times t_m(y)$	$t_n(x) = (1-N)_n {}_3F_2(-n,-x,1+n;1,1-N;1)$	$\frac{1}{\tilde{\rho}(p,N)\tilde{\rho}(q,N)}$
Krawtchouk [250]	$K_n(x;p_1,N) \times K_m(y;p_2,N)$	$K_n(x;p,N) = \sum_{k=0}^{N} a_{k,n,p} x^k$	1
Hahn [270]	$h_m^{\mu,\nu}(x,N) \times h_n^{\mu,\nu}(y,N)$	$h_n^{(u,v)}(x,N) = (N+v-1)_n (N-1)_n \times \sum_{k=0}^{n} (-1)^k \frac{(-n)_k (-x)_k (2N+\mu+v-n-1)_k}{(N+v-1)_k (N-1)_k} \frac{1}{k!}$	1
Dual Hahn [272]	$w_n^{(c)}(s,a,b) \times w_m^{(c)}(t,a,b)$	$w_n^{(c)}(s,a,b) = \frac{(a-b+1)_n (a+c+1)_n}{n!} {}_3F_2(-n,a-s,a+s+1;a-b+1,a+c+1;1)$	1
Racah [273]	$u_n^{(\alpha,\beta)}(s,a,b) \times u_m^{(\alpha,\beta)}(t,a,b)$	$u_n^{\alpha,\beta}(s,a,b) = \frac{1}{n!}(a-b+1)_n (\beta+1)_n (a+b+\alpha+1)_n {}_4F_3\left(\begin{matrix} -n,\alpha+\beta+n+1,a-s,a+s+1 \\ \beta+1,a+1-b,a+b+\alpha+1 \end{matrix};1\right)$	1

3.2.3 La théorie du chaos pour la cryptographie

L'utilisation de la théorie du chaos en cryptographie remonte à 1949. Dans son chef-d'œuvre, Shannon [187] a déclaré que : *"Les bonnes transformations de mélange sont souvent formées par des produits répétés de deux opérations simples non commutatives. Hopf a montré, par exemple, que la pâte à pâtisserie peut être mélangée par une telle séquence d'opérations. La pâte est d'abord étalée en une fine plaque, puis repliée, puis étalée, puis repliée à nouveau, etc....*
Dans une bonne transformation de mélange... les fonctions sont compliquées, impliquant toutes les variables de manière sensible. Une petite variation de n'importe quelle (variable) change (les sorties) considérablement". Même s'il n'utilise pas le mot chaos explicitement, il mentionne le mécanisme de base de d'étirement et de repliement utilisé dans la cryptographie chaotique [70]. Depuis lors, les chercheurs ont étudié différentes façons d'utiliser le chaos en cryptographie [10, 19, 70, 147].

Les cryptosystèmes basés sur le chaos sont largement utilisés pour des applications pratiques en raison de leurs propriétés telles que la dépendance sensible aux conditions initiales, les paramètres de contrôle et le comportement pseudo-aléatoire [175, 167]. Cependant, il existe une différence importante entre les algorithmes cryptographiques et les cartes chaotiques, puisque les premiers opèrent dans un espace discret alors que les secondes n'ont de sens que dans un continuum [175]. L'architecture générale d'un cryptosystème basé sur le chaos [179] est illustrée par le schéma bloc typique de la figure 3.1.

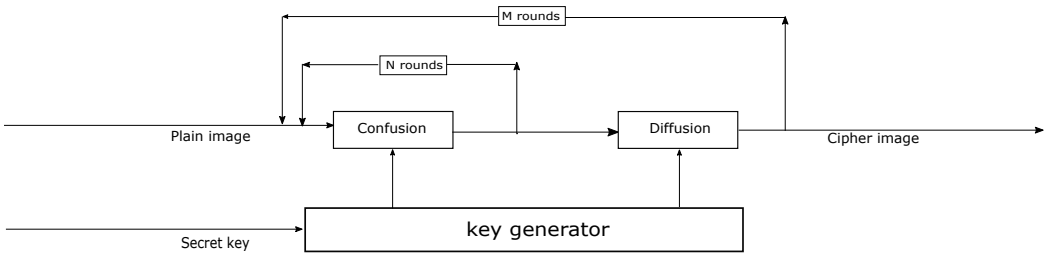


FIGURE 3.1: Architecture d'un système de chiffrement basé sur le chaos

Dans l'étape de confusion, les pixels sont permutés à l'aide d'une séquence pseudo-aléatoire sans changer les valeurs des éléments de l'image. Cette opération rend l'image méconnaissable mais n'est pas suffisante pour la rendre sécurisée [100]. L'étape de diffusion est celle où les valeurs de chaque pixel sont modifiées en utilisant la même séquence pseudo-aléatoire ou une séquence différente. Ces séquences sont obtenues en itérant une carte chaotique. Les étapes de confusion et de diffusion sont répétées un certain nombre de fois pour atteindre le niveau de sécurité requis.

3.3 Approche proposée

Nous proposons un ensemble de nouveaux algorithmes de chiffrement basés sur le chaos et opérant dans le domaine de la transformation des moments discrets en utilisant : Tchebichef, Krawtchouk, Hahn, Dual-Hahn et Racah. Dans cette section, nous présentons en détail les étapes des procédures de chiffrement d'images proposées ainsi que le processus de déchiffrement pour chaque algorithme.

3.3.1 Chiffrement

Le schéma général des algorithmes proposés est présenté à la figure 3.2. Il comprend trois phases, à savoir : la transformation des moments discrets, la confusion et la diffusion. Dans la première phase, les coefficients des moments de l'image originale sont calculés afin que l'image soit représentée dans le domaine de transformation des moments. Dans la phase de confusion, les positions des pixels sont modifiées sans changer les valeurs réelles des pixels, ce qui détruit l'affiliation entre les pixels adjacents et rend ainsi l'image méconnaissable, la phase de confusion est itérée N fois, où N est généralement supérieur à 1. Dans la phase de diffusion, les valeurs des pixels sont modifiées séquentiellement de sorte qu'un petit changement dans un pixel se propage à plusieurs pixels afin de cacher la structure statistique de l'image en clair. L'ensemble du processus de confusion-diffusion se répète M fois pour atteindre un niveau de sécurité satisfaisant. Les séquences utilisées dans les étapes de confusion et de diffusion sont générées par deux cartes logistiques avec une clé secrète d'origine en entrée. Les cartes logistiques utilisées sont données par les équations :

$$x_{n+1} = \lambda x_n(1 - x_n), x\epsilon[0, 1] \tag{3.3}$$

$$y_{n+1} = \lambda y_n(1 - x_n), y\epsilon[0, 1] \tag{3.4}$$

Tout au long de l'algorithme, nous gardons $\lambda = 3,99$ qui correspond à un cas hautement chaotique tandis que les conditions initiales (X_0 et Y_0) sont calculées à l'aide de quelques manipulations mathématiques expliquées à l'étape 1. N et M sont fixés au nombre minimal de tours 1, ce qui rend l'algorithme aussi rapide que possible et, comme le montre la section des résultats, cela n'affecte pas les performances de sécurité des algorithmes.

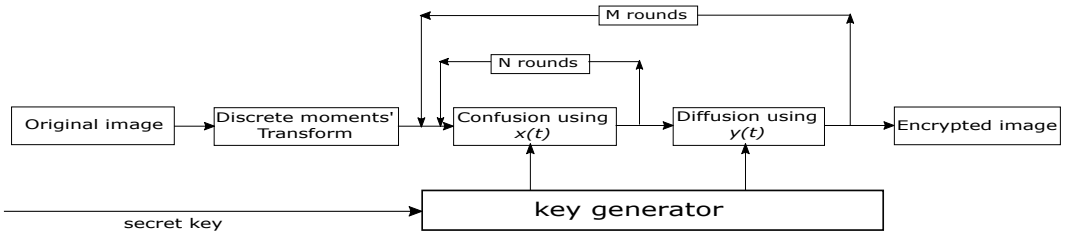


FIGURE 3.2: Architecture des algorithmes proposés

étape 1) Génération de la clé : Une clé externe de 128 bits est utilisée, la clé est divisée en deux segments de taille égale : K_1 et K_2, chaque segment de 64 bits sert de valeur initiale pour la carte logistique correspondante. Pour adopter chaque segment comme valeur initiale pour la carte logistique (une valeur entre 0 et 1), nous effectuons quelques opérations mathématiques sur la clé :
Nous notons chaque K_i dans sa représentation binaire : $K_1 = K_{11}K_{12}...K_{164}$; $K_2 = K_{21}K_{22}...K_{264}$, puis les valeurs initiales des deux cartes logistiques sont calculées comme suit :

$$X_0 = (K_{11} \times 2^0 + K_{12} \times 2^1 + ... + K_{164} \times 2^{63})/2^{64} \tag{3.5}$$

$$Y_0 = (K_{21} \times 2^0 + K_{22} \times 2^1 + ... + K_{264} \times 2^{63})/2^{64} \tag{3.6}$$

Où X_0 et Y_0 sont les valeurs initiales de la première et de la deuxième carte logistique respectivement.
étape 2) Calcul des moments : La différence entre les algorithmes de chiffrement

proposés de Tchebichef, Krawtchouk, Hahn, Dual Hahn et Racah réside dans l'étape de calcul des moments, toutes les autres étapes étant similaires. Dans cette étape, nous calculons les fonctions des moments de l'image originale. Pour chaque algorithme proposé, nous calculons les moments correspondants qui constituent la base orthogonale en utilisant la formule récursive présentée dans la section 2. Afin d'optimiser davantage les calculs des moments, nous avons utilisé la stratégie de partitionnement proposée dans [158]. L'image est donc divisée en blocs de 8 x 8 et nous calculons les moments pour ces sous-images, ce qui améliore la vitesse de calcul des moments puisque nous calculons les moments d'ordre faible. Les coefficients de ces moments sont stockés dans une matrice de la même taille que l'image originale.
étape 3) Confusion : Dans la terminologie cryptographique, la confusion fait référence au processus de substitution. Elle vise à rendre la relation entre la clé et le texte chiffré aussi complexe que possible. Dans la technique de chiffrement d'images proposée, nous générons une séquence aléatoire de taille 256*256 en utilisant la première carte logistique avec la condition initiale X0. Ensuite, nous transformons la matrice obtenue à l'étape 2 en un tableau de taille 256*256, qui est permuté selon la séquence générée par la première carte logistique.
étape 4) Diffusion : La diffusion est le processus qui consiste à modifier les propriétés statistiques de l'image en clair en répartissant l'information dans l'image en clair de sorte que la redondance soit répartie sur l'image chiffrée. Ce processus est nécessaire pour une technique de chiffrement sécurisée. En fait, le processus de diffusion élimine la vulnérabilité aux attaques différentielles en comparant les images en clair et chiffrées. Dans l'étape de diffusion, les valeurs des pixels sont modifiées séquentiellement par la séquence pseudo-aléatoire générée par la carte chaotique. Dans les techniques de chiffrement d'images proposées, nous générons une autre séquence à partir de la deuxième carte logistique avec la condition initiale Y_0, puis une opération XOR est effectuée entre la séquence générée et le tableau obtenu à l'étape 3.
étape 5) Le tableau obtenu à l'étape 4 est retransformé en une matrice de taille initiale 256*256 qui est l'image chiffrée finale.

3.3.2 Déchiffrement

L'algorithme de déchiffrement est similaire à l'algorithme de chiffrement, sauf que les étapes sont dans l'ordre inverse. Tout d'abord, l'image chiffrée est convertie en un tableau de taille 256*256. Une opération XOR est ensuite effectuée entre les éléments du tableau et la séquence aléatoire générée au début en utilisant Y0 comme valeur initiale. Les éléments du tableau résultant sont permutés selon la séquence qui utilise X0 comme valeur initiale. Le tableau résultant est retransformé en une matrice de taille 256*256. Les moments inverses sont calculés à l'aide de la fonction de moment appropriée (inverse DCT pour l'algorithme de chiffrement basé sur DCT), ce qui nous permet d'obtenir l'image originale. Comme pour l'algorithme de chiffrement nous fixons M et N à 1.

3.4 Résultats expérimentaux

Un problème important du chiffrement d'images est l'évaluation de la robustesse de l'algorithme utilisé. L'inspection visuelle peut être un indice, mais il ne faut pas s'y fier exclusivement [58]. D'autres métriques ont été proposées pour juger plus

objectivement de la performance de l'algorithme de chiffrement [4, 55, 56, 130]. Afin de valider l'efficacité des schémas de chiffrement basés sur les moments nouvellement introduits, une série d'expériences est réalisée et présentée dans quatre sous-sections. Dans la première sous-section, la robustesse aux attaques différentielles est illustrée par les paramètres NPCR et UACI. Dans la deuxième sous-section, les attaques statistiques sont abordées en étudiant le coefficient de corrélation. Dans la troisième sous-section, l'analyse de l'espace clé est décrite. Enfin, nous évaluons la sécurité des algorithmes proposés en termes d'analyse de l'entropie. Pour chaque sous-section, nous définissons formellement les paramètres utilisés, puis nous présentons les résultats des algorithmes de chiffrement basés sur les moments et nous les comparons avec l'algorithme de chiffrement basé sur la DCT et d'autres algorithmes de l'état de l'art. Nous les comparons à l'algorithme de chiffrement basé sur la DCT et à d'autres algorithmes de pointe des références [29, 141].

Dans cette étude expérimentale, nous utilisons un ensemble de douze images au niveau de gris de taille 256*256, comme le montre la figure 3.3. Un sous-ensemble d'images composé de (D22, D35, D36, D41, D52, D66 et D67) est utilisé pour tester la performance des algorithmes proposés sur des images à haute texture.
Il est important de souligner que tous les algorithmes sont mis en œuvre en utilisant MATLAB 11 sur un ordinateur portable avec un processeur Intel Core i7, 2,7 GHz, 8 gigaoctets de mémoire et 256 gigaoctets de disque dur fonctionnant sous Windows 10.

3.4.1 Attaques différentielles NPCR et UACI

Nous changeons un seul pixel de l'image originale et évaluons son influence sur l'image chiffrée. NPCR [230] (Number of Pixel Change Rate) est la différence du nombre de pixels entre deux images chiffrées, UACI [230] (Unified Average Changing Intensity) est la différence entre deux images chiffrées selon l'intensité moyenne. Elles sont définies par les formules 3.7 et 3.8 respectivement :

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{3.7}$$

$$UACI = \frac{1}{W \times H} \left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\% \tag{3.8}$$

W et H sont la largeur et la hauteur de l'image chiffrée. $C1(i,j)$ et $C2(i,j)$ sont les valeurs de pixel à la position (i, j) pour la première et la deuxième image chiffrée respectivement. Si $C1(i,j) = C2(i,j)$, alors $D(i,j) = 1$, sinon $D(i,j) = 0$. Plus le NPCR et l'UACI sont grands, plus l'algorithme est protégé contre les attaques différentielles [230]. Afin d'évaluer la sécurité des algorithmes proposés contre les attaques différentielles. Nous calculons NPCR et UACI pour chaque image chiffrée pour tous les algorithmes proposés et nous les comparons avec l'algorithme de chiffrement basé sur DCT et les algorithmes de [141, 29]. Ainsi, les images présentées dans la figure 3.3 sont chiffrées à l'aide des algorithmes de chiffrement basés sur : Tchebichef, Krawtchouk, Racah, Hahn et double moment de Hahn et comparées à l'algorithme basé sur DCT et les schémas de chiffrement dans [29, 141], puis les résultats correspondants sont illustrés dans les tableaux 3.2 et 3.3.

En examinant le tableau 3.2, il est clair que l'algorithme de chiffrement de Hahn a les valeurs les plus élevées de NPCR pour la majorité des images (à l'exception de D41 et D52 où l'algorithme de chiffrement de Tchebichef montre de meilleurs résultats), ce qui indique que l'algorithme de de Hahn présente de bonnes performances

TABLE 3.2: Résultats comparatifs en termes de valeurs NPCR des images de test.

NPCR	**Tchebichef**	**Krawtchouk**	**Racah**	**Hahn**	**Dual Hahn**	**DCT**	**Ref [141]**	**Ref [29]**
Lena	99,791	99,7559	99,7086	99,7879	99,7864	99,7864	99,6329	99,5682
Baboon	99,7955	99,8337	99,7482	99,855	99,7391	99,7864	99,5696	99,6802
cameraman	99,7574	99,7437	99,6979	99,8276	99,7406	99,791	99,6949	99,5318
Boats	99,7589	99,7681	99,7253	99,8337	99,7726	99,7681	99,7507	99,6125
Livingroom	99,8093	99,7467	99,7284	99,8276	99,7711	99,8199	99,68	99,7854
D22	99,8306	99,7833	99,7604	99,831	99,8108	99,7986	99,6268	99,7006
D35	99,8093	99,7971	99,7604	99,8177	99,7223	99,7879	99,7498	99,657
D36	99,8093	99,7772	99,7925	99,8367	99,7833	99,7971	99,5788	99,6617
D41	99,8459	99,8047	99,7818	99,8276	99,7787	99,794	99,6139	99,6902
D52	99,8383	99,8032	99,7787	99,8199	99,8047	99,8047	99,7335	99,8131
D66	99,8154	99,7772	99,791	99,8337	99,7772	99,7971	99,7371	99,5863
D67	99,7894	99,762	99,7742	99,8032	99,7986	99,7971	99,6837	99,7799

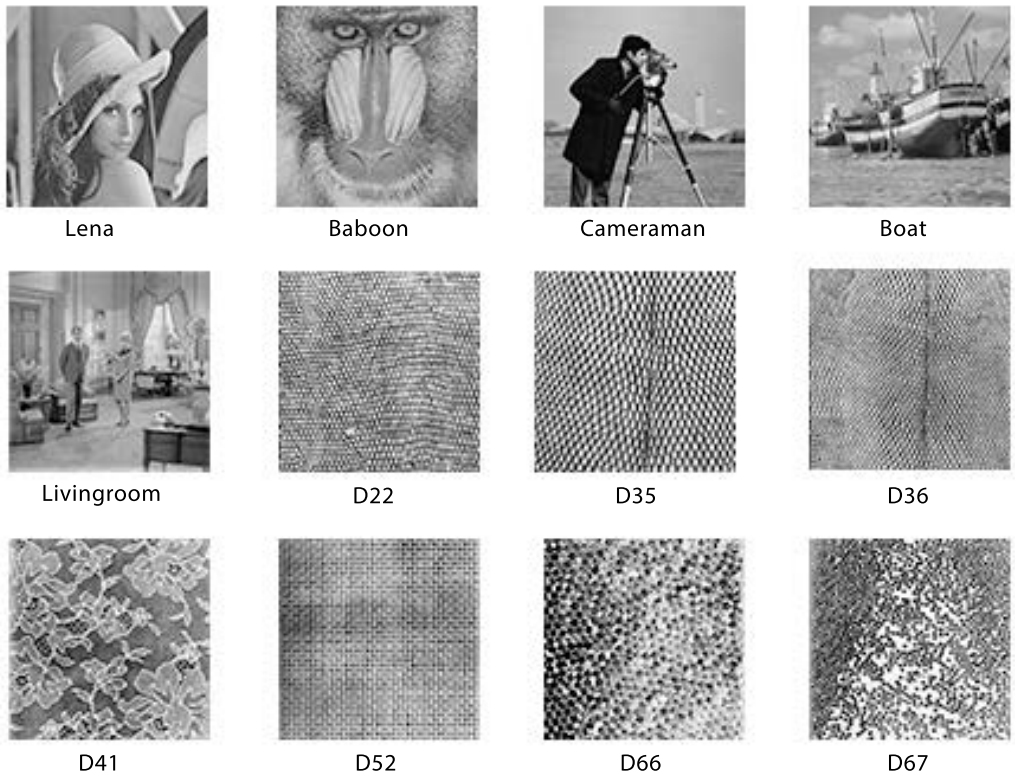


FIGURE 3.3: Images de tests

pour le NPCR.
Dans le tableau 3.3, nous montrons les résultats pour UACI. Nous voyons que les algorithmes de chiffrement basés sur les moments présentent des résultats satisfaisants, l'algorithme de chiffrement basé sur Krawtchouk est clairement plus performant pour toutes les images. De plus, on peut observer que tous les algorithmes basés sur les moments sont plus performants sur les images les plus texturées (D22, D35, D36, D41, D52, D66 et D67).
La principale conclusion de ces deux expériences est que les algorithmes basés sur les moments sont nettement plus performants que l'algorithme de chiffrement basé sur la DCT et les schémas de chiffrement dans les références [29, 141], en particulier sur les images à haute texture.

3.4.2 Analyse du coefficient de corrélation

Le coefficient de corrélation est un test statistique qui mesure la dépendance et la similarité entre l'image en clair et l'image chiffrée. Il prend une valeur comprise entre -1 et +1, une corrélation de 0 indique qu'il n'y a aucune corrélation entre les deux images. Une corrélation de 1 signifie que l'image originale et l'image chiffrée sont en parfaite corrélation et qu'il existe une forte dépendance entre les deux images. Ainsi, pour un bon algorithme de chiffrement, le coefficient de corrélation doit être proche de zéro [2].
Le coefficient de corrélation C.C est calculé entre l'image en clair x et l'image chiffrée y, lorsqu'elles sont organisées en séquences unidimensionnelles, comme suit [157]:

$$C.C = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{3.9}$$

TABLE 3.3: Résultats comparatifs en termes de valeurs UACI des images de test.

UACI	**Tchebichef**	**Krawtchouk**	**Racah**	**Hahn**	**Dual Hahn**	**DCT**	**Ref [141]**	**Ref [29]**
Lena	29,158	32,249	27,242	28,659	26,977	30,3256	30,638	31,313
Baboon	30,44	31,773	26,271	26,813	24,35	24,6456	30,17	28,846
cameraman	26,301	29,435	23,221	27,54	25,492	27,6376	27,61	26,768
Boats	25,102	27,503	21,287	25,609	21,389	26,3152	26,455	26,657
Livingroom	28,157	30,979	24,224	26,703	23,111	26,024	29,61	25,349
D22	33,617	34,55	32,651	30,36	30,371	29,496	29,537	33,164
D35	33,381	34,636	31,521	29,834	29,247	28,7616	26,283	31,002
D36	33,309	34,651	32,594	30,434	30,921	28,2256	26,489	31,366
D41	33,156	34,819	32,555	30,986	31,567	29,4944	28,162	27,707
D52	33,779	34,254	33,538	29,86	30,298	28,1968	27,501	30,603
D66	33,758	34,748	31,657	29,748	29,772	28,564	28,833	27,144
D67	33,81	34,27	32,593	30,712	30,57	30,9352	26,323	28,375

Où $cov(x,y) = \frac{1}{L}\sum_{l=1}^{L}(x(l)-E(x))(y(l)-E(y)), D(x) = \frac{1}{L}\sum_{l=1}^{L}(x(l)-E(x))^2, E(x) = \frac{1}{L}\sum_{l=1}^{L}x(l)$ et L est le nombre total de pixels dans l'image.

Afin d'évaluer la robustesse des algorithmes de chiffrement basés sur les moments proposés, nous calculons le coefficient de corrélation à l'aide de la formule 3.9 entre les images en clair et leurs chiffrages correspondants. Nous chiffrons chaque image de l'ensemble de test en utilisant les algorithmes de chiffrement basés sur Tchebichef, Krawtchouk, Racah, Hahn et double Hahn et nous comparons les résultats avec l'algorithme basé sur le chiffrement DCT et les algorithmes de [29, 141]. Les résultats obtenus sont présentés dans le tableau 3.4.

Sur la base des résultats fournis par le tableau 3.4, on peut voir que le coefficient de corrélation est proche de zéro pour tous les algorithmes de chiffrement, ce qui suggère que les algorithmes mis en œuvre ont une bonne qualité de chiffrement. En outre, les résultats expérimentaux démontrent que l'algorithme de chiffrement basé sur Hahn est relativement plus efficace que les autres algorithmes, y compris le DCT et les algorithmes de l'état de l'art.

3.4.3 Analyse des espaces clés

Pour un chiffrement d'image sécurisé, l'espace des clés doit être suffisamment grand pour rendre l'attaque par force brute infaisable. Le chiffrement d'image proposé possède $2^{128} \sim 3.4028 \times 10^{38}$ combinaisons différentes de la clé secrète. Un chiffrement d'image avec un espace de clé aussi long est suffisant pour une utilisation pratique fiable.

3.4.4 Analyse d'entropie

L'entropie est une mesure utilisée pour évaluer la sécurité d'un algorithme de chiffrement d'images, elle montre le degré d'imprévisibilité et d'aléatoire dans un système [57]. Un bon algorithme de chiffrement doit diminuer l'information mutuelle entre les pixels, et donc augmenter l'entropie. L'entropie $H(m)$ de tout message m est donnée par la formule:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \times \log_2 \frac{1}{p(m_i)} \tag{3.10}$$

TABLE 3.4: Résultats comparatifs en termes de coefficient de corrélation des images de test.

C.C	**Tchebichef**	**Krawtchouk**	**Racah**	**Hahn**	**Dual Hahn**	**DCT**	**Ref [141]**	**Ref [29]**
Lena	0,00043491	-0,0063	0,0021	0,00046734	0,0036	0,0021	-0,0023	0,004
Baboon	0,0066	0,0098	-0,0015	0,0037	0,0064	-0,0044	0,0071	0,0074
cameraman	0,0046	-0,00075892	0,0034	-0,0018	0,0019	0,0054	-0,0091	0,0071
Boats	-0,0029	-0,0102	0,0022	-0,0024	0,00023248	0,0029	-0,0052	0,0087
Livingroom	-0,0012	-0,0041	-0,0023	0,00097113	-0,001	-0,0033	0,0033	0,0027
D22	0,0051	0,0022	0,0053	0,0017	0,0076	-0,0049	-0,0096	-0,0081
D35	-0,004	-0,0012	0,00056295	-0,0007745	-0,0057	-0,001	0,0017	-0,0054
D36	-0,0052	-0,0066	-0,002	-0,0019	-0,0062	-0,0027	-0,0034	-0,0041
D41	-0,000018699	0,0038	0,0078	0,001	0,0055	0,0016	-0,0059	0,0037
D52	-0,0081	-0,00010628	-0,007	-0,0032	-0,0034	0,0038	0,0053	-0,0091
D66	0,00058458	-0,0025	-0,0041	-0,0043	-0,0014	-0,0052	-0,0056	-0,0054
D67	-0,0036	-0,0049	-0,0017	-0,0048	-0,0069	-0,0066	0,0073	0,0064

TABLE 3.5: Résultats comparatifs en termes d'entropie des images de test.

Entropy	**Tchebichef**	**Krawtchouk**	**Racah**	**Hahn**	**Dual Hahn**	**DCT**	**Ref [141]**	**Ref [29]**
Lena	7,9946	7,9953	7,9955	7,9955	7,9953	7,9945	7,9943	7,9946
Baboon	7,995	7,9956	7,9958	7,9956	7,9952	7,9948	7,9945	7,9944
cameraman	7,9944	7,9953	7,9955	7,9955	7,9951	7,9947	7,9938	7,9934
Boats	7,9946	7,9954	7,9955	7,9956	7,9953	7,9949	7,994	7,9943
Livingroom	7,9945	7,9953	7,9955	7,9956	7,9953	7,9949	7,9943	7,9933
D22	7,9952	7,9957	7,9958	7,9954	7,9954	7,9952	7,9951	7,995
D35	7,9952	7,9956	7,9959	7,9957	7,9955	7,9949	7,9929	7,9944
D36	7,9955	7,9955	7,9957	7,9955	7,9955	7,9951	7,9936	7,9945
D41	7,9953	7,9956	7,9957	7,9956	7,9956	7,9951	7,9938	7,9947
D52	7,9954	7,9956	7,9958	7,9956	7,9956	7,9947	7,9944	7,9947
D66	7,9955	7,9956	7,9957	7,9954	7,9954	7,9952	7,9952	7,9949
D67	7,9954	7,9955	7,9957	7,9956	7,9956	7,9953	7,9949	7,9944

Où $p(m_i)$ est la probabilité d'occurrence du symbole m_i. Un chiffrement d'image parfait - s'il existe - devrait avoir une valeur d'entropie de 8 et est considéré comme ne fournissant aucune information sur l'image originale [131]. Pour démontrer la sécurité des méthodes proposées par rapport à la mesure de l'entropie. Nous chiffrons chaque image représentée sur la figure 3.3, en utilisant les algorithmes de chiffrement de Tchebichef, Krawtchouk, Racah, Hahn et Dual Hahn, nous calculons l'entropie des images chiffrées et nous comparons les résultats avec l'entropie obtenue par l'algorithme de chiffrement DCT et les algorithmes de [29, 141]. Les résultats sont présentés dans le tableau 3.5. Les résultats présentés dans le tableau 3.5 montrent clairement que tous les algorithmes mis en œuvre donnent une valeur élevée d'entropie, c'est-à-dire proche de 8, ce qui témoigne d'une grande efficacité de ces algorithmes. En outre, il convient de mentionner que la plupart des algorithmes de chiffrement basés sur les moments surpassent l'algorithme de chiffrement basé sur la DCT et les algorithmes de pointe, en particulier pour les images hautement texturées, à savoir D22, D35, D36, D41, D52, D66 et D67.

Dans ce manuscrit, nous avons proposé un nouvel ensemble d'algorithmes de chiffrement d'images basé sur les moments orthogonaux discrets combinés à la théorie du chaos. Plusieurs expériences ont été utilisées pour mesurer la qualité de chiffrement des algorithmes proposés. Nous avons effectué une comparaison avec un algorithme similaire fonctionnant dans le domaine DCT et certains algorithmes de pointe en termes d'entropie, d'analyse différentielle de l'espace des clés et d'attaques statistiques. Il convient de mentionner que, dans la plupart des expériences, les algorithmes proposés donnent des résultats satisfaisants et surpassent l'algorithme de chiffrement basé sur la DCT et les méthodes l'état de l'art, en particulier pour les images très texturées.

3.4.5 Chiffrement sélectif des images basé sur le chaos et les moments de Tchebichef

Dans cette section, un nouveau schéma de chiffrement est introduit basé sur le chaos et les moments de Tchebichef, le schéma proposé est basé sur le chiffrement sélectif, ce qui le rend extrêmement rapide sans compromettre l'aspect sécurité. Dans la suite, nous expliquons en détail l'algorithme de chiffrement.

Chiffrement

Segmentation et sous-échantillonnage : Tout d'abord, l'image est segmentée en blocs 8 * 8, puis nous calculons les coefficients des moments pour chaque bloc. Afin d'accélérer le processus de chiffrement, nous sous-échantillonnons les coefficients de la matrice dans une matrice de 3 * 3. Ces coefficients englobent la plupart des informations et l'image peut donc être représentée par ce sous-échantillon sans grande perte.
Génération de la clé : K est une clé de longueur 128 bits, qui est divisée en 2 segments : K_1 et K_2.La carte logistique utilisée pour le chiffrement a en entrée une valeur comprise entre 1 et 0. Nous appliquons certaines opérations sur les segments de la clé afin de les adopter à l'entrée de la carte logistique. Chaque segment Ki est présenté par sa forme binaire qui peut être notée comme suit : $K_1 = K_{11}, K_{12}...K_{164}.K_2 = K_{21}, K_{22}...K_{264}$. Les valeurs d'entrée pour les cartes logistiques sont calculées comme suit : $X_0 = (K_{11}2^0 + K_{12}2^1 + ... + K_{164}2^{63})/2^{64}$. $Y_0 = (K_{21}2^0 + K_{22}2^1 + ... + K_{264}2^{63})/2^{64}$ Où X_0 et Y_0 sont les entrées pour les cartes logistiques X et Y.
Confusion : Nous utilisons la carte logisitique X avec l'entrée X0 pour générer une séquence de taille 96*96. La matrice dérivée de l'étape 1 est transformée en un tableau de taille 9216 (96*96). Ce tableau est permuté selon la carte générée par X.
Diffusion : Une autre séquence aléatoire est générée à partir de Y avec la condition initiale Y_0. Puis cette séquence est soumise à un test XOR avec le tableau généré à l'étape 3. Le résultat est l'image chiffrée E.

Déchiffrement

Le déchiffrement est le processus inverse du chiffrement, le but est de reconstruire l'image originale à partir de l'image chiffrée. Tout d'abord, nous convertissons l'image chiffrée E en un tableau de taille 96*96. Ce tableau est ensuite soumis à un test XOR avec la séquence générée par Y avec la condition initiale Y0. Nous permutons le tableau résultant selon la séquence générée par X avec la condition initiale X0. Ce tableau est transformé en une matrice 256*256 par échantillonnage, c'est-à-dire que les pixels restants sont mis à zéro. Ensuite, nous calculons les moments de Tchebichef inverse. On obtient ainsi l'image déchiffrée I'.

3.4.6 Étude expérimentale

Nous présentons les résultats de nos expériences dans cette section. Notre algorithme est comparé à des algorithmes de pointe pour prouver son efficacité. Les résultats de ces expériences sont donnés ci-dessous

Analyse des espaces clés

Pour un schéma de chiffrement sécurisé, l'espace clé doit être supérieur à 2^{100} [6]. L'algorithme proposé a 2^{128} combinaisons possibles de la clé de chiffrement.

Similitude d'image

La méthode proposée est un chiffrement d'image "avec perte" puisqu'elle ne prend en compte que les bits les plus significatifs dans le processus de chiffrement. Pour

TABLE 3.6: Résultats MSE

MSE	Tchebichef	RefRef[222]	Ref[220]	Ref[198]
Lena	2.1 x 10-3	0	0	0
Baboon	1.6 x 10-4	0	0	0
Cameraman	7.3 x 10-4	0	0	0

TABLE 3.7: Résultats du coefficient de corrélation

C.C	Plain image	Tchebichef	Ref[222]	Ref[220]	Ref[198]
Horizontal	0.8263	0.039	-0.0025	-0.088	0.0039
Vertical	0.9273	-0.0078	0.00126	0.079	0.002
Diagonal	0.867	0.046	-0.006	0.096	0.076

mesurer la "perte" pendant la reconstruction/déchiffrement de l'image, nous utilisons l'erreur quadratique moyenne (MSE), que nous avons définie comme suit :

$$MSE = \frac{1}{NM} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} [f(x,y) - g(x,y)]^2 \tag{3.11}$$

f(x,y) est l'image originale et g(x,y) est l'image déchiffrée de taille M *N. Les algorithmes des références [222, 220, 198] sont des algorithmes sans perte, ce qui explique la valeur 0 du MSE, c'est-à-dire que l'image déchiffrée correspond parfaitement à l'image originale. Cependant, dans l'algorithme proposé, certaines informations sont perdues en raison du processus de chiffrement sélectif. Par ailleurs, les valeurs du MSE pour les algorithmes proposés sont proches de 0, ce qui signifie que l'image originale et l'image déchiffrée sont similaires et que la différence est imperceptible à l'œil nu.

Coefficient de corrélation

Les résultats sont présentés dans le tableau 3.7. Nous calculons le coefficient de corrélation pour les pixels verticaux, horizontaux et diagonaux. Il ressort clairement des résultats que le coefficient de corrélation est proche de 0 pour tous les algorithmes, y compris l'algorithme proposé, ce qui montre que les algorithmes sont sûrs contre les attaques statistiques.

Analyse différentielle : NPCR et UACI

Nous chiffrons les images de Lena, Baboon et Cameraman en utilisant l'algorithme proposé et nous comparons les résultats aux algorithmes de pointe. D'après les tableaux 3.8 et 3.9 , les valeurs NPCR pour les algorithmes proposés sont toutes supérieures à 99,8 et les valeurs UACI sont d'environ 31, ce qui implique que notre algorithme est sûr contre les attaques différentielles. De plus, comparé aux autres algorithmes, il présente une bonne performance de sécurité.

Entropie

Les résultats sont présentés dans le tableau 3.10, les valeurs d'entropie pour les images chiffrées sont toutes supérieures à 7,99, ce qui signifie que tous les algorithmes

TABLE 3.8: Résultats NPCR

NPCR	Tchebichef	Ref[222]	Ref[220]	Ref[198]
Lena	99.8731	99.9961	99.9961	99.9955
Baboon	99.9289	99.9953	99.996	99.9958
Cameraman	99.8149	99.9959	99.996	99.9956

TABLE 3.9: Résultats UACI

UACI	Tchebichef	Ref[222]	Ref[220]	Ref[198]
Lena	31.712	33.232	33.198	33.174
Baboon	31.039	33.161	33.166	33.255
Cameraman	26.140	33.332	33.212	33.26

passent le test d'entropie. De plus, nous constatons que notre algorithme présente de bons résultats par rapport aux autres algorithmes.

Analyse de la vitesse

Notre principale contribution consiste à développer un algorithme de chiffrement léger, à la fois rapide et sûr. Afin de valider l'aspect de performance temporelle de notre schéma proposé, nous analysons la performance temporelle avec différentes tailles d'images, c'est-à-dire 256×256, 512 × 512 et 1024 × 1024 et comparons les résultats avec d'autres algorithmes. Les résultats sont présentés dans le tableau 3.11. Le schéma de chiffrement proposé est basé sur le chiffrement sélectif, ce qui le rend extrêmement rapide par rapport aux autres algorithmes. Le tableau 3.11 montre clairement que l'algorithme que nous proposons surpasse les algorithmes de pointe en termes de performance temporelle.

3.5 Conclusion

Dans ce travail, proposons un nouvel ensemble d'algorithmes de chiffrement basés sur les moments orthogonaux. Cinq algorithmes basés sur les moments de: Tchebichef, Krawtchouk, Hahn, Dual Hahn et Racah. Les algorithmes proposés ont prouvé des bons résultats par rapport aux algorithmes de l'état de l'art.

Dans une deuxième partie, nous introduisons un nouveau schéma de chiffrement sélectif basé sur les moments de Tchebichef et la théorie du chaos. Notre objectif principal était de proposer un algorithme de chiffrement rapide qui peut être déployé dans des applications du monde réel sans nuire à l'aspect sécuritaire. Nous y sommes parvenus en ne chiffrant que les bits les plus significatifs dans le domaine de transformation des moments de Tchebichef. L'algorithme de chiffrement est un algorithme "avec perte", ce qui signifie que l'image déchiffrée n'est pas similaire à

TABLE 3.10: Résultats de l'entropie

Entropy	Tchebichef	Ref[222]	Ref[220]	Ref[198]
Lena	7.9924	7.9964	7.9967	7.996
Baboon	7.996	7.9959	7.9963	7.9961
Cameraman	7.9926	7.9961	7.996	7.9952

TABLE 3.11: Résultats pour le temps de calcul

Speed Analysis	Tchebichef	Ref[222]	Ref[220]	Ref[198]
256 * 256	0.138	0.46	0.442	0.11794
512 * 512	0.330	0.979	0.466	0.27444
1024 * 1024	0.480	1.1361	0.975	0.78902

100% à l'image originale, mais la mesure de similarité montre qu'elle est suffisamment proche pour ne pas être remarquée à l'œil nu. Les résultats expérimentaux ont montré que notre schéma de chiffrement est sûr contre toutes les attaques connues, de plus l'analyse de la vitesse a prouvé que l'algorithme proposé surpasse les algorithmes de l'état de l'art. Compte tenu des résultats présentés de l'algorithme proposé, nous sommes confiants quant à sa capacité à être déployé dans des applications du monde réel.

Chapitre 4

Schéma de chiffrement chaotique rapide basé sur les moments séparables et le calcul parallèle

4.1 Introduction

La cybersécurité joue un rôle énorme dans le monde d'aujourd'hui, alors que les réseaux étendent l'interconnexion des systèmes d'information du monde, la sécurité de l'information est devenue une question d'intérêt et d'importance mondiale. Son objectif est d'assurer la continuité des activités et de minimiser les dommages causés aux entreprises en limitant l'impact des incidents de sécurité [211]. Dans la norme ISO/IEC 27002 (2005) [212], la sécurité des informations est définie comme la préservation de la confidentialité, de l'intégrité et de la disponibilité des informations. Le triangle CID est la norme industrielle pour les caractéristiques des informations qui doivent être protégées [212]. Le problème de la confidentialité peut être résolu par le chiffrement [212]. Le chiffrement protège la confidentialité des données en transformant l'information (texte clair) en une forme inintelligible (texte chiffré) à l'aide d'algorithmes mathématiques et d'une information secrète (clé) [77]. Ainsi, si une entité non autorisée a accès au dispositif de stockage ou au canal de communication, elle ne peut pas voir les données cachées.

Bien que les techniques de chiffrement puissent être utilisées pour tout type de données, le chiffrement d'images présente des difficultés particulières par rapport au chiffrement de texte en raison de certaines caractéristiques intrinsèques des images, telles que la capacité de données en masse et la corrélation élevée entre les pixels. Ainsi, les chiffrements traditionnels tels que DES, IDEA et RSA ne sont pas adaptés au chiffrement pratique des images, car ils nécessitent un temps de calcul important et des ressources informatiques élevées [129, 259]. Ces dernières années, différents algorithmes ont été spécifiquement conçus pour le chiffrement d'images [253, 128, 250]. Ces algorithmes peuvent être classés en deux catégories : les algorithmes fonctionnant dans le domaine spatial et les algorithmes fonctionnant dans le domaine fréquentiel [101, 140, 90, 91]. Si les premiers ont tendance à être une approche plus "directe", puisqu'ils manipulent directement les pixels de l'image, ils présentent un inconvénient en provoquant une non-corrélation entre les pixels et en rendant ainsi l'image chiffrée incompressible [99]. Les derniers algorithmes, au lieu de manipuler les pixels de l'image, traitent les coefficients obtenus dans le domaine de la transformation, ces algorithmes ont été signalés comme ayant une plus grande efficacité, ils sont plus robustes contre les opérations de traitement d'image et peuvent faire une récupération sans perte de l'image originale [74, 137].

Un problème courant dans le domaine du chiffrement d'images est le dilemme vitesse/sécurité [219]. Bien que les algorithmes récemment proposés aient tendance à être de plus en plus sécurisés, ils ont un coût, à savoir la vitesse de calcul [98, 275]. En fait, les algorithmes basés sur le chaos -qui sont les schémas prédominants dans le domaine du chiffrement d'images- sont généralement un "processus basé sur deux étapes", à savoir la confusion et la diffusion. Ces deux étapes séparées sont répétées jusqu'à ce qu'un niveau de sécurité satisfaisant soit obtenu [179]. Plus ces étapes sont répétées, plus l'algorithme est sûr, et plus il est lent [179, 103]. Plusieurs travaux ont été introduits afin d'améliorer les performances temporelles des algorithmes de chiffrement d'images tout en conservant un niveau de sécurité requis [226, 185, 98, 228]. Bien que ces travaux présentent de nombreuses améliorations pour résoudre le dilemme mentionné ci-dessus, ils ne sont pas adaptés aux applications du monde réel, car ils nécessitent des paramètres spécifiques ou sont encore limités en termes de performances temporelles pour les scénarios du monde réel. Ainsi, notre travail vise à résoudre le problème mentionné ci-dessus en présentant un algorithme de chiffrement rapide et sécurisé basé sur le chaos et le calcul parallèle. Dans ce travail, nous avons choisi d'utiliser les moments séparables comme domaine de transformation pour le chiffrement. Ce choix est motivé par les résultats remarquables obtenus dans différents domaines du traitement d'images [243, 11, 235]. En fait, la théorie des moments a été introduite dans le domaine du chiffrement d'images et a donné des résultats remarquables [89, 144, 134]. Dans [101], nous avons fait une première tentative pour explorer l'utilisation du domaine de transformation des moments pour le chiffrement. Dans ce travail, nous avons utilisé une carte logistique pour confondre et ensuite diffuser les coefficients des moments obtenus en utilisant : Tchebichef, Krawtchouk, Hahn, Dual Hahn et Racah. Nous avons soutenu que les algorithmes de chiffrement basés sur les moments sont plus performants que les méthodes les plus récentes [101]. Récemment, une nouvelle famille de moments appelée moments séparables [271] a été proposée, l'image est représentée comme le produit tensoriel de deux polynômes orthogonaux différents ou identiques dans une variable. Les auteurs ont proposé de nouvelles fonctions de base pour les moments orthogonaux bidimensionnels, comme un produit de moments orthogonaux bien connus. Ils affirment que les moments séparables (SM) parviennent à adopter les propriétés des deux polynômes sur lesquels ils sont définis [271, 206] . Un certain nombre de ces moments proposés ont donné de meilleurs résultats que les moments originaux [206]. Depuis leur introduction, différentes variantes des moments séparables ont été proposées, traitant de différentes configurations [11, 180, 243].

Dans ce manuscrit, nous proposons trois nouveaux algorithmes de chiffrement basés sur les moments séparables et le chaos. Nous proposons un nouveau schéma qui permet à plusieurs étapes de s'exécuter simultanément. Nous ajoutons une nouvelle étape dans le processus de chiffrement appelée "permutation des blocs". Différents threads exécutent les étapes simultanées en utilisant le calcul parallèle. Par conséquent, les résultats expérimentaux montrent que le coût de calcul est considérablement amélioré tout en améliorant les performances de sécurité des algorithmes proposés. Les trois algorithmes proposés sont basés sur le même schéma ; ils diffèrent par la fonction de moments séparables utilisée. Nous étudions en particulier les combinaisons : moments de Tchebichef-Krawtchouk (TKM), moments de Tchebichef-Hahn (THM) et moments de Krawtchouk-Hahn (KHM), le choix de ces moments particuliers est justifié par les résultats présentés dans [101]. En effet, les moments de Tchebichef, Krawtchouk et Hahn ont été les transformations les plus prometteuses en termes de performance de sécurité. Nos contributions dans ce manuscrit sont résumées comme suit :

- Améliorer la sécurité des algorithmes de chiffrement en ajoutant une nouvelle couche de sécurité au schéma classique (confusion / diffusion), à savoir la permutation de blocs.
- Proposer un schéma basé sur le calcul parallèle qui permet d'exécuter plusieurs étapes simultanément, ce qui réduit le coût en temps des algorithmes proposés.
- Introduire les moments SM dans le domaine du chiffrement d'images.

Nous avons organisé le reste de ce document de la manière suivante : le contexte de la théorie des moments séparables et de la théorie du chaos est présenté dans la section 2. La section 3 présente les détails des algorithmes proposés. L'efficacité de ces algorithmes est démontrée dans la section 4 par des résultats expérimentaux. Enfin, une conclusion est tirée dans la section 5.

4.2 Connaissances pertinentes

4.2.1 Moments séparables

Hu [89] a introduit pour la première fois les moments d'image dans l'analyse d'image en 1961, il a proposé des moments géométriques pour la reconnaissance des formes. Ces moments ne sont pas orthogonaux, ce qui entraîne une redondance de l'information. Pour surmonter cet inconvénient, Teague [203] a proposé des moments avec des fonctions de base orthogonales, à savoir : Legendre et Zernike. Bien que ces moments permettent une redondance minimale de l'information, ils présentent certains inconvénients dus à leur continuité [155, 250] tels que l'approximation numérique des intégrales continues, une grande variation dans la gamme dynamique des valeurs et la transformation de l'espace des coordonnées. Pour éliminer ces erreurs, les moments orthogonaux discrets tels que Tchebichef [155] Krawtchouk [250] et Hahn [270] ont été introduits dans l'analyse d'image. Les fonctions de base de ces algorithmes satisfont à la propriété d'orthogonalité, ce qui permet d'obtenir une représentation supérieure de l'image. En effet, il semble encourageant de produire de nouvelles familles de moments en combinant des polynômes orthogonaux discrets séparables [206].

Les moments séparables ont été récemment introduits par Zhu [271]. Ils sont construits en combinant différents polynômes orthogonaux continus ou discrets. Les SM parviennent à adopter des propriétés des deux polynômes sur lesquels ils sont définis [271].La formule générale pour calculer les moments orthogonaux discrets d'ordre n et de répétition m est la suivante :

$$M_{nm} = NF \times \sum_{i=1}^{N} \sum_{j=1}^{N} kernel_{nm}(x_i, y_j) \times f(x_i, y_j) \tag{4.1}$$

Où $kernel_{nm}$ est le noyau des moments qui consiste en des polynômes spécifiques d'ordre n et de répétition m et il constitue la base orthogonale. $f(x, y)$ est l'image originale de taille N × N et NF est le facteur de normalisation. Les coefficients de chaque famille de moments peuvent être calculés à l'aide du noyau et du NF correspondants.

L'image originale peut être reconstruite à partir des coefficients des moments en utilisant la formule :

$$F(x_i, y_j) = \sum_{n=1}^{N} \sum_{m=1}^{N} kernel_{nm}(x_i, y_j) \times M_{nm} \tag{4.2}$$

Les propriétés des moments séparables utilisés dans ce manuscrit sont résumées dans le tableau 4.1.

4.2.2 Carte logistique

Les systèmes de chiffrement du chaos sont largement utilisés dans le domaine du chiffrement d'images en raison de leur ergodicité, de leur dépendance sensible aux conditions initiales et aux paramètres de contrôle. Le schéma classique des algorithmes de chiffrement basés sur le chaos est illustré à la figure 4.1. L'algorithme de chiffrement comprend deux étapes principales, à savoir la confusion et la diffusion. Dans l'étape de confusion, les pixels sont permutés selon une carte chaotique pseudo-aléatoire, cette étape répand l'information dans l'image, ce qui relâche la dépendance entre les pixels de l'image. Dans l'étape de diffusion, les valeurs des pixels sont modifiées, rendant l'image méconnaissable.
Les cartes logistiques sont les cartes chaotiques les plus utilisées pour la génération de séquences aléatoires dans les algorithmes de chiffrement basés sur le chaos en raison de leur faible complexité, ce qui les rend appropriées pour concevoir une architecture rapide de chiffrement d'images [231]. La carte logistique est définie comme suit,

$$x_{n+1} = \mu x_n(1 - x_n) \quad x_n \epsilon (0, 4] \tag{4.3}$$

x_n est la variable d'état, n le nombre d'itérations et μ est un paramètre dans l'intervalle de paramètres $(0, 4)$. Le diagramme de bifurcation de la carte logistique est représenté dans le graphique 4.2. Lorsque μ est aux alentours de 3,57, la carte logistique présente

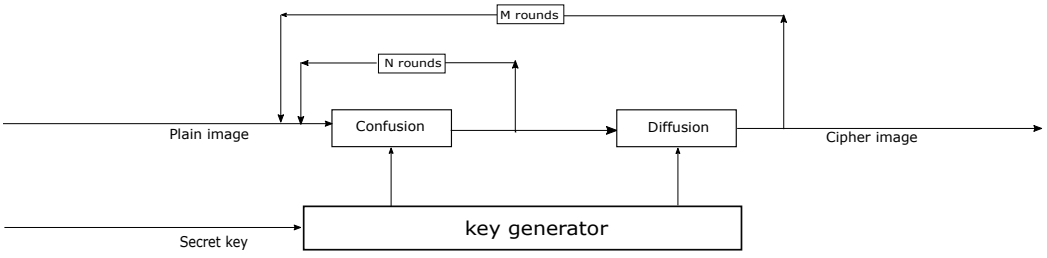


FIGURE 4.1: Schéma général pour le chiffrement basé sur le chaos

un comportement chaotique. Dans cette région, de légères variations des conditions initiales conduisent à des résultats très différents. Dans ce document, nous fixons le paramètre $\mu = 3,999$ ayant des exposants de Lyapunov positifs, comme le montre la figure 4.3.

4.3 Les algorithmes de chiffrement proposés

Dans cette section, nous présentons une vue d'ensemble, étape par étape, des algorithmes proposés. Trois algorithmes sont proposés, qui diffèrent par les fonctions

TABLE 4.1: propriétés des moments séparables utilisés

Moments	Kernel	Forme polynomial
TKM	$t_n(x) \times K_m(y; p_2, N)$	$t_n(x) = (1-N)_n {}_3F_2(-n, -x, 1+n; 1, 1-N; 1)$, $K_m(x; p, N) = \sum_{k=0}^{N} a_{k,m,p} x^k$
THM	$t_n(x) \times h_m^{\mu,\nu}(x, N)$	$t_n(x) = (1-N)_n {}_3F_2(-n, -x, 1+n; 1, 1-N; 1)$, $h_m^{(u,v)}(x, N) = (N+\nu-1)_m (N-1)_m$ $\times \sum_{k=0}^{m} (-1)^k \frac{(-m)_k (-x)_k (2N+\mu+\nu-m-1)_k}{(N+\nu-1)_k (N-1)_k} \frac{1}{k!}$
KHM	$K_n(y; p_2, N) \times h_m^{\mu,\nu}(x, N)$	$K_n(x; p, N) = \sum_{k=0}^{N} a_{k,n,p} x^k$, $h_m^{(u,v)}(x, N) = (N+\nu-1)_m (N-1)_m$ $\times \sum_{k=0}^{m} (-1)^k \frac{(-m)_k (-x)_k (2N+\mu+\nu-m-1)_k}{(N+\nu-1)_k (N-1)_k} \frac{1}{k!}$

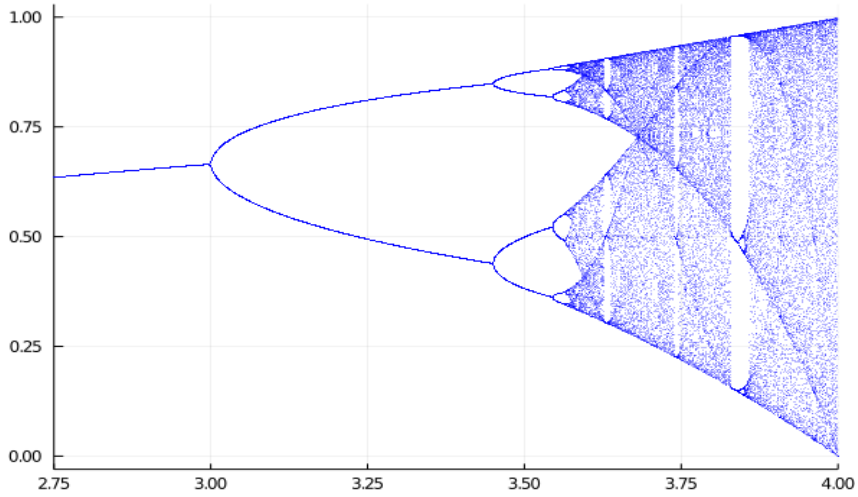


FIGURE 4.2: Diagramme de bifurcation pour la carte logistique

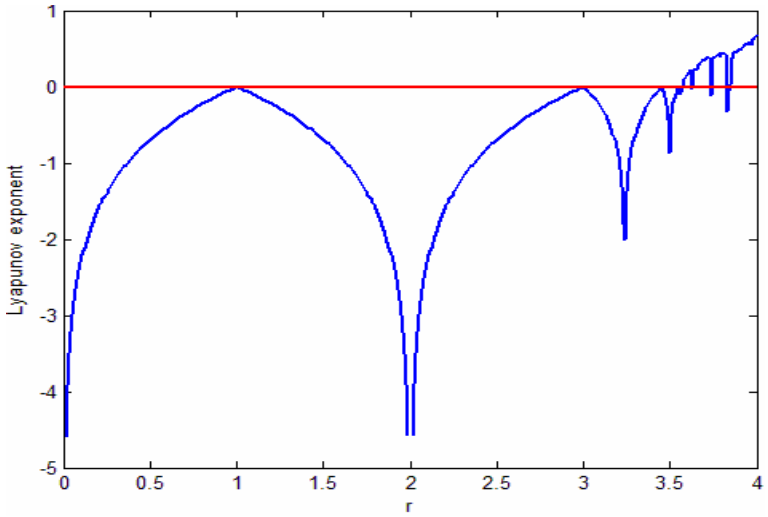


FIGURE 4.3: Exposant de Lyapunov avec $\mu = 3.999$

de moments utilisées comme domaine de transformation. Sans perte de généralité, une tentative a été faite pour explorer l'utilisation de moments séparables comme domaine de transformation pour le chiffrement. Les auteurs ont étudié en particulier les combinaisons : TKM, THM, KHM, le choix de ces moments particuliers est justifié par les résultats présentés dans [101]. En fait, les moments de Tchebichef, Krawtchouk et Hahn étaient les plus prometteurs en termes de performance de sécurité.

Le schéma proposé permet de réduire le temps de calcul sans nuire aux performances de sécurité. En fait, par rapport aux schémas de chiffrement classiques [101, 176, 88], une couche supplémentaire de sécurité a été ajoutée, à savoir la permutation des blocs. En outre, l'une de nos principales contributions dans ce document est de proposer un schéma de chiffrement dont les étapes sont exécutées simultanément. Ainsi, le calcul parallèle est utilisé pour mettre en œuvre les algorithmes proposés. À cet égard, la représentation de l'image dans le domaine de la transformation des moments et la permutation des blocs sont effectuées simultanément et sont exécutées par deux threads différents. De plus, les étapes de confusion et de diffusion des pixels sont effectuées séparément par deux autres threads. L'implémentation détaillée

des algorithmes proposés est décrite ci-dessous.

4.3.1 Chiffrement

Le schéma général de chiffrement utilisé dans les algorithmes proposés est représenté dans la figure 4.4. Le processus de chiffrement est divisé en deux étapes principales, à savoir le calcul des moments, la permutation des blocs et la confusion/diffusion. Chaque étape est composée de deux sous-étapes qui sont réalisées séparément et donc exécutées par des threads différents.

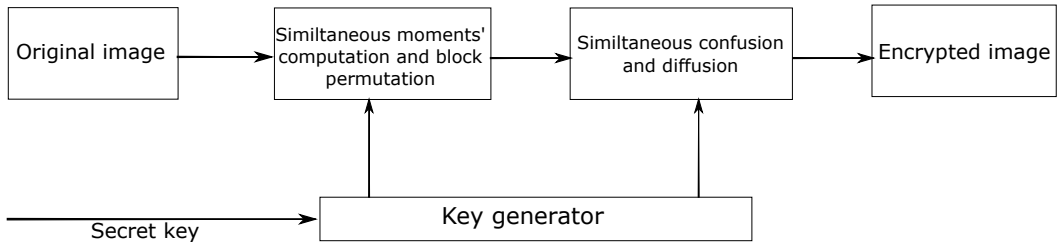


FIGURE 4.4: Le schéma de chiffrement proposé

Étape 1 *Génération de la clé* : Nous utilisons une clé externe K de longueur 192 bits, la clé est divisée en 3 segments : K1, K2 et K3. Ces segments sont utilisés comme conditions initiales pour les cartes logistiques impliquées dans le processus de chiffrement. Les cartes logistiques prennent une valeur initiale entre 0 et 1, donc afin d'adapter les segments K1, K2 et K3 comme conditions initiales, nous effectuons les opérations mathématiques suivantes :
Nous notons chaque segment Ki sous sa forme binaire :$K_1 = K_{11}, K_{12} \dots K_{164}$. $K_2 = K_{21}, K_{22} \dots K_{264}$. $K_3 = K_{31}, K_{32} \dots K_{364}$. Ensuite, les valeurs initiales des cartes logistiques sont calculées comme suit :

$X_0 = (K_{11} \times 2^0 + K_{12} \times 2^1 + \dots + K_{164} \times 2^{63})/2^{64}$
$Y_0 = (K_{21} \times 2^0 + K_{22} \times 2^1 + \dots + K_{264} \times 2^{63})/2^{64}$
$Z_0 = (K_{31} \times 2^0 + K_{32} \times 2^1 + \dots + K_{364} \times 2^{63})/2^{64}$

Où X_0 ; Y_0 et Z_0 sont les valeurs initiales des cartes logistiques X ; Y et Z respectivement
Étape 2 *Génération de séquences aléatoires* : Trois cartes logistiques sont utilisées, X, Y et Z, pour générer des séquences aléatoires. Les séquences générées sont utilisées respectivement pour la permutation des blocs, la permutation des pixels et la diffusion des pixels.

i. En utilisant la carte logistique X et la valeur initiale X0, générer une séquence aléatoire L de taille $l (l = [M \times N \times 5] = 64$ basé sur l'expérience). Pour que la séquence L convienne à la permutation par blocs, nous effectuons les opérations suivantes :

   (a) $L'_i = [L_i \times 10^{14}] mod(NB)$; où NB = Nombre de blocs 8 × 8 dans l'image, c'est-à-dire M × N=64.

   (b) Supprimer tous les doublons de L0.

   (c) Réduire la taille de L0 à NB.

ii. En utilisant la carte logistique Y et la valeur initiale Y0, générer une séquence aléatoire T de taille t (t = M × N × 3 basé sur l'expérience).

   (a) $T'_i = [T_i \times 10^{14}] mod(M \times N)$ où M et N sont les dimensions de l'image d'entrée.

   (b) Suppression des doublons de T 0.

   (c) Réduire la taille de T 0 à M × N.

iii. En utilisant la carte logistique Z et la valeur initiale Z0, générer une séquence aléatoire S de taille S = M × N.

Étape 3 *Permutation des blocs et calcul des moments* :
Entrée : image I de taille M × N, L (séquence aléatoire générée à l'étape 2).
Sortie : Matrice B de taille M × N
- Ajustez la taille de l'image si le nombre total de pixels n'est pas un multiple de 64.
- Partitionner l'image en P blocs de taille 8 × 8.
- Pour chaque bloc i :
Thread 1 : calculer les coefficients des moments en utilisant les moments séparables correspondants, à savoir, TKM (Tchebichef Krawtchouk moments), THM (Tchebichef Hahn moments) et HKM (Hahn Krawtchouk moments).
Thread 2 : changer la position du bloc en Li.
Stocker le bloc à la position Li dans la matrice B.
Étape 4 *Processus de confusion / diffusion* :
Entrée : matrice B, S et T (séquences aléatoires générées à l'étape 2).
Sortie : E image chiffrée.
- Convertir l'image dans un tableau A de taille M × N.
- Pour chaque pixel j :
Thread 1 : diffusion, changer la valeur du pixel selon Aj XOR Tj.
Thread 2 : confusion : Changez la position du pixel en Sj.
- Stocker la valeur calculée à la position Sj dans la matrice E.

4.3.2 Déchiffrement

Le déchiffrement est la procédure inverse du chiffrement qui - avec la clé appropriée - permet de récupérer l'image originale à partir de l'image chiffrée. La procédure de déchiffrement est similaire au processus de chiffrement, sauf que certaines étapes sont inversées.
Étapes 1 et 2 : La même clé de chiffrement générée à l'étape 1 et les séquences aléatoires générées à l'étape 2 des algorithmes de chiffrement sont utilisées pour le processus de déchiffrement.
Étape 3 : Inversion du processus de diffusion de la confusion.
Entrée : E image chiffrée, S et T (séquences aléatoires générées à l'étape 2).
Sortie : Matrice F.
- L'image est transformée en un tableau de taille M × N noté W.
Thread 1 : changement de la valeur du pixel selon Wi XOR Ti.
Thread 2 : modifier la position du pixel en fonction de Si.
- Inversez le tableau calculé en une matrice F de taille M × N.
Étape 4 : permutation des blocs inversés et calcul des moments inverses.
Entrée : matrice F, L (séquence aléatoire générée à l'étape 2).
Sortie : D image déchiffrée.
- Diviser l'image en blocs de taille 8 × 8 et pour chaque bloc j :
Thread 1 : calculer les moments inverses.

Thread 2 : modifier la position du bloc en fonction de L.
- Stocker les blocs calculés dans D
Le schéma de déchiffrement est résumé dans la figure 4.5 :

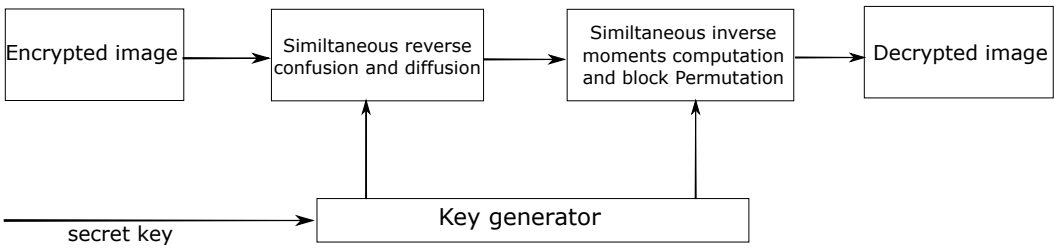


FIGURE 4.5: Le schéma de déchiffrement

4.4 Étude expérimentale

Dans cette section, nous validons les performances des algorithmes proposés en effectuant plusieurs tests. Nous utilisons cinq images connues en niveaux de gris : "Lena", "Baboon", "Cameraman", "Boats", et "Livingroom" de taille 512×512. Les résultats sont ensuite comparés aux algorithmes les plus avancés de [222, 220, 198, 101]. Tous les algorithmes sont mis en œuvre à l'aide de MATLAB 11 sur un ordinateur portable avec un processeur Intel Core i7, 2,7 GHz, 8 gigaoctets de mémoire et un disque dur de 256 gigaoctets fonctionnant sous Windows 10. Les analyses de la sécurité et des performances sont données ci-dessous.

4.4.1 Analyse des espaces clés

Un schéma de chiffrement sûr doit être sensible à la clé de chiffrement, l'espace des clés doit être suffisamment grand pour rendre l'attaque par force brute infaisable. L'espace clé des algorithmes proposés est suffisamment grand pour le rendre sûr contre les attaques par force brute. L'espace clé total est de 2^{192}, ce qui est sûr puisque l'espace clé est plus grand que 2^{100} [6].

4.4.2 Attaques différentielles

Nous chiffrons les images de test énumérées dans la figure 4.6 en utilisant l'algorithme de chiffrement proposé. Nous changeons la valeur d'un pixel dans l'image brute et la chiffrons à nouveau en utilisant les mêmes algorithmes. Les résultats sont présentés dans les tableaux 4.2 et 4.3 en comparaison avec les algorithmes les plus récents.

Les tableaux 4.2 et 4.3 montrent que tous les algorithmes produisent des résultats proches des valeurs optimales. De plus, les algorithmes proposés ont démontré de meilleurs résultats en termes d'UACI et de NPCR par rapport aux algorithmes de l'état de l'art, ce qui les rend plus sûrs contre les attaques différentielles.

TABLE 4.2: Résultats NPCR pour les algorithmes proposés par rapport aux algorithmes de l'état de l'art

NPCR	Prop. TKM	Prop. THM	Prop. KHM	Tchebichef [101]	Krawtchouk [101]	Hahn [101]	Ref [222]	Ref [220]	Ref [198]
Lena	99.8572	99.8321	99.8425	99.791	99.7559	99.7879	99.9961	99.9961	99.9955
Baboon	99.8944	99.798	99.8536	99.7955	99.8337	99.855	99.9953	99.996	99.9958
Cameraman	99.8234	99.8764	99.8896	99.7574	99.7437	99.8276	99.9959	99.996	99.9956
Boats	99.8247	99.8636	99.9005	99.7589	99.7681	99.8337	99.9955	99.9957	99.996
livingroom	99.7928	99.7779	99.7878	99.8093	99.7467	99.8276	99.9955	99.9954	99.9957

TABLE 4.3: Résultats UACI pour les algorithmes proposés par rapport aux algorithmes de l'état de l'art

UACI	Prop. TKM	Prop. THM	Prop. KHM	Tchebichef [101]	Krawtchouk [101]	Hahn [101]	Ref [222]	Ref [220]	Ref [198]
Lena	33.47	33.327	33.551	29.158	32.249	28.659	33.232	33.198	33.174
Baboon	33.462	33.541	33.35	30.44	31.773	26.813	33.161	33.166	33.255
Cameraman	33.438	33.344	33.417	26.301	29.435	27.54	33.332	33.212	33.26
Boats	33.342	33.363	33.512	25.102	27.503	25.609	33.347	33.145	33.172
livingroom	33.505	33.449	33.325	28.157	30.979	26.703	33.312	33.267	33.26

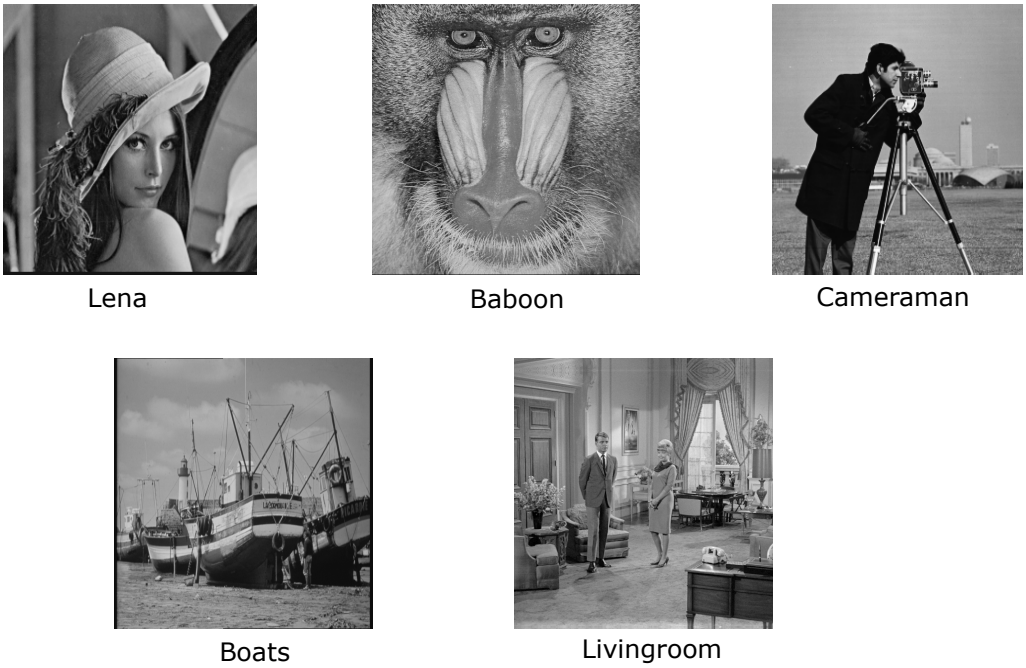


FIGURE 4.6: Images utilisées pour les expériences

4.4.3 Analyse statistique

Analyse d'histogramme

L'analyse de l'histogramme implique le comptage des distributions de fréquence des pixels de l'image. Pour une image chiffrée, plus les valeurs des pixels sont uniformément distribuées, meilleur est l'algorithme de chiffrement [198]. Un bon système de chiffrement doit cacher les propriétés statistiques de l'image chiffrée, ce qui se traduit dans un histogramme par une distribution uniforme des valeurs des pixels. Nous chiffrons l'image test "Lena" avec les trois algorithmes de chiffrement proposés, puis nous traçons les histogrammes des images chiffrées et de l'image originale. La figure 4.7 montre clairement que les histogrammes de l'image chiffrée sont presque "plats", ce qui rend ces algorithmes sûrs contre l'analyse statistique.

Corrélation des pixels adjacents

Nous calculons le coefficient de corrélation entre deux pixels verticalement adjacents, deux pixels horizontalement adjacents et deux pixels diagonalement adjacents pour l'image de Lena. Les résultats sont présentés dans le tableau 4.4.

Comme le montre le tableau des résultats, les coefficients de corrélation sont proches de 0 pour tous les algorithmes. Cependant, les algorithmes nouvellement proposés se distinguent des autres méthodes par des résultats plus proches de 0.

4.4.4 Analyse de l'entropie de l'information

Le tableau 4.5 présente une comparaison de l'entropie d'information des algorithmes proposés et des méthodes de pointe [222, 220, 198, 101]. Toutes les entropies d'information représentées dans le tableau 4.5 sont proches de 8, ce qui signifie que les images

TABLE 4.4: Coefficient de corrélation pour les algorithmes de chiffrement proposés par rapport aux algorithmes de l'état de l'art.

C.C	Plain image	P.TKM	P.THM	P.KHM	Tchebichef [101]	Krawtchouk [101]	Hahn [101]	Ref [222]	Ref [220]	Ref [198]
Horizontal	0.8263	0.00105	-0.0006	-0.003	0.0032	-0.088	0.0405	-0.0025	-0.088	0.0039
Vertical	0.9273	-0.0003	0.0007	0.0005	0.047	-0.00116	-0.0083	0.00126	0.079	0.002
Diagonal	0.867	0.001	-0.0005	0.0006	0.0088	0.021	-0.009	-0.006	0.096	0.076

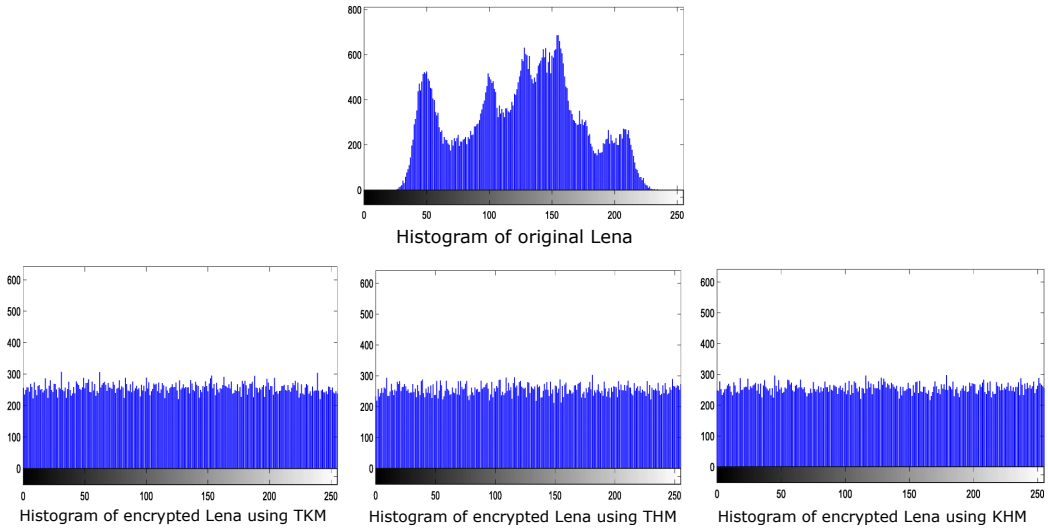


FIGURE 4.7: Analyse d'histogramme pour les algorithmes de chiffrement proposés

chiffrées sont proches d'une source aléatoire. En outre, on peut clairement voir que les algorithmes proposés sont plus performants que les méthodes de l'état de l'art.

4.4.5 Analyse de la vitesse

L'une de nos principales contributions dans ce manuscrit est de proposer un schéma de chiffrement sécurisé qui convient au calcul parallèle. En permettant aux étapes de chiffrement de s'exécuter simultanément, nous sommes en mesure de réduire considérablement la complexité temporelle sans compromettre les performances de sécurité des algorithmes proposés.

Afin de démontrer davantage la validité des algorithmes proposés, nous analysons leur complexité temporelle pour différentes tailles d'images, à savoir 128×128, 256×256, 512 × 512 et 1024 × 1024. Les résultats sont présentés dans le tableau 4.6, l'unité de temps étant la seconde.

Comme on peut le voir dans le tableau 4.6. Les algorithmes proposés montrent une amélioration importante de la complexité temporelle par rapport aux algorithmes de l'état de l'art. Le temps d'exécution des algorithmes proposés est très court ; ces algorithmes sont très rapides et ont une bonne applicabilité.

Dans cette section, nous avons présenté les résultats expérimentaux des algorithmes proposés, l'analyse de l'espace des clés, les attaques différentielles et statistiques, l'entropie de l'information et l'analyse de la vitesse ont été des moyens de valider ces nouveaux algorithmes proposés. Nous sommes arrivés à la conclusion que ces algorithmes sont robustes contre tous les types d'attaques connues et nous avons constaté leur supériorité par rapport aux méthodes de l'état de l'art.

4.5 Conclusion

Dans cet contribution, nous avons présenté trois nouveaux algorithmes de chiffrement basés sur les moments séparables et le calcul parallèle. Trois familles de moments séparables ont été utilisées comme domaine transformé pour le chiffrement, à

TABLE 4.5: Résultats de l'entropie pour les algorithmes proposés par rapport aux algorithmes de l'état de l'art

Entropy	Prop. TKM	Prop. THM	Prop. KHM	Tchebichef [101]	Krawtchouk [101]	Hahn [101]	Ref [222]	Ref [220]	Ref [198]
Lena	7.9982	7.9985	7.9997	7.9946	7.9953	7.9955	7.9964	7.9967	7.996
Baboon	7.9982	7.9989	7.9995	7.995	7.9956	7.9956	7.9959	7.9963	7.9961
Cameraman	7.9978	7.9992	7.9985	7.9944	7.9953	7.9955	7.9961	7.996	7.9952
Boats	7.9984	7.9981	7.9978	7.9946	7.9954	7.9956	7.9966	7.9966	7.9953
livingroom	7.9986	7.9983	7.9983	7.9945	7.9953	7.9956	7.9961	7.9955	7.9966

TABLE 4.6: Analyse de la vitesse des algorithmes proposés par rapport aux algorithmes de l'état de l'art

Image size	Prop. TKM	Prop. THM	Prop. KHM	Tchebichef [101]	Krawtchouk [101]	Hahn [101]	Ref [222]	Ref [220]	Ref [198]
128*128	0.0112	0.0126	0.0114	0.1148	0.0725	0.1747	0.0355	0.0263	0.0774
256*256	0.0164	0.0243	0.0223	0.285	0.4422	0.3713	0.46	0.442	0.11794
512*512	0.022	0.0333	0.0319	0.3949	0.7683	0.6207	0.979	0,466	0,27444
1024*1024	0.0493	0.0434	0.0479	0.8859	0.8671	0.7683	1.1361	0.975	0.78902

savoir TKM (moments de Tchebichef-Krawtchouk), THM (moments de Tchebichef-Hahn) et KHM (moments de Krawtchouk-Hahn). Une nouvelle couche de sécurité a été ajoutée au schéma de chiffrement chaotique traditionnel. Un nouveau schéma basé sur le calcul parallèle a été introduit qui permet à différentes étapes de s'exécuter simultanément.

L'étude expérimentale a montré l'efficacité des algorithmes de chiffrement nouvellement introduits. Selon les résultats présentés, nous concluons que les algorithmes proposés sont sécurisés contre tous les types d'attaques connues et sont suffisamment rapides pour être mis en œuvre dans des applications réelles. Une étude comparative avec les méthodes de l'état de l'art a été réalisée et nous avons montré la supériorité des algorithmes nouvellement proposés.

En conclusion, compte tenu des résultats présentés de ces nouveaux algorithmes, nous sommes confiants quant à leur capacité à être utilisés dans des scénarios du monde réel.

Conclusion générale et perspectives

Dans ce travail, nous avons présenté une étude théorique du chaos et des moments orthogonaux qui servent comme des bases théoriques pour nos contributions. Dans un premier travail nous avons proposé un ensemble d'algorithmes basés sur la théorie du chaos et les moments orthogonaux, ainsi nous avons implémenté cinq nouveaux algorithmes basés sur les moments de: Tchebichef, Krawtchouk, Hahn, Dual Hahn et Racah. Le chiffrement chaotique a été utilisé via deux cartes logistiques qui ont pour conditions initiales la clef de chiffrement. La nouveauté de ce travail consiste à appliquer pour la première fois les moments orthogonaux au chiffrement des images. Cela nous a permis d'améliorer la sécurité des données chiffrées par rapport aux algorithmes de l'état de l'art, et a ouvert une nouvelle porte pour la recherche des moments appliqués au chiffrement des données. Les résultats obtenus dans ce premier travail nous ont encouragé à développer des nouveaux algorithmes de chiffrement basés sur les moments orthogonaux. Dans cette perspective nous avons introduit un nouvel algorithme du chiffrement qui vise à améliorer le temps de calcul sans compromettre la sécurité. L'algorithme est basé sur le chiffrement sélectif et nous avons prouvé que l'algorithme est sûr contre toutes les attaques connues et suffisamment rapide pour être déployé dans les scénario réels.

Toujours dans la vision d'explorer les capacités des moments dans le chiffrement d'image et d'améliorer le temps de calcul, nous avons proposé trois algorithmes de chiffrement basés sur les moments séparables de: Tchebichef-Krawtchouk (TKM), Techbichef-Hahn (THM) et Krawtchouk-Hahn (KHM). Ces algorithmes ont été implémentés dans un schéma parallèle qui a permet de réduire le temps de calcul considérablement. Notre choix des moments séparables a été basé sur la performance des moments correspondants dans le premier travail. En effet, nous avons remarqué que les moments de Tchebichef, Krawtchouk et Hahn ont été les moments les plus performants. Du coup, nous avons combiner les moments et les résultats on été améliorer en termes de sécurité et de vitesse.

Les perspectives ouvertes dans le cadre de ces travaux peuvent être résumées comme suit :
- Implémenter les algorithmes de chiffrement d'image au chiffrement des vidéos en temps réel.
- Vu que ces algorithmes ont été implémentés pour les images niveau de gris, nous avons l'intention de les implémenté également pour les images colorées.
- Dans un nouveau travail intitulé "Un cadre pour la recherche d'images basée sur le contenu médical préservant la confidentialité", nous avons proposé schéma pour l'extraction de caractéristiques dans le domaine des données chiffrés. Notre travail courant vise à implémenter ce schéma.

Bibliographie

[1] Yaser S Abu-Mostafa and Demetri Psaltis. "Recognitive aspects of moment invariants". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 6 (1984), pp. 698–706.

[2] Jawad Ahmad, Seong Oun Hwang, and Arshad Ali. "An experimental comparison of chaotic and non-chaotic image encryption schemes". In: *Wireless Personal Communications* 84.2 (2015), pp. 901–918.

[3] Jawad Ahmad et al. "A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices". In: *Neural computing and applications* 28.1 (2017), pp. 953–967.

[4] Hossam El-din H Ahmed, Hamdy M Kalash, and OS Farag Allah. "Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images". In: *Electrical Engineering, 2007. ICEE'07. International Conference on*. IEEE. 2007, pp. 1–7.

[5] Mohammed Sadiq Al-Rawi. "Fast computation of pseudo Zernike moments". In: *Journal of Real-Time Image Processing* 5.1 (2010), pp. 3–10.

[6] Gonzalo Alvarez and Shujun Li. "Some basic cryptographic requirements for chaos-based cryptosystems". In: *International journal of bifurcation and chaos* 16.08 (2006), pp. 2129–2151.

[7] Amir Averbuch et al. "Fast and accurate polar Fourier transform". In: *Applied and computational harmonic analysis* 21.2 (2006), pp. 145–167.

[8] Robert R Bailey and Mandyam Srinath. "Orthogonal moment features for use with parametric and non-parametric classifiers". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 18.4 (1996), pp. 389–399.

[9] Vassileios Balntas et al. "HPatches: A benchmark and evaluation of handcrafted and learned local descriptors". In: *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2017, pp. 5173–5182.

[10] MS Baptista. "Cryptography with chaos". In: *Physics letters A* 240.1-2 (1998), pp. 50–54.

[11] Imad Batioua et al. "3D image analysis by separable discrete orthogonal moments based on Krawtchouk and Tchebichef polynomials". In: *Pattern Recognition* 71 (2017), pp. 264–277.

[12] Imad Batioua et al. "Image analysis using new set of separable two-dimensional discrete orthogonal moments based on Racah polynomials". In: *EURASIP Journal on Image and Video Processing* 2017.1 (2017), p. 20.

[13] Herbert Bay. "Luc Van Gool, SURF: Speeded-Up Robust Features". In: *Proceedings of the 9th European Conference on Computer Vision, 2006*. 2006.

[14] Saeid Belkasim, E Hassan, and T Obeidi. "Explicit invariance of Cartesian Zernike moments". In: *Pattern Recognition Letters* 28.15 (2007), pp. 1969–1980.

[15] Rachid Benouini et al. "Efficient 3D object classification by using direct Krawtchouk moment invariants". In: *Multimedia Tools and Applications* (2018), pp. 1–26.

[16] Rachid Benouini et al. "Fast and accurate computation of Racah moment invariants for image classification". In: *Pattern Recognition* 91 (2019), pp. 100–110.

[17] Aneta Bera, Przemysław Klęsk, and Dariusz Sychel. "Constant-time calculation of Zernike moments for detection with rotational invariance". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 41.3 (2018), pp. 537–551.

[18] AB Bhatia and E Wolf. "On the circle polynomials of Zernike and related orthogonal sets". In: *Mathematical Proceedings of the Cambridge Philosophical Society*. Vol. 50. 1. Cambridge University Press. 1954, pp. 40–48.

[19] Mark E Bianco and Dana A Reed. *Encryption system based on chaos theory*. US Patent 5,048,086. 1991.

[20] Alexander M Bronstein et al. "Shape google: Geometric words and expressions for invariant shape retrieval". In: *ACM Transactions on Graphics (TOG)* 30.1 (2011), pp. 1–20.

[21] Lisa Gottesfeld Brown. "A survey of image registration techniques". In: *ACM computing surveys (CSUR)* 24.4 (1992), pp. 325–376.

[22] Z Cai and D Huang. "Research on DES Data Encryption Technology in Network Information Security [J]". In: *Computer Measurement & Control* 25 (2017), pp. 241–247.

[23] C Camacho-Bello et al. "High-precision and fast computation of Jacobi–Fourier moments for image description". In: *JOSA A* 31.1 (2014), pp. 124–134.

[24] Patrizio Campisi and Karen Egiazarian. *Blind image deconvolution: theory and applications*. CRC press, 2017.

[25] David Casasent and R Lee Cheatham. "Image segmentation and real-image tests for an optical moment-based feature extractor". In: *Optics communications* 51.4 (1984), pp. 227–230.

[26] David Casasent and Demetri Psaltis. "New optical transforms for pattern recognition". In: *Proceedings of the IEEE* 65.1 (1977), pp. 77–84.

[27] Tristan Caulfield, Christos Ioannidis, and David Pym. "Discrete Choice, Social Interaction, and Policy in Encryption Technology Adoption (Short Paper)". In: *International Conference on Financial Cryptography and Data Security*. Springer. 2016, pp. 271–279.

[28] Xiu-Li Chai et al. "An image encryption scheme based on three-dimensional Brownian motion and chaotic system". In: *Chinese Physics B* 26.2 (2017), p. 020504.

[29] Xiuli Chai, Yiran Chen, and Lucie Broyde. "A novel chaos-based image encryption algorithm using DNA sequence operations". In: *Optics and Lasers in engineering* 88 (2017), pp. 197–213.

[30] Tsung-Han Chan et al. "PCANet: A simple deep learning baseline for image classification?" In: *IEEE transactions on image processing* 24.12 (2015), pp. 5017–5032.

[31] François Chaumette. "Image moments: a general and useful set of features for visual servoing". In: *IEEE Transactions on Robotics* 20.4 (2004), pp. 713–723.

[32] Beijing Chen et al. "Combined invariants to similarity transformation and to blur using orthogonal Zernike moments". In: *IEEE Transactions on Image Processing* 20.2 (2010), pp. 345–360.

[33] Beijing Chen et al. "Fast computation of sliding discrete Tchebichef moments and its application in duplicated regions detection". In: *IEEE Transactions on Signal Processing* 63.20 (2015), pp. 5424–5436.

[34] Beijing Chen et al. "Quaternion pseudo-Zernike moments combining both of RGB information and depth information for color image splicing detection". In: *Journal of Visual Communication and Image Representation* 49 (2017), pp. 283–290.

[35] Chao-Shen Chen and Rong-Jian Chen. "Image encryption and decryption using SCAN methodology". In: *Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT'06. Seventh International Conference on*. IEEE. 2006, pp. 61–66.

[36] Guanrong Chen. "Chaotification via feedback: the discrete case". In: *Chaos control*. Springer, 2003, pp. 159–177.

[37] Guanrong Chen and Xiaoning Dong. *From chaos to order: methodologies, perspectives and applications*. Vol. 24. World Scientific, 1998.

[38] Qing Chen, Emil Petriu, and Xiaoli Yang. "A comparative study of Fourier descriptors and Hu's seven moment invariants for image recognition". In: *Canadian conference on electrical and computer engineering 2004 (IEEE Cat. No. 04CH37513)*. Vol. 1. IEEE. 2004, pp. 103–106.

[39] Zen Chen and Shu-Kuo Sun. "A Zernike moment phase-based descriptor for local image representation and matching". In: *IEEE Transactions on Image Processing* 19.1 (2009), pp. 205–219.

[40] Emmanuel Chisanga and Ernest Ketcha Ngassam. "Towards a conceptual framework for information security digital divide". In: *2017 IST-Africa Week Conference (IST-Africa)*. IEEE. 2017, pp. 1–8.

[41] Chee-Way Chong, P Raveendran, and Ramakrishnan Mukundan. "A comparative analysis of algorithms for fast computation of Zernike moments". In: *Pattern Recognition* 36.3 (2003), pp. 731–742.

[42] Chee-Way Chong, Paramesran Raveendran, and Ramakrishnan Mukundan. "Translation and scale invariants of Legendre moments". In: *Pattern recognition* 37.1 (2004), pp. 119–129.

[43] Chee-Way Chong, Paramesran Raveendran, and Ramakrishnan Mukundan. "Translation invariants of Zernike moments". In: *Pattern recognition* 36.8 (2003), pp. 1765–1773.

[44] Wang Chun-peng, Wang Xing-yuan, and Xia Zhi-qiu. "Geometrically invariant image watermarking based on fast radial harmonic Fourier moments". In: *Signal Processing: Image Communication* 45 (2016), pp. 10–23.

[45] Davide Cozzolino, Giovanni Poggi, and Luisa Verdoliva. "Efficient dense-field copy–move forgery detection". In: *IEEE Transactions on Information Forensics and Security* 10.11 (2015), pp. 2284–2297.

[46] Frank Dachselt and Wolfgang Schwarz. "Chaos and cryptography". In: *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 48.12 (2001), pp. 1498–1509.

[47] XB Dai et al. "Reconstruction of tomographic images from limited range projections using discrete Radon transform and Tchebichef moments". In: *Pattern Recognition* 43.3 (2010), pp. 1152–1164.

[48] Xiaolong Dai and Siamak Khorram. "A feature-based image registration algorithm using improved chain-code representation combined with invariant moments". In: *IEEE Transactions on Geoscience and Remote Sensing* 37.5 (1999), pp. 2351–2362.

[49] Cheng Deng et al. "A local Tchebichef moments-based robust image watermarking". In: *Signal Processing* 89.8 (2009), pp. 1531–1539.

[50] Robert L Devaney. *An introduction to chaotic dynamical systems*. CRC press, 2018.

[51] Robert L Devaney et al. *Chaos and Fractals: The Mathematics Behind the Computer Graphics: The Mathematics Behind the Computer Graphics*. Vol. 1. American Mathematical Soc., 1989.

[52] Cecilia Di Ruberto, Lorenzo Putzu, and Giuseppe Rodriguez. "Fast and accurate computation of orthogonal moments for texture analysis". In: *Pattern Recognition* 83 (2018), pp. 498–510.

[53] Adrian-Viorel Diaconu and Khaled Loukhaoukha. "An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher". In: *Mathematical Problems in Engineering* 2013 (2013).

[54] Sahibsingh A Dudani, Kenneth J Breeding, and Robert B McGhee. "Aircraft identification by moment invariants". In: *IEEE transactions on computers* 100.1 (1977), pp. 39–46.

[55] IE El-Ashry. "Digital image encryption". In: *MS. c Thesis, Electronics and Electrical Communications Engineering Dept., Faculty of Electronic Engineering, Menofia University* (2010).

[56] Nawal F El Fishawy and Osama M Abu Zaid. "Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms." In: *IJ Network Security* 5.3 (2007), pp. 241–251.

[57] Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry. "Efficiency and security of some image encryption algorithms". In: *proceedings of the World Congress on Engineering*. Vol. 1. London. 2008, pp. 2–4.

[58] HM Elkamchouchi and MA Makar. "Measuring encryption quality for bitmap images encrypted with rijndael and kamkar block ciphers". In: *Radio science conference, 2005. NRSC 2005. Proceedings of the twenty-second national*. IEEE. 2005, pp. 277–284.

[59] Rasul Enayatifar, Abdul Hanan Abdullah, and Malrey Lee. "A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption". In: *Optics and Lasers in Engineering* 51.9 (2013), pp. 1066–1077.

[60] Jan Flusser. "On the independence of rotation moment invariants". In: *Pattern recognition* 33.9 (2000), pp. 1405–1410.

[61] Jan Flusser and Tomas Suk. "Pattern recognition by affine moment invariants". In: *Pattern recognition* 26.1 (1993), pp. 167–174.

[62] Jan Flusser, Tomáš Suk, and Stanislav Saic. "Image features invariant with respect to blur". In: *Pattern Recognition* 28.11 (1995), pp. 1723–1732.

[63] Jan Flusser, Tomás Suk, and Stanislav Saic. "Recognition of images degraded by linear motion blur without restoration". In: *Theoretical Foundations of Computer Vision*. Springer, 1996, pp. 37–51.

[64] Jan Flusser, Tomas Suk, and Barbara Zitová. *2D and 3D image analysis by moments*. John Wiley & Sons, 2016.

[65] Jan Flusser and Barbara Zitová. "Invariants to convolution with circularly symmetric PSF". In: *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.* Vol. 2. IEEE. 2004, pp. 11–14.

[66] Jan Flusser, Barbara Zitova, and Tomas Suk. *Moments and moment invariants in pattern recognition*. John Wiley & Sons, 2009.

[67] Jan Flusser et al. "Projection operators and moment invariants to image blurring". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 37.4 (2014), pp. 786–802.

[68] Jan Flusser et al. "Recognition of images degraded by Gaussian blur". In: *IEEE transactions on Image Processing* 25.2 (2015), pp. 790–806.

[69] Jiri Fridrich. "Secure image ciphering based on chaos". In: *Final report (April, 1997)* (1997).

[70] Jiri Fridrich. "Symmetric ciphers based on two-dimensional chaotic maps". In: *International Journal of Bifurcation and chaos* 8.06 (1998), pp. 1259–1284.

[71] Xinbo Gao et al. "Zernike-moment-based image super resolution". In: *IEEE Transactions on Image Processing* 20.10 (2011), pp. 2738–2747.

[72] Sugata Ghosal and Rajiv Mehrotra. "Orthogonal moment operators for subpixel edge detection". In: *Pattern recognition* 26.2 (1993), pp. 295–306.

[73] Jiuxiang Gu et al. "Recent advances in convolutional neural networks". In: *Pattern recognition* 77 (2018), pp. 354–377.

[74] Mengmeng Guan, Xuelin Yang, and Weisheng Hu. "Chaotic image encryption algorithm using frequency-domain DNA encoding". In: *IET image processing* 13.9 (2019), pp. 1535–1539.

[75] Toshiki Habutsu et al. "A secret key cryptosystem by iterating a chaotic map". In: *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer. 1991, pp. 127–140.

[76] Zhengbiao Han et al. "Risk assessment of digital library information security: a case study". In: *The electronic library* 34.3 (2016), pp. 471–487.

[77] DC Hankerson et al. *Coding theory and cryptography: the essentials*. CRC Press, 2000.

[78] You Hao et al. "Dual affine moment invariants". In: *arXiv preprint arXiv:1911.08233* (2019).

[79] Kaiming He et al. "Spatial pyramid pooling in deep convolutional networks for visual recognition". In: *IEEE transactions on pattern analysis and machine intelligence* 37.9 (2015), pp. 1904–1916.

[80] Thai Hoang. "Image representations for pattern recognition". PhD thesis. Université Nancy II, 2011.

[81] Thai V Hoang and Salvatore Tabbone. "Fast computation of orthogonal polar harmonic transforms". In: *Proceedings of the 21st International Conference on Pattern Recognition (ICPR2012)*. IEEE. 2012, pp. 3160–3163.

[82] Thai V Hoang and Salvatore Tabbone. "Fast generic polar harmonic transforms". In: *IEEE transactions on image processing* 23.7 (2014), pp. 2961–2971.

[83] Thai V Hoang and Salvatore Tabbone. "Invariant pattern recognition using the RFM descriptor". In: *Pattern Recognition* 45.1 (2012), pp. 271–284.

[84] Khalid M Hosny. "Image representation using accurate orthogonal Gegenbauer moments". In: *Pattern Recognition Letters* 32.6 (2011), pp. 795–804.

[85] Khalid M Hosny and Mohamed M Darwish. "A kernel-based method for fast and accurate computation of PHT in polar coordinates". In: *Journal of Real-Time Image Processing* 16.4 (2019), pp. 1235–1247.

[86] Khalid Mohamed Hosny, Mohamed A Shouman, and Hayam M Abdel Salam. "Fast computation of orthogonal Fourier–Mellin moments in polar coordinates". In: *Journal of Real-Time Image Processing* 6.2 (2011), pp. 73–80.

[87] Hua-Sheng Hsu and Wen-Hsiang Tsai. "Moment-preserving edge detection and its application to image data compression". In: *Optical engineering* 32.7 (1993), pp. 1596–1609.

[88] Guozhen Hu and Baobin Li. "A uniform chaotic system with extended parameter range for image encryption". In: *Nonlinear Dynamics* 103.3 (2021), pp. 2819–2840.

[89] Ming-Kuei Hu. "Visual pattern recognition by moment invariants". In: *IRE transactions on information theory* 8.2 (1962), pp. 179–187.

[90] Zhongyun Hua, Yicong Zhou, and Hejiao Huang. "Cosine-transform-based chaotic system for image encryption". In: *Information Sciences* 480 (2019), pp. 403–419.

[91] Zhongyun Hua et al. "2D Logistic-Sine-coupling map for image encryption". In: *Signal Processing* 149 (2018), pp. 148–161.

[92] Iqtadar Hussain, Tariq Shah, and Muhammad Asif Gondal. "An efficient image encryption algorithm based on S8 S-box transformation and NCA map". In: *Optics Communications* 285.24 (2012), pp. 4887–4890.

[93] Sun-Kyoo Hwang and Whoi-Yul Kim. "A novel approach to the fast computation of Zernike moments". In: *Pattern Recognition* 39.11 (2006), pp. 2065–2076.

[94] Dimosthenis Ioannidis et al. "Gait recognition using compact feature extraction transforms and depth information". In: *IEEE Transactions on Information Forensics and security* 2.3 (2007), pp. 623–630.

[95] Ahmet Iscen et al. "A comparison of dense region detectors for image search and fine-grained classification". In: *IEEE Transactions on Image Processing* 24.8 (2015), pp. 2369–2381.

[96] Ismail Amr Ismail, Mohammed Amin, and Hossam Diab. "A digital image encryption algorithm based a composition of two chaotic logistic maps." In: *Int. J. Netw. Secur.* 11.1 (2010), pp. 1–10.

[97] Kourosh Jafari-Khouzani and Hamid Soltanian-Zadeh. "Rotation-invariant multiresolution texture analysis using radon and wavelet transforms". In: *IEEE transactions on image processing* 14.6 (2005), pp. 783–795.

[98] Siva Janakiraman et al. "Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller". In: *Microprocessors and Microsystems* 56 (2018), pp. 1–12.

[99] Nanning Zheng Xiaoyi Jiang and Xuguang Lan. *Advances in machine vision, image processing, and pattern analysis*. 2006.

[100] Alireza Jolfaei, Xin-Wen Wu, and Vallipuram Muthukkumarasamy. "On the security of permutation-only image encryption schemes". In: *IEEE transactions on information forensics and security* 11.2 (2016), pp. 235–246.

[101] Abdelhalim Kamrani, Khalid Zenkouar, and Said Najah. "A new set of image encryption algorithms based on discrete orthogonal moments and Chaos theory". In: *Multimedia Tools and Applications* 79.27 (2020), pp. 20263–20279.

[102] Evangelos G Karakasis et al. "Generalized dual Hahn moment invariants". In: *Pattern Recognition* 46.7 (2013), pp. 1998–2014.

[103] Walid I Khedr. "A new efficient and configurable image encryption structure for secure transmission". In: *Multimedia Tools and Applications* (2019), pp. 1–25.

[104] Alireza Khotanzad and Yaw Hua Hong. "Invariant image recognition by Zernike moments". In: *IEEE Transactions on pattern analysis and machine intelligence* 12.5 (1990), pp. 489–497.

[105] Alireza Khotanzad and JJ-H Liou. "Recognition and pose estimation of unoccluded three-dimensional objects from a two-dimensional perspective view by banks of neural networks". In: *IEEE Transactions on Neural networks* 7.4 (1996), pp. 897–906.

[106] Nahum Kiryati, Alfred M. Bruckstein, and H Mizrahi. "Comments on:" Robust line fitting in a noisy image by the method of moments"". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 22.11 (2000), pp. 1340–1341.

[107] Ljupco Kocarev. "Chaos-based cryptography: a brief overview". In: *IEEE Circuits and Systems Magazine* 1.3 (2001), pp. 6–21.

[108] Jitka Kostková, Tomáš Suk, and Jan Flusser. "Affine invariants of vector fields". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 43.4 (2019), pp. 1140–1155.

[109] Jitka Kostková, Tomáš Suk, and Jan Flusser. "Affine moment invariants of vector fields". In: *2018 25th IEEE International Conference on Image Processing (ICIP)*. IEEE. 2018, pp. 1338–1342.

[110] Jitka Kostková et al. "Handling Gaussian blur without deconvolution". In: *Pattern Recognition* 103 (2020), p. 107264.

[111] Zbigniew Kotulski and Janusz Szczepański. "Discrete chaotic cryptography". In: *Annalen der Physik* 509.5 (1997), pp. 381–394.

[112] Louis Kruth. "Crypto and network security". In: *Cryptologia* 23.1 (1999), p. 50.

[113] Ahlad Kumar. "Deblurring of motion blurred images using histogram of oriented gradients and geometric moments". In: *Signal Processing: Image Communication* 55 (2017), pp. 55–65.

[114] Ahlad Kumar, M Omair Ahmad, and MNS Swamy. "Tchebichef and adaptive steerable-based total variation model for image denoising". In: *IEEE Transactions on image processing* 28.6 (2019), pp. 2921–2935.

[115] Deepa Kundur and Dimitrios Hatzinakos. "Blind image deconvolution". In: *IEEE signal processing magazine* 13.3 (1996), pp. 43–64.

[116] Seyed Mehdi Lajevardi and Zahir M Hussain. "Higher order orthogonal moments for invariant facial expression recognition". In: *Digital Signal Processing* 20.6 (2010), pp. 1771–1779.

[117] Max Langbein and Hans Hagen. "A generalization of moment invariants on 2D vector fields to tensor fields of arbitrary order and dimension". In: *International Symposium on Visual Computing*. Springer. 2009, pp. 1151–1160.

[118] Sung-won Lee, Seung-min Park, and Kwee-Bo Sim. "Smart door lock systems using encryption technology". In: *Journal of the Korean Institute of Intelligent Systems* 27.1 (2017), pp. 65–71.

[119] Lu Leng et al. "Dynamic weighted discrimination power analysis: a novel approach for face and palmprint recognition in DCT domain". In: *International Journal of Physical Sciences* 5.17 (2010), pp. 2543–2554.

[120] Lu Leng et al. "Dynamic weighted discrimination power analysis in DCT domain for face and palmprint recognition". In: *2010 international conference on information and communication technology convergence (ICTC)*. IEEE. 2010, pp. 467–471.

[121] Chunhu Li et al. "An image encryption scheme based on chaotic tent map". In: *Nonlinear Dynamics* 87.1 (2017), pp. 127–133.

[122] Erbo Li and Hua Li. "Isomorphism between differential and moment invariants under affine transform". In: *arXiv preprint arXiv:1705.08264* (2017).

[123] Erbo Li and Hua Li. "Reflection invariant and symmetry detection". In: *arXiv preprint arXiv:1705.10768* (2017).

[124] Erbo Li et al. "Image projective invariants". In: *IEEE transactions on pattern analysis and machine intelligence* 41.5 (2018), pp. 1144–1157.

[125] Erbo Li et al. "Shape DNA: Basic generating functions for geometric moment invariants". In: *arXiv preprint arXiv:1703.02242* (2017).

[126] Leida Li et al. "No-reference image blur assessment based on discrete orthogonal moments". In: *IEEE transactions on cybernetics* 46.1 (2015), pp. 39–50.

[127] Shujun Li and Xuan Zheng. "Cryptanalysis of a chaotic image encryption method". In: *2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No. 02CH37353)*. Vol. 2. IEEE. 2002, pp. II–II.

[128] Shujun Li et al. "A general cryptanalysis of permutation-only multimedia encryption algorithms". In: *IACR's Cryptology ePrint Archive: Report* 374 (2004), p. 2004.

[129] Shujun Li et al. "On the design of perceptual MPEG-video encryption algorithms". In: *IEEE Transactions on Circuits and Systems for Video Technology* 17.2 (2007), pp. 214–223.

[130] Shiguo Lian. *Multimedia content encryption: techniques and applications*. Auerbach Publications, 2008.

[131] Jiye Liang and Zhongzhi Shi. "The information entropy, rough entropy and knowledge granulation in rough set theory". In: *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 12.01 (2004), pp. 37–46.

[132] Meiyu Liang et al. "Video super-resolution reconstruction based on deep learning and spatio-temporal feature self-similarity". In: *IEEE Transactions on Knowledge and Data Engineering* (2020).

[133] Simon X Liao and Miroslaw Pawlak. "On the accuracy of Zernike moments for image analysis". In: *IEEE transactions on pattern analysis and machine intelligence* 20.12 (1998), pp. 1358–1364.

[134] Huibao Lin, Jennie Si, and Glen P Abousleman. "Orthogonal rotation-invariant moments for digital image processing". In: *IEEE transactions on image processing* 17.3 (2008), pp. 272–282.

[135] Ling Liu et al. "Digital chaos-masked optical encryption scheme enhanced by two-dimensional key space". In: *Optics Communications* 398 (2017), pp. 62–66.

[136] Manhua Liu and Pew-Thian Yap. "Invariant representation of orientation fields for fingerprint indexing". In: *Pattern Recognition* 45.7 (2012), pp. 2532–2542.

[137] Shi Liu, Changliang Guo, and John T Sheridan. "A review of optical image encryption techniques". In: *Optics & Laser Technology* 57 (2014), pp. 327–342.

[138] Edward N Lorenz. "Deterministic nonperiodic flow". In: *Journal of atmospheric sciences* 20.2 (1963), pp. 130–141.

[139] EN Lorenz. *Predictability Does the flap of a butterfly's wings in Brazil set off a tornado in Texas? Address at the Annual Meeting of the American Association for the Advancement of Science. Washington, DC., 1979. Cited in: The Essence of Chaos by Edward N. Lorenz*. 1993.

[140] Qing Lu, Congxu Zhu, and Xiaoheng Deng. "An efficient image encryption scheme based on the LSS chaotic map and single S-box". In: *IEEE Access* 8 (2020), pp. 25664–25678.

[141] Yuling Luo, Minghui Du, and Junxiu Liu. "A symmetrical image encryption scheme in wavelet and time domain". In: *Communications in Nonlinear Science and Numerical Simulation* 20.2 (2015), pp. 447–460.

[142] Alexander G Mamistvalov. "N-dimensional moment invariants and conceptual mathematical theory of recognition n-dimensional solids". In: *IEEE Transactions on pattern analysis and machine intelligence* 20.8 (1998), pp. 819–831.

[143] Mrinal K Mandal, Tyseer Aboulnasr, and Sethuraman Panchanathan. "Image indexing using moments and wavelets". In: *IEEE Transactions on Consumer Electronics* 42.3 (1996), pp. 557–565.

[144] deFigueiredo Markandey. "Robot sensing techniques based on high-dimensional moment invariants and tensors". In: *IEEE transactions on robotics and automation* 8.2 (1992), pp. 186–195.

[145] Judit Martínez and Federico Thomas. "Efficient computation of local geometric moments". In: *IEEE Transactions on Image Processing* 11.9 (2002), pp. 1102–1111.

[146] JM Matthews and AFJ Moffat. "WR 40: coherence or chaos?" In: *Astronomy and Astrophysics* 283 (1994), pp. 493–507.

[147] Robert Matthews. "On the derivation of a "chaotic" encryption algorithm". In: *Cryptologia* 13.1 (1989), pp. 29–42.

[148] Robert M May. "Simple mathematical models with very complicated dynamics". In: *The Theory of Chaotic Attractors*. Springer, 2004, pp. 85–93.

[149] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 2018.

[150] Qiguang Miao et al. "Three novel invariant moments based on radon and polar harmonic transforms". In: *Optics Communications* 285.6 (2012), pp. 1044–1048.

[151] Krystian Mikolajczyk and Cordelia Schmid. "A performance evaluation of local descriptors". In: *IEEE transactions on pattern analysis and machine intelligence* 27.10 (2005), pp. 1615–1630.

[152] Peckham Morse. "Man's Rage for Chaos: Biology, Behavior, and the Arts". In: (1967).

[153] R Mukundan. "Fast computation of geometric moments and invariants using Schlick's approximation". In: *International Journal of Pattern Recognition and Artificial Intelligence* 22.07 (2008), pp. 1363–1377.

[154] R Mukundan and KR Ramakrishnan. "Fast computation of Legendre and Zernike moments". In: *Pattern recognition* 28.9 (1995), pp. 1433–1442.

[155] Ramakrishnan Mukundan, SH Ong, and Poh Aun Lee. "Image analysis by Tchebichef moments". In: *IEEE Transactions on image Processing* 10.9 (2001), pp. 1357–1364.

[156] Fionn Murtagh and Jean-Luc Starck. "Wavelet and curvelet moments for image classification: application to aggregate mixture grading". In: *Pattern Recognition Letters* 29.10 (2008), pp. 1557–1564.

[157] Ensherah A Naeem et al. "Wavelet fusion for encrypting images with a few details". In: *Computers & Electrical Engineering* 54 (2016), pp. 450–470.

[158] Kiyoyuki Nakagaki and Ramakrishnan Mukundan. "A Fast 4x4 Forward Discrete Tchebichef Transform Algorithm". In: *IEEE Signal Processing Letters* 14.10 (2007), pp. 684–687.

[159] Arnold F Nikiforov, Vasilii B Uvarov, and Sergei K Suslov. "Classical orthogonal polynomials of a discrete variable". In: *Classical orthogonal polynomials of a discrete variable*. Springer, 1991, pp. 18–54.

[160] Marcel Nwali and Simon Liao. "A new fast algorithm to compute continuous moments defined in a rectangular region". In: *Pattern Recognition* 89 (2019), pp. 151–160.

[161] Alan V Oppenheim and Jae S Lim. "The importance of phase in signals". In: *Proceedings of the IEEE* 69.5 (1981), pp. 529–541.

[162] José Ramón Padilla-López, Alexandros Andre Chaaraoui, and Francisco Flórez-Revuelta. "Visual privacy protection methods: A survey". In: *Expert Systems with Applications* 42.9 (2015), pp. 4177–4195.

[163] George A Papakostas, Evangelos G Karakasis, and Dimitris E Koulouriotis. "Efficient and accurate computation of geometric moments on gray-scale images". In: *Pattern Recognition* 41.6 (2008), pp. 1895–1904.

[164] George A Papakostas, Dimitris E Koulouriotis, and Evangelos G Karakasis. "Computation strategies of orthogonal image moments: a comparative study". In: *Applied Mathematics and Computation* 216.1 (2010), pp. 1–17.

[165] George A Papakostas et al. "A new class of Zernike moments for computer vision applications". In: *Information Sciences* 177.13 (2007), pp. 2802–2819.

[166] George A Papakostas et al. "Modified factorial-free direct methods for Zernike and pseudo-Zernike moment computation". In: *IEEE Transactions on Instrumentation and Measurement* 58.7 (2009), pp. 2121–2131.

[167] Narendra K Pareek, Vinod Patidar, and Krishan K Sud. "Image encryption using chaotic logistic map". In: *Image and vision computing* 24.9 (2006), pp. 926–934.

[168] George Paschos, Ivan Radev, and Nagarajan Prabakar. "Image content-based retrieval using chromaticity moments". In: *IEEE Transactions on Knowledge and Data Engineering* 15.5 (2003), pp. 1069–1072.

[169] Matteo Pedone, Jan Flusser, and Janne Heikkilä. "Registration of Images With N-Fold Dihedral Blur". In: *IEEE Transactions on Image Processing* 24.3 (2015), pp. 1036–1045.

[170] Soo-Chang Pei and Chao-Nan Lin. "Image normalization for pattern recognition". In: *Image and Vision computing* 13.10 (1995), pp. 711–723.

[171] Yanting Pei et al. "Effects of image degradation and degradation removal to CNN-based image classification". In: *IEEE transactions on pattern analysis and machine intelligence* 43.4 (2019), pp. 1239–1253.

[172] Ziliang Ping et al. "FFT algorithm of complex exponent moments and its application in image recognition". In: *Sixth International Conference on Digital Image Processing (ICDIP 2014)*. Vol. 9159. SPIE. 2014, pp. 387–397.

[173] Aluizio Prata and WVT Rusch. "Algorithm for computation of Zernike polynomials expansion coefficients". In: *Applied Optics* 28.4 (1989), pp. 749–754.

[174] Shuren Qi et al. "A survey of orthogonal moments for image representation: theory, implementation, and evaluation". In: *ACM Computing Surveys (CSUR)* 55.1 (2021), pp. 1–35.

[175] Ahmed G Radwan, Sherif H AbdElHaleem, and Salwa K Abd-El-Hafiz. "Symmetric encryption algorithms using chaotic and non-chaotic generators: a review". In: *Journal of advanced research* 7.2 (2016), pp. 193–208.

[176] Dhivya Ravichandran et al. "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain". In: *Medical & Biological Engineering & Computing* 59.3 (2021), pp. 589–605.

[177] Jérôme Revaud, Guillaume Lavoué, and Atilla Baskurt. "Improving Zernike moments comparison for optimal similarity and rotation angle retrieval". In: *IEEE transactions on pattern analysis and machine intelligence* 31.4 (2008), pp. 627–636.

[178] José Sáez-Landete. "Comments on "fast computation of jacobi-Fourier moments for invariant image recognition"". In: *Pattern Recognition* 67 (2017), pp. 16–22.

[179] Priya R Sankpal and PA Vijaya. "Image encryption using chaotic maps: a survey". In: *Signal and Image Processing (ICSIP), 2014 Fifth International Conference on*. IEEE. 2014, pp. 102–107.

[180] Mhamed Sayyouri, Abdeslam Hmimid, and Hassan Qjidaa. "Image analysis using separable discrete moments of Charlier-Hahn". In: *Multimedia tools and applications* 75.1 (2016), pp. 547–571.

[181] Michael Schlemmer et al. "Moment invariants for the analysis of 2D flow fields". In: *IEEE Transactions on Visualization and Computer Graphics* 13.6 (2007), pp. 1743–1750.

[182] Roland Schmitz. "Use of chaotic dynamical systems in cryptography". In: *Journal of the Franklin Institute* 338.4 (2001), pp. 429–441.

[183] Bruce Schneier. *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons, 2007.

[184] KW See et al. "Image reconstruction using various discrete orthogonal polynomials in comparison with DCT". In: *Applied Mathematics and Computation* 193.2 (2007), pp. 346–359.

[185] Asif A Shah et al. "Efficient image encryption scheme based on generalized logistic map for real time image processing". In: *Journal of Real-Time Image Processing* 17.6 (2020), pp. 2139–2151.

[186] Claude Shannon. "Claude Shannon". In: *Information Theory* 3 (1948), p. 224.

[187] Claude E Shannon. "Communication theory of secrecy systems". In: *The Bell system technical journal* 28.4 (1949), pp. 656–715.

[188] Claude Elwood Shannon. "A mathematical theory of communication". In: *The Bell system technical journal* 27.3 (1948), pp. 379–423.

[189] Ling Shao et al. "From heuristic optimization to dictionary learning: A review and comprehensive comparison of image denoising algorithms". In: *IEEE transactions on cybernetics* 44.7 (2013), pp. 1001–1013.

[190] Dinggang Shen and Horace Ho-Shing Ip. "Generalized affine invariant image normalization". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 19.5 (1997), pp. 431–440.

[191] Jun Shen. "Orthogonal Gaussian-Hermite moments for image characterization". In: *Intelligent Robots and Computer Vision XVI: Algorithms, Techniques, Active Vision, and Materials Handling*. Vol. 3208. SPIE. 1997, pp. 224–233.

[192] Dongseok Shin, John K Pollard, and J-P Muller. "Accurate geometric correction of ATSR images". In: *IEEE Transactions on Geoscience and Remote Sensing* 35.4 (1997), pp. 997–1006.

[193] Chandan Singh and Sukhjeet K Ranade. "A high capacity image adaptive watermarking scheme with radial harmonic Fourier moments". In: *Digital signal processing* 23.5 (2013), pp. 1470–1482.

[194] Chandan Singh and Rahul Upneja. "Accurate calculation of high order pseudo-Zernike moments and their numerical stability". In: *Digital Signal Processing* 27 (2014), pp. 95–106.

[195] Chandan Singh and Rahul Upneja. "Accurate computation of orthogonal Fourier-Mellin moments". In: *Journal of Mathematical Imaging and Vision* 44.3 (2012), pp. 411–431.

[196] Chandan Singh and Ekta Walia. "Algorithms for fast computation of Zernike moments and their numerical stability". In: *Image and Vision Computing* 29.4 (2011), pp. 251–259.

[197] Atilla Sit, Woong-Hee Shin, and Daisuke Kihara. "Three-dimensional Krawtchouk descriptors for protein local surface shape comparison". In: *Pattern recognition* 93 (2019), pp. 534–545.

[198] Wei Song et al. "A novel batch image encryption algorithm using parallel computing". In: *Information Sciences* 518 (2020), pp. 211–224.

[199] Douglas R Stinson. *Cryptography: theory and practice*. Chapman and Hall/CRC, 2005.

[200] Tomáš Suk and Jan Flusser. "Combined blur and affine moment invariants and their use in pattern recognition". In: *Pattern Recognition* 36.12 (2003), pp. 2895–2907.

[201] Tomáš Suk and Jan Flusser. "Tensor method for constructing 3D moment invariants". In: *International Conference on Computer Analysis of Images and Patterns*. Springer. 2011, pp. 212–219.

[202] YQ Sun and XH Wang. "Information encryption technology with strong robustness based on QR code and matrix mapping [J]". In: *Packaging Engineering* 38 (2017), pp. 194–199.

[203] Michael Reed Teague. "Image analysis via the general theory of moments". In: *Josa* 70.8 (1980), pp. 920–930.

[204] Sara Tedmori and Nijad Al-Najdawi. "Image cryptographic algorithm based on the Haar wavelet transform". In: *Information Sciences* 269 (2014), pp. 21–34.

[205] C-H Teh and Roland T Chin. "On image analysis by the methods of moments". In: *IEEE Transactions on pattern analysis and machine intelligence* 10.4 (1988), pp. 496–513.

[206] ED Tsougenis, George A Papakostas, and Dimitris E Koulouriotis. "Image watermarking via separable moments". In: *Multimedia tools and applications* 74.11 (2015), pp. 3985–4012.

[207] Efstratios D Tsougenis et al. "Performance evaluation of moment-based watermarking methods: a review". In: *Journal of Systems and Software* 85.8 (2012), pp. 1864–1884.

[208] Martin Uhrin. "Through the eyes of a descriptor: constructing complete, invertible descriptions of atomic environments". In: *Physical Review B* 104.14 (2021), p. 144110.

[209] Rahul Upneja and Chandan Singh. "Fast computation of Jacobi-Fourier moments for invariant image recognition". In: *Pattern Recognition* 48.5 (2015), pp. 1836–1843.

[210] Nicole Vincent and Jean-Marc Ogier. "Shall deep learning be the mandatory future of document analysis problems?" In: *Pattern Recognition* 86 (2019), pp. 281–289.

[211] Rossouw Von Solms. "Information security management (3): the code of practice for information security management (BS 7799)". In: *Information Management & Computer Security* (1998).

[212] Rossouw Von Solms and Johan Van Niekerk. "From information security to cyber security". In: *computers & security* 38 (2013), pp. 97–102.

[213] Åke Wallin and O Kubler. "Complete sets of complex Zernike moment invariants and the role of the pseudoinvariants". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 17.11 (1995), pp. 1106–1110.

[214] Chunpeng Wang et al. "Geometric correction based color image watermarking using fuzzy least squares support vector machine and Bessel K form distribution". In: *Signal Processing* 134 (2017), pp. 197–208.

[215] Xiang-Yang Wang et al. "Pixel classification based color image segmentation using quaternion exponent moments". In: *Neural Networks* 74 (2016), pp. 1–13.

[216] Xiang-yang Wang et al. "Robust and effective multiple copy-move forgeries detection and localization". In: *Pattern Analysis and Applications* 24.3 (2021), pp. 1025–1046.

[217] Xiaoyu Wang and Simon Liao. "Image reconstruction from orthogonal fourier-mellin moments". In: *International Conference Image Analysis and Recognition*. Springer. 2013, pp. 687–694.

[218] Xing-Yuan Wang and Lin-Tao Liu. "Cryptanalysis and improvement of a digital image encryption method with chaotic map lattices". In: *Chinese Physics B* 22.5 (2013), p. 050503.

[219] Xingyuan Wang, Le Feng, and Hongyu Zhao. "Fast image encryption algorithm based on parallel computing system". In: *Information Sciences* 486 (2019), pp. 340–358.

[220] Xingyuan Wang and Suo Gao. "Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory". In: *Information sciences* 507 (2020), pp. 16–36.

[221] Xingyuan Wang, Lintao Liu, and Yingqian Zhang. "A novel chaotic block image encryption algorithm based on dynamic random growth technique". In: *Optics and Lasers in Engineering* 66 (2015), pp. 10–18.

[222] Yong Wang et al. "A new chaos-based fast image encryption algorithm". In: *Applied soft computing* 11.1 (2011), pp. 514–522.

[223] Yong-Ying Wang et al. "Optical image encryption based on binary Fourier transform computer-generated hologram and pixel scrambling technology". In: *Optics and lasers in engineering* 45.7 (2007), pp. 761–765.

[224] Chong-Yaw Wee and Raveendran Paramesran. "On the computational aspects of Zernike moments". In: *Image and Vision Computing* 25.6 (2007), pp. 967–980.

[225] Z Wen, LI Taoshen, and Z Zhang. "An image encryption technology based on chaotic sequences [J]". In: *Computer Project* 31.10 (2005), pp. 130–132.

[226] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law. "A fast image encryption scheme based on chaotic standard map". In: *Physics Letters A* 372.15 (2008), pp. 2645–2652.

[227] Chung-Ping Wu and C-C Jay Kuo. "Fast encryption methods for audiovisual data confidentiality". In: *Multimedia Systems and Applications III*. Vol. 4209. SPIE. 2001, pp. 284–295.

[228] Guo-Cheng Wu et al. "New variable-order fractional chaotic systems for fast image encryption". In: *Chaos: An Interdisciplinary Journal of Nonlinear Science* 29.8 (2019), p. 083103.

[229] Jianhua Wu et al. "Image encryption based on a reality-preserving fractional discrete cosine transform and a chaos-based generating sequence". In: *Journal of Modern Optics* 60.20 (2013), pp. 1760–1771.

[230] Yue Wu, Joseph P Noonan, and Sos Agaian. "NPCR and UACI randomness tests for image encryption". In: *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)* 1.2 (2011), pp. 31–38.

[231] Hongyue Xiang and Lingfeng Liu. "An improved digital logistic map and its application in image encryption". In: *Multimedia Tools and Applications* 79.41 (2020), pp. 30329–30355.

[232] Bin Xiao, Jian-Feng Ma, and Jiang-Tao Cui. "Radial Tchebichef moment invariants for image recognition". In: *Journal of Visual Communication and Image Representation* 23.2 (2012), pp. 381–386.

[233] Bin Xiao and Guo-yin Wang. "Generic radial orthogonal moment invariants for invariant image recognition". In: *Journal of Visual Communication and Image Representation* 24.7 (2013), pp. 1002–1008.

[234] Bin Xiao, Guo-yin Wang, and Wei-sheng Li. "Radial shifted Legendre moments for image analysis and invariant image recognition". In: *Image and Vision Computing* 32.12 (2014), pp. 994–1006.

[235] Bin Xiao et al. "Fractional discrete Tchebyshev moments and their applications in image encryption and watermarking". In: *Information Sciences* 516 (2020), pp. 545–559.

[236] Bin Xiao et al. "Lossless image compression based on integer Discrete Tchebichef Transform". In: *Neurocomputing* 214 (2016), pp. 587–593.

[237] Bin Xiao et al. "Moments and moment invariants in the Radon space". In: *Pattern recognition* 48.9 (2015), pp. 2772–2784.

[238] Ge Xin et al. "An image encryption algorithm based on spatiotemporal chaos in DCT domain". In: *Information Management and Engineering (ICIME), 2010 the 2nd IEEE International Conference on*. IEEE. 2010, pp. 267–270.

[239] Yongqing Xin, Miroslaw Pawlak, and Simon Liao. "Accurate computation of Zernike moments in polar coordinates". In: *IEEE Transactions on Image Processing* 16.2 (2007), pp. 581–587.

[240] Dong Xu and Hua Li. "3-D curve moment invariants for curve recognition". In: *Intelligent Computing in Signal Processing and Pattern Recognition*. Springer, 2006, pp. 572–577.

[241] Dong Xu and Hua Li. "Geometric moment invariants". In: *Pattern recognition* 41.1 (2008), pp. 240–249.

[242] Lu Xu et al. "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion". In: *Optics and Lasers in Engineering* 91 (2017), pp. 41–52.

[243] Mohamed Yamni et al. "Image watermarking using separable fractional moments of Charlier–Meixner". In: *Journal of the Franklin Institute* 358.4 (2021), pp. 2535–2560.

[244] Bo Yang, Jan Flusser, and Tomáš Suk. "Design of high-order rotation invariants from Gaussian–Hermite moments". In: *Signal Processing* 113 (2015), pp. 61–67.

[245] Bo Yang et al. "Rotation invariants from Gaussian-Hermite moments of color images". In: *Signal Processing* 143 (2018), pp. 282–291.

[246] Hong-ying Yang et al. "Color image zero-watermarking based on fast quaternion generic polar complex exponential transform". In: *Signal Processing: Image Communication* 82 (2020), p. 115747.

[247] Hong-ying Yang et al. "Image analysis by log-polar Exponent-Fourier moments". In: *Pattern Recognition* 101 (2020), p. 107177.

[248] Jianwei Yang et al. "Quasi Fourier-Mellin transform for affine invariant features". In: *IEEE Transactions on Image Processing* 29 (2020), pp. 4114–4129.

[249] Zhengwei Yang and Fernand S Cohen. "Cross-weighted moments and affine invariants for image registration and matching". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 21.8 (1999), pp. 804–814.

[250] P-T Yap, Raveendran Paramesran, and Seng-Huat Ong. "Image analysis by Krawtchouk moments". In: *IEEE Transactions on image processing* 12.11 (2003), pp. 1367–1377.

[251] Pew-Thian Yap, Raveendran Paramesran, and Seng-Huat Ong. "Image analysis using Hahn moments". In: *IEEE transactions on pattern analysis and machine intelligence* 29.11 (2007), pp. 2057–2062.

[252] Guodong Ye and Xiaoling Huang. "Spatial image encryption algorithm based on chaotic map and pixel frequency". In: *Science China Information Sciences* 61.5 (2018), p. 058104.

[253] Guodong Ye et al. "An efficient pixel-level chaotic image encryption algorithm". In: *Nonlinear Dynamics* (2018), pp. 1–12.

[254] Jiahong Yin, Alvaro Rodolfo De Pierro, and Musheng Wei. "Analysis for the reconstruction of a noisy signal based on orthogonal moments". In: *Applied mathematics and computation* 132.2-3 (2002), pp. 249–263.

[255] Qu Ying-Dong et al. "A fast subpixel edge detection method using Sobel–Zernike moments operator". In: *Image and Vision Computing* 23.1 (2005), pp. 11–17.

[256] LI Yu-Zhen, X Jin, G Zhao, et al. "Color image encryption scheme based on zigzag transformation and chaotic map [J]". In: *Computer Engineering & Design* 37 (2016), pp. 2001–2006.

[257] Junsong Yuan, Ying Wu, and Ming Yang. "Discovery of collocation patterns: from visual words to visual phrases". In: *2007 IEEE Conference on Computer Vision and Pattern Recognition*. IEEE. 2007, pp. 1–8.

[258] Dengsheng Zhang and Guojun Lu. "Shape-based image retrieval using generic Fourier descriptor". In: *Signal Processing: Image Communication* 17.10 (2002), pp. 825–848.

[259] Guoji Zhang and Qing Liu. "A novel image encryption method based on total shuffling scheme". In: *Optics Communications* 284.12 (2011), pp. 2775–2780.

[260] He Zhang et al. "Differential and integral invariants under Möbius transformation". In: *Chinese Conference on Pattern Recognition and Computer Vision (PRCV)*. Springer. 2018, pp. 280–291.

[261] He Zhang et al. "Fast and efficient calculations of structural invariants of chirality". In: *Pattern Recognition Letters* 128 (2019), pp. 270–277.

[262] Hui Zhang et al. "Construction of a complete set of orthogonal Fourier–Mellin moment invariants for pattern recognition applications". In: *Image and vision computing* 28.1 (2010), pp. 38–44.

[263] Kai Zhang et al. "Beyond a gaussian denoiser: Residual learning of deep cnn for image denoising". In: *IEEE transactions on image processing* 26.7 (2017), pp. 3142–3155.

[264] Xiaoyan Zhang, Chao Wang, and Sumei Li. "Image encryption technology on two-dimensional cellular automata". In: *Journal of Optoelectronics Laser* 19.2 (2008), p. 242.

[265] Yue Zhang et al. "Zernike moment-based spatial image steganography resisting scaling attack and statistic detection". In: *IEEE Access* 7 (2019), pp. 24282–24289.

[266] Liang Zhao and Larry S Davis. "Closely coupled object detection and segmentation". In: *Tenth IEEE International Conference on Computer Vision (ICCV'05) Volume 1*. Vol. 1. IEEE. 2005, pp. 454–461.

[267] Yan Zhao et al. "Robust hashing for image authentication using Zernike moments and local features". In: *IEEE transactions on information forensics and security* 8.1 (2012), pp. 55–63.

[268] Liang Zheng, Yi Yang, and Qi Tian. "SIFT meets CNN: A decade survey of instance retrieval". In: *IEEE transactions on pattern analysis and machine intelligence* 40.5 (2017), pp. 1224–1244.

[269] Chao Zhou et al. "Information security defense method of electric power control system based on digital watermark". In: *2016 3rd International Conference on Materials Engineering, Manufacturing Technology and Control*. Atlantis Press. 2016, pp. 174–179.

[270] Jian Zhou et al. "Image analysis by discrete orthogonal Hahn moments". In: *International Conference Image Analysis and Recognition*. Springer. 2005, pp. 524–531.

[271] Hongqing Zhu. "Image representation using separable two-dimensional continuous and discrete orthogonal moments". In: *Pattern Recognition* 45.4 (2012), pp. 1540–1558.

[272] Hongqing Zhu et al. "Image analysis by discrete orthogonal dual Hahn moments". In: *Pattern Recognition Letters* 28.13 (2007), pp. 1688–1704.

[273] Hongqing Zhu et al. "Image analysis by discrete orthogonal Racah moments". In: *Signal Processing* 87.4 (2007), pp. 687–708.

[274] Hongqing Zhu et al. "Translation and scale invariants of Tchebichef moments". In: *Pattern recognition* 40.9 (2007), pp. 2530–2542.

[275] Shenli Zhu, Guojun Wang, and Congxu Zhu. "A secure and fast image encryption scheme based on double chaotic S-boxes". In: *Entropy* 21.8 (2019), p. 790.

[276] Barbara Zitova and Jan Flusser. "Image registration methods: a survey". In: *Image and vision computing* 21.11 (2003), pp. 977–1000.

[277] Joviša Žunić, Kaoru Hirota, and Paul L Rosin. "A Hu moment invariant as a shape circularity measure". In: *Pattern Recognition* 43.1 (2010), pp. 47–57.