REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE FERHAT ABBAS SETIF-1

FACULTE DE TECHNOLOGIE

THESE

Présentée au Département d'Electronique

Pour l'obtention du Diplôme de

DOCTORAT EN SCIENCES

Filière : Electronique **Option : Electronique**

Par

BEKKOUCHE TOUFIK

THEME

Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes

Soutenue le 14/10/2018 devant le Jury :

HASSAM A.	**Professeur**	**Univ. F. Abbas Sétif 1**	**Président**
BOUGUEZEL S.	**Professeur**	**Univ. F. Abbas Sétif 1**	**Directeur de thèse**
SAIGAA D.	**Professeur**	**Univ. M. Boudiaf Msila**	**Examinateur**
ROUABEH K.	**M.C.A.**	**Univ. B.Ibrahimi BBA**	**Examinateur**

Sommaire

Chapitre2 : Transformées paramétriques et suites chaotiques

Remerciements

J'ai le devoir d'adresser mes remerciements les plus sincères à Monsieur ***Saad. Bouguezel****, professeur à l'Université Ferhat Abbas - Sétif 1, mon directeur de thèse, pour ses conseils et ses directives si précieux, pour sa disponibilité et sa patience, qu'il trouvera mes expressions de reconnaissance, de profonde gratitude et du grand respect.*

J'adresse aussi, mes sincères remerciements les plus profonds à Monsieur ***Abdelouahab.Hassam*** *, professeur à l'Université Ferhat Abbas - Sétif 1, à l'intérêt accordé à mon travail et qui m'a fait le grand honneur de présider ce jury.*

Mes remerciements chaleureux s'adressent également à Monsieur ***Djamel.Saigaa*** *professeur à l'Université Mohamed Boudiaf M'sila de m'avoir honoré d'examiner ce travail .je lui exprime ma profonde gratitude et mon meilleur respect.*

J'exprime ma gratitude la plus profonde et mon meilleur respect à Monsieur ***Khaled.Rouabeh*** *maître de Conférences à l'Université El Bachir El Ibrahimi-Bordj Bouarerridj , par sa présence, en acceptant examiner ce travail.*

Je tiens à remercier, mes chers amis et collègues ***D^{rs} : Daachi.Hocine****, et* ***Azoug Seif-eddine*** *pour leurs relecture, leurs remarques et conseils m'ont été, judicieux, constructifs et très bénéfiques.*

Mes remerciements s'adressent à tous mes amis enseignants, en particulier Monsieur ***Mokhnache.Salah*** *, mon compagnon du parcours, pour leurs soutien et encouragements, à tous ceux qui m'ont aidé et soutenu, je leurs dis merci.*

Enfin à toute ma famille, mes parents, ma femme, mes enfants et mes frères, je les remercie pour leurs encouragements, pour leurs contributions et leurs sacrifices dans l'élaboration de ce modeste travail.

Liste des figures

Chapitre1 : Etat de l'art du cryptage d'images

Chapitre2 : Transformées paramétriques et suites chaotiques

Chapitre3 : Proposition d'une nouvelle technique de cryptage basée sur un pré-cryptage non linéaire récursif

Chapitre4 : Proposition d'une nouvelle technique de cryptage en exploitant la symétrie de la transformée de Fourier paramétrique

Liste des tableaux

Liste des abréviations

DRPE	**D**ouble **R**andom **P**hase **E**ncoding
DFT	**D**iscrete **F**ourier **T**ransform
PLCM	**P**iecewise **L**inear **C**haotic **M**ap
C2R	**C**omplex to **R**eal
R2C	**R**eal to **C**omplex
IBM	**I**nternational **B**usiness **M**achines
NSA	*National Security Agency*
DES	**D**ata **E**ncryption **S**tandard
RSA	**R**onald **R**ivest, Adi **S**hamir et Leonard **A**dleman
AES	**A**dvanced **E**ncryption **S**tandard
PRNG	**P**seudo **R**andom **N**umber **G**enerator
DCT	**D**iscrete **C**osine **T**ransform
DWT	**D**iscrete **W**avelets **T**ransform
IDFT	**I**nverse **D**iscrete **F**ourier **T**ransform
FRFT	**F**ractional **F**ourier **T**ransform
ROP	**R**eciprocal-**O**rthogonal **P**arametric
MPDFRFT	**M**ultiple-**P**arameters **D**iscrete **F**ractional **F**ourier **T**ransform
RFRFT	**R**andom **F**ractional **F**ourier **T**ransform
MPDFRRT	**M**ultiple-**P**arameters **D**iscrete **F**ractional **R**andom **T**ransform
PSNR	**P**eak **S**ignal to **N**oise **R**atio
NPCR	**N**umber of **P**ixels **C**hange **R**ate
MSE	**M**ain **S**quare **E**rror
UACI	**U**nified **A**verage **C**hanging **I**ntensity
NIST	**N**ational **I**nstitute of **S**tandards **T**echnologie
SSL	**S**ecure **S**ockets **L**ayer
S/MIME	**S**ecure/**M**ultipurpose **I**nternet **M**ail **E**xtensions
FT	**F**ourier **T**ransform
DHT	**D**iscrete **H**artley **T**ransform
DFRFT	**D**iscrete **F**ractional **F**ourier **T**ransform
MPDFRFT-DRPE	**D**RPE **B**ased **M**PDFRFT
DFRFT- DRPE	**D**RPE **B**ased **D**FRFT
LSFR	**L**inear **F**eedback **S**hift **R**egister
CCD	**C**harge **C**oupled **D**evice

Introduction générale

Les communications ont toujours constitué un aspect important dans l'acquisition de nouvelles connaissances et l'essor de l'humanité. Le besoin d'être en mesure d'envoyer un message de façon sécuritaire est probablement aussi ancien que les communications elles-mêmes. D'un point de vue historique, c'est lors des conflits entre nations que ce besoin a été le plus vif. Dans notre monde moderne, où diverses méthodes de communication sont utilisées régulièrement, le besoin de confidentialité est plus présent que jamais à une multitude de niveaux. Par exemple, il est normal qu'une firme désire protéger ses nouveaux logiciels contre la piraterie, que les institutions bancaires veuillent s'assurer que les transactions sont sécuritaires et que tous les individus souhaitent que l'on protège leurs données personnelles. Par ailleurs, le besoin de communications sécuritaires a donné naissance à une discipline connue sous le nom de *cryptologie*. Etymologiquement, la cryptologie apparait comme la science du secret. Elle n'est cependant considérée comme une science que depuis peu de temps ; depuis qu'elle allie l'art du secret à celui de la piraterie. En effet, la cryptologie se compose de deux parties complémentaires: la cryptographie et la cryptanalyse. La première partie consiste à étudier et concevoir des procédés de chiffrement des informations alors que la seconde a pour objectif l'analyse des textes chiffrés en raison d'extraire les informations dissimulées [1]. Ces informations peuvent être sous forme de données textuelles, audio ou sous forme d'images numériques et autres multimédia.

Les images sont largement utilisées dans notre vie quotidienne, alors plus leur utilisation est croissante, plus leur sécurité est vitale. Par exemple, il est primordial de protéger les plans de bâtisses militaires, les plans de construction d'une banque ou bien les images captées par des satellites militaires. En plus avec la progression continue de la cybercriminalité, la sécurité des images numériques est devenue un thème important dans le monde des communications. Dans de telles circonstances, il est devenu nécessaire et impératif de crypter les images numériques avant de les transmettre. En effet, Plusieurs techniques de cryptage d'images ont vu le jour aussi bien dans le domaine spatial que dans le domaine fréquentiel [2].

Dans le domaine spatial, les algorithmes de cryptage proposés s'articulent essentiellement sur l'architecture de confusion-diffusion [3]. Dans la phase de confusion, les pixels subissent des changements de positions sous contrôle de suites chaotiques tandis que le changement de leurs valeurs est réalisé dans la phase de diffusion moyennant un operateur xor.

Dans le domaine fréquentiel, la technique la plus utilisée notamment en optique est certainement la fameuse Double Random Phase Encoding (DRPE) à base de la transformée de

Fourier discrète (DFT) proposée pour la première fois en 1959 par Philippe Refregier et Bahram Javidi [4]. Malgré les améliorations qu'a subi cette technique par introduction des transformées paramétriques à la place de la DFT classique [5-8], et des permutations chaotiques injectées dans le système, elle restera vulnérable vis-à-vis de quelques attaques [9], [10] à cause de la linéarité du système DRPE (ou de ses dérivées) tout entier ce qui constitue un inconvénient. Pour pallier cet inconvénient, plusieurs travaux de recherche ont été réalisés dans la littérature. Or, des techniques hybrides opto-digitales ont été proposées dans ce contexte. Celles-ci consistent à injecter un pré-cryptage digital non linéaire dans le système DRPE (ou ses dérivées). Entre autres, la technique proposée dans [11] qui s'avère d'un grand intérêt du fait qu'elle a amélioré sensiblement la sensibilité de la clé de cryptage par l'introduction d'un prétraitement digital basé sur l'opérateur xor.

Malgré le succès qu'a connu cette technique, elle nécessite encore plus une amélioration plus profonde. Sur cette lancée, nous avons proposé une technique plus complexe et plus performante [12] qui consiste en un pré-cryptage non linéaire récursif. Cela constitue la première contribution dans ce travail de thèse. Cette technique présente un double effet : une non linéarité remarquable et une récursivité qui a la propriété de cumul et de propagation de l'erreur dans le cas d'une attaque avec une clé erronée.

Quant à la seconde contribution de cette thèse, nous avons traité la problématique du système DRPE qui réside dans la forme complexe de l'image cryptée résultante (partie réelle et partie imaginaire), ce qui constitue un véritable fardeau dans sa transmission et son stockage. Pour remédier à ce problème, l'idée a été parvenue en exploitant la propriété de symétrie de la transformée de Fourier paramétrique en introduisant une conversion complexe-à-réel (C2R). Cette façon de faire nous a permis le passage de la forme complexe à la forme réelle de l'image cryptée résultante [13].

Par ailleurs, la thèse est organisée autour de quatre chapitres suivis d'une conclusion et de quelques perspectives.

Le chapitre 1 est consacré à un état de l'art sur le cryptage. En effet, Les bases fondamentales de la cryptographie et la classification des algorithmes de cryptage sont présentés. Le cryptage d'images est aussi abordé tout en passant en revue les travaux réalisés dans la littérature s'agissant de cryptages spatial et fréquentiel. Les techniques employées dans l'évaluation des algorithmes de cryptage d'images sont à leur tour décrites dans ce premier chapitre.

Dans le chapitre 2, nous présentons les transformées paramétriques tout en parlant de leur utilisation dans le système DRPE. Cela est commenté et appuyé par des présentations de quelques schémas de cryptage existants avec des explicatives et des illustrations nécessaires. Nous présentons également le chaos vu son utilité grandissante dans la plus part d'algorithmes de cryptage. En effet, deux suites chaotiques à savoir la suite logistique et la suite chaotique linéaire par morceaux (PLCM) sont présentées.

S'agissant du chapitre 3, nous abordons le problème de linéarité que présente la technique de cryptage la plus utilisée et la nécessité de penser à une solution efficace. Cela constitue justement le contexte dans lequel notre nouvelle approche a été proposée et décrite dans ce chapitre. Il s'agit d'une nouvelle technique opto-digitale de cryptage d'images basée sur un pré-cryptage récursif non-linéaire [12]. Ce pré-cryptage est effectué dans le domaine spatial à base de l'opérateur XOR puis injecté dans le système DRPE. Une comparaison avec d'autres techniques existantes dans la littérature est également présentée.

Le chapitre 4 est réservé à la présentation de notre seconde contribution [13]. Elle consiste en l'exploitation de la symétrie dont est caractérisée la transformée de Fourier paramétrique dans le domaine de cryptage d'images. Cette solution permet de transmettre et de stocker une seule image cryptée au lieu de deux (partie réelle et partie imaginaire). La technique proposée est réalisée par une simple conversion réversible du complexe vers le réel (C2R). Notons aussi que les résultats de tests d'analyse de sécurité appliquée sur les deux approches proposées sont aussi présentés dans les chapitres 3 et 4.

Chapitre 1

Etat de l'art du cryptage d'images

1.1 Introduction

Dès que les hommes apprirent à communiquer, ils durent trouver des moyens d'assurer la confidentialité d'une partie de leurs communications. Du bâton nommé « scytale » au V^{éme} siècle avant JC, en passant par le carré de Polybe ou encore le code de César, on assista au développement plus ou moins ingénieux de techniques de chiffrement expérimentales dont la sécurité reposait essentiellement dans la confiance que leur accordaient leurs utilisateurs, donc le besoin d'apporter une sécurité accrue remonte sans doute aux origines de l'homme. En effet, le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des informations, c'est-à-dire de les rendre inintelligibles sans une action spécifique. Une première révolution technologique a eu lieu après la première guerre mondiale, mais ce n'est qu'à l'avènement de l'informatique et d'Internet que la cryptographie prenne tout son sens. Les efforts conjoints d'IBM et de la NSA conduisent à l'élaboration du DES (Data Encryption Standard), l'algorithme de chiffrement le plus utilisé au monde durant le dernier quart du XXème siècle. À l'ère d'Internet, le nombre d'applications civiles de chiffrement des informations (banques, télécommunications, cartes bleues, multimédia…) explose. L'image n'a pas fait l'exception, elle est considérée sans doute comme l'une des formes d'information les plus utilisées. En effet, plusieurs techniques de cryptage d'images ont été développées dans la littérature. Vu l'intérêt grandissant de ce domaine, nous présentons dans ce chapitre un état de l'art sur le cryptage d'images. Après avoir relaté les phases les plus marquantes de l'histoire de la cryptographie en général, nous détaillons les concepts de base et la terminologie utilisés dans ce domaine tout en faisant la revue des travaux existants aussi bien dans le domaine spatial que dans le domaine fréquentiel. Nous abordons aussi les techniques d'évaluation des algorithmes de cryptage d'images.

1.2 Concepts de base

1.2.1 Cryptologie

La cryptologie est un mot composé qui tire son origine du grec : cryptos qui signifie secret et logie qui signifie science. En fait, c'est la science du secret et ne peut être vraiment considérée ainsi que depuis peu de temps. Elle englobe la cryptographie, l'écriture secrète et la cryptanalyse, l'analyse de cette dernière [1,14]. On peut dire que la cryptologie est un art ancien et une science nouvelle : un art ancien car Jules César l'utilisait déjà et il fit son apparition dans l'ancien testament sous la forme du code Atbash ; une science nouvelle parce que ce n'est que depuis les années 1970 qu'elle est devenue un thème de recherche scientifique. Cette discipline est liée à beaucoup d'autres, par exemple la théorie des nombres, l'algèbre, la théorie de la complexité, la théorie de l'information, ou encore les codes correcteurs.

1.2.2 Cryptographie

Est une discipline de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés. Elle se distingue de la stéganographie qui fait passer inaperçu un message dans un autre message alors que la cryptographie rend un message inintelligible à autre que qui-de-droit. Elle est utilisée depuis l'Antiquité, mais certaines de ses méthodes les plus importantes, comme la cryptographie asymétrique, datent de la fin du XXe siècle.

- **Chiffrement ou cryptage**

  Est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement.

- **Clé de chiffrement**

  Paramètre constitué d'une séquence de symboles et utilisé, avec un algorithme cryptographique, pour transformer, valider, authentifier, chiffrer ou déchiffrer des données.

- **Déchiffrement**

  C'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en un texte en clair.

- Texte en clair : C'est le message à protéger
- **Texte chiffré :** C'est le résultat du chiffrement du texte en clair.
- **Crypto-système** : C'est l'algorithme de chiffrement.

1.2.3 Cryptanalyse

La cryptanalyse est la technique qui consiste à déduire un texte en clair d'un texte chiffré sans posséder la clé de chiffrement. Le processus par lequel on tente de comprendre un message en particulier est appelé une *attaque*.

Une attaque est souvent caractérisée par les données qu'elle nécessite :

- Attaque sur texte chiffré seul (*ciphertext-only* en anglais) : le cryptanalyste possède des exemplaires chiffrés des messages, il peut faire des hypothèses sur les messages originaux qu'il ne possède pas. La cryptanalyse est plus ardue de par le manque d'informations à disposition.

- Attaque à texte clair connu (*known-plaintext attack* en anglais) : Le cryptanalyste possède des messages ou des parties de messages en clair ainsi que les versions chiffrées. La cryptanalyse linéaire fait partie de cette catégorie.
- Attaque à texte clair choisi (*chosen-plaintext attack* en anglais) : Le cryptanalyste possède des messages en clair peut créer les versions chiffrées de ces messages avec l'algorithme que l'on peut dès lors considérer comme une boîte noire. La cryptanalyse différentielle est un exemple d'attaque à texte clair choisi.
- Attaque à texte chiffré choisi (*chosen-ciphertext attack* en anglais) : Le cryptanalyste possède des messages chiffrés et demande la version en clair de certains de ces messages pour mener l'attaque.

1.3 Historique de la cryptographie

L'histoire du chiffrement retrace une épopée passionnante dans laquelle cryptographes (« crypteurs ») et cryptanalystes (« décrypteurs ») se livrent une bataille acharnée, éternel recommencement de développement d'un algorithme par les uns, de décodage par les autres, de développement d'un nouvel algorithme plus puissant, etc. Dans cette partie, nous allons faire un survol chronologique du chiffrement, de ses méthodes et des technologies qui ont révolutionné son histoire [15].

1.3.1 Période classique : l'Antiquité

Il semble que le premier document chiffré soit une recette secrète de potier, découverte en Irak, et datant de 1550 avant J.C. environ. Hébreux, Babyloniens, Grecs et Romains utilisèrent ensuite des systèmes cryptographiques originaux. Le « carré de Polybe » (vers -150 avant J.C.) est tout particulièrement innovant pour l'époque. Le « chiffre de Jules César », qui consistait à décaler l'alphabet de trois lettres, est resté célèbre. Comme c'est Jules César qui écrit le récit de ses combats (la Guerre des Gaules), on ignore si ce système s'est réellement révélé très solide, mais c'est fort possible.

1.3.2 Période classique : le Moyen Âge

À partir de 1379, des systèmes de chiffrements à base de nomenclateurs sont de plus en plus utilisés.

1.3.3 Méthodes de chiffrement modernes – De la Première Guerre mondiale à l'avènement des machines de cryptage mécanique

Lors de la Première Guerre mondiale, il fut très fréquent que les messages des armées ennemies soient déchiffrés. Ainsi, les Allemands furent-ils en mesure de connaître à l'avance la plupart des offensives russes, alors que les Français et les Anglais parvinrent à déchiffrer des messages allemands très Importants (télégramme Zimmerman, radiogramme de la victoire par exemple). La Seconde Guerre mondiale vit l'apparition des premiers ordinateurs (en 1944) qui vont permettre de casser les codes des armées allemandes (marine, aviation et armée de terre), ce qui va très significativement accélérer la fin de la guerre. Les ordinateurs vont d'ailleurs totalement transformer l'usage de la Cryptographie par la suite, aussi bien pour les attaques que pour la défense. Face aux Japonais, les Américains réussirent également de nombreux déchiffrements importants. Les avantages considérables obtenus par la Cryptographie vont faire que les Américains vont développer, après la guerre, des organismes nationaux puissants, chargés des écoutes, alors que l'Union soviétique, qui avait davantage profité de l'espionnage durant la Seconde Guerre mondiale (orchestre rouge par exemple), va continuer à investir massivement dans l'espionnage.

1.3.4 Méthodes de chiffrement actuelles – Le cryptage à l'ère de l'informatique et d'Internet

L'année 1976 fut une année extraordinaire pour la Cryptographie. Tout d'abord, il y eut la publication du DES, premier algorithme (à clé secrète) entièrement publié et recommandé par le gouvernement américain pour les applications civiles. Ensuite, il y eut la découverte de la Cryptographie à clé publique avec l'algorithme de Diffie-Hellman, puis en 1977 du RSA (**R**ivest Ronald, **S**hamir Adi et **A**dleman Leonard). Les mathématiques impliquées (théorie des nombres, groupes finis) ouvrirent le domaine sur des théorèmes d'algèbres développés depuis plusieurs siècles pour leur beauté et qui, soudain, se virent ouvrir des applications totalement imprévues. Vers 1976, la Cryptographie passe majoritairement des applications militaires (ou de diplomatie) aux applications civiles, en même temps que de plus en plus de chercheurs civils vont se consacrer au domaine. La période actuelle voit l'utilisation de la cryptographie à une échelle massive: paiements bancaires, téléphonie mobile, télévision, satellites, cartes d'identités, cartes de sécurité sociale, etc. En première approximation, l'apparition de moyens de calculs massifs et automatisés a donné un grand avantage aux défenseurs face aux attaquants dans les systèmes cryptographiques. En effet, il existe des algorithmes bien connus (comme l'algorithme AES en cryptographie à clé secrète) qui sont très simples à mettre en œuvre, qui se calculent très rapidement, et qui semblent permettre de générer des messages chiffrés ou de signatures

électroniques qui ne sont cassables avec les meilleurs algorithmes connus que pour des millions d'années de calculs. Cependant, la réalité sur le terrain est bien souvent très différente de cela. En effet, le monde de DVD piratés, de fraudes bancaires ou d'intrusions dans des systèmes par des pirates informatiques. De plus, récemment, l'affaire Snowden a montré que le gouvernement des États-Unis pratiquait, à grande échelle, un programme d'écoute à peine imaginable. Ceci vient principalement du fait que les failles des systèmes se sont bien souvent déplacées des algorithmes vers le matériel ou les erreurs humaines, ces erreurs humaines pouvant être volontairement provoquées (social engineering). De plus, le contrôle du matériel ou des sociétés informatiques géantes donne clairement à certains états un avantage pratique actuellement considérable. La cryptographie a souvent eu une grande importance dans l'histoire. L'apparition des ordinateurs a complètement transformé cette discipline, dont l'usage est devenu massif et dont les attaques se sont déplacées de l'analyse des algorithmes à l'analyse des matériels, des protocoles d'utilisation, des erreurs humaines et du contrôle des systèmes informatiques.

1.4 Principe d'un système cryptographique

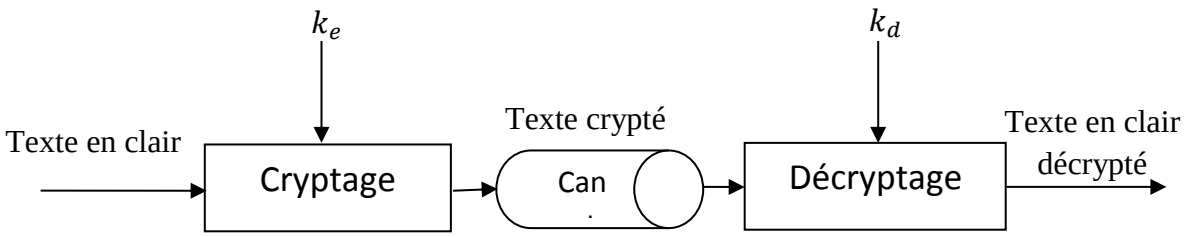


Figure 1.1 : Schéma d'un système cryptographique.

Dans le système cryptographique de la **figure 1.1,** le résultat de cryptage d'un message appelé texte en clair (plaintext) et noté P est un texte crypté (ciphertext) noté C, la fonction de cryptage notée E_{K_e} transforme P en C selon la formule suivante [16]:

$$C = E_{K_e}(P), \tag{1.1}$$

où K_e est la clé de cryptage. La fonction de décryptage, notée D_{K_d}transforme C en P selon la formule suivante :

$$P = D_{K_d}(C), \tag{1.2}$$

où K_d est la clé de décryptage.

Le type de relation qui unit les clefs K_e et K_d utilisées dans le cryptage et le décryptage permet de définir deux grandes catégories de systèmes cryptographiques [1]:

- Les systèmes à clé secrète: la clé est un secret partagé entre l'émetteur et le destinataire($K_e = K_d$) .
- Les systèmes à clé publique: aucune information secrète n'est partagée entre l'émetteur et le destinataire ($K_e \neq K_d$) .

1.5 Objectifs de la cryptographie

La cryptographie est l'étude des techniques mathématiques qui sont utilisées pour accomplir plusieurs objectifs pour garantir la sécurité de communication, ces objectifs sont [14]:

- **La confidentialité:** Il doit être possible pour le récepteur de l'image de garantir son origine. Une tierce personne ne doit pas pouvoir se faire passer pour quelqu'un d'autre.
- **L'intégrité:** Le récepteur doit pouvoir s'assurer que le message n'a pas été modifié durant sa transmission. Une tierce personne ne doit pas pouvoir substitue un message légitime (ayant pour origine l'émetteur) par un message frauduleux.
- **L'authentification:** Offrir au récepteur d'un message la possibilité de vérifier l'identité de l'émetteur pour but de garantir qu'aucune usurpation d'identité n'a eu lieu.
- **La non-répudiation :** Un émetteur ne doit pas pouvoir nier l'envoi d'un message.

1.6 Principes de Kerckhoffs en cryptographie

Un système cryptographique dont les mécanismes internes sont librement diffusés et qui résiste aux attaques continues de tous les cryptanalystes pourra être considéré comme sûr. Le premier à avoir formalisé ce principe est Auguste Kerckhoffs en 1883 dans l'article 'La cryptographie militaire paru dans le Journal des Sciences Militaires. Son article comporte en réalité six principes, connus depuis, sous le nom de *Principes de Kerckhoffs*. On en résumera ici que trois, les plus utiles aujourd'hui :

1. La sécurité repose sur le secret de la clé et non sur le secret de l'algorithme. Ce principe est notamment utilisé au niveau des cartes bleues et dans le chiffrement des images et du son sur Canal+ ;
2. Le déchiffrement sans la clé doit être impossible (en temps raisonnable) ;
3. Trouver la clé à partir du clair et du chiffré est impossible (en temps raisonnable).

1.7 Classification des algorithmes de cryptage

Les algorithmes de cryptage peuvent être classés de différentes manières: selon les clés, selon la structure du cryptage ou selon le domaine de travail [16].

1.7.1 Classification selon la clé de cryptage

Selon les clés, il existe deux types de chiffrements suivant la relation entre les clés K_e et K_d.

1.7.1.1 Cryptage symétrique

Lorsque $(K_e = K_d = k)$, le chiffrement est appelé un chiffrement à clé privée ou un chiffrement symétrique. Pour les chiffrements par clé privée, la clé de chiffrement / déchiffrement doit être transmise de l'expéditeur au destinataire via un canal sécurisé distinct. Comme illustré à la **figure 1.2**, en cryptage symétrique, les clés de cryptage et de décryptage sont identiques. Un exemple de cryptage symétrique est le fameux standard de cryptage AES (Advanced Encryption Standard).

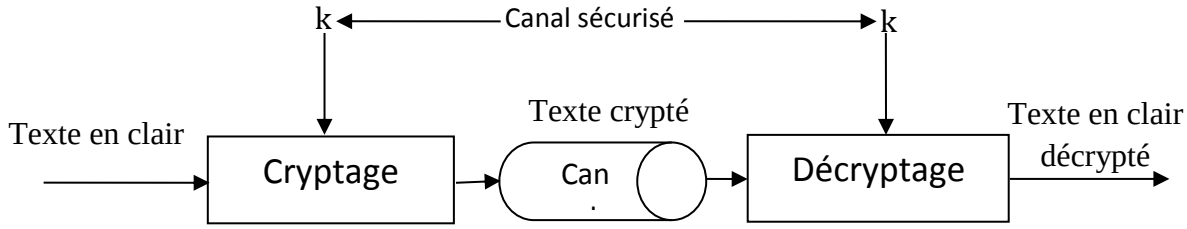


Figure 1.2 : Schéma de cryptage symétrique.

1.7.1.2 Cryptage asymétrique

Lorsque$(K_e \neq K_d)$, le chiffrement est appelé un chiffrement à clé publique ou un chiffrement asymétrique. Pour les chiffrements par clé publique, la clé de chiffrement K_e est publiée et la clé de déchiffrement K_d est gardée privée, pour laquelle aucun canal secret supplémentaire n'est nécessaire pour le transfert de la clé [16]. Le RSA fait partie des algorithmes de cryptage asymétriques.

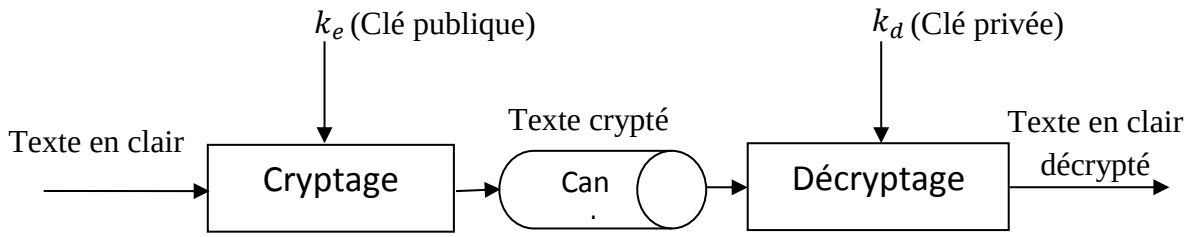


Figure 1.3 : Schéma de cryptage asymétrique.

1.7.2 Classification selon la structure du cryptage

Les algorithmes de chiffrement peuvent être classés en fonction de la structure de chiffrement en chiffrements par blocs et en chiffrements par flots [16].

1.7.2.1 Chiffrement par blocs

Un 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 plusieurs chiffrements par blocs, la taille du bloc est de 64 ou 128 bits. Plus la taille du bloc est grande, plus le chiffrement est efficace, mais plus les algorithmes et les dispositifs de chiffrement et de décryptage sont complexes. Un exemple de cryptage par blocs est le schéma (DES)

1.7.2.2 Chiffrement par flots

Contrairement aux chiffrements par blocs qui fonctionnent sur des blocs de données, les chiffrements par flots fonctionnent généralement sur de petites unités de texte en clair, généralement des bits. Ainsi, les chiffrements par flots sont beaucoup plus rapides qu'un chiffrement par blocs typique. Généralement, un chiffrement par flots génère une séquence de bits en tant que clé (appelée flux de clé) en utilisant un générateur de nombres pseudo-aléatoires (PRNG) qui étend une courte clé secrète (par exemple 128 bits) en une longue chaîne de bits (flux de clé).. Le chiffrement est effectué en combinant le flux de clé avec le texte en clair. Habituellement, l'opération XOR bit à bit est choisie essentiellement pour sa simplicité à effectuer ce chiffrement.

1.7.3 Classification selon le domaine de cryptage

Le cryptage d'images peut être effectué dans l'un des deux domaines : temporel/spatial ou fréquentiel.

1.8 Cryptage d'images dans le domaine spatial

Dans son article apparu en 1949 sur la théorie de la communication des systèmes de sécurité de base [3], Claude Shannon a présenté deux propriétés importantes en cryptographie, ce sont la confusion et la diffusion. Si ces deux propriétés sont prises en considération lors de la conception d'un algorithme de cryptage, elles garantiront la complexité de la relation entre image cryptée et image en clair, cela permet de rendre l'algorithme robuste contre les attaques. Pour réaliser cela, des techniques de substitution et des techniques de permutation sont utilisées [3].

Dans la littérature et en cryptage d'images dans le domaine spatial plusieurs algorithmes sont développées selon l'architecture dite de permutation-diffusion **figure 1.4.** Cette architecture comprend deux opérations importantes, la permutation et la diffusion, la combinaison entre les deux est aussi possible [17]. Dans la phase de permutation, les pixels de l'image en clair subissent une permutation de position sans altérer leurs valeurs puis dans la phase de diffusion les pixels de l'image permutée subissent une modification de leurs valeurs et gardent leurs positions en se servant de l'operateur Xor ayant une très bonne propriété de récupération de données dans le processus de décryptage.

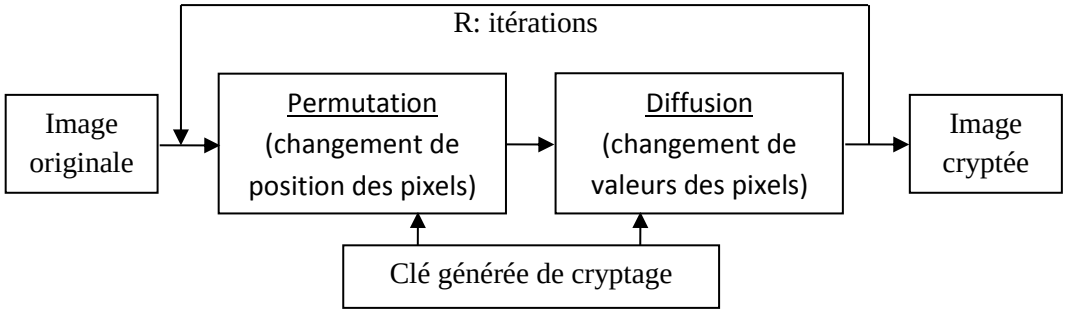


Figure 1.4 : Architecture de Permutation-Diffusion.

1.8.1 Cryptage d'images dans le domaine spatial à base du chaos

La théorie du chaos a joué un rôle déterminant dans la cryptographie moderne et spécialement en cryptage d'images. L'attraction de l'utilisation du chaos comme base pour le développement d'un système cryptographique réside principalement dans son comportement aléatoire, sa sensibilité aux conditions initiales et aux paramètres qui satisfont aux exigences classiques de confusion et de diffusion de Shannon [3]. Les algorithmes basés sur le Chaos [18] ont montré des propriétés exceptionnellement bonnes dans de nombreux aspects concernant la sécurité, la complexité, la vitesse, les surcharges de calcul, etc. Dès 1989, Matthew [19] a proposé pour la première fois un algorithme de cryptage basé sur la suite chaotique logistique. En 1998, Fridrich [20] a suggéré un schéma de chiffrement d'images basé sur le chaos contenant plusieurs itérations de permutation-diffusion. Plus tard, de nombreux chercheurs ont accordé une grande attention au cryptage d'images à base du chaos et ont proposé une variété d'algorithmes [21-28]. Dans [21], Guan et al. Ont utilisé un système de cryptage à base du chat d' Arnold couplé avec la suite chaotique Chen pour but de réaliser la permutation et la diffusion simultanément. Dans

[22], Ye et Wang ont présenté un algorithme de cryptage d'images basé sur le chat d'Arnold généralisé. Dans l'ensemble, cet algorithme comprend trois parties, à savoir, permutation circulaire, diffusion positive et diffusion opposée, et qui peut résister aux attaques de texte en clair connu et choisi. Dans [23], Liu et al. Introduisent un algorithme de cryptage chaotique d'images à clés agissant en même temps. En raison de la dynamique plus complexe de l'hyper-chaos que le chaos, Gao et al ont brouillé l'image en clair par le biais de la suite Logistique, puis ils ont utilisé l'hyper-chaos [24] pour crypter l'image brouillée. Dans [25], Zhao et al. ont proposé un schéma de chiffrement d'images basé sur un système chaotique d'ordre fractionnaire impropre. Récemment, dans [26,27], Wang et Zhang ont introduit de nouveaux réseaux spatio-temporels, qui ont une cryptographie plus performante que la suite logistique. Les résultats de la simulation ont démontré la haute sécurité et l'efficacité élevée de ces algorithmes. Dans [28], Liu et al. ont proposé un algorithme de cryptage d'images rapide basé sur une nouvelle fonction de modulation Sinus bidimensionnelle. La recherche dans ce domaine demeure un exercice perpétuel qui se renoue à chaque fois un algorithme récent est révélé par les cryptanalystes.

1.8.2 Cryptage d'images dans le domaine spatial à base de permutations (bit level)

L'idée de base de l'utilisation du 'bit level ' dans le cryptage d'images dans le domaine spatial est de décomposer l'image en clair ayant un niveau de gris allant de 0 à 255 comme illustrer dans la **figure 1.5** en huit images binaires selon la position du bit dans le pixel [2]. Afin de bien éclaircir l'idée nous donnons l'exemple de l'image binaire de bit 7, le pixel ayant un niveau de gris dépassant ou égal ($2^6 = 64$) en lui attribuant la valeur 1 sinon la valeur 0, donc en général, on assiste à une binarisation de l'image originale selon huit seuils (seuil de l'image binaire de bit 1= $2^0 = 1$; seuil de l'image binaire de bit $2 = 2^1 = 2$; seuil de l'image binaire de bit 3= $2^2 = 4$; ….. et enfin seuil de l'image binaire de bit $8 = 2^7 = 128$). Le **tableau 1.1** indique le pourcentage de contribution de chaque bit dans l'information contenue dans un pixel, calculé selon la formule suivante :

$$p(i) = \frac{2^i}{\sum_{j=0}^{7} 2^j} \times 100\%, \quad \text{où } i \in \{0,1,2,3,4,5,6,7\} \tag{1.3}$$

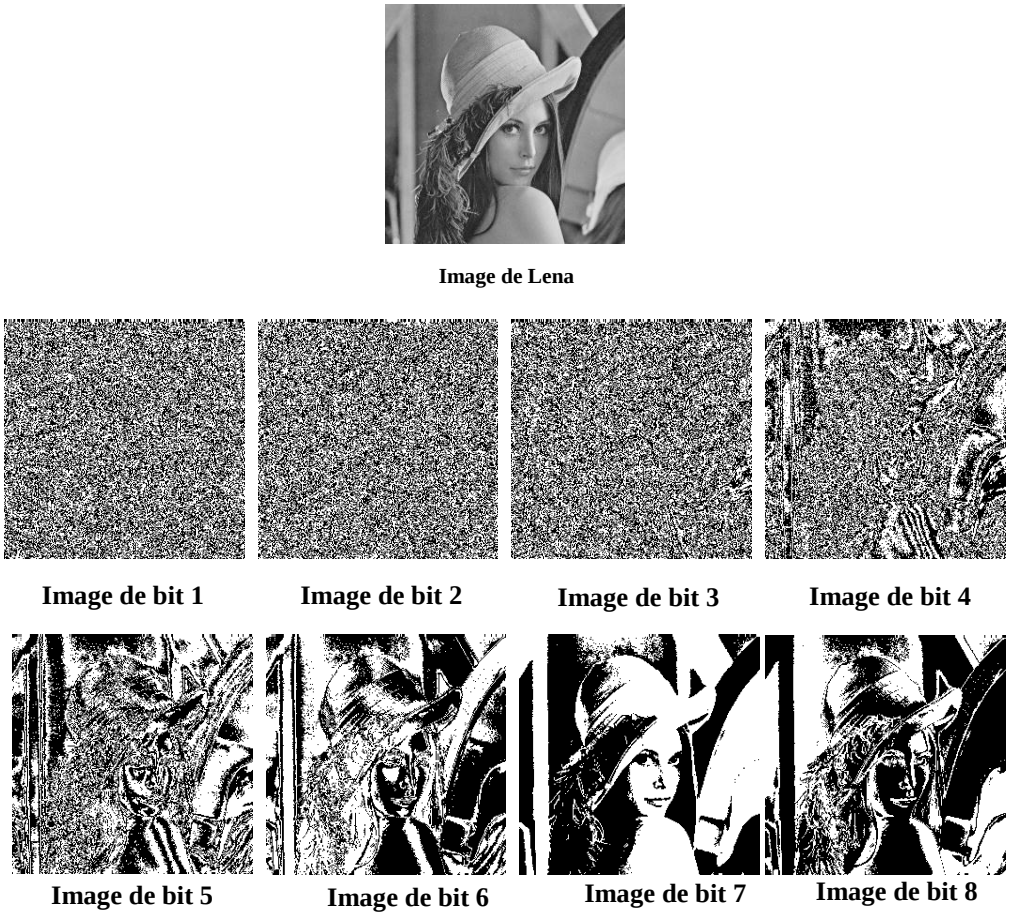


Figure 1.5 : Illustration de la décomposition de l'image de Lena en huit images binaires (bit level).

Tableau 1.1 Pourcentage de contribution de chaque bit dans l'information contenue dans un pixel.

Position i du bit dans le pixel	Pourcentage d'information $p(i)$ en % du bit dans le pixel
0	**0.3922**
1	**0.7843**
2	**1.12686**
3	**3.137**
4	**6.275**
5	**12.55**
6	**25.10**
7	**50.20**

Nous remarquons selon le **Tableau 1.1** que les quatre premiers bits de poids fort détiennent presque la totalité de l'information contenue dans le pixel avec un pourcentage de **94.125%.** Par contre, les quatre derniers bits de poids faible détiennent moins de **6%** de l'information totale. A

la lumière des explications données les algorithmes de cryptage d'images utilisant la technique de ' bit level' ne sont pas sortis des exigences classiques de confusion et de diffusion de Shannon en adoptant l'architecture de permutation-diffusion. Les permutations sont faites entre images binaires résultat de décomposition de l'image originale, les modifications des valeurs des pixels dans la phase de diffusion sont faites sur l'image reconstruite après permutation, en se servant des suites chaotiques, le chat d'Arnold ou la suite de Baker. Xiang et al. ont proposé un schéma de chiffrement d'images sélectif qui crypte les quatre bits les plus élevés de chaque pixel et laisse les quatre bits inférieurs inchangés [29]. Dans [30], Zhu et al ont présenté un schéma de permutation (bit level) au niveau des bits pour le cryptage d'images basé sur le chat d'Arnold et la suite logistique, les paramètres du chat d'Arnold sont générés par la suite logistique. Comme les quatre bits contiennent presque toutes les informations dans l'image, ils sont confus indépendamment, tandis que les quatre bits de poids faibles sont permutés seulement.

1.9 Cryptage d'images dans le domaine fréquentiel basé sur les transformées discrètes

Le cryptage d'images dans le domaine fréquentiel s'effectue par transformation de l'image à crypter au domaine fréquentiel en utilisant les transformées discrètes comme la transformée en cosinus discrète (DCT) [31], et la transformée en ondelettes discrète (DWT) [32]. En effet c'est dans ce domaine où s'opèrent les modifications nécessaires selon l'algorithme de cryptage proposé pour brouiller l'image à crypter puis revenir au domaine spatial de nouveau. Malgré les contributions et les recherches présentées par utilisation de la DCT et la DWT , la (DFT) s'avère la plus utilisée surtout dans le domaine optique, du fait que la technologie de l'information optique offre les possibilités d'un traitement parallèle des données et à grande vitesse, or la sécurité de l'information dans le domaine optique à reçu une attention particulière au cours de ces dernières années, et le cryptage d'images à base de la transformée (DFT) peut être facilement implémenté dans le domaine optique. La technique de cryptage (DRPE) est un schéma de cryptage optique classique qui utilise deux masques de phase aléatoires statistiquement indépendants ou le premier masque est appliqué dans le domaine spatial pour embrouiller l'image et le second dans le domaine de la transformée de Fourier.

1.9.1 Cryptage basé sur deux masques de phases aléatoires

Philippe Refregier et Bahram Javidi étant les pionniers et les fondateurs de la méthode de cryptage d'images DRPE dans le domaine optique en proposant en 1995 une technique de cryptage d'images dans le domaine de la transformée de Fourier et qui rendra l'image originale à crypter un bruit blanc stationnaire d'amplitude complexe [4].

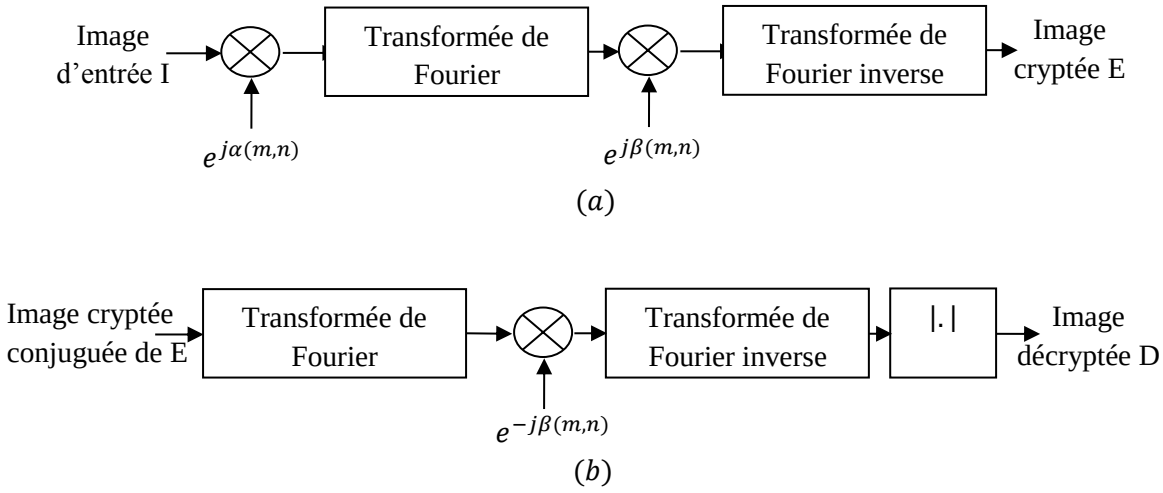


Figure 1.6 : Cryptage optique d'images proposé par Philippe Refregier et Bahram Javidi dans le domaine de la transformée de Fourier *(a)* Schéma de cryptage *(b)* Schéma de décryptage.

Le schéma de cryptage de la **figure 1.6.*(a)*** a bien illustré la technique proposé et qui consiste à (1) multiplier l'image d'entrée par le premier masque de phase aléatoire dans le domaine spatial, (2) transformer le résultat obtenu à partir de (1) en utilisant la DFT, (3) multipliant le résultat obtenu de (2) par un autre masque de phase aléatoire dans le domaine fréquentiel, et enfin (4) transformant le résultat obtenu de (3) en utilisant la transformée de Fourier discrète inverse (IDFT) pour obtenir l'image cryptée. Le deuxième masque a la même taille de l'image d'entrée et qui représente la véritable clé de cryptage.

Le schéma de décryptage est présenté dans la **figure.1.6 *(b)***, qui consiste à prendre l'image cryptée conjuguée, puis il suit exactement le chemin inverse du schéma de cryptage.

Dans le but de renforcer la sécurité de la technique de cryptage DRPE basée sur la transformée de Fourier discrète, d'autres techniques de cryptage d'images ont vu le jour en introduisant des transformées paramétriques comme la transformée de Fourier fractionnaire (FRFT) [5], transformée de Fresnel [33], transformée Gyrator [34], les transformations paramétriques réciproques-orthogonales (ROP) [6],[35] et la transformée paramétrique involutive [7]. Ces transformées ont été utilisées à la place de la DFT standard, où leurs paramètres indépendants ont été exploités comme une clé secrète supplémentaire spécifiquement la FRFT. Cette transformée ce n'est qu'une généralisation de la transformée de Fourier standard par introduction d'un paramètre indépendant dans son noyau (Kernel), Unnikrishnan et Singh [5] comme illustré dans la **figure 1.7** ont remplacé la transformée de Fourier classique dans le schéma de cryptage basée sur deux masques de phases aléatoires [4] par la FRFT et les fractions de cette transformée sont exploitées comme une clé supplémentaire pour le cryptage d'images.

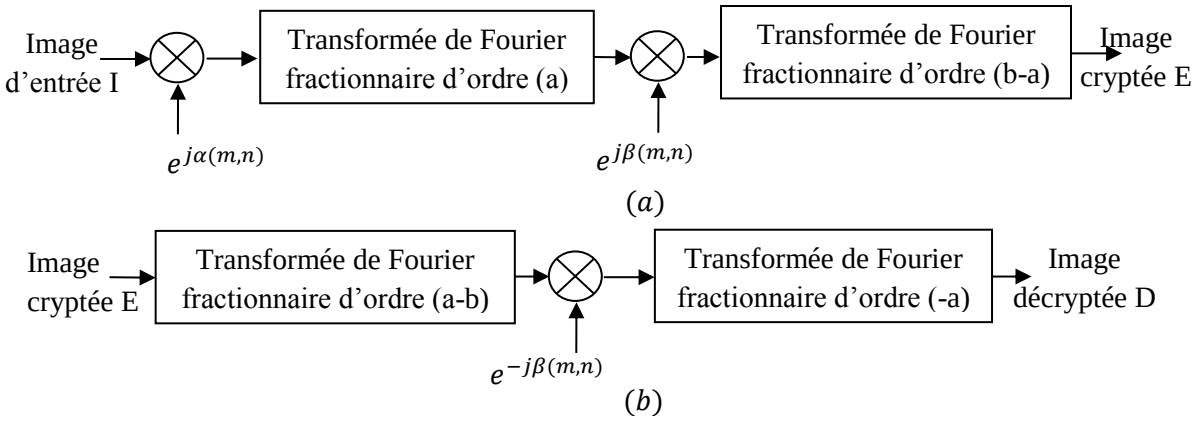


Figure 1.7 : Cryptage d'images optique proposé par Unnikrishnan et Singh dans le domaine de la transformée de Fourier fractionnaire *(a)* Schéma de cryptage *(b)* Schéma de décryptage.

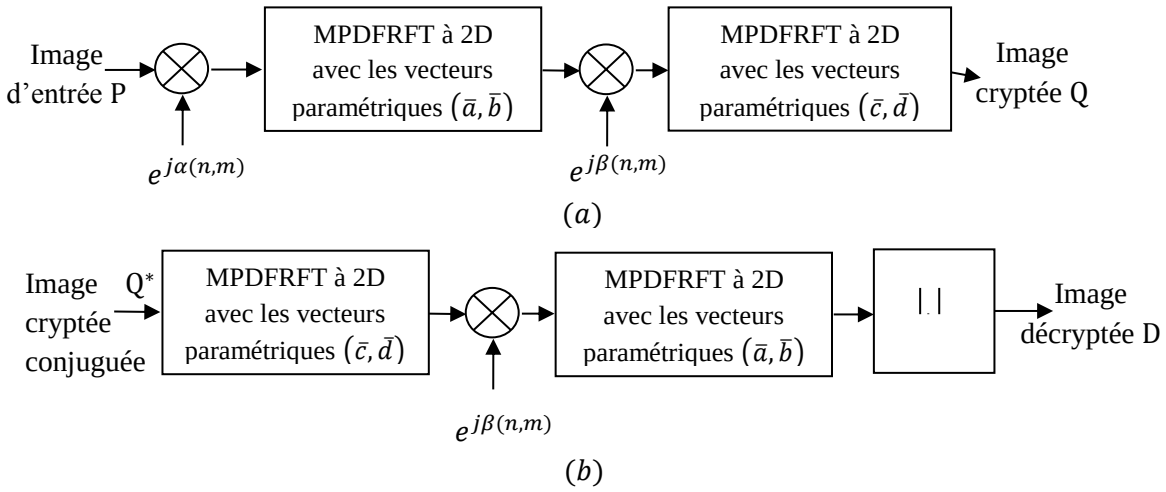


Figure 1.8 : Cryptage d'images proposé par Pie and Hsue dans le domaine de la transformée de Fourier fractionnaire discrète à paramètres multiples *(a)* Schéma de cryptage *(b)* Schéma de décryptage.

Sur la même lancée des transformées paramétriques et afin de consolider les travaux présentés par Unnikrishnan and Singh [4], Pie et Hsue [8] ont proposé une méthode de cryptage d'images basée sur deux masques de phases aléatoires dans le domaine de la transformée de Fourier fractionnaire discrète à paramètres multiples (MPDFRFT), cette transformée est une généralisation de la transformée FRFT par introduction de plusieurs paramètres indépendants (multiple ordres fractionnaires) au lieu d'un seul dans le noyau (Kernel) de la transformée FRFT, ces paramètres sont exploités avec succès dans ce schéma de cryptage comme des clés secrètes additionnelles de cryptage **figure 1.8**.

L'introduction des transformées discrètes fractionnaires aléatoires par Liu Z, et al en 2005 [36], en assignant une phase aléatoire directement aux valeurs propres de FRFT [20] suivi par la nouvelle transformée de Fourier fractionnaire aléatoire (Random Fractional Fourier Transform (RFRFT)) proposée par Z. J .Liu et al en 2007 [37] puis, la transformée Multi-Parameter Discrete Fractional Random Transform (MPDFRRT) [38], ont été bien exploitées dans le domaine de cryptage d'images et ont permis un élargissement consistant de l'espace clé de cryptage.

Bien que, ces transformations paramétriques sont attrayantes, leur utilisation directe dans la DRPE classique n'est pas très intéressante du point de vue sensibilité de la clé de cryptage et par conséquent la sécurité du système de cryptage tout entier [11], puisque tout le système DRPE peut être considéré comme une transformation linéaire, et par conséquent, il n'est pas robuste contre certaines attaques [9,10]. L'apparition des techniques d'holographie numérique [39], ont permis à une image cryptée optiquement à base de la technique DRPE d'être transmise, stockée ou déchiffrée numériquement et qui ont rendu l'application de la DRPE dans les communications numériques possible et réalisable. De ce fait plusieurs méthodes hybrides de cryptage opto-digitales ont attiré l'attention des chercheurs [40-45]. Dans [42], Singh et al ont généré numériquement les masques de la DRPE en utilisant des suites chaotiques, qui sont connus par leurs bonnes propriétés cryptographiques telles que la haute sensibilité à leurs paramètres initiaux, l'ergodicité, et leurs caractères pseudo-aléatoires [46].

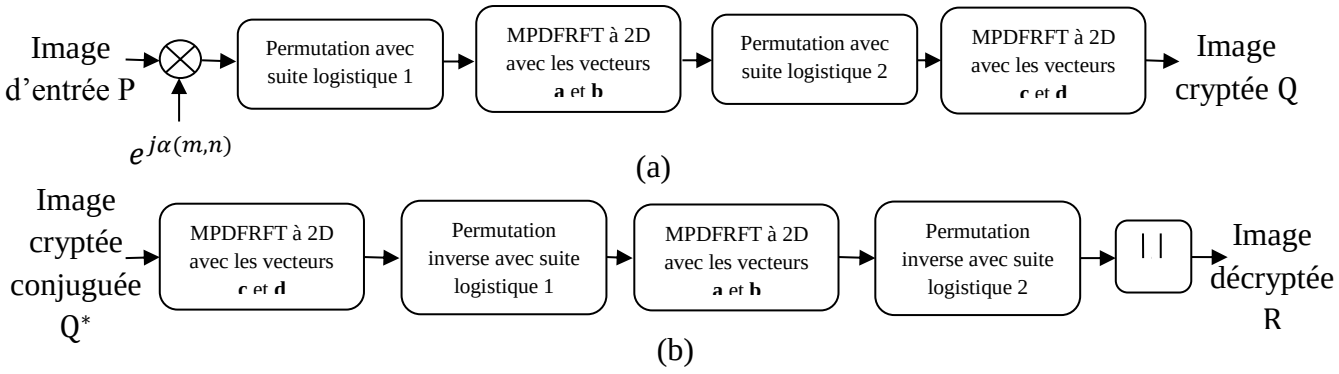


Figure 1.9 : Méthode de cryptage / décryptage d'images proposée par Lang et al basée sur la technique de brouillage de pixels à base de la suite chaotique logistique dans le domaine MPDFRFT.

Dans [43-45], des schémas de cryptage opto-numérique ont été proposés pour améliorer la DRPE classique en introduisant des techniques de permutation aléatoire numérique. Hennelly et al suggèrent dans [43] d'enlever le second masque du DRPE et effectuer des permutations sur les blocs d'image dans le domaine spatial et dans le domaine de la transformée FrFT en utilisant la transformée Jigsaw calculée numériquement. Liu et al proposent dans [44] d'enlever les deux masques de la DRPE et effectuer des permutations dans le domaine spatial et dans le domaine fréquentiel de la transformée FRFT en exploitant la transformée Jigsaw couplée au chat de permutation d'Arnold. Dans [45], Lang et al retiennent le premier masque et suggèrent une fonction de permutation basée sur la suite chaotique logistique appliquée dans les deux domaines spatial et domaine de la transformée MPDFRFT **figure.1.9**.

Même si ces méthodes qui sont basées sur les permutations s'avèrent efficaces et mieux que la DRPE classique, leur niveau de sécurité de chiffrement est encore faible du fait que les prétraitements (permutations) adoptés sont des transformations linéaires. Cela peut clairement être vu de la cryptanalyse réalisée dans [47,48], [10].

Azoug et Bouguezel [11] ont proposé une technique de cryptage d'images opto-digitale (hybride), qui consiste à modifier la DRPE classique en introduisant un nouveau prétraitement non linéaire toute en conservant le premier masque, en remplaçant le second masque par une permutation chaotique, et substituant la transformée de Fourier par la transformée MPDFRFT.

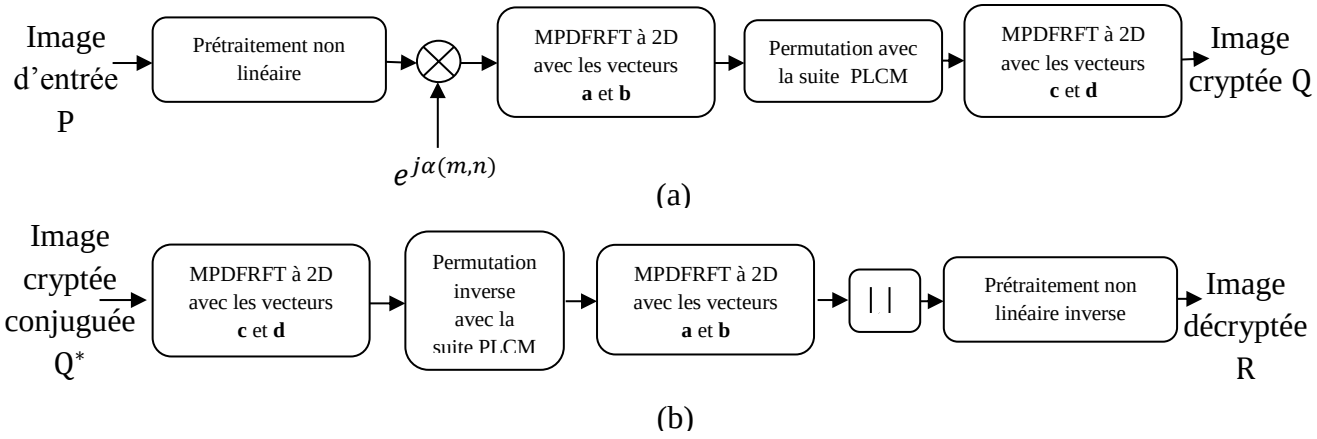


Figure 1.10 : Méthode de cryptage/décryptage d'images proposée par Azoug and Bouguezel basée sur la technique d'introduction d'un prétraitement non linéaire couplée avec la suite chaotique PLCM dans le domaine MPDFRFT.

La non-linéarité de ce prétraitement est effectuée numériquement dans le domaine spatial en utilisant la suite chaotique PLCM couplée avec OU exclusif (XOR) des bits. Ce prétraitement non linéaire est d'une grande importance pour améliorer la sécurité du système cryptographique

et surmonter le problème de linéarité mentionné ci-dessus. Le premier masque est gardé pour blanchir l'image [43,45]. La permutation chaotique est effectuée dans le domaine MPDFrFT en utilisant également un PLCM. L'opération XOR est calculée numériquement au lieu d'une implémentation XOR entièrement optique comme est fait dans [49]. Cette technique peut être classée comme étant un algorithme de cryptage symétrique, où les paramètres PLCMs avec les multiples ordres fractionnaires des MPDFRFT constituent la clé secrète privée pour le cryptage et le décryptage **figure 1.10.**

1.9.2 Cryptage basé sur deux masques d'amplitudes aléatoires

L'un des inconvénients majeurs de la technique de cryptage d'image DRPE ou ses dérivées est que l'image cryptée est complexe (partie réelle et partie imaginaire) ayant toutes les deux la même taille de l'image d'entrée à crypter, on s'affronte donc à une double image au lieu d'une seule. Cela devient un grand fardeau que se soit en transmission, en stockage et même en décryptage aussi, sans pour autant tenir compte du temps de traitement donc incommode en réelles applications. Pour remédier à ce problème, récemment Chen et Zhao [50] ont proposé une méthode dans laquelle ils ont remplacé les masques de phases aléatoires dans [4] par des masques d'amplitudes aléatoires k_1 et k_2 **figure.1.11** dans le domaine de la transformée de Hartley, cela a pour but d'exploiter les propriétés de cette transformée notamment la nature réelle, et pour garantir que l'image cryptée soit réelle aussi.

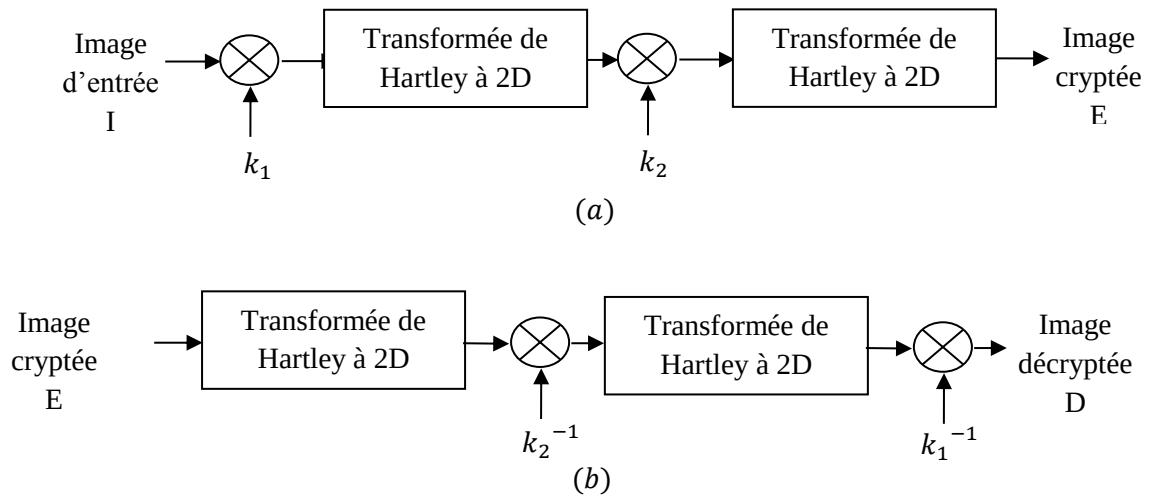
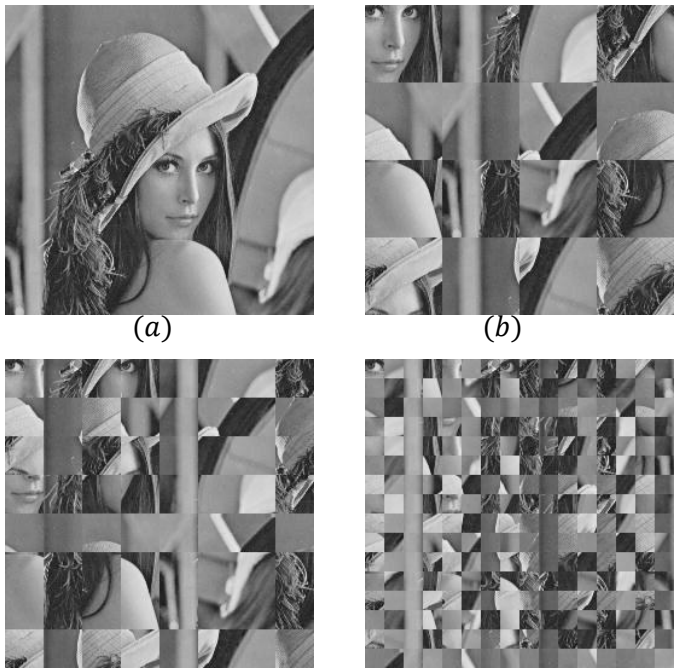


Figure 1.11 : Schéma de cryptage/décryptage d'images basé sur deux masques d'amplitudes aléatoires dans le domaine de la transformée de Hartley proposé par Chen et Zhao: (a) schéma de cryptage, (b) schéma de décryptage.

En réalité mathématiquement parlant cette transformée de Hartley ce n'est que la transformée de Fourier réelle, elle est définie comme étant la partie réelle de la transformée de Fourier ôtée de sa partie imaginaire. Cet algorithme présente une fragilité remarquable vis-à-vis de l'attaque de décryptage aveugle, c'est-à-dire un décryptage sans aucune clé. Une simple transformation inverse de Hartley peut révéler visuellement les informations de l'image. En 2009, et pour remédier à ce problème, Narendra Singh, et Aloka Sinha [51] ont proposé deux méthodes de cryptage d'images, l'une utilisant la transformée de Hartley et la transformée jigsaw **figure 1.12.** L'autre constitue une amélioration de la première en ajoutant un brouillage basé sur la suite chaotique Logistique.



(a) (b)

(c) (d)

Figure 1.12 : Illustration de la transformation jigsaw: (a) Image originale de Lena, (b) Transformation jigsaw avec des blocs de 4×4 (c) Transformation jigsaw avec des blocs de 8×8 (c) Transformation jigsaw avec des blocs de 16×16.

Encore plus, Zhengjun Liu et al ont utilisé la transformée de Hartley aléatoire dans le cryptage d'images basé sur deux masques d'amplitudes aléatoires [52], **figure 1.13.** Cette méthode est essentiellement motivée pour exploiter la nature aléatoire de cette transformée dans le cryptage d'images et qui contribue à l'élargissement de la clé de cryptage.

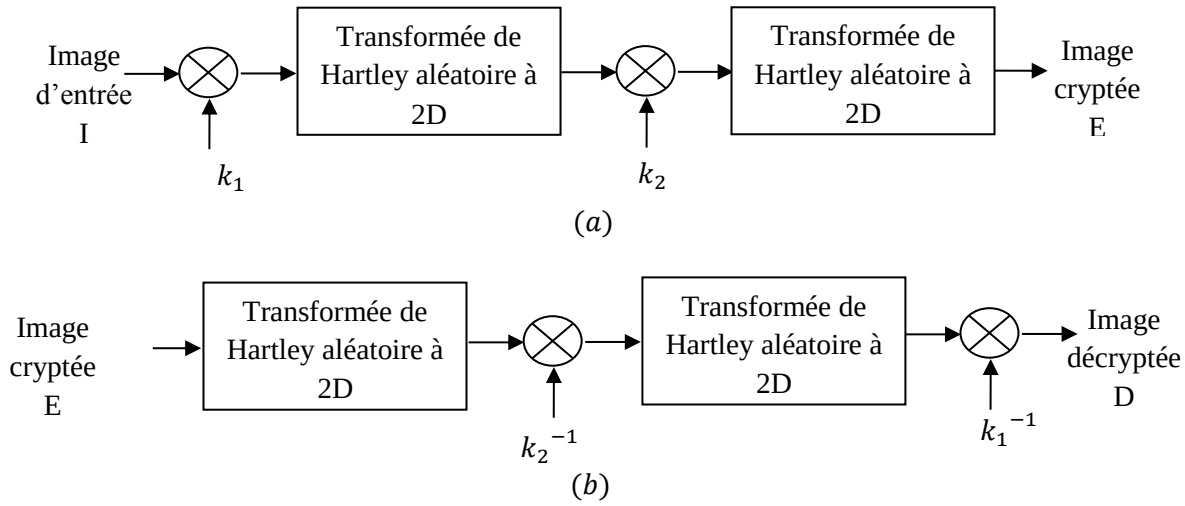


Figure 1. 13 : Schéma de cryptage / décryptage d'images basé sur deux masques d'amplitudes aléatoires dans le domaine de la transformée de Hartley aléatoire proposé par Zhengjun Liu et al: (a) schéma de cryptage, (b) schéma de décryptage.

1.10 Mesures de performances

1.10.1 PSNR

En traitement de signal , la mesure habituellement utilisée pour quantifier la distorsion entre un signal original x et ce même signal noyé dans le bruit appelé signal bruité y est le $PSNR$ (Peak Signal-to-Noise Ratio), en cryptage d'images cette mesure est basée essentiellement sur le calcul de la différence (mesures de distances) entre l'image originale et l'image cryptée qui nous renseigne sur le degré d'endommagement de l'image originale provoqué par l'application d'une telle méthode de cryptage [16].

En termes mathématiques, cette mesure est définie pour les images en niveaux de gris.

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right)\ (dB) \tag{1.4}$$

où le MSE(Mean Square Error) est l'erreur quadratique moyenne entre l'image cryptée *E* et l'image originale correspondante *I*.

$$MSE = \left(\frac{1}{M \times N}\sum_{m=1}^{M}\sum_{n=1}^{N}\left|i_{m,n} - e_{m,n}\right|^2\right) \tag{1.5}$$

où $i_{m,n}$ et $e_{m,n}$ désignent les valeurs de pixels à la position (m, n) de l'image originale et cryptée, respectivement, $M \times N$ indique la taille de l'image.

1.10.2 Coefficient de corrélation

Le coefficient de corrélation standard est utilisé pour mesurer la similarité entre les images cryptées et les images originales. Il peut être défini comme suit

$$corr(I,E) = \frac{\sum_m \sum_n (i_{m,n} - \bar{I})(e_{m,n} - \bar{E})}{\sqrt{\sum_m \sum_n (i_{m,n} - \bar{I})^2 \sum_m \sum_n (e_{m,n} - \bar{E})^2}} \quad (1.6)$$

où $\bar{I} = moyenne(I)$ et $\bar{E} = moyenne(E)$ sont les valeurs moyennes des images originales et cryptées, respectivement.

1.10.3 Analyse d'histogramme

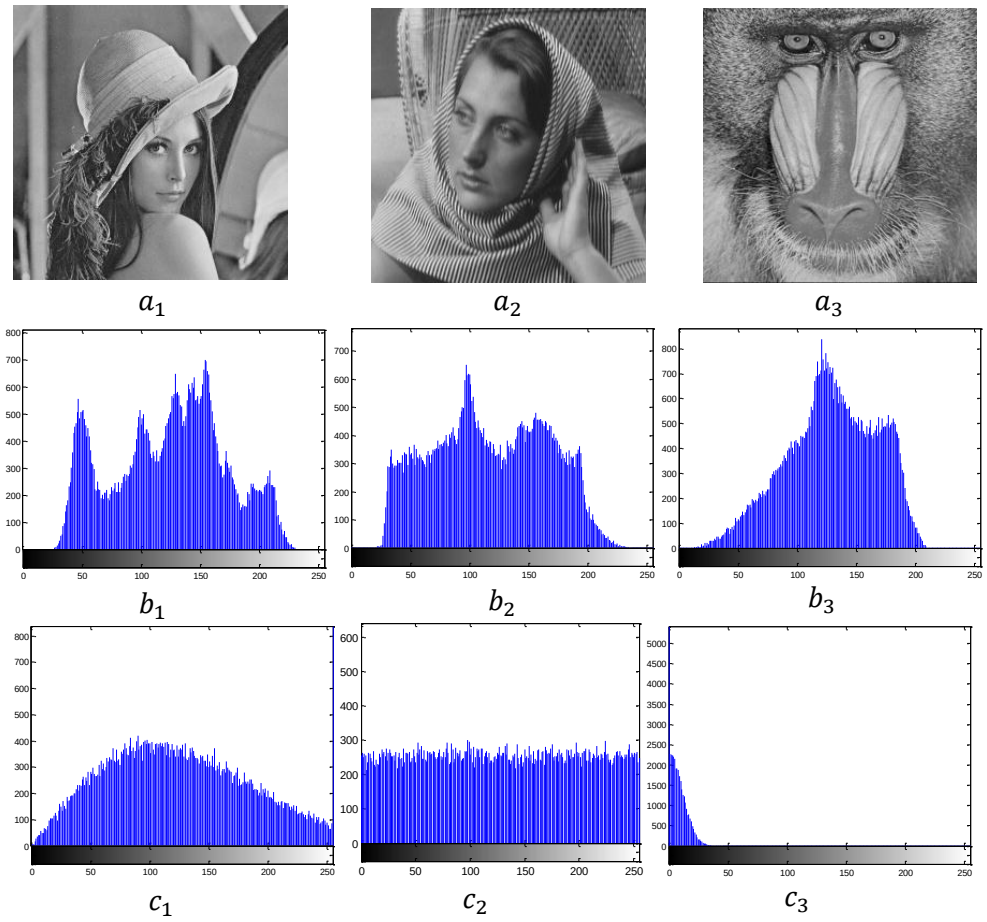


Figure 1.14 : Images originales de (a_1) Lena (a_2) Barbara (a_3) Baboon ; Leurs histogrammes (b_1), (b_2) et (b_3) respectivement ; Forme d'histogramme que peut prendre une image cryptée (c_1) Gaussienne (c_2) Uniforme (a_3) Exponentielle décroissante.

L'histogramme est une représentation graphique qui nous renseigne sur la répartition du nombre des pixels d'une image en fonction de leurs niveaux du gris, l'axe horizontal représente toutes les valeurs du niveau du gris de 0 à 255 et l'axe vertical indique le nombre de pixels ayant

le niveau du gris correspondant. En cryptage d'images, et pour assurer l'efficacité d'une telle technique de cryptage, les histogrammes des images cryptées doivent êtres tous ramenés à une forme unie et différents de ceux des images originales **figure1.14** et ils doivent y avoir une distribution aléatoire (Gaussienne, uniforme, exponentielle décroissante ou une autre forme aléatoire), dans ce cas ils ne révèlent aucune information statistique de l'image originale qui pourra être exploitée par un éventuel attaquant.

1.11 Techniques d'évaluation des algorithmes de cryptage d'images

1.11.1 Analyse de l'espace de la clé de cryptage

L'espace de la clé d'un algorithme de cryptage/décryptage est le total des clés différentes qui peuvent être utilisées dans la procédure de cryptage/décryptage. Une méthode de cryptage d'image est dite sécurisée si elle dispose d'un espace clé de cryptage le plus large possible, elle doit résister aux attaques par force brute où l'attaquant tente à retrouver la clé correcte par manipulations de toutes les combinaisons possibles [53]. Si nous supposons que la taille de cette clé est k, la recherche de la clé correcte prendra 2^k opérations pour réussir à la détecter.

1.11.2 Sensibilité de la clé de cryptage

La sensibilité de la clé de cryptage est évaluée en effectuant une légère modification dans l'un des éléments constituants la clé qui devra produire dans la phase de décryptage une image totalement cryptée et à chaque fois nous augmentons la précision dans cette modification jusqu'au début d'apparition de l'image décryptée en clair. Cette limite donnera la précision de l'élément constituant cette clé. Cette procédure se répétera pour l'ensemble des éléments de la clé, encore plus et dans le domaine fréquentiel à base des transformées paramétriques, nous effectuerons une petite erreur autour des paramètres de la transformée et nous calculons le MSE correspondant. L'ouverture relative à l'apparition de l'image correspond exactement à la précision du paramètre en question, la précision de tous les éléments constituant la clé de cryptage déterminera l'espace clé de l'algorithme de cryptage envisagé.

1.11.3 Attaque différentielle

Pour calculer l'influence d'un changement d'un seul pixel dans l'image originale et sa répercussion sur l'image cryptée correspondante pour n'importe quel algorithme de cryptage, deux grandeurs peuvent être utilisées, $NPCR$ (taux de changement du nombre de pixels), et $UACI$ (Moyenne unifiée du changement d'intensité) définis par les formules suivantes :

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \qquad (1.7)$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j}\frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% \quad (1.8)$$

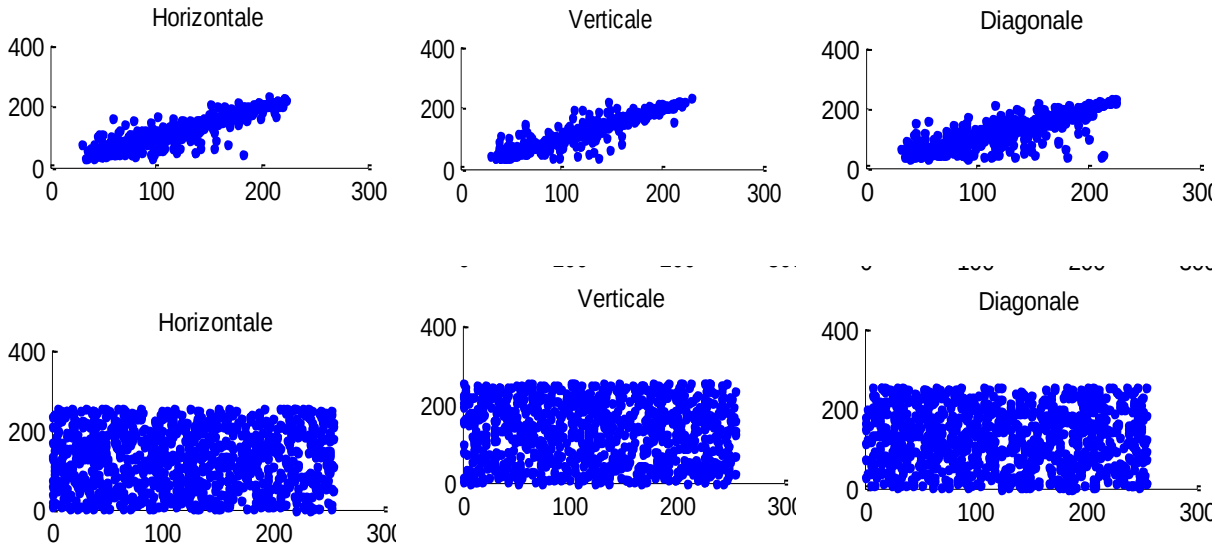
où $C_1(i,j)$ et $C_2(i,j)$ sont les images cryptées correspondants à l'image originale C avant et après modification d'un seul pixel dans l'image originale, D étant une matrice binaire ayant la même taille $M \times N$ que l'image originale est définie comme suit :

$$D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{cases} \quad (1.9)$$

Le $NPCR$ mesure le pourcentage du nombre de pixels différents entre les deux images C_1 et C_2 par rapport au nombre total de pixels, tandis que l'$UACI$ mesure la moyenne de différence d'intensités entre les deux images C_1 et C_2. Un résultat du NPCR/UACI élevé se traduit, généralement, par une forte résistance aux attaques différentielles, autrement dit si un changement mineur dans l'image en clair peut provoquer un changement significatif dans l'image cryptée, alors l'attaque différentielle devient inutile et l'attaquant ne trouve aucune relation significative entre l'image claire et celle cryptée.

1.11.4 Analyse de la corrélation entre pixels adjacents

Il est bien connu qu'il y a une redondance élevée et une forte corrélation entre les pixels voisins d'une image naturelle, et un tel algorithme de cryptage essayera toujours de désamorcer la ressemblance existante entre ces pixels voisins en vue de bloquer les attaquants d'en tirer aucune information qui pourra révéler le système de cryptage utilisé. Le test de corrélation entre pixels adjacents s'agit de sélectionner de façon aléatoire 1000 paires de pixels adjacents de l'image originale et 1000 paires de l'image cryptée et analyser les corrélations aux directions horizontale, verticale et diagonale des deux images originale et cryptée. Les diagrammes de corrélation entre les pixels adjacents aux directions horizontale, verticale et diagonale de l'image de Lena originale et de son image cryptée sont représentés sur la **figure 1.15** et les coefficients de corrélation de l'image originale dans les trois directions se rapprochent de 1, tandis que ceux de son image cryptée se rapprochent de 0. Dans ce cas, nous disons que le chiffrement a atténué considérablement la corrélation entre pixels de l'image cryptée, nous remarquons aussi sur la **figure 1.15** que la distribution des intensités des pixels de l'image originale se concentre sur la diagonale, les pixels sont alors fortement corrélés, tandis que ceux de l'image cryptée sont non-corrélés et ont une distribution uniforme.



(a) (b) (c)

Figure 1.15 : Analyse de corrélation entre pixels adjacents de l'image de Lena : (a) La distribution de l'intensité des pixels selon la direction horizontale de l'image originale et de l'image cryptée ; (b) La distribution de l'intensité des pixels selon la direction verticale de l'image originale et de l'image cryptée ; (c) La distribution de l'intensité des pixels selon la direction diagonale de l'image originale et de l'image cryptée.

1.11.5 Resistance au bruit et aux Pertes de données (Loss Data):

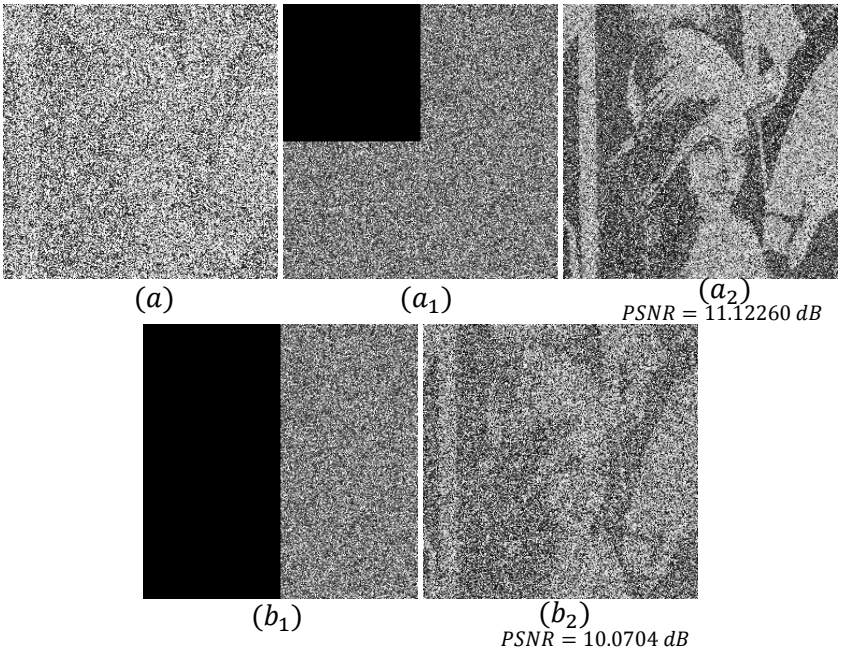
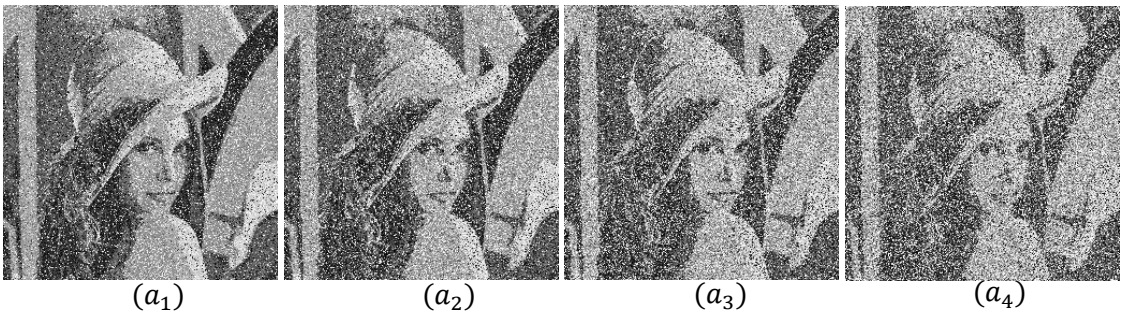


Figure 1.16 : Illustration de l'attaque par pertes de données : (a) Image cryptée de Lena ; (a_1) Image cryptée de Lena avec 25% de pertes ; (a_2) Image décryptée de Lena correspondante ; (b_1) Image cryptée de Lena avec 50% de pertes ; (b_2) Image décryptée de Lena correspondante.

Les images numériques peuvent être facilement influencées par le bruit et par les pertes de données lors de leur transmission à travers les réseaux ou pendant leur stockage dans les médias physiques. Un algorithme de cryptage d'images devrait avoir la capacité de résister à ces phénomènes anormaux. Pour tester la capacité d'une image à résister aux pertes de données, l'image originale est d'abord cryptée par la technique proposée puis nous supposons qu'une partie de ses pixels a été perdue selon différentes tailles **figure 1.16**. Le processus de décryptage est ensuite appliqué à cette image , si les images déchiffrées contiennent la plupart des informations visuelles originales, nous disons que la technique de cryptage est robuste vis-à-vis de l'attaque par pertes de données . Les évaluations objectives en termes du $PSNR$ et du coefficient de corrélation sont aussi utilisées.



(a_1) (a_2) (a_3) (a_4)

$PSNR = 17.2936\ dB$ $PSNR = 14.4159\ dB$ $PSNR = 12.7858\ dB$ $PSNR = 11.6282\ dB$

Figure 1.17 : Illustration de l'attaque par bruit additif: (a_1) Image décryptée de Lena avec $k = 0.2$; (a_2) avec $k = 0.3$; (a_3) avec $k = 0.4$; et (a_4) avec $= 0.5$.

De même pour tester la capacité d'une image à résister au bruit additif, nous supposons qu'une image cryptée C est noyée dans un bruit additif **figure 1.17** selon l'équation suivante :

$$C' = C.(1 + k.G) \tag{1.10}$$

où C' est l'image cryptée noyée dans un bruit blanc de distribution Gaussienne G, k c'est son coefficient de puissance, si Les images déchiffrées contiennent la plupart des informations visuelles originales, nous disons que la technique de cryptage est robuste vis-à-vis de l'attaque par bruit additif.

1.12 Temps d'exécution

Le temps d'exécution est important pour l'évaluation d'un algorithme de cryptage, plus ce temps là est court, plus l'algorithme est difficile à le révéler, , son calcul dépendra des caractéristiques du processeur avec lequel les simulations sont faites.

1.13 Test statistique de NIST

Les tests du NIST (National Institute of Standards and Technology) forment un paquetage statistique de tests qui sont conçus pour détecter l'aspect aléatoire des séquences binaires à la sortie des générateurs de nombres aléatoires ou pseudo-aléatoires utilisés dans des applications nécessitant de la cryptographie [55], [56]. La sortie des générateurs de nombre pseudo-aléatoires doit être imprévisible en ignorant l'entrée. Les tests du NIST se concentrent sur différents types d'aspects non-aléatoires que l'on peut trouver dans une séquence et les comparer avec une séquence aléatoire [54,56]. Quelques tests sont décomposables en un ensemble de sous-tests. L'ordre d'application des tests est arbitraire. Cependant, le test de fréquence doit être appliqué en premier lieu, puisqu'il fournit la preuve la plus évidente de l'aspect non aléatoire, qui est la non uniformité. Si le test ne réussit pas, la probabilité d'échec des tests suivants est élevée. Le résultat de chaque test est donné par une *P-Value* qui représente la probabilité qu'un générateur de nombre aléatoire parfait produise une séquence moins aléatoire que la séquence déjà testée. Cette variable a une distribution uniforme sur l'intervalle [0 1].

P-Value = 1 : aspect aléatoire parfait.

P-Value = 0 : aspect non aléatoire.

Une constante α est fixée dans l'intervalle [0.001-0.01]. Elle est appelée "niveau de signification". Si les *P-Value* sont supérieures ou égales à α, alors la séquence réussit le test sinon elle échoue. On présente par la suite les 15 tests du NIST [54].

1.13.1 Test de fréquence

Le but de ce test est de déterminer si le nombre de 0 et de 1 dans une séquence est approximativement le même comme il est prévu pour une séquence réellement aléatoire. Le test vérifie si la fraction des 1 est proche de 1/2. Les étapes du test sont comme suit :

1) Conversion en ± 1 : les 0 et les 1 de la séquence ε sont convertis respectivement en 1 et -1. On aura $S_n = X_1 + X_2 + \ldots + X_n$, tel que $X_i = 2^{\varepsilon_i} - 1$.
2) Calculer la statistique du test $S_{obs} = \frac{|S_n|}{\sqrt{n}}$
3) Calculer $P - Value = erfc\left(\frac{S_{obs}}{\sqrt{2}}\right)$, avec erfc est la fonction d'erreur complémentaire.
4) Si la $P - Value < 0.01$, alors la séquence est non-aléatoire. Sinon elle est aléatoire. Il est recommandé que la séquence testée soit d'une longueur minimale de 100 bits ($n < 100$). Avec *n* est la longueur de la chaîne de bits. ε est la séquence de bits du générateur RNG ou PRNG à tester tel que $\varepsilon = \varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots, \varepsilon_n$ et S_{obs} est la valeur absolue de la somme des X_i, avec ($X_i = 2^{\varepsilon_i} - 1 = \pm 1$).

1.13.2 Test de fréquence par bloc

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

1) Partager la séquence en N séquences, telle que $N = \left\lfloor \frac{n}{M} \right\rfloor$ et enlever les bits inutilisés.
2) Déterminer la proportion π_i des 1 dans chaque séquence de M-Bits en utilisant l'équation :

$$\pi_i = \frac{\sum_{j=1}^{M} \varepsilon_{(i-1)M+j}}{M}, pour\ 1 \leq i \leq N.$$

3) Calculer la distribution χ^2,

$$\chi^2(obs) = 4M \sum_{i=1}^{N} (\pi_i - 1/2)^2,$$

4) Calculer $P - value = igamc(N/2, \chi 2(obs)/2)$, tel que "*igamc*" est la fonction de gamma incomplète.

Il est recommandé que chaque séquence à tester ait une longueur minimale égale à 100 bits ($n \geq 100$), tel que $(n \geq M.N).M \geq 20, M > 0.01\, n$ et $N < 100$.

1.13.3 Test de somme cumulative (inverse)

Le but de ce test est de déterminer si la somme cumulative dans une séquence est trop grande ou trop petite (somme de 1 et -1). Ceci indique la présence de nombre important de 0 ou de 1. La somme cumulative peut être considérée comme une marche au hasard (Random Walk) qui est un modèle mathématique d'un système possédant une dynamique discrète composée d'une succession de pas aléatoires, ou effectuée « au hasard ». Pour une séquence aléatoire, les excursions du "Random Walk" doivent être proches de 0.

1) Former une séquence normalisée, ε est transformée en X_i, (avec $X_i = 2\, \varepsilon_i - 1. = \pm 1$).
2) Calculer les sommes partielles des sous séquences S_k, de largeurs successives, tel que

$$S_k = S_{k-1} + X_k \text{ (mode 0) ; } S_k = S_{k-1} + X_{n-k+1} \text{ (mode 1).}$$

3) Calculer la statistique du test : $z = max_{1 \leq k \leq n} |S_k|$.
4) Calculer la *P-Value*.

$$K_1 = \sum_{k=\left(\frac{-n}{2}+1\right)/4}^{\frac{n}{2}-1} \left[\Phi\left(\frac{(4k+1)z}{\sqrt{n}}\right) - \Phi\left(\frac{(4k-1)z}{\sqrt{n}}\right)\right] \quad (1.11)$$

$$K_2 = \sum_{k=\left(\frac{-n}{2}-3\right)/4}^{\left(\frac{n}{2}-1\right)/4} \left[\Phi\left(\frac{(4k+3)z}{\sqrt{n}}\right) - \Phi\left(\frac{(4k+1)z}{\sqrt{n}}\right)\right] \quad (1.12)$$

$P - value = 1 - K1 + K2;$

Telle que Φ : est la fonction de distribution cumulative (normal standard).

1.13.4 Test de série

Le « Runs Test » permet de déceler des oscillations entre les 0 et les 1 trop rapides ou trop lentes. Pour cela, il faut :

1) Calculer π, tel que : $\pi = \frac{\sum_j \varepsilon_j}{n}$
2) Calculer

$$V_n(obs) = \sum_{k=1}^{n-1} r(k) + 1$$

, $r(k) = 0$ si $\varepsilon_k = \varepsilon_{k+1}$ sinon $r(k) = 1$

3) Calculer $P - Value = erfc\left(\frac{|V_n(obs) - 2n\pi(1-\pi)|}{2\sqrt{2n}\pi(1-\pi)}\right)$

1.13.5 Test de longues séries de 1

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

Tableau 1.2: Division de la séquence en *M*.

m	n
8	128
128	6272
10^4	750.000

1) Diviser la séquence en *M* blocs. La longueur de chaque bloc doit être conforme au **tableau 1.2**
2) Classer la fréquence de la plus grande série de 1 dans chaque séquence dans des catégories selon le **tableau 1.3**.

Tableau 1.3: Classement de la fréquence.

V_i	$M = 8$		$M = 128$		$M = 10000$	
	Longueur bloc	π_i	Longueur bloc	π_i	Longueur bloc	π_i
V_0	≤ 1	0.2148	≤ 4	0.1174	≤ 10	0.0882
V_1	2	0.3672	5	0.2430	11	0.2092
V_2	3	0.2305	6	0.2493	12	0.2483
V_3	≥ 4	0.1875	7	0.1752	13	0.1933
V_4			8	0.1027	14	0.1208
V_5			≥ 9	0.1124	15	0.0675
V_6					≥ 16	0.0727

3) Calculer

$$X^2(obs) = \sum_{i=0}^{k} \frac{(V_i - N\pi_i)^2}{N\pi_i}$$

4) Calculer $P - value = igamc(K/2, X^2(obs)/2)$

1.13.6 Test de rang

Calculer le rang des sous matrices de la séquence et vérifier leur dépendance linéaire.

1) On divise la séquence en : $N = \left\lfloor \frac{n}{M^2} \right\rfloor$ sous-séquences de blocs disjoints de longueur M^2 afin de construire la matrice carrée $M \times M$ notée.
2) Déterminer le rang R_l de chaque matrice, avec $l = 1, .., N$.
3) Calculer :

$$\chi^2(obs) = \frac{(F_M - 0.2888N)^2}{0.2888N} + \frac{(F_{M-1} - 0.5776N)^2}{0.5776N} + \frac{(N - F_M - F_{M-1} - 0.1336N)^2}{0.1336N} \quad (1.13)$$

tel que F_K est le nombre de matrices de rang égal à k

4) Calculer la $P - Value = e^{-\chi^2(obs)/2}$.

1.13.7 Test de la transformée de Fourier discrète

Ce test tient compte des hauteurs des pics de la transformée de Fourier de la séquence pour détecter une périodicité. L'intention est de détecter si le nombre de pics dépassant le seuil de 95 % est largement différent de 5 %. La *P-Value* sera égale à : $erfc\left(\frac{|d|}{\sqrt{2}}\right)$

1.13.8 Non overlapping template Matching

Ce test consiste à détecter des générateurs qui produisent trop d'occurrence d'un mot apériodique donné (template).Une fenêtre de m-bits est utilisée. Si le mot n'est pas trouvé, la fenêtre est décalée d'un bit. Si le mot est trouvé, la fenêtre décale jusqu'au bit qui suit le mot trouvé.

1) Calculer les grandeurs suivantes :$\mu = \frac{M-m+1}{2^m}$ et $\sigma^2 = M\left(\frac{1}{2^m} - \frac{2m-1}{2^{2m}}\right)$

   Tel que *M* est la longueur en bits de la séquence à tester et *m* est la longueur en bits du template.

2) Calculer

$$\chi^2(obs) = \sum_{j=1}^{N} \frac{(W_j - \mu)^2}{\sigma^2}$$

3) Calculer

$$P - value \;=\; igamc(N/2, \chi 2/2).$$

1.13.9 Overlapping Template Matching

Le but de ce test est identique à celui du 8ème test, calculer le nombre d'occurrences de *B* dans chacun des *N* blocs. On crée une fenêtre de *m* bits qui traverse la séquence en comparant les bits de la fenêtre avec B. Un compteur s'incrémente quand il y a une égalité. Après chaque test, la fenêtre est décalée de 1 bit. Le nombre d'occurrences dans chaque bloc est enregistré en incrémentant un vecteur V_i.

V_0 est incrémenté quand il n'y a pas d'égalité.

V_1 est incrémenté pour une égalité dans le bloc.

1) Calculer

$$\chi^2(obs) = \sum_{j=0}^{k} \frac{(V_j - N\pi_j)^2}{N\pi_j}$$

   Avec π_j est obtenue par la formule suivante :

$$\begin{cases} \pi_j = P(U=j) = \dfrac{e^{-n}}{2^j}\displaystyle\sum_{l=1}^{j}\binom{j-1}{l-1}\dfrac{n^l}{l!} & 0 \le j \le k-1 \\ \pi_k = 1 - \displaystyle\sum_{k=0}^{k-1}\pi_k & j = k \end{cases} \tag{1.14}$$

2) Calculer $P - Value = igamc\,(5/2, \chi^2/2)$.

1.13.10 Test statistique universel : Test de Maurer

Le but de ce test est de déterminer si la séquence est compressible ou non sans perte d'information. U*ne séquence nettement compressible est considérée comme non aléatoire. La séquence de bits est di*visée en deux sous séquences : la première est un segment d'initialisation de $Q \times L$ bits non chevauchés. La deuxième est un segment de test de $K \times L$ bits non chevauchés **figure 1.18**.

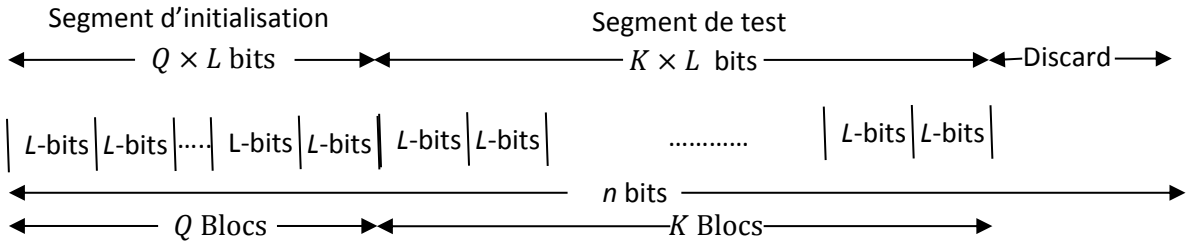


Figure 1. 18 : Sous séquences $\boldsymbol{Q}$ et $\boldsymbol{L}$.

Calculer la *P-Value* : $P - Value = erfc\left(\frac{f_n - expected\ value(L)}{\sqrt{2}\sigma}\right)$

avec :

$$f_n = \frac{1}{k}\sum_{i=Q+1}^{Q+K} log_2\left(i - T_j\right)$$

Tel que T_j est la représentation décimale du contenu du $i^{\text{ème}}$ L blocs. $T_{j=i}$ est la position du bloc L.

avec : $\sigma = \sqrt[c]{\dfrac{variance(L)}{K}}$ et $c = 0.7 - \dfrac{0.8}{L} + \left(4 + \dfrac{32}{L}\right)\dfrac{K^{\frac{-3}{L}}}{15}$

1.13.11 Test d'entropie approximative

On s'intéresse aux fréquences d'occurrences de toutes les sous-séquences possibles de longueur *m* fixée. Nous allons comparer les fréquences obtenues avec les longueurs m et $m+1$. L'entropie mesure le degré de désordre d'un système. Pour une séquence de bits donnée, il faut ajouter les $m-1$ bits de la fin de la séquence à son début.

Exemple : 001101 et $m=3$, on obtient : 00110100.

Les blocs de bits chevauchés de longueur m sont testés : $001, 011, 110, 101, 010, 100$.

1) La fréquence des blocs est comptée. $V_m^i \qquad 0 \leq i \leq 2^m$

   $V_{001} = 1, \quad V_{011} = 1, V_{110} = 1, V_{101} = 1, V_{010} = 1, V_{100} = 1$

2) Calculer $C_m^i = \frac{\#i}{n}$

3) Calculer

$$\varphi^{(m)} = \sum_{i=0}^{2^m-1} \pi_i \, log \, \pi_i$$

   Tel que $\pi_i = C_m^j$ et $j = log_2(i)$.

4) Répéter les étapes en remplaçant m par $m+1$

1.13.12 Random excursion

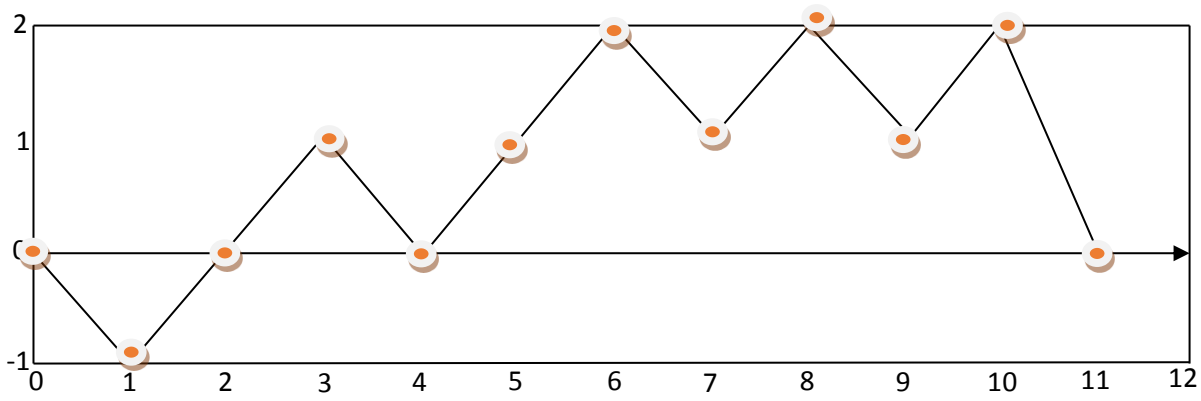


Figure 1. 19 : Exemple de marche aléatoire.

Un cycle d'une marche aléatoire (excursion) est une séquence de pas aléatoires qui commence et finit à son origine **figure 1.19**. On a recours à déterminer si le nombre de visites à un état particulier d'un cycle dévie de ce qui est attendu. Ce test est une série de 8 tests et conclusions. Un test est une conclusion pour chaque état : $-4, -3, -2, -1 \; et \; +1, +2, +3, +4$;

1) Calculer *P-Value*: $P - Value = igamc\,(5/2, \chi 2/2)$,

1.13.13 Random excursion variant

Le but de ce test est de calculer le nombre de fois où un état particulier est visité, et de détecter la déviation par rapport au nombre de visites attendu à différents états de la marche aléatoire.

Ce test est actuellement une série de tests et de conclusion, un test et une conclusion pour chaque état : $-9, -8, \dots, -1$. Et $+1, +2, \dots, +9$.

On doit convertir les 0 et les 1 de la séquence ε en -1 et 1. La nouvelle séquence sera : $X = X_1, X_2, \dots, X_n$, tel que $X_i = 2\,\varepsilon_i - 1$.

1) Calculer la somme partielle S_i, tel que $S_1 = X_1$, $S_2 = X_1 + X_2$, $S_3 = X_1 + X_2 + X_3$, $S_n = X_1 + X_2 + \dots + X_k + \dots + X_n$.

On obtient *S= {Si}*.

2) On forme ensuite une nouvelle séquence S', en ajoutant un zéro au début et à la fin de l'ensemble *S*.

3) pour les 18 états, $\xi(X)$ qui est le nombre total des fois où m' états X est vérifié tout au long des cycles *J*.

4) Calculer la $P-Value$ tel que : $P - Value = erfc\left(\frac{|\xi(X)-J|}{\sqrt{2J(4|X|-2)}}\right)$.

1.13.14 Test série (Serial Test, serial 1 & serial 2)

Ce test est basé sur la fréquence de tous les m-bits de chevauchement tout au long de la séquence. Le but de ce test est de déterminer si le nombre d'occurrences des 2^m des modèles de chevauchement des m bits est identique à celui d'une séquence aléatoire (*m* est le nombre de bits dans chaque bloc). Une séquence est aléatoire tel que chaque modèle de *m*-bits a la même chance d'apparence que d'autre m-bits. Pour *m = 1*, le test de série est équivalent au test de fréquence.

1) On commence par ajouter les $m-1$ bits au début de la séquence. Déterminer la fréquence de tout bloc de longueur m-bits, $m-1$ bits, et $m-2$ bits.

2) Calculer Ψ_m^2 , Ψ_{m-1}^2 , et Ψ_{m-2}^2 tel que :

$$\Psi_m^2 = \frac{2^m}{n}\sum_{i_1 \dots i_m}\left(V_{i_1 \dots i_m} - \frac{n}{2^m}\right)^2 = \frac{2^m}{n}\sum_{i_1 \dots i_m} V_{i_1 \dots i_m} - n \qquad (1.15)$$

3) Calculer :

$$\nabla\,\Psi_m^2 = \Psi_m^2 - \Psi_{m-1}^2$$

$$\nabla^2\,\Psi_m^2 = \Psi_m^2 - 2\,\Psi_{m-1}^2 + \Psi_{m-2}^2 \qquad (1.16)$$

4) Calculer *P-Value* :
$$\begin{cases} P - value1 = igamc(2^{m-2}, \nabla\,\Psi_m^2\ ) \\ P - value2 = igamc(2^{m-3}, \nabla\,\Psi_m^2\ ) \end{cases} \qquad (1.17)$$

1.13.15 Test de complexité linéaire (Linear complexity)

Ce test est basé sur la longueur d'un registre à décalage à rétroaction linéaire. Le but de ce test est de déterminer si la séquence est assez complexe pour être considérée comme aléatoire. Les séquences aléatoires sont caractérisées par de long LFSR (Linear Feedback Shift Register). Un LFSR trop court implique l'aspect non aléatoire.

1) Partitionner la séquence en N blocs indépendants de M bits chacun, tel que $n = M \times N$.
2) En utilisant l'algorithme de Berlekamp Massey, on détermine la complexité L_i des N blocs
   ($i = 1 \dots N$). L_i désigne la longueur de la plus courte séquence du LFSR qui génère tous les bits du bloc i.
3) Calculer :

$$\chi^2(obs) = \sum_{i=0}^{k} \frac{(V_i - N\pi_i)^2}{N\pi_i}$$

4) La P-value est donnée par la formule suivante : $P - value = igamc\left(\frac{k}{2}, \frac{\chi^2(obs)}{2}\right)$

1.14 Applications du cryptage

La cryptographie est utilisée aujourd'hui dans de nombreuses applications : dans les téléphones portables, sur Internet ou pour la télévision à péage. Dans le cas des téléphones mobiles, la cryptographie est utilisée pour assurer la confidentialité des communications. En effet, la loi sur les télécommunications oblige les opérateurs à garantir la sécurité des communications des utilisateurs. En particulier dans le cas des téléphones mobiles, les communications entre le téléphone et la station hertzienne sont chiffrées. On utilise uniquement la cryptographie à clé secrète et l'algorithme de chiffrement est un algorithme par flot appelé A5. Sur Internet, la cryptographie permet de garantir la confidentialité de certaines communications comme la transmission du code d'une carte bleue « protocole SSL (Secure Sockets Layer) » ou d'assurer la confidentialité, l'intégrité et l'authentification de l'émetteur dans les messageries électroniques « protocole S/MIME (Secure/Multipurpose Internet Mail Extensions).

1.15 Conclusion

Dans ce chapitre, nous avons discuté les concepts de base utilisés en cryptologie et les phases historiques les plus marquantes qu'a connu cette science. En outre, nous avons présenté la classification des algorithmes de cryptage d'images, une étude bibliographique des algorithmes spatiaux et fréquentiels pertinents, et les techniques d'évaluation des algorithmes de cryptage y compris le standard d'évaluation de NIST avec ses différents tests. Vu l'importance des transformées paramétriques qui sont exploitées dans cette thèse dans la conception de nouveaux algorithmes de cryptage, nous développons les outils mathématiques nécessaires de ces transformées dans le chapitre suivant.

Chapitre 2

Transformées paramétriques et suites chaotiques

2.1 Introduction

Le défi et la nécessité de sécuriser parfaitement les informations dans les réseaux de communication modernes ont poussé les chercheurs à accroître les efforts et à développer des techniques de cryptage efficaces. En effet, plusieurs techniques de cryptage ont été proposées dans la littérature et elles sont classées en deux catégories ; les techniques temporelles (ou spatiales) et les techniques fréquentielles. Les techniques fréquentielles de cryptage d'images exploitent les algorithmes rapides des transformées discrètes telles que la transformée de Fourier discrète, la transformée en cosinus discrète, la transformée de Hadamard,…etc. Malgré que ces transformées présentent une complexité réduite, elles offrent un espace de clés secrètes insuffisant. Pour remédier à ce problème, de nouvelles philosophies ont été considérées dans la conception des techniques de cryptage d'images plus robustes et plus adaptées aux applications récentes des services de communication. Les transformées paramétriques discrètes ont une implémentation facile en hardware, donc le cryptage/décryptage basé sur ces transformées peut être effectué en temps réel, en plus, les paramètres arbitraires de ces transformées peuvent être exploités comme une clé supplémentaire. Par conséquent, l'espace de la clé de cryptage sera certainement élargi.

Dans ce chapitre, nous présentons le développement mathématique des transformées paramétriques, leurs versions directes et inverses, et leurs propriétés. Nous considérons ainsi leurs utilisations dans les différents schémas de cryptage/décryptage d'images. Nous exposons aussi les suites chaotiques souvent utilisées dans ces schémas de cryptage.

2.2 Transformée de Fourier

Parmi les transformées dédiées au traitement de signal, la transformée de Fourier (FT) est la plus populaire, cela est dû essentiellement à sa large utilisation dans un grand nombre d'applications dans plusieurs domaines de la science et d'engineering. C'est une transformée unitaire à valeur complexe possédant plusieurs propriétés très intéressantes en traitement de signal.

La transformée de Fourier discrète DFT $X(n)$ d'une séquence réelle $x(k)$ de longueur N est définie comme suit :

$$X(n) = \sum_{k=0}^{N-1} x(k) W_N^{nk} \ , \qquad 0 \leq n \leq N-1, \tag{2.1}$$

et sa transformée inverse

$$x(k) = \frac{1}{N}\sum_{n=0}^{N-1} X(n)W_N^{-nk}, \qquad 0 \le k \le N-1, \tag{2.2}$$

avec $W_N = exp\left(-j\frac{2\pi}{N}\right)$ et $j = \sqrt{-1}$.

Pour une image carrée de taille $(N \times N)$, la transformée de Fourier discrète à deux dimensions (2D DFT) est donnée par [57] :

$$F(k,l) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f(i,j).e^{-i2\pi(\frac{ki}{N}+\frac{lj}{N})}, \tag{2.3}$$

où f est l'image dans le domaine spatial et le terme exponentiel est la fonction de base correspondant à chaque point $F\ (k,l)$ dans l'espace de Fourier. L'équation peut être interprétée comme étant la valeur de chaque point $F\ (k,l)$ qui est obtenue en multipliant l'image spatiale par la fonction de base correspondante et en additionnant le résultat. Les fonctions de base sont des ondes sinus et cosinus avec des fréquences croissantes, $F\ (0,0)$ représente la composante continue de l'image qui correspond à la luminosité moyenne et $F\ (N-1, N-1)$ représente la fréquence la plus élevée. De même, l'image de Fourier peut être retransformée en domaine spatial. La transformée de Fourier inverse est donnée par:

$$f(a,b) = \frac{1}{N^2}\sum_{k=0}^{N-1}\sum_{l=0}^{N-1} F(k,l).e^{+i2\pi(\frac{ka}{N}+\frac{lb}{N})} \tag{2.4}$$

2.3 Transformée de Hartley

La transformée de Hartley est une alternative de la transformée de Fourier pour les applications exigeant des signaux à valeurs réelles. Elle possède deux propriétés intéressantes; la première est que la transformée est purement réelle, l'autre est qu'elle est involutive c'est à dire que sa transformée directe et sa transformée inverse sont identiques [51].

La transformée de Hartley bidimensionnelle 2D HT d'une fonction continue et réelle $f(x,y)$ est définie par :

$$H(u,v) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y).cas[2\pi(ux+vy)]\,dxdy, \tag{2.5}$$

où $cas(.) = \cos(.) + \sin(.)$. Sa transformée inverse est définie par :

$$f(x,y) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} H(u,v).cas[2\pi(ux+vy)]\, dudv \tag{2.6}$$

Pour une image P de taille $N \times M$, la transformée de Hartley discrète à deux dimensions (2D DHT) est donnée par :

$$H(k,l) = \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} \mathrm{P}(n,m) cas\left[\frac{2\pi}{N} kn + \frac{2\pi}{M} lm\right], k = 0,1,\dots,N-1, l = 0,1,\dots,M-1 \tag{2.7}$$

2.3.1 Cryptage d'images DRPE dans le domaine de la DHT

En 2009, Narendra Singh, et Aloka Sinha [51] ont proposé deux méthodes de cryptage d'images. L'une utilisant la transformée de Hartley et la transformée jigsaw (JT_b), l'autre constitue une amélioration de la première en ajoutant un brouillage basé sur la suite chaotique Logistique. Le schéma de cryptage/décryptage de la deuxième méthode est présenté ci-dessous :

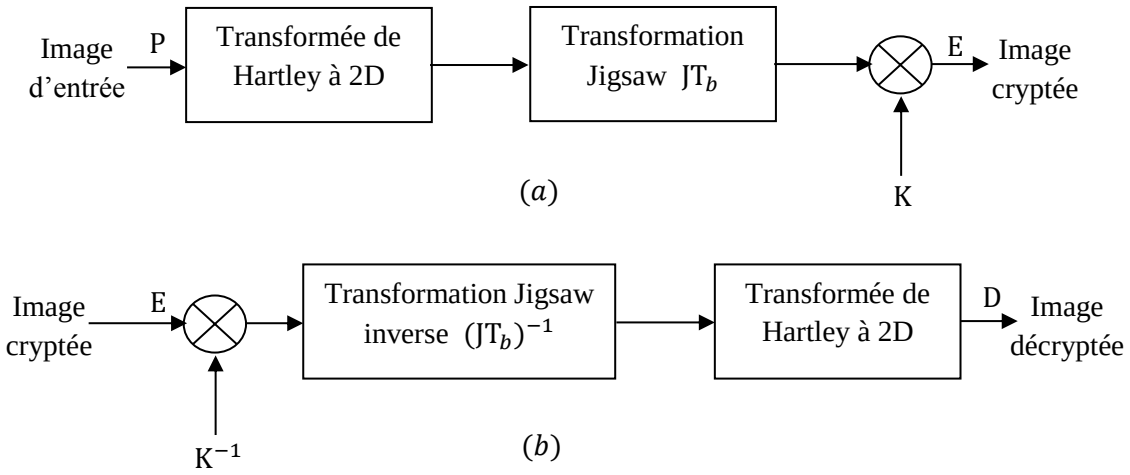


Figure 2.1 : Schéma de cryptage/décryptage d'images dans le domaine de la transformée de Hartley proposé par Narendra Singh et Aloka Sinha [51]: (a) schéma de cryptage, (b) schéma de décryptage.

Dans le schéma de cryptage de la **figure 2.1**, l'image d'entrée à crypter P de taille $(m \times n)$ est transformée au domaine fréquentiel par le biais de la transformée de Hartley 2D. La transformée obtenue est brouillée par la transformation Jigsaw désignée par JT_b de paramètre b qui est l'un des éléments de la clé de cet algorithme de cryptage, puis multipliée élément par

élément par un masque d'amplitude aléatoire de même taille que celle de l'image d'entrée généré chaotiquement par la suite logistique pour donner en sortie l'image cryptée E dont son expression mathématique est donnée par :

$$\mathrm{E}(u,v) = \mathrm{K}(u,v) \odot \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} \mathrm{P}(x,y).\, cas\left[\frac{2\pi}{N} ux + \frac{2\pi}{N} vy\right], \tag{2.8}$$

où $\odot$ dénote la multiplication élément-par-élément.

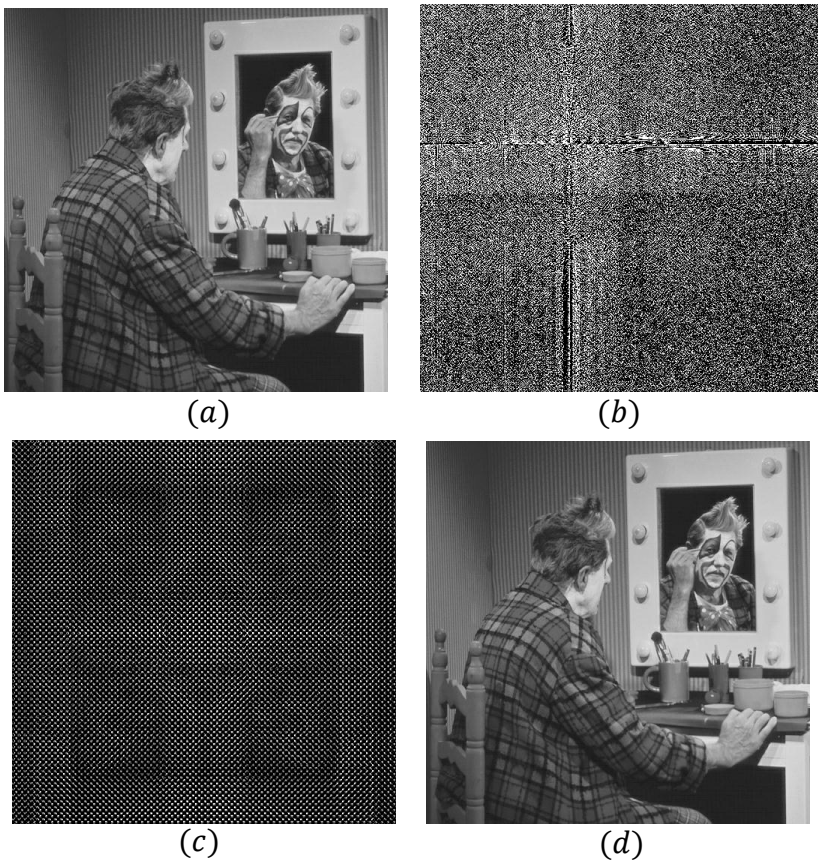


Figure 2.2 : Illustration du cryptage / décryptage d'images dans le domaine de la transformée de Hartley proposé par Narendra Singh et Aloka Sinha [51]: (a) Image d'entrée de clown, (b) Image cryptée correspondante, (c) Image décryptée correspondante avec clé erronée (d) Image décryptée correspondante avec clé correcte.

Le processus de décryptage tel que représenté sur la **figure 2.1.**($\boldsymbol{b}$) suit exactement les étapes du processus de cryptage de manière inverse pour obtenir l'image décryptée **D** dont son expression mathématique est donnée par :

$$\mathbf{D}(\boldsymbol{x},\boldsymbol{y}) = \mathbf{K}^{-1}(\boldsymbol{x},\boldsymbol{y}) \odot \sum_{\boldsymbol{u}=0}^{\boldsymbol{m}-1} \sum_{\boldsymbol{v}=0}^{\boldsymbol{n}-1} \mathbf{P}(\boldsymbol{u},\boldsymbol{v}).\, \boldsymbol{cas}\left[\frac{2\boldsymbol{\pi}}{\boldsymbol{N}}\boldsymbol{ux} + \frac{2\boldsymbol{\pi}}{\boldsymbol{N}}\boldsymbol{vy}\right] \qquad (\mathbf{2.9})$$

La **figure 2.2** est une illustration du cryptage / décryptage d'images dans le domaine de la transformée de Hartley proposé dans [51].

Désignant par (k, b) la clé de cryptage utilisée dans ce processus avec k : masque chaotique d'amplitude aléatoire et b : indique la trame des permutations Jigsaw, la **figure 2.2.**($\boldsymbol{a}$) est l'image d'entrée de clown à crypter, la **figure 2.2.**($\boldsymbol{b}$) est son image cryptée correspondante avec la clé de cryptage (k, b) , l'image décryptée correspondante avec clé erronée(k', b') autre que (k, b) est représentée dans la **figure 2.2.**($\boldsymbol{c}$) et celle de l'mage décryptée correspondante avec clé correcte est représentée dans la **figure 2.2.**($\boldsymbol{d}$).

2.4 Transformées paramétriques

Ces dernières années, il y a eu un énorme intérêt à développer des versions paramétriques des transformées fixes existantes [59,60]. Il a été montré dans ces articles que la paramétrisation des transformées peut avoir une plus large gamme d'applications comparées à leurs versions originales et peuvent fournir plus de flexibilité dans la représentation, dans l'interprétation et dans le traitement des signaux [58]. L'importance des paramètres indépendants dans les transformées discrètes peut clairement être vu dans les travaux présentés en, [8], [61-63]. Par exemple, les paramètres indépendants de la transformée discrète fractionnaire ont été utilisés comme clé secrète supplémentaire pour le tatouage [62] et le cryptage [8], [63]. Bouguezel et al, dans [58] ont introduit des paramètres indépendants dans la DFT et DHT en vue de réaliser une meilleure performance dans leurs applications. Dans ce qui suit, nous allons rappeler la construction et le développement mathématiques de ces transformées et leurs implémentations dans le système de cryptage DRPE.

2.4.1 Transformée de Fourier paramétrique

En se basant sur la transformée de Fourier discrète DFT, les auteurs ont proposé dans [58] la DFT paramétrique à trois paramètres obtenus en remplaçant convenablement quelques éléments spécifiques dans le vecteur du noyau de la DFT classique par des paramètres

indépendants. La DFT paramétrique à trois paramètres est de taille *N*, où *N* est une puissance de deux, c'est-à-dire $N=2^r$, avec *r* étant un entier positif $r > 3$. Elle est définie comme suit :

$$X^{a,b,c}(n) = \sum_{k=0}^{N-1} x(k)\, v_{F^{a,b,c}}(nk \bmod N), \quad 0 \le n \le N-1 \tag{2.10}$$

Sa transformée inverse est donnée par :

$$x(k) = \frac{1}{N}\sum_{n=0}^{N-1} X^{a,b,c}(n) \frac{1}{v_{F^{a,b,c}}(nk \bmod N)}, \qquad 0 \le k \le N-1, \tag{2.11}$$

où $v_{F^{a,b,c}}(i)$, $0 \le i \le N-1$, sont les entrées du vecteur noyau (kernel vector) données par :

$$\mathbf{V}_{F^{a,b,c}} = [1 \quad \mathbf{V} \quad c \quad -j\mathbf{V} \quad -1 \quad -\mathbf{V} \quad -c \quad j\mathbf{V}], \tag{2.12}$$

avec

$$\mathbf{V} = \left[W_N^1 \quad \dots \quad W_N^{\frac{N}{16}-1} \quad a \quad W_N^{\frac{N}{16}+1} \quad \dots \quad W_N^{\frac{N}{8}-1} \quad b \quad W_N^{\frac{N}{8}+1} \quad \dots \quad W_N^{\frac{3N}{16}-1} \quad -ja^* \quad W_N^{\frac{3N}{16}+1} \quad \dots \quad W_N^{\frac{N}{4}-1}\right], \tag{2.13}$$

et *a*, *b*, *c* étant trois paramètres différents de zéro qui peuvent être choisis arbitrairement dans le plan complexe.

Les équations (2.10) et (2.11) peuvent être écrites sous forme matricielle comme suit :

$$\mathbf{X}^{a,b,c} = \mathbf{F}_N^{a,b,c}.\boldsymbol{x} \tag{2.14}$$

$$\boldsymbol{x} = (\mathbf{F}_N^{a,b,c})^{-1}.\mathbf{X}^{a,b,c}\ , \tag{2.15}$$

où $(\mathbf{F}_N^{a,b,c})^{-1}$ est la matrice inverse de $\mathbf{F}_N^{a,b,c}$.

2.4.1.1 Propriétés de la DFT paramétrique

- La matrice $\mathbf{F}_N^{a,b,c}$de la DFT paramétrique est une matrice réciproque-orthogonale qui vérifie l'équation suivante :

$$\mathbf{F}_N^{a,b,c} \times (\mathbf{F}_N^{a,b,c})^{-1} = \mathbf{F}_N^{a,b,c} \times (\mathbf{F}_N^{a,b,c})^{\mathrm{RT}} = N.\mathbf{I_N}, \tag{2.16}$$

où $(.)^{\mathrm{RT}}$est la matrice réciproque transposée, et I_N est la matrice identité d'ordre N.

- L'un des cas particuliers les plus intéressants de la DFT à trois paramètres peut être obtenu lorsque $a = e^{j\alpha}$, avec α étant un paramètre qui peut être choisi arbitrairement dans l'intervalle [-2π, 0], $b = W_N^{N/8}$ et $c = W_N^{N/4}$, ce cas conduit à une DFT à un paramètre notée DFT$^{\alpha}$, qui sera désignée sous forme matricielle par $\mathbf{F}_N^{a}$.
- Dans le cas particulier où $a = W_N^{N/16}$, $b = W_N^{N/8}$et $c = W_N^{N/4}$, la DFT paramétrique devient la transformée de Fourier discrète classique.
- Linéarité : Soient $x_1(k), x_2(k)$, et $x(k)$ trois séquences complexes ayant comme transformées $X_1^{a,b,c}(n)$, $X_2^{a,b,c}(n)$, $X^{a,b,c}(n)$ respectivement

$$x_1(k) \overset{DFT^{a,b,c}}{\longleftrightarrow} X_1^{a,b,c}(n)$$

$$x_2(k) \overset{DFT^{a,b,c}}{\longleftrightarrow} X_2^{a,b,c}(n)$$

$$x(k) \overset{DFT^{a,b,c}}{\longleftrightarrow} X^{a,b,c}(n)$$

$$x(k) \overset{DFT^{\alpha}}{\longleftrightarrow} X^{\alpha}(n),$$

pour des constantes arbitraires β etγ, nous avions :

$$\beta x_1(k) + \gamma x_2(k) \overset{DFT^{a,b,c}}{\longleftrightarrow} \beta X_1^{a,b,c}(n) + \gamma X_2^{a,b,c}(n)$$

- Dualité :

$$x^{\alpha}(k) \overset{DFT^{\alpha}}{\longleftrightarrow} Nx(N-n).$$

- Symétrie

$$x^*(k) \overset{DFT^{\alpha}}{\longleftrightarrow} (X^{\alpha}(N-n))^*$$

$$x^*(N-k) \overset{DFT^{\alpha}}{\longleftrightarrow} (X^{\alpha}(n))^*$$

$$\mathrm{Re}\big(x(k)\big) \overset{DFT^{\alpha}}{\longleftrightarrow} \frac{1}{2}(X^{\alpha}(n) + (X^{\alpha}(N-n))^*)$$

$$j \times \mathrm{Im}\big(x(k)\big) \overset{DFT^{\alpha}}{\longleftrightarrow} \frac{1}{2}(X^{\alpha}(n) - (X^{\alpha}(N-n))^*)$$

$$\frac{1}{2}\big(x(n) + \big(x(N-k)\big)^*\big) \overset{DFT^{\alpha}}{\longleftrightarrow} Re(X^{\alpha}(n))$$

$$\frac{1}{2}\big(x(k) + \big(x(N-k)\big)^*\big) \overset{DFT^{\alpha}}{\longleftrightarrow} j \times \mathrm{Im}\big(X^{\alpha}(n)\big),$$

avec $\mathrm{Re}(.)$: partie réelle et $\mathrm{Im}(.)$: partie imaginaire.

- Propriétés de la symétrie pour une séquence réelle

$$s(k) \overset{DFT^{\alpha}}{\longleftrightarrow} F^{\alpha}(n) = \left(F^{\alpha}(N-n)\right)^{*} \tag{2.17}$$

$$\frac{1}{2}\left(s(k) + s(N-k)\right) \overset{DFT^{\alpha}}{\longleftrightarrow} \mathrm{Re}\left(F^{\alpha}(n)\right)$$

$$\frac{1}{2}\left(s(k) - s(N-k)\right) \overset{DFT^{\alpha}}{\longleftrightarrow} \mathrm{j} \times \mathrm{Im}\left(F^{\alpha}(n)\right)$$

- $\mathbf{H}_N^{\alpha} = \mathrm{Re}(\mathbf{F}_N^{\alpha}) - \mathrm{Im}(\mathbf{F}_N^{\alpha})$ est obtenue par la soustraction de la partie imaginaire de la partie réelle de la matrice DFT. Cette matrice est involutive et vérifie la relation :

$$\mathbf{H}_N^{\alpha}.\mathbf{H}_N^{\alpha} = N\mathbf{I}$$

$\mathbf{H}_N^{\alpha}$ ce n'est autre que la matrice de la transformée de Hartley paramétrique désignée par DHT^{α} , dans le cas où $\alpha = -\pi/8$, $\mathrm{H}_N^{-\pi/8}$devient la transformée de Hartley classique.

2.4.1.2 Cryptage d'images DRPE dans le domaine de la DFT paramétrique

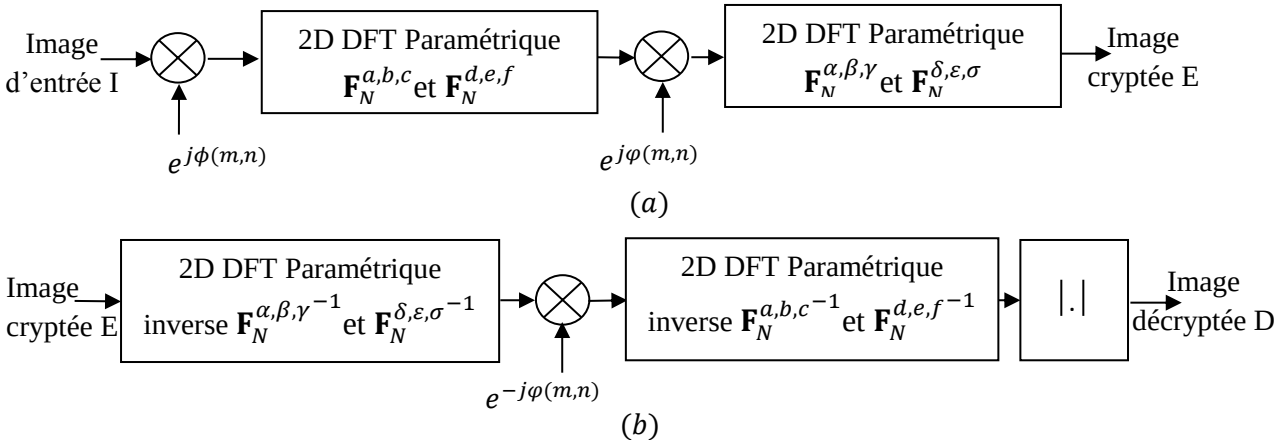


Figure 2.3 : Cryptage d'images DRPE dans le domaine de la DFT paramétrique : *(a)* Schéma de cryptage *(b)* Schéma de décryptage.

Dans cette partie, nous détaillons le principe de cryptage d'images dans le domaine de la DFT Paramétrique, en se référant à la **figure 2.3*.(a)***, qui illustre le schéma de cryptage, nous considérons une image d'entrée I carrée de taille (N, N) c.à.d. $(m = n = N)$, le processus de cryptage consiste à multiplier cette image d'entrée I, élément par élément dans le domaine spatial par une matrice de phase aléatoire $e^{j\phi(N,N)}$ ayant la même taille que l'image d'entrée I . Le résultat obtenu est transformé au domaine fréquentiel en appliquant deux transformées de Fourier paramétriques $\mathbf{F}_N^{a,b,c}$ et $\mathbf{F}_N^{c,d,e}$, nous rappelons ici que l'une des transformées $\mathbf{F}_N^{a,b,c}$ est utilisée pour transformer les lignes, l'autre $\mathbf{F}_N^{c,d,e}$pour transformer les colonnes. Ensuite nous multiplions

la matrice transformée élément par élément dans le domaine fréquentiel par une autre matrice de phase aléatoire $e^{j\varphi(N,N)}$, la résultante est transformée au domaine spatial en appliquant deux autres transformées paramétriques $\mathbf{F}_N^{\alpha,\beta,\gamma}$ et $\mathbf{F}_N^{\delta,\varepsilon,\sigma}$pour donner l'image cryptée E.

L'expression mathématique de l'image cryptée E utilisée dans le schéma de cryptage de la **figure 2.3.*(a)*** est donnée par :

$$\mathrm{E} = \frac{1}{N^2}\left(\mathbf{F}_N^{\alpha,\beta,\gamma}\left(\left(\mathbf{F}_N^{a,b,c}\left(\mathrm{I}\odot e^{j\phi(N,N)}\right)\mathbf{F}_N^{d,e,f}\right)\odot e^{j\varphi(N,N)}\right)\mathbf{F}_N^{\delta,\varepsilon,\sigma}\right) \tag{2.18}$$

Il faut noter que le processus de décryptage tel que représenté dans la **figure 2.3.*(b)*** suit exactement les étapes du processus de cryptage de manière inverse pour donner l'image décryptée D.

Son expression mathématique est donnée par :

$$\mathrm{D} = \frac{1}{N^2}\left(\left(\left(\mathbf{F}_N^{a,b,\gamma}\right)^*\left(\left(\left(\mathbf{F}_N^{\alpha,\beta,\gamma}\right)^*\mathrm{E}\left(\mathbf{F}_N^{\delta,\varepsilon,\sigma}\right)^*\right)\odot e^{-j\varphi(N,N)}\right)\left(\mathbf{F}_N^{d,e,f}\right)^*\right)\odot e^{-j\phi(N,N)}\right), \tag{2.19}$$

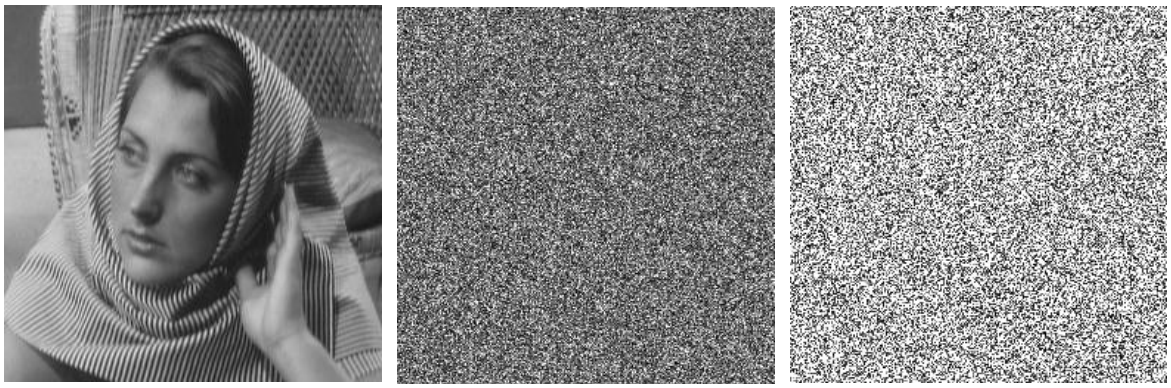
où $(.)^*$désigne la transposée du conjugué complexe des matrices, et $\odot$ dénote la multiplication élément-par-élément des matrices.

Dans le cas particulier, lorsque il s'agit d'une transformée de Fourier paramétrique à un seul paramètre, les quatre matrices transformées $\mathbf{F}_N^{a,b,c}$, $\mathbf{F}_N^{d,e,f}$, $\mathbf{F}_N^{\alpha,\beta,\gamma}$, $\mathbf{F}_N^{\delta,\varepsilon,\sigma}$ de trois paramètres chacune se réduisent à des matrices transformées d'un seul paramètre $\mathbf{F}_N^{a}$, $\mathbf{F}_N^{d}$, $\mathbf{F}_N^{\alpha}$ et $\mathbf{F}_N^{\delta}$, par conséquent, l'expression mathématique de l'image cryptée E devient :

$$\mathrm{E} = \frac{1}{N^2}\left(\mathbf{F}_N^{\alpha}\left(\left(\mathbf{F}_N^{a}\left(\mathrm{I}\odot e^{j\phi(N,N)}\right)\mathbf{F}_N^{d}\right)\odot e^{j\varphi(N,N)}\right)\mathbf{F}_N^{\delta}\right), \tag{2.20}$$

et l'expression de l'image décryptée devient :

$$\mathrm{D} = \frac{1}{N^2}\left(\left((\mathbf{F}_N^{a})^*\left(\left((\mathbf{F}_N^{\alpha})^*\mathrm{E}\left(\mathbf{F}_N^{\delta}\right)^*\right)\odot e^{-j\varphi(N,N)}\right)\left(\mathbf{F}_N^{d}\right)^*\right)\odot e^{-j\phi(N,N)}\right) \tag{2.21}$$



(a) (b)

Figure 2. 4 : Image cryptée de Barbara dans le système DRPE à base de la DFT $^{\alpha}$
(a) Module *(b)* Phase.

La **figure 2.4** est une illustration du cryptage DRPE de l'image de Barbara dans le domaine de la DFT paramétrique à un seul paramètre.

2.4.2 Transformée de Fourier fractionnaire

La transformée de Fourier Fractionnaire (FRFT) est une généralisation de la transformée de Fourier classique (TF), qui a été introduite pour la première fois par Namias [64] en 1980. Elle est aussi appelée dans certains ouvrages, transformée de Fourier rotationnelle ou transformée de Fourier angulaire car elle opère une rotation des signaux d'un angle α dans le plan temps-fréquence. En se basant sur la Référence [8] présentée par S.C.Pei et W.L.Hsue, la transformée de Fourier fractionnaire (FRFT) continue d'ordre a d'une séquence donnée $x(t)$ est donnée par :

$$X_a(u) = \int_{-\infty}^{+\infty} x(t) k_a\,(u,t) dt, \tag{2.22}$$

où $\boldsymbol{k_a(u,t)}$ est le noyau de la transformée donnée par :

$$k_a(u,t) = \sqrt{1 - jcot\alpha}\,.\,e^{j\pi\left(t^2 cot\alpha - 2tucsc(\alpha) + u^2 cot\alpha\right)}$$

$$= \sum_{n=0}^{\infty} exp\left(-\frac{jna\pi}{2}\right).\,\Psi_n(\mathrm{t})\Psi_n(u), \tag{2.23}$$

avec $\boldsymbol{\alpha = \frac{a\pi}{2}}$ et $\boldsymbol{\Psi_n(\mathbf{t})}$ désigne la fonction continue de Hermite-Gauss d'ordre a

$$\Psi_n(\mathrm{t}) = \frac{2^{\frac{1}{4}}}{2^n n!}\varphi_n(t)\sqrt{2\pi}e^{-\pi t^2}, \tag{2.24}$$

où $\varphi_n(t)$ est le *n*-iéme polynôme d'Hermite.

La matrice **F** de taille $(N \times N)$ de la transformée de Fourier discrète classique DFT est définie par :

$$\mathrm{F}_{kn} = \frac{1}{\sqrt{N}} e^{-j\frac{2\pi}{N}kn}, 0 \leq k, n \leq N-1 \tag{2.25}$$

2.4.2.1 Transformée de Fourier fractionnaire discrète

La matrice **F** de la transformée de Fourier discrète (DFT) a quatre valeurs propres distinctes : 1, -1, j, et –j. Considérons maintenant une matrice tridiagonale **S** ayant ses entrées non-zéro :

$$\begin{cases} \mathrm{S}_{n,n} = 2cos\left(\frac{2\pi}{N}.n\right), & 0 < n \leq (N-1) \\ \mathrm{S}_{n,n+1} = \mathrm{S}_{n+1,n} = 1, & 0 < n \leq (N-2) \\ \mathrm{S}_{N-1,0} = \mathrm{S}_{0,N-1} = 1. \end{cases} \tag{2.26}$$

Du moment que **S** est commutative avec **F**, c'est-à-dire $\mathbf{SF} = \mathbf{FS}$, les matrices **F** et **S** ont les mêmes vecteurs propres mais leurs valeurs propres sont différentes.

Partant de la décomposition en valeurs propres de **F,** Pei et Yeh [65] ont défini la matrice $\mathbf{F}^a$ de la transformée de Fourier fractionnaire discrète (DFRFT) d'ordre a de taille $N \times N$ comme suit :

$$\mathbf{F}^a = \mathbf{V}\boldsymbol{\Lambda}^a\mathbf{V}^{\mathrm{T}} = \begin{cases} \sum_{n=0}^{N-1} \mathrm{e}^{-j\frac{\pi}{2}na}\boldsymbol{v_n}\boldsymbol{v_n^T}, & \text{for } N \text{ impair} \\ \sum_{n=0}^{N-2} \mathrm{e}^{-j\frac{\pi}{2}na}\boldsymbol{v_n}\boldsymbol{v_n^T} + \mathrm{e}^{-j\frac{\pi}{2}Na}\boldsymbol{v_N}\boldsymbol{v_N^T}, & \text{for } N \text{ pair} \end{cases}, \tag{2.27}$$

avec $\boldsymbol{\Lambda}^a$ une matrice diagonale dont les coefficients non nuls correspondent aux valeurs propres $\lambda_n^a = \mathrm{e}^{-j\frac{\pi}{2}na}$ de chaque colonne vecteur propre $\boldsymbol{v_n}$ dans $\mathbf{V}$, $\boldsymbol{T}$ désigne la matrice transposée et $\mathbf{V} = [v_0|v_1|\ldots|v_{N-2}|v_{N-1}]$ pour N impair et $\mathbf{V} = [v_0|v_1|\ldots|v_{N-2}|v_N]$ pour N pair.

2.4.2.2 Propriétés de la DFRFT

La transformée DFRFT préserve toutes les propriétés importantes de la version continue FRFT [66].

- La matrice inverse de la transformée DFRFT est donnée par $(\mathbf{F}^a)^{-1} = \mathbf{F}^{-a}$, avec $\mathbf{F}^a.\mathbf{F}^{-a} = \mathbf{I}$ **,** où I est la matrice identité.
- L'additivité des ordres fractionnaires $\mathbf{F}^a.\mathbf{F}^b = \mathbf{F}^{a+b}$.

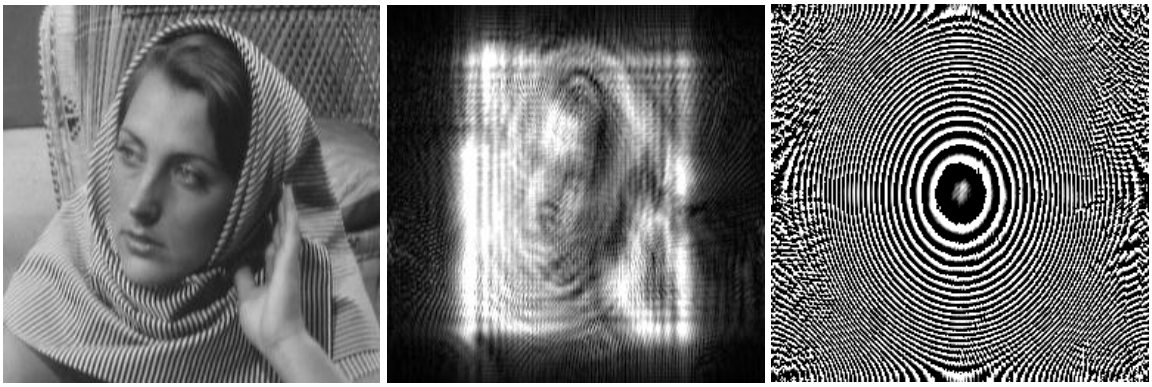
- $\mathbf{F}^0 = \mathbf{I}$, pour $= 0$, $\mathbf{F}^1 = \mathbf{F}$, pour $a = 1$ pour un angle de rotation $\alpha = \frac{\pi}{2}$.

La **figure 2.5** est un exemple concret de l'obtention de la transformée DFRFT de l'image de Barbara en se servant de l'expression suivante :

$$\mathrm{P}_{(a,b)} = \mathbf{F}^a . \mathrm{P} . \mathbf{F}^b, \tag{2.28}$$

avec

- a et b deux ordres paramétriques choisis aléatoirement de l'intervalle [0,1].
- $\mathbf{F}^a$ et $\mathbf{F}^b$ sont les matrices de la transformée DFRFT construites à partir de l'équation (2.27).
- P est la matrice image, $\mathrm{P}_{(a,b)}$est sa transformée DFRFT.



(a) (b)

Figure 2.5 : Image de Barbara et sa transformée DFRFT : *(a)* Module, *(b)* Phase.

2.4.3 Transformée de Fourier fractionnaire discrète multiple

Partant de la définition de la matrice F^{a} de la transformée de Fourier fractionnaire discrète (DFRFT) d'ordre a de taille $N \times N$ donnée en équation (2.27) [8]. Nous pouvons constater que F^a se réduit à la matrice **F** de la transformée de Fourier classique DFT de l'équation (2. 24) lorsque $a = 1$, donc la transformée DFRFT est une généralisation de la transformée DFT, à partir de l'équation (2. 27), nous pouvons aussi généraliser la transformée DFRFT si nous prenons les puissance fractionnaires des valeurs propres $\lambda_k = exp - j\frac{\pi k}{2}$ de la matrice DFT , ce qui donne la matrice $\mathbf{F}^{\bar{a}}$ de la transformée MPDFRFT exprimée par :

$$\mathbf{F}^{\bar{a}} = \begin{cases} \mathbf{V}.diag\left(\left(e^{-j\frac{\pi}{2}0}\right)^{a_0}, \left(e^{-j\frac{\pi}{2}1}\right)^{a_1} \dots \right. \\ \left. \left(e^{-j\frac{\pi}{2}(N-1)}\right)^{a_{N-1}}\right).\mathbf{V}^{\boldsymbol{T}} & pour\ N\ impair \\ \mathbf{V}.diag\left(\left(e^{-j\frac{\pi}{2}0}\right)^{a_0}, \left(e^{-j\frac{\pi}{2}1}\right)^{a_1} \dots \right. \\ \left. \left(e^{-j\frac{\pi}{2}(N-2)}\right)^{a_{N-2}}\right)\left(e^{-j\frac{\pi}{2}N}\right)^{a_N}.\mathbf{V}^{\boldsymbol{T}} & pour\ N\ pair \end{cases} \quad (2.29)$$

$\bar{\boldsymbol{a}}$ est un vecteur paramétrique de taille $1 \times N$ constitué des N ordres paramétrique de la transformée MPDFRFT

$$\bar{\boldsymbol{a}} = \begin{cases} (a_0, a_1, \dots, a_{N-1}), & pour\ N\ impair \\ (a_0, a_1, \dots, a_{N-2}\ a_N), & pour\ N\ pair \end{cases} \quad (2.30)$$

Pour simplifier la présentation, définissons $\boldsymbol{\Lambda}^{\bar{a}}$ comme étant :

$$\boldsymbol{\Lambda}^{\bar{a}} = \begin{cases} diag\left(\left(e^{-j\frac{\pi}{2}0}\right)^{a_0}, \left(e^{-j\frac{\pi}{2}1}\right)^{a_1} \dots \right. \\ \left. \left(e^{-j\frac{\pi}{2}(N-1)}\right)^{a_{N-1}}\right), & pour\ N\ impair \\ diag\left(\left(e^{-j\frac{\pi}{2}0}\right)^{a_0}, \left(e^{-j\frac{\pi}{2}1}\right)^{a_1} \dots \right. \\ \left. \left(e^{-j\frac{\pi}{2}(N-2)}\right)^{a_{N-2}}\right)\left(e^{-j\frac{\pi}{2}N}\right)^{a_N}, & pour\ N\ pair \end{cases} \quad (2.31)$$

$$\boldsymbol{\Lambda} = \begin{cases} diag\left(e^{-j\frac{\pi}{2}0}, e^{-j\frac{\pi}{2}1}, \dots e^{-j\frac{\pi}{2}(N-1)}\right) & pour\ N\ impair \\ diag\left(e^{-j\frac{\pi}{2}(N-2)}, e^{-j\frac{\pi}{2}1}, \dots \right. \\ \left. \quad e^{-j\frac{\pi}{2}(N-2)}, e^{-j\frac{\pi}{2}(N)}\right), & pour\ N\ pair \end{cases} \quad (2.32)$$

$\boldsymbol{\Lambda}$: est la matrice diagonale des valeurs propres de la transformée DFT.

L'expression (2.29) devient

$$\mathbf{F}^{\bar{a}} = \mathbf{V}\boldsymbol{\Lambda}^{\bar{a}}\mathbf{V}^{\mathbf{T}}. \quad (2.33)$$

La transformée 1D MPDFRFT $\mathbf{X}_{\bar{a}}$ d'un vecteur $\mathbf{x}$ de taille $1 \times N$ peut être calculée selon la formule suivante :

$$\mathbf{X}_{\bar{a}} = \mathbf{F}^{\bar{a}}\mathbf{x}. \quad (2.34)$$

2.4.3.1 Propriétés de la MPDFRFT

- Dans le cas où le vecteur paramétrique $\bar{\boldsymbol{a}} = (a, a, \dots, a)$, l'expression de la matrice transformée de MPDFRFT dans (2.29) se ramène à la définition de DFRFT dans (2.27), elle est donc un cas spécial de la MPDFRFT [8].
- La matrice inverse de la transformée MPDFRFT $\mathrm{F}^{\bar{a}}$ est $(\mathbf{F}^{\bar{\boldsymbol{a}}})^{-\mathbf{1}} = \mathrm{F}^{-\bar{a}}$**,** donc $\mathbf{F}^{\bar{\boldsymbol{a}}}.\mathbf{F}^{-\bar{\boldsymbol{a}}} = \mathbf{I}$ qui est la matrice identité.
- Matrice identité : Si $\bar{\boldsymbol{a}} = \bar{0} = (0, 0, \dots, 0)$, $\mathbf{F}^{\bar{\boldsymbol{a}}} = \mathbf{V}\boldsymbol{\Lambda}^{\bar{\mathbf{0}}}\mathbf{V}^{\mathbf{T}} = \mathbf{V}.\mathbf{V}^{\mathbf{T}} = \mathbf{I}$.

  Si $\bar{\boldsymbol{a}}_{\mathbf{1}}$ et $\bar{\boldsymbol{a}}_{\mathbf{2}}$ deux vecteurs paramétriques de même taille :
- $\mathbf{F}^{\bar{a}_1}.\mathbf{F}^{\bar{a}_2} = (\mathbf{V}\boldsymbol{\Lambda}^{\bar{a}_1}\mathbf{V}^{\mathbf{T}})(\mathbf{V}\boldsymbol{\Lambda}^{\bar{a}_2}\mathbf{V}^{\mathbf{T}}) = \mathbf{V}\boldsymbol{\Lambda}^{\bar{a}_1+\bar{a}_2}\mathbf{V}^{\mathbf{T}} = \mathbf{F}^{\bar{a}_1+\bar{a}_2}$
- $\mathbf{F}^{\bar{a}_1}.\mathbf{F}^{\bar{a}_2} = \mathbf{V}\boldsymbol{\Lambda}^{\bar{a}_1+\bar{a}_2}\mathbf{V}^{\mathbf{T}} = \mathbf{V}\boldsymbol{\Lambda}^{\bar{a}_2+\bar{a}_1}\mathbf{V}^{\mathbf{T}} = \mathbf{F}^{\bar{a}_2}.\mathbf{F}^{\bar{a}_1}$

2.4.3.2 Cryptage d'images DRPE dans le domaine de la transformée MPDFRFT

Dans le schéma de cryptage/décryptage d'images proposé par Unnikrishnan et Singh dans [5]. Pie and Hsue [8] ont remplacé la transformée (DFRFT) par (MPDFRFT) et ont proposé la DRPE dans le domaine MPDFRFT dont les processus de cryptage et de décryptage sont représentés sur la **figure 2.6**.

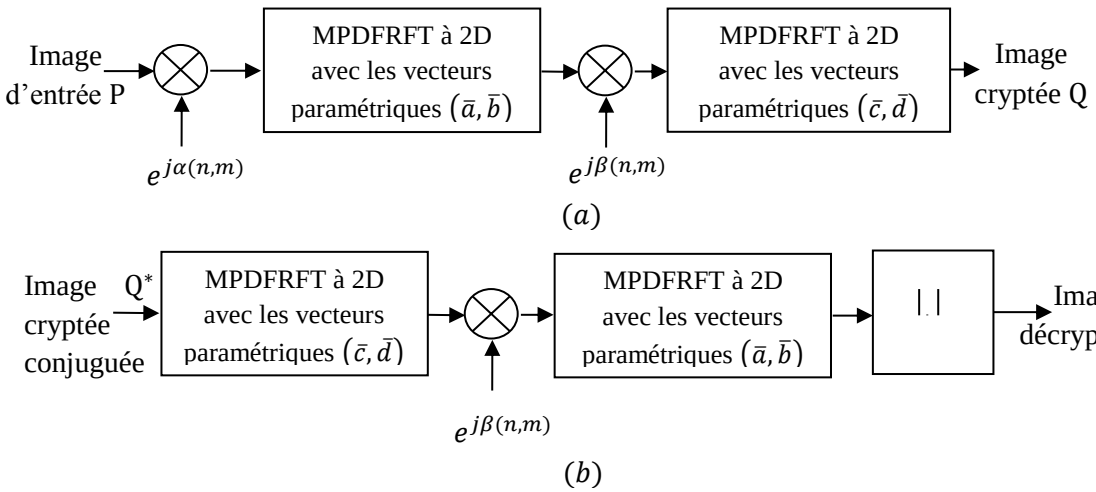


Figure 2.6 : Processus de cryptage/décryptage d'images de la Double Random Phase Encoding dans le domaine de la MPDFRFT *(a)* Schéma de cryptage *(b)* Schéma de décryptage.

La Transformée unidirectionnelle 1D- MPDFRFT peut s'étendre au cas bidirectionnel, or pour une image P de taille $(N \times M)$, la transformée bidirectionnelle 2D-MPDFRFT de cette image est donnée par :

$$\mathrm{P}_{(\bar{a},\bar{b})} = \mathbf{F}^{\bar{\boldsymbol{a}}}.\mathrm{P}.\mathbf{F}^{\bar{\boldsymbol{b}}}, \tag{2.35}$$

avec

- $\bar{\boldsymbol{a}}$ et $\bar{\boldsymbol{b}}$ deux vecteurs paramétriques de tailles $1 \times N$, $1 \times M$ respectivement.
- $\mathbf{F}^{\bar{\boldsymbol{a}}}$ et $\mathbf{F}^{\bar{\boldsymbol{b}}}$ sont les matrices de la transformée MPDFRFT construites à partir de l'équation (2.29).
- $[exp(j\alpha(n,m))]$ et $[exp(j\beta(n,m))]$ dénotent deux matrices de phase aléatoire de taille $(N \times M)$ chacune.
- $\alpha(n,m)$ et $\beta(n,m)$ sont des bruits blancs, uniformément distribués dans l'intervalle$[0, 2\pi]$, avec $1 \leq n \leq N$ et $1 \leq m \leq M$, et qui sont indépendants entre eux.

En se référant au schéma de la **figure (2.6),** l'expression mathématique reliant l'image cryptée Q et l'image d'entrée P est donnée par :

$$\mathrm{Q} = \mathbf{F}^{\bar{c}}\left\{\left(\mathbf{F}^{\bar{a}}\left(\mathrm{P} \odot \left[e^{j\alpha(n,m)}\right]\mathbf{F}^{\bar{b}}\right)\right) \odot \left[e^{j\beta(n,m)}\right]\right\}\mathbf{F}^{\bar{d}}, \tag{2.36}$$

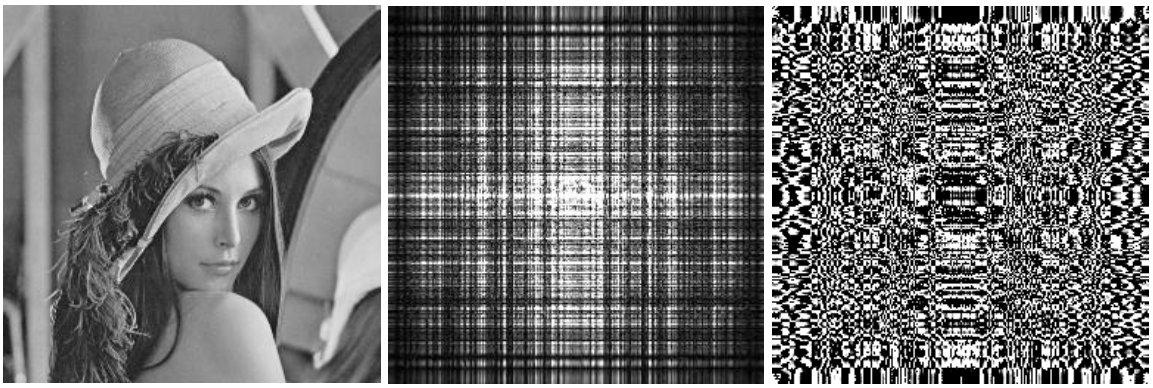
où $\odot$ dénote la multiplication élément par élément entre deux matrices. Partant de l'équation (2.33), $(\mathbf{F}^{\bar{a}})^{*} = \mathbf{F}^{-\bar{a}}$, le complexe conjugué de l'image cryptée Q est donné par :

$$\mathrm{Q}^{*} = \mathbf{F}^{-\bar{c}}\left\{\left(\mathbf{F}^{-\bar{a}}\left(\mathrm{P} \odot \left[e^{-j\alpha(n,m)}\right]\mathbf{F}^{-\bar{b}}\right)\right) \odot \left[e^{-j\beta(n,m)}\right]\right\}\mathbf{F}^{-\bar{d}} \tag{2.37}$$

L'expression mathématique de l'image décryptée R est donnée par :

$$\mathrm{R} = \left|\mathbf{F}^{\bar{a}}\left\{\left(\mathbf{F}^{\bar{c}}\mathrm{Q}^{*}\mathbf{F}^{\bar{d}}\right) \odot \left[e^{j\beta(n,m)}\right]\mathbf{F}^{\bar{b}}\right\}\right|$$

$$= \left|\mathbf{P} \odot \left[e^{j\boldsymbol{\alpha}(\boldsymbol{n},\boldsymbol{m})}\right]\right| = \mathbf{P} \tag{2.38}$$



(a) (b)

Figure 2. 7 : Image de Lena et sa transformée MPDFRFT *(a)* Module *(b)* Phase.

La **figure 2.7** ci-dessus est un exemple concret de l'obtention de la transformée MPDFRFT de l'image de Lena.

2.5 Suites chaotiques

En mathématiques, la théorie du chaos étudie le comportement des systèmes dynamiques qui sont très sensibles aux conditions initiales, un phénomène généralement illustré par l'effet papillon. Des différences infimes dans les conditions initiales (comme des erreurs d'arrondi dans les calculs numériques) entraînent des résultats totalement différents pour de tels systèmes, rendant en général toute prédiction impossible à long terme. Cela est valable même pour des systèmes déterministes, ce qui signifie que leur comportement futur est entièrement déterminé par leurs conditions initiales, sans intervention du hasard. En d'autres termes, la nature déterministe de ces systèmes ne les rend pas prévisibles. Ce comportement est connu sous le nom de chaos déterministe, ou tout simplement de chaos. Le comportement chaotique est à la base de nombreux systèmes naturels, tels que la météo ou le climat. Ce comportement peut être étudié grâce à l'analyse par des modèles mathématiques chaotiques, ou par des techniques analytiques de récurrence et des applications de Poincaré. La théorie du chaos a des applications en météorologie, sociologie, physique, informatique, ingénierie, économie, biologie et cryptographie. Les suites chaotiques peuvent être unidimensionnelles ou multidimensionnelles. Nous en citerons les deux types auxquels nous nous sommes intéressés dans notre travail de thèse, à savoir la suite logistique et la suite chaotique linéaire par morceaux ou « piecewise linear chaotic map » PLCM en anglais [67].

2.5.1 Suite Logistique (Logistic map)

La suite logistique est une fonction chaotique 1D non linéaire définie par:

$$x_{n+1} = \mu . x_n . (1 - x_n), \tag{2.39}$$

où $\mu \in [0,4]$ est le paramètre de contrôle. Elle est générée itérativement en partant de $x_0 \in [0,1]$ appelée condition initiale. La suite logistique est vraiment chaotique si $\mu \in [3.75,4]$ et purement chaotique si $\mu \cong 4$ comme illustré sur le diagramme de bifurcation de Hopf de la **figure 2.8** ci-dessus ou on observe clairement l'évolution de sa dynamique en fonction du paramètre de contrôle μ [67]. La suite montre un bon comportement et elle est fréquemment utilisée dans de nombreuses applications [68-70].

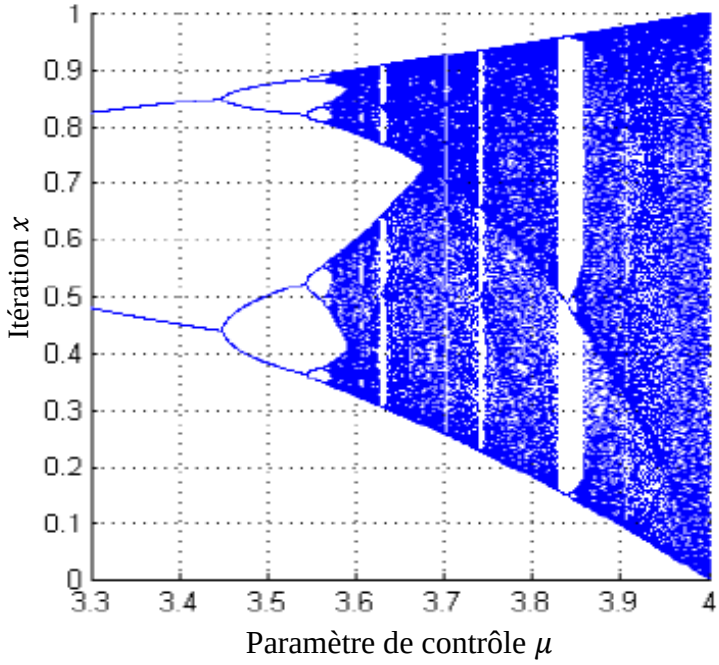


Figure 2.8: Diagramme de bifurcation de la suite logistique.

2.5.2 Suite chaotique linéaire par morceaux (PLCM map)

La Suite chaotique du système PLCM a gagné récemment une attention particulière de plusieurs chercheurs en théorie du chaos en raison de sa simplicité dans la représentation, son efficacité en implémentation, et son bon comportement dynamique [71]. La suite chaotique PLCM peut être décrite dans l'équation (2.40) par :

$$z_{k+1} = F(z_k, \lambda) = \begin{cases} \dfrac{z_k}{\lambda}, & 0 \le z_k < \lambda \\ \dfrac{z_k - \lambda}{0.5 - \lambda}, & \lambda \le z_k < 0.5 \\ F(1 - z_k, \lambda), & 0.5 \le z_k < 1 \end{cases}, \tag{2.40}$$

où $z_k \in (0,1)$ avec $n \in \mathbb{N}$ et z_0 comme condition initiale. $\lambda \in (0,0.5)$ est considéré comme étant le paramètre de contrôle. Le système PLCM a une distribution uniforme invariante, une bonne ergodicité et une bonne confusion [72-74], de sorte qu'il peut fournir une excellente séquence aléatoire, qui convient aux systèmes cryptographiques. La distribution de z avec différents λ du système PLCM est représentée sur la **figure 2.9**, où les valeurs de z sont uniformément réparties.

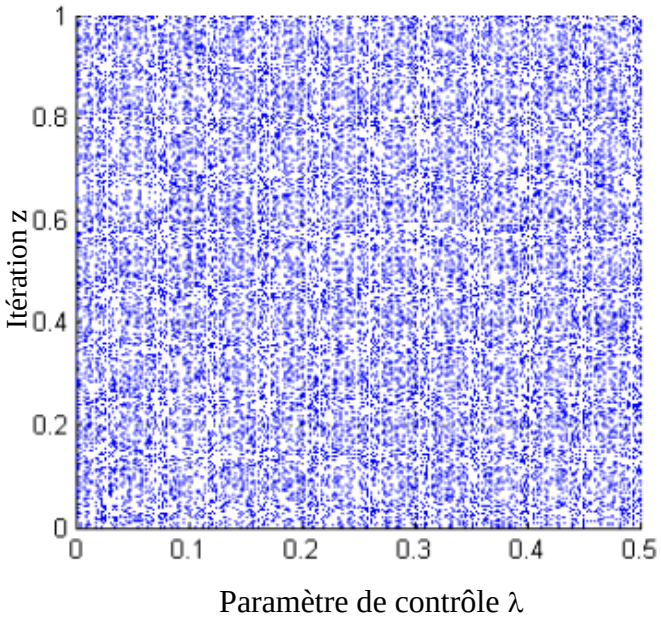


Figure 2.9: Diagramme de bifurcation de la suite chaotique PLCM.

2.5.3 Propriétés des suites chaotiques

- **Sensibilité à la condition initiale :** Un changement minime dans la condition initiale provoque en sortie un régime pseudo-aléatoire complètement différent de l'état précédent, c'est le fameux effet papillon dont on a parlé [67], [73].
- **Pseudo-aléatoires** : une suite chaotique gouvernée par une équation déterministe permet de générer un régime chaotique pseudo-aléatoire.
- **Ergodique :** un processus chaotique est ergodique, car il possède la même distribution en sortie quel que soit la distribution de la variable présente à l'entrée.

2.6 Conclusion

Dans ce chapitre, nous avons présenté les outils mathématiques nécessaires pour l'étude et la compréhension du cryptage d'images dans le domaine fréquentiel à travers des rappels portant sur les expressions mathématiques des transformées classiques comme la DFT et la DHT ainsi que leurs expressions inverses. Ces transformées représentent la base de construction des transformées paramétriques. En effet, nous avons établi un développement mathématique pour l'aboutissement aux expressions mathématiques directes et inverses de ces transformées paramétriques. Afin de valoriser leurs importances, des schémas de quelques algorithmes pertinents de cryptage d'images utilisant ces transformées ont été présentés et consolidés par des illustrations des images cryptées et décryptées. Ces transformées seront aussi utilisées

convenablement dans le chapitre suivant dans le développement d'une nouvelle méthode de cryptage d'images. Enfin, nous avons passé en revue deux suites chaotiques à savoir la suite chaotique logistique et la suite chaotique PLCM qui seront exploitées dans les chapitres qui suivent.

Chapitre 3

Proposition d'une nouvelle technique de cryptage basée sur un pré-cryptage non linéaire récursif

3.1 Introduction

Le système optique de cryptage d'images DRPE introduit pour la première fois par Refregier et Javidi [4] est d'une importance capitale [75] à cause de son traitement parallèle. Ce système optique utilise la transformée de Fourier (FT) bidimensionnelle et donc on l'appelle FT-DRPE. Afin d'augmenter la sécurité du système FT-DRPE, des transformations paramétriques telles que la transformée de Fourier fractionnaire (FRFT) [5], la transformée de Fresnel [33], la transformée de Fourier fractionnaire discrète à paramètres multiples (MPDFRFT) [8], la transformée de Gyrator [34], la transformée paramétrique réciproque-orthogonale (ROP) [35], [6] et la transformée paramétrique involutive [7] ont été utilisées à la place de la FT, où leurs paramètres indépendants ont été exploités comme une clé secrète supplémentaire. Plus précisément, la DRPE optique à base de DFRFT (DFRFT-DRPE) et DRPE MPDFRFT (MPDFRFT-DRPE) sont d'une grande importance et ont été largement considérées dans la littérature pour développer des versions plus sécurisées en y introduisant des schémas de brouillage digital [42-45], [77]. Ces versions DRPE résultantes ont généralement besoin d'un calculateur pour effectuer le brouillage et sont donc considérées comme des techniques de cryptage opto-digitales. Bien que les versions DRPE optiques et opto-digitales soient elles efficaces, elles peuvent ne pas résister à certaines attaques [9-10], [78]. Ceci est principalement dû au fait que les transformées utilisées sont linéaires et les schémas de brouillage associés peuvent également être considérés comme des transformations linéaires. Par conséquent, le système DRPE résultant est devenu linéaire et donc fragile à certaines attaques.

Afin de surmonter ce problème de linéarité, une technique de cryptage d'images basée sur un prétraitement non linéaire digital a été récemment proposée dans [11]. Ce prétraitement consiste à obtenir une image prétraitée en effectuant l'opération XOR dans le domaine spatial entre chaque pixel de l'image d'entrée et son pixel correspondant dans la même position d'une image créée aléatoirement avant d'appliquer un système DRPE quelconque. Il a été montré dans [11] que ce prétraitement non-linéaire associé avec un MPDFRFT-DRPE optique conduit à un nouveau DRPE opto-digital qui surpasse les autres versions de DRPE existantes, notamment en termes de sensibilité de la clé secrète. Quoique la technique proposée dans [11] semble efficace et attrayante, la non-linéarité offerte par l'opération XOR a été introduite dedans pour chaque pixel séparément et indépendamment des uns et des autres. Cependant, à partir d'un autre point de vue, il est hautement souhaitable de développer une technique de cryptage d'images tout en introduisant un prétraitement non linéaire plus performant. Cela constitue un premier objectif de

notre travail de thèse. En effet, il s'agit d'un développement d'une technique de cryptage d'images efficace basée sur un nouveau prétraitement ou pré-cryptage non linéaire récursif [12].

Par ailleurs, dans la suite de ce chapitre nous proposons un nouveau pré-cryptage digital non linéaire récursif qui pourra être utilisé après un DRPE quelconque. Nous présentons également l'évaluation cryptographique de ce pré-cryptage à travers un ensemble de tests effectués puis nous donnons son adjonction au système DRPE ainsi que l'implémentation opto-digital de la technique de cryptage d'images proposée résultante. Enfin, une analyse et une comparaison des performances de cette technique sont effectuées.

3.2 Pré-cryptage non linéaire récursif proposé

Il est bien connu dans les méthodes de calcul numérique que l'inconvénient principal de toute approche récursive est l'accumulation et la propagation de l'erreur. En contradiction avec ces méthodes, les techniques de cryptage recherchent fortement toute approche ayant cet inconvénient ou cette propriété. Par conséquent, nous exploitons avantageusement cette propriété de l'approche récursive dans le cryptage d'images pour obtenir la dépendance souhaitée entre les pixels de l'image prétraitée tout en introduisant un nouveau pré-cryptage non linéaire récursif. Il consiste tout d'abord à brouiller l'image d'entrée puis à appliquer récursivement l'opération de bit XOR sur chaque paire de pixels consécutifs suivant un balayage choisi de pixels. La paire de départ est formée par le pixel initial dans ce balayage et par un entier aléatoire de huit bits. La clé secrète pour le pré-cryptage digital proposé est bien cet entier aléatoire qui peut être choisi arbitrairement de 0 à 255, et les cas de brouillage possibles, qui ont $(M \times N)!$ possibilités, où $M \times N$ est la taille de l'image d'entrée. Pour les simulations faites sur ordinateur, nous considérons des images carrées, c'est-à-dire $M = N$.

La méthode de pré-cryptage non linéaire récursif proposée dans le domaine spatial s'articule sur l'architecture de substitution-diffusion évoquée il y a longtemps par Shannon [3], et qui consiste en un changement des positions des pixels de l'image à crypter (phase de substitution) selon une distribution imposée par la suite chaotique PLCM, puis à transformer les valeurs de ces pixels (phase de diffusion) en se servant de l'opérateur XOR. L'approche proposée se résume dans les points suivants :

Phase de substitution

1) Redimensionner l'image d'entrée en un vecteur **i** de longueur $1 \times (N \times N)$.

2) Générer chaotiquement un vecteur **z**, $\{z_k, k = 1, 2, 3, \dots, N \times N\}$, en utilisant la suite chaotique PLCM avec les paramètres $\{z_0, \lambda\}$.
3) Trier le vecteur **z** selon un ordre croissant pour former un vecteur **y** puis former un vecteur de carte de permutation m telle que $m_k$est la position de l'élément y_k dans le vecteur z, soit $\{y_k = z_{m_k}, k = 1, 2, 3, \dots, N \times N\}$.
4) Brouiller le vecteur **i** en utilisant le vecteur de carte de permutation **m** pour former un vecteur **s** tel que s_k est l'élément $(m_k)^{\text{éme}}$ de **i**, soit $\{s_k = i_{m_k}, k = 1, 2, 3, \dots, N \times N\}$.

Phase de diffusion

5) Effectuer l'opération XOR bit par bit récursivement sur les éléments adjacents de **s** pour former un vecteur **x** selon la formule suivante :

$$x_k = \begin{cases} s_k \oplus r, & k = 1 \\ s_k \oplus x_{k-1}, & k = 2, 3, \dots, N \times N \end{cases}, \quad (2)$$

où $r = round\left(255 * z_{(N \times N)}\right)$, c'est-à-dire que l'entier aléatoire r est choisi comme étant le dernier élément du vecteur chaotique **z** converti en un entier de huit bits.

6) Enfin, l'image pré-cryptée est obtenue en redimensionnant le vecteur **x** en une matrice $N \times N$.

L'entier aléatoire r est choisi dans l'étape 5 pour être un scalaire et le pixel pré-crypté x_k dans Eq. 2 est obtenu par une seule opération XOR. Ce pré-cryptage est adopté dans les simulations par Matlab que nous avons effectué pour sa simplicité. Cependant, un autre schéma peut être établi en choisissant **r** comme un vecteur aléatoire de taille $1 \times (N \times N)$ de huit bits, puis en effectuant une opération XOR élément par élément entre les vecteurs **s** et **r** avant d'effectuer récursivement l'opération XOR sur le éléments du vecteur résultant. Il convient de mentionner que pour tout schéma sélectionné, une application récursive de l'opération XOR dans le pré-cryptage est obligatoire pour obtenir une sensibilité de la clé élevée pour l'ensemble du système de cryptage d'image.

3.3 Evaluation cryptographique de la méthode de pré-cryptage digital proposé

L'évaluation cryptographique de la méthode de pré-cryptage proposée passe à travers des tests bien connus dans le domaine de la cryptographie et qui sont définis au Chapitre 1, pour se faire, nous nous sommes servis des trois images de test standards, celles de Lena, Barbara et Living-room de taille (256×256), (256×256) et (512×512), respectivement. La **figure 3.1** illustre le résultat de pré-cryptage de ces images où nous constatons visuellement que les images cryptées sont suffisamment brouillées, En conséquence, la méthode de pré-cryptage proposée a

une sécurité perceptuelle satisfaisante vis-à-vis du test subjectif, cela ne suffira pas. Pour confirmer l'efficacité de pré-cryptage par la méthode proposée, nous utilisons les mesures de test objectives à savoir le PSNR et le coefficient de corrélation.

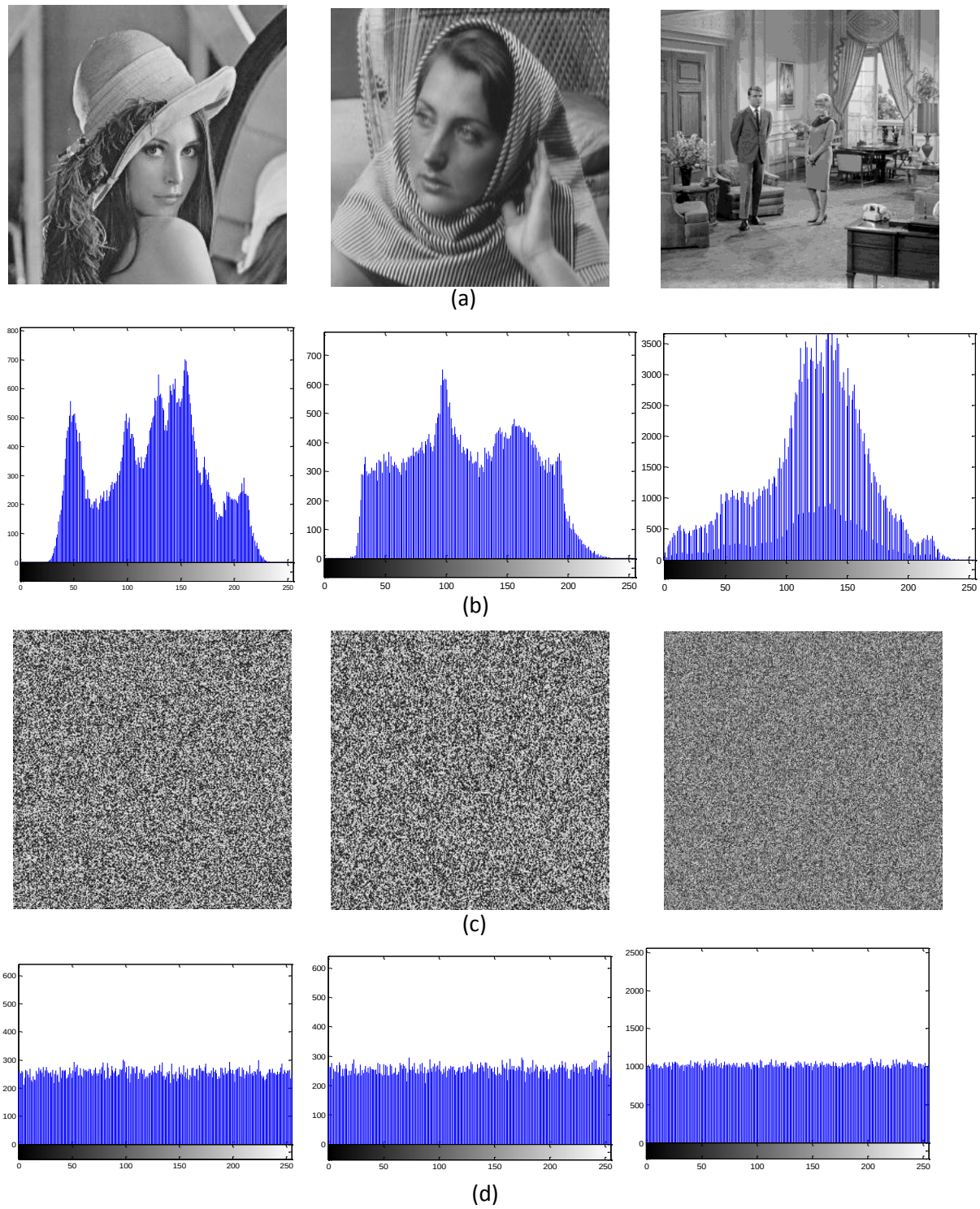


Figure 3.1 : Résultats de pré-cryptage proposé : (a) Images originales de Lena, Barbara et Living-room (b) Leurs histogrammes correspondants (c) Images pré-cryptées de Lena, Barbara et Living-room (d) Leurs histogrammes correspondants.

Le **tableau 3.1** récapitule les résultats de calcul du PSNR et du coefficient de corrélation et indique clairement l'efficacité et la supériorité du pré-cryptage proposé lorsqu'il est comparé conjointement avec le prétraitement reporté dans [11] et la méthode présentée dans [79] en termes de PSNR et de coefficient de corrélation.

Tableau 3.1 Comparaison des résultats obtenus du PSNR et du coefficient de corrélation entre la méthode de pré-cryptage proposée et celles de [11] et [79] pour différentes images de test.

Image cryptée		PSNR, dB			Corrélation		
		Méthode proposée	[11]	[79]	Méthode proposée	[11]	[79]
Lena	256 × 256	9.2014	9.2355	9.2219	-0.00043	0.0028	-0.0059
Barbara	256 × 256	9.1288	9.1457	9.1835	-0.00037	-0.0019	0.0059
Living	512 × 512	9.3840	9.3857	9 .396	-0.0043	-0.0089	0.0056

3.3.1 Analyse d'histogrammes

Nous remarquons sur la **figure 3.1**, qu'en partant d'histogrammes différents pour des images originales différentes de Lena, Barbara et Living-room, nous retrouvons les mêmes histogrammes de leurs images cryptées qui ressemblent à un bruit blanc uniforme, cela confirme que la méthode de pré-cryptage ramène toutes les images originales à des images cryptées ayant les mêmes histogrammes , ce qui empêche les attaquants d'en tirer la moindre information qui pourra révéler l'opération de cryptage et par conséquent, nous pouvons conclure que notre approche résiste aux attaques par l'analyse d'histogrammes.

3.3.2 Resistance aux pertes des données (Loss data)

Pour tester la résistance de la méthode de pré-cryptage face à l'une des erreurs qui peuvent survenir dans le canal de transmission, telle que la perte des données ou (Loss data), nous considérons le cas où une partie des pixels de l'image cryptée a été perdue au cours de la transmission. D'après les résultats de simulation illustrés dans la **figure 3.2**, Nous remarquons que suite aux différents pourcentages de pertes des donnés atteignant l''image pré-cryptée allant jusqu'a un pourcentage de (50%), l'information sur l'image pré-décryptée n'est pas éliminée totalement, en effet l'image pré-décryptée reste visible et identifiable à l'œil nu malgré qu'elle est bruitée. En conséquence, ces résultats prouvent la robustesse de la méthode proposée vis-à-vis du test Loss data et démontre sa résistance face aux erreurs de transmission.

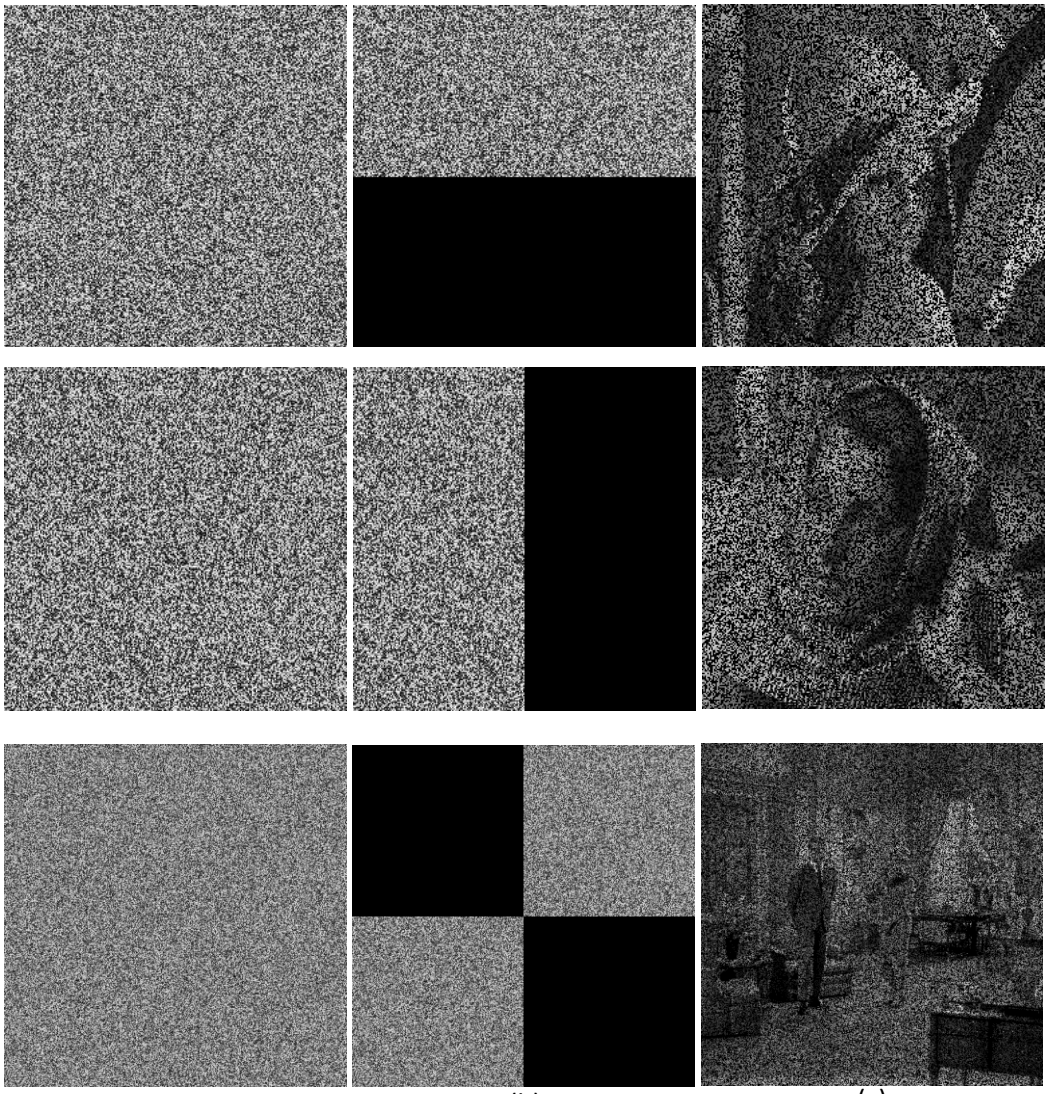


Figure 3.2: Illustration du test de pertes de données : (a) Images pré-cryptées de Lena, Barbara et Living-room (b) Leurs images pré-cryptées avec des pertes de données de 50% (c) Images pré-décryptées de Lena, Barbara et Living-correspondantes.

3.3.3 Analyse de la corrélation entre pixels adjacents

Pour vérifier le degré de destruction de la dépendance entre pixels adjacents sur une image pré-cryptée par la méthode proposée, nous avons pris aléatoirement un échantillon de 1000 pixels adjacents de cet image, nous avons mesuré le coefficient de corrélation inter pixels dans les trois directions (verticale, horizontale, diagonale) et comparer ces mesures avec celles de l'image originale correspondante. Le **tableau 3.2** récapitule les mesures des coefficients de corrélation des images pré-cryptées et de leurs images originales dans les trois directions. Les coefficients de corrélation mesurés pour les images originales sont proche de 1, alors que les coefficients de

corrélation des images pré-cryptées s'approchent de 0. On en déduit que le cryptage a atténué considérablement la corrélation entre les pixels des images pré-cryptées.

Tableau 3.2 Résultats de test et de comparaison de corrélation inter-pixels adjacents dans les trois directions de l'image de Lena entre la méthode de pré-cryptage proposée et celles de [11] et [79].

	Coefficient de corrélation Image originale / image cryptée		
Direction	**Methode proposée**	**[11]**	**[79]**
Horizontale	0.9258/0.0010	0.9258/0.0017	0.9258/0.0017
Verticale	0.9593/0.0048	0.9593/0.0148	0.9593/0.0012
Diagonale	0.9037/-0.0020	0.9037/-0.0022	0.9037/-0.0024

La **figure 3.3** représente respectivement les distributions des corrélations des pixels adjacents horizontales, verticales et diagonales de l'image originale et l'image cryptée. Cette figure confirme les résultats du **tableau 3.2**, car la distribution des intensités des pixels de l'image originale se concentre sur la diagonale, les pixels sont donc fortement corrélés, tandis que ceux de l'image cryptée sont non-corrélés et possèdent une distribution uniforme.

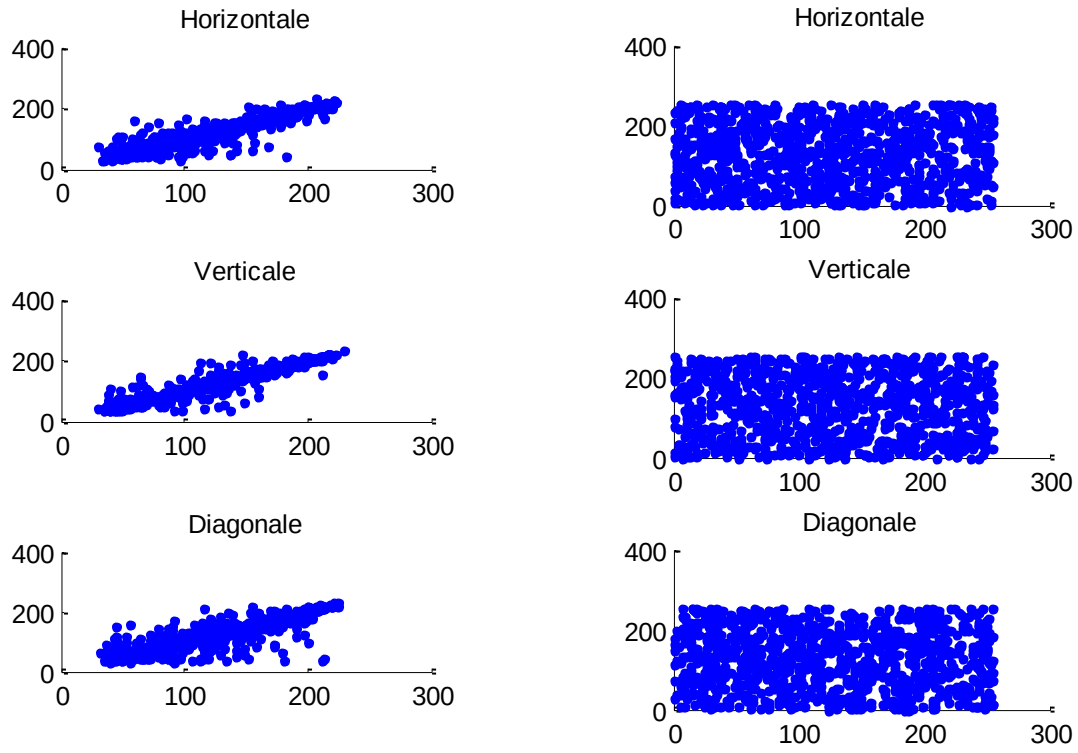
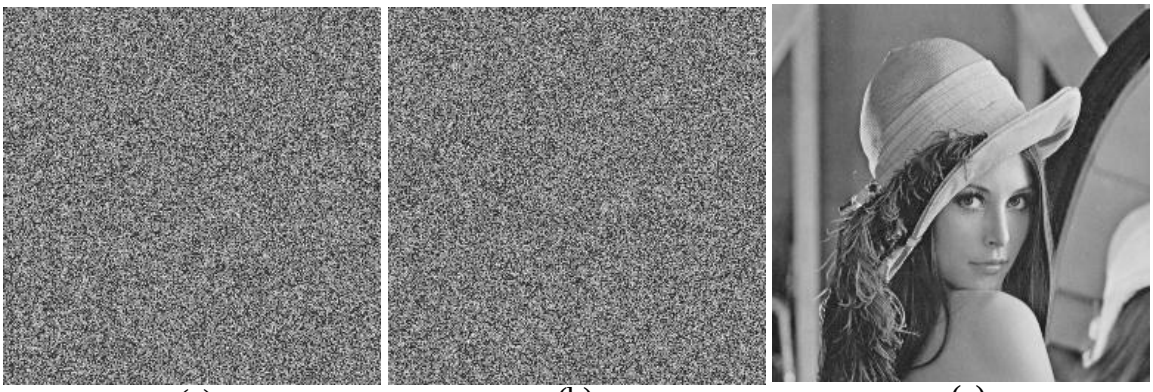


Figure 3.3 Illustration de la distribution des intensités des pixels de l'image originale de Lena et celle de son image pré-cryptée dans les trois directions (horizontale, verticale et diagonale).

3.3.4 Test de sensibilité de la clé



(a) (b) (c)

Figure 3.4 Illustration du Test de sensibilité de la clé de pré-cryptage digital : (a) Image pré-décryptée de Lena avec $\{z_0' = z_0 + 10^{-16}, \lambda' = \lambda\}$, (b) Image pré- décryptée de Lena avec $\{z_0' = z_0, \lambda' = \lambda + 10^{-16}\}$, (c) Image pré-décryptée de Lena avec $\{z_0' = z_0, \lambda' = \lambda\}$.

Tel qu'il a été mentionné dans la partie 3.2, la clé secrète du pré-cryptage digital proposé est composée de l'entier aléatoire $\boldsymbol{r}$ qui est choisi arbitrairement de 0 à 255, la succession choisie qui est l'une des cas de brouillage possibles, qui ont $(\boldsymbol{M} \times \boldsymbol{N})!$ possibilités, où $\boldsymbol{M} \times \boldsymbol{N}$ est la taille de l'image d'entrée, et les paramétres de la suite chaotique PLCM $\{\boldsymbol{z_0}, \lambda\}$, pour plus de simplification , nous admettons que la clé de pré-cryptage est composée seulement de $\{\boldsymbol{z_0}, \lambda\}$ et $\{\boldsymbol{z_0}', \lambda'\}$ est la clé de pré-décryptage correspondante, pour vérifier la sensibilité du pré-cryptage digital proposé , l'image pré-cryptée est pré-décryptée en opérant une erreur dans l'un des élements de sa composante toute en gardant les autres, la **figure 3.4** illustre les trois cas possibles $\{\boldsymbol{z_0'} = \boldsymbol{z_0} + \boldsymbol{10^{-16}}, \lambda' = \lambda\}, \{\boldsymbol{z_0'} = \boldsymbol{z_0}, \lambda' = \lambda + \boldsymbol{10^{-16}}\}$ et $\{\boldsymbol{z_0'} = \boldsymbol{z_0}, \lambda' = \lambda\}$, les deux premiers cas montrent clairement que l'image pré-décryptée est totalement brouillée , ce qui prouve la sensibilité du pré-cryptage digital à la clé $\{\boldsymbol{z_0}, \lambda\}$.

3.3.5 Test statistique de NIST

Le test statistique est employé pour calculer une *P-value*. Chaque *P-value* est la probabilité qu'un générateur de nombre aléatoire parfait produise une séquence moins aléatoire que la séquence testée. Une *P-value* égale à 1 signifie que la séquence est parfaitement aléatoire. Une *P-value* égale à 0 signifie que la séquence est non-aléatoire. Si la *P-value* ≥ α, alors l'hypothèse nulle est acceptée (i.e., la séquence apparaît aléatoire). Si *P-value* < α, alors

l'hypothèse nulle est rejetée (i.e., la séquence apparaît non aléatoire). Le niveau de signification α peut être choisi pour les tests. Il est choisi typiquement dans l'intervalle [0.001, 0.01].

- α égale à 0.001 indique qu'une séquence sur 1000 est rejetée par le test si la séquence n'est pas aléatoire. Pour une *P-value* ≥ 0.001, la séquence peut être considérée comme aléatoire. Pour une *P-value* < 0.001, une séquence peut être considérée comme non aléatoire.
- α égale à 0.01 indique qu'une séquence sur 100 est rejetée. Une *P-value* ≥ 0.01 montre que la séquence est aléatoire.

Tableau 3.3 Résultats de test statistique de NIST de la méthode de pré-cryptage proposée effectué sur les images cryptées de Lena, Barbara et de Baboon.

Test statistique	*P-value*		
	Lena	**Barbara**	**Baboon**
Frequency (monobits) test	0.753521	0.098943	0.157950
Test for frequency within a block	0.322226	0.493783	0.427333
Runs test	0.193635	0.704893	0.225509
Test for the longest run of ones in a block	0.825319	0.635556	0.347930
Random binary matrix rank test	0.188150	0.785979	0.093579
Discrete Fourier transform (spectral) test	0.354010	0.093089	0.797221
Non-overlapping (aperiodic) template matching test	0.014082	0.948289	0.704478
Overlapping (periodic) template matching Test	0.788155	0.950197	0.246692
Maurer's universal statistical test	0.232503	0.980860	0.905970
Linear complexity test	0.649625	0.038249	0.034130
Serial test	0.146951	0.531820	0.096066
Approximate entropy test	0.098851	0.001366	0.492156
Cumulative sum (cusum) test	0.675485	0.093845	0.099758
Random excursions test	0.847058	0.439047	0.814918
Random excursions variant test	0.276227	0.675158	0.397392

Le test statistique de NIST de la méthode de pré-cryptage proposée est effectuée sur trois images cryptées de Lena, Barbara et Baboon, après transformation de chaque image cryptée en un vecteur contenant tous les pixels de cette image exprimés en binaire pour avoir une longue suite formée des 0 et des 1, le niveau de signification est choisi α égale à 0.01. Les résultats de test pour les trois images sont récapitulés dans le tableau3.3, il montre que les valeurs de *P-value*

sont toutes supérieures à 0.01 pour les trois images. Ces résultats confirment le passage avec succès des 15 tests et prouve l'aspect aléatoire de la méthode proposée.

3.4 Nouvelle technique DRPE basée sur le pré-cryptage proposé

Le système de cryptage d'images DRPE consiste à (1) multiplier l'image d'entrée par un masque de phase aléatoire (RPM_1) dans le domaine spatial, (2) transformer le résultat obtenu de (1) par la transformation de Fourier bidimensionnelle, (3) multiplier le résultat obtenu de (2) par un autre masque de phase aléatoire (RPM_2) dans le domaine fréquentiel, et enfin (4) transformer le résultat obtenu de (3) par le FT bidimensionnel pour obtenir l'image cryptée. Les deux masques (RPM_1) et (RPM_2) sont statistiquement indépendants, le premier étant utilisé pour blanchir l'image, tandis que le second est utilisé comme clé secrète pour les processus de cryptage et de décryptage.

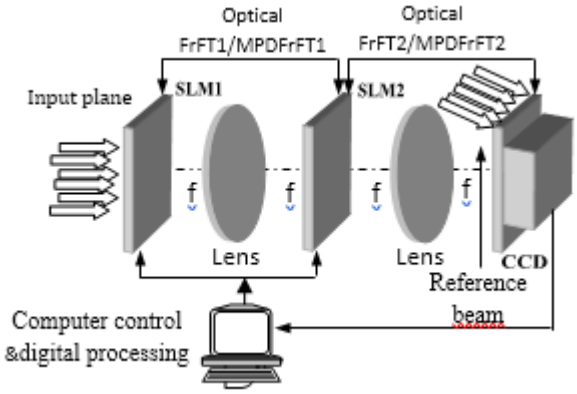


Figure 3. 5 : Implémentation opto-digitale du système proposé à base de DFRFT-DRPE/MPDFRFT-DRPE.

Le pré-cryptage digital proposé, qui combine un schéma de brouillage avec une approche non linéaire récursive et possède une clé secrète constituée des paramètres$\{z_0, \lambda\}$, peut être suivi par l'une des versions existantes de DRPE pour construire une technique de cryptage d'image sécurisée. Cette construction peut efficacement exploiter n'importe lequel des systèmes DRPE bien établis existants sans modification aucune. Le pré-cryptage proposé peut être utilisé à l'entrée du système cryptographique DFRFT-DRPE ou MPDFRFT-DRPE existant. Par conséquent, une implémentation opto-digitale similaire à celle décrite dans [75] peut être suggérée pour le cryptage/décryptage DFRFT-DRPE/MPDFRFT-DRPE proposé comme représenté sur la **figure 3.5**, dans lequel le calculateur est utilisé pour effectuer numériquement

le pré-cryptage non-linéaire récursif proposé ainsi que les permutations par suite chaotique PLCM.

Cette implémentation dispose d'une configuration optique 4-f bien connue pour la mise en œuvre optique de la DFRFT/MPDFRFT, les modulateurs spatiaux de lumière SLM1 (Spatial Light Modulator) et SLM2 sont utilisés pour afficher le signal à valeur complexe pendant les étapes de cryptage/décryptage. La caméra CCD est utilisée pour enregistrer numériquement le signal à valeur complexe en utilisant des techniques d'holographie numérique et un faisceau de référence.

Les schémas des DRPE à base du pré-cryptage proposé qui en résultent diffèrent significativement des versions DRPE basées sur le brouillage non seulement en raison de la propriété de non-linéarité, mais aussi pour la propriété récursive qui assure l'accumulation et la propagation de l'erreur à tous les pixels dans le cas d'une attaque survenue avec une clé erronée. Les **figures 3.6 et 3.7** représentent, respectivement, les systèmes de cryptage et de décryptage d'images opto-digital proposés.

Figure 3. 6: Systéme de cryptage.

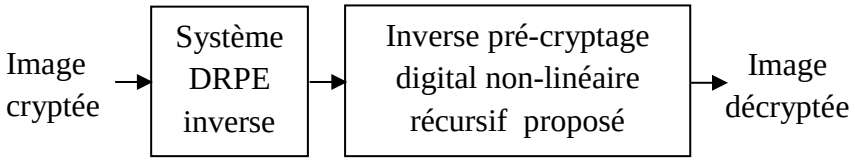


Figure 3.7: Systéme de décryptage.

Le système de décryptage prend les étapes du système de cryptage de manière inverse. Pour la phase de cryptage, l'image d'entrée, qui est généralement une image à l'échelle de gris de huit bits à valeur réelle, est passée à travers deux blocs principaux. Le premier bloc consiste à prétraiter ou pré-crypter numériquement l'image d'entrée pour obtenir une image uniformément distribuée ayant la même taille que l'image d'entrée. Si nous prenons l'image Lena de taille 256 × 256 présentée en **figure 3.8** comme étant image d'entrée, son image pré-cryptée est donnée en **figure 3.9**, qui montre clairement que l'image cryptée a une distribution uniforme.

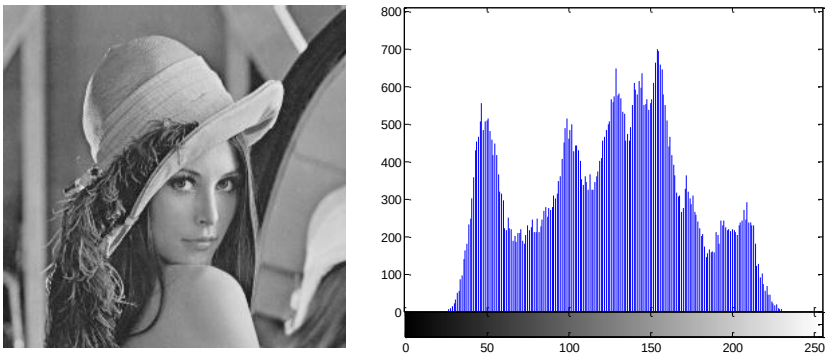


Figure 3. 8: Image d'entrée de Lena et son histogramme.

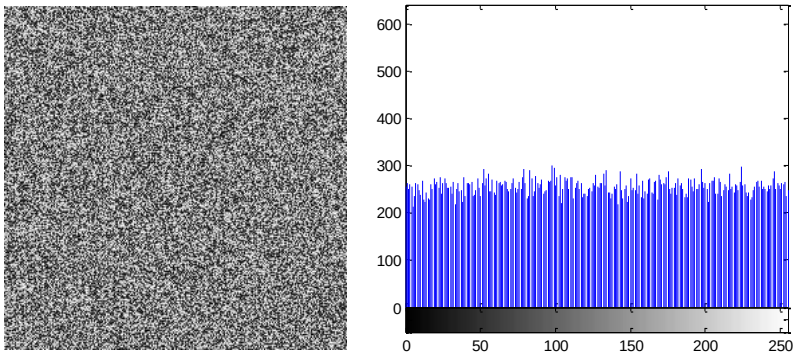
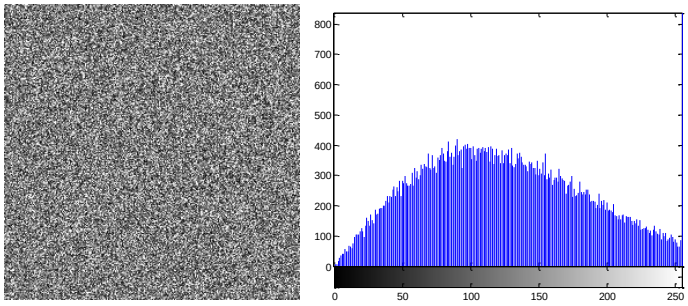
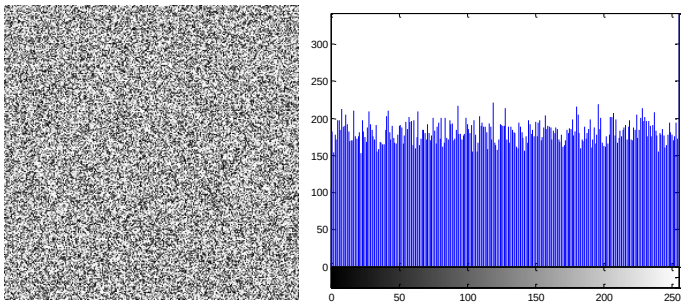


Figure 3. 9: Image pré-cryptée de Lena et son histogramme.

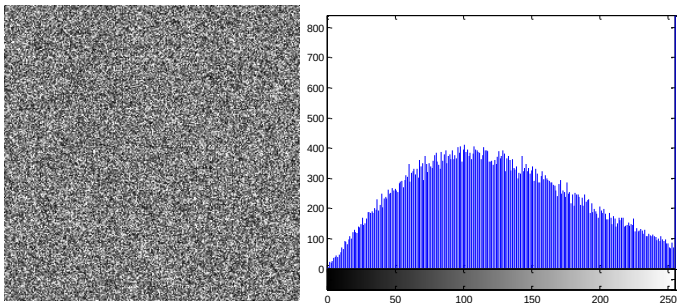


(a)

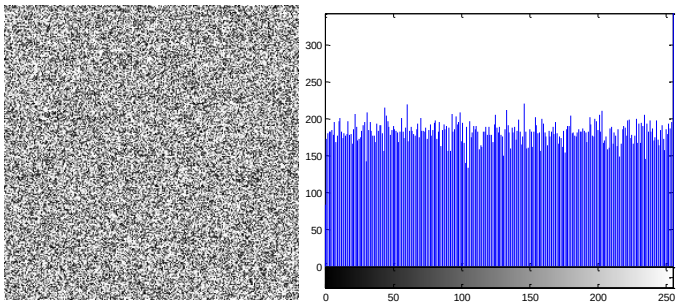


(b)

Figure 3.10: Image cryptée de Lena utilisant le système DFRFT-DRPE à base du pré-cryptage proposé: (a) le module et son histogramme, (b) la phase et son histogramme.



(a)



(b)

Figure 3.11 : Image crypteé de Lena utilisant le système MPDFRFT-DRPE à base du pré-cryptage proposé: (a) le module et son histogramme, (b) la phase et son histogramme.

L'image pré-cryptée est envoyée au second bloc, qui peut être l'un des systèmes DRPE optiques ou opto-digitaux existants, qui donnera l'image cryptée en sortie. Pour le second bloc nous avions deux cas à envisager ou bien le système DFRFT-DRPE, ayant quatre paramètres d'ordre fractionnaire indépendants$\{a, b, c, d\}$, ou bien le système MPDFRFT-DRPE, ayant quatre vecteurs indépendants de taille $1 \times N$ chacun, ayant $\{\bar{a}, \bar{b}, \bar{c}, \bar{d}\}$ paramètres d'ordre fractionnaire indépendants qui peuvent être choisis aléatoirement à partir de l'intervalle [0,2], l'image cryptée est illustrée dans la **figure 3.10** pour le cas d'un système DFRFT-DRPE ou dans la **figure 3.11** s'agissant du cas d'un système MPDFRFT-DRPE.

3.5 Analyse de performances de la technique DRPE proposée

3.5.1 Analyse d'histogrammes

Pour montrer la robustesse de la technique proposée vis-à-vis de l'analyse d'histogramme, prenant trois images différentes de Lena, Barbara et Baboon de taille 256×256, leurs histogrammes sont illustrés sur les **figures 3.8, 3.12 et 3.14**, respectivement, les histogrammes de leurs images cryptées sont présentés aux **figures 3.11, 3.13 et 3.15**, respectivement, Il ressort

de ces figures que même si les histogrammes des images originales sont complètement différents, les histogrammes du module (ou de la phase) des images cryptées correspondantes sont similaires.

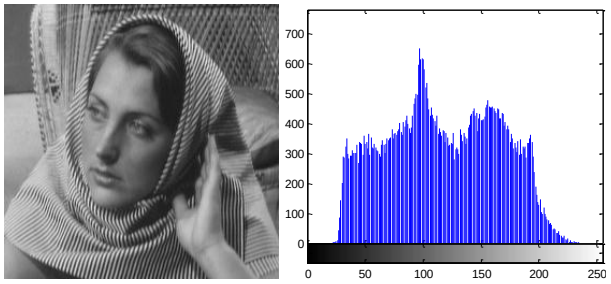
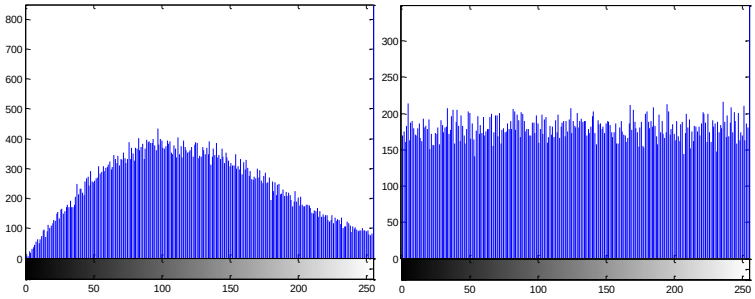


Figure 3.12: Image d'entrée de Barbara et son histogramme.

Les résultats obtenus montrent qu'aucune fuite d'information sur l'image originale ne peut être apprise par un éventuel attaquant à partir d'une analyse d'histogramme d'images cryptées, et par conséquent, nous pouvons conclure que le schéma proposé est robuste par rapport à l'analyse d'histogrammes.



(a) (b)

Figure 3.13 : Histogramme du (a) module et de (b) la phase de l'image crypteé de Barbara utilisant le système MPDFRFT-DRPE à base du pré-cryptage proposé.

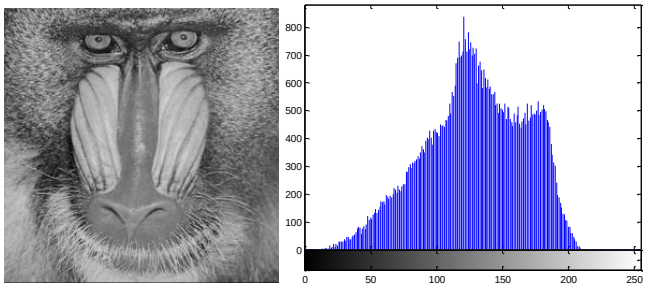
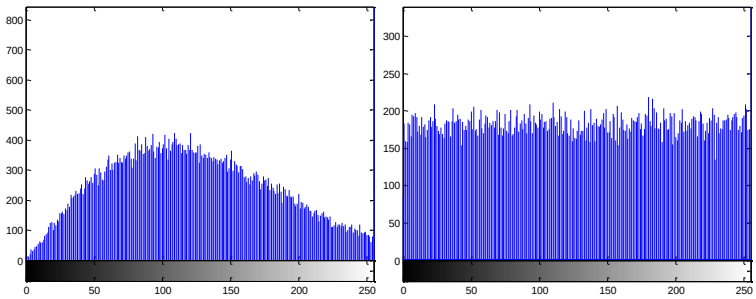


Figure 3.14: Image d'entrée de Baboon et son histogramme.



(a) (b)

Figure 3. 15: Histogramme de (a) Module et de (b) la phase de l'image crypteé de Baboon utilisant le système MPDFRFT-DRPE à base du pré-cryptage proposé.

3.5.2 Resistance au bruit additif

(a) PSNR=10.6764 dB (b) PSNR=10.6730 dB (c) PSNR=10.6918 dB

Figure 3.16 : Résultats d'attaque par bruit Gaussien dans le cas de (a) DFRFT-DRPE à base du pré-cryptage proposé, (b) MPDFRFT-DRPE à base du pré-cryptage proposé, et (c) La technique de [11].

Toute image cryptée peut être corrompue par le bruit pendant la transmission ou le stockage. Pour vérifier la résistance au bruit additif d'une technique de cryptage d'image donnée, on ajoute à l'image de Lena cryptée un bruit gaussien blanc avec une moyenne nulle et un écart type égal à l'unité. Le décryptage de l'image de Lena bruitée résultante est représenté dans la **figure 3.16** pour différentes techniques en termes de PSNR entre les images originales et celles décryptées. En examinant cette figure, nous constatons que les trois techniques ont des performances similaires dans le cas d'une attaque de bruit et que l'image originale peut être obtenue à partir de l'image bruitée décryptée par utilisation de certaines techniques de débruitage connues.

3.5.3 Analyse de l'espace clé

La clé secrète du cryptage est constituée de $\{z_0, \lambda, a, b, RPM_2, c, d\}$ dans le cas du système DFRFT-DRPE proposé et de $\{z_0, \lambda, \bar{a}, \bar{b}, RPM_2, \bar{c}, \bar{d}\}\}$ dans le cas du système MPDFRFT-DRPE proposé. Les clés de décryptage correspondantes sont respectivement $\{z_0', \lambda', a', b', RPM_2', c', d'\}$ et $\{z_0', \lambda', \bar{a}', \bar{b}', RPM_2', \bar{c}', \bar{d}'\}$,. Si $\{z_0' = z_0, \lambda' = \lambda, a' = a, b' = b, RPM_2' = RPM_2, c' = c, d' = d\}$ ou $\{z_0' = z_0, \lambda' = \lambda, \bar{a}' = \bar{a}, \bar{b}' = \bar{b}, RPM_2' = RPM_2, \bar{c}' = \bar{c}, \bar{d}' = \bar{d}\}$, alors l'image décryptée correspondante est exactement l'image originale donnée par la **figure. 3.8**.

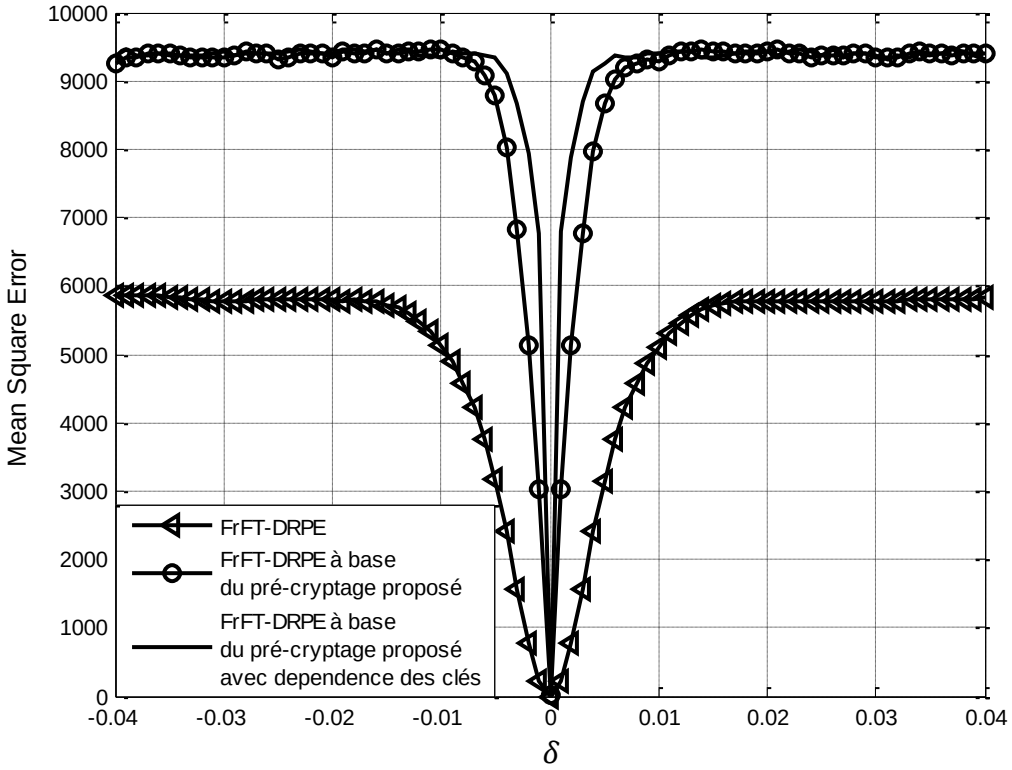


Figure 3.17: MSE en termes de l'erreur de deviation $\boldsymbol{\delta}$ pour le systéme DFRFT-DRPE proposé.

Pour vérifier la sensibilité de la clé du système proposé, l'image cryptée est décryptée en introduisant de petites erreurs dans un ou dans certains paramètres qui constituent la clé secrète. Si la clé de décryptage est définie sur $\{z_0' = z_0 + 10^{-16}, \lambda' = \lambda, a' = a, b' = b, RPM_2' = RPM_2, c' = c, d' = d\}, \{z_0' = z_0, \lambda' = \lambda + 10^{-16}, a' = a, b' = b, RPM_2' = RPM_2, c' = c, d' = d\}$, $\{z_0' = z_0 + 10^{-16}, \lambda' = \lambda, \bar{a}' = \bar{a}, \bar{b}' = \bar{b}, RPM_2' = RPM_2, \bar{c}' = \bar{c}, \bar{d}' = \bar{d}\}$ ou $\{z_0' = z_0, \lambda' = \lambda + 10^{-16}, \bar{a}' = \bar{a}, \bar{b}' = \bar{b}, RPM_2' = RPM_2, \bar{c}' = \bar{c}, \bar{d}' = \bar{d}\}$, l'image décryptée correspondante reste totalement brouillée. Cela montre que le système proposé est très sensible à la clé de pré-cryptage $\{z_0, \lambda\}$. Nous calculons maintenant l'erreur quadratique

moyenne (MSE) entre l'image d'entrée et celle décryptée par le système DFRFT-DRPE basé sur le pré-cryptage proposé en utilisant $\{z_0^{'} = z_0, \lambda^{'} = \lambda, a^{'} = a, b^{'} = b,\ RPM_2^{'} = RPM_2, c^{'} = c + \delta_1, d^{'} = d + \delta_2\}$ où les erreurs δ_1 et δ_2 sont indépendantes et uniformément réparties sur l'intervalle $\{-\delta, \delta\}$. Pour des valeurs différentes de δ, le MSE obtenu par le système proposé est représenté sur la **figure 3.17** et comparé avec le MSE correspondant obtenu en utilisant seulement le système DFRFT-DRPE considéré dans la Référence [8], pour lequel la clé de décryptage employée est :$\{a^{'} = a, b^{'} = b,\ RPM_2^{'} = RPM_2, c^{'} = c + \delta_1, d^{'} = d + \delta_2\}$.

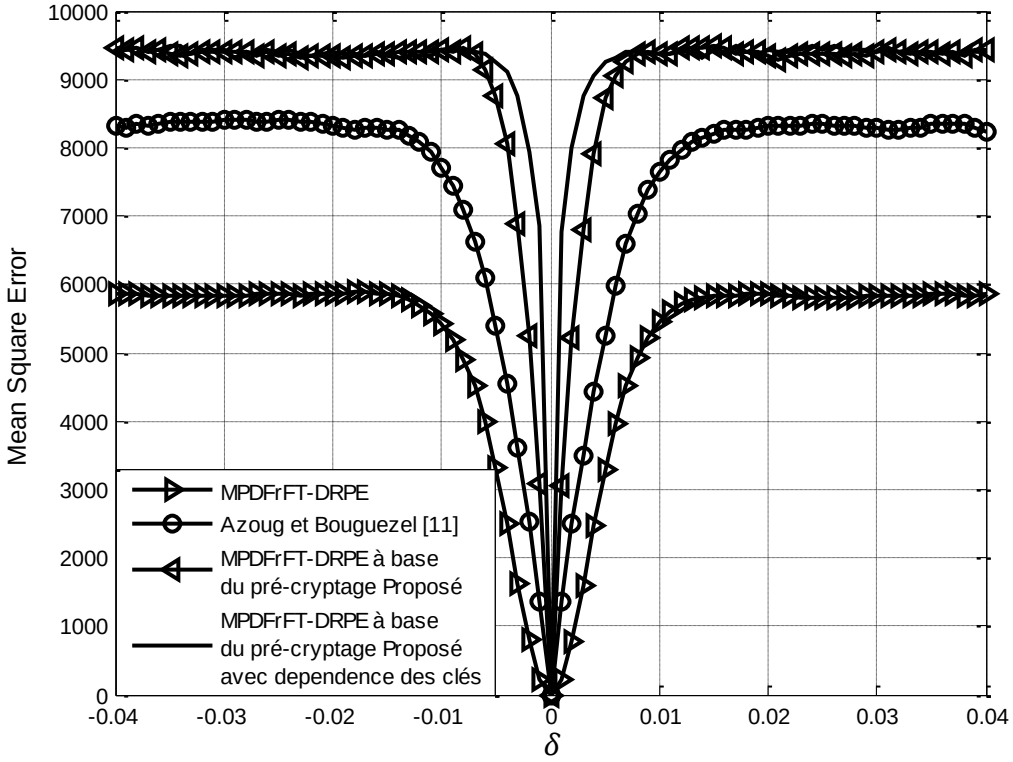


Figure 3.18: MSE en termes de l'erreur de deviation $\boldsymbol{\delta}$ pour le systéme MPDFRFT-DRPE proposé.

Il est clair qu'à partir de cette figure, le système DFRFT-DRPE basé sur le pré-cryptage proposé améliore significativement la sensibilité de la clé du système DFRFT-DRPE. Afin d'améliorer encore la sensibilité de la clé du système DFRFT-DRPE basé sur le pré-cryptage proposé, nous introduisons une dépendance entre les clés de cryptage des premier et second blocs. Par exemple, nous remplaçons z_0 par $z_0 + 0.1a + 0.1c$ dans les clés de cryptage et de décryptage. La courbe MSE résultante est représentée sur la **figure 3.17**, qui montre clairement l'importance de la dépendance introduite. Nous allons maintenant effectuer des simulations sur

le système MPDFRFT-DRPE basé sur le pré-cryptage proposé, similaires à ceux qui sont exécutés sur le système DFRFT-DRPE pré-cryptage proposé. Le MSE obtenu en utilisant $\{z_0' = z_0, \lambda' = \lambda, \bar{a}' = \bar{a}, \bar{b}' = \bar{b}, RPM_2' = RPM_2,\ \bar{c}' = \bar{c} + \bar{\delta}_1, \bar{d}' = \bar{d} + \bar{\delta}_2\}$, où les vecteurs d'erreur $\bar{\delta}_1$ et $\bar{\delta}_2$ sont indépendants et leurs éléments sont également indépendants et uniformément répartis sur l'ensemble {-δ, δ}, est représenté sur la Figure 3.18 et comparé avec le MSE correspondant obtenu en utilisant seulement le système MPDFRFT-DRPE rapporté dans [8], pour lequel la clé de décryptage utilisée est :

$$\{\bar{a}' = \bar{a}, \bar{b}' = \bar{b}, RPM_2' = RPM_2, \qquad \bar{c}' = \bar{c} + \bar{\delta}_1, \bar{d}' = \bar{d} + \bar{\delta}_2\}$$

. Il ressort de cette figure que le système proposé améliore significativement la sensibilité de la clé par rapport au système de la Référence [8]. Nous incluons également dans la figure3.18 le MSE obtenu dans la Référence [11] pour montrer que le pré-cryptage non linéaire récursif proposé conduit à une sensibilité de clé meilleure que celle atteinte par le pré-cryptage non linéaire introduit dans la même référence, qui s'est révélé être meilleur que ceux de tous les autres systèmes basés sur le DRPE. Pour améliorer davantage la sensibilité de la clé du système MPDFRFT-DRPE basé sur le pré-cryptage, nous introduisons une dépendance entre les clés de cryptage des premier et second blocs. Par exemple, nous remplaçons z_0 dans les clés de cryptage et de décryptage par $z_0 + 0.1\bar{a}(N/2) + 0.1\bar{c}(N/2)$ où les $\bar{a}(N/2)$ et $\bar{c}(N/2)$ sont les i^{ème} éléments des vecteurs $\bar{a}$ et $\bar{c}$, respectivement. La courbe MSE résultante est représentée sur la **figure 3.18**, ce qui confirme clairement à nouveau l'importance de la dépendance introduite.

Les **figures 3.17 et 3.18** comparent séparément la sensibilité de la clé des systèmes basés respectivement sur la DFRFT et la MPDFRFT, dans l'intervalle [-0,04, 0,04] de l'erreur de déviation δ. Ceci permet de montrer clairement les améliorations qui peuvent être réalisées par le système proposé aussi bien dans le domaine DFRFT que dans le domaine MPDFRFT. La comparaison entre les DPRE classiques employant ces deux domaines a déjà été effectuée dans [8] qui montre que ce dernier surpasse le premier en termes de sensibilité de la clé. Afin de comparer étroitement ces deux domaines dans le cas du système proposé, nous limitons sur la **figure 3.19** l'intervalle de l'erreur de déviation δ à [-0,01, 0,01], puis décrivons les courbes MSE obtenues par le pré-cryptage proposé basé sur les systèmes DFRFT-DRPE et MPDFRFT-DRPE.

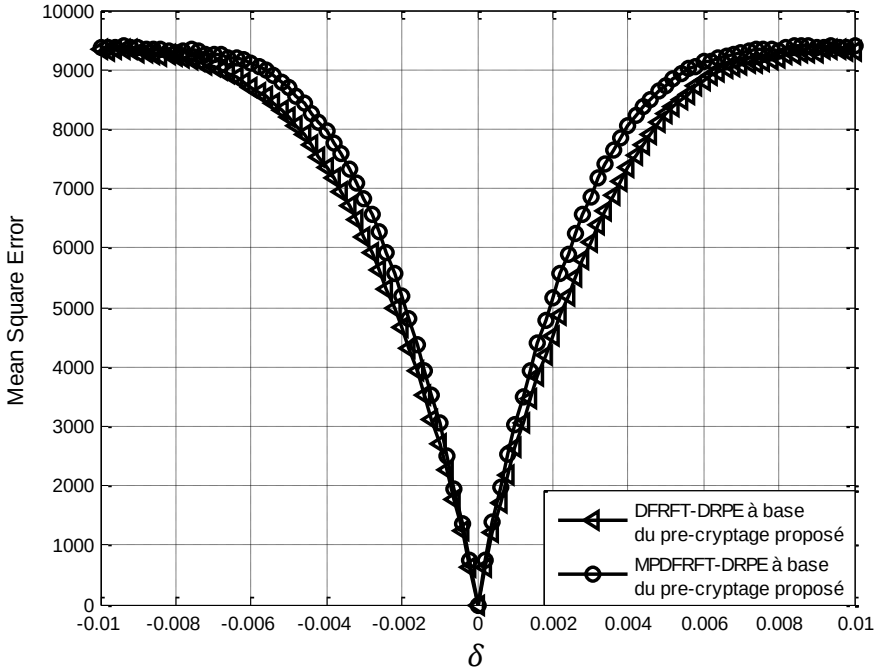


Figure 3.19 : MSE en termes de l'erreur de deviation $\boldsymbol{\delta}$ pour les systémes DFRFT- DRPE et MPDFRFT-DRPE à base du pré-cryptage proposé.

Cette figure, nous permet de constater que le système à base MPDFRFT-DRPE peut atteindre un MSE supérieur à 9000 dans l'intervalle$|\delta| \geq 6 \times 10^{-3}$, est meilleur par rapport au premier pour lequel l'intervalle correspondant est plus petit $|\delta| \geq 8 \times 10^{-3}$. Ceci est principalement dû au fait que le système MPDFRFT possède $4N$ paramètres indépendants, tandis que le système DFRFT n'en a que quatre.

3.5.4 Impact des itérations sur le pré-cryptage non linéaire récursif

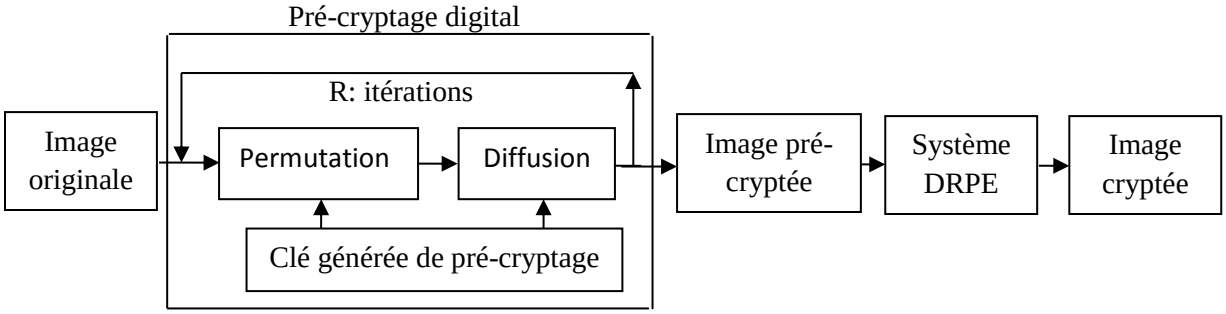


Figure 3.20 : Système de cryptage proposé avec itérations du pré-cryptage digital.

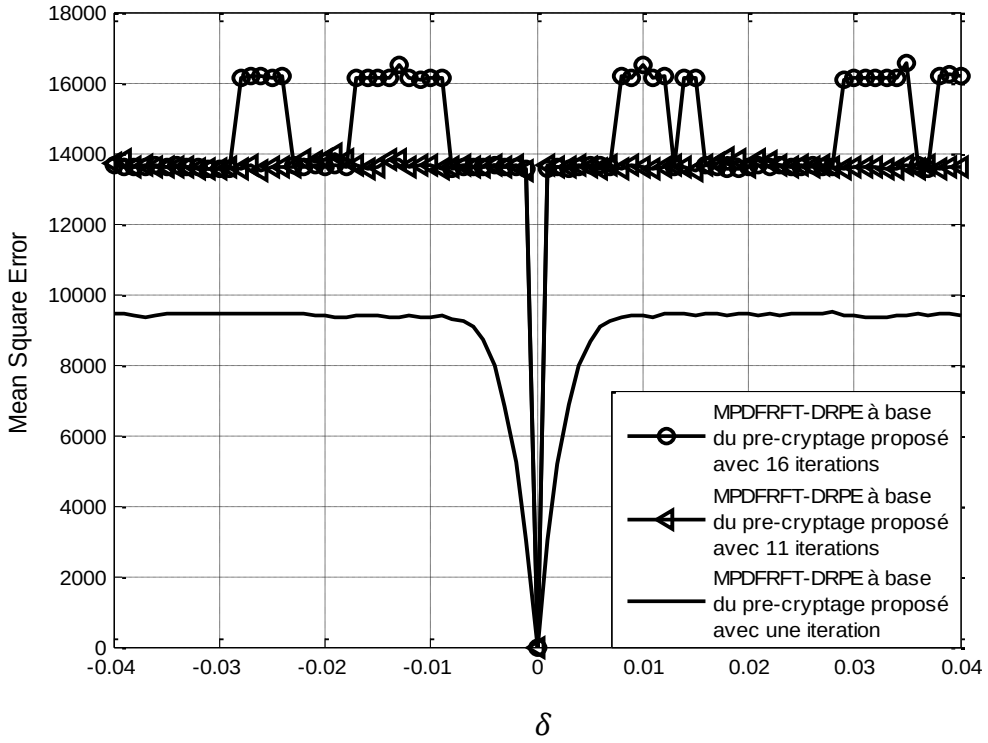


Figure 3.21: MSE en termes de l'erreur de deviation $\boldsymbol{\delta}$ du systéme MPDFRFT-DRPE à base du pré-cryptage proposé pour differents nombre d'iterations.

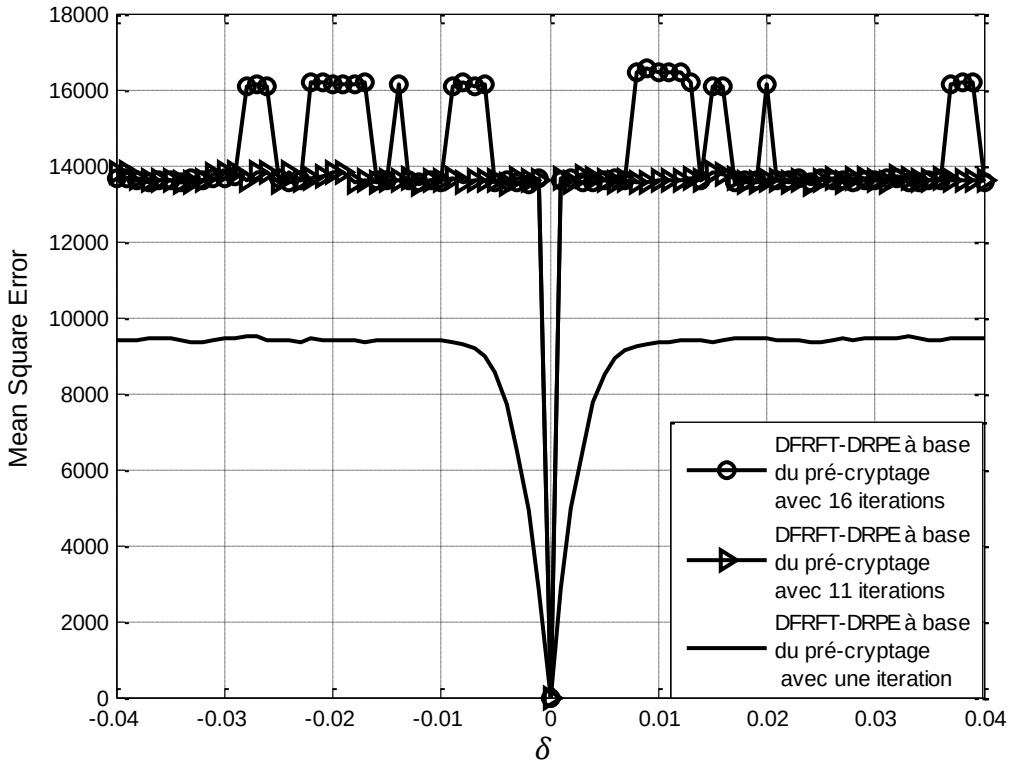


Figure 3. 22: MSE en termes de l'erreur de deviation $\boldsymbol{\delta}$ du systéme DFRFT -DRPE à base du pré-cryptage proposé pour differents nombre d'iterations.

La sensibilité de la clé de la technique de pré-cryptage proposée peut être améliorée de manière significative en répétant le pré-cryptage non linéaire récursif proposé pour un nombre de fois fixe avant d'appliquer le DRPE **figure 3.20**. Les résultats de simulation correspondant aux expériences réalisées à cet effet sont donnés aux **figures 3.21 et 3.22** pour différents nombres de répétitions ou d'itérations. Il est clair à partir de ces figures que, pour les systèmes DFRFT-DRPE et MPDFRFT-DRPE proposés, le MSE peut être augmenté d'environ 9500 pour une itération à environ 13700 pour 11 ou 16 itérations.

3.6 Temps d'exécution

Le temps d'exécution d'un algorithme de cryptage est un facteur crucial en cryptographie car dans la conception de tels algorithmes. Il faut veiller toujours à réaliser le compromis robustesse-rapidité, car plus le processus de cryptage est rapide, plus sa révélation en cryptanalyse est difficile, et comme le système DRPE trouve son application dans le domaine optique qui est caractérisé par sa rapidité en traitement, les schémas de pré-cryptages proposés en vu de l'amélioration de la sensibilité doivent satisfaire ce critère de rapidité. Afin d'évaluer le pré-cryptage proposé de point de vue temps d'exécution les tests sont faits sur trois images test standards de Lena, Barbara et Living-room, sous environnement MATLAB R2014a moyennant un micro-portable personnel ayant un processeur : Intel(R) core™ i3-4005U avec CPU1.70GHZ et RAM 4G, les résultats de test sont récapitulés dans le **tableau 3.4**. Les résultats récapitulés sur ce tableau confirment la rapidité de la méthode proposée dans [11] par rapport à la notre et également par rapport à la méthode proposée dans [79], cela est dû essentiellement à la complexité de l'algorithme de calcul, la méthode de la méthode proposée en [11] est moins complexe par rapport aux deux autres. Ces résultats confirment aussi la nécessité de réaliser toujours le compromis robustesse-rapidité selon l'importance et le degré de sécurité exigés dans le cahier de charge de l'application à sécuriser.

Tableau 3.4 Mesure du temps d'exécution pris par la méthode de pré-cryptage proposé et les méthodes de prétraitements [11] et [79] pour différentes images

	Temps d'exécution en (s)		
Image	**Methode proposée**	**[11]**	**[79]**
Lena 256×256	0.20728	0.158450	0.677074
Barbara 256×256	0.215190	0.192299	0.599814
Living-room 512×512	0.725166	0.608552	2.318195

3.7 Conclusion

Dans ce chapitre, nous avons proposé une nouvelle technique de cryptage d'images en introduisant dans le système DRPE un pré-cryptage digital efficace basé sur une approche non-linéaire récursive. De plus, il est intéressant de noter que ce pré-cryptage peut facilement être incorporé dans les systèmes DRPE optiques ou opto-digitaux existants, sans aucune modification. Pour confirmer la validité de notre approche, nous avons considéré séparément les transformées DFRFT et MPDFRFT. Nous avons également montré que des améliorations peuvent être apportées par la technique proposée en faisant une dépendance entre la clé du pré-cryptage et celle du DRPE et/ou en répétant le pré-cryptage plusieurs fois avant d'appliquer le DRPE. Pour tester les performances de la technique proposée, des simulations ont été réalisées sur différents images de test. Les résultats obtenus confirment que le système DFRFT-DRPE ou MPDFRFT-DRPE proposé est plus performant que les systèmes DRPE existants en termes de sensibilité et espace de la clé.

Dans le chapitre qui suit, nous allons proposer une approche entièrement différente de celle proposée dans ce chapitre par une exploitation adéquate de la symétrie de la transformée de Fourier paramétrique.

Chapitre 4

Proposition d'une nouvelle technique de cryptage en exploitant la symétrie de la transformée de Fourier paramétrique

4.1 Introduction

En littérature, plusieurs techniques de cryptage ont été proposées et peuvent être classées en deux catégories: techniques temporelles (spatiales) et fréquentielles. Les algorithmes de cryptage traditionnels tels que Data Encryption Standard (DES), Advanced Encryption Standard (AES) et Ronald Rivest, Shamir Adi et Adleman Leonard (RSA) [80], où le cryptage est effectué dans le domaine spatial, ne sont pas adaptés au cryptage d'images, car ils nécessitent un grand nombre d'opérations, ce qui augmente sensiblement le temps de calcul. Pour pallier ce problème, des techniques ont été proposées dans [4], [50,51], [81-84], où le cryptage est effectué dans le domaine fréquentiel pour exploiter les algorithmes de calcul rapide des transformées discrètes. Il s'agit du cryptage à double phase aléatoire bien connu basé sur la transformée de Fourier discrète (DFT) [4], [81] et le cryptage à double amplitude aléatoire basé sur la transformée discrète de Hartley [50,51], [82-84]. Pour développer des techniques de cryptage plus robustes et adaptées aux applications des services de communication récents, les transformées paramétriques ont été utilisées pour se servir de leurs paramètres indépendants comme clés secrètes supplémentaires pour le cryptage [85-87], [60,61], [7,8] [5], [35], [63]. Cependant, toutes les techniques DRPE de cryptage d'images existantes sont basées sur des transformées qui souffrent du fait que l'image cryptée résultante est complexe, ce qui nécessite le stockage ou la transmission de deux images (parties réelles et imaginaires).

Dans ce chapitre, nous montrons que le problème ci-dessus peut être résolu efficacement en exploitant la propriété de symétrie de la transformée à valeur complexe considérée et en introduisant une conversion complexe-à-réel (C2R). Cette nouvelle approche est appliquée ici pour développer une méthode de cryptage d'images réel-à-réel [13] basée sur la transformée de Fourier discrète paramétrique rapportée dans [58], qui est une transformée à valeur complexe. La méthode proposée est une technique de cryptage à double amplitude aléatoire couplée à un brouillage chaotique. Elle est conçue pour exploiter les paramètres indépendants des DFT paramétriques en tant que clé secrète supplémentaire pour le cryptage et garantir que l'image cryptée résultante soit réelle. Les suites chaotiques sont utilisées pour renforcer la clé secrète. Le reste du chapitre est organisé comme suit : nous rappelons la propriété de symétrie de la DFT paramétrique et nous passons en revue de ses propriétés, en particulier la propriété de symétrie. Nous élaborons également la conversion C2R dans les cas 1D et 2D et ensuite nous décrivons la méthode de cryptage d'images proposée puis nous présentons les résultats de simulation pour les méthodes de cryptage d'images à double amplitude aléatoire proposées et existantes. Enfin, ce chapitre est achevé par une conclusion.

4.2 Propriété de symétrie

Parmi les propriétés les plus intéressantes de la DFT paramétrique, nous citons la symétrie entre les coefficients dans le domaine fréquentiel. Soit $s(k)$ une séquence à valeur réelle de longueur N. Sa DFT paramétrique $F^{\alpha}(n)$ est une séquence complexe de longueur N ayant la propriété de symétrie donnée par l'**Equation 2.17** :

$$s(k) \overset{\text{DFT}^{\alpha}}{\longleftrightarrow} F^{\alpha}(n) = \left(F^{\alpha}(N-n)\right)^{*}$$

où $(.)^{*}$ désigne le complexe-conjugué. Cette propriété conduit au : $real\left(F^{\alpha}(n)\right) = real\left(F^{\alpha}(N-n)\right)$ et $imag\left(F^{\alpha}(n)\right) = -imag\left(F^{\alpha}(N-n)\right)$. De plus, $F^{\alpha}(0)$ et $F^{\alpha}(N/2)$ sont toujours des valeurs réelles. En examinant la propriété de symétrie de la transformée de Fourier paramétrique d'une séquence réelle, décrite ci-dessus, on peut constater que la première et la seconde moitié de sa partie réelle sont redondantes dans un ordre inversé et d'une façon similaire pour sa partie imaginaire sauf que la redondance est dans un ordre inversé avec un signe opposé. En se basant sur cette propriété de symétrie, nous convertissons la transformée de Fourier paramétrique de sa forme complexe à une forme purement réelle en concaténant les premières moitiés de ses parties réelle et imaginaire. Avec cette nouvelle forme réelle de la transformation, qui est réversible, nous sommes en mesure de traiter seulement la moitié des données par rapport à l'utilisation de la forme complexe. L'analyse mathématique de cette nouvelle forme réelle est encore clarifiée par les deux illustrations données ci-dessous.

Nous étudions d'abord la propriété de symétrie donnée par l'**Equation 2.17** dans le cas unidimensionnel (1D) puis dans le cas bidimensionnel (2D).

4.2.1 Cas unidimensionnel (1D)

Pour éclaircir l'importance de la propriété de symétrie donnée par l'**Equation 2.17**, on considère un vecteur à valeurs réelles

$$\mathbf{s} = [208 \quad 231 \quad 32 \quad 233 \quad 161 \quad 25 \quad 71 \quad 139 \quad 244 \quad 246 \quad 40 \quad 248 \quad 244 \quad 124 \quad 204 \quad 36]$$

de longueur 16. La valeur du paramètre α est choisie dans l'intervalle [-2π, 0] et définie dans cet exemple comme étant $\alpha = -0.4\pi$. Ensuite, la $\text{DFT}^{-0.4\pi}$ transformée du vecteur s, est un vecteur à valeurs complexes $\text{F}^{-0.4\pi}$ qui pourra être exprimé comme suit :

$$\text{F}^{-0.4\pi} = [\ 2486 \quad 95.8 + 134.2\text{i} \quad 62.6 - 245.3\text{i} \quad -262.6 - 118.9\text{i} \quad 510 + 30\text{i}$$

$13.8 - 152.3\text{i} \quad 31.4 - 651.3\text{i} \quad 9 - 231.2\text{i} \quad -78 \quad 9 + 231.2\text{i}$

$31.4 + 651.3\text{i} \quad 13.8 + 152.3\text{i} \quad 510 - 30\text{i} \quad -262.6 + 118.9\text{i}$

$62.6 + 245.3\text{i} \quad 95.8 - 134.2\text{i}].$

On peut facilement vérifier que la relation $F^{-0.4\pi}(n) = \left(F^{-0.4\pi}(16-n)\right)^*$ vaut pour les éléments $F^{-0.4\pi}(n)$, $1 \le n \le 15$,, du vecteur transformé $\mathbf{F}^{-0.4\pi}$. De plus, les éléments $F^{-0.4\pi}(0)$et $F^{-0.4\pi}(8)$ de $\mathbf{F}^{-0.4\pi}$ sont des valeurs réelles pures. Afin d'exploiter efficacement la relation ci-dessus, nous séparons les parties réelle et imaginaire de $\mathbf{F}^{-0.4\pi}$, respectivement, comme$real$

$$real(\mathbf{F}^{-0.4\pi}) = [2486 \;\; 95.8 \;\; 62.6 \;\; -262.6 \;\; 510 \;\; 13.8 \;\; 31.4 \;\; 9$$
$$-78 \;\; 9 \;\; 31.4 \;\; 13.8 \;\; 510 \;\; -262.6 \;\; 62.6 \;\; 95.8 \;]$$

et

$$imag(\mathbf{F}^{-0.4\pi}) = [0 \;\; 134.2 \;\; -245.3 \;\; -118.9 \;\; 30 \;\; -152.3 \;\; -651.3$$
$$-231.2 \;\; 0 \;\; 231.2 \;\; 651.3 \;\; 152.3 \;\; -30 \;\; 118.9 \;\; 245.3 \;\; -134.2]$$

Il est également clair que les relations réelles $real\left(F^{-0.4\pi}(n)\right) = real\left(F^{-0.4\pi}(16-n)\right)$ et $imag\left(F^{-0.4\pi}(n)\right) = -imag\left(F^{-0.4\pi}(16-n)\right)$ sont valables pour les deux parties du vecteur $\mathbf{F}^{-0.4\pi}$, respectivement. Ces deux relations montrent que seulement *N*/2+1=9 entrées, à savoir $real\left(F^{-0.4\pi}(n)\right)$, $n = 0, 1, \ldots, N/2$, de $real(\mathbf{F}^{-0.4\pi})$ et $N/2 - 1 = 7$ entrées, à savoir $\left(F^{-0.4\pi}(n)\right)$, $n = 1, 2, \ldots, N/2 - 1$, de $imag(\mathbf{F}^{-0.4\pi})$ sont suffisants pour représenter le vecteur transformé $\mathbf{F}^{-0.4\pi}$. Cette représentation réduite est appelée conversion complexe-à-réel (C2R) par laquelle un vecteur de la transformée d'une valeur réelle de longueur *N = 16* peut représenter le vecteur de la transformée à valeur complexe $\mathbf{F}^{-0.4\pi}$ qui peut être obtenu comme suit

$$\mathbf{R} = [2486 \;\; 95.8 \;\; 62.6 \;\; -262.6 \;\; 510 \;\; 13.8 \;\; 31.4 \;\; 9 \;\; -78 \;\; 134.2 \;\; -245.3$$
$$-118.9 \;\; 30 \;\; -152.3 \;\; -651.3 \;\; -231.2]$$

La conversion C2R ci-dessus est illustrée graphiquement sur la **figure 4.1**. Maintenant, en appliquant la conversion réelle à complexe (R2C), le vecteur de la transformée à valeur complexe $\mathbf{F}^{-0.4\pi}$peut facilement être obtenu à partir du vecteur transformé réel R en utilisant les relations ci-dessus et le concept correspondant est également illustré graphiquement sur la **figure 4.2.**

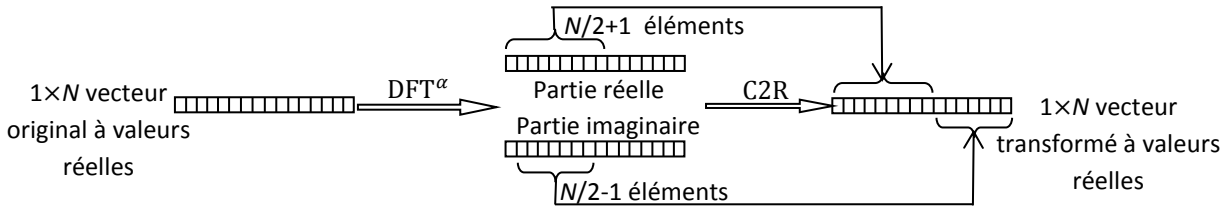


Figure 4.1 : La conversion C2R de DFT$^{\alpha}$ en un vecteur transformé à valeurs réelles.

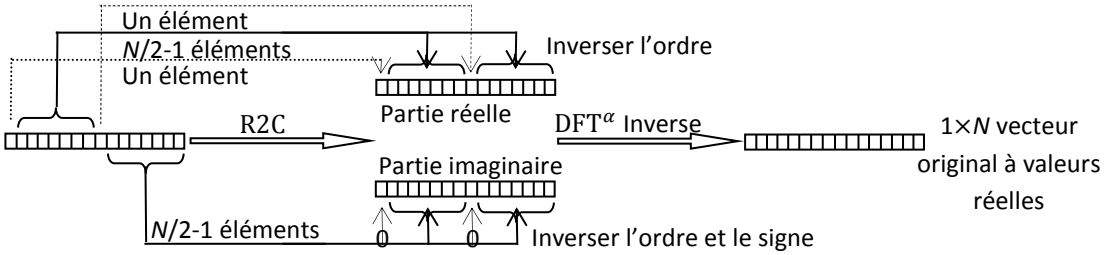


Figure 4.2 : DFT$^{\alpha}$ inverse après conversion C2R du vecteur transformé à valeurs réelles.

4.2.2 Cas bidimensionnel (2D)

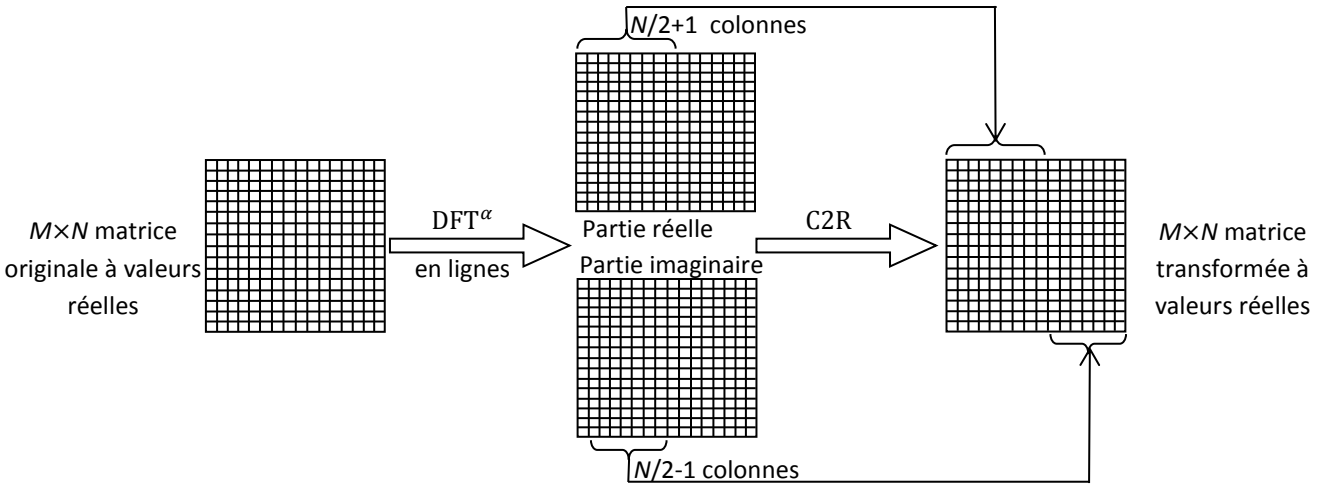


Figure 4. 3: La conversion C2R de la DFT$^{\alpha}$ des lignes de la matrice à valeurs.

L'application de la DFT$^{\alpha}$ pour transformer des séquences 2D ou des matrices peut être réalisée de différentes manières. Afin d'exploiter la propriété de symétrie donnée ci-dessus, dans le cas de matrices à valeurs réelles, nous appliquons la DFT$^{\alpha}$ sur les lignes, puis effectuons sur chaque ligne transformée la conversion C2R discutée dans le cas 1D. Par conséquent, une illustration graphique directe de ce concept est donnée dans la **figure 4.3**, qui montre que la matrice transformée résultante est également évaluée avec la même taille que la matrice d'entrée.

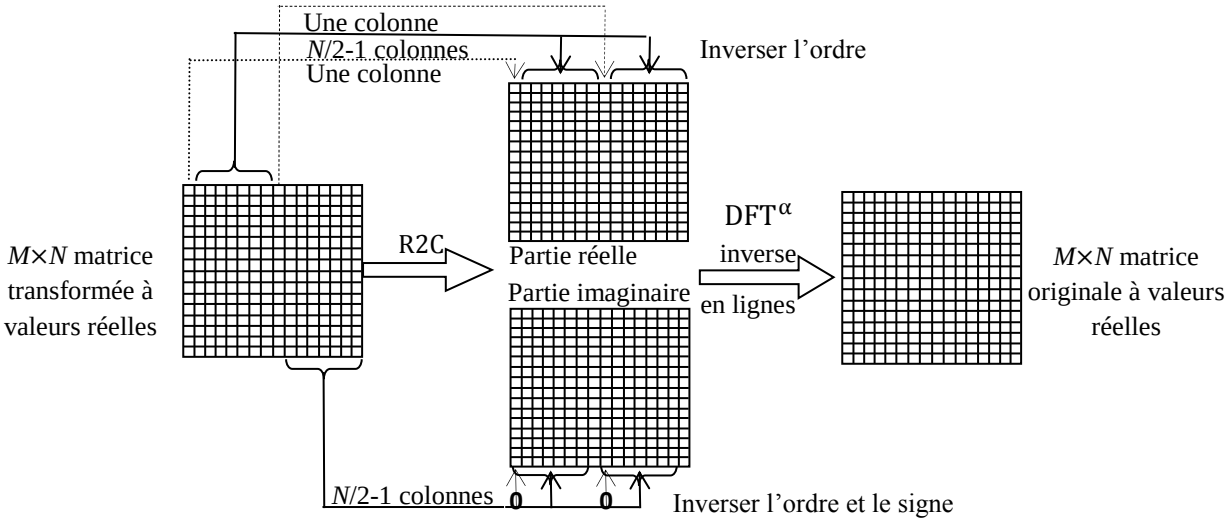


Figure 4. 4: Conversion R2C de la DFT$^{\alpha}$ inverse des colonnes de la matrice transformée à valeurs réelles.

La **figure 4.4** montre graphiquement comment obtenir la matrice d'origine à valeurs réelles à partir de la matrice à valeurs réelles transformée. L'application de la **DFT$^{\alpha}$** sur les colonnes peut être réalisée en transposant seulement la matrice originale et la matrice transformée à valeurs réelles comme indiqué sur les **figures 4.3 et 4.4**.

4.2.3 Illustration de la conversion C2R de la DFT$^{\alpha}$ sur une image en lignes et en colonnes par exploitation de la symétrie

Pour mieux éclaircir notre idée, la **figure 4.5** est une illustration de la conversion C2R de la DFT$^{\alpha}$ appliquée sur une image en lignes et en colonnes par exploitation de la symétrie. Partant d'une image originale I de Barbara **figure 4.5.(*a*),** le résultat de l'application de la DFT$^{\alpha}$ sur les lignes de cette image est une image à valeurs complexes dont la **figure 4.5.(*b*)** représente sa partie réelle et la **figure 4.5.(*c*)** sa partie imaginaire.

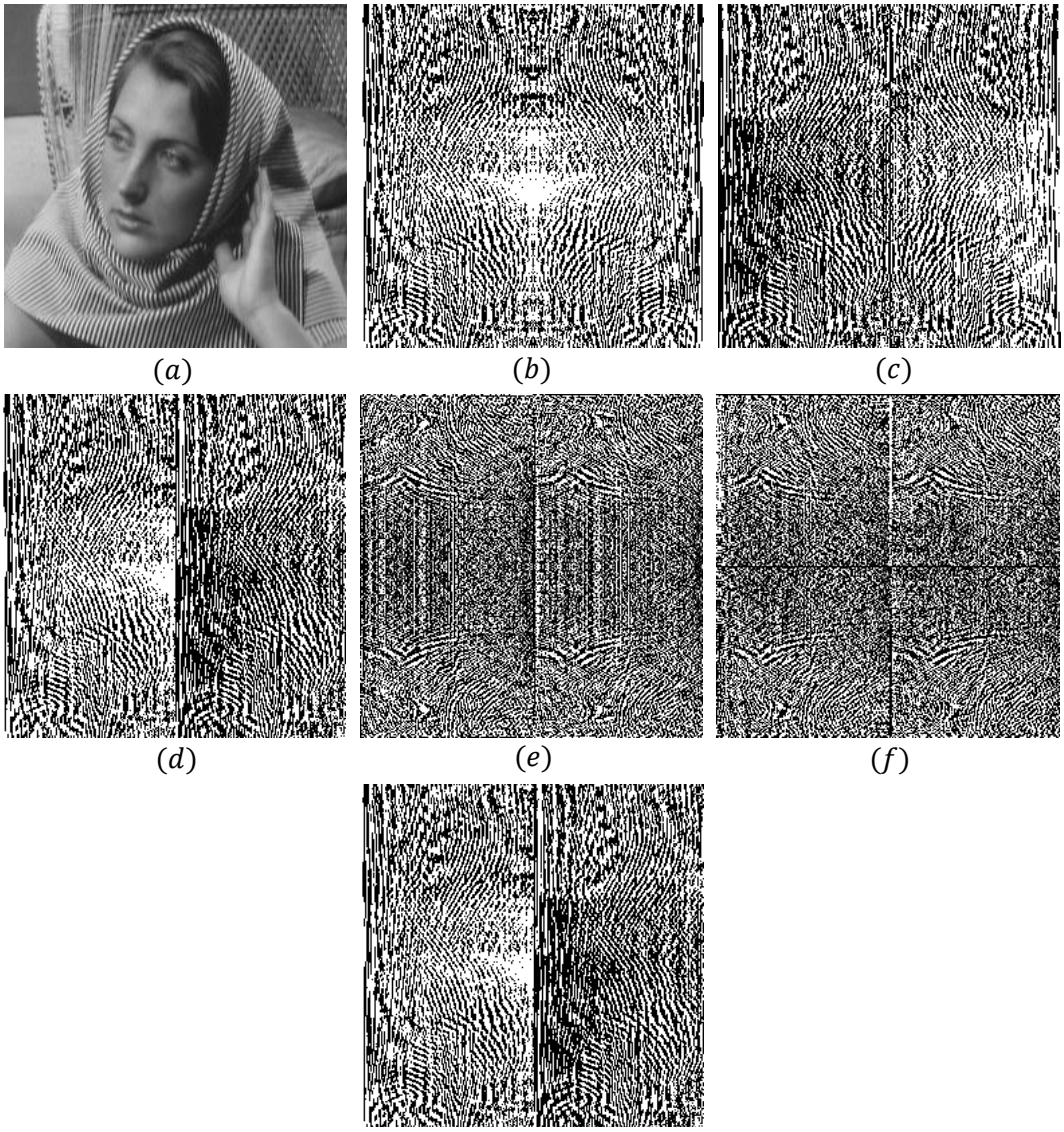


Figure 4.5: Illustration de la conversion C2R de la DFT$^{\alpha}$ sur une image en lignes et en colonnes par exploitation de la symétrie (a) Image originale de Barbara ; DFT$^{\alpha}$ en lignes de l'image originale de Barbara (b) Partie réelle (c) Partie imaginaire; (d) Image résultante de la conversion C2R de la DFT$^{\alpha}$ en lignes; DFT$^{\alpha}$ en colonnes de l'image résultante (e) Partie réelle (f) Partie imaginaire; (g) Image résultante de la conversion C2R de la DFT$^{\alpha}$ en colonnes.

Une conversion C2R à base de la propriété de symétrie est créée par une concaténation adéquate des premières moitiés de ses parties réelle et imaginaire pour donner naissance à une image résultante purement réelle **figure 4.5.(d)**. De façon similaire l'application de la DFT$^{\alpha}$ sur les colonnes de l'image réelle résultante permet d'avoir une image à valeurs complexe dont la **figure 4.5.*(e)*** est sa partie réelle et la **figure 4.5.(f)** est sa partie imaginaire. Enfin l'application de la conversion C2R par le même principe de concaténation donnera une image purement réelle **figure 4.5.*(g)***.

4.3 Technique de cryptage proposée

4.3.1 Schéma de cryptage

Le schéma de cryptage proposé tel que représenté sur la **figure4.6** peut être réalisé à travers les étapes suivantes:

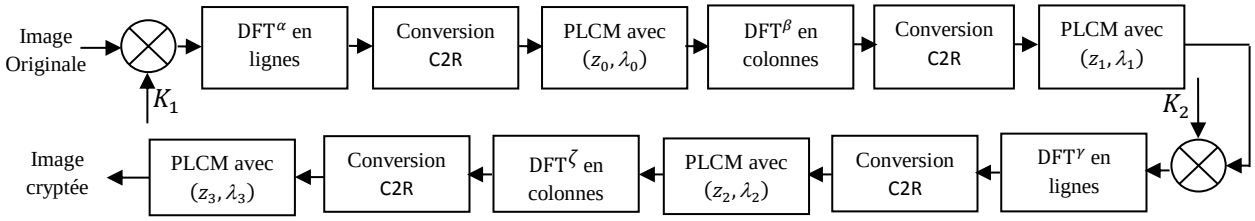


Figure 4.6: Schéma de cryptage proposé.

1) L'image originale, qui est généralement une image à valeurs réelles de taille $M \times N$, est multipliée élément par élément par le premier masque d'intensité aléatoire K_1.
2) Appliquer la DFT$^{\alpha}$ sur les lignes de l'image à valeurs réelles obtenue dans l'étape 1.
3) Appliquer la conversion C2R sur l'image à valeurs complexes obtenue dans l'étape 2.
4) Redimensionner l'image transformée à valeurs réelles obtenue à l'étape 3 en un vecteur et brouiller le résultat en utilisant la première suite chaotique PLCM avec (z_0, λ_0), le vecteur résultant est ensuite redimensionné en une image.
5) Appliquer la DFT$^{\beta}$ sur les colonnes de l'image à valeurs réelles obtenue à l'étape 4.
6) Appliquer la conversion C2R sur l'image à valeurs complexes obtenue à l'étape 5.
7) Redimensionner l'image transformée réelle obtenue à l'étape 6 en un vecteur et brouiller le résultat en utilisant la seconde suite chaotique PLCM avec (z_1, λ_1), le vecteur résultant est ensuite redimensionné en une image.
8) Multiplier l'image à valeur réelle obtenue à l'étape 7 élément par élément par le second masque d'intensité aléatoire K_2.
9) Appliquer la DFT$^{\gamma}$ sur les lignes de l'image à valeur réelle obtenue à l'étape 8.
10) Appliquez la conversion C2R sur l'image à valeurs complexes obtenue à l'étape 9.
11) Redimensionner l'image transformée réelle obtenue à l'étape 10 en un vecteur et brouiller le résultat en utilisant la troisième suite chaotique PLCM avec (z_2, λ_2), le vecteur résultant est ensuite redimensionné en une image.
12) Appliquer la DFT$^{\zeta}$ sur les colonnes de l'image à valeur réelle obtenue à l'étape 11.
13) Appliquer la conversion C2R sur l'image à valeurs complexes obtenue à l'étape 12

14) Redimensionner l'image transformée réelle obtenue à l'étape 13 en un vecteur et brouiller le résultat en utilisant la quatrième suite chaotique PLCM avec (z_3, λ_3), le vecteur résultant est ensuite redimensionné en une image.

15) L'image cryptée est l'image à valeurs réelles obtenue à l'étape 14.

4.3.2 Schéma de décryptage

Le processus de décryptage tel que représenté sur la **figure 4.7** prend exactement les étapes du processus de cryptage de manière inverse pour obtenir l'image décryptée. La clé secrète de cryptage dans le schéma de cryptage proposé est composée des deux masques d'intensité aléatoire K_1 et K_2, les paramètres $\{z_0, \lambda_0\}$, $\{z_1, \lambda_1\}$, $\{z_2, \lambda_2\}$ et $\{z_3, \lambda_3\}$ des quatre suites chaotiques, et les paramètres $(\alpha, \beta, \gamma, \zeta)$ utilisés pour les transformées de Fourier paramétriques.

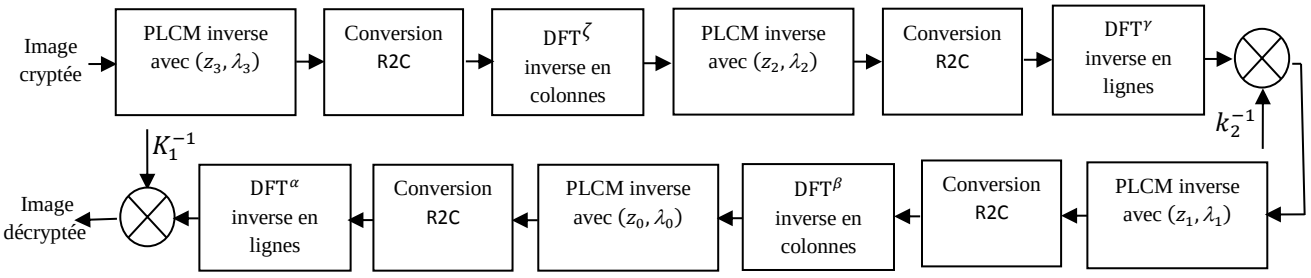


Figure 4. 7: Schéma de décryptage proposé.

Afin de renforcer encore plus la clé secrète, nous introduisons des dépendances entre les paramètres indépendants (α, β, γ, ζ) des transformées de Fourier paramétriques et les paramètres $\{z_0, \lambda_0\}$, $\{z_1, \lambda_1\}$, $\{z_2, \lambda_2\}$ et $\{z_3, \lambda_3\}$ des suites chaotiques. Par exemple, nous remplaçons dans les processus de cryptage et de décryptage les paramètres de condition initiale z_0, z_1, z_2 et z_3 par $z_0 + 0.01\alpha + 0.01\gamma$, $z_1 + 0.01\beta + 0.01\zeta$, $z_2 + 0.01\alpha + 0.01\gamma$, et $z_3 + 0.01\beta + 0.01\zeta$ respectivement.

4.4 Résultats de simulation et comparaison

Afin de démontrer l'efficacité de la méthode de cryptage d'image proposée, nous présentons dans cette partie quelques résultats de simulation en considérant des images de test standard Lena (256×256), Barbara (256×256), et Clown de taille (512×512). Les deux masques d'intensité aléatoire K_1 et K_2 sont générés aléatoirement à partir de l'intervalle] 0,1], les paramètres indépendants $(\alpha, \beta, \gamma, \zeta)$ des transformées de Fourier paramétriques sont choisis aléatoirement dans l'intervalle [-2π, 0].

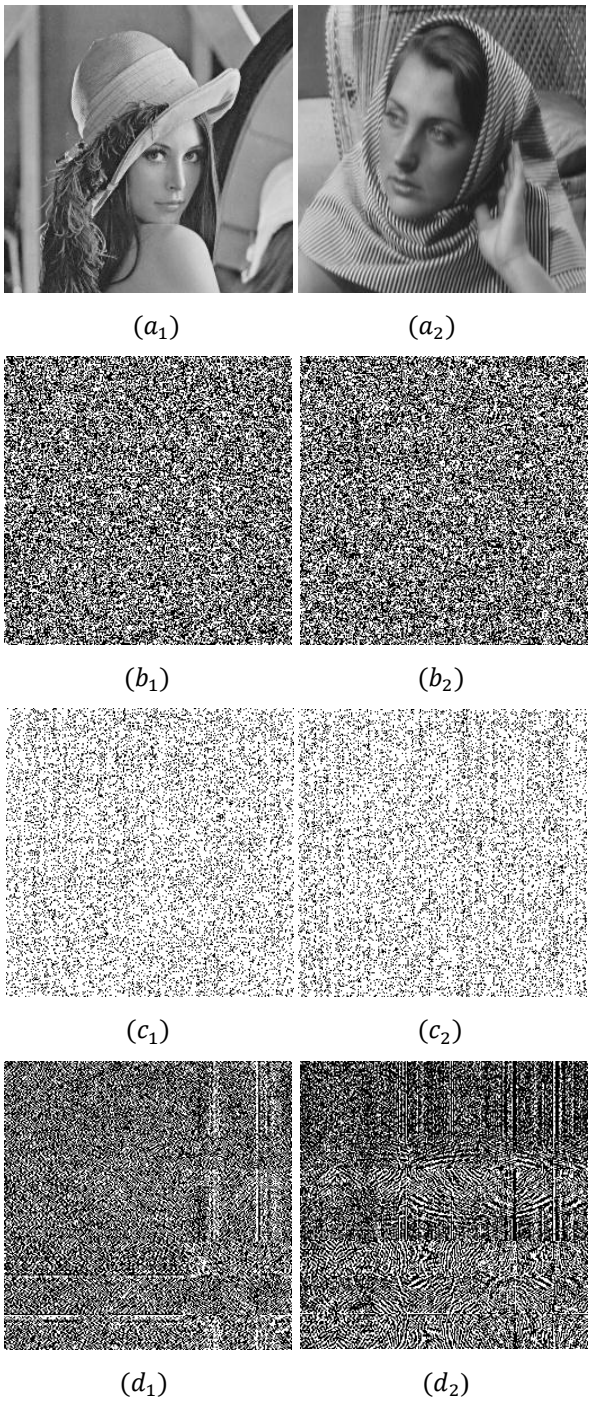


Figure 4.8 : Processus de cryptage : (a_1) et (a_2) images test originales, (b_1) et (b_2) images cryptées correspondantes utilisant la méthode de cryptage proposée, (c_1) et (c_2) images cryptées correspondantes utilisant la transformée de Hartley aléatoire [82], (d_1) et (d_2) images cryptées correspondantes utilisant la deuxième méthode de [51].

Les quatre suites chaotiques PLCM sont présélectionnées comme suit $\{z_0, \lambda_0\} = \{0.1428 + 0.01\alpha + 0.01\gamma, 0.2567\}, \{z_1, \lambda_1\} = \{0.2857 + 0.01\beta + 0.01\zeta, 0.9856\}, \{z_2, \lambda_2\} = \{0.2428 + 0.01\alpha + 0.01\gamma, 0.1567\}$ *et* $\{z_3, \lambda_3\} = \{0.1857 + 0.01\beta + 0.01\zeta, 0.8856\}$.

Les versions cryptées des différentes images de test standard obtenues en utilisant la méthode de cryptage d'image proposée décrite dans la section 3 et la méthode décrite dans la [82], basée sur la transformée de Hartley aléatoire, et la deuxième méthode de [51], qui est basée sur la transformée de Hartley aléatoire, la transformation de jigsaw et la suite logistique sont présentées sur la **figure 4.8**. On peut voir sur cette figure que les images cryptées fournies par les trois méthodes ne contiennent aucune information visuelle des images originales correspondantes.

Concernant l'implémentation des transformations dans les trois méthodes, nous avons adopté les expressions suivantes : $\mathbf{X} = \frac{1}{\sqrt{N}}\mathbf{T} \times \mathbf{x}$ et $\mathbf{x} = \frac{1}{\sqrt{N}}\mathbf{Q} \times \mathbf{X}$, $\mathbf{E} = \frac{1}{N}\mathbf{T} \times \mathbf{I} \times \mathbf{Q}$ et $\mathbf{I} = \frac{1}{N}\mathbf{Q} \times \mathbf{E} \times \mathbf{T}$, où **x** est un vecteur colonne de longueur *N* à transformer, **T** est une matrice de transformation de taille $N \times N$, **Q** est l'hermitienne de **T** lorsque **T** est unitaire (par exemple, transformée de Fourier discrète) et $\mathbf{Q} = \mathbf{T}$ lorsque **T** est involutive (par exemple, transformée de Hartley discrète), et **I** est une image de taille $N \times N$ à transformer en ligne-et en colonne.

Pour l'évaluation, nous utilisons différentes mesures métriques. Le rapport signal sur bruit maximal (PSNR) est utilisé pour mesurer le degré d'endommagement de l'image originale provoqué par l'application de la méthode de cryptage. Le coefficient de corrélation standard est utilisé pour mesurer la similarité entre les images cryptées et les images originales. Nous utilisons également le logarithme de base 10 de l'erreur quadratique moyenne (LMSE) donnée par l'expression mathématique suivante:

$$LMSE = log_{10}\left(\frac{1}{M \times N}\sum_{m=1}^{M}\sum_{n=1}^{N}\left|i_{m,n} - e_{m,n}\right|^2\right) \tag{4.1}$$

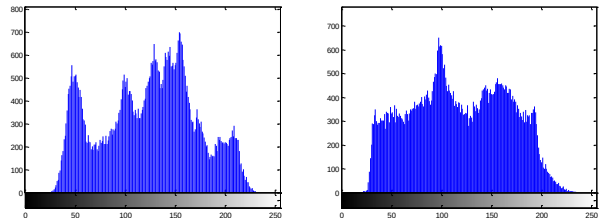
où $i_{m,n}$ et $e_{m,n}$ désignent les valeurs de pixels à la position (*m*, *n*) de l'image originale et cryptée, respectivement, $M \times N$ indique la taille de l'image.

Les résultats obtenus pour le PSNR et le coefficient de corrélation sont résumés dans le **tableau 1** pour différentes méthodes et images de test. Il ressort de ce tableau que la méthode proposée surpasse les méthodes présentées en [82,51] en termes de PSNR et de coefficient de corrélation, tandis que la seconde méthode en [51] fournit un meilleur PSNR.

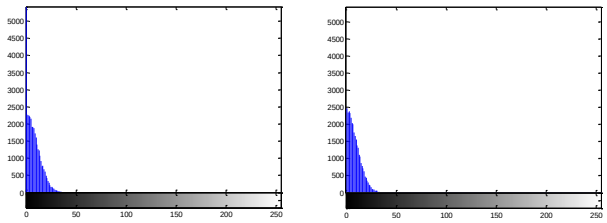
Tableau 4.1 Comparaison des résultats obtenus du PSNR et du coefficient de corrélation entre la méthode proposée et celles de [82] et [51] pour différentes images de test.

Image crypteé	**PSNR, dB**			**Correlation**		
	Methode proposée	**[82]**	**[51]**	**Methode proposée**	**[82]**	**[51]**
Lena 256 × 256	5.6086	7.3581	5.4939	0.0029	0.041	-0.0041
Barbara 256 × 256	6.0188	7.7063	5.9322	-0.0056	-0.0094	0.0057
Clown 512 × 512	6.8340	8.3326	7.683	-0.0031	-0.0068	0.0051

4.4.1 Analyse d'histogramme



(a_1) (a_2)

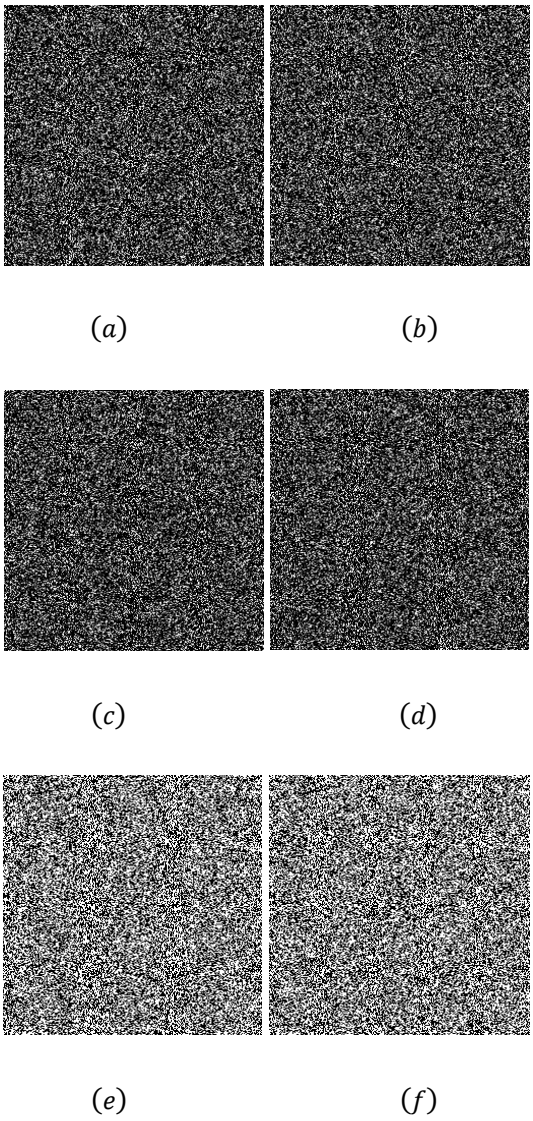


(b_1) (b_2)

Figure 4.9: Histogrammes des images originales de Lena et de Barbara (a_1) et (a_2) respectivement, (b_1) et (b_2) histogrammes de leurs images cryptées utilisant la méthode proposée.

Pour démontrer la robustesse de la méthode de cryptage proposée par rapport à l'analyse d'histogramme, nous cryptons deux images de test standard différentes à savoir de Lena et de Barbara et calculons leurs histogrammes avant et après cryptage. Les résultats sont présentés sur la **figure 4.9**. En effet, nous constatons que même si les histogrammes des images originales sont complètement différents, les histogrammes des images cryptées correspondantes sont très similaires et donc aucune information utile ne peut être extraite des images cryptées. Cela démontre que la méthode proposée est effectivement robuste contre l'analyse d'histogramme.

4.4.2 Sensibilité de la clé de cryptage



(a) (b)

(c) (d)

(e) (f)

Figure 4.10: Image décryptée de Lena avec (a) $z_0' = z_0 + 10^{-16}$; (b) $\lambda_0' = \lambda_0 + 10^{-16}$; (c) $z_1' = z_1 + 10^{-16}$; (d) $\lambda_1' = \lambda_1 + 10^{-16}$; (e) $z_2' = z_2 + 10^{-16}$;(f) $\lambda_2' = \lambda_2 + 10^{-16}$.

Comme mentionné dans la section 4. 3, la clé secrète de cryptage pour le schéma de cryptage proposé est composée des deux masques d'intensité aléatoire K_1 et K_2, les paramètres

$\{z_0, \lambda_0\}$, $\{z_1, \lambda_1\}$, $\{z_2, \lambda_2\}$ et $\{z_3, \lambda_3\}$ des quatre suites chaotiques, et les paramètres $(\alpha, \beta, \gamma, \zeta)$ utilisés pour les transformées de Fourier paramétriques. Afin de vérifier la sensibilité de la méthode de cryptage proposée aux erreurs dans les paramètres des quatre suites chaotiques PLCM, nous supposons corrects, pour le processus de décryptage, tous les paramètres des quatre suites chaotiques PLCM, les deux masques d'intensité aléatoire et les paramètres de La transformée de Fourier discrète paramétrique et un seul des paramètres des quatre suites chaotiques PLCM est légèrement différent de celui utilisé dans le processus de cryptage.

L'image Lena décryptée est présentée dans la **figure 4.10** pour différents cas. Le résultat pour les cas de z_3 et de λ_3 est similaire à ceux indiqués pour z_2 et λ_2, respectivement. Cette figure confirme que l'image décryptée reste totalement cryptée et que la méthode proposée est très sensible à toute petite erreur dans tout paramètre des PLCM.

D'une façon similaire, pour montrer la robustesse de la méthode de cryptage proposée vis-à-vis des attaques par force brute, nous supposons pour le processus de décryptage que tous les paramètres des quatre suites chaotiques PLCM et les deux masques d'intensité aléatoire sont corrects, et seulement quelques paramètres des transformées de Fourier paramétriques sont légèrement différents de ceux utilisés dans le processus de cryptage. L'image Lena décryptée est représentée sur la **figure 4.10** pour différents cas. Cette figure confirme à nouveau que l'image décryptée reste totalement chiffrée et que la méthode proposée est très sensible à toute erreur pour tout paramètre des transformées paramétriques.

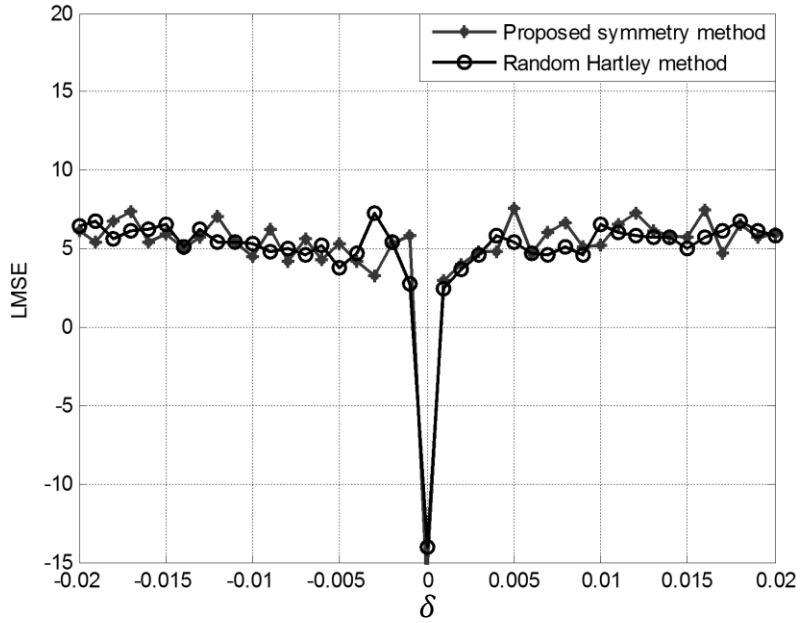


Figure 4.11: LMSE en termes de la déviation d'erreur δ pour K'_1.

Encore plus, pour vérifier la sensibilité de la clé de la méthode proposée aux deux masques d'intensité aléatoire K_1 et K_2, nous considérons que tous les paramètres constituant la clé secrète sont corrects sauf K_1 (ou K_2). Dans ce cas, l'image cryptée est décryptée en introduisant une petite erreur δ_1 (ou δ_2) dans le masque d'intensité aléatoire comme suit $K_1' = K_1 + \delta_1$ (ou $K_2' = K_2 + \delta_2$, où l'erreur δ_1 (ou δ_2) est indépendante et uniformément répartie sur l'ensemble $\{-\delta, \delta\}$. Nous calculons ensuite le LMSE entre les images originales et décryptées. Les LMSE obtenus en termes de la déviation d'erreur δ de la méthode proposée dans [82] sont représentées dans les **figures 4.11 et 4.12** pour le premier et le deuxième masque d'intensité aléatoire, respectivement.

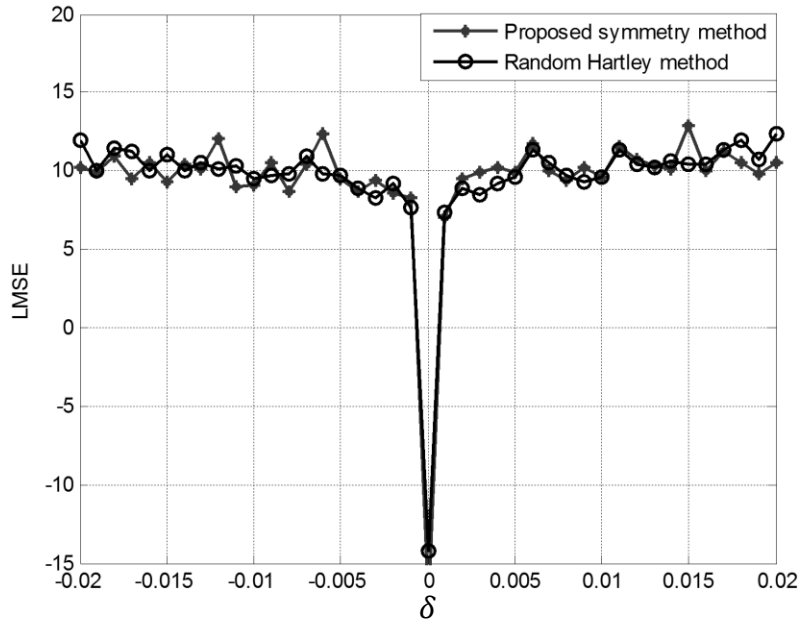


Figure 4.12: LMSE en termes de la déviation d'erreur δ pour K'_2.

Ces figures montrent que les deux méthodes ont des sensibilités similaires aux masques d'intensité aléatoire. Du fait de ce résultat, on ne prend pas en compte l'influence des deux masques d'intensité aléatoire K_1 et K_2. Dans l'analyse suivante, nous considérons que la clé secrète de cryptage est constituée uniquement des paramètres suivants : $\{z_0, \lambda_0, z_1, \lambda_1, z_2, \lambda_2, z_3, \lambda_3, \alpha, \beta, \gamma, \zeta\}$. La clé de décryptage correspondante est : $\{z_0', \lambda_0', z_1', \lambda_1', z_2', \lambda_2', z_3', \lambda_3', \alpha', \beta', \gamma', \zeta'\}, \{z_0' = z_0, \lambda_0' = \lambda_0, z_1' = z_1, \lambda_1' = \lambda_1, z_2' = z_2, \lambda_2' = \lambda_2, z_3' = z_3, \lambda_3' = \lambda_3, \alpha' = \alpha + \delta_1, \beta' = \beta + \delta_2, \gamma' = \gamma, \zeta' = \zeta\}$

Nous calculons maintenant le LMSE entre l'image originale et l'image décryptée en utilisant $\{z_0' = z_0, \lambda_0' = \lambda_0, z_1' = z_1, \lambda_1' = \lambda_1, z_2' = z_2, \lambda_2' = \lambda_2, z_3' = z_3, \lambda_3' = \lambda_3, \alpha' = \alpha + \delta_1, \beta' = \beta + \delta_2, \gamma' = \gamma, \zeta' = \zeta\}$, où les erreurs δ_1 et δ_2 sont indépendantes et uniformément réparties sur l'ensemble $\{-\delta, \delta\}$. Pour différentes valeurs de δ, le LMSE obtenu par la méthode proposée est porté sur la **figure 4.13** et comparé avec le LMSE correspondant obtenu par la

méthode donnée dans [82] pour laquelle la clé de décryptage employée est $\{s_0' = s_0 + \delta,\ s_1' = s_1 + \delta\}$, où s_0 et s_1 sont deux matrices $N \times N$ choisies arbitrairement dans l'intervalle [0 1]. Il ressort de cette figure que la méthode proposée est meilleure que celle proposée dans [82].

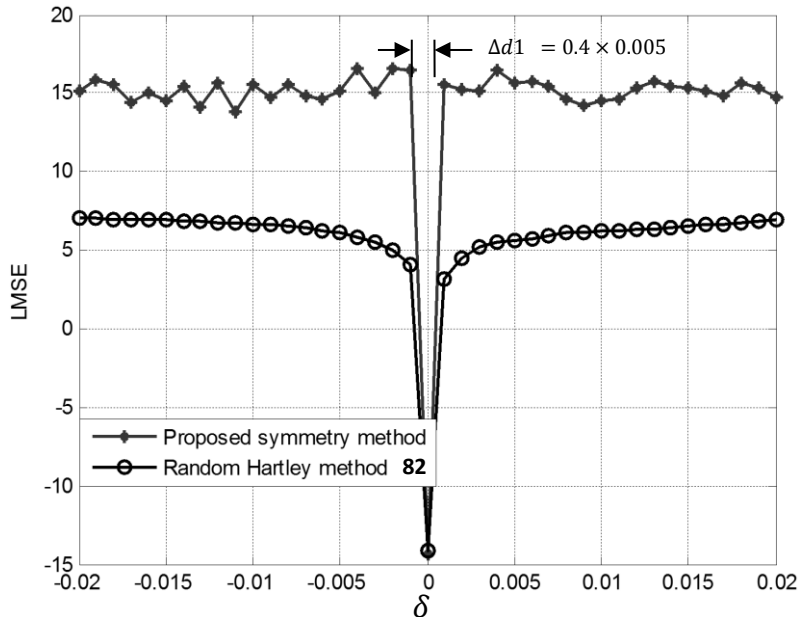


Figure 4.13: LMSE en termes de la déviation d'erreur δ pour α′ et β′ (méthode proposée) et pour s'_0 et s'_1 (méthode [82]).

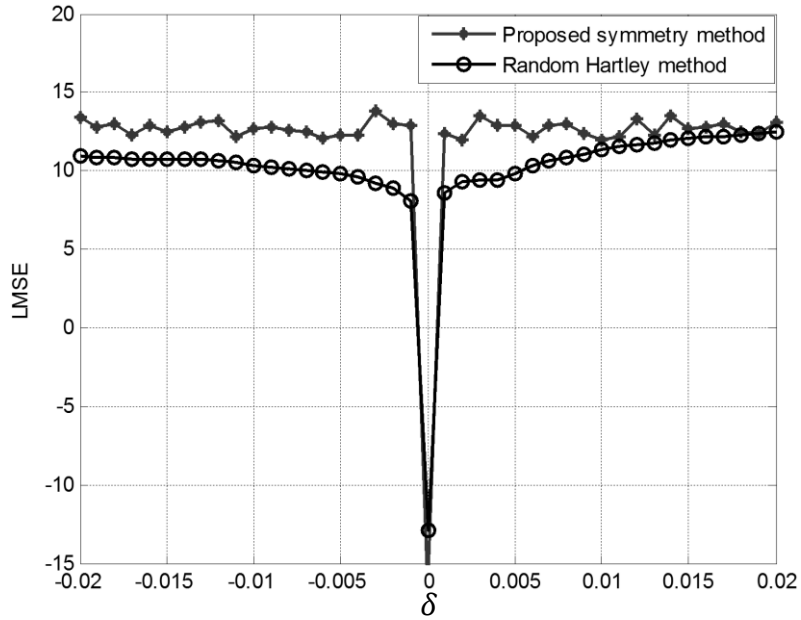


Figure 4.14: LMSE en termes de la déviation d'erreur δ pour γ′ et ζ′ (méthode proposée) et pour s'_2 et s'_3 (méthode de [82]).

Un autre LMSE est illustré sur la **figure 4.14** pour la méthode proposée avec $\{z'_0 = z_0, \lambda'_0 = \lambda_0, z'_1 = z_1, \lambda'_1 = \lambda_1,\ z'_2 = z_2, \lambda'_2 = \lambda_2, z'_3 = z_3, \lambda'_3 = \lambda_3, \alpha' = \alpha, \beta' =$

$\beta, \gamma' = \gamma + \delta_1, \zeta' = \gamma + \delta_2$ }, et pour la méthode dans [82] avec $\{s_2' = s_2 + \delta, s_3' = s_3 + \delta\}$, où s_2 et s_3 sont deux matrices aléatoires $N \times N$ choisies arbitrairement à partir de l'intervalle [0 1]. Cette figure montre également que la méthode proposée est meilleure que celle proposée en [82].

Afin de confirmer davantage l'efficacité de la méthode proposée, nous effectuons une autre comparaison avec la seconde méthode de [51], qui est plus performante que la première méthode de [51], elle est basée sur la transformée de Hartley, la transformation jigsaw et la suite logistique. Pour différentes valeurs de δ, le LMSE obtenu par la méthode proposée en utilisant $\{z_0' = z_0 + \delta,\ z_1' = z_1 + \delta\}$ est représenté sur la **figure 4.15** et comparé à celui obtenu par la méthode décrite dans [51] pour laquelle $\{x_0' = x_0 + \delta,\ \}$, où x_0 est la valeur de départ du masque d'intensité aléatoire chaotique ($CRIM$) généré par la suite logistique. **La figure 4.15** montre clairement la supériorité de la méthode proposée.

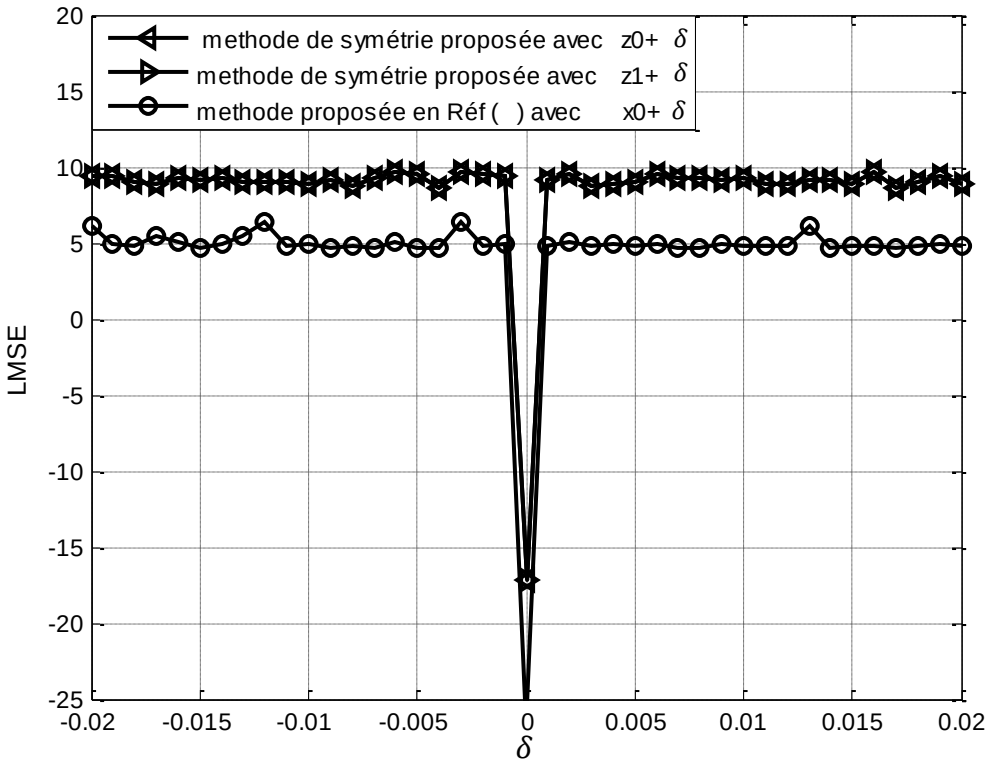


Figure 4.15: LMSE en termes de la déviation d'erreur δ pour z_0 et z_1 (méthode proposée) et pour la valeur de départ x_0 du masque $CRIM$ (méthode de [51]).

4.4.3 Analyse de l'espace clé

Comme mentionné dans la section précédente, la clé secrète de la méthode de cryptage proposée est constituée des paramètres des quatre suites chaotiques PLCM et des quatre paramètres indépendants des transformées de Fourier paramétriques DFT^{α}, DFT^{β} DFT^{γ}et DFT^{ζ},

soit $\{z_0, \lambda_0, z_1, \lambda_1, z_2, \lambda_2, z_3, \lambda_3, \alpha, \beta, \gamma, \zeta\}$. Selon les résultats présentés sur la **figure 4.10**, chacun des paramètres de ces suites chaotiques PLCM a une sensibilité de 10^{-16}, sa précision est donc 10^{+16}. D'autre part, comme le montrent les **figures 4.14 et 4.15**, la précision des paramètres, γ et ζ est évaluée approximativement par : $\frac{1}{\Delta d_1} = \frac{1}{0.4 \times 0.005} \cong 2^8$. Par conséquent, l'espace clé est approximativement égal à $10^{16\times 8} \times 4 \times 2^8 \cong 2^{435}$, ce qui est supérieur à 2^{100} proclamé dans les systèmes cryptographiques [67].

4.5 Conclusion

Dans ce chapitre, nous avons proposé une méthode de cryptage à double random amplitude encoding basée sur la transformée de Fourier discrète paramétrique couplée avec des suites chaotiques. L'idée principale derrière cette méthode est l'introduction d'une conversion complexe à réel en exploitant la propriété de symétrie de la transformée dans le cas des séquences d'entrée à valeurs réelles. Cette conversion permet à l'image cryptée d'être réelle au lieu d'être une image à valeur complexe comme dans toutes les méthodes de cryptage à double random phase encoding existantes. L'avantage est de stocker ou transmettre une seule image au lieu de deux images (parties réelles et imaginaires). Les résultats de la simulation montrent que la méthode proposée surpasse les méthodes existantes de cryptage à double random amplitude encoding en termes de robustesse et sensibilité de la clé secrète.

Conclusion générale et perspectives

Le travail réalisé dans cette thèse consiste à développer et implémenter de nouvelles techniques de cryptage d'images basées sur les transformées discrètes. La recherche bibliographique que nous avons effectuée sur les techniques de cryptage, nous a permis de faire le choix sur la technique de cryptage d'images DRPE bien connue dans le domaine optique. Celle ci s'articule sur la transformée de Fourier discrète et les deux masques de phase aléatoires. Pour élargir l'espace de la clé de cryptage et améliorer sa sensibilité, des modifications sont faites dans ce système en introduisant des transformées paramétriques. Les paramètres indépendants de ces transformées sont utilisés comme étant des clés supplémentaires de cryptage. Le chaos est aussi présent dans ces modifications pour contrôler les permutations chaotiques injectées dans le système DRPE.

Quoique ces modifications semblent attrayantes et intéressantes, mais le système DRPE demeure toujours linéaire, de ce fait, et pour créer la non linéarité dans le système, l'introduction d'un pré-cryptage digital dans le domaine spatial devient une nécessité absolue. Dans ce contexte, que s'inscrit notre première contribution pour remédier à la problématique de linéarité du système DRPE. Cela se fait par l'injection d'un pré-cryptage non linéaire récursif à base de l'opérateur XOR et de permutations chaotiques dans ce système, qui est caractérisé non seulement par sa propriété de non-linéarité, mais aussi par sa propriété de récursivité qui assure l'accumulation et la propagation de l'erreur à tous les pixels dans le cas de toute erreur dans la clé de cryptage.

La seconde problématique relative au système DRPE consiste en la forme complexe de l'image cryptée résultante. Cela nécessite le stockage et la transmission de deux images (parties réelle et imaginaire) au lieu d'une seule. Pour remédier au problème de dédoublement de l'image, nous avons proposé une nouvelle approche en exploitant la propriété de symétrie de la transformée de Fourier paramétrique tout en introduisant une conversion complexe-à-réel, ce qui fait que l'image cryptée résultante soit réelle.

Les deux approches proposées ont été testées en simulation et les tests ont été réalisés en considérant un ensemble d'attaques couramment utilisées en cryptographie. Les résultats obtenus montrent clairement que nos méthodes sont plus performantes que les méthodes issues de la littérature notamment en termes de la sensibilité de la clé de cryptage et de robustesse.

Comme perspectives et du moment que les images cryptées font l'objet de stockage et de transmission, nous envisageons à appliquer des techniques conjointes de compression et de cryptage, qui peuvent constituer un axe de recherche prometteur et attrayant, en injectant dans le système DRPE, la transformée DCT dans le cas d'une compression JPEG, et la transformée DWT dans le cas d'une compression JPEG2000. Dans le cas du cryptage opto-digital, il serait intéressant d'étudier la possibilité d'adjonction au système DRPE des techniques de pré-cryptage non linéaires à base des courbes elliptiques. Cela pourrait améliorer davantage la sensibilité de la clé de cryptage.

Bibliographie

1. B. Schneier, "*Cryptographie appliquée : Algorithme, protocoles et codes sources en C*," Vuibert Informatique, deuxième édition, janvier 2001.
2. B. Furht, E. Muharmagic, and D. Socek, "*Multimedia Encryption and Watermarking*," Springer science & Business Media, 2005.
3. C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, Vol. **28**, no. 4, pp. 656–715, 1949.
4. P. Refregier and B. Javidi, "Optical image encryption based on input plane," *Opt. Lett*., Vol. **20**, pp. 767–769, 1995.
5. G. Unnikrishnan and K. Singh, "Double random fractional Fourier-domain encoding for optical security," *Opt. Eng.*, Vol. **39**, pp. 2853–2859, 2000.
6. S. Bouguezel, M.O. Ahmad, and M.N.S. Swamy, "Image encryption using the reciprocal–orthogonal parametric transform," in: *Proceedings of the IEEE International Symposium on Circuits and Systems*, pp. 2542–2545, 2010.
7. S. Bouguezel, M.O. Ahmad, and M.N.S. Swamy, "A new involutory parametric transform and its application to image encryption," *in: Proceedings of the IEEE International Symposium on Circuits and Systems*, pp. 2605–2608, 2013.
8. S. –C. Pei, and W. Hsue, "The Multiple-Parameter Discrete Fractional Fourier Transform," *IEEE Sig. Process.,* Vol. **13**, pp. 329–332, 2006.
9. W. Qin and X. Peng, "Vulnerability to known-plaintext attack of optical encryption schemes based on two fractional Fourier transform order keys and double random phase keys," *J. Opt. A Pure Appl. Opt.,* Vol. **11**, no. 7, p. 075402, 2009.
10. Y. Zhang, D. Xiao, W. Wen, and H. Liu, "Vulnerability to chosen plaintext attack of a general optical encryption model with the architecture of scrambling then double random phase encoding," *Opt. Lett.*, Vol. **38**, pp. 4506–4509, 2013.
11. S.E. Azoug and S. Bouguezel, "A non-linear preprocessing for opto-digital image encryption using multiple-parameter discrete fractional Fourier transform," *Opt. Commun*., Vol. **359**, pp. 85–94, 2016.
12. T. Bekkouche and S. Bouguezel, "A recursive non-linear pre-encryption for opto-digital double random phase encoding," *Optik*, Vol. **158**, pp. 940–950, 2018.
13. T. Bekkouche and S. Bouguezel, "Digital double random amplitude image encryption method based on the symmetry property of the parametric discrete Fourier transform," *J. electron. Imag.,* Vol. 27, no. 2, pp. 23033–1.23033-9, 2018

14. J. Dumas, J. Roch, E. Tannier, and S. Varrette, "*Théorie des codes-compression, cryptage, correction*," *Dunod*, France, 2007.
15. J.Patarin, "*Quelques éléments d'histoire de la cryptographie*," Conférence à l'Université de Versailles-Saint-Quentin en Yvelines.
16. Abd El-Samie, Fathi E, and al., "*Image encryption : a communication perspective*," CRC press, 2013.
17. B. Wang, and al., " Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps," *Optik,* Vol. **127**, pp. 3541–3545, 2016
18. L. Xu, X. Gou, and J. Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion," *Optics and lasers in engineering*, Vol. **91**, pp. 41-52, 2017.
19. R. Matthews, "On the derivation of a chaotic encryption algorithm," *Cryptologia,* Vol. **13**, pp. 29–42, 1989.
20. J. Fridirich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcat. Chaos,* Vol. **8**, no. 6, pp. 1284–1259, 1998.
21. ZH.Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Phys. Lett A.,* Vol. **346**, pp. 153–157, 2005.
22. GD. Ye, and KW. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map," *Nonlinear Dyn.,* Vol. **69**, no. 4, pp. 2079-2087, 2012.
23. HJ. Liu, and XY. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. Appl.,* Vol. **59**, no. 10, pp 3320-3327, 2010.
24. TG. Gao, and ZQ. Chen, "A new image encryption algorithm based on hyper-chaos," *Phys. Lett A.,* Vol. **372**, no. 4, pp. 394–400, 2008.
25. J. Zhao, S. Wang, Y. Chang, and X. Li, "A novel image encryption scheme based on an improper fractional-order chaotic system," *Nonlinear Dyn.,* Vol. **80**, no. 4, pp. 1721–1729, 2015.
26. YQ. Zhang, and XY. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Appl. Soft. Comput.,* Vol. **26**, pp. 10–20, 2015.
27. YQ. Zhang, and XY. Wang, "A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice," *Inf. Sci.,* Vol. **273**, no. 20, pp. 329-351, 2014.
28. W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Opt. Lasers. Eng.,* Vol. **84**, pp. 26-36, 2016.
29. T. Xiang, and al., "Selective image encryption using a spatiotemporal chaotic system," *Chaos*, Vol. **17**, no. 3, p. 023115, 2007.

30. ZL. Zhu and al., "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Inf. Sci*., Vol. **181**, no. 6, pp. 1171-1186, 2011.
31. S.Tedmori, and N.Al-Najdawi, "Lossless Image Cryptography Algorithm Based On Discrete Cosine Transform," *Inter. Arab. Jour. of Information Technology*, Vol. **9**, no. 5, pp. 471-478, 2012.
32. S.Tedmori, and N.Al-Najdawi., "Image cryptographic algorithm based on the Haar wavelet transform," *Information sciences,* Vol. **269**, pp. 21-34, 2014.
33. G. Situ and J. Zhang, "Double random phase encoding in the Fresnel domain", *Opt. Lett.*, Vol. **29**, pp**.** 1584-1586, 2004.
34. J.A. Rodrigo, T. Alieva, and M.L. Calvo, "Applications of gyrator transform for image processing," *Opt. Commun*., Vol. **278**, pp. 279–284, 2007.
35. S. Bouguezel, "A reciprocal–orthogonal parametric transform and its fast algorithm," *IEEE Signal Process. Lett*., Vol. **19**, pp. 769–772, 2012.
36. Z. Liu, H. Zhao, and S. Liu, "A discrete fractional random transform," *Optics. commun.*, Vol. **255**, pp. 357-365, 2005.
37. Z. Liu, and S. Liu, "Random fractional Fourier transform," *Opt. Lett.*, Vol. **32**, no. 15, pp. 2088-2090, 2007.
38. N. Zhou, and al., "Novel image encryption algorithm based on multiple-parameter discrete fractional random transform," *Optics Commu.,*Vol. **283**, pp. 3037-3042, 2010.
39. B. Javidi and T. Nomura, "Securing information by use of digital holography," *Opt. Lett.*, Vol. **25**, no. 1, pp. 28-30, 2000.
40. Z. Liu, S. Li, W. Liu, and S. Liu, "Opto-digital image encryption by using Baker mapping and 1-D fractional Fourier transform," *Opt. Lasers Eng.,* Vol. **51**, pp. 224–229.2013.
41. H. Chen, J. Zhao, Z. Liu, and X. Du, "Opto-digital spectrum encryption by using Baker mapping and gyrator transform," *Opt. Lasers Eng.,* Vol. **66**, pp. 285–293.2015.
42. N. Singh, and A. Sinha, "Optical image encryption using fractional Fourier transform and chaos," *Opt. Lasers Eng*., Vol. **46**, pp. 117–123, 200
43. B. Hennelly, and J.T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Opt. Lett*., Vol. **28**, pp. 269–271, 2003.
44. S. Liu, and J. T. Sheridan, "Optical encryption by combining image scrambling techniques in fractional Fourier domains," *Opt. Commun*., Vol. **287**, pp. 73–80, 2013
45. J. Lang, R. Tao, and Y. Wang, "Image encryption based on the multiple parameter discrete fractional Fourier transform and chaos function," *Opt. Commun*., Vol. **283**, pp. 2092–2096, 2010.

46. A. Gonzalo, and S. Li, "Some basic cryptographic requirements for chaos based cryptosystems," *Int. J. Bifurcat. Chaos*., Vol. **16**, pp. 2129–2151, 2006
47. S. Li, C. Li, G. Chen, N. G. Bourbakis, and K. T. Lo, "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plain text attacks," *Signal Process. Image Commun.*, Vol. **23**, pp. 212–223, 2008.
48. C. Li, and K.-T. Lo, "Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal. Process*., Vol. **91**, pp. 949–954, 2011.
49. C. Cheng, and M. Chen, "Polarization encoding for optical encryption using twisted nematic liquid crystal spatial light modulators," *Opt. Commun.*, Vol. **237**, pp. 45–52, 2004.
50. L. Chen, and D. Zhao, "Optical image encryption with Hartley transforms", *Optics Letter*, Vol. **31**, no. 23, pp. 3438–3440, 2006.
51. N. Singh and al., "Optical image encryption using Hartley transform and logistic map," *Opt.commun*., Vol. **282**, pp. 1104–1109, 2009.
52. Z. Liu, M. A. Ahmad and S. Liu., "Image encryption based on double random amplitude coding in random Hartley transform domain," *Inter. Journal for Light and Electron Optics.*, Vol. **121**, pp. 959-964, 2008.
53. P. Chanil, and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing,* Vol. **138**, pp. 129-137, 2017.
54. NIST, A statistical test suite for Random and pseudorandom Number Generators for Cryptographic Applications, Technical report, NIST Special Publication 800-22, 2010.
55. H. Liu, and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Optics communications,* Vol. **284**, pp. 3895-3903, 2011.
56. G. Zaibi, "*Sécurisation par dynamiques chaotiques des réseaux locaux sans fil au niveau de la couche MAC,*" *Thèse de doctorat,* Université de Toulouse, 2012.
57. R. C. Gonzalez, and R. E. Woods, "*Digital Image Processing*," *Second edition,* 2002.
58. S. Bouguezel and al., "New Parametric Discrete Fourier and Hartley Transforms, and Algorithms for Fast Computation," *IEEE Trans. on Cir. and Syst.,* Vol. **58**, no.3, pp. 562-575, 2011.
59. M. H. Lee, B. S. Rajan, and J. Y. Park, "A generalized reverse jacket transform," *IEEE Trans. Circuits Syst II. Analog Digital Signal Process.,* Vol. **48**, no.7, pp.648-690, 2001.
60. S. Bouguezel, M. O. Ahmad, and M. N. S. Swamy, "A new class of reciprocal-orthogonal parametric transforms," *IEEE Trans. Circuits Syst I. Reg. Papers.,* Vol.**56**, no. 4, pp. 795-805, 2009.

61. C. C. Tseng, "Eigen values and eigenvectors of generalized DFT, generalized DHT, DCT-IV and DST-IV matrices," *IEEE Trans. Signal Process*., Vol. **50**, no. 4,pp. 866-877,2002.
62. J. Guo, Z. Liu, and S. Liu, "Watermarking based on discrete fractional random transform," *Opt.commun.*, Vol. **272**, no. 2, pp. 344-348, 2007.
63. J. M. Vilardy and al., "Digital images phase encryption using fractional Fourier transform, " *Proc. Conf. Electron. Robot. Automo.Mech, Morelos, Mexico*, pp. 15–18, Sep 2006.
64. V. Namias, "The fractional order Fourier transform and its applications to quantum mechanics," *J. Inst. Math. Appl.*, Vol. **25**, pp. 241-265, 1980.
65. S. –C. Pei, and M-H. Yeh, "Two dimensional discrete fractional Fourier transform," *Signal Process.*, Vol. **67**, pp. 99-108, 1998.
66. S. –C. Pei, and M-H. Yeh, "Improved discrete fractional Fourier transform," *Optics Letters*, Vol. **22**, no. 14, pp. 1047-1049, 1997.
67. G. Alvarez and al., "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcat. Chaos.*, Vol. **16**, no. 8, pp. 2129–2151, 2006.
68. L. Acho, "A discrete-time chaotic oscillator based on the logistic map: A secure communication scheme and a simple experiment using Arduino," *Journal of the Franklin Institute*, Vol. **352**, no. 8, pp. 3113–3121, 2015.
69. Y.Q. Zhang, and X.Y. Wang, "Spatiotemporal chaos in mixed linear–nonlinear coupled logistic map lattice", *Physica A: Statistical Mechanics and its Applications*, Vol. **402**, pp. 04 – 118,2014.
70. A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, Vol. **128**, pp. 155–170, 2016.
71. H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft Comput. J*., Vol. **12**, no. 5, pp. 1457–1466, 1457–1466, 2012.
72. A. Baranovsky, and D. Daems, "Design of one-dimensional chaotic maps with prescribed statistical Properties*," International Journal of Bifurcation and Chaos,* Vol. **5**, no. 6, pp. 1585–1598, 1995 .
73. L. Kocarevand, and S. Lian, "*Chaos-Based Cryptography - Theory, Algorithms and Applications," Springer-Verlag Berlin Heidelberg*, 2011.
74. H. Zhou, and X. Ling, "Generating chaotic secure sequences with desired statistical properties and high security," *Int. J. Bifurc. Chaos*., vol. **7**, pp. 205–213, 1997.
75. S. Liu, C. Guo, and J.T. Sheridan, "A review of optical image encryption techniques, " *Opt. Laser Technol*., Vol. **57**, pp. 327-342, 2014.

76. S. Bouguezel, M.O. Ahmad, and M.N.S. Swamy, "Image encryption using the reciprocal–orthogonal parametric transform," in: *Proceedings of the IEEE International Symposium on Circuits and Systems.*, pp. 2542–2545, 2010.
77. B. Hennelly and J.T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Opt. Lett*., Vol. **28**, pp. 269–71, 2003.
78. X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Opt. Lett*., Vol. **31**, pp. 1044–1046, 2006.
79. A. Beloucif, and O. Noui, "Design of a tweakable image encryption algorithm using chaos-based scheme," *Int. J. Information and security.,* Vol. **8**, no. 3, pp. 205-220, 2016.
80. R.F. Sewell, "Bulk Encryption Algorithm for Use with RSA," *Elec. Lett.,* Vol. **29,** no. 25, pp. 2183-2185, 1993.
81. H. Huang and al., "Colour image encryption based on logistic mapping and double random-phase encoding," *IET Imag. Process.,* Vol. **11,** no. 4, pp. 211-216, 2017.
82. Z. Liu and al., "Image encryption based on double random coding in random Hartley transform domain," *Optik*, Vol. **121**, pp. 959–964, 2010.
83. H. E.Huang, "An optical image cryptosystem based on Hartley transform in the Fresnel transform domain," *Opt. Commun*., Vol. **284**, pp. 3243–3247, 2011.
84. K.K. Kesavan and al., "Optical colour image encryption based on Hartley transform and double random phase encoding system," *3rd Inter. Cong*. On Ultra Modern Telecommunications and control systems and workshops (ICUMT). Budapest, Hungary, pp. 1-3, Oct 2011 .
85. R. Tao and al., "The multiple-parameter discrete fractional Hadamard transform," *Opt. Commun.*, Vol. **282**, pp. 1531–1535, 2009.
86. L. Sui and al., "Double-image encryption using discrete fractional random transform and logistic maps," *Opt. Lasers in Eng*., Vol. **56**, pp. 1–12, 2014.
87. H. Zhou and al., "Problems with the Chaotic Inverse System Encryption Approach," *IEEE Transactions on Circuits and Systems*, Vol. **44**, pp. 268–271, 1997.

ملخّص

في هذه الأطروحة، نقدّم مساهمتين في مجال تشفير الصّور. في أول مساهمة، نقترح تقنية جديدة لتشفير الصّور البصرية الرقمية عن طريق إدخال تشـفير جديد تراجعي غير خطّي .هذا أمر مهم لأن نظام التشـفير المقترح القائم على نظام DRPE يختلف عن إصدارات DRPE القائمة على التخليط، ليس فقط لخاصيته غير الخطيّة، ولكن أيضًا لخاصيته التراجعية التي تضمن تراكم ونشر الخطأ لكل البكسلات في حالة أي خطأ في مفتاح فك التشفير، بالإضافة إلى ذلك، فقد تم تحسين حساسية مفتاح التقنية المقترحة بشـكل ملحوظ مقارنة مع التقنيات القائمة على DRPE . في الإسـهام الثاني، نقترح اسـتخدام التناظر الموجود في تحويل فورييه الوسـيطي، من خلال تطبيقه في مجال تشـفير الصـور الثابتة في المجال التردّدي، تتيح لنا هذه الخاصـية إرسـال صـورة واحدة بدلاً من اثنتين (الجزء الحقيقي والجزء التخيّلي)، ويتم ذلك عن طريق تحويل بسـيط من المركّب إلى الحقيقي(C2R) ، وهذا التّحويل قابل للانعكاس أيضاً. هذا أمر مهم لأن هذا الأسلوب سيقلّل من مساحة التّخزين لـديـنـا ويـقـلـل سـعـة قـنـاة الإرسـال عـنـد نـقـل الـمـعـلـومـات.

الكلمات المفتاحية: تراجعي غير خطي ، إصدارات DRPE، حساسيّة المفتاح، تحويل فورييه الوسيطي، خاصية التّناظر، التّحويل من المركّب إلى الحقيقي.

Abstract

In this thesis, we present two contributions in image encryption domain. In the first contribution, we propose a novel opto-digital image encryption technique by introducing a new recursive non-linear pre-encryption. This is significant because the proposed pre-encryption-based DRPE differs from the existing scrambling-based DRPE versions not only for its non-linearity property, but also for its recursive property that ensures the accumulation and propagation of the error to all pixels in the case of any wrongness in the decryption key. In addition the key sensitivity of the proposed technique is significantly improved compared to that of the existing DRPE-based techniques. In the second contribution, we propose the use of the symmetry that exists in the parametric Fourier transform, by its application in the field of encryption of the fixed images in the frequency domain. This property allows us to send a single image instead of two (real part and imaginary part), this is done by a simple complex to real conversion, which is also reversible. This is significant because this technique reduces the storage space and the capacity of the transmission and significantly increases the robustness compared to the existing techniques.

Keywords: recursive non-linear pre-encryption, DRPE versions, key sensitivity, Parametric Fourier transform, Symmetry property, Complex-to-real conversion.

Résumé

Dans cette thèse, nous présentons deux contributions dans le domaine du cryptage d'images. Dans la première contribution, nous proposons une nouvelle technique de cryptage d'image opto-digitale en introduisant un nouveau pré-cryptage récursif non-linéaire. Ceci est important car la technique proposée diffère des versions DRPE existantes qui sont basées sur le brouillage, non seulement pour sa propriété de non-linéarité, mais aussi pour sa propriété récursive qui assure l'accumulation et la propagation de l'erreur à tous les pixels dans le cas de toute erreur dans la clé de déchiffrement. De plus, la sensibilité de la clé de la technique proposée est significativement améliorée par rapport à celle des techniques existantes à base de DRPE. Dans la deuxième contribution, nous proposons l'exploitation de la symétrie qui existe dans la transformée de Fourier paramétrique, par son application dans le domaine du cryptage des images fixes dans le domaine fréquentiel, cette propriété nous permet d'envoyer une seule image au lieu de deux (partie réelle et partie imaginaire), cela se fait par une simple conversion du complexe au réel (C2R) qui est également réversible. Ceci est important car cette technique réduit l'espace de stockage et la capacité de la transmission et augmente significativement la robustesse par rapport aux méthodes existantes.

Mots clés: pré-cryptage récursif non-linéaire, versions de DRPE, sensibilité de la clé, transformée de Fourier paramétrique, propriété de symétrie, conversion du complexe au réel.