

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE
SCIENTIFIQUE

UNIVERSITE FERHAT ABBAS –SETIF 1-
UFAS (ALGERIE)

MEMOIRE

Présenté à la Faculté de Technologie
Département d'Electronique

Pour l'obtention du Diplôme de

MAGISTER

Option : Communication

Par

M^{elle} : **Meryem BOUCHEMA**

THEME

**Exploitation des transformées paramétriques dans le
cryptage des images fixes**

Soutenu le : 28 / 10 / 2012

devant la commission d'examen :

Mr. A. ZEGADI	Prof à l'université de Sétif 1	Président
Mr. A. KHELLAF	Prof à l'université de Sétif 1	Examineur
Mr. N. AMARDJIA	M.C.C.A à l'université de Sétif 1	Examineur
Mr. S. BOUGUEZEL	M.C.C.A à l'université de Sétif 1	Rapporteur

Remerciements

Au terme de ce travail je tiens à remercier au premier lieu le bon dieu miséricordieux qui m'a éclairé le bon chemin pour m'avoir donné le courage et la volonté à amener ce travail à bon terme.

Mes vifs remerciements sont aussi adressés à mon encadreur Mr. Saad BOUGUEZEL qui m'a proposé le thème de ce mémoire pour ses orientations, ses conseils, ses remarques judicieuses et sa disponibilité, je tiens à lui exprimer ma profonde gratitude en vue du bon déroulement du travail durant l'élaboration de ce mémoire.

Je tiens à exprimer ma parfaite considération aux membres de jury pour avoir accepté de me consacrer une partie de leurs temps, afin d'examiner et de juger ce modeste travail.

Je voudrais remercier tous les enseignants qui ont contribué énormément à ma formation de près ou de loin en particulier les enseignants du département d'électronique.

Enfin je remercie toute personne ayant participé de près ou de loin à l'élaboration de ce travail.

Dédicaces

Je dédie ce modeste travail :

A mes très chers parents, pour leurs assistances, conseils, patience, soutien et sacrifices.

A mes deux grandes mères et à mon grand père, que dieu leurs accordent une saine et longue vie.

A mon très cher frère MOHAMED, et mes chères sœurs : NAFISSA, ASMA et ZEYNEB.

A tous ceux que j'aime et qui m'aiment, mes tantes et mes oncles et ses familles.

Je dédie également ce travail à ma grande famille « BOUCHEMA » et la famille « MESSAOUDI ».

Mes dédicaces vont aussi à ma belle famille « TEBBOUB » en particulier mon fiancé BILAL.

A toutes mes amies de l'université de Jijel et de l'université de Sétif.

A tous ceux qui sont proches de mon cœur et qui m'encouragent à donner le meilleur en moi.

Meryem

Table des matières

Liste des figures.....	viii
Liste des tableaux.....	xi
Liste des abréviations.....	xii
Résumé.....	xiii

Introduction générale.....	1
-----------------------------------	----------

Chapitre 1

Etat de l'art des techniques de cryptage

1.1 Introduction.....	4
1.2 Généralités sur la cryptographie.....	4
1.3 Classification des algorithmes de cryptage.....	6
1.3.1 Classification selon les clés.....	7
1.3.2 Classification selon la technique de cryptage.....	8
1.3.3 Classification selon le pourcentage des données cryptées.....	9
1.3.4 Classification selon le domaine de travail.....	9
1.4 Cryptage d'images basé sur les transformées discrètes.....	10
1.4.1 Cryptage basé sur deux masques de phases aléatoires	10
1.4.2 Cryptage basé sur deux masques d'amplitudes aléatoires	14

1.5	Cryptanalyse	15
1.6	Mesures de performances	16
1.6.1	Le Coefficient de Corrélation.....	16
1.6.2	Rapport signal à bruit en pic.....	17
1.6.3	Histogramme	18
1.7	Conclusion.....	18

Chapitre2

Les transformées paramétriques

2.1	Introduction.....	19
2.2	La transformée réciproque-orthogonale et paramétrique	19
2.2.1	Définition.....	20
2.2.2	Construction de la matrice de la transformée ROP.....	21
2.2.3	Propriétés de la transformée ROP.....	21
2.2.4	Algorithme rapide pour le calcul de la transformée ROP.....	22
2.2.5	Calcul de la complexité.....	24
2.3	Transformée de Fourier discrète paramétrique	26
2.3.1	Définition.....	26
2.3.2	Propriétés de la DFT paramétrique.....	27
2.4	Transformée de Hartley discrète paramétrique	28
2.5	Conclusion.....	29

Chapitre3

Méthodes proposées de cryptage basé sur deux masques de phases aléatoires

3.1	Introduction.....	30
3.2	Principe général de nos méthodes de cryptage d'images	30
3.3	Méthode proposée pour le cryptage d'images dans le domaine de la transformée ROP	33
3.3.1	Développement de la méthode.....	33
3.3.2	Application de la méthode : Résultats de simulation.....	35
3.4	Méthode proposée pour le cryptage d'images dans le domaine de la DFT paramétrique.....	39
3.4.1	Développement de la méthode.....	39
3.4.2	Application de la méthode : Résultats de simulation.....	41
3.5	Conclusion.....	45

Chapitre4

Méthodes proposées de cryptage basé sur deux masques d'amplitudes aléatoires

4.1	Introduction.....	46
4.2	Principe général de nos méthodes de cryptage d'images	46
4.3	Méthode proposée pour le cryptage d'images dans le domaine de la DHT paramétrique.....	48
4.3.1	Développement de la méthode.....	48
4.3.2	Application de la méthode : Résultats de simulation.....	50

4.4 Méthodes proposées pour le cryptage d'images dans le domaine de la transformée ROP à valeurs réelles.....	54
4.4.1 Cas de la transformée ROP à valeurs réelles quelconques.....	54
4.4.1.1 Développement de la méthode.....	54
4.4.1.2 Application de la méthode : Résultats de simulation.....	55
4.4.2 Cas de la transformée ROP à valeurs réelles de l'ensemble $\{\pm 2^m\}$: Méthode de cryptage d'images sans multiplications.....	58
4.5 Conclusion.....	61
Conclusion générale.....	62
Bibliographie.....	64

Liste des figures

Figure 1.1	Principe d'un système cryptographique	5
Figure 1.2	Cryptage asymétrique	7
Figure 1.3	Cryptage symétrique	8
Figure 1.4	Cryptage basé sur deux phases aléatoires dans le domaine de la transformée de Fourier	11
Figure 1.5	Cryptage basé sur deux phases aléatoires dans le domaine de la transformée de Fourier fractionnaire.....	12
Figure 1.6	Cryptage basé sur deux phases aléatoires dans le domaine de la transformée de Fourier fractionnaire de multi-paramètres	12
Figure 1.7	Cryptage basé sur deux phases aléatoires dans le domaine de la transformée ROP	13
Figure 1.8	Cryptage basé sur deux masque d'amplitudes aléatoires dans le domaine de la transformée de Hartley	14
Figure 1.9	Cryptage basé sur deux masque d'amplitudes aléatoires dans le domaine de la transformée de Hartley aléatoire	15
Figure 2.1	Le papillon paramétrique (P-B) pour le calcul de la transformée ROP.....	24
Figure 2.2	Structure de l'algorithme de la transformée ROP.....	25
Figure 3.1	Images de test utilisées dans la simulation	32
Figure 3.2	Histogrammes correspondants aux images de test utilisées	33
Figure 3.3	Cryptage par bloc proposé basé sur deux phases aléatoires et la transformée ROP	34
Figure 3.4	Image de test Lena cryptée en utilisant des tailles de bloc différentes	35

Figure 3.5	Image de test Goldhill cryptée en utilisant des tailles de bloc différentes	36
Figure 3.6	Images décryptées en utilisant des paramètres incorrects pour des tailles de bloc différentes	36
Figure 3.7	Histogramme de Lena cryptée par des blocs d'ordre 64	38
Figure 3.8	Image de test Lena décryptée par des blocs d'ordre 64 avec des paramètres incorrects.....	39
Figure 3.9	Cryptage proposé en utilisant la DFT paramétrique	40
Figure 3.10	Image de Lena cryptée en utilisant des tailles de bloc différentes.....	42
Figure 3.11	Image de Goldhill cryptée en utilisant des tailles de bloc différentes.....	42
Figure 3.12	Images décryptées en utilisant des paramètres incorrects pour des tailles de bloc différentes.....	43
Figure 3.13	Histogramme de Lena cryptée par des blocs d'ordre 64.....	44
Figure 3.14	Image de Lena décryptée par des blocs d'ordre 64 avec des paramètres incorrects.....	45
Figure 4.1	Processus de cryptage d'image par bloc proposé en utilisant deux masques d'amplitudes aléatoires et des transformées paramétriques à valeurs réelles	47
Figure 4.2	Processus de cryptage d'image par bloc proposé en utilisant deux masques d'amplitudes aléatoires dans le domaine de la DHT paramétrique	49
Figure 4.3	Images cryptées par des tailles de bloc différentes	50
Figure 4.4	Images décryptées en utilisant des paramètres incorrects pour des tailles de bloc différentes	51
Figure 4.5	Histogrammes des images cryptées en utilisant des blocs d'ordre 32.....	53
Figure 4.6	Image de test Lena décryptée par des blocs d'ordre 32 avec des paramètres incorrects.....	54

Figure 4.7	Processus de cryptage d'image par bloc proposé en utilisant deux masques d'amplitudes aléatoires dans le domaine de la transformée ROP à valeurs réelles	55
Figure 4.8	Images cryptées par tailles de bloc différentes	56
Figure 4.9	Images décryptées en utilisant des paramètres incorrects pour des tailles de bloc différentes	56
Figure 4.10	Histogrammes d'image cryptée par des blocs d'ordre 32	57
Figure 4.11	Image de Lena décryptée par des blocs d'ordre 32 avec des paramètres incorrects.....	58
Figure 4.12	Images cryptées par tailles de bloc différentes	59
Figure 4.13	Images décryptées en utilisant des paramètres incorrects pour des tailles de bloc différentes	59
Figure 4.14	Histogrammes d'image cryptée par des blocs d'ordre 32	60
Figure 4.15	Image de Lena décryptée par des blocs d'ordre 64	61

Liste des tableaux

Tableau 2.1	Complexité arithmétique de différentes transformées réelles	26
Tableau 3.1	Nombre de paramètres correspondant à la taille du bloc	35
Tableau 3.2	Evaluation objective en termes de PSNR des images de test décryptées	37
Tableau 3.3	Evaluation objective en termes de coefficient de corrélation des parties réelles et imaginaires des images de test cryptées	38
Tableau 3.4	Nombre de paramètres correspondant à la taille du bloc	41
Tableau 3.5	Evaluation objective en termes de PSNR des images de test décryptées	43
Tableau 3.6	Evaluation objective en termes de coefficient de corrélation des parties réelles et imaginaires des images de test cryptées	44
Tableau 4.1	Nombre de paramètres correspondant à la taille du bloc	51
Tableau 4.2	Evaluation objective en termes de PSNR des images de test décryptées	52
Tableau 4.3	Evaluation objective en termes de coefficient de corrélation des images de test cryptées	52
Tableau 4.4	Evaluation objective en termes de PSNR des images de test décryptées	57
Tableau 4.5	Evaluation objective en termes de coefficient de corrélation des images de test cryptées pour la transformée	57
Tableau 4.6	Evaluation objective en termes de PSNR des images de test décryptées	60
Tableau 4.7	Evaluation objective en termes de coefficient de corrélation des images de test cryptées pour la transformée	60

Liste des abréviations

AES	A dvanced E ncryption S tandard
DCT	D iscrete C osine T ransform
DES	D ata E ncryption S tandard
DFT	D iscrete F ourier T ransform
DHT	D iscrete H artley T ransform
EQM	E rreur Q uadratique M oyenne
FFT	F ast F ourier T ransform
FrFT	F ractional F ourier T ransform
GSM	G roupe S pécial M obile
MIT	M assachusetts I nstitute of T echnology
MPDFrFT	M ultiple- P arameters D iscrete F ractional F ourier T ransform
P-B	P arametric B utterfly
PSNR	P eak S ignal to N oise R atio
ROP	R eciprocal- O rthogonal P arametric
RSA	Au nom de Ronald R ivest, Adi S hamir et Leonard A dleman
WHT	W alsh- H adamard T ransform

Résumé

Ce travail considère le cryptage des images fixes en exploitant les transformées paramétriques récemment développées dans la littérature. Le mémoire présente tout d'abord une étude bibliographique sur les techniques de cryptage d'images et un état de l'art des transformées paramétriques et leurs méthodes de développement et de constructions. Cette étude nous a permis de développer deux catégories de nouvelles méthodes de cryptage d'images fixes en adoptant la technique de traitement par bloc. La première catégorie est dédiée essentiellement à l'exploitation efficace des transformées paramétriques à valeurs complexes, notamment la transformée réciproque orthogonal et paramétrique (ROP) et la transformée de Fourier discrète (DFT) paramétrique. Par contre, la deuxième catégorie est appropriée pour des transformées paramétriques à valeurs réelles, particulièrement la transformée de Hartley discrète (DHT) paramétrique et la transformée ROP pour le cas des paramètres à valeurs réelles quelconques et le cas des paramètres qui sont des puissances de deux. Les résultats expérimentaux d'analyse de la sécurité, spécifiquement l'analyse d'histogramme, les mesures objectives effectuées sur les images cryptées et décryptées et l'attaque par force brute, obtenus dans ce travail montrent clairement l'efficacité et la robustesse des méthodes proposées dans ce mémoire. En plus, ces méthodes proposées présentent un avantage de complexité réduite par rapport à celles des méthodes de cryptage d'images existantes.

Mots clés : Techniques de cryptage, Cryptage des images fixes, Transformées paramétriques.

Introduction Générale



Introduction générale

Les réseaux de communication numériques sont largement utilisés pour l'échange des informations comme texte, audio, image, vidéo etc. La sécurité de ces informations échangées est devenue une nécessité primordiale dans beaucoup d'applications des organismes civils ou militaires, citons par exemple, l'internet, la téléphonie mobile, les distributeurs de billets, les abonnements aux chaînes de télévision payantes, le commerce électronique et les cartes à puce, afin d'assurer la confidentialité et d'empêcher toute modification ou exploitation non autorisée des données. L'une des méthodes connues pour la réalisation efficace de cet objectif est le cryptage qui rend l'information complètement ou partiellement illisible et incompréhensible. En effet, la cryptographie est l'un des moyens technologiques utilisés pour fournir la sécurité et l'authenticité aux données transmises sur des systèmes de communications.

Plusieurs techniques de cryptage ont été développées pour résoudre le problème de sécurité. Elles peuvent être classifiées de différentes manières. On distingue généralement deux types de systèmes cryptographiques selon les types de clés: le cryptage asymétrique et le cryptage symétrique. Dans les systèmes asymétriques, les clés de cryptage et de décryptage sont différentes, par contre, les systèmes de cryptage symétriques utilisent les mêmes clés pour le cryptage et le décryptage. Ces derniers se répartissent en crypto-systèmes par flots qui traitent l'information bit à bit et en crypto-systèmes par blocs qui divisent l'information en blocs.

Il existe dans la littérature des techniques de cryptage temporelles/spatiales et fréquentielles. Les algorithmes traditionnels de cryptage tels que le DES (Data Encryption Standard), AES (Advanced Encryption Standard) et le RSA (Ronald Rivest, Adi Shamir et Leonard Adleman), où le cryptage se fait dans le domaine spatial [1]-[3], sont

généralement appropriés pour les signaux unidimensionnels. Cependant, ces algorithmes de cryptage ne sont pas adéquats pour le cryptage d'images, en raison de leurs caractéristiques intrinsèques. En outre, ces algorithmes exigent un grand nombre d'opérations ce qui nécessite un temps de calcul très long. Pour fournir une meilleure solution au problème de la sécurité des images, des techniques de cryptage d'images ont été proposées dans [4]-[10], où le cryptage se fait dans le domaine fréquentiel. Les techniques fréquentielles qui sont appropriées pour l'exploitation des transformées à valeurs complexes utilisent deux masques de phases aléatoires comme une clé secrète de cryptage, alors que les autres qui sont appropriées pour l'exploitation des transformées à valeurs réelles utilisent deux masques d'amplitudes aléatoires comme une clé secrète de cryptage. Une catégorie de ces techniques est celle qui exploite les transformées discrètes fixes comme la transformée de Fourier discrète (discrete Fourier transform : DFT) en utilisant deux masques de phases aléatoires [4] et la transformée de Hartley discrète (discrete Hartley transform : DHT) en utilisant deux masques d'amplitudes aléatoires [8], [10]. Afin de renforcer la clé de cryptage et de concevoir des techniques de cryptage plus robustes que celles basées sur les transformées fixes, des techniques ont été proposées pour le cryptage d'images en exploitant les paramètres indépendants des transformées fractionnaires comme une clé secrète supplémentaire de cryptage [5], [6]. Cependant, ces transformées fractionnaires souffrent de ses complexités de calculs prohibitives. Par conséquent, elles ne sont pas attractives pour le cryptage d'images dédié aux applications en temps réel. Récemment, une technique de cryptage d'images plus efficace que celles basées sur les transformées fractionnaires a été proposée dans [11]. L'efficacité de cette technique est due essentiellement à l'exploitation de la transformée réciproque orthogonale et paramétrique (ROP) présentée dans [12] qui possède des propriétés très intéressantes, telles que la complexité réduite et le nombre élevé de paramètres indépendants.

Afin de renforcer davantage la clé de cryptage et de développer des techniques de cryptage des images fixes plus robustes et plus rapides que celles mentionnées précédemment, nous adoptons dans ce travail le cryptage par bloc tout en exploitant les transformées paramétriques récemment proposées dans la littérature qui ont des complexités réduites, telles que la transformée ROP [12], la DFT paramétrique [13] et la

DHT paramétrique [13]. Ce mémoire est composé de quatre chapitres. Le premier chapitre présente des notions générales sur la cryptographie et une étude bibliographique des différentes techniques de cryptage, en particulier les techniques basées sur les transformées discrètes. Le deuxième chapitre est consacré à une description détaillée des transformées discrètes paramétriques qui sont exploitées dans les chapitres suivants. Nous proposons dans le chapitre 3 une catégorie de nouvelles techniques de cryptages des images fixes en exploitant les transformées paramétriques à valeurs complexes présentées dans le chapitre 2. Les versions réelles de ces transformées sont exploitées dans le chapitre 4 pour concevoir une autre catégorie de nouvelles techniques de cryptage des images fixes. Afin de tester la robustesse des méthodes proposées, des expériences d'analyse de la sécurité, spécifiquement l'analyse d'histogramme, les mesures objectives effectuées sur les images cryptées et décryptées et l'attaque par force brute, sont réalisées dans les deux chapitres 3 et 4.

Chapitre 1

Etat de l'art des techniques de cryptage



1.1 Introduction

Avec le développement des réseaux de communication comme Internet et les réseaux de la téléphonie mobile, le besoin d'assurer la confidentialité et l'authenticité des informations échangées a connu une croissance considérable dans ces dernières années. Ces informations sont de différentes formes : texte, audio, image, vidéo etc. Les images peuvent être considérées comme l'une des formes de l'information les plus utilisées. Il y a une variété importante des méthodes de dissimulation de l'information. Ces méthodes disposent de différentes caractéristiques et peuvent être classifiées selon leurs objectifs et leurs contraintes, elles peuvent être groupées en deux grandes familles, une famille utilise des techniques pour désordonner le message et le rendre illisible : le brouillage (scrambling) et une autre famille utilise des techniques pour rendre le message incompréhensible : la cryptographie.

Le cryptage des images et des vidéos a beaucoup d'applications dans divers domaines, tel que la communication mobile, Internet, l'imagerie médicale, la télémédecine et les communications militaires. Il existe un nombre très important de techniques de cryptage d'images. Dans ce chapitre, nous allons présenter des généralités sur la cryptographie, le principe d'un système cryptographique, les différentes techniques cryptographiques, ainsi que le cryptage d'images basé sur les transformées discrètes. Ce dernier type de cryptage fait l'objet de notre étude, particulièrement le cryptage basé sur deux masques de phases aléatoires et celui basé sur deux masques d'amplitudes aléatoires.

1.2 Généralités sur la cryptographie

Le cryptage ou chiffrement (encryption) peut être défini comme une fonction réversible de transformation des données en envisageant la protection d'information contre toute prise de connaissance du contenu (confidentialité) ou modification induite (intégrité). Le décryptage ou déchiffrement (decryption) est l'opération inverse du cryptage, il a pour but de récupérer l'information masquée [14]-[16].

Le message à crypter est également appelé texte en clair (plaintext) et le résultat du cryptage d'un texte en clair est appelé texte crypté (ciphertext). Le texte en clair est noté P , qui peut être une suite de bits, un fichier de texte, un enregistrement de voix numérisé, ou

une image numérique. Du point de vue de l'ordinateur, P n'est rien d'autre que de l'information binaire. Le texte en clair peut être transmis ou stocké [14].

Le texte crypté est noté C , c'est aussi de l'information binaire, parfois de la même taille que P et parfois plus grande. La fonction de cryptage, notée E_{K_e} , transforme P en C comme suit [14],[16]-[17]

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

où K_e est la clé de cryptage. La fonction de décryptage, notée D_{K_d} , transforme C en P comme suit

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

où K_d est la clé de décryptage. La sécurité d'un système cryptographique ne doit pas reposer sur la clé de décryptage. La figure 1.1 présente un schéma block d'un tel système cryptographique.

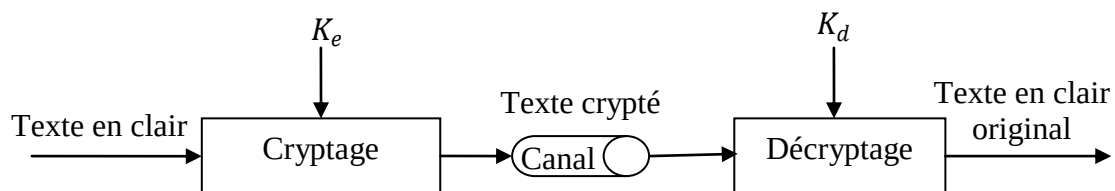


Figure 1.1 : Principe d'un système cryptographique [14]

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], [16]

- ✎ La confidentialité des données.
- ✎ L'intégrité des données.
- ✎ L'authentification des données et des communicants.
- ✎ La non-répudiation des données.

La confidentialité permet de protéger les informations contre tout accès non autorisé. Une partie indésirable de communication, appelée ennemi ne doit pas accéder au

matériel de communication. Ceci nécessite une identification précise du destinataire, et une méthodologie permettant de rendre inutilisable l'information à tout autre qu'à ce destinataire. Cet objectif de la cryptographie est une base qui a toujours été traitée et exécutée dans toute l'histoire de la pratique cryptographique.

L'intégrité des données garantit que les informations n'ont pas été manipulées de manière non autorisée. Si l'information est modifiée pendant son passage dans le réseau, toutes les parties communicantes peuvent détecter cette modification.

L'authentification permet d'assurer que les données reçues et envoyées proviennent bien des entités déclarées. Les méthodes d'authentification sont étudiées en deux groupes ; l'authentification de l'entité et l'authentification des messages. L'authentification d'entité est le processus par lequel une partie est assurée de l'identité d'une deuxième partie impliquée dans un protocole, et que le second a effectivement participé immédiatement avant le moment où la preuve est acquise. L'authentification des messages est un terme utilisé par analogie avec l'authentification d'origine des données. Il assure l'authentification d'origine des données par rapport à la source du message d'origine et l'intégrité des données.

La non répudiation consiste à éviter que, par la suite, les communicants nient leurs actions : l'émetteur nie avoir envoyé un message et le récepteur nie avoir reçu un message.

Heureusement, la cryptographie moderne a développé des techniques pour traiter tous les quatre buts de la cryptographie.

1.2 Classification des algorithmes de cryptage

Les systèmes cryptographiques peuvent être classés selon les types de clés : symétrique ou asymétrique, selon les techniques de cryptage : par bloc ou par flot, selon le pourcentage des données cryptées : total ou partiel ou selon le domaine de travail : temporel/spatial ou fréquentiel.

1.3.1 Classification selon les clés

Selon les clés, on distingue généralement deux types d'algorithmes : Les algorithmes de cryptage symétriques ou à clé privée et Les algorithmes de cryptage asymétriques ou à clé publique [14], [17].

Le cryptage à clé publique a été proposé par Diffie et Hellman en 1976 [18] (le début de la cryptologie moderne). Dans un tel schéma, la clé de cryptage K_e est différente de celle de décryptage K_d pour lesquels aucun canal secret supplémentaire et nécessaire pour le transfert de la clé. N'importe qui peut utiliser la clé de cryptage, ou clé publique, pour crypter un message, mais seul celui qui possède la clé de décryptage, ou clé privée, peut décrypter le message crypté résultant, la Figure 1.2 présente le schéma bloc d'un tel système de cryptage asymétrique. Le premier système de cryptage à clé publique a été proposé en 1978 par R. Rivest, A. Shamir et L. Adleman, trois chercheurs du MIT, qui ont donné leur nom au système baptisé RSA [17].

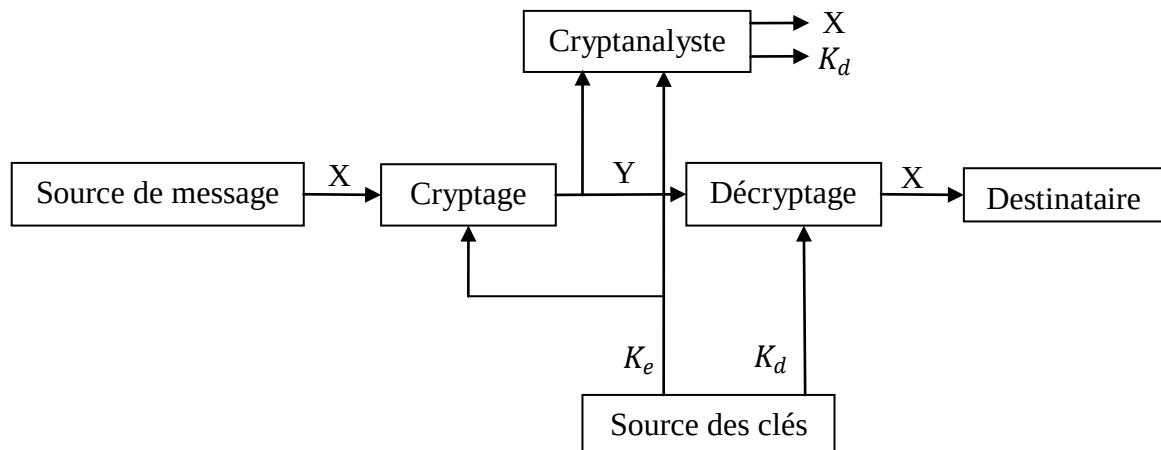


Figure 1.2 : Cryptage asymétrique

Par opposition au cryptage asymétrique, le cryptage symétrique est aussi appelé cryptage à clé secrète. C'est l'approche la plus authentique du cryptage de données et mathématiquement la moins problématique. La clé de cryptage peut être calculée à partir de la clé de décryptage et vice versa. En général, les clés de cryptage et de décryptage sont

identiques, voir Figure 1.3. L'émetteur et le destinataire doivent se mettre d'accord préalablement sur une clé qui doit être gardée secrète, car la sécurité d'un tel algorithme repose sur cette clé. Le problème de cette méthode est de trouver le moyen de transmettre de manière sécurisée la clé à son correspondant.

Un des problèmes principaux du cryptage symétrique est l'échange préalable de la clé secrète. Le cryptage à clé publique résout ce problème [19]-[21]. Le temps de cryptage/décryptage à clé publique est supérieur à celui du cryptage symétrique. Le cryptage à clé publique peut être préféré pour générer de petites séquences comme des signatures ou des clés secrètes pour le cryptage symétrique. Le cryptage symétrique peut être préféré pour crypter des grandes quantités de données comme les images.

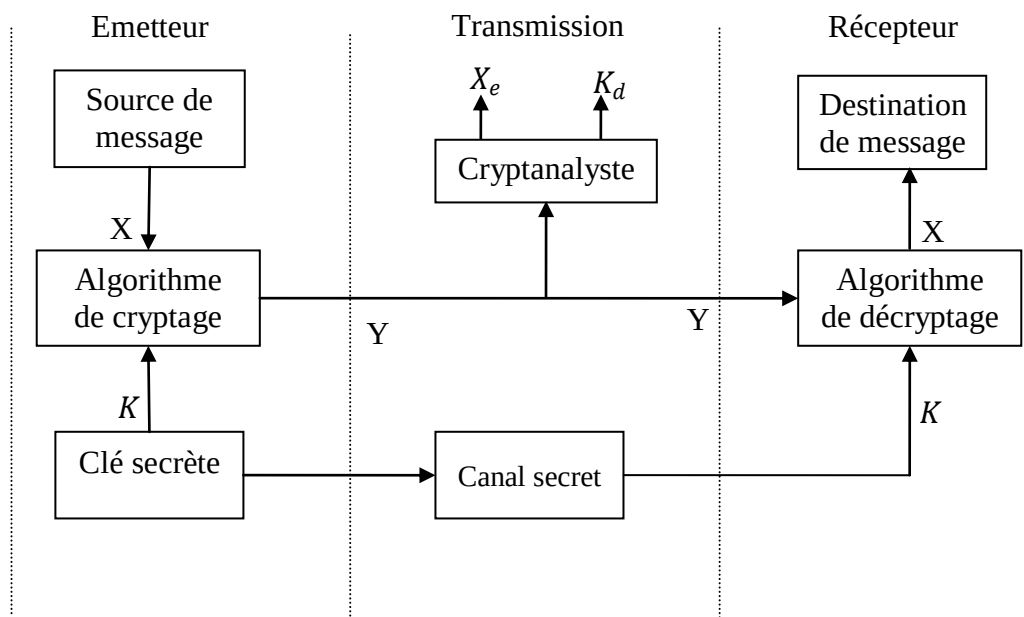


Figure 1.3 : Cryptage symétrique

1.3.2 Classification selon la technique de cryptage

Les principaux types de systèmes cryptographiques symétriques utilisés aujourd'hui se répartissent en deux grandes catégories : les crypto-systèmes par flots et les crypto-systèmes par blocs [14], [22].

Dans un schéma de cryptage par blocs, le message est divisé en blocs de bits, de longueur fixe. Chaque bloc est crypté l'un après l'autre. Un exemple de cryptage par blocs itératifs est le célèbre schéma DES [17].

Une bonne sécurité est définie par une clé assez longue. Les clés très longues sont plus coûteuses en travail à cause notamment de leur génération, de leur transmission, de leur espace mémoire et de la difficulté de s'en rappeler (mots de passe).

La taille des blocs a un impact sur la sécurité et sur la complexité : les blocs de grandes dimensions sont plus sécuritaires mais sont plus lourds à implémenter.

Contrairement au cryptage par blocs qui traite de larges blocs de données, les schémas de cryptage par flot sont appelés aussi cryptage en continu, traitent l'information bit à bit, et sont très rapides. Ils sont parfaitement adaptés à des moyens de calcul et de mémoire (cryptographie en temps réel) comme la cryptographie militaire, ou la cryptographie entre le téléphone portable GSM et son réseau.

1.3.3 Classification selon le pourcentage des données cryptées

En ce qui concerne la quantité de données cryptées, le cryptage peut être divisé en cryptage total et cryptage partiel (également appelés le cryptage sélectif), selon le pourcentage des données cryptées. Le cryptage sélectif est convenable en termes de la sécurité, du temps de traitement et de ressource de traitement.

Le cryptage sélectif peut s'appliquer avec ou non la compression. Puisque le stockage d'une image nécessite un espace de mémoire très grand, il est impuissant de crypter ou de décrypter des images, directement. Une des meilleures méthodes est de crypter et décrypter les informations qui sont utilisées par la compression de l'image seulement (cryptage partiel), pour réduire à la fois son espace de stockage et la durée de transmission [23].

1.3.4 Classification selon le domaine de travail

Il y a deux domaines dans lesquels on peut effectuer un cryptage : domaine temporel/spatial et domaine fréquentiel. Le domaine fréquentiel est obtenu par une transformation discrète comme la DCT et la DFT.

Par exemple, dans le cas d'une image le cryptage dans le domaine spatial se fait par le cryptage d'une combinaison de bits de chaque pixel. C'est une approche simple et applicable à toutes les images. Dans le domaine fréquentiel, le cryptage se fait par l'exploitation des structures et des caractéristiques de la transformée utilisée. Notre étude est principalement basée sur cette approche dont le principe et l'état de l'art sont donnés en plus de détails dans la section suivante.

1.4 Cryptage d'images basé sur les transformées discrètes

Le développement des ordinateurs, des techniques de communication et la mondialisation des échanges (Internet, commerce électronique, ...) sont confrontés à de nouveaux problèmes de sécurité de l'information. Les algorithmes de cryptage traditionnels tels que le DES et le RSA ne sont pratiquement pas appropriés au cryptage d'images dû aux quelques caractéristiques intrinsèques des images comme la taille (image de grande taille), la redondance élevée, la forte corrélation entre les pixels adjacents, etc. Ces caractéristiques rendent ainsi ces algorithmes difficiles à appliquer et lents à traiter.

Parfois, les applications d'image ont leurs propres exigences, comme le traitement en temps réel, la réservation de fidélité, la cohérence de format d'image, et la compression des données pour la transmission, etc. Pour fournir une meilleure solution aux problèmes de sécurité d'images, un certain nombre de techniques de cryptage d'images ont été proposées telles que les techniques basées sur les transformées [4]-[10], [24]. La plupart de ces méthodes utilisent une catégorie de caractère aléatoire, qui ne peut pas être conclus par les utilisateurs non autorisés. Parmi ces techniques, on distingue le cryptage basé sur deux masques de phases aléatoires [11] approprié pour les transformées en valeurs complexes et le cryptage basé sur deux masques d'amplitudes aléatoires [4] approprié pour les transformées en valeurs réelles.

1.4.1 Cryptage basé sur deux masques de phases aléatoires

Philippe Refregier et Bahram Javidi ont proposé en 1995 une méthode de cryptage des images optiques dans le domaine de la transformée de Fourier qui permet de transformer une image en un bruit blanc stationnaire d'amplitude complexe [4]. Dans cette méthode deux masques de phases aléatoires indépendants sont utilisés comme une clé de

cryptage, l'un est appliqué dans le domaine spatial et l'autre dans le domaine fréquentiel voir la figure 1.4.

Dans le schéma de décryptage, l'image cryptée est transformée par la transformée de Fourier et multipliée par le conjugué du deuxième masque et puis transformée par la transformée de Fourier inverse. L'amplitude d'image ainsi obtenue représente l'image originale.

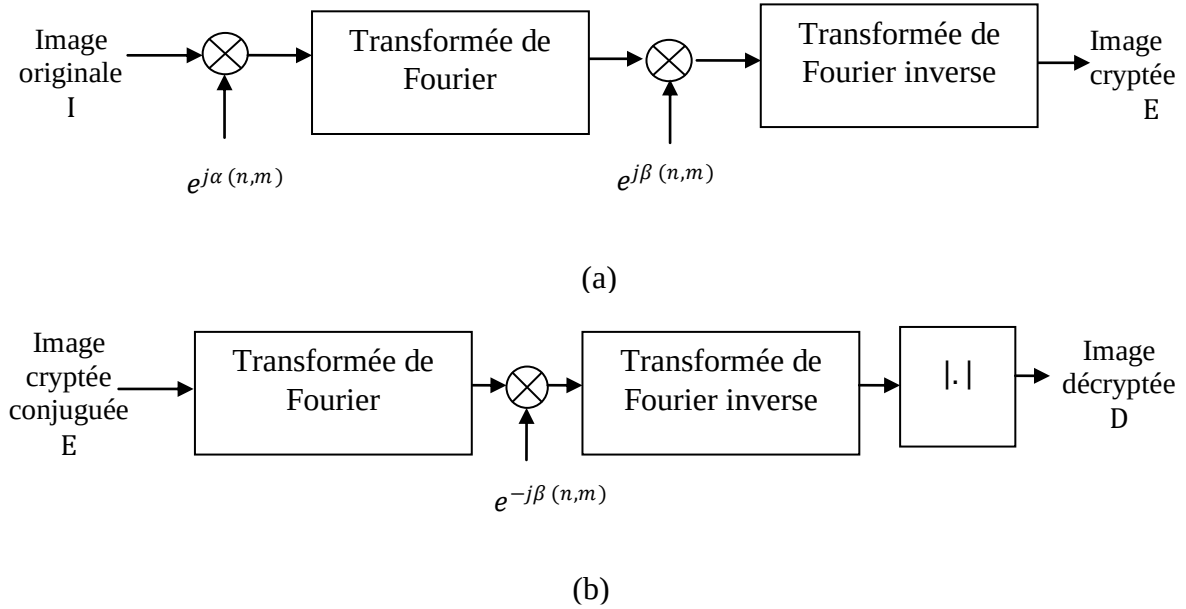


Figure 1.4 Cryptage basé sur deux phases aléatoires dans le domaine de la transformée de Fourier: (a) schéma de cryptage, (b) schéma de décryptage.

Unnikrishnan et Singh [5] ont remplacé la transformée de Fourier classique par la FrFT dans la méthode de cryptage basée sur deux masques de phases aléatoires [4] dont les fractions de la FrFT sont utilisées comme une clé supplémentaire pour le cryptage d'images, voir la figure 1.5.

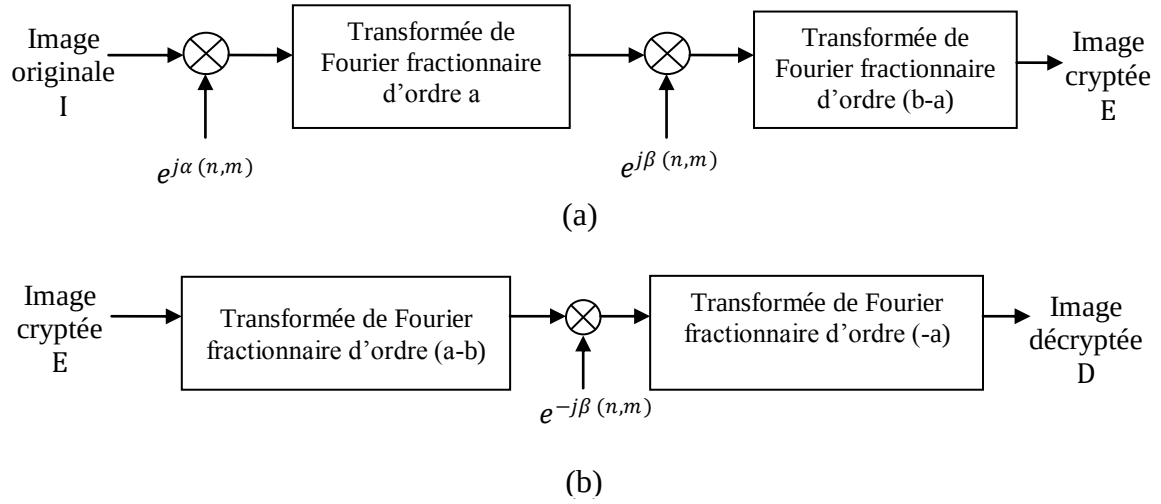


Figure 1.5 Cryptage basé sur deux phases aléatoires dans le domaine de la transformée de Fourier fractionnaire: (a) schéma de cryptage, (b) schéma de décryptage.

La reconstruction de l'image originale exige la spécification des domaines fractionnaires; il faut connaître les fractions des FrFT appliquées dans le domaine spatial et dans le domaine fréquentiel en plus de la clé de cryptage.

Afin d'augmenter la sécurité du cryptage, Pie and Hsue [6] ont proposé une méthode de cryptage d'images basée sur deux masques de phases aléatoires dans le domaine de la transformée de Fourier fractionnaire de multi-paramètres, voir la figure 1.6.

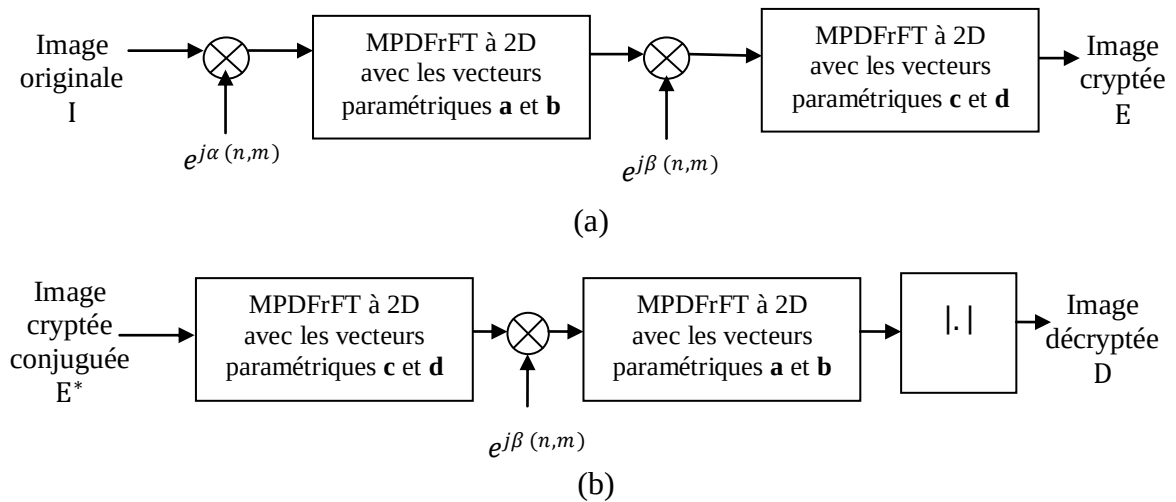


Figure 1.6 Cryptage basé sur deux phases aléatoires dans le domaine de la transformée de Fourier fractionnaire de multi-paramètres: (a) schéma de cryptage, (b) schéma de décryptage.

Les paramètres indépendants des transformées FrFT et MPDFrFT ont été utilisés avec succès comme une clé secrète supplémentaire dans [5] et [6]; cependant, ces transformées ont une grande complexité de calcul.

Bouguezel et al. ont proposé dans [11] une méthode rapide et efficace de cryptage d'images basée sur deux masques de phases aléatoires dans le domaine de la transformée réciproque orthogonale et paramétrique (ROP) développée dans [12], voir la figure 1.7. Cette transformée qui a une faible complexité de calcul comparée à celle du FrFT sera présentée dans le chapitre suivant.

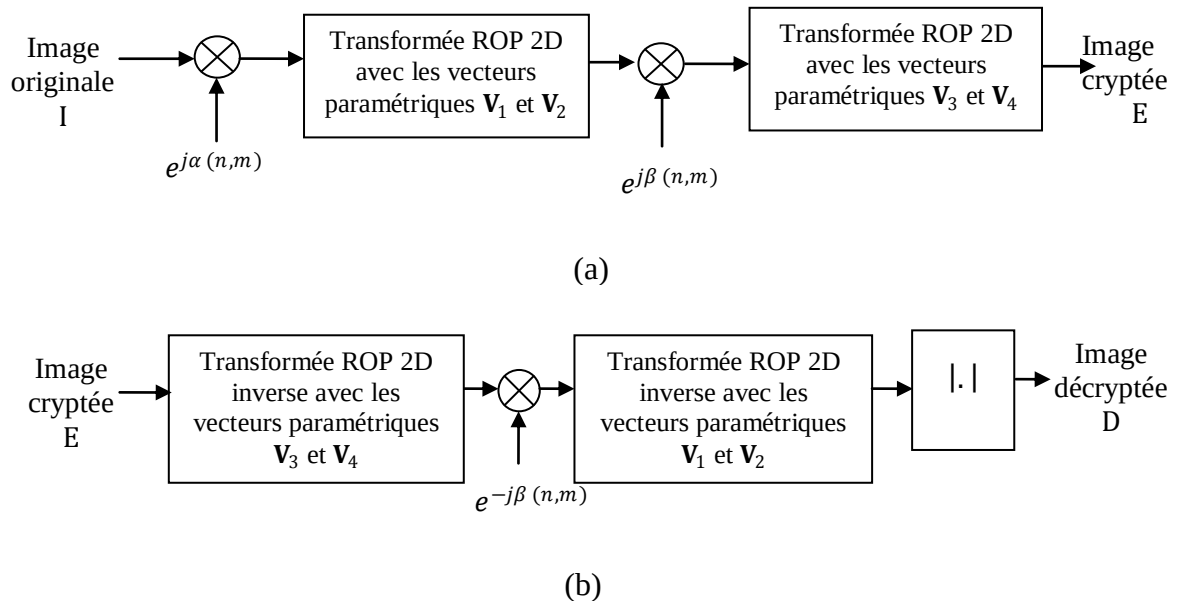


Figure 1.7 Cryptage basé sur deux phases aléatoires dans le domaine de la transformée ROP: (a) schéma de cryptage, (b) schéma de décryptage

Les méthodes de cryptage [5], [6], [11] citées précédemment sont efficaces du point de vue sécurité, malgré que l'image cryptée soit complexe. Elles sont conçues convenablement pour l'exploitation des transformées à valeurs complexes. Afin d'assurer que l'image cryptée soit purement réelle, des méthodes de cryptage d'images basées sur des masques d'amplitudes aléatoires ont été proposées [8]-[10] en exploitant les transformées à valeurs réelles.

1.4.2 Cryptage basé sur deux masques d'amplitudes aléatoires

Chen et Zhao ont remplacé les masques de phases aléatoires dans [4] par des masques d'amplitudes aléatoires dans le domaine de la transformée de Hartley [8] pour exploiter les propriétés de cette transformée notamment la nature réelle et pour garantir que l'image cryptée soit réelle. Les processus de cryptage et décryptage sont montrés dans la figure 1.8.

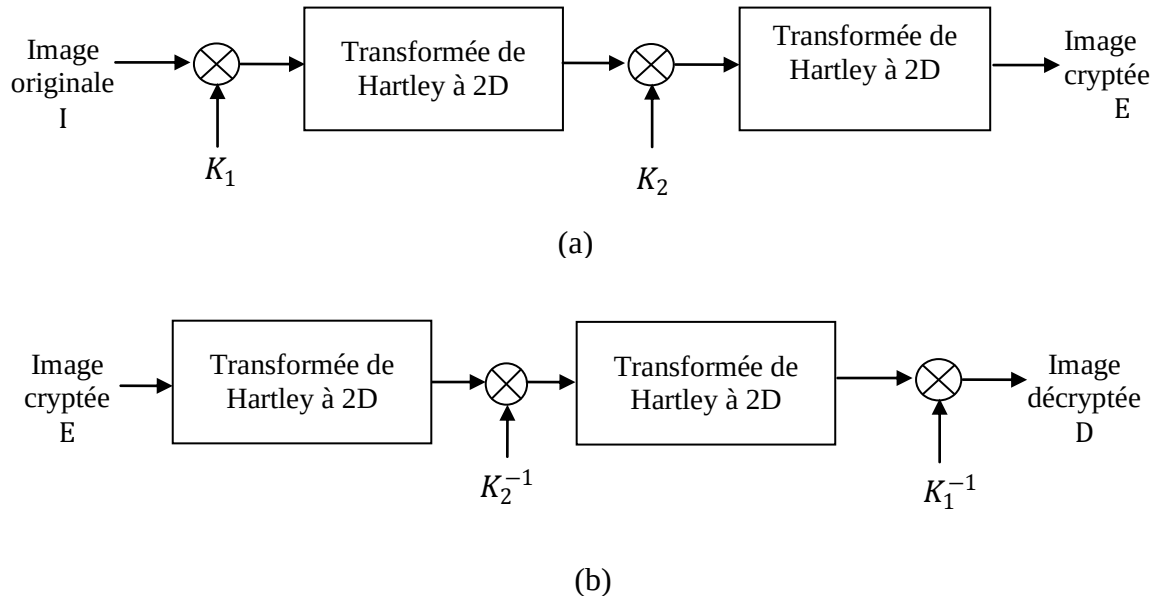


Figure 1.8 Cryptage basé sur deux masques d'amplitudes aléatoires dans le domaine de la transformée de Hartley: (a) schéma de cryptage, (b) schéma de

Pour renforcer la sécurité davantage, Zhengjun Liu et al. ont utilisé la transformée de Hartley aléatoire dans le cryptage d'images basé sur deux masques d'amplitudes aléatoires [9], voir la figure 1.9. Cette méthode est essentiellement motivée pour exploiter la nature aléatoire de cette transformée dans le cryptage d'images.

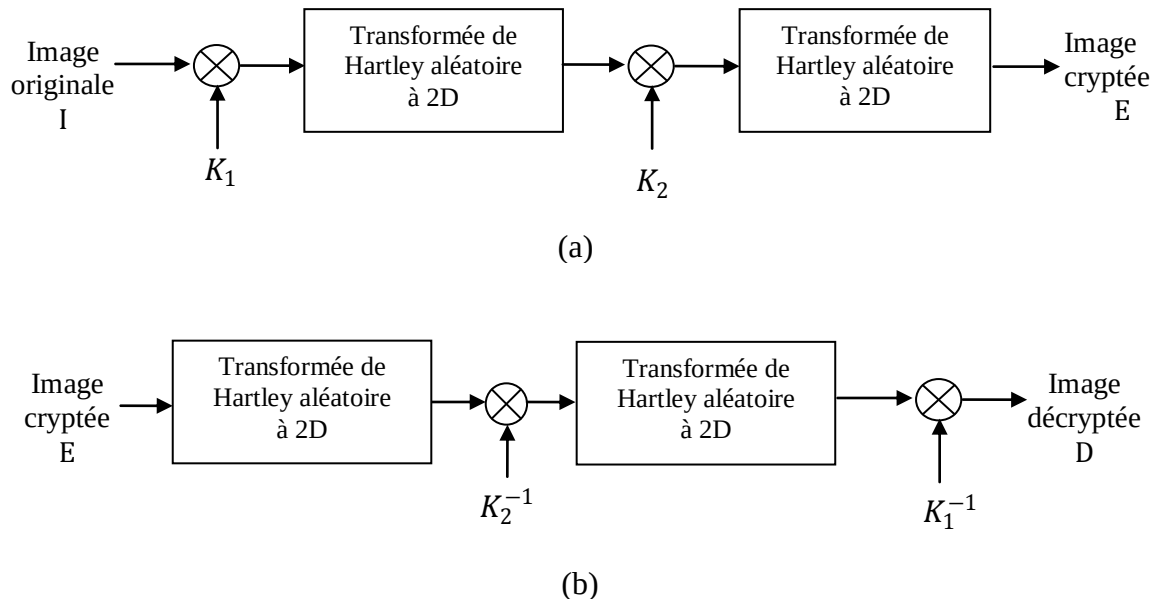


Figure 1.9 Cryptage basé sur deux masques d'amplitudes aléatoires dans le domaine de la transformée de Hartley aléatoire: (a) schéma de cryptage, (b) schéma de

1.5 Cryptanalyse

La cryptanalyse ou l'attaque regroupe tous les moyens de décrypter un texte crypté sans avoir connaissance de la clé. Les procédés de cryptanalyse pour le cryptage symétrique sont très nombreux et la plupart des attaques sont spécifiquement adaptées aux techniques de cryptage. On distingue les différents types d'attaques en fonction des données supposées connues par les attaquants [14], [25]

- L'attaque à texte crypté seulement (Ciphertext-only attack) : l'attaquant a connaissance du texte crypté de plusieurs messages.
- L'attaque à texte en clair connu (Known-plaintext attack) : le cryptanalyste a accès à plusieurs textes cryptés ainsi qu'aux textes en clair correspondants.
- L'attaque à texte en clair choisi (Chosen-plaintext attack) : l'attaquant a accès à l'algorithme de cryptage. Il l'utilise pour générer des couples (X_i, Y_i) de son choix. La différence principale par rapport à l'attaque à texte en clair connu est que le cryptanalyste peut choisir le texte à crypter.

- L'attaque à texte crypté adapté (Adaptative-Ciphertext attack) : le cryptanalyste a accès à l'algorithme de décryptage. Il peut choisir les textes à décrypter sans connaître la clé.
- L'attaque par force brute (Brute-force attack) ou l'attaque exhaustive : l'attaquant essaie toutes combinaisons de clés possibles jusqu'à l'obtention du texte en clair.

La création de techniques modernes de cryptage a fait ressortir des nouvelles méthodes de cryptanalyse.

1.6 Mesures de performances

L'application d'un algorithme de cryptage à une image change ses valeurs de pixel par rapport à l'image originale. Un bon algorithme de cryptage doit apporter ces modifications d'une façon irrégulière et également maximiser la différence en valeurs de pixel entre l'image originale et l'image cryptée. En outre, pour obtenir une bonne image cryptée, elle doit se composer de modèles totalement aléatoires qui ne révèlent aucune caractéristique de l'image originale. L'image cryptée doit être indépendante de l'image originale et elle devrait avoir une faible corrélation avec l'image originale [26]-[27].

Un des paramètres importants dans l'examen d'une image cryptée est l'inspection visuelle, plus les caractéristiques de l'image sont cachées, plus l'algorithme de cryptage est meilleur. Malheureusement, l'inspection visuelle n'est pas suffisante pour juger la clandestinité complète du contenu de l'image.

D'autres tests peuvent être utilisés pour déterminer certaines caractéristiques spécifiques des algorithmes de cryptage. Les mesures qui sont généralement utilisées sont :

1.6.1 Le Coefficient de Corrélation

Une mesure utile pour évaluer la qualité de cryptage de tout système cryptographique des images est le coefficient de corrélation entre les pixels aux mêmes indices dans l'image originale et les images cryptées [28]. Cette mesure peut être calculée comme suit :

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D_x} \sqrt{D_y}} \quad (1.3)$$

où x et y sont les valeurs de niveau de gris de deux pixel aux mêmes index dans l'image originale et l'image cryptée. Dans des calculs numériques, les formules discrètes suivantes peuvent être utilisées :

$$E(x) = \frac{1}{L} \sum_{l=1}^L x_l \quad (1.4)$$

$$D(x) = \frac{1}{L} \sum_{l=1}^L (x_l - E(x))^2 \quad (1.5)$$

$$\text{cov}(x, y) = \frac{1}{L} \sum_{l=1}^L (x_l - E(x))(y_l - E(y)) \quad (1.6)$$

où L est le nombre de Pixel compris dans les calculs. Plus la valeur de r_{xy} est proche de zéro, plus la qualité de l'algorithme de cryptage est meilleure.

1.6.2 Rapport signal à bruit en pic

Le rapport signal à bruit en pic (peak signal to noise ratio : PSNR), est une mesure de distorsion utilisée en image numérique, c'est le critère le plus couramment utilisé. Il s'agit de quantifier la performance des algorithmes de cryptage en mesurant la différence entre l'image décryptée par une fausse clé et l'image originale. Il est défini en décibel (dB) par [29] :

$$PSNR = 10 \log_{10} \frac{d^2}{EQM} \quad (1.7)$$

où d est la dynamique de l'image (la valeur maximale possible pour un pixel). Dans le cas standard d'une image où les composantes d'un pixel sont codées sur 8 bits, $d = 255$ et EQM (Erreur Quadratique Moyenne, en anglais : Mean Squar Error : MSE) définie pour deux images I_o et I_r de taille $N \times M$ comme suit:

$$EQM = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |I_o(i, j) - I_r(i, j)|^2 \quad (1.8)$$

1.6.3 Histogramme

L'histogramme est la représentation graphique de la proportion de pixels d'une image par gamme de luminosité. L'axe horizontal représente toutes les valeurs de niveau de gris possibles pour un pixel, dans l'ordre croissant, c'est-à-dire de 0 à 255 pour une image en 8 bits et l'axe vertical indique le nombre de pixels ayant la valeur considérée [30].

Pour des algorithmes de cryptage d'images, l'histogramme de l'image cryptée devrait avoir deux propriétés :

- ✓ Il doit être totalement différent de l'histogramme de l'image originale.
- ✓ Il doit avoir une distribution totalement aléatoire.

1.7 Conclusion

Dans ce chapitre, nous avons décrit le principe de la cryptographie et exposé les différentes attaques considérées dans ce domaine ainsi que les mesures de performances utilisées pour tester la robustesse d'une méthode de cryptage. Nous avons aussi présenté les différentes classifications des techniques de cryptage en donnant plus de détail sur l'état de l'art des techniques de cryptage d'images basées sur les transformées discrètes. Ces techniques, en particulier qui sont basées sur deux masques de phases ou d'amplitudes aléatoires, constituent la base de nos méthodes de cryptage d'images fixes proposées dans les chapitres 3 et 4.

Chapitre 2

Les transformées paramétriques



2.1 Introduction

La popularité de la transformée de Fourier discrète (Discrete Fourier Transform : DFT), la transformée de Hartley discrète (Discrete Hartley Transform : DHT), la transformée de Walsh-Hadamard (Walsh-Hadamard Transform : WHT), et la transformée en cosinus discrète (Discrete Cosine Transform : DCT) en traitement de signal et dans d'autres domaines scientifiques et dans l'ingénierie [31]-[34] est due non seulement à leur utilité mais aussi à l'existence des algorithmes efficaces pour leur calcul rapide. Le succès des transformées populaires existantes mentionnées précédemment a motivé beaucoup de chercheurs, ces dernières années, pour généraliser et paramétrer ces transformées afin d'élargir le domaine de leurs applications et de fournir plus de flexibilité dans la représentation, l'interprétation et le traitement de signal.

Les paramètres indépendants d'une transformée sont très utiles dans la caractérisation des signaux selon différents points de vue et peuvent être également utilisés comme une clé secrète supplémentaire pour des applications telles que le tatouage et le cryptage. Par exemple, les paramètres indépendants d'une transformée Fractionnaire discrète ont été utilisés comme une clé secrète supplémentaire dans [35] pour le tatouage et dans [6] et [7] pour le cryptage.

Nous allons présenter, dans ce chapitre, les transformées paramétriques qui seront utilisées dans les chapitres suivants pour le cryptage des images fixes, les méthodes de construction de leurs matrices et les algorithmes rapides pour leur calcul.

2.2 La transformée réciproque-orthogonale et paramétrique

La popularité de la WHT est principalement due à l'existence d'un algorithme efficace pour son calcul rapide. Elle a une large utilisation dans de nombreuses applications [32]-[34], en particulier, avec un succès remarquable, dans le cryptage [36]-[38] et le tatouage [39]-[41], mais elle n'a pas de paramètres indépendants. Par conséquent, une transformée similaire à la WHT avec une configuration d'avoir des paramètres indépendants serait plus souhaitable et pourrait avoir un domaine d'applications plus large.

Dans la littérature, divers essais ont été faits pour la généralisation et la paramétrisation des matrices de Hadamard [42]-[47]. Cependant, les transformées basées

sur les matrices généralisées de Hadamard présentées dans [42]-[44] et [45] aussi bien que celles de la transformée de jacket généralisée proposée dans [46] et [47] ont des complexités de calcul et de structure très élevées et par conséquent aucune tentative n'a été faite dans la littérature pour développer des algorithmes rapides pour leurs calculs. La transformée réciproque-orthogonale et paramétrique (ROP) proposée dans [12] en combinant convenablement un nouveau vecteur du noyau (kernel vector) paramétrique avec celui du WHT possède une structure simple et une complexité de calcul faible.

2.2.1 Définition

La transformée ROP d'une séquence complexe $x(k)$ de taille $N = 2^r$ est définie par [12]

$$X(n) = \sum_{k=0}^{N-1} x(k) a_{k,s(n)} (-1)^{kon}, \quad n = 0, 1, \dots, N-1 \quad (2.1)$$

et la transformée inverse est donnée par :

$$x(k) = \frac{1}{N} \sum_{n=0}^{N-1} X(n) \frac{1}{a_{k,s(n)}} (-1)^{kon}, \quad k = 0, 1, \dots, N-1 \quad (2.2)$$

où $kon = k_0 n_0 + k_1 n_1 + \dots + k_{r-1} n_{r-1}$, $s(n) = (-1)^{(N-1)on}$ et $a_{k,1}$ et $a_{k,-1}$ sont des paramètres complexes non nuls qui doivent satisfaire la condition suivante d'existence de la transformée inverse

$$a_{k,1} a_{N-1-k,-1} = a_{k,-1} a_{N-1-k,1} \quad (2.3)$$

Les équations (2.1) et (2.2) peuvent être exprimées sous forme matricielle comme suit :

$$\mathbf{X} = \mathbf{P}_N \mathbf{x} \quad (2.4)$$

$$\mathbf{x} = \mathbf{P}_N^{-1} \mathbf{X} \quad (2.5)$$

où $\mathbf{P}_N$ est la matrice paramétrique de la transformée ROP par contre $\mathbf{P}_N^{-1}$ est la matrice inverse de $\mathbf{P}_N$.

2.2.2 Construction de la matrice de la transformée ROP

Rappelons qu'une matrice de Hadamard $\mathbf{H}_N$ est une matrice carrée d'ordre N dont tous ces éléments sont de l'ensemble $\{+1, -1\}$ et satisfait la relation $\mathbf{H}_N \mathbf{H}_N = N \mathbf{I}_N$, où $\mathbf{I}_N$ est la matrice identité d'ordre $N = 2^r$, avec r est un nombre entier positif. Les lignes de la matrice $\mathbf{H}_N$ sont indexées par des entiers de valeurs $n = 0, 1, \dots, N - 1$. Tout nombre entier n , $0 \leq n \leq N - 1$, peut être décomposé comme suit

$$n = n_{r-1} 2^{r-1} + n_{r-2} 2^{r-2} + \dots + n_1 2 + n_0$$

où n_i , $0 \leq i \leq r - 1$, sont des chiffres binaires (0 ou 1).

On définit la fonction $s(n) = (-1)^{\sum_{i=0}^{r-1} n_i}$ qui prend deux valeurs $+1$ ou -1 . Chaque ligne de la matrice $\mathbf{H}_N$ indexée par un nombre entier n qui vérifie $s(n) = 1$ est dite ligne indexée positivement (plus-indexed row) et celle qui est indexée par un nombre entier n qui vérifie $s(n) = -1$ est dite ligne indexée négativement (minus-indexed row).

Soient $\mathbf{S}_1 = [s_1(k)]$ et $\mathbf{S}_{-1} = [s_{-1}(k)]$ deux vecteurs lignes paramétriques de longueur N , avec $s_1(k) = a_{k,1}$, $k = 0, 1, \dots, N - 1$ et $s_{-1}(k) = a_{k,-1}$, $k = 0, 1, \dots, N/2 - 1$, sont des paramètres scalaires non nuls et arbitrairement choisis du plan complexe, et $s_{-1}((N/2) + k) = a_{(N/2)+k,-1}$, $k = 0, 1, \dots, N/2 - 1$, sont obtenus à partir des éléments de $\mathbf{S}_1$ et de $N/2$ premiers éléments de $\mathbf{S}_{-1}$ par l'exploitation de la condition de l'existence de la transformée inverse donnée par l'équation (2.3) comme suit

$$a_{\frac{N}{2}+k,-1} = \frac{a_{\frac{N}{2}-k,-1} a_{\frac{N}{2}+k,1}}{a_{\frac{N}{2}-k,1}}, \quad k = 0, 1, 2, \dots, \frac{N}{2} - 1 \quad (2.6)$$

La multiplication élément-par-élément de chaque ligne indexée positivement de la matrice de Hadamard $\mathbf{H}_N$ par le vecteur $\mathbf{S}_1$ et de chaque ligne indexée négativement par $\mathbf{S}_{-1}$ donne une matrice $\mathbf{P}_N$ paramétrique réciproque-orthogonale (ROP) d'ordre N . La matrice $\mathbf{P}_N$ représente la matrice de la transformée ROP.

2.2.3 Propriétés de la transformée ROP

La matrice $\mathbf{P}_N$ de la transformée ROP est une matrice réciproque-orthogonale qui satisfait la relation suivante [12]

$$\mathbf{P}_N \times \mathbf{P}_N^{-1} = \mathbf{P}_N \times (1/N)\mathbf{P}_N^{\text{RT}} = N\mathbf{I}_N \quad (2.7)$$

où $\mathbf{P}_N^{\text{RT}}$ est la matrice réciproque transposée de $\mathbf{P}_N$ avec ses éléments sont données par

$$\mathbf{P}_N^{\text{RT}}(i, j) = 1/\mathbf{P}_N(j, i), \quad i, j = 1, 2, \dots, N \quad (2.8)$$

La matrice ROP a $3N/2$ paramètres indépendants qui peuvent être arbitrairement choisis du plan complexe. Il est simple de remarquer que quand $a_{k,1} = 1$, $k = 0, 1, \dots, N-1$ et $a_{0,-1} = 1$, la matrice $\mathbf{P}_N$ devient une matrice normalisée dont tous les éléments de sa première ligne et sa première colonne sont des $+1$. Dans ce cas, le vecteur $\mathbf{S}_{-1}$ devient symétrique et le nombre de paramètres indépendants de la matrice ROP réduit à $N/2 - 1$. Par conséquent, la construction de la matrice ROP normalisée d'ordre N consiste simplement d'une multiplication élément-par-élément de chaque ligne indexée négativement de la matrice $\mathbf{H}_N$ par le vecteur $\mathbf{S}_{-1}$.

Puisque la matrice ROP possède $3N/2$ paramètres indépendants qui peuvent être arbitrairement choisis du plan complexe, un nombre très large de matrices ROP peut être facilement obtenu. La matrice $\mathbf{P}_N$ devient la matrice $\mathbf{H}_N$ de Hadamard si tous les $3N/2$ paramètres sont choisis de l'ensemble $\{+1, -1\}$, et elle devient une matrice unitaire quand ces paramètres sont choisis du cercle d'unité. Une famille des matrices de Hadamard complexes similaires à celles proposées dans [48] peut être construite simplement si l'on choisit les paramètres indépendants de l'ensemble $\{+1, -1, +j, -j\}$, où $j = \sqrt{-1}$.

La transformée ROP définie par l'équation (2.1) devient une transformée sans-multiplications (multiplication-free transform), si tous les $3N/2$ paramètres indépendants sont de l'ensemble $\{\pm 2^m, \pm 2^n j, 2^l(\pm 1 \pm j)\}$, où m , n et l sont des nombres entiers positifs ou négatifs. Par conséquent, l'implémentation de cette transformée exige seulement des additions/soustractions et des décalages de bits. Cette transformée intéressante sera exploitée dans le chapitre 4 pour le développement d'une nouvelle méthode de cryptage d'images fixes.

2.2.4 Algorithme rapide pour le calcul de la transformée ROP

Dans cette section, nous présentons l'algorithme proposé dans [12] pour le calcul rapide de la transformée ROP. Puisque La transformée ROP directe et la transformée

inverse ont la même structure, l'algorithme rapide de calcul de la transformée ROP directe peut être utilisé pour calculer la transformée ROP inverse.

La transformée ROP donnée par l'équation (2.1) peut être écrite comme suit :

$$X(n) = \sum_{k=0}^{\frac{N}{2}-1} [x(k)a_{k,s(n)} + s(n)x(N-1-k)a_{N-1-k,s(n)}] \times (-1)^{k \circ n}, \quad n = 0, 1, \dots, N-1 \quad (2.9)$$

La décomposition de $X(n)$ donnée par (2.1) selon la valeur de $s(n)$ donne les deux séries suivantes :

$$X(n) = \sum_{k=0}^{\frac{N}{2}-1} [x(k)a_{k,1} + x(N-1-k)a_{N-1-k,1}] \times (-1)^{k \circ n} \quad 0 \leq n \leq N-1, \quad n \in S_e \quad (2.10)$$

$$X(n) = \sum_{k=0}^{\frac{N}{2}-1} [x(k)a_{k,-1} - x(N-1-k)a_{N-1-k,-1}] \times (-1)^{k \circ n} \quad 0 \leq n \leq N-1, \quad n \in S_o \quad (2.11)$$

avec S_e et S_o sont deux ensembles des nombres entiers n satisfont $S(n) = 1$ et $S(n) = -1$, respectivement.

L'utilisation de la condition d'existence de la transformée inverse donnée par l'équation (2.3) conduit à :

$$X(n) = \sum_{k=0}^{\frac{N}{2}-1} g_e(k)(-1)^{k \circ n}, \quad 0 \leq n \leq N-1, \quad n \in S_e \quad (2.12)$$

$$X(n) = \sum_{k=0}^{\frac{N}{2}-1} g_o(k)(-1)^{k \circ n}, \quad 0 \leq n \leq N-1, \quad n \in S_o \quad (2.13)$$

où les séquences d'entrée $g_e(k)$ et $g_o(k)$ sont calculées en utilisant le papillon paramétrique (parametric butterfly : P-B) présenté dans la figure (2.1) comme suit :

$$\begin{bmatrix} g_e(k) \\ g_o(k) \end{bmatrix} = \begin{bmatrix} a_{k,1} & 0 \\ 0 & a_{k,-1} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \frac{a_{N-1-k,1}}{a_{k,1}} \end{bmatrix} \begin{bmatrix} x(k) \\ x(N-1-k) \end{bmatrix},$$

$$k = 0, 1, \dots, N/2 - 1 \quad (2.14)$$

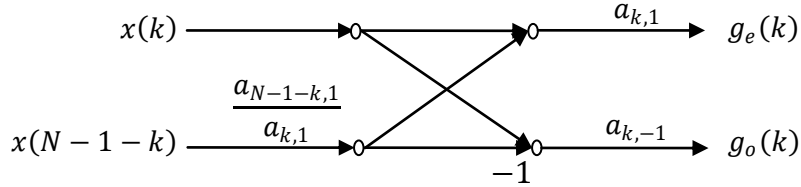


Figure 2.1 Le papillon paramétrique (P-B) pour le calcul de la transformée ROP

La sortie $X(n)$ peut être obtenue à partir de $X_e(t)$ et $X_o(t)$, les séquences de sortie de la WHT d'ordre $N/2$ et les séquences d'entrée $g_e(k)$ et $g_o(k)$, respectivement.

$$X_e(t) = \sum_{k=0}^{\frac{N}{2}-1} g_e(k) (-1)^{k \circ t}, \quad t = 0, 1, 2, \dots, N/2 - 1 \quad (2.15)$$

$$X_o(t) = \sum_{k=0}^{\frac{N}{2}-1} g_o(k) (-1)^{k \circ t}, \quad t = 0, 1, 2, \dots, N/2 - 1 \quad (2.16)$$

La structure générale de l'algorithme de calcul rapide de la transformée ROP est représentée dans la figure (2.2).

2.2.5 Calcul de la complexité

Puisque les paramètres de la transformée ROP peuvent être arbitrairement choisis du plan complexe et la séquence d'entrée $x(k)$ peut être complexe ou réelle, la complexité arithmétique varie selon le choix des paramètres [12].

Dans le cas où tous les paramètres sont complexes, mais pas de l'ensemble $\{\pm 2^m, \pm 2^n j, 2^l (\pm 1 \pm j)\}$, et la séquence d'entrée $x(k)$ est aussi complexe ; c'est le cas qui exige la complexité la plus élevée de calcul parmi tous les cas possibles, le calcul de la

transformée ROP exige $3N/2$ multiplications complexes et $N\log_2 N$ additions complexes, et le nombre de multiplications exigées par la transformée normalisée est $N/2 - 1$. Le calcul de la transformée ROP dans ce cas exige moins de nombre d'opérations arithmétiques par rapport à la DFT calculée par l'algorithme de Cooley-Tukey ; l'algorithme rapide le plus régulier, qui exige $(N/2)\log_2 N$ multiplications complexes et $N\log_2 N$ additions complexes.

Si tous les paramètres de la transformée sont réels mais pas de l'ensemble $\{\pm 2^m\}$, et la séquence d'entrée $x(k)$ est réelle, la transformée ROP exige $3N/2$ multiplications réelle et $N\log_2 N$ additions réelle pour son calcul, et le nombre de multiplications exigées par la transformée normalisée est $N/2 - 1$. Cette complexité arithmétique est comparée dans le tableau 2.1 à celles exigées par le calcul des transformées à valeurs réelles (real-valued transforms).

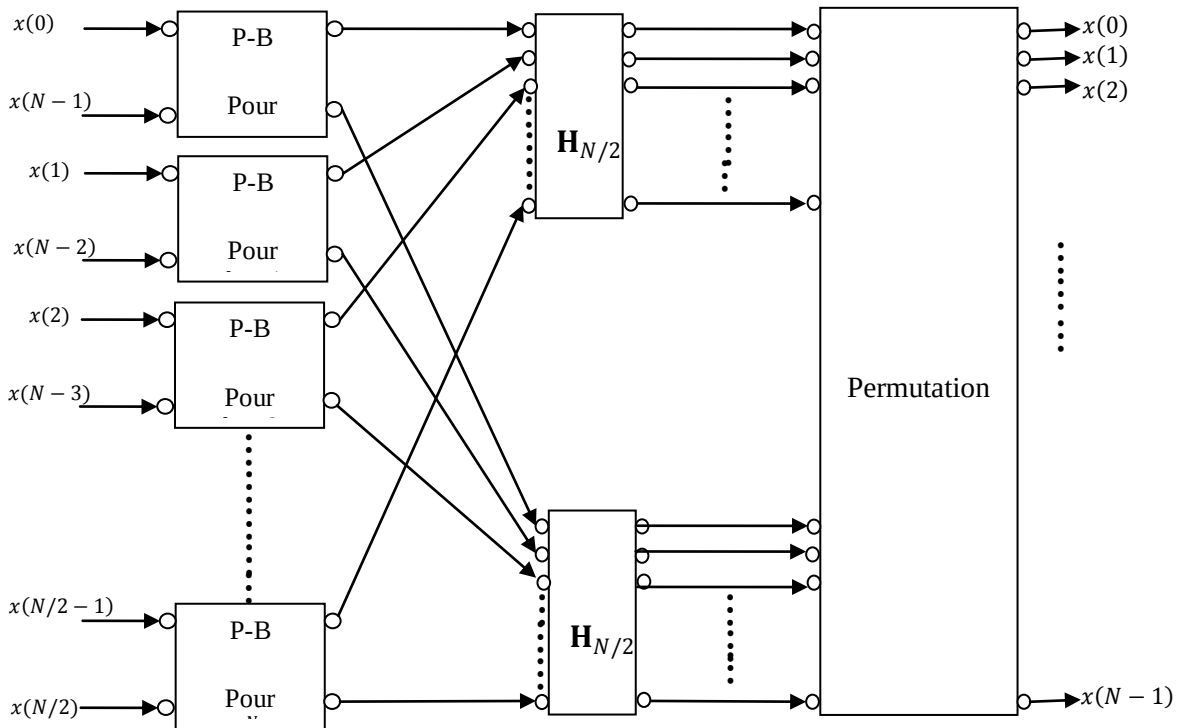


Figure 2.2 Structure de l'algorithme de la transformée ROP

Tableau 2.1 : Complexité arithmétique de différentes transformées réelles

N	DCT [49]		DHT [50]		Transformée ROP [12]		
	Multiplications	Additions	Multiplications	Additions	(non normalisée)	(normalisée)	Additions
					Multiplications	Multiplications	
8	12	29	2	28	12	3	24
16	32	81	10	74	24	7	64
32	80	209	34	178	48	15	160
64	192	513	98	420	96	31	384
128	448	1217	258	948	192	63	896

Le tableau précédent montre clairement que la transformée ROP exige moins d'opérations arithmétiques par rapport à la DCT [49] et à la DHT [50].

2.3 Transformée de Fourier discrète paramétrique

La transformée de Fourier est la transformée la plus populaire et la plus utilisée. Elle a des applications dans beaucoup de domaines de la science et de la technologie en raison de l'existence des algorithmes de transformée de Fourier rapide (Fast Fourier Transform : FFT) pour son calcul [51]-[53]. La transformée de Fourier fractionnaire (Fractional Fourier Transform : FrFT) et la transformée de Fourier discrète (DFT) paramétrique sont intéressantes pour beaucoup d'applications [6], [7],[13], [54].

La DFT paramétrique est obtenue en remplaçant convenablement quelques éléments spécifiques dans le vecteur du noyau de la DFT classique par des paramètres indépendants qui peuvent être choisis arbitrairement du plan complexe.

2.3.1 Définition

La DFT paramétrique de trois paramètres (three-parameter DFT) d'une séquence complexe $x(k)$ de taille $N = 2^r$, où $r > 3$, est définie par [13]

$$X^{a,b,c}(n) = \sum_{k=0}^{N-1} x(k) v_{Fa,b,c}(nk \bmod N), \quad 0 \leq n \leq N-1 \quad (2.17)$$

où $v_{Fa,b,c}$, $0 \leq i \leq N-1$, dénote les éléments de vecteur $\mathbf{V}_{Fa,b,c}$ donné par

$$\mathbf{V}_{F^{a,b,c}} = \begin{bmatrix} 1 & \mathbf{V} & c & -j\mathbf{V} & -1 & -\mathbf{V} & -c & j\mathbf{V} \end{bmatrix} \quad (2.18)$$

avec

$$\mathbf{V} = \begin{bmatrix} W_N^1 & \dots & W_N^{(N/16)-1} & a & W_N^{(N/16)+1} & \dots & W_N^{(N/8)-1} & b & W_N^{(N/8)+1} \\ \dots & W_N^{(3N/16)-1} & -ja^* & W_N^{(3N/16)+1} & \dots & W_N^{(N/4)-1} \end{bmatrix} \quad (2.19)$$

où $W_N = \exp(-j(2\pi/N))$ et a, b et c sont trois paramètres indépendants qui peuvent être choisis arbitrairement du plan complexe. La transformée inverse est donnée par :

$$x(k) = \frac{1}{N} \sum_{n=0}^{N-1} X^{a,b,c}(n) \frac{1}{v_{F^{a,b,c}}(nk \bmod N)}, \quad 0 \leq k \leq N-1 \quad (2.20)$$

Les deux équations (2.17) et (2.20) peuvent être écrites sous forme matricielle comme suit :

$$\mathbf{X}^{a,b,c} = \mathbf{F}_N^{a,b,c} \cdot \mathbf{x} \quad (2.21)$$

$$\mathbf{x} = (\mathbf{F}_N^{a,b,c})^{-1} \cdot \mathbf{X}^{a,b,c} \quad (2.22)$$

où les éléments de la matrice $\mathbf{F}_N^{a,b,c}$ sont

$$f_N^{a,b,c}(n, k) = v_{F^{a,b,c}}(nk \bmod N), \quad 0 \leq n, k \leq N-1 \quad (2.23)$$

2.3.2 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 :

$$\mathbf{F}_N^{a,b,c} \times (\mathbf{F}_N^{a,b,c})^{-1} = \mathbf{F}_N^{a,b,c} \times (\mathbf{F}_N^{a,b,c})^{\text{RT}} = N\mathbf{I}_N \quad (2.24)$$

Dans le cas où $a = W_N^{N/16}$, $b = W_N^{N/8}$ et $c = W_N^{N/4}$ la matrice $\mathbf{F}_N^{a,b,c}$ est équivalente à celle de la DFT classique. Quand les trois paramètres de la DFT paramétrique sont choisis du cercle d'unité, la transformée devient une transformée unitaire. Un des cas particuliers le plus intéressant est obtenu lorsque $a = e^{j\alpha}$, avec α étant un paramètre réel, $b = W_N^{N/8}$ et $c = W_N^{N/4}$, dans ce cas la DFT de trois paramètres est réduite à une transformée unitaire avec un seul paramètre $\mathbf{F}_N^\alpha$ (one-parameter DFT : DFT^α) et elle

possède la propriété de passer d'une transformée à valeurs complexes à une autre à valeurs réelles (complex-to-real property). Il est évident que $\mathbf{F}_N^{-\pi/8}$ représente la matrice DFT classique.

Les équations (2.18) et (2.19) montrent clairement que les paramètres a , b et c de la DFT paramétrique sont indépendants de la taille N de $\mathbf{F}_N^{a,b,c}$ parce qu'ils remplacent toujours les valeurs $\exp(-j\pi/8)$, $\exp(-j\pi/4)$ et $\exp(-j\pi/2)$, respectivement, du vecteur de noyau de la DFT classique. Par conséquent, le programme utilisé pour calculer la DFT paramétrique n'a pas besoin d'être changé quand la valeur de N est changée, et elle peut être calculé par les algorithmes rapides de la DFT classique [13].

2.4 Transformée de Hartley discrète paramétrique

La DHT est une transformation mathématique qui transforme une fonction temporelle ou spatiale à valeurs réelles en une fonction fréquentielle à valeurs réelles via le noyau (kernel) $\text{cas}(\omega x) \equiv \cos(\omega x) + \sin(\omega x)$, avec la variable de pulsation $\omega = 2\pi f$ où f est la variable de fréquence et x est la variable temporelle/spatiale. Elle est obtenue par la soustraction de la partie imaginaire de la partie réelle de la matrice DFT.

Comme la matrice $\mathbf{F}_N^\alpha$ d'un seul paramètre présentée dans la section précédente est une matrice unitaire de valeurs complexes qui possède la propriété de valeurs complexe-à-réelle, une matrice réelle d'un seul paramètre est obtenue en soustrayant la partie imaginaire de la partie réelle de la matrice $\mathbf{F}_N^\alpha$ [13]. La matrice résultante $\mathbf{H}_N^\alpha$ représente la matrice DHT paramétrique d'un seul paramètre (DHT^α) définie par

$$\mathbf{H}_N^\alpha = \text{Re}(\mathbf{F}_N^\alpha) - \text{Im}(\mathbf{F}_N^\alpha) \quad (2.25)$$

- **Relation entre DFT^α et DHT^α :**

Soient $\mathbf{F}^\alpha(n)$ et $\mathbf{H}^\alpha(n)$ la DFT^α et DHT^α , respectivement, d'une séquence réelle $s(k)$ et α un paramètre réel. La transformée $\mathbf{H}^\alpha(n)$ peut être présentée en fonction de $\mathbf{F}^\alpha(n)$ comme suit [13]

$$\mathbf{H}^\alpha(n) = \text{Re}(\mathbf{F}^\alpha(n)) - \text{Im}(\mathbf{F}^\alpha(n)) = \frac{1+j}{2} \mathbf{F}^\alpha(n) + \frac{1-j}{2} (\mathbf{F}^\alpha(n))^* \quad (2.26)$$

Et

$$\mathbf{F}^\alpha(n) = \frac{1-j}{2} \mathbf{H}^\alpha(n) + \frac{1+j}{2} \mathbf{H}^\alpha(N-n) \quad (2.27)$$

La DHT^α peut être calculée efficacement et rapidement en exploitant les algorithmes rapides existants de la DHT [55].

La matrice $\mathbf{H}_N^\alpha$ est une matrice involutive qui vérifie la relation (2.28) pour chaque valeur de N [30].

$$\mathbf{H}_N^\alpha \cdot \mathbf{H}_N^\alpha = N \mathbf{I}_N \quad (2.28)$$

Dans le cas où $\alpha = -\pi/8$, la matrice $\mathbf{H}_N^{-\pi/8}$ est équivalente à la matrice DHT classique pour n'importe quelle valeur de N .

2.5 Conclusion

Dans ce chapitre, nous avons présenté de manière générale les transformées paramétriques : les méthodes de construction des matrices paramétriques de ces transformées et leurs propriétés. Nous avons vu aussi que ces transformées possèdent des structures simples et exigent de faibles complexités de calcul par rapport à celles des autres transformées existantes. Dans les deux chapitres suivants, nous allons proposer des méthodes de cryptage d'images basées sur ces transformées, ainsi nous montrons que les paramètres indépendants de ces transformées peuvent être utilisés avec succès comme une clé supplémentaire dans le cryptage d'images.

Chapitre 3

*Méthodes proposées de cryptage
basé sur deux masques de
phases aléatoires*



3.1 Introduction

Les transformées discrètes jouent un rôle très important dans la cryptographie moderne. Cela est généralement dû au fait que ces transformées présentent des avantages intéressants concernant la sécurité, la complexité, la vitesse, la puissance de calcul, etc. En effet, une variété de techniques de cryptage d'images existantes sont basées sur des transformées discrètes [4]-[6], [56]-[58]. D'après l'état de l'art présenté dans le chapitre 1, les techniques qui répondent mieux aux exigences de la cryptographie sont celles qui exploitent le caractère aléatoire des transformées paramétriques, notamment les techniques proposées dans [5] et [6]. Cependant, les transformées fractionnaires présentent des complexités très élevées par rapport à celles des transformées paramétriques présentées dans le chapitre 2.

Dans ce chapitre, nous proposons deux méthodes de cryptage d'images basées sur les transformées paramétriques présentées dans le chapitre précédent; l'une exploite la transformée ROP et l'autre utilise la DFT paramétrique. Ces méthodes adoptent deux masques de phases aléatoires comme une clé secrète de cryptage et considèrent les paramètres indépendants des transformées paramétriques comme une clé secrète supplémentaire. Afin d'élargir l'espace de la clé supplémentaire (augmenter le nombre de paramètres indépendants dans le système de cryptage) et de simplifier le processus de cryptage/décryptage, nous considérons dans ces deux méthodes le cryptage en bloc. Alors, la sécurité de l'image dépend des masques aléatoires, des paramètres indépendants des transformées paramétriques et de la taille du bloc utilisé pour décomposer l'image originale. Afin de tester la robustesse de nos méthodes, nous présentons aussi, dans ce chapitre, des résultats de simulation correspondants à l'application de ces méthodes dans le cryptage des images de test.

3.2 Principe général de nos méthodes de cryptage d'images

Dans cette section, nous exposons le principe général des méthodes de cryptage d'images proposées dans ce chapitre. Dans le processus de cryptage, l'image originale $\mathbf{Q}$ de taille $M \times M$ est divisée en blocs de taille $N \times N$. Chaque bloc $\mathbf{Q}_i$, $i = 1, 2, \dots, M^2/N^2$, est multiplié élément-par-élément par une matrice de phase aléatoire $\Phi_i = [e^{j\phi_i(n,m)}]$ de taille

$N \times N$, où $\phi_i(n, m), i = 1, 2, \dots, M^2/N^2, 1 \leq n, m \leq N$, sont des bruits blancs, uniformément distribués dans l'intervalle $[0, 2\pi]$ et mutuellement indépendants. Le bloc résultant est transformé en domaine fréquentiel en appliquant une transformée bidimensionnelle en utilisant deux transformées paramétriques $\mathbf{T}_N^{1,i}$ et $\mathbf{T}_N^{2,i}$, ensuite on effectue une multiplication élément-par-élément dans le domaine fréquentiel du bloc résultant par une matrice de phases aléatoires $\boldsymbol{\phi}_i = [e^{j\phi_i(n, m)}]$ de taille $N \times N$, où $\phi_i(n, m), i = 1, 2, \dots, M^2/N^2, 1 \leq n, m \leq N$, sont des bruits blancs, uniformément distribués dans l'intervalle $[0, 2\pi]$ et mutuellement indépendants. Le bloc résultant est transformé en domaine spatial en appliquant une transformée bidimensionnelle en utilisant deux transformées paramétriques $\mathbf{T}_N^{3,i}$ et $\mathbf{T}_N^{4,i}$ pour obtenir le bloc crypté $\mathbf{E}_i$ correspondant au bloc original $\mathbf{Q}_i$ de l'image cryptée $\mathbf{E}$.

Le processus de décryptage est l'application inverse du processus de cryptage. Chaque bloc crypté $\mathbf{E}_i$ de l'image cryptée $\mathbf{E}$ est transformé en domaine fréquentiel en utilisant les transformées inverses $(\mathbf{T}_N^{3,i})^{-1}$ et $(\mathbf{T}_N^{4,i})^{-1}$, puis il est multiplié par une matrice de phase aléatoire $\boldsymbol{\phi}'_i = [e^{-j\phi'_i(n, m)}]$ de taille $N \times N$, où $\phi'_i(n, m), i = 1, 2, \dots, M^2/N^2, 1 \leq n, m \leq N$, sont des bruits blancs, uniformément distribués dans l'intervalle $[0, 2\pi]$ et mutuellement indépendants. Le bloc résultant est transformé ensuite en domaine spatial en utilisant les transformées inverses $(\mathbf{T}_N^{1,i})^{-1}$ et $(\mathbf{T}_N^{2,i})^{-1}$ et enfin il est multiplié par une matrice de phases aléatoires $\boldsymbol{\phi}'_i = [e^{-j\phi'_i(n, m)}]$ de taille $N \times N$, où $\phi'_i(n, m), i = 1, 2, \dots, M^2/N^2, 1 \leq n, m \leq N$, sont des bruits blancs, uniformément distribués dans l'intervalle $[0, 2\pi]$ et mutuellement indépendants. Le bloc résultant $\mathbf{D}_i$ représente le bloc décrypté de l'image décryptée $\mathbf{D}$.

Afin de montrer l'efficacité des méthodes de cryptage d'images proposées dans ce chapitre, spécifiquement l'importance de la clé secrète supplémentaire correspondante aux paramètres indépendants des matrices des transformées paramétriques, nous appliquons les deux méthodes proposées à six images de test aux niveaux de gris de taille 512×512 : Lena, Goldhill, boat, Barbara, Bridge et Baboon qui sont représentées dans la Figure 3.1 dont les histogrammes sont donnés dans Figure 3.2. On considère dans tous les tests de simulations que la clé secrète correspondant aux matrices aléatoires de phase est la même

pour les processus de cryptage et de décryptage. Nous réalisons l'étude sur les méthodes proposées en considérant des tailles de bloc différentes telles que 16×16 , 32×32 , 64×64 et 128×128 . En outre, afin d'augmenter le niveau de la sécurité de l'image cryptée, la clé de cryptage est changée pour chaque bloc. Ceci montre clairement que l'espace de la clé a considérablement augmenté. Les résultats et les tests de simulation présentés dans ce chapitre sont obtenus en implémentant les méthodes proposées sous MATLAB version 7.4.



Lena originale



Goldhill originale



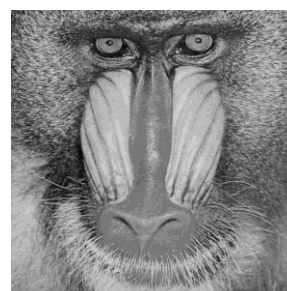
Boat originale



Barbara originale



Bridge originale



Baboon originale

Figure 3.1 Images de test utilisées dans la simulation

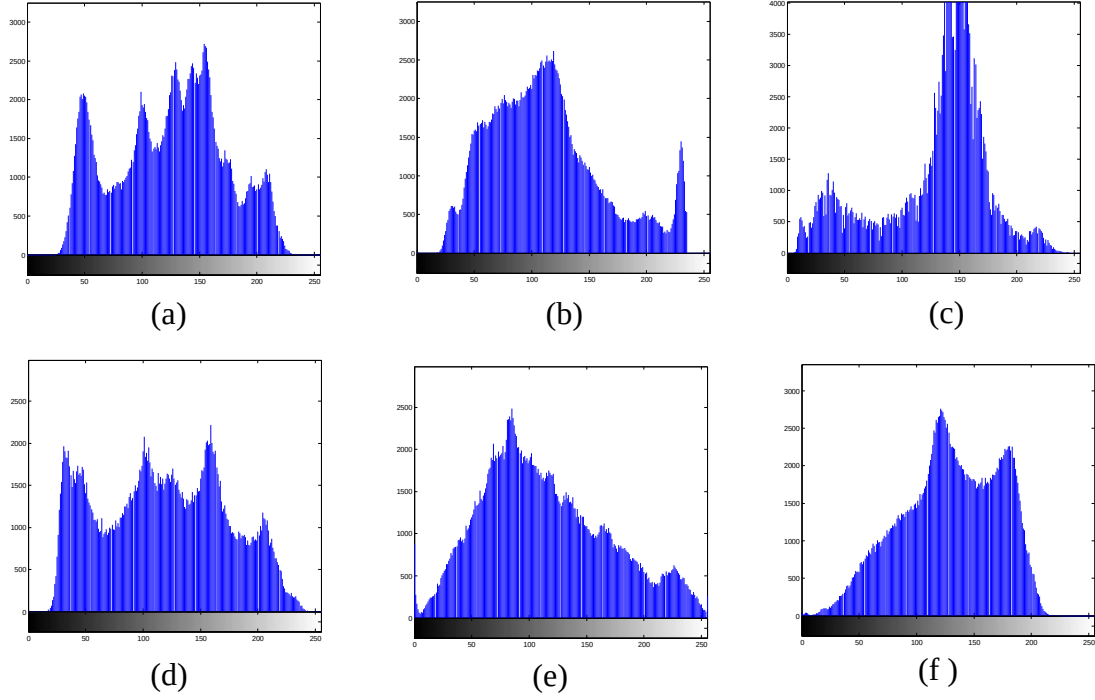


Figure 3.2 Histogrammes correspondants aux images de test utilisées

3.3 Méthode proposée pour le cryptage d'images dans le domaine de la transformée ROP

3.3.1 Développement de la méthode

Dans cette méthode, on utilise la transformée ROP [12] pour crypter l'image. Chaque bloc crypté $\mathbf{E}_i$, $i = 1, 2, \dots, M^2/N^2$, de l'image cryptée $\mathbf{E}$ de taille $M \times M$ est obtenu à partir du bloc $\mathbf{Q}_i$, $i = 1, 2, \dots, M^2/N^2$, de l'image originale $\mathbf{Q}$ de taille $M \times M$ comme suit

$$\mathbf{E}_i = \frac{1}{N^2} \left(\mathbf{T}_N^{\mathbf{y}_i} \left(\left(\mathbf{T}_N^{\mathbf{v}_i} (\mathbf{Q}_i \odot \boldsymbol{\phi}_i) \mathbf{T}_N^{\mathbf{w}_i} \right) \odot \boldsymbol{\phi}_i \right) \mathbf{T}_N^{\mathbf{z}_i} \right), \quad i = 1, 2, \dots, M^2/N^2 \quad (3.1)$$

avec les matrices de la transformée ROP $\mathbf{T}_N^{\mathbf{v}_i}$, $\mathbf{T}_N^{\mathbf{w}_i}$, $\mathbf{T}_N^{\mathbf{y}_i}$, et $\mathbf{T}_N^{\mathbf{z}_i}$ sont construites en utilisant les vecteurs paramétriques $\mathbf{v}_i$, $\mathbf{w}_i$, $\mathbf{y}_i$, et $\mathbf{z}_i$, respectivement, et $\odot$ dénote la multiplication élément-par-élément des matrices.

Tout bloc $\mathbf{E}_i$ de l'image originale utilise quatre transformées normalisées et chaque matrice ROP, $\mathbf{T}_N^{\mathbf{v}_i}$, $\mathbf{T}_N^{\mathbf{w}_i}$, $\mathbf{T}_N^{\mathbf{y}_i}$, et $\mathbf{T}_N^{\mathbf{z}_i}$, possède $N/2 - 1$ paramètres indépendants qui peuvent être choisis arbitrairement du plan complexe. Par conséquent, le processus de cryptage possède $2M^2$ phases aléatoires comme une clé de cryptage alors que les $(2N - 4)M^2/N^2$

paramètres indépendants peuvent être utilisés comme une clé supplémentaire pour le cryptage.

L'image décryptée $\mathbf{D}$ est obtenue à partir de l'image cryptée $\mathbf{E}$ dont le bloc décrypté $\mathbf{D}_i$ est donné par

$$\mathbf{D}_i = \frac{1}{N^2} \left(\left(\left(\mathbf{T}_N^{\mathbf{v}'_i} \right)^{\text{RT}} \left(\left(\left(\mathbf{T}_N^{\mathbf{y}'_i} \right)^{\text{RT}} \mathbf{E}_i \left(\mathbf{T}_N^{\mathbf{z}'_i} \right)^{\text{RT}} \right) \odot \boldsymbol{\phi}'_i \right) \left(\mathbf{T}_N^{\mathbf{w}'_i} \right)^{\text{RT}} \right) \odot \boldsymbol{\phi}'_i \right),$$

$$i = 1, 2, \dots, M^2/N^2 \quad (3.2)$$

où $\mathbf{T}_N^{\mathbf{v}'_i}$, $\mathbf{T}_N^{\mathbf{w}'_i}$, $\mathbf{T}_N^{\mathbf{y}'_i}$ et $\mathbf{T}_N^{\mathbf{z}'_i}$ sont les matrices ROP construites en utilisant les vecteurs paramétriques $\mathbf{v}'_i$, $\mathbf{w}'_i$, $\mathbf{y}'_i$, et $\mathbf{z}'_i$, respectivement.

D'après les équations (3.1) et (3.2), il est clair que le bloc décrypté $\mathbf{D}_i$ devient le bloc original $\mathbf{Q}_i$ quand $\left[e^{j\phi'_i(n,m)} \right] = \left[e^{j\phi_i(n,m)} \right]$, $\left[e^{j\phi'_i(n,m)} \right] = \left[e^{j\phi_i(n,m)} \right]$, $\mathbf{v}'_i = \mathbf{v}_i$, $\mathbf{w}'_i = \mathbf{w}_i$, $\mathbf{y}'_i = \mathbf{y}_i$, et $\mathbf{z}'_i = \mathbf{z}_i$, pour $i = 1, 2, \dots, M^2/N^2$.

Il faut noter que le processus de décryptage dans [6] utilise le conjugué complexe de l'image cryptée étant donné que la MPDFrFT est une transformée unitaire, tandis que dans le processus proposé de décryptage, on utilise le réciproque transposé des matrices ROP dû à la nature de la transformée ROP [12].

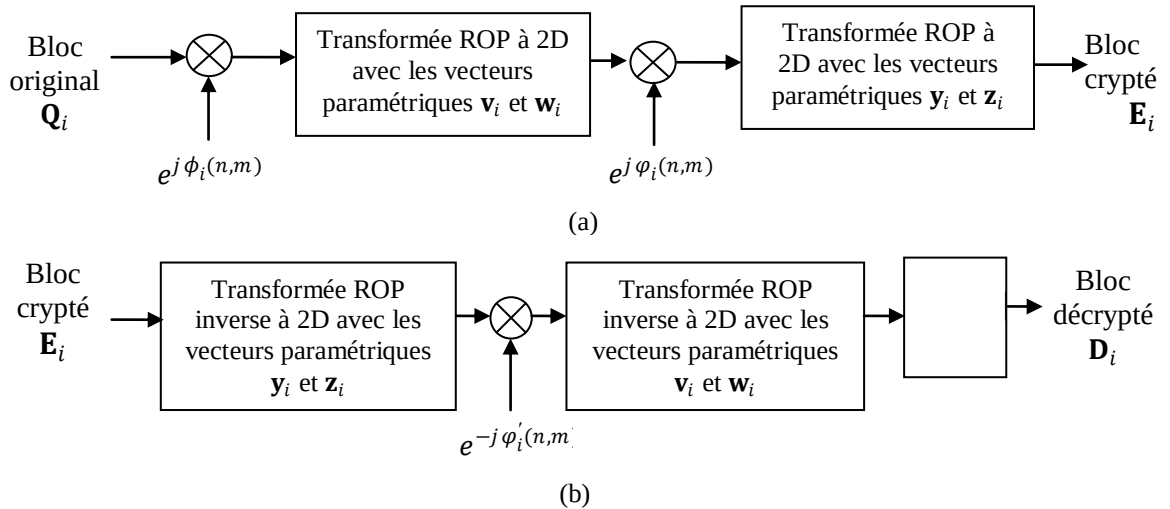


Figure 3.3 Cryptage par bloc proposé basé sur deux phases aléatoires et la transformée ROP: (a) schéma de cryptage d'un bloc, (b) schéma de décryptage d'un bloc

3.3.2 Application de la méthode : Résultats de simulation

Nous avons effectué la simulation sur les différentes images de test présentées précédemment. Cependant, nous présentons seulement les résultats de quelques images de test comme un exemple d'illustration. Les images cryptées sont données dans les Figures 3.4 et 3.5 en considérant des tailles de blocs différentes, tandis que la Figure 3.6 montre les images décryptées correspondantes en utilisant des paramètres incorrects (clé secrète supplémentaire fausse). Dans cette méthode, le nombre de paramètres indépendants utilisés dans le processus de cryptage est montré dans le Tableau 3.1 selon la taille du bloc utilisé.

Tableau 3.1 Nombre de paramètres correspondant à la taille du bloc

Taille du bloc	Nombre de paramètres indépendants
512×512	1020
256×256	2032
128×128	4032
64×64	7936
32×32	15360
16×16	28672

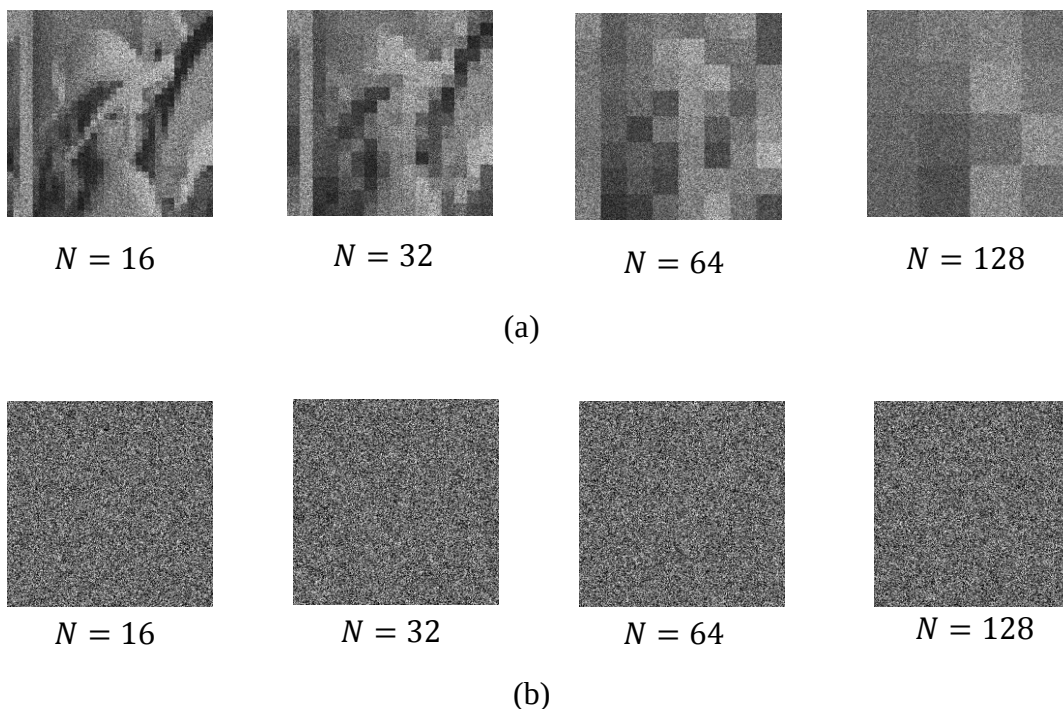


Figure 3.4 Image de test Lena cryptée en utilisant des tailles de bloc différentes :

$N = 16$, $N = 32$, $N = 64$ et $N = 128$: (a) L'amplitude, (b) La phase

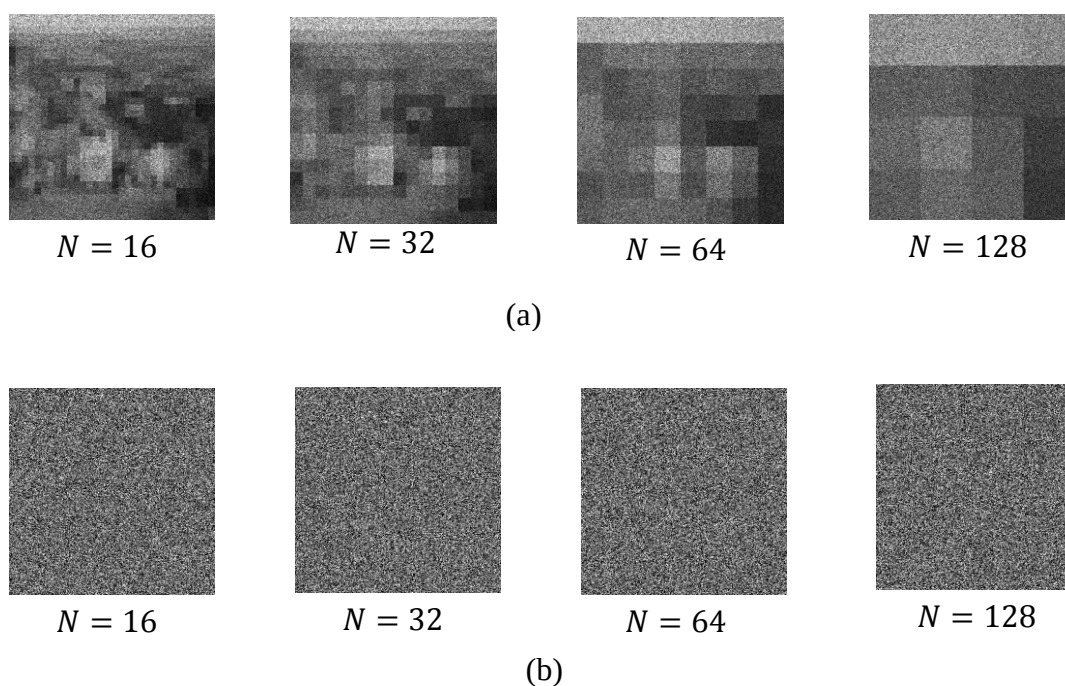


Figure 3.5 Image de test Goldhill cryptée en utilisant des tailles de bloc différentes : $N = 16$, $N = 32$, $N = 64$ et $N = 128$: (a) L'amplitude, (b) La phase

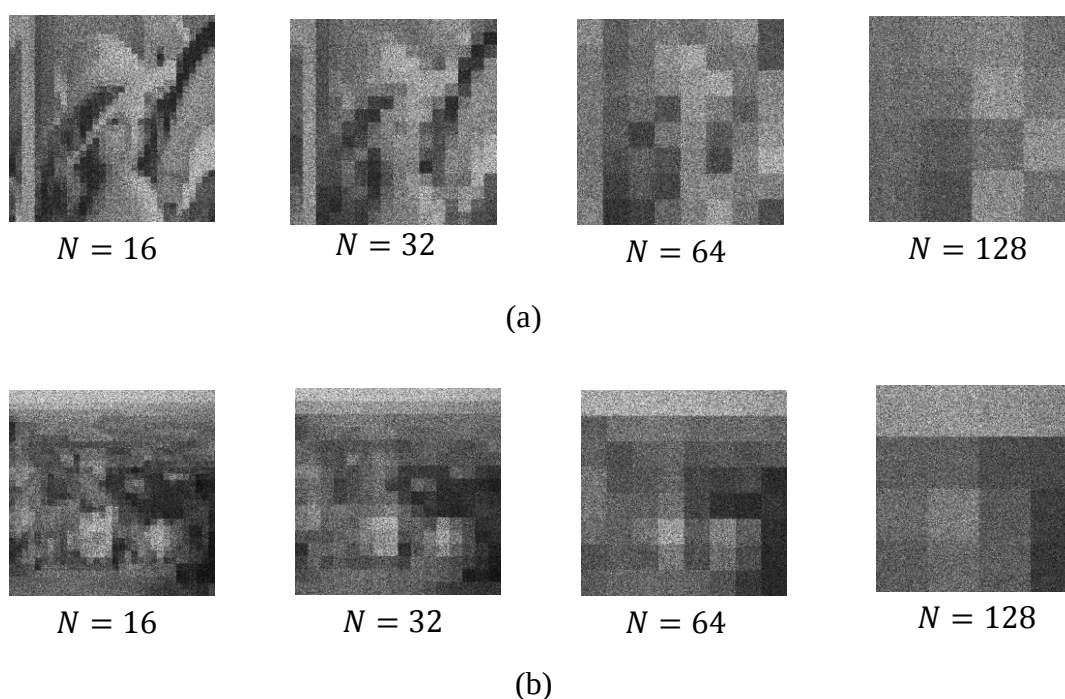


Figure 3.6 Images décryptées en utilisant des paramètres incorrects pour des tailles de bloc différentes : $N = 16$, $N = 32$, $N = 64$ et $N = 128$. (a) Lena, (b) Goldhill.

D'après ces figures, il est clair que l'image originale ne peut pas être récupérée si les paramètres utilisés dans le processus de décryptage sont incorrects. On note également de toutes les expériences effectuées que l'image cryptée devient similaire à un bruit quand les blocs utilisés sont de grande taille.

Nous évaluons objectivement les performances de la méthode proposée. Pour cela, les résultats de test des mesures de coefficient de corrélation de l'image cryptée et le PSNR de l'image décryptée en utilisant des paramètres incorrects sont présentés dans les Tableaux suivants pour les images de test utilisées en considérant des blocs de différentes tailles où r_{xy_r} représente le coefficient de corrélation de la partie réelle de l'image cryptée et l'image originale et r_{xy_i} est la valeur de corrélation entre la partie imaginaire de l'image cryptée et l'image originale. Les résultats obtenus confirment l'efficacité et la robustesse de la méthode proposée.

Tableau 3.2 Evaluation objective en termes de PSNR des images de test décryptées

Images de test	$N = 16$	$N = 32$	$N = 64$	$N = 128$
Lena	5.6405	5.3639	4.9378	4.6225
Goldhill	6.3751	6.1756	5.9154	5.4135
Boat	5.2580	5.0233	4.8265	4.6038
Barbara	5.6067	5.2303	4.7853	4.4499
Bridge	5.7072	5.4430	5.1524	4.6897
Baboon	5.2317	5.0677	4.8827	4.7405

Tableau 3.3 Evaluation objective en termes de coefficient de corrélation des parties réelles et imaginaires des images de test cryptées

Images de test	N = 16		N = 32		N = 64		N = 128	
	r_{xy_r}	r_{xy_i}	r_{xy_r}	r_{xy_i}	r_{xy_r}	r_{xy_i}	r_{xy_r}	r_{xy_i}
Lena	0.0029	0.0013	0.0026	-0.0023	0.0017	0.0040	-0.0015	0.0018
Goldhill	0.0029	-0.0015	-0.0020	-0.0051	-0.0016	0.0012	0.0015	-0.0013
Boat	-0.0022	0.0007	0.0010	-0.00017	-0.0006	-0.00067	-0.00038	-0.00084
Barbara	0.0024	0.0038	0.0012	-0.0027	-0.00043	0.0036	-0.00016	0.0018
Bridge	-0.0019	-0.0046	0.0011	0.0022	0.00088	-0.0042	0.00052	-0.0027
Baboon	0.0011	0.0017	0.0024	0.00046	-0.0035	-0.00054	-0.00082	-0.00099

Afin de tester l'efficacité de la méthode proposée, nous effectuons une analyse d'histogramme, la Figure 3.7 présente l'histogramme de l'image Lena cryptée en utilisant des blocs d'ordre 64.

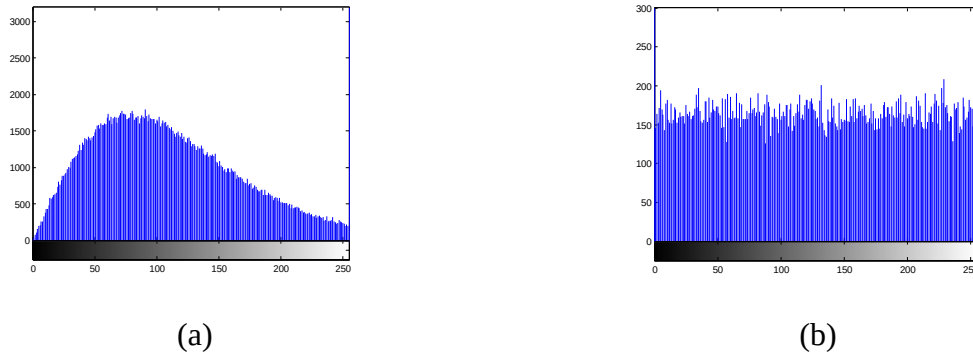


Figure 3.7 Histogramme de Lena cryptée par des blocs d'ordre 64 : (a) histogramme de l'amplitude, (b) histogramme de la phase.

La Figure 3.7 montre bien que l'histogramme de l'image cryptée est totalement différent de celui de l'image originale, et a une distribution totalement aléatoire.

Pour un système de cryptage d'image sécurisé, l'espace de la clé doit être suffisamment grand pour rendre l'attaque par force brute impossible. Pour les méthodes proposées de cryptage, la clé secrète se compose des matrices de phases aléatoires et de la

clé secrète supplémentaire qui comprend les paramètres indépendants des matrices paramétriques. La clé secrète supplémentaire dépend de la largeur de l'image et de la taille du bloc utilisé. Dans le cas des images de test de taille 512×512 et des blocs de taille 64×64 , la taille de la clé supplémentaire est $p = 7936$ paramètres indépendants qui peuvent être choisis du plan complexe.

Pour tester la robustesse de la méthode proposée contre l'attaque par force brute et pour illustrer les effets des erreurs de la clé secrète supplémentaire sur l'image décryptée, nous effectuons des expériences en considérant dans le processus de décryptage que seulement une partie du nombre de paramètres indépendants $p = (2N - 4)M^2/N^2$ est incorrecte (une partie de la clé secrète supplémentaire est incorrecte). Les résultats de cette étude pour l'image de test Lena sont donnés dans la Figure 3.8, qui montre clairement que la méthode proposée est très sensible aux erreurs sur la clé secrète supplémentaire et par conséquent, elle est robuste contre l'attaque par force brute.

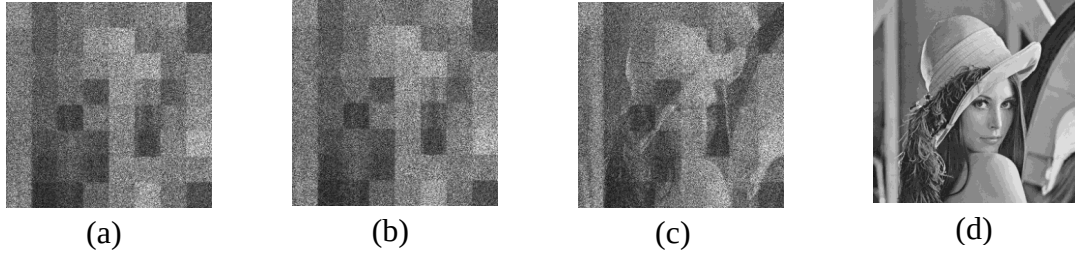


Figure 3.8 Image de test Lena décryptée par des blocs d'ordre 64 avec: (a) $3p/4$ paramètres incorrects, (b) $p/2$ paramètres incorrects, (c) $p/4$ paramètres incorrects, (d) paramètres corrects.

3.4 Méthode proposée pour le cryptage d'images dans le domaine de la DFT paramétrique

3.4.1 Développement de la méthode

Le cryptage de l'image se fait bloc par bloc, chaque bloc $\mathbf{Q}_i$, $i = 1, 2, \dots, M^2/N^2$, de l'image originale $\mathbf{Q}$ est cryptée en utilisant quatre matrices de la DFT de trois

paramètres présentée dans le chapitre précédent, $\mathbf{F}_N^{a_i, b_i, c_i}$, $\mathbf{F}_N^{d_i, e_i, f_i}$, $\mathbf{F}_N^{\alpha_i, \beta_i, \gamma_i}$ et $\mathbf{F}_N^{\delta_i, \varepsilon_i, \sigma_i}$. Le bloc crypté $\mathbf{E}_i$, $i = 1, 2, \dots, M^2/N^2$, de l'image cryptée $\mathbf{E}$ est donné par

$$\mathbf{E}_i = \frac{1}{N^2} \left(\mathbf{F}_N^{\alpha_i, \beta_i, \gamma_i} \left(\left(\mathbf{F}_N^{a_i, b_i, c_i} (\mathbf{Q}_i \odot \boldsymbol{\Phi}_i) \mathbf{F}_N^{d_i, e_i, f_i} \right) \odot \boldsymbol{\Phi}_i \right) \mathbf{F}_N^{\delta_i, \varepsilon_i, \sigma_i} \right),$$

$$i = 1, 2, \dots, M^2/N^2 \quad (3.3)$$

Le bloc décrypté $\mathbf{D}_i$ de l'image décryptée $\mathbf{D}$ est obtenu à partir du bloc crypté correspondant $\mathbf{E}_i$ de l'image cryptée $\mathbf{E}$ comme suit

$$\mathbf{D}_i = \frac{1}{N^2} \left(\left(\left(\mathbf{F}_N^{a_i', b_i', c_i'} \right)^* \left(\left(\left(\mathbf{F}_N^{\alpha_i', \beta_i', \gamma_i'} \right)^* \mathbf{E}_i \left(\mathbf{F}_N^{\delta_i', \varepsilon_i', \sigma_i'} \right)^* \right) \odot \boldsymbol{\Phi}_i' \right) \left(\mathbf{F}_N^{d_i', e_i', f_i'} \right)^* \right) \odot \boldsymbol{\Phi}_i' \right),$$

$$i = 1, 2, \dots, M^2/N^2 \quad (3.4)$$

où $(.)^*$ dénote le transposé du conjugué complexe des matrices.

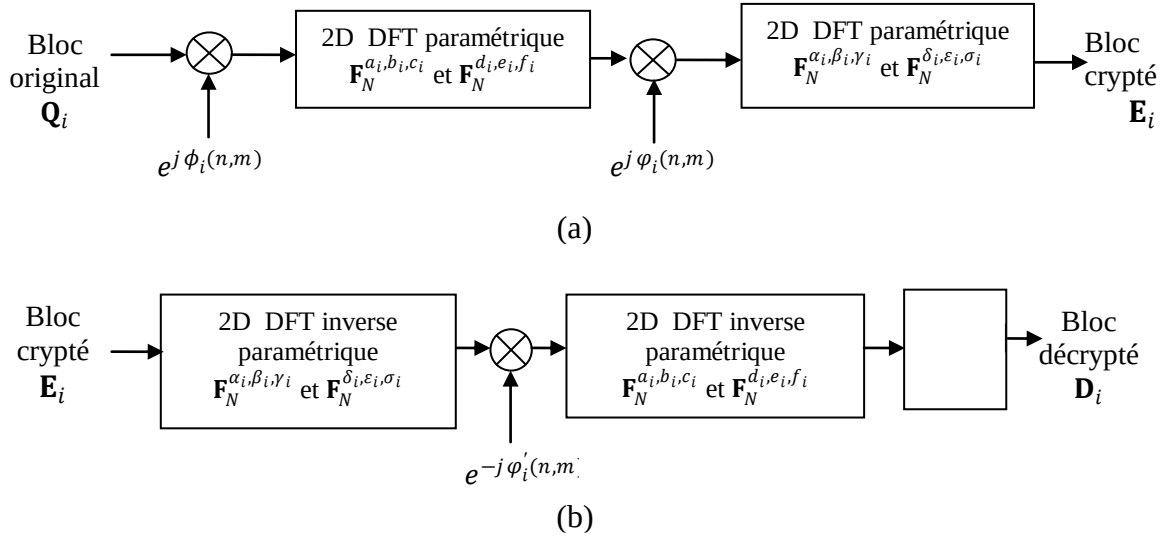


Figure 3.9 Cryptage proposé en utilisant la DFT paramétrique: (a) schéma de cryptage par bloc, (b) schéma de décryptage par bloc

En plus de la clé de cryptage, $2M^2$ phases aléatoires correspondantes aux matrices de phases aléatoires, le processus de cryptage utilise $12M^2/N^2$ paramètres $a_i, b_i, c_i, d_i, e_i, f_i, \alpha_i, \beta_i, \gamma_i, \delta_i, \varepsilon_i, \sigma_i$, $i = 1, 2, \dots, M^2/N^2$, correspondants aux paramètres indépendants des matrices paramétriques de la DFT. Ces paramètres peuvent être choisis

arbitrairement du cercle unité. Pour récupérer l'image originale à partir de l'image cryptée, il est nécessaire d'utiliser les clés de cryptage dans le processus de décryptage, i.e., $[e^{j\phi'_i(n,m)}] = [e^{j\phi_i(n,m)}]$, $[e^{j\phi'_i(n,m)}] = [e^{j\phi_i(n,m)}]$, $a'_i = a_i, b'_i = b_i, c'_i = c_i, d'_i = d_i, e'_i = e_i, f'_i = f_i, \alpha'_i = \alpha_i, \beta'_i = \beta_i, \gamma'_i = \gamma_i, \delta'_i = \delta_i, \varepsilon'_i = \varepsilon_i, \sigma'_i = \sigma_i$, pour $i = 1, 2, \dots, M^2/N^2$.

3.4.2 Application de la méthode : Résultats de simulation

La DFT paramétrique utilisée dans le processus de cryptage possède trois paramètres, par conséquent le nombre de paramètres indépendants utilisés est montré dans le Tableau 3.4 selon la taille du bloc utilisé.

Tableau 3.4 Nombre de paramètres correspondant à la taille du bloc

Taille du bloc	Nombre de paramètres indépendants
512×512	12
256×256	48
128×128	192
64×64	768
32×32	3072
16×16	12288

Les Figures 3.10 et 3.11 représentent les images cryptées basées sur des blocs de tailles différentes, et la Figure 3.12 montre bien que l'image originale ne peut pas être récupérée quand les paramètres des matrices DFT paramétriques utilisés dans le processus de décryptage sont incorrects.

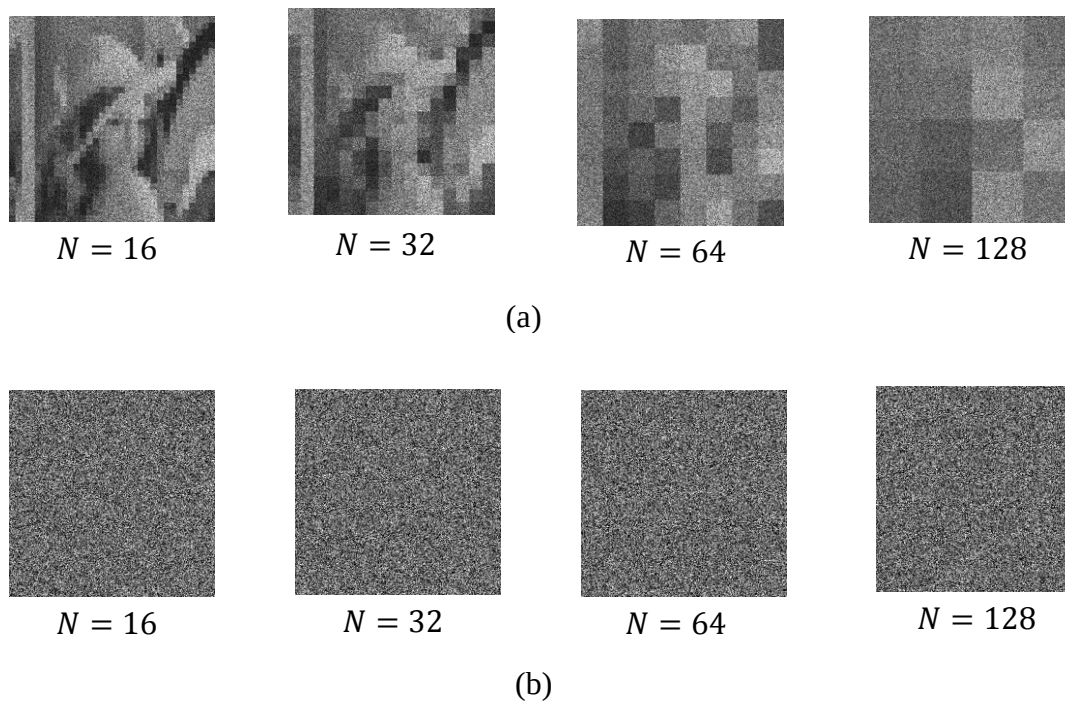


Figure 3.10 Image de Lena cryptée en utilisant des tailles de bloc différentes: $N = 16$, $N = 32$, $N = 64$ et $N = 128$: (a) L'amplitude, (b) La phase

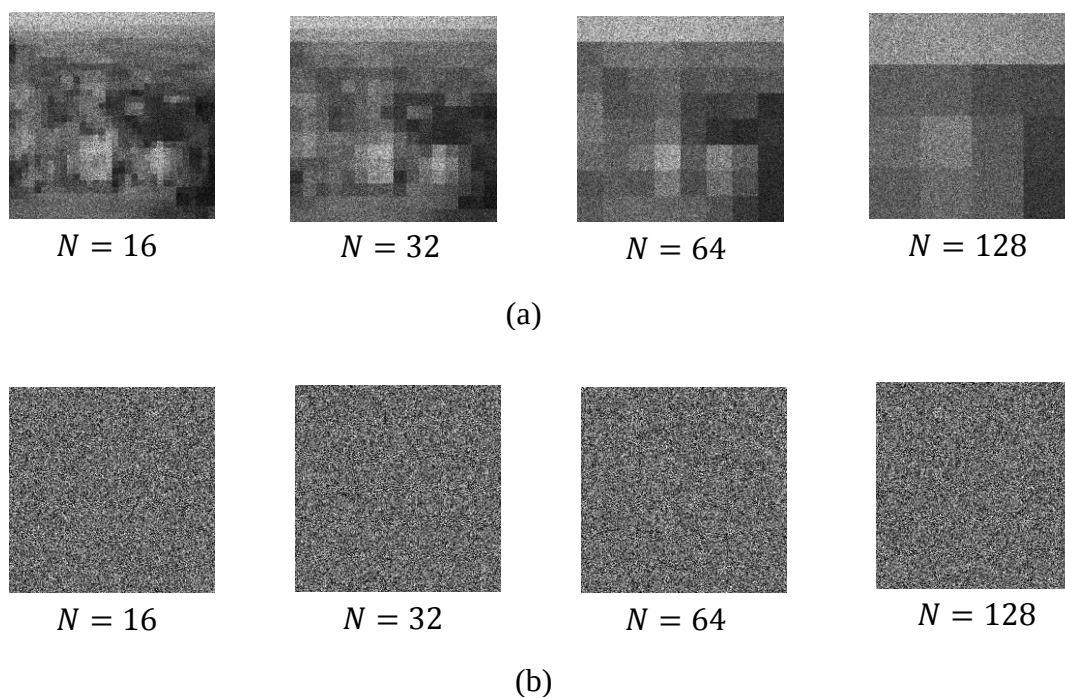


Figure 3.11 Image de Goldhill cryptée en utilisant des tailles de bloc différentes: $N = 16$, $N = 32$, $N = 64$ et $N = 128$: (a) L'amplitude, (b) La phase

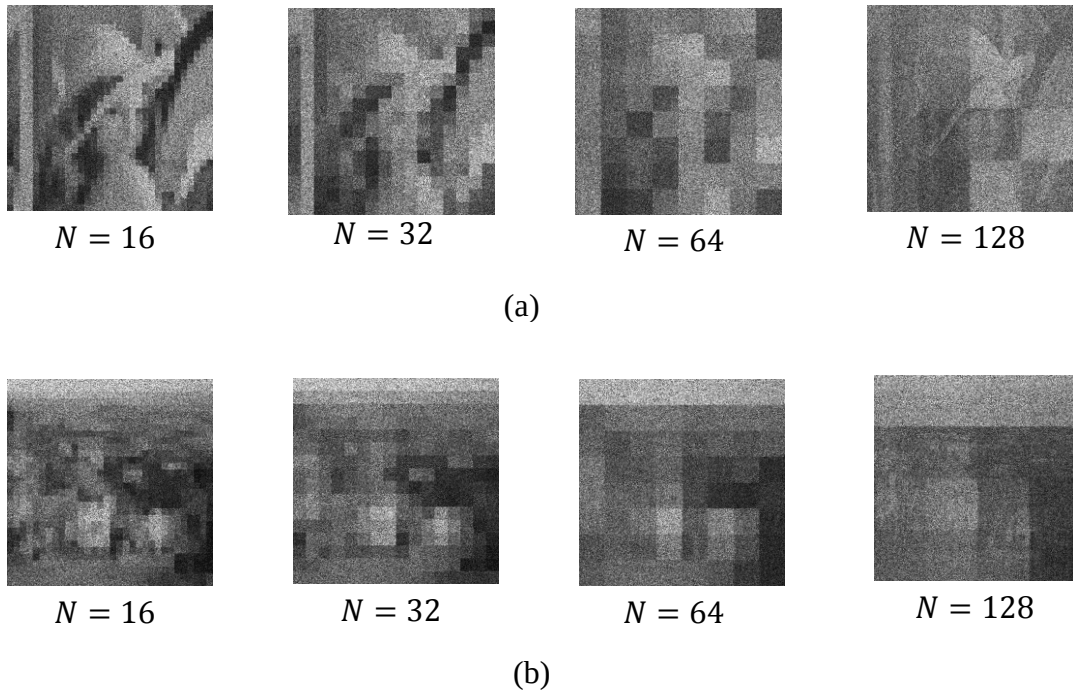


Figure 3.12 Images décryptées en utilisant des paramètres incorrects pour des tailles de bloc différentes: $N = 16$, $N = 32$, $N = 64$ et $N = 128$. (a) Lena, (b) Goldhill.

D'après les Figures 3.10, 3.11 et 3.12, on peut remarquer que l'image cryptée devient semblable à un bruit quand les blocs utilisés sont de grande taille. Cependant, le décryptage est plus robuste dans le cas du bloc d'ordre 64. Par conséquent, la méthode proposée basée sur le bloc d'ordre 64 est plus efficace pour les processus de cryptage et de décryptage.

Tableau 3.5 Evaluation objective en termes de PSNR des images de test décryptées

Images de test	$N = 16$	$N = 32$	$N = 64$	$N = 128$
Lena	5.5581	5.3015	5.0371	5.0949
Goldhill	6.3491	6.1563	6.0374	6.1183
Boat	5.2028	4.9798	4.9104	5.0107
Barbara	5.5566	5.1993	4.9095	5.0685
Bridge	5.5947	5.4057	5.2948	5.3137
Baboon	5.1713	5.0273	4.9815	5.1793

Tableau 3.6 Evaluation objective en termes de coefficient de corrélation des parties réelles et imaginaires des images de test cryptées

Images de test	N = 16		N = 32		N = 64		N = 128	
	r_{xy_r}	r_{xy_i}	r_{xy_r}	r_{xy_i}	r_{xy_r}	r_{xy_i}	r_{xy_r}	r_{xy_i}
Lena	0.4471	0.4464	0.3723	0.3758	0.2532	0.2779	0.1227	0.2297
Goldhill	0.5202	0.5234	0.4784	0.4830	0.4189	0.4444	0.2857	0.4003
Boat	0.3892	0.3892	0.3195	0.3232	0.2489	0.2804	0.1649	0.2465
Barbara	0.4815	0.4851	0.3952	0.4007	0.2814	0.3097	0.1728	0.2934
Bridge	0.4684	0.4699	0.4076	0.4076	0.3466	0.3798	0.2300	0.3438
Baboon	0.2799	0.2851	0.2346	0.2399	0.1670	0.1995	0.1030	0.2025

L'analyse d'histogramme de l'image cryptée montre que l'histogramme de l'amplitude a une distribution Gaussienne tandis que celui de la phase a une distribution uniforme, cette distribution aléatoire est totalement différente de celle d'histogramme de l'image originale, voir la Figure 3.13.

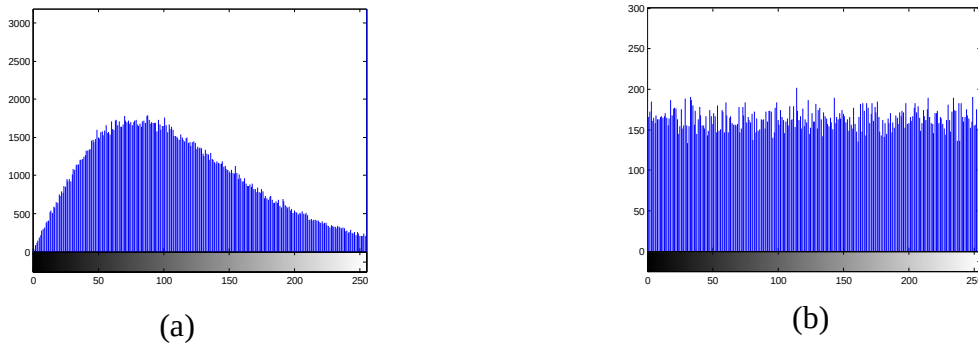


Figure 3.13 Histogramme de Lena cryptée par des blocs d'ordre 64: (a) histogramme de l'amplitude, (b) histogramme de la phase.

Les résultats de simulation de l'attaque par force brute de l'image cryptée et l'effet des erreurs sur la clé secrète supplémentaire de taille $p = 768$ paramètres indépendants qui peuvent être choisis du cercle unité sur l'image décryptée sont présentés dans la Figure 3.14.

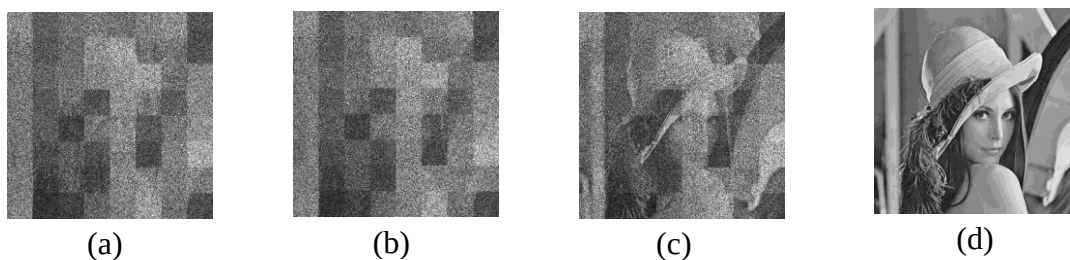


Figure 3.14 Image de Lena décryptée par des blocs d'ordre 64 avec: (a) $3p/4$ paramètres incorrects, (b) $p/2$ paramètres incorrects, (c) $p/4$ paramètres incorrects, (d) paramètres corrects.

La Figure 3.14 montre que la méthode proposée est très sensible aux erreurs sur la clé secrète supplémentaire et par conséquent, elle est robuste contre l'attaque par force brute.

3.5 Conclusion

Nous avons proposé dans ce chapitre deux méthodes de cryptage d'images par bloc basées sur deux masques de phases aléatoires en utilisant la transformée ROP et la DFT paramétrique. Nous avons montré que les paramètres indépendants de ces transformées paramétriques peuvent être utilisés avec succès comme une clé secrète supplémentaire pour le cryptage d'images. Les résultats de simulation présentés dans ce chapitre montrent clairement que ces deux méthodes sont très efficaces et robustes contre les attaques, comme l'analyse d'histogramme et l'attaque par force brute. En plus, du fait que nos méthodes exploitent efficacement deux transformées paramétriques à valeurs complexes qui ont des complexités faibles par rapport à celles des autres transformées paramétriques à valeurs complexes existantes, elles sont plus attractives que les méthodes de cryptage d'images existantes qui exploitent ces dernières. Dans le chapitre suivant, nous allons considérer le cas des transformées à valeurs réelles.

Chapitre 4

*Méthodes proposées de cryptage
basé sur deux masques
d'amplitudes aléatoires*



4.1 Introduction

Les méthodes de cryptage basées sur deux masques de phases aléatoires proposées dans le chapitre précédent sont efficaces du point de vue sécurité. Cependant, l'image cryptée obtenue dans ces méthodes est complexe. Cela est dû essentiellement à l'utilisation des transformées paramétriques à valeurs complexes. Afin de concevoir des systèmes de cryptage d'images dont l'image cryptée est purement réelle, nous exploitons dans ce chapitre la nature réelle des transformées paramétriques présentées dans le chapitre 2. Par conséquent, nous proposons ici trois méthodes de cryptage d'images basées sur deux masques d'amplitudes aléatoires; l'une utilise la DHT paramétrique et les deux autres exploitent la transformée ROP à valeurs réelles. Nous considérons dans ces méthodes le cryptage en bloc afin d'élargir l'espace de la clé supplémentaire. L'objectif principal de ces méthodes est d'augmenter le niveau de la sécurité de l'image cryptée tout en réduisant considérablement la complexité des calculs. Afin de tester la robustesse de nos méthodes, nous présentons aussi, dans ce chapitre, des résultats de simulation correspondants à l'application de ces méthodes dans le cryptage des images de test.

4.2 Principe général de nos méthodes de cryptage d'images

Nous présentons dans cette section le principe général des méthodes proposées dans ce chapitre pour le cryptage d'images. L'algorithme des méthodes proposées consiste à diviser l'image originale $\mathbf{Q}$ de taille $M \times M$, dans un premier temps, en blocs $\mathbf{Q}_i$ de taille $N \times N$. Après la décomposition de l'image, chaque bloc $\mathbf{Q}_i$, $i = 1, 2, \dots, M^2/N^2$, est crypté en utilisant deux matrices d'amplitudes aléatoires $\boldsymbol{\Phi}_i = [\phi_i(n, m)]$ et $\boldsymbol{\varphi}_i = [\varphi_i(n, m)]$ de taille $N \times N$, avec $\phi_i(n, m)$ et $\varphi_i(n, m)$, $1 \leq n, m \leq N$, sont des bruits blancs, non nuls, uniformément distribués dans l'intervalle $[-4, 4]$ et mutuellement indépendants, et quatre transformées paramétriques à valeurs réelles $\mathbf{T}_N^{1,i}$, $\mathbf{T}_N^{2,i}$, $\mathbf{T}_N^{3,i}$ et $\mathbf{T}_N^{4,i}$ comme suit

- Le bloc original $\mathbf{Q}_i$ est multiplié élément-par-élément par une matrice d'amplitudes aléatoires $\boldsymbol{\Phi}_i$.
- Transformer le bloc résultant en domaine fréquentiel en appliquant une transformée bidimensionnelle en utilisant les transformées paramétriques $\mathbf{T}_N^{1,i}$ et $\mathbf{T}_N^{2,i}$ à valeurs réels.

- Le bloc transformé est multiplié élément-par-élément dans le domaine fréquentiel par une autre matrice d'amplitudes aléatoires ϕ_i .
- Enfin, une transformation bidimensionnelle est appliquée au bloc résultant en utilisant les transformées paramétriques $\mathbf{T}_N^{3,i}$ et $\mathbf{T}_N^{4,i}$ pour revenir au domaine spatial. La matrice obtenue représente le bloc crypté $\mathbf{E}_i$ correspondant au bloc original $\mathbf{Q}_i$.

Le schéma bloc du processus de cryptage proposé est présenté dans la figure 4.1(a). L'application inverse du processus de cryptage permet de reconstituer l'image originale. La Figure 4.1(b) illustre le processus de décryptage.

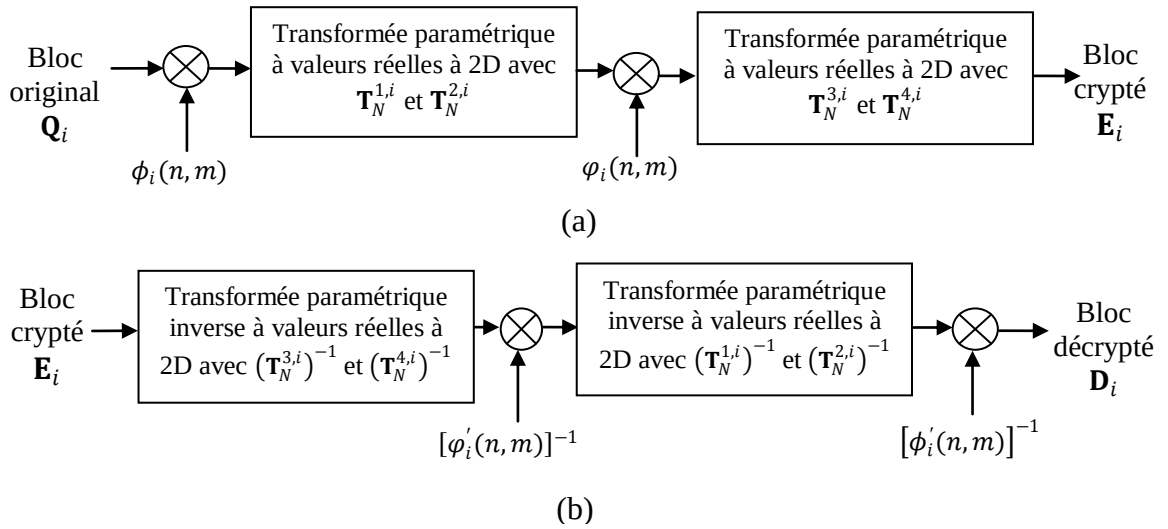


Figure 4.1 Processus de cryptage d'image par bloc proposé en utilisant deux masques d'amplitudes aléatoires et des transformées paramétriques à valeurs réelles: (a) schéma de cryptage, (b) schéma de décryptage

Chaque bloc crypté $\mathbf{E}_i$ de l'image cryptée $\mathbf{E}$ est transformé en domaine fréquentiel en utilisant les transformées inverses $(\mathbf{T}_N^{3,i})^{-1}$ et $(\mathbf{T}_N^{4,i})^{-1}$, puis il est multiplié par une matrice d'amplitude aléatoire $(\phi'_i)^{-1} = 1/\phi'_i(n, m)$ de taille $N \times N$, où $\phi'_i(n, m), i = 1, 2, \dots, M^2/N^2, 1 \leq n, m \leq N$, sont des bruits blancs, non nuls, uniformément distribués dans l'intervalle $[-4, 4]$ et mutuellement indépendants. Le bloc résultant est transformé ensuite en domaine spatial en utilisant les transformées inverses $(\mathbf{T}_N^{1,i})^{-1}$ et $(\mathbf{T}_N^{2,i})^{-1}$ et

enfin il est multiplié par une matrice d'amplitude aléatoires $(\Phi'_i)^{-1} = 1/\phi'_i(n, m)$ de taille $N \times N$, où $\phi'_i(n, m)$, $i = 1, 2, \dots, M^2/N^2$, $1 \leq n, m \leq N$, sont des bruits blancs, uniformément distribués dans l'intervalle $[-4, 4]$ et mutuellement indépendants. Le bloc résultant $\mathbf{D}_i$ représente le bloc décrypté de l'image décryptée $\mathbf{D}$.

Les méthodes de cryptage d'images proposées dans ce chapitre sont implémentées sous MATLAB pour montrer l'importance de la clé secrète supplémentaire correspondante aux paramètres indépendants des matrices des transformées paramétriques. De ce fait, la clé secrète correspondante aux matrices d'amplitudes aléatoires est considérée la même pour le processus de cryptage et de décryptage. La réalisation de cette étude est faite en considérant des tailles de bloc différentes telles que 16×16 , 32×32 , 64×64 et 128×128 . Afin d'élargir l'espace de la clé et par conséquent d'augmenter le niveau de la sécurité de l'image cryptée, la clé de cryptage est changée pour chaque bloc. Les algorithmes de cryptage sont appliqués sur différentes images de test présentées dans la Figure 3.1 dont les histogrammes sont donnés dans la Figure 3.2.

4.3 Méthode proposée pour le cryptage d'images dans le domaine de la DHT paramétrique

4.3.1 Développement de la méthode

La transformée paramétrique utilisée dans cette méthode est la DHT paramétrique [13] présentée dans le chapitre 2. On considère les matrices paramétriques $\mathbf{H}_N^{\alpha_i}$, $\mathbf{H}_N^{\beta_i}$, $\mathbf{H}_N^{\gamma_i}$ et $\mathbf{H}_N^{\delta_i}$, avec α_i , β_i , γ_i , δ_i , $i = 1, 2, \dots, M^2/N^2$, sont des paramètres réels indépendants qui peuvent être choisis arbitrairement de l'intervalle $[0, 2\pi]$. Le cryptage d'image dans ce cas est réalisé dans le domaine de la DHT paramétrique. La Figure 4.2 illustre le processus de cryptage proposé.

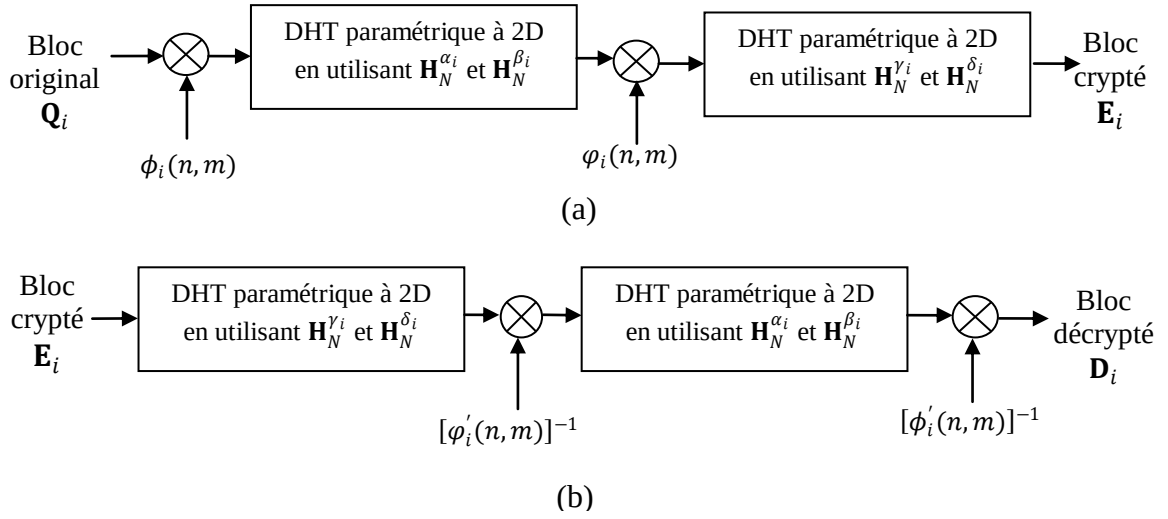


Figure 4.2 Processus de cryptage d'image par bloc proposé en utilisant deux masques d'amplitudes aléatoires dans le domaine de la DHT paramétrique: (a) schéma de cryptage, (b) schéma de décryptage

Le processus de cryptage du bloc Q_i peut être exprimé mathématiquement comme suit

$$E_i = \frac{1}{N^2} \left(H_N^{\gamma_i} \left(\left(H_N^{\alpha_i} (Q_i \odot \phi_i) H_N^{\beta_i} \right) \odot \phi_i \right) H_N^{\delta_i} \right), \quad i = 1, 2, \dots, M^2/N^2 \quad (4.1)$$

D'après l'équation 4.1, on peut remarquer que le processus de cryptage possède $2M^2$ amplitudes aléatoires comme une clé de cryptage et $4M^2/N^2$ paramètres indépendants qui peuvent être utilisés comme une clé supplémentaire pour le cryptage.

Le bloc décrypté D_i peut être obtenu facilement à partir du bloc correspondant E_i de l'image cryptée E comme suit

$$D_i = \frac{1}{N^2} \left(\left(H_N^{\alpha_i'} \left(\left(H_N^{\gamma_i'} E_i H_N^{\delta_i'} \right) \odot (\phi_i')^{-1} \right) H_N^{\beta_i'} \right) \odot (\phi_i')^{-1} \right), \quad i = 1, 2, \dots, M^2/N^2 \quad (4.2)$$

où $\mathbf{H}_N^{\alpha'_i}$, $\mathbf{H}_N^{\beta'_i}$, $\mathbf{H}_N^{\gamma'_i}$ et $\mathbf{H}_N^{\delta'_i}$ sont des matrices DHT de paramètres α'_i , β'_i , γ'_i et δ'_i , respectivement. Dans le cas où $\alpha'_i = \alpha_i$, $\beta'_i = \beta_i$, $\gamma'_i = \gamma_i$, $\delta'_i = \delta_i$, et $\boldsymbol{\Phi}'_i = \boldsymbol{\Phi}_i$, $\boldsymbol{\varphi}'_i = \boldsymbol{\varphi}_i$, $i = 1, 2, \dots, M^2/N^2$, le bloc décrypté $\mathbf{D}_i$ est identique au bloc original $\mathbf{E}_i$.

Dans le processus de décryptage proposé dans [6], le conjugué complexe de l'image cryptée est utilisé étant donné que la MPDFrFT est une transformée unitaire, tandis que le réciproque transposé des matrices ROP est utilisé dans [11] dû à la nature de la transformée ROP. Par contre, dans notre méthode, les matrices utilisées dans le processus de décryptage sont identiques à celles utilisées dans le processus de cryptage parce que la DHT paramétrique est une transformée involutive. C'est l'un des avantages de notre méthode.

4.3.2 Application de la méthode : Résultats de simulation

Nous présentons dans cette section les résultats de simulation de quelques images de test comme un exemple illustratif. La Figure 4.3 présente les images cryptées en considérant des tailles de blocs différentes, tandis que la Figure 4.4 montre les images décryptées correspondantes en utilisant des paramètres incorrects (clé secrète supplémentaire fausse).

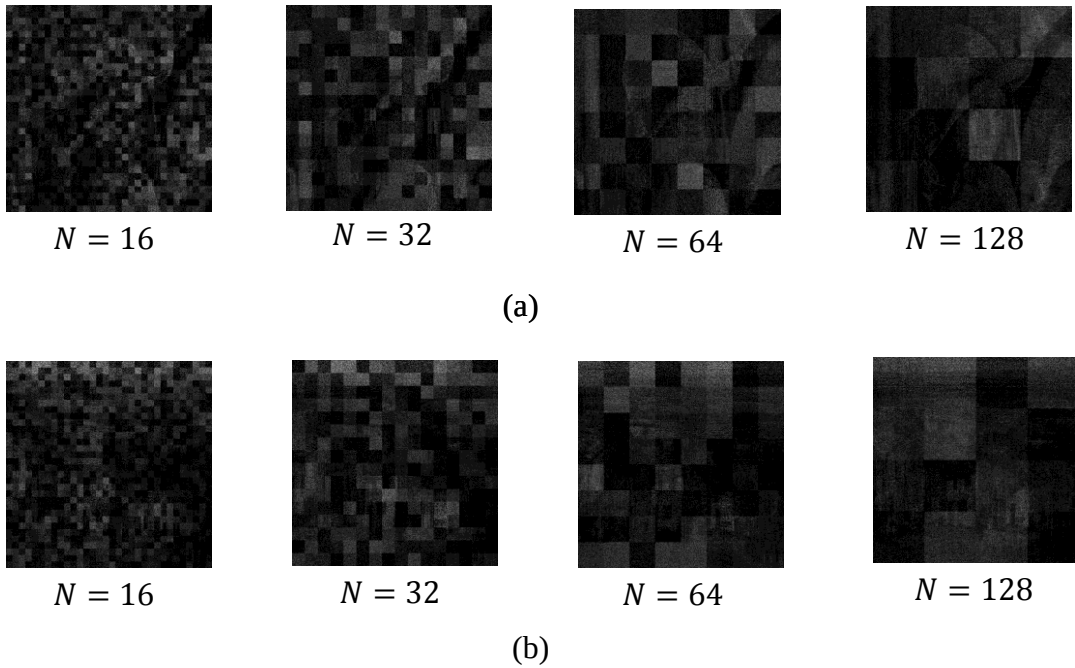


Figure 4.3 Images cryptées par des tailles de bloc différentes : $N = 16$, $N = 32$, $N = 64$ et $N = 128$. (a) Lena, (b) Goldhill.

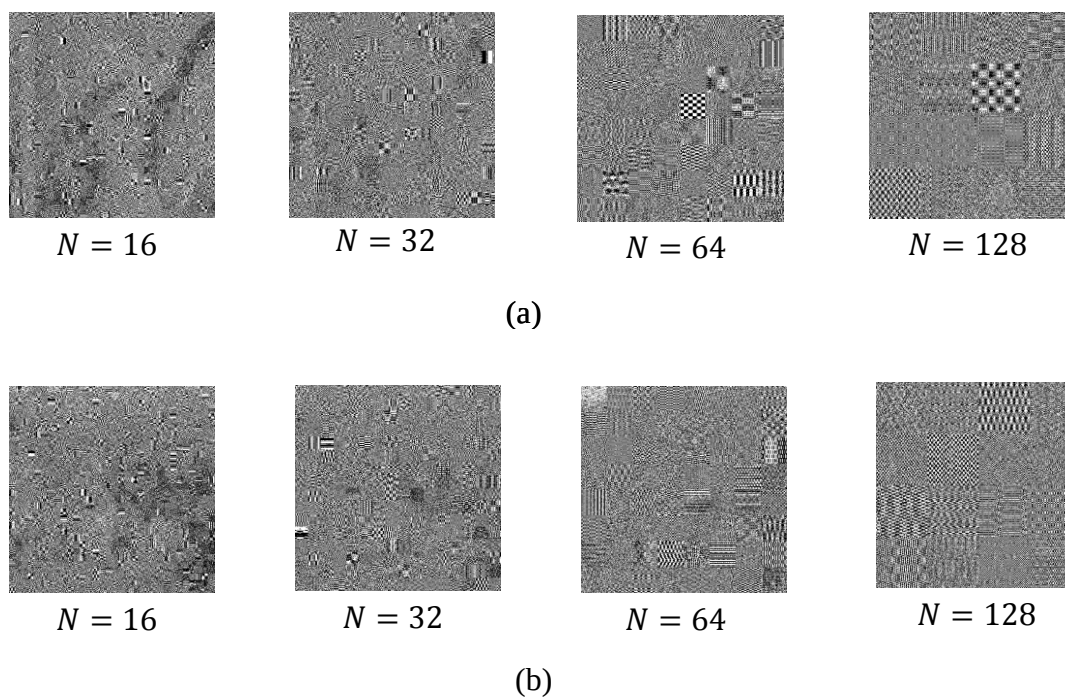


Figure 4.4 Images décryptées en utilisant des paramètres incorrects pour des tailles de bloc différentes : $N = 16$, $N = 32$, $N = 64$ et $N = 128$. (a) Lena, (b) Goldhill.

Dans cette méthode, le nombre de paramètres indépendants utilisés dans le processus de cryptage est montré dans le Tableau 4.1 en fonction de la taille du bloc utilisé.

Tableau 4.1 Nombre de paramètres correspondant à la taille du bloc

Taille du bloc	Nombre de paramètres indépendants
512×512	4
256×256	16
128×128	64
64×64	256
32×32	1024
16×16	4096

D'après ces figures, il est clair que l'image originale ne peut pas être récupérée si les paramètres utilisés dans le processus de décryptage sont incorrects, on peut remarquer aussi que la méthode est plus robuste dans le cas du bloc d'ordre 32.

L'évaluation objective des performances de la méthode proposée est effectuée en mesurant le coefficient de corrélation de l'image cryptée et le PSNR de l'image décryptée en utilisant des paramètres incorrects. Les résultats des mesures sont présentés dans les Tableaux 4.2 et 4.3 suivants. Ces résultats confirment les conclusions qui peuvent être tirées des résultats obtenus concernant la qualité visuelle des images cryptées ou décryptées.

Tableau 4.2 Evaluation objective en termes de PSNR des images de test décryptées

Images de test	$N = 16$	$N = 32$	$N = 64$	$N = 128$
Lena	-77.5951	-86.6108	-87.5015	-93.7709
Goldhill	-76.7669	-79.3582	-87.1292	-89.9917
Boat	-79.0156	-82.5585	-85.0136	-94.9711
Barbara	-87.6593	-92.8087	-93.2471	-98.7896
Bridge	-81.0250	-88.9499	-90.4725	-104.4906
Baboon	-75.4375	-84.1709	-90.2788	-93.6342

Tableau 4.3 Evaluation objective en termes de coefficient de corrélation des images de test cryptées

Images de test	$N = 16$	$N = 32$	$N = 64$	$N = 128$
Lena	0.3354	0.2893	0.3103	0.3009
Goldhill	0.3889	0.3588	0.4132	0.4326
Boat	0.3259	0.2916	0.3178	0.3611
Barbara	0.3895	0.3770	0.4209	0.4241
Bridge	0.3756	0.3665	0.3683	0.4090
Baboon	0.2609	0.2105	0.2961	0.3105

La Figure 4.5 présente les histogrammes des images « Lena » et « Goldhill » cryptées en utilisant des blocs d'ordre 32. L'analyse des histogrammes montre bien que l'histogramme de l'image cryptée a une distribution totalement aléatoire. Il est très différent de celui de l'image originale (Figure 3.2). L'algorithme de cryptage proposé fait en sorte que la dépendance des propriétés statistiques de l'image cryptée et de l'image originale soit quasi aléatoire. Ceci rend la cryptanalyse de plus en plus difficile.

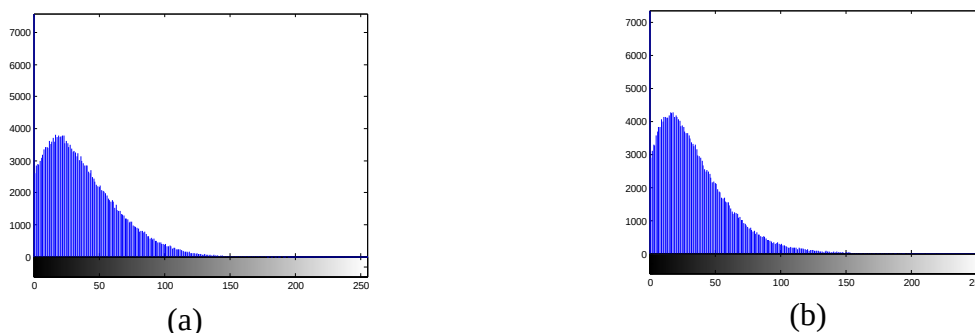


Figure 4.5 Histogrammes des images cryptées en utilisant des blocs d'ordre 32:
(a) Lena, (b) Goldhill.

Un algorithme de cryptage idéal est l'algorithme qui résiste à toutes sortes d'attaques telles que: attaque à texte crypté seulement, attaque à texte clair connu, recherche exhaustive, etc. Pour tester la robustesse de la méthode proposée contre l'attaque par force brute et pour illustrer les effets des erreurs de la clé secrète supplémentaire sur l'image décryptée, nous effectuons des expériences en considérant dans le processus de décryptage que seulement une partie du nombre de paramètres indépendants $p = 4M^2/N^2$ est incorrecte. Les résultats de cette étude pour l'image de test Lena sont donnés dans la Figure 4.6, qui montre clairement que la méthode proposée est sensible aux erreurs sur la clé secrète supplémentaire et par conséquent, elle est robuste contre l'attaque par force brute.

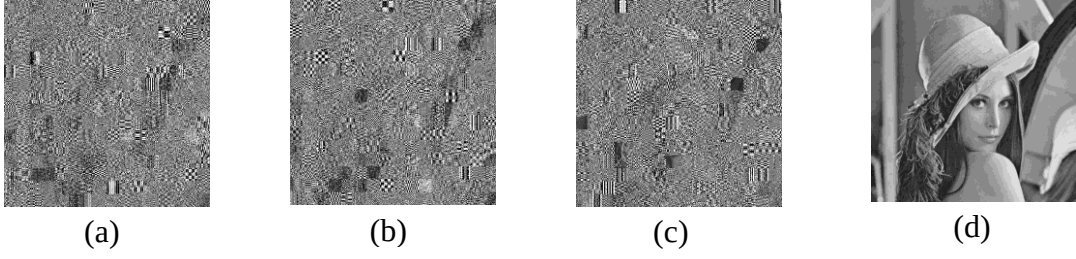


Figure 4.6 Image de test Lena décryptée par des blocs d'ordre 32 avec: (a) $3p/4$ paramètres incorrects, (b) $p/2$ paramètres incorrects, (c) $p/4$ paramètres incorrects, (d) paramètres corrects.

4.4 Méthodes proposées pour le cryptage d'images dans le domaine de la transformée ROP à valeurs réelles

4.4.1 Cas de la transformée ROP à valeurs réelles quelconques

4.4.1.1 Développement de la méthode

Nous considérons les vecteurs paramétriques à valeurs réelles $\mathbf{v}_i$, $\mathbf{w}_i$, $\mathbf{y}_i$, et $\mathbf{z}_i$ pour construire les matrices de la transformée ROP à valeurs réelles $\mathbf{T}_N^{\mathbf{v}_i}$, $\mathbf{T}_N^{\mathbf{w}_i}$, $\mathbf{T}_N^{\mathbf{y}_i}$, et $\mathbf{T}_N^{\mathbf{z}_i}$, respectivement. Le bloc crypté à valeurs réelles $\mathbf{E}_i$, $i = 1, 2, \dots, M^2/N^2$, de l'image cryptée $\mathbf{E}$ de taille $M \times M$ est obtenu à partir du bloc $\mathbf{Q}_i$, $i = 1, 2, \dots, M^2/N^2$, de l'image originale $\mathbf{Q}$ de taille $M \times M$ comme suit

$$\mathbf{E}_i = \frac{1}{N^2} \left(\mathbf{T}_N^{\mathbf{y}_i} \left(\left(\mathbf{T}_N^{\mathbf{v}_i} (\mathbf{Q}_i \odot \boldsymbol{\Phi}_i) \mathbf{T}_N^{\mathbf{w}_i} \right) \odot \boldsymbol{\Phi}_i \right) \mathbf{T}_N^{\mathbf{z}_i} \right), \quad i = 1, 2, \dots, M^2/N^2 \quad (4.3)$$

L'image $\mathbf{D}$ est obtenue à partir de l'image cryptée à valeurs réelles $\mathbf{E}$ dont chaque bloc crypté $\mathbf{E}_i$ est décrypté comme suit

$$\mathbf{D}_i = \frac{1}{N^2} \left(\left(\left(\mathbf{T}_N^{\mathbf{v}_i'} \right)^{\text{RT}} \left(\left(\left(\mathbf{T}_N^{\mathbf{y}_i'} \right)^{\text{RT}} \mathbf{E}_i \left(\mathbf{T}_N^{\mathbf{z}_i'} \right)^{\text{RT}} \right) \odot (\boldsymbol{\Phi}_i')^{-1} \right) \left(\mathbf{T}_N^{\mathbf{w}_i'} \right)^{\text{RT}} \right) \odot (\boldsymbol{\Phi}_i')^{-1} \right),$$

$$i = 1, 2, \dots, M^2/N^2 \quad (4.4)$$

Les processus de cryptage et de décryptage donnés par (4.3) et (4.4), respectivement, sont illustrés par la Figure 4.7.

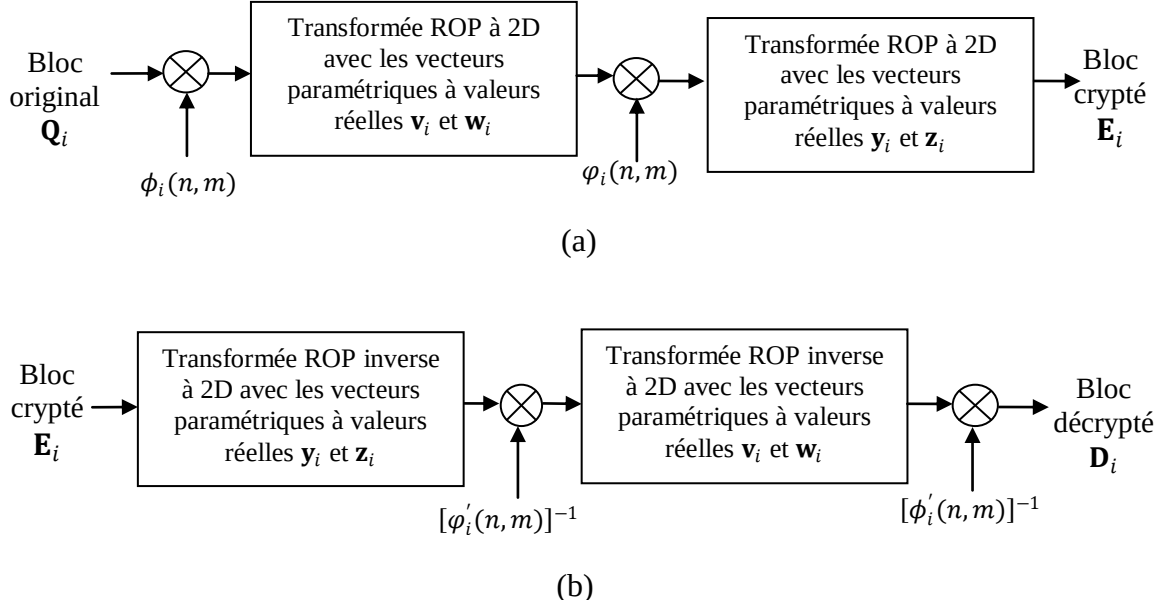


Figure 4.7 Processus de cryptage d'image par bloc proposé en utilisant deux masques d'amplitudes aléatoires dans le domaine de la transformée ROP à valeurs réelles: (a) schéma de cryptage, (b) schéma de décryptage

A partir des équations 4.3 et 4.4, il est clair que l'image décryptée peut devenir identique à l'image cryptée dans le cas où les clés secrètes (clé secrète de cryptage et clé supplémentaire) utilisées dans le processus de cryptage et de décryptage sont les mêmes.

4.4.1.2 Application de la méthode : Résultats de simulation

Dans cette section, des expériences de simulation sont effectuées pour crypter « Lena » et « Goldhill » avec la méthode de cryptage d'images proposée dans la section précédente en utilisant la transformée ROP à valeurs réelles dont les paramètres réels indépendants des matrices ROP $\mathbf{T}_N^{\mathbf{v}_i}$, $\mathbf{T}_N^{\mathbf{w}_i}$, $\mathbf{T}_N^{\mathbf{y}_i}$, et $\mathbf{T}_N^{\mathbf{z}_i}$ sont non nuls et ils sont choisis arbitrairement de l'intervalle $[-4,4]$. La méthode est testée pour des blocs de tailles différentes et les résultats de simulation sont présentés dans les figures suivantes. La Figure 4.8 représente les images cryptées tandis que la Figure 4.9 représente les images décryptées en utilisant des paramètres incorrects dans le processus de cryptage proposé.

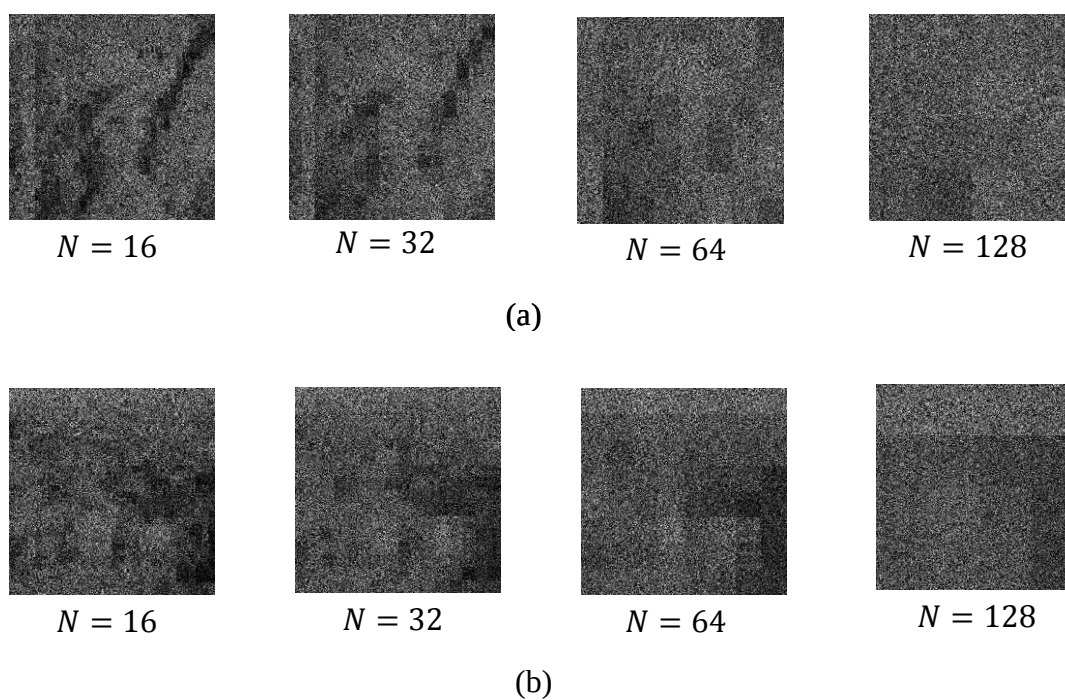


Figure 4.8 Images cryptées par tailles de bloc différentes : $N = 16$, $N = 32$, $N = 64$ et $N = 128$. (a) Lena, (b) Goldhill.

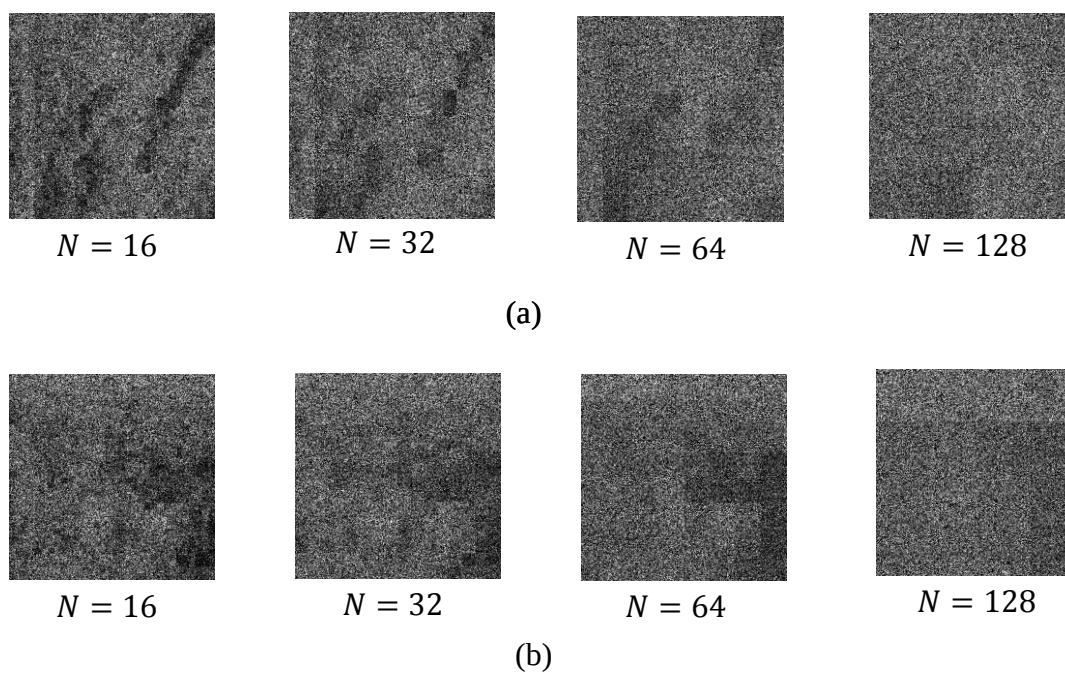


Figure 4.9 Images décryptées en utilisant des paramètres incorrects pour des tailles de bloc différentes : $N = 16$, $N = 32$, $N = 64$ et $N = 128$. (a) Lena, (b) Goldhill.

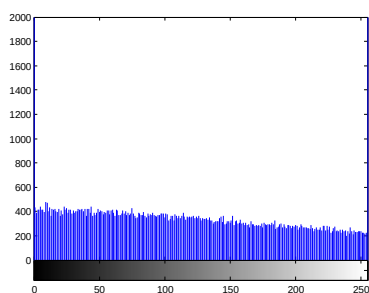
Les Figures 4.8 et 4.9 montrent que l'image cryptée est semblable à un bruit et que la reconstitution de l'image originale est impossible quand les paramètres utilisés sont incorrects.

Tableau 4.4 Evaluation objective en termes de PSNR des images de test décryptées

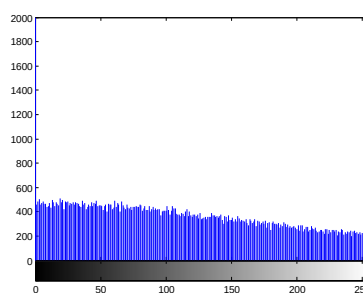
Images de test	$N = 16$	$N = 32$	$N = 64$	$N = 128$
Lena	-12.6216	-13.3723	-13.1723	-13.7869
Goldhill	-11.9749	-12.7295	-12.4104	-12.9776
Boat	-12.9119	-13.8201	-13.4299	-14.2813
Barbara	-12.4740	-13.0947	-12.9294	-13.4686
Bridge	-12.3001	-12.9087	-12.6357	-13.0131
Baboon	-12.8904	-13.5890	-13.3042	-13.9436

Tableau 4.5 Evaluation objective en termes de coefficient de corrélation des images de test cryptées

Images de test	$N = 16$	$N = 32$	$N = 64$	$N = 128$
Lena	0.0033	-0.00028	-0.0036	0.0018
Goldhill	-0.0012	-0.00029	0.0035	-0.0018
Boat	0.0010	0.00035	-0.0012	-0.0015
Barbara	-0.0015	0.0011	-0.0020	0.0019
Bridge	-0.0022	0.00038	0.0010	-0.0015
Baboon	0.0027	0.0024	0.0026	0.0031



(a)



(b)

Figure 4.10 Histogrammes d'image cryptée par des blocs d'ordre 32: (a) Lena, (b) Goldhill

Les mesures objectives données dans les tableaux 4.4 et 4.5 et l'analyse d'histogramme de l'image cryptée correspondante à la Figure 4.10 confirment les conclusions tirées des Figures 4.8 et 4.9 concernant le comportement aléatoire de l'image cryptée.

Les résultats de simulation présentés dans la Figure 4.11 concernant l'attaque par force brute montrent que la méthode proposée est très sensible aux erreurs sur la clé secrète supplémentaire et par conséquent, elle est robuste contre l'attaque par force brute.

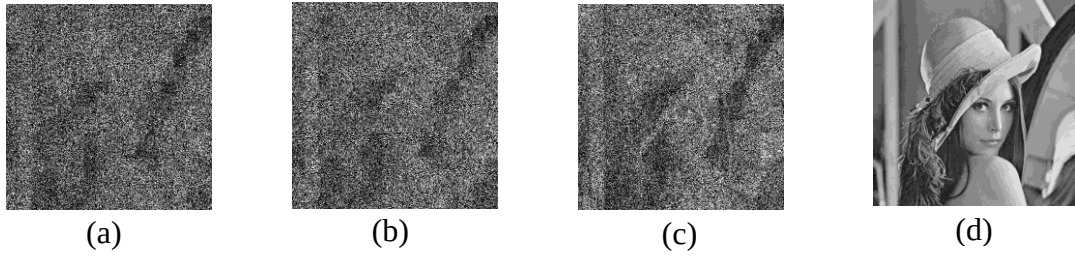


Figure 4.11 Images de Lena décryptées par des blocs d'ordre 32 avec: (a) $3p/4$ paramètres incorrects, (b) $p/2$ paramètres incorrects, (c) $p/4$ paramètres incorrects, (d) paramètres corrects.

4.4.2 Cas de la transformée ROP à valeurs réelles de l'ensemble $\{\pm 2^m\}$: Méthode de cryptage d'images sans multiplications

Le processus de cryptage proposé dans la section 4.4.1 utilise $4M^2/N^2$ matrices de la transformée ROP. Chaque matrice possède $N/2 - 1$ paramètres réels indépendants, par conséquent, le nombre de paramètres utilisés pour le cryptage est $(2N - 4)M^2/N^2$. Si tous ces paramètres indépendants sont choisis de l'ensemble $\{\pm 2^m\}$, où m est un nombre entier positif ou négatif, les matrices $\mathbf{T}_N^{\mathbf{v}_i}$, $\mathbf{T}_N^{\mathbf{w}_i}$, $\mathbf{T}_N^{\mathbf{y}_i}$, et $\mathbf{T}_N^{\mathbf{z}_i}$ de la transformée ROP à valeurs réelles n'exigent aucune multiplication [12] pour leurs calculs et ceci réduit la complexité des calculs de la méthode proposée d'une manière considérable.

Nous avons effectué une variété d'expériences sur les images de test présentées dans le chapitre précédent en considérant que les paramètres réelles des vecteurs paramétriques $\mathbf{v}_i$, $\mathbf{w}_i$, $\mathbf{y}_i$, et $\mathbf{z}_i$ sont choisis de l'ensemble $\{\pm 2^m\}$, où m est un nombre entier positif pour les vecteurs $\mathbf{v}_i$ et $\mathbf{w}_i$ et négatif pour $\mathbf{y}_i$, et $\mathbf{z}_i$.

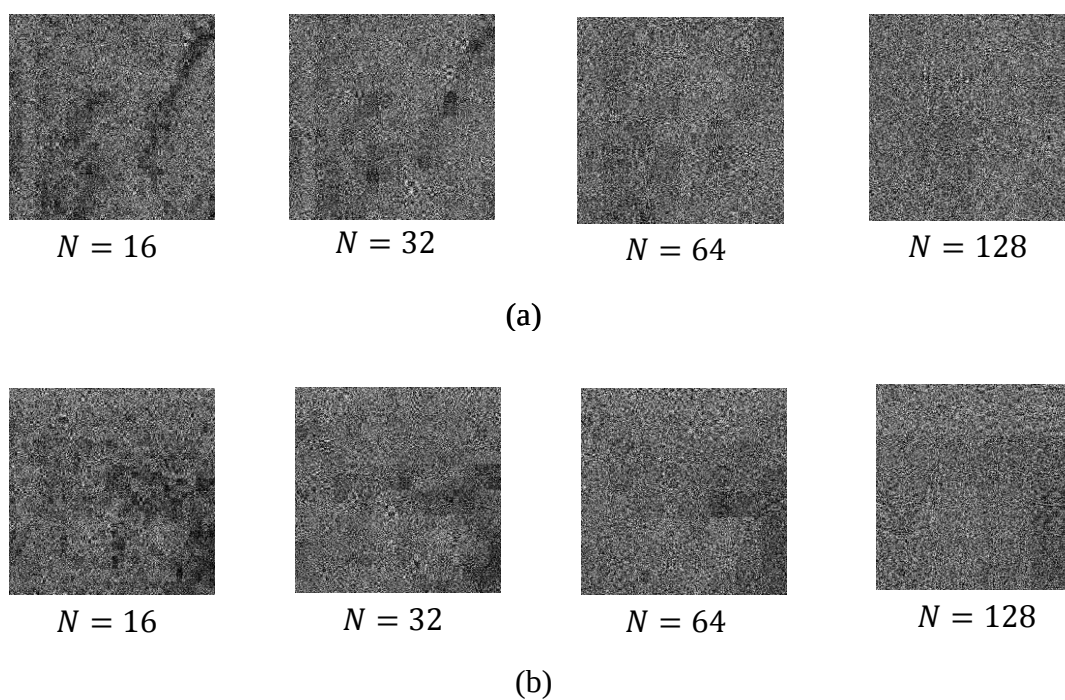


Figure 4.12 Images cryptées par tailles de bloc différentes : $N = 16$, $N = 32$, $N = 64$ et $N = 128$. (a) Lena, (b) Goldhill.

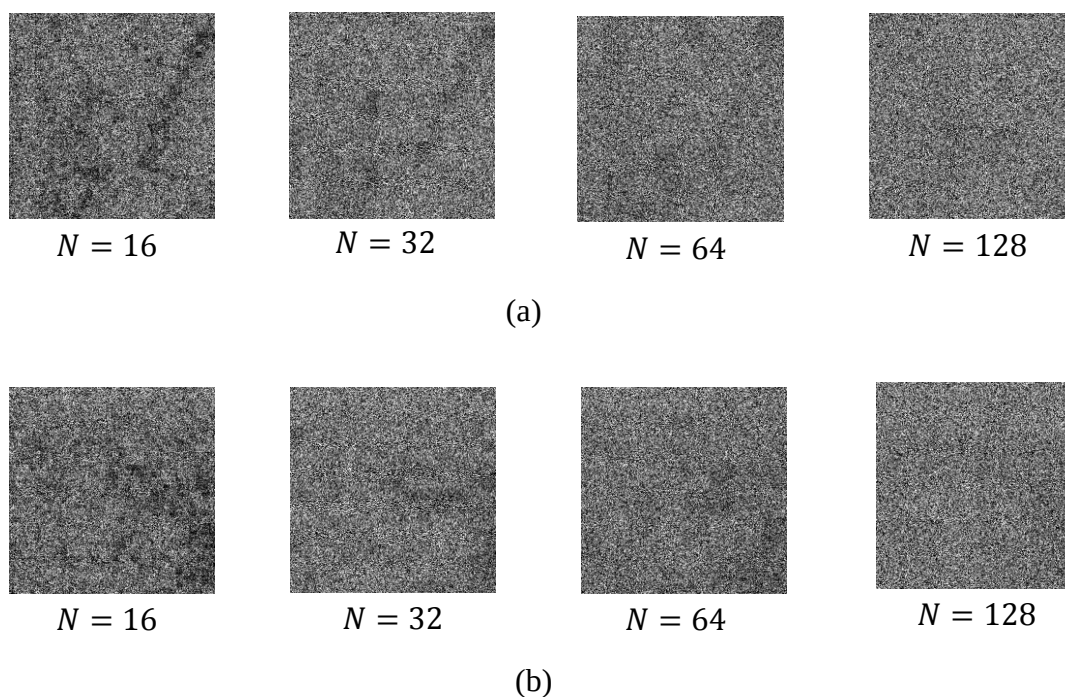


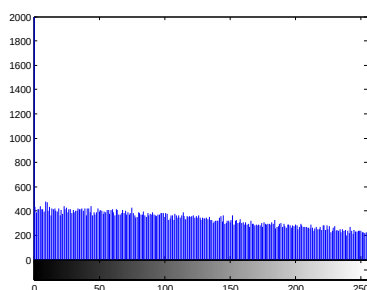
Figure 4.13 Images décryptées en utilisant des paramètres incorrects pour des tailles de bloc différentes : $N = 16$, $N = 32$, $N = 64$ et $N = 128$. (a) Lena, (b) Goldhill.

Tableau 4.6 Evaluation objective en termes de PSNR des images de test décryptées

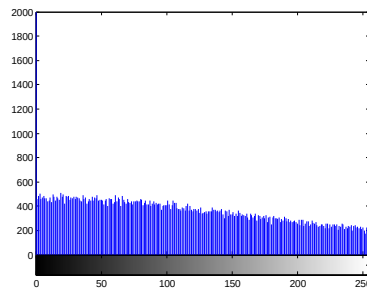
Images de test	$N = 16$	$N = 32$	$N = 64$	$N = 128$
Lena	-21.7519	-23.7646	-22.2198	-23.8561
Goldhill	-21.1526	-22.9121	-21.8806	-23.6254
Boat	-21.7293	-23.4536	-22.6829	-24.1641
Barbara	-21.3199	-23.3245	-22.1048	-23.1457
Bridge	-21.4321	-22.9977	-22.0551	-23.1421
Baboon	-21.8889	-23.5904	-22.4178	-24.2581

Tableau 4.7 Evaluation objective en termes de coefficient de corrélation des images de test cryptées

Images de test	$N = 16$	$N = 32$	$N = 64$	$N = 128$
Lena	0.00041	-0.00012	0.00030	-0.0011
Goldhill	-0.0017	-0.00047	-0.0018	-0.0012
Boat	0.0029	0.0015	-0.0022	-0.0017
Barbara	-0.0011	-0.00016	-0.0028	-0.0022
Bridge	0.0010	-0.00078	0.0013	-0.0020
Baboon	0.0016	-0.00044	-0.0015	-0.0013



(a)



(b)

Figure 4.14 Histogrammes d'image cryptée par des blocs d'ordre 32: (a) Lena, (b) Goldhill.

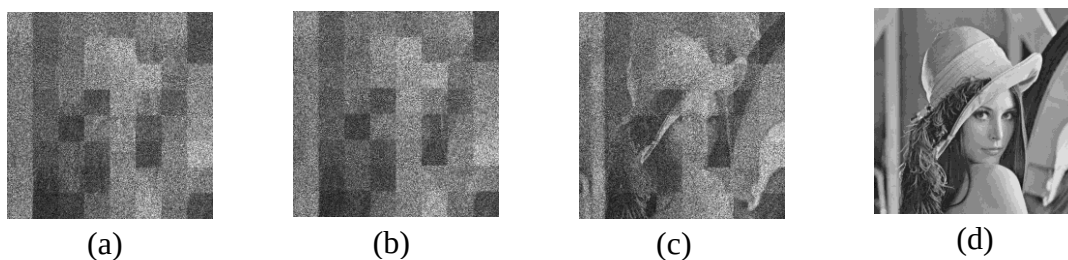


Figure 4.15 Image de Lena décryptée par des blocs d'ordre 64 avec: (a) $3p/4$ paramètres incorrects, (b) $p/2$ paramètres incorrects, (c) $p/4$ paramètres incorrects, (d) paramètres corrects.

Les résultats de simulation présentés dans les figures 4.12 et 4.13, les tableaux 4.6 et 4.7, et les figures 4.14 et 4.15 montrent clairement que la méthode sans multiplications proposée est très efficace pour le cryptage d'images et robuste contre l'analyse d'histogramme et l'attaque par force brute.

4.5 Conclusion

Dans ce chapitre, nous avons proposé trois méthodes de cryptage d'images par bloc basées sur deux masques d'amplitudes aléatoires en utilisant la DHT paramétrique et la transformée ROP à valeurs réelles. Les résultats expérimentaux d'analyse de la sécurité (analyse d'histogramme, les mesures objectives effectuées sur les images cryptées et décryptées et l'attaque par force brute) confirment l'efficacité et la robustesse des méthodes proposées dans ce chapitre. Nous avons montré aussi que les paramètres indépendants de ces transformées paramétriques peuvent être utilisés avec succès comme une clé secrète supplémentaire pour le cryptage d'images. En plus, dû au fait que les transformées paramétriques à valeurs réelles utilisées dans ces méthodes possèdent une faible complexité de calcul comparée à celles des transformées paramétriques existantes, les méthodes proposées dans ce chapitre sont plus efficaces que les méthodes existantes, en particulier, notre méthode de cryptage d'images sans multiplications est plus rapide et plus attractive pour les transmissions sécurisées des images en temps réel sur des réseaux de communication.

Conclusion Générale



Conclusion générale

Le développement rapide des réseaux de communication a provoqué de nouveaux problèmes de la sécurité des images fixes. La sécurisation des images stockées ou transmises est généralement effectuée par des techniques de cryptage dont leur développement est devenu un grand challenge dans ces dernières années. Après une étude bibliographique des techniques de cryptage d'images basées sur les transformées fixes et les transformées fractionnaires, nous avons constaté qu'elles ne sont pas très robustes aux attaques récentes et leurs vitesse d'exécution restent insuffisantes pour les applications en temps réel. Le projet que nous a été proposé a pour objectif de renforcer la robustesse des techniques de cryptage basées sur les transformées, et d'améliorer la vitesse d'exécution.

Au cours de ce travail de recherche, nous avons réalisé l'objectif ci-dessus en proposant deux catégories de nouvelles méthodes de cryptage d'images par bloc basées sur des transformées paramétriques. La première catégorie des méthodes proposées adopte deux masques de phases aléatoires comme une clé de cryptage, de ce fait, elle est consacrée à l'exploitation des transformées paramétriques à valeurs complexes; l'une de ces méthodes exploite la transformée ROP et l'autre utilise la DFT paramétrique. Par contre, la deuxième catégorie est dédiée pour l'exploitation des transformées paramétriques à valeurs réelles. Alors, les trois méthodes proposées dans cette catégorie utilisent deux masques d'amplitudes aléatoires comme une clé de cryptage; la première méthode utilise la DHT paramétrique et les deux autres exploitent la transformée ROP pour le cas des paramètres à valeurs réelles quelconques et le cas des paramètres qui sont des puissances de deux. Dans nos cinq méthodes, nous avons utilisé avec succès les paramètres indépendants des transformées paramétriques, mentionnées précédemment, comme une clé secrète supplémentaire pour le cryptage d'images.

Les résultats expérimentaux d'analyse de la sécurité, spécifiquement l'analyse d'histogramme, les mesures objectives effectuées sur les images cryptées et décryptées et l'attaque par force brute, obtenus dans ce mémoire confirment l'efficacité et la robustesse de nos méthodes. En outre, dû au fait que les transformées paramétriques utilisées dans les méthodes proposées possèdent une faible complexité de calcul comparée à celles des transformées paramétriques existantes, nos méthodes ont l'avantage de complexité réduite par rapport à celles des méthodes de cryptage d'images existantes, en particulier notre méthode de cryptage d'images sans multiplications n'exige que des additions et des décalages de bits, par conséquent, elle est plus rapide et extrêmement attractive pour les transmissions sécurisées des images en temps réel sur les réseaux de communication.

Dans ce travail, nous avons considéré le cas des images fixes. Alors, nous suggérons en perspectives l'exploitation des idées développées dans ce mémoire pour concevoir des nouvelles méthodes appropriées pour le cryptage des vidéos.

Bibliographie

- [1] J. Daemen and V. Rijmen, “AES Proposal: Rijndael,” *AES Algorithm Submission*, 3rd September 1999.
- [2] R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, “The RC6TM Block Cipher”, *M. I. T laboratory for Computer Science*, USA, 20 August 1998.
- [3] R. F. Sewell, “Bulk Encryption Algorithm for Use with RSA,” *Electronics Letters*, Vol. 29, No. 25, pp. 2183-2185, 9th December 1993.
- [4] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” *Optics. Letters*, Vol. 20, pp. 767–769, 1995.
- [5] G. Unnikrishnan and K. Singh, “Double random fractional Fourier-domain encoding for optical security,” *Optical Instrumentation Engineers*, Vol. 39, pp. 2853–2859, 2000.
- [6] S.-C. Pei and W.-L. Hsue, “The multiple-parameter discrete fractional Fourier transform,” *IEEE Signal Processing Letters*, Vol. 13, No. 6, pp. 329–332, June 2006.
- [7] J. M. Vilarly, J. E. Calderon, C. O. Torres, and L. Mattos, “Digital images phase encryption using fractional Fourier transform,” in *Proceedings IEEE Conference. Electronics, Robotics and Automotive Mechanics*, Vol. 1, pp.15–18, September 2006.
- [8] L. Chen, D. Zhao, “Optical image encryption with Hartley transforms”, *Optics Letters*, Vol. 31, No. 23, pp. 3438–3440, 1st December 2006.
- [9] Z. Liu, M. A. Ahmad and S. Liu., “Image encryption based on double random amplitude coding in random Hartley transform domain”, *International Journal for Light and Electron Optics* ,Vol. 121, pp. 959-964, 3rd December 2008.
- [10] K. K. Kesavan and M. R. kumar, “Optical color image encryption based on Hartley transform and double random phase encoding system”, 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pp.1-3, 5-7 October 2011.

- [11] S. Bouguezel, M.O. Ahmad and M.N.S. Swamy, "Image encryption using the reciprocal-orthogonal parametric transforms," *International Symposium on Circuits and Systems (ISCAS)*, pp. 2542-2545, May 30 - June 2, 2010, Paris, France.
- [12] S. Bouguezel, M.O. Ahmad, and M.N.S. Swamy, "A New Class of Reciprocal-Orthogonal Parametric Transforms" *IEEE Transactions Circuits and Systems I, Regular Papers*, Vol. 56, No.4, pp. 795-805, April 2009.
- [13] S. Bouguezel, M.O. Ahmad, and M.N.S. Swamy, "New Parametric Discrete Fourier and Hartley Transforms, and Algorithms for Fast Computation" *IEEE Transactions Circuits and Syst. I, Regular Papers*, Vol. 58, No.03, pp. 562-575, March 2011.
- [14] B. Schneier, *Cryptographie appliquée : Algorithmes, protocoles et codes sources en C*, Vuibert Informatique, deuxième édition, janvier 2001.
- [15] D. Stinson, "Cryptography: Theory and Practice", 2nd edition, Chapman & Hall CRC Boc Raton, USA, 2002.
- [16] A. Menezes, P. V. Oorschot, and S. Vanstone, *Handbook of applied cryptography*, CRC Press, 1996.
- [17] B. Martin, *Codage, cryptologie et applications*, Presses polytechniques et universitaires Romandes, 2004.
- [18] W. Diffie and M. E. Hellman. "New directions in cryptography". *IEEE Transactions on Information Theory* (IT), Vol. 22, No. 6, pp.644–654, November 1976.
- [19] S. G. Lian, J. Sun and Z. Wang, "A Novel Image Encryption Scheme Based-on JPEG Encoding", *Proceedings of 8th International Conference on Information Visualization*, pp. 217-220, 2004.
- [20] H Jin, Z. Liao, D. Zou, and C. Li, "Asymmetrical Encryption Based Automated Trust Negotiation Mode", *The 2nd IEEE International Conference on Digital Ecosystems and Technologies (DEST)*, pp. 363- 368, Feb. 2008.
- [21] R. Kusters and M Tuengerthal, "Universally Composable Symmetric Encryption", *The 2nd IEEE Computer Security Foundations Symposium (CSF)*, pp. 293- 307, July 2009.
- [22] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, 5th edition, CRC Press LLC, Florida, EUA, August 2001.

- [23] M.Benabdellah, M.Gharbi, N.Zahid, F.Regragui et E.H.Bouyakhf, "Crypto-compression des images échographiques par la transformation de Faber-Schauder et l'algorithme DES", *Proceeding du Colloque International sur l'Informatique et ses Applications*, 31 octobre 1 et 2 Novembre 2006, ENSAO, Oujda-Maroc.
- [24] M. A. B. Younes and A. Jantan, "Image Encryption Using Block-Based Transformation Algorithm", *IAENG International Journal of Computer Science (IJCS)*, Vol. 35, No. 03, 2008.
- [25] F. Dachzelt, K. Kelber and W. Schwarz, "Chaotic Coding and Cryptoanalysis", *Proceedings of IEEE International Symposium on Circuits and Systems*, Hong Kong, pp. 1061-1064, 9-12 June 1997.
- [26] N. Bourbakis and C. Alexopoulos, "Picture Data Encryption Using SCAN Patterns", *Pattern Recognition*, Vol. 25, No. 6, pp. 567 581, 1992.
- [27] C. J. Kuo, "Novel Image Encryption Technique and Its Application in Progressive Transmission", *Journal Electronic Imaging*, Vol. 2, No. 4, pp. 345 351, 1993.
- [28] D E Newton, *Encyclopedia of Cryptology*, ABC-CLIO Inc , California, USA, 1997.
- [29] S. Lian, *Multimedia content encryption: techniques and applications*, CRC Press LLC, 2009.
- [30] J. Cheng, F. Zhang, K. Yu, and J. Ma, "The Dynamic and Double Encryption System Based on Two-Dimensional Image", *International Conference on Computational Intelligence and Security*, pp. 458- 462, 2009
- [31] N. Ahmed and K. R. Rao, *Orthogonal Transforms for Digital Signal Processing*, Berlin, Germany: Springer-Verlag, 1975.
- [32] A. A. Agaian, *Hadamard Matrices and Their Applications*. Berlin, Germany: Springer-Verlag, 1985, Vol. 1168, Lecture Notes in Mathematics.
- [33] R. K. Yarlagadda and J. E. Hershey, *Hadamard Matrix Analysis and Synthesis With Applications to Communications and Signal/Image Processing*. Norwell, MA: Kluwer, 1997.
- [34] K. J. Horadam, *Hadamard Matrices and Their Applications*, Princeton, NJ: Princeton Univ. Press, 2006.
- [35] C.-C. Tseng, "Eigenvalues and eigenvectors of generalized DFT, generalized DHT, DCT-IV and DST-IV matrices," *IEEE Transactions on Signal Processing*, Vol. 50,

No. 4, pp. 866–877, April 2002.

- [36] V. Senk, V. D. Delic, and V. S. Milosevic, “A new speech scrambling concept based on Hadamard matrices,” *IEEE Signal Processing Letters*, Vol. 4, No. 6, pp. 161–163, June 1997.
- [37] D. V. De Ville, W. Philips, R. V. de Walle, and I. Lemahieu, “Image scrambling without bandwidth expansion,” *IEEE Transactions Circuits and Systems for Video Technology*, Vol. 14, No. 6, pp. 892–897, June 2004.
- [38] S. K. Pal, “Fast, reliable and secure digital communication using Hadamard matrices,” in *Proceeding IEEE International Conference on Computing Theory and Applications (ICCTA)*, pp. 526–532, Mar. 2007.
- [39] B. J. Falkowski and L. S. Lim, “Image watermarking using Hadamard transforms,” *Electronics Letters*, Vol. 36, No. 3, pp. 211–213, February 2000.
- [40] A. T. S. Ho, S. Jun, A. K. K. Chow, and J. Woon, “Robust digital image-in-image watermarking algorithm using the fast Hadamard transform,” in *Proceeding IEEE International Symposium on Circuits and Systems (ISCAS)*, Vol. 3, pp. 826–829, May 2003.
- [41] D. Coltuc and J.-M. Chassery, “Very fast watermarking by reversible contrast mapping,” *IEEE Signal Processing Letters*, Vol. 14, No. 4, pp. 255–258, April 2007.
- [42] P. Dita, “Some results on the parameterization of complex Hadamard matrices,” *Journal of Physics A, Mathematical and General*, Vol. 37, No. 20, pp. 5355–5374, May 2004.
- [43] W. Tadej and K. Kyczkowski, “A concise guide to complex Hadamard matrices,” *Open Systems and Information Dynamics*, Vol. 13, No. 2, pp. 133–177, June 2006.
- [44] F. Szollosi, “Parametrizing complex Hadamard matrices,” *European Journal of Combinatorics*, vol. 29, no. 5, pp. 1219–1234, Jul. 2007.
- [45] A. T. Butson, “Generalized Hadamard matrices,” *Proceedings of the American Mathematical Society*, Vol. 13, pp. 894–898, 1962.
- [46] M. H. Lee, B. S. Rajan, and J. Y. Park, “A generalized reverse jacket transform,” *IEEE Transactions on Circuits and System II, Analog and Digital. Signal Processing*, Vol. 48, No. 7, pp. 684–690, July 2001.
- [47] K. J. Horadam, “A generalised Hadamard transform,” in *Proceeding. IEEE*

International Symposium on Information Theory (ISIT), pp. 1006–1008 September 2005.

- [48] S. Rahardja and B. J. Falkowski, “Family of unified complex Hadamard transforms,” *IEEE Transaction Circuits Systems. II, Analog Digital Signal Processing*, Vol. 46, No. 8, pp. 1094–1100, August 1999.
- [49] M. Puschel, “Cooley–Tukey FFT like algorithms for the DCT,” in *Proceeding IEEE International Conference on Acoustics, speech and signal processing (ICASSP)*, Vol. 2, pp. 501–504, Apr. 2003.
- [50] A. M. Grigoriyan, “A novel algorithm for computing the 1-D discrete Hartley transform,” *IEEE Signal Processing Letters*, Vol. 11, No. 2, pp. 156–159, February. 2004.
- [51] J.W. Cooley and J.W. Tukey, “An algorithm for machine computation of complex Fourier series,” *Mathimatics of Computation.*, Vol. 9, pp. 297–301, 1965.
- [52] P. Duhamel and H. Hollmann, “Split radix FFT algorithm,” *Electronics. Letters*, Vol. 20, No. 1, pp. 14–16, January 1984.
- [53] S. Bouguezel, M. O. Ahmad, and M. N. S. Swamy, “A general class of split-radix FFT algorithms for the computation of the DFT of length- 2^m ,” *IEEE Transaction Signal Processing*, Vol. 55, No. 8, pp. 4127–4138, August 2007.
- [54] J. Guo, Z. Liu, and S. Liu, “Watermarking based on discrete fractional random transform,” *Optics Communications*, Vol. 272, No. 2, pp. 344–348, April 2007.
- [55] Saad Bouguezel, M. Omair Ahmad, M. N. S. Swamy, “An efficient split-radix FHT algorithm”. *International Symposium on Circuits and Systems (ISCAS)*, Vol. 3, pp. 565-568, 23-26 May 2004.
- [56] L. Krikor, S. Baba, T. Arif and Z. Shaaban, “Image Encryption Using DCT and Stream Cipher”, *European Journal of Scientific Research ISSN 1450-216X*, Vol.32, No.1, pp.47-57, 2009.
- [57] L. Chen and D. Zhao, “Optical image encryption based on fractional wavelet transform”, *Optics communications*, Vol. 254, pp. 361-367, 15 th October 2005.
- [58] N. A. Flayh, S. I. Ahson, “Wavelet Based Image Encryption ”, *9th International Conference on Signal Processing (ICSP)*, pp. 797-800, 26-29 October 2008.

ملخص

يتناول هذا العمل تشفير الصور الثابتة عن طريق استغلال التحويلات بالوسائط طورت مؤخرا. المذكرة تعرض أولا دراسة مكتبية عن تقنيات تشفير الصور والحالة التقنية للتحويلات بالوسائط وأساليب تطويرها وبنائها. هذه الدراسة سمحت لنا بتطوير نوعين من أساليب جديدة لتشفير الصور الثابتة من خلال اعتماد تقنية المعالجة بالقطع. الفئة الأولى مخصصة لاستعمال تحويلات بوسائط ذات قيم مركبة، خصوصا تحويل ROP وتحويل فورييه بالوسائط، في حين أن الفئة الثانية مناسبة للتحويلات بالوسائط ذات قيم حقيقية خاصة تحويل هارتلي بالوسائط و تحويل ROP في حالة وسائط ذات قيم حقيقية وفي حالة وسائط ذات قيم النتائج التجريبية لتحليل الأمان، وتحديدًا تحليل المدرج التكراري، القياسات التي أجريت على الصور المشفرة وغير المشفرة و القوة الغاشمة المحصل عليها في هذا العمل تبين بوضوح فعالية ومتانة الطرق المقترحة في هذه المذكرة. بالإضافة إلى ذلك، هذه الطرق المقترحة لديها ميزة خفض التعقيد مقارنة بطرق تشفير الصور الموجودة.

كلمات مفتاحية: تقنيات التشفير، تشفير الصور الثابتة، التحويلات ذات وسائط.

Résumé

Ce travail considère le cryptage des images fixes en exploitant les transformées paramétriques récemment développées dans la littérature. Le mémoire présente tout d'abord une étude bibliographique sur les techniques de cryptage d'images et un état de l'art des transformées paramétriques et leurs méthodes de développement et de constructions. Cette étude nous a permis de développer deux catégories de nouvelles méthodes de cryptage d'images fixes en adoptant la technique de traitement par bloc. La première catégorie est dédiée essentiellement à l'exploitation efficace des transformées paramétriques à valeurs complexes, notamment la transformée réciproque orthogonal paramétrique (ROP) et la transformée de Fourier discrète (DFT) paramétrique. Par contre, la deuxième catégorie est appropriée pour des transformées paramétriques à valeurs réelles, particulièrement la transformée de Hartley discrète (DHT) paramétrique et la transformée ROP pour le cas des paramètres à valeurs réelles quelconques et le cas des paramètres qui sont des puissances de deux. Les résultats expérimentaux d'analyse de la sécurité, spécifiquement l'analyse d'histogramme, les mesures objectives effectuées sur les images cryptées et décryptées et l'attaque par force brute, obtenus dans ce travail montrent clairement l'efficacité et la robustesse des méthodes proposées dans ce mémoire. En plus, ces méthodes proposées présentent un avantage de complexité réduite par rapport à celles des méthodes de cryptage d'images existantes.

Mots clés : Techniques de cryptage, Cryptage des images fixes, Transformées paramétriques.

Abstract

This work considers the encryption of images by exploiting the parametric transforms recently developed in the literature. The thesis firstly presents a literature review on image encryption techniques and a state of the art of parametric transforms and their development and construction methods. This literature review allowed us to develop two categories of new still image encryption methods by adopting the technique of block processing. The first category is mainly dedicated to the effective exploitation of complex-valued parametric transforms, including the reciprocal-orthogonal parametric (ROP) transform and the parametric discrete Fourier transform (DFT), whereas the second category is appropriate for real-valued parametric transforms, particularly the parametric discrete Hartley transform (DHT) and the ROP transform for the case of general real-valued parameters and the case of the parameters that are powers of two. The experimental results corresponding to security analysis, specifically the histogram analysis, objective measurements performed on the encrypted and decrypted images and the brute-force attack, obtained in this work clearly show the effectiveness and robustness of the methods proposed in this paper. In addition, these proposed methods have the advantage of reduced complexity compared to those of the existing image encryption methods.

Keywords : Encryption technics, image encryption, parametric transforms.