

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE  
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE  
SCIENTIFIQUE

*Université de Mohamed El-Bachir El-Ibrahimi - Bordj Bou Arreridj*

*Faculté des Sciences et de la technologie*

*Département d'Electromécanique*

# *Mémoire*

*Présenté pour obtenir*

**LE DIPLOME DE MASTER**

**FILIERE : Electromécanique**

**Spécialité : Automatique et Informatique Industrielle**

Par

- **BENDJEDDOU Saad**
- **BENMAKHLOUF Zakaria**

*Intitulé*

**Cryptage et compression conjoints des images numériques à base de  
fonctions chaotiques**

*Soutenu le : .....*

*Devant le Jury composé de :*

<i>Nom &amp; Prénom</i>	<i>Grade</i>	<i>Qualité</i>	<i>Etablissement</i>
<i>M.</i>	<i>MCB</i>	<i>Président</i>	<i>Univ-BBA</i>
<i>M.BEKKOUCHE Tewfik</i>	<i>MCA</i>	<i>Encadreur</i>	<i>Univ-BBA</i>
<i>M.</i>	<i>....</i>	<i>Examineur</i>	<i>Univ-BBA</i>

*Année Universitaire 2021/2022*

---

# Remerciements

Au terme de ce mémoire, nous tenons à exprimer nos remerciements au bon « DIEU » qui nous a donné la force, la santé et la volonté pour mener à bien ce modeste travail. Nous tenons également à exprimer nos vifs remerciements à notre encadreur : Dr Bekkouche Tewfik pour avoir d'abord proposé ce thème, pour son aide quotidienne pour faire avancer notre travail, et qui a bien voulu diriger ce travail pendant toute la durée de l'expérimentation et la mise en forme du document final. Ses nombreux conseils ne m'ont jamais fait défaut. Je suis heureux de lui exprimer ici ma respectueuse reconnaissance.

Nous tenons à remercier vivement toute personne qui nous a aidé à élaborer et réaliser ce mémoire, ainsi à tous ceux qui nous ont aidé de près ou de loin à accomplir ce travail.

Nos remerciements vont aussi à tous les enseignants qui ont contribué à notre formation. Par ailleurs, à tous les membres du jury qui ont accepté de juger notre travail.

En fin, nous tenons à exprimer notre reconnaissance à tous nos amis et collègues pour le soutien moral et matériel.

Saad Bendjeddou et Zakaria Benmakhlouf

A decorative border of repeating floral motifs surrounds the text.

## Dédicace

C'est avec un immense plaisir que Je dédie ce modeste travail à

Mon père, (Omar).

À la plus belle créature que Dieu a créée sur terre.

La plus chère à mon cœur que j'espère Dieu le garde, ma Chère mère,  
(Houria).

Mon frère Mohamed, qui m'encourage dans les instants délicats.

Et mes sœurs, ainsi que leurs enfants.

À tous mes amis (Hasni, Housseem, Amine, Larbi, Hakim, Walid, Jamel).

Et bien sûr à tout le groupe de l'automatique Master 2 promotion:2021-  
2022. Je vous remercie tous.

Enfin bien sûr au Dr Bekkouche Tewfik, qui nous a accompagnés  
pendant le long de cette période pour la finalisation de ce modeste  
travail.

Zakaria Benmakhlouf

# DEDICACE

**C'est avec un immense plaisir que je dédie ce modeste travail à:**

**Mes très chers parents**

**Hamoud et Houria**

**Aux supports de mon âme, vous mon très cher frère: Walid**

**et ma sœur: Samira**

**et mes amies: Khalil Aidel, Walid Benmessaoud, Walid Dahmani, Larbi,  
,Salaheddine et tous mes Amis Sans pour autant oublier les collègues de  
l'automatique master 2, à l'ensemble du groupe de l'automatique de la  
promotion 2021 /2022.**

**Et à toute ma Famille**

**Enfin bien sûr à Dr Bekkouche Tewfik qui nous a accompagné pendant le  
long de Cette période pour la finalisation de ce modeste travail.**

**Je vous remercie tous.**

**Saad Benjeddou**

# Sommaire

---

Introduction générale.....	1
<b>Chapitre I : Cryptage des images</b>	
I.1 Introduction.....	3
I.2 Concepts de base.....	3
I.2.A Cryptologie.....	3
I.2.B Cryptographie.....	4
• Chiffrement ou cryptage.....	4
• Clé de chiffrement.....	4
• Déchiffrement.....	4
➤ Texte en clair.....	4
➤ Texte chiffre.....	4
➤ Crypto-système.....	4
I.2.C Cryptanalyse.....	4
I.3 Les différents types de cryptographie.....	5
I.3.A La cryptographie classique.....	5
I.3.B Le chiffrement par substitution.....	5
I.3.C Le chiffrement par transposition.....	5
I.3.D La cryptographie moderne.....	5
I.3.E La cryptographie symétrique ou à clé secrète.....	6
I.3.F Chiffrement par blocs.....	6
I.3.J Chiffrement par flots.....	6
I.3.H Cryptage hybride.....	6
I.4 Les objectifs de la cryptographie.....	6
I.4.A La confidentialité.....	6
I.4.B Intégrité.....	7
I.4.C Authentification.....	7
I.4.D Non-répudiation.....	7
I.5 Principes de Kirchhoff en cryptographie.....	7
I.6 Cryptage d'images dans le domaine spatial à base de permutations (bit lève).....	7
I.7 Analyse d'histogramme.....	8
I.8 Applications du cryptage.....	10
I.9 Conclusion.....	11
<b>Chapitre II : La compression JPEG des images fixes</b>	
II.1 Introduction.....	12
II.2 Rappelles sur l'image numérique.....	12
II.2.1 définition.....	12
II.2.2 Notions de pixel et espace de couleurs.....	12
II.3 Rappel sur la comprissions des images.....	13
II.3.1 Compression avec perte et sans perte.....	14
II.3.2 La compression sans perte JPEG.....	14
II.3.3 La compression avec perte du JPEG.....	15
II.3.4 Principe général de la compression d'images.....	16
II.3.5 Décorrélation.....	16
II.3.6 Quantification.....	17
II.3.7 Codage des symboles (Symbols coding).....	17

# Sommaire

---

II.4 Notions sur la DCT.....	17
II.4.1 Définition.....	17
II.4.2 Variantes de la DCT.....	18
II.4.2.a DCT-I.....	18
II.4.2.b DCT-II.....	19
II.4.3 Propriétés de la DCT.....	19
II.4.3.a Décorrélation.....	19
II.4.3.b Concentration des coefficients.....	20
II.4.3.c Séparabilité.....	20
II.4.3.d Symétrie.....	21
II.4.3.e Orthogonalité.....	21
II.5 Processus général d'un codec JPEG d'images fixes.....	22
II.5.1 Définition.....	22
II.5.2 JPEG basée sur la DCT séquentielle.....	22
II.5.3 Découpage en sous blocs.....	22
II.5.4 Décalage de niveau (Level Shifting).....	22
II.5.5 Application de la DCT.....	22
II.5.6 Quantification.....	23
II.5.7 Exemple.....	24
II.5.8 Le codage entropique.....	25
II.5.8.a Les coefficients DC.....	25
II.5.8.b Les coefficients AC.....	26
II.5.9 Codage Hoffman.....	27
II.5.9.a Le principe est le suivant.....	28
II.5.9.b Exemple de codage Hoffman.....	28
II.6 Mise en œuvre sous Matlab.....	28
II.6 .1 Représentation d'images sous Matlab.....	28
II.7.Conclusion.....	30

## Chapitre III : Résultats et discussions

III.1 Introduction.....	31
III.2 Simulation du cryptage d'images à base de la technique permutation-diffusion.....	31
III.3 Simulation de la compression JPEG à base de la transformée DCT.....	34
III.4 Simulation de la compression et cryptage conjoints des images.....	35
III.4 Conclusion.....	37

# Liste des figures

---

## ***Chapitre1 : CRYPTAGE DES IMAGES***

Figure 1 le résultat de cryptée et décryptée d'image Lena.....	8
Figure 2.Histogramme de l'image de Lena, de l'image cryptée et de l'image décrypté.....	8
Figure 3 Résultat de l'image cryptée et décryptée de Barbara.....	8
Figure 4 Histogramme de l'image deBarbara, de l'image cryptée et de l'image décryptée.....	9
Figure 5 Image décryptée Suite à un lossdata 25 %.....	9
Figure 6 Image décryptée Suite à un loss data 25 %.....	9
Figure 7 Image décryptée Suite à un loss data 50%.....	10
Figure 8 Sensibilité de la clé de cryptage. ....	10

## ***Chapitre2 : La compression JPEG des images fixes***

Figure 1 Principe de la compression image.....	13
Figure 2 Schéma de bloc du codeur JPEG en mode sans perte.....	14
Figure 3 Le voisinage de la prédiction du prédicteur MED. ....	15
Figure 4 Chaîne de codage de l'algorithme JPEG. ....	16
Figure 5 Schéma général d'un codeur source. ....	16
Figure 6 Les argumente présentés peuvent être identiquement appliqués pour le calcul inverse de la DCT. ....	20
Figure 7 codage différentiel des coefficient DC. ....	26
Figure 8 Scan zig-zag.....	27
Figure 9 Arbre de Huffman après construction.....	29
Figure 10 Compression JPEG. ....	29
Figure 11 Comparaison des sous bloc 8*8 de l'image originale et l'image copressée.....	30

## ***Chapitre3 : Résultats et discussions***

Figure 1 Images de test de Lena et de Barbara .....	31
Figure 2 Schéma synoptique de (a) Cryptage et de (b) Décryptage d'images. ....	32
Figure 3 Images cryptées de Lena et de Barbara et leurs histogrammes. ....	32
Figure 4 Images décryptées de Lena et de Barbara et leurs histogrammes. ....	33
Figure 5 Schéma synoptique de la compression JPEG sans pertes. ....	34
Figure 6 Compression JPEG (a) Lena, sa DCT et son image compressée (b) Barbara, sa DCT et son image compressée. ....	35
Figure 7 Synoptique de compression et cryptage conjoints.....	36
Figure 8 Compression et cryptage conjoints (a) Lena, sa DCT et son image compressée et cryptée (b) Barbara, sa DCT et son image compressée et cryptée. ....	36

## Liste des tableaux

---

### ***Chapitre2 : La compression JPEG des images fixes***

Tableau.1.Catégories d'amplitudes des différences DC.....	27
Tableau.2.Symboles avec leurs probabilités.....	29
Tableau.3.Code des symboles.....	29

### ***Chapitre3 : Résultats et discussions***

Tableau 1.Mesures du PSNR et du coefficient de corrélation pour les deux images test.....	34
Tableau 2. Mesures du taux de compression, du PSNR et de l'erreur quadratique moyenne avec différents facteurs de qualité pour les deux images de test.....	35
Tableau 3. Mesures du taux de compression, du PSNR et de l'erreur quadratique moyenne avec différents facteurs de qualité pour les deux images de test .....	36



# Introduction générale

# *Introduction générale*

---

Les réseaux numériques ont tellement évolué qu'ils sont devenus un mécanisme essentiel de communication. Ils permettent de transmettre toute sorte d'informations textuelles, sonores et principalement des images. La croissance exponentielle du trafic des images est renforcée par l'apparition importante d'appareils photos numériques et utilisation des téléphones portables.

Les images sont des données particulières du fait de la quantité importante d'information et de leur disposition bidimensionnelle. La transmission des images soulève donc un nombre conséquent de problèmes qui ne sont pas tous encore résolus. De plus, les réseaux informatiques sont complexes et les écoutes illégales sont aussi nombreuses. On parlera des problèmes concernant la sécurité et l'authenticité des images transmises sur des réseaux numériques. Un premier problème est relatif à l'aspect sécurité et à l'authenticité des données pendant la transmission, mais également après réception de celles-ci. Toute information circulant peut être capturée, lue et/ou modifiée, cela impose une sécurisation indispensable.

Un deuxième problème concerne la taille de l'information transmise, les tailles des images doivent être réglables avant le transfert. Des applications exigent que l'image soit associée à des informations contextuelles. Cela exige une exploitation adéquate allouée à la transmission de telle information, la compression JPEG est l'une des solutions adoptée pour résoudre cette problématique.

Plusieurs méthodes ont été développées pour résoudre les problèmes de sécurité et d'authenticité dans le transfert des images. Toutefois, très peu de méthodes proposent à la fois une compression, un chiffrement et une IDC (insertion de données cachées). Il est utile de développer des méthodes qui permettent de décrypter une grande quantité d'information dans l'image, c'est la cadre générale sur laquelle se dérouler ce travail.

Dans ce manuscrit, on présente les différentes phases de réalisation de notre projet de fin d'étude dont le thème se rapporte sur le cryptage et la compression des images. L'importance du projet réside particulièrement dans la richesse du sujet abordé. Le projet permet de mettre en place un algorithme de cryptage-compression des images utilisant l'architecture permutation diffusion pour le chiffrement et la norme JPEG pour la compression.

# *Introduction générale*

---

Pour arriver à cette fin le manuscrit est organisé autour de trois chapitres de la façon suivante: Dans le premier chapitre, nous allons donner des généralités sur le cryptage d'images. Au chapitre deux, une analyse détaillée concerne la compression JPEG de l'image, le chapitre trois réservé à la partie pratique et l'étude expérimentale dont nous avons proposé un schéma de cryptage et compression conjoints des images numériques à base de suites chaotiques et nous terminons ce manuscrit par une conclusion et des perspectives.

# Chapitre 1

# *CHAPITRE I : Cryptage Des Images*

---

## **I.1 Introduction**

Dès que les hommes apprirent à communiquer, ils durent trouver des moyens d'assurer la confidentialité d'une partie de leurs communications. Du bâton nommé « scytale » au Vie siècle avant JC, en passant par le carré de Polybe ou encore le code de César, on assista au développement plus ou moins ingénieux de techniques de chiffrement expérimentales dont la sécurité reposait essentiellement dans la confiance que leur accordaient leurs utilisateurs, donc le besoin d'apporter une sécurité accrue remonte sans doute aux origines de l'homme. En effet, le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des informations, c'est-à-dire de les rendre inintelligibles sans une action spécifique. Une première révolution technologique a eu lieu après la première guerre mondiale, mais ce n'est qu'à l'avènement de l'informatique et d'intérêt que la cryptographie prenne tout son sens. Les efforts conjoints d'IBM et de la NSA conduisent à l'élaboration du DES (Data Encryptions Standard), l'algorithme de chiffrement le plus utilisé au monde durant le dernier quart du XXème siècle. À l'ère d'Internet, le nombre d'applications civiles de chiffrement des informations (banques, télécommunications, cartes bleues, multimédia...) explose L'image n'a pas fait l'exception, elle est considérée sans doute comme l'une des formes d'information les plus utilisées. En effet, plusieurs techniques de cryptage d'images ont été développées dans la littérature. Vu l'intérêt grandissant de ce domaine, nous présentons dans ce chapitre un état de l'art sur le cryptage d'images. Après avoir relaté les phases les plus marquantes de l'histoire de la cryptographie en général, nous détaillons les concepts de base et la terminologie utilisés dans ce domaine tout en faisant la revue des travaux existants aussi bien dans le domaine spatial que dans le domaine fréquentiel. Nous abordons aussi les techniques d'évaluation des algorithmes de cryptage d'images [9].

## **I.2 Concepts de base:**

### **I.2.A Cryptologie**

La cryptologie est un mot composé qui tire son origine du grec: cryptos qui signifie secret et logiez qui signifie science. En fait, c'est la science du secret et ne peut être vraiment considérée ainsi que depuis peu de temps. Elle englobe la cryptographie, l'écriture secrète et la cryptanalyse de cette dernière. On dire que la cryptologie est un art ancien et une science nouvelle: un art ancien car Jules César l'utilisait déjà et il fit son apparition dans l'ancien testament sous la forme du code Abasha: une science nouvelle parce que ce n'est que depuis

# *CHAPITRE I : Cryptage Des Images*

---

les années 1970 qu'elle est devenue un thème de recherche scientifique. Cette discipline est liée à beaucoup d'autres, par exemple la théorie des nombres, l'algèbre, la théorie de la complexité, la théorie de l'information, ou encore les codes correcteurs [9].

## **I.2.B Cryptographie**

Est une discipline de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés. Elle se distingue de la stéganographie qui fait passer inaperçu un message dans un autre message alors que la cryptographie rend un message inintelligible à autre que qui-de-droit. Elle utilisée depuis l'Antiquité, mais certaines de ses méthodes les plus importantes, comme la cryptographie asymétrique, datent de la fin du XXe siècle [9].

- **Chiffrement ou cryptage**

Est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement [9].

- **Clé de chiffrement**

Paramètre constitué d'une séquence de symboles et utilisé, avec un algorithme cryptographique, pour transformer, valider, authentifier, chiffrer ou déchiffrer des données [9].

- **Déchiffrement**

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

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

## **I.2.C Cryptanalyse**

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

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

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

# *CHAPITRE I : Cryptage Des Images*

---

- Attaque à texte clair commun (known-plaintext attack en anglais): Le cryptanalyste possède des messages ou des parties de messages en clair ainsi que les versions chiffrées. La cryptanalyse linéaire fait partie de cette catégorie.
- Attaque à texte clair choisi (chosen-plaintext attack en anglais): Le cryptanalyste possède des messages en clair et peut créer les versions chiffrées de ces messages avec l'algorithme que l'on peut dès lors considérer comme une boîte noire. La cryptanalyse différentielle est un exemple d'attaque à texte clair choisi.
- Attaque à texte chiffré choisi (chosen-ciphertext attack en anglais): Le cryptanalyste possède des messages chiffrés et demande la version en clair de certains de ces messages pour mener l'attaque [9].

## **I.3 Les différents types de cryptographie**

Nous pouvons regrouper les systèmes de chiffrement en deux catégories:

### **I.3.A La cryptographie classique**

Dans la cryptographie classique, la méthode et la clé de chiffrement ainsi que celle de déchiffrement sont connues par l'émetteur et le destinataire. La plupart des méthodes de chiffrement classiques reposent sur deux principes essentiels: la substitution et la transposition [10].

### **I.3.B Le chiffrement par substitution**

Le chiffrement par substitution consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou plusieurs autres entités [10].

### **I.3.C Le chiffrement par transposition**

Le chiffrement par transposition (ou le chiffrement par permutation) consiste à faire un réarrangement de l'ordre des lettres qui cache le sens initial. Cette méthode demande de découper le texte clair en blocs de taille identique, et applique la même permutation sur chacun des blocs [10].

### **I.3.D La cryptographie moderne**

La cryptographie moderne se compose de deux grandes familles selon le principe de fonctionnement [10].

# ***CHAPITRE I : Cryptage Des Images***

---

## **I.3.E La cryptographie symétrique ou à clé secrète**

La cryptographie symétrique, également dite à clé secrète (par opposition à la cryptographie asymétrique), est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé. Les algorithmes les plus répandus sont: RC4 DES, AES, 3DES,...etc. [10].

Il existe deux grandes familles de chiffrement dans ce type :

### **I.3.F Chiffrement par blocs**

On désigne par chiffrement par blocs (block-chiper en anglais), tout système de chiffrement (symétrique) dans lequel le message clair est découpé en blocs d'une taille fixée, et chacun de ces blocs est chiffré [10].

### **I.3.J Chiffrement par flots**

Dans un crypto système par flots, le cryptage des messages se fait caractère par caractère ou bit à bit. Combiner la clé aléatoire avec le message bit à bit par l'opération XOR: la taille de la clef est donc égale à la taille du message par exemple:

- RC4: chiffrement octet par octet [10].

### **I.3.H Cryptage hybride**

Le chiffrement hybride (la combinaison entre le cryptage symétrique et asymétrique) d'un message se déroule en deux étapes :

- Dans un premier temps, l'émetteur choisit une clé symétrique K aléatoire. Il utilise ensuite

Cette cle K pour chiffrer (symétriquement) le message.

- Puis il chiffre (asymétriquement) la clé K avec la clé publique du destinataire. Il envoie à son destinataire le message chiffré et de K. Le destinataire déchiffre d'abord la clé K. puis l'utilise pour retrouver le message [10].

## **I.4 Les objectifs de la cryptographie**

Les buts de la cryptographie sont :

### **I.4.A La confidentialité**

Le texte chiffré ne doit être lisible que par les destinataires légitimes. Il ne doit pas pouvoir être lu par un intrus [2].



# *CHAPITRE I : Cryptage Des Images*

---

## **I.4.B Intégrité**

Le destinataire d'un message doit pouvoir vérifier que celui-ci n'a pas été modifié en chemin. Un intrus ne doit pas être capable de faire passer un faux message pour légitime [10].

## **I.4.C Authentification**

Le destinataire d'un message doit pouvoir s'assurer de son origine. Un intrus ne doit pas être capable de se faire passer pour quelqu'un d'autre [10].

## **I.4.D Non-répudiation**

Un expéditeur ne doit pas pouvoir, par la suite, nier à tort avoir envoyé un message [10].

## **I.5 Principes de Kirchhoff en cryptographie**

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

- La sécurité repose sur le secret de la clé et non sur le secret de l'algorithme. Ce principe

est notamment utilisé au niveau des cartes bleues et dans le chiffrement des images et du son sur Canal+.

- Le déchiffrement sans la clé doit être impossible (en temps raisonnable);
- 3. Trouver la clé à partir du clair et du chiffre est impossible (en temps raisonnable)[9].

## **I.6 Cryptage d'images dans le domaine spatial à base de permutations (bit lève)**

L'idée de base de l'utilisation du 'bit lève dans le cryptage d'images dans le domaine spatial est de décomposer l'image en clair ayant un niveau de gris allant de 0 à 255 comme illustrer dans la figure 1.5 en huit images binaires selon la position du bit dans le pixel [10]

# CHAPITRE I : Cryptage Des Images



Image originale de Lena

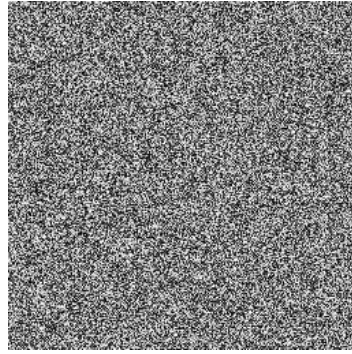


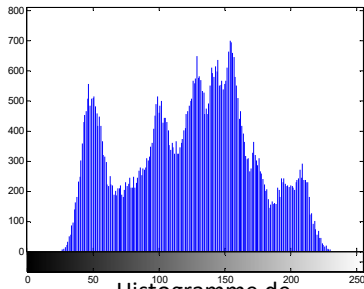
Image cryptée de Lena



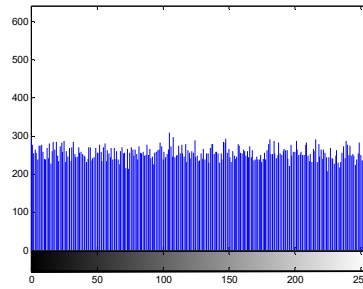
Image décryptée de Lena

Figure.1. le résultat de cryptée et décryptée d'image Lena

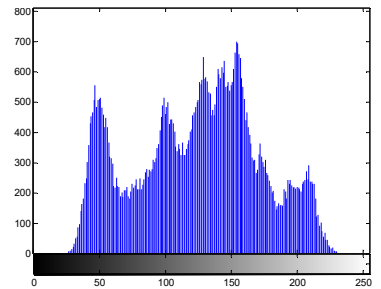
## I.7 Analyse d'histogramme



Histogramme de l'image originale de Lena



Histogramme de l'image cryptée de Lena



Histogramme de l'image décryptée de Lena

Figure.2. Histogramme de l'image de Lena, de l'image cryptée et de l'image décrypté



Image originale de Barbara

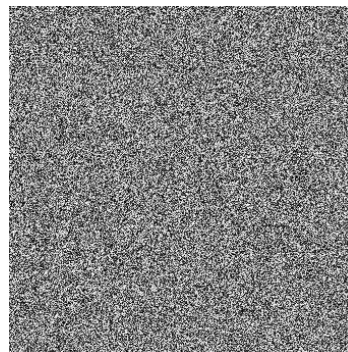


Image cryptée de Barbara



Image décryptée de Barbara

Figure.3. Résultat de l'image cryptée et décryptée de Barbara

# CHAPITRE I : Cryptage Des Images

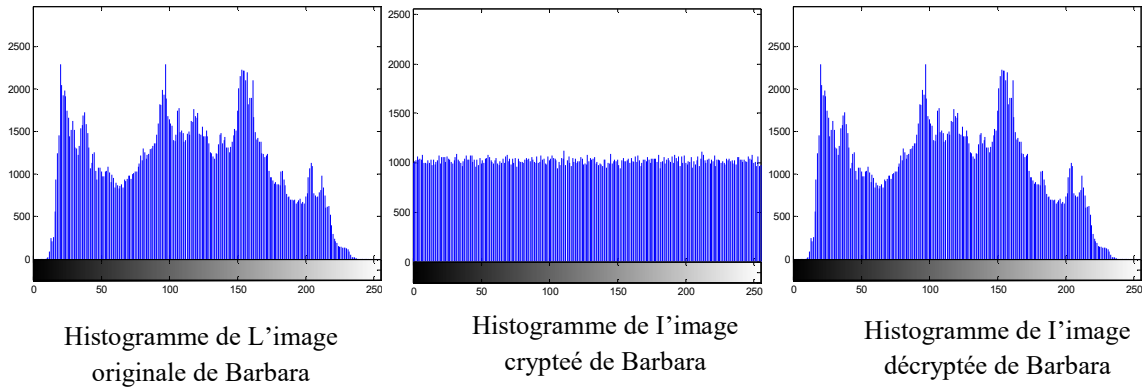


Figure.4.Histogramme de l'image de Barbara, de l'image cryptée et de l'image décryptée

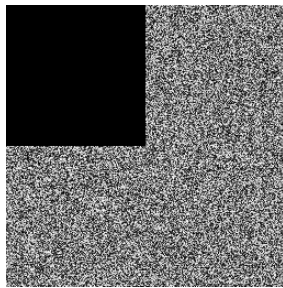


Image cryptée avec pertes de 25 %



Image dècryptée avec pertes de 25 %

Figure.5.Image dècryptée Suite à un lossdata 25 %

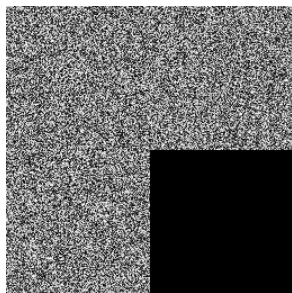


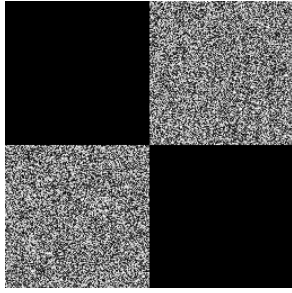
Image cryptée avec pertes de 25 %



Image dècryptée avec pertes de 25 %

Figure.6.Image dècryptée Suite à un loss data 25 %

# CHAPITRE I : Cryptage Des Images



Test de sensibilité



Image cryptée avec pertes de 50 %

Figure.7. Image décryptée Suite à un lossdata 50%

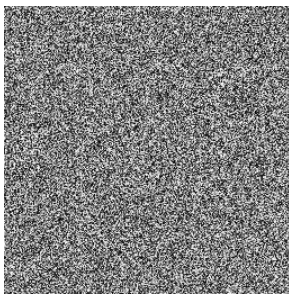


Image décryptée pour  $x1=052+10^{-16}$

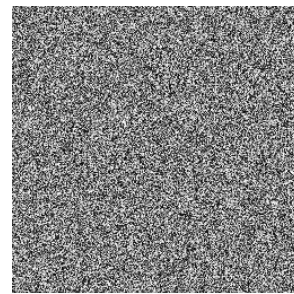


Image décryptée pour  $r1=3.98+10^{-15}$

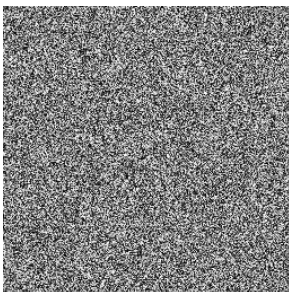


Image décryptée pour  $x2=052+10^{-16}$

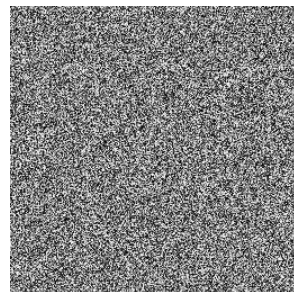


Image décryptée pour  $r2=3.98+10^{-15}$

Figure.8. Sensibilité de la clé de cryptage

## I.8 Applications du cryptage :

La cryptographie est utilisée aujourd'hui dans de nombreuses applications dans les téléphones portables, sur Internet ou pour la télévision à péage. Dans le cas des téléphones mobiles, la cryptographie est utilisée pour assurer la confidentialité des communications. En effet, la loi sur les télécommunications oblige les opérateurs à garantir la sécurité des communications des utilisateurs. En particulier dans le cas des téléphones mobiles, les communications entre le



# ***CHAPITRE I : Cryptage Des Images***

---

téléphone et la station hertzienne sont chiffrées. On utilise uniquement la cryptographie à clé secrète et l'algorithme de chiffrement est un algorithme flot appelé A5 Sur Internet, la cryptographie permet de garantir la confidentialité de certaines communications comme la transmission du code d'une carte bleue « protocole SSL (Secure Sockets Layer) » ou d'assurer la confidentialité, l'intégrité et l'authentification de l'émetteur dans les messageries électroniques protocole S/MIME (Secure/Multipurpose Internet Mail Extensions) [9].

## **I.9 Conclusion**

Dans ce chapitre, nous avons discuté les concepts de base utilisés en cryptologie, nous avons présenté la classification des algorithmes de cryptage d'images, une étude bibliographique des algorithmes spatiaux et fréquentiels pertinents, et les techniques d'évaluation des algorithmes de cryptage. La compression JPEG fera l'objet du chapitre suivant [9].

# Chapitre 2

# CHAPITRE II : La compression JPEG des images fixes

---

## II.1 Introduction

L'homme a toujours voulu découvrir la beauté des planètes, vues de l'espace. Il a donc envoyé des satellites capables de photographier celles-ci. Mais l'un des problèmes majeurs est la transmission de ces photos, du satellite à la terre. Cette communication se fait à l'aide des ondes électromagnétiques. La transmission des informations est d'autant plus facile que le nombre d'informations est faible. Il est donc avantageux d'en réduire le nombre. Une technique employée dans de nombreux domaines est la compression des informations. L'utilisation d'algorithmes de compression d'images permet en effet, une réduction importante de la quantité de données.

Nous allons étudier un algorithme très répandu et utilisé par de nombreuses personnes : le JPEG. Après un bref historique du JPEG, nous allons présenter son principe et son utilisation. Nous aborderons ensuite, un aspect plus mathématique, concernant les théorèmes fondamentaux utilisés pour la compression. Enfin, nous expliquerons la méthode de décompression de ces images. Un applet Java viendra compléter notre dossier, afin de présenter un exemple concret [2].

## II.2 Rappelles sur l'image numérique

### II.2.1 définition

Une image numérique est un signal bidimensionnelle (a deux dimensions, largeur plus Hauteur) fini discret (préalablement échantillonné et quantifié) qui peut être assimilé tel vue sur un écran d'ordinateur à une matrice  $I$   $[M \times N]$  finie où chaque élément  $I$   $(M \times N)$  décente matrice représente un point ou un élément de l'image (appelé : pixel) qui appartient à un espace de couleur fini[1].

### II.2.2 Notions de pixel et espace de couleurs

L'acronyme pixel c'est la contraction de « Picture élément », il représente un point de l'image. La clarté ou la définition de l'image est proportionnelle aux nombres de pixel, c'est la résolution d'une image. Pour une image de bonne qualité la résolution doit être au minimum de  $300\text{px}/2.54\text{cm}$  ( $2.54\text{cm} = 1$  Pouce). Par ex le nombre de pixel dans une image de résolution  $640 \times 480$  pixel:  $640 \times 480 = 307200$  pixels Chaque pixel est représenté dans un espace de couleur finis. Pour une image de niveau gris, par exemple, chaque pixel est représentée sur une échelle de 256 niveaux de gris où chaque niveau représente l'intensité de

# CHAPITRE II : La compression JPEG des images fixes

la luminosité du pixel. Cet espace de couleur nécessite 8 bits pour être codé ( $2^8=256$ ), c'est des images 8 bits.

Typiquement pour un espace de couleur RVB (Rouge, Vert, Bleu), une image chromatique nécessite pour chaque pixel trois couches de niveaux de luminosité des trois couches de couleurs RVB. Cela nécessite au total  $3*8 = 24$  bits pour coder un pixel, où chaque couleur de pixel est représentée sur une échelle de près de 16 millions de niveaux de couleurs ( $2^{24}$ ),

Problème : Le poids des données de l'image numérique sont proportionnelles à la Résolution de l'image [1].

Solution : Compresser les données de l'image numérique.

## II.3 Rappel sur la comprissions des images

La compression des données ou le codage source, permet on appliquant des algorithmes de compression spécifiques de réduire la taille d'une image sur une mémoire ou de manière équivalente de réduire son temps de transmission [3].

### Image originale

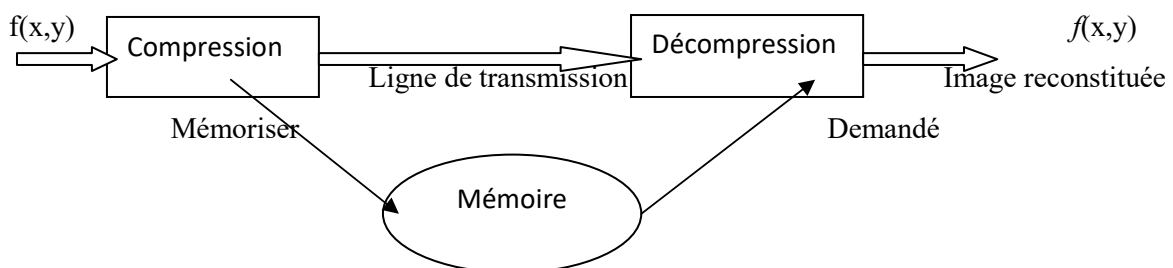


Figure.1. Principe de la compression image.

La compression peut être sans perte, l'image restera fidèle à l'image originale, soit elle sera avec perte de qualité (fidélité) pour réduire plus la taille de l'image, dans ce cas-là, la compression sera au prix de la dégradation autorisée, ces types de compression sont faites grâce aux redondances des données présentes sur l'image. Ces redondances sont :

- Redondance psycho visuel** : Des détails non perceptible à l'œil humain qu'on peut éliminer.
- Redondance inter pixel** : La possible corrélation existante entre les pixels de l'image, on dit Qu'une image a une redondance inter pixel si c'est possible de prédire la valeur d'un pixel en



# CHAPITRE II : La compression JPEG des images fixes

connaissance de la valeur des pixels voisins (suivants ou précédant), sachant que plus la Résolution de l'image est grande plus la probabilité de rencontrer des redondances inter pixel Est élevée [3].

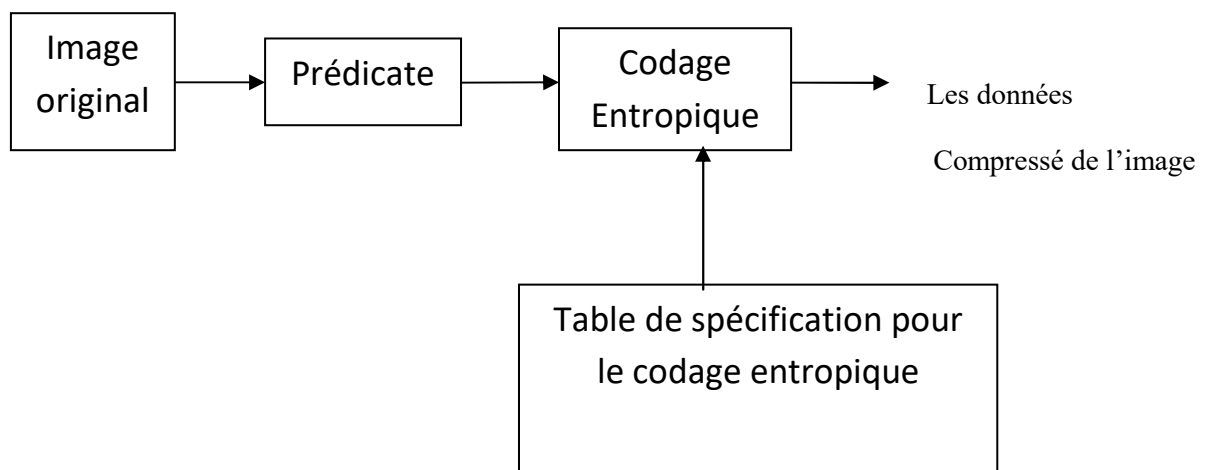
-**Redondance de codage** : séquences de répétition des bits, on rencontre cela généralement à la fin de la compression, pendant l'étape de codage[1].

## II.3.1 Compression avec perte et sans perte

On peut distinguer deux grandes familles d'algorithmes de compression : les méthodes dites sans perte ou réversibles garantissent la restitution parfaite des images, alors que les méthodes dites avec perte ou irréversibles modifient plus ou moins la valeur des pixels.

## II.3.2 La compression sans perte JPEG

Le mode de fonctionnement sans perte JPEG – LS (louses en anglais) ou non destructif est une simple méthode basée sur le codage prédictif de la méthode DPCM (Différentia Pulse Code Modulation) en utilisant les valeurs des pixels voisins. La figure II.1 montre un tel codeur .le prédicateur est de type simple DPCM où chaque pixel de chaque composante couleur est codé d'une manière différentielle .la prédiction d'un pixel d'entrée x est effectuée à partir des trois pixels voisins de la même composante de couleur. Ce prédicateur; connu sous le nom Médiane Edge Detector (MED) Voir Figure.2.



**Figure.2.** Schéma de bloc du codeur JPEG en mode sans perte.

La prédiction est ensuite soustraite de la valeur réelle du pixel à la position x et la différence est codée en entropie soit par la technique Huffman, soit par le codage arithmétique. Les

# CHAPITRE II : La compression JPEG des images fixes

---

spécifications du tableau d'entropie **figure.3.** déterminent les caractéristiques de la méthode choisie pour le codage entropique.

		C	B		
		A	X		

**Figure.3.** Le voisinage de la prédiction du prédicateur MED.

L'idée de technique prédictive est d'éliminer la redondance mutuelle entre les pixels voisins (a,b,c) et de coder seulement l'information non redondante qui représente l'erreur de prédiction c'est à dire la différence entre la valeur du pixel(x) et sa valeur prédite à partir de ses voisins [4].

### II.3.3 La compression avec perte du JPEG

Le mode de fonctionnement avec perte JPEG (Losey en anglais) permet des taux de compression nettement supérieurs, mais impose de négliger arbitrairement certaines informations de l'image, en tenant compte de sa nature et de notre perception visuelle.

Pour des raisons à la fois historiques (rapidité de calcul), de précision et enfin de corrélation entre pixels, l'algorithme de compression s'effectue sur des imageâtes de bloc, de taille 8×8. C'est à l'application de scinder chacune des composantes de l'image en de tels blocs et de régler le cas des dimensions d'images qui ne sont pas des multiples entiers de 8. Tous les blocs, ou encore vecteurs, sont traité successivement et identiquement au cours des trois étapes successives : une transformation linéaire (DCT), une quantification scalaire, un codage entropique. Le décodeur s'effectue les opérations inverses.

L'algorithme JPEG avec pertes fonctionne conformément au schéma de la **Figure.4.** L'image originale subit une transformation colorimétrique suivie d'un sous échantillonnage des composantes de chrominance. L'image résultante est découpée en blocs de 8×8. Une transformation DCT bidimensionnelle est appliquée sur chaque bloc, suivi par l'étape de

# CHAPITRE II : La compression JPEG des images fixes

quantification. Enfin, un codage entropique sans perte est appliqué sur l'ensemble des coefficients quantifiés [4].

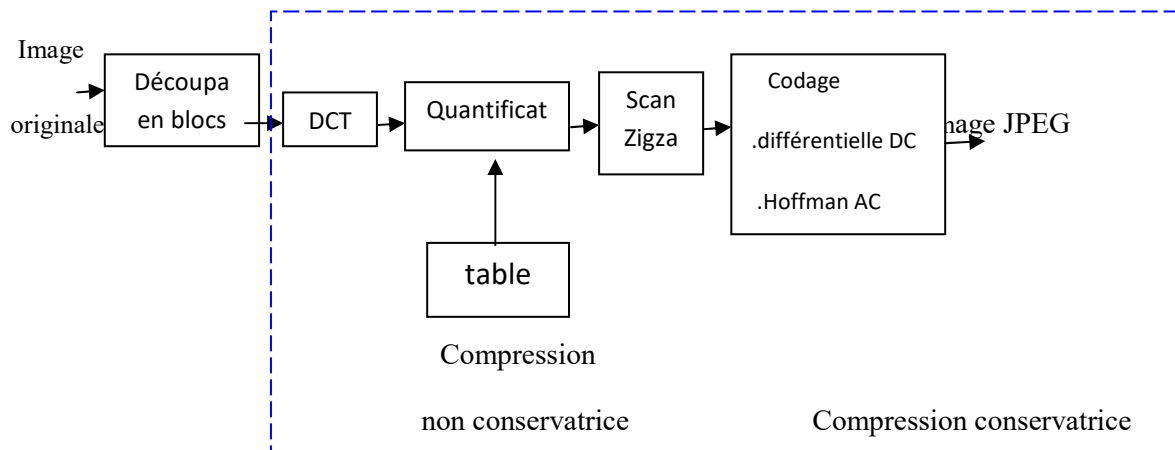


Figure .4. Chaîne de codage de l'algorithme JPEG.

## II.3.4 Principe général de la compression d'images

Le schéma fonctionnel de la compression est représenté dans la figure ci-dessous :

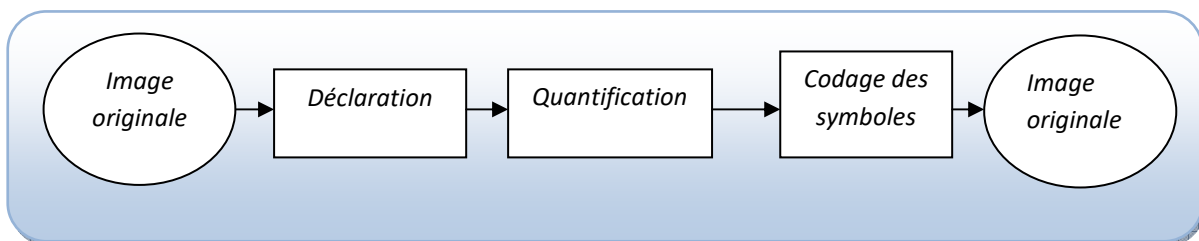


Figure.5. Schéma général d'un codeur source.

## II.3.5 Décorrélation

La dépendance existante entre chaque pixel et ses voisins (la luminosité varie très peu d'un pixel à son voisin) traduit une corrélation très forte dans l'image. On essaie donc de tirer partie de cette corrélation, pour réduire le volume d'information, en effectuant une opération de décorrélation des pixels. Cette décorrélation consiste à transformer les pixels initiaux en un ensemble de coefficients moins corrélés, c'est une opération réversible [5].

## II.3.6 Quantification

# CHAPITRE II : La compression JPEG des images fixes

---

La quantification des coefficients obtenus a pour but de réduire le nombre de bits nécessaires pour leurs représentations. Celle-ci représente une étape clé de la compression. Elle approxime chaque valeur d'un signal par un multiple entier d'une quantité  $q$ , appelée «quantum élémentaire» ou «pas de quantification».

La quantification peut être scalaire ou vectorielle. L'un des résultats fondamentaux des travaux de Shannon concernant la relation : débit/distorsion montrent que l'on obtient de meilleures performances en utilisant la quantification vectorielle.

Une fois les coefficients quantifiés, ils sont codés. Un codeur doit satisfaire à priori les conditions suivantes :

- **Unicité** : deux messages différents ne doivent pas être codés de la même façon,
- **Déchiffrabilité** : deux mots de codes successifs doivent être distingués sans ambiguïté [5].

## II.3.7 Codage des symboles (Symbols coding)

Cette étape permet de réduire la redondance de codage en utilisant des codes VLC ou Autres. Le décodage source : c'est les mêmes blocs des schémas précédents mais dans le sens Inverse et chaque bloc effectue l'opération inverse de celle au codage [3].

## II.4 Notions sur la DCT

Nous allons parler seulement de certains aspects importants à connaître pour l'achèvement de l'objet de ce travail qui est la compression d'images sans entrer dans les démonstrations Mathématiques [3].

### II.4.1 Définition

La DCT est une fonction linéaire inversible  $\mathbb{R}^N \rightarrow \mathbb{R}^N$  ou de manière équivalente une matrice carrée  $N \times N$  inversible. Il existe plusieurs légères variantes de la DCT. Voici les quatre types les plus connus. Le développement des algorithmes de calcul rapide des transformées DCT se basent sur la possibilité de décomposer la matrice de définition sous forme d'un produit de matrices dont le calcul est plus simple, et permet de réduire le nombre de multiplications scalaires, en profitant des identités remarquables de périodicité et symétries des fonctions sinusoïdales. Ainsi, on peut décomposer toute transformée DCT de  $\mathbb{R}^N$  en transformées plus simples en décomposant  $N$  en produit de facteurs premiers, et en composant des sous-transformées dans  $\mathbb{R}^n$  où  $n$  est l'un de ces facteurs. En particulier, de nombreuses optimisations ont été développées quand  $N$  est une puissance de 2. Cela revient à réécrire la

# CHAPITRE II : La compression JPEG des images fixes

---

matrice  $N \times N$  sous forme de produit de sous-matrices identiques (disposées en pavage régulier et utilisant donc des coefficients réels communs ou différenciés uniquement par leur signe) et de matrices à coefficients unitaires ou nuls (-1, 0 ou 1), ces dernières ne nécessitant pas de multiplication.

## II.4.2 Variantes de la DCT

Il existe 8 variantes de la DCT, ceux les plus connus sont DCT I, la DCT 2D ou DCT II et sa Transformée inverse IDCT ou DCT III, nous allons voir la définition de la DCT I, DCT II et DCT III qui sont la base de la compression JPEG [3].

### II.4.2.a DCT-I

$$X_K = \frac{1}{2} (x_0 + (-1)^k x_{N-1}) + \sum_{n=1}^{N-2} x_n \cos\left[\frac{\pi}{N-1} nk\right] \quad N=0, \dots, N-1. \quad (1)$$

Certains auteurs multiplient encore les termes et par et multiplient en conséquence les termes et par ce qui rend la matrice DCT-I orthogonale. Si l'on multiplie encore par un facteur d'échelle global de mais rompt la correspondance directe avec un DFT réel pair.

$$x_{N-1} \sqrt{2}, X_0 \frac{x_{N-1}}{\sqrt{2}}, \sqrt{\frac{2}{N-1}}. \quad (2)$$

Le DCT-I est exactement équivalent (jusqu'à un facteur d'échelle global de 2), à un DFT de nombres réels avec une symétrie paire. Par exemple, un DCT-I de nombres réels est exactement équivalent à un DFT de huit nombres réels (symétrie paire), divisé par deux. (En revanche, les types DCT II-IV impliquent un décalage d'un demi-échantillon dans la DFT équivalente.)

$$2(N-1)N = 5 a b c d e a b c d e d c b. \quad (3)$$

Notez, cependant, que le DCT-I n'est pas défini pour moins de 2. (Tous les autres types de DCT sont définis pour tout N N.

Ainsi, le DCT-I correspond aux conditions aux limites : est pair autour et pair autour ; de même pour  $x_n$   $n = 0$   $n = N - 1$   $X_K$ . [8]. (4)

### II.4.2.b DCT-II

# CHAPITRE II : La compression JPEG des images fixes

---

$$X_K = \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi}{N}\left(n + \frac{1}{2}\right)k\right] \quad N=0, \dots, N-1. \quad (5)$$

Le DCT-II est probablement la forme la plus couramment utilisée et est souvent simplement appelé « le DCT ». Cette transformation est exactement équivalente (jusqu'à un facteur échelle global de 2) à une DFT d'entrées réelles de symétrie paire où les éléments à index pair sont nuls. C'est-à-dire qu'il s'agit de la moitié de la DFT des entrées où pour et pour la transformation DCT-II est également possible en utilisant un signal  $2N$  suivi d'une multiplication par demi-décalage. Ceci est démontré par Mahous.

$$4N \quad y_n, y_{2n} = 0, y_{2n+1} = x_n \quad 0 \leq n < N, y_{2N} = 0, y_{4n-n} = y_n \quad 0 < n < 2N. \quad (6)$$

Certains auteurs multiplient encore le terme par et multiplient la matrice résultante par un facteur d'échelle global de (voir ci-dessous pour le changement correspondant dans DCT-III). Cela rend la matrice DCT-II orthogonale, mais rompt la correspondance directe avec une DFT réelle paire d'entrée semi-décalée. C'est la normalisation utilisée par Matlab, par exemple, voir. Dans de nombreuses applications, telles que JPEG, la mise à l'échelle est arbitraire car les facteurs d'échelle peuvent être combinés avec une étape de calcul ultérieure (par exemple, l'étape de quantification dans JPEG), et une mise à l'échelle peut être choisie qui permet de calculer le DCT avec moins de multiplications.  $X_0, 1/\sqrt{2}, \sqrt{\frac{2}{N}}$ . [8]. (7)

## II.4.3 Propriétés de la DCT

Dans la section précédente, nous avons développé la base mathématique de la DCT. Cette section expose (avec des exemples) quelques propriétés de la DCT qui sont particulièrement importantes aux applications de traitement d'image.

### II.4.3.a Décorrélation

Comme on a discuté précédemment, l'avantage principal de la transformation d'image est la réduction de redondance entre ces pixels voisins. Ceci mène à des coefficients transformés non-corrélés qui peuvent être codés indépendamment.

### II.4.3.b Concentration des coefficients

# CHAPITRE II : La compression JPEG des images fixes

---

La DCT est très efficace pour des images fortement corrélée du fait qu'elle permet décompacté les coefficients qui représente les basses fréquences dans une seule partition de la matrice image, cela permet la séparation des fréquences basses des fréquences hautes, et si c'est une image faiblement corrélée, les coefficients sont concentrés dans plusieurs différentes partitions de la matrice image [3].

### II.4.3.c Séparabilité

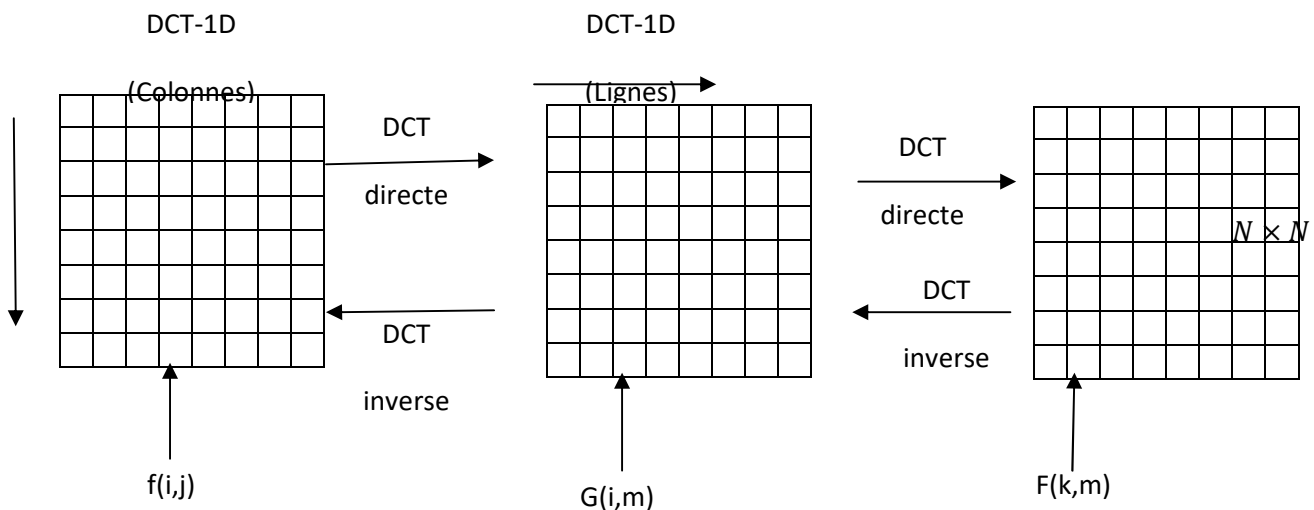
L'équation (8) de la DCT peut être exprimée comme

$$F(k, m) = a(k)a(m) \sum_{i=0}^{N-1} \cos\left[\frac{\pi(2i+1)k}{2N}\right] \sum_{j=0}^{N-1} f(i, j) \cos\left[\frac{\pi(2j+1)m}{2N}\right] \quad (8)$$

$$F(k, m) = a(k) \sum_{i=0}^{N-1} G(i, m) \cos\left[\frac{\pi(2i+1)k}{2N}\right] \quad (9)$$

$$G(i, m) = a(m) \sum_{j=0}^{N-1} f(i, j) \cos\left[\frac{\pi(2j+1)m}{2N}\right] \text{ où } k, m = 0, 1, 2, \dots, N-1, \quad (10)$$

et  $\alpha(k)$  et  $\alpha(m)$  sont donnés par l'équation (10). Cette propriété, connue par la séparabilité, a l'avantage principal où  $F(k, m)$  peut être calculé dans deux étapes par les opérations successives unidimensionnelles (1D) sur les lignes et les colonnes d'image. Cette idée est illustrée graphiquement sur la **Figure.6**. Les arguments présentés peuvent être identiquement appliqués pour le calcul inverse de la DCT [7].



**Figure.6.** Les arguments présentés peuvent être identiquement appliqués pour le calcul inverse de la DCT.

### II.4.3.d Symétrie

# CHAPITRE II : La compression JPEG des images fixes

---

Un autre regard sur l'équation (11) indique que la multiplication d'une matrice par la DCT nécessite les mêmes opérations pour les lignes que pour les colonnes, une telle transformation s'appelle une transformation symétrique. Une transformation séparable et symétrique peut être exprimée sous la forme :

$$F = T_N \times f \times T_N^t \quad (11)$$

où F est la matrice transformée, f est la matrice d'image originale et TN est la matrice de la transformée de taille N× N avec des éléments T (i j) N , donné par l'équation (12)

$$T_N(i, j) = \begin{cases} \frac{1}{\sqrt{2}} & \text{si } i = 0 \\ \sqrt{\frac{2}{N}} \cos \left[ \frac{(2j+1)i\pi}{2N} \right] & \text{si } i > 0 \end{cases} \quad (12)$$

$T_N^t$  est la matrice transposée de  $T_N$ .

C'est une propriété extrêmement utile puisqu'elle implique que la matrice transformée peut être pré-calculée et s'est appliquée alors à l'image, fournissant de ce fait une amélioration d'efficacité de calcul [7].

### II.4.3.e Orthogonalité

La matrice  $T_N$  de la DCT est orthogonale par ce qu'elle vérifie :

$$T_N \times T_N^t = I_N \quad (13)$$

où  $I_N$  représente la matrice d'identité de taille N×N. Cette propriété peut être vérifiée directement par :

$$V_i V_j^t = \sum_{k=0}^{N-1} V_{ik} V_{jk} = 0 \quad \forall i \neq j, i, j = 0, 1, \dots, N-1 \quad (14)$$

où  $V_i$  et  $V_j$  sont les vecteurs de base de  $T_N$ . Ainsi, la matrice inverse de  $T_N$  est égale à sa transposée, i.e.  $T_N^{-t} = T_N^t$ . Par conséquent, et en plus de ses caractéristiques de décorrélation, cette propriété fournit une certaine réduction dans la complexité de pré-calcul.

En exploitant l'orthogonalité de  $T_N$ , l'inverse de la transformation donnée par l'équation (I.12) est donnée par [7]:

$$f = T_N \times F \times T_N^t \quad (15)$$

## II.5 Processus général d'un codec JPEG d'images fixes



# CHAPITRE II : La compression JPEG des images fixes

---

## II.5.1 Définition

**JPEG:** Joint Photographique Experts Group.

C'est un algorithme standard de compression avec perte d'image fixe établi en 1991 basé sur le codage par la transformé en cosinus discrète DCT, et il existe plusieurs modes opératoires de compression JPEG établies selon la rapidité du codec et le besoin

- Codage basé sur la DCT séquentielle.
- Codage basé sur la DCT progressive.
- Codage sans perte.
- Codage hiérarchique [3].

## II.5.2 JPEG basée sur la DCT séquentielle

Celui que nous allons aborder sur ce travail c'est celui basé sur la DCT séquentielle, où l'image est traitée de gauche à droite et de haut en bas [3].

## II.5.3 Découpage en sous blocs

L'image au début elle est découpée en sous-bloc de 8x8 (ou 16x16), chaque sous-bloc sera traité individuellement, si c'est une image couleur il faut avant tout faire une transformation couleur ensuite un sous échantillonnage, nous n'allons pas s'étaler sur ce sujet [1].

## II.5.4 Décalage de niveau (Level Shifting)

Deuxième étape, préréglage (offset), en effectuant un décalage de niveaux, en anglais «Level shifting» (pour une image monochrome, c'est les niveaux du gris codés sur 8bits), où chaque élément de chaque sous blocs doit être amené à l'intervalle  $[-128,127]$ , pour faire cela, on soustrait à chaque élément un scalaire 128, cela va permettre d'augmenter la tolérance de précision des coefficients de la DCT [3].

## II.5.5 Application de la DCT

La norme JPEG Applique la DCT pas à l'image entière mais aux unités de données (blocs) de  $8 \times 8$  pixels.

$$F(k, m) = \frac{1}{4} \alpha(m) \sum_{i=0}^7 \sum_{j=0}^7 f(i, j) \cos \left[ \frac{\pi(2i+1)k}{16} \right] \cos \left[ \frac{\pi(2j+1)m}{16} \right] \quad (16)$$

$$\alpha = \begin{cases} \frac{1}{\sqrt{2}} & \text{pour } k = 0 \\ 1 & \text{pour } k \neq 0 \end{cases} \quad \text{et } 0 \leq i = (k, m) \leq 7 \quad (17)$$

# CHAPITRE II : La compression JPEG des images fixes

---

La matrice de la DCT pour N=8 est donnée d'après l'équation (18) par [7] :

$$T_8 = \begin{bmatrix} \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{8}} \\ \frac{1}{2} \cos \frac{\pi}{16} & \frac{1}{2} \cos \frac{3\pi}{16} & \frac{1}{2} \cos \frac{5\pi}{16} & \frac{1}{2} \cos \frac{7\pi}{16} & \frac{1}{2} \cos \frac{9\pi}{16} & \frac{1}{2} \cos \frac{11\pi}{16} & \frac{1}{2} \cos \frac{13\pi}{16} & \frac{1}{2} \cos \frac{15\pi}{16} \\ \frac{1}{2} \cos \frac{2\pi}{16} & \frac{1}{2} \cos \frac{6\pi}{16} & \frac{1}{2} \cos \frac{10\pi}{16} & \frac{1}{2} \cos \frac{14\pi}{16} & \frac{1}{2} \cos \frac{18\pi}{16} & \frac{1}{2} \cos \frac{22\pi}{16} & \frac{1}{2} \cos \frac{26\pi}{16} & \frac{1}{2} \cos \frac{30\pi}{16} \\ \frac{1}{2} \cos \frac{3\pi}{16} & \frac{1}{2} \cos \frac{9\pi}{16} & \frac{1}{2} \cos \frac{15\pi}{16} & \frac{1}{2} \cos \frac{21\pi}{16} & \frac{1}{2} \cos \frac{27\pi}{16} & \frac{1}{2} \cos \frac{33\pi}{16} & \frac{1}{2} \cos \frac{39\pi}{16} & \frac{1}{2} \cos \frac{45\pi}{16} \\ \frac{1}{2} \cos \frac{4\pi}{16} & \frac{1}{2} \cos \frac{12\pi}{16} & \frac{1}{2} \cos \frac{20\pi}{16} & \frac{1}{2} \cos \frac{28\pi}{16} & \frac{1}{2} \cos \frac{35\pi}{16} & \frac{1}{2} \cos \frac{44\pi}{16} & \frac{1}{2} \cos \frac{52\pi}{16} & \frac{1}{2} \cos \frac{60\pi}{16} \\ \frac{1}{2} \cos \frac{5\pi}{16} & \frac{1}{2} \cos \frac{15\pi}{16} & \frac{1}{2} \cos \frac{25\pi}{16} & \frac{1}{2} \cos \frac{35\pi}{16} & \frac{1}{2} \cos \frac{44\pi}{16} & \frac{1}{2} \cos \frac{55\pi}{16} & \frac{1}{2} \cos \frac{65\pi}{16} & \frac{1}{2} \cos \frac{75\pi}{16} \\ \frac{1}{2} \cos \frac{6\pi}{16} & \frac{1}{2} \cos \frac{18\pi}{16} & \frac{1}{2} \cos \frac{30\pi}{16} & \frac{1}{2} \cos \frac{42\pi}{16} & \frac{1}{2} \cos \frac{53\pi}{16} & \frac{1}{2} \cos \frac{66\pi}{16} & \frac{1}{2} \cos \frac{78\pi}{16} & \frac{1}{2} \cos \frac{90\pi}{16} \\ \frac{1}{2} \cos \frac{7\pi}{16} & \frac{1}{2} \cos \frac{21\pi}{16} & \frac{1}{2} \cos \frac{35\pi}{16} & \frac{1}{2} \cos \frac{49\pi}{16} & \frac{1}{2} \cos \frac{62\pi}{16} & \frac{1}{2} \cos \frac{77\pi}{16} & \frac{1}{2} \cos \frac{91\pi}{16} & \frac{1}{2} \cos \frac{105\pi}{16} \end{bmatrix} \quad (18)$$

## II.5.6 Quantification

Dans le bloc de 8×8 issu de la DCT, on a noté que la majorité de l'énergie du signal original est concentrée dans le coefficient DC (en haut à gauche du bloc de 8 × 8 coefficients) et dans quelques autres coefficients autour de celui-ci. En effet, les autres coefficients AC, en particulier ceux se situant en bas à gauche et à droite du bloc de 8 × 8 , représentant les hautes fréquences et n'apportent donc que de la précision sur le signal original dans le bloc. Cette analyse permet de conclure à une quantification faible (petit pas de quantification) pour les coefficients se situant en haut à gauche du bloc et à une quantification. de plus en plus forte (pas de quantification de plus en plus grand) à mesure que l'on se rapproche du coin inférieur droit et gauche du bloc. Cette quantification est donc réalisée par une matrice de quantification  $Q$  de la taille du bloc de 8 × 8 pixels. Elle s'applique sur un bloc de la DCT de telle sorte que :

$$F^*(u, v) = \text{entier le plus proche de } \frac{F(u,v)}{Q(u,v)} \quad (19)$$

Avec :

$F^*(u,v)$  est la matrice quantifiée ,  $F(u,v)$  est la matrice des coefficients à quantifier et,  $Q(u,v)$ est la table de quantification.

Et pour la quantification inverse :

$$F(u, v) = F^*(u, v) \times Q(u, v) \quad (20)$$

Avec  $F(u,v)$  représente la matrice de quantifiée .

Dans les traitements d'images actuels, la table de quantification est définie par :

# CHAPITRE II : La compression JPEG des images fixes

---

$$Q(u,v) = 1 + (1 + i + j)F_q \quad (21)$$

Où  $F_q$  : Représente le facteur de qualité de la matrice de quantification. Plus  $F_q$  est grand, plus  $Q$  rendra les coefficients de la matrice à compresser se rapprochant du coin supérieur gauche à des valeurs nulles, et donc plus le signal bidimensionnel original sera dégradé. Plus  $F_q$  est grand, plus la compression sera forte mais moins bonne sera la qualité de l'image reconstituée :  $F_q$  détermine le compromis à faire entre le gain en compression et la qualité de l'image reconstituée par rapport à l'image d'origine [6].

## II.5.7 Exemple

Soit  $F_q = 5$ , alors la matrice de quantification  $Q$  sera :

$$Q = \begin{bmatrix} 6 & 11 & 16 & 21 & 26 & 31 & 36 & 41 \\ 11 & 16 & 21 & 26 & 31 & 36 & 41 & 46 \\ 16 & 21 & 26 & 31 & 36 & 41 & 46 & 51 \\ 21 & 26 & 31 & 36 & 41 & 46 & 51 & 56 \\ 26 & 31 & 36 & 41 & 46 & 51 & 56 & 61 \\ 31 & 36 & 41 & 46 & 51 & 56 & 61 & 66 \\ 36 & 41 & 46 & 51 & 56 & 61 & 66 & 71 \\ 41 & 46 & 51 & 56 & 61 & 66 & 71 & 76 \end{bmatrix}$$

Lors de la décompression de l'image, il suffit de multiplier chaque bloc de  $8 \times 8$  coefficients quantifiée par la matrice de quantification pour obtenir une estimation du bloc original. Revenant à notre exemple précédent. Pour quantifier notre matrice  $F$  résultante de la DCT nous avons pris la matrice de quantification suivante [6]:

$$Q = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 62 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 03 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Ce qui donne comme matrice des fréquences quantifiées et arrondies en entier le plus proche :

# CHAPITRE II : La compression JPEG des images fixes

---

$$F^* = \begin{bmatrix} 79 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ -2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

## II.5.8 Le codage entropique

Ce codage combine deux étapes. La première c'est le codage intermédiaire des coefficients DC et AC et la deuxième c'est le codage d'Huffman des coefficients différentiels Diff DC et des coefficients AC[6] :

### II.5.8.a Les coefficients DC

Comme la variation des coefficients DC est très petite d'un bloc à un autre bloc adjacent, on codera non pas les coefficients DC mais la différence de deux coefficients entre deux blocs adjacents noté Diff DC ( $i$ ) = DC ( $i$ ) - DC ( $i - 1$ ). Les coefficients DC sont codés selon une prédiction unidimensionnelle entre le coefficient du bloc courant ( $i$ ) et le coefficient du bloc précédent ( $i-1$ ) (Figure.7.), seul le coefficient du premier bloc d'image sera transmis sous sa forme absolue[6].

$$\text{Diff DC } (i) = \text{DC } (i) - \text{DC } (i - 1)$$

Cette différence est codée comme suivant :

On assigne au coefficient différentiel Diff DC ( $i$ ) deux symboles de longueur variable.

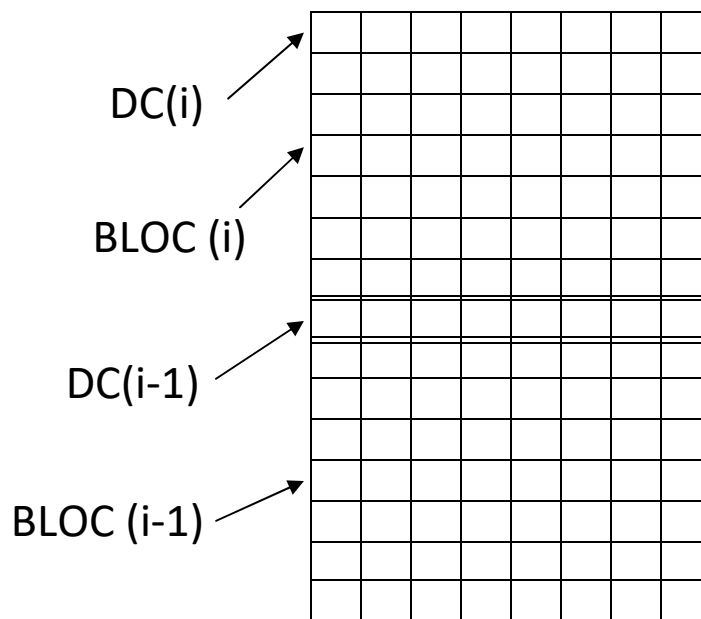
SIZE / AMPLITUDE

SIZE : définit la catégorie d'amplitude ou appartient le coefficient Diff DC ( $i$ ) (voir tableau (I I-1)) et qui est codée de 4 bits qu'on notera (SSSS) en binaire.

AMPLITUDE: représente la valeur de l'amplitude du coefficient différentiel Diff DC ( $i$ ) en binaire.

# CHAPITRE II : La compression JPEG des images fixes

---



**Figure.7.**codage différentiel des coefficient DC.

**Tableau.1.**Catégories d'amplitudes des différences DC

Catégorie	SSSS	Amplitude
0	0000	0 -
1	0001	1 à 0,0 à 1
2	0010	-3 à -2,2 à 3
3	0011	-7 à -4,4 à 7
4	0100	-15 à -8,8 à 15
5	0101	-31 à -16,16 à 31
6	0110	-63 à -32,32 à 63
7	0111	-127 à -64,64 à 127
8	1000	-255 à -128,128 à 255
9	1001	-511 à -256,256 à 1023
10	1010	-1023 à -512,512 à 1023
11	1011	-2047 à -1024,1024 à 2047

**Remarque :**

Pour les nombres négatifs on va écrire le complément à 1 de la valeur absolue en la Diff DC (i) de l'amplitude [6].

### II.5.8.b Les coefficients AC

Les coefficients AC seront récupérer sur un vecteur par un scan en zig-zag de la matrice de chaque sous bloc afin de mettre les coefficients élevées en premier et les zéros en fin comme illustré dans la figure V.3.Ensuite, ces coefficients seront codés par le codage RLC

# CHAPITRE II : La compression JPEG des images fixes

(Run Length Coding) où les suites de coefficients AC qui se suivent de même valeurs sont codées par leurs nombre de redondance sur la séquence par ex [1] :

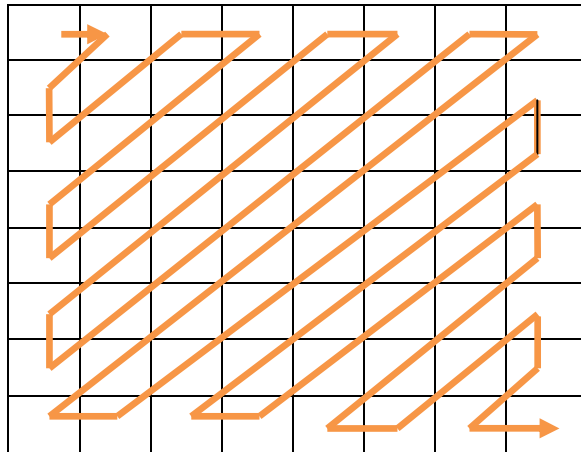


Figure.8.Scan zig-zag

Zig-zag :

```
-25  2  2  2  2  1  0  0  0  0  0  -1  0  0  0
      0  0  0  0  0  0  0  0  0  0  0  0  0  0
      0  0  0  0  0  0  0  0  0  0  0  0  0  0
      0  0  0  0  0  0  0  0  0  0  0  0  0  0
      0  0  0  0  0  0  0
```

RLC : -25 @ 5 2 1 0 1 @ 5 0 -1 EOB

EOB (End Of Block) veut dire le reste des coefficients de la matrice sont à zéros, et @ suivis du nombre de redondance de la valeur qui suit, par exemple : @ 5 0 veut dire que c'est une suite de cinq 0. Enfin, les deux vecteurs DC et AC seront réunis sur un même vecteur pour le codage entropique Huffman [1].

## II.5.9 Codage Huffman

Le codage Huffman, crée des codes à longueurs variables sur un nombre entier de bits. L'algorithme considère chaque message à coder comme étant une feuille d'un arbre qui reste à construire. L'idée est d'attribuer aux messages de plus faibles probabilités, les mots codés les plus longs et les mots codés les plus courts pour les messages de fortes probabilités [6].

# CHAPITRE II : La compression JPEG des images fixes

---

## II.5.9.a Le principe est le suivant

1. Calculer la probabilité associée à chaque symbole dans la chaîne à coder.
2. Classer les probabilités d'apparition des symboles par ordre de probabilités décroissantes.
3. Sommer les deux plus faibles probabilités correspondantes aux deux symboles de la séquence (la plus petite probabilité prene un 0 et celle plus grande prene un 1) ; ce qui nous donne une nouvelle probabilité.
4. Répéter les opérations 2 et 3, jusqu'à ce qu'il ne reste que deux probabilités (la racine).
5. Lire le code binaire de chaque symbole de haut vers le bas [6].

## II.5.9.b Exemple de codage Hoffman

Soit une source composée d'un alphabet de 8 symboles avec les probabilités données sur le **Tableau.2.**

**Tableau.2.** Symboles avec leurs probabilités.

Symbole	A	B	C	D	E	F	G	H
<b>Probabilité</b>	0.01	0.02	0.05	0.09	0.18	0.19	0.21	0.25

L'arbre de Huffman est alors donné par la **Figure.3.**

Le Codage des symboles est alors donné par le **Tableau.3** [6].

## II.6 Mise en œuvre sous Matlab

J'ai utilisé la boîte à outils de traitement d'images (Image Processing Toolbox) de Matlab pour l'opération de lecture, conversion et affichage des graphiques.

### II.6 .1 Représentation d'images sous Matlab

Matlab supporte 4 formats d'images :

- les images binaires,
- les images d'intensités ( a niveaux de gris),
- les images couleur RGB,
- les images couleur indexées.'

# CHAPITRE II : La compression JPEG des images fixes

Tableau.3.Code des symboles.

Symbole	A	B	C	D	E	F	G	H
Code	110000	110001	11001	1101	111	00	01	10

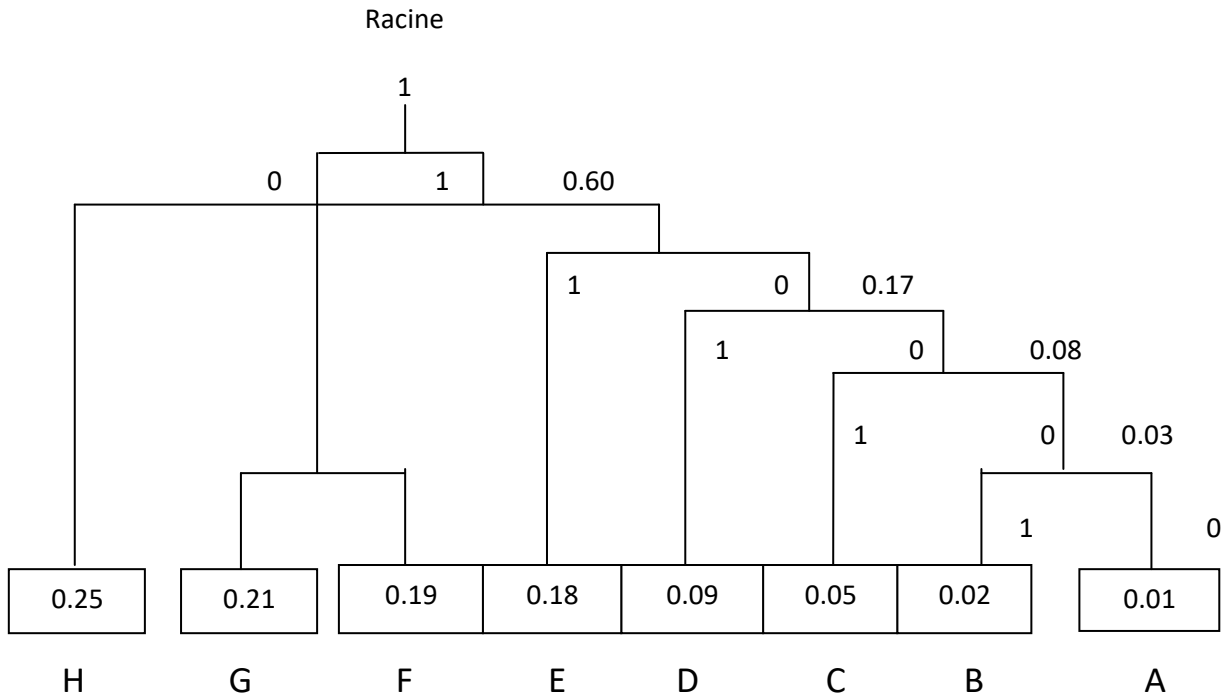


Figure.9.Arbre de Huffman après construction.

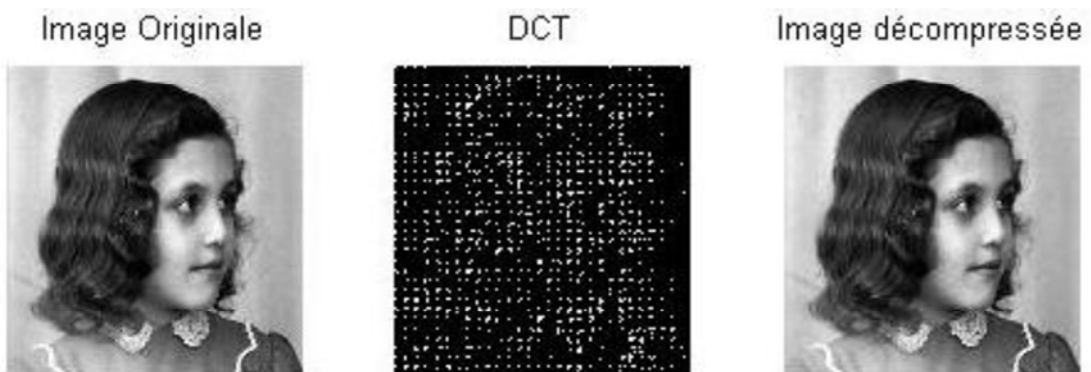


Figure.10.Compression JPEG.

On remarque que la taille de l'image a été compressé avec un taux de compression de 1.25 ce qui est acceptable on aurait pu avoir plus si on aurait pris une image plus corrélée que celle-ci. On remarque aussi que la DCT dans chaque sous blocs elle fait une concentration des coefficients basses fréquences (en blanc).

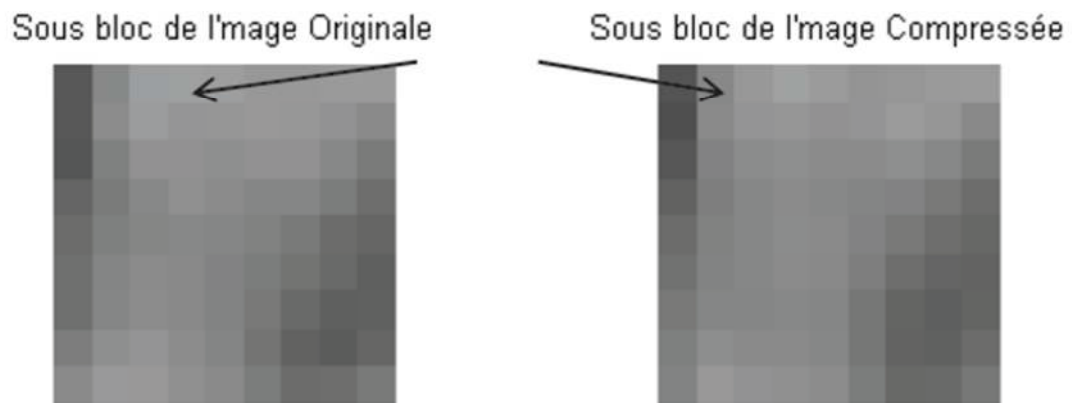
L'image n'a pas perdu de sa fidélité apparente, cela étant seulement visuellement



# CHAPITRE II : La compression JPEG des images fixes

---

Apparent, parce que l'erreur quadratique moyenne n'est pas nulle et égale à  $EQM = 25.69$  cela veut dire qu'il y'a une erreur d'une différence moyenne de 25.7 environs entre les éléments des deux matrices images mais elle n'est notable seulement à l'échelle d'un sous bloc  $8 \times 8$ , où on peut remarquer cette différence sur la **Figure.10**. [1].



**Figure.11.** Comparaison des sous bloc  $8 \times 8$  de l'image originale et l'image compressée.

## II.7. Conclusion

La compression JPEG pour qu'elle soit efficace doit être effectuée de façon optimale afin de ne pas perdre trop en qualité de l'image et en parallèle réduire le poids de l'image, c'est à dire trouver un compromis rapport taille/qualité qu'est le standard JPEG.

La compression JPEG en mode codage DCT séquentielle est une compression avec pertes non adapté aux besoins de précision, mais serait le format le mieux adapté pour les mémoires (grâce aux JPEG que les appareils photo numérique ont fait leurs apparition) ou pour le web (rapidité de transmission). La partie pratique fera l'objet du prochain chapitre.

# Chapitre 3

### III.1 Introduction

Ce chapitre est réservé à la partie pratique dont laquelle nous avons effectué des simulations utilisant le Matlab R2008a. Les images de test utilisées sont celles de Lena et Barbara de dimensions  $256 \times 256$ , comme illustré dans la **Figure.1**.



**Figure.1.** Images de test de Lena et de Barbara

Nous avons divisé ce chapitre en trois grandes parties qui sont

1. Simulation du cryptage d'images à base de la technique permutation-diffusion, l'analyse des résultats est effectuée à travers les métriques du PSNR et du coefficient de corrélation.
2. Simulation de la compression JPEG à base de la transformée DCT, l'analyse des résultats est effectuée à travers les métriques du taux de compression, le PSNR et l'erreur quadratique moyenne EQM pour différents facteurs de qualité FQ.
3. Simulation de la compression et cryptage conjoints des images, l'analyse des résultats est effectuée à travers les métriques du taux de compression et le PSNR.

### III.2 Simulation du cryptage d'images à base de la technique permutation-diffusion

Dans cette partie, nous avons établi deux programmes, l'un de cryptage et l'autre de décryptage **Figure.2**. en utilisant la fonction chaotique Logistic map et la fonction Logistic map modifiée avec les paramètres suivants (valeur initiale  $x_0 = 0.28$  et le paramètre de contrôle  $r_0 = 3.99$ ,  $x_1 = 0.52$  et  $r_1 = 3.98$ ).

## Chapitre3 : Resultats et discussions

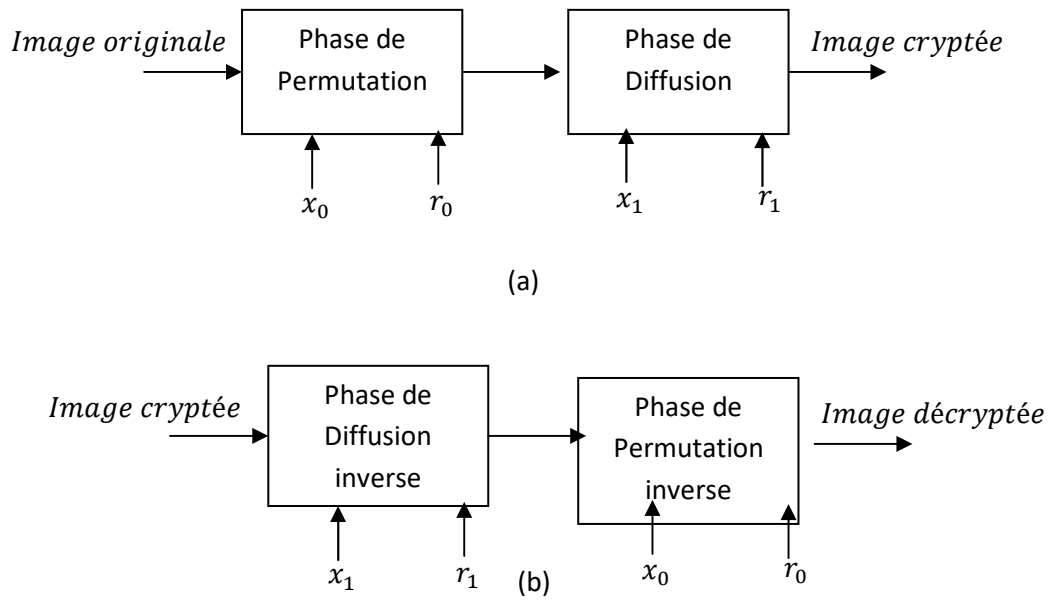


Figure.2.Schéma synoptique de (a) Cryptage et de (b) Décryptage d'images.

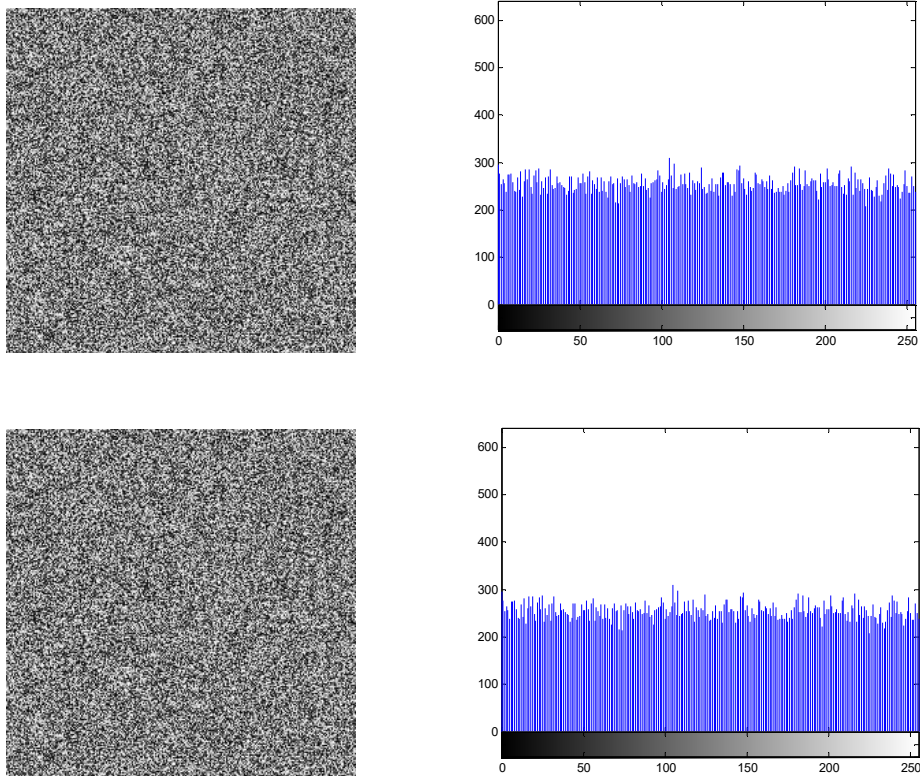
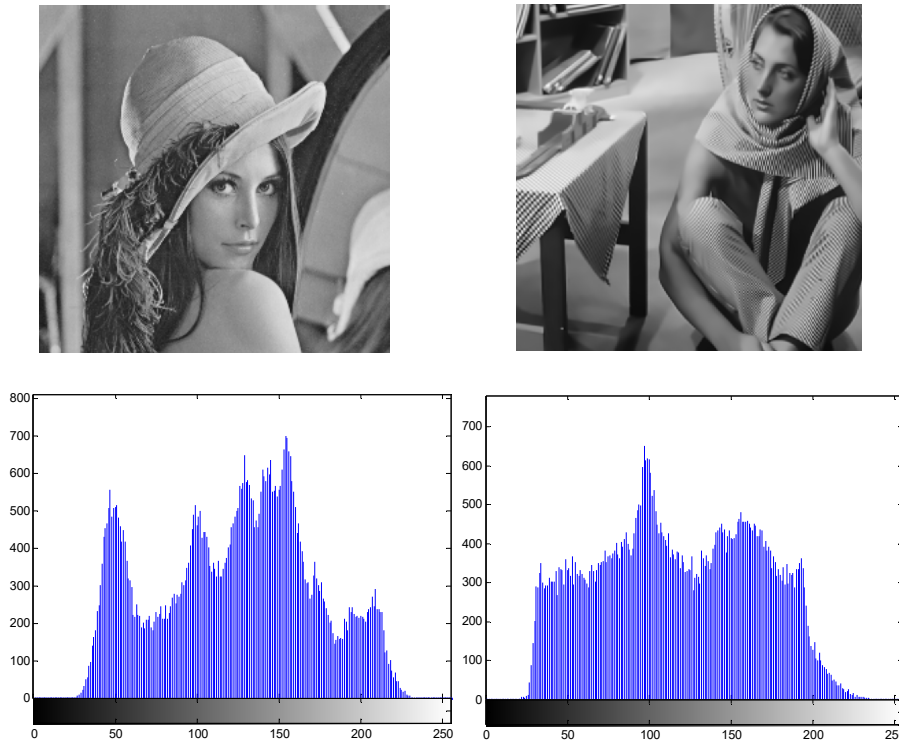


Figure.3.Images cryptées de Lena et de Barbara et leurs histogrammes.



**Figure.4.** Images d crypt es de Lena et de Barbara et leurs histogrammes.

La **Figure.3** illustre les r sultats de cryptage d'images des deux images (Lena et Barbara) obtenus, nous remarquons que les images crypt es sont totalement brouill es et leurs histogrammes ressemblent   un bruit blanc uniforme.

La **Figure.4** illustre les r sultats de l'op ration inverse qui est le d cryptage des deux images (Lena et Barbara) et leurs histogrammes, nous remarquons que les deux images sont reconstruites fid lement. Quoique l'observation visuelle nous semble efficace, mais elle ne suffit pas, nous pouvons confirmer objectivement l'efficacit  des r sultats obtenus   travers l'utilisation de deux m triques   savoir le PSNR et le coefficient de corr lation.

Les mesures de performances du PSNR et du coefficient de corr lation sont r capitul es dans le **Tableau.1.**, que se soit pour la phase de cryptage ou pour la phase de d cryptage. Nous remarquons que le PSNR lors de la phase de cryptage fr le la valeur 9 pour les deux images et le coefficient de corr lation est proche de la valeur 0, ce qui confirme le degr  de d gradation de l'image crypt e et l'impossibilit  d' tre

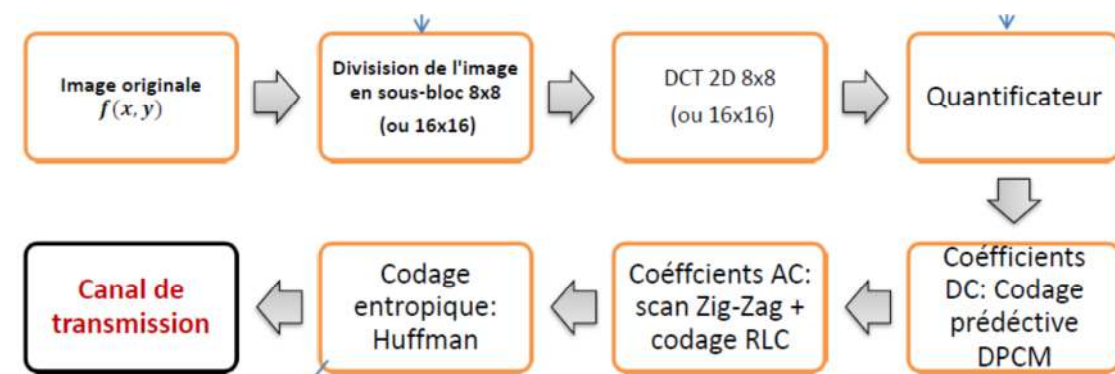
## Chapitre3 : Resultats et discussions

identifiée. Quant à la phase de décryptage, nous remarquons que le PSNR tend vers l'infini et le coefficient de corrélation vers l'unité, ce qui prouve que l'image décryptée est reconstruite fidèlement au niveau du récepteur. A la lumière de tout ce qui précède, nous confirmons que le schéma de cryptage proposé est robuste et les résultats des tests de simulation effectués confirment son efficacité.

**Tableau.1.** Mesures du PSNR et du coefficient de corrélation pour les deux images test

	<b>Image de Lena</b> Cryptage/décryptage	<b>Image de Barbara</b> Cryptage/décryptage
<b>PSNR</b>	9.2632/ infini	9.1266 / infini
<b>Coefficient de corrélation</b>	-0.0072/1	-0.0034/1

### III.3 Simulation de la compression JPEG à base de la transformée DCT



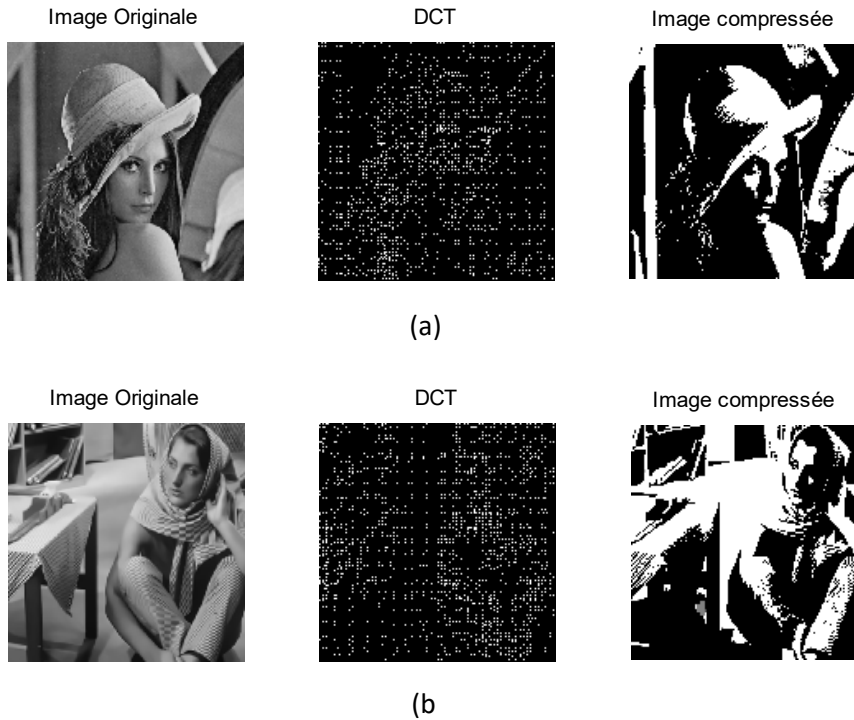
**Figure.5.** Schéma synoptique de la compression JPEG sans pertes.

Dans cette partie, nous avons procédé à la simulation de la compression JPEG sans pertes en utilisant toujours les deux images de test de Lena et de Barbara. La **Figure.5** a bien illustré les différentes étapes de ce processus de compression qui sont respectivement :

- Découpage en sous blocs.
- Décalage de niveau (Level Shifting).
- Application de la DCT.
- Quantification.
- Codage des coefficients DC et AC.
- Codage Huffman.

La **Figure.6.** illustre les résultats obtenus de la compression JPEG des deux images de test.

## Chapitre3 : Resultats et discussions



**Figure.6.**Compression JPEG (a) Lena, sa DCT et son image compressée (b) Barbara, sa DCT et son image compressée.

**Tableau.2.**Mesures du taux de compression, du PSNR et de l'erreur quadratique moyenne avec différents facteurs de qualité pour les deux images de test

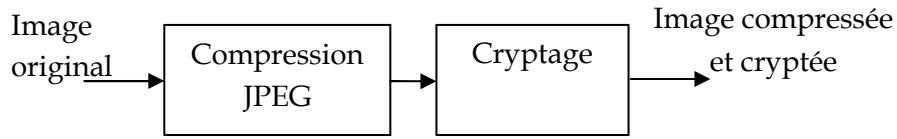
	Image de Lena		Image de Barbara	
	FQ=50	FQ=100	FQ=50	FQ=100
<b>Taux de compression</b>	6.52	7.32	6.32	7.15
<b>PSNR</b>	24.30	20.19	25.12	18.23
<b>EQM</b>	220.13	430.35	216.32	422.39

En se basant sur les résultats obtenus dans le Tableau.2, nous remarquons que plus le facteur de qualité est grand, plus le taux de compression est meilleur, encore plus, nous remarquons aussi que le EQM augmente, ce qui influence considérablement la qualité de l'image, chose traduite par la dégradation remarquable du PSNR.

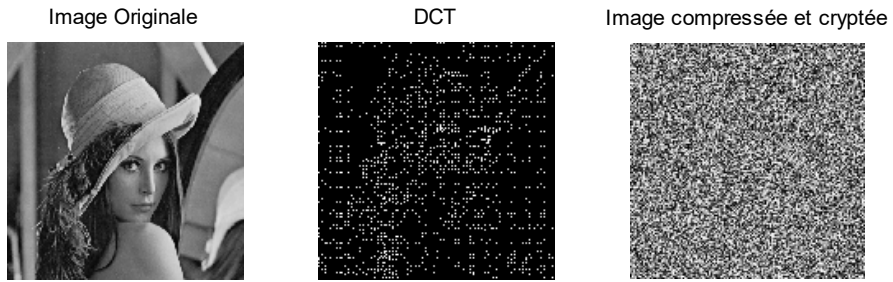
### III.4 Simulation de la compression et cryptage conjoints des images

Dans cette partie, nous avons procédé conjointement à la simulation de la compression JPEG sans pertes et le cryptage en utilisant toujours les deux images de test de Lena et de Barbara comme illustré dans la **Figure.7**

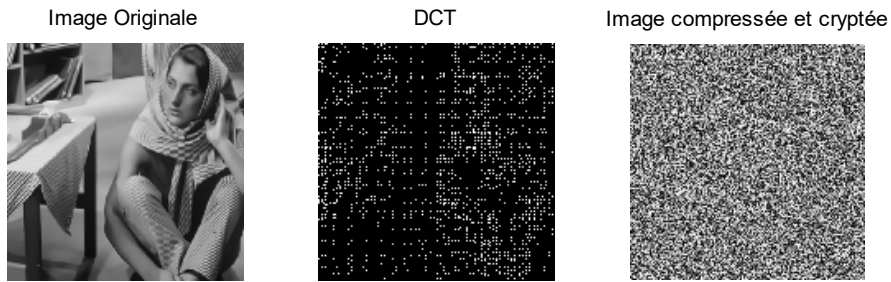
## Chapitre3 : Resultats et discussions



**Figure.7.** Synoptique de compression et cryptage conjoints.



(a)



(b)

**Figure.8.** Compression et cryptage conjoints (a) Lena, sa DCT et son image compressée et cryptée (b) Barbara, sa DCT et son image compressée et cryptée.

**Tableau.3.** Mesures du taux de compression, du PSNR et de l'erreur quadratique moyenne avec différents facteurs de qualité pour les deux images de test

	Image de Lena		Image de Barbara	
	FQ=50	FQ=100	FQ=50	FQ=100
<b>Taux de compression</b>	6.16	7.56	6.32	7.10
<b>PSNR</b>	9.32	8.16	9.12	8.08

Les résultats de simulation sont bien illustrés dans la **Figure.8.** et le **Tableau.3.** récapitule les résultats trouvés.



## Chapitre3 : Resultats et discussions

---

Nous remarquons la dégradation intensive de l'image traduite par un PSNR qui frôle la valeur 9 avec l'image de Lena et la valeur 8 avec l'image de Barbara

### III.4 Conclusion

Dans ce chapitre, nous avons accentué notre travail sur le coté pratique afin de concrétiser l'étude théorique détaillée dans les chapitres un et deux. Pour se faire, nous avons simulé trois programmes sous environnement Matlab 2008a utilisant deux images de test standard, celles de Lena et de Barbara ayant toutes les deux les dimensions de  $256 \times 256$ . En effet, le premier programme élaboré concerne le cryptage d'images à base de l'architecture permutation-diffusion puis un deuxième programme de compression JPEG à base de la transformée DCT. Une fois, réussissons ces deux programmes, nous avons proposé un troisième programme qui ce n'est qu'une compression et cryptage conjoints, les résultats obtenus ont démontré l'efficacité de la méthode proposée en utilisant plusieurs métriques dans les différents tests de performances exécutés.

# Conclusion générale

# *Conclusion générale*

---

Au cours de ce projet de fin d'étude, nous avons étudié la problématique liée à la protection des images par cryptage et entre temps la compression de ces images avant leurs transmission dans des réseaux numériques en utilisant plusieurs catégories de chiffrement (asymétrique, symétrique) (cryptage et décryptage).

Au chapitre I, nous avons donné les principes généraux de cryptage d'images ainsi que les différentes attaques existantes pour le test de robustesse. Au chapitre II, nous avons discuté la problématique de réduction de l'information dans une image sans pour autant détériorer sa qualité, cela se traduit par l'étude de la compression JPEG sans pertes. Courant le chapitre trois qui est réservé à la partie pratique, nous avons développé trois programmes sous environnement Matlab dans lesquels, nous avons concrétisé la sécurisation de l'image par cryptage symétrique, le deuxième programme traite la compression JPEG et enfin un troisième qui fait une fusion entre les deux pour donner conjointement un programme de compression et de cryptage.

Pour tester les performances des programmes développés, nous avons utilisé plusieurs métriques comme le PSNR, le coefficient de corrélation, le EQM et le BER. Les résultats obtenus sont satisfaisants et prouvent l'efficacité des programmes établis.

Pour conclure, ce projet nous a appris à implémenter des programmes de cryptage fonctionnel et de compression. Nous avons pu aussi apprécier le principe de cryptage et compression conjoints. Ce projet aura aussi été pour nous l'occasion de s'initier à la recherche scientifique, nous comptons que ce travail pourra être poursuivi par d'autres promotions et pourquoi pas son extension au traitement de la vidéo.

# *Références bibliographiques*

---

- [1] S.Azoug , “ Compression JPEG d’images fixes,”Université Ferhat Abbas,sétif, 2011
- [2]Mémoire compression d’images fixes,”compression JPAC
- [3]M.Amrane, “Crypto compression d’image par cryptage partiel,”Université Mouloud Mammeri de Tizi-Ouzou,2015
- [4] Z.Baarir, “Etude de la norme de compression d’image jpeg,”Université mohamed khider de biskra,2018-2019
- [5]N.Hemdani, “Compression d’images fixes par classification de régions en associant les ondelettes et les fractales,”Université Mouloud Mammeri de Tizi-Ouzou,2008
- [6]M.Sahir, “Compression des images numériques par la technique des ondelettes,”Université Ferhat Abbas,sétif,2011
- [7]N.Brahimi, “Développement et implémentation des algorithmes de compression d’images basés sur des transformées entières ,”Université Ferhat Abbas,sétif,2011
- [8]<https://fr.wikiwagsdisposables.com/544132-discrete-cosine-transform-FBRYKD#DCT-I>
- [9] H. Khouildat, “ Méthode de cryptage d’image basée sur la permutation et la matrice de householder, ”Université kasdi-merbah ouargla,2019.
- [10] T. Bekkouche, “ Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes, “ Université Ferhat Abbas Setif-1.

## ملخص

في موضوع أطروحة نهاية الدراسة ، تعاملنا مع مشكلة ضغط الصور وتشفيرها بشكل مشترك ، مما أدى إلى تطوير ثلاثة برامج في ظل بيئة Matlab 2014. الأول يتعلق بتشفير الصور ، والثاني يتعامل مع ضغط JPEG بدون فقدان ، والثالث اندماج بين الاثنين. تثبت النتائج التي تم الحصول عليها فعالية البرامج التي تم تطويرها باستخدام عدة مقاييس لقياس الأداء.

## Résumé

Dans ce sujet de mémoire de fin d'études, nous avons traité la problématique de compression et cryptage d'images conjointement, cela a été traduit par le développement de trois programmes sous environnement Matlab 2014. Le premier concerne le cryptage d'images, le deuxième traite la compression JPEG sans pertes et le troisième une fusion entre les deux. Les résultats obtenus prouvent l'efficacité des programmes développés en utilisant plusieurs métriques pour mesure de performance.

## Summary

In this end-of-studies dissertation subject, we have dealt with the problem of image compression and encryption jointly, this has resulted in the development of three programs under the Matlab 2014 environment. The first concerns image encryption, the second deals with lossless JPEG compression and the third a fusion between the two. The results obtained prove the effectiveness of the programs developed by using several metrics to measure performance.