



République Algérienne Démocratique et Populaire

*Ministère de l'Enseignement Supérieur et de la
Recherche Scientifique*

Université Larbi Tébessi Tébessa

*Faculté Des Sciences Exactes Et Sciences De
La Nature Et De La Vie*

Département des Mathématiques Et Informatique

MEMOIRE

Présenté en vue de l'obtention du diplôme de Master 2

Filière: Informatique

Spécialité : Réseaux et Sécurité Informatique

THEME

Un Système de crypto compression d'images basé sur le Block Cipher et la compression par Ondelettes

Présenter par :

HAMIDA Bariza

Soutenu le 13/06/2022 devant le jury composé de :

<i>Dr. DAOUADI Kheir Eddine</i>	<i>MAB</i>	<i>Président</i>	<i>Université de Tébessa</i>
<i>Dr. BOUALLEG Yaakoub</i>	<i>MCB</i>	<i>Examineur</i>	<i>Université de Tébessa</i>
<i>Dr. MENASSEL Rafik</i>	<i>MCA</i>	<i>Encadreur</i>	<i>Université de Tébessa</i>
<i>Dr. GATTAL Abdeljalil</i>	<i>MCA</i>	<i>Co-Encadreur</i>	<i>Université de Tébessa</i>

Année universitaire : 2021/2022

REMERCIEMENT

Tout d'abord, je tiens à remercier Dieu,

De m'avoir donné la santé, la volonté et la patience pour mener à terme notre formation de Master et pouvoir réaliser ce projet.

Je tiens à exprimer mes profonds remerciements à mes encadreurs D. MENASSEL Rafik et D. GATTAL Abdeljalil qui m'ont fourni le sujet de ce mémoire et m'ont guidé avec leurs précieux conseils et suggestions, et la confiance qu'ils m'ont témoigné tout au long de ce travail.

Mes vifs remerciements s'adressent aussi aux membres de jury.

J'adresse aussi mes remerciements à tous les enseignants de la filière Informatique.

Enfin, j'adresse mes sincères sentiments de gratitude et de reconnaissance à toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

DÉDICACES

*A l'homme de ma vie, mon exemple éternel, celui qui s'est toujours sacrifié pour me voir réussir, à toi mon père « **Tayeb** ».*

*A la lumière de mes jours, la source de mes efforts, la flamme de mon cœur, ma vie et mon bonheur; maman « **Baya** ».*

*A ma grande mère « **Hadhria** ».*

*A mes très chers frères **Saleh, Azzeddine, Nacer, Abdelhak, Messaoud** et **Fateh**.*

*A mes belles sœurs **Hafssa, Zina** et **Moufida**.*

A mes amies proches

A mes amies et toutes promotions Master 2 informatique spécialité Réseaux et sécurité informatique

2021/2022.

HAMIDA Bariza.

Résumé

Résumé

La compression est une étape importante dans l'optimisation de l'utilisation de grandes quantités de données dans les réseaux informatiques. L'objectif principal de la compression d'image est de réduire la quantité de données requises pour une image visuelle fidèle à l'image d'origine.

Le cryptage des données, en revanche, est généralement décrit comme le résultat d'une connexion secrète de données entre deux interlocuteurs. Dans un système informatique, cette vie privée est entravée sous plusieurs formes, notamment dans la protection du stockage, de l'accès et de la transmission des données.

Dans ce travail, nous allons mener, une étude plus détaillée au sujet du système de crypto-compression basé sur une compression avec perte DWT, et un algorithme de chiffrement moderne AES basé sur la technique du Block Cipher ou cryptage par blocs.

Mots clés : compression d'image, cryptage , DWT, Block Cipher, crypto_compression.

Abstract

Compression is an important step in optimizing the use of large amounts of data in computer networks. The main purpose of image compression is to reduce the amount of data required for a visual image that is faithful to the original image.

Data encryption, on the other hand, is usually described as the result of a secret data connection between two interlocutors. In a computer system, this privacy is impeded in several forms, notably in the protection of storage, access and transmission of data.

In this work, we will carry out a more detailed study about the crypto-compression system based on DWT lossy compression, and a modern AES encryption algorithm based on the Block Cipher technique.

Keywords: image compression, encryption, DWT, Block Cipher, crypto_compression.

ملخص

يعد الضغط خطوة مهمة في تحسين استخدام كميات كبيرة من البيانات في شبكات الكمبيوتر. الغرض الرئيسي من ضغط الصورة هو تقليل كمية البيانات المطلوبة للصورة المرئية التي تتوافق مع الصورة الأصلية.

من ناحية أخرى ، يتم وصف تشفير البيانات عادة على أنه نتيجة اتصال بيانات سري بين محاورين. في نظام الكمبيوتر ، يتم إعاقة هذه الخصوصية بعدة أشكال ، لا سيما في حماية تخزين البيانات والوصول إليها ونقلها.

في هذا العمل ، سنقوم بإجراء دراسة أكثر تفصيلاً حول نظام ضغط التشفير بناءً على ضغط DWT الضائع ، وخوارزمية تشفير AES حديثة تعتمد على تقنية Block Cipher.

الكلمات الرئيسية: ضغط الصور ، التشفير ، DWT ، Block Cipher ، crypto_compression.

Table des matières

Résumé

Abstract

ملخص

Liste des figures

Liste des tableaux

Liste des abréviations

Introduction générale----- 1

Chapitre 1 État de l'art

Introduction ----- 4

I. La cryptographie ----- 5

1. Terminologie et bref historique ----- 5

2. Définition----- 6

3. L'usage de la cryptographie ----- 6

4. Mécanisme de la cryptographie ----- 7

5. Cryptographie classique -----	7
5.1. Classification-----	8
5.1.1.Chiffrement par décalage -----	8
5.1.2. Chiffrement par substitution-----	8
5.1.3. Le code de Vigenère -----	9
6. Cryptographie moderne-----	10
6.1 La cryptographie symétrique -----	10
6.1.1. Principe -----	11
6.1.2. Les types d'algorithmes symétriques-----	11
6.1.3. La faiblesse du système symétrique-----	15
6.2. La cryptographie asymétrique -----	15
6.2.1. Principe -----	15
6.2.2. La faiblesse du système asymétrique -----	16
6.3. Comparaison entre le cryptage symétrique et asymétrique -----	17
II. La compression d'images -----	17
1. Principe -----	17
2. Définition-----	19
3. Compression physique et logique -----	20
4. Compression symétrique et asymétrique -----	20
5. Paramètres de performances des méthodes de compression d'image-----	20

5.1. Rapport et taux de compression -----	20
5.2. Mesure de distorsion-----	21
5.3. Entropie-----	22
5.4. Le temps d'exécution -----	22
6. Les objectifs de la compression -----	23
7.Type de compression -----	23
7.1. La compression sans perte-----	24
7.2. La compression avec perte -----	25
7.2.1 La compression JPEG 2000-----	26
8. Compression par ondelettes -----	27
8.1. Les ondelettes-----	27
8.1.1. Définition -----	28
8.2. Transformée en ondelette continue(CWT) -----	28
8.3. Transformée en ondelette discrète (DWT) -----	29
8.4. Le choix des ondelettes -----	31
8.5. Avantages des ondelettes -----	31
8.6. Critères de qualité des ondelettes utilisées en traitement d'images -----	32
8.7. Quelques ondelettes -----	33
8.7.1 Ondelettes orthogonales -----	33
8.7.1.1 Ondelette de Haar -----	33

8.7.1.2 Les ondelettes à support compact de Daubechies -----	34
8.7.2. Ondelettes biorthogonales -----	35
Conclusion -----	36

Chapitre 2 Crypto compression d'image

Introduction -----	37
1. Théorie des ondelettes -----	37
1.1.Limites de la Transformée de Fourier -----	38
2. Multirésolution -----	40
3. Analyse d'ondelettes -----	41
3.1. Transformation en ondelettes discrètes (DWT)-----	42
4. Ondelette de Haar-----	44
4.1. Définition-----	44
4.2. Fonctions Haar et système Haar -----	46
5. La décomposition quadtree -----	47
6. Cryptage a clé privé -----	48
6.1. L'AES (Advanced Encryption Standard) -----	48
6.1.1. L'AES : Algorithme-----	49
6.1.2. Choix de l'AES -----	50
6.1.3. Principe de fonctionnement -----	50
6.1.4. L'algorithme de cryptage -----	51
6.1.5.l'algorithme de décryptage -----	52

7.l'algorithme proposé pour la compression-----	53
7.1. Le codage de Huffman -----	54
7.2. Décodage Huffman -----	54
8.Les travaux similaires-----	55
9. Système de Crypto_Compression proposé-----	57
Conclusion -----	58

Chapitre 2 Résultats et discussion

Introduction-----	59
1.Environment de travail-----	60
1.1.Matériels utilisés -----	60
1.2.Langage de programmation -----	60
2.Aperçu du logiciel réalisé -----	62
2.1Hiérarchie -----	62
3.Principe de fonctionnement de l'application -----	64
3.1. Description des modules du système -----	65
4. Bibliothèque d'images -----	66
5. Tests expérimentaux -----	67
5.1. Résultats -----	67
5.1.1. Tests et résultats -----	68
5.1.1.1. Premier cas -----	68
5.1.2.1. Processus de traitement et Histogramme-----	69

5.1.1.2. Deuxième cas -----	71
6. Interprétation des résultats -----	73
6.1. Discussion-----	74
6.1.1. Premier cas -----	74
6.1.2. Deuxième cas -----	74
Conclusion -----	74
Conclusion générale -----	76
Bibliographie.	

Liste des figures

Figure1: Principe de code de César	8
Figure2: Exemple sur le code Vigenère	9
Figure3: Principe du chiffrement symétrique	10
Figure4: Système de cryptage / décryptage	11
Figure5: Chiffrement par Bloc	13
Figure6: Le chiffrement par Bloc mode ECB	13
Figure7: Le Chiffrement par Bloc mode CBC	14
Figure8: Le chiffrement par ECB et CBC	15
Figure9: chiffrement- déchiffrement asymétrique	16
Figure10: Principe de Compression d'images	18
Figure11: Schéma d'un codeur d'image	18
Figure12: les types de compression	24
Figure13: Compression sans perte	25
Figure14: Principe de compression avec Perte	26
Figure15: Ondelette de Daubechies	35

Figure16: -a- Image compressé avec JPEG (DCT) (Transformé de Fourier)- b- Image compressé avec JPEG2000 (DWT) (Transformé par ondelettes)	39
Figure17: Principe de la DWT	42
Figure18: schéma de décomposition	44
Figure19: Ondelette de Haar	46
Figure20: Décomposition Quadtree	48
Figure21: Le bloc présenté par l’algorithme l’AES	49
Figure22: Principe de fonctionnement de AES	51
Figure23: L’algorithme proposé pour le Cryptage AES	52
Figure24: L’algorithme proposé pour le Décryptage AES	53
Figure25: Système de Crypto-Compression proposé	58
Figure26: Organigramme du système	63
Figure27: Interface du système	64
Figure28: Principe de fonctionnement de l’application	64
Figure29: Schéma synoptique de notre système	67
Figure30: Processus de traitement et l’histogramme Lena.jpg	69
Figure31: Processus de traitement et l’histogramme Airplane.bmp	70
Figure32: Processus de traitement et l’histogramme Baboon.bmp	70
Figure33: Schéma synoptique du système deuxième cas	71

Liste des tableaux

Tableau1 : Comparaison entre le cryptage symétrique et asymétrique	17
Tableau2 : Bibliothèques des images utilisées	66
Tableau3 : Résultat d'application de notre système sur différentes images cas1 ____	69
Tableau4 : Résultat d'application de notre système sur différentes images cas2 ____	72

Liste des abréviations

- AES: Advanced Encryption Standard
- BMP: BitMaP
- CBC: Cipher Block Chaining
- CFB: Cipher Feedback
- CR: En anglais « Compression Ratio » : Rapport de compression
- CWT: Continuous Wavelet Transform
- DES: Data Encryption Standard
- DB: Le décibel ou (dB)
- DCT: Discret Cosine Transform
- DWT: Discret Wavelet Transform
- ECB: Electronic Code Book
- FFT: Fast Fourier Transform
- GSM: Global System for Mobile Communications
- GUI: Graphical User Interface
- IHM: Interface Homme Machine
- IRM: L'imagerie par résonance magnétique
- IDWT: Invers Discret Wavelet Transform
- ISO: International Organisation for Standardisation
- JPG: Joint Photographic Group
- JPEG: Joint Photographic Experts Group
- LZW: Lempel-Ziv-Welch
- MSE: En anglais « Mean Square Error » L'Erreur Quadratique Moyenne

- OFB: Output Feedback
- PSNR: En anglais « Peak Signal to Noise Ratio » Rapport signal à bruit
- RC4: Rivest Cipher 4
- RLC: Le Run-Length Encoding, appelé en français le codage par plages
- RSA: Ronald Rivest, Adi Shamir et Leonard Adleman
- RGB: Rouge, vert, bleu, abrégé en RVB ou en RGB
- RNA: Réseaux de Neurones Artificiels
- SPIHT: Set Partisioning in Hierarchic Tree
- WMSN: Wireless Multimedia Sensor Networks

INTRODUCTION GÉNÉRALE

Introduction générale

Ces dernières années, l'utilisation des technologies de l'information et des télécommunications dans la vie de tous les jours a considérablement augmenté. La compression et le chiffrement des données sont deux technologies qui gagnent rapidement en popularité dans un large éventail d'applications.

Les chercheurs ont créé une variété de méthodes de compression de données basées sur la théorie de l'information, qui couvrent un large éventail de mathématiques et d'informatique disciplines.

Le but de la compression d'image est de minimiser la taille d'une image afin qu'elle puisse être stockée et transférée plus facilement. En conséquence, nous distinguons deux familles principales de méthodes de compression : celles qui causent la perte d'information et entraînent une image reconstruite qui n'est pas fidèle à l'original, mais est de très petite taille, et ceux qui ne provoquent pas de perte d'information. D'autres approches n'entraînent pas de perte de données, mais elles ont des taux de compression plus faibles.

L'utilisation de méthodes de chiffrement par blocs pour encoder les images présente deux inconvénients. Tout d'abord, si l'image contient des zones homogènes, même

après le chiffrement, tous les blocs identiques seront identiques. L'image cryptée dans ce scénario a des sections texturées et l'entropie de l'image n'est pas à son maximum. Le deuxième problème est que les chiffrements de blocs sont sensibles au bruit. Une erreur sur un bit crypté, en fait, causera des défauts importants dans tout le bloc actuel.

L'utilisation excessive des réseaux informatiques pour la transmission de données doit, bien sûr, atteindre deux objectifs : une réduction du volume de données pour désengorger les réseaux de communication publique autant que possible, et la confidentialité pour assurer un niveau de sécurité optimal. Dans cette optique, et afin d'optimiser et de sécuriser la transmission et le stockage des images fixes, nous proposons que notre approche hybride basée sur DWT et Huffman utilise le cryptage AES. Pour mener à bien notre travail, nous avons structuré notre mémoire en trois chapitres :

Le premier chapitre c'est l'état de l'art se compose en deux parties ; la cryptographie et la compression :

- La première partie nous amène dans le monde de la cryptographie ; en commençant par une définition détaillée suivie par une présentation des méthodes de cryptage parmi les plus utilisées, ensuite nous expliquons les deux types de la cryptographie (classique et moderne), et enfin nous mettons le point sur le chiffrement par bloc.
- La deuxième partie introduit la compression : des définitions et des notions essentielles sur les différents types de compression présentées. Nous décrivons par la suite, les algorithmes utilisés ainsi que les paramètres permettant d'évaluer leurs performances et enfin en mettant le point sur la compression par ondelettes.

Le deuxième chapitre qui introduit la notion de crypto-compression, nous présentons une explication plus détaillée des deux techniques utilisées dans notre système, en commençant par la compression par ondelettes. Ensuite, nous l'approche de cryptage à base de Block Cipher en utilisant l'algorithme AES.

Le Troisième chapitre comprend la partie la plus importante de ce travail sera consacré l'approche de crypto-compression élaborée dans le cadre de ce travail ; en commençant par une présentation de l'environnement de travail et une aperçue générale de notre système, nous citons par la suite les tests expérimentaux sur des images réelles et les résultats obtenues.

CHAPITRE 01

ÉTAT DE L'ART

Chapitre 1

État de l'art

Introduction

Les systèmes de communication numérique sont largement utilisés pour échanger des informations (texte, audio, images, vidéo, etc.). Cet échange d'informations est très sûr dans de nombreuses applications destinées à la société civile ou aux organisations militaires, telles qu'Internet, les téléphones portables, les banques, les abonnements aux chaînes de télévision, le paiement, le commerce électronique et la confidentialité, et pour empêcher les changements inchangés. demande sur les cartes. ou l'utilisation des données. Une façon connue d'y parvenir est d'intégrer, de rendre les informations illisibles, fragmentaires et incompréhensibles.

Il existe des programmes qui utilisent des informations multimédias, telles que des images dans notre vie quotidienne. Par conséquent, l'édition d'images (enregistrement et publication, etc.) devient une corvée. De plus, la protection de ces informations a rendu plus intéressant pour les chercheurs de garder ces informations confidentielles. La croissance rapide de ces données nécessite des temps statistiques importants, ce qui a conduit les chercheurs à développer des plaintes et des méthodes d'analyse dédiées à une application précise qui sont simples, rapides et efficaces.

I. La cryptographie

1. Terminologie et bref historique

Dans la Grèce antique, le terme cryptographie a été inventé. Le nom "cryptographie" est composé de deux parties : "cryptos," qui se réfère au "secret," et "logos," qui se réfère au type de texte. La cryptographie est aussi vieille que l'écriture elle-même, et elle a été utilisée pour préserver les interactions militaires et diplomatiques pendant des milliers d'années. Par exemple, Jules César, le célèbre empereur romain, a utilisé des méthodes de cryptage pour sécuriser les messages transmis à son armée. Nous séparons deux notions dans le monde de la cryptographie : la cryptographie et la cryptanalyse. Quand un cryptanalyste tente de rouvrir un vieux problème en fermant son système, il va essayer de trouver des moyens d'éviter d'avoir à en parler. cryptanalyse est l'étude des processus frauduleux utilisant des fragments appelés clés, tandis que la cryptographie classique est l'étude des processus de transfert de données sécurisées.

- **Chiffrement:** Il utilise une clé pour convertir un message texte explicite (appelé texte brut) en un message non reconnu (appelé texte chiffré ou mot de passe).
- **Crypto système:** C'est un système avec un algorithme de cryptage et un algorithme de décryptage. Cela vous permet de joindre un message spécifique dans un message non joint, puis le décryptage vous permettra de restaurer le message d'origine.
- **Décryptage :** Trouvez le message texte qui correspond au message crypté avec la clé de décryptage.

- **Cryptanalyse** : Les scientifiques connaissent le mot de passe qui le sépare (sans clé). [1]

2. Définition

La cryptographie est une technique importante dans les systèmes de clés électroniques. Il est utilisé pour stocker des informations confidentielles, enregistrer des documents, protéger l'accès, etc. Les utilisateurs n'ont pas besoin de savoir comment fonctionne sa technique, mais ils doivent pouvoir choisir leur propre sécurité.[2]

3. L'usage de la cryptographie

La cryptographie est utilisée non seulement pour protéger la confidentialité des données, mais aussi pour démontrer leur fiabilité et leur sincérité.

- **Confidentialité** : C'est-à-dire connaître d'autres personnes en plus de celles qui font du commerce.
- **Intégrité** : Assurer l'exactitude des données fait référence à la décision que les données n'ont pas été modifiées au cours de l'entretien.
- **Authentification** : C'est-à-dire pour vérifier la connaissance de l'utilisateur, c'est-à-dire pour vérifier que chaque auteur est un véritable partenaire (par exemple, via un mot de passe à joindre) qui estime qu'une autorité d'accès peut se connecter pour fournir des ressources aux personnes autorisées.
- **Non-répudiation** : La connaissance suppose que l'annonceur ne peut pas refuser l'échange.

4. Mécanisme de la cryptographie

Les algorithmes de chiffrement sont des techniques mathématiques utilisées dans les opérations de déchiffrement et de tricherie. L'algorithme est lié à une clé (un mot, un nombre ou une phrase) qui correspond aux données. Différentes clés produisent différents résultats d'intégration. L'inviolabilité de la méthode de cryptage et l'anonymat de la clé sont les deux critères les plus importants pour assurer la sécurité des données cryptées.[1]

Qu'entend-on par clé ?

Une clé est une propriété qui est utilisée pour chiffrer les données à l'aide d'un algorithme cryptographique. C'est un nombre délicat avec une taille exprimée en bits. Comme vous pouvez vous y attendre, la valeur est assez grande, autour de 1024 bits. Regardez le bit d'octet. Plus le nombre de clés est élevé, plus le résultat est sûr. La combinaison d'algorithmes complexes et de touches aiguës, d'autre part, assure un résultat sûr.

Les clés doivent être stockées en toute sécurité de manière à ce que seuls leurs propriétaires puissent y accéder et les utiliser.

5. Cryptographie classique

La cryptographie ancienne a été développée avant l'invention des ordinateurs et a fourni des idées et des raisons pour le développement de certains algorithmes symétriques qui sont utilisés aujourd'hui.

Les systèmes de cryptage standard sont combinés avec un cryptage mono-alphabet et poly-alphabet. Chaque message est remplacé par une lettre ou un symbole selon l'algorithme.[3] [4]

5.1. Classification

5.1.1. Chiffrement par décalage

L'un des systèmes les plus anciens et les plus simples est le code de cryptage, aussi connu sous le nom de code César. Ce code est l'un des plus anciens. Le but est de transformer le message en un ou plusieurs objets.[3] [4]

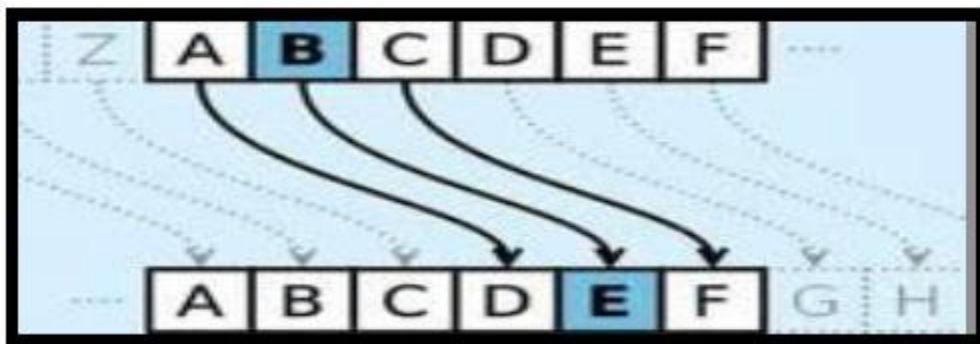


Figure 1 : Principe de code de César. [4]

5.1.2. Chiffrement par substitution

Il s'agit d'une manière courante de gérer les mots de passe. Bien sûr, chaque lettre de l'alphabet est liée à une autre, ce qui signifie que nous remplaçons toutes les lettres.

Des substitutions sont possibles pour la lettre initiale de l'alphabet, a. Il n'y en a que 25 pour la lettre b, et ainsi de suite.[3] [4]

5.1.3. Le code de Vigenère

L'image de César est significativement améliorée par le cryptage de Vigenère. Blaise de Vigenère (1523-1596), un ambassadeur français du XVIe siècle, l'a rédigé.[3] [5]

- Substitution poly-alphabétique.
- Basé sur la table de Vigenère.
- La colonne correspondante à la lettre en clair.
- La ligne correspondante à une lettre de la clé.
- La lettre chiffrée est formée par le croisement de lignes et de colonnes.
- La clé est répétée boucle autant que nécessaire.

La Figure 2 explique le principe du fonctionnement du code Vigenère.

Message clair	:	B	O	N	J	O	U	R
Clé	:	C	L	E	F	C	L	E
Message Chiffré	:	D	Z	R	O	Q	F	V

Figure 2 : Exemple sur le code Vigenère.[3]

6. Cryptographie moderne

L'étude des méthodes qui garantissent l'intégrité, l'authenticité et le secret des services dans les systèmes d'information et de communication est le but de la cryptologie moderne. Il existe deux sous-disciplines de la cryptologie :

- La cryptographie, qui permet de fournir ces services.
- Cryptanalyse, qui examine les mécanismes proposés pour détecter les défauts.

Nous pouvons utiliser des algorithmes basés sur des clés pour assurer les objectifs de la cryptographie actuelle. Plusieurs types de cryptographie actuels définissent ces algorithmes ; nous identifions deux approches :

- La cryptographie symétrique.
- La cryptographie asymétrique.

6.1. La cryptographie symétrique

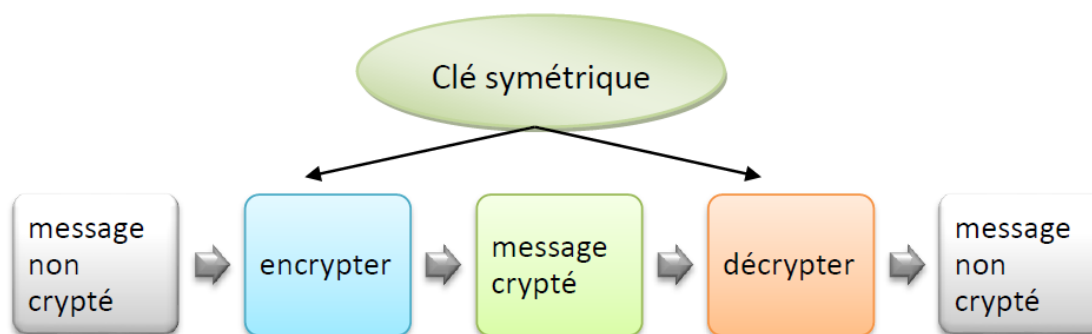


Figure 3: Principe du chiffrement symétrique. [6].

6.1.1. Principe

L'expéditeur et le destinataire partagent la même clé. En d'autres termes, en utilisant la même clé, nous pouvons chiffrer et déchiffrer les messages.

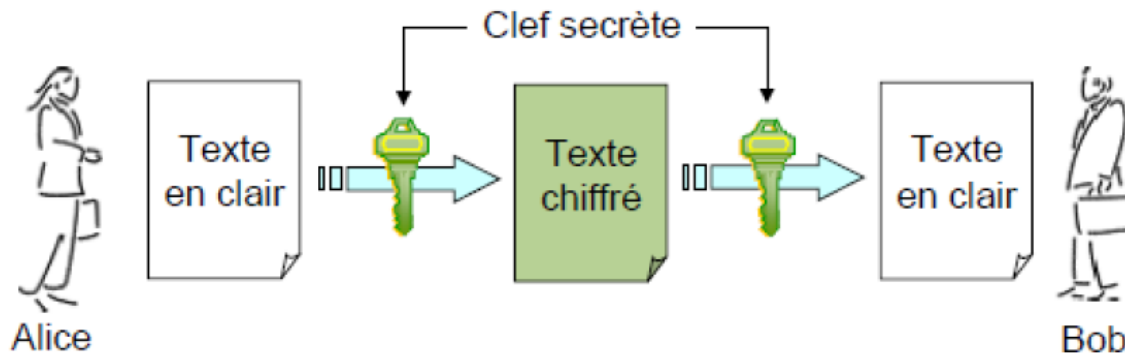


Figure 4: Système de cryptage / déchiffrement. [7].

- L'échange de la clé secrète entre les deux interlocuteurs doit s'effectuer à travers un canal sécurisé ou sécuritaire.
- Le chiffrement symétrique est le processus qui consiste à utiliser la clé privée pour effectuer une opération (algorithme) sur les données à chiffrer afin de les rendre illisibles.
- Nous envoyons le message à quelqu'un, avec la clé privée, afin qu'ils puissent le déchiffrer.
- Le cryptage symétrique fonctionne selon deux procédés catégories : par Bloc/ par Flux.

6.1.2. Les types d'algorithmes symétriques

Il existe deux types d'algorithmes symétriques :

- les techniques de chiffrement par flux, qui fonctionnent un peu à la fois sur le message brut.
- Méthodes de chiffrement par blocs, qui fonctionnent sur le message clair en blocs de bits.

a. Algorithmes de chiffrement par flux (Stream Cipher)

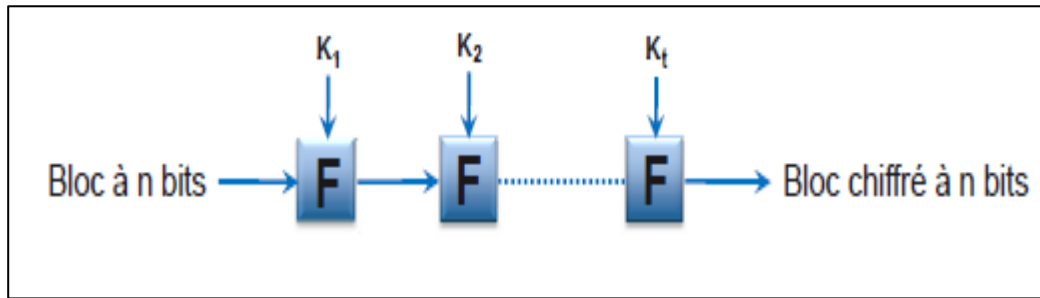
Cela fonctionne un peu à la fois sur le message clair. L'idée est de créer un flux pseudo-aléatoire puis d'utiliser la fonction XOR pour le fusionner avec l'information bit-to-bit.

Quelques algorithmes de cryptographie à flux symétrique :

- A5 : Utilisé pour crypter la communication radio entre le téléphone et la tour de téléphonie cellulaire la plus proche dans les téléphones GSM.
- RC4, le plus utilisé, conçu en 1987 pour RSA Laboratories par Ronald Rivest, l'un des fondateurs de RSA, et utilisé en particulier par le protocole WEP, ainsi qu'un algorithme Eli Biham – E0 plus récent utilisé par le protocole Bluetooth.[3]

b. Algorithmes de chiffrement par bloc (Block Cipher)

Ils fonctionnent sur la base d'un seul message clair par groupe de bits. La taille de bloc la plus courante est de 64 bits, ce qui est assez grand pour empêcher le balayage tout en étant assez petit pour être pratique.



Figur

e 5: Chiffrement par Bloc. [8].

Le chiffrement par bloc utilise quatre modes opératoires :

- Electronic Code Book(ECB)
- Cipher Block Chaining (CBC).
- Output Feedback (OFB).
- Cipher Feedback(CFB).

Electronic Code Book(ECB) : Dictionnaire de codes un message réel en général composé de nombreux blocs. La façon plus immédiate pour chiffrer un tel message est de chiffrer successivement chaque bloc, avec la même clé. Comme montrer dans la Figure 6.

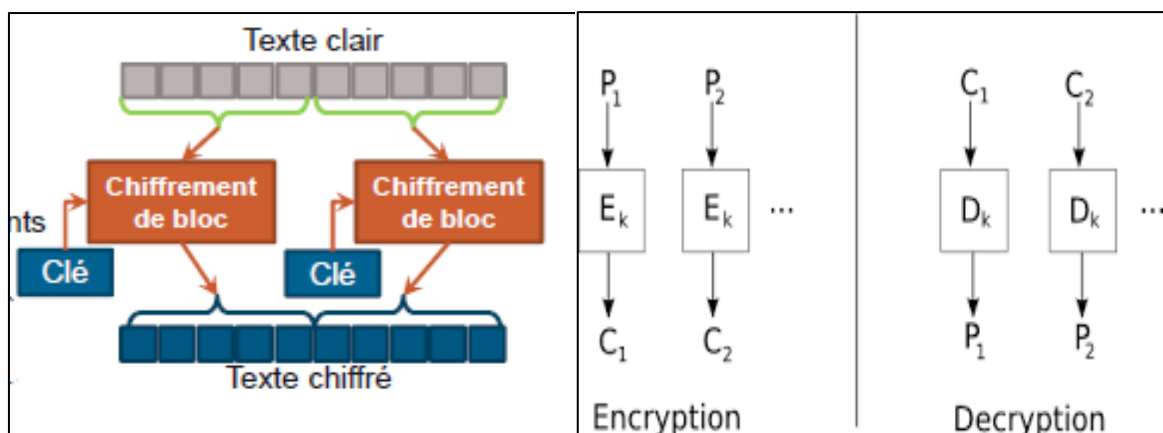


Figure 6 : Le chiffrement par Bloc mode ECB.[3]

Cipher Block Chaining (CBC) : L'enchaînement des blocs consiste, avant le chiffrement d'un bloc, à le masquer par le résultat du chiffrement du bloc précédent au moyen de l'opération XOR. Le premier bloc clair est lui aussi masqué, par une valeur habituellement notée IV (Initial Value) et de préférence variable (la date et l'heure peuvent faire une bonne (IV) pour que les chiffrements successifs du même message soient différents. La valeur initiale IV n'a pas besoin d'être secrète, et elle est en général transmise en clair avant le message chiffré. Noter que si le destinataire reçoit un bloc chiffré avec des bits erronés, cela affecte le déchiffrement de ce bloc et du suivant mais pas des autres (Voir la Figure 7).[3]

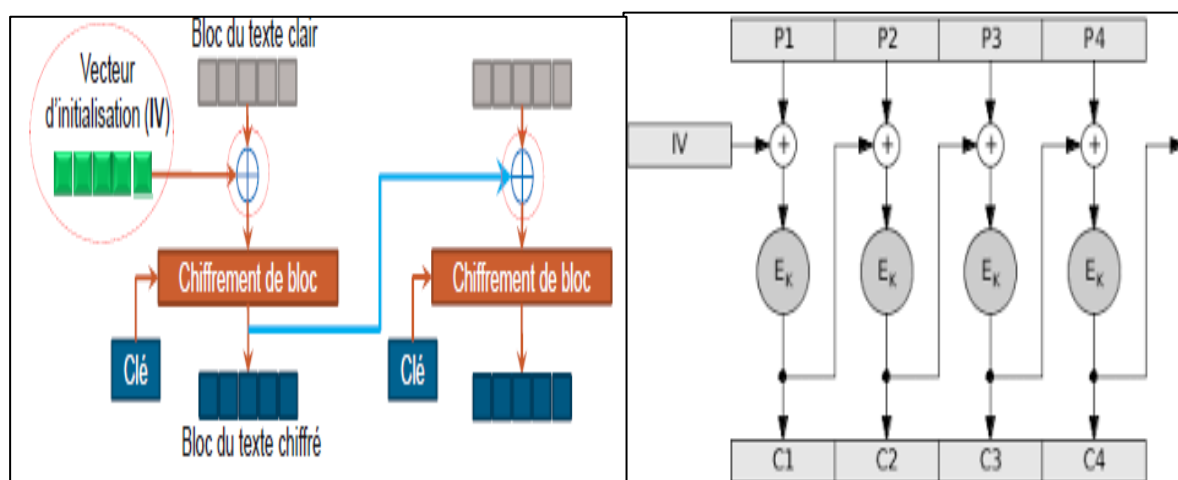


Figure 7 : Le Chiffrement par Bloc mode CBC.[3]



Figure 8: Le chiffrement par ECB et CBC.[3]

6.1.3. La faiblesse du système symétrique

Un système symétrique peut être très robuste, seule la clé doit être transmise de manière sécurisée. Le seul moyen sûr de transmettre la clé en toute sécurité est de se connecter au préalable à un canal sécurisé ou d'échanger physiquement une clé.

6.2. La cryptographie asymétrique

6.2.1 Principe

Pour mieux comprendre le principe de la cryptographie asymétrique (voire la Figure 9).

- Pas besoin d'échanger la clé secrète entre les deux interlocuteurs, seule la clé publique est partagée sur un canal non sécurisé.
- Une paire de clés : une clé publique que tout le monde connaît et une clé privée que seul le propriétaire connaît. Si un utilisateur souhaite envoyer un message à un

autre utilisateur, tout ce qu'il a à faire est de crypter le message avec la clé publique du destinataire.

- Chiffrement requiert beaucoup d'opérations et n'est pas recommandé pour de grande quantité d'informations.
- Algorithme de chiffrement RSA.

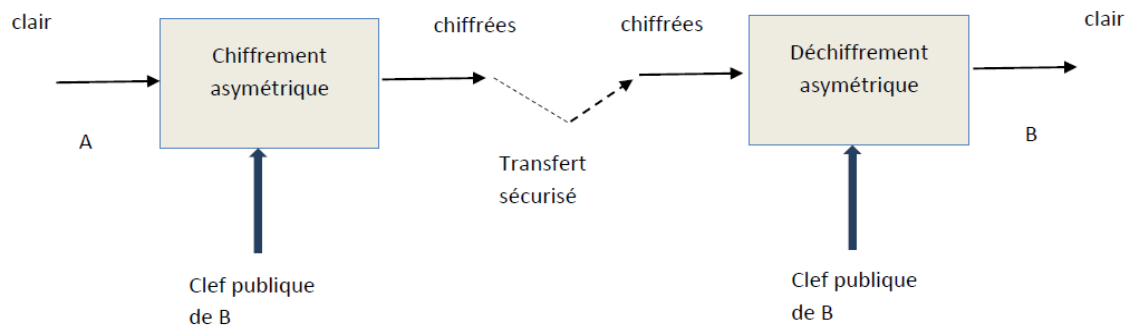


Figure 9 : chiffrement- déchiffrement asymétrique. [9].

6.2.2. La faiblesse du système asymétrique

Le plus grand danger d'utiliser des clés asymétriques est une attaque d'intermédiaire, qui est la possibilité qu'un adversaire intercepte les clés publiques transférées et les remplace par les siennes. Il a ensuite pu interpréter et signer tous les messages qui avaient été transmis.

6.3. Comparaison entre le cryptage symétrique et asymétrique

Cryptage symétrique	Cryptage asymétrique
<ul style="list-style-type: none"> • Chiffrement à clé privé (une seule clé est utilisée pour le cryptage et le déchiffrement). • Très facile. • Très rapide. • Les clés de chiffrement symétrique doivent être conservées dans un endroit sûr. 	<ul style="list-style-type: none"> • Cryptage avec clés publiques (utilisation de clés publiques pour le cryptage et clé privée pour le déchiffrement). • Comparativement au chiffrement symétrique, c'est plus difficile. • Plus lent. • Parce que l'extraction de la clé privée d'une clé publique peut prendre beaucoup de temps, les clés publiques qu'ils emploient sont sécurisées pour diffuser n'importe où.

Tableau 1: Comparaison entre le cryptage symétrique et asymétrique.

II. La compression d'images

1.Principe

La compression des données, en général, est toute méthode ou technique utilisée pour raccourcir un message long, c'est-à-dire pour réduire le volume de données sans perdre d'informations essentielles. Le but de la compression est de présenter les informations sous une forme plus compacte que l'original, ou le résultat de la compression prend

moins de place que les données d'origine. Les données peuvent être compressées avec ou sans perte.[10]. La Figure 10 présente le principe de la compression des images :

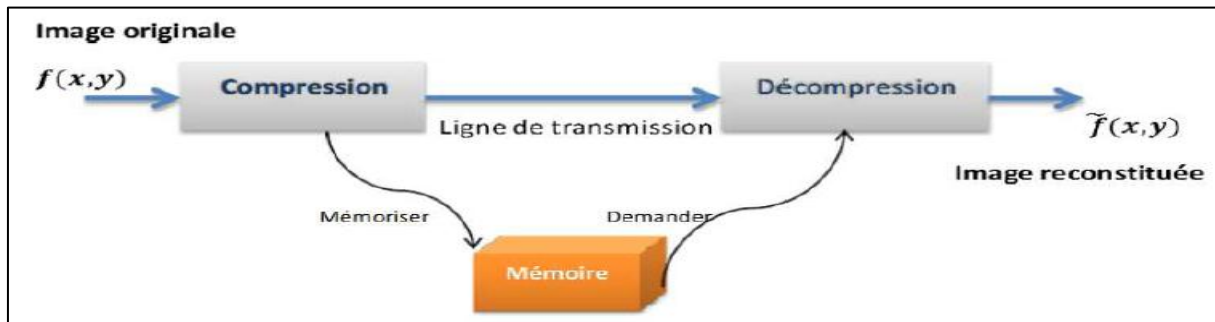


Figure 10 : Principe de Compression d'images.[11]

Les méthodes de compression d'images ont des critères d'évaluations, dont on peut citer :[12]

- Qualité de reconstruction des images.
- Le taux de compression.
- La rapidité du codeur.

La figure 11 illustre le schéma fonctionnel de compression :

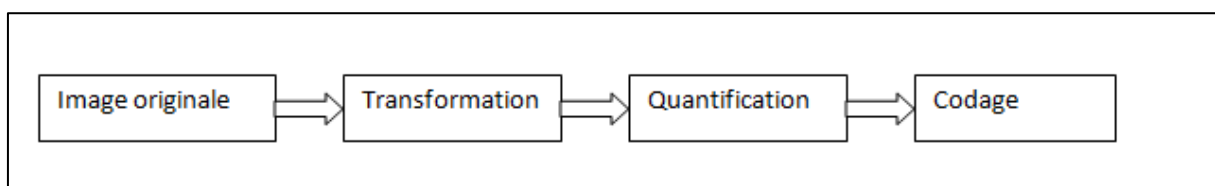


Figure 11 : Schéma d'un codeur d'image.[12]

En commençant par ce diagramme, nous allons passer en revue chaque étape pour voir quel rôle ils jouent.

Transformation:

La corrélation étroite dans l'image est reflétée par la dépendance entre chaque pixel et ses voisins (la luminosité fluctue très peu d'un pixel à l'autre).

Quantification :

Le but de la quantification des coefficients est de réduire la quantité de données qui doivent être représentées en bits. C'est un élément crucial du processus de compression.

Codage :

Les coefficients sont codés après avoir été quantifiés. Un codeur doit a priori satisfaire aux deux exigences suivantes :

- Individualité : aucun message ne doit être codé de la même façon.

Déchiffrable : deux mots de code consécutifs doivent être distingués sans ambiguïté.[12]

2.Définition

La compression d'image minimise la taille en octets des fichiers graphiques sans réduire la qualité de l'image à des niveaux inacceptables. La réduction de la taille du fichier permet de stocker plus d'images dans une quantité donnée de disque ou d'espace mémoire. Cela réduit également le temps d'envoi des images. En informatique, la compression de données est la technique consistant à utiliser une paire de fonctions C et D sur des chaînes. Le but de la fonction C est de compresser les données X et la fonction D de les décompresser. L'effet recherché est d'avoir $|C(x)| < |x|$.

3. Compression physique et logique

La compression physique : s'applique uniquement aux données de l'image. Il s'agit de translater les trains de bit d'un motif à un autre.

La compression logique: en remplaçant l'information par de l'information équivalente, on utilise le raisonnement logique pour accomplir la tâche.[13]

4. Compression symétrique et asymétrique

Parce que la même méthode est utilisée pour compresser et décompresser les données en compression symétrique, chacune de ces actions prend la même quantité de temps.

La compression asymétrique nécessite plus de travail pour l'une ou l'autre opération.

5. Paramètres de performances des méthodes de compression d'image

5.1. Rapport et taux de compression

Le taux de compression est défini comme le rapport du nombre de bits utilisés par l'image originale et du nombre de bits utilisés par l'image compressée.[14]

$$CR = \text{rapportc} = \frac{\text{nombre de bits avants compression}}{\text{nombre bits après compression}} \quad (1)$$

Le rapport de compression est un pourcentage de l'espace total occupé par les données avant compression divisé par l'espace total occupé par les données après compression. Cela signifie que le taux de compression d'un fichier compressé pleine taille est de 0%. Le taux de compression d'un fichier réduit à 0 octets est de 100%. [15]

$$T_c = \text{TauxC} = \left(1 - \frac{1}{CR}\right) * 100 \quad (2)$$

5.2.Mesure de distorsion

Nous utiliserons l'erreur quadratique moyenne (EQM) ou le rapport signal-bruit de crête pour quantifier la distorsion entre l'image reconstruite et l'image d'origine (mesure de la qualité visuelle de l'image reconstruite) (PSNR).

Etant donnée une image originale composée de pixels $a_i(i=1...N)$ et l'image décodée composée de pixels $\hat{a}_i(i=1...N)$. Alors l'erreur quadratique moyenne est donnée par:[15]

$$MSE = \frac{1}{N} \sum_1^N (a_i - \hat{a}_i)^2 \quad (3)$$

Le rapport signal-bruit de l'image reconstruite PSNR (Peak Signal to Noise Ratio) est l'autre critère objectif décrit ci-dessus. L'équation qui la définit est : [16]

$$PSNR = 10 \log_{10} \frac{(2^R - 1)^2}{MSE} \text{ DB (décibels)} \quad (4)$$

$$\text{Ou: } PSNR = 10 \log_{10} \frac{d^2}{MSE} \quad (5)$$

La valeur d'intensité maximale de l'image est d . Les valeurs sont donc encodées sur 8 bits à l'aide d'images en niveaux de gris, et dans cet exemple $d \leq 2^8 - 1$.

5.3. Entropie:

Est une métrique "surprise" dans le sens que les prédictions sont difficiles à faire si l'entropie est élevée, et si l'entropie est faible, la séquence facilement prévisible contient beaucoup d'informations si une séquence a beaucoup de "surprise." Il ne contient pas beaucoup d'informations s'il n'y a pas beaucoup de "surprises". La formule suivante le définit : [10]

$$H = \sum_{K=0}^{2^R-1} P(K) \log_2 P(K) \text{ bpp} \quad (6)$$

Avec : $P(K)$ indiquant la probabilité de niveaux de gris apparaissant dans l'image, K indiquant la valeur de gris, et R indiquant la quantité de bits par pixel. [14]

5.4. Le temps d'exécution

Lors de l'évaluation des performances de toute méthode de compression, la limitation de temps est critique ; il s'agit de calculer le temps nécessaire pour compresser et décompresser les images. En fonction de l'application visée par la compression, cette limitation s'applique plus ou moins (transmission ou archivage). En effet, il serait regrettable que le temps économisé en abaissant la quantité de données à transférer soit inférieur au temps consacré à la compression et à la décompression dans une application de transmission. [16]

6. Les objectifs de la compression

Nous mentionnons les objectifs de compression : "Aujourd'hui, la puissance des processeurs s'étend plus vite que la capacité de stockage, et considérablement plus vite que la bande passante des réseaux opérationnels."

- La rapidité de la compression et la décompression.
- La compression d'images permet de réduire énormément la taille des images.
- La réduction de la taille des données a entraîné une réduction du temps de transmission.
- Garantie de non perdu de l'image entière grâce à la robustesse de l'algorithme de compression.
- Deux qualités: le taux de compression et la qualité de l'image après un cycle de compression\décompression.

7. Type de compression

Les redondances des données présentes sur l'image sont utilisées pour compresser l'image. Ces redondances sont :

- **Redondance psycho visuel:** Détails qui ne sont pas visibles à l'œil nu et peuvent être enlevés (caractéristiques de l'œil humain).
- **Redondance inter pixel :** Du fait de la corrélation qui peut exister entre les pixels de l'image, on parle de redondance inter-pixel lorsqu'il est possible de prédire la valeur d'un pixel connaissant la valeur des pixels voisins (le plus proche ou le

précédent), sachant que plus la résolution de l'image, plus grande est la possibilité de rencontrer des redondances entre pixels.

- **Redondance de codage** : Séquence de répétition bis rencontrée pendant la phase de codage, généralement vers la fin de la compression.

Les méthodes dites sans perte ou réversibles garantissent une restitution parfaite des images, mais les méthodes dites de perte ou irréversibles affectent plus ou moins la valeur des pixels (Figure 12). [15]

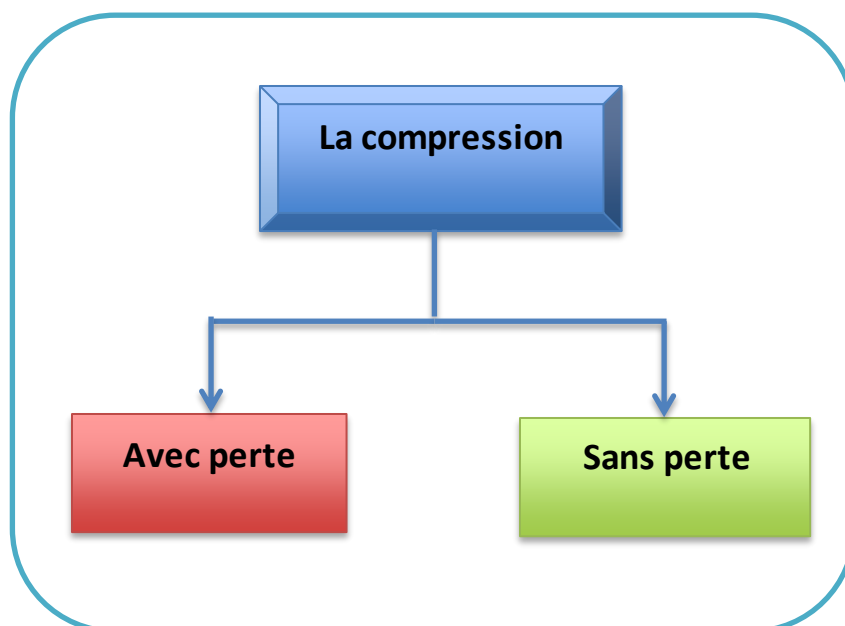


Figure 12: les types de compression.

7.1. La compression sans perte

Cette méthode de compression n'entraîne aucune perte de données, comme son nom l'indique.

Les photos médicales, l'imagerie satellitaire (les images sont coûteuses et les détails sont essentiels), le texte, les programmes et les autres types d'archives de données qui

doivent être conservés dans les "mêmes données" adopter cette compression conservatrice. Plusieurs méthodes sont utilisées, dont les suivantes :

- Codage de Huffman.
- Codage de Shannon-Fano.
- Codage arithmétique.
- Le codage par répétition ou "Run Length Coding" (**RLC**).
- Codage par dictionnaire adaptatif (LZW) (Lempel-Ziv-Welch) ou LZ77.

Ce type de compression est nécessaire pour certaines applications où la précision est majeure telles que les images médicales (IRM) ou la télédétection (imagerie satellite).

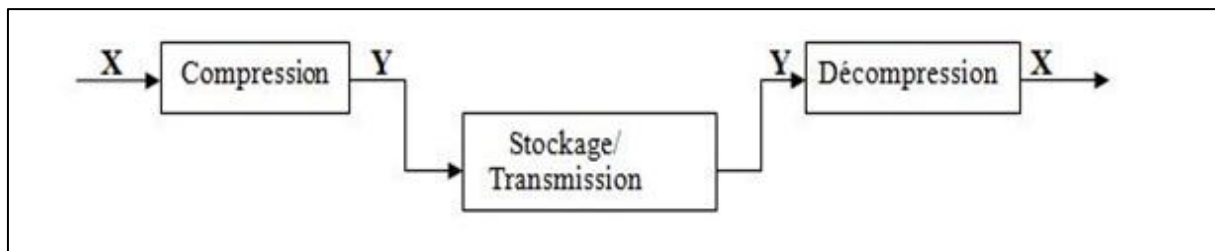


Figure 13 : Compression sans perte. [10]

7.2 La compression avec perte

Pour atteindre des taux de compression élevés, des méthodes avec perte sont utilisées. De tels algorithmes, après compression, fournissent une image différente qui contient beaucoup moins d'informations que l'image d'origine. Selon le degré de compression, ce changement est plus ou moins visible. L'attrait de cette famille est qu'elle peut produire de très gros rendements. Cependant, ce type de compression ne peut être

utilisé que pour l'audio, la vidéo et les images, pas pour les fichiers ou le texte, car ceux-ci ne devraient pas être affectés.

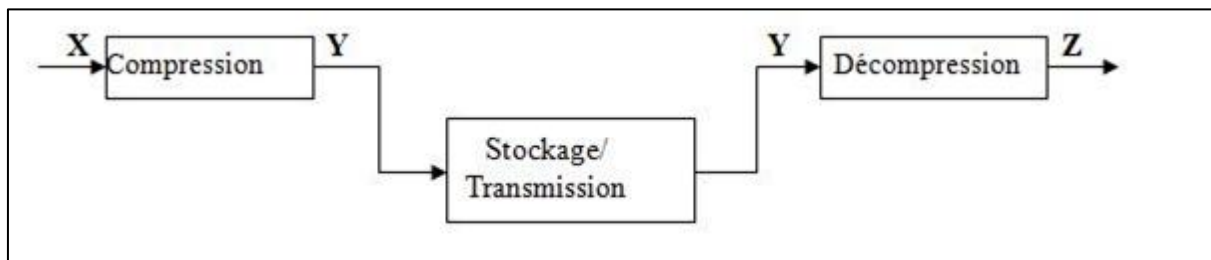


Figure 14 : Principe de compression avec Perte. [10]

Divers algorithmes de compression sont utilisés, dont les plus importants sont :

- Quantification.
- Codage par transformée.
- Le codage en sous-bandes.
- La compression fractale.
- **La compression par ondelettes.**

Quelques exemples de techniques de compression avec perte sont les suivants :

- JPEG.
- JPEG 2000.

7.2.1 La compression JPEG 2000

La norme JPEG 2000, qui doit remplacer la norme JPEG, régit le codage des photographies numériques. jp2 est utilisé pour les images JPEG 2000. L'originalité de JPEG 2000 est qu'il permet de compresser des images avec ou sans perte

d'informations. Cependant, la norme ne décrit que la méthode de décompression qui doit être utilisée pour les images dans ce format. Par conséquent, les développeurs qui souhaitent implémenter un algorithme de compression compatible JPEG 2000 peuvent faire ce qu'ils veulent, tant que leurs méthodes répondent aux exigences de la norme. La compression JPEG 2000 commence par la conversion des trois composants colorimétriques de l'image en un coefficient de luminosité et deux coefficients colorimétriques. Cette première étape de compression est optionnelle, contrairement au JPEG.

L'encodeur JPEG 2000, contrairement à JPEG, utilise un traitement en ondelettes des pixels de l'image. Il s'agit d'une conversion de pixels d'image en fréquences, chaque pixel correspondant à une seule fréquence. Dans les divisions consécutives de l'image source, cette procédure produit plusieurs sous-images [18]. Chacune de ces sous-images a une plage de fréquences. Les hautes fréquences sont moins fréquentes dans la plupart des photographies que les basses fréquences parce que les hautes fréquences indiquent que les pixels de l'image sont très dissemblables les uns des autres, ce qui est rare dans une image. Il y a ensuite l'étape de quantification, qui consiste à supprimer les fréquences les plus élevées en fonction d'un taux de compression. Toutefois, si la compression est non destructive, l'étape de quantification est ignorée.

8. Compression par ondelettes

8.1. Les ondelettes

8.1.1. Définition

- Les ondelettes sont des fonctions qui sont développées assez récemment en mathématiques.
- La première ondelette a été introduite par Grossmann et Morlet en 1984 pour modéliser des signaux sismiques.
- Les ondelettes sont obtenues à partir de la translation et de la dilatation d'une fonction unique ψ appelée « ondelette mère ». Elles permettent une représentation localisée, temps/fréquence.

8.2 Transformée en ondelette continue (CWT)

La transformation en ondelette continue produit un vecteur avec une dimension de plus que les données originales. Nous obtenons une image du plan temps-fréquence pour les données 1D. Il est donc facile de visualiser l'évolution de la fréquence du signal dans le temps et de comparer son spectre à celui d'autres signaux [19].

Des paramètres de translation et d'expansion variant continuellement sont utilisés dans la transformation des ondelettes. Les fonctions utilisées sont définies par :

$$\psi_{a,b}(x) = \frac{1}{\sqrt{|a|}} \psi\left(\frac{x-b}{a}\right) \text{ ou } a, b \in \mathbb{R}, a \neq 0 \quad (7)$$

C'est une fonction $S(a,b)$ qui associe aux paramètres " a " et " b " la valeur du coefficient $C_{a,b}$ de l'ondelette $\psi_{a,b}$ dans la décomposition du signal. La quantité " b " est le paramètre de localisation temporelle, tandis que " $\frac{1}{a}$ " est le paramètre de fréquence.

$C_{a,b}$ est une intégrale qui mesure la somme des aires algébriques décrites par la courbe produit de $S(t)$ et ψ_a .

8.3 Transformée en ondelette discrète (DWT)

La transformation discrète des ondelettes produit un vecteur de données de la même longueur que l'entrée. La majorité des valeurs de ce vecteur sont essentiellement nulles. C'est parce que la traduction et l'homothésie le décomposent en un ensemble d'ondelettes orthogonales (fonctions). En conséquence, le signal est divisé en un nombre de coefficients de spectre d'onde égal ou inférieur au nombre de points de données dans le signal. Ce spectre d'ondelettes est idéal pour la compression et le traitement du signal[19].

En 1978, Y. Meyer a prouvé que les bases d'ondelettes orthonormales pouvaient être construites en discrétisant les paramètres d'expansion et de translation a et b en utilisant l'équation :

$$(a,b) = (a_0^j K b_0 a_0^j) \quad (8)$$

Avec $(j,K) \in \mathbb{Z}^2$

$a_0 > 1$, $b_0 > 0$: pas de dilatation et translation respectivement.

Ainsi la nouvelle famille d'ondelettes peut s'écrire :

$$\psi_{j.K}(t) = a_0^{-j/2} \psi(a_0^{-j} t - Kb_0) \quad (9)$$

Avec $(j,K) \in \mathbb{Z}^2$

La transformée en ondelettes discrète d'une fonction est donnée par l'équation :

$$C_{f(j,k)} = \langle f, \psi_{j,k} \rangle = a_0^{-j/2} \int_{-\infty}^{+\infty} (a_0^{-j} t - Kb_0) f(t) dt \quad (10)$$

Mayer a montré qu'il existe des familles d'ondelettes discrètes formant des bases orthonormées de $L^2(\mathbb{R})$.

Les paramètres des dilatations et de translation sont choisis comme suit :

$$(a,b) = (a_0^j, Kb_0 a_0^j) = (2^{-j}, K2^{-j}) \text{ avec } a_0 = 2, b_0 = 1 \quad (11)$$

Nous obtenons ainsi des bases dans $L^2(\mathbb{R})$ de la forme :

$$\{\psi_{j.k}\}_{j,k \in \mathbb{Z}} = \left\{ 2^{\frac{j}{2}} t - K \right\}_{j,k \in \mathbb{Z}} \quad (12)$$

La décomposition de $f(t) \in L^2(\mathbb{R})$ peut s'écrire alors :

$$\sum_{j,k \in \mathbb{Z}} \langle f(t), \psi_{j.k}(t) \rangle \psi_{j.k}(t) \quad (13)$$

$$\text{Ou } \langle f(t), \psi_{j.k}(t) \rangle = 2^{-\frac{j}{2}} \int_{-\infty}^{+\infty} f(t) \overline{\psi_{j.k}(2^{-j}t - k)} dt \quad (14)$$

$\langle f(t), \psi_{j.k}(t) \rangle$ Représenté les coefficients qui sont décorrélés entre eux.

La fonction continue f est alors entièrement représentée par la fonction discrète $C_{f(j.k)}$

$$C_{f(j.k)} = \langle f(t), \psi_{j.k}(t) \rangle \quad (15)$$

8.4. Le choix des ondelettes

Il n'y a pas d'ondelette supérieur. Tout dépend du logiciel que vous utilisez. Dans certaines circonstances, l'ondelette la plus basique (cheveux) est la meilleure option. Ce sera la pire option pour d'autres applications. En pratique, le nombre de moments nuls est le facteur le plus critique. Pour la plupart des applications, avoir les coefficients d'onde les plus nuls est préférable, et donc avoir plus de moments nuls équivaut à une meilleure transformation. Les ondelettes avec plus de moments, d'autre part, ont un support plus élevé, ce qui signifie que si la fonction ou le signal contient des discontinuités abruptes, il sera plus sensible au phénomène de Gibbs [19].

8.5. Avantages des ondelettes

- Même avec des rapports de compression élevés, la compression des ondelettes est une approche très efficace (plus de 90 %).
- Le taux de compression est prédit à l'aide de cette méthode.

- Il n'a pas d'effet mosaïque.
- L'algorithme est plus simple, ce qui signifie qu'il est plus rapide.
- Il est possible de créer des images assez petites (ordre KO).
- Il existe deux méthodes de décompression d'une image compressée en ondelettes.
- Sa résolution est fixe, mais sa taille augmente avec le temps.
- Sa taille est fixe, mais sa résolution s'améliore au fil du temps.
- Les bases d'ondelettes sont constituées d'une seule fonction qui est développée et traduite [19].

8.6. Critères de qualité des ondelettes utilisées en traitement d'images

Les ondelettes sont des fonctions qui peuvent être caractérisées par certaines propriétés remarquables ; comme ces derniers ne sont pas compatibles entre eux, cela signifie que des décisions doivent être prises en fonction de l'application souhaitée. Nous donnons des propriétés communes et des exemples d'ondelettes [19].

- ❖ **Régularité** : certaines peuvent être de classe $C^{+\infty}$ (comme les dérivées de gaussienne), d'autres de classe $C^k, k \in \mathbb{N}$ (ondelettes splines), alors que certaines peuvent être discontinues (ondelettes de Haar) ou présenter une régularité Lipchitzienne inférieure à 1 (comme certaines ondelettes de Daubechies).
- ❖ **Support compact** : $\{x \in \mathbb{R} / \psi(x) \neq 0\}$ borné. Les ondelettes utilisées sont localisées dans le plan espace-fréquence (contrairement aux fonctions $(t \rightarrow e^{ikt})_{k \in \mathbb{Z}}$, lesquelles ne sont pas localisées en espace mais uniquement en fréquence).

❖ **Parité:** $\forall x \in \mathbb{R}, \psi(-x) = \psi(x)$

❖ **Décroissance rapide :** une ondelette sera dite à rapide si:

$$\forall m \in \mathbb{N}, \exists C_m > 0 / \forall t \in \mathbb{R}, |\psi(t)| \leq \frac{C_m}{1+|t|} \quad (16)$$

❖ **Nombre de moments nuls :** pour $n \in \mathbb{N}$, une ondelette admet n moments nul si:

$$\forall k = 0 \dots n - 1 \int_{-\infty}^{+\infty} t^k \psi(t) dt = 0 \quad (17)$$

❖ **Orthogonalité :** une ondelette ψ est dite orthogonale si pour tout $(j, j', n, n') \in \mathbb{Z}^2$

$$\langle \psi_{j,n}, \psi_{j',n'} \rangle = \delta_{j,j'} \delta_{n,n'} \quad (\delta_{j,j'} = 0 \text{ si } j \neq j', \delta_{jj} = 1) \quad (18)$$

8.7. Quelques ondelettes

Nous allons présenter quelques exemples d'ondelettes analysantes ainsi que leurs principales caractéristiques.

8.7.1. Ondelettes orthogonales

8.7.1.1. Ondelette de Haar

La première ondelette a été proposée par Haar(1909) .l'intérêt de cette base d'ondelettes est la grande simplicité des filtres associés donc de l'algorithme de calcul.

a-Décomposition suivant la base de Haar

Les filtres [Truchetet, 1998] associés à la décomposition sont :

$$\tilde{h}(n) = \left\{ \frac{1}{\sqrt{2}} \mid \frac{1}{\sqrt{2}} \right\} \tilde{g}(n) = \left\{ -\frac{1}{\sqrt{2}} \mid \frac{1}{\sqrt{2}} \right\} \quad (19)$$

b-Reconstruction suivant la base de Haar

Les filtres [Truchetet, 1998] associés à la décomposition sont :

$$h(n) = \left\{ \frac{1}{\sqrt{2}} \mid \frac{1}{\sqrt{2}} \right\} g(n) = \left\{ \frac{1}{\sqrt{2}} \mid -\frac{1}{\sqrt{2}} \right\} \quad (20)$$

8.7.1.2. Les ondelettes à support compact de Daubechies

Les ondelettes les plus connues et les plus utilisées sont celles de Daubechies en raison de leurs propriétés remarquables qui les distinguent des autres types d'ondelettes. Leur expression analytique n'existe pas, mais le carré du module de la fonction de transfert de h est connu et on peut déduire leurs coefficients de certaines manipulations mathématiques. Nous choisissons une ondelette de Daubechies dans l'ordre de son moment. On n'a donc qu'une seule ondelette par instant, et en fixant l'ordre on obtient les coefficients des filtres associés. Les ondelettes de Daubechies représentent une base orthonomique et sont supportées de manière optimale pour un certain nombre de moments nuls [19].

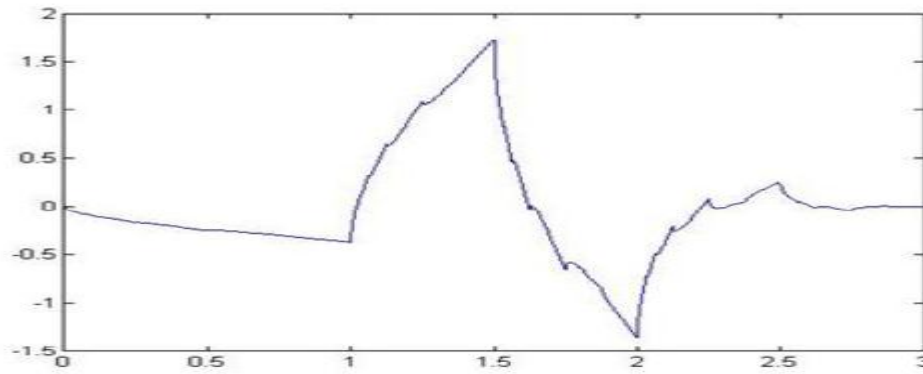


Figure 15: Ondelette de Daubechies.[19]

8.7.2. Ondelettes biorthogonales

Les ondelettes biorthogonales sont définies de manière analogue aux ondelettes orthogonales, mais on écrit les décompositions à partir de résolutions multiples biorthogonales [19]:

$$V_{j-1} = V_j \oplus W_j \text{ avec } W_j \subset (V_j^*)^1 \quad (21)$$

$$V_{j-1}^* = V_j^* \oplus W_j^* \text{ avec } W_j^* \subset (V_j)^1 \quad (22)$$

De manière analogue au cas orthogonal, un signal f de L^2 peut s'écrire:

$$\begin{aligned} f(t) &= \sum_{j,n \in \mathbb{Z}} \langle f, \psi_{j,n}^* \rangle \psi_{j,n}(t) \quad (23) \\ &= \sum_{n \in \mathbb{Z}} \langle f, \phi_{j,n}^* \rangle \phi_{j,n}(t) \\ &\quad + \sum_{k \leq j, n \in \mathbb{Z}} \langle f, \psi_{k,n}^* \rangle \psi_{k,n}(t) \\ &= \sum_{j,n \in \mathbb{Z}} \langle f, \psi_{j,n} \rangle \psi_{j,n}^*(t) \end{aligned}$$

$$= \sum_{n \in Z} \langle j, \phi_{j,n} \rangle \phi_{j,n}^*(t) \\ + \sum_{k \leq j \in Z} \langle f, \psi_{k,n} \rangle \psi_{k,n}^*(t)$$

Conclusion

Dans ce premier chapitre, nous avons présenté une introduction générale sur la cryptographie et la compression. Dans la première partie, nous avons commencé par un bref historique et une définition de la cryptographie avec une mention de l'usage et le mécanisme et nous avons distingué deux classes importantes des méthodes de chiffrement, aussi montré la puissance et la faiblesse de chaque type d'algorithme de chiffrement et fait la différence entre eux, puis dans la deuxième partie, nous avons essayé de faire un récapitulatif sur les notions élémentaires de la compression d'images en présentant les deux types de compression et citer quelques techniques et nous mettons également en évidence la compression par ondelettes, sans oublier de parler sur les paramètres de performance qui servent à évaluer ces techniques et nous avons parlé en détail sur la compression par ondelettes.

La combinaison de ces deux techniques, à savoir la compression et le cryptage, et le choix de l'algorithme de compression et de cryptage pour en faire un système hybride de crypto-compression, tout ça sera détaillé dans le deuxième chapitre.

CHAPITRE 02

CRYPTO COMPRESSION D'IMAGE

Chapitre 2

Crypto Compression d'image

Introduction

La réduction de la taille des bits présentés dans l'image est devenue de plus en plus importante dans le stockage, puis la confidentialité de celle-ci, la cryptographie est également devenue un critère très important dans la transmission sécurisée des images. Pour assurer ces deux critères, il faut des techniques qui combinent les deux technologies de compression et de chiffrement d'image, conduisant aux techniques de crypto-compression qui ont émergé ces dernières années. Le concept vise à combiner les méthodes de chiffrement et de compression. L'objectif est d'acquérir un petit volume de données avec une confidentialité robuste. Le travail présenté dans ce chapitre concerne une approche de crypto-compression basée sur le Block Cipher et un algorithme de compression par ondelettes.

1. Théorie des ondelettes

L'analyse par ondelettes a été introduite au début des années 1960 pour l'analyse des signaux et le contexte de l'exploration pétrolière. Le problème à l'époque était de

savoir comment représenter le signal de manière à ce que les informations temporelles (position dans le temps, durée) et fréquentielle puissent être affichées simultanément pour identifier les propriétés physiques de la source du signal. Depuis, les ondelettes n'ont cessé de se développer et de trouver de nouveaux domaines d'application. [21]

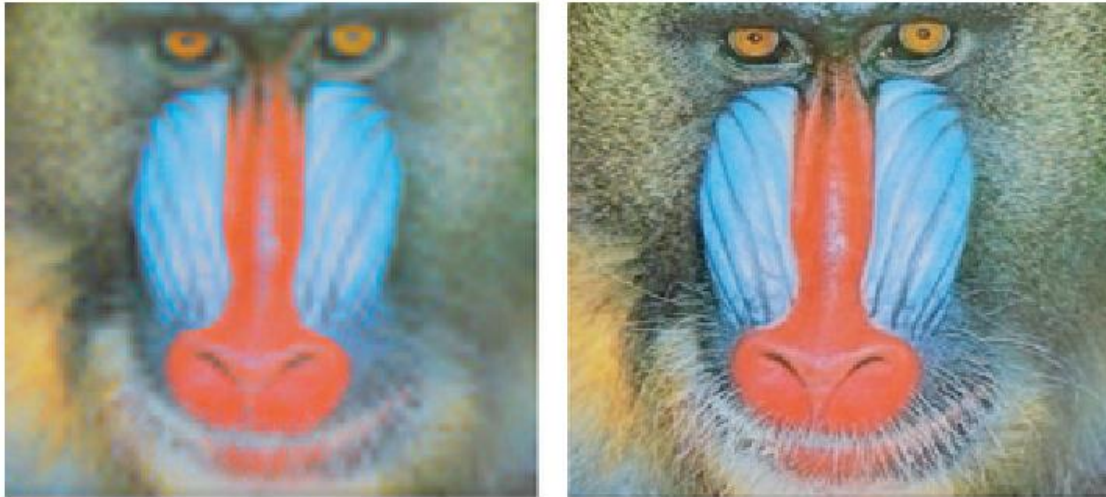
1.1. Limites de la Transformée de Fourier

On dit que l'analyse d'un signal à travers des ondelettes est similaire à son analyse Fourier car il convertit également un signal en ses composants principaux l'analyser. Cependant, la transformation de Fourier n'est plus suffisante ici. Bien qu'il soit incapable de dire quelles parties du signal changent lentement ou rapidement, nous devons distinguer les zones riches en informations de celles qui ne le sont pas.

DWT (Discrete Wavelet Transform) est une méthode de compression basée sur les ondelettes utilisé par le format naissant JPEG 2000 (en passe de devenir une norme internationale), le successeur de JPEG, qui est basé sur DCT (Discrete Cosine Transform). Grâce à l'utilisation des ondelettes, ce format bénéficie d'une compression 50 à 100 fois supérieure à son ancêtre JPEG, tout en conservant une bien meilleure définition des détails dans l'image finale.

Cas des images Il est avéré que les ondelettes apportent de bien meilleurs résultats que l'algorithme le plus utilisé actuellement en imagerie multimédia pour la compression : la DCT. En effet, contrairement à la DCT, la DWT s'applique à la totalité de l'image et non pas à des blocs de pixels, ce qui permet d'éviter l'apparition de carrés uniformes lorsque le taux de compression est élevé. De plus, l'utilisation

d'une ondelette réversible permet une compression sans perte de données, ce qui n'était pas possible avec le format JPEG par exemple. Voici une comparaison de ces deux méthodes de compression.[21]



-a-

-b-

Figure16:-a- Image compressée avec JPEG (DCT) (Transformé de Fourier)

-b- Image compressée avec JPEG2000 (DWT) (Transformé par ondelettes).[21]

- Si on modifie une valeur d'un coefficient de la transformée de Fourier d'un signal tout le signal va se déformer. Maintenant, si on fait la même chose, mais en passant par la transformée en ondelettes, on ne va dégrader qu'une partie du signal
- Avec les ondelettes, le signal est découpé en différents morceaux qui sont des versions translatées et dilatées d'une même fonction (l'ondelette mère). Il en résulte une superposition d'ondelettes décalées et dilatées qui ne diffèrent entre elles que par leur taille. On obtient une transformée en ondelettes, fonction composée de deux variables : le temps et la fréquence.

- Le point fort de cette technique est que les ondelettes s'adaptent en fonction des caractéristiques recherchées : hautes fréquences (l'ondelette est très ne) ou basses fréquences (l'ondelette s'étire). On parlera alors de multirésolution.[21]

2. Multirésolution

Une résolution multiple est une famille particulière de sous-espaces fermés de $L^2(\mathbb{R})$

Il s'agit d'un outil de construction basé sur les ondelettes. D'une multirésolution sélectionnée en fonction des caractéristiques du signal traité, on peut travailler avec différentes ondelettes : ondelettes de Haar (dans notre cas), ondelettes de Daubechies.

L'une des principales raisons du succès des méthodes repose sur la transformée de Fourier est due aux algorithmes de calcul rapides qui lui sont associés (la fameuse FFT: Fast Fourier Transform). Cependant, il a été trouvé que les transformations en ondelettes discrètes sont naturellement associées à des algorithmes qui peuvent être encore plus efficaces que les algorithmes FFT si l'ondelette est choisie de manière appropriée. Les coefficients d'ondelettes d'un signal sont obtenus à partir d'une série d'opérations de lissage sur le signal à des résolutions progressivement plus grossières. La note clé est que ce lissage peut être effectué de manière récursive, systématiquement à l'aide d'un seul opérateur de lissage.[21]

3. Analyse d'ondelettes

Actuellement, le sujet des ondelettes devient attractif dans le domaine des mathématiques et de l'ingénierie. Comme l'analyse de Fourier, l'ondelette a deux unités mathématiques : "transformée en ondelettes intégrale" et "transformée en ondelettes en série". Supposons que dans un espace quadratiquement intégrable, une fonction à valeurs réelles (multiplication de deux fonctions scalaires) existe là et une sommation sur cet espace, une série de sommations est obtenue et une fonction décalée et mise à l'échelle de la fonction de base est réalisée. Ces deux fonctions sont liées par une expression ou une équation appelée transformée en ondelettes. L'équation est:

$$[\Phi_{u,v}(y) = 2^{\frac{u}{2}} \Phi(2^u - v)] \quad (24)$$

Si 'u' va être fixe, cela signifie que pour une valeur de mise à l'échelle particulière, s'il y a est une variation de la valeur du paramètre de décalage, alors il y aura quelques sous-espace et espace des différences dans un espace de carré intégrable $L^2(\mathbf{R})$, c'est-à-dire rien d'autre qu'une idée conceptuelle du concept mathématique abstrait. À partir de ces deux conceptions de l'espace, on peut développer l'idée de « Fonction de mise à l'échelle » et la « Fonction d'ondelettes ». L'équation des deux fonction s'écrivent ainsi

$$\Phi(\mathbf{n}) = \sum_b r_\Phi(\mathbf{n}) \sqrt{2} \Phi(2\mathbf{n}-\mathbf{b}) \quad \Psi(\mathbf{n}) = \sum_b r_\Psi(\mathbf{n}) \sqrt{2} \Phi(2\mathbf{n}-\mathbf{b}) \quad (25)$$

Ici, le $\Phi(\mathbf{n})$ est appelé la fonction de mise à l'échelle et le $\Psi(\mathbf{n})$ est appelé la Fonction ondelettes. Ils sont tous deux la classe différente de la fonction et la fonction de base est la somme de l'ordre supérieur de la fonction. C'est signifié que toute fonction dans

l'espace carré intégrable $L2(R)$, va être approximative par la somme de la version décalée de la mise à l'échelle fonction, qui est en fait une fonction d'ondelettes.[22]

3.1 Transformation en ondelettes discrètes (DWT)

Le principe de l'algorithme est de découper l'image en quatre parties à chaque iteration: trois blocs concernent les détails de l'image et le quatrième correspond à celui information la plus importante pour l'œil (basses fréquences), qui sert de base pour la prochaine itération. Par conséquent, pour décomposer cette image, nous utilisons deux filtres résultant du choix de l'ondelette : un filtre passe-haut et un filtre passe-bas.

À partir de ces ondelettes, nous formons donc les deux filtres : nous noterons H le filtre passe-haut, et L le filtre passe-bas. Cette phase s'appelle la phase d'analyse.

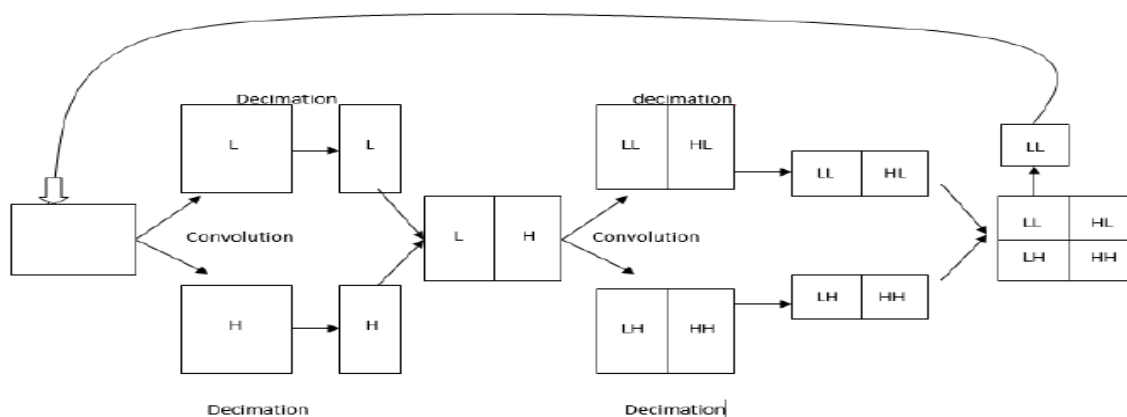


Figure 17: Principe de la DWT.[23]

La ligne supérieure correspond aux images convoluées avec le filtre L. La ligne inférieure

correspond aux images convoluées avec le filtre H L'itération suivante est effectuée en prenant pour l'image de base la partie LL correspondant à la convolution par le filtre passe-bas (horizontal et vertical). Le format JPEG2000 limite le nombre d'itérations D entre 0 et 32, avec des valeurs par défaut majoritairement entre 4 et 8. Si l'on considère plus généralement l'effet de cette transformation, il semble que cet algorithme concentre l'énergie de l'image dans le Blocs LL de niveau de décomposition plus élevé. Ensuite, tous les autres blocs ne sont que des détails de l'image. Ainsi, la manière de compresser une partie des coefficients de cette matrice, et donc de la mettre à zéro, revient à analyser les blocs les plus décomposés et à faire une hypothèse : les valeurs faibles dans les hauts degrés de décomposition tendent progressivement vers zéro. Vous montez les niveaux. Ce procédé va permettre de comprimer énormément les zones, qui sont relativement continues, mais en préservant toutes les discontinuités, en suivant le contour de l'image, puisque les filtres passe-haut sont appliqués dans toutes les directions : vertical, horizontal et diagonal (une combinaison des deux).[23]

La figure suivante résume le principe de fonctionnement.

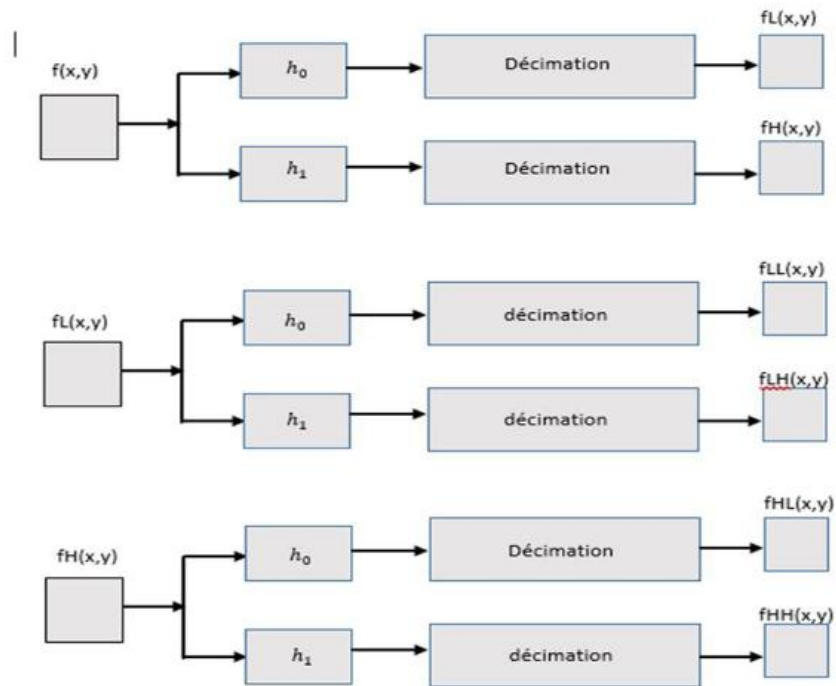


Figure 18: schema de décomposition. [23]

Donc nous avons choisi la plus simple ondelette pour faire notre système de crypto compression: l'ondelette de Haar.

4. Ondelettes de Haar

4.1. Définition

En mathématiques, l'ondelette de Haar est une séquence de fonctions "en forme de carré" remises à l'échelle qui forment ensemble une famille ou une base d'ondelettes. L'analyse on ondelettes est similaire à l'analyse de Fourier en ce qu'elle permet de représenter une fonction cible sur un intervalle en termes de base orthonormée. La

séquence de Haar est maintenant reconnue comme la première base d'ondelettes connue et largement utilisée comme exemple d'enseignement.

La séquence de Haar a été proposée en 1909 par Alfred Haar. **Haar** a utilisé ce système orthonormé pour l'espace des fonctions carrées intégrables sur l'intervalle unitaire [0,1]. L'étude des ondelettes, et même le terme "ondelettes", n'est venue que bien plus tard. En tant que cas particulier de l'ondelette de Daubechies, l'ondelette de Haar est également connue sous le nom de Db1.

L'ondelette de Haar est aussi l'ondelette la plus simple possible. L'inconvénient technique de l'ondelette de Haar est qu'elle n'est pas continue, et donc non différentiable. Cette propriété peut cependant être un avantage pour l'analyse de signaux à transitions brusques (signaux discrets), comme la surveillance de panne d'outils dans les machines. [24]

La fonction d'ondelette mère de l'ondelette de Haar peut être décrite comme $\psi(t)$

$$\psi(t) = \begin{cases} 1 & 0 \leq t < \frac{1}{2}, \\ -1 & \frac{1}{2} \leq t < 1, \\ 0 & \text{otherwise.} \end{cases} \quad (26)$$

Sa fonction de mise à l'échelle peut être décrite comme $\varphi(t)$

$$\varphi(t) = \begin{cases} 1 & 0 \leq t < 1, \\ 0 & \text{otherwise} \end{cases} \quad (27)$$

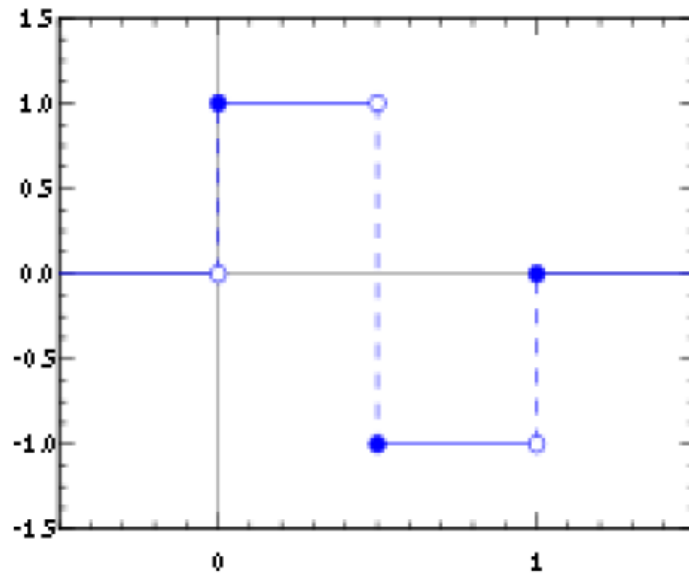


Figure 19: Ondelette de Haar.[24]

4.2. Fonctions Haar et système Haar

Pour tout couple n, k des nombres entiers, la fonction de Haar de $l_{n,k}$ est défini sur la ligne réelle par la formule $\mathbb{Z} \mathbb{R}$

$$\psi_{n,k}(t) = 2^{\frac{n}{2}} \psi(2^n t - k), \quad t \in \mathbb{R} \quad (28)$$

Cette fonction est supportée sur l'intervalle d'ouverture à droite $l_{n,k} = [k 2^{-n}, (k+1)2^{-n}]$, c'est-à-dire qu'elle s'annule en dehors de cet intervalle. Il est d'intégrale 0 et de norme 1 dans l'espace de Hilbert $L^2(\mathbb{R})$,

$$\int_{-\infty}^{+\infty} \psi_{n,k}(t) dt = 0, \quad \|\psi_{n,k}(t)\|_{L^2(\mathbb{R})}^2 = \int_{-\infty}^{+\infty} \psi_{n,k}(t)^2 dt = 1. \quad (29)$$

Les fonctions de Haar sont orthogonales deux à deux,

$$\int_{-\infty}^{+\infty} \psi_{n_1, k_1}(t) \psi_{n_2, k_2}(t) dt = \delta_{n_1, n_2} \delta_{k_1, k_2}, \quad (30)$$

ou représente le delta de Kronecker. Voici la raison de l'orthogonalité: lorsque les deux intervalles d'appui et ne sont pas égaux, alors ils sont soit disjoints, soit le plus petit des deux appuis, disons, est contenu dans la moitié inférieure ou dans la moitié supérieure de l'autre intervalle, sur dont la fonction reste constante. Il s'ensuit dans ce cas que le produit de ces deux fonctions de Haar est un multiple de la première fonction de Haar, donc le produit a l'intégrale 0. $\delta_{ij} I_{n_1, k_1} I_{n_2, k_2} I_{n_1, k_1} \psi_{n_2, k_2}$

le système Haar sur la ligne réelle est l'ensemble des fonctions

$$\{\psi_{n,k}(t) : n \in \mathbb{Z}, k \in \mathbb{Z}\} \quad (31)$$

Il est complet en $L^2(\mathbb{R})$: le système de Haar sur la droite est une base orthonormée en $L^2(\mathbb{R})$. [24]

5. La décomposition Quadtree

La décomposition quadtree est une technique bien connue et établie dans le domaine de la compression d'images. Il est très utile avec les images fractales de compression qui contiennent également des motifs non linéaires infinis et complexes dans l'image. Une image en niveaux de gris naturels peut être segmentée en régions avec une certaine variété d'informations. Une technique quadtree permet de subdiviser cette image en une segmentation 2D basée sur un seuil donné (Samet, 1984). Il divise d'abord l'image entière en quatre rectangles ou carrés en forme de bloc. Ensuite, le

processus est exécuté de manière itérative avec la limite de seuil calculée et produit les blocs de plage et de plage, où les blocs de plage sont quatre fois plus grands que les blocs de plage. La figure 20 montre cette analyse de décomposition. [22]

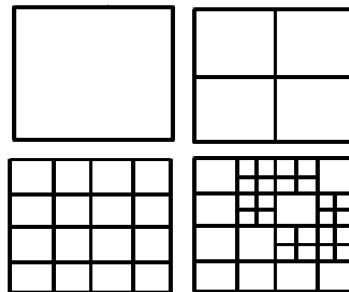


Figure 20: Décomposition Quadtree. [22]

6. Cryptage a clé privé

En fait, la cryptographie moderne aborde les problèmes de sécurité des communications de manière plus générale. L'objectif est d'offrir une gamme de services de sécurité telle que la confidentialité, l'intégrité, l'authentification des données transmises. La confidentialité est historiquement le premier problème rencontré par la cryptographie (comme dans les systèmes bancaires, télécoms ou militaires). Il est résolu par la notion de cryptage.[23]

6.1. L' AES (Advanced Encryption Standard)

L' AES opère sur des blocs de 128 bits (texte clair P) qu'il convertit en blocs chiffrés de 128 bits (C) par une séquence de Nr opérations ou "tours" à partir d'une clé de 128, 192 ou 256 bits. Selon la taille, le nombre de tours varie : 10, 12 et 14 tours respectivement.

6.1.1. L'AES : Algorithmme

Bloc divisé en octets répartis dans des matrices 4x4 (1 octet = 8 bits) (Figure 21).

- **Séquence de 4 transformations répétées :**
 - ✓ 1ère étape : substitution (confusion)
 - ✓ 2ème étape : décalage des lignes (diffusion)
 - ✓ 3ème étape : brouillage des colonnes (diffusion)
 - ✓ 4ème étape : addition des sous-clés.
- **Les tours :**
 - ✓ Tour initial: addition XOR des sous-clés aux blocs
 - ✓ Tours similaires itérés: les 4 étapes sont répétées.
 - ✓ Dernier tour: transformation sans la 3ème étape.

Étapes de chiffrement sont inversées et réordonnées pour produire un algorithme de déchiffrement. [25]

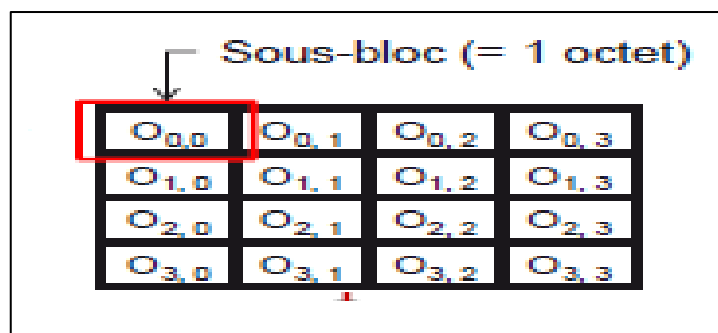


Figure 21 : Le bloc présenté par l'algorithme l'AES. [25]

6.1.2. Choix de l'AES

Le choix de cet algorithme répond à de nombreux critères plus généraux dont nous pouvons citer les suivants :

- sécurité ou l'effort requis pour une éventuelle cryptanalyse.
- facilité de calcul : cela entraîne une grande rapidité de traitement
- besoins en ressources et mémoire très faibles
- flexibilité d'implémentation : cela inclut une grande variété de plateformes et d'applications ainsi que des tailles de clés et de blocs supplémentaires
- hardware et software : il est possible d'implémenter l'AES aussi bien sous forme logicielle que matérielle (câblé)
- simplicité : le design de l'AES est relativement simple [23].

6.1.3. Principe de fonctionnement

Le schéma suivant (figure 22) décrit succinctement le déroulement du chiffrement :

- `BYTE_SUB` (Byte Substitution) est une fonction non-linéaire opérant indépendamment sur chaque bloc à partir d'une table dite de substitution.
- `SHIFT_ROW` est une fonction opérant des décalages (typiquement elle prend l'entrée en 4 morceaux de 4 octets et opère des décalages vers la gauche de 0, 1, 2 et 3 octets pour les morceaux 1, 2, 3 et 4 respectivement).
- `MIX_COL` est une fonction qui transforme chaque octet d'entrée en une combinaison linéaire d'octets d'entrée et qui peut être exprimée mathématiquement par un produit matriciel sur le corps de Galois (28).

- Le + entouré d'un cercle désigne l'opération de OU exclusif (XOR).
- K_i est la i ème sous-clé calculée par un algorithme à partir de la clé principale K . Le déchiffrement consiste à appliquer les opérations inverses, dans l'ordre inverse et avec des sous-clés.[23]

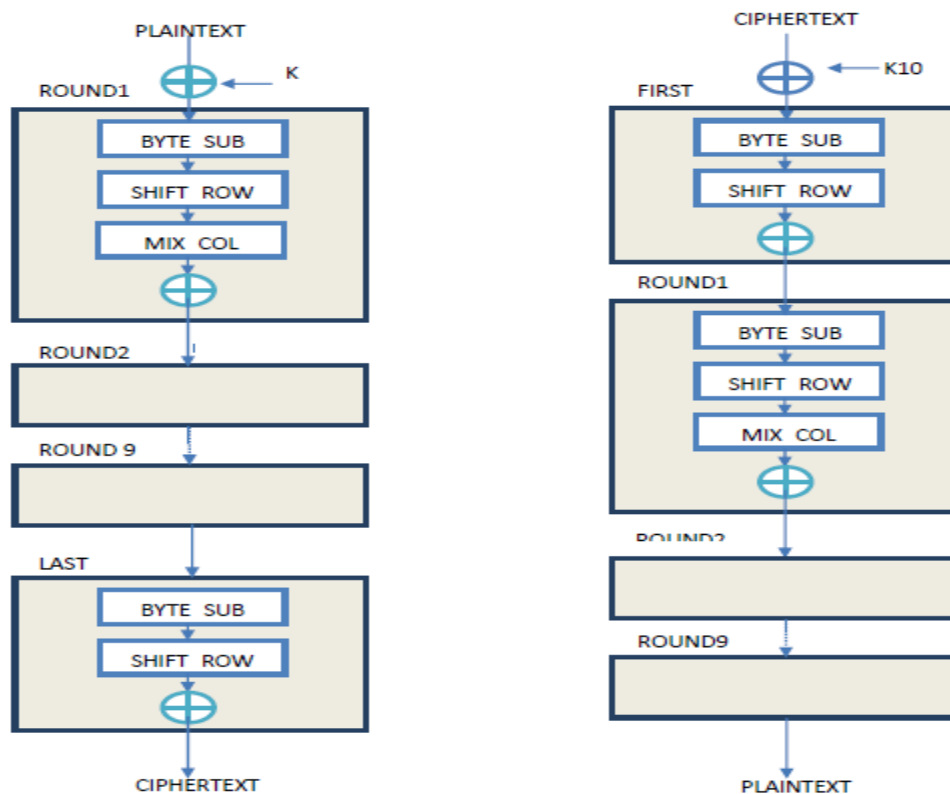


Figure 22: Principe de fonctionnement de AES.[23]

6.1.4. L'algorithme de cryptage

L'implémentation de l'algorithme de chiffrement et de déchiffrement AES-128 à l'aide du logiciel MATLAB est effectuée. Dans laquelle l'entrée est une image et la clé au format hexadécimal et la sortie est la même que celle de l'image d'entrée. Pour le processus de cryptage, divisez d'abord l'image et rendez-la en $4 * 4$ octets, c'est-à-dire au format matriciel. Calculez le nombre de tours en fonction de la taille de la clé et

développez la clé à l'aide de notre clé. Et il y a $(n-1)$ tours effectués qui sont des octets de substitution, décalent les lignes, mélangent les colonnes et ajoutent une clé. Le dernier tour « n » ne comprend pas de colonne de mélange dans l'itération. La Figure 23 montre le flux de l'algorithme.[26]

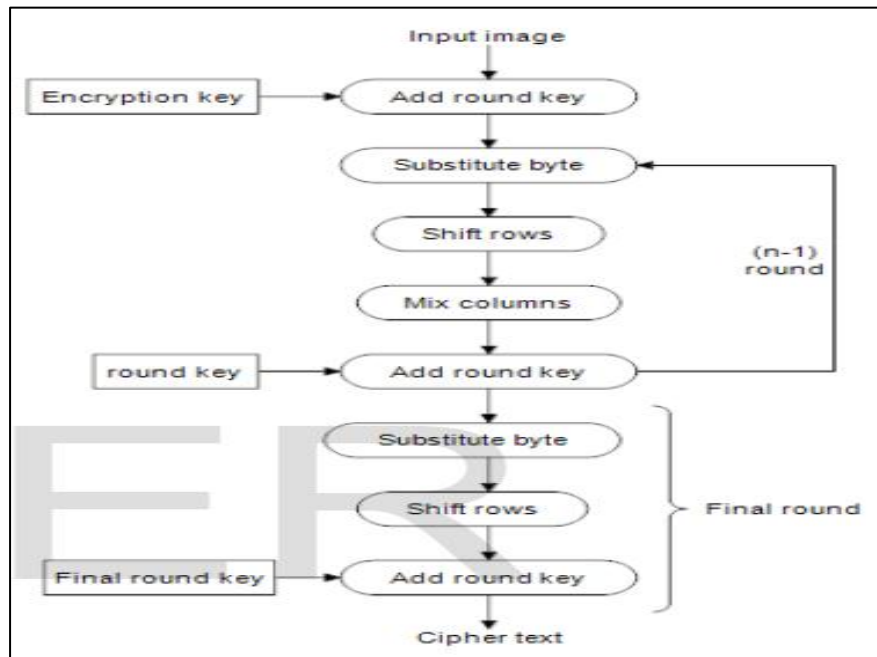


Figure 23: L'algorithme proposé pour le Cryptage AES. [26]

6.1.5.L'algorithme de décryptage

Le processus de décryptage AES est le processus inverse de celui du processus de cryptage. La figure 24 ci-dessus montre le flux de l'algorithme de décryptage AES. Composé de texte chiffré comme entrée, la clé est la même pour le processus de déchiffrement que pour le chiffrement. En cas de déchiffrement, l'octet de substitution inverse, les lignes de décalage inverses et les colonnes de mélange inverses doivent être implémentés. Alors que la touche d'ajout de rond reste la même.[26]

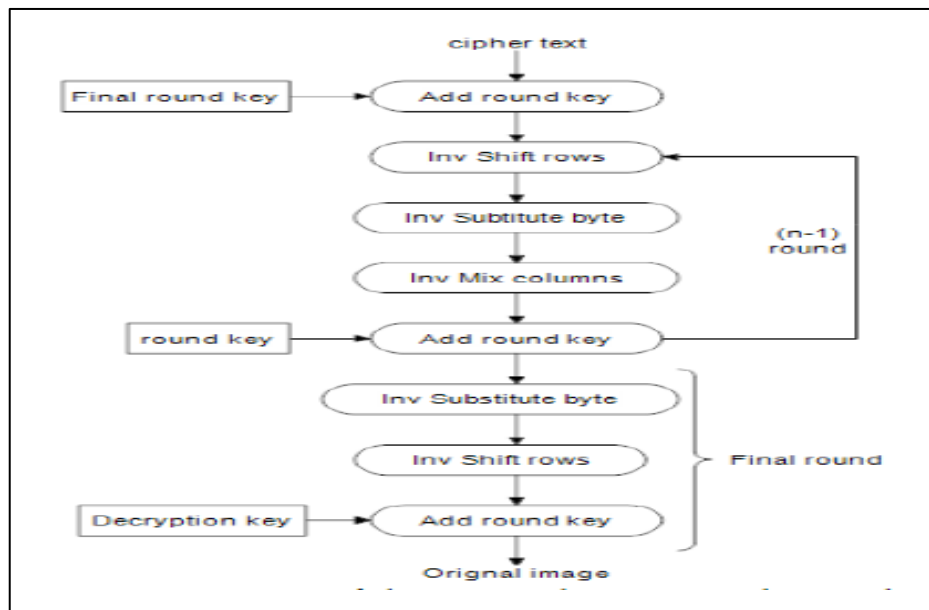


Figure 24: L'algorithme proposé pour le Décryptage AES.[26]

7.L'algorithme proposé pour la compression

Les étapes de l'algorithme sont les suivantes.

Etape01: Lire l'image couleur.

Etape02: Convertissez l'image couleur en image en niveaux de gris.

Etape03: Appliquer la DWT.

Etape04: Appliquez la décomposition quadtree sur l'image résultante après le redimensionner du seuil est de 0.2, minimum La dimension minimale et la dimension maximale sont respectivement 2 et 64.

Etape05: Enregistrez les valeurs des coordonnées x et y, la valeur moyenne et la taille du bloc de Quadtree Décomposition.

Etape06: Enregistrez les informations du DWT pour terminer le codage de l'image à l'aide du codage Huffman et calculer le taux de compression.

Etape07: Pour l'image codée, on applique le décodage Huffman et IDWT pour reconstruire l'image et calculer le MSE et PSNR.

7.1. Le codage de Huffman

L'algorithme de codage Huffman commence par construire une liste de tous les symboles de l'alphabet dans ordre décroissant de leurs probabilités.

Il construit ensuite, de bas en haut, un arbre binaire avec un symbole à chaque feuille. Cela se fait par étapes, où à chaque étape deux symboles avec le plus petit les probabilités sont sélectionnées, ajoutées en haut de l'arborescence partielle, supprimées de la liste et remplacées avec un symbole auxiliaire représentant les deux symboles originaux. Lorsque la liste est réduite à un seul symbole auxiliaire (représentant tout l'alphabet), l'arbre est complet. L'arbre est alors traversé pour déterminer les mots de code des symboles.[22]

7.2. Décodage Huffman

Avant de commencer la compression d'un fichier de données, l'encodeur doit déterminer les codes. Il fait ça sur la base des probabilités de fréquences d'occurrence des symboles. Les probabilités ou les fréquences doivent être écrites, comme information latérale, sur la sortie, de sorte que tout décodeur Huffman pourra décompresser les données. C'est facile, car les fréquences sont des nombres entiers et les probabilités peuvent être écrites sous forme d'entiers mis à l'échelle.

Il ajoute normalement quelques centaines d'octets à la production. Il est également possible d'écrire les codes de longueur variable eux-mêmes sur la sortie, mais cela peut être maladroit, car les codes ont des tailles différentes. Il est également possible d'écrire l'arbre Huffman sur la sortie, mais cela peut nécessiter plus d'espace que les seules fréquences. Dans tous les cas, le décodeur doit savoir ce qui se trouve au début du fichier compressé, le lire et construire le Huffman arbre pour l'alphabet. Ce n'est qu'alors qu'il peut lire et décoder le reste de son entrée.

L'algorithme pour le décodage est simple. Commencez à la racine et lisez le premier bit de l'entrée (le fichier compressé). Si c'est zéro, suivez le bord inférieur de l'arbre; s'il en est un, suivez le bord supérieur. Lisez le bit suivant et déplacez un autre bord vers les feuilles de l'arbre. Lorsque le décodeur arrive sur une feuille, il y trouve le symbole original, non compressé, et ce code est émis par le décodeur. Le processus commence à nouveau à la racine avec le bit suivant.[22]

8. Les travaux similaires

En 2003,[27] Mohammed Salim.B et al. Présente un schéma efficace de crypto_compression destiné aux images médicales dans le quelle ont développent une nouvelle approche concernant l'intégration du cryptage à l'intérieur des algorithme de compression basés sur la DCT.

En 2004,[28] S.Ftérich et C.Ben Amar. Proposent une nouvelle approche hybride de crypto_compression qui applique un cryptage à base de l'algorithme AES sur les paramètres de la compression par la technique de Quadtree optimisée.

En 2009 ,[29] CHAOUCH.M, propose un schéma efficace de crypto_compression. Une nouvelle approche concernant l'intégration du cryptage RSA dans un processus de compression JPEG 2000.

En 2015,[30] AMRANE.M, propose une approche hybride de crypto_compression, qui repose sur une association d'algorithmes de cryptage tel que l'algorithme DES et L'algorithme AES avec des algorithmes de compression DCT.

En 2018,[31] Hajjaji et al, proposent un nouvel algorithme de crypto-compression d'images médicales basé sur les réseaux de neurones artificiels (RNA) et le système chaotique. L'objectif principal de cet algorithme est d'améliorer la sécurité des images médicales et de préserver les informations qu'elles contiennent. Les auteurs proposent de compresser l'image à l'aide des réseaux de neurones artificiels. Ensuite, les cartes d'Arnold ont été utilisées pour mélanger la matrice de poids et enfin, les cartes chaotique linéaire par morceaux sont utilisées pour modifier la valeur de la couche cachée du réseau. L'algorithme proposé a été appliqué sur des images médicales, de différents types, comme l'IRM, les images échographiques et radiographiques. Les résultats expérimentaux, confirment les performances et l'efficacité de l'algorithme proposé en termes de sécurité et de qualité des images non compressées.

En 2019, [32] Mr. Iyad présente une approche qui combine une excellente compression, nommée SPIHT (Set Partitioning in Hierarchic Tree), avec un chiffrement sélectif intégré dans le cycle du processus de compression. L'approche est adaptée et capable d'être utilisée dans les WMSN et de limiter les ressources de ces appareils. Les résultats obtenus, prouvent la haute performance, l'approche proposée avec un surcoût inférieur à 0, 2914% et un débit de transfert constant.

En 2020, [33] RODRIGUES et al. Ont proposé une nouvelle méthode de compression-cryptage d'images 2D dont la qualité est démontrée par une reconstruction précise d'images 2D à des taux de compression plus élevés. La méthode est basée sur la transformation d'ondelettes discrète DWT où des sous-bandes haute fréquence sont connectées avec un nouvel algorithme de crypto_compression Hexadata au stade de la compression et un nouvel algorithme de recherche à correspondance rapide au stade du décodage.

Les méthodes de crypto compression se multiplient du point de vue de la nécessité de ce type de systèmes pour optimiser et sécuriser le transfert des informations via les réseaux de télécommunication. Nous avons pu voir quelques systèmes (les plus récents) parmi tous ceux qui existent pour prendre idée sur la forme que prendra notre système de crypto_compression.

9.Système de Crypto_Compression proposé

L'idée primordiale est de réaliser un système combinant la compression (DWT-Huffman) et le cryptage AES. On va essayer d'appliquer les deux techniques de compression et de cryptage dans un ordre où le cryptage sera en premier lieu, suivi de la compression et la décompression et enfin le décryptage. Donc l'architecture du système va être comme la figure 25 le montre :

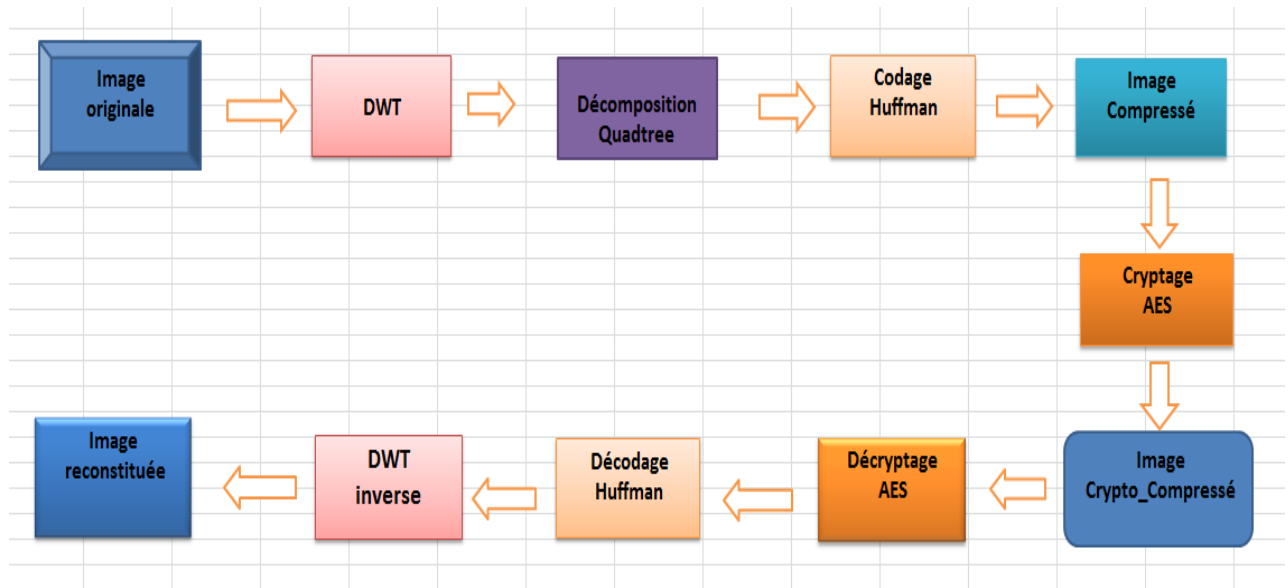


Figure 25: Système de Crypto-Compression proposé .

Conclusion

Dans ce chapitre, nous avons commencé par une présentation détaillée sur la compression par ondelettes avec l'attribution de l'étude sur la transformée en ondelettes discrètes (DWT) et la plus simple ondelette que nous prendrons en compte dans notre système (Ondelette Haar), la décomposition Quadtree. Ensuite, nous avons présenté l'approche de cryptage AES et les travaux similaires.

Enfin, on a terminé avec la présentation du système de crypto-compression proposé.

L'implémentation de l'algorithme du système proposé sera présentée dans le chapitre suivant avec comparaison des différents résultats.

CHAPITRE 03

RESULTAT ET DISCUSSION

Chapitre 3

Résultat et discussion

Introduction

Pour la réalisation de l'interface d'analyse, deux solutions s'offraient :

- Utilisation d'un langage de programmation qui offre une richesse graphique conséquente.
- Utilisation d'un langage dédié au calcul scientifique et qui offre une interprétation évoluée.

Cette ouverture permet d'ajouter une fonction à la même, qui est assemblé sous la forme d'une boîte à outils, étendant le champ d'action à des domaines tels que le contrôle, l'optimisation, le traitement de l'image, et, bien sûr, le traitement du signal.

Nous avons opté pour la deuxième option, qui contient des programmes comme Mathematica, Maple, Mathcad et Matlab. Nous avons finalement opté pour MATLAB parce qu'il répond à toutes nos exigences logicielles.

1. Environnement de travail

1.1. Matériels utilisés

L'implémentation de notre application « APP » a été réalisée sur un micro-portable fonctionnant sous le système d'exploitation Microsoft Windows 7 Edition Intégrale dont les performances sont les suivantes :

- Processeur : Intel core (TM) i3-7020U CPU 2.30Ghz.
- Fréquence de 2.30 GHz.
- Mémoire installé (RAM) : RAM de 4 Go.
- Type de système : système d'exploitation 32 bits, processeur x32.

1.2. Langage de programmation

MATLAB

Matlab est un logiciel de manipulation et de programmation de données numériques qui est principalement utilisé dans le domaine des sciences appliquées. Son but, en comparaison avec d'autres langues, est de rendre la transcription d'un problème mathématique en code informatique aussi simple que possible, en employant un style d'écriture qui est aussi proche du langage scientifique naturel que possible. Le logiciel est compatible avec Windows et Linux. Son interface de manipulation IHM tire parti des ressources de l'en-tête multi-standards. Son apprentissage nécessite seulement une

compréhension de base de quelques principes de base, à partir de laquelle l'utilisation de fonctionnalités avancées est assez intuitive grâce au guidage intégré.

Dans notre travail proposé on va créer une interface graphique. Qu'est-ce qu'une interface graphique ?

Les interfaces graphiques (ou interfaces homme-machine) sont appelées GUI (pour Graphical User Interface) sous MATLAB. Elles permettent à l'utilisateur d'interagir avec un programme informatique, grâce à différents objets graphiques (boutons, menus, cases à cocher...). Ces objets sont généralement actionnés à l'aide de la souris ou du clavier. Malgré le fait que les interfaces graphiques semblent secondaires par rapport au développement du cœur d'une application, elles doivent néanmoins être conçues et développées avec soin et rigueur. Leur efficacité et leur ergonomie sont essentielles dans l'acceptation et l'utilisation de ces outils par les utilisateurs finaux.

Une bonne conception et un développement maîtrisé permettent également d'en assurer une meilleure maintenabilité. [23]

Depuis la version 5.0 (1997), MATLAB possède un outil dédié à la création des interfaces graphiques appelé GUIDE (pour Graphical User Interface Développement Environnement). Le GUIDE est un constructeur d'interface graphique qui regroupe tous les outils dont le programmeur a besoin pour créer une interface graphique de façon intuitive.

2. Aperçu du logiciel réalisé

Le logiciel que nous avons construit est simple à utiliser : il n'y a pas de mots-clés à retenir ou de programmes à écrire, et l'utilisateur est constamment guidé en cliquant sur les boutons qui correspondent à nos préférences.

2.1 Hiérarchie

Notre interface présente une structure arborescente qui offre à l'utilisateur un bon suivi des applications effectuées et une meilleure représentation de ses données. Toutes les applications sont utilisées automatiquement à la fin de chaque session, la figure 26 illustre l'organigramme du système.

L'application « APP », développée sous environnement MATLAB, consacre la première partie à la compression et le chiffrement des images suivant l'algorithme hybride basé sur la décomposition Quadtree et le codage Huffman, et pour le chiffrement, nous appliquerons l'algorithme d'AES.

En deuxième partie, nous faisons le déchiffrement et la décompression, pour bien valider la qualité de l'image reconstruite on calcul les paramètres de la distorsion à savoir le PSNR et MSE.

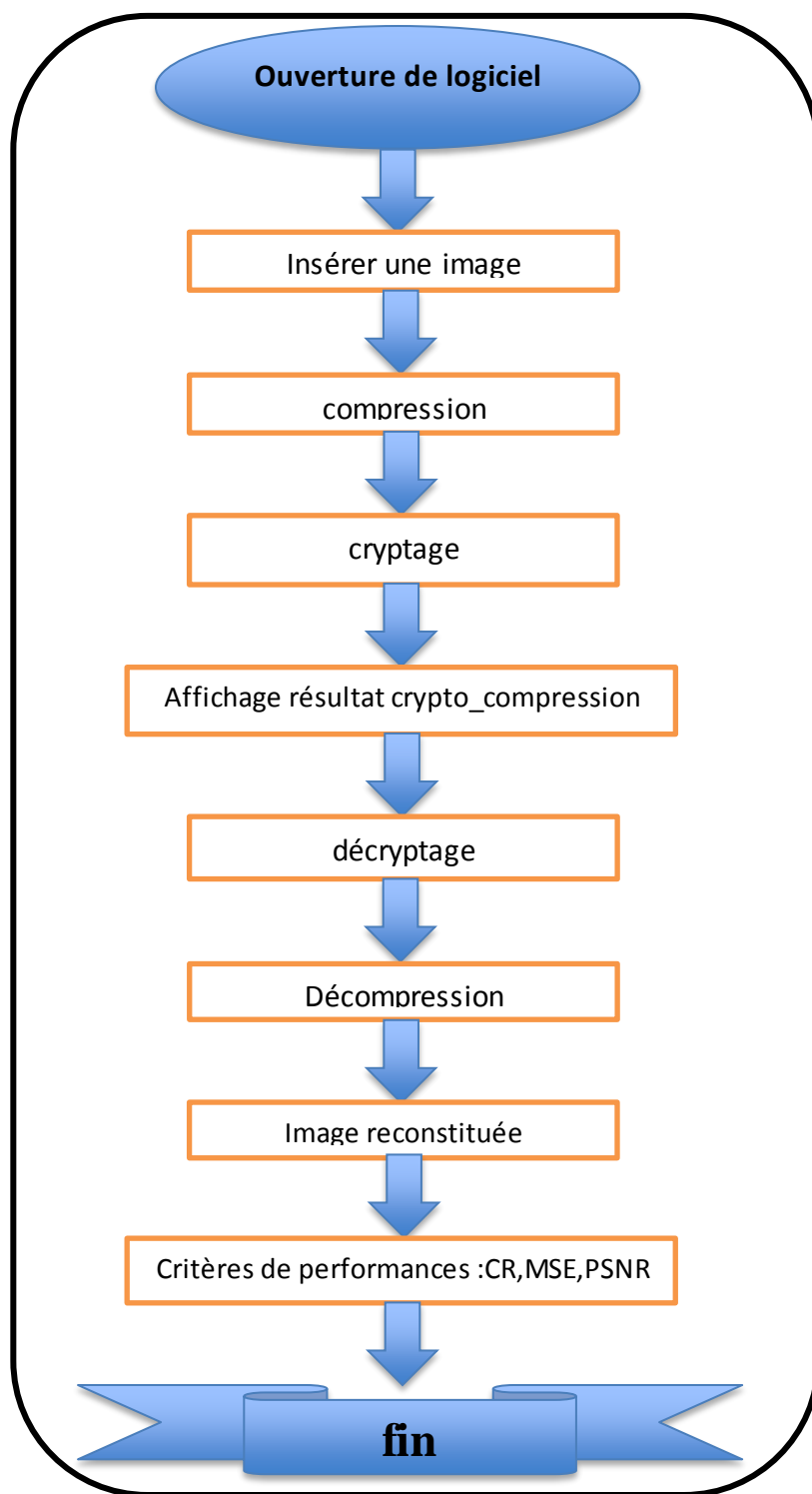


Figure 26: Organigramme du système.

3.Principe de fonctionnement de l’application

La figure ci-dessous présente l’interface de l’application qui s’intitule « Système Crypto Compression d’image ».

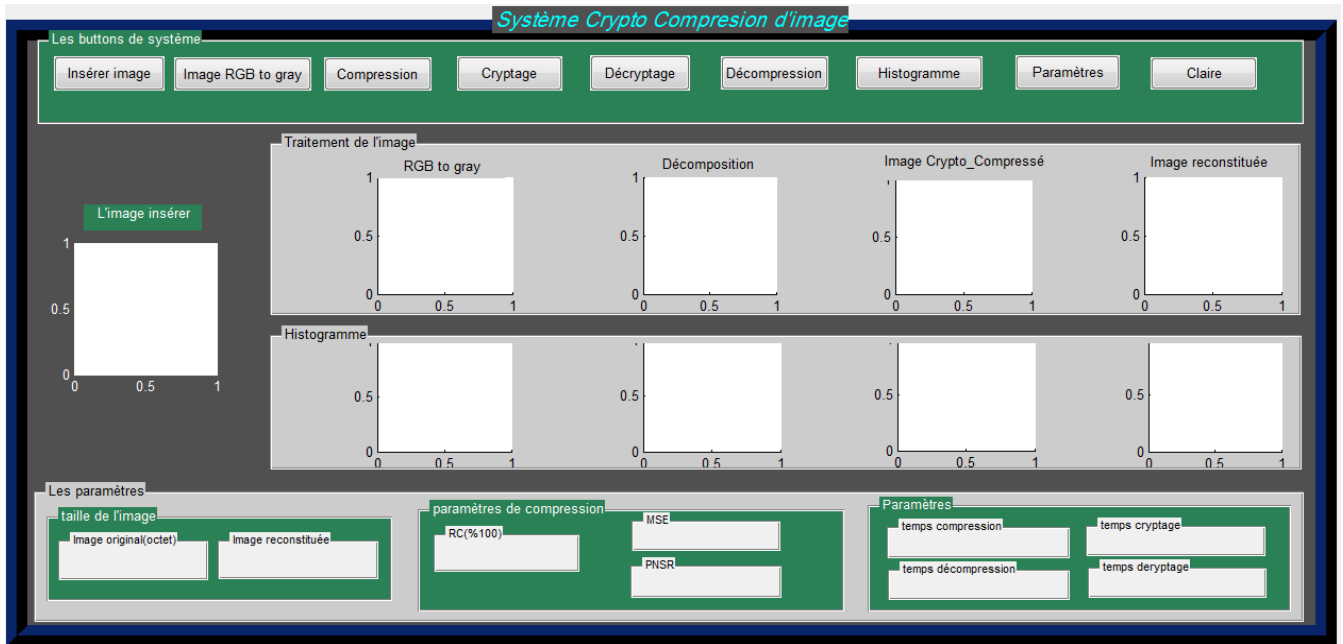


Figure27: Interface du système.

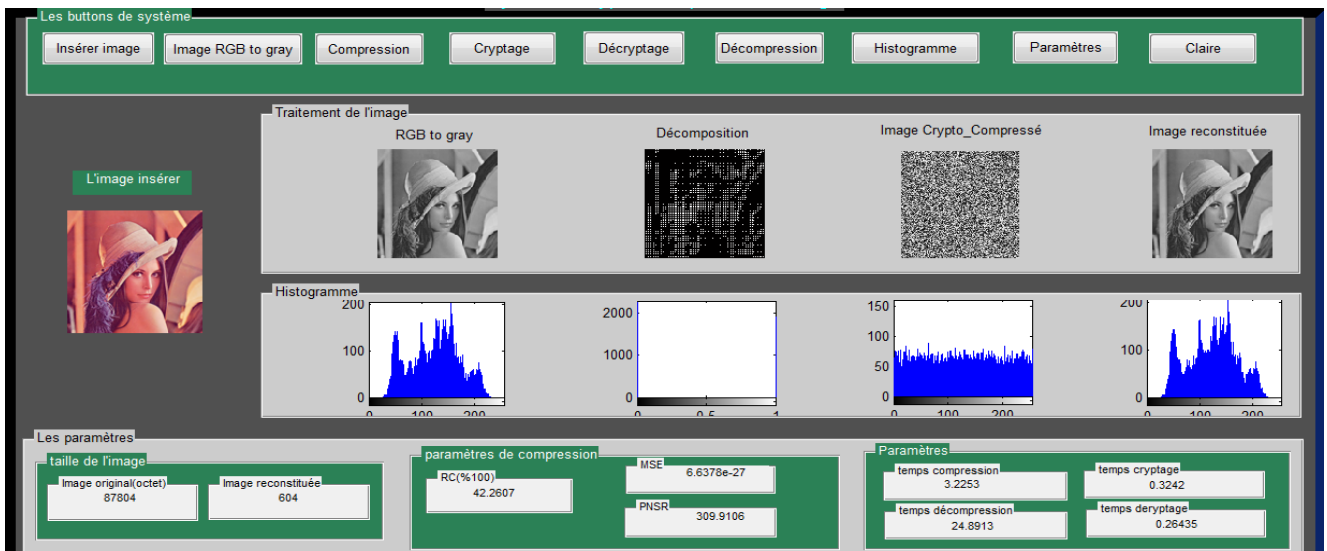


Figure28: Principe de fonctionnement de l’application.

3.1. Description des modules du système

1. Module "Insérer image" : Permet de charger une image à partir de n'importe qu'elle endroit du PC.
2. Module de "Image RGB to gray" : Permet de changer la couleur de l'image de RGB au gris.
3. Module "Compression" : Ce module est le plus important dans notre système; il contient l'algorithme hybride «décomposition Quadtree, et le codage de Huffman», il permet de faire la compression DWT de l'image originale, l'algorithme est réalisé on Matlab pour coder et décoder les images «La valeur de Threshold est 0.2, maximum dimension est 64 et minimum dimension est 2 pour la décomposition Quadtree.
4. Module "Cryptage" : Ce module permet de crypter une image par le système de chiffrement AES,. La clé utilisée est la même clé pour le module de décryptage.
5. Module "Décryptage" : Ce module permet de décrypter l'image crypté. L'entrée de ce module est la sortie du module précédent.
6. Module "Décompression" : Il permet de décompresser l'image et afficher l'image reconstruite. Ce module c'est la dernière étape dans notre système de Crypto-Compression, d'autre façon c'est la sortie de notre système qui donne l'image reconstruite.
7. Module de "Histogramme" : Ce module permet de calculer l'histogramme de chaque étape du processus de crypto-compression.
8. Module "Paramètres" : Ce module est très important pour tester les performances de l'algorithme utilisé, en se basant sur trois paramètres, l'erreur quadratique

moyenne (Mean Square Error, MSE), le rapport crête signal sur bruit (Peak Signal to Noise Ratio, PSNR), et l'entropie.

9. Module de "Clair": Ce module permet de supprimer toutes les champs dans l'interface .

4. Bibliothèque d'images









Bibliothèque des images			
<p>Nom : Lena Taille Physique : 18.5 ko Dimension : 128 X 128 Type de fichier : BMP Type de fichier après transformation : JP2</p>		<p>Nom : Airplane Taille Physique : 27.7 ko Dimension : 128 X 128 Type de fichier : BMP Type de fichier après transformation : JP2</p>	
<p>Nom : Cameraman Taille Physique : 3.55 ko Dimension : 128 X 128 Type de fichier : BMP Type de fichier après transformation : JP2</p>		<p>Nom : Cablecar Taille Physique : 20.3 ko Dimension : 128 X 128 Type de fichier : BMP Type de fichier après transformation : JP2</p>	
<p>Nom : Barbara Taille Physique : 9.29 ko Dimension : 128 X 128 Type de fichier : BMP Type de fichier après transformation : JP2</p>		<p>Nom : Pepperc Taille Physique : 22 ko Dimension : 128 X 128 Type de fichier : BMP Type de fichier après transformation : JP2</p>	
<p>Nom : BoatsColor Taille Physique : 18.5 ko Dimension : 128 X 128 Type de fichier : BMP Type de fichier après transformation : JP2</p>		<p>Nom : Venus Taille Physique : 25.8 ko Dimension : 128 X 128 Type de fichier : JPG Type de fichier après transformation : JP2</p>	

Tableau 2: Bibliothèques des images utilisés.

5. Tests expérimentaux

Nous présentons dans ce qui suit, les résultats issus de notre application, sur chacune des images abordées :

5.1. Résultats

En première partie, nous allons tenter la compression de nos images, ensuite nous appliquons le cryptage et décryptage de ces images et enfin la décompression (comme le montre la Figure29), en discutant sur les paramètres de performances de cette dernière, parmi ses paramètres : MSE, PSNR, le taux de compression, le temps de cryptage et décryptage et le temps de compression décompression. Le Tableau 03 présente les résultats obtenus.

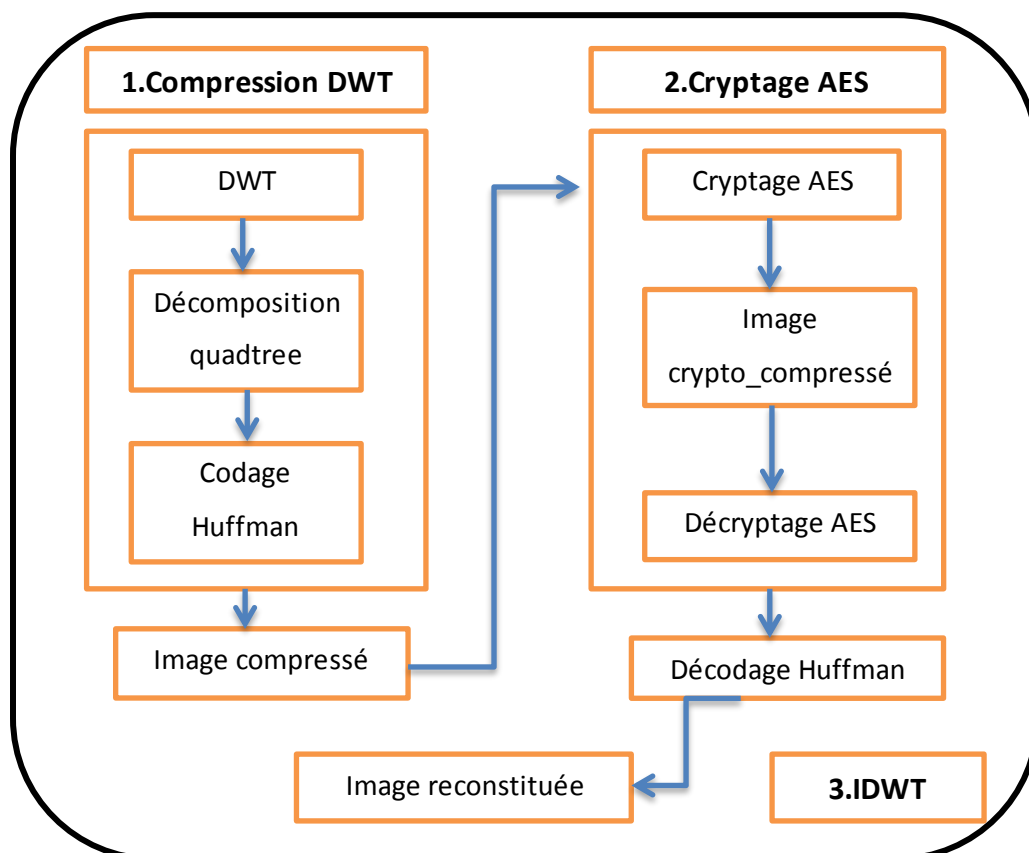


Figure29 : Schéma synoptique de notre système.

5.1.1 Tests et résultats

Les images de la collection étudiée, sont compressées avec la compression DWT suivant l'algorithme hybride Décomposition Quadtree -Codage Huffman, et chiffré suivant l'algorithme AES -128 CBC(Cipher Block Chaining).

5.1.1.1. Premier cas

Notre système applique la compression comme une première étape, ensuite le cryptage et le décryptage et enfin la décompression, alors c'est notre premier test, et voilà le Tableau 03 qui présente les résultats obtenus.

L'image		test		Paramètres						
Nom	Dimensions	Type		CR%	MSE (Err)	PSNR (db)	Tcom (s)	Tdecom (s)	Tcry (s)	Tdecry (s)
Taille Orig	Taille Rec									
Lena 18.5 Ko	128*128	Bmp	01	1.04	6.63	49.70	2.94	24.74	0.2101	0.2739
Airplane 17.8 Ko 1.09 Ko	128*128	Bmp	02	1.13	1.23	51.81	3.89	23.49	0.2387	0.2825
Baboon 27.7 Ko 246 O	128*128	Bmp	03	1.06	4.40	41.34	2.54	24.29	0.2180	0.2791
Barbara 9.29 Ko 246 O	128*128	Bmp	04	1.04	5.53	48.34	2.75	25.00	0.2965	0.2758
BoatsColor 18.5 Ko 7.90 Ko	128*128	Bmp	05	1.06	6.81	50.29	2.86	24.57	0.2328	0.2835

Cablecar 20.3 Ko 1.86 Ko	128*128	Bmp	06	1.05	7.33	48.70	2.84	24.64	0.2304	0.2774
Cameraman 9.18 Ko 246 O	128*128	Bmp	07	1.11	1.15	53.08	3.68	23.93	0.2210	0.267
Pepperc 22 Ko 11.8 Ko	128*128	Bmp	08	1.02	6.37	49.01	2.90	25.45	0.2268	0.2631
Venus 25.8 Ko 4.82 Ko	128*128	JPG	09	1.18	3.71	45.67	2.23	21.45	0.2227	0.2776

Tableau 3: Résultat d'application de notre système sur différentes images cas1.

5.1.1.2. Processus de traitement et Histogramme

- Test 01 : Lena.jpg :

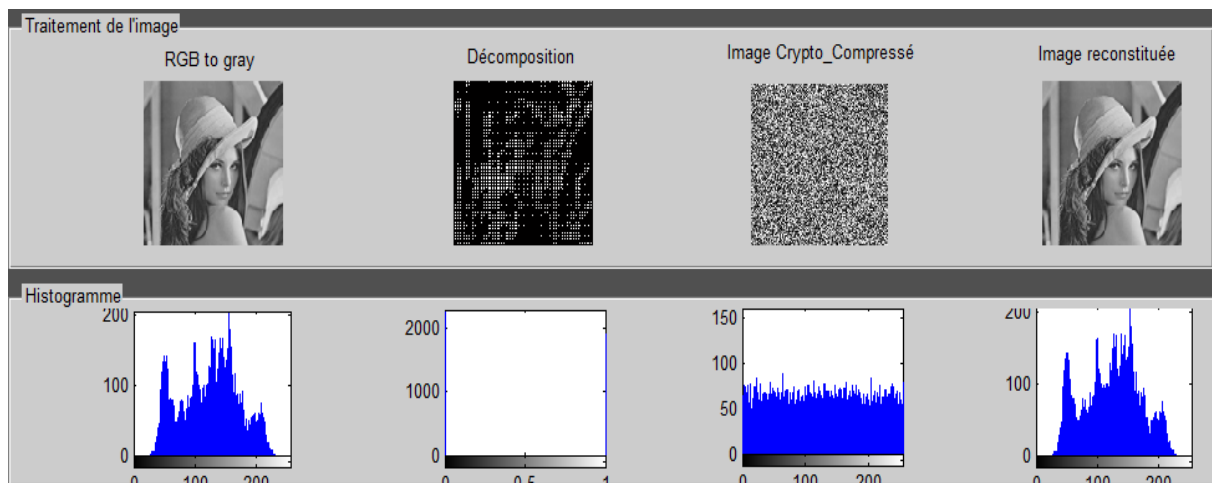


Figure 30 : Processus de traitement et l'histogramme Lena.jpg.

- **Test 02 : Airplane.bmp :**

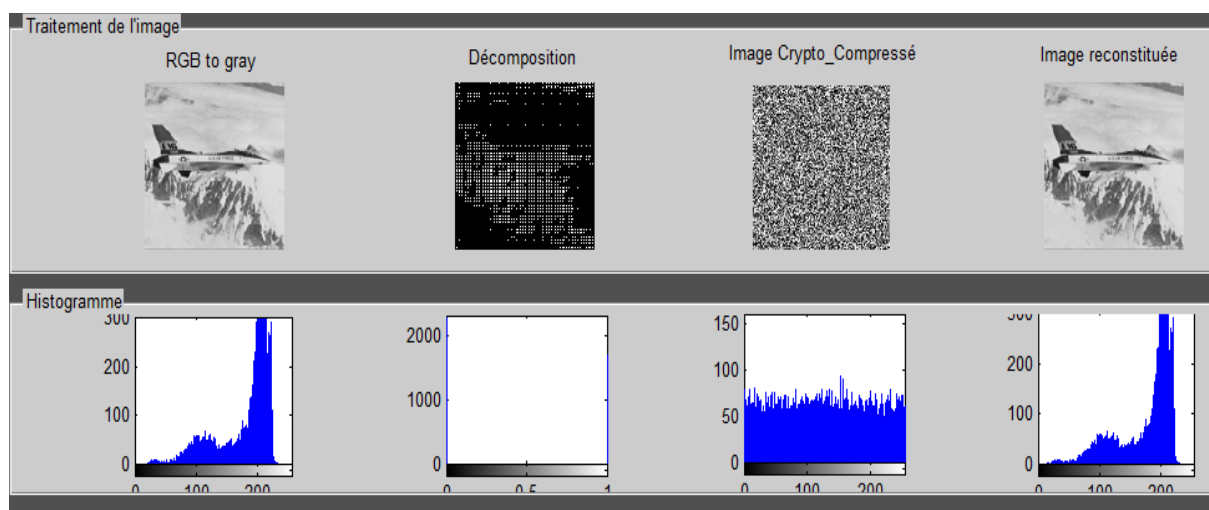


Figure31 : Processus de traitement et l'histogramme Airplane.bmp.

- **Test 03 : baboon.bmp :**

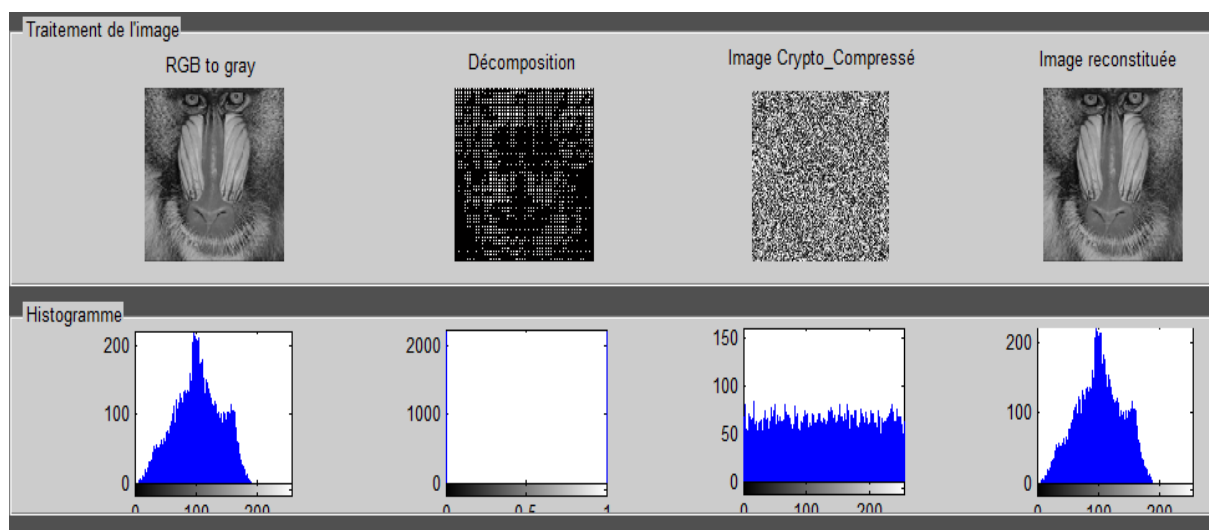


Figure32 : Processus de traitement et l'histogramme Baboon.bmp.

5.1.1.3. Deuxième cas

Nous essayons de changer l'ordre d'application des étapes de notre système, c'est-à-dire que nous appliquons le chiffrement dans le premier cas, puis appliquons la compression et la décompression et enfin déchiffons les mêmes images utilisées dans le premier cas.

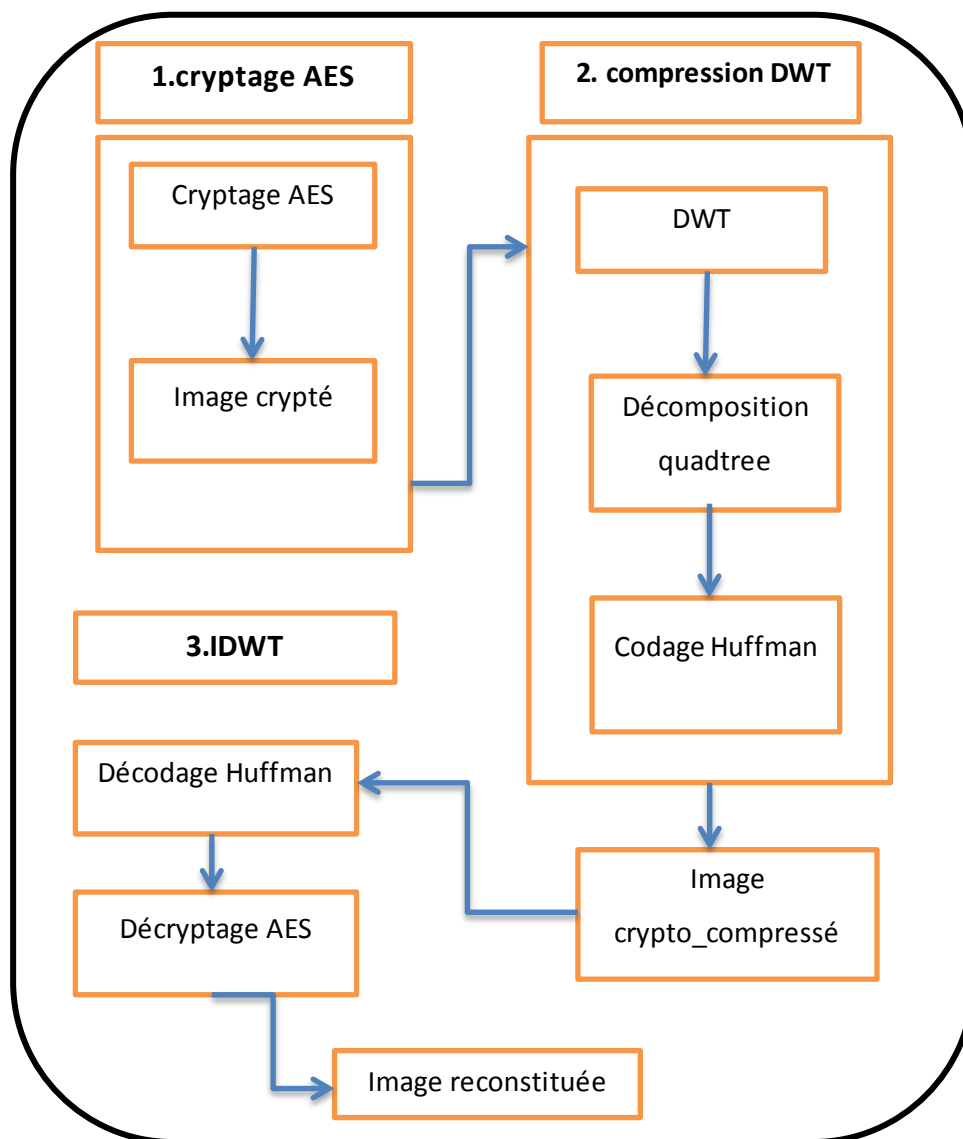


Figure33 : Schéma synoptique du système deuxième cas.

L'exécution d'enchaînement des étapes dans ce cas se fait parfaitement sans aucune erreur d'exécution.

L'image		test		Paramètres						
Nom	Dimensions	Type		CR%	MSE (Err)	PSNR (db)	Tcom (s)	Tdecom (s)	Tcry (s)	Tdecry (s)
Taille Orig	Taille Rec									
Lena 18.5 Ko 604 O	128*128	Bmp	01	0.96	399.35	22.11	3.14	28.21	0.2101	0.2739
Airplane 17.8 Ko 1.09 Ko	128*128	Bmp	02	0.97	405.70	22.04	4.89	26.49	0.2387	0.2825
Baboon 27.7 Ko 246 O	128*128	Bmp	03	0.95	375.55	22.38	3.54	27.29	0.2180	0.2791
Barbara 9.29 Ko 246 O	128*128	Bmp	04	0.97	402.75	22.08	3.75	24.50	0.2965	0.2758
BoatsColor 18.5 Ko 7.90 Ko	128*128	Bmp	05	0.96	406.33	22.04	3.86	27.57	0.2328	0.2835
Cablecar 20.3 Ko 1.86 Ko	128*128	Bmp	06	0.98	380.51	22.32	3.84	28.64	0.2304	0.2774
Cameraman 9.18 Ko 246 O	128*128	Bmp	07	0.95	376.36	22.37	4.68	26.93	0.2210	0.267
Pepperc 22 Ko 11.8 Ko	128*128	Bmp	08	0.96	397.67	22.13	4.90	25.45	0.2268	0.2631
Venus 25.8 Ko 4.82 Ko	128*128	JPG	09	0.97	398.64	22.12	3.23	26.45	0.2227	0.2776

Tableau 4: Résultat d'application de notre système sur différentes images cas2.

6. Interprétation des résultats

- Comme on a vu dans le premier chapitre, pour mesurer la distorsion entre l'image reconstruite et l'image originale (Mesure de la qualité visuelle de l'image reconstruite) on va utiliser l'Erreur Quadratique Moyenne MSE (Mean Square Error) ou du rapport signal à bruit PSNR (Peak Signal to Noise Ratio). Dans le Tableau 03, les valeurs des PNSR dans l'intervalle [41,53] sont un peu élevés. Et MSE dans l'intervalle [01,07] ceci explique la fidélité du DWT.
- On remarque que les valeurs de PSNR sont des nombres considérables dans notre système de Crypto-Compression que l'approche appliquée pour les images avec un taux d'erreur important, ce qui nous prouve que notre système fonctionne parfaitement avec une perte d'information.
- L'histogramme d'une image mesure la distribution des niveaux de gris dans l'image. Pour un niveau de gris x , l'histogramme permet de connaître la probabilité de tomber sur un pixel de valeur x en tirant un pixel au hasard dans l'image.
- dans un deuxième cas nous allons chiffrer les images par le système de cryptage AES et voir l'effet de chiffrement sur la compression. Dans ce cas le déroulement du système il est parfait, il n'y a pas de bruit sur l'image reconstituée comme ce que nous avons vu dans les autres systèmes.

6.1. Discussion

6.1.1. Premier cas

D'après les résultats présentés dans les autres travaux, on remarque bien que le chiffrement AES agit sur la robustesse des techniques de compressions et agit sur la reconstruction de l'image comme on a vu, dans ce cas de notre système il y a une grande dégradation dans la taille d'image cela n'a pas affecté sa qualité, ce qui nous fait dire que la compression par ondelettes (DWT) très forte par rapport aux autres techniques de compression.

6.1.2. Deuxième cas

D'après les résultats obtenus le chiffrement AES a agi sur la compression, MSE (l'erreur quadratique moyenne) augmente et PSNR diminue ce qui veut dire la fidélité de la compression par ondelettes, et la reconstitution elle est fidèle.

Conclusion

Dans la première partie de ce chapitre, nous avons présenté l'environnement de travail et le langage de programmation que nous avons utilisé, ainsi que des captures d'écrans de notre système de crypto-compression et ces modules.

Nous avons testé plusieurs images à l'entrée de notre système, et nous avons enregistré les résultats.

Dernièrement on a discuté les résultats obtenus, et d'après les résultats présentés, on remarque bien que le chiffrement AES agit sur la robustesse des techniques compressions ainsi sur la reconstruction de l'image.

CONCLUSION GENERALE

Conclusion générale

En raison de l'avancement des réseaux de télécommunications, la compression des données devrait jouer un rôle encore plus important. Son importance découle principalement de l'écart entre les capacités physiques des appareils que nous utilisons et les besoins exprimés par les applications. En outre, la cryptographie est utilisée pour protéger les données envoyées dans cet échange croissant de données. Nous avons créé une technique de compression et de sécurité des images dans ce mémoire pour faciliter l'archivage des images et assurer la confidentialité des images.

Dans ce mémoire de Master on s'est intéressé à la combinaison de ces deux techniques, à savoir l'objectif principale est de mettre en oeuvre un nouveau crypto système basé sur une compression avec perte DWT et un algorithme de cryptage AES fondé sur la méthode de chiffrement par blocs (Block Cipher).

D'après les résultats obtenus, on a pu constater que l'ordre de combinaison dans le système proposé n'est pas obligatoire soit nous appliquons le cryptage avant la compression ou le contraire.

On a essayé d'inverser la compression et le cryptage, heureusement, ça marché, contrairement à d'autres systèmes précédemment utilisés.

Ici, nous démontrons la puissance de la compression par ondelettes, qui est un sujet qui mérite d'être travaillé et appliqué dans notre domaine de spécialisation.

Bibliographie

[1]: <http://dspace.univ-tlemcen.dz/bitstream/112/1076/5/chapitre1.pdf>.

[2]: Introduction to cryptography, Johannes Buchmann, 2000.

[3]: S. TAG, Écrivain, Support de Cours de 1er Année Master Sécurité Informatique. [Performance]. 2018-Octobre.

[4]: A. L. DAHMANE Zouhir, «Implémentation d'un algorithme de cryptage sur un circuit FPGA,» chez mémoire de Master, Mai 2017, pp. 8-12.

[5]: «Guide de Network Associates International BV sur la cryptographie».

[6]: http://igm.univ-mlv.fr/~dr/XPOSE2007/vma_PKI/concepts_de_base.html.

[7]: https://www.researchgate.net/figure/Principe-de-fonctionnement-dun-algorithme-de-cryptage-symetrique-Cryptographie_fig24_277474499.

[8]: <http://dspace.univ-tlemcen.dz/bitstream/112/1046/8/chapitre2.pdf>.

[9]: H. BENZENINE et K. AMARA : ‘‘La cryptographie appliquée sur les fichiers audio (son)’’, Mémoire de Master en Informatique, Université Abou Bakr Belkaid–Tlemcen Faculté des Sciences Département d’Informatique, Option : Système d’Information et de Connaissances (S.I.C) ,2011.

- [10]: S. PIGEON, Contribution à la compression de données, Thèse présentée à la Faculté des arts et sciences en vue de l'obtention du grade Philosophie Doctor en Informatique, Montréal, Canada: Département d'informatique et de recherche opérationnelle, 2001.
- [11]: A. MOURAD, «Crypto compression d'image par cryptage partiel En vue de l'obtention d'un Master II en Réseau et télécommunication,» Université Mouloud Mammeri de Tizi-Ouzou, 2015.
- [12]: Z. ATHMANE, «Ondelettes et techniques de compression d'images numérique,» THESE pour l'obtention du Diplôme de Doctorat en Sciences en Electronique, pp. 5-16, 2012/2013.
- [13]: S. RENARD, «La compression des données,» chez Club Photoshop de Nantes, 14 Octobre 1999.
- [14]: L. DIANE, Rapport de recherche "Cours de traitements d'images" , Centre National de la Recherche Scientifique,, ISRN I3S/RR-2004-05-FR, 22 Janvier 2004.
- [15]: C. TAOUCHE, «Implémentation d'un Environnement Parallèle pour la Compression d'Images à l'aide des Fractales , Memoire Pour l'obtention du diplôme de Magister en Informatique Option Information & Computation,» Université Mentouri Faculté des Sciences de l'Ingénieur Département d'Informatique, Constantine, 2005.
- [16]: M. ALDOSSARI, «Nouvelle méthode optique de compression et de cryptage simultanés des images (fixes/vidéo) pour les systèmes télécommunication,» " HAL" Thèse de Doctorat université de bretagne occidentale , p. 28, 02 Février 2006.

[17]: P. PLUMÉ, «Techniques de compression de données,» Edition EYROLLES et la revue « PC EXPERT », pp. 1-6, Janvier 1995.

[18]: M.Lahdir : "nouvelle approche de compression d'images basé sur les ondelettes et les fractales : application aux images météosat ", Thèse de doctorat en électronique option : télédétection, université mouloud Mammeri, Tizi-Ouzou ,2010.

[19]:KADRI Oussama:"compression d'images fixes par ondelettes géométriques par utilisation des curvelets et différents types d'interplotation dans la quantification scalaire", thèse de Magistère en Electronique, univ Mohammed Khider Biskera,2014.

[20]: <http://nolot.perso.math.cnrs.fr/ProjetL3>.

[21]: ZEDEK.S,"compression d'images hyperspectrales par ondelettes",
du Diplôme d'Ingénieur d'Etat en Electronique,option communication,2010.

[22]: Sukhendu Jana, Soumaya Mandal,"Dwt Based Image Compressing Using Quadtree Decomposition And Huffman Encoding", open access article.

[23]: "Conception et réalisation d'un système hybride pour la compression et la sécurisation des documents", Mémoire Master, Spécialité système de télécommunication .

[24]: https://stringfixer.com/fr/Haar_wavelet.

[25]: S.GUILLEM-LESSARD, "Tutoriel de Cryptographie", 2002.

[26]: P. DESHMUKH, «An image encryption and decryption using AES algorithm,» International Journal of Scientific & Engineering Research, Vols. %1 sur %2Volume 7, Issue 2, n° %1212, pp. 210-213, February-2016.

- [27]: MOHAMMED SALIM BOUHLEL, MOEZ ABDELMOULA, Mourad ELLOUMI, Lotfi Kamoun. Nouveau Schema de crypto_compression des images médicales, LETI(Laboratoire d'electronique et des technologies de l'information). Ecole national d'ingénieurs de Sfax; B.P.W, 3038 Sfax, Tunisie.
- [28] S.FETRICH, C.BEN AMAR. Crypto_compression d'images fixes par la méthode de quadtree optimisée et AES, PEGIM(Groupe de Recherche sur les Machines Intelligentes).
- [29]: CHOUCH. M, Crypto_compression des images d'empreintes digitales, diplôme de MAGISTER, USTHB.
- [30]: AMRANE .M, Crypto_compression d'image par cryptage partiel, diplôme Master02 ,Spécialité réseaux et télécommunication .
- [31] : HAJJAJI, M.A., Dridi, M. & Mtibaa, A. A medical image crypto-compression algorithm based on neural network and PWLCM. *Multimed Tools Appl* 78, 14379–14396 (2019).
- [32] : IYAD M. Hraini, Joint Crypto-Compression Based on Selective Encryption for WMSNs, Thesis submitted in partial fulfillment of the requirements of the degree Master of Science in Informatics, Palestine Polytechnic University.
- [33]: RODRIGUES Marcos and SIDDEQ Mohammed (2019). A Novel Hexadata Encoding Method for 2D Image Crypto-Compression. *Multimedia Tools and Applications*, 79 (9), 6045-6059.