République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Cheikh Larbi Tebessi Tébessi

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

Département : Mathématiques Et Informatique

MEMOIRE

Présenté en vue de l'obtention du diplôme de Master

Filière: informatique

Spécialité : Réseaux et sécurité informatique

Un Système de crypto compression d'images basé sur le Stream Cipher et la compression JPEG

Présenter par :

BRAHMIA Asma

Encadré par :

Dr. MENASSEL Rafik

Devant le jury composé de:

Dr. Abdellatif Sahraoui MCB Président

Dr. Ahmed Zeggari MCB Examinateur

Soutenu le 08 juin 2023

Année universitaire : 2022/2023

REMERCIEMENT

Tout d'abord, je tiens à remercier Allah, De ma donné la santé, la volonté et la patience pour mener à terme ma formation de Master et pouvoir réaliser ce projet.

Je tiens à exprimer mes profonds remerciements et mon immense respect à mon encadreur Docteur MENASSEL Rafik pour la qualité de son encadrement, sa disponibilité, ses hautes qualités morales et scientifiques qui ma fourni le sujet de ce mémoire et ma guidés de ses précieux conseil et suggestions, et la confiance qu'il ma témoignés tout au long de ce travail et qu'il d'avoir dirigé mes travaux de thème et de son soutien durant mon étude et la réalisation de ce projet.

Je tiens à gratifier aussi les membres de jury ''Dr. ZEGGARI Ahmed'' et '' Dr.ABDELLATIF Sahraoui '' d'avoir accepté d'examiner et d'évaluer mon travail.

Enfin, j'adresse également mes sincères sentiments et remerciements à mes amis Abdelaali et Bariza pour m'aider au cours pour l'accomplissement de mon travail du fin d'étude.

Dédicaces

Je dédié ce mémoire à :

A mes chers Parents : qui ont fait tant de sacrifice pour m'aider à avancer dans la vie. Pour les valeurs nobles, l'éducation et le soutien.

A ma tante et ma grande mère : Pour ses précieux conseils, pour toute son assistance dans ma vie, qui n'ont cessé d'être là pour moi des exemples de courage et de générosité.

A toutes mes amies proches

BRAHMIA Asma.

Résumé

Résumé

La compression et le cryptage des données représentent deux technologies dont l'importance est en croissance exponentielle et ce dans une multitude d'applications. De plus, l'utilisation excessive de réseaux informatiques pour le transfert de données doit évidemment obéir à un double objectif : la réduction du volume de données afin d'encombrer le moins possible les réseaux de communication publics et la confidentialité afin d'assurer un niveau optimal de sécurité. D'une part, la compression d'images a pour but de réduire la taille d'une image afin de faciliter son stockage aussi bien que son transfert. Ainsi on distingue deux grandes familles de méthodes compression, à savoir celles qui provoquent des pertes d'information causant une image reconstruite non fidèle à l'originale mais de taille très réduite. Les autres méthodes ne provoquent pas de perte d'information mais présentent des taux de compression réduits. D'autre part, le cryptage des données est généralement décrit à partir d'une communication secrète d'informations entre deux interlocuteurs. Dans un système informatique, cette confidentialité intervient dans plusieurs formes, en particulier dans la protection du stockage, de l'accès et transmission de l'information.

Dans ce travail, nous allons mener, une étude plus détaillée au sujet du système de crypto-compression basé sur une compression avec perte JPEG et un algorithme de chiffrement RC4 basé sur la technique du Stream Cipher ou cryptage par flot.

Mots clés : compression d'images, cryptage, JPEG , Stream Cipher , crypto-compression

Abstract

Data compression and encryption are two technologies whose importance is growing exponentially in a multitude of applications. Additionally, excessive use of computer networks for the transfer of data must obviously obey a double objective: the reduction of the volume of data in order to clutter the public communication networks as little as possible and confidentiality in order to ensure an optimal level of security. On the one hand, image compression aims to reduce the size of an image in order to facilitate its storage as well as its transfer. Thus, there are two main families of methods compression, namely those that cause loss of information causing a reconstructed image not faithful to the original but of very reduced size. Other methods do not cause loss information but have reduced compression rates. On the other hand, data encryption is generally described from a secret communication of information between two interlocutors. In a computer system, this confidentiality comes into play in many forms, particularly in protecting the storage, access and transmission of information.

In this work, we will carry out a more detailed study about the crypto-compression system based on JPEG lossy compression and an RC4 encryption algorithm based on the Stream Cipher technique.

Keywords: image compression, encryption , JPEG, Stream Cipher, crypto-compression.

ملخص

يعد ضغط البيانات و تشفيرها تقنيتين تتزايد أهميتهما بشكل كبير في العديد من التطبيقات.بالإضافة إلى ذلك ,من الواضح أن الاستخدام المفرط لشبكات الكمبيوتر لنقل البيانات يجب أن يخضع لهدف مزدوج : تقليل حجم البيانات من أجل تشفيرشبكات الاتصال العامة بأقل قدر ممكن و السرية من أجل ضمان المستوى الأمثل للأمن.

من ناحية, يهدف ضغط الصور إلى تقليل حجم الصورة من أجل تسهيل تخزينها وكذلك نقلها. وبالتالي فإننا نميز بين عائلتين كبيرتين من طرق الضغط, و هما تلك التي تسبب فقدان المعلومات مما يتسبب في صورة معاد بناؤها ليست وفية للأصل و لكن بحجم صغير جدا.لا تتسبب الطرق الأخرى في فقدان المعلومات و لكنها تخفض معدلات الضغط.

من ناحية أخرى, يتم وصف تشفير البيانات بشكل عام من خلال الاتصال السري للمعلومات بين اثنين من المحاورين في نظام الكمبيوتر, تتدخل هذه السرية بعدة أشكال, لاسيما في حماية تخزين المعلومات والوصول إليها و نقلها.

في هذا العمل, سنقوم بإجراء دراسة أكثر تفصيلا حول نظام ضغط التشفير بناءً على ضغط JPEGالمفقود و خوارزمية تشفير RC4بناءً على تقنية Stream Cipher.

الكلمات الرئيسية:ضغط الصور, التشفير,Stream Cipher, RC4, JPEG.

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

- **ASCII: American Standard Code for Information Exchange**
- **AES : Advanced Encryption Standard**
- **A5/1 : Algorithme de chiffrement par flot**
- **API: Application Programming Interface**
- **APP: Application**
- **BMP: BitMaP**
- **BPP: Bits par pixel**
- **CBC: Cipher Block Chaining**
- **CFB: Cipher Feedback**
- **CPU: Central Processing Unit**
- **CR : Compression Ratio**
- **CWT : Continuous Wavelet Transform**
- **DES : Data Encryption**
- **DB : Le décibel ou (dB)**
- **AC: Alternative Component**
- **DC: Direct Component**
- **DCT: Discret Cosine Transform**
- **DCT I: Discret Cosine Transform I**
- **DCT II: Discret Cosine Transform II**
- **DCT III: Discret Cosine Transform III**
- **DSA: Digital Signature Algorithm**
- **DWT: Discrete Wavelet Transform**
- **ECB: Electronic Code Book**
- **ECC: Elliptic curve cryptography**
- **GSM: Global System for Mobile Communications**
- **GUI: Graphical User Interface**
- **IHM: Interface Homme Machine**
- **IDCT: Inverse discrete cosine transform**
- **IDEA: International Data Encryption Algorithm**
- **ISO: International Organisation for Standardisation**

- **JPG: Joint Photographic Group**
- **JPEG: Joint Photographic Experts Group**
- **JPEG 2000 : Norme de compression d'images commune à l'ISO**
- **KSA: Key Schedule Algorithm**
- **LZW: Lempel-Ziv-Welch**
- **MSE: Mean Square Error**
- **MATLAB: Matrix Laboratory**
- **OFB: Output Feed back**
- **PGP: Pretty Good Privacy**
- **PSNR: Peak Signal to Noise Ratio**
- **PRGA : Pseudo-Random Generation Algorithm**
- **RC4: Rivest Cipher 4**
- **RLE: Run-Length Encoding**
- **RSA: Ronald Rivest, Adi Shamir et Leonard Adleman**
- **RGB : Rouge, vert, bleu, abrégé en RVB ou en RGB**
- **SPIHT: Set partitioning in hierarchical trees**
- **TC : Temps de compression**
- **XOR : eXclusive OR**

INTRODUCTION GENERAL

Introduction général

Les données multimédias sont largement utilisées dans plusieurs domaines grâce au développement rapide des technologies de l'information et de la communication en particulière les images qui sont transférées ou stockées sur les réseaux informatiques donc il est devenu impératif de protéger les images confidentielles contre tout accès non autorisé, ceci impose de disposer des techniques fiables, qu'ils offrent une excellente qualité et sécurité des images. Par conséquent, la compression et le cryptage des images sont deux technologies dont l'importance est considérable en raison de nombreuses applications.

Beaucoup de chercheurs ont créé de nombreuses méthodes de compression de données qui s'inspirent de la théorie de l'information et utilisent de nombreux domaines de la mathématique et de l'informatique.

D'une part, La compression d'image est un sujet de recherche populaire car elle vise à améliorer les algorithmes de compression tout en réduisant la taille des images et en les rendant plus faciles à stocker.

Il existe deux méthodes différentes pour compresser les images : Les méthodes réversibles, c'est-à-dire sans pertes, produisent de faibles taux de compression, celles connues sous le nom d'irréversibles, qui permettent une compression élevée des images, mais entraînent des Distorsions.

D'autre part, Le cryptage des données en général est décrit comme une communication privée d'informations entre deux personnes. Cette confidentialité intervient dans un système informatique sous plusieurs formes, en particulier dans la protection du stockage, de l'accès et transmission de l'information.

L'intégration du cryptage et de la compression a suscité une attention considérable en raison de son potentiel d'amélioration de la sécurité des données tout en minimisant le stockage et de transmission.

Dans ce mémoire, on présente un travail qui consiste à combiner à la fois les deux techniques de sécurité pour les images joignant ainsi le cryptage et la compression dans un seul système (crypto-compression).

Le système proposé est basé sur la compression JPEG et l'algorithme RC4 en utilisant le mode de chiffrement par flot d'un type particulier de représentation de l'information qui est l'image.

Ce système réduit la quantité de calcul nécessaire et conserve le format JPEG et le taux de compression et fourni une solution robuste et efficace pour protéger les données d'image sensibles et garantit l'intégrité, la confidentialité et la compression efficace des images.

Ce mémoire est organisé en trois chapitres structurés comme suit :

Le premier chapitre : présentant l'état de l'art et divisé en deux grandes parties à savoir la cryptographie et la compression :

La première partie introduit la compression et qui contient aussi des notions générales théoriques sur les images, la compression avec 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 pour choisir une méthode de compression Par rapport aux autres suivant les conditions d'usage et enfin en mettant le point sur la compression JPEG nous montrons ça avec des différentes illustrations. La deuxième partie détaille la cryptographie et rappelle les concepts de base en commençant par une définition détaillée suivi par une présentation des méthodes de cryptage parmi les plus utilisées, ensuit nous expliquons les deux types de la cryptographie (classique et moderne), et enfin nous mettons le point sur la cryptographie par flot.

Le deuxième chapitre est consacré à présenter quelques travaux précédentes de crypto-compression d'images ensuite nous présentons une explication plus détaillés des deux techniques utilisées dans notre système, en commençant par la compression JPEG ensuite le cryptage RC4.

A la fin de ce chapitre nous exposons en détails notre approche proposée, qui s'articule sur une méthode de compression avec perte «JPEG» et la méthode de chiffrement par flots « RC4».

Le Troisième chapitre c'est le cœur de ce travail comprenant la partie la plus importante et se il sera consacré l'approche de crypto-compression élaborée dans le cadre de ce travail, il présente l'application MATLAB tout d'abord l'environnement logiciel et matériel utilisé ainsi que l'interface générale de notre application, Ce chapitre contient aussi l'ensemble des tests expérimentaux sur des images réelles et regroupe toutes les études, les simulations et interprétations des résultats obtenues avec une discussion de ces derniers.

Nous terminerons ce mémoire par une conclusion générale, résumant le travail réalisé.

CHAPITRE 01

Notions Générales Sur l'image, La compression, La cryptographie

Introduction

Le développement rapide des systèmes de communication numériques, qui sont largement utilisés pour échanger des informations multimédias (des jeux, des transmissions satellite, du texte, de l'audio, des images, des vidéos, etc.), a accompagné l'augmentation considérable du nombre d'applications informatiques dans les différents domaines de notre vie. Par conséquent, l'édition d'images (enregistrement et publication, etc.), le stockage ou encore la transmission de ces images devient une question stratégique qui se pose.

De ce fait, La protection de ces données est devenue un domaine fascinant pour les chercheurs qui veulent préserver la confidentialité de ces données. Les chercheurs ont développé des méthodes d'analyse de cryptage dédiées à une application précise qui sont simples et efficaces car le volume et la croissance rapide de ces données nécessitent un temps de statistiques et de calcul de plus en plus grand , donc il est nécessaire de ''compresser'' les images ce qui permet de réduire la taille de mémoire occupée par ces image tout en perdant un minimum de qualité.

Ce premier chapitre se compose en deux parties primordiales, la première se concentre sur des

Généralités concernant la Compression d'images on mettre l'accent sur la compression JPEG. Toute en passant par une recherche bibliographique des méthodes de compression d'images, tandis que la deuxième partie se focalise sur les méthodes de cryptage, où on verra en détails la notion de cryptographie mettre l'accent sur le Stream Cipher.

Dans la première partie on s'intéresse en premier lieu sur des notions générales d'images (notion de pixel, définition d'images, types d'images…),tout en passant par les différents systèmes de représentation de couleurs ainsi que les caractéristiques des méthodes de compression, ensuite nous étudierons les différents algorithmes de compression de données des deux familles Avec et Sans perte de données et ce en se focalisant sur la compression JPEG.

Dans la deuxième partie on s'intéresse sur la cryptographie, ses différents types et les propriétés de chaque type, tout en mettant en évidence la cryptographie symétrique précisément le Stream Cipher.

I. Notions d'images et de compression

I.1. Notion de pixel

Représente le plus petit élément constitutif, chaque pixel est représenté sous forme d'un petit carré, et composé de trois points de couleurs (rouge, vert, bleu).

I.2. Définition d'une image

C'est une toute image binaire qui a été créée, acquise, traitée ou stockée.

I.3. Taille des données d'une image

La taille d'une image est calculée en multipliant le nombre total de pixels par le nombre de bits par pixel dans l'image.

$$Taille = C \times L \times M$$

C: est le nombre de colonnes.

L: est le nombre de lignes.

M: est le nombre de bits par pixel.

I.4. Types d'images

Les images de matrice et les images vectorielles sont les deux catégories d'images:

1) **Images matricielles (ou images bitmap) :** Il est composé d'une matrice (table) de points multidimensionnels, dont chacun représente l'une des dimensions suivantes :
   - Spatiale (hauteur, largeur, profondeur).
   - Temporelle (durée).
   - Niveau de résolution.
2) **Images vectorielles:** exprimer les données visuelles en utilisant des règles géométriques compréhensibles mathématiquement. [3]

I.5. Compression

C'est une méthode de réduire le nombre de bits. (le volume de données au niveau de la transmission sans perdre d'informations essentielles, qui permet d'augmenter le volume des données transférées ou par rapport aux données d'origine, le produit comprimé nécessite moins d'espace de stockage et de temps de traitement. [1][2]

I.6. Les caractéristiques des méthodes de compression

- **Taux de compression :** est le ratio de la quantité d'espace économisée après la compression à la totalité de l'espace nécessaire pour les données avant la compression.

- **Entropie :** Il agit comme un baromètre de la qualité de l'information.
- **Mesures de distorsion :** On va utiliser l'Erreur Quadratique Moyenne 1 MSE ou le rapport signal-bruit PSNR 2 pour mesurer la distorsion entre l'image reconstruite et l'image originale.

I.7. Compression physique et logique

I.7.1. La compression physique

Le résultat d'un bloc de données compressées est plus petit que l'original car l'algorithme de compression physique a retiré la redondance.

I.7.2. La compression logique

Est accomplie à travers le processus de substitution logique qui consiste à remplacer un symbole alphabétique, numérique ou binaire en un autre.

I.8. Compression symétrique et asymétrique

I.8.1. La compression symétrique

La compression est dite symétrique lorsque le codeur et le décodeur utilisent le même procédé et le temps d'exécution est égal pour les deux étapes.

I.8.2. La compression asymétrique

Elle demande plus de travail pour l'une des deux opérations, la plupart des algorithmes demande plus de temps de traitement pour la compression que pour la décompression.[6]

I.9. Techniques de compression

I.9.1. Compression sans pertes

'**Techniques réversibles'**, elles ne causent pas de pertes de contenu d'information, et lorsqu'ils sont décompressés, l'image source peut être restaurée à son état d'origine.

- Les principaux algorithmes de compression sans perte sont :
  - Méthode d'Huffman.
  - Méthode arithmétique.
  - L'algorithme LZW.

- Codage par plage.
- Codage par prédiction linéaire.

I.9.2. Compression avec pertes

'Techniques irréversibles', elles causent des pertes de contenu d'information, et lorsqu'ils sont décompressés, l'image source ne peut être pas restaurée à son état d'origine.

- Les principaux algorithmes de compression avec perte sont :
  - Codage prédictif avec pertes.
  - Codage par transformation.
  - La compression Fractales.
  - La Compression par Ondelettes.
  - La compression JPEG. [8]

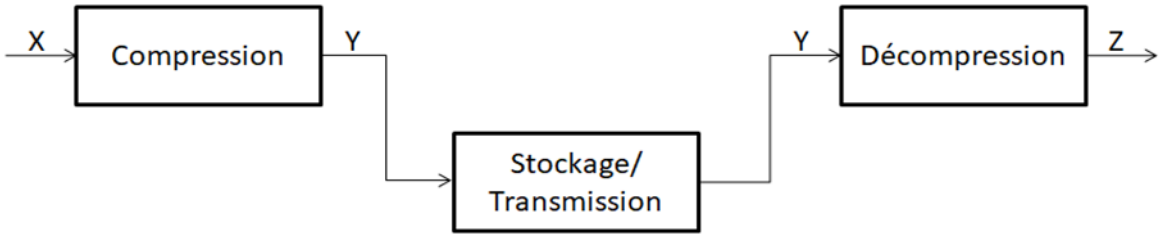


Figure I. 1Principe de compression avec perte [2]

I.10. La Compression JPEG

I.10.1. Théorie des JPEG

JPEG a été développé à la fin des années 1980 dans le but de compresser des images fixes en couleur et à des niveaux de gris pour les stocker sur des supports numériques. Il a été conçu dans le but de couvrir la plus large gamme d'applications tout en tenant compte des limitations pratiques par rapport aux applications les plus visibles.

Afin de fournir un taux de compression beaucoup plus fascinant que d'autres approches, il s'agit de procéder à une dégradation de l'image invisible à l'œil. Par conséquent, cette compression est une compression avec perte car il y a une perte certaine d'informations, mais elle est aussi incroyablement efficace car elle peut réduire la taille d'une image d'environ 90 %. La méthode DCT, la quantification et le codage entropique constituent la base de JPEG. [18] [32] [50]

I.10.2. Définition

JPEG (Joint Photographic Experts Group) est une méthode de compression d'image avec perte largement utilisée pour les images numériques, qui fournit une bonne compression pour une qualité très correcte. La compression JPEG réduit la taille d'une image tout en maintenant la qualité visuelle.

I.10.3. Historique :

- Les normes de ce format ont été établies entre 1978 et 1980.
- La norme JPEG déposée en 1991.
- Elle est adoptée en 1992.
- IBM est considérée comme la propriétaire de ce format, mais Forgent l'a revendiqué en 2006 et Global Patent Holdings en 2007. **[9]**

I.10.4. Avantages de la compression d'images JPEG

Compression efficace : La compression JPEG réduit la taille des images avec une qualité d'image satisfaisante. Cela le rend excellent pour le stockage et la transmission d'images sur les réseaux. Les taux de compression de JPEG peuvent être modifiés pour répondre à diverses exigences.

Large compatibilité : JPEG fonctionne avec presque tous les logiciels d'édition d'images, les navigateurs Web et les systèmes d'exploitation, ce qui le rend compatible avec de nombreuses plateformes et appareils.

Préserve le contenu visuel : la compression JPEG est spécialement conçue pour les images photographiques, où le système visuel humain est moins sensible à certains détails. En supprimant les informations moins visibles, telles que les composants hauts fréquence et les variations de couleur

Encodage progressif : L'encodage progressif permet d'afficher d'abord un aperçu basse résolution de l'image, dont la qualité s'améliore ensuite progressivement au fur et à mesure que davantage de données sont reçues. Cette fonctionnalité améliore l'expérience utilisateur en fournissant un aperçu rapide pendant le chargement de l'image complète.

I.10.5. Inconvénients de la compression d'images JPEG

- **Compression avec perte :**

la compression JPEG est une technique de compres- sion avec perte, ce qui signifie qu'elle supprime certaines informations d'image pendant le processus de compression. Cette perte de données peut entraîner une réduction de la qualité de l'image et l'introduction d'artefacts de compression, tels que l'effet de bloc, le flou et la distorsion des couleurs.

- **Adaptation limitée au texte et aux dessins au trait :**

La compression JPEG est principalement conçue pour les images photographiques avec des tons continus et des scènes naturelles.

Il n'est pas bien adapté à la compression d'images contenant des bords nets, du texte ou des dessins au trait, car ces types d'images ont des limites distinctes et des détails à haute fréquence qui sont sensibles aux arte- facts de compression.

- **Irréversibilité :**

En raison de la nature avec perte de la compression JPEG, l'image décompressée n'est pas identique à l'image d'origine. Les informations supprimées ne peuvent pas être entièrement récupérées, ce qui entraîne une perte de détails et de qualité.

- **Artefacts de compression :**

La compression JPEG peut introduire des artefacts notables, qui incluent le bloc, la sonnerie, le saignement des couleurs et la perte de détails fins. Ces artefacts peuvent devenir plus importants et répréhensibles à mesure que le niveau de compression augmente, ce qui a un impact sur la fidéli- té visuelle de l'image.

- **Vulnérabilité aux cycles de compression multiples :**

La compression et la dé- compression répétées des images JPEG peuvent entraîner une perte cumulative de qualité. Chaque cycle de compression-décompression introduit des artefacts et des pertes supplémentaires, qui peuvent dégrader considérablement l'image au fil du temps.

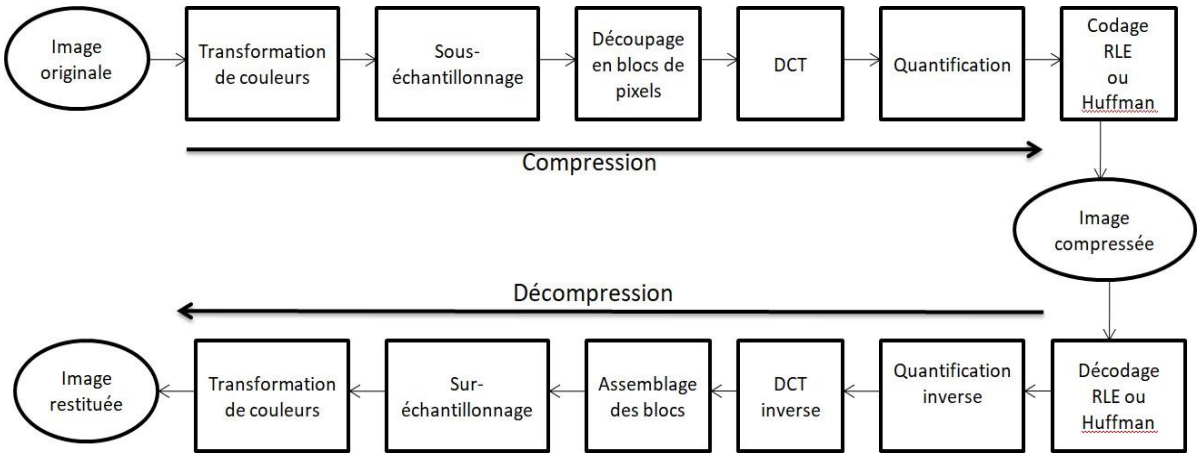


Figure I. 2 La Compression / Décompression JPEG d'une image [20]

I.10.6. Les étapes de la compression JPEG

1) Transformation de couleurs :

JPEG est capable de transformer l'espace RGB (mo- dèle initial des couleurs)vers l'espace YcbCr(YUM) (modèle de type chromi- nance/luminance) pour augmenter l'efficacité de compression . **[14][16]**

Figure I. 3étape 1 de la compression JPEG (Transformation de couleurs) [14]

2) Le sous-échantillonnage :

Consiste à sous-échantillonner les signaux de chrominance pour réduire l'information occupée par la chrominance, qui est La technique la plus simple pour profiter de la diminution de la sensibilité au chrome dans les yeux Les quatre principaux formats de sous-échantillonnage que JPEG définit sont les suivants: [14] [16]

- **Le format 4:4:4 :** Aucune compression n'est utilisée dans ce format, de sorte qu'aucune dégradation de la qualité ne peut être capturée (sans sous-échantillonnage). **[14] [16]**

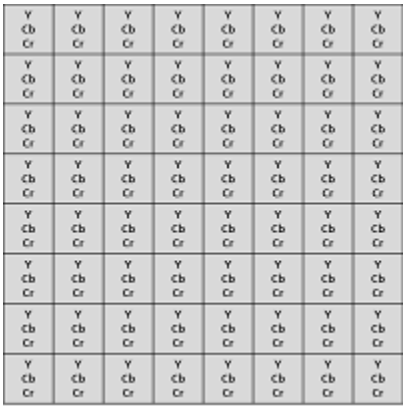


Figure I. 4 Le sous-échantillonnage (Le 4 :4 :4) [14]

- **Le format 4:2:2 :** Enlever les informations de la chrominance, rien n'est vertical et (un échantillon) sur deux est horizontal. **[16]**

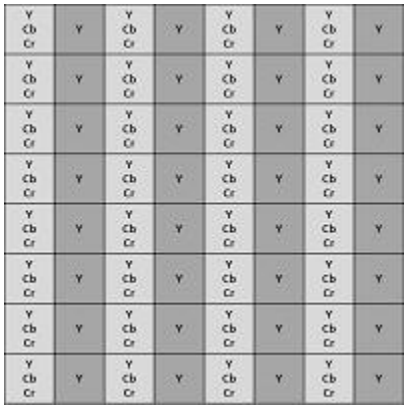


Figure I. 5 Le sous-échantillonnage (Le 4 :2 :2) [14]

- **Le format 4:2:0 :** Supprimer un échantillon de deux en les séparant horizontalementet verticalement, ou en exécutant la procédure le long des lignes (divisant l'informa- tion de chrominance par quatre).**[14] [16]**

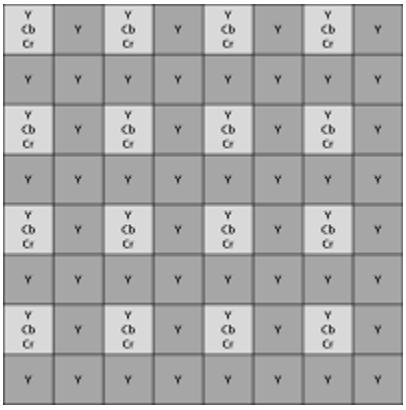


Figure I. 6 Le sous-échantillonnage (Le 4 :2 :0) [14]

- **Le format 4:1:1 :** Horizontalement, supprimer trois (03) échantillons sur quatre (04) tout en ne faisant rien verticalement. [16]

3) **Le découpage en bloc de pixels :** L'image originale est divisée en blocs de 8 à 64 pixels, ce qui raccourcit la procédure de calcul et accélère les processus de traitement ultérieurs. [16]

$$f = \begin{bmatrix} 139 & 144 & 149 & 153 & 155 & 155 & 155 & 155 \\ 144 & 151 & 153 & 156 & 159 & 156 & 156 & 156 \\ 150 & 155 & 160 & 163 & 158 & 156 & 156 & 156 \\ 159 & 161 & 162 & 160 & 160 & 159 & 159 & 159 \\ 159 & 160 & 161 & 162 & 162 & 155 & 155 & 155 \\ 161 & 161 & 161 & 161 & 160 & 157 & 157 & 157 \\ 162 & 162 & 161 & 163 & 162 & 157 & 157 & 157 \\ 162 & 162 & 161 & 161 & 163 & 158 & 158 & 158 \end{bmatrix}$$

Figure I. 7 Le découpage en bloc de pixels [14]

4) **La transformation DCT :** La DCT (Discrete Cosine Transform) : divise les trois composants de couleur de l'image en beaucoup de blocs 8.Pour éliminer la redondance des données d'une image à 8 bits, il est possible d'évaluer l'amplitude des changements d'un pixel à l'autre**. [16] [17]**

$$f = \begin{bmatrix} 139 & 144 & 149 & 153 & 155 & 155 & 155 & 155 \\ 144 & 151 & 153 & 156 & 159 & 156 & 156 & 156 \\ 150 & 155 & 160 & 163 & 158 & 156 & 156 & 156 \\ 159 & 161 & 162 & 160 & 160 & 159 & 159 & 159 \\ 159 & 160 & 161 & 162 & 162 & 155 & 155 & 155 \\ 161 & 161 & 161 & 161 & 160 & 157 & 157 & 157 \\ 162 & 162 & 161 & 163 & 162 & 157 & 157 & 157 \\ 162 & 162 & 161 & 161 & 163 & 158 & 158 & 158 \end{bmatrix} \Rightarrow F = \begin{bmatrix} 1260 & -1 & -12 & -5 & 2 & -2 & -3 & 1 \\ -23 & -17 & -6 & -3 & -3 & 0 & 0 & -1 \\ -11 & -9 & -2 & 2 & 0 & -1 & -1 & 0 \\ -7 & -2 & 0 & 1 & 1 & 0 & 0 & 0 \\ -1 & -1 & 1 & 2 & 0 & -1 & 1 & 1 \\ 2 & 0 & 2 & 0 & -1 & 1 & 1 & -1 \\ -1 & 0 & 0 & -1 & 0 & 2 & 1 & -1 \\ -3 & 2 & -4 & -2 & 2 & 1 & -1 & 0 \end{bmatrix}$$

Figure I. 8 La transformation DCT [14]

5) **La Quantification :** la quantification engendrant des pertes d'informations majeures et aussi de gagner plus de place au sein de la chaine de compression, Afin de réduire les fréquences élevées d'une image que le DCT a souligné, nous devons simplement diviser notre matrice de fréquence par la matrice quantifiée pour obtenir notre matri- cielle quantifiée. [14] [15]

$$F = \begin{bmatrix} 1260 & -1 & -12 & -5 & 2 & -2 & -3 & 1 \\ -23 & -17 & -6 & -3 & -3 & 0 & 0 & -1 \\ -11 & -9 & -2 & 2 & 0 & -1 & -1 & 0 \\ -7 & -2 & 0 & 1 & 1 & 0 & 0 & 0 \\ -1 & -1 & 1 & 2 & 0 & -1 & 1 & 1 \\ 2 & 0 & 2 & 0 & -1 & 1 & 1 & -1 \\ -1 & 0 & 0 & -1 & 0 & 2 & 1 & -1 \\ -3 & 2 & -4 & -2 & 2 & 1 & -1 & 0 \end{bmatrix} \Rightarrow F^* = \begin{bmatrix} 79 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ -2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Figure I. 9 La Quantification [14]

6) **Le codage :** L'étape finale du compression est le codage des valeurs quantifiées (Ré-ordonnancement des coefficients de l'image en une séquence zig-zag, codage des coefficients) Le codage DCT quantifiée s'effectue en zigzag (RLE, HUFFMAN), pour éliminer les redondances restants, utilisez la technique de Huffman pour coder le résultat.

- **Le codage RLE :** est très simple car le nombre de caractères suivant peut facilement être utilisé pour remplacer tous les caractères identiques. **[14][17][18]**
- **Le codage de Huffman :** Utilisez le moins de bits possibles pour représenter avec précision les caractères les plus courants. **[15]**

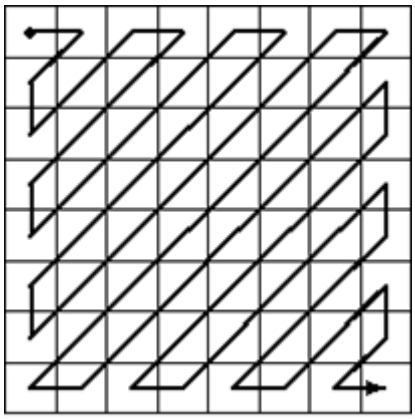


Figure I. 10 Le Codage [14]

I.10.7. Les étapes de la décompression JPEG

La décompression implique de ré-péter les mêmes étapes de manière inversée.

		Avantages	Inconvénients
Les méthodes par transformation			

	La transformation en Cosinus Discrète (DCT)	-Compression de haute performance. -Transformation rapide dans l'utilisation d'une image compressée).**[42]** -Facile à mettre en œuvre (efficacité mathématique). **[43]**	- Le codage d'entrée doit être divisé en blocs 2d non chevauchants. -Transformation d'image complète effectuée demanière incorrecte. -Taux de compression faible. **[42]**
	La transformation par ondelettes discrètes (DWT)	-la plus performante à l'heure actuelle. -Les taux de compression élevés donnent de très bons résultats. -Permet un téléchargement progressif de l'image. -L'algorithme est plus simple. **[44]** -Technique récente. - Simple à utiliser. -Excellentes caractéristiques de décorrélation. - Représenter de plusieurs résolutions .**[45]**	-Produit la perte d'informations. -Processus relativement complexe. -Manque de localisation des ondelettes. -Le temps de compression accru. - Le calcul DWT pourrait être plus coûteux que le calcul DCT. - Mauvais choix de direction pour les propriétés diagonales. -Faible résolution conjointe (temps/fréquence) **[46]**

		-Transformation de l'image complète (ajoute une échelle par défaut). -Amélioration de la détection d'informations pertinentes à la perception humaine. -Calcul très rapide. **[46]**	
Les méthod esspatiale (directes)			
	Méthode par fractale	-La détection de récurrence de motifs. -éliminant la redondance d'information dans l'image. - Utilisation d'un zoom fractal fort pour agrandir une image sans pixellisation. - Le taux de compression offre de nombreux avantages. **[47]**	-Elle n'a pas encore été publié comme norme. - Malgré les progrès, la compression reste lente. L'image est floue enraison de la compression. **[47]**

	Méthode JPEG2000	-La transmission progressive. - Un débit fixe. - Traitement direct des données et accès au train de données . - Le codage temps réel ou Avoir la capacité de compresser et de décompresser séquentiellement des images. - Robustesse vis-à-vis des erreurs binaires. - La protection des images, avec le watermarking. - La rétro-compatibilité, ou un transcodage facile. - Meilleures performances. - Format plus flexible. **[49]**	-A utiliser ave c précautions car ça peut brouiller l'image. -Un processus très complexe. -Technique de compression d'image sn'est pas fixes. -Elle ne profite pas de lacompression. -Un taux de compression inférieur. **[48]**

Table 1 Avantages et inconvénients des méthodes de compression d'images avec perte (irréversibles)

II. Cryptographie

II.1. Historique

L'Egypte a utilisé la cryptographie il y a 4000 ans, Il a été créé dans la Grèce antique. Le terme "cryptographie" est composé de deux parties : "cryptos" qui signifie "secret" et "logos" qui signifie "type de texte".

La cryptographie a été utilisée pour préserver les interactions militaires et diplomatiques pendant des milliers d'années. Cependant, la première attestation de l'utilisation délibérée d'un moyen de chiffrement des messages vint de la Grèce vers le VIème siècle avant J.C, et se nomme le scylate.

Plus tard, les romains adoptèrent un chiffrement qui consistait en une substitution mono alphabétique simple. Puis, pendant des siècles, on assista à la mise au point de plusieurs techniques de chiffrement, on peut citer parmi ces techniques:

- À la fin de la Première Guerre mondiale, les Allemands ont mis en place le système ADFGVX en 1918, et Arthur Scherbius a reçu un brevet pour le dispositif de cryptage Enigma.
- Le nombre de Hill a été créé par Lester S. Hill en 1929.
- Le système de codage de caractères à 8 bits connu sous le nom de code ASCII, qui a 256 caractères potentiels, a été approuvé en tant que norme en 1960.
- La technologie de cryptage DES (Data Encryption Standard) a été soumise à la Standardisation par le Bureau of Standards des États-Unis en 1975. **[2] [21]**

II.2. Définition

La cryptographie permet la conversion de texte clair (texte ordinaire) en texte chiffré (ce processus est appelé cryptage, puis l'inverse est appelé décryptage).

Le processus de cryptographie assure la sécurité et l'intégrité des messages confiden- tiels utilisant différentes formes de chiffrement et de déchiffrement, il aussi un proces- sus de stockage, conception et de transmission de données sous forme cryptée pour protéger les données. **[22]**

II.3. Terminologie de base

- **Chiffrer :** Convertir un message M (Plaintext) en un message C (Ciphertext).
- **Crypto-système :** C'est un système avec l'algorithme(cryptage,décryptage) qui permet de chiffrer des données. **[29]**
- **Déchiffrer :** Conversion de texte chiffré en texte en clair. **[26]**
- **Cryptographie :** C'est l'étude des techniques qui permettent de communiquer des données sur un support spécifique d'une manière privée.
- **Cryptanalyse :** Le déchiffrement, le décodage et le cryptage des messages non autorisés sont toutes des formes d'art. Toutes les méthodes d'attaques de systèmes crypto- graphiques tombent dans cette catégorie. En identifiant les faiblesses des méthodes employées, il cherche à récupérer du texte clair des extensions cryptées. **[24].**
- **Cryptologie :** Cryptologie = Cryptographie + Cryptanalyse. **[30].**
- **Stéganographie :** L'art de cacher une communication secrète au sein d'un autre message porteur, est connu sous le nom de steganographie (du grec steganos = couvert, graphène = écriture). **[28].**

II.4. Les objectifs de la cryptographie

Les principales exigences de sécurité pour la protection des données sont les suivantes :

- **Confidentialité de l'information :** Caractéristique la plus utilisée qui permet de s'assurer qu'aucune autre personne ne peut lire le message à l'exception du destinataire prévu, pour le protéger contre le risque d'être accédé par des personnes indésirables.
- **Intégrité de l'information :** S'assurer que le message reçu n'a pas été modifié (diminué) de l'original sans autorisation.
- **Authentification (Détection de l'altération de l'information par une entité non-autorisée) :** Sécuriser l'identité d'un utilisateur pour contrôlé l'accès à des ressources.
- **Non-répudiation :** permet de s'assurer que l'expéditeur ne peut pas refuser ce message, empêché qu'une entité soit participée dans un échange de données. **[22]**

II.5. Cryptographie classique

II.5.1. Définition

Les crypto systèmes basés sur des lettres (ou des caractères) étaient le centrede la cryptographie classique .Diverses techniques de chiffrement ont traduit ou remplacé certains caractères pour

d'autres. Les deux processus, qui sont divisés en deux familles significatives de cryptage (par substitution, par transposition) ont été effectués par les meilleurs systèmes. **[24]**

II.5.2. Catégories de la cryptographie classique

II.5.2.1. Cryptographie par substitution

chaque caractère du texte en clair d'un message Est remplacé par un caractère différent dans le texte chiffré. Il existe quatre variétés de cryptage par substitution : mono alphabétique, poly alphabétique, homophonique et poly grammes.

a. Substitution mono-alphabétique: Chaque lettre du message simple doit être remplacée par une lettre correspondante dans le message chiffré (le chiffre de César). **[23]**

- ✓ **Le code de César :** L'armée romaine a utilisé la plus ancienne technique, inventée par Jules César au premier siècle avant notre ère, qui consistait à déplacer les lettres de n rangs dans l'alphabet. **[31] [23]**

b. Substitution poly-alphabétique

Utiliser régulièrement une suite de chiffres mono alphabétiques. Le chiffre de Vigenère est souvent l'exemple le plus célèbre. **[23]**

- ✓ **Le chiffre de Vigenére :** En 1587, Alberti, Tri thème et Porta ont publié les résultats de leurs recherches sur les techniques suggérées. Il propose un crypto système polyal phabétique. on utilise une table composée de 26 alphabets, écrits dans l'ordre, mais décalés de ligne en ligne d'un caractère. On peut résumer ces décalages avec un carré de Vigenére. **[25] [31] [29]**

II.5.2.2. Cryptographie par transposition

L'ordre des caractères du texte en clair demeurent inchangés mais dont les positions respectives sont modifiées (caractères d'une phrase, pixels d'une image...), ce qui permet de mieux cacher le message. **[24] [31]**

II.6. Cryptographie moderne

Le but principal de la cryptologie moderne est l'étude des techniques pour garantir les services de confidentialité, d'intégrité et d'authenticité dans les systèmes d'information car les techniques de cryptographie ont évolué.

Le nombre de clés utilisées pour chiffrer et déchiffrer distingue la cryptographie en deux catégories :

- ✓ Cryptographie symétrique (les méthodes à clef secrète).
- ✓ Cryptographie asymétrique (les méthodes à clef publique/clef privée). **[22]**

II.6.1. La cryptographie symétrique (à clé secrète)

Le terme «cryptographie», qui se ré- fère à une méthode de cryptage dans laquelle l'expéditeur et le destinataire partagent la même clé secrète, est utilisé pour décrire le plus ancien type de chiffrement. Elle est classée en deux catégories :

- ✓ Chiffrements par blocs (Block ciphers).
- ✓ Chiffrements de flux (Stream cipher).

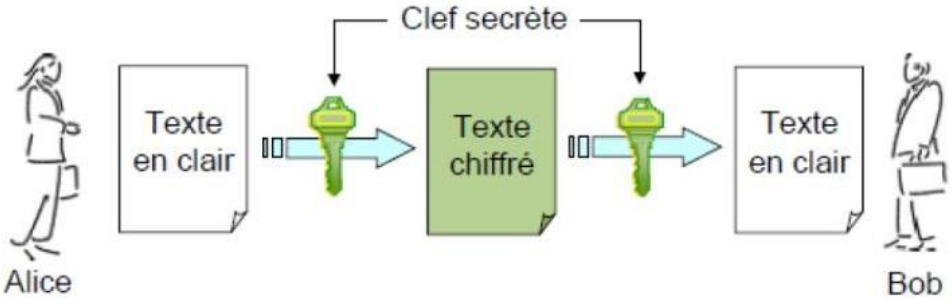


Figure I. 11 Principe de chiffrement symétrique [23]

II.6.1.1. Crypto systèmes par flots (Stream Cipher)

Le Stream Cipher fonctionnent sur des petites unités (des bits), le principe est de créer un long flux de clé de même longueur que le message, qui est crypté bit par bit avec le texte clair.

Dans une technique de chiffrement de flux, une étape interne (configurée avec une clé privée) cachée est utilisée pour créer le texte chiffré de sortie. **[22]**

Les algorithmes de cryptographie symétrique par flot sont : RC4, Bluetooth E0/1, GSM A5/1…

Il existe deux grandes catégories d'algorithmes par flot :

1. **Les algorithmes adaptés à une implantation logicielle** : réaliser des vitesses de chiffrement extrêmement élevées (plusieurs Gbits/s).
2. **Les algorithmes adaptés à une implantation matérielle :**

- ✓ Les installations sont efficaces en termes de taille ou de consommation d'énergie.

- ✓ La séquence qui sert au chiffrement dépend de la clé mais pas du message clair.
- ✓ Le cryptage et le décryptage sont effectués à l'aide de XOR.
- ✓ Un composant du message décodé ne souffre que si une partie du message chiffré est modifiée pendant que le message est transmis. **[24]**

II.6.1.1.1. Algorithme RC4 (Rivest Cipher 4)

a. Principe du RC4 : il Fonctionne de la façon suivante :

- ✓ En utilisant la clé RC4 autant de fois que nécessaire pour remplir la table, vous pouvez initialiser une table de 256 octets.
- ✓ Ensuite, des actions très basiques sont effectuées: les octets sont ajoutés à la table et y sont déplacés, mélangeant la table.
- ✓ Enfin, nous avons un ensemble de bits pseudo- aléatoires qui peuvent être combinés en utilisant la méthode XOR pour chiffrer les données. **[25]**

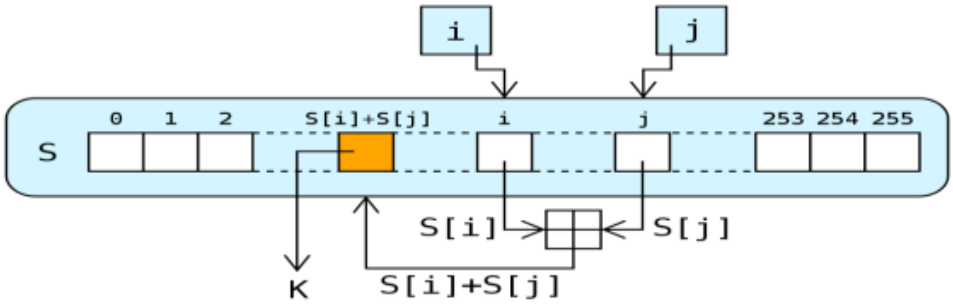


Figure I. 12 Principe de RC4 [25]

II.6.1.1.2. Algorithme A5

Utilisé pour chiffrer la communication radio entre un appareilmobile et l'antenne de relais la plus proche dans les téléphones mobiles GSM. **[26]**

II.6.1.2. Crypto systèmes par blocs (Block Cipher)

Permet de diviser le message brut en blocs de taille fixe et les chiffrer un par un pour produire des blocs de chiffrement de même taille. Au lieu de numériser les caractères individuels, le cryptage de blocs utilise des blocs de texte clair. [22]

- ❖ Parmi les algorithmes qui utilisent chiffrement par bloc :

- DES (clef de 56 bits codée sur 64 bits).
- IDEA ou CAST-128 (clef de 128 bits).

- Blowfish (longueur de clef variable, jusqu'à 448 bits).
- AES (Rijndael, longueur de clef variable : 128, 192 ou 256 bits) **[23]**

II.6.1.3. Les avantages du cryptage symétrique

- L'exécution est très rapide jusqu'à 100 fois plus rapide que les solutions asymétriques.
- La facilité de mise en œuvre (gestion d'une seule clé).
- Les clés sont assez courtes (entre 64 et 128 bits). [27]

II.6.1.4. Les inconvénients du cryptage symétrique :

- Il est nécessaire de distribuer N*(N-1)/2 clés dans un réseau de N entités susceptibles decommuniquer secrètement.
- Gestion des clés difficiles (nombreuses clés). Point faible = l'échange de la clé secrète. **[27]**
- Un système symétrique peut être très robuste, seule la clé doit être transmise de manièresécurisée.
- L'échange physique d'une clé ou la connexion à un canal sécurisé sont les seuls moyens sûrsde transmettre une clé en toute sécurité. **[2]**

II.6.2. La cryptographie asymétrique (à clé publique)

Whitfield Diffie et Martin Hellman de l'université Stanford ont proposé un principe de chiffrement en 1976, s'oppose que la clé publique est distribuée parmi les expéditeurs de message par destinataire, tandis que son privé apparié la clé reste secrète pour le destinataire.

La clé publique est utilisée pour chiffrement, la clé secrète est utilisée pour le déchiffrement. [22]

Les principaux algorithmes asymétriques à clé publiques sont : RSA, DSA, ECC, PGP,Diffie-Hellman.

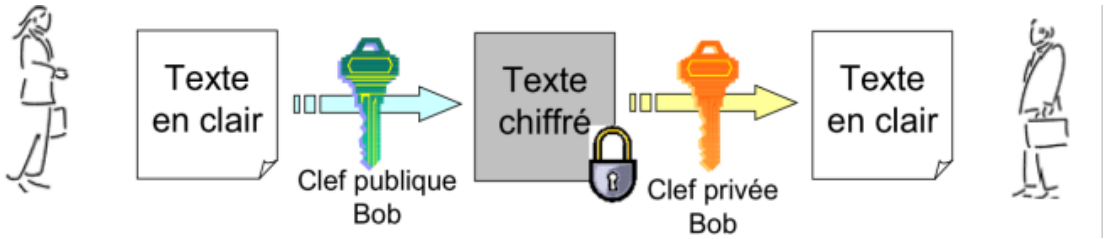


Figure I. 13 Principe de chiffrement asymétrique [23]

II.6.2.1. Les Avantages du cryptage asymétrique

- Comme la clé privée n'est connue que par l'utilisateur, elle élimine le problème de l'envoi d'une clef privée vers un réseau non sécurisé.
- Il est possible d'utiliser la signature électronique.
- Pour créer des séquences courtes, telles que des signatures ou des clés secrètes pour le cryptage symétrique, le chiffrement à clé publique peut être préférable.
- La durée de vie d'une paire de clés (public/secret) est plus longue que celle d'une seule clé.
- Il est impossible de décrypter le message si une personne non autorisée l'intercepte.
- L'élimination de la problématique de la distribution de la clé privée.[27] [28]

II.6.2.2. Les inconvénients du cryptage asymétrique

- Le risque d'attaques par substitution de clés.
- Le plus grand danger d'utiliser des clés asymétriques est une attaque d'intermédiaire, qui est la possibilité qu'un adversaire oppose les clés publiques transférées et les remplace par les siennes.
- Les clés ont une taille supérieure à celle des systèmes symétriques (plus de 512 bits).
- Le temps d'exécution est inférieur au cryptage symétrique. [2] [27]

II.6.2.3. Algorithme RSA (RIVEST, SHAMIR, ADLEMAN)

Est connue sous le nom d'algorithme RSA qui Il a été créé en 1977 par trois mathématiciens : Rivest Ronald, Shamir Adi et Adleman Leonard. Il a été développé en raison de la difficulté de factoriser un nombre important en produit de deux facteurs principaux.[22] [25]

II.6.2.3.1. Principe :

- ✓ **Génération et Distribution des clés :**

p , q deux nombres premiers : n = pq .

Le nombre e : n'a aucun facteur en commun avec $\varphi\ (N)\ =\ (p-1)(q-1)$. e, d : deux entiers, tels que $ed\ =\ 1\ mod\ \varphi(n)$.

Le couple (e, n) : la clé publique, le couple (d,n) : la clé privée.[29]

- ✓ **Chiffrement du message :**

Si *M* (un message) : entier naturel inférieur à n , le message chiffré représenté par :

$C \equiv M * e \ (mod\ n)$ /*C*: entier naturel inférieur à *n*.

- ✓ **Déchiffrement du message :**

Pour déchiffrer C, on utilise d, l'inverse de e modulo *(p – 1)(q – 1)*, le message clair *M* :

$M \equiv C * d \ (mod\ n)$[25].

Conclusion

Dans ce premier chapitre, on a vu que la compression est une étape cruciale pour optimiser l'utilisation des grandes quantités d'informations dans les réseaux informatiques.

De plus, nous avons tenté de donner un aperçu général des concepts de compression d'images en présentant les deux types de compression, en mettant l'accent sur la compression JPEG et parlé en détail de la compression JPEG.

En revanche, nous avons examiné la cryptographie avec une brève histoire, citer ses différents types, tout en mettant l'accent sur la cryptographie symétrique.

Nous avons également distingué deux classes importantes de méthodes de cryptage et présenté les avantages et les inconvénients de chaque type d'algorithme de cryptage. Les principaux algorithmes de cryptage symétrique, asymétrique, par flot et par bloc ont également été présentés dans ce chapitre.

Le deuxième chapitre décrit la mise en œuvre de la possibilité de combiner les deux techniques de compression et de cryptage, pour en faire un système de compression cryptographique d'images basé sur le Stream Cipher et la compression JPEG.

CHAPITRE 02

CRYPTO COMPRESSION D'IMAGE

Introduction

L'utilisation de technologies spécifiques s'est développée dans la vie quotidienne principalement pour améliorer et sécuriser le stockage et la transmission des images qui est très importante, car certain nombre de méthodes de cryptage et de compression d'image ont récemment été développés de telle sorte proposer un schéma efficace sert à combiner les deux technologies (compression /cryptage) des images de manière jointe qui ont signifié aux techniques de Crypto-compression, pour réduire la taille d'une image numérique pour un haut niveau de confidentialité. Le travail de ce chapitre traite un système de crypto-compression basé sur le Stream Cipher et d'un algorithme de compression Jpeg. Nous allons commencer tout d'abord par faire une comparaison des différentes techniques de compression d'images avec perte (points forts/points faibles). Ensuite nous avons citer quelques travaux similaires

développés dans le domaine et qui sont distingués les uns des autres par le type de compression et de cryptage utilisées dans le système de crypto-compression.

I. Travaux connexes

- En 2004 Jean-Claude Borie et William Puech et Michel Dumas dans cette propo- sent deux cryptosystèmes qui discute le transfert sécurisé d'images médicales. Le premier est un algorithme de chiffrement par blocs très rapide (TEA), tandis que le second est un algo- rithme de chiffrement par flots qui crée une variante (Vigenére). Et soulignent les distinctions entre ces deux systèmes, en particulier en ce qui concerne la combinaison de la compression et du cryptage d'images. Les résultats des images médicales montrent les deux approches. [39]
- En 2006 William Puech et José Marconi Rodrigues présente dans un article une méthode de chiffrement partiel ou sélectif d'images médicales JPEG. Il est basé sur le cryptage des coefficients DCT quantifiés. La méthode proposée entraîne une réduction significative du chiffrement et du déchiffrement temps de traitement. Il est rapide et ne réduit pas les performances de compression de l'algorithme JPEG. [36]
- En 2006 William Puech et José Marconi Rodrigues présente dans un article une méthode de chiffrement partiel ou sélectif d'images médicales JPEG. Il est basé sur le cryptage des coefficients DCT quantifiés. La méthode proposée entraîne une réduction

significative du chiffrement et du déchiffrement temps de traitement. Il est rapide et ne réduit pas les performances de compression de l'algorithme JPEG. [36]

- En 2007, Mohammed BENABDELLAH propose deux nouvelles approches Hybrides brides de crypto-compression, La compression de transformation multi-échelle de Faber- Schauder, qui est basée sur des outils de compression et de crypto compression, qui s'appuient sur le cryptage basé sur l'algorithme DES et l'algorithmes AES des coefficients dominants dans la représentation à l'échelle mixte: applications pour les images fixes et vidéo. [32]
- En 2009 BOUMARAF propose un schéma de crypto-compression efficace qui intègre le cryptage RSA dans un processus de compression JPEG2000 sera d'abord présenté, puis développé, puis critiqué. [18]
- En 2011 Y. Benlcouiri et al. proposent dans ce travail un nouvel hybride approche de crypto-compression qui applique un chiffrement basé sur l'algorithme AES sur les paramètres de la compression par réseau de neurone multicouche. [1]
- S. Ftérich et C. Ben Amar1 propose 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 qui est présenté par un Crypto- Compression d'Images Fixes Par la méthode de Quadtree optimisée et AES. [33]
- En 2015 Bobby Jasuja et Abhishek Pandya proposent dans un article une technique utile pour réduire la taille des données, augmenter le taux de transfert de données et fournir sécurité pendant la communication, qui est basé sur le codage entropique comme l'arithmétique codage qui peut être utilisé pour atteindre un haut niveau de compression dans les topologies de réseau actuelles pour l'échange de données avec plus sécurité et compression. [22]
- En 2015 Mr AMRANE Mourad propose une approche hybride Crypto compression d'image par cryptage partiel, qui repose sur une association d'algorithmes de cryptage tel que l'algorithme DES et l'algorithme AES avec des algorithmes de compressions. Cette méthode de crypto-compression a bien montré sa bonne performance concernant sont usage dans différents domaines tel que les réseaux informatique, la transmission et le transfert de données. [35]

- En 2017 Vincent Itier et William Puechpropose une méthode de crypto compression qui permet une recompression sans aucune information sur la clé de chiffrement. Cette méthode est efficace pour recompresser une image JPEG cryptée en termes de taux de compression.[13]
- En 2019 Mohammed M. Siddeq& Marcos A. Rodrigues proposent une nouvelle méthode de compression-chiffrement 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 basé sur la transformation DWT avec un nouvel algorithme de crypto- compression Hexadata à l'étape de compression et un nouveau algorithme de recherche correspondant à l'étape de décodage. La nouvelle méthode de crypto-compression consiste de quatre étapes principales. Enfin il ont testé la technique sur des images 2D notamment en streaming à partir de vidéos, les Résultats montrent que la méthode de crypto-compression proposée donne des taux de compression élevés jusqu'à 99 % avec des images de haute qualité perceptuelle.[40]
- En 2020 on trouve deux travaux de Master à l'université de Tébessa : BADAOUI, Propose un système de crypto-compression d'images basé sur le Block Cipher et la compression fractale ,consiste à combiner à la fois des techniques de compression et de cryptage des images, il utilise une approche de compression hybride basé sur la décomposition Quadtree et le codage de Huffman pour terminer le codage et calculer les paramètres de performances du compression ,il applique l'algorithme de cryptage L'AES pour le chiffrement à base de block Cipher, et calcule les temps d'exécution.[27]
- DJEFFALI, propose un système de crypto-compression d'images basé sur le Stream Cipher et la compression RLE, par une étude sur le sujet des systèmes de crypto-compression basé sur une compression sans perte RLE, et un algorithme de chiffrement moderne RC4 basé sur la technique du Stream Cipher ou cryptage par flot. [38]
- En 2021 Pauline Puteaux et Zichi Wang et Xinpeng Zhang et William Puech proposent une hiérarchie approche de masquage de données à haute capacité (HHCDH) pour les images JPEG cryptées. Après chiffrement de tous les coefficients non nuls, ils sont traités des basses aux hautes fréquences, pour obtenir une valeur de charge utile élevée, tout en préser- vant une très bonne qualité des images JPEG reconstruite.[37]
- En 2021 IYAD HRAINI et MOUSA FARAJALLAH et NABIL ARMAN et WAS-SIM HAMIDOUCHE proposent un Crypto-Compression basée sur le chiffrement

sélectif pour les WMSN. Par un algorithme de compression nommé Set Partitioning In Hierarchical Tree (SPIHT).L'approche proposée est appropriée et capable d'être utilisés dans le WMSN en tenant compte de leurs limites de ressources. Les résultats obtenus confirment la haute per- formance de l'approche proposée avec un surcoût inférieur à 1 %.Cette approche est appli- cable pour les applications en temps réel.[41]

- En 2022 HAMIDA, l'université de Tébessa, et dans le cadre d'un mémoire de Mas- ter propose un Système de crypto compression d'images basé sur le Block Cipher et la compression par Ondelettes, avec une étude plus détaillée au sujet du système de crypto- compression basé sur une compression avec perte DWT, et un algorithme de chiffrement mo- derne AES basé sur la technique du Block Cipher ou cryptage par blocs. [2]
- En 2022 , L.H. Abed et M.N. Rashid et O.M. Al Okashi, présente une approche de pointe de crypto-compression utilisant ''Discrete Cosine Transform'' (DCT) et Daubechies 4 ondelettes visant à terme à améliorer le stockage d'images basé sur le cloud en termes de sécu- rité et efficacité. Les résultats expérimentaux illustrent que le cryptage accompli était assez robuste contre diverses attaques avec une valeur PSNR décente de 36,64 au total et un taux de compression efficace de 6,66 en moyenne sous le thème partiel crypto-compression for cloud- based photo storageusing DCT and daubechies 4 wavelet. [34]

II. Crypto-Système proposé (Compression JPEG par flot « RC4 »)

Pour notre système de crypto-compression on a proposé de combiner la méthode de cryptage Stream Cipher avec un algorithme de chiffrement RC4 et une compression JPEG avec perte par la technique DCT.

II.1. Transformation en cosinus discrète (DCT) :

II..2.1. Définition :

C'est le noyau de la méthode de compression JPEG, est une transformée mathématique complexe conçue qui Créer une image dans le domaine de fréquence à partir de l'image spatiale d'origine (8*8) :

- Composante DC (Direct Component) : Le coefficient le plus élevé de la matrice

est la valeur moyenne des éléments avant la transformation a une valeur plus grande qui est inversement proportionnelle à la luminosité moyenne du bloc de 64 pixels.

- Composantes ACs (Alternative Component) : 63 de ces composants restent.
- Les magnitudes des fréquences spatiales horizontales et verticales du bloc sont montrées par ceci :

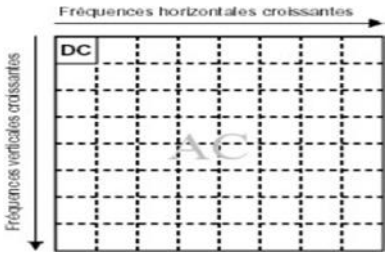


Figure II. 1 La DCT d'une fenêtre 8×8 [51]

En 1974, Ahmed, Natarajan et Rao ont mis en équation la DCT. Elle permet à Décomposer un signal (une fonction) réel discret en une combinaison linéaire de cosinus, s'applique à chaque bloc et couleur, deux variantes sont utilisées par la norme JPEG: la DCT (généralement appelée simplement la DCT) est utilisée pour compresser les images et la DCT inverse (IDCT) est utilisée pour décompresser l'image. [51] [18]

II..2.2. Pourquoi la DCT ?

Le but du DCT est de passer à travers des champs fréquents, ce qui peut afficher les données

dans un espace qui peut être compressé. Elle est facilement détectable à l'œil nu, ce qui équivaut à supprimer les hautes fréquences de l'image et à garder les basses fréquences représentatives de l'ensemble de l'image. [52]

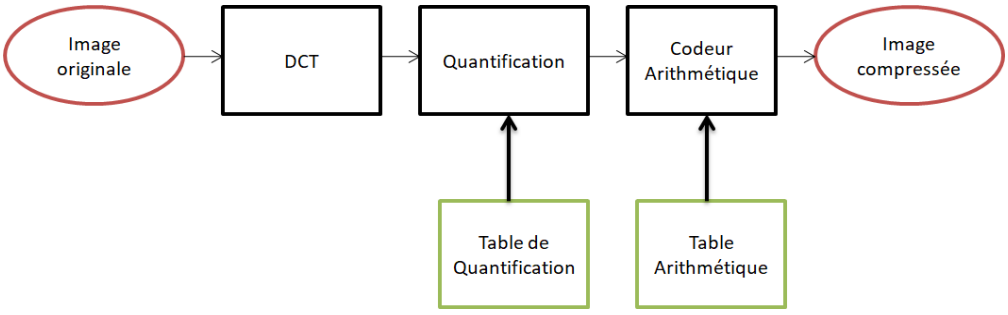


Figure II. 2 Compression DCT. [53]

Au lieu d'utiliser des pixels et des couleurs, cette méthode décrit chaque bloc comme une carte de fréquences et d'amplitudes.

Avant d'appliquer la DCT sur une image on la découpe en blocs (de taille 8x8, 4x4, 4x8 ou 8x4) qui sont traités indépendamment les uns des autres.

a) La DCT produit une matrice carrée N x N de coefficients de fréquence à partir d'une matrice carrée N x N de valeurs de pixels.

b) Des blocs de 8 x 8 pixels (tables de 64 valeurs) sont utilisés pour diviser la matrice complète en plus petites pièces.

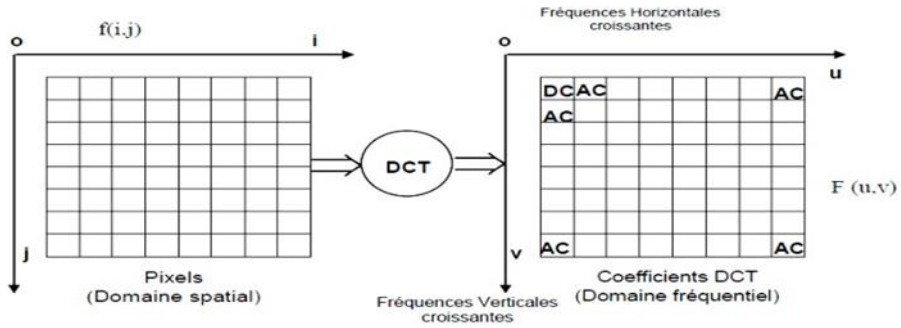


Figure II. 3 Représentation de la DCT d'un bloc de 8×8 pixels [44]

c) Le coefficient continu à la position (0,0) dans la sortie d'une matrice DCT est la va- leur qui indique la moyenne de la taille globale de la matrice d'entrée.

d) La valeur moyenne de tous ces coefficients est placée en haut à gauche de ce bloc (processus totalement réversible) où les 64 valeurs converties (de chaque bloc) sont positionnées d'une certaine manière.

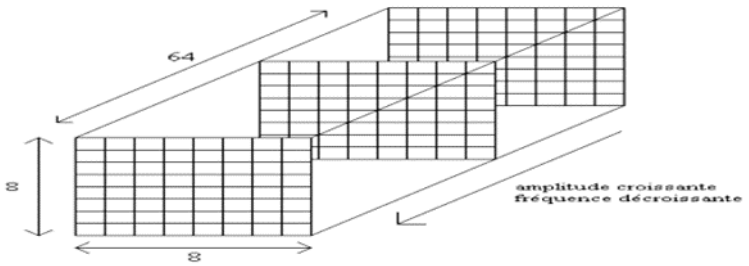


Figure II. 4 Matrice tridimensionnelle 8×8x64 [54]

e) La représentation de l'image de la matrice de sortie est centrée par la DCT.

f) Les coefficients inférieurs et supérieurs de cette matrice incluent des données moins claires. [35]

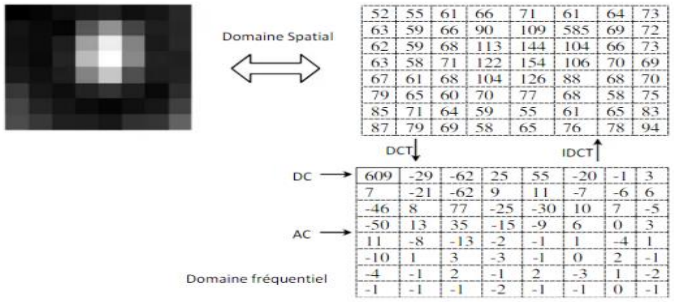


Figure II. 5 Principe de fonctionnement de la DCT. [16]

Le codage par transformation DCT permet de séparer l'information la plus importante de l'image de celle moins importante. La formule mathématique de la DCT est la suivante à chaque bloc de pixels :

$$DCT(i,j) = \frac{2}{N} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \cos\left(\frac{(2\mathrm{x}+1)\mathrm{i}\pi}{2\mathrm{N}}\right) \cos\left(\frac{(2y+1)j\pi}{2N}\right) pixel(x,y)$$

La transformation inverse de la DCT permet de récupérer les données d'origine (s'il n'y a pas d'erreurs d'arrondis) IDCT s'exprime par :

$$pixel(x,y) = \frac{2}{N} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} C(i)C(j) \cos\left(\frac{(2x+1)i\pi}{2N}\right) \cos\left(\frac{(2y+1)j\pi}{2N}\right) DCT(i,j) \ldots (2)$$ **[55]**

i, j : représente les indices de la matrice de DCT.

x, y : représente les indices de l'image de départ.

N : représente la taille d'un bloc.

C(i) et C(j) : représente les facteurs d'orthogonalité de la transformée.

Pixel (x, y) : représente la valeur du pixel de l'image initiale à transformer à la position (x, y)(coordonnées spatiales) dans le bloc de l'image originale de 8× 8 pixels.

DCT (i, j) : correspond au coefficient de la DCT (la valeur de la DCT au point de coordonnées fréquentielles (i, j) dans le bloc résultat de 8 × 8 pixels).

La constante C dans les deux cas est :

$$C(x) = \begin{cases} \frac{1}{\sqrt{2}} \; pour \; x = 0 \\ 1 \quad pour \; x > 0 \end{cases} \quad \ldots\ldots (3)$$ **[55] [16]**

II..2.3. Les types de la Transformation en cosinus discrète (DCT) :

Les variantes les plus connus DCT I, DCT II, DCT III qui sont les principaux composants de la compression JPEG.

a) DCT I : la DCT I s'exprime par :

$$C(u) = \alpha(u) \sum_{x=0}^{n-1} f(x) \cos\left[\frac{\pi(2x+1)u}{2n}\right] \ldots\ldots. (4)$$ **[56]**

$$\text{Et : } \alpha(u) = \begin{cases} \sqrt{\frac{1}{n}} & u = 0 \\ \sqrt{\frac{2}{n}} & u \neq 0 \end{cases} \ldots\ldots (5)$$

b) DCT II : Il s'agit d'une extension directe de DCT I, sa formule mathématique est :

$$C(u,v) = \alpha(u)\alpha(v) \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} f(x+y) \cos\left[\frac{\pi(2x+1)u}{2n}\right] \cos\left[\frac{\pi(2y+1)v}{2n}\right] \ldots. (6)$$ **[56]**

$(u)\ et\ (v)$ ce calculent de la même façon ,on remarque que :

$$u = v = 0 \rightarrow C(u=0, v=0) = \frac{1}{n} \sum_{x=0}^{n-1} f(x,y) \ldots. (7)$$ **[56]**

Le coefficient DC est représenté par ce coefficient, tandis que les coefficients AC sont représentés par les autres coefficients. Nous verrons plus tard ce que cela signifie en compression JPEG.

c) DCT III : La formule de l'inverse de la DCT II est fournie par :

$$f(x,y) = \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} \alpha(u)\alpha(v) C(u,v) \cos\left[\frac{\pi(2x+1)u}{2n}\right] \cos\left[\frac{n(2y+1)v}{2n}\right] \ldots (8)$$ **[56]**

II..2.4. Caractéristiques de la DCT:

- ✓ **Dé-corrélation :** Les pixels sont dé corrélés afin de réduire la variance des pixels voisins dans l'image, ce qui permet une compression efficace en codant chaque pixel in- dépendamment.
- ✓ **Concentration des coefficients :** Le DCT est très efficace pour les images hautement corrélées car il permet la compression des coefficients qui représentent les basses

fréquences dans une seule partition de matrice, permettant la séparation de la basse de la haute fréquence, et si c'est une image mal corrélée, les coefficaces sont concentrées dans plusieurs partitions de la matrice.

- ✓ **Séparabilité :** présente un avantage de base Les opérations 1-D sur les lignes et les colonnes d'une image sont utilisées pour calculer C (u, v) en deux étapes. La division de DCT II peut être effectuée comme suit :

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{n-1}\cos\left[\frac{\pi(2x+1)u}{2n}\right]\sum_{y=0}^{n-1}f(x,y)\cos\left[\frac{\pi(2y+1)v}{2n}\right]\ldots. (9)$$ **[56]**

$$u,v = 0,1 \ldots\ldots n-1 \ldots. (10)$$

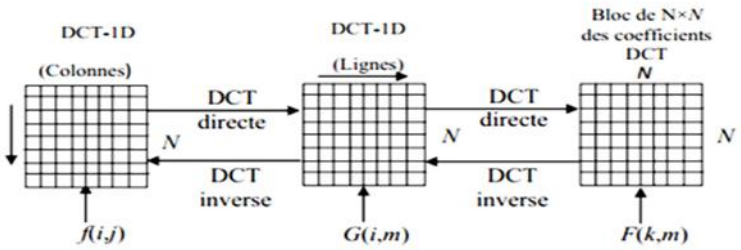


Figure II. 6 Calcul de la DCT-2D en utilisant la propriété de séparabilité. [57]

- ✓ **Symétrie :** propriété qui permet de déconnecter la matrice de transformation avant de l'appliquer à l'image, augmentant ainsi l'efficacité de calcul par des ordres de grandeur.
- ✓ **Orthogonalité** : les fonctions de base DCT sont orthogonales. Cette caractéristique réduit la complexité du pré calcul. **[57]**

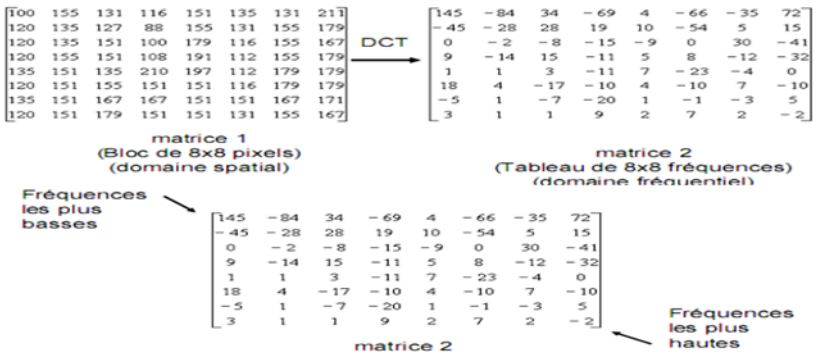


Figure II. 7 Basses fréquences/ Hautes fréquences. [58]

- Basses fréquences : plage de couleurs uniforme.
- Hautes fréquences : variations brusques de couleur d'un pixel à l'autre.

Puisque les basses fréquences ont des coefficients plus élevés que les hautes, elles sont plusimportantes. **[58]**

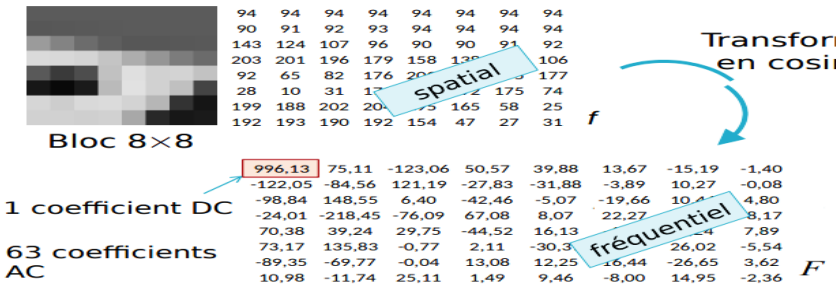


Figure II. 8 Exemple de la DCT. [59]

II..2.5. Intérêt de la DCT pour la compression d'images :

- Excellentes bonnes caractéristiques subjectives pour la représentation spatiale de la fréquence.
- Il utilise un algorithme DCT (8x8) et 64*6 ensembles d'opérations pour fonctionner très rapidement sur les PC.
- Il n'est pas possible de créer les quatre boucles imbriquées, y compris la double somme, car le cosinus permet de créer de nombreuses symétries périodiques.
- La transformation en nombres réels peut être inversée avec précision, mais lorsque l'on utilise des nombres entiers (réels arrondis), l'inversion ne restitue pas complètement l'original.
- Un ensemble unique de valeurs avec autant de coefficients que de pixels transformés, sans aucune symétrie autour d'un point central.
- Uniquement des valeurs réelles, pas de nombres complexes. **[60]**

II.2. Algorithme RC4 :

II..2.1. Choix de RC4(Rivest Cipher 4) :

Ronald Rivest a inventé la technologie de cryptage de flux en 1987. RC4 est plus simple et rapide et plus adapté à l'application en continu de cryptage des données. Il acquiert moins de temps CPU, moins d'utilisa- tion des ressources et aussi facile à mettre en œuvre.

II..2.2. Principe général de fonctionnement du l'algorithme RC4 :

- RC4, qui crée des bits pseudo-aléatoires, l'algorithme permet de créer une permutation S aussi aléatoirement que possible ses étapes sont les suivants :
- En utilisant la clé RC4 autant de fois que nécessaire pour remplir la table, vous pouvez initialiser une table de 256 octets.
- Les octets sont déplacés dans la table et des ajouts sont effectués, deux processus très basiques.
- L'objectif est de changer le conseil d'administration autant que vous le pouvez.
- Nous obtenons une série de bits apparemment aléatoires.
- Le produit final sera une suite qui peut être utilisée pour crypter les données XOR.
- Les octets sont ce que cet algorithme utilise. Par conséquent, la longueur variable de la clé peut aller de 1 à 256 octets (ou 8 à 2048 bits). Il est utilisé pour démarrer un vecteur S de 256 octets. S a toujours une permutation de toutes les cellules qui le composent.
- Pour le déchiffrement on applique le même algorithme de chiffrement puisque l'opération XOR est une opération symétrique. **[38]**

II..2.3. Description détaillée du RC4

le combiner, le déchiffrement se fait de la même manière. Pour générer le flot de bits, l'algorithme dispose d'un état interne, tenu secret, qui comprend deux parties :

- Une permutation S de tous les 256 octets possibles.
- Deux pointeurs de 8 bits, i et j, qui fonctionnent comme l'index d'un tableau. La clé de taille variable de Schedule RC4, qui est normalement comprise entre 40 et 256 bits, est utilisée pour initialiser la permutation.

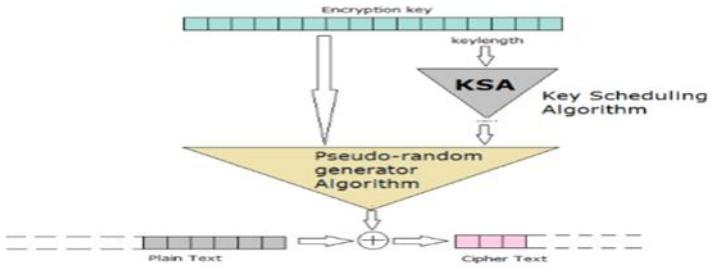


Figure II. 9 : Schéma de représentation RC4. [61]

Initialisation: un tableau [S] de 256 éléments est créé en l'initialisant avec des valeurs allant de 0 à 255 dans l'ordre croissant:

S [0] = 0, S [1] = 1,..., S [255] =255

Figure II. 10 Initialisation 1. [62]

De plus, un vecteur temporaire de longueur T (de longueur égale à S) est produit dans le but de recevoir la clé.

La clé K est simplement recopiée dans T si sa longueur, L, est égale à 256.

k est recopiée dans T jusqu'à atteindre la taille de T si elle est inférieure à 256 octets. utilisez le tableau d'octets de clé secrète [K].

2.4 Algorithme de planification de clé (Key Schedule Algorithm):

Pour créer la permutation initiale de (S), nous utilisons T. Nous pouvons exprimer la première permutation de S comme suit. Pour chaque cellule S[i] de S, celle-ci sera échangée avec une autre cellule de S conformément à un calcul basé sur la valeur contenue dans la cellule associée T[i].

```
Int j=0 ;
For (inti ;i<256 ; i++)
{
J = (j+S[i] + K[i] ) % 256 ;
Swap (S[i], S[j] ); // On échange les valeurs de S[i] et S[j]
}
```

Key Schedule Algorithm, ou KSA (les deux dernières lignes de code), est leur nom.

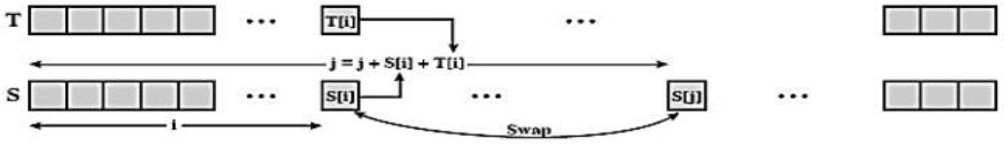


Figure II. 11 Initialisation 2 [62]

- ✓ **Génération du flux pseudo aléatoire (Pseudo-random generation algorithm):**

C'est la génération de flux pseudo-aléatoire. Une technique dépendant de la configura- tion courante de S sera utilisée pour échanger chaque S[i] avec un octet différent de S.

La procédure redémarre à la cellule S[0] après avoir atteint S[255]. La permutation initiale de S peut être illustrée par ce qui suit.

```
I = j = 0 ;
While (output_bytes)
{
 I = ( I+1 ) % 256 ;
J = (j + S [i]) % 256 ;
```

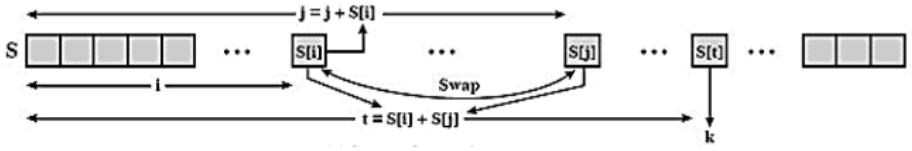


Figure II. 12 Génération de Flux RC4. [62]

L'utilisation de la valeur de k soit le même pour le chiffrement (avec l'octet suivant de texte en clair), soit pour le déchiffrement (avec l'octet suivant de texte chiffré). **[62]**

Main script

```
key = 'ASMA';

plaintext = 'Mission Accomplished';

Z = uint8(PRGA(KSA(key), size(plaintext,2)));

P = uint8(char(plaintext));

res = bitxor(Z, P);

%printing result in hex and Unicode res_in_hex=
mat2str(dec2hex(res,2)) res_in_unicode = char(res)
```

KSA (Key Schedule Algorithm):

```
function [ S ] = KSA( key ) key = char(key);

key = uint16(key);

key_length = size(key,2);

S=0:255;

j=0;

fori=0:1:255

j = mod ( j + S(i+1) + key(mod(i, key_length) + 1), 256);

S([i+1 j+1]) = S([j+1 i+1]);

end end
```

PRGA(Pseudo-random generation algorithm) :

```
function [ key ] = PRGA( S, n )

%S is the result from KSA function

%n number of characters to be encrypted i = 0;

j = 0;

key = uint16([]);

%each iteration we will append one key value while n> 0

n = n - 1;

i = mod(i + 1, 256);

j = mod(j + S(i+1), 256);

S([i+1 j+1]) = S([j+1 i+1]);

K = S( mod( S(i+1) + S(j+1)   , 256) + 1 );

key = [key, K];
```

```
end

end
```

II..2.6. L'algorithme JPEG :

La compression JPEG avec perte consiste à éliminer les redondances de façon permanente et basés sur l'algorithme de transformée en cosinus discrète DCT, l'algorithme JPEG combine le filtrage de fréquences avec la perception psycho-visuelle – La vision humaine est : Moins sensible au couleur qu'à l'intensité, peu sensible aux hautes fréquences spatiales.

II.2.6.1. L'algorithme proposé pour la compression JPEG :

JPEG (Joint Photographic Experts Group):

```
I = jpeg(I)('passport_jaishree.jpg'); %initial image T = I;
%backup of image

I=rgb2gray(I);

I=double(I);

[size1,size2]=size(I);

if(mod(size1,8)==0)

Ia=size1-8;

Else

Ia=size1-(8+mod(size1,8));

End

if(mod(size2,8)==0)

Ib=size2-8;

Else

Ib=size2-(8+mod(size2,8));

End

D_C=discrete_cosine(I,1,Ia,Ib);
```

```
Q=quantise(D_C,1,Ia,Ib);

Z=zig_zag(Q,1,Ia,Ib);

A2=[];

P2=[];

disp('This loop will run till the iteration value reaches')
disp(Ia*Ib/64);

fori=1:1:Ia*Ib/64 a=length(A2);

A2=encode(Z(i,:),A2);

P2=decode(A2,P2,a+1,i);

disp(i);

end

J=zig_zag(P2,2,Ia,Ib);

J=quantise(J,2,Ia,Ib);

I2=discrete_cosine(J,2,Ia,Ib);

I2=uint8(I2);

I=uint8(I); %final image on decoding
```

III. L'approche de Crypto-Compression proposée :

La nouvelle méthode de crypto-compression comprend quatre étapes principales:

Compression : Un DCT est appliqué suivie d'une quantification et zig zag + codage Huffman à une image pour réduire sa taille afin que faciliter le processus de compression.

Cryptage : crypter l'image sélectionnée par l'utilisateur avec la méthode de chiffrement Stream Cipher avec un algorithme RC4 (KSA, PRGA), qui va nous aider à continuer le reste du processus dans un contexte plutôt sécurisé.

Décryptage : restaurer l'image cryptée (pas encore claire), c'est après la sécurisation des données, vient le décryptage avec l'algorithme RC4.

Décompression : c'est la dernière étape se fait avec la DCT inverse (IDCT) pour reconstruire l'image originale chez le récepteur.

Schéma de Principe de l'approche de Crypto- Compression proposée :

Pour notre système on va essayer d'appliquer les deux techniques de compression et de cryptage L'approche introduite est basée sur deux algorithmes: un pour compresser et crypter l'image et l'autre pour reconstruire l'image dans un ordre où la compression sera en premier lieu, suivi du cryptage et le décryptage et enfin la décompression.

Donc l'architecture du système proposé avec deux variantes du système comme les 2 figures le montre :

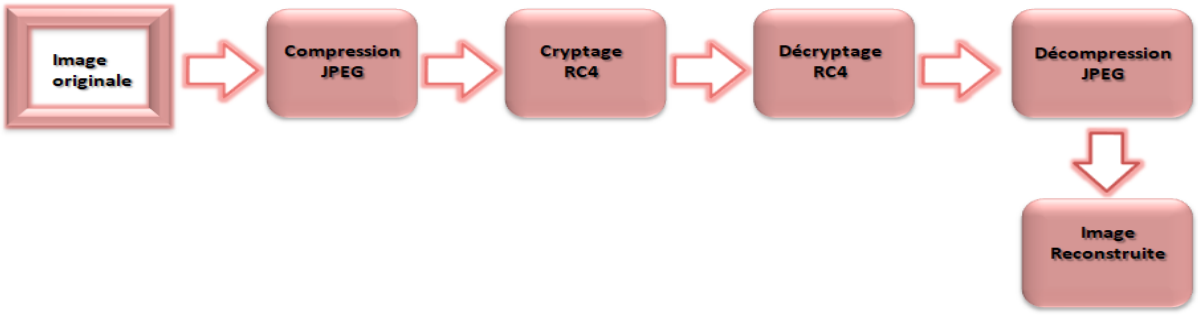


Figure II. 13 Première variante du Système de Crypto-Compression proposé

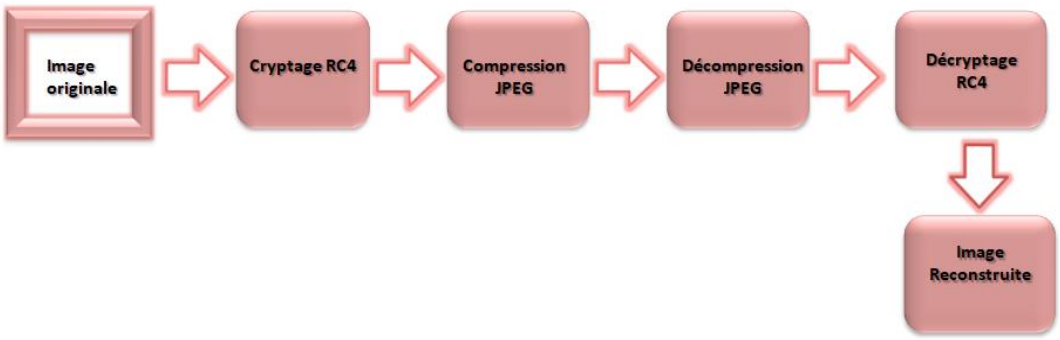


Figure II. 14 Deuxième variante du Système de Crypto-Compression proposé

- ✓ Les variantes du système sont basées sur l'ordre des techniques utilisées.

Conclusion

Au début de ce chapitre nous avons construire un tableau qui contient les avantages et les inconvénients des méthodes de compression d'images avec perte (irréversible), ensuite nous avons cité les travaux similaires dans le domaine des systèmes de crypto-compression d'image, et plus particulièrement dans le chiffrement par flot (RC4) et la compression d'image JPEG.

En revanche nous avons aussi discuté et détaillé la compression par transformation en cosinus discrète (DCT) que nous prendrons en compte dans notre, par donner une description simplifiée. Ensuite on a essayé de faire une étude sur l'algorithme RC4 et comment ça marche qui est associé à une compression avec perte de données JPEG. A première vue et théoriquement parlé les deux variantes de notre système ont le même impact sur l'image d'entrée.

Enfin on a terminé avec la présentation du système de crypto-compression proposé. Nous avons illustré l'approche de Crypto-Compression proposée avec un schéma. L'implémentation de l'algorithme du système proposé sera présentée dans le chapitre suivant

avec comparaison des différents résultats

CHAPITRE 03

RESULTAT

ET

DISCUSSION

Introduction

Notre travail consiste à développer un système de crypto-compression basé sur la compression JPEG (compression avec perte) et le cryptage de flux en utilisant une transformée en cosinus discrète(DCT) et un cryptage RC4 pour renforcer la sécurité.

Pour réaliser ce projet, nous avons utilisé le logiciel libre "MATLAB".

Dans notre approche on utilise des mesures de qualité qui sont indispensables pour l'évaluation des performances du système, à savoir le PSNR, MSE.

Dans ce chapitre, nous allons donner une description de l'environnement de travail qu'on a utilisé que ce soit côté matériel ou coté logiciel puis à dégager et élaborer les composants de notre système (application).

I. Environnement de travail

I.1. Matériels utilisés

L'implémentation de notre application « APP » a été réalisée sur un micro-portable fonctionnant sous le système d'exploitation Microsoft Windows 10 dont les performances sont les suivantes :

- Processeur : Intel Celeron N4000 Core™ i7-8565u de 8e génération.
- Fréquence de (Dual-Core 1.1 GHz / 2.6 GHz Rafale).
- Mémoire installé (RAM) : RAM de 4 Go de mémoire DDR4 2400 MHz.
- Type de système : système d'exploitation windows 10 (64 bits, processeur x64).
- Stockage :
- SSD 128/256 Go (SATA ou PCIe)+disque dur 1 To.
- Disque dur 500 Go/1 To/2 To.
- SSD M.2 PCle de 512 Go.

I.2. Langage de programmation

- **MATLAB :**

MATLAB est un langage de programmation simple signifie : « Matrix laboratory », développée par la société «The MathWorks ». il est un logiciel de manipulation et de programmation de données numériques qui est principalement utilisé dans le domaine des sciences appliquées avec de haute performance pour l'informatique technique.

- **L'interface de programme d'application MATLAB (API) :**

Nous avons utilisé la version R2016a dans notre projet.

I.3. Images de test :

Pour notre application, nous avons utilisé des images testes de différents types et de différentes tailles.

I.4. Paramètres d'évaluation :

Les paramètres les plus utilisés témoignés de la qualité des images ainsi que leurs tailles mémoire occupée sont le rapport signal sur bruit crête (PNSR), et le temps de compression/décompression, le temps de cryptage/décryptage.

II. 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.

II.1. Hiérarchie :

Notre interface présente une structure arborescente qui offre à l'utilisateur un bon suivi des applications effectuée et une meilleure représentation de ses données. Toutes les applications sont utilisées automatiquement à la fin de chaque session, la figure26 illustre l'organigramme du système.

L'application « APP », développée sous environnement MATLAB, consacre la première partie à la compression et le chiffrement des images basé sur la DCT, et pour le chiffrement nous appliquerons l'algorithme RC4. En deuxième partie nous faisant 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.

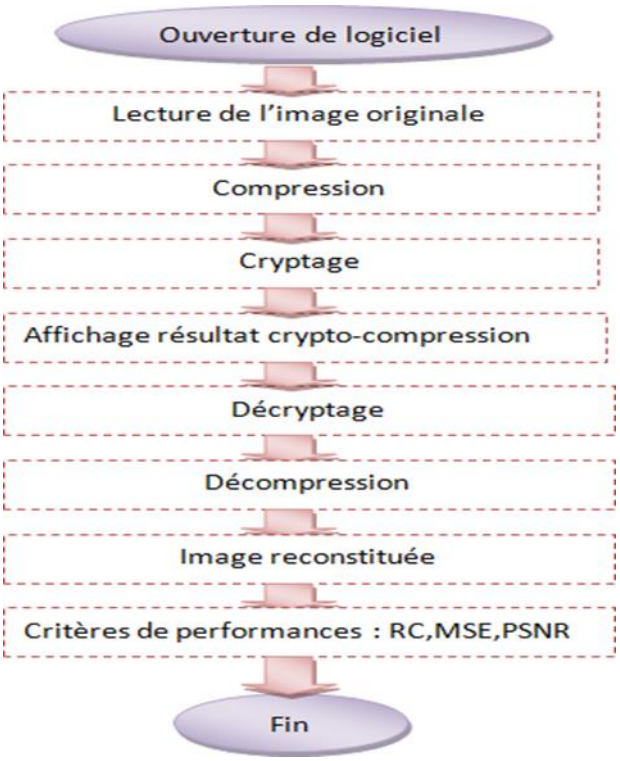


Figure III. 1 Organigramme du système.

III. Principe de fonctionnement de l'application :

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

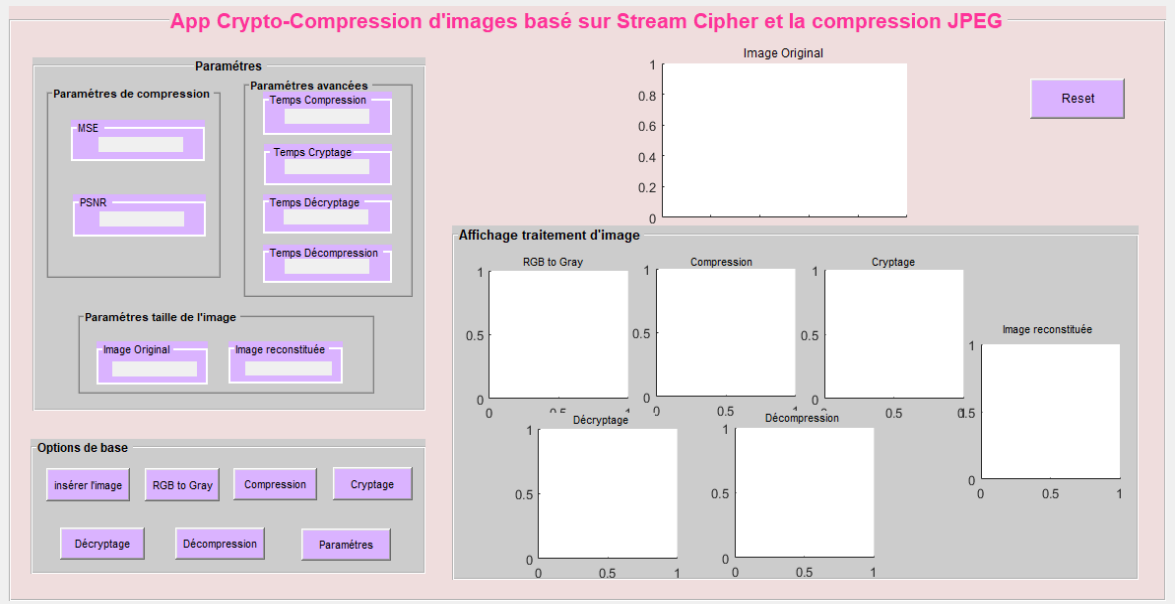


Figure III. 2 Interface du système

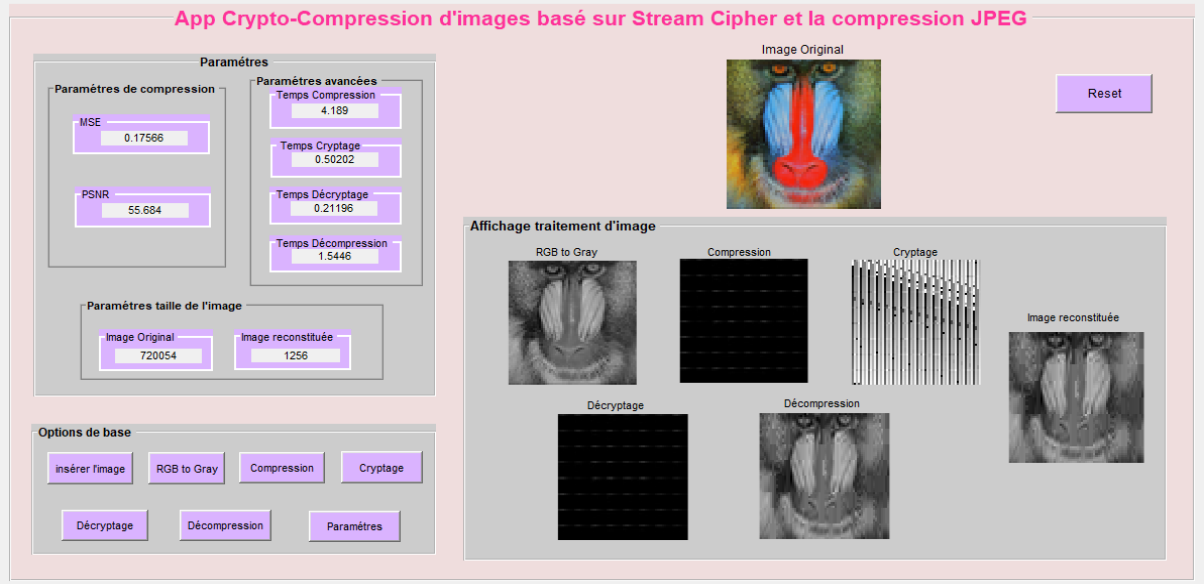


Figure III. 3 : Interface de l'application après exécution

III.1. Description des modules du système

- Module "Insérer l'image" : Permet de charger une image à partir de n'importe qu'elle endroit du PC et l'afficher dans le bouton «Image Original».
- Module de "RGB to Gray" : Permet de changer la couleur de l'image de RGB au gris et l'afficher dans le bouton «RGB to Gray».
- Module "Compression" : Pour compresser l'image choisi et l'afficher dans le bouton

- «Compression». Ce module est le plus important dans notre système; il contient la Conversion RGB en image YCBCR, appliquer la DCT, la quantification, codage zigzag, et le codage de Huffman», il permet de faire la compression DCT de l'image originale, l'algorithme est réalisé on MATLAB pour coder et décoder les images.
- Module "Cryptage" : Ce module permet de crypter l'image compressée par le système de cryptage RC4et l'afficher dans le bouton «Cryptage».La clé utilisé est la même clé pour le module de décryptage.
- Module "Décryptage" : Ce module permet de décrypter l'image crypté par appliquer l'algorithme de déchiffrement RC4. L'entrée de ce module est la sortie du module de précédent (cryptage) et l'afficher dans le bouton «Décryptage».La clé utilisé est la même clé pour le module de cryptage.
- Module "Décompression" : Il permet de décompresser l'image et afficher l'image reconstruite dans le bouton «Décompression».

  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.

  Il contient la conversion YCBCR en RGB et applique le décodage huffman, décodage zigzag et la quantification inverse « IDCT ».
- Module "Paramètres" : Ce module est très important pour tester les performances de l'algorithme utilisé, en se basant sur deux paramètres, l'erreur quadratique moyenne (Mean Square Error, MSE), le rapport crête signal sur bruit (Peak Signal to Noise Ratio, PSNR),

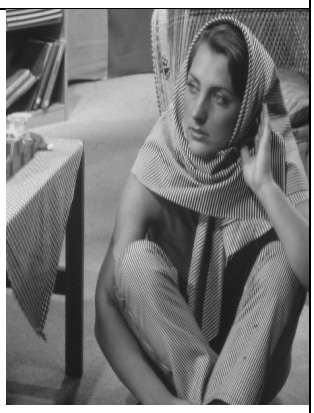
- On calcul ces paramètres : pour afficher MSE (Mean Square Error) dans le bouton «MSE», PSNR (Peak Signal to Noise Ratio) dans le bouton «PSNR».

- On a deux Paramètres de taille de l'image : pour afficher la taille de l'image originale dans le bouton «Image Original» et la taille de l'image reconstruite dans le bouton «Image reconstituée».

- On a quatre Paramètres avancées : pour afficher le temps de compression dans le bouton «Temps Compression», le temps de cryptage dans le bouton «Temps Cryptage», le temps de décryptage dans le bouton «Temps Décryptage», le temps de décompression dans le bouton «Temps Décompression».

- Module de "Reset": Ce module permet de supprimer toutes les champs dans l'interface et l'afficher dans le bouton «Image Original».

IV. Bibliothèque d'images

Nom : Lena Taille -Physique : 257 ko -Dimension : 128 X 128 -Type de fichier : BMP -Type de fichier après transformation : JPG		Nom : Cameraman -Taille Physique : 65.0 ko -Dimension : 128 X 128 -Type de fichier : BMP -Type de fichier après transformation : JPG	
Nom : baboon -Taille Physique :703 ko -Dimension : 128 X 128 -Type de fichier : BMP -Type de fichier après transformation : JPG		Nom : Barbara -Taille Physique : 257 ko -Dimension : 128 X 128 -Type de fichier : BMP -Type de fichier après transformation : JPG	
Nom : Clown -Taille Physique :257 ko -Dimension : 128 X 128 -Type de fichier : BMP -Type de fichier après transformation : JPG		Nom : BoatsColor -Taille Physique : 1.29 Mo -Dimension : 128 X 128 -Type de fichier : BMP -Type de fichier après transformation : JPG	

Nom : Pepperc -Taille Physique : 768 ko -Dimension : 128 X 128 -Type de fichier : BMP -Type de fichier après transformation : JPG		Nom : Venus -Taille Physique : 4.30 Mo -Dimension : 128 X 128 -Type de fichier : JPG -Type de fichier après transformation : JPG	

Table 2 Bibliothèque d'images

V. Tests expérimentaux

Pour faire l'exécution de notre application on exécute notre fichier de code qui contient des fonctions qu'elle utilise la compression JPEG (DCT) et le Stream Cipher (RC4) comme méthodes de compression et de cryptage d'image. Nous présentons dans ce qui suit, les résultats issus de notre application, sur chacune des images abordées :

V.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 Figure 32), en discutant sur les paramètres de performances comme : MSE, PSNR, le temps de cryptage et décryptage et le temps de compression décompression.

Le Tableau 03 présente les résultats obtenus.

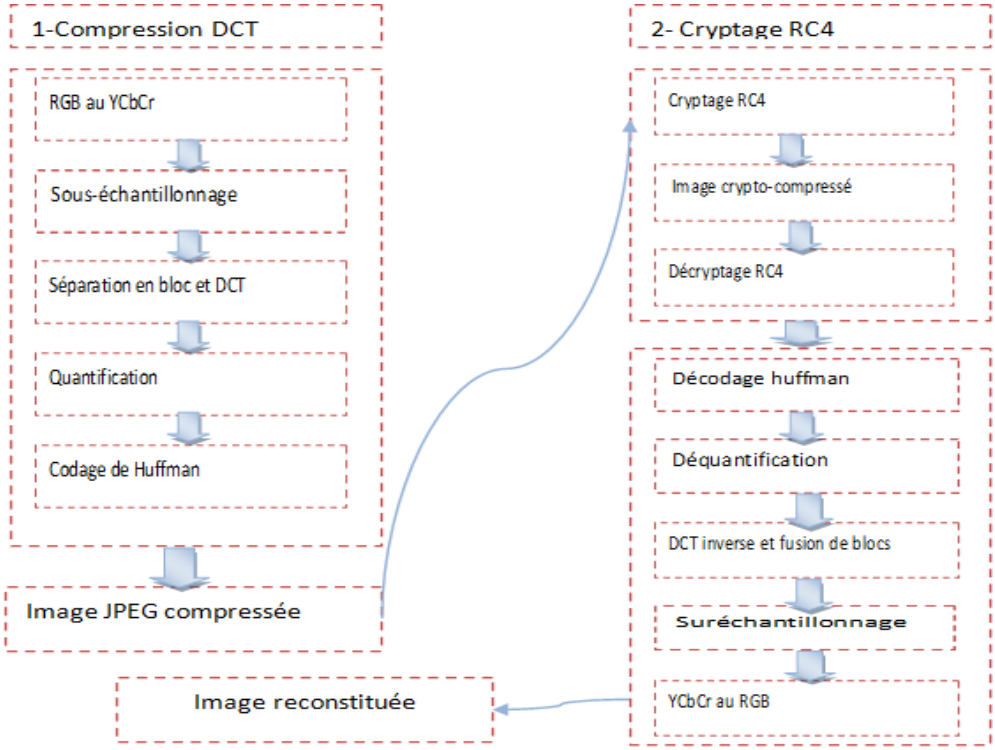


Figure III. 4 Schéma synoptique de notre système de la Première variante

V.1.1. Tests et résultats

Les images de la collection étudiée, sont compressées avec la compression DCT et chiffré suivant l'algorithme RC4 (Rivest Cipher 4).

V.1.1.2. Première variante

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.

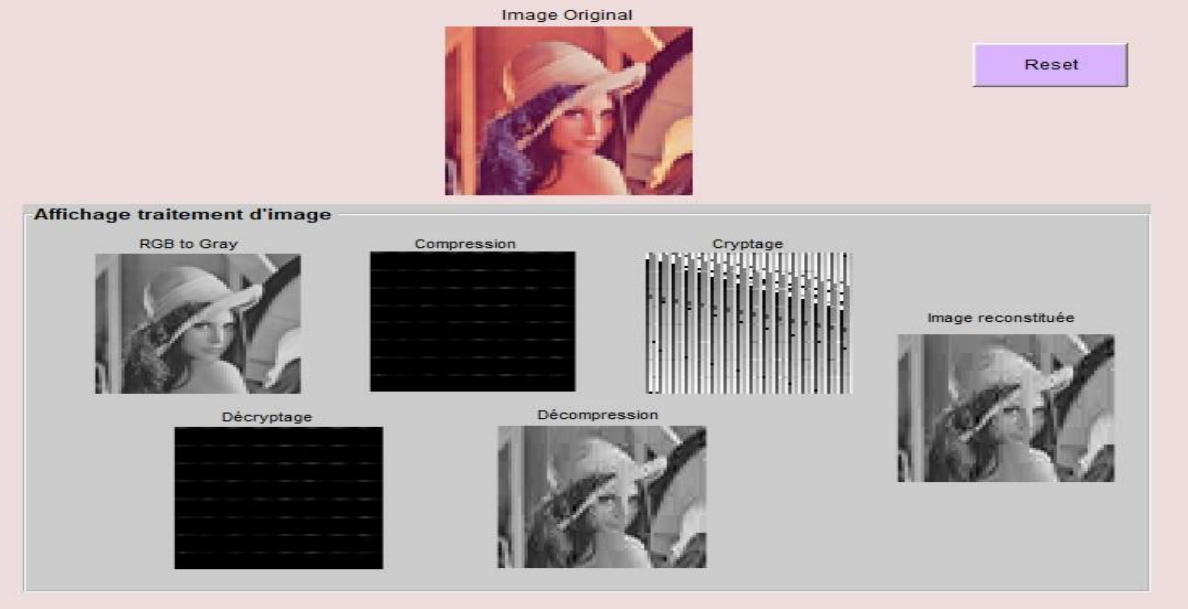
L'image			**Paramètres**					
-Nom **-TailClehapi Orig** **-Taille** **Rec**	Dimensi treo3ns	Ty pe	MSE (Err)	PSNR (db)	Tcom (s)	Tdeco m R(sé)su lt	Tcry at et(sd) iscu	**Tdecry ssion(s)**
-Airplane 768 KO **1301 O**	128*12 8	Bm p	0.5030 2	51.1149	8.132	5.569	2.2905	**0.57483**
-Lena **-768 KO** **-1392 O**	128*12 8	Bm p	0.2465 8	54.2112	2.0023	1.8834	0.35351	**0.091966**
Pepperc 768 KO **1521 O**	128*12 8	Bm p	0.2535 3	54.0905	0.9299 8	1.759	0.09618	**0.10011**
Baboon 703 KO **1256 O**	128*12 8	Bm p	0.1756 6	55.684	1.0804	0.6797	0.14759	**0.15152**
Monarch **1.12 MO** **1401 O**	128*12 8	Bm p	0.1825	55.5181	0.7784 9	0.6747 5	0.12631	**0.09714**
BoatsCol or **1,29 MO** **1403 O**	128*12 8	Bm p	0.2583 2	54.0092	0.6181 9	0.5263 7	0.1858	**0.11214**
Fruits 720 KO **1177 O**	128*12 8	Bm p	0.1455 8	56.4997	1.0274	0.6791 5	0.21795	**0.09825**
Cablecar 720 KO **1376 O**	128*12 8	Bm p	0.3011 4	53.3431	0.8029 6	0.5529 8	0.13092	**0.097041**

barbara c **1.18 MO** **1501 O**	**128*128**	**Bmp**	**0.20482**	**55.0172**	**0.56417**	**0.59185**	**0.13116**	**0.13298**

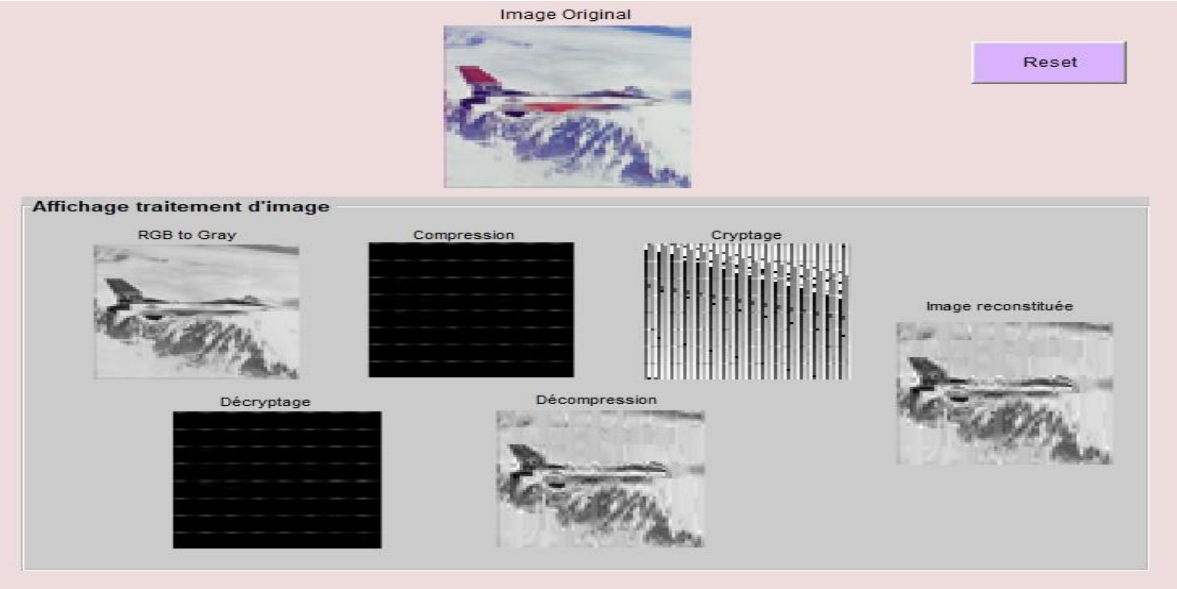
Table 3 Résultat d'application de notre système sur différentes images (Première variante)

V.1.1.1. Processus de traitement :

Test 01 : Lena.jpg :



Test 02 : Airplane.jpg



Test 03 : Pepperc.jpg :

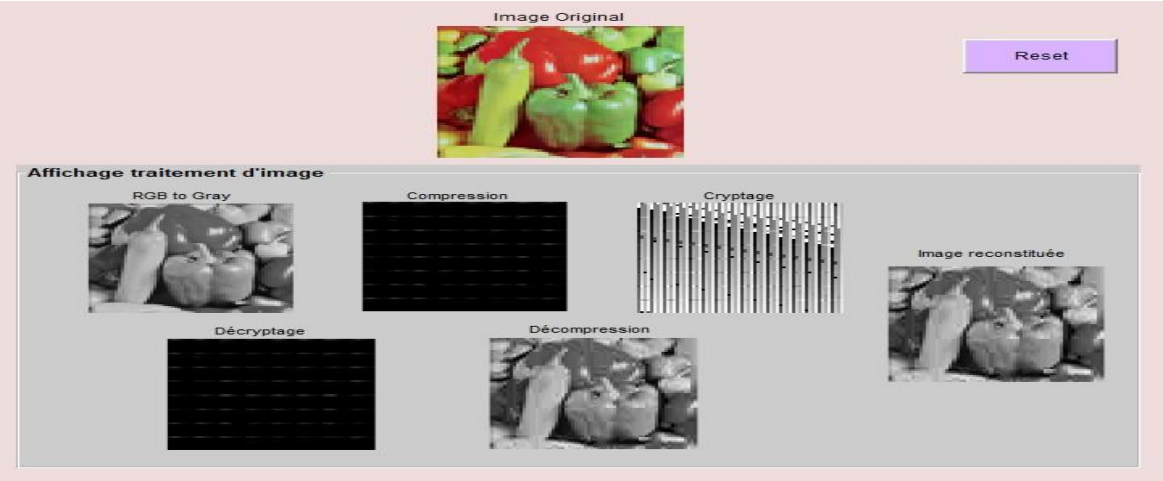


Figure III. 5 Processus de traitement Lena.jpg (Première variante)

5.1.1.3. Deuxième variante :

Nous essayons de changer l'ordre d'application des étapes de notre système, nous appliquons le cryptage dans le premier cas, puis la compression et la décompression et enfin décryptage. Nous avons utilisées les mêmes images pour le premier cas.

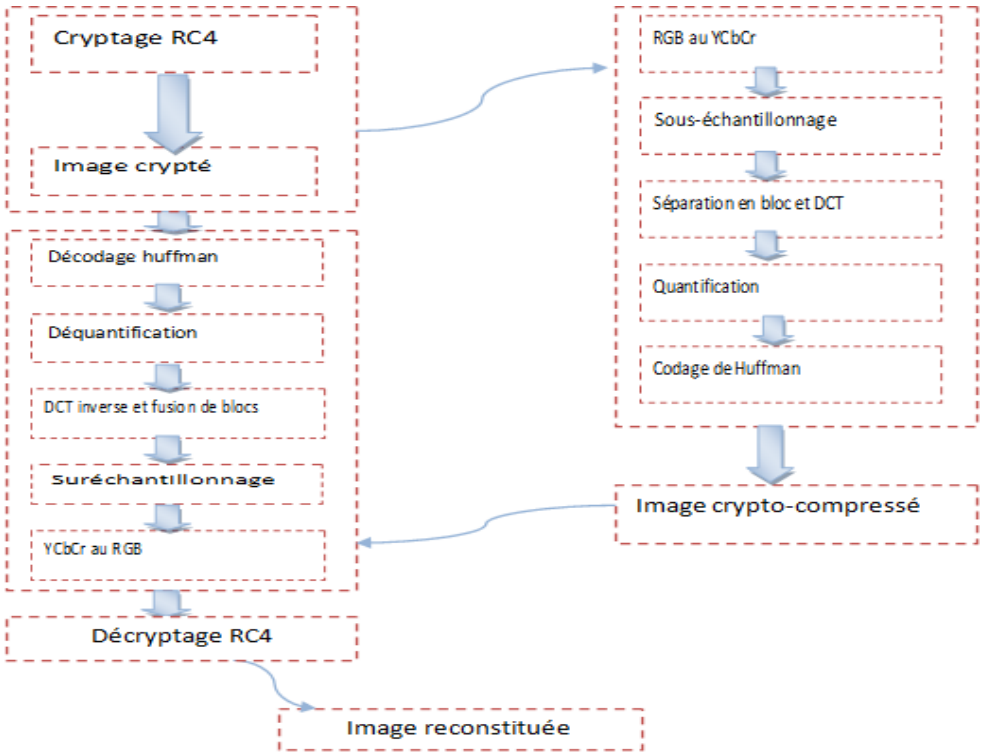


Figure III. 6 Schéma synoptique de notre système de la deuxième variante

V.1.1.4. Processus de traitement :

Test 01 : Lena.jpg :

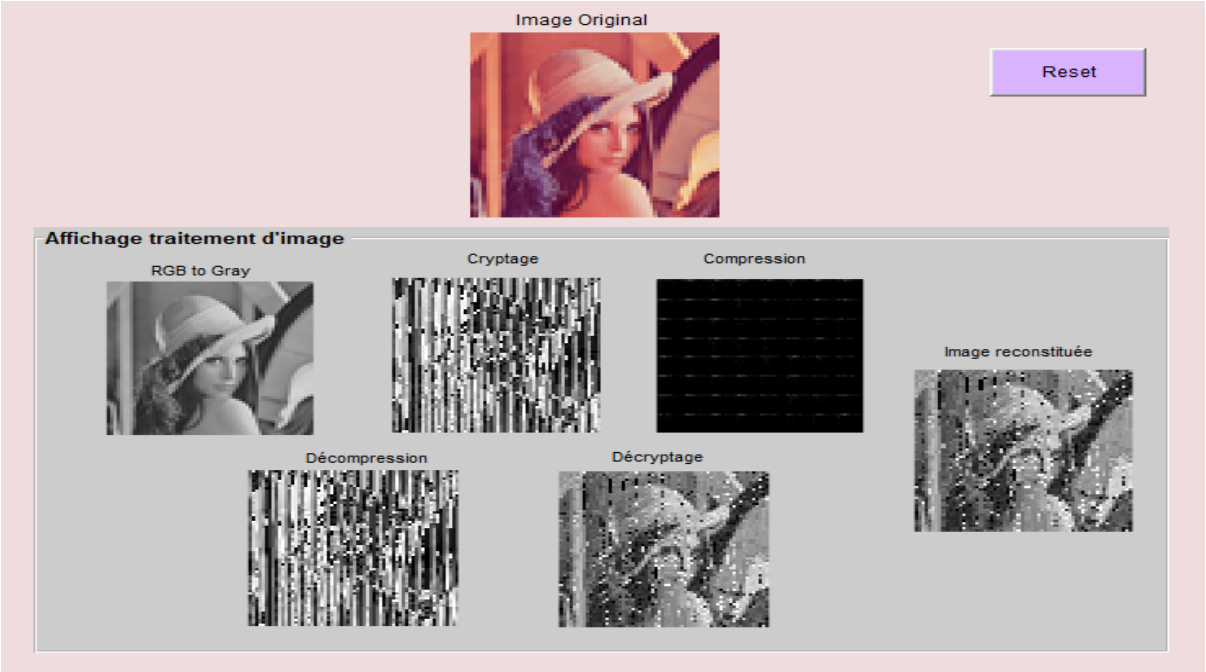


Figure III. 7 Processus de traitement Lena.jpg (Deuxième variante).

Test 02 : Airplane.jpg

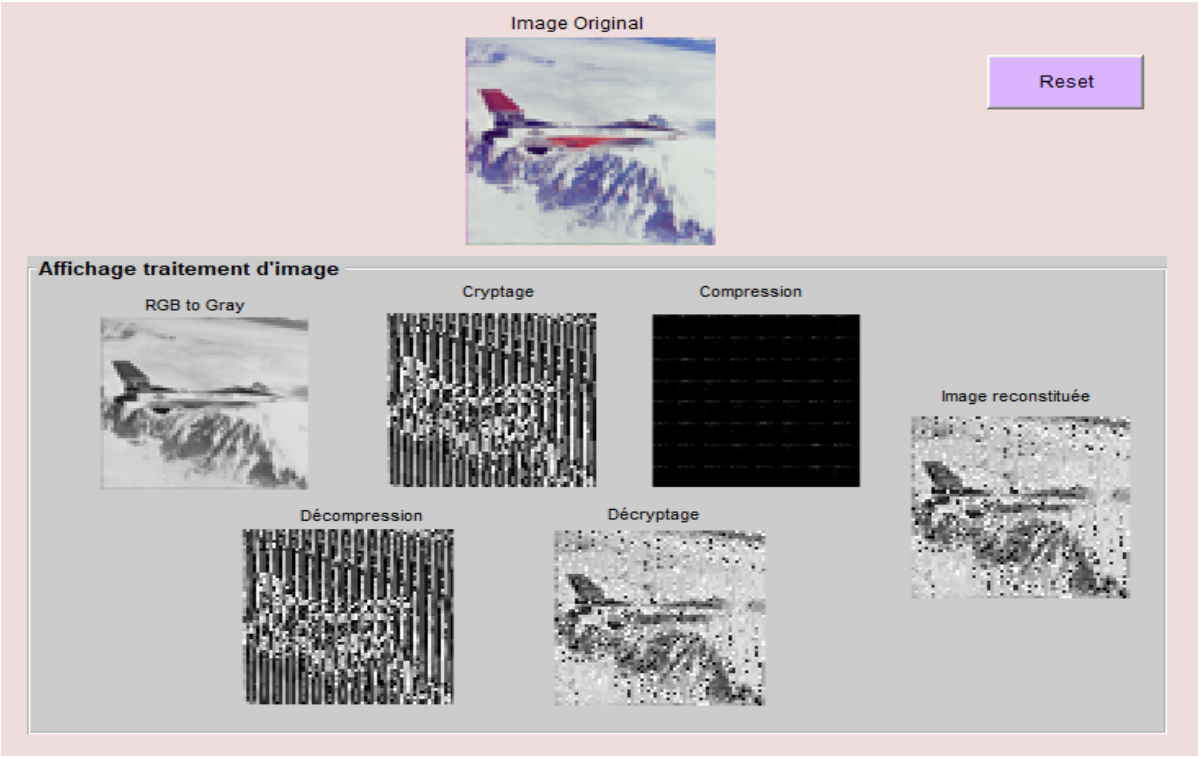


Figure III. 8 Processus de traitement Airplane.jpg (Deuxième variante)

Test 03 : Pepperc.jpg

Figure III. 9 Processus de traitement Pepperc.jpg (Deuxième variante

L'image			**Paramètres**					
-Nom **-Taille Orig** **-Taille Rec**	Dimensions	Type	MSE (Err)	PSNR (db)	Tcom (s)	Tdecom (s)	Tcry (s)	Tdecry (s)
-Lena **-768 KO** **-2058 O**	128*128	Bmp	0.1141	57.5581	0.78208	0.49794	0.18764	0.24051
-Airplane **768 KO** **2071 O**	128*128	Bmp	0.14806	56.4264	0.74171	0.69608	0.095307	0.21132
Pepperc **768 KO**	128*128	Bmp	0.12418	57.1902	0.75959	0.56733	0.09376	0.17795

2175 O								

Table 4 présente les résultats obtenus.

VI. Discussion

VI.1. Première variante de système

D'après les résultats présentés dans les autres travaux on remarque bien que :

La taille de l'image compressée est inférieure à celle de l'image originale, ce qui indique un gain d'espace minimal.

MSE proches de 0 indiquent une excellente qualité d'image. L'image compressée correspond étroitement à l'image d'origine avec un minimum de distorsion ou de bruit.

PSNR supérieures à 40 dB indiquent une excellente qualité d'image. L'image compressée ressemble beaucoup à l'original et la différence visuelle est minime.

Dans ce cas de notre système le chiffrement RC4 peut être utilisé pour chiffrer les données d'image, les rendant illisibles sans la clé de déchiffrement correspondante et l'utilisation de RC4 pour le chiffrement n'est pas recommandée en raison de ses faiblesses, Des taux de compression plus élevés introduisent une perte de qualité d'image. La quantité de données perdues et la dégradation de l'image dire que JPEG une compression avec perte très forte.

VI.2. Deuxième variante de système

D'après les résultats obtenu le chiffrement RC4 a agi sur la compression, donne des meilleurs résultats en termes de PSNR, MSE car MSE (l'erreur quadratique moyenne) diminue et PSNR augmente ce qui veux dire la fidélité de la compression JPEG mais il y'a un bruit ce qu'il donne une qualité mauvaise de l'image reconstruite.

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 quelques 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. Finalement on a discuté les résultats obtenus, et d'après les résultats présentés, on remarque bien que le chiffrement RC4 n'est plus considéré comme sécurisé pour la plupart des applications, pour sécuriser des images JPEG, il est recommandé d'utiliser des algorithmes de chiffrement modernes considérés comme sûrs, comme AES (Advanced Encryption Standard). AES est largement adopté et offre un haut niveau de sécurité pour la protection des données sensibles.

Conclusion générale

Conclusion générale

La compression des données à prendre un rôle encore plus importante à mesure que les réseaux de télécommunications se développent. Son importance est en croissance exponentielle avec l'utilisation des multitudes applications. En outre, cet échange de données en expansion utilise la cryptographie pour protéger les données transmises et assurer la sécurité en chiffrant les données compressées pour cela nous avons élaboré une technique de compression et de sécurité d'images pour faciliter l'archivage et assurer la confidentialité d'images.

Ce mémoire de master est consacré de visait à proposé la combinaison de deux techniques la compression et le cryptage, à savoir l'objectif principale est de mettre en œuvre un nouveau crypto-compression système basé sur une compression avec perte JPEG et un algorithme de cryptage RC4 fondé sur la méthode de chiffrement par flots (Stream Cipher).

Pour ce faire, nous avons commencé par un état de l'art des méthodes et techniques de compression et de cryptage existantes. On a combiné la compression et la cryptographie dans des ordres différents selon le contexte d'application de ce système.

Grâce aux différentes fonctions prédéfinies sur MATLAB nous avons fait des tests sur plusieurs images dans le but de voire la robustesse de l'approche proposée, et d'après les résultats obtenus, on a découvert que l'ordre de combinaison dans le système proposé est obligatoire et appliquer la compression avant le cryptage sert à valider notre première variante du système comme suit :

Compression → Cryptage → Décryptage → Décompression.

Donc dans ce cas les résultats ont montré que notre méthode fournit un PSNR satisfaisant, une sécurité suffisante et des résultats de confidentialité efficace avec un niveau de qualité d'image reconstruite visuelle acceptables.

On a essayé aussi d'inverser la compression et le cryptage comme suit :

Cryptage → Compression → Décompression → Décryptage

Pour voir l’impact de l’ordre des techniques sur les résultats, mais malheureusement ça n’a pas marché, On a remarqué qu'il y’a un bruit sur l’image reconstruite et la qualité de ce dernier est mauvaise.

Pour conclure, les techniques de compression avec perte tels que JPEG fournissent des taux de compression élevés, Pour faire la compression des images il faut préserver la qualité de base de l'image originale, c'est-à-dire un bon compromis entre le PSNR et le taux de compression.

De plus, les chiffrements par flots sont très rapides et efficaces, ils peuvent offrir la confidentialité des images compressées.

Ce travail m’a donné l’occasion de découvrir beaucoup de choses dans deux domaines aussi vaste qui sont la compression et le cryptage des images.

Perspectives :

D'après les études qu'on a faites dans notre projet de fin d’étude nous déduirons que le domaine de la compression est toujours ouvert pour l’amélioration, son but est d’arriver à une compression optimale en termes de temps de compression, de taux de bits et en termes de qualité de l’image reconstruite. Nous pensons au futur d’enrichir le volet lié à l'optimisation de notre système crypto-compression car les recherches se poursuivent pour le développer et l’améliorer afin d’atteindre de meilleurs résultats à partir de s'adapter à la nature des données à compresser et utiliseront l’intelligence artificielle.

Un autre perspective est de faire une extension de notre système crypto-compression dans le domaine de la vidéo (images animées) est tout à fait possible afin d'améliorer davantage la robustesse.

Bibliographie

[1]: Y. Benlcouiri · M. Benabdellah · M. C. Ismaili · A. Azizi ,'' Crypto-Compression of Images Based on The ANNs and The AES Algorithm''Received: 10 July 2011/ Accepted: 23 July 2011.

[2]: HAMIDA Bariza, ''Système de crypto compression d'images basé sur le Block Cipher et la compression par Ondelettes'', Université Cheikh Larbi Tebessi Tébessa, 2021/2022.

[3]: Memoire Online - Compression d'image animmée par le codage EZW 3D - Guenidi Sif Eddine, Kebairi Athmane.

[4]: Implementation_dunenvironnement_parallele_wsefsc.pdf.

[5]: ZITOUNI Athmane, Ondelettes et techniques de compression d'images numérique, 2012/2013.

[6]: BELGUESSOUM Aissa , Compression des données avec la nouvelle méthode VLC adaptative temps réel, UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU, 2012/2013.

[7]: F. LUBIN, "La compression audio-numerique," Enseignement des Métiers de la Communication.

[8]: M Aldossarin'' Nouvelle méthode optique de compression et de cryptage simultanés des images (fixes/vidéo) pour les systémes télécommunication''. Sciences de l'ingénieur [physics].UBO, 2014.Français.

[9]: Caméras industrielles avec compression d'images JPEG intégrée | Baumer Switzerland

[10]: Formats d'images | Images et documents | Nmédia (nmedia.ca).

[11]: Format Jpeg : avantages et défauts du plus répandu des formats photo (avecunphotographe.fr).

[12]: Question du C2i : Quel format compressé pour les images convient le mieux à la photographie d'un coucher de: soleil sur la mer ? (c2i-revision.fr).

[13]: Vincent Itier, William Puech, "How to recompress a JPEG crypto-compressed image?", LIRMM, UMR 5506 CNRS, University of Montpellier.

[14]: La compression de données - Le format JPEG (univ-mlv.fr).

[15]: Donald NOKAM KUATÉ, Thèse de doctorat de l'Université Paris-Saclay préparée à l'Université Paris Sud,''Cryptographie homomorphe et transcodage d'image/vidéo dans le domaine chiffré'', Thèse présentée et soutenue à Palaiseau, CEA LIST - Centre Nano-INNOV, 14 décembre 2018.

[16]: NEGOUDI AHMED AMMAR -BOUZGAG MABROUK, ''Conception d'un application de tatouage numérique "Watermark" robuste aux imges JPEG'', Université Kasdi Merbah Ouaregla, 2017/2018.

[17] : Nabila BRAHIMI, Développement et implémentation des algorithmes de copression d'images basés sur des transformaées entiéres,UNIVERSITE FERHAT ABBAS-SETIF ,13/01/2011.

[18] : BOUMARAF eps CHAOUCH Messaouda, ''Crypto-compression Des Images D'Empreintes Digitales'',Université de sciences et de la technologie Houari BOUMEDIENE ,08/07/2009.

[19] : Chérif TAOUCHE,''Implémentation d'un Environnement Parallèle pour la Compression d'Images à l'aide des Fractales'', Université Mentouri Constantine, 2005.

[20] : CHIBANI Hidaya, ''Optimisation d'un algorithme de compression d'images en utilisant des métaheuristiques'', Université L'arbi Ben M'hidi d'Oum El Bouaghi.

[21] : TORCHE Ridha et BOUAKAZ Moussa, Evaluation des images chiffres par l'algorithme AES-128 et AES-256, Master Académique, Université Larbi Tébessi – Tébessa, 2020/2021.

[22] : Bobby Jasuja, Abhishek Pandya,''Crypto-Compression System: An Integrated Approach using Stream Cipher Cryptography and Entropy Encoding'', Department of Information Technology Medicaps Institute of Science and Technology, Indore, India,

International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 21, April 2015.

[23]: Crypto_CM_chap1.pdf.

[24]: Dr. BENIDRIS Fatima zohra,'' Cryptographie'', UNIVERSITE ABDELHAMID IBN BADIS MOSTAGANEM, Juin, 2020.

[25] : Bousnoubra Yasser - Hamada Aymen , '' La cryptographie des images numériques par la carte logistique chaotique'', Université 8Mai 1945 – Guelma, Septembre 2020.

[26] : Aissam Djemaa Aissa Boubednikh ,'' Réalisation d'un Système de Cryptage des Images Numérique basé sur le Chaos'', Université Mohamed Sadik BENYAHIA de Jijel, 2021.

[27] : BADAOUI Youcef Islem,'' Un système de crypto-compression d'images basé sur le Block Cipher et la compression fractale'', Université Larbi Tébessa - Tébessa, 13 Juin 2020.

[28] : TOLBA Bouzid, ''Cryptage d'images pour une sécurité élevée de transmission sur le réseau '', Université Larbi Tébessi – Tébessa , 15/09/2020.

[29] : Guenaél Renault, POLSYS LIP6/UPMC/INRIA, Les bases de la Cryptologie.

[30] : Benzerrouki Aïcha Essedikia, Guemidi Zoulikha,''Application des systèmes chaotiques à la cryptographie '', UNIVERSITE Dr. TAHAR MOULAY SAIDA, Septembre 2018.

[31] : BOUSSAYOUD Ryma Dr. BENHADJI Chehla - CHIOUKH Labiba - AFER Doha - BOUCHAIR Djihan - TITI Nesrine,'' Cryptage / Chiffrement & Tatouage des données numériques'', Université Mohamed Seddik Benyahia – Jijel , 2019/2020.

[32] : Mohammed BENABDELLAH,'' OUTILS DE COMPRESSION ET DE CRYPTOCOMPRESSION : APPLICATIONS AUX IMAGES FIXES ET VIDEO'', UNIVERSITE MOHAMMED V-AGDAL FACULTE DES SCIENCES RABAT,le 20 Juin 2007 à 16h30.

[33] : S. Ftérich et C. Ben Amar, '' Crypto-Compression d'Images Fixes Par la méthode de Quadtree optimisée et AES'', Ecole Nationale d'Ingénieurs de Sfax (ENIS).

[34] : L.H. Abed et M.N. Rashid et O.M. Al Okashi ,‘’PARTIAL CRYPTO-COMPRESSION FOR CLOUD-BASED PHOTO STORAGE USING DCT AND DAUBECHIES 4 WAVELET’’,Department of Computer Systems, Anbar Technical Institute, Middle Technical University, Baghdad, Iraq, September 2022.

[35] : Mr AMRANE Mourad, ’’ Crypto compression d’image par cryptage partiel’’, Université Mouloud MAMMERI de Tizi-Ouzou, Septembre 2015.

[36] : William Puech, José Marconi Rodrigues. Crypto-Compression d’Images Médicales par Cryptage Partiel des Coefficients DCT. JSTIM: Journées SciencesTechnologies et Imagerie pour la Médecine, Mar 2005, Nancy (France), pp.149-150. fflirmm-00106477.

[37] : Pauline Puteaux, Zichi Wang, Xinpeng Zhang, William Puech. Hierarchical High Capacity Data Hiding in JPEG Crypto-compressed Images.EUSIPCO 2020 - 28th European Signal Processing Conference, Jan 2021, Amsterdam (virtual), Netherlands.pp.725-729, ff10.23919/Eusipco47968.2020.9287376ff. ffhal-03161511f.

[38] : DJEFFALI Khaled,‘’Un système de crypto-compression d’images basé sur le Stream Cipher et la compression RLE’’, Université Larbi Tébessa - Tébessa,Juin 2020.

[39] : Jean-Claude Borie, William Puech, Michel Dumas. Crypto-Compression Using TEA’s Algorithm and a RLC Compression. MediaNet’04: Intelligent Access to the Multimedia Documents on the Internet, Nov 2004, Tozeur, Tunisia. pp.5-16. fflirmm-00108826f.

[40] : Mohammed M. Siddeq1 & Marcos A. Rodrigues 1,’’ A novel Hexa data encoding method for 2D image crypto-compression ‘’, Multimedia Tools and Applications (2020),Received: 26 July 2018 /Revised: 29 July 2019 /Accepted: 22 September 2019 /Published online: 12 December 2019.

[41] :IYAD HRAINI , MOUSA FARAJALLAH , NABIL ARMAN , AND WASSIM HAMIDOUCHE ‘’Joint Crypto-Compression Based on Selective Encryption for WMSNs’’, Received November 3, 2021, accepted November 25, 2021, date of publication November 30, 2021, date of current version December 13, 2021,College of Graduate Studies, Palestine Polytechnic University, Hebron 00970, Palestine 2Department of Computer Engineering, Palestine Polytechnic University, Hebron 00970, Palestine 3Department of Computer Science and Information Technology, Palestine Polytechnic University, Hebron 00970, Palestine

4Department of Electrical Engineering, Univ. Rennes, INSA Rennes, CNRS, IETR-UMR 6164, 5700 Rennes, France.

[42] : BOUAMER Bouhafs et DEHANE Youcef,‘’Compression D’Image Par La Méthode TCD (Transformée En Cosinus Discrète)’’, Université de Ghardaïa Faculté des Sciences et Technologies,25/06/2019.

[43] : REZKALLAH Meriem et YOUSFI Noura, ‘’Compression d’images par transformée en ondelettes’’, UNIVERSITE DE MSILA, septembre 2020.

[44] : Boucif Samira et ToutahMariem ‘’Compression d’images : Compression entre la méthode DCT et les ondelettes’’, Université AKLI MOhANd OULHADJ – Bouira, 2018-2019.

[45] : Bensennia Sara ‘’ COMPRESSION HYBRIDE DES IMAGES MEDICALES’’, Université Abou BakrBelkaïd de Tlemcen ,25mai2016.

[46] : Mr. Lasgaa Ismail, ‘’ Synthèse et Etude comparative sur les méthodes de compression d’images DCT et DWT’’, Université Abou BakrBelkaid– Tlemcen,02/05/2018 à 10h.

[47] : MANSOURI Dou el kefel ‘’LA COMPRESSION DES IMAGES 3D’’, SCIENTIFIQUE UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE D'ORAN - MOHAMMED BOUDIAF- USTO-MB, 2011.

[48] : BadisAmarouche, ‘’Compression et Cryptage des vidéos : application en IoT’’, Université Mohamed Seddik BEN YAHIA de Jijel, 2020-2021.

[49] : Ziani Leila,’’ Compression des images numeriques par la technique des ondelettes (JPEG2000)’’, Université Akli Mohand Oulhadj–Bouira, 2016- 2017.

[50] : ISSAAD Kahina, KHOUDI Hayet ’’Compression temps réel des pages web ‘’, Université Mouloud Mammeri, Tizi-Ouzou Faculté de Génie Electrique et d’Informatique, 2012.

[51] : Sid Ahmed‘’ Compression des images médicales fixes en vue d’une interprétation: Application au télédiagnostic ’’, Faculté de Mathématiques et Informatique, 2017/2018.

[52] : BOUAMER BELKHIR'' Compression d'images par la méthode décomposition en valeurs singulières'', Université de Ghardaïa, 2021/ 2022.

[53] : SAITI Hamza, BEN KHELIF Abdelghafour ''APPROCHE HYBRIDE DCT ET DWT POUR LA COMPRESSION D'IMAGES '', Université de Ghardaïa, 2020/2021.

[54] : AMEUR Nacima '' Etude comparative entre deux méthodes de compression VLC et Huffman'', Université Mouloud Mammeri, Tizi-Ouzou, 2010/2011.

[55] : Belkebir Djalila '' Insertion d'une signature dans une image basée sur la projection d'une vue en rotation'', Université Larbi Ben M'hidi Oum El Bouaghi,28/29 Juin 2011.

[56] : AHMED Oussama'' DEVELOPPEMENT ET EVALUATION DES TECHNIQUES CLASSIQUES DE COMPRESSION'', UNIVERSITE MOHAMED BOUDIAF - M'SILA, JUIN 2016.

[57] : BENABDELAZIZ Naima, NOUFEL Zakaria ''Compression d'image numérique par la transformée d'ondelette'', Université Saad Dahleb Blida 1,11 juillet 2021.

[58] : Mr. KARIM MEZZOUG '' TRAITEMENT ET ANALYSE DES IMAGES NUMERIQUES'', Université Ibn Khaldoun – Tiaret, 2019/2020.

[59] : Rémi Giraud ''Introduction au traitement d'images, Chapitre 6 : Compression'', 2021-2022.

[60] : Pierre Nerzic, ''Codage et compression d'images et de vidéo'', automne/hiver 2007.

[61] : Aimeur Akram ''Conception et implémentation d'un système hybride pour la sécurité de données : application aux images numériques'', UNIVERSITE MOHAMED BOUDIAF - M'SILA, 2016 /2017.

[62] : GHEMBAZA Hayat KAID SLIMANE Imane '' Cryptographie symétrique des messages dans un réseau P2P sur JXTA'', Université AboubakrBelkaïd – Tlemcen –, 03/ 07/2017.

[63] : Mounir Boukadoum ''Compression de signaux numériques'', Basé sur L. Tan, le standard G.726 de l'UIT et plusieurs sources sur Internet, université de québec à montréal.