الجمهورية الجزائرية الديمقراطية الشعبية
Republique Algerienne Democratique Et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة العربي التبسي – تبسة
Université Larbi Tébessi – Tébessa –
Faculté des Sciences et de la Technologie
Département de génie électrique

MEMOIRE

Présenté pour l'obtention du **diplôme** de **Master Académique**

En : Télécommunications

Spécialité : Réseau et Télécommunication

Par : TORCHE Ridha et BOUAKAZ Moussa

Sujet

Evaluation des images chiffres par l'algorithme AES-128 et AES-256

Evaluée, le / / , devant le jury composé de :

Dr Mahmoud MAAMERI	**MCA**	**Président**
Dr Riad SAIDI	**MCA**	**Rapporteur**
Dr Tarek BENTAHAR	**MCB**	**Examinateur**

Promotion : 2020/2021

Dédicaces

A mes chers parents,

Pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

A mes chères sœurs,

Pour leurs encouragements permanents, et leur soutien moral

A mes chers frères,

Pour leur appui et leur encouragement,

A toute ma famille pour leur soutien tout au long de mon parcours universitaire,

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fuit de votre soutien infaillible,

Merci d'être toujours là pour moi.

Torche Et Bouakaz

Remerciements

Avant tout, je remercie le bon Dieu qui m'a éclairé le chemin et m'a donné la patience et le courage pour réaliser ce travail.

Mes profonds remerciements vont à mon encadrant ***Dr. SAIDI RIAD.*** *Qui a accepté d'encadrer mes travaux pour ses encouragements, ses conseil et sa Disponibilité. Nous avons été satisfaites de votre qualité exceptionnelle de bonne Enseignante, merci de nous avoir guidés avec patience et d'avoir consacré autant Heuré pour les corrections de ca manuscrit ; nous ne pouvons, madame, que Sincèrement vous exprimé notre respect et notre gratitude*

Nous tenons à remercier à la présidente de jury de notre mémoire ***Dr.MAAMERI MAHMOUD.***

Toute ma considération à l'égard de ***Dr.BENTAHER TAREK.*** *Qui m'a fait l'honneur de juger le présent travail.*

Je remercie ma famille et surtout mes parents pour leur soutien moral, leurs encouragement set leur patience durant les étapes difficiles de ce travail.

Merci à toutes les personnes qui ont accepté de m'aider

Liste des symboles

AES: Advanced Encryption Standard

BMP: Bitmap

CBC: Cipher Block Chaining

CFB: Choper FeedBack

CTR: CounTeR

DES: Data Encryption Standard

ECB: Electronic Code Book

GIF: Graphics Interchange Format

JPEG: Joint Photographic Experts Group

JFIF: JPEG Interchan ge File Format.

LZW: Lempel Ziv Welch

MSE: Mean Squared Error

NIST: National Institute of Standards and Technology

Nr : Nombre de rondes

Nr : Nombre de columns

OFB: Output FeedBack

PNG: Portable Network Graphics

PSNR: Peak Signal to Noise Ratio

RC: Rivest Cipher

RGB: Red Green Blue

RSA: Rivest Shamir Adelman

SSIM: Structural Similarité Mesure

SBox: Substitution Box

TIFF: Tagged Image File Format

XOR : Exclusive OR

Liste Des Tableaux

Liste des figures

ملخص

في الوقت الحاضر ، يصعب الاستغناء عن استخدام وسائل الكمبيوتر لتبادل المعلومات سواء كانت صوتًا أو صورًا أو غيرها. غالبًا ما تكون وسائل الاتصال هذه مرتبطة بشبكات مفتوحة عبر روابط لاسلكية غير آمنة. هذا يجعل المعلومات المتبادلة أكثر عرضة للخطر. في الواقع ، يسمح تطور الأنظمة المضمنة بتطوير أنظمة تشفير معقدة بشكل متزايد. يبحث هذا العمل في جانب التشفير ، الذي يقع في إطار أمان الصور ، بواسطة خوارزميات AES. طابع هذا العمل هو تقييم جودة الصور المشفرة بواسطة خوارزمية AES-128 وخوارزمية AES-256 ، باستخدام تشفير وضع CBC و OFB لضمان السرية. من خلال استغلال القياسات المختلفة مثل SSIM و MSE و PSNR من خلال نظام تشفير الكتلة. تشير النتائج التي تم الحصول عليها في هذا العمل إلى أن وضعي التشفير مع نوعي الخوارزمية AES-128 و AES-256 يعطوننا نتائج جيدة لتأمين الصور ذات الامتدادات المختلفة.

الكلمات الرئيسية: التشفير العام ، تشفير الكتلة ، النظام المتماثل ، خوارزمية AES-128 ، خوارزمية AES-256، SSIM، MSE، PSNR ، الرسم البياني.

Abstract

Nowadays, it is difficult to do without the use of computer means for the exchange of information, whether it is voice, images or others. Often these means of communication are linked to open networks via unsecured wireless links. This makes the information exchanged more vulnerable. In fact, the evolution of embedded systems allows the development of increasingly complex crypto-systems.

This work looks at the cryptographic side, which falls within the framework of image security, by AES algorithms. The character of this work is the evaluation of the quality of the images encrypted by the AES-128 algorithm and the AES-256 algorithm, using CBC and OFB mode encryption to ensure confidentiality. By exploiting different metries such as SSIM, MSE, PSNR through a block cipher system. The results obtained in this work indicate that the two encryption modes with the two types of the algorithm AES-128 and AES-256 give us good results for securing images of different extensions.

Keywords: Cryptography generality, block encryption, symmetric system, AES-128 algorithm, AES-256 algorithm, SSIM, MSE, PSNR, histogram.

Résumé

A Nos jours, il est difficile de s'en passer de l'utilisation des moyens informatiques pour l'échange de l'information, que ce soit de la voix, des images ou d'autres. Souvent ces moyens de communication sont liés à des réseaux ouverts via des liaisons sans fil non sécurisés. Ce qui rend l'information échangée plus vulnérables. En fait, l'évolution des systèmes embarqués permet de développer des crypto-systèmes de plus en plus complexes.

Ce travail se penches sur le côté cryptographique, qui s'inscrit dans le cadre de la sécurité des images, par l'algorithmes AES. Le caractère de ce travail consiste à l'évaluation de la qualité des images chiffres par l'algorithme AES-128 et l'algorithme AES-256, utilisant de modes de chiffrement le CBC et le mode OFB pour assurer la confidentialité. En exploitant différentes métries tel que SSIM, MSE, PSNR à travers un système de chiffrement par bloc. Les résultats obtenus dans ce travail nous indiquent que les deux modes de chiffrement avec les deux types de l'algorithme AES-128 et AES-256 nous en donnes de bons résultats pour la sécurisation des images de différentes extensions.

Mots –clés : Généralité sur la Cryptographie, chiffrement par bloc, système symétrique, Algorithme AES-128, Algorithme AES-256, SSIM, MSE, PSNR, histogramme.

Table de matière

Chapitre I : Généralités sur la cryptographie

Introduction Générale

Introduction générale

Durant le long de l'histoire, l'humanité a tenté de transmission des informations d'une manière sécurisée. Le chiffrement d'information a été utilisé comme instrument de sécurisation pour des stratégies militaires et des échanges de données secrètes. Le portage sécurisé d'information est nécessaire et énormément utilisé dans le monde numérique.
Les améliorations technologiques récents dans les réseaux informatiques, tel que l'Internet, ont conduit à un accroissement de l'utilisation des ordinateurs et des systèmes de communication pour partager les données, où dans de nombreuses applications une connexion sécurisée est nécessaire.

Les images transmises sur ces réseaux sont des données particulières du fait de leur quantité importante d'information. La transmission des images rassemble un nombre important de problèmes.

Nous citons, par exemple la confidentialité, l'authentification et l'intégrité des données, ce qui a conduit les chercheurs à la cryptographie.

La cryptographie joue un rôle important dans la protection des données échangées contre les attaques et diminue le risque de vol de l'information et donne un haut niveau de sécurité par ses deux types de cryptographies symétrique et asymétrique.

Nombreuse technique de chiffrement sont présentées pour répondre aux exigences de la sécurité ; nous trouvons parmi elles, l'algorithme public symétrique AES (Advanced Encryptions Standard) qui a prouvé de nos jours sa robustesse contre les différents types d'attaques, et l'algorithme IDEA (International Data Encryption Algorithm). Notre crypto système est applique pour la transmission des images, pour assurer la confidentialité, puisque notre objectif est l'évaluation de la qualité des images déchiffres par deux algorithme AES-128 et AES-256.

Notre travail a pour objectif de faire une évaluation de la qualité de quelque type d'images chiffres par deux crypto système l'un basé sur le chiffrement avec algorithme AES -128 l'autre sur avec algorithme AES 256, en utilisant des métries tel que MSE, le PSNR, SSIM et GSSIM, ainsi que l'histogramme.

Dans ce mémoire, nous avons partage notre travail en trois chapitres :

- Le premier chapitre donne des généralités sur la cryptographie, nous avons commencé par donnes quelque définissions sur la cryptologie et son historique, nous avons, aussi fourni un aperçu des différentes techniques de la cryptographie et la cryptanalyse.
- Le deuxième chapitre donne une description détaillée de l'algorithme AES ainsi que de ces transformations.
- Le troisième chapitre présente les résultats de Simulation et évaluations, qui est consacré à des techniques de cryptage pour la transmission sécurisée des images basé sur les chiffrements avec AES-128 et AES-256 avec les deux modes CBC et OFB, ainsi que la Comparaison entre AES-128 et AES-256

Finalement nous terminerons notre travaille par une conclusion, ainsi qu'une perspective.

CHAPITRE I : GENERALITES SUR LA CRYPTOGRAPHIE

I.1. Introduction

La sécurité informatique est un domaine très important dans notre vie qui protège nos informations et nos données dans les réseaux de communication, donc pour garantir la sécurité d'informatique on utilise la cryptographie.

La cryptographie est l'art du secret désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles.

Dans ce chapitre, nous donnons des généralités et des définitions, ainsi que des explications les terminologies de base de la cryptographie, puis nous allons parler sur leurs objectifs et ces différents types. Enfin, on termine par les types des attaques.

I.2. Généralités sur la Cryptologie

La cryptologie est la science du secret, cette science est née de la volonté des hommes de partager certaines informations uniquement avec quelques personnes [1].

La cryptologie du grec *kruptos* « secret, caché » et *logos* « discours » qui embrasse à la fois la cryptographie et la cryptanalyse. Elle se partage entre la cryptographie, qui inclut la conception des mécanismes destinés à assurer les fonctions suivantes : confidentialité, intégrité, authentification et traçabilité (non répudiation), et la cryptanalyse dont le but est de déjouer les protections ainsi mises en place [2].

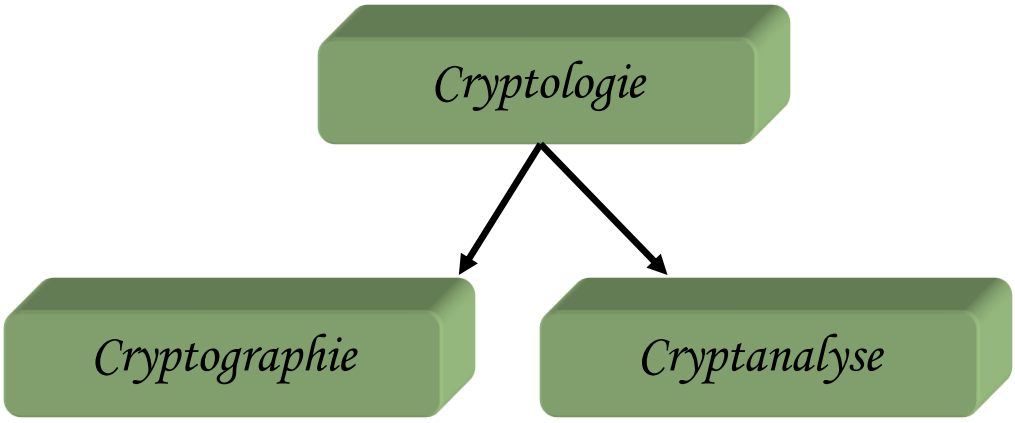


Figure I.1 : Les branches de la cryptologie.

I.3. Historique de la Cryptographie

L'origine de la cryptographie remonte sans doute aux origines des hommes, dès que ceux-ci apprirent à communiquer. Alors, ils durent trouver des moyens d'assurer la confidentialité d'une partie de leurs communications. On rapporte son utilisation en Egypte il y a 4000 ans.

Cependant, la première attestation de l'utilisation délibérée d'un moyen de chiffrement des messages vint de la Grèce vers le VI^{eme} siècle avant J.C, et se nomme le *scylate*, qui était un bâton sur lequel l'expéditeur enroulait une bandelette autour et écrivait longitudinalement le message sur le bâton, puis déroulait la bandelette et l'expédiait au destinataire. Sans la connaissance du diamètre du bâton qui jouait le rôle de clé, il était impossible de déchiffrer le message. Plus tard, les romains adoptèrent un chiffrement qui consistait en une substitution mono alphabétique simple en décalant de trois lettres de l'alphabet. Cette technique était connue sous le nom de chiffre de *Jules César* [1].

Puis, pendant des siècles, on assista à la mise au point de plusieurs techniques de chiffrement mais qui étaient pour la plupart limitées aux besoins de l'armée et de la diplomatie ; on peut citer parmi ces techniques [2]:

- En 1918 le système ADFGVX a été mis dans le service par les allemands à la fin de la première guerre mondiale et Arthur Scherbius fait breveter sa machine à chiffrer *Enigma*.
- En 1929 : Lester S. Hill invente le chiffre de Hill. C'est un chiffre polygraphique où l'on utilise des matrices et des vecteurs.
- En 1960 : le code ASCII est adopté comme standard. Il permet le codage de caractères sur 8 bits, soit 256 caractères possibles.

Dans les années 70, le développement de l'informatique et l'émergence des réseaux de communications modifient la situation. La sécurité des nouveaux moyens de communications doit être assurée. C'est pourquoi, en 1975, le Bureau Américain des Standards propose de normaliser un système de chiffrement : le DES (Data Encryption Standard) qui est un système de chiffrement par blocs de 64 bits basée sur l'utilisation d'une clé secrète identique pour le chiffrement et le déchiffrement dont la taille est de 56 bits.

Plusieurs organismes ont analysé le DES et l'ont trouvé mathématiquement sain mais la longueur de sa clé a été jugée trop faible pour des applications de haute sécurité. Ainsi le DES a été remplacé par le nouvel algorithme AES (*Advanced Encryption Standard*) qui a des clés de longueur plus importante (128, 192 et 256 bits) ainsi que des blocs de taille plus grande (128 bits contre 64 pour DES) [2].

Le standard de chiffrement AES fut adopté en 2000 par le NIST en remplacement du DES.

Ce chiffrement est constitué de substitutions, de décalages, de « ou exclusif » et de multiplications dans un corps fini de polynômes fixes ; ces opérations sont élémentaires, simples et rapides à calculer.

Il permet de crypter des blocs de 128, 192 ou 256 bits en utilisant des clés symétriques de 128, 192 ou 256 bits. Le choix de la taille de la clé et de la taille des blocs sont indépendants, il y a donc au total 9 combinaisons possibles. Ceci laisse une plus grande flexibilité à l'utilisateur de l'AES en fonction du niveau de sécurité et de la vitesse de calcul désirés.

Parallèlement en 1976, *W. Diffie* et *M. E. Hellman* publient leur célèbre papier « New *Directions in Cryptography* ». Ils y décrivent les fondements de la cryptographie asymétrique moderne permettant de résoudre en partie les problèmes d'échange des clés secrètes. Ce type de crypto système utilise une clé secrète pour le déchiffrement, alors que c'est une clé publique qui est employée pour chiffrer le message.

La première application pratique de la cryptographie asymétrique est le système **RSA** proposée en 1978 par R.L. Rivest, A. Shamir et L. Adleman. Ce système est d'ailleurs le crypto système asymétrique le plus répandu à l'heure actuelle [3].

I.4. Crypto systèmes classiques

Un crypto système est un ensemble de primitives cryptographiques utilisées pour fournir des services de sécurité de l'information. Le terme est souvent utilisé pour décrire le cryptage.

Les premiers algorithmes utilisés pour le chiffrement d'une information étaient assez rudimentaires dans leur ensemble et ils sont trop simples pour offrir la moindre sécurité. Pour cacher la substance d'un texte, ils utilisent la substitution de caractères

par d'autres ou les transposer dans des ordres différents. De ce fait, la confidentialité de l'algorithme de chiffrement était donc la pierre angulaire de ce système pour éviter un décryptage rapide. On appelle généralement cette classe de méthodes : le chiffrement **à usage restreint** [2].

a- Cryptographies par substitution

La substitution signifie que chaque lettre (ou groupe de lettres) est substituée par une (ou groupe) lettre(s), chiffre(s) ou symbole(s). Le déchiffrement consiste à effectuer la substitution inverse. Selon la façon de substituer [2], on quatre catégories :

- ✓ **Substitution simple (mono-alphabétique)**

Le codage par substitution mono-alphabétique (ou encore les alphabets désordonnés) est le plus simple à imaginer. Chaque lettre dans le message clair est remplacée dans le message chiffré par une autre lettre différente unique pour toutes les occurrences de celle-ci. Dans la littérature, plusieurs algorithmes ont été proposés, entre autres, nous citons : le chiffre de César, le chiffre Atbash, le carré de Polybe, etc [2].

- ✓ **Substitution poly-alphabétique**

Au lieu de remplacer une lettre par une même autre lettre dans tout le message comme dans la substitution simple, elle est remplacée périodiquement par différentes lettres. L'exemple le plus fameux de chiffre poly-alphabétique est sans doute le chiffre de Vigenère, qui a résisté aux cryptanalyses pendant trois siècles [2].

- ✓ **Substitutions homophoniques**

Au lieu d'associer un seul caractère crypté à un caractère en clair, on dispose d'un ensemble de possibilités de substitution de caractères dans lequel on choisit aléatoirement.

Par exemple : C=>S, K ; G=>G, J ; Q=>K ; S=>S, Z ; PH=>F ; …etc [2].

- ✓ **Substitution par polygrammes**

Au lieu de substituer des caractères, on substitue par exemple des digrammes : groupe de deux caractères. Pour se faire, deux moyen sont utilisés : soit par table (Chiffre de Playfair) ou par transformation mathématique (Chiffre de Hill) [2].

b- Cryptographies par transposition

Elle consiste à permuter les lettres du message à chiffrer entre elles, afin de le rendre inintelligible [2].

Plusieurs variations de transposition sont utilisées, parmi eux on trouve:

- ✓ **Transposition simple (à base matricielle)**

Elle consiste à écrire le texte en clair dans une matrice de *n* colonnes (une lettre dans chaque case), et ensuite de construire le texte chiffré en prenant les lettres à partir de cette matrice colonne par colonne. La clef dans ce cas est le nombre *n* [2].

- ✓ **Transposition avec substitution simple**

L'idée dans ce cas est de combiner la transposition avec une substitution simple. Il s'agit ainsi de chiffrer le message clair par une méthode de substitution simple, et en suite d'en appliquer une transposition. Une autre astuce est souvent utilisée qui consiste à appliquer une fonction de permutation sur l'ordre d'arrangement des colonnes. On cite à titre d'exemple : le chiffre de DELASTELLE [2].

I.5. Principe de Chiffrement et Déchiffrement

Le chiffrement est un moyen qui permet de transformer une donnée intelligible à une donnée incompréhensible à l'aide d'une clé de chiffrement afin de protéger l'information contre l'accès non autorisé.

Le déchiffrement est le moyen qui permet la reconstruction du message en clair à partir du message chiffré en utilisant la clé de déchiffrement [4]. La figure I.2 ci-dessous illustre le principe de chiffrement et de déchiffrement

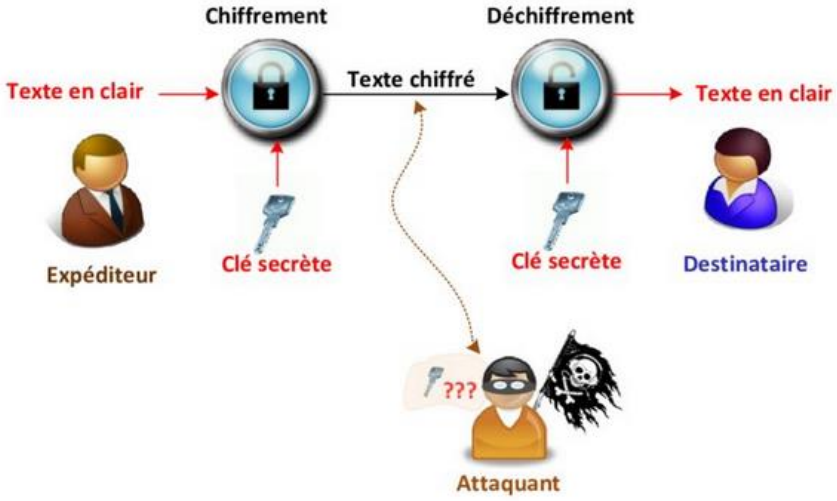


Figure I.2 : Les branches de la cryptologie [5].

I.6. Chiffrement par Blocs

Un chiffrement par bloc est une méthode de cryptage qui décompose le texte en clair en chaînes (appelés blocs) d'une longueur fixe *t*, et le chiffrement se fait bloc par

bloc (un bloc à la fois). Pour les algorithmes de chiffrements par bloc modernes, la taille typique de blocs est 64 bits, assez grande pour empêcher l'analyse et assez petite pour être pratique [4].

I.7. Réseau de Feistel

Un réseau de Feistel qui est représenté par la figure I.3, est une méthode générale de transformation de n'importe quelle fonction en une permutation. Il a été inventé par Horst Feistel pour le design de Lucifer et popularise par le DES. On le retrouve dans bon nombre d'algorithmes de chiffrement par bloc dont CAST-128, Blowfish ou encore RC5. Concrètement, dans ce schéma, un bloc de texte en clair est découpe en deux ; la transformation est appliquée lors de ce tour à une des deux moitiés, et le résultat est combine avec l'autre moitié par un ou exclusif.

Les deux moitiés sont alors inversées pour l'application du tour suivant. Deux tours complémentaires forment un cycle. Lorsqu'un cycle est complet, chaque bit du bloc de texte à traiter a été modifié une fois [6].

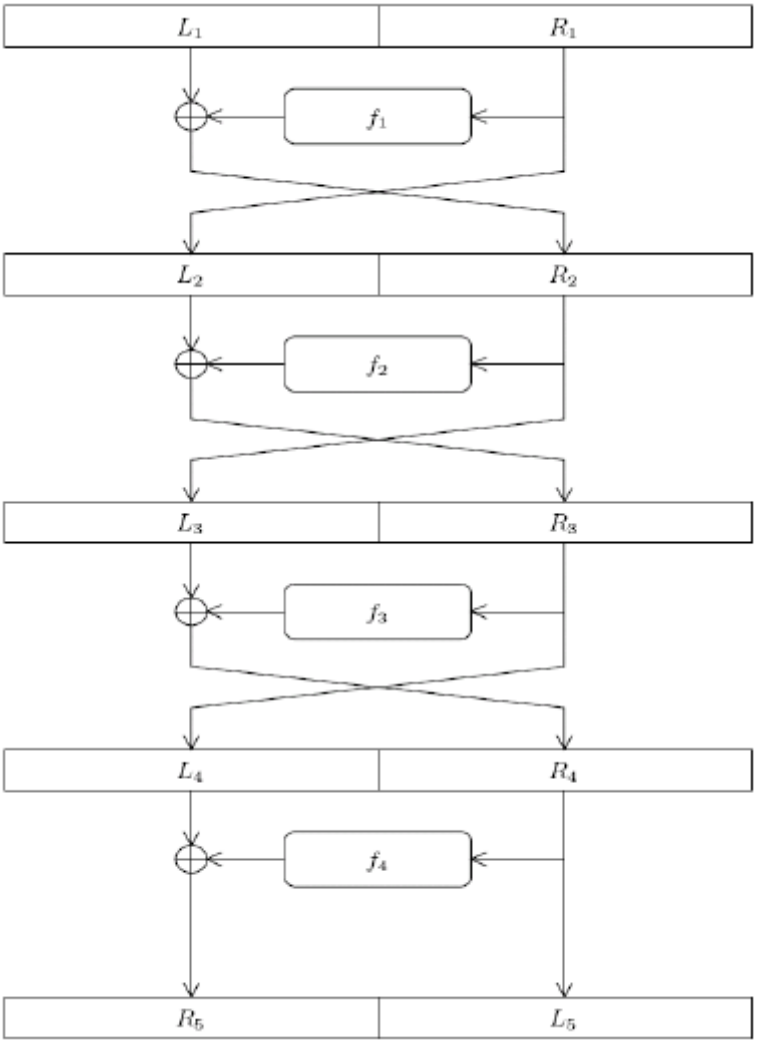


Figure I.3 : Un schéma de Feistel a quatre tours [5]

I.8. Notion de sécurité

La sécurité se base sur quatre critères essentiels qui sont :

1. **La confidentialité**

La confidentialité permet d'assurer que seuls les utilisateurs autorisés ont accès aux informations. Nous devons protéger nos informations confidentielles. Une organisation doit se prémunir contre les actions malveillantes qui mettent en danger la confidentialité de ses informations [4].

2. **L'intégrité**

L'information doit être changée constamment. L'intégrité signifie que les changements doivent être effectués uniquement par des entités autorisées en utilisant les mécanismes autorisés [4].

3. L'authentification

L'authentification garantit simplement que la personne est bien celle qu'elle prétend être, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être [4].

4. Le non repudiation

La non-répudiation permet de s'assurer qu'un message transféré a été envoyé et reçu par les bonnes parties. La non-répudiation est un moyen de garantir que l'expéditeur d'un message ne peut pas plus tard nier l'envoie du message et que le destinataire ne peut pas nier la réception du message [4].

I.9. Algorithmes de chiffrement et clefs

Le chiffrement est l'action de transformer une information claire, compréhensible de tout le monde, en une information chiffrée, incompréhensible. Le chiffrement est toujours associé au déchiffrement, l'action inverse. Pour ce faire, le chiffrement est opéré avec un algorithme à clé publique (asymétrique) ou avec un algorithme à clé privée (symétrique) et la combinaison entre les de type qui s'appelé le chiffrement hybride, la clef s'agit du paramètre impliqué et autorisant des opérations de chiffrement/ou déchiffrement [6].

Parmi les algorithmes les plus rependues l'AES (Advanced Encryption Standard), aussi connu sous le nom de Rijndael, qui est un algorithme de chiffrement symétrique. Il remporta en octobre 2000, le concours AES, lancé en 1997 par le NIST et devient le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis. Nous utilisons dans notre crypto système, l"AES pour le chiffrement des images Météosat MSG, pour les nombreux avantages qu'il représente en comparaison avec d'autres algorithmes symétriques [6].

I.9.1. Chiffrement asymétrique

Le concept du chiffrement asymétrique a été créé à partir des problèmes liés au chiffrement symétrique.

Le premier problème est la distribution des clés. Le partage initial d'une clé secrète peut être fait en utilisant un canal sécurisé qui peut être mis en œuvre, par exemple, en utilisant un service de messagerie fiable. En outre, cette option est susceptible d'être

indisponible pour plusieurs entités qui n'ont pas les moyens de partager les clés de cette manière. Un procédé plus pragmatique qui permet à deux parties de partager une clé est l'utilisation d'un centre de distribution de clés.

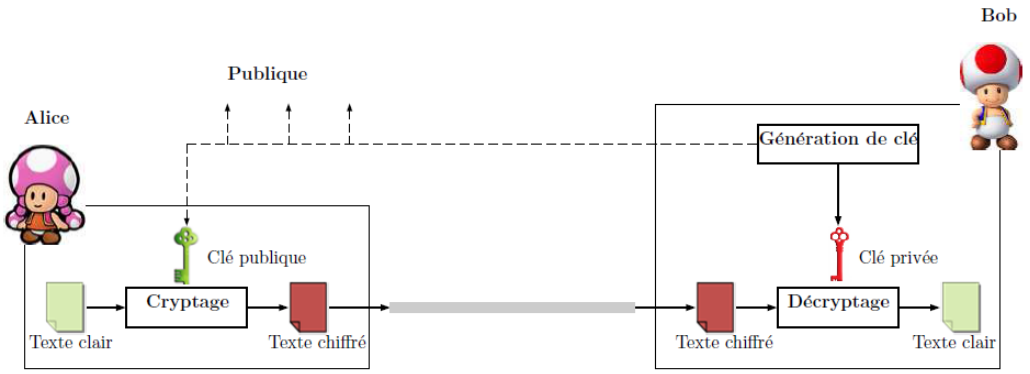
Le deuxième problème est les signatures numériques. Si l'utilisation de la cryptographie est à se généraliser, et pas seulement dans des situations militaires, les messages électroniques et les documents auraient besoin de l'équivalent de signatures utilisées dans les documents papier.

Dans les systèmes de chiffrement asymétrique chaque entité *A* a une clé publique *e* et la clé privée correspondante *d*. Dans les systèmes sécurisés calculer *d* à partir de *e* est mathématiquement impossible. Si une entité *B* souhaite envoyer un message *m* à *A*, elle doit obtenir une copie authentique d'une clé publique *e*, elle utilise la transformation de cryptage pour obtenir le texte chiffré, ensuite elle transféra le message chiffré à *A*. Pour décrypter le message chiffré *A* appliqué la transformation de décryptage afin d'obtenir le message d'origine *m* [4].

$$E_e(M) = C \quad \text{(I.1)}$$

$$D_d(C) = M \quad \text{(I.2)}$$

Le chiffrement asymétrique est illustré dans la figure (I.4)



FigureI.4 : Le chiffrement asymétrique [5].

I.9.2. Chiffrement symétrique

Le chiffrement symétrique est aussi appelé chiffrement à clé secrète. La clé de chiffrement peut être calculée à partir de la clé de déchiffrement et vice versa. En général, les clés de chiffrement et de déchiffrement sont identiques. L'émetteur et le destinataire doivent se mettre d'accord préalablement sur une clé qui doit être gardée secrète, car la sécurité d'un tel algorithme repose sur cette clé [4].

Le chiffrement à clés publique et le chiffrement symétrique présentent chacun des avantages. Par exemple, le temps de chiffrement/déchiffrement du chiffrement à clé publique est supérieur à celui du chiffrement symétrique. Un des problèmes principaux du chiffrement symétrique est l'échange préalable de la clé secrète. Le chiffrement à clé public peut être préféré pour générer de petites séquences comme des signatures ou des clés secrètes pour le chiffrement symétrique. Le chiffrement symétrique peut être préféré pour chiffrer des grandes quantités de données [4].

Le chiffrement et le dé chiffrement d'un message *M* en utilisant la clé secrète *K* avec un algorithme symétrique sont désignés par les équations suivantes [4]:

$$E_K(M) = C \tag{I.3}$$

$$D_K(C) = M \tag{I.4}$$

Le chiffrement symétrique est illustré dans la figure (I.5)

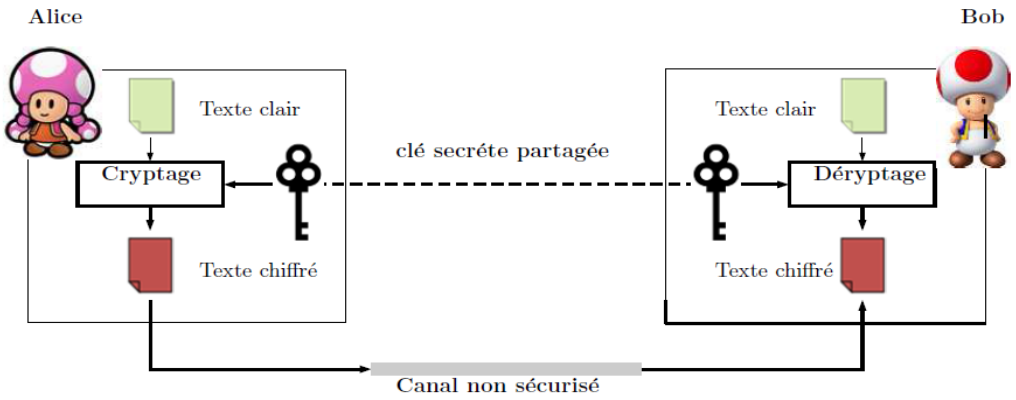


Figure I.5 : Le chiffrement symétrique [5].

I.9.3. Chiffrement hybride

Le chiffrement asymétrique est beaucoup plus lent que le chiffrement symétrique qui brille par sa rapidité. En revanche, cette dernière souffre d'une grave lacune ; assurer une transmission secrète de la clé. Pour pallier ce défaut et cumuler les avantages des deux méthodes on a fait recourt au chiffrement hybride. On code tout d'abord les données avec une clé privée dite *clé de session*, ensuite cette clé est cryptée à l'aide d'une clé publique classique. Comme la clé est courte, on utilise l'algorithme asymétrique puisqu'il prend peu de temps. En revanche, chiffrer l'ensemble du message avec un algorithme asymétrique serait plus lourd. Il suffit ensuite d'envoyer le message chiffré avec une clé privée et accompagné de cette

dernière chiffrée avec une clé publique. Le destinataire procède inversement, il commence à déchiffrer la clé symétrique avec sa clé privée pour obtenir la clé de session, qui sera utilisée, par la suite, via un déchiffrement symétrique pour retrouver le message original.

Ainsi, les performances seront améliorées en associant la rapidité des systèmes de chiffrement symétriques et la bonne sécurisation des systèmes de chiffrement asymétriques.

Alors le chiffrement hybride est une combinaison des fonctionnalités du chiffrement asymétrique et le chiffrement symétrique.

PGP est un système de chiffrement inventé par *Philip Zimmermann*, un analyste informaticien. Lorsqu'un utilisateur chiffre un texte avec **PGP**, les données sont d'abord compressées. Cette compression des données permet de réduire le temps de transmission par modem, d'économiser l'espace disque et, surtout, de renforcer la sécurité cryptographique.

Cette méthode de chiffrement associe la facilité d'utilisation du chiffrement asymétrique à la vitesse du chiffrement symétrique. Le chiffrement symétrique est environ 1000 fois plus rapide que le chiffrement asymétrique.

Le chiffrement asymétrique résout le problème de la distribution des clés. Utilisées conjointement, ces deux méthodes améliorent la performance et la gestion des clés, sans pour autant compromettre la sécurité. Il est très rapide et sûr ce qui le rend quasiment impossible à cryptanalyse [2].

I.10. Classification des algorithmes

La figure I.6 suivant illustre les différentes classes de la cryptographie [2] :

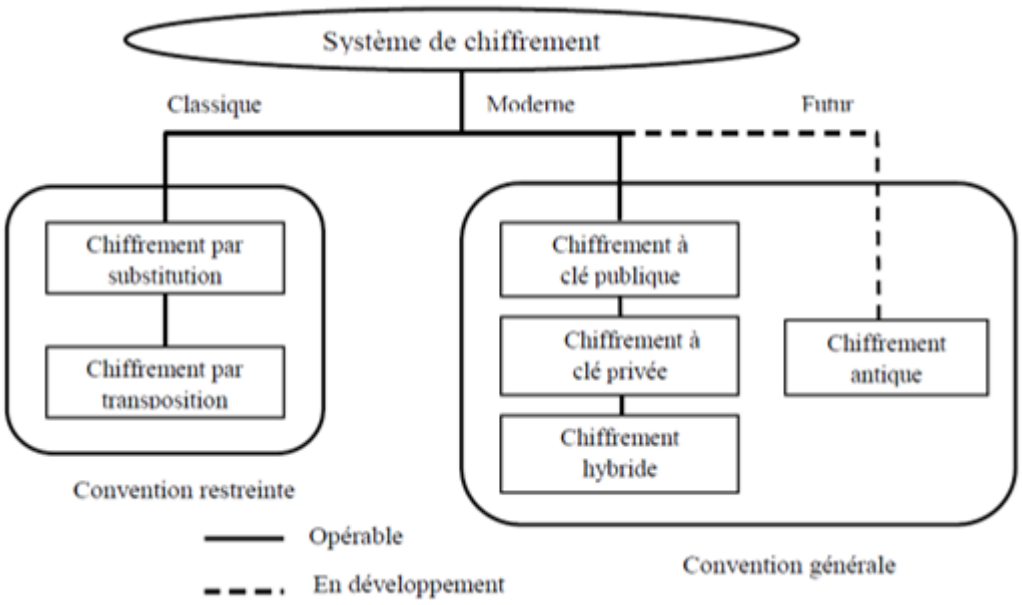


Figure I.6 : Les classes de la cryptographie [2].

I.11. Cryptanalyse

C'est l'art d'étude des crypto systèmes en cherchant leurs familles et leurs vulnérabilités afin de retrouver des messages clairs correspondant à des messages chiffrés sans avoir à connaître les clés utilisées dans le chiffrement. Lorsque tous les éléments de la méthode utilisée pour coder des messages sont repérés, on dit qu'on a **cassé** ou **brisé** le système cryptographique utilisé. Plus un système est difficile à briser, plus il est sûr.

La personne qui pratique la cryptanalyse est appelée : cryptanalyste. Il tente à décrypter le message chiffré pour découvrir son secret. On a distingué entre le verbe « décrypter » et « déchiffrer » puisque ce dernier est réservé pour le déchiffrement par le destinataire légitime [7].

a- Types de cryptanalyse

On distingue plusieurs types d'attaques :

- ***Attaque sur texte chiffré seul (ciphertext-only)*** : l'attaquant a seulement la possibilité d'intercepter un ou plusieurs messages chiffrés. La cryptanalyse est plus ardue de par le manque d'informations à disposition.

- ***Attaque à texte clair connu (known-plaintext attack)*** : se base sur la connaissance d'une partie du texte en clair pour déduire le reste du message. La tâche est de retrouver la clef utilisée pour chiffrer ce message.
- ***Attaque à texte clair choisi (chosen-plaintext attack)*** : se base sur la possibilité de choisir un texte clair et d'obtenir son chiffrement et en ayant la possibilité de générer les versions chiffrées de messages clair avec un algorithme considérer comme une **boîte noire** tel que les algorithmes à clé publique puisque l'algorithme est public.
- ***Attaque à texte chiffré choisi (chosen-ciphertext attack)*** : le cryptanalyste possède des messages chiffrés et essaye de les déchiffrer de son choix. Sa tâche est de retrouver la clef.

b- Familles d'attaques cryptanalytiques

Il existe plusieurs familles d'attaques cryptanalytiques, les plus connues sont les suivantes :

- **L'analyse fréquentielle** : examine les répétitions des lettres du message chiffré afin de trouver la clé. Cette technique est découverte par Al-Kindi au IXe siècle [7] contre les chiffrements mono-alphabétiques. Elle est inefficace contre les chiffrements modernes tels que DES, RSA. Elle est basée sur le fait que, dans chaque langue, certaines lettres ou combinaisons de lettres apparaissent avec une certaine fréquence.
- **L'attaque par dictionnaire** : le mot testé est pris dans une liste prédéfinis contenant les mots de passe les plus courants et aussi des variantes de ceux-ci. Ces listes sont généralement dans toutes les langues les plus utilisées, elles contiennent des mots existants ou des mots diminutifs (par exemple « powa » pour « power » ou « K7 » pour « cassette »). Ells sont souvent liées à l'attaque par force brute.
- **L'attaque par force brute** : s'appuie sur le cassage d'un mot de passe en testant tous les mots de passe possibles. C'est le seul moyen de récupérer la clé dans les algorithmes les plus modernes et encore inviolés comme AES.
- **La cryptanalyse linéaire** : c'est une attaque à texte clair inventée par le japonais Mitsuru Matsui [7]. L'idée est de trouver des approximations linéaires entre les bits de sortie, les bits d'entrée et les bits de la clé. Si certaines de ces approximations apparaissent avec une probabilité suffisante,

on a alors démontré que la correspondance entre entrée et sortie n'est pas purement aléatoire. Le nombre de clés à envisager pour déchiffrer le message est restreint.

- **La cryptanalyse différentielle** : découverte par deux cryptologies israéliennes : Bihan et Shamir. Elle consiste à comparer les sorties de l'algorithme quand on lui met en entrée deux messages ayant une différence fixe. On étudie comme variant les sorties si les deux messages ne diffèrent que par un seul bit. Si en déplaçant ce bit à l'intérieur des messages, certains bits des sorties restent inchangés, on a alors trouvé une faille dans l'algorithme et celui-ci est attaquable.

I.12.Conclusion

Dans ce chapitre, nous avons commencé par donnes quelque définitions sur la cryptologie et la cryptographie et leurs historiques, nous avons fourni un aperçu des différentes techniques de la cryptographie et la cryptanalyse. Ce chapitre a introduit aussi, les principaux algorithmes de cryptage symétrique, asymétrique, par flot et par bloc, et a présenté également les différentes formes d'attaques et leurs classifications.

CHAPITRE II : LE CRYPTAGE DES IMAGES PAR L'AES

II.1. Introduction

La sécurité informatique est devenue une préoccupation majeure pour tous ceux qui sont intéressés par l'informatique et à cette fin la plupart des développeurs se concentrent sur les techniques de cryptage pour fournir de bons résultats. Dans ce chapitre, nous allons parler sur la classification des algorithmes de cryptage par AES 128-192-256 en détail avec les types et la présentation des différences entre eux. Puis nous allons parler sur les types des méthodes pour crypter les images, et que nous allons parler sur des différents critères pour mesurer l'efficacité des algorithmes de cryptage d'image.

II.2. Architecture de l'algorithme AES

L'algorithme peut être employé avec les trois longueurs principales différentes indiquées ci-dessus, et peuvent désigner sous le nom de "AES-128", de "AES-192", et de "AES-256 ». Pour chacun la taille de bloc (données) d'entrée et de sortie est toujours de 128 bits.
Pour les trois cas de l'algorithme, la longueur de clé et le nombre de rondes (tours) sont définit dans le tableau 2.1 :

Tableau 2.1 : Combinaisons Clé-Bloc-Ronde [8].

	Longueur de Clé (NK : Mot 32bits)	**La taille de bloc (NK : Mot 32bits)**	**Nombre de rondes (tour) (Nr)**
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

L'ordonnancement des étapes est illustré dans la figure II.1 :

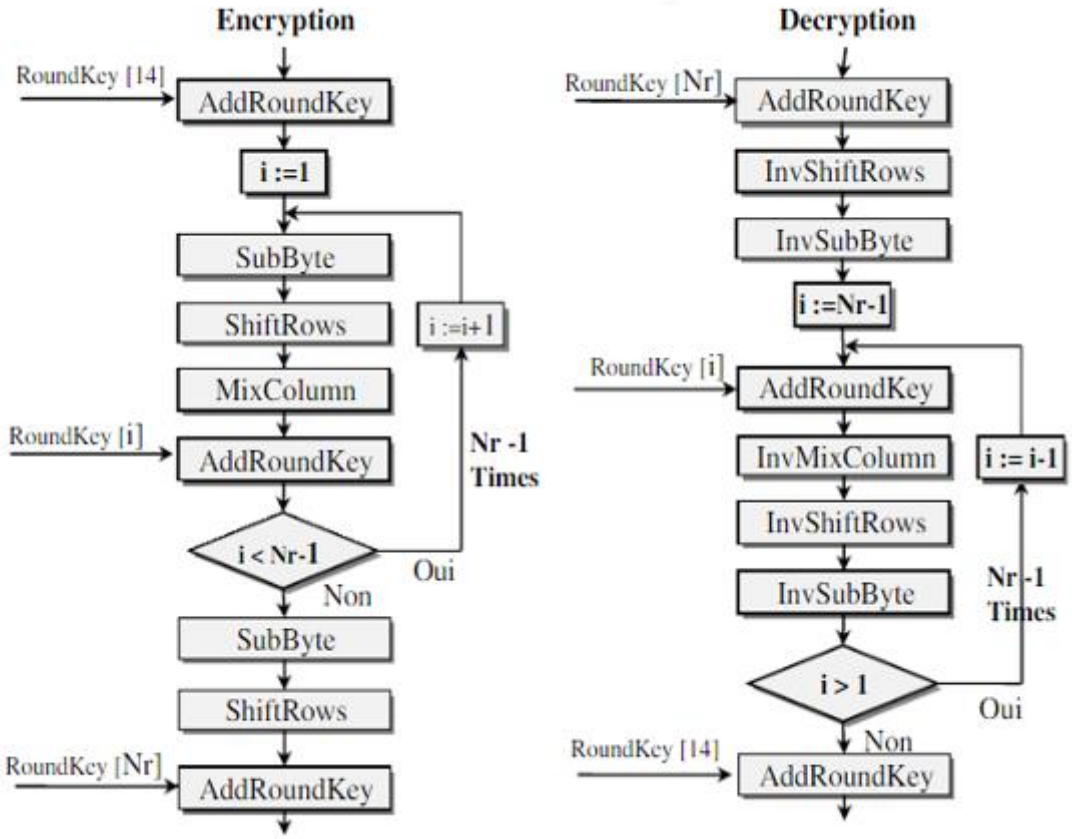


Figure II.1: L'organigramme général des différentes étapes[8].

Le Rijndael a été conçu de manière à ce que les étapes SubBytes et ShiftRows soient interchangeables. La même remarque reste vraie dans le cas du déchiffrement.

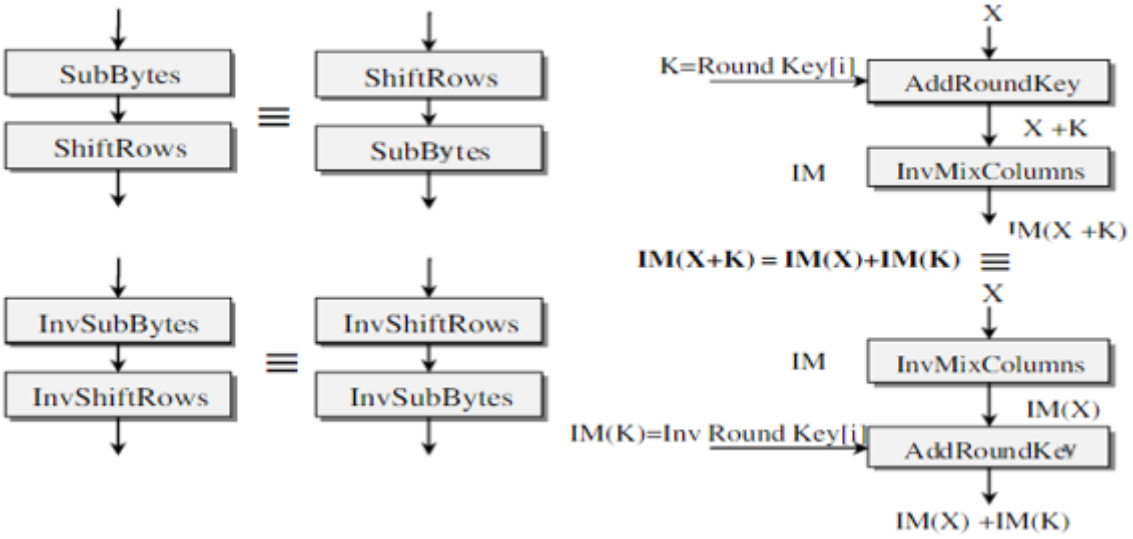


Figure II.2 : Particularité des transformations [8].

II.2.1. Description de l'architecture (AES-128, 192, 256)

Le chiffrement et le déchiffrement de Rijndael se fait par Nr tours (10,12 ou 14) pour un bloc (message) de taille 128 bits et une clé de tour à une longueur (128,192 ou 256) bits, à chaque ronde, quatre transformations sont appliquées [9] :

1. Substitution d'octets dans le tableau de message.

2. Décalage des rangées dans le tableau de message.

3. Mélange des colonnes dans le tableau de message (sauf à la dernière ronde)

4. Addition d'une "clef de ronde" qui varie à chaque ronde

Le schéma d'un seul tour est illustré dans la figure II.3 :

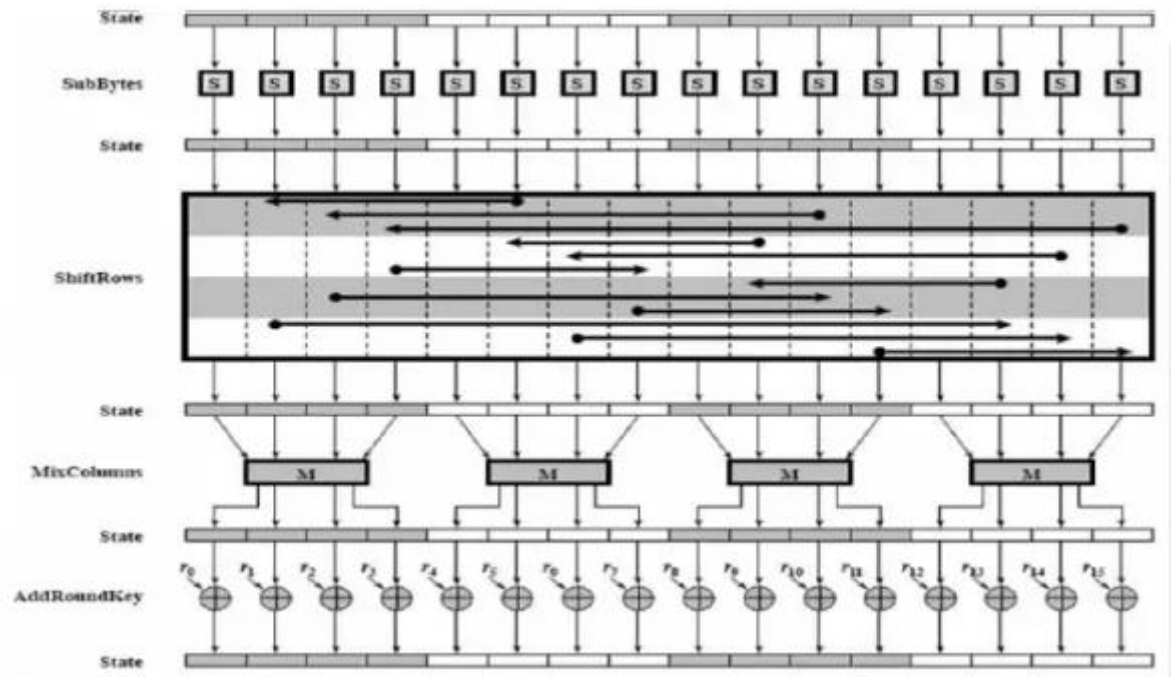


Figure II.3: Schéma des étapes d'un seul tour [9].

Pour simplifier les transformations et augmenter la vitesse de chiffrement/déchiffrement le message et la clé sont conservés sous forme de tables comme la figure II.4 (exemple de128 bits). Le nombre de colonnes dépend de taille de bloc et de la clé (pour clé de 192, 256).

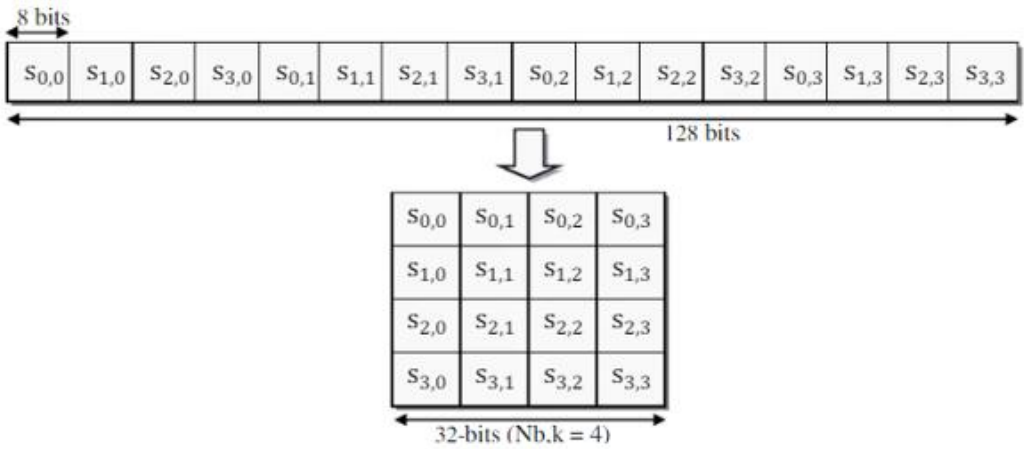


Figure II.4: Transformation d'un bloc à une table

II.2.1.1. Chiffrement

a. La substitution (S-Box /SubByte)

La transformation de SubByte (Figure II.5) est une substitution non linéaire d'un bloc de 8-bits (byte) qui fonctionne indépendamment sur chaque byte de bloc en utilisant une table de substitution (boîte de substitution). Cette boîte de substitution (Figure II.6), qui est inversible, une seule boîte est suffisante pour toute la phase de chiffrement [10].

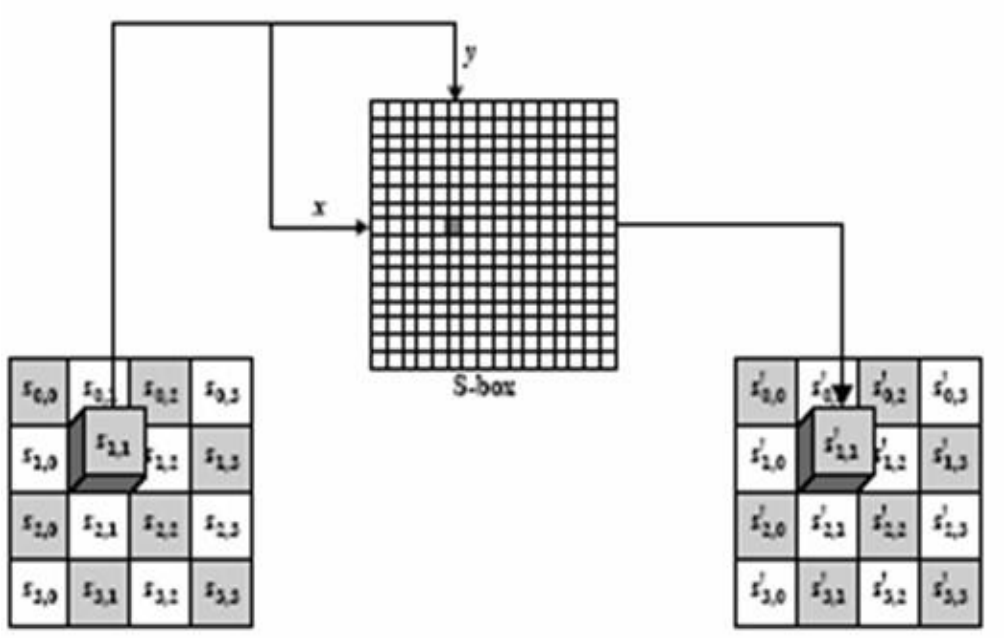


Figure II.5 : Table d'état des clés[9].

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure II.6 : S-Box inversible [11]

b. Le décalage de rangées (ShiftRows)

Cette étape augmente la diffusion dans la ronde selon la figure II.7.

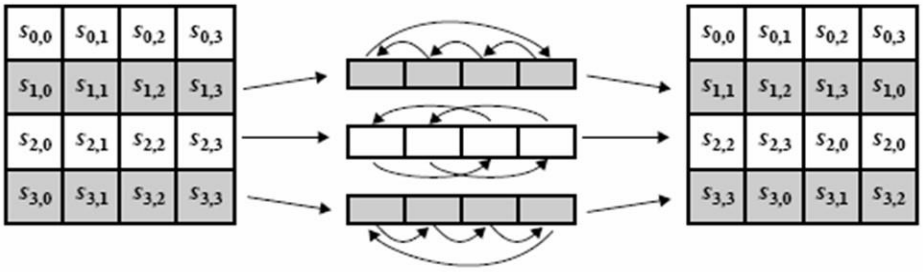


Figure II.7 : Schéma de l'étape ShiftRow [11].

Selon la taille des blocs de message (c'est-à-dire la valeur de Nb), les décalages ne seront pas toujours identiques.

– La ligne 0 n'est jamais décalée,

– La ligne 1 est décalée de C_1,

– La ligne 2 est décalée de C_2,

– La ligne 3 est décalée de C_3.[10]

	C_1	C_2	C_3
N_B=4	1	2	3
N_B=6	1	2	3
N_B=8	1	3	4

Figure II.8 : Décalage selon la taille des blocs de messages[11].

c. Mélange des colonnes (MixColumns)

Une différence sur 1 byte d'entrée se propage sur les 4 bytes de sortie. On a donc encore une étape de diffusion. La matrice utilisée est définie par Rijndael. Elle contiendra toujours ces valeurs [9], qui est illustré par la figure II.9.

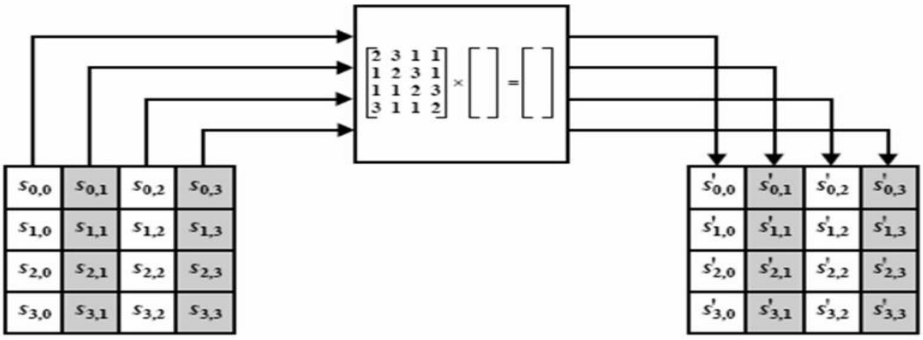


Figure II.9 : Etape du MixColumn [11].

d. Addition d'une clé de ronde (*AddRoundKey*)

C'est un simple ⊕ des clés. Il s'agit d'additionner des sous-clés aux sous-blocs correspondants suivant la figure II.10.

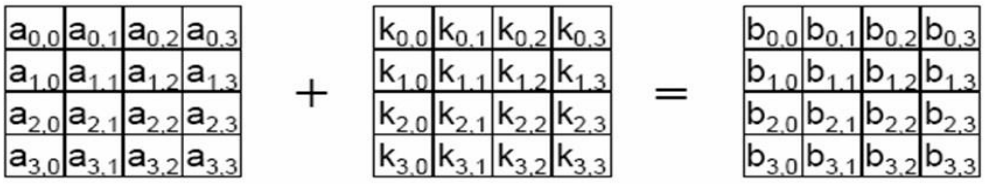


Figure II.10 : AddRound Key [11].

e. Génération (extension) des clés

Après avoir subi une extension (*Key Expansion*), la clé sera découpée en sous-clés (appelées clés de rondes), comme indiqué à la figure (II.11).

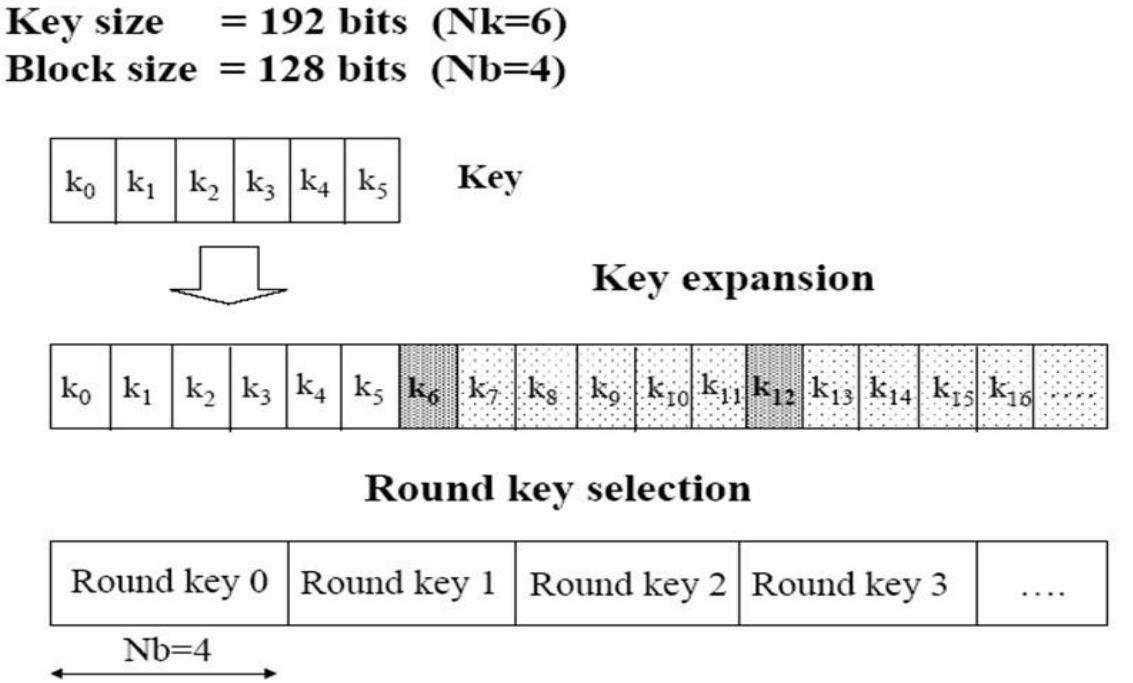


Figure II.11: Schéma des opérations effectuées sur la clé[12].

II.3. Les modes de chiffrement de l'AES

Deux modes de chiffrements utilisés par les algorithmes contemporains :

- **Cryptages par blocs**: chiffrements des blocs clairs de taille fixe généralement identique à la taille de la clé (128 ou 256 bits) [13].

-Electronic Code Book (ECB)

-Cipher Book Chaining (CBC)

- **Cryptages par flot** en continu (Stream): chiffrent les octets au fur et à mesure sans contrainte de taille [13].

  -Cipher Feedback (CFB) Mode

  -Output Feedback (OFB) Mode

  -Counter (CTR).

II.3.1. Mode ECB (Mode Electronic Code-Book)

Dans ce mode Chiffrer/déchiffrer chaque bloc indépendamment des autres [13] ; suivant la figure II.12.

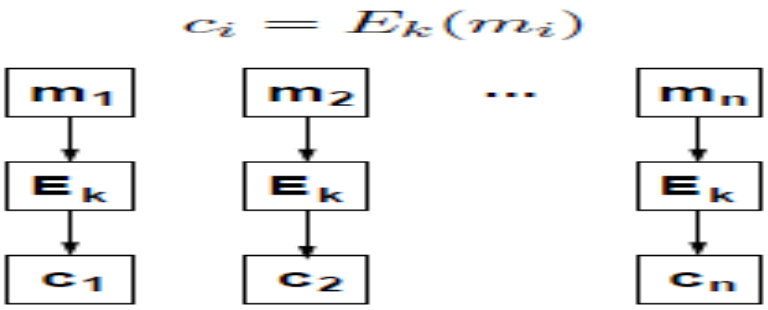


Figure II.12 : Mode ECB [13].

II.3.2. Mode CBC (Cipher Bloc Chaining)

Dans ce mode marquer chaque bloc par une opération de XOR avec le chiffré du bloc précédent avant de la chiffrer. Le premier bloc est marqué par un vecteur initiale IV [13], selon la figure II.13.

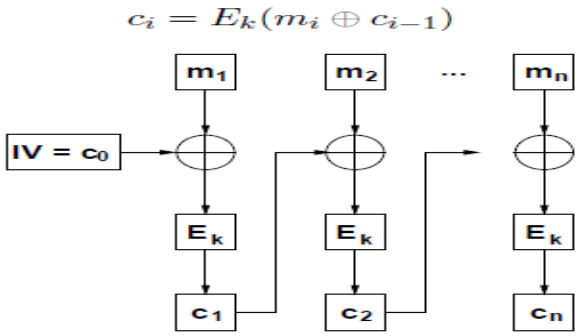


Figure II.13 : Mode CBC [13].

II.3.3. Mode CFB (Output Feed Back)

Pour ce mode, il consiste à chiffrer un vecteur initial (IV) puis l'utiliser pour l'exore avec un bloc du message en clair puis. Le IV est chiffré itérativement pour chaque bloc [13], selon la figure II.14.

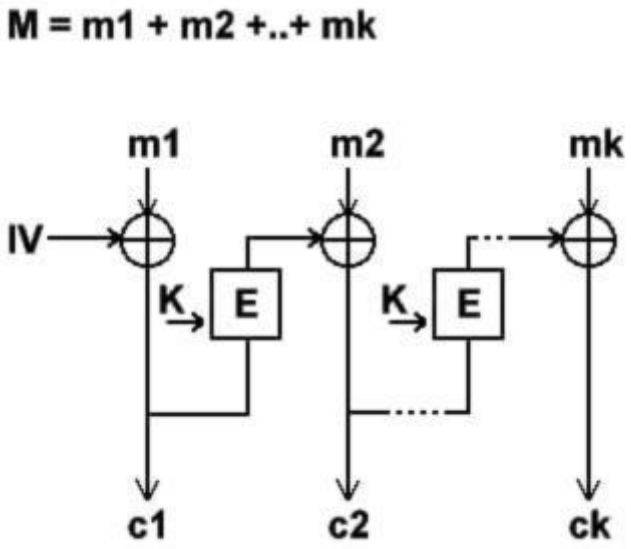


Figure II.14 : Mode CFB [13].

II.3.4. Mode OFB (Cipher FeedBack)

Dans ce mode en utilise le même principe d'OFB sauf que chaque bloc est masqué par le chiffrement du résultat du masquage du bloc précédent [13], qui montre par la figure II.15.

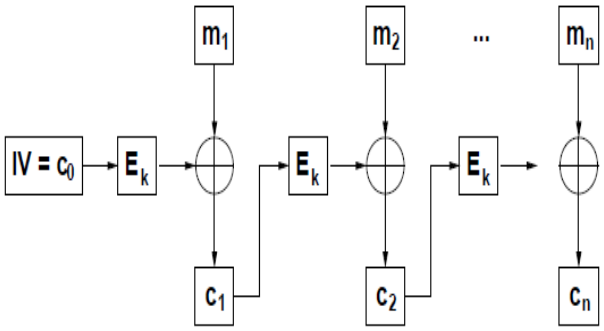
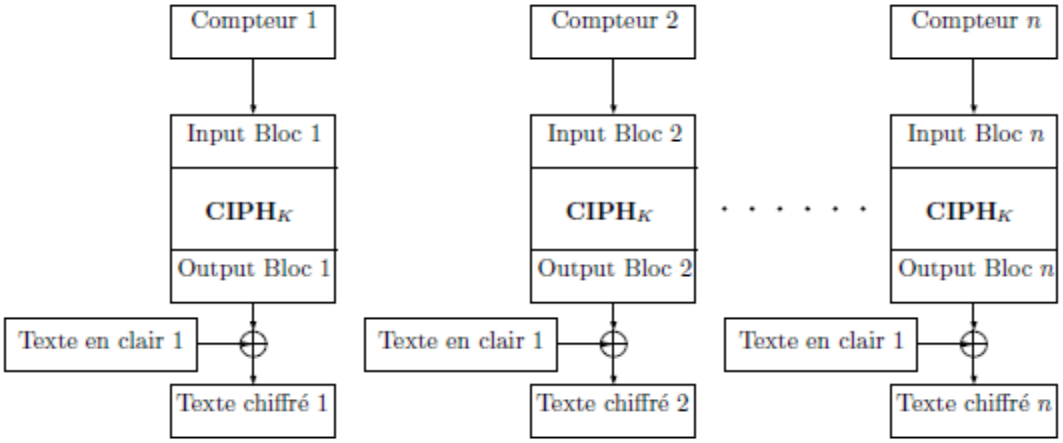


Figure II.15 : Mode OFB [13].

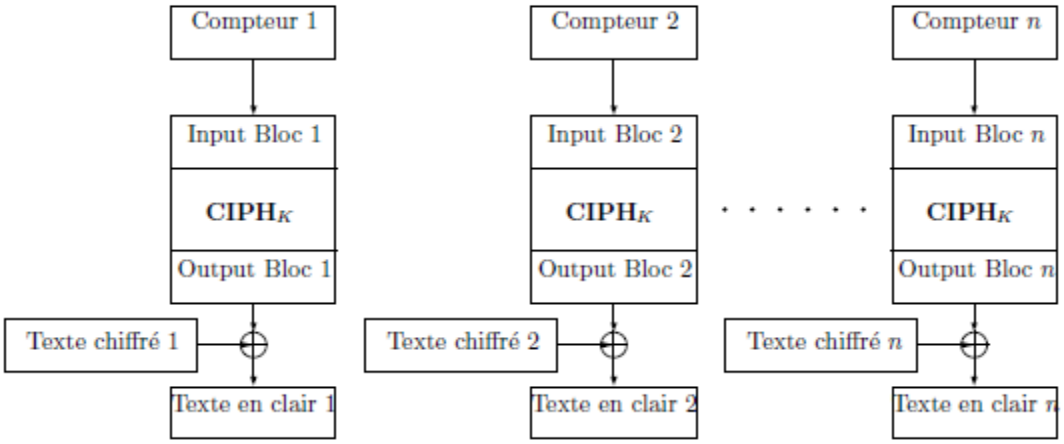
II.3.5. Mode CTR (Counter-mode encryption)

Ce mode de fonctionnement est moins fréquent que le mode CBC, mais il a un certain nombre d'avantages. Comme avec OFB, le mode CTR peut aussi être aussi considéré comme un moyen de générer un flux pseudo-aléatoire à partir d'un algorithme de chiffrement par bloc.

Dans le cryptage CTR, la fonction de chiffrement avant est prétendue sur chaque bloc du compteur, l'opérateur binaire XOR est appliqué entre les blocs de sortie résultants et les blocs de texte en clair correspondants pour produire les blocs de texte chiffré [13], présenté par la figure II.16.



(a) Cryptage en mode CTR



(a) Déryptage en mode CTR

Figure II.16 : Mode CTR [13].

II.4. Critère d'évaluation

Pour pouvoir analyser les performances des résultats issues du chiffrement avec l'algorithme AES seul ou avec les différents modes, en a utilisés différentes métrise

d'évaluations des qualités des résultats des images chiffres par rapport des images original ou en clair. Les outils utilisés dans ce travail sont [14] :

- L'erreur quadratique moyenne (**MSE**).
- Le rapport crête signal sur bruit (**PSNR**).
- Indice de Similarité structurelle (**SSIM)**.

a. MSE (Erreur quadratique moyenne)

L'image déchiffrée $\hat{I}$ est toujours comparée à l'image originale I ou en claire pour déterminer son rapport de similitude. Ce critère est le plus utilisé. Il est basé sur la mesure de l'erreur quadratique moyenne (MSE) calculée entre les pixels originaux et celle déchiffrées [15] :

$$\mathrm{MSE} = \frac{1}{\mathrm{M}*\mathrm{N}}\sum_{\mathrm{m}=1}^{\mathrm{M}} \qquad \text{(II. 1)}$$

Où (M × N) qui désigne la taille de l'image original et déchiffrée, et $I\,p$ et $\hat{I}\,p$ sont respectivement les amplitudes des pixels sur les images originale et déchiffrée. Il est vraisemblable que l'oeil tienne beaucoup plus compte des erreurs à grandes amplitudes, ce qui favorise la mesure quadratique. Plus la valeur de MSE est faible, plus l'erreur est faible.

b. PSNR (Rapport crête signal sur bruit)

Pour ce critère d'évaluation, au lieu de mesurer la distorsion, la valeur (Peak Signal to Noise Ratio, PSNR) mesure la fidélité de l'image déchiffrée par rapport à l'original ou en clair, puisqu'elle est proportionnelle à la qualité. Comme nous pouvons le voir selon l'équation III.3, elle est une fonction de

MSE ; sa définition et son utilisation proviennent du domaine du traitement de signal [15]

$$PSNR = 10Log_{10}\left[\frac{\frac{1}{N}\sum I^2}{MSE}\right] \qquad \text{(II. 2)}$$

Pour une image à niveau de gris, *Imax* désigne la luminance maximale possible. Une valeur de PSNR infini correspond à une image non dégradée. Et cette valeur décroît en fonction de la dégradation. Le PSNR relie donc le MSE à l'énergie maximale de l'image [15]. Plus le PSNR est élevé, l'image déchiffrée est similaire à l'originale.

L'erreur quadratique moyenne (MSE) et le rapport signal / bruit de crête (PSNR) sont utilisés à l'origine pour comparer la qualité de compression d'image nous les avons utilisés pour évalués la qualité des images déchiffrées par rapport à l'original.

c. SSIM (Indice de similarité structurelle)

SSIM est une mesure de similarité entre deux images numériques. Elle a été développée pour mesurer la qualité visuelle d'une image déformée, par rapport à l'image originale. L'idée de SSIM est de mesurer la similarité de structure entre les deux images, plutôt qu'une différence pixel à pixel comme le fait par exemple le PSNR. L'hypothèse sous-jacente est que l'œil humain est plus sensible aux changements dans la structure de l'image [15].

La métrique SSIM est calculée sur plusieurs fenêtres d'une image. On dénote *x* et *y* l'image originale et l'image déformée respectivement.

La similarité compare la luminance, le contraste et structure entre chaque couple de fenêtres. La luminance est estimée par la mesure de l'intensité moyenne de chaque fenêtre [15]:

$$u_x = \frac{1}{N}\sum_{1}^{N} x_i \qquad (II.3)$$

Où :

N : le nombre de pixels de chaque fenêtre.

x_i : l'intensité d'un pixel.

II.5. Analyse statistique

1) L'histogramme

Dans un contexte de traitement d'image, l'histogramme d'une image désigne un histogramme des valeurs d'intensité des pixels. Cet histogramme est un graphique illustrant le nombre de pixels dans une image à chaque valeur d'intensité trouvée dans cette image. Pour une image grise il y a 256 intensités différentes possibles, ainsi, l'histogramme s'affiche graphiquement en utilisant 256 chiffres indiquant la distribution des pixels entre ces valeurs de niveaux de gris. Les histogrammes peuvent également être pris d'images en couleur ; soit des histogrammes individuels des canaux rouge, vert et bleu, ou un seul histogramme 3-D avec les trois axes représentant les trois plans, et la luminosité dans chaque point représente le nombre de pixels. En conséquence, l'histogramme d'une image ne représente pas la répartition spatiale ; ainsi, deux images différentes peuvent disposer le même histogramme.

Dans un contexte de chiffrement d'image, l'histogramme de l'image chiffrée doit être uniforme pour qu'un adversaire ne puisse extraire aucune information à partir de cet histogramme [16].

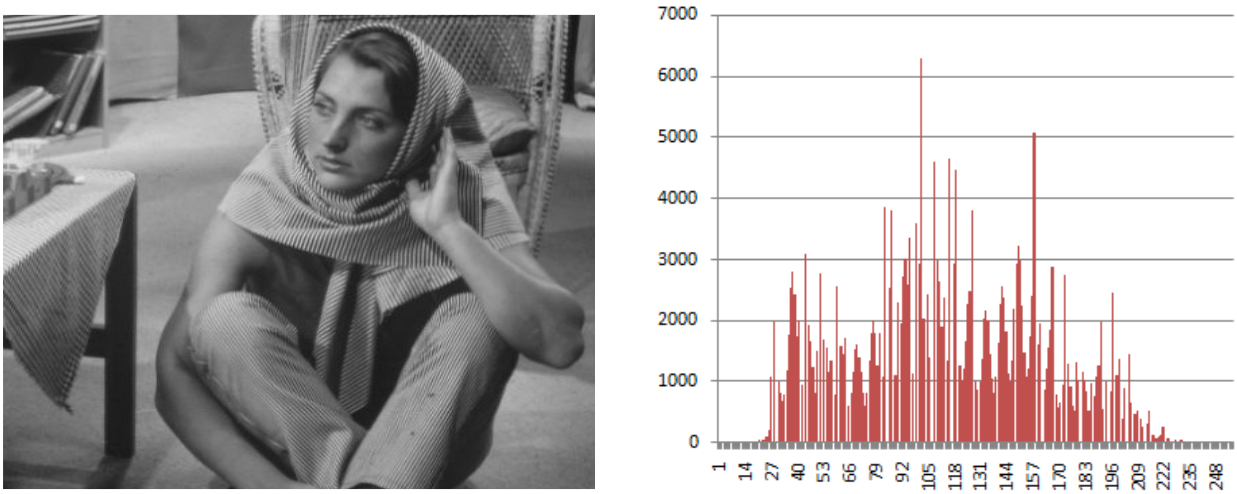


Figure II.17 : Illustration d'histogramme d'une image[16].

2) La corrélation

La corrélation est une technique qui permet de comparer deux images pour estimer les déplacements des pixels d'une image par rapport à une autre image de référence. Les pixels adjacents d'une image standard ont une forte corrélation. Un bon schéma de cryptage d'image doit supprimer une telle corrélation afin d'assurer la sécurité contre l'analyse statistique. Afin de tester la corrélation entre deux images on choisit au hasard 10 000 paires de deux pixels adjacents dans les trois directions ; horizontal, vertical et diagonal à partir des composants R, G, B de l'image claire et son image chiffrée et les coefficients de corrélation de chaque paire ont été calculées en utilisant les formules suivantes [16] :

$$r = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad \text{(II.4)}$$

Où :

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big) \quad \text{(II.5)}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad \text{(II.6)}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)^2 \quad \text{(II.7)}$$

Le résultat du calcul est une valeur réelle appartenant à l'intervalle [0,1]. Si le coefficient est 1 donc les deux images sont égales. Sinon, Si la valeur obtenue est 0 ou proche de 0 alors les deux images sont différentes.

3) L'entropie

Selon la théorie de Shannon, l'entropie d'une information est la quantité d'information englobée ou libérée par une source d'information. En particulier, plus la source est redondante, moins elle contient d'information. En absence de contraintes particulières, l'entropie est maximale pour une source dont tous les symboles sont équiprobables. Ainsi, elle est l'une des principales mesures de l'aléatoire de l'information [16].

Les valeurs de l'entropie élevée manifestent un haut degré de caractère aléatoire ; et pour tout message codé sur *M* bits, la limite supérieure de l'entropie est *M*. La formule utilisée pour calculer l'entropie d'une source *m* est comme suit :

$$H(M) = \sum_{i=0}^{2^n-1} p(m_i)\log_2\left(\frac{1}{p(m_i)}\right) \quad \text{(II.8)}$$

Donc pour un crypto système de chiffrement d'images parfait la valeur de l'entropie doit être très proche de 8 pour chaque plan [16].

II.6. Conclusion

Dans ce chapitre, nous avons présenté le principe de l'AES. Les principales opérations utilisées dans cet algorithme de chiffrement ont été exposées où nous avons remarqué que 75% de la sécurité de cet algorithme repose sur l'opération SubBytes.

Nous avons aussi évoqué les métries utilises pour l'évaluation de la qualité des images qui seront chiffres par les deux types d'AES évidemment le AES-128 et le AES 256 avec deux mode chiffrement.

Nous avons aussi donné les définitions des cinq modes utilises pour augmente la sécurité.

CHAPITRE III : SIMULATION ET EVALUATION

III.1. Introduction

Dans ce chapitre, nous présentons la simulation et l'évaluation pour le chiffrement des images en utilisent l'algorithme AES-128 et AES-256. Ce choix a pour objectif, de voir quelle est le mieux pour le chiffrement des images. En a utilisé deux modes de chiffrement qui sont utilisés pour renforce la sécurité tel que Cipher Bloc Chaining (CBC) et Output FeedBack (OFB).

Des métrise sont utilisées pour évoluer la qualité des images après opération de déchiffrement.

III.2. Les types d'image utilisés

Il existe deux types d'images numériques :

III.2.1. Matricielle

Formée d'une grille composée de pixels. Plus on zoom, plus les pixels deviennent apparents [17].

Les photos numériques et les images scannées sont de ce type [18]. Les formats d'images bitmap : BMP, JPEG , GIF, TIFF , PNG :

a) BMP (Bitmap) :

Le format BMP est un des formats les plus simples développé conjointement par Microsoft et IMB. Un fichier BMP est un fichier bitmap. C'est-à-dire un fichier d'image graphique stockant les pixels sous forme de tableau de points et g errant les couleurs soit en couleur vraie soit grâce à une palette indexée. Le format BMP a été étudié de telle maniérée à obtenir un bitmap indépendant du périphérique d'affichage [18], la figure (III.1) illustre un exemple.

Figure III.1 : image sous matlab -mat-[19]

b) JPEG (Joint Photographie Experts Group) :

JPEG (Joint Photographic Experts Group) est une méthode de compression avec perte, Les images JPEG compressées sont généralement stockées dans le format de fichier JFIF (JPEG Interchange File Format). Le format de fichier d'image est le plus utilisé. Les formats JPG est plus utilisé dans les appareils photo numériques et les pages Web [20], la figure (III.2) présente un exemple.

Figure III.2 : image sous matlab jpeg[19].

c) GIF (Graphical Interchange Format) :

GIF (Graphics Interchange Format), C'est un format léger pour les animations. Et de transparence compression efficace Très répandu sur le Web malgré ses faiblesses et un problème de droit sur son format de compression. À déconseiller pour les photos [21].

d) TIFF (Tagged Image File Format) :

Le format TIFF est un format matriciel. Conçu au départ pour n'accepter que les images en RGB. Elle offre l'avantage d'occuper mois d'espace disque. Grâce à son propre algorithme de compression appelé LZW. C'est un choix à éviter pour le Web puisqu'aucun navigateur Web ne le lit directement [17] , la figure (III.3) illustre un exemple.

Figure III.3 : image sous matlab -tif-[19].

e) PNG (Portable Network Graphics) :

Le format de fichier PNG (Portable Network Graphics), Il permet de stocker des images en noir et blanc (jusqu'à 16 bits par pixels), en couleurs réelles (True color, jusqu'à 48 bits par pixels) ainsi que des images indexées, faisant usage d'une palette de 256 couleurs. Il offre enfin une couche alpha de 256 niveaux pour la transparence [22,20], la figure (III.4) donne un exemple.

Figure III.4 : image sous matlab -png-[19].

III.2.2. Vectorielle

Formée de lignes calculées de manière géométrique. Lors d'un zoom avant ou arrière, la forme est recalculée en fonction de notre position sans perdre de qualité [17].

Le processeur est chargé de "traduire" ces formes en informations interprétables par la carte graphique (images Word, Publisher, CorelDraw - format WMF, CGM, etc.)

Les avantages d'une image vectorielle : les fichiers qui la composent sont petits, les redimensionnements sont faciles sans perte de qualité.

Les inconvénients : une image vectorielle ne permet de représenter que des formes simples. Elle n'est pas donc utilisable pour la photographie notamment pour obtenir des photos réalistes [18]

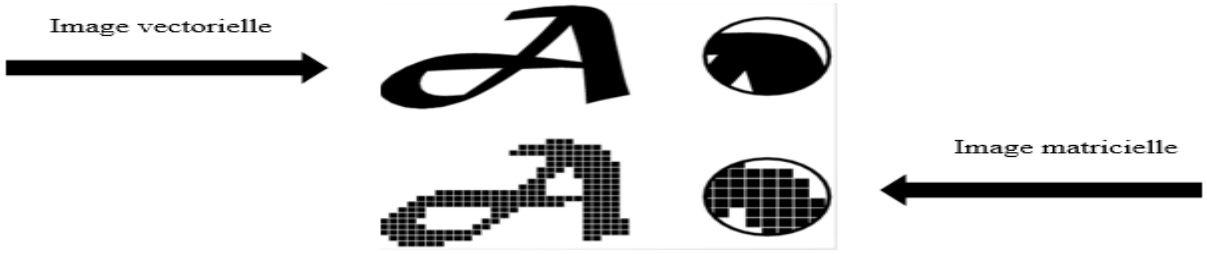


Figure III.5 : Différence entre image vectorielle et image matricielle [18].

Dans notre projet on va utiliser seulement l'image matricielle avec des formats (BMP, JPEG, PNG,TIF,GIF)

III.3. Crypto système à base d'AES-128

La tâche de notre algorithme est constituée de deux étapes : la première consiste à chiffrer un document en utilisant une clef privée, et la deuxième permet d'inverser le processus, soit de déchiffrer le document résultant de la première opération, en utilisant la même clef privée, comme présenté sur la figure (III.6).

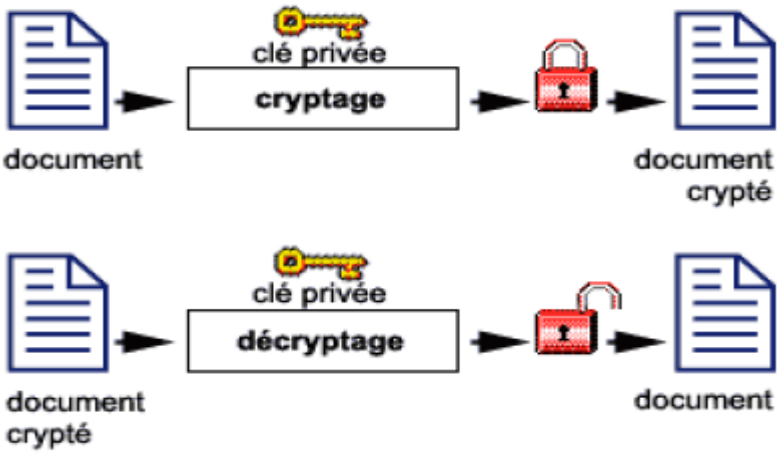


Figure III.6 : Schéma général de la tache de l'application du chiffrage déchiffrage.

Cet algorithme chiffre et déchiffre des données représentées sous forme de texte ou d'image. Dans notre cas. On s'intéresse à la forme image, on suit les étapes suivantes :

- ✓ On parcoure l'image ;
- ✓ L'image se divisera en blocs dont la taille est égale à celle de la clef (128 bits) ;
- ✓ On charge chaque bloc dans une matrice de dimensions 4*4(16 octets) ;
- ✓ On applique l'algorithme AES-128 de cryptage à chacune des matrices ;
- ✓ On obtiendra par conséquence pour chacune de ces matrices une autre qui constitue alors le bloc crypté ; l'ensemble des blocs cryptés représente l'image cryptée ;
- ✓ Cette image pourra être enregistré à l'aide d'un bouton y associé ;
- ✓ Le processus inverse redonnera la matrice cryptée à son origine ; on reconstruira alors notre image.

C’est la forme du cryptage qui implique 10 tours de substitution de transposition et de mixage pour un niveau de sécurité exceptionnellement élevé :

La génération des clés est orienté mots, où 1 mot = 32 bits. Les 11 sous-clés sont stockées dans la matrice Key expansion w qui est constituée des mots (*W* [0], . . ., *W* [43]) comme le montre la figure 3.8 [22].

La première sous-clé est la clé d'origine AES qui est copiée dans les quatre premiers éléments de W. Les autres éléments de la matrice sont calculés comme suit :

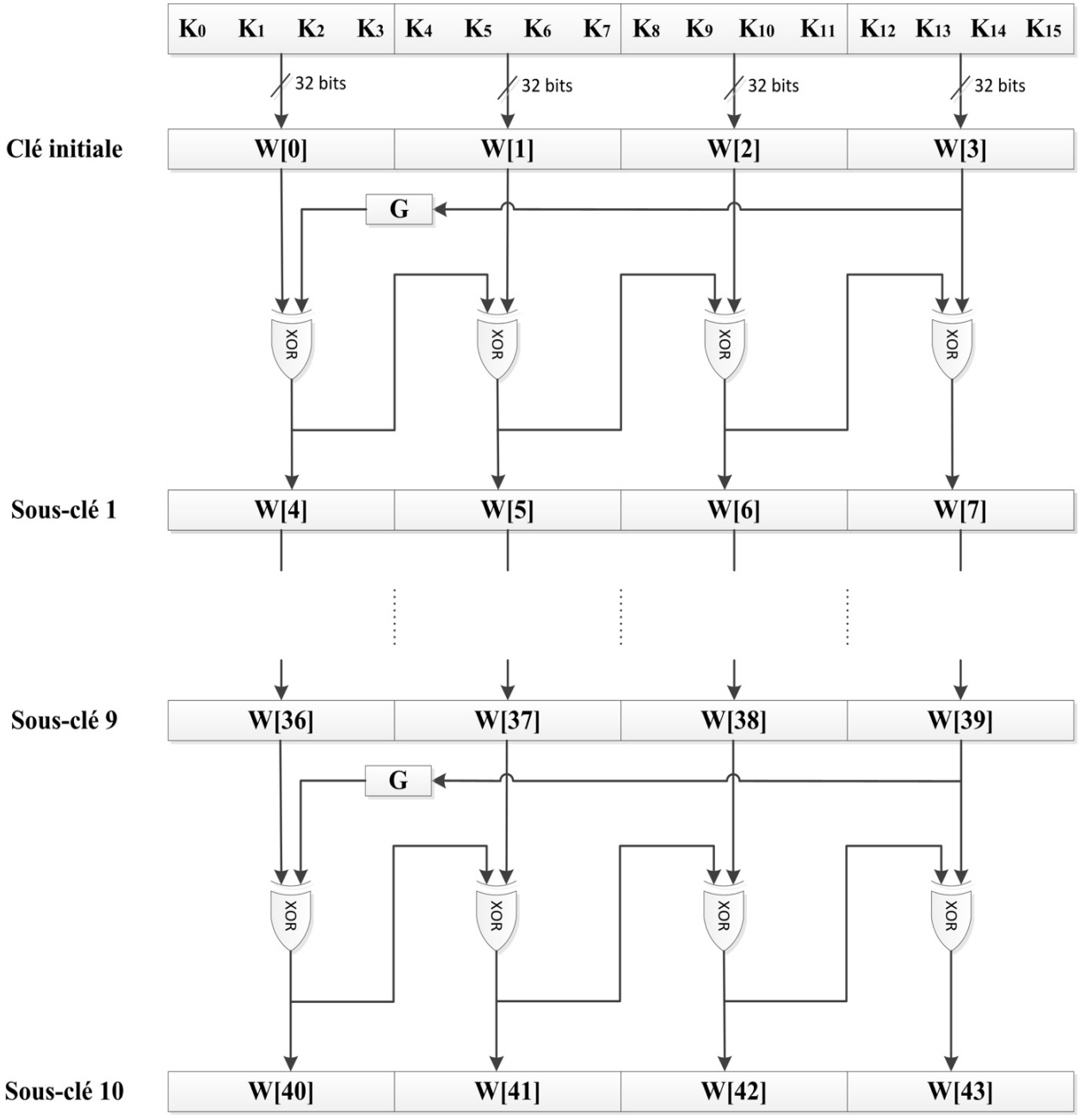
Chaque mot *W[i]* dépend du *W [i-1]* et *W [i-4]*. Pour le mot dont sa position est un multiple de 4, une fonction plus complexe *g* est utilisée [23]. g () est une fonction non linéaire avec une entrée et une sortie à quatre octets qui consiste à exécuter un décalage vers le haut d’un octet, substituer chaque octet en utilisant la table *Sbox* et ajouter un coefficient RC à elle.

Le coefficient RC est seulement ajouté à l'octet le plus à gauche dans la fonction g ().

Ce coefficient varie d’un tour à un autre selon la règle suivante :

$$\begin{aligned} RC[1] &= x^0 = (00000001)_2, \\ RC[2] &= x^1 = (00000010)_2, \\ RC[3] &= x^2 = (00000100)_2, \\ &\vdots \\ RC[10] &= x^9 = (00110110)_2. \end{aligned}$$

Figure III.7 : variation du coefficient



FigureIII.8 : Génération des sous clés à partir d'une clé de 128 bits [25].

III.3.1. Algorithme AES-128

Le fonctionnement de l'AES 128 est basé en premier lieu sur le découpage du message à chiffré en bloc de 128 bits (16 octets) [8]. Ces octets sont ensuite placés dans une matrice de 4x4 éléments, on la note la matrice *State*. La figure III.9 montre le processus de découpage.

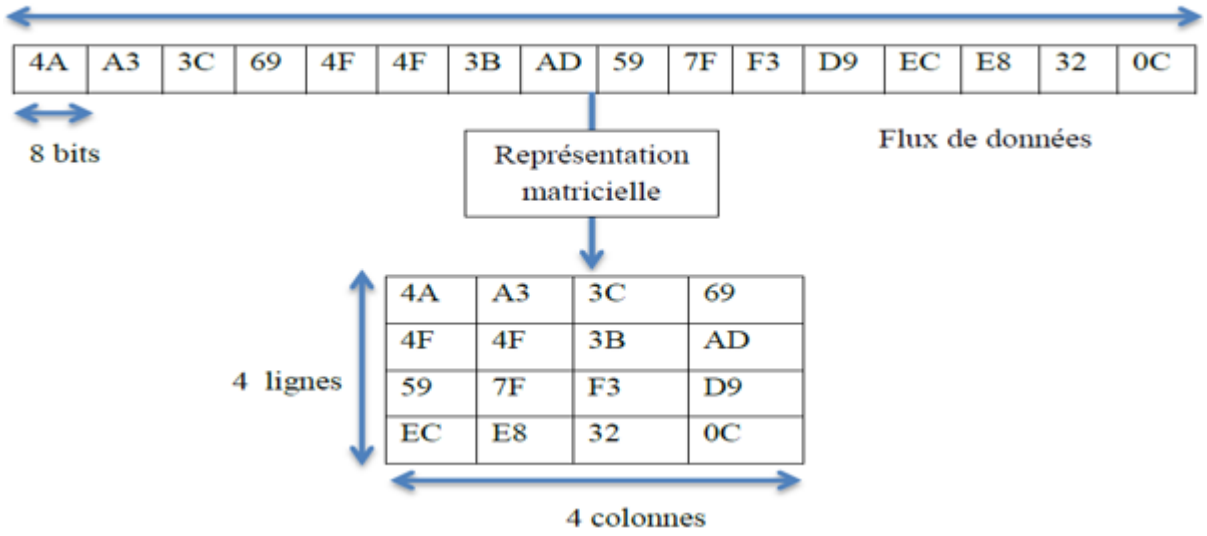


Figure III.9 : Découpage du message en matrice 4*4 [25].

A partir de la figure (III.10), nous pouvons constater que l'algorithme de chiffrement par l'AES est itératif. Il est découpé en 3 blocs :

- ✓ ***Le tour N0:*** Cette étape effectue une seule opération *AddRoundKey* en utilisant la clé de chiffrement.
- ✓ ***De 1 à 9 tours:*** Cette étape permet d'effectuer Nr itérations réguliers. Chaque itération exécute les opérations suivantes : *SubBytes*, *ShiftRows*, *MixColumns*, *AddRoundKey* dans cet ordre.

La figure (III.9) représente l'architecture globale du chiffrement/déchiffrement par L'AES-128.

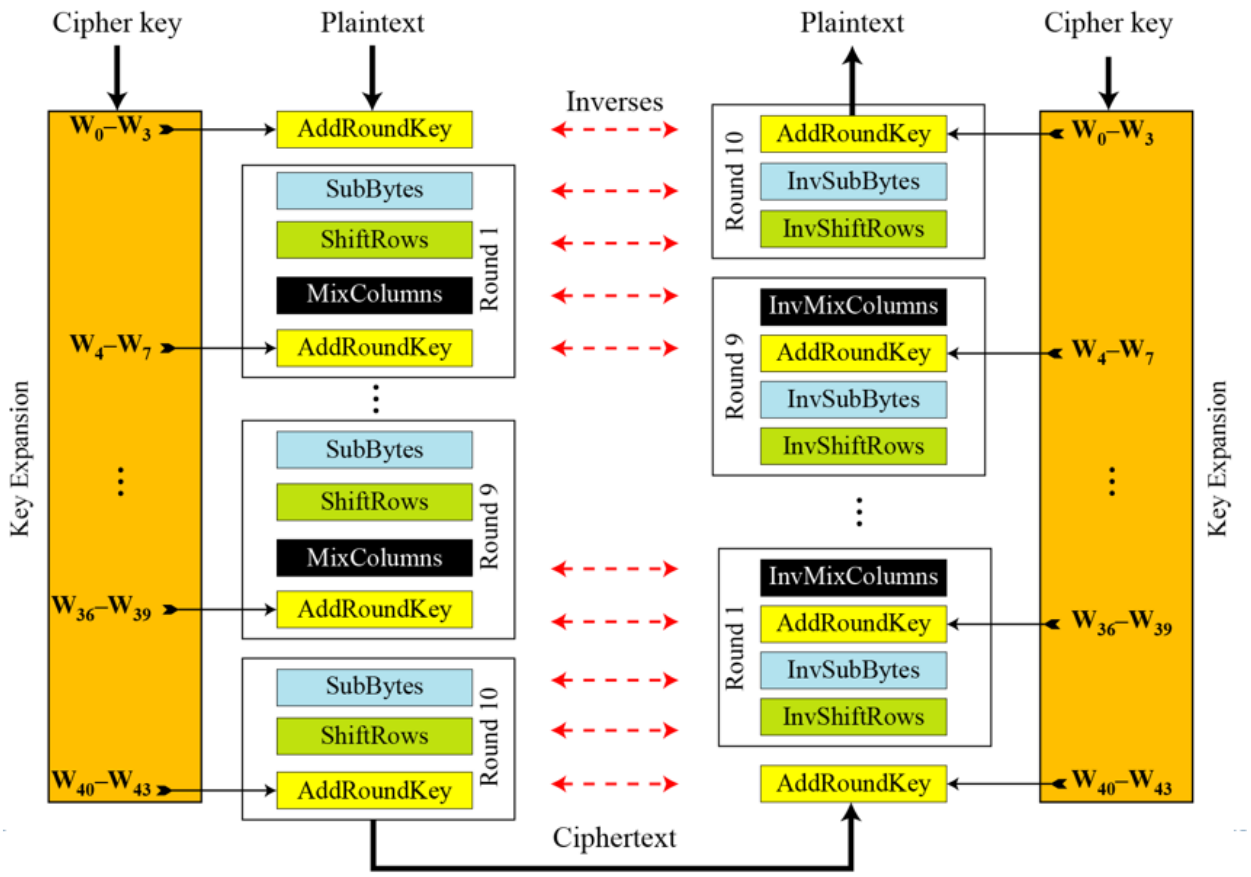


Figure III.10 : Diagramme du bloc de chiffrement et déchiffrement de l'AES-128[25].

Chaque tour utilise son propre sous clé qui est générée à partir de l'opération Key Expansion. Cette dernière sera discutée par la suite :

- ✓ ***Le tour N10:*** Ce tour exécute *SubBytes*, *ShiftRows* ET *AddRoundKey*.

Le processus de déchiffrement consiste à inverser l'algorithme de chiffrement, en commençant par le tour final. Chaque opération de chiffrement a son opération inverse pour le déchiffrement. L'inverse de AddRoundKey est lui-même.

L'AES exécute une séquence de rondes qui seront détaillées par la suite. On note Nr le nombre de rondes qui doivent être effectuées. Ce nombre dépend des valeurs de Nb et de Nk. Nb indique le nombre de colonnes de la matrice state qui est égal à la longueur du bloc, divisé par 32 et N_k représente le nombre de colonnes de la clé qui est égal à la longueur de la clé divisée par 32 [25].

Le nombre de tours produits dans l'algorithme dépend des tailles de la clé et du texte clair.

III.3.2. Les modes de chiffrement utilisés

Pour adapter la taille du message à celle de la clef on décompose le message par blocs de taille fixe correspondant aux tailles des clés que l'on chiffre ensuite un a un et que l'on envoie successivement. Pour cela deux modes de chiffrement par blocs utilisée : CBC et OFB

III.3.2.1. Le mode CBC

Le mode CBC, Le message M, est découpé en blocs, (Mi) avec i≥1, et chaque bloc est crypté de la manière suivante. On commence par choisir un bloc initial C0. Chaque bloc clair mi est d'abord modifié en faisant un XOR de ce bloc avec le bloc crypté précédent, Ci−1 puis on crypte le résultat obtenu par Exorcisation avec la clef par [26] :

$C_1 = E_k(M_1 \oplus C_0)$ $C_2 = E_k(M_2 \oplus C_1)$ . . . . . $C_i = E_k(M_i \oplus C_{i-1})$

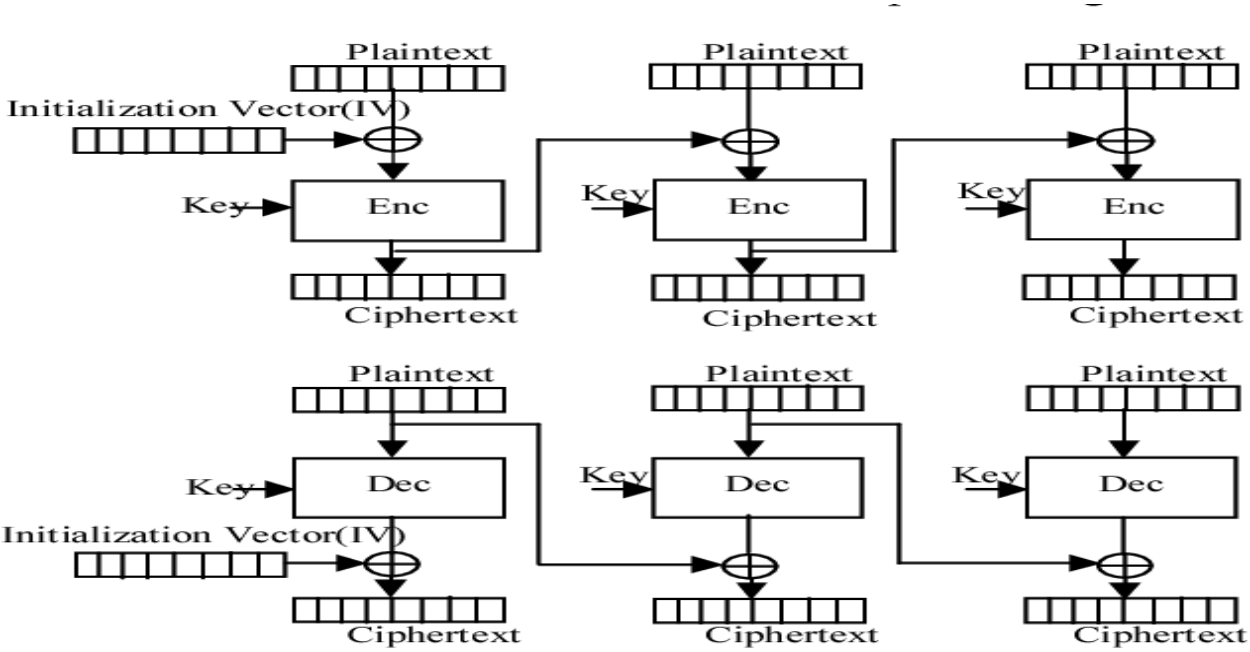


Figure III.11 : Chiffrement et déchiffrement par mode CBC [26].

III.3.2.2. Le mode OFB

Le mode OFB, Output FeedBack, est une variante de CFB qui permet d'avoir un cryptage et un décryptage totalement symétrique :

$Z = E_k(Z_{i-1})$; $C_i = M_i \oplus Z_i$

Ce mode est utilisé par exemple pour la sécurisation des donnés satellites. La figure (III.12) illustre le fonctionnement de ce mode [26]**.**

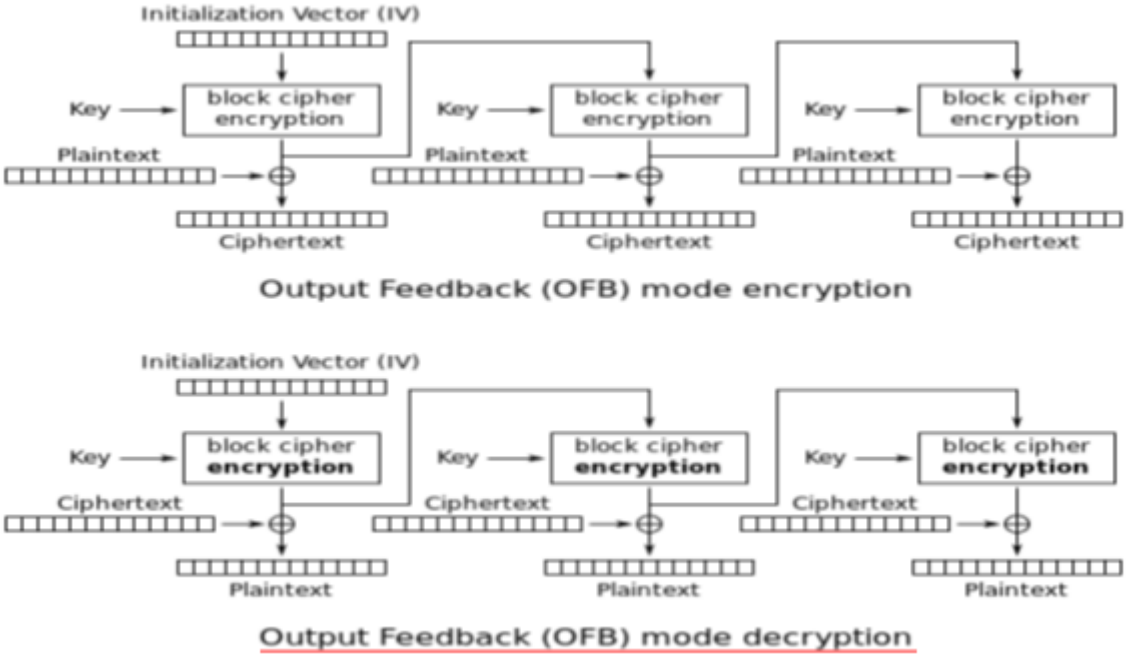


Figure III.12 : Chiffrement et déchiffrement par mode OFB [26].

III.4. Crypto système à base d'AES-256

La tâche de notre algorithme est constituée de deux étapes : la première consiste à chiffrer une image en utilisant une clef privée, et la deuxième permet d'inverser le processus, soit de déchiffrer l'image résultant de la première opération, en utilisant la même clef privée.

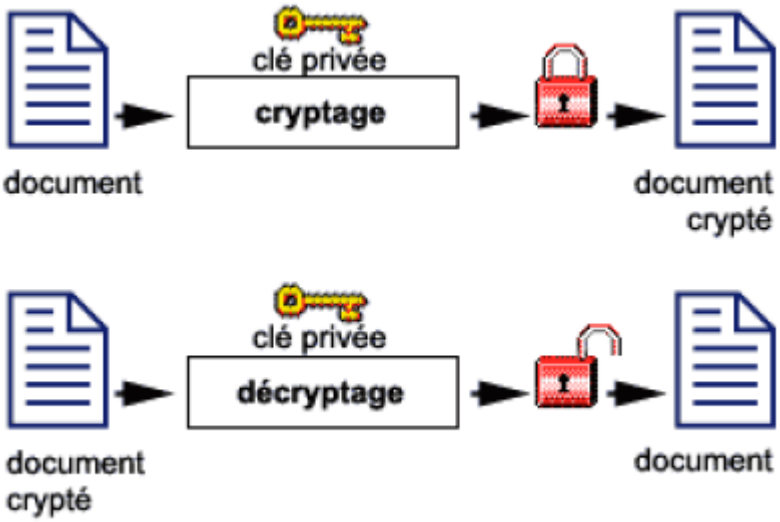


Figure III.13 : Schéma général de la tache de l'application du chiffrage déchiffrage.

Cet algorithme chiffre et déchiffre des données représentées sous forme de texte ou d'image. Dans notre cas .on s'intéresse à la forme image, on suit les étapes suivantes :

- ✓ On parcoure l'image ;
- ✓ L'image se divisera en blocs dont la taille est égale à celle de la clef (256 bits) ;
- ✓ On charge chaque bloc dans une matrice de dimensions 4*8(32 octets) ;
- ✓ On applique l'algorithme AES-256 de cryptage à chacune des matrices ;
- ✓ On obtiendra par conséquence pour chacune de ces matrices une autre qui constitue alors le bloc crypté ; l'ensemble des blocs cryptés représente l'image cryptée ;
- ✓ Cette image pourra être enregistré à l'aide d'un bouton y associé ;
- ✓ Le processus inverse redonnera la matrice cryptée à son origine ; on reconstruira alors notre image.

La version clé d'AES 256 bits est la forme la plus avancée du cryptage qui implique 14 tours de substitution, de transposition et de mixage pour un niveau de sécurité exceptionnellement élevé :

AES avec une clé de 256 bits a besoin de 15 sous-clés. Les sous-clés sont stockées dans les 60 mots W[0], . . ., W[59]. Le calcul des éléments du tableau est similaire à celui de la clé de 128 bits et le Key Schedule comprend 7 itérations, où chacune calcule huit mots pour

les sous-clés. La sous-clé pour le premier tour est formée par les éléments du tableau (W[0],W[1], W[2], W[3]), la deuxième sous-clé par les éléments (W[4], W[5], W[6], W[7]), et ainsi de suite. Il y a sept coefficients RC[1] . . . RC[7], nécessaires dans la fonction g(), qui sont calculés comme dans le cas de 128 bits. Le Key Schedule a une fonction h() avec des entrées/sortie de 4 octets. La fonction applique la S-Box à tous les quatre octets d'entrée. La figure (III.14) montre le processus de génération de clé dans le cas de 256 bits [23].

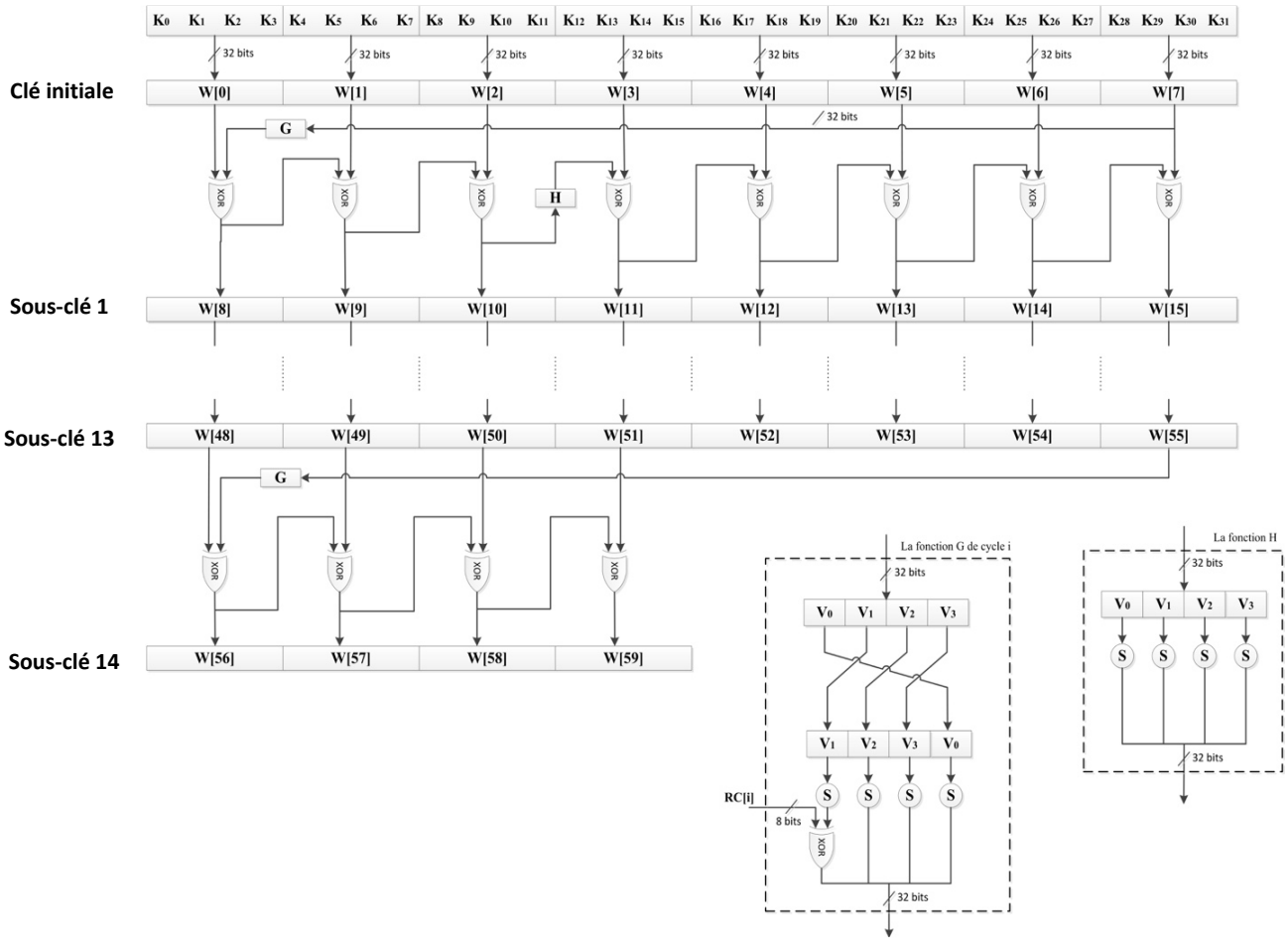


Figure III.14: Processus de génération de clés pour 256 bits [23].

III.4.1. Algorithme AES-256

Le fonctionnement de l'AES 256 est basé en premier lieu sur le découpage du message à Chiffré en bloc de 256bits (32 octets) . Ces octets sont ensuite placés dans une matrice de 4x8 éléments, On la note la matrice *State*.

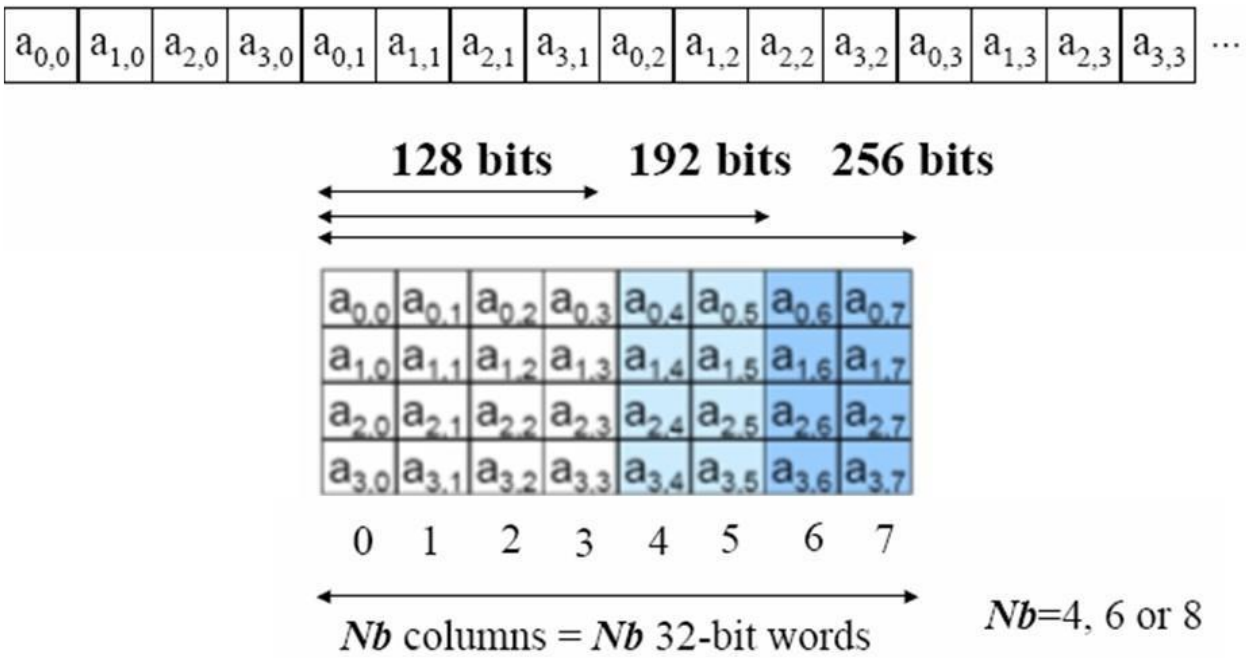


Figure III.15: Découpage du message en matrice 4*8 [23].

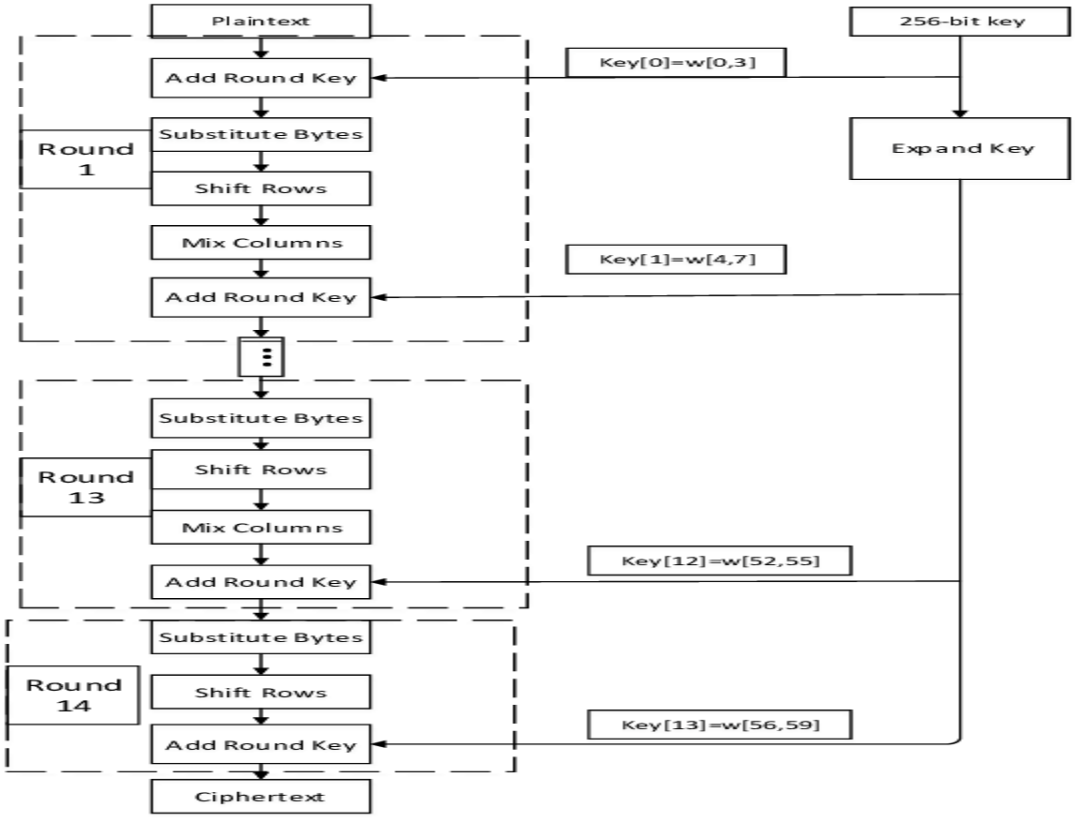


Figure III.16 : chiffrement et déchiffrement de l'AES-256 [23].

III.5. Evaluation des images cryptes par AES-128

Pour le premier choix c'est le chiffrement par l'algorithme AES-128 sans utilisation des modes. Dans cette partie une image BMP 128 bits est chiffrée avec l'algorithme AES-128 sans utilisation des modes l'image est redimensionnée pour avoir un multiple de block 4x4 = 16, qui sera de même taille avec la clé, le résultat de chiffrement est présenté par la figure (III.17).

Figure III.17 : chiffrement et déchiffrement par AES-128.

III.5.1. Evaluation des images cryptes par AES-128 mode CBC

Dans cette étape en a utilisés un crypto système utilisant l'algorithme AES-128 avec le mode CBC pour augmente la sécurité, la figure (III.18) représenté le résultat de chiffrement et déchiffrement, après exécution une image chiffrée est affichée ainsi que l'image déchiffrée. Ce mode a plusieurs avantages, Le mode CBC chiffre le même message clair différemment avec des blocs d'initialisation différents.

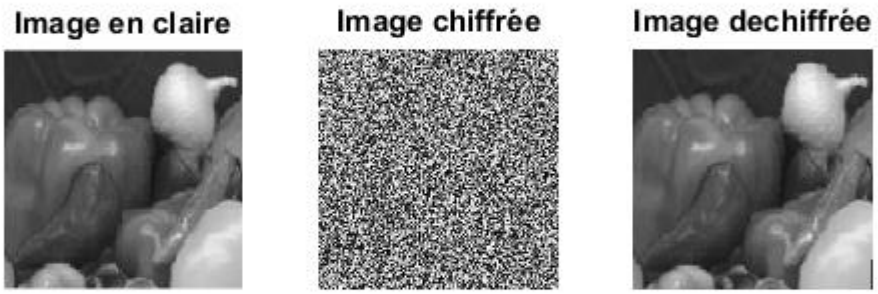
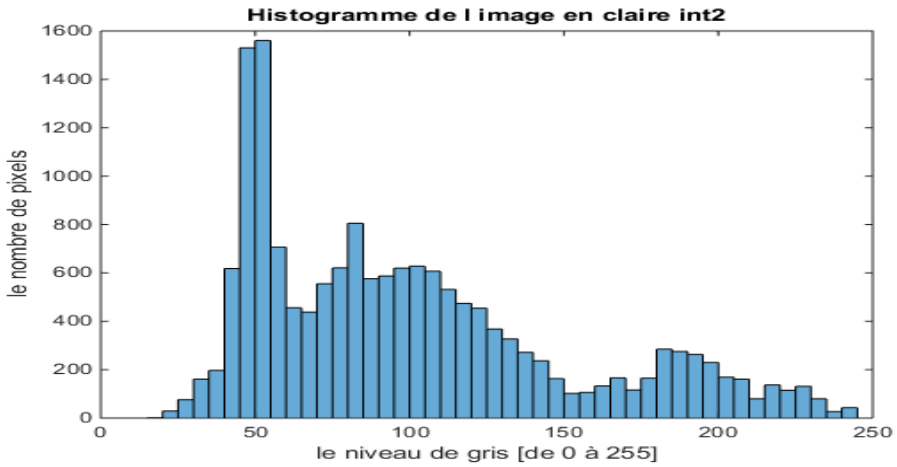


Figure III.18 : chiffrement et déchiffrement par AES-128 mode CBC.

Nous pouvons voir dans la figure (III.19), que l'histogramme des images clair et déchiffrées est le même, qui est différent de l'histogramme de l'image chiffrée, indiquant que l'image déchiffrée et identique à l'image en clair.



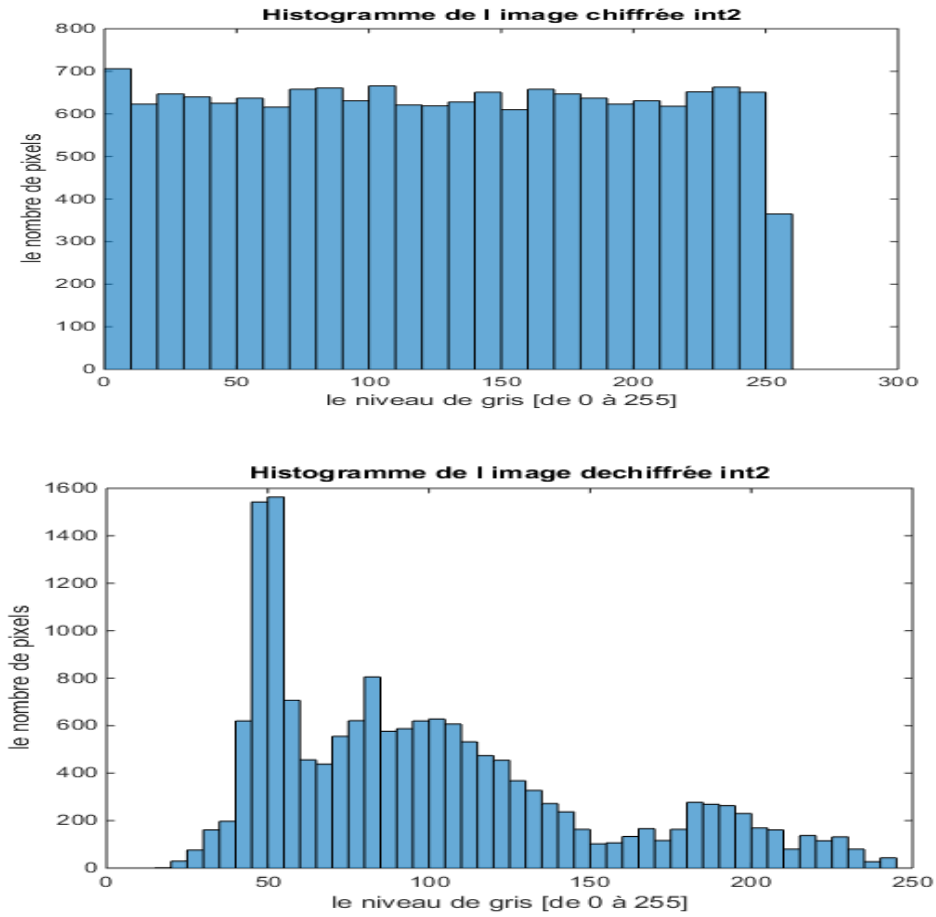


Figure III.19 : Histogrammes des images chiffrer et Déchiffrer par AES-128 mode CBC

Cette figure qui représente les histogrammes des images pour comparer la qualité entre l'image originale et l'image déchiffré.

III.5.2. Evaluation des images cryptées par AES-128 mode OFB

Le mode de chiffrement de rétroaction de sortie (mode OFB, Output Feed Back) a aussi un esprit très différent des modes ECB et CBC. Il s'agit-il aussi d'utiliser la fonction de chiffrement CK comme un générateur pseudo-aléatoire de clés. Le résultat de chiffrement est présenté par la figure (III.20) :

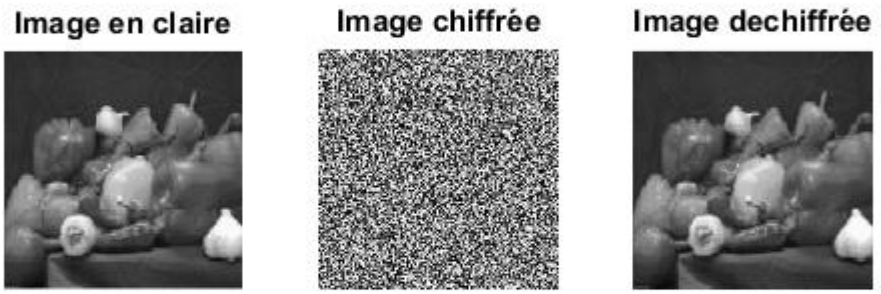
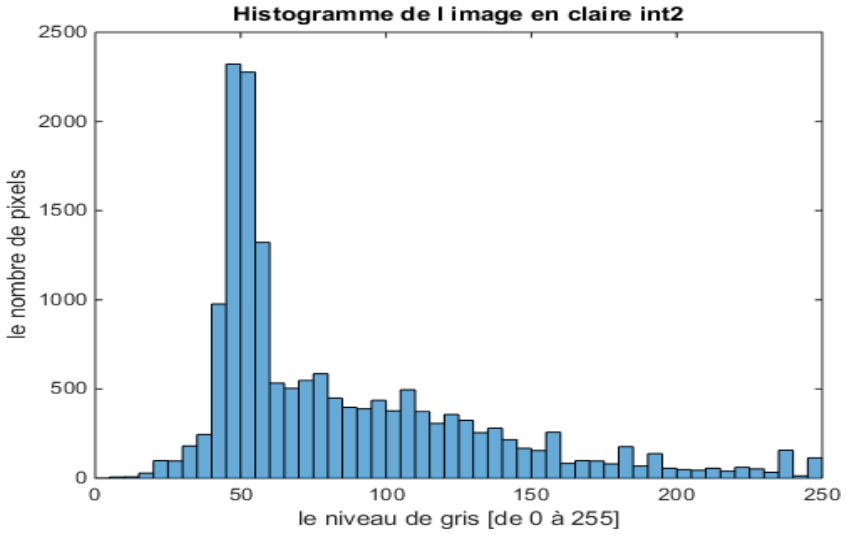


Figure III.20 : chiffrement et déchiffrement par AES-128 par mode OFB.



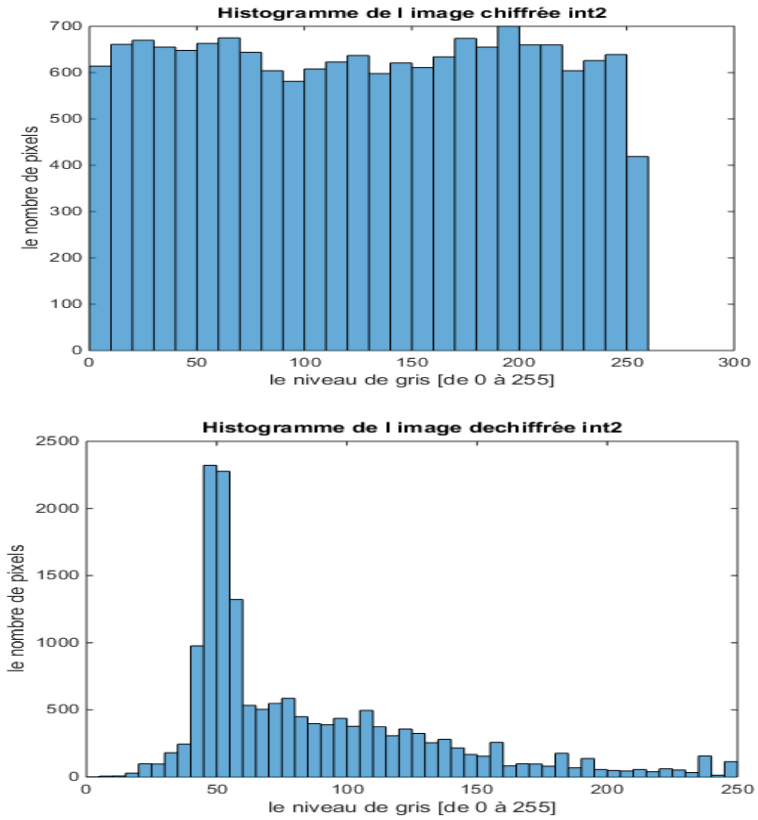


Figure III.21 : Histogrammes des images chiffrer et Déchiffrer par AES-128 mode OFB.

Cette figure (III.21) qui représente les histogrammes des images en clair, chiffrée et celle déchiffrée, nous informe que l'image chiffrée est totalement différente de celle en clair et déchiffrée.

III.5.3. MSE (Erreur quadratique moyenne)

L'image déchiffrée $\hat{I}$ est toujours comparée à l'image originale I ou en claire pour déterminer son rapport de similitude. Ce critère est le plus utilisé, il est basé sur la mesure de l'erreur quadratique moyenne (MSE) calculée entre les pixels originaux et celle déchiffrées :

$$MSE = \frac{1}{M*N}\sum_{m=1}^{M}\big(I(m,n) - I(m,n)\big)^2 \qquad (III.1)$$

Tableau III.1 : Valeur MSE pour l'AES-128 et les deux modes

Chiffrement	AES-128	AES-128-OFB	AES-128-CBC
MSE	0	0	0

On remarque selon le tableau (III.1) que la valeur du MSE entre l'image en clair et celle

chiffrée est égale à zéro dans l'AES-128 et les deux modes, qui impliquent que les images déchiffrées et l'originales sont identiques.

III.5.4. PSNR (Rapport crête signal sur bruit)

Pour ce critère d'évaluation, au lieu de mesurer la distorsion, la valeur (Peak Signal to Noise Ratio, PSNR) mesure la fidélité de l'image déchiffrée par rapport à l'original ou en clair, puisqu'elle est proportionnelle à la qualité. Comme nous pouvons le voir selon l'équation III.2, elle est une fonction de

MSE ; sa définition et son utilisation proviennent du domaine du traitement de signal

$$PSNR = 10Log_{10}\left[\frac{\frac{1}{N}\sum I^2}{MSE}\right] \qquad (III.2)$$

Tableau III.2 : Valeur PSNR pour l'AES et les deux modes.

Chiffrement	AES-128	AES-128-OFB	AES-128-CBC
PSNR	Inf	Inf	Inf

On remarque selon les résultats indiques dans le tableau (III.2), que la valeur du PSNR des images en clair et celle déchiffrée pour l'AES et les deux modes est égale à l'infinie, qui veux dire que les images déchiffrées et l'originales sont identiques.

III.5.5 SSIM (Indice de similarité structurelle)

SSIM est une mesure de similarité entre deux images numériques. Elle a été développée pour mesurer la qualité visuelle d'une image déformée, par rapport à l'image originale. L'idée de SSIM est de mesurer la similarité de structure entre les deux images, plutôt qu'une différence pixel à pixel comme le fait par exemple le PSNR. L'hypothèse sous-jacente est que l'œil humain est plus sensible aux changements dans la structure de l'image

$$u_x = \frac{1}{N}\sum_{1}^{N} x_i \qquad (III.3)$$

Tableau III.3: Valeur SSIM pour l'AES-128 et les deux modes.

Chiffrement	AES-128	AES-128-OFB	AES-128-CBC
SSIM	1	1	1

Selon les résultats présentés dans le tableau (III.3). On va remarquer que la valeur du SSIM des trois images est égale à 1 dans la l'AES-128 et les deux modes, donc les images déchiffrées et l'originales sont identiques.

III.6. Evaluation des images cryptes par AES-256 mode CBC

Dans le premier choix c'est le chiffrement par l'algorithme AES-256 avec utilisation du mode CBC. Dans cette partie une image BMP-256 bits est chiffrée avec l'algorithme AES-256 avec utilisation du mode CBC, l'image est redimensionnée pour avoir un multiple de block 4x8 = 32, qui sera de même taille avec la clé.

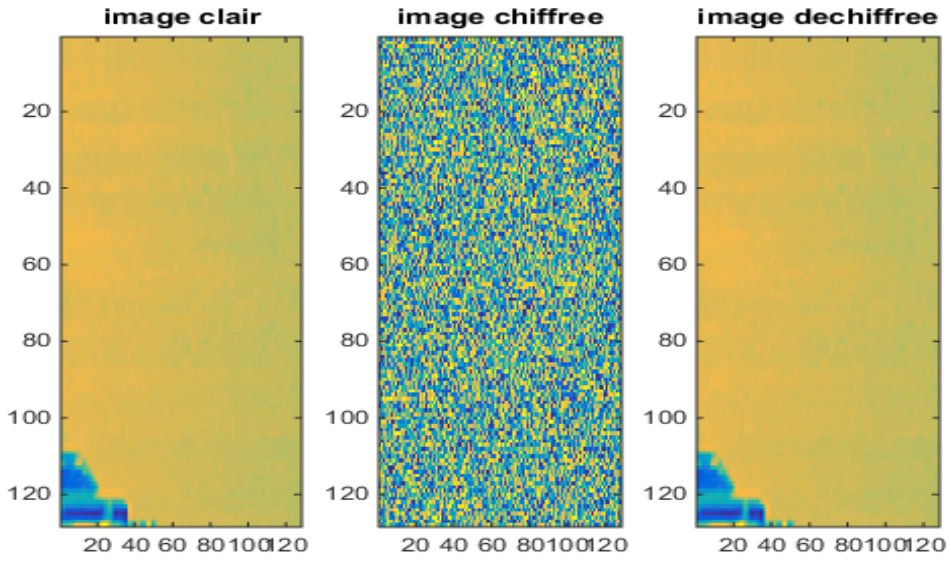


Figure III.22 : chiffrement et déchiffrement par AES-256 mode CBC.

Avec l'œil nu et selon la figure (III.22), représentant l'opération de chiffrement et déchiffrement ave AES-256-CBC, que l'image en clair et la même déchiffrée.

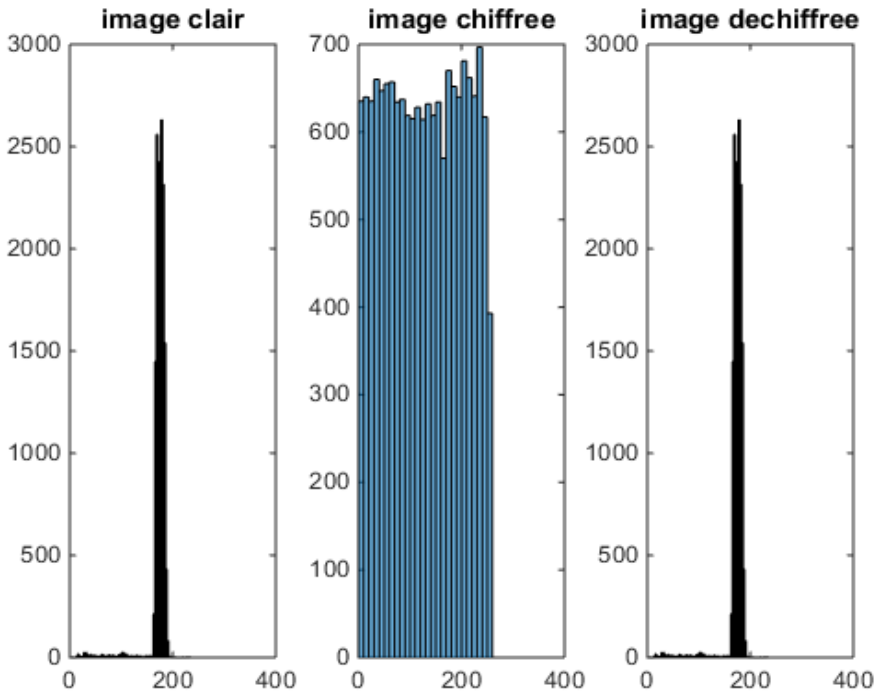


Figure III.23 : Histogrammes des images chiffrer et Déchiffrer par AES-256 mode CBC.

La figure (III.23) illustre les histogrammes des trois images en clair, chiffrée, et déchiffrée. Qui nous informons de la similitude des images en clair, et déchiffrée, de leur différence avec celle chiffrée.

III.6.1. Evaluation des images cryptes par AES-256 mode OFB

Dans cette partie c'est le chiffrement par l'algorithme AES-256 avec utilisation du mode OFB. Dans cette partie une image BMP-256 bits est chiffrée avec l'algorithme AES-256 avec utilisation du mode OFB, l'image est redimensionnée pour avoir un multiple de block 4x8 = 32, qui sera de même taille avec la clé.

.

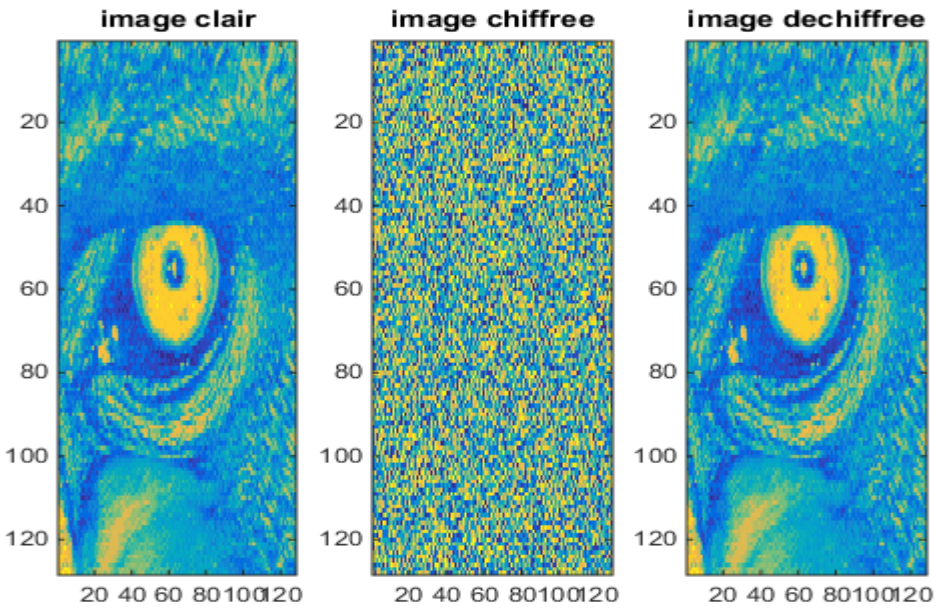


Figure III.24 : chiffrement et déchiffrement par AES-256 mode OFB.

Avec l'œil nu et selon la figure (III.24), représentant l'opération de chiffrement et déchiffrement ave AES-256-OFB, que l'image en clair et la même déchiffrée.

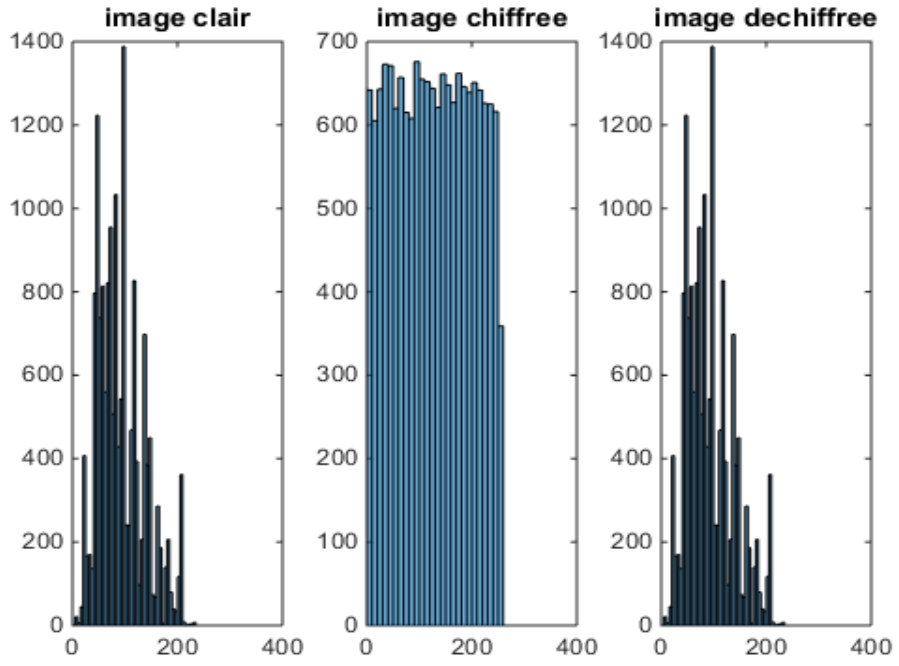


Figure III.25 : Histogrammes des images chiffrer et Déchiffrer par AES-256 mode OFB.

La figure (III.25) illustre les histogrammes des trois images en clair, chiffrée, et déchiffrée. Qui nous informons de la similitude des images en clair, et déchiffrée, de leur différence avec celle chiffrée.

III.6.2. Résultat d'évaluation des images cryptes par AES-256 par les maitrises MSE, PSNR et SSIM

Après les chiffrements et déchiffrements on à résumer les résultats des différentes métrise (SSIM, PSNR, MSE) dans ce tableau (III.4):

Tableau III.4 : Résultats des métrise par l'AES-256 et les modes CBC, OFB

Mode de chiffrement	AES-256	Mode CBC	Mode OFB
MSE	0	0	0
PSNR	Inf.	Inf.	Inf.
SSIM	1	1	1

Dans ce tableau on va réduire tous les maitrise des tous les images, donc l'image d'origine identique avec l'image chiffrée par les deux modes et le chiffrement par AES-256.

III.7. Comparaison entre AES-128 et AES-256 (résultats des différents modes).

Après les chiffrements et déchiffrements on à résumer les résultats des différentes métrise (SSIM, PSNR, MSE) dans ce tableau :

Tableau III.5:Résultats des métrise.

Mode chiffrement par l'AES-128	**CBC**			**OFB**		
métrise	**MSE**	**PSNR**	**SSIM**	**MSE**	**PSNR**	**SSIM**
	0	Inf	1	0	Inf	1
Mode chiffrement par l'AES-256	**CBC**			**OFB**		
métrise	**MSE**	**PSNR**	**SSIM**	**MSE**	**PSNR**	**SSIM**
	0	Inf	1	0	Inf	1

Les résultats du tableau (III.5), indiquent que les deux modes de chiffrement avec les deux types de l'algorithme AES-128 et AES-256, nous en donnes de bons résultats pour la sécurisations des images de différentes extensions.

III.8. Conclusion

Dans ce chapitre nous avons utilisé l'algorithme AES-128 et AES-256 pour chiffrer différentes images avec les deux modes CBC et OFB. Et pour l'évaluation des résultats nous avons utilisé trois métrises tel que MSE, SSIM, et le PSNR, où les résultats ont été satisfaisantes, et nous avons également conclu que :

-la taille d'une après le cryptage et le décryptage reste inchangée qu'il s'agisse L'AES-128 ou L'AES-256

-Une image ne peut être décryptée qu'avec la clef utilisée pour son cryptage

-L'image ne peut être décryptée qu'avec une clef de longueur de 128 bits (16 octets) et clef de longueur de 256 (32 octets)

-Tout format d'image peut être cryptée et décryptée avec cette algorithme AES-128 et AES-256.

Conclusion Générale

Conclusion générale

L'un des systèmes de cryptographiques les plus utilisés de nos jours est le standard de chiffrement avancé (Advanced Encryption Standard ou AES), aussi connu sous le nom de Rijndael.

L'AES est un algorithme de chiffrement par bloc symétrique qui utilise une clé de (128-192 et 256) bits. Le choix de cet algorithme répond à de nombreux critères : c'est un algorithme qui ne présente qu'une seule étape (un bloc). Par conséquent, le calcul est simple, ce qui entraine une grande rapidité de traitement. C'est directement la force de l'algorithme et l'utilisation des clés secondaires construites par extension de la clef originale complique quant à elle les attaques liées aux clés en cassant les symétries.

Dans ce mémoire, nous avons étudié le problème lié à la protection des images. Qui concerne la transmission sécurisée d'images ainsi d'assurer la fonction de confidentialité des images transmis. Pour cela nous avons utilisés un crypto système qui se base sur l'algorithme AES-128 et AES-256.

Nous avons présenté en détail notre travail qui se penches sur le côté cryptographique, qui s'inscrit dans le cadre de la sécurité des images, par l'algorithme AES-128 et AES-256. Le caractère de ce travail consiste à évoluée un Crypto système à base de l'algorithme AES-128 et AES-256 pour assurer la confidentialité. Nous avons présenté en général la constitution de ces éléments de base, une description de l'algorithme AES ainsi que les types d'images utilisé qui est décrites afin de l'adapter pour une transmission en mode chiffré. Notre Crypto système est composé deux étages : étage d'émission et celui de la réception. A l'émission la clef est introduite puis l'image que nous voulons transmettre est sélectionnée. Ensuite nous avons chiffré cette dernière par les deux algorithmes AES-128 et AES-256 seul afin de garantir la confidentialité. A la réception de ces images, des fonctions réversibles sont élaborés pour les déchiffrer, puis l'utilisation des deux modes de chiffrement tel que CBC et OFB sont introduits en association avec l'AES pour augmenter la sécurité.

Pour tester notre Crypto système et analyser ces résultats, nous avons exploitées plusieurs métriques d'évaluation de la qualité des images déchiffrement (calcul de l'indice de similitude SSIM, le calcule erreur quadratique moyenne MSE et le calcule aussi du Rapport crête signal sur bruit PSNR) entre l'image originale et celle déchiffrée.

A partir des résultats obtenus, nous avons remarqué que toutes les métrise exploitées dans ce travail tel que SSIM, MSE, et PSNR pour les deux modes d'opérations (CBC et OFB) sont de valeurs qui nous indiques que l'image déchiffrée et la même que l'image original, ce qui signifie que les informations que porte l'image ne sont pas altérer.

Dans la perspective de ce travail, et pour démontrer l'altération de l'image chiffrée et de l'image originale, nous améliorerons notre approche de chiffrement d'image robuste en ajoutant une étape d'encodage et de compression des données pour augmenter la sécurité.

Bibliographies

Bibliographies

[1] Joëlle Roue.,(2015), « Analyse de la résistance des chiffrements par blocs aux attaques linéaire et différentielles », université Pierre et Marie Curie Paris VI .

[2] SOUICI Ismahane,(2013), « Sécurisation évolutionnaire du transfert d'images », Thèse de Doctorant, UNIVERSITE BADJI MOKHTAR-ANNABA.

[3] E. Ramaraj, S. Karthikeyan and M. Hemalatha, (2009), A Design of Security Protocol using Hybrid Encryption Technique AES- Rijndael and RSA, International Journal of the Computer, the Internet and Management Vol. 17, No1, pp 78-86.

[4] Beloucif Assia, (2016), « Contribution à l'étude des mécanismes cryptographiques », Thèse Doctorat, Université de Batna 2,

[5] Bruce Schneier, (2007), *Applied cryptography: protocols, algorithms, and source code inC*. john wiley & sons,

[6] FILALI Mohamed Amine, (2015), « Etude et Implémentation Pipeline sur FPGA de L'algorithme de Chiffrement AES », Thèse de Magister, Université des Science et Technologie d'Oran Mohamed Boudiaf.

[7] Aicha TEKKOUK, (2010), « Etude et Implémentation d'une méthode cryptanalyse pour le chiffrement continu », Thèse de Magister, Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf.

[8] National Institude of standard and Technology (NIST) Advanced encryption standard (AES),(2001).FIPS.197

[9] Salhi asma, Bakiri kamilia,(2015), « FPGA-Based cryptosystem «, these de master, Institute of Eloctronical and Electronic Engineering, University Mhamed Bougara, Boumerdes, juin

[10] Zine El Abidine ALAOUI ISMAILI, Ahmed MOUSSA, (2009), « Self-Partial and Dynamic Reconfiguration Implementation for AES using FPGA», IJCSI International Journal of Computer Science Issues, Vol. 2, National School of Applied Sciences, Morocco.

[11] Sambasiva Reddy, Y. Amar Babu, (2013), «Evaluation of Microblaze and Implementation of AES Algorithm using Spartan-3E», Babu2 International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 7, Juillet.

[12] Nabil Litayem, **(**2014 **), «** Contributions méthodologiques à la conception et optimisation de systèmes embarqués », thèse de doctorat, Université De Carthage**,** Juillet.

[13] Sandrine julia **«** TECHNIQUES DE CRYPTOGRAPHIES ».

[14] https://www.math.Univ-paris13.fr/~boyer / enseignement / Poly Crypto 2010. pdf.

[15] Z . Wang .A.C.Bovik.H.R.Sheikh and E.P.Simocelli , **«** Image Quality Assessment».

[16] Yue Wu, Joseph P. Noonan, Sos Agaian, (2011), **«** NPCR and UACI Randomness Tests for Image Encryption », Journal of Selected Areas in Telecommunications, pp. 31-38.

[17] Léon Robichaud, **«** L'image numérique Pixels et couleurs », support de cours, Département d'histoire, Université de Sherbrooke.

[18] O. Poutarédy,(2015 **), «** Différences entre image Bitmap et image vectorielle », Site des enseignantsen Arts Appliqués de l'académie d'Orléans-Tours,

[19] https://briot-jerome.developpez.com/matlab/tutoriels/introduction-gestion-images/

[20] Serge WACKER, **«** Les formats d'images numériques », C2I niveau 1,

[21] Image file formats. Wikipedia, Https://en.wikipedia.org/wiki/Image_file_formats. http://serge.wacker.free.fr/technoprimaire/c2i/revisions/formats_image.pdf , consulté le 19-04-2018.

[22] Florent Bruguier, Pascal Benoit et Lionel Torres, (2016), « Théorie et Mise en Pratique sous la Forme d'un Stage Technologique », Formation en Sécurité Numérique, Université de Montpellier, France, 5 Jan.

[23] R.Isdant.(2009),Traitement numérique de l'image .Http://www.montpellier.iufm.fr/technoprimaire, consulté le: 02/06/2019.

[24] C. Paar , J. Pelzl,(2010), «Understanding Cryptography, Springer-Verlag Berlin Heidelberg«, ISBN 978-3-642-04100-6.

[25] O. Azzouzi, (2014), Système embarqué flexible pour un chiffrement hybride symétrique / asymétrique, Mémoire de Magistère en Informatique, Ecole
Nationale Supérieure, Oued Smar, Algérie,
[26] Thomas Roche, (2010), « Dimensionnement et intégration d'un chiffre symétrique dans le contexte d'un système d'information distribué de grande taille », mémoire de master, Université de Grenoble.