Université KASDI-MERBAH Ouargla

Faculté des Nouvelles Technologies de l'information et de la Communication

Département d'informatique et des Technologie de l'information

Mémoire de Fin de Cycle

Présenté pour l'obtention du diplôme de

MASTER ACADEMIQUE

Domaine : Mathématiques et Informatique

Filière : informatique

Spécialité : Administration et sécurité des réseaux

Présenté par: Khouildat Hadjer

Thème:

Méthode de cryptage d'image basée sur la permutation et la matrice de Householder

Soutenu en 02 juillet 2019 devant le Jury

Mme. Khelili Farida	Président	UKM Ouargla
Mme. Djebaili Karima	Encadreur	UKM Ouargla
Mme. Merzougui Naima	Examinateur	UKM Ouargla

Année Universitaire :2018/2019

Remerciement

Avant tous, nous tiens à remercier Dieu de nous avoir donné la chance de suivre le Chemin de la science.

A l'issue de ce modeste travail, nous tiens à exprimer mes sincère

Remerciements à :

Notre encadreur, madame Md Karima Djebaili, Qui nous a aidé par Ses orientations et ses précieux conseils pour l'élaboration De cette étude.

Tous les enseignants de département d'informatique (Filière d'informatique) Qui ont participé à notre formation

Nous exprimons toute nos gratitude et nos respect aux membres de jury qui

Nous feront l'honneur d'apprécier ce modeste travail.

Dédicace

Je dédie ce travail à mes très chers parents, pour leur soutien et tous les efforts Qu'on m'a donnée le long de mon parcours et je

Leurs souhaite bonne santé et longue vie.

Je dédie ce travail aussi à mes frères et mes sœurs.

A toute ma famille, tous mes amis

Et tous ceux que j'aime et qui m'aiment

A tous mes enseignants qui ont fait leurs possibles pour nous Donner le maximum d'informations concernant notre étude

Merci infiniment

Résumé

Avec le grand développement de l'utilisation des réseaux de communication, beaucoup des informations sont transmets sur ce réseau tel que les images numériques sont des informations qui ont besoin de protection, donc la meilleure solution pour ce problème est l'utilisation de système de cryptage.

Dans ce mémoire, nous proposons une nouvelle méthode de cryptage d'image basée sur la matrice Householder, pour éliminer la complexité de calculé l'inverse de la clé de déchiffrement, ainsi, facilite la transmission de la clé secret. Aussi, nous utilisons une technique de permutation des pixels pour assurer les propriétés de la confusion et la diffusion, pour chiffrer les images qui contiennent des grandes zones d'une couleur unique.

Les résultats expérimentaux tels que les tests statistiques et les testes différentielles montre l'efficacité de notre méthode ainsi sa résistance aux attaques de texte claire connues et choisies. Enfin, le temps d'exécution et le temps de transmission sont rapides.

Mots clés : cryptage d'image, matrice Householder, attaque en texte claire connu, attaque en texte claire choisie.

Abstract

With the great development of the use of communication networks, a lot of information is transmitted over this network such as digital images are information that need protection, so the best solution for this problem is the use of encryption system.

In this memoir, we propose a new method of image encryption based on the Householder matrix, to eliminate the complexity of computed the inverse of the decryption key, thus, facilitates the transmission of the secret key. Also, we use a pixel permutation technique to ensure the properties of confusion and diffusion, to encrypt images that contain large areas of a single color.

Experimental results such as statistical tests and differential tests show the effectiveness of our method to resist known and chosen plaintext attacks. Finally, the execution time and the transmission time are fast.

Keywords: Image Encryption, Householder matrix, known plaintext attack, chosen plaintext attack.

ملخص :

إن التطور الكبير في استخدام شبكات الاتصال، ساهم كثيرا في نقل العديد من المعلومات عبر هذه الشبكة، مثل الصور الرقمية فهي معلومات تحتاج إلى الحماية و الأمن، وبالتالي فإن أفضل حل لهذه المشكلة هو استخدام نظام التشفير.

في هذه المذكرة، نقترح طريقة جديدة لتشفير الصور وذالك باستعمال مصفوفة الهوس هولدر التي تساهم في نزع التعقيد الحسابي لإيجاد المفتاح العكسي لفك التشفير. كما يسهل نقل المفتاح السري.كما نستخدم تقنية تبادل البكسل لضمان خصائص التشويش والانتشار. لتشفير الصور التي تحتوي على لون واحد.

تُظهر النتائج التجريبية، مثل الاختبارات الإحصائية والاختبارات التفاضلية، بان الطريقة المقترحة لتشفير فعالة كما أنها مقاومة لاختراقات وهجمات النص العادي المعروف والمختار. أخيرًا هدفنا من الطريقة المقترحة هو تسريع وقت تنفيذ البرنامج وتسريع إرسال المفتاح السري.

الكلمات المفتاحية: تشفير الصور، مصفوفة الهوس هولدر، هجوم النص العادي المعروف، هجوم النص المختار.

Table des matières

Liste des figures

Liste des Tableaux

Introduction Générale

Introduction Générale:

Aujourd'hui, le monde connait un grand développement dans le domaine des technologies de l'information et des réseaux de communication, spécialement la croissance rapide de transmission des informations multimédia telles que les vidéos, et les images (l'imagerie médicale, les communications militaires ……etc.) à travers ces réseaux.

Le problème qui se pose; comment protégé la transmission d'une image numérique à travers des canaux de communication non sécurisé ? Donc, il est nécessaire de chiffrer les images avant leur transmission sur le réseau. La cryptographie transforme l'image en clair en image cryptée (incompréhensible). Les cryptosystémes textuels tels que DES, Triple-DES, AES et RSA ne peuvent pas être utilisés pour chiffrer l'image, a cause de sa taille ainsi, ces algorithmes ne considère pas les propriétés statistiques de l'image tel que la forte corrélation entre les pixels.

De nombreux algorithmes ont été proposés pour chiffrer l'image, tels que le chiffrement de Hill, le chiffre de Vigenère et le chiffre d'Affine, ces cryptosystèmes sont vulnérable aux attaques ; telles que les attaques en texte clair choisies ou connues, et la difficulté de transmet la clé secret a cause de ce taille.

Dans ce mémoire, nous proposons une nouvelle méthode de cryptage d'image basée sur la matrice Householder, pour éliminer la complexité de calculé l'inverse de la clé de déchiffrement, ainsi facilite la transmission de cette clé. Aussi, nous utilisons une technique de permutation des pixels pour assurer les propriétés de la confusion et la diffusion, pour chiffrer les images qui contiennent des grandes zones d'une couleur unique.

Organisation du mémoire

Notre mémoire est organisé comme suit:

Dans le premier chapitre, nous présentons les concepts fondamentaux et la terminologie de la cryptographie, puis nous présentons leurs objectifs et ces différents types.

Le deuxième chapitre, décrit les notions de base et les différents types des images numériques.

Le troisième chapitre, présente en détaille notre méthode utilisée pour le cryptage d'image et son implémentation puis, nous terminons par un ensemble des tests qui montrent l'efficacité de cette méthode.

Enfin, nous terminons notre mémoire par une conclusion générale et des perspectives.

Chapitre I :
La Cryptographie

1. Introduction :

La sécurité informatique est un domaine très important dans notre vie qui protège les informations et les données dans les réseaux de communication, donc pour garantir la sécurité d'informatique en 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 expliquons les terminologies de base de la cryptographie, puis nous allons parler sur leurs objectifs et ces différents types. Enfin, en termine par les types des attaques.

1) Introduction à la sécurité informatique

2.1 Sécurité Informatique

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles [1].

2.2 La vulnérabilité

Faiblesse / faille : faute accidentelle ou intentionnelle introduite dans spécification, conception ou configuration du système [2].

2) La terminologie de la cryptographie

3.1 Cryptologie

Il s'agit d'une science mathématique comportant deux branches: la cryptographie et la cryptanalyse [3].

Cryptologie = Cryptographie + Cryptanalyse

3.2 Cryptographie

Discipline incluant les principes, les moyens et les méthodes de transformation des données, dans le but de masquer leur contenu, d'empêcher leur modification ou leur utilisation illégale [4].

3.3 La cryptanalyse

Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés [3].

3.4 Clef

Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement [3].

Le principe général d'un algorithme de chiffrement ce montre dans la figure sous-dessus

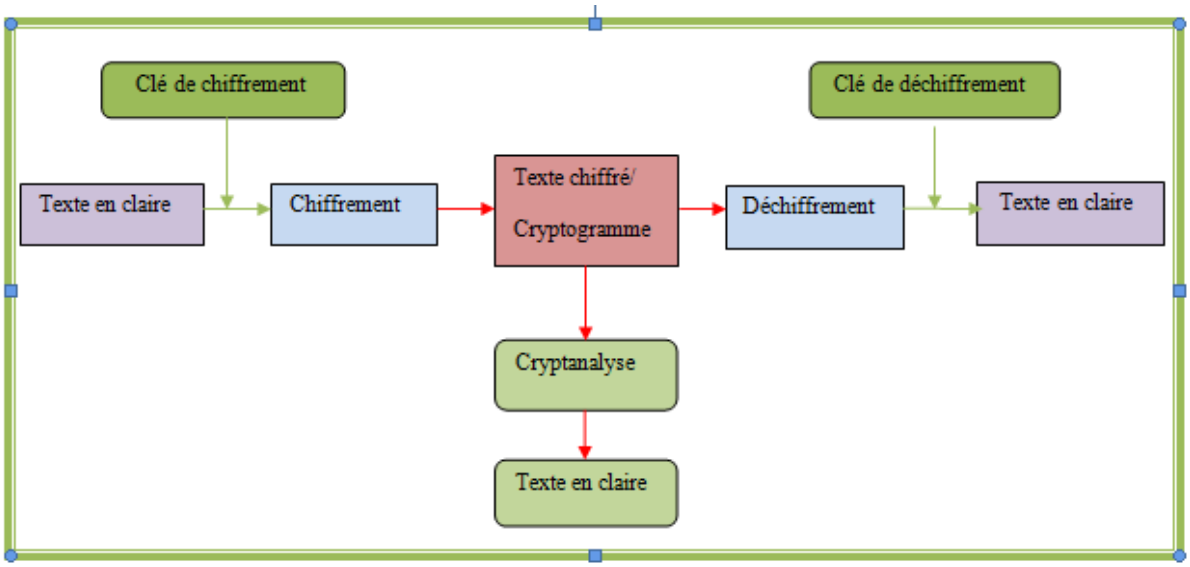


Figure 1.1: Principe générale d'un algorithme de chiffrement

3) Les objectifs de la cryptographie [5]

Les buts de la cryptographie sont :

3.1. La confidentialité

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

3.2. Intégrité

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

4.3. Authentification

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

4.4. Non-répudiation

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

5. Les différents types de cryptographie

Nous pouvons regrouper les systèmes de chiffrement en deux catégories:

5.1 La cryptographie classique.

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

5.1.1 Le chiffrement par substitution

Le chiffrement par substitution consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou plusieurs autres entités [3].

5.1.2 Le chiffrement par transposition

Le chiffrement par transposition (ou le chiffrement par permutation) consiste à faire un réarrangement de l'ordre des lettres qui cache le sens initial. Cette méthode demande de découper le texte clair en blocs de taille identique, et applique la même permutation sur chacun des blocs [3].

5.2 La cryptographie moderne

La cryptographie moderne se compose de deux grandes familles selon le principe de fonctionnement, comme montre la figure 1.2:

- La cryptographie symétrique.
- La cryptographie asymétrique.

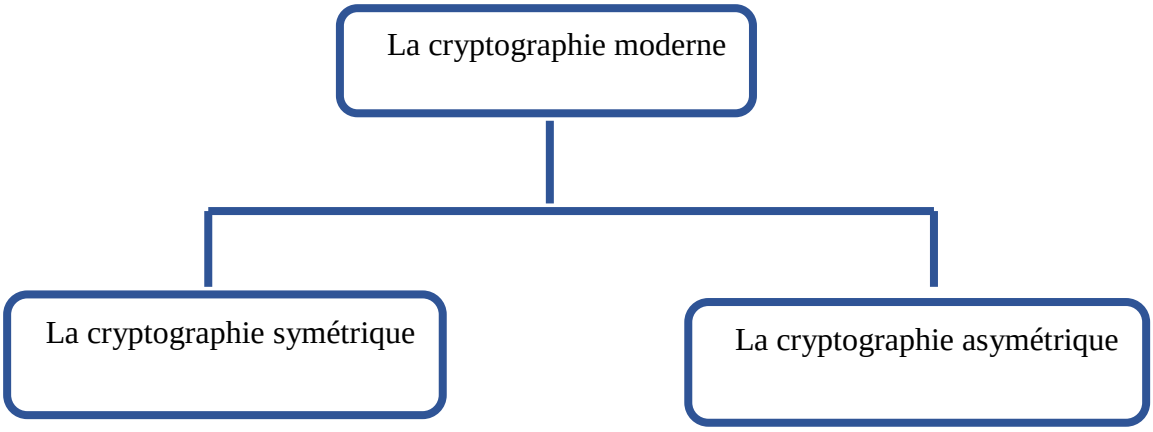


Figure 1.2: les méthodes de la cryptographie moderne.

5.2.1. La cryptographie symétrique ou à clé secrète

La cryptographie symétrique, également dite à clé secrète (par opposition à la cryptographie asymétrique), est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé [11].

Les algorithmes les plus répandus sont : RC4 DES, AES, 3DES, …etc.

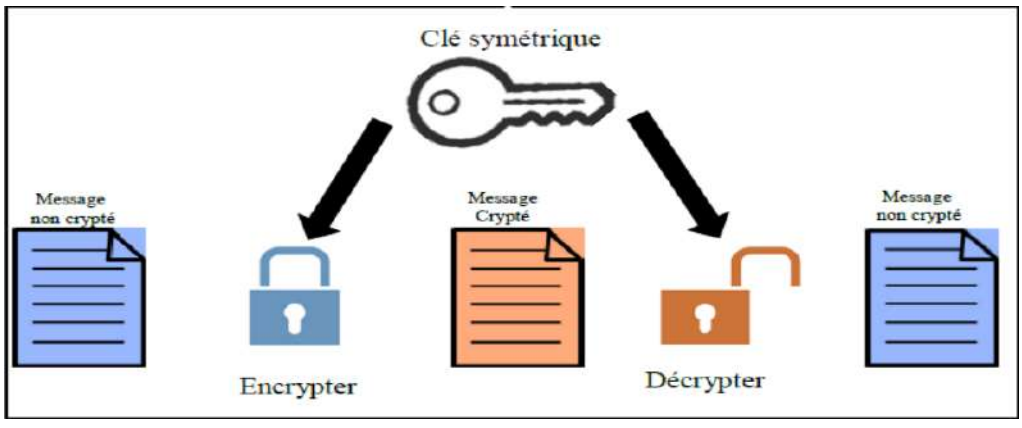


Figure 1.3 : La cryptographie symétrique [7].

Il existe deux grandes familles de chiffrement dans ce type :

5.2.1.1. Chiffrement par blocs

On désigne par chiffrement par blocs (block-chiper en anglais), tout système de chiffrement (symétrique) dans lequel le message clair est découpé en blocs d'une taille fixée, et chacun de ces blocs est chiffré [8].

5.2.1.2. Chiffrement par flots

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

– RC4 : chiffrement octet par octet.

5.2.1.3. Les limites du chiffrement symétrique

Le principal inconvénient de cryptographie symétrique provient de l'échange des clés. Ce qui peut constituer une faille à la sécurité du système. Un échange de clé en main propre est préféré lorsque cela est possible.

5.2.2. La cryptographie asymétrique ou à clé public

Le principe de chiffrement asymétrique (appelé aussi chiffrement à clés publiques) est apparu en 1976, avec la publication d'un ouvrage sur la cryptographie par Whitfield Diffie et Martin Hellman. Dans un cryptosystème asymétrique (ou cryptosystème à clés publiques), les clés existent par paires :

- Une clé publique pour le chiffrement.
- Une clé secrète pour le déchiffrement [14].

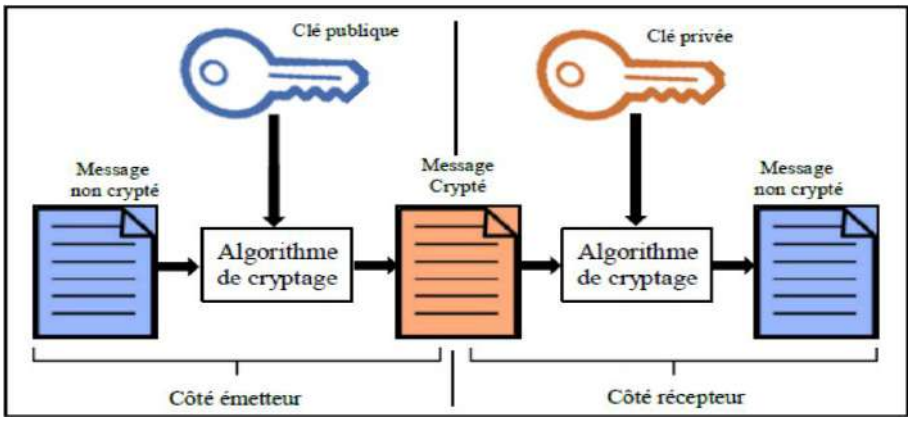


Figure 1.4 : Cryptographie asymétrique [7].

5.2.2.1. Les limites du chiffrement asymétrique

Le principal inconvénient de cryptographie asymétrique est lié à l'échange de clé via un canal non sécurisé. Ces derniers restent beaucoup moins efficaces en termes de temps de calcul que les algorithmes symétriques.

5.2.3. Comparaison entre la cryptographie symétrique et asymétrique

La figure ce dessus montre le tableau de comparaison entre la cryptographie symétrique et symétrique :

Le type de crypto système	Les avantages	Les inconvénients
Symétrique (clé secrete)	• Clés relativement courtes (128 ou 256 bits) • Rapide • Facile	• Gestion des clés difficiles (nombreuses clés) • Difficulté de distribuer la clé secrète • Ne permet pas de signature électronique
Asymétrique (clé public)	• Utilise deux clés différentes • Fournit des garanties d'intégrité et de non répudiation par signature électronique • Très utile pour échanger les clés	• Des clés plus longues (1024 à 4096 bits) • Lenteur de calcul • Difficile

Tableau 1.1: La comparaison entre la cryptographie symétrique et asymétrique [15].

5.2.4. Cryptage hybride

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

– Dans un premier temps, l'émetteur choisit une clé symétrique K aléatoire. Il utilise ensuite Cette clé K pour chiffrer (symétriquement) le message.

– Puis il chiffre (asymétriquement) la clé K avec la clé publique du destinataire. Il envoie à son destinataire le message chiffré et de K. Le destinataire déchiffre d'abord la clé K, puis l'utilise pour retrouver le message [16].

6. Les types d'attaques

Différents types d'attaques de chiffrement sont décrits ci-dessous:

6.1 Attaque par texte chiffré uniquement

Cryptanalyse à texte chiffré de plusieurs messages, qui ont tous été chiffrés à l'aide du même algorithme de chiffrement. Le travail de cryptanalyse consiste à récupérer le texte en clair ou à en déduire la clé utilisée pour chiffrer le message, afin de décrypter d'autres messages chiffrés avec les mêmes clés [16].

6.2 Attaque en texte clair connu

Le cryptanalyse a non seulement accès aux textes chiffrés de plusieurs messages, mais aussi aux textes clairs correspondants. La tâche est de retrouver la ou les clés qui ont été utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer d'autres messages chiffrés avec ces mêmes clés [6].

6.3 Attaque en texte clair choisi

Le cryptanalyse a non seulement accès aux textes chiffrés et aux textes clairs correspondants, mais de plus il peut choisir les textes en clair. Cette attaque est plus efficace que l'attaque à texte clair connu, car le cryptanalyse peut choisir des textes en clair spécifiques qui donneront plus d'informations sur la clé [6].

6.4 Une attaque sur texte chiffré choisi

Le cryptanalyse peut choisir différents textes chiffrés à déchiffrer. Les textes déchiffrés lui sont alors fournis. Par exemple, le cryptanalyse a un dispositif qui ne peut être désassemblé et qui fait du déchiffrement automatique. Sa tâche est de retrouver la clé [6].

7. État de l'art sur les techniques de cryptage d'image

7.1 Fibonacci

Leonardo Fibonacci (v. 1175 à Pise - v. 1250) est un mathématicien italien. Il avait, à l'époque, pour nom d'usage «Leonardo Pisano» (il est encore actuellement connu en français sous l'équivalent « Léonard de Pise »), et se surnommait parfois lui-même « Leonardo Bigollo » (bigollo signifiant « voyageur » en italien). S'il est connu pour la suite de Fibonacci, il joue surtout un rôle d'une importance considérable en faisant le lien entre le savoir mathématique des musulmans, notamment des chiffres indoarabes, et l'Occident [19].

7.2 Choas

Le chaos est défini par un comportement lié à l'instabilité et à la non-linéarité dans des systèmes dynamiques déterministes. La relation entre l'instabilité et la chaoticité est alors que le système manifeste une très haute sensibilité aux changements de conditions est ce qu'affirmait Henri Poincaré à la fin du 19ème siècle : «Une cause très petite, qui nous échappe, détermine un effet considérable que nous ne pouvons pas ne pas voir, et alors nous disons que cet effet est dû au hasard (...). Il peut arriver que de petites différences dans les conditions initiales en engendrent de très grandes dans les phénomènes finaux. Une petite erreur sur les premières produirait une erreur énorme sur les derniers. La prédiction devient impossible et nous avons le phénomène fortuit» [17]. Les cartes chaotiques peuvent être utilisées, dans les applications liées à la sécurité de l'information, pour la génération des clés secrètes dans les algorithmes de cryptage et de tatouage numérique [32].

7.3 Permutation

La permutation d'image basée sur le changement de place d'une partie de l'image, il existe trois techniques de ce mécanisme :

7.3.1. Permutation binaire (permutation des bits)

L'image peut être considérée comme un tableau de pixels, chacun avec huit bits pour 256 niveaux de gris. Dans cette technique de permutation les bits de chaque pixel pris de l'image sont permutés avec la clé choisie à partir de l'ensemble de touches à l'aide du générateur d'index Pseudo aléatoire. Toute la gamme de ces les pixels permutés forme l'image chiffrée. L'image chiffrée obtenue à partir du bit la technique de permutation est transmise au récepteur par le canal non sécurisé [22].

7.3.2. Permutation par pixel

Dans ce schéma, chaque groupe de pixels est extrait de l'image. Les pixels du groupe sont permutés en utilisant la touche sélectionnée à partir de l'ensemble de touches. La procédure de cryptage et de décryptage est la même que la technique de permutation des bits. La taille du groupe de pixels est identique à la longueur des clés, et toutes les clés sont de même longueur. Si la longueur des touches est supérieure à la taille du groupe de pixels, le l'information de perception diminue [22].

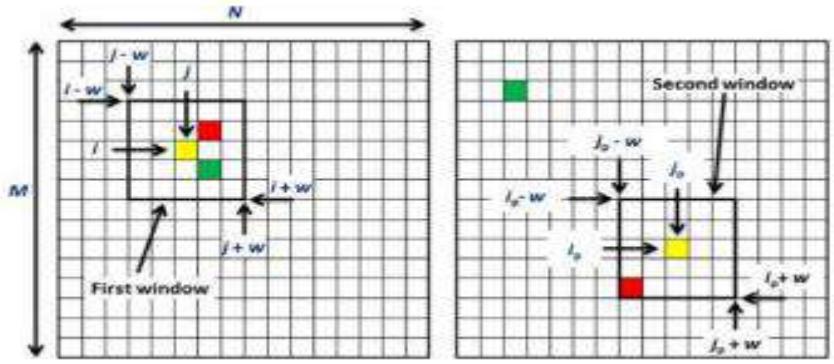


Figure 1.5 : Exemple sur la permutation pixel [23].

7.3.3. Permutation par bloc

Dans cette technique, l'image peut être décomposée en blocs. Un groupe de blocs est tiré de la l'image et ces blocs sont permutés mêmes que les permutations de bits et de pixel. Pour un meilleur cryptage la taille du bloc doit être inférieure. Si les blocs sont très petits, alors les objets et ses bords n'apparaissent clairement. Dans ce bloc de permutation les blocs sont permutés horizontalement dans l'image. La permutation des blocs le long du côté vertical est également semblable à la permutation horizontale de bloc latéral [22].

8. Conclusion

Dans ce chapitre, nous avons expliqué les terminologies de base de la cryptographie, puis nous avons parlé sur leurs objectifs et ces différents types. Enfin, en termine par les types des attaques. Dans le chapitre suivant, nous allons présenter les notions de base sur les images numériques.

Chapitre II :

Généralité Sur Les Images Numériques

1. Introduction :

Dans ce chapitre, nous allons parler aux concepts de base sur l'imagerie et l'imagerie numérique. Puis nous allons parler sur les attributs et les types et les formats d'image. Enfin nous avons parlé sur ces différents modes de couleurs.

2. Notions de base sur l'image

2.1. Définition de l'image

Une image peut être définie comme une fonction bidimensionnelle, f (x, y), où x et y sont des coordonnées spatiales (plan), et l'amplitude de f à n'importe quelle paire de coordonnées (x, y) s'appelle l'intensité ou le niveau de gris de l'image à ce point [12].

2.2. L'image numérique

Une image numérique est composée des cases appelées « pixels ». Ces pixels seront affectés de nombres binaires permettant de définir des teintes de gris ou des couleurs [13].

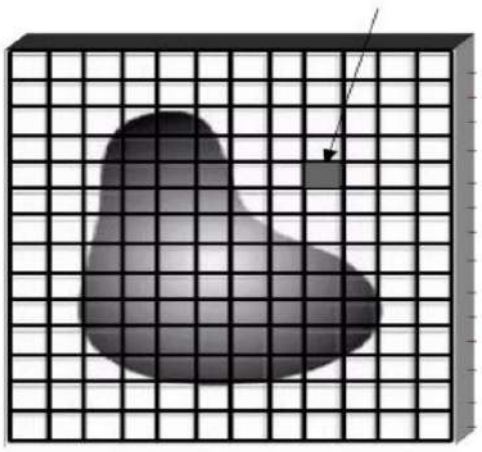


Figure 2.1 : Image numérique.

2.3. Les attributs des images

2.3.1. Pixels

Le pixel représente la plus petite unité d'une image numérique appelé en anglais (**PIC**ture **El**ement). Les nombres des pixels de ligne et les nombres des colonnes déterminent la démentions de l'image, et chaque pixel représente valeur (couleur).

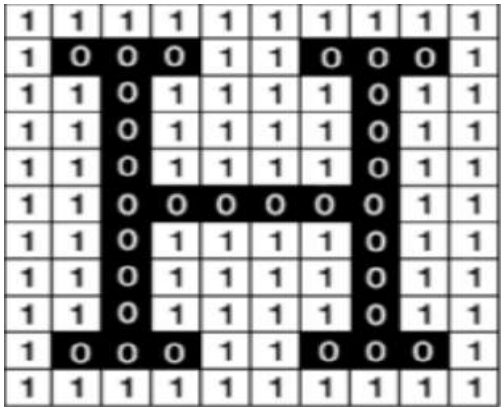


Figure 2.2 : Les pixels d'une image numérique.

2.3.2 La taille

La taille de l'image est la place qu'elle occupe dans le codage binaire. Son unité est «l'octet» [13].

Taille = nombre d'octets pour chaque pixel × définition

2.3.3 Résolution

La résolution d'une image c'est le nombre de pixels par unité de longueur dpi (dot per inch). Si la résolution est élevée alors la meilleure qualité d'image.

3. Types d'image numérique.

Il existe deux types d'images numériques :

3.1 Les images matricielles

Formée d'une grille composée de pixels. Plus on zoom, plus les pixels deviennent apparents [24]. Les formats d'images bitmap : BMP, PCX, GIF, JPEG, TIFF. On obtient également des images matricielles à l'aide d'un appareil photo numérique, d'une caméra vidéo numérique ou d'un scanner [9].

3.2 Les images vectorielles

L'image vectorielle utilise également la technique du Pixel, mais cette fois, leur position et leur couleur.

Autrement dit, pour afficher une ligne par exemple, le logiciel détermine le point de départ, le point d'arrivée puis la trajectoire à suivre. Ensuite, il calcule et positionne l'ensemble des pixels nécessaires pour afficher cette ligne [27].

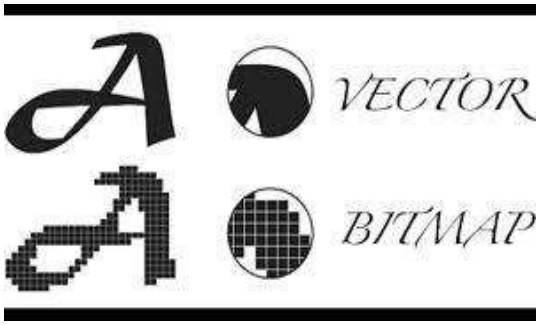


Figure 2.3 : Les images vectorielles et les images matricielles

4. Les différents formats d'images

4.1. JPEG

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 [30].

4.2. TIFF

Le format TIFF (Tagged Image File Format), Il permet de stocker des images de haute qualité en noir et blanc, couleurs RVB jusqu'à 32 bits par pixels. Il supporte aussi les images indexées faisant usage d'une palette de couleurs, les calques et les couches alpha (transparence) [29,30].

4.3. GIF

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 [9].

4.4. PNG

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 [29,30].

5. Les différents modes de couleurs des images

5.1. Mode binaire (noir et blanc)

Appelé aussi Mode bitmap, il est possible d'afficher des images en deux couleurs pour chaque pixel : noir et blanc. Par example 0 pours le noir et 1 pour le blanc.

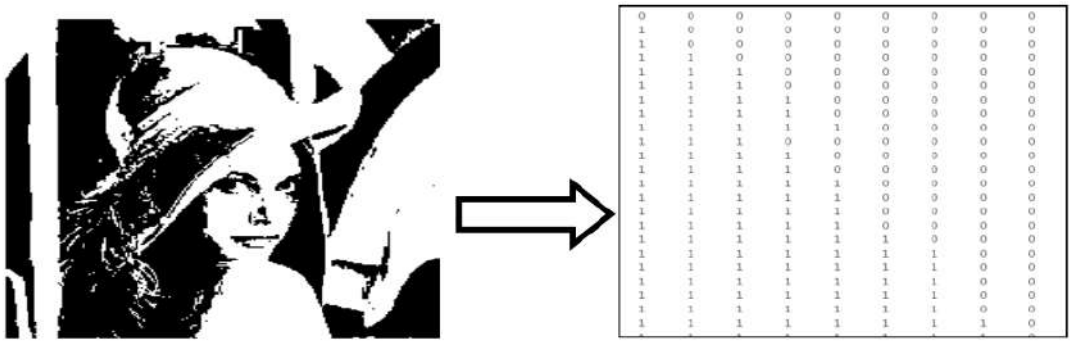


Figure 2.4 : Image noire et blanc [10].

5.2. Mode niveau de gris

Ce mode utilise en générale 8 bits, ce qui donne 256 niveaux de gris possibles pour les pixels, 0 pour le noir à 255 pour le blanc [10]. Avec n le nombre de bits pour chaque pixel. Il y aura alors 2^n niveaux de gris.

2^n=$2^8 = 256$ niveaux de gris allant du blanc au noir.

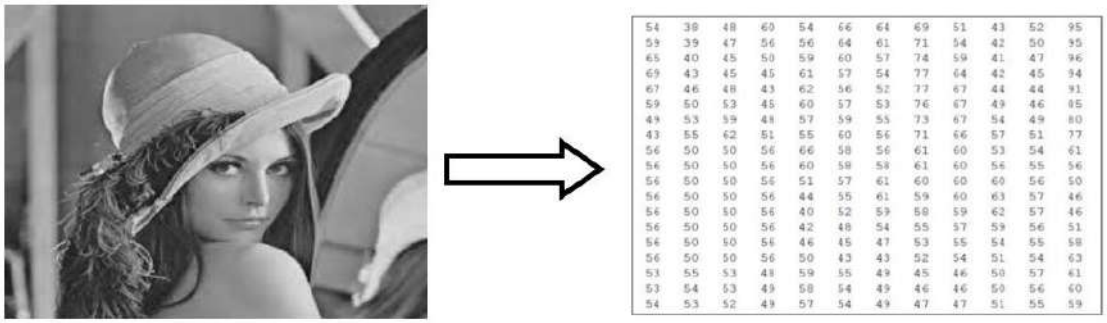


Figure 2.5: Image niveau de gris [10].

5.3. Mode couleur (RVB)

La couleur de chaque pixel est définie par 3 composantes : Rouge, Vert et Bleu (système RVB où RGB en anglais). L'intensité de chaque composante est codée sur 8 bits, donc chaque composante à une valeur comprise entre 0 et 255.

Ainsi la couleur d'un pixel nécessite 24 bits (3 octets) pour être codée.

La couleur du pixel est obtenue par synthèse additive (RVB), en particulier :

Si les 3 composantes sont à 0, on obtient du noir.

Si les 3 composantes sont identiques on obtient une nuance de gris.

Si les 3 composantes sont à 255, on obtient le blanc [10].

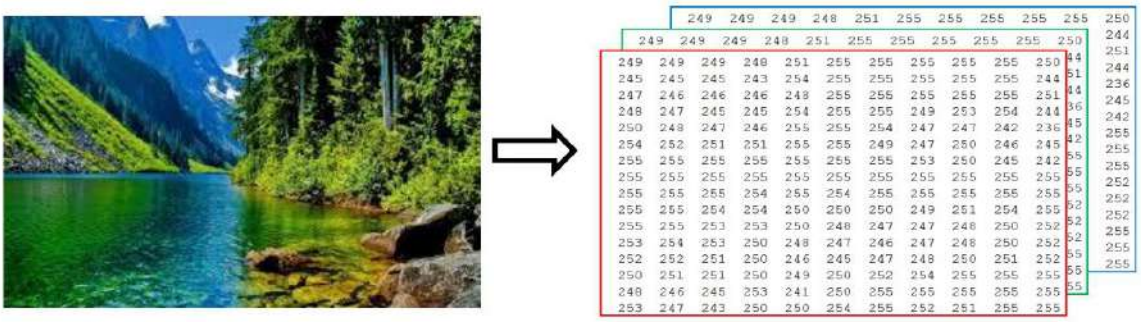


Figure 2.6 : Représentation numérique d'une image en couleur [10].

6. Conclusion

Dans ce chapitre, nous avons présenté les concepts de base sur l'imagerie numérique. Puis nous avons présenté les attributs et ces types et ces formats d'image. Enfin nous nous avons décrit ces différents modes de couleurs. Dans le chapitre suivant, nous allons présenter la méthode de cryptage d'image proposé, leur implémentation et les résultats expérimentaux.

Chapitre III :
Méthode Proposée

1. Introduction

Dans ce chapitre, nous proposons un nouvel algorithme de cryptage d'image basée sur la matrice Householder, pour éliminer la complexité de calculé l'inverse de la clé de déchiffrement, ainsi facilite la transmission de vecteur de clé secret. Aussi, nous utilisons une technique de permutation des pixels pour assurer les propriétés de la confusion et la diffusion. Enfin, nous allons présenter leur implémentation et un ensemble des tests qui montre l'efficacité et la sécurité de notre méthode proposé.

2. Méthode proposée

Le nouvel algorithme de cryptage d'image basé sur deux étapes

2.1 Fonction de chiffrement

Les étapes de la fonction de chiffrement sont décrites ci-dessous :

2.1.1 Étape 01 : génération de la clé

Pour générer la clé, nous utilisons la matrice Householder

2.1.1.1 Matrice Householder

a) - La matrice Householder H est une matrice carré, l'inverse de cette matrice H^{-1} est un méme taille de H et on appelle inversible matrice si: H H^{-1}=I.

b) - Une matrice Householder est symétrique et orthogonal: HH^t =I.

c) - La matrice Householder H est une matrice n× n de la forme suivant: H=I-2vv^t

2.1.1.2 La génération de vecteur de clé Householder

Supposons que V= $(v_{1,}v_{2,\dots,}v_{n,}) \epsilon Z_n$ est un vecteur aléatoire secret de la matrice Householder. Si $\sum_{i=1}^{n} V_i{}^2 \bmod n = 1$ (1)

2.1.1.3 La transposé de vecteur de clé Householder

L'inverse de vecteur aléatoire secret de la matrice Householder.

Si V'= $\begin{pmatrix} v_1 \\ v_2 \\ . \\ . \\ v_n \end{pmatrix}$.

2.1.1.4 Matrice identité

La matrice identité de taille n, notée I_n, la matrice carré de taille n et les coefficients sont 1 sur la diagonal et 0 ailleurs.

$$I_n = \begin{bmatrix} 1 & 0 \cdots & 0 \\ \vdots & 1 \ddots & \vdots \\ 0 & 0 \cdots & 1 \end{bmatrix}$$

Pour calculer la matrice Householder H en utilise l'équation suivant :

$$\mathbf{H=I-2\ VV'} \qquad (2)$$

2.1.2 Étape 02 : le chiffrement

Dans cet algorithme nous avons utilisés les notions suivantes :

a. A représente l'image de 256 × 256 pixels.

b. X représente la matrice de l'image A

c. n indique le nombre des lignes et des colonnes de X.

d. x (i, j) désigne l'indice de pixels dans matrice X.

e. V désigne le vecteur clé privée.

f. H est un matrice Householder.

g. V' la transposé de vecteur V.

h. D désigne l'image crypté.

Dans cette étape pour chiffré une image doit être faire un produit matricielle :

2.1.2.1 Produit matricielle

Après, pour le chiffrement nous avons utilisée X comme matrice de l'image A multiplie par la clé H comme suite :

$$D = H \times X \bmod 256 \qquad (3)$$

2.1.2.2 Principe de permutation

La permutation est une technique utiliser pour améliorer le système de cryptage par l'utilisation deux propriétés sont: la confusion et la diffusion qui permuter les pixels d'images aléatoirement pour crypter l'image qui contient une grande zone de couleur unique.

L'opération OU-exclusif (XOR): le tableau suivant montre L'opération XOR entre les valeurs :

X	Y	X⊕Y
0	0	0
0	1	1
1	0	1
1	1	0

Tableau 3.1: L'opération OU-exclusif (XOR) entre les valeurs

2.1.2.3 Ajouter le concept de confusion

Le processus de confusion faire une permutation entre les éléments de données entre eux (les pixels de l'image selon une matrice de mélange total). Dans notre algorithme, nous utilisons cette méthode pour changer les valeurs aléatoirement des pixels d'une image pour crypter, et l'inverse pour décrypter. Nous appliquons la propriété de confusion à la fonction de chiffrement, pour changer aléatoirement les valeurs des pixels de matrice D pour obtenir la matrice E comme suite :

$$E(i, j) = D(j, i), \text{ pour } i, j = 1, 2, \ldots n. \quad (4)$$

2.1.2.4 Ajouter le concept de diffusion

La diffusion permet de changer un caractère du texte clair, alors un caractère du texte chiffré devrait changer, le texte en clair est diffusé sur plusieurs caractères dans le texte chiffré. Dans notre algorithme, nous appliquons cette méthode pour changer les valeurs des pixels, nous avons appliqué l'opérateur logique XOR entre chaque octet de la matrice d'image qui contient une grande zone de couleur unique avec un caractère de la clé pour obtenir l'image crypté.

Nous utilisons la propriété de diffusion à la fonction de chiffrement, en applique l'opération XOR entre la matrice E et la clé H par l'utilisation de formule suivant:

$$Q(i, j) = \text{mod}(E(i, j) \oplus H(i, j), n) \text{ pour } i, j = 1, 2,3, \ldots n \quad (5)$$

La figure au dessous montre la méthode de diffusion :

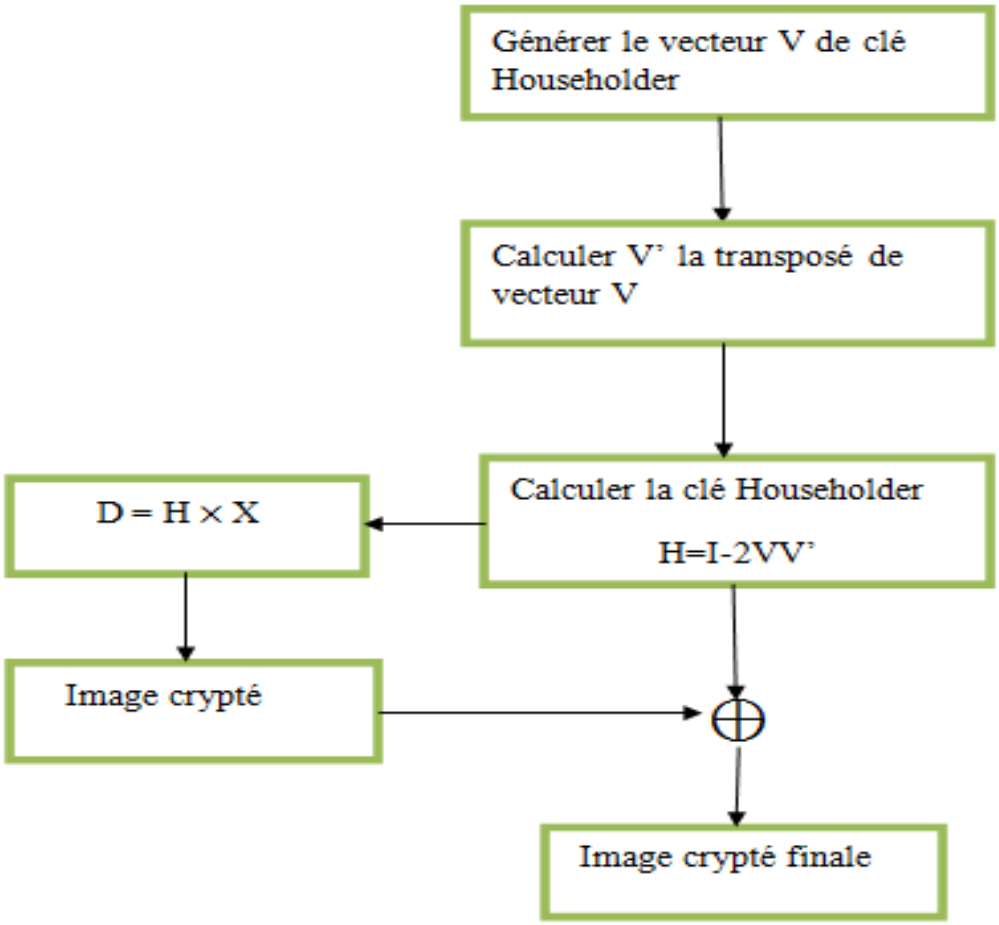
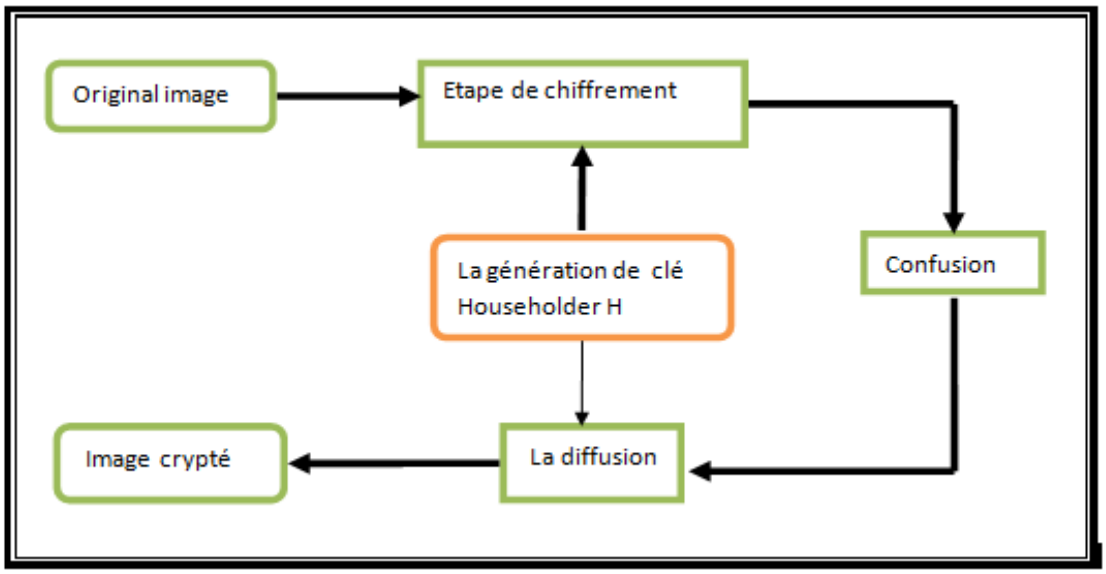


Figure 3.1: Méthode de diffusion

Le schéma au dessous montre le processus de chiffrement :



La figure 3.2 : Schéma de processus de chiffrement.

2.3 Fonction de déchiffrement

La fonction de déchiffrement est similaire à la fonction de chiffrement mais avec le fonctionnement inverse. Les étapes de cette fonction est décri ci dessous :

2.3.1 Étape 01 : Génération de la clé inverse

En utilisant le vecteur de clé Householder V pour calcule la clé H en utilisant l'équation (2).Après en calcule l'inverse de la clé Householder H^{-1}.

2.3.2 Étape 02 : L'inverse de permutation

Dans la fonction de déchiffrement, en applique le principe de permutation inverse pour récupérer les matrices E et D comme suite:

2.3.2.1 La propriété de diffusion

Dans La diffusion, en appliqué l'opérateur logique XOR entre chaque octet de la matrice d'image crypté avec un caractère de la clé Householder pour obtenir l'image claire.

En applique la propriété de diffusion à la fonction de déchiffrement pour récupérer la matrice E comme suit:

$$E(i, j) = \mathrm{mod}\,(Q(i, j) \oplus H(i, j), n) \text{ pour } i, j = 1, 2, 3, \ldots n \qquad (5)$$

2.3.2.2 La propriété de confusion

Nous appliquons la propriété de confusion à la fonction de déchiffrement, pour changer aléatoirement les valeurs des pixels de matrice E pour récupérer la matrice D comme suite :

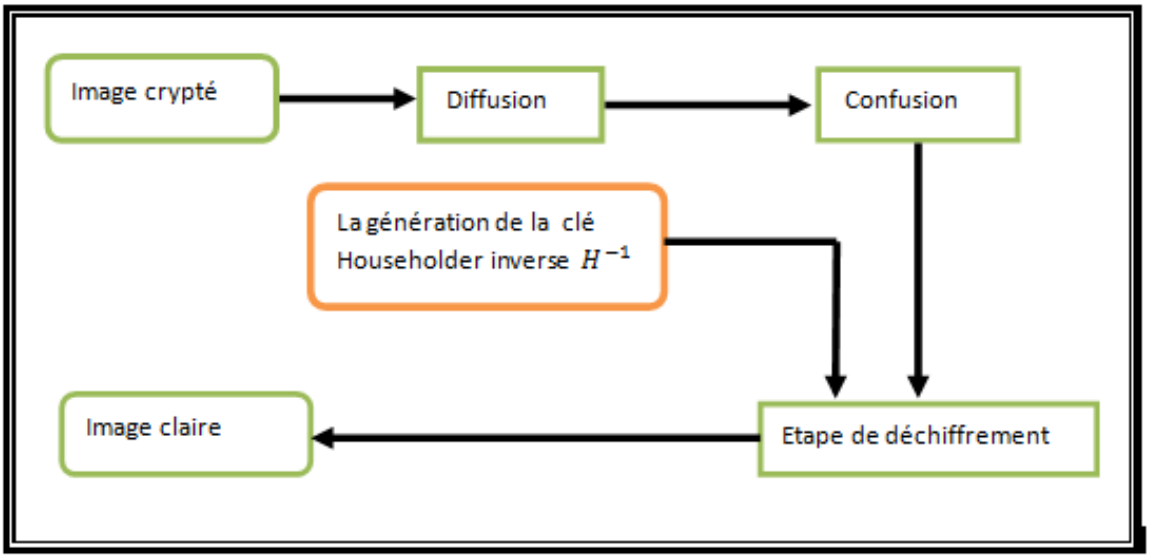
$$D(i, j) = E(j, i), \text{ pour } i, j = 1, 2, \ldots n. \qquad (6)$$

2.3.3 Étape 03 : le déchiffrement

A cette étape, pour déchiffrer l'image crypté en utilise D multiplie par la clé. Comme suit:

$$A = H^{-1} \times D \bmod 256. \qquad (7)$$

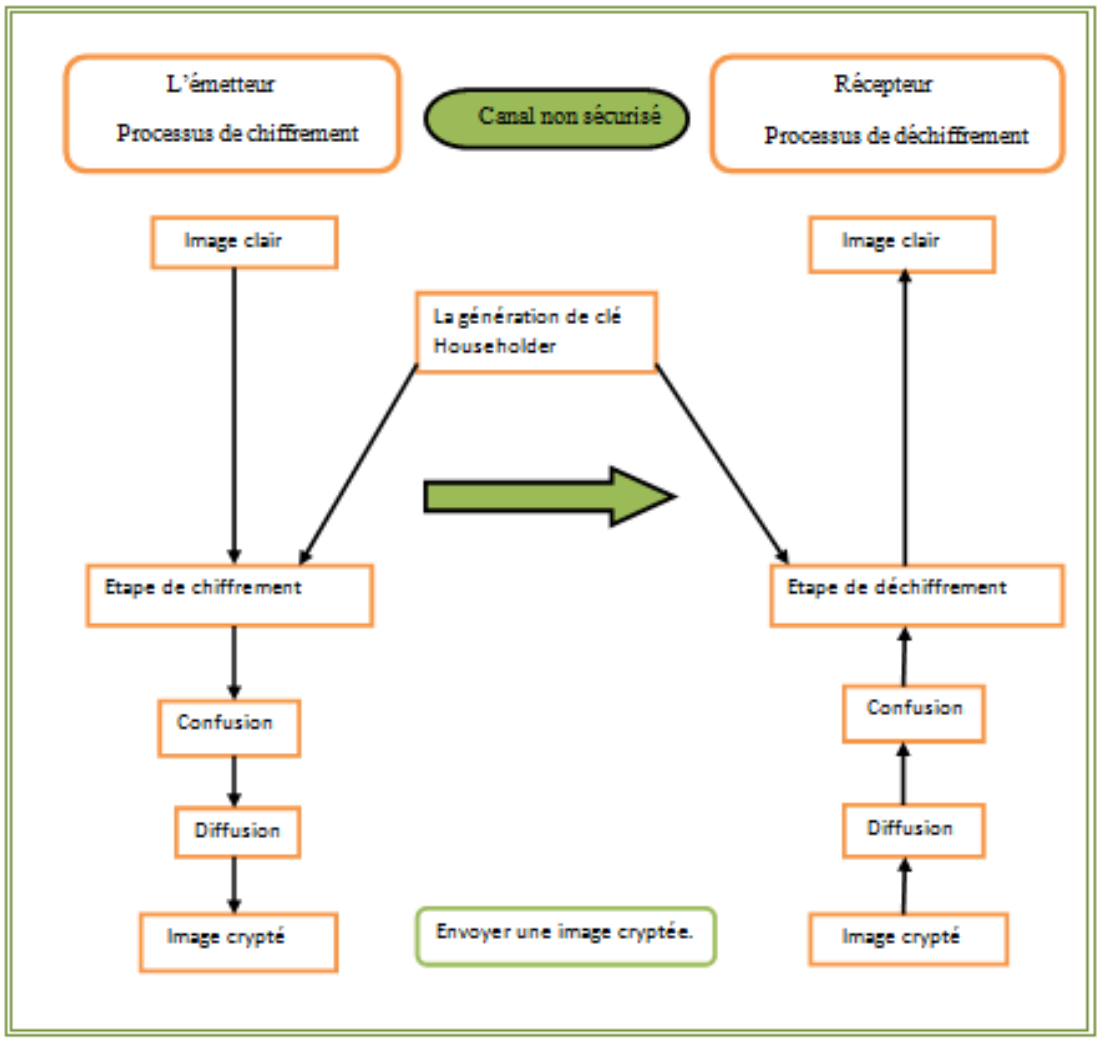
Le schéma au dessous montre le processus de déchiffrement :



La figure 3.3 : Schéma de processus de déchiffrement.

2.4 Schéma total de cryptage d'image

La figure ce dessus montre le schéma total de cryptage d'image qui comporte deux étapes (le chiffrement et le déchiffrement).



La figure 3.4: Schéma total de cryptage (chiffrement et déchiffrement).

3. Résultats expérimentaux

Avant de présenter l'application développée, nous allons présenter les outils utilisés pour l'implémentation : le matériel et le langage.

3.1 Environnement de développement

Dans cette partie nous allons citer l'environnement matériel (Hardware) et logiciel (Software) utilisés.

3.1.1 Environnement matérielle

Matériel utilisé pour le développement

L'application a été développée sur un PC ayant les caractéristiques suivantes :

- Processeur : Intel® Pentium®3558U @ 1.70GHz 1.70 GHz
- Type de système : Windows 8 Professionnel 64 bits
- RAM: 4, 00 GO.

3.1.2 Environnement logiciel

Nous avons implémenté notre application avec le langage de programmation Matlab avec la version Matlab R2016a.

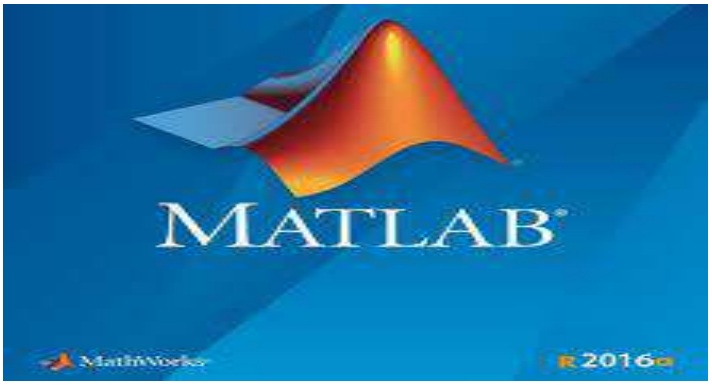


Figure 3.5: Matlab R2016a

Pour les raisons principales suivantes :

- Est un logiciel de Traitement d'image
- Développer des solutions des problèmes techniques.
- Réaliser des calculs numériques et scientifiques et tracer des graphiques.
- Analyser les données.
- Est un langage de programmation interactif.

3.2 Les interfaces du logiciel développé

Au démarrage, le système affiche l'interface de notre application présentée dans cette figure :

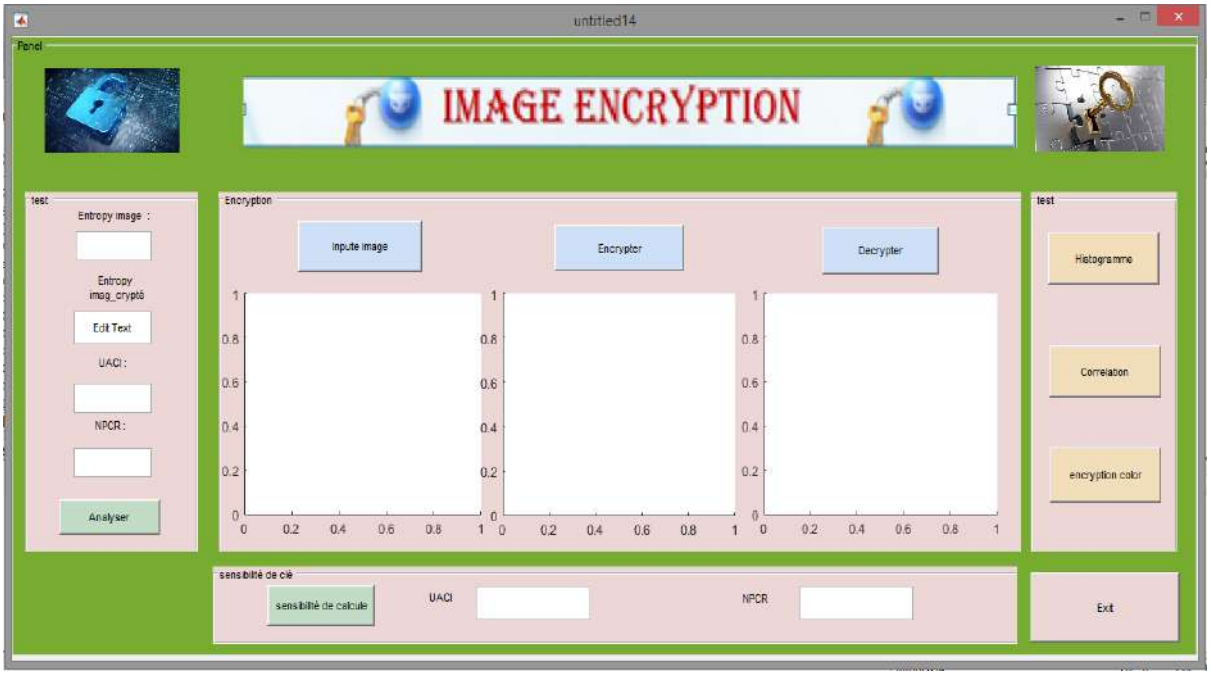


Figure 3.6: La fenêtre principale.

Cette interface contient trois panneaux qui sont constitués d'un ensemble des boutons chacun sa fonctionnalité, et des zones d'affichage:

Nous pouvons détailler ces composants comme suit : Le rôle de chaque bouton est présenté dans ce tableau :

Nom de bouton	Rôle
Input image	Pour charger l'image.
Encrypter	Pour crypter l'image clair.
Décrypter	Pour décrypter l'image clair.
Histogramme	Permet d'afficher l'histogramme de l'image clair et crypté.
Corrélation	Permet d'afficher la corrélation horizontale et verticale et diagonale de l'image clair et crypté.
Analyser	Pour afficher l'entropie de l'image clair et crypté, et affiche les valeurs de UACI (intensité unifiée moyenne évolutive) et NPCR (taux de changement de nombre de pixels).
Exit	Pour quitter l'application.

Tableau 3.2 : Les rôles des boutons de l'interface

L'interface au-dessous se montre la forme de cryptage et de décryptage de l'image clair

Figure 3.7 : Forme de Cryptage (Mode cryptage et décryptage).

L'interface au-dessous ce montre les tests statistique et différentielle de l'image clair et de crypté tel que (l'histogramme, l'entropie, UACI, NPCR).

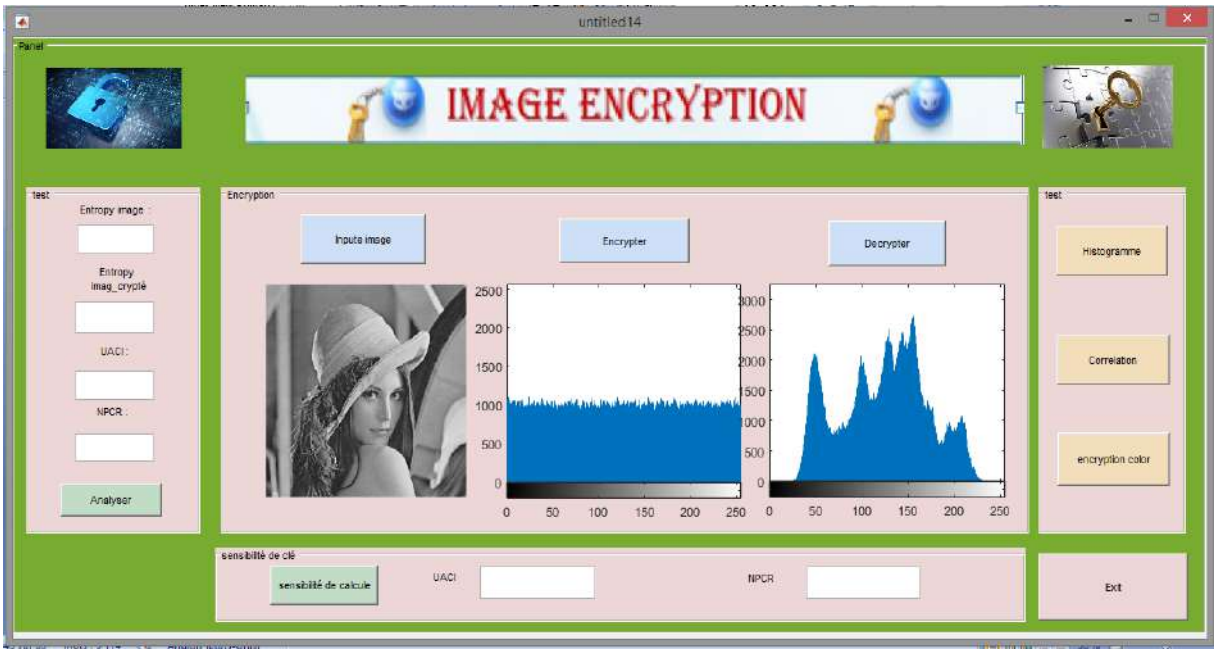


Figure 3.8: Forme d'évaluation : Tests statistique et différentielle

L'interface au-dessous montre la courbe graphique des corrélations (horizontales, verticales, diagonales) de l'image originale et crypté.

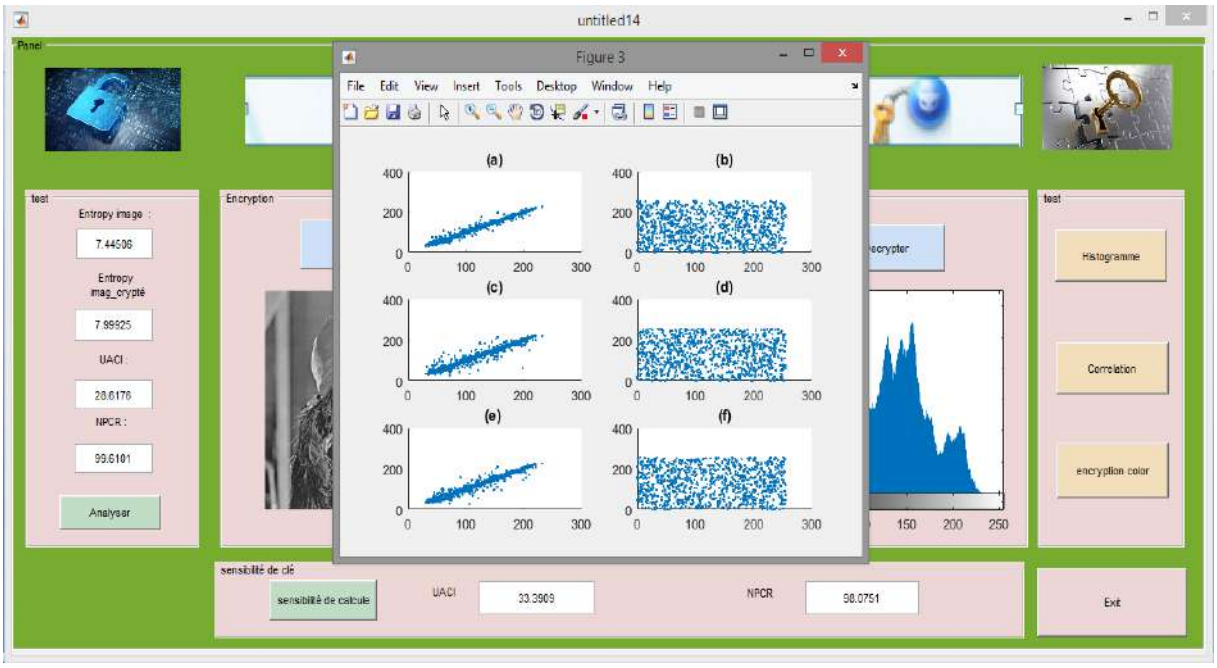


Figure 3.9 : Forme d'évaluation : Tests statistique et différentielle.

Les données utilisées dans notre mémoire, est une base de données d'images, Ils sont disponibles gratuitement sur les sites Web suivantes : University of Waterloo [20], Et le dernier University of Wisconsin-Madison [21]. Ces images sont conçues pour le traitement et d'analyse d'un cryptage d'images numériques.

Afin d'étudier le comportement de notre algorithme de cryptage, nous avons appliqué sur différents type d'images (binaire, niveau de gris, médicale, Image contienne grande zone de couleur unique). La section suivante présente quelques exemples :

3.3 Images binaires

Nous avons appliqué l'algorithme de chiffrement sur une image binaire avec une clé de chiffrement .Aprés en obtenu une image crypté dans la figure 3.10.

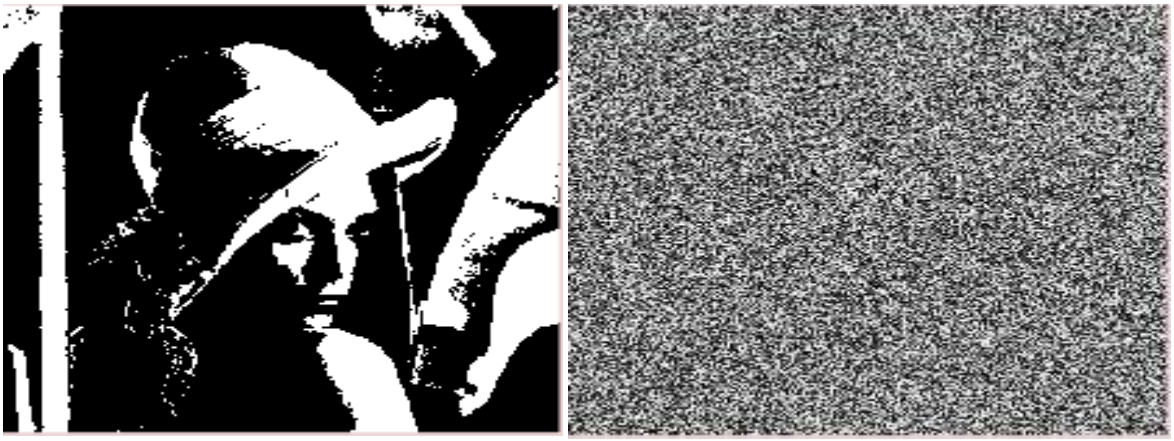


Figure 3.10: le résultat de cryptage d'image binaire.

3.4 Image au niveau de gris

Les figures au-dessous montrent plusieurs images au niveau de gris de différentes tailles sont cryptées en utilisant l'algorithme proposé.

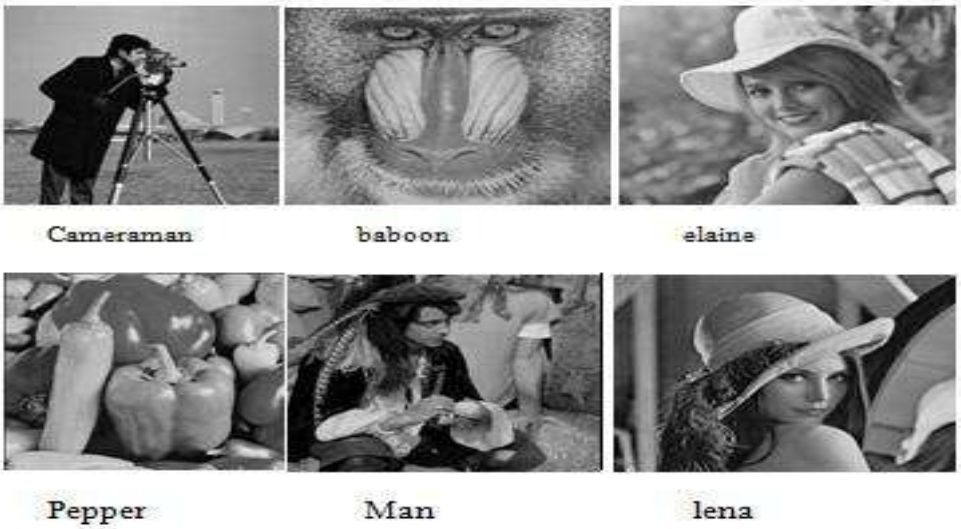


Figure 3.11 : Les images claires.

Les figures au-dessous montrent plusieurs images au niveau de gris de différentes tailles sont cryptées.

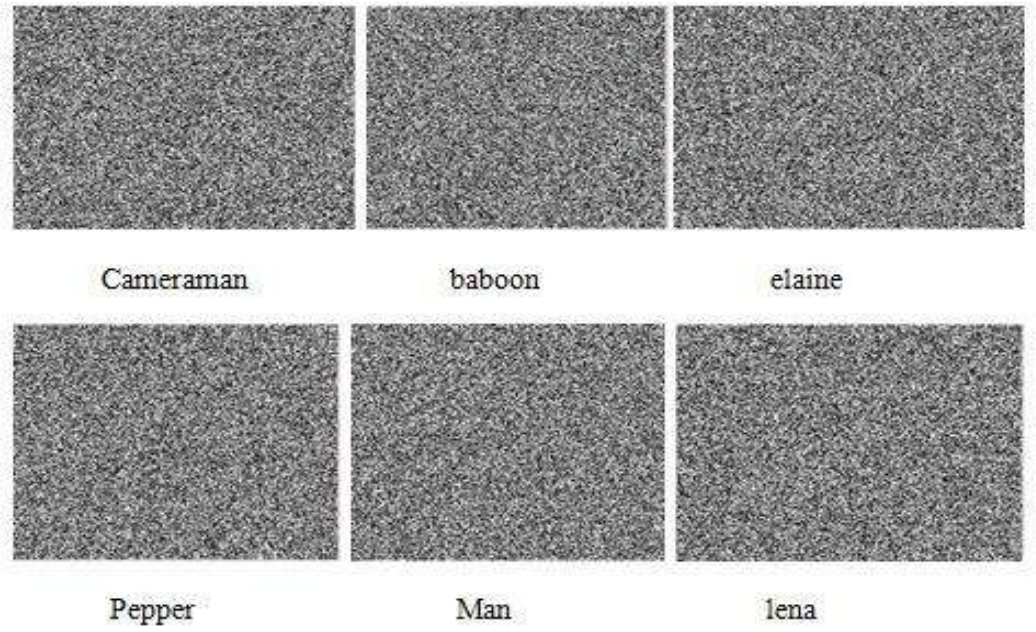


Figure 3.12 : Les images cryptées.

Les figures au-dessous montrent plusieurs images au niveau de gris de différentes tailles sont décryptées.

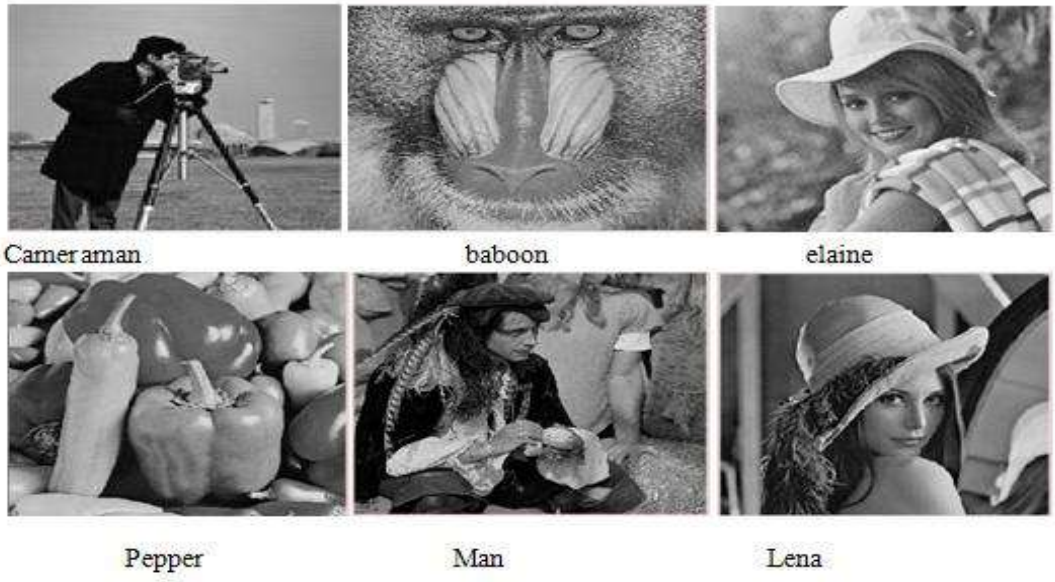


Figure 3.13 : Les images décryptées.

3.5 Image médicale

Les dossiers médicaux ont été envoyés sur les réseaux d'internet. Alors les images médicales doivent être cryptées avant d'être envoyées sur ces réseaux. Donc Les figures au-dessous montre plusieurs images médicales sont cryptées. Aprés, en décrypter en utilisant l'algorithme proposée.

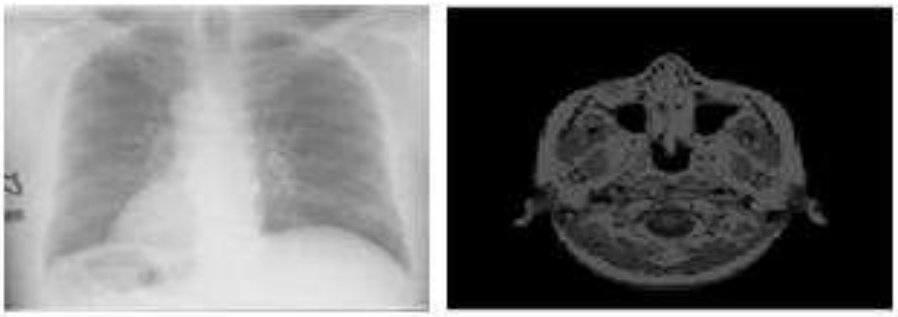


Figure 3.14 : Les images médicales clairs.

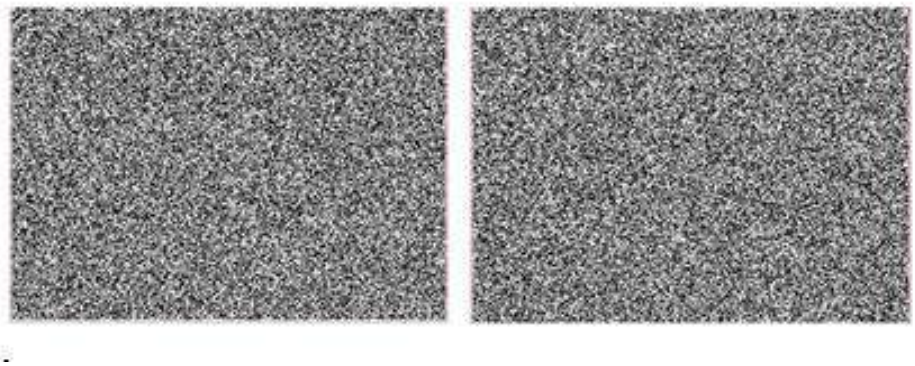


Figure 3.15 : Les images médicales cryptées.

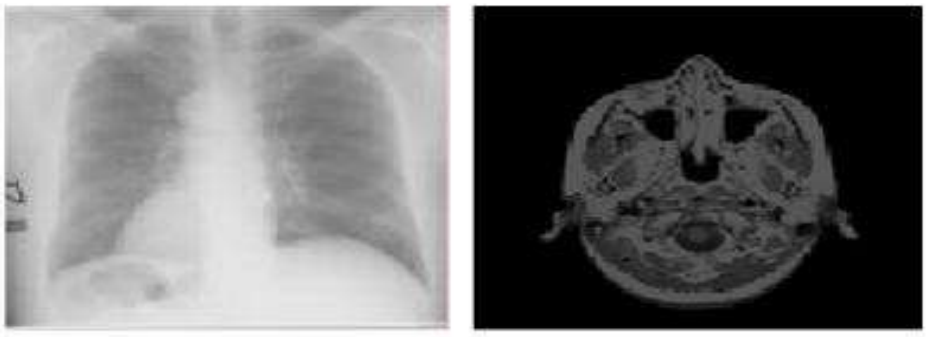


Figure 3.16 : Les images médicales décryptées.

3.6 Image contienne grande zone de couleur unique

Les figures au-dessous montrent deux images contienne grande zone de couleur unique sont cryptées. Aprés, en décryptées en utilisant l'algorithme proposée.

Figure 3.17 : Les images contienne grande zone de couleurs uniques claires.

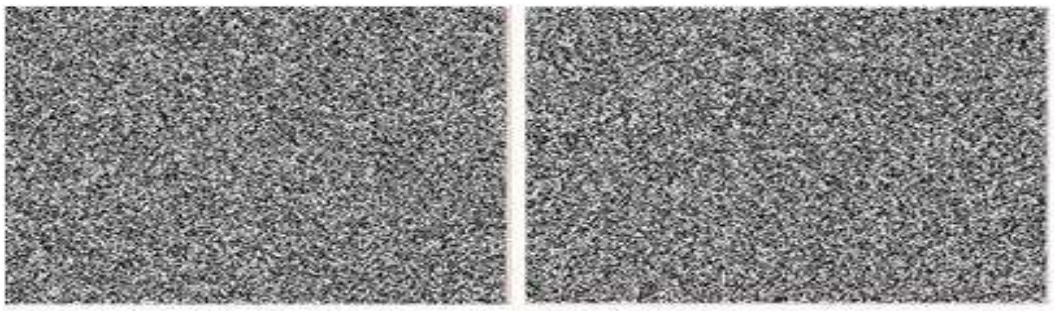


Figure 3.18 : Les images contienne grande zone de couleurs uniques cryptés.

Figure 3.19 : Les images contienne grande zone de couleurs uniques Décryptés.

4. Critères d'évaluation

Un bon système de cryptage devrait résister des attaques connu, Donc en utilisant différentes mesures d'évaluation pour montrer la sécurité et l'efficacité de l'algorithme proposé. Nous allons présenter les plus important comme : tests statistique tel que (l'histogramme, la corrélation, l'entropie) et les tests différentielle tel que (UACI, NPCR), l'espace de clés, la sensibilité de la clé.

4.1 Les tests statistiques

En utilisant différentes tests pour l'image et l'image crypté tell que : l'histogramme, la corrélation, l'entropie.

4.1.1 L'histogramme

L'histogramme est une représentation graphique qui permet de connaître la répartition des intensités lumineuses des pixels [25].

Quatre images de tests ont été utilisées dans l'analyse : Les tracés des histogrammes des images et les images cryptées sont montrés dans les figures au-dessous

Figure 3.20 : Les images clairs.

Histogramme de l'image lena binaire

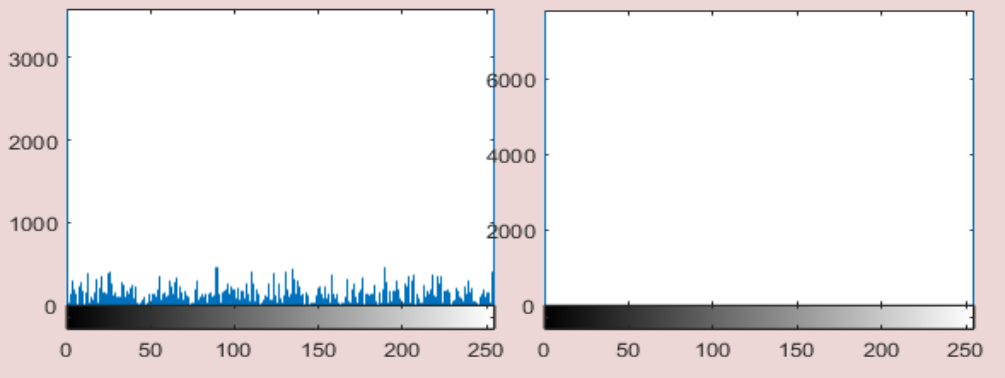


Figure 3.21 : Histogramme de l'image et l'image cryptée

Histogramme de l'image Pepper:

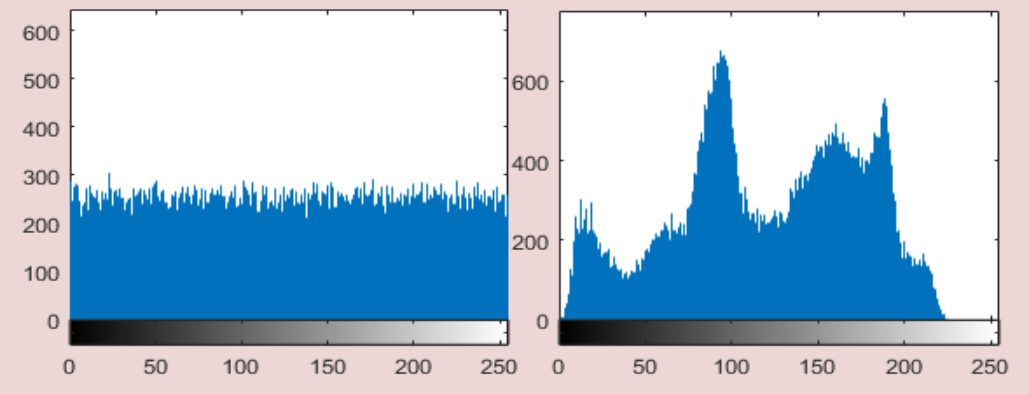


Figure 3.22 : Histogramme de l'image et l'image cryptée.

Histogramme de l'image medical:

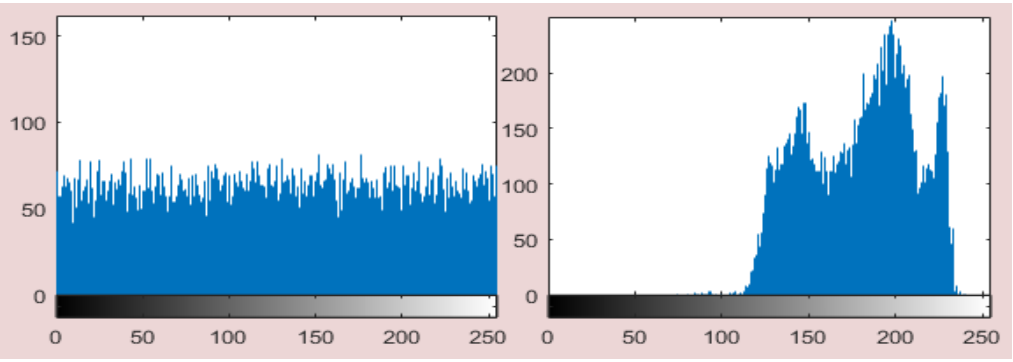


Figure 3.23 : Histogramme de l'image et l'image cryptée.

Histogramme de l'image Nike:

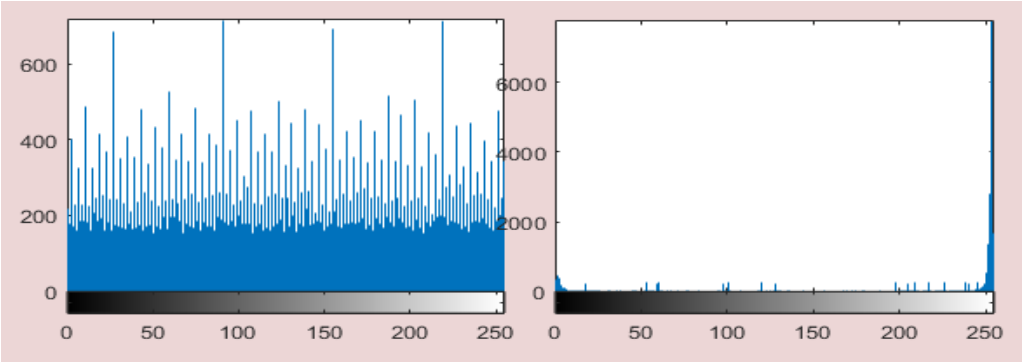


Figure 3.24 : Histogramme de l'image et l'image cryptée.

Les résultats montrent que les histogrammes des images cryptées sont uniformes par rapport les histogrammes des images clair sont non uniformes. Par conséquent l'attaquant ne peut pas extraire l'information à partir de l'histogramme de l'image cryptée.

4.1.2 La corrélation

Les pixels adjacents dans une image claire sont fortement corrélés, mais dans une image cryptée par un algorithme de cryptage optimal, ces derniers deviennent faiblement corrélés. Le calcul du coefficient de corrélation entre les pixels adjacents nous donne une idée sur la capacité de notre algorithme de cryptage à résister aux attaques. Le coefficient de corrélation est défini par la formule suivante [26] :

$$r_{xy} = cov(x,y)/(\sqrt{D(X)D(Y)}) \quad (3.1)$$

Ou $$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (3.2)$$

Et $$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i) \quad (3.3)$$

Et $$cov(x, y) = \frac{1}{N} = \sum_{i=1}^{N}((x_i - E(x)(y_i - E(y))) \quad (3.4)$$

Tel que :

r : la corrélation.

cov : la covariance.

E : l'espérance mathématique.

D : la variance.

x, y : les valeurs des pixels des images.

Pour étudier la corrélation, en utilise l'algorithme de cryptage proposé pour crypter l'image de lena. Ensuit nous calculons les coefficients de corrélation dans les trois directions (verticale, horizontale et diagonale) entre l'image et l'image cryptée. La figure au-dessus montre les courbes des corrélations entre les deux images.

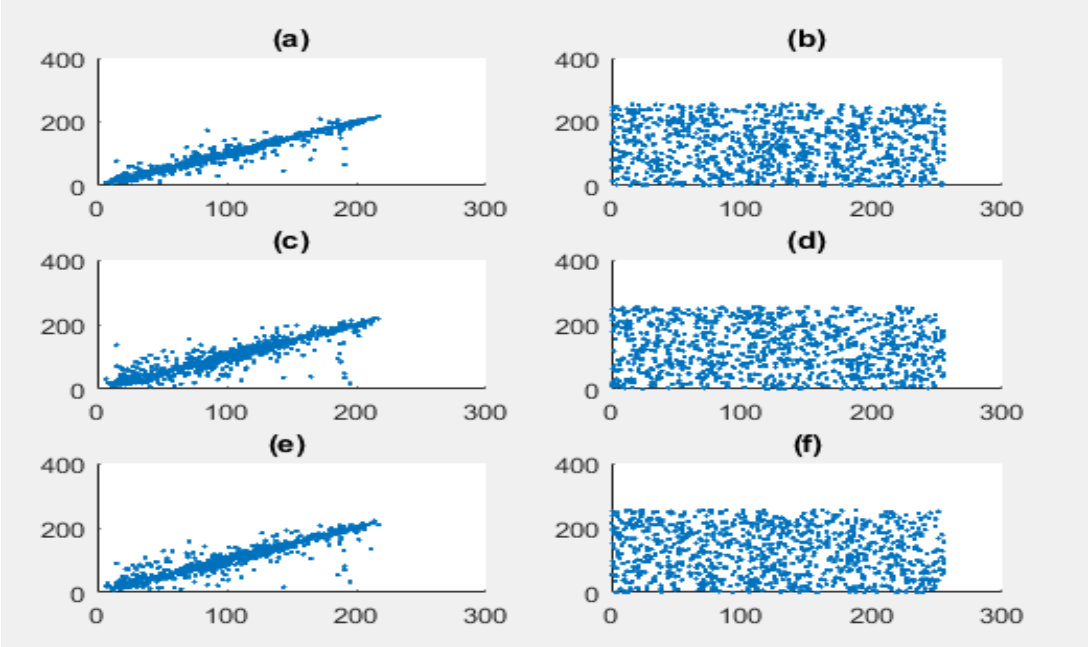


Figure 3.25 : (a, c, e) les corrélations horizontale, vertical et diagonal des pixels de l'image origine. (b, d, f) les corrélations horizontale, vertical et diagonal des pixels de l'image crypté.

Les résultats de calcul dans le tableau au dessous montrent que la corrélation de l'image chiffré est très faible dans les trois niveaux (diagonal, horizontal, vertical) par rapport la correlation de l'image claire.

Corrélation	**Image claire**	**Image chiffré**
Diagonal	0.9178	-6.8972e-04
Horizontal	0.9693	0.0028
Vertical	0.9399	-0.0024

Tableau 3. 3: Coefficients de corrélation entre l'image originale et l'image chiffrée.

4.1.3 L'entropie

L'entropie indique le niveau d'incertitude dans système de communication. L'entropie H (x) de toute donnée peut être calculée comme [26]:

$$H(m) = \sum_{i=0}^{2^n-1} p(m)_i \log_2 \frac{1}{p(m_i)} \qquad (3.5)$$

La valeur de l'entropie doit être très proche de 8, Parce que si l'entropie est inférieure à 8, il existe des degrés de prévisibilité, Pour l'image cryptée avec 256 symboles, donc on ne peut pas assurer la sécurité contre l'attaque par entropie.

Le tableau au-dessous se montre la liste des valeurs de l'entropie des images claires et leurs chiffrées en utilisant le schéma proposé.

Nom de l'image	Description de l'image	Taille	Type	Entropie de l'image en claire	Entropie de l'image chiffré
Pepper.tif	Pepper	256×256	Niveau de gris	7.59306	7.9979
Lena.tif	Lena	256×256	Niveau de gris	7.56943	7.9973
4. tif	Cameraman	128×128	Niveau de gris	7.1267	7.9862
elaine512.tif	elaine	512×512	Niveau de gris	7.5060	7.9993

Tableau 3.4: Les valeurs de l'entropie des images claires et des images cryptées.

Les résultats de tableau montre que les valeurs de l'entropie des images chiffrée est plus proche à la valeur 8. Cela montre qu'il est difficile d'avoir la prévisibilité d'information.

4.2 Les tests différentiels

Pour tester l'influence d'un changement d'un pixel sur l'image entière chiffré par n'importe quel algorithme de cryptage, deux paramètres communs peuvent être utilisé: NPCR et UACI. Laissez les deux images chiffrées, dont les images simples correspondantes n'ont qu'une différence de pixel, soit notée par C1 et C2.Label les valeurs de niveaux de gris des pixels à la grille (i, j) en C1 et C2 par C1 (i, j) et C2 (i, j), respectivement. Définissez une matrice binaire D avec la même taille que les images C1 et C2. Ensuite, D (i, j) est déterminé par C1 (i, j) et C2 (i, j). Si C1 (I, j) = C2 (i, j), alors D (i, j) = 0;Sinon, D (i, j) = 1.

4.2.1 NPCR

NPCR (taux de changement de nombre de pixels) entre deux images de même taille sont définies comme suit [26]:

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100 \qquad (3.6)$$

Le NPCR mesure le pourcentage de pixels différents dans les deux images.

Le tableau ci-dessous ce montre la liste des valeurs de NPCR de entre deux images claire et chiffrées en utilisant le schéma proposé.

Nom de l'image	Description de l'image	Taille	Type	La valeur de NPCR
Pepper.tif	Pepper	256×256	Niveau de gris	99.6185
lena.tif	lena	256×256	Niveau de gris	99.6063
medicale.tif	medicale	128×128	médicale	99.5789
nike.tif	nike	256× 256	Image contienne grande zone de couleur	99.5911

Tableau 3.5: Les valeurs de NPCR entre deux images claires et chiffrées.

4.2.2 UACI

UACI (intensité unifiée moyenne évolutive) entre deux images de même taille est définie comme suit [26]:

$$\text{UACI} = \frac{1}{M \times N}\left[\sum_{i,j} \frac{C1(i,j) - C2(i,j)}{255}\right] \times 100\% \qquad (3.7)$$

Le tableau ci-dessous se montre la liste des valeurs UACI entre deux images (claire et chiffrées) en utilisant le schéma proposé.

Nom de l'image	Description de l'image	Taille	Type	La valeur d'UACI
Pepper.tif	Pepper	256×256	Niveau de gris	29.5984
lena.tif	lena	256×256	Niveau de gris	30.5483
medicale.tif	medicale	128×128	médicale	30.6128
nike.tif	nike	256×256	Image contienne grande zone de couleur	47.6642

Tableau 3.6: Les valeurs d'UACI entre deux images (claires et chiffrées).

Les résultats des tableaux ces montres que les valeurs de NPCR et UACI sont élevées, alors le cryptage d'image sera élevé.

4.3 Espace de clés

Pour empêcher certaines attaques comme force brute, l'espace de clé devrait être grand. Donc, le système de cryptage est sécurisé si son espace de clé est assez grand. Dans notre algorithme, l'espace clé K peut être égal à $K = 2^{256}$ octets, c'est très grand, car un attaquant doit essayer toutes les clés possibles [23]. Donc notre modèle est libre de l'attaque par force brute.

4.4 La sensibilité de la clé

La sensibilité à la clef secrète est une caractéristique essentielle pour un bon cryptage qui garantit la sécurité de ce dernier contre touts les attaque exhaustive [31]. Cela signifie qu'un changement d'un seul bit de la clé secrète devrait produire une image cryptée complètement différente. Et le mesure d'UACI et NPCR sont changées.

Le tableau ci-dessous se montre la liste de sensibilité de la clé (les valeurs UACI et NPCR) entre deux images (claire et chiffrées) en utilisant le schéma proposé.

Nom de l'image	Taille	Type	La valeur d'UACI	La valeur d'NPCR
Pepper.tif	256×256	Niveau de gris	32.9282	97.4701
lena.tif	256×256	Niveau de gris	33.1478	98.2208
medicale.tif	128×128	médicale	33.713	99.3225
nike.tif	256×256	Image contienne grande zone de couleur	33.5354	99.3134

Tableau 3.7: Les valeurs de sensibilité de la clé (UACI et NPCR) entre deux images (claires et chiffrées).

4.5 Cryptanalyse

Le processus de cryptage est efficace s'il est libre de la vulnérabilité cryptanalyse, où la cryptanalyse est une science de la récupération de l'image originale sans accès à la clé privée (appelée code cracking ou code-break). Les analyses qui sont utilisées pour démontrer la faiblesse de certaines attaques célèbres dans le cryptage des images tel que attaque en texte clair connu/choisi dans ces attaques, l'attaquant a une connaissance préalable du processus de cryptage ainsi que le processus de cryptage est efficacement libre pour une paire d'images originale et cryptée.

L'objectif est de trouver la clé privée, supposons que l'attaquant tente de déchiffrer une image cryptée en utilisant l'algorithme proposé par choisir au hasard une clé, et compare l'image décryptée obtenue à l'image d'origine. La probabilité de trouver la bonne clé serait environ 1/K où K est l'espace de clé, cette probabilité est très faible pour trouver la bonne clé. Une autre technique permettait à l'attaquant de décomposer le cryptage d'image est l'utilisation d'images particulières (ex: image de bloc zéro) pour obtenir des informations utiles sur l'image secrète. Les figures (fig.3.17 et fig.3.18 a démontré l'efficacité de notre modèle où cryptage de toutes les images de bloc zéro est totalement une image déférente).

5. Etude comparative

Dans cette étude, nous avons comparé notre algorithme proposé avec les autres techniques de cryptage d'image. On commence par la première comparaison, c'est l'algorithme proposé avec d'autres des algorithmes de cryptage d'image.

Le tableau ci-dessous liste : la comparaison entre l'algorithme proposé et les autres algorithmes de cryptage, Et aussi la corrélation (horizontal, vertical, diagonal) a été utilisée pour cette comparaison.

	Plainimage	HC	HCM-PT	HillMRIV	MHBCM	Algorithme proposé
Horizontal	0.9863	0.0186	0.0155	0.0517	0.0429	0.0028
Vertical	0.9319	0.0303	0.0248	0.0335	0.0022	-0.0024
Diagonal	0.9089	0.0173	0.0232	0.0006	0.0004	-6.8972e-04

Tableau 3.8 : la comparaison externe de corrélation entre les algorithmes

Les résultats de tableau montre que les mesurés de coefficients de corrélation de l'image chiffrée sont proches de 0. Cela indique que l'algorithme proposé supprimé avec succès la corrélation des pixels adjacent que les autres des algorihmes.

Le tableau suivant se montre le test de sensibilité de clé à l'aide des différents schemas:

HC	HC-PMT	HillMRIV	MHBC	Algorithme proposé
0.7797	0.1953	0.1953	99.68	99.91

Tableau 3.9: la comparaison de sensibilité de clé entre l'algorithme proposé et des autres algorithms.

Il y a 99, 61% de déférence entre les deux image cryptées selon le schéma proposé. Seuls le schéma proposé et le MHBCM sont résistants aux tests de sensibilité des clés.

La figure ci- dessous se montre les valeurs de NPCR et UACI de l'algorithme proposé et les autres algorithms.

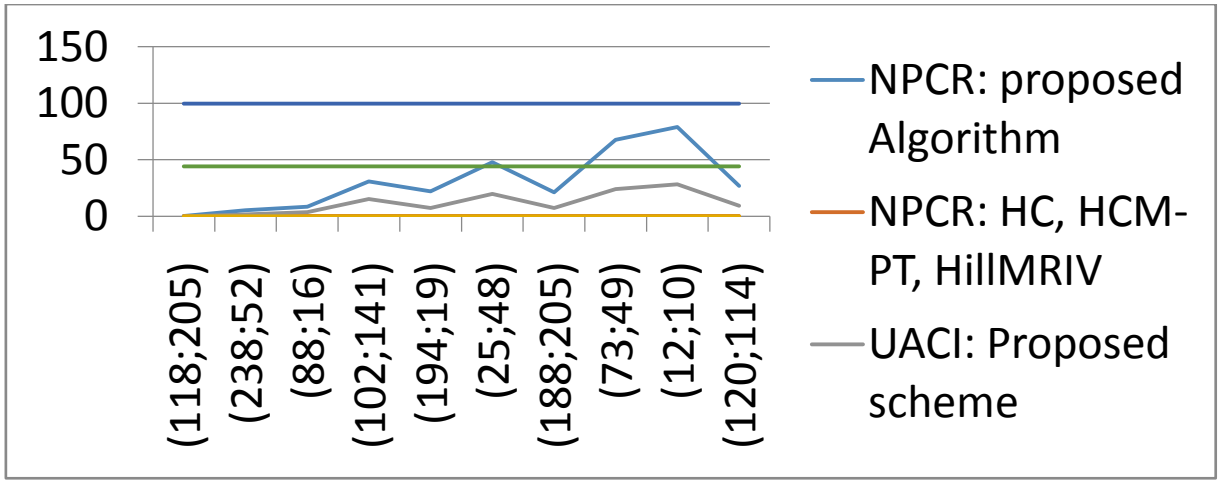


Figure 3.26: Comparison entre les valeurs de NPCR et UACI de l'algorithme proposé et les autres algorithms.

La simulation montre que NPCR et UACI du schéma proposé sont les meilleurs. Le schéma proposé resister aux attaques différentielles.

6. Conclusion

Dans ce chapitre, nous allons proposer un nouvel algorithme de cryptage d'image basée sur la matrice Householder, pour éliminer la complexité de calcule l'inverse de la clé lors du déchiffrement, ainsi, facilite la transmission de cette clé. Et une technique de permutation des pixels pour assurer les propriétés de confusion et diffusion. Et son implémentation. Aprés, nous terminons par un ensemble des tests qui résister les attaques de texte claire connu et choisi pour valider l'efficacité de cette méthode. Et qui permet un temps d'exécution des quelques millisecondes.

Conclusion Générale

Conclusion Générale

Aujourd'hui, le monde connu un grand développement dans le domaine de réseaux de communication. Donc, la plupart des recherches se concentrent sur l'amélioration des méthodes de la cryptographie pour augmenter le taux de sécurité et de confidentialité des données. L'algorithme proposé basée sur la matrice Householder, pour éliminer la complexité de calcul l'inverse de clé du déchiffrement, ainsi, facilite la transmission de cette clé. Et une technique de permutation des pixels pour assurer les propriétés de confusion et diffusion. Les résultats expérimentaux montrent clairement que l'analyse d'histogramme des images cryptées sont uniformément distribuées, donc l'algorithme est sécurisé devant les attaques d'analyse de fréquence. Et ainsi l'espace clé est suffisamment grand, ce qui rend une attaque force brute infaisable. Par conséquent l'histogramme d'image chiffrée est très uniforme après le cryptage, voire, l'attaquant il ne peut pas extraire l'information à partir de l'histogramme de l'image cryptée. Également l'algorithme proposé a été atteintes beaucoup amélioré sur l'entropie et la corrélation entre les pixels adjacents.

Les deux mesures ont été utilisées : NPCR et UACI pour montrer un changement entre l'image crypté et l'image d'origine. Il y a un cryptage efficace pour chiffrer les images. De ce fait l'algorithme proposé montre l'efficacité et la sécurité de notre système proposé. Peut aussi être facilement résisté les attaques en texte clair connues/choisies. Finalement les comparaisons avec les schémas de chiffrement d'image existants qui ont été réalisées, montrent que l'algorithme proposé offre des performances très favorables.

Comme perspective à ce travail, nous allons améliorer notre approche sur tous les formats des images médicales en général et les images couleur entre eux en particulier.

Référence

Référence:

[1] LESCOP Yves [V1.6], La sécurité informatique, Post BTS R2i, 2002, http://ylescop.free.fr/mrim/cours/securite.pdf, consulté le 18-05-2019.

[2] Mme L.SAOUDI, initiation à la cryptographie, support de cours du module Sécurité informatique, Département d'informatique, université de Msila, Année 2015/2016.

[3] R. Dumont, Cryptographie et Sécurité informatique, Notes de cours provisoires, Université de Liège, 2009 – 2010.

[4] A. bayad. Introduction à la cryptographie. Université d'evry val d'essonne, 2008.

Https://www.maths.univ-evry.fr/.

[5] Principe de base de la cryptographie http://dspace.univ telmcen.dz/ bitstream /112 /1046 /8/chapitre2.pdf.

[6] DR. Abdelhabib BOUROUIS, cour : « Sécurité informatique », Université LARBI BEN M'HIDI, OUM EL BOUAGHI, Année 2014/2015, 19p.

[7] Nabil LITAYEM : « Contributions méthodologiques à la conception et optimisation de systèmes embarqués », thèse de doctorat, Université De Carthage, Juillet 2014.

[8] Pierre-Louis Cayrel. Chiffrement par blocs. Université de Limoges, 2015.

https://www.cayrel.net/.

[9] Les formats d'images numériques, Serge WACKER – C2I niveau 1, http://www.montpellier.iufm.fr/technoprimaire, consulté le: 02/06/2019.

[10] Belkadi Imane, Amiar Narimen : « Cryptage d'image par considération des plans de bits des pixels séparément par ordre de leurs poids avec une clé publique de taille libre », Mémoire de Master en informatique vision artificielle, Université LARBI BEN M'HIDI, OUM EL BOUAGHI, Année 2017-2018.

[11] G. Labouret. Introduction à la cryptographie. HSC - Herve Schauer Consultants - Cabinet de consultants en sécurité informatique 2001, Http://www.hsc.fr/.

[12] Rafael C Gonzalez and Richard E Woods. Digital image processing 3rd edition 2007

[13] Numeriksciences, http://numeriksciences.fr, consulté le 18-02-2019.

[14] Les systèmes à clé publiques. CCM - Comment ça marche - Communauté informatique, http://www.commentcamarche.net/contents/201-les-systemes-a-cle-publiques/.

[15] Merdjal choumaissa, Merakchi Ahlam : « Cryptage d'image par un signal unidimensionnel quelconque », Mémoire de Master informatique vision artificielle, Université LARBI BEN M'HIDI, OUM EL BOUAGHI, Année 2018.

[16] HADJI Faiçal : « Conception et réalisation d'un système de cryptage pour les images médicales », Mémoire de Master informatique Académique, Université MOHAMED BOUDIAF, M'SILA, Année universitaire 2017 /2018.

[17]T. Hamaizia, Systèmes Dynamiques et Chaos "Application à l'optimisation a l'aide d'algorithme chaotique", These pour obtenir le titre de Docteur en Sciences de l'Université de Constantine 1, 2013.

[18] Wikipédia, https://fr.wikipedia.org/wiki/Entropie_de_Shannon, consulté le 16-04-2019.

[19] Wikipédia, https://fr.wikipedia.org/wiki/Leonardo_Fibonacci, consulté le 26-03-2019.

[20] University of Southern California, Base de données d'images, http://sipi.usc.edu/database/database.php?volume=misc, consulté le 15-03-2019.

[21] University of Waterloo, Base de données d'images, http://links.uwaterloo.ca/Repository.html, consulté le 15-05-2019.

[22] Avi Dixit, Dahale Bhagwan, Pratik Dhruve, IMAGE ENCRYPTION USING PERMUTATION AND ROTATIONAL XOR TECHNIQUE, SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, pp. 01–09, 2012.

[23] Jean De Dieu Nkapkop, Joseph Effa, Monica Borda, Laurent Bitjoka, and Mohamadou Alidou, Chaotic Encryption Scheme Based on A Fast Permutation and Diffusion Structure, University of Ngaoundéré, Cameroon, 1,8 pp, October 7, 2015.

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

[25] Utiliser l'histogramme. PhotoFiltre Studio, http://www.photofiltrestudio.com/doc/histogramme.htm.

[26] A. Beloucif, Contribution à l'étude des mécanismes cryptographiques, thése En vue de l'obtention du diplôme de Doctorat en Informatique, Université de Batna2, 2016.

[27] O. Poutarédy. Différences entre image Bitmap et image vectorielle. Site des enseignants en Arts Appliqués de l'académie d'Orléans-Tours, 2015

[28] Image file formats. Wikipedia, Https://en.wikipedia.org/wiki/Image_file_formats.

[29] R. Isdant. Traitement numérique de l'image.2009

[30] Image file formats. Wikipedia, Https://en.wikipedia.org/wiki/Image_file_formats.

[31] Cryptage complet/partiel d'une image/vidéo par un signal sinusoïdal, Présenté par Ounzar Asma, Université Larbi Ben M'hidi Oum El Bouaghi, Soutenue 2014-2015.

[32]S. BELKACEM, Chaos based image watermarking, These Présentée pour l'obtention du diplôme de DOCTORAT en Science en Electronique, université de Batna 2.