# le cryptage d'images médicales

## Introduction

Les chercheurs de cryptographie ont été proposés plusieurs techniques de chiffrement d'images médicales. Parmi eux il y a des algorithmes qui basés sur les théories comme la théorie de chaos, la permutation, et aussi des algorithmes qui basés sur différentes technologies comme : le séquençage de l'ADN et beaucoup d'autres techniques.

Dans ce chapitre nous allons présenter les différentes techniques de chiffrement d'images médicales et leurs résultats.

## Les travaux de cryptage d'images médicales

### Transfert sécurisé d'images médicales par codage conjoint : cryptage sélectif par AES en mode par flot OFB et compres- sion JPEG (2006)

William Puech, José Marconi Rodrigues et Jean-Eric Develay-Morice proposé une nouvelle méthode de cryptage sélectif (CS) pour des images médicales comprimées avec JPEG. Cette méthode est basée sur l'algorithme AES (Advanced Encryptions Standard) en utilisant le mode de chiffrement par flot OFB (Output Feedback Block) dans l'étape du codage de Huffman de l'algorithme JPEG.
Cette méthode par cryptage sélectif protège les parties les plus importantes des images tout en minimisant le temps de calcul pour des applications temps réel[44].

**Principe :**

L'idée principale de la méthode proposée est illustrée figure4 et résumée ci-dessous : 1.Prendre les coefficients AC non nuls du flux binaire de Huffman, des plus hautes fréquences vers les basses fréquences afin de construire le vecteur du message en clair Xi.

Ces coefficients AC obtenue à partir l'application de la méthode de transformée cosinus discret (DCT) qui transforme les blocs d'une image du domaine spatial a domaine fréquentiel.

2. Coder Xi avec l'algorithme AES en mode OFB.
3. Substituer le flux binaire de Huffman par l'information cryptée qui est de même taille.

**Résultats de cette méthode**

—Les méthodes ont été appliquées sur plusieurs dizaines d'images médicales en niveau de gris.

—Appliqué sur les images cinq valeurs pour la contrainte C (128, 64, 32, 16 et 8).

—Deux images médicales différentes une est de type rayonsX de taille 320 * 496 pixels et l'autre est de type scanner CT de taille 512 * 512 pixels.

—Les résultats sont présenté dans les tableaux 3.1 et 3.2 pour deux images médicales.

| | information créptée | | | | |
|---|---|---|---|---|---|
| C | Coefficients | Bits | Bits% | Pixels changés % | PSNR (db) |
| 128 | 26289 | 81740 | 23.0 | 85.7 | 23.39 |
| 64 | 23987 | 71900 | 202. | 85.7 | 20.42 |
| 32 | 10835 | 52101 | 14.6 | 85.3 | 25.02 |
| 16 | 10966 | 31106 | 8.8 | 83.5 | 27.66 |
| 8 | 6111 | 16765 | 4.7 | 76.1 | 30.90 |

TABLE 3.1 – Résultats pour l'image rayons X d'un cancer du colon, figure 5.a, 320 * 496 pixels.


FIGURE 3.1 – (a) image médicale originale d'un cancer du colon, 320 * 496 pixels, (b) image cryptée pour c = 128.

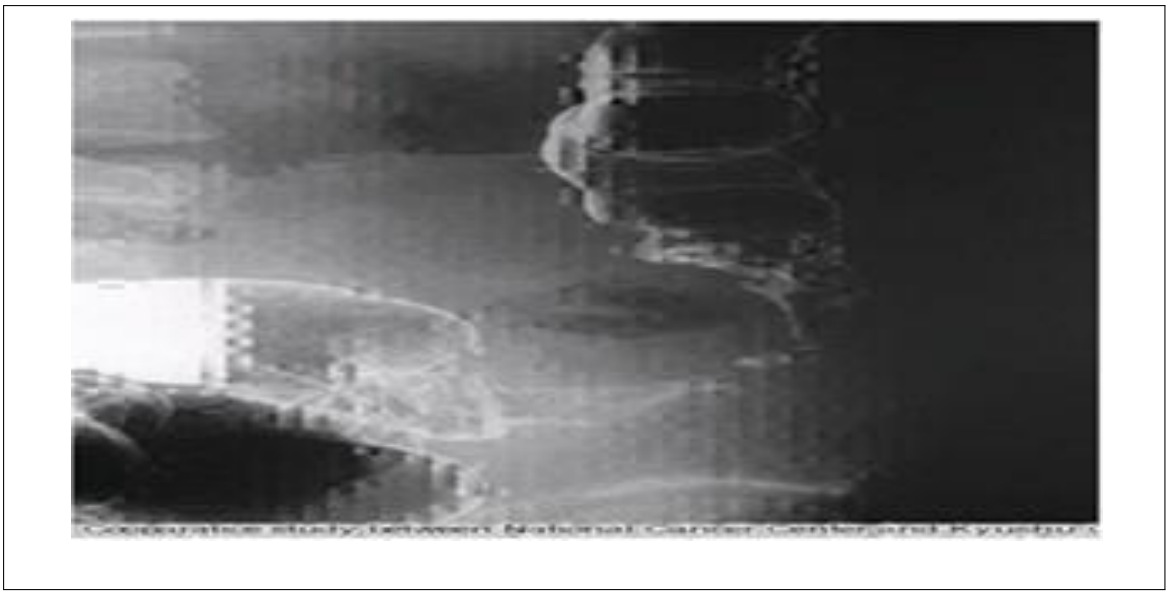

FIGURE 3.2 – image cryptée pour C =8 .

| | information créptée | | | | |
|---|---|---|---|---|---|
| C | Coefficients | Bits | Bits% | Pixels changés % | PSNR (db) |
| 128 | 51147 | 131127 | 26.7 | 87.9 | 28.18 |
| 64 | 47656 | 119423 | 24.3 | 87.9 | 28.31 |
| 32 | 18957 | 95850 | 19.5 | 87.9 | 29.15 |
| 16 | 10966 | 53083 | 10.8 | 85.0 | 30.45 |
| 8 | 9633 | 26606 | 4.7 | 74.7 | 33.06 |

TABLE 3.2 – Résultats pour l'image médicale scanner CT, 512*512 pixels

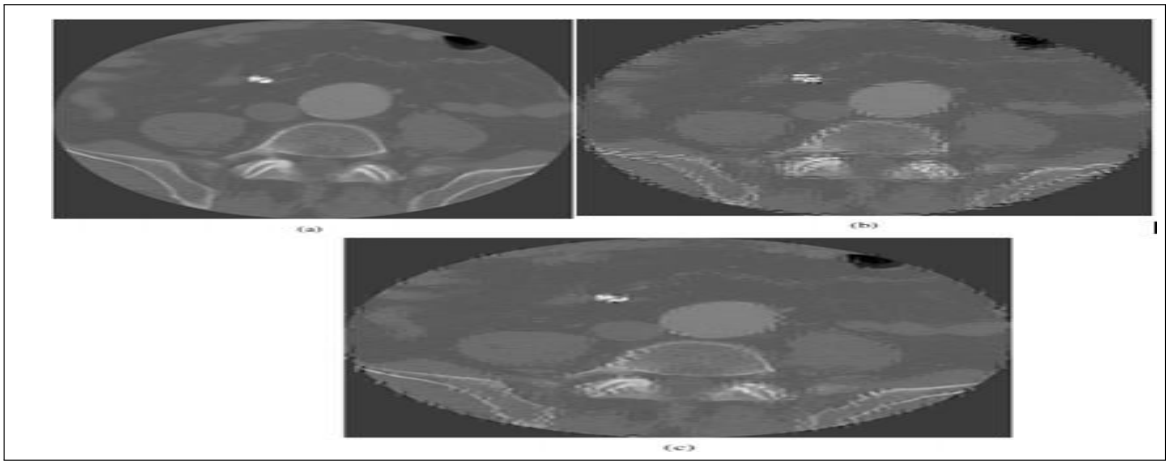

FIGURE 3.3 – (a) Image médicale d'un scanner 512*512 pixels. (b) image cryptée pour C =128 (c) image cryptée pour C = 8 .

## Une méthode de cryptage sans perte pour les images médicales à l'aide de cartes de bord (2009)

.

Yicong Zhou, Member, IEEE, Karen Panetta, Fellow, IEEE, and Sos Agaian proposent un nouvel algorithme, EdgeCrypt, pour crypter les images médicales à l'aide d'une carte de bord dans le domaine de la non-compression[45].

### Principe

La base sous-jacente de l'algorithme EdgeCrypt est de crypter les images médicales en modifiant les données d'image sans compresser les images.

- **EdgeCrypt** obtient la carte de bord de l'image médicale en appliquant un type spécifique de détecteur de bord tel que Canny, ou Sobel, ou Prewitt, ou tout autre, avec une certaine valeur seuil.
- L'algorithme décompose ensuite l'image médicale en plusieurs plans de bits binaires a partir la méthode de décomposition des plans de bit binaire..
- Crypter tous les plans de bits en effectuant une opération XOR entre la carte de bord et chaque plan de bits.
- Crypter la carte de bord en utilisant une séquence de bits aléatoire générée à partir de la carte logique chaotique, entrelace la carte de bord cryptée parmi les plans de bits *XORed.*
- Inverser l'ordre de tous les plans de bits et les combine pour obtenir les images médicales cryptées finales.

Le schéma fonctionnel de l'algorithme **EdgeCrypt** est illustré à la figure 3.4.

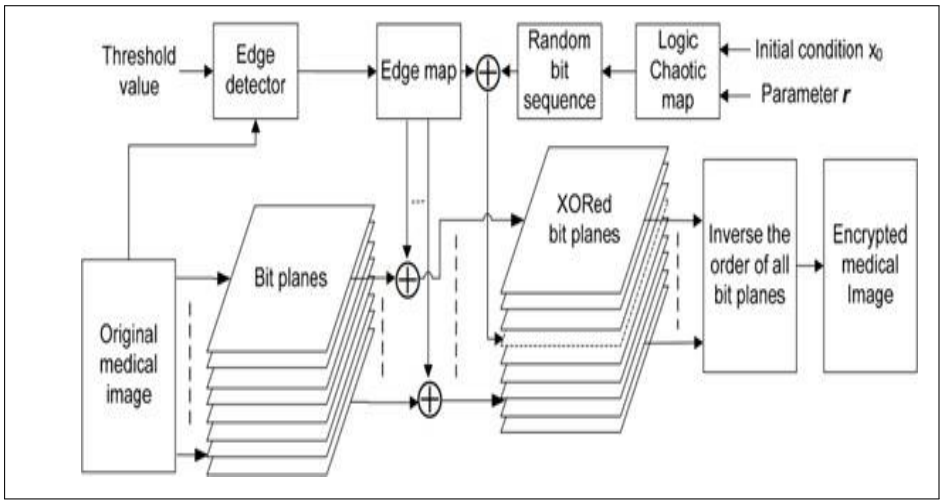


FIGURE 3.4 – Le schéma de principe de l'algorithme EdgeCrypt.

- Le processus de décryptage décompose d'abord l'image cryptée en plans de bit binaires. Il inverse ensuite l'ordre de tous les plans de bits et extrait la carte des bords des plans de bits. La carte des bords est reconstruite à l'aide de clés de sécurité. L'algorithme

effectue une opération XOR entre la carte de bord et chaque plan binaire et combine les plans binaires XOR pour obtenir l'image médicale reconstruite.

**Résultats**

- L'algorithme EdgeCrypt a été implémenté avec succès dans plus de 16 images médicales en niveau de gris.
- Les images est de types IRM, radiographiques, CT. les tailles de ces images sont 512*512 pixel.
- L'histogramme obtenu du cryptage des images IRM.

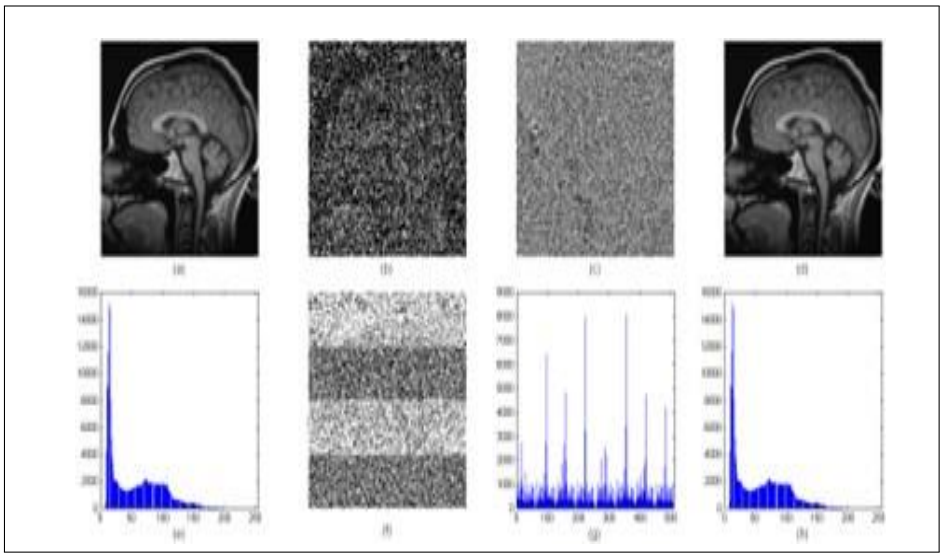

FIGURE 3.5 – Cryptage des images IRM. (a) L'image IRM originale ; (b) La carte des bords obtenue par le détecteur de bords Sobel avec un seuil de 0,5 ; (c) l'image IRM cryptée, (d) l'image IRM reconstruite ; (e) Histogramme de l'image IRM originale ; (f) la carte des bords chiffrée, x0 = 0,6, r = 3,65 ; (g) Histogramme de l'image IRM cryptée ; (h) Histogramme de l'image IRM reconstruite..

- L'histogramme obtenu du cryptage du l'image CT.

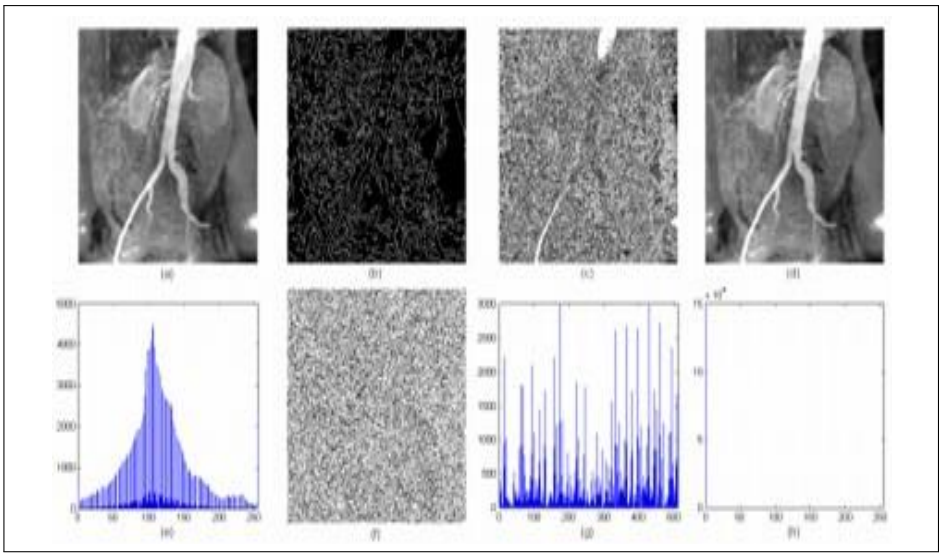

FIGURE 3.6 – Cryptage de l'image CT. (a) L'image CT originale; (b) La carte de bord obtenue par le détecteur de bord Canny avec un seuil de 0,1; (c) l'image CT cryptée, (d) l'image CT reconstruite; (e) Histogramme de l'image CT originale; (f) la carte de bord chiffrée, 0 x = 0,2, r = 3,8; (g) Histogramme de l'image CT cryptée; (h) Histogramme de la différence entre (a) et (d).
.

‡ L'histogramme obtenu du cryptage des images radiographiques.L'algorithme Edge- Crypt peut être utilisé pour protéger les objets ou régions sélectionnés dans les images médicales qui peuvent contenir des informations importantes ou privées sur les patients.

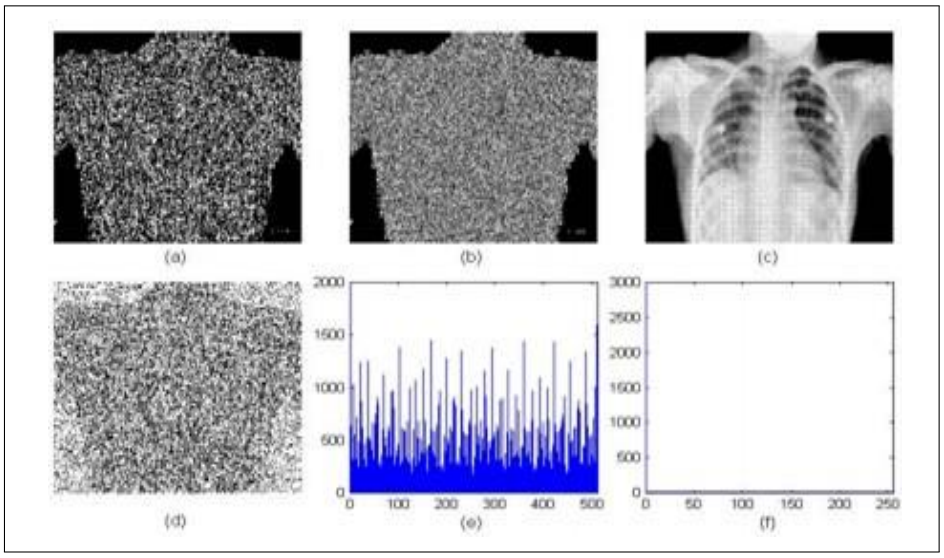


FIGURE 3.7 – Cryptage des images radiographiques. (a) La carte des bords obtenue par le détecteur de bords Prewitt avec un seuil de 0,3; (b) L'image radiographique cryptée; (c) L'image radiographique reconstruite; (d) la carte de bord chiffrée, 0 x = 0,8, r = 3,7; (e) Histogramme de l'image radiographique cryptée ; (f) Histogramme de la différence entre l'image radiographique originale et l'image reconstruite..

‡ Pour montrer l'efficacité de l'algorithme EdgeCrypt pour le cryptage des images

médicales, il a été comparé à l'algorithme AES implémenté dans sur plusieurs images.

Une image du cerveau par IRM 512 * 512 est utilisée comme exemple des résultats obtenus. Le temps d'exécution de ce cryptage d'image IRM à l'aide de l'algorithme EdgeCrypt, puis de l'algorithme AES, est mesuré dans meme environnement. L'algorithme AES prend 521,67 secondes pour crypter cette image IRM. Cependant, l'algorithme Ed- geCrypt ne passe que 17,78 secondes pour crypter la même image IRM. Cela montre que la vitesse de l'algorithme EdgeCrypt est beaucoup plus rapide que celle de l'algorithme AES.

## Cryptage d'images médicales à l'aide de cartes de bord(EMMIE)(2016)

Weijia Cao, Yicong Zhou, C.L. Philip Chen et Liming Xia proposent un algorithme de cryptage d'images médicales utilisant des cartes de bord dérivées d'une image source. L'algorithme est composé de trois parties : la Décomposition du plan de bits, le générateur de séquence aléatoire et la permutation (la méthode de brouillage)[46].

### Description d'EMMIE

L'organigramme d'EMMIE est représenté sur la figure 3.8.

1. Une image médicale à chiffrer est d'abord décomposée en certains plans de bit avec un procédé de décomposition réversible. Cette décomposition se fait par différentes méthodes, par ex. Décomposition du plan de bit binaire, décomposition des plans bi- naires du code P de Fibonacci et décomposition des plans binaires du code P tronqué de Fibonacci .
2. Les cartes de bord sont générées àpartir d'une image source avec des seuils identiques ou différents et ce sont des images binaires de même taille que les plans binaires d'origine. Certains détecteurs de bord sont généralement appliqués pour générer des cartes de bord d'images 2D, par ex. Détecteurs Prewitt, Sobel et Canny .
3. Ensuite, EMMIE effectue une opération XOR entre les plans de bits et les cartes de bords.
4. Enfin, les positions binaires de tous les plans binaires XOR sont brouillées puis combinées avec une diffusion de pixels pour composer une image chiffrée.

Le décryptage est le processus inverse des étapes ci-dessus :

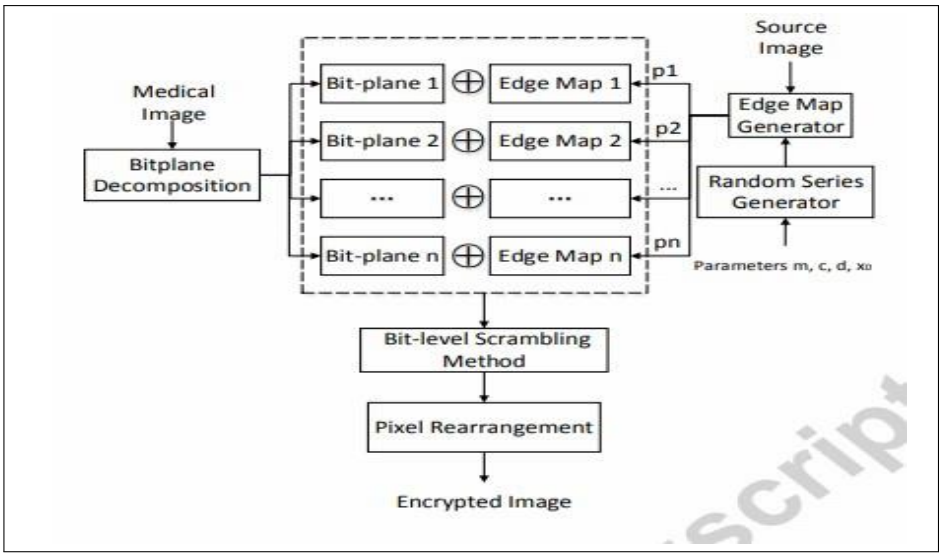


FIGURE 3.8 – l'organigramme d'EMMIE.

**Résultats**

÷ Vingt images en niveau de gris ont été expérimentées. les types de ces images est IRM, radiographiques, CT et américaines. les tailles de quelque image sont 256 * 256, et les tailles des autres images sont de 512 * 512.

÷ la figure 3.9 représente les résultats de cryptage EMMIE de l'image IRM avec une carte de bord sélectionnée à partir d'une autre image IRM.

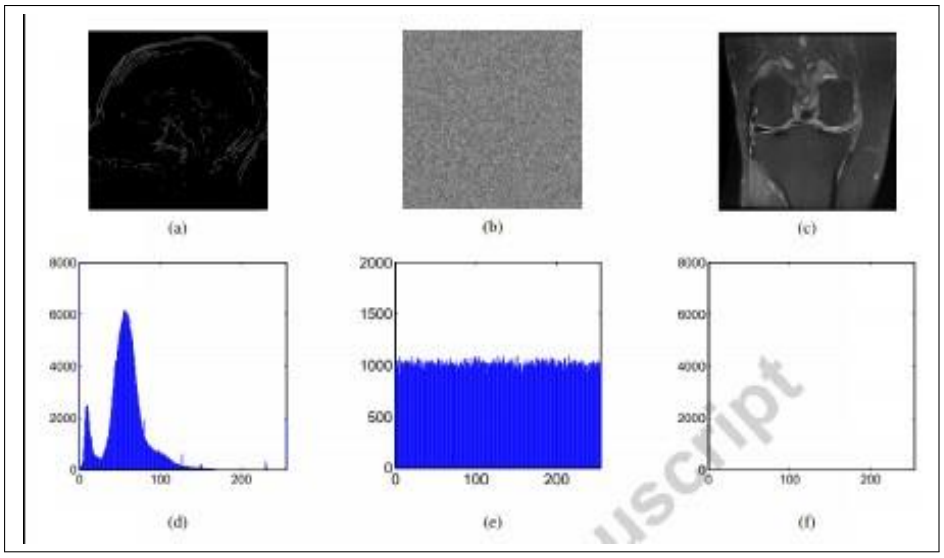


FIGURE 3.9 –
résultats de cryptage EMMIE de l'image IRM : (a) la carte des bords par le détecteur Sobel; (b) l'image chiffrée; (c) l'image IRM reconstruite; (d) l'histogramme de l'image originale; (e) l'histogramme de (b); (f) l'histogramme de la différence entre l'image originale et (c).

÷ la figure 3.10 représente les résultats de cryptage EMMIE de l'image CT avec une carte

de bord extraite d'une image de source non médicale.

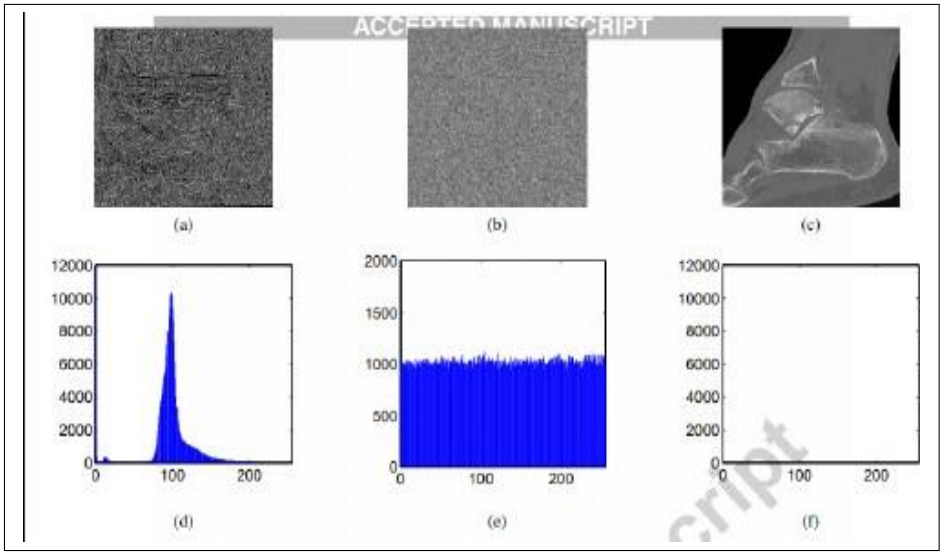


FIGURE 3.10 –
résultats de cryptage EMMIE de l'image CT : (a) la carte de bord par le détecteur Sobel; (b) l'image chiffrée; (c) l'image CT reconstruite; (d) l'histogramme de l'image originale; (e) l'histogramme de (b); (f) l'histogramme de la différence entre l'image originale et (c)

÷ la figure 3.11 représente les histogrammes d'image cryptée à l'aide des cartes de bord avec différents détecteurs et le même seuil.

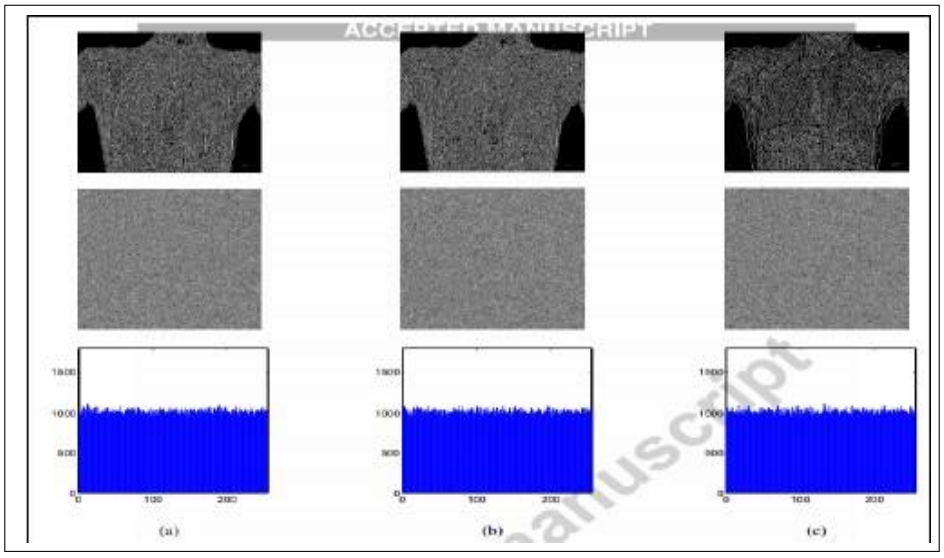


FIGURE 3.11 –
Les histogrammes de l'image cryptée en utilisant les cartes de bord avec différents détecteurs. dans la première rangée en utilisant différents détecteurs avec un seuil de 0,02 :
(a) Prewitt, (b) Sobel, (c) Canny detectors, dont les images chiffrées et leurs histogrammes sont affichés dans les deux dernières lignes

÷ la figure 3.12 présente les résultats de cryptage de la même image originale en utilisant

des cartes de bord générées à partir de la même image source avec trois seuils, 0.1, 0.01, 0.001 et un même détecteur de bord (Sobel).

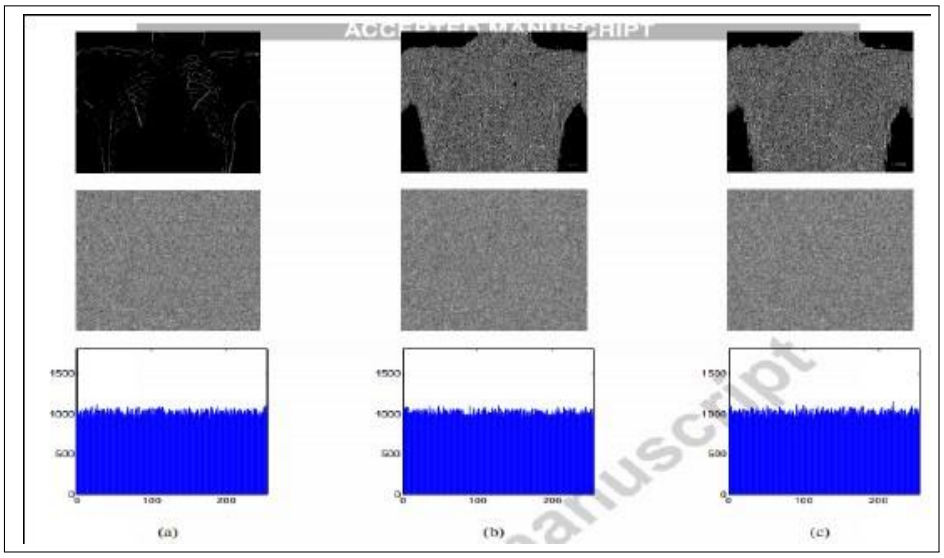


FIGURE 3.12 –
Les histogrammes des images cryptées en utilisant les cartes de bord en utilisant un détecteur Sobel avec différents seuils dans la première ligne : (a) 0,1, (b) 0,01, (c) 0,001, dont le chiffre les images et leurs histogrammes sont affichés dans les deux dernières lignes.

÷ la figure 3.13 montre la corrélation des pixels adjacents à partir des images d'origine et chiffrées.

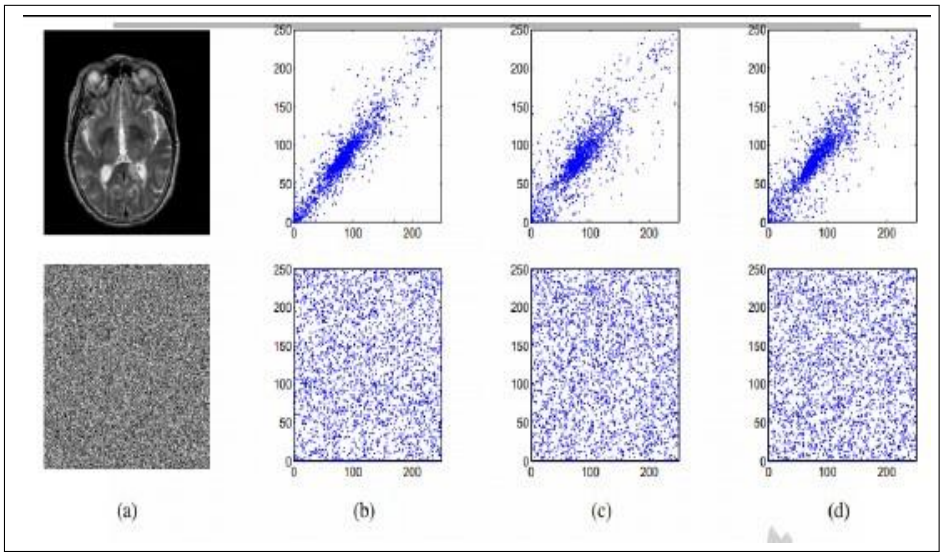


FIGURE 3.13 –
Analyse de corrélation dans différentes directions. Les rangées du haut et du bas représentent les paires voisines de (a) l'image d'origine et l'image chiffrée dans les directions
(b) horizontale, (c) verticale et (d) diagonale, respectivement

÷ La figure 3.14 montre les résultats de simulation de l'analyse d'histogramme pour les deux schémas de cryptage d'image (DecomCrypt (vue précédent) et EMMIE).

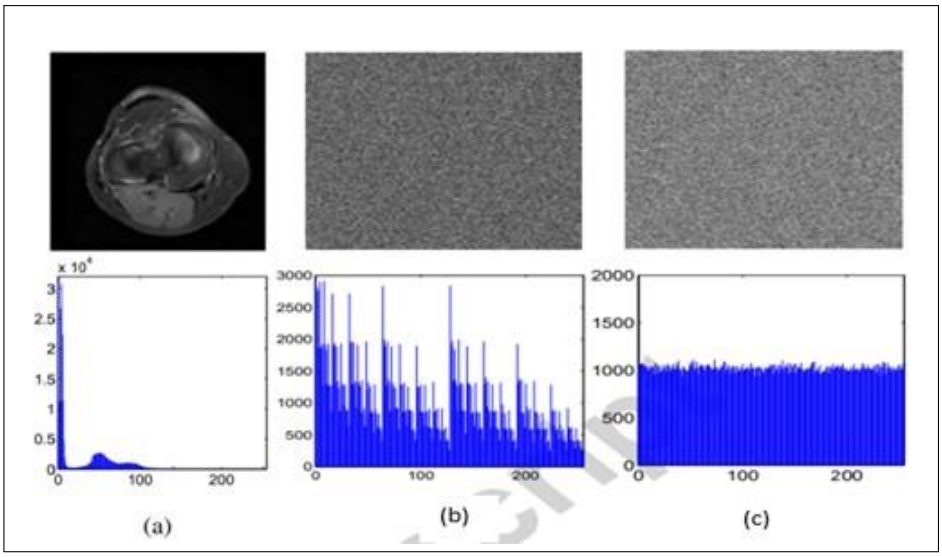


FIGURE 3.14 –
Analyse de l'histogramme. (a) L'image originale et son histogramme; (b) - (c) sont les images chiffrées et leurs histogrammes basés sur les schémas de (b) DecomCrypt et (e) EMMIE.

÷ la figure 3.15 représente le temps de cryptage d'EMMIE, la courbe bleue est dessinée de 0,0129 à 1,846 secondes avec différentes tailles d'image (change de8 x 8 à 512 x 512), ce qui est inférieur aux autres schémas comme DecomCrypt.

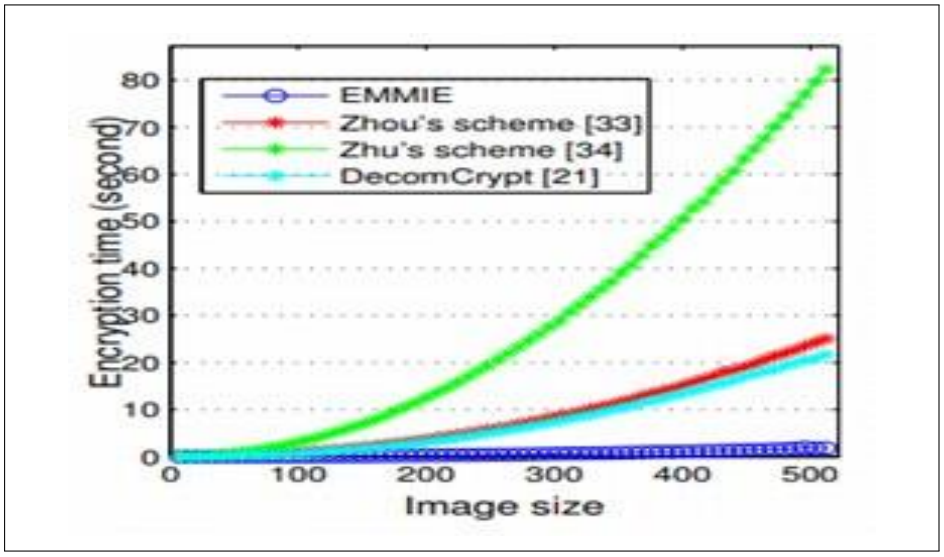


FIGURE 3.15 –
Les temps de cryptage des schémas de DecomCrypt et EMMIE avec l'augmentation de la taille de l'image d'origine . Les lignes , bleu-vert et bleu représentent les méthodes de Zhu, Zhou, DecomCrypt et EMMIE, respectivement

## Cryptage d'images médicales basé sur l'arrangement des pixels et la permutation aléatoire pour la sécurité de la trans- mission(2007)

K.Usman, H.Juzojil, I.Nakajimal, S.Soegidjoko, M.Ramdhani, T.Hori, S.Igiproposent une méthode de cryptage basé sur l'arrangement des pixels et la permutation aléatoire pour la sécurité de la transmission[47].

### Permutation aléatoire et arrangement de pixels Permutation

- **de colonne et permutation deLigne**

Une image numérique rectangulaire X est utilisée qui a M pixels en ligne et N pixels en colonne.

**La permutation de colonne :** est définie de la manière suivant :

1. La colonne de l'image est divisée en P intervalles, $N_1, N_2, .., N_p$. La valeur de $N_1$ à Np est tout nombre entier positif. La somme des intervalles devrait à nouveau être égale à N. ($N_1 + N_2 + .. + N_p = N$)
2. L'image X s'est ensuite divisée en sous-images selon ces intervalles pour produire des sous-images M * $N_1$, M x $N_2$,.., M * $N_p$.
3. Après ces processus de partition, les sous-images sont permutées au hasard pour produire l'image modifiée F.

**La permutation de lignes :** est définie de manière similaire. Comme suit :

1. La ligne d'images est divisée en Q intervalles, $M_1, M_2, .. , M_Q$. La somme de tous Miest égale à M. ($M_1 + M_2 + .. + M_Q = M$)
2. Nous obtient des sous-images M1 x N, M2 x N, MQx N. Encore une fois, est appliqué une permutation aléatoire sur ces sous-images pour produire une image modifiée Z.

La figure 3.16 illustre les processus.

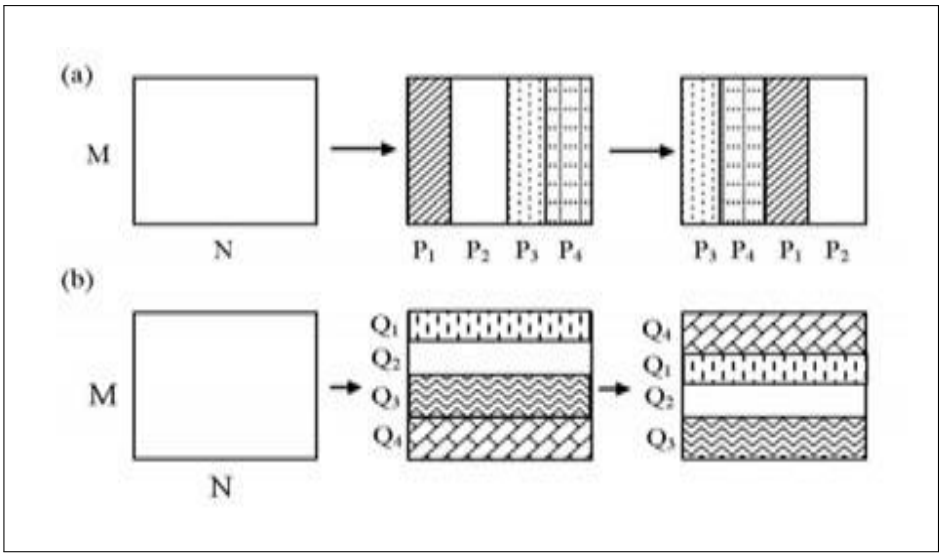


FIGURE 3.16 – permutation aléatoire sur une image. (a) Permutation de colonne, (b) Permu- tation de ligne. À gauche : image originale. Milieu : processus de partition. À droite : résultat après permutation. .

**Arangement des pixels**

L'arrangement des pixels réorganise la position des pixels selon une certaine règle. Pour l'image numérique X avec M pixels en ligne et N pixels en colonne, la position des pixels est réarrangée pour produire un résultat Y de la taille de K pixels en ligne et L pixels en colonne. Où K * L = M * N, et K n'est pas égal à M. Après avoir effectué une telle transformation de taille, il existe de nombreuses possibilités pour mapper les pixels X à Y. La figure 3 montre un exemple d'arrangements de 3 * 5 pixels à 5 * 3 pixels.

L'arrangement des pixels de M par N à K par L comme illustré sur la figure 3.17.

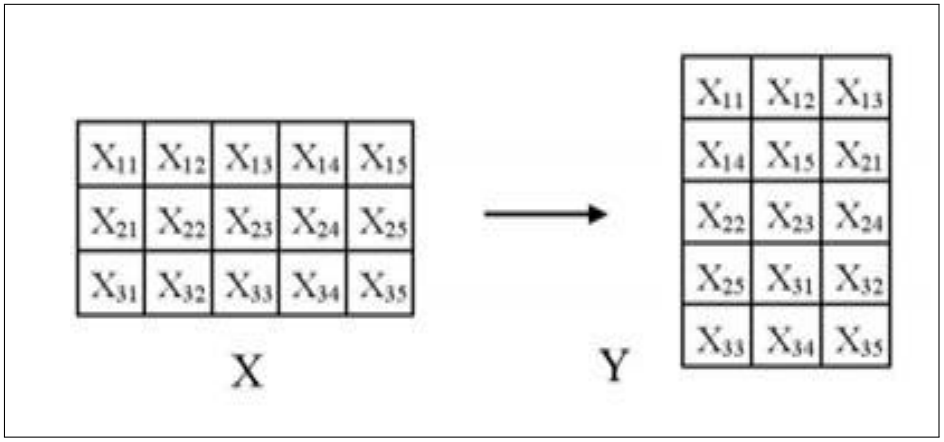


FIGURE 3.17 – Disposition des pixels. X : original, Y : résultat.

✍ **Principe**

Ce Schéma de cryptage pour le cryptage des images médicales comprend les étapes suivantes :

1. Génération de clé.
2. Faire Arrangement des pixels.
3. Faire Permutation de colonne.
4. Faire Permutation de ligne.
5. Répétez les étapes 2, 3 et 4 pour N round.

✍ **Résultats**

La figure 3.18 montre le cryptage et le décryptage de plusieurs images médicales comme : microbiologie, Microbiologie, Radiologie, Echographie, Electrocardiographie. Le tableau 1 montre le temps de calcul pour le cryptage et le décryptage de chaque image utilisée sur la figure 3.18.

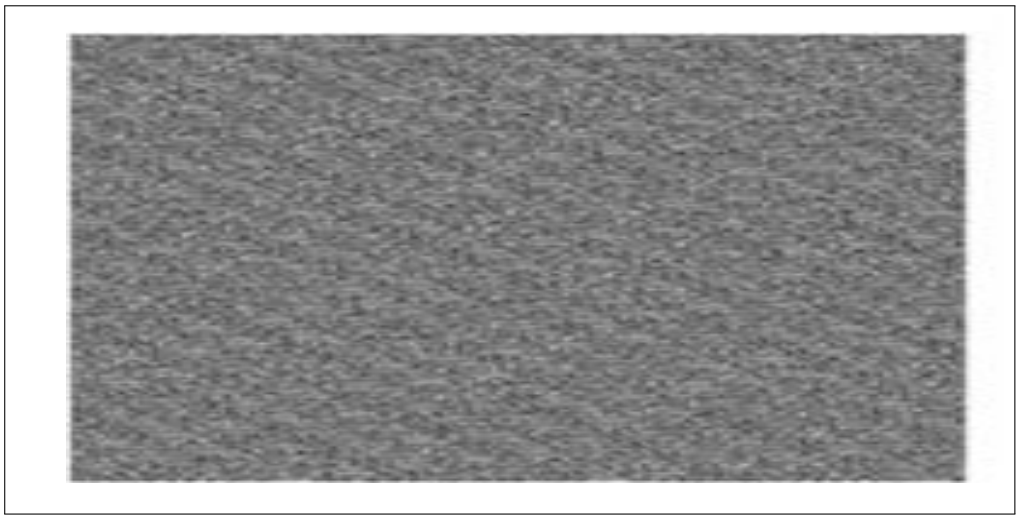

FIGURE 3.18 – Exemples de cryptage d'images médicales. L'image de gauche est le fi- chier d'origine et l'image de droite est le résultat chiffré. Dix séries d'itérations sont ap- pliquées pour chaque image. A. Microbiologie C. Thrombus ventriculaire gauche, échographie D.Electrocardiographie.

| Image | Size(MxN) | Average encryption time(s) | Average encryption time(s) |
|---|---|---|---|
| A | 475*700 | 1.231 | 1.093 |
| B | 500*446 | 0.849 | 0.562 |
| C | 400*568 | 0.706 | 0.600 |
| D | 434*823 | 1.333 | 1.309 |

TABLE 3.3 – Temps de traitement du cryptage et du décryptage des images échantillons..

## Schéma de cryptage d'images médicales basé sur la séquence d'ADN(2018)

J.Sher Khan, J.Ahmad, S.FarooqAbbasi, Arshad et S.KocKayhansont proposent un schéma de cryptage d'images médicales basé sur une séquence d'ADN (acide désoxyribonucléique) et une carte logistique entrelacée[48]..

**Principe**

L'organigramme du schéma de chiffrement basé sur la séquence d'ADN proposé est présenté sur la figure 3.20. Cet organigramme contient principalement quatre étapes :

1. **Génération de clés secrètes et de nombres aléatoires**
   Une séquence d'ADN aléatoire peut être sélectionnée dans la base de données ADN . Pour des raisons d'expérimentation, la séquence d'ADN numérotée NZ ABLK01000602 est sélectionné au hasard parmi 163 millions de séquences d'ADN comme entrée de la fonction de hachage. Pour la valeur susmentionnée de la séquence d'ADN, utilisez l'algorithme SHA-512 pour obtenir une valeur de hachage de 512 bits (128 caractères).
   À partir de cette valeur de hachage de 512 bits, calculez les conditions initiales x0, y0 et z0 pour la carte logistique entrelacée.
2. **Permutation**
   Les 256 dernières valeurs des vecteurs aléatoires x et y sont triées et les résultats sont stockés dans x' et y'. La taille des vecteurs x' et y' est de 1 * 256. Afin de permuter les lignes et les colonnes de l'image en clair P (taille 256 * 256), utilisez les vecteurs aléatoires x' et y', respectivement, et enregistrez les résultats dans PS.
3. **Diffusion**
   Organisez le troisième vecteur aléatoire z dans une matrice M de taille 256 * 256, puis XOR au niveau du bit avec l'image mélangée comme suit : PD = bitxor (PS, M).
4. **Transformation affine**

Dans la dernière étape, appliquez une transformation affine sur chaque pixel PD (i, j) À des fins de décryptage, appliquez toutes les étapes de cryptage dans l'ordre inverse.

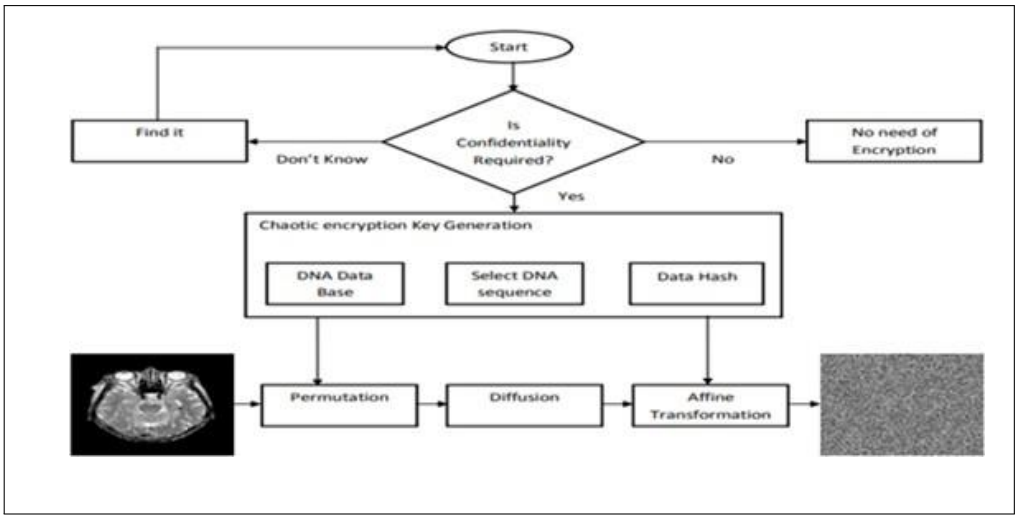


FIGURE 3.19 – organigramme du schéma proposé.

**Résultats**

- Le schéma de cryptage d'image médicale proposé a été testé sur des images DICOM et CTHEAD (256 * 256).
- la figure 3.20 représente le chiffrement et les résultats de l'histogramme pour les images DICOM et CTHEAD.

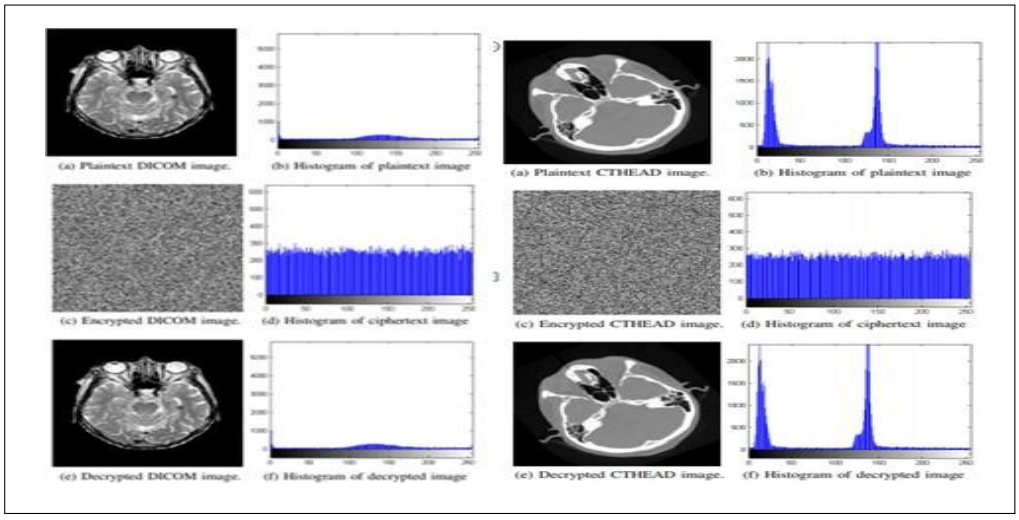


FIGURE 3.20 – résultats de chiffrement et l'histogramme pour l'image CTHEAD à gauche et résultats de chiffrement et l'histogramme pour l'image DICOM à gauche

- la figure 3.21 représente l'analyse de corrélation pour l'image DICOM et l'image CTHEAD.

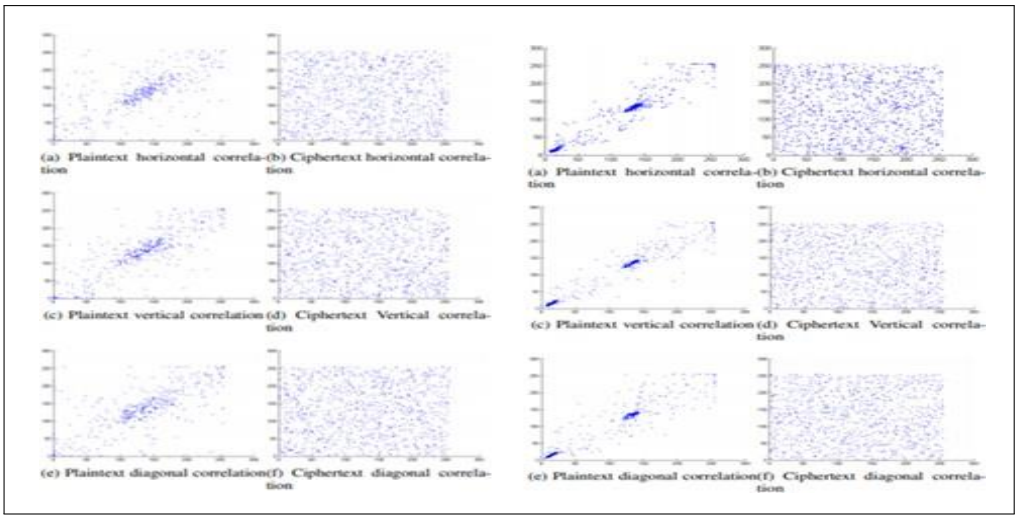


FIGURE 3.21 – tracés d'analyse de corrélation pour l'image CTHEAD à gauche et tracés d'analyse de corrélation pour l'image DICOM à droite

÷ La figure 3.22 montre la sensibilité de l'image cryptée à un petit changement de clé secrète.

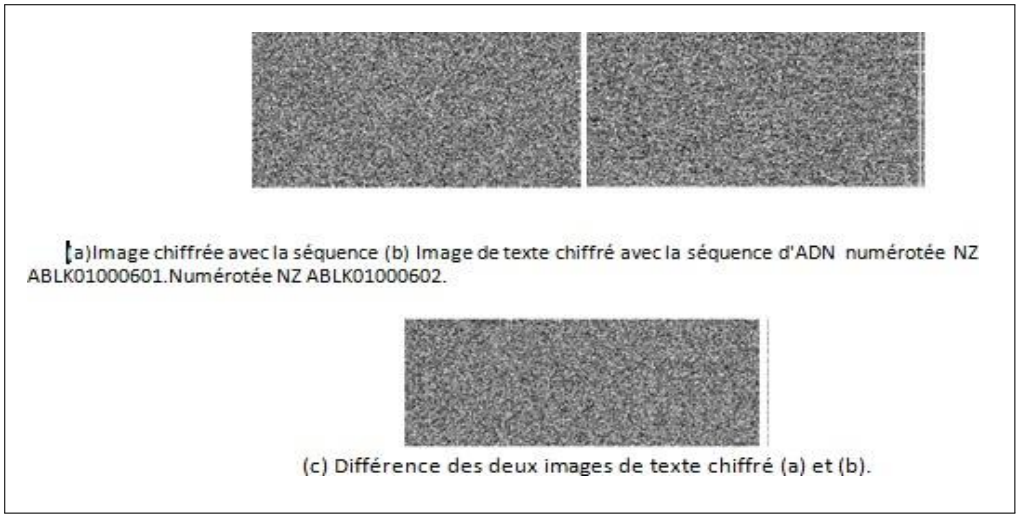


FIGURE 3.22 – Test de sensibilité clé

## Cryptage d'images médicales basé sur le chaos à l'aide de la cryptographie symétrique (2008)

M.Ashtiyani, P.MoradiBirgani, Hesam M. Hosseini sont proposent un schéma de cryptage d'image médicale basé sur la combinaison d'une carte chaotique pour le brouillage des adresses des pixels et d'un AES chaotique simplifié (S-AES) pour le cryptage (des valeurs de pixels correspondantes)[49].

**Principe d'algorithme**

Cet algorithme se compose de deux parties, à savoir le brouillage et le cryptage. Tous deux utilisent le chaos. La figure 1 illustre le schéma de principe de cet algorithme.
Comme illustré, les pixels de l'image ont d'abord été brouillés via la carte chaotique de Chat. Ensuite, la deuxième étape fournit la diffusion pour la modification des valeurs de pixels dans l'image en appliquant l'algorithme S-AES (avec S-box chaotique) à chaque pixel.

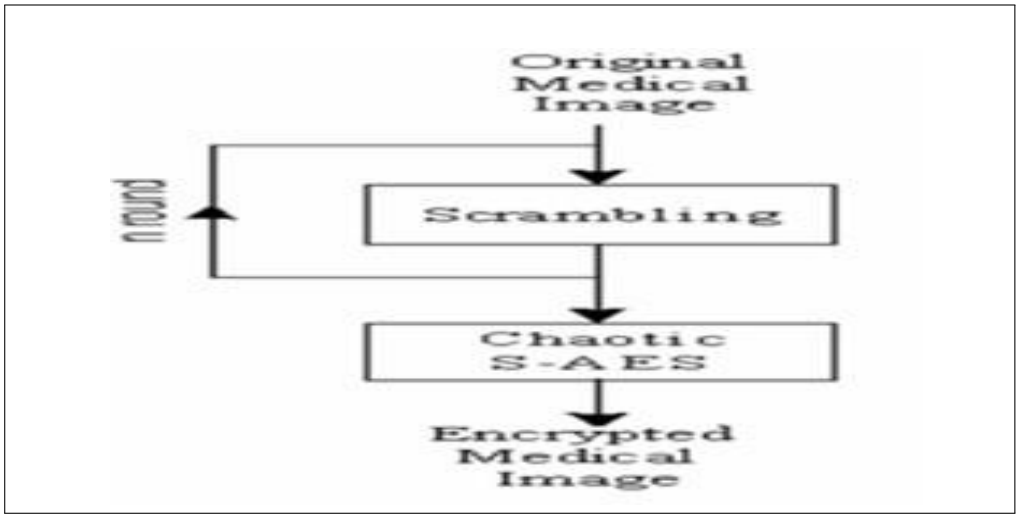


FIGURE 3.23 – schéma de principe de ce projet.

**La méthode de brouillage (SCRAMBLING) :**
Cette étape est appelée étape de confusion qui permute les pixels de l'image médicale sans changer ses valeurs en appliquant un algorithme de brouillage.
L'algorithmede brouillage utilisé ici est la carte du chat.

**La carte de chat :**
La carte du chat est une carte chaotique bidimensionnelle introduite par Arnold et Avez. Elle est nommée en raison de sa démonstration avec le visage d'un chat habituellement.

**CHAOTIC S-AES :**
L'algorithme utilise la carte chaotique de Lorenz dans le processus de cryptage en l'utilisant dans la procédure de conception S-box.
Ici, l'algorithme utilise l'approche présentée et produisons une S-box chaotique pour S-AES. S-AES est une version simplifiée de l'algorithme AES . Il fonctionne sur des textes clairs 16 bits et génère des texteschiffrés 16 bits, en utilisant la clé étendue k0, k1, .., k47.

**Résultats**

- ÷ L'image de mammographie ordinaire de taille 256 * 256 et 256 niveaux de gris est utilisée.
- ÷ Les histogrammes obtenu de l'image mammographie.

FIGURE 3.24 – image de mammographie originale

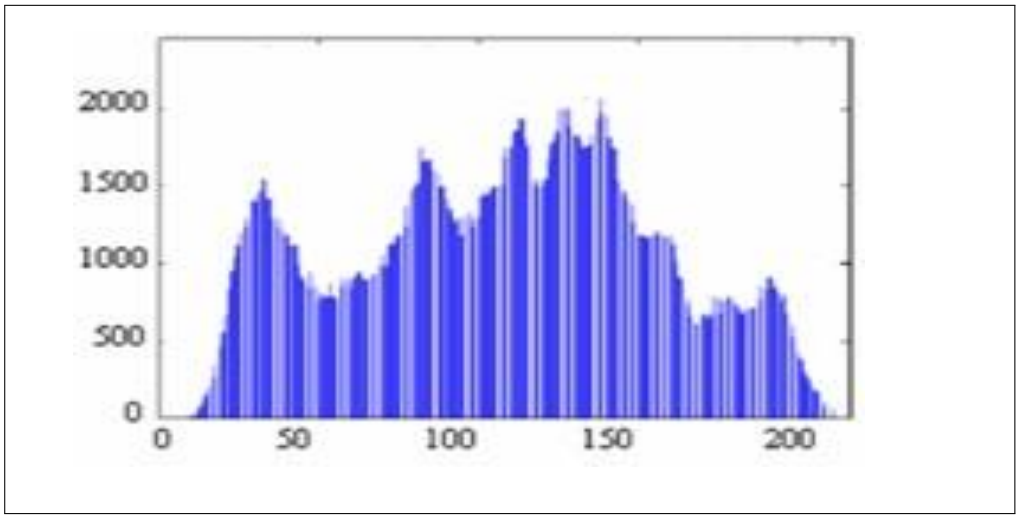


FIGURE 3.25 – histogramme de l'image médicale de la figure 3 (24)

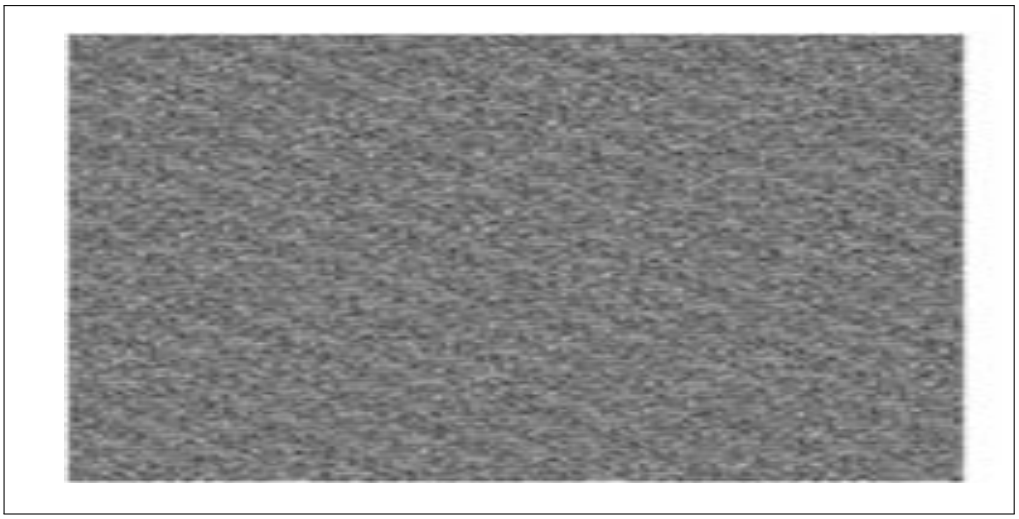

FIGURE 3.26 – image médicale brouillée.

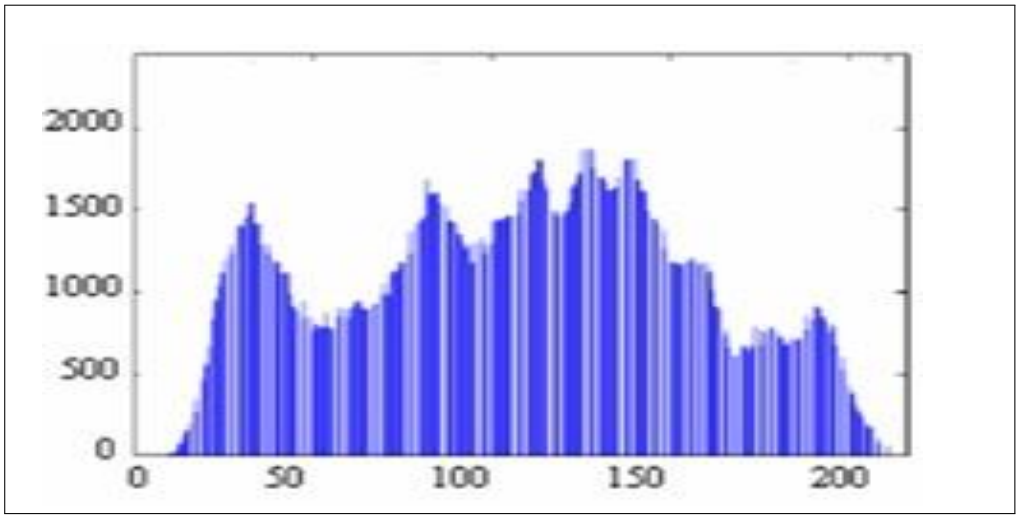


FIGURE 3.27 – histogramme de l'image médicale brouillée de la figure 3 (26)

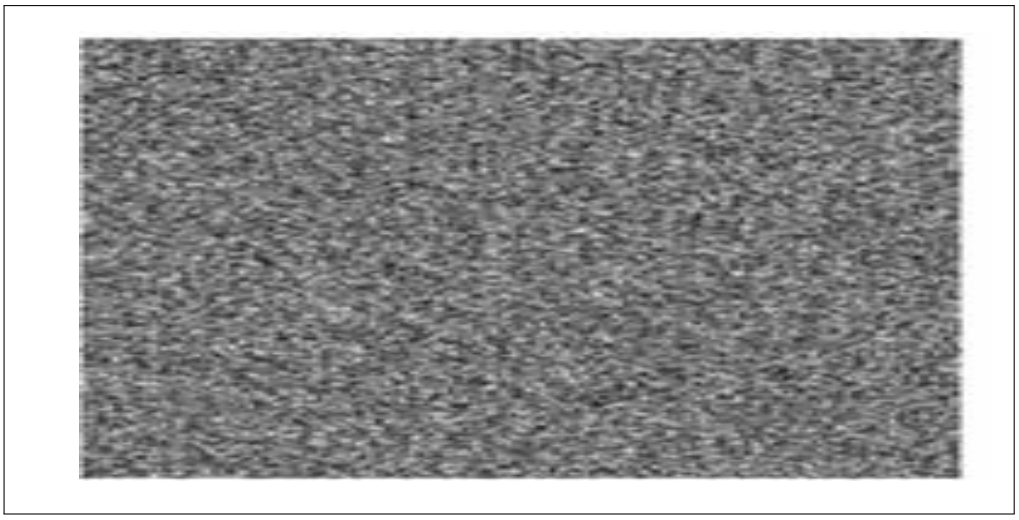

FIGURE 3.28 – image brouillée et cryptée

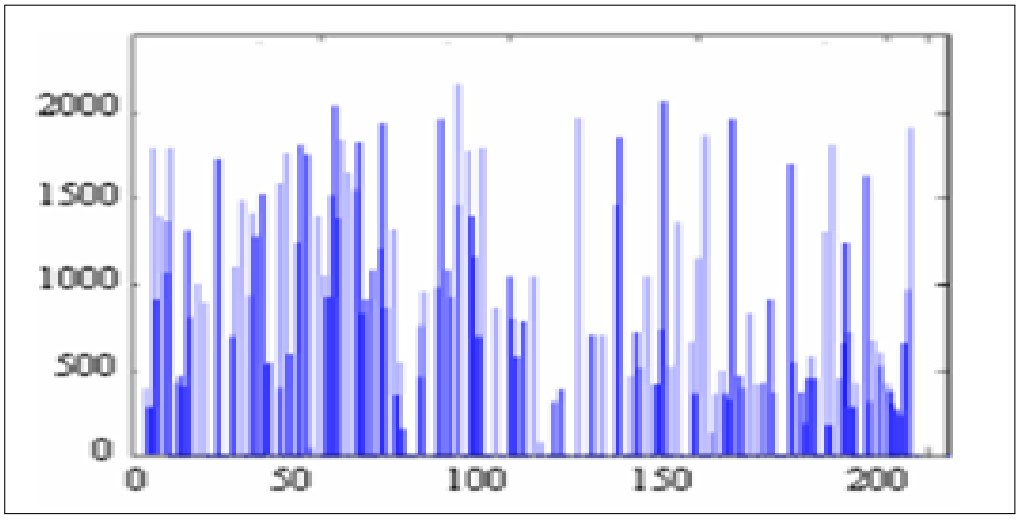


FIGURE 3.29 – histogramme de l'image médicale brouillée et cryptée de la figure 3 (28)

## Cryptage des images médicales à l'aide de la carte chaotique Norme de cryptage avancée améliorée(2018)

R. Singh Bhogal, B.Li, A.Gale and Y.Chen proposent un algorithme qui utilise une carte chaotique combinée avec AES en mode CBC (Cipherblockchaining) et l'avons testé contre AES dans sa forme standard. L'algorithme développé, CAT-AES, effectue une itération sur la carte de chat d'Arnold avant le cryptage un certain nombre de fois, alors que le cryptage AES standard ne le fait pas.

L'algorithme examine les images DICOM 16 bits au lieu des images 8 bits testées dans MeghdadAshtiyani et al. Papier dans la méthode précédent de ce chapitre. Cet algorithme similaire à MeghdadAshtiyani et al. Algorithme, Au lieu de S-AES, il utilisé AES comme algorithme de chiffrement pour être conforme à la norme DICOM[50].

**Principe**

Deux algorithmes ont été utilisés dans cet algorithme AES et l'algorithme développé, CAT-AES, qui est basé sur l'algorithme proposé par MeghdadAshtiyani et al.

- AES est implémenté pour prendre une image DICOM 16 bits en entrée, puis l'étendre horizontalement. Cela se fait en divisant chaque pixel 16 bits en deux pixels 8 bits. Le cryptage AES est ensuite appliqué, suivi de la concaténation des pixels adjacents, de nouveau en pixels simples de 16 bits pour former l'image cryptée.
- CAT-AES a la même structure, avec une étape supplémentaire, qui applique la carte de chat de manière itérative I catmap avant le cryptage.

La figure 3.30 illustre le Processus de cryptage CAT-AES.

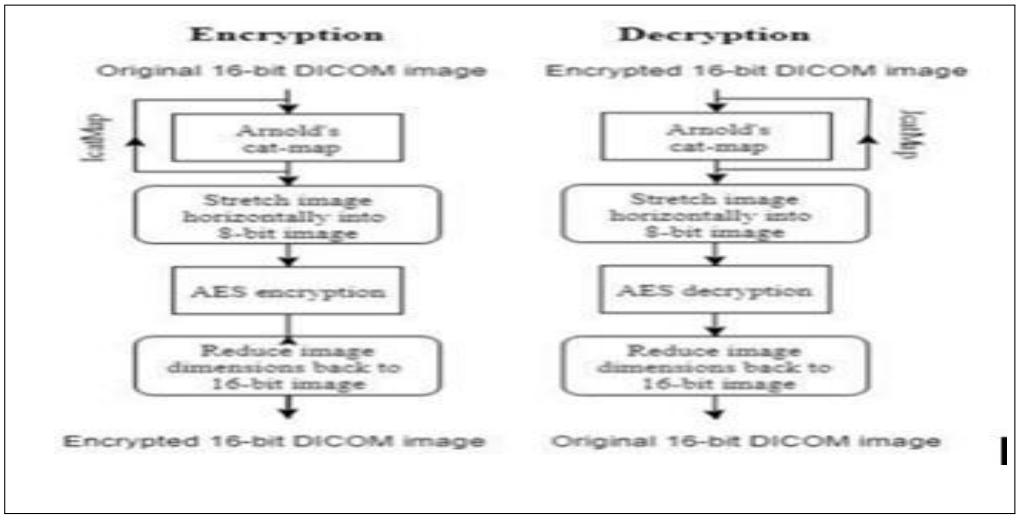


FIGURE 3.30 – Processus de cryptage CAT-AES. Le processus pour AES a la même structure, sans l'étape de carte de chat

**Résultats**

- Les deux algorithmes AES et CAT-AES ont été évalués sur deux ensembles 16 bits d'images DICOM : un ensemble de 20 images IRM cérébrales (256 * 256 pixels) et un ensemble de 26 images IRM du cancer du sein (320 * 320 pixels).
- la figure 3.31 et la figure 3.32 illustre le coefficient de corrélation absolu sur des ensemble d'images médicales.

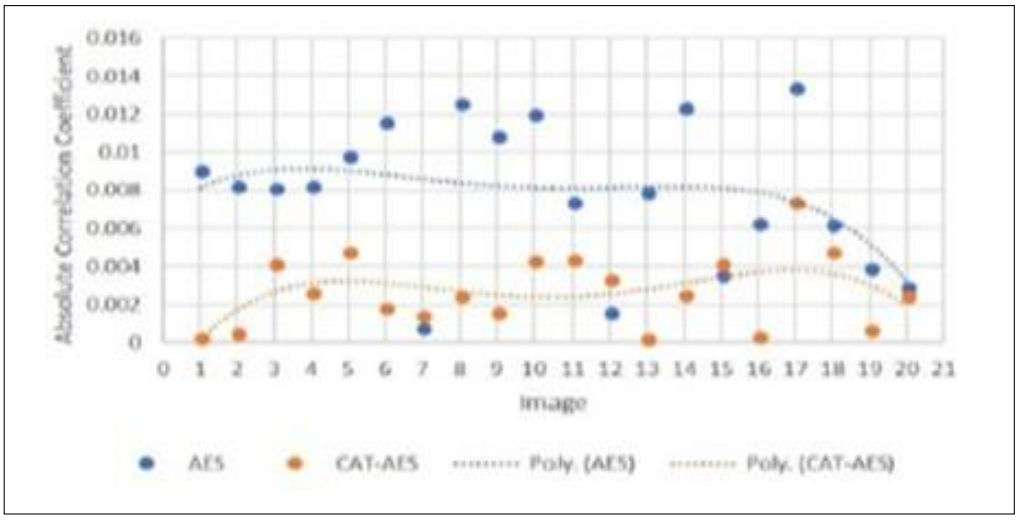


FIGURE 3.31 – coefficient de corrélation absolu sur 20 256 * 256 IRM cérébrale

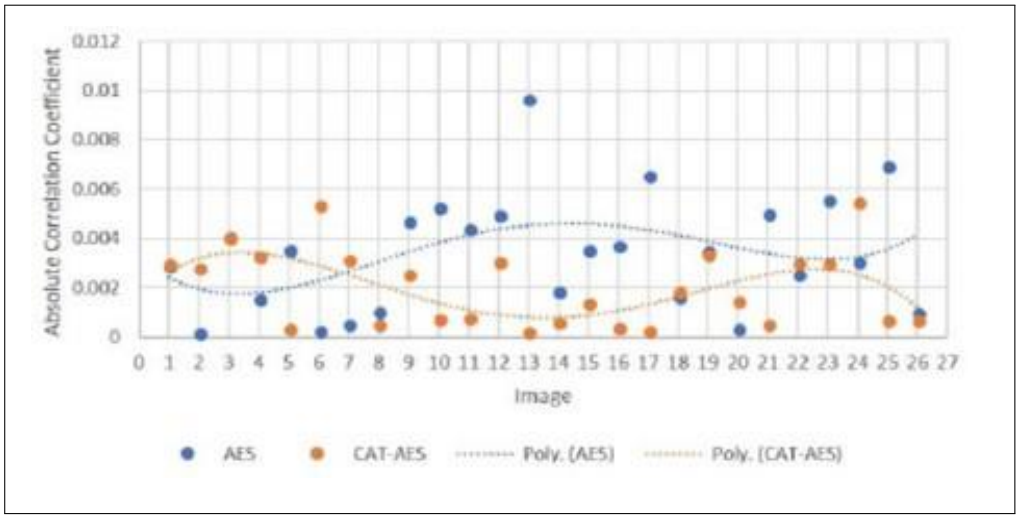


FIGURE 3.32 – coefficient de corrélation absolu sur 26 320 * 320 IRM du cancer du sein

÷ la figure 3.33 représente l'histogramme de l'image médicale du cerveau et l'image chiffré.

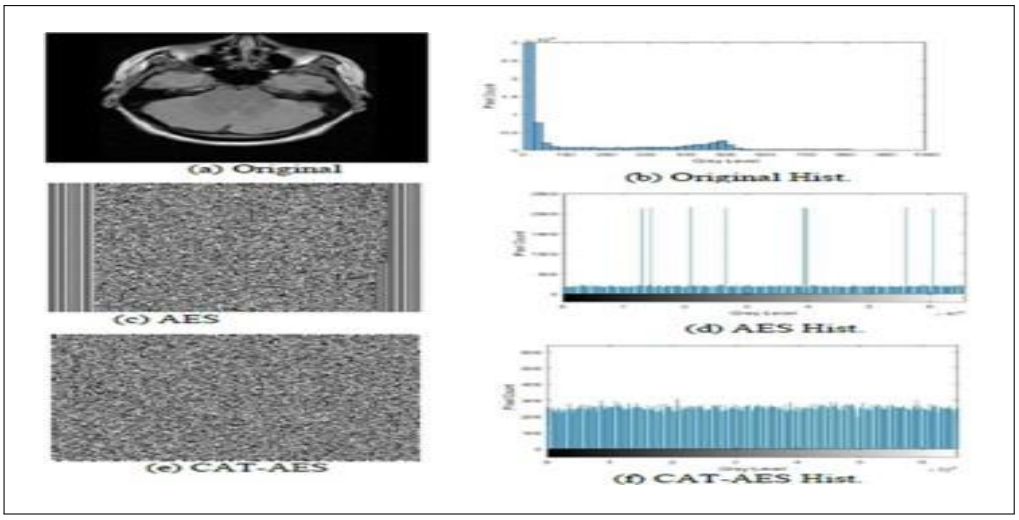


FIGURE 3.33 – images et histogrammes de cryptage cérébral.

÷ la figure 3.34 représente l'histogramme de l'image médicale IRM du cancer du sein et l'image chiffré.

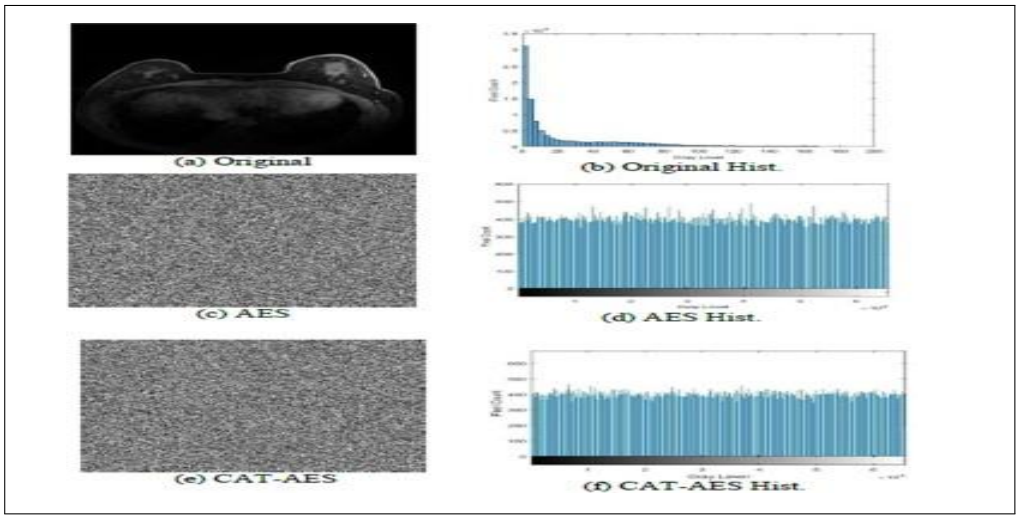


FIGURE 3.34 – images et histogrammes de cryptage du cancer du sein

÷ le cryptage CAT-AES a pris plus de temps en raison de l'étape supplémentaire de la carte de chat.
La carte du chat a pris 25,1du temps de cryptage et 23,9du temps de décryptage pour l'image du cerveau, 19,9
du temps de cryptage et 22,8du temps de décryptage pour l'image du cancer du sein.

÷ Les deux algorithmes ont également été testés sur un ensemble de 26 images IRM de la cuisse de 12 bits. Ces images ont été complétées avec des zéros à 16 bits avant le cryptage.
La figure 3.35 représente l'image de cuisse originale, et l'image cryptée par AES et cryptée par CAT-AES avec leurs histogrammes respectifs.

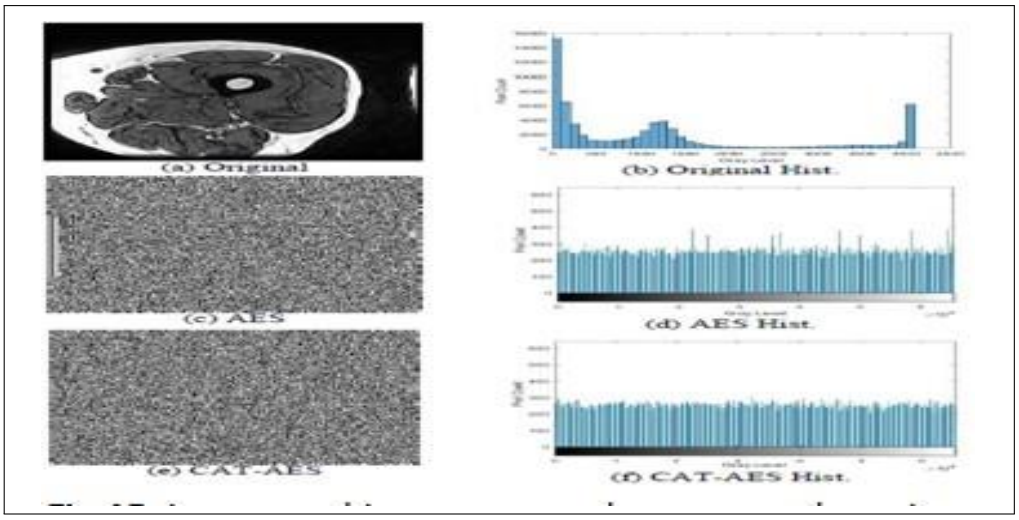


FIGURE 3.35 – images et histogrammes de cryptage des cuisses

## Système de cryptage et de compression d'images médicales utilisant la détection par compression et l'approche de per- mutation basée sur l'échange de pixels (2015)

Li-bo Zhang,Zhi-liang Zhu, Ben-qiang Yang, Wen-yuan Liu, Hong-feng Zhu et Ming- yu Zou proposent un schéma pour crypter et compresser l'image médicale en utilisant une approche de permutation basée sur la détection compressive (CS) et l'échange de pixels[51].

**Principe**

L'ensemble du processus de cette méthode se compose de deux étapes :

- **1er étape :** la procédure CS basée sur le chaos qui est utilisée pour compresser et fournir la protection de premier niveau.
- **2ème étape :** est un module de cryptage par permutation-diffusion basé sur le chaos. Dans la phase CS, l'image simple est compressée et cryptée par la matrice de mesure de Bernoulli basée sur le chaos, qui est générée sous le contrôle de la carte de Chebyshev introduite. Les mesures quantifiées sont ensuite chiffrées par un chiffrement chaotique de type permutation-diffusion pour la protection de second niveau.
  Le schéma du système de cryptage et de compression d'images médicales proposé est illustré à la figure 3.36.

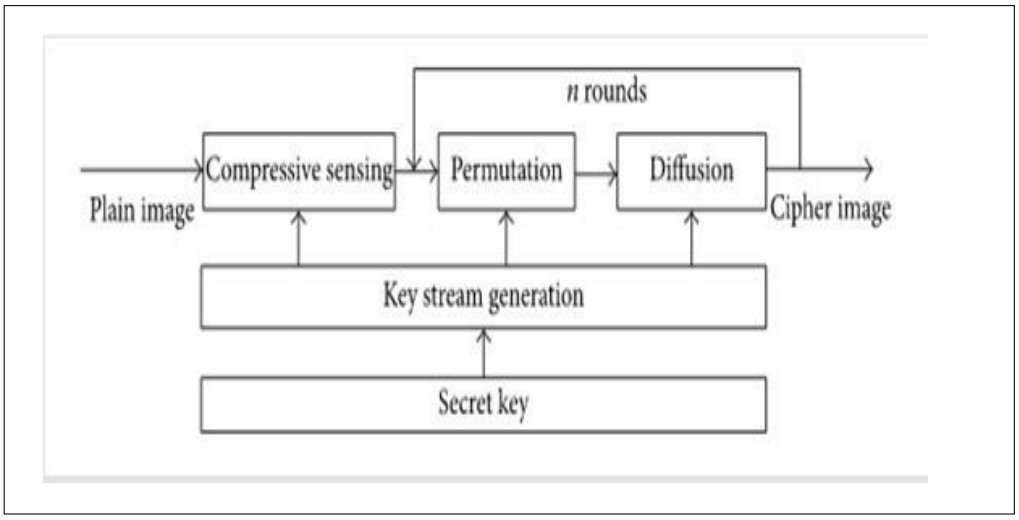


FIGURE 3.36 – le schéma du système proposé

**Résultats**

÷ Quatre images médicales de taille 512 * 512 sont utilisées, nommées respectivement CT Abdomen, CT Paranasal Sinus, MR Knee et X Lungs.

÷ La figure 3.37 illustre les histogrammes des images originales et des images cryptées.

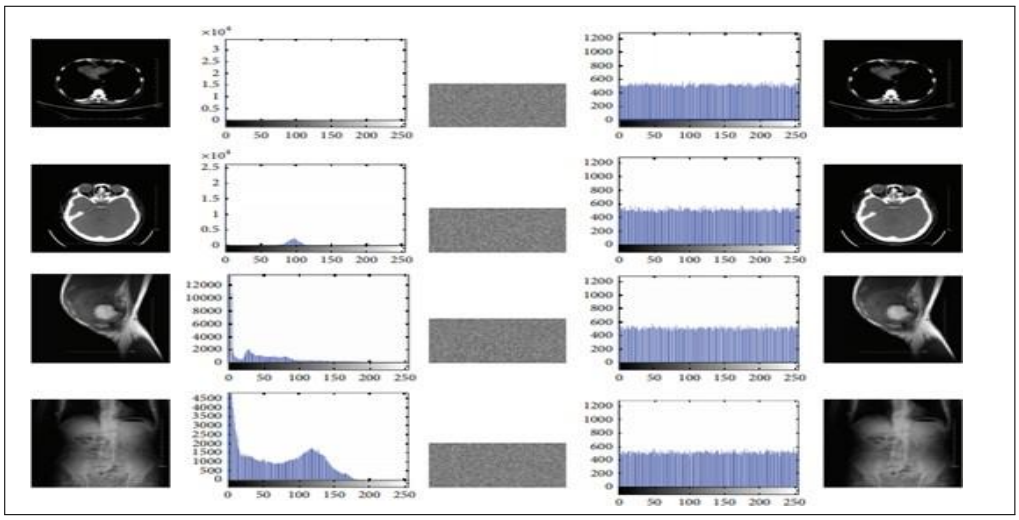

FIGURE 3.37 – Résultats de simulation du schéma proposé : de la première à la cinquième colonne sont respectivement le texte en clair, l'histogramme du texte en clair, le texte chiffré, l'histogramme du texte chiffré et les images récupérées.

÷ La figure 3.38 représente le graphique PSNR de différents taux de compression. Où on peut voir que le PSNR peut dépasser 30 dB lorsque le taux de compression est supérieur à 0,3.

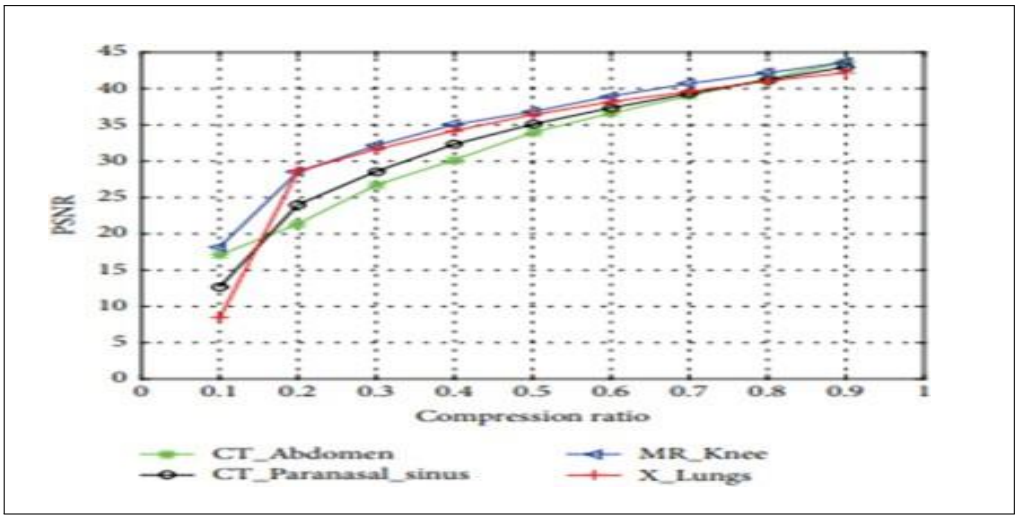


FIGURE 3.38 – Graphique PSNR des différents taux de compression.

÷ La figure 3.39 représente Les coefficients de corrélation des pixels adjacents dans l'image simple et son image chiffrée.

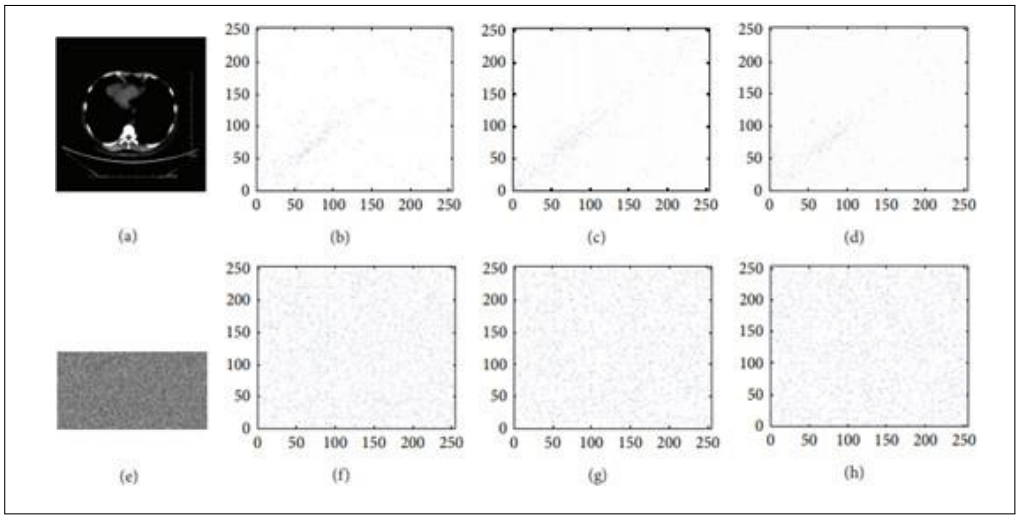


FIGURE 3.39 – Tracés de corrélation de deux pixels adjacents : (a) image simple, tracés de corrélation de l'image simple dans les directions (b) horizontale, (c) verticale, (d) et diagonale ; (e) image chiffrée, tracés de corrélation de l'image chiffrée dans les directions (f) horizontale, (g) verticale, (h) et diagonale..

÷ le tableau 3.40 représente l'entropie d'images médicales et d'images chiffrées les entro- pies des images chiffrées sont très proches de la valeur théorique de 8, ce qui signifie que la fuite d'informations dans la procédure de chiffrement est négligeable et que le crypto-système proposé est sécurisé contre les attaques par entropie.

| Test images | Plain images | Cipher images |
|---|---|---|
| CT_Abdomen | 1.675035 | 7.9983 |
| CT_Paranasal_sinus | 3.328586 | 7.9986 |
| MR_Knee | 5.384937 | 7.9984 |
| X_Lungs | 6.966350 | 7.9986 |

FIGURE 3.40 – entropies d'images simples et d'images chiffrées

## Cryptage d'images médicales utilisant le brouillage à grande vitesse et la diffusion adaptative des pixels (2017)

Z.Hua, S. Yi et Y.Zhou proposent un nouveau système de cryptage de protection des images médicales basée sur le brouillage à grande vitesse et la diffusion adaptative des pixels. Tout d'abord, certaines données aléatoires sont insérées dans l'environnement de l'image[52].

Ensuite, deux cycles de brouillage à grande vitesse et de diffusion adaptative de pixels sont effectués pour mélanger de manière aléatoire les pixels voisins et répartir ces données aléatoires insérées sur toute l'image. Le schéma de cryptage proposé peut être directement appliqué aux images médicales avec n'importe quel format de représentation. Il existe deux types d'opérations pour implémenter la diffusion adapta- tive des pixels : XOR bit à bit (BX) et arithmétique modulo (MA). Le premier a une efficacité élevée dans les plates-formes matérielles, tandis que le second peut atteindre une vitesse rapide dans les plates-formes logicielles.
Le schéma de chiffrement proposé utilisant BX est appelé MIE-BX et celui utilisant MA est appelé MIE-MA.

÷ **Principe**

La figure 3.41 représente le schéma de chiffrementdans laquelle la clé secrète K a une longueur de 256 bits.

- ÷ La distribution declé consiste à décomposer la clé secrète pour obtenir des sous- clés pour le brouillage et la diffusion pour cela Le système Logistic-Sine (LSS) proposé est utiliséet est désigné par LSS-PRNG.
- ÷ Les opérations de brouillage et de diffusion consistent à mélanger de manière aléatoire les positions des pixels (Il modifie simultanément les positions des lignes et des colonnes des pixels)et à changer les valeurs des pixels, respectivement.

÷ L'insertion de données aléatoires consiste à ajouter des valeurs aléatoires aux environs de l'image. Cela peut garantir que le résultat chiffré de chaque exécution de schéma de chiffrement est unique et différent, même lorsque vous utilisez une même clé sécurisée pour chiffrer plusieurs fois une image identique.

÷ Ce schéma de cryptage proposé utilise deux tours.

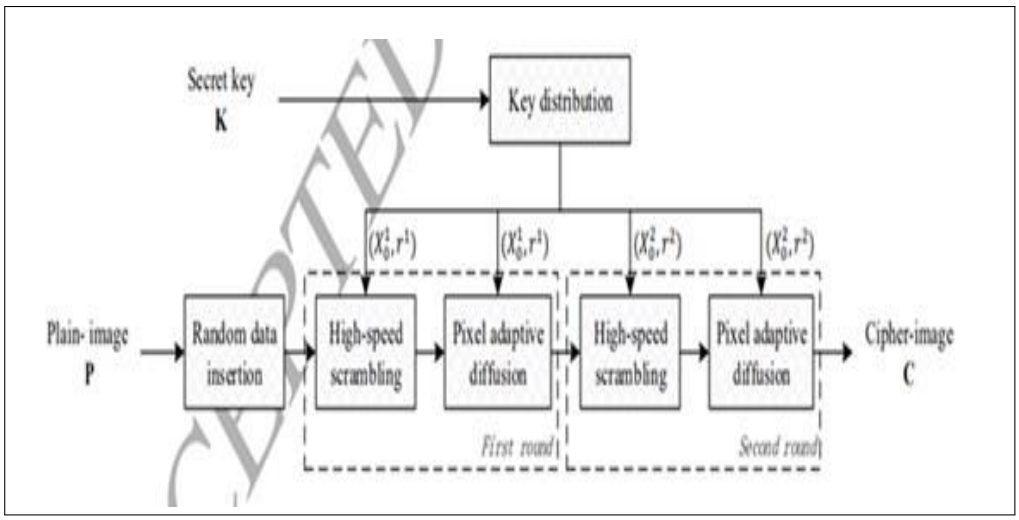


FIGURE 3.41 – Structure du schéma de cryptage d'images médicales proposé.

÷ **Résultats**

÷ Les figures 3.42 montre les procédures de cryptage de MIE-BX et MIE-MA pour des images médicales 8 bits, 16 bits et 24 bits, respectivement. Pour les images médicales 16 bits, il faut transforme linéairement leurs valeurs de pixels dans la plage [0, 255].

Pour les histogrammes d'images médicales 24 bits, une image médicale24 bits est divisée en trois images 8 bits, puis calculer les histogrammes de ces images 8 bits.

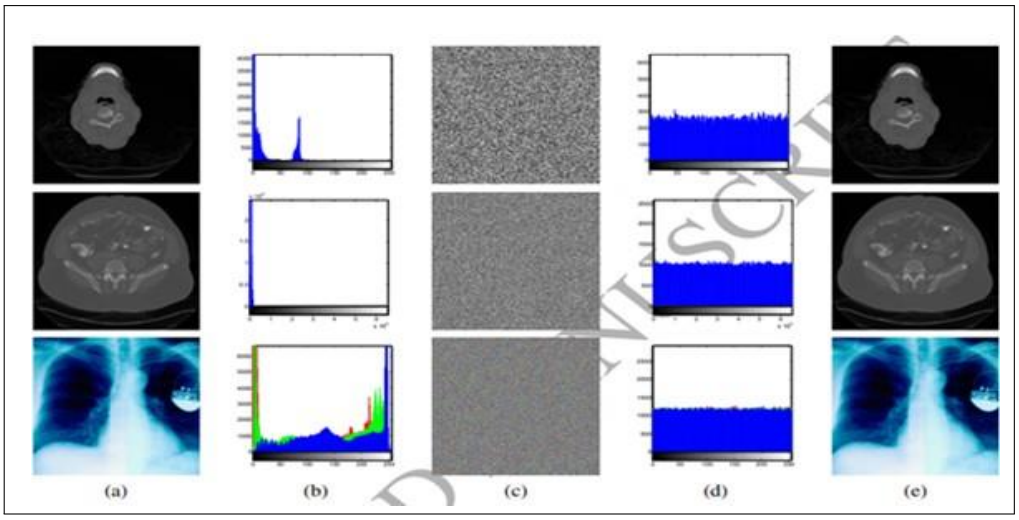


FIGURE 3.42 – Résultats de simulation de MIE-BX. Les images de haut en bas sont des images 8 bits, 16 bits et 24 bits. (a) Images simples ; (b) les histogrammes de (a) ; (c) des images chiffrées ; (d) histogrammes de (c) ; (d) images déchiffrées.

÷ La figure 3.43 montre les vitesses moyennes de cryptage et de décryptage de différents schémas de cryptage pour une image de différentes tailles.MIE-MA peut atteindre une vitesse beaucoup plus rapide que d'autres systèmes.

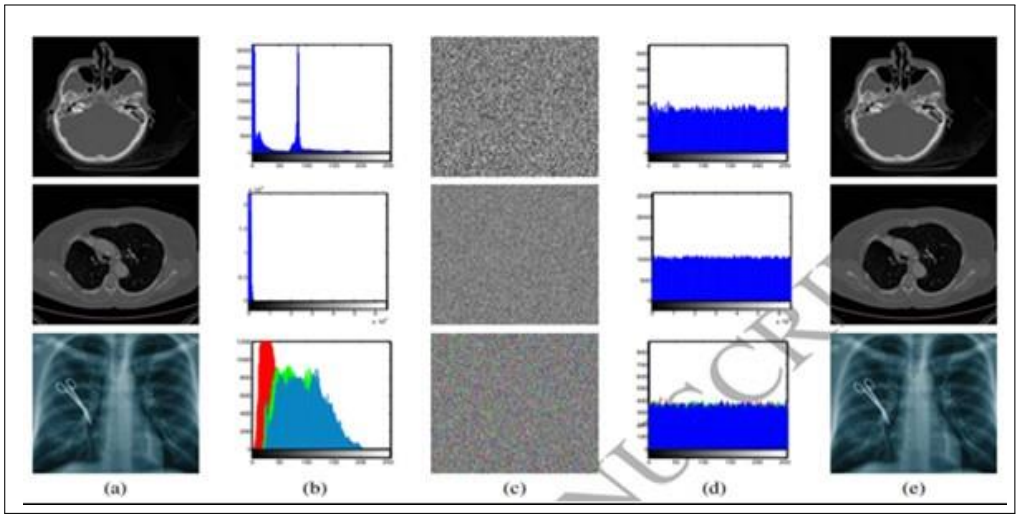


FIGURE 3.43 – Résultats de simulation de MIE-MA. Les images de haut en bas sont des images 8 bits, 16 bits et 24 bits. (a) Images simples ; (b) les histogrammes de (a) ; (c) des images chiffrées ; (d) histogrammes de (c) ; (d) images décryptées.

÷ le tableau illustre les entropies d'information de ces images simples et de ces images chiffrées.

| | MIE-BX | | | MIE-MA | | |
|---|---|---|---|---|---|---|
| | 8-bit | 16-bit | 24-bit | 8-bit | 16-bit | 24-bit |
| Plain-images | 4.2051 | 5.6775 | 6.3962 | 5.2431 | 5.7915 | 6.8723 |
| Cipher-images | 7.9977 | 7.9994 | 7.9981 | 7.9969 | 7.9994 | 7.9965 |

FIGURE 3.44 – Les entropies d'information de différentes images simples et leurs images chiffrées cryptées par MIE-BX et MIE-MA. Pour toutes les images 8 bits, 16 bits et 24 bits, 256 bits sont utilisés.

÷ la figure 3.45 montre leurs vitesses moyennes de cryptage et de décryptage de vingt images 8 bits, 16 bits, 24 bits et 32 bitsen fixant la taille de l'image à 512*512.

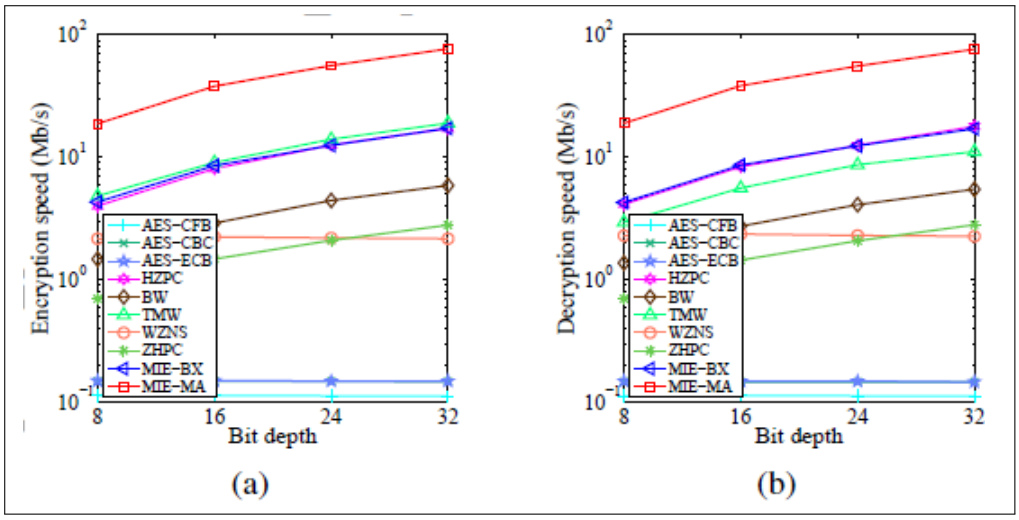


FIGURE 3.45 – Vitesses moyennes des différents schémas de cryptage par rapport à la taille de l'image : (a) vitesse de cryptage; (b) vitesse de décryptage..

**Autre méthode**

Plusieurs autres algorithmes de chiffrement d'image médicale existant ont été proposés :

÷ T.Amina , B.Zahia, B.Hamid, F. MOSTEFAI, M.K. Kholladi proposent Une nou- velle technique de chiffrement sélectif appliquée au flux JPEG 2000 des images médicales. L'algorithme de chiffrement AES (Advanced Encryption System) en mode CFB (Cipher FeedBack) associé à une étape de permutation est appliqué à

un certain nombre de codes blocks sélectionné du flux compressé. L'idée de combiner la permutation et le chiffrement est de minimiser au maximum la quantité de données à crypter tout en assurant un niveau de sécurité adéquat. A cet effet, le chiffrement de moins de 15des données suffit pour obtenir un niveau de sécurité satisfaisant avec une dégradation visuelle accentuée.

- B. Mustapha, R.Yasser, and Mohamed Salah Azzaz présentent une étude comparative entre deux approches de cryptage à savoir les courbes elliptiques (ECC) et le chaos. C'est la première fois qu'une comparaison entre un cryptage symétrique basé sur le chaos et un cryptage asymétrique basé sur la CEE est introduite pour la protection des images médicales. Les résultats obtenus montrent que Les deux techniques ont de bonnes compétences en matière de sécurité. En effet, l'approche basée sur le chaos présente une implémentation simple et un bon temps d'exécution. En revanche, l'approche ECC est basée sur le problème du logarithme discret, difficile à casser mais qui reste très coûteuse en termes de temps d'exécution lié à l'étape d'encodage des données, qui prend suffisamment de temps.

Les résultats obtenus montrent que Les deux techniques ont de bonnes compétences en matière de sécurité. En effet, l'approche basée sur le chaos présente une implémentation simple et un bon temps d'exécution. En revanche, l'approche ECC est basée sur le problème du logarithme discret, difficile à casser mais qui reste très coûteuse en termes de temps d'exécution lié à l'étape d'enco- dage des données, qui prend suffisamment de temps.

- S.S.Moafimadani, Y. Chen et C.Tang proposent un nouvel algorithme basé sur des systèmes chaotiques et des systèmes SHA-256 pour protéger les images couleur médicales contre les attaques. Cet algorithme comporte deux parties principales :

un processus de permutation à grande vitesse et une diffusion adaptative, qui conduisent à une approche très efficace et fiable à cet égard.

**Analyses et critiques :**

Après avoir vu quelques travaux de cryptage d'images médicales, Nous avons fait un résumé complet.

Le cryptage sélectif d ?image médicale par AES en mode par flot OFB et compression JPEG fournit un niveau de confidentialité acceptable pour le transfert d'images médicales avec visualisation rapide à distance en temps réel puisque il est chiffrer qu'un petit nombre des bits des images médicales (entre 5 et 30 ). Les résultats appliqués sur des images médicales ont montré que cette méthode masquant bien l'information parce que le PSNR est inferieur a 30 d B. Le cryptage d'images médicales à l'aide de cartes de bord est un processus sans perte. Il y a deux méthodes basées sur les cartes de bord qui sont EdgeCrypt et EMMIE. L'histogramme de l'image chiffrée par la méthode EdgeCrypt a une distribution non uniforme. D'autre part, l'histogramme d'EMMIE se dis- tribue presque également ce qui démontre que la distribution de l'histogramme d'EMMIE à une performance meilleure que méthode d'EdgeCrypt.Le temps de

cryptage d'EMMIE est dessinée de 0,0129 à 1,846 secondes avec différentes tailles d'image, ce qui est inférieur aux EdgeCrypt. Par conséquent, la vitesse d'EMMIE est plus rapide qu'EdgeCrypt. La méthode EdgeCrypt peut également crypter d'autres types d'images telles que des images en couleur. EMMIE possède une corrélation de pixels plus élevée, une sensibilité de clé et une robustesse aux erreurs plus fortes, et une meilleure performance contre les attaques différentielles avec moins de temps.

Le cryptage basé sur l'arrangement des pixels et la permutation aléatoire ne nécessite aucune manipulation mathématique contrairement aux méthodes mentionnées précédemment. Cette fonctionnalité est particulièrement très utile pour l'image médicale où l'image peut être très grande. Cet algorithme ne fonctionne qu ?une image non compressée. Dans les images compressées ce schéma n'est pas applicable. Le temps de calcul pour le cryptage et le décryptage de chaque image implémenté ne dépasse pas 1.333 seconds.

L'algorithme de cryptage d'images médicales basé sur la séquence d'ADN utilise la transformation affine qui rendre le schéma résistant à de nombreuses attaques. En outre, la plupart des algorithmes mentionnésprécédemment utilise un espace de clé plus grand ce qui confirme que le système proposé à une sécurité plus

élevée contre les attaques par force brute.

L'algorithme CAT-AES a généralement bien performé sur les ensembles d'images médicales expérimentés par rapport à l'algorithme qui utilise S-AES. Ce dernier utilise le chaos dans les procédures de brouillage et de cryptage contrairement

à l'algorithme CAT-AESqui utilise le chaos seulement dans les procédures de brouillage. D'autre part, les deux algorithmes ont pris plus de temps en raison de l'étape supplémentaire de la carte de chat. L'histogramme de l'algorithme CAT-AES est plus uniforme et plus régulière comparé à l'algorithme de S-AES. Ce qui signifie que l'algorithme CAT-AES vaincre les attaques statistiques.

Les histogrammes de la méthode qui utilise CS avec permutation basée sur l'échange de pixels sont uniformément répartis, ce qui indique que la redondance de l'image simple a été masquée avec succès après le cryptage et ne fournit par conséquent aucun indice pour appliquer des attaques statistiques.

Le cryptage en utilisant un brouillage à grande vitesse et une diffusion adaptative des pixels est protéger les images médicales;Il a un niveau de sécurité élevé car il peut crypter une image identique en différentes images chiffrées, même en utilisant la même clé secrète ; et à une vitesse plus rapide et une meilleure robustesse que plusieurs schémas de cryptage typiques.Ce cryptage utilise deux types d'opérations pour implémenter la diffusion adaptative des pixels : XOR

bit à bit et arithmétique modulo. Le premier a une efficacité élevée dans les plates-formes matérielles, tandis que le second peut atteindre une vitesse rapide dans les plates-formes logicielles.

# Outils élémentaires d'analyse d'un algo- rithme du cryptage d'image (mesures de perfor- mance)

## Espace de clés

La taille de l'espace de clé est le nombre de paires de clés de cryptage/décryptage qui sont disponibles dans le système de chiffrement [53], elle est nécessaire pour assurer la sécurité contre l'attaque par force brute.

## La corrélation entre les pixels adjacents

La corrélation est une technique qui permet de comparer deux images pour es- timer 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 [1].

## L'histogramme

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 graphique- ment en utilisant 256 chiffres indiquant la distribution des pixels entre ces valeurs de niveaux de gris [54]. 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 [1].

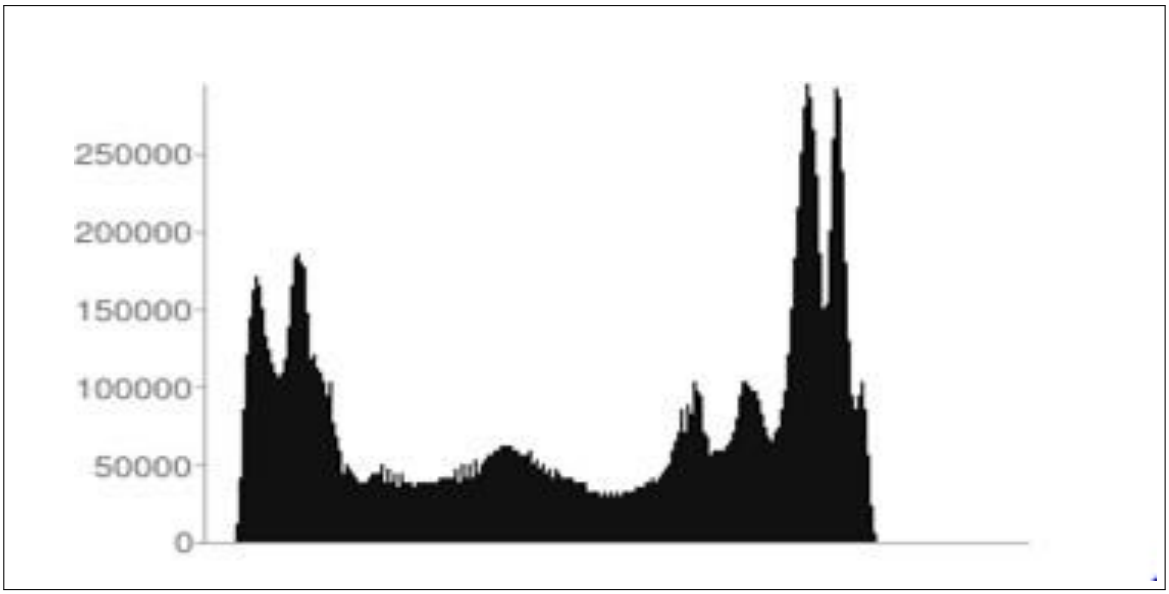


FIGURE 3.46 – Histogramme d'une image niveau de gris [55]

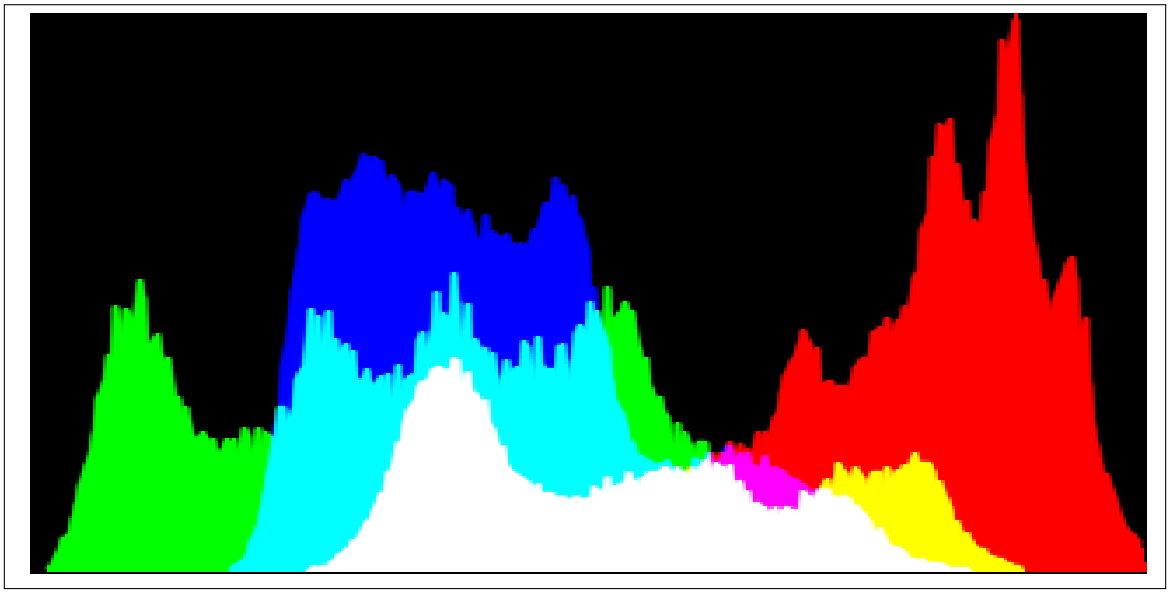

FIGURE 3.47 – Histogramme d'une image couleur [56]

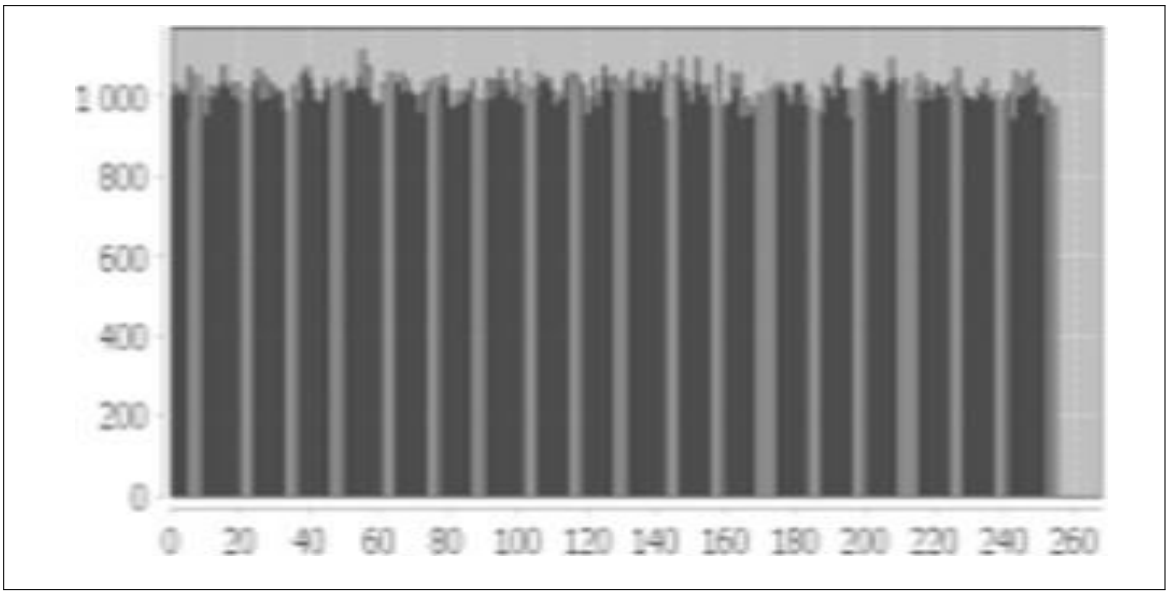


FIGURE 3.48 – Histogramme d'une image chiffrée [57]

## L'entropie

Selon la théorie de Shannon [58], 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 [59]. 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. 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.

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

# Conclusion

Dans ce chapitre, nous avons présenté les techniques existantes pour chiffrer l'image médicale et leurs résultats.

Dans le prochain chapitre, nous allons implémenter les algorithmes RSA, AL Gamal et un algorithme basé sur les courbes elliptiques.