République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université Ahmed Draia - Adrar

Faculté des Sciences et de la Technologie

Département des Mathématiques et Informatique

Mémoire de fin d'étude, en vue de l'obtention du diplôme de Master en informatique Option : Réseaux et Systèmes Intelligents

Thème

Proposition d'un algorithme de chiffrement d'image

Préparés par

AKEDI Fatma et ELAZZAOUI Noura

Encadré par

Dr. TOUABI Abdelkader

Président : Dr. OMARI

Examinateur1:Mr. RABHI

Examinateur2:Mr. OUAHAB

Année Universitaire 2016/2017

Résumé

La cryptographie a contribué (cryptage) depuis l'antiquité à la réussite des opérations militaires en fournissant des moyens pour permettre le contenu des messages pour se cacher, même si est tombé entre les mains de l'ennemi. Les techniques de chiffrement dans l'ère actuelle des techniques nécessaires pour sécuriser les communications numériques en se basant sur la conversion capable mutuelle de données numériques en regard d'information pour ceux qui ne peuvent pas être reçus par hasard compris qu'après avoir obtenu les systèmes clés de chiffrement. L'objectif principal de notre projet est le choix et la comparaison les différents algorithmes symétriques de cryptage dans plusieurs façons utilisés pour le chiffrement et la protection des images. D'après les résultats obtenus avec les différentes comparaisons effectuées on a conclu que les algorithmes RC6 puis RC5 sont plus performants en termes déviation d'histogramme pour mode ECB, déviation irrégulière pour mode CFB, et NPCR et UACI pour mode ECB. Cet algorithme est faible par rapport les autres algorithmes pour les métriques vitesses de cryptage, coefficient de corrélation et PSNR. On peut dire aussi que l'algorithme RC5 était mieux efficace pour le cas du coefficient de corrélation pour les modes à l'exception ECB. Tandis que l'algorithme XOR il était mieux efficace pour PSNR pour les modes ECB et CFB à RC5 et RC6 , vitesse de cryptage, Coefficient de corrélation pour mode ECB à RC5 et RC6, déviation irrégulière pour mode ECB à RC5 et RC6 et meilleur mode est CFB qui donne toujours les meilleurs résultats à la différence de mode ECB qui donne toujours les pires résultats.

Mots des clés : cryptographie, clé symétrique, RC5, RC6, XOR,

Abstract

Cryptography has contributed (encryption) from antiquity to the success of military operations by providing means to allow the content of messages to hide even if fell into the hands of the enemy. The techniques of encryption in the current era of the techniques necessary to secure digital communications based on the mutually capable conversion of digital data against information for those who can not be received by chance understood only after having obtained the Key encryption systems. The main objective of our project is the choice and comparison of different symmetric encryption algorithms in several ways used for encryption and protection of images. From the results obtained with the various comparisons made, it was concluded that the RC6 and then RC5 algorithms are more efficient in terms of histogram deviation for ECB mode, irregular deviation for CFB mode, and NPCR and UACI for ECB mode. This algorithm is weak compared to the other algorithms for the encryption speed, correlation coefficient and PSNR metrics. It can also be said that the RC5 algorithm was more efficient for the case of the correlation coefficient for the modes with the exception of ECB. While the XOR II algorithm was more efficient for PSNR for ECB and CFB modes to RC5 and RC6, encryption speed, Correlation coefficient for ECB mode to RC5 and RC6, Irregular deviation for ECB mode to RC5 and RC6 and best mode is CFB which always gives the best results at the ECB difference which always gives the worst results.

Keyword: cryptography, symmetric key, RC5, RC6, XOR,

ملخص

ساهم الترميز (التشفير) من العصور القديمة إلى نجاح العمليات العسكرية من خلال توفير وسائل للسماح لمحتوى الرسائل بالإختباء، حتى لو سقطت في أيدي العدو. وتعتبر تقنيات التشفير في العصر الحالي من التقنيات اللازمة لتأمين الاتصالات الرقمية على أساس متبادل قادرة تحويل البيانات الرقمية فيما يتعلق بالمعلومات بالنسبة لأولئك الذين لا يمكن أن تلقى شملت بطريق الخطأ بعد الحصول على أنظمة تشفير المفتاح. والهدف الرئيسي من مشروعنا هو اختيار ومقارنة مختلف خوارزميات التشفير متناظرة تستخدم في العديد من الطرق لتشفير وحماية الصور. ومن خلال الدراسة المقارنة التي قمنا بها خلصنا إلى أن الخوارزميات RC6 يليه RC5 هي أكثر كفاءة من حيث المقياس(histogram deviation) بالنسبة لنسق ECB ، (Déviation irrégulière) بالنسبة لنسقCFB ، وNPCR وUACI. هذه الخوارزمية منخفضة مقارنة مع خوارزميات أخرى لسرعات التشفير ، معامل الارتباط و.PSNR يمكن القول أيضا أن الخوارزمية RC5 كانت أكثر فعالية في حالة معامل الارتباط ماعدا النسق ECB. في حين أن الخوارزمية XOR كانت أفضل فعالية من حيث PSNR بالنسبة لنسقين ECB و CFB وسرعة التشفير ، معامل الارتباط لنسق ECB ل RC5 وRC6، وأفضل نسق هو CFB يعطي أفضل النتائج دائما عكس ECB .

الكلمات المفتاحية: الترميز، مفتاح متماثل، RC5، RC6، XOR.

Remerciements

Le Messager d'Allah, paix soit sur lui dit : **«لَا يَشْكُرُ اللّٰهَ مَنْ لَا يَشْكُرُ النَّاسَ»**

En préambule à ce mémoire, nous souhaitent adressons nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année universitaire. Nous adressons nos sincères remerciements à nos parents qui ont f ait la fête sur notre éducation et notre éducation et à M. le ***Dr. TAOIBI Abd-El-Kader****, qui, en tant que encadreur de mémoire, s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration, l'aide et le temps qu'elle a bien voulu nous consacrer et sans qui ce mémoire n'aurait jamais vu le jour.*

Nous exprimons également notre gratitude à nos valeurs, nos enseignants qui aidez-nous dans cette note en particulier le ***Dr. OMARI Mohammed,*** *le* ***Dr. KOUHILLI Mohammed, le CHARRAGUI Mohammed Amine,*** *la camarade* ***BOTTADARAH Nadia*** *et toute les professeurs et les étudiants de faculté des Sciences et de Technologie surtout département Mathématiques et Informatique.*

Nous tenons à la fin de ce travail à remercier ALLAH le tout puissant de nous avoir donné la foi et de nous avoir permis d'en arriver là.

Dédicace

Je dédie cette humble à ceux qui étaient la cause de mon travail de la vie:

Au printemps tendresse qui Fatiguésur mon éducation et de l'éducation mes chers mères.

Pour la couronne de ma tête qui a planté ne récoltera Dieu précieux fait le lieu de repos du paradis : mon cher père.

Pour un jumeau spirituel, qui m'a soutenu financièrement et moralement ne pas lui écrire pour assister à la fin, mon mari bien-aimé et la miséricorde de Dieu soient sur Jmni dans le paradis éternel de Dieu.

A tous sœurs et mes frères Aïcha, Marieme, Abd al-Rahman et Ahmed.

A mes frères qui ai gagné-je: Ma sœur Djamaa, Lamia et NourEddine.

Pour les enfants de ma sœur et mes bénédictions de frères Ambarka, Nariamane, Farouk, Fatima Zahra, Boudjamaa, Ghassan, Retaj » et M'hamed Salem.

A mes oncles et tantes et oncles et leurs familles surtout oncle Boudjamaa et sa femme et ses enfants et oncle Salah.

A mes amis : Fatima, Aïcha, Warda, Achoura, Zohra, Malika et Mabrouka.

A mon collègue et ma binôme qui partageait mes recherches ce Nora en conséquence Dieu payé vers le bas.

Pour tous mes camarades de classe dans l'étude, les enseignants et les professeurs, et tout les familles AKEDI, FATHI, HADJOUB, et AZOI.

Fatma

Dédicace

Toutes les lettres ne sauraient trouver les mots qu'il faut. Tous les mots ne sauraient exprimer la gratitude, le respect, la reconnaissance…

je dédie ce mémoire à nous chers parents qui n'ont épargné aucun effort pour nous soutenir depuis le début de nos études jusqu'à leur fin.

A tous mes sœurs : Zohra, Fatima, Hajjar, et Widad

A tout mes frères : Abd-Allah, Nour Adinne, Attahar, Kacem, Hamza, Touffik.

A les enfants de mes sœur et de mon frères Ilyass, Yazid, Souhilla, Serrine, Noura.

A mes oncles et tantes et leurs familles.

A mon collègue et ma binôme qui partageait mes recherches

ce Fatma en conséquence Dieu payé vers le bas.

A tous mes amis et mes collègues. A touts les familles ELAZZAOUI, HAFSSI, HAMMED LAMINE , LAMCHEACHEA , ABD ALAOUI...

A tous mes amis Iman, Hajjar, Khayra ,Sara…

Pour tous mes camarades de classe dans l'étude, les enseignants et les professeurs.

Noura

Sommaire

Chapitre 02: Méthode de protéger des images

Chapitre 03: Les algorithmes retenus

Liste des figures

Liste des tableaux

Introduction générale

Aujourd'hui, le monde connait un grand développement dans tous les domaines(le domaine culturel, social, et économique…) surtout le domaine de l'informatique.

Ce qui a mené vers la création de beaucoup des appareils et des programmes pour faciliter l'échange des idées et des opinions concernant les documents secrets tel que les textes, les vidéos, et les images.

Le problème qui se pose pour ce la comment protéger toutes ces sortes de documents ?

Dans notre mémoire, on va se baser sur une sorte seulement c'est la protection des images.

On a plusieurs méthodes pour sécurité et protégé les images comme stéganographie, watermarking, et cryptographie.

On va traiter le cryptage en comparant trois algorithmes suivants : XOR, RC5, et RC6.

Le cryptage demande l'existence de la clé ainsi les modes pour suggérer une meilleure méthode du cryptage.

Dans cette recherche, nous étudierons les algorithmes de comparaison (XOR, RC5 , et RC6) avec clé symétrique.

Ce mémoire est organisé en quatre chapitres:

Dans le premier chapitre, nous présenterons la traitement des images , le deuxième chapitre comporte les méthode de protéger des images, , le troisième chapitre contient Les Algorithmes retenu, et le quatrième

chapitre, comporte une Etude comparative entre les algorithmes de cryptographie selon sept métriques il est suivant :

Déviation d'histogramme, coefficient de corrélation, déviation irrégulière, NPCR, UACI, la durée de cryptage et de décryptage et la vitesse, et PSNR.

Chapitre 1

Traitement des images

1.1. Introduction [01]

Le traitement d'images est une discipline de l'informatique et des mathématiques appliquées qui étudie les images numériques

On distinguer par traitement d'images numériques l'ensemble des techniques permettant de modifier une image numérique dans le but de l'améliorer ou d'en extraire des informations ou sont inchangées dans le but de protection.

1.2. Définition d'une image [02]

Qu'est-ce qu'une image ?

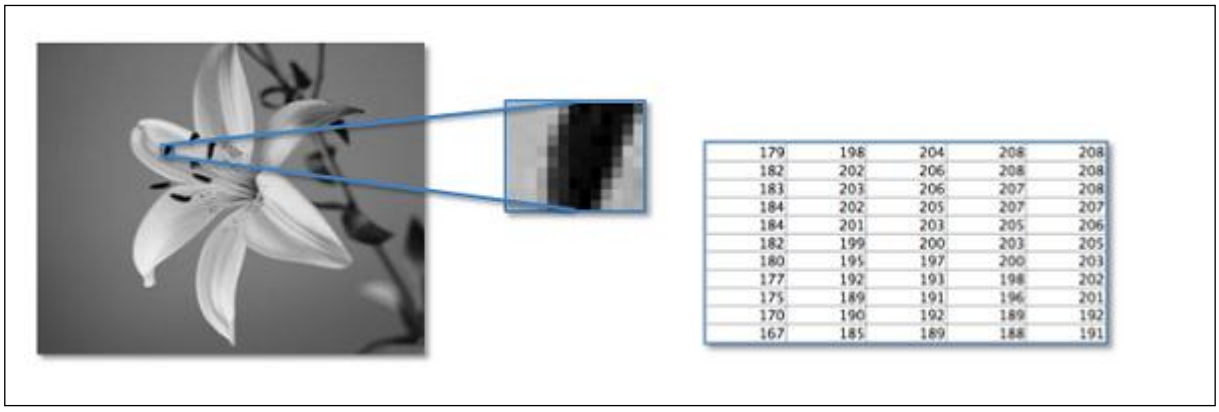


Figure 1.1 : Vision discrète [02]

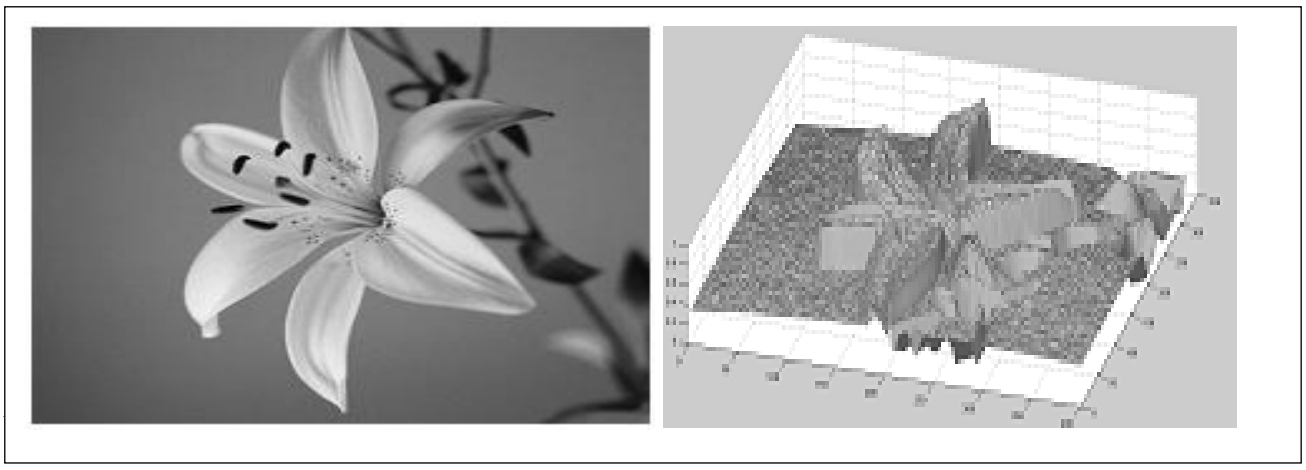


Figure 1.2 : Vision surfacique [02]

Une image est représentée :

- par fonction continue f (x, y), x, y ∈ R ;
- par une fonction numérique f (i, j) (ou f (n, m)), i, j ∈ N (n, m ∈ N) et f ∈ N+, après numérisation.

Image analogique → image numérique : numérisation en deux étapes :

1. échantillonnage spatial : discrétisation des coordonnées de l'image réelle ;
2. quantifications des luminances : discrétisation des intensités de l'image réelle.

Une image numérique est composée d'un ensemble fini d'éléments, appelés Picture élément, ou pixels.
Après échantillonnage spatial : notations

- N le nombre de lignes de l'image ;
- M le nombre de colonnes de l'image ;
- (i, j) les coordonnées spatiales d'un élément de l'image (ligne i, colonne j) ;
- fj (i), ou encore f (i), la ligne i ;
- fi (j), ou encore f (j), la colonne j.

Après quantification : notations

- f (i, j) l'amplitude en du pixel (i, j) ;
- k (ou f) un niveau de gris ;
- m le nombre de bits sur lesquels est codée la valeur d'un niveau de gris ;
- L la dynamique de l'image, soit l'étendue des valeurs qu'un pixel peut prendre.

Alors, L = 2m, donc k ∈ [0,…. 2m-1]

Représentation d'une image numérique

Représentation matricielle :

- Représentation lexicographique de l'image, soit une matrice

f = [0, . . ., N − 1] × [0, . . ., M − 1]

- La largeur de l'image est donnée par le nombre de colonnes M de f,

Sa hauteur par le nombre de lignes N

- Le pixel au croisement de la ligne i et de la colonne j est désigné par f (i, j)
-

Représentation vectorielle :

- Les lignes de l'image sont juxtaposées de manière à former un

Vecteur v = $[0, . . ., M \times N - 1]^t$

Le pixel (i, j) correspond à la composante v = $[0, . . ., M \times N - 1]^t$

1.3. Les représentations de la couleur [01]

Pour pouvoir manipuler correctement des couleurs il est nécessaire de disposer de moyens permettant de les catégoriser et de les choisir. Ainsi, il n'est pas rare d'avoir à choisir la couleur d'un produit avant même que celui-ci ne soit fabriqué. Dans ce cas, une palette de couleurs nous est présentée, dans laquelle nous choisissons la couleur convenant le mieux à notre envie ou notre besoin. La plupart du temps le produit (véhicule, bâtiment, ...) possède une couleur qui correspond à celle que l'on a choisie.

En informatique, de la même façon, il est essentiel de disposer d'un moyen de choisir une couleur parmi toutes celles utilisables. Or la gamme de couleur possible est très vaste et la chaîne de traitement de l'image passe par différents périphériques : par exemple un numériseur (scanner), puis un logiciel de retouche d'image et enfin une imprimante. Il est donc nécessaire de pouvoir représenter faiblement la couleur afin de s'assurer de la cohérence entre ces différents périphériques.

On appelle ainsi espace de couleurs la représentation mathématique d'un ensemble de couleurs. Il en existe plusieurs, parmi lesquels les plus connus sont :

1.3.1. Le codage RGB

Le codage RGB correspond à la façon dont les couleurs sont codées informatiquement, ou plus exactement à la manière dont les tubes cathodiques des écrans d'ordinateurs représentent les couleurs. Il consiste à affecter une valeur à chaque composante de Rouge, de Vert et de Bleu.

Ainsi, le modèle RGB propose de coder sur un octet chaque composante de couleur, ce qui correspond à 256 intensités de rouge (28), 256 intensités de vert et 256 intensités de bleu, soient 16777216 possibilités théoriques de couleurs différentes, c'est-à-dire plus que ne peut en discerner l'œil humain (environ 2 millions). Toutefois, cette valeur n'est que théorique car elle dépend fortement du matériel d'affichage utilisé.

Etant donné que le codage RGB repose sur trois composantes proposant la même gamme de valeur, on le représente généralement graphiquement par un cube dont chacun des axes correspond à une couleur primaire :

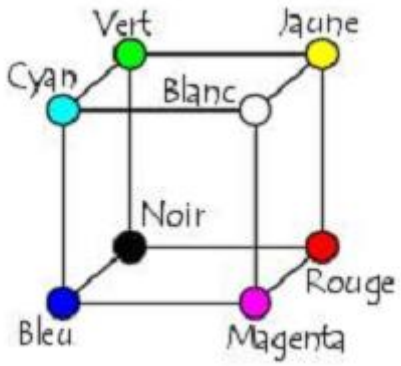


Figure 1.3 : Représentation graphique du codage RGB [01]

1.3.2. Le codage HSL

Le modèle HSL (Hue, Saturation, Luminance, ou en français TSL), s'appuyant sur les travaux du peintre Albert H.Munsell (qui créa l'Atlas de Munsell), est un modèle de représentation dit " naturel ", c'est-à-dire proche de la perception physiologique de la couleur par l'œil humain. En effet, le modèle RGB aussi adapté soit-il pour la représentation informatique de la couleur ou bien l'affichage sur les périphériques de sortie, ne permet pas de sélectionner facilement une couleur.

En effet, le réglage de la couleur en RGB dans les outils informatiques se fait généralement à l'aide de trois glisseurs ou bien de trois cases avec les valeurs relatives de chacune des composantes primaires, or l'éclaircissement d'une couleur demande d'augmenter proportionnellement les valeurs respectives de chacune des composantes. Ainsi le modèle HSL a-t-il été mis au point afin de pallier à cette lacune du modèle RGB.

Le modèle HSL consiste à décomposer la couleur selon des critères physiologiques:

– La teinte (en anglais Hue), correspondant à la couleur de base (T-shirt mauve ou orange),

– La saturation, décrivant la pureté de la couleur, c'est-à-dire son caractère vif ou Terne (T-shirt neuf ou délavé),

– La luminance, indiquant la brillance de la couleur, c'est-à-dire son aspect clair ou sombre (T-shirt au soleil ou à l'ombre).

Voici une représentation graphique du modèle HSL, dans lequel la teinte est représentée par un cercle chromatique et la luminance et la saturation par deux axes :

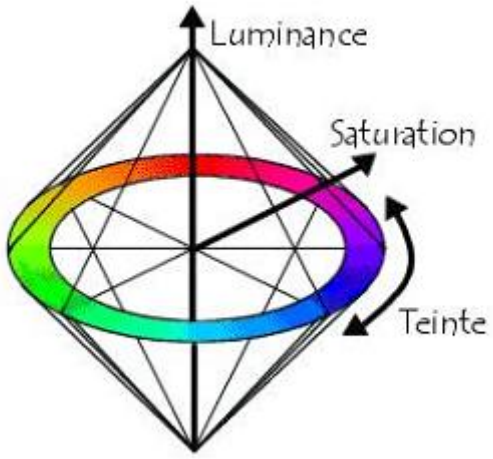


Figure 1.4: Représentation graphique du codage HSL [01]

Le modèle HSL a été mis au point dans le but de permettre un choix interactif rapide d'une couleur, pour autant il n'est pas adapté à une description quantitative d'une couleur.

Il existe d'autres modèles naturels de représentation proches du modèle HSL :

– HSB : Hue, Saturation, Brightness soit Teinte, Saturation, Brillance en français.

– HSV : Hue, Saturation, Value soit Teinte, Saturation, Valeur en français.

– HSI : Hue, Saturation, Intensity soit Teinte, Saturation, Intensité en français.

1.3.3. Le codage CMY

Le codage CMY (Cyan, Magenta, Yellow, ou Cyan, Magenta, Jaune en français, soit CMJ) est à la synthèse additive, ce que le codage RGB est à la synthèse soustractive. Ce modèle consiste à décomposer une couleur en valeurs de Cyan, de Magenta et de Jaune.

1.3.4. Le codage CIE

Les couleurs peuvent être perçues différemment selon les individus et peuvent être affichées différemment selon les périphériques d'affichage. La Commission Internationale de l'Eclairage (CIE) a donc défini des standards permettant de définir une couleur indépendamment des périphériques utilisés. A cette fin, la CIE a défini des critères basés sur la perception de la couleur par l'œil humain, grâce à un triple stimulus.

En 1931 la CIE a élaboré le système colorimétrique xy, Y représentant les couleurs selon leur chromaticité (axes x et y) et leur luminance (axe Y). Le diagramme de chromaticité, issu d'une transformation mathématique représente sur la périphérie les couleurs pures, repérées par leur longueur d'onde. La ligne fermant le diagramme (donc le spectre visible)se nomme la droite des pourpres :

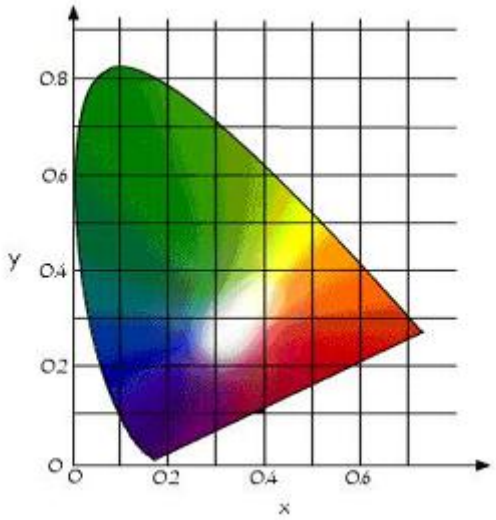


Figure 1.5 :Système colorimétrique CIE [01]

Toutefois ce mode de représentation purement mathématique ne tient pas compte des facteurs physiologiques de perception de la couleur par l'œil humain, ce qui résulte en un diagramme de chromaticité laissant par exemple une place beaucoup trop large aux couleurs vertes.

En 1960 la CIE a mis au point le modèle Lu*v*.

Enfin en 1976, afin de pallier aux lacunes du modèle xyY, la CIE développe le modèle colorimétrique La*b* (aussi connu sous le nom de CIE Lab), dans lequel une couleur est repérée par trois valeurs :

– L, la luminance, exprimée en pourcentage (0 pour le noir à 100 pour le blanc),

– a et b deux gammes de couleur allant respectivement du vert au rouge et du bleu

au jaune avec des valeurs allant de -120 à +120.

Le mode Lab couvre ainsi l'intégralité du spectre visible par l'œil humain et le représente de manière uniforme. Il permet donc de décrire l'ensemble des couleurs visibles indépendamment de toute technologie graphique. De cette façon il comprend la totalité des couleurs RGB et CMY, c'est la raison pour laquelle des logiciels tels que Photoshop utilisent ce mode pour passer d'un modèle de représentation à un autre.

Il s'agit d'un mode très utilisé dans l'industrie, mais peu retenu dans la plupart des logiciels étant donné qu'il est difficile à manipuler.

Les modèles de la CIE ne sont pas intuitifs, toutefois le fait de les utiliser garantit qu'une couleur créée selon ces modèles sera vue de la même façon par tous ! .

1.3.5. Le codage YUV

Le modèle YUV (appelé aussi CCIR 601) est un modèle de représentation de la couleur dédié à la vidéo analogique. Il s'agit du format utilisé dans les standards PAL (Phase Alternation Line) et SECAM (Séquentiel Couleur avec Mémoire). Le paramètre Y représente la luminance (c'est-à-dire l'information en noir et blanc), tandis que U et V permettent de représenter la chrominance, c'est-à-dire l'information sur la couleur. Ce modèle a été mis au point afin de permettre de transmettre des informations colorées aux téléviseurs couleurs, tout en s'assurant que les téléviseurs noir et blanc existant continuent d'afficher une image en tons de gris.

Voici les relations liant Y à R,G et B, U à B et à la luminance, et enfin V à B et à la luminance :

– $Y = 0.299R+0.587G+0.114B$

– $U = - 0.147R - 0.289G + 0.463B = 0.492(B - Y)$

– $V = 0.615R - 0.515G - 0.100B = 0.877(B - Y)$

1.3.6. Le codage YIQ

Le modèle YIQ est très proche du modèle YUV. Il est notamment utilisé dans le standard vidéo NTSC (utilisé entre autres aux États-Unis et au Japon).

Le paramètre Y représente la luminance. I et Q représentent respectivement l'Interpolation et la Quadrature. Les relations entre ces paramètres et le modèle RGB sont les suivantes :

– $Y = 0.299R + 0.587G + 0.114B$

– $I = 0.596R - 0.275G - 0.321B$

– $Q = 0.212R - 0.523G + 0.311B$

1.4. Représentation des couleurs [03]

Nous l'avons vu une image apparait comme une matrice où chaque case contient des nombres associés à une couleur. Usuellement on distingue 3 grands types de couleurs pour une image numérique :

- Le noir et blanc ;
- Les niveaux de gris ;
- La couleur.

Ces types sont généralement à choisir lors d'une numérisation par scanner ou lors de la configuration d'un appareil photographique.

1.4.1. Image couleur

La couleur d'un pixel est obtenue, comme le ferait un peintre, par le mélange de couleurs fondamentales. Il ne s'agit pas ici de décrire toutes les techniques utilisées. Nous allons décrire un des principes les plus couramment utilisé qui est celui de la synthèse additive. Selon Les représentations de la couleur

Figure 1.6 : Image originale couleur[05]

1.4.2. Image noir et blanc

Le noir et blanc est le plus simple. Le contenu de chaque case de la matrice est soit un 0 (noir) soit 1 (blanc). Le nombre de couleurs n'est que de 2 et le rendu de l'image le moins performant mais parfois suffisant dans le cadre par exemple de documents scripturaux.

Figure 1.7 : Image noire et blanc

1.4.3. Niveaux de gris

Le codage dit en niveaux de gris permet d'obtenir plus de nuances que le simple noir et blanc. Il offre des possibilités supplémentaires pour coder le niveau de l'intensité

lumineuse. La couleur est codée souvent sur un octet soit 8 bits ce qui offre la possibilité d'obtenir 256 niveau de gris (0 pour le noir et 255 pour le blanc). On peut aussi le faire avec 16 niveaux de gris (4 bits).

Tableau 1.1 : 256 niveaux de gris [03]

Figure 1.8 : Image niveaux de gris

1.5. Les formats standards d'images [03]

Formats d'image Le format d'un fichier, que ce soit une image, de la musique, un tableau ou du traitement de texte, désigne la structure de ce fichier. Cette structure est l'organisation des données interne au fichier, et détermine le logiciel nécessaire à son traitement.

Les fichiers Excel se terminent par .xls, les fichiers Word par .doc, les fichiers Jpeg par. Jpg etc….

Concernant les images, il existe une grande variété de formats de fichiers, qui ont chacun des caractéristiques propres.

Consistent à la fois des bits comprenant les informations de l'image et d'en-tête concernant la lecture et l'interprétation du fichier. Les formats de fichiers varient en termes de résolution, profondeur de bit, capacités de couleurs et support pour la compression et les métadonnées.

Le plus connu est le Jpeg. Il s'est largement démocratisé car il compresse les images pour les enregistrer.

	Type(matriciel/ vectoriel)	**Compression des données**	**Nombre de couleurs supporées**	**Affichage progressif**	**Anima-tion**	**transparence**
JPEG	Matriciel	Oui, réglable (avec perte)	16 millions	Oui	Non	Non
JPEG 2000	Matriciel	Oui,(avec ou sans perte)	4 millions	Oui	Oui	Oui

GIF	Matriciel	Oui, (sans perte)	256 maxi (palette)	Oui	Oui	Oui
PNG	Matriciel	Oui, (sans perte)	Palettisé (256 couleurs ou moins) ou 16 millions	Oui	Non	Oui (couche Apha)
TIFF	Matriciel	Compression ou pas avec ou sans pertes	De monochrome à 16 millions	Non	Non	Oui (couche Apha)
SVG	Vectoriel	Compression possible	16 millions	Ne s'applique pas	Oui	Oui (par nature)

Tableeau 1.2 :comparatif des format d'image [03]

1.6. Filtrage [04]

Le principe du filtrage est de modifier la valeur des pixels d'une image, généralement dans le but d'améliorer son aspect. En pratique, il s'agit de créer une nouvelle image en se servant des valeurs des pixels de l'image d'origine.

1.6.1. Définition filtre :

Un filtre est une transformation mathématique (appelée produit de convolution) permettant de modifier la valeur d'un pixel en fonction des valeurs des pixels avoisinants, affectées de coefficients.

Les calculs sont faits pour chacune des trois composantes de couleur. Le filtre est représenté par un tableau (une matrice), caractérisé par ses dimensions et ses coefficients, dont le centre correspond au pixel concerné. La somme des coefficients doit faire 1.

1.6.2. Types filtrage :

Nous avons plusieurs types de filtration, dont Le filtre médian

1.6.2.1. Le filtre médian

La technique de filtre médian est largement utilisée en traitement d'images numériques, car il permet de réduire le bruit tout en conservant les contours de l'image.

L'idée principale du filtre médian est de remplacer chaque pixel par la valeur médiane de son voisinage Considérons neuf pixels en niveaux de gris, dont une valeur est aberrante (ici 255) :

2	4	12
2	255	3
7	9	3

Tableeau 1.3 : Les valeurs numériques d'Image niveaux de gris

Le filtre médian va d'abord trier ces valeurs par ordre croissant :

2, 2, 3, 3, 4, 7, 9, 12, 255

Et prendre la valeur médiane (la cinquième valeur), ici la valeur 4. La sortie du filtre donnera :

2	4	12
2	4	3
7	9	3

Tableeau 1.4 : Les valeurs numériques La sortie du filtre donnera

Que nous utilisons dans le calcul PSNR dans le dernier chapitre.

Image niveaux de gris avec Noise

Image après filtrage médian

Tableeau 1.5 : exemple application filtrage médian

1.7. Photomontage [04]:

Regardez attentivement la série de 9 images A, B, C, D, E, F, G, H, I. Chacune a été obtenue à partir de la précédente en réduisant la taille de l'image de moitié, ce qui a donné quatre morceaux analogues qu'on a placés en carrefour obtenir une image ayant la même taille que l'image d'origine. Le nombre de pixels a été exactement conservé et en fait, on a seulement déplacé chacun des pixels (sans en changer la couleur). Précisément on a découpé l'image initiale en paquets carrés de quatre pixels (2x2), puis pour chaque paquet carré de quatre pixels, on a utilisé celui du haut à gauche pour l'image réduite de Mona Lisa en haut à gauche, celui en haut à droite pour l'image au haut à droite de Mona Lisa, etc. Cette opération produit bien quatre versions réduites de Mona Lisa. Cette transformation s'appelle la transformation du photomaton. L'image B comporte 4 Mona Lisa. L'image C en comporte 16. L'image D en comporte 64, etc. Il se produit quelque chose d'étrange car, au bout de neuf étapes, l'image de Mona Lisa est réapparue. Précisons que c'est bien la même transformation qui a été utilisée pour déduire les unes après les autres les images de la série

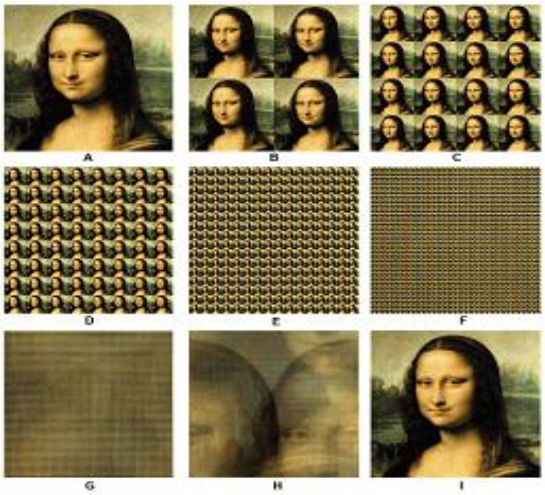


Figure 1.9 : application photomontage l'image de Mona Lisa [04]

1.8. Conclusion :

Dans ce chapitre, on donne vue générale des les images et une relation leur quel formats, et les codages des images. A la fin, nous avons présenté la Photomontage.

Chapitre 2

Méthode de cryptage des images

2.1. Introduction

Cryptographie ou le chiffrement depuis les temps anciens, a été utilisé dans le domaine militaire, Le cryptage est le processus de maintien de la confidentialité de l'information en utilisant des programmes Sa capacité à se transformer et à traduire cette information en symboles Donc, si ce qui a été consulté par des gens pas autorisés à le faire, ils ne peuvent pas comprendre tout. Parce eux le résultat est un mélange de symboles et de chiffres et lettres incompréhensibles

Dans notre Chapitre, nous allons appliquer le concept de chiffrement sur les images

2.2. Définition de Cryptographie [01]

Depuis longtemps, la transmission de données sensibles a nécessité l'utilisation d'un système de sécurisation performant. Les services secrets des grandes puissances économiques et politiques, de tout temps très impliqués, ont développé, tout d'abord, des codages alphabétiques et numériques simples, puis des techniques cryptographiques plus poussées, grâce à l'outil mathématique pour rendre inviolable set inexploitables directement leurs données sensibles.

La cryptologie, véritable science régissant le codage de l'information, a connu une réelle explosion avec le développement des systèmes informatiques, passant d'une ère artisanale et confidentielle à des systèmes de très hautes technologies nécessitant une importante puissance de calcul. Elle a connu un plus large essor encore avec l'arrivée des systèmes de communications modernes (internet, etc.) où il y a une nécessité absolue de protéger les données échangées pour respecter les individus.

2.3. Les techniques de cryptographie [01]

La cryptologie, science fondamentale qui régit la cryptographie, est essentiellement basée sur l'arithmétique. Ainsi dans le cas d'un texte, il s'agit de transformer les lettres qui composent le message en une succession de chiffres (sous forme de bits dans le cas de l'informatique pour permettre le fonctionnement binaire des ordinateurs), puis ensuite de faire des calculs sur ces chiffres pour:

- d'une part les modifier et les rendre incompréhensibles. Le résultat de cette modification(le message chiffré) est appelé cryptogramme,
- d'autre part, faire en sorte que le destinataire sache les déchiffrer en utilisant les outils préétablis ou joints aux données.

Le fait de coder un message de façon à le rendre secret s'appelle chiffrement. La méthode inverse consistant à retrouver le message original, est appelée déchiffrement.

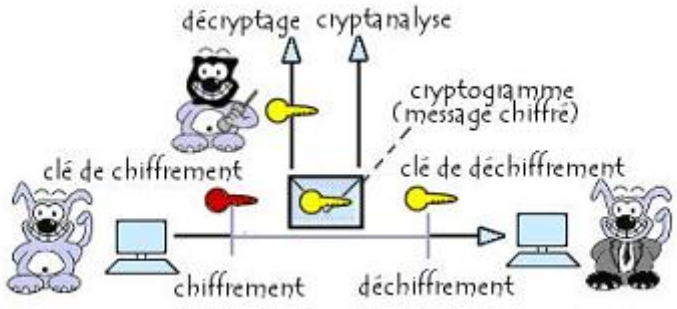


Figure 2.1 : Schéma de chiffrement et déchiffrement[01].

Le chiffrement se fait généralement à l'aide d'une clef de chiffrement, le déchiffrement avec une clef de déchiffrement. On distingue généralement deux types de clefs :

- Les clés symétriques : on utilise des clés identiques à la fois pour le chiffrement et pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète. Ils 'agit de la cryptographie à clé privée.
- Les clés asymétriques : on utilise de clés différentes pour le chiffrement et le déchiffrement.

On parle alors de chiffrement asymétrique. Il s'agit de la cryptographie à clé publique.

Au cours des années soixante-dix, un système de sécurisation basé sur la polarisation des photons est apparu : la cryptographie quantique. Cette technique est différente des autres crypto systèmes à clé puisqu'elle fonctionne sur des propriétés physiques intrinsèques au système.

2.3.1. La cryptographie à clé privée [01]

Le chiffrement à clé privée, aussi appelé chiffrement symétrique ou chiffrement à clé secrète, consiste à utiliser la même clé pour le chiffrement et le déchiffrement.

Si A veut envoyer un message à B, tous deux doivent au préalable s'être transmis la clé. Celle-ci est identique chez l'émetteur et le destinataire du message. Les deux parties doivent se communiquer la clé à un moment ou à un autre, ce qui constitue un risque non négligeable d'interception. Elle peut servir pour plusieurs messages ou être modifiée à chaque échange. Dans le premier cas, elle repose sur la confiance en l'utilisateur.

Les systèmes à clé privée posent un second problème. Si une clé différente est mise en œuvre pour chaque paire d'utilisateurs du réseau, le nombre total des clés augmente beaucoup plus

rapidement que celui de protagonistes. Dans les années 20, Gilbert Vernam et Joseph Marlogne

Figure 2.2 : Schéma de chiffrement à clé symétrique[01]

Mettent au point la méthode de l'one time pad (méthode du masque jetable), basée sur une clé privée générée aléatoirement, utilisée une et une seule fois puis détruite. Plus tard, le Kremlin et la Maison Blanche sont reliés par le fameux téléphone rouge, dont les communications étaient cryptées par une clé privée selon la méthode du masque jetable. La clé était alors échangée au moyen de la valise diplomatique (jouant le rôle de canal sécurisé).

Dans les années 80, Claude Shannon démontra que pour être totalement sûr, les systèmes à clef privée doivent utiliser les clefs d'une longueur au moins égale à celle du message à chiffrer, ce qui pose problème.

De plus, le chiffrement symétrique impose d'avoir un canal sécurisé pour l'échange de la clé, ce qui dégrade sérieusement l'intérêt d'un tel système de chiffrement.

2.3.2. La cryptographie à clé publique [01]

La cryptologie moderne est née en 1976 avec l'introduction par deux chercheurs de l'Université de Sanford, Whitfield Diffie et Martin Hellman, du concept de clé publique.

Le principe émet que seule l'opération de déchiffrement doit être protégée par une clé gardée secrète. Le chiffrement peut parfaitement être exécuté à l'aide d'une clé connue publiquement, à condition, bien sûr, qu'il soit virtuellement impossible d'en déduire la valeur de la clé secrète. On parle alors de " cryptographie asymétrique ". Les deux inventeurs butent cependant sur la difficulté de proposer un véritable crypto système à clé publique ; la solution vient du MIT en1978, avec la publication d'un procédé de chiffrement mettant en œuvre les idées de Diffue et Hellman. Ils constatent que la clé publique permet le transport des clés conventionnelles, qui ne repose pas sur l'existence d'une hiérarchie cloisonnée. C'est bien ainsi que fonctionne le système actuellement. Ils savent également qu'un système de chiffrement peut être utilisé comme mode d'authentification : c'est le principe de l'I.F.F. (Identification Friands and Foes), mis au point dans les années 1950 par l'armée de l'air américaine, qui identifie les appareils amis par leur capacité à déchiffrer un message choisi au

hasard et inclus dans le signal radar. Dans le contexte de la clé publique, pouvoir déchiffrer un message produit la preuve qu'on est en possession de la clé secrète. Contrairement au mode conventionnel, cette preuve est opposable aux tiers, puisque quiconque peut vérifier par chiffrement public qu'on restitue le message initial. On réalise l'analogue d'une signature manuscrite liant un document à son auteur. C'est précisément ce mécanisme de signature numérique qui se met en place aujourd'hui pour les besoins du commerce électronique.

Au-delà de l'invention de la clé publique, l'un des apports de la cryptologie moderne est d'avoirs fournir un cadre conceptuel cohérent pour analyser qualitativement les menaces potentielles contre un système cryptographique. La sécurité est algorithmique : elle fait l'hypothèse quel 'adversaire éventuel dispose d'une puissance de calcul importante mais bornée ; ceci est contraire à la théorie de Shannon qui attribue à l'ennemi une capacité infinie de calcul et conduit de ce fait ce qu'on appelle la " sécurité inconditionnelle ". Cette dernière mène à des systèmes peu utilisés puisque la clé a nécessairement une longueur au moins égale au texte à chiffrer. Elle est toutefois parfaitement réalisable par combinaison du texte clair - supposé d'une suite de bits (c'est-à-dire0 et 1) avec une autre suite constituant la clé, la combinaison étant réalisée par une addition de bits à bits, analogue à l'addition ordinaire, à ceci près que 1+1 vaut 0. Ce mécanisme, connu sous le nom de " chiffrement de Vernal ", est parfaitement sûr lorsque chaque clé n'est utilisée qu'une seule fois. On peut imaginer d'autres mécanismes de sécurité qui ne soient ni algorithmiques ni inconditionnels ; c'est ainsi qu'on envisage aujourd'hui la possibilité de procédés de cryptographie sur les lois de la physique quantique

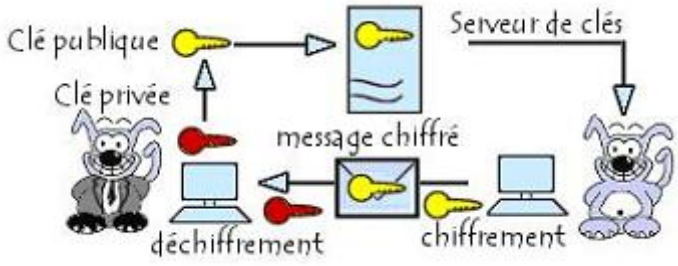


Figure 2.3 : Schéma de chiffrement à clé publique[01]

2.4. Quelques applications de la cryptographie [01]

Les banques, la médecine, le militaire, mais aussi de nombreuses entreprises, échangent couramment des informations confidentielles sous la forme de données télématiques par l'intermédiaire d'ordinateurs. Ces données sont en général transmises par le réseau

téléphonique ou par d'autres réseaux publics, si bien qu'il convient de mettre au point des cryptages efficaces pour les protéger. En combinant les systèmes de cryptographie évoqués ci-dessus, on peut ainsi créer des chiffres de complexité variée, avec la contrainte que les clés sont elles aussi amenées à être transmises sur ces réseaux. Avec suffisamment de temps et de matériel, on peut résoudre la plupart des codes chiffrés et découvrir ainsi leurs clés. Aussi la complexité du code doit-elle être adaptée afin qu'il soit impossible de le découvrir en un temps raisonnable. Par exemple, des ordres militaires qui ne doivent rester secrets que pendant quelques heures peuvent être cryptés au moyen d'un chiffre qui ne conviendrait pas au codage de rapports diplomatiques exigeant une confidentialité à long terme.

Avec ses pages interactives, ses images, ses documents sonores, le réseau Internet a permis le développement d'une forme plus spectaculaire de commerce électronique que celui déjà connu par le minitel. Désormais, les entreprises de vente par correspondance peuvent concevoir des catalogues illustrés sous forme électronique et les achats peuvent s'effectuer au moyen d'une carte de crédit (les jeux téléchargés permettent de faire l'économie du prix de l'emballage).Il existe cependant un obstacle majeur : le seul standard actuel de paiement électronique est la carte bleue. C'est donc ici qu'intervient le cryptage, qui n'est pourtant pas encore légal dans tous les pays. En effet, un problème d'Internet est la question de la sécurité et de la confidentialité.

Par nature Internet, étant ouvert à tous, se prête facilement aux piratages de toute nature. Des logiciels de cryptographie permettent d'assurer une relative confidentialité des échanges.

2.5. Autres façons de protéger les images [02].

Stéganographie et cryptographie Le tatouage d'images peut être perçu comme une branche de la stéganographie. La stéganographie est l'art de cacher un message secondaire dans un message primaire. Le message primaire reste lisible de tous, tandis que le message secondaire n'est lisible que par une ou plusieurs personnes propriétaires d'une information secrète. La stéganographie se distingue de la cryptographie dans la mesure où l'objectif principal en cryptographie est de rendre illisible un message primaire à toute personne ne possédant pas une information secrète adéquate. De plus, alors que la cryptographie offre une sécurité plutôt a priori (contrôle d'accès, par exemple), la stéganographie offre une sécurité plutôt a posteriori, dans la mesure où le message secondaire est supposé rester accessible même après recopies et manipulations du message primaire.

Le tatouage permet une vérification ou une extraction efficace et automatique de certaines informations liées à l'origine, au contenu ou même à la diffusion d'une l'image.

2.5.1. Définition du tatouage [03]

Le tatouage numérique est l'un des concepts techniques qui soulève la problématique et permet à chacun de donner sa définition, et en raison de l'absence d'une définition normalisée, nous présentons quelques définitions parmi plusieurs, proposées par différents auteurs du domaine informatique, électronique ou autre.

2.5.1.1. Définition Miller et Cox 1997

Le tatouage numérique signifie l'incorporation d'une information numérique dans un contenu multimédia, comme une vidéo, un audio ou une image de telle manière que l'information insérée doit être imperceptible pour un observateur humain, puis à tenter de la récupérer après que le document tatoue ait éventuellement subi des manipulations de nature variée.

2.5.1.2. Définition Kundur et Hatzinakos 1998

Le processus du tatouage numérique implique la modification des données multimédia originales pour insérer un watremark contenant des informations clés telles que les codes d'authentification ou de droit d'auteur. La méthode d'insertion doit conserver les données originales visuellement inchangés, mais d'imposer des modifications qui peuvent être détectes à l'aide d'un algorithme d'extraction. Les types de signaux à tatouer sont des images, le son, vidéo et le texte.

2.5.1.3. Définition Petit colas, Anderson et Kuhn 1999

Définition Le tatouage numérique signifie l'intégration d'une information dans un document numérique de façon à ce que cette information soit imperceptible pour un observateur humain, mais facilement détectée par l'ordinateur. Le watremark est une information transparente, invisible qui est insère dans un document source en utilisant un algorithme informatique.

2.5.1.4. Définition Christian REY et Jean-Luc DUGELAY 2001

Le tatouage numérique est une technique qui consiste à cacher dans un document numérique une information subliminale (i. e, invisible ou inaudible suivant la nature du

document) permettant d'assurer un service de sécurité (copyright, intégrité, non répudiation, etc.) ou à but d'information.

Une des particularités du tatouage numérique par rapport à d'autres techniques, comme par exemple un stockage simple de l'information dans l'en-t été du fichier, est que le watremark est lie de manière intime et résistante aux données. De ce fait, le tatouage est théoriquement indépendant du format de fichier et il peut être détecte ou extrait même si le document a subi des modifications ou s'il est incomplet.

2.5.1.5. Définition Chun-Shien Lu 2004

Le tatouage numérique est un signal intègre de façon permanente dans des données numériques (audio, image, vidéo et texte) qui peut être détecte ou extrait plus tard par l'exécution d'un algorithme informatique afin de faire des affirmations sur les données. Le tatouage est caché dans le document hôte de telle manière qu'il est inséparable des données et qu'il est résistant à de nombreuses opérations, sans dégrader la qualité du document hôte. Ainsi, par le biais du tatouage, le travail est encore accessible, mais définitivement marque. Quelque soit la manière d'exprimer la définition de la technique du tatouage, son principe estes exigences restent les mêmes. Dans les sections suivantes, nous présentons ce principe (à travers un modèle générique) et les exigences d'une technique du tatouage invisible.

2.5.2. Tatouage visible et invisible [03]

On distingue généralement deux classes du tatouage : visible et invisible. L'idée derrière le tatouage visible est très simple. Il est équivalent à l'estampage d'un watremark sur le papier, et pour cette raison il est appelé parfois estampage numérique. Le tatouage visible altère le signal ou le fichier (par exemple ajout d'une image pour en marquer une autre). Ilets fréquent que les agences de photo ajoutent un watermark visible en forme de copyright aux versions de prévisualisation (basse résolution) de leurs photos. Ceci afin d'éviter que ces versions ne se substituent aux versions hautes résolutions payantes.

Le tatouage visible est un sujet à controverse. Il y a une branche de chercheurs qui disent que si le watremark est visible, alors elle peut être facilement attaquée. Néanmoins, nous trouvons des applications qui demandent que le watremark soit visible, c'est le cas du logo des sociétés dans les programmes t télévisuels. Dans la catégorie du tatouage visible, nous distinguons les travaux.

En revanche, le tatouage invisible est un concept beaucoup plus complexe. Le tatouage invisible modifie le signal d'une manière imperceptible par l'utilisateur final. Pour reprendre l'exemple de l'agence de photo, les photos hautes résolutions vendues par l'agence possèdent elles au contraire un watermark invisible, qui ne dégrade donc pas le contenu visuel, mais qui permet de détêterl'éventuelle source d'un vol. Le message cache par le tatouage peut être un identifiant de l'acheteur par exemple. En cas d'utilisation non-autorisée, l'agence peut alors se retourner contre l'acheteur.

Le tatouage invisible est l'approche la plus développée qui attire la plupart des chercheurs. La majorité des techniques concernant la protection de propriété intellectuelle suit l'abranche du tatouage invisible.

Dans ce qui se suit, nous nous concentrons sur cette dernière catégorie, et le mot "Tatouage "est pris au sens du tatouage invisible.

2.5.3. Comment tatouer un document numérique ? [04]

Comme expliqué au début, le tatouage numérique consiste à modifier spatialement l'image : c'est à dire, ajouter une marque distinctive à l'image comme par exemple un signe copyright, ou un texte mis en fond.

L'ajout d'un tatouage visible est assez simple, puisqu'il s'agit seulement d'apposer sur le document une marque distinctive. Le problème est que ce tatouage est facilement altérable, en même temps que le document. Il existe une réponse à ce problème, une autre méthode de tatouage.

La deuxième méthode consiste à modifier la fin d'une série de bits dans l'image, de façon à ne pas altérer la qualité de l'image : la modification est invisible à l'œil nu. De plus, cette modification du message permet d'ajouter différentes informations, comme l'auteur, date de création, etc.

2.5.4. Lecture du tatouage numérique [04]

Le tatouage numérique est inséré dans l'image l'aide d'un algorithme censé être suffisamment difficile à retrouver. Malheureusement cette technique de dissimulation n'étant pas totalement discrète, le tatouage est protégé à l'aide d'une clé numérique dont seul le propriétaire est en possession.

En effet, le tatouage peut être aisément retrouvé à l'aide d'un scanner spécifiquement désigné pour cet usage.

L'utilisation de cette clé permet ainsi d'éviter le retrait du tatouage s'il est retrouvé sur une copie du document.

En conclusion, le tatouage numérique, c'est d'abord une signature intégrée à un document visuel (ou audio, ça peut également marcher) de façon explicite, ou invisible (vous le verrez mieux dans la partie suivante), sécurisé grâce à une clé pour éviter les attaques.

Figure 2.4 : Image appliquée par tatouage [04].

2.6. La stéganographie

2.6.1. Définition [05]

La stéganographie (du grec stégano, couvert et graphie, écriture) est l'art de cacher un message secret au sein d'un autre message porteur (texte, image, son, vidéo...) de caractère anodin, de sorte que l'existence même du secret en soit dissimulée. Alors qu'avec la cryptographie, la sécurité repose sur le fait que le message chiffré soit incompréhensible pour les personnes non autorisées, avec la stéganographie, la sécurité repose sur le fait que la présence même d'un message secret ne sera sans doute pas soupçonnée et détectée.

2.6.2. La Méthode LSB (Least Significant Beat)[06]

Ou méthode de bit de poids faible Cette méthode consiste à modifier le bit de poids faible des pixels codant l'image. Une image est un tableau constitué d'un ensemble de pixels. Pour chaque pixel, on code la couleur avec trois octets : un pour le rouge, un pour le vert, un pour le bleu. Chaque octet indique l'intensité de la couleur correspondante, sur un niveau allant de 0 à 255. 255 correspond à la couleur native. Passer d'un niveau N à un niveau N – n, où n est suffisamment petit ne modifie que de peu la couleur, et c'est précisément sur cela que repose la

méthode LSB. Mise en pratique On prend un octet correspondant à l'une des trois couleurs d'un pixel, par exemple 01101011. Si on change les quatre derniers bits, cela ne change que de peu la couleur. Dans notre exemple, 01101011, 1011 correspond donc aux bits de poids faible. L'idée est de remplacer ces bits de poids faible par ceux de l'information que l'on souhaite dissimuler.

2.6.3. Cacher une image dans une autre

Soit un octet de l'image qui cache 01101011 et un octet de l'image que l'on souhaite cacher 10011101. Le but est de remplacer les bits de poids faible de l'image qui cache par les bits de poids fort de l'image qu'on souhaite cacher. Ainsi, on obtiendra l'octet 01101001. Attention, on effectue des changements sur des détails. Il faut choisir une image qui cache qui présente suffisamment de changements, auquel cas l'image cacée s'apercevra.

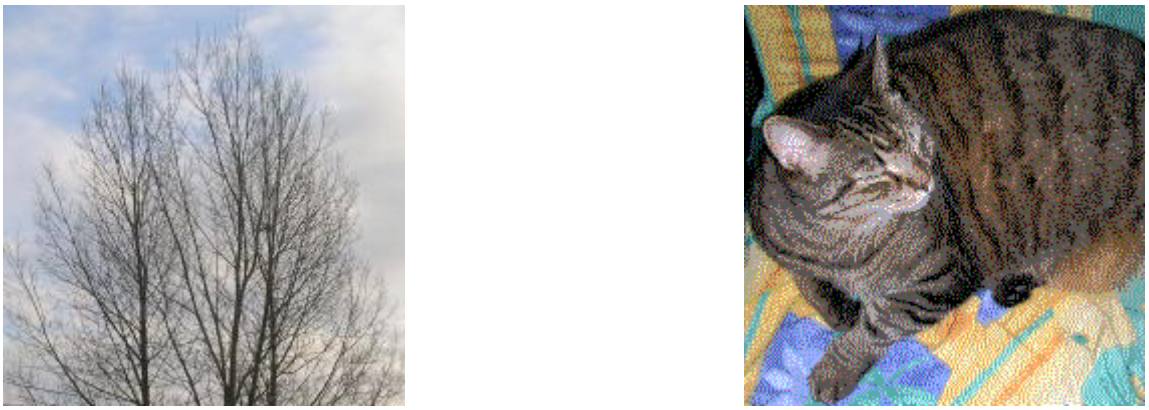


Figure 2.5 : Stéganographie original et La stéganographie est récupérée

2.6.4. **Stganalysis [**06] :

La stganalysis rend l'usage terroriste de la sténographie techniquement risqué. Steganalysis est la science de la détection de messages cachés et de là la science de la détection de la sténographie. Tout comme un cryptanalyseur applique la cryptanalyse dans une tentative de noix de poche ou de messages chiffrés, le steganolyst est celui qui applique de la steganolyse pour tenter de détecter l'existence d'informations cachées. En cryptanalyse, des parties du texte en clair (si elles sont disponibles) et des parties du texte chiffré sont analysées. En stanolyse, des comparaisons sont faites entre l'objet de couverture, l'objet stego et les parties possibles du

message. En cryptographie, le résultat final est le texte chiffré; En sténographie, le résultat final est l'objet stego. Avec la sténographie, le message caché peut ou non être chiffré.

2.7. Cryptanalyse [7]

Lorsqu'un crypto-système est synthétisé, il faut s'assurer qu'il est effectivement robuste face a des attaques pirates. Cette étape de validation est appelée la cryptanalyse. Elle consiste a tester les crypto-systèmes afin de déceler leurs éventuelles faiblesses.

Une étape essentielle de la validation d'un schéma de transmission est la cryptanalyse.

La cryptanalyse est l'étude des attaques possibles sur les crypto systèmes afin de déceler leurs éventuelles faiblesses

Omar et Ali essaient de communiquer de façon sécurisée, un adversaire, Charlie, tente de faire échouer la communication secrète entre Omar et Ali. Il peut, par exemple, intercepter le signal transitant sur le canal dans le but de récupérer le texte clair, il peut modifier le signal toutes ces tentatives sont des attaques sur le crypto-système

2.7.1. Définition

La cryptanalyse est l'étude des probabilités de succès des attaques possibles sur les crypto-systèmes afin de déceler leur éventuelles faiblesses un des principaux objectifs de la cryptanalyse est de tester si un adversaire peut déchiffrer le texte clair ou récupérer la clé secrète. Pour cela, le cryptanalyse se met a place de l'adversaire.

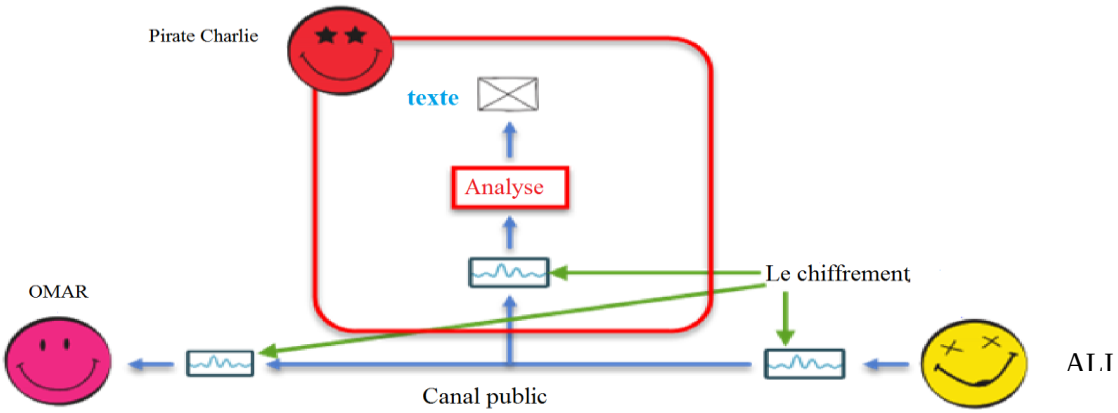


Figure 2.6 : Schéma de communication

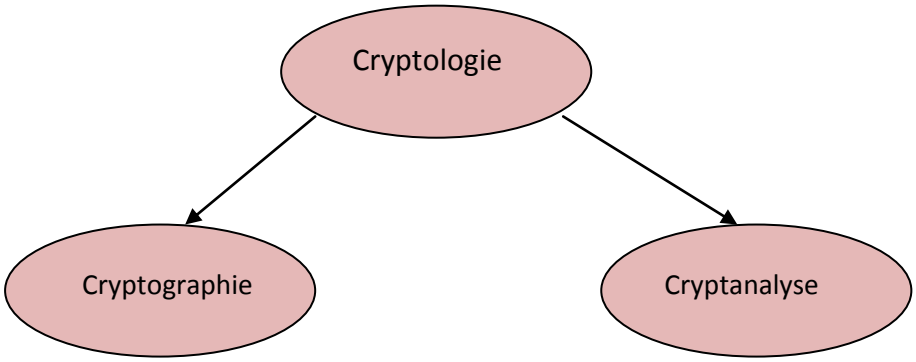


Figure 2.7 : Schéma Cryptologie

La cryptographie et la cryptanalyse sont deux domaines d'études évoluant constamment et en parallèle. En effet, de nouveaux crypto-systèmes, toujours plus complexes, sont développés pour remplacer ceux que ont été ‘‘cassés’’ par la cryptanalyse et de nouvelles techniques de cryptanalyse sont inventées pour tester ces nouveaux crypto-systémes. Le problème de la Cryptographie est de concevoir des systèmes sure et de faire en sorte que la durée nécessaire pour ‘‘cassés’’ un crypto-système soit supérieur à sa durée de validité.

La tendance actuelle est de chercher a prouver la sécurité d'un système sur la base d'hypothèses, sur la puissance de calcul requis ou sur la quantité de texte.

La réussite pratique d'un attaque dépend d'un certain nombre d'éléments, comme les connaissances nécessaires a priori, l'effort demandé (complexité, temps de calcul), la quantité Et la qualité des informations pouvant être déduites de l'attaque (déchiffrement de la clé Secrète, algorithme de chiffrement découvert sans connaitre la clé secrète, informations sur le texte clair,…..).

La complexité de l'attaque se caractérise par le temps en nombre d'opérations effectuées clair et texte chiffré) requises.

A travers les années, de nombreuses attaques possibles contre les crypto systèmes ont Été identifiée, de telle sorte qu'il est difficile d'en établir une liste exhaustive. En revanche, on distingue deux classes d'attaques :

Les attaques actives et les attaque passives.

2.7.2. Attaques actives :

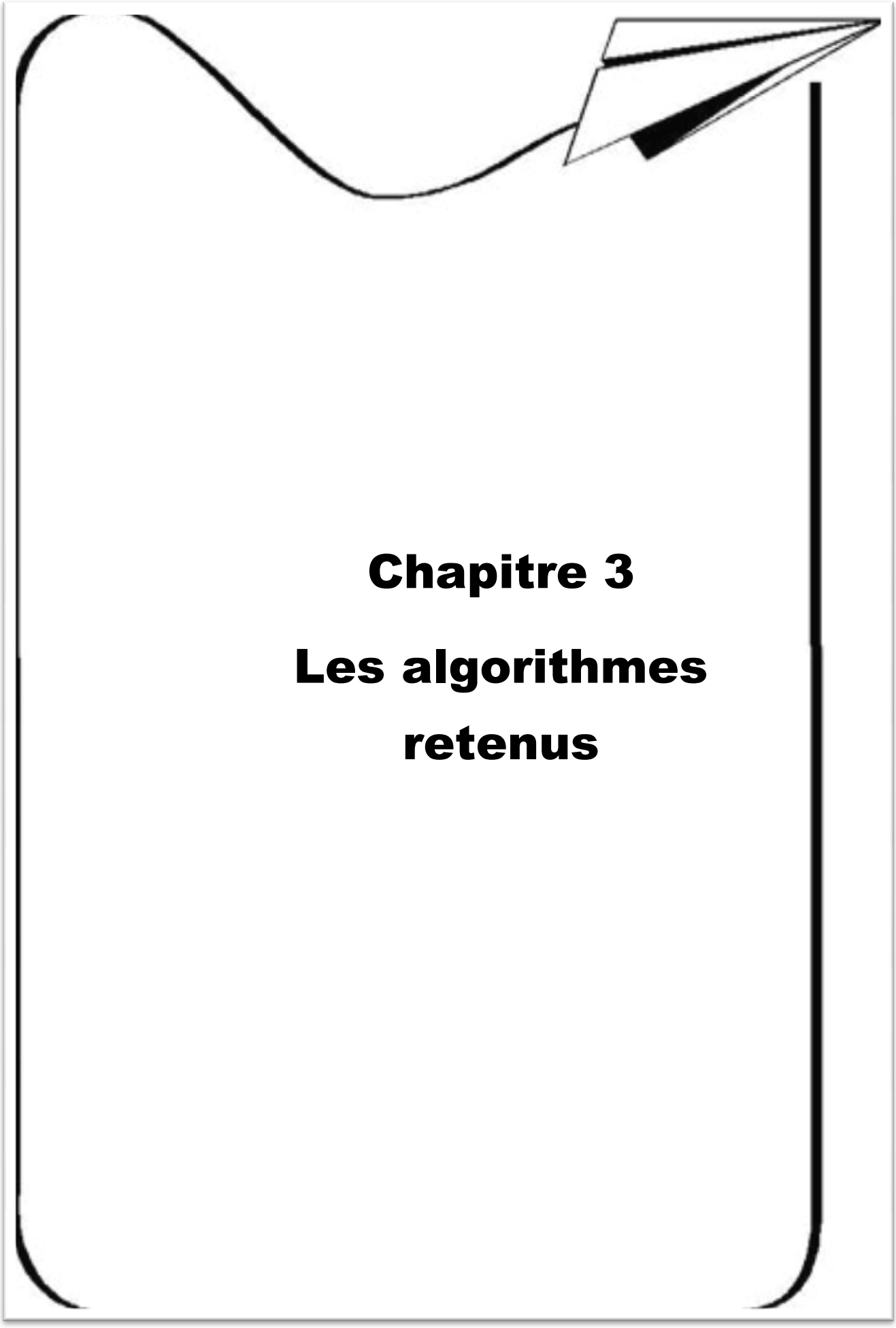
Dans les attaques actives, l'adversaire agit sur l'information. Il altère l'intégrité des données, l'authentification et la confidentialité. Il peut chercher à altérer la transmission du message sur le canal, par exemple, en modifiant le message (suppression, ajout, modification des séquences du message), en retardant(ou empêchant) sa transmission,
En répétant son envoi.

2.7.3. Attaque passives :

Dans les attaques passives, l'adversaire observe des informations qui transitent sur le canal sans les modifier. Il cherche à récupérer des informations sur le crypto système sans l'altérer, telles que le message, la clé secrète,….dans ce cas, l'adversaire touche à la confidentialité des données.

2.8. Conclusion

En conclusion, nous avons présenté dans ce chapitre la définition de cryptographie On distingue généralement deux types de clefs Les clés symétriques et Les clés asymétriques et autres façons de protéger les images (tatouer un document numérique, et la stéganographie)



Chapitre 3

Les algorithmes retenus

3.1. Introduction

Dans ce chapitre, nous avons présenté les algorithmes retenu de cryptage après cela, nous avons parlé de différent types modes de chiffrement, dans la dernière, nous avons parlé sur Mesure de l'évaluation du cryptage la plus importante

3.2. Les Algorithmes retenu [01]

3.2.1. Algorithme RC5

Le bloc itéré RC5 a été introduit par Rivest , Shamir et Adleman en 1994. La principale caractéristique de la RC5 est la lourde l'utilisation des rotations dépendantes des données. RC5 a une taille de mot variable w, a nombre variable de tours r, et une clé secrète.

Il est représenté par RC5 w / r / b. La valeur nominale de 32 bits, et RC5 crypte des blocs de deux mots. Le RC5 se compose de cryptage, décryptage et expansion de clés. La clé développée contient T = 2 × (r + 1) mots. Les opérations primitives de la RC5 sont illustrées Dans le tableau 3.1. Généralement, RC5 est un code à bloc symétrique rapide qui est Adapté aux implémentations matérielles et logicielles nécessitant peu de mémoire. Il offre une sécurité élevée lorsque de bons paramètres sont choisis.

a + b	Addition en nombre entier module 2w
a – b	Soustraction entière modulo 2w
a ⊕b	XOR bit par bit de mots w-bit
a * b	Multiplication en nombre entier modulo 2w
a <<<b	Tournez le mot w-bit a à gauche par le montant donné par le Moins important lg w bits de b
a >>>b	Faites pivoter le mot w-bit a à droite par le montant donné par le Moins important lg w bits de b

Tableau 3.1 Opérations primitives de RC5 [01]

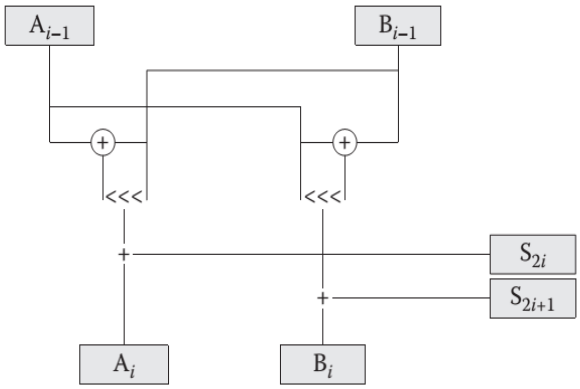


Figure 3.1 : Diagramme du cryptage à bloque symétrique RC5 W / r / b[01]

3.2.1.1. Algorithme de chiffrement RC5

Nous supposons que le bloque d'entrée est Donné dans deux registres w-bit A et B, et nous supposons également que la clé d'expansion a déjà été réalisée de sorte que S [0], S [1], ..., S [t1] ont été calculés. Les étapes de l'algorithme de cryptage peuvent être données comme suit:

A = A+S [0];

B = B+S [1];

For I = 1 to r do

A = ((A ⊕B) <<< B) +S [2i];

B = ((B ⊕A) <<< A) +S [2i+1];

End

À chaque tour de RC5, les deux registres A et B sont mis à jour comme indiqué dans la Figure 3.1.

3.2.1.2. Algorithme de décryptage RC5

L'étape de décryptage peut être résumée comme suit:

For I = r down to 1 do

B = ((B - S [2i+1]) >>> A) ⊕A;

A = ((A - S [2]) >>> B) ⊕B;

End

B = B-S [1];

A = A-S [0];

3.2.1.3. Expansion de clé

L'expansion des clés RC5 étend la clé secrèteK pour remplir le tableau de clés déployées S, ce qui fait que S est similaire à un tableau de t = 2 (r + 1) mots binaires aléatoires. Deux constantes magiques, P_w Et Q_w, sont utilisées dans ce processus. Ces constantes sont définies comme

P_w =Odd((e-2)2^w)

Q_w=Odd((Φ-1)2^w)

où

E = 2,718281828459 .... (base des logarithmes naturels)

Φ = 1.618033988749 .... (Rapport d'or)

Et Odd (x) est l'entier impair le plus proche de x. Pour w = 16 et 32, ces

Les constantes sont données en hexadécimal:

P16= b7e1; Q16= 9e37

P32= b7e15163; Q32= 9e3779b9,

L'expansion commence par copier la clé secrète K [0 .... b-1] dans un Tableau L [0 .... c-1] où c= [b/u] mots, et u = w / 8 est le nombre d'octets par mot. U octets de clé consécutifs de K sont utilisés pour remplir chaque mot successif dans L commençant pas l'ordre bas jusqu'à le haut. Tout les octets non remplis de L sont remplis pas zéro.

Pour initialiser le tableau S, nous utilisons les étapes suivantes:
S [0] = P_W;

For i= 1 to t-1 do

S [i] = S [i-1] + Q_W;

End

La dernière étape sert à inclure la clé secrète sans les tableaux S et L :

i = j = 0;

A = B = 0;

Do 3*max (t, c) times:

A = S [i] = (S [i] +A+B) <<<3;

B = L[j] = (L[j] + A+ B) <<< (A+B);

i = (i+1) mod (t);

j = (j+1) mod (c);

3.2.2. Algorithme RC6

Le RC6, qui est un cryptage par bloque, est une version modifiée de RC5 qui utilise quatre registres de travail au lieu de deux et la multiplication entière comme une opération primitive supplémentaire. Le processus de multiplication des nombres entiers améliore la diffusion obtenue par cycle, ce qui conduit à une plus grande sécurité avec moins d'itération et un débit étalé. Le calendrier des clés de RC6 est similaire à celui de RC5. La seuledifférence est que pour RC6, plus de mots dérivent de la clé fournie par l'utilisateur pendant le cryptage et le décryptage. L'utilisateur fournit une clé de b bytes, où $0 \leq b \leq 255$, et à partir de cette clé, 2r + 4mots (w bits chacun) sont dérivés et stockés dans le tableau S [0, ..., 2r + 3].Ce tableau est utilisé à la fois dans le cryptage et le décryptage.

Généralement, RC6 se compose de deux réseaux dont les données sont mélangées via des rotations de données. Les opérations dans un seul tour de RC6 contiennent deux applications de la fonction de quadrillage f (x) = x (2x + 1) mod 2^{32}, deux rotations fixes de 32 bits, deux rotations 32 bits dépendant de la donnée, deux XOR, et deux addition modulo 2^{32}.

Les étapes du cryptage RC6 et du décryptage sont résumées ci-après, et les diagrammes du bloque de cryptage et décryptage RC6 sont présentés dans les figures 3.2 et 3.3, respectivement.

3.2.2.1. RC6 Encryption Algorithm

Entrées: 4valeurs en clair (de taille w bits) A, B, C, et D

r: Nombre d'itération

S[0, …, 2r+3]: clé d'itérations (de taille w bits)

Sorties: 4 valeurs cryptées (de taille w bits) sauvegardées dans A, B, C, et D

Procedure: B = B + S [0]; D = D + S [1];

For i= 1 to r do

{t = (B × (2B + 1)) <<<lgw; u = (D × (2D + 1)) <<<lgw; A = ((A ⊕t) <<< u) + S [2i]; C = ((C ⊕u) <<< t) + S [2i + 1]; (A, B, C, D) = (B, C, D, A);}

End

A = A + S [2r + 2];

C = C + S [2r + 3];

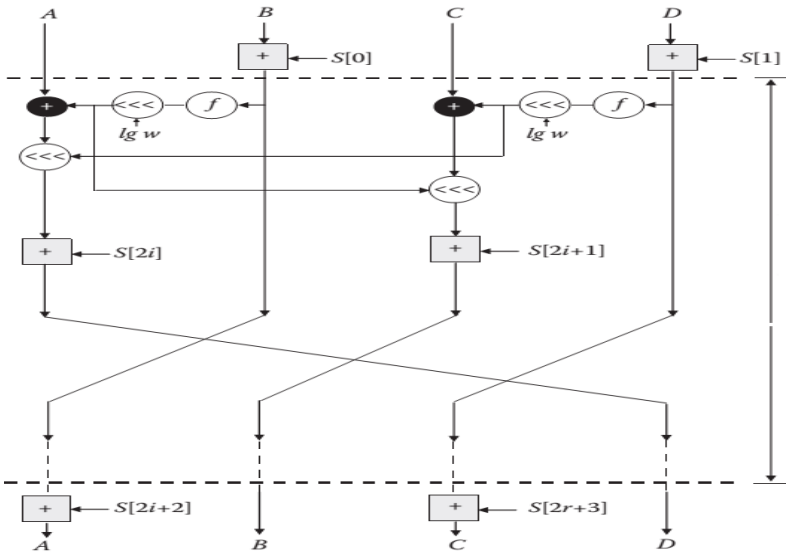


Figure 3.2 : Cryptage avec l'algorithme RC6[01]

3.2.2.2. RC6 Algorithme de décryptage RC6

Entrées: 4 valeurs cryptées (de taille w bits) sauvegardées dans A, B, C, et D

r: Nombre d'itération

S[0, …, 2r+3]: clé d'itérations (de taille w bits)

Sorties: 4 valeurs en clair (de taille w bits) A, B, C, et D

Procédure: B = B + S [0]; D = D + S [1];
Pour i = 1 à r do
{T = (B × (2B + 1)) <<<lgw; U = (D × (2D + 1)) <<<lgw; A = ((A ⊕t) <<< u) + S [2i]; C = ((C ⊕u) <<< t) + S [2i + 1]; (A, B, C, D) = (B, C, D, A);}
Fin
A = A + S [2r + 2];
C = C + S [2r + 3];

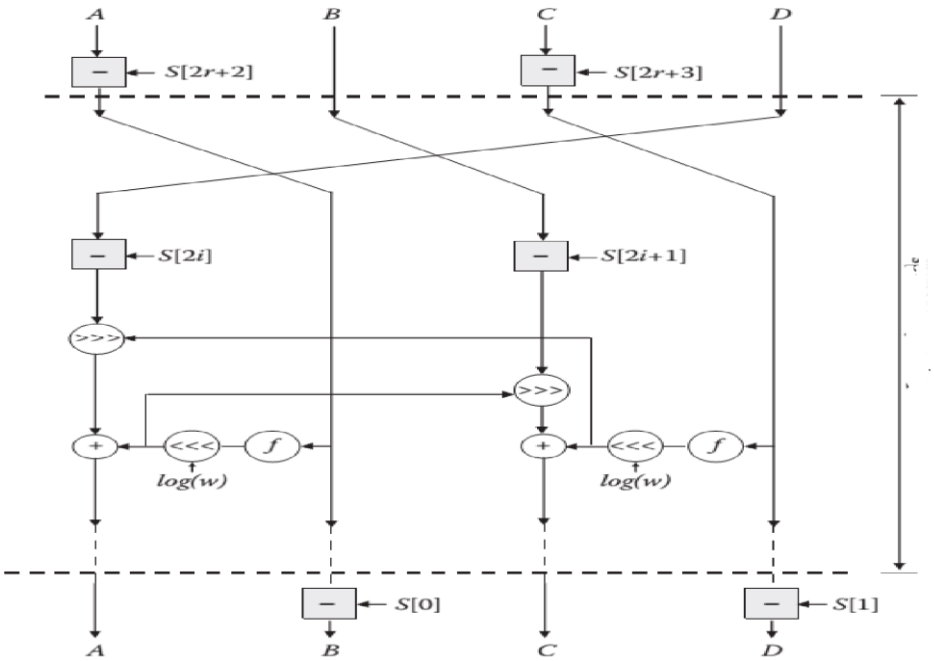


Figure 3.3 : Décryptage avec l'algorithme RC6 [01].

A = ((A − S [2i]) >>> u) ⊕t ;}

End

D = D − S [1]; B = B − S [0];

3.2.3. Algorithme XOR [02]

Origine : Le cryptage XOR est un système de cryptage basique mais pas trop limité. Ainsi, il a beaucoup été utilisé dans les débuts de l'informatique et continue à l'etre encore aujourd'hui car il est facile à implémenter, dans toutes sortes de programmes.

Mécanisme : Le XOR est un opérateur logique qui correspond à un « OU exclusif » : c'est le (A OU B) qu'on utilise en logique mais qui exclue le cas où A et B sont simultanément vrais, tableau suivant :

A	B	A XOR B
FAUX	FAUX	FAUX
FAUX	VRAI	VRAI
VRAI	FAUX	VRAI
VRAI	VRAI	FAUX

Table 3.2 : de vérité du XOR

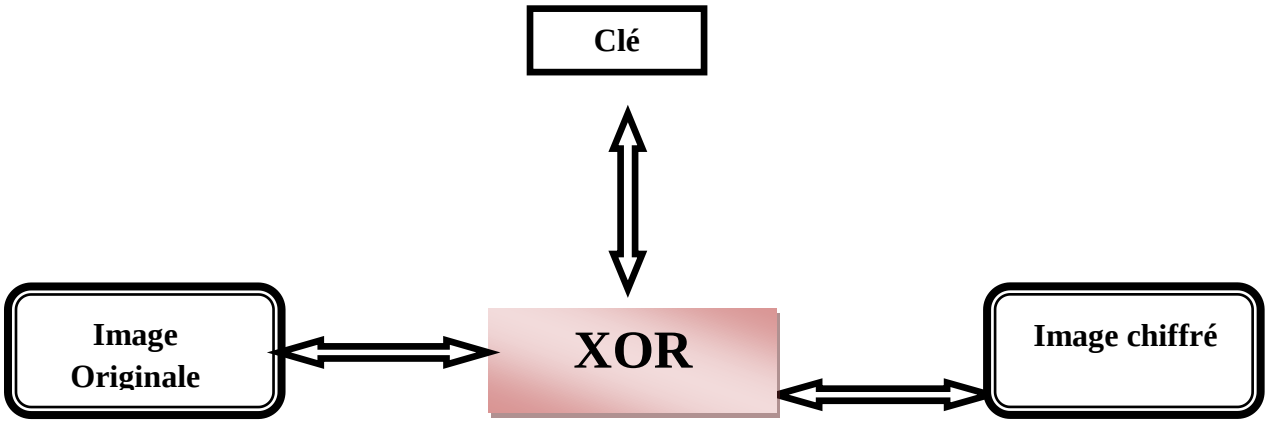


Figure 3.4 : schéma de principe de l'algorithme

3.3. Modes de chiffrement [03]

Les algorithmes de chiffrement fonctionnent soit par flux, c'est à dire qu'ils prennent chaque Octet du texte en clair au fil de l'eau et le chiffre, soit ils fonctionnent par blocs, c'est à dire qu'ils prennent en paramètre un certain nombre d'octets (on parle plutôt en bits) du message en clair pour le chiffrer.

Afin de chiffrer des messages longs (d'une taille plus grande qu'un seul bloc), nous avons plusieurs façons de procéder.

3.3.1. Mode Electronique Code Block (ECB)

Ceci est le mode de chiffrement le plus simple. On prend chaque partie du texte clair que nous chiffrons avec l'algorithme de chiffrement symétrique choisi (exemple : AES).

Le déchiffrement est identique, en remplaçant le texte en clair par le texte chiffre. La figure 3.5 montrent le fonctionnement.

Le principal désavantage de cette méthode est que deux messages en clair identiques donneront le même texte chiffre. La conséquence a cela est qu'on ne cache pas les motifs qui peuvent être utilises dans le texte clair dans son intégralité.

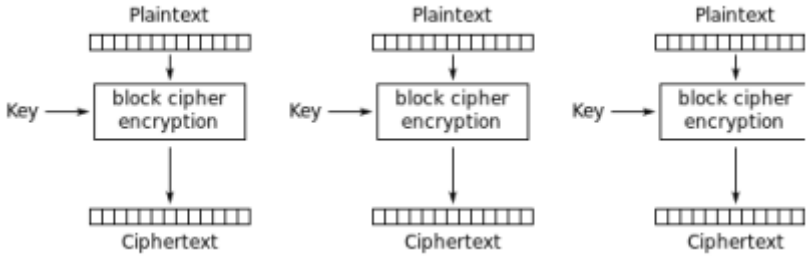


Figure 3.5 : Electronic codebook (ECB) mode encryption [03]

3.3.2. Mode Cipher Block Chaining (CBC)

Un autre mode possible est le chiffrement par chainage de blocs (Chiper Block Chaining, CBC).Cela veut dire que nous utilisons un vecteur d'initialisation (IV, une suite de bits arbitraires et uniques) et le premier bloc du message que nous souhaitons chiffrer, nous appliquons une opération XOR sur ces deux parties, puis nous chiffrons le bloc. Le bloc chiffre est ensuite réutilise comme faisant partie du texte chiffre final mais aussi comme vecteur d'initialisation pour le bloc suivant et ainsi de suite jusqu'a arriver a un message chiffre complètement. Le déchiffrement est effectue en prenant un bloc du texte chiffre et en le faisant déchiffre par l'algorithme de chiffrement précédemment utilise, puis on applique une opération XOR avec le résultat et le vecteur d'initialisation utilise précédemment pour le chiffrement. Ce même bloc de texte chiffre est réutilise comme le vecteur d'initialisation pour le bloc suivant. Le fonctionnement est explique sur les figures 3.6 et 3.7.

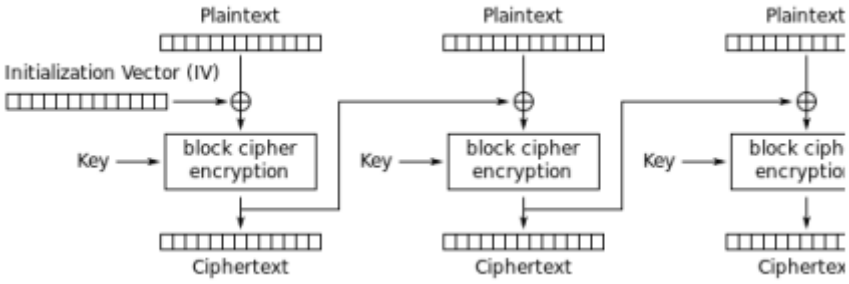


Figure 3.6: Cipher Block Chaning (CBC)mode encryption[03]

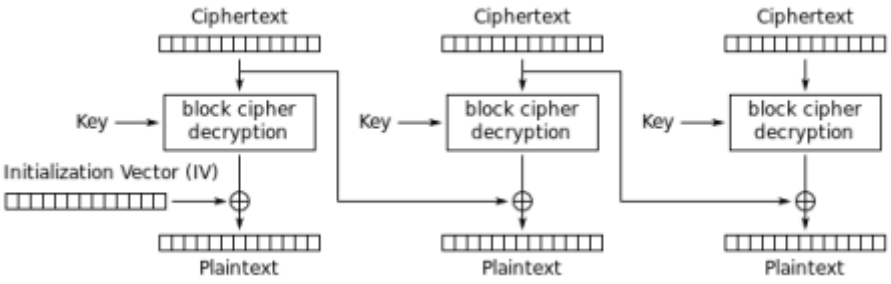


Figure 3.7: Cipher Block Chaining (CBC) mode decryption [03]

3.3.3. Modes de flot Mode CFB [04]

3.3.3.1.Définition

Le mode CFB (Chiper Feedback) fabrique un registre à décalage en mode CTAK (CipherText Auto Key), pour obtenir un chiffrement de flot. Le mode CFB est paramètre par un entier l inferieur à b et utilise un registre de b bits, initialise par une valeur publique IV (Initial Value) convenue a l'avance. Le message est découpe en blocs de taille l. A chaque coup d'horloge, on calcule l'image du registre par E_K, dont on extrait l bits qu'on appelle r_i . Le bloc est chiffre par ou exclusif : $c_i = m_i \oplus r_i$. La nouvelle valeur du registre est obtenue en faisant un décalage de l bits, et en y entrant la valeurc_i.

Chiffrement	$s_{-1} = \mathsf{IV}$	$r_i = [\mathsf{E_k}(s_{i-1})]_{(1\ldots\ell)}$	$c_i = m_i \oplus r_i$	$s_i = [s_{i-1}]_{(\ell+1\ldots b)} \| c_i$
Déchiffrement	$s_{-1} = \mathsf{IV}$	$r_i = [\mathsf{E_k}(s_{i-1})]_{(1\ldots\ell)}$	$m_i = c_i \oplus r_i$	$s_i = [s_{i-1}]_{(\ell+1\ldots b)} \| c_i$

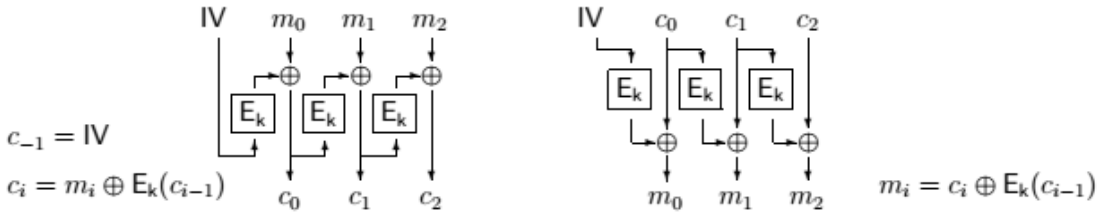


Figure 3.8 :Chiffrement et déchiffrement en mode CFB, avec l = b.[04]

3.3.3.2.Propriétés :

- Expansion.

Si la valeur de IV a été convenue a l'avance, c'est un mode sans expansion : si la longueur du message n'est pas un multiple de l, on utilise une valeur tronquée pour le dernier r_i

- Performance.

Le chiffrement CFB ne peut être parallélise, mais le d chiffrement CFB peut être totalement parallélise.

Le chiffrement et le déchiffrement utilisent tous deux la fonction E_K, et donc le temps de calcul de D_K n'a aucune influence sur les performances du mode CFB. En revanche, il faut un appel à E_K tous les l bits du message.

- Résistance aux erreurs de transmission.

Si un bloc c_i est modifie, seul le bloc m_i et quelques autres seront modifiés.

Si un nombre de bits multiple de l est perdu par la transmission, seuls les blocs correspondants sont perdus.

- Sécurité.

Le mode CFB ne présente aucune détection d'intégrité et est donc vulnérable aux attaques actives. Comme le mode CBC, c'est à partir du chiffrement de $2^{b/2}$blocs qu'un attaquant obtient éventuellement de l'information sur le message (grâce au paradoxe des anniversaires).

Les contraintes de sécurité sur la fonction E_K sont d'autant moins sévères que l est petit.Il n'y a pas d'objection à chiffrer plusieurs messages avec la même clef, avec une valeurIV différente a chaque fois, si cette valeur est choisie aléatoirement. On conseille donc dans ce contexte l'utilisation de E_K(IV) au lieu de IV.

3.3.4. Mode OFB

3.3.4.1.Définition

Le mode OFB (Output Feed Back) fabrique un registre à décalage en mode KAK (Key Auto Key), pour obtenir un chiffrement de flot .Le mode OFB est paramétré par un entier l inferieur à b et utilise un registre de b bits, initialisé par une valeur publique IV (Initial Value) convenue a l'avance. Le message est découpe en blocs de taille l.A chaque coup d'horloge, on calcule l'image du registre par $E_K$dont on extrait l bits qu'on appellerr_i. Le bloc est chiffré par ou exclusif : $c_i = m_i \oplus r_i$. La nouvelle valeur du registre est obtenue en faisant un décalage de l bits, et en y entrant la valeur r_i.

Chiffrement	$s_{-1} = \mathsf{IV}$	$r_i = [\mathsf{E_k}(s_{i-1})]_{(1\ldots\ell)}$	$c_i = m_i \oplus r_i$	$s_i = [s_{i-1}]_{(\ell+1\ldots b)} \| r_i$
Déchiffrement	$s_{-1} = \mathsf{IV}$	$r_i = [\mathsf{E_k}(s_{i-1})]_{(1\ldots\ell)}$	$m_i = c_i \oplus r_i$	$s_i = [s_{i-1}]_{(\ell+1\ldots b)} \| r_i$

$s_{-1} = \mathrm{IV} \quad s_i = \mathrm{E_k}(s_{i-1})$

$c_i = m_i \oplus s_i$

$m_i = c_i \oplus s_i$

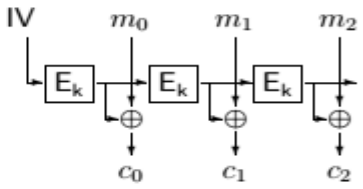


Figure 3.9 : Chiffrement ou déchiffrement en mode OFB, avec l= b[04]

3.3.4.2.Propriétés :

- Expansion.

Si la valeur de IV a été convenue a l'avance, c'est un mode sans expansion : si la longueur du message n'est pas un multiple de l, on utilise une valeur tronquée pour le dernier r_i.

- Performance.

Le chiffrement ni le déchiffrement OFB ne peuvent être parallélises. La séquence des s_i peut être pré calculée avant de connaître le message.Le chiffrement et le déchiffrement utilisent tous deux la fonction E_K, et donc le temps de calcul de D_K n'a aucune influence sur les performances du mode OFB. En revanche, il faut un appel à E_K tous les l bits du message.

- Résistance aux erreurs de transmission.

Si un bloc $c_i$est modifie, seul le bloc m_i sera modifié.

Si quelques bits sont perdus par la transmission, toute la fin du message est perdue.

- Sécurité.

Le mode OFB ne présente aucune détection d'intégrité et est donc vulnérable aux attaques actives. Les contraintes de sécurité sur la fonction E_K sont d'autant moins sévères que l est petit. Pour $l = b$, si on utilise une fonction E_K in distinguable d'une permutation aléatoire, alors la valeur s_i fera un cycle avant d'avoir parcouru les 2^b valeurs possibles. On pourra donc préférer utiliser un système de chiffrement par blocs tel que chaque permutation E_K a un unique cycle. Il n'y a pas d'objection à chiffrer plusieurs messages avec la même clef, avec une valeur IV différente a chaque fois, si cette valeur est choisie aléatoirement. On conseille donc dans ce contexte l'utilisation de E_K (IV) au lieu de IV.

3.4. Mesure de l'évaluation du cryptage[01]

Cette section traite en détail de deux familles de paramètres de cryptage; La première famille évalue la capacité de l'algorithme de cryptage à remplacer L'image originale avec une image chiffrée. Dans cette famille, on étudie cinq mesures: Déviation d'histogramme (histogram deviation) D_H, le coefficient de corrélation r_{xy}, Déviation irrégulière (irregular deviation) D_I, l'histogramme L'uniformité et l'écart par rapport à l'idéalité. La deuxième famille évalue Les caractéristiques de diffusion de l'algorithme de cryptage.

Dans cette famille, trois mesures sont étudiées: l'effet avalanche, le nombre de taux de changement de pixels (NPCR) et l'intensité changeante moyenne unifiée (UACI).

3.4.1. Déviation d'histogramme (Histogram Deviation)

La déviation d'histogramme mesure la qualité du cryptage en termes de façon de maximiser l'écart entre l'original et les images cryptées. Les étapes pour calculer cette métrique sont les suivantes:

1. Estimation de l'histogramme de l'image originale et cryptée.

2. Estimez la différence absolue entre les deux histogrammes.

3. Estimez la zone sous la courbe de différence absolue divisée par la surface totale de l'image comme suit:

$$D_H = \frac{\frac{d_0+d_{255}}{2}+\sum_{i=1}^{254} d_i}{M \times N} \qquad (3.1)$$

Où d_i est l'amplitude de la différence absolue au niveau de gris i. M et N sont les dimensions de l'image à chiffrer. Plus la valeur de D_H est élevée, meilleure est la qualité de l'image cryptée. Bien que cette métrique donne de bons résultats sur la façon dont l'image cryptée déviante de l'image d'origine.

3.4.2. Coefficient de corrélation (correlation coffcient)

Une mesure utile pour évaluer la qualité de cryptage de tout crypto-système d'image est le coefficient de corrélation entre les pixels aux mêmes indices dans la plaine et les images chiffrées. Cette métrique peut être calculée comme suit:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (3.2)$$

Où x et y sont les images simples et de chiffrement. Dans les calculs numériques, Les formules discrètes suivantes peuvent être utilisées:

$$E(x) = \frac{1}{L}\sum_{l=1}^{L} x_l \quad (3.3)$$

$$D(x) = \frac{1}{L}\sum_{l=1}^{L}(x_l - E(x))^2 \quad (3.4)$$

$$cov(x,y) = \frac{1}{L}\sum_{l=1}^{L}\big(x_l - E(x)\big)(y_l - E(x)) \quad (3.5)$$

Où L est le nombre de pixels impliqués dans les calculs. Plus la valeur de r_{xy} est proche de zéro, meilleure sera la qualité de l'algorithme de cryptage.

3.4.3. Déviation irrégulière (Irrgular Deviation)

La déviation irrégulier mesure la qualité du cryptage en termes de combien la déviation causé par le cryptage (sur l'image cryptée) est irrégulier. Les étapes pour calculer cette métrique sont les suivantes:

1. Calculer la différence absolue entre l'image cryptée et l'image originale.

2. Estimation de l'histogramme H de cette matrice de différence absolue.

3. Estimez la valeur moyenne M_H de cet histogramme.

4. Estimez l'absolue des écarts d'histogramme par rapport à cette valeur moyenne comme suit:

$$H_D(i) = |H(i) - M_H| \quad (3.6)$$

L'écart irrégulier D_I est calculé comme suit:

$$D_I = \frac{\sum_{i=0}^{255} H_D(i)}{M \times N} \tag{3.7}$$

Plus la valeur de D_I est faible, meilleure sera la qualité de cryptage.

3.4.4. NPCR et UACI

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.Le NPCR est défini comme

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{3.8}$$

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

L'UACI est défini comme

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% \tag{3.9}$$

Il mesure l'intensité moyenne des différences entre les deux images. Plus les valeurs de NPCR et UACI sont élevées, plus le cryptage sera élevé.

3.4.5. Immunité au bruit

L'immunité au bruit reflète la capacité du crypto-système d'image à tolérer le bruit. Pour tester l'immunité au bruit, le bruit avec différents rapports signal-bruit (SNR) est ajouté à l'image cryptée, puis l'algorithme de décryptage est effectué. Si l'image déchiffrée est proche de l'image originale, on peut dire que le crypto-système en main est à l'abri de bruit. Cette proximité peut être vérifiée visuellement ou numériquement avec la valeur de rxyd, qui représente le coefficient de corrélation entre l'image d'origine et l'image déchiffrée et le rapport signal / bruit de pointe (PSNR) de l'image déchiffrée, qui est définie comme suit :

$$PSNR = 10 \times log_{10}\left[\frac{M \times N \times 255^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}|(f(m,n)-f_d(m,n)|^2}\right] \quad (3.10)$$

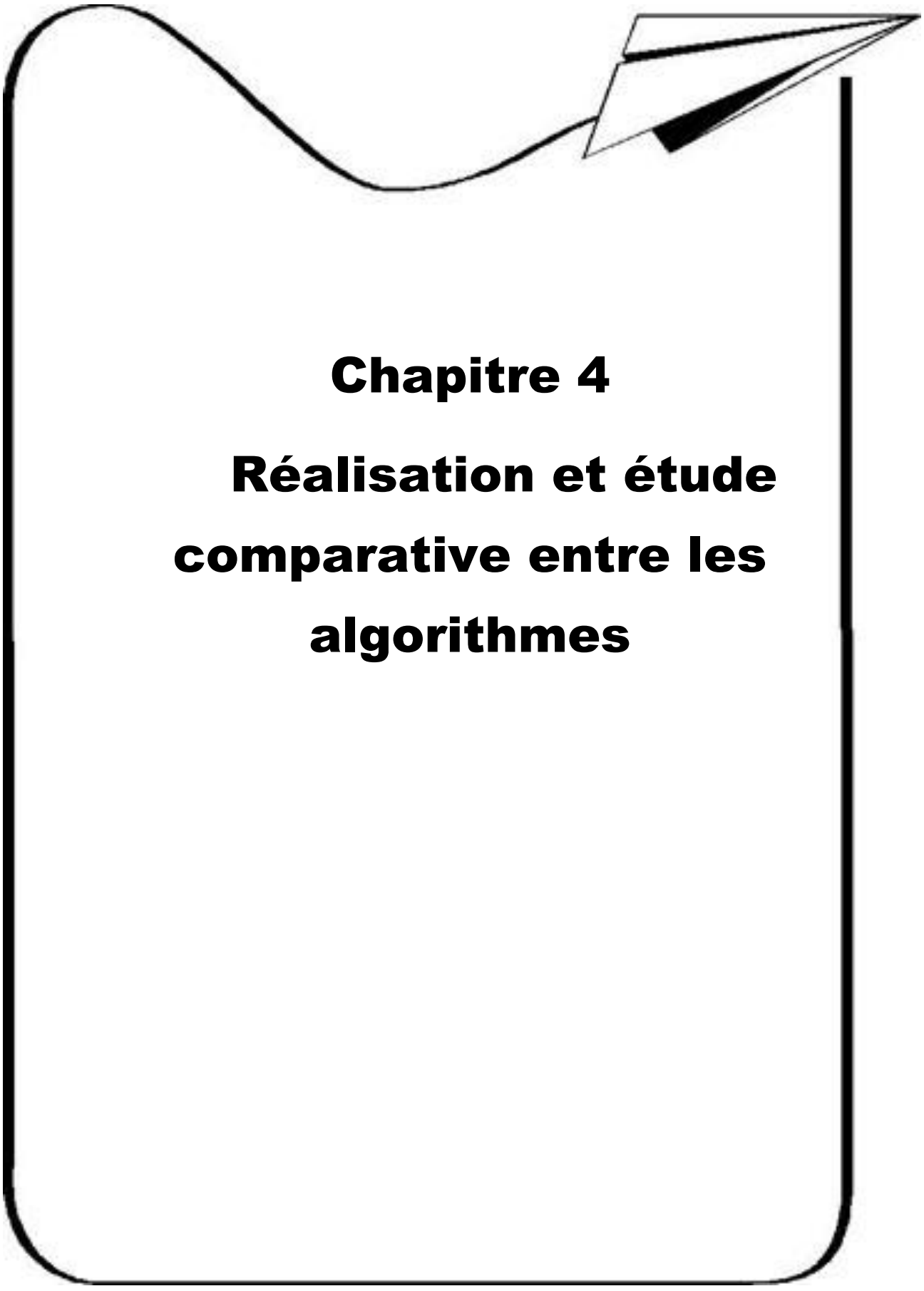
Où $f\ (m,n)$ est l'image originale, et $f_d(m,n)$ est l'image déchiffrée.

3.4.6. Le temps de traitement

Le temps de traitement est le temps requis pour crypter et décrypter une image. Plus la durée de traitement n'est faible, meilleure sera l'efficacité du cryptage.

3.5. Conclusion :

En conclusion, nous avons présenté dans ce chapitre tous les outils que nous appliquerons dans le dernier chapitre des algorithmes (RC5 ,RC6 et XOR) et modes de chiffrement (ECB CBC CFB OFB) et Mesure de l'évaluation du cryptage($D_{H,}$ r_{xy} , D_I, NPCR , UACI , $PSNR$ Le temps de traitement).



Chapitre 4

Réalisation et étude comparative entre les algorithmes

4.1. Introduction

Ce chapitre tente de présenter une comparaison équitable entre les algorithmes RC5, XOR et RC6les plus utilisées dans le domaine de cryptage de données. Pour comprendre les privilèges pour RC6 ajoutés par RC5 Et l'impact sur l'efficacité de chaque Modes d'opération (ECB , CBC, CFB et OFB).

Ce chapitre est divisé en 2 parties :

- Partie 1 : Présentation de l'application.
- Partie 2 : évaluation de la qualité de cryptage de ces algorithmes.

4.2. Environnement de développement

Avant de commencer l'implémentation de l'application, il y a lieu d'abord de spécifier les outils utilisés et que l'on être le bon choix vu les avantages fournis par le logiciel de renommée tel que MATLAB.

4.2.1. Ressources matériel

On a développé notre application sur une machine de microprocesseur Core i3 avec 1.70 GHz de mémoire RAM 4.00 GO.

4.2.2. Logiciels

Concernant les ressources logicielles un Microsoft Windows 7 Edition Intégrale est installée sur cet ordinateur, avec langage de programmation MATLAB 13.0 qui est utilisée pour l'implémentation du travail.

MATLAB peut être utilisé dans une grande variété d'applications, incluant le traitement d'images.

4.2.3. Les images utilisées pour étudier

Comme il apparaît dans la figure 4.1**,** nous avons utilisé huit (8) photos de différentes tailles et d'extension.

Figure 4.1 : Les images utilisées pour étudier

Afin d'appliquer les critères pour faire sa conversion gris est représentée sur la Figure 4.17

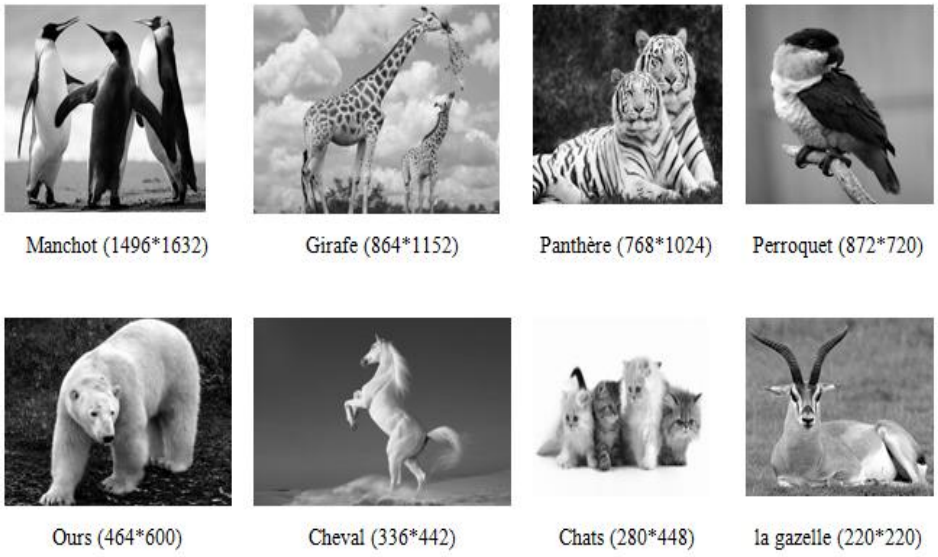


Figure 4.2 : Les images utilisées pour étudier avec gris

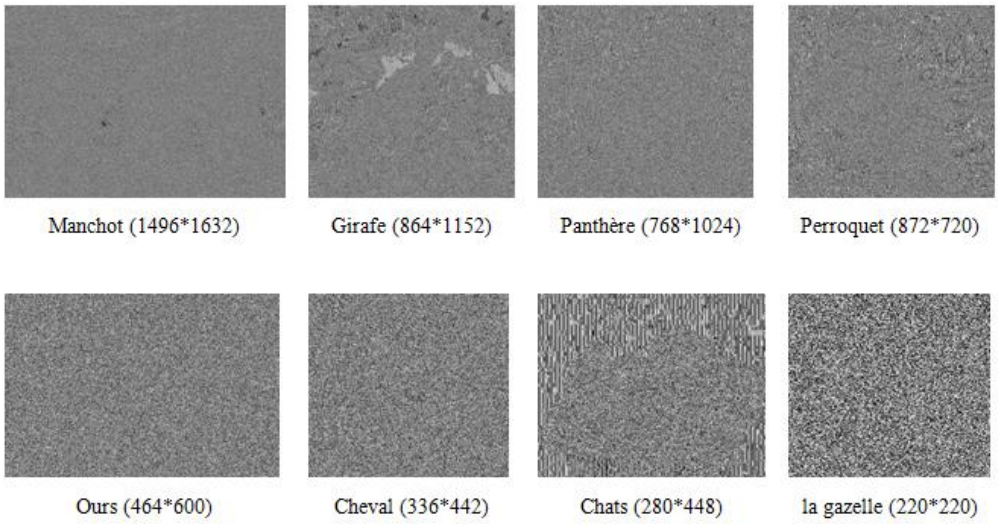


Figure 4.3 : Images d'encrypté d'algorithme RC5 en modes de chiffrement ECB

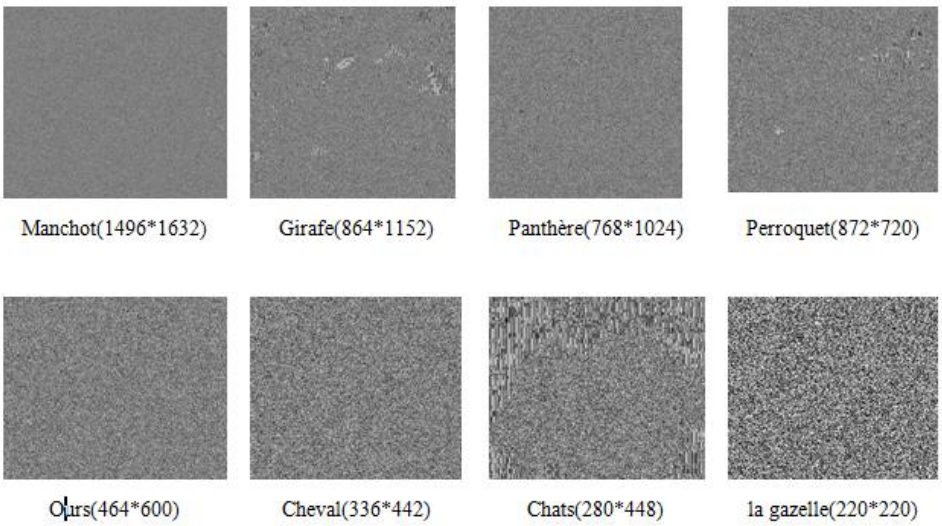


Figure 4.4 : Images d'encrypté d'algorithme RC6 en modes de chiffrement ECB

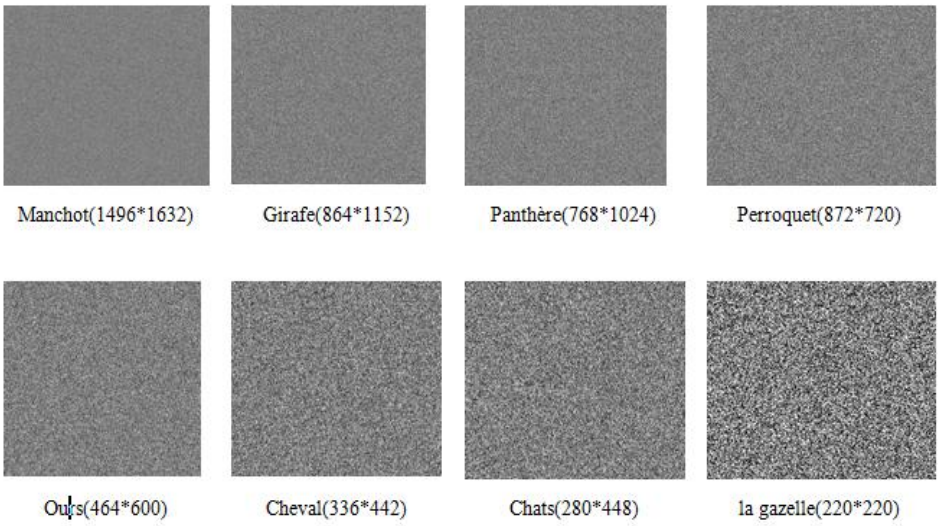


Figure 4.5 : Images d'encrypté d'algorithme XOR

4.3. Présentation de l'application

Afin d'étudier les algorithmes de cryptographie, on a développé cette application de chiffrement reparti selon le mode de chiffrement pour sécuriser les images qui on composé les sept Interfaces graphiques de notre application, Ceci est la première interface sous la Figure 4.6

Figure 4.6 : La première Interface graphique de L'application

Après avoir appuyé sur l'entrée, on passe à la deuxième interface à travers laquelle on définit comment introduire l'image comme il apparaît dans figure 4.7

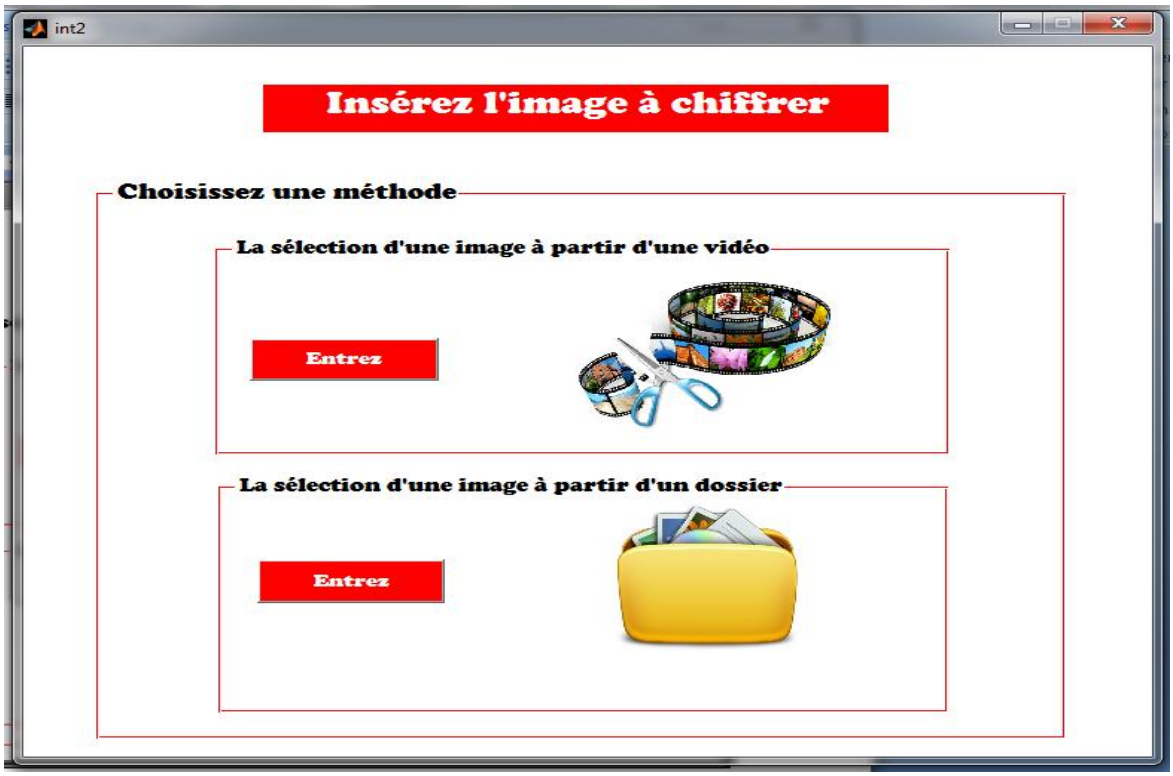


Figure 4.7: la seconde interface graphique de L'application

Sur la figure4.7, on peut déterminer l'image à coder de deux manières :

Elle peut être pris d'une vidéo après la conversion en une série d'images et de l'enregistrer dans un dossier à condition que l'extension d'une vidéo.wmv, après avoir cliqué sur l'entrée en panel la sélection d'une image à partir d'une vidéo voir l'interface figure 4.8

Figure 4.8 : La sélection d'une image à partir d'une vidéo

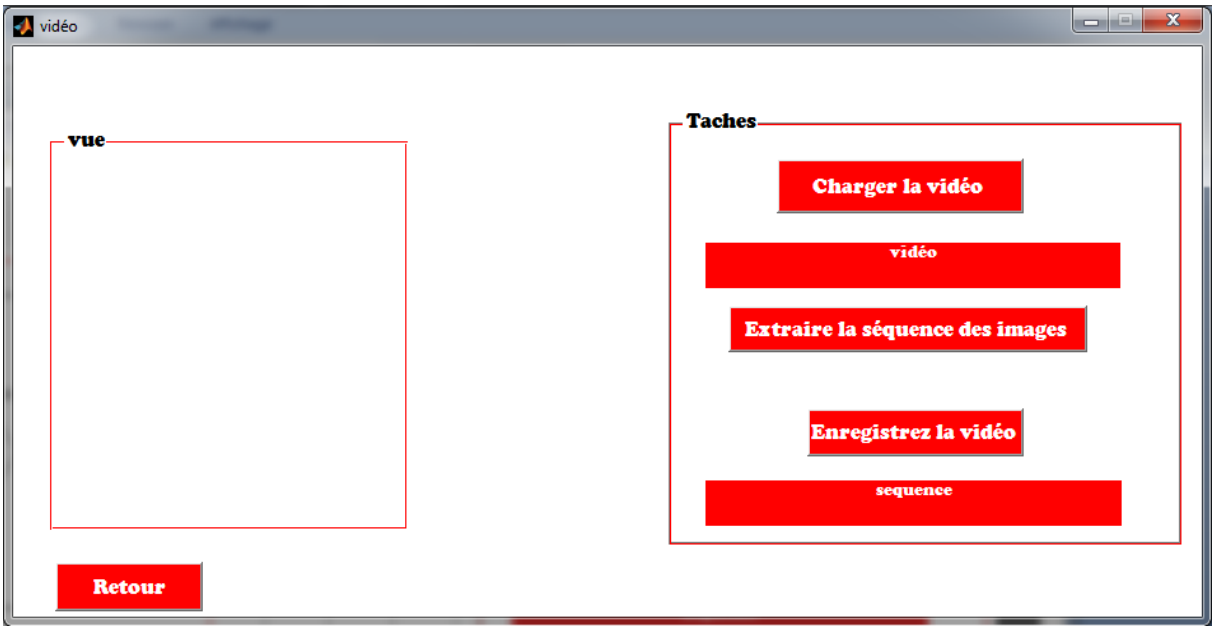


Figure 4.9 : L'interface sélection d'une image à partir d'une vidéo avant la sélection

Après avoir appuyé sur le bouton charger la vidéo Identifier la vidéo à partir de tout point connecté à l'ordinateur, ensuite on montre l'adresse au fond de celui-ci de vidéo sélectionné , ensuite appuyé sur bouton extraire la séquence des images et affiche l'image du deuxième vidéo, puis sur bouton enregistrez la vidéo, puis images de réservation dans l'adresse qui apparaît en bas dans figure 4.10

Figure 4.10 :L'interface sélection d'une image à partir d'une vidéo après la sélection

Ensuite, nous persévérons bouton Retour, retour à nous la seconde interface graphique de l'application comme le montre la figure 4.7. On choisit cette fois-ci la sélection d'une image à partir d'un dossier et faire appuyer sur le bouton Entrez tel il est indiqué dans figure 4.11

Figure 4.11 : La sélection d'une image à partir d'un dossier

Dans figure 4.12et après avoir appuyé sur bouton sélectionnez l'image, nous sélectionnons l'image de tout point connecté à votre ordinateur quelle que soit l'extension et type (couleur ou gris) ensuite on montre l'image dans l'interface et toutes les informations, telles que extension et taille, Par exemple, après que nous identifions l'image girafe voir la figure 4.13

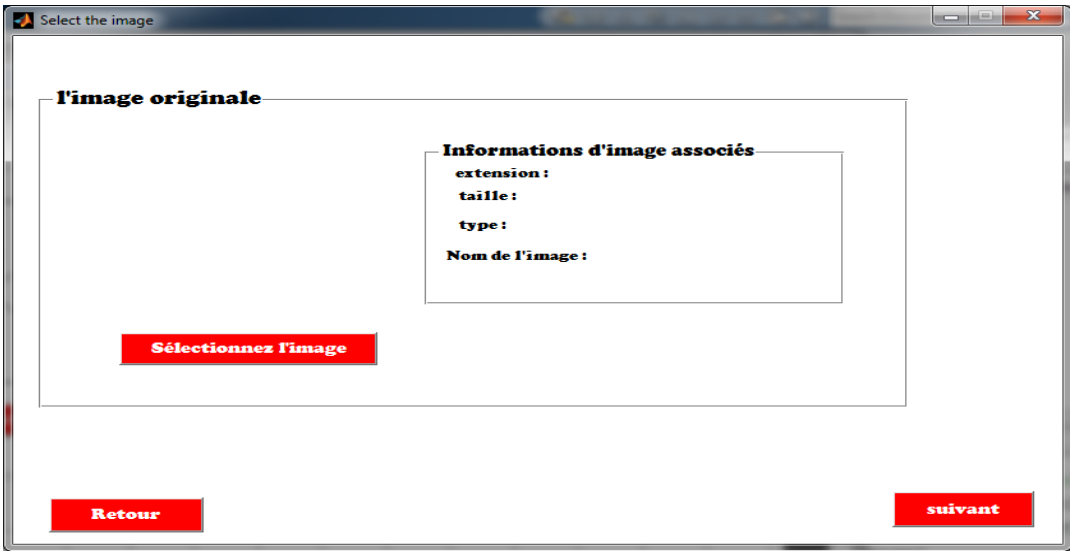


Figure 4.12:interface Sélection d'une image avant la réalisation

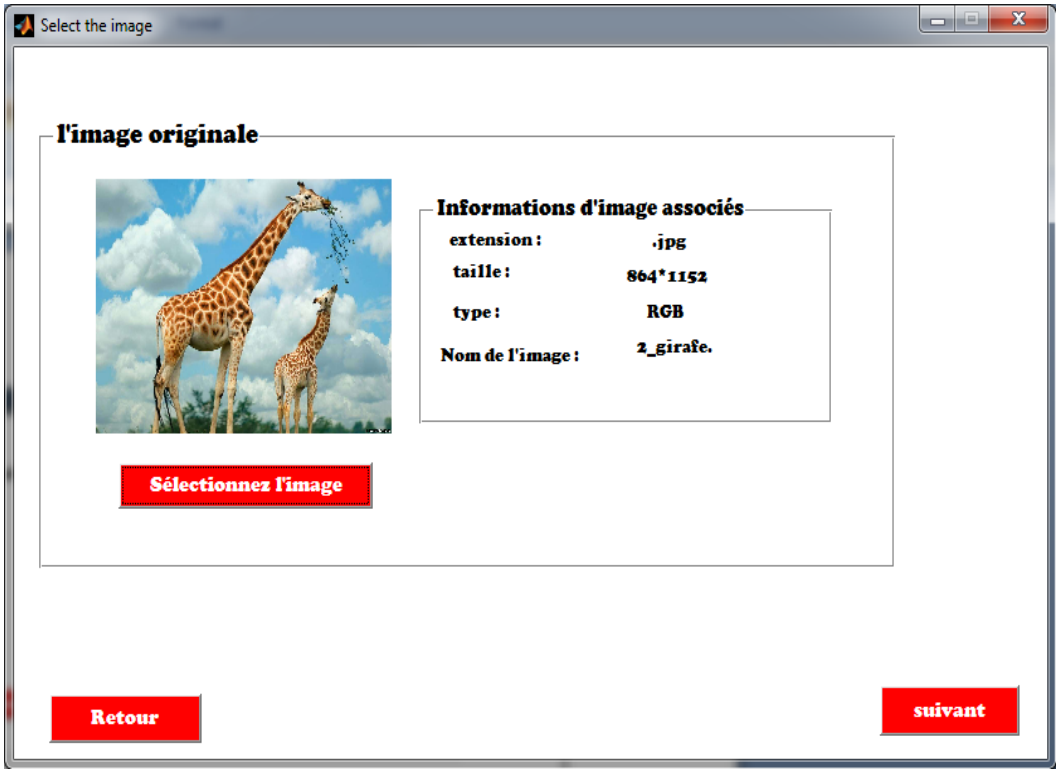


Figure 4.13 : interface Sélection d'une image après la réalisation

Nous pouvons battre en retraite pour revenir à la forme précédente et nous pouvons également continuer à faire pression sur bouton suivant pour montrer l'interfacer pour la détermination de l'algorithme de cryptage et modes d'opération figure 4.14 , comme d'habitude, nous pouvons battre en retraite que nous pouvons continuer après sélection

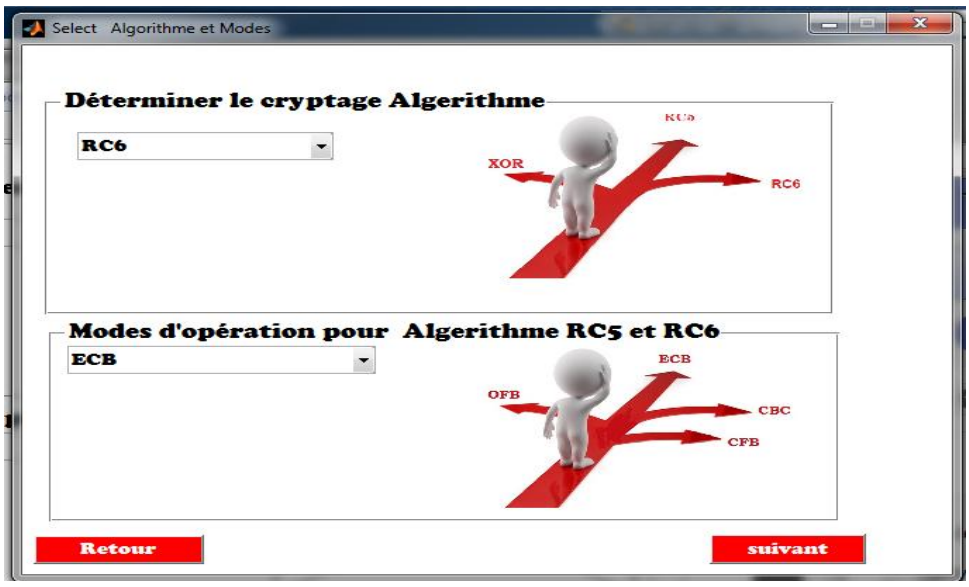


Figure 4.14 : interface Déterminer le cryptage algorithme et modes d'opération

Si vous sélectionnez algorithme XOR L'interface suivante est ***Figure 4.15***

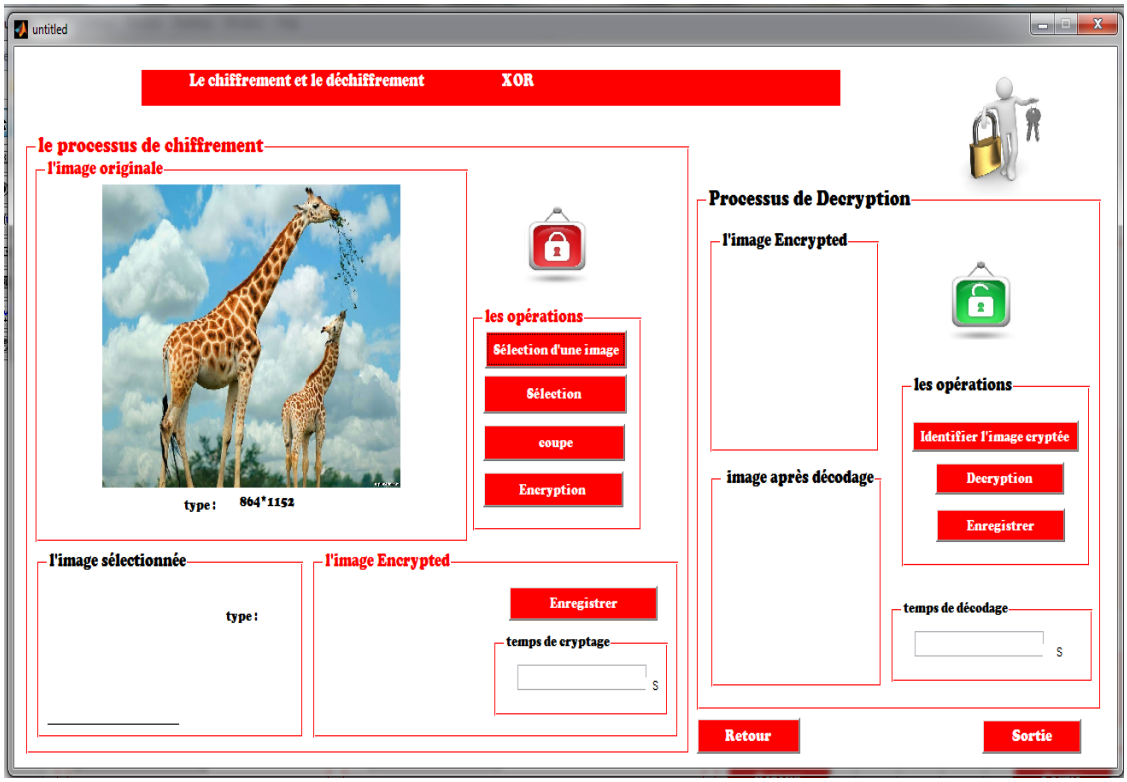


Figure 4.15 : interface Le chiffrement et le déchiffrement XOR avant la réalisation

Après avoir appuyé sur la sélection montrons la naissance afin de déterminer l'espace de l'image, mais la pièce n'est pas nécessaire parce qu'un XOR rapide et la pièce peut déterminer toute l'image. Après la pièce, cryptons l'image codée avec le temps qu'il faut comme dans la figure 4.16 dans l'espace. Le processus de chiffrement après cela, nous montrent l'image que nous pouvons nous sauver chiffré le nom de toute extension et est mis en place lors de la perte d'informations, telles que (jpg), Il est préférable d'utiliser PMB Parce qu'il présente moins de perte d'informations.

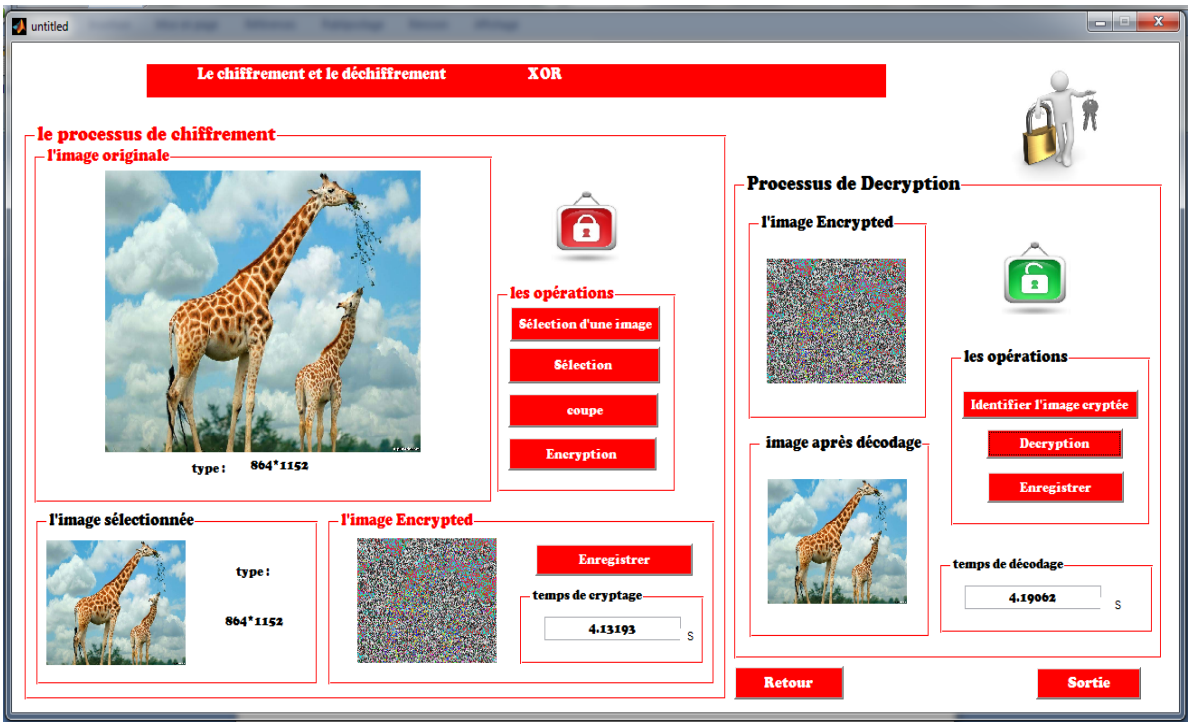


Figure 4.16 : interface Le chiffrement et le déchiffrement XOR après la réalisation

On note également que la taille 864*1152 de l'image girafe qui ont été codés en un temps d'environ 4 secondes, dans l'espace Le processus de décryptage après avoir appuyé sur bouton Identifier l'image cryptée. Nous pouvons déterminer l'image cryptée à partir de tout point connecté à l'ordinateur et nous affiche dans l'espace l'image encryptée après avoir appuyé sur le bouton décryptions.

Le décodage se fait et affiche l'image dans l'espace image et le temps montre également le décodage et l'affichage dans l'espace-temps de décodage. Si nous choisissons, par exemple, l'interface RC5 qui apparaîtra figure 4.17

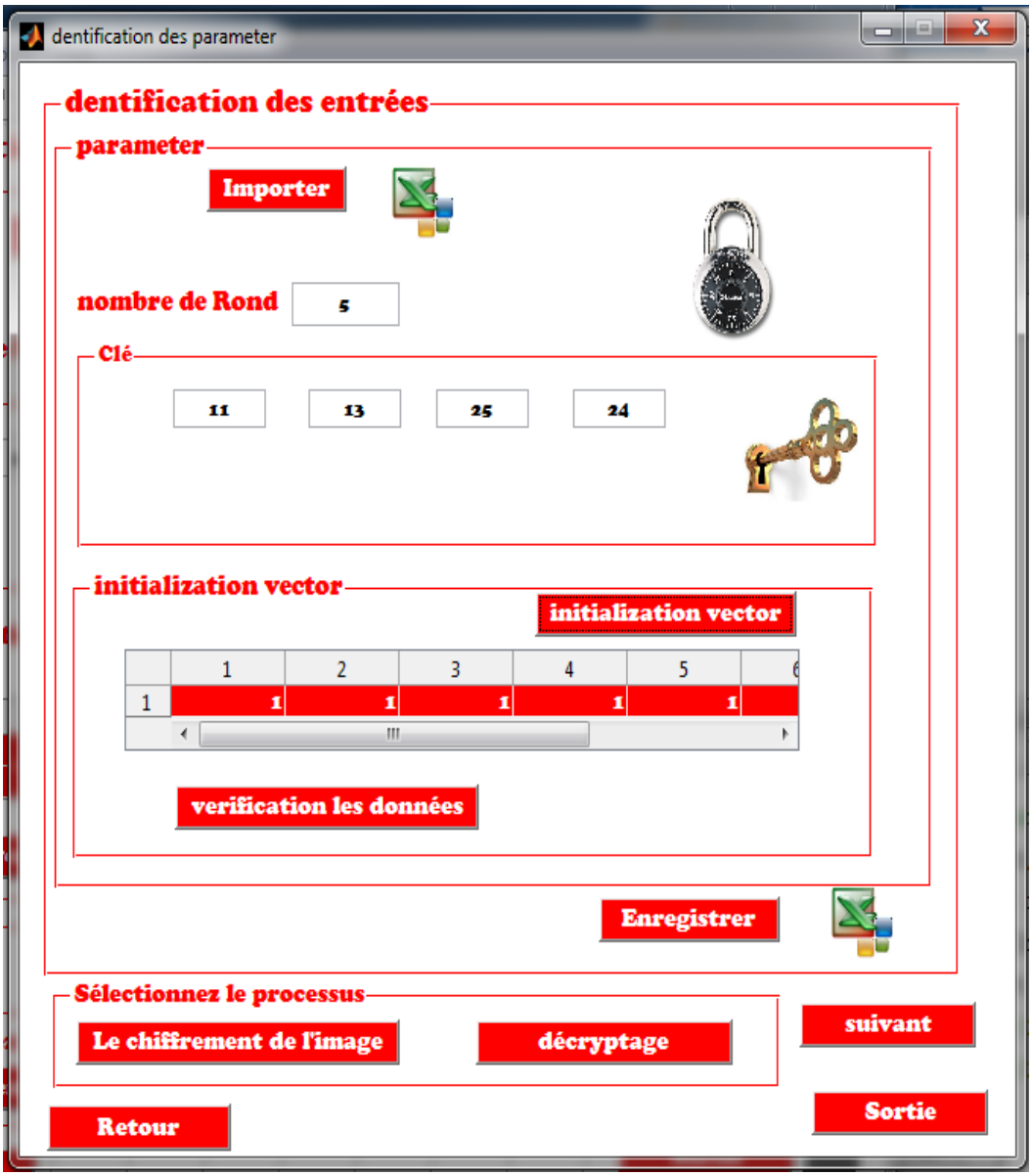


Figure 4.17 : interface densification de paramètre RC5 et RC6

Les principales valeurs pour chaque critère pour calcul. On peut changer ces valeurs que nous pouvons les sauvegarder le retour ou la sortie, plus important encore, la pièce dans l'espace sélectionnez le processus, là où nous avons deux boutons. Le chiffrement de l'image et décryptage, si vous appuyez sur le bouton le chiffrement de l'image il nous montrera la forme figure 4.18

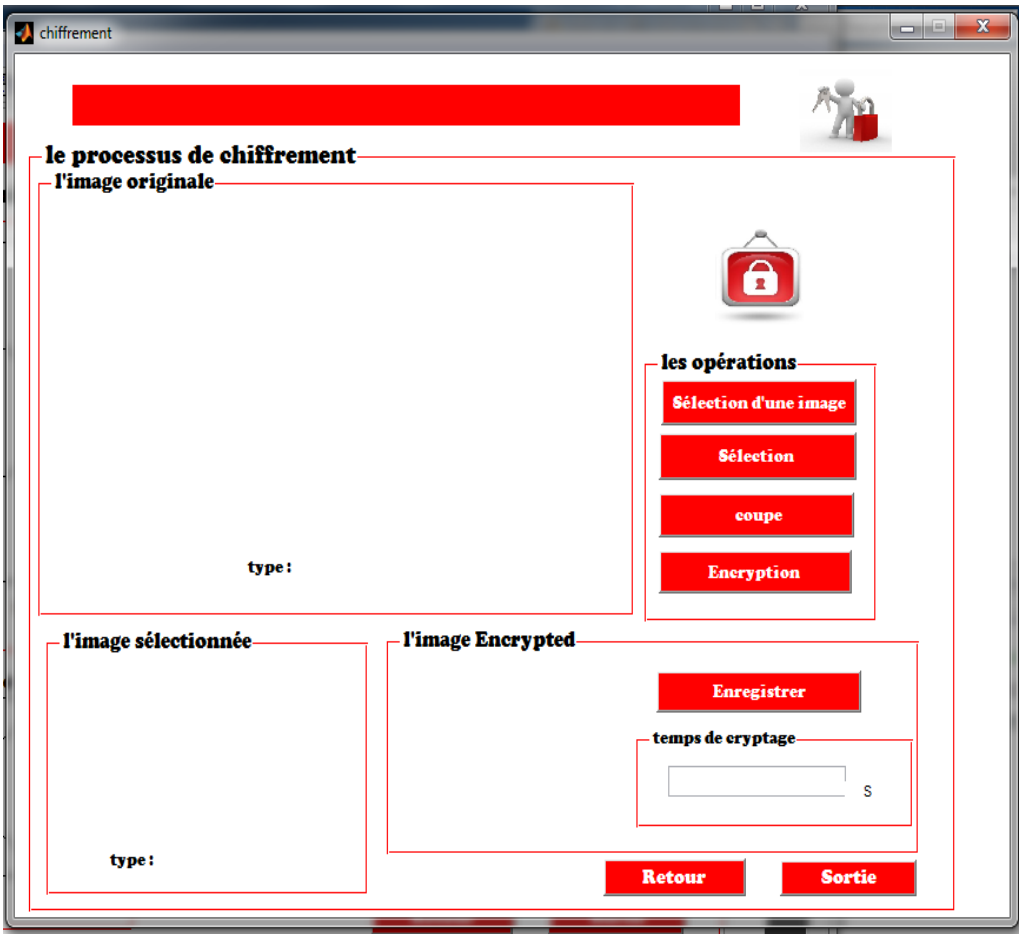


Figure 4.18 : Le chiffrement RC5 et RC6 avant la réalisation

Avant la sélection d'une image et déterminer l'espace à chiffrer et la pression de cryptage nous montre l'interface figure 4.19 et déterminer l'espace à chiffrer et la pression de cryptage l'interface obtenue. On peut noter, le plus grand temps de cryptage d'entre eux par rapport à XOR ici au profit de l'espace telle apparue dans la Figure 4.20

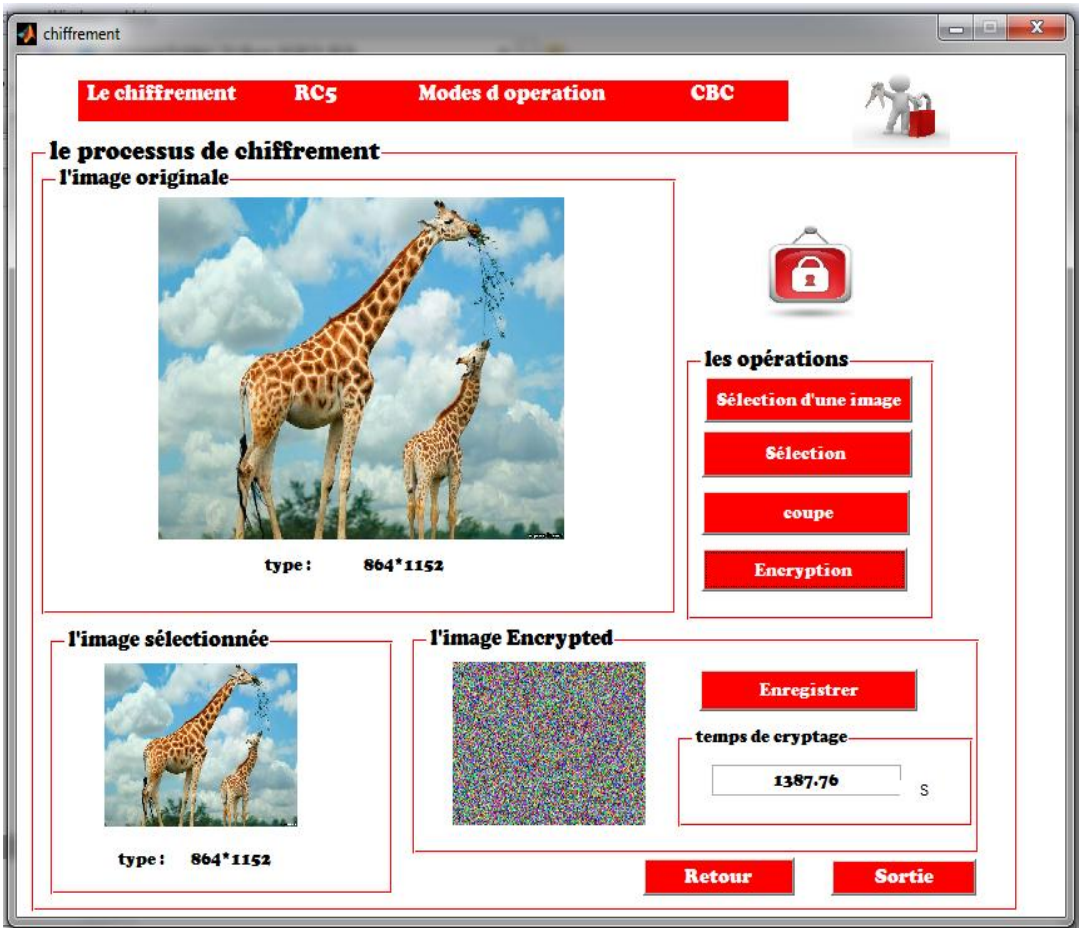


Figure 4.19: Le chiffrement RC5 et RC6 après la réalisation

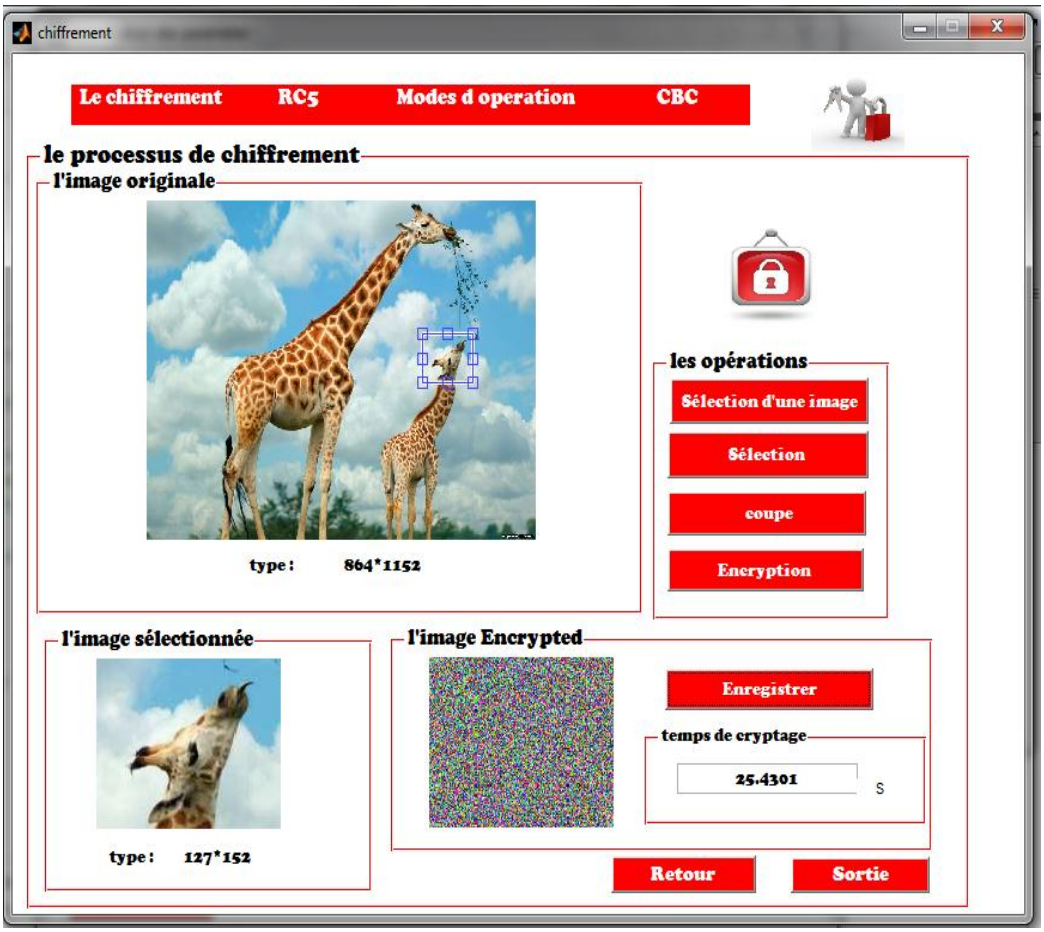


Figure 4.20 : Le chiffrement RC5 et RC6 lorsque vous sélectionnez une image à partir

Après une pression sur le bouton Retour, on choisit de revenir sur décoder comme dans la figure 4.21

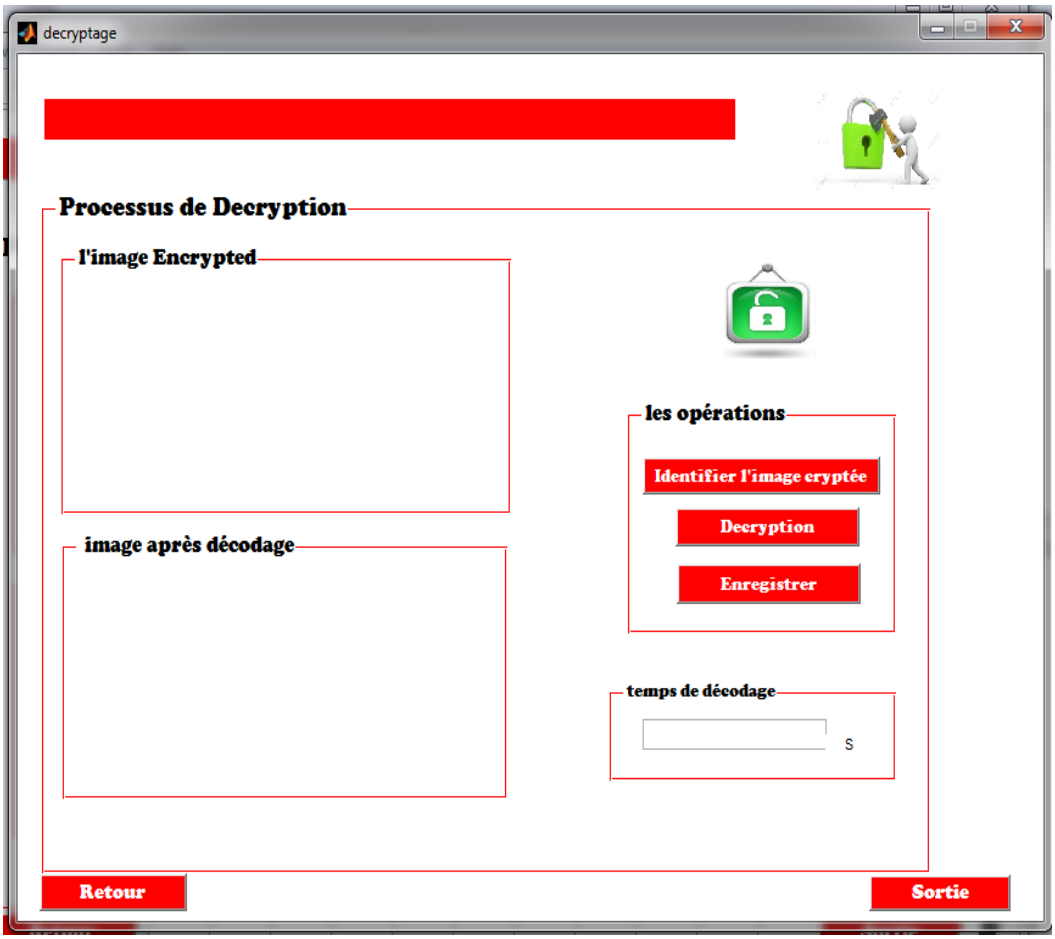


Figure 4.21 : Le déchiffrement RC5 et RC6 avant la réalisation

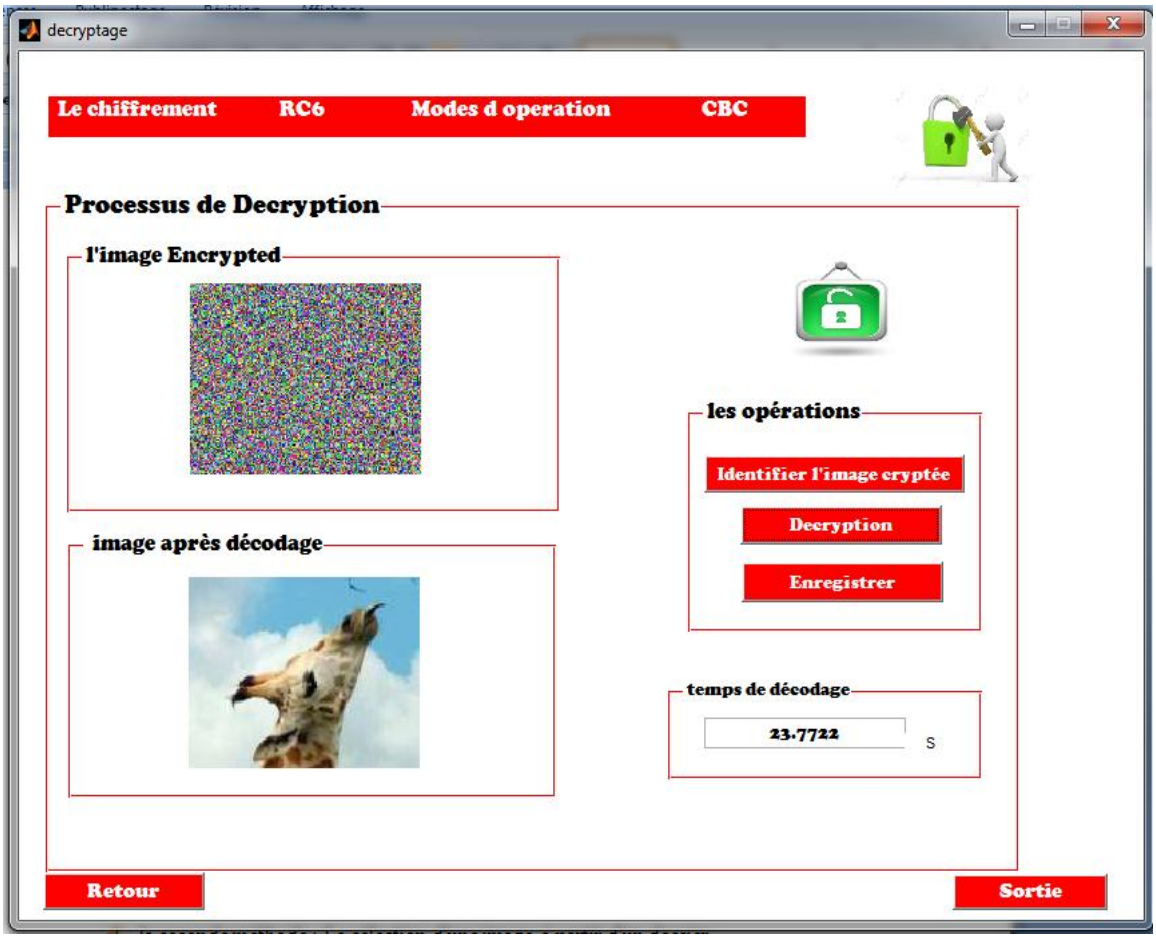


Figure 4.22 : Le déchiffrement RC5 et RC6 après la réalisation

4.4. Évaluation de la qualité de cryptage de ces algorithmes

4.4.1. Déviation d'histogramme (HistogrammeDéviation)

ID photo	Nom de l'image	D_H_RC6	D_H_RC5	D_H_XOR
1	Manchot	0,000168955	4,07541E-05	0,000212167
2	Girafe	0,003993156	0,003592283	0,003886658
3	Panthère	0,003787359	0,003568649	0,003643672
4	Perroquet	0,003720693	0,003331263	0,003779625
5	Ours	0,01724866	0,001558131	0,001541749
6	Cheval	0,004019877	0,003790939	0,004009777
7	Chats	0,040736607	0,003643645	0,003738019
8	la gazelle	0,002582645	0,002427686	0,002407025
	moyenne D_H	0,002909288	0,002744169	0,002902337

Tableau 4.1 : Déviation d'histogramme de algorithme RC5, RC6 et XOR

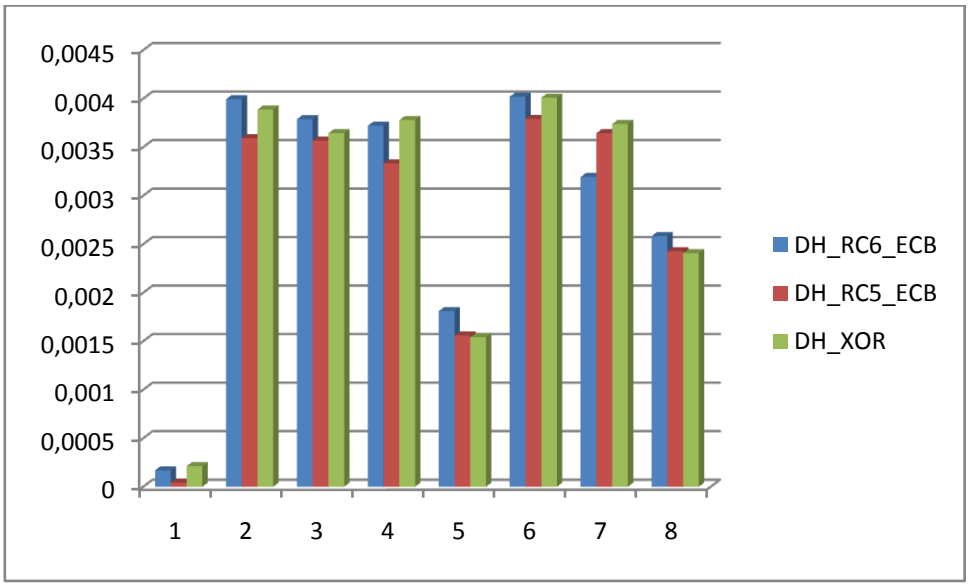


Figure 4.23 : diagramme de Déviation d'histogramme de algorithme RC5 , RC6 et XOR

Selon cette mesure (Déviation d'histogramme), le algorithme RC6 est celui qui donne les meilleurs résultats par rapport algorithme XOR et RC5 ceci est presque dans toute les images comme montre la Figure 4.23

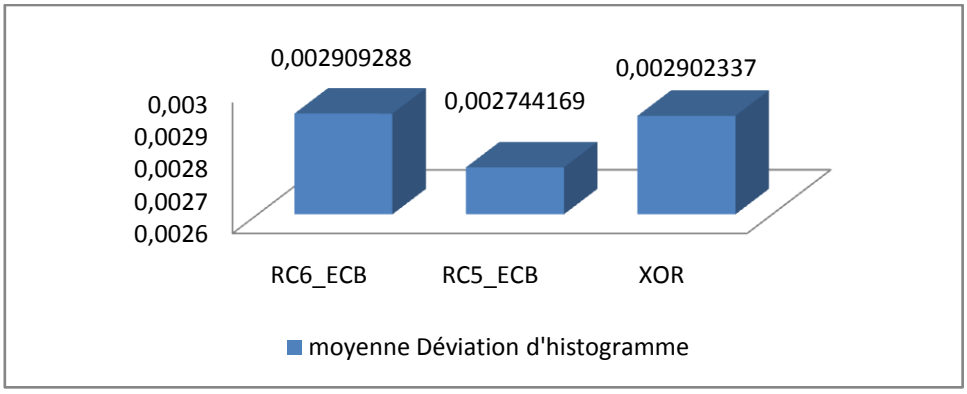


Figure 4.24 : diagramme de moyenne déviation d'histogramme d'algorithme RC5, RC6 et XOR

La figure 4.24 montre que l'algorithme RC6 est nettement supérieur à algorithme XOR suivi par RC6 avec petite différence.

4.4.2. Coefficient de corrélation (corrélationcoefficient)

ID photo	Nom de l'image	Coefficient de corrélation _RC5_ECB	Coefficient de corrélation _RC5_CBC	Coefficient de corrélation _RC5_CFB	Coefficient de corrélation _RC5_OFB	Coefficient de corrélation _XOR
1	Manchot	0,004074797	0,000497023	0,00019372	0,000613843	0,000639026
2	Girafe	0,01372515	0,00049358	0,001066395	0,001612292	0,000866258
3	Panthère	0,002036937	0,000229436	4,78129E-05	0,000101685	0,000874093
4	Perroquet	0,004229429	0,000506698	0,000904258	0,00105252	0,001567091
5	Ours	0,004005641	0,002504605	0,00053356	0,000577934	0,003452475
6	Cheval	0,000377743	0,000385791	0,000536015	0,000718347	0,002161307
7	Chats	0,020146473	0,000498108	0,002467731	0,000154868	0,001850209
8	la gazelle	0,009802867	0,004855113	7,75196E-05	0,003120768	0,002194858
	moyenne Coefficient de corrélation	0,00729988	0,001246294	0,000728376	0,000994032	0,001700665

Tableau 4.2 : Coefficient de corrélation de l'algorithme RC5 en fonction de modes de chiffrement et XOR

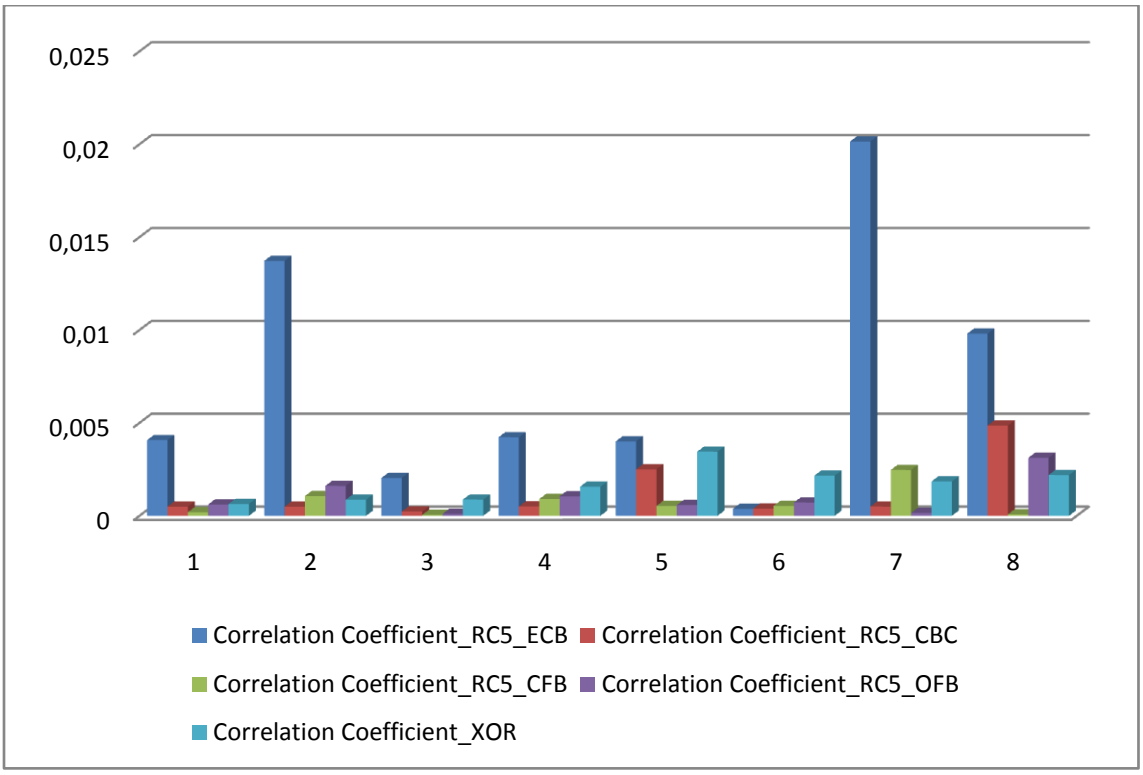


Figure 4.25 : diagramme de coefficient de corrélation RC5 En fonction de Modes de chiffrement et XOR

Dans la Figure 4.25, on ne peut pas juger tout les modes de chiffrement qui est le meilleur. Exemple pour l'image gazelle, le meilleur mode est la plus petite valeur de coefficient de corrélation qui est le mode CFB en ce qui concerne l'image de perroquet le meilleur est CBC, donc nous représentons la moyenne comme dans la figure 4.26

Le meilleur nous introduit en contrebande mode CFB ensuite OFB ensuite CBC ensuite algorithme XOR à des taux proches et le pire mode concernant le coefficient de corrélation est ECB, Ceci est pour l'algorithme RC5.

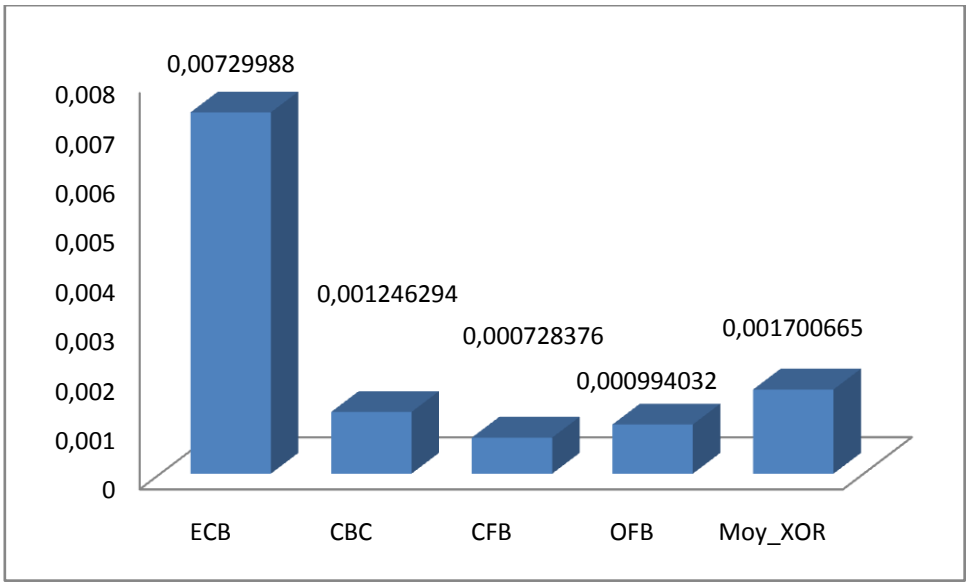


Figure 4.26 : diagramme de moyenne coefficient de corrélation RC5 en fonction de modes de chiffrement et XOR

Nos résultats dans le Figure 4.27 le cas du coefficient de corrélation d'algorithme RC6 en fonction de modes de chiffrement et XOR nous avons les mêmes notes. Donc nous ne pouvons pas juger les modes de chiffrement qui est le meilleur, ils sont différents les uns des autres selon l'image donc nous choisissons la moyenne comme dans la figure 4.28

Notons tout d'abord que toutes les valeurs convergent à la différence de RC5

Le meilleur nous introduit en contrebande mode CFB ensuite algorithme XOR ensuite OFB ensuite CBC, le pire mode on en ce qui concerne coefficient de corrélation est ECB.

Nous notons le même ordre dans modes de chiffrement pour un moyen coefficient de corrélation pour l'algorithme RC5 et RC6, la différence apparaît alors dans l'ordre de l'algorithme XOR, Où il a organisé quatre (4) pour RC5 et organisé deux (2) pour RC6.

ID photo	Nom de l'image	Coefficient de corrélation _RC6_ECB	Coefficient de corrélation _RC6_CBC	Coefficient de corrélation _RC6_CFB	Coefficient de corrélation _RC6_OFB	Coefficient de corrélation _XOR
1	Manchot	3,02877E-05	0,001581435	0,000289882	8,77842E-05	0,000639026
2	Girafe	0,001512502	0,000741977	1,61403E-05	0,001229429	0,000866258
3	Panthère	0,000429034	0,001164776	0,003317299	0,000223785	0,000874093
4	Perroquet	0,00035634	0,001584364	0,00024058	0,000258672	0,001567091
5	Ours	0,001633533	0,00343834	0,002047927	0,00242491	0,003452475
6	Cheval	0,002025081	7,41983E-05	0,001111515	0,002898948	0,002161307
7	Chats	0,008365496	0,002913268	0,002381821	0,002431655	0,001850209
8	la gazelle	0,007178406	0,006199747	0,007958139	0,002535634	0,002194858
	moyenne Coefficient de corrélation	0,002691335	0,002212263	0,002170413	0,001511352	0,001700665

Tableau 4.3 : Coefficient de corrélation d'algorithme RC6 En fonction de modes de chiffrement et XOR

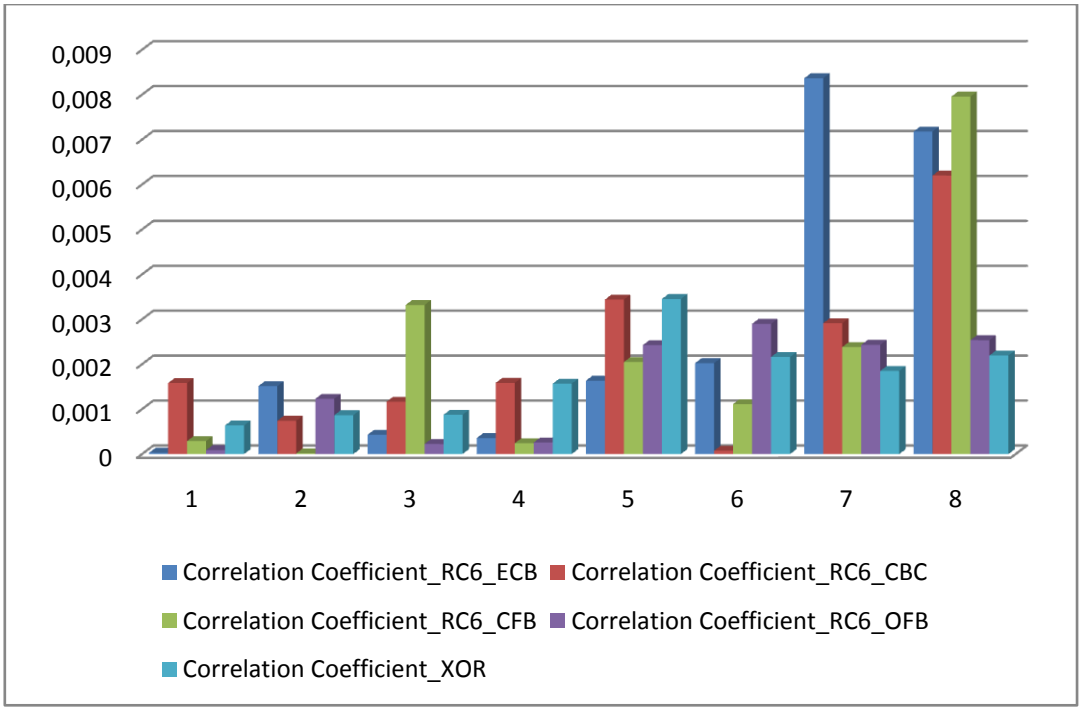


Figure 4.27 : diagramme de coefficient de corrélation RC6 en fonction de modes de chiffrement et XOR

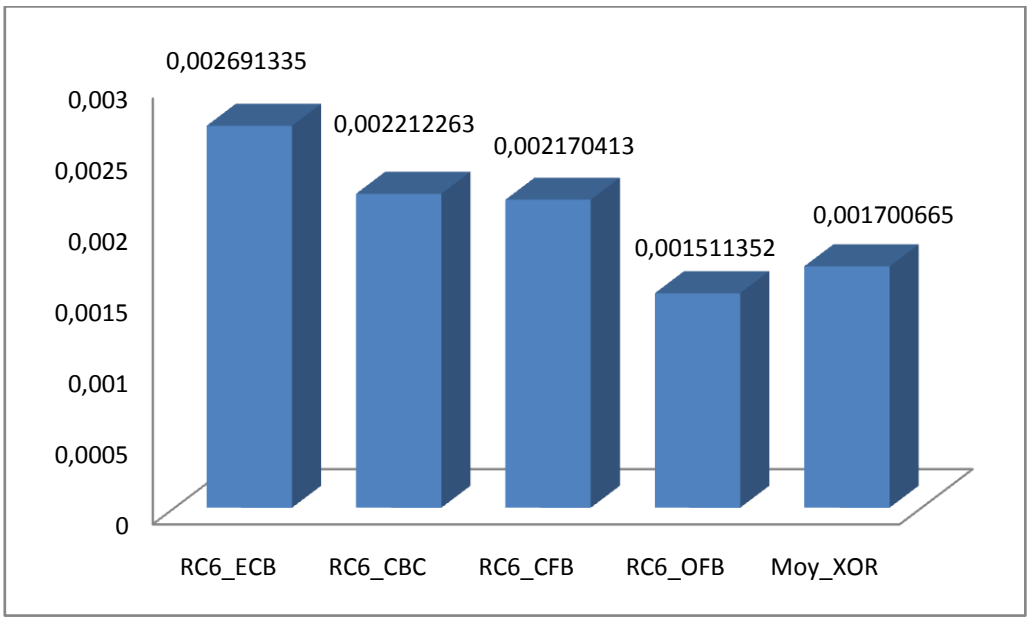


Figure 4.28 : diagramme de moyen coefficient de corrélation RC6 en fonction de modes de chiffrement et XOR

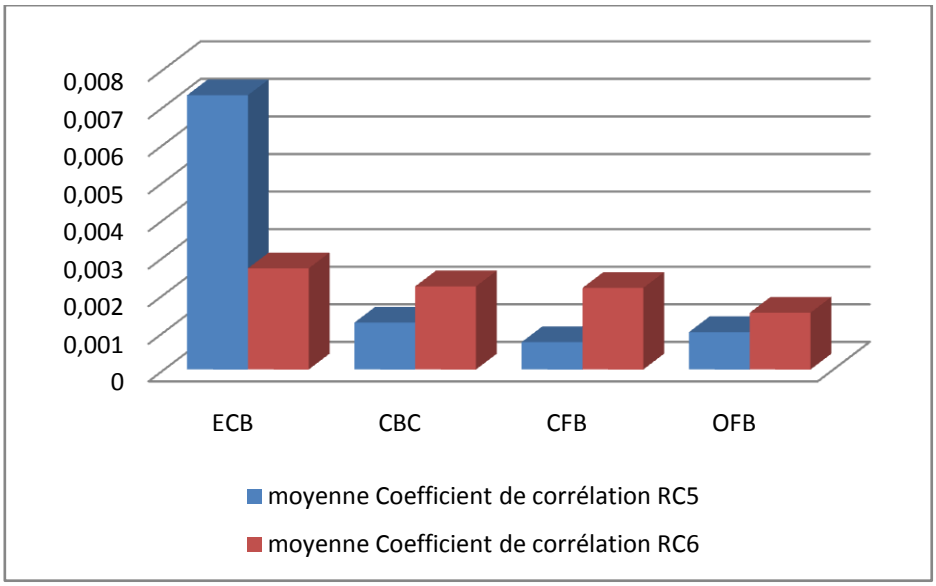


Figure 4.29 : diagramme de moyenne coefficient de corrélation RC5et RC6 en fonction de Modes de chiffrement

La figure 4.29 représente le diagramme de moyen coefficient de corrélation RC5 et RC6 en fonction de modes chiffrement on note que RC5 est supérieure dans chacun des modes de chiffrement à l'exception du mode ECB.

4.4.3. Déviation irrégulière (Irregular Deviation)

ID photo	Nom de l'image	D_I_RC6_ECB	D_I_RC5_ECB	D_I_XOR
1	Manchot	0,924218668	0,924781443	0,92392786
2	Girafe	0,684751157	0,717146508	0,674069252
3	Panthère	1,180142721	1,182729085	1,182037354
4	Perroquet	1,027019623	1,026473305	1,026417559
5	Ours	1,240358423	1,260298387	1,261529122
6	Cheval	1,256763763	1,257989253	1,255979315
7	Chats	0,553135627	0,777303282	0,372866375
8	la gazelle	0,926071798	0,925018079	0,931766529
	moyenne Déviation irrégulière	0,974057722	1,008967418	0,953574171

Tableau 4.4 : Déviation irrégulière d'algorithme RC5 , RC6 pour mode ECB et XOR

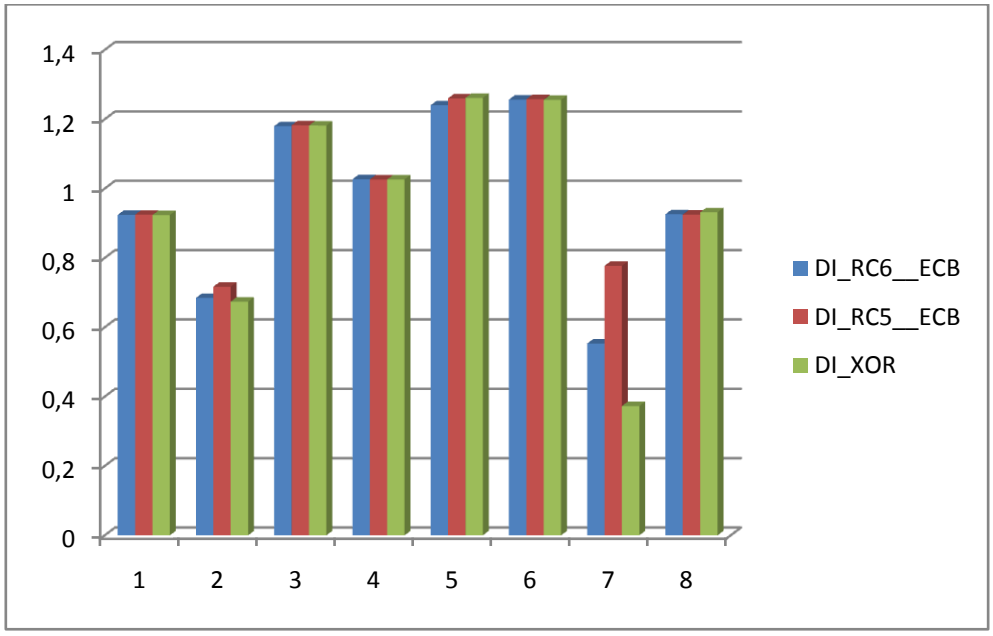


Figure 4.30 : diagramme de déviation irrégulière d'algorithme RC5, RC6 pour mode ECB et algorithme XOR

Selon cette mesure (Déviation irrégulière), la valeur plus petite est meilleure donc notez que les valeurs convergentes les algorithmes RC5, RC6 et XOR dans toutes les images sauf l'image des chats.

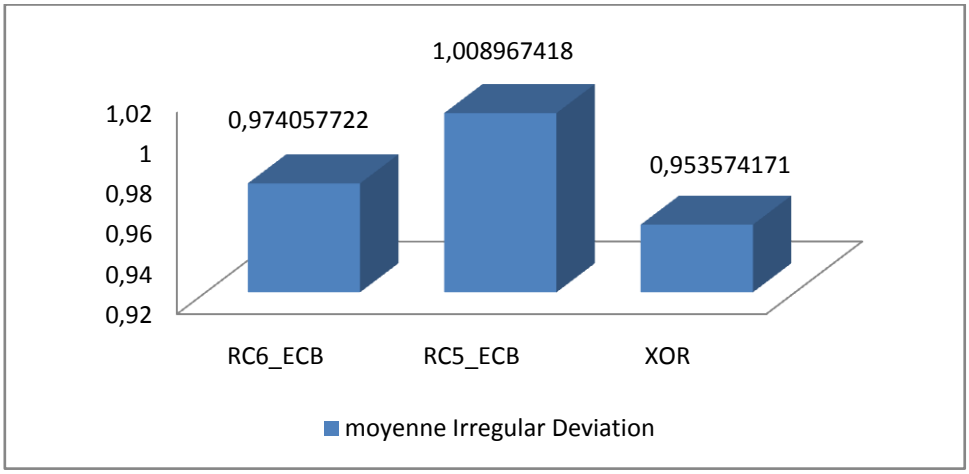


Figure 4.31 : diagramme de moyenne déviation irrégulière de algorithme RC5, RC6 pour mode ECB et algorithme XOR

La figure 4.31 montre que l'algorithme XOR meilleur ensuite RC6 ensuite RC5 par petite différence.

4.4.4. NPCR (number of changing pixel rate)

ID photo	Nom de l'image	NPCR_RC6	NPCR _RC5	NPCR _XOR
1	Manchot	0,000655342	0,000327671	4,09589E-05
2	Girafe	0,00160751	0,000803755	0,000100469
3	Panthère	0,002034505	0,001017253	0,000127157
4	Perroquet	0,00254842	0,00127421	0,000159276
5	Ours	0,022939068	0,002867384	0,000358423
6	Cheval	0,01077354	0,00538677	0,000673346
7	Chats	0,051020408	0,025510204	0,000790826
8	la gazelle	0,066115702	0,049586777	0,004132231
	moyenne NPCR	0,019711812	0,010846753	0,000797836

Tableau 4.5 : NPCR d'algorithme RC5, RC6 pour mode ECB et pour mode ECB et algorithme XOR

Ces résultats dans le tableau 4.5 obtenus après le modifiez la valeur de pixel au milieu de l'image comme une image la gazelle et chats comme il est indiqué dans l'espace rouge comme dans la figure 4.32

NPCR_RC6=0,066115702 NPCR_RC5=0,049586777 NPCR_XOR=0,004132231

Figure 4.32 : Image Ghazala avant et après le changement d'un pixel pour calculer NPCR

NPCR_RC6=0,051020408 NPCR_RC5=0,025510204 NPCR_XOR=0,000790826

Figure 4.33 : Image ghazala avant et après le changement d'un pixel pour calculer NPCR

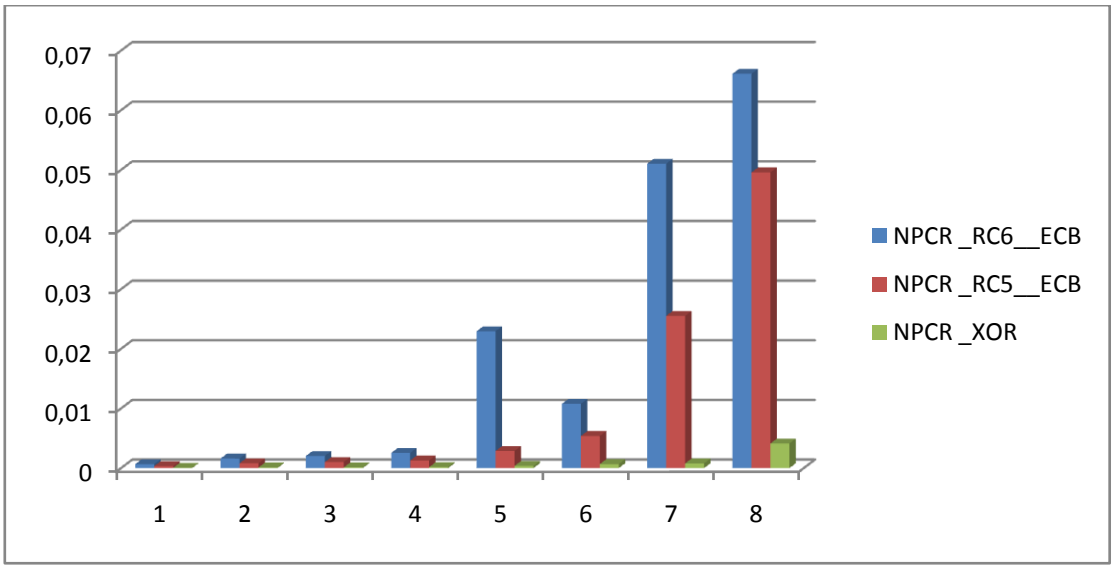


Figure 4.34 : diagramme de NPCR d'algorithme RC5, RC6 pour mode ECB et algorithme XOR

Selon cette mesure (NPCR), la plus grande valeur est meilleure Donc on voit clairement qu'à partir de figure 4.34 que la RC6 est supérieure au reste suivi dans le dernier RC5 est XOR pour toutes les images.

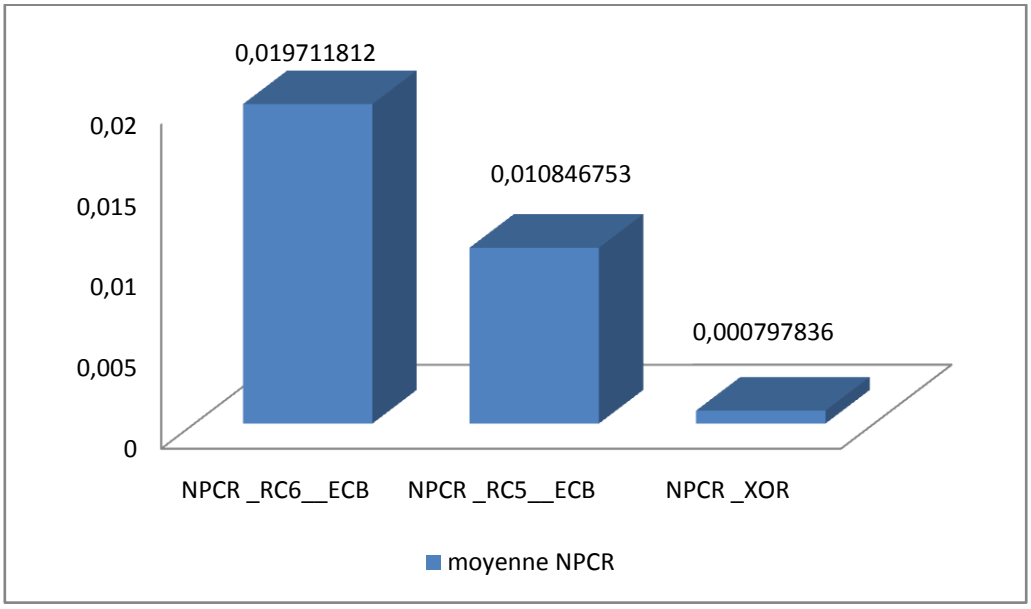


Figure 4.35 : diagramme de moyenne de NPCR de algorithme RC5, RC6 pour mode ECB et algorithme XOR

À partir de Figure 4.35Ce qui représente de moyenne de NPCR de algorithme RC5, RC6 pour mode ECB et algorithme XOR

Trouvez la différence entre RC5 et RC6 petit tandis que XOR négligé avant de lesRC6 et RC5

4.4.5. UACI (unified averaged changed intensity)

ID photo	Nom de l'image	UACI _XOR	UACI _RC5	UACI _RC6
1	Manchot	2,8109E-05	8,04722E-05	5,67E-05
2	Girafe	3,74298E-05	0,000269494	0,0002691
3	Panthère	0	0,000312656	0,000463748
4	Perroquet	0	0,00025734	0,000296066
5	Ours	0	0,000469464	0,00342821
6	Cheval	4,22492E-05	0,000789531	0,002273534
7	Chats	0	0,003670218	0,006527611
8	la gazelle	0,000956085	0,004853346	0,005185545
	moyenne UACI	0,000132984	0,001337815	0,002312564

Tableau 4.6 : UACI d'algorithme RC5, RC6 pour mode ECB et algorithme XOR

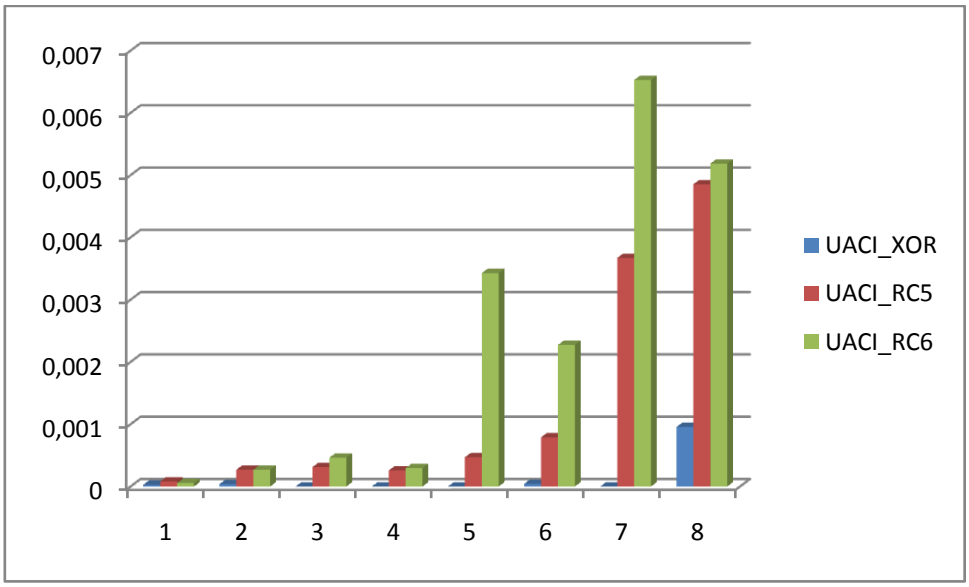


Figure 4.36 : diagramme de UACI d'algorithme RC5, RC6 pour mode ECB et algorithme XOR

Exactement comme (NPCR) la plus grande valeur est meilleure donc clairement à partir de figure 4.36 que la RC6 est supérieure au reste suivi dans le dernier RC5 est XOR pour toutes les images

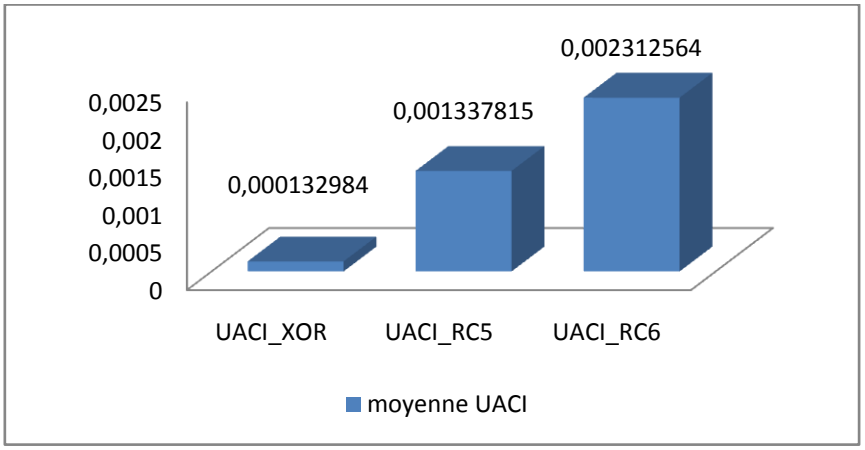


Figure 4.37 : diagramme de moyenne de UACI de algorithme RC5, RC6 et XOR

La même chose observé sur de moyenne de NPCR de algorithme RC5, RC6 et XOR appliquer à moyenne de UACI de algorithme RC5, RC6 et XOR toujours XOR négligé pour les autres (RC6 et RC5).

4.4.6.La durée de cryptage et de décryptage et la vitesse

ID photo	Nom de l'image	Taille (pixel)	Chiffrement Durée_RC6_ECB(s)	Chiffrement Durée_RC6_CBC(s)	Chiffrement Durée_RC6_CFB(s)	Chiffrement Durée_RC6_OFB(s)	Chiffrement Durée_XOR(s)
1	Manchot	7324416	1983,54076	1207,031346	1164,341182	1198,217822	0,535968185
2	Girafe	2985984	630,2942711	477,7108806	465,3333792	484,3959913	0,1821443
3	Panthère	2359296	458,3124145	380,2340715	382,1802371	363,688223	0,15610652
4	Perroquet	1883520	343,1467202	289,665845	294,3077199	290,3902884	0,114692381
5	Ours	837000	131,3874557	135,3030645	131,6718316	135,3199383	0,048325333
6	Cheval	445536	129,1203817	71,54441404	71,05649809	69,66611968	0,02764948
7	Chats	379350	85,63793252	62,45193095	57,60158227	57,47327961	0,022791289
8	la gazelle	145200	33,11570453	22,14546019	22,7999447	22,62958106	0,011168578
	moyenne	2045037,75	474,319455	330,7608766	323,6615469	327,7226554	0,137355758

Tableau 4.7 : Chiffrement durée d'algorithme RC6 en fonction de modes de chiffrement et algorithme XOR

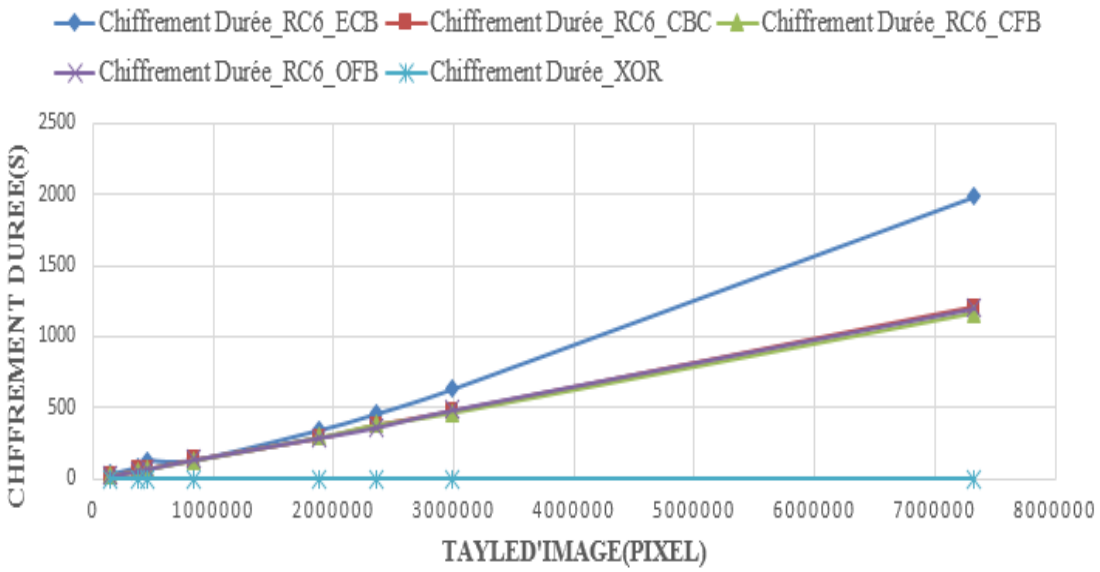


Figure 4.38 : Chiffrement durée d'algorithme RC6 en fonction de taille d'image

Notez que la relation positive entre la taille de l'image et le temps de chiffrement et de déchiffrement pour chaque algorithmes comme il apparaît dans les courbes dans les figure 4.38 , figure 4.39, figure 4.41 et figure 4.42 et durée d'algorithme XOR négligé pour les autres durée de mode et le plus haut toujours mode ECB et l'autre (CFB, CBC et OFB) semi – égalité.

ID photo	Nom de l'image	Taille (pixel)	Chiffrement Durée_RC5_ECB(s)	Chiffrement Durée_RC5_CBC(s)	Chiffrement Durée_RC5_CFB(s)	Chiffrement Durée_RC5_OFB(s)	Chiffrement Durée_XOR(s)
1	Manchot	7324416	6176,130725	2241,485191	1578,53607	1930,76938	0,535968185
2	Girafe	2985984	736,9521438	833,6462387	522,2554944	604,0461525	0,1821443
3	Panthère	2359296	560,1364313	754,3729305	572,8891634	630,711759	0,15610652
4	Perroquet	1883520	391,7469241	378,2552517	373,9370311	369,4560798	0,114692381
5	Ours	837000	145,5224997	146,929031	167,118824	220,8052727	0,048325333
6	Cheval	445536	138,5716256	99,15520145	138,5814248	122,021045	0,02764948
7	Chats	379350	96,18815449	92,93929026	102,3430794	96,40352533	0,022791289
8	la gazelle	145200	41,0186065	46,91973349	39,82365637	35,31411948	0,011168578
	moyenne	2045037,75	1035,783389	574,2128585	436,935593	501,1909167	0,137355758

Tableau 4.8 : Chiffrement durée d'algorithme RC5 en fonction de modes de chiffrement et algorithme XOR

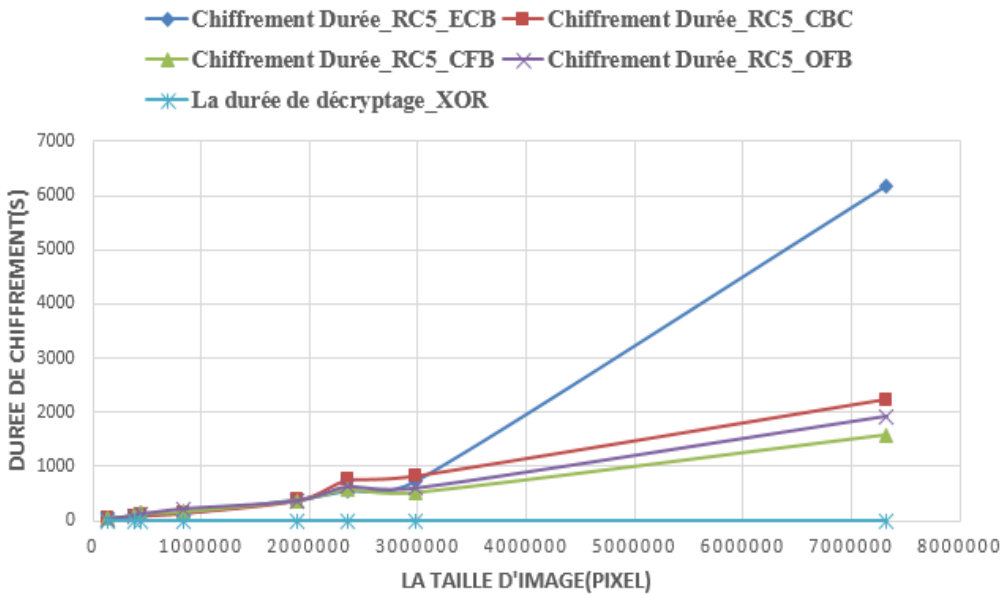


Figure 4.39 : Chiffrement durée d'algorithme RC5 en fonction de taille d'image

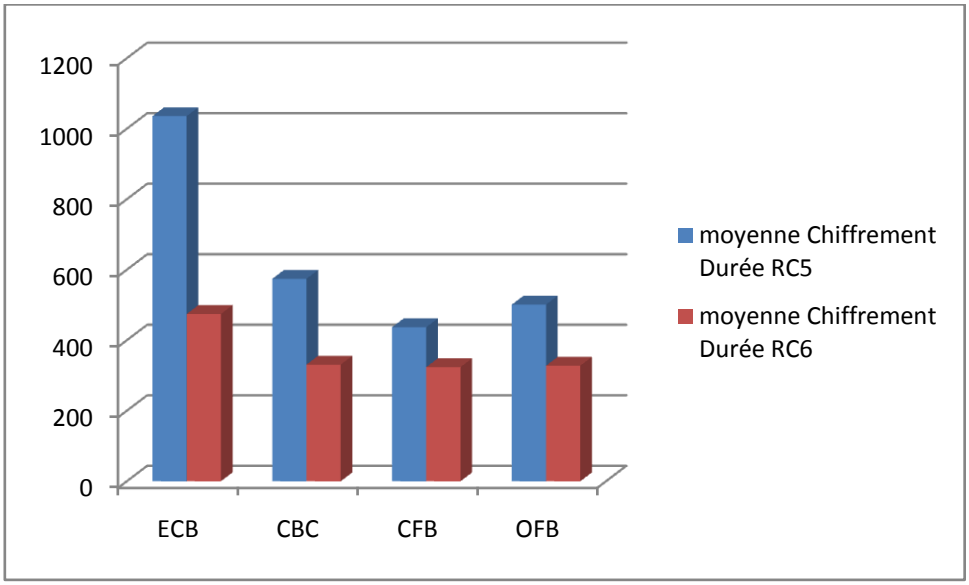


Figure 4.40 : diagramme de moyenne chiffrement durée d'algorithme RC5 et RC6 en fonction de modes de chiffrement

Sur la figure 4.40 est clair pour nos algorithme RC6 moins chiffrement durée donc il est préférable pour chaque modes de chiffrement et mieux mode est CFB, OFB, CBC et ECB successivement pour algorithme RC5Et pour algorithme RC6 les modes CFB, OFB et CBC semi –égalité et ECB pire pour chiffrement durée.

ID photo	Nom de l'image	Taille (pixel)	La durée de décryptage_XOR	La durée de décryptage_RC5_ECB	La durée de décryptage_RC5_CBC	La durée de décryptage_RC5_CFB	La durée de décryptage_RC5_OFB
1	Manchot	7324416	0,55069841	2665,81915	1737,795587	1428,4132	1843,832043
2	Girafe	2985984	0,247584268	1731,177118	594,7471523	543,2425425	605,9541989
3	Panthère	2359296	0,221085513	643,423256	668,8058806	610,6234809	493,3012871
4	Perroquet	1883520	0,142664286	386,1263272	395,5280685	768,1781059	331,9596397
5	Ours	837000	0,059419934	151,9130532	157,9781678	202,4698709	226,0401308
6	Cheval	445536	0,031443324	116,8868366	101,8044745	119,4533201	113,1100252
7	Chats	379350	0,020595033	120,9633569	103,4472635	108,9822671	103,6593554
8	la gazelle	145200	0,009739045	41,71288074	40,59584437	42,82653981	40,8466653
	moyenne	2045037,75	0,160403727	732,2527473	475,0878048	478,0236659	469,8379182

Tableau 4.9 : La durée de décryptage d'algorithme RC5 en fonction de modes de chiffrement et algorithme XOR

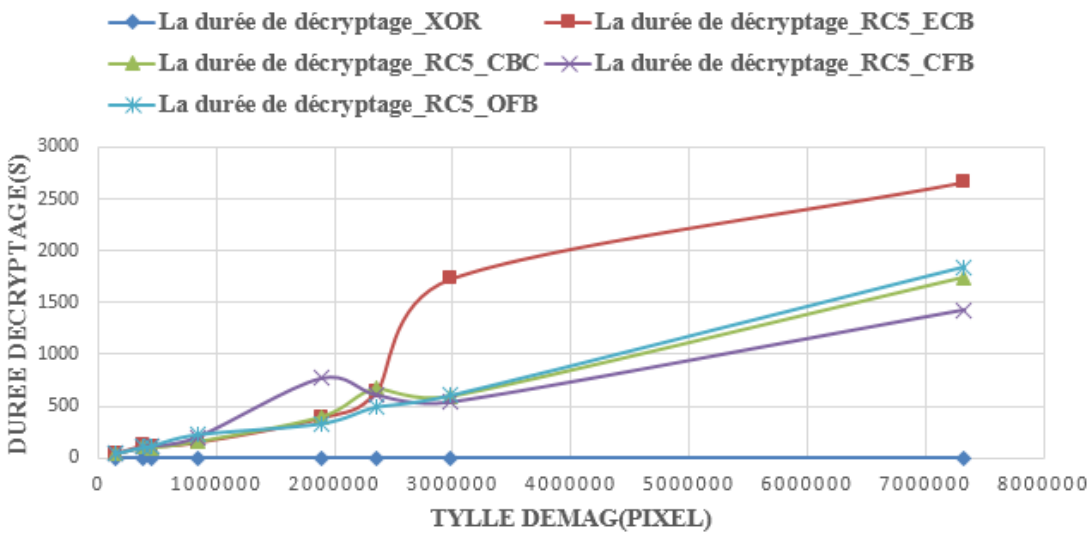


Figure 4.41 : La durée de décryptage d'algorithme RC5 en fonction de taille d'image

ID photo	Nom de l'image	Taille (pixel)	La durée de décryptage_XOR	La durée de décryptage_RC6_ECB	La durée de décryptage_RC6_CBC	La durée de décryptage_RC6_CFB	La durée de décryptage_RC6_OFB
1	Manchot	7324416	0,55069841	1467,013548	1328,509505	1142,826647	1149,566989
2	Girafe	2985984	0,247584268	723,4029059	497,9510999	485,2073865	482,335546
3	Panthère	2359296	0,221085513	463,2657688	409,2174139	366,9596585	364,3421316
4	Perroquet	1883520	0,142664286	425,1167828	311,5857898	290,621849	286,0685818
5	Ours	837000	0,059419934	141,7064286	140,381329	131,8119747	130,6472204
6	Cheval	445536	0,031443324	132,8144156	75,53203506	69,51143745	74,00321489
7	Chats	379350	0,020595033	106,2636346	63,55750844	58,93465841	59,420576
8	la gazelle	145200	0,009739045	45,36236451	24,69579082	23,71417152	23,38576406
	moyenne	2045037,75	0,160403727	438,1182312	356,4288091	321,1984728	321,221253

Tableau 4.10 :La durée de décryptage d'algorithme RC6 en fonction de modes de chiffrement et algorithme XOR

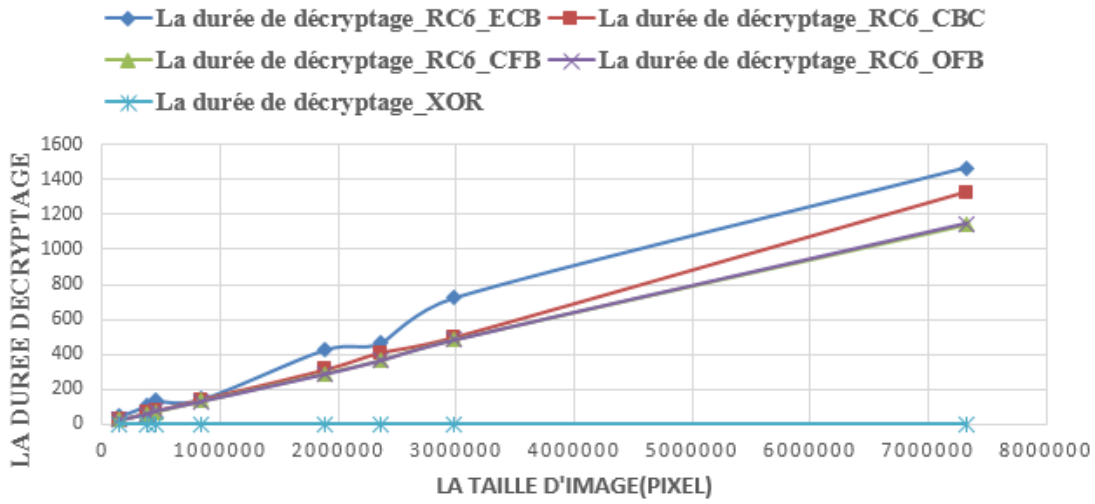


Figure 4.42 : La durée de décryptage d'algorithme RC6 en fonction de taille d'image

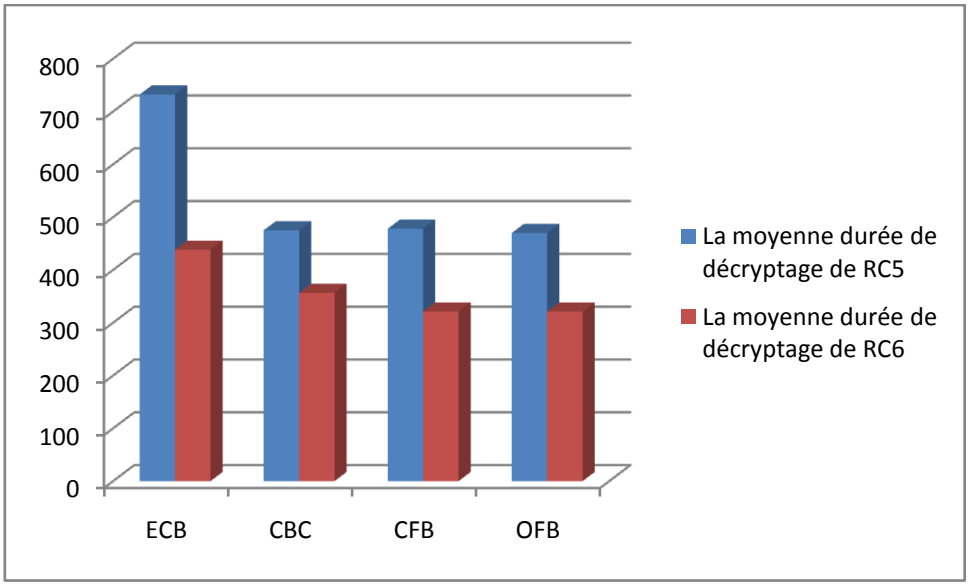


Figure 4.43 : diagramme de moyenne de la durée de décryptage d'algorithme RC5 et RC6 en fonction de modes de chiffrement

Presque comme moyenne chiffrement Durée, Sur la figure 4.43 est clair pour nous algorithme RC6 moins durée de décryptage donc il est préférable pour chaque modes de chiffrement et mieux mode est CFB, OFB, CBC et ECB successivement pour algorithme RC6 et pour algorithme RC5 les modes CFB, OFB et CBC semi –égalité et ECB pire pour la durée de décryptage.

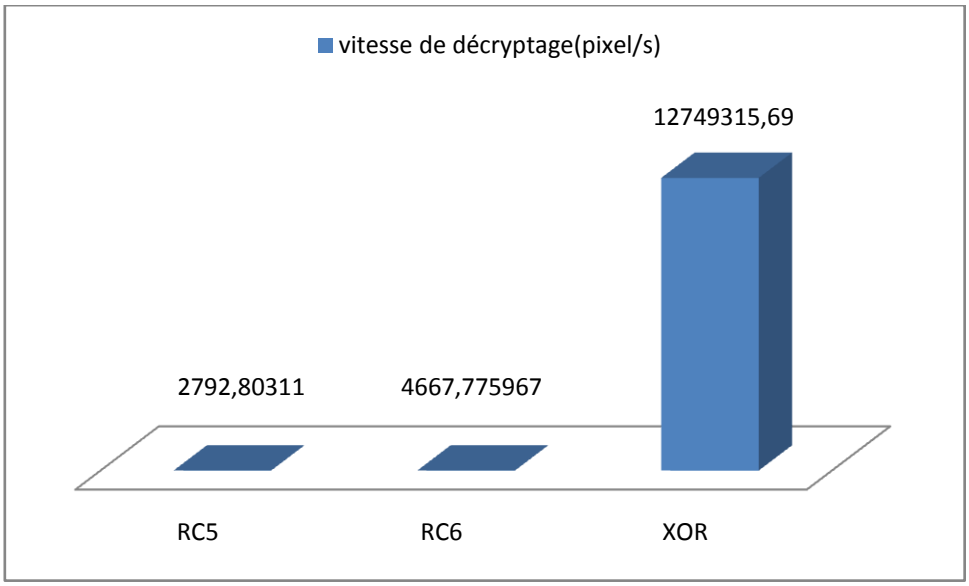


Figure 4.44 : diagramme moyenne de vitesse de décryptage d'algorithme RC5, RC6 et XOR

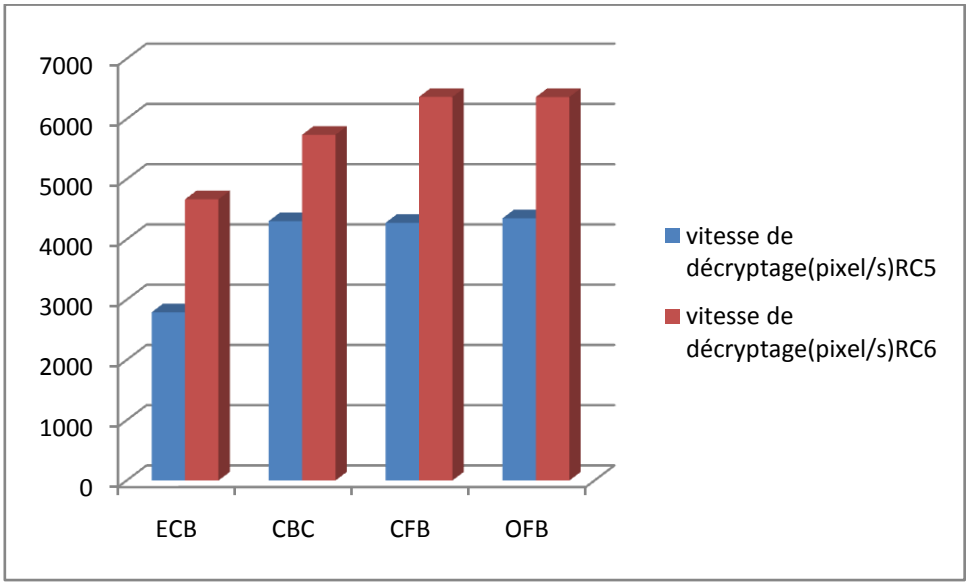


Figure 4.45 : diagramme moyenne de vitesse de décryptage d'algorithme RC5 et RC6 En fonction de modes de chiffrement

Sur la figure 4.45 et Figure 4.46, on conclut que le mode de chiffrement CFB a de meilleures performances que d'autres modes de chiffrement suivi OFB, CBC en ordre et lente modes de chiffrement ECB.

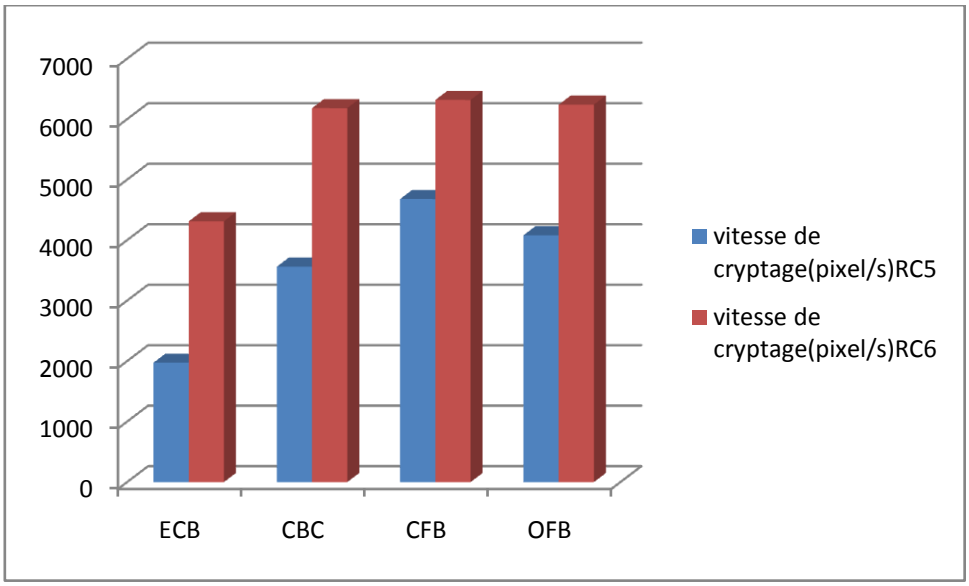


Figure 4.46 : diagramme moyenne de vitesse de décryptage d'algorithme RC5 et RC6 en fonction de modes de chiffrement

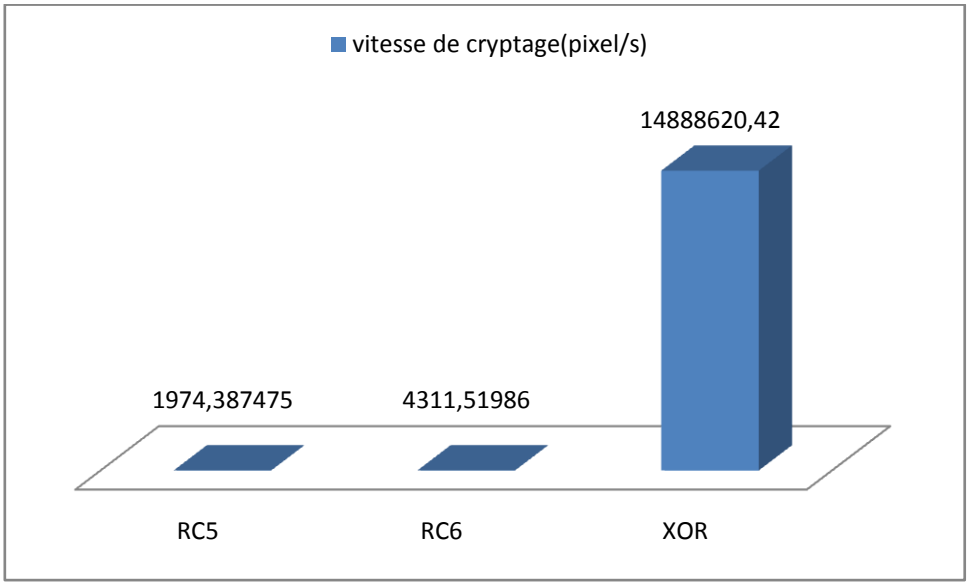


Figure 4.47 : diagramme moyenne de vitesse de cryptage d'algorithme RC5, RC6 et XOR

Sur la Figure 4.44 et Figure 4.47 vitesse de cryptage et décryptage presque égal et il est le algorithme XOR plus rapide pour algorithme RC5 et RC6, mais RC6 mieux que RC5

4.4.7. L'histogramme

L'histogramme d'une image fait référence à un graphique du pixel valeurs d'intensité. L'histogramme est un graphique montrant le nombre de pixels dans une image à différentes valeurs d'intensité trouvé dans l'image. Dans une image en niveaux de gris de 8 bits, il existe

256 différentes intensités possibles, et donc l'histogramme affichera 256 nombres montrant la distribution de pixels parmi ces valeurs en niveaux de gris. Pour un bon cryptage, la répartition des échelles de gris dans l'image cryptée devrait être assez uniforme.

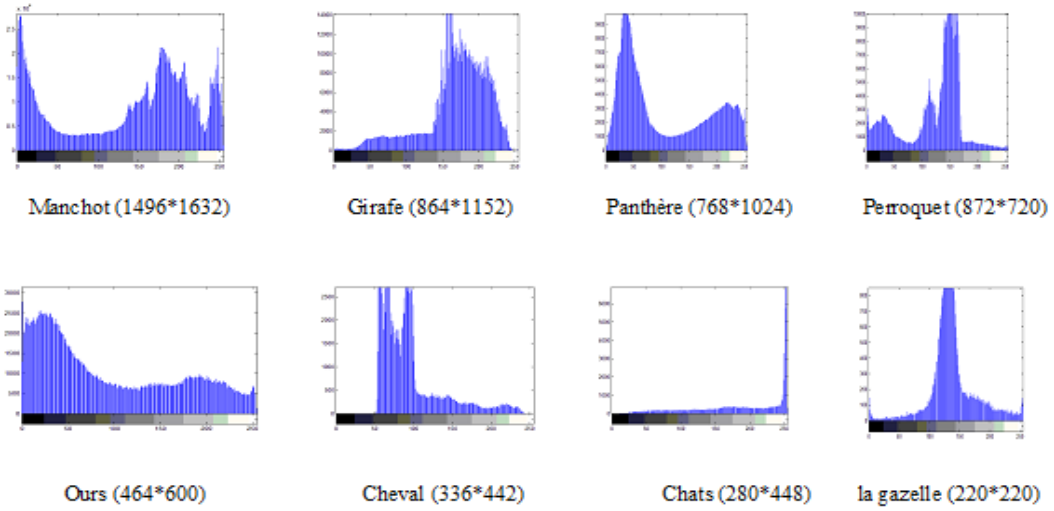


Figure 4.48: L'histogramme des images originales de la figure 4.2

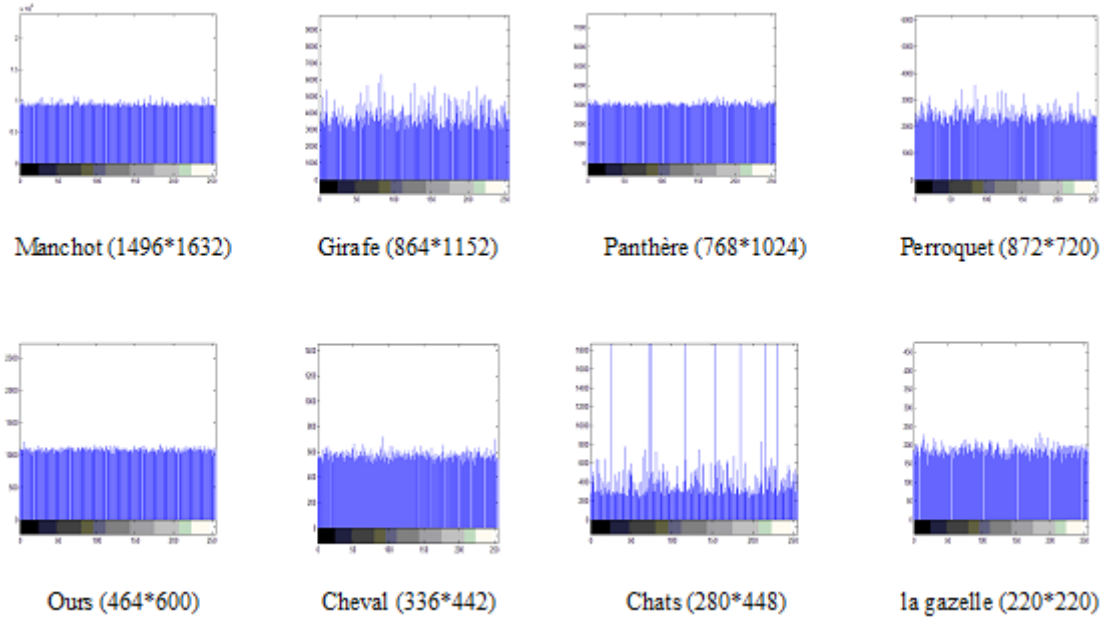


Figure 4.49 : L'histogramme images d'encrypté d'algorithme RC5 de la figure 4.3

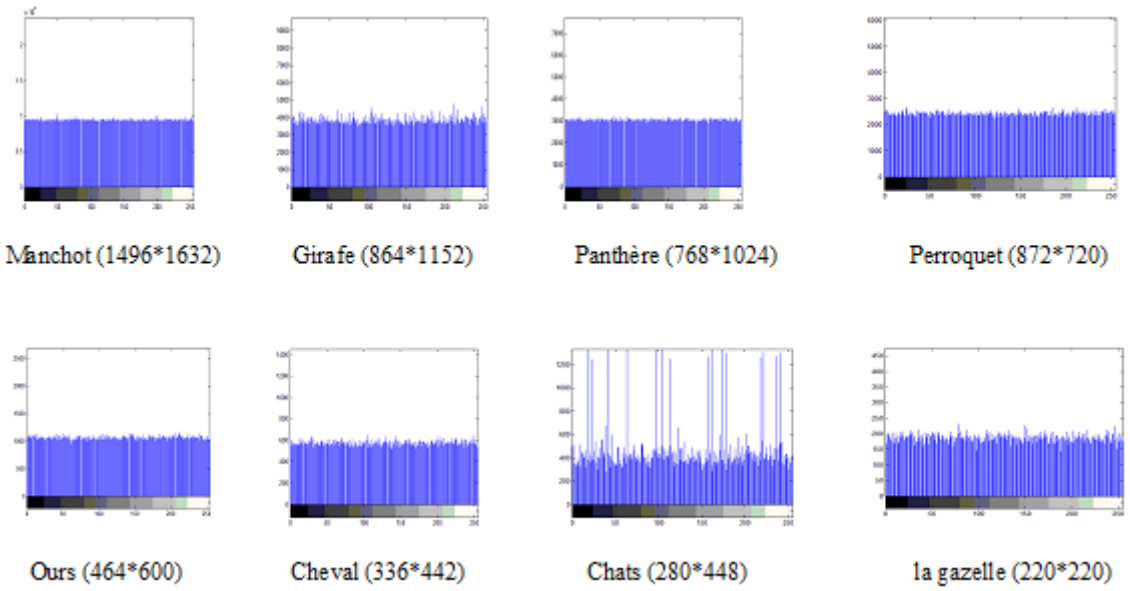


Figure 4.50: L'histogramme images d'encrypté d'algorithme RC6 de la figure 4.4

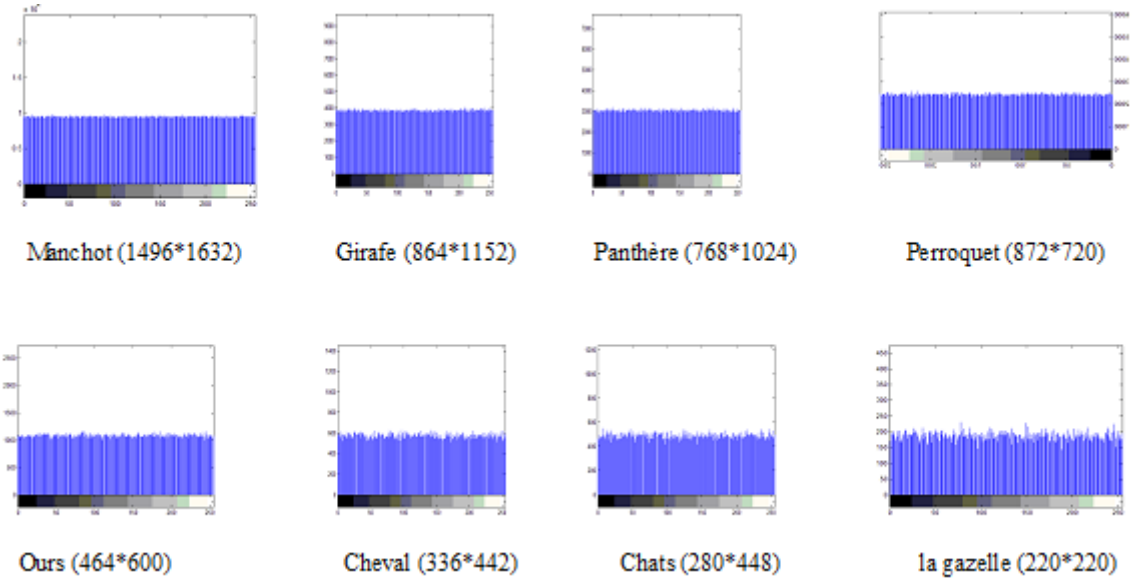


Figure 4.51 : L'histogramme images d'encrypte d'algorithme XOR de la figure 4.5

- Analyse des histogrammes

Il ressort donc des figures d'histogrammes, que les histogrammes des images chiffrées sont uniformément distribués par rapport aux histogrammes des images d'origines. Par rapport aux trois algorithmes. Ceci rend la cryptanalyse de plus en plus difficile.

4.4.8. (PSNR)peak signal-to-noise ratio

Après avoir changé la valeur d'un pixel Au centre de chaque image, nous obtenons les résultats dans le tableau 4.11

ID photo	Nom de l'image	PSNR _RC6	PSNR _RC5	PSNR _XOR
1	Manchot	85,05250432	∞	98,027921
2	Girafe	78,02446411	81,00083463	84,04506402
3	Panthère	75,92798361	79,80387756	83,02201357
4	Perroquet	83,18673271	∞	∞
5	Ours	69,61580914	71,53174379	78,52144384
6	Cheval	64,32173691	67,33203687	75,78301727
7	Chats	69,2957272	∞	75,08459014
8	la gazelle	61,67511949	63,13234292	94,97925723

Tableau 4.11:PSNR ***d'algorithme RC5, RC6 et XOR Après avoir changé un seul pixel***

Figure 4.52 : PSNR d'algorithme RC5, RC6 et XOR après avoir changé un seul pixel l'image du cheval

ID photo	Nom de l'image	PSNR _RC6	PSNR _RC5	PSNR _XOR
1	Manchot	70,5423198	74,17901304	81,55800563
2	Girafe	66,94438838	69,84324062	78,02446411
3	Panthère	72,44848549	74,99494689	80,01171361
4	Perroquet	66,87892674	68,61966481	82,04389162
5	Ours	64,36058885	66,56950416	75,51114388

6	Cheval	60,81100967	63,61592617	71,01180472
7	Chats	56,93376337	59,56817697	69,06399023
8	la gazelle	55,42286069	58,12631941	67,89504822
	moyenne	64,29279287	66,93959901	75,64000775

Tableau 4.12: PSNR d'algorithme RC5, RC6 et XOR après avoir changé 6 pixels

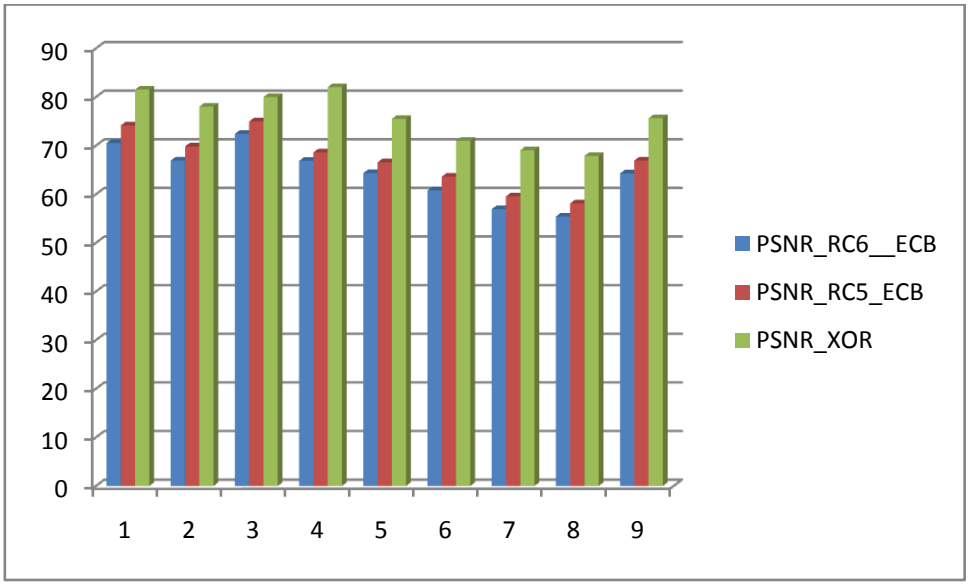


Figure 4.53 : diagramme de PSNR d'algorithme RC5, RC6 et XOR pare mode ECB

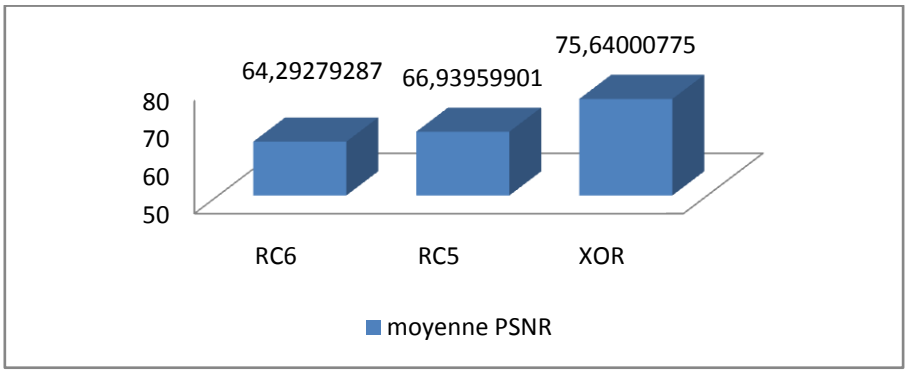


Figure 4.54 : diagramme de moyenne de PSNR d'algorithme RC5, RC6 et XOR pare mode ECB

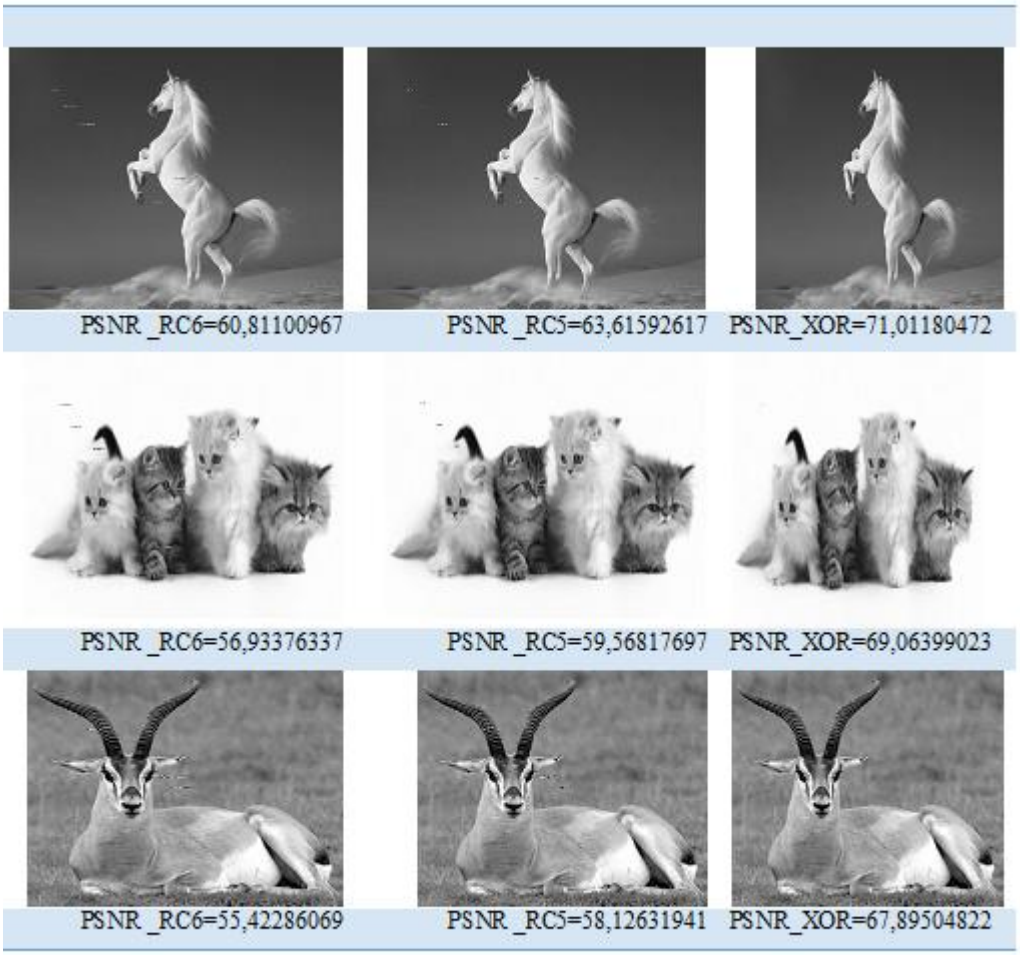


Figure 4.55 : PSNR de algorithme RC5, RC6 et XOR après avoir changé 6 pixel l'image du cheval , chats et la gazelle pour mode ECB

Selon cette mesure (PSNR) la plus grande valeur est la meilleure Donc on conclut que clairement à partir de figure 4.52 que la XOR est supérieure au reste suivi dans le dernier RC5 est pour toutes les images.

A partir de Figure 4.54 Ce qui représente la moyenne de PSNR d'algorithme RC5, RC6 et XOR est mieux XOR suivi par RC5 ensuite RC6 par petite différence et la figure 4.55 montre clairement la différence.

ID photo	Nom de l'image	PSNR _RC6	PSNR _RC5	PSNR _XOR
1	Manchot	69,99416935	73,01458921	81,55800563
2	Girafe	65,58994945	68,37364664	78,02446411
3	Panthère	70,71251808	71,70796578	80,01171361
4	Perroquet	65,24783152	68,19940867	82,04389162
5	Ours	63,52619019	66,88608859	75,51114388
6	Cheval	60,15286223	63,02245616	71,01180472
7	Chats	49,96088573	58,82299867	69,06399023
8	la gazelle	54,46040344	57,47725995	67,89504822
	Moyenne	62,45560125	65,93805171	75,64000775

Tableau 4.13: PSNR d'algorithme RC5, RC6 et XOR après avoir changé 6 pixels pour mode CFB

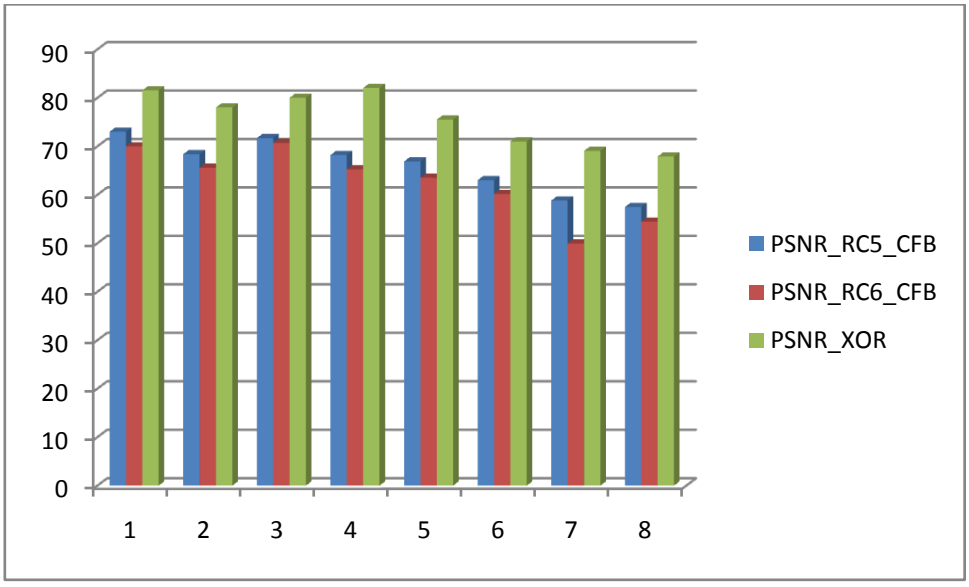


Figure 4.56 : diagramme de PSNR de algorithme RC5, RC6 et XOR par mode CFB

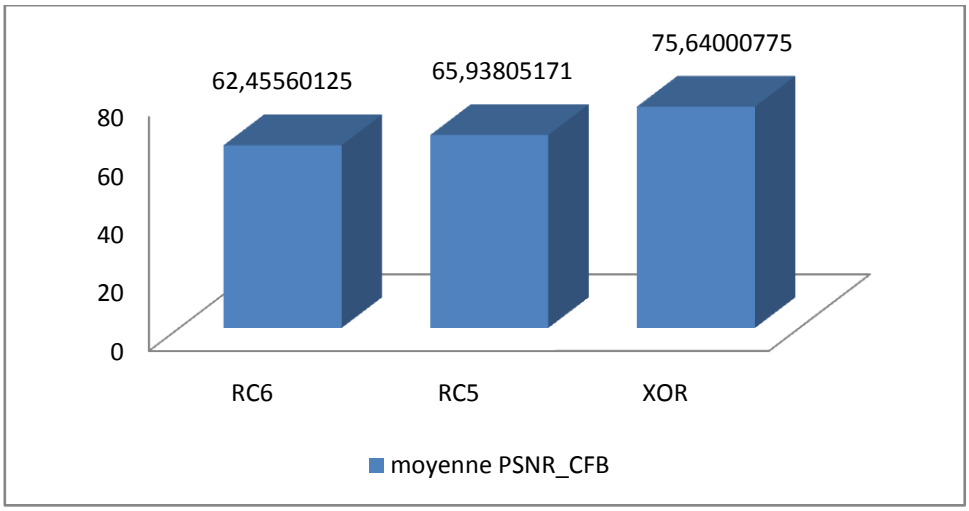


Figure 4.57 : diagramme de moyenne de PSNR d'algorithme RC5, RC6 et XOR pour mode CFB

le même résultat pour PSNR des algorithmesRC5 ,RC6 et XOR après avoir changé six(6) pixel pour mode ECB ,Où il a maintenu le même ordre pour PSNR de l'algorithme RC5 ,RC6 et XOR après avoir changé 6 pixel pour mode CFB efficace XOR suivi par RC5 et RC6 . Cependant, PSNR pour mode ECB mieux que mode CFB après avoir comparé les deux figures : Figure 4.58 et Figure 4.55 .

4.4.9. Déviation irrégulière (Irregular Déviation) pour mode CFB

ID photo	Nom de l'image	D_I_RC6_CFB	D_I_RC5_CFB	D_I_XOR
1	Manchot	0,924570095	0,924350556	0,92392786
2	Girafe	0,672763149	0,672536089	0,674069252
3	Panthère	1,180371602	1,177881877	1,182037354
4	Perroquet	1,026567278	1,025958843	1,026417559
5	Ours	1,243892473	1,262540995	1,261529122
6	Cheval	1,256326088	1,258974022	1,255979315
7	Chats	0,357390273	0,366263345	0,372866375
8	la gazelle	0,932649793	0,921678719	0,931766529
	moyenne Déviation irrégulière	0,931766529	0,951273056	0,953574171

Tableau 4.14 : Déviation irrégulière de algorithme RC5, RC6 pour mode CFB et algorithme XOR

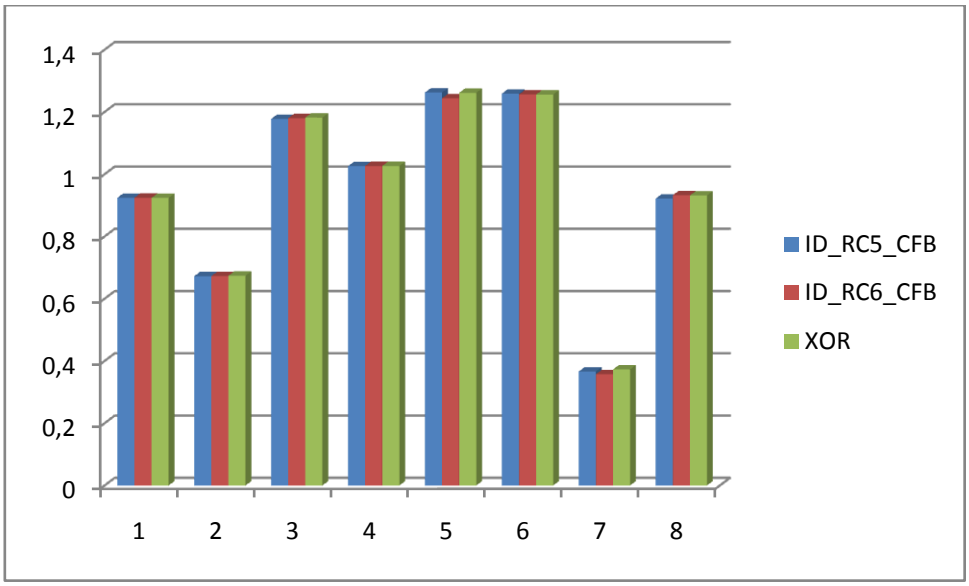


Figure 4.58:diagramme de déviation irrégulière d'algorithme RC5, RC6 pour mode CFB et algorithme XOR

Selon cette mesure (Déviation irrégulière), la valeur plus petite est meilleure. Donc on note que les valeurs convergentes des algorithmes RC5, RC6 et XOR Par toutes les images à travers la figure 4.58.

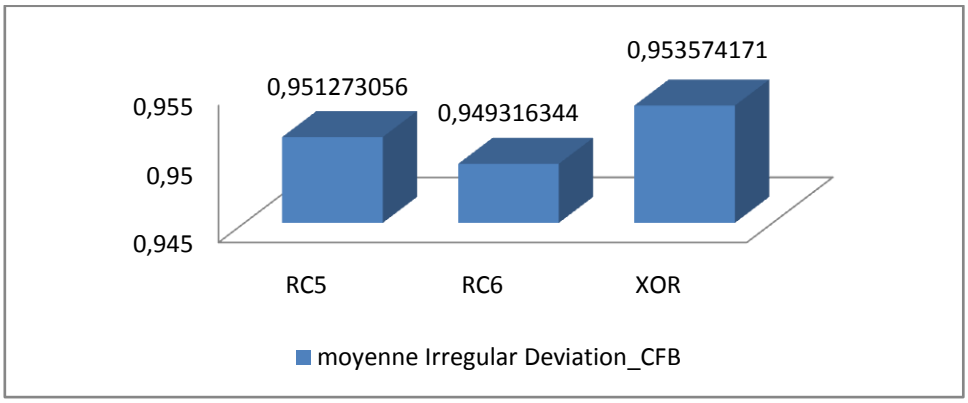


Figure 4.59:diagramme de moyenne Déviation irrégulière de algorithme RC5, RC6 pour mode CFB et XOR

La figure 4.59 montre que l'algorithme RC6 est meilleur ensuite RC5 ensuite XOR par petite différence. Contrairement aux résultats pour mode ECB.

4.5. Conclusion

A partir des résultats obtenus on peut conclure que le algorithme le plus performant dans le cryptage des images est RC6 selon les résultats de la plupart des mesure de l'évaluation du cryptage Il a été mieux pour :

- Déviation d'histogramme pour mode ECB
- Déviation irrégulière pour mode CFB
- NPCR et UACI pour mode ECB

Mais ce même algorithme est moins efficace pour :

- vitesse de cryptage
- Coefficient de corrélation
- PSNR

On peut conclure aussi que l'algorithme RC5 Il était mieux efficace pour le cas du coefficient de corrélation pour les modes à l'exception ECB. Tandis que l'algorithme XOR Il était mieux efficace pour :

- PSNR pour les modes ECB et CFB à RC5 et RC6
- vitesse de cryptage
- Coefficient de corrélation pour mode ECB à RC5 et RC6
- Déviation irrégulière pour mode ECB à RC5 et RC6

Finalement chaque algorithme possède des points forts et des points faibles mais les différents algorithmes sont favorables pour différentes situations.

Enfin le meilleur mode est CFB qui donne toujours les meilleurs résultats à la différence de mode ECB qui donne toujours les pires résultats.

Conclusion générale

Le chiffrement a cette science aujourd'hui un grand prestige parmi les sciences, que des applications pratiques modifiées pour inclure plusieurs domaines, comme domaine diplomatique et militaire, la sécurité, commerciale, économique, des médias et de la banque et l'informatique.

Au cours de cette mémoire, nous avons étudié et implémenté les trois algorithmes de chiffrements symétrique (RC5, RC6, XOR).

Nous sommes basés sur sept critères de comparaisons pour évaluer l'opération de chiffrement qui sera appliqué sur des images :

Le premier critère c'est déviation d'histogramme,

Le deuxième critère c'est La Coefficient de corrélation,

Le troisième critère c'est la Déviation irrégulière,

Le quatrième critère c'est NPCR,

Le cinquième critère c'est UACI,

Le sixième critère c'est La durée de cryptage et de décryptage et la vitesse,

Et a la fin PSNR.

D'après les résultats obtenus avec les différentes comparaisons effectuées nous pouvons conclure que les algorithmes RC6 puis RC5 sont plus performants en termes Déviation d'histogramme pour mode ECB, Déviation irrégulière pour mode CFB, et NPCR et UACI pour mode ECB.

Cet algorithme est faible par rapport les autres algorithmes pour les métrique: vitesse de cryptage, Coefficient de corrélation, et PSNR.

On peut conclure aussi que l'algorithme RC5 Il était mieux efficace pour le cas du coefficient de corrélation pour les modes à l'exception ECB. Tandis que le algorithme XOR Il était mieux efficace pour :

PSNR pour les modes ECB et CFB à RC5 et RC6 , vitesse de cryptage, Coefficient de corrélation pour mode ECB à RC5 et RC6, Déviation irrégulière pour mode ECB à RC5 et RC6 et meilleur mode est CFB qui donne toujours les meilleurs résultats à la différence de mode ECB qui donne toujours les pires résultats.

Comme perspective de notre travail, nous souhaitons pour les prochains :

- Utilisation du système de distribution pour accélérer le temps de chiffrement.
- Par rapport RC6 avec AES.

Références

[01]BENABDELLAH Mohammed,20 Juin 2007,"OUTILS DE COMPRESSION ET DE CRYPTOCOMPRESSION : APPLICATIONS AUX IMAGES FIXES ET VIDEO",THESE DE DOCTORATUNIVERSITE MOHAMMED V-AGDAL

[02]THOME Nicolas ,13 Septembre 2016, "Bases du traitement des images Introduction fondements",

[03] KARAM FOUAD et IMOULOUDENE SALAH EDDINE, 24 Juin 2015,"Transfert sécurisé des données visuelles (images) dans un réseau intranet selon l'architecture client/serveur"

[04] DIDIER Müller, juin2016 ,"Chapitre 4 Traitement d'images"

https://www.apprendre-en-ligne.net/info/images/images.pdf

[05] http://files2.fatakat.com/2013/11/13838533841806.jpg ,30/04/2017 16:04

[06]DUGELAY Jean-Luc et ROCHE Stéphane 'INTRODUCTION AU TATOUAGED'IMAGES', https://liris.cnrs.fr/seminaires/sem_ancien_axe2/dugelay_tatouage

[07] http://www.memoireonline.com/08/13/7255/m_Evaluation-dun-algorithme-de-cryptage-chaotique-des-images-base-sur-le-modele-du-perceptron0.html
6/3/2017, 14 23

[08]https://perso.esiee.fr/~barjonej/Site/questce_que_le_tatouage_numrique.htm, 4/3/2017,23 :12

[09]DALIA Battikh, 19 Feb 2016 , 'Sécurité de l'information par steganographie basee sur les séquences chaotiques'

[10] ROGERIE Grégory,' la stéganographie',http://www.univ-orleans.fr/mapmo/membres/louchet/teaching/timo/Rogerie.pdf ,30/03/2017 ,11 :02

[11] N.KOUDRI MOUSTEFAI, Année univesitaire 2013/2014, 'tests de validation pour les crypto-systèmes chaotiques'

[12]Fathi E. Abd El-Samie ,HossamEldin H. Ahmed ,Ibrahim F. Elashry ,Mai H. Shahieen, 2014,‘IMAGEENCRYPTIONA Communication Perspective’,.

[13]N.KOUDRI MOUSTEFAI, Année univesitaire 2013/2014, ‘tests de validation pour les crypto-systèmes chaotiques’

[14]Philippe Pittoli ,‘Sécurité dans les réseaux de capteurs Ajout de la sécurité au protocole CASAN’, , t.karchnu.fr/cours/mémoire-philippe-pittoli.pdf

[15]GRANBOULAN Louis , NGUYEN Phong et POINTCHEVAL David ,‘Conception et preuves d’algorithmes cryptographiques’, Edition 2004, http://www.di.ens.fr/~wwwgrecc/Enseignement/CoursCryptoMMFAI.pdf

Glossaire

RGB : Rouge, de Grine et de Bleu.

HSL : Hue, Saturation, Luminance

HSB : Hue, Saturation, Brightness

HSV : Hue, Saturation, Value

HSI : Hue, Saturation, Intensity

CMY : Cyan, Magenta, Yellow

CIE : Commission Internationale de l'Eclairage

PAL : Phase Alternation Line

SECAM : Séquentiel Couleur avec Mémoire)

I.F.F : Identification Friands and Foes

LSB : Least Significant Beat

ECB : Electronique Code Block

CBC: Cipher Block Chaining

CFB : Chiper Feedback

CTAK: CipherText Auto Key

OFB : Output FeedBack

KAK: Key Auto Key

PSNR: peak signal-to-noise ratio

UACI: unified averaged changed intensity

NPCR : number of changing pixel rate