République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Batna 2
Faculté de mathématiques et d'informatique

Thèse

En vue de l'obtention du diplôme de
Doctorat en Informatique

Contribution à l'étude des mécanismes cryptographiques

Présentée Par

Beloucif Assia

Soutenue le: 22 / 09 / 2016

Membres du jury :

Président:	Bilami Azeddine	Professeur	Université de Batna 2
Rapporteur:	Noui Lemnouar	Professeur	Université de Batna 2
Examinateurs:	Ali pacha Adda	Professeur	Université USTO Oran
	Seghir Rachid	MCA	Université de Batna 2
	Guenda Kenza	MCA	Université USTHB Alger

قال الله تعالى:
((وقل رب زدني علما))
سورة طه :١١٤

A mes chers parents...
A mes soeurs et frères...
A tous ceux qui me sont chers...

Remerciements

Grand merci à Allah, Miséricordieux, le tout puissant qui m'a donnée la force, la persévérance et la patience d'accomplir mon travail.

Ma gratitude, mes vifs remerciements et mes respects à mon encadreur Pr. Lemnouar Noui professeur au département de mathématiques université de Batna 2, pour tous ses judicieux conseils, son temps qu'il m'a consacré et pour m'avoir toujours orientée vers un esprit purement scientifique.

Je remercie l'ensemble des membres du jury qui m'ont fait l'immense plaisir de juger ce travail. Sincères remerciements au Président du jury, Azeddine Bilami, Professeur à l'université de Batna 2, aux rapporteurs Adda Ali pacha, Professeur à l'USTO d'Oran, Rachid Seghir, MCA à l'université de Batna 2 , Kenza Guenda MCA à l'USTHB Alger.

J'exprime également mes remerciements à mes chers parents qui n'ont jamais cessé de m'encourager à bien mener mes travaux. Et à tous ceux qui m'ont encouragée et soutenue moralement et intellectuellement.

Résumé

Depuis que l'image a pu être introduite et traitée sous forme informatique, ses applications n'ont eu cessé de s'enrichir. Ainsi, elle est devenue numérique et elle est exploitée aussi bien par des utilisateurs simples que par des professionnels (architecture, médecine, audiovisuel, commerce, militaire, . . .). Le développement permanent des dispositifs d'acquisition d'images, des réseaux informatiques et de l'augmentation rapide des écoutes illégales font apparaître de nombreux et de nouveaux mécanismes de chiffrement qui contribuent à l'amélioration continue de la qualité des schémas de chiffrement des images numérique, en fonction des différentes technologies. La plupart de ces travaux, au niveau de la sécurité, montrent plusieurs défaillances. Dans ce travail, nous avons exploré les bénéfices de deux techniques différentes afin de pallier les limitations des algorithmes de chiffrement d'images existant. La première proposition consiste en un algorithme de chiffrement des images en niveau de gris basé sur des transformations matricielles et le OU exclusif, tandis que la deuxième proposition présente un algorithme tweakable de chiffrement des images en couleur basé sur l'utilisation de la carte chaotique non linéaire PWLCM. Des comparaisons avec des schémas de chiffrement d'images récemment proposés ont été réalisées montrant que les algorithmes proposés offrent des performances très favorables.

Mots clés : Sécurité multimédia, confidentialité, chiffrement d'images

Abstract

Since the image has been introduced and treated in a computerized form, its applications have been constantly enriched. Thus, it has become digital and is operated by simple users as well as professionals (architecture, medicine, audiovisual, Business, military,...). The continued development of image acquisition devices, computer networks and the rapid increase in illegal eavesdropping reveal many new encryption mechanisms contributing to the continuous improvement of the quality of image encryption schemes using different technologies. However, most of the proposed schemes have several failures at the security level. In this study, we explored the benefits of two different techniques to overcome the limitations of the existing image encryption algorithms. The first proposition is an encryption algorithm, which can be applied to gray scale images, based on matrix transformations and XOR operation. Whereas the second proposal exhibits a tweakable color images encryption algorithm based on the use of the nonlinear chaotic map PWLCM. Comparisons with recent algorithms of images encryption were performed showing that the proposed algorithms provide highly favorable performances.

key words: Multimedia security, confidentiality, image encryption

ملخص

منذ أن تم عرض الصور ومعالجتها في شكل محوسب، يتواصل إثراء تطبيقاتها باستمرار. فقد أصبحت رقمية، ويتم استغلالها من قبل المستخدمين العاديين والمتخصصين(الهندسة المعمارية، والطب، والسمعي البصري، التجارة والجيش، ...) على حد سواء. لكن، في ظل التطور المستمر في أجهزة التقاط الصورو شبكات الكمبيوتر والزيادة السريعة في عمليات التنصت غير المشروعة وجب ضمان خصوصية الصور الرقمية مما أدى إلى ظهور العديد من آليات التشفير الجديدة مع استعمال تقنيات مختلفة. بالرغم من أن هذه الآليات تساهم في التحسين المستمر لنوعية برامج تشفير الصور الرقمية غير أن معظم هذه الأعمال تظهر العديد من الإخفاقات على مستوى الأمن. في هذه الدراسة، سنكشف فوائد تقنيتين مختلفتين في تجاوزقيود خوارزميات تشفير الصور الموجودة. الاقتراح الأول هو خوارزمية خاصة بتشفير الصور الرمادية باستعمال عمليات على المصفوفات وخواريزمية او الاستبعادي . في حين أن الاقتراح الثاني يمثل خوارزمية لتشفيرالصور الملونة باستخدام نظرية الشواش. مقارنة أجريت مع مخططات حديثة لتشفيرالصور تبين أن الخوارزميات المقترحة توفر أداءا تنافسيا للغاية.

الكلمات المفتاحية : أمن الوسائط المتعددة، الخصوصية، تشفير الصور.

Liste de publications

- BELOUCIF Assia and NOUI Lemnouar. **A lossless image encryption algorithm using matrix transformations and XOR operation**. *International Journal of Information and Communication Technology*. (In press)
- BELOUCIF Assia, Noui Oussama and NOUI Lemnouar. **Design of a tweakable image encryption algorithm using chaos based schema**. *International Journal of Information and Communication Technology*. 8(3) :205–220.(2016)
- BELOUCIF Assia and NOUI Lemnouar. **A symmetric image encryption algorithm based on diagonal matrices and the XOR operation**. Information Technology for Organization Development (IT4OD), 2014.
- BELOUCIF Assia and NOUI Lemnouar. **Total Break of a Hill cipher based on circulant matrices**. International Conference on Coding and Cryptography (ICCC), 2015.
- BELOUCIF Assia and NOUI Lemnouar. **Une nouvelle strategie de chiffrement d'images**. International workshop in cryptography and its applications(IWCA16), 2016.
- BELOUCIF Assia and NOUI Lemnouar. **Encryption based on companion matrices** Cimpa school : Number theory and application,2016.

Table des matières

Table des figures

Liste des tableaux

Liste des Algorithmes

Glossaire des acronymes

- **AES :** Advanced Encryption Standard
- **CA :** Automate cellulaire
- **CBC :** Enchaînement des blocs
- **CCA :** Attaque texte chiffré choisi
- **CFB :** Chiffrement à rétroaction
- **CML :** Coupled map lattice
- **CNCM :** Coupled Nonlinear Chaotic Map
- **CNN :** Cellular Neural Network
- **COA :** Attaque sur texte chiffré seul
- **CPA :** Attaque texte clair choisi
- **CTR :** Chiffrement basé sur un compteur
- **DCML :** Delayed Coupled Map Lattices
- **DES :** Data Encryption Standard
- **ECB :** Dictionnaire de Codes
- **FrRnWT :** Transformation Aléatoire en Ondelette Fractionnée
- **FWT :** Transformation en Ondelette Fractionnée
- **GIF :** Graphics Interchange Format
- **HSV :** Teinte, Saturation, Valeur
- **IV :** Vecteur Initial
- **JPEG :** Joint Photographic Experts Group

- **MD5 :** Message Digest 5
- **NPCR :** Number of Pixels Change Rate
- **OCML :** One-way Coupled-Map Lattices
- **OFB :** Chiffrement à Rétroaction de Sortie
- **PNG :** Portable Network Graphics
- **PWLCM :** Piecewise Linear Chaotic Map
- **RVB :** Rouge Vert Bleu
- **RGB :** Red Green Blue
- **TAE :** Tweakable Authenticated Encryption
- **TC :** Tweak Chaining
- **TIC :** Technologies de l'Information et de la Communication
- **TIE :** Tweak Incrementation Encryption
- **TIFF :** Tagged Image File Format
- **TRNG :** Vrai Générateur de Nombres Aléatoires
- **TSL :** Teinte, Saturation, Luminosité
- **TTP :** Autorité de Confiance
- **UACI :** Unified Average Changing Intensity
- **XOR :** OU exclusif

Introduction générale

Au cours des dernières années, les technologies de l'information et de la communication ont connu un immense développement. L'internet est l'une des dernières technologies de l'information et de la communication TIC qui est devenue très répandue et utilisée dans tous les domaines. Par conséquent, l'échange, le stockage et la manipulation des informations, sous toutes ses formes, à travers l'Internet sont devenus des éléments essentiels dans la société moderne. Ainsi, l'Internet a permis la collaboration et l'appui d'interactivités entre les individus, les organismes gouvernementaux, les institutions académiques et les entreprises. Subséquemment, les gens sont devenus dépendants de l'Internet pour des usages personnels et professionnels.

En parallèle, avec le développement de l'Internet, le risque d'intrusion ou de fraude a augmenté ; puisqu'elle représente un canal non sécurisé pour l'échange d'informations. En effet, assurer la sécurité des donnés notamment les données confidentielles est le plus grand défi à relever pour le bon fonctionnement du réseau internet. Certainement, la tâche la plus importante est celle de rendre les informations confidentielles inaccessible pour tout autre que le destinataire légitime. Afin de protéger les informations sensibles quand elles sont sauvegardées ou transmises à travers un réseau non sûr : c'est à dire contre tout accès non autorisé, le chiffrement s'avère être la principale solution conçue pour assurer cette fonctionnalité. Dans la littérature, les chercheurs ont conçu plusieurs méthodes de chiffrement en utilisant une variété de techniques.

De nos jours, les images numériques représentent un énorme type d'information impliquées dans les communications modernes et qui sont utilisées dans plusieurs domaines sensibles tels que le commerce électronique, les affaires militaires et les dossiers médicaux. Cependant, il est devenu clair que nous ne pouvons pas utiliser les méthodes de chiffrement classiques conçues pour les données textuelles comme RSA [2], DES [3], AES [4] pour le chiffrement des images puisque les images numériques sont caractérisées par la redondance élevée, la forte corrélation et la taille volumineuse. Par conséquent, un intérêt spécial est nécessaire lors du chiffrement de ces données. Selon Shannon [5] : la confusion (substitution) et la diffusion (permutation) sont les deux principales méthodes élaborées pour éliminer les redondances élevées et la forte corrélation. La confusion crée une forte relation entre la clé et le texte chiffré. D'un autre

côté, la diffusion réduit la redondance du texte en clair en la propagation sur la totalité du texte chiffré.

En utilisant généralement l'architecture confusion/diffusion plusieurs algorithmes de chiffrement d'images existant ont été proposés en fonction de différentes technologies tel que : les paternes de balayage(SCANE) [6, 7], les cartes chaotiques[8, 9, 10], les transformations matricielles[11, 12], la transformation en ondelette[13, 14], le Séquençage de l'ADN[15, 16] et beaucoup d'autres méthodes. Ces algorithmes peuvent être classés en deux grandes catégories : les méthodes du domaine spatial et les méthodes dans le domaine fréquentiel. Dans le domaine spatial, on applique le schéma de cryptage sur le plan d'images lui-même, et les approches de cette catégorie sont basées sur une manipulation directe des pixels d'une image. Dans ces algorithmes, le chiffrement détruit la corrélation entre les pixels et rend les images cryptées incompressibles. Les pixels de l'image peuvent être reconstruits complètement par un processus inverse sans aucune perte d'information. En revanche, Les schémas de cryptage dans le domaine fréquentiel sont basés sur la modification de la fréquence de l'image en utilisant une transformation, ainsi, la reconstruction des pixels de l'image originale dans le processus de décryptage cause une perte d'information. Dans la première catégorie, il n'y a aucune différence entre l'image décryptée et l'image originale ; par conséquent, ces méthodes sont plus applicables dans de nombreux domaines sensibles où la non perte est nécessaire. Cependant, dans la seconde catégorie, l'image déchiffrée n'est pas la même image d'origine et il y a un peu de différence entre elles, l'oeil humain ne peut pas la détecter. L'image décryptée avec petite différence est généralement acceptable selon les applications du schéma.

Contribution

En parallèle à l'énorme développement des algorithmes de cryptage d'images contribués, dont le but est d'améliorer les algorithmes de cryptage d'images. Ces dernières années, les chercheurs ont accordé plus d'attention à l'étude de ces techniques en termes d'analyse de sécurité. Ils ont constaté que plusieurs cryptosystèmes souffrent d'un ou plusieurs problèmes tel que la faible sensibilité à la variation de l'image en claire [17, 18],l'espace de clés restreint [17], les clés faibles et les clés équivalentes [19, 20, 21, 18], l'irrésistibilité à l'attaque texte clair connu [22, 23, 24, 25] et l'irrésistibilité à l'attaque texte claire choisi [22, 26, 23, 27, 25]. Afin de sécuriser encore les protocoles existants et d'obtenir de meilleures performances, nous allons présenter dans cette thèse deux méthodes que nous avons développées.

La première méthode :

Afin d'assurer que notre contribution est applicable dans les domaines sensibles, nos recherches sont centrées sur le cryptage sans perte. Nous avons proposé un nou-

veau schéma de cryptage d'image au niveau de gris qui est caractérisé par les points suivants :

- L'algorithme possède un grand espace de clé.
- Les résultats de la simulation montrent l'efficacité de la contribution.
- L'algorithme est basé sur l'utilisation d'une transformation matricielle et l'opération XOR.
- La comparaison avec l'algorithme AES montre la supériorité de notre approche en terme de chiffrement d'images avec des grandes zones de la même couleur.
- Puisque les images au niveau de gris sont représentées comme chaine de symboles dans l'intervalle [0 255]. Le système proposé pourrait être appliqué au cryptage de texte.
- Des simulations d'analyse de la sécurité ont été effectuées pour assurer l'efficacité du système proposé contre l'analyse statistique, analyse de l'espace clé et l'analyse de sensibilité.
- L'étude de la complexité de l'algorithme proposé montre qu'il exige moins d'instructions primitives en le comparant avec les autres algorithmes, ce qui signifie que le schéma proposé est le plus rapide.

La deuxième méthode :

En se basant sur le mécanisme de confusion/diffusion, nous avons proposé un autre schéma de cryptage des images et cette fois-ci en couleurs. Ce schéma est :

- Basé sur un mode de cryptage sûr contre l'attaque CPA.
- Basé sur l'utilisation de la carte chaotique non linéaire PWLCM qui possède des propriétés dynamiques parfaites.
- Des performances satisfaisantes de sécurité ont été obtenus en utilisant une seule ronde de chiffrement.
- Au lieu de chiffrer chaque canal de couleur à part, une étape de mélange de canaux est utilisé pour mélanger les données provenant de différents canaux et donc fournir un autre aspect de la confusion dans l'image chiffrée résultante.
- Aussi sans perte
- Comparé avec des schémas de chiffrement d'image couleur existants pour montrer que le régime proposé offre des performances très avantageuses.

Cette nouvelle méthode est testée en utilisant la simulation, les résultats des simulations obtenues confirment l'efficacité et la sécurité de notre schéma en utilisant les différentes mesures de sécurité.

Organisation de la thèse

Notre travail est réparti en deux parties, la première partie présente le contexte de notre travail, alors que la seconde partie expose notre contribution. La première partie est composée de trois chapitres. Dans un premier lieu , le premier chapitre donnera une brève présentation des notions de base en mathématiques nécessaires utilisées dans le reste de la thèse. Dans le deuxième chapitre nous mettrons en avant les outils et les techniques cryptographiques, et particulièrement les grandes classes des cryptosystèmes. Le troisième met le point sur les différentes techniques de cryptage d'images.

La deuxième partie de notre travail, laquelle est divisée en deux chapitres, consiste à présenter les deux contributions que nous avons proposées. Le manuscrit s'achève par une conclusion générale et quelques perspectives pouvant aider dans l'amélioration du système dans le futur.

Première partie

Introduction sur le domaine de recherche

Chapitre 1

Outils mathématiques

1.1 Introduction

La cryptographie est basée sur certains domaines spécifiques des mathématiques, y compris la théorie des nombres, l'algèbre linéaire, et les structures algébriques. Dans ce chapitre, on va acquérir brièvement les notions de base nécessaires pour comprendre le reste de notre thèse. Tout d'abord, on va examiner l'arithmétique modulaire en passant par l'arithmétique entière. Ensuite nous allons présenter trois structures algébriques : les groupes, les anneaux, et les corps. Finalement, on va décrire brièvement les matrices citons : les matrices particulières, les opérations sur les matrices et quelques matrice inversibles spéciales.

1.2 L'arithmétique entière

1.2.1 L'ensemble des entiers

L'ensemble des entiers, noté $\mathbb{Z}$, contient tous les nombres entiers (sans fraction) de l'infini négatif à l'infini positif comme le présente la figure.1.1.

$$\mathbf{Z = \{\ \ldots, \text{-}2, \text{-}1, 0, 1, 2, \ldots\}}$$

FIGURE 1.1 – L'ensemble des entiers

1.2.2 Les opérations binaires

Dans la cryptographie, nous nous intéressons à trois opérations binaires appliquées à l'ensemble des entiers. Une opération binaire prend deux entrées et retourne une sortie (voir la figure 1.2).

1.2.3 La division entière

Dans l'arithmétique entière, si on divise a par n, nous obtiendrons q et r comme le montre la figure 1.3.

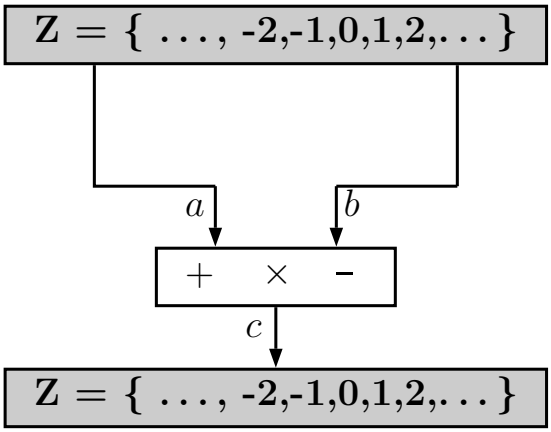


FIGURE 1.2 – Les opérations binaires

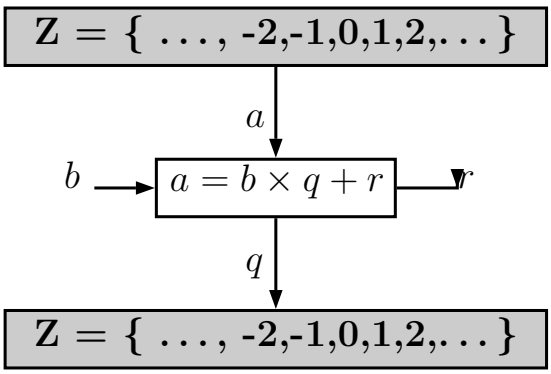


FIGURE 1.3 – La division entière

La relation entre ces quatre nombres peut être présentée comme suit :

$$a = q \times b + r \quad 0 \leq r < b \tag{1.1}$$

1.2.4 Divisibilité

Soient : a, b, et m trois nombres entiers tel que : $b \neq 0$.
On dit que b divise a si $a = m \times b$. Autrement dit, si le reste de la division de a par b est 0.
La notation $b|a$ est généralement utilisée pour signifier que b divise a. En outre, si $b|a$, nous disons que b est un diviseur de a.

Propriété

- Si $a|1$ alors $a = \pm 1$.
- Si $a|b$ et $b|a$, alors $a = \pm b$.
- $\forall b \neq 0$, alors b divise 0.
- Si $a|b$ et $b|c$ alors $a|c$.
- Si $b|g$ et $b|h$ alors $b|(mg + nh)$ tel que $n, m \in \mathbb{Z}$

Remarques

- Le nombre entier 1 a un seul diviseur qui est 1.
- Chaque nombre entier positif a au moins deux diviseurs 1 et le nombre lui même.

1.2.5 L'algorithme d'Euclide

L'algorithme d'Euclide [28, 29] est une technique de base dans la théorie des nombres, il présente une simple procédure permettant de déterminer le plus grand commun diviseur de deux nombres.

Le plus grand commun diviseur

Un nombre entier c est dit le plus grand commun diviseur de a et b Si :

1. c divise a et b.
2. Tout diviseur de a et b est un diviseur de c

Notation On note le plus grand commun diviseur de a et b par : pgcd(a, b)

Propriétés

- On définit pgcd(0,0) = 0.

- $\forall a \neq 0$, pgcd(a,0) = $|a|$.
- On dit que deux entiers a et b sont premiers entre eux si : pgcd$(a,b) = 1$.

Trouver le plus grand commun diviseur

On va illustrer l'algorithme d'Euclide [30] désigné pour trouver facilement le plus grand commun diviseur de deux nombres.

Soient a, b et c trois nombres entiers tel que $c = \text{pgcd}(a,b)$. En divisant a par b, on obtiendra :

$$a = q_1 \times b + r_1 \qquad 0 \leq r_1 < b \tag{1.2}$$

Si $r_1 = 0$, alors $b|a$ et $d = \text{pgcd}(a,b) = d$.
Mais, si $r_1 \neq 0$, alors $b > r_1$ donc on peut diviser b par r_1 comme suit :

$$b = q_2 \times r_1 + r_2 \qquad 0 \leq r_2 < r_1 \tag{1.3}$$

Comme précédemment, le processus de division se continue jusqu'à l'apparition d'un reste nul dans un stage $n+1$. Le résultat est présenté dans le système d'équation suivant :

$$\left.\begin{array}{ll} a = q_1 \times b + r_1 & 0 \leq r_1 < b \\ b = q_2 \times r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 = q_3 \times r_2 + r_3 & 0 \leq r_3 < r_2 \\ \vdots & \vdots \\ r_{n-2} = q_n \times r_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} = q_{n+1} \times r_n + 0 & \\ d = \text{pgcd}(a,b) = r_n & \end{array}\right\} \tag{1.4}$$

Dans chaque itération, on a $d = \text{pgcd}(r_i, r_{i+1})$ jusqu'à l'itération finale ou $d = \text{pgcd}(r_n, 0) = r_n$.
Ainsi, on peut obtenir le plus grand commun diviseur de deux entiers en utilisant des divisions successives. Ce schéma est connu par l'algorithme d'Euclide.
La table 1.1 présente un exemple qui démontre la puissance de l'algorithme d'Euclide en utilisant des grands nombres.

$a = q_1 b + r_1$	98657544960 = 4 × 21346752440 + 13270535200	d = pgcd(21346752440, 13270535200)
$b = q_2 r_1 + r_2$	21346752440 = 1 ×13270535200 + 8076217240	d= pgcd(13270535200, 8076217240)
$r_1 = q_3 r_2 + r_3$	13270535200 = × 8076217240 +5194317960	d = pgcd(8076217240, 5194317960)
$r_2 = q_4 r_3 + r_4$	8076217240 = × 5194317960 + 2881899280	d = pgcd(5194317960, 2881899280)
$r_3 = q_5 r_4 + r_5$	5194317960 = × 2881899280 + 2312418680	d = pgcd(2881899280, 2312418680)
$r_4 = q_6 r_5 + r_6$	2881899280 = × 2312418680 + 569480600	d = pgcd(2312418680, 569480600)
$r_5 = q_7 r_6 + r_7$	2312418680 = × 569480600 + 34496280	d = pgcd(569480600, 34496280)
$r_6 = q_8 r_7 + r_8$	569480600 = × 34496280 + 17540120	d = pgcd(34496280, 17540120)
$r_7 = q_9 r_8 + r_9$	34496280 = × 17540120 + 16956160	d = pgcd(17540120, 16956160)
$r_8 = q_{10} r_9 + r_{10}$	17540120 = × 16956160 +583960	d = pgcd(16956160, 583960)
$r_9 = q_{11} r_{10} + r_{11}$	16956160 = × 583960 +21320	d = pgcd(583960, 21320)
$r_{10} = q_{12} r_{11} + r_{12}$	583960 = × 21320 +8320	d = pgcd(21320, 8320)
$r_{11} = q_{13} r_{12} + r_{13}$	21320 = × 8320 + 4680	d = pgcd(8320, 4680)
$r_{12} = q_{14} r_{13} + r_{14}$	8320 = × 4680 + 3640	d = pgcd(4680, 3640)
$r_{13} = q_{15} r_{14} + r_{15}$	4680 = × 3640 + 1040	d = pgcd(3640, 1040)
$r_{14} = q_{16} r_{15} + r_{16}$	3640 = × 1040 + 520	d = pgcd(1040, 520)
$r_{15} = q_{17} r_{16} + r_{17}$	1040 = × 520 +0	d = pgcd(520, 0) = 520

TABLE 1.1 – pgcd(98657544960, 21346752440)

1.3 L'arithmétique modulaire

La relation de division précédente(Eq.(1.3)) a deux entrées et deux sorties, dans l'arithmétique modulaire (mod), nous nous intéressons seulement par une seule sortie, le reste r comme le montre la figure 1.4.

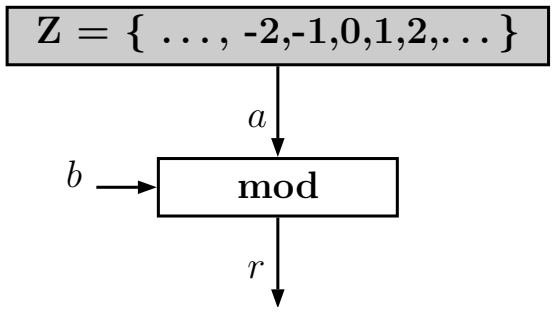


FIGURE 1.4 – L'opérateur mod

1.3.1 L'ensemble $\mathbf{Z}_n$

L'opération modulo crée un ensemble, noté $\mathbf{Z}_n$. La figure 1.5 montre quelques ensembles $\mathbf{Z}_n$.

$$\mathbf{Z}_n = \{\ 0,\ 1,\ 2,\ 3,\ \ldots,\ (n\text{-}1)\ \}$$

$\mathbf{Z}_2 = \{\ 0,\ 1\ \}$ $\mathbf{Z}_6 = \{\ 0,\ 1,\ 2,\ 3,\ 4,\ 5\ \}$ $\mathbf{Z}_{10} = \{\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\ \}$

FIGURE 1.5 – Quelques ensembles $\mathbf{Z}_n$

1.3.2 L'opérateur de congruence

Pour montrer que deux entiers sont congrus, nous utilisons l'operateur de congruence ($\equiv$).

Propriétés

1. $a \equiv b \bmod n$ Si $n|(a-b)$
2. $a \equiv b \bmod n \Longrightarrow b \equiv a \bmod n$
3. $a \equiv b \bmod n$and $b \equiv c \bmod n \Longrightarrow a \equiv c \bmod n$

Les classes de congruance Une classe de congruance $[a]$ ou $[a]_n$ est l'ensemble des entiers congrus modulo n.

$$[a] = r : \text{un entier} / r \equiv a \bmod n \tag{1.5}$$

Exemple Les classes de congruance modulo 5 sont comme suit :
$[0] = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$
$[1] = \{\ldots, -16, -11, -6, 1, 6, 11, 16, \ldots\}$
$[2] = \{\ldots, -17, -12, -7, 2, 7, 12, 17, \ldots\}$
$[3] = \{\ldots, -18, -13, -8, 3, 8, 13, 18, \ldots\}$
$[4] = \{\ldots, -19, -14, -9, 4, 9, 14, 19, \ldots\}$

1.3.3 Les opérations dans $\mathbf{Z}_n$

Les trois opérations binaires dont nous avons discuté pour l'ensemble $\mathbb{Z}$ peuvent également être définies pour l'ensemble $\mathbf{Z}_n$ en utilisant l'opérateur mod (Voir la figure 1.6). Les tables 1.2 et 1.3 présentent des illustrations de l'addition et de la multipli-

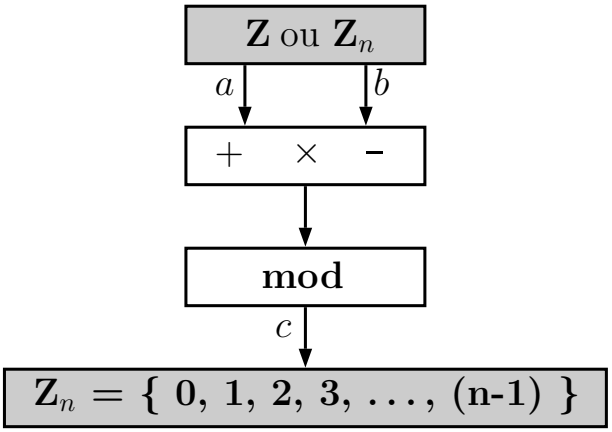


FIGURE 1.6 – Les opérations binaires dans $\mathbf{Z}_n$

cation modulaires modulo 8. En regardant plus, les résultats sont simples, et les deux matrices sont symétriques par rapport à la diagonale principale.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

TABLE 1.2 – Addition modulo 8

Propriétés

1. $[(a \bmod n) + (b \bmod n) = (a+b) \bmod n]$
2. $[(a \bmod n) - (b \bmod n) = (a-b) \bmod n]$
3. $[(a \bmod n) \times (b \bmod n) = (a \times b) \bmod n]$

1.3.4 Inverses

Dans l'arithmétique modulaire, nous aurons souvent besoin de trouver l'inverse d'un nombre par rapport à une opération, un inverse additif (par rapport à une opéra-

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

TABLE 1.3 – Multiplication modulo 8

tion d'addition) ou un inverse multiplicatif (par rapport à une opération de multiplication).

- **Inverse additif :** Dans $\mathbf{Z}_n$, deux nombres a et b sont inverses l'un de l'autre additivement si :

$$a + b \equiv 0 \bmod n \tag{1.6}$$

- **Inverse multiplicatif :** Dans $\mathbf{Z}_n$, deux nombres a et b sont inverses l'un de l'autre multiplicativement si :

$$a \times b \equiv 1 \bmod n \tag{1.7}$$

1.3.5 L'algorithme d'Euclide

L'algorithme d'Euclide peut être basé sur le théorème suivant :
Pour tout entier positif a, b :

$$\text{pgcd}(a, b) = \text{pgcd}(b, a \bmod b) \tag{1.8}$$

Nous pouvons définir l'algorithme d'Euclide en utilisant la fonction récursive suivante :

Algorithm 1 Euclid(a, b)

```
1: if (b = 0) then return a
2: else
       return Eclide(b, a mod b)
```

1.3.6 L'algorithme d'Euclide Étendu

Pour des entiers donnés a et b, l'algorithme d'Euclide étendu [31] non seulement calcule le plus grand commun diviseur d, mais aussi deux entiers supplémentaires x et y tel que :

$$ax + by = d = \text{pgcd}(a, b) \tag{1.9}$$

Ainsi, si $d = 1$, l'algorithme d'Euclide étendu permet de calculer l'inverse multiplicatif d'un nombre.

1.4 Les structures algébriques

La cryptographie exige des ensembles de nombres entiers et des opérations spécifiques qui sont définies pour ces ensembles. La combinaison des ensembles et des opérations qui sont appliqués aux éléments de l'ensemble est appelé une structure algébrique. Dans cette section, nous allons définir trois structures algébriques : les groupes, les anneaux, et les corps.

1.4.1 Groupe

On appelle groupe [32, 33, 34] tout ensemble $(G, \bigstar)$ muni d'une loi de composition interne vérifiant les trois propriétés suivantes :

1. la loi $\bigstar$ est associative
2. $(G, \bigstar)$ possède un élément neutre e.
3. tout élément de G est inversible pour la loi $\bigstar$.

Exemple L'ensemble des entiers de résidus avec l'opérateur d'addition, $G = (\mathbf{Z}_n, +)$, est un groupe commutatif. Nous pouvons effectuer l'addition et la soustraction sur les éléments de cet ensemble sans sortir de l'ensemble.

Sous groupe

Soit H une partie non vide d'un groupe $(G, \bigstar)$, alors H est dite sous groupe de $(G, \bigstar)$ si :

1. $x, y \in H \Longrightarrow x \bigstar y \in H$
2. $x \in H \Longrightarrow x^{-1} \in H$

Groupe cyclique

En particulier on note $\langle g \rangle$ le sous groupe engendré par $\{g\}$. Ce sous groupe est constitué de la suite :

$$g^0, g, g^2, g^3, ...g^n \tag{1.10}$$

S'il est fini ce groupe est dit cyclique.

1.4.2 Anneau

Soit $\mathbb{A}$ un ensemble muni de deux opérations notées + et $\cdot$

1. On dit que $(\mathbb{A}, +, \cdot)$ est un pseudo-anneau si et seulement si :
   - $(\mathbb{A}, +)$ est un groupe abélien
   - $\cdot$ est associative
   - $\cdot$ est distributive sur +
2. On dit que $\mathbb{A}$ est un anneau si et seulement si :
   - $\mathbb{A}$ est un pseudo-anneau
   - $\mathbb{A}$ admet un élément neutre pour $\cdot$
3. On dit que $\mathbb{A}$ est un anneau commutatif si et seulement si :
   - $\mathbb{A}$ est un anneau
   - $\cdot$ est commutative

1.4.3 Corps

Un ensemble $\mathbb{K}$ muni de deux lois : + et · est appelé corps si et seulement si :

1. $\mathbb{K}$ est un anneau
2. Tout élément non nul de $\mathbb{K}$ admet un inverse pour · dans $\mathbb{K}$

Corps fini

Un corps fini est un corps commutatif qui est par ailleurs fini. Généralement trois types de corps finis sont utilisés dans la cryptographie :

- **Corps premier F_p :** Lorsque $n = 1$, le corps fini F_p peut être l'ensemble $Z_p = 0, 1, ..., p - 1$, avec deux opérations arithmétiques.
- **Corps binaire F_{2^n} :** Un corps binaire F_{2^n} est un ensemble de 2^n éléments. Les éléments de cet ensemble sont des mots de n bits.
- **Les corps F_{p^n}**

1.5 Les matrices

1.5.1 Définition

Une matrice A de dimention $m \times n$ est un tableau de m lignes et n colonnes formées d'éléments d'un ensemble $\mathbb{K}$[35] .

Les nombres qui composent la matrice sont appelés les coefficients de la matrice (ou aussi les éléments). Une matrice à m lignes et n colonnes est dite matrice d'ordre (m, n) ou de dimension $m \times n$. On note alors :

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & a_{ij} & \vdots \\ a_{n1} & \dots & \dots & a_{nm} \end{pmatrix}$$

1.5.2 Matrices particulières

Matrice nulle

On appelle une matrice dont tous les éléments sont nuls une matrice nulle.

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & 0 \end{pmatrix} = (0)$$

Matrice colonne

On appelle matrice-colonne une matrice d'ordre $(n, 1)$.

$$A = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}$$

Matrice ligne

On appelle matrice-ligne une matrice d'ordre $(1, m)$.

$$A = \begin{pmatrix} a_1 & a_2 \dots & a_m \end{pmatrix}$$

Matrice carrée

On appelle matrice carrée d'ordre n une matrice d'ordre (n, n).
L'ensemble des matrices carrées de dimension n dans $\mathbb{K}$ est notée $M_{n,n}(\mathbb{K})$ ou $M_n(\mathbb{K})$.

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & a_{ij} & \vdots \\ a_{n1} & \dots & \dots & a_{nn} \end{pmatrix}$$

Propriété L'ensemble des matrices carrées $M_n(\mathbb{K})$ possède pour l'addition et la multiplication une structure d'anneau.

Sous matrice

On appelle sous-matrice (ou matrice extraite) de A toute matrice obtenue en supprimant dans A un certain nombre de lignes et/ou de colonnes.

Matrice triangulaire supérieure

On appelle matrice triangulaire supérieure toute matrice carrée d'ordre n dont les valeurs sous la diagonale principale sont nulles ($\forall j < i, m_{ij} = 0$).

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & \dots & a_{1n} \\ 0 & a_{22} & \dots & \dots & a_{2n} \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & a_{nn} \end{pmatrix}$$

Matrice triangulaire inférieure

Une matrice triangulaire inférieure est une matrice carrée dont les valeurs au-dessus de la diagonale principale sont nulles ($\forall j > i, m_{ij} = 0.$).

$$A = \begin{pmatrix} a_{11} & 0 & \dots & \dots & 0 \\ a_{21} & a_{22} & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & 0 \\ a_{n1} & a_{n2} & \dots & \dots & a_{nn} \end{pmatrix}$$

Matrice diagonale

On appelle matrice diagonale une matrice à la fois triangulaire inférieure et triangulaire supérieure. Les seuls coefficients pouvant être non nuls sont donc ceux de la diagonale.

$$A(a_1, a_2, \ldots, a_n) = \begin{pmatrix} a_1 & 0 & \ldots & 0 & 0 \\ 0 & a_2 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & a_{n-1} & 0 \\ 0 & 0 & \ldots & 0 & a_n \end{pmatrix}$$

Matrices scalaires

Ce sont les matrices diagonales dont tous les coefficients diagonaux sont égaux. Par exemple :

$$A = \begin{pmatrix} \pi & 0 & \ldots & 0 & 0 \\ 0 & \pi & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & \pi & 0 \\ 0 & 0 & \ldots & 0 & \pi \end{pmatrix}$$

Matrice identité

C'est la matrice scalaire dont tous les coefficients diagonaux valent 1. On note I_n la matrice identité d'ordre n. Par exemple :

$$I_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

1.5.3 Opérations sur les matrices

Égalité de deux matrices

On dit que deux matrices sont égales si elles sont de même type et si les coefficients situés à la même place sont égaux.

Addition de matrices

Définition L'addition des matrices est définie pour deux matrices de même type. La somme de deux matrices de type (m,n), $A=(a_{ij})$ et $B=(b_{ij})$, notée $A+B$, est une matrice (c_{ij}) de type (m,n) obtenue en additionnant les coefficients situés aux mêmes emplacement($c_{ij}=a_{ij}+b_{ij}$).

Propriété L'addition ainsi définie est une loi de composition interne. Cette loi munit l'ensemble des matrices du type (n,m) d'une structure de groupe abélien représentée dans le tableau suivant :

$A+B=B+A$	commutativité
$A+(B+C)=(A+B)+C$	associativité
$A+0=0+A=A$	élément neutre (0 représente la matrice nulle)
$A+(-A)=0$	élément symétrique

TABLE 1.4 – Structure de groupe abélien formée par l'addition de deux matrices

Multiplication d'une matrice par un scalaire

Définition Le produit d'une matrice A par un scalaire, noté $a \in K$, est la matrice obtenue en multipliant chaque élément de A par a [36, 37] :

$$C=aA \Longleftrightarrow c_{ij}=aa_{ij} \tag{1.11}$$

Propriétés La multiplication d'une matrice par un scalaire est une loi de composition externe vérifiant les propriétés :

- $\forall(\alpha,\beta)\in\mathbb{K}^2$ et $\forall(A,B)\in M^2_{n,m}(\mathbb{K})$
- $\alpha(A+B)=\alpha A+\alpha B$
- $(\alpha+\beta)A=\alpha A+\beta A$
- $\alpha(\beta A)=(\alpha\beta)A$
- $1A=A$

Produit de deux matrices

Soient : $A = (a_{ik})$ et $B = (a_{kj})$ deux matrices de type (n, m) et (m, p) respectivement. A et B peuvent se multiplier.
Le produit de ces deux matrices est une matrice $C = (c_{ij})$ de type (n, p), où l'élément c_{ij} de C est obtenu en multipliant la i$^{\text{ème}}$ ligne de A par la j$^{\text{ème}}$ colonne de B.

$$C = AB \Longleftrightarrow c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{im}b_{mj} = \sum_{k=1}^{m} a_{ik}b_{kj} \tag{1.12}$$

1.5.4 Transposition d'une matrice

On appelle matrice transposée d'une matrice A de type (n, m) , la matrice notée A^t obtenue en échangeant les lignes et les colonnes de même indice i de A :

$$A = a_{ij} \Longleftrightarrow A^t = a^t_{ij} = a_{ji} \tag{1.13}$$

1.5.5 Déterminant d'une matrice

Le déterminant d'une matrice carée $A \in M_n(\mathbb{K})$ noté : **det(**A**)** est un scalaire calculé récursivement comme suit :

1. Si $n = 1$, $\det(A) = a_{11}$
2. Si $n > 1$, $\det(A) = \sum_{i=1}^{m}(-1)^{i+j} \times a_{ij} \times \det(A_{ij})$.
   Où A_{ij} est la matrice obtenue en supprimant la i$^{\text{ème}}$ ligne et la j$^{\text{ème}}$ colonne de A.

1.5.6 Inversion de matrices

Définition L'inverse d'une matrice carrée $A \in M_n(\mathbb{K})$ est une matrice carrée $B \in M_n(\mathbb{K})$ telle que $AB = BA = I$(I matrice identité).
La matrice B est alors notée : A^{-1}.

Propriété

- Deux matrices B_1 et B_2 inverses de la même matrice A sont égales.

- Il suffit qu'une matrice B vérifie l'une des relations $AB = I$ et $BA = I$ pour qu'elle vérifie l'autre.
- Si deux matrices A et B sont inversibles, leur produit est inversible et l'inverse du produit est le produit des inverses effectué dans l'ordre inverse. $(AB)^{-1} = B^{-1}A^{-1}$
- L'inverse de la transposée d'une matrice A est égale à la transposé de l'inverse : $[{}^tA]^{-1} = {}^t[A^{-1}]$.
- Déterminant de l'inverse d'une matrice : $\det(A^{-1}) = \det(A)^{-1}$.

Une matrice carrée n'admettant pas d'inverse est dite singulière. Une matrice carrée admettant une inverse est dite inversible ou régulière.

1.5.7 Matrices inversibles spéciales

Matrice diagonale

La matrice diagonale définie dans la section 1.5.2 est inversible si tous les éléments de la diagonale sont non nul. On peut écrire $D^{-1}(D_1, D_2, \ldots, D_n)$ l'inverse de $D(D_1, D_2, \ldots, D_n)$ comme suit :

$$D^{-1}(D_1, D_2, \ldots, D_n)) = \begin{pmatrix} \frac{1}{D_1} & 0 & \ldots & 0 & 0 \\ 0 & \frac{1}{D_2} & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & \frac{1}{D_{n-1}} & 0 \\ 0 & 0 & \ldots & 0 & \frac{1}{D_n} \end{pmatrix}$$

Matrice de Frobenius

Une matrice $F(F_1, F_2, \ldots, F_{m-1})_{n,n}(\mathbb{K})$ est dite matrice de Fronenius [38] si :

- $F(i, j) = 1$ pour $i = j$.
- Les éléments sous la diagonale d'une colonne choisie arbitrairement comme $F_1, F_2, \ldots, F_{m-1}$.
- $F(i, j) = 0$ autrement

Ainci, une matrice de Frobenius peut s'écrire comme suit :

$$F(F_1,F_2,\ldots,F_{m-1}) = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ F_1 & 1 & 0 & \ldots & 0 \\ F_2 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ F_{m-1} & 0 & 0 & \ldots & 1 \end{pmatrix}$$

$F^{-1}(F_1,F_2,\ldots,F_{m-1})$ l'inverse de la matrice $F(F_1,F_2,\ldots,F_{m-1})$ est une matrice de Frobenius en changeant le signe des éléments arbitraires.

$$F^{-1}(F_1,F_2,\ldots,F_{m-1}) = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ -F_1 & 1 & 0 & \ldots & 0 \\ -F_2 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -F_{m-1} & 0 & 0 & \ldots & 1 \end{pmatrix} = F(-F_1,-F_2,\ldots,-F_{m-1})$$

Matrice compagnon

Une matrice $C(C_1,C_2,\ldots,C_n)_{n,n}(\mathbb{K})$ est dite matrice compagnon [39] si :

- $C(i,i-1) = 1$
- Les élements de la dernière colonne sont choisis arbitrairement comme $C_1,C_2,\ldots,C_n$.
- $C(i,j) = 0$ autrement.

$$C(C_1,C_2,\ldots,C_n) = \begin{pmatrix} 0 & 0 & \ldots & 0 & C_1 \\ 1 & 0 & \ldots & 0 & C_2 \\ 0 & 1 & \ldots & 0 & C_3 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & C_n \end{pmatrix}$$

Une matrice compagnon est inversible si l'élément arbitraire $C_1 \neq 0$. C^{-1} l'inverse de $C(C_1, C_2, \ldots, C_n)$, est définie comme suit :

$$C^{-1}(C_1, C_2, \ldots, C_n) = \begin{pmatrix} \frac{-C_2}{C_1} & 1 & 0 & 0 & \ldots & 0 \\ \frac{-C_3}{C_1} & 0 & 1 & 0 & \ldots & 0 \\ \frac{-C_4}{C_1} & 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{-C_n}{C_1} & 0 & 0 & 0 & \ldots & 1 \\ \frac{1}{C_1} & 0 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

1.6 Conclusion

Dans ce chapitre, nous avons examiné le bagage mathématique qui sera utilisé dans la suite de la thèse. Une briève description de l'arithmétique entière et l'arithmétique modulaire a été fournie tout en présentant l'algorithme d'Euclide et l'algorithme d'Euclide étendu et en exposant leurs utilités. On a illustré aussi les structures algébriques et les matrices.

Dans le prochain chapitre, nous présenterons les outils et les techniques cryptographiques essentiels qui sont nécessaires dans cette thèse. Nous allons donner les terminologies de base, les objectifs de la cryptographie ainsi que les grandes classes des cryptosystèmes.

Chapitre 2

Concepts de base dans la Cryptographie

2.1 Introduction

Depuis des siècles, les gouvernements et leurs responsables d'armée ont créé des moyens pour qu'ils puissent communiquer en toute sécurité. Ces méthodes ont comme but d'assurer que seulement les personnes souhaitées puissent lire le contenu de leurs communications, ainsi, si un ennemi obtient une lettre il ne peut pas la lire[40]. Toutefois, pendant le Moyen Age, la cryptographie a commencé à progresser. Tous les gouvernements d'Europe occidentale utilisent la cryptographie, et les codes ont commencé de devenir plus populaires. C'est pourquoi les chiffres ont été couramment utilisés pour garder le contact avec les ambassadeurs.

Quand à l'histoire, les premières avancées majeures en cryptographie ont été faites en Italie [41]. Une organisation élaborée a été crée en 1452 à Venise ; dont le seul but est d'améliorer la cryptographie. Ils ont eu trois secrétaires de chiffrement qui ont créé des chiffres pour leur gouvernement. Comme ceci, le développement dans le domaine de la cryptographie continue ; elle n'est plus utilisée seulement dans le domaine militaire comme au début, néanmoins, la cryptographie fait partie de notre vie quotidienne : la création des mots de passe, la biométrie, les achats par internet, l'authentification et la signature numérique ainsi que beaucoup d'autres applications dans différents domaines.

En parallèle avec le développement de la cryptographie, une autre science a été développée et avait un grand succès semblable au succès de la cryptographie ; qui est la cryptanalyse. Pendant l'âge d'or de la civilisation islamique, El Kindi a créé la première méthode de cryptanalyse, connue comme l'analyse de fréquence, elle a été utilisée pour casser le cryptosystème de César [42] vers 1000 CE. De même, le progrès dans ce domaine accompagne le progrès de la cryptographie. D'ailleurs, Shannon [43] a confirmé que les chiffrements sont cassables avec suffisamment de texte chiffré.Il a également présenté deux concepts importants pour les cryptosystèmes modernes qui sont la "diffusion" et la "confusion" ; ceux-ci forment la base de nombreux systèmes cryptographiques modernes parce qu'ils ont une tendance à augmenter la charge de travail de la cryptanalyse [41].

Dans ce chapitre, nous introduisons les terminologies de base de la cryptographie, on décrit brièvement les objectifs de la cryptographie ainsi que les principes de la cryptanalyse. Nous abordons, par la suite, les deux principales familles de cryptosystèmes en énumérant par la suite les algorithmes de chiffrement symétrique et les différents modes du chiffrement symétrique moderne, et on termine par les avantages et les inconvénients des chiffres symétriques et asymétriques.

2.2 Terminologie de base

2.2.1 La cryptologie

La cryptologie est une science fondée sur les mathématiques ; elle comporte deux branches : la cryptographie et la cryptanalyse.

2.2.2 La cryptographie

La cryptographie [44] est une science portée sur la conceptualisation, la définition et la construction de systèmes informatiques qui répondent aux préoccupations de sécurité. La conception des systèmes cryptographiques doit être fondée de manière à maintenir une fonctionnalité souhaitée, même sous tentatives malveillantes visant à les faire dévier de leur fonctionnalité prescrite.

2.2.3 La cryptanalyse

La cryptanalyse est la science ou l'art d'étudier des chiffres, textes-chiffrés ou systèmes cryptographiques en utilisant des techniques mathématiques en vue de trouver des faiblesses qui permettront la récupération du texte clair à partir du texte chiffré, sans nécessairement connaître la clé du chiffrement.

2.2.4 Cryptosystème

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

2.2.5 Algorithme cryptographique

Est un ensemble d'instructions suivies afin de répliquer à une ou plusieurs préoccupations de sécurité.

2.2.6 Le chiffrement

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

2.2.7 Le déchiffrement

Est le moyen qui permet la reconstruction du message en clair à partir du message chiffré en utilisant la clé de déchiffrement.

2.3 Objectifs de la cryptographie

2.3.1 La confidentialité

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

2.3.2 L'intégrité

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

2.3.3 L'authentification

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

2.3.4 La non répudiation

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

2.4 Principe de la cryptanalyse

2.4.1 Principe de Kirchhoff

Le principe de Kerckhoffs[45] est l'un des principes de base de la cryptographie moderne. Il a été formulé à la fin du XIXe siècle par le cryptologue français Auguste Kerckhoffs. Le principe a été décrit comme suit : Un système cryptographique doit être sécurisé, même si tout ce qui concerne le système, à l'exception de la clé, est public.

Les publications les plus connues de Kerckhoffs sont deux articles publiés dans une revue française en 1883 dans le « Journal des sciences militaires» sous le titre «La Cryptographie Militaire » [46]. Ces deux articles ont une approche pratique, fondée sur l'expérience, y compris six principes de conception des algorithmes de chiffrement militaires :

1. Le système doit être matériellement, sinon mathématiquement indéchiffrable ;
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;
4. Il faut qu'il soit applicable à la correspondance télégraphique ;
5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;
6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

2.4.2 Types d'attaque sur un chiffrement

Attaque sur texte chiffré seul(COA)

L'attaque texte chiffré Connue (COA) est une méthode d'attaque utilisée dans la cryptanalyse quand l'attaquant a un accès aux textes Chiffrés et n'a pas accès aux textes clairs Correspondant. Une attaque COA réussie quand on peut déterminer le texte en claire à partir le texte chiffré. Parfois, l'attaquant peut même extraire la clé de chiffrement utilisée (Seuls les algorithmes faibles ne peuvent pas résister à l'attaque texte chiffré seule). L'attaque texte chiffré seul est illustrée dans la figure 2.1.

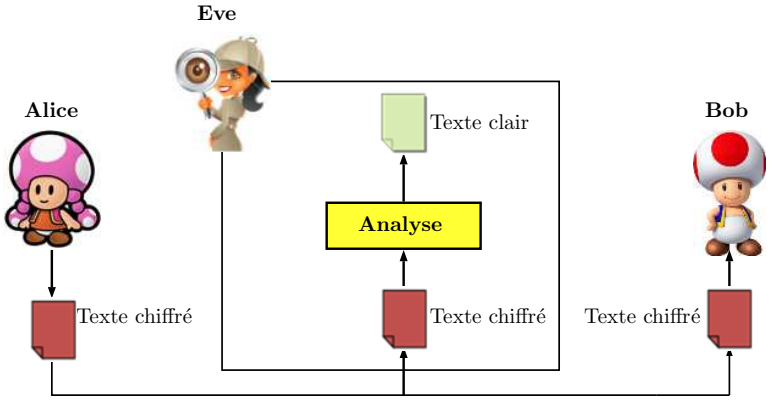


FIGURE 2.1 – Attaque texte chiffré seul

Attaque texte clair connu(KPA)

Ici, l'attaquant analyse une ou plusieurs paires de textes claires/chiffrés cryptées en utilisant la même clé. Le but de l'adversaire est de casser le reste du chiffrement (pour lequel il ne connaît pas le texte en clair correspondant). L'attaque texte clair connu est illustrée dans la figure 2.2.

Attaque texte clair choisi(CPA)

L'idée de base de l'attaque texte clair choisi est que l'adversaire dans ce cas est classé comme active ; il est autorisé à proposer différents textes clairs qu'il a choisit de manière adaptative. Ceci est formalisé en permettant l'adversaire à interagir librement avec un oracle de cryptage qui est considéré comme une boîte noire pour lui. Cette boite noire crypte les messages au choix de l'adversaire, et les textes chiffrés sont calculés en utilisant la clé secrète inconnue pour cet adversaire ; lorsque l'adversaire

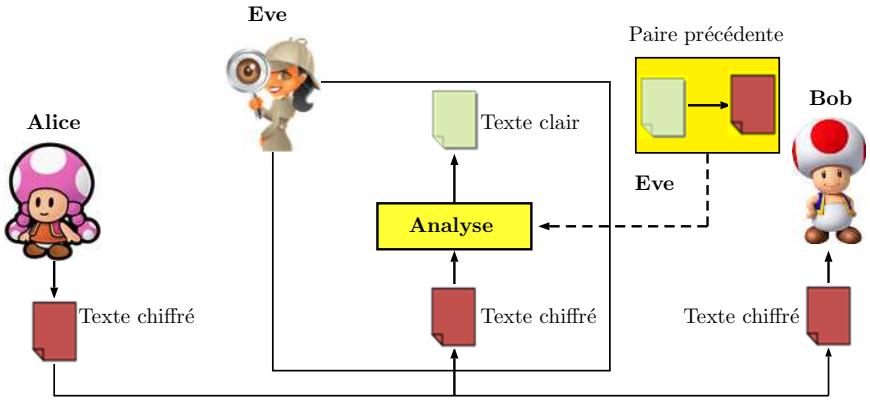


FIGURE 2.2 – Attaque texte clair connu

interroge son Oracle en fournissant un texte en clair comme entrée, l'oracle retourne un le texte chiffré comme réponse. L'attaque CPA est illustré dans la figure 2.3.

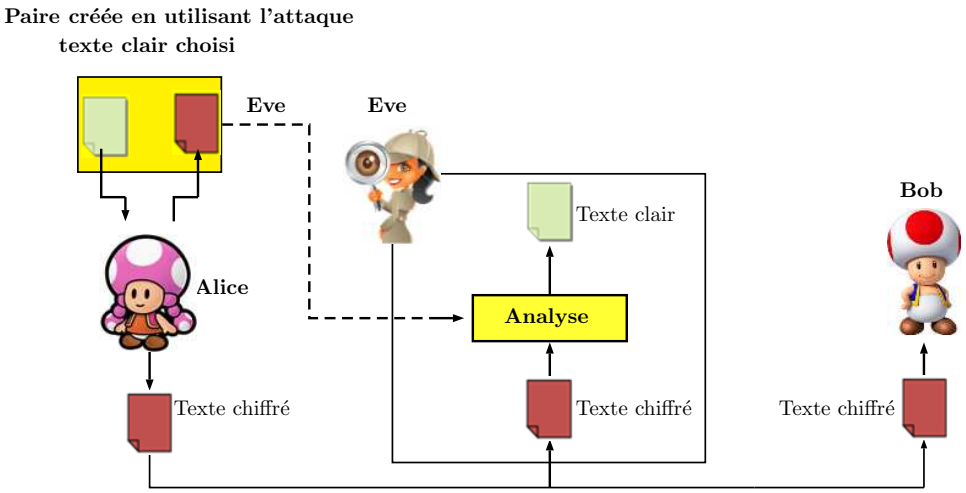


FIGURE 2.3 – Attaque CPA

Attaque texte chiffré choisi(CCA)

Dans une attaque texte chiffré choisie, l'adversaire a la possibilité de crypter tous les messages de son choix comme dans une attaque de type texte clair choisi, et aussi l'adversaire a la capacité de décrypter tout texte chiffré de son choix. Formellement, nous donnons à un adversaire l'accès à un oracle de décryptage et à un oracle de cryptage. L'attaque CPA est illustrée dans la figure 2.4.

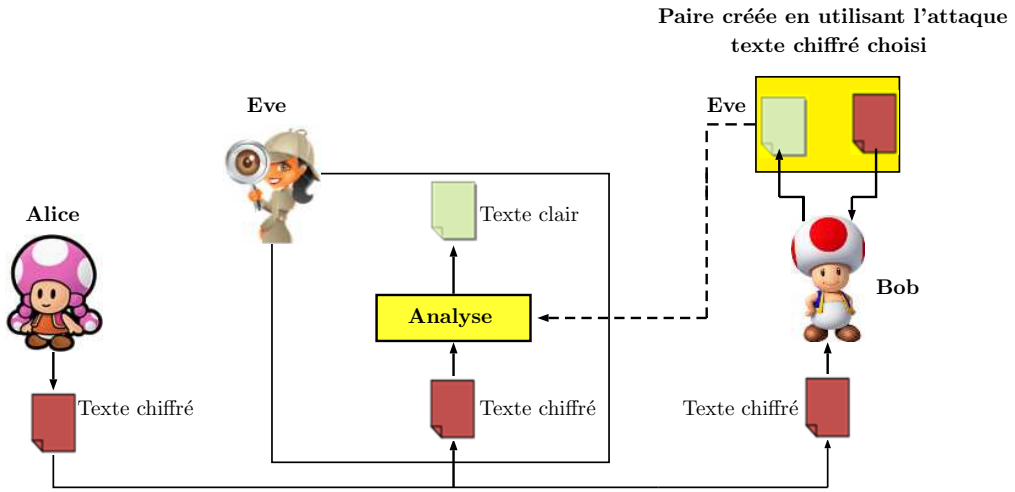


FIGURE 2.4 – Attaque CCA

2.5 Classification des systèmes cryptographiques

Les algorithmes de chiffrement sont classés en deux types : symétrique et asymétrique. Dans les algorithmes asymétriques on utilise la même clé pour le chiffrement et le déchiffrement, tandis que, dans les algorithmes asymétriques chaque entité a une clé publique et la clé secrète correspondante.

Dans les cryptosystèmes asymétriques, la clé publique ne doit pas être gardé secrète, et, en fait, peut être largement disponible ; alors que, son authenticité est nécessaire pour garantir qu'un interlocuteur est en effet la seule partie qui connaît la clé privée correspondante. Un avantage principal de ces systèmes est que la fourniture de clés publiques authentiques est généralement plus facile que de distribuer des clés secrètes en toute sécurité dans les systèmes à clé symétrique.

Les systèmes de chiffrement à clé publique sont généralement beaucoup plus lents que les algorithmes de chiffrement symétriques. Pour cette raison, le chiffrement à clé publique est plus utilisé dans la pratique pour le transport de clés symétriques et d'autres applications, y compris l'intégrité des données et l'authentification, et pour le cryptage des petits éléments de données telles que les numéros de cartes de crédit et codes PIN.

2.5.1 Cryptosystèmes symétriques

Les algorithmes symétriques, parfois appelés algorithmes classiques, sont les algorithmes où la clé de chiffrement peut être calculée à partir de la clé de déchiffrement, et

vice versa. Dans la plupart des algorithmes symétriques, la clé de chiffrement et la clé de déchiffrement sont les mêmes. Ces algorithmes exigent que l'émetteur et le récepteur se font d'accord sur une clé secrète, avant de commencer leurs communications, en toute sécurité. La sécurité d'un algorithme symétrique repose sur la clé ; divulguer la clé signifie que n'importe qui pourra chiffrer et déchiffrer des messages. Tant que la communication doit rester secrète, la clé doit rester secrète [47].

Le cryptage et le décryptage d'un message M en utilisant la clé secrète K avec un algorithme symétrique sont désignés par les équations suivantes :

$$E_K(M) = C \tag{2.1}$$

$$D_K(C) = M \tag{2.2}$$

Le cryptage symétrique est illustré dans la figure 2.5.

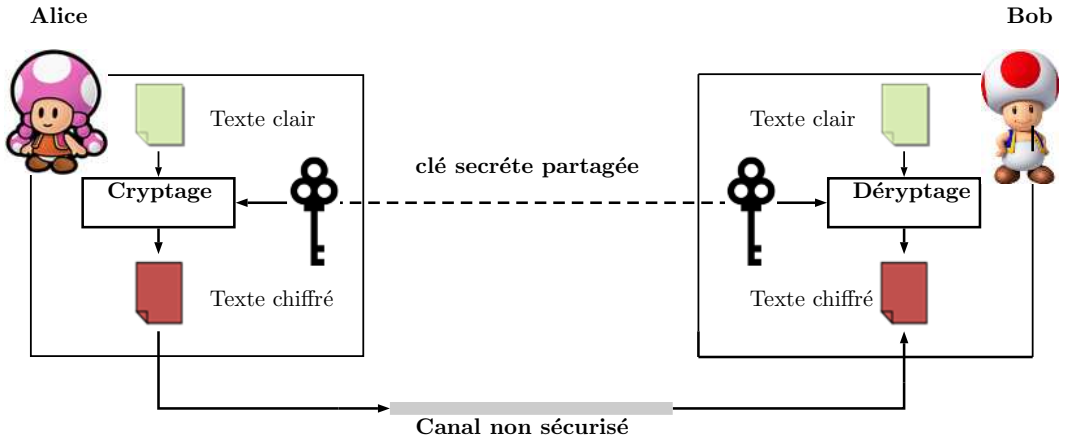


FIGURE 2.5 – Cryptage symétrique

2.5.2 Cryptosystèmes asymétriques

Le concept de la cryptographie à clé publique a été créé à partir des problèmes liés au chiffrement symétrique. Le premier problème est la distribution des clés. Le partage initial d'une clé secrète peut être fait en utilisant un canal sécurisé qui peut être mis en oeuvre, par exemple, en utilisant un service de messagerie fiable. En outre, cette option est susceptible d'être indisponible pour plusieurs entités qui n'ont pas les moyens de partager les clés de cette manière. Un procédé plus pragmatique qui permet à deux

parties de partager une clé est l'utilisation d'un centre de distribution de clés.

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

En 1976, Whiteld Diffie et Martin Hellman ont publié un document appelé « New Directions in Cryptography »[48] et l'influence de ce document a été énorme. Diffie et Hellman ont observé qu'il y a une asymétrie dans le monde : il y a certaine opérations qui peuvent être facilement réalisées mais ne peuvent pas être facilement inversées. Par exemple, de nombreux cadenas peuvent être verrouillés sans clé mais ne peuvent pas être rouvertes. Algorithmiquement, ils ont remarqué qu'il est facile de multiplier deux grands nombres premiers, mais difficile à retrouver ces nombres premiers à partir leur produit (le problème de factorisation). L'existence de tels phénomènes ouvre la possibilité de construction d'un schéma de chiffrement pour lequel les clés de chiffrement et de déchiffrement sont différentes.

Dans les systèmes de chiffrement à clé publique chaque entité A a une clé publique e et la clé privée correspondante d. Dans les systèmes sécurisés calculer d à partir de e est mathématiquement impossible. Si une entité B souhaite envoyer un message m à A, elle doit obtenir une copie authentique d'une clé publique e, elle utilise la transformation de cryptage (Voir équation(2.3)) pour obtenir le texte chiffré, ensuite elle transféra le message chiffré à A. Pour décrypter le message chiffré A applique la transformation de décryptage (Voir équation(2.5.2)) afin d'obtenir le message d'origine m. Le cryptage asymétrique est illustré dans la figure 2.6.

$$E_e(M) = C \tag{2.3}$$

$$D_d(C) = M \tag{2.4}$$

Les problèmes mathématiques basés sur la théorie de nombre qui forment la base de sécurité pour les systèmes de chiffrement à clé publique les plus connus sont énumérés dans le tableau 2.1.

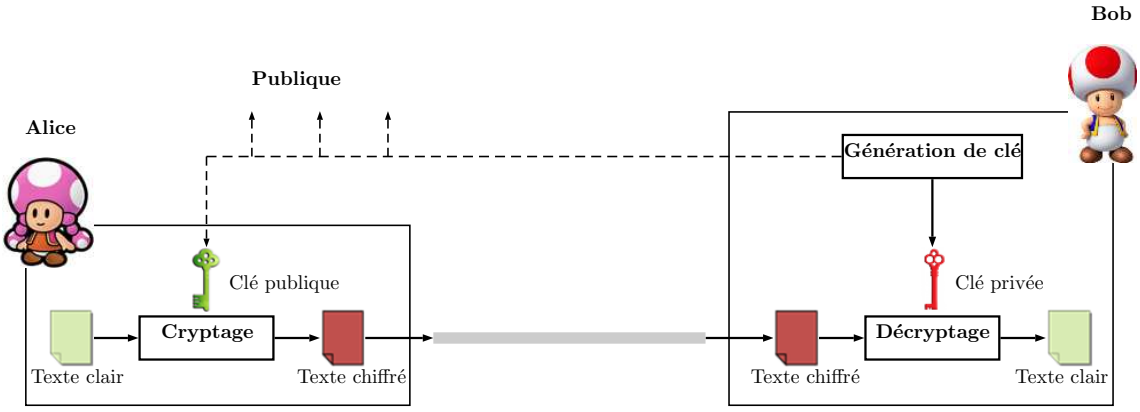


FIGURE 2.6 – Cryptage asymétrique

Cryptosystème assymétrique	Problèmes mathématiques
RSA [2]	Décomposition en produit de facteurs premiers
Rabin [49]	Factorisation des entier Résidu quadratique
ElGamal	Le logarithme discret
McEliece [50]	Problème de décodage des codes linéaires
Cryptosystème de Merkle-Hellman [51]	Problème de la somme de sous-ensembles

TABLE 2.1 – Systèmes de chiffrement à clé publique et les problèmes mathématiques connexes sur lesquels se fonde leur sécurité.

2.6 Classification des algorithmes de chiffrement symétrique

2.6.1 Chiffrement par blocs

Un chiffrement par bloc est une méthode de cryptage qui décompose le texte en clair en chaînes (appelés blocs) d'une longueur fixe t, et le chiffrement se fait bloc par bloc (un bloc à la fois). Pour les algorithmes de chiffrements par bloc modernes, la taille typique de blocs est 64 bits [47] ; assez grande pour empêcher l'analyse et assez petite pour être pratique.

Les techniques de cryptage à clé symétrique les plus connues sont des algorithmes de chiffrement par blocs. Il existe deux classes importantes de chiffrement par blocs : les algorithmes de chiffrement par substitution et les algorithmes de chiffrement par transposition.

Selon Shannon, la confusion et la diffusion sont les deux techniques de base pour masquer la redondance d'un message en clair. Ainsi, une substitution permet d'ajouter la confusion à un processus de cryptage tandis que la transposition permet d'ajouter la diffusion. La confusion est destinée à faire le lien entre la clé et le cryptosystème aussi complexe que possible. La diffusion se réfère à réarranger ou permuter les bits dans le message de sorte d'allonger la redondance du texte en clair sur le texte chiffré. Un tour peut alors être du à ajouter à la fois la confusion et la diffusion au cryptage. La plupart des systèmes de chiffrement par bloc modernes appliquent un certain nombre de tours, de confusion et diffusion, pour réussir le chiffrement.

Chiffrement par substitution

Un cryptage par substitution est celui dans lequel chaque caractère dans le texte en clair est remplacé par un autre caractère dans le texte chiffré. Le récepteur inverse la substituabilité du texte chiffré pour récupérer le texte en clair.

Dans la cryptographie classique, il existe quatre types de chiffrement par substitution :

La substitution simple : Un chiffrement par substitution simple, on peut dire aussi un chiffre monoalphabétique, est celui où chaque caractère du texte en clair est remplacé par le caractère correspondant du texte chiffré.

Si le nombre de caractères du l'alphabet est n alors le nombre de chiffres de substitutions distinctes est $n!$, il est indépendant de la taille de bloc dans le chiffre. En conséquence, un chiffre par substitution simple fournis une sécurité insuffisante, même lorsque l'espace de clé est extrêmement grand.

D'autre part, la répartition des fréquences des lettres est conservée dans le texte chiffré. Par exemple, la lettre E survient plus fréquemment que les autres lettres dans le texte français ordinaire. D'où la lettre produisant le plus fréquemment dans une séquence de blocs de texte chiffré est la plus susceptible de correspondre à la lettre E dans le texte en clair. En observant une quantité modeste de blocs de texte chiffré, un adversaire peut déterminer la clé[52].

Chiffrement homophone : Un chiffrement par substitution homophonique est comme un système de chiffrement par substitution simple, sauf qu'un caractère du texte en clair peut être assigné à un caractère parmi plusieurs caractères de texte chif-

fré. Par exemple, le caractère "A" pourrait correspondre soit à 7, 11, 19, ou 23, et ainsi de suite.

Un cryptage homophone peut être utilisé pour rendre la fréquence d'occurrence des symboles de texte chiffré plus uniformes. Le décryptage n'est pas aussi facile que celui de chiffre de substitution simple, mais toujours ne pas occulter toutes les propriétés statistiques de la langue en claire. Avec une attaque texte clair connu ou texte chiffré uniquement, les chiffres sont cassables.

Chiffrement par substitution polygramme : Un cryptage de substitution de polygramme est celui où les blocs de caractères sont cryptés en groupes. Le chiffre de Playfair [30] et le chiffrement de Hill [53] sont deux exemples du chiffre polygramme, les deux chiffres ont été cassés.

Chiffrement par substitution polyalphabetique : Un chiffrement par substitution polyalphabétique est constitué de plusieurs chiffres de substitution simples. Le chiffrement de Vigenère [53] est un exemple de chiffres de substitution polyalphabétiques.

2.6.2 Chiffrement par flot

Un chiffrement de flux repose sur de simples transformations de chiffrements (tel que l'opération XOR) en utilisant le flux de clé. Le flux de clé pourrait être généré au hasard, ou par un algorithme qui génère le flux de clé à partir d'un premier seed, ou à partir d'un seed et des symboles de texte chiffré précédents. Ce type de chiffrement arrive à traiter les données de longueur quelconque et n'a pas besoin de les découper.

2.7 Chiffrement symétrique moderne (NIST 800-38A)

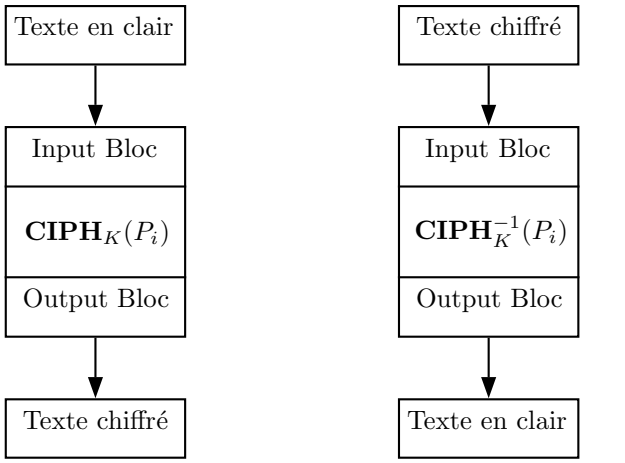
2.7.1 Dictionnaire de codes (ECB)

Il représente le mode de fonctionnement le plus naïf possible. Etant donné un message clair, la fonction de chiffrement est appliquée directement et indépendamment sur chaque bloc de texte en clair. La séquence résultante des blocs de sortie représente le texte chiffré. Réciproquement, l'opération du décryptage est appliquée directement

et indépendamment à chaque bloc de texte chiffré. La séquence résultante de blocs de sortie est le texte en clair. Le mode de cryptage ECB est illustré dans la figure 2.7 et l'algorithme 2.

Algorithm 2 Cryptage ECB

1: **input :** texte en claire : P ; clé secrète : K ;
2: **output :** texte chiffré : C
3: **for** i = 1 **to** n **do**
4: $C_i \leftarrow \text{CIPH}_K(P_i)$
5: **return** C



(a) Cryptage ECB **(b)Décryptage ECB**

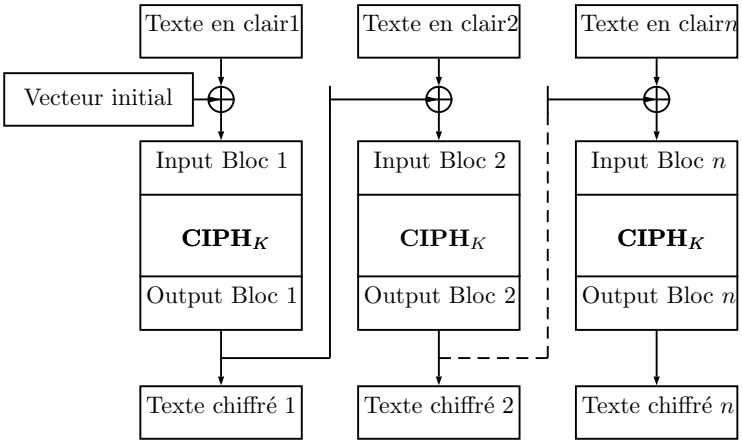
FIGURE 2.7 – Mode de cryptage ECB

Le processus de cryptage ici est déterministe, en utilisant la même clé le résultat de cryptage d'un bloc de texte en clair est toujours le même bloc de texte chiffré, donc le mode de fonctionnement ECB n'est pas sécurisé contre les attaques CPA. Si cette propriété est indésirable dans des applications particulières qui nécessitent un niveau élevé de sécurité où le mode ECB ne devra pas être utilisé.

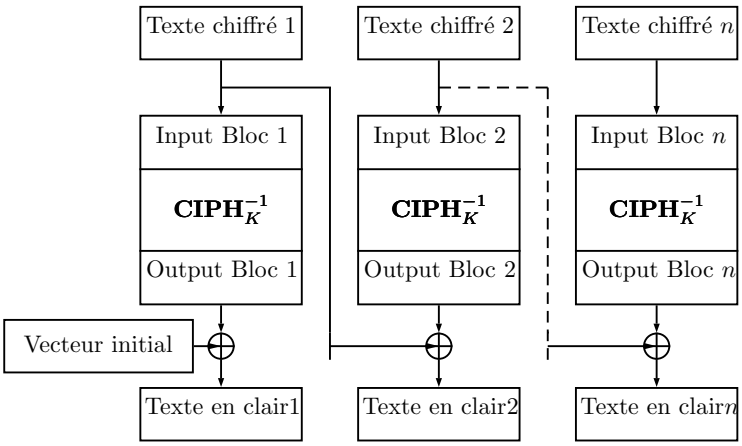
2.7.2 Enchaînement des blocs (CBC)

Dans ce mode, un vecteur initial aléatoire (IV) est d'abord choisi, pour le combiner avec le premier bloc de texte en clair, en utilisant l'opération XOR, avant d'être crypté. Après le chiffrement du premier bloc de texte en clair, le texte chiffré résultant est mémorisé dans un registre de rétroaction pour le combiner avec le deuxième bloc du texte en clair avant d'être crypté. Le texte chiffré ainsi obtenu est de nouveau stocké dans le

registre de rétroaction, pour le combiner avec le prochain bloc du texte en clair avant d'être crypté, et ainsi de suite jusqu'à la fin du message. Subséquemment, le chiffrement de chaque bloc dépend de tous les blocs précédents. L'enchaînement des blocs (CBC) est illustré dans la figure 2.8, et l'algorithm 3.



(a) Cryptage en mode CBC



(b) Déryptage en mode CBC

FIGURE 2.8 – Mode CBC

Dans le décryptage CBC, l'inverse de la fonction de chiffrement est appliqué sur le premier bloc de texte chiffré, puis on applique sur le bloc résultant un Ou exclusif avec le vecteur d'initialisation pour récupérer le premier bloc de texte en clair. L'inverse de la fonction de chiffrement est également appliqué au deuxième bloc de texte chiffré, puis on applique sur le bloc résultant un Ou exclusif avec le premier bloc de texte chiffré pour récupérer le deuxième bloc de texte en clair. En général, pour récupérer un bloc

Algorithm 3 Cryptage CBC

1: **input :** texte en claire : P, clé secrète : K, vecteur initial : IV ;
2: **output :** texte chiffré : C
3: $C_1 \leftarrow \text{CIPH}_K(P_1 \oplus IV)$
4: **for** i = 1 **to** n **do**
5: $\quad C_i \leftarrow \text{CIPH}_K(P_i \oplus IV)$
6: **return** C

de texte en clair (sauf le premier), l'inverse de la fonction de chiffrement est appliqué au bloc de texte chiffré correspondant, puis on applique sur le bloc résultant un Ou exclusif avec le bloc de texte chiffré précédent.

Le plus important, est que le cryptage en mode CBC est probabiliste. En effet, il été prouvé que si la fonction du cryptage est une permutation pseudo-aléatoire, alors le chiffrement CBC est CPA sécurisé [54]. Le vecteur IV ne doit pas être un secret ; il peut être transmis en clair avec le texte chiffré. Ceci est crucial pour que le déchiffrement soit réalisable (sans IV, il est impossible pour le destinataire d'obtenir le premier bloc de texte en clair).

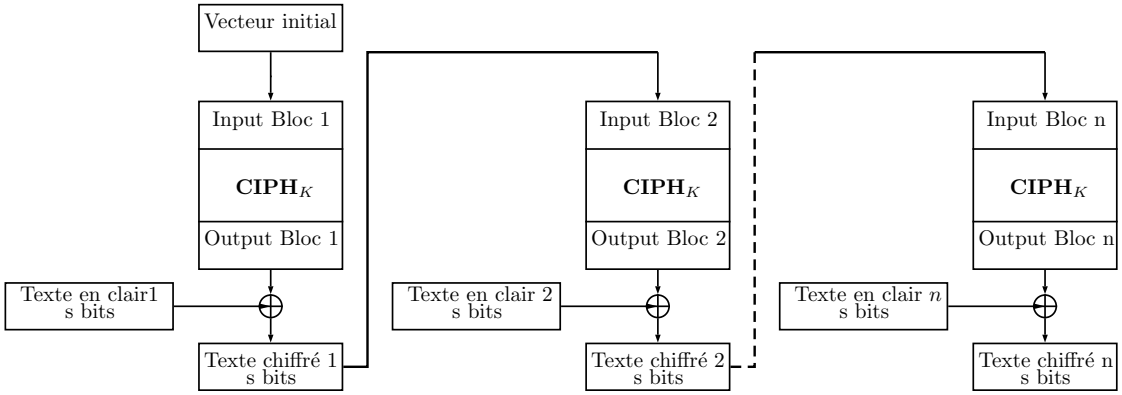
2.7.3 Chiffrement à rétroaction(CFB)

Le mode CBC traite le texte en clair par n bits à la fois (en utilisant un chiffrement par blocs de taille n bits), alors que, certaines applications nécessitent que les unités de texte en clair de taille r bits, où $r < n$ (R souvent = 1 ou r = 8), soient cryptées et transmises sans délai. Dans ce cas, on peut utiliser le mode de rétroaction de chiffrement (CFB).

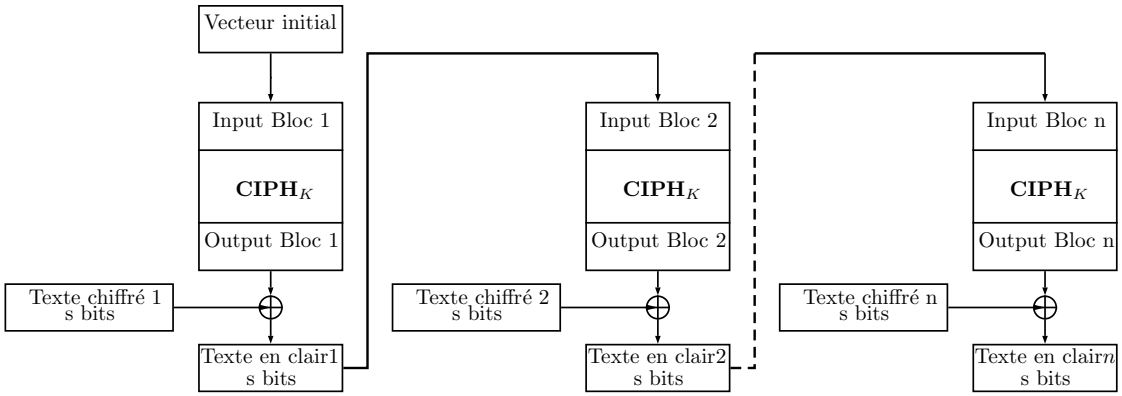
Le mode de cryptage à rétroaction est présenté dans la figure 2.9, tandis que une présentation algorithmique de la fonction de cryptage est donnée dans l'algorithmes 4.

Dans le cryptage CFB, le premier bloc entré est le IV, et l'opération de chiffrement-avant est appliquée à IV pour produire le premier bloc de sortie. Le premier segment de texte chiffré, qu'on peut transmettre, est produit en appliquant l'opération OU-Exclusif au premier segment de texte en clair avec les s bits les plus significatifs du premier bloc de sortie. (Les bits b-s restants du premier bloc de sortie sont ignorés).

Les s-b bits les moins significatifs de l'IV sont ensuite concaténés avec les s bits du premier segment de texte chiffré pour former le deuxième bloc d'entrée. On applique sur les bits du deuxième bloc d'entrée un décalage circulaire vers la gauche, et alors le



(a)Cryptage en mode CFB



(b)Déryptage en mode CFB

FIGURE 2.9 – Mode CFB

segment de texte chiffré remplace les s bits les moins significatifs du résultat. Ainsi, On continue de chiffrer le reste du texte en clair de la même manière.

2.7.4 Chiffrement à rétroaction de sortie (OFB)

Le mode OFB exige un nonce IV, à savoir que IV doit être unique pour chaque exécution du mode en utilisant une clé donnée. Le nonce IV est chiffré pour produire le premier bloc de sortie. On applique sur le bloc de sortie un Ou exclusif avec le premier bloc clair, pour produire le premier bloc de texte chiffré. La fonction de chiffrement est ensuite invoquée sur le premier bloc de sortie pour produire le deuxième bloc de sortie. On applique sur le deuxième bloc de sortie un Ou exclusif avec le deuxième bloc clair, pour produire le deuxième bloc de texte chiffré, et la fonction de chiffrement est invoquée sur le deuxième bloc de sortie pour produire le troisième bloc de sortie. Ainsi,

Algorithm 4 Cryptage CFB

input : texte en claire : P, clé secrète : K, vecteur initial : IV ;
output : texte chiffré : C
$I_1 \leftarrow IV$
$O_1 \leftarrow \text{CIPH}_K(I_1)$
$C_1 \leftarrow P_1 \oplus \text{MSB}_s(O_1)$
for i = 1 **to** n **do**
    $I_i \leftarrow \text{LSB}_{b-s}(I_{i-1})|C_{i-1}$
    $O_i \leftarrow \text{CIPH}_K(I_i)$
    $C_i \leftarrow P_i \oplus \text{MSB}_s(O_i)$
return C

les blocs de sorties successives sont produits à partir le chiffrement des blocs de sortie précédent, et les blocs de sortie sont invoqués pour une opération XOR avec les blocs de texte en clair correspondant pour produire les blocs de texte chiffré.

Comme dans le mode CBC, dans le mode OFB un texte chiffré dépend de tout le texte en clair précédent. Cependant, le IV doit être unique. Si le IV n'aura pas être unique, un adversaire peut récupérer le texte en clair correspondant. Il peut être un numéro de série, qui s'incrémente après chaque message et ne se répète pas pendant la durée de vie d'une clé.

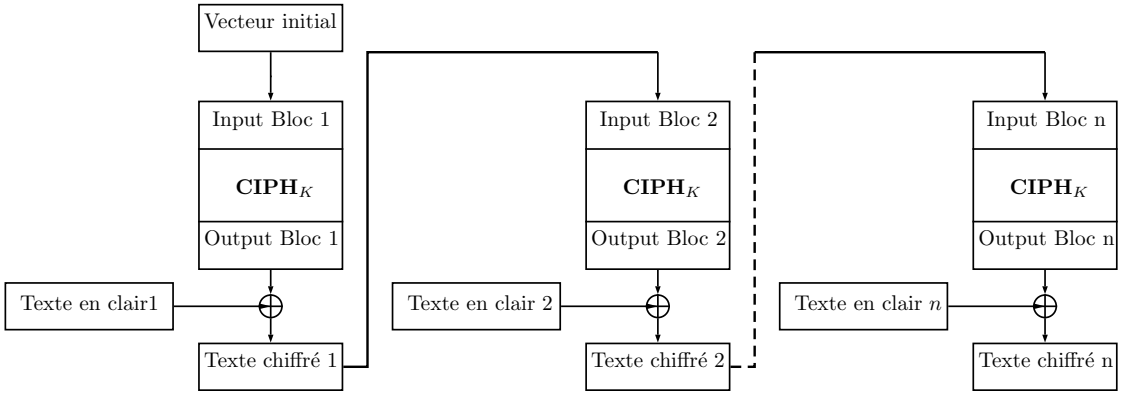
Le mode OFB est illustré sur la figure 2.10, et l'algorithme de cryptage 5.

Algorithm 5 Cryptage OFB

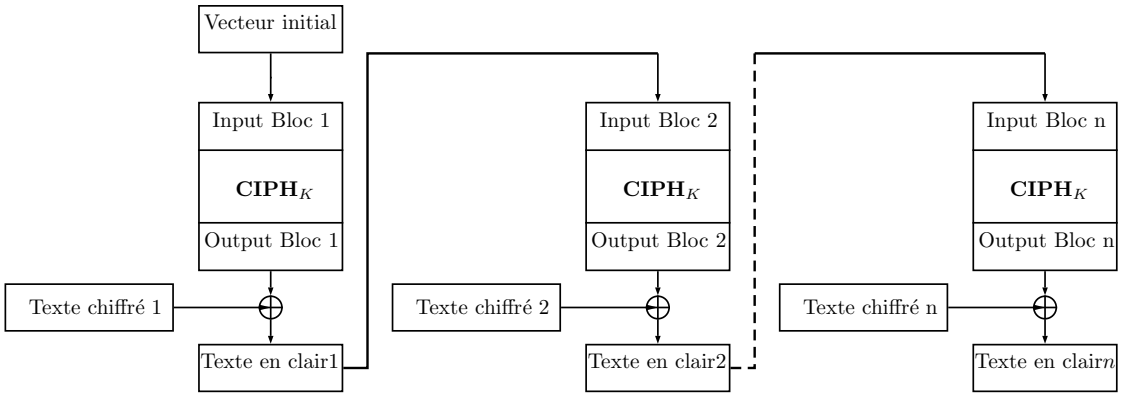
input : texte en claire : P, clé secrète : K, vecteur initial : IV ;
output : texte chiffré : C
$I_1 \leftarrow IV$
$O_1 \leftarrow \text{CIPH}_K(I_1)$
$C_1 \leftarrow P_1 \oplus (O_1)$
for i = 1 **to** n-1 **do**
    $I_i \leftarrow O_{i-1}$
    $O_i \leftarrow \text{CIPH}_K(I_i)$
    $C_i \leftarrow P_i \oplus O_i$
$C_n \leftarrow P_n \oplus \text{MSB}_u(O_i)$
return C

2.7.5 Chiffrement basé sur un compteur (CTR)

Ce mode de fonctionnement est moins fréquent que le mode CBC, mais il a un certain nombre d'avantages. Comme avec OFB, le mode CTR peut aussi être aussi consi-



(a)Cryptage en mode OFB



(b)Déryptage en mode OFB

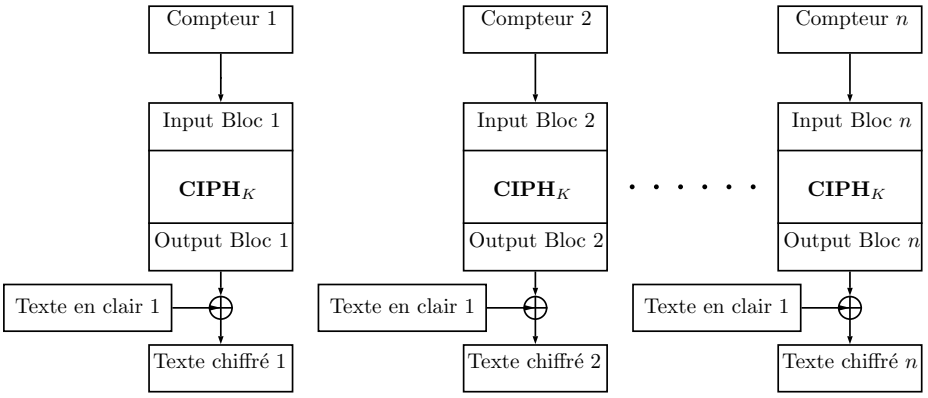
FIGURE 2.10 – Mode OFB

déré comme un moyen de générer un flux pseudo-aléatoire à partir d'un algorithme de chiffrement par bloc.

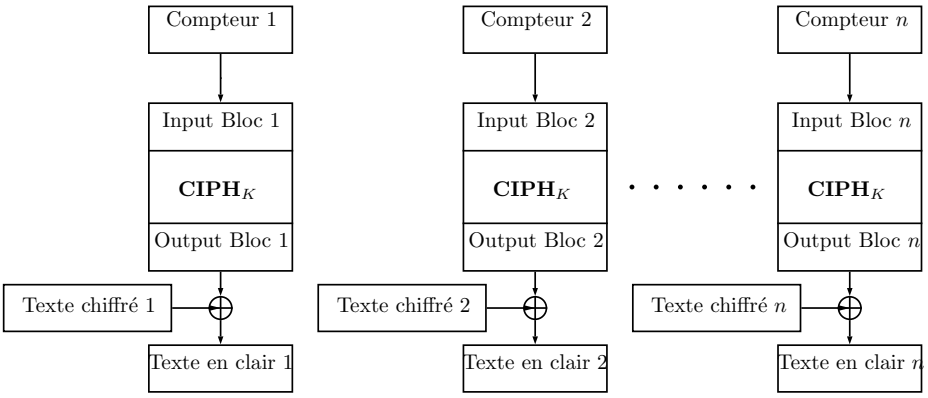
Dans le cryptage CTR, la fonction de chiffrement avant est invoquée sur chaque bloc du compteur, l'opérateur binaire XOR est appliqué entre les blocs de sortie résultants et les blocs de texte en clair correspondants pour produire les blocs de texte chiffré. Le mode OFB est illustré sur la figure 2.11, et l'algorithme de cryptage 6.

Algorithm 6 Cryptage CTR

1: **input :** texte en claire : P, clé secrète : K, vecteur initial : $T[1 \dots n]$;
2: **output :** texte chiffré : C
3: **for** i = 1 **to** n-1 **do**
4: $\quad O_i \leftarrow \text{CIPH}_K(T_i)$
5: $\quad C_i \leftarrow P_i \oplus O_i$
6: $O_n \leftarrow \text{CIPH}_K(T_n)$
7: $C_n \leftarrow P_n \oplus \text{MSB}_u(O_i)$
8: **return** C



(a) Cryptage en mode CTR



(a) Déryptage en mode CTR

FIGURE 2.11 – Mode CTR

2.8 Cryptographie symétrique vs. asymétrique

Menezes et al.[55] ont déduit dans leur ouvrage 'Handbook of applied cryptography' que les schémas de chiffrement à clé symétrique et à clé publique ont divers avantages et inconvénients, dont certains sont communs aux deux. Cette section souligne une traduction du contenu de leur section.

2.8.1 Avantages de la cryptographie symétrique

1. Les algorithmes de chiffrements symétriques peuvent être conçus pour avoir des taux élevés de débit de chiffrement de données. Certaines implémentations matérielles atteignent des taux de plusieurs centaines de méga-octets par seconde, alors que les implémentations logicielles peuvent atteindre des débits des méga-octets par seconde.

2. Les clés dans les cryptosystèmes symétriques sont relativement de petite taille.

3. Les algorithmes de chiffrement à clé symétrique peuvent être utilisés comme des primitives pour construire divers mécanismes cryptographiques, y compris les générateurs de nombres pseudo-aléatoires, les fonctions de hachage, et des schémas de signature numérique.

4. Les chiffres à clé symétrique peuvent être composés pour produire des chiffres plus forts. Ils sont basés sur des transformations simples qui sont faciles à analyser, mais sur leur propre faiblesse, peuvent être utilisés pour construire des chiffres forts.

5. Le cryptage à clé symétrique est perçue comme ayant une longue histoire, mais il faut reconnaître que malgré l'invention de machines à rotor, une grande partie de la connaissance dans ce domaine a été acquise à la suite de l'invention de l'ordinateur numérique, et en particulier, la conception du Data Encryption Standard au début des années 1970.

2.8.2 Inconvénients de la cryptographie symétrique

1. Dans une communication entre deux entités, la clé doit rester secrète aux deux extrémités.

2. Dans un grand réseau, il y a beaucoup de paires de clés à gérer. Par conséquent, une gestion efficace des clés nécessite l'utilisation d'une autorité de confiance.

3. Dans une communication à deux parties entre deux entités A et B, la pratique cryptographique dicte que la clé doit être changée fréquemment, et peut-être pour chaque session de communication.

4. Les mécanismes de signature numérique provenant du cryptage à clé symétrique nécessitent généralement soit de grandes clés pour la fonction de vérification ou l'utilisation d'une autorité de confiance.

2.8.3 Avantages de la cryptographie asymétrique

1. Seule la clé privée doit être gardée secrète.

2. L'administration de clés sur un réseau nécessite la présence d'une autorité de confiance (TTP) seulement d'une manière "off-line".

3. Selon le mode d'utilisation, une paire de clé peut rester inchangée pour des périodes de temps considérables, par exemple, de nombreuses sessions (voire plusieurs années).

4. Beaucoup de systèmes à clé public fournissent des mécanismes de signature numérique relativement efficaces. La taille des clés utilisées pour décrire la fonction de vérification publique est généralement beaucoup plus petite que celle avec clé symétrique.

5. Dans un grand réseau, le nombre de clés nécessaires pourrait être considérablement plus petit que dans le scénario de clé symétrique.

2.8.4 Inconvénients de la cryptographie asymétrique

1. Les débits pour les méthodes les plus populaires de chiffrement à clé publique sont plus lents que les schémas à clés symétriques les plus connus.

2. Les tailles de clé sont généralement beaucoup plus grandes que celles requises pour le chiffrement à clé symétrique, et la taille des signatures à clé publique est plus grande que celle des étiquettes fournissant l'authentification de l'origine des données à partir des techniques symétriques.

3. Aucun système à clé publique n'a été prouvé pour être sûr (la même chose peut être dite pour le chiffrement par blocs). La sécurité des systèmes de chiffrement à clé publique les plus efficaces à ce jour repose sur la difficulté supposée d'un petit ensemble de problèmes numériques théoriques.

4. La cryptographie à clé publique n'a pas un aussi vaste historique que le cryptage à clé symétrique, puisque elle a été découverte seulement dans le milieu des années 1970.

2.9 Conclusion

Dans ce chapitre, nous avons fourni un aperçu des différentes techniques de la cryptographie. Nous avons concentré également sur le chiffrement symétrique et ses différentes classifications et les modes de cryptage.

Dans le prochain chapitre, nous allons voir les notions de base sur les images numériques.

Chapitre 3

Les techniques de cryptage d'images

3.1 Introduction

De nos jours, l'échange de l'information à travers l'Internet est devenu un élément essentiel dans la société moderne, en particulier avec l'énorme croissance des réseaux et des technologies de communication, et surtout avec l'utilisation intensive et la généralisation des Smartphones. Un énorme type d'information qui est généralement impliqué dans les communications modernes est les images numériques qui sont utilisées dans plusieurs domaines sensibles tels que le commerce électronique, les affaires militaires et les dossiers médicaux. Afin de protéger les informations sensibles contre tout accès non autorisé, lors de leur sauvegarde et leur transmission à travers un réseau non sûr, l'utilisation du chiffrement reste une solution primordiale.

Cependant, il est devenu clair que nous ne pouvons pas utiliser les méthodes de chiffrement classiques conçues pour les données textuelles comme RSA [2], DES [3], AES [4] pour le chiffrement des images puisque les images numériques sont caractérisées par la redondance élevée, la forte corrélation et la taille volumineuse. Par conséquent, un intérêt spécial est nécessaire lors du chiffrement de ces données. Selon Shannon [5] : la confusion (substitution) et la diffusion (permutation) sont les deux principales méthodes pour éliminer les redondances élevées et la forte corrélation. La confusion crée une forte relation entre la clé et le texte chiffré. D'un autre côté, la diffusion réduit la redondance du texte en clair en la propagation sur la totalité texte chiffré.

3.2 Notions de base sur l'imagerie

3.2.1 L'image numérique

Une image peut être définie comme une fonction bidimensionnelle $f(x, y)$, ou x et y sont les coordonnées spatiales et l'amplitude f associée aux coordonnées x et y représente l'intensité ou le niveau de gris à ce point là. En réalité, f est continue sur x et y mais en pratique cette dernière a une valeur discrète dans une image numérique [56].

3.2.2 Pixel

"Contraction de l'anglais de pix (pour picture) et element ; la plus petite composante d'une image numérique affichée en mode point sur un écran ou un capteur

(pixel). Le nombre de pixels par ligne et le nombre de lignes par image déterminent la définition de l'image. A chaque pixel est associée une couleur, décomposé en trois composantes primaires (rouge, vert et bleu). Pour l'informatique, un point est codé sur plusieurs bits ; ainsi un point noir et blanc prend un bit, 16 couleurs : 4 bits, 256 couleurs : 1 octet ou 8 bits, 65 536 couleur : 2 octets et 16 777 216 couleurs : 3 octets." [57]

3.2.3 Définition

La définition ou la dimension d'une image est le nombre total de ces pixels.

3.2.4 Résolution

La résolution est le nombre de pixels par unité de longueur dans cette image. Plus la résolution est élevée (plus le pas de discrétisation est faible), mieux les détails seront représentés.

3.3 Les différents types d'image

Les images peuvent être classifiées en trois catégories selon leurs couleurs :

3.3.1 Images binaires

Les images binaires sont des images dont les pixels peuvent avoir seulement deux valeurs d'intensité. Ils sont affichés en noir et blanc. Numériquement, les deux valeurs sont souvent 0 pour le noir, et soit 1 ou 255 pour le blanc. Une image binaire est souvent produite par le seuillage d'une image, de niveaux de gris ou de couleur, afin de séparer un objet dans l'image de l'arrière-plan. La figure 3.1 présente une image binarisée.

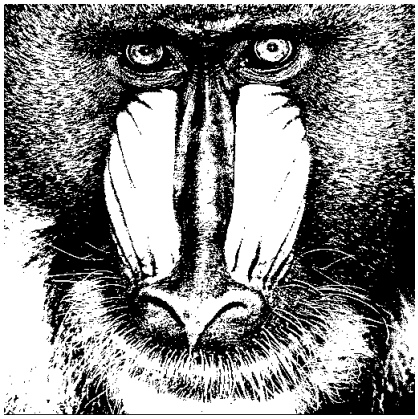


FIGURE 3.1 – Image codée en binaire.

3.3.2 Images couleurs

Il est presque possible de construire toutes les couleurs visibles en combinant les trois couleurs primaires : le rouge, le vert et le bleu, parce que l'oeil humain possède seulement trois récepteurs différents de couleurs ; chacun d'entre eux sensible à une des trois couleurs. Différentes combinaisons de la stimulation des récepteurs permettent à l'oeil humain de distinguer environ 350 000 couleurs [58].

Une image couleur est une image multi-spectrale avec une bande pour chaque couleur, produisant ainsi une combinaison des trois couleurs primaires pour chaque pixel. Une image couleur codée sur 24 bits, une valeur codée sur 8 bits pour chaque couleur : le rouge de 0 à 255 , le vert de 0 à 255, le Bleu de 0 à 255(Voir la figure 3.2), étant ainsi capable d'afficher 2^{24} = 16 777 216 couleurs différentes.

Toutefois, utiliser une image codée sur 24 bits pour stocker la couleur de chaque pixel est coûteux et souvent pas nécessaire dans certaines applications. Par conséquent, la couleur de chaque pixel est souvent codée dans un seul octet, résultant en une image couleur codée sur 8 bits. Le processus de réduction de la représentation de couleur de 24 bits à 8 bits est connus comme la quantification des couleurs [59, 60, 61].

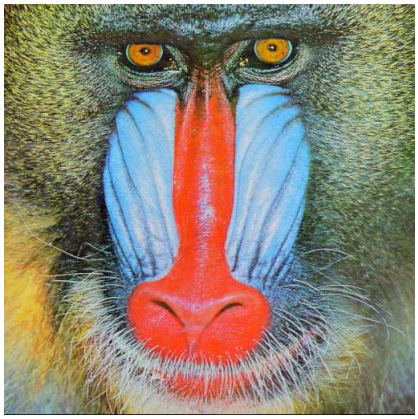


FIGURE 3.2 – Image codée en couleurs 24 bits.

3.3.3 Images au niveau de gris

Une image en niveaux de gris a des couleurs qui sont des nuances de gris. La raison pour différencier ces images de toute autre sorte d'image couleur est que moins d'informations doivent être fournies pour chaque pixel. En fait, une couleur grise est celle dans laquelle les composantes rouge, vert et bleu ont tous une intensité égale dans l'espace RVB, et il est donc seulement nécessaire de spécifier une seule valeur d'intensité pour chaque pixel, par opposition, trois intensités sont nécessaires pour spécifier chaque pixel dans une image couleur.

Souvent, l'intensité au niveau de gris est stockée comme un entier de 8 bits produisant 256 nuances de gris du noir au blanc. La figure 3.3 illustre l'image Baboon codée au niveaux de gris.

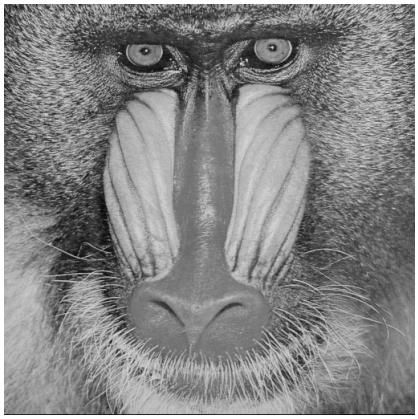


FIGURE 3.3 – L'image Baboon au niveau de gris.

3.4 Les espaces de couleur

La modélisation de la couleur en informatique s'appuie sur la théorie de Maxwell. Un espace de couleurs est une représentation mathématique d'un ensemble de couleurs. Les trois modèles de couleurs les plus populaires sont RGB (utilisé en infographie) ; YIQ, YUV ou YCbCr (utilisé dans les systèmes de vidéo) ; et CMJN (utilisé dans l'impression couleur). Cependant, aucun de ces espaces de couleurs n'est directement lié à des notions intuitives de la teinte, la saturation et la luminosité. Cela a abouti à la poursuite temporaire des autres modèles, notamment HSI et HSV, pour simplifier la programmation, le traitement et la manipulation finale des images numériques [62].

Tous les espaces de couleurs peuvent être tirés de l'information RVB fourni par des dispositifs tels que des appareils photo et des scanners.

3.4.1 L'espace RVB : " Rouge Vert Bleu "

Le rouge, vert et bleu (RGB en anglais) est un espace de couleur largement utilisé pour l'infographie. Le rouge, le vert et le bleu sont les trois couleurs primaires additives (composants individuels additionnés pour former une couleur souhaitée(voir la figure 3.4)) et sont représentés par un cube tridimensionnel tel que le rouge, vert et bleu se situent dans les coins de chaque axe, le noir à l'origine et le blanc à l'opposé. L'échelle du niveau de gris suit la ligne du noir au blanc, dans un système graphique de 24 bits avec 8 bits pour chaque canal, le rouge est (255, 0, 0) tandis que dans le cube de couleur

est (1, 0, 0) (voir le figure 3.5).

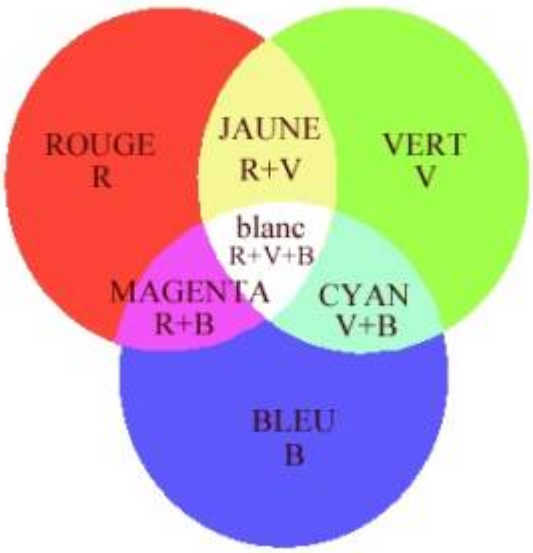


FIGURE 3.4 – Espace additif [1]

L'espace de couleur RVB est le choix le plus répandu pour les graphiques informatiques, car les écrans en couleur utilisent le rouge, vert et bleu pour créer la couleur désirée. Par conséquent, le choix de l'espace de couleur RGB simplifie l'architecture et la conception du système. En outre, un système qui est conçu en utilisant l'espace de couleur RVB peut profiter d'un grand nombre de routines logicielles existantes, puisque cet espace de couleur existe depuis un certain nombre d'années.

Cependant, les composantes rouge, vert et bleu d'une couleur sont fortement corrélées et le principal inconvénient de cet espace de couleur vient du fait qu'il ne tient pas compte de la variation de la sensibilité de l'oeil.

3.4.2 L'espace TSL

Le TSL (Teinte, Saturation, Luminosité) est un modèle de couleur qui définit un espace de couleur en fonction de trois éléments constitutifs (voir la figure 3.6) :

- **La teinte** : le type de couleur (comme le rouge, bleu ou jaune). Varie de 0 à 360 ° dans la plupart des applications. (Chaque valeur correspond à une couleur : 0 est rouge, 45 est une nuance d'orange et 55 est une nuance de jaune).

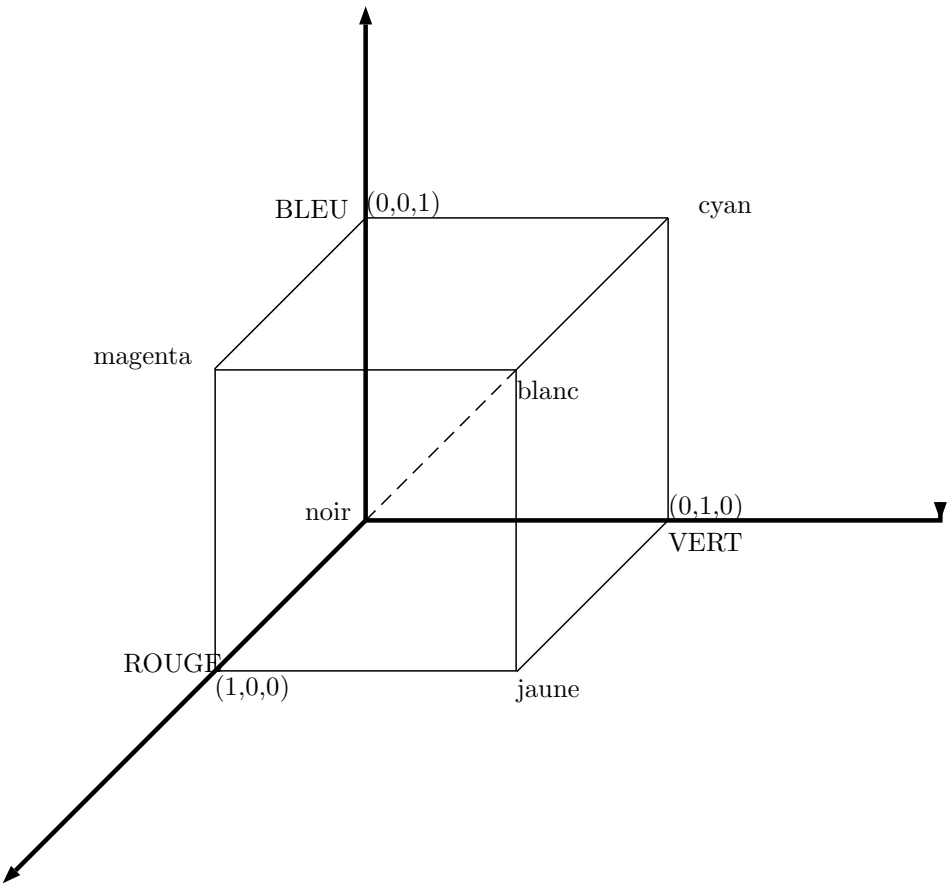


FIGURE 3.5 – Le cube tridimensionnel représentant l'espace de couleur RGB

- **Saturation** : l'intensité de la couleur. Varie de 0 à 100% (0 signifie pas de couleur, qui est une nuance de gris entre le noir et le blanc ; 100 % signifie une couleur intense).
- **Luminosité (ou la valeur)** : la luminosité de la couleur est comprise entre 0 et 100% (0 est toujours noir ; en fonction de la saturation, 100% peut être blanc ou une couleur plus ou moins saturée).

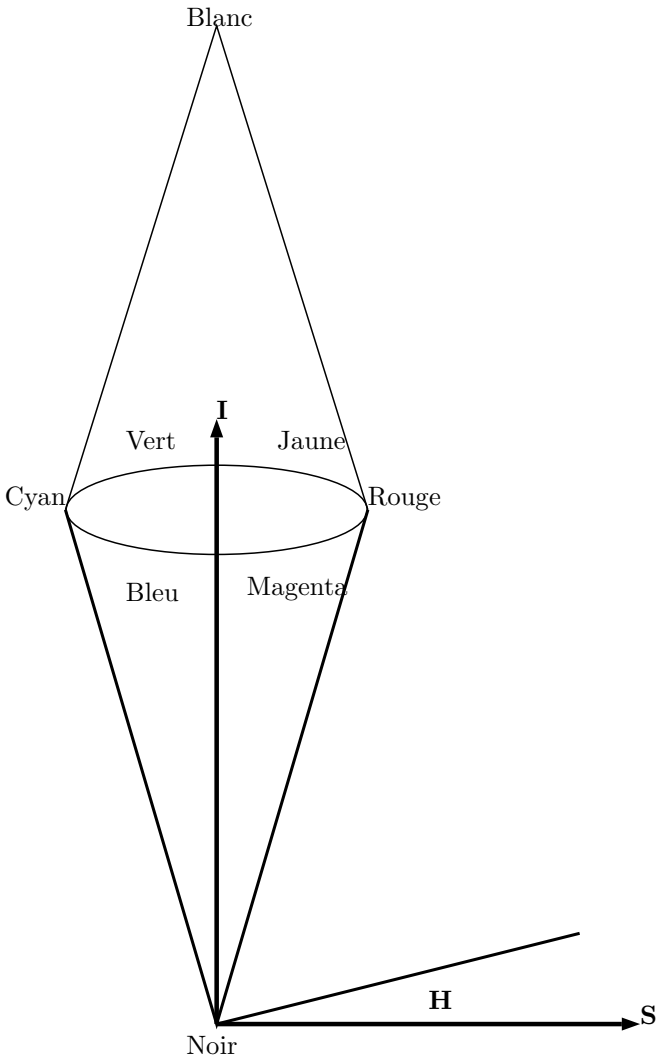


FIGURE 3.6 – Représentation de l'espace HSV

Le modèle TSL est également connu comme le HSV (Teinte, Saturation, Valeur) modèle. Le modèle HSV a été créé en 1978 par Alvy Ray Smith [63]. Il représente une transformation non linéaire de l'espace de couleur RGB. En d'autres termes, la couleur ne se définit pas comme une simple combinaison (addition / soustraction) de couleurs primaires mais comme une transformation mathématique.

L'espace HSV n'est pas, malheureusement, uniforme c'est-à-dire une distance entre deux couleurs visuellement proches peut être très grande, d'où la création de l'espace Lab afin de résoudre cette difficulté.

3.4.3 L'espace Lab

Il caractérise une couleur à l'aide d'un paramètre d'intensité correspondant à la luminance et de deux paramètres de chrominance qui décrivent la couleur [64, 65].

- Lightness : correspond à la lumière. (0 rendements noir et 100 indique Blanc).
- A et B : représentent la couleur. le paramètre a entre le magenta et vert (les valeurs négatives indiquent verte tandis que les valeurs positives indiquent magenta) et le b indique la position entre le jaune et le bleu (les valeurs négatives indiquent bleu et les valeurs positives indiquent jaune).

3.5 Formats d'enregistrement d'une image

Les formats d'enregistrement d'images numériques sont généralement décomposés en deux catégories de base : des images matricielles et des images vectorielles. Une image matricielle ou encore appelée image bitmap, se représente sous forme d'une matrice de points, ces points codés sont rangés en lignes et en colonnes. Tandis qu'une image vectorielle est décrite en termes de formes élémentaires : (lignes, cercles, rectangles,...). Ces formes sont décrites par des attributs géométriques et par des attributs d'épaisseur, de couleur, de genre, ...

Les formats des images les plus courants et les plus importants pour les caméras, l'impression et l'Internet, sont JPG, TIF, PNG et GIF

3.5.1 JPEG

JPEG (Joint Photographic Experts Group) est une méthode de compression avec perte ; Les images JPEG compressées sont généralement stockées dans le format de fichier JFIF (JPEG Interchange File Format). Il est le format de fichier d'image le plus utilisé. Les appareils photo numériques et les pages Web utilisent des fichiers JPG. Cependant JPEG utilise la compression avec perte, qui peut conduire à une réduction significative de la taille du fichier. Cependant, la compression affecte la qualité visuelle du résultat ce qui est un inconvénient majeur pour les images de grandes tailles. JPEG fournit également le stockage d'image sans perte, mais la version sans perte n'est pas largement prise en charge[66, 67].

L'extension du fichier JPEG / JFIF est JPG ou JPEG. Presque chaque appareil photo numérique peut enregistrer des images au format JPEG / JFIF, qui code sur huit bits des images au niveau de gris et sur 24 bits les images couleurs (huit bits chaque plan) [67].

3.5.2 TIFF

Le format TIFF (Tagged Image File Format) est un format flexible qui enregistre normalement huit bits ou seize bits par couleur (rouge, vert, bleu) des totaux 24-bits et 48-bits, respectivement, en utilisant généralement soit TIFF ou TIF comme nom de l'extension. La structure a été conçue pour être facilement extensible, et de nombreux fournisseurs ont introduit des balises propriétaires à usage spécial de fichier TIFF.

Le format TIFF peut être avec ou sans perte, certains offrent relativement une bonne compression sans perte d'images. Certains appareils photo numériques peuvent enregistrer des images au format TIFF, en utilisant l'algorithme de compression LZW pour le stockage sans perte. Et TIF est le plus polyvalent, sauf que les pages Web ne supportent pas les fichiers TIFF[66, 67].

3.5.3 GIF

GIF (Graphics Interchange Format) a été inventé par CompuServe dans les premiers jours de l'ordinateur 8 bits vidéo, avant JPG, pour l'affichage vidéo. Le format GIF est conçu pour l'usage courant, limité à une palette 8-bit, ou 256 couleurs, GIF peut avoir une palette de couleurs 24 bits, mais seulement 256 d'entre eux au maximum (les couleurs qui dépendent de couleurs de l'image).

Le format GIF est le plus approprié pour le stockage de graphiques avec peu de couleurs comme les diagrammes simples, les formes et les logos car il utilise la compression sans perte LZW qui est plus efficace lorsque de grands espaces ont une couleur unique, et moins efficace pour les images photographiques ou les images tramées. Grâce à ses capacités d'animation inclus, il est encore largement utilisé pour fournir des effets d'animation [66, 67].

3.5.4 PNG

Le format de fichier PNG (Portable Network Graphics) a été créé comme alternative open-source au format GIF. Le format PNG prend en charge les images avec une palette de huit bits (avec la transparence en option pour toutes les couleurs de la palette) et 24-bit TrueColor (16 millions de couleurs) ou 48-bit TrueColor, alors que le GIF prend en charge 256 couleurs uniquement et une seule couleur transparente. PNG est conçu pour fonctionner dans des applications de visualisation en ligne comme les navigateurs Web et peut être entièrement diffusée avec une option progressive d'affichage. PNG est robuste, fournissant à la fois l'intégrité des fichiers de vérification et une simple détection des erreurs de transmissions [66, 67].

LesFormats animés provenant de PNG sont MNG et APNG. Ce dernier est supporté par Mozilla Firefox et Opera et est rétro-compatible avec PNG [67].

3.6 Méthodes de cryptage d'images

Il existe deux grandes différences entre les données textuelles et les images numériques rendant les méthodes de cryptage de texte pour la plupart des cas inapplicable au cryptage des images. La principale différence réside dans la taille, en effet la quantité d'informations contenues dans l'image est beaucoup plus volumineuse que celles contenues dans les données textuelles. La seconde différence concerne la perte de données, lorsqu'une technique de compression est appliquée. Contrairement aux images, l'utilisation d'une méthode de compression avec perte est totalement interdite lors du chiffrement d'un texte, par conséquent, les chercheurs ont étudié plusieurs méthodes de chiffrement d'image avec/sans perte. D'autre part, les algorithmes de chiffrement des images peuvent être classés selon le domaine d'application : les méthodes du domaine spatial ou bien celle du domaine fréquentiel.

3.6.1 Méthodes dans le domaine spatial

Dans le domaine spatial, on applique le schéma de cryptage sur le plan d'image lui-même, et les approches de cette catégorie sont basées sur une manipulation directe des pixels d'une image. Dans ces algorithmes, le chiffrement détruit la corrélation entre les pixels et rend les images cryptées incompressibles. Les pixels de l'image peuvent être reconstruits (récupérés) complètement par un processus inverse sans aucune perte d'information.

Les algorithmes de cryptage d'image dans le domaine spatial existants peuvent être classés en deux catégories. Dans la première catégorie, un pixel est considéré comme le plus petit élément, et une image numérique est considérée comme un ensemble de pixels. Toutefois, dans la deuxième classe, un pixel peut être en outre divisé en bits, sur lesquels des opérations au niveau de bits sont effectuées. Par exemple, un pixel dans une image en niveaux de gris est généralement constitué de 8 bits.

3.6.2 Méthode dans le domaine fréquentiel

Les schémas de cryptage dans le domaine fréquentiel sont basés sur la modification de la fréquence de l'image en utilisant une transformation, ainsi, la reconstruction des pixels de l'image originale dans le processus de décryptage cause généralement une perte d'information.

3.7 Outils élémentaires d'analyse d'un algorithme de cryptage d'image

3.7.1 Espace de clés

La taille de l'espace de clé est le nombre de paires de clés de cryptage/décryptage qui sont disponibles dans le système de chiffrement [55]. Une condition nécessaire, mais pas suffisante à un schéma de cryptage pour qu'il soit sûr est que l'espace clés soit suffisamment grand pour assurer la sécurité contre l'attaque par force brute.

3.7.2 Analyse statistique

L'histogramme

Dans un contexte de traitement d'image, l'histogramme d'une image désigne un histogramme des valeurs d'intensité des pixels. Cet histogramme est un graphique illustrant le nombre de pixels dans une image à chaque valeur d'intensité trouvée dans cette image. Pour une image grise il y a 256 intensités différentes possibles, ainsi, l'histogramme s'affiche graphiquement en utilisant 256 chiffres indiquant la distribution des pixels entre ces valeurs de niveaux de gris [68].

Les histogrammes peuvent également être pris d'images en couleur ; soit des histogrammes individuels des canaux rouge, vert et bleu, ou un seul histogramme 3-D avec les trois axes représentant les trois plans, et la luminosité dans chaque point représente le nombre de pixels. En conséquence, l'histogramme d'une image ne représente pas la répartition spatiale ; ainsi, deux images différentes peuvent disposer le même histogramme [69].

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

La corrélation

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

$$r = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{3.1}$$

Où :

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{3.2}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, D(x) = \sum_{i=1}^{N}(x_i - E(x))^2 \tag{3.3}$$

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

L'entropie

Selon la théorie de Shannon [43], l'entropie d'une information est la quantité d'information englobée ou libérée par une source d'information. En particulier, plus la source est redondante, moins elle contient d'information [70]. En absence de contraintes particulières, l'entropie est maximale pour une source dont tous les symboles sont équiprobables. Ainsi, elle est l'une des principales mesures de l'aléatoire de l'information. Les valeurs de l'entropie élevée manifestent un haut degré de caractère aléatoire ; et pour tout message codé sur M bits, la limite supérieure de l'entropie est M. La formule utilisée pour calculer l'entropie d'une source m est comme suit :

$$H(M) = \sum_{i=0}^{2^n-1} p(m_i) \log_2(\frac{1}{p(m_i)}) \tag{3.4}$$

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

3.7.3 Analyse de sensitivité

Attaques différentiels

Afin de détecter la relation entre l'image originale et l'image cryptée, un adversaire fait un petit changement sur l'image claire, ensuite utilise l'algorithme de cryptage pour crypter l'image avant et après le changement, dans le but de tester comment une petite modification dans l'image originale affecte l'image cryptée. Ce genre d'attaque est appelé attaque différentiel.

Pour assurer la sécurité d'un schéma de cryptage d'image contre l'analyse différentielle, deux mesures quantitatives sont utilisés : le NPCR (Number of Pixels Change Rate) et l'UACI (Unified Average Changing Intensity).

Le NPCR représente le taux de pixels différents entre les deux images chiffrées, tandis que l'UACI représente la différence de l'intensité moyenne. La formule utilisée pour calculer ces deux pourcentages est définie comme suit :

$$\text{NPCR} = \frac{\sum_{i,j} f(i,j)}{W \times H} \times 100\% \tag{3.5}$$

$$\text{UACI} = \frac{1}{H \times W}\left[\sum_{i,j}\frac{\left|C_1(i,j) - C_2(i,j)\right|}{255}\right] \times 100\% \tag{3.6}$$

Où W et H représentent la largeur et la hauteur de l'image respectivement. $C_1(i,j)$ est l'image cryptée et $C_2(i,j)$ est l'image cryptée après avoir changé un pixel de l'image clair. Pour les pixels à la position (i,j), si $C_1(i,j) \neq C_2(i,j)$, alors $f(i,j) = 1$; sinon $f(i,j) = 0$.

Un NPCR > 99,6094% et un UACI > 33,4635% assure qu'un schéma de chiffrement d'image est sécurisé contre cette attaque [71].

Sensitivité de la clé

Un algorithme idéal de chiffrement d'image doit être sensible à la clé. C'est à dire le changement d'un seul bit dans la clé secrète devrait produire une image cryptée complètement différente. Pour tester la sensibilité de la clé de chiffrement, nous avons effectué les étapes suivantes [72] :

- Une image originale est chiffrée en utilisant la clé secrète.
- La même image originale est cryptée en faisant une légère modification dans la clé secrète.
- Ensuite, on compare les deux images chiffrées en utilisant les deux mesures NPCR et UACI.
- Ainsi, si les valeurs de l'NPCR et l'UACI obtenues sont supérieurs à 99,6094% et à 33,4635% respectivement : on dit que le schéma est sensible à la clé.

3.7.4 Propriétés aléatoires de l'image cryptée

Un bon algorithme de chiffrement doit avoir d'excellentes propriétés aléatoires. Pour atteindre ces propriétés, les images chiffrées produites à partir des images en clairs doivent avoir une distribution statistique impossible à la distinguer d'une séquence aléatoire.

Deux tests sont utilisés pour tester les propriétés aléatoires des images cryptées : la suite de tests NIST SP 800-22 et la suite de tests Diehard.

Suite de tests NIST SP 800-22

La Suite de tests NIST SP 800-22 [73] est un progiciel statistique constitué de 16 tests qui ont été développés à l'Institut national des normes et de la technologie (the National Institute of Standards and Technology) par les employés du gouvernement fédéral dans le cadre de leurs fonctions officielles, pour tester le caractère aléatoire des séquences binaires (arbitrairement longue), produites soit par un logiciel, soit par un matériel, ces derniers représentent des générateurs de nombres cryptographiques aléatoires ou pseudo-aléatoire. Ces tests se concentrent sur une variété de différents types de non-aléatoire qui pourraient exister dans une séquence. Voici la description des tests [74] :

Frequency (Monobit) Test Le focus du test est la proportion de zéros et de uns dans la totalité de la séquence. Le but de ce test est de déterminer si le nombre de uns et de zéros dans une séquence sont à peu près les mêmes que l'on pouvait s'y attendre pour une séquence réellement aléatoire.

Frequency Test within a Block Le focus du test est la proportion des uns au sein de blocs de M bits. Le but de ce test est de déterminer si la fréquence des uns dans un bloc de M bits est d'environ $M/2$.

Runs Test Le focus de ce test est le nombre total de runs dans la séquence ; où un run est une suite ininterrompue de bits identiques. Un run de longueur k consiste exactement à k bits identiques et est bornée avant et après avec un bit opposée. Le but du test des runs consiste à déterminer si le nombre de runs de uns et de zéros de différentes longueurs est aussi comme on l'a prévu pour une suite aléatoire. En particulier, ce test détermine si l'oscillation entre les zéros et les uns est trop rapide ou trop lent.

Test for the Longest Run of Ones in a Block Le focus du test est la plus longue série de uns au sein des blocs de M bits. Le but de ce test est de déterminer si la longueur de la plus longue série de uns dans la séquence testée est compatible avec la longueur de la plus longue série de uns attendu dans une suite aléatoire. Notez que l'irrégularité dans la longueur prévue de la plus longue série de uns implique qu'il ya aussi une irrégularité dans la longueur prévue de la plus longue série de zéros. Par conséquent, seulement un test pour les uns est nécessaire.

Binary Matrix Rank Test Le focus du test est le rang de sous-matrices disjointes de la séquence entière. Le but de ce test est de vérifier la dépendance linéaire entre les chaînes de longueur fixe de la séquence originale.

Discrete Fourier Transform (Spectral) Test Le focus de ce test est la hauteur des pics dans la transformée de Fourier discrète de la séquence. Le but de ce test est de détecter les caractéristiques périodiques dans la séquence éprouvée qui indiquerait un écart par rapport à l'hypothèse du hasard. Le but est de détecter si le nombre de pics qui dépassent le seuil de 95% est significativement différent de 5%.

Non-overlapping Template Matching Test Le focus de ce test est le nombre d'occurrences d'une chaîne pré-spécifiée. Le but de ce test est de détecter les générateurs qui produisent trop d'occurrences d'un modèle non périodique donné.

Overlapping Template Matching Test Le focus de ce test est le nombre d'occurrences de chaînes pré-spécifié. Comme pour le test précédent, si le modèle est introuvable, la fenêtre glisse une position binaire. La différence entre ce test et le test précédent est que lorsque le modèle est trouvé, la fenêtre glisse un seul bit avant de reprendre la recherche.

Maurer's "Universal Statistical" Test Le focus de ce test est le nombre de bits entre les modes assortis (une mesure qui est liée à la longueur d'une séquence compressée). Le but du test est de détecter si la séquence peut être compressée d'une façon significative sans perte d'information. Une séquence significativement compressible est considérée comme étant non aléatoire.

Lempel-Ziv Compression Test Le focus de ce test est le nombre de modèles cumulativement distincts (mots) dans la séquence. Le but du test vise à déterminer à quelle distance la séquence testée peut être compressée. La séquence est considérée comme étant non aléatoire si elle peut être compressée d'une manière significative. Une séquence aléatoire aura un nombre caractéristique de modèles distincts.

Linear Complexity Test Le focus de ce test est la longueur d'un registre à décalage linéaire (LFSR). Le but de ce test vise à déterminer si la séquence est suffisamment

complexe pour être considérée comme aléatoire. Les séquences aléatoires sont caractérisées par des LFSRs plus longues. Un LFSR trop court implique le non aléatoire.

Serial Test Le focus de ce test est la fréquence de tous les m-bits modèles de chevauchement possibles à travers toute la séquence. Le but de ce test est de déterminer si le nombre d'occurrences des 2m m-bits modèles en chevauchement est approximativement le même qu'on peut s'y attendre pour une séquence aléatoire. Les séquences aléatoires ont l'uniformité ; chaque m-bits modèle a la même chance d'apparaître comme tout autre m-bits modèle. Notez que pour m = 1, le test de série est équivalent au test de fréquence de la section 3.7.4.

Approximate Entropy Test Comme avec le test de série de la section 3.7.4, le focus de ce test est la fréquence de tous les m-bits modèles de chevauchement possibles dans toute la séquence. Le but du test est de comparer la fréquence des blocs de chevauchement de deux longueurs consécutives/adjacentes (M et M + 1) avec le résultat attendu pour une séquence aléatoire.

Cumulative Sums (Cusum) Test Le focus de ce test est l'excursion maximale (allant de zéro) du cheminement aléatoire défini par la somme cumulée des chiffres ajustés (-1, +1) dans la séquence. Le but du test est de déterminer si la somme cumulée des séquences partielles qui se produisent dans la séquence testée est trop large ou trop petite par rapport au comportement attendu de cette somme cumulative de séquences aléatoires. Cette somme cumulative peut être considérée comme une marche aléatoire. Pour une séquence aléatoire, les excursions de la marche aléatoire devraient être proches de zéro. Pour certains types de séquences non aléatoires, les excursions de cette marche aléatoire à partir de zéro seront larges.

Random Excursions Test L'objectif de ce test est le nombre de cycles ayant exactement K visites dans une somme cumulative marche aléatoire. La somme cumulative marche aléatoire est dérivée à partir des sommes partielles après que la séquence (0,1) est transférée à une séquence (-1, 1) appropriée. Un cycle d'une marche aléatoire consiste en une séquence d'étapes de longueur unitaire prises au hasard qui commencent et revenir (qui reviennent) à l'origine.

Ce test vise à déterminer si le nombre de visites à un état particulier dans un cycle écarte est ce que l'on attendrait d'une séquence aléatoire. Ce test est en fait une série

de huit essais (et conclusions), un test et une conclusion pour chacun des états : -4, -3, -2, -1 et 1, 2, 3, 4.

Random Excursions Variant Test Le focus de ce test est le nombre total de fois où un état particulier est visité dans une somme cumulative marche aléatoire. Le but de ce test est de détecter les écarts par rapport au nombre attendu de visites aux différents états de la marche aléatoire. Ce test est en réalité une série de dix-huit tests (et conclusions), un test et une conclusion pour chacun des Etats : -9, -8, ..., -1 et +1, +2, ..., 9.

Suite de tests Diehard

La suite de tests Diehard est une batterie de tests statistiques pour mesurer la qualité d'un générateur de nombres aléatoires [75, 76, 77]. Elle a été développée par George Marsaglia au fil de plusieurs années et premièrement publiée en 1995 sur un CD-ROM.

La plupart des tests dans DIEHARD retournent une p-valeur, qui doit être uniforme sur l'intervalle [0,1] si le fichier d'entrée contient des bits aléatoires véritablement indépendants. Les valeurs p sont obtenues par $p = F(X)$, où F est la distribution hypothétique de l'échantillon aléatoire variable X. Quand un flux de bits ECHOUE vraiment le résultat du test serai une valeur P égal à 0 ou 1 à six ou plusieurs endroits. On ne doit pas penser qu'une valeur P <0.025 ou P > 0,975 signifie que notre suite a échoué le test au niveau 0.5. Cette valeur de P puisse se produire parmi des centaines de valeurs produites par la suite de test DIEHARD.

La suite est constituée de 15 tests, leurs descriptions est comme suit :

Birthday spacings Choisir m anniversaires dans une année de n jours, listant les espacements entre les anniversaires. Déterminer ensuite une ligne du meilleur ajustement et déterminer l'écart de la fonction de distribution prévu. Cet écart détermine la qualité de ce test.

Overlapping permutations Analyser des séquences de cinq nombres aléatoires consécutifs. Les 120 ordres possibles devraient se produire avec une probabilité statistiquement égale.

Ranks of matrices Sélectionner un certain nombre de bits de certains nombre de nombres aléatoires pour former une matrice sur 0,1, puis déterminer le rang de la matrice. (Compter les rangs)

Monkey tests Traiter des séquences de certains nombre de bits comme des «mots». Compter les mots en chevauchement dans un flux. Le nombre de «mots» qui ne figurent pas doivent suivre une distribution connue.

Count the 1s Utiliser un échantillon de 256 000, et déterminer combien de fois les mots de 8 lettres et 5 lettres apparaissent et puis calculer la variance. Y'en a deux types de tests : l'un sur un flux d'octets et l'autre sur des octets spécifiques.

Parking lot test Placer Aléatoirement 8.000 points dans un carré de 10.000 × 10.000, puis trouver la distance minimale entre les paires. Le carré de cette distance devrait être distribué de façon exponentielle avec une certaine moyenne.

Random spheres test Choisir au hasard 4 000 points dans un cube de bord 1 000. Centrer une sphère sur chaque point, dont le rayon est la distance minimale vers un autre point. Le volume de la plus petite sphère doit être distribué de façon exponentielle avec une certaine moyenne.

The squeeze test Multiplier 2^{31} par des nombre aléatoires sur (0,1) jusqu'à ce qu'on atteint 1. Répéter ceci 100 000 fois. Le nombre des nombres nécessaires pour atteindre 1 doit suivre une certaine distribution.

Overlapping sums test Générer une longue séquence de flotteurs aléatoires sur (0,1). Ajouter des séquences de 100 flotteurs consécutifs. Les sommes devraient être distribuées normalement avec une caractéristique moyenne et une variance.

Runs test Générer une longue séquence de flotteurs aléatoires sur (0,1). Compter les runs ascendant et descendant. Les chiffres devraient suivre une certaine distribution.

The craps test Jouer 200.000 jeux de craps, en comptant les victoires et le nombre de touche par jeu. Chaque compte doit suivre une certaine distribution.

3.8 Etat de l'art sur les techniques de cryptage d'image

3.8.1 Méthodes basées sur SCAN

Un scanninig (balayage) [78, 6] d'un tableau à deux dimensions est un ordre selon lequel chaque élément de la matrice est accédé seulement une fois. Le SCAN est une méthodologie spatiale qui permet de représenter et de générer un grand nombre de chemins de balayage facilement. Chaque langage SCAN est défini par une grammaire et dispose d'un ensemble de modèles de balayage de base, un ensemble de transformations des modes de balayage, et un ensemble de règles permettant de composer des modèles de balayage simples pour obtenir des modèles de balayage complexes.

Maniccam, and Bourbakis [6] ont proposé une nouvelle méthodologie qui assure à la fois la compression sans perte et le cryptage des images binaires et au niveau de gris, basées sur des modèles SCAN générés par la méthodologie SCAN. La méthode de chiffrement-compression proposée compresse une image binaire donnée, en spécifiant un chemin de balayage de l'image et, en spécifiant la séquence de bits dans une forme codée. Au cœur de la méthode de compression l'algorithme détermine un près optimale ou un bon trajet de balayage qui minimise le nombre total de bits nécessaires pour représenter le trajet de balayage et la séquence codée de bits codés le long de la trajectoire de balayage. Après la compression de l'image binaire, les bits de l'image compressée sont réarrangés pour obtenir l'image compressée-cryptée. Le réarrangement est effectué en utilisant un ensemble de chemins de balayage qui sont gardés secrets, cet ensemble de chemins constitue la clé de chiffrement.

Chen and Chen [79] ont recommandé un schéma de chiffrement d'image basé sur le réarrangement des pixels de l'image, le réarrangement est effectué par le balayage des modèles qui ont généré par la méthode SCAN. Le cryptage ici a besoin d'une méthodologie pour spécifier et générer un plus grand nombre de chemins de balayage efficace.

Maniccam, and Bourbakis [80] ont présenté une nouvelle méthode pour le cryptage d'images et de vidéos. La méthode de cryptage d'image proposé est basée sur une permutation des pixels de l'image et un remplacement des valeurs de pixels. La permutation se fait par des modèles de balayage (clés de chiffrement) générés par la méthodologie SCAN et les valeurs de pixels sont remplacées en utilisant une simple règle de substitution, les opérations de permutation et de substitution dans ce schéma sont appliquées de façon entrelacée et itérative. La méthode de chiffrement proposée est basée sur l'application répétée et entrelacée de permutation et de substitution.

Chen and Horng [7] ont abordé un nouvel algorithme de chiffrement d'image basé sur les patterns SCAN-CA, le chiffrement proposé appartient aux cryptosystèmes de chiffrement par flux. La méthode de cryptage d'image proposée satisfait les propriétés de confusion et diffusion ; la permutation se fait par des modèles de balayage qui sont générés par l'approche SCAN. Les valeurs de pixels sont remplacées en utilisant un automate cellulaire(CA) récursive avec une séquence de données CA qui est générée à partir des règles d'évolution de CA.

3.8.2 Méthodes basées sur la théorie du chaos

Les cartes chaotiques sont des fonctions simples itérées rapidement. Le chaos est un phénomène naturel découvert par Edward Lorenz en 1963 tout en étudiant l'effet papillon dans les systèmes dynamiques. L'effet papillon décrit la sensibilité des conditions initiales comme mentionné dans le document de Lorenz intitulé "Does the Flap of a Butterfly's Wings in Brazil set off a Tornado in Texas ?" [81].

Les battements d'ailes représentent une infime variation dans les conditions initiales du système dynamique qui provoque une chaîne d'événements conduisant à des changements à grande échelle dans l'avenir. Si le papillon ne battit pas ses ailes, la trajectoire du système aurait pu être très différente. En général, cela signifie qu'une petite variation dans les paramètres initiaux pourrait donner des résultats très divergents. Par conséquent, pour un système chaotique, rendant prédiction à long terme est en général impossible. Cela signifie que ; avoir les conditions initiales de ces systèmes rend leur comportement futur prévisible. Ce comportement, qui découle d'un phénomène naturel, est connu comme des expositions de cartes chaotiques. Ces cartes sont classées comme des cartes continues [82] et des cartes discrètes [83].

Une différence importante entre le chaos et la cryptographie repose sur le fait que les systèmes utilisés dans le chaos sont définis sur les nombres réels, tandis que la cryptographie traite des systèmes définis sur des corps fini d'entiers. Néanmoins, les deux disciplines peuvent bénéficier l'une de l'autre. Ainsi, par exemple, de nouveaux algorithmes de cryptage peuvent être dérivés des systèmes chaotiques. D'autre part, la théorie du chaos peut aussi bénéficier de la cryptographie : nouvelles techniques pour l'analyse du chaos peuvent être développées à partir de la cryptographie [84]. On peut citer aussi, la confusion et la diffusion qui sont deux principes généraux dans la conception d'algorithmes de cryptographie qui mènent à la dissimulation de la structure statistique de pixels dans une image simple et à une diminution de la dépendance statistique d'une image simple et une image chiffrée correspondante. L'application d'une propriété de mélange sur des algorithmes de cryptage par chaos va augmenter

la complexité de l'image chiffrée.

Une méthode de cryptage d'image en utilisant une carte chaotique de chat 3D est présenté dans [85]. Ces cartes chaotiques, avec un choix aléatoire de conditions et de paramètres initiaux, sont utilisées pour générer trois séquences chaotiques discrètes avec une sensibilité élevée par les itérations. Deux séquences sont utilisées pour concevoir une permutation à deux dimensions utilisées pour permuter les coordonnées de chaque pixel de l'image. Ensuite, les éléments de la troisième séquence sont tronqués et utilisés pour confondre les valeurs de pixels en utilisant une combinaison OU exclusif et des opérations de décalage cycliques.

Gao and Chen [86] ont suggéré un nouveau schéma de cryptage d'image. Le cryptage proposé ici se compose de deux processus, premièrement, ils mélangent l'image en fonction d'une matrice globale de brassage généré en utilisant la carte logistique, puis ils cryptent l'image mélangée en utilisant l'hyper-chaos.

Chen et al.[87] ont proposé une nouvelle approche pour le chiffrement d'image rapide et sécurisée. Depuis que les images numériques sont généralement représentées comme des tableaux en deux dimensions, afin de de-corréler rapidement les relations entre les pixels, une carte chaotique de dimension supérieure est conçue et ensuite utilisée pour mélanger les positions des pixels de l'image. Pour confondre la relation entre l'image claire et l'image chiffrée, un processus de diffusion, auprès des pixels, est effectué en utilisant le Chat d'Arnold [88].

Mazloom and Eftekhari-Moghadam [89] ont conçus un nouvel algorithme chaotique qui a les propriétés de non-linéarité et une structure couplée. Ils proposent un nouveau cryptosystème, basé sur le chaos, pour le chiffrement d'image couleur fonctionnant comme un algorithme de chiffrement symétrique par flux. Afin d'augmenter la sécurité de l'algorithme proposé, une clé secrète de taille 240 bit est utilisée pour générer les conditions initiales et les paramètres de la carte chaotique en apportant quelques transformations algébriques à la clé. Les transformations algébriques peuvent améliorer la sensibilité du changement d'un bit de la clé. Ces transformations, ainsi que la structure de couplage et la non-linéarité de la carte chaotique CNCM ont amélioré la sécurité du cryptosystème.

Rhouma et al.[90] ont décrit un schéma de cryptage d'image couleur basé sur la carte chaotique OCML(one-way coupled-map lattices). Une clé externe de longueur 192 bits est choisie pour générer les conditions initiales et les paramètres de la carte OCML en appliquant des transformations algébriques afin d'améliorer la sensibilité aux changements d'un bit de la clé. Les trois plans de couleur (rouge, vert et bleu) sont cryptés de façon couplée de telle manière à renforcer la sécurité de cryptosystème.

La recherche présentée dans [10] propose un schéma cryptographique basé sur deux cartes chaotiques robustes. Ils ont utilisé un véritable générateur de nombres aléatoires (TRNG) pour générer les clés en utilisant le haché (MD5) des positions de la souris. Leur principale source d'entropie vient de l'échantillonnage des positions de la souris afin d'assurer que les clés ont un niveau élevé d'entropie. Chaque item dans le flux de clé est généré par de différentes conditions.

un schéma de chiffrement d'image en couleur basée sur la carte skew tent et le hyper système chaotique du 6 ordre CNN a été conçu dans [8]. L'essence du cryptage d'image est confondu et diffusé les pixels, la carte skew tent est appliquée pour générer la séquence de la confusion, tandis que, l'hyper système chaotique du sixième ordre CNN est appliquée pour générer la séquence de diffusion, pour 6 variables d'état du système, il ya au total 120 combinaisons. Pour chaque pixel de l'image claire, une combinaison est choisie pour le cryptage des composantes rouge, verte et bleue, et la combinaison est déterminée par l'une des variables d'état. Chaque pixel est chiffré par le chiffré du pixel précédent et la valeur de combinaison du système CNN.

Dans [9] les auteurs ont utilisé la carte lattices couplée (DCML) avec un time-delay dans un nouveau schéma de chiffrement d'image basée sur l'architecture substitution-diffusion. En utilisant la carte tent pour mélanger les positions des pixels de l'image, puis la carte lattices couplés (DCML) pour confondre la relation entre l'image et son image chiffrée. Dans le processus de génération du flux de clés, le délai variant dans le temps est également intégré dans le schéma proposé pour améliorer la sécurité.

3.8.3 Méthodes basées sur la transformation en ondelettes

Dans l'analyse du signal et de l'image, afin de traduire un signal (image) dans différentes formes différentes transformations mathématiques sont utilisées en fonction de leur adéquation à différentes applications.

Les ondelettes [91] sont des fonctions localisées dans une fréquence autour d'une valeur centrale et qui sont limitées dans le temps. Ils n'ont ni forme d'onde constante ni support fini. Les ondelettes sont générées à partir d'une seule fonction appelée fonction mère d'ondelettes en la détaillant et traduisant dans le paramètre de temps.

Dans la référence [13] un nouveau système de cryptage a été proposé pour sécuriser plusieurs images lors d'une communication et d'une transmission sur un canal non sécurisé. Le schéma de chiffrement d'image proposé est basé sur la transformation en ondelettes et les cartes chaotiques.

Chen and Zhao [92] ont fourni un nouveau procédé pour chiffrer et déchiffrer les images basé sur la transformation en ondelette fractionnée (FWT). Ils cryptent l'image en utilisant deux ordres fractionnaires et une série de facteurs d'échelle. Ils utilisent deux séries de clés dans cette méthode, le déchiffrement d'une image cryptée ne pourrait être réalisé qu'après la connaissance de toutes les clés.

Une nouvelle transformation mathématique à savoir la transformation aléatoire en ondelette fractionnée (FrRnWT) a été proposé dans [14]. En exploitant ces excellentes propriétés mathématiques, un système de cryptage d'empreintes digitales a été proposé afin d'assurer leurs sécurités lors de des communications et transmissions sur des canaux non sécurisés.

3.8.4 Méthodes basées sur des transformations matricielles

Les auteurs de [11] ont adapté certaines transformations matricielles pour créer un nouveau schéma asymétrique de chiffrement d'image par bloc. Premièrement, tous les pixels et dans chaque bloc de l'image originale sont permutés. Ensuite une paire de clés est créée en fonction de transformation matricielle. Puis, l'image est chiffrée en utilisant la clé privée. Finalement, le récepteur utilise la clé publique pour décrypter les messages cryptés.

Acharya et al. [93] ont proposé une méthode qui permet de générer des matrices auto-inversibles. Les matrices auto-inversibles proposées sont ensuite utilisé dans une méthode efficace pour le chiffrement d'image en utilisant des transformations matricielles et l'algorithme de chiffrement de Hill. La méthode proposée demande une complexité de calcul moins élevée que les autres algorithmes vue que le calcul de la matrice inverse n'est pas nécessaire lors du décryptage.

Wang et al. [94] ont suggéré un nouveau schéma pour le chiffrement d'image. Ils ont réalisé une modification des valeurs de pixels au niveau de gris de l'image en fonction de la transformation affine de n-dimension, cette modification rend la transformation du domaine intégrante au domaine intégrante à coefficients entiers.

Dans [12] les auteurs ont proposé une technique de chiffrement d'image numérique qui emploie deux types de transformation non linéaire de pixels et le chiffre traditionnel de Hill qui est une transformation matricielle. Pendant que le chiffre de Hill atteint une bonne diffusion, les deux transformations non-linéaires assurent l'effet de la confusion.

3.8.5 Autres Méthodes

Beaucoup d'algorithmes de chiffrement d'image existant ont été proposées en fonction de différentes technologies, tel que : l'optique [95, 96, 97, 98, 99, 100, 101], la transformation p-Fibonacci [102, 103, 104], le séquençage de l'ADN [15, 16, 105, 106, 107], l'automate cellulaire [108, 109, 110, 111], la transformation de Fourier [112, 113, 114] et beaucoup d'autres techniques.

3.9 Discussion

Assurer la sécurité des images numérique distribuées ou enregistrées dans un réseau non sur est fortement lié à l'algorithme de chiffrement d'images utilisé. Cependant, en raison de sa caractéristique de grandes quantités de données et la forte corrélation entre les pixels, le chiffrement d'une image numérique est en général difficile à manipuler en utilisant les algorithmes de chiffrement classiques tel que le RSA, l'AES et le DES.

Afin de pallier ce problème, Plusieurs cryptosystèmes de chiffrement d'images ont été proposé en se basant sur différentes techniques et stratégies. Néanmoins, la plupart de ces cryptosystèmes souffrent d'un ou de plusieurs problèmes tel que la faible sensibilité à la variation d'image en claire [17, 18],l'espace de clés restreint [17], les clés faibles et les clés équivalentes [19, 20, 21, 18], l'irrésistibilité à l'attaque texte claire connu [22, 23, 24, 25] et l'irrésistibilité à l'attaque texte claire choisi [22, 26, 23, 27, 25].

Dans nos recherches, nous nous sommes concentrés dans un premier temps à proposer un nouveau schéma de cryptage d'image en niveau de gris, le schéma proposé est basée sur l'utilisation d'un grand vecteur d'entiers comme clé secrète pour pouvoir assurer sa sécurité contre les attaques de brute force, ainsi éliminer les pénuries liées à ce problème. Dans un deuxième temps le schéma proposé vise à optimiser le temps d'exécution ; ainsi la complexité de notre algorithme a été évaluée ; le nombre d'instructions primitives a été calculé et la comparaison avec les schémas existants montre que le schéma proposé est le plus rapide.

Néanmoins, le grand problème est dans la résistance à l'attaque texte claire choisi. En effet, plusieurs chercheurs ont pensé à introduire les cryptosystèmes probabilistes où le multiple cryptage d'une image numérique en utilisant le même algorithme et la même clé secrète donne différentes résultats. Mais, la résistance d'un chiffre aux attaques textes clairs choisis nécessite aussi une démonstration pour assurer sa sé-

curité. Ainsi, dans un deuxième temps, nos recherches été concentrés à proposer un deuxième algorithme de cryptage d'image robuste contre ces attaques. Ainsi, notre point de vu consiste à se baser sur un mode de cryptage sûr contre cette attaque et sa sécurité a été déjà démontré.

3.10 Conclusion

Dans ce chapitre, nous avons essayé de mettre le point sur les différentes techniques de cryptage d'images. Ce dernier représente un domaine de recherche très vaste, dont plusieurs techniques ont été adaptées et utilisées. Comparées aux techniques de cryptages conventionnels dédiés au cryptage du texte, les techniques de cryptage d'images sont confrontées à des contraintes supplémentaires. En effet, différentes techniques utilisées dans des cryptosystèmes de cryptage d'images, ont démontré leur futilité. Par conséquent, nous sommes contraints à explorer de nouveaux horizons de recherche afin d'améliorer encore les performances. Le chapitre suivant sera dédié à notre première contribution dans le domaine de cryptage d'images. Le nouveau schéma de chiffrement sans perte proposé est basé sur une combinaison de transformations matricielles et l'opération OU exclusif.

Deuxième partie

Contributions

Chapitre 4

Algorithme de cryptage d'images sans perte basé sur des transformations matricielles et l'opération XOR

4.1 Introduction

Dans le chapitre précédent, nous avons présenté un état de l'art sur les algorithmes de cryptage d'images qui sont basée sur différentes techniques. Nous avons montré que les systèmes de cryptage d'images sont classés en deux catégories : sans perte ou avec perte. Dans la première catégorie, il n'y a pas de différence entre l'image décryptée et l'image originale ; par conséquent, ces méthodes sont plus applicables dans de nombreux domaines sensibles où la non perte est nécessaire. Cependant, dans la deuxième catégorie, l'image déchiffrée n'est pas la même image d'origine et il y a un peu de différence entre elles, dont l'oeil humain ne peut pas la détecter. L'image décryptée avec une petite différence est généralement acceptable selon les applications du schéma. La recherche dans ces domaines a été très généreuse ces dernières années avec l'utilisation de déférentes techniques, elle est ouverte pour de nouvelles idées afin de sécuriser encore les protocoles existants pour obtenir les meilleures performances.

Ce chapitre est destiné à nos contributions de recherche dans le domaine de cryptage d'images sans perte. Il s'agit d'un nouveau schéma symétrique de chiffrement sans perte qui fait une forte relation entre l'image chiffrée et la clé secrète afin de prévenir la connaissance de l'image claire sans la connaissance de la clé. L'algorithme de chiffrement proposé est basé sur des transformations matricielles et l'opération XOR. Contrairement aux systèmes cryptographiques à base de permutation avec de petits espaces de clés, l'algorithme de chiffrement d'images proposé possède un grand espace de clé. Ainsi, il empêche l'analyse par force brute. Les résultats de la simulation montrent l'efficacité et la sécurité de notre système proposé. En outre, l'algorithme AES et autres algorithmes symétriques ont été investigués et la comparaison avec l'algorithme proposé montre la supériorité du schéma proposé. D'un autre coté le calcul de nombre d'instructions primitives du schéma proposé affirme que notre contribution est la plus rapide en la comparant avec des algorithmes récemment proposés .

Le contenu de ce chapitre est organisé comme suit : la section 4.2 décrit la méthode de chiffrement ainsi que la méthode de déchiffrement du cryptosystème proposé. Bien que l'analyse de la sécurité, les performances et les résultats expérimentaux sont discutés dans la section 4.3. La section 4.4 étudie les applications possibles de l'algorithme proposé. Finalement, des conclusions sont tirées dans la section 4.5.

4.2 Méthode proposée

L'objectif principal du système de cryptage d'images sans perte proposé est d'avoir un niveau élevé de confusion en utilisant une forte relation entre l'image-chiffrée et la clé secrète. Dans le schéma proposé le chiffrement d'un pixel de l'image originale dépend des autres pixels. La clé utilisée dans notre système est un vecteur S de taille $1 \times n$ où $n \times n$ est la taille de l'image originale. Les composants de la clé secrète sont des entiers impairs moins de 256, parce que nous allons utiliser la clé secrète pour construire une matrice diagonale inversible.

Puisque le schéma proposé est sans perte, et le texte et les images au niveau gris sont finalement représenté comme des chaines de symboles dans l'intervalle [0 255]. Le système proposé pourrait être appliqué au cryptage de texte.

En revanche l'algorithme de chiffrement d'image proposée traite les images carrées ; dans le cas d'images non-carrés, nous divisons l'image original en blocs de taille 16×16 , nous appliquons ensuite notre schéma à chaque bloc. Si la taille de l'image n'est pas un multiple de 256 un schéma de remplissage peut être utilisé.

4.2.1 Fonction de chiffrement

Etape.1 Tout d'abord, une matrice diagonale $D(S)$, son inverse $D^{-1}(S)$ et une matrice circulante Circ(S) sont construites en utilisant la clé secrète S.

Etape.2 Soit I l'image originale de taille $n \times n$. Calculer la matrice $\acute{I}$ en utilisant la diffusion suivante :

$$\acute{I}(i,j) = (I(i,j) + \acute{I}(i,j-1)) \bmod 256 \oplus Cir(i,j) \tag{4.1}$$

Ici, la valeur initiale $\acute{I}(1,0) = 0$ et $\acute{I}(i,0) = \acute{I}(i-1,n)$ et le symbole $\oplus$ représente l'opération OU exclusif.

Etape.3 La matrice obtenue $\acute{I}$ est multipliée à gauche par la matrice diagonale $D(S)$ et à droite par la matrice $D^{-1}(S)$.

$$C_1 = D(S) \times \acute{I} \times D^{-1}(S) \bmod 256 \ . \tag{4.2}$$

Etape.4 Répéter **Etape.2** une autre fois en utilisant la matrice C_1 afin d'obtenir la ma-

trice chiffrée C.

$$C(i,j) = (C_1(i,j) + C(i,j-1)) \bmod 256 \oplus Cir(i,j) \tag{4.3}$$

4.2.2 Fonction de déchiffrement

Etape.1 Tout d'abord, une matrice diagonale $D(S)$, son inverse $D^{-1}(S)$ et une matrice circulante Circ(S) sont construites en utilisant la clé secrète S.

Etape.2 Soit C l'image chiffrée. Calculer les valeurs de coefficients de C_1 en utilisant la diffusion suivante :

$$C_1(i,j) = ((C(i,j) \oplus Cir(i,j)) - C_1(i,j-1)) \bmod 256 \tag{4.4}$$

Ici, la valeur initiale $C_1(1,0) = 0$ et $C_1(i,0) = C_1(i-1,n)$ et le symbole $\oplus$ représente l'opération OU exclusif.

Etape.3 La matrice obtenue C_1 est multipliée à gauche par la matrice diagonale $D(S)$ et à droite par la matrice $D^{-1}(S)$.

$$\acute{I} = D^{-1}(S) \times C_1 \times D(S) \bmod 256 \ . \tag{4.5}$$

Etape.4 Répéter **Etape.2** une autre fois en utilisant la matrice $\acute{I}$ afin d'obtenir l'image originale I.

$$I(i,j) = ((\acute{I}(i,j) \oplus Cir(i,j)) - \acute{I}(i,j-1)) \bmod 256 \tag{4.6}$$

4.3 Analyses de performances

Des simulations numériques ont été effectuées en utilisant différentes mesures de sécurité pour montrer la sécurité et l'efficacité de l'algorithme proposé. Plusieurs images au niveau de gris de déffirentes tailles sont cryptées en utilisant l'algorithme proposé. Les figures 4.1,4.2 et 4.3 montrent les image claires leurs résultats du chiffrement et du déchiffrement respectivement.

FIGURE 4.1 – Les images claires

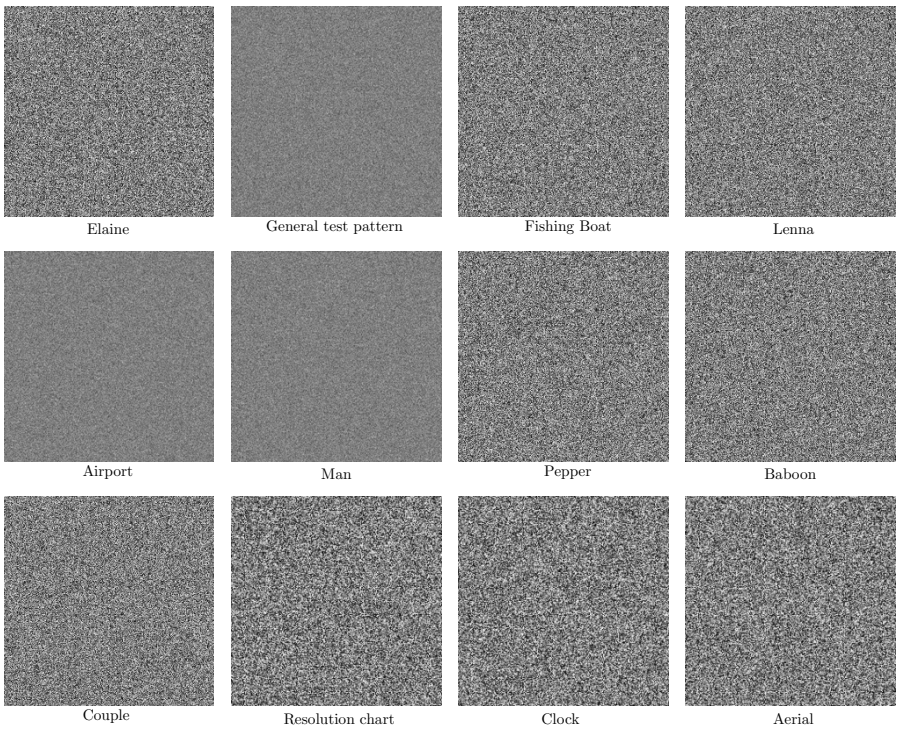


FIGURE 4.2 – Les images cryptées

FIGURE 4.3 – Les images décryptées

4.3.1 Espace de clés

La clé utilisée dans notre schéma est le vecteur S. La taille de la clé secrète S est n où $n \times n$ est la taille de l'image originale. Chaque élément du vecteur S est codé sur 7 bits (des entiers impaires inférieurs à 256). D'où le nombre de bits de chaque élément est $7 \times n$ et l'espace de clés est $2^{7\times n}$. Par exemple pour une image de taille 256×256 l'espace de clés est $2^{7\times 256}$. Ainsi, l'espace de clé est suffisamment grand ce qui rend les attaques par force brute infaisable.

4.3.2 Analyse statistique

L'histogramme

Quatre images de tests ont été utilisées dans l'analyse : Lena, Pepper, Baboon et l'image zéro. Les tracés des histogrammes des images et les images chiffrées sont montrés dans la figure 4.4.

Le résultat montre que les histogrammes des images chiffrées sont uniformes après le cryptage. Subséquemment, il empêche l'adversaire d'extraire des informations significatives en utilisant les histogrammes des images chiffrées voire l'utilisation d'une image spéciale telle que l'image avec la valeur de tous les pixels est zéro.

La corrélation entre les pixels adjacents

Le tableau 4.1 liste les coefficients de corrélation des images claires et leurs chiffrées en utilisant le schéma proposé. Les coefficients de corrélations mesurées des images claires sont prés de 1 tandis que ceux des images chiffrées sont proches de 0. Basant sur les résultats obtenus, nous pouvons affirmer que l'algorithme proposé a supprimé avec succès la corrélation des pixels adjacents.

	image claire			image chiffrée		
	Horizontale	Verticale	Diagonale	Horizontale	Verticale	Diagonale
Lena	0.9852	0.9736	0.9626	0.0031	0.0087	0.0052
Baboon	0.9405	0.9676	0.9158	0.0004	0.0011	0.0076
Pepper	0.9823	0.9805	0.9713	0.0024	0.0014	0.0079
Lena de ref.[115]	0.9201	0.9573	0.9198	0.0050	0.0006	0.0025

TABLE 4.1 – Coefficients de corrélation de deux pixels adjacents

La figure 4.5 montre les corrélations de deux pixels adjacents verticalement horizontalement et diagonalement dans l'image claire et son chiffrée. Il est clair que les pixels adjacents après le cryptage n'ont pas de corrélation.

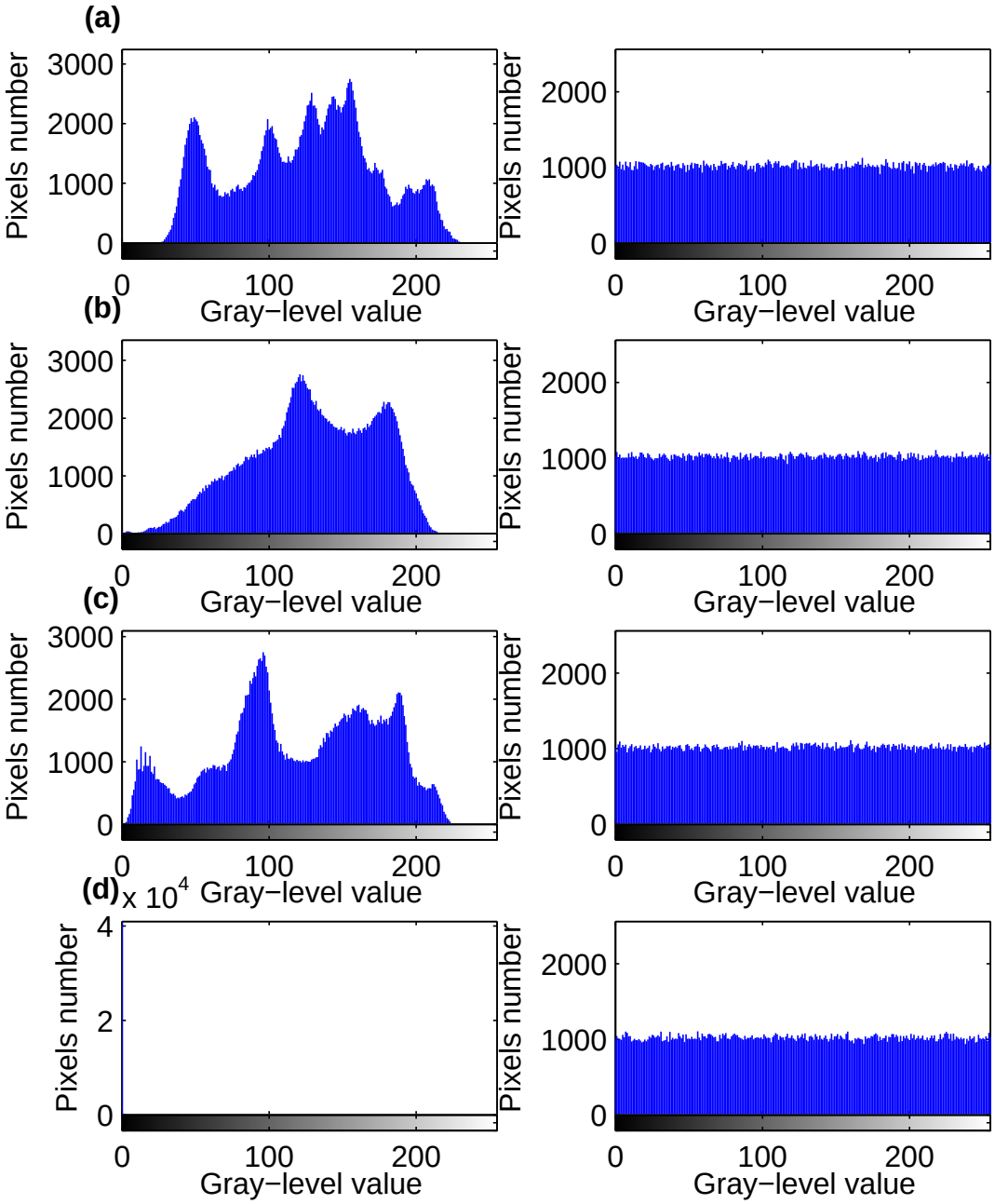


FIGURE 4.4 – L'analyse de l'histogramme des images originales/chiffrées (a) Lena, (b) Baboon, (c) Pepper, (d) Zéro

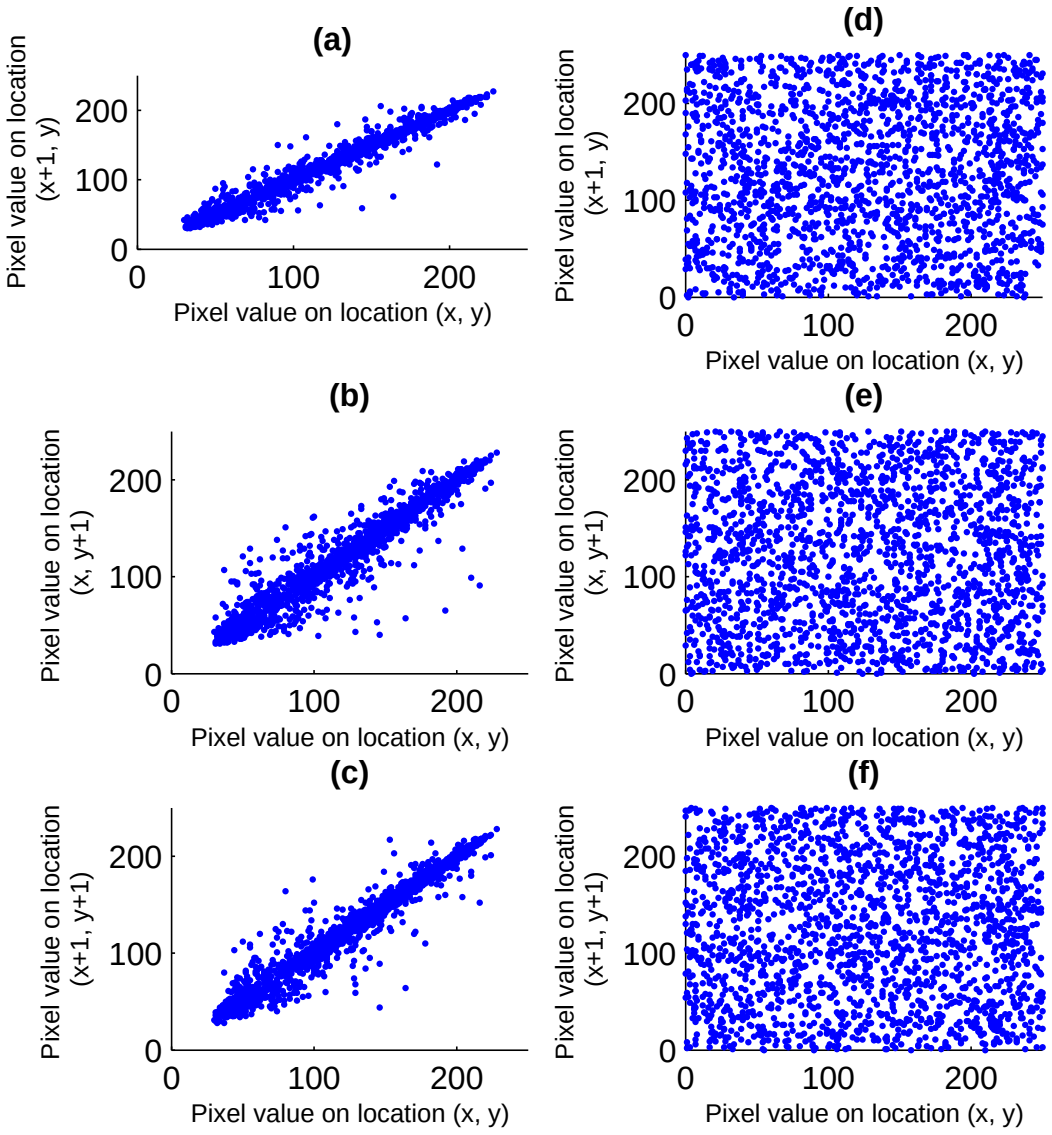


FIGURE 4.5 – Corrélation de deux pixels adjacents horizontalement, diagonalement et verticalement dans l'image originale et l'image chiffrée : (a), (b) et (c) sont pour l'image ; (d), (e) et (f) sont pour l'image cryptée.

4.3.3 Analyse de la sensibilité

Sensibilité de la clé

L'image Lena de taille 512×512 a été chiffrée en utilisant une clé choisie au hasard S de taille 1×512. Ensuite, 512 modifications ont été faites pour tester la sensibilité de la clé en changeant séquentiellement la valeur du dernier bit significatif d'un seul élement de la clé secrète S, suivi par le chiffrement de l'image à l'aide de la clé modifié.

Les deux images chiffrées par les deux clés légèrement différentes sont comparées, le résultat de la simulation est présenté dans la figure 4.6. Nous pouvons facilement noter que les différences sont très élevées pour chaque modification (entre 99 % et 100 %) et donc le chiffrement est très sensible à la clé secrète.

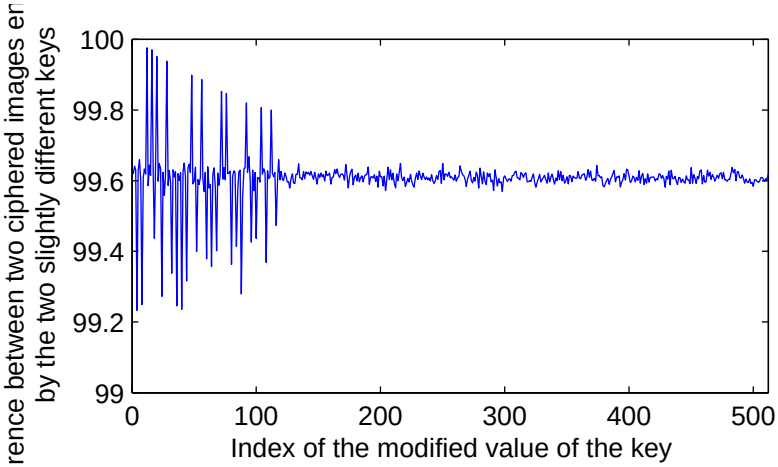


FIGURE 4.6 – Sensibilité de la clé aux modifications d'un seul bit

Analyse de sensibilité aux attaques différentielles

Deux images ont été utilisées dans les tests. La première image est l'image originale, et l'autre est obtenue en changeant la valeur du dernier pixel avec une différence de 1. Ensuite, nous chiffrons les deux images en utilisant la même clé de chiffrement pour obtenir les images correspondantes C_1 et C_2. Les mesures NPCR et UACI en utilisant six images claires sont illustrées dans le tableau 4.2.

	Lena	Baboon	Boat	Pepper	Tiffany	Elaine
NPCR%	99.6059	99.6410	99.5739	99.6399	99.5991	99.6201
UACI%	33.4160	33.4483	33.4798	33.3926	33.4635	33.4707

TABLE 4.2 – Les valeurs NPCR et UACI obtenues en utilisant plusieurs images

Les résultats de la simulation confirment la sensibilité de notre algorithme aux petites modifications de l'image claire. Ainsi, il résiste les attaques différentielles.

4.3.4 L'entropie

Le tableau 4.3 illustre différentes valeurs d'entropie obtenues pour des images claires et chiffrées de différentes tailles. La plus grande valeur d'entropie dans ce cas est 8 donc on peut confirmer que l'algorithme proposé fournit les plus bonnes propriétés d'aléatoire.

Image testée	taille	image claire	image chiffrée
Lena	128×128	7.5888	7.9899
Baboon	256× 256	7.3461	7.9975
Cameraman	256× 256	7.0097	7.9975
Boat	512×512	7.4842	7.9993
Pepper	512×512	7.5937	7.9994

TABLE 4.3 – Analyse de l'entropie du schéma proposé

4.3.5 Propriétées aléatoire de l'image cryptée

Suite de testes NIST 800-22

Etant donné que ce test statistique a besoin de grandes quantités de données, plusieurs images chiffrées de taille 512×512 ont été utilisées pour former une seule suite qui est ensuite utilisée dans le test . Les détails des résultats de la simulation sont décrits dans le tableau 4.4 montrant que la suite passe tous les tests du NIST. Ainsi, les images cryptées en utilisant le schéma proposé ont de bonnes propriétés de caractère aléatoire.

TABLE 4.4: Résultats de la suite de tests NIST 800-22 en utilisant les images cryptées.

Test statistique	**Paramètre**	**Résultat du teste**	**R**
Frequency		0.351337	SUCCESS
Block Frequency	m = 128	0.092575	SUCCESS
Cumulative-sums	Forward	0.621921	SUCCESS
	Reverse	0.507320	SUCCESS

Test statistique	Paramètre	Résultat du teste	R
Runs		0.898836	SUCCESS
Longest-runs		0.020197	SUCCESS
Rank		0.466365	SUCCESS
FFT		0.832839	SUCCESS
Non-overlapping-templates	000000001	0.453117	SUCCESS
Overlapping-templates		0.871630	SUCCESS
Universal		0.157358	SUCCESS
Approximate entropy	10	0.714444	SUCCESS
Random-excursions	x = -4	0.229584	SUCCESS
	x = -3	0.457910	SUCCESS
	x = -2	0.493392	SUCCESS
	x = -1	0.276305	SUCCESS
	x = 1	0.549540	SUCCESS
	x = 2	0.982281	SUCCESS
	x = 3	0.503181	SUCCESS
	x = 4	0.639004	SUCCESS
Random-excursions variant	x = -9	0.739528	SUCCESS
	x = -8	0.817623	SUCCESS
	x = -7	0.678313	SUCCESS
	x = -6	0.865728	SUCCESS
	x = -5	0.917287	SUCCESS
	x = -4	0.850555	SUCCESS
	x = -3	0.669173	SUCCESS
	x = -2	0.199451	SUCCESS
	x = -1	0.056021	SUCCESS
	x = 1	0.589177	SUCCESS
	x = 2	0.755203	SUCCESS
	x = 3	0.845343	SUCCESS
	x = 4	0.918712	SUCCESS
	x = 5	0.787149	SUCCESS
	x = 6	0.821630	SUCCESS
	x = 7	0.853746	SUCCESS
	x = 8	0.901833	SUCCESS
	x = 9	0.943775	SUCCESS
Serial	16	0.686863	SUCCESS
	16	0.412791	SUCCESS
Linear-complexity	500	0.178839	SUCCESS

Suite de testes Diehard

Plus de 40 images chiffrées ont été utilisées dans ce teste. Les résultats du teste sont rapportés dans le tableau 5.7. A partir des résultats obtenus, nous pouvons confirmer que les sorties du système cryptographique passent tous les testes statistiques fournies par Diehard, et ceci signifie que les images chiffrées ne peuvent pas être distingués des séquences aléatoires uniformes.

Nom du teste	Paramètre	P-value	Résultat
BIRTHDAY SPACINGS		0.344827	Pass
OVERLAPPING 5-PERMUTATION		0.318721	Pass
BINARY RANK TEST	31×31	0.452689	Pass
	32×32	0.943838	Pass
	6×8	0.929990	Pass
BITSTREAM		0.05338	Pass
COUNT-THE-1's	stream	0.171824	Pass
COUNT-THE-1's	specific	0.388759	Pass
PARKING LOT		0.566958	Pass
MINIMUM DISTANCE		0.954872	Pass
3DSPHERES		0.917177	Pass
SQEEZE		0.207491	Pass
OVERLAPPING SUMS		0.134431	Pass
RUNS	Up	0.839628	Pass
	Down	0.534730	Pass
CRAPS	no. of wins	0.322741	Pass
	throws/game	0.411150	Pass

TABLE 4.5 – La moyenne des résultats obtenus en utilisant la suite de tests Diehard

4.3.6 Complexité de l'algorithme

Afin d'évaluer la complexité de l'algorithme proposé l'image Lena de taille 256 × 256 a été utilisée dans le test. Les résultats obtenus en utilisant l'algorithme proposé sont comparés avec ceux des algorithmes [116, 16, 117, 118, 119, 120] dans le tableau 4.6.

Le tableau 4.6 a montré que l'algorithme proposé exige moins d'instructions primitives par pixel par round par rapport aux autres algorithmes, ce qui signifie que le

schéma proposé est le plus rapide.

	Nombre d'instructions primitives par pixel par round	Nombre de pixels	Nombre de rounds	Nombre total d'instructions primitives
Notre schéma	256	65,536	1	16,777,216
Ref.[116]	3	65,536	128	25,165,824
Ref.[16]	465	65,536	1	30,670,848
Ref.[117]	327	65,536	2	42,860,544
Ref.[118]	1358	65,536	2	177,995,776
Ref.[119]	942	65,536	1	61,734,912
Ref.[120]	1337	65,536	1	87,621,632

TABLE 4.6 – Comparaison en terme nombre d'instructions primitives

4.4 Applications du schéma

4.4.1 Images avec une grande région de la même couleur

Le chiffrement d'images numériques est généralement difficile à gérer par les algorithmes de chiffrement classiques comme AES en raison des caractéristiques des images tel que la redondance, la forte corrélation entre les pixels et la taille volumineuse. D'une autre part de tels algorithmes ne sont pas convenable pour chiffrer des images qui contiennent de grandes zones d'une seule couleur comme les images médicales et les logos. Cependant, notre proposition chiffre correctement ce type d'images.

Des simulations numériques ont été faites pour confirmer les bonnes performances de notre schéma. La figure 4.7 montre le cryptage de deux images qui contiennent une grande zone de couleur unique en utilisant l'algorithme AES et le schéma proposé. Les résultats de chiffrement montrent la supériorité de notre proposition.

4.4.2 Images médicales

Récemment, les dossiers médicaux électroniques ont été envoyés largement sur les réseaux et l'Internet afin d'améliorer les services [121, 122, 123]. Les images médicales doivent être cryptées avant d'être envoyées sur les réseaux. Cependant, un système

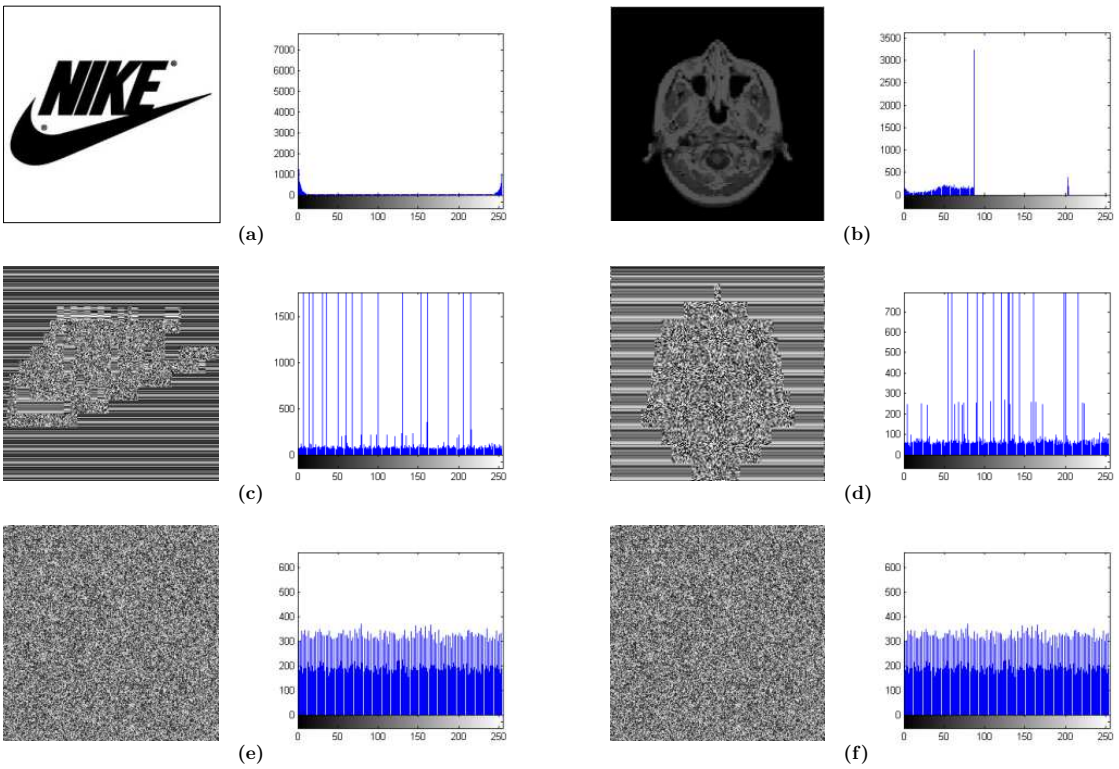


FIGURE 4.7 – (a) L'image Nike et son histogramme, (b) L'image Mri et son histogramme, (c) L'image Nike chiffrée par AES et son histogramme, (d) L'image Mri chiffrée par AES et son histogramme, (e) L'image Nike chiffrée par l'algorithme proposé et son histogramme et (f) L'image Mri chiffrée par l'algorithme proposé et son histogramme.

de cryptage d'image utilisé pour de telles données devrait garantir la non-perte d'informations et l'image décryptée devraient être la même que la image originale. La figure 4.8 illustre le chiffrement et le déchiffrement de plusieurs images médicales en utilisant le schéma proposé.

Une opération de soustraction pixel par pixel entre l'image claire et l'image déchiffrée a été faite et le résultat est zéro. Il est clair qu'il n'y a pas de perte de données en utilisant le schéma proposé, il est donc approprié pour des applications de chiffrement et de transmission d'images médicales.

4.4.3 Chiffrement de texte

Un autre avantage des systèmes de chiffrement sans perte par rapport aux algorithmes de chiffrement avec pertes est que l'adaptation de la première classe pour le chiffrement de texte. Un exemple complet de cryptage de texte en utilisant le schéma

proposé est expliqué par la suite.

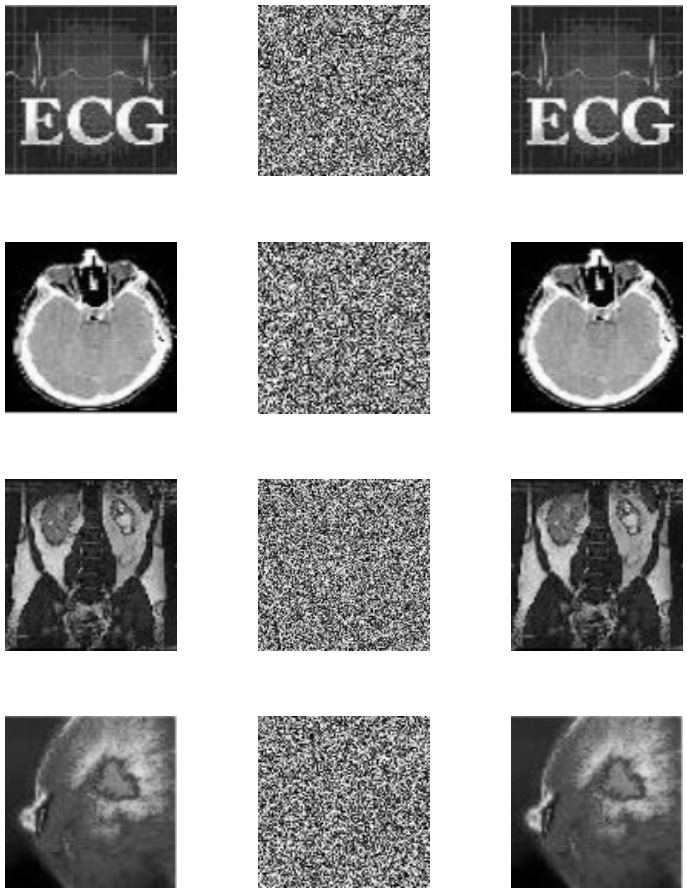


FIGURE 4.8 – De haut en bas, les images médicales ECG, Brain, MRI and Mammogram, de droite à gauche, la figure présente les images originales et leurs chiffrées et déchiffrées

Cryptage

1. Soit P le texte en clair qui est un ensemble de chaine de caractères du code ASCII. P = Cryptography is the study of mathematical techniques linked to the information security aspects like confidentiality, integrity and authenticity. Encryption is the way to transform an intelligible data into unintelligible one to ensure the confidentiality.

2. Exprimer chaque caractère de P par sa valeur ASCII
   I = 67 114 121 112 116 111 103 114 97 112 104 121 32 105 115 32 116 104 101 32 115 116 117 100 121 32 111 102 32 109 97 116 104 101 109 97 116 105 99 97 108 32 116 101 99 104 110 105 113 117 101 115 32 108 105 110 107 101 100 32 116 111 32 116 104 101 32 105 110 102 111 114 109 97 116 105 111 110 32 115 101 99 117 114 105 116 121 32 97 115 112 101 99 116 115 32 108 105 107 101 32 99 111 110 102 105 100 101 110 116 105 97 108 105 116 121 44 32 105 110 116 101 103 114 105 116 121 32 97 110 100 32 97 117 116 104 101 110 116 105 99 105 116 121 46 32 69 110 99 114 121 112 116 105 111 110 32 105 115 32 116 104 101 32 119 97 121 32 116 111 32 116 114 97 110 115 102 111 114 109 32 97 110 32 105 110 116 101 108 108 105 103 105 98 108 101 32 100 97 116 97 32 105 110 116 111 32 117 110 105 110 116 101 108 108 105 103 105 98 108 101 32 111 110 101 32 116 111 32 101 110 115 117 114 101 32 116 104 101 32 99 111 110 102 105 100 101 110 116 105 97 108 105 116 121 46

3. Soit S la clé secrète.
   S = 208 231 32 233 161 24 71 140 245 247 40 248 245 124 204 36

4. Former une matrice carrée en utilisant le vecteur I, ensuite appliquer le schéma de cryptage proposé pour obtenir le chiffré C
   C = 224 39 190 52 165 144 34 70 156 121 179 99 43 85 163 159 7 59 26 117 195 37 152 78 22 161 47 108 253 208 154 43 167 250 234 217 165 33 209 226 213 18 18 16 220 140 159 14 78 167 237 148 147 149 252 239 147 161 37 173 118 15 219 151 63 231 45 248 3 89 108 19 108 231 237 194 147 111 172 83 199 137 36 167 122 161 109 143 45 2 117 10 184 66 180 44 112 71 101 125 220 46 109 195 64 171 152 234 78 241 221 60 44 216 29 181 36 22 212 227 31 117 100 111 243 253 134 1 169 106 218 86 4 183 154 16 113 97 104 139 11 189 138 166 190 236 182 133 124 150 149 108 243 186 20 191 92 16 130 94 118 171 227 17 203 150 178 45 232 232 252 211 93 88 19 210 14 66 212 52 195 25 26 72 60 93 155 179 32 24 159 243 187 213 60 201 125 125 235 148 132 192 195 188 233 180 51 31 39 137 196 19 179 40 37 135 132 237 26 116 251 76 43 203 251 188 209 90 246 47 191 211 125 227 75 109 134 215 155 7 255 146 77 189 48 119 33 202 251 252 251 84 80 51 68 151

Décryptage Suivre les mêmes étapes de cryptage, mais en utilisant le texte chiffré et la fonction de décryptage afin d'obtenir les données décryptées D.
D = 67 114 121 112 116 111 103 114 97 112 104 121 32 105 115 32 116 104 101 32 115 116 117 100 121 32 111 102 32 109 97 116 104 101 109 97 116 105 99 97 108 32 116 101 99 104 110 105 113 117 101 115 32 108 105 110 107 101 100 32 116 111 32 116 104 101 32 105 110 102 111 114 109 97 116 105 111 110 32 115 101 99 117 114 105 116 121 32 97 115 112

101 99 116 115 32 108 105 107 101 32 99 111 110 102 105 100 101 110 116 105 97 108 105 116 121 44 32 105 110 116 101 103 114 105 116 121 32 97 110 100 32 97 117 116 104 101 110 116 105 99 105 116 121 46 32 69 110 99 114 121 112 116 105 111 110 32 105 115 32 116 104 101 32 119 97 121 32 116 111 32 116 114 97 110 115 102 111 114 109 32 97 110 32 105 110 116 101 108 108 105 103 105 98 108 101 32 100 97 116 97 32 105 110 116 111 32 117 110 105 110 116 101 108 108 105 103 105 98 108 101 32 111 110 101 32 116 111 32 101 110 115 117 114 101 32 116 104 101 32 99 111 110 102 105 100 101 110 116 105 97 108 105 116 121 46

Remplacer chaque valeur ASCII par le caractère correspondant afin d'obtenir le texte déchiffré :
P = Cryptography is the study of mathematical techniques linked to the information security aspects like confidentiality, integrity and authenticity. Encryption is the way to transform an intelligible data into unintelligible one to ensure the confidentiality.

4.5 Conclusion et perspectives

Ce chapitre présente notre première proposition, qui est une nouvelle technique sécurisée et efficace qui assure le chiffrement d'image sans perte. Afin de surmonter la faiblesse des systèmes de chiffrement à base de permutation avec de petits espaces de clés, l'algorithme de chiffrement d'image proposé a un grand espace de clés et peut empêcher avec succès l'attaque par force brute. Des simulations d'analyse de la sécurité ont été effectuées pour assurer l'efficacité du système proposé contre l'analyse statistique, l'analyse de l'espace de clé, analyse de sensibilité, etc. D'un autre part, le calcul du nombre d'instructions primitives de notre contribution confirme la rapidité de notre algorithme en le comparant avec les algorithmes de cryptage d'image récemment proposés.

En se basant sur les résultats obtenus, nous pouvons affirmer que le schéma proposé est adapté pour les applications de chiffrement d'image et de transmission. Dans le chapitre qui suit, nous allons introduire notre deuxième contribution, qui consiste en un cryptosystème pour les images numériques basée sur l'architecture confusion-diffusion en utilisant la théorie du chaos.

Chapitre 5

Algorithme ajustable-flexible de cryptage d'images en couleurs basé sur la théorie du chaos

5.1 Introduction

Selon Shannon [5] ; la confusion et la diffusion sont deux méthodes principales pour éliminer les redondances et la forte corrélation de pixels. La diffusion permet la modification des valeurs de pixels en utilisant la clé. D'autre part, la confusion diminue la redondance en répartissant les pixels sur toute l'image chiffrée [124, 125].

De nombreux mécanismes de chiffrement d'image ont été proposés dans la littérature en utilisant diverses méthodes. Au cours des dernières années, l'utilisation de systèmes chaotiques en cryptographie a attiré l'attention d'un grand nombre de chercheurs, en raison de leur sensibilité au valeurs initiales et la non linéarité [126, 127, 128, 129].

Notre contribution vise à proposer un nouvel algorithme, basé sur la théorie du chaos, qui a une structure simple et les propriétés de variabilité dans le but de renforcer La sécurité. Nous introduisons un algorithme ajustable-flexible de cryptage d'image en couleur basée sur l'architecture confusion/diffusion en utilisant la carte chaotique non linéaire PWLCM qui possède des propriétés dynamiques parfaites. Des performances satisfaisantes de sécurité ont été obtenues en utilisant une seule ronde de chiffrement. Le rendement de notre proposition est renforcé en le comparant avec les cryptosystèmes de chiffrement d'image en couleur récemment proposés. Les résultats expérimentaux indiquent que l'algorithme proposé est sûr et est efficace. Néanmoins, le chiffrement de chaque pixel ne dépend pas seulement du pixel en clair qui le génère, mais sur tous les pixels de l'image. Ainsi, un petit changement dans un pixel de l'image claire cause une image chiffrée complètement différente. De plus, avec l'addition du ajustement, si on chiffre une image plusieurs fois en utilisant la même clé on obtiendra des images chiffrées différentes à chaque fois. En plus l'algorithme proposé est basé sur un mode de cryptage sûr (par démonstration) contre l'attaque texte clair choisi qui est le défie principal des cryptosystèmes de nos jours.

Le reste du chapitre est organisé comme suit : Dans la section 5.2, nous illustrons le système chaotique PWLCM. Une brève introduction au chiffrement par blocs ajustable-flexible est présentée dans la section 5.3. Dans les sections 5.4 et 5.5, nous décrivons le schéma proposé. Les performances et l'analyse de la sécurité sont présentées dans la section 5.6 et la conclusion est conçue dans la section 5.7.

5.2 La carte chaotique PWLCM

Le système PWLCM a une très bonne ergodicité et très sensible aux valeurs initiales ce qui est adéquat pour la cryptographie. Le système PWLCM est présenté par l'équation (5.1).

$$x_{i+1} = F_p(x_i) = \begin{cases} x_i/p, & 0 \le x_i \le p \\ (x_i - p)/(0.5 - p), & p \le x_i \le 0.5 \\ F_p(1 - x_j), & 0.5 \le x_i \le 1 \end{cases} \tag{5.1}$$

La carte est chaotique si $x \in [0,1)$ et le paramètre de contrôle $p \in (0,5,0)$ [130]. Dans cet article, les valeurs initiales de cette carte x et les paramètres de contrôle p sont utilisées comme des clés secrètes.

Le système chaotique PWLCM est utilisé à la fois dans la permutation et la diffusion du schéma proposé. Dans la phase de confusion, nous convertissons une séquence aléatoire à une séquence entière en utilisant l'équation suivante :

$$\alpha_i = \text{fix}(\text{bitsll}(x_i, 8)) \tag{5.2}$$

Où fix(n) retourne la partie entière de n, et bitsll(n, i) renvoie la valeur entière du résultat de décalage logique à gauche de l'entrée n par i bits.

5.3 Chiffrement par blocs ajustable-flexible

Un chiffrement par blocs classique prend deux entrées : une clé $K \in \{0,1\}^k$ et un message (ou texte clair) $M \in \{0,1\}^n$ et génère une seule sortie : un texte chiffré $C \in \{0,1\}^n$. La signature d'un chiffrement par bloc est donc :

$$\{0,1\}^k \times \{0,1\}^n \longrightarrow \{0,1\}^n \tag{5.3}$$

Le chiffrement par blocs (permutations pseudo-aléatoires) est intrinsèquement déterministe : chaque chiffrement d'un message donné avec une clé donnée sera le même. Afin de pallier ce problème, Liskove, Rivest et Wagner [131] ont proposé de réviser la notion d'un chiffrement par bloc de sorte qu'elle contienne un mécanisme pour la variabilité. La primitive révisée a été appelée chiffrement par bloc tweakable(ajustable-flexible), a la signature suivante :

$$\phi : \{0,1\}^k \times \{0,1\}^t \times \{0,1\}^n \longrightarrow \{0,1\}^n \tag{5.4}$$

Donc un chiffrement par bloc ajustable-flexible prend trois entrées : une clé $K \in \{0,1\}^k$, un ajustement $T \in \{0,1\}^t$, et un message (ou texte clair) $M \in \{0,1\}^n$ et produit en sortie un texte chiffré $C \in \{0,1\}^n$.

Dans la conception d'un chiffrement par blocs ajustable-flexible, les auteurs de [131] avez certains objectifs. Ils veulent construire des chiffrements par blocs ajustable-flexible aussi efficace que possible. En outre, ils s'attendent aux ajustements pour être changés fréquemment, donc dans un chiffrement par bloc ajustable-flexible la propriété de changer l'ajustement doit être efficace. Pour le chiffrement par blocs ajustable-flexible construits à partir d'un chiffrement par bloc, la modification de l'ajustement ne devrait pas nécessiter la recomposition du chiffrement par blocs. Et, pour tout chiffrement par bloc ajustable-flexible, changer l'ajustement devrait être moins coûteux que changer la clé.

Un chiffrement par blocs ajustable-flexible devrait également être sécurisé, ceci signifie que même si un adversaire a contrôlé l'ajustement entré, les auteurs veulent que le chiffrement par bloc ajustable-flexible reste sécurisé. Ils distinguent ainsi, soigneusement entre la fonction de la clé, qui est de fournir l'incertitude à l'adversaire, et le rôle de l'ajustement, qui est de fournir la variabilité. L'ajustement n'est pas destiné à fournir une incertitude supplémentaire à un adversaire, et garder l'ajustement secret ne doit pas fournir une grande résistance cryptographique selon les auteurs.

5.3.1 Modes d'opération ajustable-flexible

Liskove, Rivest et Wagner prétendent qu'il est plus facile de concevoir et de prouver la sécurité des applications en utilisant le chiffrement par blocs ajustable-flexible. Ainsi, ils ont présenté trois modes de fonctionnement ajustable-flexible, avec des preuves de sécurité pour chacun. Dans les trois cas, ils n'ont pas suggéré que le mode ajustable-flexible est supérieur aux modes de fonctionnement existants. Mais, ils soulignèrent que ces modes devraient être prises avant tout comme une démonstration des avantages conceptuels acquise en travaillant avec les chiffrements par bloc ajustable-flexible.

EnchaînementT de weak (TC)

L'enchaînement des blocs ajustable-flexible (TC) est un mode de chiffrement symétrique modelé après l'enchaînement des blocs(CBC). Un ajustement initiale T_0 joue le rôle d'un vecteur d'initialisation (IV) pour CBC. Chaque bloc de message M_i est chiffré en utilisant la clé de chiffrement K et un ajustement T_{i-1}, où $C_i = T_i$ pour $i > 0$(voir

la figure 5.1).

Le texte chiffré final est $(T_0, C_1 \circ\circ\circ\circ C_l)$. Pour déchiffrer, nous calculons $M_1 = D_K(T_0, C_1)$ et $M_i = D_K(C_{i-1}, Ci)$ pour $i > 1$.

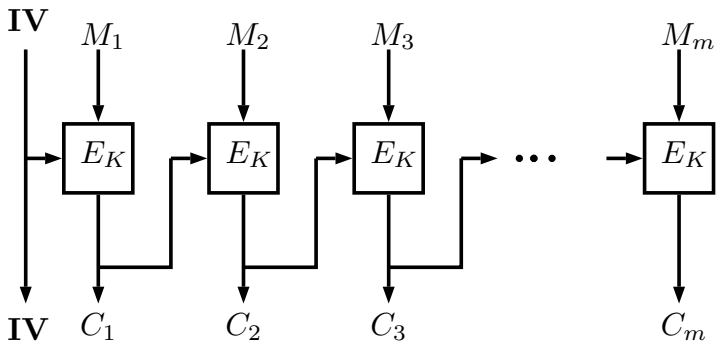


FIGURE 5.1 – Enchaînement des blocs ajustable-flexible

La sécurité de ce mode de cryptage contre l'attaque texte clair choisi est assurée. Une démonstration complète se trouve dans la référence [131].

Cryptage d'incrémentation ajustable-flexible (TIE)

Un autre schéma de chiffrement symétrique est le mode " cryptage d'incrémentation ajustable-flexible " (TIE) qui est censé être similaire au mode CTR de chiffrement par bloc. En mode TIE, le message est divisé en blocs $M_0, \ldots, M_m$. Un ajustement initiale IV est utilisé, et chaque bloc de texte chiffré est généré comme suit :$C_i = E(IV + i, M_i)$, où $IV + i$ se réfère à la simple addition de i et IV modulo 2^t. Voir la figure 5.2.

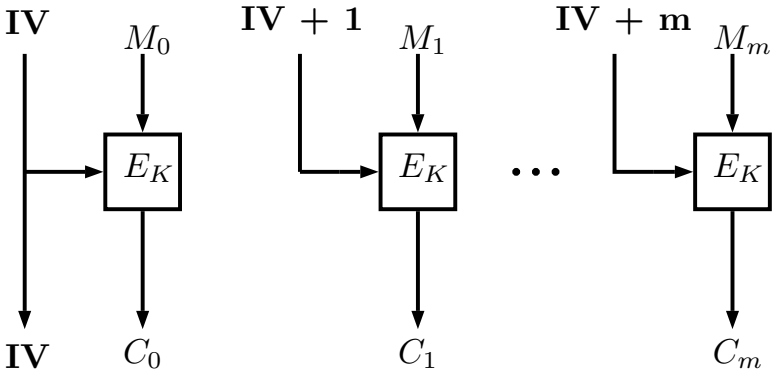


FIGURE 5.2 – Cryptage d'incrémentation ajustable-flexible

La preuve que le mode TIE est sécurisé est extrêmement semblable à la preuve que le mode TBC est sécurisé, mais encore plus simple, et la démonstration est dans la référence [131].

Chiffrement authentifié ajustable-flexible(TAE)

Dans cette section, Les auteurs proposent un mode de chiffrement authentifié (TAE) basée sur l'utilisation d'un chiffrement par bloc ajustable-flexible. Ce mode peut être considéré comme une paraphrase ou le retraitement de l'architecture du mode OCB (dictionnaire de décalage proposé par Rogaway et al. [132]). Une modification est faite afin d'employer la notion du chiffrement par blocs ajustable-flexible.

Le mode de cryptage a été classé comme Un chiffrement par bloc ajustable-flexible fort ; ainsi, sa sécurité contre l'attaque texte chiffré choisi adaptatif a été démontré [131].

5.4 Schéma de chiffrement d'images proposé

5.4.1 Processus de Permutation

Afin d'éliminer la corrélation entre les pixels adjacents une permutation est effectuée aux pixels de l'image ordinaire à l'aide de la carte chaotique PWLCM. Deux séquences aléatoires sont utilisées dans cette étape afin d'améliorer l'espace de permutation et la sécurité du schéma.

Soit I l'image claire en couleur de taille $H \times W \times 3$. Le processus de permutation est exprimé comme suit.

1. Itérer la carte chaotique PWLCM deux fois en utilisant les clés secrètes $(x_1,\ p_1)$ et $(x_2,\ p_2)$ dans le but d'obtenir deux séquences aléatoires $\{x'_1, x'_2, \ldots, x'_{3\times H\times W/2}\}$, $\{x''_1, x''_2, \ldots, x''_{3\times H\times W/2}\}$, les deux séquences ont la même taille $3 \times H \times W/2$.

2. Affecter alternativement les valeurs successives des deux séquences pour décrire une nouvelle séquence $S = \{x'_1, x'_2, \ldots, x'_{3\times H\times W/2}, x''_1, x''_2, \ldots, x''_{3\times H\times W/2}\}$. Puis arranger S dans l'ordre croissant pour obtenir O l'index de l'ordre de la séquence $\{O_i, i = 1, \ldots, 3 \times H \times W\}$

3. Remodeler l'image claire à un vecteur U ; permuter le vecteur U en utilisant O afin d'obtenir le vecteur permuté P.

5.4.2 Processus de Diffusion

Dans le schéma proposé, chaque pixel-chiffré est lié non seulement au pixel en clair qui le produit, mais à tous les autres pixels. Ainsi, un petit changement dans un pixel de l'image claire conduit à une image chiffrée complètement différente.

En outre, la notion de cryptage ajusté a été utilisée afin d'assurer la variabilité du schéma proposé. Ainsi, avec l'ajout de l'ajustement, une image claire est cryptée à différentes images en utilisant la même clé secrète. Ainsi, le rôle de l'ajustement est d'assurer la variabilité du schéma [131].

Soit ϕ le processus de diffusion du schéma proposé, qui prend trois entrées : une clé secrète $K \in \{0,1\}^k$(k est l'espace de clé), un ajustement $T \in \{0,1\}^t (t = 256 \times 256)$, et le vecteur permuté $P \in \{0,1\}^n (n = H \times W \times 3\ )$ et produit en sortie une image chiffrée $C' \in \{0,1\}^n$. la signature de la fonction ϕ est définie par l'équation suivante :

$$\begin{array}{rcl} \phi : \{0,1\}^k \times \{0,1\}^t \times \{0,1\}^n & \longrightarrow & \{0,1\}^n \\ (K,T,P) & \longrightarrow & C' \end{array} \tag{5.5}$$

La figure 5.3 illustre le modèle de diffusion utilisé dans le schéma proposé. Une explication algorithmique de notre méthode de diffusion est détaillée dans l'algorithme 7.

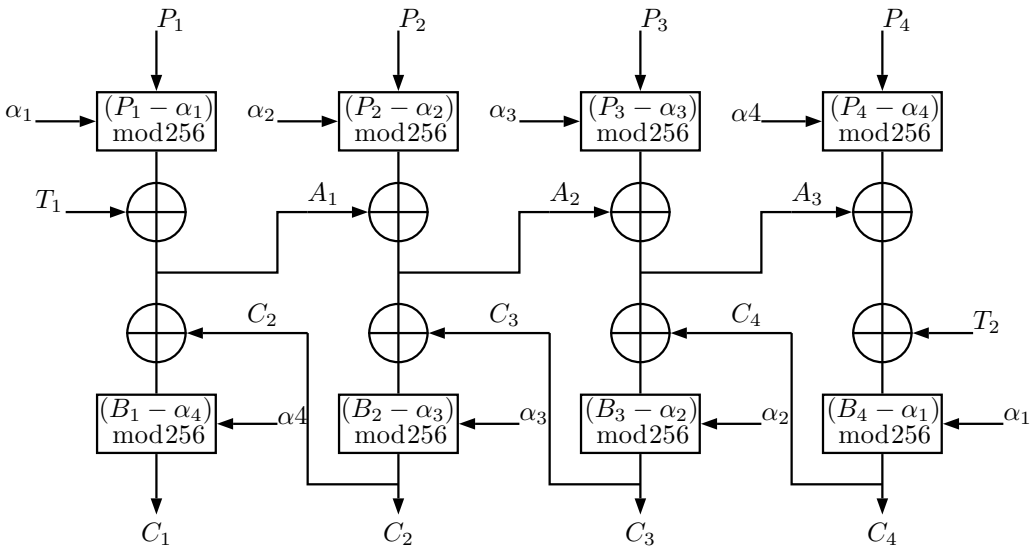


FIGURE 5.3 – Modèle de diffusion du schéma proposé en utilisant 4 pixels.

Algorithm 7 Diffusion

input : Shuffled_vector : P ; secret_parameters : x_3, p_3 ; tweak : T_1, T_2 ; images_size : H, W
output : Cipher_image : C'
Utiliser x_3, p_3 pour obtenir une séquence chaotique X de taille $3 \times H \times W$ en utilisant Eq.(5.1)
Convertir X à une séquence d'entier nommée α en utilisant Eq.(5.2)
$A_0 \leftarrow T_1$
$m \leftarrow 3 \times H \times W$
for i = 1 **to** m **do**
    $R_i \leftarrow (P_i - \alpha_i) \bmod 256$
    $A_i \leftarrow R_i \oplus A_{i-1}$
$B_m \leftarrow A_m \oplus T_2$
$C_m \leftarrow (B_m - \alpha_1) \bmod 256$
for i = m-1 **to** 1 **do**
    $B_i \leftarrow A_i \oplus C_{i-1}$
    $C_i \leftarrow (B_i - \alpha_{m-i+1}) \bmod 256$
Remodeler le résultat obtenu C en une matrice 3D afin d'obtenir l'image chiffrée C'
return C'

5.5 Algorithme de déchiffrement d'image proposé

5.5.1 Algorithme de diffusion inverse

L'inverse du mécanisme de notre diffusion prend en entrée trois paramètres : la clé secrète $K \in \{0,1\}^k$, l'ajustement $T \in \{0,1\}^t$, et l'image chiffrée $C' \in \{0,1\}^n$ et produit en sortie le vecteur permuté $P \in \{0,1\}^n$.

Une explication algorithmique de la diffusion inverse est détaillée dans l'algorithme. 8

5.5.2 Algorithme de permutation inverse

1. Itérer la carte chaotique PWLCM deux fois en utilisant les clés secrètes (x_1, p_1) et (x_2, p_2) dans le but d'obtenir deux séquences aléatoires $\{x'_1, x'_2, \ldots, x'_{3\times H\times W/2}\}$, $\{x''_1, x''_2, \ldots, x''_{3\times H\times W/2}\}$, les deux séquences ont la même taille $3 \times H \times W/2$.

2. Affecter alternativement les valeurs successives des deux séquences pour décrire une nouvelle séquence $S = \{x'_1, x'_2, \ldots, x'_{3\times H\times W/2}, x''_1, x''_2, \ldots, x''_{3\times H\times W/2}\}$. Puis

Algorithm 8 Diffusion_invrse

input : cipher_image : C' ; secret_parameters : x_3, p_3 ; tweak : T_1, T_2 ; images_size : H, W
output : shuffled_vector : P
Remodeler l'image cryptée C' en un vecteur C
Utiliser x_3, p_3 pour obtenir une séquence chaotique X de taille $3 \times H \times W$ en utilisant Eq.(5.1)
Convertir X à une séquence d'entier nommée α en utilisant Eq.(5.2)
$m \leftarrow 3 \times H \times W$
$B_m \leftarrow (C_m + \alpha_1) \bmod 256$
$A_m \leftarrow B_m \oplus T_2$
for i = m-1 **to** 1 **do**
    $B_i \leftarrow (C_i + \alpha_{m-i+1}) \bmod 256$
    $A_i \leftarrow B_i \oplus C_{i-1}$
$A_0 \leftarrow T_1$
for i = 1 **to** m **do**
    $R_i \leftarrow A_i \oplus A_{i-1}$
    $P_i \leftarrow (R_i + \alpha_i) \bmod 256$
return P

arranger S dans l'ordre croissant pour obtenir O l'index de l'ordre de la séquence $\{O_i, i = 1, \ldots, 3 \times H \times W\}$

3. Calculer O' la permutation inverse de O.

4. Permuter le vecteur P en utilisant la permutation inverse O' afin d'obtenir le vecteur U.

5. Transformer le vecteur U à l'image couleur déchiffrée I.

5.6 Sécurité et analyse de performances

Des simulations numériques ont été réalisées pour prouver la robustesse du système de chiffrement proposé en utilisant les différentes mesures de sécurité. Plusieurs images en couleur standards de différentes tailles sont employées comme des images claires dans les tests. Les paramètres de contrôle de données et les valeurs d'initialisation sont définies comme suit : $x_1 = 0.3425, x_2 = 0.7759, x_3 = 0.9286, p_1 = 0.4549, p_2 = 0.2543$ et $p_3 = 0.1974$, et la valeur de l'ajustement est $T_1 = 174, T_2 = 210$. Les résultats de la simulation sont présentés dans les figures 5.4, 5.5 et 5.6. Comme nous voyons, les images claires sont illustrées dans la figure 5.4, tandis que la figure 5.5 illustre les images cryptées et la figure 5.6 illustre les images décryptées.

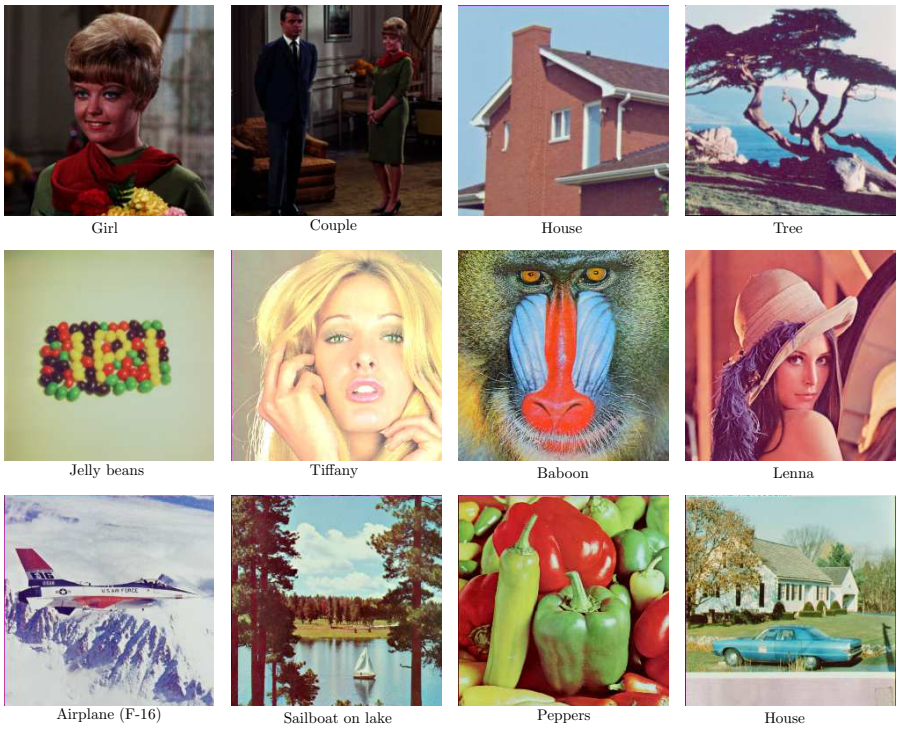


FIGURE 5.4 – Les images couleurs claires.

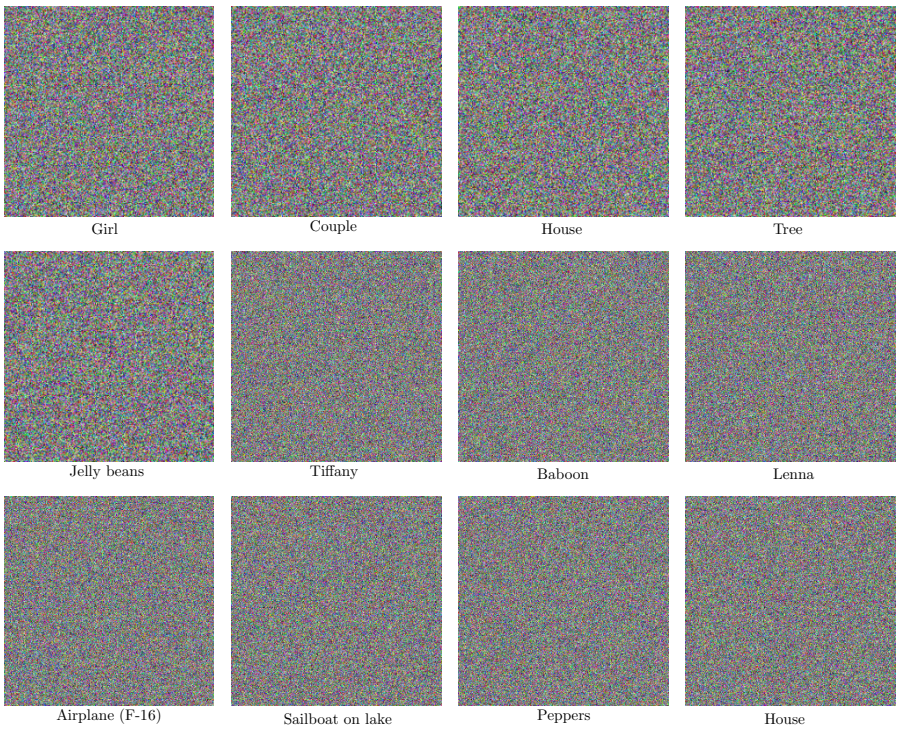


FIGURE 5.5 – Les images couleurs cryptées.

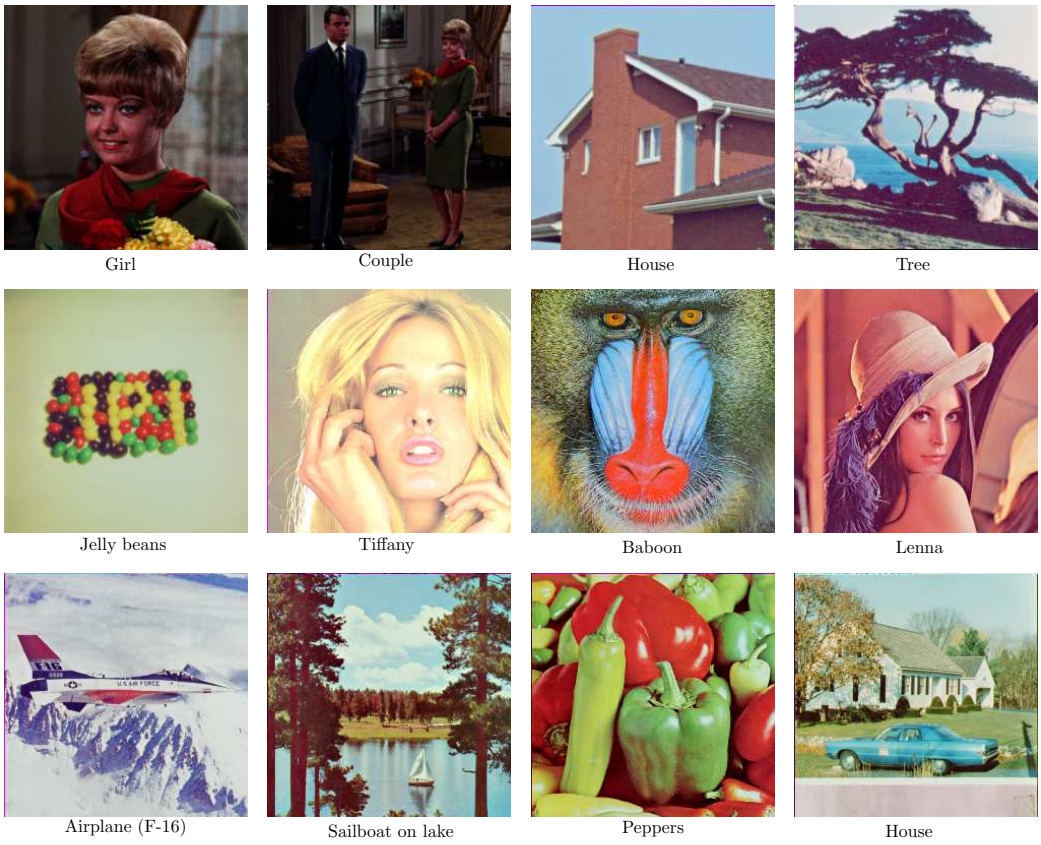


FIGURE 5.6 – Les images couleurs décryptées.

5.6.1 Espace de clés

Dans l'algorithme de chiffrement d'image proposé, la clé secrète comprend :

1. Les paramètres de contrôle p_1, p_2, p_3
2. Les valeurs d'initialisation x_1, x_2, x_3

Pour la carte chaotique PWLCM, la sensibilité des paramètres de contrôle et des valeurs d'initialisation est considérée 10 ^{16} [133]. Par conséquent, l'espace de chaque valeur d'initialisation est de 10^{16}. Tandis que les paramètres de contrôle p_1, p_2, p_3 sont dans l'intervalle (0, 0,5), alors l'espace de clés pour chacun est $0,5 \times 10^{16}$. Ainsi, l'espace de clés du schéma proposé est $0,125 \times 10^{96}$. Il est assez grand pour assurer la résistance du schéma contre les attaques par force brute.

5.6.2 L'analyse statistique

La corrélation entre les pixels adjacents

Le tableau 5.1 résume les résultats de corrélations obtenus en utilisant le schéma proposé et démontre que le schéma proposé supprime avec succès la corrélation entre des pixels adjacents.

Direction	Image claire			Image chiffrée		
	R	G	B	R	G	B
Horizontale	0.9680	0.9441	0.9179	0.0054	0.0027	0.0096
Verticale	0.9516	0.9204	0.8955	0.0013	0.0104	0.0003
Diagonale	0.9087	0.8729	0.8513	0.0027	0.0003	0.0047

TABLE 5.1 – L'analyse de la corrélation entre les pixels adjacents en utilisant l'image claire Lena.

En outre, les coefficients de corrélation de l'image originale et l'image cryptée ont été étudiés et des comparaisons avec les schémas existants ont été effectuées. Les résultats des analyses expérimentales sont présentés dans le tableau 5.2.

Algorithme	Image originale			Image chiffrée		
	Horizontale	Verticale	Diagonale	Horizontale	Verticale	Diagonale
Proposé	0.9715	0.9478	0.9346	0.0007	0.0013	0.000001
Ref.[134]	0.9764	0.9546	0.9263	0.0098	0.0050	0.0013
Ref.[135]	0.9271	0.9230	0.9847	0.0058	0.0026	0.0024
Ref.[136]	0.9271	0.9230	0.9847	0.0580	0.0024	0.0170

TABLE 5.2 – L'analyse de corrélation entre l'image claire et l'image chiffrée.

Le résultat souligne que le coefficient de corrélations des pixels de l'image claire est proche de 1, tandis que celui de l'image cryptée est proche de 0 d'une part. D'une autre part, la comparaison avec les algorithmes de chiffrement d'images recemment proposés montre que le schéma proposé est le meilleur.

5.6.3 Analyse de l'histogramme

Nous pouvons voir dans la figure 5.7 que l'histogramme des trois images chiffrées est assez uniforme et un adversaire ne peut extraire aucune information en utilisant l'attaque par l'analyse de l'histogramme.

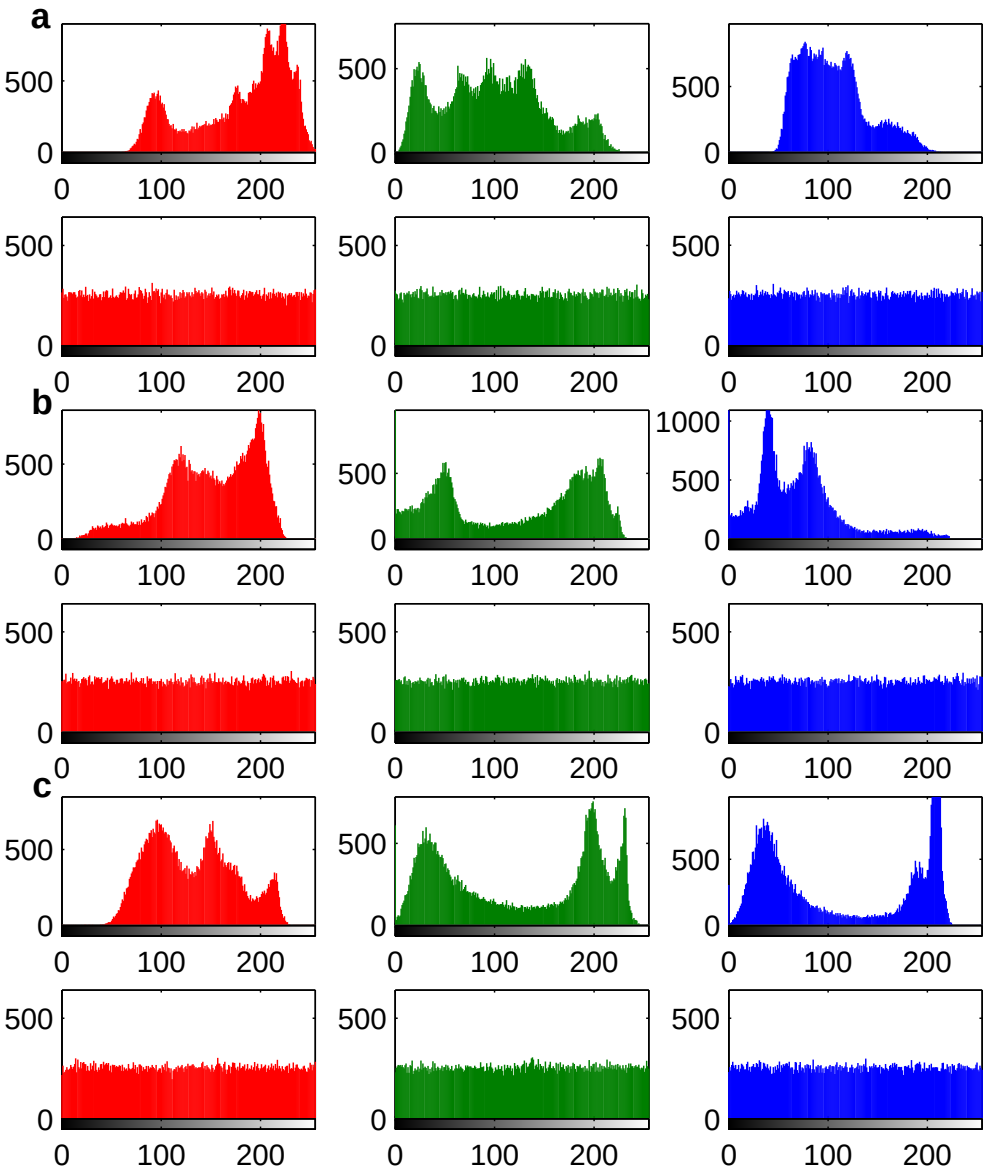


FIGURE 5.7 – Histogrammes des images claires/chiffrées : (a)Lena, (b)Pepper et (c) Boat.

5.6.4 Analyse de la sensibilité

Sensibilité de clés

Pour estimer la sensibilité de la clé secrète de l'algorithme proposé deux clés sont utilisées dans le test. La première clé est la clé d'origine tandis que nous avons fait une modification de 10^{-16} dans un seul paramètre de la clé et nous laissons les cinqs autres paramètres sans modification. Puis, les deux clés légèrement différentes sont utilisées pour chiffrer l'image Lena.

Les deux images chiffrées sont comparées. Les résultats sont récapitulés dans le tableau 5.3 montrant la sensibilité élevée de la clé du schéma proposé. En outre, si une petite modification est effectuée sur la clé, puis la clé modifiée est utilisée pour décrypter l'image chiffrée, le décryptage échoue totalement. La figure 5.8 illustre le résultat de ce test.

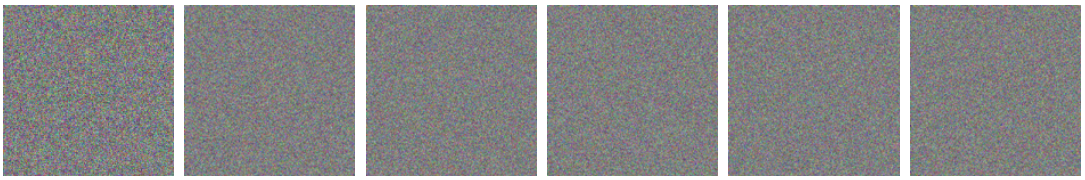
Paramétre Modifié	NPCR %			UACI %		
	R	G	B	R	G	B
p_1	99.5918	99.6235	99.6044	33.4980	33.4622	33.5187
p_2	99.6326	99.5975	99.6227	33.4481	33.4973	33.4648
p_3	99.6109	99.6349	99.6162	33.4513	33.5476	33.4739
x_1	99.6243	99.6033	99.6204	33.4405	33.4446	33.4838
x_2	99.6082	99.6254	99.5922	33.4800	33.4686	33.5027
x_3	99.6204	99.6120	99.6140	33.5223	33.5197	33.4917

TABLE 5.3 – Sensibilité de la clé en utilisant les différents paramètres.

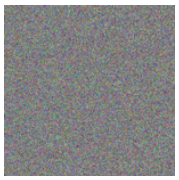
Sensibilité du l'ajustement

En revanche, la sensibilité de l'ajustement a été étudiée dans cette section afin d'assurer la variabilité du schéma proposé. Pour évaluer la sensibilité de l'ajustement seul le dernier bit significatif de l'un des deux ajustements a été modifié. Les deux images cryptées en utilisant la même clé secrète et un ajustement légèrement différent ont été comparés.

Le tableau 5.4 montre l'évaluation de la sensibilité du ajustement du schéma proposé. Ainsi, le schéma proposé est très sensible à l'altération de l'ajustement.

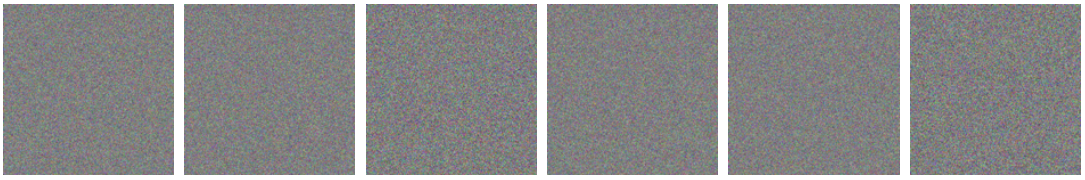


(a) $x'_1 = x_1 + 10^{-16}$ **(b)** $x'_2 = x_2 + 10^{-16}$ **(c)** $x'_3 = x_3 + 10^{-16}$ **(d)** $p'_1 = p_1 + 10^{-16}$ **(e)** $p'_2 = p_2 + 10^{-16}$ **(f)** $p'_3 = p_3 + 10^{-16}$



(g)

(h): (g) - (a) **(i):** (g) - (b) **(j):** (g) - (c) **(k):** (g) - (d) **(l):** (g) - (e) **(m):** (g) - (f)



(n) $x'_1 = x_1 + 10^{-16}$ **(o)** $x'_2 = x_2 + 10^{-16}$ **(p)** $x'_3 = x_3 + 10^{-16}$ **(q)** $p'_1 = p_1 + 10^{-16}$ **(r)** $p'_2 = p_2 + 10^{-16}$ **(s)** $p'_3 = p_3 + 10^{-16}$

FIGURE 5.8 – Analyses de la sensibilité de la clé. 1ère ligne : L'image Lenna, 2ème ligne : Images cryptées en utilisant la clé secrète modifiée avec seulement 10^{-16} dans un seul paramètre à la fois, 3ème ligne : Image cryptée en utilisant la clé secrète d'origine, 4ème ligne : Les différences, 5ème ligne : Image décryptée en utilisant la clé secrète d'origine, 6ème ligne : Images décryptées en utilisant une clé secrète modifiée.

Ajustement modifié	NPCR %			UACI %		
	R	G	B	R	G	B
T_1	99.5865	99.6170	99.6231	33.6509	33.5369	33.4196
T_2	99.6201	99.6094	99.5941	33.4452	33.5396	33.4855

TABLE 5.4 – Analyse de la sensibilité de l'ajustement en utilisant l'image originale Lena.

Sensibilité de l'image chiffrée à l'image originale

Seulement le plus faible bit d'un seul pixel choisi au hasard de l'image originale est modifié. Les deux mesures NPCR et UACI ont été calculées en utilisant différentes images.

Le test est effectué 50 fois. Les résultats de l'expérience sont présentés dans le tableau 5.5. En outre, des comparaisons avec les systèmes de cryptage d'image couleur existants ont été effectuées montrant que le schéma proposé offre des performances très fougueuses.

Algorithme	NPCR %			UACI %		
	R	G	B	R	G	B
Proposé	99.9281	99.8346	99.6896	33.5821	33.6687	33.5408
Ref.[134]	99.6124	99.6134	99.6192	33.4438	33.5232	33.5010
Ref.[137]	99.6231	99.6338	99.6170	33.4747	33.5683	33.3382
Ref.[138]	99.6755	99.6622	99.6619	33.4216	33.4211	33.4308
Ref.[139]	99.63	99.60	99.61	33.31	33.34	33.43
Ref.[8]	99.5643	99.6258	99.6285	35.4560	33.2199	33.0184

TABLE 5.5 – Sensibilité de l'image originale de notre schéma.

5.6.5 Propriétés aléatoire de l'image cryptée

Suite de tests NIST SP 800-22

Trois images chiffrées de taille 512×512 ont été utilisées dans ce test. Les détails des résultats de la simulation sont décrits dans le tableau 5.6 montrant que toutes les images cryptées passent tous les tests du NIST. Ainsi, les images cryptées en utilisant le schéma proposé ont de bonnes propriétés de caractère aléatoire.

TABLE 5.6: Résultats de la suite de tests NIST 800-22 en utilisant les images cryptées.

Test	**Paramètre**	**image testée**		
		Lena	Pepper	Boat
Frequency		0.753521	0.098943	0.157950
Block Frequency	m = 128	0.322226	0.493783	0.427333
Cumulative-sums	Forward	0.675485	0.093845	0.099758
	Reverse	0.855466	0.077657	0.102114
Runs		0.193635	0.704893	0.225509
Longest-runs		0.825319	0.635556	0.347930
Rank		0.188150	0.785979	0.093579
FFT		0.354010	0.093089	0.797221
Non-overlapping-templates		0.014082	0.948289	0.704478
Overlapping-templates		0.788155	0.950197	0.246692
Universal		0.232503	0.980860	0.905970
Approximate entropy		0.098851	0.001366	0.492156
Random-excursions	x = -4	0.046411	0.439047	0.290255
	x = -3	0.759126	0.870684	0.358732
	x = -2	0.846077	0.726333	0.321719
	x = -1	0.847058	0.439047	0.814918
	x = 1	0.501239	0.545809	0.744872
	x = 2	0.283535	0.293765	0.083727
	x = 3	0.039720	0.127314	0.019437
	x = 4	0.117157	0.359108	0.745323
Random-excursions variant	x = -9	0.468272	0.089344	0.934566
	x = -8	0.375099	0.176192	0.670038
	x = -7	0.319598	0.228656	0.694207
	x = -6	0.225720	0.153860	0.964383
	x = -5	0.212286	0.181202	0.887832
	x = -4	0.214821	0.267526	0.872933
	x = -3	0.170167	0.384216	0.570234
	x = -2	0.361785	0.368817	0.642523
	x = -1	0.634497	0.436398	0.949391
	x = 1	0.276227	0.675158	0.397392
	x = 2	0.156585	0.446997	0.769398
	x = 3	0.045959	0.059084	0.939662
	x = 4	0.054306	0.048993	0.410134

Statistical test	Paramètre	Lena	Pepper	Boat
	x = 5	0.080417	0.021736	0.241720
	x = 6	0.142711	0.030998	0.385634
	x = 7	0.266945	0.139461	0.642957
	x = 8	0.375099	0.129803	0.934693
	x = 9	0.482070	0.113489	0.849418
Serial		0.146951	0.531820	0.096066
		0.183719	0.755228	0.260585
Linear-complexity		0.649625	0.038249	0.034130

Suite de tests Diehard

Plus de 20 images chiffrées sont utilisées dans ce test, et les résultats sont rapportés dans le tableau 5.7. Les résultats obtenus montrent que les sorties du système cryptographique passent tous les tests statistiques fournies par Diehard, et ceci signifie que les images chiffrés ne peuvent pas être distingués des séquences aléatoires uniformes.

Nom du test		P-value	Resultat
BIRTHDAY SPACINGS		0.298032	Pass
OVERLAPPING 5-PERMUTATION		0.328022	Pass
BINARY RANK TEST	31×31	0.810286	Pass
	32×32	0.716763	Pass
	6×8	0.953168	Pass
Monkey	20 bits per word	0.52112	Pass
COUNT-THE-1's	stream	0.619800	Pass
	specific	0.895149	Pass
PARKING LOT		0.145885	Pass
3DSPHERES		0.178039	Pass
SQEEZE		0.571284	Pass
OVERLAPPING SUMS		0.660804	Pass
RUNS		0.771397	Pass
CRAPS	no. of wins	0.917979	Pass
	throws/game	0.872965	Pass

TABLE 5.7 – Les résultats obtenus en utilisant la suite de tests Diehard

5.6.6 Analyse de l'entropie

Le tableau 5.8 illustre que la valeur de l'entropie de l'image chiffrée en utilisant la méthode proposée est très proche de 8 pour les trois canaux de couleur et le schéma proposé peut surmonter avec succès l'analyse de l'entropie.

image chiffrée	Composants		
	R	G	B
Lena	7.9968	7.9973	7.9972
Pepper	7.9971	7.9973	7.9974
Boat	7.9974	7.9973	7.9974

TABLE 5.8 – Les résultats de l'analyse de l'entropie.

5.6.7 L'attaque texte clair choisi

Dans le schéma proposé le cryptage d'un pixel dépend de tous les autres pixels, en plus un ajustement choisi au hasard est utilisé pour chaque chiffrement. En outre, si un adversaire tente de chiffrer une image ordinaire deux fois il obtiendra deux images chiffrées différentes et le schéma proposé est probabiliste. De plus, le schéma proposé présente un mode de cryptage chinage-ajusté et une preuve complète de la sécurité de ce mode contre l'analyse texte clair choisi est présentée dans la référence [131].

5.7 Conclusion

En prenant la sécurité comme objectif, nous avons proposé un nouveau cryptosystème pour le chiffrement d'images numériques couleurs. Dans notre proposition, nous sommes basés sur un mode de cryptage sûr contre l'attaque texte clair choisi pour désigner notre schéma. Notre approche est basée sur l'architecture confusion/diffusion en utilisant la carte chaotique non linéaire PWLCM. La carte chaotique PWLCM possède des propriétés dynamiques parfaites. Ainsi, nous l'avons utilisé pour générer des séquences pseudo-aléatoires durant tout le processus de cryptage. Des performances de sécurité satisfaisantes sont atteintes en un seul tour de chiffrement. L'efficacité du chiffre proposé contre les différentes attaques est améliorée en le comparant aux schémas de chiffrement d'image en couleur existants. Les résultats de simulation obtenus confirment l'efficacité et la sécurité de notre schéma en utilisant les différentes mesures de sécurité.

Conclusion générale

Le réseau Internet ne cesse pas de se développer étonnamment vite. Plusieurs services ont été numérisés et les entités n'ont plus besoin de se déplacer afin d'acquérir leurs besoins. Cependant, les interlocuteurs sont très préoccupés par la sécurité de leurs informations transmises ou stockées sur des réseaux non sûrs. La confidentialité des services électroniques est très importante, voire, elle est une exigence non négociable pour la réussite de ces services. La confidentialité peut être mise en place grâce à des méthodes de chiffrement qui transforment les données intelligibles à un format inintelligible. Bien sûr il existe plusieurs différences entre les données textuelles et les images numériques, ce qui ne permet pas d'appliquer les mêmes mécanismes de chiffrement. Au cours des dernières années, cela a attiré une attention croissante des recherches et plusieurs techniques ont été utilisées. Mais, plusieurs cryptosystèmes souffrent d'un ou plusieurs problèmes.

Subséquemment. Dans cette thèse nous avons proposé deux schémas de chiffrement d'image en basant sur deux techniques différentes. Le premier schéma consiste en un algorithme de cryptage d'image sans perte, basé sur une approche algébrique dans l'anneau Z_{256} en utilisant des transformations matricielles et le OU exclusif. L'objectif principal du système de cryptage d'image sans perte proposé est d'avoir un niveau élevé de confusion en utilisant une forte relation entre l'image-chiffrée et la clé secrète, et ainsi empêcher la possibilité de reconstruire l'image claire sans la connaissance de la clé. La clé utilisée dans cet algorithme est un vecteur d'entiers qui dépend de la taille de l'image. L'analyse de l'espace de clés montre qu'il est suffisamment grand, ce qui rend une attaque force brute infaisable. Une comparaison avec les cryptosystèmes qui existent y compris l'algorithme AES montre la supériorité de notre approche.

Notre deuxième contribution consiste à développer un algorithme de chiffrement d'image en couleur basé sur l'utilisation d'une carte chaotique. Dans cette contribution, nous avons introduit un schéma ajustable-flexible de cryptage d'image couleur basé sur l'architecture confusion/diffusion en utilisant la carte chaotique non linéaire

PWLCM pour générer des séquences pseudo-aléatoires durant le processus de cryptage. Avec l'ajout de l'ajustement, une image claire est chiffrée à différentes images chiffrées en utilisant la même clé secrète. Des performances satisfaisantes de sécurité ont été atteintes en un round de chiffrement et l'efficacité est beaucoup améliorée. Les comparaisons avec les schémas de chiffrement d'image couleur existants qui ont été réalisées montrent que l'algorithme proposé offre des performances très favorables.

Bien que les contributions proposées soient assez efficaces, les solutions obtenues ne sont pas optimales. Cependant, Il existe plusieurs points qui peuvent être améliorés. Par exemple, l'utilisation de la notion de parallélisme, dont le but est de traiter les images d'une manière simultanée, va permettre d'optimiser le temps d'exécution des deux propositions.

D'un autre côté, les ressources informatiques restent des fois limitées face à une quantité énorme d'informations à stocker ou à transférer. Dans l'objectif d'optimisation du temps de transmission de chaque image ainsi que de son espace de stockage, une approche de compression d'image doit être combinée avec les schémas de cryptages proposés.

Bibliographie

[1] La couleur des corps. `http://lab.phys.free.fr/site/laboratoire/articles.php?lng=fr&pg=88`.

[2] Ronald L Rivest, Adi Shamir, and Len Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2) :120–126, 1978.

[3] PUB FIPS. 46-3 : Data encryption standard (des). *National Institute of Standards and Technology*, 25(10) :1–22, 1999.

[4] NIST FIPS Pub. 197 : Advanced encryption standard (aes). *Federal Information Processing Standards Publication*, 197 :441–0311, 2001.

[5] Claude E Shannon. Communication theory of secrecy systems*. *Bell system technical journal*, 28(4) :656–715, 1949.

[6] SS Maniccam and Nikolaos G Bourbakis. Lossless image compression and encryption using scan. *Pattern Recognition*, 34(6) :1229–1245, 2001.

[7] Rong-Jian Chen and Shi-Jinn Horng. Novel scan-ca-based image security system using scan and 2-d von neumann cellular automata. *Signal Processing : Image Communication*, 25(6) :413–426, 2010.

[8] Abdurahman Kadir, Askar Hamdulla, and Wen-Qiang Guo. Color image encryption using skew tent map and hyper chaotic system of 6th-order cnn. *Optik-International Journal for Light and Electron Optics*, 125(5) :1671–1675, 2014.

[9] Yang Tang, Zidong Wang, and Jian-an Fang. Image encryption using chaotic coupled map lattices with time-varying delays. *Communications in Nonlinear Science and Numerical Simulation*, 15(9) :2456–2468, 2010.

[10] Hongjun Liu and Xingyuan Wang. Color image encryption based on one-time keys and robust chaotic maps. *Computers & Mathematics with Applications*, 59(10) :3320–3327, 2010.

[11] Yang Shuangyuan, Lu Zhengding, and Han Shuihua. An asymmetric image encryption based on matrix transformation. In *Communications and Information Technology, 2004. ISCIT 2004. IEEE International Symposium on*, volume 1, pages 66–69. IEEE, 2004.

[12] J Mastan, GA Sathishkumar, and K Bhoopathy Bagan. Digital image security using matrix and non-linear pixel transformation. In *Computer, Communication and Electrical Technology (ICCCET), 2011 International Conference on*, pages 80–85. IEEE, 2011.

[13] Gaurav Bhatnagar, QM Jonathan Wu, and Balasubramanian Raman. Discrete fractional wavelet transform and its application to multiple encryption. *Information Sciences*, 223 :297–316, 2013.

[14] Gaurav Bhatnagar, QM Wu, and Baranidharan Raman. A new fractional random wavelet transform for fingerprint security. *Systems, Man and Cybernetics, Part A : Systems and Humans, IEEE Transactions on*, 42(1) :262–275, 2012.

[15] Rasul Enayatifar, Abdul Hanan Abdullah, and Ismail Fauzi Isnin. Chaos-based image encryption using a hybrid genetic algorithm and a dna sequence. *Optics and Lasers in Engineering*, 56 :83–93, 2014.

[16] Qiang Zhang, Ling Guo, and Xiaopeng Wei. A novel image fusion encryption algorithm based on dna sequence operation and hyper-chaotic system. *Optik-International Journal for Light and Electron Optics*, 124(18) :3596–3600, 2013.

[17] David Arroyo, Chengqing Li, Shujun Li, Gonzalo Alvarez, and Wolfgang A Halang. Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm. *Chaos, Solitons & Fractals*, 41(5) :2613–2616, 2009.

[18] Xingyuan Wang, Dapeng Luan, and Xuemei Bao. Cryptanalysis of an image encryption algorithm using chebyshev generator. *Digital Signal Processing*, 25 :244–247, 2014.

[19] Chengqing Li, Shujun Li, Muhammad Asim, Juana Nunez, Gonzalo Alvarez, and Guanrong Chen. On the security defects of an image encryption scheme. *Image and Vision Computing*, 27(9) :1371–1381, 2009.

[20] Chengqing Li, Shujun Li, Gonzalo Alvarez, Guanrong Chen, and Kwok-Tung Lo. Cryptanalysis of a chaotic block cipher with external key and its improved version. *Chaos, Solitons & Fractals*, 37(1) :299–307, 2008.

[21] Yong Wang, Peng Lei, Huaqian Yang, and Huiying Cao. Security analysis on a color image encryption based on dna encoding and chaos map. *Computers & Electrical Engineering*, 2015.

[22] Shujun Li and Xuan Zheng. Cryptanalysis of a chaotic image encryption method. In *Circuits and Systems, 2002. ISCAS 2002. IEEE International Symposium on*, volume 2, pages II–708. IEEE, 2002.

[23] Wenqi He, Xiang Peng, and Xiangfeng Meng. A hybrid strategy for cryptanalysis of optical encryption based on double-random phase–amplitude encoding. *Optics & Laser Technology*, 44(5) :1203–1206, 2012.

[24] Meihua Liao, Wenqi He, Xiang Peng, Xiaoli Liu, and Xiangfeng Meng. Cryptanalysis of optical encryption with a reference wave in a joint transform correlator architecture. *Optics & Laser Technology*, 45 :763–767, 2013.

[25] Yuansheng Liu, Jie Tang, and Tao Xie. Cryptanalyzing a rgb image encryption algorithm based on dna encoding and chaos map. *Optics & Laser Technology*, 60 :111–115, 2014.

[26] Yong Zhang. Cryptanalysis of a novel image fusion encryption algorithm based on dna sequence operation and hyper-chaotic system. *Optik-International Journal for Light and Electron Optics*, 126(2) :223–229, 2015.

[27] Chengqing Li, Yuansheng Liu, Leo Yu Zhang, and Kwok-Wo Wong. Cryptanalyzing a class of image encryption schemes based on chinese remainder theorem. *Signal Processing : Image Communication*, 29(8) :914–920, 2014.

[28] Ivan Matveevich Vinogradov. *Elements of number theory*. Courier Corporation, 2003.

[29] John Stillwell. Mathematics and its history. *The Australian Mathem. Soc*, page 168, 2002.

[30] Stallings William and William Stallings. *Cryptography and Network Security, 4/E*. Pearson Education India, 2006.

[31] Christof Paar and Jan Pelzl. *Understanding cryptography : a textbook for students and practitioners*. Springer Science & Business Media, 2009.

[32] Paul Moritz Cohn. *Basic algebra*. Springer Science & Business Media, 2003.

[33] Clive Reis. *Abstract algebra : an introduction to groups, rings and fields*. World Scientific, 2011.

[34] Louis Rowen. Algebra : groups, rings, and fields. *AMC*, 10 :12, 1994.

[35] Dennis S Bernstein. *Matrix mathematics : theory, facts, and formulas*. Princeton University Press, 2009.

[36] Renzo Cairoli. *Algèbre linéaire*. PPUR presses polytechniques, 1991.

[37] unisciel. Multiplication dúne matrice par un scalaire. `http://uel.unisciel.fr/physique/outils_nancy/outils_nancy_ch11/co/apprendre_ch11_11.html`.

[38] Gene H Golub and Charles F Van Loan. *Matrix computations*, volume 3. JHU Press, 2012.

[39] Roger A Horn and Charles R Johnson. *Matrix analysis*. Cambridge university press, 2012.

[40] Simon Singh. *Histoire des codes secrets : de l'Égypte des pharaons à l'ordinateur quantique*. JC Lattès, 1999.

[41] Fred Cohen et al. A short history of cryptography. *Fred Cohen & Associates*, 2001.

[42] Lance Bryant and JoAnn Ward. Caesar ciphers : An introduction to cryptography. *Purdue University, Portugal*, 2007.

[43] Claude Elwood Shannon. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1) :3–55, 2001.

[44] Oded Goldreich. *Foundations of cryptography : volume 2, basic applications*. Cambridge university press, 2004.

[45] Auguste Kerckhoffs. *La cryptographie militaire*. University Microfilms, 1978.

[46] Fabien Petitcolas. La cryptographie militaire., 1883.

[47] Bruce Schneier. *Applied cryptography : protocols, algorithms, and source code in C*. john wiley & sons, 2007.

[48] Whitfield Diffie and Martin E Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6) :644–654, 1976.

[49] Michael O Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical report, DTIC Document, 1979.

[50] Robert J McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN progress report*, 42(44) :114–116, 1978.

[51] Ralph C Merkle and Martin E Hellman. Hiding information and signatures in trapdoor knapsacks. *Information Theory, IEEE Transactions on*, 24(5) :525–530, 1978.

[52] Shmuel Peleg and Azriel Rosenfeld. Breaking substitution ciphers using a relaxation algorithm. *Communications of the ACM*, 22(11) :598–605, 1979.

[53] Behrouz A Forouzan. *Cryptography & Network Security*. McGraw-Hill, Inc., 2007.

[54] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography*. CRC Press, 2014.

[55] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 1996.

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

[57] André Roy. *Dictionnaire général du cinéma : du cinématographe à Internet : art, technique, industrie*. Les Editions Fides, 2007.

[58] Ashley Walker Erik Wolfart Robert Fisher, Simon Perkins. A to z of image processing concepts. `http://homepages.inf.ed.ac.uk/rbf/HIPR2/glossary`.

[59] Dan S Bloomberg. Color quantization using octrees, 2008.

[60] Michael T Orchard, Charles Bouman, et al. Color quantization of images. *Signal Processing, IEEE Transactions on*, 39(12) :2677–2690, 1991.

[61] Michael Gervautz and Werner Purgathofer. A simple method for color quantization : Octree quantization. In *New trends in computer graphics*, pages 219–231. Springer, 1988.

[62] Erik Dahlman, Claude Oestges, Alan C Bovik, Bruce A Fette, Keith Jack, Farid Dowla, Stefan Parkvall, Johan Skold, Casimer DeCusatis, Ed da Silva, et al. *Communications engineering desk reference*. Academic Press, 2009.

[63] colorizer. `http://colorizer.org/`.

[64] Randy Crane. *Simplified approach to image processing : classical and modern techniques in C*. Prentice Hall PTR, 1996.

[65] Andreas Koschan and Mongi Abidi. *Digital color image processing*. John Wiley & Sons, 2008.

[66] Wayne Fulton. A few scanning tips. http://www.scantips.com/basics09.

[67] Wikipedia. Image file formats. https://en.wikipedia.org/wiki/Image_file_formats.

[68] Ashley Walker Erik Wolfart Robert Fisher, Simon Perkins. Image processing learning resources explore with java. http://homepages.inf.ed.ac.uk/rbf/HIPR2/hipr_top.

[69] Diane Lingrand. Introduction au traitement d'images. 2008.

[70] wikipedia. Entropie de shannon. https://fr.wikipedia.org/wiki/Entropie_de_Shannon.

[71] Yue Wu, Joseph P Noonan, and Sos Agaian. Npcr and uaci randomness tests for image encryption. *Cyber journals : multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, pages 31–38, 2011.

[72] Narendra K Pareek, Vinod Patidar, and Krishan K Sud. Image encryption using chaotic logistic map. *Image and Vision Computing*, 24(9) :926–934, 2006.

[73] NIST. Nist 800-22 tests. http://csrc.nist.gov/groups/ST/toolkit/random_number.

[74] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, DTIC Document, 2001.

[75] James Bellamy. Randomness of d sequences via diehard testing. *arXiv preprint arXiv :1312.3618*, 2013.

[76] Juan Soto. Statistical testing of random number generators. In *Proceedings of the 22nd National Information Systems Security Conference*, volume 10, page 12. NIST Gaithersburg, MD, 1999.

[77] Wikipedia. Diehard tests. https://en.wikipedia.org/wiki/Diehard_tests#cite_note-1.

[78] N Bourbakis. A language for sequential access of two dimensional array elements. In *IEEE Workshop on LFA, Singapore*, pages 52–58, 1986.

[79] Chao-Shen Chen and Rong-Jian Chen. Image encryption and decryption using scan methodology. In *Parallel and Distributed Computing, Applications and*

Technologies, 2006. PDCAT'06. Seventh International Conference on, pages 61–66. IEEE, 2006.

[80] Suchindran S Maniccam and Nikolaos G Bourbakis. Image and video encryption using scan patterns. *Pattern Recognition*, 37(4) :725–737, 2004.

[81] Edward Lorenz. *Predictability : does the flap of a butterfly's wing in Brazil set off a tornado in Texas ?* na, 1972.

[82] Michal Fečkan. *Bifurcation and chaos in discontinuous and continuous systems*. Springer Science & Business Media, 2011.

[83] Saber N Elaydi. *Discrete Chaos : With Applications in Science and Engineering*. CRC Press, 2007.

[84] Goce Jakimoski, Ljupco Kocarev, et al. Chaos and cryptography : block encryption ciphers based on chaotic maps. *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 48(2) :163–169, 2001.

[85] Guosheng Gu and Jie Ling. A fast image encryption method by using chaotic 3d cat maps. *Optik-International Journal for Light and Electron Optics*, 125(17) :4700–4705, 2014.

[86] Tiegang Gao and Zengqiang Chen. A new image encryption algorithm based on hyper-chaos. *Physics Letters A*, 372(4) :394–400, 2008.

[87] Guanrong Chen, Yaobin Mao, and Charles K Chui. A symmetric image encryption scheme based on 3d chaotic cat maps. *Chaos, Solitons & Fractals*, 21(3) :749–761, 2004.

[88] G Chen and X Dong. From chaos to order : methodologies, perspectives and applications, 1998, 1999.

[89] Sahar Mazloom and Amir Masud Eftekhari-Moghadam. Color image encryption based on coupled nonlinear chaotic map. *Chaos, Solitons & Fractals*, 42(3) :1745–1754, 2009.

[90] Rhouma Rhouma, Soumaya Meherzi, and Safya Belghith. Ocml-based colour image encryption. *Chaos, Solitons & Fractals*, 40(1) :309–318, 2009.

[91] Stephane G Mallat. A theory for multiresolution signal decomposition : the wavelet representation. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 11(7) :674–693, 1989.

[92] Linfei Chen and Daomu Zhao. Optical image encryption based on fractional wavelet transform. *Optics Communications*, 254(4) :361–367, 2005.

[93] Bibhudendra Acharya, Sarat Kumar Patra, and Ganapati Panda. Image encryption by novel cryptosystem using matrix transformation. In *Emerging Trends in Engineering and Technology, 2008. ICETET'08. First International Conference on*, pages 77–81. IEEE, 2008.

[94] Fangchao Wang, Sen Bai, Guibin Zhu, and Zhenghui Song. An image encryption algorithm based on n-dimension affine transformation. In *Computer and Information Science, 2009. ICIS 2009. Eighth IEEE/ACIS International Conference on*, pages 579–585. IEEE, 2009.

[95] Isha Mehra and Naveen K Nishchal. Optical asymmetric image encryption using gyrator wavelet transform. *Optics Communications*, 354 :344–352, 2015.

[96] Wen Chen and Xudong Chen. Optical color image encryption based on an asymmetric cryptosystem in the fresnel domain. *Optics Communications*, 284(16) :3913–3917, 2011.

[97] Shutian Liu, Quanlin Mi, and Banghe Zhu. Optical image encryption with multistage and multichannel fractional fourier-domain filtering. *Optics Letters*, 26(16) :1242–1244, 2001.

[98] G Unnikrishnan, J Joseph, and Kehar Singh. Optical encryption by double-random phase encoding in the fractional fourier domain. *Optics Letters*, 25(12) :887–889, 2000.

[99] Pramod Kumar, Joby Joseph, and Kehar Singh. Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator. *Applied optics*, 50(13) :1805–1811, 2011.

[100] Xiaopeng Deng. Optical image encryption based on real-valued coding and subtracting with the help of qr code. *Optics Communications*, 349 :48–53, 2015.

[101] Xiangling Ding and Guangyi Chen. Optical color image encryption using position multiplexing technique based on phase truncation operation. *Optics & Laser Technology*, 57 :110–118, 2014.

[102] Yicong Zhou, Karen Panetta, Sos Agaian, and CL Philip Chen. Image encryption using p-fibonacci transform and decomposition. *Optics Communications*, 285(5) :594–608, 2012.

[103] Yicong Zhou, Sos Agaian, Valencia M Joyner, and Karen Panetta. Two fibonacci p-code based image scrambling algorithms. In *Electronic Imaging 2008*, pages 681215–681215. International Society for Optics and Photonics, 2008.

[104] Xiao-Wei Li, Sung-Jin Cho, In-Kwon Lee, and Seok-Tae Kim. Three-dimensional image security system combines the use of smart mapping algorithm and fibonacci transformation technique. *Journal of applied research and technology*, 12(6) :1092–1102, 2014.

[105] Qiang Zhang and Xiaopeng Wei. A novel couple images encryption algorithm based on dna subsequence operation and chaotic system. *Optik-International Journal for Light and Electron Optics*, 124(23) :6276–6281, 2013.

[106] Noorul Hussain UbaidurRahman, Chithralekha Balamurugan, and Rajapandian Mariappan. A novel dna computing based encryption and decryption algorithm. *Procedia Computer Science*, 46 :463–475, 2015.

[107] Qiang Zhang, Ling Guo, and Xiaopeng Wei. Image encryption using dna addition combining with chaotic maps. *Mathematical and Computer Modelling*, 52(11) :2028–2035, 2010.

[108] Olu Lafe. Data compression and encryption using cellular automata transforms. In *Intelligence and Systems, 1996., IEEE International Joint Symposia on*, pages 234–241. IEEE, 1996.

[109] Rong-Jian Chen and Jui-Lin Lai. Image security system using recursive cellular automata substitution. *Pattern Recognition*, 40(5) :1621–1631, 2007.

[110] Xiao Wei Li, Sung Jin Cho, and Seok Tae Kim. A 3d image encryption technique using computer-generated integral imaging and cellular automata transform. *Optik-International Journal for Light and Electron Optics*, 125(13) :2983–2990, 2014.

[111] Faraoun Kamel Mohamed. A parallel block-based encryption schema for digital images using reversible cellular automata. *Engineering Science and Technology, an International Journal*, 17(2) :85–94, 2014.

[112] Narendra Singh and Aloka Sinha. Optical image encryption using fractional fourier transform and chaos. *Optics and Lasers in Engineering*, 46(2) :117–123, 2008.

[113] Dezhao Kong and Xueju Shen. Multiple-image encryption based on optical wavelet transform and multichannel fractional fourier transform. *Optics & Laser Technology*, 57 :343–349, 2014.

[114] Liansheng Sui, Kuaikuai Duan, Junli Liang, Zhiqiang Zhang, and Haining Meng. Asymmetric multiple-image encryption based on coupled logistic maps in fractional fourier transform domain. *Optics and Lasers in Engineering*, 62 :139–152, 2014.

[115] CK Huang, Chin-Wen Liao, SL Hsu, and YC Jeng. Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system. *Telecommunication Systems*, 52(2) :563–571, 2013.

[116] Qing Zhou and Xiaofeng Liao. Collision-based flexible image encryption algorithm. *Journal of Systems and Software*, 85(2) :400–407, 2012.

[117] S Behnia, A Akhshani, H Mahmodi, and A Akhavan. A novel algorithm for image encryption based on mixture of chaotic maps. *Chaos, Solitons & Fractals*, 35(2) :408–419, 2008.

[118] A Akhshani, S Behnia, A Akhavan, H Abu Hassan, and Z Hassan. A novel scheme for image encryption based on 2d piecewise chaotic maps. *Optics Communications*, 283(17) :3259–3266, 2010.

[119] Xiaojun Tong, Minggen Cui, and Zhu Wang. A new feedback image encryption scheme based on perturbation with dynamical compound chaotic sequence cipher generator. *Optics Communications*, 282(14) :2722–2728, 2009.

[120] Xing-yuan Wang, Feng Chen, and Tian Wang. A new compound mode of confusion and diffusion for block encryption of image based on chaos. *Communications in Nonlinear Science and Numerical Simulation*, 15(9) :2479–2485, 2010.

[121] A Kanso and M Ghebleh. An efficient and robust image encryption scheme for medical applications. *Communications in Nonlinear Science and Numerical Simulation*, 2015.

[122] JB Lima, F Madeiro, and FJR Sales. Encryption of medical images based on the cosine number transform. *Signal Processing : Image Communication*, 35 :1–8, 2015.

[123] Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic, and Ch Roux. An a priori and a posteriori protection by means of data hiding of encrypted images : application to ultrasound images. In *The International Conference on Health Informatics*, pages 220–223. Springer, 2014.

[124] Abdul Hanan Abdullah, Rasul Enayatifar, and Malrey Lee. A hybrid genetic algorithm and chaotic function model for image encryption. *AEU-International Journal of Electronics and Communications*, 66(10) :806–816, 2012.

[125] Vinod Patidar, NK Pareek, G Purohit, and KK Sud. A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. *Optics communications*, 284(19) :4331–4339, 2011.

[126] Ljupco Kocarev, Goce Jakimoski, Toni Stojanovski, and Ulrich Parlitz. From chaotic maps to encryption schemes. In *Circuits and Systems, 1998. ISCAS'98. Proceedings of the 1998 IEEE International Symposium on*, volume 4, pages 514–517. IEEE, 1998.

[127] G Alvarez, F Montoya, G Pastor, and M Romera. Chaotic cryptosystems. In *Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on*, pages 332–338. IEEE, 1999.

[128] Jiun-In Guo et al. A new chaotic key-based design for image encryption and decryption. In *Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on*, volume 4, pages 49–52. IEEE, 2000.

[129] Hun-Chen Chen, Jiun-In Guo, Lin-Chieh Huang, and Jui-Cheng Yen. Design and realization of a new signal security system for multimedia data transmission. *EURASIP Journal on Applied Signal Processing*, 2003 :1291–1305, 2003.

[130] JS Armand Eyebe Fouda, J Yves Effa, Samrat L Sabat, and Maaruf Ali. A fast chaotic block cipher for image encryption. *Communications in Nonlinear Science and Numerical Simulation*, 19(3) :578–588, 2014.

[131] Moses Liskov, Ronald L Rivest, and David Wagner. Tweakable block ciphers. *Journal of cryptology*, 24(3) :588–613, 2011.

[132] Phillip Rogaway, Mihir Bellare, and John Black. Ocb : A block-cipher mode of operation for efficient authenticated encryption. *ACM Transactions on Information and System Security (TISSEC)*, 6(3) :365–403, 2003.

[133] Hongjun Liu and Xingyuan Wang. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Optics Communications*, 284(16) :3895–3903, 2011.

[134] Xingyuan Wang and Hui-li Zhang. A color image encryption with heterogeneous bit-permutation and correlated chaos. *Optics Communications*, 342 :51–60, 2015.

[135] Chang'e Dong. Color image encryption using one-time keys and coupled chaotic systems. *Signal Processing : Image Communication*, 29(5) :628–640, 2014.

[136] Hongjun Liu, Xingyuan Wang, and Abdurahman Kadir. Color image encryption using choquet fuzzy integral and hyper chaotic system. *Optik-International Journal for Light and Electron Optics*, 124(18) :3527–3533, 2013.

[137] Hongjun Liu and Abdurahman Kadir. Asymmetric color image encryption scheme using 2d discrete-time map. *Signal Processing*, 2015.

[138] Yushu Zhang and Di Xiao. Self-adaptive permutation and combined global diffusion for chaotic color image encryption. *AEU-International Journal of Electronics and Communications*, 68(4) :361–368, 2014.

[139] MA Murillo-Escobar, C Cruz-Hernández, F Abundiz-Pérez, RM López-Gutiérrez, and OR Acosta Del Campo. A rgb image encryption algorithm based on total plain image characteristics and chaos. *Signal Processing*, 109 :119–131, 2015.