REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université de Mohamed El-Bachir El-Ibrahimi-Bordj Bou Arreridj

Faculté des Sciences et de la technologie

Département d'Electronique

Mémoire

Présenté pour obtenir

LE DIPLOME DE MASTER

FILIERE : **ELECRTONIQUE**

SPECIALITE : **ELECTRONIQUE DES SYSTEMES EMBARQUES**

Par

- **KADRI Lounis**
- **ZEGHDOUCHE Yacine**

Intitulé

Etude d'un système de cryptage d'image couleurs basé sur des suites bidimensionnelles et la transformée de Fourier fractionnaire

Soutenu le :

25/06/2024

Devant le Jury composé de :

Nom & Prénom	*Grade*	*Qualité*	*Etablissement*
Rabah HAMDINI	**MCB**	**Président**	**Univ-BBA**
Seif Eddine AZOUG	**MCB**	**Encadrant**	**Univ-BBA**
Fouzia HAMADACHE	**MAA**	**Examinateur**	**Univ-BBA**

Année Universitaire 2023/2024

Abstract :

In this work, we study the encryption of color images that exploits parametric transforms in combination with 2D chaotic maps. We first give an introduction and a general overview about color image encryption, its objectives, and techniques, both symmetric and asymmetric, while introducing the use of parametric transforms and two-dimensional chaotic maps. Then, we focus on image encryption using the Double Random Phase Encoding (DRPE) technique with parametric transforms and 2D chaotic maps. The experimental results of the comparative study evaluate the cryptosystem performances in terms of security, robustness, and efficiency.

Keywords : DRPE, *Fractional* transforms, image encryption, 2D chaotic maps.

Résumé :

Dans ce travail, nous étudions le cryptage des images couleur qui exploite des transformations paramétriques en combinaison avec des suites chaotiques 2D. Nous commençons d'abord avec une introduction et un aperçu général sur le cryptage des images couleur, ses objectifs et les techniques, à la fois symétriques et asymétriques, tout en introduisant l'utilisation de transformations paramétriques et de suites chaotiques bidimensionnelles. Ensuite, nous nous concentrons sur le chiffrement d'image à l'aide de la technique DRPE (Double Random Phase Encoding) avec des transformations paramétriques et des suites chaotiques 2D. Les résultats expérimentaux de l'étude comparative évaluent les performances du cryptosystème en termes de sécurité, de robustesse et d'efficacité.

Mots-clés : Cryptage d'image, DRPE, suites chaotiques 2D, Transformations fractionnelles.

الملخص

في هذا العمل، ندرس تشفير الصور الملونة التي تستعمل التحويلات البارامترية مع المتتاليات العشوائية ثنائية الأبعاد. نقدم أولاً مقدمة ولمحة عامة عن تشفير الصورة الملونة وأهدافها وتقنياتها، سواء كانت متماثلة أو غير متماثلة، مع إدخال استخدام التحويلات البارامترية و المتتاليات العشوائية ثنائية الأبعاد. بعد ذلك، نركز على تشفير الصورة باستخدام تقنية تشفير المرحلة العشوائية المزدوجة(DRPE) مع التحويلات البارامترية والأجنحة الفوضوية ثنائية الأبعاد..

تقوم النتائج التجريبية للدراسة المقارنة بين طريقة DRPE جنبًا إلى جنب مع أجنحة فوضوية مختلفة ثنائية الأبعاد بتقييم أداء نظام التشفير من حيث الأمان والقوة والكفاءة

الكلمات المفتاحية : المتتاليات العشوائية ثنائية ، تحويلات كسرية، تشفير الصورة، DRPE

Remerciements

Avant tout on tient notre remerciement à notre Dieu tout puissant de nous avoir donné la foi, la force et le courage pour achever ce modeste travail

Nous exprimons nos sincères remerciements à notre encadrant Dr. Seif Eddine AZOUG qui a dirigé ce travail par son savoir, sa compétence, ces encouragements, son expérience et sa disponibilité permanente durant la période de ce travail.

Enfin, la même pensée, toutes nos familles et amis pour leur soutien durant nos études de master.

Liste des figures

1.1 Illustration des pixels d'une image numérique binaire 03
1.2 Image binaire (0 ,1) 04
1.3 Nuance de 256 gris /Image codée en niveau de gris 04
1.4 Codage RVB 16bits 05
1.5 La cryptographie symétrique 06
1.6 Cryptographie asymétrique 07
1.7 Cryptage par bloc Vs Cryptage par flot 08
1.8 Cryptage DRPE dans le domaine de la transformée de Fourier 09
2.1 Méthode de cryptage DRPE dans le domaine TFFrD.....12
2.2 Diagramme de bifurcation de la suite logistique 14
2.3 Exemple d'utilisation de suite logistique en cryptage 14
2.4 Algorithme de cryptage.....18
2.5 Algorithme de décryptage 18
3.1 Images de Test RVB simples de taille « 256 × 256 ».....20
3.2 Algorithme de simulation en cryptage. 22
3.3 Algorithme de simulation en décryptage.....23
3.4 Résultats de simulation du cryptage de l'image couleur « Peppers » 24
3.5 Résultats de simulation du cryptage de l'image couleur « Barbara » 25
3.6 Résultats de simulation du cryptage de l'image couleur « Airplane » 25
3.7 Résultats de comparaison de l'analyse histogramme de l'image cryptée « Peppers ».....27
3.8 Résultats de comparaison de l'analyse histogramme de l'image cryptée « Barbara ».....28
3.9 Résultats de comparaison de l'analyse histogramme de l'image cryptée « Airplane ».....29
3.10 Résultats visuels du décryptage de l'image « Peppers » en présence de bruit « AWGN. »…….34
3.11 Résultats visuels du décryptage de l'image « Barbara » en présence de bruit « AWGN. »……..35
3.12 Résultats visuels du décryptage de l'image « Airplane » en présence de bruit « AWGN. »…….35
3.13 Résultats visuels du décryptage de l'image « Barbara » en présence de bruit « Speckle. »……..37
3.14 Résultats visuels du décryptage de l'image « Barbara » en présence de bruit « Speckle. »……..38
3.15 Sensibilité des paramètres chaotiques de la clé de décryptage à une erreur de déviation "δ" …….42
3.16 Comparaison MSE en fonction de l'erreur canal rouge……43
3.17 Comparaison MSE en fonction de l'erreur canal vert……...43
3.18 Comparaison MSE en fonction de l'erreur canal bleu……..44

Liste des tableaux

3.1 Suites chaotiques bidimensionnelles évaluées 21
3.2 Paramètres fractionnaires DFrFT choisis 21
3.3 Résultats de comparaison de l'entropie des composantes RVB des images cryptées. 30
3.4 Résultats de comparaison du coefficient de corrélation des images couleurs cryptées 32
3.5 Résultats de comparaison du PSNR des images décryptées en présence de bruit « AWGN. » 34
3.6 Résultats de comparaison du PSNR des images décryptées en présence de bruit « Speckle » 36
3.7 Résultats comparaison PSNR des images décryptées en présence de bruit « SALT & PEPPER » 37
3.8 Résultats NPCR et UACI 40

Liste des acronymes

AES	Advanced Encryptions Standard
CM	Chaotic Maps
DCT	Discrete Cosine Transform
DES	Data Encryptions Standard
DRPE	Double Random Phase Encoding
MSE	Mean Squared Error
NPCR	Number of Pixels Change Rate
PSNR	Peak Signal-to-Noise Ration. Rapport signal/bruit de crête.
TF	Transformé de Fourier
TFFrD	Transformé de Fourier fractionnaire discrète
UACI	Unified Average Changing Intensity
2D	Deux dimensions

Table des matières

Résumé .....
Remerciements .....
Liste des figures .....
Liste des tableaux .....
Liste des abréviations .....
Introduction générale ……..…….....…01

Chapitre 1 : Généralités sur le cryptage d'images couleurs

1.1 Introduction.....02
1.2 Rappels sur l'image numérique 02
1.2.1 Définition…… ...02
1.2.2 Attributs 02
1.2.3 Modes de couleur……. 04
1.3 Cryptage et cryptographie 05
1.3.1 Définition…… 05
1.3.2 Objectif…… 05
1.3.3 Cryptage à clé symétrique 06
1.3.4 Cryptage à clé asymétrique 06
1.3.5 Cryptanalyse 07
1.4 Techniques de cryptage d'image couleurs à clé symétrique 07
1.4.1 Objectif 07
1.4.2 Cryptage spatiale classique des images …… 07
1.4.3 Cryptage dans le domaine fréquentiel …… 08
1.4.4 Exploitation des transformées fractionnaires/paramétrique.....09
1.4.5 Usage des suites chaotiques unidimensionnels/multidimensionnels.....10
1.5 Conclusion 10

Chapitre 2 : Cryptage d'image basée sur la transformée TFFrD et les suites chaotiques 2D

2.1 Introduction 11
2.2 Transformée de Fourier fractionnaire discrète TFFrD.....11
2.2.1 Définition…… 11
2.2.2 Propriétés ……. 12
2.3 Cryptage dans le domaine de la TFFrD …….....12
2.4 Les suites chaotiques 13
2.4.1 Définition……. 13
2.4.2 Propriétés…….....13
2.4.3 Diagramme de bifurcation 13
2.4.4 Exemple d'utilisation en cryptage image …….....14
2.5 Les suites chaotiques bidimensionnelles 2D…… 15
2.5.1 Avantage sur les suites 1D…… 15
2.5.2 Suite chaotique 2D-IICM…….....15
2.5.3 Suite chaotique 2D-LSCM.....16
2.5.4 Suite chaotique 2D-LSM…….....16
2.5.5 Suite chaotique 3D-DCT……..... 17

2.6 Etude comparative proposée 17
2.6.1 Algorithme de cryptage 17
2.6.2 Algorithme de décryptage 18
2.7 Conclusion 19

Chapitre 3 : **RESULTATS ET DISCUSSIONS**

3.1 Introduction 20
3.2 Environnement de développement 20
3.3 Organigramme générale de simulation 20
3.4 Résultats des simulations 24
3.4.1 Analyse visuelle 24
3.4.2 Analyse par histogramme 26
3.4.3 Entropie 30
3.4.4 Coefficient de corrélation 31
3.4.5 Résistance aux bruits 33
3.4.6 NPCR/UACI 39
3.4.7 Sensibilité de la clé 40
3.5 Discussions 44
3.6 Conclusion 47

Conclusion Générale 48
Bibliographie .....

INTRODUCTION GENERALE

INTRODUCTION GENERALE

Le cryptage est un moyen essentiel pour la protection des informations, en particulier celles de nature sensible et son utilisation s'est développée à travers les âges. Avec l'avancement des sciences et de la technologie, ainsi que la forte augmentation des échanges des données multimédias telles que les images sur les réseaux et les plateformes numériques, le besoin de protéger les données visuelles est devenu plus qu'urgent compte tenu de l'évolution des techniques et des méthodes utilisées pour casser leurs sécurités et confidentialités.

Dans ce contexte, le cryptage est devenu un élément indispensable pour protéger nos données personnelles et financières et garantir la sécurité de notre vie privée dans un monde caractérisé par des menaces continus.

Dans ce travail, on vise à étudier un système de cryptage innovant utilisant des suites et des transformées mathématiques bidimensionnelles 2D pour le cryptage d'images couleurs.

L'étude comprend une analyse comparative dans le cadre du chiffrement d'images en couleur en termes de performances et de sécurité. Grâce à cette étude, une compréhension plus approfondie de l'amélioration de la sécurité des données visuelles et du développement de solutions de chiffrement innovantes protégeant plus efficacement les images en couleur peut être réalisée, contribuant ainsi à renforcer la confidentialité et la sécurité des images couleurs.

Le plan de travail de notre mémoire est divisé en trois chapitres :

✓**Chapitre 1 : Généralités sur le cryptage d'images couleurs**

Introduction aux concepts de base des systèmes cryptographiques et leurs principes ainsi qu'aux différentes approches de cryptage d'image couleurs existantes.

✓**Chapitre 2 : Théorie de la méthode DRPE et des suites chaotiques**

Présentation du principe de cryptage d'images par l'utilisation de la technique DRPE avec des transformées paramétriques et de suites chaotiques unidimensionnelles et bidimensionnelles. Description détaillée de l'algorithme de cryptage et de décryptage de l'étude comparative à suivre.

✓**Chapitre 3 : Résultats et analyses comparatives**

Présentation des résultats de l'étude comparative de la méthode DRPE combinée avec différentes suites chaotiques bidimensionnels en termes de sécurité, de robustesse et d'efficacité.

Enfin, on finit notre travail par une conclusion générale avec une synthèse des principaux résultats et propositions avec des perspectives pour la continuité du travail dans le domaine de la sécurité de l'information.

CHAPITRE 1 :

GÉNÉRALITÉS SUR LE CRYPTAGE D'IMAGES COULEURS

1.1. Introduction

Dans ce chapitre, nous allons revoir les fondements de l'image numérique et les bases du cryptage et de la cryptographie. Nous commencerons par un rappel sur l'image numérique. Ensuite, nous nous pencherons sur le domaine de la cryptographie, en définissant ses objectifs et en explorant les techniques de cryptage à clé symétrique et asymétrique, ainsi que la cryptanalyse. Enfin, notre attention sera portée sur les techniques spécifiques de cryptage des images en couleur à clé symétrique, telles que le cryptage classique bit par bit, par pixel ou par bloc de pixels, dans le domaine fréquentiel et à travers l'exploitation de transformations mathématiques et de suites numériques chaotiques.

1.2 Rappels sur l'image numérique

1.2.1 Définition

Les images numériques naissent de la conversion de données analogiques, en données numériques, représentées par des 0 et des 1, à travers un processus appelé échantillonnage.

Chaque image numérique est une matrice d'éléments appelés "pixels". Ces pixels seront affectés à des nombres binaires permettant de définir leurs teintes en gris ou en couleurs [1].

1.2.2 Attributs

L'image numérique possède plusieurs caractéristiques ou attributs :

-Pixel : abréviation de "Picture Element". Les pixels représentent le plus petit élément constitutif d'une image numérique. Ils sont organisés sous forme matricielle où chaque pixel possède sa propre couleur/valeur [2] comme le montre la figure 1.1.

-Résolution : La résolution d'une image est définie par le nombre de pixels par pouce. Cette résolution dépendra de la qualité de l'échantillonnage/numérisation.

-Taille : La taille d'une image correspond à son codage binaire, mesurée en octets où Taille = nombre d'octets par × définition.

-Mode couleur

Il existe plusieurs types de représentation des images couleurs, parmi lesquels on retrouve :

•La représentation en couleurs réelles

La représentation en couleurs réelles utilise 24 bits pour chaque point de l'image. Chaque composante de couleur (rouge, verte et bleue) est décrite sur huit bits. Ainsi, huit bits sont assignés à la composante rouge (R), huit bits à la composante verte (V) et huit bits à la composante bleue (B). Cette méthode permet de représenter environ 16,7 millions de couleurs différentes simultanément [3].

•La représentation en couleurs indexées

Dans la représentation en couleurs indexées, une palette de couleurs est associée à l'image pour réduire l'espace occupé par l'information de couleur. Les pixels de l'image ne portent plus la couleur effective, mais font référence à une entrée dans une table de correspondance appelée table de consultation (look-up table ou LUT en anglais). Cette table contient la représentation complète de chaque couleur utilisée dans l'image. Ainsi, chaque valeur de pixel renvoie à une couleur spécifique définie dans la palette, ce qui permet de réduire la quantité d'information nécessaire pour stocker l'image tout en préservant la qualité visuelle [3].

-Format : La taille d'une image numérique à l'état brut est volumique. Il est donc nécessaire d'avoir un format compressé ayant un compromis compression/qualité. BMP, TIFF, JPEG ou PNG sont parmi les formats plus connus.

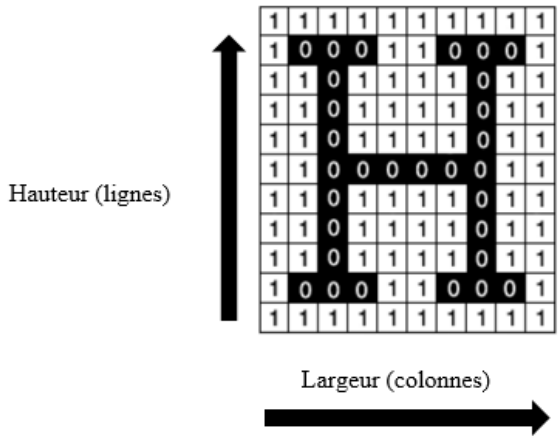


Figure 1.1 : Illustration des pixels d'une image numérique binaire [3]

1.2.3 Modes de couleurs

-Mode binaire

Ce mode permet d'avoir des images numériques en deux couleurs noir et blanc où chaque pixel est codé en 1 bit par pixel (bpp): 0 pour le noir et 1 pour le blanc comme le montre la figure 1.2.

1	1	1	1	1	1	1	1	1	1
1	1	1	0	0	0	0	1	1	1
1	1	0	1	1	1	1	0	1	1
1	0	1	1	1	1	1	1	0	1
1	0	1	0	1	1	0	1	0	1
1	0	1	1	1	1	1	1	0	1
1	0	1	0	1	1	0	1	0	1
1	0	1	1	0	0	1	1	0	1
1	1	0	1	1	1	1	0	1	1
1	1	1	0	0	0	0	1	1	1
1	1	1	1	1	1	1	1	1	1

Figure 1.2 Image binaire (0 ,1) [4]

-Mode niveau de gris

Dans ce mode, chaque pixel est codé avec un nombre variant de «0» (pour le noir) à «2^n-1» (pour le blanc) où n le nombre de bits pour chaque pixel. Soit 2^n niveaux de gris.

Par exemple, si n = 8 bits par pixel, on aura 256 niveaux de gris. Si n =16 bits par pixel, on aura 65536 niveaux de gris variant du noir au blanc, comme le montre la figure 1.3 :

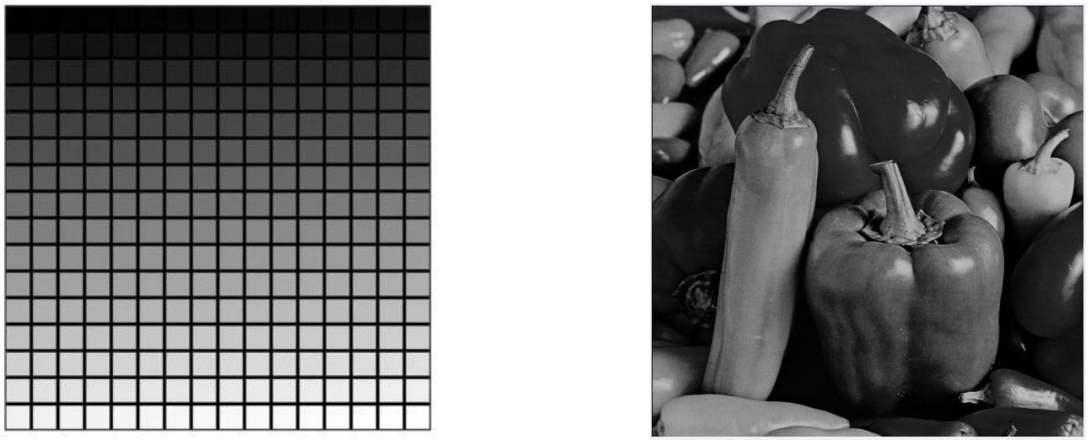


Figure 1.3 Nuance de 256 gris /Image codée en niveau de gris [4]

-Mode couleur RVB

Le mode couleur RVB (Rouge, Vert, Bleu) permet de reproduire un vaste éventail de nuances en mélangeant les trois couches de couleur. Dans un codage RVB 8 bits par couche, chaque couche utilise 8bits (1 octet), soit 256 nuances possibles : 8 bits pour le Rouge, 8 bits pour le Vert et 8 bits pour le Bleu. Soit 3 x 8 bits = 24 bits au total ou 16,7 milions comme le montre la figure 1.3,1.4. Dans le cas du codage RVB 16bits on a 4 milliards de nuances possibles, comme le montre la figure 1.4:

a) Le mode RVB **b)** : Image codée en couleur

Figure 1.4 Codage RVB 16bits [3]

1.3 Cryptage et cryptographie

1.3.1 Définitions

La cryptographie consiste en l'étude des méthodes permettant de transmettre des données de manière confidentielle. Pour protéger un message, on applique une transformation qui le rend incompréhensible, ce qu'on appelle le chiffrement ou le cryptage.

Le cryptage ou le chiffrement prend un texte en clair et le transforme en un texte chiffré ou cryptogramme. En revanche, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré, en inversant la transformation initiale.

1.3.2 Objectifs

Les buts de la cryptographie sont la confidentialité des données, l'intégrité des données, l'authentification et la non répudiation des données.

-La confidentialité : Un aspect crucial en cryptographie. Le texte crypté doit être conçu de manière à ce qu'il ne soit lisible que par les destinataires légitimes du message. Ainsi, il doit être rendu illisible pour tout intrus qui tenterait d'accéder à son contenu[4].

-Intégrité : Le destinataire d'un message doit pouvoir vérifier que celui-ci n'a pas été modifié en chemin. Un intrus ne doit pas être capable de faire passer un faux message pour légitime[4].

-Authentification : Le destinataire d'un message doit pouvoir s'assurer de son origine. Un intrus ne doit pas être capable de se faire passer pour quelqu'un d'autre[4].

- Non-répudiation : Un expéditeur ne doit pas pouvoir, par la suite, nier à tort avoir envoyé un message[4].

1.3.3 Cryptage à clé symétrique

Le cryptage à clé symétrique, également appelé cryptographie symétrique ou à clé secrète, est l'une des formes les plus anciennes de chiffrement. Dans ce système, le même mot clé est utilisé à la fois pour crypter et décrypter les messages. Les algorithmes les plus répandus sont : RC4 DES, AES, 3DES, …etc.

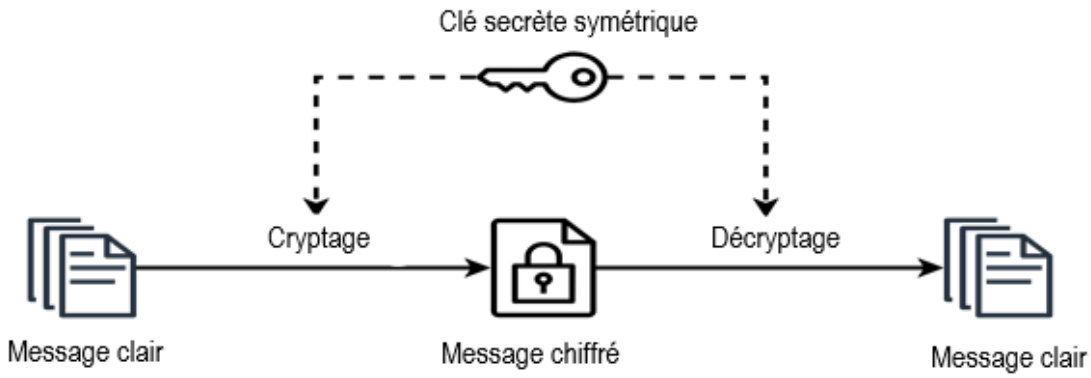


Figure 1.5 La cryptographie symétrique

1.3.4Cryptage à clé asymétrique

Dans un système de cryptage asymétrique, les clés existent par paires :

-Une clé publique utilisée pour chiffrer les messages.

-Une clé privée, gardée secrète, utilisée pour déchiffrer les messages chiffrés avec la clé publique correspondante.

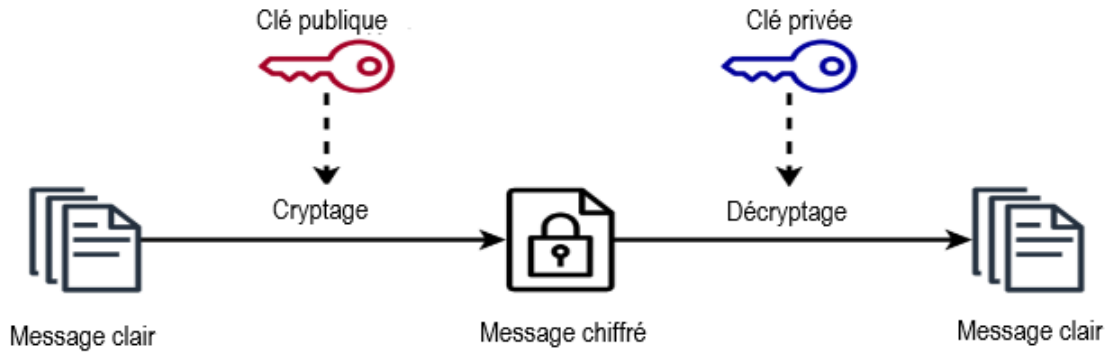


Figure 1.6 Cryptographie asymétrique

1.3.5 Cryptanalyse

La cryptanalyse est la science qui étudie les techniques à utiliser pour récupérer le message original d'un message crypté sans avoir accès à la clé privée.

Elle vise à démontrer les faiblesses des systèmes de cryptage, notamment en mettant en évidence des attaques bien connues telles que l'attaque en texte clair connu/choisi.

Dans ces attaques, l'attaquant possède une connaissance préalable du processus de cryptage et dispose de paires d'images originales et chiffrées. Il tente de déchiffrer une image chiffrée en utilisant diverses clés puis compare l'image décryptée obtenue avec l'image originale [5],[6].

1.4 Techniques de cryptage d'image couleurs à clé symétrique

1.4.1 Objectif

Les techniques de cryptage d'images couleur à clé symétrique visent à assurer la confidentialité des images en les rendant illisibles pour toute personne n'ayant pas la clé appropriée. Elles ont pour but d'empêcher tout accès non autorisé aux informations visuelles contenues dans les images, que ce soit lors de leur stockage, de leur transmission ou de leur manipulation.

1.4.2 Cryptage spatiale classique des images

En cryptage classique, chaque pixel ou bloc de pixels du domaine spatiale est considéré comme un bit ou une suite de bits en utilisant des techniques classiques connus de cryptage par flot de bits (stream cipher) ou cryptage par bloc de bits (block cipher) comme le montre la figure 1.7.

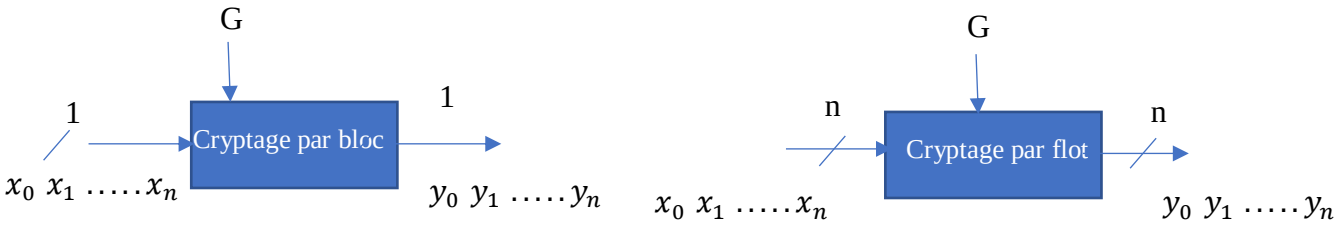


Figure 1.7 : Cryptage par bloc vs Cryptage par flot

- Le cryptage par bloc (bloc cipher) effectue les opérations de chiffrement sur un bloc du contenu du texte clair de taille "b". Utilisé dans les applications internet.

- Le cryptage par flot (stream cipher) effectue les opérations de chiffrement sur un seul bit avec un XOR. Ce genre de chiffrement est utilisé comme une implémentation hardware dans les appareils à faible capacité (téléphone ou appareil embarqué).

-Le cryptage par flot ou par bloc n'est pas exclusif pour le cryptage d'images, en effet, il est conçu pour le cryptage de n'importe quelle donnée multimédia sous forme binaire (texte, audio, parole, image, vidéo…etc…) peu importe son type. Cependant, il peut être vulnérable à certaines attaques, notamment les attaques par texte clair connu et les attaques par rejeux si le flux de clé n'est pas correctement géré. Pour garantir la sécurité, il est essentiel d'utiliser des générateurs de nombres pseudo-aléatoires robustes et des protocoles de gestion des clés appropriés [6].

-Certains exemples d'algorithmes de chiffrement symétrique par flot incluent A5, utilisé dans les téléphones mobiles de type GSM pour chiffrer les communications radio, ainsi que RC4, conçu par Ronald Rivest, qui est largement utilisé, notamment par le protocole WEP (Wired Equivalent Privacy) et le protocole Bluetooth [6].

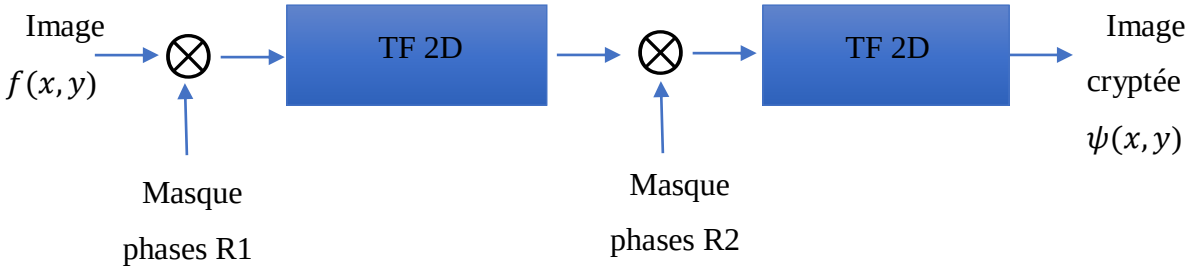
1.4.3 Cryptage dans le domaine fréquentiel

-Le cryptage classique des images est un cryptage brut qui ne prend pas en considération les caractéristiques de l'image ou les propriétés des pixels de l'image.

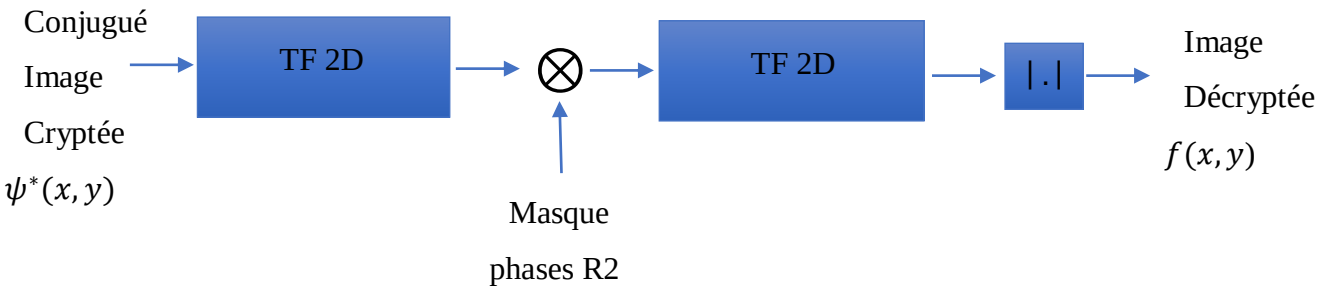
-De ce fait, de nouvelles techniques de cryptage d'images dans le domaine fréquentiel ont vu le jour. Ces techniques reposent sur des techniques telles que la transformation en cosinus discrète (DCT) et la transformation en ondelettes discrètes (DWT).

-Ces transformations permettent de convertir l'image en un domaine de fréquences, offrant ainsi la possibilité d'appliquer différents algorithmes de cryptage. Bien que la DCT et la DWT soient des méthodes importantes, la transformée de Fourier discrète (DFT) est également largement utilisée, notamment dans le domaine optique pour son traitement rapide des données.

Le cryptage optique, comme le schéma DRPE dans la figure 1.8, utilise deux masques de phases aléatoires pour brouiller l'image dans les deux domaines, spatial et fréquentiel. Cette approche offre une méthode sécurisée pour le cryptage des images, particulièrement adaptée aux applications optiques à grande vitesse [7].



a) Algorithme de cryptage



b) algorithme de décryptage

Figure 1.8 Cryptage DRPE dans le domaine de la transformée de Fourier [12],

1.4.4 Exploitation des transformées fractionnaires/paramétrique

L'utilisation de transformées fractionnaires dans la cryptographie représente une approche innovante pour sécuriser les données, y compris les images. Les transformées fractionnaires telles que la transformée de Fourier fractionnaire (FRFT) et la transformée en ondelettes fractionnaires (FWT) offrent des propriétés uniques qui peuvent être exploitées pour le cryptage.

Ces transformées permettent la manipulation des données à des échelles fractionnaires, offrant ainsi une flexibilité supplémentaire pour le cryptage. Par exemple, la FRFT permet de moduler l'angle de rotation de la transformée de Fourier, ce qui peut être utilisé pour brouiller les informations de manière complexe et non linéaire.

De même, la FWT fractionnaire permet une analyse multi résolution des données, ce qui peut être exploité pour crypter les images à différentes échelles spatiales de manière sélective.

L'exploitation de ces transformées fractionnaires dans la cryptographie ouvre de nouvelles perspectives pour le développement d'algorithmes de cryptage robustes et sécurisés, capables de résister aux attaques modernes.

Cependant, leur utilisation nécessite une compréhension approfondie des propriétés mathématiques sous-jacentes et des techniques de cryptographie adaptées pour garantir leur efficacité et leur sécurité [8],[9].

1.4.5 Usage des suites chaotiques unidimensionnels/multidimensionnels

Les suites chaotiques sont des suites mathématiques. Ces suites ont un comportement lié à l'instabilité et à la non-linéarité dans des systèmes dynamiques déterministes. Il peut arriver que de petites différences dans les conditions initiales engendrent de très grandes différences dans les phénomènes finaux. Une petite erreur sur les premières produirait une erreur énorme sur les dernières. La prédiction devient impossible et nous avons donc un comportement chaotique.

Ces suites chaotiques se présentent en forme unidimensionnelles ou multidimensionnelles qui peuvent être utilisées dans les applications liées à la sécurité de l'information, notamment pour la génération de clés secrètes dans les algorithmes de cryptage et de tatouage numérique. Ces suites chaotiques fournissent une source de données aléatoire et imprévisible, renforçant ainsi la sécurité des systèmes cryptographiques [10].

1.5 Conclusion

Dans ce chapitre, nous avons vu les notions de base sur les images numériques et la cryptographie. Nous avons également revu brièvement les techniques de cryptage d'image couleurs. Dans le chapitre suivant, nous allons expliquera le cryptage d'image basée sur la transformée TFFrD et les suites chaotiques 2D.

CHAPITRE 2 :

CRYPTAGE D'IMAGE BASÉE SUR LA TRANSFORMÉE TFFrD ET LES SUITES CHAOTIQUES 2D

2.1 Introduction

Ce chapitre explore le cryptage d'images en utilisant la transformée de Fourier fractionnaire discrète (TFFrD) et les suites chaotiques bidimensionnelles 2D. Nous commençons par présenter la TFFrD, ses principes et ses propriétés, puis examinons son utilisation pour le cryptage d'images.

Ensuite, nous plongeons dans les suites chaotiques, en définissant leur nature, leurs propriétés et en illustrant leur application dans le cryptage d'images couleur. Nous mettons en avant les avantages des suites chaotiques bidimensionnelles 2D par rapport aux suites unidimensionnelles. Enfin, nous proposons une étude comparative des algorithmes de cryptage et de décryptage.

2.2 Transformée de Fourier fractionnaire discrète TFFrD

2.2.1 Définition

La transformée de Fourier fractionnaire discrète TFFrD (DFrFT) d'ordre α et de taille N × N est définie comme suit :

$$F^{\bar{a}} = V\Lambda^{\bar{\alpha}}V^{\top} = \begin{cases} \sum_{n=0}^{N-1} \lambda_n^{\alpha} V_n V_n^{\top} & si\ N\ impair \\ \sum_{n=0}^{N-2} \lambda_n^{\alpha} V_n V_n^{\top} + \lambda_N^{\alpha} v_N V_N^{\top} & si\ N\ pair \end{cases} \quad (2.1)$$

- $(.)^{\top}$ Signifie la transposée.
- Pour N impair : $V = [v_0|v_1|.....|v_{N-2}|v_{N-1}]$.
- Pour N pair : $V = [v_0|v_1|.....|v_{N-2}|v_N]$.
- Λ^{α}une matrice diagonale dont les coefficients non nuls correspondent aux valeurs propres λ_n^{α}où $\lambda_n^{\alpha} = e^{-j\frac{\pi}{2}\alpha n}$et $\alpha = \frac{\pi}{2\alpha}n$ de la matrice S de taille $N \times N$ défini comme suit où $\omega = \frac{2\pi}{N}$ [19], [20] :

$$S = \begin{bmatrix} 2 & 1 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 2\cos\omega & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 2\cos 2\omega & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & & \vdots & \vdots \\ 1 & 0 & 0 & 0 & \cdots & 1 & 2\cos(N-1)\omega \end{bmatrix} \quad (2.2)$$

Les matrices S et F auront les mêmes vecteurs propres si S commutative avec F et si l'égalité suivante est satisfaite S. F = F. S. Ils n'auront pas les mêmes valeurs propres car la matrice de Fourier F a seulement quatre valeurs propres distinctes {1, j, -1, j} [12].

2.2.2 Propriétés

Parmi les propriétés importantes de la TFFrD on trouve [12] :

-L'additivité : $F^b.F^a = F^{a+b}$.

-L'inverse de la transformé : $F^{-a}.F^a = I$. Où I indique la matrice identité.

2.3Cryptage dans le domaine de la TFFrD

Le cryptage dans le domaine de la TFFrD repose sur le principe de la méthode DRPE vu sur le chapitre 1. Elle consiste à crypter une image de dimensions $N \times M$ avec deux masques des phases aléatoires.

Ces phases sont générées aléatoirement à partir du plan complexe à l'aide de deux fonctions distinctes $\alpha(n,m)\ et \beta(n,m)$ [12].

Comme illustré dans la figure 2.1, le premier masque M1 est appliqué dans le domaine spatial, tandis que le second masque M2 est appliqué dans le domaine fréquentielle [13].

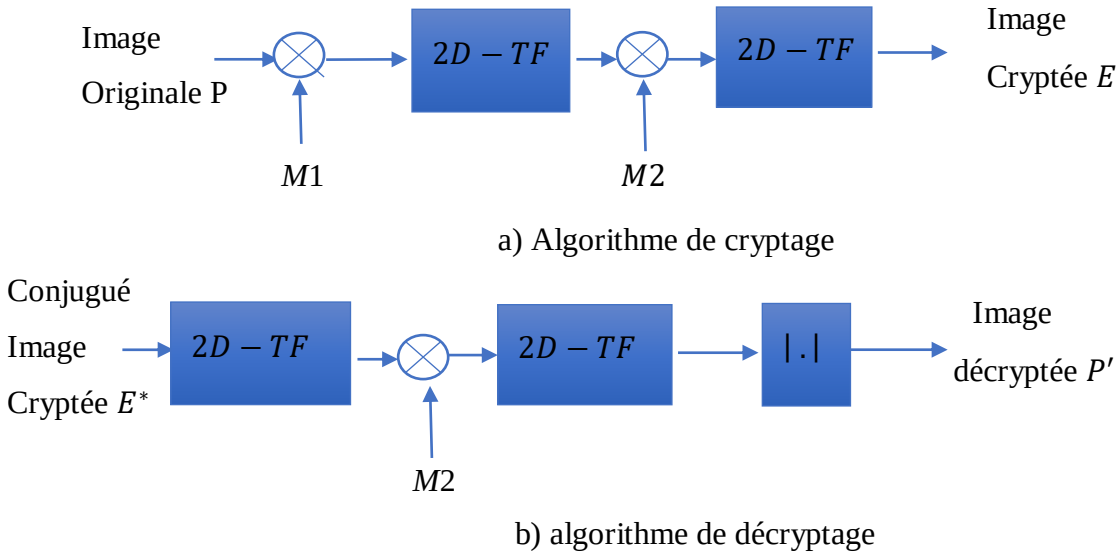


Figure 2.1 Méthode de cryptage DRPE dans le domaine TFFrD,

La figure 2.1 illustre la technique de chiffrement et de déchiffrement par double masquage de phases aléatoires (DRPE) combinée avec la transformée de Fourier fractionnaire discrète (DFrFT) ce qui complique davantage le déchiffrement et rend la récupération de l'image originale extrêmement difficile sans les clés appropriées.

Lors du chiffrement, des phases aléatoires sont ajoutées à l'image en utilisant DRPE, suivies de l'application de la DFrFT pour augmenter la complexité. Pour déchiffrer, on multiplie par le conjugué de l'image.

2.4 Les suites chaotiques

2.4.1 Définition

Une suite chaotique est une séquence de nombres générée par un système dynamique chaotique qui présente deux caractéristiques importantes [20] :

-Le phénomène de sensibilité aux conditions initiales ;

-Une forte récurrence.

Pour visualiser ce comportement chaotique de manière graphique, on utilise un diagramme appelé diagramme de bifurcation [12].Cette sensibilité élevée est utilisée dans le domaine de la cryptographie, où les paramètres des suites chaotiques sont considérés comme une clé de cryptage secrète [12][11].

2.4.2 Propriétés

-Sensibilité aux conditions initiales : Les suites chaotiques présentent une sensibilité extrême à leurs conditions initiales, de sorte qu'une petite modification dans l'état initial peut entraîner des changements radicaux dans l'état final [11].

-Pseudo-aléatoires : bien que les systèmes chaotiques soient déterministes, tous les états d'un système chaotique exhibent des caractéristiques aléatoires [10].

-Ergodique : l'ergodicité d'un processus chaotique signifie que sa distribution en sortie reste constante, quelle que soit la distribution de la variable à l'entrée [10].

2.4.3 Diagramme de bifurcation

La bifurcation est un processus observé dans les systèmes chaotiques où une petite perturbation ou un changement dans les règles directrices provoque un changement d'état ou de comportement du système [16].

C'est un concept important pour comprendre la théorie du chaos et peut conduire à l'émergence de nouveaux modèles ou comportements qui n'étaient pas présents dans le système auparavant [16].

Prenons l'exemple d'une suite logistique. Une suite logistique qui est la plus simple des suites chaotiques unidimensionnelles est générée itérativement en utilisant l'équation quadratique [12] :

$$x_{n+1} = r.x_n.(1 - x_n) \qquad (2.3)$$

Où r ∈ [0,4] est le paramètre de contrôle. Elle est générée itérativement en partant de $x_0 \in [0,1]$ appelée condition initiale.

La figure 2.2 montre le diagramme de bifurcation de la suite logistique en fonction de son paramètre de contrôle r. On remarque que la suite logistique est vraiment chaotique si $\mu \in [3.75,4]$ et purement chaotique

si $\mu \cong 4$. La suite montre un bon comportement et elle est fréquemment utilisée dans le cryptage d'image [14].

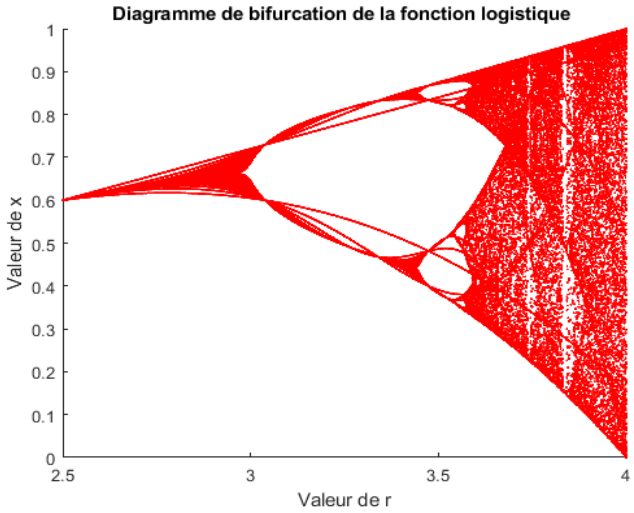


Figure 2.2 Diagramme de bifurcation de la suite logistique

2.4.4 Exemple d'utilisation en cryptage image couleur

Dans cet exemple simple, nous avons utilisé une suite logistique afin de crypter une image niveau de gris par permutation. Cette technique consiste à permuter des blocs de pixels de l'image dans le domaine spatial comme le montre la figure 2.3.

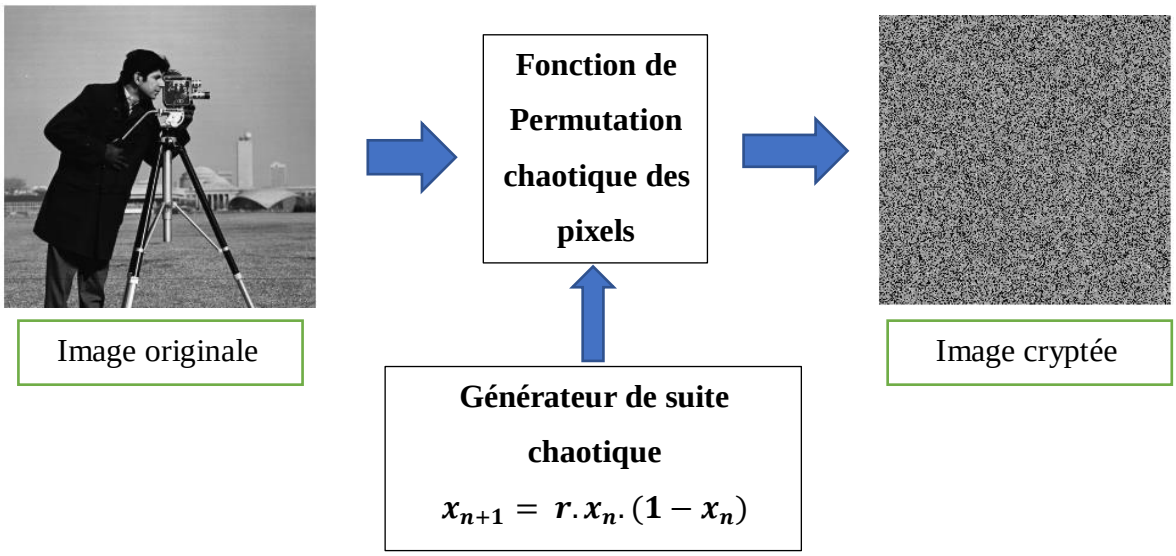


Figure 2.3 Exemple d'utilisation de suite logistique en cryptage image

2.5 Les suites chaotiques bidimensionnelles 2D

Il existe plusieurs types de suites chaotiques bidimensionnelles qui peuvent être utilisées à des fins de cryptage. Voici un aperçu de quelques-unes des suites chaotiques 2D les plus connues [16] :

-La suite de Hénon.

-La suite de Lozi.

-La suite standard 2D.

-La suite d'Arnold.

2.5.1 Avantage sur les suites 1D

Les systèmes chaotiques 1D sont connus pour leur structure simple et leur facilité de mise en œuvre [15], cependant, ils ne disposent que d'un seul paramètre de contrôle.

En revanche, les suites chaotiques bidimensionnelles comportent deux paramètres ou plus. Cette caractéristique implique que l'espace des paramètres des suites chaotiques 2D est plus vaste que celui des suites chaotiques 1D, ce qui peut renforcer la sécurité de l'algorithme de cryptage.

Une autre distinction importante réside dans le fait que les suites chaotiques 1D génèrent une séquence unidimensionnelle de nombres, tandis que les suites chaotiques bidimensionnelles génèrent une séquence bidimensionnelle. Par conséquent, les suites chaotiques 2D peuvent être utilisées pour crypter des données bidimensionnelles, telles que des images ou des vidéos, alors que les suites chaotiques 1D sont généralement utilisées pour crypter des données unidimensionnelles, telles que des fichiers audios ou des textes [15].

2.5.2 Suite chaotique 2D-IICM

- **Définition mathématique :**

La suite chaotique 2D-IICM (Two-Dimentional Infinite Collapse Hyperchaos) est une extension du concept de l'effondrement infini 1D-IICM à deux dimensions [17],[18]. Voici le principe mathématique de la suite :

$$\chi_{n+1} = \sin(\mu/\chi_n) \quad (2.4)$$

Lorsque le paramètre $\mu \neq 0$, la suite chaotique est dans état chaotique, et la séquence χ est dans l'intervalle [-1,1].

Afin d'obtenue les meilleures caractéristiques chaotiques il faut d'ajuster la formule 2.4 pour obtenir l'hyperchaos 2D-IICM, où $b \in [0,1]$.

$$\begin{cases} \chi_{n+1} = \sqrt{1 - by_n^2}\sin(\alpha/\chi_n) \\ \chi_{y+1} = \sqrt{1 - b\chi_n^2}\sin(\alpha/y_n) \end{cases} \quad (2.5)$$

2.5.3 Suite chaotique 2D-LSCM

La 2D-LSCM (Two-Dimentional Logistic-Sine-Coupling Map) est dérivée de deux suites chaotiques 1D existantes [21], à savoir la suite Logistique et map Sinus. La suite Logistique est définie comme suit :

$$\chi_{i+1} = 4\eta\chi_i(1 - \chi_i)\ . \quad (2.6)$$

Oùη est un paramètre de contrôle $\eta \in [0, 1]$.

$$\chi_{i+1} = \beta\sin(\pi\chi_i)\ . \quad (2.7)$$

Où β est un paramètre de contrôle $\beta \in [0, 1]$.

Les maps Logistique et Sinus présentent de nombreux inconvénients tels que des comportements simples et des intervalles chaotiques fragiles, et ces inconvénients peuvent avoir des effets négatifs pour certaines applications sur les bases chaotiques [21]. Cependant, Lorsque en couplant les maps Logistique et Sinus, on peut obtenir une nouvelle map chaotique 2D-LSCM, qui peut être définie comme suit :

$$\begin{aligned} \chi_{i+1} &= \sin(\pi(4\theta\chi_i(1 - \chi_i) + (1 - \theta)\sin(\pi y_i))) \\ y_{i+1} &= \sin(\pi(4\theta y_i(1 - y_i) + (1 - \theta)\sin(\pi\chi_{i+1}))) \end{aligned} \quad (2.8)$$

Oùθ est un paramètre de contrôle $\theta \in [0, 1]$.

Comme on peut l'observer dans sa définition, la 2D-LSCM est obtenue en couplant d'abord les maps Logistique et Sinus ensemble, puis en effectuant une transformation sinus sur le résultat du couplage, et enfin en étendant la dimension de 1D à 2D. De cette manière, la complexité de la map Logistique et de la map Sinus peut être suffisamment mélangée, ce qui permet d'obtenir un comportement chaotique complexe [21].

2.5.4 Suite chaotique 2D-LSM

Cette suite 2D-LSM (Two-Dimentional Logistic Sine Map) est une combinaison de deux systèmes chaotique 1D non-linéaire.

Les deux systèmes chaotiques utilisées sont des suites logistiques et Sinus [23], comme définie dans les équations suivantes :

$$\chi_{i+1} = 4\alpha\chi_i(1-\chi_i) \qquad (2.9)$$

$$\chi_{i+1} = b\sin(\pi\chi_i) \qquad (2.10)$$

Oùα et $b \in [0,1]$, donc, la 2D-LDM peut être écrire comme suit :

$$\begin{cases}\chi_{i+1} = \cos(4\alpha\chi_i\,(1-\chi_i) + b\sin(\pi y_i) + 1);\\ y_{i+1} = \cos(4\alpha y_i\,(1-y_i) + b\sin(\pi\chi_i) + 1);\end{cases} \qquad (2.11)$$

La 2D-LSM possède deux paramètres de contrôle α et b. Comme les résultats, en 2D-LSM on peut élargir les plages de deux paramètres α et b [22].

2.5.5 Suite chaotique 3D-DCT

Ce nouveau système de mappage chaotique 3D-DCT (Discrete Cosine Transform) basé sur les maps logistiques et Hénon [23], comme le montre l'équation suivante :

$$\mathrm{f}(\chi_{i+1}, y_{i+1}) = \begin{cases}\sin(\frac{y_n}{\chi_n} - \alpha \times \chi_n^2 + \alpha)\\ \frac{\pi}{2} \times arcsin(\cos(b \times \chi_n))\end{cases} \qquad (2.12)$$

2.6 Etude comparative proposée

Algorithme de cryptage

-L'image P est représenté dans une matrice $P(x_i, y_j)$ de dimensions $N \times M$,où i et j représentent les coordonnées des pixels.

$$P(x_i, y_j) = \left[P_R(x_i, y_j), P_G(x_i, y_j), P_B(x_i, y_j)\right] \quad (2.13)$$

-Utilisation d'une des suites chaotiques 2D précédentes dans une fonction de permutation chaotique que l'on nommera de façon généralisé 2DCM afin de permuter les positions des pixels de l'image, introduisant une forme de confusion temporelle.

-

$$\boldsymbol{E_1}[P(x_i,y_j)] = \begin{bmatrix} \boldsymbol{FrFT}\left[\boldsymbol{2DCM}\left[P_R(x_i,y_j)\, e^{(j2\pi\theta_{r(x_i,y_j))}}\right]\right] \\ \boldsymbol{FrFT}\left[\boldsymbol{2DCM}\left[P_G(x_i,y_j)\, e^{(j2\pi\theta_{g(x_i,y_j))}}\right]\right] \\ \boldsymbol{FrFT}\left[\boldsymbol{2DCM}\left[P_B(x_i,y_j)\, e^{(j2\pi\theta_b(x_i,y_j))}\right]\right] \end{bmatrix} \quad (2.15)$$

- Multiplication par le premier masque de phase aléatoire. Ensuite, application de la FrFT pour chaque canal de l'image modulée, introduisant une forme de confusion optique.

$$\boldsymbol{E_1}(x_i,y_j) = \begin{bmatrix} \boldsymbol{FrFT^{-1}}\left[\boldsymbol{2DCM}\left[\boldsymbol{FrFT}[P_R(x_i,y_j)]\, e^{(j2\pi\theta_r(x_i,y_j))}\right] e^{(j2\pi\omega_r(u_i,v_j))}\right], \\ \boldsymbol{FrFT^{-1}}\left[\boldsymbol{2DCM}\left[\boldsymbol{FrFT}[P_G(x_i,y_j)]\, e^{(j2\pi\theta_g(x_i,y_j))}\right] e^{(j2\pi\omega_g(u_i,v_j))}\right], \\ \boldsymbol{FrFT^{-1}}\left[\boldsymbol{2DCM}\left[\boldsymbol{FrFT}[P_B(x_i,y_j)]\, e^{(j2\pi\theta_b(x_i,y_j))}\right] e^{(j2\pi\omega_b(u_i,v_j))}\right], \end{bmatrix} \quad (2.16)$$

-Les masques de phase aléatoires, les angles et les ordres de la 2D-FrFT sont utilisés comme clés de cryptage supplémentaires afin de renforcer la sécurité du système de cryptage

-L'image crypté $E(x_i,y_j)$ est obtenue contient les informations cryptées de l'image d'origine. Toutes les étapes de cryptage précédentes sont résumées sur la figure 2.4.

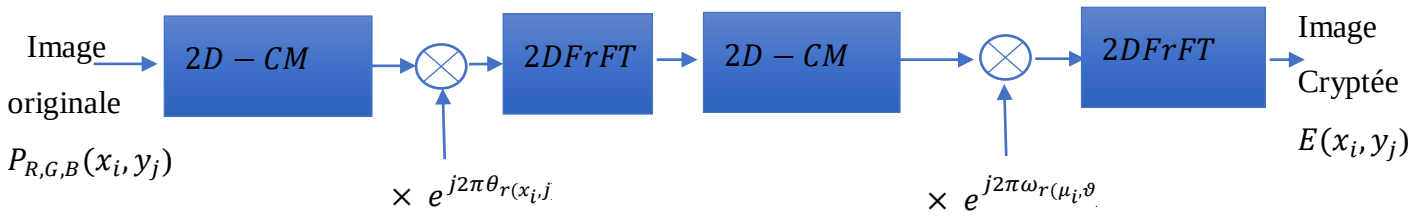


Figure 2.4 Algorithme de cryptage

2.6.1 Algorithme de décryptage

Les étapes de décryptage de l'image cryptée E consistent à prendre l'inverse des étapes précédentes de cryptage [12]. Ces étapes de décryptage peuvent être résumées par l'équation et figures suivantes :

$$p(x_i,y_j) = \begin{bmatrix} \boldsymbol{2DCM^{-1}}\left[\boldsymbol{FrFT^{-1}}\left[\boldsymbol{2DCM^{-1}}\left[\boldsymbol{FrFT}\,[\,E_R(x_i,y_j)]e^{(-j2\pi\omega_r(u_i,v_j))}\right]\right] e^{(-j2\pi\theta_r(x_i,y_j))}\right], \\ \boldsymbol{2DCM^{-1}}\left[\boldsymbol{FrFT^{-1}}\left[\boldsymbol{2DCM^{-1}}\left[\boldsymbol{FrFT}\,[\,E_G(x_i,y_j)]e^{(-j2\pi\omega_g(u_i,v_j)}\right]\right] e^{(-j2\pi\theta_g(x_i,y_j))}\right], \\ \boldsymbol{2DCM^{-1}}\left[\boldsymbol{FrFT^{-1}}\left[\boldsymbol{2DCM^{-1}}\left[\boldsymbol{FrFT}\,[\,E_B(x_i,y_j)]e^{(-j2\pi\omega_b(u_i,v_j)}\right]\right] e^{(-j2\pi\theta_b(x_i,y_j))}\right], \end{bmatrix} \quad (2.17)$$

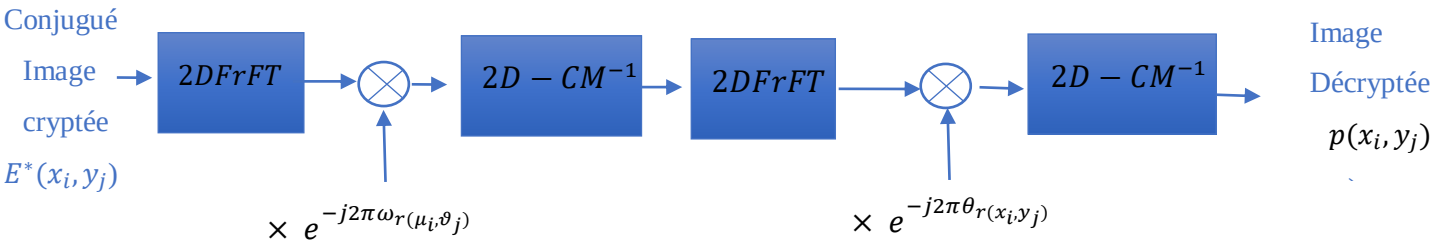


Figure 2.5 Algorithme de décryptage

2.7 Conclusion

Dans ce chapitre, nous avons étudié le cryptage d'images en utilisant la transformée de Fourier fractionnaire discrète (TFFrD) et les suites chaotiques bidimensionnelles 2D.

La TFFrD introduit des transformations complexes pour renforcer la confidentialité des données, tandis que les suites chaotiques offrent une sécurité accrue grâce à leur sensibilité aux conditions initiales et à leurs propriétés pseudo-aléatoires.

De plus, nous avons présenté la fonction de permutation chaotique 2D-IICM et trois autres suites, offrant des caractéristiques chaotiques améliorées pour le cryptage d'images

CHAPITRE 3 :

RESULTATS ET DISCUSSIONS

3.1 Introduction

L'idée repose sur l'utilisation de suites chaotiques 2D afin de renforcer la sécurité des systèmes de cryptage d'image dans le domaine fréquentiel de la transformée TFFrD.

Vu l'existence de plusieurs suites chaotiques 2D dans la littérature **[30]**, dans ce chapitre, nous présenterons une analyse comparative de l'utilisation de plusieurs suites chaotiques 2D dans le but d'évaluer leurs performances et leurs sécurités dans les systèmes de cryptage d'image couleur à base de transformée TFFrD.

L'analyse des résultats contribuera à comprendre l'étendue des performances et les multiples avantages que les chaînes chaotiques 2D peuvent apporter en matière de codage d'images couleur, et nous permettra ainsi de guider notre utilisation éventuelle des meilleures options dans des opérations réelles.

3.2 Environnement de développement

Nous avons utilisé le logiciel MATLAB 2021 et un PC i5 2.1Ghz pour nos tests, simulations et analyses des résultats.

Nous avons choisi des images couleur RVB de taille 256 × 256 pixels illustrées dans la figure 3.1 pour nos simulations.

Ces images ce sont des images de tests standards connues telles que "Peppers", "Barbra" "Airplane"…etc…

Name	Peppers	Barbara	Air plane
Images			

Figure 3. 1 Images de Test RVB simples de taille « 256 × 256 »

3.3 Organigramme générale de simulation

Des simulations ont été réalisées pour évaluer le système de cryptage des images couleur DFrFT en utilisant les séquences chaotiques bidimensionnelles 2D et des paramètres fractionnaires mentionnées sur le tableau 3.1 et tableau 3.2.

Tableau 3.1 Suites chaotiques bidimensionnelles évaluées.

Suite Chaotique	Abréviation Utilisée	Définition mathématique	Clé utilisée
2D-IICM	CM1	$\begin{cases} \chi_{n+1} = \sqrt{1 - by_n^2}\sin(\alpha/\chi_n) \\ \chi_{y+1} = \sqrt{1 - b\chi_n^2}\sin(\alpha/y_n) \end{cases}$	$b = 1$ $a_1 = 20 \quad a_4 = 23$ $a_2 = 21 \quad a_5 = 24$ $a_3 = 22 a_6 = 25$
3D-DCT	CM2	$\begin{cases} x_{n+1=} \sin(y_n/x_n - ax_n^2 + a) \\ y_{n+1=} \frac{\pi}{2}\arcsin(\cos(bx_n)) \end{cases}$	$b = 6.8$ $a_1 = 1.5 \quad a_4 = 2.25$ $a_2 = 1.75 \quad a_5 = 2.75$ $a_3 = 2 a_6 = 3$
2D-LSM	CM3	$\begin{cases} x_{n+1=} \cos\left(\pi^2\left(4ax_n(1-x_n) + by_n(1-y_n^2) + \frac{\pi}{2}\right)\right) \\ y_{n+1=} \cos\left(\pi^2\left(4ay_n(1-y_n) + bx_n(1-x_n^2) + \frac{\pi}{2}\right)\right) \end{cases}$	$b = 8.78$ $a_1 = 0.25 \; a_4 = 1.5$ $a_2 = 0.5 \quad a_5 = 1.75$ $a_3 = 1 \quad a_6 = 2$
2D-LSCM	CM4	$\begin{cases} x_{n+1} = \cos(4ax_n(1-x_n) + b\sin(\pi y_n) + 1) \\ y_{n+1} = \cos(4ay_n(1-y_n) + b\sin(\pi x_n) + 1) \end{cases}$	b = 50 $a_1 = 1 \quad a_4 = 4$ $a_2 = 2 \quad a_5 = 5$ $a_3 = 3 a_6 = 6$

Tableau 3.2 Paramètres fractionnaires DFrFT choisis

	Canal rouge	**Canal vert**	**Canal bleu**
Paramètre fractionnaire: a	a_r =0.51	a_g =0.45	a_b =0.35
Paramètre fractionnaire: b	b_r =0.35	b_g =0.25	b_b =0.40
Paramètre fractionnaire: c	c_r =0.65	c_g =0.55	c_b =0.50
Paramètre fractionnaire: d	d_r =0.23	d_g =0.30	d_b =0.25

Ces tests ont porté sur les mêmes images, et leur performance a été comparée dans le cadre du système de cryptage optique basé sur DFrFT suivant les organigrammes des algorithmes sur les figures 3.2 et 3.3. Le système proposé pour le cryptage des images en couleur, basé sur l'utilisation d'une suite chaotique bidimensionnelle et d'une transformation de Fourier fractionnaire, utilise deux étapes de mélange, l'une temporelle et l'autre fréquentielle.

Le processus commence par mélanger les emplacements des pixels de l'image d'origine à l'aide d'une suite chaotique bidimensionnelle, puis une transformation de Fourier fractionnaire est appliquée à l'image mélangée. Ensuite, l'image complexe transformée en RVB est à nouveau mélangée en utilisant une autre fois la suite chaotique bidimensionnelle, et enfin, une nouvelle transformation optique est effectuée à l'aide d'une transformation de Fourier partielle (le conjugué du DFrFT) pour revenant à l'image précédente.

Des masques à phases aléatoires doubles sont appliqués après chaque étape de mélange pour garantir une sécurité optimale en assurant un grand aléatoire (Randomness). Des suites CM bidimensionnelles ont été appliquées pour renforcer la sécurité de cryptage, les angles et les paramètres de la transformation de Fourier fractionnaire sont utilisés comme clés de cryptage supplémentaires**.**

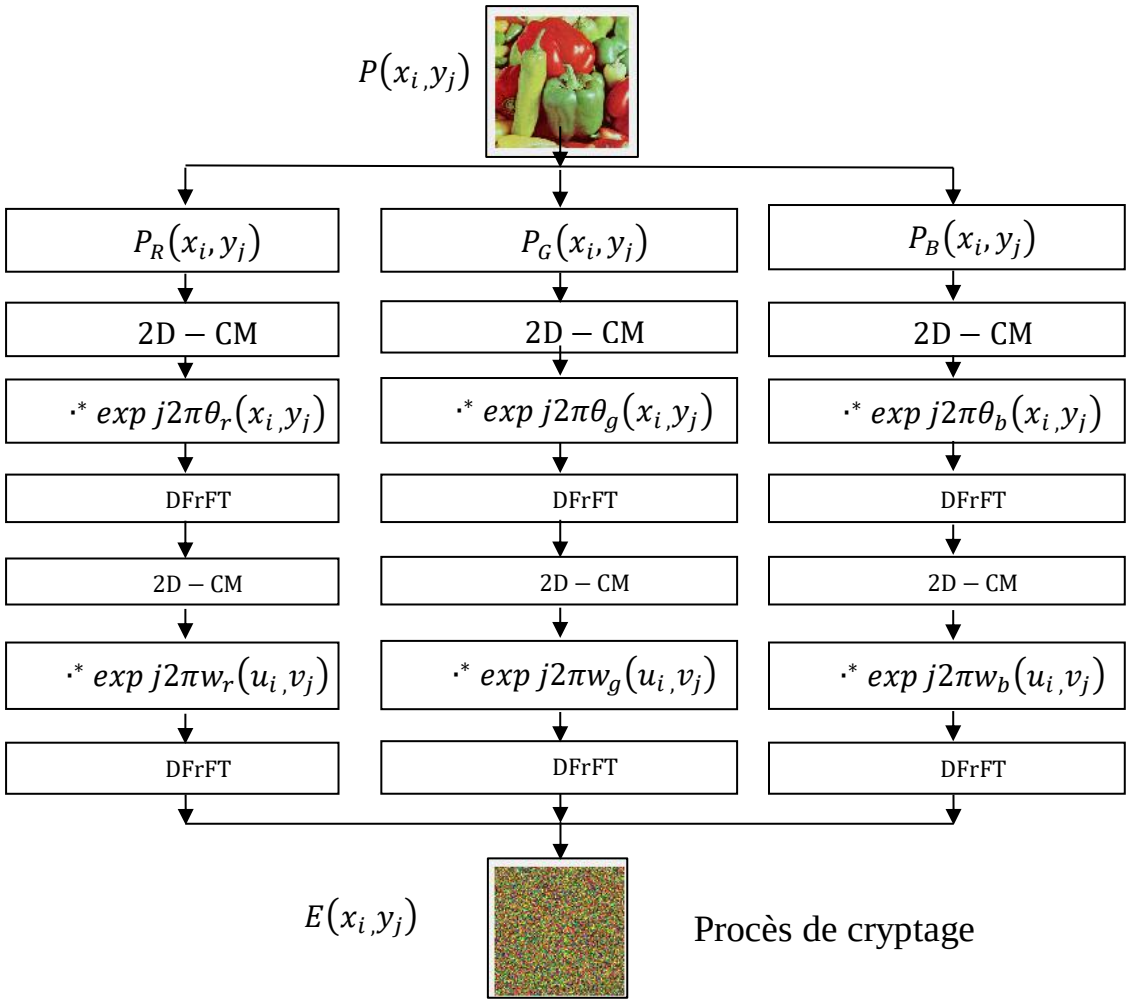


Figure 3.2 Algorithme de simulation en cryptage.

Les paramètres de contrôle optimaux correspondants ont été utilisés comme clé de cryptage pour chaque suite, avec des tests similaires pour toutes les suites concernant les paramètres de transformation associés, choisis avec la même fréquence partielle pour garantir une comparaison fiable entre les quatre séquences en vue d'évaluer leur performance réelle et correcte.

La qualité des images cryptées a été évaluée à l'aide d'indicateurs de sécurité courants tels que l'analyse visuelle, le test d'entropie, le test d'histogramme, divers tests de bruit, et la sensibilité de la clé, etc.

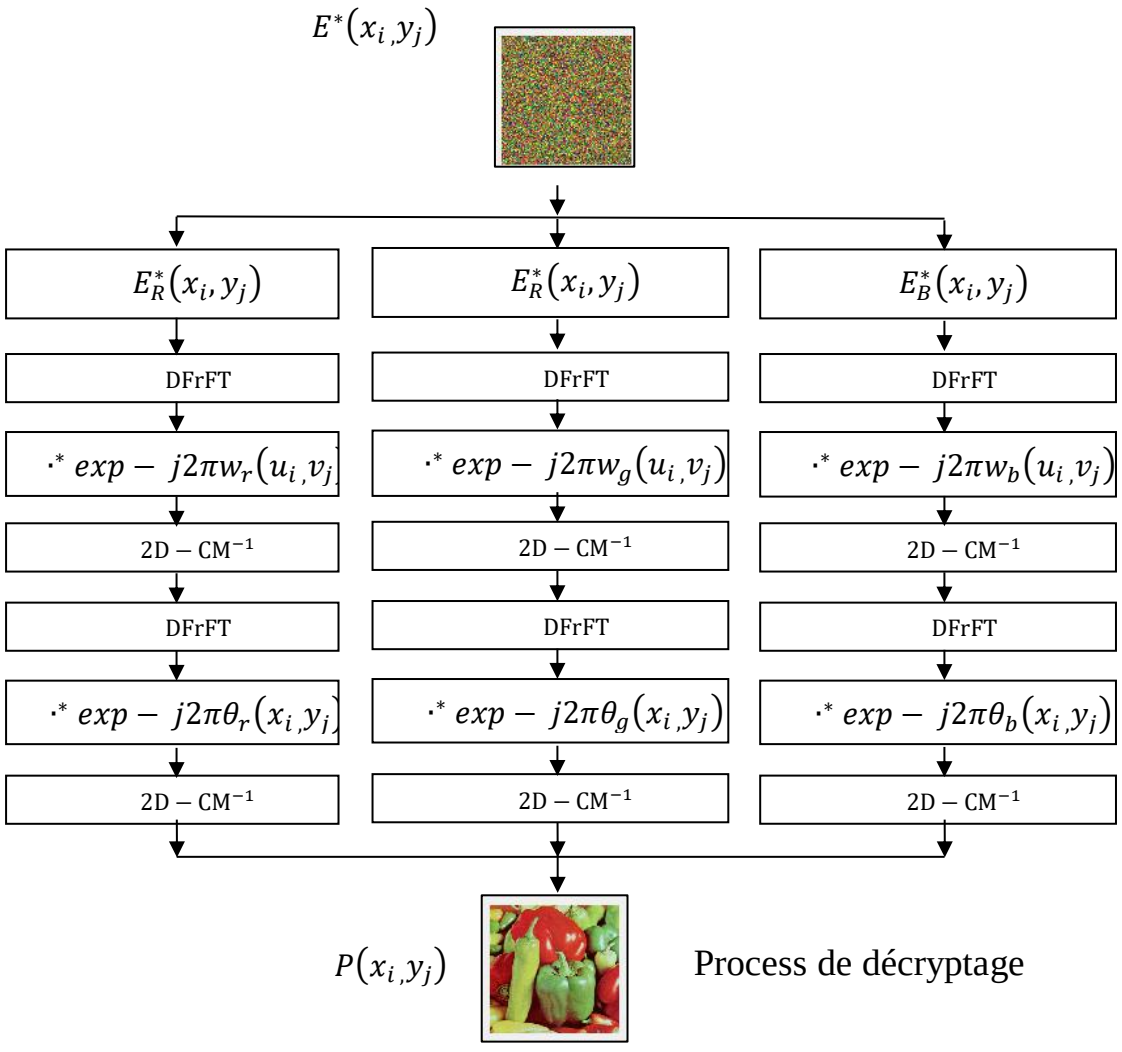


Figure 3.3 Algorithme de simulation en décryptage.

3.4 Résultats des simulations

3.4.1 Analyse visuelle.

L'analyse visuelle est une méthode d'évaluation de la qualité du cryptage qui repose sur l'observation directe des images cryptées. Bien qu'elle soit moins avancée sur le plan technologique par rapport à d'autres méthodes, elle est considérée comme la plus simple et intuitive. Dans le contexte du cryptage d'images couleur, cette méthode consiste à examiner les images cryptées et à évaluer la conservation des détails visuels ainsi que l'uniformité du chiffrement à travers les différents composantes couleur (rouge, vert, bleu) et l'image RVB globale.

En utilisant cette approche, les résultats obtenus pour les images de test (telles que Barbra, Peppers et Airplane) à l'aide du système de cryptage d'images couleurDFrFT basé sur 2D_CM sont présentés visuellement dans des figures spécifiques.

Pour chaque image, chaque composante de couleur (rouge, vert, bleu) a été codée individuellement à l'aide du système proposé, et les résultats sont affichés visuellement dans les Figures 3.4, 3.5 et 3.6

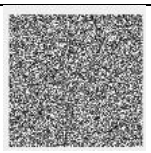
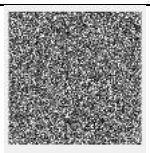
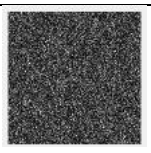
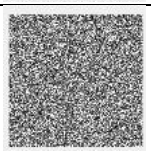
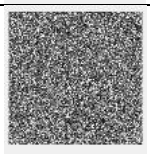
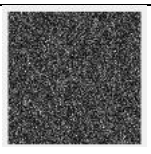
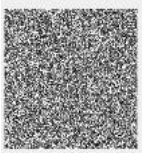
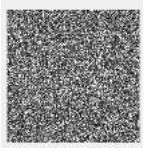
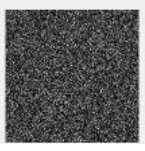
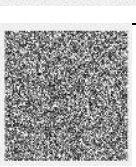
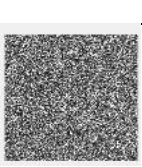
Peppers	R	G	B	RGB
CM1 + DFrFT				
CM2 + DFrFT				
CM3 + DFrFT				
CM4 + DFrFT				

Figure 3.4 Résultats de simulation du cryptage de l'image couleur « Peppers »

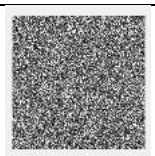
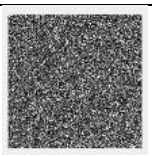
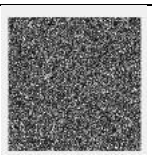
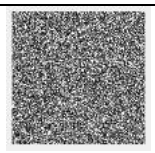
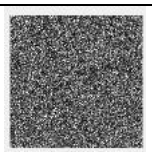
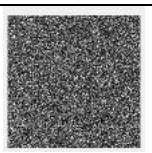
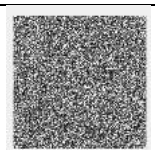
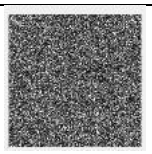
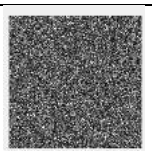
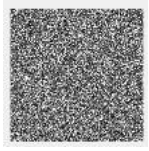
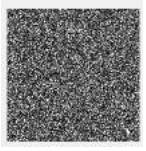
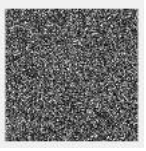
Barbara	R	G	B	RGB
CM1 + DFrFT				
CM2 + DFrFT				
CM3 + DFrFT				
CM4 + DFrFT				

Figure 3.5 Résultats de simulation du cryptage de l'image couleur « Barbara »

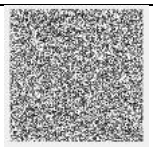
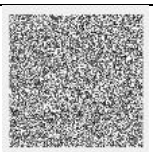
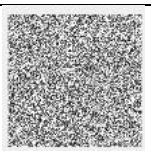
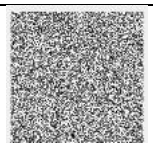
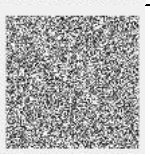
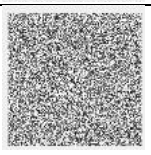
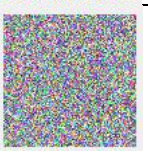
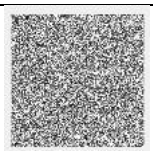
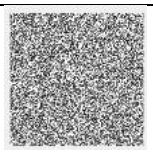
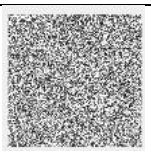
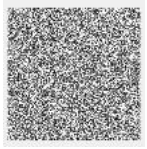
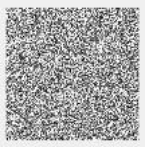
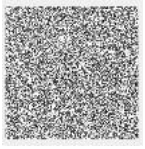
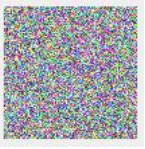
Airplane	R	G	B	RGB
CM1 + DFrFT				
CM2 + DFrFT				
CM3 + DFrFT				
CM4 + DFrFT				

Figure 3.6 Résultats de simulation du cryptage de l'image couleur « Airplane »

La comparaison entre différentes suites dans le cadre de l'analyse visuelle dépend de deux éléments principaux :

- **Masquage des Détails Visuels** : La capacité du système de cryptage à rendre les détails de l'image originale méconnaissables dans les images cryptées.
- **Uniformité du cryptage** : La cohérence de la qualité du cryptage à travers les trois composants de couleur (rouge, vert, bleu) ainsi que dans l'image RGB globale.

- **CM1**: Les images cryptées montrent une bonne dissimulation des détails, rendant les images originales reconnaissables avec consistance dans le masquage des détails pour tous les composants de couleur et l'image RGB.
- **CM2** : Comparable à CM1, mais une évaluation minutieuse est nécessaire pour identifier de légères différences. Avec bonne consistance, similaire à CM1.
- **CM3** : Efficace, mais pourrait présenter des différences subtiles dans la dissimulation des détails par rapport à CM1 et CM2.Avec Cohérente, mais de légères variations peuvent exister.
- **CM4** : Très similaire aux autres configurations, mais des tests plus détaillés sont nécessaires pour identifier des distinctions fines. Avec Uniformité comparable, bien que des variations minimes puissent être présentes

Toutes les suites semblent offrir des performances similaires en dissimulant les détails des images originales "Peppers", "Barbara" et "Airplane". L'analyse a porté sur divers aspects, notamment le masquage des détails et l'uniformité du cryptage des images.

3.4.2 Analyse par histogramme

L'analyse des histogrammes consiste à visualiser la répartition des intensités des pixels dans une image en comptant le nombre de pixels associés à chaque niveau d'intensité. Pour les images en couleur RGB, cette analyse est réalisée séparément pour chaque canal de couleur. Dans le cas des images cryptées en RGB, cryptées à l'aide du schéma de cryptage d'images couleur DFrFT basé sur 2D_CM, les histogrammes sont affichés dans les figures 3.7 , 3.8 et 3.9 .

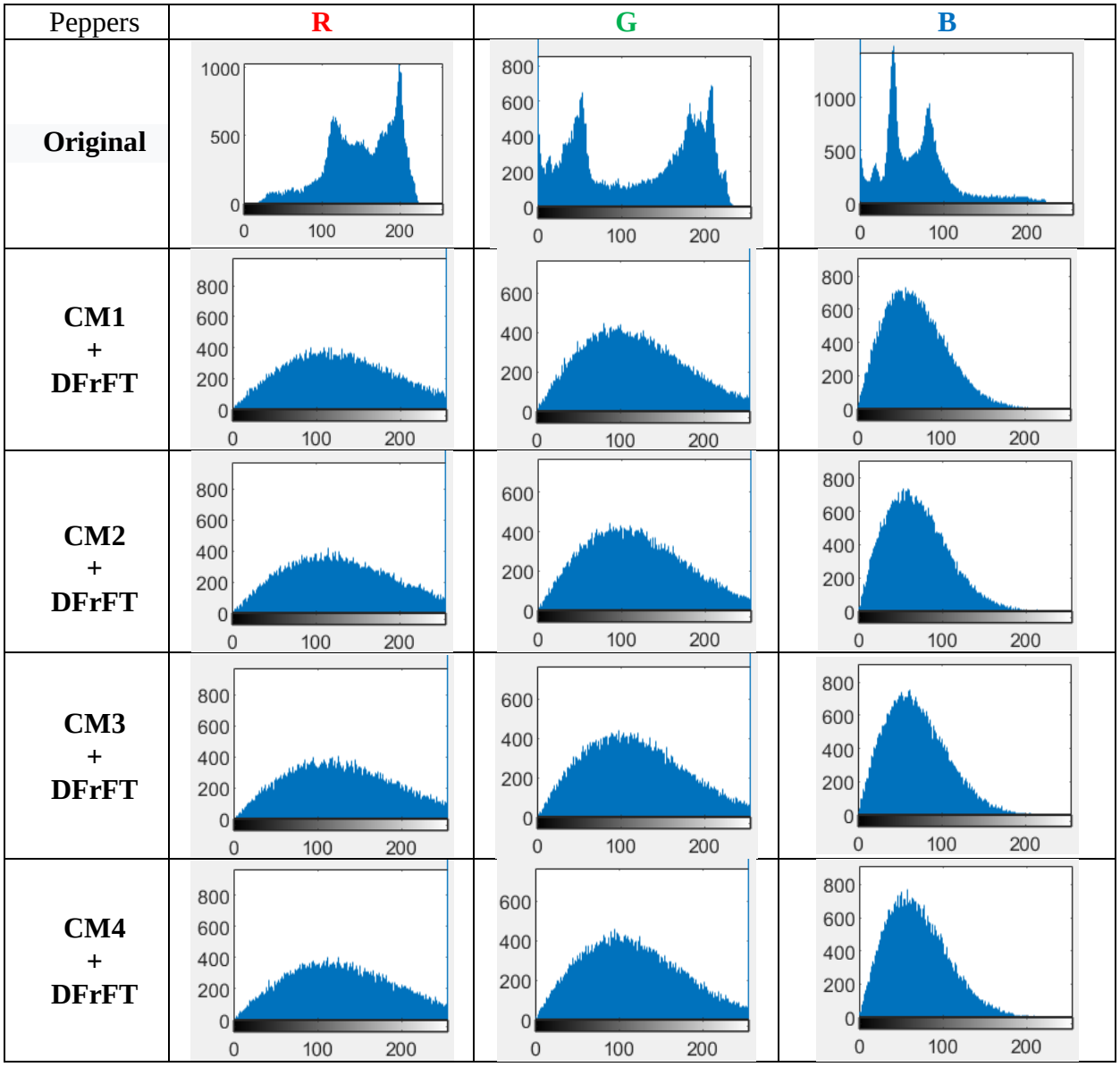


Figure 3.7 Résultats de comparaison de l'analyse histogramme de l'image cryptée « Peppers ».

Étant donné que le schéma de cryptage 2D-CM ne fait que permuter les pixels sans modifier leurs valeurs, on s'attend à ce que les histogrammes des images cryptées couleur obtenues avec cette méthode soient presque identiques à ceux de leurs images originales correspondantes. Cependant, lorsque la DFrFT optique et le schéma de cryptage d'images couleur DFrFT basé sur 2D_CM sont utilisés, les valeurs des pixels sont modifiées en raison d'un processus de diffusion.

Par conséquent, les histogrammes des images cryptées couleur, comme illustré dans Les mêmes Figures, sont nettement différents de ceux de leurs images originales correspondantes présentées dans les mêmes Figures aussi. La distinction entre les histogrammes des images cryptées et ceux des images originales confirme l'efficacité du schéma de cryptage d'images couleur DFrFT basé sur 2D_CM proposé.

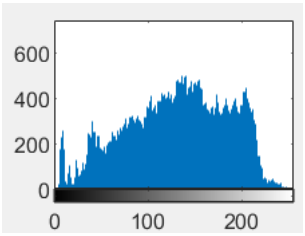
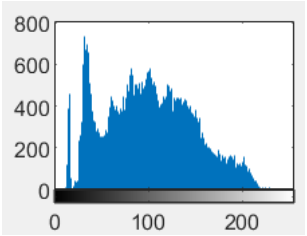
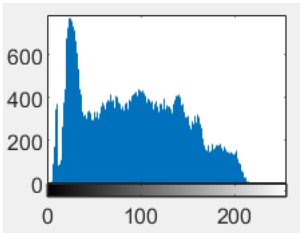
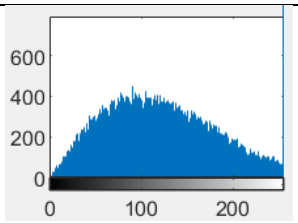
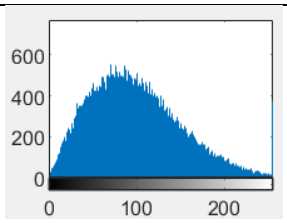
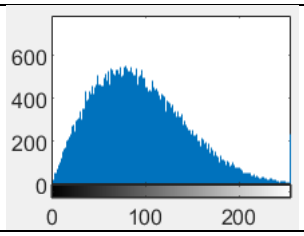
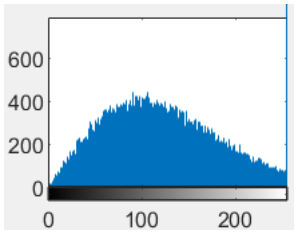
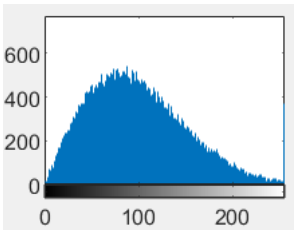
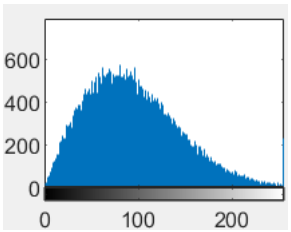
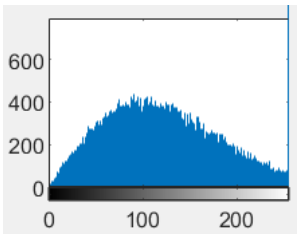
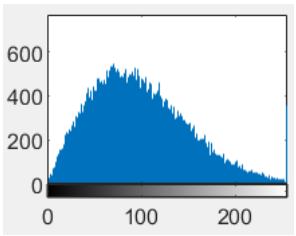
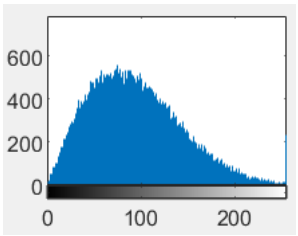
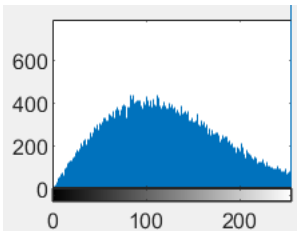
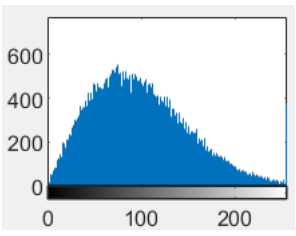
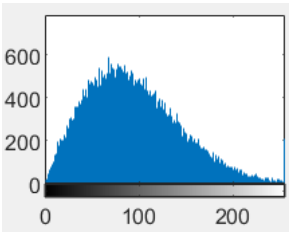
Barbara	**R**	**G**	**B**
Original			
CM1 + DFrFT			
CM2 + DFrFT			
CM3 + DFrFT			
CM4 + DFrFT			

Figure 3.8 Résultats de comparaison de l'analyse histogramme de l'image cryptée « Barbara ».

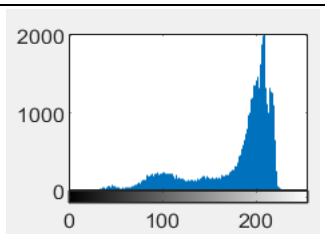
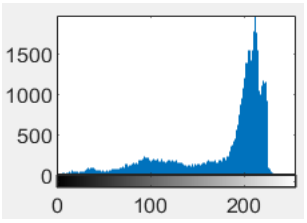
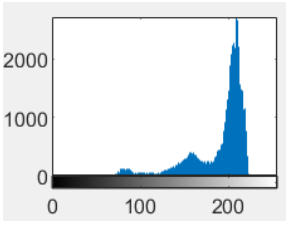
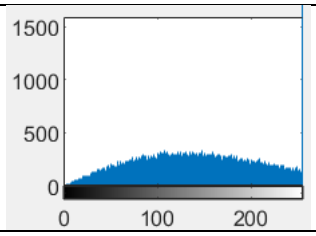
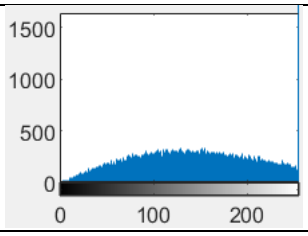
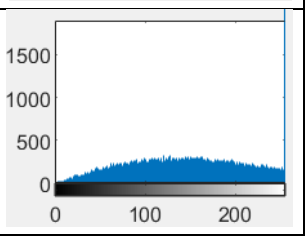
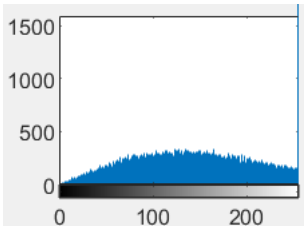
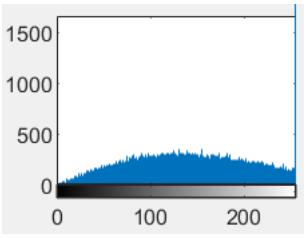
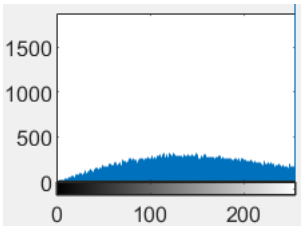
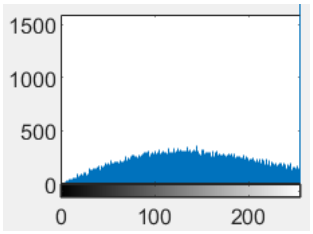
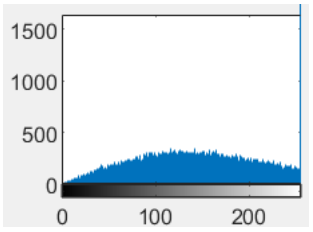
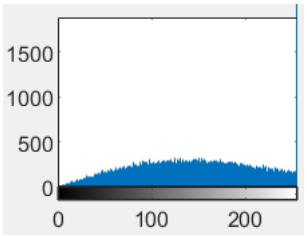
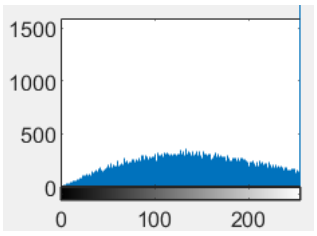
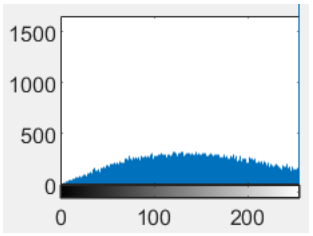
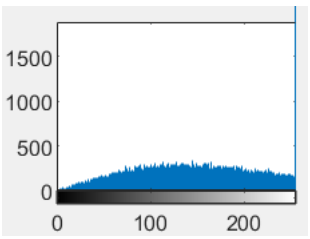
Airplane	R	G	B
Original			
CM1 + DFrFT			
CM2 + DFrFT			
CM3 + DFrFT			
CM4 + DFrFT			

Figure 3.9 Résultats de comparaison de l'analyse histogramme de l'image cryptée « Airplane ».

La comparaison des quatre suites en termes de résultats de l'analyse d'histogramme repose sur quatre critères :

- **Écart complet par rapport à l'image originale :** CM1, CM2, CM3, CM4 : Toutes les suites produisent des histogrammes d'images cryptée présentant une différence totale par rapport aux images originales, couvrant l'ensemble des canaux de couleur.

- **Préservation des valeurs des pixels :** CM1, CM2, CM3, CM4 : Chaque suite maintient les valeurs des pixels inchangées pendant la permutation, assurant ainsi l'intégrité des données
- **Capacité à résister aux attaques statiques :** CM1, CM2, CM3, CM4 : Les modifications apportées par chaque suite rendent les histogrammes des images cryptées suffisamment différents pour résister efficacement aux attaques statiques.
- **Performances en matière de cryptage :** CM1, CM2, CM3, CM4 : Toutes les suites produisent des histogrammes cryptés distincts des images originales, bien que comparables entre elles, démontrant ainsi des performances équivalentes en termes de cryptage.

En résumé, bien que chaque suite présente des nuances dans ses performances, toutes se révèlent efficaces pour le cryptage des images, avec des résultats visuels similaires et une résistance adéquate aux attaques statiques. Cependant, des tests supplémentaires pourraient être nécessaires pour déterminer la suite la plus performante dans des cas d'utilisation spécifiques

3.4.3 Test d'Entropie :

L'entropie est une mesure de la quantité d'incertitude ou de chaos dans un ensemble de données. Dans le contexte de l'analyse d'images, l'entropie est utilisée pour évaluer les détails de l'image et comparer l'intensité des détails entre différentes images

$$E_{R/G/B}(x) = -\sum_{i=1}^{2^N-1} P_{(x_i)} log_2 P_{(x_i)} \qquad (3.1)$$

Une entropie proche de 8 dans un schéma de cryptage d'images signifie que l'image est totalement différente de l'originale, reflétant un haut niveau d'aléatoire. Cela indique que les valeurs de pixels sont réparties de manière uniforme, couvrant toutes les nuances de couleur possibles.

Tableau 3.3 Résultats de comparaison de l'entropie des composantes RVB des images cryptées.

Images		Image original	CM1	CM2	CM3	CM4
Peppers	R	**7.3009**	**7.6670**	**7.6630**	**7.6621**	**7.6651**
	G	**7.5570**	**7.7519**	**7.7498**	**7.7497**	**7.7498**
	B	**7.0929**	**7.1711**	**7.1656**	**7.1706**	**7.1702**
Barbara	R	**7.6702**	**7.7441**	**7.7470**	**7.7485**	**7.7446**
	G	**7.4582**	**7.6281**	**7.6277**	**7.6315**	**7.6282**
	B	**7.5363**	**7.5798**	**7.5768**	**7.5717**	**7.5757**
Airplane	R	**6.7254**	**7.3261**	**7.3274**	**7.3324**	**7.3255**
	G	**6.8253**	**7.2905**	**7.3018**	**7.2920**	**7.2985**
	B	**6.2078**	**7.1642**	**6.2078**	**7.1520**	**7.1570**

- **CM1** : Cette suite semble fournir des valeurs d'entropie plus élevées que les autres méthodes pour la plupart des composants RVB et des images. Cela peut indiquer une meilleure distribution des valeurs, ce qui peut contribuer à une meilleure sécurité de l'image.

- **CM2** :Cette suite semble avoir des valeurs d'entropie légèrement faible que CM4, mais généralement faibles que CM1 et CM3. Cela pourrait signifier une moins bonne distribution des valeurs, ce qui pourrait affecter la sécurité de l'image.

- **CM3** : Les valeurs d'entropie de cette suite sont généralement légèrement plus basses que celles de CM1, mais restent relativement élevées. Cela suggère également une bonne répartition des valeurs dans l'image

- **CM4** : Les valeurs d'entropie de CM4 sont comparables à celles de CM2, avec peut-être une légère tendance à être légèrement plus faibles. Cela pourrait indiquer une légère perte d'information par rapport aux méthodes CM1 et CM3

CM1 offre les valeurs d'entropie les plus élevées, suggérant une meilleure distribution des valeurs et donc une meilleure sécurité de l'image, suivi de près par CM3 avec des valeurs d'entropie légèrement plus basses mais toujours élevées. CM4 et CM2 montrent des performances légèrement inférieures en termes d'entropie, avec CM2 ayant les valeurs les plus basses parmi les quatre. En résumé, CM1 semble offrir les meilleures performances en termes d'entropie, suivi de près par CM3, tandis que CM4 et CM2 montrent des performances légèrement inférieures, avec CM2 ayant les valeurs d'entropie les plus basses parmi les quatre méthodes.

3.4.4 Test de Corrélation :

Le coefficient de corrélation est utilisé pour évaluer l'efficacité du cryptage d'une image. En considérant une image originale X et sa version cryptée Y, le coefficient de corrélation entre ces deux images, noté $\boldsymbol{r_{XY}}$, est calculé de la manière suivante :

$$\boldsymbol{r_{XY}} = \frac{\boldsymbol{cov(x,y)}}{\sqrt{\boldsymbol{D(X)}}\sqrt{\boldsymbol{D(Y)}}} \quad (3.2)$$

Où cov (x, y) est la covariance. D(x) et D(y) sont la variance de X et Y avec :

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

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

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

Où L le nombre de pixels de l'image et E l'espérance X.

Dans ce cas, la qualité du chiffrement est optimale lorsque le coefficient de corrélation entre l'image originale X et l'image cryptée Y est proche de zéro.

Tableau 3.4 Résultats de comparaison du coefficient de corrélation des images couleurs cryptées

IMAGES		CM1+DFrFT			CM2+DFrFT			CM3+DFrFT			CM4+DFrFT		
		R	G	B	R	G	B	R	G	B	R	G	B
Peppers	**r(x,y)**	**-0.0070**	**0.0027**	**-0.0022**	**-0.0029**	**-0.0072**	**0.0028**	**0.0048**	**0.0028**	**0.0027**	**-0.0027**	**-0.0031**	**-0.0079**
Barbara	**r(x,y)**	**0.0044**	**0.0010**	**-0.0025**	**0.0024**	**-0.0022**	**-0.0011**	**-0.0014**	**0.0040**	**0.0036**	**0.0072**	**-0.006**	**-0.0020**
Airplane	**r(x,y)**	**0.0019**	**-0.0015**	**0.0011**	**0.0056**	**0.0056**	**-0.0057**	**0.0053**	**-0.0014**	**0.0032**	**0.0014**	**0.0064**	**0.0088**

En résumé, les différences entre les suites CM1, CM2, CM3 et CM4 sont principalement liées à la dispersion des données dans les images analysées. Les suites CM1 et CM3 tendent à présenter une dispersion plus uniforme des données, tandis que CM2 et CM4 montrent parfois une dispersion légèrement plus élevée. Cependant, dans l'ensemble, ces différences sont subtiles et dépendent de la nature spécifique de chaque image analysée.

Donc, la suite CM1 démontre une meilleure dispersion des données, avec la suite CM3 suivant de près. Concernant l'ordre de classement des suites en fonction de leur capacité à exprimer cette dispersion, CM1 se positionne en première place, suivie de CM3, puis de CM4, et enfin de CM2.

3.4.5 Résistance aux bruits

La qualité des images et l'efficacité de la robustesse du système de cryptage d'images couleur DFrFT basé sur les : 2D_CM proposer ont été évaluées en présence de bruits de canal, en utilisant le rapport signal sur bruit (PSNR).

Le PSNR (Peak Signal to Noise Ratio), en décibels (dB), est utilisé pour évaluer la qualité visuelle d'une image. Considérons une version cryptée ou bruitée I' d'une image originale non-cryptée et non-bruitée I.

Dans ce cas, le PSNR entre l'image originale et l'image cryptée est calculé de la manière suivante :

$$\boldsymbol{PSNR_{R/G/B} = 10\ \log 10\left[\frac{(255^2)}{EQM(I', I)}\right]} \quad (3.6)$$

En résumé, le PSNR est une mesure de la qualité d'une image, où des valeurs plus élevées indiquent une meilleure qualité. Le lien avec le MSE est inverse : un MSE plus petit conduit à un PSNR plus grand, et vice versa. C'est pourquoi on considère souvent le PSNR comme une mesure de la qualité, où des valeurs plus élevées sont préférées.

Les effets du bruit gaussien additif (AWGN), du bruit (SALT & PEPPER) , ainsi que du bruit ponctuel (SPECKLE) ont été testés et analysés. Ces types de bruits ont été conçus pour simuler la contamination des images cryptées.

Dans nos simulations, chaque type de bruit a été testé individuellement, avec exemple de deux valeurs d'intensité (0.05, 0.15), afin d'examiner et d'évaluer leur efficacité et leur impact sur la qualité des images cryptées.

Le bruit gaussien additif (AWGN), le bruit (SALT & PEPPER) , ainsi que le bruit ponctuel (SPECKLE) ont été testés sur l'image "Barbra" uniquement tandis que le bruit gaussien additif (AWGN) a été testé sur toutes les images.

Le bruit gaussien additif (AWGN) a été appliqué à toutes les images pour l'évaluation, tandis que le bruit sel et poivre (SALT &PEPPER) ainsi que le bruit ponctuel (SPECKLE) ont été exclusivement évalués sur l'image "Barbra" afin d'éviter une répétition seulement.

3.4.5.1. Résultats bruit blanc gaussien additif « AWGN »

IMAGE		CM1+DFrFT		CM2+DFrFT		CM3+DFrFT		CM4+DFrFT	
		0.05	0.15	0.05	0.15	0.05	0.15	0.05	0.15
Peppers	R	33.2602	23.7752	33.2659	23.7337	33.2857	23.7264	33.2970	23.8014
	G	34.1747	24.7053	34.2115	24.6672	34.1831	24.6298	34.2277	24.7407
	B	38.9753	29.4018	38.9496	29.4334	38.9858	29.4573	38.9631	29.4857
Barbara	R	34.0965	24.6348	34.1379	24.6254	34.1341	24.7275	34.1730	24.6521
	G	36.1095	26.7123	36.1439	26.7329	36.1110	26.6914	36.1489	26.7260
	B	36.5208	27.1777	36.5404	27.1545	36.5538	27.1507	36.5763	27.1752
Airplane	R	31.8848	22.5001	31.8853	22.4571	31.8873	22.4552	31.9089	22.4627
	G	31.8275	22.4207	31.7735	22.4205	31.8410	22.3340	31.9037	22.3972
	B	31.4389	22.0634	31.4155	22.0368	31.4143	21.9772	31.5147	21.9722

Tableau 3.5 Résultats comparaison du PSNR des images décryptées en présence de bruit « AWGN. »

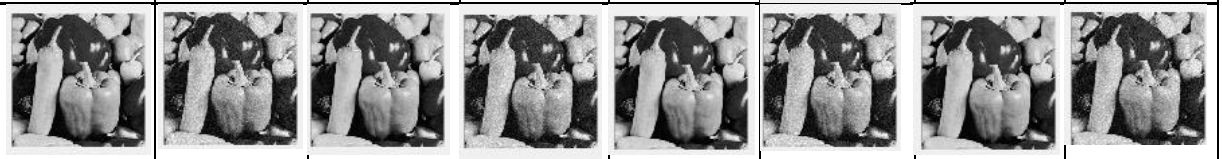
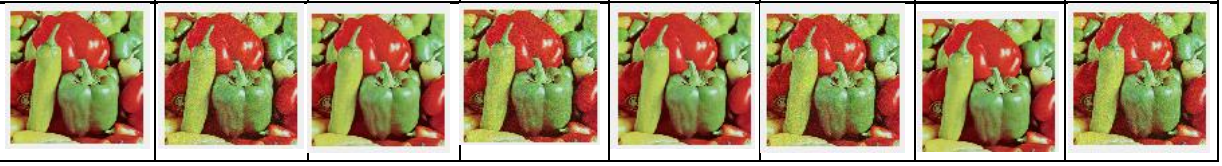
	AWGN							
	CM1		CM2		CM3		CM4	
	0.05	0.15	0.05	0.15	0.05	0.15	0.05	0.15
R								
G								
B								
RGB								

Figure 3.10 Résultats visuels du décryptage de l'image « Peppers » en présence de bruit « AWGN»

	AWGN							
	CM1		CM2		CM3		CM4	
	0.05	0.15	0.05	0.15	0.05	0.15	0.05	0.15
R								
G								
B								
RGB								

Figure 3.11 Résultats visuels du décryptage de l'image « Barbara » en présence de bruit « AWGN. »

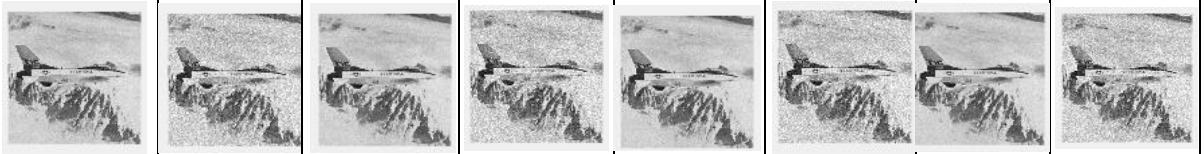
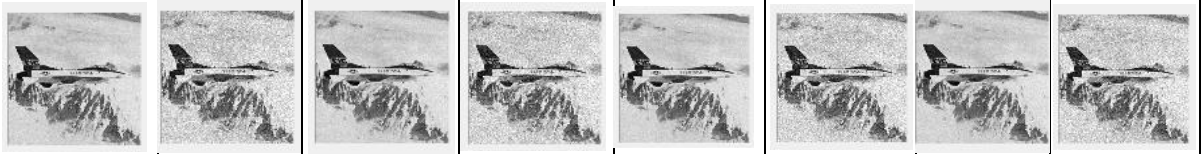
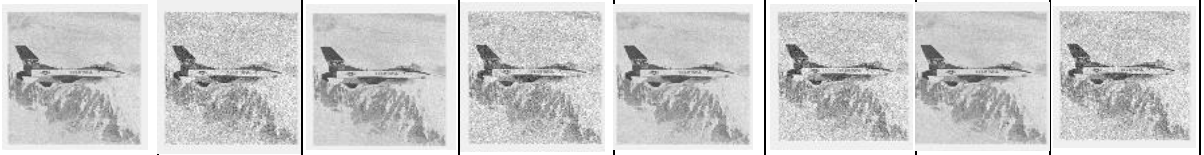
	AWGN							
	CM1		CM2		CM3		CM4	
	0.05	0.15	0.05	0.15	0.05	0.15	0.05	0.15
R								
G								
B								
RGB								

Figure 3.12 Résultats visuels du décryptage de l'image « Airplane » en présence de bruit « AWGN. »

- Pour la composante R, les valeurs PSNR sont généralement plus élevées avec CM1 et CM3 par rapport à CM2 et CM4. Cela suggère que CM1 et CM3 offrent une meilleure qualité d'image pour cette composante.
- Pour la composante G, CM1 et CM3 ont à nouveau des valeurs PSNR plus élevées, indiquant une meilleure qualité d'image par rapport à CM2 et CM4.
- Pour la composante B, CM1 et CM3 montrent également des valeurs PSNR plus élevées, ce qui indique une meilleure qualité d'image par rapport à CM2 et CM4.

Les tendances observées pour Barbara sont similaires à celles de Peppers. CM1 et CM3 montrent des valeurs PSNR plus élevées pour toutes les composantes, indiquant une meilleure qualité d'image par rapport à CM2 et CM4. Pour Airplane, les différences entre les méthodes de cryptage sont moins prononcées, mais on observe toujours une tendance similaire. CM1 et CM3 montrent généralement des valeurs PSNR légèrement plus élevées que CM2 et CM4 pour toutes les composantes.

3.4.5.2. Résultats bruit « SPECKLE »

Image		CM1		CM2		CM3		CM4	
		0.05	0.15	0.05	0.15	0.05	0.15	0.05	0.15
Barbra	R	12.4277	11.5210	12.4010	11.4899	12.3429	14.7913	12.4284	11.5006
	G	17.5663	14.9369	17.2044	14.8322	17.4387	14.7913	17.3810	14.7973
	B	18.6149	15.3505	18.4640	15.4086	18.6366	15.3433	18.6479	15.3622

Tableau 3.6 Résultats de comparaison PSNR des images en présence de bruit « Speckle »

Pour toutes les composantes de couleur (R, G, B), CM1 a tendance à avoir des valeurs PSNR légèrement plus élevées que les autres suites.

CM2 et CM4 ont tendance à avoir des valeurs PSNR légèrement plus faibles que CM1 et CM3, mais les différences sont généralement minimes.

CM3 et CM4 peuvent avoir des valeurs PSNR légèrement plus élevées que CM2 dans certaines composantes de couleur, mais cela peut varier.

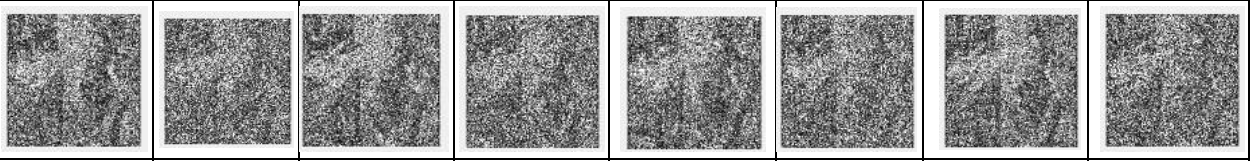
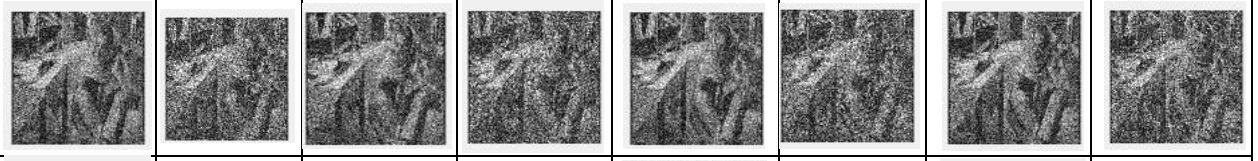
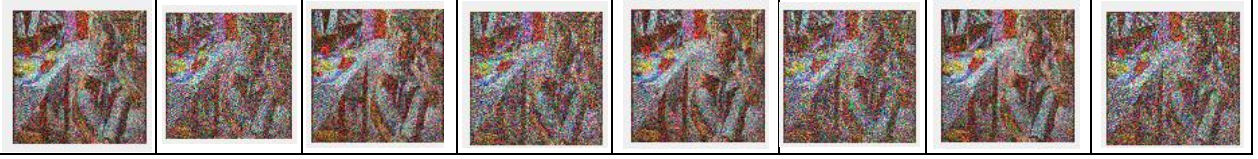
	SPECKLE							
	CM1		CM2		CM3		CM4	
	0.05	0.15	0.05	0.15	0.05	0.15	0.05	0.15
R								
G								
B								
RGB								

Figure 3.13 Résultats visuels du décryptage de l'image « Barbara » en présence de bruit « SPECKLE. »

3.4.5.3. Résultats bruit « SALT & PEPPER »

Image		CM1		CM2		CM3		CM4	
		0.05	0.15	0.05	0.15	0.05	0.15	0.05	0.15
Barbra	R	13.0868	11.6975	13.0862	11.7377	13.2061	11.7472	13.0563	11.7053
	G	16.9540	13.5278	16.8918	13.3872	16.9430	13.5286	17.1983	13.4833
	B	17.3517	13.3815	17.2911	13.4570	17.4691	13.3861	17.2576	13.4241

Tableau 3.7 Résultats comparaison PSNR des images en présence de bruit « SALT &PEPPER »

Pour toutes les composantes de couleur (R, G, B), CM1 a tendance à avoir des valeurs PSNR légèrement plus élevées que les autres suites.

CM2 et CM4 ont tendance à avoir des valeurs PSNR légèrement plus faibles que CM1 et CM3, mais les différences sont généralement minimes.

CM3 et CM4 peuvent avoir des valeurs PSNR légèrement plus élevées que CM2 dans certaines composantes de couleur.

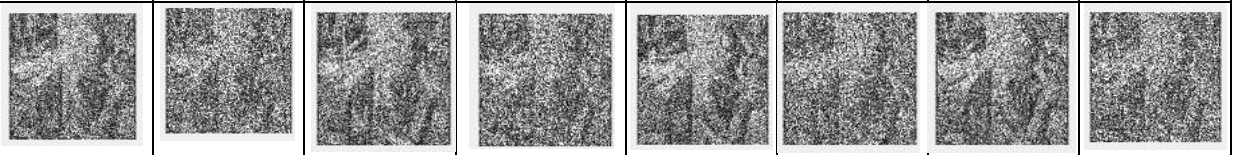
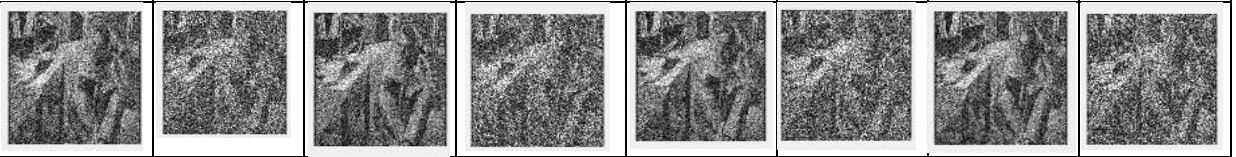
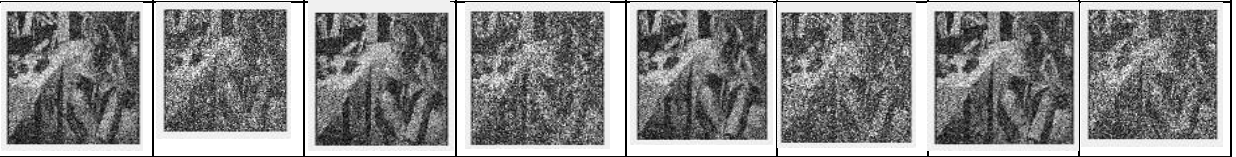
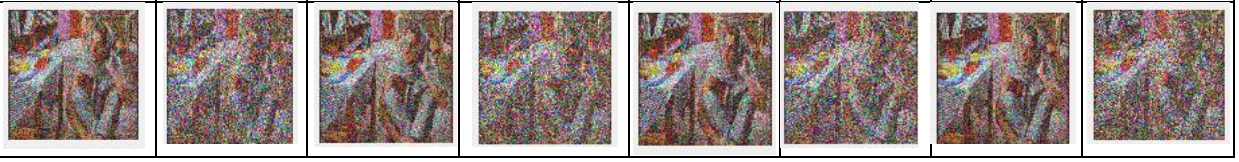
	SALT & PEPPER							
	CM1		CM2		CM3		CM4	
	0.05	0.15	0.05	0.15	0.05	0.15	0.05	0.15
R								
G								
B								
RGB								

Figure 3.14 Résultats visuels du décryptage de l'image « Barbara » en présence de bruit « Speckle. »

Au final, les observations suivantes peuvent être faites :

Pour le bruit "AWGN" :

- Pour les images "Peppers" et "Barbara", CM1 et CM3 montrent généralement des valeurs PSNR plus élevées pour toutes les composantes de couleur (R, G, B) par rapport à CM2 et CM4.
- Pour l'image "Airplane", les différences entre les méthodes de cryptage sont moins prononcées, mais CM1 et CM3 tendent à avoir des valeurs PSNR légèrement plus élevées que CM2 et CM4.

Pour le bruit "SPECKLE" :

- Pour toutes les composantes de couleur, CM1 a tendance à avoir des valeurs PSNR légèrement plus élevées que les autres suites.
- CM2 et CM4 montrent des valeurs PSNR légèrement plus faibles que CM1 et CM3, bien que les différences soient généralement minimes.

Pour le bruit "SALT &PEPPER " :

- Pour toutes les composantes de couleur, CM1 a tendance à avoir des valeurs PSNR légèrement plus élevées que les autres suites.
- CM2 et CM4 ont tendance à avoir des valeurs PSNR légèrement plus faibles que CM1 et CM3, mais les différences sont généralement minimes.
- CM3 et CM4 peuvent avoir des valeurs PSNR légèrement plus élevées que CM2 dans certaines composantes de couleur, mais cela peut varier.

En résumé, CM1 montre généralement les meilleures performances en termes de résistance au bruit, suivie de CM3, CM4, et enfin CM2. Cependant, il est important de noter que ces tendances peuvent varier en fonction des caractéristiques spécifiques de l'image et du bruit.

3.4.6 Tests NPCR et UACI

Le NPCR (Normalized Pixel Change Rate) et l'UACI (Unified Average Changing Intensity) sont des mesures utilisées pour évaluer la robustesse des systèmes de cryptage d'images. Le NPCR mesure le pourcentage de pixels qui changent de valeur entre une image chiffrée et une autre, tandis que l'UACI mesure l'intensité moyenne de ces changements.

Dans l'idéal, le $NPCR_{R/G/B}$ devrait être de 99,60 % et$L'UACI_{R/G/B}$ devrait être de 33,33 %. Ces valeurs idéales indiquent un haut degré de variation des pixels avec une faible variation de l'intensité moyenne, ce qui est souhaitable pour la sécurité du cryptage.

$$\boldsymbol{UACI_{R/G/B}} = \frac{\mathbf{1}}{\boldsymbol{W \times H}} \left[\sum_{\boldsymbol{i=1}}^{\boldsymbol{W}} \sum_{\boldsymbol{j=1}}^{\boldsymbol{H}} \frac{\boldsymbol{C_{1R/G/B}(i,j) - C_{2R/G/B}(i,j)}}{\mathbf{255}} \right] \times \mathbf{100\%} \quad (3.7)$$

$$\boldsymbol{NPCR_{R/G/B}} = \frac{\sum_{\boldsymbol{i=1}}^{\boldsymbol{W}} \sum_{\boldsymbol{j=1}}^{\boldsymbol{H}} \boldsymbol{D_{R/G/B}(i,j)}}{\boldsymbol{W \times H}} \times \mathbf{100}\ \% \quad (3.8)$$

- **CM1** : Cette suite semble fournir des valeurs de NPCR et UACI légèrement plus élevées que les autres suites pour la plupart des canaux RVB et des images. Cela peut indiquer une meilleure conservation des caractéristiques de l'image et une distribution plus uniforme des valeurs, contribuant ainsi à une meilleure sécurité de l'image.

- **CM2** : Les valeurs NPCR et UACI du CM2 sont les plus basses par rapport aux autres séries. Cela peut indiquer une perte d'informations et donc de moins bonnes performances en termes de sécurité des images.
- **CM3** : Les valeurs de NPCR et UACI de cette suite sont généralement légèrement inférieures à celles de CM1, mais restent relativement élevées. Cela suggère également une bonne conservation des caractéristiques de l'image et une distribution raisonnable des valeurs dans l'image.
- **CM4** : Cette suite semble avoir des valeurs de NPCR et UACI légèrement plus faibles que CM3, mais généralement plus élevées que CM2. Cela pourrait signifier une légère dégradation de la conservation des caractéristiques de l'image et une distribution moins uniforme des valeurs, ce qui pourrait affecter légèrement la sécurité de l'image.

IMAGES		CM1+DFrFT			CM2+DFrFT			CM3+DFrFT			CM4+DFrFT		
		R	G	B	R	G	B	R	G	B	R	G	B
PEPPERS	NPCR	99.4431	99.6490	99.2737	99.4568	99.3469	97.7875	99.5773	99.6674	99.2538	99.5544	99.6552	99.2599
	UACI	39.0350	39.0350	39.0350	38.9931	38.9237	38.3803	39.0499	39.0852	38.9231	39.0410	39.0805	38.9255
BARBARA	NPCR	99.2737	*99.4598*	*99.4446*	*99.2722*	*98.6542*	*98.2864*	99.5590	99.4339	99.4263	99.5682	99.4629	99.5071
	UACI	39.0428	39.0428	39.0428	38.9303	38.6879	38.5437	39.0428	38.9937	38.9907	39.0463	39.0051	39.0224
AIRPLANE	NPCR	*99.6323*	*99.6338*	*99.6231*	*99.5102*	*99.5560*	*99.6582*	99.6582	99.6552	99.6628	99.6353	99.6597	99.5926
	UACI	39.0715	39.0715	39.0715	39.0236	39.0416	39.0816	39.0816	39.0805	39.0834	39.0727	39.0822	39.0559

Tableau 3.8 Résultats NPCR et UACI

D'après cette analyse, il semble que la suite le plus efficace soit CM1. Cette dernière affiche généralement des valeurs de NPCR et UACI légèrement plus élevées que les autres suites pour la plupart des canaux RVB et des images, ce qui suggère une meilleure préservation des caractéristiques de l'image et une distribution plus uniforme des valeurs, contribuant ainsi à améliorer la sécurité de l'image. Malgré des performances similaires à CM1, les suites CM3 et CM4 montrent des valeurs légèrement inférieures de NPCR et UACI. En revanche, CM2 présente généralement des valeurs de NPCR et UACI légèrement plus faibles que les autres, le plaçant ainsi en dernière position parmi les suites mentionnées.

3.4.7 Sensibilité de la clé

Dans le domaine spatial, la sensibilité de la clé décryptage est évaluée en effectuant de légères modifications sur l'un des éléments constitutifs de la clé, que ce soit pour les paramètres de contrôle ou les valeurs initiales sélectionnées, de manière à ce qu'elle produise, lors de la phase de décryptage, une image entièrement cryptée.

Nous augmentons progressivement la précision de cette modification pour chaque canal de couleur jusqu'à ce que l'image décryptée soit clairement visible. Ce seuil nous donne la précision de l'élément constituant cette clé.

Cette procédure est répétée pour tous les éléments de la clé. Dans le domaine fréquentiel, basé sur les transformations paramétriques, nous introduisons progressivement une petite erreur autour des paramètres de la transformation pour différentes fréquences, et nous calculons le MSE (L'erreur quadratique moyenne) correspondant. L'ouverture relative à l'apparition de l'image correspond exactement à la précision du paramètre en question.

La précision de tous les éléments constituant la clé de chiffrement déterminera l'espace de clé de l'algorithme qui se base al les suites mentionnées proposé.

Pour évaluer la sensibilité de la clé dans un système de cryptage, on utilise généralement l'erreur quadratique moyenne MSE (Mean Squared Error). Tel que L'MSE est une mesure qui quantifie la différence moyenne entre les valeurs réelles et les valeurs prédites.

Pour calculer l'erreur quadratique moyenne (MSE) dans le contexte du cryptage, on compare les images originales avec les images décryptées à l'aide de différentes clés. Plus l'MSE est faible, plus les images décryptées sont similaires aux images originales, ce qui indique une meilleure sensibilité de la clé.

Mathématiquement, l'MSE est calculée en prenant la moyenne des carrés des différences entre les pixels des images originales et les pixels des images décryptées, pour tous les pixels de l'image :

$$\boldsymbol{MSE(I', I) = \frac{1}{N \times M} \sum_{n=1}^{N} \sum_{m=1}^{M} \left(I'(n, m) - I(n, m) \right)^2} \quad (3.9)$$

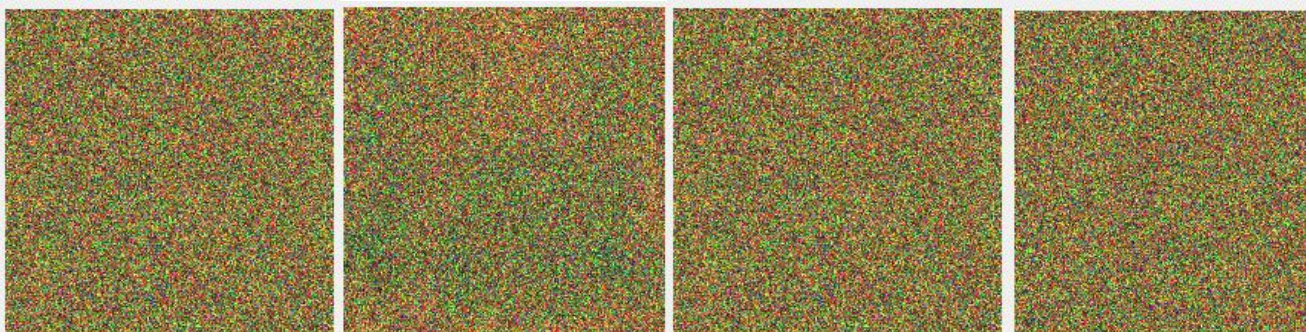
Ou

- N : représente le nombre de lignes dans la matrice de l'image.
- M : représente le nombre de colonnes dans la matrice de l'image.
- I′(n, m) est la valeur du pixel à la position (n, m) dans l'image reconstruite I′.
- I(n,m) est la valeur du pixel a la position (n ,m) dans l'image originale I.

Plus l'MSE est proche de zéro, plus les images décryptées sont fidèles aux images originales, ce qui indique une clé sensible et efficace.

En revanche, un MSE plus élevé indique des différences significatives entre les images originales et les images décryptées, suggérant une clé moins sensible ou des problèmes de cryptage.

Au niveau pratique, on ajuste progressivement les valeurs des paramètres de contrôle pour toutes les suites 2D avec erreur δ. Nous avons commencé par modifier les paramètres d'une couleur, puis les paramètres de toutes les couleurs, ce qui nous a permis de remarquer des changements significatifs dans l'image encodée. La valeur ajoutée « δ » est estimée à environ10^{-16} jusqu'à ce que l'image originale soit complètement restaurée, ce qui est une valeur que nous considérons comme la sensibilité principale pour les trois combinaisons CM1, CM3 et CM4 mais pour CM2 l'image montre encore de petits détails jusqu'à ce que l'erreur soit estimée comme le montre la Figure 3.15.



CM1	CM2	CM3	CM4
$\delta = 10^{-16}$	$\delta = 10^{-2}$	$\delta = 10^{-16}$	$\delta = 10^{-16}$

Figure 3 .15 Sensibilité des paramètres chaotiques de la clé de décryptage à une erreur de déviation "δ" : cas de l'imagePeppers

De plus, nous avons constaté que le test de sensibilité des clés sur toutes les séquences 2DCM produit des résultats similaires, indiquant que de légers changements dans les valeurs des paramètres de contrôle entraînent des modifications substantielles dans l'image cryptée.

Il est évident que le principe de sensibilité de la clé est lié aux variations des paramètres, même lorsqu'ils sont appliqués progressivement à d'autres paramètres comme l'ordre alpha fractionnaire. En utilisant la même méthodologie, nous avons effectué de petits ajustements sur l'angle de fréquence fractionnaire pour chaque canal de couleur, puis pour tous les canaux, sur une plage de (-0,5 à 0,5) avec un pas de 0,01. Cette approche permet de couvrir un large éventail de valeurs pour chaque canal de couleur.

Connaître la sensibilité de la clé et son espace nous permet d'évaluer l'efficacité de cette méthode face aux attaques par force brute. Les figures 3.16, 3.17 et 3.18 illustrent une comparaison de l'erreur estimée précédemment en termes de MSE (L'erreur quadratique moyenne) pour les trois canaux.

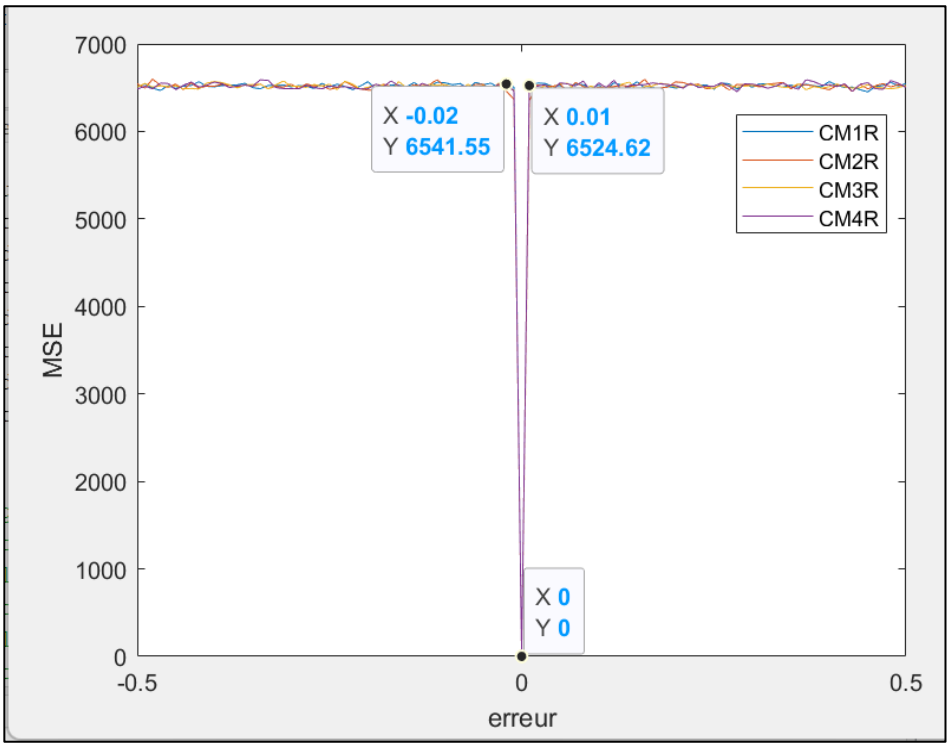


Figure 3.16 Comparaison MSE en fonction de l'erreur canal rouge

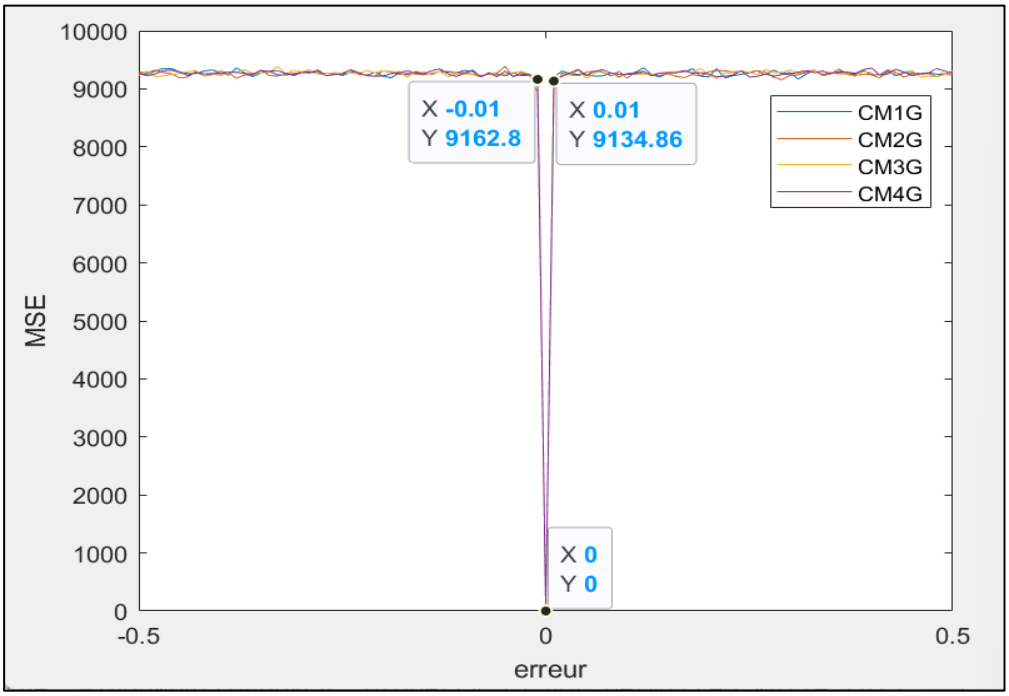


Figure 3.17 Comparaison MSE en fonction de l'erreur canal vert

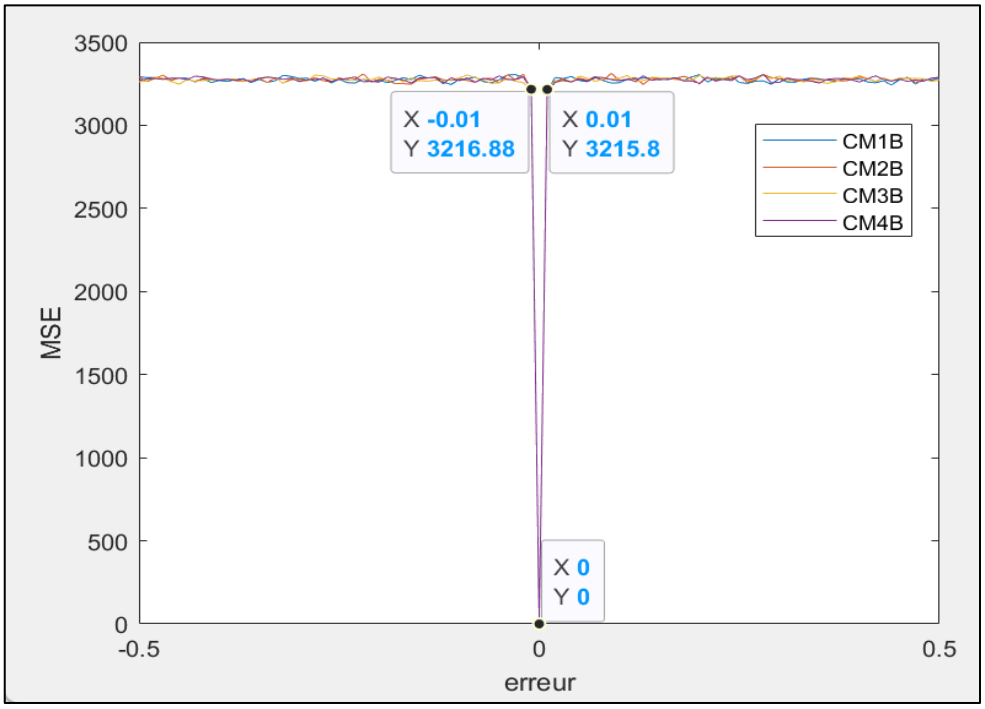


Figure 3.18 Comparaison MSE en fonction de l'erreur canal bleu

En résumé, nous notons que CM1, CM3 et CM4 offrent une sensibilité de clé élevée, ce qui signifie que de petites différences dans les valeurs des paramètres de contrôle entraînent des changements importants dans l'image codée. Ces variations peuvent être de petits ajustements dans les valeurs initiales des paramètres ou des variations graduées sur d'autres paramètres, tels que des valeurs d'angle fractionnaires, couvrant ainsi une large gamme de valeurs pour chaque canal de couleur. Contrairement à la série CM2, qui présentait une sensibilité de touche très faible, atteignant 10^{-2}.

Malgré d'éventuelles différences de performances entre les suies, les trois suites mentionnées ont toutes des performances globales élevées, garantissant une sécurité accrue dans le cryptage des images. Bien que la suite CM2 puisse être légèrement sous-performant à certains égards par rapport à d'autres, elles peuvent toutes être considérées comme des options valables avec des performances acceptables dans différentes situations d'application.

3.5 Discussions

- **Analyse Visuelle**

L'analyse visuelle des suites de cryptage CM1, CM2, CM3 et CM4 révèle que toutes parviennent à dissimuler efficacement les détails des images originales telles que "Peppers", "Barbara" et "Airplane". Cette capacité est essentielle pour empêcher la reconnaissance des images après cryptage. CM1 se distingue par un potentiel de cryptage particulièrement solide, offrant une efficacité notablement comparable, voire supérieure, aux autres suites. La qualité du masquage des détails par CM1 est remarquable, rendant les images cryptées totalement méconnaissables et maintenant une uniformité exceptionnelle à travers tous les composants de couleur et pour l'image RGB. CM3, bien que performant, requiert une inspection minutieuse pour discerner des différences subtiles par rapport à CM1. CM2 et CM4 montrent des performances légèrement inférieures en termes de masquage des détails et d'uniformité, mais restent globalement efficaces. Dans cet ordre, CM1 est la plus performante, suivie de CM3, CM4, et enfin CM2.

- **Analyse par Histogramme**

L'analyse comparative des quatre ensembles de cryptage (CM1, CM2, CM3, CM4) révèle qu'ils présentent des performances similaires. Ils fournissent tous un cryptage efficace avec de légères variations dans les résultats visuels. De plus, ils démontrent tous la capacité à préserver les valeurs des pixels sans altération pendant le processus de cryptage, ce qui témoigne de l'efficacité de leur

méthode de cryptage respective. Cependant, il est difficile de distinguer précisément les différences entre les images cryptées de chaque ensemble uniquement à partir des résultats visuels. Par conséquent, évaluer l'efficacité de chaque ensemble nécessite des tests supplémentaires pour comprendre l'impact du cryptage sur les données et mieux résister aux attaques statiques. Néanmoins, la capacité à maintenir les valeurs des pixels et à résister aux attaques statiques confirme l'efficacité de tous les ensembles (CM1, CM2, CM3, CM4) dans la sécurisation des données par le cryptage.

- **Test d'Entropie**

L'entropie mesure le degré de désordre ou de randomisation des données dans une image cryptée. CM1 affiche les valeurs d'entropie les plus élevées parmi les quatre suites, indiquant une meilleure distribution des valeurs des pixels et donc une sécurité renforcée. Une entropie élevée signifie que l'image cryptée est plus aléatoire et donc plus difficile à prévoir ou à attaquer. CM2 suit de près avec des valeurs d'entropie légèrement plus basses mais toujours élevées, assurant également une bonne sécurité. CM3 et CM4 montrent des performances légèrement inférieures en termes d'entropie, avec CM4 ayant les valeurs les plus basses, ce qui pourrait indiquer une vulnérabilité accrue dans certaines applications de sécurité critiques.

- **Test de Corrélation**

Les tests de corrélation entre les pixels adjacents de l'image originale et de l'image cryptée sont essentiels pour évaluer la qualité du cryptage. Une faible corrélation indique une meilleure diffusion des valeurs des pixels, ce qui est souhaitable. Les suites CM1 et CM3 tendent à présenter une dispersion des données plus uniforme, démontrant ainsi une corrélation plus faible et une meilleure sécurité. CM2 et CM4, en revanche, montrent parfois une dispersion légèrement plus élevée, indiquant une corrélation un peu plus forte entre les pixels adjacents. Globalement, CM1 démontre la meilleure dispersion des données, suivi de CM3, CM4 et enfin CM2.

- **Test de Résistance au Bruit**

La résistance au bruit est une mesure de la robustesse du cryptage face à des perturbations externes. Lors des tests de résistance au bruit, CM1 se révèle être la suite la plus performante, capable de maintenir l'intégrité de l'image cryptée malgré l'ajout de bruit. CM3 suit en deuxième position, puis CM4, et enfin CM2. Une meilleure résistance au bruit signifie que l'image cryptée

peut conserver sa qualité et son intégrité même en présence de perturbations, ce qui est crucial pour la robustesse du cryptage.

- **UACI/NPCR**

Les valeurs de NPCR (Number of Pixels Change Rate) et UACI (Unified Average Changing Intensity) sont des indicateurs clés de l'efficacité d'un cryptage en termes de changement de pixel et d'intensité. CM1 affiche généralement des valeurs de NPCR et UACI légèrement plus élevées que les autres suites, suggérant une meilleure préservation des caractéristiques de l'image et une distribution plus uniforme des valeurs après cryptage. CM3 et CM4 montrent des performances similaires mais légèrement inférieures, tandis que CM2 a les valeurs les plus faibles, le plaçant en dernière position pour ces critères.

- **Sensibilité de la Clé**

Les suites de cryptage CM1, CM3 et CM4 étudiées offraient une sensibilité de clé élevée, ce qui signifie que même de petites variations dans les paramètres de contrôle entraînent des changements significatifs dans l'image codée. Cette sensibilité est essentielle à la sécurité car elle garantit qu'une clé incorrecte, même légèrement différente, ne pourra pas décryptée correctement l'image. Cette fonctionnalité offre plus de sécurité en rendant presque impossible le décryptage sans la bonne clé. Ce que nous n'avons pas montré, c'est la série CM2, car elle a montré une très faible sensibilité qui la place au dernier rang parmi les quatre suites.

3.6 Conclusion

En conclusion, bien que chaque suite de cryptage CM présente des nuances dans ses performances, elles se sont toutes révélées efficaces en matière de cryptage d'images, fournissant des résultats visuels similaires et une résistance suffisante aux attaques statiques. Cependant, en combinant toutes les évaluations, le CM1 se démarque comme la suite le plus performant, offrant les meilleures performances en termes de masquage des détails, d'uniformité, d'entropie, de dispersion des données, de résistance au bruit et de valeurs NPCR/UACI.

CM3 suit de près, ce qui démontre également des performances élevées et une sécurité renforcée. Vient ensuite le CM4 avec des performances légèrement inférieures mais toujours efficaces, tandis que le CM2, malgré son efficacité dans les différents critères précédents, affiche des performances inférieures par rapport aux autres suites, notamment en ce qui concerne la

sensibilité des touches qui peut être prise en compte. Il descend donc au dernier rang. Le classement final est : CM1, CM3, CM4, et enfin CM2

Cette analyse détaillée met en évidence la supériorité de CM1 dans presque tous les aspects évalués, ce qui en fait la suite de cryptage la plus recommandée pour les applications nécessitant une sécurité maximale et des performances fiables. Le CM3, bien que légèrement inférieur, reste un choix très solide, tandis que le CM4 et le CM2, malgré leurs performances acceptables, sont plus adaptés aux applications moins critiques.

CONCLUSION GENERALE

CONCLUSION GENERALE

À travers notre plan de travail structuré en trois chapitres distincts, nous avons exploré les fondements des systèmes de cryptage modernes, plongeant ensuite dans la théorie de la méthode DRPE et des séquences chaotiques bidimensionnelles. Nous avons ensuite réalisé une analyse comparative rigoureuse des résultats obtenus, en mettant en avant les aspects de sécurité, d'efficacité, de performance et d'efficience.

Nous avons constaté que l'utilisation de DRPE basée sur DFrFT en combinaison avec des séquences chaotiques bidimensionnelles pouvait considérablement renforcer la sécurité des systèmes de cryptage d'images, tout en ajoutant des niveaux de complexité pour contrer les attaques potentielles et préserver l'intégrité des données.

Ces résultats mettent en lumière l'importance cruciale du choix des séquences chaotiques pour améliorer la robustesse et l'efficacité des systèmes de sécurité de l'information.

En résumé, nos recherches démontrent de manière éloquente l'efficacité remarquable des séquences 2D par leur classification comparative dans le contexte d'un codage basé sur une transformation paramétrique partielle.

Ces séquences apparaissent comme des outils fiables pour relever les défis croissants en matière de sécurité de l'information, offrant des perspectives prometteuses pour l'avenir du cryptage des images couleur et rendant les processus de décryptage plus complexes et plus résistants aux attaques.

Les résultats de notre étude ouvrent également des perspectives prometteuses pour l'avenir du cryptage des données. L'optimisation des séquences chaotiques peut grandement améliorer la sécurité et l'efficacité des systèmes cryptographiques.

En étendant l'application de la méthode DRPE à d'autres types de données et en approfondissant l'analyse de la complexité informatique, nous pouvons rendre les algorithmes plus efficaces et plus pratiques et les intégrer à des technologies de sécurité, telles que l'intelligence artificielle et autres. Développer et adapter notre approche pour répondre aux futurs défis en matière de sécurité de l'information.

REFERENCES BIBLIOGRAPHIQUES

[1] L. Grazide, L'image électronique
http://auch2.free.fr/Documents/Informatique/Image_electronique.pdf.

[2] Rafael C Gonzalez and Richard E Woods. Digital image processing 3rd edition, Pearson Prentice Hall, Upper Saddle River, 2007.

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

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

[5] B. Schneier, *Cryptographie appliquée : Algorithme, protocoles et codes sources en C*, Vuibert Informatique, deuxième édition, janvier 2001.

[6] F. Dachselt, K. Kelber and W. Schwarz, "Chaotic Coding and Cryptoanalysis",*Proceedings of IEEE International Symposium on Circuits and Systems*, HongKong, pp. 1061-1064, 9-12 June 1997.

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

[8] S.-C. Pei and W.-L. Hsue, "The multiple-parameter discrete fractional Fourier transform," *IEEE Signal Processing Letters*, Vol. 13, No. 6, pp. 329–332, June 2006.

[9] J. M. Vilardy, J. E. Calderon, C. O. Torres, and L. Mattos, "Digital images phase encryption using fractional Fourier transform," *in Proceedings IEEE Conference.Electronics, Robotics and Automotive Mechanics*, Vol. 1, pp.15–18, September 2006.

[10] G. Alvarez and al., "Some basic cryptographic requirements for chaos-based cryptosystems," Int. J. Bifurcat. Chaos., Vol. 16, no. 8, pp. 2129–2151, 2006.

[11**]** Krim Mohamed. thèse doctorat (Implémentation des séquences chaotiques sur les systèmes de communication moderne :Etalement de spectre à séquence directe DS-SS) université de la séence et de la technologie MOHAMMED BOUDHIAF à Oran .2018/2019 .

[12] Azoug- Seif Eddine, thèse doctorat " Développement et implémentation des techniques de cryptage des signaux image et vidéo ", Université Ferhat Abbass –Sétif , 2016.

[13] BEKKOUCHE Toufik, thèse –doctorat Université Ferhat abbas –Sétif " *Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes* ", Université Ferhat Abbass –Sétif, 2018.

[14] L. Acho, "A discrete-time chaotic oscillator based on the logistic map: A secure communication scheme and a simple experiment using Arduino," *Journal of the Franklin Institute*, Vol. **352**, no. 8, pp. 3113–3121, 2015.

[15] N. MEKKI, M. HAMDI, T. AGUILI, T. h. kim, a real-time chaotic encryption for multimedia data and application to secure surveillance framework for IOT system », 978-1-5386-4609-0/18,2018.

[16] A. Arshad, S.Shaukat, A. Ali , A. Eleyan ,S. A. Shah and J. Ahmad, « Chaos Theory and its Application: An Essential Framework for Image Encryption », Chaos Theory and Applications, vol.2, no.1, pp.15-20, 2020

[17]. Gao X (2021) Image encryption algorithm based on 2d hyperchaotic map. Optics Laser Technol, School of of Electrical Engineering, Longdong University, Gansu, Qingyang 745000 China, volume 142, octobre 2021, 107252

[18] An image encryption algorithm for visually meaningful ciphertext based on adaptive compressed, 2D-IICM hyperchaos and histogram cyclic shift by**Jing Shiwei · Li Jianjun**Decembre 2023

[19] -ShiguoLian. Multimedia content "encryption-technique and application " CRC Press.2009.

[20] David Ruelle. UTLS. (2000, 5 août). Chaos, imprédictibilité, hasard , in Des particules à l'antimatière : la matière et son organisation. [Vidéo]. Canal-U. https://doi.org/10.60527/fpng-g484.

[21] 2D Logistic-Sine-Coupling Map for Image Encryption Zhongyun Hua, Fan Jin, Binxuan Xu, Hejiao Huang, School of Computer Science and Technology, Harbin Institute of Technology Shenzhen Graduate School, Shenzhen 518055, China

[22]Color image encryption using orthogonal Latin squares and a new 2D chaotic system Zhongyun Hua · Zhihua Zhu · Yongyong Chen · Yuanman Li, Volume 104, pages 4505–4522, (2021), May 2021

[23] A color image encryption algorithm with a novel coupled chaotic system and 3D-DCT. Yan Wen, jingmingSu, Pingshun Gong,Anhui university of science and technology, Huainan 232001, China, March 11th, 2022