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 .

Filière : Electronique.

Spécialité : ELECTRONIQUE DES SYSTEMES EMBARQUE.

Par :

- Kamra KERAI .
- Yasmina MOHAMMED MARICHE .

Thème

Cryptage d'image basé sur les transformée paramétrique et le chaos.

Soutenu le : 14-09-2019.

Devant le jury :

- Pr.Zoubeida MESSALI Président.
- Dr. Latifa HACINI Examinateur.
- Dr. Seif Eddine AZOUG Encadreur.

Année Universitaire 2018/2019

Remerciements

Tout d'abord nous remercions Allah le tout puissant qui nous a donné la patience, la force morale & physique et le courage d'élaborer notre modeste travail.

Nous exprimons nos sincères remerciements à notre encadrant Dr.Seif Eddine AZOUG qui a dirigé ce travail par son savoir, sa gentillesse, ces encouragements, son expérience et sa disponibilité permanente durant notre stage, ses conseils éclairés et les discussions fructueuses que nous avons eues avec lui

Nous tenons à exprimer notre parfaite considération aux membres du jury pour avoir accepté de consacrer une partie de leurs temps afin d'examiner et de juger ce modeste travail.

Nous ne saurions oublier de remercier les enseignants de la faculté des Sciences et de la Technologie de l'université Mohamed El Bachir El Ibrahimi BORDJ BOU ARRERIDJ qui ont contribués à notre formation.

Nous associons dans la même pensée, tous nos ami(e)s pour leur soutien moral durant nos études de master.

Enfin, nos derniers remerciements et non les moindres vont à nos parents et à tous les membres de nos familles avec toute nos affectueusesgratitude pour leur soutien etleurs encouragements.

Dédicaces

Je dédie ce travail à mes chers parents
Mon Père, Ma Mère

Vous représentez pour moi le symbole de la bonté par excellence, la source de la tendresse et l'exemple du dévouement qui n'a pas cessé de m'encourager et de prier pour moi.

A mon chère frère : FOUAD pour m'avoir soutenu tout le temps

A mes chères sœurs : NESSRINE, ISMAHANE, et la petite RADHIA

A Mon chère amie et binôme

KAMRA

A tous mes chères amies chacun par son nom.

A ma grande famille « MOHAMMED MARICHE ».

YASMINA

Dédicaces

Je dédie ce modeste travail

A mes très chers parents pour leurs sacrifices.

A Mes chers frères : NOURDINE, FARESSE et HAWASS

A Ma sœur Salma et ma cousine AKila.

A tous mes amis.

Je n'omettrai pas de dédier ce mémoire à mon binôme Yasmina

A tous ceux qui me sont chers.

A tous ceux qui m'aiment.

A tous ceux que j'aime.

KAMRA

Liste des acronymes

DES	Data Encryptions Standard
AES	Advanced Encryptions Standard
RSA	Au nom de Ronald Rivest, Adi Shamir et Leonard Adleman
DRPE	Double Random Phase Encoding
EQM	Erreur Quadratique Moyenne
TF	Transformée de Fourier
TFFrD	Transformée de Fourier fractionnaire discrète
PSNR	Peak Signal-to-Noise Ratio, Rapport signal/bruit crête à crête.
PWLCM	Piece wise Linear Chaotic Map, Suite chaotique linéaire par morceaux.
ROP	Réciproque-Orthogonale Paramétrique
2D	Deux dimensions / bidimensionnelle.

Liste des tableaux

Liste des figures

Table des matières

Introduction Générale

Introduction générale

Dissimuler une information est un besoin qui préoccupe l'humanité depuis son existence où la confidentialité des informations militaires et diplomatiques apparaissait comme un besoin vital pour gagner la guerre. De nos jours, ce besoin de confidentialité ne se limite plus aux militaires et aux diplomates à cause de la démocratisation des ordinateurs et d'INTERNET pour les échanges bancaires ou simplement nos échanges privés ou professionnels sur messageries.

Pour assurer la sécurité de nos informations privés ou professionnels il faut recourir à la cryptographie moderne qui permet d'assurer la confidentialité, l'intégrité, l'authenticité des informations lors de leurs échanges dans les réseaux de télécommunication en offrant différentes méthodes et algorithmes cryptographiques selon l'application visée. Cependant, quand l'information à crypter est une image, les algorithmes traditionnels de cryptage tels que **DES [1]** (Data Encryptions Standard), **AES** [2] (Advanced Encryptions Standard) et **RSA** [2] (Ronald Rivest, Adi Shamir et Leonard Adleman) restent des algorithmes de cryptage bit par bit et dans le domaine spatial qui ne prennent pas en compte les propriétés de l'image à crypter telle que la redondance des pixels [3].

En conséquence, d'autres algorithmes et méthodes de cryptages image ont été explorées telle que la fameuse méthode DRPE « Double Random Phase Encoding» qui peut être implémentée optiquement ou numériquement [4]. Elle est basée sur l'utilisation de deux masques de phases aléatoires et d'une transformée standard telle que la transformée de Fourier ou des transformées paramétriques telle que la transformée de Fourier fractionnaire discrète qui est une transformée de Fourier modifiée de sorte à avoir des paramètres indépendants qui peuvent servir comme une clé secrète de cryptage.

Pour améliorer sa sécurité, Lang et al. [5]Ont proposé d'introduire l'utilisation de suites logistiques dans la méthode DRPE. Ces suites ont un comportement chaotique, cependant, ils ce sont limité seulement à la suite logistique avec la transformée de Fourier fractionnaire discrète alors qu'il existe plusieurs autres types de transformées paramétriques et de suites logistiques. De ce fait, nous proposons dans ce manuscrit de mener une étude comparative sur la méthode de Lang avec différentes suites chaotiques et différentes transformées paramétriques.

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

- Premier chapitre : Présentation de généralités sur les systèmes cryptographiques modernes.

- Deuxième chapitre : Revoir la théorie de la méthode DRPE ainsi que ses transformées paramétriques discrètes les plus connues telles que la transformée ROP, transformée ROP récursive, transformée TFFrD et la transformée TFFrD à paramètres multiples.

- Troisième chapitre : Revoir la théorie de plusieurs suites chaotiques ainsi que le principe de la méthode Lang pour le cryptage d'images.

- Quatrième chapitre : Présentation des différents résultats et analyses de l'étude comparative proposée sur la méthode de Lang avec différentes suites chaotiques et transformées paramétriques.

Le travail ainsi mené s'achève avec une conclusion générale et des perspectives.

CHAPITRE 1

Généralités sur la cryptographie

1 .1.Introduction

La cryptologie est la science du secret de l'information [6]. En plus de la cryptanalyse et de la stéganographie, la cryptographie est l'un des principaux domaines de recherche en cryptologie [1].Le mot cryptographie vient des mots latin « cryptos » ou secret et « graphie » ou écriture ou « écriture secrète » [2].La cryptographie consiste à développer des algorithmes qui ont pour objectif principal la transformation d'un message compréhensible en un message chiffré incompréhensible à l'aide d'une clé pré calculée [1][2]. Cette transformation est réversible et elle est appelée cryptage/décryptage(ou chiffrement/déchiffrement).

Sa première utilisation remonte à l'ère des pharaons en Egypte ainsi qu'au temps de l'empereur Jules César qui utilisa un algorithme de cryptage basée sur des décalages alphabétique [6].Avec l'arrivée des ordinateurs, plusieurs algorithmes de cryptage ont été développées et implémentés dans différents domaines d'applications multimédia [1][6].

Dans ce chapitre nous allons présenter des généralités sur la cryptographie telles que ses objectifs, le concept de base d'un algorithme de cryptage ainsi que les différentes classes d'algorithmes de cryptage.

1.2. Objectifs de la cryptographie

En plus d'assurer la confidentialité de l'information, la cryptographie permet aussi d'assurer l'intégrité des données, l'authentification ainsi que la non-répudiation de l'information [1].L'information appelée texte en claire peut être un message textuel, une piste audio, une image ou une séquence d'images vidéo ou autres [3].

1.2.1. La confidentialité

L'objectif principal de la cryptographie est d'assurer la confidentialité de l'information par l'utilisation d'un algorithme de cryptage [2].Une clé secrète est nécessaire pour le cryptage et le décryptage du texte crypté n'est possible que par celui qui détient la clé secrète adéquate [1][2]. Cela permet de protéger l'information contre tout accès indésirable.[3].

1.2.2. L'intégrité des données

L'intégrité des données assure que le texte crypté n'a pas été modifié par une partie tierce. Des algorithmes dits algorithmes de hachage sont utilisés dans ce cas afin de détecter un quelconque changement dans l'intégrité des données de l'information originale [3].

1.2.3. L'authentification

L'authentification permet de vérifier l'identité de l'émetteur par le récepteur de l'information afin d'assurer qu'il n'y a pas eu d'usurpation d'identité en utilisant des protocoles d'authentification [2] [7].

1.2.4. La non-répudiation

La non répudiation des données permet d'assurer que les participants dans un échange d'informations cryptées ne peuvent nier l'envoi ou la réception des informations grâce à l'utilisation d'algorithmes de signatures électroniques [2].

1.3. Structure d'un système cryptographique

Un système cryptographique peut être modélisé par les blocs suivants [1] [2]:

- Le texte en claire noté M
- Le texte crypté noté C
- Un algorithme de cryptage E(.)
- La clé de décryptage noté K_D
- La clé de cryptage noté K_E
- Un algorithme de décryptage D(.)

L'algorithme de cryptage est modélisé par une fonction mathématique E(.) qui permet de crypter un texte en clair M en un texte crypté C à l'aide d'une clé de cryptage K_E. L'algorithme de décryptage est modélisé par une fonction mathématique D(.) qui permet de faire l'opération inverse en transformant le texte chiffré C en un texte claire M à l'aide d'une clé de décryptage K_d. Cela peut être résumé par l'équation (1.1) et la figure 1.1.

$$\begin{cases} E_{K_e}(M) = C \\ D_{K_D}(C) = M \end{cases} \qquad (1.1)$$

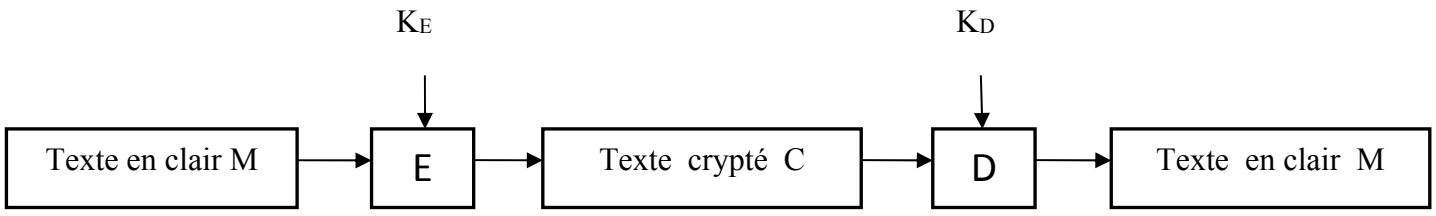


Figure 1.1. Structure d'un système cryptographique

1.4. Concept des algorithmes de cryptage

La sécurité de l'information repose essentiellement sur la robustesse de l'algorithme de cryptage qui est la partie la plus importante du système cryptographique [2].

Shannon a montré qu'un algorithme de cryptage doit avoir deux caractéristiques importantes qui sont la confusion et la diffusion [8]. Pour réaliser cela pratiquement, le cryptage par permutation est utilisé pour assurer la confusion et le cryptage par substitution est utilisé pour assurer la diffusion [2].

1.4.1. Cryptage par permutation

Le cryptage par permutation assure la propriété de la confusion en permutant les emplacements des données du texte en clair M [9]. Ce changement dans l'arrangement des données permet de brouiller la relation existante entre le texte en clair M et le texte crypté C [2] [10]. La figure 1.2 illustre un exemple de permutation.

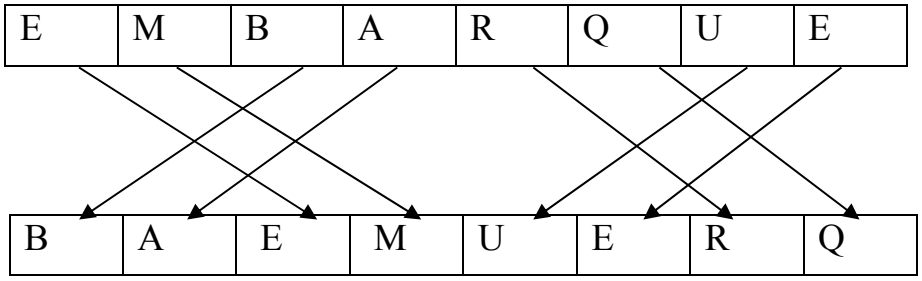


Figure1.2. Exemple sur le cryptage par permutation

1.4.2. Cryptage par substitution

Le cryptage par substitution consiste à remplacer les données du texte en clair M à crypter par d'autres données totalement différentes en utilisant des fonctions mathématiques réversibles [10]. Ce principe de substitution permet de diffuser la redondance des données ce qui permet de supprimer la relation existante entre le texte en clair M et le texte chiffré C. Cela a pour but de décourager les différentes attaques statistiques [10][2].

La figure 1.3montre un exemple sur le cryptage de César qui est un cryptage par substitution basé sur le décalage de chaque lettre par un nombre prédéfini (trois dans ce cas) de lettres dans l'ordre alphabétique [10]

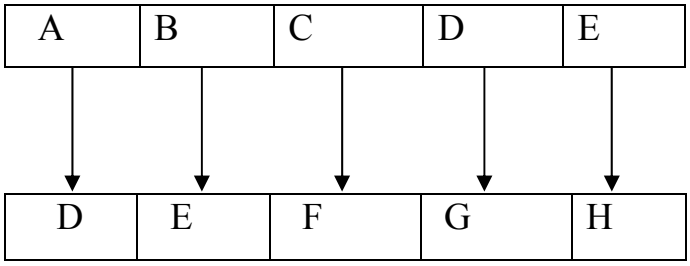


Figure 1.3. Exemple sur le cryptage par substitution

1.5. Classification des algorithmes de cryptage

Les algorithmes de cryptage peuvent être classés selon plusieurs paramètres comme suit [1][3] :

- Classification selon le type de la clé
- Classification selon le pourcentage de donnée à crypter (total ou partiel).
- Classification selon la taille des données à crypter (flot ou bloc).
- Classification selon le domaine du cryptage (spatial ou fréquentiel)

1.5.1. Classification selon le type de la clé

Il existe deux classes d'algorithmes de cryptages selon le type de la clé : les algorithmes à cryptage symétrique et les algorithmes à cryptage asymétrique [1] [3].

1.5 .1.1.Algorithmes de cryptage symétrique

Dans cette classe d'algorithmes de cryptage, la clé de cryptage K_E et la clé de décryptage K_D sont identiques comme le montre la figure 1.4 [2].

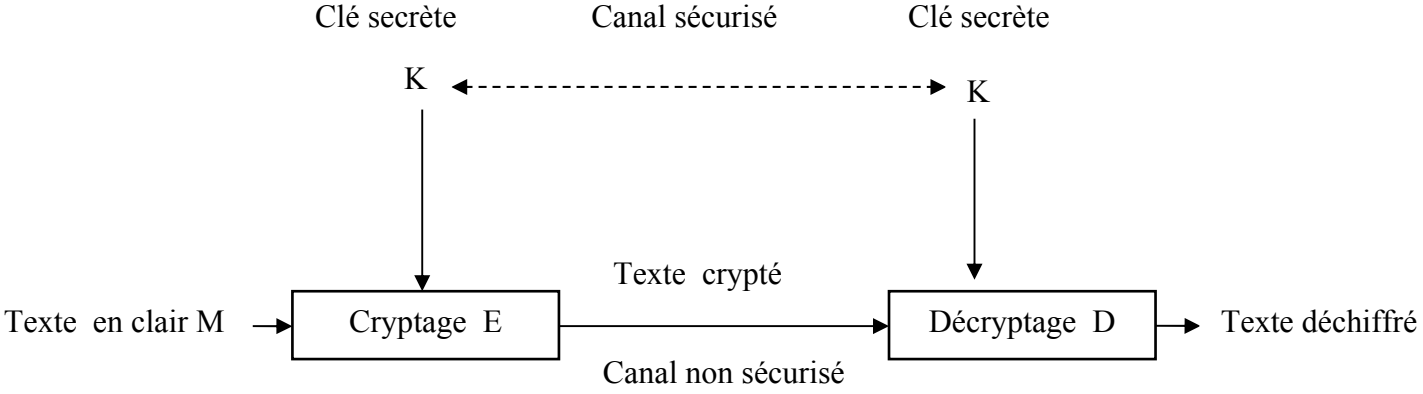


Figure1.4. Algorithme de cryptage symétrique

Dans ce cas, l'équation (1.1) précédente devient [1] :

$$\begin{cases} E\ k(M) = C \\ D\ k(C) = M \end{cases} \qquad (1.2)$$

Où la clé secrète K doit être échangé à travers un canal sécurisé entre l'émetteur et le récepteur [2][10].

1.5 .1.2 .Algorithmes de cryptage asymétrique

Dans cette classe d'algorithmes de cryptage, la clé de cryptage K_E et la clé de décryptage K_D ne sont pas identiques.

Dans ce cas, le texte en clair est crypté avec une clé K_E publique (non secrète) et décrypté avec une clé K_D privée (secrète) [2]. Cela a pour avantage de supprimer la nécessité d'un canal sécurisé pour l'échange des clés entre l'émetteur et le récepteur [7] [1] comme le montre la figure 1.5 [2].

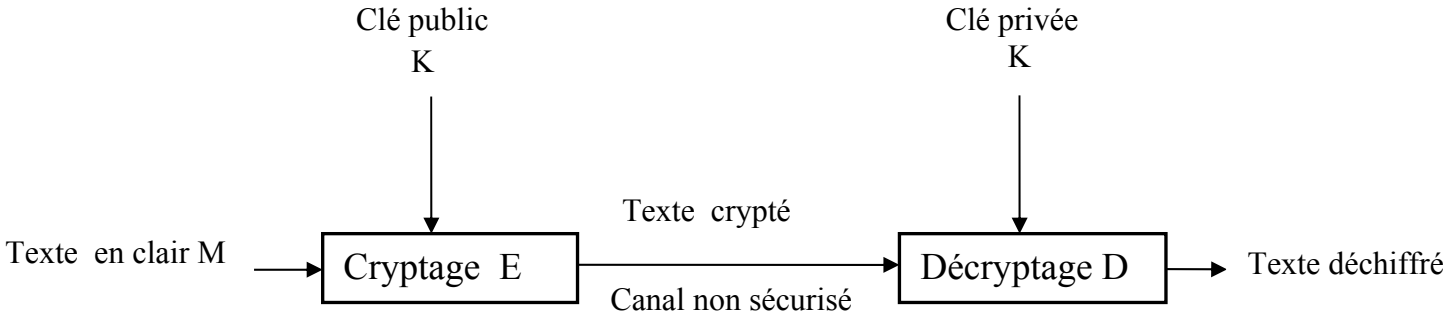


Figure 1.5. Algorithme de cryptage asymétrique

1.5.2. Classification selon le pourcentage des données à crypter

Il existe deux classes d'algorithmes de cryptages selon le pourcentage des données à crypter [2] [3]:

- Algorithmes de cryptage total
- Algorithmes de cryptage partiel

Les algorithmes de cryptage partiel contrairement aux algorithmes de cryptage total permettent un cryptage sélectif des données selon le type d'application comme par exemple dans le cas de l'opération de la compression de données [9].

1.5.3. Classification selon le flux de données

Il existe deux classes d'algorithmes de cryptages selon le flux de données [2] [3] sont :

- Cryptage par bloc où le message à crypter est divisé en blocs de bits et chaque bloc est crypté séparément l'un après l'autre [2][3].
- Cryptage par flux où le message est crypté bit par bit. Ce cryptage est rapide et nécessaire dans le cas du cryptage en temps réel [3].

1.5.4Classification selon le domaine de travail

Ce type de classification est effectuée selon le domaine de travail de la fonction du cryptage ce qui nous permet d'avoir un cryptage dans le domaine spatial et un cryptage dans le domaine fréquentiel [3] [11].

1.5.4.1. Domaine spatial

Lorsque la donnée a crypté est une image, Le cryptage est fait dans le domaine spatial (temporel) par le cryptage d'une combinaison de bit pour chaque pixel [3]

1.5.4.2. Domaine fréquentiel

Le cryptage fréquentiel se fait dans le domaine d'une transformée discrète standard telle que la transformée de Fourier discrète (TFD) ou dans le domaine des transformées paramétrique discrète où leurs paramètres indépendants sont considérés comme des clés secrètes additionnelles [3].

1.6. Conclusion

Dans ce chapitre nous avons vu que l'objectif principal de l'utilisation de la cryptographie c'est d'assurer la confidentialité des informations à crypter. Ensuite, nous avons vu que le concept des algorithmes de cryptage repose sur l'utilisation du cryptage par permutation afin d'assurer la propriété de la confusion et sur l'utilisation du cryptage par substitution afin d'assurer la propriété de diffusion. Enfin, nous avons vu les différentes classes d'algorithmes de cryptage dont les algorithmes de cryptage symétrique/asymétrique et les algorithmes de cryptage spatial/fréquentiel. Ces notions de base sur la cryptographie permettent de bien comprendre les techniques de cryptage basées sur les transformées paramétriques et le chaos qui font l'objet de notre étude dans les chapitres suivants.

CHAPITRE 2

Cryptage d’images basé sur les transformées paramétriques

2.1. Introduction

Parmi les techniques de cryptage d'images qu'on trouve en littérature il y a la fameuse méthode de cryptage à double masques de phases aléatoires ou Double Random Phase Encoding (DRPE) en anglais qui est une méthode de cryptage d'images basée sur la transformée de Fourier (TF)[12].

Afin d'améliorer la sécurité de la technique DRPE, des transformées paramétrique ont été introduites [12] [2] où leurs différents paramètres indépendants sont exploités comme une clé secrète additionnelle.

Dans ce chapitre, nous allons présenter la méthode DRPE ensuite nous allons revoir en détail les différentes définitions mathématiques des transformées paramétriques qui font l'objet de notre étude ainsi que leurs applications en cryptage d'images DRPE.

2.2. Cryptage d'images à double masques de phases aléatoires DRPE

Le principe de la méthode DRPE est simple et repose sur le masquage d'une image de taille $N \times M$ par deux masques comprenant des phases aléatoires. Ces phases sont générées à partir du plan complexe à l'aide de deux fonctions différentes $\alpha(n,m)$et $\beta(n,m)$[3].

Comme le montre la figure 2.1, le premier masque $e^{j\alpha(n,m)}$est appliqué dans le domaine spatial et le second masque $e^{j\beta(n,m)}$est appliqué dans le domaine de la transformée de Fourier (TF) [12].

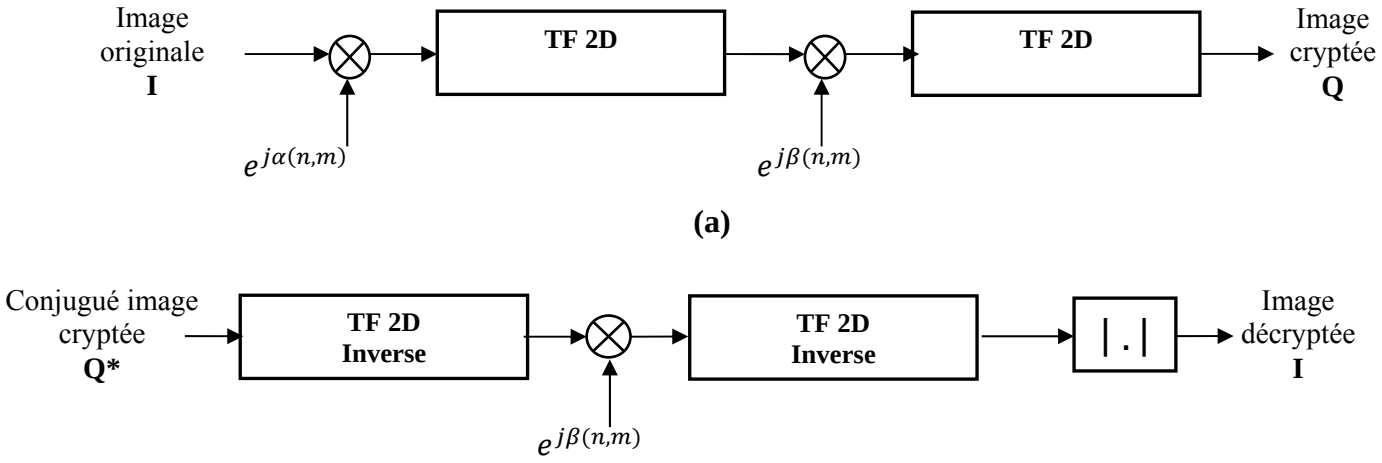


Figure 2.1.Méthode DRPE de cryptage d'images (a) Cryptage, (b) Décryptage

Ce dernier masque est considéré comme l'unique clé secrète [2]. Il faut noter que cette clé a la même taille que l'image. En décryptage, l'image décryptée est obtenue seulement si on a la clé secrète correcte $\beta(n,m)$ alors que $\alpha(n,m)$est ignoré en prenant le module de l'image décryptée à la fin. En effet, ce premier masque n'a pour rôle ici que de bruiter l'image en vue de son cryptage afin d'améliorer sa sécurité [2].

2.3. Transformées paramétriques et DRPE

Afin d'améliorer la sécurité de la méthode DRPE, la TF a été remplacé depuis par des transformées paramétriques à paramètres indépendants [13]. Ce type de transformées sont dérivées d'une transformée standard telle que la TF sauf qu'ils possèdent en plus des paramètres indépendants qui peuvent être considérés comme une clé de cryptage additionnelle.

Dans le domaine discret, la transformée de Fourier fractionnaire discrète (TFFrD) à paramètre unique [14] ou à paramètres multiples [15] ainsi que la transformée réciproque-orthogonal paramétrique (ROP) [16] sont parmi les transformées paramétriques discrètes les plus connues.

2.3.1. Transformé de Fourier Fractionnaire discrète (TFFrD)

La TFFrD a été proposée pour la première fois par Candan et al. [14]. Une matrice TFFrD d'ordre $\boldsymbol{a}$ et de taille$N \times N$ que l'on note $F^{\boldsymbol{a}}$est définie comme suit [15] [17] [2] :

$$F^{\tilde{\alpha}} = \mathbf{V}\,\Lambda^{\tilde{\alpha}}V^{T} = \begin{cases} \sum_{n=0}^{N-1} \lambda_n^{\alpha}\ \boldsymbol{v_n}\ \boldsymbol{v_n^{T}} & si\ N\ impair \\ \sum_{n=0}^{N-2} \lambda_n^{\alpha}\ \boldsymbol{v_n} + \lambda_N^{\alpha}\ \boldsymbol{v_N}\ \boldsymbol{v_N^{T}} & si\ N\ pair \end{cases} \quad \textbf{(2 .1)}$$

$(.)^{T}$ signifie la transposée. $\mathbf{V}= [v_0\,|v_1\,|.....|v_{N-2}\,|v_{N-1}\,]$ pour N impair. Pour N paire on a

$\mathbf{V}= [\ v_0\,|v_1\,|.....|v_{N-2}\,|\quad v_N\quad]$, Λ^{α}indique la matrice diagonale et les valeurs propres $\lambda_{\boldsymbol{n}}^{\boldsymbol{\alpha}}$où $\lambda_{\boldsymbol{n}}^{\boldsymbol{\alpha}}= e^{-j\frac{\pi}{2}an}$et $\alpha = \frac{\pi}{2a}$n de la matrice **S** de taille N×N défini comme suit où $\boldsymbol{\omega = 2\pi/\ N}$ [9][19] :

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

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} [17].

Parmi les propriétés importantes de la TFFrD on trouve [2] :

- L'additivité : $\boldsymbol{F^{b}.F^{a}=F^{a+b}}$
- L'inverse de la transformé : $\boldsymbol{F^{-1}=F^{-a}}$
- $\boldsymbol{F^{a}.F^{-a}=I}$ où I indique la matrice identité.

Dans le cas d'une image **I** de taille $N \times M$, sa TFFrD bidimensionnelle 2D est donnée comme suit [18] [2] :

$$\mathbf{F^{(a,b)}[I] = F^{a}.I.F^{b}} \qquad \textbf{(2.3)}$$

En profitant des propriétés de la TFFrD, l'inverse de la TFFrd2D est défini comme suit :

$$\left(\mathbf{F^{(a,b)}[I]}\right)^{-1} = \mathbf{F^{-a}.I.F^{-b}} \qquad \textbf{(2.4)}$$

De plus, l'ordre de chaque matrice TFFrD est un paramètre indépendant qui peut être exploité par la technique DRPE comme une clé secrète additionnelle comme le montre la figure 2.2 [12].

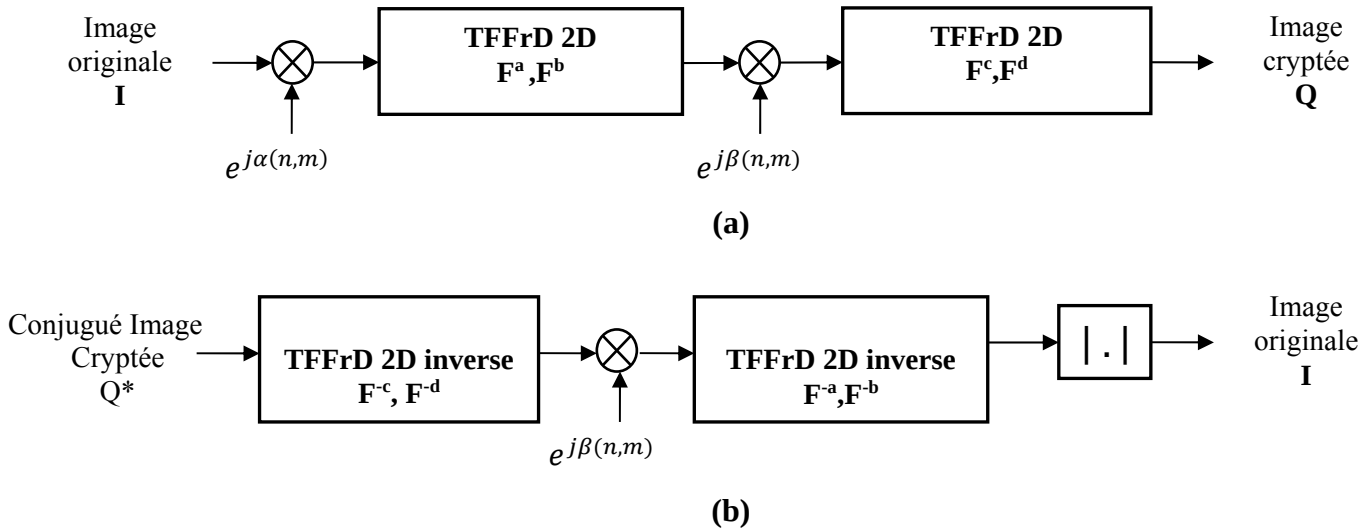


Figure 2.2. Technique de cryptage DRPE basée sur la TFFrD : (a) Cryptage, (b) Décryptage

2.3.2. TFFrD à paramètres multiples

Pei et al. ont proposé la TFFrD à paramètres multiples comme une généralisation de la TFFrD [17].Dans ce cas, une matrice $\mathbf{F}^{\bar{a}}$ est une matrice TFFrD à paramètres multiples définie comme suit [15] [2] :

$$F^{\bar{\alpha}} = \mathbf{V}\,\Lambda^{\bar{\alpha}} V^{T} \quad \textbf{(2.5)}$$

$$\Lambda^{\bar{\alpha}} = \begin{cases} diag\left(\lambda_0^{\alpha_0}, \lambda_1^{\alpha_1}, \dots, \lambda_{N-1}^{\alpha_{N-1}}\right) \\ diag\left(\lambda_0^{\alpha_0}, \lambda_1^{\alpha_1}, \dots, \lambda_{N-2}^{\alpha_{N-2}}, \lambda_N^{\alpha_{N-2}}\right) \end{cases} \quad (\mathbf{2.6})$$

$$\bar{\alpha} = \begin{cases} (\alpha_0, \alpha_1, \dots, \alpha_{N-1}) \text{si N impair} \\ (\alpha_0, \alpha_1, \dots, \alpha_{N-2}, \alpha_N) \quad \text{si N pair} \end{cases} \quad \textbf{(2.7)}$$

Où $\bar{\alpha}$vecteur paramétrique de la transformée qui contient N ordres actionnaire et les éléments propres $\lambda_{\frac{m}{N}} = e^{-j\frac{\pi}{2}an}$, où $\alpha_n = 2\alpha_n \backslash \pi$.

De ce fait, on remarque que la TFFrD est un cas particulier de la TFFrFT à paramètres multiples mais avec une complexité de calcul identique et possèdent les mêmes propriétés telles que [15] [2] [5] :

- L'inverse de la transformé :$(\boldsymbol{F}^{\bar{\alpha}})^{-1} = \boldsymbol{F}^{-\bar{\alpha}}$
- L'additivité : $\boldsymbol{F}^{\bar{\alpha}_1} . \boldsymbol{F}^{\bar{\alpha}_2} = \boldsymbol{F}^{\bar{\alpha}_1 + \bar{\alpha}_2}$où $\bar{\alpha}_1$ et $\bar{\alpha}_2$ deux vecteurs paramétriques.
- La matrice identité **I** est obtenu lorsque $\bar{\alpha}$ = (0, 0,…, 0) : $F^{\bar{\alpha}} = \mathbf{V}\Lambda^{\mathbf{0}} V^{T} = \mathbf{V}V^{T} = \mathbf{I}$

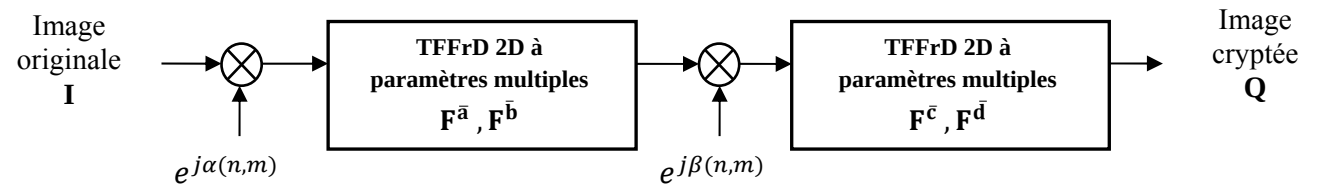
Dans le cas d'une image **I** de taille $N \times M$, la TFFrD bidimensionnelle 2D à paramétres multiples est donnée comme suit [2] :

$$\boldsymbol{F}^{(\bar{\mathbf{a}},\bar{\mathbf{b}})}[\mathbf{I}] = \boldsymbol{F}^{\bar{\mathbf{a}},} . \mathbf{I} . \boldsymbol{F}^{\bar{\mathbf{b}}} \quad \textbf{(2 .8)}$$

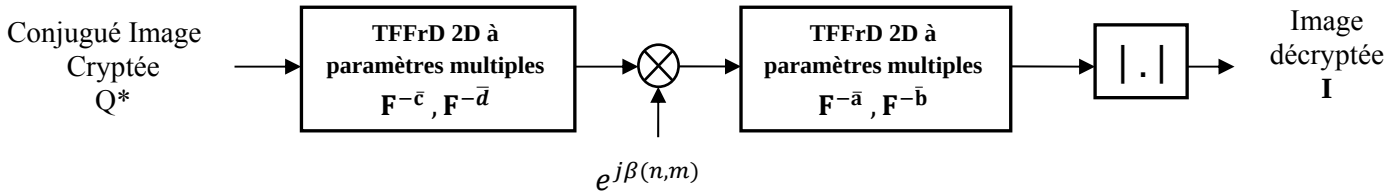
En profitant des propriétés de la TFFrD, l'inverse de la TFFrD 2D est obtenu comme suit :

$$\left(\boldsymbol{F}^{(\bar{\mathbf{a}},\bar{\mathbf{b}})}[\mathbf{I}]\right)^{-1} = \boldsymbol{F}^{\overline{-\mathbf{a}},} . \mathbf{I} . \boldsymbol{F}^{\overline{-\mathbf{b}}} \quad \textbf{(2.9)}$$

De plus, les vecteurs d'ordres fractionnaires des matrices TFFrD peuvent être exploités par la technique DRPE comme une clé secrète additionnelle comme le montre la figure 2.3 [3].



(a)



(b)

Figure 2.3.Méthode de cryptage DRPE basée sur la TFFrD à paramètres multiples :
(a) Cryptage, (b) Décryptage

2.3.3. Transformée Réciproque-Orthogonale Paramétrique (ROP)

Bouguezel et al.ont proposé une transformée discrète réciproque-orthogonale paramétrique (ROP) [19] qui possède une structure simple ayant une complexité de calcul faible contrairement à la TFFrD [16].

La transformée ROP est basée sur la transformée Walsh-Hadamard. Soit une matrice Hadamard $\boldsymbol{H_N}$de taille N×Ndéfinie comme suit :

$$\boldsymbol{H_N = H_2 \otimes H_2 \ldots \otimes H_2} \quad \textbf{(2.10)}$$

Où $\boldsymbol{H_2} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, représente le produit de Kronecker et$\boldsymbol{H_N}$. $\boldsymbol{H_N}$= N $\boldsymbol{I_N}$où $\boldsymbol{I_N}$N=2^ravec r un nombre entier positif [16]-[3].Les numéros des lignes de la matrice $\boldsymbol{H_N}$sont des entiers n= 0,1,…, N-1, 0 < n < N-1[16][3][20][2] qui peut être écris en binaire sous la forme [10][1][21]:

$$\mathbf{n= } \boldsymbol{n_{r-1}2^{r-1}+n_{r-2}2^{r-2}+ \ldots + n_1 2 + n_0} \quad \textbf{(2.11)}$$

Avec 0< i< r-1.Soit une fonction $s_{(n)}$= (-1)$^{\sum_{i=0}^{r-1} \boldsymbol{n_i}}$ qui peut avoir la valeur 1 ou 0 selon $\boldsymbol{n_i}$[16]. Ainsi, une ligne d'indice $\boldsymbol{n_i}$de la matrice $\boldsymbol{H_N}$est considérée comme une ligne d'indice négatif si $s_{(n)}$= 1.

Soit V un vecteur paramétrique défini comme suit [2]:

$$\mathbf{V}=\left[1 \quad \alpha_1 \quad \alpha_2 \quad \dots \quad \alpha_{\frac{N}{2}-1} \quad \alpha_{\frac{N}{2}-1} \quad \dots \alpha_2 \quad \alpha_1 \quad 1\right] \textbf{(2.12)}$$

Où α_i , où i= 1, 2, …, N/2 -1 sont des paramètres indépendants non nuls aléatoirement choisis du plan complexe .De ce fait, une matrice ROP T_N^V d'ordre N peut être construite en multipliant simplement le vecteur paramétrique **V** élément par élément avec les lignes de la matrice de Hadamard $\boldsymbol{H_N}$ dont l'indice est qualifié de négatif [2].

La matrice ROP T_N^V ainsi obtenu aura pour propriétés [16]:

- Réciprocité et orthogonalité **:** T_N^V**.** $(T_N^V)^{\mathrm{RT}} = N\mathbf{I}$ où **I** est la matrice identité et $(T_N^V)^{\mathrm{RT}}$ la matrice réciproque-transposée.
- Inverse de la transformée :$(T_N^V)^{-1} = \frac{1}{N} (T_N^V)^{\mathrm{RT}}$

Dans le cas d'une image **I** de taille$N \times M$, sa transformée ROP que l'on note **R** est donnée comme suit [19] :

$$\mathbf{R}^{(\mathbf{V_1},\mathbf{V_2})}[\mathbf{I}] = \mathbf{R}_{\mathbf{N}}^{\mathbf{V_1}}.\mathbf{I}.\mathbf{R}_{\mathbf{M}}^{\mathbf{V_2}} \qquad \textbf{(2.13)}$$

En profitant des propriétés de la transformée ROP on obtient l'inverse de la transformée comme suit :

$$\left(\mathbf{R}^{(\mathbf{V_1},\mathbf{V_2})}[\mathbf{I}]\right)^{-1} = \frac{1}{N^2}.\left(\mathbf{R}_{\mathbf{N}}^{\mathbf{V_1}}\right)^{\boldsymbol{RT}}.\mathbf{I}.\left(\mathbf{R}_{\mathbf{M}}^{\mathbf{V_2}}\right)^{\boldsymbol{RT}} \textbf{(2.14)}$$

Nous remarquons que l'inverse de la transformée est obtenu seulement en prenant la réciproque transpose de la transformée directe.

De plus, les éléments des vecteurs paramétriques$\mathbf{V_1}$et$\mathbf{V_2}$peuvent être exploités par la technique DRPE comme une clé secrète additionnelle comme le montre la figure 2.4[16].

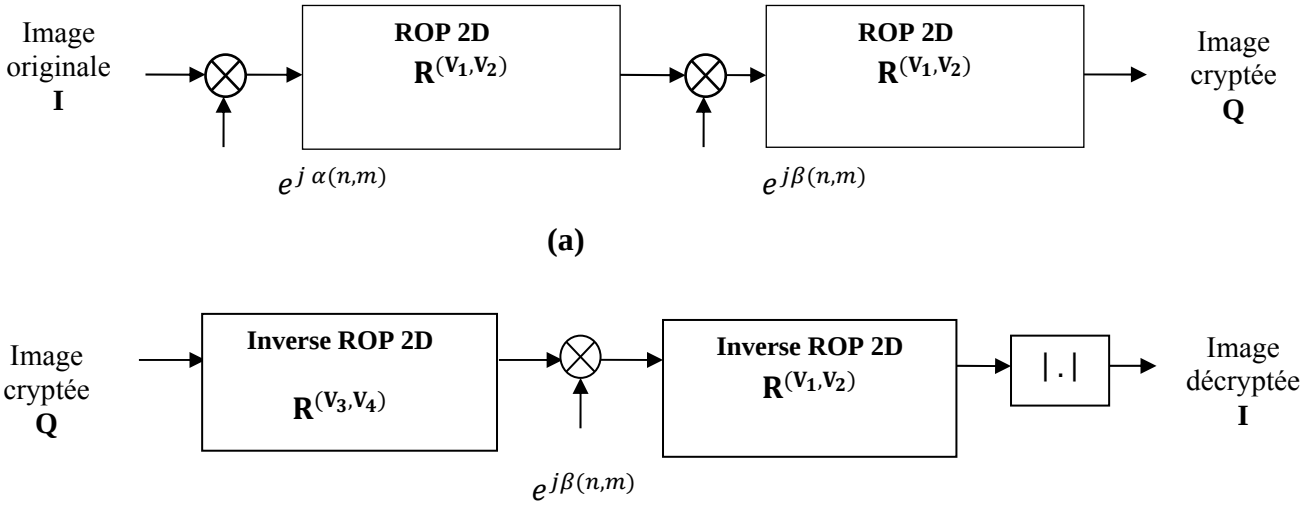


Figure 2.4. Technique de cryptage DRPE basée sur la transformée ROP :
(a) Cryptage, (b) Décryptage

2.3.4. Transformée Réciproque-Orthogonale Paramétrique (ROP) récursive

Bouguezel et al. ont proposé une transformée réciproque-orthogonale paramétrique (ROP) récursive discrète [22] qui possède une structure récursive. La transformée ROP récursive est basée sur l'utilisation récursive de la transformée ROP vu dans la section précédente afin d'augmenter de façon significative le nombre de paramètres indépendants [22].Du fait de sa récursivité, sa complexité de calcul est réduite grâce à un algorithme de calcul rapide [2]. Ainsi, une matrice ROP récursive que l'on note$\mathbf{T}_{2N}$ d'ordre 2N est définie comme suit [22]:

$$T_{2N}=(\prod_{s=1}^{r}(I_{2^{s-1}}\otimes H_2\otimes I_{2^{r+1-s}})E^{(s)})\,(I_2^r\otimes H_2) \quad \textbf{(2.15)}$$

Avec N=2^r avec r ϵ N^* et $E^{(s)}$défini comme suit :

$$E^{(s)} = diag\left(E_{(1)}^{(s)}E_{(2)}^{(s)}E_{(2^{s-1})}^{(s)}\right), s = 1,2,3 \dots r \textbf{(2.16)}$$

$$E_{(n)}^{(s)}=\begin{bmatrix} I_{2^{r+1-s}} & O_{2^{r+1-s}} \\ O_{2^{r+1-s}} & D_n^s \end{bmatrix}, \text{s=1, 2, 3 …r; n=1, 2, 3…} 2^{(s-1)} \textbf{(2.17)}$$

Avec O une matrice nulle et D_n^s défini comme suit :

$$D_{(n)}^{(s)} = diag\left(1, d_{(n,1)}^{(s)}, d_{(n,2)}^{(s)},, \dots, d_{(n,2^{r+1}-1)}^{(s)}\right) \qquad \textbf{(2.18)}$$

Où $d_{(n,m)}^{(s)}$, n =1, 2,3,…,2^{s-1} et m = 1, 2,3, …,2^{r+1-s}-1, ce sont des paramètres indépendants.

La transformée ROP récursive offre $\mathrm{N}\log_2\left(\frac{N}{2}\right)+1$ paramètres indépendants grâce à l'utilisation d'une approche récursive par la décomposition des matrices ROP en un produit Kronecker de matrices creuses. De plus, la transformée ROP récursive maintient les propriétés de la transformée ROP.

Les paramètres indépendants des matrices ROP peuvent être exploités par la méthode DRPE comme une clé secrète additionnelle comme le montre la figure 2.5 [22][3].

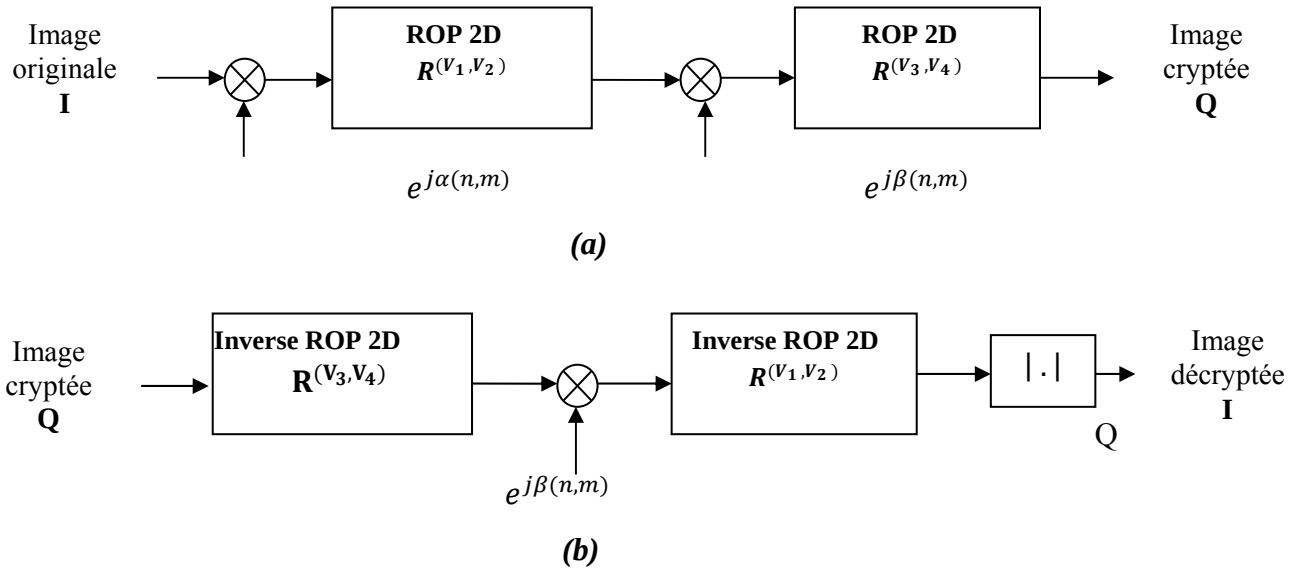


Figure 2.5.Méthode de cryptage DRPE basée sur la transformée ROP récursive (b) Cryptage, (b) Décryptage

2.4. Conclusion

Dans ce chapitre, nous avons vu le concept de cryptage d'images basé sur la méthode DRPE. Ensuite, nous avons vu comment il est possible d'améliorer la sécurité de la méthode DRPE par l'introduction de transformées paramétriques. Nous avons également revu la théorie des transformées paramétriques les plus utilisées en cryptage DRPE telles que la transformée TFFrD, la TFFrD à paramètres multiples, la transformée ROP ainsi que la transformée ROP récursive.

CHAPITRE 3

Introduction du chaos

3.1. Introduction

La théorie du chaos consiste à étudier le comportement des systèmes dynamiques non linéaires [21] représenté par des équations déterministes qui peuvent avoir un comportement chaotique si elles sont utilisées de façon itérative en des suites dites chaotiques [23].

Le comportement chaotique de ces suites est dû à la forte sensibilité et dépendance à leurs paramètres et conditions initiales [21]. Cette sensibilité a été exploitée par Lang et al. [5]en cryptage DRPE basé sur les transformées paramétriques où des fonctions de permutations chaotiques spatiales et/ou fréquentielles ont été introduites [5].Ces permutations sont basées sur des suites chaotiques où leurs paramètres et conditions initiales peuvent être considérées comme une clé secrète de cryptage additionnelle [2][5].

Dans ce chapitre, nous allons présenter tous d'abord l'analogie entre les propriétés des suites chaotiques et les propriétés de confusion et de diffusion en cryptographie ensuite nous allons revoir en détail les différentes définitions mathématiques de différentes suites chaotiques connues. Enfin, nous allons revoir en détail la fameuse méthode de Lang qui fait l'objet de notre étude comparative lors du prochain chapitre.

3.2. Propriétés du chaos en cryptographie

Autre que la sensibilité aux conditions initiales, les suites chaotiques sont pseudo-aléatoires et ergodiques [2]. Ces propriétés sont analogues aux propriétés de la confusion et la diffusion en cryptographie [11].

3.2.1. Sensibilité aux conditions initiales

Les suites chaotiques sont très sensibles à leurs conditions initiales où un petit changement dans l'état initiale peut provoquer un changement radical dans l'état final [2][23]. Il existe un digramme dit diagramme de bifurcation qui permet d'observer ce comportement chaotique de manière graphique [2][23]. Cette grande sensibilité est exploitée en cryptographie où leurs paramètres sont considérés comme une clé secrète de cryptage [24][2].

3.2.2. Pseudo-aléatoires

Les suites chaotiques sont basées sur des équations déterministes et non probabiliste, cela veut dire que des équations déterministes peuvent avoir un comportement aléatoire [2][23] ce

qui permet d'exploiter les suites chaotiques en cryptographie comme des générateurs de nombres pseudo-aléatoires [2][23].

3.2.3. Ergodiques

Un processus chaotique est ergodique parce que quel que soit la distribution de la variable présente en entré il possède la même distribution en sortie [2].

3.3. Les suites chaotiques

Dans le cadre de notre étude on se limitera seulement aux suites chaotiques les plus utilisées en cryptographie telles que la suite logistique [2][23], la suite Tente[23], la suite Henon [23] et les suites chaotiques linéaires par morceaux PWLCM (Piece wise Linear Chaotic Map) [2][23]

3.3.1. Suite logistique

Une suite logistique ou Logistic Map en anglais est définie comme suit [2][23]

$$x_{i+1} = \mu . x_i . (1 - x_i) \qquad \textbf{(3.1)}$$

où $x_i \in (0,1)$ avec $i \in \mathbb{N}$, x_0 comme condition initiale et $\mu \in (0,4)$ comme paramètre de contrôle.

La figure 3.1 illustre le diagramme de bifurcation de la suite logistique qui représente le comportement de la suite logistique en fonction de x_i et de μ dans le cas de plusieur sitérations.

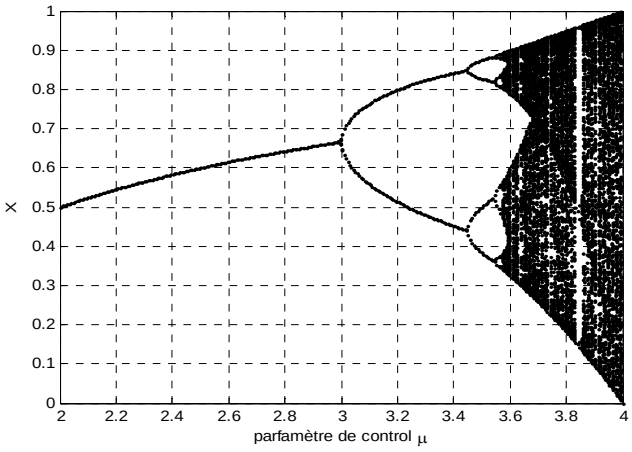


Figure 3.1. Diagramme de bifurcation de la suite logistique

D'après ce diagramme on peut remarquer que le comportement est linéaire au début puis il devient chaotique lorsque $\mu \in (3.52, 4)$. On remarque aussi qu'il y a des intervalles non

chaotiques appelés fenêtres [25]. Ainsi la suite logistique devient purement chaotique seulement lorsque $\mu = 4$.

3.3.2. Suite Tente :

La suite Tente est obtenue à partir de l'équation mathématique suivante [26] :

$$X_{n+1} = T_{\mu}(x_n) = \begin{cases} \mu\, x_n & , \ x_n < \frac{1}{2} \\ \mu\,(1 - x_n) & , \ \frac{1}{2} \leq x_n \end{cases} \quad \textbf{(3.2)}$$

Où x_n varie dans l'intervalle (0,1) et μ le paramètre de contrôle varie dans l'intervalle (0.2) .La figure (3.2) illustré la forme de la suite tente.

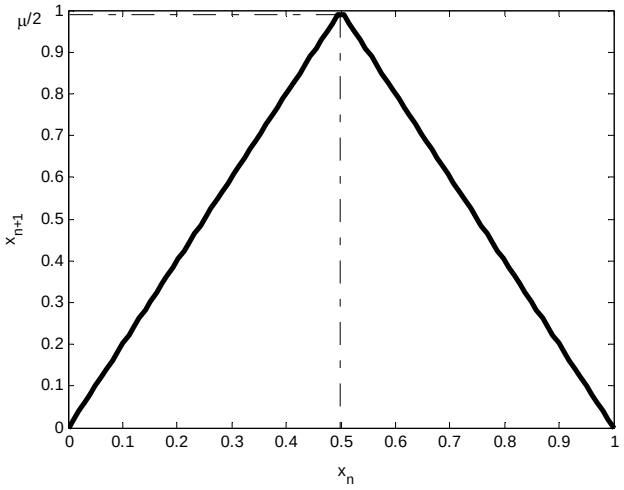


Figure 3.2. Forme de la fonction de la suite tente

La figure (3.3) illustre le diagramme de bifurcation de la suite Tente.

D'après le diagramme de bifurcation on remarque qua la suite chaotique tente est purement chaotique lorsque $\mu = 2$.

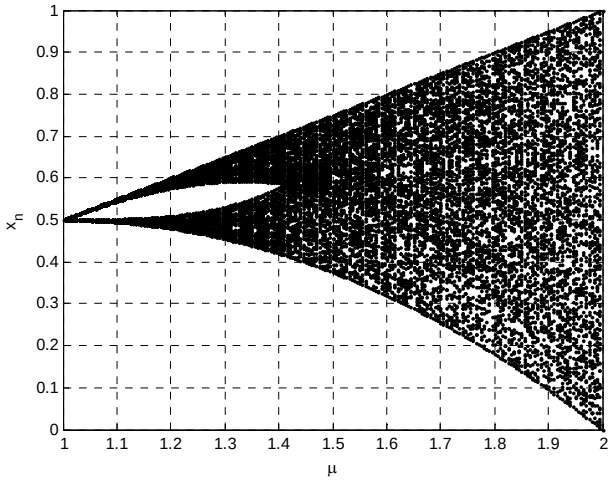


Figure 3.3. Diagramme de bifurcation de la suite Tente

3.3.3. Suite Henon :

La suite de Henon est définie comme suit [21] :

$$\begin{cases} x = 1 - \mathrm{a}.\mathrm{x}^2 + \mathrm{y} \\ y = b.x \end{cases} \qquad \textbf{(3.3)}$$

Il faut noter que l'équation **(3.3)** peut être écrite sous une forme unidimensionnelle lorsque en remplace y par son équivalant

$$x = 1 - \mathrm{a}.\mathrm{x}^2 + \mathrm{b}.\mathrm{x} \quad \textbf{(3.4)}$$

Où a est un paramètre de control de non linéarité et b la dissipation de chaque itération. Leurs valeurs sont en général constantes : a=1.4 et b=0.3.

La figure 3.4illustre le diagramme de bifurcation de la suite Henon qui représente le comportement de la suite en fonction de x_i et a pour plusieurs itérations.

D'après le diagramme de bifurcation on remarque qu'il devient chaotique seulement lorsque a $\in$ (1.05, 1.4) mais il y a toujours des fenêtres non chaotiques. On peut dire que la fonction et purement chaotique seulement lorsque a= 1.4 [21].

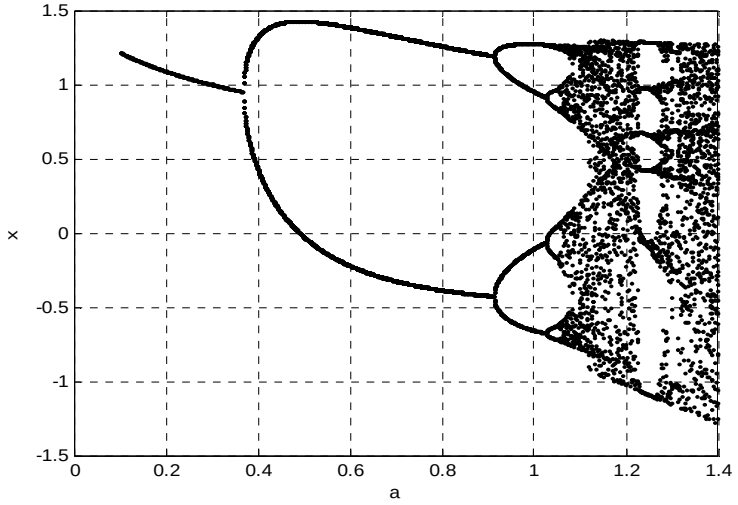


Figure 3.4 Diagramme de bifurcation de la suite Henon

3.3.4. Suite chaotique linéaire par morceaux PWLCM

Une suite chaotique linéaire par morceaux ou PWLCM est définie comme suit [2][23]:

$$x(n+1) = F(z_i, \lambda)\begin{cases} \frac{z_i}{\lambda}\ 0 \le z_i < \lambda \\ \frac{z_i-\lambda}{0.5-\lambda}\lambda \le z_i < 0.5 \\ F(1-z_i, \lambda) 0.5 \le z_i < 1 \end{cases} \quad (3.5)$$

où $z_i \in (0,1)$ avec $i \in \mathbb{N}$, z_0 comme condition initiale et $\lambda \in (0,0.5)$ comme paramètre de contrôle.

Contrairement aux autres suites chaotiques, la suite chaotique linéaire par morceaux PWLCM est chaotique sur tout l'intervalle de définition du paramètre de controlλ comme l'illustre le diagramme de bifurcation dans la figure 3.5.

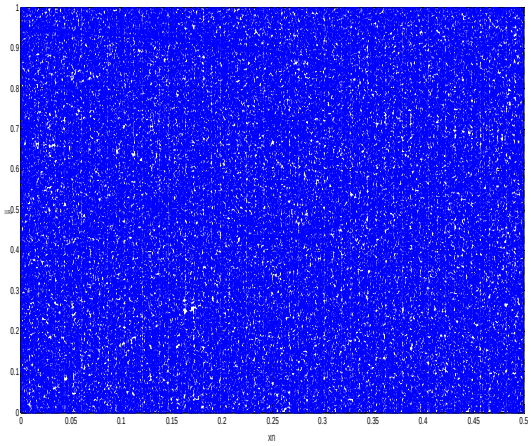


Figure 3.5. Diagramme de bifurcation de la suite chaotique linéaire par morceaux PWLCM

3.4. Présentation de la méthode de Lang

Lang et al. ont proposé dans [5] d'introduire l'utilisation des suites chaotiques dans la méthode DRPE de cryptage d'images en remplaçant le masque complexe de phases aléatoires dans le domaine fréquentiel par une fonction de permutation basée sur une suite logistique chaotique ce qui a pour but de rendre l'algorithme de cryptage plus simple mais avec un niveau de sécurité plus élevé[5].

3.4.1. Fonction de permutation basée sur la suite logistique

Soit une image **I** de taille $N \times M$. Lang et al. ont proposé dans [5] une fonction de permutation basée sur la suite logistique définit selon les étapes suivantes [2] [5]:

- Générer un vecteur **X** de nombres réels aléatoires en utilisant L'équations (3.1) de suite logistique avec x_0 conditions initiales et k le paramètre de contrôle soigneusement choisi de sorte que la suite logistique reste purement chaotique. Choisir un nombre arbitraire **t** pour identifier le début de la suit chaos généré et on fait une troncation d'une vecteur de 1×N×M a partir de vecteur **X** généré par la suite chaotique utilisée.
- Trier les éléments du vecteur **X** dans un ordre croissant ou bien un ordre décroissant.
- Enregistrer les différents changements dans les index des éléments du vecteur **X** dans un vecteur **Y** appelé vecteur de permutation.
- Redimensionner la matrice d'image **I** en un vecteur de taille $1 \times N \times M$
- Permuter les éléments du vecteur de l'image selon les éléments du vecteur de permutation **Y** afin d'obtenir un nouveau vecteur **K** tel que :$\mathbf{k}_n = \mathbf{i}_n(\mathbf{y}_n)$

- Redimensionner le vecteur **K** obtenue en une matrice de taille $N \times M$ afin d'obtenir la matrice de l'image permutée.

Les étapes précédentes sont présentées par une fonction de permutation notée $P\{x, k, t\}$, x est la condition initiale de la suite chaos et k est le paramètre de control et t est la valeur de début de la troncation.

Pour faire l'inverse de permutation il suffit d'inverser les étapes précédentes et la fonction de permutation inverse noté$P^{inv}\{x, k, t\}$.

3.4.2. Algorithme de cryptage

Soit une image **I** de taille **N×M.** selon Lang et al et nous avons prendre le domaine de la **TFFrD** a paramètre multiple. L'algorithme de cryptage est définit par les étapes suivantes [5] :

- Multiplication élément par élément avec un masque de phases aléatoire $e^{j\alpha(n,m)}$
- Permutation par une première fonction de permutation chaotique $P_1\{x_1, k_1, t_1\}$ou x_1, k_1, t_1 sont respectivement, la condition initiale, le paramètre de contrôle et le paramètre de troncation de la suite logistique.
- Application de la **TFFrD** a paramètre multiple **2D** $\mathbf{F}^{\vec{a}}$, $\boldsymbol{F}^{\vec{b}}$ où $\vec{a}$ et $\vec{b}$ sont les vecteurs d'ordres fractionnaires (paramètres) de la transformée.
- Permutation par une deuxième fonction de permutation chaotique $P_2\{x_2, k_2, t_2\}$ou x_2, k_2, t_2 sont respectivement, la condition initiale, le paramètre de contrôle et le paramètre de troncation de la suite logistique.
- Application de la **TFFrD** a paramètre multiple **2D** $\mathbf{F}^{\vec{c}}$, $\boldsymbol{F}^{\vec{d}}$ où $\vec{c}$et $\vec{d}$ sont les vecteurs d'ordres fractionnaires (paramètres) de la transformée pour obtenir l'image cryptée finale que l'on note **Q**.

Toutes ces étapes de l'algorithme de cryptage peuvent être résumées par l'équation (3.6) et dans la figure **3.6**.

$$Q = F^{(\vec{c}\ ,\ \vec{d})}\left[P_{2\ \{x2,\ k2\ ,\ t2\}}\left(F^{(\vec{a}\ ,\ \vec{b})}\left[P_{1\{x1,k1,t1\}}\left(I\ \odot\ \left[e^{j\,\alpha\,(x,y)}\right]\right)\right]\right)\right] \quad (3.6)$$

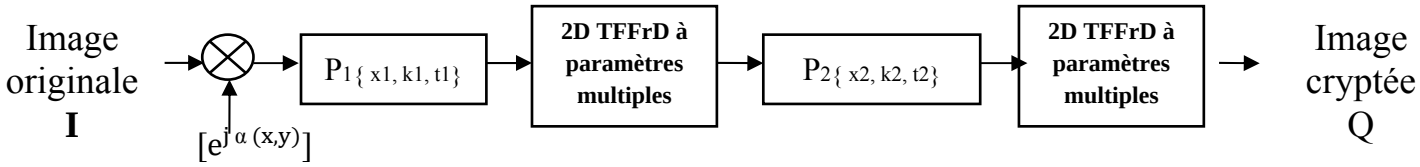


Figure 3.6 Algorithme de cryptage de la méthode de Lang

La clé secrète de cryptage est composée des vecteurs des paramètres de la transformé$\vec{a}$, $\vec{b}$, $\vec{c}$,$\vec{d}$,mais aussi des paramètres de la fonction de permutation chaotique qui sont la condition initiale x_0, le paramètre de control k et le nombre de troncation t.

3.4.3. Algorithme de décryptage

Soit l'image cryptée **Q** précédente**.** Son algorithme de décryptage est définit par les étapes suivantes [5]

- Calculer **Q*** qui est le conjugué de l'image cryptée **Q**.
- Application de la transformé **TFFrD** a paramètre multiple 2D $F^{\vec{c}}, F^{\vec{d}}$
- Permutation par une fonction de permutation chaotique inverse $P_2^{inv}\{x_2, k_2, t_2\}$ avec les paramètres x_2, k_2, t_2précédents.
- Application de la transformé **TFFrD** a paramètre multiple 2D $F^{\vec{a}}, F^{\vec{b}}$
- Permutation par une fonction de permutation chaotique $P_1^{inv}\{x_1, k_1, t_1\}$avec les paramètres x_1, k_1, t_1 précédents.
- Prendre le module de l'image complexe ainsi obtenu pour retrouver l'image originale **I**.

Toutes ces étapes de l'algorithme de décryptage peuvent être résumées par l'équation **(3.7)** mais aussi par la figure **3.7**.

$$\mathbf{D} = | [P_1^{inv}{}_{\{x1,k1,t1\}} (F^{(\vec{a}\ ,\ \vec{b})} [P_2^{inv}{}_{\{x2,\ k2\ ,\ t2\}} (F^{(\vec{c}\ ,\ \vec{d})} (Q^*))])] | \quad (3.7)$$

Q* est la conjugue de l'image cryptée I.

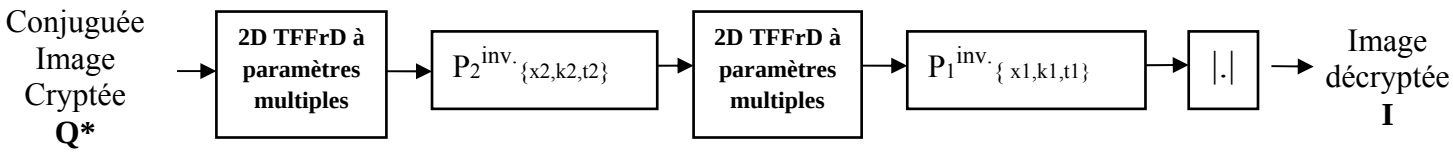


Figure 3.7 Algorithme de décryptage de la méthode de Lang

La clé secrète de décryptage est composé de les paramètres de la transformé **TFFrD** a paramètre multiple inverse $\vec{a},\vec{b},\vec{c},\vec{d}$, et aussi de les paramètres de les fonction de permutation chaotique inverse ; la condition initiale x_0, la condition de control k et le début de la troncation t.

3.5. Conclusion :

Dans ce chapitre nous avons vu quatre suites chaotiques qui sont la suite logistique, la suite tente, la suite Hénon et la suite chaotique linéaire par morceaux PWLCM. Nous avons aussi vu les algorithmes de cryptage et de décryptage de la méthode de Lang ; Le chapitre contient aussi une explication bien détaillé sur la fonction de la permutation chaotique utilisé ;tous cela pour faire une étude comparative dans le chapitre suivants entre les différents suites chaos et les transformé paramétriques de la méthode de Lang.

CHAPITRE 04

Etude comparative

4.1. Introduction

Dans la méthode de Lang, les auteurs ont utilisé la suite logistique dans la fonction de permutation spatiale et fréquentielle et la transformée TFFrD à paramètre multiple comme transformées paramétriques, cependant, il existe plusieurs transformées paramétriques et il existe aussi différentes suites chaotiques.

De ce fait, nous présentons dans ce chapitre une étude comparative basée sur la méthode de Lang en fonction de la transformée paramétrique

Sélectionnée parmi les transformées paramétriques connues telles que la transformée ROP et sa version récursive, ainsi que la transformée TFFrD. De la même façon, nous présentons dans ce chapitre une étude comparative basée sur la méthode de Lang en fonction de la suite chaotique sélectionnée parmi les suites chaotiques connues telles que de la suite PWLCM, Tente ou Henon. Mais avant cela, nous présentons quelques tests et critères d'évaluation et de comparaison qui nous servirons à mener à bien notre étude comparative.

4.2. Critères d'évaluation et de comparaison

Il existe plusieurs tests d'évaluation des méthodes de cryptage basés sur les transformées paramétriques et le chaos [2].Tous ces tests serviront dans notre étude comparative comme des critères d'évaluation et de comparaison en termes de performances et de sécurité.

4.2.1. Erreur quadratique moyenne EQM

Le calcul de l'erreur quadratique moyenne (EQM) permet de déterminer la sensibilité de la clé secrète [9] et ainsi déterminer l'espace de la clé de la méthode de cryptage étudiée.

Supposons une image décryptée I′ de taille N × M et son image originale I. L'équation de l'EQM dans ce cas est définie comme suit :

$$EQM\ (I', I)\ =\ \frac{1}{N \times M} \sum_{n=1}^{N} \sum_{m=1}^{M} \left(I'(n,m) - I(n,m) \right)^2 \qquad \textbf{(4.1)}$$

4.2.2. Analyse des histogrammes

Un histogramme est une représentation graphique de la distribution des différents pixels d'une image [2].

Dans le cas du cryptage d'images basé sur les transformées paramétriques, l'image cryptée est de forme complexe, de ce fait, il faudra calculer l'histogramme du module ainsi que celui de la phase après normalisation [2].

L'analyse des histogrammes des images cryptées a pour rôle de vérifier la robustesse de la méthode étudiée contre d'éventuelles attaques statistiques. Ces histogrammes doivent être [27] :

- Complètement différent de l'histogramme de l'image originale.
- Avoir une distribution pseudo-uniforme ou uniforme peu importe l'image à crypter.

4.2.3. Coefficient de corrélation

Le coefficient de corrélation permet d'évaluer la qualité de cryptage d'une image [2] [27].

Supposons une image originale X et sa version cryptée Y, le coefficient de corrélation entre ces deux images que l'on note $\boldsymbol{c_{XY}}$ est calculé comme suit [3]:

$$\boldsymbol{c_{XY}} = \frac{\boldsymbol{cov(X,Y)}}{\sqrt{\boldsymbol{D(X)}}\sqrt{\boldsymbol{D(Y)}}} \textbf{(4.2)}$$

Où cov (x, y)est la covariance. D(x) et D(y) sont la variance de X et Y avec [2]:

$$E\ (X)\ = \frac{1}{L}\sum_{l=1}^{\mathrm{L}} \boldsymbol{x_l} \textbf{(4.3)}$$

$$D\ (X)\ = \frac{1}{L}\sum_{l=1}^{L}(\boldsymbol{x_l}\text{- E(x)})^2 \textbf{(4.4)}$$

$$Cov\ (X,Y) = \frac{1}{L}\sum_{l=1}^{L}(\boldsymbol{x_l} - \text{E(x)})\ (\boldsymbol{y_l} - \text{E}(\boldsymbol{y}\ \ )) \textbf{(4.5)}$$

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

Dans ce cas, la qualité du cryptage est meilleure lorsque le coefficient de corrélation entre l'image originale X et l'image cryptée Y est proche du zéro [2].

4.2.4. Rapport signal sur bruit crête à crête

Le rapport signal/bruit crête à crête ou PSNR (Peak Signal to Noise Ratio) exprimé en décibel (dB) permet de mesurer la qualité visuelle d'une image.

Supposons une image cryptée ou bruitée I' et sa version originale non-cryptée et non-bruitée I. Dans ce cas, le PSNR entre l'image originale et l'image altérée est calculé comme suit [3] [2] :

$$\text{PSNR} = 10\ \log_{10}\left[\frac{(255)^2}{\text{EQM}(I',I)}\right] \textbf{(4.6)}$$

4.2.5. Résistance au bruit additif blanc gaussien

Pour vérifier la résistance d'une méthode de cryptage contre le bruit additif gaussien définit comme suit [4]:

$$c' = c\ (1 + \sigma G) \quad \textbf{(4.7)}$$

Où c' est l'image cryptée bruitée, et σ le coefficient de puissance. G est un bruit blanc de distribution Gaussienne [2].

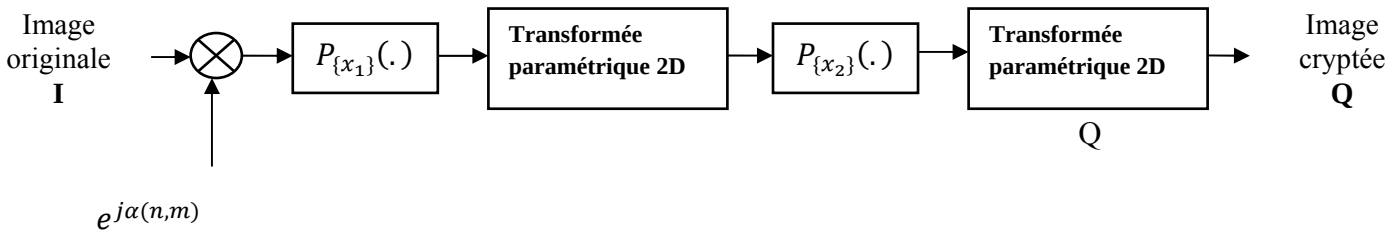
Après le décryptage correct de l'image cryptée et bruitéec'on doit calculer le PSNR et EQM entre l'image originale et l'image décryptée afin d'évaluer la résistance de la méthode de cryptage au bruit additif blanc gaussien [2].

4.3. Etude comparative selon les transformées paramétriques

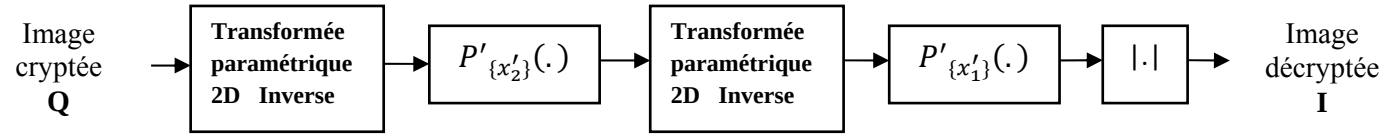
Dans un premier temps, nous proposons une étude comparative entre les performances des transformées paramétriques dans la méthode de Lang (voir chapitre 3 section (3.4 .1)). Pour réaliser cela, nous allons remplacer la TFFrD à paramètres multiples dans la méthode originale de Lang par d'autres transformées paramétriques connues en comparant leurs performances et résistances aux différents tests et attaques.

La figure 4.1 montre la méthode de Lang modifiée dans ce cas-là où la transformée paramétrique utilisée peut être :

- Transformée ROP.
- Transformée ROP récursive.
- Transformée TFFrD.
- Transformée TFFrD à paramètres multiples.



(a)



(b)

Figure 4.1. Méthode de Lang modifiée en fonction de la transformée paramétrique
(a) Cryptage, (b) Décryptage

4.3.1. Résultats des simulations et discussions

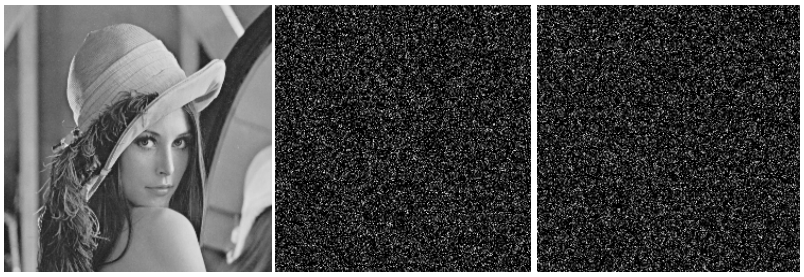
Nos simulations ont été réalisées sous le logiciel MATHSWORK MATLAB 2013. Nous avons utilisé des images standards de niveau gris8bits de tailles carrées 256 x 256 telles que Lenna, Cameraman, Mandrill et Boat.

Vu le nombre important des résultats identiques entre les images on se limitera seulement au cas de l'image Lenna, pour le reste des images, on se limitera seulement aux résultats plus intéressants.

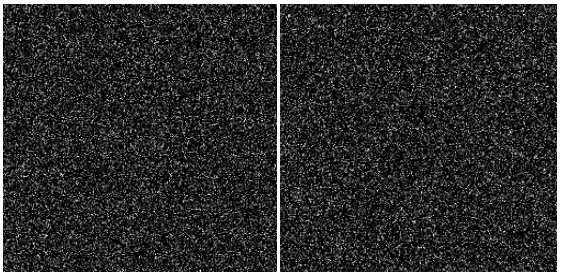
La clé de cryptage utilisée dans tous les cas est donnée comme suit :

- {x1, k1, t1} = {0.24, 3.81, 4000}
- {x2, k2, t2} = {0 .31, 3.71, 4200}
- Paramètres des transformées choisis selon la transformée paramétrique à étudier

Soit l'image Lenna sur la figure 4.2 (a). Dans ce cas, la figure 4.2 (b), (c), (d) et (e) montrent les résultats de cryptage de l'image Lenna en fonction de la transformée paramétrique utilisée dans la méthode de Lang.



a) Image Lenna b) ROP c) ROP récursive



d) TFFrD e)TFFrD à paramètres multiples

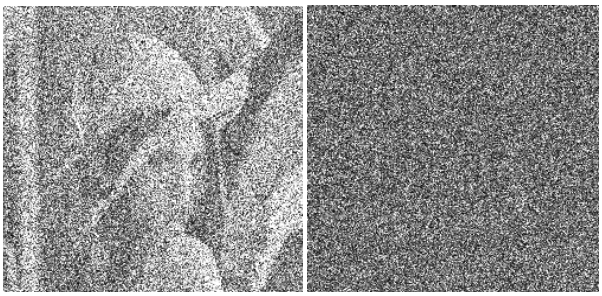
Figure 4.2. Résultats de comparaison du cryptage en fonction de la transformée paramétrique

D'après la figure4.2 nous remarquons que l'image originale est complètement cryptée quel que soit la transformée paramétrique utilisée dans la méthode de Lang. Cependant, cette comparaison reste subjective.

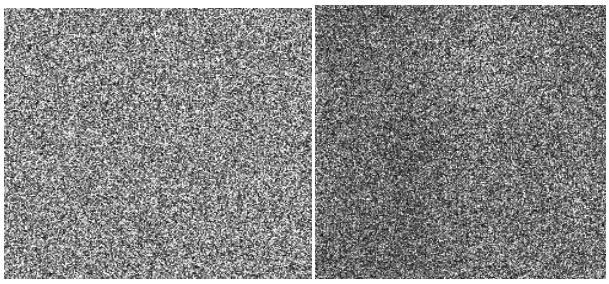
4.3.2. Comparaison de la sensibilité de la clé

Pour déterminer la sensibilité des paramètres de chaque transformée paramétrique dans la méthode de Lang nous avons introduit à chaque fois une erreur de déviation dans les paramètres correctes de la transformée lors de l'étape du décryptage de l'image Lenna. Les résultats sont présents dans la figure 4.3.

D'après la figure 4.3, nous remarquons que dans la méthode de Lang modifiée, les transformées paramétriques ROP récursive, TFFrD et TFFrD à paramètres multiples ont protégé avec succès l'image Lenna originale malgré la présence d'une déviation minime dans leurs paramètres alors que la transformée ROP n'a pas réussi à cela du fait de sa sensibilité moins élevée par rapport aux autres transformées paramétriques. Cependant, cette comparaison reste subjective.



a) Cas ROP b) Cas ROP récursive



c) Cas TFFrD d) Cas TFFrD à paramétres multiples

Figure 4.3. Résultats décryptage avec les paramètres de la transformée paramétrique incorrect

Pour déterminer de manière objective la sensibilité des paramètres de chaque transformée paramétrique dans la méthode de Lang nous avons calculons l'EQM entre l'image Lenna originale et sa version décryptée en fonction d'une erreur de déviationδtrès minime introduite dans les paramètres de la transformée. Les résultats de calcul sont présentés dans la figure 4.4.

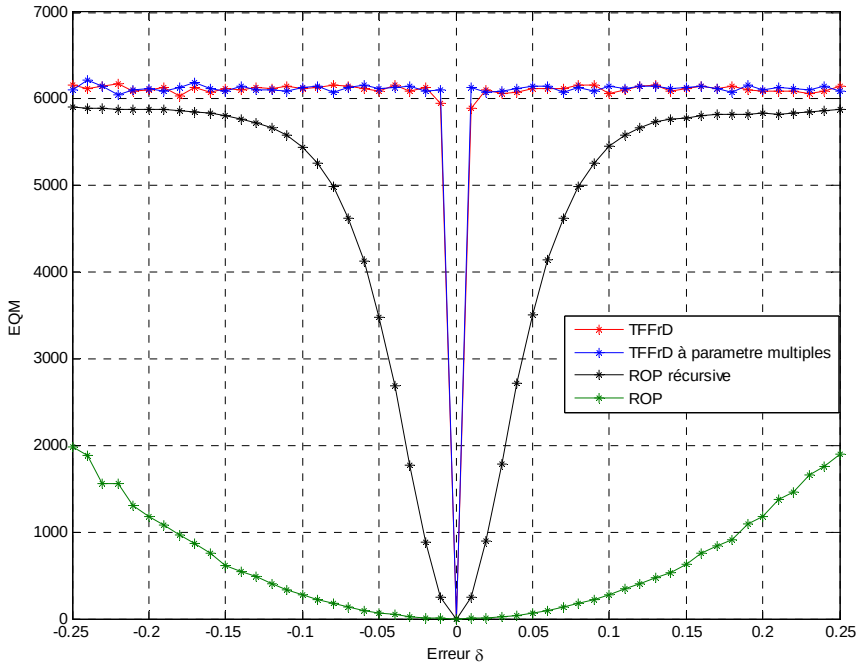


Figure 4.4. Résultats de comparaison de l'EQM en fonction de la transformée paramétrique

D'après les résultats de la figure 4.4, nous remarquons que les paramètres de la TFFrD à paramètres multiple sa une sensibilité très élevée par rapport aux autres transformées paramétriques, cette sensibilité est de l'ordre de 0.01

La TFFrD à paramètre unique sa sensibilité est de l'ordre de 0.01, la transformée ROP et ROP récursive ont respectivement une sensibilité de l'ordre de 0.25 et 0.1

4.3.3. Comparaison de l'espace de la clé

Pour N = 256, le tableau 4.1. Montre le nombre de paramètres indépendants qu'offre chaque transformée paramétrique (voir chapitre 2) utilisée dans notre étude comparative.

Tableau 4.1. Nombre de paramètres d'une transformée paramétrique dans le cas N=256

Transformée paramétrique	**Nombre de paramètres**
ROP	127
ROP récursive	769
TFFrD	1
TFFrD à paramétre multiples	256

D'après le tableau 4.1, on remarque à l'avance que le nombre de paramètres de la transformée ROP récursive est largement supérieur à celui des autres transformées. Néanmoins, vu les résultats précédents de la sensibilité de la clé, le nombre de paramètres ne peut être considéré comme un critère de comparaison de l'espace de la clé de la méthode de Lang utilisée sans en prendre en considération la sensibilité des paramètres aux erreurs.

Pour déterminer l'espace de la clé de la méthode de Lang en fonction des transformées paramétriques, nous devons exploiter les résultats précédents de la sensibilité de chaque clé, à savoir la sensibilité de la clé aux paramètres des transformées en plus de sa sensibilité aux paramètres des suites logistiques.

La sensibilité de la méthode Lang aux paramètres des fonctions de permutation est de l'ordre de 10^{10}[17], soit un espace clé de l'ordre de 10^{10}x10^{10}.

De la même façon, en exploitant les résultats précédents sur la sensibilité de la méthode de Lang aux paramètres des transformées nous obtenons le tableau 4.2 qui détermine l'espace clé globale de la méthode Lang en fonction de la transformée paramétrique utilisée.

Tableau 4.2. Espace de la clé de la méthode Lang en fonction des transformées paramétriques

Transformée paramétrique utilisée	Espace de la clé
ROP	$64^{4\times127} \times 10^{20}$.
ROP récursive	$400^{4\times769} \times 10^{20}$
TFFrD	$200^{4} \times 10^{20}$
TFFrD à paramétre multiples	$200^{4\times256} \times 10^{20}$

D'après les résultats obtenus dans le tableau précédent on remarque que l'espace de clé est toujours supérieur au seuil de2^{128} garantissant une résistance aux attaques par force brute [18].

4.3.4. Analyse des histogrammes

Nous avons calculé les histogrammes de Lenna originale, Lenna cryptée (module et phase) par la méthode de Lang en fonction de la transformée paramétrique utilisée. Les résultats sont illustrés dans les figures 4.5, 4.6 et 4.7.

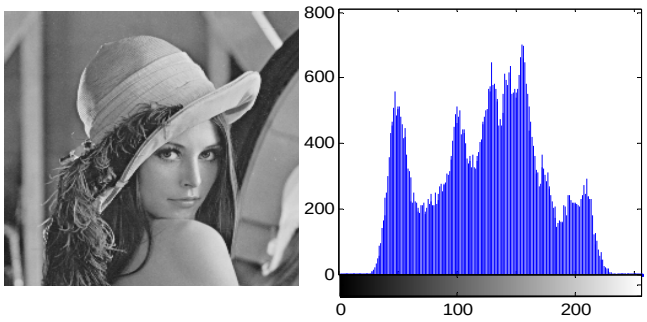
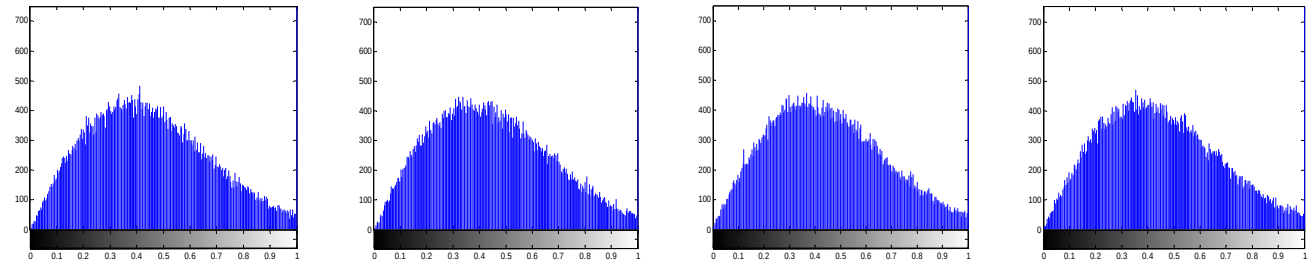
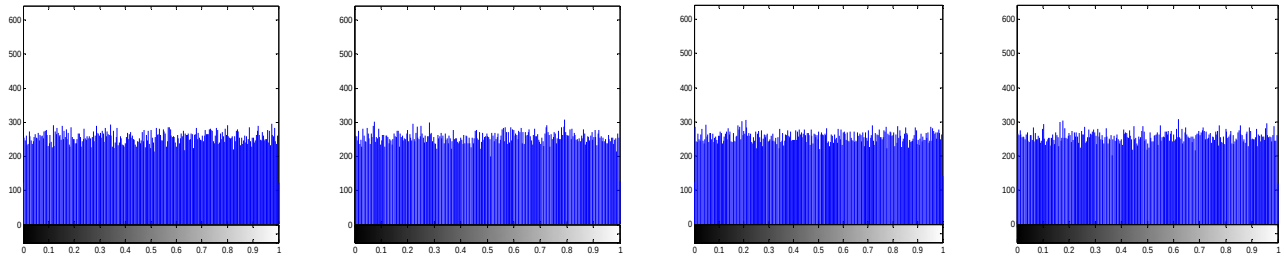


Figure 4.5. Histogramme de l'image Lenna



a) ROP b) ROP récursive c) TFFrD d) TFFrD à paramètres multiples

Figure 4.6. Histogrammes du module de l'image Lenna cryptée complexe



a) ROP b) ROP récursive c) TFFrD d) TFFrD à paramètres multiples

Figure 4.7. Histogramme de la phase de l'image Lenna cryptée complexe

D'après ces figures, on remarque que l'histogramme du module et l'histogramme de la phase de l'image complexe cryptée est totalement différents de l'image originale quel que soit la transformée paramétrique utilisée. On peut dire que ces histogrammes sont uniformes et ne contiennent pas une information sur l'image originale ce qui montre que peu importe la transformée paramétrique utilisée, la méthode Lang maintient sa résistance contre les attaques statistiques.

4.3.5. Qualité du cryptage

Afin d'évaluer la qualité de cryptage de façon objective, nous calculons le PSNR et le coefficient de corrélation entre l'image cryptée et sa version originale. Comme l'image cryptée est complexe, nous calculons le coefficient de corrélation C_r de la partie réelle ainsi que le coefficient de corrélation c_i de la partie imaginaire. Les résultats sont présents dans les tableaux 4.3 et 4.4 en fonction de la transformée paramétrique utilisée et pour différentes images de tests standards.

D'après le tableau 4.4, nous remarquons que dans tous les cas le coefficient de corrélation entre l'image cryptée et l'image originale est proche du zéro. Cela démontre que la qualité de cryptage est acceptable quel que soit la transformée paramétrique utilisée.

Tableau 4.3.PSNR en fonction de la transformée paramétrique utilisée

Transformée / Image	ROP	ROP récursive	TFFrD	TFFrD à paramètres multiples
Lenna	19.2502	10.4394	10.2576	10.2655
Mandrill	19.0859	10.4822	10.8287	10.8165
Boat	19.1005	10.2136	10.2197	10.2453
Cameraman	19.4398	07.3110	06.8937	06.8615

Tableau 4.4. Coefficient de corrélation en fonction de la transformée paramétrique utilisée

Transformée / image	ROP		ROP récursive		TFFrD		TFFrD à paramètres multiples	
	c_r	c_i	c_r	c_i	c_r	c_i	c_r	c_i
Lenna	0.0034	-0.0085	-0.0080	-0.0085	0.0030	0.0053	-0.0068	-0.0057
Mandrill	-0.0070	-0.0020	-0.0053	0.0030	-0.0052	0.0016	0.0058	0.0041
Baot	0.0023	-0.0028	-0.0056	0.0023	-0.0029	0.0051	0.0014	-0.0016
Cameraman	0.0026	0.0097	0.0085	-0.0030	-0.0025	0.0049	0.0018	0.0022

4.3.6. Résistance au bruit du canal

Pour tester la résistance de ces méthodes contre l'attaque du bruit nous avons ajouté un bruit blanc gaussien de coefficient de puissance σ ensuite nous avons tracé l'EQM en fonction de la transformée paramétrique utilisée dans la méthode Lang. Les résultats de simulation sont donnés dans la figure 4.8.

Nous remarquons que lorsque le coefficient du bruit est supérieur à 0.5, l'EQM devient important dans le cas de la transformée TFFrD alors qu'il est moindre dans le cas de la transformée ROP, cependant, cela n'influe pas beaucoup la qualité de décryptage comme le montre la figure 4.9 où on remarque que lorsque le coefficient du bruit est égal à 0.9nous constatons que l'image Lenna reste reconnaissable malgré un EQM différent. Par conséquent, ces résultats démontrent la résistance de la méthode de Lang contre le bruit additif quel que soit la transformée utilisée.

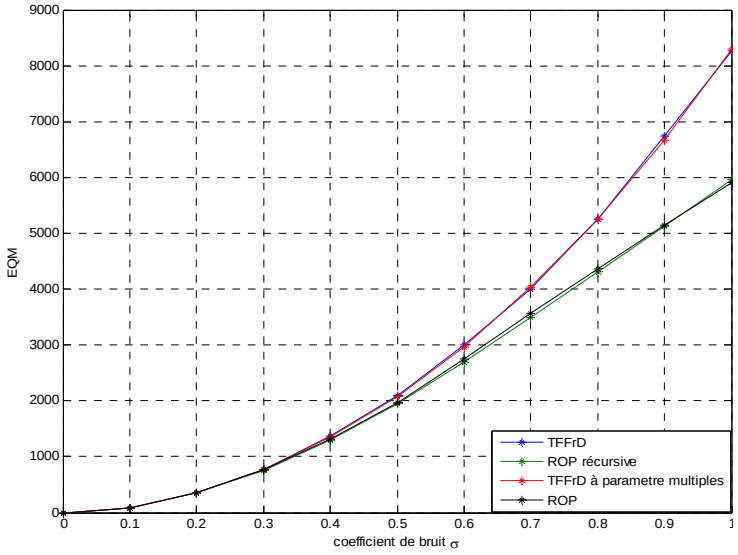
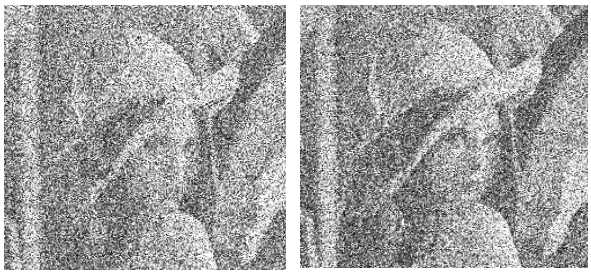
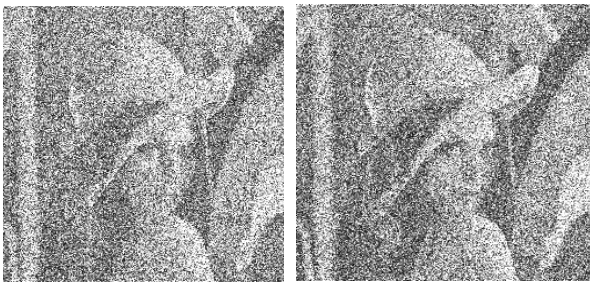


Figure 4.8.EQM en fonction du bruit additif et des transformées paramétriques



a) ROP, PSNR=10.4121 *b) ROPrécursive, PSNR=11.0255*



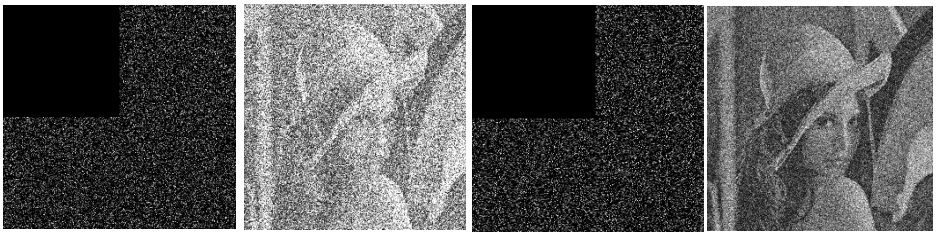
c)TFFrD, PSNR=9.8445 d) TFFrDà paramètres multiples, PSNR=9.8402

Figure 4.9. Résultats décryptage en fonction des transformées paramétriquesavec$\sigma = 0.9$

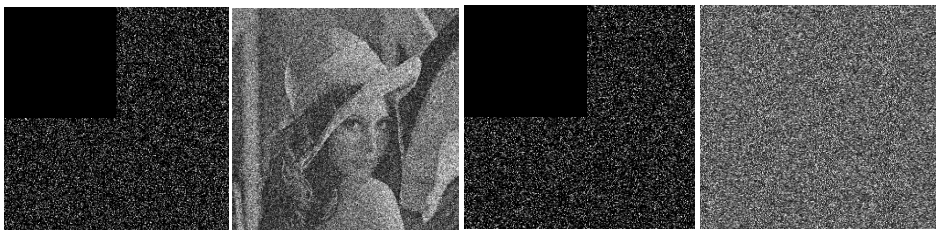
4.3.7 Résistance aux pertes d'informations

Pour tester la résistance de la méthode Lang contre les erreurs de transmission en fonction de la transformée paramétrique utilisée, nous remplaçant volontairement une zone des pixels de l'image Lenna cryptée par une zone de pixels noire d'une surface déterminée. Les résultats obtenus sont illustrés dans la figure 4.10 dans le cas d'une perte de 25% des pixels et la figure 4.11 dans le cas d'une perte de 50%.

D'aprés les Figures 4.10 et 4.11, nous remarquons que malgré un PSNR faible, l'image Lenna originale reste reconnaissable quelque soit la transformée sauf dans le cas de la TFFrD à paramètres multiples. En conséquence, ces résultats démontrent que la méthode Lang ne peut résister aux erreurs de transmission dans le cas où la transformée paramétrique utilisée est la TFFrD à paramétres multiples.

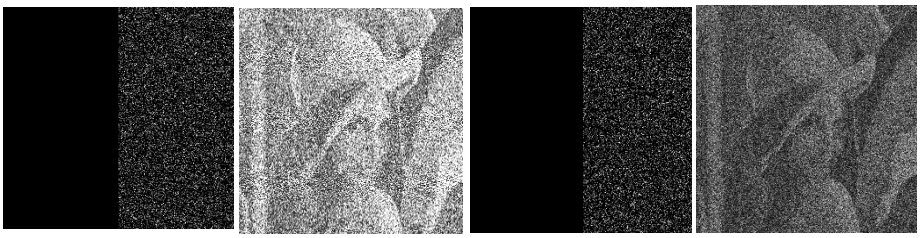


a) ROP, PSNR=10.4121 b)ROP récursive, PSNR=15.03

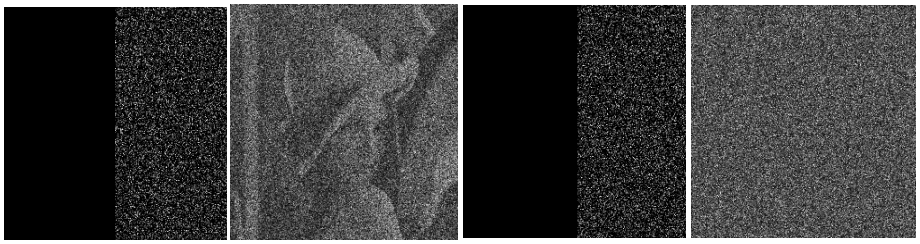


c)TFFrD, PSNR=*14.9923* d)TFFrD à paramétres multiples,PSNR=10.6400

Figure 4.10. Image décryptée dans le cas d'une perte de 25%



a)ROP, PSNR=10.3446 b) ROP récursive, PSNR=11.9473



c)TFFrD, PSNR=*11.9375* d) TFFrD à paramétres multiples,PSNR=10.4747

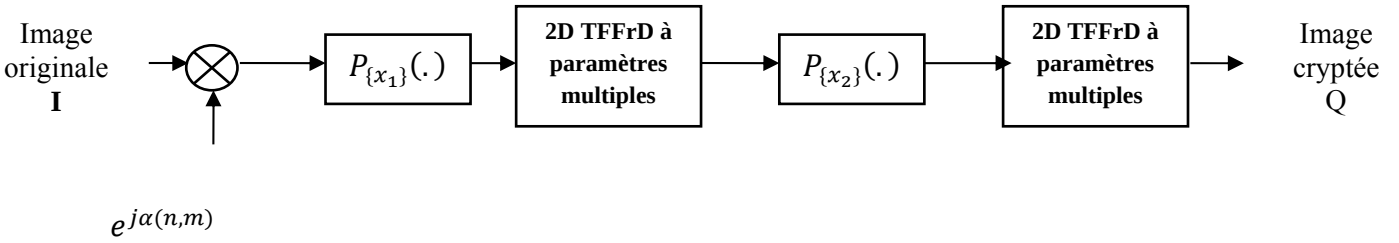
Figure 4.11. Image décryptée dans le cas d'une perte de 50%

4.4. Etude comparative selon les suites chaotiques

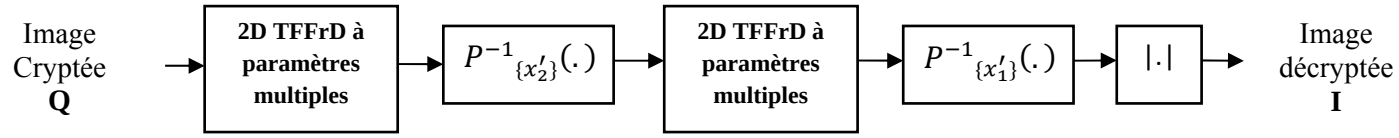
Dans l'étude comparative selon les transformées paramétriques nous avons vu que dans la méthode de Lang la TFFrD à paramètres multiples est plus performante que les autres transformées paramétriques, cependant, nous avons utilisé seulement la suite logistique comme suite chaotique, de ce fait, nous proposons une autre étude comparative selon les suites chaotiques en modifiant la méthode de Lang (chapitre 3 section 3.4) en laissant la TFFrD à paramètres multiples comme

transformée paramétrique et en remplaçant la suite logistique utilisée par la fonction de permutation par d'autres suites chaotiques connues dans le but de comparer leurs performances et leurs résistances aux différentes attaques et tests.

La figure 4.12 montre l'algorithme de la méthode de Lang modifiée dans ce cas-là.



(a) Cryptage



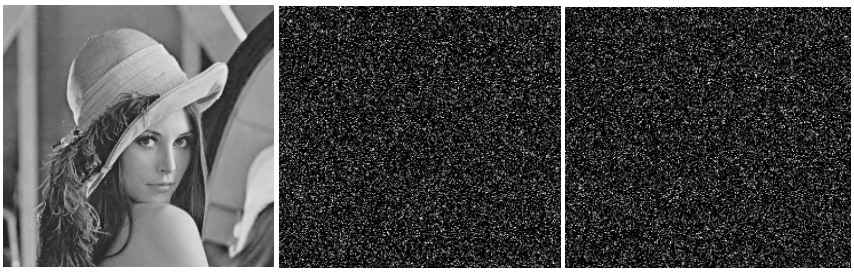
(b) décryptage

Figure 4.12.Méthode de Lang modifiée selon les suites chaotiques

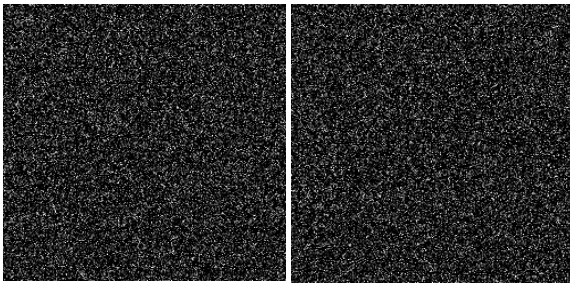
4.4.1. Résultats des simulations et discussions

Nos simulations ont été réalisées sous le logiciel Mathswork MATLAB version 2013 en utilisant des images standards monochrome 8bits de tailles carrées 256 x 256 telles que Lenna, Cameraman, Mandrill et Boat.

Ainsi, la figure 4.13 montre les résultats de cryptage de l'image Lenna dans le cas la méthode de Lang modifiée en fonction de différentes suites chaotiques .D'après la figure 4.13 nous remarquons que l'image originale est complètement cryptée quel que soit les suites chaotiques utilisées dans la méthode de Lang. Cependant, cette comparaison reste subjective.



a) Lenna b) logistique c)Henon



d) Tent e)PWLCM

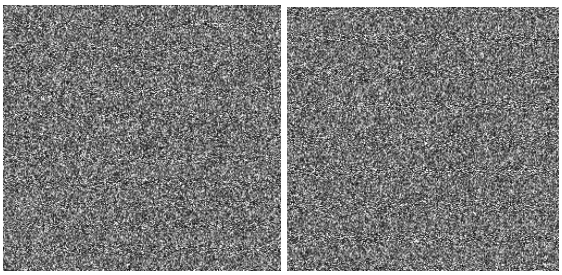
Figure 4.13. Résultats de comparaison du cryptage en fonction des suit chaotiques

4.4.2. Comparaison de la sensibilité de la clé

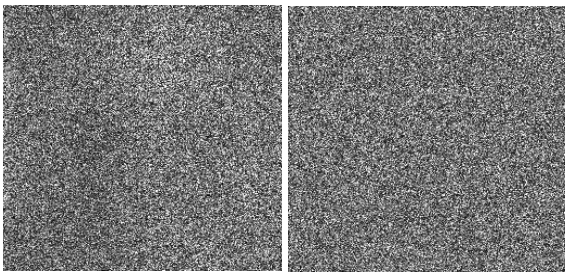
Afin de déterminer la sensibilité de la clé secrète de la méthode de Lang en fonction des différentes suites chaotiques sélectionnées, nous avons introduit à chaque fois une erreur de déviation minime dans les paramètres des fonctions de permutation, les résultats sont illustrés dans la figure 4.14.

D'après la figure 4.14, nous remarquons que la méthode de Lang a réussi à protéger l'image Lenna originale quelque soir la suite chaotique utilisée dans les fonctions de permutation.

Pour déterminer de manière objective la sensibilité des paramètres de ces suites chaotiques dans la méthode de Lang nous avons calculé l'EQM entre l'image Lenna originale et sa version décryptée en fonction d'une erreur de déviation δ très minime introduite dans les paramètres de la transformée TFFrD à paramètres multiples. Les résultats de calcul sont présentés dans la figure 4.15.



a) Cas suit logistique b) Cas Henon



c) Cas Tent d) Cas PWLCM

Figure 4.14. Résultats du décryptage avec les paramètres des fonctions de permutation incorrect

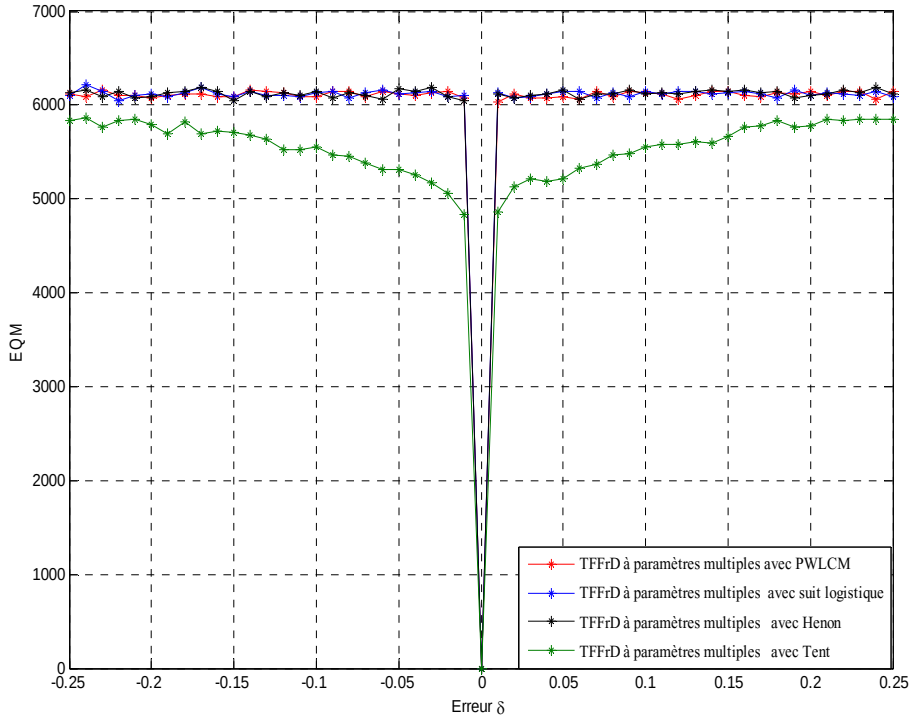


Figure 4 .15.Résultats de comparaison de l'EQM en fonction des suites chaotique

D'après les résultats de la figure 4.15, nous remarquons que la clé secrète de la méthode de Lang dans le cas du PWLCM a un EQM élevé par rapport aux autres méthodes avec une sensibilité de l'ordre de0.01 soit un espace clé de $\left(\frac{2}{0.01}\right)^{4\times256} = 200^{4\times256}$

4.4.3. Comparaison de l'espace de la clé

Tableau 4.5. Espace de la clé de la méthode Lang en fonction de les suit chaotiques

Suite chaotiques utilisée	**L'espace de clé**
Henon	$200^{4\times256} \times10^{0.7}\times10^{0.7}$
Suit Logistique	$200^{4\times256} \times10^{32}$
Pwlcm	$200^{4\times256} \times10^{32}\times 25 \times10^{32}$
Tent	$200^{4\times256}$

D'après les résultats obtenus dans le tableau précédent on remarque que l'espace de clé est toujours supérieur au seuil de 2^{128} garantissant une résistance aux attaques par force brute [18].

4.4.4. Analyse des histogrammes

Nous avons calculé les histogrammes de Lenna originale, Lenna cryptée (module et phase) par la méthode de Lang en fonction de la suite chaotique sélectionnée. Les résultats sont illustrés dans les figures 4.16 ,4 .17, 4.18.D'après ces figures, on remarque que l'histogramme du module et l'histogramme de la phase de l'image complexe cryptée est totalement différents de l'image originale quel que soit les suit chaotiques. On peut dire que ces histogrammes sont uniformes et ne contiennent pas une information sur l'image originale ce qui montre que peu importe les méthodes utilisée, la méthode Lang maintient sa résistance contre les attaques statistiques.

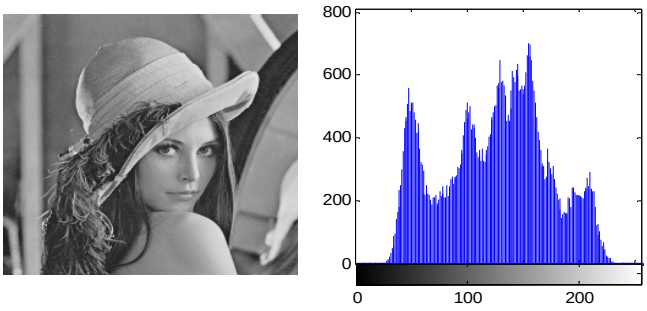
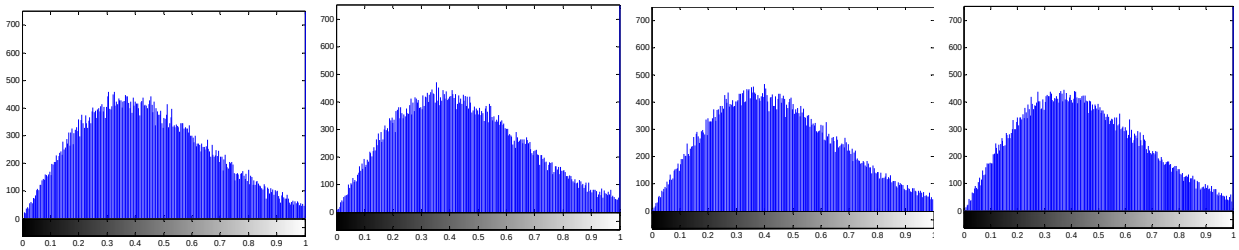
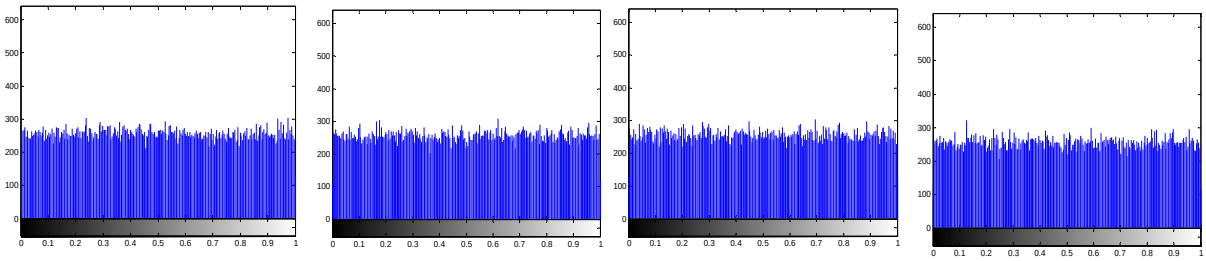


Figure 4.16. Histogramme de l'image Lenna



(a)Henon (b) Logistique (c) Tente (d) PWLCM

Figure 4.17. Histogrammes du module de l'image Lenna cryptée complexe



(a) Henon (b) Logistique (c) Tente (d) PWLCM

Figure 4.18. Histogrammes de la phase de l'image Lenna cryptée complexe

4.4.5. Qualité de cryptage

Afin d'évaluer la qualité de cryptage de façon objective, nous calculons le PSNR et le coefficient de corrélation entre l'image cryptée et sa version originale. Comme l'image cryptée est complexe, nous calculons le coefficient de corrélation C_r de la partie réelle ainsi que le coefficient de corrélation c_i de la partie imaginaire.

Les résultats sont présents dans les tableaux 4.6 et 4.7 en fonction de la transformée paramétrique utilisée et pour différentes images de tests standards.

Tableau4.6.PSNR en fonction de la suit chaotique utilisée

Chaos / Images	Henon	Suit logistique	PWLCM	Tent
Lenna	10.2633	10.2655	10.2446	10.4354
Mandarille	10.8375	10.8165	10.8243	10.9319
Baot	10.2091	10.2453	10.2273	10.4596
Cameraman	6.9053	6.8615	6.8885	7.5017

Tableau 4.7. Coefficient de corrélation en fonction de la suit chaotique utilisée

Chaos / Images	Henon		Suit logistique		PWLCM		Tent	
	c_r	c_i	c_r	c_i	c_r	c_i	c_r	c_i
Lenna	0.0044	-0.0052	-0.0068	-0.0057	0.0030	-0.0010	0.0029	0.0024
Mandrill	-0.0012	0.0039	0.0058	0.0041	0.0051	0.0020	0.0216	-0.0057
Baot	-0.0038	-0.0026	0.0014	-0.0016	0.0015	0.0046	0.0163	0.0039
Cameraman	-0.0074	-0.0015	0.0018	0.0022	-0.0014	-0.0024	0.0246	-0.0036

D'après le tableau 4.7, le coefficient de corrélation entre l'image cryptée et l'image originale dans tous les cas est très proche du zéro. Cela assure que la qualité de cryptage reste acceptable quel que soit la suit chaotiques utilisée avec TFFrD à paramètres multiples.

4.4.6 Résistance au bruit de canal

Pour tester la résistance de ces méthodes contre l'attaque du bruit nous avons ajouté un bruit blanc gaussien de coefficient de puissance σ ensuite nous avons tracé l'EQM en fonction de la transformée paramétrique utilisée dans la méthode Lang. Les résultats de simulation sont donnés dans la figure 4.19

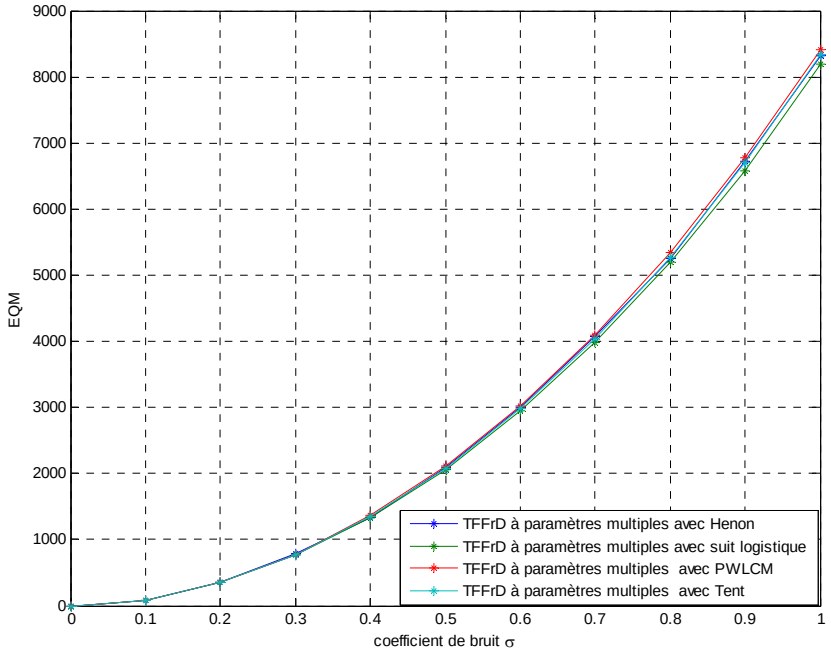
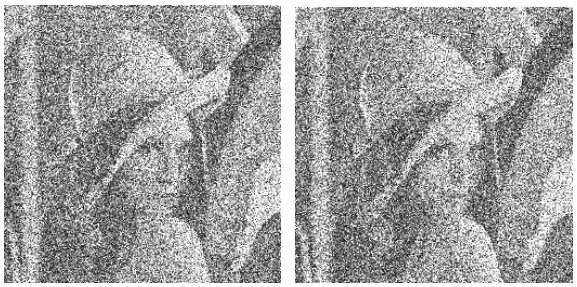
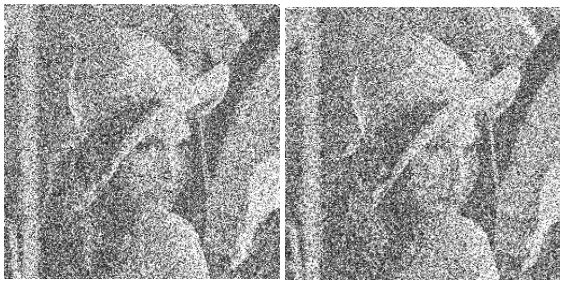


Figure 4.19. EQM en fonction du bruit additif et des transformées TFFrD à paramètres multiples avec les suit chaotiques.

La figure 4.19 montre où on remarque que lorsque le coefficient du bruit est égal à 0.9 nous constatons que l'image Lenna reste reconnaissable malgré un EQM différent. Par conséquent, ces résultats démontrent la résistance de la méthode de Lang contre le bruit additif quel que soit la suite chaotique utilisée.



a) Hénon, PSNR=**9.8501** ***b)*** suit logistique, PSNR=**9.8402**



c)PWLCM, PSNR=**9.8834** ***d)*** Tent, PSNR=**9.8305**

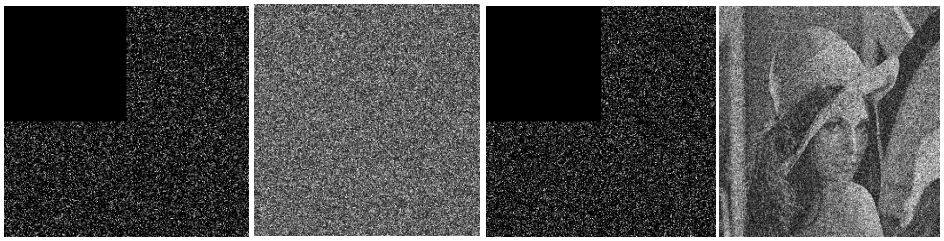
Figure 4.20.Résultats décryptage en fonction des suites chaotiques $\sigma = 0.9$

4.4.7 Résistance aux pertes d'informations

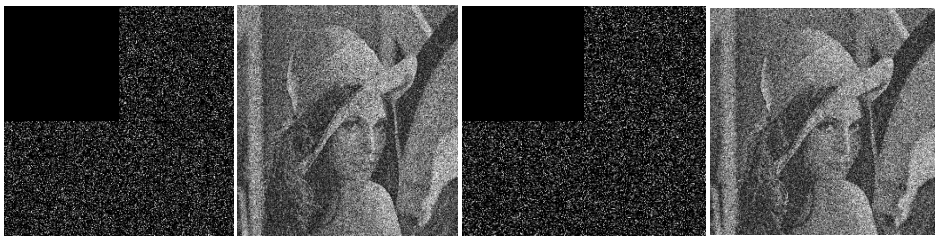
Pour tester la résistance de la méthode Lang contre les erreurs de transmission en fonction de la transformée TFFrD à paramètres multiples avec les différent suit chaotique utilisée, nous remplaçant volontairement une zone des pixels de l'image Lenna cryptée par une zone de pixels noire d'une surface déterminée.

Les résultats obtenus sont illustrés dans la figure 4.21 dans le cas d'une perte de 25% des pixels et la figure 4.22 dans le cas d'une perte de 50%.

D'aprés la Figure 4.21 et 4.22, nous remarquons que malgré un PSNR faible, l'image Lenna originale reste reconnaissable quelque soit la suit choas sauf dans le cas de la TFFrD à paramètres multiples avec suit logistique. En conséquence, ces résultats démontrent que la méthode Lang ne peut résister aux erreurs de transmission.

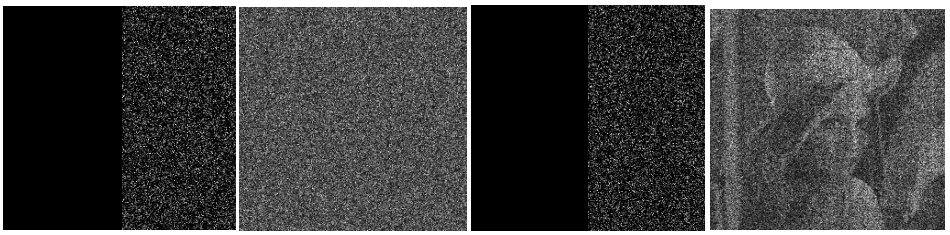


a)Logistique, PSNR=14.9923 b) Tente, PSNR=*13.9230*

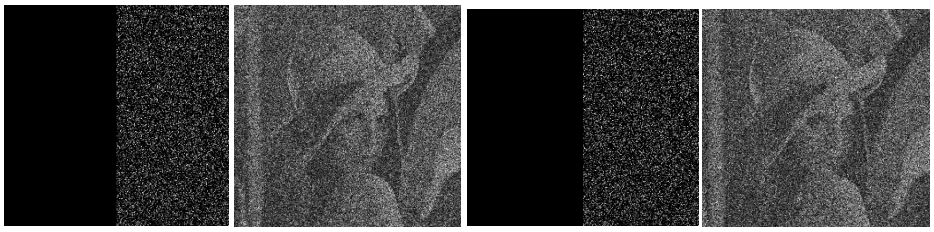


c)Henon,PSNR=13.9230 d) PWLCM, PSNR=*14.5197*

Figure 4.21. Image décryptée dans le cas d'une perte de 25%



a) Logistique, PSNR=11.9375 b) Tente , PSNR=*10.1023*



c)Henon, PSNR=10.8883 d) PWLCM, PSNR=*11.9811*

Figure 4.22. Image décryptée dans le cas d'une perte de 50%

4.5. Conclusion

D'après les études et les résultats de test obtenus nous concluons que la TFFrD à paramètres multiples dans la méthode de Lang est la transformée la plus efficace et la plus robuste par rapport aux autres transformées paramétriques étudiées.

D'autre part, nous avons fait la comparaison entre l'utilisation de différentes suites chaotiques que la suite logistique, les résultats de l'étude comparative ont montré que la suite chaotique PWLCM est plus robuste que les autres suites chaotiques étudiées et particulièrement dans le cas des attaques par force brute grâce à ces deux paramètres qui sont la condition initial x_0 et le paramètre de controlλ.

A la fin Nous pouvons dire que la TFFrD à paramètres multiples avec PWLCM est la meilleure façon d'optimiser la méthode de Lang.

.

Conclusion générale

Conclusion générale

Les techniques de cryptage d'images basées sur les transformées paramétriques et le chaos ont fait l'objet de ce travail.

Dans un premier temps nous avons revus le concept de base d'un système cryptographique ainsi que ses principaux objectifs qui sont la confidentialité, l'intégrité, l'authenticité et la non-répudiation.

Ensuite, nous avons vu le concept de base de la fameuse méthode DRPE qui est une méthode symétrique pour le cryptage d'images qui peut être implémenté optiquement ou numériquement. Cette méthode est basée sur l'utilisation de masques de phases aléatoires et des transformées paramétriques discrètes telles que la transformée ROP, la transformée ROP récursive, la transformée TFFrD et la transformée TFFrD à paramètres multiples où leurs paramètres aléatoires indépendants ont été utilisés comme une clé secrète.

Nous avons vu ensuite que la méthode de Lang a permis l'amélioration de la sécurité de la méthode DRPE par l'introduction de fonctions de permutations basées sur des suites chaotiques en remplacement du masque de phase aléatoire présent dans le domaine de la transformée paramétrique TFFrD à paramètres multiples, cependant, la méthode de Lang se limité seulement à l'utilisation de la suite logistique avec la TFFrD à paramètres multiples sans en prendre en considération la présence d'autres transformées paramétriques ou de suites chaotiques plus ou moins performantes.

De ce fait, dans le dernier chapitre, nous avons mené une étude comparative en modifiant dans un premier temps la méthode de Lang en fonction de la transformée paramétrique utilisée qui peut être la transformée ROP, sa version récursive, la transformée TFFrD ou sa version à paramètres multiples. Les résultats des tests comparaison ont montré clairement que la transformée TFFrD à paramètres multiples est plus efficace que les méthodes existantes en termes de sensibilité ce qui justifie le choix de Lang dans ce cas.

Ensuite, nous avons mené une autre étude comparative en modifiant la méthode de Lang en fonction de la suite chaotique utilisée dans la fonction de permutation de Lang. Cette suite chaotique peut être la suite logistique, la suite de Henon, la suite Tente ou la suite PWLCM. Les résultats des tests de comparaison ont montré que la suite PWLCM est plus robuste que les autres suites chaotiques sélectionnée set possède un espace clé meilleur que celui de la suite Logistique utilisée dans la méthode originale de Lang ce qui nous a amené à la coclusion que la TFrFD à paramètres multiples avec PWLCM est la meilleure façon d'optimiser la méthode de Lang.

Bibliographie

[1]- Image encryption El-samie, Abd Fathi, E,H, Hossam Eladin Ibrahim, F Mai, Osama, S Saleh, A. Taylor & Francis Group. CRC Press.2014.

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

[3]-MeryemBouchema. UniversitéFerhat abas –Sétif 1 mémoire de magister [Exploitation destransformées paramétriques dans le cryptage des images fixes]**.**2012.

[4]-B.Javidi et P.Refregier . « OPTICS LETTERS ». 767. Avril 1995.

[5]- Jun Lang , Ran Tao, Yue Wang Department "Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function " ,2010.

[6]-B. Furht, E. Muharemagic, and D. Socek " Multimedia Encryption and Watermarking, Springer Science & Business Media", 2005.

[7]-J. Dumas, J. Roch, E. Tannier, and S. Varrette, " Théorie des codes - Compression, cryptage, correction," Dunod, France. 2007

[8]-C. E. Shannon, " Communication Theory of Secrecy Systems, Bell System Technical Journal, " vol. 28, no. 4, pp. 656–715 1949.

[9] -Shiguo Lian. Multimedia content "encryption-technique and application " CRC Press.2009.

[10] -B. Schneier "Cryptographie appliquée: algorithmes, protocoles et codes source en C, Vuibert Informatique " 2001

[11]-Bekouche .T thèse de doctorat Université Ferhat Abbas – Sétif « développement et implémentation des techniques de cryptage des donnés basées sur les transformées discrètes ».

[12]- G. Unnikrishnan Kehar Singh " Double random fractional Fourier-domain encoding encoding for optical security" Nov. 29, 1999; revised manuscript received Apr. 4, 2000; accepted for publication June 22, 2000.

[13]-Xiaolei Wang, HongchenZhai∗, Zhilei Li, Qi Ge" Double random-phase encryption based on discrete quaternion fourier-transforms" journaleOptik 2011

[14]-CagatayCandan "The Discrete Fractional Fourier Transform, Student Member, IEEE, M. AlperKutay, Member, IEEE, and Haldun M. Ozaktas"

[15]- Wen-Liang Hsue and Soo-Chang Pei " the Multiple-Parameter Discrete Fractional Fourier Transform and Its Application ".

[16]- Saad Bouguezel, M. Omair Ahmad, Fellow, IEEE, and M. N. S. Swamy, Fellow, IEEE "A New Class of Reciprocal–Orthogonal Parametric Transforms 2013.

[17]-Azoug Seif Eddine, Saad Bouguezel " A non-linear preprocessing for opto-digital image encryption using multiple-parameter discrete fractional Fourier transform Laboratoire" 2016

[18]- Soo-Chang Pei*, Min-Hung Yeh "Two dimensional discrete fractional Fourier transform"

[19]-Saad Bouguezel, M. Omair Ahmad “Image Encryption using the Reciprocal-Orthogonal “

[20]-Ferenc Szöllősi ‘’ Parametrizing complex Hadamard matrices’’European Journal of Combinatorics 29 (2008) 1219–1234-Jul. 2007.

[21]-Julio Alexander AGUILAR ANGULO-THESE doctorat " Conception d’un Générateur de Valeurs aléatoires en Technologie CMOS AMS 0.35µm" ,ECOLE DOCTORALE Equipe conception de circuit Juin 2015

[22]- Saad Bouguezel, M. Omair Ahmad “A New Involuntary Parametric Transform and its Application to Image Encryption”

[23]-krimmohamed .thése 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 a Oran .2018/2019 .

[24]- Kwok-Wo Wong ,Department of Computer Engineering and Information Technology, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong.2002 Elsevier Science B.V.

[25]- L. Kocarev and S. Lian, “Chaos-Based Cryptography - Theory, Algorithms and Applications”, Springer-Verlag Berlin Heidelberg, 2011

[26]-Crampin, M. and Heal, Benedict, On the Chaotic Behavior of the Tent Map, Teaching Mathematics Applications (1994) 13(2): 83-89.

[27]- Security analysis of a chaos-based image encryption algorithm” ShiguoLian ,JinshengSun, Zhiquan Wang” 22 January 2005 .

Cryptage d'images basé sur les transformées paramétriques et le chaos

Résumé :

La vulgarisation de l'utilisation des données multimédias et particulièrement des images numériques a créé un réel besoin de préservation de confidentialité. Cela a incité le développement de différentes approches de cryptage d'images telle que la méthode DRPE en cryptage d'image qui est basée sur l'utilisation de masques de phases aléatoires et de transformées paramétriques telle que la transformée de Fourier fractionnaire discrète où les paramètres de la transformée sont utilisés comme des clés secrètes. La méthode de Lang est une méthode DRPE qui permet d'améliorer la sécurité de cette dernière en remplaçant un des masques de phases par des suites chaotiques considérés comme générateurs de clés de cryptage. Dans ce travail, des simulations sous MATLAB ont été effectués pour l'implémentation de la méthode de Lang puis une étude comparative a été menée avec différentes transformées paramétriques et différentes suites chaotiques afin d'évaluer sa sécurité contre les attaques par force brute, les attaques par histogramme et les attaques de canal.

Mots clés : Cryptage image, DRPE, transformées paramétriques, suites chaotiques

Image Encryption Based on Parametric Transforms and Chaos

Abstract:

The popularization of the use of multimedia data and especially digital images has created a real need for confidentiality preservation. This has prompted the development of different image encryption approaches such as the DRPE method in image encryption which is based on the use of random phase masks and parametric transforms such as discrete fractional Fourier transform where the parameters of the transform are used as secret keys. The Lang method is a DRPE method that improves the security of the latter by replacing one of the phase masks with chaotic sequences considered as encryption key generators. In this work, simulations under MATLAB were carried out for the implementation of Lang's method, then a comparative study was conducted with different parametric transforms and different chaotic sequences to evaluate its security against brute force attacks, attacks by histogram and channel attacks.

Keywords: Image Encryption, DRPE, Parametric Transforms, Chaotic Suites

تشفير الصور بناء على التحولات المعلمية والفوضى

ملخص :

أدى تعميم استخدام الوسائط المتعددة والصور الرقمية إلى خلق حاجة حقيقية للحفاظ على السرية. تم تطوير هذه الطريقة و هي طريقة تعمل على تحسين أمان النظام. في هذا العمل ، تم إجراء Langفي سياق استخدام طرق التشفير المختلفة. ثم أجريت دراسة مقارنة مع مختلف التحولات البارامترية Lang لتنفيذ طريقة MATLAB عمليات محاكاة بموجب تسلسلات الفوضى المختلفة لتقييم قواتها ضد هجمات القوة الغاشمة ، والهجمات من قبل المدرج الإحصائي وهجمات القنوات

الكلمات المفتاحية: تشفير الصور ،DRPE ،التحويلات البارامترية ، أجنحة الفوضى