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 : Electronique

Mémoire

Présenté pour obtenir

LE DIPLOME DE MASTER

FILIERE : **Electronique**

Spécialité : Electronique des systèmes embarqués

Par

➢ **Talhaoui Adel**

Intitulé

Cryptage d'images dans le système DRPE utilisant un Pré-cryptage à base de Jigsaw

Soutenu le : 04/07/2023

Devant le Jury composé de :

Nom & Prénom	*Grade*	*Qualité*	*Etablissement*
M.DJELLAL Djamel	*MAA*	*Président*	*Univ-BBA*
M.DAACHI Mohamed El Hossine	*MCA*	*Encadreur*	*Univ-BBA*
M.LATOUI Abdelhakim	*MCA*	*Examinateur*	*Univ-BBA*

Année Universitaire 2022/2023

Remerciements

Avant tout on tient notre remerciement à notre dieu tout puissant de nous avoir donné la foi, la force et le courage.

Je remercie mon encadreur Daachi Houcine, de sa Disponibilité, sa générosité professionnelle et ses précieux conseils.

Je remercie les membres du jury qui m'ont honoré de leur présenceet d'avoir accepté de juger mon travail.

Merci à tous.

Dédicaces

Je dédie ce travail à mes très chers parents, pour leur soutien ettous les efforts Qu'on m'a donnée le long de mon parcours et jeleurs souhaite bonne santé et longue vie.

Je dédie ce travail aussi à mes frères et mes sœurs.

A toute ma famille, tous mes amis Et tous ceux que j'aime et qui m'aiment

A tous mes enseignants qui ont fait leurs possibles pour nous donner le maximum d'informations concernant notre étude

Merci infiniment.

Talhaoui Adel

Résumé

Le travail réalisé dans ce mémoire s'inscrit dans le cadre de cryptage d'images en utilisant un cryptage basée sur la technique double masques de phases aléatoires **DRPE** (**D**ouble **R**andom **P**hase **E**ncoding). Dans sa version basique, cette technique consiste en l'introduction de deux masques, l'un dans le domaine spatial quant à l'autre, il est introduit dans le domaine fréquentiel moyennant une simple instruction issue de Matlab. Dans notre travail, nous avons appliqué la technique DRPE améliorée. En effet, les phases aléatoires introduites dans les deux masques sont basées sur l'une des variantes de la fonction (suite) chaotique. De plus, un pré cryptage basé sur la transformation JIGSAW, qui consiste en la division de l'image sujet de cryptage en blocs qui seront réarrangés d'une façon aléatoire en lignes et en colonnes. Pour étudier les performances de la technique de cryptage proposée, des tests par simulation ont été réalisés dans l'environnement Matlab en utilisant les différents critères d'évaluation connus en cryptographie.

Les mots clés : DRPE, Jigsaw, Cryptographie, chaotique, image numérique

Abstract

The work we have done consists of image encryption which is based on Double Random Phase Encoding (DRPE). In its basic version, this technique consists of the introduction of two masks, one in the spatial domain, while the other is introduced in the frequency domain by means of a simple instruction from Matlab. In this work, we applied the improved DRPE technique. Indeed, the random phases introduced in the two masks are based on a chaotic (sequence) function. In addition, a pre-encryption based on the JIGSAW transformation which consists of dividing the image subject of encryption into blocks which will be randomly rearranged in rows and columns. To study the performance of the proposed encryption technique, simulation tests were carried out in the Matlab environment using the various evaluation criteria known in cryptography.

Keywords: DRPE, Jigsaw, Cryptography, chaotic, digital image

ملخص

يندرج العمل المنفذ في هذه الأطروحة في إطار تشفير الصورة باستخدام تشفير يعتمد على تقنية قناع الطور العشوائي المزدوجDRPE (تشفير الطور العشوائي المزدوج). في نسختها الأساسية ، تتكون هذه التقنية من إدخال قناعين ، أحدهما في المجال المكاني ، بينما يتم إدخال الآخر في مجال التردد عن طريق تعليمات بسيطة من .Matlab في عملنا ، قمنا بتطبيق تقنية DRPEالمحسنة. في الواقع ، تستند المراحل العشوائية التي تم إدخالها في القناعين على أحد متغيرات الوظيفة الفوضوية (الجناح). بالإضافة إلى ذلك ، تشفير مسبق يعتمد على تحويل JIGSAW ، والذي يتكون من تقسيم الصورة الخاضعة للتشفير إلى كتل سيتم إعادة ترتيبها عشوائيًا في صفوف وأعمدة. لدراسة أداء تقنية التشفير المقترحة ، أجريت اختبارات المحاكاة في بيئة Matlab باستخدام معايير التقييم المختلفة المعروفة في التشفير.

الكلمات المفتاحية: دربيو ، جيقساو، التشفير ، الفوضى ، الصورة الرقمية

Liste des abréviations

DRPE (Double Random Phase Encoding).

PNG (Portable Network Graphics)

BMP (Bitmap)

GIF (Graphics Interchange Format)

TIFF (Tagged Image File Format)

PSD (Photoshop Document)

ICO (Microsoft Icon)

RVB image couleur (Rouge-Vert-Bleu)

Ppp (points par pouce)

FRFT (La transformée fractionnaire de Fourier)

AES (Advanced Encryption Standard)

RSA (Rivest-Shamir-Adleman)

DES (Data Encryption Standard)

ECC (Elliptic Curve Cryptography)

PSNR (sigle de Peak Signal to Noise Ratio)

Table des matières

Liste des figures

Liste des tableaux

Introduction générale

Le développement de la technologie a contribué davantage à l'amélioration des dispositifs et moyens de communication (transmission et réception de données) ce qui a rendu facile notre vie quotidienne. En revanche, la sécurisation des données transmises est devenue une nécessité absolue, vu le développement d'outils logiciels et matériels permettant une interception de ces données. Parmi les techniques de sécurisation couramment utilisées dans la littérature, et pour ne citer que cela, nous trouvons le cryptage. Par ailleurs, plus la technique de cryptage est compliquée plus la qualité du cryptage est meilleure. Aussi, l'utilisation d'un pré-cryptage fait augmenter davantage les performances du cryptage.

Le travail à réaliser dans ce mémoire s'inscrit dans le cadre de cryptage d'images en utilisant un cryptage basée sur la technique double masques de phases aléatoires **DRPE** (**D**ouble **R**andom **P**hase **E**ncoding). Dans sa version basique, cette technique consiste en l'introduction de deux masques, l'un dans le domaine spatial quant à l'autre, il est introduit dans le domaine fréquentiel. Cette technique est présentée pour la première fois en 1995 [1] S'agissant de la technique DRPE améliorée que nous allons étudier dans ce mémoire, les phases aléatoires introduites dans les deux masques sont basées sur une fonction chaotique. De plus, un pré cryptage basé sur la transformation JIGSAW, qui consiste en la division de l'image en question en blocs puis d'en réaliser la permutation de ces blocs, sera également réalisé [2]. Pour étudier les performances de la technique de cryptage proposée, des tests par simulation seront réalisés dans l'environnement Matlab en utilisant les différents critères d'évaluation connus en cryptographie.

Par ailleurs, notre manuscrit est organisé autour de trois chapitres suivis d'une conclusion générale et des perspectives. Dans le premier chapitre, nous allons présenter des généralités sur l'image. Dans le deuxième chapitre, nous présenterons un état de l'art sur les différentes techniques de cryptage issues de la littérature tout en mettant l'accent sur la technique DRPE. Dans le troisième chapitre représentant le cœur de notre travail, nous présenterons la technique de cryptage utilisée avec également les résultats de simulation à réaliser dans l'environnement MATLAB. Nous terminerons notre manuscrit par une conclusion générale et quelques perspectives au présent travail.

CHAPITRE I

GENERALITES SUR L'IMAGE

I. Introduction sur l'image numérique :

Par définition, l'image numérique est une représentation visuelle d'une scène ou d'un objet sous forme d'une matrice formée d'un ensemble de pixels. Chaque pixel est un point élémentaire de l'image qui contient des informations sur la couleur et la luminosité de ce point. Les images numériques sont utilisées dans de nombreuses applications, telles que la photographie, le cinéma, la vidéo, les jeux vidéo, la réalité virtuelle, les graphismes informatiques, la reconnaissance d'images, etc. Les images numériques sont créées à l'aide d'appareils photo numériques, de scanners ou de logiciels de conception graphique.

Les images numériques sont souvent représentées par des nombres binaires (0 et 1). Chaque pixel est représenté par un certain nombre de bits qui déterminent le nombre de couleurs différentes qui peuvent être représentées dans l'image [18].

Dans ce chapitre, nous présentons les différents formats et types d'images numériques ainsi que leurs caractéristiques. Nous présentons également les différents traitements que subie une image tels que le filtrage, la segmentation etc…

I.1 Formats d'image courants (JPEG, PNG, BMP, GIF, TIFF et PSD) :

- JPEG (Joint Photographic Experts Group) : Le format JPEG est un format d'image compressé largement utilisé pour les photographies et les images sur le web. Il offre un bon équilibre entre qualité d'image et taille de fichier, ce qui en fait un choix populaire pour le partage en ligne.
- PNG (Portable Network Graphics) : Le format PNG est un format d'image sans perte qui prend en charge la transparence et une plus grande gamme de couleurs que le format JPEG. Il est souvent utilisé pour les images avec des éléments transparents, comme les logos et les icônes.
- BMP (Bitmap) : Le format BMP est un format d'image non compressé largement utilisé sur les systèmes Windows. Il stocke les données de l'image pixel par pixel, offrant une qualité d'image élevée, mais avec des fichiers de taille plus importante que les formats compressés tels que JPEG et PNG.

- GIF (Graphics Interchange Format) : Le format GIF est couramment utilisé pour les images animées et les courtes séquences vidéo. Il utilise une palette de couleurs limitée (256 couleurs au maximum) et une compression sans perte pour réduire la taille des fichiers. Le format GIF prend également en charge la transparence.
- TIFF (Tagged Image File Format) : Le format TIFF est souvent utilisé pour le stockage d'images de haute qualité et de grande taille, notamment pour l'impression professionnelle et l'édition graphique. Il prend en charge diverses options de compression, y compris la compression sans perte, ce qui permet de conserver une qualité d'image élevée.

- PSD (Photoshop Document) : Le format PSD est le format de fichier natif du logiciel Adobe Photoshop. Il prend en charge des fonctionnalités avancées telles que les calques, les masques et les ajustements non destructifs. Le format PSD est principalement utilisé pour la manipulation et l'édition d'images dans Photoshop [28].

Tableau I. 1:indique les formats d'image.

Abréviation	Format de fichier	Type MIME	Extension(s)	Prise en charge navigateur
BMP	Bitmap	image/bmp	.bmp	Chrome, Edge, Firefox, Internet Explorer, Opera, Safari
ICO	Microsoft Icon	image/x-icon	.ico, .cur	Chrome, Edge, Firefox, Internet Explorer, Opera, Safari
TIFF	Tagged Image File Format	image/tiff	.tif, .tiff	Aucune prise en charge native, addons nécessaires

I.2 Types d'image numérique :

Il y a deux types d'images numériques, matricielle est basé sur les pixels et vectorielles basé sur des formules mathématique:

La figure suivant présentée une image Numérique :

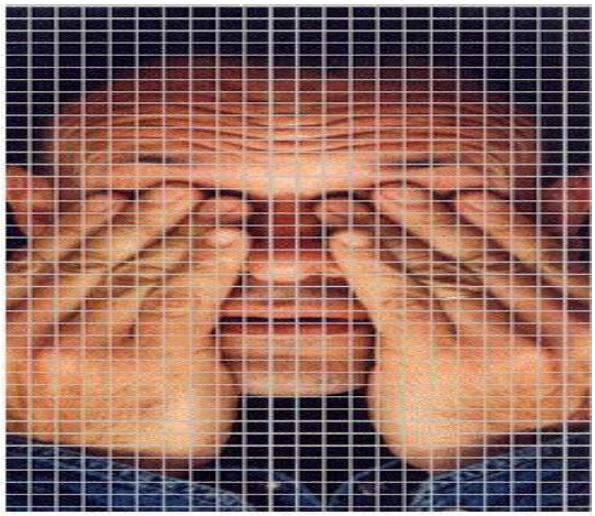


Figure I. 1: Image numérique

I.2.1 Les images matricielles :

Voici une formule générale pour représenter une image matricielle (bitmap) :

$$I(x, y) = C$$

Où :

- I est la matrice représentant l'image matricielle.
- (x, y) sont les coordonnées du pixel dans la matrice.
- C représente la couleur du pixel à ces coordonnées.

Dans cette formule, chaque pixel de l'image matricielle est représenté par une paire de coordonnées (x, y) qui indique sa position dans la matrice. Le pixel porte une information de couleur (C), qui peut être représentée de différentes manières selon le format d'image utilisé. Les formats courants pour les images matricielles sont BMP, PCX, GIF, JPEG, et TIFF.

Il est important de noter que cette formule est une représentation conceptuelle générale de l'image matricielle, et la manière spécifique de stocker les valeurs de couleur peut varier en fonction du format d'image utilisé [3].

I.2.2 Les images vectorielles :

La représentation des images vectorielles est basée sur des formules mathématiques décrivant les formes géométriques. Voici une formule générale pour représenter une forme géométrique dans une image vectorielle :

$F(x) = G$ Où :

- F est la fonction mathématique représentant la forme géométrique.
- x représente les paramètres de la forme géométrique, tels que les coordonnées, les dimensions, les angles, etc.
- G représente les instructions et les attributs graphiques associés à la forme géométrique, tels que la couleur de remplissage, la couleur de contour, l'épaisseur de trait, etc.

Dans cette formule, chaque forme géométrique dans une image vectorielle est représentée par une fonction mathématique (F) qui dépend des paramètres (x) spécifiques à cette forme. Les instructions graphiques (G) sont également associées à la forme pour définir ses propriétés visuelles [3].

Les images vectorielles offrent plusieurs avantages, notamment :

- Les fichiers vectoriels sont généralement de petite taille, car ils se basent sur des descriptions mathématiques des formes plutôt que sur des pixels individuels.
- Les redimensionnements des images vectorielles sont faciles et ne conduisent pas à une perte de qualité, car les formes géométriques peuvent être recalculées avec précision pour s'adapter à différentes tailles.
- Les images vectorielles sont adaptées aux formes géométriques simples et aux illustrations graphiques, offrant une précision et une netteté élevées pour ces types d'images.

Cependant, les images vectorielles présentent des limitations :

- Elles ne sont pas adaptées à la représentation de formes complexes ou de détails réalistes, tels que ceux présents dans les photographies.
- La représentation des images vectorielles est basée sur des formes géométriques simples, ce qui peut limiter la complexité des images pouvant être créées.

Il est important de noter que la formule donnée est une représentation conceptuelle générale des images vectorielles et qu'il existe de nombreux formats et techniques spécifiques pour représenter et manipuler ces images. Pour obtenir des détails plus précis sur la représentation des images vectorielles dans un format spécifique, il est recommandé de consulter des ressources spécialisées sur le sujet [3].

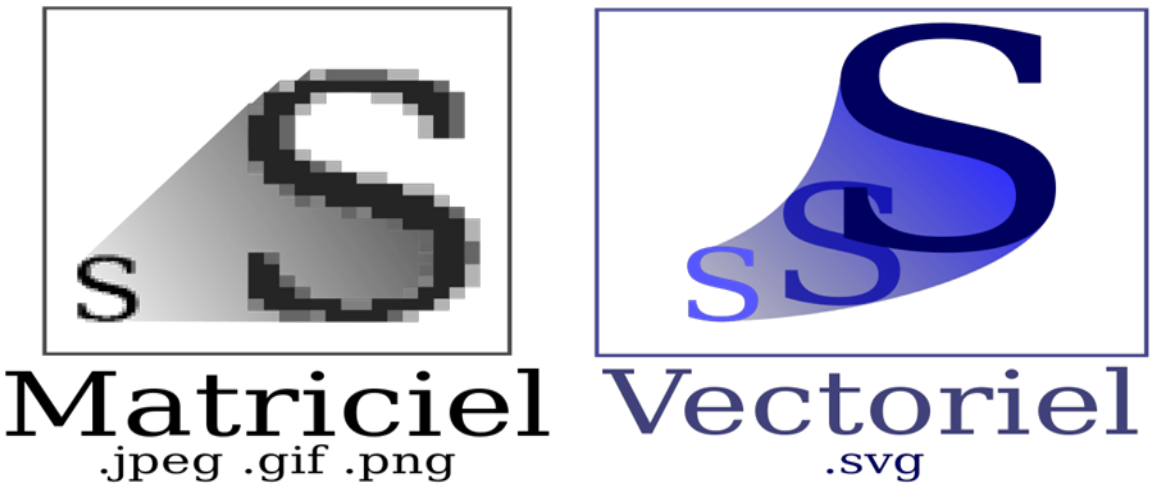


Figure I. 2: Image matricielle et image Vectoriel.

I.3 Prérequis :

I.3.1 Représentation d'une image numérique (matricielle) :

Nous avons vu qu'une image numérique est un tableau de points représentant les couleurs (pixels). Il existe plusieurs formats de codage de l'information de couleur des pixels :

I.3.1.1 Image noir et blanc :

Un seul bit suffit pour coder l'information, par exemple 0 pour la couleur noir et 1 pour la couleur blanc.

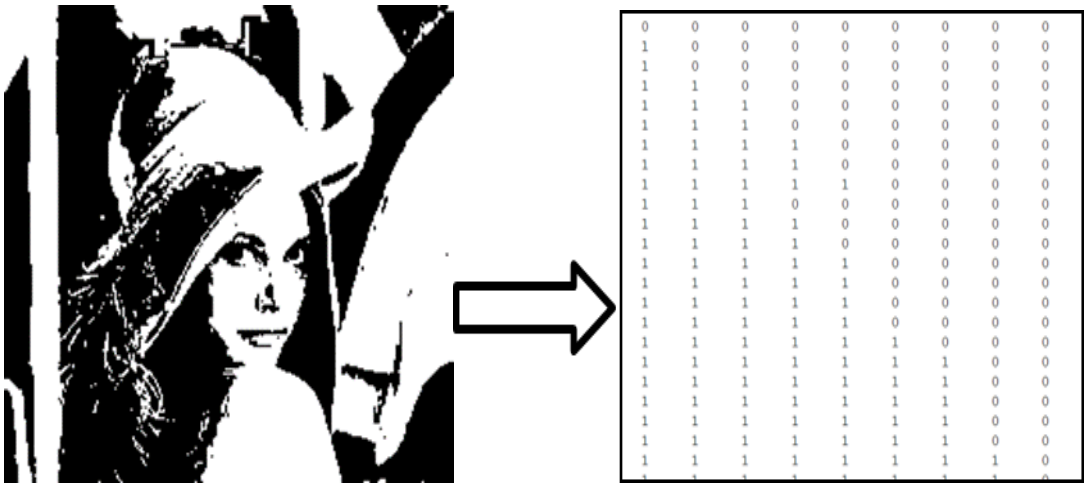


Figure I. 3:image noir et blanc.

I.3.1.2 Image niveau de gris :

On utilise en générale 8 bits, ce qui donne 256 nuances de gris possibles pour le pixel,de 0 pour le noir à 255 pour le blanc.

54	38	48	60	54	66	64	69	51	43	52	95
59	39	47	56	56	64	61	71	54	42	50	95
65	40	45	50	59	60	57	74	59	41	47	96
69	43	45	45	61	57	54	77	64	42	45	94
67	46	48	43	62	56	52	77	67	44	44	91
59	50	53	45	60	57	53	76	67	49	46	85
49	53	59	48	57	59	55	73	67	54	49	80
43	55	62	51	55	60	56	71	66	57	51	77
56	50	50	56	66	58	56	61	60	53	54	61
56	50	50	56	60	58	58	61	60	56	55	56
56	50	50	56	51	57	61	60	60	60	56	50
56	50	50	56	44	55	61	59	60	63	57	46
56	50	50	56	40	52	59	58	59	62	57	46
56	50	50	56	42	48	54	55	57	59	56	51
56	50	50	56	46	45	47	53	55	54	55	58
56	50	50	56	50	43	43	52	54	51	54	63
53	55	53	48	59	55	49	45	46	50	57	61
53	54	53	49	58	54	49	46	46	50	56	60
54	53	52	49	57	54	49	47	47	51	55	59

Figure I. 4: Image niveau de gris.

I.3.1.3 Image couleur (RVB) :

La description que vous avez donnée correspond au système de codage des couleurs RVB (ou RGB en anglais) utilisé dans de nombreux formats d'image numérique. Voici une formule générale pour représenter la couleur d'un pixel en utilisant les composantes RVB :

$$Couleur\_pixel = (R, V, B)$$

Où :

- R représente la composante rouge, avec une valeur comprise entre 0 et 255.
- V représente la composante verte, avec une valeur comprise entre 0 et 255.
- B représente la composante bleue, avec une valeur comprise entre 0 et 255.

Chaque composante de couleur (R, V, B) indique l'intensité de la couleur correspondante pour un pixel donné. L'intensité maximale (255) correspond à la couleur la plus vive, tandis que l'absence de couleur est représentée par une valeur de 0.

En utilisant la synthèse additive, la combinaison de différentes valeurs de R, V et B permet de créer une large gamme de couleurs. Par exemple :

- Si toutes les composantes RVB sont définies à 0, cela donne la couleur noire, car aucune intensité de couleur n'est présente.
- Si toutes les composantes RVB sont définies à la même valeur (par exemple,$R = V = B = 128$), cela donne une nuance de gris, où l'intensité de la couleur est égale pour chaque composante.
- Si toutes les composantes RVB sont définies à 255, cela donne la couleur blanche, car chaque composante atteint son intensité maximale.

Il est important de noter que cette formule est une représentation générale du système RVB et de la synthèse additive des couleurs. Les valeurs des composantes RVB peuvent varier en fonction du format d'image utilisé et des algorithmes de conversion de couleurs spécifiques [4].

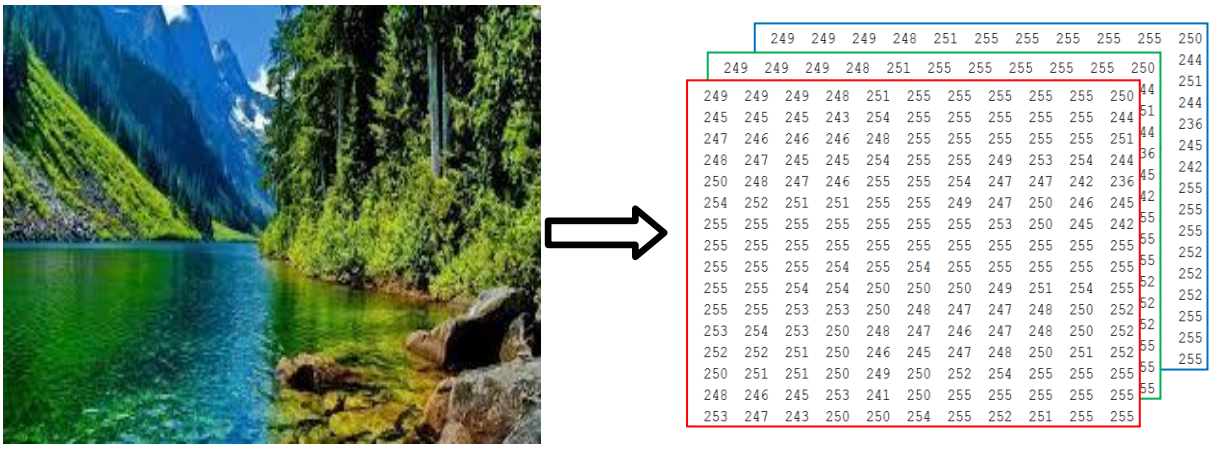


Figure I. 5: Représentation numérique d'une image en couleur.

I.4 Propriétés des images numériques :

I.4.1 Résolution :

La résolution d'une image numérique correspond à sa densité de pixels. Elle est mesurée en pixels par pouce (ppp) ou en pixels par centimètre (ppcm). Plus la résolution est élevée, plus l'image sera détaillée et nette. Les résolutions courantes pour les images numériques sont 72 ppp (pour les écrans), 300 ppp (pour l'impression professionnelle), 600 ppp (pour la photogravure) et 2400 ppp (pour l'impression haute résolution) [5].

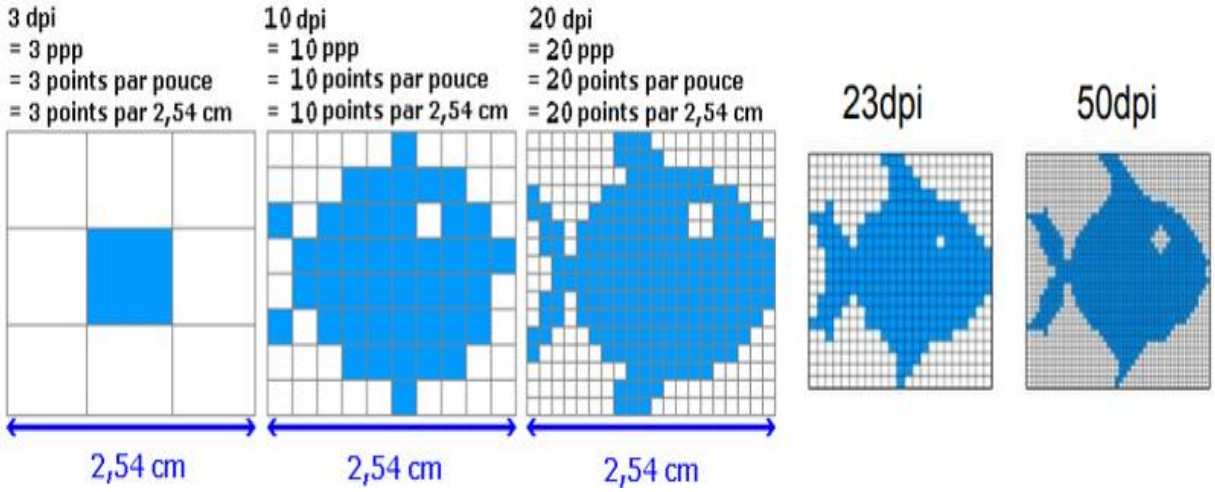


Figure I. 6: Schéma explicatif de résolution d'une image numérique.

I.4.2 Taille de fichier :

La taille de fichier d'une image numérique dépend de plusieurs facteurs, notamment la résolution, la profondeur de couleur et le format de fichier. Les images haute résolution avec une profondeur de couleur élevée (comme les images RAW) ont tendance à être plus volumineuses que les images à basse résolution avec une profondeur de couleur réduite (comme les images JPEG). Les formats de fichiers tels que le JPEG et le PNG peuvent compresser les images pour réduire leur taille de fichier [11].

Le tableau indique les tailles des images et son capacité de la mémoire :

Tableau I. 2: Tailles et poids de fichiers RAW.

Qualité d'image	Taille du fichier	Nombre d'image	Capacité de la mémoire tampon
NEF(RAW) compression sans perte, 12 bits	32.4 Mo	133	21
NEF(RAW) compression sans perte, 14 bits	41.3 Mo	103	17
NEF(RAW) compression, 12 bits	29.0 Mo	182	25
NEF(RAW) compression, 14 bits	35.9 Mo	151	20
NEF(RAW) pas de compression, 12 bits	57.0 Mo	133	18
NEF(RAW) pas de compression, 14 bits	74.4 Mo	103	16

I.4.3 Profondeur de couleur :

La profondeur de couleur d'une image numérique correspond au nombre de bits utilisés pour stocker les informations de couleur de chaque pixel. Les images en noir et blanc ont une profondeur de couleur de 1 bit, tandis que les images en couleurs peuvent avoir une profondeur de

couleur allant de 8 bits (256 couleurs) à 16 bits (65 536 couleurs) à 24 bits (plus de 16 millions de couleurs) [9].

Figure I. 7: profondeur de couleur d'une image numérique.

I.4.4 Format de fichier :

Le format de fichier d'une image numérique définit la manière dont les données de l'image sont stockées. Les formats de fichiers courants pour les images numériques comprennent JPEG, PNG, GIF, BMP et TIFF [10].

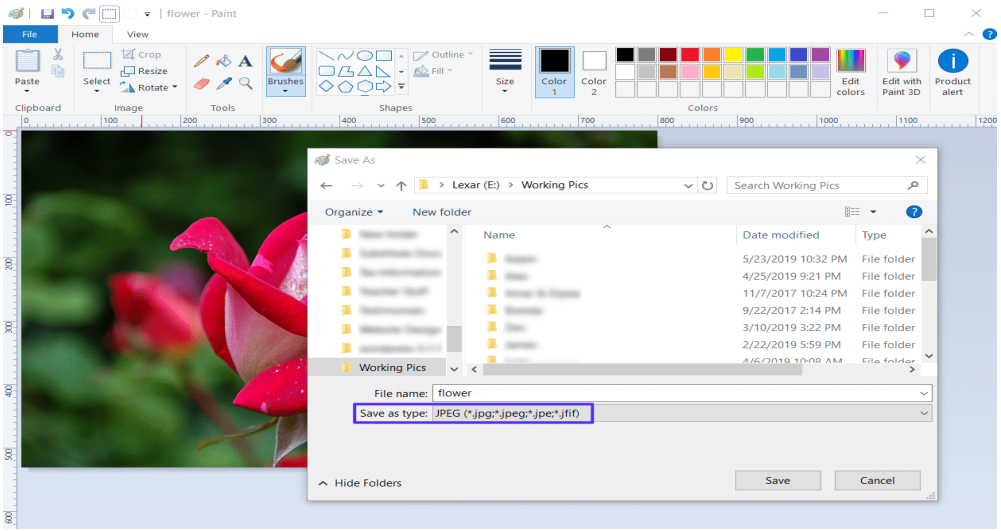


Figure I. 8: format de fichier d'une image numérique.

I.5 Présentation des traitements d'image :

Les techniques de traitement d'image sont utilisées pour améliorer la qualité d'une image, extraire des informations utiles ou segmenter l'image en différentes parties. Voici quelques techniques de traitement d'image courantes :

I.5.1 Filtrage d'image :

Le filtrage d'image est une technique utilisée pour supprimer le bruit de l'image et améliorer sa qualité. Les filtres peuvent être de différents types, tels que les filtres moyenneur, gaussien, passe-bas, passe-haut, médian, etc. [29].

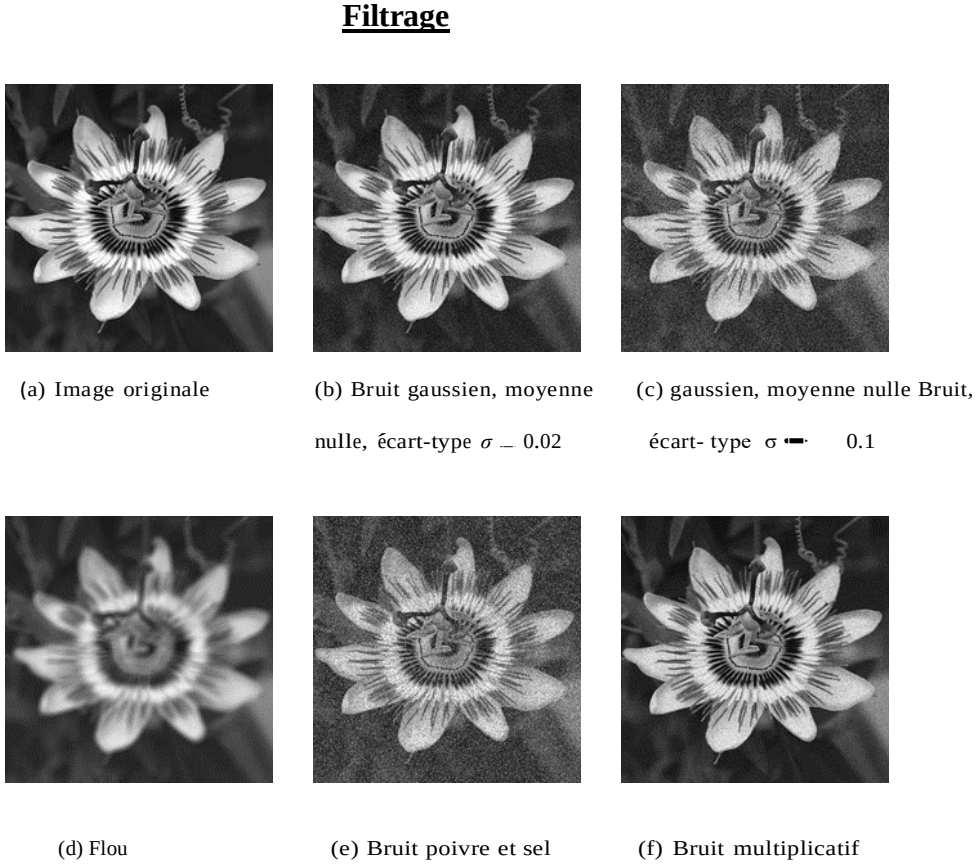


Figure I. 9: Exemples de perturbations d'une image (bruits et flou).

I.5.2 Segmentation d'image :

La segmentation d'image est une technique utilisée pour diviser une image en différentes régions ou objets. Les techniques de segmentation comprennent la segmentation basée sur les seuils, la segmentation basée sur la région, la segmentation par contour actif, etc. [22].

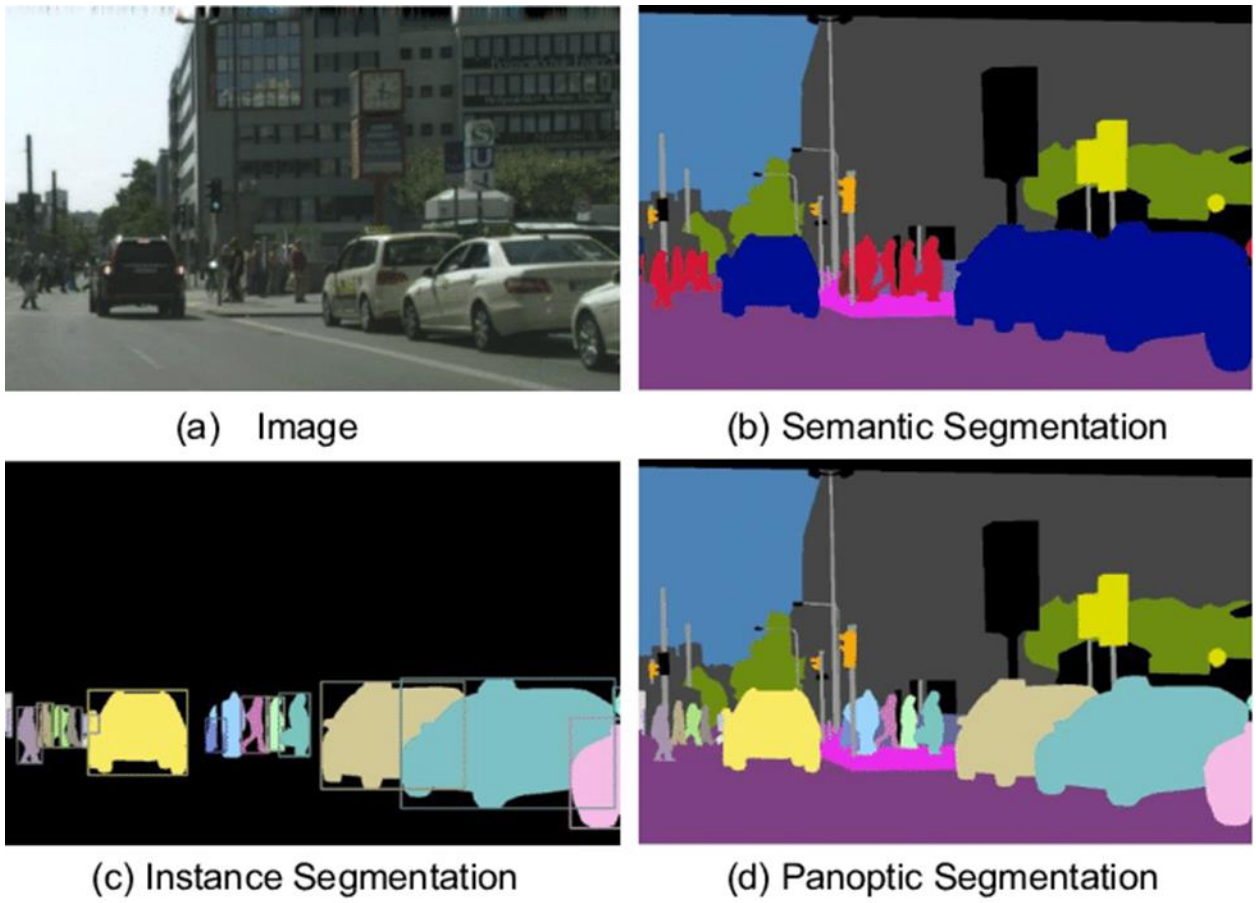


Figure I. 10: Combinaison des 2 types de segmentations.

I.5.3 Détection de contours :

La détection de contours est une technique utilisée pour détecter les bords d'une image. Les techniques de détection de contours comprennent la détection de contours de Sobel, la détection de contours de Canny, la détection de contours de Roberts. Les contours représentent les limites entre différentes régions de l'image qui présentent des caractéristiques visuelles distinctes. La détection de contours est une étape fondamentale dans de nombreuses applications de traitement

d'images, telles que la segmentation d'objets, la reconnaissance de formes, la détection d'objets etc. [23].

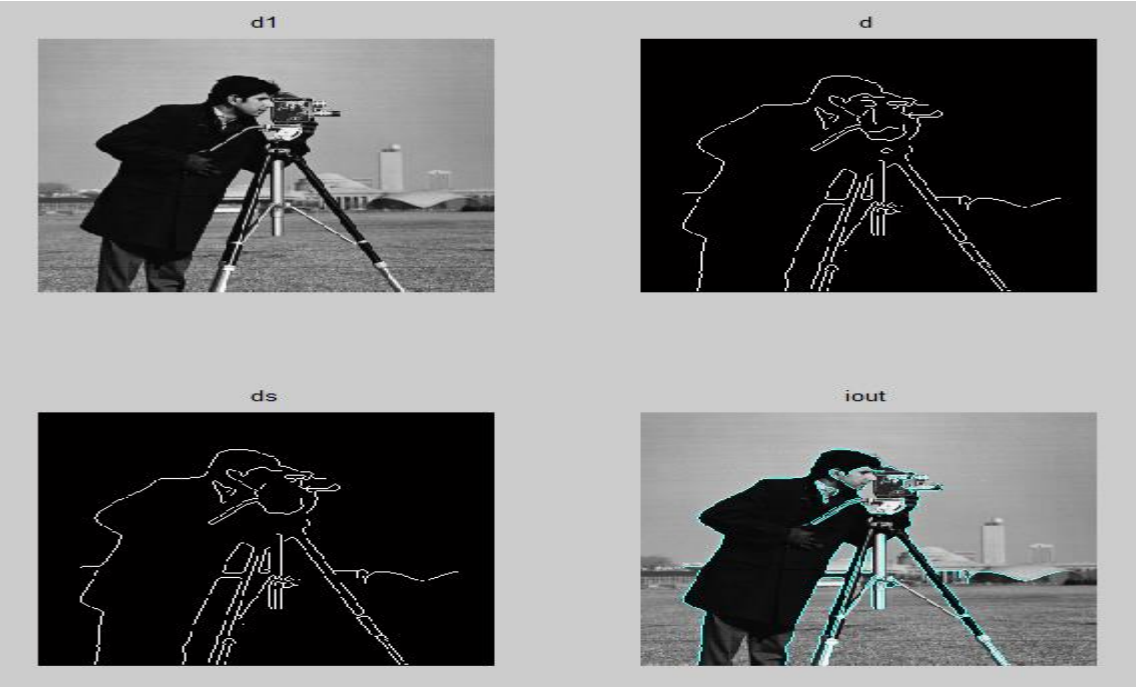


Figure I. 11: Exemple de détection de contours (Sobel).

I.5.4 Transformée de Fourier :

La transformée de Fourier est une technique utilisée pour convertir une image d'un espace de domaine spatial à un espace de domaine fréquentiel. Cela permet d'analyser la fréquence des différentes composantes de l'image [24].

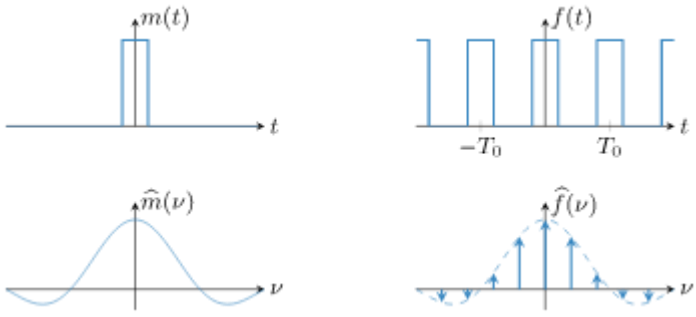


Figure I. 12: transformée de Fourier d'un signal périodique.

I.5.5 Reconnaissance de forme :

La reconnaissance de forme est une technique utilisée pour identifier des formes ou des objets dans une image. Les techniques de reconnaissance de forme comprennent la reconnaissance de forme basée sur la texture, la reconnaissance de forme basée sur la géométrie, etc. [25].

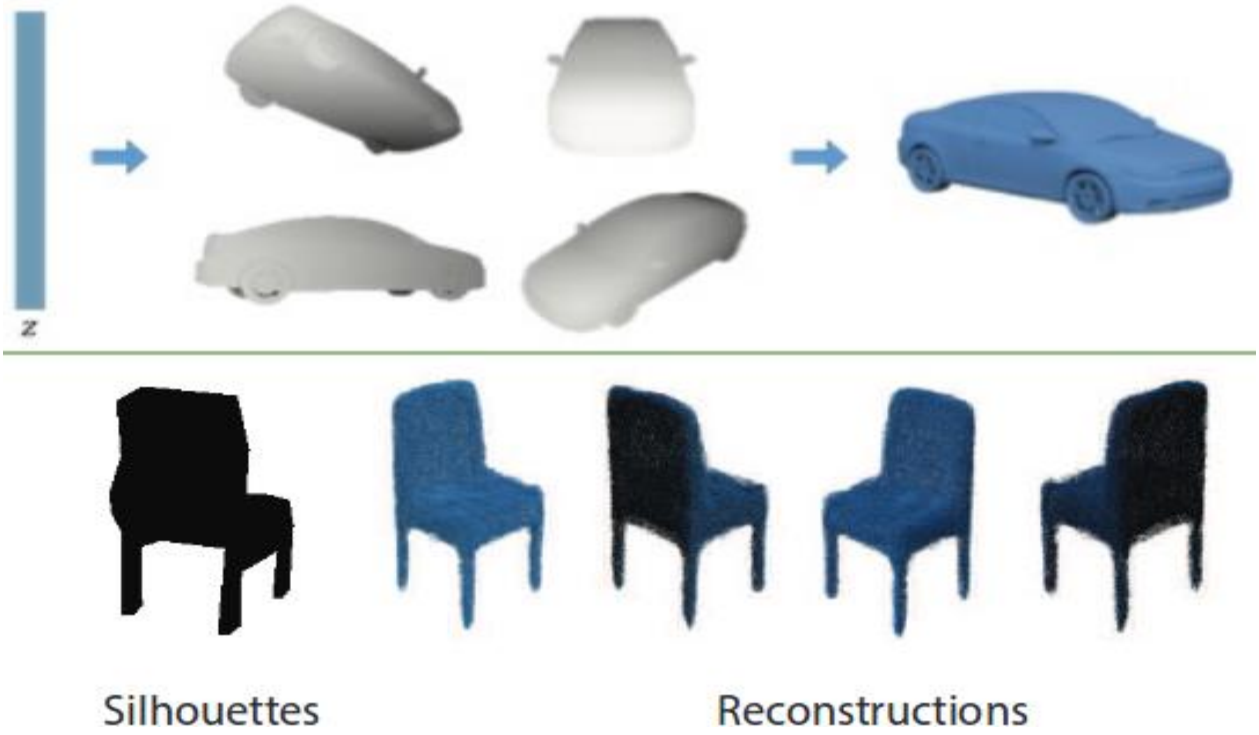


Figure I. 13: Reconnaissance de forme à partir de modélisation en 3D.

I.6 Conclusion :

Dans ce chapitre, nous avons présenté différents types d'images numériques ainsi que leurs propriétés. Aussi, nous avons présenté quelques techniques de traitement d'image issues de la littérature. L'étude que nous avons réalisée dans ce premier chapitre va servir comme une base pour l'étude du cryptage faisant l'objet du chapitre qui suit.

CHAPITRE II

CRYPTAGE D'IMAGE

II. Introduction :

La cryptographie utilise des algorithmes mathématiques pour transformer les messages originaux en une forme chiffrée. Le chiffrement peut être effectué de plusieurs manières, comme le chiffrement symétrique et le chiffrement asymétrique.

Le chiffrement symétrique utilise une même clé secrète pour chiffrer et déchiffrer le message. Le chiffrement asymétrique, en revanche, utilise deux clés distinctes - une clé publique et une clé privée - pour chiffrer et déchiffrer le message.

La cryptographie est essentielle pour assurer la confidentialité, l'authenticité et l'intégrité des informations et des communications sensibles. Ensuite, il y a plisseur exemple sur la cryptographie comme le cryptage d'image qui base sur les pixels de l'image, ce fiat des échanges mathématiques est utilisée plisseur méthodes pour avoir des bons résultats de cryptage.

Dans ce chapitre, nous nous intéressons plus particulièrement à la cryptographie qui consiste en une méthode pour sécuriser les informations et les communications en transformant les messages et les images en un format cryptée. Elle utilise des algorithmes mathématiques pour chiffrer les données (messages, images) et peut être utilisée de plusieurs manières, notamment avec le chiffrement symétrique, asymétrique, DRPE etc...

II.1.1 Définition de la cryptologie :

La cryptologie est l'étude des techniques de communication secrètes ou confidentielles utilisant des méthodes de chiffrement et de déchiffrement. Elle comprend deux sous-domaines: la cryptographie, qui traite de la création de messages chiffrés, et la cryptanalyse, qui se concentre sur la recherche de méthodes pour casser les codes et déchiffrer les messages cryptés [19].

II.1.2 Définition de la cryptographie :

La cryptographie est une technique de protection de l'information qui consiste à transformer un message clair en un message chiffré à l'aide d'un algorithme de chiffrement et d'une clé secrète.

Le message chiffré ne peut être déchiffré sans connaître la clé appropriée, ce qui garantit la confidentialité et l'intégrité des données. La cryptographie est utilisée dans de nombreux domaines, tels que la sécurité des communications électroniques, les transactions financières, la protection des données personnelles, la défense nationale, entre autres [19].

II.2 Les différents types de cryptage (symétrique, asymétrique) :

Il existe deux principaux types de cryptage : le cryptage symétrique et le cryptage asymétrique. Voici une brève description de chacun de ces types de cryptage.

II.2.1 Symétrique :

Cryptage symétrique : Le cryptage symétrique est une méthode de cryptage qui utilise une clé secrète unique pour chiffrer et déchiffrer les données. Cette clé est partagée entre les parties qui communiquent et doit être gardée secrète. Les algorithmes de cryptage symétrique les plus courants sont AES (Advanced Encryptions Standard) et DES (Data Encryptions Standard) [6].

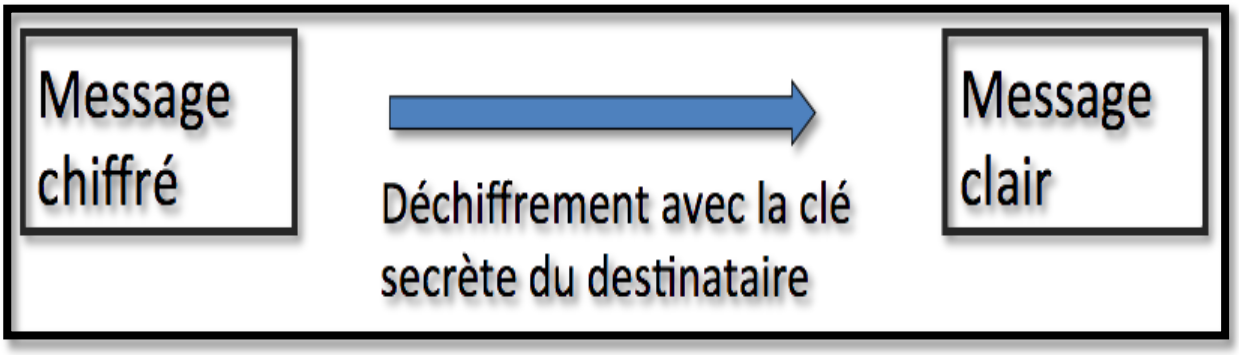


Figure II. 1: Principe de cryptage symétrique.

II.2.2 Asymétrique :

Cryptage asymétrique : Le cryptage asymétrique, également appelé cryptage à clé publique, utilise deux clés différentes pour chiffrer et déchiffrer les données. Une clé est publique et peut être partagée avec n'importe qui, tandis que l'autre clé est privée et doit être gardée secrète. Les

algorithmes de cryptage asymétrique les plus courants sont RSA (Rivest-Shamir-Adleman) et ECC (Elliptic Curve Cryptography)[7].

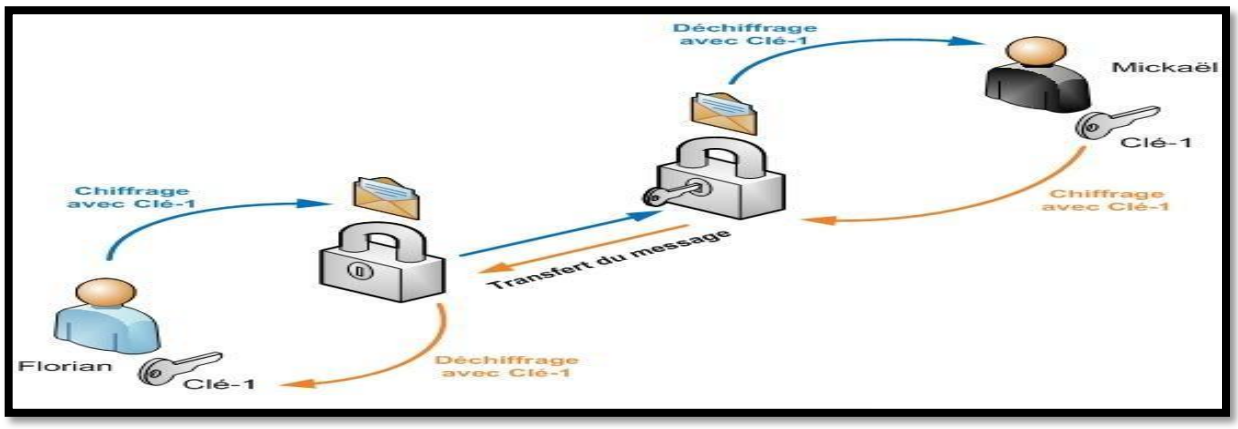


Figure II. 1: Principe de cryptage asymétrique.

II.2.3 Les avantages et les inconvénients :

Il est important de noter que les deux types de cryptage ont leurs avantages et leurs inconvénients. Le cryptage symétrique est généralement plus rapide et plus efficace pour chiffrer de grandes quantités de données, tandis que le cryptage asymétrique est plus sûr et plus pratique pour échanger des clés de manière sécurisée.

En résumé, le cryptage symétrique utilise une clé secrète unique pour chiffrer et déchiffrer les données, tandis que le cryptage asymétrique utilise deux clés différentes, l'une publique et l'autre privée. Les deux types de cryptage ont leurs avantages et leurs inconvénients et sont utilisés pour protéger les données sensibles dans diverses applications [7-8].

II.3 La cryptographie visuelle:

Figure II. 2: Les images originales.

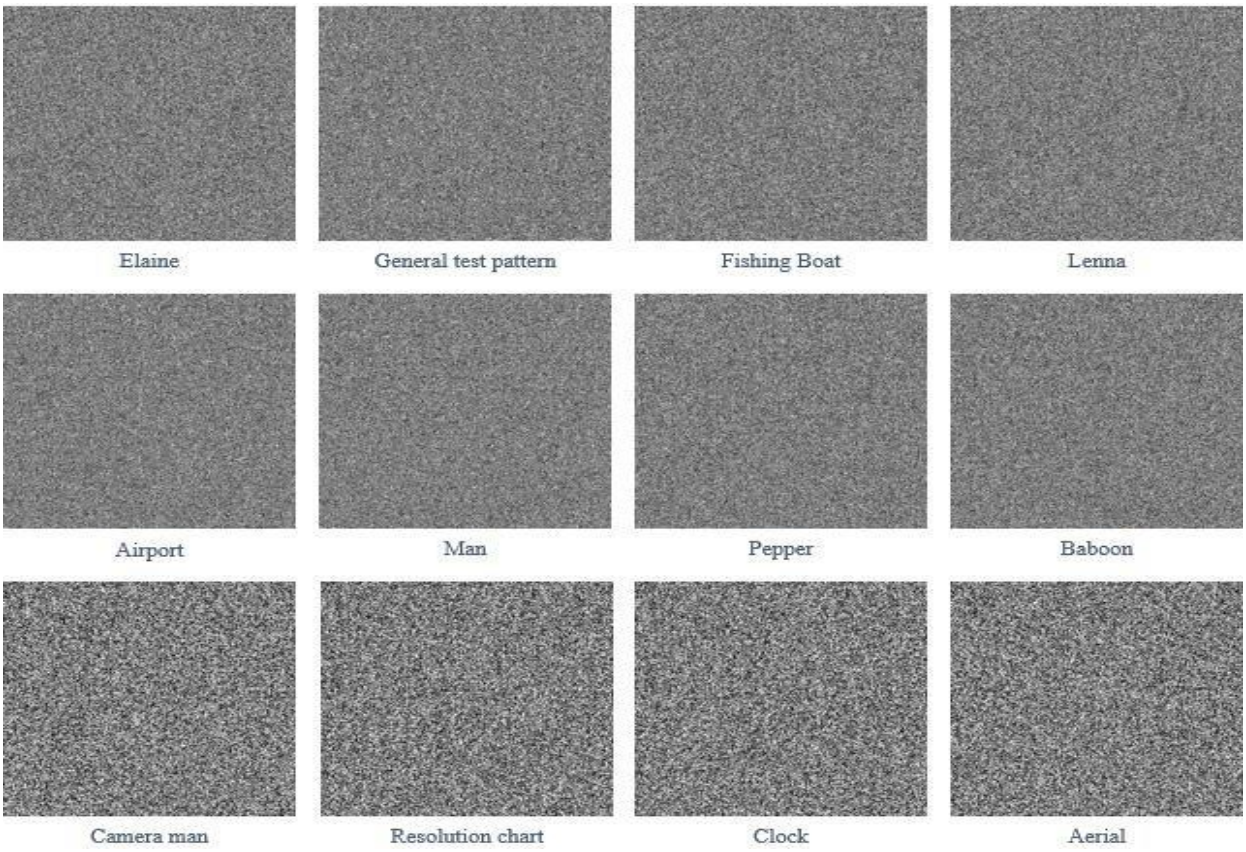


Figure II. 3: Les images cryptées.

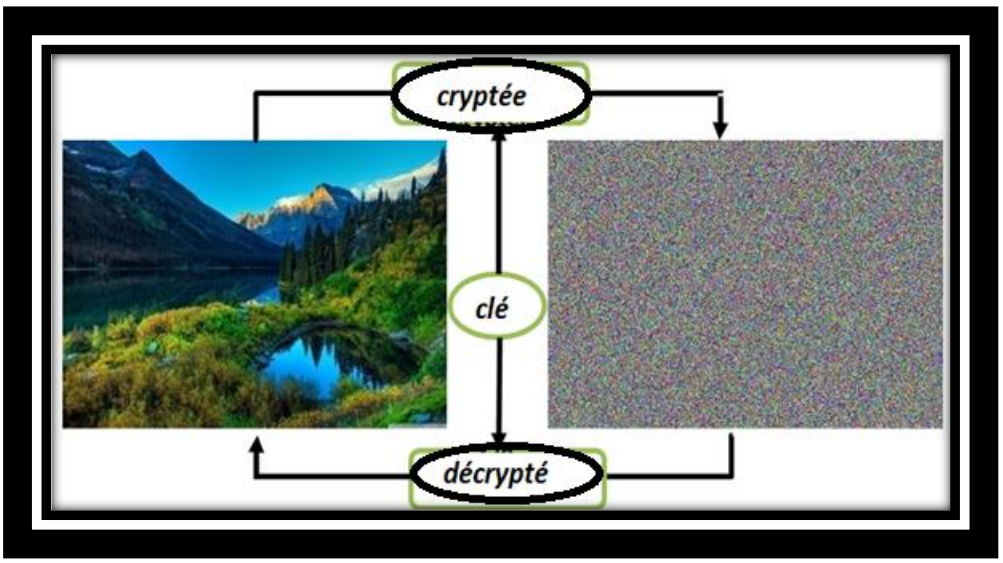


Figure II. 4: Cryptage d'image.

II.4 Le système DRPE :

II.4.1 Double codage de phase aléatoire (DRPE) :

La technique du Double Codage de Phase Aléatoire (DRPE) consiste à modifier la distribution spectrale d'une image. Le système optique DRPE se compose de trois plans : le plan d'entrée, le plan de transformée de Fourier (FT) et le plan de sortie. Entre ces plans, il y a deux objectifs séparés par quatre longueurs focales, comme illustré dans la Figure II.6. L'algorithme DRPE repose sur l'application de deux masques de phase aléatoires (RPM) ($d1$ et $d2$) pour chiffrer l'image d'entrée. L'un de ces masques est appliqué au plan d'entrée, tandis que l'autre est appliqué au plan FT. Pour une image d'entrée $\{F(x,y)\}$ avec des dimensions L et M, les deux masques aléatoires peuvent être représentés par $D1 = \{d1(x,y)\}$ et $D2 = \{d2(\mu,\nu)\}$, où $d1 = e^{j2\pi a(x,y)}$ et $d2 = e^{j2\pi b(\mu,\nu)}$. Les coordonnées (x,y) et (μ,ν) représentent respectivement le plan d'image d'entrée et les coordonnées du second plan de masque. Les valeurs $a(x,y)$ et $b(\mu,\nu)$ sont dispersées aléatoirement dans l'intervalle$[0,1]$, et j représente la partie imaginaire. Enfin, l'image cryptée au niveau du plan de sortie peut être notée$Fen = \{Fen(x,y)\}$, où$Fen(x,y) = IFT(FT(F(x,y).e^{j2\pi a(x,y)}).e^{j2\pi b(\mu,\nu)})$. Le DRPE est facile à configurer et peut être appliqué à l'aide d'un système optique ou d'un logiciel. Il peut être efficacement utilisé pour crypter des images de visages. Les Figures II.6 et II.7 illustrent le système optique DRPE [17].

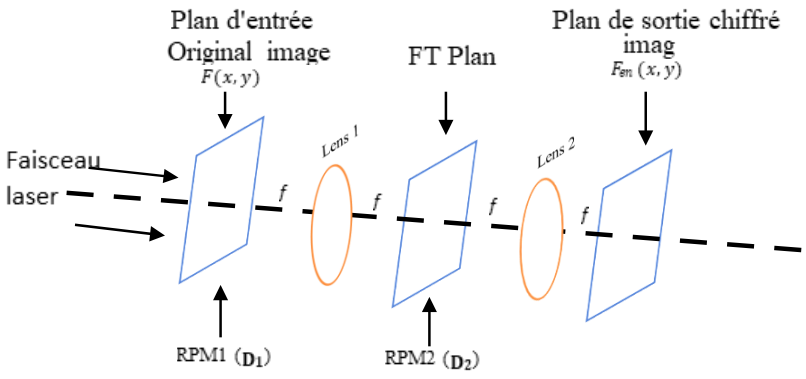


Figure II. 5: Implémentation optique du système DRPE.

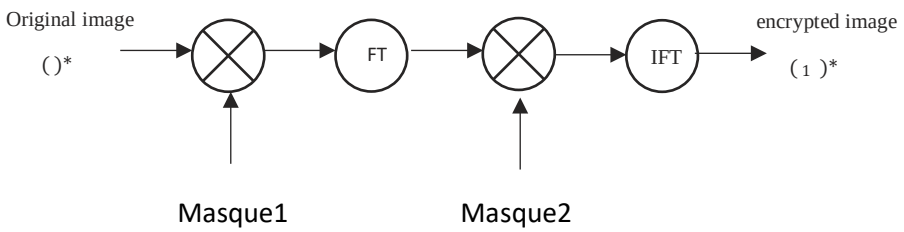


Figure II. 6: Implémentation mathématique du système DRPE.

II.5 Concepts de base :

II.5.1 Chaotique Baker map (logistique Baker map) :

La méthode de chiffrement d'image appelée Chaotique Baker map est largement réputée et couramment utilisée. Son objectif principal est de rendre les pixels adjacents moins corrélés en modifiant aléatoirement leur position. Pour cela, la Baker map opère sur une matrice carrée et utilise une clé secrète, notée k, pour diviser la matrice en rectangles empilés. On représente cette version discrétisée de la Baker map par$I(n1, n2, \ldots, nk)$, où k entiers sont disposés dans une séquence : $n1, n2, \ldots, nk$. Chaque entier ni est choisi de manière à diviser le nombre m, et $mi = n1 + n2 + \ldots + ni$.

Pour chaque paire d'indices (r, g), telle que $mi \leq r < mi + ni \, et \, 0 \leq g \leq m$, l'élément correspondant dans la matrice initiale est déplacé vers une nouvelle position selon la formule suivante [21] :

$$I(n1, \ldots, nk)(r, g) =$$

$$[(r - mi) + g \, mod \, (m/ni), (g - g \, mod \, (m/ni)) + mi]$$

La matrice carrée $Im \times m$ est divisée en k rectangles verticaux, chacun ayant une hauteur de m et une largeur de ni. À l'intérieur de chaque rectangle, on trouve ni cases, et chacune de ces cases contient m points. Ces cases sont ensuite réarrangées en lignes en la transférante colonne par colonne [21]. La figure 2.9 présente un exemple d'une permutation de matrice 8 × 8 avec la clé k définie comme étant (2, 4, 2). Ainsi, dans cet exemple, nous avons $m = 8, n1 = 2, n2 = 4 \, et \, n3 = 2$.

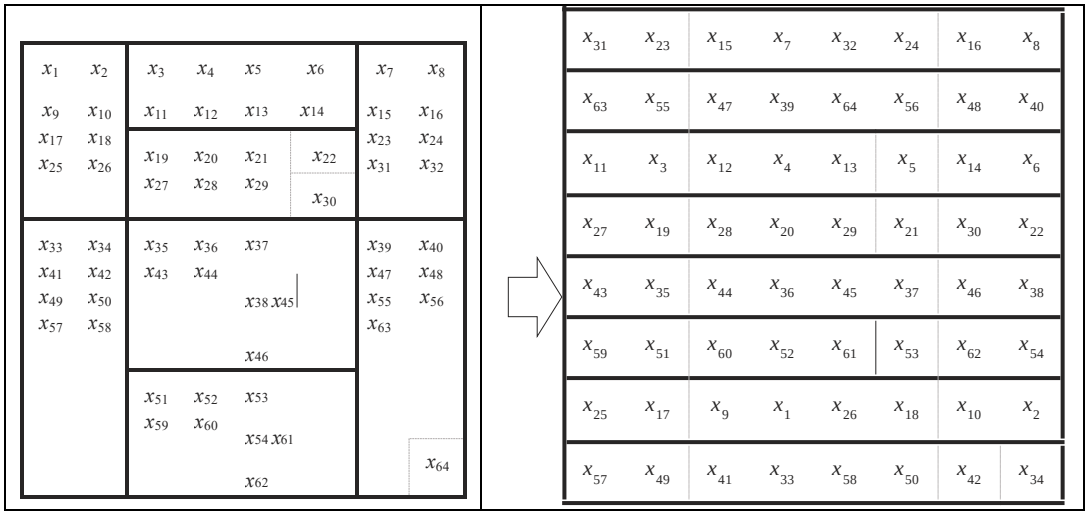


Figure II. 7: Cryptage de carte chaotique Baker discrétisé pour une image 8 × 8 pixels.

II.5.2 Chiffrement et déchiffrement :

La transformée fractionnaire de Fourier (FRFT) est une généralisation de la transformée de Fourier classique. Dans cette explication, nous utiliserons une notation unidimensionnelle pour simplifier les symboles. Soit x_0 et a_x les coordonnées respectives dans le domaine spatial d'entrée et le domaine fractionnaire de sortie. La FRFT d'une fonction $f(x)$ d'ordre a peut être définie [27] de la manière suivante :

La méthode de chiffrement que nous proposons peut être illustrée par la Figure 1. Considérons $f(x)$ et $g(x)$ comme les deux images principales avec une amplitude normalisée à crypter ensemble. J désigne l'opération de brouillage de pixels [26], qui consiste à intervertir les pixels selon une permutation spécifique. L'image perturbée peut ensuite être récupérée en appliquant une commande spéciale pour repositionner les pixels. Pour le chiffrement, le brouillage des pixels est appliqué à l'une des images principales$g(x)$, puis le résultat brouillé J [g(x)] est encodé dans une fonction [3, 6, 7], qui peut être mathématiquement exprimée comme $e^{[iJ(g(x))\pi]}$ dans la plage de variation de phase $[0, \pi]$. Cette fonction résultante est ensuite multipliée par l'autre image principale $f(x)$ pour obtenir le signal complexe combiné $C(x)$ [26].

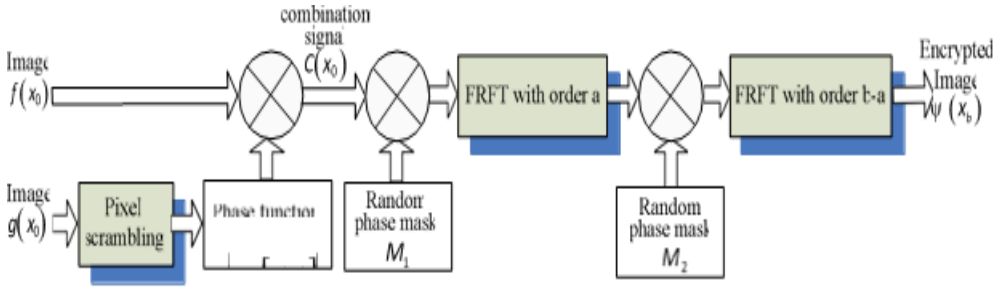


Figure II. 8: Schématique de cryptage.

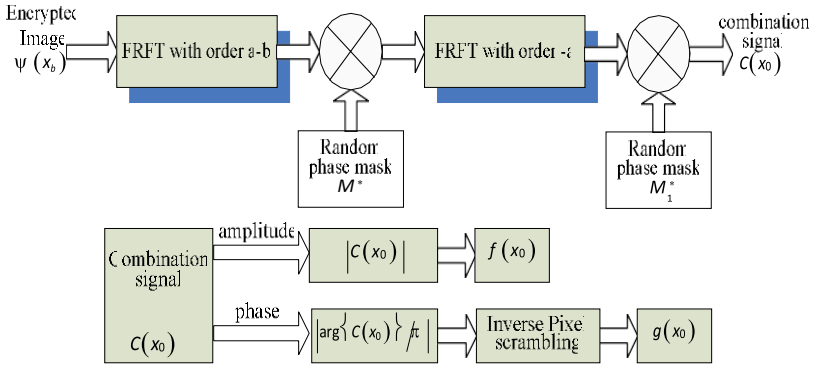


Figure II. 9: Schématique de décryptage.

II.6 Les algorithmes de cryptage courants (AES, RSA, etc.) :

Il existe de nombreux algorithmes de cryptage courants utilisés dans les applications de sécurité informatique. Voici une liste de quelques-uns des algorithmes les plus utilisés, avec une référence bibliographique pour approfondir chaque sujet :

II.6.1 AES (Advanced Encryption Standard) :

AES est un algorithme de cryptage symétrique qui utilise des blocs de 128 bits pour chiffrer les données. Il a été adopté par le gouvernement américain comme standard de cryptage et est utilisé dans de nombreux protocoles de sécurité, tels que SSL/TLS [12].

II.6.2 RSA (Rivest-Shamir-Adleman) :

RSA est un algorithme de cryptage asymétrique qui utilise une paire de clés pour chiffrer et déchiffrer les données. Il est largement utilisé pour la sécurisation des communications en ligne, des transactions financières et des certificats numériques [13].

II.6.3 DES (Data Encryption Standard) :

DES est un algorithme de cryptage symétrique qui utilise une clé de 56 bits pour chiffrer et déchiffrer les données. Il est considéré comme moins sûr que AES en raison de la longueur de la clé relativement courte [14].

II.6.4 ECC (Elliptic Curve Cryptography) :

ECC est un algorithme de cryptage asymétrique qui utilise des courbes elliptiques pour générer des paires de clés pour chiffrer et déchiffrer les données. Il est considéré comme plus sûr et plus efficace que RSA pour des clés de même longueur [15].

En résumé, AES, RSA, DES et ECC sont des algorithmes de cryptage courants utilisés dans les applications de sécurité informatique. Chacun de ces algorithmes a des avantages et des inconvénients et peut être utilisé dans différents scénarios pour protéger les données sensibles.

II.7 Techniques de cryptage pour les images :

Les techniques de cryptage pour les images peuvent être classées en deux catégories principales : les modèles de confusion et les modèles de diffusion. Les modèles de confusion cherchent à cacher les relations entre les pixels de l'image, tandis que les modèles de diffusion cherchent à étaler les données d'une image dans l'ensemble de l'image.

II.7.1 Modèle de confusion :

Les modèles de confusion cherchent à rendre les relations entre les pixels de l'image difficiles à comprendre. Les techniques de cryptage basées sur le modèle de confusion comprennent le chiffrement de flux, le chiffrement par permutation, le chiffrement par substitution, etc.

II.7.2 Modèle de diffusion :

Les modèles de diffusion cherchent à étaler les données d'une image dans l'ensemble de l'image, de sorte qu'un petit changement dans une partie de l'image se propage à travers toute l'image. Les techniques de cryptage basées sur le modèle de diffusion comprennent la transformation de Fourier discrète, la transformée de Walsh-Hadamard, la transformée en ondelettes, etc [30].

Il est important de noter que les techniques de cryptage pour les images doivent être choisies en fonction des besoins de sécurité de l'application, car chaque technique a des avantages et des inconvénients. En général, les techniques de cryptage basées sur le modèle de confusion sont plus adaptées pour les images avec des zones uniformes de couleur, tandis que les techniques de cryptage basées sur le modèle de diffusion sont plus adaptées pour les images avec des motifs complexes.

II.8 Sécurité et performances des techniques de cryptage d'images :

La sécurité et les performances des techniques de cryptage d'images sont des considérations importantes pour les applications de sécurité des données :

Les techniques de cryptage d'images en termes de sécurité et de performances. Elle passe en revue les différentes techniques de cryptage d'images basées sur les modèles de confusion et de diffusion, en évaluant leurs performances en termes de temps de traitement et de taux de compression, ainsi que leur résistance aux attaques cryptographiques telles que l'attaque par force brute, l'attaque par dictionnaire, etc.

Propose également une discussion sur les normes de cryptage d'images telles que JPEG2000, qui combine des techniques de cryptage et de compression, et fournit une analyse des performances et de la sécurité des différentes techniques de cryptage utilisées dans cette norme. Enfin, les techniques de cryptage d'images en termes de sécurité et de performances, et peut être utile pour ceux qui cherchent à comprendre et à évaluer les différentes techniques de cryptage d'images disponibles**.**

II.9 Conclusion :

Dans ce chapitre, nous avons tout d'abord présenté des notions de base sur la cryptographie d'une manière générale. Ensuite, nous avons mis en relief les différentes techniques de cryptage relevant de la littérature. Aussi, nous avons mis l'accent sur la technique DRPE qui va être exploitée dans le prochain chapitre.

CHAPITRE III

CRYPTAGE D'IMAGES A BASE DE JIGSAW DANS LE SYSTEME DRPE

III. Introduction :

Dans ce chapitre, nous allons présenter et étudier les performances de la technique de cryptage utilisée. En effet, elle consiste en la technique de cryptage double masques de phases aléatoires DRPE améliorée, basée sur un pré cryptage réalisé par la transformation jigsaw. A la différence de la version basique de la DRPE, les phases dans les deux masques sont introduites moyennant une fonction chaotique.

La technique de cryptage étudiée est testée par simulation dans l'environnement Matlab pour différentes images. Quant aux performances de la technique étudiée, elles sont évaluées via des critères d'évaluation connus (PSNR et Corrélation). De même, un décryptage, opération inverse, est également réalisé.

III.1 Présentation de la technique de cryptage utilisée :

Par définition le cryptage d'image est un processus de sécurité qui transforme l'image en une forme codée, afin de protéger son contenu contre l'accès non autorisé ou la lecture. Le système DRPE (Double Random Phase Encoding) est une technique de cryptage d'image qui utilise deux masques aléatoires pour générer une image codée. La méthode Jigsaw quant à elle est une technique de prétraitement d'image qui divise l'image en plusieurs fragments et les mélange avant de les réarranger dans une nouvelle image. Autrement dit, dans le système DRPE basé sur la méthode Jigsaw, l'image à crypter est d'abord découpée en plusieurs morceaux comme des blocs. Chaque bloc est ensuite mélangé aléatoirement, puis réarrangé en une nouvelle configuration. D'ailleurs ce processus crée une image désorganisée qui est difficile à comprendre sans les informations de décryptage appropriées mais ce n'est pas encore suffisant. La technique DRPE est appliquée par la suite utilisant les deux masques contenant des phases générées de façon aléatoires. Le premier masque est introduit dans le domaine spatial quant à l'autre, il est introduit dans le domaine fréquentiel. Par conséquent, il y aura création d'une image cryptée qui ne peut être décrypté que si les deux masques sont connus et utilisés dans l'ordre approprié.

En ce qui concerne la génération des phases aléatoire pour les deux masques, nous avons employé des fonctions chaotiques.

III.1.1 Organigramme de la technique DRPE utilisée :

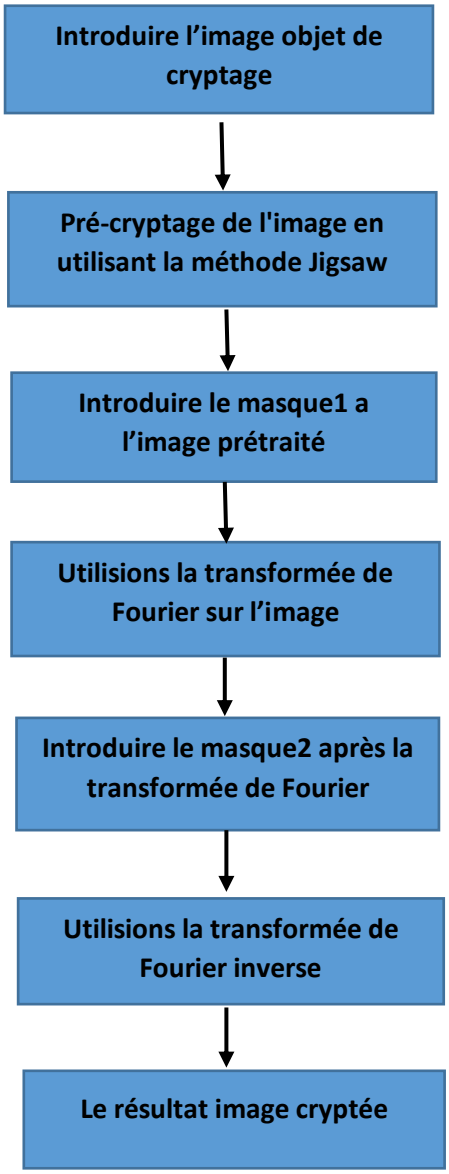


Figure III. 1: Organigramme de la technique DRPE (cryptage).

III.1.2 Schéma synoptique de la technique DRPE utilisée :

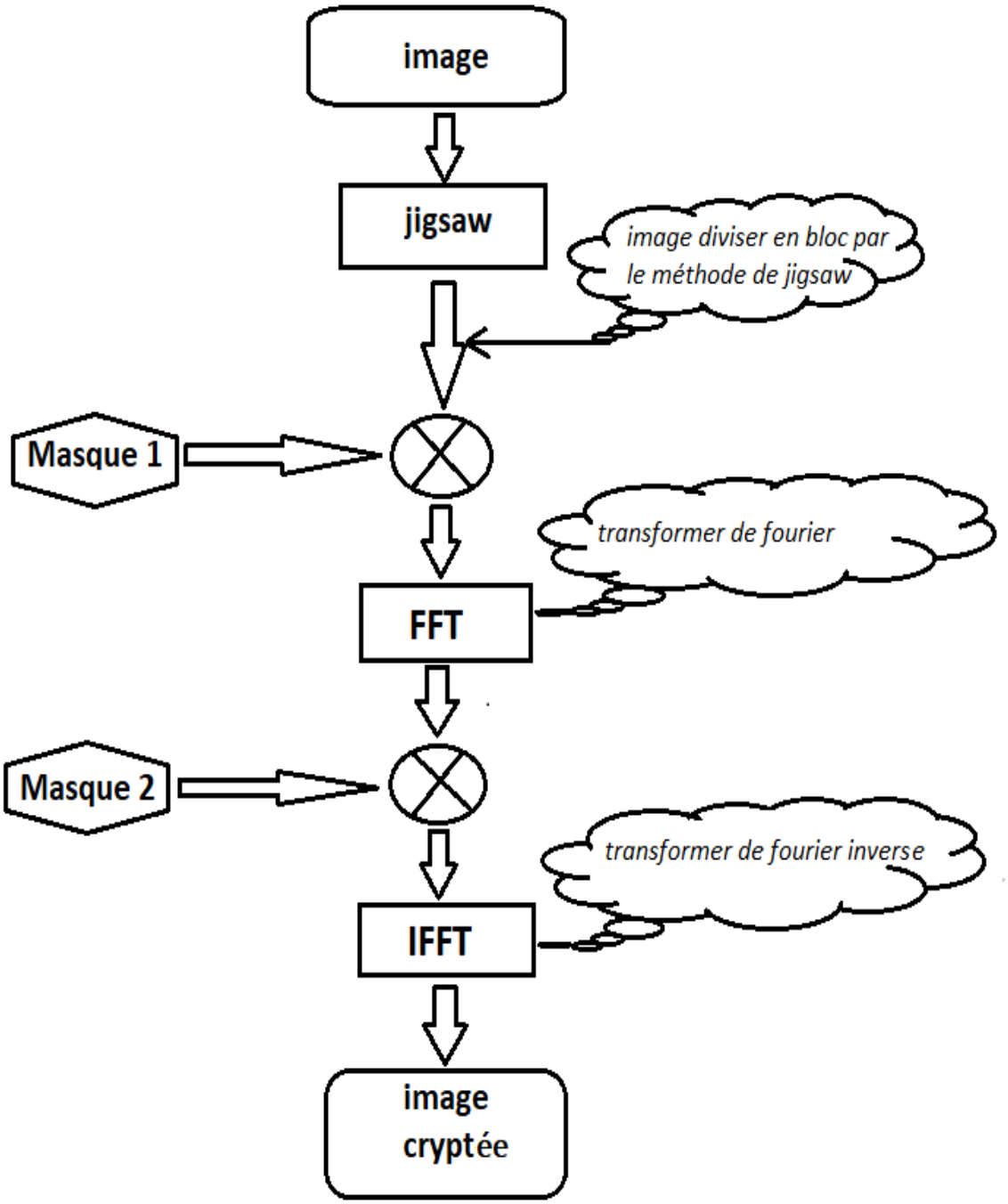


Figure III. 2: schéma synoptique de cryptage.

Sous forme mathématique, le cryptage réalisé dans ce chapitre est donné par l'expression suivante :

$$\boldsymbol{Image_{cryptée} = FFT^{-1}[FFT((Image\_Jigsaw \times masque1)) \times masque2]}$$

Avec: $\boldsymbol{masque1 = e^{j2\pi f_1(x)}}$ $\boldsymbol{masque2 = e^{j2\pi f_2(x)}}$

$\boldsymbol{f_1(x)}$ et $\boldsymbol{f_2(x)}$ sont des fonctions chaotiques.

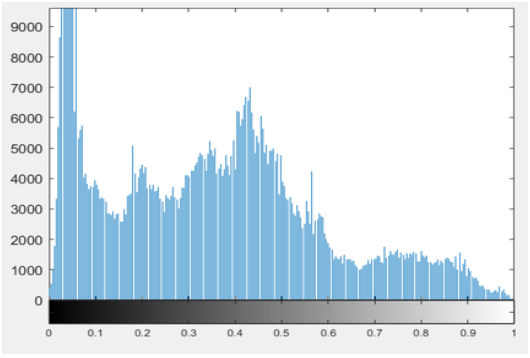
S'agissant de la DRPE classique, la création des masques (création de phases aléatoires entre 0 et$\boldsymbol{2\pi}$) est réalisée selon l'expression :$\boldsymbol{masque = e^{j2\pi.rand(m,n)}}$

Avec $\boldsymbol{m, n}$ les dimensions de l'image.

III.2 Résultats de simulation :

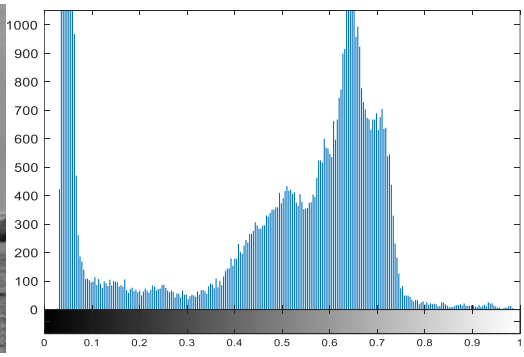
Pour étudier les performances de la technique de cryptage utilisée, nous allons la tester par simulation dans l'environnement Matlab en considérant deux types d'images: Lena et Cameraman.

a. Lena image



b. histogramme

c. Cameraman image



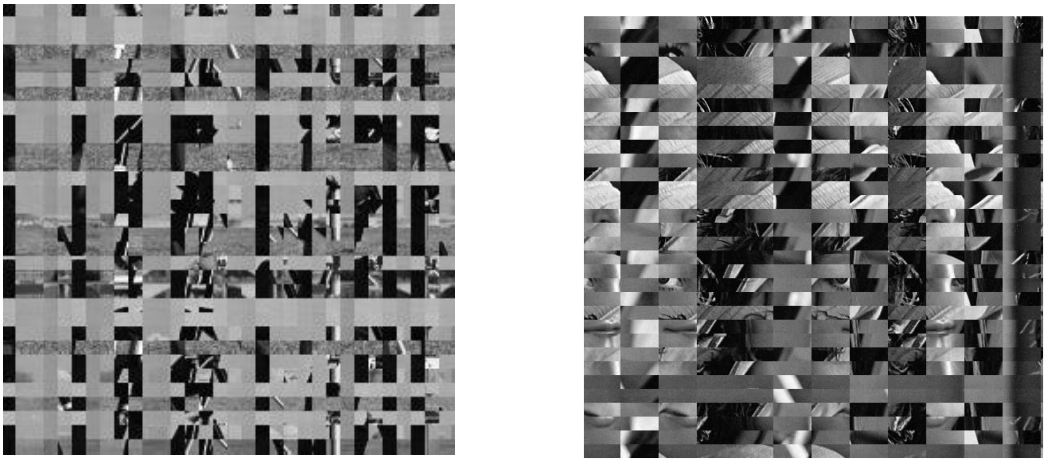
d. histogramme

Figure III. 3: images (Lena et cameraman) avec leurs histogrammes.

III.3 Pré cryptage :

Cette phase contribue d'avantage à l'amélioration du cryptage : en effet, elle consiste en la division de l'image en blocs élémentaires répartis d'une façon aléatoire en lignes et en colonnes.

L'image subit la transformation Jigsaw est représentée dans les Figure III.3.d'apres cette figure il est clair que l'image est complètement désordonnée et qui va subir à son tour un cryptage en utilisant la méthode DRPE ce qui contribue davantage à l'amélioration du cryptage.



a. Jigsaw de Cameraman b. Jigsaw de Lena

Figure III. 4: images (Lena, cameraman) après la transformation Jigsaw.

III.4 Cryptage par la méthode DRPE améliorée :

Dans cette phase, il s'agit de réaliser un cryptage de l'image déjà subie un pré cryptage par la transformation Jigsaw. Il est à noter que la création des masques est réalisée utilisant des fonctions chaotiques à la différence de la DRPE classique utilisant une simple instruction issue de Matlab pour la création de phases aléatoires :

En effet, deux fonctions chaotiques ont été utilisées. L'une pour le masque 1, quant à l'autre c'est pour le masque 2. Chacune d'entre elles est caractérisée par ses propres paramètres (paramètre de contrôle et valeur initiale). La fonction chaotique utilisée est exprimée par

$\boldsymbol{x(i+1) = mod\left(ue^{x(i)} \times \left(1 - e^{x(i)}\right), 1\right)}$, avec $\boldsymbol{u}$ ***le paramètre de contrôle***.

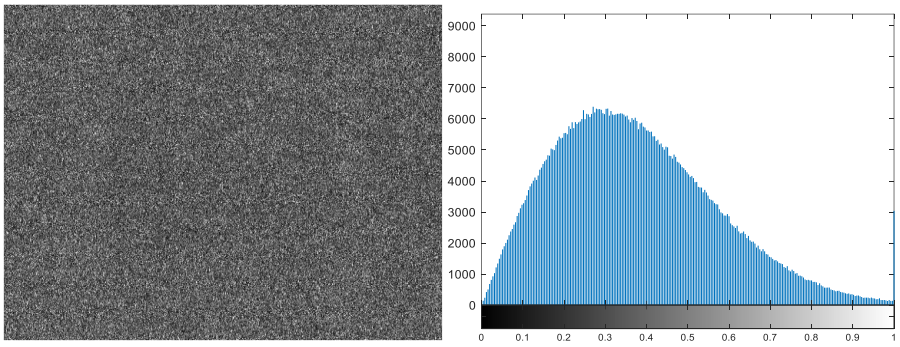
- Il est à noter que pour les deux masques, nous utilisons la même fonction chaotique avec des paramètres (clés) différents (paramètres de contrôle et valeur initiale).

a. Pour la première fonction: Valeur initiale $\boldsymbol{x(1) = 0.28}$, Paramètre de controle: $\boldsymbol{u_1 = 3.99}$

b. Pour la deuxième fonction: Valeur initiale$\boldsymbol{x(1) = 0.38}$, Paramètre de controle: $\boldsymbol{u_2 = 4.99}$

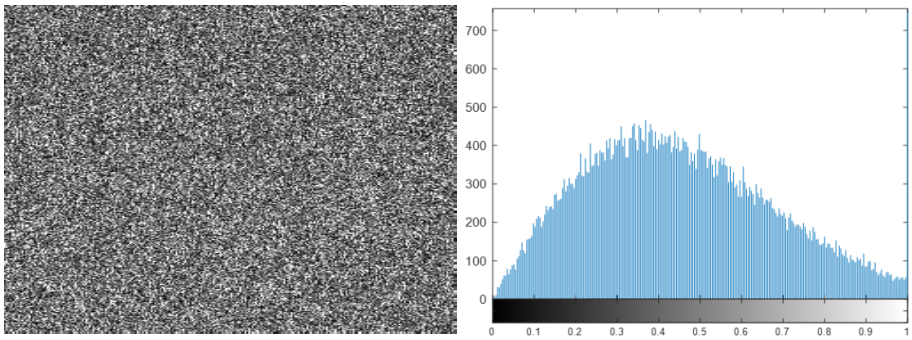
Pour s'assurer justement des performances de la fonction chaotique utilisée, il est serait intéressant de faire une comparaison avec la DRPE classique, où les phases aléatoires sont créées par une simple instruction (rand).

Apres avoir appliqué la méthode DRPE modifiée, nous avons obtenu les résultats suivants (pour les deux types d'images):



a. image cryptée (Lena) **b.** histogramme

Figure III. 5: Image Lena cryptée.



c. image cryptée (Cameraman) **d.** histogramme

Figure III. 6: Image Cameraman cryptée.

D'après les deux figures (III.5 et III.6), il est clair que nous ne pouvons extraire aucune information que ce soit de l'image cryptée ou bien de son histogramme. Néanmoins, la qualité de cryptage ne peut être mesurée à l' œil nue, mais plutôt avec l'utilisation de critères d'évaluation connus dans le domaine de cryptographie tels que le PSNR et la Corrélation.

Pour ce faire, nous avons préféré de calculer les valeurs des critères pour les deux cas de cryptage : celui avec fonction chaotique et l'autre employant la DRPE classique.

Les résultats sont donnés dans les tableaux 1 et 2 qui suivent:

Tableau III. 1: Critères d'évaluation concernant l'image cameraman.

Critère / fonction	DRPE avec une Fonction chaotique	DRPE classique
$\boldsymbol{Correlation}$	$\mathbf{5.8618 \times 10^{-4}}$	$\mathbf{0.0065}$
$\boldsymbol{PSNR}$	$\mathbf{5.5408}$	$\mathbf{14,7025}$

D' après les résultats donnés dans le tableau1, nous pouvons conclure qu'il y a une dégradation totale de l'image après cryptage. En effet, la valeur de la corrélation est proche de zéro indique qu'il n'y a aucune ressemblance entre l'image cryptée et l'image originale. Ceci, est beaucoup plus valable dans le cas d'utilisation d'une fonction chaotique améliorée. La valeur finie relativement petite du PSNR révèle aussi une dégradation totale de l'image après avoir subi un cryptage.

Tableau III. 2: Critères d'évaluation concernant l'image Lena.

Critère / fonction	DRPE avec une Fonction chaotique	DRPE classique
$\boldsymbol{Correlation}$	$\mathbf{2.7336 \times 10^{-4}}$	$\mathbf{0.0047}$
$\boldsymbol{PSNR}$	$\mathbf{4.6849}$	$\mathbf{16,4025}$

De même que précédemment, nous pouvons conclure qu'il s'agit aussi d'une dégradation quasi-totale de la qualité de l'image obtenue après cryptage. Aussi, la valeur de la corrélation est proche de zéro ce qui signifie qu'il n'y a pas de ressemblance entre l'image cryptée et l'image originale. Ceci, est beaucoup plus valable dans le cas d'utilisation d'une fonction chaotique améliorée. La valeur finie relativement petite du PSNR révèle aussi une dégradation totale de l'image après avoir subi un cryptage.

III.5 Décryptage :

En effet, cette phase consiste en l'opération inverse du cryptage, c'est-à-dire de reconstituer l'image originale. Il s'agit donc de réaliser l'inverse des étapes du cryptage dans l'ordre inverse.

L'expression analytique de cette opération est donnée comme suit :

$$\boldsymbol{Image_{décryptée} = JIGSAW^{-1}\left(masque1^{*}\left[FFT^{-1}\left(\left(FFT(Image_{cryptée}) \times masque2^{*}\right)\right)\right]\right)}$$

Avec :

$\boldsymbol{masque1^{*}}$ est le conjugué de $\boldsymbol{masque1}$;

$$\boldsymbol{masque1^{*} = e^{-j2\pi f_1(x)}}$$

$\boldsymbol{masque2^{*}}$ est le conjugué de $\boldsymbol{masque2}$;

$$\boldsymbol{masque2^{*} = e^{-j2\pi f_2(x)}}$$

III.5.1 Organigramme du décryptage effectué :

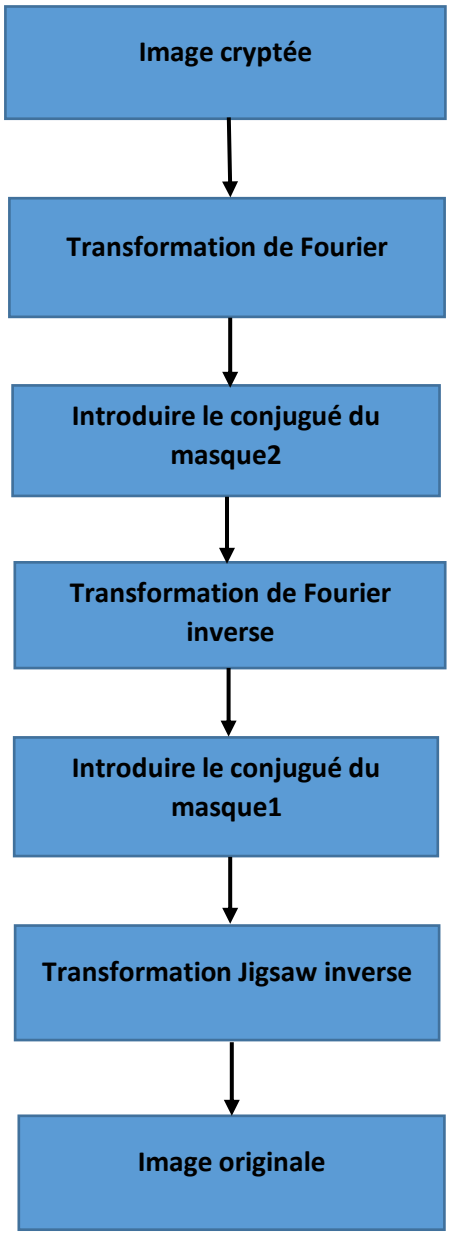


Figure III. 7: Organigramme de la technique DRPE inverse (décryptage).

III.5.2 Schéma synoptique de la technique DRPE inverse :

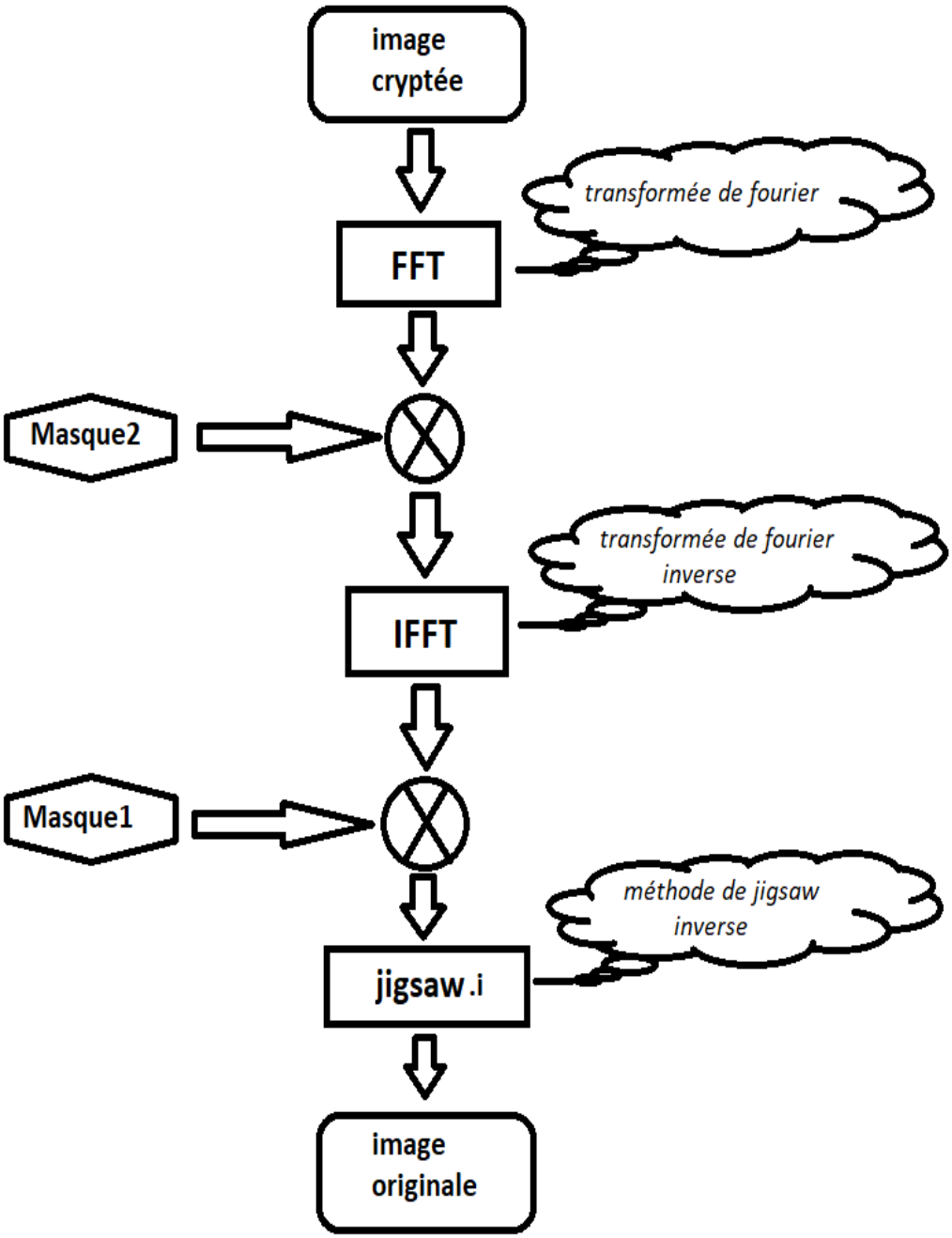
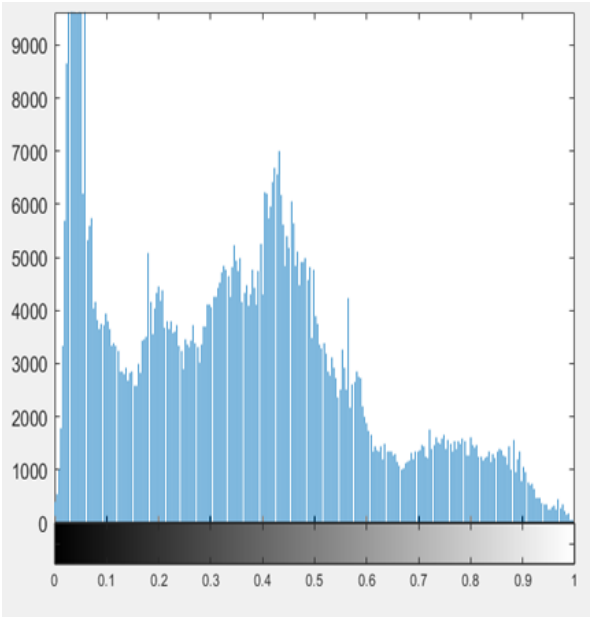


Figure III. 8: schéma synoptique de décryptage.

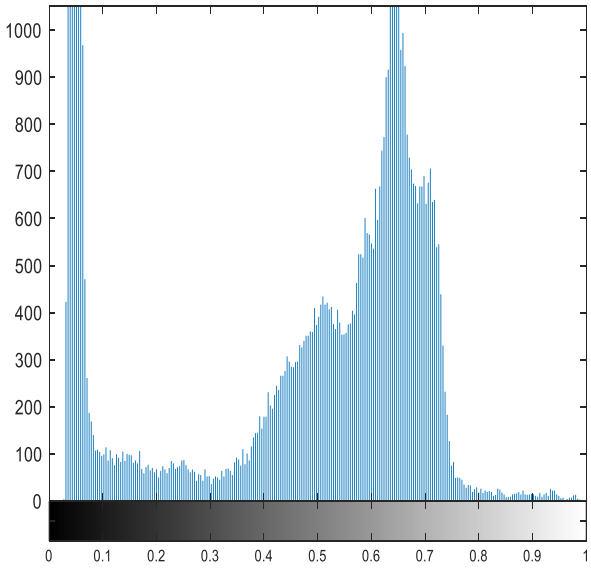
III.5.3 Résultat de décryptage concernant les deux images (Lena et Cameramen) :

a. Lena image décryptée



b. histogramme

c. Cameraman image décryptée



d. histogramme

Figure III. 9: images décrypté (Lena et Cameraman) avec son histogramme.

En visualisant la figure III.9 : on constate que les images obtenues après décryptage ressemblent

parfaitement aux images originales. Aussi, des informations à partir des histogrammes peuvent être obtenues. Néanmoins, il est nécessaire d'employer les critères d'évaluation pour voir justement si les images après décryptage ressemblent vraiment aux images originales. Les résultats issus de l'emploi de la fonction chaotique améliorés sont donnés dans les tableaux 3 et 4 suivants :

Tableau III. 3: Critère d'évaluation du décryptage (Cameraman).

$\boldsymbol{PSNR}$	Infinie
$\boldsymbol{Correlation}$	1

Tableau III. 4: Critère d'évaluation du décryptage (Lena).

$\boldsymbol{PSNR}$	Infinie
$\boldsymbol{Correlation}$	1

Les résultats obtenus confirment que l'opération de cryptage et décryptage sont correctement réalisées, et que les images apparaissent à la réception après décryptage telles qu'elles sont transmises.

III.6 Conclusion :

Dans ce chapitre, nous avons présenté la technique de cryptage modifiée (DRPE) basée sur un pré-cryptage utilisant la transformation Jigsaw. A la différence de la technique DRPE en sa forme basique utilisant une simple instruction issue de Matlab pour le calcul des phases aléatoires, le calcul des phases aléatoires est faite moyennant une fonction chaotique. Les résultats obtenus confirment bel et bien l'efficacité de la technique DRPE modifiée.

Conclusion générale

Dans notre projet de fin d'étude, nous nous sommes intéressés en particulier au cryptage d'images en utilisant la technique DRPE qui consiste en l'introduction de phases (masques) aléatoires dans les domaines spatial et fréquentiel. Un pré-cryptage à base de JIGSAW est également réalisé en raison d'améliorer la qualité du cryptage.

Pour la réalisation de notre mémoire, nous avons tout d'abord réalisé une recherche sur les différents types d'images. Puis, nous avons établi un état de l'art sur les différentes techniques de cryptage relevant de la littérature. En effet, nous avons mis en relief la technique DRPE sur laquelle se base notre étude. Donc, la technique de cryptage que nous avons utilisée dans notre application se base sur la technique DRPE après lui avoir associée un pré-cryptage moyennant la méthode JIGSAW. Concernant le pré-cryptage, il s'agit de diviser l'image que nous désirons crypter en blocs répartis de manière aléatoire en lignes et en colonnes. Cette façon de faire permet d'améliorer davantage les performances de la technique de cryptage employée. Quant à la technique DRPE, il s'agit d'introduire des phases aléatoires dans le domaine spatial puis dans le domaine fréquentiel. A la différence de la technique DRPE classique où les phases aléatoires sont crées moyennant une simple instruction issue de MATLAB, une fonction chaotique est employée La technique de cryptage utilisée a été testée par simulation dans l'environnement MATLAB pour deux types d'images. Les résultats de simulation obtenus sont très satisfaisants. Les performances de la technique utilisée ont été évaluées via des critères d'évaluation connus dans le domaine de la cryptographie. (PSNR et corrélation).

Comme perspectives à ce présent travail, nous envisageons appliquer la technique de cryptage étudiée dans le domaine de la biométrie en introduisant d'autres paramètres avec également l'utilisation de fonctions chaotiques récentes

Bibliographie

[1] Refregier, P. and Javidi, B. Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding. Optics Letters, volume 20, pp 767-769, (1995).

[2] Tewfik BekKouche, Thèse de doctorat Université Ferhat Abbas – Sétif « développement et implémentation des techniques de cryptage des donnés basées sur les transformées discrètes ».

Maïtine Bergounioux. Quelques méthodes de filtrage en Traitement d'Image. 2011. ffhal-00512280v2

[3]http://serge.wacker.free.fr/technoprimaire/c2i/revisions/formats_image.pdf

[4]M. Bergounioux, {Introduction au traitement mathématique des images-méthode déterministes

[5] Les images vectorielles et matricielles. http://www.imedias.pro/cours-en-ligne/graphismedesign/definition-resolution-taille-image/les-images-vectorielles-matricielles/.

[6] R. Dumont. Cryptographie et Sécurité informatique, Université de liége faculté des sciencesappliquées 2007, https://www.ulg.ac.be.

[8]https://www.maxicours.com/se/cours/comprendre-le-chiffrement-symetrique/

[9] https://www.hisour.com/fr/color-depth-23902/]

[10] https://kinsta.com/fr/blog/jpg-vs-jpeg/

[11] https://developer.mozilla.org/fr/docs/Web/Media/Formats/Image_types]

[12]- Rijndael, J. Daemen, and V. Rijmen. "The design of Rijndael: AES—the advanced encryption standard." Springer, 2002.

[13] - Rivest, R. L., Shamir, A., & Adleman, L. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM, 1978.

[14]National Institute of Standards and Technology (NIST). "Digital Signature Standard (DSS)." Federal Information Processing Standards Publication 186-4, 2013.

[15]N. Koblitz. "Elliptic curve cryptosystems." Mathematics of Computation, 1987.

[16]Z. Liu, Z. Zhong, and X. Li, "A double random phase encoding scheme for image encryption based on jigsaw and permutation techniques," Optik - International Journal for Light and Electron Optics, vol. 125, no. 18, pp. 5414-5419, 2014

[17]. O. Faragallah, M. alzain, H. El-Sayed, J. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naeem, and B. Soh, “Block-based optical color image encryption based on double random phase encoding”, in IEEE Access, 7, 4184-4194, (2018).

[18]https://www.c2i-revision.fr/complement.php?id_con=108

https://developer.mozilla.org/fr/docs/Web/Media/Formats/Image_types

[19] A. bayad. Introduction à la cryptographie. Université d'evry val d'essonne, 2008. Https://www.maths.univ-evry.fr/.

[20] G. Labouret. Introduction à la cryptographie. HSC - Herve Schauer Consultants - Cabinet de consultants en sécurité informatique 2001, Http://www.hsc.fr/.

[21]Y. Ma, C. Li et B. Ou, "Cryptanalyse d'un algorithme de chiffrement de blocs d'images basé sur des cartes chaotiques", Journal pour Information Security et application 54, 102566 (2020).

[22] https://larevueia.fr/quest-ce-que-la-segmentation-dimages/

[23] Rital S. « Hypergraphe de Voisinage Spatiocolorimétrique. Application en traitement d’images : Détection de contours et du bruit»; Thèse De Doctorat. Université de Bourgogne –Dijon, France, 2004.

[24]emto-physique.fr/omp/transformee-de-fourier.php /Janv. 2020

[25] Master Informatique Option : MID M.Benazzouz 2018-2019/univ.tlemcen.

[26] J. Zhao, H. Lu, X.S. Song, J.F. Li, and Y.H. Ma, “Optical image encryption based on multistage fractional Fourier transforms and pixel scrambling technique,” Opt. Commun. 249, 493-499, (2005).

[27]H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, *The fractional Fourier transform with Applications inOptics and Signal Processing*. (John Wiley & Sons, Chichester, 2001)
[28] https://en.wikipedia.org/wiki/ **(**JPEG,PNG,BMP,GIF,TIFF et PSD**).**

[29] Maïtine Bergounioux. Quelques méthodes de filtrage en Traitement d’Image. 2011. ffhal-00512280v2

[30] https://www.ni.com/docs/en-US/bundle/labview/page/lvanls/walsh_hadamard.html