République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université 8Mai 1945 – Guelma
Faculté des sciences et de la Technologie
Département d'Electronique et Télécommunications

Mémoire de fin d'étude

Pour l'obtention du diplôme de Master Académique

Domaine : **Sciences et Technologie**
Filière : **Télécommunications**
Spécialité : **Système de Télécommunications**

Cryptage des images en optique

Présenté par :

Sadaoui Imane
Sota Nesrine

Sous la direction de :

Mr . HALASSI Abdelrezzaq

Juin 2023

REMERCIEMENTS

Tout d'abord, nous remercions ALLAH le tout puissant de nous avoir donné le courage, patience, santé et volonté tout au long de nos études.

J'exprime mes profonds remerciements à mon encadreur, monsieur le docteur A.HALASSI pour l'aide compétente qu'il m'a apporté, pour sa patience et son encouragement. Son regard critique m'a été très précieux pour structurer le travail et pour améliorer la qualité des différentes sections. Je veux vraiment vous remercier car j'ai eu beaucoup de chance de vous avoir comme encadreur.

Je remercie sincèrement aussi les membres du jury qui m'ont honoré par l'acceptation de l'évaluation de la thèse de ce Master.

Sans oublier tous les enseignants du Département d'Electronique et Télécommunications

DÉDICACE

Dieu tout puissant pour tous ses bienfaits.
Je dédie ce travail :

A mon cher père
A ma chère mère
A mes frères « Imed et leur épouse Amira , Aymen, Med Elamine et Ibrahim »
A « ma tante et son fils amir »
A tous mes amis spécialement « Rayane , wala et roubila »
ainsi qu'à tous mes collègues en particulier « rayane, imane, aya, chaima , manal , meryem »

Nesrine

DÉDICACE

Dieu tout puissant pour tous ses bienfaits.
Je dédie ce travail :

A mon cher père
A ma chère mère

A mes sœurs « zayneb , manal , et mon frère salah eddine »

A « ma tante asma et ses enfants raouf et joury »

A tous mes amis spécialement « aya , manal , roua et hadil »
Ainsi qu'à tous mes collègues en particulier « nesrine , rayane , aya, chaima , meryem »

Imane

Résumé

La protection des informations sensibles est une importance capitale pour éviter qu'elles ne soient vulnérables à un accès non autorisé. Le cryptage est largement utilisé pour garantir une sécurité élevée des images. Dans ce mémoire, notre attention est portée sur le cryptage des images optiques en exploitant les propriétés remarquables de la cryptographie. Pour ce faire, nous présentons différentes méthodes de cryptage des images en utilisant le logiciel MATLAB. Les résultats obtenus sont encourageants et démontrent un niveau de sécurité élevé.

Abstract

The protection of sensitive information is of paramount importance to prevent it from being vulnerable to unauthorized access. Encryption is widely used to ensure high security for images. In this study, we focus on the encryption of optical images by leveraging the remarkable properties of cryptography. To achieve this, we present various methods of image encryption using the MATLAB software. The obtained results are encouraging and demonstrate a high level of security.

ملخص

حماية المعلومات الحساسة أمر بالغ الأهمية لمنعها من التعرض للوصول غير المصرح به. يُستخدم التشفير على نطاق واسع لضمان أمان عالٍ للصور. في هذه الأطروحة، نركز على التشفير البصري للصور من خلال استغلال خصائص التشفير. لتحقيق ذلك، نقدم طرقًا باستخدام برنامج ماتلاب. النتائج المتحصل عليها محفزة وتبين قدرة الخوارزميات علي التشفير مختلفة للتشفير المحكم.

TABLE DES MATIERES

Remerciements	**i**
Dédicace	**ii**
Résumé	**iv**
Table des matières	**v**
Liste des Figures	**viii**
Liste des Tableaux	**x**
Liste des Acronymes	**xi**
Introduction Générale	**1**
Chapitre 1 NOTIONS SUR LA POLARISATION	
1.1. Introduction	2
1.2. Phénomaine de polarisation de la lumière	2
1.2.1. C'est quoi la lumière ?.	2
1.2.2. Représentation algébrique des états de polarisation	3
1.2.3. Formalismes mathématiques	5
1.2.3.1. Formalisme de Jones	6
1.2.3.2. Formalisme de stokes	7
1.3. Milieux anisotropes	11
1.3.1. Tenseur diélectrique d'un milieu anisotrope	11
1.3.2. Biréfringence	12
1.3.3. Eléments biréfringents	13
1.4. Matrices de Jones des éléments optiques	16
1.5. Cristaux liquides	19
1.5.1. Phases des cristaux liquides	19
1.6. Corrélateur de Vander-lugt (montage 4f)	20
1.7. Modulateur spatial de lumière (SLM)	22
1.7.1. Catégories de SLM	22
1.7.2. Utilisations des SLM	22
1.7.3. Propriétés des NLC	23
1.7.4. Propriétés optiques des NLC	23

1.8. Conclusion	24
Chapitre 2 CRYPTAGE DES IMAGES	
2.1. Introduction	25
2.2. Cryptographie Différents types de cryptographie	25
2.2.1. Objectifs de la cryptographie	26
2.2.2. Différents types de cryptographie	27
2.2.2.1. Cryptographie Classique	27
2.2.2.2. Cryptographie moderne	28
2.2.2.3. Comparaison entre la cryptographie symétrique et asymétrique	29
2.2.2.4. Chiffrement hybride	30
2.3. Cryptographie visuelle	30
2.3.1. Image numérique	30
2.3.2. Types d'image numérique	31
2.3.2.1. Images matricielles	31
2.3.2.2. Images vectorielles	31
2.3.3. Formats standards d'image	32
2.3.4. Techniques de cryptage d'image	32
2.3.5. Classification des crypto-systèmes d'image	33
2.3.5.1. Crypto-systèmes d'image par bloc	33
2.3.5.2. Crypto-systèmes d'image par flux	34
2.4. Critère d'évaluation	34
2.4.1. Histogramme	34
2.4.2. Entropie	34
2.4.3. Corrélation	35
2.5. Conclusion	36
Chapitre 3 ALGORITHMES DE CRYPTAGE	
3.1. Introduction	37
3.2. Classification des algorithmes de cryptage selon le domaine de cryptage	37
3.2.1. Cryptage d'images dans le domaine spatial	37
3.2.2. Cryptage d'image dans le domaine fréquentiel basé sur les transformées	38

discrètes	
3.2.2.1. Méthode DRPE de BAHRAM JAVIDI	38
3.3. Méthode de CHACHOUA	39
3.3.1. Structure de système de cryptage de CHACHOUA	40
3.3.2. Algorithme de cryptage	40
3.3.3. Algorithme de Décryptage	43
3.4. Résultats de simulation	46
3.5. Conclusion	48
Conclusion Générale	49
Référence	50

Liste des Figures

1.1.	Ellipse de polarisation.	4
1.2.	Représentation de différents états de polarisation.	5
1.3.	Structure d'une onde plan se propageant dans un milieu anisotrope	12
1.4.	Lame biréfringence	13
1.5.	Action d'un polariseur vertical sur une lumière naturelle	13
1.6.	Lame biréfringente entre Polariseur et Analyseur [2].	14
1.7.	Action d'une lame demi-onde sur une vibration rectiligne	15
1.8.	Action d'une lame quarte d'onde sur une vibration rectiligne.	15
1.9.	Polariseur linéaire avec un axe de passage incliné à un angle θ par rapport à l'axe x.	16
1.10.	Retardateur linéaire avec son axe rapide incliné à un angle θ par rapport à l'axe x.	17
1.11.	Arrangements moléculaires pour différents types de cristaux liquides. Quand il le faut, les couches ont été séparées pour plus de clarté. [11]	20
1.12.	Corrélateur optique de Vander Lugt (montage 4f)	21
1.13.	(a) Arrangements moléculaires dans une cellule à cristaux liquides lorsque les directions de polissages des couches d'alignement sont perpendiculaires. (b) Alignement des axes moléculaires avec le champ électrique.	23
2.1.	Shéma général de la cryptographie	25
2.2.	Principales techniques en cryptographie	27
2.3.	Chiffrement asymétrique	28
2.4.	Chiffrement symétrique	29
2.5.	Cryptage d'image	30
2.6.	a) Image originale, b) Image cryptée avec un algorithme de chiffrement par bloc	33
2.7.	(a) image originale, (b) image cryptée Les résultats de la technique de permutation	33
2.8.	a) Image originale, b) Image cryptée avec un algorithme de chiffrement par	34

flux	
3.1 Architecture de Permutation-Diffusion [21].	38
3.2 Schéma synoptique de cryptage DRPE	39
3.3 Schéma synoptique de décryptage DRPE	39
3.4 Système de cryptage de CHACHOUA[23].	41
3.5 Décryptage par modulation de cohérence	43
3.6 Image à crypter.	46
3.7 Images cryptées, (a) Méthode de CHACHOUA (b) Méthode de JAVIDI l'histogramme des images cryptés est illustré sur la figure	46
3.8 Histogrammes, (a) Méthode de CHACHOUA (b) Méthode de JAVIDI	47
3.9 Résultat de décryptage de la méthode de CHACHOUA, (a) image cible (b) image cryptée (c) image décryptée	47
3.10 Résultat de décryptage de la méthode de JAVIDI, (a) image cible (b) image cryptée (c) image décryptée	48

Liste des Tableaux

1.1.	Vecteurs de Stokes [7]	9
2.1.	La comparaison entre la cryptographie symétrique et asymétrique [30]	29

Liste des Acronymes

- BMP : Windows Bitmap
- CCD : Dispositif à transfert de Charge
- CM : Modulateur de Cohérence
- DOP : Degré de Polarisation
- DCT : Transformée en cosinus Discrète
- DWT : Transformée en ondelettes Discrètes
- DFT : Transformée de Fourier
- EASLM : SLM à Adressage Electrique
- GIF : Graphic Interchange Format
- HWP : Half-Wave Plate
- JTC : Joint Transform Correlator
- JPEG : Joint Photographique Experts Group
- NLC : Cristaux Liquides Nématiques
- OASLM : SLM à Adressage Optique
- OPD : Retard de chemin optique
- PCE : Peak to Correlation Energy
- POF : Filtre de phase pure
- PLV : Polariseur linéaire vertical
- PLH : Polariseur linéaire horizontal
- PLG : Polariseur linéaire gauche
- PLD : Polariseur linéaire droite
- PL : Polarisé linéairement
- PCX : PiCture eXchange
- QWP : Quarter-Wave Plate
- SOP : Etat d'Orientation de Polarisation
- SLM : Modulateur Spatial de Lumière
- TF : Transformée de Fourier
- T-DPES : Transmission-based Dual-stage Polarization Encryption System

Introduction Générale

De nos jours, les technologies de l'information et les réseaux de communication connaissent un développement considérable. Parmi les avancées les plus remarquables, nous constatons une croissance exponentielle de la transmission d'informations multimédias, telles que les vidéos et les images, à travers ces réseaux. Des domaines tels que l'imagerie médicale et les communications militaires ont particulièrement bénéficié de ces progrès.

Cependant, cette expansion de la transmission d'images soulève une problématique majeure : comment protéger efficacement la transmission d'une image à travers des canaux de communication non sécurisés ? Il devient donc impératif de recourir au chiffrement des images avant leur envoi sur le réseau. Cette discipline de la cryptographie permet de transformer une image en clair en une version chiffrée, rendant ainsi son contenu illisible pour les personnes non autorisées.

Face à ces défis, de nouvelles technologies de chiffrement d'images ont été développées. Elles prennent en compte les caractéristiques spécifiques des images pour garantir une meilleure sécurité et une plus grande confidentialité. Certaines de ces méthodes exploitent des algorithmes de chiffrement symétriques ou asymétriques adaptés aux images, tandis que d'autres se basent sur des techniques de stéganographie pour dissimuler des informations sensibles à l'intérieur même de l'image.

Le premier chapitre de ce travail de recherche se concentrera sur la polarisation de la lumière, en mettant notamment l'accent sur les trois états fondamentaux souvent utilisés dans la conception de dispositifs de cryptage optiques.

Le deuxième chapitre, quant à lui, sera composé de deux parties : une étude de la cryptographie, en présentant ses objectifs et ses différentes méthodes de chiffrement, afin de décrire les notions de base et les différents types d'images numériques, ainsi que les techniques de chiffrement d'image.

Enfin, dans le troisième chapitre, nous présenterons des méthodes de chiffrement optique. Nous étudierons les principes fondamentaux de ces méthodes, telles que la polarisation de la lumière et les dispositifs de cryptage optiques. Nous analyserons les avantages de ces approches en termes de sécurité des images, en les comparant aux méthodes traditionnelles de chiffrement optique telles que la DRPE (Double Random Phase Encoding).

Chapitre 1

Notions sur la polarisation

1.1. Introduction

La polarisation de la lumière est une propriété importante qui peut être utilisée pour manipuler et contrôler la lumière dans de nombreuses applications optiques. Une polarisation biréfringente est une polarisation où la lumière se déplace à des vitesses différentes dans des directions perpendiculaires, en raison des propriétés anisotropes du matériau à travers lequel elle se propage.

Dans ce chapitre, nous allons nous concentrer sur la polarisation de la lumière, notamment les trois états fondamentaux qui sont souvent utilisés dans la conception de dispositifs de cryptage optiques.

1.2. Phénomaine de polarisation de la lumière

1.2.1. C'est quoi la lumière ?

La lumière est une onde électromagnétique associée à la propagation de champs électriques et magnétiques. La direction de propagation de la lumière est évidemment une propriété fondamentale, mais les directions de ses champs électriques et magnétiques sont également très importantes : plus précisément, la direction du champ électrique caractérise ce qu'on appelle la polarisation de la lumière.

Le concept de polarisation est issu des travaux du physicien Etienne Malus qui démontra en 1809 que la lumière réfléchie par une surface de verre peut être polarisée linéairement et parallèlement à la surface. L'œil humain y est à peine sensible, mais la polarisation de la lumière est un phénomène très courant dans la nature et dans les nouvelles technologies de notre vie quotidienne. La lumière visible est une onde électromagnétique de longueur d'onde λ dans le vide Entre 400 nm pour le violet et 800 nm pour le rouge.

Les ondes lumineuses sont physiquement associées à la propagation de champs électriques et magnétiques vibrant à une fréquence notée ν très élevé, environ 10^{15} Hz, et dépendant de la longueur d'onde selon $\nu = c/\lambda$ Où c c'est la vitesse de la lumière dans le vide. La lumière

naturelle, comme la lumière du soleil, n'est pas polarisée. Le champ électrique d'une onde électromagnétique émise par le soleil oscille dans une direction pendant un certain temps, puis saute brusquement dans une nouvelle direction aléatoire tout en restant perpendiculaire à la direction de propagation. Il en va de même pour la lumière d'une ampoule ou d'une enseigne au néon [1].

1.2.2. Représentation algébrique des états de polarisation

L'état de polarisation de l'onde est défini par la courbe décrite par extrémité du vecteur champ électromagnétique dans le plan d'onde. Les coordonnées de cette courbe dans le temps sont,

$$\begin{cases} E_x = A_x\, cos(\omega t - kz + \varphi_x) \\ E_y = A_y\, cos(\omega t - kz + \varphi_y) \end{cases} \quad (1.1)$$

- A_x et A_y : les amplitudes des composantes du champ électrique .
- ω: la pulsation.
- $k = 2\pi\lambda$: la norme du vecteur d'onde.
- $\varphi_x\ et\ \varphi_y$: sont les phases des composantes.

Supposant z=0 et le déphasage entre deux champ est φ donc l'expression (1.1) peut s'écrire sous la forme,

$$\begin{cases} E_x = A_x\, cos(\omega t) \\ E_y = A_y\, cos(\omega t + \Delta\varphi) \end{cases} \quad (1.2)$$

$$\begin{cases} \frac{E_x}{A_x} = cos(\omega t) \\ \frac{E_y}{A_y} = cos(\omega t + \Delta\varphi) = cos(\omega t).cos(\Delta\varphi) - sin(\omega t).sin(\Delta\varphi) \end{cases} \quad (1.3)$$

Manipulant l'équation (1.3) on obtient,

$$\frac{E_y}{A_y} = \frac{E_x}{A_x}.cos(\Delta\varphi) - sin(\omega t).sin(\Delta\varphi) \quad (1.4)$$

D'après la transformation trigonométrique suivante,

$$cos^2(x) = 1 - sin^2(x) \tag{1.5}$$

L'équation (1.4) devient,

$$\left(\frac{E_y}{A_y}\right)^2 + \left(\frac{E_x}{A_x}\right)^2 - 2\frac{E_x E_y}{A_x A_y} cos(\Delta\varphi) = sin^2(\Delta\varphi) \tag{1.6}$$

Qui est l'équation d'une ellipse ? Dans le cas général, l'état de polarisation d'une onde lumineuse est donc elliptique et ses caractéristiques sont entièrement déterminées par la connaissance des grandeursA_x, A_y et φ. La Figure 1.1 donne une représentation de l'ellipse dans le plan Oxy [2].

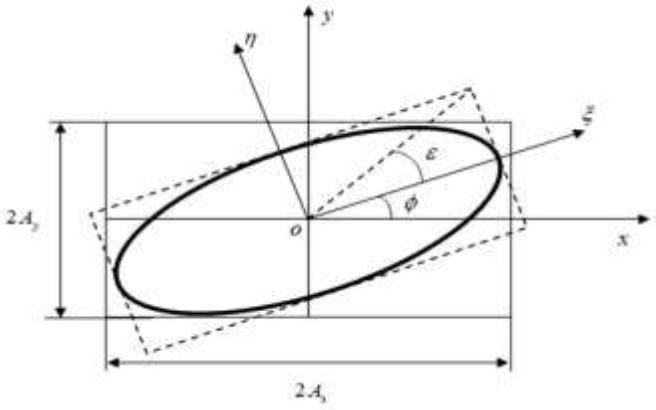


Figure1.1. Ellipse de polarisation.

Si φ est constant dans le temps, l'onde est alors dite polarisée elliptiquement et l'équation correspond à une ellipse (cas général). C'est à dire son ellipticité ε, son angle d'orientation ϕ, le déphasage $\Delta\varphi$ et son sens de rotation (qui dépend directement du signe de $\Delta\varphi$), et qui sont relient par les deux équations suivantes,

$$tan(2\Psi) = \frac{2A_x A_y}{A_x^2 - A_y^2} cos(\Delta\varphi)$$

$$sin(2\varepsilon) = \frac{2A_x A_y}{A_x^2 + A_y^2} sin(\Delta\varphi) \tag{1.7}$$

Quelques états de polarisation sont représentés sur la Figure 1.3. En particulier, lorsque $\Delta\varphi$ =0, l'onde est polarisée rectilignement et lorsque $\Delta\varphi \leq \pm\frac{\pi}{2}$ avec $A_x = A_y$, l'onde est polarisée Circulairement (gauche ou droite selon le signe du déphasage). [3]

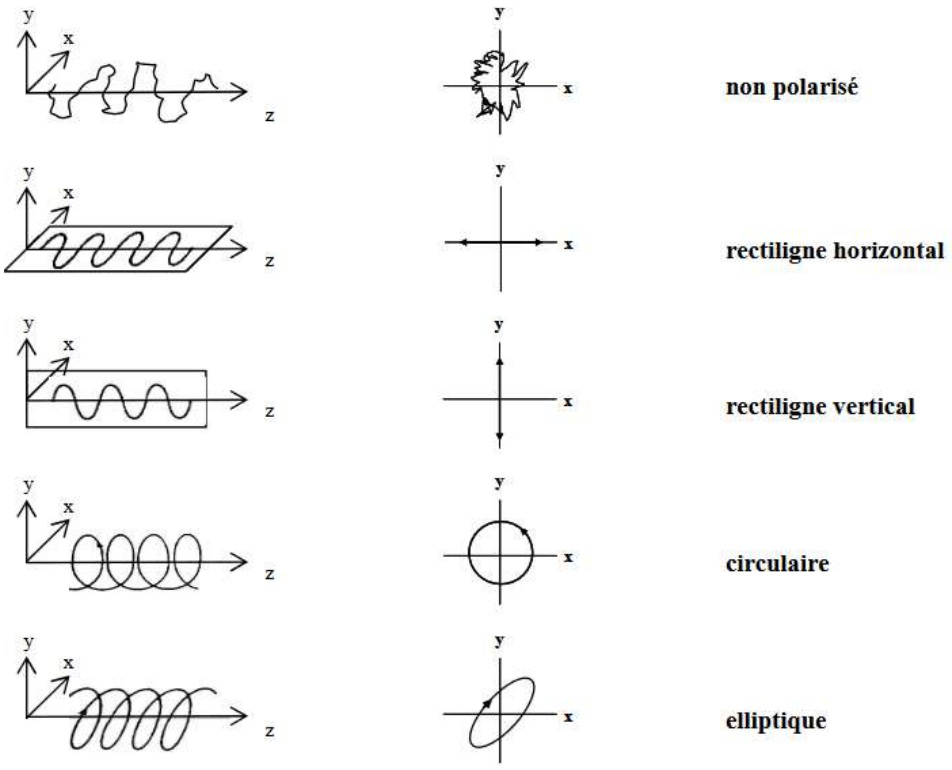


Figure 1.2. Représentation de différents états de polarisation.

On ne peut parler d'état complètement polarisé que si l'évolution du champ électrique est déterministe, c'est-à-dire si les grandeurs A_x , $A_y$et $\Delta\varphi$ sont indépendantes du temps pendant la durée de la mesure. Si le champ électrique évolue de manière totalement aléatoire, alors l'onde est dite non polarisée. En général, une onde lumineuse est composée d'une partie totalement polarisée et d'une partie non polarisée.

1.2.3. Formalismes mathématiques

Il peut être nécessaire de représenter mathématiquement un état de polarisation de lumière, par exemple, afin de suivre son évolution à travers un système optique. On peut notamment utiliser :

- Le formalisme de Jones, particulièrement adapté à la représentation d'états complètement polarisés
- Les paramètres de Stokes, associés aux matrices de Mueller, qui permettent de décrire également la lumière partiellement polarisée.

1.2.3.1. Formalisme de Jones

Formalisme de représentation mathématique de la polarisation d'une onde lumineuse. Ce formalisme fût introduit par **Robert Clark *Jones*** en 1941 et décrit uniquement une onde monochromatique entièrement polarisée. Ce formalisme s'écrit sous forme d'un vecteur appelé vecteur de Jones, où se trouvent deux informations sur l'onde : son amplitude et sa phase. La forme du vecteur quant à elle nous décrit la nature de la polarisation de l'onde.

Le vecteur de champ électrique d'une onde lumineuse arbitrairement polarisée peut-être décrit en termes de deux composantes orthogonales et linéairement polarisées [4] Comme,

$$E=A_x.\,e^{i(wt-kz+\varphi x)}i+A_y.\,e^{i(wt-kz+\varphi y)}j \tag{1.8}$$

La forme matricielle,

$$E=\begin{bmatrix}E_x\\E_y\end{bmatrix}=\begin{bmatrix}A_x e^{i(\omega t-kz+\varphi x)}\\A_y e^{i(\omega t-kz+\varphi y)}\end{bmatrix}$$

$$=\ e^{i(wt-kz)}\begin{bmatrix}A_x e^{i.\varphi x}\\A_y e^{i.\varphi y}\end{bmatrix} \tag{1.9}$$

Où,

$$V=\begin{bmatrix}A_x e^{i.\varphi x}\\A_y e^{i.\varphi y}\end{bmatrix} \tag{1.10}$$

Ce vecteur est de nature complexe, l'intensité du champ associé à ce vecteur est donnée par,

$$I=E.\,E^*=\begin{matrix}A_x e^{i.\varphi x}\\A_y e^{i.\varphi y}\end{matrix}\cdot\begin{bmatrix}A_x e^{-i.\varphi x}\\A_y e^{-i.\varphi y}\end{bmatrix}=\left[A_x^2+A_y^2\right] \tag{1.11}$$

C'est le carré du module de E.

Pour un état de polarisation rectiligne orienté suivant l'angle θ par rapport à l'axeO_x, son vecteur de Jones normalisé, dans le repèreO_{xy}, est :

$$V = \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix} \tag{1.12}$$

On peut lui associer son état orthogonal, qui est rectiligne et polarisé suivant la direction θ+π/2 par rapport à l'axe O_x. Son vecteur de Jones est tel que :

$$V = \begin{bmatrix} -\sin\theta \\ \cos\theta \end{bmatrix} \tag{1.13}$$

Vecteur de Jones des différents états de polarisation :

La polarisation linéaire suivant x ou y est exprimée par [5],

$$x = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad , \quad y = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.14}$$

La polarisation linéaire suivant une direction générale format l'angle θ avec l'axe **x** s'écrit,

$$J(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} \tag{1.15}$$

La polarisation circulaire sont données par,

$$D = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} \quad , \quad L = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix} \tag{1.16}$$

Enfin la polarisation elliptique exprimée dans le système d'axes propres de l'ellipse s'écrit,

$$J(y = 0, x) = \begin{pmatrix} \cos x \\ \sin x\, e^{-i\frac{\pi}{2}} \end{pmatrix} \tag{1.17}$$

1.2.3.2 Formalisme de Stokes

(a) Cas d'une onde polarisée rectiligne et circulaire

La représentation moderne de la lumière polarisée trouve en fait son origine en 1852 dans les travaux de G. G. Stokes. Il a introduit quatre quantités qui ne sont que des fonctions d'observables de l'onde lumineuse et qui sont maintenant connues sous le nom de paramètres de Stokes. L'état de polarisation d'un faisceau de lumière (soit naturelle, soit totalement ou partiellement polarisée) peut être décrit en fonction de ces quantités. Ainsi, le vecteur de Stokes s'écrie à partir du vecteur de Jones comme suit [6],

$$V=\begin{bmatrix} A_x e^{-j\varphi/2} \\ A_y e^{j\varphi/2} \end{bmatrix} \tag{1.18}$$

En manipulant l'équation (1.6) en trouve les paramètres de Stockes,

$$\begin{cases} S_0 = A_x^2 + A_y^2 \\ S_1 = A_x^2 - A_y^2 \\ S_2 = 2.A_x A_y \cos\varphi \\ S_3 = 2.A_x A_y \sin\varphi \end{cases} \tag{1.19}$$

Ces quatre paramètres peuvent être s'écrire en fonction des intensités de l'onde. Ces intensités dans le plan transverse sont notées I_x, I_y , $I_{+45°}, I_{-45°}$,pour la composante rectiligne dans le plan d'onde O_{xy} suivant les axes x, y et les angles $+45°, -45°$ par rapport à l'axeO_x, respectivement. Par sa définition, il est certain que le paramètre S_0 représente l'intensité totale de l'onde optique. Le paramètre S_1 représente la différence des intensités entre les composantes rectilignes suivant $O_x$et O_y. Alors, on peut s'écrire ces deux premiers paramètres comme,

$$S_0 = I_x + I_y$$

$$S_1 = I_x - I_y \tag{1.20}$$

Pour le reste des paramètres, nous décomposons l'état V sur la base des états circulaires droits et gauches, avec leurs intensités sont notées I_D et I_G , respectivement. En utilisant les matrices de changement de base adéquates, V devient,

$$V_{45°} = \frac{1}{\sqrt{2}}\begin{bmatrix} A_x e^{-j\varphi/2} + A_y e^{+j\varphi/2} \\ A_x e^{-j\varphi/2} - A_y e^{+j\varphi/2} \end{bmatrix}$$

$$V_{cir} = \frac{1}{\sqrt{2}}\begin{bmatrix} A_x e^{-j\varphi/2} - jA_y e^{+j\varphi/2} \\ A_x e^{-j\varphi/2} + jA_y e^{+j\varphi/2} \end{bmatrix} \tag{1.21}$$

Maintenant, nous calculons la différence des intensités dans chacune des deux bases, nous trouvons,

$$I_{+45°} - I_{-45°} = 2A_x A_y \cos\varphi = S_2$$

$$I_G - I_D = 2A_x A_y \sin\varphi = S_3 \tag{1.22}$$

Le vecteur de Stokes peut être écrit comme,

$$S = \begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} I_0 \\ I_x - I_y \\ I_{+45^\circ} - I_{-45^\circ} \\ I_G - I_D \end{pmatrix} \quad (1.23)$$

Les vecteurs de Stokes sont souvent normalisés par rapport à la composante. Six états de polarisation d'une onde lumineuse remarquables peuvent être exprimés de la façon suivante,

Tableau 1.1 Vecteurs de Stokes [7].

$\boldsymbol{PLH}$	$\boldsymbol{PLV}$	$\boldsymbol{PL+45^\circ}$	$\boldsymbol{PL-45^\circ}$	$\boldsymbol{PLD}$	$\boldsymbol{PCG}$
$(\boldsymbol{S_0})$	(S_{90°)	(S_{+45°)	(S_{135°)	(S_D)	(S_G)
$\begin{bmatrix} \mathbf{1} \\ \mathbf{1} \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix}$	$\begin{bmatrix} 1 \\ -1 \\ 0 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 1 \\ -1 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix}$

(b) Cas d'une onde non polarisée

Dans ce cas, $A_x = A_y = A, et\ \Delta\varphi$, varie aléatoirement dans le temps. Par conséquent, $\langle cos\Delta\varphi \rangle = \langle sin\Delta\varphi \rangle$. Ce qui donne [4],

$$\begin{cases} S_0 = A_x^2 + A_y^2 = 2A^2 \\ S_1 = 0 \\ S_2 = 0 \\ S_3 = 0 \end{cases} \quad (1.24)$$

Ainsi, le vecteur de Stokes normalisé correspondant est donné par,

$$S = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad (1.25)$$

On peut noter que, dans ce cas,

$$S_0^2 > S_1^2 + S_2^2 + S_3^2 \quad (1.26)$$

(c) Cas d'une onde partiellement polarisée et matrice de Mueller

Une onde lumineuse quelconque de vecteur de Stokes S pourra se décomposer en une partie Complètement polarisée et en une partie non polarisée, cette décomposition est unique :

$$S_{par} = S_{POL} + S_{N\,POL} \tag{1.27}$$

La forme matricielle peut être exprimée comme suite,

$$\begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix} = \begin{bmatrix} pS_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix} = \begin{bmatrix} (1-p)S_0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{1.28}$$

Avec p, est le degré de polarisation, que nous appellerons DOP,

$$P = \frac{\sqrt{S_1^2+S_2^2+S_3^2}}{S_0} \tag{1.29}$$

Qui est appelé degré de polarisation. Le degré de polarisation p est égal à 1 pour la lumière totalement polarisée et égal à 0 pour la lumière non polarisée (naturelle). Les colonnes de Stokes avec un degré de polarisation entre 0 et 1 représentent des faisceaux de lumière partiellement polarisés. Les vecteurs de Stokes de faisceaux de lumière partiellement polarisés peuvent également être représentés à l'aide de la sphère de Poincaré. On peut établir un formalisme de matrices qui relie le vecteur de Stokes d'un faisceau de lumière sortant d'un dispositif optique aux vecteurs de Stokes du faisceau d'entrée. Cette matrice est appelée matrice de Mueller d'après son inventeur. C'est une matrice 4 × 4 avec des éléments réels. Les vecteurs de Stokes S sont ensuite transformés par cette matrice

$$S' = \begin{pmatrix} S'_0 \\ S'_1 \\ S'_2 \\ S'_3 \end{pmatrix} = \begin{pmatrix} M_{11} & M_{12} & M_{13} & M_{14} \\ M_{21} & M_{22} & M_{23} & M_{24} \\ M_{31} & M_{32} & M_{33} & M_{34} \\ M_{41} & M_{42} & M_{43} & M_{44} \end{pmatrix} \begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} \tag{1.30}$$

Toutes les matrices réelles 4 × 4 ne peuvent pas être une matrice de Mueller M. Il existe des conditions pour tester la cohérence d'une matrice pour qu'elle soit une matrice de Mueller (Brosseau, 1998). Ces conditions peuvent être formulées comme des inégalités. Les matrices de Mueller peuvent également être spécifiées pour des dispositifs non dépolarisants et sont alors appelées matrices de Mueller-Jones [8].

1.3. Milieux anisotropes

Un milieu est anisotrope optiquement si ses propriétés optiques diffèrent suivant la direction de propagation de l'onde. La réponse du milieu dépendra en fait de la direction du champ électrique associé à l'onde.

Sous l'effet du champ électrique E et le champ magnétique B d'un milieu dépendent des directions des vecteurs de champs, les relations entre les champs peuvent être écrites sous la forme suivante [5],

$$\mathrm{D} = \varepsilon_0[\varepsilon]\mathrm{E}$$
$$\mathrm{H} = \mu_0[\mu]\mathrm{B} \qquad (1.31)$$

Avec [ε] et [μ], sont respectivement, le tenseur de permittivité relative et le tenseur de perméabilité.

1.3.1. Tenseur diélectrique d'un milieu anisotrope

Pour les milieux anisotropes, la permittivité du milieu dans un système d'axesO_{xyz}, devient alors,

$$\begin{cases} \mathrm{D_x} = \varepsilon_{xx}.\mathrm{E_x} + \varepsilon_{xy}.\mathrm{E_y} + \varepsilon_{xz}.\mathrm{E_z} \\ \mathrm{D_y} = \varepsilon_{yx}.\mathrm{E_x} + \varepsilon_{yy}.\mathrm{E_y} + \varepsilon_{yz}.\mathrm{E_z} \\ \mathrm{D_z} = \varepsilon_{zx}.\mathrm{E_x} + \varepsilon_{zy}.\mathrm{E_y} + \varepsilon_{zz}.\mathrm{E_z} \end{cases} \qquad (1.32)$$

Ce tenseur est alors diagonalisable, autrement dit, il existe un système d'axes particuliers dans lequel les composantes $(\varepsilon_{ij}(i \neq j))$ sont nulles. Dans ce repère propre au milieu matériel, les axes de coordonnés sont les axes principaux du milieu. Le tenseur diélectrique est alors donné par,

$$\varepsilon = \begin{pmatrix} \varepsilon_x & 0 & 0 \\ 0 & \varepsilon_y & 0 \\ 0 & 0 & \varepsilon_z \end{pmatrix} \qquad (1.33)$$

Par analogie avec les milieux isotropes, nous écrivons,

$$\begin{cases} \mathrm{n_x^2} = \varepsilon_x \\ \mathrm{n_y^2} = \varepsilon_y \\ \mathrm{n_z^2} = \varepsilon_z \end{cases} \qquad (1.34)$$

On peut classer les milieux en isotrope, anisotrope uniaxe et anisotrope biaxe,

(a) $n_1 \neq n_2 \neq n_3$: le milieu est dit biaxe.

$D_i = \varepsilon_0 n_i^2 E_i (i = 1,2\ ou\ 3) et\ les$ 3 "vecteurs propres" $E_i/||E_i||$ Forment une base orthogonale : on appelle ces trois directions les directions principales.

(b) $n_2 = n_3 \neq n_1$: le milieu est dit uniaxe.

E_1 définit une direction perpendiculaire à $(E_2\ , E_3)$

(c) $n_1 = n_2 = n_3$: toutes les directions sont équivalentes et le milieu est isotrope.

On appelle alors milieu uniaxe un milieu où deux des permittivités diélectriques principales sont égales entre elles, et différentes de la troisième : $\varepsilon X = \varepsilon Y \neq \varepsilon Z$.

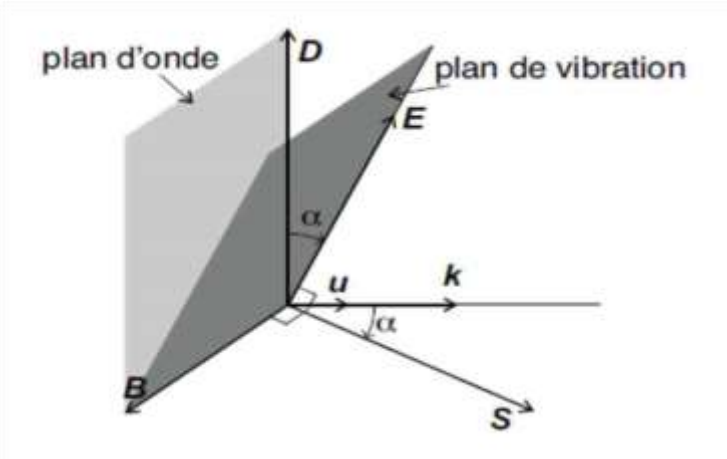


Figure1.3. Structure d'une onde plane se propageant dans un milieu anisotrope.

1.3.2. Biréfringence

La biréfringence est une propriété de certains cristaux transparents anisotropes qui ont la propriété de décomposer la lumière en deux rayons de polarisation croisée. Cette double réfraction est due au fait qu'il existe dans le cristal une direction particulière (axe de biréfringence) ou l'indice n_e dit indice extraordinaire est différent de l'indice dans les directions perpendiculaires n_o dit indice ordinaire [9].

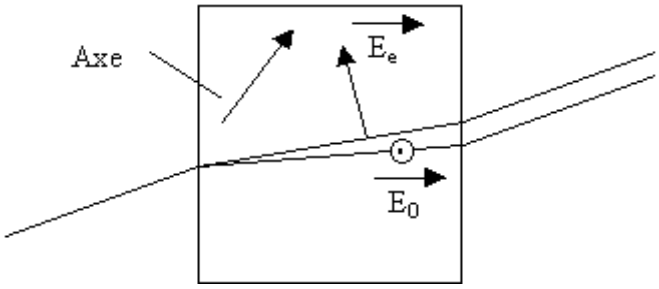


Figure1.4. Lame biréfringence.

1.3.3. Eléments biréfringents

(a) Polariseur linéaire :

Un polariseur transforme de la lumière non polarisée ou naturelle en une lumière polarisée. Il est caractérisé par son axe de transmission. Si la direction du vecteur champ électrique $\overrightarrow{E}$ de l'onde lumineuse est parallèle à son axe de transmission, celle-ci est transmise. Si non, elle est bloquée. Donc un polariseur transmet un état de polarisation et bloque l'état de polarisation orthogonal, dans le cas idéal. Cependant en pratique on a toujours une fraction de l'état orthogonal qui est transmise. Tout polariseur rectiligne peut servir d'analyseur, et inversement. En d'autres termes, il y a bien une différence de fonction entre polariseur et analyseur, mais pas de différence de nature. En fait, un analyseur est tout simplement un dispositif exactement identique à un polariseur mais dont le but est d'agir sur une onde déjà polarisée [6].

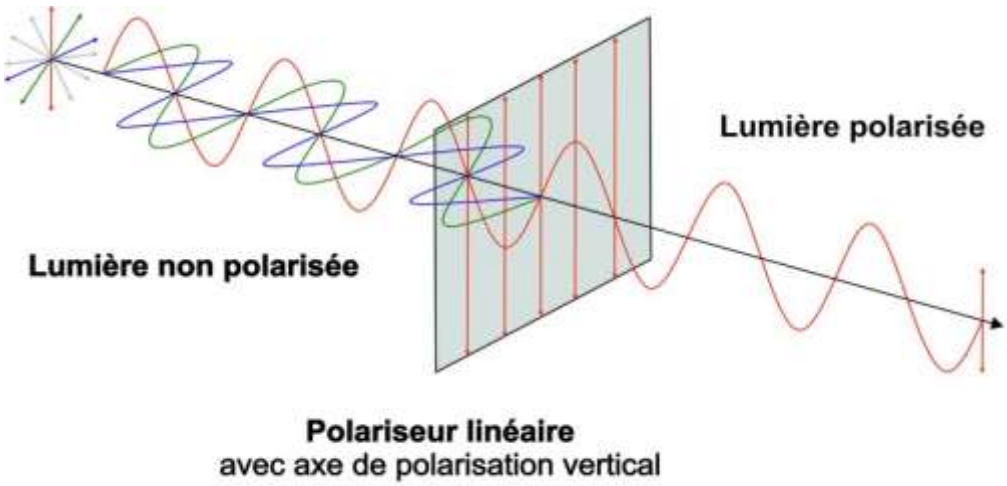


Figure1.5. Action d'un polariseur vertical sur une lumière naturelle.

(b) Lame biréfringente

Lame biréfringente (ou déphaseur) est une lame mince taillée dans un matériau anisotrope de sorte que l'axe extraordinaire et l'axe z soit parallèle aux faces de la lame. Cette lame présente deux directions orthogonales S et F (axes optiques).

Le champ d'une onde plane monochromatique polarisée rectilignement pénètre dans la lame anisotrope donne deux ondes polarisées rectilignement suivant deux directions orthogonales suivant chacune des deux directions principales de la lame, avec deux vitesse différentes tel que l'onde lumineuse polarisée suivant l'axe rapide f, se propage avec une vitesse supérieure à celle de l'onde polarisée suivant l'axe lent s, qui permet de retarder une onde à l'autre ce qui provoque un déphasage, qui s'écrit[4],

$$\Delta\varphi = \frac{2\pi.\Delta n.e}{\lambda} \qquad (1.35)$$

e : Épaisseur de la lame,

Δn : $(ns - nf)$,Biréfringence de la lame dans le plan F-S,

λ : Longueur d'onde.,

T : la différence de marche ($T = \Delta n.e$).

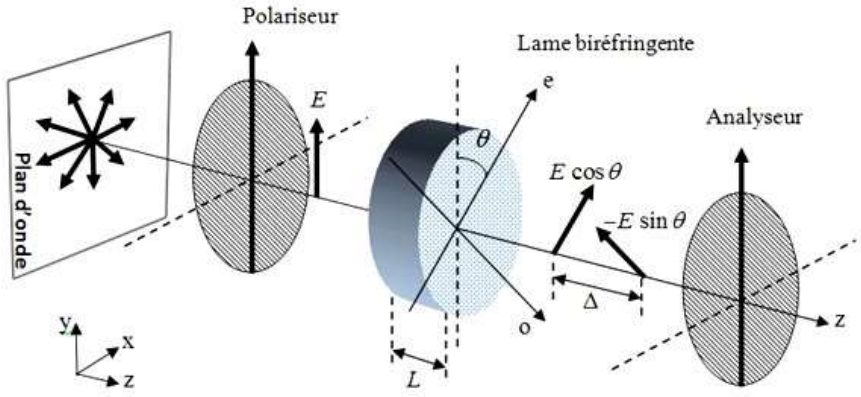


Figure1.6. Lame biréfringente entre Polariseur et Analyseur [2].

➢ **Lame demi-onde**

Une lame biréfringente est demi-onde, également notée lame $\boldsymbol{\lambda/2}$, si elle introduit un retard de phase $\Delta\varphi = (k\pi)$, avec *k* un entier. La différence de marche optique [6].

$$\Delta\varphi = \pi \Leftrightarrow \Delta n = \lambda/2$$

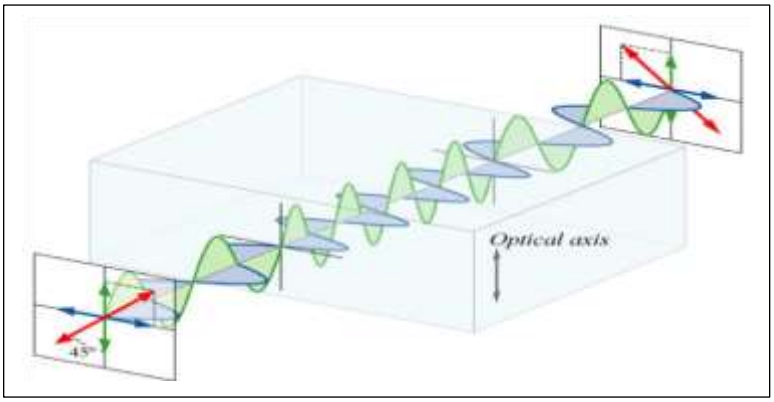


Figure1.7. Action d'une lame demi-onde sur une vibration rectiligne.

➢ **Lame quarte d'onde**

Une lame biréfringente est quarte onde, également notée lame λ/4, si elle introduit un retard de phase $\Delta\varphi = (2p+1)\frac{\pi}{2}$, avec *p* un entier,

$$\Delta\varphi = \frac{\pi}{2} \leftrightarrow \Delta n = \frac{2\pi}{\varphi} = \lambda/4$$

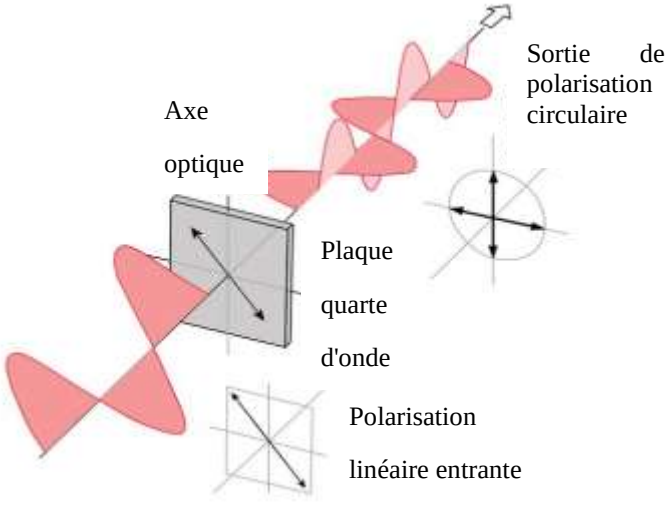


Figure 1.8. Action d'une lame quarte d'onde sur une vibration rectiligne.

1.4. Matrices de Jones des éléments optiques

La représentation vectorielle de Jones permet de déterminer l'effet d'un composant de polarisation sur un état d'orientation de polarisation (SOP) en multipliant le vecteur Jones d'entrée par une matrice $2x2$ appelée matrice de Jones du composant. Si un état de polarisation A donné passe à travers un dispositif polarisant dont la matrice de Jones est J, l'état de polarisation de sortie A' sera donné par$A' = J\,A$. S'il y a deux dispositifs en série avec des matrices de Jones $J1\ et\ J2$ respectivement, la matrice de Jones de la combinaison est donnée par $J2\,J1$ et l'état de polarisation de sortie sera donné par $A' = J2\,J1$A. Dans la section suivante, nous obtenons des matrices de Jones pour certains composants de polarisation de base [7].

- Un polariseur linéaire filtre un seul composant polarisé linéairement d'un État d'Orientation de Polarisation donné, l'axe de passage définit la direction de polarisation**.**

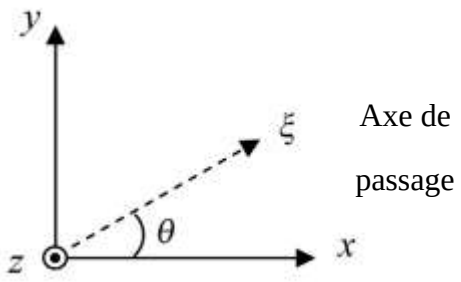


Figure 1.9. Polariseur linéaire avec un axe de passage incliné à un angle θ par rapport à l'axe x.

Si un faisceau lumineux avec des composantes $x\ et\ y\ , Ex\ et\ Ey$ passe à travers le polariseur donné, l'État d'Orientation de Polarisation de sortie sera linéairement polarisé, donc la matrice de Jones d'un polariseur est donnée par,

$$T(\theta) = \begin{pmatrix} cos^2\,\theta & sin\,\theta\,cos\,\theta \\ sin\,\theta\,cos\,\theta & sin^2\,\theta \end{pmatrix} \tag{1.36}$$

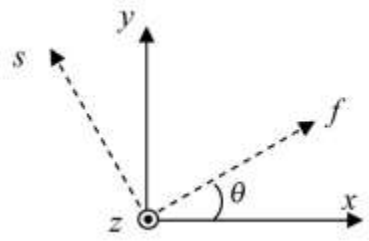
En substituant $\theta = 0, \pi/4\ ou\ \pi/2$ dans l'équation (1.36), on obtient des matrices de Jones pour un polariseur linéaire avec son axe de passage orienté dans les directions $x,\ \theta = \pi/4$ et y, respectivement :

$$T(0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$T\left(\frac{\pi}{2}\right) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad (1.37)$$

$$T(\pi/4) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Un retardateur linéaire sépare l'État d'Orientation de Polarisation d'entrée en deux composants linéaires orthogonaux (lent et rapide) et introduit une certaine différence de phase φ(retard) entre eux. Que l'axe rapide du retardateur donné forme un angle θ avec l'axe x,



Axe rapide

Figure 1.10. Retardateur linéaire avec son axe rapide incliné à un angle θ par rapport à l'axe x.

L'État d'Orientation de Polarisation de sortie correspondant à un faisceau lumineux incident (Ex, Ey) peut être obtenu comme suit : nous obtenons d'abord les composants de l'État d'Orientation de Polarisation incident le long des axes rapides et lents($f\ et\ s$), qui sont donnés par,

$$\begin{pmatrix} E_f \\ E_s \end{pmatrix} = \begin{pmatrix} cos\,\theta & sin\,\theta \\ -sin\,\theta & cos\,\theta \end{pmatrix}\begin{pmatrix} E_x \\ E_y \end{pmatrix} \quad (1.38)$$

Ces composants en passant à travers le retardateur, le composant rapide est avancé en phase de φ et les composants correspondants à la sortie du retardateur sont alors donnés par,

$$E_f{}' = e^{i\varphi}E_f$$

$$E_s{}' = E_s \quad (1.39)$$

Donc,

$$\begin{pmatrix} E_f' \\ E_s' \end{pmatrix} = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} E_f \\ E_s \end{pmatrix} \tag{1.40}$$

Une fois que nous connaissons les composantes E_f' et E_s', les composantes le long des axes $\boldsymbol{x}$ et y à la sortie sont obtenues en tournant les axes de coordonnées dans le sens des aiguilles d'une montre d'un angle θ. Ces composantes sont données par,

$$\begin{pmatrix} E_x' \\ E_y' \end{pmatrix} = \begin{pmatrix} cos\,\theta & -sin\,\theta \\ sin\,\theta & cos\,\theta \end{pmatrix} \begin{pmatrix} E_f' \\ E_s' \end{pmatrix} \tag{1.41}$$

En utilisant les équations (1.38) et (1.39) dans l'équation (1.41), il est facile de montrer que les vecteurs Jones des faisceaux d'entrée et de sortie sont liés par la relation,

$$\begin{pmatrix} E_x' \\ E_y' \end{pmatrix} = T(\theta) \begin{pmatrix} E_x \\ E_y \end{pmatrix} \tag{1.42}$$

Où,

$$T(\theta) = \begin{pmatrix} cos\,\theta & -sin\,\theta \\ sin\,\theta & cos\,\theta \end{pmatrix} \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} cos\,\theta & sin\,\theta \\ -sin\,\theta & cos\,\theta \end{pmatrix}$$

$$= \begin{pmatrix} e^{i\varphi}\cos^2\theta\sin^2\theta & \left(e^{i\varphi}-1\right)\sin\theta\cos\theta \\ \left(e^{i\varphi}-1\right)\sin\theta\cos\theta & e^{i\varphi}\sin^2\theta+\cos^2\theta \end{pmatrix} \tag{1.43}$$

Cela représente la matrice de Jones d'un retardateur linéaire dont l'axe rapide forme un angle θ avec l'axe x. Les retardateurs linéaires les plus couramment utilisés sont la plaque demie d'onde (HWP) et la plaque quarte d'onde (QWP), dont les matrices de Jones peuvent être obtenues à partir de l'équation précédente en substituant $\varphi = \pi\ et\ \pi/2$, respectivement. Ainsi, les matrices de Jones pour une HWP ou une QWP dont l'axe rapide est orienté à un angle θ avec l'axe x sont données

HWP: $$T_{\mathrm{HWP}}(\theta) = \begin{pmatrix} -cos\,2\theta & -sin\,2\theta \\ -sin\,2\theta & cos\,2\theta \end{pmatrix} \quad (1.44)$$

QWP: $$T_{\mathrm{QWP}}(\theta) = \begin{pmatrix} i\ cos^2\theta\, sin^2\theta & (i-1)\,sin\,\theta\, cos\,\theta \\ (i-1)\,sin\,\theta\, cos\,\theta & i\ cos^2\theta\, sin^2\theta \end{pmatrix} \quad (1.45)$$

En outre, en substituant $\theta = 0\ et\ \pi/2$ dans l'équation (1.43), on obtient les matrices de Jones suivantes pour des retardateurs linéaires, avec l'axe rapide parallèle aux axes x et y,

$$T(0) = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & 1 \end{pmatrix} \quad et \quad T(\pi/2) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \quad (1.46)$$

En remplaçant $\varphi = \pi/2$ et π dans l'équation précédente, on obtient les matrices Jones correspondantes pour un QWP et un HWP, tels que donnés par,

$$T_{\mathrm{QWP}}(0) = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \quad ; \quad T_{\mathrm{QWP}}(0) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$T_{\mathrm{HWP}}(0) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \ ; \quad T_{\mathrm{HWP}}(0) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad (1.47)$$

1.5. Cristaux liquides

Les cristaux liquides sont des substances qui présentent à la fois des propriétés cristallines et des propriétés liquides. Ils sont en fait des composés moléculaires qui ont une structure ordonnée à l'échelle microscopique, mais qui peuvent se déformer et se déplacer comme un liquide.

1.5.1 Phases des cristaux liquides

Les phases des cristaux liquides sont différentes structures de molécules dans lesquelles les molécules d'un cristal liquide sont organisées et alignées d'une manière particulière. Il existe plusieurs phases différentes de cristaux liquides, chacune ayant des propriétés uniques, telles que la forme, la texture, la mobilité et la transparence des molécules. Les trois phases les plus connues sont [10].

- **Phase nématique**

La phase nématique du cristal liquide est la plus simple, dans laquelle les molécules sont alignées dans une direction moyenne, mais sans ordre plus strict.

- **Phase smectique**

La phase smectique est la phase plus complexe, dans laquelle les molécules sont alignées dans une direction moyenne et forment également des couches continues, ce qui leur permet de glisser les unes sur les autres.

- **Phase cholestérique**

Dans cette phase, les molécules forment une structure hélicoïdale. Ces différentes phases peuvent être obtenues en modifiant la température, la pression ou les conditions environnementales, ce qui peut entraîner une transition entre les phases.

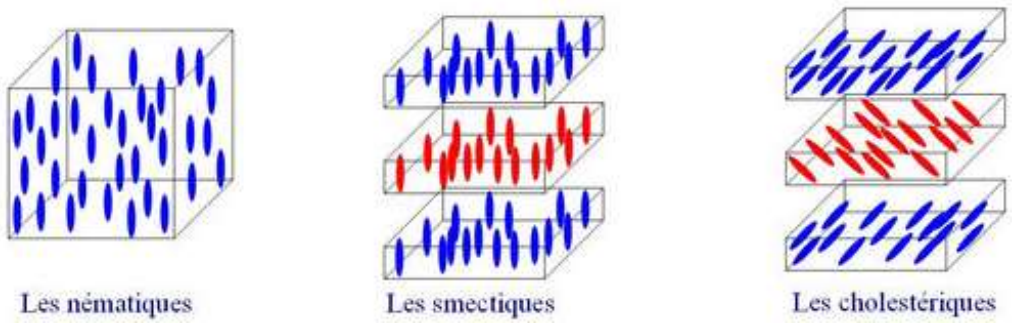


Figure 1.11. Arrangements moléculaires pour différents types de cristaux liquides. Quand il le faut, les couches ont été séparées pour plus de clarté [11].

1.6. Corrélateur de Vander-lugt (montage 4f)

Les méthodes de traitement par corrélation optique ont connu une évolution constante, ce qui a élargi leur champ d'application à des domaines de surveillance et d'identification, aussi bien militaires (reconnaissance d'avions, de bateaux, ...) que civils (reconnaissance de panneaux de signalisation routière, identification de personnes à des fins bancaires ou de sécurité telles que dans les aéroports, les métros, ...). La corrélation est ainsi devenue un outil de décision très puissant, principalement en raison de son caractère global et de sa robustesse au bruit. En effet, la corrélation est particulièrement adaptée à l'optique en raison de la transformée de Fourier, qui est le noyau de la corrélation et qui est naturelle en optique.

Les avancées dans le traitement de l'information par voie optique sont dues non seulement aux améliorations des qualités des lasers (faisceaux quasi-parallèles, haute puissance, cohérence et

monochromatisme), mais également à l'introduction de nouvelles interfaces optoélectroniques basées sur des cristaux liquides (SLM : modulateur spatial de lumière) et des matrices (CCD : dispositif à transfert de charge). La littérature décrit deux grandes familles de corrélateurs : le Corrélateur à transformée de Fourier conjointe JTC (Joint Transform Correlator) et le Corrélateur de Vander-Lugt. Ce dernier utilise un montage "4f", compare l'image cible avec une image de référence provenant d'une base d'apprentissage, et détecte simplement un pic de corrélation. Cette mesure évalue le degré de similitude entre l'image cible et l'image de référence

En 1964, Vander-Lugt a introduit le premier corrélateur optique basé sur l'analyse de Fourier. Ce corrélateur utilise deux transformations de Fourier successives, effectuées optiquement par le biais de deux lentilles convergentes tel que la lentille de Fourier est un dispositif optique utilisé en traitement d'image et en analyse de Fourier. Le schéma optique de base de ce corrélateur est montré sur la figure 1.12.

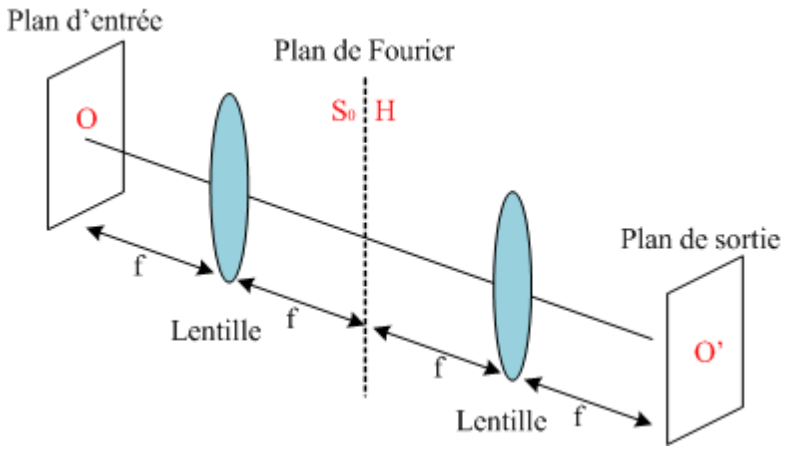


Figure 1.12. Corrélateur optique de Vander-Lugt (montage 4f) .

Dans le corrélateur optique, l'objet cible O est placé dans le plan d'entrée et éclairé par une onde plane monochromatique. Une lentille convergente forme la transformée de Fourier (TF) de l'objet cible, notée S0, dans son plan focal image (plan de Fourier ou plan spectral). Dans ce plan, un filtre de corrélation H est placé, qui est calculé en fonction du traitement souhaité. Ensuite, une deuxième lentille effectue une seconde TF dans le plan de sortie (plan de corrélation). Ce plan contient ou non un point lumineux, appelé pic de corrélation, dont l'intensité dépend du degré de ressemblance entre l'image cible et l'image utilisée pour fabriquer le filtre de corrélation.

Pour modifier la répartition spectrale de l'objet, on utilise le filtrage dans le plan de Fourier. Ensuite, la prise de décision se fait dans le plan de sortie, en utilisant le critère de performance PCE (Peak to Correlation Energy), qui représente le rapport de l'énergie du pic de corrélation à l'énergie totale du plan de corrélation

$$\text{PCE} = \frac{\text{l'énergie du pic de corrélation}}{\text{l'énergie totale du plan de corrélation}}$$

Le corrélateur de Vander-Lugt permet de corréler une image avec différents types de filtres, selon la figure 1.14. Les chercheurs ont proposé plusieurs formes de filtres pour améliorer la robustesse et la discrimination du corrélateur. Parmi ces filtres, on peut citer le filtre adapté, le filtre de phase pure (POF), le filtre composite et le filtre segmenté [12].

1.7. Modulateur spatial de lumière (SLM)

Un modulateur spatial de lumière est un appareil programmable électroniquement qui peut moduler la sortie de lumière sur la base d'un motif spatial fixe spécifique (pixel), projetant essentiellement de la lumière qui est contrôlée en amplitude uniquement, en phase uniquement ou les deux (amplitude de phase).

1.7.1. Catégories de SLM

Il ya deux catégories de SLM sont :

- SLM à adressage électrique (EASLM), qui sont utilisés si l'information est collectée par des composants optoélectroniques tels que des photodiodes, une caméra CCD ou une simulation numérique.
- SLM à adressage optique (OASLM), qui sont utilisés si l'information est sous forme optique, par exemple la sortie d'un moniteur vidéo ou la sortie d'un système d'imagerie quelconque [11].

1.7.2. Utilisations des SLM

A l'origine les modulateurs spatiaux de lumière ont été développés pour une utilisation dans des processeurs optiques tels que :

1. Convertir une image incohérente en image cohérente

2. Amplifier une faible image
3. Convertir les longueurs d'ondes (passer de l'I.R. dans le visible)
4. Modifier le filtre spatial utilisé dans le plan de Fourier (spectral)

1.7.3. Propriétés des NLC

En polissant les surfaces des couches d'alignement des cristaux liquides nématiques dans une direction donnée, il est possible de contrôler leur orientation en imposant des conditions aux limites. Les axes moléculaires en contact avec la surface ont tendance à s'aligner avec les petites rayures créées par le polissage. Pour assurer la continuité de l'alignement des axes, une torsion peut être appliquée à la cellule, comme illustré dans la figure 1.13(a). En appliquant un champ électrique, un dipôle électrique est induit dans chaque molécule, alignant ainsi le grand axe de la molécule (où le dipôle apparaît) avec le champ électrique, comme le montre la figure 1.13(b).

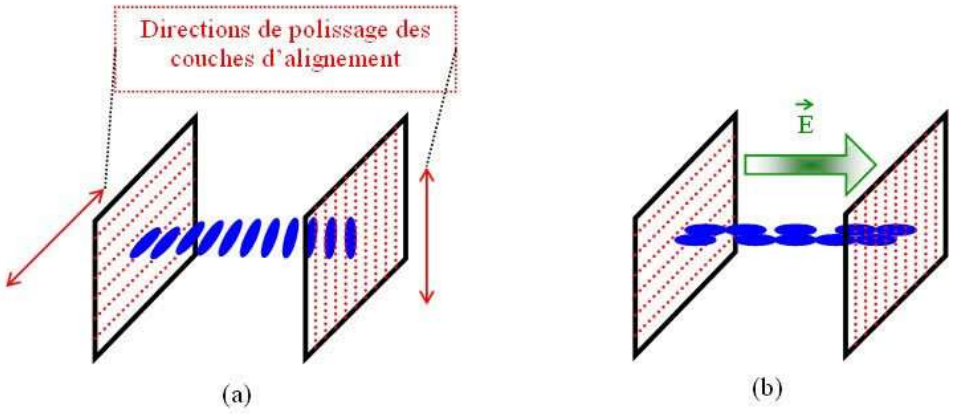


Figure 1.13. (a) Arrangements moléculaires dans une cellule à cristaux liquides lorsque les directions de polissages des couches d'alignement sont perpendiculaires. (b) Alignement des axes moléculaires avec le champ électrique.

1.7.4. Propriétés optiques des NLC

- Les molécules sont allongées ce qui provoque une anisotropie induisant une biréfringence importante. La variation d'indice est élevée ce qui permettra d'avoir des épaisseurs au niveau des cellules relativement faibles $\Delta n = n_e - n_0 = 0.2$ (n_e suivant l'axe de la molécule et n_0 perpendiculaire à l'axe)

- Si les molécules sont disposées de façon hélicoïdale (figure 1.13(a)) nous avons un pouvoir rotatoire important.

En combinant ces deux propriétés on peut réaliser des modulations d'intensité de la lumière

1.18. Conclusion

Ce chapitre avait pour objectif d'introduire quelques notions élémentaires sur le phénomène de polarisation de la lumière. Nous avons vu les différents éléments optiques nécessaires pour la conception de notre système de cryptage. Nous avons également présenté des différentes méthodes de représentation algébrique des états de polarisation tel que les formalismes de Jones et stocks. Nous avons terminé ce chapitre par une introduction au modulateur spatial de lumière qui est un élément incontournable dans le traitement optique de l'information.

Chapitre 2

Cryptage des images

2.1. Introduction

La cryptographie est l'art de protéger les informations sensibles en les transformant de manière à ce qu'elles ne soient compréhensibles que par les personnes autorisées. Elle est basée sur des algorithmes mathématiques sophistiqués qui permettent de chiffrer et de déchiffrer les messages de manière sécurisée. Le chiffrement est le processus de transformation du message original en un message chiffré, qui ne peut être compris sans une clé de déchiffrement, tandis que le déchiffrement permet de retrouver le message original à partir du message chiffré et de la clé de déchiffrement. La cryptographie est devenue essentielle dans notre monde numérique pour la protection de la vie privée et de la sécurité de l'information, ainsi que dans d'autres domaines tels que la sécurité informatique, la protection des logiciels, la vérification de l'identité et la preuve d'authenticité des documents numériques.

Ce chapitre, sera composé de deux parties : une étude de la cryptographie, en présentant ses objectifs et ses différentes méthodes de chiffrement, afin de décrire les notions de base et les différents types d'images numériques, ainsi que les techniques de chiffrement d'image.

2.2. Cryptographie

La cryptographie utilise des algorithmes mathématiques et des protocoles spécifiques pour chiffrer les données, c'est-à-dire les rendre illisibles, et pour déchiffrer les données chiffrées, afin de les rendre à nouveau compréhensibles. Elle implique l'utilisation de clés cryptographiques qui servent à contrôler l'accès et à protéger les informations.

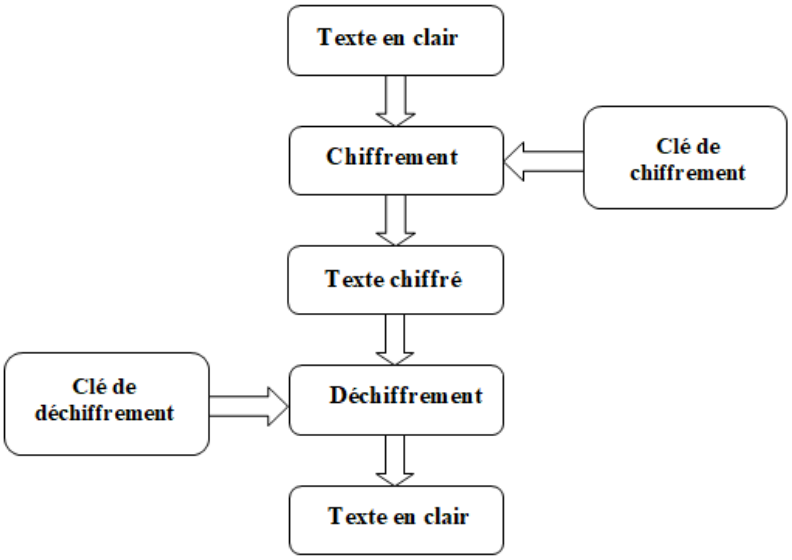


Figure.2.1. Shéma général de la cryptographie

Texte en clair : est le message à protéger (à chiffrer).

Texte chiffré : est le résultat du chiffrement du texte en clair.

Chiffrement : est une opération de transformation d'un message intelligible, appelé texte clair en un message incompréhensible ou inintelligible, appelé texte chiffré. Cette opération est effectuée à l'aide d'une clé de chiffrement, et si l'on ne dispose pas de la clé de déchiffrement appropriée, le texte chiffré demeure illisible (on parle alors de cryptographie)

Déchiffrement : est l'opération inverse du chiffrement, qui consiste à transformer un texte chiffré en un texte clair en utilisant une clé de déchiffrement appropriée. Cette opération permet de récupérer l'information initiale qui avait été protégée par le chiffrement. Le déchiffrement est une étape essentielle de la cryptographie, car il permet aux destinataires autorisés de lire le contenu d'un message crypté en utilisant la clé appropriée. Cependant, pour les attaquants non autorisés.

Clé : est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré (clé de chiffrement) et pour déchiffrer le texte chiffré en texte en clair (clé de déchiffrement). On peut parfaitement concevoir un algorithme qui n'utilise pas de clé, dans ce cas c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé [13].

2.2.1. Objectifs de la cryptographie

Le but fondamental de la cryptographie est de respecter adéquatement les objectifsmajeurs de la sécurité suivante :

- ✓ **Confidentialité :** Il s'agit de rendre la lecture du message inintelligible à des tiers non autorisés.
- ✓ **Authentification :** Il s'agit principalement de s'assurer que le correspondant connecté est bien le correspondant souhaité et de s'assurer du signataire de l'acte.
- ✓ **Intégrité :** Il s'agit de s'assurer que le message n'a pas été modifié durant latransmission.
- ✓ **Non répudiation :** l'expéditeur ne peut pas nier, ultérieurement, avoir envoyé lemessage. Cet aspect est sous-entendu dans l'authentification [14].

2.2.2. Différents types de cryptographie

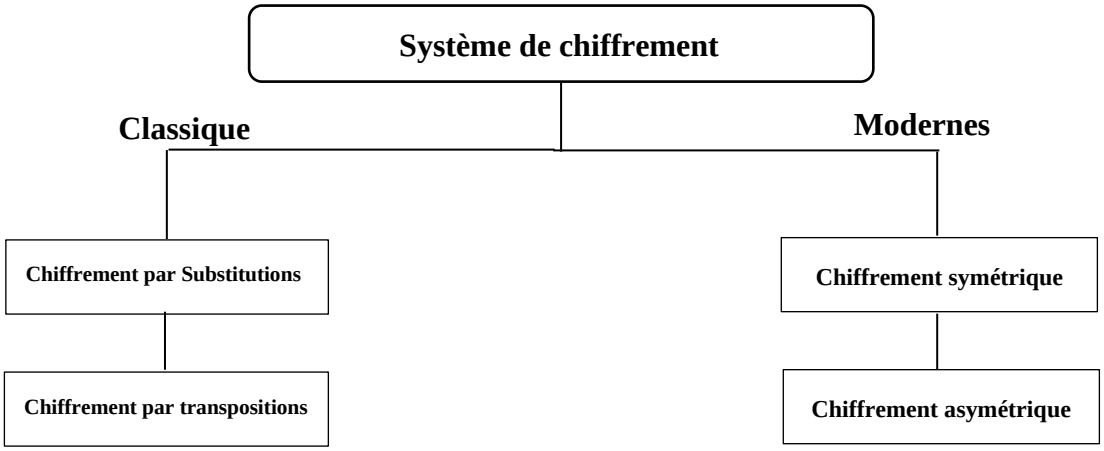


Figure.2.2. Principales techniques en cryptographie.

2.2.2.1. Cryptographie classique

Dans la cryptographie classique, la méthode et la clé de chiffrement ainsi que celle de déchiffrement sont connues par l'émetteur et le destinataire. La plupart des méthodes de chiffrements classiques reposent sur deux principes essentiels : la substitution et la transposition

(a) Le chiffrement par substitution

Le chiffrement par substitution consiste à remplacer dans un message une ou plusieurs entités par une ou plusieurs autres entités [15]. Il existe plusieurs types de systèmes de chiffrement par substitution qui peuvent être distingués.

- ✓ **Substitution mono-alphabétique**

  Est le plus simple à imaginer consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet. Comme le chiffrement par décalage.

- ✓ **Substitution poly alphabétique**

  Consiste à utiliser une suite de chiffres mono-alphabétique réutilisée périodiquement.

- ✓ **Substitution homophonique**

  Permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères.

- ✓ **Substitution de poly grammes**

  Consiste à substituer un groupe de caractères (poly gramme) dans le message par un autre groupe de caractères.

(b) Le chiffrement par transposition

Le chiffrement par transposition (ou le chiffrement par permutation) consiste à faire un réarrangement de l'ordre des lettres qui cache le sens initial. Cette méthode demande de découper le texte clair en blocs de taille identique, et applique la même permutation sur chacun des blocs.

2.2.2.2. Cryptographie moderne

La cryptographie moderne se caractérise par l'utilisation d'algorithmes de chiffrement sophistiqués qui offrent un haut niveau de sécurité dans la protection des données et des informations sensibles. Certaines des techniques de cryptographie moderne comprennent [10] :

(c) Chiffrement asymétrique (à clé publique)

Le chiffrement symétrique (aussi appelé chiffrement à clé publique) est un système de cryptographie qui utilise deux clés différentes pour chiffrer et déchiffrer des données. La clé publique est distribuée largement, tandis que la clé privée est gardée secrète par le propriétaire des données.

En utilisant cette méthode, les utilisateurs peuvent envoyer des données confidentielles en toute sécurité sans avoir besoin de partager leur clé privée. Le chiffrement à clé publique est utilisé dans de nombreux systèmes de sécurité en ligne, y compris la sécurisation des transactions financières et la protection des communications électroniques.

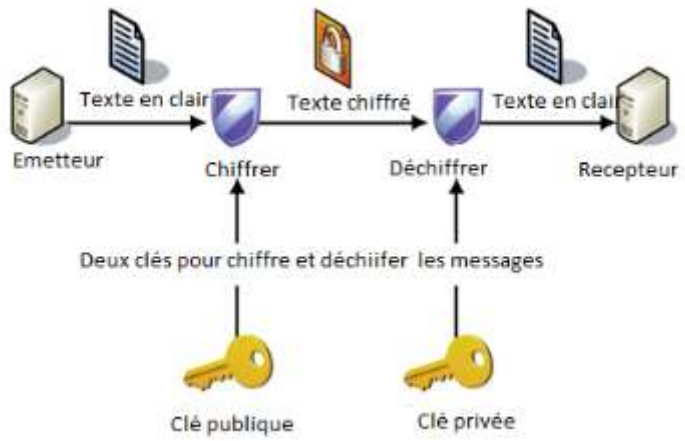


Figure.2.3. Chiffrement asymétrique.

✓ **Chiffrement symétrique (à clé secrète)**

Le chiffrement symétrique (aussi appelé chiffrement à clé privée ou chiffrement à clé Secrète) est un système de cryptographie qui utilise la même clé pour le chiffrement et le déchiffrement. Le chiffrement à clé secrète a des origines lointaines, et a toujours été associé

à des applications militaires. Les algorithmes les plus répandus sont : RC4 DES, AES, 3DES, etc…

Figure.2.4. Chiffrement symétrique

Il existe deux grandes familles de chiffrement dans cette classe :

✓ **Chiffrement par blocs**

Les messages sont découpés en blocs de taille à une relation avec la taille de clé (après le remplacement de chaque caractère par un code binaire), basé sur les deux catégories de chiffrement (par substitution et par transposition) et la combinaison entre eux, par exemple :

- DES : blocs de 64 bits, clés de 56 bits
- AES : blocs de 128 bits [16].

✓ **Chiffrement par flots**

Les données sont traitées en flux (traitement bit par bit), par exemple :

- RC4 : Chiffrement octet par octet

2.2.2.3. Comparaison entre le chiffrement symétrique et asymétrique

Le tableau ce dessus montre la comparaison entre le chiffrement symétrique et asymétrique :

Tableau.2.1. La comparaison entre le chiffrement symétrique et asymétrique [17].

	Chiffrement Symétrique	**Chiffrement Asymétrique**
Définition	Le chiffrement symétrique utilise une seule clé pour le cryptage et le déchiffrement.	Le chiffrement asymétrique utilise une clé différente pour le cryptage et le décryptage.
Performance	Le chiffrement symétrique est rapide en exécution.	Le chiffrement asymétrique est lent a l'exécution en raison de la charge de calcul élevée.
Algorithmes	AES ,DES,3DES et RC4.	Diffie-Hellman, RSA.
Objectif	Le chiffrement symétrique est utilisé pour la transmission de données en masse.	Le chiffrement asymétrique est souvent utilisé pour l'échange de clés secrètes.

2.2.2.4. Chiffrement hybride

Le chiffrement hybride (la combinaison entre le cryptage symétrique et asymétrique) d'un message se déroule en deux étapes :

- Dans un premier temps, l'émetteur choisit une clé symétrique K aléatoire. Il utilise en suite cette clé K pour chiffrer (symétriquement) le message
- Puis il chiffre (asymétriquement) la clé K avec la clé publique du destinataire. Il envoie à son destinataire le message chiffré et de K. Le destinataire déchiffre d'abord la clé K, puis l'utilise pour retrouver le message [15].

2.3. Cryptographie visuelle

La cryptographie visuelle est une branche de la cryptographie qui utilise des techniques d'encodage pour cacher des informations dans des images. Elle repose sur le principe que deux images peuvent être superposées pour créer une nouvelle image qui contient des informations cachées. Cette technique est souvent utilisée pour envoyer des messages secrets ou des images sensibles.

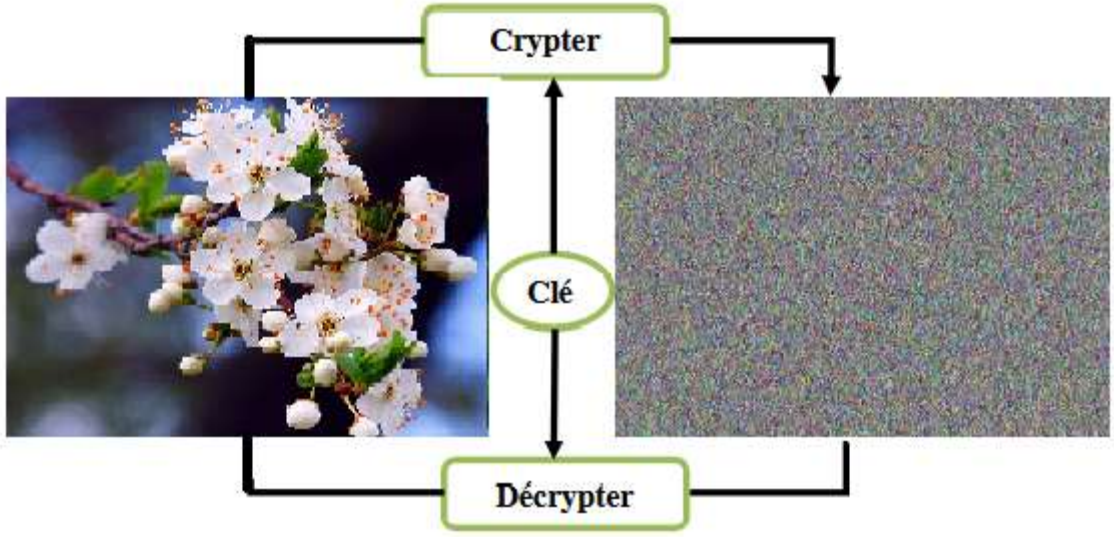


Figure 2.5. Cryptage d'image

2.3.1. Image numérique

L'image numérique tramée est formée d'un assemblage de pixels dont on doit comprendre les caractéristiques afin de bien saisir l'objet dans son ensemble. Cette présentation permettra de découvrir les concepts de base (pixel, bit, résolution, couleur, compression) et de comprendre comment ils influencent l'acquisition, l'archivage, le traitement et la diffusion des images numérisées ou créées en format numérique.

L’image numérique est caractérisée par les paramètres suivants :

- **Pixel**

Représente la plus petite unité d'une image numérique, les nombres des pixels de ligne et les nombres des colonnes déterminent la démentions de l’image, et chaque pixel représente valeur (couleur) [15].

- **Définition**

La définition est le nombre de pixels constituants l’image.

- **Résolution**

La résolution d’une image est définie par le nombre de pixels par unité de longueur dpi (dot per inch = point d’encre par pouce) pour une imprimante ou (ppp = pixels par pouce pour un fichier d’image).

- **Taille**

La taille de l’image est la place qu’elle occupe dans le codage binaire. Son unité est «l’octet» [16].

Taille = nombre d’octets pour chaque pixel × définition

2.3.2. Types d’image numérique

Il existe deux types d’images numériques :

2.3.2.1. Images matricielles

Sont des types d'images numériques qui sont composées d'une matrice de pixels, chacun ayant une valeur de couleur et de luminosité. Les images matricielles sont créées en utilisant des appareils tels que des scanners, des caméras numériques ou des caméras de surveillance qui capturent une image en la divisant en une grille de pixels, Elles peuvent être stockées dans différents formats tels que JPEG, PNG, BMP, TIFF, etc

2.3.2.2. Images vectorielles

Sont un type d'images numériques qui sont composées de vecteurs, tels que des lignes, des courbes et des formes géométriques, plutôt que de pixels. Les images vectorielles sont créées à l'aide de logiciels de dessin vectoriel qui utilisent des formules mathématiques pour créer des objets graphiques, Les formats de fichiers courants pour les images vectorielles incluent SVG, AI, PDF et EPS

2.3.3. Formats standards d'image

✓ **BMP (Windows Bitmap)**

C'est le format actuel utilisé par Windows. Il produit des images de bonne qualité et est reconnu par de nombreuses applications. C'est le format le plus utilisé, par contre, il est extrêmement volumineux lorsqu' il utilise le codage en « truecolors ».

✓ **PCX (PiCture eXchange)**

Le format défini par Paint rush. Il accepte les modes de couleur, indexés, niveaux de gris et le noir et blanc

✓ **GIF (Graphic Interchange Format)**

Créé par Compuserve, utilise aussi le codage RGB, mais le format GIF n'utilise pas toutes les 16 millions de couleurs. Il prend les 256 couleurs les plus courantes pour réaliser l'image au format GIF. Cela permet une bonne compression et un affichage rapide de l'image

✓ **JPG ou JPEG (Joint Photographique Experts Group)**

Créé par un consortium industriel, ce format très utilisé sur Internet, permet d'afficher les images en mode 16 millions de couleurs. Il est conçu pour réduire le plus possible la taille des fichiers graphiques en acceptant éventuellement de légères pertes de qualité. Il est destiné à la transmission rapide d'information. Ces résultats de compression sont extraordinaires.

✓ **TIFF (Tag Image File Format)**

C'est un format d'excellente qualité, mais qui présente des problèmes de compatibilité du fait d'une multiplicité de version. Il existe aussi une version compressée qui fournit des fichiers très compacts sans perte notoire de qualité. Ce format est compatible avec d'autres plates-formes (macintosh). Il est utilisé par les professionnels [18].

2.3.4. Techniques de cryptage d'image

Les techniques de bases pour un système de cryptage d'image peuvent être classées en deux catégories principales : la confusion et la diffusion.

- **Confusion**

La confusion consiste à rendre le lien entre les pixels de l'image clair d'origine et l'image cryptée complexe et difficile à déchiffrer. Cela se fait généralement en utilisant des opérations mathématiques complexes, telles que des substitutions non linéaires (par exemple, des tables de substitution) ou des transformations polynomiales. L'objectif est de rendre la relation entre l'image claire et l'image chiffrée aussi aléatoire que possible.

- **Diffusion**

La diffusion consiste à répartir les informations de l'image claire sur l'ensemble de l'image chiffrée. L'idée est de garantir que chaque pixel de l'image chiffrée dépende de plusieurs pixels de l'image claire. Cela rend plus difficile l'analyse statistique et l'extraction d'informations à partir de l'image chiffrée. Les techniques de diffusion sont souvent basées sur des opérations telles que le mélange des pixels, les permutations, les rotations ou les transpositions.

2.3.5. Classification des crypto-systèmes d'image

Les crypto-systèmes d'image peuvent être classés selon les techniques de chiffrement appliqué en deux grandes familles [19] :

2.3.5.1. Crypto-systèmes d'image par bloc

Dans cette technique consiste à découper l'image en blocs de taille généralement fixe. Les blocs sont ensuite chiffrés les uns après les autres au moyen de la clé et d'un mode opératoire.

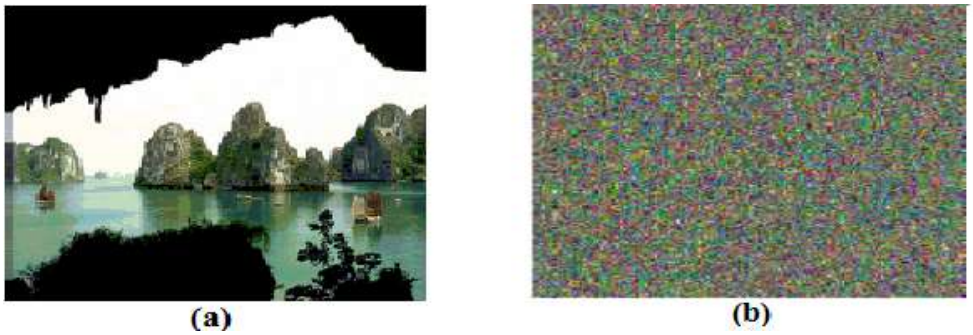


Figure 2.6. a) Image originale, b) Image cryptée avec un algorithme de chiffrement par bloc

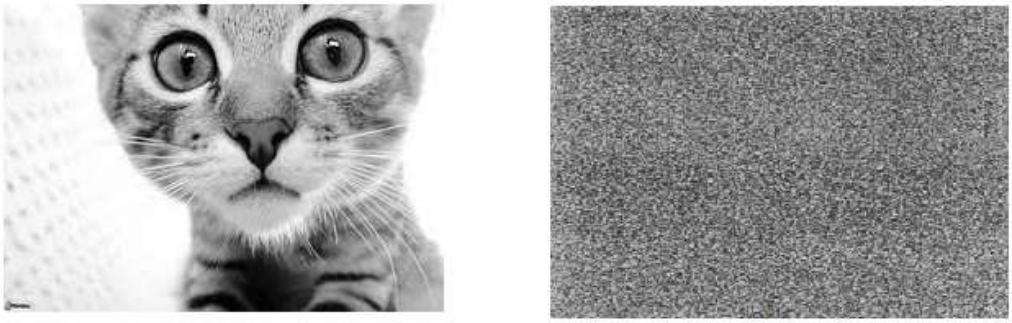
- **Cryptage d'image en utilisant une technique de permutation**

Cette technique consiste à faire un réarrangement des bits en fonction de la clé entrée, et l'algorithme utilisé.

Figure 2.7. (a) image originale, (b) image cryptée Les résultats de la technique de permutation

2.3.5.2. Crypto-systèmes d'image par flux

Un chiffrement d'image par flux traite les images de taille quelconque sans avoir besoin de les découper. Il se présente souvent sous la forme d'un générateur de nombres pseudo aléatoires avec lequel on opère un XOR (exclusive OR) entre un bit à la sortie du générateur et un bit provenant de l'image.



(a) (b)

Figure 2.8. a) Image originale, b) Image cryptée avec un algorithme de chiffrement par flux

2.4. Critères d'évaluation

2.4.1. Histogramme

L'histogramme est la représentation graphique de la proportion de pixels d'une image par gamme de luminosité. L'axe horizontal représente toutes les valeurs de niveau de gris possibles pour un pixel, dans l'ordre croissant, c'est-à-dire de 0 à 255 pour une image en 8 bits et l'axe vertical indique le nombre de pixels ayant la valeur considérée.

Pour des algorithmes de cryptage d'images, l'histogramme de l'image cryptée devrait avoir deux propriétés :

- ✓ Il doit être totalement différent de l'histogramme de l'image originale.
- ✓ Il doit avoir une distribution totalement aléatoire [20].

2.4.2. Entropie

L'entropie indique le niveau d'incertitude dans système de communication. L'entropie H (x) de toute donnée peut être calculée comme :

$$H(m)=\sum_{i=0}^{2^{n-1}} P(m)_i log_2 \frac{1}{P(m_i)} \quad (1.48)$$

La valeur de l'entropie doit être très proche de 8, Parce que si l'entropie est inférieure à 8, il existe des degrés de prévisibilité, Pour l'image cryptée avec 256 symboles, donc on ne peut pas assurer la sécurité contre l'attaque par entropie [15].

2.4.3. Corrélation

La corrélation est une mesure statistique qui exprime la notion de liaison linéaire entre deux variables (ce qui veut dire qu'elles évoluent ensemble à une vitesse constante). C'est un outil courant permettant de décrire des relations simples sans s'occuper de la cause et de l'effet.

Les pixels adjacents dans une image claire sont fortement corrélés, mais dans une image cryptée par un algorithme de cryptage optimal, ces derniers deviennent faiblement corrélés. Le calcul du coefficient de corrélation entre les pixels adjacents nous donne une idée sur la capacité de notre algorithme de cryptage à résister aux attaques.

Le coefficient de corrélation est défini par la formule suivante [15],

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

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

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i)$$

$$cov(x,y) = \frac{1}{N} = \sum_{i=1}^{N}(x_i - E(x)(y_i - E(y)) \qquad (1.49)$$

Tel que :

r_{xy} : la corrélation.

$cov(x,y)$: la covariance.

$E(x)$: l'espérance mathématique.

$D(x)$: la variance.

x, y : les valeurs des pixels des images.

2.5. Conclusion

Dans ce chapitre, nous avons fait une étude sur les notions fondamentales de la cryptographie et de l'image. En premier lieu, nous avons donné quel est l'objet de la cryptographie et Principaux concepts cryptographiques, Puis nous avons cité les différents types de cryptage et il est important de comprendre les caractéristiques de base d'image et cryptographie pour protéger et sécurisé efficacement dès l'information.

Enfin. Nous avons examiné les différentes propriétés des images numériques, les formats connus les plus célèbres et leurs caractéristiques.

Chapitre 3

Algorithmes de cryptage

3.1. Introduction

Dans ce chapitre nous examinerons de plus près ces deux méthodes de DRPE de JAVIDI et TDPES de CHACHOUA, en explorant les principes fondamentaux sur lesquels elles reposent, et nous mettrons également en évidence les résultats prometteurs obtenus.

3.2. Classification des algorithmes de cryptage selon le domaine de cryptage

Il est possible de catégoriser les algorithmes de cryptage de diverses manières : en fonction des clés utilisées, de la structure du cryptage ou encore du domaine de cryptage. Dans la suite, nous nous concentrons sur la catégorisation des algorithmes de cryptage en fonction de leur domaine d'application.

3.2.1. Cryptage d’images dans le domaine spatial

Dans son article publié en 1949 sur la théorie de la communication des systèmes de sécurité de base, Claude Shannon a introduit deux propriétés fondamentales en cryptographie : la confusion et la diffusion. Lors de la conception d'un algorithme de cryptage, prendre en compte ces deux propriétés garantit la complexité de la relation entre l'image chiffrée et l'image en clair, ce qui rend l'algorithme résistant aux attaques. Pour atteindre cet objectif, des techniques de substitution et de permutation sont utilisées.

Dans la littérature sur le cryptage d'images dans le domaine spatial, plusieurs algorithmes ont été développés selon l'architecture appelée permutation-diffusion, comme illustré dans la Figure 3.1 Cette architecture comprend deux opérations essentielles : la permutation et la diffusion, ainsi que leur combinaison éventuelle. Lors de la phase de permutation, les pixels de l'image en clair subissent une permutation de leurs positions sans altérer leurs valeurs. Ensuite, lors de la phase de diffusion, les pixels de l'image permutée subissent une modification de leurs valeurs tout en conservant leurs positions, en utilisant l'opérateur XOR qui présente une excellente propriété de récupération de données lors du processus de décryptage.

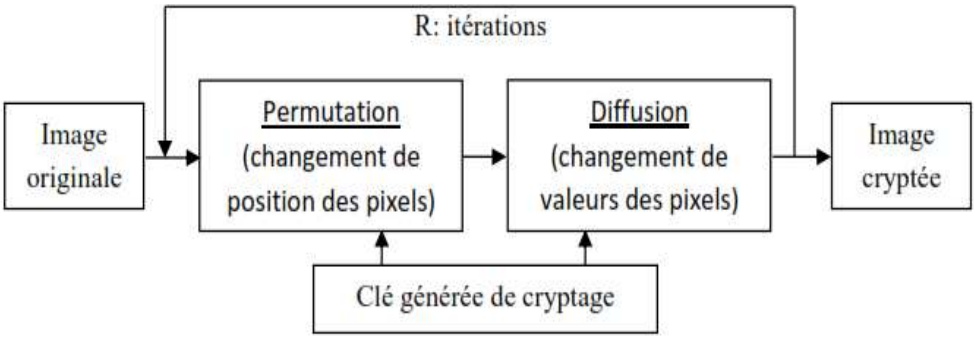


Figure 3.1. Architecture de Permutation-Diffusion [21].

3.2.2. Cryptage d'images dans le domaine fréquentiel basé sur les transformées discrètes

Le cryptage d'images dans le domaine fréquentiel est réalisé en transformant l'image à crypter dans le domaine fréquentiel à l'aide de transformées discrètes telles que la transformée en cosinus discrète (DCT) et la transformée en ondelettes discrètes (DWT) . C'est dans ce domaine que les modifications nécessaires sont effectuées selon l'algorithme de chiffrement proposé pour brouiller l'image à chiffrer, puis l'image est ramenée dans le domaine spatial. Malgré les contributions et les recherches portant sur l'utilisation de la DCT et de la DWT, la transformée de Fourier (DFT) reste la plus couramment utilisée, en particulier dans le domaine optique. En effet, la technologie de l'information optique offre des possibilités de traitement parallèle des données à grande vitesse. De plus, la sécurité de l'information dans le domaine optique a reçu une attention particulière ces dernières années, et le chiffrement d'images basé sur la transformée de Fourier (TF) peut être facilement implémenté dans ce domaine. La technique de chiffrement (DRPE) est un schéma de chiffrement optique classique qui utilise deux masques de phase aléatoires statistiquement indépendants. Le premier masque est appliqué dans le domaine spatial pour brouiller l'image, tandis que le second est utilisé dans le domaine de la transformée de Fourier.

3.2.2.1. Méthode DRPE de BAHRAM JAVIDI

Philippe REFREGIER et BAHRAM JAVIDI ont été les pionniers et les concepteurs de la méthode de chiffrement d'images DRPE dans le domaine optique [22]. En 1995, ils ont proposé

une technique de chiffrement d'images basée sur la transformée de Fourier, qui transforme l'image originale à chiffrer en un bruit blanc stationnaire d'amplitude complexe.

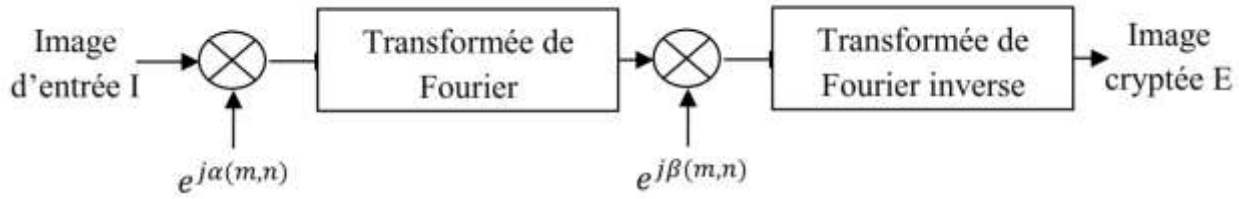


Figure 3.2. Schéma synoptique de cryptage DRPE

Le schéma de cryptage de la figure 3.2. a bien illustré la technique proposé et qui consiste à : (1) multiplier l'image d'entrée par le premier masque de phase aléatoire dans le domaine spatial, (2) transformer le résultat obtenu à partir de (1) en utilisant la transformer de Fourier, (3) multipliant le résultat obtenu de (2) par un autre masque de phase aléatoire dans le domaine fréquentiel, et enfin (4) transformant le résultat obtenu de (3) en utilisant la transformée de Fourier inverse pour obtenir l'image cryptée. Le deuxième masque a la même taille de l'image d'entrée et qui représente la véritable clé de cryptage.

Le schéma de décryptage est présenté dans la Figure 3.3, qui consiste à prendre l'image cryptée conjuguée, puis il suit exactement le chemin inverse du schéma de cryptage.

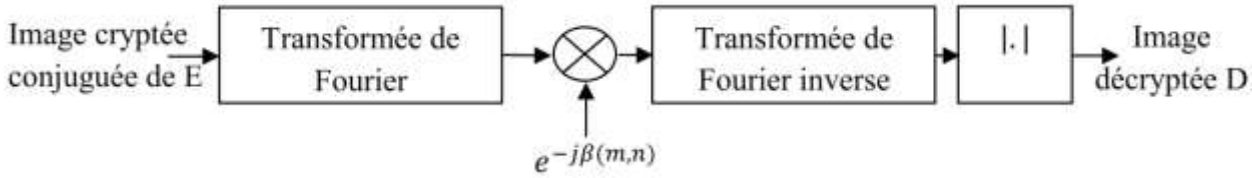


Figure 3.3. Schéma synoptique de décryptage DRPE

Également que notre méthode peut surmonter les problèmes de la méthode classique de filtrage inverse dans le domaine de Fourier, qui conduit à une faible efficacité optique.

3.3. Méthode de CHACHOUA

Cette méthode repose sur le formalisme de Mueller-Stokes et offre une approche intéressante pour la transmission sécurisée d'images optiques en utilisant la notion de la polarisation. pour encoder des informations dans un signal optique. Le principe de cet algorithme consiste à utiliser

les paramètres de Stokes pour caractériser et manipuler la polarisation de la lumière. Les paramètres de Stokes sont des quantités mesurables qui décrivent complètement l'état de polarisation d'un signal optique. Un aspect important abordé ici est la robustesse de cet algorithme contre le décryptage non autorisé. En d'autres termes, cette méthode a été testée contre les tentatives de décryptage non autorisées. Les résultats de ces tests ont démontré la fiabilité de l'algorithme, renforçant ainsi son utilité pour la transmission sécurisée d'images optiques.

3.3.1. Structure de système de cryptage de CHACHOUA

La figure 3.4 représente la configuration du T-DPES (Transmission-based Dual-stage Polarization Encryption System), qui comprend une source qui éclaire trois images : l'image cible d'entrée I_i, l'image clé I_k et l'image blanche I_w. Chacune de ces trois images passe à travers un polariseur correspondant avec un axe de transmission orienté à l'angle ψ. Étant donné que les trois signaux obtenus sont polarisés à l'angle ψ, ils peuvent être additionnés à l'aide du combineur de faisceau, ce qui donne une image I'_r qui représente le premier niveau de chiffrement. Pour des raisons de simplicité, nous supposerons par la suite ψ = 0. L'image I'_r passe ensuite à travers le polariseur pixelisé avec des angles de polarisation adaptés, ce qui représente le deuxième niveau de chiffrement pour obtenir une image crypté en sortie.

3.3.2. Algorithme de cryptage

Commençant par la définitions des éléments optiques. La matrice de Mueller du polariseur linéaire est définie par,

$$\boldsymbol{M_{pol}}(\psi) = \frac{1}{2}\begin{pmatrix} 1 & \cos(2\psi) & \sin(2\psi) & 0 \\ \cos(2\psi) & \cos^2(2\psi) & \cos(2\varphi)\sin(2\psi) & 0 \\ \sin(2\psi) & \cos(2\varphi)\sin(2\psi) & \sin^2(2\psi) & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{3.1}$$

avec, ψ l'angle de rotation du polariseur par rapport à l'axe du laboratoire (Ox ou Oy). La matrice de la lame biréfringente peut s'écrire,

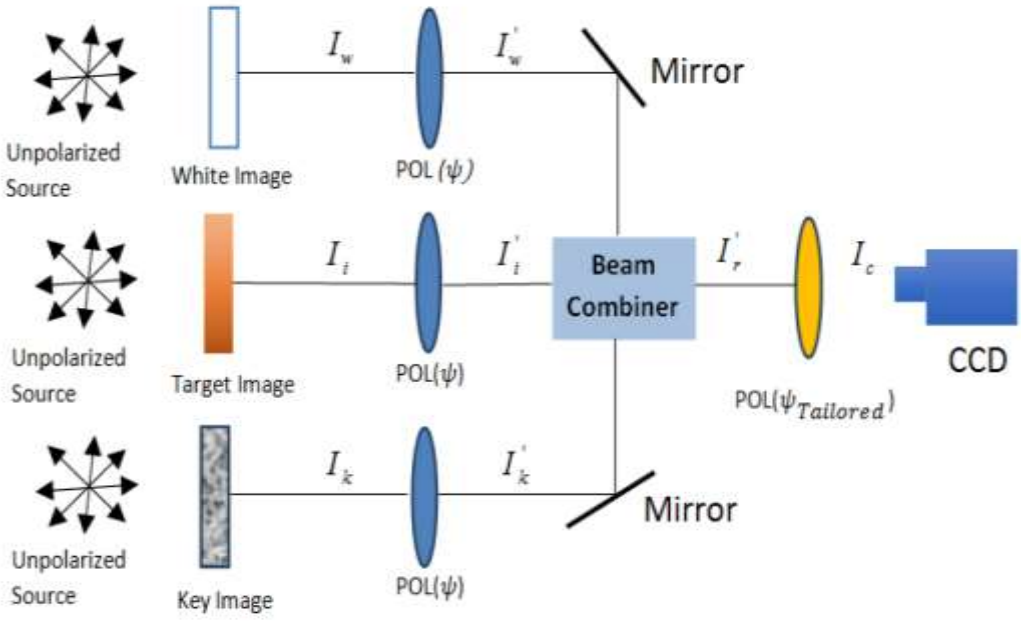


Figure 3.4. Système de cryptage de CHACHOUA [23].

Le signal d'entrée partiellement polarisé est représenté par un vecteur de Stokes, $I = (I_{i0}, I_{i1}, I_{i2}, I_{i3})^T$, qui est incident sur l'image à crypter, représentant l'image cible sur la figure 3.3. L'état de polarisation est déterminé par la configuration des éléments de polarisation. Le vecteur de Stokes de sortie $I_i^{'}$, est obtenu en multipliant la matrice de Mueller-Stokes, $\boldsymbol{M_{pol}}(\psi)$ par le vecteur d'entrée I_I comme suit,

$$I_i^{'} = \boldsymbol{M_{pol}}(\psi).\ I_i \qquad (3.2)$$

De manière similaire, deux signaux, représentés par les vecteurs de Stokes $I_K = (I_{K0},\ I_{k1},\ I_{k2},\ I_{k3})^T$ et $I_w = (I_{w0},\ I_{w1},\ I_{w2},\ I_{w3})^T$ sont envoyés vers une image clé k et une image blanche respectivement (Cf. Figure 3.3). Ces signaux passent également à travers les polariseurs, les signaux de sortie représentant sont donnés par $I_k^{'}$ et $I_w^{'}$ respectivement.

On considère la situation la plus simple des signaux non polarisés, ce qui signifie que seules les composantes I_{i0}, I_{k0} et I_{w0} sont non nulles dans les vecteurs de Stokes I_i, I_k et I_w respectivement. d'autre part, nous fixons les angles de polarisation tels que, $\psi 1 = \psi 2 = \psi 3 = \psi = 0$. En manipulant l'équation (3.2) on obtient,

$$I'_i = (I'_{i0} I'_{i1} I'_{i2} I'_{i3})^T = \frac{1}{2}(I_{i0}\ I_{i0}\ 0\ 0)^T \qquad (3.3)$$

$$I'_w = (I'_{w0}I'_{w1}I'_{w2}I'_{w3})^T = \frac{1}{2}(I_{w0}\ I_{w0}\ 0\ 0)^T \quad (3.4)$$

$$I'_k = (I'_{k0}I'_{k1}I'_{k2}I'_{k3})^T = \frac{1}{2}(I_{k0}I_{k0}\ 0\ 0)^T \quad (3.5)$$

Ensuite, les trois signaux sont multiplexés à l'aide d'un combineur de faisceau, comme illustré dans la Figure 3.4. Le signal résultant, I'_R, est donné par la formule,

$$I'_R = I'_i + I'_w + I'_k = 1/2(I_{i0} + I_{k0} + I_{w0} \quad I_{i0} + I_{k0} + I_{w0}\ 0\ \ 0)^T \quad (3.6)$$

Après le combineur de faisceau, l'image cryptée par l'image clé a une valeur d'intensité minimale égale à 255.

$$\min(I'_R) = \min(I'_w) + \min(I'_k) + \min(I'_i) = 255 + 0 + 0 \quad (3.7)$$

Afin d'avoir une intensité uniformément distribuée à la sortie I_{c0}, quelle que soit l'image cible d'entrée, nous devons calculer les angles Ψ_{Tailored}. L'intensité uniformément distribuée I_{c0} est donnée par,

$$I_{c0}(i,j) = \frac{1}{4}\left(1 + \cos(2\,\Psi^{ij}_{\text{Tailored}})\right)[I_{i0} + I_{k0} + I_{w0}] \quad (3.8)$$

Il est intéressant de noter que I_{w0} est utilisé comme image d'amplification pour garantir, selon l'équation (3.8), que les angles adaptés Ψ_{Tailored} ont toujours des valeurs réelles pour n'importe quelle image cible d'entrée et n'importe quelle image clé. Les angles adaptés Ψ_{Tailored} sont trouvés être,

$$\Psi_{\text{Tailored}} = 0.5 * arcos\left(\frac{4*I_{c0}}{(I_{i0}+I_{k0}+I_{w0})} - 1\right) \quad (3.9)$$

Les valeurs des angles adaptés Ψ_{Tailored} doivent être choisies dans la plage de 0 à π pour le processus de cryptage. La caméra CCD ne capture que I_{c0}, mais même si un attaquant capture l'un des trois autres paramètres de Stokes restants, I_{c1}, I_{c2} et I_{c3}, il ne pourra pas récupérer l'image d'origine.

3.3.2 Algorithme de Décryptage

Le processus de décryptage de T-DPES peut être réalisé à la fois de manière optique ou numérique. L'implémentation numérique est limitée aux images de petite taille, tandis que le déchiffrement optique est utilisé pour déchiffrer des images de grande taille.

Pour la configuration de décryptage optique, nous utilisons, une configuration entièrement optique basée sur la modulation de cohérence (Cf. Fig.3.5). La configuration comprend un polariseur suivi d'un polariseur pixélisé afin d'éliminer l'effet du polariseur pixélisé de cryptage. L'image résultante alimente un premier modulateur électro-optique, l'image clé alimente un deuxième modulateur électro-optique et l'image cible d'entrée est récupérée en utilisant la technique de modulation de cohérence à la sortie de l'interféromètre.

Dans le processus de décryptage utilisant le formalisme de Mueller-Stokes, seul le premier paramètre de Stokes I_{c0} est utilisé. Le vecteur de Stokes de l'image cryptée I_c est ensuite donné par,

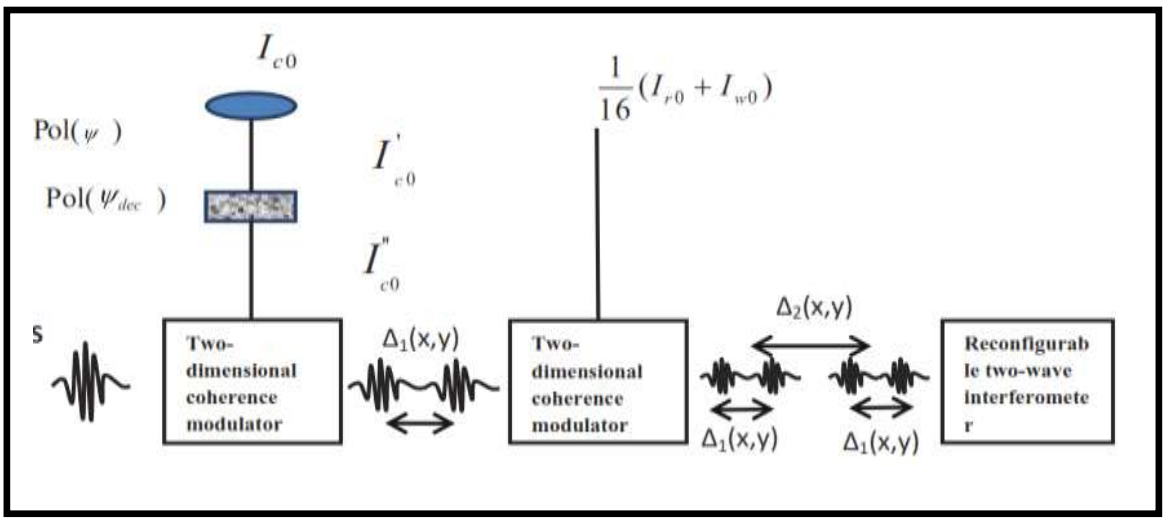


Figure 3.5. Décryptage par modulation de cohérence

$$I_c(i,j) = (I_{c0}(i,j),\ 0,\ 0,\ 0)^T \tag{3.10}$$

Selon la Figure 3.4, et après avoir traversé le premier polariseur, I'_c peut s'écrire,

$$I_c'(i,j) = \begin{pmatrix} \frac{1}{2} * I_{c0} \\ \frac{1}{2} * I_{c0} \\ 0 \\ 0 \end{pmatrix} \tag{3.11}$$

Ce faisceau lumineux est polarisé linéairement avec un angle ψ et passe à travers le polariseur pixélisé pour obtenir $I_c^{''}$. Le polariseur pixélisé a des angles Ψ_{dec}^{ij}. Ces angles sont calculés de manière à inverser l'effet du polariseur pixélisé utilisé dans le processus de chiffrement. L'intensité de l'image après le polariseur pixélisé est alors écrite comme suit,

$$I_c'' = \frac{1}{4} * I_{c0} * \left(\cos(2 * \Psi_{\text{dec}}^{ij}\right) + 1) \tag{3.12}$$

Selon l'équation (3.11), I_c'' peut être écrit comme suit,

$$I_{c0}'' = \frac{1}{16} * (I_{i0} + I_{k0} + I_{w0} * \left(\cos(2 * \psi_{dec}\right) + 1)\left(\cos(2 * \psi_{tailored}\right) + 1) \tag{3.13}$$

Le but, comme mentionné précédemment, est d'inverser l'effet du polariseur pixélisé de cryptage. Ainsi, en se référant à l'équation (3.8), la condition pour ψ_{dec} est la suivante,

$$(\cos(2 * \psi_{\text{dec}}) + 1)(\cos(2 * \psi_{\text{tailored}}) + 1) = 1 \tag{3.14}$$

Par conséquent, ψ_{dec} peut être écrit comme suit,

$$\psi_{dec} = 0.5 * arcos\left(\frac{1}{(\cos(2 * \psi_{tailored}) + 1)} - 1\right) \tag{3.15}$$

Les angles ψ_{dec} choisis lors du processus de chiffrement doivent être pris dans la plage $[0, \pi] - \{\pi/2\}$. Après le polariseur pixélisé du processus de décryptage, l'intensité doit être égale à,

$$I_{c0}'' = \frac{1}{16} * (I_{i0} + I_{k0} + I_{w0}) \tag{3.16}$$

Pour récupérer l'image cible I_{i0}, nous effectuons la modulation de cohérence comme illustré dans la Figure 3.4. L'image I_{c0}'', l'image clé I_{k0} ainsi que I_{w0} sont encodées par le Modulateur de

Cohérence (CM) composé d'une lame biréfringente (Q) et d'un Modulateur de Lumière Spatiale (SLM) qui permet d'encoder chaque pixel de l'image I''_{c0}, et de l'image clé I_{k0} et I_{w0} en tant que retard de chemin optique (OPD) donné respectivement par,

$$\Delta_1 = \Delta_{01} + K * \frac{1}{16} * I''_{c0}(x,y) \qquad \Delta_2 = \Delta_{02} + K * \frac{1}{16} * \left(I_{k0}(x,y) + I_{w0}(x,y)\right) \tag{3.17}$$

où Δ_{0i} est le retard de chemin optique introduit par les plaques biréfringentes Qi dans chaque CM, où i = 1, 2 et K est le constant du CM. Une source cohérente S est utilisée pour illuminer les deux CM. Cette source a une longueur de cohérence L_c donnée par,

$$L_c = \frac{{\lambda_0}^2}{\Delta\lambda} \tag{3.18}$$

où λ_0 est la longueur d'onde centrale et $\Delta\lambda$ est la largeur spectrale de la source. Il convient de noter que les OPDs des deux CMs sont supérieurs à la longueur de cohérence de la source. Le choix de la modulation de cohérence est fait pour renforcer davantage la configuration de décryptage. En effet, même si un attaquant avait accès à la configuration lors de la réalisation du processus de décryptage, il ne serait pas en mesure de récupérer l'image décryptée car l'image cible d'entrée est cachée dans le retard de chemin optique Δ_1 du Modulateur de Cohérence 1. L'intensité I_{out} calculée après le deuxième Modulateur de Cohérence est donnée par,

$$\begin{aligned} I_{out}(d,x,y) = {} & \frac{I_0}{2} + \frac{I_0}{2}\Gamma(d) + \frac{I_0}{4}\Gamma(d-\Delta_1) + \frac{I_0}{4}\Gamma(d+\Delta_1) + \frac{I_0}{4}\Gamma(d+\Delta_2) \\ & + \tfrac{I_0}{4}\Gamma(d-\Delta_2) + \tfrac{I_0}{8}\Gamma(d-(\Delta_1-\Delta_2) + \tfrac{I_0}{8}\Gamma(d+(\Delta_1-\Delta_2) \\ & + \tfrac{I_0}{8}\Gamma(d-(\Delta_1+\Delta_2) + \tfrac{I_0}{8}\Gamma(d+(\Delta_1+\Delta_2) \end{aligned} \tag{3.19}$$

où d est la différence de chemin optique variable introduite par l'interféromètre à deux ondes et Γ est la fonction de covariance de la source. L'expression de l'intensité à la sortie de l'interféromètre donnée dans l'équation (3.20). Comme le montre la Figure 7, les franges situées

le long de l'axe d sont directement liés aux retards optiques Δ_1 et Δ_2. Introduits par les CMs, et donc à l'image I''_{c0} et $I_{k0} + I_{w0}$. L'objectif est de calculer la soustraction de I''_{c0} et $I_{k0} + I_{w0}$ pour

extraire l'image cible d'entrée I_{i0}. Il est évident, selon l'équation (23), que cette soustraction est effectuée en utilisant la frange située à $\Delta_1 - \Delta_2$. Ainsi, selon l'équation (23), l'intensité décryptée I_{dec} et donc l'image cible d'entrée I_{i0} est donnée par,

$$I_{dec}(x, y) = \frac{1}{16} * (I''_{c0} - (I_{k0} + I_{w0}) = I_{i0}) \quad (3.20)$$

3.4. Résultats de simulation

L'efficacité du processus de cryptage est évaluée à l'aide de métriques d'évaluation pour les deux méthodes présentées précédemment, dans la partie de cryptage, nous nous intéressons à l'analyse d'histogramme qui permet d'examiner la répartition des valeurs des pixels dans l'image chiffrée, à titre d'exemple nous avant choisi l'image Lina de 256*256 (Cf. Figure 3.6).

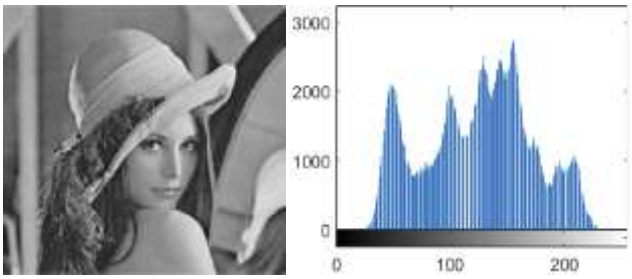
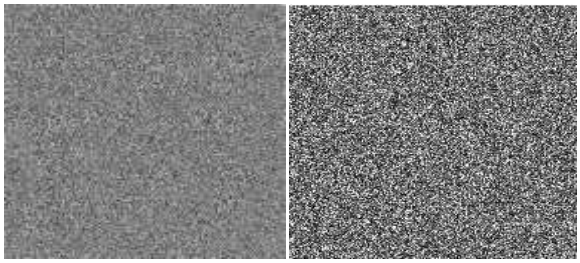


Figure 3.6. Image à crypter.

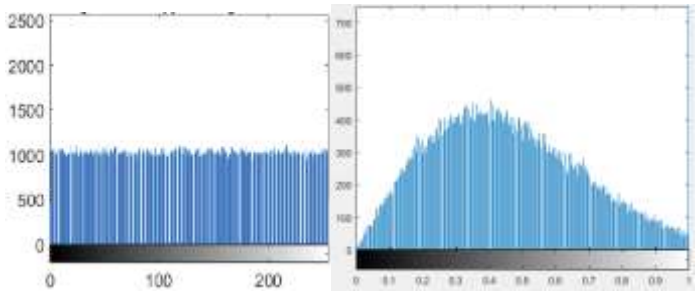
Le résultat de cryptage pour les deux méthodes est montré sur la figure 3.7,



(a) (b)

Figure 3.7. Images cryptées, (a) Méthode de CHACHOUA (b) Méthode de JAVIDI

l'histogramme des images cryptés est illustré sur la figure 3.8.

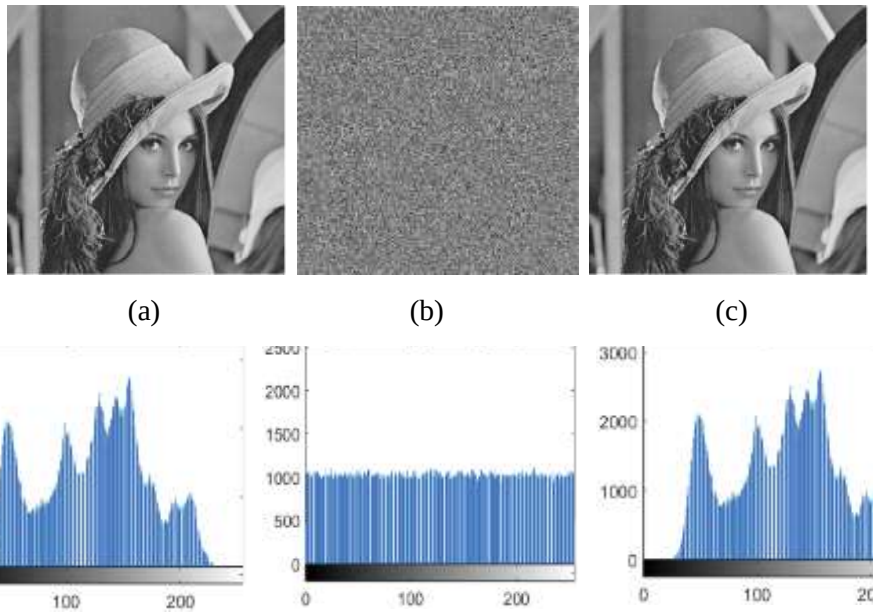


(a) (b)

Figure 3.8. Histogrammes, (a) Méthode de CHACHOUA (b) Méthode de JAVIDI

La comparaison des histogrammes de deux Méthodes permet d'évaluer la différence entre leurs distributions de valeurs de pixels. Comme on peut le voir, l'histogramme de l'image issu de la méthode de JAVIDI est réparti de manière aléatoire tends dis que celui de CHAHOUA présente un histogramme uniformément distribué, ce qui montre que le cryptage par la méthode de CHACHOUA est plus dure par rapport au cryptage de JAVIDI.

Concernant la partie de décryptage de la méthode de CHACHOUA, la Figure 3.9 montre les résultats de décryptage en utilisant la technique de modulation de cohérence. On remarque que, l'image récupérée Figure 3.9.c correspond bien à l'image cible d'entrée Figure 3.9.a.



(a) (b) (c)

(d) (e) (f)

Figure 3.9. Résultat de décryptage de la méthode de CHACHOUA,
(a)image cible (b)image cryptée (c) image décryptée,
Histogrammes, (d) image cible (e)image cryptée (f) image décryptée

Pour la méthode de JAVIDI, les résultat de la simulation est illustré sur la figure 3.10.

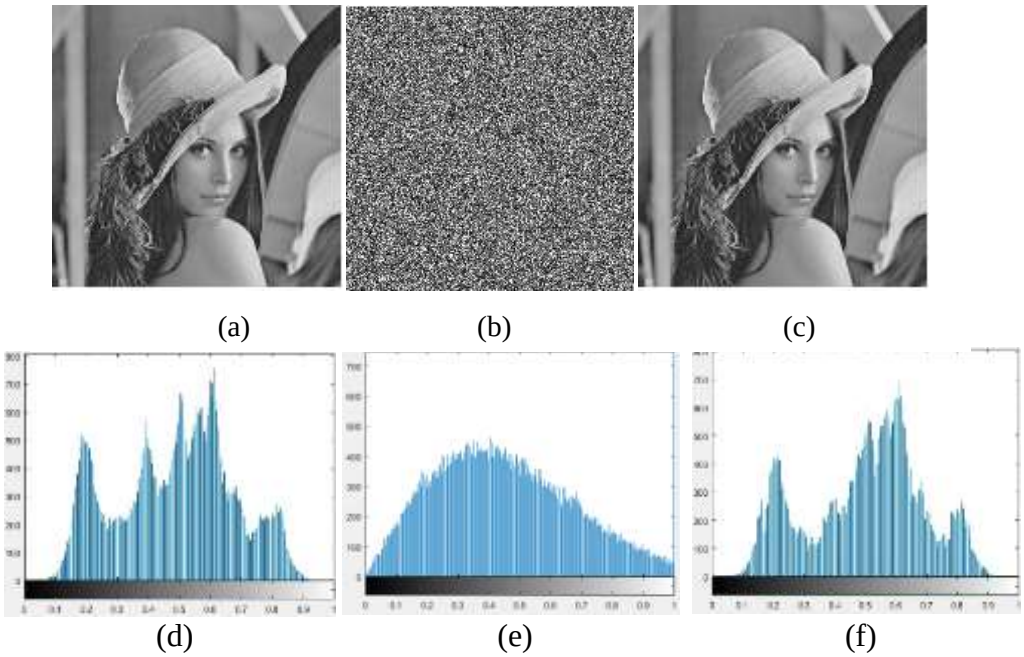


Figure 3.10. Résultat de décryptage de la méthode de JAVIDI,
(a) image cible (b) image cryptée (c) image décryptée .
Histogrammes, (d) image cible (e) image cryptée (f) image décryptée

3.5. Conclusion

Nous avons présenté deux méthodes de cryptage d'images : la Méthode de JAVIDI et celle de CHACHOUA. La Méthode de JAVIDI utilise une approche de cryptage basée sur le masque de phase, ce qui la rendre vulnérable à certaines attaques telles que l'attaque par force brute.

Le système T-DPES proposé par CHACHOUA, quant à lui, améliore la sécurité du cryptage en introduisant la notion de polarisation de la lumière. Cela rend le système T-DPES plus résistant aux attaques. De plus, il génère des images cryptées prédéfinit avec une distribution uniforme renforçant ainsi la sécurité du système.

En conclusion, le T-DPES de CHACHOUA présente des améliorations significatives en termes de sécurité par rapport au DRPE de JAVIDI, offrant ainsi une meilleure protection des images cryptées. Cependant, la sélection de la méthode de cryptage d'images doit être basée sur une analyse complète des exigences spécifiques et des compromis entre la sécurité et la complexité du système.

Conclusion Générale

Le développement rapide des réseaux de communication a provoqué de nouveaux problèmes de la sécurité des données. La sécurisation des données stockées ou transmises est généralement effectuée par des techniques de cryptage dont leur développement est devenu un grand challenge dans ces dernières années. Il existe effectivement une variété d'algorithmes de chiffrement qui ont démontré leurs performances et leur efficacité pour les informations visuelles. Ces algorithmes sont spécifiquement conçus pour le chiffrement des données visuelles, telles que les images et les vidéos, afin de garantir la confidentialité et la sécurité des informations qu'elles contiennent.

Dans le premier chapitre, nous avons étudié les formalismes mathématiques qui décrivent les états de polarisation de la lumière. Les formalismes matriciels de Jones pour les ondes totalement polarisées et de Stokes-Mueller pour les ondes partiellement polarisées ont été présentés. Nous avons également introduit le modulateur spatial de lumière, qui est un élément essentiel dans le traitement optique de l'information.

Le deuxième chapitre avait pour objectif d'introduire quelques notions élémentaires de cryptographie et d'imagerie. Nous avons abordé l'objet de la cryptographie ainsi que les principaux concepts cryptographiques. De plus, nous avons mentionné les différents types de chiffrement. Il est essentiel de comprendre les caractéristiques de base de la cryptographie et de l'imagerie afin de protéger et de sécuriser efficacement les informations. Enfin, nous avons examiné les types d'images existants, ainsi que les formats les plus utilisés.

Dans le troisième chapitre, et après une étude comparative de quelques algorithmes nous avons conclu qu'il est essentiel de comprendre que le chiffrement des images est un processus en constante évolution. Il est important de suivre les dernières avancées en matière de sécurité des images et d'adopter les meilleures pratiques pour préserver la confidentialité des données. La sécurisation des images contribue à créer un environnement sécurisé où la confidentialité et la protection des données sont garanties.

Référence

[1] Site Internet : https://culturesciencesphysique.ens-lyon.fr/ressource/simu-polarisation.xml.

[2] Abde Rezzaq HALASSI, Thèse de Doctorat, ‘’Contribution à l’Etude et à la Mise en œuvre de Filtres Dynamiques Dédiés aux Architectures de Télécommunications Optiques Nouvelle Génération’’, université Guelma 8 Mai 1945,19 octobre 2016.

[3] Matthieu DUBREUIL, Thèse de Doctora, ‘’ Développement d'un polarimètre de Mueller instantané par codage en longueur d'onde. Application à la caractérisation de cristaux liquids ferroélectriques’’, université de Bretagne Occidentale, le 10/12/10.

[4] Djeroud Irsal , Mémoire de Master, ‘’ Filtrage biréfringent interférentiel : Application à la compensation de la dispersion chromatique’’, université 8 mai 1945 Guelma, Juillet 2021.

[5] Grini leila , Cour master1, ‘’système de transmission et architectures optique ‘’ univarsite 8 mai 1945, 2022.

[6] Drioche Youcef, Thèse de Doctora, ‘Contribution à la réalisation de fonctions tout-optiques dédiées aux réseaux WDM transparents : dispositifs interférentiels flexibles en longueur d'onde pour la mise en forme d'impulsion laser’’, université 8 mai 1945 Guelma, juin 2018.

[7] A. Kumar, A. Ghatak, ”Polarization of ligth with applications in optical fibers”, SPIE, 2011.

[8] John Wiley & Sons, Inc., Hoboken, New Jersey, ’’ POLARIZED LIGHT INLIQUID CRYSTALS AND POLYMERS’’, 2007

[9] Biréfringence et Activité optique par Gilbert Gastebois.

[10] Site Internet :

http://www.optiqueingenieur.org/fr/cours/OPI_fr_M02_C02/co/Contenu_02.html]

[11] Mohamed Aldossari, Thèse de Doctora , ‘’ Nouvelle méthode optique de compression et de cryptage simultanés des images (fixes/vidéo) pour les systèmes télécommunication . Sciences de l’ingénieur [physics]. UBO, 2014. Français.

[12] Site Internet : https://fr.theastrologypage.com/spatial-light-modulator.

[13] site web : http://dspace.univ-tlemcen.dz/bitstream/112/1046/8/chapitre2.pdf.

[14] Site Internet : https://repository.usthb.dz/bitstream/handle/123456789/3526/TH4946.pdf?equence=3&isAllowed=y.

[15] Khouildat Hadjer, Mémoire de master,'' Méthode de cryptage d'image basée sur la permutation et la matrice de Householder'', Université KASDI-MERBAH Ouargla ,le 02 juillet 2019.

[16] HADJI Faiçal, Mémoire de master,'' Mémoire Conception et réalisation d'un système de cryptage pour les images médicales'', Université Mohamed Boudiaf- Msila, 2019-11-12.

[17] Site Internet : https://waytolearnx.com/2018/07/difference-entre cryptage symetrique et asymetrique.html .

[18] Aissam Djemaa Aissa Boubednikh, Mémoire de master,'' Réalisation d'un Système de Cryptage des Images Numérique basé sur le Chaos'', Université Mohamed Sadik BENYAHIA de Jijel, en 2021.

[19] Merdjal choumaissa et Merakchi Ahlam, Mémoire de master ,'' Cryptage d'image par un signal unidimensionnel quelconque'', université Ben Mhidi Oum El Bouaghi , en 2019.

[20] Meryem BOUCHEMA, Mémoire de master,'' Exploitation des transformées paramétriques dans le cryptage des images fixes'',l'université de Sétif 1 ,le : 28 / 10 / 2012.

[21] Bekkouche Toufik, Thèse de Doctora,'' Développement et implémentation des techniques de cryptage des données basées sur les transformées discrètes'', UNIVERSITE FERHAT ABBAS SETIF-1, le 14/10/2018.

[22] B. Javidi and P. Refregier, "Optical image encryption based on input plane and Fourier plane random encoding," OPTICS LETTERS , Vol. 20, No. 7 , April 1, 1995.

[23] Chachoua Marwan Dhiyaeddine, Hamdi Rachid, Ayman Alfalou, Halassi Abderezzaq, And Benkelfat Badr-Eddine,'' Tailored dual polarization encryption-coherence modulation-based decryption scheme for a predefined uniformly distributed noisy output image'',

Université 8 mai 1945 Guelma, L@bISEN, SAMOVAR, Optics Express 17400, Vol. 30, No. 10 / 9 May 2022,