THÈSE / UNIVERSITÉ DE BRETAGNE OCCIDENTALE

sous le sceau de l'Université européenne de Bretagne

pour obtenir le titre de
DOCTEUR DE L'UNIVERSITÉ DE BRETAGNE OCCIDENTALE
Mention : Sciences et Technologies de d'Information et de la Communication
École Doctorale SICMA

présentée par

Mohammed ALDOSSARI

Préparée dans l'équipe Vision
ISEN Brest

Nouvelle méthode optique de compression et de cryptage simultanés des images (fixes/vidéo) pour les systèmes télécommunication

Thèse soutenue le 15 Décembre 2014
devant le jury composé de :

Christian BROSSEAU
Professeur, Université de Bretagne Occidentale/ Président

Mohammad ALAM
Professeur, University of South Alabama, USA/ Rapporteur

Denis HAMAD
Professeur, Université du Littoral Côte d'Opale/ Rapporteur

Ayman ALFALOU
Professeur, ISEN Brest/ Directeur de thèse

Gilles KERYER
Professeur, Directeur de la recherche ISEN Brest/ Invité

Remerciement

Je voudrais tout d’abord remercier mon pays l’Arabie Saoudite de m’avoir octroyé une bourse afin de faire cette thèse de doctorat.

J'exprime mes profonds remerciements à mon directeur de thèse, le professeur Ayman Alfalou pour l'aide précieuse qu'il m'a apportée, pour sa patience et son encouragement tout au long de ce travail. Son œil critique a été très crucial pour structurer le travail et pour améliorer la qualité de résultats de différentes étapes. Sans lui rien n’aurait été possible.

Je tiens aussi à remercier, le professeur Christian BROSSEAU pour sa bienveillance et ses conseils avisés, pour l’aide et l’orientation durant ma préparation doctorale et pour avoir accepté de présider mon jury de thèse.

Je remercie infiniment les rapporteurs, professeur Denis HAMAD et M. S. ALAM, qui se sont donnés la peine de se pencher sur mon travail pour le comprendre et le juger.

Je suis reconnaissant envers tous ceux qui ont pris du temps pour relire mon manuscrit : Ayman ALFALOU, Alain LOUSSERT et Yousri OUERHANI.

Je remercie également toute l’équipe Vision ainsi que le personnel de l’Isen-Brest pour leur accueil et pour les discussions enrichissantes que nous avons engagées ensemble.

En fin, je souhaite remercier ma femme et mes enfants pour supporter le mal de pays et venir avec moi en France pour cette thèse.

Dédicace

Je dédie cette thèse à toute ma famille et surtout à mes chers fils Nawaf et Fahad (ce sera à vous de jouer)

Table des matières

Résumé

L'objectif de cette thèse est de proposer et valider une nouvelle méthode optique optimisée de compression et de cryptage simultanés des images (fixes ou issues d'une séquence vidéo). En effet, la plupart des méthodes de compression et de cryptage des images sont proposées d'une manière séparée et sont implantées en cascade (l'une après l'autre). Cependant les deux méthodes sont liées et l'une influence l'autre. Cela conduit à une baisse dans leurs performances et une complexité dans leur réalisation. Pour palier à ces problèmes, nous proposons de réaliser ces deux opérations (à savoir la compression et le cryptage) simultanément et d'une manière dépendante. Pour ce faire, notre approche de compression propose une opération de filtrage spectrale basée sur un critère de sélection et une fusion spéciale visant à multiplexer les informations représentatives de chaque image cible. De plus, nous cherchons à augmenter le niveau cryptage de notre système tout en gardant un bon taux de compression. Pour ce faire, nous utilisions une technique de segmentation spécialement adaptée au domaine de Fourier. Cette technique est basée sur l'utilisation, dans le plan image et dans le plan de Fourier, d'un ou plusieurs masques (clés d'amplitude et/ou de phase). Pour décrypter, il sera nécessaire de disposer à la fois des images qui ont servi à fabriquer ces masques de cryptage ainsi que de la technique de segmentation spectrale.

Mots clés : corrélation, transformée de Fourier optique, compression, cryptage, filtrage optique, segmentation spectrale, masque aléatoire,

Abstract

The main objective of my PhD thesis is to propose and validate the principle of a new optimized simultaneously optical compression and encryptions method of multiple images (pictures or coming from a video sequence). Indeed, most compression and encryption methods are optimized in a separate manner and used in cascade. However, both are related and influence each other. This leads to decrease the quality of reconstructed images and to increase their implementation complexity. To overcome these problems, we propose to perform these two operations (i.e. compression and encryption) together in a dependent manner. In addition, we propose different optimizations of compression and plan to increase the encryption level of our system while keeping a good compression ratio. For that, we used a specific segmentation technique specially adapted to the Fourier domain in order to merge together several target images and to create several encryption keys. Those keys (amplitude and/or phase) are used in the image plane and in the Fourier plane. To decrypt the transmitted information, it is necessary to have both encryptions keys and the used spectral segmentation technique.

Keywords: Correlation, optical Fourier transform, compression, encryption, optical filtering, spectral segmentation, random phase.

Table des figures

Acronymes

AEC	**A**dvanced **E**ncryption **S**tandard
DCT	**D**iscrete **C**osine **T**ransform
TF	**T**ransformé de **F**ourier
TFI	**T**ransformé de **F**ourier **I**nverse
RGB	**Red, Green, Bleu**
RVB	**R**ouge, **V**ert, **B**leu
VLC	**V**ander-**L**ugt **C**orrelator
JTC	**J**oint **T**ransform **C**orrelator
SPJTC	**S**hifted **P**hase-encoded **J**oint **T**ransform **C**orrelator
POF	**P**hase **O**nly **F**ilter
BPOF	**B**inary **POF**
PCE	**P**eak to **C**orrelation **E**nergy
MSE	**M**ean **S**quare **E**rror
PSNR	**P**eak **S**ignal to **N**oise **R**atio
SLM	**S**patial **L**ight **M**odulator
NLC	**N**ematic **L**iquid **C**ristal
FLC	**F**erroelectric **L**iquid **C**ristal
DRP	**D**ouble **R**andom **P**hase
DES	**D**ata **E**ncryption **S**tandard
CCD	**C**harged **C**oupled **D**evice
PSI	**P**hase Shifting Inerferometry
PSIDH	**P**hase **S**hifting **I**nerferometry **D**igital **H**olography
IFF	**I**dentification **F**riends or **F**oes
JPEG	**J**oint **P**hotographic **E**xperts **G**roup
JPEG2000	**J**oint **P**hotographic **E**xperts **G**roup 2000
ICA	**I**ndependent **C**omponent **A**nalyses
MOICE	**M**ultiple-image **O**ptical **I**mages **C**ompression and **E**ncryption
RMS	**R**oot-**M**ean-**S**quare Duration
RP	**R**andom **P**hase **M**ask

Introduction

De nos jours, la puissance des processeurs de systèmes informatiques et de télécommunications augmente plus vite que les capacités de stockage, et énormément plus vite que la bande passante de réseaux de télécommunications. En effet, cela demandera d'énormes changements dans les infrastructures telles que les installations téléphoniques. Ainsi, on préfère réduire la taille des données en exploitant la puissance des processeurs plutôt que d'augmenter les capacités de stockage et de transmission. Pour l'utilisation des images numériques, il faut comprimer les fichiers dans lesquels elles sont enregistrées. L'image consomme une quantité impressionnante d'octets quand elle est numérisée. Aujourd'hui, on parle de "qualité mégapixel" pour les appareils photo numériques; cela signifie que chaque image comporte environ un million de pixels dont chaque pixel nécessite trois octets pour les composantes RVB (rouge, vert, bleu). Donc, sans compression, cela représenterait un peu plus de 3 Mo (Mégaoctets) pour une seule photographie.

D'autre part, pour garder la confidentialité des informations représentées dans les images on a recours à la cryptographie. La cryptographie moderne s'attaque en fait plus généralement aux problèmes de sécurité des communications. Le but est d'offrir un certain nombre de services de sécurité comme la confidentialité, l'intégrité, l'authentification des données transmises. Pour cela, on utilise un certain nombre de mécanismes basés sur des algorithmes cryptographiques. La confidentialité est historiquement le premier problème posé à la cryptographie (comme dans les systèmes bancaires, de télécommunications ou militaires). Il se résout par la notion de chiffrement.

Cependant, la plupart des techniques proposent seulement des systèmes ayant de bonnes performances adaptées soit à la compression soit au cryptage des images fixes [1-8]. Ainsi, ils ne permettent pas de traiter la vidéo, ni de réaliser les deux opérations de compression et de cryptage simultanément. Or, ces deux opérations (compression et cryptage) sont nécessaires pour la plupart des applications de télécommunications.

Les récents développements survenus dans le domaine optique grâce à l'apparition des interfaces optoélectroniques comme les modulateurs spatiaux de lumière (SLM) ont donné lieu à de nombreux algorithmes de compression et de cryptage optiques. De plus, l'optique cohérente offre la possibilité de réaliser la transformation d'une image bidimensionnelle quasi-instantanée (par exemple la transformation de Fourier). Cette propriété est utilisée depuis longtemps pour rechercher un objet particulier (cible) dans une scène quelconque (technique de corrélation optique). Pour ces raisons, une partie de la communauté scientifique s'oriente vers la compression et le cryptage optiques. Nous avons de plus en plus recours à des traitements parallèles de l'information pour lesquels l'optique semble bien adaptée grâce à son parallélisme massif.

Ainsi, dans cette thèse nous allons nous intéresser à la compression et au cryptage simultanés des images (binaire et en niveau de gris) réalisables optiquement. En utilisant une méthode de compression développée au sein du laboratoire Vision de l'ISEN-Brest. Cette méthode est basée sur une fusion spéciale des informations spectrales pertinentes pour la reconstruction des images cibles [8-11]. Pour ce faire, nous nous basons sur la propriété intuitive du traitement optique de l'information permettant de manipuler facilement les informations propres à une image, à savoir le filtrage optique, plus communément appelé "montage 4f"[12]. Ainsi il est possible d'intervenir directement sur le spectre d'une image à un stade intermédiaire entre la lecture et la formation de l'image pour la comprimer. Une autre application de ce montage de filtrage optique qui a attiré l'attention de beaucoup de chercheurs à travers le monde, consiste à comprimer et à crypter une image. En effet, en appliquant un filtre spécifique, nous pouvons supprimer des informations redondantes d'une image (Compression) ou changer la répartition spectrale de ses fréquences pour les rendre inexploitables (Cryptage) [1].

De plus, les efforts ainsi que l'intérêt des chercheurs vis-à-vis de ces méthodes de compression et de cryptage sont asymétriques. En effet, les systèmes de cryptage ont mobilisé la plupart des efforts réalisés dans ce domaine au détriment des systèmes de compression i.e. ces systèmes de cryptage conduisent parfois à augmenter la taille des informations relatives à une image. En effet, beaucoup de ces systèmes de cryptage sont basées sur le traitement séparé de la partie réelle et imaginaire générées par le system DRP (Double Random Phase) [1,7]. A noter que les efforts, côté compression, ont été plus concentrés dans le domaine holographique pour réduire la taille des informations utiles pour reconstruire l'objet cible [13-17]. Mais très peu de méthodes existent pour traiter simultanément la compression et le cryptage des images multiples de nature très proches i.e. vidéo [13].

Notre approche est composée de deux niveaux de cryptage. Le premier niveau consiste à segmenter le spectre fusionné des images clés selon un critère bien défini et ensuite de changer la répartition spectrale dans le domaine de Fourier pour cacher les informations dans ce spectre. Le deuxième niveau de cryptage est composé de deux étapes. La première consiste à multiplier le spectre cible issu du premier niveau après le changement spectral par un masque aléatoire (amplitude et phase). Et pour augmenter la robustesse de notre méthode, l'étape deux consiste à multiplier à nouveau le spectre issu du premier niveau par un deuxième masque aléatoire (amplitude et phase) qui sera la deuxième clé de cryptage.

Notre nouvelle méthode permet de trouver un bon compromis entre le taux de compression et la qualité des images reconstruites en sortie de système et un niveau de cryptage robuste avec plusieurs clés de cryptage.

Le plan de la thèse sera décliné en quatre chapitres :

- Le premier chapitre expose le contexte et l'objectif de la thèse. En effet dans cette partie nous allons présenter le contexte de la thèse en détaillant les différentes techniques de traitement optique de l'information. Ensuite nous allons aborder

l'intérêt de la compression, puis la compression de données, la caractérisation, les types, les méthodes et les principes de base de la compression. Et nous terminons par une conclusion.

- Le deuxième chapitre présente l'état de l'art. En effet nous allons passer en revue les méthodes de compression et de cryptage des images. Ensuite nous discutons des méthodes les plus connues en évaluant leurs performances.

- Le troisième chapitre est réservé au développement de la nouvelle méthode de compression et cryptage simultanés des images fixes. Dans un premier temps, nous allons présenter en détail la méthode. Ensuite, nous expliquerons nos approches de compression et de cryptage. Puis, nous terminerons ce chapitre par une étude de performances de notre méthode en termes de taux de compression et de qualité des images reconstruites.

- Le quatrième chapitre s'occupe de l'optimisation de notre méthode en termes de compression et de cryptage simultanés. Dans ce cadre, nous allons proposer des nouvelles techniques d'optimisation pour améliorer les performances de ces deux opérations de compression et le cryptage. Cela se fera par un nouvel algorithme exploitant la propriété de la symétrie dans le domaine de Fourier pour augmenter le taux de compression. Puis, nous allons adapter notre méthode de compression et de cryptage aux images vidéo.

  Côté cryptage, nous allons proposer une nouvelle approche pour fabriquer la clé du cryptage optimisée avec un deuxième masque afin de garantir un bon niveau de sécurité de la méthode et la rendre plus robuste.
  Nous terminerons ce chapitre par une extension de notre travail en utilisant des images polarisées à l'entrée de système.

Nous finaliserons notre mémoire de thèse par une conclusion générale et quelques perspectives.

Première partie

Contexte et objectifs de la thèse

Chapitre 1

1. Traitement de l'information par filtrage optique

Sommaire

1.1 Introduction

Le traitement de l'information est une activité de recherche en pleine essor ces dernières années grâce, entre autres, à l'accroissement des capacités d'implantation des algorithmes classiques de traitement du signal et de l'image (reconnaissance de formes, compression, cryptage, etc.). Dans ce domaine, l'utilisation de l'optique s'est tout naturellement imposée comme une solution intéressante pour stocker ou transmettre le volume des données grandissant des systèmes modernes comme les systèmes de télécommunications ou bancaires. En effet, le fort parallélisme de l'optique et l'apparition des interfaces optoélectroniques très performantes comme les modulateurs spatiaux de lumière (SLM) ont attiré l'attention d'une partie de la communauté scientifique pour implanter optiquement des algorithmes du traitement d'images.

Nous commençons ce chapitre par une brève présentation du principe d'une chaîne de télécommunication. Ensuite, nous définissons l'optique de Fourier et la Transformée de Fourier (TF). Cela va nous permettre d'identifier les blocs susceptibles d'être implantés optiquement. Dans cette partie, nous nous attardons sur les possibilités d'implantation optique de cette transformée [12]. Puis, nous présentons le montage optique de base permettant d'implanter optiquement les algorithmes de traitements d'images appelé "montage 4f". Pour illustrer nos propos nous prenons comme exemple la corrélation avec l'architecture du corrélateur Vander-Lugt [18]. Ensuite, nous allons décrire la corrélation optique comme une technique de reconnaissance des formes et lister les différents types de filtres utilisés dans la littérature pour rendre cette corrélation plus performante en termes de robustesse et/ou de discrimination.

1.2 Principe d'une chaîne de télécommunication

Les techniques de transmission numérique sont aujourd'hui largement répandues dans les systèmes de diffusion de l'information. Leur but est de transporter l'information entre une source (émetteur) et un destinataire (récepteur) par l'intermédiaire d'un canal de transmission. Ce dernier peut être une propagation en espace libre, sur support physique comme un câble (coaxial,…) ou une fibre optique. Les signaux transportés, qu'ils soient d'origine numérique (texte…) ou d'origine analogique (parole, images,…), doivent être adaptés au canal de transmission (numérique ou analogique). Cette adaptation ne doit pas altérer la tâche principale d'un système de transmission qui est d'acheminer l'information de la source vers le destinataire le plus rapidement possible et avec la plus grande fiabilité.

Le schéma de principe d'une chaîne de télécommunication est présenté sur la figure 1.1. Cette dernière peut être divisée en trois parties :

- L'émetteur : la source de l'information et son système de codage.
- Le canal de transmission
- Le récepteur : le destinataire et son système de restitution.

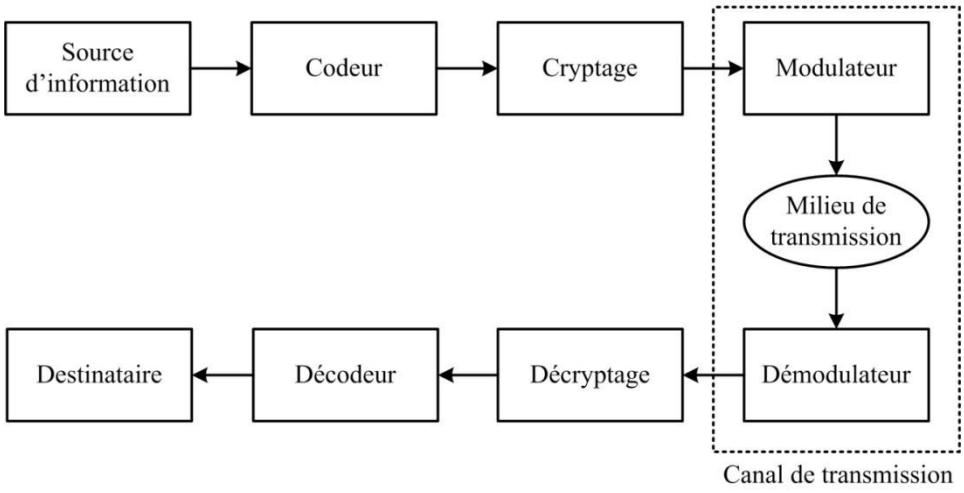


Figure 1.1 Schéma synoptique d'une chaîne de télécommunication.

Dans ce qui suit, nous allons décrire brièvement les différentes fonctions qui interviennent dans une chaîne de télécommunication [19] :

Le premier bloc désigne la source dans laquelle est générée l'information à transmettre. Cette information peut être numérique ou analogique.
Le deuxième bloc représente le codeur. Il se divise en deux parties : le codage de source et le codage canal.

- Le codage de source a pour objectif de transformer le message émis par la source en un message aussi court que possible permettant en particulier d'éliminer la redondance de manière à réduire la quantité d'informations à transmettre. On réalise donc une compression des données.
- Le codage canal, aussi appelé codage détecteur et/ou correcteur d'erreur, permet d'améliorer la qualité de la transmission dans le canal. Cela peut prêter à confusion, mais tout simplement les deux codages ne visent pas les mêmes types d'informations redondantes. Nous pouvons remarquer que les objectifs du codage de source et du codage de canal se révèlent contradictoire : le codage de source vise à une concision maximale par la suppression de la redondance, ce qui entraîne un accroissement de la vulnérabilité aux erreurs, alors que le codage canal protège contre les erreurs de transmission introduisant de la redondance. Cette remarque suggère que ces deux fonctions ne doivent pas être considérées comme totalement indépendantes l'une de l'autre lors de la conception d'une chaîne de transmission.

Le troisième bloc est le cryptage qui permet de modifier l'information source suivant un algorithme bien défini et de façon complexe afin qu'elle devienne inintelligible, sauf pour le destinataire autorisé à lire le message, donc seul à connaître les règles utilisées pour le décryptage.

Le quatrième bloc est le canal de transmission. Il est divisé en trois parties :

- Le modulateur qui a pour objectif de transformer le message numérique délivré par le codeur de canal en un signal d'onde utilisant une fréquence porteuse adaptée au milieu de transmission par exemple.

- Le milieu de transmission désigne le support physique sur lequel se propagent les signaux. Il peut s'agir d'un câble coaxial, d'une fibre optique ou simplement de l'espace libre (communication radio mobile). Il est à noter que le milieu de transmission est le siège de phénomène de propagation et de perturbations d'origines diverses (imperfections des équipements, présence de bruit, affaiblissement).

- Le démodulateur réalise la fonction inverse du modulateur.

En réception, la fonction de décryptage sert à déchiffrer (restituer) le message reçu et à le rendre lisible par le récepteur possédant la ou les clés de cryptage.

Cette description de différents blocs nous permet de constater que la qualité des informations nécessaire pour assurer une bonne qualité du signal à transmettre est directement liée au type de codage utilisé. De même, le bloc cryptage est nécessaire pour assurer la confidentialité de ces informations. Cependant le besoin grandissant d'augmenter la cadence de transmission tout en assurant la confidentialité des messages échangés a poussé une partie de la communauté scientifique à s'intéresser de plus en plus à ces deux opérations et à utiliser des mécanismes de codage et de sécurité évolués.

En effet, beaucoup d'algorithmes de compression et de cryptage numériques ont été introduits pour assurer la rapidité et gagner en sécurisation d'un tel échange. Or coder numériquement des informations complexes (images haute résolution à hautes cadences,…) exige un temps de calcul et des traitements électroniques réalisés en parallèle très coûteux.

De plus, les images sont à l'origine optiques, ainsi il est intéressant d'essayer de réaliser ces deux opérations de compression et de cryptage optiquement lorsqu'on parle des images de très grandes tailles. Ainsi cette thèse a pour but principal de proposer et de valider des méthodes permettant d'implanter ces deux opérations optiquement en se basant sur l'optique de Fourier. Par conséquent nous commençons par une introduction de l'optique de Fourier dans le paragraphe suivant.

1.3 L'optique de Fourier

L'optique de Fourier est le domaine qui traite du comportement ondulatoire de la lumière à travers un système de lentilles et d'ouvertures dans l'approximation paraxiale. Dans cette thèse nous nous intéressons seulement à l'optique de Fourier d'un point de vu de la réalisation

optique d'une transformée de Fourier (TF). Ainsi, dans ce paragraphe nous détaillons directement cette TF optique même si cela néglige un certain nombre d'étapes nécessaires à la compréhension du phénomène. Pour cela, nous invitons les lecteurs à consulter la référence [12] pour plus de détails.

1.3.1 Transformée de Fourier 1D

Découverte par le mathématicien et physicien français Joseph Fourier (1768-1830), la transformée de Fourier consiste à décomposer tout signal continu en une somme de sinusoïdes. La transformée permet ainsi de convertir la représentation temporelle d'un signal d'entrée en une représentation fréquentielle. Pour ce faire, le signal est représenté sous forme d'une combinaison linéaire infinie des fonctions trigonométriques de toutes les fréquences qui forment son spectre. Ainsi la transformée de Fourier permet donc de donner une vue du signal (vue fréquentielle) différente de la vue temporelle pour permettre une analyse du signal.

Nous rappelons ici la définition de la transformée de Fourier puis définissons les différentes techniques qui permettent de la réaliser optiquement [12]. Pour simplifier les calculs, on utilise souvent la notion de convolution.

Soit un signal S(t) dépendant d'une seule variable t. Sa transformée de Fourier S(v) est définie par la formule suivante :

$$\mathrm{S}(v) = \int_{-\infty}^{+\infty} s(t) e^{-2i\pi vt} dt \tag{1}$$

Avec v représentant les fréquences et t représentant le temps

Cette transformation est inversible et son expression est donnée par la formule :

$$\mathrm{S}(t) = \int_{-\infty}^{+\infty} s(v) e^{+2i\pi vt} dv \tag{2}$$

Dans cette thèse nous nous intéressons aux images qui peuvent être définies comme un signal à deux dimensions. Ainsi par la suite nous définissions cette TF par un signal 2D.

1.3.2 Transformée de Fourier 2D

La transformée de Fourier 2D est une extension de la transformée de Fourier 1D. Soit un signal $f(x,y)$, une image peut par exemple être décrite comme une répartition spatiale et f un éclairement. La transformation de Fourier 2D est donnée par la relation suivante :

$$F(\mu, v) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} f(x,y) e^{-2i\pi[\mu x + vy]} dx dy \tag{3}$$

Cette transformation est inversible, et sa transformation inverse est donnée par la relation (4)

$$f(x,y) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} F(\mu, v) e^{+2i\pi[\mu x + vy]} d\mu dv \tag{4}$$

1.3.3 Implantation optique d'une TF

L'optique cohérente offre la possibilité de réaliser naturellement une transformée de Fourier bidimensionnelle. En effet, si on place un objet (par exemple, une diapositive) dans le plan d'entrée d'une lentille convergente et si on l'éclaire avec une source de lumière cohérente, on obtient dans son plan focal image sa transformée de Fourier exacte en amplitude et en phase (figure 1.2). A condition qu'on respecte la distance focale de cette lentille *f*.

Dans cette condition on a :

$$f = \frac{N \times de \times df}{\lambda}$$

avec

- f la focale de la lentille L.
- *N* le nombre des pixels dans le plan d'entrée.
- *de* et *df* représentent respectivement la taille du pixel (résolution) du plan d'entrée et celle du plan de Fourier.
- λ la longueur d'onde.

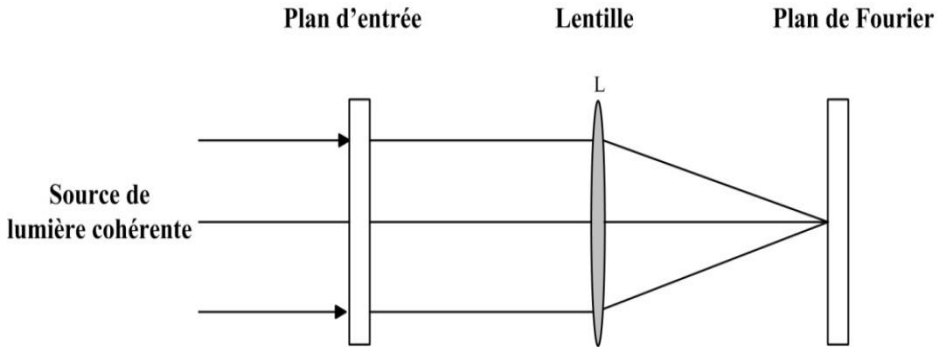


Figure 1.2 Implantation optique d'une transformée de Fourier

1.3.4 Corrélateur de Vander-lugt (montage 4f)

L'utilisation des méthodes de traitement par corrélation optique n'a cessé d'évoluer. Ainsi leur champ d'application s'est étendu à des applications de surveillance et d'identification aussi bien militaires (reconnaissance des avions, bateaux,…) que civiles (reconnaissance des panneaux de signalisation routière, identification des personnes à des fin bancaires, ou sécuritaires comme dans les aéroports, le métro, …). Ainsi la corrélation est un outil de décision très puissant principalement du fait de son caractère global et de sa robustesse au bruit. En effet, la corrélation est particulièrement appropriée à l'optique essentiellement du fait de la transformée de Fourier, le noyau de la corrélation, qui est naturelle en optique.

Outre les progrès inhérents aux qualités des lasers (faisceaux quasi-parallèles, haute puissance, cohérence et monochromatisme), le traitement de l'information par voie optique a

fait d'énormes progrès surtout grâce à l'introduction des interfaces optoélectroniques à base de cristal liquide (SLM : Spatial Light Modulator) et des matrices (CCD : Charge-Coupled Device). Pour ce faire, deux grandes familles de corrélateurs existent dans la littérature : le Corrélateur à transformée de Fourier conjointe JTC (Joint Transform correlator) et le Corrélateur de Vander-Lugt. Ce dernier se base sur l'utilisation d'un montage « 4f », sur une comparaison entre l'image cible et une image référence issue d'une base d'apprentissage et sur une simple détection d'un pic de corrélation. Cette dernière mesure le degré de ressemblance entre l'image cible et l'image référence.

En 1964 Vander Lugt [18] a publié le premier corrélateur optique basé sur l'analyse de Fourier. Le principe de ce corrélateur consiste à effectuer deux transformations de Fourier successives réalisées optiquement par le moyen de deux lentilles convergentes et un filtrage dans le domaine spectral. Le montage optique de base de ce corrélateur est illustré sur la figure 1.3.

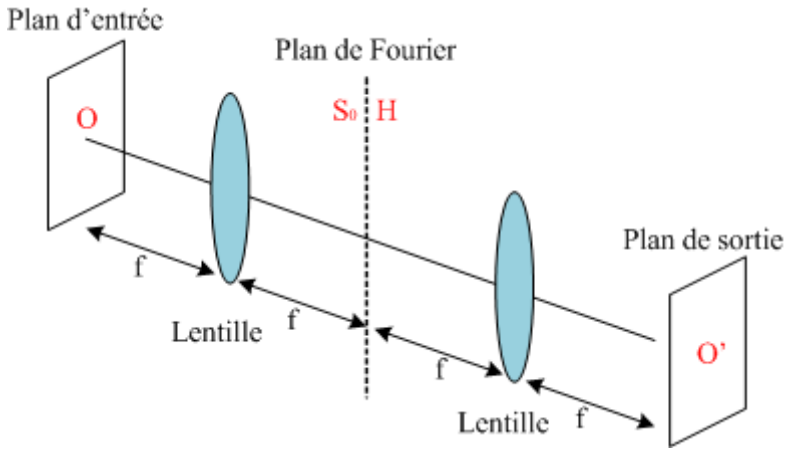


Figure 1.3 Corrélateur optique de Vander Lugt (montage 4f)

L'objet cible *O*, supposé plan, est placé dans le plan d'entrée et éclairé par une onde plane monochromatique [20]. Une lentille convergente forme S_0 la TF (Transformée de Fourier) de l'objet cible dans son plan focal image (plan de Fourier ou plan spectral) où est placé un filtre de corrélation H. Ce dernier est calculé en fonction du traitement désiré [21]. Enfin, une deuxième lentille effectue une seconde TF dans le plan de sortie (plan de corrélation). Ce plan contient ou pas un point lumineux (aussi appelé pic de corrélation) plus ou moins intense selon le degré de ressemblance entre l'image cible et l'image utilisée pour fabriquer le filtre de corrélation.

Le principe du filtrage consiste à agir sur le spectre de l'objet, donc dans le plan de Fourier, de façon à modifier sa répartition spectrale. La prise de décision dans le plan de sortie est généralement basée sur un critère de performance appelé PCE (Peak to Correlation Energy) [22]. Le PCE représente le rapport de l'énergie du pic de corrélation par rapport à l'énergie totale du plan de corrélation.

$$PCE = \frac{\boldsymbol{Energie\ du\ pic\ de\ corrélation}}{\boldsymbol{Energie\ du\ plan\ de\ corrélation}} \quad (5)$$

Selon la figure. 1.3, il est possible de corréler une image avec toutes sortes de filtres, cela dépendra du filtre introduit dans le plan de Fourier. Ainsi, plusieurs formes de filtres ont été proposées par les chercheurs afin d'améliorer la robustesse ainsi que la discrimination du corrélateur VLC. Parmi ces filtres nous citons le filtre adapté, le filtre de phase pure (POF), le filtre composite et le filtre segmenté.

1.3.5 Corrélateur à transformée de Fourier conjointe (JTC)

Il existe une deuxième famille d'architecture de corrélateur optique appelé JTC (Joint Transform correlator). Ce corrélateur a été proposé par Weaver et Goodman en 1966 [23] comme une alternative à l'architecture du VLC pour convoluer deux fonctions. Ils mettent en évidence la principale difficulté de mise en œuvre du corrélateur VLC, à savoir l'alignement du filtre avec le spectre du signal d'entrée (estimé à quelques microns). La solution proposée par Weaver et Goodman consiste à placer les deux images (cible et référence) que nous pouvons convoluer (ou à corréler) dans un même plan. Une transformée de Fourier appliquée à ce plan permet d'obtenir le spectre joint de ces deux images. Ensuite, une TF de ce plan permet d'obtenir la corrélation entre les deux images. L'avantage de cette architecture est qu'il n'y pas de problème d'alignement, puisqu'il n'y pas de filtre à introduire dans le plan de Fourier.

En revanche, il y a une étape d'enregistrement photographique à chaque opération, alors que dans le système de Vander-Lugt, le filtre est enregistré une seule fois. D'autre part, il est nécessaire d'utiliser un faisceau de laser de référence pour pouvoir enregistrer l'image dans la bonne gamme d'exposition. De plus, une perte du produit espace bande passante du plan d'entrée est observée comme cela est expliqué dans [24].

Une des premières réalisations de ce type de corrélateur a été rapportée dans [25]. Ce type de corrélateur est largement étudié dans la littérature notamment en raison de sa simplicité d'implantation pour une application de suivi comme cela est montré dans les différents travaux réalisés dans le laboratoire d'Isen-Brest [21].

Dans cette thèse, nous sommes intéressés par l'architecture de Vander-Lugt pour son aptitude au filtrage fréquentiel. En effet, nous considérons la compression comme une sélection des informations pertinentes nécessaires pour reconstruire l'image cible. Ainsi, il suffit d'adapter le filtre dans le plan de Fourier pour répondre à cette exigence de compression. Idem pour le cryptage qui consiste à introduire un filtre capable de modifier la réparation temporelle de l'image.

1.4 La corrélation (outil de filtrage du point de vu algorithmique)

Dans cette partie nous allons aborder la corrélation d'un point de vu algorithmique comme technique de reconnaissance des formes i.e. nous allons essayer de montrer les liens entre la corrélation et les techniques de compression et de cryptage. En effet, la corrélation a suscité depuis les années 80 une grande curiosité et d'importantes recherches. Les applications de la corrélation concernent un grand nombre de domaines tels que l'automatisation et le transport par exemple. En particulier, elle est utilisée à des fins sécuritaires (reconnaissance de visages, d'empreintes digitales, etc...). Son principe est simple, il s'agit de comparer l'image à analyser (ou image cible) à une image référence connue, issue d'une base d'apprentissage (aussi appelée base de référence) comme le montre la figure 1.4

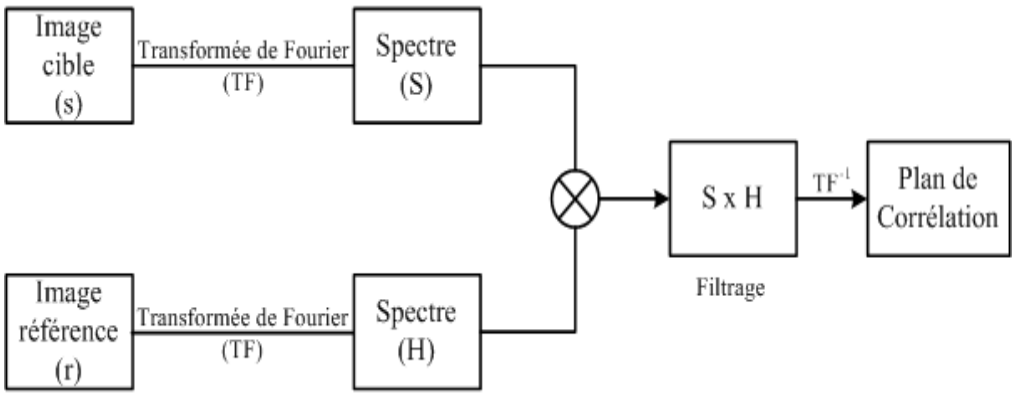


Figure 1.4 Schéma synoptique de la corrélation optique

Les développements des algorithmes adaptés à la corrélation ont permis d'accroître considérablement les performances des corrélateurs tant dans leur capacité de traitement que dans leurs applications.

Cependant, pour dépasser les limites d'une décision prise par une simple détection d'un pic de corrélation, il est nécessaire d'utiliser des algorithmes de décision moins sommaires. Une combinaison modulable de résultats binaires peut permettre d'atteindre cet objectif [21]. Ceci passe par l'intégration de nouveaux filtres de corrélation et la réalisation en parallèle de plusieurs corrélations, ce qu'on l'on peut obtenir par des architectures multivoies rapides et reconfigurables.

1.4.1 Quelques filtres de corrélation

Pour comprendre les effets du filtrage (montage 4f), nous allons citer dans ce paragraphe quelques filtres de corrélation qui sont en lien avec notre approche de compression et de cryptage proposés dans cette étude.

1.4.1.1 Filtre adapté

Ce filtre adapté est le filtre de base qui a été utilisé dans le traitement optique. Il est simple à obtenir car il est défini comme étant le conjugué du spectre de l'image référence. L'avantage principal de ce filtre est de présenter un bon rapport signal/bruit (SNR) en sortie, même en présence de bruit. Mais son principal inconvénient est de donner un pic de corrélation très large dans le plan de corrélation, ce qui entraine une faible discrimination ainsi qu'une faible précision sur la position de l'objet présent dans la scène. Il est obtenu de la façon suivante :

$$H_{adapte}(u,v) = R^*(u,v) \qquad (6)$$

Où H_{adapte} est le filtre adapté et u,v sont les coordonnées du filtre dans le plan de Fourier. R^* est le spectre conjugué de l'image référence.

Pour tester sa robustesse et son faible pouvoir discriminant, nous avons testé ce filtre sur des visages présentés dans la figure 1.5. L'image cible présente (figure 1.5-a [à gauche]) le visage d'une personne avec une rotation de 45 degrés en horizontal et de 0 degré en vertical et l'image référence présente (figure 1.5-a) à droite) le visage de la même personne avec une rotation de zéro degré en horizontale et en vertical. Ces deux visages font partie d'une même base de données. Malgré la grande rotation entre l'image cible et l'image référence, le filtre adapté donne un pic de corrélation bien visible (figure 1.5-b) ce qu'il atteste de sa bonne robustesse mais avec un faible pouvoir discriminant.

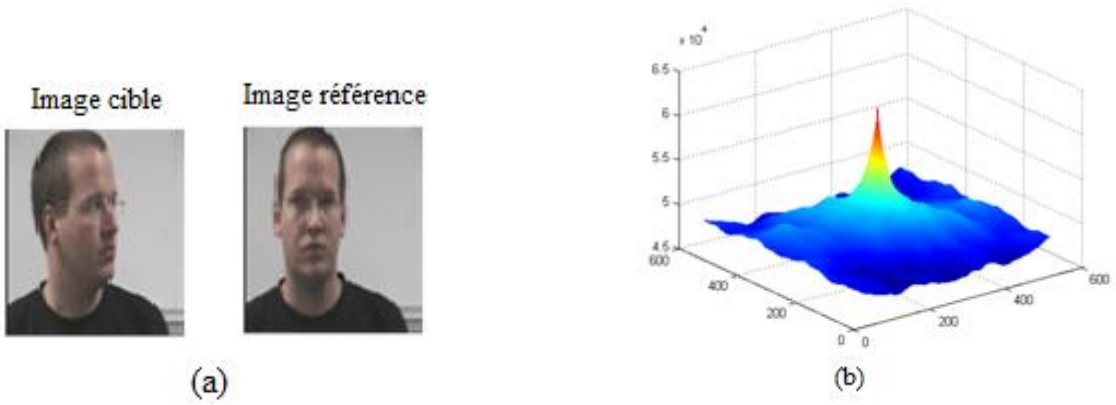


Figure 1.5 Résultat de simulation de Corrélation filtre adapté, en (a) les images cible et référence. (b) le plan de corrélation

1.4.1.2 Filtre de phase pure POF (Phase Only Filtre)

Depuis la publication du premier corrélateur optique conçu par Vander-Lugt [18] beaucoup de recherches ont été effectuées pour le rendre plus performant. En effet, Horner [26] s'appuie sur le constat qui stipule que l'information contenue dans la phase de la transformée de Fourier d'un objet est beaucoup plus importante que celle contenue dans l'amplitude et il a proposé un filtre de phase pure (POF : Phase Only Filter). A la base, c'est un filtre adapté dont l'amplitude a été mise à 1 en tout point. Pour ce faire, on divise le conjugué du spectre de l'image référence par son module en chaque point. Ce filtre est connu par son pouvoir discrimination important par rapport au filtre adapté ainsi que pour sa simplicité d'implantation [21]. Il est donné par l'équation suivante :

$$H_{POF}(u,v) = \frac{\boldsymbol{R}^*(u,v)}{|\boldsymbol{R}(u,v)|} \tag{7}$$

Où R est le spectre de l'image référence et R^* son conjugué.

Pour montrer le bon pouvoir discriminant de ce type de filtre, nous l'avons testé avec l'image représentée dans la figure 1.6-a) pour reconnaitre cette image avec la même image cible. Cela donne un plan de corrélation avec un pic très fin et bien intense qui permet d'obtenir une bonne décision (figure 1.6-b). Cependant ce filtre manque de robustesse car il est sensible au changement (rotation) de l'image cible par rapport à l'image référence qui se traduit par une baisse significative de la hauteur du pic de corrélation.

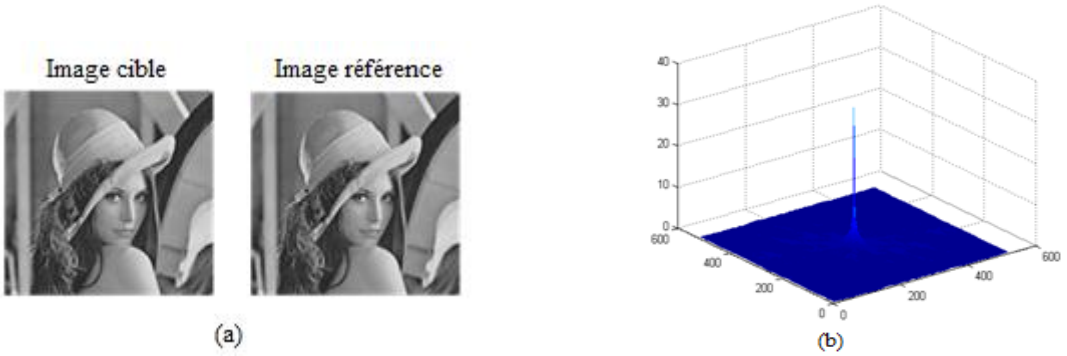


Figure 1.6 Résultat de simulation de Corrélation filtre POF, en (a) les images référence et cible. (b) le plan de corrélation

1.4.1.3 Filtre BPOF

Le filtre BPOF (Binary Phase Only Filter) a été créé pour faciliter l'implémentation optique de filtre POF ainsi que sa manipulation. Pour ce faire Horner [27] propose d'étudier le signe de la partie réelle du filtre POF :

$$H_{BPOF} = B[H_{POF}] \tag{8}$$

$$H_{BPOF} = \begin{cases} 1 & si\ Real(HPOF) > 0 \\ -1 & sinon \end{cases} \tag{9}$$

L'opérateur *Real* désigne la partie réelle d'un nombre complexe. La figure 1.7 illustre le plan de corrélation entre les images référence et cible présentées dans la figure 1.6 (a).

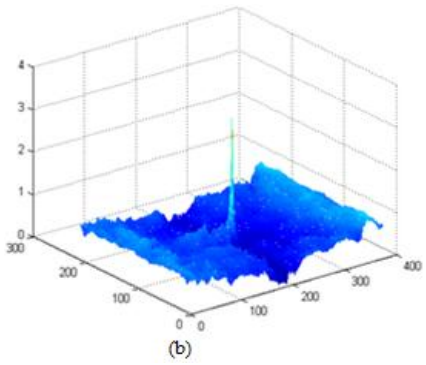


Figure 1.7. Résultat de simulation de Corrélation filtre BPOF

Nous pouvons remarquer que les filtre POF et BPOF permettent la même souplesse et efficacité de reconnaissance, ainsi que les mêmes inconvénients liés à leur robustesse.

1.4.1.4 Filtre composite

Le principe de base du filtre composite consiste à former une combinaison de différentes références pondérées par des constantes afin d'optimiser une fonction de coût choisie pour une application donnée. Ce filtre est défini par [28, 29]:

$$H_{composite} = \sum a_i R_i \tag{10}$$

Avec ce filtre, nous pouvons multiplexer deux ou plusieurs références en faisant par exemple une simple addition. Donc chaque pixel du plan de filtre est la somme des valeurs issues des différents spectres d'images références considérées. Lorsqu'il est composé de quelques spectres références (3 ou 4 maximum), ce filtre est très efficace. Mais lorsque le nombre de références augmente, ce filtre présente un phénomène de saturation qui entraine une baisse significative des ses performances. Notons que cette addition spectrale peut être considérée comme une fusion des différents spectres et ainsi ressemble à une compression i.e à la place de stocker *n* filtres nous n'avons plus à manipuler qu'un seul filtre qui contient les informations *n* images références.

1.4.1.5 Filtre segmenté

Pour palier le problème de saturation locale rencontré avec le filtre composite Alfalou et al [24] ont proposé une version optimisée du filtre composite. Le principe de ce filtre appelé filtre segmenté consiste à diviser le plan de Fourier du filtre en plusieurs zones. Chacune de ces zones sera allouée à un spectre d'une des images références utilisées pour la construction du filtre (Figure 1.8).

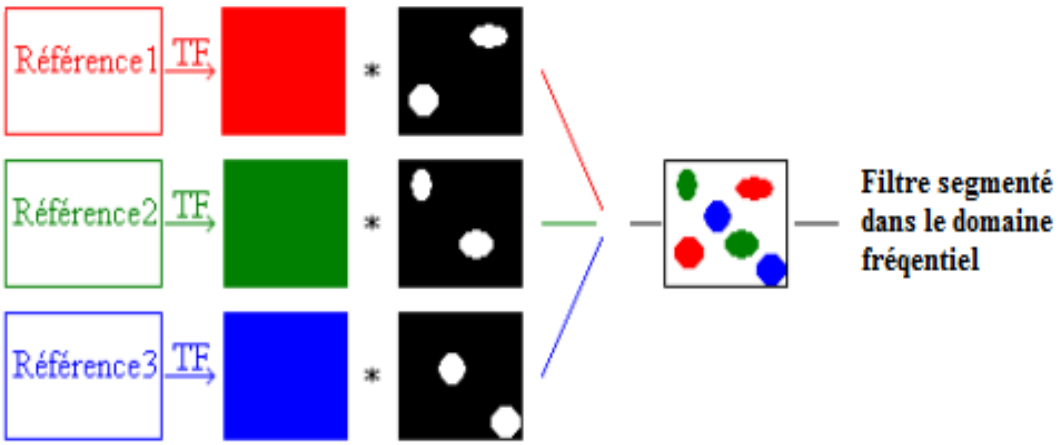


Figure 1.8 Principe de fabrication du filtre segmenté

Dans la Figure 1.8, il est indiqué que la construction du filtre segmenté s'effectue en fusionnant, sans recouvrement, des éléments des spectres des images références en se basant sur un critère de sélection bien précis d'une des images références. Un des critères de segmentation utilisé consiste à prendre la valeur maximale de l'énergie normalisée en chaque point (un exemple est présenté sur la figure 1.9). Mathématiquement, on calcule, pour chacun des spectres des images références, l'énergie relative du pixel (*i; j*). Le pixel qui a l'énergie relative la plus importante est sélectionné.

La même opération est effectuée pour tous les pixels. Avec cette approche basée sur le choix point par point, il est possible de trouver des pixels isolés (un seul pixel appartenant à la référence i parmi les pixels du voisinage). Plus le nombre de références à multiplexer est élevé plus le nombre de pixels isolés est élevé. Il alors possible que le filtre ne soit pas très efficace du fait que peu de pixels consécutifs appartiennent à la même référence. Mais ce filtre donne des bonnes performances en termes de robustesse et de discrimination comparé aux filtres composites [24].

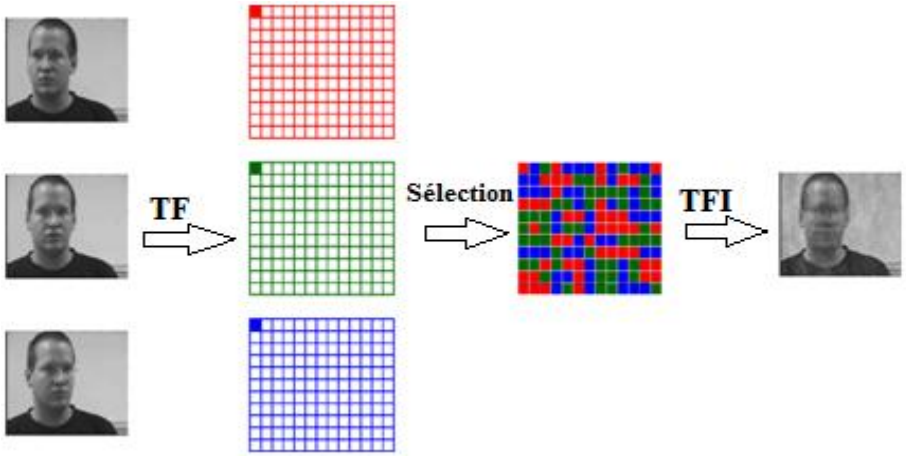


Figure 1.9 Fabrication d'un filtre segmenté à partir de 3 références

Ce nouveau filtre permet le multiplexage de plusieurs classes d'objet à reconnaître. Ce tri de l'information contenue dans la scène et son adéquation à l'une des classes sont réalisés dans le plan spectral. Ce qui permet une identification optimale de la forme cherchée. Pour ce faire, un critère de partition des fréquences et d'affectation à une classe, dans un premier temps énergétique (mais où l'on peut également introduire la phase), a été utilisé. Ce type de filtre peut être utilisé dans de nombreux traitements optiques des images, comme c'est le cas pour la corrélation des images couleurs, la reconnaissance des formes 3D, la compression et le cryptage optiques [32, 33, 34] des images.

Grâce aux travaux développés dans le cadre de la corrélation, comme la technique de reconnaissance multi-décisions, nous avons appris à manipuler les informations dans le domaine spectral. Cette manipulation nous a permis de fabriquer un filtre segmenté de corrélation incorporant non pas une mais plusieurs références en même temps. Dans nos travaux dans le domaine de la communication nous allons utiliser le principe de ce filtre segmenté pour faire de la compression et du cryptage des images.

Nous venons de voir que grâce au montage 4f et au principe de filtrage qu'il est possible de chercher une information bien précise dans le plan de sortie. Pour la corrélation, c'est un pic de corrélation représentant le degré de ressemblance entre l'image cible et l'image référence. De plus, l'introduction du filtre POF a montré que la manipulation de la phase est plus importante que celle de l'amplitude d'un spectre.

Ainsi, nous allons utiliser cette propriété pour ajouter un masque de phase dans notre système de communication permettant de modifier le spectre des images cibles i.e réaliser ainsi le cryptage de ces images. Le principe de la fusion développé dans le cadre du filtre segmenté nous montre qu'il est possible de sélectionner les informations pertinentes à la reconnaissance. Le même principe peut être adapté pour comprimer différentes images cibles en adaptant le critère de sélection et d'affectation pour permettre la reconnaissance des images cibles. Nous terminons ce chapitre en rappelant le principe des interfaces optoélectronique utilisées dans le montage 4f introduisant le filtre dans ce montage.

1.5 Introduction au modulateur spatial de lumière (SLM)

Comme nous l'avons vu auparavant, pour effectuer l'opération de filtrage optique, il faut disposer des interfaces qui permettent d'intervenir sur l'image dans le plan de Fourier pour la filtrer. C'est le rôle du modulateur spatial de lumière (SLM).

Le premier cristal liquide a été découvert en 1889 par O.Lehmann qui a publié son article dans la revue scientifique allemande "Zeitschrif für physikalische chemie"[30]. Il y est fait état d'une nouvelle forme de la matière et notamment de substances organiques ne présentant pas une transition unique de l'état solide vers l'état liquide mais plutôt une succession de phases transitoires dont les propriétés mécaniques et de symétrie sont intermédiaires entre celles des liquides amorphes et des solides cristallins.

Dans la littérature, il est possible d'utiliser les propriétés électro-optiques de certains cristaux pour créer ou enregistrer en temps réel les données optiques qui interviennent dans le système destiné au traitement optique du signal.

On distingue deux catégories de SLM :

- SLM à adressages électriques, utilisés si l'information est collectée par des composants optoélectroniques.
- SLM à adressages optiques, utilisés si l'information est sous forme optique.

Dans tous les cas, par définition la sortie (du composant SLM) est toujours optique.

1.5.1 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)
5. ...

Mais c'est le développement de modulateurs pour des applications grands publics comme les vidéo-projecteurs qui a permis d'accroitre les travaux de recherches sur les processeurs optiques de reconnaissance de formes que l'on connaît aujourd'hui.

1.5.2 Propriétés des cristaux liquides

L'utilisation des cristaux liquides est répandue (affichage digital, écrans...). La tension appliquée aux électrodes provoque une variation dans l'intensité de la lumière transmise ou réfléchie par l'afficheur. Les cristaux liquides peuvent être vus comme composés de molécules ellipsoïdales. Ces molécules se regroupent entre elles de différentes façons formant 3 classes (ou phases) de cristaux liquides : les nématiques, les smectiques et les cholestériques (figure 1.10) [31].

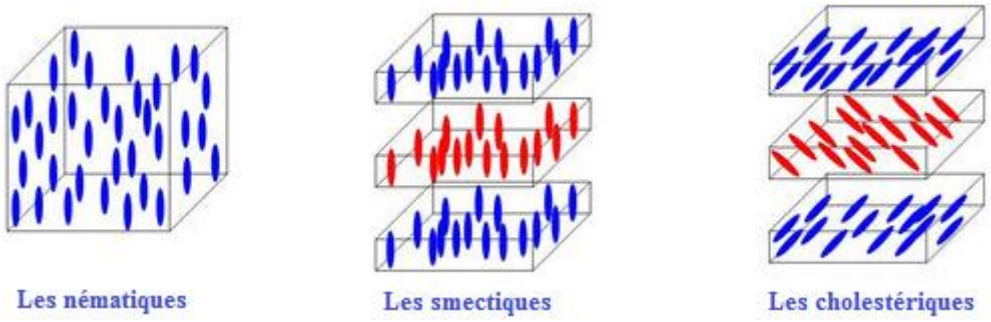


Figure 1.10 Arrangements moléculaires pour différents types de cristaux liquides. Quand il le faut, les couches ont été séparées pour plus de clarté.

Ainsi pour introduire un filtre de compression et de cryptage dans le domaine de Fourier, il faut utiliser des interfaces à plusieurs niveaux de gris. Dans notre laboratoire nous disposons d'un SLM NLC c'est la raison pour laquelle nous allons détailler par la suite le fonctionnement de ce type de modulateur.

1.5.3 Propriétés des NLC :

Les SLM utilisent principalement les cristaux nématiques (NLC) et une classe spéciale des smectiques (C*) appelée les « Ferroelectric Liquid Cristal » (FLC). Il est possible d'imposer des conditions aux limites pour orienter les cristaux liquides nématiques en polissant les surfaces des couches d'alignement dans une direction donnée. Les axes des molécules en contact avec la paroi ont tendance à s'aligner avec les petites rayures du polissage au niveau de la surface. Pour garder une continuité au niveau de l'alignement des axes on peut appliquer une torsion à la cellule comme le montre la figure 1.11-a. En appliquant un champ électrique, on induit un dipôle électrique dans chaque molécule. Le grand axe de la molécule (où le dipôle apparaît) s'aligne avec le champ électrique (figure 1.11-b).

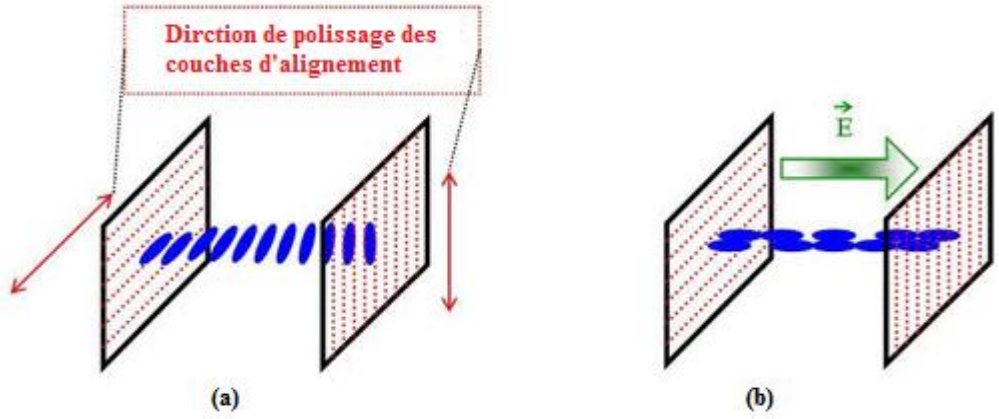


Figure 1.11 (a) Arrangements moléculaires dans une cellule à cristaux liquides lorsque les directions de polissage des couches d'alignement sont perpendiculaires.
(b) Alignement des axes moléculaires avec le champ électrique.

1.5.4 Les 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 I-10 (a)), nous avons un pouvoir rotatoire important.

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

- Exemple de fonctionnement

En l'absence d'un champ électrique (figure 1.12), la lumière polarisée à 45° des axes *xOy* rencontre l'axe de la molécule orienté à la verticale.

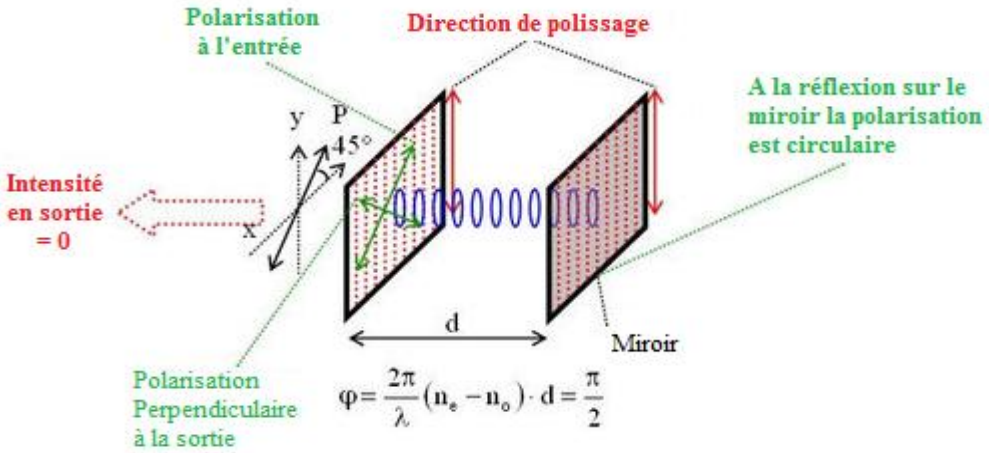


Figure 1.12 En l'absence de champ électrique, l'intensité de la lumière réfléchie par la cellule est nulle.

Elle voit donc le grand ainsi que le petit axe de la molécule. Les composantes du champ lumineux suivant *x* et *y* subissent un déphasage différent (suivant n_e et $-n_o$). Au niveau du miroir au fond de la cellule, la lumière sera polarisée circulairement si on s'arrange pour que le déphasage φ soit égal à $\pi/2$. Ceci est réalisé en choisissant une épaisseur *d* de cellule convenable. Après l'aller-retour (réflexion sur le miroir), la lumière sera polarisée rectilignement et orientée à 90° de la lumière incidente. Elle rencontre le polariseur *P* placé à l'entrée en position croisée. L'intensité sera donc minimale à la sortie de la cellule.

En revanche et en présence d'un champ électrique suffisant, les molécules seront alignées avec le champ électrique appliqué. Les composantes sur *x* et sur *y* de la lumière rencontrent cette fois ci le petit axe de la molécule (voir figure 1.13). Il n'y aura pas de déphasage entre les composantes du champ lumineux. La lumière est polarisée rectilignement en se réfléchissant sur le miroir et reste parallèle à elle-même en arrivant sur le polariseur *P* après l'aller-retour. L'intensité lumineuse en sortie est donc maximale.

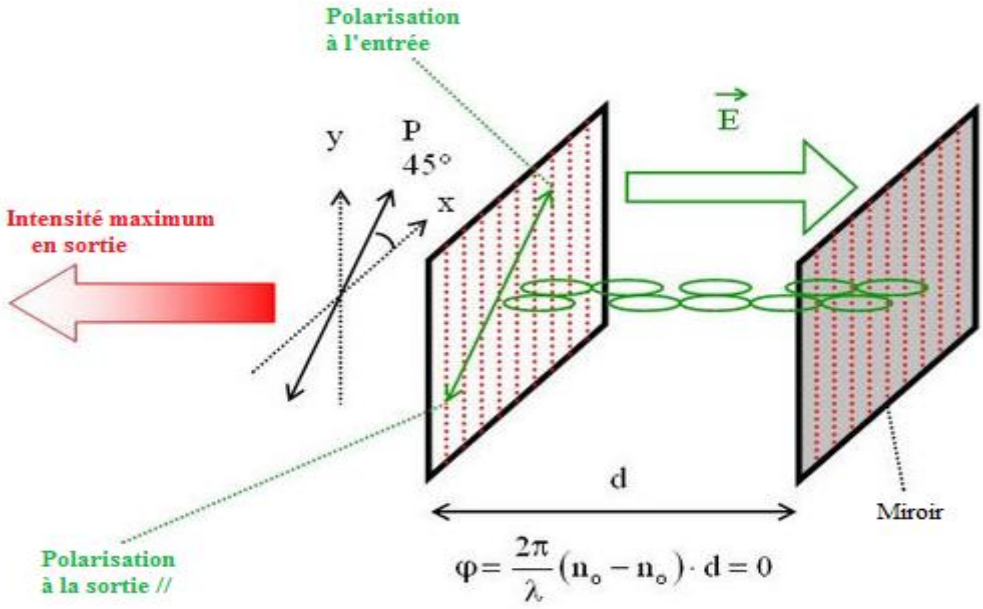


Figure 1.13 En présence d'un champ électrique suffisant l'intensité de la lumière réfléchie par la cellule est maximale.

Si le champ électrique n'est pas suffisant pour faire aligner toutes les molécules dans la cellule, il en résulte une réflexion partielle.

Caractéristiques techniques typiques

- Tension à appliquer : *5 – 10 V*
- Épaisseur des cellules : 1 - 10μm
- Temps de réponse d'alignement des molécules : 50 -100 μs
- Temps de réponse de relaxation des molécules : *20 ms*

Le nombre de pixels ou de cellules dans un SLM (typiquement 600x800), appelée communément et à tort résolution), peut varier selon l'application envisagée. Il faut noter que bien que des modulateurs spatiaux de lumière aient été développés pour une utilisation dans des processeurs optiques, c'est le développement de modulateurs pour des applications comme les vidéo-projecteurs qui a permis les travaux de recherches très nombreux sur les processeurs optiques de reconnaissance de formes au cours des 15 dernières années.

1.6 Conclusion

Nous avons commencé ce chapitre par une présentation du contexte de la thèse. Dans une première partie, nous avons décrit une chaîne classique de télécommunication et isolé les blocs qui nous intéressent à savoir les blocs de codage et cryptage. Ensuite, nous avons introduit brièvement les bases fondamentales du filtrage optique ainsi que les éléments matériels utilisés dans le traitement optique de l'information. En effet, nous avons vu qu'il est possible d'utiliser le montage 4f pour rechercher une information dans le plan de sortie d'un système ; cela va nous permettre par la suite, d'utiliser ce montage pour faire de la compression et du cryptage en adaptant le filtre à introduire dans plan de Fourier. 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

2. Etat de l'art de la compression et du cryptage optique de l'information

Sommaire

2.1 Introduction

Les applications qui utilisent des données multimédias, comme les images, sont de plus en plus présentent dans notre vie quotidienne. Ainsi manipuler les images (stocker ou transmettre,…) devient un enjeu stratégique. Du plus, la protection de ces données est devenue à son tour un domaine attirant pour les chercheurs afin de préserver la confidentialité de ces données. Le volume grandissant de ces données nécessite un temps de calcul de plus en plus grand, ce qui a amené les chercheurs à développer des techniques de compression et de cryptage dédiées à une application donnée et qui sont simples, rapides et efficaces.

Dans ce chapitre, nous allons dresser un état de l'art de quelques méthodes et techniques de compression et de cryptage optique en lien directe avec nos travaux. Nous allons commencer tout d'abord par présenter les méthodes de compression des images. Ensuite, nous présenterons une approche historique du cryptage optique ainsi que quelques techniques développées et validées dans la littérature. Enfin, nous nous attarderons sur différentes méthodes qui traitent simultanément ces deux opérations (la compression et le cryptage des images).

2.2 Compression optique des images

Dans ce travail nous adaptons la définition suivante : la compression est une opération qui consiste à réduire les informations utilisées pour représenter une image sans dégrader ou avec une dégradation contrôlée de la qualité de cette dernière lors de sa reconstruction. Dans la littérature existe deux types de compression avec ou sans pertes d'information.

2.2.1 Intérêt de la compression

Les systèmes de télécommunications utilisent déjà de manière significative les technologies de compression, notamment pour la téléphonie mobile (DCS, CT2, DECT ...). Les techniques numériques de compression/décompression connaissent aujourd'hui un essor très important dans tous les secteurs. Cependant, cette utilisation grandissante exige une très bonne qualité des informations échangées, ce qui pose de nombreux problèmes de transmission et de stockage liés à la quantité et à la qualité d'informations qu'il faut avoir pour garantir des performances suffisantes. Pour gagner aussi bien en temps qu'en mémoire, il est nécessaire d'éliminer les informations redondantes dans les images à transmettre. Ces informations redondantes peuvent être de trois types [78] :

- La redondance spatiale entre pixels ou blocs voisins dans l'image.
- La redondance spectrale entre plans de couleur ou bandes spectrales.
- La redondance temporelle entre images successives dans une séquence vidéo.

2.2.2 Techniques de compression

2.2.2.1 Compression sans pertes

Connue aussi sous le nom '**techniques réversibles'**. En effet, elles n'introduisent pas de pertes dans le contenu informationnel et l'image source peut être restituée à l'identique lors de la décompression. Il existe trois types d'algorithmes de compression sans pertes [78] :

- Codages statistique dont le but consiste à réduire le nombre de bits utilisés pour le codage des caractères fréquents et à augmenter ce nombre pour les caractères rares.
- Substitution de séquences qui sert à comprimer les séquences de caractères identiques.

Ces méthodes qui ne possèdent pas un bon taux de compression, ne nous intéressent pas dans ce travail.

2.2.2.2 Compression avec pertes

Ce sont des '**techniques dites irréversibles**' ; leur résultat étant le fruit d'un compromis entre la qualité du résultat et le taux de compression obtenu. Cela est réalisée sans contrainte de retour possible à l'image originale i.e généralement, ces méthodes consistent à éliminer (à définir selon la méthode de la compression choisie et l'application) certaines informations pour réduire les volumes de données nécessaires reconstruire les images i.e les données à stocker ou à transmettre.

2.2.3 Critères de performance

Différents critères sont présentés et validés dans la littérature pour évaluer les performances des méthodes de compression. Deux types de critères sont généralement utilisés pour une telle évaluation :

1. Critères subjectifs de fidélité.
2. Critères objectifs de fidélité.

- Critères subjectifs de fidélités : basés sur l'évaluation de la qualité par des observateurs humains. Ces méthodes consistent à faire attribuer une note de qualité (Mean Opinion Score ou MOS) par un panel d'observateurs. Cette notation, lourde à mettre en œuvre, est adaptée lorsque les images sont exploitées par des observateurs humains (photo-interprètes).

- Critères objectifs de fidélité : basés sur des équations mathématiques pour évaluer la qualité des images. Dans ce travail, nous nous intéressons à ce genre des critères [78].

Cependant, pour définir ces critères objectifs, il est nécessaire de pouvoir exprimer la perte d'informations entre l'image originale et l'image reconstruite. Pour ces critères de qualité utilisés pour mesurer les performances d'une image nous citons, par exemple : le Rapport signal/Bruit (RSB ou SNR) et l'erreur quadratique moyenne (en anglais MSE) entre l'image d'entrée et l'image de sortie.

- L'erreur quadratique moyenne MSE est définie par l'équation (11)

$$MSE = \frac{1}{NXN}\sum_{i=1}^{N}\sum_{j=1}^{N}\left|I_d(i,j) - I\ (i,j)\right|^2 \qquad (11)$$

Où I_d et I représentent l'image d'origine et l'image reconstruite de taille N x N, i *et* j sont les cordonnées dans le plan de l'image.

- L'autre critère objectif cité plus haut est le rapport signal sur bruit de l'image reconstruite PSNR (en anglais **P**eak **S**ignal to **N**oise **R**atio). Il est défini par l'équation (12) :

$$PSNR = 10\log 10\frac{d^2}{MSE} \qquad (12)$$

d représente la valeur d'intensité maximale de l'image. En utilisant des images en niveau de gris, les valeurs sont ainsi codées sur 8 bits et dans ce cas de figure $d \leq 2^8\text{-}1$.

Dans notre étude, nous avons fait le choix d'utiliser ces deux critères le MSE et PSNR pour évaluer la qualité des images reconstruites en sortie de notre système.

2.3 Justification du choix otique

Dans ce paragraphe, nous rappelons brièvement notre choix de réaliser un système de compression et de cryptage implantable optiquement. En effet, nous pouvons justifier ce choix par le fait que le traitement numérique des images nécessite un temps de calcul très élevé ainsi qu'un espace de stockage très grand. De plus, l'image est à l'origine optique, or son traitement s'effectue le plus souvent devant l'écran d'un ordinateur. Cette origine a amené les chercheurs et nous aussi à s'intéresser aux techniques de compression et de cryptage optique des images car l'optique cohérente permet de traiter l'image dans sa globalité et avec un parallélisme massif.

2.4 Méthodes de compression optiques des images

Nous commençons cette partie en décrivant différentes techniques de compression optique développées ces dernières années pour réduire la taille de l'information à stoker ou à transmettre. Comme ses semblables numérique le souci majeur, de ces méthodes de compression optique, est de proposer des techniques permettant de réduire au minimum la quantité d'information afin d'obtenir une bonne qualité de reconstruction pour une application donnée (holographie, corrélation, stockage d'images, transmission d'images, …).

- **Méthode 1**

Le principe de la technique proposée par [35, 36] (figure 2.1) consiste à regrouper les spectres des différentes images (issues d'une séquence vidéo par exemple) à comprimer selon un critère bien défini. Auparavant, les auteurs de [36] rajoutent un terme de phase propre à chacun de ces spectres dans le but de séparer les différentes images dans le plan de sortie [11,12] (après avoir réalisé une deuxième transformation de Fourier de ce plan segmenté). Le critère de segmentation utilisé dans [35] compare, pour chaque pixel (k,l), le quotient de l'énergie d'un pixel ($E_i(k,l)$) d'une image donnée (« i ») sur l'énergie totale de cette image dans le plan de Fourier, avec le quotient d'énergies des autres images. La décision d'affecter ce pixel à une image ou à une autre, est prise en fonction des résultats obtenus pour l'ensemble de ces comparaisons (équation 13).

$$\frac{E_i(k,l)}{\sum_{m=0}^{N}\sum_{n=0}^{N} E_i(m,n)} = Max\left(\frac{E_j(k,l)}{\sum_{m=0}^{N}\sum_{n=0}^{N} E_j(m,n)}\right) \quad \forall \quad i \neq j \tag{13}$$

Cette technique présente un inconvénient majeur lorsque les images à comprimer se ressemblent (et par conséquent leurs spectres aussi) comme c'est le cas dans une séquence vidéo. Le degré de dégradation des images avec cette technique dépend donc des images à comprimer et du critère de segmentation utilisé. En effet, le problème vient essentiellement du fait que cette segmentation est locale. Ainsi dans certaines zones importantes et en fonction de la ressemblance des images, il risque d'y avoir beaucoup de pixels "isolés" (un pixel isolé est un pixel provenant d'une image entouré de pixels provenant d'autres images). Ce phénomène des pixels isolés dégrade incontestablement la qualité de l'image, une fois reconstruite.

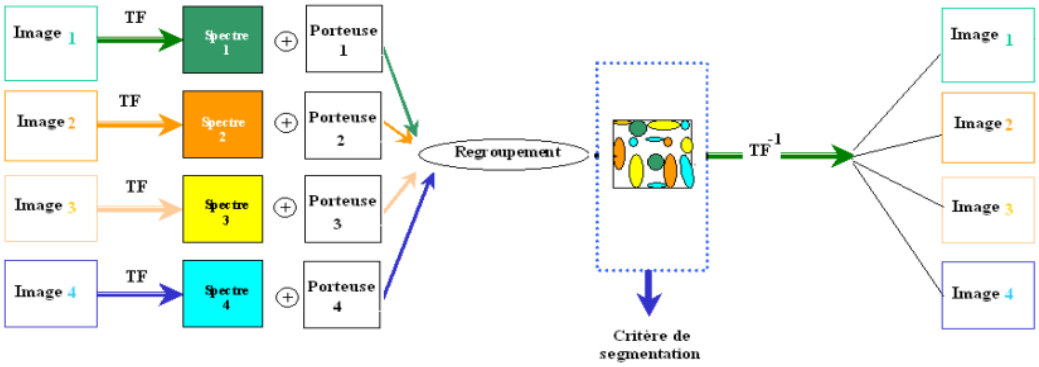


Figure 2.1: Schéma de la méthode de compression et de multiplexage optique par fusion spectrale

Pour surmonter ce problème, les auteurs ont commencé dans [36] une première tentative qui consiste à améliorer la segmentation du plan de Fourier en utilisant différents critères de segmentation. Pour cela, ils ont proposé des critères prenant en compte non seulement l'énergie pour fusionner les différentes informations mais aussi la phase du gradient. Cependant, l'utilisation de ces différents critères sur plusieurs types d'image a montré que le choix des critères n'améliore que très peu la qualité des images en sortie du système de compression. Cela est essentiellement dû au phénomène de chevauchement entre les différents spectres des images à comprimer. Ainsi dans ce travail [37], ils proposent de réorganiser les différents plans de Fourier de manière à éviter que des zones importantes propres à chaque image ne se chevauchent. Cela est obtenu entre-autres en décalant les centres des différents spectres comme cela est montré sur la figure 2.2. Ainsi, en appliquant le critère de segmentation après cette étape de décalage, nous diminuons considérablement le problème de chevauchement et par conséquent nous améliorons la qualité de reconstruction des images.

Le décalage des différents centres dans le plan de Fourier a minutieusement été étudié pour trouver l'emplacement idéal pour une application donnée (cela fera l'objet du chapitre suivant). L'application de cette approche sur une séquence vidéo a permis de montrer le bon comportement de cette technique [37]. Cependant, cette technique nécessite une étude continue des différents plans spectraux des images à comprimer afin de bien sélectionner les zones pertinentes à garder. Cela rend très complexe une implantation tout optique de cette technique. L'enregistrement des différents spectres (amplitude et phase) regroupés dans le plan de Fourier avant transmission, nécessite l'utilisation des techniques comme celles utilisées pour l'enregistrement des hologrammes optiques [12]. Ainsi, par la suite nous allons présenter une technique de compression adaptée à l'enregistrement holographique.

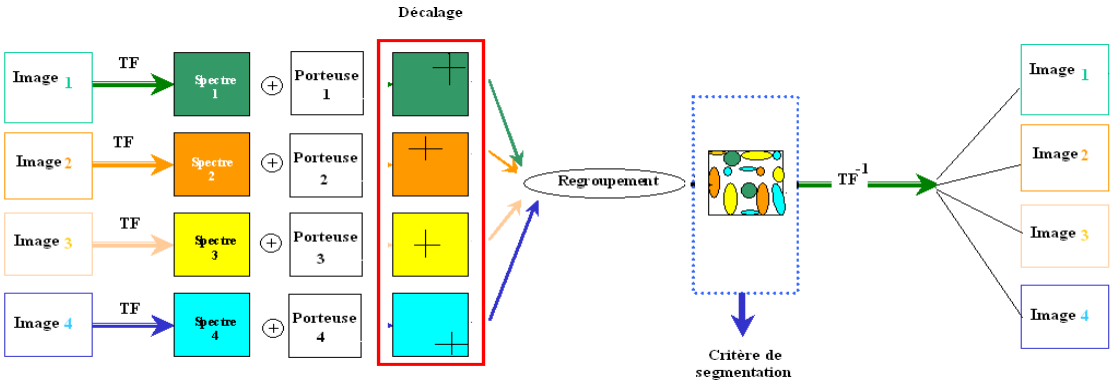


Figure 2.2 Schéma du regroupement appliqué sur l'image avec décalage spectrale

- **Méthode 2**

La méthode proposée en [38] est basée sur une compression des hologrammes **PSI DH** (**P**hase **S**hifting **I**nterferometrry **D**igital **H**olography [39]) incluant des corrélations spatiales afin d'augmenter l'efficacité et les performances de ce genre de méthodes par rapport à d'autres citées dans la littérature (figure 2.3). Ainsi, le front de l'onde propagée possède plus de corrélations spatiales que le front de l'onde dans le plan de la caméra, ce qui augmentera la qualité de la scène reconstruite dans le plan de sortie (reconstruction plane).

L'holographie (Figure 2.3) a largement été étudiée dans la littérature [12,39] dans le but de simplifier et d'améliorer la qualité de son enregistrement sur des composants numériques de type caméra CCD, par exemple. L'amélioration de cet enregistrement permettra ainsi d'augmenter la qualité de la reconstruction (affichage d'une manière optique ou numérique). Le schéma de principe utilisé pour l'enregistrement d'un hologramme (**P**hase **S**hifting **I**nterferometrry **D**igital **H**olography **PSI-DH)** est présenté sur la figure 2.3. L'onde issue d'un laser est divisée en deux parties grâce à un cube séparateur. La première partie du faisceau éclaire l'objet qu'on désire traiter et la deuxième partie est réfléchie sur un miroir qui dans ce montage a pour but de changer la phase de l'onde référence.

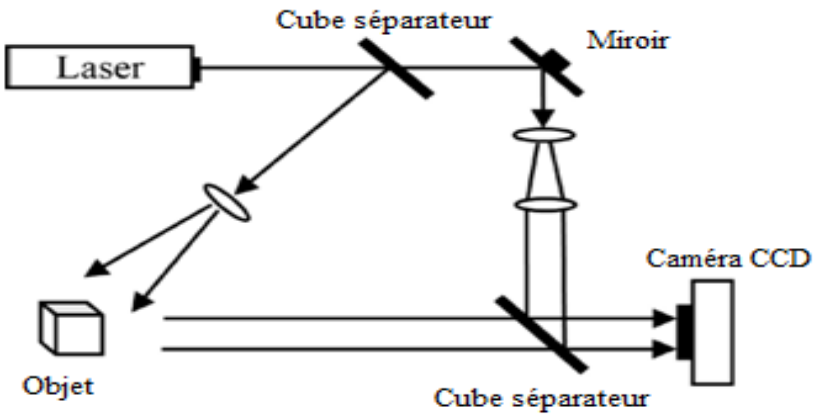


Figure 2.3 : Schéma principe de le l'enregistrement numérique d'un hologramme PSI [15].

Pour avoir un bon taux de compression sans pour autant perdre en qualité de reconstruction Darakis et all propose [38] d'utiliser la technique de quantification réalisant la technique appelé (K-means quantization) développé dans [40]. Les résultats donnés par les auteurs montrent très bien les bonnes performances de cette compression dans le plan de reconstitution. En effet, ils ont montrée une nette amélioration de la qualité reconstruite de l'objet par rapport aux autres techniques comme par exemple la compression directement dans le plan de la caméra.

De plus, une comparaison avec la méthode de compression JPEG2000 a conforté les auteurs dans leur choix. Cette méthode est intéressante car elle permet de réduire considérablement la quantité d'information à enregistrer pour un hologramme tout en gardant une bonne qualité de reconstruction de ce dernier. Mais cette méthode est très difficilement applicable sur des images issues des séquences vidéo.

- **Méthode 3**

Les auteurs de l'article [41] ont mis en avant un problème très crucial lié à la grande taille de l'hologramme PSI (à enregistrer et/ou à transmettre) nécessaire pour avoir une bonne qualité de reconstruction d'objet 3D (figure 2.4-a). En effet, pour des applications de corrélation 3D [42,43], il est nécessaire de pouvoir reconstruire l'image avec une bonne qualité après stockage et/ou transmission afin d'avoir une bonne performance d'identification et de reconnaissance.

Les hologrammes sont très gourmands en taille ; cela rend très difficile le traitement temps réel pour une recherche et une identification des objets 3D existants dans une scène. Une solution pour résoudre ce problème est de comprimer ces hologrammes avant leur stockage ou transmission (figure 2.4).

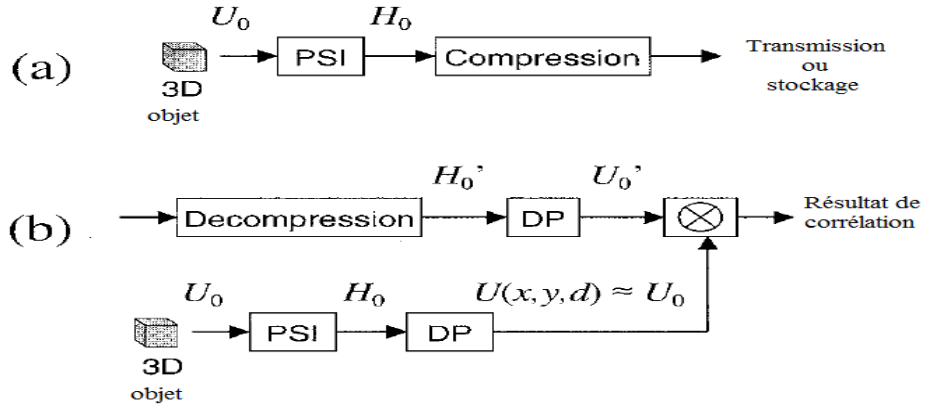


Figure 2.4 Illustration de la technique de compression des hologrammes PSI

Pour ce faire les auteurs [41], commencent par utiliser une technique de compression sans perte appelée « Lossless data compression » en garantissant que la scène reconstruite « U' » est identique à celle d'origine U. Pour réaliser cette compression (avant l'enregistrement de l'hologramme PSI) les auteurs ont utilisé et testé quatre techniques : Huffman [44], Lempel-

ziv [45], Lempel–Ziv–Welch [46] et Burrows–Wheeler [47]. Les résultats de cette méthode en appliquant ces différentes techniques sur plusieurs scènes contenant des objets différents, montrent bien les faibles performances de ces algorithmes. Ainsi les auteurs ont exploré d'autre type de compression comme la compression "Resampling". Cependant, cette technique introduit aussi une baisse de performances, comme cela est montré par les auteurs et nécessite le réajustement de la distance « z » ; la distante à laquelle il faut reconstruire la scène.

- **Méthode 4**

En bénéficiant des avantages et de la simplicité qu'offre la technique de compression JPEG [48], les auteurs dans la référence [49] ont proposé et validé un montage permettant d'implanter optiquement la méthode de compression JPEG (figure 2.5). Sachant que la compression JPEG est basée sur la transformation en cosinus discrets « DCT » (Discrete Cosine transform) les auteurs ont utilisé, pour proposer ce montage optique, la similitude qui existe entre cette dernière et une autre transformation (la TF) qui est implantable optiquement avec une simple lentille convergente. Pour cela, ils ont trouvé les formules de passage permettant de réaliser la DCT avec une TF [50].

Pour ce faire, ils commencent par dupliquer l'image à comprimer placée en entrée du montage d'une manière spéciale, permettant d'éliminer la partie « sinus » dans la transformation de Fourier. Ensuite, en utilisant des hologrammes de normalisation, ils ont réussi à proposer un montage tout optique permettant de réaliser la DCT optiquement (figure 2.5-a). Toutefois, ils ont utilisé un simple filtre passe-bas pour réduire les informations nécessaires pour la reconstruction de l'image, réduisant ainsi la taille de l'information nécessaire pour le stockage et/ou la transmission. Pour la reconstruction de l'image (décompression), ils proposent le montage présenté sur la figure 2.5-b qui comporte les étapes inverses utilisées dans le montage de la figure 2.5-a.

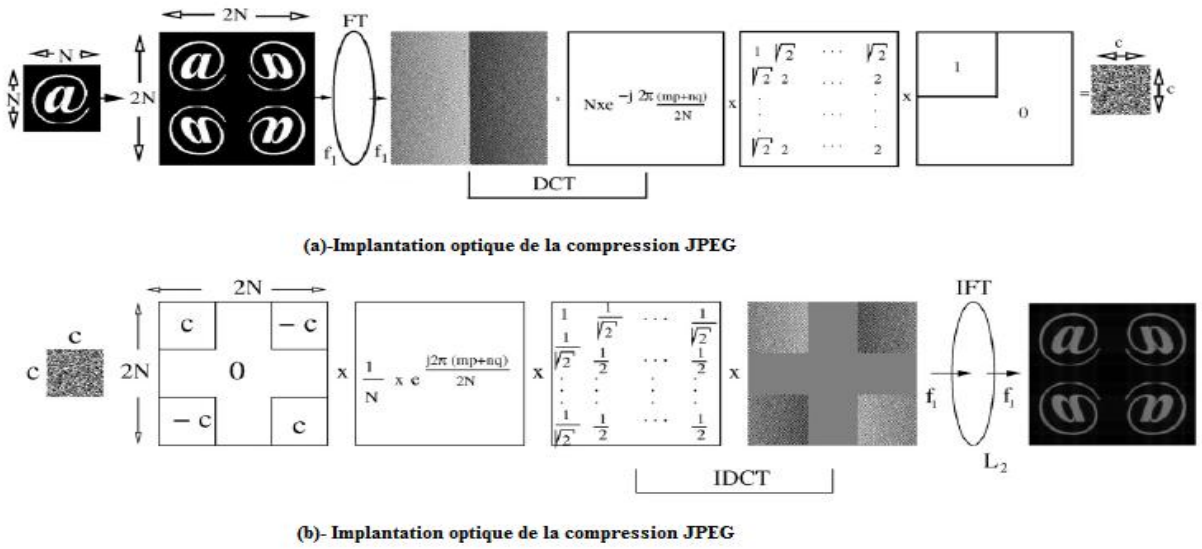


Figure 2.5 Schéma synoptique de l'implantation optique de compression et de décompression JPEG

Pour valider leur montage, ils l'ont testé, par des simulations numériques, sur des images binaires puis sur des images à plusieurs niveaux de gris. Les bons résultats obtenus (un très fort rapport signal sur bruit de l'image reconstruite avec un très grand taux de compression ont permis aux autres [50] d'adapter leur technique pour comprimer des images couleurs. Pour cela, ils ont utilisé l'espace colorimétrique appelé (RGB) pour décomposer l'image couleur (image à comprimer) en ses trois composantes de base, puis d'appliquer sur chacune de ces composantes leur montage optique (Figure 2.6).

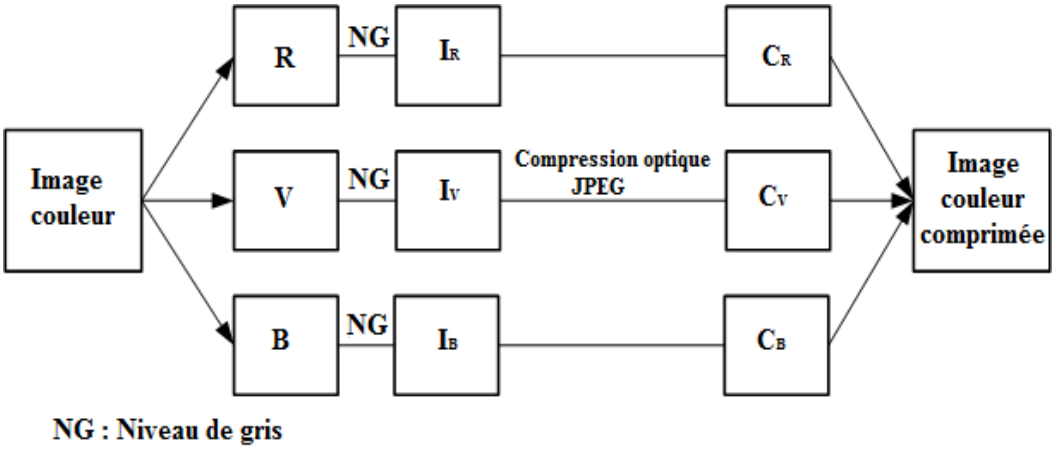


Figure 2.6 : Principe de la compression optique des images couleurs en utilisant la méthode de séparation des couleurs de base (Rouge, Vert et Bleu).

Malgré les très bons résultats obtenus par des simulations numériques, les auteurs n'ont proposé qu'une implantation partielle de leur technique (la partie décompression). En effet, une implémentation complète de la méthode compliquera sérieusement le montage optique nécessitant l'utilisation de plusieurs modulateurs spatiaux de lumière avec tous les problèmes optiques que cela peut engendrer (alignement, …).

Après cette brève introduction de quelques méthodes de compression, nous allons présenter dans la partie suivante le principe du cryptage optique.

2.5 La cryptographie

La cryptographie est la science qui a pour but de garantir la protection des communications transmises sur un canal public contre les différents types d'adversaires. Cette protection des informations se définit en termes de confidentialité, d'intégrité et d'authentification de message et/ou de personnes.

- **La Confidentialité** garantit que les données transmises ne soient pas dévoilées à une tierce personne.

- **L'intégrité** assure que ces données n'aient pas été modifiées entre l'émission et la réception.
- **L'authentification** de message assure qu'il provient bien de la bonne entité et de la bonne personne (aussi appelée identification).

2.5.1 Historique

La cryptographie est une science très ancienne qui date de 1900 ans avant Jésus-Christ. Des recherches indiquent qu'un scribe égyptien a employé des hiéroglyphes non conformes à la langue pour écrire un message. De ce temps-là et au long de l'histoire, la cryptographie a été utilisée exclusivement à des fins militaire.

Une des premières techniques cryptographiques est le chiffrement par transportation ; pour chiffrer un message l'ordre des lettres du message original, est permuté. Pour le déchiffrer, il suffit d'appliquer la méthode inverse. Un des premiers exemples connus d'un tel chiffrement est appelé bâton de Plutarque. Elle était utilisée au cinquième siècle avant Jésus-Christ par les grecs. Il s'agit d'un bâton, autour duquel est enroulée une lanière de cuir. L'expéditeur écrit son message sur la lanière, puis une fois terminé la déroule et l'envoi. Le récepteur enroule à son tour la lanière reçue sur un bâton de même diamètre, ce qui lui permet ainsi de retrouver le texte original.

Une autre technique appelée chiffrement par substitution consiste à changer l'alphabet utilisé pour chiffrer un message. Elle était déjà utilisée du temps des romains sous le nom de « chiffrement de César ». Pour chiffrer un message, il faut décaler de trois lettres dans l'alphabet chaque lettre du message à transmettre. Le processus de déchiffrement consiste à décaler chacune des lettres de trois positions dans le sens inverse de l'alphabet. Par exemple sur l'image de la figure 2.7 la lettre de l'alphabet B devient E dans le texte chiffré.

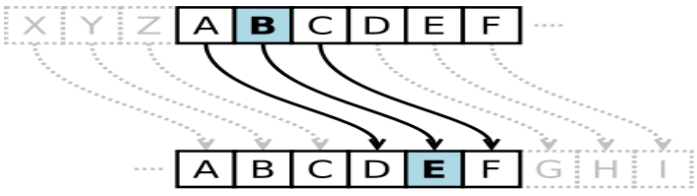


Figure 2.7 Chiffrement de César

Dans la figure 2.7, l'alphabet clair est présenté dans l'ordre normal et l'alphabet chiffré est décalé de trois caractères, et donc B devient E dans le texte codé. Le chiffrement de Vigenère (XVI^{ème} siècle) est un autre chiffrement par substitution. Il s'agit d'une forme plus évoluée du chiffrement de César de sorte que l'on applique 26 chiffrements de César dans un certain ordre. Cet ordre correspond à un mot ou une phrase connue de l'expéditeur et du récepteur du

message. Cette information partagée constitue une clé qui permet d'effectuer dans le bon ordre les différents chiffrements de César. Ainsi, la même clé permet à la fois de chiffrer et déchirer un message.

Pendant la seconde guerre mondiale, les allemands mirent au point la machine « ENIGMA». Celle-ci permettait de chiffrer un message grâce à un dispositif électromécanique qui, avec une clé donnée, réalisait une certaine combinaison de substitutions poly-alphabétiques et de transpositions. Ainsi les allemands pensaient communiquer des informations en toute sécurité à leurs troupes. Mais les alliés, sous la direction d'Alan Turing, mirent au point « COLOSSUS », un des premiers ordinateurs qui a permis de déchiffrer les messages générés par « ENIGMA ».

Historiquement, la plupart des systèmes cryptographiques se sont fondés sur le secret total du processus de chiffrement et de déchiffrement. Cependant, dans les 60 dernières années, il a été réalisé que les systèmes de sécurité reposant fondamentalement sur le secret du mécanisme de chiffrement souffrent de sérieuses limitations. Ceci a été réalisé après la rupture de code allemand d'enigma pendant le début des années 40 [51,52].

En 1979, Whitfield Diffie et Martin Hellman [53] ont inventé le concept d'un système cryptographique à clé publique. La théorie de ce système a marqué le début de la cryptographie moderne. Ils ont aussi inventé le premier standard de l'algorithme DES (Data Encryption Standard). Cet algorithme est devenu aujourd'hui populaire grâce aux résultats des travaux effectués sur la cryptographie quantique par les chercheurs Charles H.Bennett et Gilles Brassard en 1990. En 2000, un autre algorithme a remplacé celui du DES et est connu sous le nom de l'algorithme AES l'acronyme de (Advanced Encryption Standard). Il a été créé par Johan Daemen et Vincent Rijmen. C'est une technique de cryptage à clé symétrique. Il est le résultat d'un appel à contribution mondiale pour la définition d'un algorithme de cryptage ; appel issu de l'institut national des standards et de la technologie du gouvernement américain (NIST).

De nombreuses autres techniques furent aussi inventées récemment comme le tatouage (en anglais (*watermarking*). Une technique qui permet de dissimuler le copyright d'une image sans qu'il n'apparaisse sur l'image.

Le cryptage se fait généralement à l'aide d'une clé de cryptage et le décryptage avec une clé de décryptage. On distingue généralement deux types de clés privées ou publiques.

2.5.2 Cryptage à clé privée

Le cryptage à clé privée, aussi appelé cryptage symétrique ou cryptage à clé secrète, consiste à utiliser la même clé pour le chiffrement et le déchiffrement [54].

Si A veut envoyer un message à B, tous deux doivent au préalable s'être transmis la clé. Celle-ci est identique chez l'émetteur et le destinataire du message. Les deux parties doivent se communiquer la clé à un moment ou à un autre, ce qui constitue un risque non négligeable

d'interception. Elle peut servir pour plusieurs messages ou être modifiée à chaque échange. Dans le premier cas, elle repose sur la confiance en l'utilisateur [55].

Les systèmes à clé privée posent un second problème. Si une clé différente est mise en œuvre pour chaque paire d'utilisateurs du réseau, le nombre total des clés augmente beaucoup plus rapidement que celui de protagonistes. Dans les années 20, Gilbert Vernam et Joseph Marlogne mettent au point la méthode d'un masque jetable (one time pad), basée sur une clé privée générée aléatoirement, utilisée une et une seule fois puis détruite. Plus tard, le Kremlin et la Maison Blanche sont reliés par le fameux téléphone rouge, dont les communications étaient cryptées par une clé privée selon la méthode du masque jetable. La clé était alors échangée au moyen de la valise diplomatique (jouant le rôle de canal sécurisé).

Dans les années 80, Claude Shannon démontra que pour être totalement sûr, les systèmes à clef privée doivent utiliser les clefs d'une longueur au moins égale à celle du message à chiffrer, ce qui pose problème [56]. De plus, le chiffrement symétrique impose d'avoir un canal sécurisé pour l'échange de la clé, ce qui dégrade sérieusement l'intérêt d'un tel système de chiffrement.

2.5.3 Cryptage à clé publique

Le cryptage à clé publique est basé sur le principe que seule l'opération de décryptage doit être protégée par une clé gardée secrète. Le cryptage peut parfaitement être exécuté à l'aide d'une clé connue publiquement, à condition, bien sûr, qu'il soit virtuellement impossible d'en déduire la valeur de la clé secrète. On parle alors de " cryptographie asymétrique ". Les deux inventeurs de cette technique Whitfield Diffie et Martin Hellman butent sur la difficulté de proposer un véritable cryptosystème à clé publique ; la solution vient du MIT en 1978, avec la publication d'un procédé de cryptage mettant en œuvre les idées de Diffie et Hellman [57]. Ils constatent que la clé publique permet le transport des clés conventionnelles, qui ne repose pas sur l'existence d'une hiérarchie cloisonnée. C'est bien ainsi que fonctionne le système actuellement.

Ils savent également qu'un système de chiffrement peut être utilisé comme mode d'authentification : c'est le principe de l'I.F.F. (Identification Friends and Foes), mis au point dans les années 1950 par l'armée de l'air américaine, qui identifie les appareils amis par leur capacité à déchiffrer un message choisi au hasard et inclus dans le signal radar. Dans le contexte de la clé publique, pouvoir déchiffrer un message produit la preuve qu'on est en possession de la clé secrète.

Contrairement au mode conventionnel, cette preuve est opposable aux tiers, puisque quiconque peut vérifier par chiffrement public qu'on restitue le message initial. On réalise l'analogue d'une signature manuscrite liant un document à son auteur. C'est précisément ce mécanisme de signature numérique qui se met en place aujourd'hui pour les besoins du commerce électronique.

2.6 Quelques méthodes de compression et de cryptage optique

- **Méthode 1 (Javidi + Godail + Refregier)**

A l'origine de ces travaux, nous trouvons la référence [2]. Leur technique est basée sur un montage très utilisé optiquement qui n'est autre que le montage 4f [12](figure 1.2). Cette technique consiste à crypter une image placée dans le plan d'entrée du montage 4f (Figure 2.8-a) en modifiant sa répartition spectrale. Pour ce faire, ils proposent de multiplier le spectre de l'image à crypter par un masque de phase aléatoire : clé de cryptage. Cependant dans la première version de cette méthode optique, seulement la phase du spectre de l'image est cryptée en laissant l'amplitude en clair.

Afin d'augmenter le niveau de sécurisation de cette méthode, une version optimisée est proposée et validée par les auteurs de la DRP « double random phase » figure 2.8-b [58]. Cette extension consiste à multiplier l'image par une première clé (un premier masque de phase) puis de multiplier le spectre de ce produit par une deuxième clé de cryptage (un deuxième masque de phase). Ensuite une deuxième transformation de Fourier est réalisée pour retrouver l'image cryptée dans le domaine spatial (équation-13). L'utilisation de deux clés de cryptage, une en entrée et une dans le domaine de Fourier, nous permet l'obtention d'un bruit aléatoire très dense qui vient se greffer à l'image cible en sortie du montage 4f assurant le cryptage de cette image.

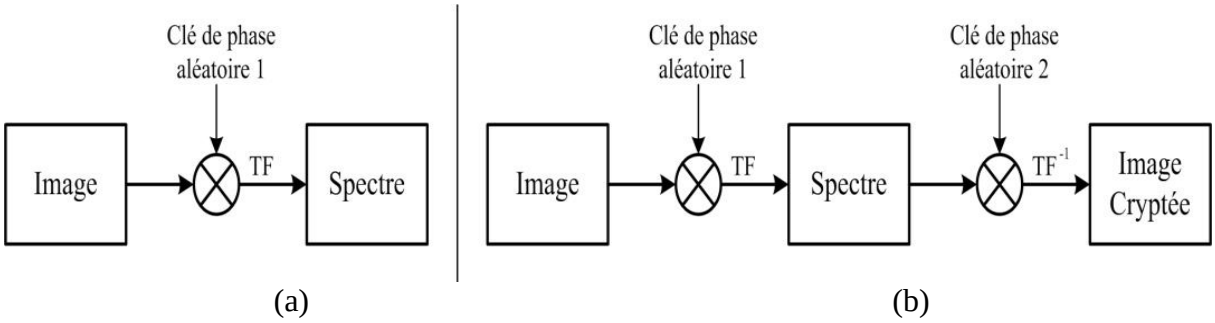


Figure 2.8 Schéma synoptique du système DRP (Double Random Phase)

La simplicité du principe de cette méthode a incité une large utilisation de cette technique dans la littérature. Cependant, elle n'offre pas un très bon taux de cryptage [73]. En effet, l'attaque la plus dangereuse pour ce genre de méthode se produise si le pirate a accès au système. Dans ce cas, il suffit qu'il choisisse comme image à l'entrée du système un « Dirac ». Ainsi, dans le plan de Fourier du système nous trouvons donc le spectre d'un « Dirac » multiplié avec le deuxième masque de phase. En sortie du système, nous avons la transformation de Fourier du deuxième masque de cryptage. Il suffit donc de réaliser une

transformation de Fourier inverse pour trouver cette deuxième clef de cryptage. Ainsi le système est complément craqué.

A coté de ce cas désastreux, Y. Frauel et all ont étudié avec détails [59] un large panel d'attaques afin de montrer les avantages et les faiblesses de cette technique DRP. De plus, ils ont proposé quelques conseils pour augmenter le taux de cryptage comme par exemple l'utilisation de clés de cryptage à très grande taille et l'obligation de les changer très souvent.

- **Méthode 2 (Multiple encoding retrieval for optical security)**

Parmi les différentes technique proposées pour augmenter le taux de cryptage du système utilisant deux clés de phases aléatoires, nous allons nous intéresser à celle proposée par Barrera et al [60] (figure 2.9). Ils proposent de crypter l'image par multiples étapes de phase aléatoire avec une opération de multiplexage. L'image réelle est enregistrée dans un multi-registre appelé (encodegram). Pour reconstruire l'image, ils proposent d'utiliser des masques de phase aléatoires appropriés (RP_1 et RP_2) et un protocole pour récupérer l'image d'origine.

Afin d'augmenter le niveau de sécurisation de l'image cryptée et de créer une confusion pour les intrus, ils rajoutent au multi-registre une fausse image cryptée avec différent teneurs [60]. Cette fausse image n'a qu'un petit effet pour retrouver l'image décryptée d'origine, en raison de la propriété spécifique de ce protocole.

Pour décrypter l'image d'origine, il est nécessaire d'appliquer le protocole inverse pour les deux cyphertexts [60], un pour le multi-registre (encodegram) contenant l'image cryptée d'origine et la fausse image et l'autre processus pour aider à retrouver la clé de phase aléatoire et en conséquence décrypter l'image originale.

Cette méthode présente un schéma de cryptage simple et performant utilisant une phase d'image virtuelle pour camoufler le masque cryptage original et une technique de décryptage optique robuste. Le système proposé ne souffre pas des termes d'autocorrélation. Cependant, ces termes contribuent aux propriétés de cryptage.

De plus, la présence de la clé de décryptage dans le système peut causer une attaque par un itinéraire alternatif. Des nouvelles règles d'affectation peuvent améliorer le niveau de sécurité de la clé de décryptage de ce système. Ils présentent ces règles d'une manière appelée (encodegrams) basée sur une opération de multiplexage secrète.

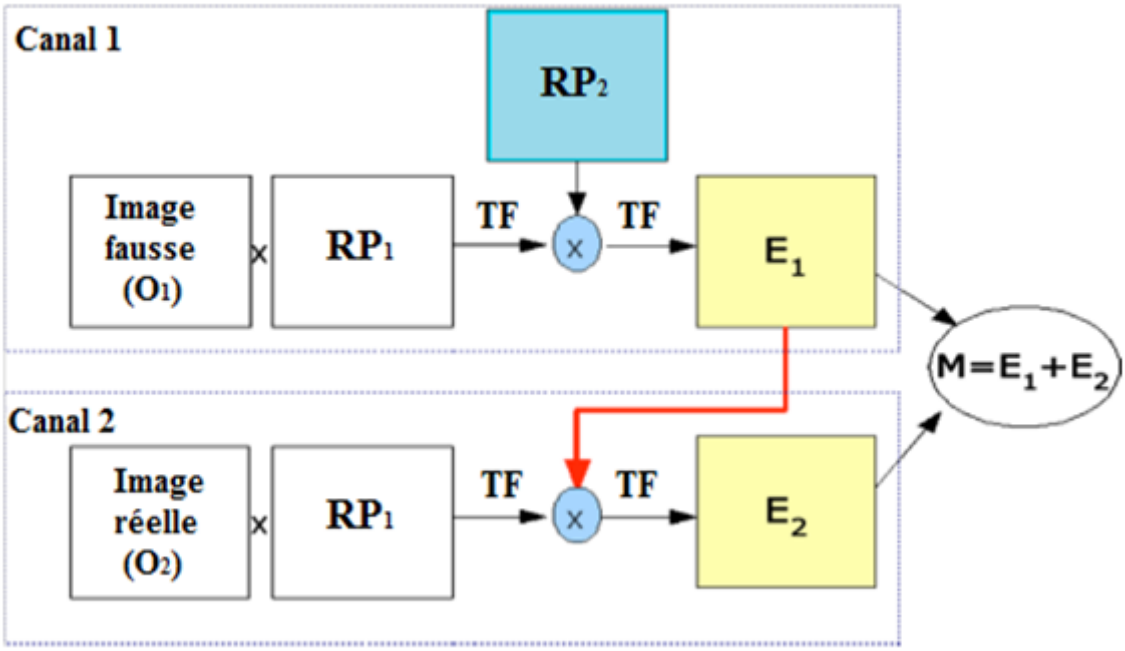


Figure 2.9 Diagramme synoptique de la méthode 2 (Multiple encoding retrieval for optical security)

- **Méthode 3 (cryptage d'images couleurs utilisant un corrélateur JTC)**

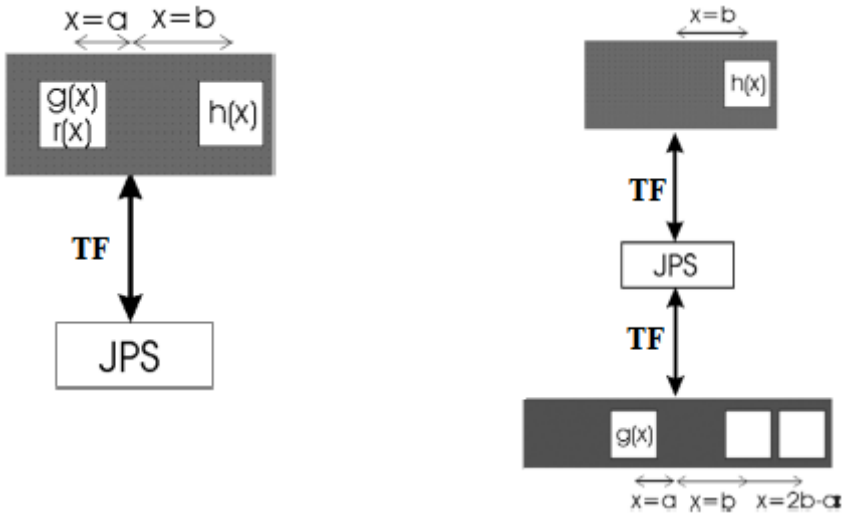
Dafne Amaya et all décrivent dans leur article [71] une technique de cryptage des images couleurs basée premièrement sur l'utilisation des clés de phase aléatoire pour crypter séparément chacune des couleur de base (RGB) que constitue l'image couleur cible et sur une opération de multiplexage des longueurs d'onde. Pour se faire ils ont adapté le montage optique largement utilisé d'un corrélateur JTC [74,75].

Dans ce paragraphe, nous allons exposer la technique proposée par Amaya et all [71], afin d'avoir une idée générale sur les méthodes utilisant ce montage JTC, nous allons décrire leur schéma de cryptage présenté en figure 2.10. Le plan d'entrée éclairé par un faisceau de lumière parallèle contient d'une part (à distance x = a) l'image cible à crypter « g(x) » multipliée par un premier masque de phase aléatoire « r(x) » (appelé input Random phase code) et d'autre part un deuxième masque de phase aléatoire « h(x) ». Ensuite, nous réalisons la transformation de Fourier de ce plan en utilisant une lentille convergente pour obtenir le spectre crypté de JPS (JPS : **J**oint **P**ower **S**pectrum) (équation 14).

$$JPS(v) = \left| \approx [r(x-a)g(x-a) + h(x-b)] \right|^2 \qquad (14)$$

Cette équation décrit le cryptage JPS éclairé avec une seule longueur d'onde. Pour appliquer cette technique au cryptage des images couleurs les auteurs décomposent l'image

cible couleur en ses trois composantes de couleurs de base : rouge, vert, et bleu. Ensuite, ils cryptent séparément ces trois composantes en introduisant dans le plan d'entrée une seule composante à la fois (rouge ou verte ou bleue). Puis ils multiplexent ces trois JPS ensemble pour les enregistrer sur un seul et même support [71]. Ce multiplexage des longueurs d'ondes est obtenu grâce à la modification de l'éclairage du plan correspondant à la composante de l'image cible introduite dans le plan d'entrée.



(a) : Cryptage (b) : Décryptage

Figure 2.10 Schéma principe de la méthode3 (JPS :Joint Power Spectrum).

En effet, pour décrypter, les auteurs proposent d'utiliser un montage issu d'un corrélateur JTC (figure 2.10-b). Le principe consiste à éclairer, avec une seule longueur d'onde à la fois (rouge, vert ou bleu), un plan contenant à une distance (x=b) la clé de cryptage h(x) utilisée dans la phase de cryptage Ainsi le spectre crypté de JPS est éclairé par H(n)exp(-2piibn). Après une deuxième Transformation de Fourier (TF), nous obtenons en sortie g(x)*r(x) à la distance x=a comme cela est montré dans l'équation (15). Il suffit donc de prendre le module pour retrouver l'image cible décryptée. Cette opération est à répéter trois fois en utilisant les trois longueurs d'onde (rouge, vert et bleu) pour retrouver l'image cible décryptée en couleur.

$$\begin{aligned} s(x) = {} & h(x) \otimes [r(x)g(x)] \bullet [r(x)g(x)] \otimes \delta(x-b) \\ & + h(x) \otimes \delta(x-b) \\ & + h(x) \otimes h(x) \bullet [r(x)g(x)] \otimes \delta(x-2b+a) \\ & + r(x)g(x) \otimes \delta(x-a). \end{aligned} \tag{15}$$

Les simulations numérique présentés dans cet article montrent bien l'avantage de cette technique par rapport à ses semblables sans le multiplexage des longueurs d'ondes. Elle présente un avantage par rapport à d'autres techniques de cryptage des images couleur comme celles présentées dans [69,70] (la première est basée sur l'utilisation du multiplexage des

longueurs d'ondes et la transformation holographique de Fresnel sans lentilles, tandis que la deuxième est basée sur l'utilisation de la transformation de Fourier fractionnelle (Fractional Fourier Transfrom).

De plus et d'un point de vue implantation optique, la technique présenté par Amaya et all [71] présente deux avantages par rapport à celles basées sur un montage 4f (méthodes à double clés de cryptage aléatoire [58]) ; premièrement pour le décryptage, elle ne nécessite pas la réalisation du conjugué de la clé de cryptage aléatoire et deuxièmement, elle ne nécessite pas une attention particulière d'alignement (problème récurrent du montage 4f) [18]. Cependant, malgré ces nombreux avantages cette technique souffre du problème de gestion de son plan d'entrée [72]. En effet, elle nécessite une grande taille pour contenir à la fois l'image cible de taille NxM pixels et la clé en respectant une distance de (a+b) entre les deux.

- **Méthode 4 (Optical security system employing shifted phase encoded joint transform correlation)**

Une autre application du montage JTC pour la sécurisation des informations est montrée par Nazrul Islam M. et all [61,76]. Dans ce dernier les auteurs proposent un nouveau montage de cryptage et de décryptage basé sur un «Shifted Phase-encoded Joint Transfrorm Correlation» (SPJTC). Ce montage a pour but d'améliorer la qualité des images décryptées en utilisant un simple montage JTC sans décalage de phase. Le schéma de principe avec décalage de phase est présenté en figure 2.11-a. Après la réalisation d'une transformation de Fourier du code « c(x,y-yc) », sa transformation de Fourier est multipliée par la TF d'un masque de phase aléatoire Phi(x,y) dans un premier canal. Dans un second canal ils appliquent une phase décalée de 180 degrés avant de le multiplier par le masque de phase aléatoire. Ensuite, ils repassent dans le domaine spatial en réalisant une TFI inverse, et obtiennent :

- $c1(x,y) = c(x, y - y_c) \otimes \phi(x,y)$ dans un premier canal et (a)

- $c2(x,y) = c(x, y - y_c) \otimes \phi(x,y)$ dans l'autre avec une phase décalée. (b)

Dans ce plan ils rajoutent, dans chaque canal, l'image « t(x, y-yt) » placée à la distance (0, -yt) du centre. Ensuite, ils réalisent séparément une TF de ces deux plans pour obtenir le JPS correspondant à chaque canal. Pour obtenir l'image cryptée s(x,y) (équation a), ils additionnent les deux JPS ensemble comme cela est montré sur la figure 2.11-a, puis ils réalisent une TF inverse. Pour décrypter (figure 2.11-b), ils commencent par réaliser la transformation de l'image cryptée. Puis ils multiplient son spectre avec la TF du masque de phase aléatoire Phi(x,y) et le code (utilisés lors de la phase du cryptage). Ensuite, ils utilisent

un FAF «Fring-adjusted filter» [62] pour minimiser la distorsion pour le cas où $|TF(c(x,y)|^2$ serait différents de zéro ; dans le cas contraire, il n y a pas besoin d'utiliser ce filtre. Enfin une transformation inverse est nécessaire pour obtenir le plan de cryptage (plan de sortie).

$$S(x,y) = 2[t(x,y-y_t) \otimes c^*(x,y-y_C) \otimes \phi^*(x,y) + t^*(x,y-y_t) \otimes c(x,y-y_C) \otimes \phi(x,y)] \quad (16)$$

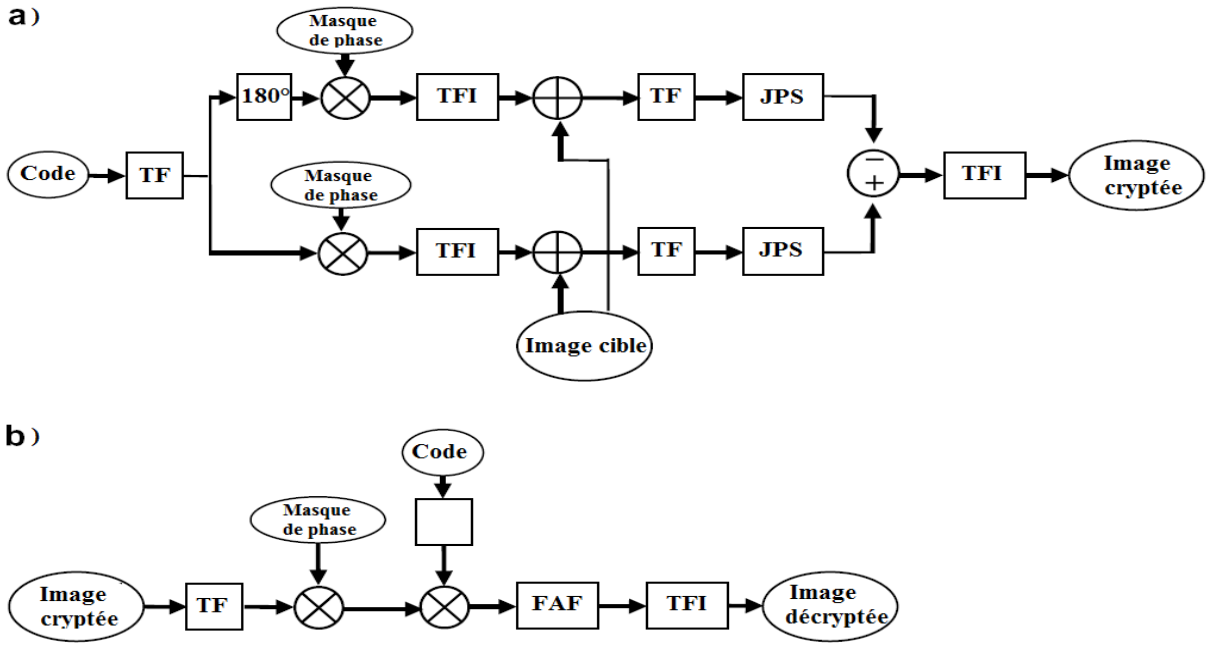


Figure 2.11 : Schéma de principe de la méthode4 (Shifted phase encoded JTC system).

Pour valider et montrer l'efficacité de ce montage les auteurs l'ont testé avec des simulations numériques sur des images binaires, à plusieurs niveaux de gris avec et sans bruit. Les différents tests présentés montrent bien qu'ils ont réussi à valider le montage tout en améliorant la qualité de l'image décryptée par rapport au montage classique sans décalage de phase.

- **Méthode 5**

Une autre application de ce type de codage a été largement étudiée dans la littérature ces dernières année qui consistait à réaliser un double cryptage basé sur l'utilisation des différents masques et l'utilisation de la transformée de Fourier fractionnelle [63]. Afin d'illustrer et d'avoir un aperçu de ce type de codage, nous allons développer la technique présenté par Zhengjum et all [64]. Dans ce papier, les auteurs proposent une autre utilisation de la transformation de Fourier fractionnelle. Leur technique permet de crypter, simultanément et avec un mode itératif, deux images en une seule image/amplitude.

Afin d'augmenter les performances en terme de cryptage de leur approche, ils proposent de rajouter dans leur processeur l'utilisation des phases aléatoires associées aux différentes images à crypter. Pour ce faire, ils regroupent les deux images initiales dans le domaine de Fourier fractionnel. À partir de l'image cryptée et de sa phase, nous pouvons obtenir séparément les deux images originales en utilisant la transformée de Fourier fractionnelle avec deux ordres " α " et " β ". L'algorithme itératif de cryptage est détaillé en figure 2.12. Avec F^{α} défini la transformation de Fourier fractionnelle d'ordre « α ». A_1, A_2 sont les deux images originales à crypter. ϕ_i est la fonction de phases aléatoires associée à chacune des images cibles (images à crypter). Touts les paramètres utilisés dans l'élaboration de cet algorithme peuvent être considérés comme des clés de cryptage supplémentaires.

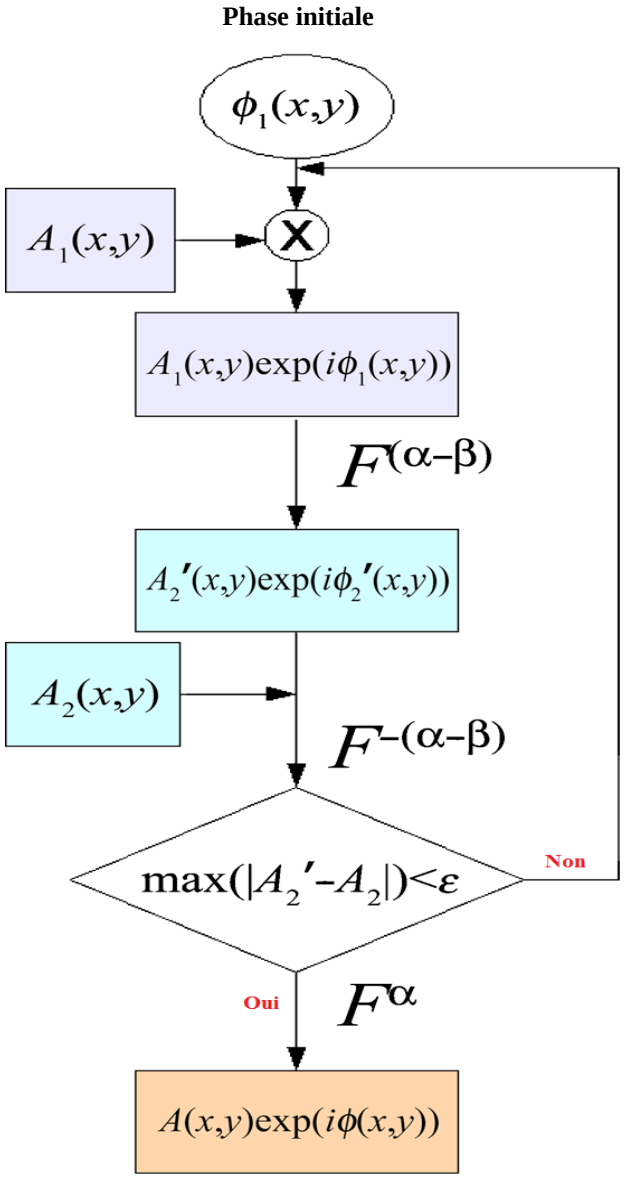


Figure 2.12 Algorithme itératif de cryptage (méthode 5)

- **Méthode 6 (All-optical video-image encryption with enforced security level using independent component analysis)**

Cependant toutes les techniques optiques, citées plus haut, consistent uniquement à sécuriser l'information sans se soucier de sécuriser leur transmission. Ainsi, dans la référence [65] les auteurs proposent une amélioration de ces techniques optiques, permettant à la fois de crypter l'information et le canal de transmission. Pour cela, ils ont développé une nouvelle approche de cryptage basée sur l'utilisation des méthodes de cryptage par filtrage fréquentiel et analyse des composantes indépendantes « ICA » (**I**ndependent **C**omponent **A**nalyses).

Afin d'illustrer le principe de cette technique et présenter son aptitude à augmenter le niveau de cryptage des techniques optiques existantes sans pour autant d'affecter la qualité de l'image décryptée en sortie, prenons un exemple : supposons que nous voulons crypter une séquence vidéo composée de trois images (NxN) pixels (figure 2.13-a). La première étape de cette technique consiste à crypter les différentes images de la séquence avec une des techniques optiques (figure 2.13-b). Ensuite, ils mixent ensemble ces différentes images cryptées (figure 2.13-c) en utilisant un mixeur linéaire (Mix1= $a_{11}D_1+a_{12}D_2+ a_{13}D_3$: avec D_1, D_2, D_3 les trois images cryptées optiquement et a_{11}, a_{12}, a_{13} les différents paramètres de mixage) pour avoir plus des détails, il faut se référer à l'article [65].

Ce mixage linéaire va donner trois autres images cryptées. Ainsi nous obtenons une série d'images cryptées deux fois en utilisant des clés différentes et deux méthodes de cryptages différentes, ce qui a pour but d'augmenter le niveau de cryptage de ces images figure (2.13-d).

Avant de transmettre ces différentes images, considérées comme trois matrices, de (NxN) pixels chacune, et afin d'augmenter davantage le niveau de sécurisation, ils les convertissent en un seul vecteur ligne de taille ($3xN^2$). Ensuite, ils changent l'ordre des différents pixels que constitue ce vecteur en utilisant un critère bien défini (ce critère sera utilisé comme clé supplémentaire de cryptage). Ensuite ce vecteur sera divisé en trois vecteurs et envoyé séparément sur trois canaux différents figure (2.13-e).

Ainsi, quiconque intercepte un de trois messages ne pourra pas remonter à la source et trouver les informations en clair. Pour décrypter l'information transmise, nous devons réaliser les étapes inverses en utilisant les différentes clés de cryptage utilisées par l'émetteur pour crypter la séquence en question figure (2.13-f) ainsi qu'utiliser la méthode ICA [65,77] pour retrouver les trois images mixées.

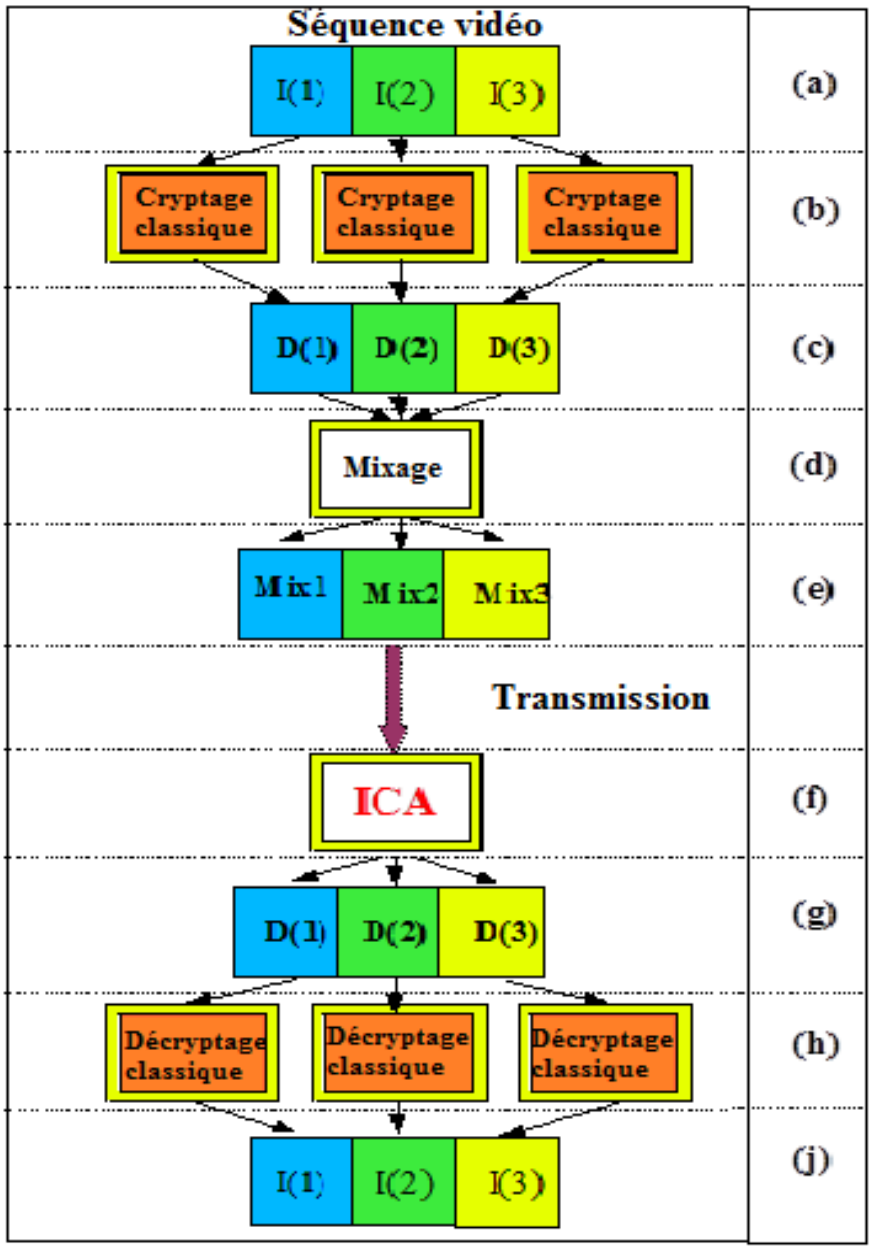


Figure 2.13 Synoptique d'un système de cryptage-décryptage renforcé en utilisant les techniques ICA

De plus les auteurs de l'article [65] ont proposé une implantation optiquement de leur système basée sur l'utilisation du montage « 4f » qui vient s'insérer dans le montage d'un processeur de cryptage optique classique figure 2.14. Le faisceau Laser est divisé en deux en utilisant un cube séparateur. Une première partie vient d'éclairer la première image. Tandis que la deuxième partie illumine la deuxième image. Ensuite, nous multiplions ces images avec leurs coefficients respectifs, en introduisant dans le montage les transmittances de ces coefficients (l'introduction des images et des coefficients dans le montage est réalisé grâce à des interfaces optoélectroniques comme les SLM. En rassemblant les images deux par deux, nous obtenons alors, les images mixées.

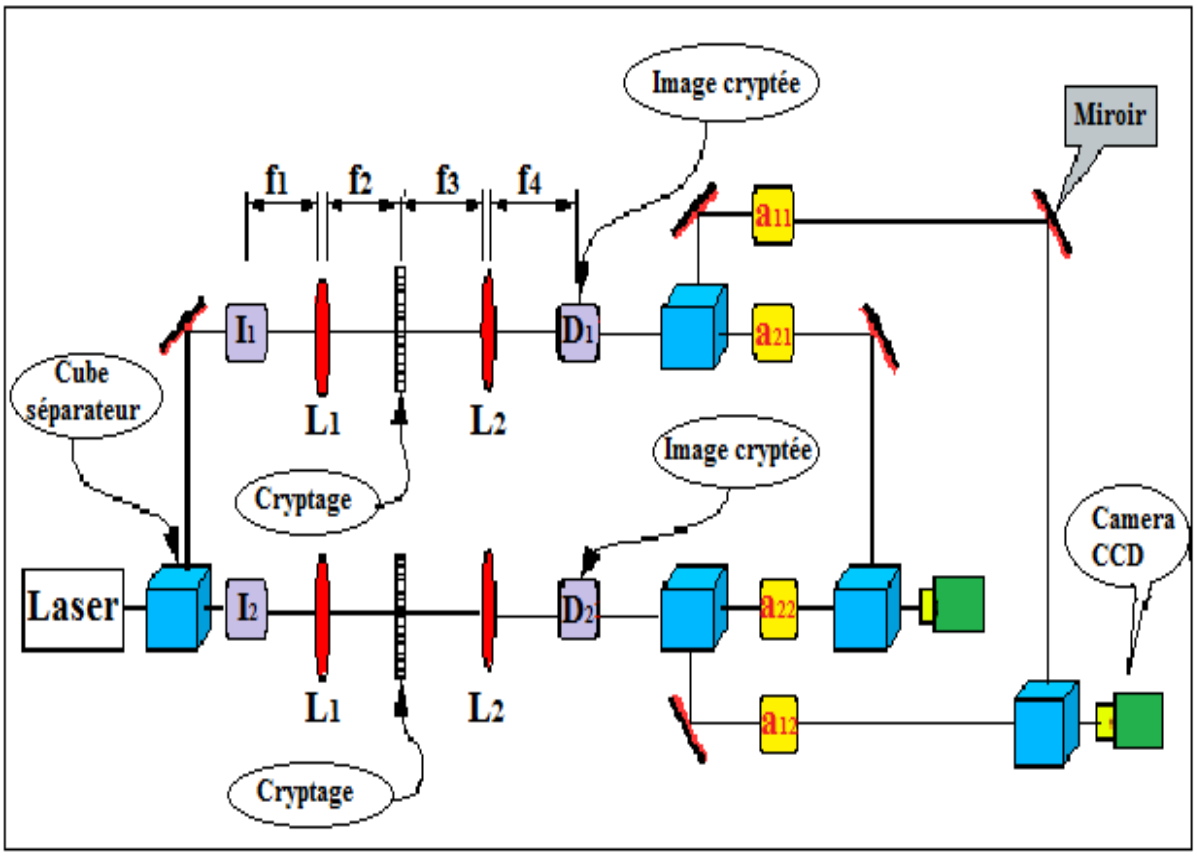


Figure 2.14 : Implantation optique de la méthode (**All-optical video-image encryption with enforced security level)**

Cependant pour utiliser ce système et pour avoir une bonne application de la méthode ICA, il faut respecter la contrainte de créer une version indépendante de ces différentes images. Cela est rendu possible, grâce à la multiplication des différentes images par différents masques aléatoires [66]. Cette multiplication a pour but d'uniformiser les spectres des images et ainsi les rendre indépendantes les unes des autres, même si elles appartiennent à la même séquence vidéo.

2.7 Compression et cryptage optique simultanés

Comme nous venons de le voir, l'intérêt grandissant porté pour échanger les informations rapidement (compression) et faiblement (sécurisé), a nécessité de redoubler d'efforts pour comprimer et pour crypter ces informations.

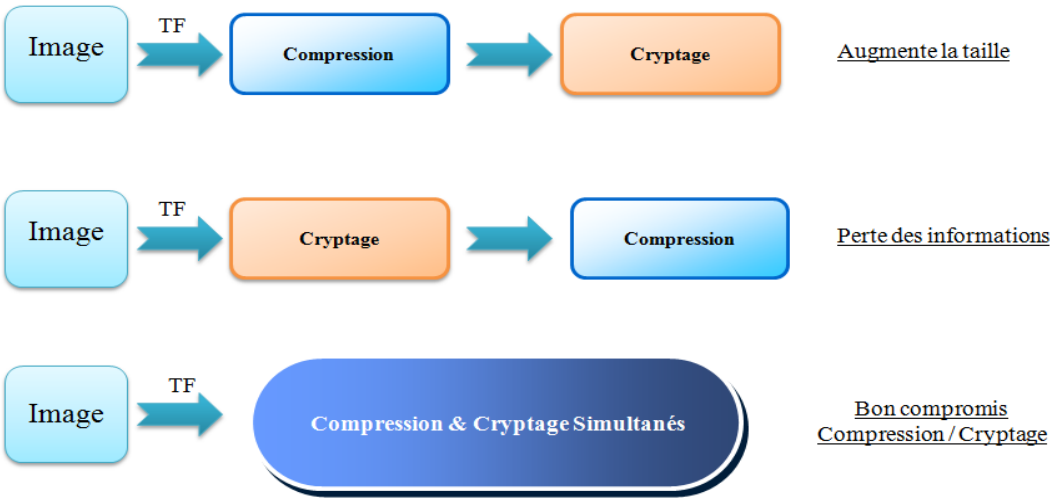


Figure 2.15 Schématisation de techniques de compression et cryptage

Dans cette partie, nous allons nous intéresser à une autre approche développée au sein du laboratoire Isen-Brest. En effet cette approche utilise à la fois le montage optique de la DCT (figure 2.15) et le principe du filtrage fréquentiel [67]. De plus, cette approche permet tout en comprimant les images cibles de les crypter. Ainsi, le cryptage est réalisé d'une manière dépendante de la méthode de compression.

Cette technique de compression et de cryptage constitue une avancée dans ce domaine car les deux opérations en question (compression et cryptage) sont généralement réalisées en cascade et ne tiennent pas compte des contraintes que l'une peut imposer à l'autre.

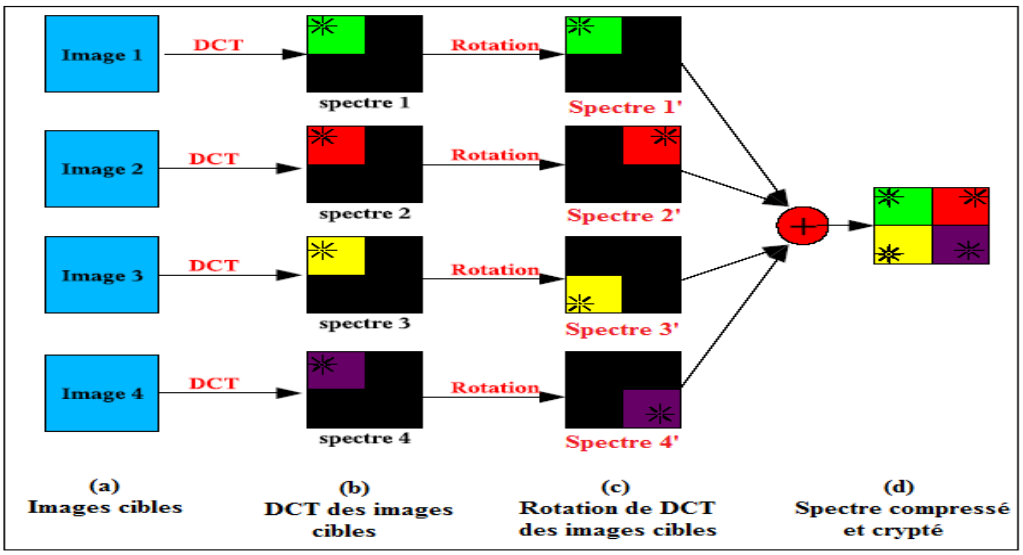


Figure 2.16 Diagramme synoptique de la méthode de compression et de cryptage simultanés

La figure 2.16 présente le diagramme synoptique de cette approche. La première étape consiste à réaliser séparément les DCTs de différentes images cibles (images à comprimer et à crypter). En se basant sur la propriété de DCT, qui permet de regrouper les informations dans le coin haut gauche du spectre, nous appliquons aux différents spectres un filtre passe bas. Après, il suffit de regrouper (par une simple opération d'addition par exemple) ces différents spectres filtrés pour n'en obtenir qu'un seul qui contient toutes les informations nécessaires pour reconstruire toutes les images cibles en sortie.

Cependant, cette technique montre assez vite ses limites avec l'apparition d'un problème de saturation surtout lorsque l'on veut augmenter le nombre d'images à multiplexer ensemble. Cette saturation est dûe au fait que l'on regroupe les différents spectres dans la même zone (coin haut gauche) du plan spectral, d'où la nécessité d'optimiser ce regroupement.

Pour réaliser cette optimisation, nous pouvons remarquer qu'après le filtrage des différents spectres, nous n'utilisons qu'une petite partie du plan spectral, en laissant les autres parties libres. Dans ces parties libres, nous pouvons mettre les autres spectres mais il faut auparavant réaliser une rotation à 90 degrés (figure 2.16-c) à chaque fois pour mieux optimiser le plan spectral et garder le maximum de pixels représentatifs des spectres.

2.8 Conclusion

Dans ce chapitre, nous avons présenté un état de l'art des méthodes et techniques de compression et de cryptage optique les plus citées dans la littérature. Ces dernières présentent des avantages lorsqu'il s'agit de traiter un grand volume d'information grâce au parallélisme qu'offre la lumière cohérente. Les opérations de compression et du cryptage sont souvent réalisés séparément. Dans notre laboratoire nous avons proposé et validé le principe d'une méthode qui réalise ces deux opérations simultanément. Cette méthode est basée sur l'utilisation de la DCT (Discrete Cosine Transform) pour la compression et une approche de cryptage qui utilise plusieurs masques aléatoire pour crypter les images cible.

Deuxième partie

Développement et validation de la méthode

Chapitre 3

3. Nouvelle méthode optique de compression et de cryptage simultanés des images multiples

Sommaire

3.1 Introduction

En se basant sur la forte expérience du laboratoire vision de l'Isen-Brest dans le domaine de la compression et de cryptage optique, nous proposons et validons dans ce chapitre une nouvelle méthode de compression et de cryptage simultanés des images. Cette méthode doit garantir un taux de compression optimal et un niveau de sécurisation élevé. Un premier travail a été proposé par Boumezzough en 2005[68] a permis de valider le principe d'une méthode de compression des images fondée sur une segmentation spectrale spécialement développée dans le laboratoire pour faire de la compression. Fort de cette expérience, dans ce chapitre nous proposons une nouvelle méthode de compression des images basée sur de nouveaux critères et adaptée au cryptage.

3.2 Approche de compression

Comme nous l'avons vu la compression et la décompression nécessitent deux algorithmes. Le premier transforme les données de façon à ce qu'elles occupent moins de place. Le second effectue la transformation inverse pour reconstituer les informations d'origine. Cette compression est jugée selon que le résultat de ces deux transformations permet de retrouver ou pas les données de départ. Dans l'approche de la compression d'images qui nous intéresse dans ce chapitre, il est acceptable de perdre un peu d'information, si cela permet d'obtenir un taux de compression plus élevé. Les images résultantes ne sont donc pas identiques, bien qu'elles soient très proches visuellement des images originelles. On dit alors que c'est une compression avec perte d'informations.

Pour y arriver, notre approche de compression utilise un nouveau critère pour chercher les informations pertinentes dans le spectre de l'image. Ce critère est basé sur l'utilisation de la taille utile du spectre de l'image (en anglais **R**oot-**M**ean-**S**quare-Duration). Cette taille utile (RMS) du spectre représente les pixels qui contiennent les informations importantes de l'image. Ainsi, en ne gardant qu'une partie du spectre, nous pouvons multiplexer un certain nombre de spectres d'image cible et ainsi nous avons une utilisation optimale du produit espace-bande passante (SBWP) dans le domaine de Fourier.

3.2.1 Principe de la méthode de compression par fusion spectrale (MOICE)

Nous allons commencer par un rappel de la méthode de compression et de cryptage simultanés des images (MOICE : Multiple-image Optical Images Compression and Encryption) développé au sein du laboratoire Vision. En effet, cette méthode (MOICE) est basée sur la compression avec perte qui réduit la quantité d'informations à utiliser pour représenter une image. Cette perte contrôlée d'informations conduit à une dégradation mesurée de la qualité de l'image cible après reconstruction. Dans cette thèse, nous nous intéressons aux méthodes susceptibles d'être implantées optiquement. En effet, l'apparition des systèmes optiques travaillant en temps réel a favorisé le développement des méthodes de

compression optique [1]. Parmi ces méthodes, on peut distinguer les méthodes qui exploitent la phase spectrale de l'image.

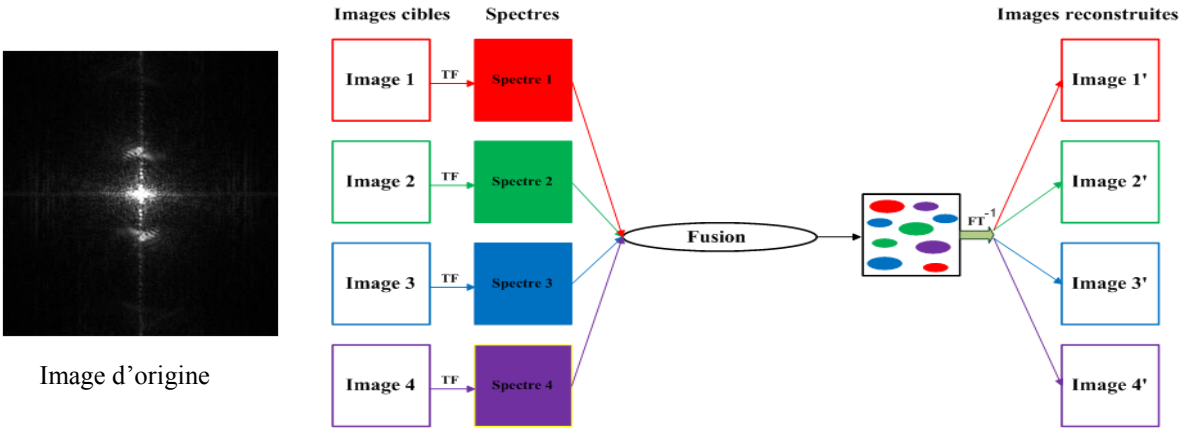
Le principe de base de la méthode développée dans cette partie est inspiré des travaux d'Alfalou et al [8]. Cette méthode consiste à faire la transformée de Fourier des images cibles (figure. 3.1-b) pour obtenir les spectres. Ensuite, nous appliquons une technique de fusion selon un critère bien défini. Puis pour la décompression, nous appliquons le processus inverse.

Le résultat de cette fusion sera un unique spectre contenant les informations des images cibles (compression). Pour ce faire, nous allons nous baser sur le fait que le spectre utile d'une image donnée n'occupe pas l'ensemble du plan de Fourier (figure. 3.1-a). Cette figure 3.1-a montre bien que l'amplitude spectrale d'une image est localisée dans des endroits bien précis du plan de Fourier.

Dans ce chapitre, nous allons nous focaliser sur le choix de ces parties pertinentes ainsi, nous allons utiliser ce constat pour fusionner d'autres informations provenant d'autres images (figure. 3.1-b). Toute la question réside donc dans le choix d'un critère qui permet dans un premier temps, de sélectionner les informations pertinentes pour une image et ensuite les fusionner ensemble.

3.2.2 Compression sans décalages spectral

La figure 3.1-b présente ce principe qui regroupe, dans le domaine spectral, les informations issues de plusieurs images selon un critère de regroupement. En réalisant différents tests et quel que soit le critère de sélection et de fusion utilisé [8, 9], les résultats des simulations de cette approche sont de très mauvaises qualités (table 1 colonne 2). Cela est dû essentiellement au chevauchement entre les différents spectres. Et donc la perte des informations essentielles dans chacune des images cibles.



(a) (b)

Figure 3.1 (a) Exemple d'un spectre d'une image donnée, (b) schéma synoptique de la méthode fusion spectrale

3.2.3 Effet de décalage spectral

Pour minimiser la dégradation de qualité des images reconstruites, liée au chevauchement, nous avons proposé de décaler les centres des différents spectres avant l'application du critère de sélection et de fusion (figure. 3.2-a). Pour ce faire, nous commençons par faire une transformée de Fourier des images cibles pour obtenir leurs spectres. Ensuite, nous décalons le spectre des différentes images afin de réduire au minimum le chevauchement dans les zones utilisées. Par la suite, nous appliquons un critère de fusion adapté (ce critère sera détaillé dans le paragraphe suivant). Ainsi en appliquant un critère de sélection après l'étape de décalage, nous réduisons d'une façon conséquente le problème de chevauchement (figure 3.2-b) et par conséquence nous améliorons la qualité des images reconstruites.

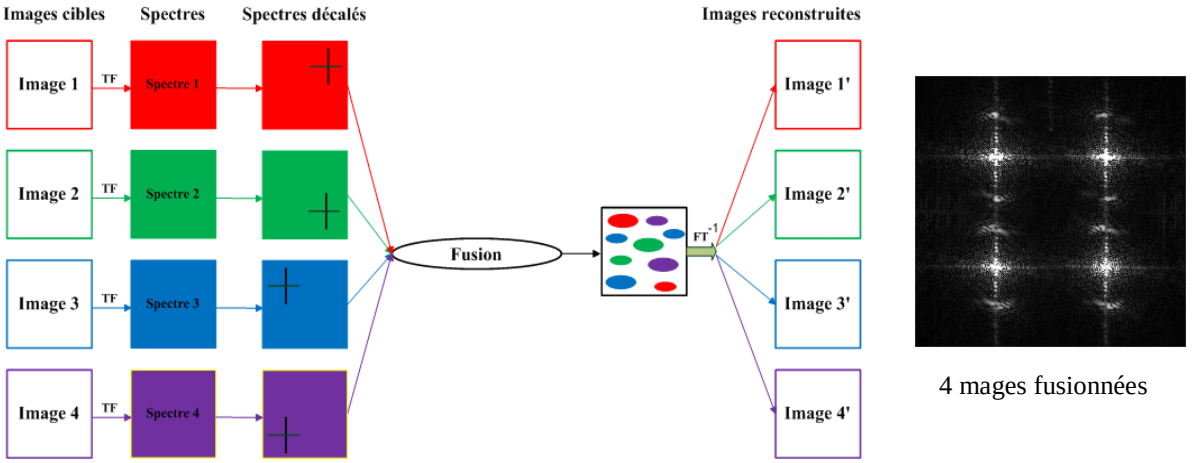


Figure 3.2 (a) Schéma synoptique de la méthode MIOCE (multiple-image optical compression and encryption), (b) Exemple d'un plan de Fourier représentant quatre spectres décalés et fusionnés.

Avant d'analyser les effets du décalage sur la qualité des images reconstruites, nous proposons de rappeler le principe de la fusion spectrale utilisée. En effet, ce principe utilise un critère de fusion basé sur une segmentation spectrale locale [8].

3.2.4 Critère de segmentation spectrale

Le critère de fusion utilisé dans la MIOCE [8] consiste, premièrement, à diviser le plan spectral-MIOCE (figure 3.2-a) en une multitude de petites zones. Ensuite, nous affectons à chacune de ces zones une information issue du spectre d'une des images cibles. Pour ce faire, le choix s'est porté sur un critère énergétique local. Pour bien comprendre le principe et le rôle de ce critère, considérons seulement deux images cibles de taille N pixels (A et B) (figure. 3.3). La première étape consiste à réaliser le spectre de chacune de ces deux images séparément. Ensuite, nous comparons, pour chaque pixel du plan de Fourier, l'énergie spectrale relative de l'image (A) au pixel (i,j) (i.e. l'énergie E_{ij}^{A} divisée par l'énergie spectrale

totale de l'image (A) : $\sum\sum E_{ij}^{A}$) avec l'énergie spectrale relative de l'image (B), i.e. l'énergie E_{ij}^{B} divisée par l'énergie spectrale totale de l'image (B) : $\sum\sum E_{ij}^{B}$. La décision d'attribuer le pixel à l'un des deux spectres est prise par rapport à la plus grande importance relative de l'énergie qu'il présente. Le but de cette segmentation est d'optimiser l'espace-bande passante du plan de Fourier qui va contenir la fusion des spectres entre deux images cibles. La segmentation résultante de cette comparaison spectrale peut s'écrire :

$$\frac{(\boldsymbol{E_{ij}^{A}})}{\sum_{i=1}^{M}\sum_{j=1}^{N}(\boldsymbol{E_{ij}^{A}})} \quad \begin{matrix}\geq \\ \leq\end{matrix} \quad \frac{(\boldsymbol{E_{ij}^{B}})}{\sum_{i=1}^{M}\sum_{j=1}^{N}(\boldsymbol{E_{ij}^{B}})} \tag{17}$$

Avec E_{ij}^{A} : l'énergie spectrale du pixel (i,j) appartenant à l'image (A), E_{ij}^{B} : l'énergie spectrale du pixel (i,j) appartenant à l'image (B). Le résultat de toutes les comparaisons donnera un seul plan spectral. Ce dernier contient les informations les plus pertinentes pour la reconstruction de deux images cibles (A, B).

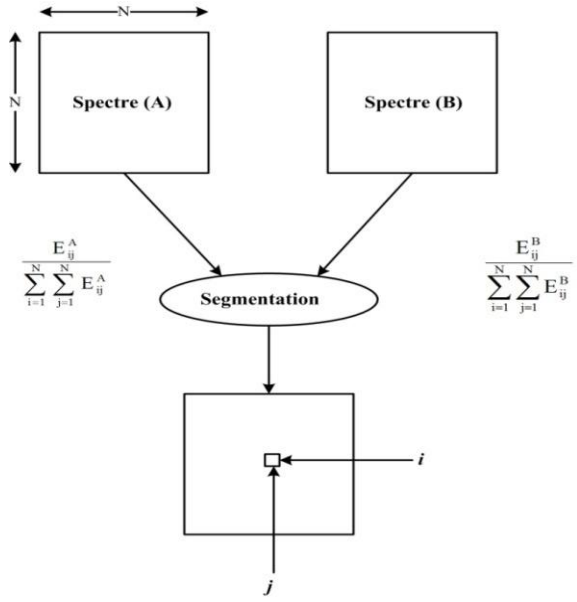


Figure 3.3 Critère de segmentation et d'affectation spectrale

3.2.5 Résultat des images obtenues avec le critère de segmentation (avec et sans décalage des spectres).

Comme nous l'avons dit, les différents tests réalisés ont montré que le critère de fusion, et malgré son importance, ne permet pas à lui tout seul de résoudre le problème de la dégradation de la qualité des images reconstruites (Tableau 1–colonne 3). En effet, le principe de comparaison locale de ce critère conduit à diviser le plan de Fourier en de toutes petites zones et par conséquent conduit à l'apparition de pixels isolés, un pixel isolé est un pixel du spectre de l'image (A) entouré des pixels issus du spectre d'une autre image (B).

Ce phénomène s'accentuera avec des images-vidéo (images qui se ressemblent). Pour quantifier la qualité des images reconstruites avec et sans décalage, nous avons utilisé le

critère de l'erreur quadratique moyenne (MSE) (en anglais **M**ean **S**quare **E**rror). Ce dernier mesure la différence entre l'image cible et l'image reconstruite ; il est défini par la formule suivante :

$$MSE = \frac{1}{NXN}\sum_{i=1}^{N}\sum_{j=1}^{N}\left|I_d(i,j) - I\ (i,j)\right|^2 \qquad (18)$$

Avec N : La taille en pixel de l'image cible (256 pixels), I_d : L'image décompressée et I est l'image cible.

Pour justifier la nécessité du décalage spectral, considérons quatre images issues d'une séquence vidéo représentant une personne qui avance dans le plan d'une caméra (Tableau 1 colonne 2). La colonne 1 présente le numéro de l'image considérée. Comme cela est montré colonne (3) les images reconstruites (en utilisant seulement le critère de segmentation pour fusionner les quatre spectres ensemble) sont de très mauvaises qualité. Cela est dû essentiellement au chevauchement entre les différents spectres. Cela est aussi prouvé par les valeurs de MSE très grandes. Cette qualité se dégrade davantage en augmentant le nombre d'images cibles en entrée.

N°	**Images cibles**	**Images reconstruites sans décalage**	**Images reconstruites avec décalage et le critère RMS**
1		 MSE=0,0294	 MSE=0,0013
2		 MSE=0,2982	 MSE= 0,0012
3		 MSE=0,3547	 MSE= 0,0012
4		 MSE=0,3068	 MSE= 0,0015

Tableau 1. Résultats de la reconstruction des images en utilisant le critère de segmentation : colonne (3) sans décalage, colonne (4) avec décalage et le critère RMS.

Cependant, la colonne 4 montre les images reconstruites en utilisant le même critère de sélection et de fusion appliquées après le décalage de différents spectres. La qualité visuelle ainsi que les valeurs de MSE obtenues montrent bien les bonnes performances de cette optimisation.

3.2.6 Utilisation de critère RMS-Duration

Dans le paragraphe précédent, nous montrons l'intérêt du décalage spectral. Dans cette partie, nous proposons d'étudier ce décalage afin de déterminer sa valeur. Rappelons que cette réorganisation des spectres dans le plan de Fourier a pour but d'éviter une segmentation trop forte dans les zones importantes pour la reconstruction de chacune des images. Ainsi pour éviter les chevauchements dans ces zones (dites importantes), il a fallu définir ces zones, propres à chacune des images. Pour ce faire, nous nous basons sur le critère (RMS-Duration). Ce critère permet de déterminer la taille utile de chacun des spectres des images cibles. Il est défini par :

$$\Delta_I = n\sqrt{\int_{-\infty-\infty}^{+\infty+\infty}(u^2+v^2)\left|S_I(u,v\right|^2 dudv} \qquad (19)$$

I représente l'une des images cibles, $S_I(u,v)$ son spectre, (u,v) sont les coordonnées dans le plan de Fourier et n est un paramètre qui détermine la taille minimale du spectre considéré. Ce critère permet de définir la zone utile d'un spectre relatif à une image donnée (figure 3.4). Ainsi, nous proposons de réorganiser le plan spectral de sorte à ce qu'il n'y ait pas de chevauchement dans ces zones utiles comme cela est montré par *X* et *X'* en figure 3.4. Ces zones représentent les tailles calculées avec la formule (19) des spectres des deux images cibles considérées dans cet exemple.

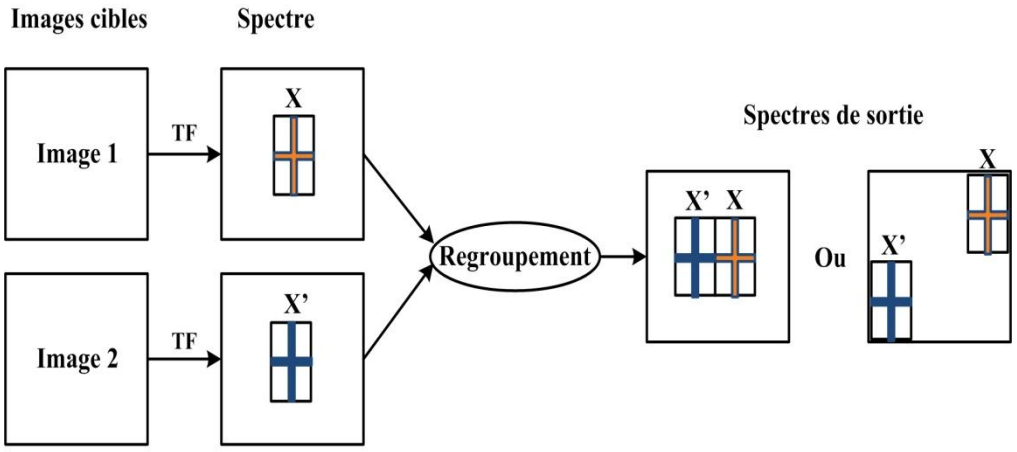


Figure 3.4 Diagramme synoptique du critère utilisant le (RMS-Duration) pour calculer le décalage.

En appliquant cette méthode de décalage avec ce nouveau critère sur l'exemple considéré dans le tableau (1), nous obtenons les résultats donnés dans le tableau 1-colonne 4. En comparant ces images reconstruites avec décalage avec celles obtenues sans décalages (colonne 3), nous pouvons aisément observer visuellement l'apport positif dû à cette méthode. Cela est aussi confirmé par les très petites valeurs de l'erreur quadratique moyenne (MSE).

Cependant, les différents tests que nous avons réalisés ont montré que le choix du décalage influence beaucoup, à la fois la qualité des images, ainsi que le taux de compression. Par exemple, dans la figure 3.4, nous avons présenté deux possibilités de décalage. La première configuration nécessite la conservation d'une petite partie du plan spectral i.e. égale à ($X+X^{'}$). Tandis que la deuxième configuration nécessite l'envoie et/ou le stockage de tout le plan spectral. Ainsi, la première configuration nécessite la manipulation d'un nombre de pixels plus petit et par conséquence, le taux de compression de la première configuration est nettement moins important que celui de la deuxième configuration. Ainsi, le décalage des différents centres des spectres dans le plan de Fourier doit être minutieusement étudié afin de trouver un bon compromis entre la qualité des images reconstruites et le taux de compression. Dans le paragraphe suivant, nous proposons une nouvelle optimisation afin de trouver ce compromis entre le décalage, la qualité des images et le taux de compression.

3.3 Optimisation des performances en termes de taux de compression et de qualité des images reconstruites.

Comme nous venons de le voir, il est primordial de bien choisir le décalage dans le plan de Fourier. Pour montrer l'importance de ce décalage, considérons l'exemple de trois spectres décalés de quatre façons différentes (figure 3.5). A noter que dans les quatre cas de figures, nous avons un décalage supérieur à la taille utile (RMS) calculé avec l'équation (19).

3.3.1 Positionnement spectral

La valeur du décalage du spectre ainsi que la position dans laquelle il est positionné sont très importantes [79]. Le but principal est de diminuer le chevauchement entre les spectres dans le domaine de Fourier pour sélectionner tous les pixels déterminants d'une image. Pour cela, nous avons mené une étude utilisant trois spectres (figure 3.5). Notre objectif étant de montrer l'importance de la position du décalage en calculant pour chacune des configurations l'erreur quadratique moyenne (MSE).

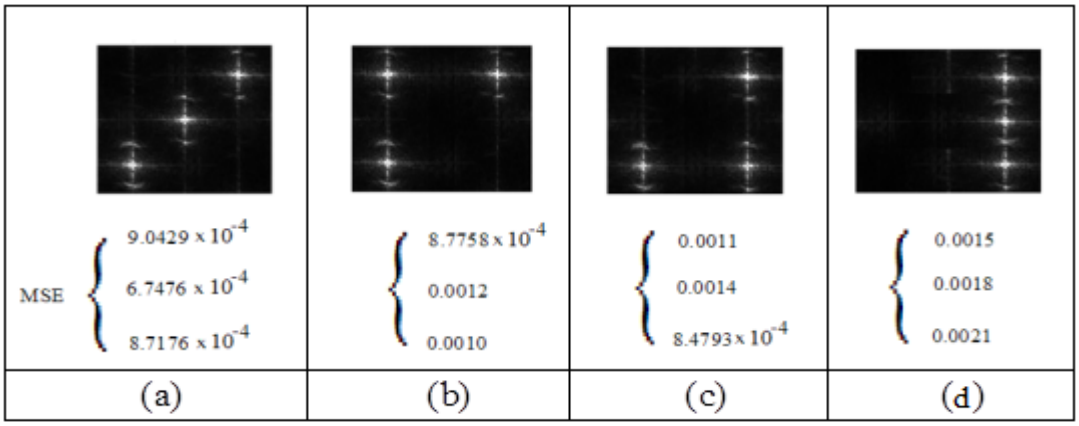


Figure 3.5. Effets du choix de la position des spectres sur la qualité des images reconstruites.

La figure (3.5-a) présente les valeurs de MSE les plus petites en comparaison avec les valeurs de MSE obtenues sur les figure (3.5-b, c et d). En effet, dans la figure 3.5-a, (décalage suivant la diagonale), nous avons le chevauchement le plus petit entre les trois spectres considérés. Par contre, nous remarquons que les plus grandes valeurs de MSE sont obtenues en figure 3.5-d, i.e. en position verticale. Cela est du au chevauchement le plus élevé observé dans cette configuration.

3.3.2 Calcul de décalage et la taille du filtre

Dans cette partie, nous développons une méthode pour calculer le bon décalage entre les différents spectres considérés pour une application donnée, i.e. le décalage « *d* » opéré avec le minimum des pixels et qui nous donnent un bon compromis entre le taux de compression (Tc) et la qualité des images reconstruites (figure 3.6). Pour ce faire, nous avons considérés 4 images avec un décalage donné « *d* » (figure 3.6). Ensuite, nous construisons un filtre de taille « *t* » en ne gardant que les informations pertinentes pour la reconstruction des images en sortie. Pour calculer la taille du filtre « *t* », nous proposons d'utiliser la formule suivante :

$$t = 2\Delta I + x = 2\Delta I + d/\sqrt{2} \tag{20}$$

Avec t : la taille du filtre dans le plan de Fourier, ΔI : la taille utile du spectre calculé avec l'équation 19 de l'image I, et d : le nombre de pixels de décalage. Ainsi, avec cette équation, la taille de filtre dépend de la taille utile (RMS) de chacune des images considérées ainsi que du décalage entre les différents spectres fusionnés [80].

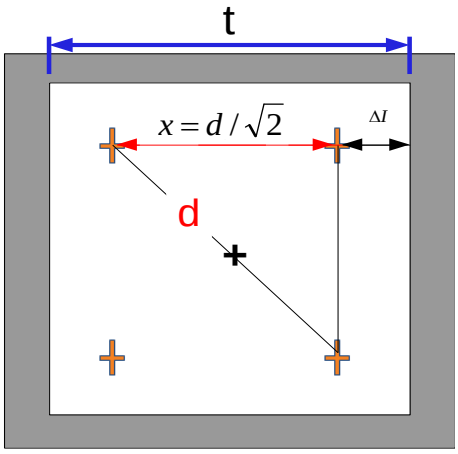


Figure 3.6 Construction de filtre dans le plan de Fourier.

Pour bien analyser les effets du décalage avec filtrage, nous avons simulé cette méthode avec un décalage « *d* » ayant une valeur croissante exprimée en pixels : $d \in [4,64]$ pixels. La figure 3.7-a présente les quatre spectres décalés de $d = 4$ et segmentés avec le critère énergétique (équation 17). La figure 3.7-b présente le filtre associé selon l'équation 20. Le résultat du filtrage avec un décalage égal à *d*=4 est présenté sur la figure 3.7-c. Pour un décalage de *d*=64, nous avons les résultats présentés sur la figure 3.7 (d, e et f).

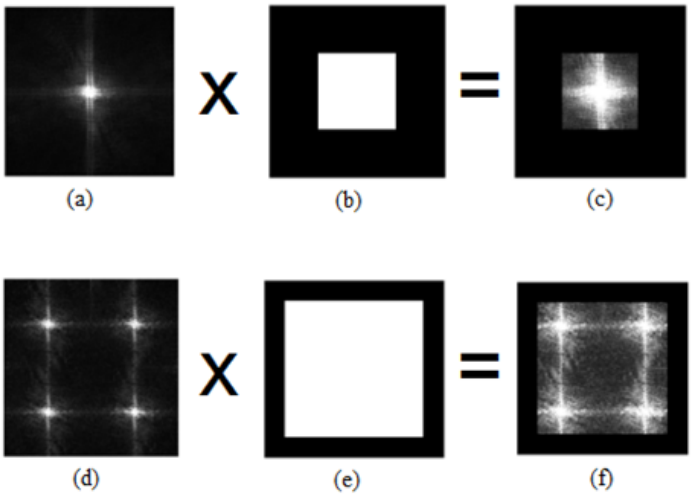


Figure 3.7 Le spectre des quatre images cibles fusionnés, décalés et filtrés obtenues avec notre méthode.

La figure 3.7 montre bien que la configuration de la figure 3.7-c présente le plan spectral le plus petit en taille. Cependant, cette configuration présente aussi une baisse notable dans la qualité des images reconstruites (cas du décalage des centres d=4 pixels). En effet, dans ce cas nous avons le chevauchement le plus important entre les spectres. Par contre nous avons une meilleure qualité des images reconstruites avec un décalage de 64 pixels car nous avons gardé

la plupart des informations représentées dans chaque image i.e. la taille du plan spectral filtré la plus élevée.

Pour mesurer les effets du décalage entre les spectres, nous avons calculé l'erreur quadratique moyenne (MSE) en fonction du nombre de pixels de décalage. Les résultats sont résumés sur la courbe de la figure 3.8. En abscisse nous avons la taille du décalage opéré et en ordonnées nous avons les valeurs de MSE correspondante.

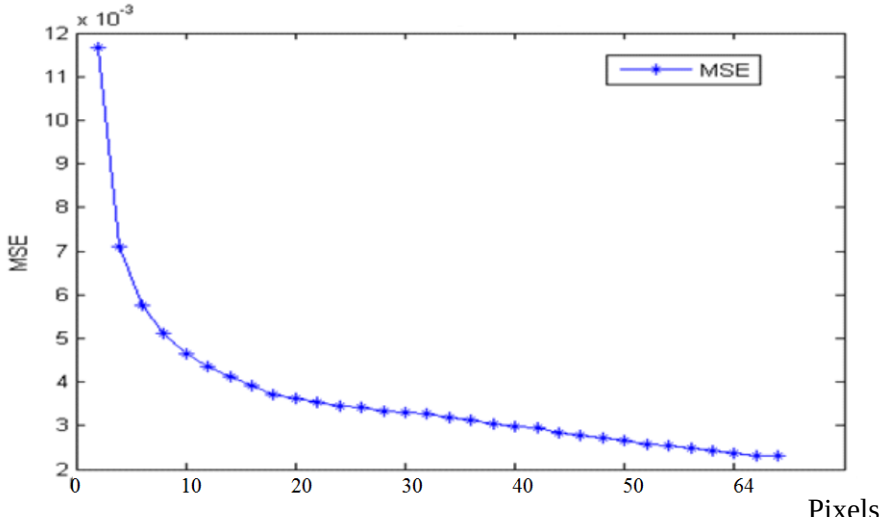


Figure 3.8. Effet du décalage spectral sur la qualité des images reconstruites : calcul des valeurs de MSE

Nous remarquons sur cette courbe (figure 3.8) que les valeurs de MSE diminuent très rapidement jusqu'à la valeur de décalage correspondante à d=16 pixels. Ensuite, les valeurs de MSE décroissent très lentement. Cela signifie que la séparation entre les centres des différents spectres considérés n'apporte pas en terme de qualité des images reconstruite au-delà de 16 pixels de décalage. Ainsi, nous pouvons nous arrêter au décalage de 16 pixels et utiliser le reste de la bande passante du plan spectral pour rajouter d'autres images cibles et ainsi augmenter le taux de compression tout en conservant la même qualité des images reconstruites.

3.3.3 Taux de compression

Dans cette partie nous calculons le taux de compression en fonction du nombre de pixels de décalage entre les spectres. Le taux de compression utilisé dans cette partie, pour des images de taille *256 X 256* pixels, est calculé avec l'équation suivante :

$$\boldsymbol{Taux\ de\ compression} = \mathbf{1} - \frac{\mathbf{256} * \mathbf{256} * \boldsymbol{Pri} * \boldsymbol{Bitd}}{\mathbf{256} * \mathbf{256} * \boldsymbol{n} * \boldsymbol{Bitc}} * \mathbf{100} \qquad (21)$$

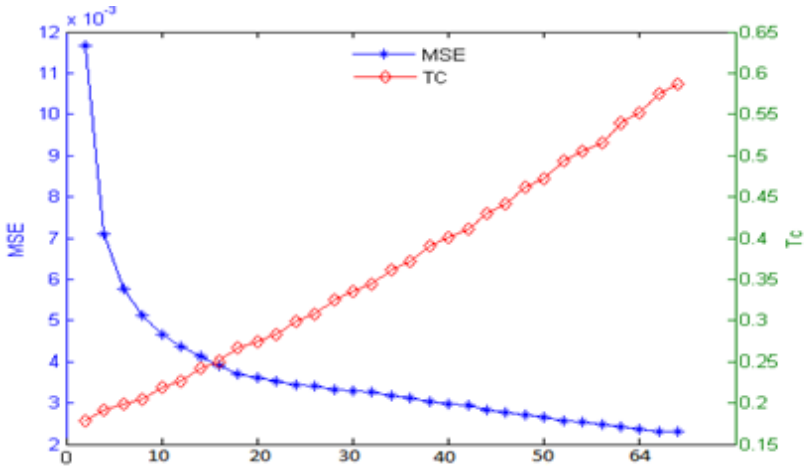
Avec :

- *Pri* égale à 2, cette valeur présente les deux parties du spectre compressé : parties réelles et imaginaires.
- *Bitd* est le nombre de bits utilisés pour coder le spectre compressé. Dans ce travail, nous avons fixé cette valeur à 16 bits.
- *n* est le nombre d'images cibles considérées.
- *Bitc* est le nombre de bits utilisés pour coder l'image cible. Dans ce travail, nous avons considéré des images cibles réelles à plusieurs niveaux de gris (i.e. *Bitc* =8 bits).

Nous en déduisons que le taux de compression de notre méthode peut s'écrire :

$$Taux\ de\ compression = 1 - \frac{4}{n} \text{X}100 \qquad (22)$$

La figure 3.9-a présente la courbe des valeurs du taux de compression (Tc), ainsi que la courbe des valeurs de MSE en fonction du nombre de pixels de décalage.



(a)

(b)

Figure 3. 9 (a) Taux de compression et valeurs de MSE en fonction du nombre de pixels de décalage, (b) Image reconstruite avec un décalage égal à 16 pixels.

Sur cette figure 3.9, nous pouvons observer un point d'intersection entre la courbe des valeurs de MSE et la courbe du taux de compression. Ce point est obtenu avec un décalage égal à 16 pixels. Cela nous donne le compromis recherché entre la qualité des images reconstruites et le taux de compression. Ainsi, nous avons montré qu'il est possible de trouver

un bon compromis entre le taux de compression et la qualité des images reconstruites en sortie de notre système.

3.3.4 Résultat de compression en utilisant des images multiples issues d'une séquence vidéo

Nous allons maintenant appliquer les deux critères de (1) segmentation et (2) la taille utile d'un spectre (RMS) que nous avons proposé pour fusionner 13 spectres d'images en un seul spectre. En effet, les simulations ont montré qu'au-delà de 13 images cibles nous perdons beaucoup en qualité images reconstruites. La figure 3.10 représente le spectre résultant regroupant les informations de ces 13 spectres des images fusionnées avec notre méthode.

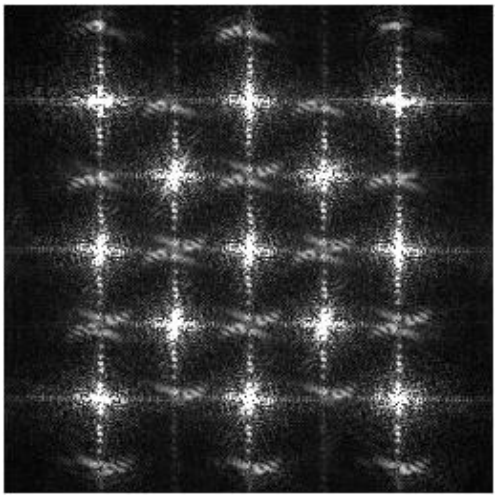


Figure 3.10 Exemple de 13 spectres fusionnés et compressées avec notre méthode.

Pour montrer les bonnes performances de notre méthode nous avons simulé et calculé l'erreur quadratique moyenne MSE pour l'image reconstruite en augmentant le nombre d'images cible de 1 à 13 images comme cela est présenté dans la figure 3.11. Nous pouvons remarquer que les valeurs de MSE de l'image n°1 (tableau 2) sont très petites et les images reconstruites sont de bonne qualité visuelle (voir figure 3.11). Nous avons calculé avec l'équation 22 le taux de compression pour 13 images est de 69.2% ; ce qui est un bon taux de compression.

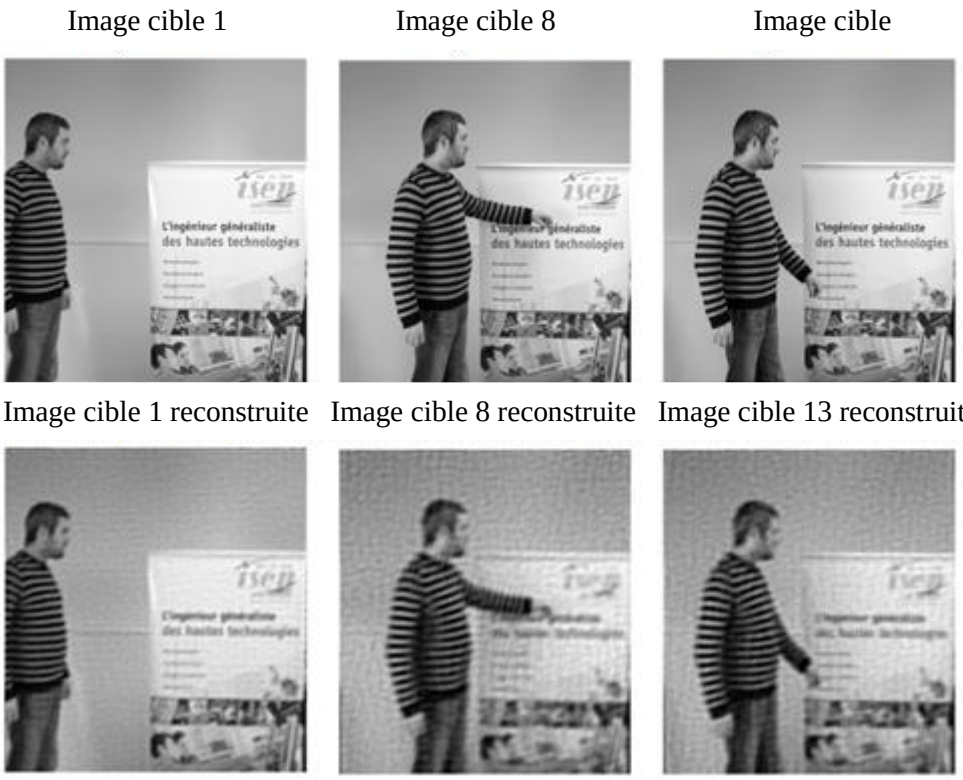


Figure 3.11 Résultat de simulation de compression et décompression des images fixes.

Valeurs des MSE correspondantes	
Image 01	$MSE=3.9\times10^{-3}$
Image 02	$MSE=5.4\times10^{-3}$
Image 03	$MSE=5.7\times10^{-3}$
Image 04	$MSE=8.6\times10^{-3}$
Image 05	$MSE=9.1\times10^{-3}$
Image 06	$MSE=8.8\times10^{-3}$
Image 07	$MSE=9.2\times10^{-3}$
Image 08	$MSE=11.1\times10^{-3}$
Image 09	$MSE=13.3\times10^{-3}$
Image 10	$MSE=13.4\times10^{-3}$
Image 11	$MSE=13.6\times10^{-3}$
Image 12	$MSE=13.7\times10^{-3}$
Image 13	$MSE=14.7\times10^{-3}$

Tableau. 2 Valeurs de MSE pour 13 images cible

3.3.5 Discussion

Nous avons proposé dans cette section, une nouvelle approche de compression des images fixes. Cette approche est basée sur l'optimisation de deux critères. Le premier consiste à calculer la taille utile des spectres (RMS) puis de décaler les centres des spectres d'images cibles de façon à minimiser le chevauchement des spectres. Le deuxième critère consiste à appliquer une technique de segmentation afin de sélectionner les informations importantes propres à chaque image cible. Les résultats de simulation ont montré les bonnes performances de notre méthode. Cela est prouvé par un taux de compression très élevé avec des très petites valeurs de MSE. Dans la section suivante, nous allons proposer et détailler notre approche de cryptage et la combiner avec la méthode de compression.

3.4 Notre approche de cryptage

3.4.1 Principe de l'approche

Nous avons vu en chapitre 2 que les techniques de cryptage consistent à cacher les informations représentées dans l'image pour les préserver et garantir la confidentialité. Nous avons aussi détaillé les deux types de cryptage qui existent (cryptage avec une clé privée ou publique). Dans cette section, notre objectif est de développer une nouvelle approche de cryptage capable de bruiter efficacement le spectre fusionné (figure 3.12).

Le but étant de conserver la confidentialité des informations représentant une séquence vidéo. Pour ce faire, nous nous basons sur le principe de segmentation spectrale décrit dans la section (3.2.4) pour changer la répartition spectrale dans le domaine de Fourier. Ainsi, après le passage dans le domaine de Fourier, la première étape consiste à multiplier le spectre segmenté des images cibles (figure 3.12) par un masque aléatoire (amplitude et de phase). Pour développer notre approche de cryptage nous avons considéré le cas de deux images cibles (figure 3.12). Pour plus d'images il suffit de dupliquer le processus développé dans ce paragraphe.

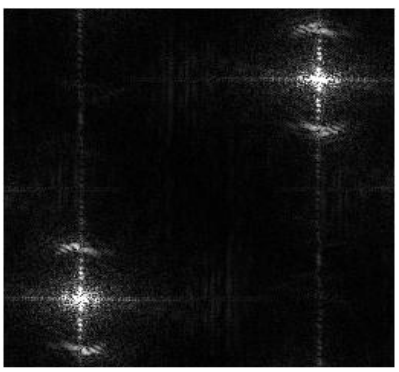


Figure 3.12 Exemple d'un spectre cible : plan spectral fusionnant deux images.

3.4.2 Fabrication du masque de cryptage

Pour fabriquer le masque de cryptage (clé) nous proposons le schéma présenté figure 3.13. La multiplication de ce masque avec le spectre cible (figure 3.12) doit modifier suffisamment la répartition spectrale de ce dernier afin de bien crypter (cacher) toutes les informations présentes.

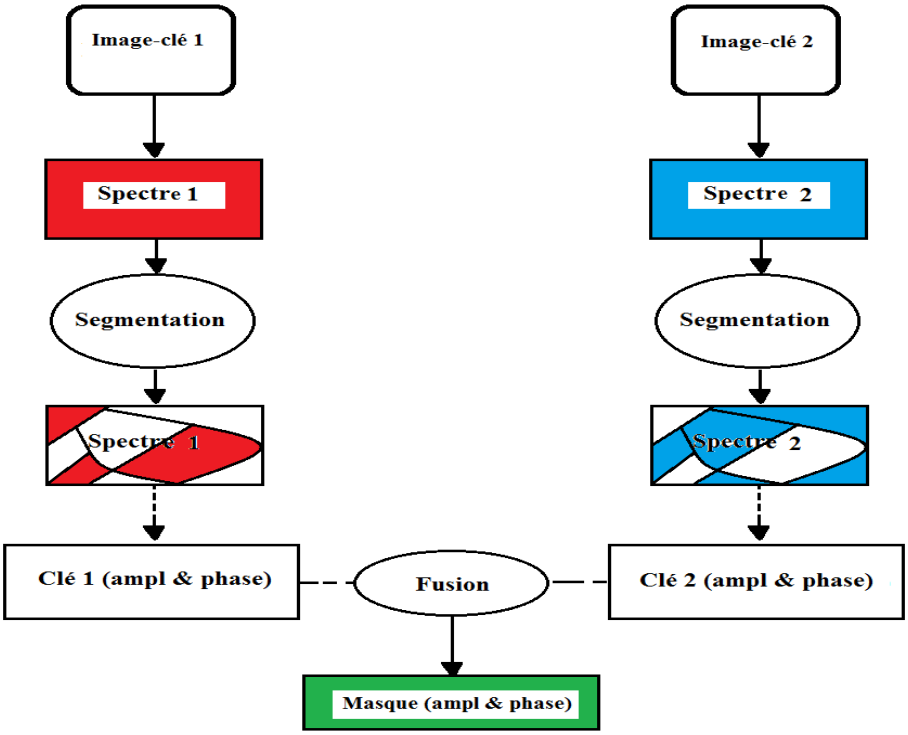


Figure 3.13 Schéma synoptique de la fabrication du masque de cryptage.

Comme cela est présenté sur la figure 3.13, pour fabriquer ce masque de cryptage, nous commençons par choisir deux images clés. Ces deux images clés doivent appartenir à la même classe des images cibles. Ensuite, nous réalisons une fusion spectrale de ces deux images clés (en suivant le même principe développé dans la section 3.2.4). Par la suite, en utilisant les informations spectrales (valeurs maximales et valeurs minimales) de deux spectres clés, nous construisons un masque aléatoire d'amplitude et de phase. Les valeurs d'amplitude de ce masque sont comprises entre les Min et les Max déterminées auparavant. Finalement, nous multiplions ce masque avec le spectre cible (fusionnant deux images cibles figure 3.12). Le résultat de ce premier cryptage est présenté la figure 3.14.

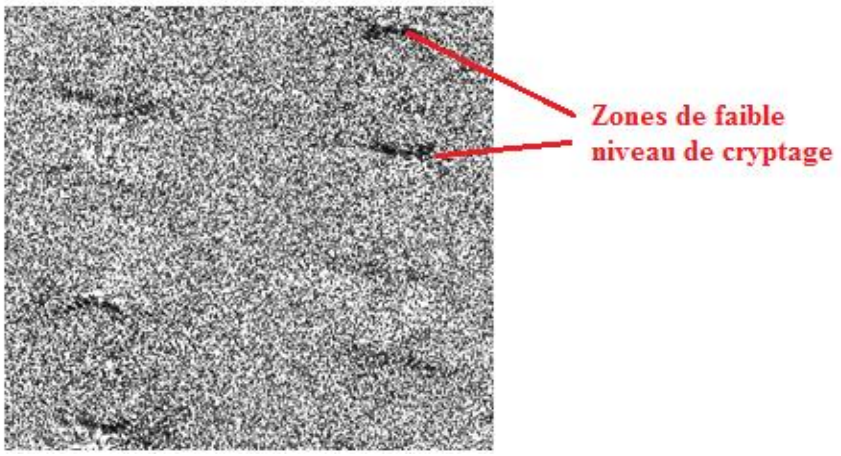
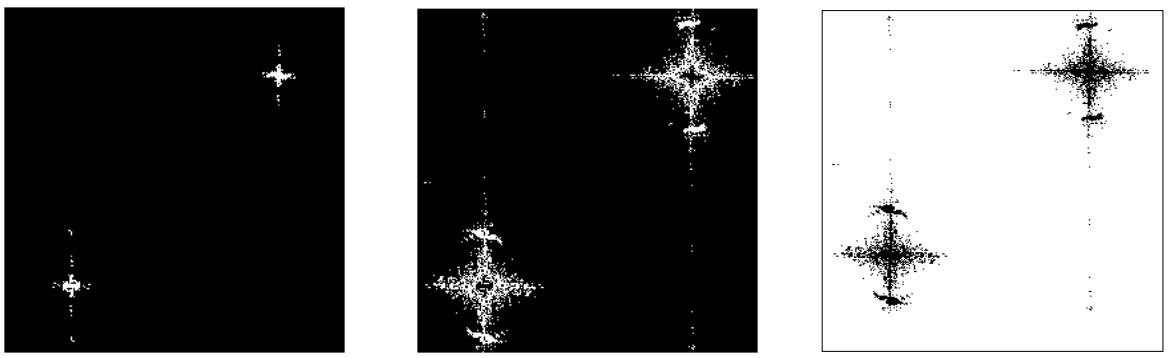


Figure 3.14. Spectre cible crypté avec un masque aléatoire

Sur cette figure 3.14, nous pouvons aisément constater des lacunes dans le cryptage. En effet, des zones sont toujours visibles indiquant au pirate l'emplacement des informations utiles. Cela est dû essentiellement à la dynamique très élevée d'un spectre (la différence entre la valeur Max et la valeur Min). Dans l'exemple de la figure 3.14, nous avons créé un masque de cryptage ayant des valeurs aléatoires comprises entre la valeur Min et la valeur Max. Ainsi en divisant le spectre de la figure 3.12 par ce masque, les petites valeurs sont ainsi divisées aléatoirement par des valeurs très grandes. Cela conduit parfois à la création des ces zones visibles.

3.4.3 Masque de cryptage optimisé

Pour surmonter ce phénomène, nous proposons de diviser le masque de cryptage en trois zones et de traiter ces zones séparément. Ces trois zones correspondent aux hautes fréquences, moyennes fréquences et basses fréquences (figure 3.15). Ensuite, nous construisons un masque aléatoire correspondant à chaque partie. En utilisant, les valeurs Min et Max dans chacune de trois parties séparément.



Hautes fréquences : Masque M1 Moyennes fréquences: Masque M2 Basses fréquences: Masque M3

Figure 3.15 Répartition du masque de cryptage en trois sous-masques

Le critère de séparation en trois sous-masques est le suivant :

- D'abord, en utilisant la figure 3.12, nous calculons la valeur max dans les zones de faible amplitude : M_{max}.
- M1 correspond aux fréquences ayant des amplitudes $\geq M_{\max}$.
- M2 correspond aux fréquences ayant des amplitudes $\left]\frac{1}{4}M_{\max}, M_{\max}\right[$.
- M3 correspond aux fréquences ayant des amplitudes $\leq \frac{1}{4}M_{\max}$.

Cette séparation en trois sous-masques nous permet d'adapter notre clé de cryptage pour les trois composantes fréquentielles (M1, M2, M3). Ces trois composantes vont être utilisées pour fabriquer les trois sous-masques aléatoires : S1cryp, S2cryp et S3cryp (figure 3.16).

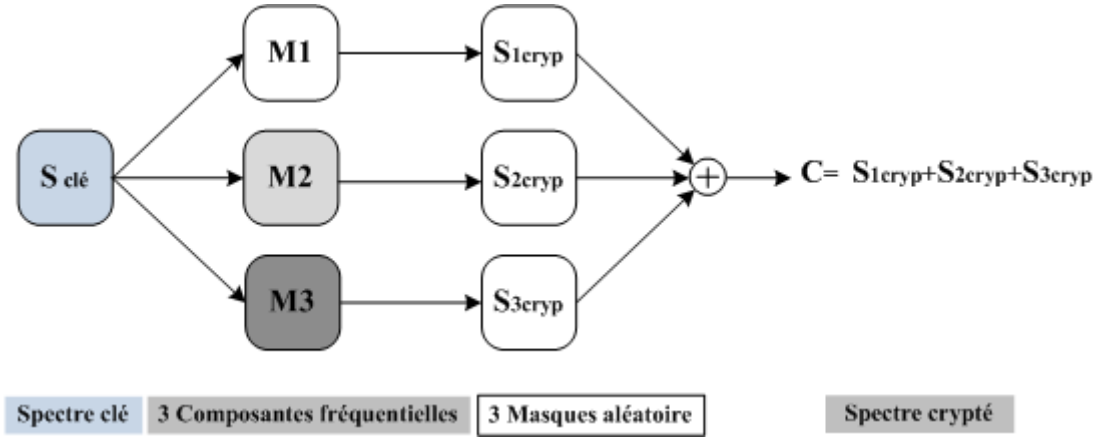
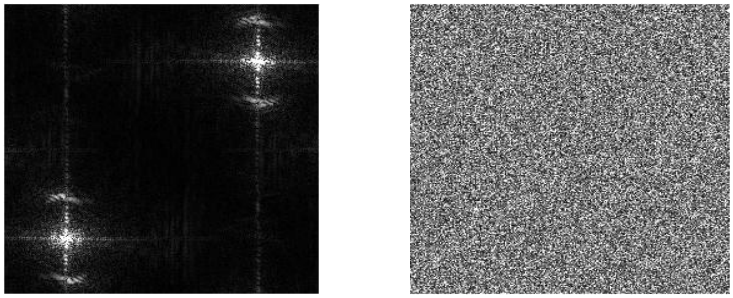


Figure 3.16 Fabrication du masque de cryptage optimisé : C= S_{1cryp}+ S_{2cryp} + S_{3cryp}

L'équation utilisée pour calculer les masques des sous-clés de cryptage sont décrites par :

$$\begin{aligned} S_{1Ccryp} &= rand\left[\min(M1), Max(M1)\right] \\ S_{2Ccryp} &= rand\left[\min(M2), Max(M2)\right] \\ S_{3Ccryp} &= rand\left[\min(M3), Max(M3)\right] \end{aligned} \qquad (7)$$

Ensuite, ce masque de cryptage optimisé (C= S_{1cryp}+ S_{2cryp}+S_{3cryp}) est utilisé pour crypter le spectre cible (figure 3.17-a). La figure 3.17-b présente le spectre crypté obtenu avec ces trois masques. Cette dernière montre bien la bonne qualité de cryptage de notre méthode. En effet, nous avons réussi à crypter les zones visibles présentées sur la figure 3.14.



(a) (b)

Figure 3.17 (a) Spectre cible fusionnant deux images, (b) Spectre cryptage avec la clé $C= S_{1cryp}+ S_{2cryp} + S_{3cryp.}$

3.5 Conclusion

Dans ce chapitre, nous avons proposé et validé le principe d'une nouvelle méthode de compression des images multiples basée sur une segmentation spectrale et l'utilisation des nouveaux critères de sélection de l'information. Les bonnes performances de notre méthode permettent d'avoir un taux de compression élevé avec une très bonne qualité d'images reconstruites. Cela est prouvé par les faibles valeurs de MSE et une bonne qualité visuelle. Fort de ce constat, nous avons proposé une nouvelle approche de cryptage optimisée qui peut être implantée simultanément avec notre méthode de compression. Cette approche de cryptage consiste à modifier le plan spectral de l'image cible à l'aide un masque de phase aléatoire optimisé. Dans la suite, nous allons faire une extension de nos travaux pour optimiser notre méthode et pouvoir l'appliquer sur des séquences vidéo. Cela peut se faire en utilisant de la propriété de la symétrie spectrale de l'optique cohérente. Ainsi nous pouvons augmenter le nombre d'images cibles à fusionner jusqu'à 26 images. Coté cryptage, nous pensons qu'un seul niveau de cryptage ne rends pas notre méthode robuste contre les attaques, il est donc nécessaire de l'améliorer en rajoutant un deuxième niveau de cryptage. Ces optimisations font l'objet du chapitre suivant.

Chapitre 4

4. Optimisation et application de la méthode de compression et de cryptage simultanés.

Sommaire

4.1 Introduction

Dans le chapitre précédent, nous avons proposé et validé une nouvelle méthode de compression et de cryptage simultanés des images multiples. Cette méthode possède l'avantage de réaliser les deux opérations de compression et de cryptage simultanément. Elle permet aussi d'obtenir un taux de compression élevé avec un bon niveau de cryptage, un système de cryptage fiable et un temps de calcul réduit. Nous avons aussi présenté les résultats de simulation qui attestent de la validité de notre méthode.

Dans ce chapitre, nous allons profiter des propriétés de l'optique de Fourier pour optimiser davantage la compression en augmentant le nombre d'images cible à fusionner. Ensuite, nous allons adapter notre méthode de compression et de cryptage aux images vidéo. Pour garantir un bon niveau de sécurité de la méthode, nous allons développer un deuxième masque de cryptage afin d'augmenter la robustesse de notre méthode contre les attaques.

4.2 Optimisation de la technique de compression pour les séquences vidéo

Notre objectif est de proposer une optimisation qui cherche à trouver une utilisation optimale du produit espace bande passante dans le domaine de Fourier. Pour cela, nous allons essayer d'augmenter le nombre d'images à multiplexer en utilisant la propriété de symétrie spectrale. C'est, en effet, une propriété de l'optique de Fourier qui permet la symétrie par rapport au centre de spectre.

4.2.1 Fusion spectrale par symétrie

Pour traiter des séquences vidéo, il faut tout d'abord pouvoir augmenter le nombre des images à multiplexer dans le plan de Fourier (plan dans lequel nous fusionnons et cryptons les informations spectrales sélectionnées pour représenter les différentes images cibles). Pour cela, nous proposons une optimisation de notre technique de compression en utilisant une des propriétés de la transformation de Fourier i.e. la symétrie du spectre. En effet, dans le domaine de Fourier tous les points sont symétriques par rapport au centre du spectre. Pour cela, et avant d'appliquer le décalage et la fusion, nous commençons par construire un filtre binaire constitué de deux blocs symétriques par rapport à la verticale et passant par le centre ; le premier a des pixels de valeur égale à '1' et l'autre égale à '0' (figure 4.1). Ensuite, nous multiplions deux par deux les spectres des images cibles avec ce filtre construit comme cela est montré (figure 4.1). Ainsi, pour chacun de deux spectres considérés, nous ne conservons que la moitié d'informations. En ne gardant que la moitié du spectre d'une image donnée, nous pouvons retrouver l'autre moitié en utilisant le conjugué de la moitié conservée.

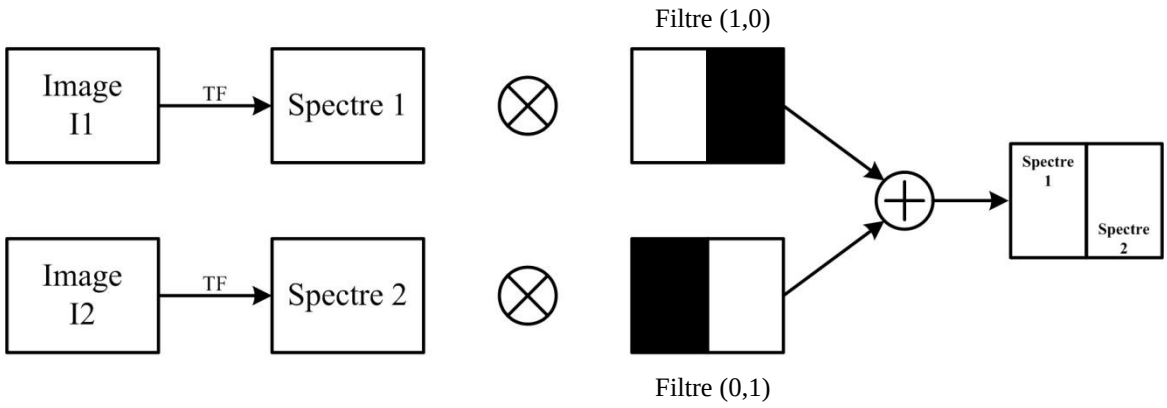


Figure 4.1 Schéma synoptique de la compression par symétrie.

4.2.2 Technique de regroupement des images

En utilisant cette propriété de symétrie décrite auparavant, mous allons maintenant essayer de regrouper deux par deux les images d'une séquence vidéo (figure 4.1). En fixant un nombre d'images d'une séquence à 26 images (ce nombre est calculé en trouvant un compromis entre le taux de compression et la qualité des images voulues en sortie), nous avons divisé la séquence considérée en petites séquences de 26 images chacunes. Ensuite, nous regrouperons les 26 images ensemble deux par deux : I_n avec I_{n+13} comme cela est montrée en figure 4.2.

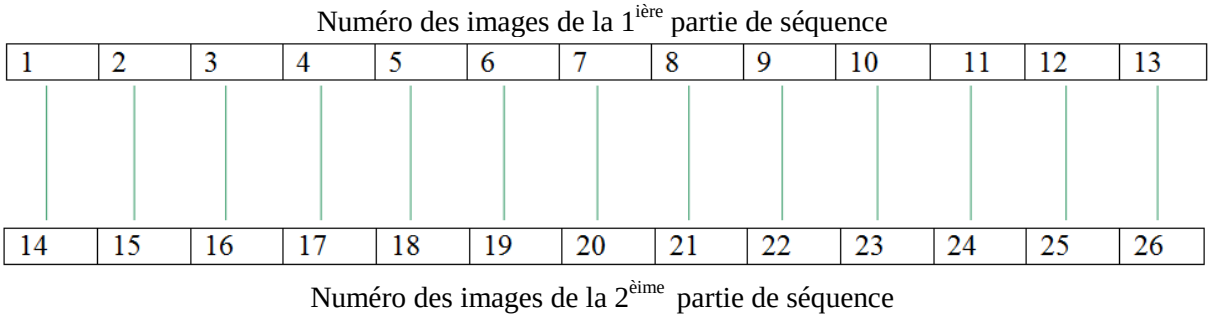


Figure 4.2 Regroupement deux par deux d'une séquence vidéo de 26 images.

4.2.3 Adaptation de notre technique de compression aux séquences vidéos

Dans cette partie, nous allons présenter une adaptation de notre méthode de compression afin de traiter des images issues d'une séquence vidéo. En effet, après la réalisation de la fusion par symétrie (figure 4.1) et le regroupement des images cibles comme il est montré sur la figure 4.2. Nous pouvons maintenant appliquer notre adaptation. Les différentes étapes de la méthode utilisée pour comprimer une séquence vidéo sont résumées sur la figure 4.3. Cette

technique de compression par symétrie nous a permis de regrouper les spectres de 26 images en seulement un seul plan spectral comme cela est montré sur la figure 4.3.

Les étapes de cette adaptation consistent à réaliser la transformation de Fourier pour les images de la séquence vidéo (26 images cibles). Ensuite, nous multiplions chaque spectre avec le filtre (1,0) ou (0,1) (figure 4.1) afin d'en supprimer la moitié, puis nous effectuons la technique de regroupement pour rassembler chaque deux moitiés de spectres ensemble (figure 4.2). Les spectres résultants de ce regroupement deux par deux sont introduits dans notre système de segmentation expliqué dans le chapitre 3 section 3.3. La dernière étape de cette adaptation consiste à décaler les spectres et à appliquer le critère de segmentation pour fusionner les spectres en un seul qui sera transmit ou stocké. Cette technique est présentée sur la figure 4.3.

Le résultat de simulation de cette adaptation est illustré sur la figure 4.4. Le spectre résultant contient les spectres formés à partir de vingt-six moitiés de spectres d'images issus de la séquence vidéo.

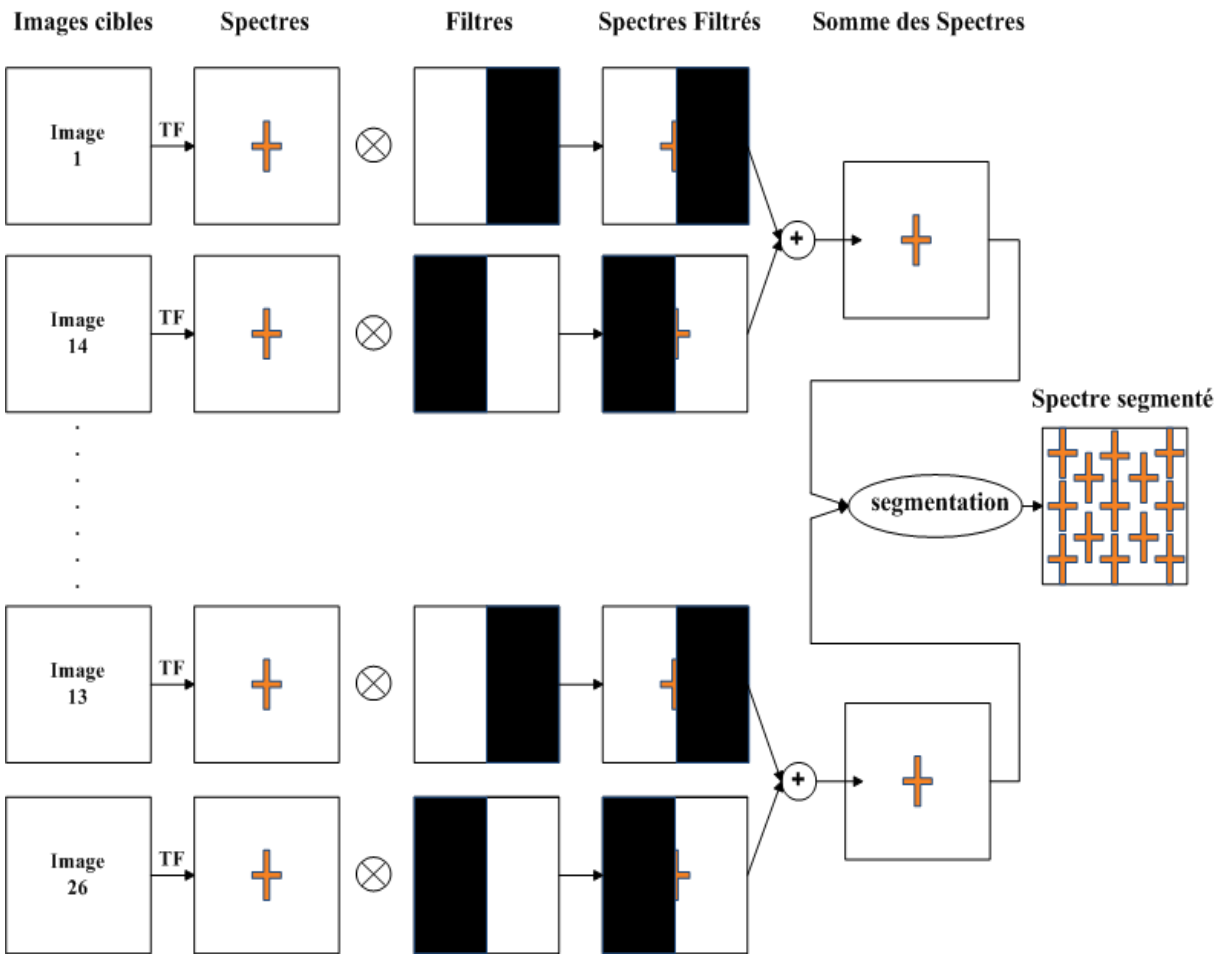


Figure 4.3 Schéma synoptique de l'adaptation de notre méthode aux séquences vidéo.

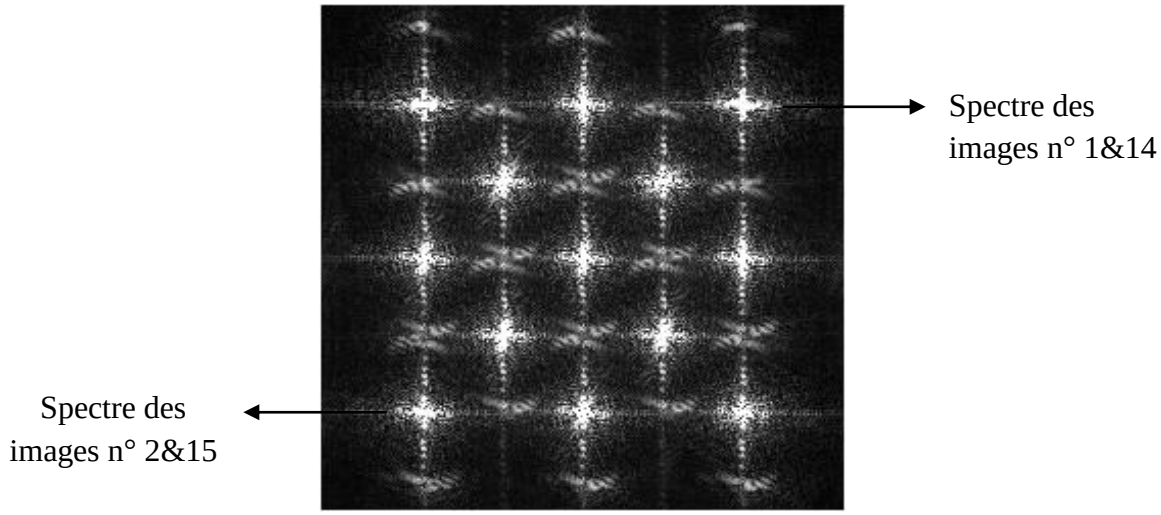


Figure 4.4 Exemple de 26 spectres fusionné et compressées.

4.2.4 Décompression et reconstruction des images de la séquence vidéo

La phase de la décompression de notre méthode consiste, à partir du spectre segmenté reçu (figure 4.4), de faire l'inverse du processus de compression. Premièrement, nous séparons les 13 spectres grâce à une multiplication par une porteuse spécifique et propre à chacun des 13 spectres i.e. cette porteuse peut être rajoutée lors de l'étape de segmentation. Ensuite, nous sélectionnons seulement la moitié d'un de ces 13 spectres. Nous reconstruisons ensuite l'autre moitié en complétant le spectre par le conjugué de la partie reçue. Finalement, nous réalisons une transformation de Fourier inverse pour retrouver les images reconstruites.

4.2.5 Analyse des résultats avec le critère de MSE

Pour montrer les bonnes performances de notre approche, nous avons considéré une séquence vidéo de 26 images puis nous avons calculé l'erreur quadratique moyenne MSE. Nous pouvons observer sur la figure 4.5 l'évolution des valeurs MSE en fonction de nombre d'images cibles. La figure 4.5-a montre que les valeurs de MSE augmentent (i.e. la qualité des images reconstruite diminue) avec le nombre des images cibles. En effet, plus il y a d'images cibles et plus petit est l'espace alloué à chacune des images dans le plan spectral.

De plus, nous observons un phénomène de palier dans la courbe des valeurs de MSE. Cela est lié à la position des spectres après le décalage dans le domaine spectral. En effet, nous avons choisi de commencer par placer les spectres le plus loin possible de l'image n°1

(spectre en haut à droite de la figure 4.4) et en s'approchant de cette image les valeurs de MSE augmentent.

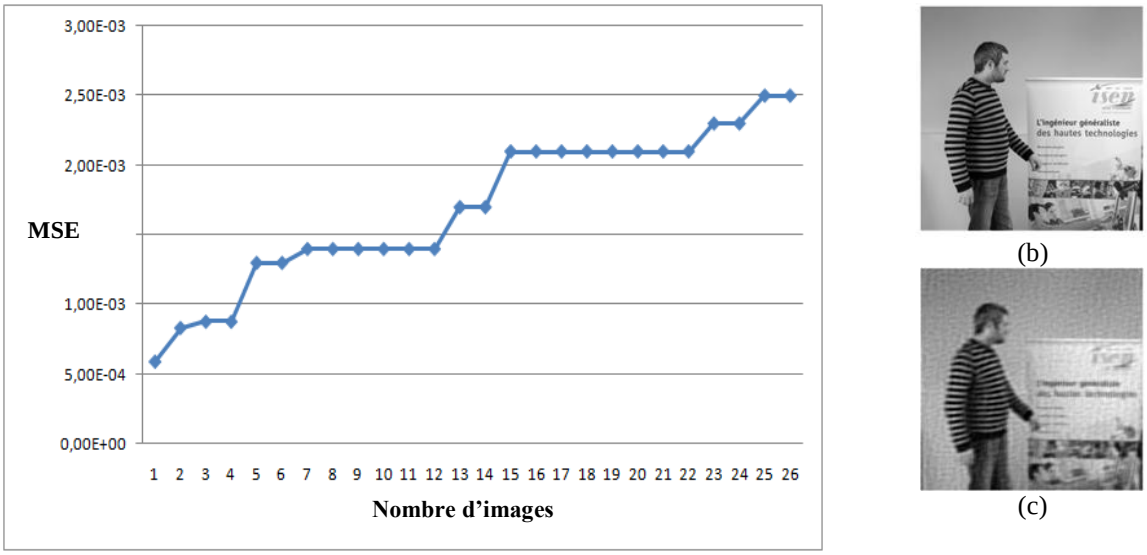


Figure 4.5 (a) Valeurs MSE en fonction du nombre d'images cibles, (b) Exemple d'une image cible et (c) l'image reconstruite.

De plus, nous constatons que les valeurs de MSE sont très petites (même pour 26 images). Cela atteste bien de la bonne qualité des images reconstruites et des bonnes performances de notre méthode de compression. Pour justifier la bonne qualité de reconstruction, nous pouvons comparer visuellement l'image d'entrée (figure 4.5-b), i.e. cette image faisant partie des 26 images de la séquence considérée, avec la même image reconstruite en sortie de notre système (figure 4.5-c). Cette comparaison montre bien la bonne qualité des images reconstruites.

4.2.6 Taux de compression

Pour quantifier ces bonnes performances, nous résumons dans le tableau (3), en fonction de l'augmentation du nombre d'images dans la séquence considérée $n \leq 26$, le taux de compression correspondant (pour $n = 26$ nous avons un $MSE \approx 3{,}9 \times 10^{-3}$).

Nombre d'images	Taux de compression Tc
5	20%
6	34%
7	43%
8	50%
9	56%
10	60%
11	64%
12	67%
13	70%
14	71,5%
15	73,3%
16	75%
17	76,5%
18	78,8%
19	79%
20	80%
21	81%
22	81,8%
23	82,6%
24	83,3%
25	84%
26	84,6%

Tableau 3 : Résultat des taux de compression pour une séquence vidéo de 26 images.

Dans le tableau (3), nous avons choisi de commencer avec un nombre d'images cibles à 5 images, en effet, notre méthode commence à comprimer à partir de 5 images cibles à l'entrée du système. Ces résultats montrent bien que nous avons réussi à comprimer une séquence vidéo en fusionnant 26 images ensemble. Pour n = 26, nous avons un taux de compression allant jusqu'à 84,6% pour 26 images. C'est-dire qu'avec seulement 15% des informations de chacune des images cibles, nous sommes capables de reconstruire la séquence avec une petite valeur de MSE égale à $3{,}9X\ 10^{-3}$.

Ces résultats des simulations numériques montrent que nous avons réussi à reconstituer les images cibles dans le plan de sortie de notre système avec une très bonne qualité visuelle tout en gardant un taux de compression très intéressant pour leur transmission ou leur stockage. Les faibles valeurs de MSE obtenues attestent de la bonne performance de cette méthode de compression.

- Séquence « Char »

Nous allons présenter dans cette partie les résultats de simulation de notre méthode en prenant un autre type d'images cible. En effet, nous avons testé une séquence vidéo d'un char se déplaçant à une vitesse constante. Les résultats obtenus (voir tableau 4) montrent que notre méthode est fiable et robuste quelles que soient les images cibles. Dans le tableau 4, nous pouvons remarquer que les images reconstruites sont de très bonne qualité et les valeurs de MSE sont petites, cela prouve que la méthode peut être utilisé pour différents types d'applications avec des objets fixe ou mouvants. Ces résultats sont résumés dans le fichier multimédia (https://www.youtube.com/watch?v=5CS1rNLyALs) composé de trois parties comme cela est présenté sur le tableau 4 : dans la partie gauche les images cibles, une image représentant les 26 spectres fusionnés au milieu et la partie de droite présente les images reconstruites avec un $MSE = 1{,}8 \times 10^{-3}$.

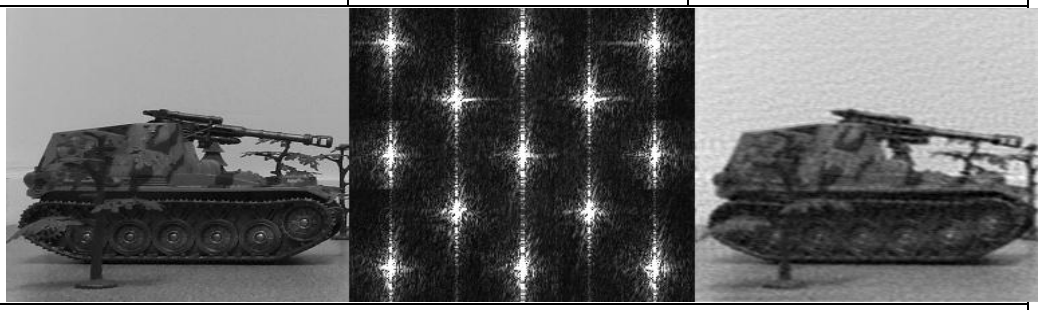
	Image cible (Taille 256x256 pixels)	**Spectre envoyé** (Taille 256x256 pixels)	**Image reconstruite** (Taille 256x256 pixels)
Exemple			
	$MSE = 1{,}8 \times 10^{-3}$		

Tableau 4. Résultats de compression avec une séquence « Char » : voir aussi le fichier multimédia (https://www.youtube.com/watch?v=5CS1rNLyALs).

4.3 Optimisation de l'approche de cryptage

Nous avons proposé, dans le chapitre 3, une nouvelle approche de cryptage basée principalement sur la fabrication d'un masque aléatoire dans plan spectral. Ce dernier est construit à partir de trois sous-masques en fonction de trois composantes de fréquence. Le résultat de simulation de ce premier niveau de cryptage montre que nous avons réussi à sécuriser les informations représentées dans le spectre fusionné. Toutefois, une séquence peut avoir des images blanches, ce qui risque de donner aux éventuels pirates des informations sur les clés du cryptage utilisées. Ainsi, nous considérons qu'un seul niveau de cryptage est insuffisant.

Afin d'augmenter le niveau de cryptage de notre méthode, nous devons développer un deuxième niveau. Pour ce faire, nous allons utiliser une méthode très connue en cryptage optique qui est le cryptage à double phase aléatoire DRP (en anglais : Double Random Phase). Cette méthode est décrite en détail dans le paragraphe 2.6 méthode 1.

4.3.1 Deuxième niveau de cryptage

Pour rajouter ce deuxième niveau, nous récupérons le spectre complexe crypté avec le premier niveau (figure 3.17-b). Nous l'utilisons à l'entrée d'un système DRP comme cela est présenté en figure 4.6. Ensuite, nous multiplions séparément la partie réelle et la partie imaginaire avec des clés de phase aléatoires. Puis nous multiplions les spectres avec des nouvelles clés de phase aléatoire. Finalement, en passant dans le plan de sortie, nous obtenons notre image cryptée avec deux niveaux. Cette technique à deux phases aléatoires va augmenter le niveau de cryptage de notre méthode.

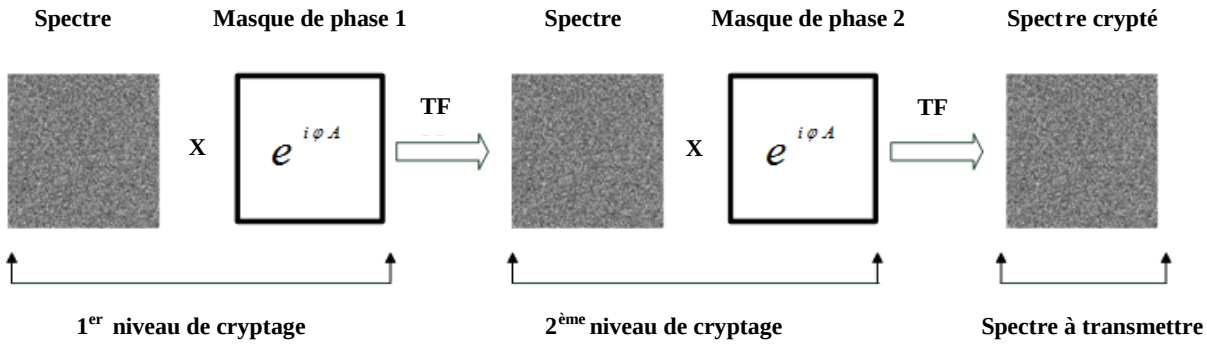


Figure 4.6 Schéma synoptique du deuxième niveau de cryptage.

La figure 4.6 montre les étapes réalisées pour fabriquer ce deuxième niveau de cryptage en utilisant la méthode DRP. En effet, la simplicité qu'offre cette méthode nous a permis de l'utiliser pour optimiser notre approche de cryptage.

4.3.2 Décryptage

Une fois le spectre crypté reçu par le destinataire, nous effectuons tout d'abord la phase de décryptage en réalisant le processus inverse de cryptage, c'est-à-dire supprimer les deux phases aléatoires rajoutées avec les deux niveaux de cryptage (figure 4.6). Puis nous réalisons la transformée de Fourier inverse et nous appliquons le processus de décryptage décrit dans le chapitre 3. Une fois que nous avons les images clés décryptées, nous pouvons par conséquent retrouver les images cibles.

Les résultats de simulation de compression/cryptage – décryptage/décompression sont présentés dans la figure 4.7.

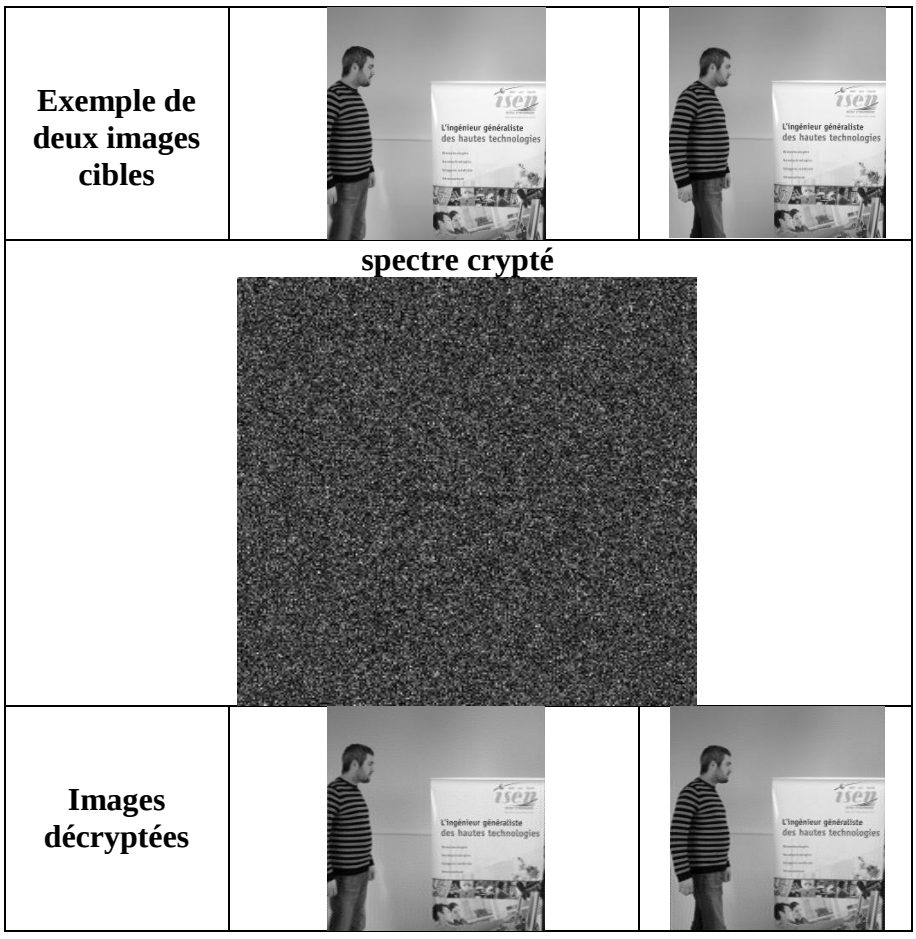


Figure 4.7 Résultat de simulation de décryptage en utilisant deux images cibles.

Ces résultats attestent bien des bonnes performances en termes de compression et de cryptage de notre méthode. Pour vérifier cela, nous avons appliqué notre approche en utilisant une vidéo présentant un char qui avance dans le plan d'une caméra (Fichier https://www.youtube.com/watch?v=5CS1rNLyALs). Les résultats de cette vidéo (tableau 5)

montrent dans la première partie à gauche les images cibles. Ensuite, la deuxième partie présente le spectre des 26 images multiplexées. La troisième présente le spectre crypté avec deux niveaux. Finalement, la partie à droite montre les images reconstruites après décompression et décryptage. La qualité des images décompressées et décryptées atteste bien de la bonne performance de notre approche proposée dans ce chapitre.

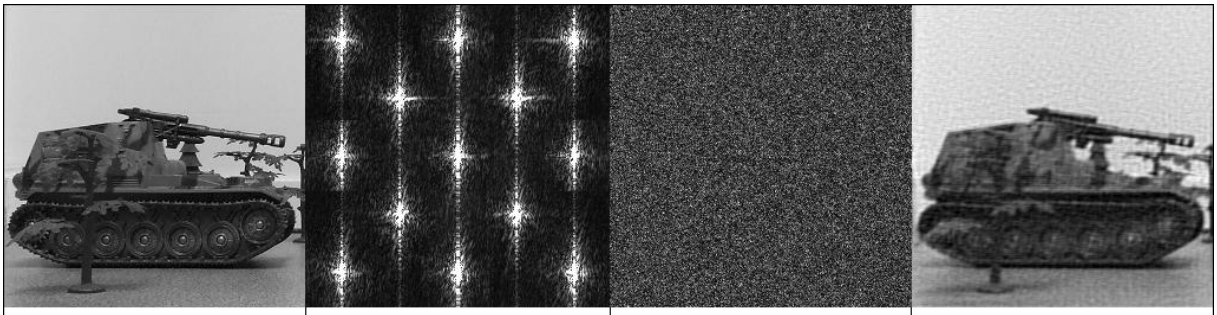


Image cible	Spectre compressé	Spectre crypté	Image décompressée et décryptée

Tableau 5. Résultat de décompression et décryptage avec une séquence « Char » : voir aussi le fichier multimédia (https://www.youtube.com/watch?v=5CS1rNLyALs).

4.3.3 Test de résistance de la méthode contre les attaques

Afin d'évaluer l'efficacité de la méthode de cryptage contre les attaques et pour tester sa robustesse, nous avons généré sous Mathlab une simulation d'attaque qui consiste à réaliser le processus de décryptage en générant un masque de phase aléatoire d'une manière arbitraire pour le multiplier avec le spectre de l'image cryptée. Ainsi, nous avons laissé le programme tourner pendant plusieurs jours jusqu'à atteindre 10^5 itérations. Les résultats de ces attaques sont présentés sur la figure 4.8 sous forme d'un calcul de MSE entre l'image cible et l'image piratée en essayant de la décrypter avec un masque de phase calculé d'une manière aléatoire.

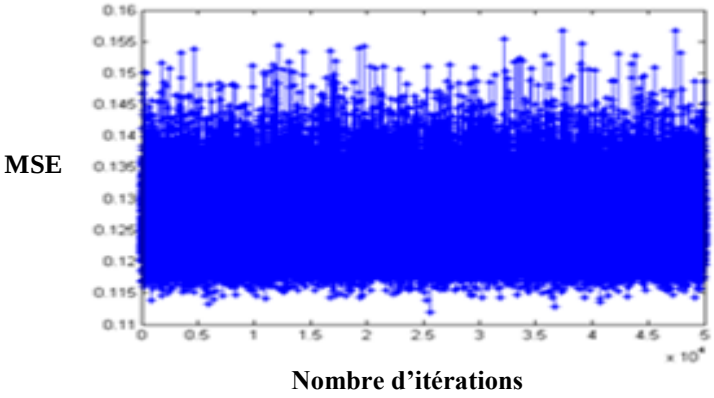


Figure 4.8 Résultat de simulation d'attaques.

Pour qu'il y ait craquage de cryptage il faut obtenir un MSE=0 or après 10^5 itérations la valeur de la MSE n'est pas égale à 0, elle reste aux alentour de 0,13 ce qui reste une valeur élevée. Cela atteste du bon comportement de notre méthode contre ce genre d'attaques. En effet, retrouver les combinaisons du deuxième masque de phase (une matrice aléatoire) correspondant dans le cas d'une image de taille de256x256 à trouver :

- (256 X 256) valeurs des phases situées aléatoirement entre 0 et π.

4.4 Application perspective : images polarisées

Auparavant, nous avons testé avec succès notre méthode avec plusieurs types d'images fixes ou vidéo. Dans cette partie, nous pensons faire une extension de nos travaux de recherche en appliquant notre méthode aux images polarisées.

En effet, l'intérêt de la polarisation de la lumière pour acquérir des images en milieu sous marin ne cesse de grandir depuis les années 1960. Le milieu sous marin est un milieu diffusant qui atténue la lumière. De nombreux articles relatent le gain apporté par l'utilisation de la polarisation de la lumière dans l'imagerie sous-marine. Gilbert et all ont montré, dans leur article [80], que l'utilisation de la polarisation circulaire permet d'augmenter le contraste et la distance de visibilité de la cible. Ces résultats ont été confirmés par Lewis et al. [81], qui ont montré que pour un contraste donné, la distance de visibilité avec une lumière polarisée peut être doublée par rapport à la distance obtenue avec un système qui n'utilise pas la polarisation. Il est donc utile d'étudier et de comprendre le principe de la polarisation de la lumière.

Nous commençons cette partie par une présentation des principes fondamentaux de la polarisation. Ensuite, nous nous intéressons au degré de polarisation (DOP). Puis nous allons appliquer ce principe des images polarisées sur des échantillons placés dans trois différents milieux air, eau et eau avec du lait.

4.4.1 Les principes fondamentaux de la polarisation

La lumière peut être décrite par une onde plane électromagnétique. Elle possède un champ électrique $\vec{E}$ et un champ magnétique $\vec{B}$ perpendiculaires entre eux et perpendiculaires à la direction de propagation de l'onde $\vec{Z}$ (figure 4.9). Le champ électrique s'écrit [84] :

$$\vec{E} = E_x \vec{x} + E_y \vec{y} + E_z \vec{z} \qquad (23)$$

Selon l'expression des termes Ex et Ey, on connait l'état de polarisation de la lumière (figure 4.10).

- La lumière a une polarisation linéaire si

$$\begin{aligned} E_x &= E_{0x}\cos(\omega t - kz) \\ E_y &= E_{0y}\cos(\omega t - kz) \\ \text{et } E_{0x} &= E_{0y} \end{aligned} \tag{24}$$

Les polarisations linéaires les plus couramment utilisées sont les polarisations verticales, horizontales et orientées à +45 °ou -45 ° par rapport au plan d'incidence.

- La lumière a une polarisation circulaire si

$$\begin{aligned} E_x &= E_{0x}\cos(\omega t - kz) \\ E_y &= E_{0y}\sin(\omega t - kz) \end{aligned} \tag{25}$$

- La lumière a une polarisation elliptique si

$$\begin{aligned} E_x &= E_{0x}\cos(\omega t - kz) \\ E_y &= E_{0y}\cos(\omega t - kz - \varphi) \end{aligned} \tag{26}$$

où E_{0x} et E_{0y} représentent l'amplitude maximale de l'onde plane, ω la pulsation, t le temps, k est le nombre d'onde, z la direction de propagation et φ le déphasage entre les composantes Ex et Ey.

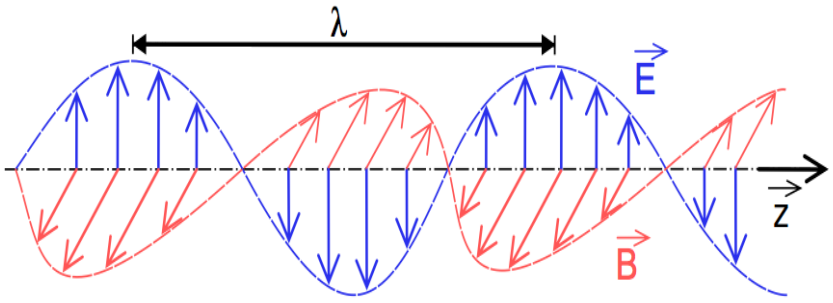


Figure 4.9 Onde plane polarisée linéairement de longueur d'onde **λ.**

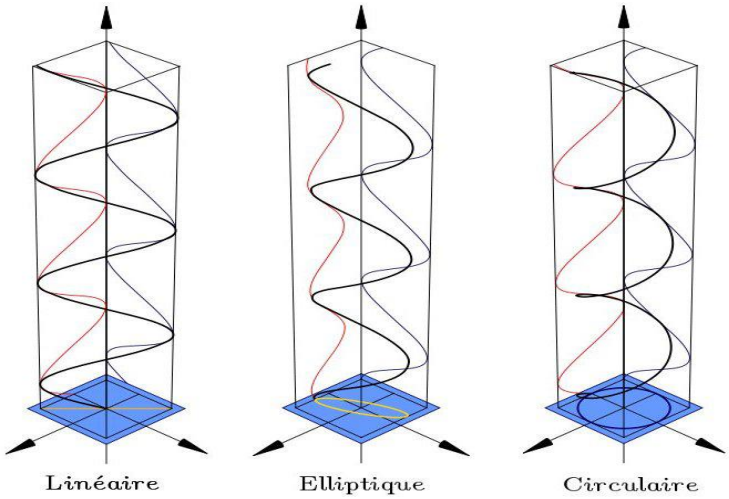


Figure 4.10 États de polarisation d'une onde : Les courbes rouge et bleue modélisent les composantes du champ électrique *E* (courbe noire).

Dans le cas d'une lumière dépolarisée, où les ondes n'ont pas toutes la même phase, la polarisation est aléatoire et ne correspond donc à aucun des trois cas précédents.

4.4.2 Degré de polarisation DOP

Une notion importante pour la compréhension de la polarisation est le degré de polarisation DOP (Degree Of Polarization) de la lumière. En effet, la plupart des lumières ne sont que partiellement polarisées, c'est-à-dire que seule une partie du vecteur champ électrique décrit dans le temps une trajectoire non aléatoire. Pour décrire ces ondes on utilise le formalisme de Stokes et Mueller. Le degré de polarisation de la lumière correspond au pourcentage du flux lumineux qui ne varie pas de façon aléatoire. Par exemple, si, après avoir été réfléchie sur un objet, une lumière est polarisée rectilignement à 80%, cela veut dire que 80% de la lumière à une trajectoire déterministe linéaire.

Le modèle de Stokes permet de représenter les états de polarisation de la lumière, via des grandeurs relatives aux intensités des composantes du champ ou à des combinaisons de ces intensités. Le principe est basé sur la détermination de quatre paramètres :

- S_0, représentant l'intensité totale de l'onde.
- S_1, S_2 et S_3, caractérisant son état de polarisation.

Avec cette représentation, il est possible de définir un coefficient DOP correspondant au degré de polarisation de l'onde :

$$DOP = \frac{I_{POL}}{I_{TOT}} = \frac{\sqrt{S_1^2 + S_2^2 + S_3^2}}{S_0} \qquad (27)$$

Sa valeur est comprise entre 0 pour une lumière non polarisée et 1 pour une lumière totalement polarisée. Les degrés de polarisation linéaire et circulaire sont définis de la manière suivante :

$$DOPL = \frac{\sqrt{S_1^2 + S_2^2}}{S_0}$$

$$DOPC = \frac{S_3}{S_0} \tag{28}$$

Pour connaître le DOP d'une lumière selon un état de polarisation donné, on utilise la formule suivante :

$$DOP = \frac{I_{//} - I_{\perp}}{I_{//} + I_{\perp}} \tag{29}$$

Où

- $I_{//}$ est l'intensité de la lumière dans l'état de polarisation où l'on souhaite connaître le degré de polarisation.
- $I_{\perp}$ est l'intensité de la lumière dans l'état de polarisation orthogonal (croisé) à l'état dans lequel on calcule le degré de polarisation.

Ainsi, pour connaître le degré de polarisation selon la direction linéaire horizontale, nous calculons :

$$DOP = \frac{I_{hor} - I_{vert}}{I_{hor} + I_{vert}} \tag{30}$$

Où

- I_{hor} est l'intensité en polarisation rectiligne horizontale.
- I_{vert} est l'intensité en polarisation rectiligne verticale.

De même, pour connaître le degré de polarisation selon l'état circulaire droit, nous calculons :

$$DOP = \frac{I_{CD} - I_{CG}}{I_{CD} + I_{CG}} \tag{31}$$

Où

- I_{CD} est l'intensité en polarisation circulaire droite.
- I_{CG} est l'intensité en polarisation circulaire gauche.

4.4.3 Montage expérimental

Pour obtenir des images polarisées, le laboratoire de l'ISEN dispose d'un montage expérimental conçu pour réaliser des images avec plusieurs états de polarisation. Le schéma synoptique de ce montage est présenté sur la figure 4.11.

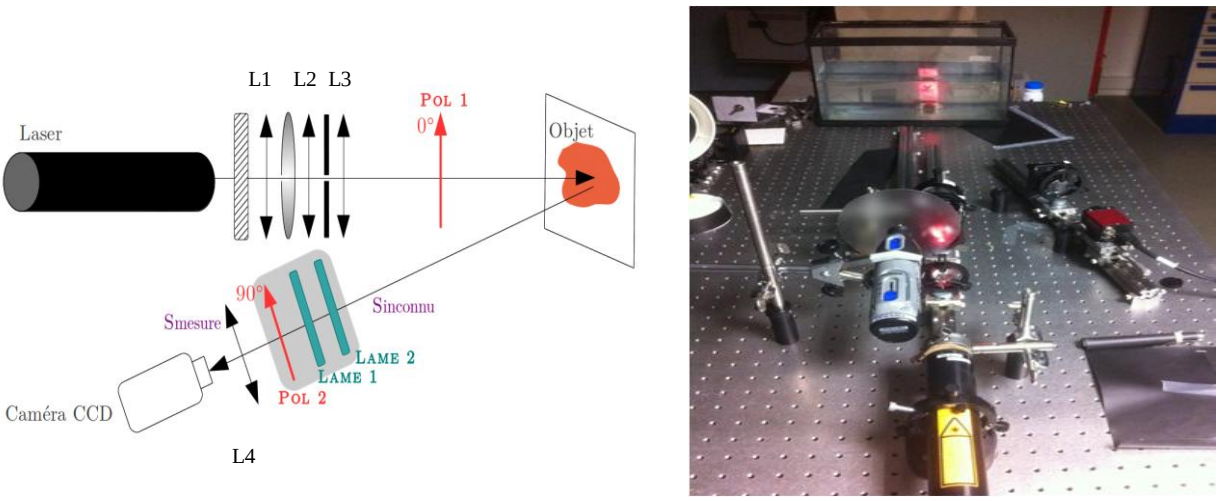


Figure 4.11 Schéma et photo du montage expérimental de polarisation des images.

Nous avons utilisé ce montage pour acquérir des images polarisées. Ce montage est composé d'une source Laser He-Ne 632 nm, d'un «Rotating diffuser», d'un filtre spatial composé d'une lentille convergente et d'un «Pinhole». Ensuite, nous avons une lentille collimatrice L3. Sur ce montage, nous avons deux polariseurs « Pol » l'un placé avant l'échantillon à étudier et l'autre après.

4.4.4 Compression et cryptage des images polarisées

Dans cette partie, nous allons étudier notre méthode de compression et cryptage avec des images polarisées à l'entrée de notre système. Dans notre cas nous avons opté pour un montage fonctionnant en réflexion (avant un angle de 10°) (figure 4.12). Deux lames de quart d'onde QWP sont placées avant et après l'échantillon à étudier (figure 4.12). L'échantillon étudié dans ce papier est composé de différents matériaux : le «smiley» en liège, et à coté des boules en plastique en haut à droite de l'image et en plomb en bas à droite. Cet échantillon est placé, soit dans l'air, soit plongé dans un aquarium rempli d'eau pure ou avec du lait pour simuler les effets de la rétrodiffusion. Enfin, nous avons une caméra CCD pour recueillir les images polarisées moyennant une lentille L4.

Figure 4.12 Échantillon à étudier pour les images polarisées.

4.4.5 Résultat des images polarisées dans l'air, dans l'eau et dans l'eau avec du lait

Avec ce montage, nous obtenons quatre images : Figure.4.13 (a-1) image circulaire croisée, (a-2) image circulaire parallèle, (a-3) image linéaire croisée et (a-4) l'image linéaire parallèle. En appliquant notre méthode de compression et de cryptage nous obtenons le plan comprimé et crypté présenté (b). Les images polarisées décomprimées et décryptées sont présentés en figure 2(c). Ces images montrent bien les bonnes performances de notre approche comme cela est attesté par des valeurs MSE très faibles. À partir de ces images, nous avons calculé les DOPL et DOPC [83] (figure 4.13-b).

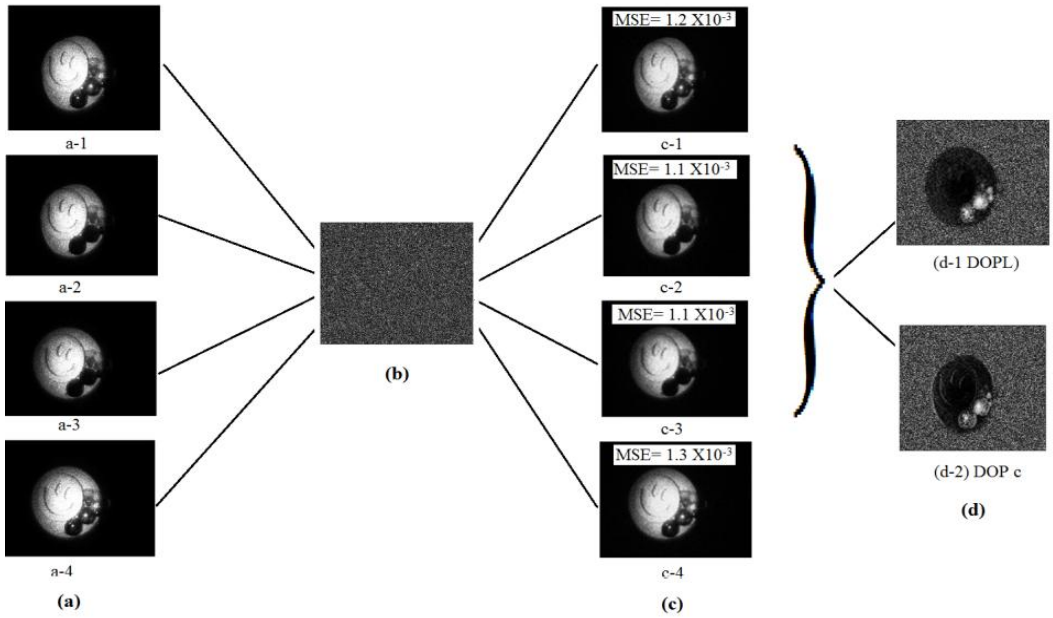


Figure 4.13 Résultat expérimental obtenu des images polarisées dans l'air.

Les résultats obtenus dans de l'eau pure et dans de l'eau avec du lait sont présentés dans les tableaux 6 et 7. La colonne 1 présente les images polarisées obtenues après décryptage et décompression ainsi que les DOPL et DOPC circulaire correspondantes. Les images obtenues dans de l'eau avec du lait sont présentés ligne 2. Les différentes images obtiennes dans l'air, dans l'eau pure ou avec du lait montrent bien le bon comportement de notre approche. En effet, comme cela est montré, les images reconstruites conservent les informations basses et hautes fréquences ; ainsi les images conservent aussi bien les informations contenues que les contours. De plus, notre méthode permet de recalculer avec une très bonne qualité les images DOP.

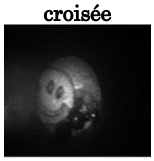
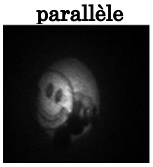
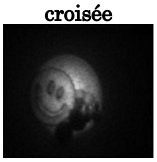
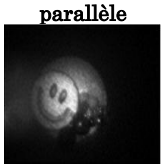
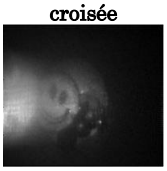
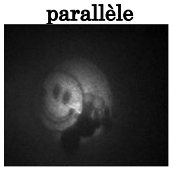
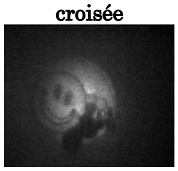
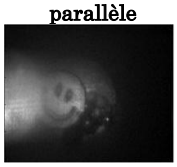
	Circulaire croisée	Circulaire parallèle	Linéaire croisée	Linéaire parallèle
Images polarisées dans de l'eau pure	 5.34 X10^{-4}	 4.15X10^{-4}	 3.52X10^{-4}	 6.75X10^{-4}
Images polarisées dans du lait	 1.96X10^{-4}	 1.83X10^{-4}	 3.12X10^{-4}	 1.92X10^{-4}

Tableau 6: Résultat expérimental des images reconstruites après compression et cryptage

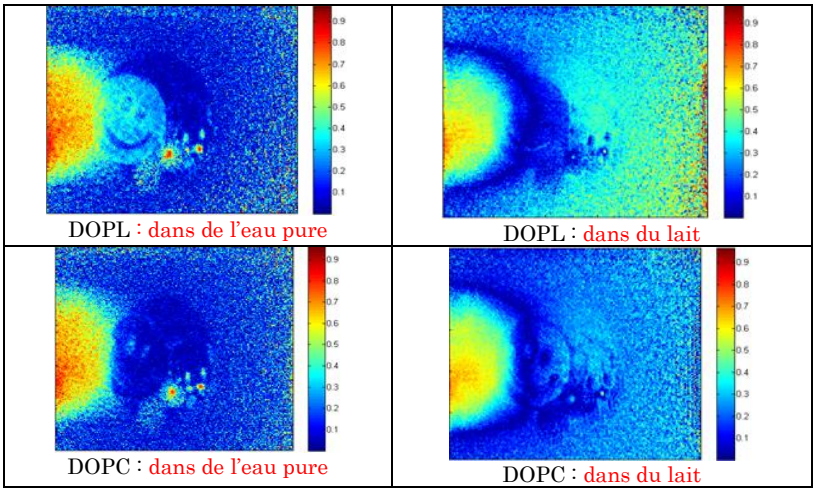


Tableau 7: Résultat expérimental des DOPC et DOPL d'images reconstruites après compression et cryptage

Dans cette partie, nous avons proposé et adapté l'utilisation de la méthode de compression et de cryptage dans le cas des images polarimétriques. Malgré la ressemblance entres les quartes images utilisées, nous obtenons une bonne qualité des images reconstruites cela est prouvé par les petites valeurs MES calculées. Notre méthode est donc parfaitement adaptée pour comprimer et crypter les images polarimétriques.

4.5 Conclusion

Dans la première partie de ce chapitre, nous avons proposé une optimisation qui se base sur la fusion par symétrie spectrale. Cette fusion nous a permis d'augmenter le nombre d'images cible jusqu'à 26 images multiplexées dans un seul spectre. Cette optimisation nous a aussi permis d'adapter notre méthode de compression et cryptage aux séquences vidéo. Cela est montré à travers les différents tests que nous avons réalisés. En effet, nous avons testé plusieurs types de séquences vidéo à l'entrée de notre méthode et cela donne des images reconstruites après décompression et décryptage de bonne qualité avec des petites valeurs de MSE.

Dans la deuxième partie de ce chapitre, nous avons proposé une nouvelle approche de cryptage optimisée avec deux niveaux de cryptage pour sécuriser les informations à caractère confidentiel dans les images cibles. Cette approche utilise un système de DRP classique pour crypter le spectre issu du premier niveau de cryptage. Les simulations que nous avons réalisées montrent que notre approche est robuste contre les attaques de craquage.

La troisième partie de ce chapitre est consacrée à une application perspective qui consiste à utiliser des images polarimétriques pour les comprimer et crypter. Les résultats obtenus ont montré que notre méthode est capable de traiter ce type d'images. La qualité des images reconstruites atteste que la méthode est performante quelque soit le type des images utilisées.

Conclusion générale et perspectives

Conclusion générale et perspectives

La compression des données est appelée à prendre un rôle encore plus important en raison du développement des réseaux de télécommunications. Son importance est surtout due au décalage qui existe entre les possibilités matérielles des dispositifs que nous utilisons et les besoins qu'expriment les applications. De plus, cet échange grandissant des données fait appel à la cryptographie pour sécuriser les informations transférées. Dans la littérature, il existe beaucoup de méthodes qui traitent de ces deux besoins : à savoir la compression et le cryptage de données. Cependant, la plupart de ces méthodes réalisent séparément la compression et le cryptage (en mode cascade), ce qui mène à une baisse de ces performances. Pour palier à ces problèmes, nous nous sommes intéressés dans cette thèse à des méthodes susceptibles de réaliser ces deux opérations (la compression et le cryptage) conjointement et d'une manière dépendante.

Pour ce faire, nous avons commencé cette thèse par un état de l'art des méthodes et techniques de compression et de cryptage existantes. Cette étude, nous a permis de constater que les méthodes à base de fusion spectrale sont parmi les méthodes les plus adaptées à la compression et au cryptage simultanés des images de notre point de vue. Ainsi, pour réaliser ces deux opérations simultanément, il fallait proposer des nouvelles approches qui permettent de trouver un bon compromis entre le taux de compression et le niveau de cryptage recherché.

Dans cette optique, nous avons mené un travail exploratoire des méthodes optiques de traitement d'information proposées dans la littérature et nous en avons simulées quelques-unes pour évaluer leurs performances. À travers cette étude, le montage 4f s'est imposé tout naturellement. De plus, nous avons constaté que la corrélation optique permet de faire la reconnaissance de formes en utilisant un simple filtre dans le domaine spectral. En effet, le filtrage consiste à éliminer les informations inutiles dans le plan spectral pour ne garder (dans le plan de sortie) qu'un pic de corrélation résultat de la comparaison entre l'image cible et l'image référence. Par conséquence, nous nous sommes intéressés à cette opération de filtrage pour faire de la compression en éliminant les informations redondantes.

Basé sur cette opération de filtrage, nous avons proposé et validé le principe d'une nouvelle méthode optimisée pour réaliser simultanément la compression et le cryptage des images. La méthode proposée est basée sur : (1) un filtrage spécial et (2) la réorganisation du plan spectral pour minimiser le plus possible le chevauchement entre les différents spectres d'images cible. (3) Une fusion pour multiplexer plusieurs informations des spectres en un seul.

La fusion spectrale utilise des critères comme la taille utile d'un spectre RMS et le critère d'énergie spectrale afin de sélectionner les informations représentatives de chaque image cible et d'augmenter ainsi la qualité des images reconstruites. Cette optimisation nous a permis une utilisation optimale du produit espace bande passante dans le plan spectral afin de transmettre les images rapidement.

Coté cryptage, nous avons aussi proposé et validé une approche robuste capable de bruiter efficacement le spectre fusionné issu du bloc de compression de notre système. En effet, nous avons proposé une nouvelle méthode basée sur la réalisation de deux niveaux de cryptage dans le plan spectral. Le premier niveau consiste à fabriquer une clé de cryptage optimisée avec un masque de phase aléatoire. Ce masque est développé à partir d'une répartition spectrale optimisée en fonction de trois composantes fréquentielles (BF, MF et HF). Le deuxième niveau de cryptage a pour objectif d'augmenter la sécurité de notre méthode. Il consiste à utiliser une technique de cryptage à double phase aléatoire (DRP) pour crypter le spectre issu du premier niveau.

Enfin, nous avons adapté notre méthode pour traiter les images vidéo en utilisant la symétrie spectrale et par conséquence augmenter le nombre d'images cible à l'entrée de notre système. Nous avons aussi fait une extension de nos travaux de recherche en appliquant notre méthode avec des images polarimétriques. Les tests de simulation que nous avons réalisés sont encourageants et montrent bien les bonnes performances de notre méthode à réaliser simultanément la compression et le cryptage de ce genre d'images. En effet, notre méthode est capable de traiter les images cibles quel que soit leur type avec une bonne robustesse contre les attaques.

Les perspectives que nous pouvons envisager consistent, dans un premier temps, à proposer des nouvelles optimisations pour améliorer la qualité des images décompressées. Cela se fera par l'utilisation de nouveaux critères pour sélectionner plus d'informations dans chaque image cible. Nous pouvons aussi tester notre méthode en prenant en compte le bruit stationnaire.

Quant au cryptage, nous pensons que les écarts entre les différentes composantes de fréquences peuvent présenter un point faible dans notre approche. Il faut donc étudier davantage la technique proposée pour l'améliorer ou proposer des nouvelles approches. Nous envisageons aussi de tester notre méthode avec d'autres types d'attaques pour évaluer sa vraie résistance contre le piratage. L'envoi de la clé de cryptage devrait être étudié pour choisir le type de clé publique ou privée qu'il faut utiliser.

Dans notre laboratoire, nous travaillons actuellement à l'implantation numérique de notre méthode sur une cible programmable de type GPU ou FPGA. Ainsi, cela va nous permettre de choisir une implantation sur un banc de tests, soit tout numérique, soit tout optique ou encore hybride (les filtres seront programmés sur carte électronique). Nous pensons que c'est cette dernière méthode qui sera la plus performante.

Troisième partie

Production Scientifique

Production Scientifique

1- Mohammed Adossari, Ayman Alfalou and Christian Brosseau, "Image Quality Assessment Based on a Multiple Image Optical Compression and Encryption," in *Frontiers in Optics 2011/Laser Science XXVII*, OSA Technical Digest (Optical Society of America, 2011), paper FThY4.

2- Mohammed Aldossari, Ayman Alfalou and Christian Brosseau, "Optimized fusion method based on adaptation of the RMS time-frequency criterion for simultaneous compression and encryption of multiple images ", *Proc. SPIE* 8748, Optical Pattern Recognition XXIV, 87480B (April 29, 2013).

3- Mohammed Aldossari, Ayman Alfalou, and Christian Brosseau, "Simultaneous compression and encryption of closely resembling images: application to video sequences and polarimetric images," Opt. Express **22**, 22349-22368 (2014).

4- Mohammed Aldossari, Ayman Alfalou, and Christian Brosseau, "Simultaneous Compression and Encryption of Polarimetric Images," in *Frontiers in Optics 2014*, OSA Technical Digest (online) (Optical Society of America, 2014).

5- Yousri Ouerhani, Mohammed Aldossari, Aman Alfalou, Christian Brosseau, "Numerical implementation of the multiple-image optical compression and encryption technique". Optical Pattern Recognition XXVI, SPIE Defense + Security (2015). (en cours)

Image Quality Assessment Based on a Multiple Image Optical Compression and Encryption

M. Aldossari[1], A. Alfalou[1] and C. Brosseau[2]

[1] *Département Optoélectronique, Laboratory L@BISEN, ISEN-BREST, 20 rue Cuirassé Bretagne, CS 42807, 29228 Brest Cedex 2, France*

[2] *Université Européenne de Bretagne, Université de Brest, Lab-STICC and Département de Physique, CS 93837, 6 avenue Le Gorgeu, 29238 Brest Cedex 3, France.* ayman.al-falou@isen.fr

Abstract: We test the ability of a multiple image optical compression and encryption (MIOCE) method to compress multiple images (video sequence). We investigate the influence of the number of images to be multiplexed in the Fourier domain and the spectral position of the phase-carrier on the quality of reconstructed images**.**

OCIS codes: 100.5010, 100.2000, 100.3008

1. Introduction

Optical encryption and compression methods have been in the forefront of image processing [1]. These two operations are generally achieved separately in a cascaded manner. An important manifestation of their interplay has been suggested to exist which may lead to image quality degradation. Unfortunately, previously demonstrated technologies which are capable of simultaneously realizing both operations are rare [2]. We recently suggested such method [3] for that specific purpose. As a proof-of-principle demonstration of its capability, we first describe how this method proceeds to merge the different images. Next, we optimize this procedure by shifting the different spectra in order to increase the quality of the reconstructed images. We accomplish this by considering a set of images belonging to a video sequence.

2. Principle of Multiple-Image Optical Compression and Encryption (MIOCE)

We first consider briefly the principle of the MIOCE method. The interested reader may consult Ref.[3] for more detail. Fig. 1 shows a synoptic diagram of this method. In a first step, the Fourier transform (FT) of the different images I_i considered is done. Next, a shifting procedure of the corresponding spectra S_i is realized. These spectra are then merged according segmentation and assignment rules which are analogous to those described in [3]. One main advantage of this procedure is that it permits to avoid isolated pixels. In addition to use a first encryption key, i.e. one of the input images, the

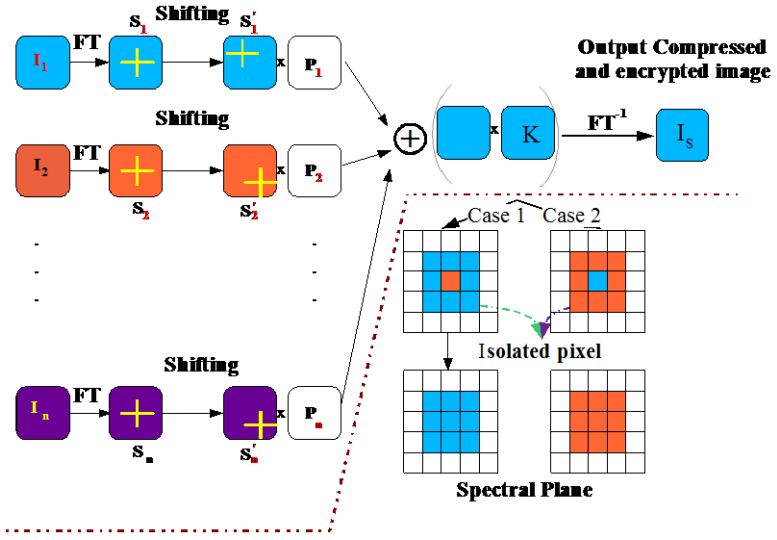


Fig 1. Synoptic diagram of the RMS time-frequency compression and encryption method for multiple-image

spectra are multiplied by a phase mask K. In the last stage, an inverse Fourier transform (FT^{-1}) is done in the Fourier plane to get a single encrypted image Is which contains the necessary information to reconstruct the target images I_i. To set a performance benchmark for the MIOCE's effectiveness in image processing applications, we consider the influence of the number of target images to be multiplexed. These images belong to a video sequence and have very similar spectral characteristics.

3. Results and discussion

Fig. 2 shows the evolution of the mean-square error (MSE) measure [3] as a function of the number of target images to be multiplexed. We point out that the close to zero MSE values is an indication of the good performance of the criterion used in this study. Fig. 2 (a) shows an example of a spectral plane with 13 multiplexed target images. The blue line in Fig. 2 (b) shows the MSE values obtained by comparing the target image I_1 with its

reconstructed image $I_1^{'}$ (the images have been normalised for the purpose of comparison). As an example of the functionality of our method the inset in Fig. 2 (b) indicates the calculated MSE values for the 13 target images. Our method achieves low values of the MSE. By exploiting the symmetry property of the real part of the spectra 26 images can be multiplexed with the same quality of those displayed in Fig. 2 (b).

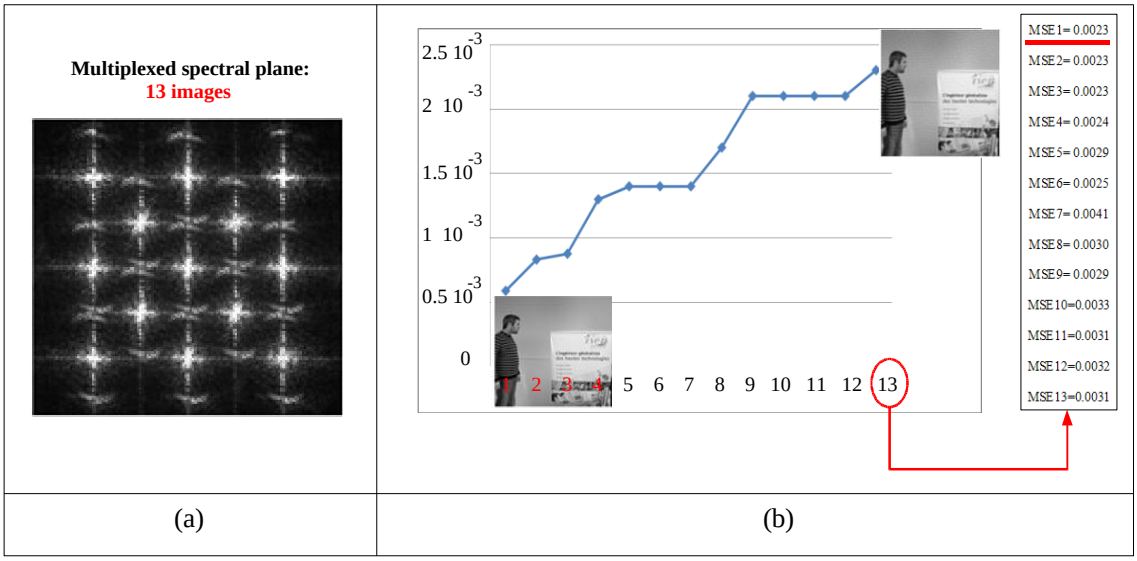


Fig2. Calculated MSE values as a function of the number of target images in the input plane.

It is interesting to observe a "step function" phenomenon in Fig. 2 (b), e.g. the MSE values are very close for 4, 5, 6 and 7 target images of the input plane. We believe this effect is related to the phase-carrier and shifting operation realized in the spectral domain. To confirm this point we have considered 3 target images and changing only the spectral position (Fig. 3). We observe that the MSE values differ according the choice considered (Fig. 3). That displayed in Fig. 3 (a) shows the lowest values of MSE. This specific configuration of the

target images is consistent with the minimum overlap between the spectra. Very few fundamental limitations exist apply to our procedure. However, the spectral positions of the images are of key importance for optimizing the multiplexing operation of the MIOCE method.

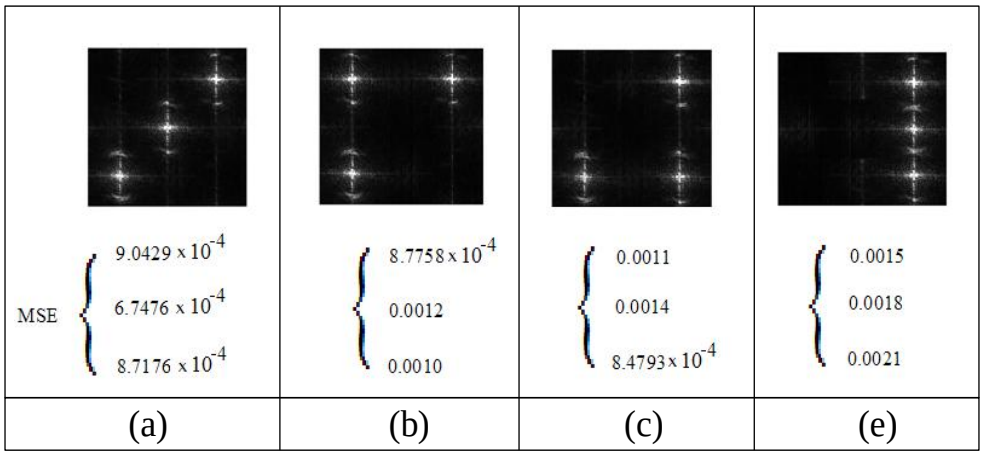


Fig3. Influence of the phase-carrier positions on the quality of the reconstructed images.

4. **References**

1. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon. **1**, 589-636 (2009).
2. G. Cristobal, P. Schelkens , H. Thienpont," Optical and Digital Image Processing: Fundamentals and Applications," Wiley, New York (2011).
3. A. Alfalou and C. Brosseau, "Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption," Opt. Lett. **35**, 1914-1916 (2010).

Optimized fusion method based on adaptation of the RMS time-frequency criterion for simultaneous compression and encryption of multiple images

M. Aldossari,[1] A. Alfalou,[1,*] and C. Brosseau[2]

[1]ISEN Brest, Groupe Vision, L@bISEN, 20 rue Cuirassé Bretagne, CS 42807, 29228 Brest Cedex 2, France.

[2]Université Européenne de Bretagne, Université de Brest, Lab-STICC and Département de Physique, CS 93837, 6 avenue Le Gorgeu, 29238 Brest Cedex 3, France.

*ayman.al-falou@isen.fr

ABSTRACT

An extension of the recently proposed method of simultaneous compression and encryption of multiple images [Opt. Lett. 35, 1914-1916 (2010)] is developed. This analysis allows us to find a compromise between compression rate and quality of the reconstructed images for target detection applications. This spectral compression method can significantly reduce memory size and can be easily implemented with a VanderLugt correlator (VLC). For that purpose, we determine the size of the useful spectra for each target image by exploiting the root-mean-square time-frequency criterion. This parameter is used to determine the allowed area of each target image within the compressed spectrum. Moreover, this parameter is adapted in order to minimize overlapping between the different spectra. For that purpose we add a shift function adapted to each spectra. Finally, the spectra are merged together by making use of a segmentation criterion. The latter compares the local energy relative to each pixel for each spectrum. Furthermore, it optimizes assignment of the considered pixel by taking into account the adjacent areas to the considered pixel. This permits to avoid the presence of isolated areas and small sized areas (less than 10 pixels). In this paper, we analyse and optimize the shift function needed to separate the different spectra. We use mean square error (MSE) for comparing compression rates. A series of tests with several video sequences show the benefit of this shift function on the quality of reconstructed images and compression rate.

Keywords: FFT, optical Fourier transform, compression, encryption, (MIOCE), RMS time-frequency criterion.

1- INTRODUCTION

Compression and encryption are necessary to transmit images in a secure manner. Optical compression and encryption have inspired many studies over the years [1-3]. Compression and encryption of a single image can be realized using different transforms [4-7], e.g. Fourier transform (FT), fractional FT (FrT). Over the last few decades, several methods have been proposed for considering multiple images [6-10]. However, very few studies have investigated compression and encryption simultaneously. A first step in this direction was reported recently in [11]. This work relied on image fusion in the spectral domain and use of the properties of the discrete cosine transform (DCT). In this study, we present an alternative procedure relying on the multiple-image optical compression and encryptions (MIOCE) [12-14], and apply it to several tests.

2- MULTIPLE-IMAGE OPTICAL COMPRESSION AND ENCRYPTION

The MIOCE procedure has four steps. The first step consists in Fourier transforming each target image. Secondly, the root-mean-square time-frequency criterion provides a means to quantify the size of each spectrum

$$\Delta I_1 = n\sqrt{\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}(u^2+v^2)\left|S_{I1}(u,v)\right|^2 dudv}\,, \tag{1}$$

where I_1 denotes a target image with spectrum $S_{I_1}(u,v)$, and the constant n is introduced to define the minimal size of the spectrum [12-14]. Thirdly, the different spectra are merged in the Fourier domain after shifting each spectrum of at least ΔI_1. In the fourth step, the encryption is realized. In this work, we analyze the influence of this shift on the quality of the reconstructed images and compression rate.

3- EFFECT OF THE SHIFT FUNCTION

In this section we show that our approach provides a quantitative means to find a compromise between the quality of the reconstructed images and the compression rate. We shall consider four target images of size (256×256) pixels and encoded over 8 bits. Figure 1 shows the synoptic diagram of the MIOCE method. After Fourier transforming each target image the four spectra are merged together using a segmentation criterion which is detailed in Refs. [12-14], and applying a shifting operation to minimize the effect of spectral overlap. For example, let us shift the center of each spectrum from its Fourier plane center along the diagonal as illustrated in Fig. 2. Then, the multiplexed spectrum is multiplied by a filter whose size depends of the size of the spectrum and shift (Fig 2). The filter's size is evaluated as

$$t = 2\Delta I + x = 2\Delta I + \sqrt{2}d\,, \tag{2}$$

where t is the filter's size in the Fourier plane, ΔI is the size of the image I spectrum (Eq. 1), x is the distance between S_i and S_j (S_i: is the center of spectrum i, S_j: center of spectrum j), and d is the shift (in pixels).

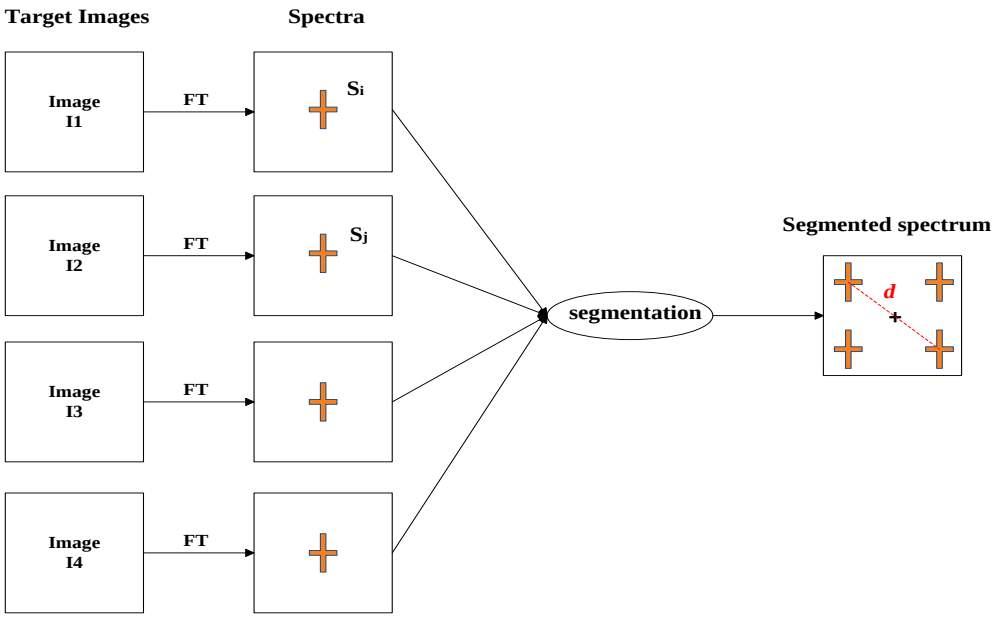


Fig.1: MIOCE synoptic diagram.

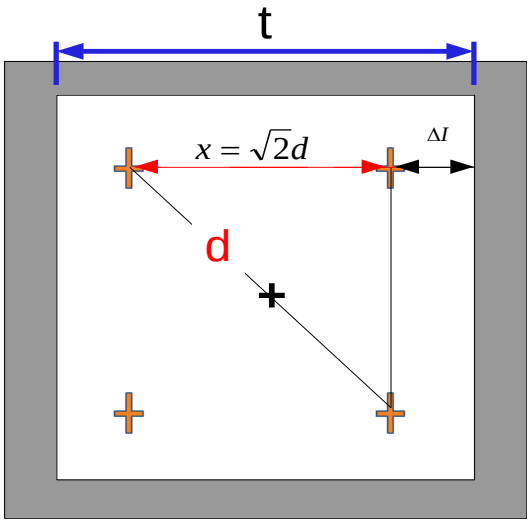


Fig. 2: Filter's size in the Fourier plane.

The result of this procedure is presented in Fig. 3. Figure 3(a) shows the four spectra with a shift set to 4 pixels. Each spectrum is multiplied by the filter represented in Fig. 3(b). Multiplexing these four spectra lead to Fig. 3(c). Corresponding results for a shift set to 64 pixels are respectively shown in Fig. 3(d), Fig. 3(e), and Fig. 3(f). As is evidenced in Fig. 3(c), a small value of the shit induces a spectral loss, and consequently a degradation of the reconstructed images. In contrast, a large value of the shift leads to a much better quality of images (Fig.3 (f)).

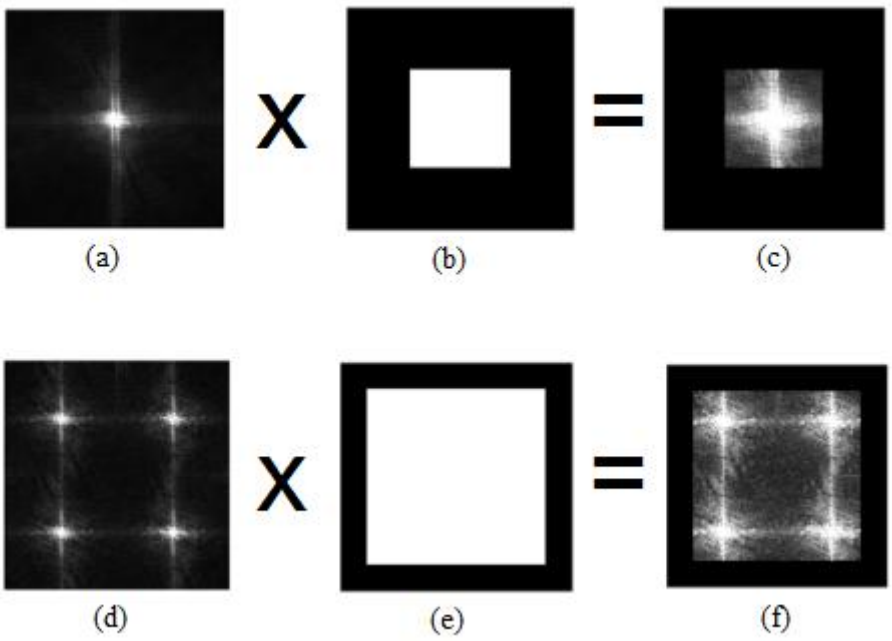


Fig. 3: Shift and filtering of the multiplexed spectra with (a, b, c) *d*=4 pixels and (d, e, f) *d*= 64 pixels.

In this study, the metric used for analyzing the quality of the reconstructed images is the mean square error (MSE) was calculated as a function of the number of pixels related to the shift (Fig. (4)). In Fig. 4, the horizontal axis shows the shift (in pixels) of the spectra with respect to the center of the Fourier plane.

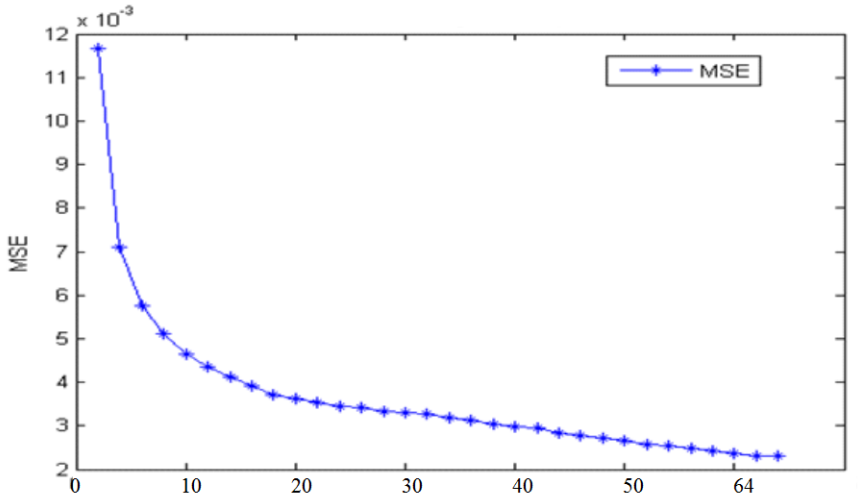


Fig. 4: Effect of spectral shift on the MSE.

As expected, the MSE values decrease monotonically with *d*. For *d*>20 we observe that the overlapping of the spectra is small and affects only weakly the quality of the reconstructed images. Using Eq. (1), one finds $\Delta I = 16$ (n=1). Now, the compression rate T_c is defined as

$$Tc = 1 - \frac{size\ of\ output\ file}{size\ of\ the\ four\ input\ images} = 1 - \frac{t^2 NO_{bits}}{2 \times 256^2 NI_{bits}}, \qquad (3)$$

where t is the size of the filter, $2t^2$ is the size of the filtered spectrum, NO_{bits} is the number of bits to encode the multiplexed spectrum, and NI_{bits} is the number of bits used to encode the target images. Figure 5 shows MSE and compression rate T_C. As shown in this figure, T_c increases with the shift value. Interestingly, the intersection between the curve of MSE and that of T_C for $\Delta I = 16$ constitutes a good compromise between the quality of the reconstructed images and the compression rate. Our numerical findings are also shown in Table 1. The main observation from these reconstructed images is that a good compromise between MSE and T_C corresponds to $d = \Delta I$.

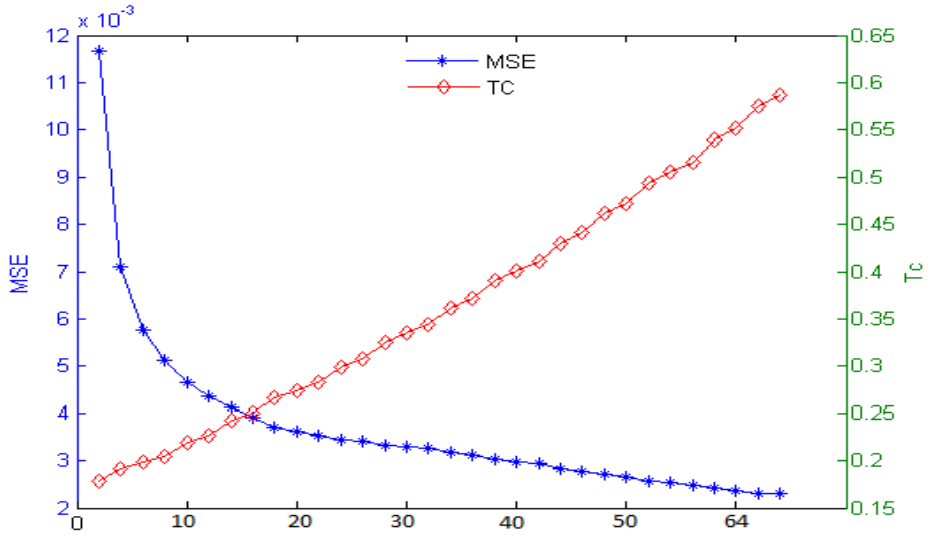


Fig. 5: Quality of the reconstructed images and the compression rate versus the shift distance.

4- CONCLUSION

In conclusion, we have developed a MIOCE method which can be used successfully to reconstruct images. It has been established that a shifting operation affects significantly the quality of the reconstructed images. We have shown how it is possible to estimate the shift value to obtain a good compromise between the quality of the reconstructed images and the compression rate. We find that the shift value should be close to the size of the spectrum obtained from Eq. (1).

Shift d (pixels)	Reconstructed image
d=4	
d=16	
d=36	
d=64	

Table 1: Reconstructed images by our procedure.

5- REFERENCES

[1] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon., 1, 589-636 (2009).

[2] A. Alfalou, A. Mansour, M. Elbouz, and C. Brosseau, "Optical compression scheme to multiplex & simultaneously encode images", in Optical and Digital Image Processing Fundamentals and Applications, G. Cristobal, P. Schelkens, and H. Thienpont (Editors), ISBN: 978-3-527-40956-3, Wiley, 463-483 (April 2011).

[3] A. Razzaque and N. V. Thakur, "An approach to image compression and encryptions," Int. J. Image Process. and Vision Sci., 1, 2278 – 1110 (2012).

[4] Q. Wang, "Optical image encryption with silhouette removal based on interference and phase blend processing," Opt. Commun., 285, 4294–4301 (2012).

[5] X. Wang and D. Zhao, "Optical image hiding with silhouette removal based on the optical interference principle," Appl. Opt. 51, 686-691 (2012)

[6] X. Yong-Liang, X. Su, S Li, X Liu, and S Zeng, “Key rotation multiplexing for multiple-image optical encryption in the Fresnel domain,” Optics & Laser Technology, 43, 889–894 (2011).
[7] Z. Liu, Y. Zhang, S. Li, W. Liu, W. Liu,Y. Wang, and S. Liu, “Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains,“ Opt. & Laser Technol., 47, 152–158 (2013)
[8] A. Alfalou, M. Elbouz, Ali Mansour, and G. Keryer, "New spectral image compression method based on an optimal phase coding and the RMS duration principle,” J. Opt., 12, 115403 (12 pp) (2010).
[9] N. K. Nishchal and T. J. Naughton, “ Flexible optical encryption with multiple users and multiple security levels,” Opt. Commun., 284, 735–739 (2011)
[10] Sudheesh K. Rajput and Naveen K. Nishchal, "Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform," Appl. Opt. **52**, 871-878 (2013)
[11] A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, “Simultaneous fusion, compression, and encryption of multiple images“ Opt. Express 19, Issue 24, 24023-24029 (2011).
[12] A. Alfalou and C. Brosseau, "Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption," Opt. Lett. 35, 1914-1916 (2010).
[13] A. Alfalou and C. Brosseau, "Using the RMS Time-frequency Structure for Multiple-image Optical Compression and Encryption," in FIO *Frontiers in Optics*, OSA Technical Digest, JTuA51 (2010). http://www.opticsinfobase.org/abstract.cfm?URI=FiO-2010-JTuA51
[14] M. Aldossari, A. Alfalou, and C. Brosseau, "Image Quality Assessment Based on a Multiple Image Optical Compression and Encryption," in FIO *Frontiers in Optics*, OSA Technical Digest, FThY4 (2011). http://www.opticsinfobase.org/abstract.cfm?URI=FiO-2011-FThY4

Simultaneous compression and encryption of closely resembling images: application to video sequences and polarimetric images

M. Aldossari,[1] A. Alfalou,[1,*] and C. Brosseau[2]

[1]Equipe Vision, L@BISEN, ISEN-Brest, 20 rue Cuirassé Bretagne CS 42807, 29228 Brest Cedex 2, France
[2]Lab-STICC, Université de Brest, CS 93837, 6 avenue Le Gorgeu, 29238 Brest Cedex 3, France
[*] ayman.al-falou@isen.fr

Keywords: optical filtering, spectral fusion, double random phase, compression, encryption, optical processing, polarimetric imaging.

Abstract: This study presents and validates an optimized method of simultaneous compression and encryption designed to process images with close spectra. This approach is well adapted to the compression and encryption of images of a time-varying scene but also to static polarimetric images. We use the recently developed spectral fusion method [Opt. Lett. **35**, 1914-1916 (2010)] to deal with the close resemblance of the images. The spectral plane (containing the information to send and/or to store) is decomposed in several independent areas which are assigned according a specific way. In addition, each spectrum is shifted in order to minimize their overlap. The dual purpose of these operations is to optimize the spectral plane allowing us to keep the low- and high-frequency information (compression) and to introduce an additional noise for reconstructing the images (encryption). Our results show that not only can the control of the spectral plane enhance the number of spectra to be merged, but also that a compromise between the compression rate and the quality of the reconstructed images can be tuned. We use a root-mean-square (RMS) optimization criterion to treat compression. Image encryption is realized at different security levels. Firstly, we add a specific encryption level which is related to the different areas of the spectral plane, and then, we make use of several random phase keys. An in-depth analysis at the spectral fusion methodology is done in order to find a good trade-off between the compression rate and the quality of the reconstructed images. Our new proposal spectral shift allows us to minimize the image overlap. We further analyze the influence of the spectral shift on the reconstructed image quality and compression rate. The performance of the multiple-image optical compression and encryption method is verified by analyzing several video sequences and polarimetric images.

OCIS codes*:* **(**100.2000) Digital image processing; (100.3008) Image recognition, algorithms and filters; (100.5010) Pattern recognition; (110.5405) Polarimetric imaging.

References and links

A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon. **1**, 589-636 (2009).

P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767-769 (1995).

Q. Wang, Q. Guo, and L. Lei, "Asymmetric multiple-image hiding using phase retrieval technique based on amplitude- and phase-truncation in fractional Fourier domain," Optik **124**, 3898-3902 (2013).

Z Liu, L Xu, T Liu, H Chen, P Li, C Lin, and S Liu, "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," Opt. Commun. **284**, 123-128 (2011).

Z. Liu, Y. Zhang, S. Li, W. Liu, W. Liu, Y. Wang, and S. Liu, "Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains," Opt.. & Laser Technol. **47**, 152-158 (2013).

S. K. Rajput and N. K. Nishchal, "Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform," Appl. Opt. **52**, 871-878 (2013).

Q. Wang "Optical image encryption with silhouette removal based on interference and phase blend processing," Opt. Comm. **285**, 4294-4901 (2012).

A. Alfalou and C. Brosseau, "Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption," Opt. Lett. **35**, 1914-1916 (2010).

A. Alfalou, A. Mansour, M. Elbouz, and C. Brosseau, "Optical compression scheme to multiplex and simultaneously encode images", in *Optical and Digital Image Processing Fundamentals and Applications*, (Wiley, 2011), pp. 463-483.

A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, "Simultaneous fusion, compression, and encryption of multiple images," Opt. Express **19**, 24023-24029 (2011).

A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, "Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks," Opt. Express **21**, 8025-8043 (2013).
J. W. Goodman, *Introduction to Fourier Optics*, 2nd ed. (McGraw-Hill, 1966).
A. Alfalou, C. Brosseau, and M. S. Alam, "Smart pattern recognition," Proc. SPIE 8748, Optical Pattern Recognition XXIV, 874809 (2013).
P. Katz, A. Alfalou, C. Brosseau, and M. S. Alam, "Correlation and Independent Component Analysis Based Approaches for Biometric Recognition," in Face Recognition: Methods, Applications and Technology, Adamo Quaglia (Editor) and Calogera M. Epifano (Editor), Chap 11, 201-229 (2012). ISBN: 978-1-61942-663-4.
M.R. Abuturab, "Color image security system using double random-structured phase encoding in gyrator transform domain," Appl. Opt. **51**, 3006-3016 (2012).
M.R. Abuturab, "Color information cryptosystem based on optical superposition principle and phase-truncated gyrator transform," Appl. Opt. **51**, 7994-8002 (2012).
S. K. Rajput and N.K. Nishchal, "Image encryption using polarized light encoding and amplitude and phase truncation in the Fresnel domain," Appl. Opt. **52**, 4343-4352 (2013).
M. Paturzo, P. Memmolo, L. Miccio, A. Finizio, P. Ferraro, A. Tulino, and B. Javidi, "Numerical multiplexing and demultiplexing of digital holographic information for remote reconstruction in amplitude and phase," Opt. Lett. 33, 2629-2631 (2008).
T. J. Naughton, Y. Frauel, B. Javidi, and E. Tajahuerce, "Compression of interference digital holograms for three dimensional object reconstruction and recognition," Appl. Opt.. **41**, 4124-4132 (2002).
E. Darakis and J. J. Soraghan, "Reconstruction domain compression of phase-shifting digital holograms," Appl. Opt. **46**, 351-356 (2007).
T. Tahara, K. Ito, T. Kakue, M. Fujii, Y. Shimozato, Y. Awatsuji, K. Nishio, S. Ura, T. Kubota, and O. Matoba, "Parallel phase-shifting digital holographic microscopy," Biomed. Opt. Express **1**, 610-616 (2010).
P. Xia, Y. Shimozato, T. Tahara, T. Kakue, Y. Awatsuji, K. Nishio, S. Ura, T. Kubota and O. Matoba, "Image reconstruction algorithm for recovering high-frequency information in parallel phase-shifting digital holography," Appl. Opt. **52**, A210-A215 (2013).
A. Alfalou and C. Brosseau, "Implementing compression and encryption of phase-shifting digital holograms for three-dimensional object reconstruction", Opt. Commun. **307,** 67-72 (2013).
F. Mosso, J. F. Barrera, M. Tebaldi, N. Bolognini, and R. Torroba, "All-optical encrypted movie," Opt. Express **19**, 5706-5712 (2011)
W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photon. **6**, 120-155 (2014).
W. Chen, X. Chen, A. Stern and B. Javidi, "Phase-modulated optical system with sparse representation for information encoding and authentication," IEEE Photon. J. **5**, 6900113 (2013).
E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett. **36**, 22-24 (2011).
W. Chen and X. Chen, "Double random phase encoding using phase reservation and compression," J. Opt. **16**, 025402 (2014).
N. Neji, M. Jridi, A. Alfalou, and N. Masmoudi, "A CABAC codec of H.264AVC with secure arithmetic coding," Proc. SPIE 8656, Real-Time Image and Video Processing 2013, 86560G (2013).
N. Neji, M. Jridi, A. Alfalou, and N. Masmoudi, "Evaluation and Implementation of Simultaneous Binary Arithmetic Coding and Encryption for HD H264/AVC Codec. SSD'13-IEEE, (2013).
M. Dubreuil, P. Delrot, I. Leonard, A. Alfalou, C. Brosseau, and A. Dogariu, "Exploring underwater target detection by imaging polarimetry and correlation techniques," Appl. Opt. **52**, 997-1005 (2013).
https://www.youtube.com/watch?v=5CS1rNLyALs

1. Introduction

As the amount of information to be transmitted become larger and faster, data compression is becoming a critical challenge in, e.g. video imaging. The objective of image compression is to reduce irrelevance and redundancy of the image data in order to be able to store or transmit data in an efficient form [1-7]. Image compression can be classified as lossy or lossless. Lossless compression is preferred for archival purposes and is often used for medical imaging. Lossy compression methods, especially when used at low bit rates, introduce compression artefacts. Lossy methods are especially suitable for natural images such as photographs in applications where minor (sometimes imperceptible) loss of fidelity is acceptable to achieve a substantial reduction in bit rate. In this work, we focus on lossy data compression. In an attempt to cope with the problem, several studies have been conducted in the past in academic institutions and industry, especially for telecommunications, access control, biometrics, and security systems. But only in the last few years quantitative techniques have been developed for simultaneous compression and encryption of images [1-11], and we have made contributions to this development [8-11]. These techniques open the way to a fuller control of the reconstruction of target images.

In the following, we shall focus our optical image processing analysis on the 4*f* system [12]. The justification for such an approach follows from the fact that image spectra can be manipulated between the reading and formation steps of the process. Using such an approach, the correlation between images has most recently been studied in numerical simulations and experimental observations for face recognition applications [13-14]. Very recently, Alfalou and Brosseau [1] pointed out that the 4*f* system gives a consistent way to compress and encrypt an image with a specific filter. On the one hand, redundant information can be suppressed. On the other hand, changing the distribution of the frequencies in images can dramatically change the representation of the data and allows us to render them useless for a hacker [1]. The problem one encounters is that the proposed methods have

either good performances in terms of compression or encryption of static images [1-8]. In general, these methods are useless if one wishes to process video sequences and realize simultaneously compression and encryption. Simultaneous compression and optical encryption schemes have been scarcely proposed and experimentally demonstrated. Most of the efforts have been restricted to encryption. For example, Abuturab and co-workers [14-15] suggested different approaches for encrypting color images based on the gyrator transform. Rajput and co-workers [16] used polarization for encrypting images in the Fresnel domain. Hence, the full taxonomy of the methods for simultaneously compress and encrypt multiple images which closely resemble like those of a video sequence still does not exist. For some problems, see Refs. [17-24]. In an earlier study [23], we reported on a simultaneous compression and encryption method based on the use of the discrete cosine transform (DCT). The 2D DCT gives an image of the intensity of low frequency to high frequency information, but the low frequency information is in the top-left corner and the high frequency information is in the bottom-right corner**.** This makes the information easier to manipulate. Mosso and co-workers [24] introduced a method to perform encryption of video images which combines standard double random phase encoding [2] and a specific fusion in the output plane. This method shows good performances but does not optimize compression, i.e. the fusion is done without taking into account the possible spectra overlap in the output plane. More specifically, this method requires large encoding bit sizes which has for effect to increase significantly the amount of data to be transmitted and/or stored. In addition, the role played by the size of the encrypted image in double random phase-amplitude optical encryption has attracted much interest [25-28]. For example, the authors in [28] proposed a method via phase compression to enhance double random-phase encoding security. In their method, only a compressed phase distribution is available in the CCD plane, and the amplitude component is not available or requested for optical decryption. Using a nonlinear correlation algorithm for authenticating the decrypted image high security can be achieved for this scheme.

In this study, we shall use different fusion methods [8-11] which are motivated by their application to face recognition in video sequences. Our primary objective is to develop a technique to operate simultaneously compression and encryption. We point out that our algorithm is rapid and accurate. Our results distinguish well among existing state-of-the-art by the ability of the proposed method to achieve simultaneously compression and encryption. The robustness and performances of our analysis were tested against experimental data, i.e. static images, video sequences, and polarimetric images. In each case, the images show close resemblance. It is further important to observe at the outset that video sequences were treated as multiple images without taking care of temporal redundancy, motion detection, or binary encoding [29-30], which are outside the scope of this study.

This article is structured as follows. In the succeeding section, we begin by presenting some important results on a simple method of compression and encryption using a spectral data fusion technique. In section 3 we analyze the performances of the suggested optimization and its impact on the compression rate and quality of the reconstructed images. The most important point of this work stems from the data in sections 7 and 9. In section 7, this approach is specialized to the analysis of video sequences. As an additional outcome of this approach, we study the double level encryption issue in section 9. We provide examples of decompression and decryption video, demonstrating the validity of the proposed technique. It will also be shown below that our analysis offers good performances for polarimetric images. In Section 10, we offer some conclusions.

2. Multiple-image optical compression and encryption (MIOCE) method

We have recalled that lossy compression consists of a transformation to reduce the amount of data needed to represent an image. In general, compression leads to degraded quality of the reconstructed image. As systems for performing real time optical comparisons (e. g. using an optical correlator which permits to compare a sampled image to a wide variety of reference images) have appeared optical compression is becoming a critical challenge [1-11]. Among those methods, those dealing with the phase of the Fourier transform (FT) of the image are notable. Figure 1 shows a much simplified schematics of the scheme [8]. We take advantage of the fact that the useful spectrum of an image does not spread over the entire Fourier plane (Fig. 1(a)). The rightmost panel of Fig. 1 shows that the spectral amplitude is localized in specific areas of the Fourier plane. This property can be used to realize data fusion with other images. For a proper understanding of this scheme it is important to be able to choose a criterion allowing us to select relevant data for each image. This arises because when an inappropriate fusion criterion is used (Fig.1 (b)), the reconstructed images have generally poor quality. This is due to the overlapping of the different spectra [8-9].

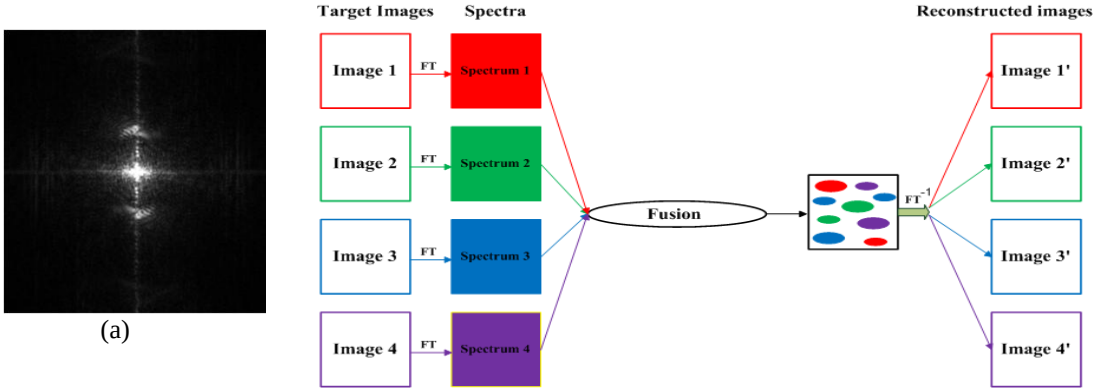


Fig. 1: (a) A spectrum of a typical image, (b) Schematic of typical spectral fusion.

It has been proposed [8] that this can be overcome by shifting the spectra before the fusion is realized (Fig 2(a)). We first estimate the spectrum width of each target image. For that, we used an adapted criterion based on the root-mean-square (RMS). Commonly accepted band-pass root-mean-square (RMS) criterion to determine the spectrum' width is expressed in our case as

$$\Delta_I = n\sqrt{\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}\left(u^2+v^2\right)\left|S_I\left(u,v\right)\right|^2 dudv}\,, \qquad (1)$$

where the index I denotes a target image, $S_I(u,v)$ is its spectrum, (u,v) are the spectral coordinates, and n is a parameter characterizing the minimal width of the spectrum. Each spectrum is then shifted in order to minimize their overlap. Next, the fusion criterion detailed in section 3 is carried out (Fig. 2(b)).

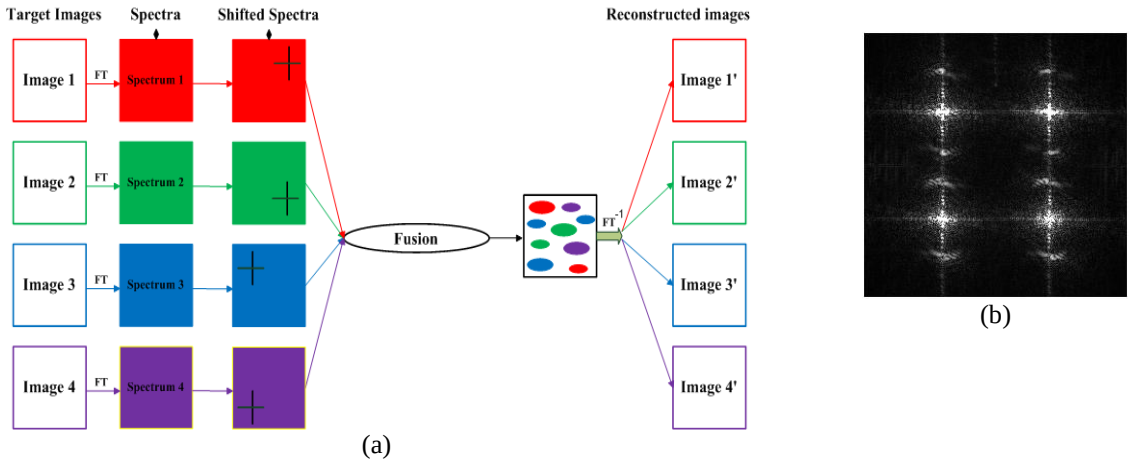


Fig. 2: (a) Schematic illustration of the MIOCE (multiple-image optical compression and encryption) method, (b) An example showing four shifted and merged spectra.

3. Spectral segmentation

Our explicit fusion strategy in the MIOCE method begins by partitioning the spectral plane into a large number of small regions (Fig 2(a)). To each of these regions is assigned information from the spectrum of the target images. Fig. 3 shows the key aspects of this assignment based on local energy. A simple example dealing with two target images (A and B), each with N pixels can be useful. Our analysis begins by calculating the spectrum of these two images. Then, for each pixel of the Fourier plane, we compare the (relative) spectral energy of the

image A in pixel (i,j), i.e. $X^{\mathrm{A}}{}_{\mathrm{ij}} = E_{ij}^{A} \Big/ \sum_{i=1}^{N}\sum_{j=1}^{N} E_{ij}^{A}$,with its counterpart for image B $X^{\mathrm{B}}{}_{\mathrm{ij}} = E_{ij}^{B} \Big/ \sum_{i=1}^{N}\sum_{j=1}^{N} E_{ij}^{B}$. The decision about pixel assignment to one of the two spectra is taken by comparing the (relative) spectral energies of A and B. This spectral segmentation has for aim to optimize the band-pass RMS of the Fourier plane which contains the fusion of the two spectra of the target images. Segmentation's rule can be expressed as:

$$\begin{cases} Pixel(i,j) = Spectrum\_A(i,j) & if \quad X_{ij}^{A} \geq X_{ij}^{B} \\ Pixel(i,j) = Spectrum\_B(i,j) & if \quad X_{ij}^{A} \prec X_{ij}^{B} \end{cases} \tag{2}$$

The success of this approach provides strong support for the contention that a single spectral plane provides all pertinent information for reconstructing the target images A and B (Fig.3).

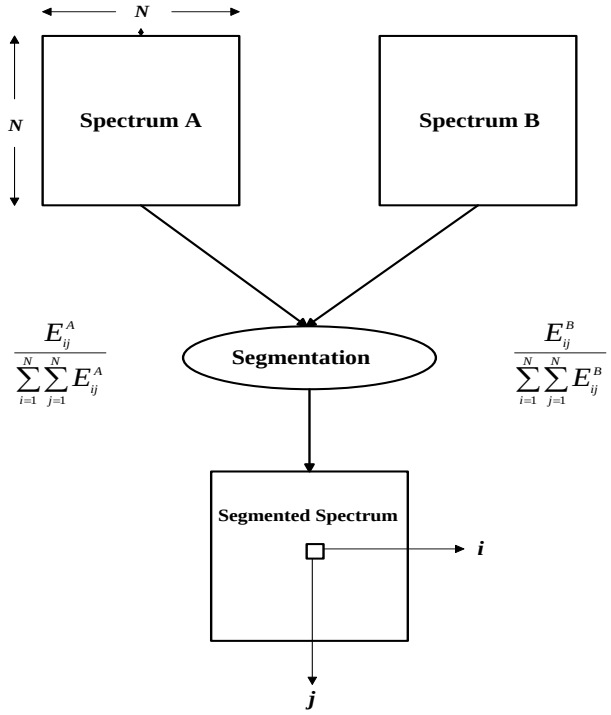


Fig. 3: Segmentation criterion and spectral assignment.

4. Image reconstruction with the segmentation criterion and without spectral shifting

One detrimental features of this segmentation protocol (proposed in [8]) is the occurrence of isolated pixels, i.e. an isolated pixel represents a pixel of a spectrum of image A which is surrounded by pixels of the spectrum of other images. This issue can be critical since this paper deals with sets of reference images bearing a strong resemblance (video sequence). A common descriptor of the quality of the reconstructed images is the mean square error (MSE) which characterizes the differences between the target and reconstructed images

$$\mathrm{MSE} = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left|I_d(i,j) - I(i,j)\right|^2 \tag{3}$$

where N is the number of pixels of the target image (here, set to 256), I_d is the decompressed image, and I is the target image. Preliminary results are shown in Table 1 for 4 selected images of a video sequence showing a person walking (column 2 of Table 1). The first column of Table 1 denotes the number in the sequence of numbered images. It is noticeable how poorly the reconstructed images (without spectral shifting, column 3 of Table 1) are. We attribute this low performance to the overlap between the different spectra, as is also evident from the large MSE values in this particular case. Similar degradations are observed when the number of input target images is increased.

Table 1: Reconstructed images obtained by making use of our fusion criterion. Columns 3 and 4 correspond respectively to without and with spectral shifting.

N°	Original images	Output images without spectral shifting	Output images with spectral shifting
1		 MSE=0.0294	 MSE=0.0013
2		 MSE=0.2982	 MSE= 0.0012
3		 MSE=0.3547	 MSE= 0.0012
4		 MSE=0.3068	 MSE= 0.0015

5. Influence of spectral shifting on the quality of the reconstructed images

The same analysis was performed with spectral shifting in order to avoid overlap as is shown in Fig. 4, where X and X' denote the spectral width (Eq. (1)) of the spectrum of each target images considered in this specific example.

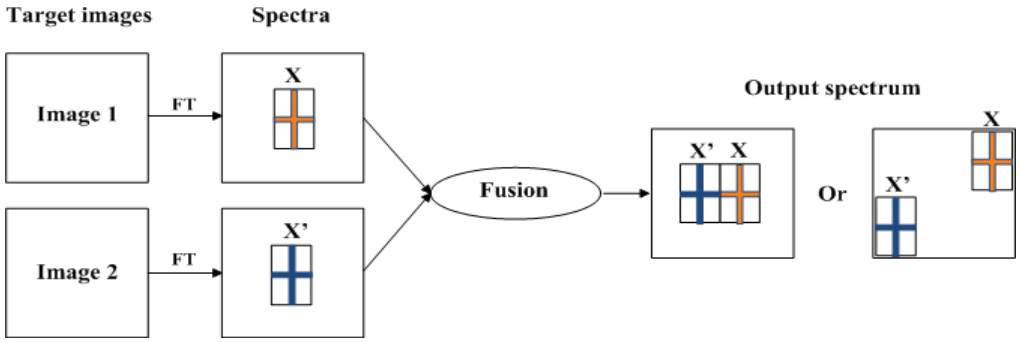


Fig. 4: Synoptic diagram of the MIOCE method optimized by making use of the shifted (RMS) criterion.

A few words are in order about our methodology. The results of using this spectral shifting to the above example are shown in Table (1-column 4). This technique achieves good performances if we compare visually with the results of column 3. This is also consistent with the smaller MSE values. Many tests have shown that this very effective technique has great impact on both on the image detail and compression rate. These tests also demonstrated that careful manipulation of the center of the spectrum image should be studied in order to provide a good trade-off between image quality and compression rate. The choice of shifting configuration influences the compression ratio. As an example, we have presented tow possibilities for this shifting. To find the good shifting configuration, for a given application, we propose the optimization presented on section 6.

6. Optimization of the MIOCE method and performance analysis as function of compression rate and quality of reconstructed images

6.1 Spectral shift

The above outlined method showed that the shifting operation in the Fourier plane is a crucial step. As an illustration of the manner in which the shifting of the center of three spectrum images can affect the reconstructed and decompression images (i.e. the MSE values), four situations are compared in Fig. 5. Note that in each case the spectral shift is larger than the spectral width calculated from Eq. (1).

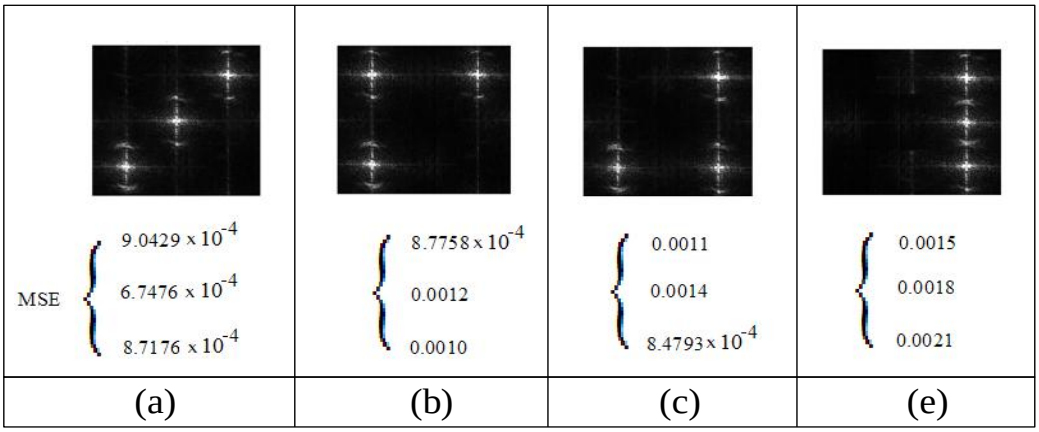


Fig. 5: Influence of the spectrum's position on the quality of reconstructed images.

It is revealing to see that the smallest MSE values are seen in Fig. 5(a), illustrating a spectral shift along the main diagonal. To this arrangement corresponds the smallest overlap between the three spectra. In contrast, the larger values of the MSE observed for the situations illustrated in Fig. 5(d) are consistent with the large overlap between the spectra.

6.2 Influence of the spectral shift of multiple target images on the quality of reconstructed images

The problem we address in this subsection is how the spectral shift d (Fig. 6) between the different spectra should be chosen? Or stated in other words, how d is chosen to get a good trade-off between reconstructed image detail and compression rate (Fig. 6).

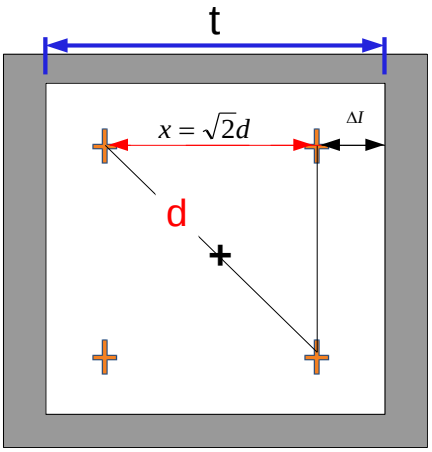


Fig. 6: Filter fabrication in the Fourier plane.

Figure 6 presents a given spectral plan $(N \times N)$ pixels . In this figure, we consider 4 images and a given shift d (in pixels). Then, the filter' size in the Fourier plane t is chosen by keeping only the pertinent information for reconstructing output images. The expression of t is

$$t = 2\Delta I + x = 2\Delta I + \sqrt{2}d \qquad (4)$$

where ΔI is obtained from Eq. (1). Consider the influence of the spectral shift d in the range [4, 64] pixels on the image quality. Figure 7(a) shows the four shifted spectra ($d = 4$ pixels) and segmented by making use of the energy criterion (Eq. (2)). Figure 7(b) shows the corresponding filter and Fig. 7(c) shows the results of the filtering operation. Figures 7(d)-7(f) show similar results for d=64.

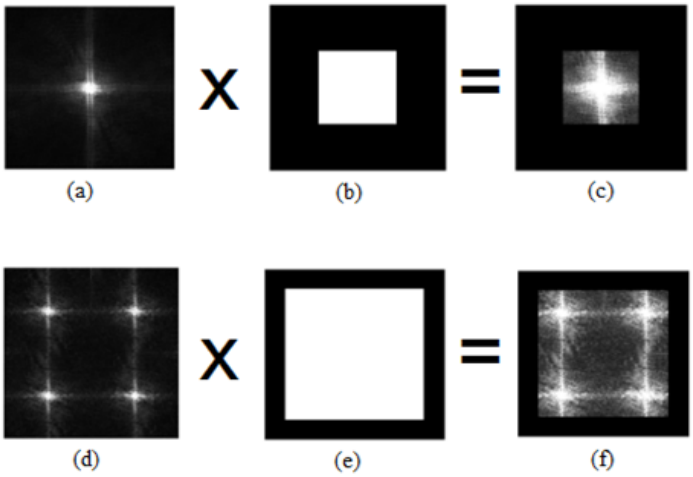


Fig. 7: Spectrum corresponding to four merged, shifted, and filtered target images.

In Fig. 7, we show that the spectral arrangement displayed in Fig. 6 presents the spectral plane with minimal width, but with poor quality of the reconstructed images (d=4 pixels) since there is a strong overlap between the spectra. Increasing d to 64 pixels has for effect to obtain a significantly better quality of images. In Fig. 8, we plot the MSE as a function of d (in pixels).

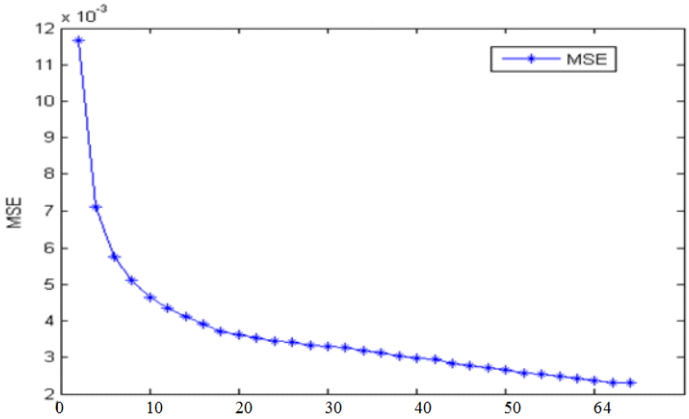


Fig. 8: Influence of the spectral shift on the reconstructed image quality: MSE as a function of the number of shifting pixels.

Figure 8 shows that the MSE decreases strongly up to d=16 pixels, and then slowly decreases. It is worrying how poorly the quality of the reconstructed images is improved using this technique for d>16 pixels. To avoid the need for search for an appropriate d every time, we set d=16 pixels in the following and use the remaining band-pass of the Fourier plane for merging more target images. Hence, compression rate T_c is increased while the images are reconstructed correctly.

6.3 Compression rate

The compression rate T_c is calculated as a function of the number of shifting pixels between spectra from

$$T_c = \left(1 - \frac{256 \times 256 \times Pri \times Bitd}{256 \times 256 \times n \times Bitc}\right) \times 100 \qquad (5)$$

where Pri is set to 2 (the spectrum is complex), $Bitd$ is the number of bits used for encoding the compressed spectrum (set to 16), n is the number of target images, and $Bitc$ is the number of bits used for encoding the target images (set to 8 for the gray level images considered). Hence

$$T_c = \left(1 - \frac{4}{n}\right) \times 100 \qquad (6)$$

Figure 9(a) summarizes the compression rate T_c and MSE as a function of the number of shifting pixels. As shown in Fig. 9(a), for the full range of parameters examined we consistently found that the T_c and MSE curves intersect at $d \approx 16$ pixels, consistent with our previous observation.

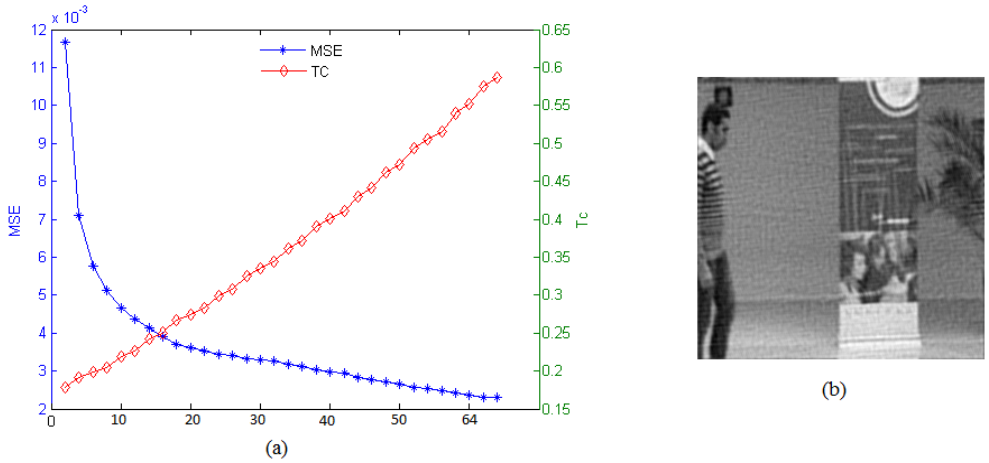


Fig. 9: (a) Compression rate and MSE as a function of the number of shifting pixels, (b) reconstructed image with a spectral shift set to 16 bits.

7. Adaptation to the compression of video images: Fusion and conjugate symmetry

To demonstrate the efficiency of the optimized-MIOCE method, we employ it to images of a scene with moving objects and varying illumination. Because one of our primary applications is the analysis of video sequence, we would like to process a large number of images. For that purpose, the use of symmetry of the spectrum allows us to eliminate half of the spectrum plane. Before the shifting and fusion operations are achieved, we begin by fabricating a binary filter with two blocks such as that shown in Fig. 10. The first block has pixels equal to 1 while the other has pixels set to 0. Then, the images spectra are multiplied two by two with this filter in the manner shown in Fig. 10. This approach has the advantage of keeping only 50% of each spectrum; the other 50% can be found by the conjugate symmetry which a basic property of the FT.

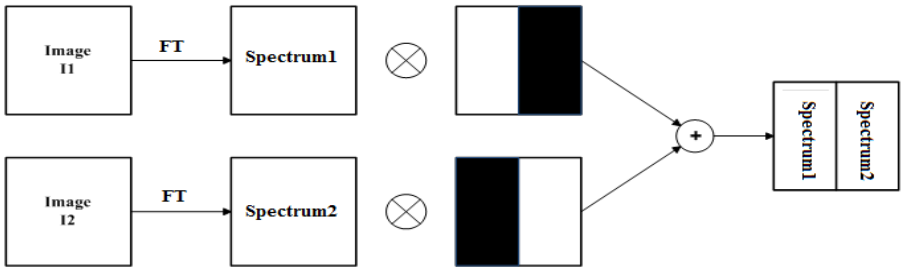


Fig.10: Synoptic diagram of the compression scheme par conjugate symmetry.

In the following, we consider a video sequence with 26 images (Fig. 11). These 26 images are then grouped two by two following the rule I_n and I_{n+13} as shown in Fig. 11.

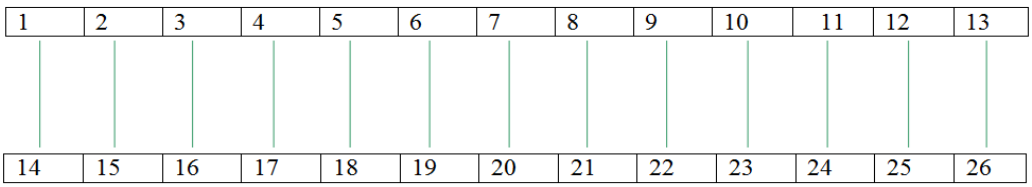


Fig. 11: Two by two grouping of a video sequence with 26 images.

The spectral shifting and the segmentation operations are then applied. This compression technique allows has to group 26 images in a single Fourier plane (Fig. 12).

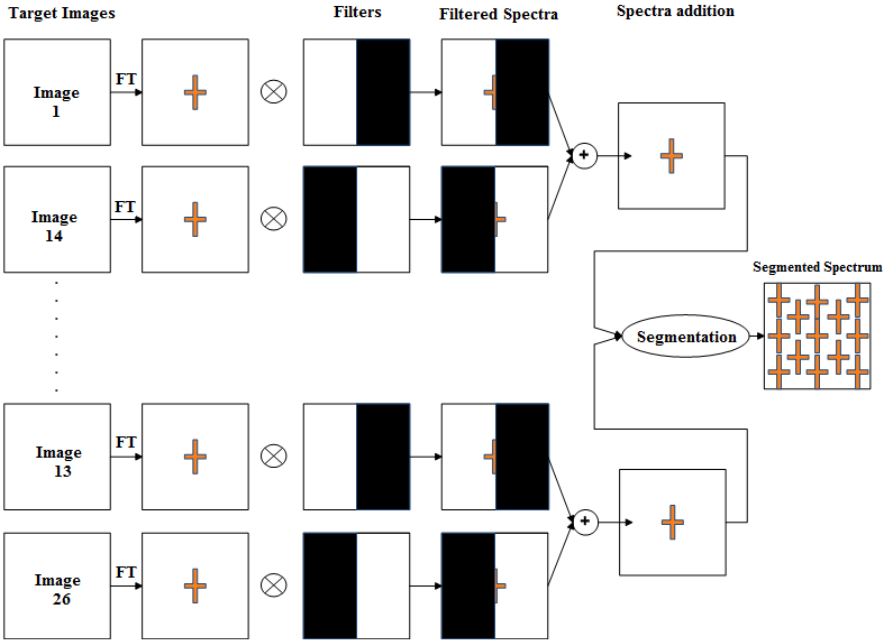


Fig. 12: Synoptic diagram of our compression technique adapted to video sequences.

8. Decompression and reconstruction of video images

Decompression is realized by applying the reverse of the compression operation. The 13 spectra are separated by multiplication with using a specific carrier signal. Only half of these 13 spectra are selected. The other half is reconstructed by making use of the conjugate symmetry. Finally, the inverse FT is realized to obtain the reconstructed image. We now apply our strategy of compression and encryption to special cases of video sequences. As a proof of principle, let us first consider a video sequence 1 (26 images). In Fig. 13 we present the spectrum resulting from the merging of 26 images of a video sequence.

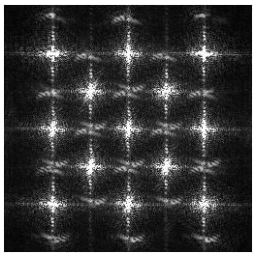
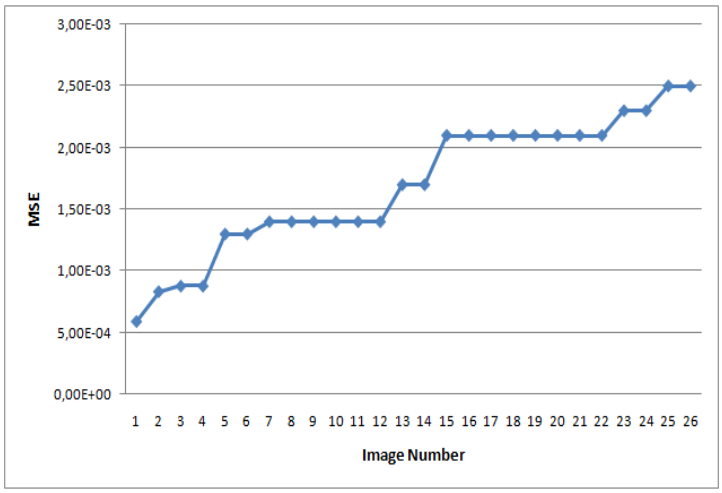


Fig. 13: An example dealing with the merging of 26 compressed spectra.

In Fig.14, the corresponding MSE is illustrated as a function of the number of target images. We show in Fig. 14(a) that the MSE increases (i.e. the quality of the reconstructed images decreases) as this number is increased. This is consistent with the fact that the large the number of target images is the small the band-pass of each spectral plane is. Additionally, several plateaus can be observed. These plateaus are related to the spectra localization after the spectral shifting. We begin by positioning the spectra as far as possible from image number 1 (upper right corner of Fig. 13). Close to this image the MSE values increase.



(a)

(b)

(c)

Fig. 14: (a) MSE as a function of the number of target images, (b) Examples of input and reconstructed images.

The fact that the MSE values are very small (even for the case of 26 images) demonstrates the good performances of our compression technique. This technique achieves good quality of the reconstructed images as shown by the comparison between the image in Fig. 14(b), i.e. one of the 26 images of the sequence, and the reconstructed image at the output of the system (Fig. 14(c)). We now consider the second example dealing 26 images of a second video sequence.

Table 2 summarizes the compression rate T_c as a function of the number of images (for 26 images, MSE=3.9 $\times 10^{-3}$).

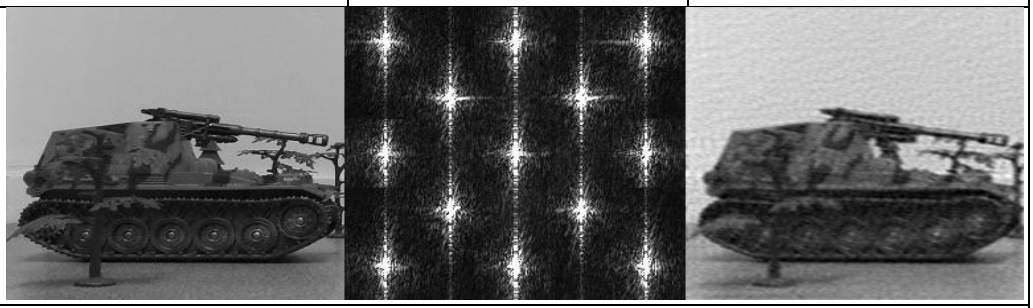
Table 2: Simulation results for the second video sequence (15sec.avi).

Number of target images	**Compression rate T_c**
5	20%
6	34%
7	43%
8	50%
9	56%
10	60%
11	64%
12	67%
13	70%
14	71.5%
15	73.3%
16	75%
17	76.5
18	78.8
19	79%
20	80%
21	81%
22	81.8%
23	82.6%
24	83.3%
25	84%
26	84.6%

We first consider the case of five target images to be compressed. Taking a quantitative example from Table 2, if one considers 26 images, then the compression rate achieves its largest value of 84.6%, i.e. with only 25% of the information contained in each image. Our algorithm is effective to reconstruct the sequence with minimal MSE (3.5×10^{-3}). Our technique results in a good reconstructed image quality and a good compression rate is achieved.

The third example deals with video containing 26 images of a tank moving at a constant speed (15sec.avi [32]). We present the compressed and merged spectrum to transmit and/or to store. Next, the compressed and encrypted spectrum is shown. The right part shows the reconstructed images obtained from our compression and decompression technique. The results of using our method to this example are shown in Table 3. The reconstructed images have good quality and the MSE values are small. This is clear indication that our method is robust and easy to implement even for moving targets. See the video results d-15sec.avi [32] for details.

Table 3: Compression results with tank video (See d_15sec.avi for details in [32]).

	Target image Size : 256 × 256 pixels	**Transmitted spectrum** Size: 256 × 256 pixels	**Reconstructed image** Size: 256 × 256 pixels
Example of d-15sec			
	MSE= 0.0018		

9. Encryption

In this section, our objective is to provide an effective encryption protocol to encrypt of the merged and compressed spectrum (e. g. Fig. 15). It is of interest to see how the confidentiality of data in video sequences is preserved. For that, we used the principle of spectral segmentation (described in section 3) to change the spectral distribution in the Fourier domain. Once the spectral plane merging the spectra of the different target images is obtained (Fig. 15), it is multiplied by a random mask (amplitude and phase). The latter should be fabricated for the considered application and it should allow us to hide the amplitudes as well as the phases of the merged spectra. It is worth emphasizing that the use of a simple phase mask in the spectral plane is insufficient to hide all information since the spectral amplitude remains unaffected like in the double random phase scheme. Additionally, one cannot apply phase masks to the target images since they will impact the segmentation operation described in section 3. As an alternative we suggest to fabricate an encryption mask allowing us to encrypt both amplitude and phase in the spectral plane. To illustrate this encryption approach we consider the case of two target images (Fig. 15)

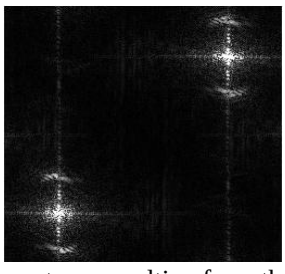


Fig. 15: Example of target spectrum resulting from the merging of two target images.

The fabrication of the encryption mask is presented in Fig. 16. First, we consider two key images (for m target images, m key images should be considered). After applying the FT to these key images the spectral segmentation scheme developed in section 3 is applied. Hence, two key spectra are obtained. In Fig. 16, we illustrate the selected (blue and red) areas for each spectrum. Next, two random amplitude and phase masks are fabricated by considering the maximum values ($rand \in [0, m_{max}]$) of the two key spectra (m_{max}: denotes the

maximum value of the spectrum's amplitude according to the considered spectrum). Next the two key spectra are merged to obtain the amplitude and phase encryption mask. Finally, this mask is multiplied by the target spectrum shown in Fig. 15.

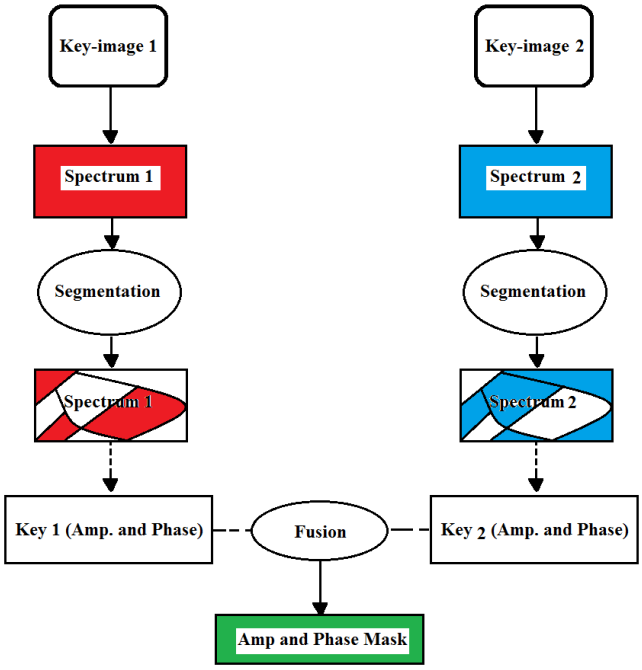


Fig.16: Illustrating the fabrication of the encryption mask.

Figure 17 shows clearly that this is not an effective encryption technique. Several regions can still be detected which may be used by a hacker to look for useful information. This arises because of the dynamics of the frequencies contained in the spectrum, i.e. the value of max-min. For the illustrative example shown in Fig. 17, an encryption mask with random values ranging between min and max is fabricated.

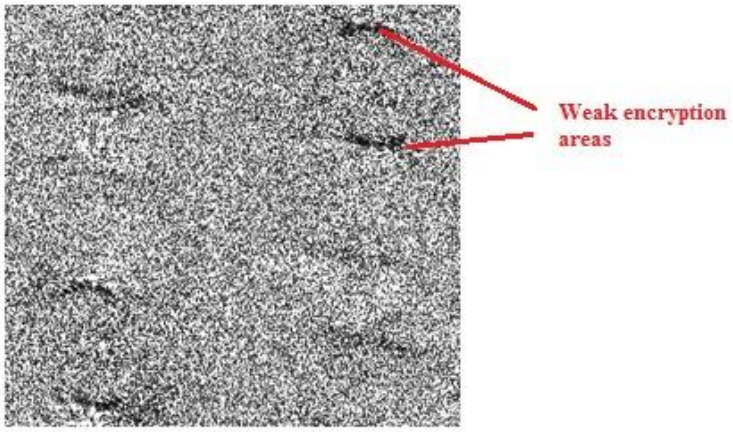
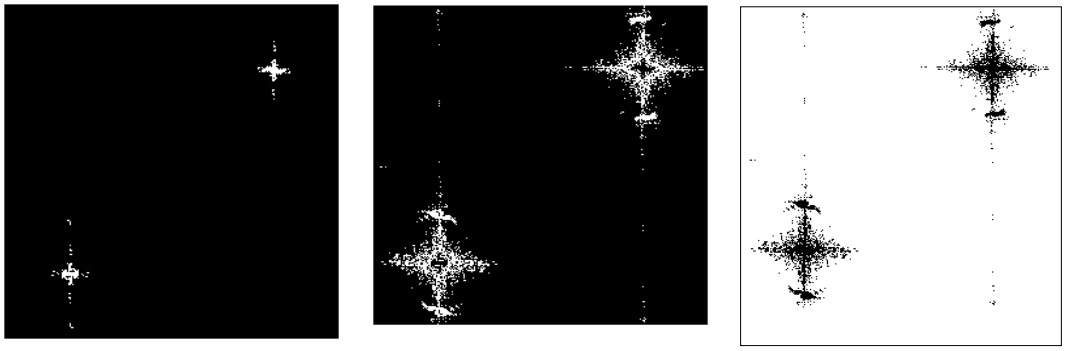


Fig. 17: Target spectrum encrypted with a random mask.

9.1 Optimization of the encryption key

To overcome this problem, we proceed as follows. We divide the encryption mask in three regions corresponding to high, intermediate, and low frequencies, which are processed separately (Fig. 18). For each region a random mask is fabricated by determining the min and max values for each region.



High frequencies : Mask M1 | Intermediate frequencies : Mask M1 | Low frequencies : Mask M1

Fig. 18: Division of the encryption mask in three regions (M1, M2, and M3).

In a first step, we calculate the maximum value of the amplitude spectrum $m_{\max}$ in the weak encryption area (shown in Fig. 17). Then we divide the spectral plane into three parts (Fig. 18): M1 correspond to frequencies with amplitude $> m_{\max}$, M2 correspond to frequencies with amplitude in the range $\left]\frac{m_{\max}}{4}, m_{\max}\right[$, and M3 corresponds to frequencies with amplitude $\leq \frac{m_{\max}}{4}$. These three components are used to fabricate three random masks $S1_{\text{cryp}}$, $S2_{\text{cryp}}$, and $S3_{\text{cryp}}$ (see Fig. 19).

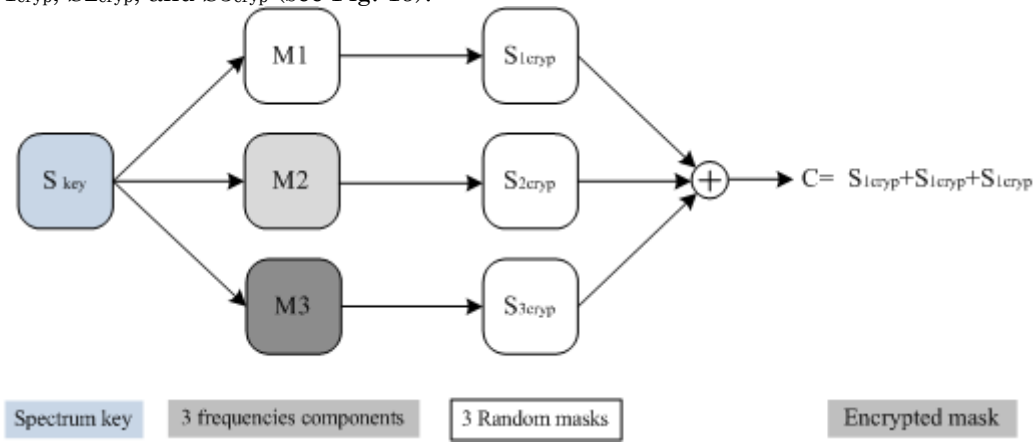
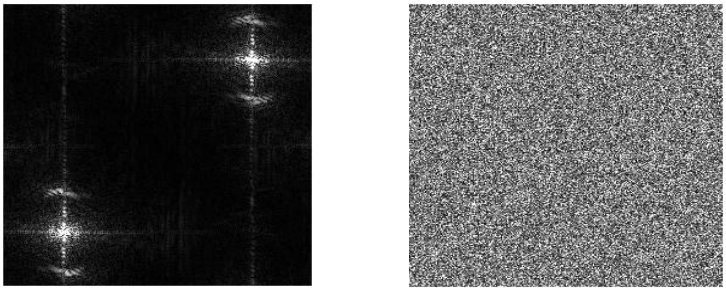


Fig. 19: Fabrication of the encrypted mask: $C=S_{1\text{cryp}}+S_{2\text{cryp}}+S_{3\text{cryp}}$.

The three random masks satisfy

$$\begin{aligned} S_{1cryp} &= rand[\min(M1), \max(M1)] \\ S_{2cryp} &= rand[\min(M2), \max(M2)] \\ S_{3cryp} &= rand[\min(M3), \max(M3)] \end{aligned} \tag{7}$$

where the function *rand* (*a*,*b*) generates a random number between *a* and *b*. Encryption of the target spectra is realized using the key $C=S_{1\text{cryp}}+S_{2\text{cryp}}+S_{3\text{cryp}}$ (Fig. 20(a)). The encrypted spectrum with these three masks is displayed in Fig. 20(b). This produces improvement in encryption quality for each test realized.



(a) (b)

Fig. 20: (a) Target spectrum merging two images, (b) encrypted spectrum with key $C=S_{1\text{cryp}}+S_{2\text{cryp}}+S_{3\text{cryp}}$

9.2 Second encryption level

A second encryption key, based on the double random-phase encryption scheme, is considered to improve the security level of our method. The spectrum obtained at the first encryption level (Fig. 20(b)) $C = S_{1cryp} + S_{2crup} + S_{3cryp}$ is multiplied by the random phase ϕ^1_{Ran} (with the constraint that $\phi_{\text{Encryp}} + \phi^1_{\text{Ran}} \neq 0$)

$$C' = \left(S_{1\text{Encryp}} + S_{2\text{Encryp}} + S_{3\text{Encryp}}\right)\exp\left(\text{i}\phi^1_{\text{Ran}}\right) = S_{\text{Encryp}}\exp\left[\text{i}\left(\phi_{\text{Encryp}} + \phi^1_{\text{Ran}}\right)\right]. \quad (8)$$

Figure 21 illustrates the second level encryption scheme. The input of our system is the first-level encrypted complex plane (Fig. 20(b)). Then the real and imaginary parts of the spectrum are independently multiplied by random phase keys. After a FT we obtain the encryption image that is multiplied by the second encryption random phase key ϕ^2_{Ran}. Then,

$$C'' = \text{FT}\left(C'\right)\exp\left(\text{i}\phi^2_{\text{Ran}}\right) = \text{FT}\left\{S_{\text{cryp}}\exp\left[\text{i}\left(\phi_{\text{Encryp}} + \phi^1_{\text{Ran}}\right)\right]\right\}\exp\left(\text{i}\phi^2_{\text{Ran}}\right). \quad (9)$$

Finally, after a second FT, the two-level encrypted image in the output plane is obtained

$$T_{\text{two\_level}} = \text{FT}\left\langle \text{FT}\left\{\text{S}_{\text{Encryp}}\exp\left[\text{i}\left(\phi_{\text{Encryp}} + \phi^1_{\text{Ran}}\right)\right]\right\} \times \exp\left(\text{i}\phi^2_{\text{Ran}}\right)\right\rangle . \quad (10)$$

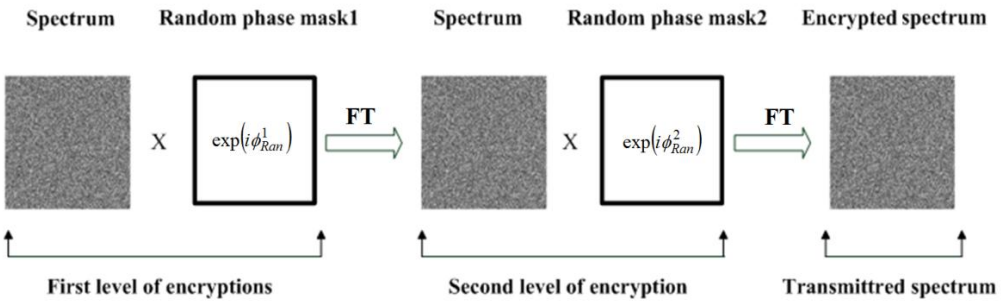
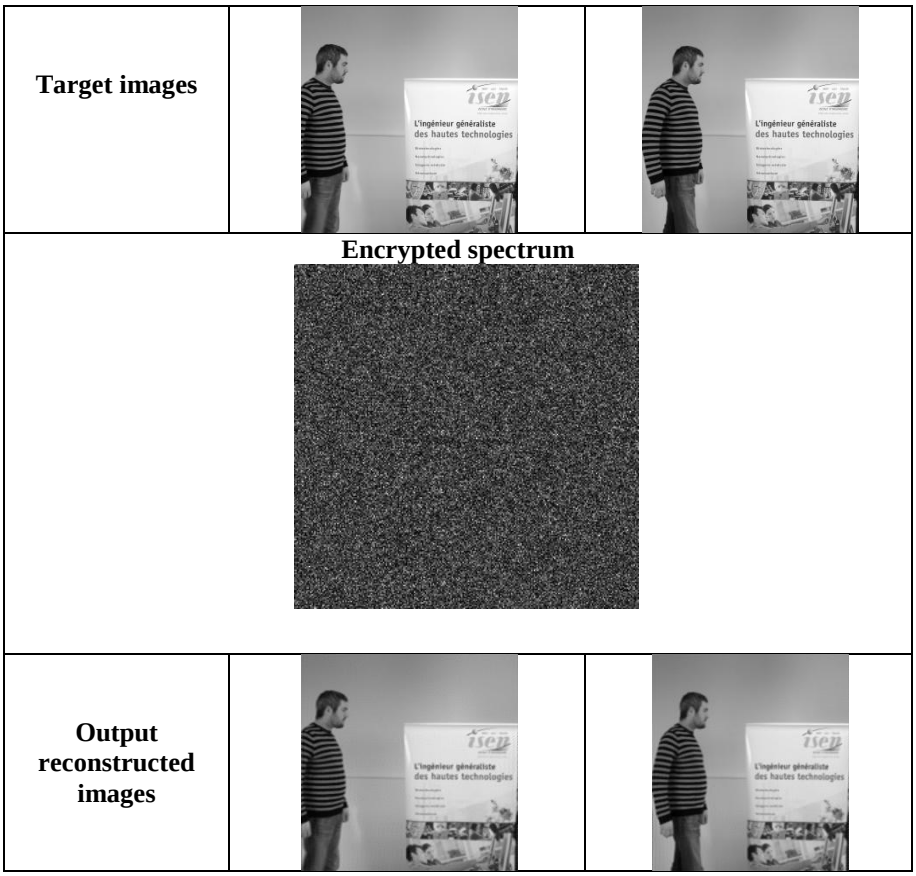


Fig.21: Illustrating the second level of encryption.

Once the encrypted spectrum is obtained, the reverse encryption operation (decryption) is done by suppressing the two random phases, then the inverse FT is realized to find the images used for fabricating the encryption keys, and eventually find the target images. The results of using this compression/encryption–decryption/decompression algorithm are shown in Table 4.

Table 4: Simulation results with two target images.



We now briefly comment these results. These observations, taken together, provide strong support that our method has good performances in terms of compression and encryption. To validate our approach, we use the sequence video containing images of a tank moving at a constant speed (see supplemental material T-15seco.avi for details: see ref. [32], and Fig. 22. This video sequence shows the target images (Fig. 22(a)), the multiplexed spectrum (Fig. 22(b)), the two-level encrypted spectrum (Fig. 22(c)), and the reconstructed images (Fig. 22(d)).

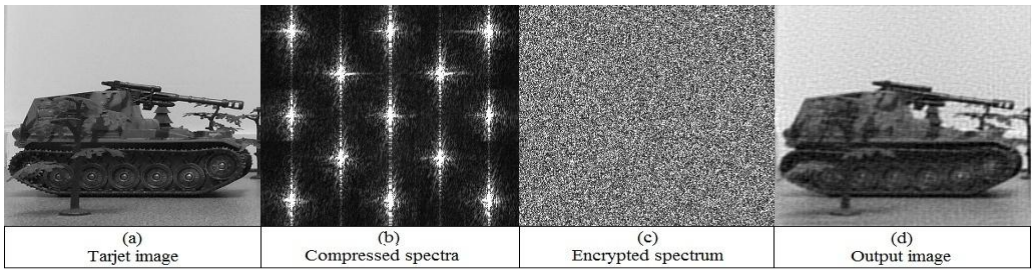


Fig. 22: Compression and encryption results with tank video: Example (See d_15sec.avi [32] for details).

9.3 *Compression and encryption of polarimetric images*

We now discuss the analysis of polarimetric images by our method. Figure 23(a) illustrates the optical setup described in detail in [27]. The light from a He-Ne (632 nm) laser source passes through a rotating diffuser, a spatial filter composed of a convergent lens and a pinhole, and the collimating lens L_3. Two polarizers (Pol) and two quarterwave plates (QWP) are used to select and analyze polarization states. The light is detected on a CCD camera thanks to the lens L_4. The sample (Fig. 23(b)) used in this study is a Smiley (cork) nearby plastic (top right) and lead (bottom right) spheres. Our experiments were performed in air. Four images can be obtained depending on the generated (linear or circular) and analyzed (crossed or parallel) polarized states [31]. These four images were encrypted and compressed, and then reconstructed after transmission. Finally, the DOPL (degree of linear polarization) and DOPC (degree of circular polarization) images were calculated [31].

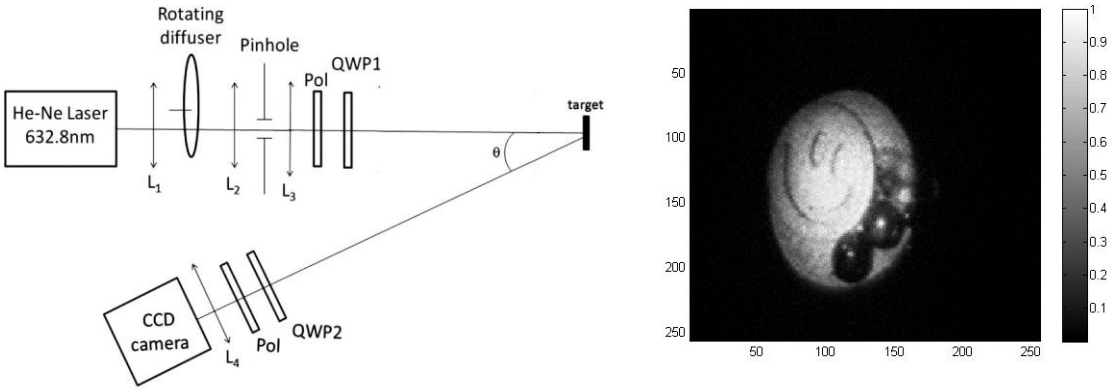


Fig. 23: (a) Scheme of the experimental setup for obtaining polarimetric images ($\theta = 10°$). POL: polarizer; QWP: quarterwave plate; L: lens; (b) The sample considered (see text).

Figure 24(a) shows the four images : (a-1) obtained with circularly polarized light and crossed polarizers, (a-2) obtained with circularly polarized light and parallel polarizers, (a-3) obtained with linearly polarized light and crossed polarizers, and (a-4) obtained with linearly polarized light and parallel polarizers. Figure 24 (b) shows the image after compression and encryption following our approach. In Fig. 24 (c), we show the reconstructed images and their corresponding MSE values : (c-1) obtained with circularly polarized light and crossed polarizers, (c-2) obtained with circularly polarized light and parallel polarizers, (c-3) obtained with linearly polarized light and crossed polarizers, and (c-4) obtained with linearly polarized light and parallel polarizers. These images show the good performances of our method since the MSE values are very small. The DOP images are shown in Fig. 24(d). The good quality of the DOP is also remarkable, i.e. the low- and high-frequency spectral information are preserved although the four images closely resemble.

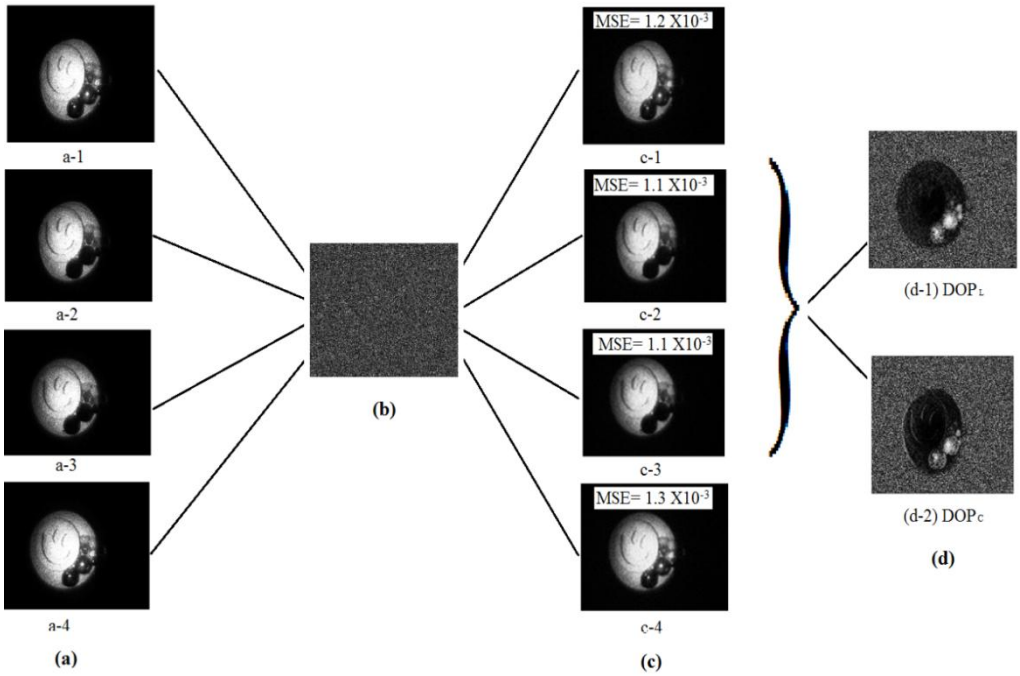


Fig. 24: Experimental results of simultaneous compression and encryption of polarimetric images.

10. Summary and conclusions

We have introduced a new and versatile method to compress and encrypt closely resembling images. The novelty of this scheme is that not only both operations are realized simultaneously but also it enables to deals with video sequences and polarimetric images. Our technique overcomes the bottleneck associated with fusion information in the Fourier plane. It relies on an optimization of the spatial-frequency spectrum of the image using a specific segmentation criterion. That is an energy criterion allowing us to merge several image spectra into one spectrum which contains pertinent information required for reconstructing the target images. This

procedure allows us to include all pertinent information required for reconstructing the multiple images in a spectrum of size $N \times N$ pixels. The optimization of the MIOCE method requires realizing three operations: (1) a shifting, (2) a segmentation (i.e. assignment of a specific spectral area to a target spectrum), and (3) a filtering. As mentioned above, this method allows us to increase significantly the number of images to be merged in the specrum of size $N \times N$ pixels. In practice, this permits to reduce significantly the amount of information to send or to store. In addition, we presented a robust encryption scheme to overcome the constraint of the double random phase-amplitude optical encryption method.The performance of this multiple-image optical compression and encryption method is verified by analyzing several video sequences and polarimetric images.

Direct testing with numerical simulations and experiments shows the efficiency of this simultaneous compression and encryption method of closely resembling images. This work might be extended in several directions, including (a) the experimental implementation of this numerical scheme, (b) the extension to noisy situations will be considered in future work, and (c) the investigation of the protocol's immunity to attacks.

Acknowledgment:

This work is partly supported by the Royal Saudi Navy-RSNF, Ministry of Defense.

#212407 – Received 22 May 2014; revised 6 Aug 2014; accepted 7 Aug; published 8 Sep 2014
 │Vol. 22, No. 19│DOI:10.1364/OE.22.022349│POTICS EXPRESS 22368

Simultaneous compression and encryption of polarimetric images

M. Aldossari,[1] A. Alfalou,[1*] and C. Brosseau[2]

[1]*Equipe Vision, L@BISEN, ISEN-Brest, 20 rue Cuirassé Bretagne CS 42807, 29228 Brest Cedex 2, France*
[2]*Lab-STICC, Université de Brest, CS 93837, 6 avenue Le Gorgeu, 29238 Brest Cedex 3, France*
**Corresponding author: ayman.al-falou@isen.fr*

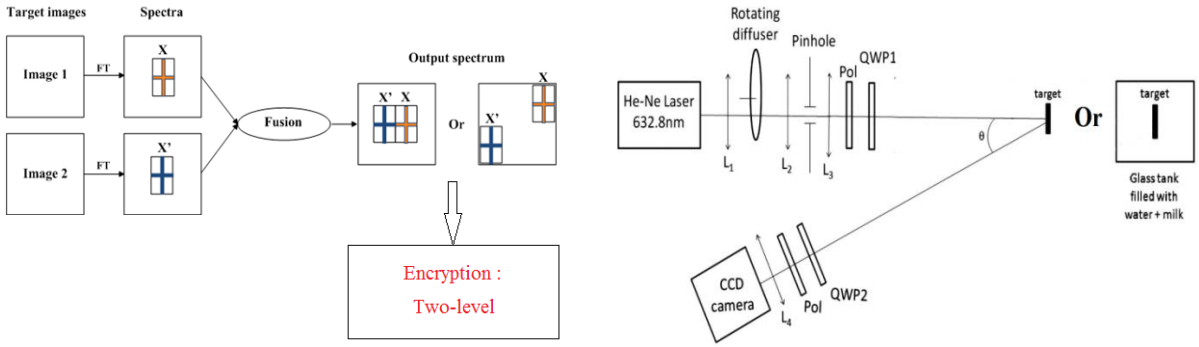
Abstract: A series of experiments is performed to test a scheme of simultaneoues compression and encryption of polarimetric images. The ability to discriminate between objects embedded in scattering media makes this scheme suited to applications of underwater mine detection.
OCIS codes: 100.5010, 100.2000, 100.3008, 110.5405

1. Motivation and context

The ability to remotely detect the presence of an object, and its scattering properties, embedded in a host matrix has been a long-standing goal in optics with applications in underwater mine detection and video imaging. Taking images of such object is complicated by the multiple scattering (and eventually absorption) phenomenon. In the most extreme case, this leads to the inability of detection of the object. Proposals for detecting underwater objects using optical methods have been suggested, but they are often limited by the trade-off between real-time information processing and signal loss due to backscattering and absorption. Here, we present a scheme to detect a target object in a scattering medium by polarimetric techniques. At its heart is the simultaneous compression and encryption of images described in the next paragraph.

2. Simultaneous compression and encryption of images

Figure 1(a) illustrates this compression and encryption scheme. Its basic principle consists in merging the spectra of target images in the Fourier plane. Our technique overcomes the bottleneck associated with fusion information in the Fourier plane. It relies on an optimization of the spatial-frequency spectrum of the image using a specific segmentation criterion. That is an energy criterion allowing us to merge several image spectra into one spectrum which contains pertinent information required for reconstructing the target images [1]. This spectral fusion represents a first level of encryption. A second level of encryption is used to render this protocol immune to attacks.



(a) (b)

Fig.1: (a) Synoptic diagram of the simultaneous compression and encryption method, (b) Experimental setup ($\theta = 10°$) for obtaining polarimetric images [2].

3. Compression and encryption of polarimetric images

The polarization optics setup is illustrated in Fig. 1(b). It consists of a laser He-Ne 632 nm source, a rotating diffuser, spatial filter composed of convergent lens and a pinhole, followed by a collimating lens L_3. Two polarizers (Pol) and two quarterwave plates (QWP) are used. The sample used in this study is a Smiley (cork) nearby plastic (top right) and lead (bottom right) spheres. The experiments were performed when the sample is either positioned in air or placed in a tank filled with water or milk (strongly diffusing medium). A CCD camera collects the polarimetric images. Four kinds of images are considered in this work (with reference to Fig. 2), i.e. (a-1) obtained with circularly polarized light and crossed polarizers, (a-2) obtained with circularly polarized light and parallel polarizers, (a-3) obtained with linearly polarized light and crossed polarizers, and (a-4) obtained with linearly polarized light and parallel polarizers. Next, our method of simultaneous compression and encryption was applied to obtain the compressed and encrypted spectral plane, i.e. (b). We first consider the case of air. The decompressed and decrypted polarimetric images are shown in Fig. 2(c). These images show the good performances of our method since the mean square error (MSE) which characterizes the differences between the target and reconstructed images are very small. The degree of linear DOPL and circular DOPC polarization [2] were also estimated from these images (Fig. 2(d)). We now turn to the case when the sample is placed in water or in milk. Table 1 shows the polarimetric images obtained after après decryption and de compression, and the corresponding DOPL and DOPC. The DOPC is more strongly affected by multiple scattering of waves in milk as expected [3]. Further, we observe that the DOPL and DOPC metrics allows us to discriminate between the types of materials of the sample and the embedding matrix. As shown in Fig. 2 and Table 1, good reconstructed image quality can be achieved, i.e. low- and high-frequency spectral information is preserved. The good quality of the DOP is also remarkable.

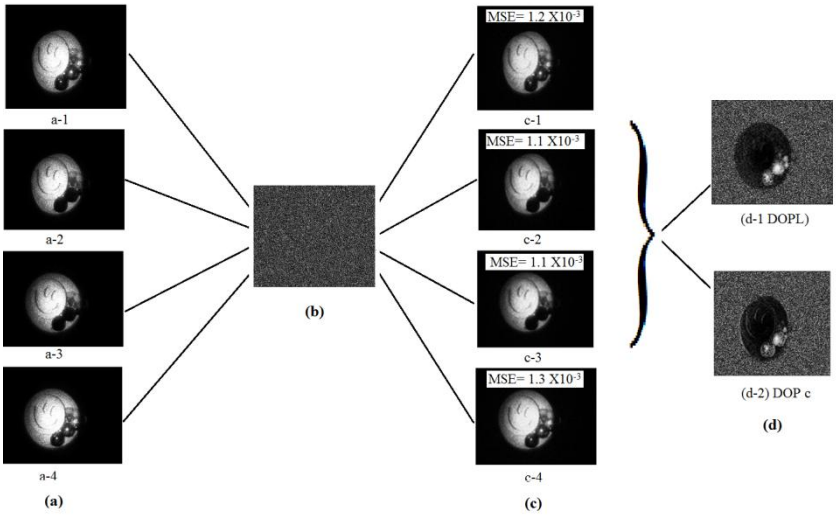


Fig. 2: Experimental results obtained in air.

Polarimetric images in water	Circular crossed	Circular parallel	Linear crossed	Linear parallel
MSE	5.34×10^{-4}	4.15×10^{-4}	3.52×10^{-4}	6.75×10^{-4}
Polarimetric images in milk	Circular crossed	Circular parallel	Linear crossed	Linear parallel
MSE	1.96×10^{-4}	1.83×10^{-4}	3.12×10^{-4}	1.92×10^{-4}
DOPL (water)		DOPL (milk)		
DOPC (water)		DOPC (milk)		

Table 1: Reconstructed images of the sample, when it is placed in water or milk, after compression and encryption.

4. Conclusion

The success of our spectral fusion methodology is validated by analyzing several polarimetric images which demonstrate that good reconstructed image quality can be achieved. Such a property is crucial for underwater mine detection by imaging polarimetry techniques.

5. References

[1] A. Alfalou and C. Brosseau, "Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption," Opt. Lett. **35**, 1914-1916 (2010).
[2] M. Dubreuil, P. Delrot, I. Leonard, A. Alfalou, C. Brosseau, and A. Dogariu, "Exploring underwater target detection by imaging polarimetry and correlation techniques," Appl. Opt. **52**, 997-1005 (2013).
[3] C. Brosseau, *Fundamentals of Polarized Light: A Statistical Optics Approach* (Wiley, New York, 1998).

A new optical simultaneously compression and encryption method of images

Abstract

The main objective of my PhD thesis is to propose and validate the principle of a new optimized simultaneously optical compression and encryptions method of multiple images (pictures or coming from a video sequence). Indeed, most compression and encryption methods are optimized in a separate manner and used in cascade. However, both are related and influence each other. This leads to decrease the quality of reconstructed images and to increase their implementation complexity. To overcome these problems, we propose to perform these two operations (i.e. compression and encryption) together in a dependent manner. In addition, we propose different optimizations of compression and plan to increase the encryption level of our system while keeping a good compression ratio. For that, we used a specific segmentation technique specially adapted to the Fourier domain in order to merge together several target images and to create several encryption keys. Those keys (amplitude and/or phase) are used in the image plane and in the Fourier plane. To decrypt the transmitted information, it is necessary to have both encryptions keys and the used spectral segmentation technique.

Keywords: Correlation, optical Fourier transform, compression, encryption, optical filtering, spectral segmentation, random phase.

Introduction:

The development of secure transmission systems becomes the priority of many research and engineering institutions. In fact, extensive studies have been carried out to apply coherent optics methods for real-time communication and image transmission. This is especially true when a large amount of information needs to be processed, e.g. high-resolution imaging. Because of its optical nature its conversion into a digital form is necessary in order to transmit, store, compress, and/or encrypt it. It is fair to say that it requires an important computing time, or eventually an image quality reduction. Thus, to compress optically an image can be a good solution. One key advantage of optics compared to digital methods lies in its capability to provide massively parallel operations in a two-dimensional space. Approaches which consist in processing the data closer to the sensors to pick out the useful information before storage or transmission is a topic that has generated great interest from both academic and practical perspectives. Compression and encryption operations are often carried out separately, although they are strongly related and influence each other. There is small number of studies proposing de do this two operations simultaneously.

In this thesis we present several optimizations for the new method dealing with simultaneously compression and encryption of images. My manuscript is divided into four chapters. The first chapter presents the context and objective of the thesis. The second one explores the state-of-the-art of coherent optical compression and encryption methods. In addition, we present in this chapter some simulations results of the very important methods in the literature.

The third chapter presents the development of our new method in both operations (compression & encryption) and we propose different optimizations and criterions to select the related information of each target image and increase the compression ratio. This allows us to multiplexing several targets images together and forming one with the same size (compression). Then we introduce our encryption approach to secure the information in the compressed spectrum. This will be related to the different areas of spectral plane. Then we use several specific random phase keys.

The fourth chapter deals with compression using the symmetry in Fourier plan to increase the number of target images to be merge together. We also propose an adaptation of our method to video sequences. The last section of this chapter is dedicated to a perspective application using polarimetric images.

Chapter 1

We start this chapter by explain the context and objectives of our study. First of all, we introduce the information processing by optical filtering. In this section we develop the Fourier optics and its optical implementation, Vander-lugt and JTC correlator. We gave the basic notions of mathematics to perform a FT then explain the principe of the all-optical 4f setup which is the basic concept of optical filtering. This setup helps us to work in the Fourier domain and reorganize it to make a compression or encryption. After that we study the correlation technique which consists in multiplying the target image in the Fourier plane with a correlation filter to get a peak of correlation in the output plane. In fact the correlation peak allows us to filtering the Fourier plane in order to select the pertinent pixel and compress or encrypt the target images spectrum in the output plane.

We also present the simulation result of some correlation filters (Matched, POF, BPOF, composed and segmented filters). In fact we use this filters to extract the relevant information to recognize an object in a complex scene. The segmented filter allows the multiplexing of several target images which leads to make an information compression.

In last section of this chapter we detailed the spatial light mutilator (SLM). The new SLM is the very important optoelectronic device in the last two decades. Because it allows to modulate light by the transmittance of an image. We present the several type of SLM like EASLM and OASLM. At the end of this chapter we gave a conclusion.

Chapter 2

The first section of this chapter is devoted to the state-of-the-art of all-optical compression and encryption methods. We start by a presentation of the interest and types of optical image compression and justified our optical choice. Then we study and analyze the most important methods like those presented in reference 1&2. The authors suggest a new technique for optical image compression, based on image phase spectrum properties. It consists on an algebraic multiplication of the image spectrum with some particular segmented amplitude mask (SAM) in the Fourier domain. The ref 2 proposes a new spectral segmentation of the Fourier plane to reduce quantity of information. Their technique gave a good quality of reconstructed image.

In the ref 3 authors present a technique based on (Phase-shifting Interferometry Digital Holography Compression). This method has the advantage of increased

reconstruction quality but in practical digital holography is limited to static scenes.

In method ref 4 authors presented the results of applying lossless and lossy data compression to a 3D object reconstruction and recognition technique. They suggest a digital hologram compression technique based on Fourier-domain processing. The main problem of this method is the large size of hologram for real-time applications

We present in the ref 5 the method based on a fall optical implementation using the JPEG compression. In fact JPEG compression relies on the DCT. The numerical simulation of this technique gave good performances. However, these authors proposed only a partial optical implementation of their technique.

In the second section of this chapter we present the fundamental and a historical introduction of the cryptography. Then we explore and discuses optical compression and encryption methods. The first method was Double Random Phase DRP proposed by Refregier, & Javidi (ref 6). Their technique consists in encrypting an image displayed in the input plane of the 4f setup. To encode image, they change both amplitude and phase information, because it is possible to reconstruct the image by using only the amplitude or phase spectral information. In their technique they use two random phase mask one in the input plane and another in the Fourier domain which leads to a good level of encryption. However, the DRP encryption system presents some weakness against attacks because a hacker can access random phase keys in both the input plane and the Fourier plane. We also discuss ref 7 in this article Alfalou and co-workers suggested a new method to carry out compression and encryption simultaneously suing the DCT. It consists to demonstrate the possibility of multiplexing spectral information and realizing DCT optically. The important property of DCT is to group relevant information of an image in the left-hand corner of its spectrum. The compression is obtained after filtering the spectrum and multiplexing of several spectra. For the encryption, they multiply the compressed spectrum by a random mask.

Chapter 3

In this chapter we propose and validate our new method of compression end encryption simultaneously of images (static or video sequences). Our approach uses several optimizations to do the compression. The first one consists to use the root-mean-square (RMS) criterion to determine the minimal size of each target spectrum then we shift these spectra to minimize their overlapping. Next, we apply a spectral fusion to multiplex the information coming from each spectrum of the target images. This fusion is based on a specific spectral segmentation which has for aim to optimize the band-pass RMS of the Fourier plane. These optimizations provide us a high level of compression ratio with a very good quality of reconstructed images. (For more details see publication conf-2)

In the second section of this chapter, we propose and validate an approach of encryption to secure the merged and compressed spectrum issuing of the compression process. It consists to change the spectral distribution in Fourier domain and fabricate an encryption mask (amplitude and phase). This mask is obtained from tree optimized sup-mask on function three frequencies (high, intermediate, and low). The simulation results show that we succeeded to hide the information in the target spectrum. (see publication Art 1)

Chapter 4

We propose in this chapter to optimize our method in both techniques compression and encryption. The first optimization is using the property of the symmetry in the Fourier domain to eliminate half of the spectrum plane this will double the target images to be merged. An adaptation our method to video images is presented in the section. We also calculate the MSE of the reconstructed images to qualified their quality and performance of the method. Simulations and MSE values show the good performance of our technique.

The second section of chapter deals with a second encryption level. In fact, we think that to completely secure the transmitted spectrum we must perform second encryption key. For that we use a double random phase system (DRP) to improve the security of our method. To do that we multiply the spectrum obtained of the first encryption level by a random phase key. After a FT we obtain the encryption image that is multiplied by the second encryption random phase key. Finally, after second FT we obtain the two-level encrypted image in the output plane. We test our optimized method with different type of images

(man & tank moving). It has good performance in terms of compression and encryption.
(see supplemental material https://www.youtube.com/watch?v=5CS1rNLyALs it shows the target images, the multiplexed and compressed spectrum, the tow-level encrypted spectrum and the reconstructed images)

In the last section of chapter, we test and discuss our method with polarimetric images. We get these images from our lab setup. Tests of DOP linear and DOP circular polarized images in different environment (air, water and milk) were performed. The decompressed and decrypted polarimetric images are shown. These images show the good performances of our method since the mean square error (MSE) which characterizes the differences between the target and reconstructed images are very small. (see publication Conf 3)

Conclusion

We have proposed in this thesis a new and versatile method to compress and encrypt closely resembling images. The novelty of this method is that not only both operations are realized simultaneously but also it enables to deals with video sequences and polarimetric images. Our technique overcomes the bottleneck associated with fusion information in the Fourier plane. It relies on an optimization of the spatial-frequency spectrum of the image using a specific segmentation criterion. That is an energy criterion allowing us to merge several image spectra into one spectrum which contains pertinent information required for reconstructing the target images. This procedure allows us to include all pertinent information required for reconstructing the multiple images in a spectrum. In addition, we presented a robust encryption scheme to overcome the constraint of the double random phase-amplitude optical encryption method. The performance of this multiple-image optical compression and encryption method is verified by analyzing several video sequences and polarimetric images.

References

1- Boumezzough A., AlFalou A., Collet C., « Optical image compression based on filtering of the redundant information in Fourier domain with a segmented amplitude mask (SAM) **».** CSIMT -IEEE-See, Complex Systems, Intelligence and Modern Technological applications (CSIMTA 04), pp. (566-570), Cherbourg-FRANCE, 19-22 September 2004.

2- Soualmi S., Alfalou A. and Hamam H., « Optical image compression based on segmentation of the Fourier plane: new approaches and critical analysis **»** J. Opt. A: Pure Appl. Opt., Vol. **9, pp.** 73-80, 2007.

3- Darakis E., Soraghan J.J., « Reconstruction domain compression of phase-shifting digital holograms **».** Applied Optics, Vol. **46** Issue 3, pp.351-356, 2007.

4- Naughton T. J., Frauel Y., Javidi J., and Tajahuerce E., « Compression of digital holograms for three-dimensional object reconstruction and recognition**».** APPLIED OPTICS, Vol. **41**, No. 20, pp.4124-4131, 2002.

5- Alkholidi A., Alfalou A., and Hamam H, "A new approach for optical colored image compression using the JPEG standards". Signal Process. Vol. 87, pp. 569-583, 2007.

6- P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767 (1995).

7- A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, "Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks," Opt. Express **21**, 8025-8043 (2013)

Bibliographie

Bibliographie

[1] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon. **1**, 589-636 (2009). http://dx.doi.org/10.1364/AOP.1.000589

[2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767 (1995).

[3] Q. Wang, Q. Guo, L. Lei, "Asymmetric multiple-image hiding using phase retrieval technique based on amplitude- and phase-truncation in fractional Fourier domain," Optik, In Press (2013).

[4] Z Liu, L Xu, T Liu, H Chen, P Li, C Lin, S Liu, "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," Opt. Commun., 284, 123 (2011).

[5] Z. Liu, Y. Zhang, S. Li, W. Liu, W. Liu, Y. Wang, S. Liu, "Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains," Optics & Laser Technology **47**, 152 (2013).

[6] S. K. Rajput and N. K. Nishchal, "Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform," Appl. Opt. **52**, 871 (2013).

[7] Q. Wang "Optical image encryption with silhouette removal based on interference and phase blend processing," Opt. Comm. **285**, 4294 (2012).

[8] A. Alfalou and C. Brosseau, "Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption," Opt. Lett. **35**, 1914-1916 (2010).

[9] Alfalou, A. Mansour, M. Elbouz, C. Brosseau, "Optical compression scheme to multiplex & simultaneously encode images", in Optical and Digital Image Processing Fundamentals and Applications, (Wiley, New York, 2011), pp.463-483.

[10] A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, "Simultaneous fusion, compression, and encryption of multiple images" Opt. Express **19**, Issue 24, 24023-24029 (2011).

[11] A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, "Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks," Opt. Express **21**, 8025-8043 (2013).

[12] J.W. Goodman,"Introduction to Fourier Optics (2nd ed.)," New York: McGraw-Hill *(1966)*.

[13] M. Paturzo, P. Memmolo, L. Miccio, A. Finizio, P. Ferraro, A. Tulino, and B. Javidi, "Numerical multiplexing and demultiplexing of digital holographic information for remote reconstruction in amplitude and phase," Opt. Lett. 33, 2629 (2008).

[14] T. J. Naughton, Y. Frauel, B. Javidi, and E. Tajahuerce, "Compression of interference digital holograms for three dimensional object reconstruction and recognition," Appl. Opt., **41,** 4124 (2002).

[15] E. Darakis and J. J. Soraghan, "Reconstruction domain compression of phase-shifting digital holograms," Appl. Opt. **46**, 351 (2007).

[16] T. Tahara, K. Ito, T. Kakue, M. Fujii, Y. Shimozato, Y. Awatsuji, K. Nishio, S. Ura, T. Kubota, and O. Matoba, "Parallel phase-shifting digital holographic microscopy," Biomed. Opt. Express **1**, 610 (2010).

[17] P. Xia, Y. Shimozato, T. Tahara, T. Kakue, Y. Awatsuji, K. Nishio, S. Ura, T. Kubota and O. Matoba, "Image reconstruction algorithm for recovering high-frequency information in parallel phase-shifting digital holography," Appl. Opt. **52**, A210 (2013).

[18] A. B. VanderLugt, "*Signal detection by spatial filtering*," IEEE Trans. inf. Theory **IT-10** (1964).

[19] A. Glavieux et M. Joindot, "Communication numériques" Masson, 1996.

[20] A. Alfalou, "Implantation optique de corrélateurs multivoies temps-réel," Thèse de doctorat, Université de Rennes I, 1999.
[21] A. Alfalou and C. Brosseau, *face Recognition.* In-Tech 2010 ch "Understanding Correlation Techniques for Face Recognition: From Basics to Applications," pp. 353-380.
[22] J. L. Honer, "Metrics for assessing pattern-recognition performance," Applied. Optics, vol. 31,n. 2, pp. 165-166,1992.
[23] C.S. Weaver et J. W. Goodman , "A Technique for Optically Convolving two Function," *Applied Optics*, vol. 5, pp. 1248-1249, 1966.
[24] A. Alfalou, G. Keryer et J. L. de Bougrenet de la Tocnaye, "Optical Implementation of Segmented Composite Filtering," *Applied Optics*, vol. 38 pp. 4773-4801, 1999.
[25] J. E. Rau, "Detection of Differences in Real Distributions," OSA, vol.56, pp.1450-1494, 1966.
[26] J. Horner et P. Gianino, "Phase-Only Matched Filtering," *Applied Optics*, vol.23, pp.812-816, 1984.
[27] J. Horner, B. Javidi, et J. Wang, "Analysis of the Binary Phase-Only Filter," Optics Communication, vol. 91,pp. 189-192, 1992.
[28] J. L. de Bougrenet de la Tocnaye, E. Quémener et Y. Pétillot, "Composite Versus Multi-channel Binary Phase-Only Filtering," *Applied Optics*, vol. 36, 1997.
[29] B. V. K. V. Kumar, "Tutorial Survey of Composite Filter Designs for Optical Correlators," *Applied Optics*, vol. 31, 1992.
[30] O.Lehman. "Über fliessende krystalle,". Z. physical. Chem., 4:462, 1889.
[31] Cours du professeur Georges BOUDEBS- Université d'Anger.OPI. http://www.optique-ingenieur.org/fr/cours/OPI_fr_M02_C02/co/Contenu_02.html
[32] M. Elbouz, A. Alfalou, C. Brosseau, M. S. Alam and S. Qasmi "A three-level correlation technique for face recognition and color change detection" *Optics Communications **311**, 186-200 - 2013.*
[33] A. Alfalou, C. Brosseau, M. S. Alam, "Smart pattern recognition, " Proc. SPIE 8748, Optical Pattern Recognition XXIV, 874809 (April 29, 2013). doi:10.1117/12.2018249. http://dx.doi.org/10.1117/12.2018249
[34] A. Alfalou, C. Brosseau, "Implementing compression and encryption of phase-shifting digital holograms for three-dimensional object reconstruction" optics comm. **307,** 67-72 (*2013*).
[35] Boumezzough A., AlFalou A., Collet C., « Optical image compression based on filtering of the redundant information in Fourier domain with a segmented amplitude mask (SAM) ». CSIMT - IEEE-See, Complex Systems, Intelligence and Modern Technological applications (CSIMTA 04), pp. (566-570), Cherbourg-FRANCE, 19-22 September 2004.
[36] Soualmi S., Alfalou A. and Hamam H., « Optical image compression based on segmentation of the Fourier plane: new approaches and critical analysis » J. Opt. A: Pure Appl. Opt., Vol. 9, pp. 73-80, 2007.
[37] Cottour A., Alfalou A., Hamam H., « Optical video image compression: a multiplexing method based on the spectral fusion of information ».Proc. IEEE, ICTTA 2008, pp. 1-6, April 2008.
[38] Darakis E., Soraghan J.J., « Reconstruction domain compression of phase-shifting digital holograms ». Applied Optics, Vol. 46 Issue 3, pp.351-356, 2007.
[39] Yamaguchi I. and Zhang T., « Phase-shifting digital holography ». Optics. Letters, Vol. 22, pp. 1268-1270, 1997.
[40] Shortt A. E., Naughton T. J., and Javidi B., « Nonuniform quantization compression techniques for digital holograms of three dimensional objects ». In *Optical Information Systems II*, B. Javidi and D. Psaltis, eds., Proc. SPIE Vol. 5557**,** 30–41, 2004.

[41] Naughton T. J., Frauel Y., Javidi J., and Tajahuerce E., « Compression of digital holograms for three-dimensional object reconstruction and recognition ». APPLIED OPTICS, Vol. 41, No. 20, pp.4124-4131, 2002.
[42] B. Javidi and E. Tajahuerce, "Three-dimensional object recognition by use of digital holography," Optis. Letters, Vol. **25,** 610–612, 2000.
[43] Y. Frauel, E. Tajahuerce, M.-A. Castro, and B. Javidi, "Distortion-tolerant three-dimensional object recognition with digital holography," Applied. Optics, Vol. 40, pp. 3887–3893, 2001.
[44] D. A. Huffman, "A method for the construction of minimum redundancy codes," Proc. IRE 40, pp. 1098–1101, 1952.
[45] J. Ziv and A. Lempel, "A universal algorithm for sequential data compression.". IEEE Transaction, IT-23, pp. 337–343, 1977.
[46] T. A. Welch, "A technique for high performance data compression". IEEE Computer, Vol. 17, pp**.** 8–19, 1984.
[47] M. Burrows and D. J. Wheeler, "A block-sorting lossless data compression algorithm," Digital SRC Report 124, 1994.
[48] W. B. Pennebaker and J. L. Mitchell, "JPEG: Still Image Data Compression Standard*"*, Van Nostrand Reinhold, 1993.
[49] Alkholidi A., Alfalou A., and Hamam H, "A new approach for optical colored image compression using the JPEG standards". Signal Process. Vol. 87, pp. 569-583, 2007.
[50] A. AlFalou, A. Alkholidi, "Implementation of an all-optical image compression architecture based on Fourier transform which will be the core principle in the realisation of DCT". SPIE, Opto-Ireland 2005, vol. 5823, pp. 183-190, 2005.
[51] S. Singh"The code book: The Secret History of codes and code-breaking". Fourth Estate, New Ed , 2000.
[52] D. Kahn "The code-breaking: The Comprehensive History of Secret Communication from Ancient Times to the Internet". New York, Simon & Schuster; 2nd revised edition, 1997.
[53] W. Diffie, M. E. Hellman "New directions in cryptography". IEEE Transaction on Information Theory, Vol.22, pages 644-654, 1976.
[54] Encyclopedie Hachette.
[55] Le Quid.
[56] Encyclopedie Larousse.
[57] La Cryptologie, édition P.U.F (III).
[58] P. Refregier and B. Javidi "Optical image encryption based on input plane and Fourier plane random encoding". Opt. Lett. **20**(7), 767-769(1995).
[59] Y. Frauel, A Castro, T. J. Naughton and B. Javidi "Resistance of the double random phase encryption against various attaks,". Opt. Express. **15**, 10253-10265(2007).
[60] J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognimi "Multiple-encoding retrieval for optical security". Opt. Commun. **276**, 231-236(2007).
[61] M. Nazrul Islam and M. S. Alam "Optical security system employing shifted phase-encoded joint transform correlation,". Opt. Commun. **281**, 248-254(2008).
[62] O. Matoba, T.J Naughton, Y. Frauel, N. Bertaux, and J. Bahram "Real-time three-dimensional object reconstruction by use of a phase-encoded digital hologram,". Appl. Opt.**41**, 6187-6192 (2002).
[63] Z. Xin, Y. S. Wei, and X. Jian,"Affine cryptosystem of double-random phase encryption on the fractional Fourier transform,". Appl. Opt.**45**, 8434-8439 (2006).
[64] Z. Liu, and S. Liu, "Double image encryption based on iterative fractional Fourier transform,". Opt. Commun. **275**, 324-329 (2007).

[65] A. Alfalou and A. Mansour “New Image Encryption Method Based on ICA,”. In Proceedings of the 10th IAPR Conference on Machine Vision Application, J. Tajima, ed. (International Association for Pattern Recognition, 2007), pp. 16-18.

[66] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon. **1**, 589-636 (2009).

[67] A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, "Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks," Opt. Express **21**, 8025-8043 (2013)

[68] A. Boumezzough, "Vers un processeur optoélectronique holographique de cryptage des données à haut débit pour les télécommunications," Université Louis Pasteur- Strasbourg 1- Isen-Brest, 2005.

[69] L. Chen and D. Zhao, "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms," Opt. Express **14**, 8552-8560 (2006).

[70] M. Joshia, Chandrashakherb, and K. Singh, "Color image encryption and decryption using fractional Fourier transform," Opt. Commun. **279**, 34-42 (2007).

[71] D. Amaya, M. Tebaldi, R. Torroba and N. Bolognini, "Digital color encryption using a multi-wavelength approach and joint transform correlator," J. Opt. A Pure Appl. Opt. **10**, 104031-104035 (2008).

[72] G. Keryer, J. L. de Bougrenet de la Tocnaye, and A. Alfalou, "Performance comparison of ferroelectric liquid-crystal-technology-based coherent optical multichannel correlators," Appl. Opt. **36**, 3043-3055 (1997).

[73] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attaks," Opt. Express **15**, 10253-10265 (2007).

[74] C. S Weaver and J. W. Goodman, , "A technique for optically convolving two functions," Appl. Opt. **5**, 1248-1249 (1966).

[75] Bahram Javidi and Chung-Jung Kuo, "Joint transform image correlation using a binary spatial light modulator at the Fourier plane," Appl. Opt. **27**, 663-665 (1988).

[76] M. R. Haider, M. Nazrul Islam, M. S. Alam, and J. F. Khan, , "Shifted phase-encoded fringe-adjusted joint transorm correlation for multiple target detection," Opt. Commun. **248**, 69-88 (2005).

[77] A. Mansour and Kawamoto, "ICA papers classified according to their applications and performances," IEICE Trans. Fundamentals **E86-A**, 620-633 (2003).

[78] Pascal PLUME, "Compression de données," Edition Eyrolles (1993).

[79] M. Adossari, A. Alfalou and C. Brosseau, "Image Quality Assessment Based on a Multiple Image Optical Compression and Encryption," in *Frontiers in Optics 2011/Laser Science XXVII*, OSA Technical Digest (Optical Society of America, 2011), paper FThY4.

[80] M. Aldossari, A. Alfalou and C. Brosseau, "Optimized fusion method based on adaptation of the RMS time-frequency criterion for simultaneous compression and encryption of multiple images ", *Proc. SPIE* 8748, Optical Pattern Recognition XXIV, 87480B (April 29, 2013).

[81] G. Gilbert, and J. Pernicka, "Improvement of underwater visibility by reduction of backscatter with a circular polarization technique ", Applied Optics, vol.6, pp. 741-746, 1967.

[82] G. Lewis, D. Jordan and P. Roberts, "Backscattering target detection in a turbid medium by polarization discrimination", Applied Optics, vol. 38, pp. 3937-3944, 1999.

[83] M. Dubreuil, P. Delrot, I. Leonard, A. Alfalou, C. Brosseau, and A. Dogariu, "Exploring underwater target detection by imaging polarimetry and correlation techniques," Appl. Opt. **52**, 997-1005 (2013).

[84] C. Brosseau, "Fundamentals of polarized light a statistical optics approach," J. Wiley and sons Editors, Wiley Interscience publication, 1998.