



HAL
open science

Optical image compression and encryption methods

Ayman Alfalou, C. Brosseau

► **To cite this version:**

Ayman Alfalou, C. Brosseau. Optical image compression and encryption methods. *Adv. Opt. Photon.*, 2009, 1, pp.589-636. hal-00516980

HAL Id: hal-00516980

<https://hal.science/hal-00516980>

Submitted on 13 Sep 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Optical image compression and encryption methods

A. Alfalou¹ and C. Brosseau^{1,*}

¹ISEN Brest, L@bISEN, 20 rue Cuirassé Bretagne CS 42807, 29228 Brest Cedex 2, France

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

*Corresponding author: brosseau@univ-brest.fr

Received March 30, 2009; revised September 26, 2009; accepted October 1, 2009; published October 28, 2009 (Doc. ID 109461)

Over the years extensive studies have been carried out to apply coherent optics methods in real-time communications and image transmission. This is especially true when a large amount of information needs to be processed, e.g., in high-resolution imaging. The recent progress in data-processing networks and communication systems has considerably increased the capacity of information exchange. However, the transmitted data can be intercepted by nonauthorized people. This explains why considerable effort is being devoted at the current time to data encryption and secure transmission. In addition, only a small part of the overall information is really useful for many applications. Consequently, applications can tolerate information compression that requires important processing when the transmission bit rate is taken into account. To enable efficient and secure information exchange, it is often necessary to reduce the amount of transmitted information. In this context, much work has been undertaken using the principle of coherent optics filtering for selecting relevant information and encrypting it. Compression and encryption operations are often carried out separately, although they are strongly related and can influence each other. Optical processing methodologies, based on filtering, are described that are applicable to transmission and/or data storage. Finally, the advantages and limitations of a set of optical compression and encryption methods are discussed.

© 2009 Optical Society of America

OCIS codes: 070.0070, 090.0090, 100.0100, 200.3050, 200.4560.

1. Introduction	591
2. Optical Image Compression Methods.	595
2.1. Phase-Shifting Interferometry Digital Holography Compression.	597
2.2. Compression Methods for Object Recognition.	598
2.3. Efficient Compression of Fresnel Fields for Internet Transmission of 3D Images.	602
2.4. Compression of Full-Color 3D Integral Images.	604
2.5. Optical Colored Image Compression Using the Discrete Cosine	

Transform.	607
2.6. Real-Time Optical 2D Wavelet Transform Based on the JPEG2000 Standard.	608
2.7. Fourier-Transform Method of Data Compression and Temporal Fringe Pattern Analysis.	609
2.8. Radon Transform and Fourier Transform for a Bandwidth-Compression Scheme.	610
2.9. Compression and Multiplexing: Information Fusion by Segmentation in the Spectral Plane.	611
3. Optical Image Encryption Methods.	614
3.1. Double Random Phase Encryption System.	614
3.2. Resistance of DRP against Attacks.	615
3.3. Multiple-Encoding Retrieval for Optical Security.	616
3.4. Image Encryption Approaches Based on Joint Transform Correlator System.	617
3.4a. Digital Color Encryption Using a Multiwavelength Approach and a Joint Transform Correlator.	617
3.4b. Optical Security System Employing Shifted Phase-Encoded Joint Transform Correlation.	619
3.5. Image Encryption Based on Fractional Fourier Transform.	620
3.6. All-Optical Video-Image Encryption with Enforced Security Level Using Independent Component Analysis.	621
4. Optical Image Compression and Encryption Methods.	624
5. Summary and Perspectives.	626
Appendix A: Acronyms.	627
Acknowledgments.	628
References.	628

Optical image compression and encryption methods

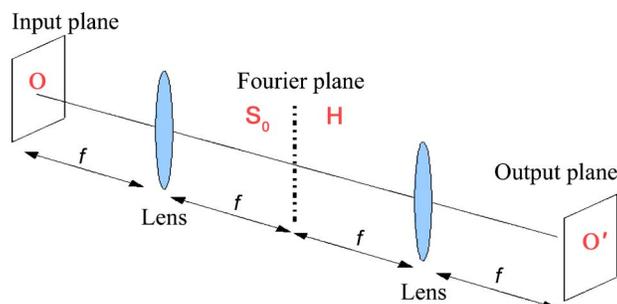
A. Alfalou and C. Brosseau

1. Introduction

Over the years intensive research has been directed toward coherent optics, especially the issues of compression and encoding, because of the potential for new technological applications in telecommunications. In this tutorial review we study optical information processing techniques (such as image spectral filtering and holography) in real time, in close relationship with their implementation on optical processors. This implementation is generally performed by using an optical setup called $4f$ [1,2]; see Fig. 1.

This $4f$ setup will be the basic concept on which most optical spectral filtering methods described in this tutorial are based. The inherent parallelism of optics provides an appropriate framework for information processing techniques. However, from a practical point of view, it is worth emphasizing that the latter is conditioned largely by the existence of powerful electro-optical interfaces. One of the main concerns of this review is to place the algorithmic developments side by side with the interfaces needed to implement them. This research area advances the frontiers of signal processing and pattern recognition. In this area, a

Figure 1



Principle of the all-optical filtering $4f$ setup. The $4f$ setup is an optical system composed of two convergent lenses. The 2D object O is illuminated by a monochromatic wave. A first lens performs the Fourier transform FT of the input object O in its image focal plane, S_0 . In this focal plane, a specific filter H is positioned. Next, a second convergent lens performs the inverse Fourier transform (FT^{-1}) in the output plane of the system to get the filtered image O' .

decision theory tool like *correlation* is based on the use of *classical matched filtering* and is optically implemented by the $4f$ optical setup [1–5] (see box).

Correlation technique: *This technique consists in multiplying the target image spectrum (spectrum of the image to be recognized) with a correlation filter (belonging to a learning (reference) base) and then performing a FT^{-1} (inverse Fourier transform). This results in a peak (located at the center of the output plane, i.e., the correlation plane) that is more or less sharp depending on the degree of similarity between the target and the reference images.*

Classical matched filter (H_{CMF}): *This filter is given by $H_{CMF}(u, v) = \alpha S_{R_i}^*(u, v) / N(u, v)$, where $S_{R_i}^*$ denotes the conjugate of the reference spectrum image, N is the spectral density of the background noise, and α is a constant. This filter is very robust, but presents a low discriminating power [1–5].*

Correlation is perceived as a filtering that aims to extract the relevant information in order to recognize a pattern in a complex scene. This led to the concept of the classical matched filter (carried out from a single reference) whose purpose is to decide whether a particular object is present in the scene. To obtain a reliable decision about the presence or absence of an object in a given scene, we must correlate the target object, using several correlation filters and taking into account the possible modifications of the target object. However, this approach requires a lot of correlation data and is difficult to realize in real time. Moreover, a simple decision based on whether a correlation peak is present (thresholding) is insufficient. Thus, the use of adequate performance criteria, such as those developed in [5,6], is necessary. The matched filter is appropriate to extract features from the scene. Postprocessing is required for merging these different features in order to make a reliable decision. If some knowledge about the pattern recognition is specified in the filter, less postprocessing is needed.

This perspective led to the concept of the *composite filter* [7–9], for which various reference images are integrated in a single filter (see box). This results from

Composite filter H_{COM} : *This filter allows us to merge multiple versions $H_{COM} = \sum_i \alpha_i R_i$ of a reference image R_i . This filter can be defined as a linear combination of different reference versions, where α_i represents coefficients to optimize a cost function defined for a specific application.*

an optimization of a performance criterion in relation to the trade-off between good detection and false alarm. This leads to the possibility of gathering the information relative to several reference images in only one filter, thus reducing the size of the database needed to obtain a better decision. An extension of the composite filter to a multichannel correlation filter, H_{Seg} , can be carried out by introducing a new *segmentation* concept in the Fourier plane [10,11].

Segmented filter H_{Seg} : *A segmented filter is an optimized version of the composite filter developed to overcome the saturation problem that is due to a combination of a large number of references. The filter H_{Seg} optimizes the use of the space-bandwidth product in the spectral plane filter.*

This new segmented filter allows the multiplexing of several types of shape that need to be recognized. A selection of the information present in the scene, in correspondence to one of these types, is carried out in the spectral plane. A partition criterion of the frequencies and an assignment of the different areas to the types allow an optimal identification of the form sought. Typically, this filter consists in gathering M classical matched filters ($N \times N$ pixels each) in only one spectral plane. To realize such filter, only the relevant information about the different filters in the Fourier plane of the segmented filter H_{Seg} can be considered according to a specific selection criterion; e.g., in [10] an energetic selection criterion was used to select the information needed. Then, the information (for different possible rotations of the object) was merged into a single filter, i.e., antirotation filter. This permits restriction of the knowledge about a filter to its main part ($N \times N/M$ pixels).

In a similar way, this filter allows us to introduce extra information and consequently hide other information, i.e., encoding authentication. Thus, it is possible to use this filtering concept to carry out compression and encoding of an image simultaneously. Compression consists in selecting relevant information in the image spectrum. Encryption is obtained by scrambling both the amplitude and the phase distribution of the spectrum. In point of fact, an object can be easily reconstructed from the amplitude or the phase of its Fourier transform (FT) [12,13]. As the phase information in the Fourier plane is of higher importance than the amplitude information [12], much research in optical compression and encryption has been directed toward the characterization of the phase.

Because of the optical nature of the image its conversion into a digital form is necessary in order to transmit, store, compress, and/or encrypt it. It is fair to say that this requires important computing time, or eventually image quality reduction. Thus, to compress and encrypt an image optically can be a good solution. One key advantage of optics compared with digital methods lies in its capability to provide massively parallel operations in a 2D space. Approaches that 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, as evidenced by the special *Applied Optics* issue on Specific Tasks Sensing [14]. As we explain in some detail, in fact these methods become more and more complex to implement optically, especially when we are interested in color images or video sequences, every time the rate of

image encryption increases. Carrying out a part of the processing digitally is a relevant solution to solve this complexity while maintaining a reasonable speed. One major difference between the work presented here and the literature already existing is that we are interested in optical filtering operations and the possibilities they offer for compression and encryption. More specifically, we pay special attention to compression and encryption methods that can be realized simultaneously.

In this tutorial we are interested in compression and encryption methods that can be implemented optically. These methods have progressed through the work of many research teams. Space allows us to mention only a sample from well-known groups, from which the interested reader may gain a sense of the scope and power of these new ideas. To achieve this goal, optoelectronic devices, i.e., *spatial light modulators* (SLMs), need to be used.

Spatial light modulator: *A SLM consists of an array of optical elements (pixels) for which each pixel acts independently, like an optical valve, to adjust or modulate the intensity or the phase of light.*

SLMs are used to modulate light (pixel by pixel) by the transmittance of an image, filter, etc. Pixel modulation is controlled electronically from digital data, by converting digital information from the electronic domain into coherent light, or optically. In the last, one needs a writing light beam containing the modulation information and a reading coherent light beam. Standard optically addressed modulators are not easy to design. Electrically addressed modulators generally have two significant drawbacks: unwanted diffraction light generated because of the pixel structure and low light utilization efficiency that is due to the small filling factor. The past decade has seen much progress in the resolution of these problems. The development of SLMs has retained the attention of many researchers for two reasons. On the one hand, they are increasingly being used in commercial devices, e.g., video projectors. On the other hand, they are used in specialized applications such as maskless lithography systems [15]. In the problem at hand, applications concern diffractive optical elements for holographic display [16,17], visio projection [18], adaptive optics [19], polarization imaging [20], image processing [21], correlation [22], and holographic data storage setup to encode information into a laser beam in the same fashion as a transparency does for an overhead projector. Many types of efficient and reliable SLM are available, with optical or electrical addressing, in transmission or reflection mode, electrically [23] or optically [24–26] addressed, in intensity or phase modulation mode, containing micromirrors or twisting mirrors (microelectromechanical systems or acousto-optics), or using liquid crystal technology. All of these modulators differ in terms of speed, resolution, and modulation capacity.

The rest of this tutorial survey is structured as follows. In Section 2, we present a brief yet detailed summary of relevant studies related to the optical compression methods developed for information reduction. The major aim of the optical compression methods we discuss here is to propose techniques allowing us to reduce the quantity of information to be stored for good reconstruction quality in relation to a given application. Following this, in Section 3, we focus on the issue

of information encoding methods. Indeed, this section will enable us to help the reader appreciate optical encoding techniques based on the modification of the spectral distribution of target information. In Section 4, we present several studies illustrating approaches for which encoding and compression are carried out simultaneously. Finally, in the concluding section, remarks are made regarding the viability of several optical implementations.

2. Optical Image Compression Methods

Data compression methods attempt to reduce the file sizes [27]. This reduction makes it possible to decrease the processing time and the transmission time, as well as the storage memory. As this review will make clear, the past decade has seen dramatic progress in our understanding of optical compression algorithms, especially those exploiting the phase of the FT of an image. It is a well-known fact that the spectrum phase is of utmost importance for reconstructing an image. Matoba *et al.* [28] demonstrated that it is possible to optically reconstruct 3D objects by using only phase information of the optical field calculated from phase-shifting digital *holograms*. In practice, this can be done thanks to a *liquid crystal SLM*.

Holography: *Holography is a 3D technique in which both the amplitude and the phase of the light wave reflected from objects can be determined. With digital holography a CCD camera is used to digitally capture interference patterns. To do this, we generally use the interference between the wave reflected by this object and the reference wave [2,29,30]. There are several methods to perform this optically and to optimize the reconstructed image. In this tutorial, we are interested in phase shifting interferometry digital holography (PSIDH), which uses several interference patterns corresponding to different reference wave phases to determine the complex wavefront at the plane of the camera. Color PSIDH triples the amount of data per hologram, as three wavefronts (one for each of the main colors) need to be stored. Digital holography has seen renewed interest with the recent development of megapixel digital sensors with high spatial resolution and dynamic range.*

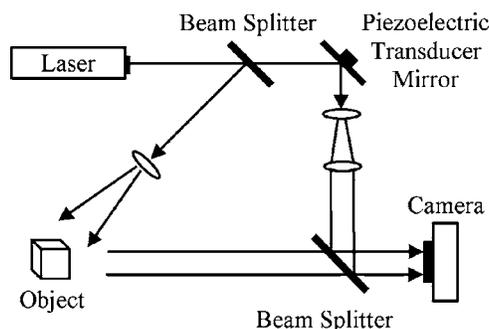
Liquid crystal SLM Modulator based on liquid crystal technologies.

Despite the interesting results provided by the PSIDH technique for the reconstruction of 3D objects, the use of PSIDH remains questionable in some instances, mainly because it generates files of very large size. Consequently, the

storage and/or transmission may cause serious problems, especially, for real-time applications. Therefore, it is an important task to reduce (compress) the size of these holograms in order that they can be manipulated in real time. For this reason, Subsection 2.1 introduces a technique that permits the PSIDH data to be compressed while retaining good-quality reconstruction of 3D objects. Optical correlation is widely used in the optical information processing domain to identify, recognize, and locate objects in a given scene. It measures the degree of similarity between a target object (object to recognize) and a reference object belonging to a reference database. To evaluate this similarity and make a decision, one needs to use all available information on the 3D object. Subsection 2.2 discusses several compression methods that have been proposed recently in the area of optical correlation for optical pattern recognition. First a technique aimed at compressing PSIDH data, which is adapted to optical correlation, is discussed. Next, a compression technique based on a wavelet transform (JPEG2000), designed for face recognition, is presented. Last, a compression method based on wavelets suitable for volume holographic image recognition is described. A compression method of holographic data adapted to the reconstruction of 3D objects transmitted by the Internet is discussed in Subsection 2.3. Some of the problems associated with the reconstruction of 3D objects are indicated in Subsection 2.4, problems that can be alleviated by using the integral imaging (II) method. As was noticed above for the hologram case, the II technique requires handling a large number of data. To reduce these data, a compression method using a discrete cosine transform (DCT) adapted to II is further discussed. Another setup to implement the JPEG2000 standard optically, while using a FT will be discussed in Subsection 2.6. Subsections 2.7 and 2.8 explore two other compression methods based on a FT and a Radon transform. Finally, in Subsection 2.9, an optical image compression method using a FT and based on a selection of spectral information to be transmitted and/or stored according to a selection criterion is discussed.

PSIDH Principle. The setup for PSIDH recording is displayed in Fig. 2 [31]. As is shown in Fig. 2, a laser source provides the reference beam that illuminates the object to be recorded. Using a beam splitter, a portion of the reference beam is separated and reflected by a mirror that is controlled by a piezoelectric transducer. The object is at a distance z_0 from the CCD camera. The distribution of the light that is reflected by the object at the plane of the camera is given by the Fresnel–Kirchoff diffraction integral

Figure 2



Setup for digital recording of the PSI hologram [31].

$$U_0 = \int \int_{\infty} U_{z_0}(x,y) \exp\left(\frac{ik}{2z_0}[(x-x')^2 + (y-y')^2]\right) dx' dy', \quad (1)$$

where k is the wavenumber and U_{z_0} denotes the distribution of the light reflected by the object at its plane,

$$U_{z_0} = A_{z_0}(x,y) \exp\{i\phi_{z_0}(x,y)\}, \quad (2)$$

where $A_{z_0}(x,y)$ and $\phi_{z_0}(x,y)$ are the amplitude and the phase of the wavefront on point (x,y) , respectively. The phase-shifted reference beam propagates through a second beam splitter toward the camera. Its distribution at the plane of the camera reads as ($U_R = A_R(x,y) \exp\{i\phi_R(x,y) + \phi\}$) with some specific values $\phi \in (0, \pi/2, 3\pi/2, \pi)$, $A_R(x,y)$ and $\phi_R(x,y)$ being the amplitude and the initial phase of the reference wave, respectively. The two waves interfere with each other, and the interference patterns

$$I(x,y;\phi) = |U_R(x,y;\phi) + U_0(x,y)|^2 \quad (3)$$

are recorded by the camera. The propagated wavefront due to the object, called a phase shifting interferometry (PSI) hologram or a Fresnel field, at the plane of the camera can be determined by the four recorded interference patterns as

$$U(x,y) = \frac{1}{4A_R} \left[(I(x,y;0) - I(x,y;\pi)) + i \left(I\left(x,y;\frac{\pi}{2}\right) - I\left(x,y;\frac{3\pi}{2}\right) \right) \right]. \quad (4)$$

2.1. Phase-Shifting Interferometry Digital Holography Compression

Darakis and Soraghan described a method for compressing interference patterns based on off-axis (phase-shifting) digital holography using the PSIDH hologram compression scheme [31]. Compared with other digital holography techniques this method has the advantage of increased reconstruction quality, as the unwanted zero-order and twin image terms are eliminated.

As several interferograms have to be recorded, in practice digital holography is limited to static scenes, as the light distribution from the object should remain constant over the recording. Another disadvantage of digital holography is that the resulting wavefront consists of complex floating point numbers occupying a large amount of storage space. Moreover, the use of standard compression techniques leads to a wrong 3D reconstruction object from a digital hologram. This is mainly because these methods lead to a loss of the holographic speckle that carries 3D information. The originality of the PSIDH method is to propose a compression (based on quantification and a Burrows–Wheeler transform [32]) in the reconstruction plane rather than in the spatial domain (complex wavefront or interference pattern). In spite of a significant speckle noise in the reconstruction, that the spatial correlations are higher in the rebuilding plane than in the holographic plane allows larger (lossless) compression rates in comparison with other methods found in the literature [33–37].

The results given by Darakis and Soraghan showed clearly that if a compression is carried out in the reconstructed plane, one will have a better *normalized root-mean-square* (NRMS) error than that obtained with other techniques. Their results indicate that, e.g., compression rates of approximately 20 and 27 can be ob-

tained with the JPEG and JPEG2000 methods, respectively, while a quality level of NRMS=0.7 is retained.

Finally, it is interesting to mention that, by taking advantage of the ability to

Normalized Root-Mean-Square (NRMS) error: *The NRMS error is used as a quantitative quality measure of the reconstructed image I' and is defined as*

NRMS

$$= \sqrt{\frac{\sum_{i=1}^{N_x} \sum_{j=1}^{N_y} \{I(i,j) - I'(i,j)\}^2}{\sum_{i=1}^{N_x} \sum_{j=1}^{N_y} \{I(i,j)\}^2}},$$

where the integers i and j define the locations of pixels, N_x and N_y are the dimensions of the images, and I and I' are the original and the reconstructed images, respectively.

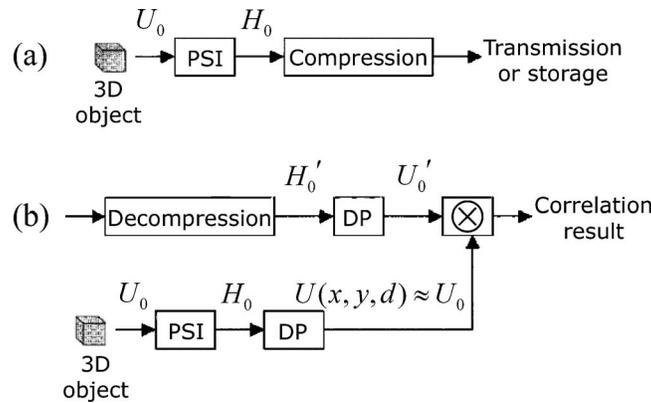
choose the quality factor offered by both the JPEG and JPEG2000 algorithms, this new holographic compression method substantially increases flexibility by offering a wide range of compression rates for specific quality levels.

2.2. Compression Methods for Object Recognition

Digital holography, which has been used for 3D measurement and inspection, requires an intensive storage memory. Such a requirement is important in PSIDH, which provides the means for 3D object recognition [38]. Each digital hologram encodes multiple views of the object from a small range of angles. Their digital nature means that these holograms are in a suitable form for processing and transmission. Furthermore, storage space and transmission time make compression of paramount importance. Based on the PSIDH technique, Naughton *et al.* presented the results of applying lossless and lossy data compression to a 3D object reconstruction and recognition technique [39]. They suggest a digital hologram compression technique based on Fourier-domain processing.

The principle of this operation is illustrated in Fig. 3. Naughton *et al.* recorded digital holograms with an optical system based on a Mach-Zehnder interferometer. Figure 3(a) presents their storage and transmission setup. U_0 denotes the complex amplitude distribution in the plane of the object. The camera-plane complex object H_0 is the PSI hologram obtained with the four reference waves. The holograms, of dimensions (2028×2044) pixels, are recorded by a camera using 8 bytes for both amplitude and phase information. These PSI holograms are then compressed (by using an adapted compression method) before storage and transmission. In Fig. 3(b), the authors presented the decompressed and reconstructed 3D object U'_0 for recognition application: \otimes is the normalized cross correlation operation, and DP denotes the digital propagation (reconstruction) stage. To realize a good reconstruction for 3D objects, PSI holograms having a significant resolution (large size) are needed. Thus, for real-time applications, holograms have to be compressed

Figure 3



Synoptic diagrams [39]: (a) 3D object recording in compressed hologram form (transmitter), (b) decompression and reconstructing the 3D object (receiver). PSI, image capture and interferometry stage; DP, digital propagation (reconstruction) stage; \otimes , normalized cross-correlation operation.

for transmission and storage. Such a large size is a crucial problem for pattern recognition applications based on correlation, especially for 3D object recognition [40,41]. Before discussing the compression methods, we give the reader a quick overview of the basic principle of correlation.

We briefly pause to introduce correlation techniques. Correlation filters have been devised for pattern recognition techniques based on the comparison between a target image and several reference images belonging to a database. There are two main correlators in the literature, i.e., the *VanderLugt correlator* (VLC) [1] and the *joint transform correlator* (JTC), which are summarized in the box.

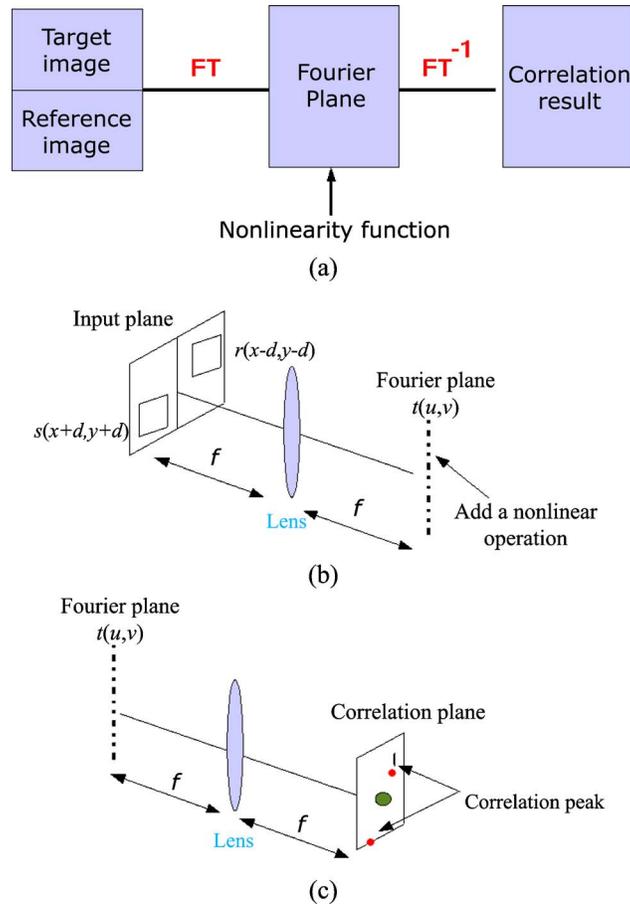
In [39], Naughton and co-workers compared their results to those obtained from various techniques using digitalized PSI holograms (treated either as single binary data streams with alternating amplitude and phase angle components, or as two separated real and imaginary data streams), such as Huffman coding [44], where an entropy-based technique is used, Lempel–Ziv coding [45], which takes advantage of repeated substrings in the input data, and Lempel–Ziv–Welch [46] and Burrows–Wheeler [32] codings, which transform the input through a sorting operation into a format that can be easily compressed. Naughton and co-workers [39] showed that the compression performances (the metric is the correlation peak height between the original and reconstructed images) are rather poor and proposed new lossy compression schemes; i.e., the hologram is first resized by a resampling technique, then quantization is applied directly to the complex-valued holographic pixels, followed by selective removal of discrete FT coefficients. In addition, Naughton and co-workers [39] demonstrated that digital holograms are very sensitive to resampling, probably because of the effects of speckle, which can be reduced by means of a high degree of median filtering. Hologram resampling resulted in a high degradation of reconstructed image quality, but for resizing to a side length of 0.5 and in the presence of a high degree of median filtering a compression factor of 18.6 could be achieved. Quantization proved to be a very effective technique. Each real and imaginary com-

VanderLugt correlator (VLC): *The synoptic diagram of the VLC (or frequency correlator plane) is presented in Fig. 4. It is based on the multiplication of the spectrum, S_0 , of the target image O by a correlation filter, H , made from a reference image. The input plane is illuminated with a linearly polarized incident parallel beam. Located in the rear focal plane of a Fourier lens, a SLM is used in order to display the chosen correlation filter in the Fourier plane of the optical setup. Many approaches for designing this filter can be found in the literature according to the specific objects that need to be recognized [1–11]. A second FT is then performed with a lens in a CCD Camera (correlation plane). This results in a more or less intense central correlation peak depending on the degree of similarity between the target object and the image reference.*

Joint Transform Correlator (JTC): *A simplified synoptic diagram of the JTC setup is presented in Fig. 5(a). Basically, it is an arrangement based upon the $4f$ setup with a nonlinear operation in its Fourier plane [42]. Its principle is to introduce, in the input plane, both the target and reference images separated by a given distance and to separate the writing and reading phases. In [43], this nonlinear operation was achieved by using an optically addressed SLM in the Fourier plane. A first beam coming from a laser illuminates the input plane that contains the scene, $s(x,y)$, i.e., the target image to be recognized, and the image reference, $r(x-d,y-d)$, where d represents the distance between the target and the reference images. The joint spectrum is recorded by the optically addressed SLM modulator and yields $t(x,y)$ [writing stage, Fig. 5(b)]. After an inverse FT of the joint spectrum of a second beam [reading stage, Fig. 5(c)], the correlation between the target and the reference image on a CCD camera is obtained. The correlation plane has several peaks that correspond to the autocorrelation of the whole scene in the center (zero order), and two correlation peaks (corresponding to the reference and target images). The location of the different correlation peaks depends on the positions of the reference and the target images within the scene.*

ponent can be reduced to as little as 4 bits while maintaining a high correlation peak and an acceptable reconstruction error, resulting in a compression rate of 16. The technique, based on the removal of discrete FT coefficients, achieves approximate compression rates of up to 12.8 for good cross correlation and up to 4.6 for rea-

Figure 4

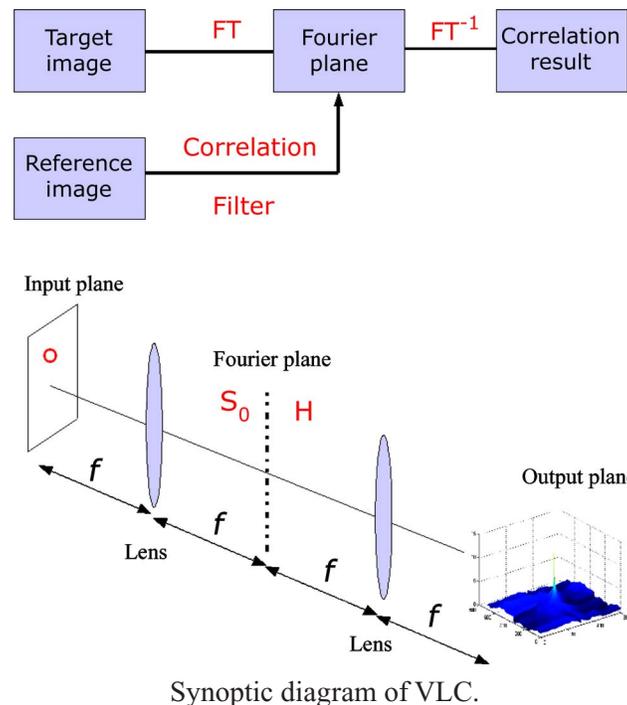


Nonlinear JTC principle setup: (a) synoptic diagram, (b) write-in setup, (c) read-out setup.

sonable reconstruction integrity. It is further anticipated that this can be improved by applying lossless compression or quantization to the remaining discrete FT coefficients. To give numbers, on the basis of a compression rate of 10.7 (6 bit quantization), and without exploiting interframe redundancy, complex valued holographic video frames of dimensions 640×640 pixels could be streamed over a 100 Mbit/s connection at a 20 Hz rate of frames with 1024×1024 pixels at 8 Hz.

Also, Wijaya *et al.* [47] developed advanced correlation filters that can perform illumination-tolerant face verification of compressed test images at low bit rates by use of the JPEG2000 wavelet compression standard. This scheme is ideal for face recognition systems that use devices such as cell phones because the recognition can be performed remotely. In fact, owing to limitations in communication bandwidth, it is necessary to transmit a compressed version of the image. This approach is based on the compression standard JPEG2000, which is a wavelet-based compression engine used to compress the face images to low bit rates suitable for transmission over low-bandwidth communication channels. At the receiver end, the face images are reconstructed with a JPEG2000 decoder and are fed into the verification engine [47]. Furthermore, Wijaya *et al.* explored how correlation filters, such as the minimum average correlation energy filter,

Figure 5



perform by using face images captured under different illumination conditions and encoded with different bit rates under the JPEG2000 wavelet-encoding standard.

For completeness, the work of Ding *et al.* [48] is also worth mentioning. These authors proposed and validated an optical image recognition system based on the mechanism of crystal volume holography and the wavelet packet compression method. Volume holographic associative storage in a photorefractive crystal has some special properties and can provide a suitable mechanism to develop an optical correlation system for image recognition. The method of wavelet packet compression was introduced in this optical system to reduce the number of images stored in the crystal. Through optimal wavelet packet basis selection, a set of best eigenimages, which are stored in the crystal as the reference images for recognition, are extracted from a large number of training images. Correlating the output of these eigenimages and the input ones may be used for classification and recognition according to the different light intensities of angularly separated beams. In their experiments, Ding *et al.* [48] showed that this scheme is practical and can significantly compress the data stored in the crystal while maintaining a high rate of recognition; e.g., 800 original images can be compressed into 15 eigenimages, which can recognize these original images with an accuracy of more than 97%

2.3. Efficient Compression of Fresnel Fields for Internet Transmission of 3D Images

Naughton *et al.* [49] proposed and validated a new scheme of multiple-client compression and transmission of 3D objects. These authors used the PSIDH

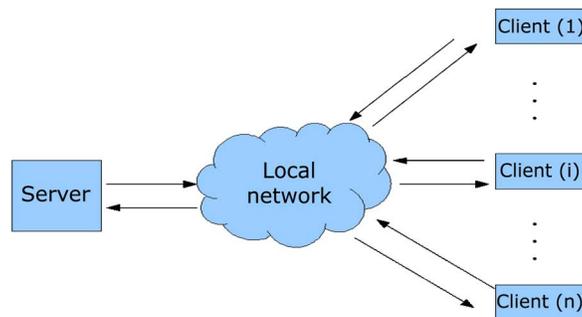
technique for recording multiple views of a 3D object (Fresnel fields). The digital Fresnel fields have the dimensions of (2028×2044) pixels and a storage mode of 8 bytes for the amplitude information and 8 bytes for the phase information for each pixel. Then Naughton *et al.* constructed an Internet-based Fresnel field compression application to measure reliably and accurately the interaction between compression times and transmission times. This client–server application and associated compression algorithms were written in Java, allowing them to develop a platform-independent environment for experimentation over the Internet. An overview of the operation of the networking application is displayed in Fig. 6. Thanks to this system, multiple clients through their user interfaces access the server and request particular views of 3D objects stored as Fresnel fields. The server responds by providing the appropriate window of pixels, and the clients reconstruct views of the 3D objects locally. This reconstruction can be done optically or digitally.

Unfortunately, in [49], Naughton *et al.* performed only digital reconstruction of the received and compressed PSIDH. As noted above, each of the various Fresnel holograms (PSIDHs) recorded and stored in the server has a very large size. For rapid transmission it is essential to reduce the amount of information in order to accelerate the transmission between the server and the clients. Thus, it is necessary to compress these Fresnel holograms. However, the compression of digital holograms differs from standard image compression, mainly because PSIDH stores 3D information in complex-valued pixels, and also because of the inherent speckle content that gives them a white-noise appearance. To achieve good compression, Naughton *et al.* proposed a lossy compression method in two stages. The first step consisted of a rescaling and quantization operation on the Fresnel fields (and digital holograms). It is defined for individual pixels as

$$H'(x,y) = \text{round}[H(x,y)\sigma^{-1}\beta], \quad (5)$$

where H denotes the original Fresnel field, H' is the compressed field, $\beta = 2^{(b-1)} - 1$ with b representing the number of bits per real and imaginary value, $x \in [1, N_x]$, $y \in [1, N_y]$, with N_x (N_y) being the number of samples in the x (y) direction, and $\sigma = \max\{|\min(\text{Im } H)|, |\max(\text{Im } H)|, |\min(\text{Re } H)|, |\max(\text{Re } H)|\}$. The actual reduction of data (bit packing) was performed in the second step, where the appropriate b bits were extracted from each value. A Fresnel field window of $N \times N$ pixels requires exactly $[(2N^2 \times b)/8]$ bytes. In their networking system, a Fresnel field H is compressed and then decompressed as H' , and an object U_0 is reconstructed by numerical propagation.

Figure 6



Synoptic diagram of the network-independent multiple system proposed by Naughton *et al.* in [49].

The quality of the reconstruction from the compressed field can be evaluated in terms of the NRMS defined above (see the box). A refined speedup metric was also defined that avoids the bias effects that would be introduced by including the reading, formatting, and imaging operations. These operations are independent of compression strategy and significant in comparison to transmission time. The refined speedup s' is calculated from

$$s' = \frac{\bar{t}_u}{(v + \bar{t}_c + \bar{d})}, \quad (6)$$

where t_u and t_c are the uncompressed and compressed transmission times, respectively, c and d are the times to compress and decompress, respectively, and the overbar denotes the mean of 40 trials. To give numbers, for windows of size 64×64 pixels or greater there is significant speedup (over 2.5) for quantizations of 8 bits or lower. This speedup rises to over 20 for 512×512 pixel windows. Finally, it of interest that this Internet-based compression application and full timing results are accessible on line [49].

2.4. Compression of Full-Color 3D Integral Images

There has been also great interest in 3D object imaging and visualization [50] using the *II technique*.

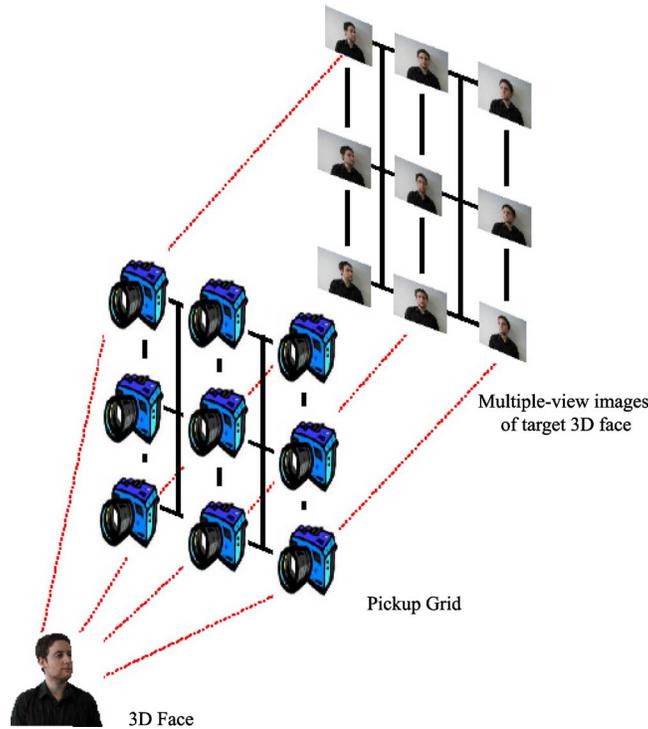
As mentioned in the box, the II technique requires a large amount of data. The

Integral Imaging (II) technique: *This technique records multiple views of a 3D object (each view is called an elemental image). For that purpose, multiple cameras deployed in a well-defined pickup grid are used. Each multiview image gives a unique perspective of the scene. These elemental images are used to reconstruct the 3D object. These elemental images can be considered consecutive frames in a moving picture for the purpose of compression.*

size of II data can be huge, especially with full-color components. Thus, it has become a critical issue to handle such a large data set for practical purposes such as storing on a media device or transmitting in real time. Yeom *et al.* [51] presented an II compression technique by *MPEG-2 encoding*.

MPEG-2 encoder: *MPEG-2 (Motion Picture Experts Group) is the ISO standard 13818 (or ITU-T Recommendation H.262). It is a popular coding technique for moving pictures and associated audio information on digital storage media [51,52].*

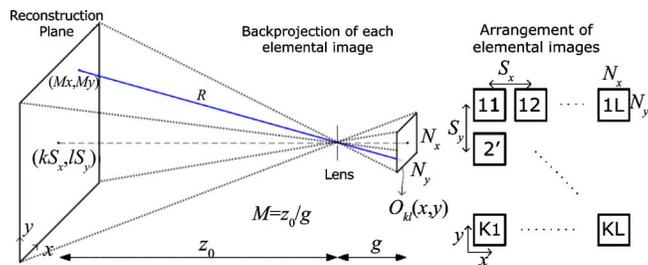
Figure 7



Principle of decomposition of the 3D object into several multiple-view images: elemental images.

3D Reconstructed Object Using the II Technique. The II technique is easy to achieve and does not require complex amplitudes as in the case of a digital hologram [50]. The first step in this technique consists in decomposing the 3D object into many elemental 2D images (with reference to Fig. 7). For that purpose, a pickup grid, made up of three rows of cameras (a row with a -15° view of the object, a second at 0° , and the third with a view at $+15^\circ$), is required. In the example shown in Fig. 7, the cameras were placed at a distance equal to 3 cm from each other. The reconstruction consists in combining all of these 2D elemental images in the output plane in a special way as shown in Fig. 8 and by using Eq. (7),

Figure 8



Left, schematic of image reconstruction in II process; right, arrangement of elemental images as in Tavakoli *et al.* [50].

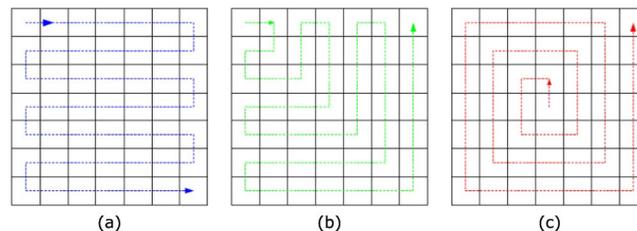
$$I(x,y,z_0) = \frac{\sum_{k=1}^K \sum_{l=1}^L I_{kl}(x,y,z_0)}{R^2(x,y)}, \quad (7)$$

where $I_{kl}(x,y,z_0) = O_{kl}(-x + (1 + 1/M)S_x k, -y + (1 + 1/M)S_y l)$ denotes the flipped and shifted original elemental image O_{kl} (with reference to Fig. 8), the integers k, l characterize the locations of the elemental image, z_0 is the distance between the reconstructed plane and the sensor along the optical axis, M is a magnification factor ($M = z_0/g$), g is the distance from the image to the plane from each lens, S_x and S_y denote the separation of the sensors in the x and y directions at the pickup plane, respectively, and the parameter R is used to compensate for the intensity variation due to the different distances from the object to the elemental image on the sensor. The parameter R is defined as

$$R^2(x,y) = (z_0/g) + [(Mx - S_x k)^2 + (My - S_y l)^2] \left(\frac{1}{M} + 1 \right). \quad (8)$$

As mentioned above it is possible to reconstruct a 3D object by using II. However, it should be recollected that this requires a very large amount of data (elemental images in II) to accurately reconstruct a 3D object. Furthermore, the data amount becomes huge for 3D color objects. For this specific purpose, Yeom *et al.* [51] proposed to use the method of MPEG-2 video compression [52]. To adapt the II technique to video compression technology, they consider the matrix of elemental images of II (Fig. 7) as a video sequence. To convert the matrix of elemental images in a video sequence, three different scanning topologies for elemental images in II were considered (Fig. 9). Parallel scanning is a sequential scanning in a parallel direction. It is suitable for II with different sizes in horizontal and vertical directions. Perpendicular and spiral topologies are other scanning methods to minimize motion compensation between elemental images. Spiral scanning can be adopted if more focused images are located at the center of II. Compression of the sequence by the MPEG scheme was then applied to take advantage of the high cross correlations between elemental images. Experimental results are presented in [51] to illustrate the image quality of the MPEG scheme characterized by the *peak-to-peak signal-to-noise ratio* (PSNR) of decompressed images (box).

Figure 9



Three different scanning topologies for converting an II into a sequence of elemental images: (a) parallel scanning, (b) perpendicular scanning, (c) spiral scanning. [51]

PSNR is defined as a metric to evaluate the efficiency of compression

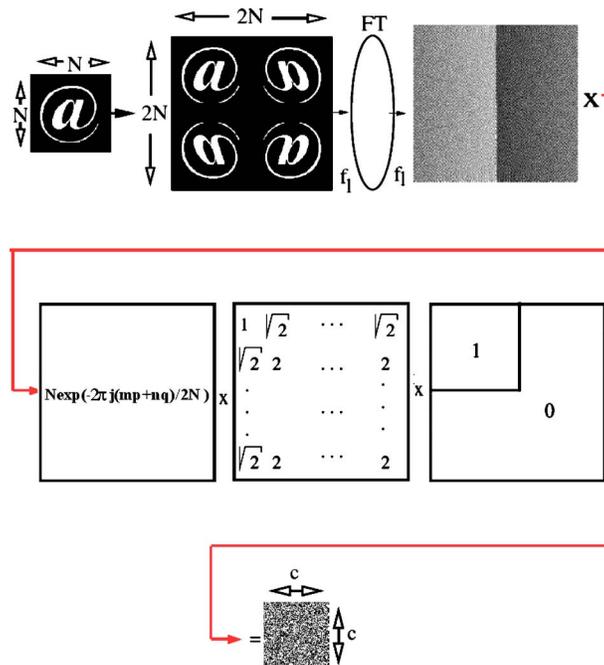
$$\text{PSNR}(A,B) = 10 \log_{10} \left(\frac{P^2}{\frac{1}{N_x N_y} \sum_{i=1}^{N_x} \sum_{j=1}^{N_y} |A(i,j) - B(i,j)|^2} \right),$$

where A and B denote the original and reconstructed images, P is the maximum value in one pixel, and (N_x, N_y) are the number of pixels in the x and the y axes of the image.

2.5. Optical Colored Image Compression Using the Discrete Cosine Transform

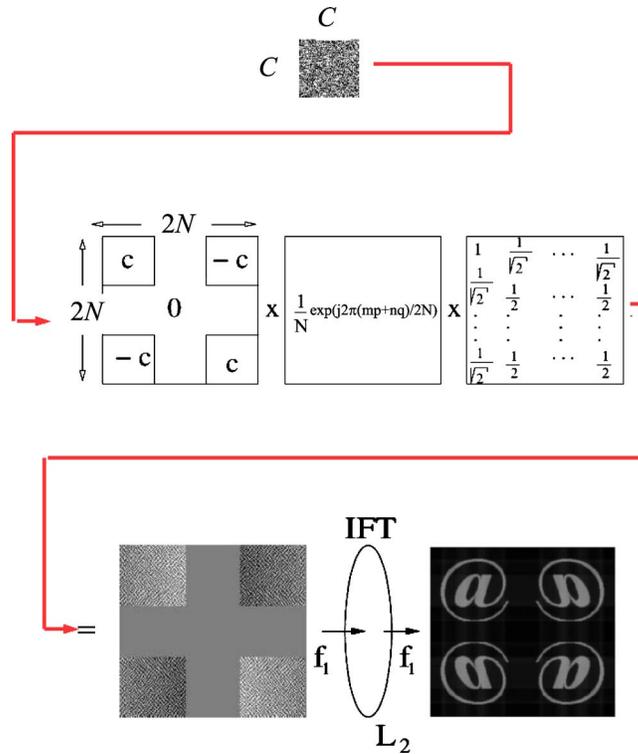
Thanks to the advantages and simplicity offered by the JPEG compression technique [53], Alkholidi *et al.* [54] suggested and validated a setup allowing a full optical implementation of their method (Figs. 10 and 11). Based on the fact that the JPEG compression relies on the DCT, these authors used the similarity existing between the DCT and the FT. Fourier transforming can be optically implemented by using a simple convergent lens [2]. In this context, Alfalou *et al.* [55] developed formulas to carry out the DCT with a fractional FT. For this purpose, they started by duplicating the target image (to be compressed), making it possible to eliminate the sinus part in the FT. Then, by using some holograms, they

Figure 10



Synoptic diagram of the proposed step implementing the DCT optically.

Figure 11



Synoptic diagram of optical JPEG decomposition.

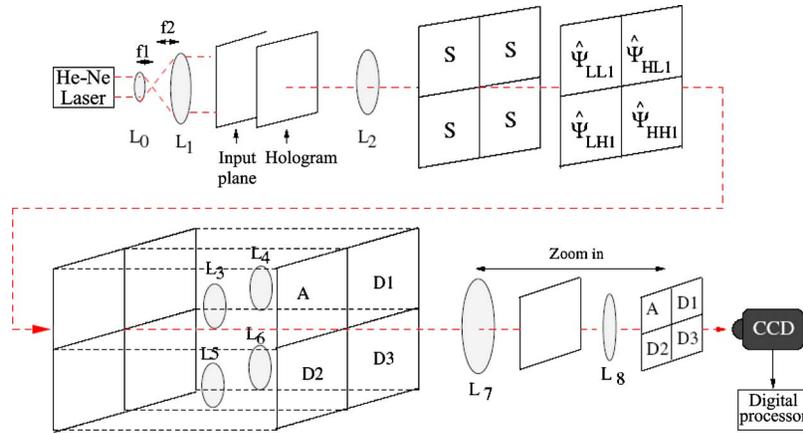
succeeded in implementing the DCT optically; see Fig. 10. It is worth noting that the authors multiply the DCT spectrum obtained by a low-pass filter in order to eliminate the DCT coefficients that are not located at the top left-hand corner, thus reducing the size of the data set to be stored and/or transmitted.

For the image decomposition, they proposed to use the setup presented shown in Fig. 11, consisting of the inverse stages carried out in Fig. 10. The validation of this setup was tested by numerical simulations using binary and multiple gray level images. Good performance was obtained with this method, which can also be adapted to compress color images. However, these authors proposed only a partial optical implementation of their technique, i.e., the decompression part. Indeed, a full experimental implementation of this method would necessitate the use of several SLMs and introduce difficult optical problems, e.g., alignment.

2.6. Real-Time Optical 2D Wavelet Transform Based on the JPEG2000 Standard

Taking inspiration from the JPEG2000 method, Alkholidi *et al.* [56] suggested and tested a technique of optical compression of images before any digital recording, based on the optical implementation of the wavelet transform [57]; see Fig. 12. The input plane, illuminated with a He–Ne laser beam, contains the image to be compressed ($N \times N$ pixels). Each pixel has a size Δx . Then, the spectrum S is separated into four samples by using a special periodic hologram. The FT is realized at the back focal plane of a convergent lens L_2 . In the spectral

Figure 12



Optical part of optoelectronic JPEG2000 compression setup.

plane, the four replicas are multiplied point by point by a second phase hologram representing the FT of the Haar wavelet (Ψ); LL denotes the low-frequency filtering (lines and columns, coarse image), LH is a low-frequency filtering of the columns consecutively with a high-frequency filtering of the lines, HL results from a high-frequency filtering of the columns after a low-frequency filtering of the lines, and HH corresponds to a high-frequency filtering of both lines and columns (difference image). By carrying out the FT^{-1} of the four spectra multiplied by the corresponding filter, four images (A, D1, D2, and D3) are obtained. A telescope including two convergent lenses (L7 and L8) is also used. A CCD camera is used to digitize the four images in order to perform the remaining stage of the JPEG2000, i.e., the entropy coding. Simulation results show that this optical JPEG2000 compressor–decompressor scheme can achieve high image qualities. Finally, it should be noted that an adaptation of this technique to colored images was also proposed in [57].

2.7. Fourier-Transform Method of Data Compression and Temporal Fringe Pattern Analysis

There are two main approaches to fringe pattern analysis: spatial and temporal. In the spatial fringe pattern analysis the phase is defined modulo 2π , e.g., [58–60]. The actual phase values have to be computed by means of a subsequent unwrapping operation. However, there are some practical problems in using this operation owing to discontinuities and low-modulation regions in the spatial fringe pattern. Temporal fringe pattern analysis is invaluable in studies of transient phenomena but necessitates large data storage for two essential sets of data, i.e., fringe pattern intensity and deformation phase [61–64]. Temporal fringe pattern analysis was first proposed by Huntley and Saldner [62] to circumvent the problems of discontinuities and low-modulation data points [63,64]. Ng and Ang [61] described a compression scheme based on the FT method for temporal fringe data storage that permits retrieval of both the intensity and the deformation phase. Basically, it consists in recording the values of the local spatial contrast, $s(x,y)$, for the band-limited spectrum of $T(u,v,k)$, where $T(u,v,k)$ is the FT of the intensity function, $t(x,y,k)$, that corresponds to each spatial point (x,y) and frame k on a typical fringe pattern

$$t(x,y,k) = \frac{1}{2}s(x,y)\exp[i(\phi(x,y) + \Delta(x,y,k) + \psi(x,y,k))]. \quad (9)$$

Here $\phi(x,y)$ is the random phase, $\Delta(x,y,k)$ is the phase deformation, $\psi(x,y,k)$ is the temporal carrier phase that is introduced, and $r(x,y)$ is the background variation. The intensity $i(x,y,k)$ can be written as

$$i(x,y,k) = r(x,y) + t(x,y,k) + t^*(x,y,k). \quad (10)$$

If the FTs of $r(x,y)$ and $t^*(x,y,k)$ are filtered out, the remaining spectrum, inverse transformed, will give $t(x,y,k)$ alone. If we assume that $\Delta(x,y,0) = \phi(x,y)$, taking the real and the imaginary parts of $t(x,y,k)$ will then allow us to derive

$$\Delta(x,y,k) + \psi(x,y,k) = \tan^{-1}\left(\frac{\text{Im}(t(x,y,k))}{\text{Re}(t(x,y,k))}\right) - \Delta(x,y,0). \quad (11)$$

Because ψ is known for every spatial point and frame, it is then possible to derive Δ for every spatial point and frame by a simple differencing operation. Essentially, this scheme takes advantage of the band-limited and symmetrical nature of the Fourier spectrum to perform the compression. It should be also noted that only one FT^{-1} operation—which is the most computationally intensive—is needed to restore the intensity or deformation phase of the fringe pattern at each spatial point from the stored data. With the scheme described here applied to the wavefront interferometry intensity fringe patterns, a file that was 34.2 Mbytes in size was created. A huge compression ratio (defined as the ratio of the original file size to the compressed file size) of 10.77 was achieved, wherein the useful data ratio (defined as the ratio of the number of spatial data points used during the compression scheme to the number of original spatial data points) was still significant at 0.859. The average root-mean-square error in phase value restored was very small, i.e., 0.0015 rad, indicating the accuracy of the phase retrieval process.

2.8. Radon Transform and Fourier Transform for a Bandwidth-Compression Scheme

As was mentioned in Section 1, we are interested in optical information processing techniques based on FT and/or filtering. In this context, we begin the first part of this tutorial by describing a bandwidth-compression scheme for 2D images developed by Smith and Barrett [65]. For the purpose of reducing the size of the information necessary to reconstruct an image, this technique uses a Radon transform and filtering, threshold, and quantification steps. The Radon transform makes the 2D FT of a 2D image readily accessible without 2D operations' actually having to be performed. Moreover, the Radon transform lends itself to FT compression for at least three reasons: the coding process can be performed with state-of-the-art 1D devices, the large dynamic range typical of the components of the FT is significantly reduced by the filtering operation, and one line through the center of the 2D FT can be examined at a time and adaptively compressed.

To compress a 2D image $f(\mathbf{r}) = f(x,y)$, Smith and co-workers begin by carrying out its Radon transform, which can be expressed by a set of 1D projections of $f(\mathbf{r})$ along a given direction ϕ as

$$\lambda_\phi(p) = \int \int_{-\infty}^{\infty} f(\mathbf{r}) \delta(p - \mathbf{n} \cdot \mathbf{r}) d^2r, \quad (12)$$

where $\delta(p - \mathbf{n} \cdot \mathbf{r})$ is a 1D Dirac delta function restricting the integration of f to a line (with normal \mathbf{n}) located a distance p from the origin. For each projection direction ϕ , a 1D function $\lambda_\phi(p)$ is constructed. The set of all $\lambda_\phi(p)$ ($p \in]-\infty, +\infty[$ and $\phi \in [0, \pi]$) constitutes the Radon transform of $f(x, y)$. Performing the 1D FT of Eq. (12) and using the shifting property of the delta function allows us to write to the 2D FT of $f(\mathbf{r})$, evaluated along the line $\rho = \mathbf{n} \nu$, where \mathbf{n} in the frequency domain is parallel to \mathbf{n} in the spatial domain, as follows:

$$F(\nu) = \int \int_{-\infty}^{\infty} f(\mathbf{r}) \exp(-2\pi i \nu \mathbf{n} \cdot \mathbf{r}) d^2r. \quad (13)$$

Here ν is the frequency-variable conjugate to p , and ρ is the frequency-variable conjugate to \mathbf{r} . Each line (FT of the Radon projection $F(\nu)$) is multiplied by the frequency filter $|\nu|$ before being compressed. Then, the FT^{-1} is applied to this product and evaluated at $\rho = \mathbf{n} \nu$. The compression step is accomplished by thresholding and quantizing the components of each Fourier line. Thresholding was realized by truncating each line past some cutoff frequency C_ϕ , which is variable from line to line, i.e., depends on ϕ . The value of C_ϕ is found from [65]

$$\int_0^{C_\phi} |\nu| |F(\rho)_{\rho=\nu \mathbf{n}}| d\nu = \left(\frac{\int_0^\infty |\nu| |F(\rho)_{\rho=\nu \mathbf{n}}| d\nu}{\max\left(\int_0^\infty |\nu| |F(\rho)_{\rho=\nu \mathbf{n}}| d\nu\right)} \right)^T \int_0^\infty |\nu| |F(\rho)_{\rho=\nu \mathbf{n}}| d\nu. \quad (14)$$

Here, T is a parameter that controls the degree of truncation, and $\max(\int_0^\infty |\nu| |F(\rho)_{\rho=\nu \mathbf{n}}| d\nu)$ is the largest value of $\int_0^\infty |\nu| |F(\rho)_{\rho=\nu \mathbf{n}}| d\nu$ for $\phi \in [0, \pi]$. After truncating the line, Smith and Barrett quantize the components by dividing the full dynamic range specific to the line into a series of uniform, discrete ranges. To demonstrate the method a gray scale image was compressed. The region to be compressed is a circle with a radius of 64 pixels. Smith and Barrett [65] showed that it is possible to reconstruct this gray-scale image with a good visual rendering, with truncation of 66% of components with 3 bit quantization. They had also a good visual result with truncation of 48% of the Fourier components with 2 bit quantization. Three interesting features of this approach are that only 1D operations are required, the dynamic range requirements of the compression are reduced by a filtering step associated with the inverse Radon transform, and the technique is readily adapted to the data structure. But this technique can be complicated to achieve with an all-optical system. In addition, it necessitates information about each FT line to adapt the filter and the compression. Thus it is very difficult for this technique to be effective in real time.

2.9. Compression and Multiplexing: Information Fusion by Segmentation in the Spectral Plane

An attempt to develop optical image compression in video sequences was made by Boumezzough *et al.* [66]. Subsequently Soualmi *et al.* [67] developed this preliminary study by exploiting the properties of the image phase spectrum. This technique [with reference to Fig. 13(a)] consists in merging the spectra of the

Figure 13

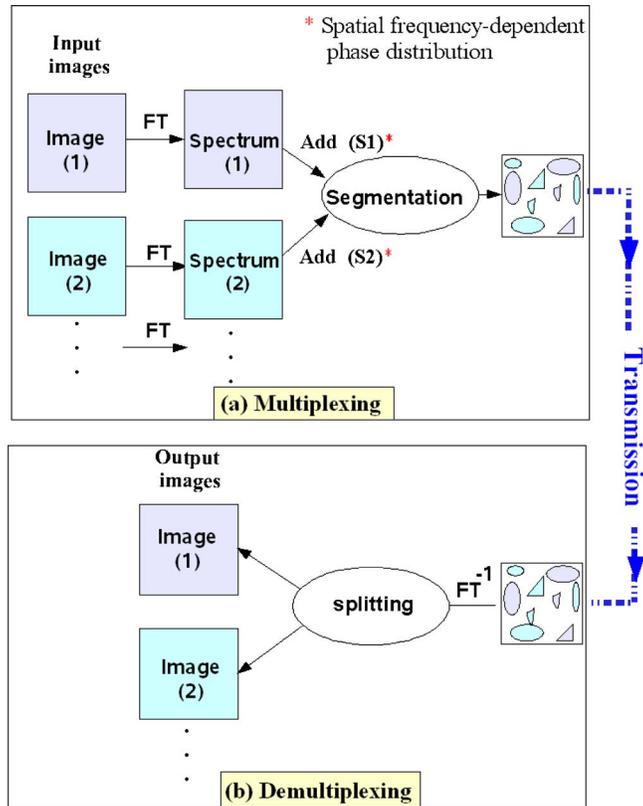


Diagram of optical compression with multiplexing from a spectral fusion schema: (a) multiplexing, (b) demultiplexing.

various images of the video sequence and compressing them according to a well-defined criterion. A linear variable spatial-frequency-dependent phase distribution is then added for each of the spectra in order to separate the corresponding images in the output plane after a second FT in the segmented spectral plane [Fig. 13(b)]. For each pixel (k, l) , the segmentation criterion compares the relative energy $E_i(k, l)$, normalized to the total energy, associated with this pixel for image i to the energy in the other images. From these comparisons over the sequence, a winner-takes-all decision assigns this pixel to a specific image according to

$$\frac{E_i(k, l)}{\sum_{m=0}^N \sum_{n=0}^N E_i(m, n)} = \text{Max} \left(\frac{E_j(k, l)}{\sum_{m=0}^N \sum_{n=0}^N E_j(m, n)} \right) \quad \forall i \neq j. \quad (15)$$

A specific linear spatial-frequency-dependent phase distribution is added to each attributed area of the image spectrum in order to separate each image in the final operation. Then, a demultiplexing step is performed simply by FT^{-1} . However, this technique presents a major drawback when the images to be compressed resemble each other, as is the case in a video sequence. Indeed, the selection operation based on a pixel-by-pixel comparison for different spectra leads to the decom-

position of the spectral plane into many small areas. If the images are very similar, these areas will be very small, i.e., *isolated pixels*.

*An **isolated pixel** is defined as a winner pixel that represents one frequency of the spectrum of image, say 1, surrounded with pixels from another image, say 2. However, a single pixel is not enough to correctly diffract light.*

Thus, the degree of degradation of the reconstructed images with this technique depends on both the image content and the segmentation criterion. This is due to the locality of the segmentation. Because of image similarities, two problems need to be considered. First, if the pixels belonging to the spectral plane are attributed mainly to the spectrum of one specific image to be multiplexed, the reconstruction will not be optimal for the other images. Thus, it is necessary to get a uniform repartition of the different images for the segmentation. The second problem concerns the significant spreading of the spectrum plane (isolated pixel). These two aspects degrade the rebuilt image quality. In order to overcome these difficulties, an attempt was made to improve the Fourier plane segmentation by using different segmentation criteria and considering not only the energy, but other information such as the phase and the gray level gradient [67]. However, the use of these various criteria on several types of image showed that the criteria choice improves the reconstructed image quality only slightly, notably because of the overlapping of the various image spectra to be compressed. To prevent overlapping Cottour *et al.* [68] proposed to reorganize the various Fourier planes by shifting the centers of the various spectra (Fig. 14). On applying this approach to a representative video sequence, simulations showed the good performance of this technique [68]. However, it requires interrogation of the whole image spectral planes to select the relevant zones. In this regard, coherent optics can be a solution. But an all-optical implementation of this technique is

Figure 14

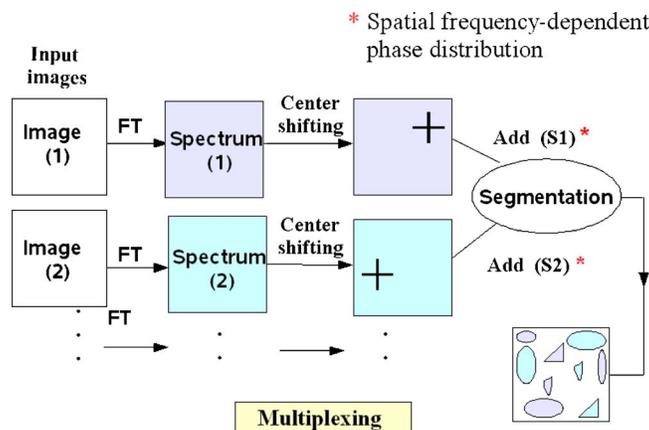


Diagram showing how to optimally gather information from different images.

rather complex to develop. Studies are currently in progress in order to carry out this segmentation stage digitally. Furthermore, this technique requires a numerical recording of the various merged spectra (amplitude and phase) in the Fourier plane before transmission.

3. Optical Image Encryption Methods

The global economic infrastructure is becoming increasingly dependent on information technology, with computer and communication technology being essential and vital components of government facilities, power plant systems, medical infrastructures, financial centers, and military installations, to name a few. Finding effective ways to protect information systems, networks, and sensitive data within the critical information infrastructure is challenging even with the most advanced technology and trained professionals. The increasing number of information-security-related incidents, organized crimes, and phishing scams means that securing information is becoming a major issue in the current information-based economy. To secure information, many research directions have been suggested in the past decade. Some security systems rely on the secrecy of the protocol for the algorithm encoding the information or on cryptography (software approaches), and some rely on aspects of the architecture (hardware approaches). In fact, electronic devices consume power, take time to compute, and emit electromagnetic radiation highly correlated with the decoding processing.

In this tutorial we focus on the software approach. We distinguish two kinds of software solution. First, there are solutions based on cipher techniques, like the symmetric data encryption standard (DES) [69] or asymmetric Rivest–Shamir–Adleman (RSA) [70]. As these techniques rely on factorials of large numbers, they are easily correlated to hardware aspects. The second type of solution consists in encoding the input image into two chosen noise functions by using the $4f$ setup, i.e., convolution between the input image multiplied by the first noise function and the impulse response of the second function noise. It is the latter that will be investigated here. These encryption techniques originate in the optical image processing community and continue to pose many challenges in several areas [71–89], e.g., double random phase, digital holography in the Fourier and Fresnel domains, multiplexing, polarized light, and interferometric techniques.

Among those techniques, the optical encryption technique, called digital correlation hologram, proposed by Abookasis *et al.* [89], based on a spatial correlation between two separated computer generated holograms, deserves special attention. These authors used an optical JTC architecture. Note that alternative JTCs have also been proposed in the literature [90–93]. The fractional FT has been shown to be a key element in other optical encryption algorithms [94–99]. Multiple-image encryptions methods were also suggested [100,101]. Their principle is based on encoding two original images into amplitude and phase in the input plane, followed by a combination of these images into a single one.

3.1. Double Random Phase Encryption System

With their pioneering work on double random phase (DRP) encoding, Réfrégier and Javidi [71] paved the way for many subsequent proposals for optical security and encryption systems. Their technique consists in encrypting an image dis-

played in the input plane of the $4f$ setup (Fig. 15) into a stationary white noise, while modifying its spectrum. In fact, images have a colored spectral density; thus, to encode images they propose to modify the color spectral density to obtain white spectral density. To encode an image, we must change both amplitude and phase information, because it is possible to reconstruct the image by using only the amplitude or the phase spectral information. For this purpose, Refrégier and Javidi multiply the input image (to be encrypted) $I(x,y)$ by a first key (a first random phase mask $RP_1 = \exp(i2\pi n(x,y))$, where $n(x,y)$ is a white noise uniformly distributed in $[0,1]$), then multiply the spectrum of this product by a second encryption key (a second random phase mask $RP_2 = \exp(i2\pi b(\nu,\mu))$, where $b(\nu,\mu)$ is a white noise uniformly distributed in $[0,1]$ and being independent of $n(x,y)$). Returning to the schematics of Fig. 15, we note that a second FT is realized in order to find the encrypted image in the output plane I_c ,

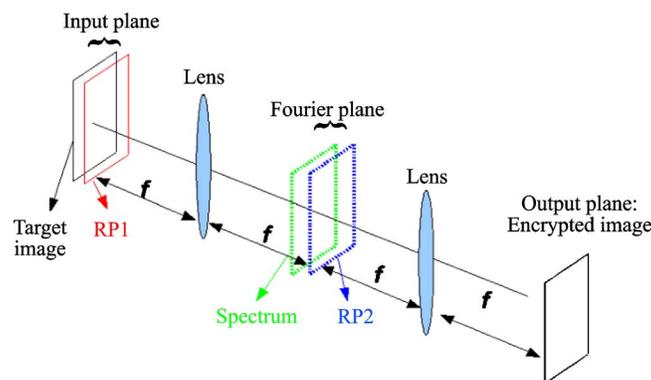
$$I_c(x,y) = (I(x,y)\exp(i2\pi n(x,y))) \otimes h(x,y), \quad (16)$$

where \otimes denotes the convolution operation and $h(x,y)$ is the impulse response of the second random phase function $h(x,y) = \text{FT}^{-1}[\text{RP}_2] = \text{FT}^{-1}[\exp(i2\pi b(\nu,\mu))]$. Then, the double-encoded image is recorded in a CCD camera (we must recode both its real part and its imaginary part). We can also record it as a digital hologram in a CCD camera, using a reference plane wave [102]. By using two encoding keys (one in the input plane and another one in the Fourier domain), a dense random noise is obtained, which is superimposed on the target image at the $4f$ setup output, ensuring very efficient image encoding. Using the $4f$ setup, this method can be implemented optically with maximum optical efficiency. In fact, the use of only the random phase function allows us to get all the input energy at the encrypted image. After transmission and for the purpose of decoding $I_c(x,y)$ Refrégier and Javidi proposed using a $4f$ optical setup illuminated by coherent light. After achieving a first FT of I_c , they multiply the result by $\text{RP}_2^* = \exp(-i2\pi b(\nu,\mu))$, and by recording the FT^{-1} of this multiplication in a CCD camera placed in the output plane, they finally obtain $|I(x,y)\exp(i2\pi n(x,y))|^2 = |I(x,y)|^2$.

3.2. Resistance of DRP against Attacks

In practice, however, the DRP encryption scheme presents some weakness against attackers [103–105]. Indeed, if hackers can again access to the system it

Figure 15



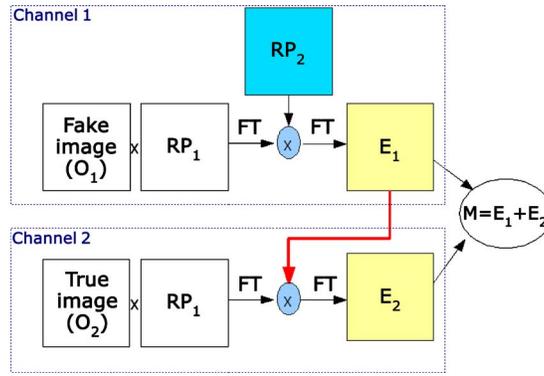
Synoptic diagram of the double random phase encrypted system.

is easy for them to introduce a Dirac signal image in the input system. Thus, in the Fourier plane, we find the spectrum of the Dirac signal multiplied by the second RP_2 key, while in the output plane, we get the FT of the second encryption key. Thus, a FT^{-1} is sufficient for finding this second encryption RP_2 key, and the security system is cracked. It should be emphasized that Frauel and co-workers [103] have studied in detail a broad panel of attacks against the DRP encryption scheme. These attacks are demonstrated on computer-generated ciphered images. Some of these attacks are impractical, and other are very effective. Frauel and co-workers showed that an exhaustive search of the key is generally intractable, even when applying some simplifications to reduce the number of combinations. However, these authors have presented chosen and known plaintext attacks that are able to efficiently recover the keys of the system. More specifically, the most dangerous attack was found to require only two known plain images. Furthermore, given the risks involved in the attacks presented, they advise extreme caution when using DRP encryption and suggested the use of large keys of at least 1000×1000 pixels and, if possible, avoiding reuse of the same keys for different images. A safer alternative to the original DRP encryption is to use variant schemes such as keys in the Fresnel domain or fractional FT encryption (see Subsection 3.5). It should be also noticed that Carnicer *et al.* [104] presented a chosen ciphertext attack in which an attacker can retrieve the key by inducing a legitimate user to decipher many specially crafted ciphered images. DRP is also vulnerable to a different type of attack, for which an enemy can access random phase keys in both the input plane and the Fourier plane [105].

3.3. Multiple-Encoding Retrieval for Optical Security

Among the various techniques that have been suggested in the literature for using random phase encryption keys, making it possible to increase the encoding rate significantly, we focus on the approach proposed by Barrera *et al.* [106]. This technique consists in encrypting the target image by a multiple-step random phase encoding with an undercover multiplexing operation. The true image is stored in a multiple record (called an encodegram). To increase the security of the true hidden image and confuse unauthorized receivers, an encoded fake image with different content is added to the encodegram. This fake image has only a small effect on the retrieval of the true hidden image. Owing to the specific property of a retrieval protocol and by using the appropriate random phase masks, the authors are able to reconstruct this image. The schematic undercover encryption diagram is presented in Fig. 16. The diagram consists of two channels based on the $4f$ architecture. In the first one, a fake image, O_1 , is multiplied by a first random phase function RP_1 . Next, the spectrum is multiplied with a second random phase function RP_2 . By carrying out a second FT, the double-encrypted fake image, E_1 , is obtained. In the second channel, the true object is multiplied by the first random key used in channel 1. After Fourier transforming it, the resulting spectrum is multiplied with the double-encrypted fake image E_1 . By performing a FT, the second double-encrypted image E_2 is obtained. These two encrypted images are added to obtain a multiplexed encrypted image (encodegram), i.e., $M = E_1 + E_2$. The diagram in Fig. 16 presents a simple and improved image encryption scheme that uses a virtual phase image to jam the original decoding mask [83]. To decrypt the information, the authors proposed the use of the following protocol. First, a conjugated version of M is realized. Then, by multiplying the spectrum of M^* with the second random phase function RP_2 , two terms are obtained: the first, called K , is equal to $FT(O_1 \times RP_1)$, and the second is equal to $FT(O_2 \times RP_1^*) \times E_1^* \times RP_2$. After filtering out the second term, K is multiplied with the conjugate of RP_2 , followed by

Figure 16



Undercover encryption diagram.

a FT, getting E_1^* . Going back to the multiplexed information M , Fourier transforming it, and multiplying it by E_1^* results in

$$\text{FT}(M)E_1^* = \text{FT}(O_1\text{RP}_1)\text{RP}_2(E_1)^* + \text{FT}(O_2\text{RP}_1)E_1E_1^*. \quad (17)$$

Then, after filtering out the first term in Eq. (17) and performing a second FT in the remaining second term, the authorized user finally recovers the true image O_2 . A series of computer simulations with different images has verified the effectiveness of this method for image encryption [106]. Digital implementation of this method makes it particularly suitable for the remote transmission of information.

3.4. Image Encryption Approaches Based on Joint Transform Correlator System

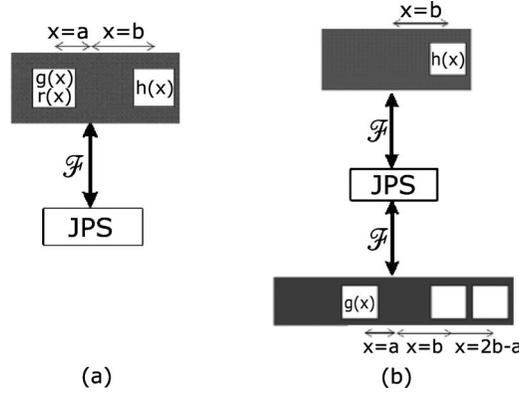
3.4a. Digital Color Encryption Using a Multiwavelength Approach and a Joint Transform Correlator

Amaya *et al.* [93] proposed a digital color image encryption technique using a JTC architecture [107] and a wavelength multiplexing operation. In their optical arrangement, the color image to be encrypted is separated into three channels: red, green, and blue. The principle of the JTC setup [93] for encryption of a color image is shown in Fig. 17. One of the JTC apertures contains the input image information corresponding to a determined color channel bonded to a random phase mask, while the other JTC aperture contains the reference random phase key code. Let us specify the notation. For simplicity, 1D notation is used. The target image (image to be encrypted) is $g(x)$. Two random phase codes are considered: $r(x)$ is the input random phase code, and $h(x)$ is the reference random phase key code. Both random phase codes have uniform amplitude transmittance, and they are statistically independent. Then, $r(x)$ and $g(x)$ are placed together on the input plane at coordinate $x = a$, and $h(x)$ is placed on the input plane at the coordinate $x = b$. The encrypted joint power spectrum (JPS) in the Fourier plane reads as

$$\text{JPS}(\nu) = |\text{FT}[r(x - a)g(x - a) + h(x - b)]|^2. \quad (18)$$

Equation (18) describes the encrypted JPS lighted with a single wavelength. Since the speckle size generated by the random phase masks is wavelength de-

Figure 17



JTC encryption architecture: (a) write-in setup and (b) read-out setup; $g(x)$ is the input object, $r(x)$ and $h(x)$ are the encoding phase masks; \mathcal{F} stands for FT [93].

pendent, the illuminating wavelength variation will produce a corresponding JPS modification. As expected, if the illumination wavelength changes, maintaining the reference random phase key code, the encrypted spectrum changes as well. As previously mentioned, a color image can be represented by three primary RGB colors. In their color image encryption method, Amaya *et al.* [93] each color channel is encrypted independently and multiplexed in a single medium by using the JTC scheme, thereby generating the multiplexed JPS, i.e., $\text{MJPS} = \text{JPS}(\text{green}) + \text{JPS}(\text{blue}) + \text{JPS}(\text{red})$. An example of a storing medium to perform this operation in practice is a photorefractive material. Multiplexing is achieved by keeping the random phase masks in each encrypting step and only changing the illuminating wavelength. Stated in other words, this approach can be considered an extension of the conventional JTC encryption architecture to include wavelength multiplexing. To record the three JPSs in a single plane, an apochromatic optical system can be used [104]. To decrypt the encrypted multiplexed JPS, Amaya *et al.* proposed the setup displayed in Fig. 17(b) [93]. All channels work in the same way. Thus, we can consider the decryption of the JPS associated with a specific wavelength (λ_{red} , λ_{green} , or λ_{blue}). If the storage medium transmittance behaves as an intensity linear register, after plane wave illumination and FT^{-1} , the stored JPS(ν) gives

$$\begin{aligned} \text{JPS}(x) = & [r(x)g(x)] \cdot [r(x)g(x)] + \delta(x) + h(x) \cdot [r(x)g(x)] \otimes \delta(x - b + a) \\ & + [r(x)g(x)] \cdot h(x) \otimes \delta(x - a + b), \end{aligned} \quad (19a)$$

where the symbol \cdot denotes correlation. The cross correlations of $r(x)$, $g(x)$, and $h(x)$ are obtained at the output at coordinates $x = a - b$ and $x = b - a$. The autocorrelation of $r(x)g(x)$ is obtained at coordinate $x = 0$. When the key code $h(x)$ is placed at coordinate $x = b$, the encrypted power spectrum JPS(ν) is illuminated by $H(\nu)\exp[-2\pi i b \nu]$ (Fig. 13). By FT^{-1} , $O(\nu) = \text{JPS}(\nu)H(\nu)\exp[-2\pi i b \nu] = \text{TF}[o(x)]$, $o(x)$ is

$$\begin{aligned} o(x) = & h(x) \otimes [r(x)g(x)] \cdot [r(x)g(x)] \otimes \delta(x - b) + h(x) \otimes \delta(x - b) + h(x) \\ & \otimes h(x) \cdot [r(x)g(x)] \otimes \delta(x - 2b + a) + r(x)g(x) \otimes \delta(x - a). \end{aligned} \quad (19b)$$

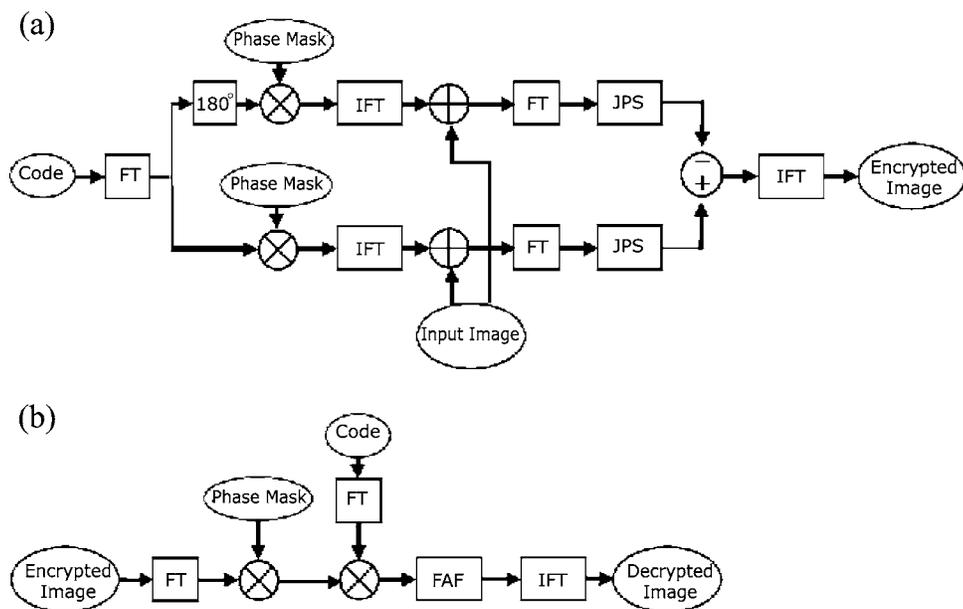
The intensity of the fourth term on the right-hand side of Eq. (19b) produces the

input image, given that $g(x)$ is positive, and an intensity-sensitivity device removes the phase function $r(x)$. The input image is obtained at coordinate $x=a$. The undesired terms are spatially separated from the recovered image. Then, the operation is repeated three times by using the three wavelengths (λ_{red} , λ_{green} , and λ_{blue}) to find the decrypted color target image, the wavelength appearing as an extra coding key in the same way as the reference phase encoding mask. This elegant approach has several advantages with respect to other color image encryption techniques [108,109], and in comparison to DRP coding. The standard $4f$ DRP encrypting architecture needs to produce a conjugate of the encryption data or the encryption random phase mask key in order to retrieve the input data (see Subsection 3.1). Also, the $4f$ scheme requires an extremely precise alignment; the JTC, in contrast, is not subject to this constraint. However, although this approach is elegant, it requires a large size input plane to contain both the target image and the encryption key within a distance $a+b$ between them [110].

3.4b. Optical Security System Employing Shifted Phase-Encoded Joint Transform Correlation

Another adaptation of the JTC setup to encrypt information was proposed recently by Nazrul Islam and Alam [111]. This system uses a shifted phase-encoded JTC (SPJTC) architecture. The SPJTC technique has been used for optical pattern recognition, where it shows excellent correlation performance [112]. The proposed technique offers a simple architecture, as no complex conjugate of the address code is required for decrypting the input information. The encrypted information remains well secured, because no unwanted decryption is possible. The encryption method proposed by Nazrul Islam and Alam [111] is presented in Fig. 18(a). After a FT the address code $c(x,y)$ ($c(x,y) = \text{FT}^{-1}[C(u,v)]$, where $C(u,v)$ is a phase-only 2D signal) shifted by y_c in the input plane of the JTC setup, Nazrul Islam and Alam multiply the spectrum by the phase

Figure 18



Block diagram of the SPJTC architecture: (a) encryption process, and (b) decryption process [111]. IFT is synonymous with the FT^{-1} .

key (random phase mask) ϕ in a first channel. The second channel is phase shifted by 180° to the spectrum of the chosen address code, then multiplied by the FT of the phase mask, which has a random phase varying from $-\pi$ to π . Thereafter, the FT^{-1} of the two signals emanating from the two channels yields the phase-encoded address codes, i.e., for the first channel $c_1(x,y) = c(x,y-y_c) \otimes \phi(x,y)$, and for the second channel $c_2(x,y) = -c(x,y-y_c) \otimes \phi(x,y)$. Next, the two phase-encoded address codes are combined with the input image to form two input joint images, which are then introduced in the two parallel channels. If $t(x,y-y_t)$ represents the input image to be encrypted, then the two input joint images for the two parallel channels can be written as $s_1(x,y) = c(x,y-y_c) \otimes \phi(x,y) + t(x,y-y_t)$ and $s_2(x,y) = -c(x,y-y_c) \otimes \phi(x,y) + t(x,y-y_t)$, respectively. After applying the FT operation to these signals, the corresponding two JPSs are obtained. To obtain the encrypted image $s(x,y)$ [Eq. (20)], the difference [Fig. 18(a)] between these two JPSs is taken, and a FT^{-1} of the result yields

$$s(x,y) = 2[t(x,y-y_t) \otimes c^*(x,y-y_c) \otimes \varphi^*(x,y) + t^*(x,y-y_t) \otimes c(x,y-y_c) \otimes \varphi(x,y)]. \quad (20)$$

The decryption stage is presented in Fig. 18(b). Basically, it consists in first realizing the FT of the encrypted image, followed by a multiplication of the encrypted image spectrum by the phase mask and the address code used in the same phase encryption (this multiplication is realized in the Fourier domain). By performing a FT^{-1} of the result, the decrypted image is found at the output plane. In this plane, two scenarios can be considered. First, a single phase address code is used ($|C(u,v)|^2 = 1$), and the decrypted image without any distortion is obtained, i.e., $t(x,y-y_t) + \text{noise}$. Second, if $|C(u,v)|^2 \neq 1$, Nazrul Islam and Alam suggested using a fringe-adjusted filter to minimize the distortion operating in the decrypted image [113]. The performance of the proposed optical security system using the SPJTC technique was investigated by developing numerical simulations, using the MATLAB software package, employing both binary images and gray levels and both noise-free and noisy images. Their results indicate that this method improves the quality of the decrypted images compared with conventional approaches, i.e., those presented in Subsection 3.2.1, without phase shifting [111]. Indeed, this approach permits elimination of the distortions induced in the decrypted image with satisfactory reproduction capability. However, the optical implementation of this setup remains complicated in practice and does not lead to an optimal use of the spatial bandwidth product at the input and the output planes.

3.5. Image Encryption Based on Fractional Fourier Transform

Other optical information security and image encryption methods based on the fractional FT were recently put forward by several authors [73,96,98,114–118]. The fractional FT has been extensively studied for its significant applications to digital image and image processing as well as optical information processing. It can be interpreted as the quadratic phase modulated near-field diffraction of light and hence is a powerful tool in optical information processing. To illustrate these methods, we spend some time presenting the technique of Liu and Liu [118]. Liu and Liu presented an algorithm to simultaneously encrypt two images into a single one as the amplitudes of fractional FTs with different orders. In addition, to increase their encryption rate, Liu *et al.* proposed to add some random phase keys associated with different target images (images to encrypt). In their scheme, Liu and Liu combine two initial images in the fractional Fourier do-

main. From the encrypted image together with its phase, two original images through fractional FT^{-1} with two different fractional orders α and β are obtained. Therefore, the phase corresponding to the encrypted image serves as the decryption key. Without knowing it, one cannot retrieve the secret image correctly. The numbers α and β can be considered the extra keys. Consequently, this image encryption scheme is free of the use of random phases.

The synoptic diagram of this method is illustrated in Fig. 19, while the iterative encryption algorithm is shown in Fig. 20. The notation is as follows: F^r denotes the fractional FT at order r , $A_1(x,y)$ and $A_2(x,y)$ are the two original target images, $A(x,y)$ is the encrypted image (which contains the encrypted information of the two target images) and φ_i is the phase function associated with each target image ($i=1$ or $i=2$). The two original images should satisfy the following relation: [118]

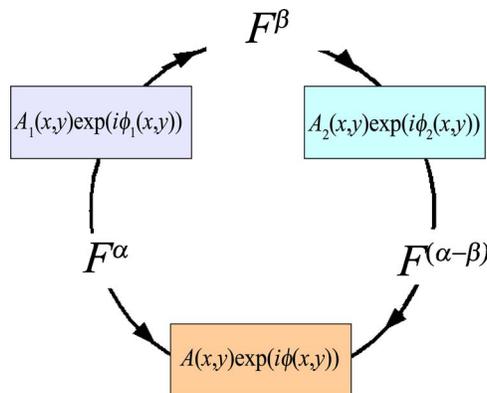
$$F^\alpha(A_1 \exp(i\varphi_1)) = F^\beta(A_2 \exp(i\varphi_2)). \quad (21)$$

To obtain the two phases φ_1 and φ_2 the iterative algorithm displayed in Fig. 20 should be used. In short, this algorithm consists in setting φ_1 to a fixed value, then finding the φ_2 that minimizes $\max(|A_2' - A_2|)$, where $A_2' \exp(i\varphi_2') = F^{\alpha-\beta}(A_1 \exp(i\varphi_1))$. It should be emphasized that this process is interesting because multiple-image encryption can be achieved by encoding multiple images in the fractional Fourier domains and the decryption processes can be multiplexed by different fractional orders. Thus, the encrypted image at the output plane contains all information relating to different target images, with the important consequence that the encryption rate will be increased. Numerical simulations have demonstrated the effectiveness of this image encryption scheme. However, the specific role of the different parameters on the degradation of the decrypted image quality and the convergence analysis, which was not considered in [118], need further investigation.

3.6. All-Optical Video-Image Encryption with Enforced Security Level Using Independent Component Analysis

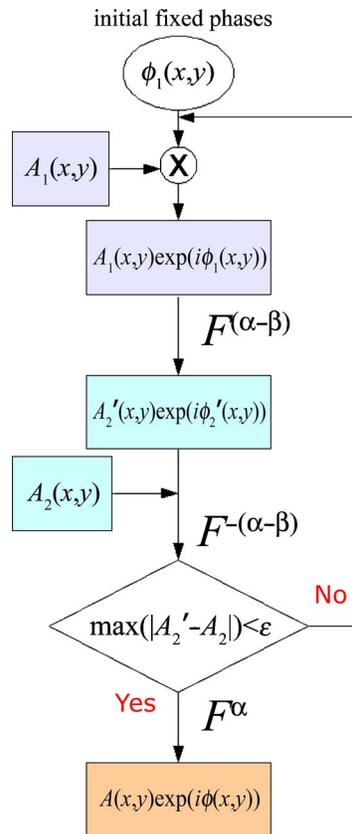
All-optical techniques mentioned above are used to secure information without worrying about securing the transmission channels. As an alternative, Alfalou

Figure 19



Synoptic diagram of the image encryption method based on the fractional FT [118].

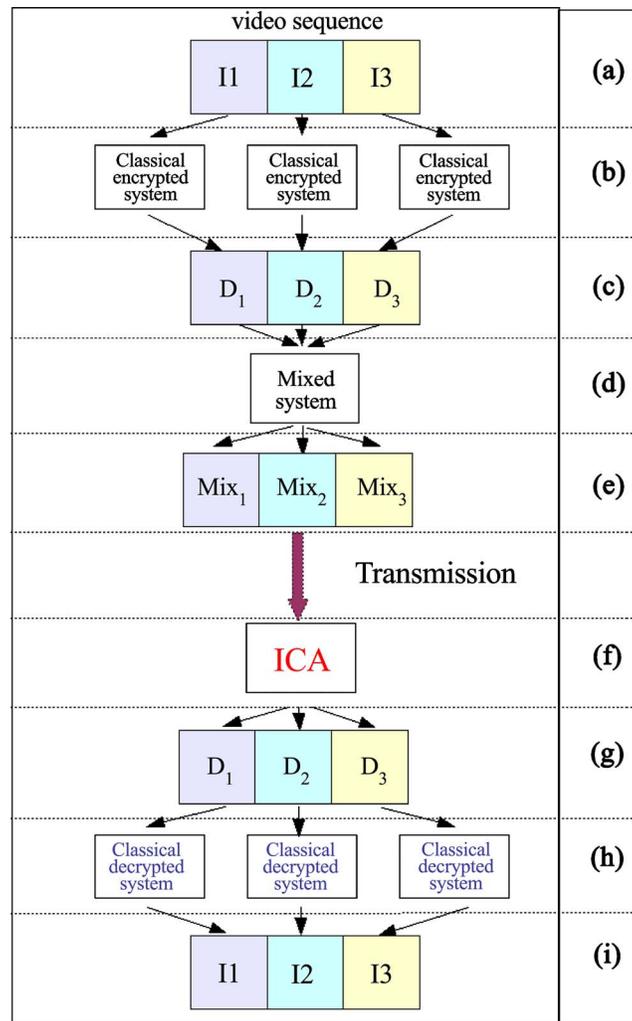
Figure 20



Flow chart of the iterative phase retrieval algorithm used in the image encryption scheme of Liu and Liu [118]. Two images are assigned to two complex functions $A_1 \exp(i\varphi_1)$ and $A_2 \exp(i\varphi_2)$ as the magnitudes, while one complex function is a fractional FT of another. F^r denotes the fractional FT at order r , A_1 and A_2 are the two original target images, A is the encrypted image, and φ_i is the phase function associated with each target image ($i=1, 2$).

and Mansour [119] suggested and validated an improvement of these optical techniques, allowing one to encrypt information and secure transmission channels simultaneously. For this purpose, Alfalou and Mansour developed an encryption scheme based on independent component analyses (ICA) [120–122]. To illustrate the principle of this technique [119] and to illustrate its ability to increase the encryption level, i.e., rendering attacks more and more complicated compared with conventional techniques, Alfalou and Mansour considered the encryption of a video sequence composed of three $N \times N$ pixel images [Fig. 21(a)]. The first step of this technique consists in separately encrypting the different images (I1, I2, I3) [with reference to Fig. 21(b)]. For this purpose, Alfalou and Mansour selected the optical technique presented in [23]. Basically, it consists in combining several encryption keys in the Fourier domain by using a segmentation technique developed previously by Alfalou and co-workers [10,11]. To validate their approach, they used sequences without compression, but the same steps can be applied to sequences with compression. Then, the different encrypted images are mixed together [Fig. 21(c)] by using a linear mixer ($\text{Mix}_1 = a_{11}D_1 + a_{12}D_2 + a_{13}D_3$, with D_1, D_2, D_3 being the three encrypted images

Figure 21



Enforced encryption–decryption system using the ICA technique.

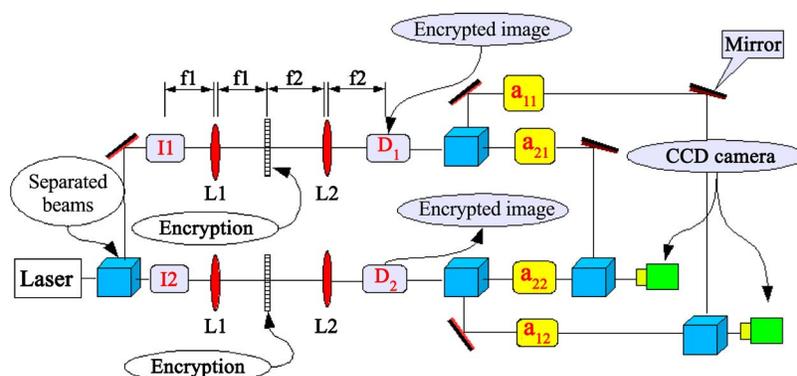
and a_{11} , a_{12} , and a_{13} denoting mixing parameters) [119]. This combination yields three other encrypted images. Thus, three doubly encrypted images are generated by using different keys and two different encryption methods, leading to an increase of the encryption level of these images [Fig. 21(d)]. A subsequent study by Alfalou and Mansour, using the standard DRP encryption system, showed the compatibility of the above technique with the DRP system [119]. Before sending these doubly encrypted images, taken as three matrices ($N \times N$ pixels each), and in order to increase the security level, they are converted into a large vector V_1 ($3 \times N^2$ pixels). Then, the order of the different pixels is changed by using a defined criterion: this criterion is being used as an additional encryption key. This vector is subsequently divided into three vectors V_{11} , V_{12} , V_{13} , which are sent separately by using three different channels [Fig. 21(e)]. Consequently, anyone who intercepts one, two, or all three vectors will not be able to trace the source and find the decrypted information. To decode the transmitted information, one must follow the inverse path with different encryption keys used by the sender to encrypt the sequence [Fig. 21(f)], and the ICA algorithm [123,124] to find the three mixed images. What is also notable is that Alfalou and Mansour [119] have proposed an optical implementation of their method based on

the use of a $4f$ setup (Fig. 22). For simplicity, a setup with two target images is shown. The laser beam is first divided by a separator cube. The two target images are separately encrypted and are multiplied by each other with some respective coefficients. The introduction of images and the coefficients in the optical setup are realized with optoelectronic interfaces, i.e., SLMs [125,126]. However, a successful implementation of the ICA method requires that the different images to be encrypted should be independent. This can be made possible thanks to the multiplication of different images by different random masks [127–129]. This multiplication is intended to standardize the image spectra and make them independent of one another even if they belong to the same video sequence. However, this technique, despite its good performance in terms of encryption, remains very difficult to implement optically. In addition, it suffers from a problem of convergence that is specific to ICA methods; i.e., all images must be independent of one another. But this is not generally the case in a video. Therefore this constraint requires the multiplication of the images with random functions in order to ensure independence [129]. It is interesting to observe that another problem occurs with such methods: the decrypted output images are not delivered in the same order as the input images. This requires an additional step that identifies the sequence of the different images in order to classify them in the correct order.

4. Optical Image Compression and Encryption Methods

As we have seen previously, the increasing interest in exchanging reliable, i.e., secure, information quickly, i.e., in compressed form, necessitates an intensive effort to compress and encrypt information. Although both operations are related to each other, they are often carried out separately. Alfalou and co-workers [130,131] suggested a scheme to carry out compression and encryption simultaneously based on a biometric key and DCT [27,53]. Their approach consists in taking advantage of standard optical compression and encryption methods, on the one hand, and, on the other hand, in using some powerful signal processing tools to secure the transmitted data by using independent transmitters. More specifically, these authors [130,131] used techniques of optical compression based

Figure 22

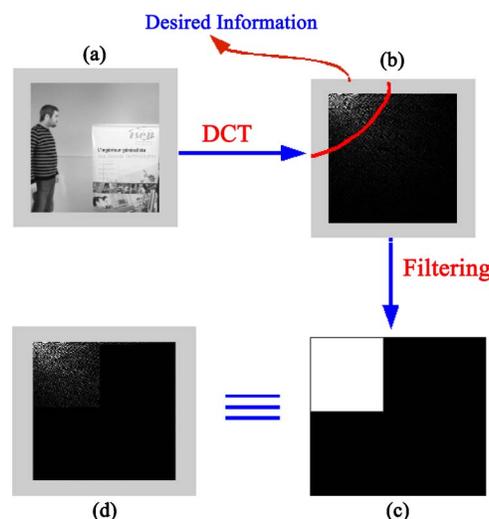


All-optical video-image encryption with enforced security level.

on FT [67,54,14,132]. The studies [130,131] demonstrated the possibility of multiplexing spectral information and realizing DCTs optically, two operations that can also be used to alter the spectral distribution of an image and in consequence to encrypt it. The important property of DCT to be emphasized here is its ability to group relevant information to rebuild an image in the top left-hand corner of its spectrum [Fig. 23].

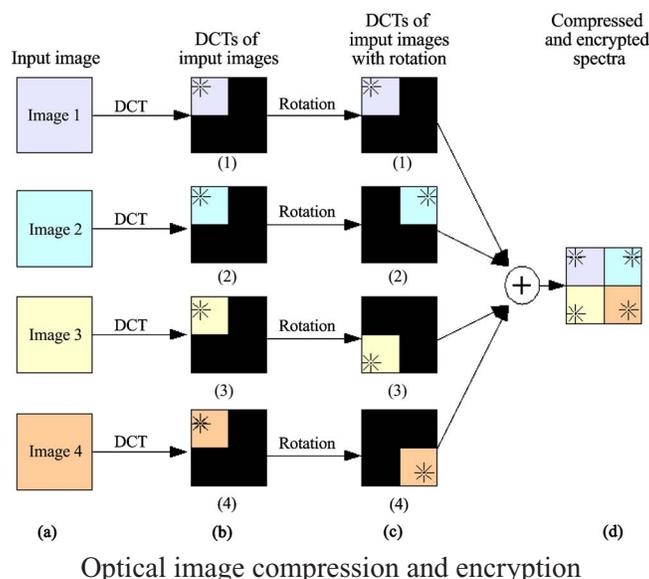
As in the JPEG method, Loussert and co-workers [131] used DCT to group relevant information in order to propose an optical approach of compression and encryption. The optical compression step requires a filtering operation after obtaining the image spectrum by using DCT [Fig. 24(b)]. After this filtering, a spectrum of size $(c \times c)$ pixels is obtained with $c \ll N$, N being the original size of the image in pixels [Fig. 23(a)]. This results in releasing a large part of the spectral plane. While regrouping these various spectra in a single plane in a non-destructive way, the compression and the multiplexing of the various images can be achieved [130,131]. The number of images that can be multiplexed together depends on the size of the spectra. One must keep in mind that it is necessary to find a balance between the desired quality and the size of spectrum to be filtered. This nondestructive regrouping has as its effect that it significantly changes the frequency distribution in the spectral plane. To ensure a good encryption level against any hacking attempt, Loussert and co-workers proposed to change the rotation of the frequencies of the various images before gathering them [Fig. 23(c)]. This ensures that whoever does not have the necessary information on the number of spectra and their distribution in the spectral plane will not be able to decrypt this information quickly [Fig. 23(d)]. Without the rotation of the image spectra, the shape of the spectra obtained with the DCT is easily detectable thanks to the amplitude, which decreases gradually while moving away from the top left-hand corner toward the bottom right-hand corner of the spectrum. This can be achieved by multiplying the spectra with a random mask, thus modifying the characteristic spectral distribution of the DCT [110]. The key-mask would

Figure 23



Regrouping and selection of information with a DCT: (a) image with several levels of gray (256,256) pixels, (b) its transformation into DCT, (c) low-pass filter, (d) the filtered spectrum containing the desired information.

Figure 24



be sent separately as a private encryption key. After applying this method and transmitting compressed and encrypted information, the extraction of the images after reception is done by repeating the various steps of the transmission method but in the reverse order. The received images are multiplied by the inverse of random mask, and rotations are applied in the opposite direction. Finally, the inverse DCT is performed to obtain the original images [131]. Validation tests of this principle need to be improved to measure the encryption rate and the compression ratio by using different images.

5. Summary and Perspectives

In this tutorial, we have presented several recent studies concerning optical compression and encryption applications. The main focus of this tutorial was on optical filtering methods. These methods have been used to find an object in a target scene, but they are not confined to this specific application. They can be used to filter redundant information in the spectral domain (for compression) and to modify the spectral distribution of given information (for encryption). It is worth mentioning again that the significance of these optical filtering methods lies in their ability to perform compression and encryption simultaneously in the spectral domain.

The first part of this tutorial was devoted to the presentation of several optical compression methods. Even if satisfactory results can be obtained by these methods, they remain below expectations. Indeed, they have been developed for some specific applications, e.g., the holography domain. Other methods have attempted to implement optical compression methods such as JPEG or JPEG2000, but they encountered a serious problem due to the complexity of the setup required for implementing them optically. Another issue concerns the poor quality of the decompressed images obtained as compared with digital ones. Moreover, the implementation of these optical compression methods causes some limita-

tions concerning the quality and quantity of information to be recorded. To solve this problem many studies have been performed to improve the quality of the reconstructed images [133–135]. Another limitation concerning these types of method is the need to use optoelectronic interfaces, i.e., SLMs, to display images and as filters.

In the second part of this tutorial, several optical encryption methods based on DRP were described. These methods have received special interest because of the simplicity of their principles. However, these techniques are characterized by a serious weakness against attacks. To overcome this problem several studies have been developed to improve the encryption rate. This led to an increase of the implementation complexity. There are significant limitations of these methods due to the use of optoelectronic interfaces. Generally speaking, optical implementations are based on a holographic set or on the $4f$ setup. The latter allows us to achieve two consecutive FTs and is operative in the spectral domain.

Although we hope to have provided a taste of some of the techniques and ideas of compression and encryption methods in this tutorial, our strategy has been to give only a few examples. For more on the compression techniques, we recommend [136–141]. For readers more interested in encryption techniques, we recommend [142–151]. For a deeper understanding and further applications of these ideas the interested reader is invited to consult the cited literature, which is a selection of what we found particularly useful. In closing, we can notice that the methods of encryption and compression have been developed separately, knowing that they are linked and influence each other. We strongly believe that mixed methods for simultaneous encryption and compression will be developed in the future to meet the needs of information technology. In addition, we feel that hybrid methods (optical–digital) need to be further developed for two reasons. On the one hand, they let us simplify problems associated with optical implementation, such as the need to use several SLMs, and the problem of alignment. On the other hand, they can increase compression and encryption rates. The potential developed here could be used in other interesting research directions, such as (i) encryption methods based on polarization [152,153] that allow encryption of images not only rapidly, but also at the source, (ii) multiplexing methods using the spatial coherence principle, permitting mathematical operations to be performed at the source without any preprocessing [154,155], and (iii) the Fresnel field [156].

Appendix A: Acronyms

DCT	=	Discrete cosine transform
DRP	=	Double random phase encryption system
FT, FT^{-1}	=	Fourier transform, inverse Fourier transform
II	=	Integral imaging
ICA	=	Independent component analyses
JPEG	=	Joint Photographic Experts Group
JPEG2000	=	Joint Photographic Experts Group 2000
JTC	=	Joint transform correlator
JPS	=	Joint power spectrum
MPEG	=	Motion Picture Experts Group
NRMS	=	Normalized root-mean-square error
PSI	=	Phase shifting interferometry

PSIDH = Phase shifting interferometry digital
holography
RGB = Red, green, and blue
RP = Random phase mask
SLM = Spatial light modulator
SPJTC = Shifted phase-encoded JTC
VLC = VanderLugt correlator

Acknowledgments

It is a pleasure to acknowledge insightful discussions with G. Keryer. We apologize for not mentioning other research here, either because of an oversight on our part or because we felt our understanding of it to be inadequate. We apologize also if we have misinterpreted anyone's research. Lab-STICC is Unité Mixte de Recherche CNRS 3192.

References

1. A. B. VanderLugt, "Signal detection by complex spatial filtering," *IEEE Trans. Inf. Theory* **IT-10**, 139–145 (1964).
2. J. W. Goodman, *Introduction to Fourier Optics* (McGraw-Hill, 1968).
3. J. L. Horner and P. D. Gianino, "Phase-only matched filtering," *Appl. Opt.* **23**, 812–816 (1984).
4. B. Javidi, S. F. Odeh, and Y. F. Chen, "Rotation and scale sensitivities of the binary phase-only filter." *Appl. Opt.* **65**, 233–238 (1988).
5. B. V. K. Vijaya Kumar and L. Hassebrook, "Performance measures for correlation filters," *Appl. Opt.* **29**, 2997–3006 (1990).
6. J. L. Horner, "Metrics for assessing pattern-recognition performance," *Appl. Opt.* **31**, 165–166 (1992).
7. J. L. de Bougrenet de la Tocnaye, E. Quémener, and Y. Pétilot, "Composite versus multichannel binary phase-only filtering," *Appl. Opt.* **36**, 6646–6653 (1997).
8. Y. Petillot, L. Guibert, and J. L. de Bougrenet de la Tocnaye, "Fingerprint recognition using a partially rotation invariant composite filter in a FLC JTC," *Opt. Commun.* **126**, 213–219 (1996).
9. B. V. K. V. Kumar, "Tutorial survey of composite filter designs for optical correlators," *Appl. Opt.* **31**, 4773–4801 (1992).
10. A. Alfalou, G. Keryer, and J. L. de Bougrenet de la Tocnaye, "Optical implementation of segmented composite filtering," *Appl. Opt.* **38**, 6129–6136 (1999).
11. A. Alfalou, M. Elbouz, and H. Hamam, "Segmented phase-only filter binarized with a new error diffusion approach," *J. Opt. A Pure Appl. Opt.* **7**, 183–191 (2005).
12. A. V. Oppenheim and J. S. Lim, "The importance of phase in signals," *Proc. IEEE* **69**, 529–541 (1981).
13. J. R. Fienup, "Reconstruction of an object from the modulus of its Fourier transform," *Opt. Lett.* **3**, 27–29 (1978).
14. Feature issue on Task Specific Sensing, *Appl. Opt.* **45**, 2857–3070 (2006).
15. M. Kessels, M. El Bouz-Alfalou, R. Pagan, and K. Heggarty, "Versatile stepper based maskless microlithography using a liquid crystal display for

- direct-write of binary and multi-level microstructures,” *J. Micro/Nanolith. MEMS MOEMS* **6** (2007).
16. C. Slinger, C. Cameron, and M. Stanley, “Computer-generated holography as a generic display technology,” *Computer* **38**, 46–53 (2005).
 17. C. Kohler, X. Schwab, and W. Osten, “Optimally tuned spatial light modulators for digital holography,” *Appl. Opt.* **45**, 960–967 (2006).
 18. M. Madec, J. B. Fasquel, W. Uhring, P. Joffre, and Y. Herve, “Optical implementation of the filtered backprojection algorithm,” *Opt. Eng.* **46**, 1–16 (2007).
 19. J. Porter, H. Queener, J. E. Lin, K. Thorn, and A. A. S. Awwal, *Adaptive Optics for Vision Science: Principles, Practices, Design, and Applications* (Wiley, 2006).
 20. B. Culshaw, A. G. Mignani, H. Bartelt, and L. R. Jaroszewicz, “Implementation of high-speed imaging polarimeter using a liquid crystal ferroelectric modulator,” *Proc. SPIE* **6189**, 618912 (2006).
 21. M. Madec, W. Uhring, J. B. Fasquel, P. Joffre, and Y. Hervé, “Compatibility of temporal multiplexed spatial light modulator with optical image processing,” *Opt. Commun.* **275**, 27–37 (2007).
 22. R. M. Turner, K. M. Johnson, and S. Serati, *High Speed Compact Optical Correlator Design and Implementation* (Cambridge Univ. Press, 1995).
 23. S. G. Batsell, J. F. Walkup, and T. F. Krile, *Design Issues in Optical Processing* (Cambridge Univ. Press, 1995).
 24. S. Coomber, C. Cameron, J. Hughes, D. Sheerin, C. Slinger, M. A. G. Smith, and M. Stanley, “Optically addressed spatial light modulators for replaying computer-generated holograms,” *Proc. SPIE* **4457**, 9–19 (2001).
 25. B. Landreth and G. Modde, “Gray scale response from optically addressed spatial light modulators incorporating surface-stabilized ferroelectric liquid crystals,” *Appl. Opt.* **31**, 3937–3944 (1992).
 26. H. Xu, A. B. Davey, T. D. Wilkinson, W. A. Crossland, J. Chapman, W. L. Duffy, and S. M. Kelly, “Comparison between pixelated-metal-mirrored and non-mirrored ferroelectric liquid crystal OASLM devices,” in *Proceedings of the 19th International Liquid Crystal Conference* (2004), pp. 527–536.
 27. H. Guitter, *La Compression des Images Numériques* (Hermes, 1995).
 28. 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).
 29. D. Gabor, “A new microscopic principle,” *Nature* **161**, 777–778 (1948).
 30. L. P. Yaroslavskii and N. S. Merzlyakov, *Methods of Digital Holography* (Izdatel’stvo Nauka, 1977), in Russian.
 31. E. Darakis and J. J. Soraghan, “Reconstruction domain compression of phase-shifting digital holograms,” *Appl. Opt.* **46**, 351–356 (2007).
 32. M. Burrows and D. J. Wheeler, “A block-sorting lossless data compression algorithm,” SRC Research Report (Digital Systems Research Center, May 10, 1994).
 33. E. Darakis and J. J. Soraghan, “Compression of interference patterns with application to phase-shifting digital holography,” *Appl. Opt.* **45**, 2437–2443 (2006).
 34. T. J. Naughton, Y. Frauel, O. Matoba, B. Javidi, and E. Tajahuerce, “Compression of digital holograms for three-dimensional video,” in *Three-Dimensional Television, Video, and Display Technologies*, B. Javidi and F. Okano, eds. (Springer-Verlag, 2002), pp. 273–295.

35. A. E. Shortt, T. J. Naughton, and B. Javidi, "Compression of digital holograms of three-dimensional objects using wavelets," *Opt. Express* **14**, 2625–2630 (2006).
36. E. Darakis and J. J. Soraghan, "Compression of phase-shifting digital holography interference patterns," *Proc. SPIE* **6187**, 61870Y (2006).
37. A. E. Shortt, T. J. Naughton, and B. Javidi, "Nonuniform quantization compression techniques for digital holograms of three-dimensional objects," *Proc. SPIE* **5557**, 30–41 (2004).
38. I. Yamaguchi and T. Zhang, "Phase-shifting digital holography," *Opt. Lett.* **22**, 1268–1270 (1997).
39. T. J. Naughton, Y. Frauel, B. Javidi, and E. Tajahuerce, "Compression of digital holograms for three-dimensional object reconstruction and recognition," *Appl. Opt.* **41**, 4124–4131 (2002).
40. B. Javidi and E. Tajahuerce, "Three-dimensional object recognition by use of digital holography," *Opt. Lett.* **25**, 610–612 (2000).
41. Y. Frauel, E. Tajahuerce, M. A. Castro, and B. Javidi, "Distortion-tolerant three-dimensional object recognition with digital holography," *Appl. Opt.* **40**, 3887–3893 (2001).
42. B. Javidi, "Nonlinear joint power spectrum based optical correlation," *Appl. Opt.* **28**, 2358–2367 (1989).
43. L. Guibert, G. Keryer, A. Servel, M. Attia, H. Mackenzie, P. Pellat-Finet, and J. L. de Bougrenet de la Tocnaye, "On-board optical joint transform correlator for real-time road sign recognition," *Opt. Eng.* **34**, 101–109 (1995).
44. D. A. Huffman, "A method for the construction of minimum redundancy codes," *Proc. IRE* **40**, 1098–1101 (1952).
45. J. Ziv and A. Lempel, "A universal algorithm for sequential data compression," *IEEE Trans. Inf. Theory* **IT-23**, 337–343 (1977).
46. T. A. Welch, "A technique for high performance data compression," *Computer* **17**, 8–19 (1984).
47. S. L. Wijaya, M. Savvides, and B. V. K. Vijaya Kumar, "Illumination-tolerant face verification of low-bit-rate JPEG2000 wavelet images with advanced correlation filters for handheld devices," *Appl. Opt.* **44**, 655–665 (2005).
48. L. Ding, Y. Yan, Q. Xue, and G. Jin, "Wavelet packet compression for volume holographic image recognition," *Opt. Commun.* **216**, 105–113 (2003).
49. T. J. Naughton, J. John B. McDonald, and B. Javidi, "Efficient compression of Fresnel fields for Internet transmission of three-dimensional images," *Appl. Opt.* **42**, 4758–4764 (2003).
50. B. Tavakoli, M. Daneshpanah, B. Javidi, and E. Watson, "Performance of 3D integral imaging with position uncertainty," *Opt. Express* **15**, 11889–11902 (2007).
51. S. Yeom, A. Stern, and B. Javidi, "Compression of 3D color integral images," *Opt. Express* **12**, 1632–1642 (2004).
52. V. Bhaskaran and K. Konstantinides, *Image and Video Compression Standards*, 2nd ed. (Kluwer Academic, 1997).
53. W. B. Pennebaker and J. L. Mitchell, *JPEG: Still Image Data Compression Standard* (Van Nostrand Reinhold, 1993).
54. A. Alkholidi, A. Alfalou, and H. Hamam, "A new approach for optical colored image compression using the JPEG standards," *Signal Process.* **87**, 569–583 (2007).
55. A. Alfalou and 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,” Proc. SPIE **5823**, 183–190 (2005).
56. A. Alkholidi, A. Cottour, A. Alfalou, H. Hamam, and G. Keryer, “Real-time optical 2D wavelet transform based on the JPEG2000 standards,” Eur. Phys. J. Appl. Phys. **44**, 261–272 (2008).
 57. R. K. Young, *Wavelet Theory and Its Applications* (Kluwer Academic, 1993).
 58. D. W. Robinson, “Automatic fringe analysis with a computer image processing system,” Appl. Opt. **22**, 2169–2176 (1983).
 59. K. Creath, “Phase shifting speckle interferometry,” Appl. Opt. **24**, 3053–3058 (1985).
 60. M. Takeda, H. Ina, and S. Kobayashi, “Fourier transform method of fringe pattern analysis for computer based topography and interferometry,” J. Opt. Soc. Am. **72**, 156–160 (1982).
 61. T. W. Ng and K. T. Ang, “Fourier-transform method of data compression and temporal fringe pattern analysis,” Appl. Opt. **44**, 7043–7049 (2005).
 62. J. M. Huntley and H. Saldner, “Temporal phase unwrapping algorithm for automated interferogram analysis,” Appl. Opt. **32**, 3047–3052 (1993).
 63. J. M. Kilpatrick, A. J. Moore, J. S. Barton, J. D. C. Jones, M. Reeves, and C. Buckberry, “Measurement of complex surface deformation by high-speed dynamic phase-stepped digital speckle pattern interferometry,” Opt. Lett. **25**, 1068–1070 (2000).
 64. T. E. Carlsson and A. Wei, “Phase evaluation of speckle patterns during continuous deformation by use of phase-shifting speckle interferometry,” Appl. Opt. **39**, 2628–2637 (2000).
 65. W. E. Smith and H. H. Barrett, “Radon transform and bandwidth compression,” Opt. Lett. **8**, 395–397 (1983).
 66. A. Boumezzough, A. Alfalou, and C. Collet, “Optical image compression based on filtering of the redundant information in Fourier domain with a segmented amplitude mask (SAM),” in *Proceedings of Complex Systems, Intelligence and Modern Technological Applications*, M. Rouff and M. Cot-saftis, eds (Society of Environmental Engineers, 2004), pp. 566–570.
 67. S. Soualmi, A. Alfalou, and H. Hamam, “Optical image compression based on segmentation of the Fourier plane: new approaches and critical analysis,” J. Opt. A Pure Appl. Opt. **9**, 73–80 (2007).
 68. A. Cottour, A. Alfalou, and H. Hamam, “Optical video image compression: a multiplexing method based on the spectral fusion of information,” in *3rd International Conference on Information and Communication Technologies: from Theory to Applications, 2008. ICTTA 2008* (IEEE, 2008), pp. 1–6.
 69. D. Coppersmith, “The Data Encryption Standard (DES) and its strength against attacks,” IBM J. Res. Dev. **38**, 243–250 (1994).
 70. R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM **20**, 120–126 (1978).
 71. P. Réfrégier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett. **20**, 767–769 (1995).
 72. F. Goudail, F. Bollaro, B. Javidi, and P. Réfrégier, “Influence of a perturbation in a double phase-encoding system,” J. Opt. Soc. Am. A **15**, 2629–2638 (1998).
 73. G. Unnikrishnan, J. Joseph, and K. Singh, “Optical encryption. by double-

- random phase encoding in the fractional Fourier domain,” *Opt. Lett.* **25**, 887–889 (2000).
74. S. Kishk and B. Javidi, “Information hiding technique with double phase encoding,” *Appl. Opt.* **41**, 5462–5470 (2002).
 75. J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, and R. Torroba, “Multiplexing encrypted data by using polarized light,” *Opt. Commun.* **260**, 109–112 (2006).
 76. L. G. Neto and Y. Sheng, “Optical implementation of image encryption using random phase encoding,” *Opt. Eng.* **35**, 2459–2463 (1996).
 77. N. Towghi, B. Javidi, and Z. Luo, “Fully phase encrypted image processor,” *J. Opt. Soc. Am. A* **16**, 1915–1927 (1999).
 78. G. Unnikrishnan and K. Singh, “Optical encryption using quadratic phase systems,” *Opt. Commun.* **193**, 51–67 (2001).
 79. B. Javidi and N. Takanori, “Securing information by use of digital holography,” *Opt. Lett.* **25**, 28–30 (2000).
 80. E. Tajahuerce and B. Javidi, “Encrypting three-dimensional information with digital holography,” *Appl. Opt.* **39**, 6595–6601 (2000).
 81. G. Situ and J. Zhang, “Double random-phase encoding in the Fresnel domain,” *Opt. Lett.* **29**, 1584–1586 (2004).
 82. O. Matoba and B. Javidi, “Encrypted optical memory system using three-dimensional keys in the Fresnel domain,” *Opt. Lett.* **24**, 762–764 (1999).
 83. R. Arizaga, R. Henao, and R. Torroba, “Fully digital encryption technique,” *Opt. Commun.* **221**, 43–47 (2003).
 84. Y. Guo, Q. Huang, J. Du, and Y. Zhang, “Decomposition storage of information based on computer-generated hologram interference and its application in optical image encryption,” *Appl. Opt.* **40**, 2860–2863 (2001).
 85. J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, and R. Torroba, “Multiple image encryption using an aperture-modulated optical system,” *Opt. Commun.* **261**, 29–33 (2006).
 86. O. Matoba and B. Javidi, “Encrypted optical storage with angular multiplexing,” *Appl. Opt.* **38**, 7288–7293 (1999).
 87. L. Cai, M. He, Q. Liu, and X. Yang, “Digital image encryption and watermarking by phase-shifting interferometry,” *Appl. Opt.* **43**, 3078–3084 (2004).
 88. M. He, L. Cai, Q. Liu, and X. Yang, “Phase-only encryption and watermarking based on phase-shifting interferometry,” *Appl. Opt.* **44**, 2600–2606 (2005).
 89. D. Abookasis, A. Batikoff, H. Famini, and J. Rosen, “Performance comparison of iterative algorithms for generating digital correlation holograms used in optical security systems,” *Appl. Opt.* **45**, 4617–4624 (2006).
 90. D. Abookasis, O. Arazi, J. Rosen, and B. Javidi, “Security optical systems based on a joint transform correlator with significant output images,” *Opt. Eng.* **40**, 1584–1589 (2001).
 91. T. Nomura and B. Javidi, “Optical encryption using a joint transform correlator architecture,” *Opt. Eng.* **39**, 2031–2035 (2000).
 92. T. Nomura, S. Mikan, Y. Morimoto, and B. Javidi, “Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator,” *Appl. Opt.* **42**, 1508–1514 (2003).
 93. D. Amaya, M. Tebaldi, R. Torroba, and N. Bolognini, “Digital color encryption using a multi-wavelength approach and a joint transform correlator,” *J. Opt. A Pure Appl. Opt.* **10**, 104031–104035 (2008).
 94. Z. Xin, Y. S. Wei, and X. Jian, “Affine cryptosystem of double-random-

- phase encryption based on the fractional Fourier transform,” *Appl. Opt.* **45**, 8434–8439 (2006).
95. Z. Liu and S. Liu, “Double image encryption based on iterative fractional Fourier transform,” *Opt. Commun.* **275**, 324–329 (2007).
 96. S. Liu, Q. Mi, and B. Zhu, “Optical image encryption with multistage and multichannel fractional Fourier-domain filtering,” *Opt. Lett.* **26**, 1242–1244 (2001).
 97. W. Xiaogang, Z. Daomu, and C. Linfei, “Image encryption based on extended fractional Fourier transform and digital holography technique,” *Opt. Commun.* **260**, 449–453 (2006).
 98. B. M. Hennelly and J. T. Sheridan, “Image encryption techniques based on fractional Fourier transform,” *Proc. SPIE* **5202**, 76–87 (2003).
 99. M. Joshi, Chandrashakher, and K. Singh, “Color image encryption and decryption for twin images in fractional Fourier domain,” *Opt. Commun.* **281**, 5713–5720 (2008).
 100. M. Z. He, L. Z. Cai, Q. Liu, X. C. Wang, and X. F. Meng, “Multiple image encryption and watermarking by random phase matching,” *Opt. Commun.* **247**, 29–37 (2005).
 101. X. F. Meng, L. Z. Cai, M. Z. He, G. Y. Dong, and X. X. Shen, “Cross-talk-free double-image encryption and watermarking with amplitude-phase separate modulations,” *J. Opt. A Pure Appl. Opt.* **7**, 624–631 (2005).
 102. O. Matoba and B. Javidi, “Optical retrieval of encrypted digital holograms for secure real-time display,” *Opt. Lett.* **27**, 321–323 (2002).
 103. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, “Resistance of the double random phase encryption against various attacks,” *Opt. Express* **15**, 10253–10265 (2007).
 104. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, “Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys,” *Opt. Lett.* **30**, 1644–1646 (2005).
 105. X. Peng, P. Zhang, H. Wei, and B. Yu, “Known-plaintext attack on optical encryption based on double random phase keys,” *Opt. Lett.* **31**, 1044–1046 (2006).
 106. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, “Multiple-encoding retrieval for optical security,” *Opt. Commun.* **276**, 231–236 (2007).
 107. C. S. Weaver and J. W. Goodman, “A technique for optically convolving two functions,” *Appl. Opt.* **5**, 1248–1249 (1966).
 108. L. Chen and D. Zhao, “Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms,” *Opt. Express* **14**, 8552–8560 (2006).
 109. M. Joshia, Chandrashakherb, and K. Singh, “Color image encryption and decryption using fractional Fourier transform,” *Opt. Commun.* **279**, 34–42 (2007).
 110. 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).
 111. M. Nazrul Islam and M. S. Alam, “Optical security system employing shifted phase-encoded joint transform correlation,” *Opt. Commun.* **281**, 248–254 (2008).
 112. M. R. Haider, M. Nazrul Islam, M. S. Alam, and J. F. Khan, “Shifted phase-encoded fringe-adjusted joint transform correlation for multiple target detection,” *Opt. Commun.* **248**, 69–88 (2005).

113. A. R. Alsamman and M. S. Alam, "Face recognition through pose estimation and fringe-adjusted joint transform correlation," *Opt. Eng.* **42**, 560–567 (2003).
114. B. Zhu, S. Liu, and Q. Ran, "Optical image encryption based on multifractional Fourier transforms," *Opt. Lett.* **25**, 1159–1161 (2000).
115. B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Opt. Lett.* **28**, 269–271 (2003).
116. B. Hennelly and J. T. Sheridan, "Image encryption and the fractional Fourier transform," *Optik (Stuttgart)* **114**, 251–265 (2003).
117. N. K. Nishchal, J. Joseph, and K. Singh, "Securing information using fractional Fourier transform in digital holography," *Opt. Commun.* **235**, 253–259 (2004).
118. Z. Liu, S. Liu, "Double image encryption based on iterative fractional Fourier transform," *Opt. Commun.* **275**, 324–329 (2007).
119. A. Alfalou and A. Mansour, "All-optical video-image encryption with enforced security level using independent component analysis," *J. Opt. A Pure Appl. Opt.* **9**, 787–796 (2007).
120. A. Hyvarinen and E. Oja, "Independent component analysis: algorithms and applications," *Neural Networks* **13**, 411–430 (2000).
121. A. Mansour and M. Kawamoto, "ICA papers classified according to their applications and performances," *IEICE Trans. Fundamentals* **E86-A**, 620–633 (2003).
122. P. Comon, "Independent component analysis, a new concept?," *Signal Process.* **36**, 287–314 (1994).
123. R. El Sawda, A. Alfalou, G. Keryer, and A. Assoum, "Image encryption and decryption by means of an optical phase mask," in *2nd Information and Communication Technologies, 2006. ICTTA '06 (IEEE, 2006)*, Vol. 1, pp. 1474–1477.
124. A. Alfalou and A. Mansour, "New Image Encryption Method Based on ICA," in *Proceedings of the 10th IAPR Conference on Machine Vision Applications*, J. Tajima, ed. (International Association for Pattern Recognition, 2007), pp. 16–18.
125. M. Madec, E. Hueber, W. Uhring, J. B. Fasquel, and Y. Hervé, "Procedures for SLM image quality improvement," in *Proceedings of the European Optical Society Annual Meeting*, Proceedings on CD (European Optical Society, 2008).
126. D. J. McKnight, K. M. Johnson, and R. A. Serati, "256 × 256 liquid-crystal-on-silicon spatial light modulator," *Appl. Opt.* **39**, 2775–2783 (1994).
127. A. Mansour, A. Kardec Barros, and N. Ohnishi, "Blind separation of sources: methods, assumptions and applications," *IEICE Trans. Fundamentals* **E83-A**, 1498–512 (2000).
128. C. Jutten and J. Herault, "Blind separation of sources, Part 1: an adaptive algorithm based on neuromimetic architecture," *Signal Process.* **24**, 1–10 (1991).
129. A. Mansour and A. Alfalou, "Performance indices of BSS for real-world applications," in *Proceedings of the 14th European Signal Processing Conference (EUSIPCO 2006)*, Proceedings on CD (EURASIP, 2006).
130. A. Alfalou, A. Loussert, A. Alkholidi, and R. El Sawda, "System for image compression and encryption by spectrum fusion in order to optimize image transmission," in *Future Generation Communication and Networking (FGCN 2007)* (IEEE Computer Society, 2007), vol. 1, pp. 590–593.
131. A. Loussert, A. Alfalou, R. El Sawda, and A. Alkholidi, "Enhanced system

- for image's compression and encryption by addition of biometric characteristics," *Int. J. Software Eng. Its Appl.* **2**, 111–118 (2008).
132. J. H. Reif and A. Yoshida, "Optical techniques for image compression," in *Data Compression Conference, 1992. DCC '92* (IEEE, 1992), pp. 32–40.
 133. I. Yamaguchi and T. Zhang, "Phase-shifting digital holography," *Opt. Lett.* **22**, 1268–1270 (1997).
 134. I. Yamaguchi, K. Yamamoto, G. A. Mills, and M. Yokota, "Image reconstruction only by phase data in phase-shifting digital holography," *Appl. Opt.* **45**, 975–983 (2006).
 135. G. A. Mills and I. Yamaguchi, "Effects of quantization in phase-shifting digital holography," *Appl. Opt.* **44**, 1216–1225 (2005).
 136. J. D. He and E. L. Dereniak, "Error-free image compression algorithm using classifying-sequencing techniques," *Appl. Opt.* **31**, 2554–2559 (1992).
 137. R. Shahnaz, J. F. Walkup, and T. F. Krile, "Image compression in signal-dependent noise," *Appl. Opt.* **38**, 5560–5567 (1999).
 138. F. Domingo and C. Saloma, "Image compression by vector quantization with noniterative derivation of a codebook: applications to video and confocal images," *Appl. Opt.* **38**, 3735–3744 (1999).
 139. A. Bilgin, G. Zweig, and M. W. Marcellin, "Three-dimensional image compression with integer wavelet transforms," *Appl. Opt.* **39**, 1799–1814 (2000).
 140. J. C. Dagher, M. W. Marcellin, and M. A. Neifeld, "Efficient storage and transmission of ladar imagery," *Appl. Opt.* **42**, 7023–7035 (2003).
 141. E. Darakis, T. J. Naughton, and J. J. Soraghan, "Compression defects in different reconstructions from phase-shifting digital holographic data," *Appl. Opt.* **46**, 4579–4586 (2007).
 142. Y. Li, K. Kreske, and J. Rosen, "Security and encryption optical systems based on a correlator with significant output images," *Appl. Opt.* **39**, 5295–5301 (2000).
 143. A. Zlotnik, Z. Zalevsky, and E. Marom, "Optical encryption by using a synthesized mutual intensity function," *Appl. Opt.* **43**, 3456–3465 (2004).
 144. D. Abookasis, O. Montal, O. Abramson, and J. Rosen, "Watermarks encrypted in a concealogram and deciphered by a modified joint-transform correlator," *Appl. Opt.* **44**, 3019–3023 (2005).
 145. H. T. Chang and C. L. Tsan, "Image watermarking by use of digital holography embedded in the discrete-cosine-transform domain," *Appl. Opt.* **44**, 6211–6219 (2005).
 146. U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," *Opt. Express* **14**, 3181–3186 (2006).
 147. R. Tao, Y. Xin, and Y. Yang, "Double image encryption based on random phase encoding in the fractional Fourier domain," *Opt. Express* **15**, 16067–16079 (2007).
 148. D. S. Monaghan, U. Gopinathan, T. J. Naughton, and J. T. Sheridan, "Key-space analysis of double random phase encryption technique," *Appl. Opt.* **46**, 6641–6647 (2007).
 149. S. Yuan, X. Zhou, D.-H. Li, and D.-F. Zhou, "Simultaneous transmission for an encrypted image and a double random-phase encryption key," *Appl. Opt.* **46**, 3747–3753 (2007).
 150. X. Wang and Y. Chen, "Securing information using digital optics," *J. Opt. A Pure Appl. Opt.* **9**, 152–155 (2007).
 151. M. Ragulskis, A. Aleksa, and L. Saunoriene, "Improved algorithm for im-

- age encryption based on stochastic geometric moiré and its application,” *Opt. Commun.* **273**, 370–378 (2007).
152. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, “Multiplexing encrypted data by using polarized light,” *Opt. Commun.* **260**, 109–112 (2006).
 153. U. Gopinathan, T. J. Naughton, and J. T. Sheridan, “Polarization encoding and multiplexing of two-dimensional signals: application to image encryption,” *Appl. Opt.* **45**, 5693–5700 (2006).
 154. E. H. Horache, “Optical multiplex correlation based in spatial coherent modulation for wide spectral sources: applications for pattern recognition,” Ph.D. thesis (University of Marne-La-Vallée, 2001).
 155. B.-E. Benkelfat, E. H. Horache, and Q. Zou, “Multiplex signal processing in optical pattern recognition,” in *Proceeding of Optics and Optoelectronics, Theory, Devices and Applications*, O. P. Nijhanram, A. K. Gupta, A. K. Musla, Kehar Singh, eds. (Narosa, 1999), pp. 84–87.
 156. T. J. Naughton, J. B. McDonald, and B. Javidi, “Efficient compression of Fresnel fields for Internet transmission of three-dimensional images,” *Appl. Opt.* **42**, 4758–4764 (2003).