Chapter 33
Optical Data Encryption

María Sagrario Millán García-Varela and Elisabet Pérez-Cabré

Supplements

WILEY-VCH Verlag GmbH & Co. KGaA

Optical and Digital Image Processing: Fundamentals and Applications, First Edition. Edited by Gabriel Cristóbal, Peter Schelkens, and Hugo Thienpont.

ISBN: 978-3-527-40956-3

Contents

Optical and Digital Image Processing: Fundamentals and Applications, First Edition. Edited by Gabriel Cristóbal, Peter Schelkens, and Hugo Thienpont.

ISBN: 978-3-527-40956-3

Chapter 33
Optical Data Encryption

Supplements

This annex complements Chapter 33. Figures and references are numbered with cardinals consecutive to those that appear in the main text.

33.2
Optical techniques in encryption algorithms (continued)

33.2.3
Resistance of DRPE against attacks (continued)

Recently, some additional possibilities to break the linearity of the technique and defence against plaintext attacks have been reported. Cheng et al. [44] introduce an undercover amplitude-modulating operation in the conventional DRPE technique. This operation acts as an additional key that enhances the security of the system. Rueda et al. [45] improve the security of the system by an efficient masking of the message with a chaotic signal. The RPMs of the DRPE are obtained using a nonlinear system in chaotic regime. An authorised end user can extract the message (primary image) using a synchronization procedure, thus allowing a continuous change of the encrypting and decryption keys. In [45], there is no need to send the decryption mask to the authorised user. Moreover, the encrypted image and the key construction data can be sent through public open channels at no risk.

33.2.5
Holographic memory (continued)

Several variants of this method have been proposed. In the angular multiplexing, the photorefractive crystal is used to record a number of holograms (encrypted functions) in the same volume by changing the angle

Optical and Digital Image Processing: Fundamentals and Applications, First Edition. Edited by Gabriel Cristóbal, Peter Schelkens, and Hugo Thienpont.

ISBN: 978-3-527-40956-3

of the plane wave reference beam [7]. The three-dimensional positions of the two RPMs in the Fresnel domain have been used as new keys for successful recovery of the original data in the encrypted optical memory system [19]. Similarly, the in-plane shifting of the second RPM to encrypt-decrypt multiples images have been proposed in [46]. By an appropriate repositioning of the RPM and together with the phase conjugation operation, each primary image can be recovered.

33.2.7
Fresnel domain (continued)

Encryption in the Fresnel domain has also been used to cipher multiple images in a single encrypted distribution. Situ and Zhang [29] proposed to encrypt multiple images by modifying the lensless system of Fig. 33.8. Two RPMs were used for encryption, one of them located at the input plane along with the primary image, and the other in a certain position of the Fresnel domain. The distribution corresponding to the RPMs and their location remained unchanged for all the images to be encrypted. As a key parameter for the encryption of a given image, an axial shift of the output plane is introduced (varying z_2 of Fig. 33.8). Finally, all the encrypted images were superposed in a single final ciphered distribution. Decryption of a given image is achieved by using the same setup but in the reverse direction. It is necessary to put the correct RPMs at their fixed locations, and axially shift the encrypted distribution to the correct position. The contribution of the other encrypted images becomes a cross-talk noise that will limit the multiplexing capacity of the system.

Following the idea of increasing the number of keys to achieve much higher security, two different methods of optical encryption and decryption using the Fresnel transform were analysed in Ref. [47]. The first proposal, named the random phase method, uses three random phase codes in different Fresnel domains. In addition to these phase codes, the Fresnel propagation distances as well as the illuminating light wavelength are the necessary keys for correct decryption. The second method proposed is dubbed the jigsaw method where three jigsaw transforms are applied in a number of Fresnel domains. Apart from the Fresnel propagation distances and the illuminating light wavelength, the jigsaw permutations are the keys used for decryption. Both methods require the use of holographic recording in the encryption/decryption process. Both methods were simulated using different numerical algorithms, and the different keys were investigated with respect to blind decryption.

Optical and Digital Image Processing: Fundamentals and Applications, First Edition. Edited by Gabriel Cristóbal, Peter Schelkens, and Hugo Thienpont.

ISBN: 978-3-527-40956-3

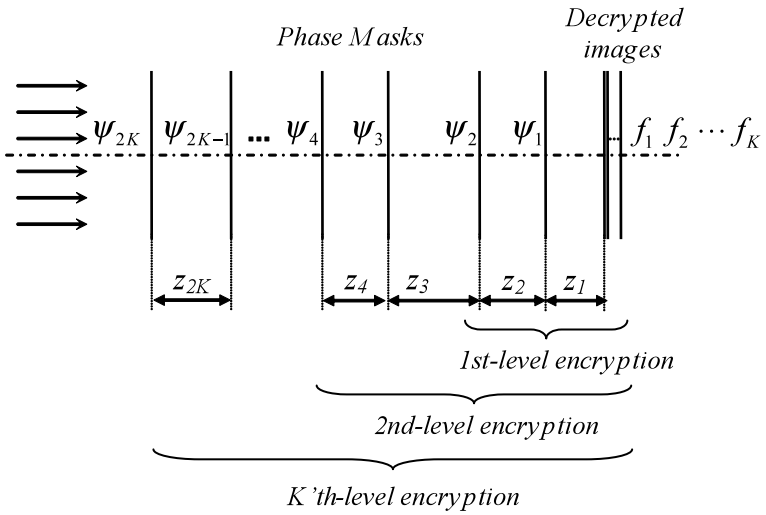


Figure 33.17 Hierarchical multiple-image encryption system in Fresnel domain.

Following the line of the work first proposed by Wang and collaborators [21] (Sect. 33.2.4 and Fig. 33.5), other contributions exist in the literature that extend their encryption method to the Fresnel domain. As an example, Meng and collaborators [31] proposed a different approach to encrypt a number of primary images by using phase masks in the Fresnel domain. They computed pairs of phase-only masks by iterative phase retrieval that permit to encrypt and afterwards decipher a given image. Following a hierarchical scheme (Fig. 33.17), the first couple of phase-only masks along with a second pair of computer phase-only masks, allow the authors to encrypt a second image. The position of each phase mask consist of a supplementary keys needed for the decryption step. Every additional image to be encrypted needs of a couple of phase-only masks that will be used simultaneously with the previous computed masks.

33.2.8
Fractional Fourier transforms (continued)

The technique of DRPE using FRFT has been widely developed introducing many variants. For instance, in [48] the encryption scheme uses the first RPM and a sequence of jigsaw and FRFT transforms. An optical encryption algorithm based on a more generalized FRFT operation, with periodicity extended beyond the four-integer order Fourier transforms, is developed in [49]. The primary image can be encrypted directly by this kind of generalized FRFT spectrum without the addition of RPMs. In [50] a

Optical and Digital Image Processing: Fundamentals and Applications, First Edition. Edited by Gabriel Cristóbal, Peter Schelkens, and Hugo Thienpont.

ISBN: 978-3-527-40956-3

method based on extended FRFT and digital holography is proposed. The method uses the interference with a wave from another RPM to store the encrypted data as a digital hologram. In all these proposals, the number and type of keys is modified in order to make the encryption-decryption processes more secure but without adding much more complexity than the prior methods in FRFT domain.

33.2.9 Phase-shifting interferometry

Primary images can be encrypted following a number of techniques, such those aforementioned in this chapter, and in most of the cases, the obtained ciphered data are fully complex with their corresponding magnitude and phase distributions. From a practical point of view, it is interesting to transform the complex information of the encrypted function into intensity variations that can be easily stored and transmitted via conventional digital communication channels.

One of the first contributions that introduces this approach was done by Tajahuerce and collaborators [51]. The authors adapt the digital phase-shifting interferometry technique to optically encrypt the Fraunhofer or Fresnel diffraction pattern of a primary image. A random-like intensity distribution is obtained in the CCD plane if a RPM is attached to the primary image in the object beam, and another RPM is located at a variable position in the reference beam of a Mach-Zehnder phase-shifting interferometer architecture (Fig. 33.18).

In a common phase-shifting interferometry approach, the phase and the magnitude distribution of the complex light field at the output plane can be obtained by recording four interferograms with different phase shifts. In the proposal, the phase shifting is accomplished by selecting the appropriate orientation of two retarder plates located in the path of the reference beam. Due to the presence of the RPMs, it is impossible to extract the complex amplitude distribution generated by the object beam, and hence to retrieve the primary image by just inverse Fourier transforming this last distribution.

The ciphered data are satisfactory decrypted only with the knowledge of the reference RPM and its three-dimensional position, which is acting as the key. Phase-shifting interferometry is again applied to obtain the key complex distribution generated by the reference beam. This information is needed to finally decipher the primary image.

Optical and Digital Image Processing: Fundamentals and Applications, First Edition. Edited by Gabriel Cristóbal, Peter Schelkens, and Hugo Thienpont.

ISBN: 978-3-527-40956-3

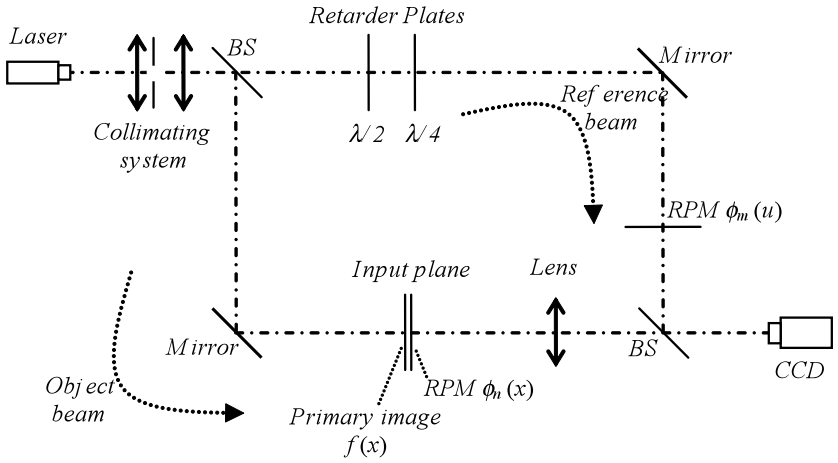


Figure 33.18 Phase-shifting interferometer used to encrypt the Fraunhofer diffraction pattern of a primary image.

In [52], the complex-amplitude encrypted information is registered by using a three-step phase-shifting interfometry. Authors use a phase-only distribution as a RPM, which is one of the keys used for decryption along with the correct geometric parameters, which are the RPM correct location and exact illuminating wavelength. Only when all these parameters are correct, the hidden image is retrieved by using a specific algorithm. To further secure the information data, the authors included a watermarking technique by adding some trivial images as fake information to confuse unauthorized receivers. Such images have little effect on the decrypted information as the authors proved in their work.

More recently, the combination of a two-step phase-shifting interferometry (it uses only two interferograms) with the DRPE technique in the Fresnel domain has been shown as another method for securing information [53].

33.2.10 Polarization

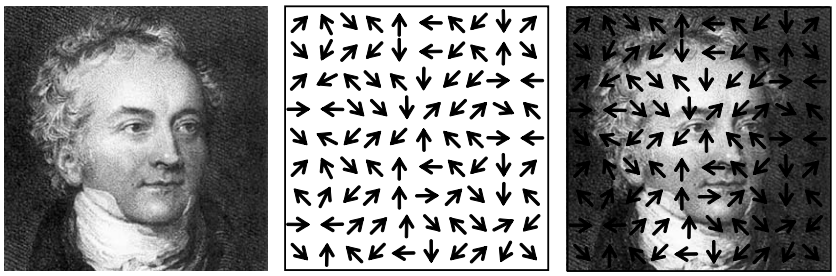
Quite early, the polarization state of the light was shown as another tool for securing information. Javidi and Nomura [54] proposed a random polarization encoded mask consisting of multiple linear polarizers randomly oriented (Fig. 33.19) to protect a piece of information without altering its

Optical and Digital Image Processing: Fundamentals and Applications, First Edition. Edited by Gabriel Cristóbal, Peter Schelkens, and Hugo Thienpont.

ISBN: 978-3-527-40956-3

visual perception. The polarization-encoded primary image was optically authenticated by correlating it with a known reference polarization mask.

Later on, polarization was introduced to hide information under an encrypted distribution, so that the primary image could not be noticed at a glance by human inspection. The basic idea was given by Han and co-workers [55] who took into consideration the performance characteristics of spatial light modulators regarding polarization. Since the encryption procedure is initially carried out by the exclusive-OR (XOR) operation (Fig. 33.20-a), it is necessary to consider binary data. Thus, the gray-level primary image is first converted into eight binary planes (corresponding to bit planes) for image encryption. Digital encryption algorithms are used to generate a binary key bit stream. Then, the optical XOR operations between the key bit stream and each bit plane of the primary image can be optically performed by using the properties of liquid crystals devices on the polarization of the light (Fig. 33.20-b). The resulting eight planes from each XOR operation are combined to produce the encrypted gray-level distribution. To retrieve the original primary image, the same number of XOR operations need to be performed between the key bit stream and the eight bit planes from the encrypted distribution. Two different contributions showed the experimental verification of the XOR encryption of binary images by using the polarization states provided by ferroelectric spatial light modulators [56] and twisted-nematic SLMs [57].



Primary image | *Polarization encoded mask* | *Polarization encoded image*

Figure 33.19 Example of a polarization encoded mask consisting of randomly oriented linear polarizers. The mask is superposed on the primary image. The resulting polarization-encoded image will have the same visual appearance as the original primary image.

Optical and Digital Image Processing: Fundamentals and Applications, First Edition. Edited by Gabriel Cristóbal, Peter Schelkens, and Hugo Thienpont.

ISBN: 978-3-527-40956-3

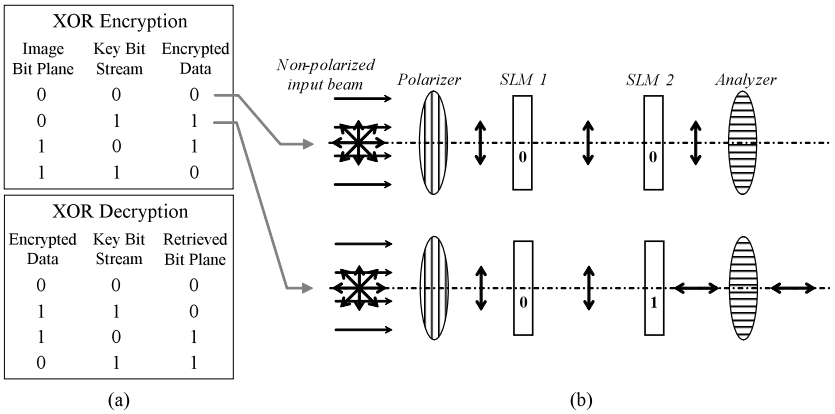


Figure 33.20 (a) XOR encryption and decryption using the same key bit stream. (b) Examples of optical XOR logic operation using two SLMs. In the each SLM, number "0" indicates a switch-off state whereas "1" corresponds to the switch-on state of the cell.

A different approach is considered in Ref. [58]. A diagram of the procedure is depicted in Fig. 33.21. A binary primary image is first encoded using two orthogonal linear polarization states. This distribution is multiplied in the input plane by a random polarization-modulation mask. This mask can rotate the direction of the principal axes of the elliptically polarized light and can change the phase retardation of each pixel. The resulting function has a random polarization distribution that does not give information of the original polarization state without knowing the mask. The encoded polarization distribution is stored in an optical storage material sensitive to the polarization state. The original primary image can be retrieved by using again the mask of the encryption step and by taking advantage of the phase-conjugation readout of the optical storage material. Otherwise, the reconstructed polarization state will be still scrambled. A polarizer in front of a CCD camera converts the polarization state information into the binary primary image.

Posteriorly, following a similar technique, Matoba and Javidi [59] extended the DRPE technique to the polarization domain. After expressing a binary primary image in terms of a polarization state instead of the amplitude modulation, they encrypted the information by using two polarization-modulation masks located at the input and Fourier planes. Each mask converts an input polarization state into an arbitrary elliptical polarization state. The use of the same masks permits recovering the original polarization state. Thus, after decryption, the binary primary image is retrieved by using a polarizer.

Optical and Digital Image Processing: Fundamentals and Applications, First Edition. Edited by Gabriel Cristóbal, Peter Schelkens, and Hugo Thienpont.

ISBN: 978-3-527-40956-3

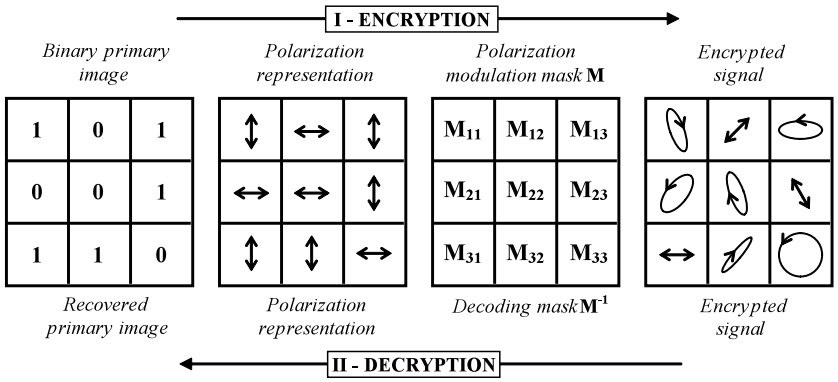


Figure 33.21 Steps for the polarization encryption and decryption techniques. Note that the polarization modulation mask M for encryption is inverted (M^{-1}) for the decryption process.

33.2.11
Compression of encrypted data

For pure-phase or pure-amplitude encrypted information it is reasonable to think that data can be easily stored electronically or transmitted over conventional communication channels. Complex-amplitude encrypted distributions can be recorded by digital holography, to obtain intensity patterns that would be also electronically delivered or transmitted. This motivates the study of how conventional compression techniques could be applied to these data and how they would affect the decrypted information.

In particular, Naughton and Javidi [60] presented the results of applying data compression techniques to encrypted three-dimensional objects. The objects are captured using phase-shift digital holography and encrypted using a RPM in the Fresnel domain. The authors analyse the effects of compression on encrypted digital holograms of 3-D objects. They reported that lossy compression techniques, such as quantization, permit important reduction on the amount of data and have resulted in good decompressed and decrypted 3-D object reconstruction (Fig. 33.22). However, if digital holograms are treated as binary data streams, lossless data compression techniques perform very poorly on encrypted digital holograms, mainly due to their white noise characteristics.

Optical and Digital Image Processing: Fundamentals and Applications, First Edition. Edited by Gabriel Cristóbal, Peter Schelkens, and Hugo Thienpont.

ISBN: 978-3-527-40956-3

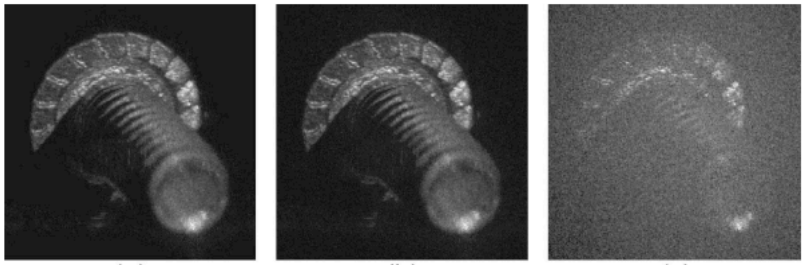


Figure 33.22 Decompressed and decrypted digital hologram of a 3-D object [60]. Quantization was applied as a lossy compression technique so that real and imaginary values of the hologram were recorded with: (a) 4 bits, (b) 3 bits and (c) 2 bits.

33.3
Applications to security systems (continued)

33.3.1
Optical techniques and DRPE in digital cryptography (continued)

For electronic mail exchanges, the public-key cryptosystem [35] preserves two important features of the ordinary postal mail system: messages are *private* and can be *signed*. To achieve these properties, two related keys are used to separate the ability of encryption from that of decryption. Each user of the public-key crytography places an encryption procedure E and a public key in a public database. The user keeps secret the details of the decryption algorithm D and its private key. There is no need to transmit a key in the process of transmitting secret information. The security in this system is based on the private key, so it cannot (at least in any reasonable amount of time) be calculated from the public data.

To assure privacy when, for instance, Bob sends a message M to Alice in a public-key cryptosystem, he will first cipher the message by using Alice public encryption method E_A, that will be $E_A(M)$, and he will send the resulting ciphertext to Alice. Only Alice will be able to decipher the message by using her decryption algorithm and private key, $D_A\left(E_A(M)\right) = M$. Any unauthorized user will not obtain the original message from Bob.

On the other hand, an electronic signature implies a more complex operation. To implement signatures with a public key cryptosystem, the procedure must be dependant on the message, as well as on the signer to

Optical and Digital Image Processing: Fundamentals and Applications, First Edition. Edited by Gabriel Cristóbal, Peter Schelkens, and Hugo Thienpont.

ISBN: 978-3-527-40956-3

prevent modification of the message itself while keeping the signature, or attaching a signature to a different message. In public key cryptography, Bob can send a signed message M to Alice by first computing his signature S for the message M using his secret decryption algorithm and private key. Thus, obtaining $S = D_B(M)$. Afterwards, he encrypts S using the Alice public encryption method and key, $E_A(S)$, and sends the result to Alice. Note, that there is no need for Bob to send M to Alice as well, because the message can be extracted from S. When Alice receives the ciphertext, she decrypts it with her private decryption method and key, $D_A(E_A(S)) = S$. Provided she knows the sender of the signature, she can decrypt the message with the encryption procedure of the sender, which is available on the public database. So, she obtains the original message $E_B(S) = M$. Hence, Alice possesses a message-signature pair (M, S) with similar properties of those of a signed paper document. Bob cannot later deny having sent Alice this message, since no one else could have created $S = D_B(M)$. Moreover, Alice clearly cannot modify the message M to a different version since she would have to create the corresponding signature using the secret decryption algorithm of Bob.

In comparison to cryptographic algorithms that use the same key for encryption and decryption, the public-key cryptosystem has been shown as very convenient for the management and assignment of keys.

Optical and Digital Image Processing: Fundamentals and Applications, First Edition. Edited by Gabriel Cristóbal, Peter Schelkens, and Hugo Thienpont.

ISBN: 978-3-527-40956-3

References

44. Cheng, et al. (2008) Security enhancement of double-random phase encryption by amplitude modulation. *Opt. Lett.,* **33**, 1575-7.
45. Rueda, E., et al. (2008) Synchronized chaotic phase masks for encrypting and decrypting images, *Opt. Commun.*, **281**, 5750-5.
46. Barrera, J. F., et al. (2006) Multiplexing encryption-decryption via lateral shifting of a random phase mask, *Opt. Commun.*, **259**, 532-6.
47. Hennelly, B. M. and Sheridan, J. T. (2004) Random phase and jigsaw encryption in the Fresnel domain, *Opt. Eng.*, **43**, 2239-49.
48. Hennelly, B. and Sheridan, J.T. (2003) Optical image encryption by random shifting in fractional Fourier domains, *Opt. Lett.*, **28**, 269-71.
49. Zu, B. et al. (2000) Optical image encryption based on multifractional Fourier transforms, *Opt. Lett.*, **25**, 1159-61.
50. Wang, X., et al. (2006) Image encryption based on extended fractional Fourier transform and digital holography technique, *Opt. Commun.*, **260**, 449-53.
51. Tajahuerce, E., et al. (2000) Optoelectronic information encryption with phase-shifting interferometry, *Appl. Opt.*, **39**, 2313-20.
52. Cai, L. Z., et al. (2004) Digital image encryption and watermarking by phase-shifting interferometry, *Appl. Opt.*, **43**, 3078-84.
53. Meng, X. F., et al. (2006) Two-step phase-shifting interferometry and its application in image encryption, *Opt. Lett.*, **31**, 1414-6.
54. Javidi, B. and Nomura, T. (2000) Polarization encoding for optical security systems, *Opt. Eng.*, **39**, 2439-43.
55. Han, J. W., et al. (1999) Optical image encryption based on XOR operations, *Opt. Eng.,* **38**, 47-54.
56 Unnikrishnan, G., et al. (2000) A polarization encoded optical encryption system using ferroelectric spatial light modulator, *Opt. Commun.*, **185**, 25-31.
57. Cheng, C. J. and Chen, M. L. (2004) Polarization encoding for optical encryption using twisted nematic liquid crystal spatial light modulators, *Opt. Commun.*, **237**, 45-52.
58. Tan, X., et al. (2001) Secure optical memory system with polarization encryption, *Appl. Opt.,* **40**, 2310-5.
59. Matoba, O. and Javidi, B. (2004) Secure holographic memory by double-random polarization encryption, *Appl. Opt.*, **43**, 2915-9.
60. Naughton, T. J. and Javidi, B. (2004) Compression of encrypted three-dimensional objects using digital holography, *Opt. Eng.*, **43**, 2233-8.

Optical and Digital Image Processing: Fundamentals and Applications, First Edition. Edited by Gabriel Cristóbal, Peter Schelkens, and Hugo Thienpont.

ISBN: 978-3-527-40956-3