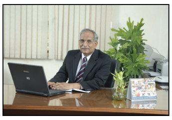
Optical Cryptosystems

Online at: https://doi.org/10.1088/978-0-7503-2220-1

IOP Series in Advances in Optics, Photonics and Optoelectronics

SERIES EDITOR



Professor Rajpal S Sirohi Consultant Scientist

About the Editor

Rajpal S Sirohi is currently working as a faculty member in the Department of Physics, Alabama A&M University, Huntsville, Alabama (USA). Prior to this, he was a consultant scientist at the Indian Institute of Science Bangalore, and before that he was chair professor in the Department of Physics, Tezpur University, Assam. During 2000–11, he was academic administrator, being vice chancellor to a couple of universities and the director of the Indian Institute of Technology Delhi. He is the recipient of many international and national awards and the author of more than 400 papers. Dr Sirohi is involved with research concerning optical metrology, optical instrumentation, holography, and speckle phenomenon.

About the series

Optics, photonics and optoelectronics are enabling technologies in many branches of science, engineering, medicine and agriculture. These technologies have reshaped our outlook, our way of interaction with each other and brought people closer. They help us to understand many phenomena better and provide a deeper insight in the functioning of nature. Further, these technologies themselves are evolving at a rapid rate. Their applications encompass very large spatial scales from nanometers to astronomical and a very large temporal range from picoseconds to billions of years. The series on the advances on optics, photonics and optoelectronics aims at covering topics that are of interest to both academia and industry. Some of the topics that the books in the series will cover include bio-photonics and medical imaging, devices, electromagnetics, fiber optics, information storage, instrumentation, light sources, CCD and CMOS imagers, metamaterials, optical metrology, optical networks, photovoltaics, freeform optics and its evaluation, singular optics, cryptography and sensors.

About IOP ebooks

The authors are encouraged to take advantage of the features made possible by electronic publication to enhance the reader experience through the use of colour, animation and video, and incorporating supplementary files in their work.

Do you have an idea of a book you'd like to explore?

For further information and details of submitting book proposals see iopscience.org/books or contact Ashley Gasque on Ashley.gasque@iop.org.

Optical Cryptosystems

Naveen K Nishchal
Department of Physics, Indian Institute of Technology Patna, Patna, Bihar, India

IOP Publishing, Bristol, UK

ISBN 978-0-7503-2220-1 (ebook)
ISBN 978-0-7503-2218-8 (print)
ISBN 978-0-7503-2221-8 (myPrint)
ISBN 978-0-7503-2219-5 (mobi)

DOI 10.1088/978-0-7503-2220-1

Version: 20191201

IOP ebooks

British Library Cataloguing-in-Publication Data: A catalogue record for this book is available from the British Library.

Published by IOP Publishing, wholly owned by The Institute of Physics, London

IOP Publishing, Temple Circus, Temple Way, Bristol, BS1 6HG, UK

US Office: IOP Publishing, Inc., 190 North Independence Mall West, Suite 601, Philadelphia, PA 19106, USA

असतो मा सदगमय ॥ तमसो मा ज्योतिर्गमय ॥ मृत्योर्मामृतम् गमय ॥

- बृहदारण्यक उपनिषद् 1.3.27

'Asato ma sadgamaya, Tamaso ma jyotirgamaya, Mrityorma amritamgamaya'

Oh Almighty! Lead us from the unreal (falsity) to the real (truth),
From darkness to light!
From death to immortality!
–Brihdaranyaka Upanisada 1:3:27 - India

अप्प दीपो भव।

"Appa Deepo Bhavah"
Be a Light unto Yourself.

Gautama Buddha

Dedicated to the memory of my parents
Shrimati Kamini Devi and Shri Balram Prasad Singh

Contents

Preface

In the digital era of contemporary society, information in any form, such as a message, text, data, image, audio, or video, can be treated as wealth. Therefore, securing information is as important as protecting property. In the history of the human race, the significance of security in one form or the other can easily be traced. Though cryptographic techniques have been in use for protecting information for thousands of years, the systematic study of cryptology as a science started around one hundred years ago. Julius Caesar (around 100 BC) was known to use a form of encryption to convey secret messages to his Army Generals. In modern times, digital techniques of information security are already in use wherein there exists scope for further improvements in terms of security level and computation cost.

Owing to the unique features of light, such as parallel processing, high speed, and several degrees of freedom, it is envisaged that information can be highly secured and communicated to the intended recipients or authentic users employing optical technologies. It can be foreseen that with the multifaceted uses of advanced technologies, such as *Artificial Intelligence*, *Big Data*, *Cloud Computing*, and *Internet-of-Things,* security will always remain an important challenge. Technologies provide several opportunities, but, at the same time, they also pose threats to information theft or misuse. Searching for a cyber expert or the attackers who attacked the digital algorithm would be very hard, because they can exist in large numbers anywhere in the world. On the other hand, finding out an attacker in the optics domain would be relatively easier. The security can be in terms of storage, in dissemination of the message, communication/transmission over conventional channels, protection of copyright/ownership, and steganography. Therefore, developments of newer alternative technologies are required to meet the challenges in the domains of scientific investigation.

This book intends to provide a collection of optical technologies for secure storage, secure communication, and the protection of copyright in terms of watermarking. Most of the optical techniques reported in literature can be traced around a double random phase encoding algorithm. Furthermore, many variants of this scheme have been proposed and demonstrated with improvements and different levels of complexity. This book aims to provide help to researchers in the field to get first-hand information of its progress.

This book starts with a general discussion on digital algorithms already in use in chapter 1 with more emphasis on the principles of optical techniques for image/data security in chapter 2. The growth of literature on optical technologies has been exponential with the publication of the first report in 1995. A bar chart has been provided that shows the growth of the literature. Use of fully-phased data provides additional security and robustness against noise, therefore such techniques have been dealt with in chapter 3. There is another aspect associated with security that is called authentication, in which the retrieval of original information is not intended. This can be solved with the use of an optical correlator, called a joint transform correlator, which is discussed in chapter 4. Optical techniques of watermarking and hiding are discussed in chapter 5. Polarization is one of the important properties of light, which is suited to developing a practical system because in this case the parameter that is dealt with is intensity, not the phase. Therefore, storage and transmission of intensity data is easier than phase-only information. This has been detailed in chapter 6.

Digital holography helps record 3D data and recording with digital sensors offers advantages in image/data security. The digital holograms can be stored in a personal computer and transmitted anywhere in the world and can be numerically reconstructed at any point of time. This has been discussed in chapter 7. Processing and security of multispectral data is very important in many applications, particularly in defence, remote sensing, and surveillance. This has been discussed in chapter 8. Chaos has always been very attractive in cryptographic studies in key design. Chapter 9 has been devoted to this topic, which has the ability to combine with other optical technologies. Phase retrieval techniques are important in regenerating object-dependent phase keys used for securing data. There are different algorithms reported in literature, which find use in image security. This has been dealt with in chapter 10.

No cryptographic technique can be considered very strong and useful unless cryptanalysis is carried out. There are several types of attacks reported in literature, which have been stated in terms of optical technologies in chapter 11. The optical technologies differ with digital counterparts, whereby in optical schemes either physical keys are used or keys are designed considering physical parameters as compared to digital keys used in electronic systems. There are various types of keys implemented in optical methods, which are discussed in chapter 12.

In all the chapters, the basic principles have been explained with examples. In some of the chapters, numerical simulation results have been provided for better understanding of the subject. Considering the requirement on some of the relevant topics, MATLAB codes have been provided. At the end of each chapter, a list of relevant literature has been provided.

The book is open to comments, criticisms, and suggestions from the readers in improving the quality of the book for future editions.

Acknowledgement

First of all, I would like to thank my mentors at the Indian Institute of Technology (IIT) Delhi during my doctoral studies. I especially thank my PhD supervisors, Professor Kehar Singh and Professor Joby Joseph, for introducing me to the exciting world of optical information processing research. Over the years they have been much more than just a thesis advisor to me. I am sure that they will be happy to see this book out in print. I must thank Dr G Unnikrishnan from IRDE Dehradun with whom I have had numerous discussions. I wish to extend my sincere thanks to Dr A K Gupta, Ex-Director IRDE Dehradun and Professor R S Sirohi, Ex-Director, IIT Delhi, for their encouragement.

My colleagues at IIT Patna deserve due acknowledgments for their encouragement. I acknowledge my gratitude to IIT Patna for providing facilities and a congenial environment. I must thank my colleagues from abroad, Professor Bahram Javidi, University of Connecticut; Professor John T Sheridan, University College Dublin; Professor Thomas J Naughton, Maynooth University; Professor Ayman AlFalou, ISEN/Yncrea; Professor Christian Brosseau, Universite Britagne Occidentale; Professor Cornelia Denz, Universitat Muenster; Professor Yan Zhang, Capital Normal University; Professor Takanori Nomura, Wakayama University; Professor Osamu Matoba, Kobe University; Professor Guohai Situ, Shanghai Institute of Optics and Fine Mechanics; and Professor Xiang Peng, Shenzhen University with whom I have had the opportunity to interact and learn the subject.

I must thank Elsevier, OSA, and SPIE for allowing me to reuse some of their diagrams/images published in various journals. Thanks are due to Jessica Fricchione, Poppy Emerson, and Sarah Armstrong from IOP Publishing, UK, for guiding me on many issues while preparing the manuscript.

I wish to extend my sincere thanks to all my students, Dr Sudheesh K Rajput, Dr Isha Mehra, Dr Dhirendra Kumar, Dr Areeba Fatima, Alok K Gupta, Avishek Kumar, Praveen Kumar, and Yatish. My continuous interactions with them have led me to a deeper understanding of the subject. They helped me in preparing this manuscript and drawing some of the difficult diagrams.

Finally, I owe a lot to my family—particularly to my wife Rinki and my son Anvit for allowing me to spend long hours in preparing this manuscript and for their support throughout. I also thank my other family members in appreciation of their patience, encouragement, and constant support while this manuscript was being prepared.

Author biography

Naveen Kumar Nishchal

Dr Naveen Kumar Nishchal is an associate professor in the Department of Physics at the Indian Institute of Technology (IIT) Patna. He joined IIT Patna in December 2008. Dr Nishchal received his PhD degree in physics from IIT Delhi in 2005. He joined Instruments Research and Development Establishment, Dehradun, under Defence Research and Development Organisation, as a Scientist 'C' in July 2004 and worked until June 2007. Subsequently, he moved to IIT Guwahati and worked as an assistant professor in the Department of Physics from June 2007 to November 2008. He has been a visiting researcher to the Oulu Southern Institute, University of Oulu, Finland. His research interests include optical information processing, image encryption, watermarking, digital holography, interferometry, correlation-based optical pattern recognition, and fractional Fourier transform-based signal processing. Dr Nishchal is a senior member of OSA, SPIE, and life member of the Optical Society of India. He is a life member of Indian Science Congress Association, and Lasers and Spectroscopy Society of India. He has authored or co-authored 60 peer-reviewed international journal papers, two book chapters, and 150 papers in various conferences/seminars/symposia.

List of acronyms

AES	Advanced encryption standard
AT	Amplitude-truncated
BE	Beam expander
BR	Bacteriorhodopsin film
BS	Beam splitter
CC	Cross-correlation
CCA	Chosen-ciphertext attack
CCD	Charge-coupled device camera
CGH	Computer generated hologram
CMOS	Complementary metal-oxide semiconductor
COA	Ciphertext-only attack
CPA	Chosen-plaintext attack
CS	Compressive sensing
CT	Computed tomography
1D	One-dimensional
2D	Two-dimensional
3D	Three-dimensional
DCT	Discrete cosine transform
DES	Data encryption standard
DH	Digital holography
DOE	Diffractive optical element
DRPE	Double random phase encoding
DWT	Discrete wavelet transform
EFJPS	Encrypted fractional joint power spectrum
EMD	Equal modulus decomposition
ERA	Error reduction algorithm
FT	Fourier transform
FFT	Fast Fourier transform
FRT	Fractional Fourier transform
FrT	Fresnel transform
FWT	Fractional wavelet transform
GSA	Gerchberg–Saxton algorithm
GT	Gyrator transform
GWT	Gyrator wavelet transform
HIOA	Hybrid input–output algorithm
HM	Holographic mask
HOE	Holographic optical element
HT	Hartley transform
HWP	Half wave plate
IDEA	International data encryption algorithm
IFT	Inverse Fourier transform
JPS	Joint power spectrum
JTC	Joint transform correlator
KPA	Known-plaintext attack
LC	Liquid crystal
LCT	Linear canonical transform
LCTV	Liquid crystal television
LED	Light-emitting diode

MATLAB	Matrix laboratory
MEMS	Micro-electro-mechanical systems
MO	Microscope objective
MGSA	Modified Gerchberg–Saxton algorithm
MRI	Magnetic resonance imaging
MSE	Mean square error
MZI	Mach–Zehnder interferometer
NIST	National Institute of Standards and Technology
NPCR	Number of pixel change rate
OAC	Optical asymmetric cryptosystem
OD	Optical device
PCE	Peak-to-correlation energy
PCF	Phase contrast filter
PCI	Photon counting imaging
PD	Plastic diffuser
PI	Peak intensity
PK	Private key
POCSA	Projection-onto constraints sets algorithm
POF	Phase-only function
POM	Phase-only mask
PPM	Plasmonic phase mask
PRA	Phase retrieval algorithm
PRX	Photorefractive crystal
PSDOE	Polarization selective diffractive optical element
PSI	Phase-shifting interferometry
PSNR	Peak signal-to-noise ratio
PSR	Peak-to-sidelobe ratio
PT	Phase-truncated
PTFT	Phase-truncated Fourier transform
QPS	Quadratic phase system
QR	Quick response code
QWP	Quarter wave plate
RAM	Random amplitude mask
RE	Relative error
RGB	Red, green, blue
RP	Retardation plate
RPM	Random phase mask
RSAA	Rivest, Shamir, Adleman algorithm
SAA	Simulated annealing algorithm
SC	Symmetric cryptosystems
SHA	Secure hash algorithm
SLM	Spatial light modulator
SNR	Signal-to-noise ratio
SPM	Structured phase mask
SSE	Sum squared error
SWG	Subwavelength grating
UACI	Unified average change in intensity
VAR	Variance
VLC	VanderLugt correlator
WT	Wavelet transform
XOR	Exclusive OR

IOP Publishing

Optical Cryptosystems

Naveen K Nishchal

Chapter 1

Digital techniques of data and image encryption

1.1 Introduction

Information security is of paramount importance in today's digitally connected world. This is also called the *digital era*, in which the encryption is being considered as a fast-moving trend. Though advanced modern information security tools, storage, and retrieval mechanisms have been developed there are still enormous challenges posed by hacking tools, unsecure transmission channels, and ubiquity of the Internet. Therefore, there has been a rise in cyber security challenges globally, hence the users must be cyber prepared. Cyber security is impacting the industry. With the advent of advanced technologies such as *Internet-of-Things*, *Cloud Computing*, and *Artificial Intelligence*, it is envisaged that billions of devices would be connected. While such technologies provide several opportunities, they also pose threats to information security. Today most of the global web traffic is encrypted and it is expected that in future almost all the global web traffic will be fully encrypted. While this has enabled much greater privacy and helped prevent data breaches, cyber criminals are using these encrypted channels to propagate malware and exfiltrate data knowing that they can bypass traditional security inspection solutions that do not decrypt traffic [1–4].

The art and science of concealing information/data is called cryptography. The information/data/message to be concealed is called a plaintext (clear text) and the concealed form of message is called a ciphertext (encrypted text). In other words, cryptography is a process of converting plaintext into ciphertext and vice versa. The process of conversion from plaintext to ciphertext is called ***encryption*** and the reverse process that retrieves plaintext from ciphertext is called ***decryption***. The ciphertext is a message that cannot be understood by anyone or is a meaningless message. A cipher is an algorithm used for encryption and decryption. The ciphertext is stored and transmitted to the intended user. The cryptography is not only used for protecting the information from theft or alteration but it is also used for user authentication [5–7].

doi:10.1088/978-0-7503-2220-1ch1

A cryptosystem, also referred to as a cipher system, is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. Though cryptographic techniques have been in use for protecting information for thousands of years, the systematic study of cryptology as a science started around one hundred years ago. Therefore, cryptology is considered as a young science. Julius Caesar (around 100 BC) was known to use a form of encryption to convey secret messages to his Army Generals. The substitution cipher, known as the Caesar cipher is probably the most mentioned historic cipher in academic literature [3]. In this method, each character of a plaintext is substituted by another character to form the ciphertext. The variant used by Caesar was a shift by three ciphers. Each character was shifted by three places, so the character ‘A’ was replaced by ‘D’ and character ‘B’ was replaced by ‘E’ and so on. The characters would wrap around at the end, so character ‘X’ would be replaced by ‘A’. An example of the character substitution based on Caesar’s algorithm has been shown in figure 1.1.

Figure 1.2 shows the schematic of the modern encryption-decryption process. A plaintext is converted into a ciphertext through the encryption process, which upon use of correct keys returns the decrypted plaintext [4].

A basic cryptosystem has the following components [5]:

- Plaintext
- Encryption algorithm
- Ciphertext
- Decryption algorithm
- Encryption key
- Decryption key.

Figure 1.1. Example of character substitution based on Caesar’s algorithm.

Figure 1.2. Encryption-decryption process.

A plaintext is converted into a ciphertext by applying the encryption algorithm and encryption key. The key space is a string of different keys that can be used to break the algorithm. It is generally accepted that a secure algorithm should use a key with length greater than 100 bits, because the number of bit permutation operations required to try 2^{100} keys is considered to be computationally infeasible for a conventional digital computing technique. A secure encryption algorithm is extremely sensitive to its keys. Various encryption algorithms have been developed and are being practiced. A ciphertext returns the plaintext only after use of the appropriate decryption algorithm and correct decryption key. A slight change to the keys would result in different ciphers. Thus for the successful retrieval of the plaintext, use of the correct decryption key and appropriate decryption algorithm is a must. In different types of cryptosystems, different encryption and decryption algorithms are used and correspondingly different encryption and decryption keys are generated.

While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking a secure communication. The professionals involved in the process are called cryptanalysts. They are also called attackers. Attackers always wish to get the access of the encryption-decryption key so that plaintext can be retrieved. In classical cryptanalysis, several things are involved in the process, such as the interesting combination of analytical reasoning, the application of mathematical tools, pattern finding, patience, determination, and luck. With the passage of time, newer and reliable cryptosystems have been developed. On the other hand, attackers have also been creating improved logic to analyze the process to access the data. The pace of the development of information security technology is characterized by the creation of new methods and means of protection in the context of the storage, processing, and transmission of information. To date, much attention has been paid to the development of newer methods of intellectualization of various automated systems.

The cryptology embraces both cryptography and cryptanalysis. The cryptography can provide the following services [6].

- **Confidentiality (secrecy)**: it ensures that no one can read the concealed message except the authentic receiver. The data is kept secret from those who do not have proper credentials, even if that the data travels through an insecure medium.
- **Integrity (anti-tampering)**: it is assured that the authentic receiver has received message and it has not been altered in any way from the original.
- **Authentication**: it helps establish identity for authentication purposes. Actually, the process proves one’s identity.
- **Non-repudiation**: it is a mechanism to prove that the sender really sent this message. Neither the sender nor the receiver can deny the transmission of the message.
- **Access control**: it requires that the access to information resources may be controlled by or for the authentic system.
- **Availability**: it requires that the system assets be available to authorized personnel, as and when needed.

1.2 Types of cryptography

Depending on the common uses, cryptography can be classified into two categories; *symmetric key cryptography* and *asymmetric key cryptography*. Symmetric key cryptography is a classical encryption method. It is referred to as a situation in which the key used for encryption is as used for decryption. In this case, key distribution must be performed prior to data transfer. Therefore, the security key plays a highly significant role because security directly depends on the nature of the key. Asymmetric key cryptography is an advanced encryption method. It is referred to as a situation in which the key used for encryption is different than the key used for decryption. In this case, a pair of keys, public and private keys, are used. The security is very high compared to the classical method of encryption.

Of late, hash functions are also considered as a type of cryptography, which establishes the authenticity of the user [7].

1.2.1 Symmetric key cryptography

Symmetric key cryptography, also known as secret key cryptography or conventional cryptography, refers to an encryption system in which the sender and receiver share a single common key that is used to encrypt and decrypt the message. The process is shown in figure 1.3. The used algorithm is known as the symmetric algorithm or secret key algorithm. The key is defined as a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher. The key used for encrypting and decrypting a message has to be known to all the authentic recipients or else the message could not be decrypted by conventional means [6]. The examples of symmetric key cryptography are discussed below.

- **Data encryption standard (DES)**: the DES was published in 1977 by the US National Bureau of Standards. It uses a 56-bit key and maps a 64-bit input block of plaintext onto a 64-bit output block of ciphertext. 56 bits is a rather small key for today's computing power.
- **Triple DES**: it is an improved version created after overcoming the shortcomings of DES. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES. It has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break the DES.
- **Advanced encryption standard (AES)**: the AES is an encryption standard adopted by the US Government. The standard comprises three block ciphers, AES-128, AES-192, and AES-256. Each AES cipher has a 128-bit block size with key sizes of 128, 192, and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide.

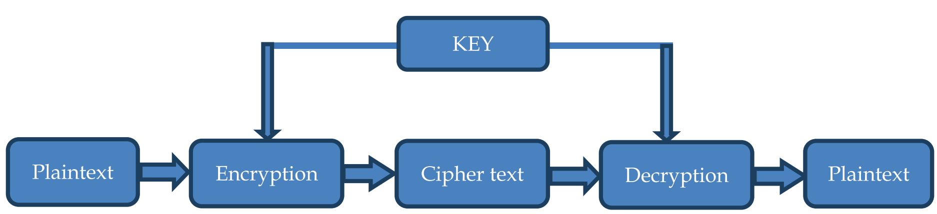


Figure 1.3. Symmetric key cryptography.

- **International data encryption algorithm (IDEA)**: the IDEA was developed in 1991. It uses a 128-bit key to encrypt a 64-bit block of plaintext into a 64-bit block of ciphertext. IDEA's general structure is very similar to DES. It performs 17 rounds, each round taking 64 bits of input to produce a 64-bit output, using per-round keys generated from the 128-bit key.

Key management in symmetric key systems

The symmetric key systems are simpler and faster but their main drawback is that the two parties must somehow exchange the key in a secure way and keep it secure after that. The key management caused a nightmare for the parties using the symmetric key cryptography. The worry was about how to get the keys safely and securely across all users so that the decryption of the message would be possible. This gave the chance for third parties to intercept the keys in transit to decode the secret messages. Thus, if the key was compromised, the entire coding system was compromised and a 'secret' would no longer remain a 'secret'.

1.2.2 Asymmetric key cryptography

Asymmetric key cryptography is also known as public key cryptography. It refers to a cryptographic algorithm which requires two separate keys, one of which is private and another is public. The public key is used to encrypt the message and the private one is used to decrypt the message. This method was developed to address the key management issue of symmetric key cryptography. The process of asymmetric cryptography is shown in figure 1.4. It is a very advanced form of cryptography. Officially, it was invented by Whitfield Diffie and Martin Hellman in 1975. The basic technique of public key cryptography was first discovered in 1973 by the British Clifford Cocks of Communications-Electronics Security Group but this was a secret until 1997. The examples of symmetric key cryptography are discussed below [6].

- **Digital signature standard (DSS)**: the DSS is a digital signature algorithm developed by the US National Security Agency to generate a digital signature for the authentication of electronic documents. DSS was put forth by the National Institute of Standards and Technology (NIST) in 1994.
- **RSA**: (Rivest, Shamir, and Adleman who first publicly described it in 1977) It is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic

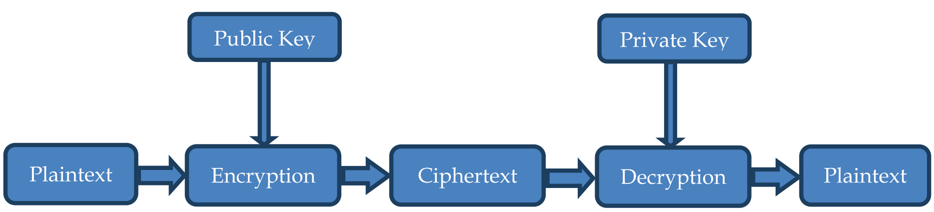


Figure 1.4. Asymmetric key cryptography.

commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

- **ElGamal**: ElGamal is a public key method. It is used in both encryption and digital signing. The encryption algorithm is similar in nature to the Diffie–Hellman key agreement protocol and is used in many applications and uses discrete logarithms. ElGamal encryption is used in the free GNU Privacy Guard software.

1.2.3 Hash functions

A cryptographic hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic hash value such that any (accidental or intentional) change to the data will (with very high probability) change the hash value [7]. The data to be encoded is often called the message, and the hash values are sometimes called the message digest or simply digest. The ideal cryptographic hash function has four main properties:

- It is easy to compute the hash value for any given message.
- It is infeasible to generate a message that has a given hash.
- It is infeasible to modify a message without changing the hash.
- It is infeasible to find two different messages with the same hash.

The examples of hash functions are discussed below.

- **Secure hash algorithm (SHA)**: SHA hash functions are a set of cryptographic hash functions designed by the National Security Agency and published by the NIST as a US Federal Information Processing Standard. Because of the successful attacks on MD5, SHA-0 and theoretical attacks on SHA-1, NIST perceived a need for an alternative, dissimilar cryptographic hash, which became SHA-3. In October 2012, the NIST chose the Keccak algorithm as the new SHA-3 standard.

As multimedia, image, and video are becoming increasingly part of modern economy and social companions, ensuring security from malicious interference, theft, and unauthorized use has become the demand of the hour. Encryption of images is one of the well-known mechanisms to preserve confidentiality of images/data over a reliable unrestricted public media, which is vulnerable to attacks. The image encryption algorithms can be classified into frequency-domain and spatial-domain algorithms. Both are able to protect the data/image with a high level of security. Their output encrypted images are either texture-like or noise-like images. From a security point of view, it is an obvious visual sign indicating the presence of an encrypted image that may contain some important information. It is apprehended that this will attract people's attention and can result in a significantly large number of attacks and analysis. The solution has been reported in the form that the original image is transformed into visually meaningful encrypted images. This is because people generally consider these images as normal images rather than encrypted ones.

Securing data/image is important in all the domains including medical diagnosis. There is a fear that patients' computed tomography (CT) and medical resonance imaging (MRI) scan results can easily be changed by hackers, thereby deceiving radiologists and artificial intelligence algorithms that diagnose malignant tumors. The hackers could access to add or remove medical conditions from the scans for the purpose of insurance fraud, ransom, and even homicide. A large number of techniques have been proposed in literature to date, each have an edge over the other, to catch up to the ever-growing need of security. The focus has been devising a mechanism for image encryption that should have the following characteristics.

• **Low correlation**	The value of correlation between the original and the encrypted image should be as low as possible. Ideally its value should be zero.
• **Large key space**	The key size should be very large since the more the key space, the higher the brute force search time would be.
• **Key sensitivity**	The image encryption algorithm should have high key sensitivity. In other words, a slight change in the key value should change the encrypted image significantly.
• **Entropy**	It is a measure of the degree of randomness or disorder. As the level of disorder rises, the entropy rises, and events become less predictable. The minimum entropy value should be zero and it happens when the image pixel value is constant in any location. The maximum value of entropy for an image depends on the number of gray scales. For an image with 256 gray scales, the maximum entropy is log 2(256) = 8. The maximum value happens when all bins of the histogram have the same constant value, or, image intensity is uniformly distributed in [0,255].
Low time complexity	Usually, an encryption algorithm with high computational time is not recommended for practical applications. Therefore, an image encryption algorithm should have low time complexity.

The technology for information security using digital methods is being enhanced by applying more powerful algorithms. Longer key lengths are chosen such that current computers using the best cipher-cracking algorithms would require an unreasonable amount of time to break the key. When encryption key length becomes longer, the processing speed of digital techniques goes down. In order to counter the processing speed and security problem, in 1995 a new technology was proposed that used physical keys employing the principles of classical optics. Owing to the speed of light, it is envisaged that data can be secured at unparalleled speed along with parallel processing. Additionally, optics offers several degrees of freedom that could help encode information more securely [8–14]. Also, there is a natural match between optical processing for optical communications.

With the belief that cryptology based on the optics principle would provide a more complex environment and would be more resistant as compared to purely digital techniques, developing optical cryptosystems have gained much emphasis [13, 14]. Since 1995, a large number of research articles have appeared with so many different techniques. These topics are discussed in detail in the following chapters.

References

[1] Al Falou A (ed) 2018 *Advanced Secure Image Processing for Communications* (Bristol: IOP Publishing)

[2] Ramakrishnan S (ed) 2018 *Cryptographic and Information Security Approaches for Images and Videos* (Boca Raton, FL: CRC Press)

[3] Vacca J R (ed) 2017 *Computer and Information Security Handbook* 3rd edn (Amsterdam: Elsevier)

[4] Pfleeger C P, Pfleeger S L and Margulies J 2018 *Security in Computing* 5th edn (Noida: Pearson India)

[5] Beckett B 1988 *Introduction to Cryptology* (Oxford: Blackwell)

[6] Stallings W 2000 *Cryptography and Network Security; Principles and Practice* 2nd edn (Hoboken, NJ: Prentice Hall)

[7] van Tilborg H C A 2000 *Fundamentals of Cryptology* (Boston, MA: Kluwer)

[8] Naughton T J and Sheridan J 2005 Optics in information systems *SPIE Int. Tech. Gr. Newsletter* **16** 1–12

[9] Javidi B (ed) 2005 *Optical and Digital Techniques for Information Security* (Berlin: Springer)

[10] Javidi B (ed) 2006 *Optical Imaging Sensors and Systems for Homeland Security Applications* (New York: Springer)

[11] Alfalou A and Brosseau C 2009 Optical image compression and encryption methods *Adv. Opt. Photon* **1** 589–636

[12] Chen W, Javidi B and Chen X 2014 Advances in optical security systems *Adv. Opt. Photon* **6** 120–55

[13] Javidi B *et al* 2016 Roadmap on optical security *J. Opt.* **18** 083001

[14] Muniraj I and Sheridan J T 2019 *Optical Encryption and Decryption* (Bellingham, WA: SPIE Press)

Full list of references

Chapter 1

[1] Al Falou A (ed) 2018 *Advanced Secure Image Processing for Communications* (Bristol: IOP Publishing)

[2] Ramakrishnan S (ed) 2018 *Cryptographic and Information Security Approaches for Images and Videos* (Boca Raton, FL: CRC Press)

[3] Vacca J R (ed) 2017 *Computer and Information Security Handbook* 3rd edn (Amsterdam: Elsevier)

[4] Pfleeger C P, Pfleeger S L and Margulies J 2018 *Security in Computing* 5th edn (Noida: Pearson India)

[5] Beckett B 1988 *Introduction to Cryptology* (Oxford: Blackwell)

[6] Stallings W 2000 *Cryptography and Network Security; Principles and Practice* 2nd edn (Hoboken, NJ: Prentice Hall)

[7] van Tilborg H C A 2000 *Fundamentals of Cryptology* (Boston, MA: Kluwer)

[8] Naughton T J and Sheridan J 2005 Optics in information systems *SPIE Int. Tech. Gr. Newsletter* **16** 1–12

[9] Javidi B (ed) 2005 *Optical and Digital Techniques for Information Security* (Berlin: Springer)

[10] Javidi B (ed) 2006 *Optical Imaging Sensors and Systems for Homeland Security Applications* (New York: Springer)

[11] Alfalou A and Brosseau C 2009 Optical image compression and encryption methods *Adv. Opt. Photon* **1** 589–636

[12] Chen W, Javidi B and Chen X 2014 Advances in optical security systems *Adv. Opt. Photon* **6** 120–55

[13] Javidi B *et al* 2016 Roadmap on optical security *J. Opt.* **18** 083001

[14] Muniraj I and Sheridan J T 2019 *Optical Encryption and Decryption* (Bellingham, WA: SPIE Press)

Chapter 2

[1] Refregier P and Javidi B 1995 Optical image encryption using input plane and Fourier plane random encoding *Proc. SPIE* **2565** 62–8

[2] Refregier P and Javidi B 1995 Optical image encryption based on input plane encoding and Fourier plane random encoding *Opt. Lett.* **20** 767–9

[3] Javidi B and Ahouzi E 1998 Optical security system with Fourier plane encoding *Appl. Opt.* **3** 6247–55

[4] Goodman J W 2007 *Introduction to Fourier Optics* 3rd edn (New Delhi: Viva Books)

[5] Alfalou A and Brosseau C 2009 Optical image compression and encryption methods *Adv. Opt. Photon.* **1** 589–636

[6] Liu S, Guo C and Sheridan J T 2014 A review of optical image encryption techniques *Opt. Laser Technol.* **57** 327–42

[7] Chen W, Javidi B and Chen X 2014 Advances in optical security systems *Adv. Opt. Phot.* **6** 120–55

[8] Javidi B *et al* 2016 Roadmap on optical security *J. Opt.* **18** 083001

[9] Javidi B and Horner J L 1994 Optical pattern recognition for validation and security verification *Opt. Eng.* **33** 1752–6

[10] Healy J J, Kutay M A, Ozaktas H M and Sheridan J T (ed) 2015 *Linear Canonical Transform: Theory and Applications* (Berlin: Springer)
[11] Unnikrishnan G, Joseph J and Singh K 1998 Optical encryption system that uses phase conjugation in a photorefractive crystal *Appl. Opt.* **37** 8181–5
[12] Lohmann A W 1993 Image rotation, Wigner rotation, and the fractional Fourier transform *J. Opt. Soc. Am.* A **10** 2181–6
[13] Ozaktas H M, Arikan O, Kutay M A and Bozdagi G 1996 Digital computation of the fractional Fourier transform *IEEE Trans. Signal Process.* **44** 2141–50
[14] Garcia J, Mas D and Dorsch R G 1996 Fractional Fourier transform calculation through the fast Fourier transform algorithm *Appl. Opt.* **35** 7013–8
[15] Khan G S, Nishchal N K, Jospeh J and Singh K 2001 Fractional Fourier transform and its applications: a bibliographic review *Asian J. Phys.* **10** 251–99
[16] Ozaktas H M, Zalevsky Z and Kutay M A 2001 *The Fractional Fourier Transform with Applications in Optics and Signal Processing* (Chichester: Wiley)
[17] Unnikrishnan G and Singh K 2000 Double random fractional Fourier-domain encoding for optical security *Opt. Eng.* **39** 2853–9
[18] Unnikrishnan G, Joseph J and Singh K 2000 Optical encryption by double-random phase encoding in the fractional Fourier domain *Opt. Lett.* **25** 887–9
[19] Unnikrishnan G, Joseph J and Singh K 2001 Fractional Fourier domain encrypted holographic memory by use of an anamorphic optical system *Appl. Opt.* **40** 299–306
[20] Unnikrishnan G and Singh K 2001 Optical encryption using quadratic phase systems *Opt. Commun.* **193** 51–67
[21] Hua J, Liu L and Li G 1997 Extended fractional Fourier transforms *J. Opt. Soc. Am.* A **14** 3316–22
[22] Nishchal N K, Joseph J and Singh K 2003 Optical encryption using cascaded extended fractional Fourier transform *Opt. Memory Neural Net.* **12** 139–45
[23] Situ G and Zhang J 2004 Double random phase encoding in the Fresnel domain *Opt. Lett.* **29** 1584–6
[24] Shi Y, Situ G and Zhang J 2007 Multiple-image hiding in the Fresnel domain *Opt. Lett.* **32** 1914–6
[25] Rodrigo J A, Alieva T and Calvo M L 2006 Optical system design for orthosymplectic transformations in phase space *J. Opt. Soc. Am.* A **23** 2494–500
[26] Rodrigo J A, Alieva T and Calvo M L 2007 Applications of gyrator transform for image processing *Opt. Commun.* **278** 279–84
[27] Singh H, Yadav A K, Vashisth S and Singh K 2014 Fully phase image encryption using double random-structured phase masks in gyrator domain *Appl. Opt.* **53** 6472–81
[28] Mallat S 2008 *A Wavelet Tour of Signal Processing* 3rd edn (New York: Academic)
[29] Chen L and Zhao D 2005 Optical image encryption based on fractional wavelet transform *Opt. Commun.* **254** 361–7
[30] Vilardy J M, Useche J, Torres C O and Mattos L 2011 Image encryption using the fractional wavelet transform *J. Phys.: Conf. Ser.* **274** 012047
[31] Mehra I and Nishchal N K 2014 Image fusion using wavelet transform and its application to asymmetric cryptosystem and hiding *Opt. Express* **22** 5474–82
[32] Mehra I and Nishchal N K 2015 Wavelet-based image fusion for securing multiple images through asymmetric keys *Opt. Commun.* **335** 153–60

[33] Mehra I and Nishchal N K 2015 Optical asymmetric image encryption using gyrator wavelet transform *Opt. Commun.* **354** 344–52
[34] Mehra I, Fatima A and Nishchal N K 2018 Gyrator wavelet transform *IET Image Process* **12** 432–7
[35] Zhou N, Wang Y and Gong L 2011 Novel optical image encryption scheme based on fractional Mellin transform *Opt. Commun.* **284** 3234–42
[36] Meng X F, Cai L Z, Yang X L, Xu X F, Dong G Y, Shen X X, Zhang H and Wang Y R 2007 Digital color image watermarking based on phase-shifting interferometry and neighboring pixel value subtraction algorithm in the discrete-cosine-transform domain *Appl. Opt.* **46** 4694–701
[37] Singh P, Yadav A K and Singh K 2017 Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition *Opt. Lasers Eng.* **91** 187–95

Chapter 3

[1] Longhurst R S 1986 *Geometrical and Physical Optics* 3rd edn (London: Orient Longman)
[2] Zernike F 1955 How I discovered phase contrast *Science* **121** 345–9
[3] Naughton T J 2010 Phase in optical image processing *AIP Confer. Proc.* **1236** 235–40
[4] Neto L G 1998 Implementation of image encryption using the phase-contrast technique *Proc. SPIE* **3386** 284–90
[5] Towghi N, Javidi B and Luo Z 1999 Fully phase encrypted image processor *J. Opt. Soc. Am.* A **16** 1915–27
[6] Tan X, Matoba O, Shimura T, Kuroda K and Javidi B 2000 Secure optical storage that uses fully phase encryption *Appl. Opt.* **39** 6689–94
[7] Javidi B, Towghi N, Maghzi N and Verrall S C 2000 Error reduction techniques and error analysis for fully phase and amplitude based encryption *Appl. Opt.* **39** 4117–30
[8] Goodman J W 2007 *Introduction to Fourier Optics* 3rd edn (New Delhi: Viva Books)
[9] Gluckstad J 1996 Phase contrast image synthesis *Opt. Commun.* **130** 225–30
[10] Unnikrishnan G, Joseph J and Singh K 1998 Optical encryption system that uses phase conjugation in a photorefractive crystal *Appl. Opt.* **37** 8181–5
[11] Vorontsov M A, Justh E W and Beresnev L A 2001 Adaptive optics with advanced phase contrast techniques I. High-resolution wave front sensing *J. Opt. Soc. Am.* A **18** 1289–99
[12] Castillo M D I, Sanchez-de-la-Llave D, Garcia R R, Olivos-Perez L I, Gonzalez L A and Rodriguez-Ortiz M 2001 Real-time self-induced nonlinear optical Zernike type filter in a bacteriorhodopsin film *Opt. Eng.* **40** 2367–8
[13] Mogensen P C and Gluckstad J 2000 Phase-only optical encryption *Opt. Lett.* **25** 566–8
[14] Mogensen P C and Gluckstad J 2001 Phase-only optical decryption of a fixed mask *Appl. Opt.* **40** 1226–35
[15] Mogensen P C and Gluckstad J 2000 A phase image optical encryption system with polarization encoding *Opt. Commun.* **173** 177–83
[16] Seo D H and Kim S J 2003 Interferometric phase-only optical encryption system that uses a reference wave *Opt. Lett.* **28** 304–6
[17] Nishchal N K, Joseph J and Singh K 2003 Fully phase encryption by phase contrast using electrically addressed spatial light modulator *Opt. Commun.* **217** 117–22
[18] Nishchal N K, Joseph J and Singh K 2003 Fully phase encryption using fractional Fourier transform *Opt. Eng.* **42** 1583–8

[19] Nishchal N K, Joseph J and Singh K 2004 Fully phase-based encryption using fractional order Fourier domain random phase encoding: error analysis *Opt. Eng.* **43** 2266–73
[20] Nishchal N K, Joseph J and Singh K 2004 Fully phase encrypted memory using cascaded extended fractional Fourier transform *Opt. Lasers Eng.* **42** 141–51
[21] Liu J, Xu J, Zhang G and Liu S 1995 Phase contrast using photorefractive $LiNbO_3$:Fe crystals *Appl. Opt.* **34** 4972–5

Chapter 4

[1] VanderLugt A B 1964 Signal detection by complex filters *IEEE Trans. Inf. Theory* **10** 139–45
[2] Weaver C S and Goodman J W 1966 Techniques for optically convolving two functions *Appl. Opt.* **5** 1248–9
[3] Javidi B and Horner J L 1994 Optical pattern recognition for validation and security verification *Opt. Eng.* **33** 1752–6
[4] Javidi B and Wang J 1996 Position-invariant two-dimensional image correlation using a one-dimensional space integrating optical processor: application to security verification *Opt. Eng.* **35** 2479–86
[5] Brasher J D and Johnson E G 1997 Incoherent optical correlators and phase encoding of identification codes for access control or authentication *Opt. Eng.* **36** 2409–16
[6] Weber D and Trolinger J 1999 Novel implementation of nonlinear joint transform correlators in optical security and validation *Opt. Eng.* **38** 62–8
[7] Nomura T and Javidi B 2000 Optical encryption using joint transform correlator architecture *Opt. Eng.* **39** 2031–5
[8] Li Y, Kreske K and Rosen J 2000 Security and encryption optical systems based on a correlator with significant output images *Appl. Opt.* **39** 5295–301
[9] Abookasis D, Arazi O, Rosen J and Javidi B 2001 Security optical systems based on joint transform correlator with significant output images *Opt. Eng.* **40** 1584–9
[10] Park S J, Kim J Y, Bae J K and Kim S J 2001 Fourier plane encryption technique based on removing the effect of phase terms in a joint transform correlator *Opt. Rev.* **18** 413–5
[11] Nomura T, Mikan S, Morimoto Y and Javidi B 2003 Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator *Appl. Opt.* **42** 1508–14
[12] Lin L C and Cheng C J 2005 Optimal key mask designs for optical encryption based on joint transform correlator architecture *Opt. Commun.* **285** 144–54
[13] Mela C L and Iemmi C 2006 Optical encryption using phase-shifting interferometry in a joint transform correlator *Opt. Lett.* **31** 2562–4
[14] Vilardy J M, Millán M S and Pérez-Cabré E 2014 Nonlinear optical security system based on a joint transform correlator in the Fresnel domain *Appl. Opt.* **53** 1674–82
[15] Rajput S K and Nishchal N K 2014 An optical encryption and authentication scheme using asymmetric keys *J. Opt. Soc. Am.* A **31** 1233–8
[16] Chang H T and Chen C C 2006 Fully phase asymmetric image verification system based on joint transform correlator *Opt. Express* **14** 1458–67
[17] Amaya D, Tebaldi M, Torroba R and Bolognini N 2008 Multichanneled encryption via a joint transform correlator architecture *Appl. Opt.* **47** 5903–7
[18] Amaya D, Tebaldi M, Torroba R and Bolognini N 2008 Digital color encryption using a multiwavelength approach and a joint transform correlator *J. Opt. A: Pure Appl. Opt.* **10** 104031

[19] Amaya D, Tebaldi M, Torroba R and Bolognini N 2009 Wavelength multiplexing encryption using joint transform correlator architecture *Appl. Opt.* **48** 2099–104
[20] Barrera J F, Vargas C, Tebaldi M, Torroba R and Bologini N 2010 Known plaintext attack on a joint transform correlator encrypting system *Opt. Lett.* **35** 3553–5
[21] Barrera J F, Vargas C, Tebaldi M and Torroba R 2010 Chosen plaintext attack on a joint transform correlator encrypting system *Opt. Commun.* **283** 3917–21
[22] Qin W, Peng X and Meng X 2011 Cryptanalysis of optical encryption schemes based on joint transform correlator architecture *Opt. Eng.* **50** 028201
[23] Lin C and Shen X J 2012 Analysis and design of impulse attack free generalized joint transform correlator optical encryption scheme *Opt. Laser Technol.* **44** 2032–6
[24] Mehra I, Rajput S K and Nishchal N K 2013 Collision in Fresnel domain asymmetric cryptosystem using phase truncation and authentication verification *Opt. Eng.* **52** 028202
[25] Mehra I, Rajput S K and Nishchal N K 2014 Cryptanalysis of an image encryption scheme based on joint transform correlator with amplitude- and phase-truncation approach *Opt. Lasers Eng.* **52** 167–73
[26] Perez-Cabre E, Cho M and Javidi B 2011 Information authentication using photon-counting double-random-phase encrypted images *Opt. Lett.* **36** 22–4
[27] Rajput S K, Kumar D and Nishchal N K 2015 Optical encryption system based on phase mask multiplexing and photon counting imaging for multiple image authentication and digital hologram security *Appl. Opt.* **54** 1657–66
[28] Rajput S K, Kumar D and Nishchal N K 2014 Photon counting imaging and polarized light encoding for secure image verification and hologram watermarking *J. Opt.* **16** 125406
[29] Chen W and Chen X 2013 Object authentication in computational ghost imaging with the realizations less than 5% of Nyquist limit *Opt. Lett.* **38** 546–8
[30] Shi X and Zhao D 2011 Image hiding in Fourier domain by use of joint transform correlator architecture and holographic technique *Appl. Opt.* **50** 766–72
[31] Wang X, Chen W and Chen X 2015 Optical encryption and authentication based on phase retrieval and sparsity constraints *IEEE Photon.* J **7** 7800310
[32] Wang X, Chen W and Chen X 2015 Optical information authentication using compressed double-random-phase-encoded images and quick-response codes *Opt. Express* **23** 6239–53
[33] Zea A V, Ramirez J F B and Torroba R 2016 Three-dimensional joint transform correlator cryptosystem *Opt. Lett.* **41** 599–602
[34] Rajput S K and Nishchal N K 2012 Image encryption and authentication verification scheme using fractional nonconventional joint transform correlator *Opt. Lasers Eng.* **50** 1474–83
[35] Lohmann A W and Mendlovic D 1997 Fractional joint transform correlator *Appl. Opt.* **36** 7402–7
[36] Kumar A, Fatima A and Nishchal N K 2018 An optical Hash function construction based on equal modulus decomposition for authentication verification *Opt. Commun.* **428** 07–14
[37] Fatima A and Nishchal N K 2018 Image authentication using vector beam with sparse phase information *J. Opt. Soc. Am.* A **35** 1053–62
[38] Nishchal N K, Goyal S, Aran A, Beri V K and Gupta A K 2006 Binary differential joint transform correlator based on a ferroelectric liquid crystal electrically addressed spatial light modulator *Opt. Eng.* **45** 026401–10

Chapter 5

[1] Kundur D and Hatzinakos D 1998 Improved robust watermarking through attack characterization *Opt. Express* **3** 485–90
[2] Wang H J M, Su P C and Jay Kuo C C 1998 Wavelet-based digital image watermarking *Opt. Express* **3** 491–6
[3] Wang Y, Deherty J F and vanDyck R E 2002 A wavelet-based watermarking algorithm for ownership verification of digital images *IEEE Trans. Image Process.* **11** 77–88
[4] Kumari B P and Rallabandi V P S 2008 Modified patchwork-based watermarking scheme for satellite imagery *Sig. Process* **88** 891–904
[5] Takai N and Mifune Y 2002 Digital watermarking by a holographic technique *Appl. Opt.* **41** 865–73
[6] Kishk S and Javidi B 2002 Information hiding technique with double phase encoding *Appl. Opt.* **41** 5462–70
[7] Kishk S and Javidi B 2003 Watermarking of three-dimensional objects by digital holography *Opt. Lett.* **28** 167–9
[8] Kishk S and Javidi B 2003 3D watermarking by a 3D hidden object *Opt. Express* **11** 874–88
[9] He M Z, Cai L Z, Liu Q, Yang X C and Wang X F 2005 Multiple image encryption and watermarking by random phase matching *Opt. Commun.* **247** 29–37
[10] Abookasis D, Montal O, Abramson O and Rosen J 2005 Watermarks encrypted in a concealogram and deciphered by a modified joint transform correlator *Appl. Opt.* **44** 3019–23
[11] He M Z, Cai L Z, Liu Q and Yang X L 2005 Phase-only encryption and watermarking based on phase-shifting interferometry *Appl. Opt.* **44** 2600–6
[12] Zhou X, Chen L and Shao J 2005 Investigation of digital hologram watermarking with double binary phase encoding *Opt. Eng.* **44** 067007
[13] Chang H T and Tsan C L 2005 Image watermarking by use of digital holography embedded in the discrete-cosine-transform domain *Appl. Opt.* **44** 6211–9
[14] Liu Z, Xu L, Guo Q, Lin C and Liu S 2010 Image watermarking by using phase retrieval algorithm in gyrator transform domain *Opt. Commun.* **283** 4923–7
[15] Singh N and Sinha A 2010 Digital image watermarking using gyrator transform and chaotic maps *Optik* **121** 1427–37
[16] Javidi B (ed) 2005 *Optical and Digital Techniques for Information Security* (Berlin: Springer)
[17] Liu S, Hennelly B M, Guo C and Sheridan J T 2015 Robustness of double random phase encoding spread-space spread-spectrum watermarking technique *Signal Process.* **109** 345–61
[18] Lu Y, You S, Zhang W, Yang B, Peng R and Zhuang S 2016 Watermarking scheme for microlens-array-based four-dimensional light field imaging *Appl. Opt.* **55** 3397–404
[19] Yadav A K, Vashisth S, Singh H and Singh K 2015 A phase-image watermarking scheme in gyrator domain using devil's vortex Fresnel lens as a phase mask *Opt. Commun.* **344** 172–80
[20] Rajput S K, Kumar D and Nishchal N K 2014 Photon counting imaging and polarized light encoding for secure image verification and hologram watermarking *J. Opt.* **16** 125406
[21] Nishchal N K 2009 Optical image watermarking using fractional Fourier transform *J. Opt. (Springer-India)* **38** 22–8
[22] Kim H and Lee Y H 2005 Optimal watermarking of digital hologram of 3D objects *Opt. Express* **13** 2881–6

[23] Nishchal N K, Pitkaaho T and Naughton T J 2010 Digital Fresnel hologram watermarking *Proc. 9th Euro-American Workshop on Information Optics (Helsinki, Finland, July 11–16, 2010)*

[24] Gu Q, Liu Z and Liucora S 2011 Image watermarking algorithm based on fractional Fourier transform and random phase encoding *Opt. Commun.* **284** 3918–23

[25] Nishchal N K 2011 Hierarchical encrypted image watermarking using fractional Fourier domain random phase encoding *Opt. Eng.* **50** 097003

[26] Deng K, Yang G and Xie H 2011 A blind robust watermarking scheme with non-cascade iterative encrypted kinoform *Opt. Express* **19** 10241–51

[27] Kim T Y, Choi H, Lee K and Kim T 2004 An asymmetric watermarking system with many embedding watermarks corresponding to one detection watermark *IEEE Signal Process. Lett.* **11** 375–7

[28] Fu Y-G 2012 Asymmetric watermarking scheme based on shuffling *Procedia Eng.* **29** 1640–4

[29] Mehra I and Nishchal N K 2014 Optical asymmetric watermarking using modified wavelet fusion and diffractive imaging *Opt. Lasers Eng.* **68** 74–82

Chapter 6

[1] Brosseau C 1998 *Fundamentals of Polarized Light: A Statistical Optics Approach* (New York: Wiley)

[2] Mogensen P C and Gluckstad J 2000 A phase image optical encryption system with polarization encoding *Opt. Commun.* **173** 177–83

[3] Davis J A, Mc Namara D E, Cottrell D M and Sonehara T 2000 Two-dimensional polarization encoding with a phase-only liquid crystal spatial light modulator *Appl. Opt.* **39** 1549–54

[4] Javidi B and Nomura T 2000 Polarization encoding for optical security systems *Opt. Eng.* **39** 2439–43

[5] Unnikrishnan G, Pohit M and Singh K 2000 A polarization encoded optical system using ferroelectric spatial light modulator *Opt. Commun.* **185** 25–31

[6] Tu H Y, Cheng C J and Chen M L 2004 Optical image encryption based on polarization encoding by liquid crystal spatial light modulator *J. Opt. A: Pure Appl. Opt.* **6** 524–28

[7] Eriksen R, Mogensen P and Gluckstad J 2001 Elliptical polarization encoding in two dimensions using phase-only spatial light modulators *Opt. Commun.* **187** 325–36

[8] Tan X, Matoba O, Okada-Shudo Y, Ide M, Shimura T and Kuroda K 2001 Secure optical memory system with polarization encryption *Appl. Opt.* **40** 2310–5

[9] Biener G, Niv A, Kleiner V and Hasman E 2005 Geometrical phase image encryption obtained with space-variant subwavelength gratings *Opt. Lett.* **30** 1096–8

[10] Biener G, Niv A, Kleiner V and Hasman E 2006 Space-variant polarization scrambling for image encryption obtained with subwavelength gratings *Opt. Commun.* **261** 5–12

[11] Unnikrishnan G, Naughton T J and Sheridan J T 2006 Polarization encoding and multiplexing of two-dimensional signals: application to image encryption *Appl. Opt.* **45** 5693–700

[12] Martinez J L, Moreno I and Mateos F 2008 Hiding binary optical data with orthogonal circular polarizations *Opt. Eng.* **47** 030504

[13] Moreno I, Iemmi C, Campos J and Yzuel M J 2011 Jones matrix treatment for optical Fourier processors with structured polarization *Opt. Express* **19** 4583–94

[14] Alfalou A and Brosseau C 2010 Dual encryption scheme of images using polarized light *Opt. Lett.* **35** 2185–7

[15] Dubreuil M, Alfalou A and Brosseau C 2012 Robustness against attacks of dual polarization encryption using the Stokes–Mueller formalism *J. Opt.* **14** 094004
[16] Li X, Lan T-H, Tien C-H and Gu M 2012 Three-dimensional orientation-unlimited polarization encryption by a single optically configured vectorial beam *Nature Commun.* **998** 1–6
[17] Lin C, Shen X, Hua B and Wang Z 2015 Three-dimensional polarization marked multiple-QR code encryption by optimizing a single vectorial beam *Opt. Commun.* **352** 25–32
[18] Zhu N, Wang Y, Liu J, Xie J and Zhang H 2009 Optical image encryption based on interference of polarized light *Opt. Express* **17** 13418–24
[19] Rajput S K and Nishchal N K 2012 Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask *Appl. Opt.* **51** 5377–86
[20] Rajput S K and Nishchal N K 2013 Image encryption using polarized light encoding and amplitude- and phase-truncation in Fresnel domain *Appl. Opt.* **52** 4343–52
[21] Rajput S K, Kumar D and Nishchal N K 2014 Photon counting imaging and polarized light encoding for secure image verification and hologram watermarking *J. Opt.* **16** 125406
[22] Lin C, Shen X, Wang Z and Zhao C 2014 Optical asymmetric cryptography based on elliptical polarized light linear truncation and a numerical reconstruction technique *Appl. Opt.* **53** 3920–8
[23] Maluenda D, Carnicer A, Martinez-Herrero R, Juvells I and Javidi B 2015 Optical encryption using photon-counting polarimetric imaging *Opt. Express* **23** 655–66
[24] Carnicer A, Juvells I, Javidi B and Martinez-Herrero R 2017 Optical encryption in the axial domain using beams with arbitrary polarization *Opt. Lasers Eng.* **89** 145–9
[25] Fatima A and Nishchal N K 2018 Optical image security using Stokes polarimetry of spatially variant polarized beam *Opt. Commun.* **417** 30–6
[26] Wang Q, Xiong D, Alfalou A and Brosseau C 2018 Optical image encryption method based on incoherent imaging and polarized light encoding *Opt. Commun.* **415** 56–63
[27] Zhang S and Karim M A 1999 Color image encryption using double random phase encoding *Microw. Opt. Technol. Lett.* **21** 318–23
[28] Joshi M, Shakher C and Singh K 2007 Color image encryption and decryption using fractional Fourier transform *Opt. Commun.* **279** 35–42
[29] Chen W and X Chen X 2011 Optical color image encryption based on asymmetric cryptosystem in the Fresnel domain *Opt. Commun.* **284** 3913–7
[30] Zhou N, Wang Y, Gong L, He H and Wu J 2011 Novel single channel color image encryption based on chaos and fractional Fourier transform *Opt. Commun.* **284** 2789–96
[31] Deng X and Zhao D 2012 Single channel color image encryption based on asymmetric cryptosystem *Opt. Laser Technol.* **44** 136–40
[32] Wei D, Ran Q, Li Y, Ma J and Tan L 2009 A convolution and product theorem for the linear canonical transform *IEEE Trans. Signal Process. Lett.* **16** 853–6

Chapter 7

[1] Hariharan P 2002 *Basics of Holography* (Cambridge: Cambridge University Press)
[2] Poon T-C and Liu J-P 2014 *Introduction to Modern Digital Holography with MATLAB* (Cambridge: Cambridge University Press)
[3] Schnars U, Falldorf C, Watson J and Juptner W 2015 *Digital Holography and Wavefront Sensing; Principles, Techniques, and Applications* (Berlin: Springer)

[4] Khare K, Ali P T S and Joseph J 2013 Single shot high resolution digital holography *Opt. Express* **21** 2581–91

[5] Khare K and George N 2003 Direct coarse sampling of electronic holograms *Opt. Lett.* **28** 1004–6

[6] Javidi B and Nomura T 2000 Securing information by use of digital holography *Opt. Lett.* **25** 28–30

[7] Lai S and Neifeld M A 2000 Digital wavefront reconstruction and its application to image encryption *Opt. Commun.* **178** 283–9

[8] Tajahuerce E and Javidi B 2000 Encrypting three-dimensional information with digital holography *Appl. Opt.* **39** 6595–601

[9] Tajahuerce E and Javidi B 2001 Three-dimensional image security *Proc. SPIE* **10298** 102980G

[10] Matoba O, Naughton T J, Frauel Y, Bertaux N and Javidi B 2002 Real-time three-dimensional object reconstruction by use of a phase-encoded digital holograms *Appl. Opt.* **41** 618792

[11] Nomura T, Okazaki A, Kameda M, Morimoto Y and Javidi B 2001 Digital holographic data reconstruction with data compression *Proc. SPIE* **4471** 235–42

[12] Naughton T J, Tajahuerce E, McDonald J B and Javidi B 2004 Three-dimensional image sensing, encryption, compression, and transmission using digital holography *Proc. SPIE* **5611** 24–32

[13] Naughton T J and Javidi B 2004 Compression of encrypted three-dimensional objects using digital holography *Opt. Eng.* **43** 2233–8

[14] Pitkaaho T, Pitkakangas V, Niemela M, Rajput S K, Nishchal N K and Naughton T J 2018 Space-variant video compression and processing in digital holographic microscopy sensor networks with application to potable water monitoring *Appl. Opt.* **57** E190–8

[15] Nishchal N K, Joseph J and Singh K 2004 Securing information using fractional Fourier transform in digital holography *Opt. Commun.* **235** 253–9

[16] Nishchal N K, Joseph J and Singh K 2004 Fully phase encryption using digital holography *Opt. Eng.* **43** 2959–66

[17] Cuche E, Marquet P and Depeursinge C 1999 Simultaneous amplitude-contrast and quantitative phase-contrast microscopy by numerical reconstruction of Fresnel off-axis holograms *Appl. Opt.* **38** 6994–7001

[18] Chang H T and Tsan C L 2005 Image watermarking by use of digital holography embedded in the discrete-cosine-transform domain *Appl. Opt.* **44** 6211–9

[19] Javidi B, Tajahuerce E, Naughton T J, Frauel Y and Matoba O 2005 Three-dimensional image encryption, transmission and processing by using digital holography *Proc. SPIE* **5954** 595403

[20] Gil S K, Jeon S H, Kim N and Jeong J R 2006 Successive encryption and transmission with phase-shifting digital holography *Proc. SPIE* **6136** 613615

[21] Nishchal N K and Naughton T J 2011 Flexible optical encryption with multiple users and multiple security levels *Opt. Commun.* **284** 735–9

[22] Gao Q, Wang Y, Li T and Shi Y 2014 Optical encryption of unlimited-size images based on ptychographic scanning digital holography *Appl. Opt.* **53** 4700–7

[23] Lin C, Shen X and Li B 2014 Four-dimensional key design in amplitude, phase, polarization and distance for optical encryption based on polarization digital holography and QR code *Opt. Express* **22** 20727–39

[24] Shiu M T, Chew Y K, Chan H T, Wong X Y and Chang C C 2015 Three-dimensional information encryption and anticounterfeiting using digital holography *Appl. Opt.* **54** A84–8
[25] Mehra I, Singh K, Agarwal A K, Gopinathan U and Nishchal N K 2015 Encrypting digital hologram of three-dimensional object using diffractive imaging *J. Opt.* **17** 035707
[26] Rajput S K, Kumar D and Nishchal N K 2015 Optical encryption system based on phase mask multiplexing and photon counting imaging for multiple image authentication and digital hologram security *Appl. Opt.* **54** 1657–66
[27] Rajput S K and Matoba O 2017 Optical voice encryption based on digital holography *Opt. Lett.* **42** 4619–22

Chapter 8

[1] Sadjadi F 2002 Invariant algebra and the fusion of multi-spectral information *Inf. Fusion* **3** 39–50
[2] Blum R S and Liu Z (ed) 2005 *Multi-Sensor Image Fusion and Its Applications* (Boca Raton, FL: CRC Press)
[3] Zyczkowski M, Szustakowski M, Ciurapinski W, Kastek M, Dulski R, Karol M, Kowalski M and Markowski P 2013 Multispectral solutions in surveillance systems: the need for data fusion *WIT Trans. Built Environ.* **134** 285–93
[4] Young R K 1993 *Wavelet Theory and Its Applications* (Amsterdam: Kluwer)
[5] Zhang S and Karim M A 1999 Color image encryption using double random phase encoding *Microw. Opt. Technol. Lett.* **21** 318–23
[6] Javidi B, Ferraro P, Hong S H, DeNicola S, Ginizio A, Alfieri D and Pierattini G 2005 Three-dimensional image fusion by use of multiwavelength digital holography *Opt. Lett.* **30** 144–6
[7] Javidi B, Do C M, Hong S H and Nomura T 2006 Multispectral holographic three-dimensional image fusion using discrete wavelet transform *J. Disp. Technol.* **2** 411–7
[8] Joshi M, Chandrashakher and Singh K 2007 Color image encryption and decryption using fractional Fourier transform *Opt. Commun.* **279** 35–42
[9] Alfalou A, Brosseau C, Abdallah N and Jridi M 2011 Simultaneous fusion, compression, and encryption of multiple images *Opt. Express* **19** 24023–9
[10] Mehra I and Nishchal N K 2014 Image fusion using wavelet transform and its application to asymmetric cryptosystem and hiding *Opt. Express* **22** 5474–82
[11] Muniraj I, Kim B and Lee B G 2014 Encryption and volumetric 3D object reconstruction using multispectral computational integral imaging *Appl. Opt.* **53** G25–32
[12] Yi F, Moon I and Lee Y H 2014 A multispectral photon-counting double random phase encoding scheme for image authentication *Sensors* **14** 8877–94
[13] Muniraj I, Guo C, Lee B-G and Sheridan J T 2015 Interferometry based multispectral photon-limited 2D and 3D integral image encryption employing the Hartley transform *Opt. Express* **23** 15907–20
[14] Rawat N, Kim B, Muniraj I, Situ G and Lee B G 2015 Compressive sensing based robust multispectral double-image encryption *Appl. Opt.* **54** 1782–93
[15] Shinoda K, Watanabe A, Hasegawa M and Kato S 2015 Multispectral information hiding in RGB image using bit-plane-based watermarking and its application *Opt. Rev.* **22** 469–76
[16] Mehra I and Nishchal N K 2015 Optical asymmetric watermarking using modified wavelet fusion and diffractive imaging *Opt. Lasers Eng.* **68** 74–82

[17] Mehra I and Nishchal N K 2015 Wavelet-based image fusion for securing multiple images through asymmetric keys *Opt. Commun.* **335** 153–60
[18] Chen H, Tanougast C, Liu Z, Blondel W and Hao B 2018 Optical hyperspectral image encryption based on improved Chirikov mapping and gyrator transform *Opt. Lasers Eng.* **107** 62–70
[19] Manjappa M, Pitchappa P, Singh N, Wang N, Zheludev N I, Lee C and Singh R 2018 Reconfigurable MEMS Fano metasurfaces with multiple-input-output states for logic operations at terahertz frequencies *Nature Commun.* **9** 1–10
[20] Kumar P and Nishchal N K 2019 Enhanced exclusive-OR and quick response code-based image encryption through incoherent illumination *Appl. Opt.* **58** 1408–12
[21] Kumar P, Fatima A and Nishchal N K 2019 Image encryption using phase-encoded exclusive-OR operations with incoherent illumination *J. Opt.* **21** 065701

Chapter 9

[1] Lorenz E N 1963 Deterministic nonperiodic flow *J. Atmos. Sci.* **20** 130–41
[2] Pecora L M and Carroll T L 1990 Synchronization in chaotic systems *Phys. Rev. Lett.* **64** 821–4
[3] Banerjee S, Yorke J A and Grebogi C 1998 Robust chaos *Phys. Rev. Lett.* **80** 3049–52
[4] Alligood K T, Sauer T D and Yorke J A 2001 *Chaos: An Introduction to Dynamical Systems* (New York: Springer)
[5] Goedgebuer J P, Larger L and Porte H 1998 Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode *Phys. Rev. Lett.* **80** 2249
[6] Larger L, Goedgebuer J P and Delorme F 1998 Optical encryption system using hyperchaos generated by an optoelectronic wavelength oscillator *Phys. Rev.* E **57** 6618–24
[7] Cuenot J B, Larger L, Goedgebuer J P and Rhodes W T 2001 Chaos shift keying with an optoelectronic encryption system using chaos in wavelength *IEEE J. Quant. Electron.* **37** 849–55
[8] Pareek N K, Patidar V and Sud K K 2006 Image encryption using chaotic logistic map *Image Vision Comput.* **24** 926–34
[9] Singh N and Sinha A 2008 Optical image encryption using fractional Fourier transform and chaos *Opt. Laser Eng.* **46** 117–23
[10] Lang J, Tao R and Wang Y 2010 Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function *Opt. Commun.* **283** 2092–6
[11] Zhou N, Wang Y, Gong L, He H and Wu J 2011 Novel single channel color image encryption based on chaos and fractional Fourier transform *Opt. Commun.* **284** 2789–96
[12] Ye R 2011 A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism *Opt. Commun.* **284** 5290–8
[13] Wang X, Zhao J and Liu H 2012 A new image encryption algorithm based on chaos *Opt. Commun.* **285** 562–6
[14] Fu C, Chen J J, Zou H, Meng W H, Zhan Y F and Yu Y W 2012 A chaos-based digital image encryption scheme with an improved diffusion strategy *Opt. Express* **20** 2363–78
[15] Liu H and Nan H 2013 Color image security system using chaos-based cyclic shift and multiple-order discrete fractional cosine transform *Opt. Laser Technol.* **50** 1–7
[16] Liu J, Jin H, Ma L and Jin W 2013 Optical color image encryption based on computer generated hologram and chaotic theory *Opt. Commun.* **307** 76–9

[17] Elshamy A M, Rashed A N Z, Mohamed A E N A, Faragalla O S, Mu Y, Alshebeili S A and Samie F E A E 2013 Optical image encryption based on chaotic Baker map and double random phase encoding *J. Lightwave Technol.* **31** 2533–9
[18] Norouzi B, Seyedzadeh S M, Mirzakuchaki S and Mosavi M R 2015 A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos *Multimed. Tools Appl.* **74** 781–811
[19] Liu X, Mei W and Du H 2016 Simultaneous image compression, fusion and encryption algorithm based on compressive sensing and chaos *Opt. Commun.* **366** 22–32
[20] Wang Z, Lv X, Wang H, Hou C, Gong Q and Qin Y 2016 Hierarchical multiple binary image encryption based on a chaos and phase retrieval algorithm in the Fresnel domain *Laser Phys. Lett.* **13** 036201
[21] Chatterjee M R, Mohamed A and Almehmadi F S 2018 Secure free-space communication, turbulence mitigation, and other applications using acousto-optic chaos *Appl. Opt.* **57** C1–13
[22] Kumar A and Nishchal N K 2019 Quick response code and interference-based optical asymmetric cryptosystem *J. Inform. Sec. Appl.* **45** 35–41

Chapter 10

[1] Peng X, Wie H and Zhang P 2006 Asymmetric cryptography based on wavefront sensing *Opt. Lett.* **31** 3579–681
[2] Qin W and Peng X 2010 Asymmetric cryptosystem based on phase-truncated Fourier transforms *Opt. Lett.* **35** 118–20
[3] Wang X and Zhao D 2012 A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms *Opt. Commun.* **285** 1078–81
[4] Wang X and Zhao D 2011 Security enhancement of a phase truncation based image encryption algorithm *Appl. Opt.* **50** 6645–51
[5] Rajput S K and Nishchal N K 2012 Asymmetric color cryptosystem that uses polarization selective diffractive optical element and structured phase mask *Appl. Opt.* **51** 5377–86
[6] Ding X, Deng X, Song K and Chen G 2013 Security improvement for asymmetric cryptosystem based on spherical wave illumination *Appl. Opt.* **52** 467–73
[7] Liu W, Liu Z and Liu S 2013 Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm *Opt. Lett.* **38** 1651–3
[8] He W, Meng X and Peng X 2013 Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm: comment *Opt. Lett.* **38** 4044
[9] Liu W, Liu Z and Liu S 2013 Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm: reply *Opt. Lett.* **38** 4045
[10] Rajput S K and Nishchal N K 2014 An optical encryption and authentication scheme using asymmetric keys *J. Opt. Soc. Am.* A **31** 1233–8
[11] Lin C, Shen X, Wang Z and Zhao C 2014 Optical asymmetric cryptography based on elliptical polarized light linear truncation and a numerical reconstruction technique *Appl. Opt.* **53** 3920–8
[12] Cai J, Shen X, Lei M, Lin C and Dou S 2015 Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition *Opt. Lett.* **40** 475–8
[13] Mehra I and Nishchal N K 2015 Optical asymmetric image encryption using gyrator wavelet transform *Opt. Commun.* **354** 344–52

[14] Fatima A, Mehra I and Nishchal N K 2016 Optical image encryption using equal modulus decomposition and multiple diffractive imaging *J. Opt.* **18** 085701
[15] Yatish, Fatima A and Nishchal N K 2018 Optical image encryption using triplet of functions *Opt. Eng.* **57** 033103
[16] Yadav A K, Singh P, Saini I and Singh K 2019 Asymmetric encryption algorithm for colour images based on fractional Hartley transform *J. Mod. Opt.* **66** 629–42
[17] Gerchberg R W and Saxton W O 1972 A practical algorithm for the determination of phase from image and diffraction plane pictures *Optik* **35** 237–50
[18] Fienup C and Dainty J 1987 Phase retrieval and image reconstruction for astronomy *Im. Recov.: Theor Appl.* **231** 275
[19] Candes E J, Li X and Soltanolkotabi M 2015 Phase retrieval via Wirtinger flow: theory and algorithms *IEEE Trans. Inform. Th.* **61** 1985–2007
[20] Metzler C, Schniter P, Veeraraghavan A and Baraniuk R 2018 prDeep: robust phase retrieval with a flexible deep network *35th Intl Confer. Machine Learning (JMLR.org)* pp 3498–507
[21] Butola M, Rajora S and Khare K 2019 Phase retrieval with complexity guidance *J. Opt. Soc. Am.* A **36** 202–11
[22] Shechtman Y, Eldar Y C, Cohen O, Chapman H N, Miao J and Segev M 2015 Phase retrieval with application to optical imaging: a contemporary overview *IEEE Sig. Process. Mag.* **32** 87–109
[23] Millane R P 1990 Phase retrieval in crystallography and optics *J. Opt. Soc. Am.* A **7** 394–411
[24] Faulner H M L and Rodenburg J M 2004 Movable aperture lensless transmission microscopy: a novel phase retrieval algorithm *Phys. Rev. Lett.* **93** 023903
[25] Chen W, Chen X and Sheppard C J 2012 Optical image encryption based on phase retrieval combined with three-dimensional particle-like distribution *J. Opt.* **14** 075402
[26] Hwang H E, Chang H T and Lie W N 2009 Multiple-image encryption and multiplexing using a modified Gerchberg–Saxton algorithm and phase modulation in Fresnel transform domain *Opt. Lett.* **34** 3917–9
[27] Wang R K, Watson I A and Chatwin C 1996 Random phase encoding for optical security *Opt. Eng.* **35** 2464–9
[28] Chang H T, Lu W C and Kuo C J 2002 Multiple-phase retrieval for optical security systems by use of random-phase encoding *Appl. Opt.* **41** 4825–34
[29] Hennelly B and Sheridan J T 2003 Fractional Fourier transform-based image encryption: phase retrieval algorithm *Opt. Commun.* **226** 61–80
[30] Rajput S K and Nishchal N K 2014 Fresnel domain nonlinear image encryption scheme based on Gerchberg-Saxton phase retrieval algorithm *Appl. Opt.* **53** 418–25
[31] Perez-Cabre E, Abril H C, Millan M S and Javidi B 2012 Photon-counting double-random-phase encoding for secure image verification and retrieval *J. Opt.* **14** 094001
[32] Chen W, Chen X, Stern A and Javidi B 2013 Phase-modulated optical system with sparse representation for information encoding and authentication *IEEE Photon.* J **5** 6900113
[33] Cho M and Javidi B 2013 Three-dimensional photon counting double-random-phase encryption *Opt. Lett.* **38** 3198–201
[34] Markman A and Javidi B 2014 Full-phase photon-counting double-random-phase encryption *J. Opt. Soc. Am.* A **31** 394–403
[35] Maluenda D, Carnicer A, Martinez-Herrero R, Juvells I and Javidi B 2015 Optical encryption using photon-counting polarimetric imaging *Opt. Express* **23** 655–66

[36] Rajput S K, Kumar D and Nishchal N K 2015 Optical encryption system based on phase mask multiplexing and photon counting imaging for multiple image authentication and digital hologram security *Appl. Opt.* **54** 1657–66
[37] Rajput S K and Nishchal N K 2017 Optical asymmetric cryptosystem based on photon counting and phase-truncated Fresnel transforms *J. Mod. Opt.* **64** 878–86

Chapter 11

[1] www.crypto-it.net/eng/theory/kerckhoffs.html
[2] Frauel Y, Castro A, Naughton T J and Javidi B 2007 Resistance of the double random phase encryption against various attacks *Opt. Express* **15** 10253–65
[3] Guo C, Muniraj I and Sheridan J T 2016 Phase retrieval-based attacks on linear canonical transform-based DRPE systems *Appl. Opt.* **55** 4720–8
[4] Toughi S, Fathi M H and Sekhavat Y A 2017 An image encryption scheme based on elliptic curve pseudo random and advanced encryption system *Sig. Process* **141** 217–27
[5] Peng X, Chang P, Wei H and Yu B 2006 Known plaintext attack on optical encryption based on double random phase keys *Opt. Lett.* **31** 1044–6
[6] Gopinathan U, Monaghan D S, Naughton T J and Sheridan J T 2006 A known-plaintext heuristic attack on the Fourier plane encryption algorithm *Opt. Express* **14** 3181–6
[7] Liu W, Yang G and Xie H 2009 A hybrid heuristic algorithm to improve known-plaintext attack on Fourier plane encryption *Opt. Express* **17** 13928–38
[8] Barrera J F, Vargas C, Tebaldi M, Torroba R and Bologini N 2010 Known plaintext attack on a joint transform correlator encrypting system *Opt. Lett.* **35** 3553–5
[9] Tashima H, Takeda M, Suzuki H, Obi T, Yamaguchi M and Ohyama N 2010 Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack *Opt. Express* **18** 13772–81
[10] Rajput S K and Nishchal N K 2013 Known-plaintext attack on encryption domain independent optical asymmetric cryptosystem *Opt. Commun.* **309** 231–5
[11] Peng X, Wei H and Zhang P 2006 Chosen-plaintext attack on lensless double random phase encoding in Fresnel domain *Opt. Lett.* **31** 3261–3
[12] Barrera J F, Vargas C, Tebaldi M and Torroba R 2010 Chosen plaintext attack on a joint transform correlator encrypting system *Opt. Commun.* **283** 3917–21
[13] Zhang Y, Xiao D, Wen W and Liu H 2013 Vulnerability to chosen-plaintext attack of a general optical encryption model with the architecture of scrambling-then-double random phase encoding *Opt. Lett.* **38** 4506–9
[14] Carnicer A, Usategui M M, Arcos S and Juvells I 2005 Vulnerability to chosen-cyphertext attacks of the optical encryption schemes based on double random phase keys *Opt. Lett.* **30** 1644–6
[15] Kumar P, Kumar A, Joseph A and Singh K 2009 Impulse attack free double random phase encryption scheme with randomized lens-phase functions *Opt. Lett.* **34** 331–3
[16] Wang X and Zhao D 2012 A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms *Opt. Commun.* **285** 1078–81
[17] Fatima A and Nishchal N K 2016 Discussion on comparative analysis and a new attack on optical asymmetric cryptosystem *J. Opt. Soc. Am.* A **33** 2034–40
[18] Nishchal N K and Fatima A 2018 Phase retrieval in optical cryptography chapter 3 *Cryptographic and Information Security* ed S Ramakrishnan (Boca Raton, FL: CRC Press)

[19] Ding X, Yang G and He D 2015 A simple public-key attack on phase-truncation-based double-images encryption system *Opt. Commun.* **346** 141–8
[20] Wu J, Liu W, Liu Z and Liu S 2015 Cryptanalysis of an 'asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition *Appl. Opt.* **54** 8921–4
[21] Fatima A and Nishchal N K 2018 Equal modulus decomposition based asymmetric optical cryptosystems chapter 5 *Advanced Secure Image Processing for Communications* ed A AlFalou (Bristol: IOP Publishing)
[22] Wang Y, Quan C and Tay C J 2016 New method of attack and security enhancement on an asymmetric cryptosystem based on equal modulus decomposition *Appl. Opt.* **55** 679–86
[23] Situ G, Monaghan D S, Naughton T J, Sheridan J T, Pedrini G and Osten W 2008 Collision in double random phase encoding *Opt. Commun.* **281** 5122–5
[24] Mehra I, Rajput S K and Nishchal N K 2013 Collision in Fresnel domain asymmetric cryptosystem using phase truncation and authentication verification *Opt. Eng.* **52** 028202
[25] Nishchal N K, Joseph J and Singh K 2004 Fully phase-based encryption using fractional order Fourier domain random phase encoding: error analysis *Opt. Eng.* **43** 2266–73
[26] Fatima A, Mehra I and Nishchal N K 2016 Optical image encryption using equal modulus decomposition and multiple diffractive imaging *J. Opt.* **18** 085701
[27] Rajput S K and Nishchal N K 2012 Image encryption and authentication verification scheme using fractional nonconventional joint transform correlator *Opt. Lasers Eng.* **50** 1474–83

Chapter 12

[1] Refregier P and Javidi B 1995 Optical image encryption based on input plane encoding and Fourier plane random encoding *Opt. Lett.* **20** 767–9
[2] Johnson E G and Brasher J D 1996 Phase encryption of biometrics in diffractive optical elements *Opt. Lett.* **21** 1271–3
[3] Tompkin W R and Staub R 1996 Low-density diffractive optical memories for document security *Opt. Eng.* **35** 2513–8
[4] Javidi B, Zhang G and Li J 1997 Encrypted optical memory using double-random phase encoding *Appl. Opt.* **36** 1054–8
[5] Yoshikawa N, Itoh M and Yatagai T 1998 Binary computer generated holograms for security applications from a synthetic double-exposure method by electron-beam lithography *Opt. Lett.* **23** 1483–5
[6] Unnikrishnan G, Joseph J and Singh K 1998 Optical encryption system that uses phase conjugation in a photorefractive crystal *Appl. Opt.* **37** 8181–5
[7] Unnikrishnan G, Joseph J and Singh K 2001 Fractional Fourier domain encrypted holographic memory by use of an anamorphic optical system *Appl. Opt.* **40** 299–306
[8] Kral E L, Walkup J F and Hagler M O 1982 Correlation properties of random phase diffusers for multiplex holography *Appl. Opt.* **21** 1281–90
[9] Mogensen P C and Glueckstad J 2000 Phase-only optical encryption *Opt. Lett.* **25** 566–8
[10] Tajahuerce E, Matoba O, Verrall S C and Javidi B 2000 Optoelectronic information encryption with phase-shifting interferometry *Appl. Opt.* **39** 2313–20
[11] Seo D-H and Kim S-J 2003 Interferometric phase-only optical encryption system that uses a reference wave *Opt. Lett.* **28** 304–6
[12] Nishchal N K, Joseph J and Singh K 2003 Fully phase encryption using fractional Fourier transform *Opt. Eng.* **42** 1583–8

[13] Nishchal N K, Joseph J and Singh K 2003 Optical phase encryption by phase contrast using electrically addressed spatial light modulator *Opt. Commun.* **217** 117–22

[14] Nishchal N K, Joseph J and Singh K 2004 Securing information using fractional Fourier transform in digital holography *Opt. Commun.* **235** 253–9

[15] Barerra J F, Henao R and Torroba R 2005 Optical encryption method using toroidal zone plate *Opt. Commun.* **248** 35–40

[16] Tebaldi M, Furlan W D, Torroba R and Bolognini N 2009 Optical data storage readout technique based on fractal encrypting masks *Opt. Lett.* **34** 316–8

[17] Rajput S K and Nishchal N K 2012 Asymmetric color cryptosystem that uses polarization selective diffractive optical element and structured phase mask *Appl. Opt.* **51** 5377–86

[18] Singh H, Yadav A K, Vashisth S and Singh K 2015 Double phase image encryption using gyrator transforms and structural phase masks in the frequency plane *Opt. Lasers Eng.* **67** 145–56

[19] Barerra J F, Henao R, Tebaldi M, Torroba R and Bolognini N 2006 Multiple image encryption using an aperture-modulated optical system *Opt. Commun.* **261** 29–33

[20] Singh M and Kumar A 2007 Optical encryption and decryption using sandwich random phase diffuser in the Fourier plane *Opt. Eng.* **46** 055201

[21] Grosges T and Barchiesi D 2010 Toward nanoworld-based secure encryption for enduring data storage *Opt. Lett.* **35** 2421–3

[22] Francois M, Grosges T, Barchiesi D and Erra R 2011 Generation of encryption keys from plasmonics *PIERS Online* **7** 296–300

[23] Fatima A, Mehra I and Nishchal N K 2014 Plasmonics-based keys for optical image encryption *Int. Conf. Fibre Optics and Photonics* OSA Technical Digest S5A.52

[24] Sui L, Bei Z, Xiaojuan N and Ailing T 2016 Optical image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain *Opt. Express* **24** 499–515

[25] Zamrani W, Ahouzi E, Lizana A, Campos J and Yzuel M J 2016 Optical image encryption technique based on deterministic phase masks *Opt. Eng.* **55** 1031081

[26] Sahoo S K, Tang D and Dang C 2017 Enhancing security of incoherent optical cryptosystem by a simple position-multiplexing technique and ultra-broadband illumination *Sci. Rep.* **7** 17895

[27] Sun W, Wang L, Wang J, Li H and Wu Q 2018 Optical image encryption using gamma distribution phase masks in the gyrator domain *J. Eur. Opt. Soc. Rapid Publications* **14** 28

[28] Schipf D R and Wang W-C 2018 Optical encryption using a liquid phase mask *OSA Continuum* **1** 1026–40

[29] Burckhardt C B 1970 Use of a random phase mask for the recording of Fourier transform holograms of data masks *Appl. Opt.* **9** 695–700

[30] Stewart W C, Firester A H and Fox E C 1972 Random phase data masks: fabrication tolerance and advantages of four phase level masks *Appl. Opt.* **11** 604–8