J. Opt. 18 (2016) 083001 (39pp) doi:10.1088/2040-8978/18/8/083001

Roadmap

Roadmap on optical security

Bahram Javidi[1,22], Artur Carnicer[2,22], Masahiro Yamaguchi[3], Takanori Nomura[4], Elisabet Pérez-Cabré[5], María S Millán[5], Naveen K Nishchal[6], Roberto Torroba[7], John Fredy Barrera[8], Wenqi He[9], Xiang Peng[9], Adrian Stern[10], Yair Rivenson[11], A Alfalou[12], C Brosseau[13], Changliang Guo[14], John T Sheridan[14], Guohai Situ[15], Makoto Naruse[16], Tsutomu Matsumoto[17], Ignasi Juvells[2], Enrique Tajahuerce[18], Jesús Lancis[18], Wen Chen[19], Xudong Chen[20], Pepijn W H Pinkse[21], Allard P Mosk[21] and Adam Markman[1]

[1] Electrical and Computer Engineering Department, University of Connecticut, 371 Fairfield Road, Storrs, Connecticut 06269, USA
[2] Universitat de Barcelona (UB), Facultat de Física, Departament de Física Aplicada, Martí i Franquès 1, 08028 Barcelona, Spain
[3] Department of Information Processing, Tokyo Institute of Technology, 4259-G2-28, Nagatsuta, Midori-ku, Yokohama 226-8503, Japan
[4] Faculty of Systems Engineering, Wakayama University, 930 Sakaedani, Wakayama 640-8510, Japan
[5] Grup d'Òptica Aplicada i Processament d'Imatges (GOAPI), Departament d'Òptica i Optometria, Universitat Politècnica de Catalunya-BarcelonaTech (UPC), Violinista Vellsolà 37, 08222 Terrassa, Spain
[6] Department of Physics, Indian Institute of Technology Patna, Bihta, Patna 801118, India
[7] Centro de Investigaciones Ópticas (CONICET La Plata-CIC) and UID OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, PO Box 3, C.P 1897, La Plata, Argentina
[8] Grupo de Óptica y Fotónica, Instituto de Física, Facultad de Ciencias Exactas y Naturales, Universidad de Antioquia UdeA, Calle 70 No. 52-21, Medellín, Colombia
[9] College of Optoelectronics Engineering, Key Laboratory of Optoelectronic Devices and Systems of Ministry of Education and Guangdong Province, Shenzhen University, Shenzhen 518060, People's Republic of China
[10] Department of Electro-Optical Engineering, Ben-Gurion University of the Negev, PO Box 653, Beer-Sheva 84105, Israel
[11] Electrical Engineering Department, University of California, Los Angeles, USA
[12] Equipe Vision, L@BISEN, ISEN-Brest, 20 rue Cuirassé Bretagne, CS 42807, 29228 Brest Cedex 2, France
[13] Université de Brest, Lab-STICC, 6 avenue Le Gorgeu, CS 93837, 29238 Brest Cedex 3, France
[14] School of Electrical, Electronic and Communications Engineering, Communications and Optoelectronic Research Centre, The SFI-Strategic Research Cluster in Solar Energy Conversion, College of Engineering and Architecture, University College Dublin, Belfield, Dublin D4, Ireland
[15] Shanghai Institute of Optics and Fine Mechanics, Chinese Academy of Sciences, Shanghai 201800, People's Republic of China
[16] Network System Research Institute, National Institute of Information and Communications Technology, 4-2-1 Nukui-kita, Koganei, Tokyo 184-8795, Japan
[17] Graduate School of Environment and Information Sciences, Yokohama National University, Hodogaya, Yokohama, Kanagawa, Japan
[18] GROC·UJI, Institute of New Imaging Technologies, Universitat Jaume I, 12071 Castelló, Spain
[19] Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, People's Republic of China
[20] Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583, Singapore
[21] Complex Photonic Systems (COPS), MESA+ Institute for Nanotechnology, University of Twente, 7500 AE Enschede, The Netherlands

2040-8978/16/083001+39$33.00

E-mail: bahram@engr.uconn.edu and artur.carnicer@ub.edu

Received 26 January 2016
Accepted for publication 1 February 2016
Published 22 July 2016

Abstract

Information security and authentication are important challenges facing society. Recent attacks by hackers on the databases of large commercial and financial companies have demonstrated that more research and development of advanced approaches are necessary to deny unauthorized access to critical data. Free space optical technology has been investigated by many researchers in information security, encryption, and authentication. The main motivation for using optics and photonics for information security is that optical waveforms possess many complex degrees of freedom such as amplitude, phase, polarization, large bandwidth, nonlinear transformations, quantum properties of photons, and multiplexing that can be combined in many ways to make information encryption more secure and more difficult to attack. This roadmap article presents an overview of the potential, recent advances, and challenges of optical security and encryption using free space optics. The roadmap on optical security is comprised of six categories that together include 16 short sections written by authors who have made relevant contributions in this field. The first category of this roadmap describes novel encryption approaches, including secure optical sensing which summarizes double random phase encryption applications and flaws [Yamaguchi], the digital holographic encryption in free space optical technique which describes encryption using multidimensional digital holography [Nomura], simultaneous encryption of multiple signals [Pérez-Cabré], asymmetric methods based on information truncation [Nishchal], and dynamic encryption of video sequences [Torroba]. Asymmetric and one-way cryptosystems are analyzed by Peng. The second category is on compression for encryption. In their respective contributions, Alfalou and Stern propose similar goals involving compressed data and compressive sensing encryption. The very important area of cryptanalysis is the topic of the third category with two sections: Sheridan reviews phase retrieval algorithms to perform different attacks, whereas Situ discusses nonlinear optical encryption techniques and the development of a rigorous optical information security theory. The fourth category with two contributions reports how encryption could be implemented at the nano- or micro-scale. Naruse discusses the use of nanostructures in security applications and Carnicer proposes encoding information in a tightly focused beam. In the fifth category, encryption based on ghost imaging using single-pixel detectors is also considered. In particular, the authors [Chen, Tajahuerce] emphasize the need for more specialized hardware and image processing algorithms. Finally, in the sixth category, Mosk and Javidi analyze in their corresponding papers how quantum imaging can benefit optical encryption systems. Sources that use few photons make encryption systems much more difficult to attack, providing a secure method for authentication.

S Online supplementary data available from stacks.iop.org/JOPT/18/083001/mmedia

(Some figures may appear in colour only in the online journal)

Contents

I. Encryption technologies

[22] Guest editors of the roadmap.

II. Compression and Encryption

III. Cryptanalysis

IV. Micro- and nano- techniques

V. Ghost imaging encryption

VI. Quantum cryptosystems

1. Secure optical sensing

Masahiro Yamaguchi

Tokyo Institute of Technology

Status

The security of information systems is increasingly crucial in our lives, as everything is going to be connected to the Internet. Information security technology is mostly constructed on the basis of mathematical theories of cryptography. However, the threat to information systems is still growing, and it is definitely important to consider system-level security to protect information resources against human error and malicious attacks. Although the mathematical theory for information security plays a central part for this purpose, there is a limitation in all-digital based security measures. Hence it is advantageous to integrate physical measures against increasing security threats.

The role of imaging and sensing is growing in information systems and so the security of imaging and sensing systems becomes crucial. Biometrics, surveillance, inspection, medical and health monitoring are all fields where security is quite important. In order to protect such data from theft, falsification, and counterfeiting, the application of cryptographic technology is recommended. Once image data is captured, the digital data faces various security threats. Software-based systems cannot avoid vulnerability that can be exploited by software-based attacks. Therefore, it is beneficial to consider protecting image data before being converted into digital format; namely, secure optical imaging. If optical security technology can be appropriately integrated in digital imaging systems, the security risk in the system will be considerably reduced.

A well-known optical encryption technique suitable for imaging applications is double random phase encoding (DRPE) [1]. In DRPE, the input image is represented by the amplitude of light, which is modulated by random phase and then Fourier transformed. In the Fourier domain, another random phase mask is multiplied as an encryption key. The complex amplitude in the Fourier domain or the spatial domain is considered as ciphertext. There have been variations of DRPE developed using Fresnel or fractional Fourier transforms. It can be applied to the encryption of digital data in optical data storage systems, and secure imaging is another promising application field. Optical encryption with digital holography [2] is mathematically nearly equivalent to DRPE and also suitable for encrypted imaging. DRPE has also been integrated with compressive sensing, which is also suitable for secure optical imaging [3].

Current and future challenges

Encrypted imaging by DRPE is realized by digital holography, where an object is illuminated with a random phase pattern and the reference beam is encoded with another random phase pattern that works as the encryption key. The original object is reconstructed only if the correct random phase key is used. A serious issue in this system is speckle noise. While speckle noise can be suppressed by capturing multiple images with a changing illuminating random phase pattern [4], it increases the amount of data and may affect the strength of security.

DRPE is an encryption method but can also be considered as a pattern matching scheme, since the multiplication of a random phase in the Fourier domain implies matched filtering. By appropriately designing the random phase pattern, it can be applied to 'cancellable biometrics' authentication systems [5]. Because biometric authentication is based on the unique features of the individual, the biometric template must be protected against security threats and must also be replaceable. Therefore the application of DRPE is advantageous since it enables a secure biometrics sensor with template protection and cancellable biometrics.

On the other hand, the security of optical encryption is still under active investigation [6, 7]. Optical phenomena are essentially linear processes, and encryption through linear systems is vulnerable to various kinds of attacks. DRPE involves nonlinearity in the phase encoding process, but most of the transformations are linear. It has been pointed out that encryption by DRPE is not resistant to certain types of attacks, but limited analysis has been done until now. Although it can be said that certain types of optical encryption are not secure in some cases, the conditions are yet unclear. Moreover, security improvements have been continuously reported.

Although DRPE is based on Fourier analysis, it can also be modeled by algebraic mathematics; namely, vector-matrix multiplication as shown in figure 1 [8]. The multiplication of random phase corresponds to random projection onto a higher-dimensional space. This kind of analysis is valuable, for it clarifies the trait of the algorithm, and will suggest more secure methods; for example, more complicated projection techniques. Furthermore, an algebraic technique enables implementation by an incoherent optical system.

Advances in science and technology to meet challenges

DRPE and its extension can be portrayed by algebraic equations and it allows application to incoherent imaging systems. If encrypted imaging technology is realized by an imaging system with a normal incoherent illumination source, the application field will be extended. Recently the technology of computational imaging is being deployed in practice, and it is expected to be applied to 'secure imaging'.

For practical optical encryption purposes, much deeper security analysis is needed. At the same time, we should be aware of the fact that it is very difficult to achieve an equivalent security level to conventional encryption techniques based on cryptographic theory, which employ a more complicated mathematical model. Even if the security of optical encryption is not perfect, it is still beneficial because the information is physically protected.

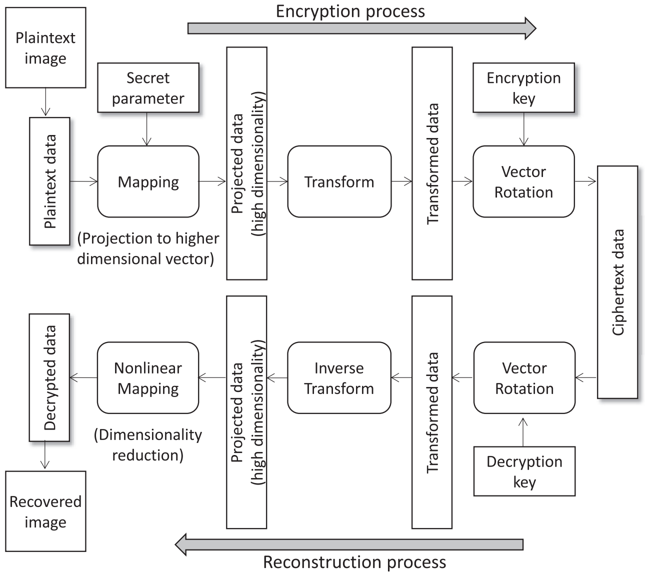

Figure 1. Algebraic model of DRPE. The 'Secret parameter' corresponds to the random phase pattern at the input plane. 'Encryption and decryption keys' are the random phase on the Fourier plane. All processes can be described with vector-matrix multiplications except the nonlinear mapping at the final step.

Figure 2 shows two examples of optical encryption in biometrics verification systems; cancellable biometrics and secure optical sensors. Optical encryption will be used not only for secrecy but also for authentication of the user, data, time, or device in the secure optical imaging system. For example, it will be possible to authenticate the sensing device, resulting in the enhancement of reliability of the data.

When considering system implementation, firstly we need to have answers to questions like: what types of attack is this optical encryption technique vulnerable to? Since secure optical sensing systems are uncommon, it is necessary to define the class of attacks that should be considered for secure optical sensing systems. Then a combination of physics-based and mathematical cryptography-based security technologies will be designed such that the vulnerability of the total system is extinguished. An important issue is the method of key handling, i.e. how the key data is shared between different entities, how the key is updated, etc. For this, the security profile of the system needs to be evaluated [9]. Case studies as well as practical deployment will motivate extensive research and practical applications of the technology.

The reduction of speckle is a very important issue that affects the security strength of the system as mentioned above. Optical and digital techniques for speckle reduction [10, 11] should be integrated with the secure sensing system.

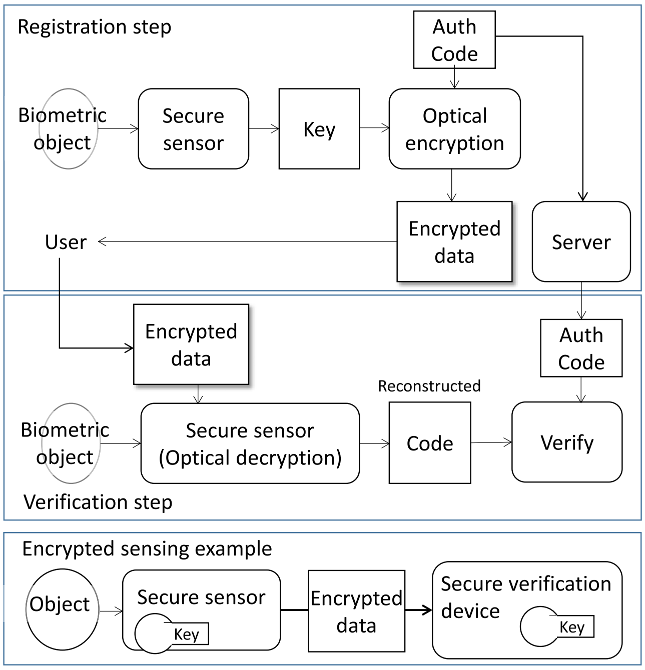

Figure 2. Secure sensing system examples. Upper and middle: registration and verification steps of the optical cancellable biometrics system. Bottom: an example of an encrypted sensing system.

Finally, more advances are also expected in the technologies of nonlinear materials and devices, since introducing nonlinearity is the key to enhance the security of optical encryption systems.

Concluding remarks

The current status and challenges of secure optical sensing technology are discussed. DRPE is an example, but it can be thought of as a starting point for other types of optical encryption techniques. If the system-oriented aspect is more keenly addressed, this technology will be widely utilized in IoT (Internet of Things) or IoE (Internet of Everything) contexts.

Acknowledgments

The author sincerely acknowledges Dr Hiroyuki Suzuki, Tokyo Institute of Technology, Dr Kazuya Nakano, Tokyo University of Science, and Masafumi Takeda, Sundisk Corp. for exceptionally valuable discussions on this subject.

2. Digital holographic encryption in free space optical technique

Takanori Nomura

Wakayama University

Status

Research on optical encryption has increased rapidly since the double random phase encoding method was published [1]. Originally the method used two random phase masks in both an input plane and the Fourier plane. The optical system described in the paper is based on a correlational optical system. Therefore, lots of researchers studying optical computers rushed into the field of optical encryption. To decode the encrypted data, phase information of the mask (complex data) is mandatory. Holography is used to obtain the phase data. For this reason, it is somewhat difficult for researchers from other areas of optical information processing to enter research in optical encryption. Fortunately, in line with advances in imaging devices such as CCDs, digital holography is accessible to record/detect complex data. Therefore, digital holography is a powerful tool to realize double random phase encoding optical encryption. This was a trigger for many people to start research on optical encryption. In those days, the size of an imaging device was not so small (~10 μm) and the number of pixels was not enough (~640 by 480) either. However, some pioneers challenged optical encryption using digital holography. Double random phase encoding optical encryption was experimentally demonstrated combined with digital holography [12]. Expanding the encryption into the Fresnel region was also demonstrated with digital holography [2, 13]. Furthermore, a virtual optical encryption system was accomplished [14]. Owing to it being virtual, there is no requirement to encrypt and record the object in an optical system.

In spite of the poor performance of the imaging devices, it is true that the amount of journal papers on digital holography increased rapidly. Caclulation performance progress of personal computers continues to be considerable. Under the background of digital holography, research on optical encryption progresses.

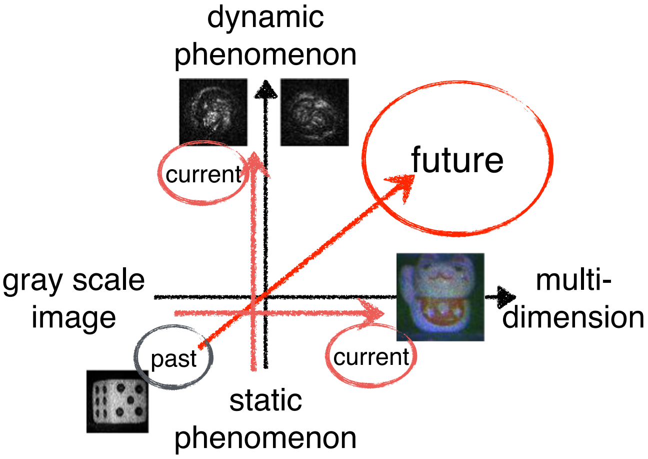

Figure 3. Progress in digital holography; from a gray scale image to a multi-dimensional image, and from a static phenomenon to a dynamic phenomenon.

Current and future challenges

The double random phase encoding optical encryption method is widely applied to various fields, especially combined with other imaging techniques. One example is a photon-counting imaging system. In imaging systems, images can have a limited number of photons by controlling the expected number of incident photons. The use of photon-counting imaging to obtain a photon-limited version of the encrypted distribution was proposed [15]. The decrypted image cannot be easily visualized so that an additional layer of information protection is achieved.

Integral imaging can provide the range information of a three-dimensional object using passive sensing. Therefore, a three-dimensional information encryption technique with a double-random phase-encoded method and photon counting integral imaging was proposed [16]. It enables one to realize the encryption and verification of the three-dimensional object at different depths. Another combination of the double random phase encoding method with optical techniques is compressive imaging [3]. It is shown that the model described in the literature can be applied for recovering images from a general image degrading model caused by both diffraction and geometrical limited resolution.

Digital holography has made rapid progress. Sequential phase-shifting techniques are used to remove a conjugate image and dc term. However, those techniques are only applied to static phenomena. That is because at least two phase-shifted holograms are recorded sequentially at different times. To solve this problem, single-exposure phase-shifting techniques have been proposed. These techniques are based on wave splitting. The reference wave is spatially modulated to distribute a certain phase-shift onto each pixel of an imaging device. The hologram recorded using the reference wave is divided by each pixel of the phase shift. The lack of pixel values generated by this division is interpolated by the adjacent pixel values. Consequently, phase-shifted holograms can be obtained by a single recording. Typically, a combination of pixelated polarizing devices are used for phase-shifting [17]. In these methods, the algorithms for obtaining a complex amplitude distribution of an object wave are the same as the sequential phase-shifting techniques. Therefore, the quality of reconstructed images depends on the accuracy of the phase-shifting devices and their alignment. To avoid the use of a special phase-shifting device, single-exposure phase-shifting digital holography using a random-complex-amplitude encoded reference wave was proposed. The amplitude and phase of the reference wave are generalized in the algorithm [18].

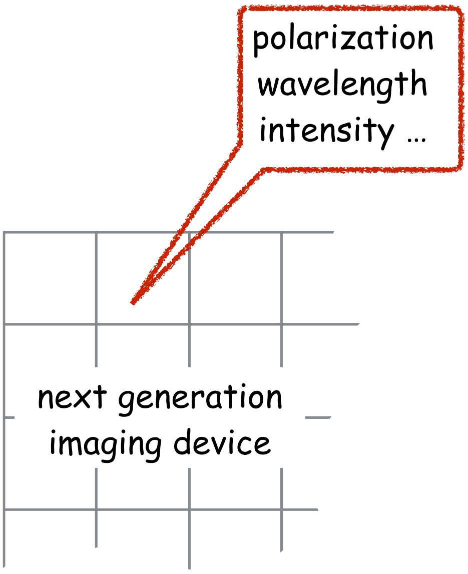

Figure 4. A next-generation imaging device can detect various physical parameters in a single pixel.

Advances in science and technology to meet challenges

Figure 3 shows the progress in digital holography. Due to this, the application fields of optical encryption (double random phase encoding method) will expand much more. However, both dynamic phenomena and multi-dimensional data are yet to be realized because dynamic recording is accomplished with the aid of polarization or spectroscopy. This is why available imaging devices detect only intensity information. Furthermore, spatial resolution is sacrificed to realize dynamic recording. For the purpose of applying multi-dimensional dynamic digital holography to optical encryption, new imaging devices to detect other optical parameters in addition to intensities are desired. For example, the device should detect the wavelength, polarization state, and intensity in a single pixel as shown in figure 4. A smaller size of pixels is preferable to obtain high spatial resolution. The number of pixels is also important. Smaller sized pixels and lots of pixels give a large space-bandwidth product.

Concluding remarks

Digital holography is a powerful tool for optical encryption. However the performance of available imaging devices is not good enough. In the last two decades progress in both optical encryption and digital holography has been significant. For further progress, new devices as well as new algorithms for optical encryption are mandatory. In this section, although verification and validation are not mentioned, digital holography also plays an important role in these applications. Introducing new fields of optics, such as terahertz imaging, optical vortices, etc, will accelerate the study of optical encryption.

3. Simultaneous encryption and authentication of multiple signals

Elisabet Pérez-Cabré and María S Millán

Universitat Politècnica de Catalunya

Status

Multifactor optical encryption-authentication (MOEA) (figure 5) was first introduced in 2006 [19] to provide simultaneous encryption of up to four factors or signals (named $r(x)$, $s(x)$, $b(x)$ and $n(x)$) into a single complex-valued distribution ($\psi(x)$) given by:

$$\psi(x) = t_{r+2b}(x) \; * \; t_s(x) \; * \; \mathrm{FT}^{-1}[t_{2n}(x)], \qquad (1)$$

and subsequent simultaneous authentication of all those signals. In equation (1) all factors are phase-encoded, that is, for a general function $a(x)$, $t_a(x) = \exp[j\pi a(x)]$ (in the case of two signals placed together $t_{r+2b}(x) = t_r(x)t_{2b}(x)$), FT^{-1} denotes an inverse Fourier transform and $*$ is the convolution operation. The signals to encrypt can be of various natures: biometrics, logos, traces, random codes, text or others. They are scrambled all together into a dim, noisy-like encrypted function that does not reveal any piece of information of the factors being protected. The MOEA procedure permits the simultaneous optical authentication of the whole set of factors hidden in function $\psi(x)$ by means of their comparison with *in situ* captured images and information obtained from a database. An optical processor composed of a joint transform and a 4f correlator linked through a nonlinear operation (figure 5) provides a sharp and intense output peak only when all the factors are verified positively. Otherwise, when one or more checked images differ from the factors previously encrypted the output does not reveal the presence of any signal.

Encryption and authentication of multiple signals is an important achievement in optical security applications that increases system reliability because its response does not rely on the verification of a single factor but on a set of factors [19, 20]. They all must obtain positive authentication to provide a final validation. For instance (figure 5(b)), one can verify the driver identity through their retina scan $r(x)$ along with the vehicle plate $s(x)$, the place intended to be accessed through the code $b(x)$ and the contents of the parcel to be delivered $n(x)$.

Unlike sequential encryption methods, the MOEA technique achieves digital encoding of all the signals at the same time in the same ciphering plane. The resulting encrypted function can be further manipulated to obtain an identity (ID) tag for remote surveillance or tracking of vehicles or moving objects (figure 6) [21, 22]. The ID tag can be designed to require near infrared (NIR) illumination to retrieve its content. This makes it invisible to the naked eye, to most common inspection cameras and, therefore, more secure [21]. Furthermore, information redundancy on the designed ID tag has been proved to allow verification robustness against scratches or data loss due to handling or wear damage [21, 22].

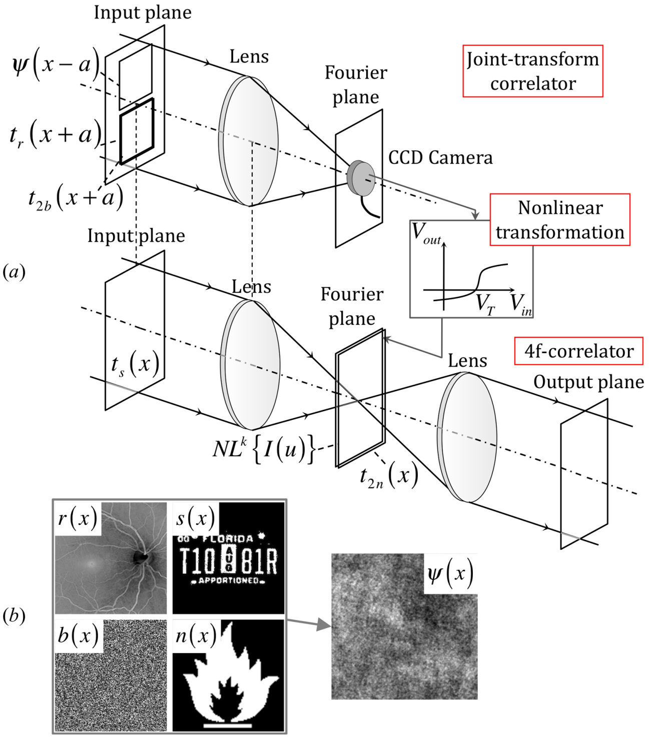

Figure 5. (a) MOEA setup (see [25] for details). (b) Four factors of different nature and MOEA complex-valued encrypted function.

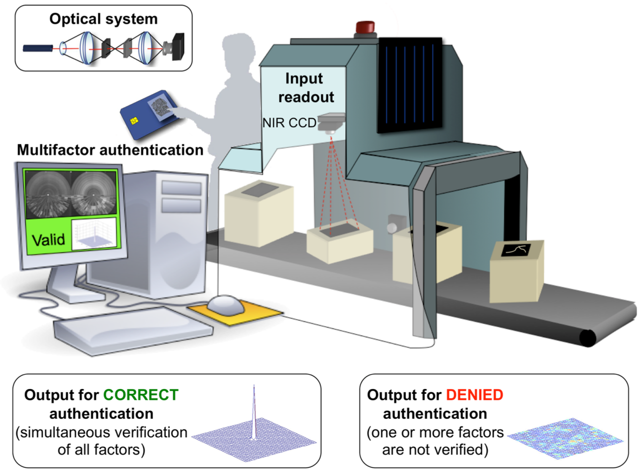
Optical system
Input readout
NIR CCD
Multifactor authentication
Valid
Output for CORRECT authentication (simultaneous verification of all factors)
Output for DENIED authentication (one or more factors are not verified)

Figure 6. High-level security MOEA application as presented in [21]. The moving parcels are verified along with the identity of the delivery person and other information from a database. Additional features: non-visible, NIR remotely readable ID tag, certain tolerance to scale and in-plane rotations, resistance to damage produced by common handling.

Current and future challenges

Data compression is actually a challenge for better fulfilling the general requirements of information protection, storage and transmission for optical encryption systems (see for instance, category II). The original MOEA technique already compresses the information of up to four signals into a single encrypted distribution with the same spatial resolution as the primary images. But this might not be enough. Similarly to other ciphering methods, the resultant encrypted function

$\psi(x)$ is a complex-valued distribution that involves certain difficulties when trying to capture or reproduce it by commonly available optical means (cameras, spatial light modulators (SLMs)). The separate representation of the magnitude and phase information into a novel designed ID tag produces a more compact and experimentally feasible tag with improved distortion tolerance [23]. Additionally, satisfactory verification results are obtained when the amplitude information is reproduced with a single bit (binary information) or when both amplitude and phase use only 2 bits each for their representation in the ID tag [23].

In practice, further reduction or simplification of the encrypted content to be transmitted may be necessary.

Photon-counting imaging techniques have been recently implemented along with encryption techniques [15] (see section 16). In photon-counting systems, images are captured under photon starving conditions by controlling the expected number of incident photons. For complex-valued distributions, as the encrypted function $\psi(x)$, the photon-counting technique is applied to the amplitude, thus keeping the phase information of the pixels that receive at least one photon count. This procedure strongly reduces the number of pixels with relevant information of the encrypted function, producing sparse distributions to be processed or transmitted. In fact, only the phase of the selected pixels is considered for decryption and authentication stages. For the widely used encryption technique double-random phase encoding (DRPE) [1], further compression is achieved by limiting the number of bits used for representing the phase information in the photon-limited encrypted distribution. Only 2 bits, or equivalently 4 grey levels, suffice to achieve satisfactory authentication results [24]. A recent application of the photon-counting imaging technique to MOEA shows the preservation of the good qualities of the multifactor encryption, and sheds light on a more powerful and secure system in comparison to the original version [25].

It is important to point out that common optical encryption systems usually entail strict setup alignment requirements for their experimental implementation, because it is necessary to assure pixel-by-pixel positioning of the random key code when decryption is carried out by optical means. Currently, this is probably the biggest issue for all-optical security systems, and this is the main reason why hybrid optical-digital systems or only digital are the most widespread. Attempts to achieve simpler optical processors have been made recently [26, 27]. In [26], the introduction of a nonlinear operation in a two-step joint-transform processor permits the alleviation of the experimental realization of the optical encryption-decryption. Additionally, the implementation of the encryption technique in the Fresnel domain reduces the number of lenses required in the experimental procedure [27].

Advances in science and technology to meet challenges

Advances in photon-counting cameras will allow the experimental realization of sparse encryption functions recorded with a limited number of photon-counts. Even though the technology exists, its applicability is still limited and not widespread. As mentioned before, photon-limited phase-only encrypted distributions keep the essential properties of encryption systems while increasing their security and permitting further information compression.

The security strength of optical cryptography resides in the ability of optics to process the information in a hyperspace of states, where variables such as amplitude, phase, polarization, wavelength, spatial position and fractional spatial frequency domain can all be used to hide the signal with greater concealment. Moreover, optical processing has the valuable property of inherent parallelism, which allows for fast encryption and decryption of large volumes of data. However, the vast majority of encryption-decryption proposals are based on hybrid optical-digital systems in an attempt to overcome the strict requirements for the alignment of optical processors that perform both the encryption and the decryption stages [28]. In this regard, compact processors containing spatial light modulators (SLMs) jointly display several functions such as a programmable phase Fresnel lens, an input image, a phase mask and a filter. Research on SLM devices, novel architectures and algorithms will ease this bottleneck [29].

Concluding remarks

Simultaneous encryption-authentication of multiple factors is a highly secure optical encryption method for demanding security systems. Recent research in this field has demonstrated the potential of MOEA combined with photon-counting imaging techniques for the secure surveillance of different items, with simultaneous verification of multiple factors, thus allowing significant data compression with proved resistance against unauthorized attacks. However, as for many other optically inspired security systems, MOEA still suffers from strict alignment constraints if its all-optical implementation is pursued. Further research has to be done in this direction to increase the current applicability of optical encryption methods.

Acknowledgments

The authors thank the Spanish Ministerio de Economía y Competitividad and FEDER for financial support (project number DPI2013-43220-R).

4. Amplitude- and phase-truncation based optical asymmetric cryptosystem

Naveen K Nishchal

Indian Institute of Technology Patna

Status

In the present information age, which we may call the digital era, massive dissemination of data is being allowed through current communication technologies. As such, it is of common interest to protect the privacy of data to avoid its unauthorized access. In the last few decades, optical techniques for information security have advanced. This now forms an adequate framework for developing robust data protection techniques, as is evidenced by the availability of literature on this research area [1, 20, 22, 30, 31].

Most reported optical security techniques in the literature belong to the category of symmetric cryptosystems, in which the keys used for encryption are identical to the decryption keys. It is believed that under an environment of network security, a symmetric cryptosystem would suffer from problems in key distribution, management, and delivery. Hence, it is necessary to develop an attack free asymmetric cryptosystem [30]. Cryptanalysis indicates that the weakness of security originates from the linearity of the cryptosystem. Qin and Peng [31] proposed an asymmetric cryptosystem based on twice phase-truncated Fourier transforms (PTFT), in which the encryption key differs from the decryption key, and the technique overcomes the weakness of linearity of conventional optical cryptosystems [32].

The PTFT is a Fourier transform process with an operation of phase truncation. It means that only the amplitude of the Fourier spectrum is retained, while the phase part of the spectrum is truncated. Similarly in amplitude truncation only the phase part of the spectrum is retained, while the amplitude part is truncated [33]. Section 6 also discusses in detail the asymmetric and one-way cryptosystem. Figure 7 shows a block diagram for an optical asymmetric cryptosystem. The decryption keys generated here are object/plaintext dependent. It has been reported in the literature that plaintext dependent public and private key generation should not be called an asymmetric cryptosystem; rather, they should be called a secret sharing method. In this regard, it is necessary to define the secret sharing scheme, in which a secret can be divided among N people so that any n ($n < N$) people can get together to reconstruct the secret. But this is not the case with an asymmetric cryptosystem. This is because in asymmetric cryptosystems, unless all the decryption keys are known, the original information cannot be decrypted successfully.

Current and future challenges

With the development of the optical asymmetric scheme, it was assumed that the technique would survive all existing attacks and hence was treated as a robust method. But it has proved to be vulnerable to a special attack [35–37]. In a special attack, the attacker uses a randomly generated random phase mask with the encrypted image and tries to retrieve the original information. Several image encryption techniques have been demonstrated improvising the basic asymmetric framework with enhanced strength. The improvement is mainly with the use of polarization encoding and different optical transforms, such as the Fresnel transform, fractional Fourier transform, gyrator transform, and wavelet transform [33–39]. Also, the use of conventional random phase masks has been replaced with commercially available diffusers, structured phase masks (zone plates), holographic plates (after removing the silver halide emulsion), and the use of phase-only spatial light modulators.

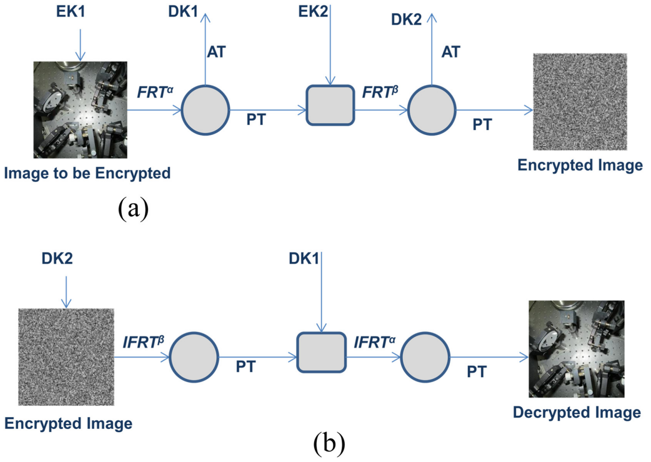

Figure 7. Block diagram for an amplitude–and phase-truncation based optical asymmetric cryptosystem. (a) Encryption process and (b) decryption process. EK: encryption key, DK: decryption key, AT: amplitude truncation, PT: phase truncation, FRT: fractional Fourier transform.

It is believed that information security employing optical technologies would be fast and highly secure as compared to their digital counterparts. The repeated cycle of attack followed by appropriate defense is the natural lifecycle of any cryptosystem. The optical asymmetric cryptosystem is undergoing this phase. Various aspects of the cryptosystem have been theoretically studied and reported in the literature. The challenge lies in hardware implementation with low cost commercially available components and devices but without any compromise on security. A suggestion could be the development of a hybrid security system, which uses both digital as well as optical technology. It can be a combination of an optically implementable encryption algorithm with actual optical computing. The idea is the development of a computer chip for implementing the digital algorithm. The optical part should use an LED source, a lens system, a display device, and a digital camera. The developed technology must resist all existing attacks. Another important issue with key generation is that the public and private keys should be independent of the plaintext. Therefore, the challenge is designing a scheme for key generation which does not depend on plaintexts and resists all attacks. However, no scheme would be perfect in all senses but perfection in specific types of applications could be achieved.

Advances in science and technology to meet challenges

Considering the fact that color information could contribute to a higher level of security than binary or grayscale images, optical techniques for securing color information have also attracted the attention of the research community [30, 34]. Binary or grayscale images are encrypted and decrypted by monochromatic light; therefore, the decrypted images do not preserve their color information. The color information of an image is useful in many practical applications, including security verification of human facial images. Figure 8 shows a block diagram for color image encryption, in which there are two schemes; three channel systems, as shown in figure 8(a), and single channel systems, as shown in figure 8(b). Each of these schemes is suitably combined with the asymmetric encryption approach as shown in figure 7.

Further, securing multispectral data is becoming an important issue because such data received from satellites and airborne sensors are increasingly available for further processing and analysis in various applications. For multispectral data security, asymmetric cryptosystems employing image fusion techniques have been proposed [38, 39]. In a fusion technique, the low and high frequency components are merged together to improve the information content. The wavelet transform is the best suited candidate for fusion applications. The security of fused multispectral data is a relatively new research topic and a limited amount of literature is available. Therefore, further detailed studies and analysis must be carried out. Study from a hardware implementation viewpoint is also necessary.

With the amount of literature available on the topic, it is fair to state that the fundamental physical mechanisms governing optical asymmetric image encryption techniques are reasonably well understood. The framework is defined. In order to strengthen security in optical encryption setups, nonlinear functions must be incorporated into the optical encryption system by using optoelectronic devices. For delocalizing the ciphertext, multiple intensity planes should be recorded. For decryption, iterative phase retrieval algorithms, such as the Gerchberg–Saxton algorithm, can be used to retrieve the complex field of the ciphertext. In optical encryption setups, eliminating speckle noise in the decryption stage is one of the great challenges. Optics have promising scalability advantages over their purely electronic counterparts as, in principle, the size of the encryption key can be increased without increasing the encryption/decryption processing time.

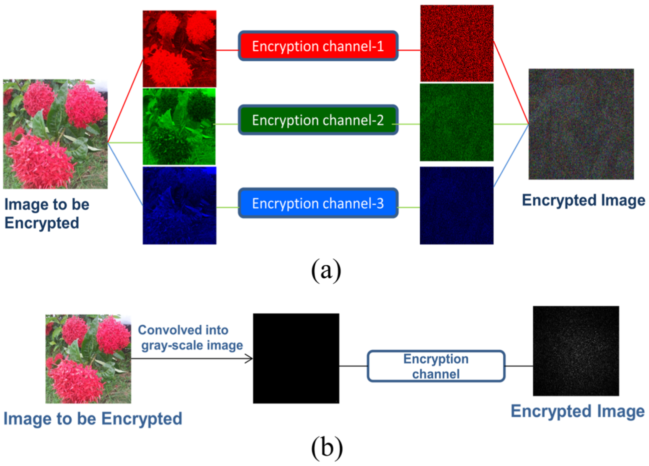

Figure 8. Block diagram for colour image encryption: (a) three channel and (b) single channel.

Concluding remarks

Optical technology is perfectly suited to scenarios where one might like to dynamically trade-off data integrity in the encryption-decryption process against efficiency. To encourage the widespread use of optical asymmetric cryptosystems, the technology should offer a cohesive and fully featured suite of practical and unique applications. It is hoped that optical security systems will take their shape and become available for various applications including watermarking and hiding of two-dimensional as well as three-dimensional information. Since the whole world is moving towards miniaturization, which is the futuristic demand, there is plenty of scope for optical security in the nanoworld. Generation of encryption keys based on plasmonics has already been reported and much more is yet to be explored.

Acknowledgments

I thankfully acknowledge fruitful discussions with Sudheesh, Isha, Dhirendra and Areeba.

5. Optical security: dynamical processes and noise-free recovery

Roberto Torroba[1] *and John Fredy Barrera*[2]

[1]Universidad Nacional de La Plata
[2]Universidad de Antioquia

Status

Aside from the security aspect given by optical methods [1, 20, 40–49], a successful dynamical encoding information exchange highly depends on non-overlapping of the decoded data, in addition to a noise-free recovering of the decrypted content. A secure multiuser and/or dynamical scheme shares a common encrypting architecture, and a single or several decoding keys depending on the access level granted to the users or the visualization of the dynamical event [40–43]. In optics, dynamical encoding is a term used to refer to a process where multiple data are handled corresponding to the time evolving scenario (movie) and ideally are combined into one package to be used over a shared medium. A 4f double random phase encoding architecture could be used, beside synchronizing the frames sequence that composes a dynamic scene constituting a movie. A modulation technique should be applied to every encrypted frame before multiplexing the sequence. In this way, during decryption the modulation technique will help in spatially separating the different frames, avoiding overlapping [40]. As a rule for efficiency, the decoding or extracting process requires a simple operation. For example, the procedure should be accomplished in one step, and all information retrieved in the corresponding time sequence. Additionally, another important issue is the noise over the decoded results generated by the encoding mechanism itself: the speckles. Despite how effective the encrypting procedure may be, there is always a residual speckle noise affecting the quality of the final decoded result. This fact conspires against the adoption of optical encryption by the general public. Unadulterated decoding demands another strategy, and the use of 'data containers' seems to be the right answer. Instead of over the message, we perform the encryption over the 'container'. Quick response (QR) codes were used as the first instrument in this new strategy [45–48]. QR code reading is resistant to speckle noise, and is widely decoded by using popular means, like smartphones or tablets. Among other breakthroughs in this field, these facts serve as impetus to the roadmap for quantifying recent progress in this area of research and in the development of new methods.

Current and future challenges

Encoding of dynamical processes has shown impressive results, although these developments are limited to rather few images. In the example of figure 9 (Media 1 and 2), we display a color movie of a drinking bird where in (a) we present the outcome of incorrect decryption with no results other than a moving speckle pattern, while in (b) we see the right decoding although polluted with speckle noise [41]. A key task is the experimental implementation of optical processors for encrypting color videos, whose recovery is made in optical or virtual optical systems. On the other hand, to show the improvements achieved by using QR codes [45, 46], in figure 10(a), a panel containing several QR codes is displayed after performing the right retrieving protocol [47]. As each code contains the information of a single character, the final step is scanning the panel using the appropriate sequence for revealing the hidden message of figure 10(b) (Media 3). The new security protocol allows the recovery of secret messages with no noise, while in classical optical security protocols the retrieved message contains noise arising from processing, as in figure 10(c). As QR codes were intended for other purposes than to serve as 'containers', they are not prepared to support large data content compatible with being speckle noise resistant. When a QR code becomes denser as the contained information increases it is affected by speckles, no longer being noise resistant. Also, they were not designed for images, so movies cannot be stored in QRs. Therefore, the goal is to achieve the design of another type of 'container' to meet the required storing capabilities but keeping the same noise response. Nevertheless, developing an appropriate system is still not easy. Over the past 20 years, the field of optical cryptography has grown, but is still an amazingly fertile source of inspiration for fundamental research. Including other facts to be explored, we need to meet the challenge of large encoded packages handling. Likewise, we need modification of the encrypting optical architectures to make them compact, while preserving the security of the process.

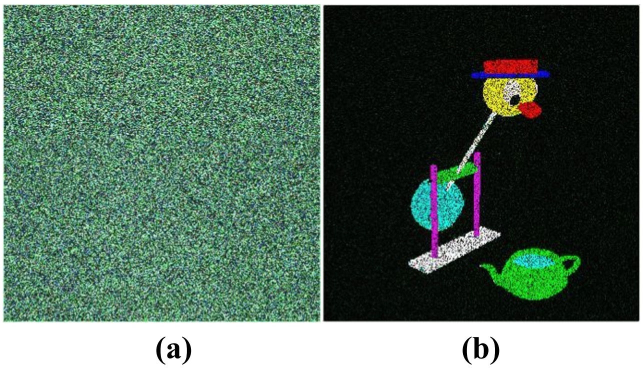

Figure 9. Decryption of a video: (a) wrong decoding, (b) right decoding showing a drinking bird (see supplementary data stacks.iop.org/JOPT/18/083001/mmedia, Media 1 and 2, respectively) (reproduced with permission from [41]).

Advances in science and technology to meet challenges

Although many advances in the physics of these problem have been made, we still need to develop new contributions in optical security that allow an implementation of dynamical processes in real time. This last requirement implies improvements in the optical architectures already in existence, and alternative strategies to deal with sequential encoding. The detailed sequential mechanism and role of different arrangements to avoid image overlapping are still a

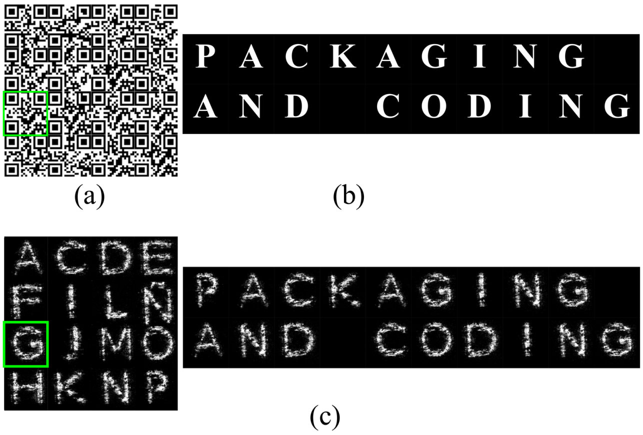

Figure 10. (a) QR panel, (b) recovered message with the proposed protocol (see supplementary data stacks.iop.org/JOPT/18/083001/mmedia, Media 3), and (c) message retrieved with the classical procedure (reproduced with permission from [47]).

question of discussion, even for the simplest optical system. As is well known, pupil size determines the cut off frequency for the input image content. Consequently, when we are thinking about the extent of a given movie we have to balance the frequency content on any given input frame versus the number of frames contained in the movie. As the input object is simpler, we can manage a larger number of frames without further degrading the image. Certainly, we envisage alternatives that when combined will influence movie quality, but this comprehensive analysis will be the subject of future innovations. On the other side, we need some technological borderlines to be pushed forward, like designing a prototype for *in situ* encoding-decoding. Speckle noise induces potential clients of the method to be reluctant to widely accepting it for their operations; therefore the development of 'containers' seems to be the next challenge to meet. The display of the input into the optical encoding processor, either in a dynamical event or in multiple data, besides its processing and synchronization during encrypting and recovering, also requires a technological development that reflects and handles at a convenient rate the actual evolution of the situation. This implies that the encrypting mechanism also must follow the same rate. Along the same line, another objective is the theoretical proposal and consequent design and experimental implementation of new optical elements and electro-optical devices, aimed to improve the performance of optical cryptosystems.

In an era where computing resources are seemingly becoming unbounded, there is a tendency to address the subject solely using computer simulations, but basic laboratory approaches are needed as technological launchers that will help in future applications.

Concluding remarks

The chief progress necessary to meet the challenges listed above is the acceptance of dynamical encrypting methods as a common tool by the community. Optical security with quality services (noiseless) is a significant barrier to making it adopted by a public system. The use of 'containers' in dynamical or steady optical encoding protocols establishes an efficient approach. Over the last year, QR codes have appeared on the horizon as a new tool in this regard. However, the larger the amount of symbols used, the denser the QR code becomes. Therefore, when the sizes of inner blocks and individual speckles compete with each other, then QR codes are no longer noise resistant to speckle noise. To overcome this practical problem, the challenge is to design new data reservoirs. In this sense their use in optical encrypting protocols keeps dynamical encrypting methods as promising candidates for future public adoption.

Acknowledgments

This contribution was performed under grants from Estrategia de Sostenibilidad 2014-2015 and Comité para el Desarrollo de la Investigación -CODI- (Universidad de Antioquia UdeA-Colombia), COLCIENCIAS (Colombia), MINCyT-COLCIENCIAS CO/13/05, CONICET Nos. 0863/09 and 0549/12 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I168 (Argentina). John Fredy Barrera Ramírez acknowledges support from The International Centre for Theoretical Physics (ICTP) Associateship Scheme and The World Academy of Sciences (TWAS).

6. Cryptanalysis and attempts on optical asymmetric and one-way cryptosystems

Wenqi He and Xiang Peng

Shenzhen University

Status

Information security is becoming increasingly important for data protection, in particular, for higher dimensional data protection. In the past three decades the security issue addressed by optical techniques has been explored extensively due to the inherent characteristics of optics, such as capability of parallel processing and operation in high-dimensional space.

As a milestone in this field, the optical encryption scheme based on double random phase encoding (DRPE) was invented by Refregier and Javidi in 1995 [1]. Since then, a large number of research works have been reported in the scientific literature, including DRPE in the Fresnel domain, DRPE in the fractional Fourier domain, and DRPE in other transform domains. The concept of DRPE has been combined with other optical techniques such as digital holography, joint transform correlator (JTC), as well as photon counting imaging. In addition to encryption, other security issues have also been addressed from an optics point of view, including authentication based on interference, coherent diffractive imaging, ptychography, and phase-space optics [44]. On the other hand, Carnicer *et al* first pointed out a potential security risk of the DRPE-based optical cryptosystem from the perspective of cryptanalysis in 2005 [50]. Soon after, Peng *et al* also presented an effective attack on DRPE by taking advantage of the phase retrieval algorithm [51]. Moreover, Peng's method can be modified to break down most derivative optical cryptosystems that originated from the DRPE technique, due to their common property of linearity.

Nevertheless, it is worth being aware that, from the historical view of developments of traditional security technologies, the theories and techniques concerning 'encryption' and 'cryptanalysis' are always a pair of rivals and compete with each other. This intensive competition has promoted further developments for both of them in the long run [52]. To this point, it is clear that optical information security researchers should make continuous efforts in designing various schemes for data security systems while evaluating security strength at the same time.

Current and future challenges

As mentioned above, the major security flaw that exists in current optical cryptosystems originates from the linear nature of the involved optical transformation. This security flaw brings fatal damage to the reliability of most currently developed optical security schemes. For example, a phase retrieval algorithm could always be applied to find the plaintext by extracting the secret key(s) of an optical cryptosystem with the help of some prior knowledge, e.g. plaintext-ciphertext pair(s), or even just ciphertext(s). It should be noted that the prior knowledge can come from Kerckhoffs' principle, which is regarded as a fundamental rule in the field of cryptanalysis [52]. One possible solution to overcome the security flaw due to the linearity lies in exploring a nonlinear optical transformation that can be used to construct optical cryptosystems. The concept of combining DRPE with photon counting imaging would be one good attempt in this endeavor.

Another big challenge is how to realize those proposed optical security schemes with optoelectronic devices and systems. Unfortunately, most reported works in this area are limited to exploiting theoretical feasibilities of optical cryptosystems while successful experimental demonstrations, even in the early stage of proof-of-concept, appear much less. This awkward situation is mainly caused by a paradox between off-the-shelf available optical components/devices and desired ones. Unavoidable systematical errors are another reason that doing optical security technique experiments is troublesome.

For now, let us turn to the theoretical attempts in the field of optical information security. We would like to mention that most of the contributions are categorized into three areas [52]: (1) image encryption, (2) information hiding, and (3) personal authentication. But for their further sub-classes, there are still some important issues that need to be explored, e.g. optical asymmetric cryptosystems and optical one-way cryptosystems. And the major challenge at this stage is that it is not a trivial task to dig out an optical theory or technique to construct an effective one-way function with trap-door or good performance of the avalanche effect.

Advances in science and technology to meet challenges

As already mentioned, one of the major challenges in optical information security is attributed to the lack of a suitable nonlinear optical transform to construct an asymmetric optical cryptosystem and/or an optical one-way Hash function. To do this, we would like to introduce some of our research efforts in this direction. One of our preliminary attempts was to construct an 'optical compressive function' (phase-truncated Fourier transform, PTFT). PTFT was exploited to create an optical Hash function in an optical one-way cryptosystem while having to fulfil the basic requirements for a compressive function: (1) the length of output bits is much less than that of inputs; (2) the implementation process should be irreversible. Thus, it is straightforward for us to cascade a series of PTFTs combined with some digital manipulating skills to design an optical one-way cryptosystem (also known as the Hash function). [53]. Another work involved constructing an optical asymmetric cryptosystem [31]. The proposed PTFT (refer to [31, 53] for more details) is easily implemented with digital and/or optical methods. And it has been confirmed that the created optical Hash function has an incredible avalanche performance, which is almost the same as MD5 and SHA-1. However, this proposed technique requires too many digital operations, making its optical realization unpractical. Meanwhile, we have also developed an optical asymmetric encryption scheme based on PTFT, in which the encryption keys differed from the decryption keys. Although it seems to have violated the basic principles for a strict asymmetric cryptosystem, e.g. the trap door information becomes a part of the ciphertext, resulting in sacrificing critical features [54], it was still regarded as a valuable exploration. Furthermore, it should be pointed out that although the operator PTFT is a linear process, it involves a nonlinear operation (phase truncation) introduced to the output. This feature also gives rise to a weakness for attackers [55].

Therefore, it is necessary to continue research efforts in searching for a more efficient nonlinear optical transformation to enhance the security strength of current optical cryptosystems. In our opinion, advances in nonlinear optics and even phase-space optics may provide some opportunities to explore new versions of enhanced optical cryptosystems. Meanwhile, micro- and nano-fabrication facilities such as laser direct writing lithography (LDWL) and electro-beam lithography (EBL) have become increasingly popular, leading to the possibility of fabricating some compact and integrated optical devices and systems with the functionalities of encryption or authentication. This will further push forward the applications of optical security technologies.

Concluding remarks

In conclusion, we have briefly reviewed state-of-the-art of optical security approaches with an emphasis on asymmetric optical cryptosystems and optical one-way cryptosystems. Further efforts to search for more efficient nonlinear transformations in order to construct an optical one-way Hash function and enhance the security strength are absolutely needed.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (61171073 and 61307003) and the Sino-German Center for Research Promotion (GZ 760).

7. Compressive sensing for optical encryption

Adrian Stern[1] *and Yair Rivenson*[2]

[1]Ben-Gurion University of the Negev
[2]University of California, Los Angeles

Status

Since its first publication a decade ago, the innovative theory of compressive sensing (CS) [56] has taken the scientific community by storm. Its potential application for digital and optical encryption was also recognized by several research groups. In recent years there has been a rapid increase in the number of publications that combine CS theory with optical encryption techniques.

CS is a signal acquisition theory that provides a framework for sensing and reconstructing an N-dimensional signal $\mathbf{f}$ with $M < N$ measurements, $\mathbf{g}$, using a linear sensing scheme, $\mathbf{g} = \mathbf{\Phi f}$. CS relies on the assumption that the object, $\mathbf{f}$, is sparse or it has a sparse representation in some domain. This assumption holds true for all human intelligible images. The sensing matrix $\mathbf{\Phi}$ must obey some information preserving properties [56]. For universal sensing, the most common type of sensing matrix $\mathbf{\Phi}$ is a random matrix, that is, a matrix with i.i.d. entries drawn from a Gaussian, Bernoulli or sub-Gaussian distribution. In such a case, only $M = \mathcal{O}(K\log N)$ samples are required for full recovery of $\mathbf{f}$, where K denotes the number of non-zero elements in $\mathbf{f}$. Other common types of sensing matrices are composed from random ensembles of vectors chosen from some unitary basis (e.g. Fourier, Fresnel, Hadamarad). The signal $\mathbf{f}$ is reconstructed from the measurement by applying an l_1 minimization or greedy algorithms [56].

The impetus for using CS for encryption is the random type of transform together with dimensionality reduction (compression). The obtained 'image' $\mathbf{g} = \mathbf{\Phi f}$ has: (1) a lower dimension ($M < N$), and (2) is visually unperceivable. The random matrix $\mathbf{\Phi}$ can be considered as an encryption key. For common image size, N, the keys space spanned by all possible random $\mathbf{\Phi}$ is extremely large.

Figure 11 shows an example of a combination of CS with the well-known double random phase encoding (DRPE) encryption scheme [1]. Such a combination was first proposed in [3], for super-resolution purposes. Obviously, such a system poses the encryption properties of the DRPE augmented by the CS. The plaintext image, $f(x, y)$, of N pixels, is multiplied by a random phase mask (RM1) with the same amount of pixels. The resulting field passes through a 4f system with another random phase mask (RM2) of N pixels located in the Fourier plane. The output field $g(x, y)$ is captured with a sensor that has $M < N$ pixels. The overall system can be regarded as a CS system with random entries [3]. The entropy of the encrypted image in figure 11(c) is with more than 10 bits/pixel higher than of the plaintext. The plaintext $f(x, y)$ is recovered from the ciphertext $g(x, y)$ by using algorithms prescribed by CS theory (in this example TwIST [56]). The reconstruction mean square error in this example is negligible (MSE ~ 10^{-5}). For the setup shown in figure 11 the phase masks act as keys and CS is utilized to allow a detector with fewer pixels than the encoded image.

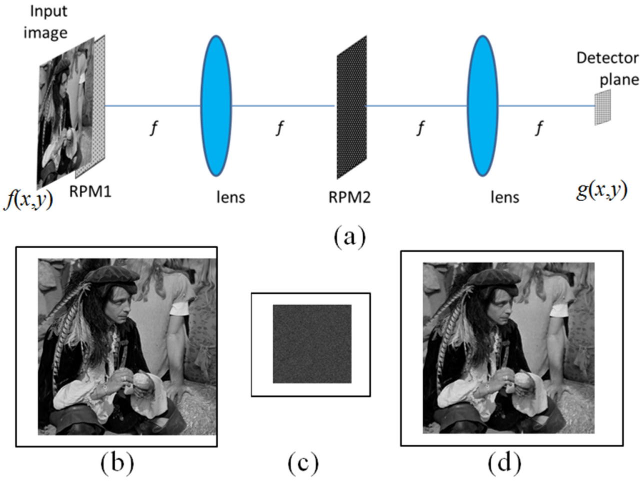

Figure 11. (a) CS-DRPE scheme. (b) Plaintext image (1024 × 1024 pixels). (c) Encrypted image (400 × 400 pixels.). (d) Decrypted image (reconstruction mean square error of 10^{-5}).

During the past few years several techniques have been proposed that combine CS with optical encryption. Here, adopting a system point of view, we offer a taxonomy according to the way the CS is included in the optical encryption:

1. Encryption techniques that use a digital CS step in addition to a common optical encryption scheme (e.g. [57–59]). With these techniques a digital CS process is typically applied on the input image. The CS compressed data is then introduced to a standard optical encryption step (e.g. DRPE). The digital CS step works as an additional encryption layer and as a preconditioner to the optical encryption step.

2. Encryption techniques that utilize CS within the optical setup. For example, the CS approach has been embedded with various DRPE schemes (e.g. [60, 61]), included in holographic schemes (e.g. [62]), applied with various ghost imaging schemes (e.g. [63] and section 13) and for photon entangled sensing (e.g. [64, 65]).

Current and future challenges

The benefits, limitations, and challenges in using CS for optical encryption are given in this section. The main benefit of CS-based optical encryptions is the combined encryption-and-compression performance (see also section 8). Encryption and compression are related, therefore a holistic, or at least combined, approach is natural. Combined encryption-and-compression optical techniques were pursued before the introduction of CS in the field with limited success [32]. CS theory introduces a powerful boost toward this aim. The joint approach offers several benefits:

1. Reduction of the encrypted image acquisition effort. Due to the dimensionality reduction property ($M < N$),

systems that embed CS in the optical encrypting step have smaller cipher texts therefore smaller sensors arrays are required. This is important if the cipher text is captured with expensive sensors (e.g. phonon counting sensors that can be used in quantum imaging, see section 16). It is also useful if very large images need to be encrypted; in such a case the optical compression may reduce the image to be captured to the size of standard imaging arrays. In applications that would normally employ a scanning process to capture the cipher text, the CS approach may significantly shorten the overall acquisition time and suggest a more economical use of photons for low-light-level [65].
2. Cipher text size reduction. This may enable efficient and secure information exchange due to reduction in the amount of information transmitted and stored.
3. Additional encryption layer. If the key $\mathbf{\Phi}$ is safe, then the CS step can be considered as an additional encryption layer that improves the security of the overall encryption process. This encryption layer may include, for example, random placement of the sensor detectors.
4. Preconditioning the input signal for the optical encryption system. A digital CS applied on the plaintext reduces its dimension; therefore such a step can be beneficial when applied prior to the field propagation through the optical system with a limited space-bandwidth product.

Nevertheless there are several limitations and challenges in application of CS for optical encryption:

1. For a completely random sensing matrix $\mathbf{\Phi}$ enormous storage and memory resources are required. Therefore if it is used as an encryption key it renders too large to distribute and memorize or store. Nevertheless, in applications in which the matrix $\mathbf{\Phi}$ can be deliberately chosen (e.g. displayed on an SLM) there are several solutions to this problem, such as generating it from pseudorandom sequences, and others such as in [66].
2. Compressive sensing is a linear process and therefore suffers from the common weakness of linear encrypting systems. In terms of encryption, CS is suboptimal from a theoretical point of view [67]. For instance its security is limited because $\mathbf{\Phi}$ can be recovered, in principle, from N linearly independent plaintext-cipher text pairs by solving a linear system of equations with the $M \cdot N$ entries of $\mathbf{\Phi}$ as unknowns. Even less effort is needed for this purpose if the matrix is generated by a pseudo-random matrix [68]. Another source of vulnerability is due to the fact that the encoded information yields a non-uniform distribution of the cipher image which leaks statistics to the analyst.
3. The decompression process requires nonlinear algorithms which are much more involved than linear operations.

Advances in science and technology to meet challenges

From a technological point of view, CS-optical encryption is limited by the individual limitations of optical encryption designs and of optical CS designs [69]. Probably the most prominent ones are the limited size, time response of commercial spatial light modulators, their high cost, dynamic range of the components, and limitation related to incoherent optical realization.

From a system design point of view, CS-optical encryption is still in its infancy. Basically all the CS-encryption schemes proposed until now are based on existing optical encryption schemes (e.g. DRPE, ghost imaging), with some modifications or additional steps. There is room for new designs that may offer improved performance.

Concluding remarks

The utilization of CS in optical encryption schemes may provide valuable benefits. The main benefits are due to addressing the issues of encryption and compression jointly. Besides the regular benefits of compression (e.g. reduction of the transmitted and stored information), encryption techniques that have CS embedded in the optical step may possess unique benefits that would be otherwise difficult to achieve with alternative optical schemes. For instance, they facilitate implementations that require exotic and expensive sensors. Additionally, CS included in optical encryption offers an additional encryption layer. This increases the complexity of the system and therefore increases its security. However we should keep in mind that CS is designed as a sensing theory therefore it is not optimized for encryption, nor for compression. Consequently, if CS is implemented digitally in conjunction with an optical encryption step, its advantages and disadvantages should be evaluated in comparison to alternative digital processes (e.g. nonlinear ones) in terms of security and computational complexity.

As a last remark, as already pointed out before, all the CS-based optical encryption techniques presented until now rely on ‘classical’ optical encryption techniques. We believe that the development of new, independent schemes may offer additional improvements in terms of encryption performance, optical implementation complexity and cost.

8. Advances in secure optical image processing approaches

A Alfalou[1] *and C Brosseau*[2]

[1]ISEN-Brest
[2]Université de Brest

Status

The ability to realize secure optical image processing (OIP) is important for a range of applications, e.g. optical encryption for data transmission [1, 70], images or video streams for information technology security, ranging from biometric authentication over digital image forensics to visual passwords [70, 71]. Here we focus on optical techniques allowing us to encrypt images and identify targets in a given scene along with their limitations and constraints. In many applications, secure OIP represents a first stage of a complex hybrid (optical-numerical) protocol, i.e. optics is used to encrypt an image and/or search for a target in a scene while a numerical step is applied in a second stage [70, 71]. Thus, a second physical encryption key increases the security level.

Current and future challenges

Compression and encryption

Optical encryption has emerged as a framework for studying information processing [6, 32, 44, 70]. However, it is well established that the standard double random phase encryption (DRPE) exhibits vulnerability to various attacks, as shown in [6, 32, 44], and it requires a large number of bits to encode the output plane. Hence, a compression method is necessary [72–74]. Image compression can be classified as lossy or lossless. Lossless compression, e.g. the Lempel–Ziv–Welch technique, is preferred for archival purposes and is often used for medical imaging. Lossy compression methods, e.g. JPEG, especially when used at low bit rates, introduce compression artifacts. Lossy methods are especially suitable for natural images such as photographs in applications where minor (sometimes imperceptible) loss of fidelity is acceptable to achieve a substantial reduction in bit rate. The choice of the compression method is related to the given application and depends on the encryption technique.

Recent simultaneous (or not) encryption and compression techniques have generated interest (figure 12) [80]. A first approach consists of realization image compression and then its encryption. Overall, this procedure provides a good quality reconstructed image at the output of the system, but is clearly detrimental to image reconstruction since it requires a lot of information. A second scheme consists of first encrypting the image and then applying a compression technique. This scheme allows a significant decrease of information size at the system output but generally does not provide a good quality reconstructed image. A third technique consists of simultaneously realizing encryption and compression [72, 74].

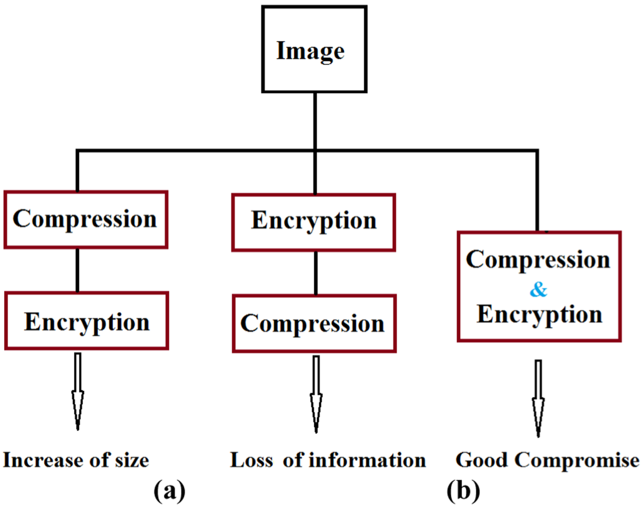

Figure 12. Three approaches: (1) compression followed by encryption; (2) encryption followed by compression; and (3) compression and encryption realized simultaneously.

This analysis allows us to find a compromise between compression rate and quality of the reconstructed images for target detection applications. Several methods have been reported in the literature to deal with image encryption and compression, i.e. a method based on the 4f optical setup and a specific fusion without overlapping of the target image spectra [72, 74–76].

The basic principle is based on three concepts: (1) a local choice of relevant spectral information coming from each target image, (2) the shift of the different spectra according to a criterion calculating the minimum size of a given spectrum (root square mean-duration), and (3) a fusion of different relevant spectral information, without overlapping, to carry out a good compression and encryption. A wealth of studies has appeared to reduce the size of useful information required for reconstruction of the target image by holographic techniques [77–79, 81]. However, there is a paucity of methods dealing with simultaneous compression and encryption of multiple images which resemble each other, e.g. images in a video sequence. Within this context, it is interesting to refer to [77], which deals with a small part of a specific spectrum and can be used in the optical encryption domain. Recently, [80] presented a method of compression and encryption based on the discrete cosine transform (DCT) that makes it possible to multiplex digital holograms.

During the last decade, there has been a growing level of interest in proposing new algorithms of image encryption [1, 32, 35, 77, 81, 82, 83, 84] but they are detrimental to compression. Other encryption techniques such as those based on the fractional Fourier transform [85], DCT and Arnold transform [82], quantum cryptography [86] and chaotic cryptography [87] have received considerable attention and can be reliable tools to advance this field.

Correlation

Correlation between images has most recently been studied in numerical simulations and experimental observations for face recognition applications. Interest in the field of correlation techniques has been recently rekindled due to their high discriminating power, their high robustness against various types of noise, and because they allow us to simultaneously identify and determine the spatial position of specific images in a scene. Two important architectures implementing correlation are the joint transform correlator and VanderLugt correlator [71]. Additionally, the use of specific treatments of the input and correlation planes permits significant a increase in the correlator's performance. These methods are found to have significantly superior correlation discrimination capability and provide better decisional performances of the correlator. Intense interest in optical correlation techniques over a prolonged period has focused substantially on filter designs. By specifically considering the input and output planes, correlation performances can be significantly increased. In spite of the aforementioned achievements, optical processing techniques continue to suffer from the point of view of optical implementation. While images are originally optical, digital processing is often realized to fully exploit their information content. As the resources required for all-optical processing come within experimental reach, it is desirable to develop a toolbox sufficiently versatile to allow the implementation of a wide class of optical schemes.

Advances in science and technology to meet challenges

A powerful approach to secure OIP task requires: (i) encryption methods which optimize the information size to be encrypted and which are adapted to the transmission channel and/or storage capacity [74]; (ii) consideration of correlation as part of a decision making system, e.g. based on fuzzy logic [88]; (iii) the development of hybrid techniques (numerical-optical using an optoelectronic interface) as substitutes for all-optical techniques which are not the universal panacea and have their drawbacks and stringent requirements, i.e. aberration effects, alignment of components, limitation of the overall speed by how fast the information can be updated on the input and output devices, and need of a costly optoelectronic interface. Furthermore, use of optics cannot be justified for many applications, especially when the target image size is small. Moreover, recent advances in reprogrammable targets such as GPUs, or field-programmable gate arrays (FPGAs) make it possible to manipulate computer graphics efficiently and process large blocks of data rapidly.

Concluding remarks

Overall, OIP is useful in applications in which high parallelism and real time processing can be effectively realized. Although the methods of optical pattern recognition by correlation have a long history, OIP techniques designed for encryption and compression are still in their early days. There are a number of directions into which the field is likely to move in the coming years, e.g. promote architectures allowing us to perform simultaneously optical compression and optical encryption. Moreover, we believe that hybrid techniques, e.g. numerical implementation of correlation, can be considered an alternative to all-optical methods because they show a good compromise between performance and simplicity. Various compression and encryption methods were discussed in this article, see sections 9 and 15. In our section, we focused on describing methods of simultaneous optical compression and optical encryption based on (1) the Fourier transform and (2) special and nondestructive selection of information in the spectral domain.

Acknowledgments

The Lab-STICC is part of Unité Mixte de Recherche CNRS 6285. E-mail: ayman.al-falou@isen.fr.

9. Attacking linear canonical transform based double random phase encryption systems

Changliang Guo and John T Sheridan

University College Dublin

Status

We discuss the application of several new iterative phase retrieval algorithms which have recently been used to perform known plaintext ciphertext attacks (KPCAs) on linear canonical transform (LCT) based amplitude encoding (AE) double random phase encryption (DRPE) systems.

Many optical encryption techniques have recently been proposed potentially capable of encrypting large quantities of information in parallel when employing the two-dimensional (2D) imaging capabilities of optics and the parallelism achievable when using optical signal processing. Since Refregier and Javidi proposed the DRPE method in 1995 [1], many optical encryption techniques have been developed which employ variations of the classical Fourier transform (FT) based DRPE system such as the fractional Fourier transform (FRT) [89], Fresnel transform (FST) [90], linear canonical transform (LCT) [93] and gyrator transform (GT) based DRPE systems [94].

Cryptanalysis of the FT based AE DRPE system was first reported by Carnicer [50] in 2005 who proved that the classical FT based AE DRPE system has a security flaw against chosen-ciphertext attack (CCA). In [95, 96] the authors proposed three iterative new phase retrieval algorithms, the Spatial Phase Perturbation GS algorithm (SPP GSA), the Gerchberg–Saxton/Hybrid Input Output algorithm (GS/HIOA) and the Error Reduction/Hybrid Input Output algorithm (ER/HIOA). The first two algorithms are used to perform KPCA on both AE and phase encoding (PE) FT based DRPE systems. In the AE case cipher only attacks were also examined.

Current and future challenges

When using FST, FRT and general LCT based AE DRPE systems, additional alternate keys are introduced that make the DRPE system more robust against various kinds of attack. For example, in the FST based AE DRPE system, the wavelength λ, and the distance parameters z_1 and z_2 in the systems provide additional keys to achieve higher security [90–92]. To our knowledge, methods of attacking FST, FRT and LCT based AE DRPE systems are only now beginning to be fully examined.

Advances in science and technology to meet challenges

In this paper we will discuss KPCAs on LCT based AE DRPE systems, i.e. given an input and the corresponding ciphertext from an LCT based AE DRPE system, both random phase keys, (RPKs), D1 and D2 are determined.

LCT based AE DRPE systems

The LCT [93] is a three-parameter class of linear integral transform. The 2D separable LCT of an input image field I is:

$$\Theta_{\alpha,\beta,\gamma}\{I\} = C_1 \iint_{-\infty}^{+\infty} I \times \mathbf{exp}\{\mathrm{i}\pi[\alpha(x^2+y^2) - 2\beta \times (ux+vy) + \gamma(u^2+v^2)]\}\mathrm{d}x\mathrm{d}y \tag{2}$$

As a variation of the FT based AE DRPE system, the LCT based AE DRPE system is given by [93]

$$E(x'', y'') = \Theta_{\alpha_2,\beta_2,\gamma_2}\{\Theta_{\alpha_1,\beta_1,\gamma_1}\{I \times D1\} \times D2\}, \tag{3}$$

where $D1(x, y) = \mathbf{exp}\{\mathrm{i}2\pi n_1(x, y)\}$ and $D2(x', y') = \mathbf{exp}\{\mathrm{i}2\pi n_2(x', y')\}$.

The encrypted image $E(x'', y'')$ can then be rewritten as

$$E(x'', y'') = \mathbf{exp}\{\mathrm{i}\pi\gamma_2(x''^2 + y''^2)\}\mathbf{FT} \times \{\mathbf{FT}\{I \times D1'\} \times D2'\}, \tag{4}$$

where

$$D2' = D2 \times \mathbf{exp}\{\mathrm{i}\pi[\gamma_1(x'^2 + y'^2) + \alpha_2(x'^2 + y'^2)]\}.$$

In this case $D1' = D1 \times \mathbf{exp}\{\mathrm{i}\pi\alpha_1(x^2 + y^2)\}$.

Known plain text attack

For a KPCA process, the input image $I(m, n)$ and the ciphertext $E(m'', n'')$ are available to the attacker. The first step in the process is to determine the parameter γ_2 which is used as the chirp multiplication. The parameter γ_2 appearing in equation (4) can be found by searching between 0 and 1 in increments of $\Delta\gamma$. We denote the lth value in this search by $\gamma_l = \Delta\gamma l$. The total number of increments is denoted by L, therefore $\Delta\gamma L = 1$.

The following equation describes the decryption process.

$$|\mathrm{FFT}\{I(m, n) \times D1'\}| = |\mathrm{IFFT}\{E(m'', n'') \times \mathbf{exp}\{-\mathrm{i}\pi\gamma_l[(m'')^2 + (n'')^2]\}\}| \tag{5}$$

$|\mathrm{IFFT}\{E(m'', n'') \times \mathbf{exp}\{-\mathrm{i}\pi\gamma_l[(m'')^2 + (n'')^2]\}\}|$ represents the lth guessed amplitude in the Fourier domain (Fourier image), while $I(m, n)$ is the amplitude in space domain (object image).

Given the lth guessed Fourier image and the object image $I(m, n)$, we can apply the HIOA to perform iterative phase retrieval. Our method involves performing one iteration using the HIOA for each estimated chirp multiplication parameter value γ_l, i.e. $\mathbf{exp}\{-\mathrm{i}\pi\gamma_l[(m'')^2 + (n'')^2]\}$. We then calculate the sum-squared-error (SSE) value (discussed later) between the retrieved amplitude in the Fourier domain and the given lth guessed amplitude in the Fourier domain. The SSE values found following one iteration of the HIOA for each of the chirp multiplication factors, i.e. $\mathbf{exp}\{-\mathrm{i}\pi\gamma_l[(m'')^2 + (n'')^2]\}$, for $l = 1, 2, \ldots, L$, are obtained. The chirp multiplication that results in the lowest SSE value is used to determine the most appropriate γ_l value, which is denoted by γ'. During this process the same random phase in the Fourier domain is employed at the start of the phase retrieval process for each of the L estimated amplitudes in the Fourier domain, i.e.

$$|\mathrm{IFFT}\{\boldsymbol{E}(\boldsymbol{m}'', \boldsymbol{n}'') \times \mathbf{exp}\{-\mathrm{i}\pi\gamma_l[(\boldsymbol{m}'')^2 + (\boldsymbol{n}'')^2]\}\}|.$$

Following the determination of γ', equation (6) can be rewritten as

$$|\mathbf{FFT}\{\boldsymbol{I}(\boldsymbol{m}, \boldsymbol{n}) \times \boldsymbol{D1}'\}| = |\mathbf{IFFT}\{\boldsymbol{E}(\boldsymbol{m}'', \boldsymbol{n}'') \times \mathbf{exp}\{-\mathrm{i}\pi\gamma'[(\boldsymbol{m}'')^2 + (\boldsymbol{n}'')^2]\}\}| \quad (6)$$

In the next step, GS/HIOA is used to perform KPCA to retrieve the correct RPKs. In order to proceed we define the SSE:

$$\mathbf{SSE} = \mathbf{10log}_{10} \times \left\{\frac{\sum_{m=1}^{M}\sum_{n=1}^{N}\{|\boldsymbol{F}'(\boldsymbol{m}, \boldsymbol{n})| - |\boldsymbol{F}(\boldsymbol{m}, \boldsymbol{n})|\}^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}\{|\boldsymbol{F}(\boldsymbol{m}, \boldsymbol{n})|\}^2}\right\}. \quad (7)$$

In all the cases examined $\boldsymbol{I}'$ and $\boldsymbol{I}$ denote the decrypted and initial images which are of size $M \times N = 128 \times 128$.

The GS/HIOA [95, 96] is applied to retrieve the LCT based AE DRPE RPKs. The process for performing the KPCA is illustrated in figure 13.

In this process applied here the GSA is applied once and then the HIOA is applied for 39 iterations. This process is repeated. We designate this algorithm GS/HIOA (1, 39).

Testing results

In order to test the validity of our approach, a test image, see figure 14, is encrypted using the same RPKs and the same LCT operations as were used for the original input I image field. After retrieving the RPKs, we decrypt the encrypted test image using the resulting iteratively retrieved RPKs.

The results presented in figure 14 indicate that the chirp multiplication factor γ, and the RPKs found by the GS/HIOA (1, 39) based KPCA have been accurately retrieved. Comparing the known input images and the retrieved results, a mean squared error (MSE) value of 0.16161 for the decrypted ‘Cameraman’ image above, is calculated. These provide quantitative evidence that the test image has been accurately retrieved.

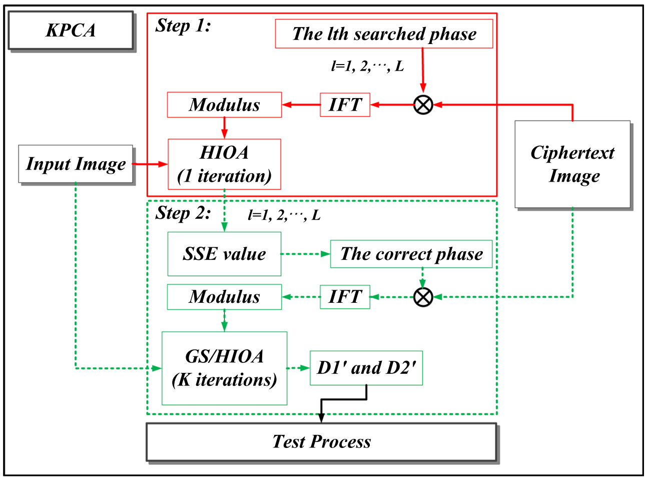

Figure 13. Flow diagram of the iterative KPCA process.

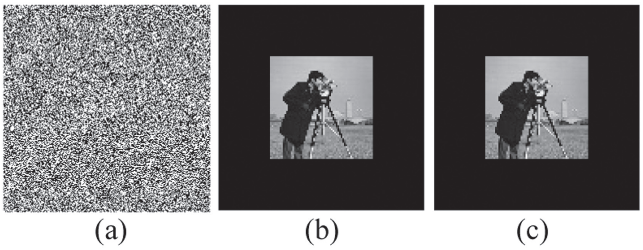

Figure 14. Testing the results of the KPCA on an LCT based AE DRPE system. Cameraman image: (a) encrypted; (b) plaintext; and (c) the decrypted image.

Concluding remarks

The vulnerability of the LCT based AE DRPE system to KPCA is examined using the phase retrieval methods developed. It is demonstrated that algorithms (GS/HIOA) can successfully retrieve the two RPKs used in LCT based AE DRPE systems.

Acknowledgments

Irish Research Council for Science, Engineering and Technology (IRCSET); Science Foundation Ireland (SFI). C Guo is supported by a University College Dublin China Scholarship Council joint scholarship. E-mail: john.sheridan@ucd.ie.

10. Security issues and the need to develop optical information security theory

Guohai Situ

Shanghai Institute of Optics and Fine Mechanics, Chinese Academy of Sciences

Status

It is well known that optical systems provide a number of advantages for the applications in information security, including parallel processing and encoding using various parameters such as phase, polarization, and even coherence. Among these, image encryption using double random-phase masks has received the most attention [1]. This is typically done using a coherent 4f imaging system, with two statistically independent random phase masks placed at the input and the Fourier planes. It has been mathematically proven that this system can transform an image into white noise. In this system, the random phase mask placed at the Fourier plane plays a more important role in decryption, serving as the key to the system. It actually can be regarded as a point in the abstract key space, which is a set composing all the possible distributions for the key. It is generally believed that the double random phase encoding (DRPE) technique is very secure as the key space has the size of $\boldsymbol{\Omega}^{\boldsymbol{M}\times \boldsymbol{N}}$, where $\boldsymbol{M} \times \boldsymbol{N}$ is the size of the random phase masks, and $\boldsymbol{\Omega}$ is the quantified level. Given an image of $\boldsymbol{M} = \boldsymbol{N} = \mathbf{512}$, and $\boldsymbol{\Omega} = \mathbf{256}$, which is of normal size, the size of the key space is equal to **22, 097, 152**, a number even larger than the number of sand granules in the Sahara desert! It is extremely unlikely to find the exact random phase keys by using a burst force attack, as the probability is on the order of finding a certain sand grain in the Sahara desert. Owing to this reason, the DRPE technique has been proposed for applications in secure holographic storage, information hiding and watermarking, authentication verification, etc. The original DRPE technique has also been extended to the fractional Fourier domain, Fresnel domain, as well as using other canonical transforms such as the Hartley transform and gyrator transform. However, not all these optical encryption techniques have undergone systematic cryptanalysis, although people usually believe that they have extremely large key space. This will lead to security issues and affect their practical applications.

Current and future challenges

It was not until 10 years after the DRPE technique was proposed that Carnicer and co-workers [50] made the first cryptanalysis to this technique. They designed a chosen-cyphertext attack by using a delta function as the input to the decryption machine, and found that one can obtain the full complex-value spectrum of the random-phase mask at the output plane, subject to a constant bias. Frauel *et al* have made a serious resistance analysis of the DRPE technique against various attacks [6]. They have found that with the knowledge of two plaintext-cyphertext pairs, one can solve a set of linear equations, and obtain the keys to the system. With the computation resources of that time, it took them 2 h to find a key of size 100×100 pixels. The linear relationship between the plaintext and cyphertext is the biggest challenge that the DRPE technique has currently encountered. Due to this linearity issue, as well as the phase modulation principle of the technique, people have developed various cryptanalysis techniques based on phase retrieval algorithms [97–99] to find the key to the system with the knowledge of a few plaintext-cyphertext pairs. These attacks have been demonstrated to be very efficient. One can refer to sections 6 and 9 for more details about cryptanalysis of such optical security schemes.

In my opinion, the other big challenge is the development of optical information security theory. So far we have already had many different kinds of optical security systems, working in either optical or numerical mode. But we need rigorous information security theory to provide a unified framework for all these optical techniques. Taking a look at the counterpart of quantum information security [100], we get an impression of what a serious situation our community is faced with. Without this theory, not to say that it is hard to communicate with colleagues in the general field of information security, we do not even have a rigorous merit to measure the security level of an optical security system.

Advances in science and technology to meet challenges

To address the linearity issue, an intuitive strategy is to develop nonlinear optical security systems. For example, we have developed an encryption scheme by taking the bilinearity advantage of the phase space distributions, such as the ambiguity function (AF) [101]. The encryption is a two-step process: we first transform the signal into its AF, which is then encrypted into white noise using any available optical encryption technique (the traditional DRPE technique was used for demonstration in our study). We have demonstrated that this encryption in phase space is resistant against various attacks including the impulse response attack designed by Carnicer *et al* [50], and phase-retrieval-based attacks [97] due to the bilinearity and complex value of the AF.

One can even replace the various canonical transforms used in traditional DRPE by a true nonlinear transform. For instance, as depicted in figure 15, one can place a photorefractive crystal such as strontium-barium niobate ($\mathrm{Sr}_x\mathrm{Ba}_{(1-x)}\mathrm{Nb}_2\mathrm{O}_6$, SBN) in between the two neighboring planes in the DRPE system, connecting them with a nonlinear, rather than linear [90], propagation that is described by the nonlinear Schrödinger equation [102]:

$$\begin{aligned}\frac{\partial\psi}{\partial z} &= \left[\mathbf{i}\frac{1}{2k\boldsymbol{n}_0}\boldsymbol{\nabla}_\perp^2 + \mathrm{i}\boldsymbol{k}\boldsymbol{\Delta n}(|\psi|^2)\right]\psi \\ &\equiv [\boldsymbol{D} + \boldsymbol{N}(|\psi|^2)]\,\psi,\end{aligned} \tag{8}$$

where $\psi(\boldsymbol{x}, \mathbf{y}, \mathbf{z})$ is the complex amplitude, $\boldsymbol{k} = \mathbf{2}\boldsymbol{\pi}/\boldsymbol{\lambda}$ the wave number, $\boldsymbol{\lambda}$ the wavelength of the laser beam in vacuum, $\boldsymbol{n}_0$ the linear refractive index and the crystal $\boldsymbol{\Delta}\mathbf{n}(|\psi^2|)$ the nonlinear refractive index, and by definition the operators D

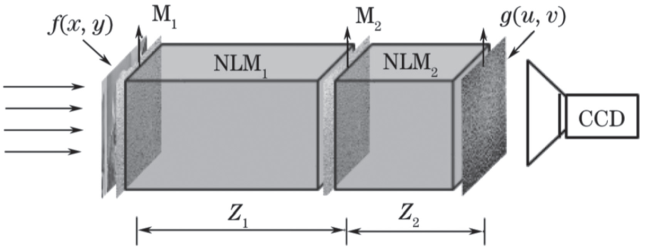

Figure 15. A proposed nonlinear optical encryption scheme. Here the linear canonical transform between two neighbouring planes in the traditional DRPE is replaced by a nonlinear propagation by virtue of the two nonlinear photorefractive crystals (NLM1, and NLM2). The linear relationship between the cyphertext and plaintext does not hold in this nonlinear optical encryption system, resulting in the enhancement of security.

and N describe the linear and nonlinear interaction, respectively, between the light and the crystal. Thus, the encryption of the plaintext $\boldsymbol{f}(\boldsymbol{x})$ can be written as

$$g(u, v) = \mathrm{NLT2}\{\mathrm{NLT1}\{f(x, y)\exp \times [\mathrm{i}\varphi_1(x, y)]\}\exp[\mathrm{i}\varphi_2(x', y')]\} \qquad (9)$$

where $\boldsymbol{\varphi_1}(\boldsymbol{x}, \boldsymbol{y})$ and $\boldsymbol{\varphi_2}(\boldsymbol{x}', \boldsymbol{y}')$ are two statistically independent random distribution in $[0,\ 2\boldsymbol{\pi}]$, and NLT1 and NLT2 denote nonlinear propagation in the nonlinear media 1 and 2, whose lengths are $\mathbf{Z}_1$ and $\mathbf{Z}_2$, respectively.

It is clearly seen from equation (8) that the propagation is now dependent on the intensity profile $|\psi|^2$. The change of refractive index is also dependent on the voltage that applies to the crystal c-axis:

$$\boldsymbol{\Delta n}(|\psi|^2) = \frac{1}{2}\boldsymbol{n}_0^3\boldsymbol{r}_{\mathbf{eff}}\boldsymbol{E}_0\frac{\bar{\boldsymbol{I}}}{1+\bar{\boldsymbol{I}}}. \qquad (10)$$

where $\mathbf{r}_{\mathbf{eff}}$ is the electro-optic coefficient relative to the applied field $\boldsymbol{E}_0$ and the crystalline c axis, $\bar{\boldsymbol{I}}$ is the input intensity $\boldsymbol{I} = |\psi|^2$ normalized to a background (dark current) intensity. Depending on the sign of the applied voltage, $\boldsymbol{\Delta n}$ can be positive or negative valued, corresponding to the self-focusing and self-defocusing modulation of the input beam, respectively. In either way, the intensity profile of the plaintext has a very strong effect on the formation of the cyphertext. Our primary numerical study shows that the random phase key function obtained using phase-retrieval-based attacks is strongly affected by the plaintext-cyphertext pairs that were known, making any attack of this kind fail to recover the original key. We are carrying out an experimental investigation on this problem now.

In comparison to the nonlinear optical encryption techniques, the development of a rigorous optical information security theory seems to be untouched. I have tried to develop the theory based on information theory, but did not succeed. One critical key point is that it is hard (or even, whether it is necessary) to define the entropy of a complex wave field, whereas the traditional information theory only deals with intensity data [103]. One may think about using the joint amplitude-phase probability distribution, or the joint real-imaginary probability distribution, as people did in statistical optics. My recent exposure to phase space optics [104] makes me believe that the Wigner distribution function may be a good starting point as well. But either way, this is a very complicated research topic.

Concluding remarks

We have highlighted two big challenges encountered in optical security: linearity and the development of optical information security theory. We have discussed the advances in addressing these issues. To address the linearity issue, we have discussed two different nonlinear optical encryption strategies. i.e. phase space optics and nonlinear propagation. It is worth mentioning that there are other techniques such as photon-counting encryption [105, 106] under development to address this issue as well. Detailed discussion can be found in section 16 of this article.

The development of optical information security theory is more challenging and more important as it will provide a framework for rigorous analysis of the security of optical security techniques. Furthermore, it will provide a bridge of communication between the community of optical security and other branches of information security; and this will be beneficial for the further development of optical security itself.

Acknowledgments

This study was supported by the National Nature Science Foundation of China under the grant 61377005, and the Recruitment Program of Global Youth Experts.

11. Optical security based on near-field processes

Makoto Naruse[1] *and Tsutomu Matsumoto*[2]

[1]National Institute of Information and Communications Technology
[2]Yokohama National University

Status

Conventional optical security technologies in use today have been facing increasingly stringent demands to safeguard against greater threats such as counterfeiting of holograms and side-channel attacks, by which information is tampered with either invasively or noninvasively; for instance, merely by monitoring electromagnetic leaks or power consumption. Hence innovative physical principles and technologies to overcome their limitations are required [107]. In this vein, optical processes in the subwavelength-scale (or optical near-fields) are able to break through the diffraction limit of conventional propagating light [108]. Moreover, optical near-fields exhibit a number of unique attributes such as localized optical energy transfer and a hierarchical nature, which strongly assist in paving the way for novel security functionalities [109]. Technologically, the geometry of nanostructures such as their size, position, shape, and layout should be well controlled to obtain the intended optical near-field interactions. The rapid progress of technologies for fabricating nanostructures, such as size-controlled quantum dots and shape-controlled metal nanostructures, has afforded a variety of device and system prototyping to come into the marketplace, including hierarchical information retrieval or watermarking [110], hierarchical holograms [111], and authentication [112, 113]. In addition, the hierarchical nature of optical near-fields allows the co-existence of optical security aspects in the propagating-light regime and in the subwavelength regime. This tendency is observed in the demonstration of the hierarchical hologram, which acts as a conventional hologram in optical far-fields, while simultaneously containing additional information retrieved only via optical near-fields (figure 16) [111].

Current and future challenges

One of the current and future challenges of optical near-fields to the domain of information security is the application of *artifact metrics* [114]. Artifact metrics use physical features unique to individual objects in terms of their physical properties, including electromagnetic, mechanical, and/or optical properties. For an artifact metric to function, it should satisfy four separate conditions: (1) individuality, (2) measurement stability, (3) durability, and (4) clone resistance. The critical-security battlefield in which artifact metrics are used is analogous to a 'defender and attacker' relationship in which the former tries to produce patterns that are difficult to copy, while the latter seeks to counterfeit such patterns. In an ultimate situation, the defender, who wants to prevent counterfeiting, must fabricate fine-structured patterns such that the attacker, who wants to copy the authentic device, will not be able to intentionally reproduce the subject pattern. However, this condition implies a *paradoxical* situation because it is assumed that high technologies for the observation and fabrication of nanostructures are available to *both* defenders and attackers. In other words, the battle is perpetual. To help overcome this paradox, one critical approach is to exploit the *physically unavoidable uncertainty* at the nanometer scale; this idea is called *nano-artifact metrics* [115], which exploits levels of physical randomness that are technologically impossible to reproduce. This concept is discussed in further detail below.

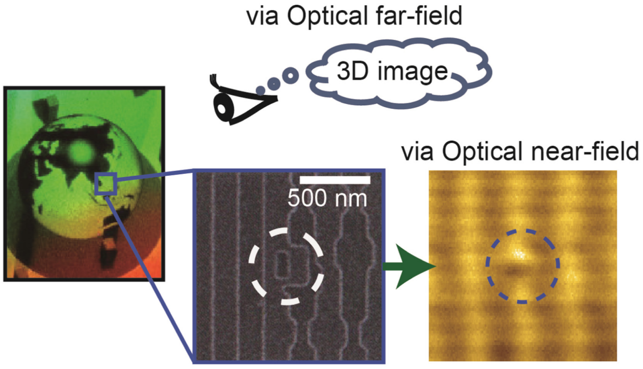

Figure 16. Hierarchical hologram that acts as a conventional hologram in the optical far-field but contains additional information retrieved only via optical near-fields.

Other important challenges of subwavelength optics include the applications of optical metamaterials or metasurfaces [116, 117] for security applications. For example, unidirectional light propagation, or non-reciprocal light propagation, made possible by optical metamaterials [118, 119], is useful for novel tamper-resistant hardware to help prevent side-channel attacks via optical channels. Unlike conventional optical isolators with electromagnetic materials, metamaterial approaches realize equivalent functions via the use of isotropic materials. Optical near-field interactions in nanostructured matter are thus playing crucial roles at present, and as such, their fundamental principles, designs, and fabrication technologies should be furthermore developed. A theoretical approach in this regard is discussed below.

Advances in science and technology to meet challenges

Silicon nanostructured patterns have been experimentally demonstrated as the first prototype of nano-artifact metrics [115]. Resist collapse in electron-beam lithography occasionally provides structures with technological limitations that are finer than the original. As an experimental trial supporting this research endeavor, an array of pillars from a layer of resist was fabricated. The pillars had a cross-sectional area of 60 nm × 60 nm, had a height of 200 nm, and were positioned on a grid of 120 nm × 120 nm squares. After post-exposure bake and resist development, the structure was rinsed, which was ultimately the juncture when the random collapse of the resist pillars occurred. Figure 17(a) shows a scanning electron microscopy (SEM) image of collapsed resist pillars. In total, 2401 samples were fabricated and evaluated per their use for potential security applications. As observed in figure 17(b), various different morphologies, with a minimum dimension smaller than 10 nm, were obtained. A false match rate (FMR), which is an indicator of individuality, and a false non-match rate (FNMR), which implies measurement stability, were subsequently calculated. As shown in figure 17(c), the FMR and FNMR curves are well separated from each other, which means that it is possible to obtain sufficiently small FMR and FNMR by choosing adequate threshold values. In addition, clone match rates (CMRs) were analyzed to quantify the difficulty of fabricating clones. Similarly, CMRs are well separated from FNMR, which implies the notion that constructing clones is altogether extremely difficult, or equivalently, the subject original authentic patterns are sufficiently random. From these results, it can be concluded that the first prototype based on silicon nanostructured patterns (formed via the random collapse of resist) could serve as a superior nano-artifact metric. Further upcoming advancements in these principles and technologies are expected, such as improvements in alignment tolerances, hierarchical information retrieval, and a host of others.

In realizing novel tamper-resistant hardware based on optical metamaterials, a theoretical foundation is indispensable for understanding underlying physical mechanisms, in addition to potential device design and optimization. Optical near-field processes that are associated with the nanostructured matter should be taken into account. In [119], the theory of angular spectrum representation of optical near-fields is successfully applied to account for unidirectional light propagation through two-layer nanostructured matter. As such, further advancements are expected in this regard in both theoretical and experimental aspects.

Concluding remarks

To transcend the fundamental limitations of far-field light, the understanding and utilization of optical processes in the subwavelength regime, and its associated technologies, are crucial. Of additional emphasis is the fact that unique characteristics made possible by near-field light and nanometer-scale physics provide novel principles for security applications.

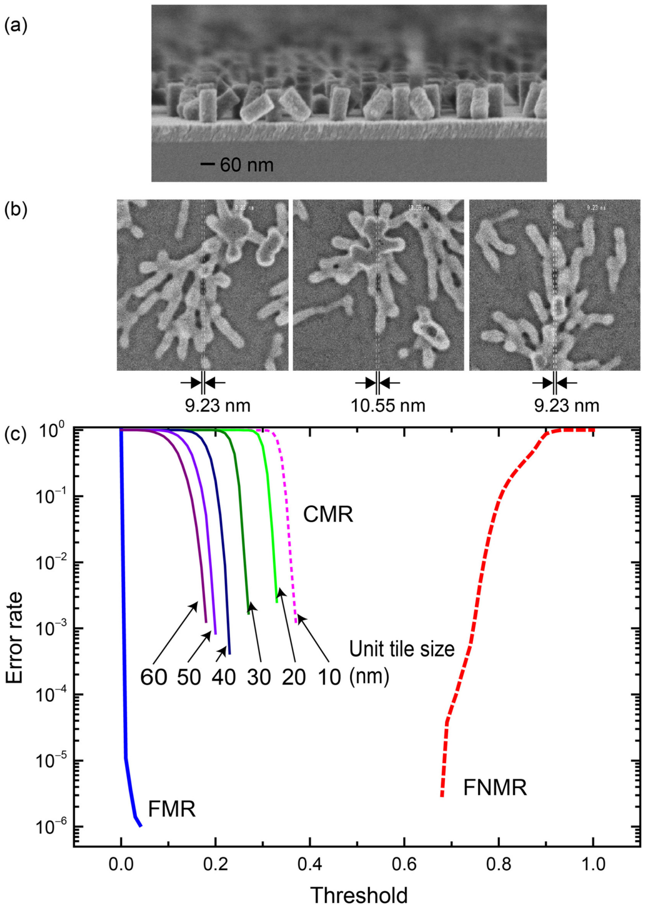

Figure 17. Nano-artifact metrics. See text for details.

Acknowledgments

The authors are grateful to N Tate (Kyushu University), M Hoga, M Ishikawa, and S Nishio (Dai Nippon Printing Co. Ltd) for their intensive research collaborations. This work was supported in part by Grants-in-Aid for Scientific Research and the Core-to-Core Program, A Advanced Research Networks from the Japan Society for the Promotion of Science.

12. Highly focused vector fields encryption

Artur Carnicer and Ignasi Juvells

Universitat de Barcelona

Status

Optical encryption techniques derived from the original double random phase encryption method have attracted the interest of many authors [1, 20]. Images can be easily encoded using a 4f system and only those who know the decryption key can access the plain-text message.

Several attacks have been described in the literature [50] but security can be enhanced by increasing the number of degrees of freedom of this approach. Among many others methods, the use of polarized light [120], a combination of real and virtual optics methods [121] or recording the encrypted distribution in photon starving conditions [15] have been suggested. In this contribution we sketch the possibility of manipulating fields in the focal area for optical security applications: the information could be encoded in the longitudinal component of the focussed field. The energy associated with this component is very weak and difficult to detect since it is embedded in the transversal part of the field. For this reason fields in the focal area could be used in optical encryption.

Current and future challenges

Paraxial beams are propagated using the Fresnel diffraction formula. In this case, the electromagnetic field is assumed transverse to the direction of propagation. Despite the fact the Fresnel framework provides very accurate results, in general, transverse paraxial beams do not fulfil Maxwell's equations because the Gauss law is not satisfied $\nabla \cdot \mathbf{E} \neq 0$. This means that, with a few exceptions (plane waves, azimuthally polarized beams), the irradiance associated with the electric field component in the direction of propagation is never zero. Since the Gauss law has to be verified, it provides a way to evaluate the longitudinal component of the field (see [122, 123]).

The description of the propagation of highly focused beams requires a more general formulation. The Richards and Wolf equation describes the behaviour of the electric field E at the focal plane of a high numerical aperture (NA) microscope lens following the sine condition [124]:

$$\mathbf{E}(r, \phi, 0) = A\int_0^{\theta_0}\int_0^{2\pi}\sqrt{\cos\theta}\,(f_1\mathbf{e_1} + f_2\,\mathbf{e_2}) \times \exp(\mathrm{i}kr\sin\theta\cos(\phi - \varphi))\sin\theta\mathrm{d}\theta\mathrm{d}\varphi. \tag{11}$$

Here, A is a proportionality constant, k is the wavenumber, r and ϕ are the polar coordinates at the focal plane, θ and ϕ are the polar and azimuthal angles at the exit pupil and θ_0 is the semi-aperture angle, i.e. NA $=$ sin θ_0. Functions f_1 and f_2 are the azimuthal and radial parts of the transverse input field E_0:

$$f_1 = \mathbf{E_0}\cdot\mathbf{e_1}\ \text{and}\ f_2 = \mathbf{E_0}\cdot\mathbf{e_2^i}, \tag{12}$$

$\mathbf{e_1}$ and $\mathbf{e^i_2}$ are unit vectors in the radial and azimuthal directions and $\mathbf{e_2}$ is the projection of $\mathbf{e^i_2}$ on the convergent wave-front surface. Note that $\mathbf{e_2}$ displays a non-zero component in the direction of propagation (see figure 18 of [125] for details). Despite fact that the incident beam is purely transverse, the electric field in the focal area E shows a non-negligible longitudinal component E_z. In general, the irradiance I_z associated with the longitudinal component is very weak compared with the irradiance of the transverse part I_t. For instance, when the input beam is circularly polarized, the value of I_z is as small as 0.3% of the irradiance of the transverse part of the beam [123].

Note that the longitudinal component of the focal electric field cannot be easily separated from the other two components using optical equipment. However, E_z could be numerically accessed by means of the Gauss law $\nabla \cdot \mathbf{E} = 0$. In Fourier space, the divergence theorem reads

$$\alpha\tilde{E}_x + \beta\tilde{E}_y + \gamma\tilde{E}_z = 0, \tag{13}$$

being $\tilde{\mathbf{E}} = (\tilde{E}_x, \tilde{E}_y, \tilde{E}_z)$ the Fourier transform of the field at the focal plane $\mathbf{E}$. Variables α and β are the spatial frequencies and $\gamma = -\sqrt{1 - \alpha^2 - \beta^2}$. Using equation (13), the longitudinal component of $\mathbf{E}$ could be determined from the transverse part of the field. Note that the transverse components of the focused field can be measured using conventional optics.

Because the irradiance I_z is small and difficult to isolate from the transverse component, it is suggested to use E_z for encoding information. In this way the message propagates with the field but cannot be easily accessed. If the message is encrypted, the proposed cryptosystem takes advantage of the properties of focused fields to improve security.

The information to be encoded in the longitudinal component determines the design of the incident beam. But notice that the polarization of the input beam is also an important issue to be taken into account. This fact opens multiples scenarios that have to be analysed in order to develop the appropriate strategy depending on the illuminating source (circular, radial, spiral, etc).

Different encryption schemes can designed using focused fields. Nevertheless, it is worth pointing out that encoding information in the longitudinal component does not improve per se the quality of encryption. It is expected that the same attacks designed to break conventional paraxial cryptosystems can be used as well. On the other hand, methods designed for avoiding such attacks can be adapted in order to be used within the context of highly focused fields. For instance, photon starved techniques [15, 106] could be good candidates for enhancing security. After propagation, the field components in the focal area hide the encrypted longitudinal component.

Advances in science and technology to meet challenges

The encryption procedure described can be implemented optically by means of an optical system able to tailor beams with custom amplitude and polarization [125, 126]. These systems enable the manipulation of arbitrary polarization information and, thus, increase the degrees of freedom available when compared with conventional scalar optical systems. Moreover, focused fields have to be described in terms of rigorous vector diffraction which is a more complex approach when compared with Fraunhofer or Fresnel propagation theories. The use of these optical systems is required in order to design an incident field that generates the designed beam in the focal area.

Figure 18 sketches the optical setup required to perform focused vector fields encryption. The system is illuminated by a collimated coherent source. The beam is split into two beams by means of a polarizing beam splitter (PBS). Reflected by mirrors M_1 or M_2 the split beam passes through translucent spatial light modulators displaying cell-oriented computer generated holograms to encode complex transmittances. The holograms encode information of the input polarization, the image to be encrypted and the random key masks. The beam is focused by means of a high numerical aperture microscope objective and then the light distribution is reflected on the observation plane (dotted line). Finally, the transverse part of the field is imaged on the CCD with the help of lens L4 and the complex light distribution is recoded using holographic techniques.

Finally, the longitudinal component is numerically evaluated and eventually decrypted using the imaged transverse part of the field.

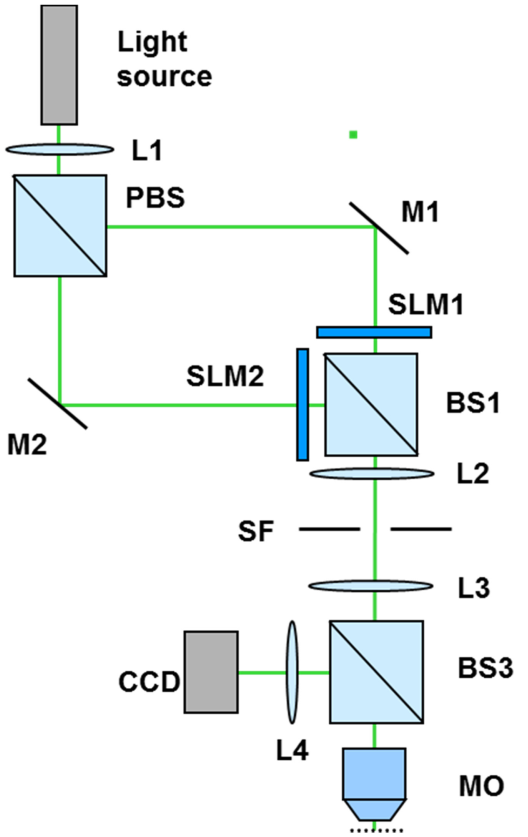

Figure 18. Focalization system and detection setup. L1 collimating lens, L2 and L3 relay optics, L4 imaging lens, M1 and M2 mirrors, PBS polarizer beam splitter, BS1 and BS3 beam splitters, SF spatial filter, SLM1 and SLM2 spatial light modulators, CCD camera, MO high NA microscope objective. The dotted line shows the observation plane.

Concluding remarks

We have outlined an optical cryptosystem based on encoding the information in the longitudinal component of a highly focused beam. The use of this design presents two advantages: (i) the irradiance associated with this component is embedded in the total detected field and (ii) the energy associated with the longitudinal component is very low. This makes detection of the longitudinal component very difficult. However, information can be properly decoded by an authorized user with access to the encryption keys by using the Gauss law. The encoding procedure has to be used in combination with nonlinear encryption techniques or in low light illumination conditions to avoid conventional attacks. The system we propose can be implemented in the laboratory.

Acknowledgments

The authors are grateful to Prof Rosario Martínez-Herrero and Dr David Maluenda for helpful discussions. This research is funded by Ministerio de Economía y Competitividad (Spain), project FIS2013-46475-C3-2-P.

13. Optical encryption by computational ghost imaging

Enrique Tajahuerce and Jesús Lancis

Universitat Jaume I

Status

Computational imaging uses digital sensors, optics, and computation, together with microstructured illumination or coded apertures, to develop novel imaging applications. It operates by optical coding followed by computational decoding, as do many optical security and encryption techniques. In fact, the well-known double-random phase encryption procedure can be understood as a secure coded-aperture imaging technique [1]. Likewise, digital holographic encryption techniques require computation to decode encrypted images from interferometric information [127]. In this section we focus on the application of computational ghost imaging (CGI) to encryption.

Computational imaging with single-pixel detectors enables spatial information to be obtained of an object by sampling the scene with a set of microstructured light patterns [128]. A simple bucked detector records the signal associated with each pattern and the image is reconstructed by mathematical algorithms. In the case of ghost imaging, the information is encoded in the correlation of the intensity fluctuations of two light signals [129]. The first, the reference signal, measures the intensity distribution of the light illuminating the object, while the second, the object signal, collects the total amount of light interacting with the object. The computational version, CGI, emulates numerically the optical propagation through the reference arm, enabling imaging the object by just a bucket detector [130].

Image encryption with CGI is a cryptography technique with a modified symmetric key [63]. The idea is outlined in figure 19(a). The coherent light beam illuminates a phase-only spatial light modulator (LCoS) codifying a set of N different random phase distributions sequentially. Propagation of the light beam generates a corresponding set of N speckle patterns onto the object (O) which can be evaluated numerically. By measuring the total intensity, the bucked detector (BD) provides the projections of the object onto the patterns. The object is recovered by correlating the speckle patterns and the measured projections. Only with the proper set of speckle patterns, the key, is it possible to recover the image of the object. The bottom pictures in figure 19 show an example of encryption. Figure 19(b) is the image to be encrypted, (c) the decrypted image, and (c) an attempt of decryption with the wrong key. An outline of the optical encryption methods is depicted in figure 20. Several encryption techniques based on this idea have recently been reported [131, 132]. A similar approach for information authentication can be seen in section 14.

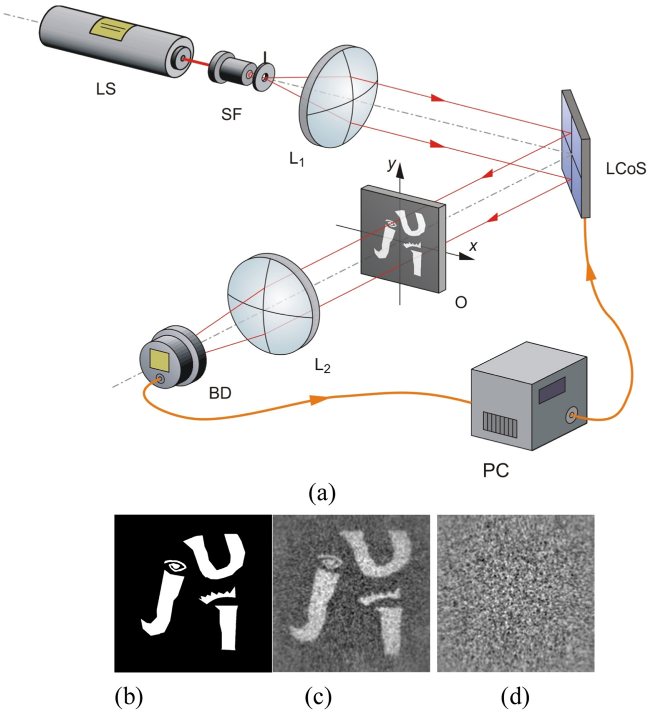

Figure 19. Optical encryption by using computational ghost imaging. Reproduced with permission from [63].

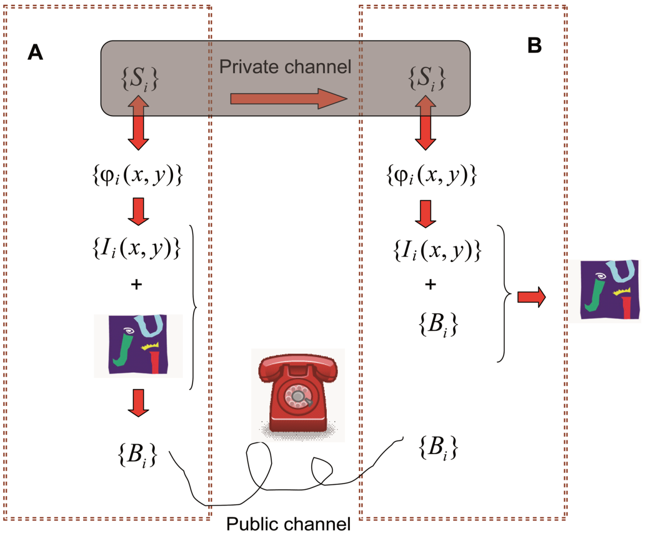

Figure 20. Outline of the optical encryption system [63]. The transmitter (A) and the receiver (B) share a secret key {Si} generating the phase distributions ϕ_i(x, y) in the SLM (LCoS) in figure 19. The information is encrypted on a vector containing the intensity values {Bi} detected by the single-pixel detector (BD) in figure 19.

Current and future challenges

Optical systems employed in encryption by CGI are simple, robust, and secure. In contrast to other optical security techniques, the encrypted version of the object is not a complex-valued matrix but just an intensity vector, which reduces the number of bits to be sent. Moreover, by avoiding sensor arrays it is possible to add new degrees of freedom to the sensing process. However there are still some limitations and challenges to face related with security, acquisition time and detection schemes.

Some recent research in encryption by CGI has focused on increasing the security of the method against eavesdropping attacks. In one approach the sensing pattern is not reproduced in the computer but measured by a digital camera, and security is increased by manipulating the correlation position of the reference and object beams [133]. One challenge in this direction could be to explore the use of non-thermal sources such as those used for quantum ghost imaging for ghost encryption.

Because of the sequential nature of the projection method, it will be crucial to decrease the acquisition time to improve the performance of this encryption technique. One approach is by using recent advances in compressive sensing techniques (see section 7). In fact, computational imaging with single-pixel techniques is very well adapted to apply compressive sensing strategies. This will improve the reconstruction quality by using the same, or even less, number of realizations. The first schemes have already been proposed both in CGI and optical encryption by CGI [134]. Another approach to reduce the acquisition time is by employing faster spatial light modulators (SLMs) operating at high frequencies. To this end, it could be necessary to find new ways to codify phase distributions. Finally, an interesting method in this direction may be to use adaptive techniques that reduce the number of sensing patterns by iterative approaches.

The single-pixel detection scheme characteristic of ghost imaging techniques should allow systems to be developed with very sensitive light sensors, to explore unusual spectral bands for imaging, or to use exotic photodetectors such as spectropolarimeters. These ideas, which have been developed already in other single-pixel imaging techniques, could improve encryption operations by CGI.

Advances in science and technology to meet challenges

As happens with other optical encryption techniques, the main advance to increase security in encryption by CGI will arise by developing non symmetric keys (see sections 4 and 6). In this way it will be possible to use public keys for encryption and private keys for decryption, avoiding transmission of the key by secure channels. We also believe that encryption by CGI will benefit from general advances in quantum imaging [129]. Most likely, the advantages of using quantum properties of light will enhance security in ghost imaging devices.

Regarding time acquisition issues, on the one hand, the development of new compressive sensing strategies will be fundamental for practical applications of encryption by CGI. Some research in this field tries to find appropriate combinations of the base of functions to generate the sensing patterns and the base of functions used to apply the compression algorithms. Also, development of encryption techniques using deterministic patterns for sampling, instead of random ones, can be the key to develop new efficient applications. On the other hand, optical encryption by CGI, as for any other single-pixel imaging technique, will benefit from the development of faster SLMs. Currently, the fastest 2D devices are ferroelectric liquid crystal SLMs, able to work at frequencies of the order of kHz, and digital micromirror devices (DMDs), which modulate patterns at frequencies of the order of tenths of kHz. A promising technique for very fast modulation is that of microelectromechanical system (MEMS) based diffractive SLMs, which are able to work at hundreds of kHz but in linear array configurations.

Advances in light detectors will have a significant impact in the development of optical encryption by CGI. The development of sensors with high sensitivity, high dynamic range and low noise will allow using fast SLMs even with low light levels. Besides, by using multidimensional detectors, able to measure different optical parameters such as polarization, phase, or spectral content, it will be possible to consider more keys, and the technique will improve into a more versatile and secure encryption method.

Concluding remarks

Encryption by CGI is a promising optical security method with several advantages over other optical approaches. The optical system is simple and robust providing a high level of security. The simplicity of the light sensor device makes it a good approach to encrypt multidimensional information. However several challenges still remain, such as the need of a symmetric key and the time required for sequential operation. Recent advances in SLM technology and light detectors will allow these encryption systems to operate at high speed. Besides, the fact that CGI comes from the evolution of quantum imaging, and therefore both techniques are closely related, could be further explored in the near future giving rise perhaps to more secure optical encrypting methods.

Acknowledgments

We acknowledge financial support from MINECO (grant FIS2013-40666-P), Generalitat Valenciana (grants PROMETEO2012-021 and ISIC 2012/013), and Universitat Jaume I (P1-1B2012-55).

14. Single-pixel optical information authentication

Wen Chen[1] *and Xudong Chen*[2]

[1]The Hong Kong Polytechnic University
[2]National University of Singapore

Status

Since double random phase encoding [1] was proposed, optical encryption has attracted much attention in the information security field. In double random phase encoding, input information can be converted into stationary white noise by using two statistically-independent random phase-only masks respectively placed in the input plane and spatial frequency domain. Until now, a number of optical principles and infrastructures [44], such as holography, have been successfully applied to enrich the optical security field. Remarkable characteristics of optical security systems are briefly described as follows. (1) Optical devices possess some inherent capabilities, such as parallel processing and high speed. (2) High security is guaranteed by using optical technologies, and input information can be flexibly encoded, such as into phase and intensity. (3) Multidisciplinary backgrounds are required, and a laborious procedure will be needed to decode input information by attackers.

However, it has been found that there is a linear characteristic in double random phase encoding. Optical security systems may be vulnerable to some attacking algorithms, such as known-plaintext attack and chosen-ciphertext attack. It is desirable that optical algorithms and infrastructures can be further developed for optical encoding systems to enhance security. Optical information authentication without visual disclosure of input information [15] is proposed as one of the most effective methods for security enhancement. However, a complex-valued wavefront should be extracted and applied in conventional optical systems. In addition, compact and varied encryption-based optical information authentication systems have not been fully studied yet.

Current and future challenges

In recent years, it has been found that single-pixel imaging [135] is a promising approach for optical information security. A schematic setup for single-pixel imaging is shown in figure 21. For the sake of brevity, the reference beam arm is not presented. The imaging is well known as ghost imaging, and the setup usually consists of two correlated beams and spatially-separated detectors. In a single-pixel secured imaging system, input information can be recovered by correlating intensity signals recorded by two detectors, and input information can be obtained at the plane where it is not located [135].

In the single-pixel secured imaging system, random phase-only masks or intensity patterns recorded at the reference beam arm can be used as principle security keys [63]. A series of intensity points recorded at the object beam arm is employed as ciphertexts. It has been found that when security keys or ciphertexts are further processed (such as with compression) [132, 136, 137, 138], it is possible to conduct data authentication without visual disclosure of input information. Figures 22(a) and (b) show a typical series of one-dimensional ciphertexts and a typical optical information authentication result, respectively. In practice, original input information can be stored in remote databases [137], and only a communication interface is given to the receivers to carry out information authentication without visual disclosure of the original data [137]. This strategy provides an additional security layer for conventional optical security systems.

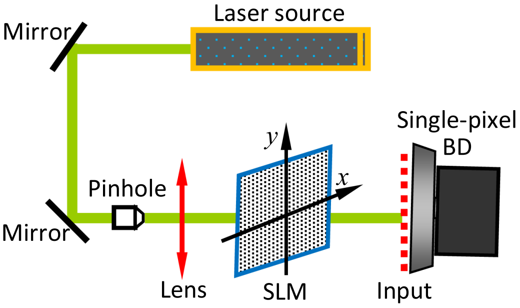

Figure 21. Schematic setup for single-pixel optical security [132, 136, 137, 138]: SLM, phase-only spatial light modulator; BD, bucket detector. The series of phase-only masks is sequentially embedded into the SLM. For the sake of brevity, the reference beam arm is not presented.

In single-pixel optical information authentication systems, different optical encryption principles can be introduced. In other words, information authentication is established by using an optical encryption setup, and the keys play an important role for recovering the input image followed by information verification.

However, conventional single-pixel optical information authentication systems do not possess a sufficiently large number of varied strategies to conduct information authentication via encryption, and phase-only masks are simply generated as principal keys. The encoding strategy and key-generation procedure might be guessed by hostile hackers. In addition, when the series of security keys or ciphertexts are contaminated during information storage or transmission, decoding and verification quality will be affected. Hence, effective designs of key distribution strategies, such as multiple receivers, are also important.

Advances in science and technology to meet challenges

Although there are some challenges in single-pixel optical information authentication systems, it is expected that advances in science and technology will help overcome the challenges.

Spatial light modulators play an important role in the implementation of single-pixel optical information

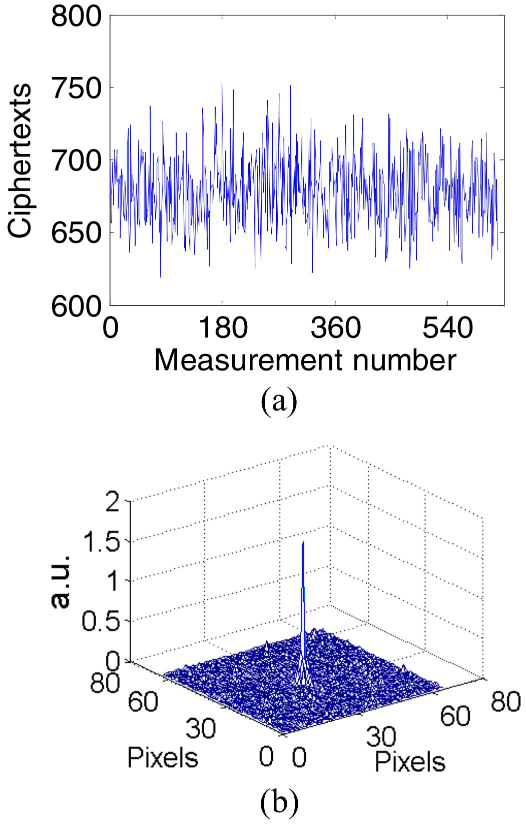

Figure 22. (a) A typical series of one-dimensional ciphertexts, (b) a typical optical information authentication distribution.

authentication. Nowadays, some types of spatial light modulators are already available [139]. As the technologies related to spatial light modulators develop, more powerful devices, such as those with higher diffraction efficiency, can be applied to enhance the decoding and verification quality in single-pixel optical information authentication systems.

In the optical security field, many optical encoding infrastructures [22, 44, 140–143] have been developed and successfully applied, such as phase retrieval. It is believed that a number of single-pixel optical information authentication systems can be established based on conventional encoding principles or setups. Hence, system flexibility and variety will be guaranteed, and more studies can be conducted in this research direction.

Various image or signal processing algorithms can be studied and further introduced for single-pixel optical information authentication systems. For instance, compressive sensing methods have been extensively investigated for various applications, and it can also be modified to be applied to single-pixel optical information authentication systems.

Real-time information verification can be a big challenge in practical application. Optical processing possesses unique advantages (such as high speed and parallel processing), and an effective mixture of optical and electronic principles can be important. When electronic encoding is also integrated into single-pixel optical information authentication systems, it is believed that more interesting and powerful infrastructures can be established.

Concluding remarks

With rapid developments of modern technologies, information security will play a more important role in our complex world. Securing information via optical means has been considered as one of the most promising technologies, and its remarkable characteristics have been continually studied. It has been illustrated that single-pixel optical information authentication is an interesting topic in the optical security field, and much more effort can be made in the future to overcome its challenges. It is expected that discussions related to the challenges may shed some light on future studies about single-pixel optical information authentication.

Acknowledgments

This work was supported by the startup grant (1-ZE5F) from The Hong Kong Polytechnic University, and also the Singapore MINDEF-NUS Joint Applied R&D Cooperation Programme (JPP) Project: MINDEF/NUS/JPP/14/01/02.

15. Multiple-scattering materials as physical unclonable functions

Pepijn W H Pinkse and Allard P Mosk

Complex Photonic Systems MESA+ Institute for Nanotechnology University of Twente, The Netherlands

Status

Authentication of keys plays a critical role in society, preventing unauthorized access to buildings and resources. Current authentication methods are based on verification of secret information, e.g. stored in a smart card, which has the disadvantage that the secret information can be probed by a technologically sufficiently advanced adversary. Ideally, an authentication key should be easy to produce, yet impossible to copy, and easy to read out or verify without the requirement of physical contact or human intervention. Such 'hands off' verification will become an essential feature of authentication systems as the holder of a key should be reluctant to insert it into an untrusted device or hand it to an untrusted individual.

Optical methods for protecting information from copying and decoding have been proposed based on phase masks [1, 20], for a review see [44], which are harder to copy than intensity patterns. However, in high-security systems that protect critical assets or large sums of money, one has to assume that an attacker has access to advanced optical and nanofabrication equipment. Due to their two-dimensional nature, phase masks can be read out and replicated in seconds with such equipment, creating opportunities for attacks based on key duplication.

Optical physical unclonable functions (PUFs) are ideal authentication keys [144]. In general, PUFs are physical objects that are impossible to copy because their manufacture inherently contains uncontrollable steps. An optical PUF is a three-dimensional structure such as white paint containing scatterers at random positions. When an optical PUF is illuminated by a laser, the reflected light shows a random interference pattern known as speckle. The properties of the illumination, such as wavelength, position and shape of the wavefront, constitute a 'challenge'; the reflected speckle pattern is the 'response' which is a rapidly varying function of both the challenge and the positions of the scatterers.

Even if an unclonable key is used, a classical readout mechanism offers no protection against an emulation attack. In such an attack, an attacker may have learned the characteristics of the key, e.g. by data theft. He then measures the challenge and fools the verifier by returning a computer-generated image of the expected response speckle pattern.

Reducing the photon number has shown to be an effective method to protect optically encrypted information from attacks that attempt to retrieve the secret properties of a phase-screen key [15]. In PUF-based quantum secure authentication (QSA) on the other hand, the properties of the unclonable key do not need to be kept secret. Duplication attacks are impossible, and emulation attacks on the unclonable key, even if its properties are known to the attacker, are thwarted by the quantum noise properties of readout with few photons [145]. The principle of QSA is shown in figure 23. The use of optical PUFs provides high security against forging and emulation. With developments to reduce the cost of the readout hardware and improve convenience, it can become the method of choice for securing financial transactions and access to facilities.

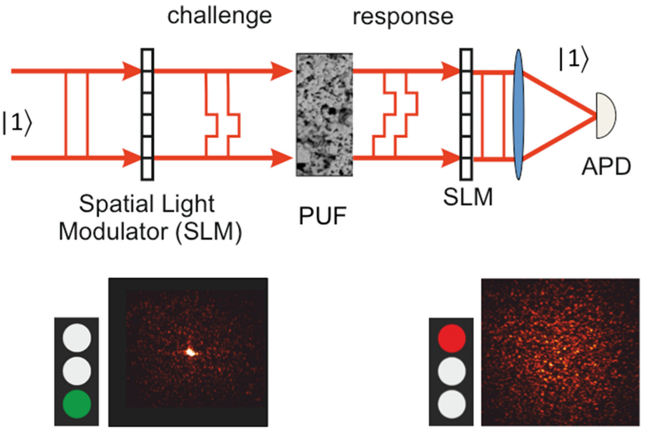

Figure 23. Schematic of quantum secure authentication [145]. A few-photon wavefront is shaped into a complex wavefront by an SLM. The response is transformed again with another SLM such that only with the correct key, the output light will be focussed to a point, where an APD behind a pinhole measures the amount of light falling into the target spot. With the wrong key, the output is a speckle pattern that will result in a much lower signal.

Current and future challenges

The challenges that need to be faced before optical PUF based authentication can become widespread are related to proving the security against various attack types, improving the convenience and speed of the readout process, reducing cost of the readout unit and developing durable key materials.

The most obvious attack is a duplication of the key. Direct copying of a 3D structure to the required level of accuracy is not likely to become possible for decades. A more realistic attack is to mimic the optical response of the PUF. Fabrication technology is progressing, in particular in nanophotonics, where low-loss 2D networks with tens of adjustable coupling elements have become possible [146]. In the future this can probably be scaled up to 10^4 to 10^5, which approaches the degrees of freedom of a PUF [147]. It is an ongoing challenge to design a key system that is robust against decades of technological progress.

A second relevant question is if QSA is secure against 'quantum hacking' [148], the term coined for hacking of quantum protocols by exploiting classical weaknesses in their implementation. Simple blinding attacks can be thwarted using standard methods such as spoof challenges, to which a negative response is expected [145]. Conceivably, a hacker with sophisticated equipment could find out the settings of the spatial light modulators of a flawed readout device, and use this information in a more advanced emulation attack. The implementation of a readout system that can be proven to be robust against such attacks is an important challenge.

Optical PUFs have already been proposed to provide random keys that can be used as a one-time pad [149]. An open and intriguing question is if PUFs can be integrated with other quantum-information protocols, such as quantum key distribution, to provide intrinsic authentication with a physical key.

An obvious problem with physical keys is that they are not immune to theft. Biometric keys have this problem to a much lesser extent. It would therefore be desirable to either find biometric PUFs that can be read out in a quantum secure way, or to make physical keys that contain biometric information as well as a PUF in a way that cannot be separated without destroying the PUF.

Advances in science and technology to meet challenges

To unlock the full potential of optical PUF-based authentication a range of basic scientific and technological challenges must be met.

Firstly, it is an ongoing challenge to ensure the level of security of any authentication method in the light of ongoing developments in technology. While for most optical PUF systems it is possible to quantify what technological progress would be needed to enable copying or emulation of the PUF, it is much more difficult to predict the rate of such technological progress. The importance of such predictions scales with the security level.

Secondly, many technological challenges are to be met to make optical readout as fast, reliable and convenient as possible. One may envision combinations of biometric and PUF-based authentication. Advanced readout systems may also be able to compensate for slight degradation or accumulation of dirt on the PUF.

Thirdly, advances in the understanding of propagation of complex-shaped light in scattering materials and in the fabrication of such materials will yield keys that are durable and resistant to wear, and can be integrated easily in cards, documents or mobile phones.

In some cases it may be beneficial to read out a key at some distance, e.g. via an optical fiber. Keys based on optical scattering will need to be accessed through a high-mode number multimode fiber. For remote readout via such fibers, significant advances are necessary in the fast compensation of the effects of varying mode coupling in these fibers.

Concluding remarks

Optical PUFs form a very versatile and promising system for secure authentication. While the unclonability of the PUFs is not a physical principle but a result of limited capabilities of technology, it is possible to construct keys of which the cloning is far beyond any technology currently envisioned. Moreover, the optical keys can be small (0.1 mm or smaller) and cheap to produce. An important technological challenge is to make the secure readout process fast and convenient for the user, to be able to compete with less secure but more convenient wireless authentication methods. Optical PUFs with convenient and secure readout will be essential tools to meet the ever-increasing risk of security breaches and identity theft.

Acknowledgments

We thank S A Goorden, A Lagendijk, B Škorić and W L Vos for support and discussions. This research was funded through NWO/Vici and ERC grant 279248.

16. Optical security and encryption with quantum imaging

Adam Markman, Bahram Javidi

University of Connecticut

Status

Since two approaches were proposed for using optics in security, authentication and encryption [1, 20], many variations of these approaches have been reported [15, 16, 22, 44, 91, 105, 113, 150, 151]. An advantage of optical security and encryption has been its ability to use multiple degrees of freedom in optics to generate complex multi-dimensional security keys including wavelength, polarization, 3D coordinates [91], and complex amplitude [1, 20, 44, 91].

Recently, optical security and encryption have been implemented with a few photons to substantially increase resistance against unauthorized attacks [15, 105, 150]. The implementation of photon counting optical keys makes the duplication of the keys extremely difficult due to the low number of available photons.

Traditional optical encryption schemes can be implemented either optically or digitally as researched by many different groups [44] although optical implementations are resistant against digital attacks. One popular optical encryption technique is the double-random-phase encryption (DRPE) [20]. This technique encrypts an image by multiplying it by two random phase masks, one in the spatial domain and one in the frequency domain or Fresnel domain [91]. The encrypted data is speckle-like and randomized. A user, knowing the correct phase keys, can decrypt the image revealing the original input image. The decryption is the reverse of the encryption process using conjugate phase masks [1, 15, 105].

Recently, optical security and encryption [1, 20] have been combined with quantum imaging or photon-counting [15, 16, 105, 150], which performs security authentication or encryption of the data with far fewer photons than conventional approaches. For authentication, the decrypted image is reconstructed with a few photons. Various optical correlation or image authentication approaches may be used [1, 105] to authenticate the photon counting decrypted image.

Figure 24(a) depicts an encryption or authentication scheme using DRPE. Using quantum imaging concepts, the encryption and decryption can be performed optically with a few photons using photon-counting devices. In figure 24(b), a computer-generated photon-limited encrypted image is obtained using 30 000 photons or 0.1144 photons/pixel. This image can then be decrypted and authenticated through the use of various algorithms such as correlation. The authentic scenario produces a sharp correlation peak whereas the wrong key response is low level noise as displayed in figure 24(c). The correlation peak for the authentic decrypted image is normalized to unity while the normalized correlation peak for the decrypted image using incorrect phase keys is substantially lower. Optical encryption with a few photons creates very sparse encrypted data which allows us to use storage and communication of data with small bandwidth such as quick response (QR) codes for optical security. In [150], the data was encrypted using DRPE with a few photons and was made sufficiently sparse to be stored in QR codes. The information stored in the optically encoded QR codes was scanned using a smartphone, decompressed and decrypted. The data was then authenticated using a nonlinear correlation filter [152].

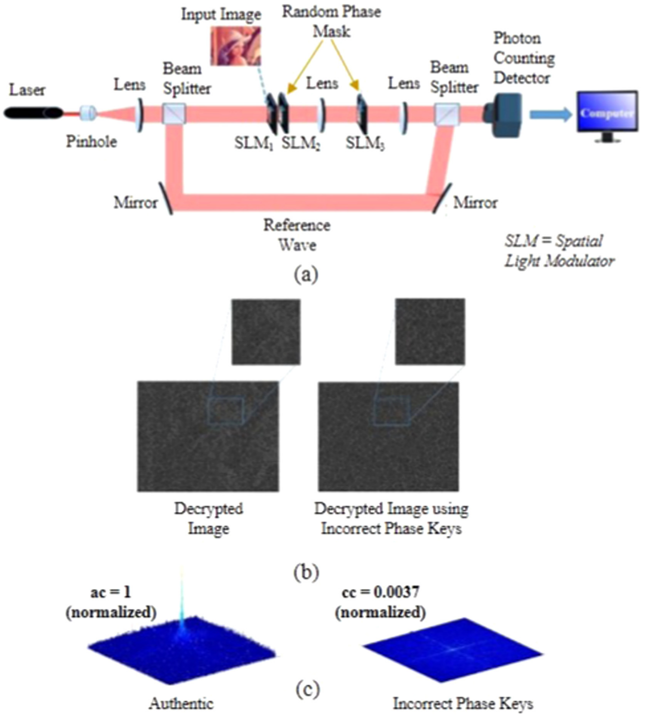

Figure 24. (a) Authentication scheme combining double-random-phase encryption (DRPE) with photon counting. A photon counting detector is used to record the encrypted image. The decryption is the reverse of the encryption process using conjugate phase masks [1, 15, 105]. (b) The computer-generated photon counting encrypted image using 30 000 photons in the scene or 0.1144 photons/pixel along with the correct decrypted image and decrypted image using incorrect phase keys. (c) Nonlinear correlation filters are then used to authenticate the decrypted images shown in (b).

Current and future challenges

Currently, there is ongoing research in authentication and encryption for hardware security. Counterfeit integrated circuits (IC) are being introduced into the market and given to consumers such as the military or medical device companies. Counterfeit circuits can be benign in that they perform just as well as an authentic chip. However, these counterfeit circuits can also be designed to fail after a particular number of working hours or can fail to work all together. Identifying these issues is critical. Optical security can be one method to validate an IC. All ICs have information written on them similar to a barcode. In [150], information about the IC was encrypted, compressed, and stored in a QR code which was placed on an IC and had an optical phase tag placed on it. The tag was illuminated by a laser and the resulting speckle signature was captured by a CCD. This signature was used to authenticate the optical phase mask. Moreover, given the correct decryption keys, the QR code was able to be scanned using a smartphone and the stored data was decompressed and decrypted, revealing information about the IC.

Another challenge is secure 3D display. In [16], a 3D authentication technique was introduced by combining a 3D imaging technique known as integral imaging with DRPE and photon counting. Although the photon-limited reconstruction is difficult to visually authenticate, the image can still be authenticated using image recognition such as nonlinear correlation filters.

Placing an inconspicuous phase-tag on an item that can be used for authentication is a current challenge. Recently, nano-encoding techniques have been integrated with optical security systems. A novel authentication scheme was introduced in [113] by embedding nanoparticle structures inside of an 840 × 840 μm^2 QR code. Upon visual inspection, it is impossible to see the structures with the naked eye. The nanoparticles produce a unique polarimetric signature when illuminated. This information can then be used to uniquely authenticate the object, such as the QR code.

Generally speaking, 3D integral imaging requires multiple 2D perspectives of a scene known as elemental images (EI). Transferring the images from one party to another in a secure way can be difficult. In [48], QR codes were used for secure 3D display. The RGB elemental images used for integral imaging had photon counting applied to them followed by compression and DRPE. The encrypted RGB images were then stored in multiple QR codes. Knowing the decryption keys to DRPE, the elemental images were fully recovered. Once all of the elemental images were recovered, a 3D image was reconstructed.

Advances in science and technology to meet challenges

Utilizing quantum imaging in encryption systems introduces a unique scheme that provides additional security. Photon counting [15, 105] or quantum imaging techniques can be combined with optical encryption schemes. This is done by limiting the number of photons that arrive at a pixel according to the photon counting regime. Photon counting may be mathematically modelled using a Poisson distribution under certain assumptions [153]. Other distributions may be used including the geometric distribution, which is used to model photon statistics of thermal light, or the binomial distribution, which can be used for photon statistics in non-classical light [154]. For a lower number of photons, a sparse and noise-like image is generated. This additional layer of security is advantageous over a conventional optical encryption system, which can be susceptible to attacks including chosen-ciphertext and chosen-plaintext if their encryption keys are not continuously updated. By applying quantum imaging to the system, this security risk can be mitigated. As shown in figure 24, when DRPE is combined with photon counting, the decrypted image is very sparse and the attacker would not be able to determine what the message is with certainty.

Embedding nanoparticles [113] into an object is also a topic of interest. These nanoparticles cannot be observed by the human eye; however, when illuminated by a light source such as a laser, a unique pattern is generated. The polarization signature can be found for a sample, which can then be used with classification algorithms, such as support vector machines, for authentication. Further exploration of embedding nanoparticles into objects is needed. Nanoparticles can be of particular interest in authenticating military, commercial, and medical devices.

Concluding remarks

Recently, quantum imaging has been combined with optical encryption algorithms such as DRPE. Rather than recovering the original image after decryption, a sparse noise-like image is obtained which can be authenticated, such as through the use of nonlinear correlation algorithms. Object authentication can also be performed by utilizing optical encoding, whether it is by placing an optical tag on an object or embedding an object with nanoparticles. When illuminated, the optical tags create a unique spatial or polarimetric signature which can be used to authenticate the object. Moreover, additional research has been done in using optically encoded QR codes for image security, and for secure 3D display. Variations of the approaches presented here for optical security are possible using multiple degrees of freedom provided by optics [22]. Further advances are still needed in cyber security to address the needs of object and data authentication and encryption in a non-invasive and secure manner. Optical security can aid this requirement.

Acknowledgments

We wish to acknowledge Honeywell for its support.

References

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

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

[3] Rivenson Y, Stern A and Javidi B 2010 Single exposure super-resolution compressive imaging by double phase encoding *Opt. Express* **18** 15094–103

[4] Takeda M, Nakano K, Suzuki H and Yamaguchi M 2015 Encrypted sensing based on digital holography for fingerprint images *Opt. Photon. J.* **5** 6–14

[5] Suzuki H, Yamaguchi M, Yachida M, Ohyama N, Haneishi H and Obi T 2006 Experimental evaluation of fingerprint verification system based on double random phase encoding, *Opt. Express* **14** 1755–66

[6] 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

[7] Nakano K, Takeda M, Suzuki H and Yamaguchi M 2014 Security analysis of phase-only DRPE based on known-plaintext attack using multiple known plaintext–ciphertext pairs *Appl. Opt.* **53** 6435–43

[8] Nakano K, Takeda M, Suzuki H and Yamaguchi M 2014 Encrypted imaging based on algebraic implementation of double random phase encoding *Appl. Opt.* **53** 2956–63

[9] ISO/IEC 15408-1: 2009 Information technology—Security techniques—Evaluation criteria for IT security. 1: Introduction and general model

[10] Hsu W-F and Yeh C-F 2011 Speckle suppression in holographic projection displays using temporal integration of speckle images from diffractive optical elements *Appl. Opt.* **50** H50–5

[11] Maycock J, McDonald J B and Hennelly B M 2013 Speckle reduction of reconstructions of digital holograms using three dimensional filtering *Opt. Commun.* **300** 142–55

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

[13] Tajahuerce E, Matoba O, Verrall S C and Javidi B 2000 Optoelectronic information encryption with phase-shifting interferometry *Appl. Opt.* **39** 2313–20

[14] Nomura T, Uota K and Morimoto Y 2004 Hybrid encryption of a 3D object using a digital holographic technique *Opt. Eng.* **43** 2228–32

[15] Pérez-Cabré E, Cho M and Javidi B 2011 Information authentication using photon-counting double-random-phase encrypted images *Opt. Lett.* **36** 22–4

[16] Cho M and Javidi B 2013 Three-dimensional photon counting double-random-phase encryption *Opt. Lett.* **38** 3198–201

[17] Awatsuji Y, Sasada M and Kubota T 2004 Parallel quasi-phase-shifting digital holography *Appl. Phys. Lett.* **85** 1069–71

[18] Imbe M and Nomura T 2013 Study of reference waves in single-exposure generalized phase-shifting digital holography *Appl. Opt.* **52** 4097–102

[19] Millán M S and Pérez-Cabré E 2006 Multifactor authentication reinforces optical security *Opt. Lett.* **31** 721–3

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

[21] Pérez-Cabré E, Millán M S and Javidi B 2007 Near infrared multifactor identification tags *Opt. Express* **15** 15615–27

[22] Matoba O, Nomura T, Pérez-Cabré E, Millán M S and Javidi B 2009 Optical techniques for information security *Proc. IEEE* **97** 1128–48

[23] Horrillo S, Pérez-Cabré E and Millán M S 2010 Information compression for remote readable ID tags *J. Opt.* **12** 115404

[24] Pérez-Cabré E, Abril H C, Millán M S and Javidi B 2012 Photon-counting double-random-phase encoding for secure image verification and retrieval *J. Opt.* **14** 094001

[25] Pérez-Cabré E, Mohammed E A, Millán M S and Saadon H L 2015 Photon-counting multifactor optical encryption and authentication *J. Opt.* **17** 025706

[26] Vilardy J, Millán M S and Pérez-Cabré E 2013 Improved decryption quality and security of a joint-transform correlator-based encryption system *J. Opt.* **15** 025401

[27] Vilardy J, Millán M S and Pérez-Cabré E 2014 Nonlinear optical security system based on a joint transform correlator in the Fresnel domain *App. Opt.* **53** 1674–82

[28] Millán M S and Pérez-Cabré E 2011 Optical data encryption *Optical and Digital Image Processing: Fundamentals and Applications* ed G Cristóbal *et al* (New York: Wiley)

[29] Millán M S 2012 Advanced optical correlation and digital methods for pattern matching—50th anniversary of Vander Lugt matched filter *J. Opt.* **14** 103001

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

[31] Qin W and Peng X 2010 Asymmetric cryptosystem based on phase-truncated Fourier transforms *Opt. Lett.* **35** 118–20

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

[33] Rajput S K and Nishchal N K 2012 Image encryption based on interference that uses fractional Fourier domain asymmetric keys *Appl. Opt.* **51** 1446–52

[34] 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

[35] Rajput S K and Nishchal N K 2013 Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform *Appl. Opt.* **52** 871–8

[36] Rajput S K and Nishchal N K 2013 Known-plaintext attack on encryption domain independent optical asymmetric cryptosystem *Opt. Commun.* **309** 231–5

[37] 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

[38] 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

[39] Mehra I and Nishchal N K 2015 Wavelet-based image fusion for securing multiple images through asymmetric keys *Opt. Commun.* **335** 153–60

[40] Mosso F, Barrera J F, Tebaldi M, Bolognini N and Torroba R 2011 All-optical encrypted movie *Opt. Express* **19** 5706–12

[41] Mosso F, Tebaldi M, Barrera J F, Bolognini N and Torroba R 2011 Pure optical dynamical color encryption *Opt. Express* **19** 13779–86

[42] Barrera J F, Vélez A and Torroba R 2013 Experimental multiplexing protocol to encrypt messages of any length *J. Opt.* **15** 055404

[43] Aldossari A, Alfalou A and Brosseau C 2014 Simultaneous compression and encryption of closely resembling images: application to video sequences and polarimetric images *Opt. Express* **22** 22349–68

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

[45] Barrera J F, Mira A and Torroba R 2013 Optical encryption and QR codes: secure and noise-free information retrieval *Opt. Express* **21** 5373–8

[46] Graydon O 2013 Cryptography: Quick response codes *Nat. Photonics* **7** 343

[47] Trejos S, Barrera J F and Torroba R 2015 Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval *J. Opt.* **17** 85702

[48] Markman A, Wang J and Javidi B 2015 Three-dimensional integral imaging displays using a quick-response encoded elemental image array *Optica* **1** 332–5

[49] Guo L and Sheridan J T 2014 A review of optical image encryption techniques *Opt. Laser Technol.* **57** 327–42

[50] Carnicer A, Montes-Usategui M, Arcos S and Juvells I 2005 Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys *Opt. Lett.* **30** 1644–6

[51] Peng X, Zhang P, Wei H and Yu B 2006 Known-plaintext attack on optical encryption based on double random phase keys *Opt. Lett.* **31** 1044–6

[52] Schneier B 1996 *Applied Cryptography: Protocols, Algorithms, and Source Code in C* 2nd edn (Hoboken, NJ: Wiley)

[53] He W, Peng X, Qin W and Meng X 2010 The keyed optical Hash function based on cascaded phase-truncated Fourier transforms *Opt. Commun.* **283** 2328–32

[54] 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

[55] Wang X and Zhao D 2012 A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms *Opt. Commun.* **285** 1078–81

[56] Eldar Y C and Kutyniok G 2012 *Compressed Sensing: Theory and Applications*

[57] Lu P, Xu Z, Lu X and Liu X 2013 Digital image information encryption based on compressive sensing and double random-phase encoding technique *Optik* **124** 2514–8

[58] Deepan B, Quan C, Wang Y and Tay C 2014 Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique *Appl. Opt.* **53** 4539–47

[59] Rawat N, Kim B, Muniraj I, Situ G and Lee B 2015 Compressive sensing based robust multispectral double-image encryption (invited) *Appl. Opt.* **54** 1782–93

[60] Rawat N, Hwang I, Shi Y and Lee B 2015 Optical image encryption via photon-counting imaging and compressive sensing based ptychography *J. Opt.* **17** 065704

[61] 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

[62] Li J, Li H, Li J, Pan Y and Li R 2015 Compressive optical image encryption with two-step-only quadrature phase-shifting digital holography *Opt. Commun.* **344** 166–71

[63] Clemente P, Durán V, Torres-Company V, Tajahuerce E and Lancis J 2010 Optical encryption based on computational ghost imaging *Opt. Lett.* **35** 2391–3

[64] Zerom P, Chan K W C, Howell J C and Boyd R W 2011 Entangled-photon compressive ghost imaging *Phys. Rev.* A **84** 061804

[65] Lum D J, Knarr S H and Howell J C 2015 Fast Hadamard transforms for compressive sensing of joint-systems: measurement of a 3.2 million-dimensional bi-photon probability distribution *Opt. Express* **23** 27636–49

[66] Zhou N, Zhang A, Zheng F and Gong L 2014 Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing *Opt. Laser Technol.* **62** 152–60

[67] Rachlin Y and Baron D 2008 The secrecy of compressed sensing measurements *46th Annual Allerton Conf. on Communication, Control, and Computing*

[68] Cambareri V, Mangia M, Pareschi F, Rovatti R and Setti G 2015 On known-plaintext attacks to a compressed sensing-based encryption: a quantitative analysis *IEEE Trans. Inf. Forensics Security* **10** 2182–95

[69] Stern A, Auguts Y and Rivenson Y 2013 Challenges in optical compressive imaging and some solutions *10th Int. Conf. on Sampling Theory and Applications SampTa* vol 24

[70] Alfalou A and Brosseau C 2015 Recent advances in optical image processing *Progress in Optics* ed E Wolf vol 60 pp 119–262

[71] Alfalou A, Brosseau C and Alam M S 2013 Smart pattern recognition *Proc. SPIE* **8748** 874809

[72] Alfalou A, Mansour A, Elbouz M and Brosseau C Optical compression scheme to multiplex & simultaneously encode images *Optical and Digital Image Processing Fundamentals and Applications* ed G Cristobal *et al*

[73] Darakis E, Naughton T J and Soraghan J J 2007 Compression defects in different reconstruction from phase-shifting digital holographic data *Appl. Opt.* **46** 4579–86

[74] Alfalou A, Brosseau C, Abdallah N and Jridi M 2013 Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks *Opt. Express* **21** 8025–43

[75] Shortt A, Naughton T J and Javid B 2006 Compression of encrypted digital holograms using artificial neural networks *IEEE J. Display Technol.* **2** 401–10

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

[77] Paturzo M, Memmolo P, Miccio L, Finizio A, Ferraro P, Tulino A and Javidi B 2008 Numerical multiplexing and demultiplexing of digital holographic information for remote reconstruction in amplitude and phase *Opt. Lett.* **33** 2629–31

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

[79] Xia P, Shimozato Y, Tahara T, Kakue T, Awatsuji Y, Nishio K, Ura S, Kubota T and Matoba O 2013 Image reconstruction algorithm for recovering high-frequency information in parallel phase-shifting digital holography [Invited] *Appl. Opt.* **52** A210–5

[80] Alfalou A and Brosseau C 2013 Implementing compression and encryption of phase-shifting digital holograms for three-dimensional object reconstruction *Opt. Commun.* **307** 67–72

[81] Wang Q, Guo Q and Lei L 2013 Asymmetric multiple-image hiding using phase retrieval technique based on amplitude- and phase-truncation in fractional Fourier domain Optik **124** 3898–902

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

[83] Wang Q 2012 Optical image encryption with silhouette removal based on interference and phase blend processing *Opt. Commun.* **285** 4294

[84] Liu Z, Zhang Y, Li S, Liu W, Liu W, Wang Y and Liu S 2013 Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains *Opt. Laser Technol.* **47** 152

[85] Sahin A, Ozaktas H M and Mendlovic D 1995 *Opt. Commun.* **120** 128–34

[86] Duraffourg L, Merolla J M, Goedgebuer J P, Mazurenko Y and Rhodes W T 2001 Compact transmission system using single-sideband modulation of light for quantum cryptography *Opt. Lett.* **26** 1427

[87] Guglielmi V, Fournier-Prunaret D, Taha A K, Pinel P, Rouabhi S and Beneteau L 2002 Encryption using chaotic dynamics of two noninvertible maps *Proc. Workshop on Nonlinear Dynamics of Electronic Systems (NDES'02) (Izmir, Turquie)*

[88] Ouerhani Y, Desthieux M and Alfalou A 2015 Road sign recognition using Viapix module and correlation *Proc. SPIE 9477, Optical Pattern Recognition XXVI* 94770H

[89] Hennelly B M and Sheridan J T 2003 Fractional Fourier transform-based image encryption phase retrieval algorithm *Opt. Commun.* **226** 61–80

[90] Situ G and Zhang J 2004 Double random-phase encoding in the Fresnel domain *Opt. Lett.* **29** 1584–6

[91] Matoba O and Javidi B 1999 Encrypted optical memory system using three-dimensional keys in the Fresnel domain *Opt. Lett.* **24** 762–4

[92] Matoba O and Javidi B 1999 Encrypted optical storage with wavelength key and random codes *Appl. Opt.* **38** 6785–90

[93] Unnikrishnan G and Singh K 2001 Optical encryption using quadratic phase systems *Opt. Commun.* **193** 51–67

[94] Singh N and Sinha A 2009 Gyrator transform-based optical image encryption, using chaos *Opt. Las. Eng.* **47** 539–46

[95] Guo C, Liu S and Sheridan J T 2015 Iterative phase retrieval algorithms. I: Optimization *Appl. Opt.* **54** 4698–708

[96] Guo C, Liu S and Sheridan J T 2015 Iterative phase retrieval algorithms. II: Attacking optical encryption systems *Appl. Opt.* **54** 4709–19

[97] Situ G, Gopinathan U, Monaghan D S and Sheridan J T 2007 Cryptanalysis of optical security systems with significant output images *Appl. Opt.* **46** 5257–62

[98] 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

[99] Situ G, Pedrini G and Osten W 2010 Strategy for cryptanalysis of optical encryption in the Fresnel domain *Appl. Opt.* **49** 457–62

[100] Imai H and Hayashi M 2006 *Quantum Computation and Information* (Berlin: Springer)

[101] Liu J, Xu X, Wu Q, Sheridan J T and Situ G 2015 Information encryption in phase space *Opt. Lett.* **40** 859–62

[102] Hou J, Huang S and Situ G 2015 Nonlinear optical image encryption *Conf. of LTO (Shanghai, March 16–17)* (in Chinese) (doi:10.3788/aos201535.0807001)

[103] Torroba R, Rabal H and Ruiz B 1992 An entropy approach to light propagation *J. Mod. Opt.* **39** 1939–46

[104] Situ G 2015 Phase-space optics: applications in computational imaging and optical image processing *Proc. SPIE* **9524** 952405

[105] Markman A and Javidi B 2014 Full-phase photon-counting double-random-phase encryption *J. Opt. Soc. Am.* A **31** 394–403

[106] 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

[107] van Renesse R L 2005 *Optical Document Security* (Boston: Artech House)

[108] Naruse M, Tate N, Aono M and Ohtsu M 2013 Information physics fundamentals of nanophotonics *Rep. Prog. Phys.* **76** 056401

[109] Naruse M, Tate N and Ohtsu M 2012 Optical security based on near-field processes at the nanoscale *J. Opt.* **14** 094002

[110] Naruse M, Hori H, Kobayashi K, Ishikawa M, Leibnitz K, Murata M, Tate N and Ohtsu M 2009 Information theoretical analysis of hierarchical nano-optical systems in the subwavelength regime *J. Opt. Soc. Am.* B **26** 1772–9

[111] Tate N, Naruse M, Yatsui T, Kawazoe T, Hoga M, Ohyagi Y, Fukuyama T, Kitamura M and Ohtsu M 2010 Nanophotonic code embedded in embossed hologram for hierarchical information retrieval *Opt. Express* **18** 7497–505

[112] Tate N, Sugiyama H, Naruse M, Nomura W, Yatsui T, Kawazoe T and Ohtsu M 2009 Quadrupole–dipole transform based on optical near-field interactions in engineered nanostructures *Opt. Express* **17** 11113–21

[113] Carnicer A, Hassanfiroozi A, Latorre-Carmona P, Huang Y and Javidi B 2015 Security authentication using phase-encoded nanoparticle structures and polarized light *Opt. Lett.* **40** 135–8

[114] Matsumoto H and Matsumoto T 2003 Clone match rate evaluation for an artifact-metric system *IPSJ J.* **44** 1991–2001

[115] Matsumoto T, Hoga M, Ohyagi Y, Ishikawa M, Naruse M, Hanaki K, Suzuki R, Sekiguchi D, Tate N and Ohtsu M 2014 Nano-artifact metrics based on random collapse of resist *Sci. Rep.* **4** 6142

[116] Zheludev N I and Kivshar Y S 2012 From metamaterials to metadevices *Nat. Mater.* **11** 917

[117] Martínez A, García-Meca C, Ortuno R, Rodríguez-Fortuño F J and Martí J 2009 Metamaterials for optical security *Appl. Phys. Lett.* **94** 251106

[118] Naruse M, Hori H, Ishii S, Drezet A, Huant S, Hoga M, Ohyagi Y, Matsumoto T, Tate N and Ohtsu M 2014 Unidirectional light propagation through two-layer nanostructures based on optical near-field interactions *J. Opt. Soc. Am.* B **31** 2404–13

[119] Naruse M, Hori H, Kobayashi K and Ohtsu M 2007 Tamper resistance in optical excitation transfer based on optical near-field interactions *Opt. Lett.* **32** 1761–3

[120] Matoba O and Javidi B 2004 Secure holographic memory by double-random polarization encryption *Appl. Opt.* **43** 2915–9

[121] Chen W and Chen X 2010 Space-based optical image encryption *Opt. Express* **18** 27095–104

[122] Novotny L and Hecht B 2012 *Principles of Nano-Optics* (Cambridge: Cambridge University Press)

[123] Carnicer A, Juvells I, Maluenda D, Martínez-Herrero R and Mejías P M 2012 On the longitudinal component of paraxial fields *Eur. J. Phys.* **33** 1235–47

[124] Richards B and Wolf E 1959 Electromagnetic diffraction in optical systems. II: Structure of the image field in an aplanatic system *Proc. R. Soc.* A **253** 358–79

[125] Maluenda D, Martínez-Herrero R, Juvells I and Carnicer A 2014 Synthesis of highly focused fields with circular polarization at any transverse plane *Opt. Express* **22** 6859–67

[126] Maluenda D, Juvells I, Martínez-Herrero R and Carnicer A 2013 Reconfigurable beams with arbitrary polarization and shape distributions at a given plane *Opt. Express* **21** 5432–9

[127] Frauel Y, Naughton T J, Matoba O, Tajahuerce E and Javidi B 2006 Three-dimensional imaging and processing using computational holographic imaging *Proc. IEEE* **94** 636–53

[128] Duarte M F, Davenport M A, Takhar D, Laska J N, Sun T, Kelly K F and Baraniuk R G 2008 Single-pixel imaging via compressive sampling *IEEE Signal Proc. Mag.* **25** 83–91

[129] Gatti A, Brambilla E and Lugiato L A 2008 Quantum imaging *Prog. Opt.* **51** 251

[130] Bromberg Y, Katz O and Silberberg Y 2009 Ghost imaging with a single detector *Phys. Rev.* A **79** 053840

[131] Tanha M, Kheradmand R and Ahmadi-Kandjani S 2012 Gray-scale and color optical encryption based on computational ghost imaging *Appl. Phys. Lett.* **101** 101108

[132] Chen W and Chen X 2013 Ghost imaging for three-dimensional optical security *Appl. Phys. Lett.* **103** 221106

[133] Kong L J, Li Y, Qian S X, Li S M, Tu C and Wang H T 2013 Encryption of ghost imaging *Phys. Rev.* A **88** 013852

[134] Zhao S, Wang L, Liang W, Cheng W and Gong L 2015 High performance optical encryption based on computational ghost imaging with QR code and compressive sensing technique *Opt. Comm.* **353** 90–5

[135] Erkmen B I and Shapiro J H 2010 Ghost imaging: from quantum to classical to computational *Adv. Opt. Photon.* **2** 405–50

[136] 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

[137] Chen W and Chen X 2015 Grayscale object authentication based on ghost imaging using binary signals *Europhys. Lett.* **110** 44002

[138] Chen W and Chen X 2014 Marked ghost imaging *Appl. Phys. Lett.* **104** 251109

[139] Savage N 2009 Digital spatial light modulators *Nat. Photon.* **3** 170–2

[140] 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

[141] Chen W and Chen X 2014 Arbitrarily modulated beam for phase-only optical encryption *J. Opt.* **16** 105402

[142] Chen W and Chen X 2015 Ghost imaging using labyrinth-like phase modulation patterns for high-efficiency and high-security optical encryption *Europhys. Lett.* **109** 14001

[143] Chen W, Chen X and Sheppard C J R 2010 Optical image encryption based on diffractive imaging *Opt. Lett.* **35** 3817–9

[144] Pappu R, Recht B, Taylor J and Gershenfeld N 2002 Physical one-way functions *Science* **297** 2026

[145] Goorden S A, Horstmann M, Mosk A P, Škorić B and Pinkse P W H 2014 Quantum-secure authentication of a physical unclonable key *Optica* **1** 421

[146] Carolan J *et al* 2015 Universal linear optics *Science* **349** 711

[147] Miller D A B 2013 How complicated must an optical component be? *J. Opt. Soc. Am.* A **30** 238–51

[148] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 Hacking commercial quantum cryptography systems by tailored bright illumination *Nat. Photon.* **4** 686

[149] Horstmeyer R, Judkewitz B, Vellekoop I M, Assawaworrarit S and Yang C 2013 Physical key-protected one-time pad *Sci. Rep.* **3** 3543

[150] Markman A, Javidi B and Tehranipoor M 2014 Photon-counting security tagging and verification using optically encoded QR codes *IEEE Photon. J.* **6** 1–9

[151] Markman A, Wang J and Javidi B 2014 Three-dimensional integral imaging displays using a quick-response encoded elemental image array *Optica* **1** 332–5

[152] Javidi B 1989 Nonlinear joint power spectrum based optical correlation *Appl. Opt.* **28** 2358–67

[153] Goodman G W 1985 *Statistical Optics* (New York: Wiley) pp 467–8

[154] Narravula S R, Hayat M M and Javidi B 2010 Information theoretic approach for assessing image fidelity in photon-counting arrays *Opt. Express* **18** 2449–66