Roadmap on optical security

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

Affiliations

[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 i Òptica, Martí i Franquès 1, 08028 Barcelona, Spain

[3]Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China

[4]Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583, Singapore

[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]Photonic Network Research Institute, National Institute of Information and Communications Technology, 4-2-1 Nukui-kita, Koganei, Tokyo 184-8795, Japan

[7]Graduate School of Environment and Information Sciences, Yokohama National University, Hodogaya, Yokohama, Kanagawa, Japan

[8]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

[9]Shanghai Institute of Optics and Fine Mechanics, Chinese Academy of Sciences, Shanghai 201800, China

[10]Department of Physics, Indian Institute of Technology Patna, Bihta, Patna 801 118, India

[11]College of Optoelectronics Engineering, Key Laboratory of Optoelectronic Devices and Systems of Ministry of Education and Guangdong Province, Shenzhen University, Shenzhen 518060, China

[12] Department of Electro-Optical Engineering, Ben-Gurion University of the Negev, P.O. Box 653, Beer-Sheva 84105, Israel

[13]Electrical Engineering Department, University of California, Los Angeles, USA

[14]Complex Photonic Systems (COPS), MESA+ Institute for Nanotechnology, University of Twente, 7500 AE Enschede, The Netherlands

[15]Global Scientific Information and Computing Center, Tokyo Institute of Technology, 2-12-1, Ookayama, Meguro-ku, Tokyo 152-8550, Japan

[16]Faculty of Systems Engineering, Wakayama University, 930 Sakaedani, Wakayama 640-8510, Japan

[17]Centro de Investigaciones Opticas (CONICET La Plata-CIC) and UID OPTIMO, Facultad de Ingenieria, Universidad Nacional de La Plata, PO Box 3, C.P 1897, La Plata, Argentina

[18]Grupo de Optica y Fotónica, Instituto de Fısica, Facultad de Ciencias Exactas y Naturales, Universidad de Antioquia UdeA, Calle 70 No. 52-21, Medell´ın, Colombia

[19]Equipe Vision, L@BISEN, ISEN-Brest, 20 rue Cuirassé Bretagne, CS 42807, 29228 Brest Cedex 2, France

[20]Université de Brest, Lab-STICC, 6 avenue Le Gorgeu, CS 93837, 29238 Brest Cedex 3, France

[21]Institute of New Imaging Technologies, Universitat Jaume I, 12071 Castelló, Spain

Abstract:

To be completed by guest editors

Contents

1. Single-pixel optical information authentication –

Wen Chen[1,2] 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 [1] by using two statistically-independent random phase-only masks respectively placed in input plane and spatial frequency domain. Until now, a number of optical principles and infrastructures [2], such as holography [2], 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) Multi-disciplinary background is requested, 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 the security. Optical information authentication without visual disclosure of input information [3] 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 [4] is a promising approach for optical information security. The single-pixel imaging is usually conducted based on photon correlation [4], and a schematic setup is shown in Fig. 1. 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 [4–8]. In a single-pixel secured imaging system, input information can be recovered by correlating intensity signals recorded by two detectors [4–8], and input information can be obtained at the plane where it is not located.

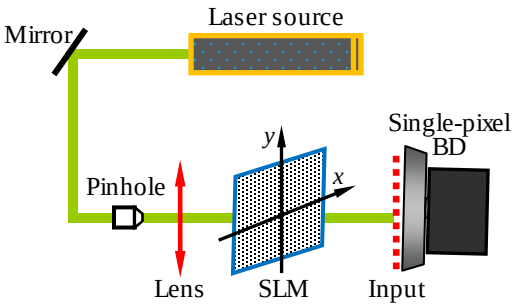


Figure 1 – Schematic setup for single-pixel optical security [5–8]: SLM, phase-only spatial light modulator; BD, bucket detector. The series of phase-only masks is sequentially embedded into the SLM. For the sake of brevity, reference beam arm is not presented.

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. The 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 compression) [5–8], it is possible to conduct data authentication without visual disclosure of input information. Figures 2(a) and 2(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 [7], and only a communication interface is given to the receivers to carry out information authentication without visual disclosure of the original data [7]. This strategy provides an additional security layer for conventional optical security systems.

In single-pixel optical information authentication systems, different optical encryption principles can be introduced. In other words, information authentication is conducted based on optical encryption, and security keys used in conventional optical security systems are considered as important parameters for verifying the decoded information.

However, conventional single-pixel optical information authentication systems do not possess a sufficiently large number of varied strategies to conduct information authentication via the 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.

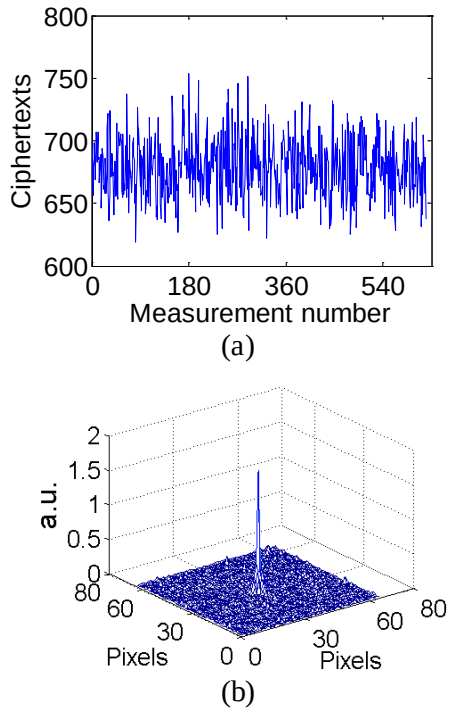


Figure 2 – (a) A typical series of one-dimensional ciphertexts, (b) a typical optical information authentication distribution.

Advances in Science and Technology to Meet Challenges – Although there are some challenges in single-pixel optical information authentication systems, it is expected that the 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 authentication. Nowadays, some types of spatial light modulators are already available [9]. As the technologies related to spatial light modulator 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 have been developed and successfully applied, such as phase retrieval [10]. 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. In addition, single-pixel imaging with computational strategy [4] can greatly facilitate the implementation of optical authentication systems, and the recordings at the reference beam arm can be avoided.

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 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 the discussions related to the challenges may shed some light on the future studies about single-pixel optical information authentication.

Acknowledgments. This work was supported by the Singapore MINDEF-NUS Joint Applied R&D Cooperation Programme (JPP) Project: MINDEF/NUS/JPP/14/01/02.

References

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

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

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

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

[5] 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

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

[7] Chen W and Chen X 2015 Grayscale object authentication based on ghost imaging using binary signals *EPL* **110** 44002

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

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

[10] 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

2. Simultaneous encryption and authentication of multiple signals -

Elisabet Pérez-Cabré and María S. Millán
Universitat Politècnica de Catalunya

Status – Multifactor optical encryption-authentication (MOEA) (Fig. 1) was firstly introduced in 2006 [1] 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:

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

and subsequent simultaneous authentication of all those signals. In Eq. (1) all factors are phase-encoded, that is, for a general function $a(x)$, $t_a(x) = \exp\left[j\pi a(x)\right]$, FT^{-1} denotes an inverse Fourier transform and $*$ is the convolution operation. The signals to encrypt can be of different nature: 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 (Fig. 1) 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 the system reliability because its response does not rely on the verification of a single factor but on a set of factors. They all must obtain a positive authentication to provide a final validation. For instance (Fig. 1b), 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 content of the parcel to deliver $n(x)$.

Unlike sequential encryption methods, the MOEA technique achieves the 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

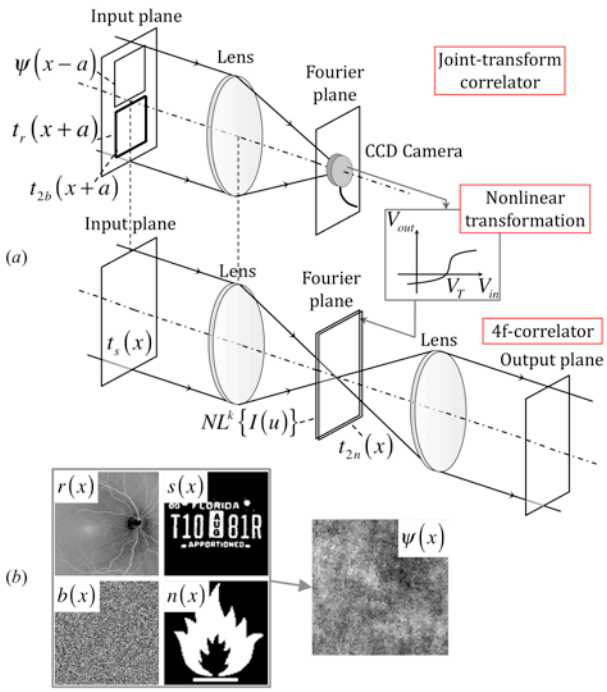


Figure 1 – (a) MOEA setup; (b) Four factors of different nature and MOEA complex-valued encrypted function.

surveillance or tracking of vehicles or moving objects (Fig. 2) [2,3]. 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 [2]. 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 [2,3].

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. 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). 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 [4]. 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 [4].

In practice, further reduction or simplification of the encrypted content to transmit can be necessary.

Photon-counting imaging techniques have been recently implemented along with encryption techniques [5]. 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 the decryption and authentication stages. For the widely used encryption technique of the double-random phase encoding (DRPE), 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, are suffice to achieve satisfactory authentication results [6]. 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 [7].

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 recently made [8-9]. In [8], the introduction of a nonlinear operation in a two-step joint-transform processor permits to alleviate 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 [9].

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.

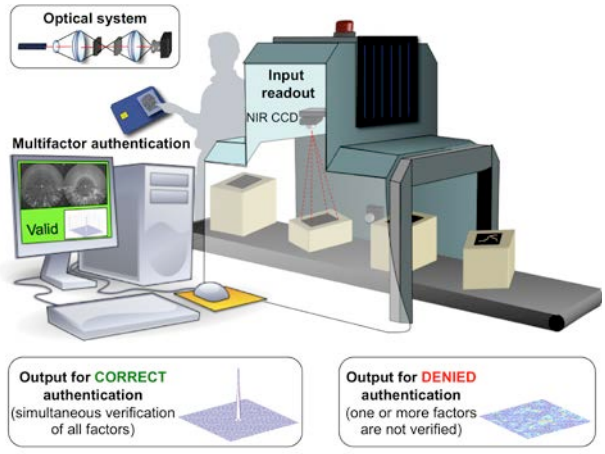


Figure 2 – High-level security MOEA application. The moving parcels are verified along with the identity of the delivering person and other information from a database. Additional features: non-visible, NIR remotely readable ID tag, certain tolerance to scale and in-plane rotations, Resistance to damage produced by common handling.

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 a 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 [10]. In this regard, compact processors contain spatial light modulators (SLM) for the joint display of 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 permit to ease this bottleneck [11].

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 a significant data compression with proved resistance against unauthorized attacks. However, as 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 line to increase the current applicability of optical encryption methods.

References

[1] M. S. Millán, E. Pérez-Cabré (2006) "Multifactor authentication reinforces optical security," Opt. Lett, 31, 721-723.

[2] E. Pérez-Cabré, M. S. Millán, B. Javidi (2007) "Near infrared multifactor identification tags," Opt. Express, 15, 15615-15627.

[3] O. Matoba, T. Nomura, E. Pérez-Cabré, M. S. Millán, B. Javidi (2009) "Optical techniques for information security," Proc. IEEE, 97, 1128-1148.

[4] S. Horrillo, E. Pérez-Cabré, M. S. Millán (2010) "Information compression for remote readable ID tags," J. Opt., 12, 115404.

[5] E. Pérez-Cabré, M. Cho, B. Javidi (2011) "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett., 36, 22-24.

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

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

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

[9] J. Vilardy, M. S. Millán, E. Pérez-Cabré (2014) "Nonlinear optical security system based on a joint transform correlator in the Fresnel domain," App. Opt., 53, 1674-1682.

[10] M. S. Millán, E. Pérez-Cabré (2011) "Optical data encryption" in *Optical and Digital Image Processing: Fundamentals and Applications*, Edited by G. Cristóbal, P. Schelkens and H. Thienpont, Wiley-VCH Verlag GmbH&Co. KGaA.

[11] M. S. Millán (2012) "Advanced optical correlation and digital methods for pattern matching - 50th anniversary of Vander Lugt matched filter," J. Opt., 14, 103001.

Acknowledgments and Funding Information

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

3. Optical security based on near-field processes –

M. Naruse[1] and T. Matsumoto[2]
[1]National Institute of Information & 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, requiring innovative physical principles and technologies to overcome their limitations [1]. Along this vein, optical processes in the subwavelength-scale (or optical near-fields) are able to break through the diffraction limit of conventional propagating light [2]. 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 [3]. 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 [4], hierarchical holograms [5], and authentication [6]. 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 (Fig. 1) [5].

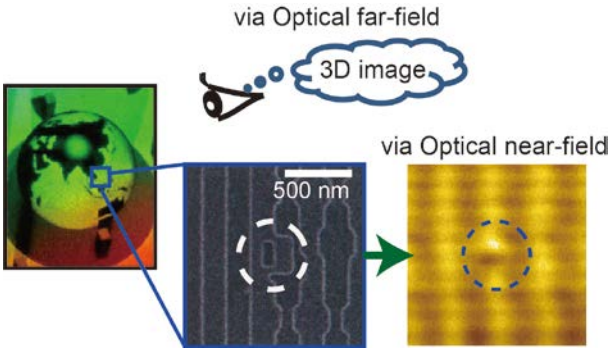


Figure 1 – Hierarchical hologram that acts as a conventional hologram in the optical far-field but contains additional information retrieved only via optical near-fields.

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* [7]. 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* [8], which exploits levels of physical randomness that are technologically impossible to reproduce. This concept is discussed in further detail below.

Other important challenges of subwavelength optics include the applications of optical metamaterials or metasurfaces [9] for security applications. For example, unidirectional light propagation, or non-reciprocal light propagation, made possible by optical metamaterials [10], 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 [8]. 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. Fig. 2(a) shows a scanning electron microscopy (SEM) image of collapsed resist pillars. In total, 2,401 samples were fabricated and evaluated per their use for potential security applications. As observed in Fig. 2(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 Fig. 2(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 [10], 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 highly 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.

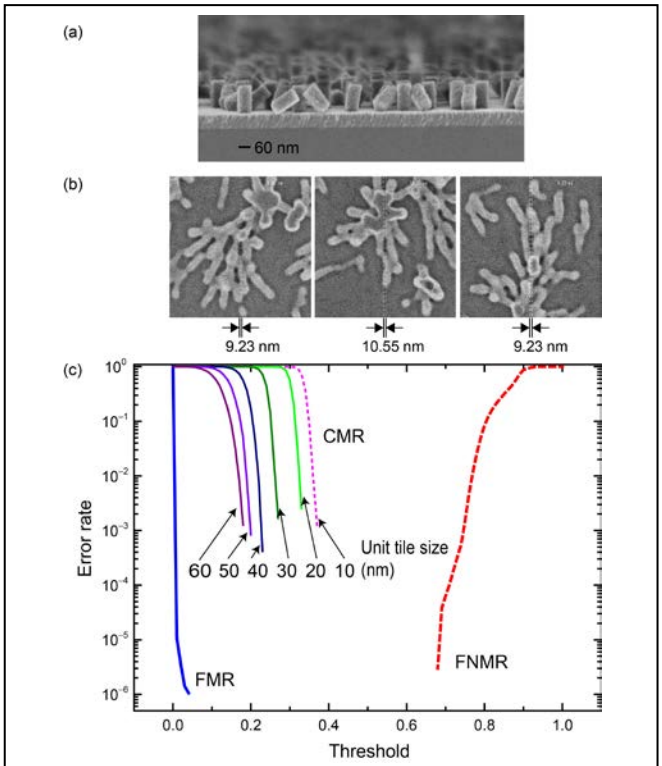


Figure 2 – Nano-artifact metrics. See text for details.

References

[1] R. L. van Renesse, Optical Document Security (Boston, Artech House Publishers, 2005).

[2] M. Naruse, N. Tate, M. Aono, and M. Ohtsu: Information physics fundamentals of nanophotonics, Reports on Progress in Physics, Vol. 76, No. 5, pp. 056401 1-50 (2013).

[3] M. Naruse, N. Tate, and M. Ohtsu, Optical security based on near-field processes at the nanoscale, Journal of Optics, Vol. 14, No. 9, pp. 094002 1-13 (2012).

[4] M. Naruse, H. Hori, K. Kobayashi, M. Ishikawa, K. Leibnitz, M. Murata, N. Tate, and M. Ohtsu, Information theoretical analysis of hierarchical nano-optical systems in the subwavelength regime, Journal of the Optical Society of America B, Vol. 26, No. 9, pp. 1772–1779 (2009).

[5] N. Tate, M. Naruse, T. Yatsui, T. Kawazoe, M. Hoga, Y. Ohyagi, T. Fukuyama, M. Kitamura, and M. Ohtsu, Nanophotonic code embedded in embossed hologram for hierarchical information retrieval, Optics Express Vol. 18, No. 7, pp. 7497-7505 (2010).

[6] N. Tate, H. Sugiyama, M. Naruse, W. Nomura, T. Yatsui, T. Kawazoe, and M. Ohtsu, Quadrupole–Dipole Transform based on Optical Near-Field Interactions in Engineered Nanostructures, Optics Express, Vol. 17, No. 13, pp. 11113-11121 (2009).

[7] H. Matsumoto and T. Matsumoto, Clone match rate evaluation for an artifactmetric system, IPSJ Journal Vol. 44, pp. 1991–2001 (2003).

[8] T. Matsumoto, M. Hoga, Y. Ohyagi, M. Ishikawa, M. Naruse, K. Hanaki, R. Suzuki, D. Sekiguchi, N. Tate, and M. Ohtsu, Nano-artifact metrics based on random collapse of resist, Scientific Reports, Vol. 4, Article No. 6142 (2014).

[9] N. I. Zheludev and Y. S. Kivshar, From metamaterials to metadevices, Nature Materials, Vol. 11, pp. 917 (2012).
[10] M. Naruse, H. Hori, S. Ishii, A. Drezet, S. Huant, M. Hoga, Y. Ohyagi, T. Matsumoto, N. Tate, and M. Ohtsu, Unidirectional light propagation through two-layer nanostructures based on optical near-field interactions, Journal of Optical Society of America B Vol. 31, No. 10, pp. 2404-2413 (2014).

Acknowledgments and Funding Information

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.

4. Attacking linear canonical transform based DRPE 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 Phase 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 1990 [1], many optical encryption techniques have been developed which employ variations of the classical Fourier transform (FT) based DRPE system such as Fractional Fourier transform (FRT) [2], Fresnel transform (FST) [3], Linear Canonical transform (LCT) [4] and Gyrator transform (GT) based DRPE systems [5].

Cryptanalysis of the FT based Amplitude Encoding (AE) DRPE system was first reported by Carnicer [6] in 2005 who proved that the classical FT based AE DRPE system has a security flaw against chosen-ciphertext attack (CCA). In [7, 8] 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 known plaintext and ciphertext attack (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 $\boldsymbol{z_1}$ and $\boldsymbol{z_2}$ in the systems provide additional keys to achieve higher security [3]. To our knowledge, method 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 [4] is a three-parameter class of linear integral transform. The 2D separable LCT of an input image field *I* is:

$$\boldsymbol{\Theta_{\alpha,\beta,\gamma}\{I\}} = \boldsymbol{C_1}\iint_{-\infty}^{+\infty}\boldsymbol{I}\times\exp\{i\pi[\alpha(x^2+y^2)-2\beta(ux+vy)+\gamma(u^2+v^2)]\}dxdy. \quad (1)$$

As a variation of FT based AE DRPE system, the LCT based AE DRPE system is given by [4]

$$\boldsymbol{E(x'',y'')} = \boldsymbol{\Theta_{\alpha_2,\beta_2,\gamma_2}\{\Theta_{\alpha_1,\beta_1,\gamma_1}\{I\times D1\}\times D2\}}, \quad (2)$$

where $\boldsymbol{D1(x,y)} = \exp\{i2\pi n_1(x,y)\}$ and $\boldsymbol{D2(x',y')} = \exp\{i2\pi n_2(x',y')\}$.

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

$$\boldsymbol{E(x'',y'')} = \exp\{i\pi\gamma_2(x''^2+y''^2)\}FT\{FT\{I\times D1'\}\times D2'\}, \quad (3)$$

where

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

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

Known Plain Text Attack: For a KPCA process, the input image $\boldsymbol{I(m,n)}$ and the ciphertext $\boldsymbol{E(m'',n'')}$ are available to the attacker. The first step in the process is to determine the parameter $\boldsymbol{\gamma_2}$ which is used as the chirp multiplication. The parameter $\boldsymbol{\gamma_2}$ appearing in Eq. (3) can be found by searching between 0 and 1 in increments of $\Delta\boldsymbol{\gamma}$. We denote the l^{th} value in this search by $\boldsymbol{\gamma_l} = \Delta\boldsymbol{\gamma l}$. The total number of increments is denoted by *L*, therefore $\Delta\boldsymbol{\gamma L} = \boldsymbol{1}$.

The following equation describes the decryption process.

$$|\boldsymbol{FFT}\{\boldsymbol{I(m,n)}\times\boldsymbol{D1'}\}| = \left|\boldsymbol{IFFT}\left\{\boldsymbol{E(m'',n'')}\times\exp\{-i\pi\gamma_l[(m'')^2+(n'')^2]\}\right\}\right|. \quad (4)$$

$\left|\boldsymbol{IFFT}\left\{\boldsymbol{E(m'',n'')}\times\exp\{-i\pi\gamma_l[(m'')^2+(n'')^2]\}\right\}\right|$ represents the l^{th} guessed amplitude in the Fourier

domain (Fourier image), while $\boldsymbol{I(m,n)}$ is the amplitude in space domain (object image).

Given the l^{th} guessed Fourier image and the object image $\boldsymbol{I(m,n)}$, 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 $\boldsymbol{\gamma_l}$, i.e. $\boldsymbol{\exp\{-i\pi\gamma_l[(m'')^2+(n'')^2]\}}$. We then calculate the Sum-Squared-Error (SSE) value (discussed later) between the retrieved amplitude in the Fourier Domain and the given l^{th} 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. $\boldsymbol{\exp\{-i\pi\gamma_l[(m'')^2+(n'')^2]\}}$, for l=1, 2, … , L, are obtained. The chirp multiplication that results in the lowest SSE value is used to determine the most appropriate $\boldsymbol{\gamma_l}$ value, which is denoted by $\boldsymbol{\gamma'}$. 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.

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

Following the determination of $\boldsymbol{\gamma'}$, Eq. (4) can be rewritten as

$$\boldsymbol{|FFT\{I(m,n)\times D1'\}|} = \left|\boldsymbol{IFFT}\left\{\boldsymbol{E(m'',n'')}\times\boldsymbol{\exp\{-i\pi\gamma'[(m'')^2+(n'')^2]\}}\right\}\right|. \quad (5)$$

In the next step, GS/HIOA is used to perform KPCA to retrieve the correct RPKs. In order to proceed we define the Sum-Squared-Error (SSE).

$$\boldsymbol{SSE = 10\log_{10}\left\{\frac{\sum_{m=1}^{M}\sum_{n=1}^{N}\{|F'(m,n)|-|F(m,n)|\}^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}\{|F(m,n)|\}^2}\right\}}. \quad (6)$$

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

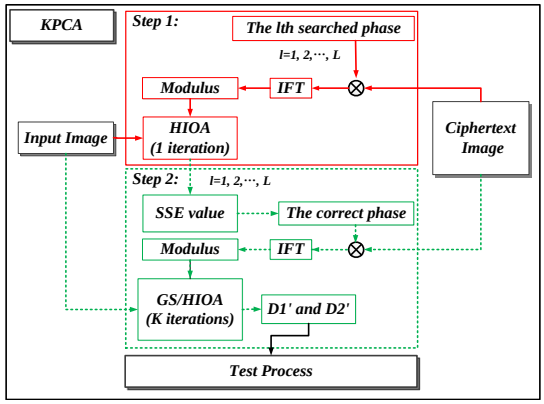


Fig. 1. Flow diagram of the iterative KPCA process.

The GS/HIOA [7, 8] is applied to retrieve the LCT based AE DRPE RPKs. The process for performing the KPCA is illustrated in Fig. 1.

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 by GS/HIOA (1, 39)

Testing results: In order to test the validity of our approach, two other test images, see Fig. 2, are encrypted using the same RPKs and the same LCT operations as were used for the original input I image field. After retrieving the two RPKs, we decrypt the encrypted test images using the resulting iteratively retrieved RPKs.

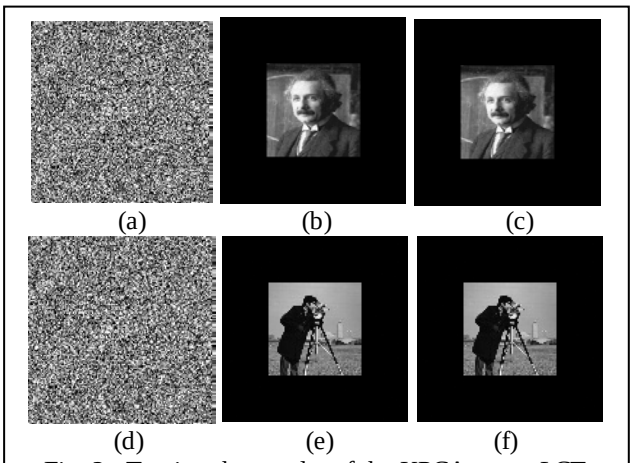


Fig. 2. Testing the results of the KPCA on an LCT based AE DRPE system. Einstein image: (a) encrypted; (b) plaintext; (c) the decrypted image. Cameraman image: (d) encrypted; (e) plaintext; and (f) the decrypted image.

The results presented in Fig. 2 indicate that the chirp multiplication factor $\boldsymbol{\gamma}$, 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 Mean Squared Error (MSE) values of 0.14236 and 0.16161 for the decrypted 'Einstein' and 'Cameraman' image above, are calculated. These provide quantitative evidence that the test images have been accurately retrieved.

Concluding Remarks – The vulnerability of the Linear Canonical transform (LCT) based Amplitude Encoding (AE) Double Random Phase Encryption (DRPE) system to Known-Plaintext Ciphertext Attack (KPCA) is examined using the phase retrieval methods developed. It is demonstrated that the algorithms (GS/HIOA) can successfully retrieve the two Random Phase Keys (RPKs) used in LCT based AE DRPE systems.

References

[1] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett., 20(7), 767-769 (1995).
[2] B. M. Hennelly and J. T. Sheridan, “Fractional Fourier transform-based image encryption phase retrieval algorithm,” Opt. Commun., 226, 61-80 (2003).
[3] G. Situ and J. Zhang, “Double random-phase encoding in the Fresnel domain,” Opt. Lett., 29(14), 1584-1586 (2004).
[4] G. Unnikrishnan and K. Singh, “Optical encryption using quadratic phase systems,” Opt. Commun., 193, 51-67 (2001).
[5] N. Singh and A. Sinha, “Gyrator transform-based optical image encryption, using chaos,” Opt. Las. Eng., 47(5), 539–546 (2009).
[6] A. Carnicer, M. M. Usategui, “Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys,” Opt. Lett., 30(13), 1644-1646 (2005).
[7] C. Guo, S. Liu, and J. T. Sheridan, “Iterative phase retrieval algorithms. I: Optimization,” Appl. Opt., 54(15), 4698-4708 (2015).
[8] C. Guo, S. Liu, and J. T. Sheridan, “Iterative phase retrieval algorithms. Part II: Attacking optical encryption systems,” Appl. Opt., 54(15), 4709-4719 (2015).

Acknowledgments and Funding Information

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.
Email: *john.sheridan@ucd.ie*

5. Highly focused vector fields encryption –

Artur Carnicer and Ignasi Juvells
Universitat de Barcelona

Status – Optical encryption techniques derived from the original double random keys method have attracted the interest of many authors [1]. 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 [2] but security can be enhanced by increasing the number of degrees of freedom of this approach. Among many others, it has been suggested the use of polarized light [3], a combination of real and virtual optics methods [4] or recording the encrypted distribution in photon starving conditions [5]. In this contribution we introduce a new approach for optical encryption based on the manipulation of fields in the focal area: the information is encoded in the longitudinal component of the focussed field. The energy associated to this component is very weak and difficult to detect since it is embedded in the transversal part of the field. Nevertheless, information can be authenticated or decrypted by an authorised user with the help of the Gauss law.

Current and Future Challenges –The electric field **E** at the focal plane of a high numerical aperture (NA) microscope lens following the sine condition is described by the so-called Richards-Wolf integral [6]:

$$\mathbf{E}(r,\phi,0) = A\int_0^{\theta_0}\int_0^{2\pi} \mathbf{E}_\infty(\theta,\varphi) \times \exp\left(ikr\sin\theta\cos(\phi-\varphi)\right)\sin\theta\, d\theta\, d\varphi \quad (1)$$

where A is a proportionality constant, k is the wavelength, 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. $\mathbf{E}_\infty$ is the vector angular spectrum of plane waves, described as [7]:

$$\mathbf{E}_\infty = \sqrt{\cos\theta}\,(f_1\mathbf{e_1} + f_2\mathbf{e_2}). \quad (2)$$

Functions f_1 and f_2 are the azimuthal and radial parts of the transverse input field $\mathbf{E_0} = (E_{0x}, E_{0y}, 0)$

$$\begin{aligned} f_1 &= \mathbf{E_0}\cdot\mathbf{e_1} = -E_{ox}\sin\varphi + E_{0y}\cos\varphi \\ f_2 &= \mathbf{E_0}\cdot\mathbf{e_2^i} = E_{0x}\cos\varphi + E_{0y}\sin\varphi \end{aligned}; \quad (3)$$

where $\mathbf{e_1}$ and $\mathbf{e_2}$ 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 (see Fig. 1 for details):

$$\begin{aligned} \mathbf{e_1} &= (-\sin\varphi, \cos\varphi, 0) \\ \mathbf{e_2^i} &= (\cos\varphi, \sin\varphi, 0) \\ \mathbf{e_2} &= (\cos\theta\,\cos\varphi, \cos\theta\sin\varphi, \sin\theta) \end{aligned}. \quad (4)$$

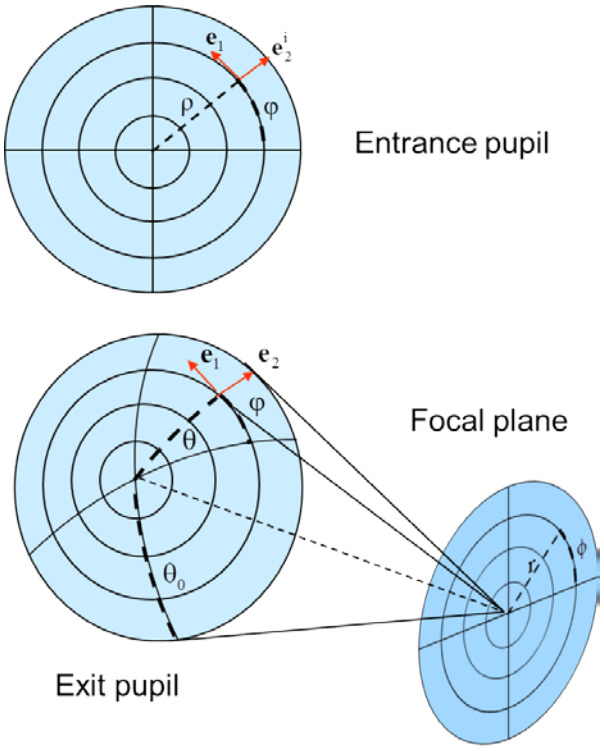


Figure 1 – Notation and coordinate systems at the entrance and exit pupils, and at the focal plane.

It is worth to point out that despite that the incident beam is purely transverse, i.e. E_{0z}=0, the electric field in the focal area E shows a non-negligible longitudinal component E_z and thus polarization has to be described as a 3D phenomenon. Nevertheless, the irradiance associated to the longitudinal component I_z

$$I_z = \int |E_z|^2 dr d\phi \quad (5)$$

is very small when compared with the irradiance of the transverse component I_t

$$I_t = \int \left(|E_x|^2 + |E_y|^2\right) dr d\phi\,. \quad (6)$$

For instance, when the input beam is circularly polarized, i.e. E_{0x} = i E_{0y}, $I_z \approx 0.003 I_t$ [7]. Note that the z-component of the focal electric field cannot be easily separated from the other two components using linear polarizers and holographic recording. However, E_z can be numerically accessed by means of the Gauss law $\nabla\cdot\mathbf{E} = 0$. In Fourier space, the divergence theorem reads

$$\begin{aligned} &\mathbf{s}\cdot\tilde{\mathbf{E}} = 0 \\ &\alpha\tilde{E}_x + \beta\tilde{E}_y + \gamma\tilde{E}_z = 0 \end{aligned}, \quad (7)$$

being $\tilde{\mathbf{E}} = \left(\tilde{E}_x, \tilde{E}_y, \tilde{E}_z\right) = \mathrm{FT}[\mathbf{E}]$ the Fourier transform of the field at the focal plane **E**; α and β are the spatial frequencies and $\gamma = \sqrt{1-\alpha^2-\beta^2}$. Since $E_z \ll E_x, E_y$ the longitudinal component E_z can be deduced from [8]:

$$\tilde{E}_z(\alpha,\beta) = -\frac{\alpha\tilde{E}_x + \beta\tilde{E}_y}{\sqrt{1-\alpha^2-\beta^2}} \quad . \qquad (8)$$
$$E_z = \mathrm{FT}^{-1}\left[\tilde{E}_z\right]$$

The presented formalism enables the possibility to encode information in the longitudinal component E_z; but note that only the transversal components *x* and *y* are physically accessible. According to Eq. (2), the longitudinal component of the vector angular spectrum reads

$$E_{\infty z} = \sqrt{\cos\theta}\left(E_{0x}\cos\varphi + E_{0y}\sin\varphi\right)\sin\theta \, . \qquad (9)$$

If circularly polarized light is used, then $E_{\infty z} = E_{0x}\sqrt{\cos\theta}\sin\theta\exp(i\varphi)$. However, note that any polarization of the input beam can be used (linear, radial, azimuthal, spiral, and etcetera). Here we select circular polarization for the sake of simplicity. From Eq. (1) it follows that E_z and $E_{\infty z}$ are related by an inverse Fourier transform, $E_{\infty z} = \mathrm{FT}^{-1}[E_z]$, and thus the input beam E_0 = (E_{0x}, iE_{0x}, 0) that generates a custom E_z distribution becomes

$$E_{0x} = \frac{e^{i\phi}}{\sqrt{\cos\theta}\sin\theta}\mathrm{FT}^{-1}[E_z] \, . \qquad (10)$$

Eq. (10) describes how to encode an image in the longitudinal component E_z. It is also possible to encrypt the information using a double random phase encoding approach by using phase masks M_1 and M_2,

$$E'_{0x} = \frac{e^{i\phi}M_2}{\sqrt{\cos\theta}\sin\theta}\mathrm{FT}^{-1}[M_1 E_z] \, . \qquad (11)$$

To enhance security we use two different masks M_{2x} and M_{2y} for the *x* and *y* components of the incident beam. Moreover, in order to avoid conventional attacks against double random mask cryptosystems, these distributions can be recorded in photon starved conditions [5,9]. After propagation, the field components in the focal area E'_x and E'_y hide the encrypted z-component. Nevertheless, the information can be decrypted or verified (if photon-counting is used) by means of

$$E_z = \left|\mathrm{FT}^{-1}\left[-\frac{\alpha\tilde{E}'_x/M_{2x} + \beta\tilde{E}'_y/M_{2y}}{\sqrt{1-\alpha^2-\beta^2}}\right]\right| \quad . \qquad (12)$$

Advances in Science and Technology to Meet Challenges – The encryption procedure described can be implemented optically using an optical system able to tailor beams with custom amplitude and polarization [10]. These systems enable to manipulate arbitrary polarization information and thus, increase the degrees of freedom available when compared with conventional scalar cryptosystems. 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. Figure 2 sketches the optical setup required to perform focused vector fields encryption. The input 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 computer generated holograms to encode complex transmittances E'_{ox} and E'_{oy}. The beam is focused by means of a high NA microscope objective, reflected in the observation plane and finally, holographically recorded by the CCD camera.

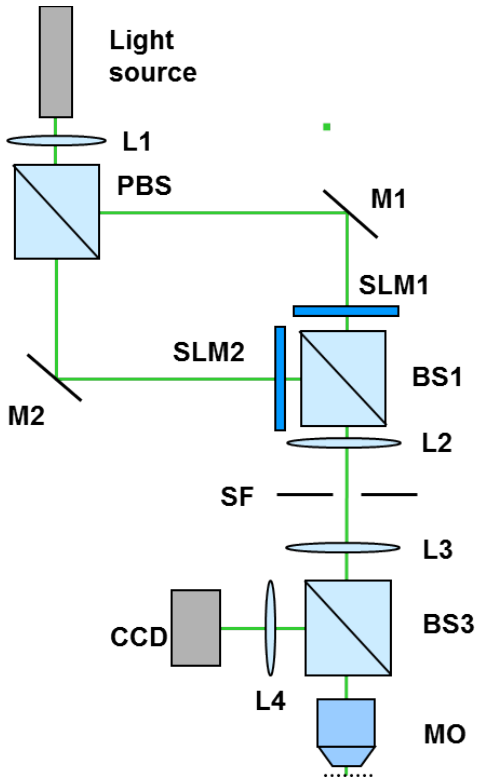


Figure 2 – Focalization system and detection setup. L1, L2, L3 lenses, M1 and M2 mirrors, PBS polarizer beam splitter, BS1 and BS2 beam splitters, SF spatial filter, SLM1, and SLM2 spatial light modulators, CCD camera, and MO high NA microscope objective. The dotted line shows the observation plane.

Concluding Remarks – We have proposed 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 to this component is embedded in the total detected field and (ii) the energy associated to the *z*-component is very low. This makes detection of the longitudinal component very difficult. However,

information can be properly decoded by an authorised user with access to the encryption keys by using the Gauss law. The system we propose can be implemented in practice with conventional optical elements.

References

[1] P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767–769 (1995).

[2] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett. **30**, 1644-1646 (2005)

[3] O. Matoba and B. Javidi, "Secure holographic memory by double-random polarization encryption," Appl. Opt. 43(14), 2915–2919 (2004).

[4] W. Chen and X. Chen, "Space-based optical image encryption," Opt. Express 18, 27095-27104 (2010)

[5] E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett. **36**, 22–24 (2011).

[6] B. Richards and E. Wolf, "Electromagnetic diffraction in optical systems. II. Structure of the image field in an aplanatic system," P. Roy. Soc. London A Mat. **253**, 358–379 (1959).

[7] D. Maluenda, R. Martínez-Herrero, I. Juvells, and A. Carnicer, "Synthesis of highly focused fields with circular polarization at any transverse plane," Opt. Express **22**, 6859-6867 (2014).

[8] A. Carnicer, I. Juvells, D. Maluenda, R. Martínez-Herrero and P. M Mejías, "On the longitudinal component of paraxial fields," Eur. J. Phys. **33**, 1235-1247 (2012).

[9] D. Maluenda, A. Carnicer, R. Martínez-Herrero, I. Juvells, and B. Javidi, "Optical encryption using photon-counting polarimetric imaging," Opt. Express **23**, 655-666 (2015).

[10] D. Maluenda, I. Juvells, R. Martínez-Herrero, and A. Carnicer, "Reconfigurable beams with arbitrary polarization and shape distributions at a given plane," Opt. Express **21**, 5432-5439 (2013)

Acknowledgments and Funding Information

The authors are grateful to Prof. Rosario Martínez-Herrero and Mr. David Maluenda for helpful discussions.

This research is funded by Ministerio de Economía y Competitividad (Spain), project FIS2013-46475-C3-2-P.

6. Security issues and the urge for the development of 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, 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 of all the possible distributions for the key. It was 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 $\mathbf{2}^{\mathbf{2,097,152}}$, 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 the 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, and authentication verification, et al. The original DRPE technique has also been extended to the fractional Fourier domain, Fresnel domain, as well as using other canonical transforms such as 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 [2] 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 [3]. 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 resource at that time, it took them 2 hours to find the key of the size $\mathbf{100}\times\mathbf{100}$ pixels. The linear relationship between the plaintext and the 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 [4-6] 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.

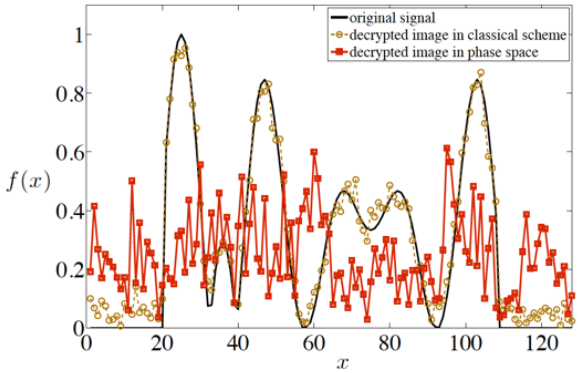


Figure 1. Resistance of the encryption technique in phase space against the phase-retrieval-based attacks [4]. In the simulations, we assumed that 4 pairs of plaintext-cyphertext were known to the attacker. With this information, the cryptanalysis algorithm attempts to recover the two RPKs, and subsequently use the recovered RPKs as keys to decode a cyphertext of an unknown plaintext (black solid line). The results clearly suggest that the cryptanalysis failed to to attack the proposed scheme (red curve with square markers). [from Ref. [8]]

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 system, working in either optical or numerical mode. But we need a rigorous information security theory to provide a unified framework for all these optical techniques. Taking a look at the counterpart of quantum information security [7], we get an impression of what a serious situation our community is faced with. Without this theory, not to say it is hard to communicate with the 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, a logical 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) [8]. The encryption is a two-step process: we first transform the signal into its AF, which is then encrypted into white noise using the traditional DRPE technique. We have demonstrated that this encryption in phase space is resistant against various attacks including the impulse response attack designed by Carnicer et al [2], and the phase-retrieval-based attacks [4], as depicted in Fig. 1. One can even replace the various canonical transforms used in traditional DRPE by a true nonlinear transform. For instance, one can place a photorefractive crystal in between the two neighboring planes in the DRPE system, connecting them with a nonlinear, rather than linear, wave propagation that is described by the nonlinear Schrödinger equation [9]. Owing to the self-modulation effect, nonlinear propagation in this way is intensity dependent, meaning that the intensity pattern 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 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 we did not know how to represent the entropy of a complex wave field, whereas the traditional information theory only deals with intensity data. 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 makes me believe that the Wigner distribution function may be a good starting point as well. But ieither way, this is a very comprehensive 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 to mention that there are other techniques such as photon-counting encryption [10] under development to address this issue as well. Detailed discussion is out of the scope of this article.

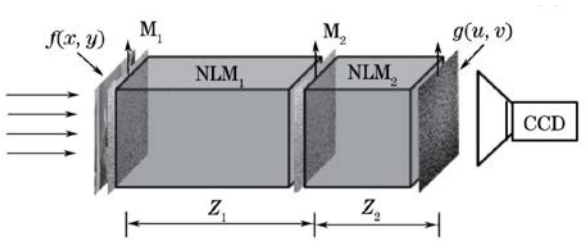


Figure 2. A proposed nonlinear optical encryption scheme. Here the linear canonical transform between two neighbouring planes in the traditional DRPE is replaced by a nonlinear propagation by virtue of the two nonlinear photorefractive crystals (NLM1, and NLM2). The linear relationship between the cyphertext and plaintext does not hold in this nonlinear optical encryption system, resulting in the enhancement of security

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.

References

[1] P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. 20, 767–769 (1995)..

[2] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnearability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett., 30, 1644-1646 (2005).

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

[4] G. Situ, U. Gopinathan, D. S. Monaghan, and J. T. Sheridan, "Cryptanalysis of optical security systems with significant output images," Appl. Opt. 46, 5257 – 5262 (2007).

[5] G. Situ, D. S. Monaghan, T. J. Naughton, J. T. Sheridan, G. Pedrini and W. Osten, "Collision in double random phase encoding," Opt. Commun. 281, 5122 – 5125 (2008).

[6] G. Situ, G. Pedrini, and W. Osten, "Strategy for cryptanalysis of optical encryption in the Fresnel domain," Appl. Opt. 49, 457-462 (2010).

[7] H. Imai, and M. Hayashi, Quantum Computation and Information, Springer (2006).

[8] J. Liu, X. Xu, Q. Wu, J. T. Sheridan, and G. Situ, "Information encryption in phase space," Opt. Lett., 40, 859-862 (2015).

[9] J. Hou, S. Huang, and G. Situ, “Nonlinear optical image encryption,” (in Chinese), in conference of LTO, Shanghai Mar. 16-17 (2015).
[10] D. Maluenda, A. Carnicer, R. Martinez-Herrero, I. Juvells , and B. Javidi, “Optical encryption using photon-counting polarimetric imaging,” Opt. Express 23, 655-666 (2015).

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

7. 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 as 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 the data to avoid its unauthorized access. In the last few decades, optical techniques for information security have advanced. It has now formed an adequate framework for developing robust data protection techniques. This is evidenced with the availability of literature on this research area [1-10].

Most of the reported optical security techniques in 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 [1]. Cryptanalysis indicates that the weakness of security originated from the linearity of the cryptosystem. Qin and Peng [2] 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 the conventional optical cryptosystems [3].

The PTFT is a process of Fourier transform 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 [4]. Figure 1 shows the 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 special attack [6-8]. In special attack, the attacker uses a randomly generated random phase mask with the encrypted image and tries to retrieve the original information. Further, several image encryption techniques have been demonstrated with improvising the basic asymmetric framework with enhanced strength. The improvement is mainly with the use of polarization encoding and different optical transforms, such as, Fresnel transform, fractional Fourier transform, gyrator transform, and wavelet transform [4-10]. 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 use of phase-only spatial light modulators.

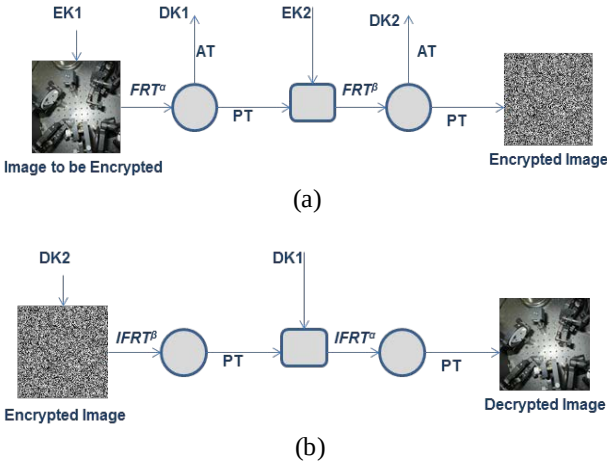


Figure 1 – Block diagram for amplitude – and phase-truncation based optical asymmetric cryptosystem. (a) Encryption process and (b) decryption process. EK: encryption key, DK: decryption key, AT: amplitude truncation, PT: phase truncation, FRT: fractional Fourier transform

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 publication of an attack followed by publication of an 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 challenges lie in terms of hardware implementation with low cost commercially available components and devices but without any compromise with 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 the 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 subject to 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 gray-scale images, optical techniques for securing color information have also attracted attention of the research community [1,5]. Binary or gray-scale images are encrypted and decrypted by a 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 2 shows the block diagram for color image encryption, in which there are two schemes; three channel systems, as shown in Fig. 2(a), and single channel systems, as shown in Fig. 2(b). Each of these schemes is suitably combined with the asymmetric encryption approach as shown in Fig. 1.

Further, securing multispectral data is becoming an important issue because such data received from satellites and airborne sensors are being increasingly available for further processing and analysis for various applications. For multispectral data security, asymmetric cryptosystems employing image fusion techniques have been proposed [9,10]. In a fusion technique, the low and high frequency components are merged together to improve the information content. 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 are to be carried out. The 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

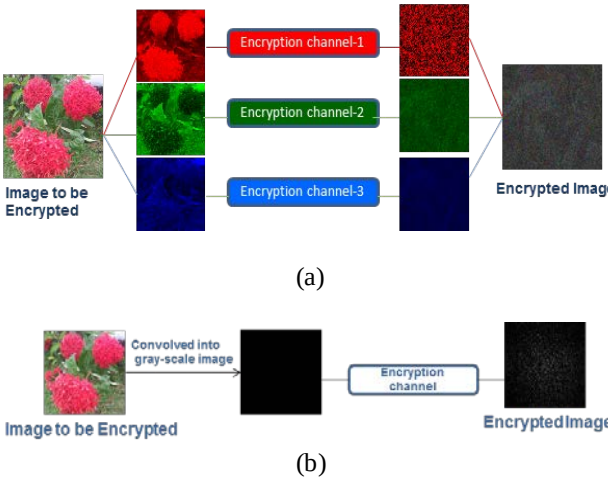


Figure 2 – Block diagram for colour image encryption. (a) three channel and (b) single channel.

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.

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 the 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. Now 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 have already been reported and much more is yet to be explored.

References

[1] B. Javidi, Ed., *Optical and Digital Techniques for Information Security*, Springer, 2005.

[2] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," Opt. Lett. 35 (2010) 118-120.

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

[4] S. K. Rajput and N. K. Nishchal, "Image encryption based on interference that uses fractional Fourier domain asymmetric keys," Appl. Opt. 51 (2012) 1446-1452.

[5] S. K. Rajput and N. K. Nishchal, "Asymmetric color cryptosystem that uses polarization selective

diffractive optical element and structured phase mask," Appl. Opt. 51 (2012) 5377-5386.
[6] S. K. Rajput and N. K. Nishchal, "Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform," Appl. Opt. 52 (2013) 871-878.
[7] S. K. Rajput and N. K. Nishchal, "Known-plaintext attack on encryption domain independent optical asymmetric cryptosystem," Opt. Commun. 309 (2013) 231-235.
[8] S. K. Rajput and N. K. Nishchal, "Fresnel domain nonlinear image encryption scheme based on Gerchberg-Saxton phase retrieval algorithm," Appl. Opt. 53 (2014) 418-425.
[9] I. Mehra and N. K. Nishchal, "Image fusion using wavelet transform and its application to asymmetric cryptosystem and hiding," Opt. Express 22 (2014) 5474-5482.
[10] I. Mehra and N. K. Nishchal, "Wavelet-based image fusion for securing multiple images through asymmetric keys," Opt. Commun. 335 (2015) 153-160.

Acknowledgments
I thankfully acknowledge the fruitful discussions with Sudheesh K. Rajput, Isha Mehra, Dhirendra Kumar, and Areeba Fatima.

8. Cryptanalysis and attempts on optical asymmetric and one-way cryptosystems –

Wenqi He and Xiang Peng
Shenzhen University

Status – The issue for 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 Fresnel domain, DRPE in fractional Fourier domain, DRPE in other transform domains. The concept of the 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 [2]. 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 [3]. Soon after, Peng *et al.* also presented an effective attack to DRPE by taking advantage of the phase retrieval algorithm [4]. Moreover, Peng's method can be modified to break down most of the 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 [5]. To this point, it is clear that the investigators of optical information security should make continuous efforts on designing various schemes for data security systems while evaluating the 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 out the plaintext by extracting the secret key(s) of an optical cryptosystem with the help of some priori knowledge, e.g. plaintext-ciphertext pair(s), or even just ciphertext(s). It should be noted that the priori knowledge can come from Kerckhoffs' principle, which is regarded as a fundamental rule in the field of cryptanalysis [5]. 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, a number of the reported works in this area are limited to exploit theoretical feasibilities of optical cryptosystems while successful experimental demonstrations, even in the early stage of proof-of-concept, appear much less than theoretical works. This awkward situation is mainly caused by a paradox between the off-the-shelf available optical components/devices and the really desired ones. The unavoidable systematical errors are another reason that doing experiments for optical security techniques are troublesome.

For now, let's turn to the theoretical attempts in the field of optical information security. We'd like to indicate that most of the contributions are categorized as three aspects [5]: (1) image encryption, (2) information hiding, and (3) personal authentication. But for their further sub-classes, there are still some important issues 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 non-linear 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 made on this aspect. 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 it has to fulfill 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). [6]. Another work involved constructing an optical asymmetric cryptosystem [7]. The proposed PTFT (refer to Ref. [6-7] 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 the 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 the 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 [8]. 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 [9].

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, the advances in nonlinear optics and even the 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 to fabricate some compact and integrated optical devices and systems with the functionalities of encryption or authentication. That will further push forward the applications of optical security technologies.

Concluding Remarks – In conclusion, we have briefly reviewed the 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.

References

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Optics Letters, 20(7), 767-769 (1995).

[2] W. Chen, B. Javidi, and X. Chen, "Advances in Optical security system," Advances in Optics and Photonics, 6(2), 120-155 (2014).

[3] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," Optics Letter, 30(13), 1644-1646 (2005).

[4] X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Optics Letters, 31(8), 1044-1046 (2006).

[5] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, second ed., John Wiley & Sons, Hoboken, 1996.

[6] W. He, X. Peng, W. Qin, and X. Meng, "The keyed optical Hash function based on cascaded phase-truncated Fourier transforms," Optics Communications, 283(11), 2328-2332 (2010).

[7]. W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," Optics Letters, 35(2), 118-120 (2010).

[8] W. He, X. Meng, and X. Peng, "Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm: comment," Optics Letters, 38(20), 4044 (2013).

[9] X. Wang and D. Zhao, "A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms," Optics Communications, 285(6), 1078-1081 (2012).

Acknowledgments and Funding Information

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

9. Compressive sensing for optical encryption –

Adrian Stern[1] and Yair Rivenson[2]
[1]Ben-Gurion University of the Negev
[2]University of California

Status – Since its first publication less than a decade ago, the innovative theory of Compressive Sensing (CS) [1] 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 the CS theory with optical encryption techniques.

Compressive sensing 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, $\mathbf{g}=\mathbf{\Phi f}$. Compressive sensing 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 [1]. For universal sensing, the most common type of sensing matrix $\mathbf{\Phi}$ is a random matrix, that is, a matrix with independent and identically distributed 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 [1] .

The impetus for using CS for encryption is the random type of transform together with the dimensionality reduction (compression). The obtained "image" $\mathbf{g}=\mathbf{\Phi f}$ has: 1) a lower dimension ($M<N$), and 2) it 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 1 shows an example of a combination of CS with the well-known double random phase encoding (DRPE) encryption scheme [2]. 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 4-F 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

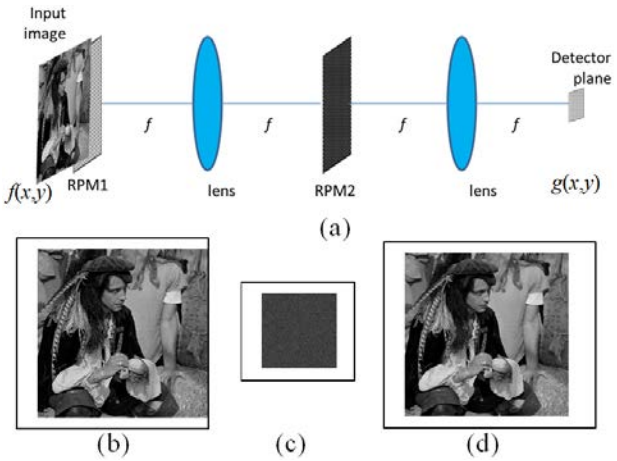


Figure 1. (a) CS-DRPE scheme. (b) plaintext image (1024x1024 pixels), (c) encrypted image (400x400 pixels.), (d) decrypted image.

CS system with random entries [3]. The entropy of the encrypted image in Fig. 1(c) is with more than 10 bits/pixel higher than of the plaintext. The plaintext $f(x,y)$ is recovered from the cipher text $g(x,y)$ by using algorithms prescribed by the CS theory (in this example TwIST [1]). For the results shown in Fig. 1 the phase masks act as keys and the CS is utilized to allow a detector with fewer pixels than the encoded image.

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., [4-6]). 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 utilized CS within the optical setup. For example, the CS approach has been embedded with various DRPE schemes (e.g., [7, 8]), included in holographic schemes (e.g., [9]), applied with various ghost imaging schemes (e.g., [10]) and for photon entangled sensing (e.g., [11, 12]).

Current and Future Challenges – the benefits, limitations, and challenges in using CS for optical encryption. The main benefit of CS-based optical encryptions is the combined encryption-and-compression performance. Encryption and compression are related, therefore through 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 [13]. 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 the 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). 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 [12].
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 [14].
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 [15]. 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 [16]. 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 [17]. 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 posess 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 the 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 relay on "classical" optical encryption techniques. We believe that development of new, independent, schemes may offer additional improvements in terms

of encryption performance, optical implementation complexity and cost.

References

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

[2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, pp. 767-769, 1995.

[3] Y. Rivenson, A. Stern and B. Javidi. Single exposure super-resolution compressive imaging by double phase encoding. *Optics Express 18(14)*, pp. 15094-15103. 2010.

[4] P. Lu, Z. Xu, X. Lu and X. Liu. Digital image information encryption based on compressive sensing and double random-phase encoding technique. *Optik-International Journal for Light and Electron Optics 124(16)*, pp. 2514-2518. 2013.

[5] B. Deepan, C. Quan, Y. Wang and C. Tay. Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique. *Appl. Opt. 53(20)*, pp. 4539-4547. 2014.

[6] N. Rawat, B. Kim, I. Muniraj, G. Situ and B. Lee. Compressive sensing based robust multispectral double-image encryption [invited]. *Appl. Opt. 54(7)*, pp. 1782-1793. 2015.

[7] N. Rawat, I. Hwang, Y. Shi and B. Lee. Optical image encryption via photon-counting imaging and compressive sensing based ptychography. *Journal of Optics 17(6)*, pp. 065704. 2015.

[8] X. Wang, W. Chen and X. Chen. Optical information authentication using compressed double-random-phase-encoded images and quick-response codes. *Optics Express 23(5)*, pp. 6239-6253. 2015.

[9] J. Li, H. Li, J. Li, Y. Pan and R. Li. Compressive optical image encryption with two-step-only quadrature phase-shifting digital holography. *Opt. Commun. 344*pp. 166-171. 2015.

[10] P. Clemente, V. Durán, E. Tajahuerce and J. Lancis. Optical encryption based on computational ghost imaging. *Opt. Lett. 35(14)*, pp. 2391-2393. 2010.

[11] P. Zerom, K. W. C. Chan, J. C. Howell and R. W. Boyd. Entangled-photon compressive ghost imaging. *Physical Review A 84(6)*, pp. 061804. 2011.

[12] D. J. Lum, S. H. Knarr and J. C. Howell. Fast-hadamard transforms for compressive sensing of joint-systems: Measurement of a 16.8 million-dimensional entangled probability distribution. *To Appear in Optics Express* 2015.

[13] A. Alfalou and C. Brosseau. Optical image compression and encryption methods. *Advances in Optics and Photonics 1(3)*, pp. 589-636. 2009.

[14] N. Zhou, A. Zhang, F. Zheng and L. Gong. Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. *Optics & Laser Technology 62*pp. 152-160. 2014.

[15] Y. Rachlin and D. Baron. The secrecy of compressed sensing measurements. Presented at Communication, Control, and Computing, 2008 46th Annual Allerton Conference On. 2008, .

[16] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti and G. Setti. On known-plaintext attacks to a compressed sensing-based encryption: A quantitative analysis. *To Appear in IEEE Transactions on Information Forensics and Security* 2015.

[17] A. Stern, Y. Auguts and Y. Rivenson. Challenges in optical compressive imaging and some solutions. Presented at 10th International Conference on Sampling Theory and Applications SampTa, Vol. 24. 2013 .

10. Multiple-scattering materials as physical unclonable functions – Pepijn W.H Pinkse and Allard P. Mosk

University of Twente

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 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 Physical Unclonable Functions (PUFs) are ideal authentication keys [1]. 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.

Although the PUF cannot be copied, there is the risk of emulation: an attacker may have learned the characteristics of the PUF by covertly measuring them or by data theft. He then measures the challenge and fools the verifier by returning a computer-generated image of the expected speckle pattern. Quantum Secure Authentication (QSA) [2] has shown that PUF technology can be combined with quantum physics to provide a secure way of reading out optical PUFs even in a hands-off situation.

In practical authentication mechanisms one needs to consider cost and convenience as well as security. The use of optical PUFs provides high security against forging and emulation. With developments to reduce cost of the readout hardware and improve convenience, it can become the method of choice for securing financial transactions and access to facilities.

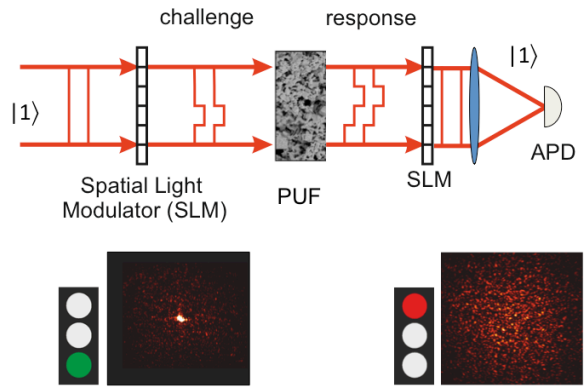


Figure 1 – Schematic of Quantum Secure Authentication. [2]. A few-photon wavefront is shaped into a complex wavefront by an SLM. The response is transformed again with another SLM such that only with the correct key, the output light will be focussed to a point, where an APD behind a pinhole measures 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, to 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 [3]. In future this can probably be scaled up to 10^4 to 10^5, which approaches the degrees of freedom of a PUF [4]. At the same time there is progress in the design of mode converters that convert 2D to 3D inputs and outputs, although the number of degrees of freedom is still small [5]. 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" [6], the term coined for hacking of quantum protocols by exploiting classical weaknesses in their implementation. For example, a hacker with sophisticated equipment could find out the settings of the spatial light modulators of a flawed readout device. The implementation of a readout system needs to be designed to be robust against such attacks.

Optical PUFs have already been proposed to provide random keys that can be used as one-time pad [7]. 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 against 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 technological progress. The importance of such predictions scales with the security level. For applications such as detection of product forgery [8], it is sufficient that the cost of forging the PUF is higher than that of the genuine product. Highly secure authentication systems that protect critical assets must be safe even under the assumption that an adversary has an infinite budget.

Secondly, many technological challenges are to be met to make optical readout as fast, reliable and convenient as possible. One may envision optical tracking systems that can read out the PUF on an ID card of a worker in passing, while at the same time performing biometrical authentication [9]. 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 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. Since these advances are also needed for the application of multimode fibers in endoscopic imaging [10] one can hope that the significant efforts being undertaken in that area will bring a solution which is also useful for remote readout of PUFs.

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.

References

[1] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, *Physical one-way functions*, Science **297**, 2026 (2002).

[2] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić, and P. W. H. Pinkse, *Quantum – Secure Authentication of a Classical Key*, Optica **1**, 421 *(2014)*

[3] J. Carolan *et al.*, *Universal Linear Optics*, Science DOI:10.1126/science.aab364 (2015)

[4] D. A. B. Miller, *How complicated must an optical component be?*, J. Opt. Soc. Am. A **30**, 238-251 (2013)

[5] J.-F. Morizur *et al.*, *Programmable unitary spatial mode manipulation*, J. Opt. Soc. Am. A **27**, 2524 (2010).

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

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

[8] W. Chen, B. Javidi, and X. Chen, *Advances in optical security systems*, Adv. Opt. Photon. **6**, 120-155 (2014).

[9] Y-L Chen *et al.*, *Extended depth of field system for long distance iris acquisition*, Proc. SPIE **8487**, 84870K; doi:10.1117/12.928192 (2012).

[10] S. Gigan, *Endoscopy slims down*, Physics **5**, 127 (2012)

Acknowledgments and Funding Information

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

11. Secure optical sensing – Masahiro Yamaguchi

Tokyo Institute of Technology

Status – The security of information systems is increasingly much more crucial in our life, as everything is going to be connected to the Internet. The information security technology is mostly constructed on the basis of mathematical theories of cryptography. However, the threat to information systems is still growing more, and it is definitely important to consider the system-level security to protect information resource 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 the all-digital based security measures. Then it is advantageous to integrating physical measures against increasing security threat.

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

A well-known optical encryption technique suitable for imaging applications is the one called 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 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 a 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 the 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.

Current and Future Challenges – The 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 the speckle noise can be suppressed by capturing multiple images with a changing illuminating random phase pattern [3], it increases the amount of data and may affect the security strength.

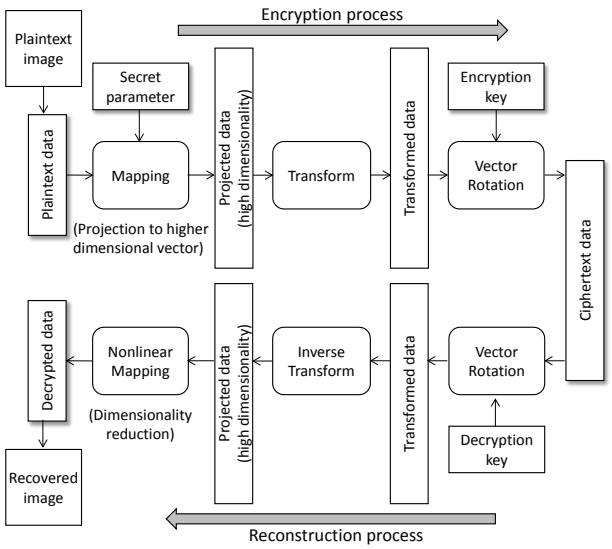


Figure 1 – Algebraic model of DRPE. "Secret parameter" corresponds the random phase pattern at the input plane. "Encryption and decryption keys" are the random phase on the Fourier plane. All process can be described with vector-matrix multiplications except the nonlinear mapping at the final step.

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 system [4]. Because the biometric authentication is based on the unique feature of the individual, the biometric template must be protected against security threats and also must 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 [5,6]. Optical phenomena are essentially linear processes, and the 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, improvements of security 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 fig. 1 [7]. The multiplication of random phase corresponds to the 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 the 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 the application to incoherent imaging systems. If encrypted imaging technology is realized by an imaging system with normal incoherent illumination source, the application field will be extended. Recently the technology of computational imaging is being deployed into practice, and it is expected to apply the technology to "secure imaging".

For practical use of optical encryption, much deeper security analysis is needed. At the same time, we should be aware of the fact that it is absolutely difficult to achieve an equivalent security level as conventional encryption techniques based on cryptographic theory, which employs 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.

Fig. 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 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 the system implementation, firstly we need to have answers to the questions like: what type of attacks 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 the secure optical sensing systems. Then the 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. Then the security profile of the system needs to be evaluated [8]. Case studies as well as practical deployment will promote the technology into extensive research and practical applications.

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 the optical encryption systems.

Concluding Remarks – The current status and challenges of secure optical sensing technology is discussed. DRPE is an example, but it can be a hint for other type 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) context.

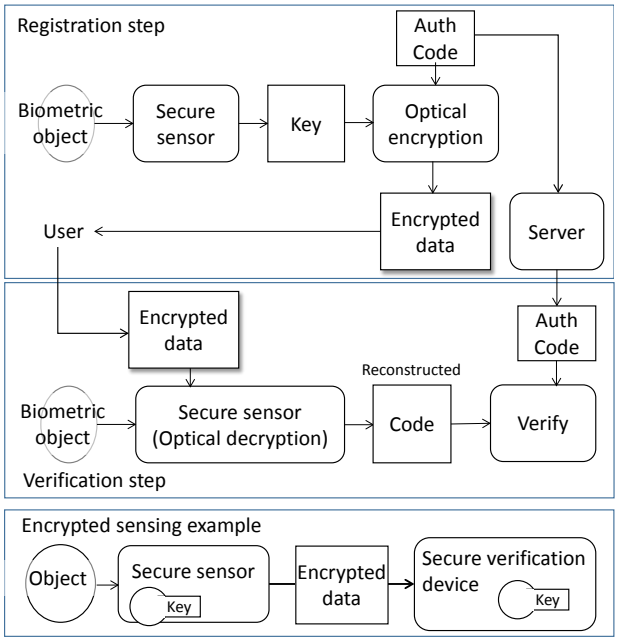


Figure 2 – Secure sensing system examples. Upper and middle: registration and verification steps of the optical cancellable biometrics system. Bottom: an example of encrypted sensing system.

References

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

[2] E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," Appl. Opt. 39, 6595-6601, (2000).

[3] M. Takeda, K. Nakano, H. Suzuki, M. Yamaguchi, "Encrypted Sensing Based on Digital Holography for Fingerprint Images," Optics and Photonics Journal, 5, 6-14 (2015).

[4] H. Suzuki, M. Yamaguchi, M. Yachida, N. Ohyama, H. Haneishi, T. Obi, "Experimental evaluation of fingerprint verification system based on double random phase encoding," Optics Express, 14, 1755-1766 (2006).

[5] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Opt. Express 15, 10253-10265 (2007)
[6] K. Nakano, M. Takeda, H. Suzuki, and M. Yamaguchi, "Security analysis of phase-only DRPE based on known-plaintext attack using multiple known plaintext–ciphertext pairs," Appl. Opt. 53, 6435-6443 (2014)
[7] K. Nakano, M. Takeda, H. Suzuki, M. Yamaguchi, "Encrypted imaging based on algebraic implementation of double random phase encoding," Applied Optics, 53, 2956-2963 (2014).
[8] ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model

Acknowledgments and Funding Information
The author sincerely acknowledge 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.

12. 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 who researched optical computers rushed into the field of optical encryption. To decode the encrypted data, phase information of the mask, complex data, is mandatory. Therefore a holographic technique is required. This makes it somewhat difficult to join the research from other areas of optical information processing. Fortunately, in line with advances in imaging devices such as CCDs, digital holography is accessible to record/detect the complex data. Therefore, digital holography was a powerful tool to realize double random phase encoding optical encryption. This was a trigger for many people to start the 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 the optical encryption using digital holography. The double random phase encoding optical encryption was experimentally demonstrated combining with digital holography [2]. Expanding the encryption into the Fresnel region was also demonstrated with digital holography [3, 4]. Furthermore, a virtual optical encryption system was also accomplished [5]. 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 journal papers on digital holography increased rapidly. The progress of the performance of calculation of a personal computer is considerable. Under the background of digital holography, research on optical encryption progresses.

Current and Future Challenges – The double random phase encoding optical encryption method is widely applied to various fields. Especially some other techniques on imaging are combined with the encryption. 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 [6]. The decrypted image cannot be easily visualized so that an additional layer of information protection is achieved.

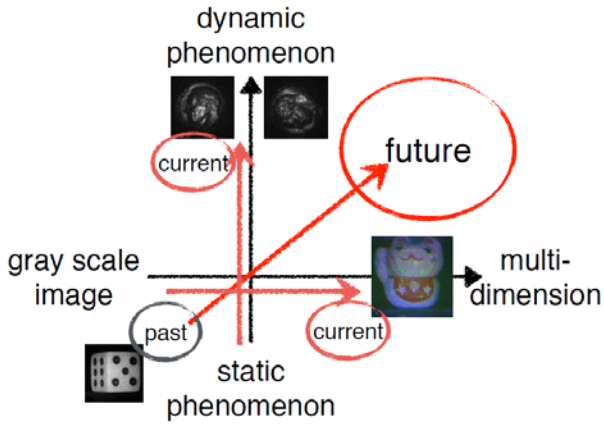


Figure 1 – Progress in digital holography; from a gray scale image to a multi-dimensional image, and from a static phenomenon to a dynamic phenomenon.

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 [7]. It realized encryption and verification of the three-dimensional object at different depths.

Digital holography 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 the 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, the phase-shifted holograms can be obtained by the single recording. Typically, a combination of pixelated polarizing devices are used for the phase-shifting [8]. 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 the alignment of them. 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 [9].

Advances in Science and Technology to Meet Challenges – Figure 1 shows the progress in digital holography. Due to the progress in digital holography, the application fields of optical encryption (double random phase encoding method) will expand much more. However, either dynamic phenomena or multi-dimensional data are realized because the dynamic recording is accomplished with the aid of polarization or spectroscopy. Furthermore, spatial resolution sacrifices for them. This is why available imaging devices detect only intensity information. For the purpose of applying multidimensional 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 2. A smaller size of pixels is preferable to obtain high spatial resolution. The number of pixels is also important. The smaller sized pixels and lots of pixels give the large space-bandwidth product.

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

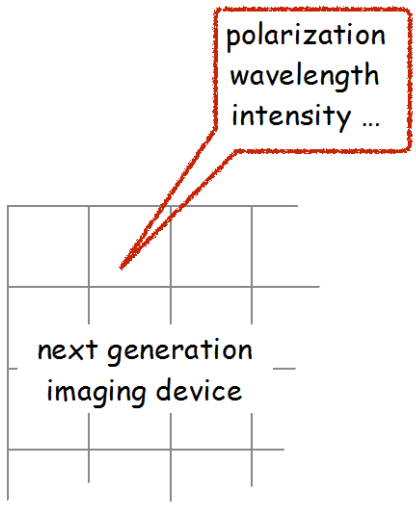


Figure 2 – A next generation imaging device can detect various physical parameters in a single pixel.

References

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

[2] B. Javidi and T. Nomura, "Securing information by use of digital holography," Opt. Lett., vol. 25, pp. 28-30, 2000.

[3] E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry," Appl. Opt., vol. 39, pp. 2313-2320, 2000.

[4] E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," Appl. Opt., vol. 39, pp. 6595-6601, 2000.

[5] T. Nomura, K. Uota, and Y. Morimoto, "Hybrid encryption of a 3-D object using a digital holographic technique," Opt. Eng., vol. 43, pp. 2228-2232, 2004.

[6] E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett., vol.36, pp. 22-25, 2011.

[7] M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," Opt. Lett., vol. 38, pp. 3198-3201, 2013.

[8] Y. Awatsuji, M. Sasada, and T. Kubota, "Parallel quasi-phase-shifting digital holography," Appl. Phys. Lett., vol. 85, pp.1069-1071 (2004).

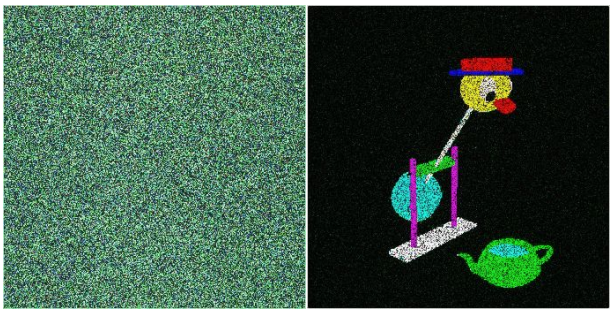
[9] M. Imbe and T. Nomura, "Study of reference waves in single-exposure generalized phase-shifting digital holography," Appl. Opt., vol. 52, pp. 4097-4102 (2013).

13. Optical security: dynamical processes and noise-free recovery – R. Torroba and John Fredy Barrera

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

Status – Aside from the security aspect given by optical methods [1-10], a successful dynamical encoding information exchange highly depends on the 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 [1-4]. In optics, dynamical encoding is a term used to refer to a process where multiple data is 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, besides 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 [1]. 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" seem to be actually the right answer. Instead of the message we perform the encryption over the "container". Quick Response (QR) codes were used as the first instrument in this new strategy [6-9]. QR codes reading is resistant to speckle noise, and are widely decoded by using popular means as smartphones or tablets. Among other breakthroughs in this field, these facts serve as the impetus to the roadmap for quantifying recent progress in this area of research and in the development of new methods.

Current and Future Challenges – The encoding of dynamical processes showed impressive results, although these developments are limited to rather few images. In the example of Figure 1 (Media 1 and 2), we display a color movie of a drinking bird where in



(a) **(b)**

Figure 1. Decryption of a video (a) wrong decoding, (b) right decoding showing a drinking bird (Media 1 and 2 respectively).

(a) we present the outcome of a wrong decryption with no results other than a moving speckle pattern, while in (b) we see the right decoding although polluted with speckle noise [2]. 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 [6, 7], in Figure 2(a), a panel containing several QR codes is displayed after performing the right retrieving protocol [8]. 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 2(b) (Media 3). The new security protocol allows recovering secret messages with no noise, while in classical optical security protocols the retrieved message contains the noise arising from the processing, as in Figure2(c). As QR codes were intended for other purposes than to serve as "containers", they are not prepared to support a large data content compatible with being speckle noise resistant. When a QR code becomes denser as the contained information increases it is affected by the speckles, no longer being noise resistant. Also, they were not designed for images, so movies cannot be stored in QR's. Therefore, the goal is to achieve the design of another type of "container" to meet the required storing capabilities but keeping the same condition referred to noise. Nevertheless, developing an appropriate system is still not easy. Over the past twenty years, optical cryptography has grown, but the field 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.

Advances in Science and Technology to Meet Challenges – Although many advances in the physics of the problem were 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 images overlapping are still a question of discussion, even for the simplest optical system. As it is well known, the 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 combined will influence the movie quality, but so far 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 the 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 to handle at a convenient rate that reflects 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 the 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 laboratory approaches are basically needed as technological launchers that will help in future applications.

Concluding Remarks – The chief progress that is necessary to meet the challenges listed above is the acceptance of dynamical encrypting methods as a common tool by the community. The optical security with quality services (noiseless) is a significant need in 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 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 it as a promising candidate for future public adoption.

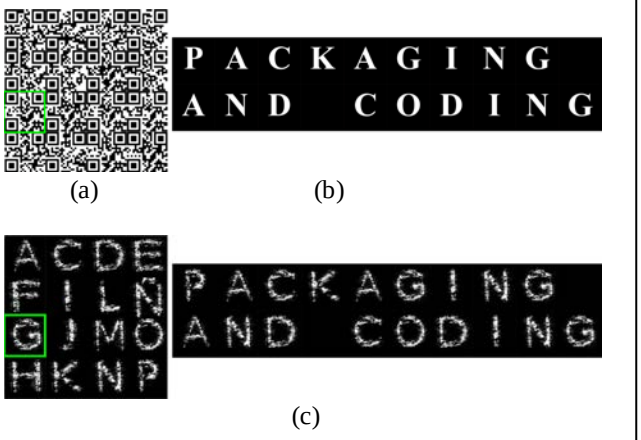


Figure 2. (a) QR panel, (b) recovered message with the proposed protocol (Media 3), and (c) message retrieved with the classical procedure.

References

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

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

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

[4] 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** 223

[5] Chen W, Javidi B and Chen X 2014 Advances in optical security systems *Advances in Optics and Photonics* **6** 120

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

[7] Graydon O 2013 Quick response codes *Nature Photonics* **7** 343

[8] 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

[9] Markman A, Wang J and Javidi B 2015 Three-dimensional integral imaging displays using a quick-response encoded elemental image array *Optica* **1** 332
[10] Liu S, Guo C and Sheridan J T 2014 A review of optical image encryption techniques *Opt. Laser Technol.* **57** 327 (2014).

Acknowledgments and Funding Information

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 the support from The International Centre for Theoretical Physics ICTP Associateship Scheme and The World Academy of Sciences TWAS.

14. 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 [1-2], images or video streams for information technology security, ranging from biometric authentication over digital image forensics to visual passwords [1,3]. 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 [1,3]. Thus, a second physical encryption key allows increasing the security level.

Current and Future Challenges – *Compression and Encryption*: Optical encryption has emerged as a framework for studying information processing [1,4-6]. However, it is well established that the standard double random phase encryption (DRP) exhibits vulnerability to various attacks, as shown in Refs. [4-6], and it requires a large number of bits to encode the output plane. Hence, a compression method is necessary [7-9]. 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 (Fig. 1) [7]. A first approach consists to realize image compression and then its encryption. Overall, this procedure permits to get a good quality of the 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 to first encrypt the image and then apply a compression technique. This scheme allows a significant decrease of information size at the system output but generally does not provide a good quality of the reconstructed image. A third technique consists to realize simultaneously encryption and compression [7,9].

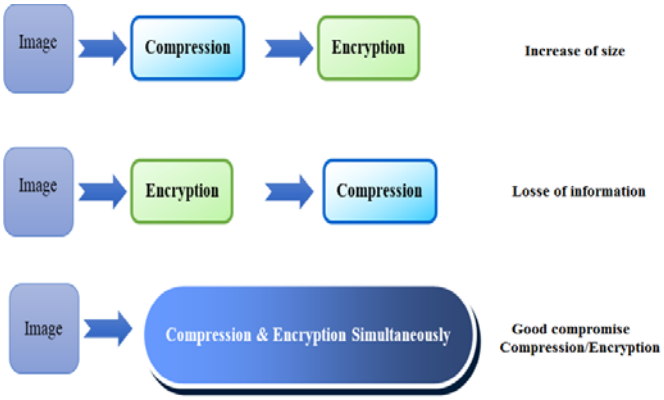


Fig. 1. Three approaches: (1) compression/encryption; (2) encryption/compression or (3) Compromise: Compression & encryption simultaneously.

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 simultaneous image encryption and compression, i.e. method, based on the 4*f* optical setup and a specific fusion without overlapping of the target image spectra [7,9].

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 the useful information required for reconstruction of the target image by holographic techniques [Naughton, Frauel, Javidi, & Tajahuerce, 2002; Darakis, & Soraghan, 2007 ; Paturzo, Memmolo, Miccio, Finizio, Ferraro,Tulino & Javidi, 2008; Tahara, Ito, Kakue, Fujii, Shimozato, Awatsuji, Nishio, Ura, Kubota, & Matoba, 2010; Xia, Shimozato, Tahara, Kakue, Awatsuji, Nishio, Ura, Kubota & Matoba, 2013]. 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 Paturzo, Memmolo, Miccio, Finizio, Ferraro, Tulino & Javidi (2008), which deals with a small part of a specific spectrum and can be used in the optical encryption domain. Recently, Alfalou & Brosseau (2013) presented a method of compression and encryption based on DCT (discrete cosine transform) 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 [Refregier & Javidi, 1995 ; Alfalou & Brosseau, 2009 ; Wang, Guo & Lei, 2013 ; Liu, Xu, Liu, Chen, Li, Lin & Liu, 2011 ; Wang, 2012 ; Liu, Zhang, Li, Liu, Liu, Wang & Liu, 2013 ; Rajput & Nishchal, 2013 ; Paturzo, Memmolo, Miccio, Finizio, Ferraro,Tulino & Javidi, 2008] but they are detrimental to compression. Other encryption techniques such as those based on the fractional Fourier transform (Sahin, Ozaktas, Mendlovic, 1995), DCT and Arnold transform [Liu, Xu, Liu, Chen, Li, Lin & Liu (2011), quantum cryptography [Duraffourg, Merolla, Goedgebuer, Mazurenko & Rhodes, 2001], chaotic cryptography (Guglielmi, Fournier-Prunaret, Taha, Pinel, Rouabhi & Beneteau, 2002) 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 [3]. Additionally, the use of specific treatments of the input and correlation planes permits significant increase in the correlator's performances. 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 the 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 the secure OIP task requires: (i) propose encryption methods which optimize the information size to be encrypted and which are adapted to the transmission channel and /or storage capacity [9] ; (ii) consider correlation as part of a decision making system, e.g. based on fuzzy logic [10] ; (iii) develop 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 the GPU, or the field-programmable gate array (FPGA) 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 a high parallelism and real time processing can be effectively realized. OIP is still in its early days, and there are a number of directions into which the field is likely to move in the coming years. 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.

References

[1] A. Alfalou and C. Brosseau, "Recent advances in optical image processing" Progress in Optics, E. Wolf ed., 60, 1-145 (2015).

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

[3] A. Alfalou, C. Brosseau, and M. S. Alam, "Smart pattern recognition," Proc. SPIE 8748, Optical Pattern Recognition XXIV, 874809 (2013).

[4] Y. Frauel, A. Castro, T. Naughton, et al.,"Resistance of the double random phase encryption against various attacks," Opt. Exp. 15, 10253–10265 (2007).

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

[6] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photon. **6**, 120-155 (2014).

[7] A. Alfalou, A. Mansour, M. Elbouz, and C. Brosseau, "Optical compression scheme to multiplex & simultaneously encode images", in Optical and Digital Image Processing Fundamentals and Applications, G. Cristobal and P. Schelkens eds., Hugo Thienpont

[8] E. Darakis, T. Naughton, T. and J. J. Soraghan, "Compression defects in different reconstruction from

phase-shifting digital holographic data", Appl. Opt. **46**, 4579-4586 (2007).
[9] A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, "Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks," Opt. Express 21, 8025–8043 (2013).
[10] Y. Ouerhani, M. Desthieux, and A. Alfalou, "Road sign recognition using Viapix module and correlation," Proc. SPIE 9477, Optical Pattern Recognition XXVI, 94770H (2015).

Acknowledgments and Funding Information
The Lab-STICC is Unité Mixte de Recherche CNRS 6285. Email: *ayman.al-falou@isen.fr*

15. Optical security and encryption with quantum imaging – Adam Markman and Bahram Javidi

University of Connecticut

Status – Since two approaches were proposed for using optics in security, authentication and encryption [1-2], many variations of these approaches have been reported [3-10]. 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 [3], and complex amplitude [1-4].

Recently, optical security and encryption have been implemented with a few photons to substantially increase resistance against unauthorized attacks [5-8]. The implementation of the photon counting optical keys make 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 [4] although optical implementations are resistant against digital attacks. One popular optical encryption technique is the double-random-phase encryption (DRPE) [2]. 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 [3]. 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, 5, 6].

Recently, optical security and encryption [1-2] have been combined with quantum imaging or photon-counting [5-8], which performs security authentication or encryption of the data with far fewer photons than conventional approaches. For authentication, the decrypted image is reconstructed with few photons. Various optical correlation or image authentication approaches may be used [1, 6] to authenticate the photon counting decrypted image.

Figure 1(a) depicts an encryption or authentication scheme using the double-random-phase encryption (DRPE). Using quantum imaging concepts, the encryption and decryption can be performed optically with a few photons using photon-counting devices. In Fig. 1(b), a computer-generated photon-limited encrypted image is obtained using 30,000 photons or 0.144 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 Fig. 1(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.

In another recent development, nano-encoding techniques have been integrated with optical security systems. A novel authentication scheme was introduced in [9] by embedding nanoparticle structures inside of an 840 x 840 μm^2 quick response (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.

Optical encryption with a few photons creates a very sparse encrypted data which allows us to use storage and communication of data with small bandwidth such as QR codes for optical security. In [7], the data was encrypted using the 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 [B. Javidi, "Nonlinear Joint Power Spectrum Based Optical Correlation," Applied Optics, 1989].

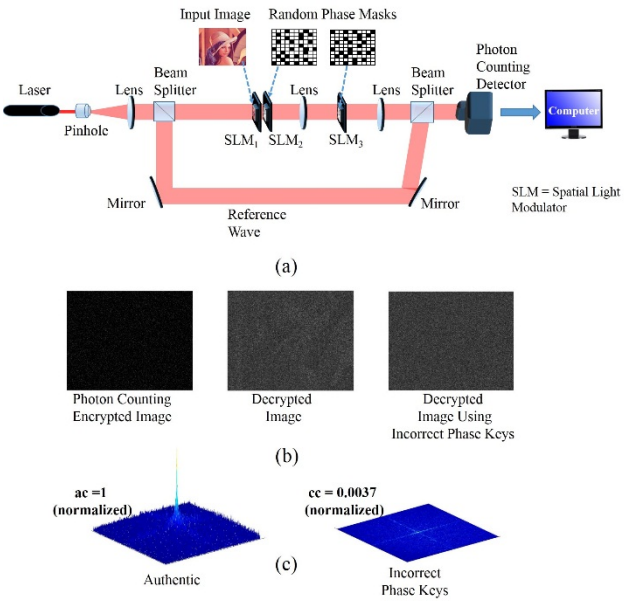


Figure 1. (a) Authentication scheme combining the double-random-phase encryption (DRPE) with photon counting. A photon counting detector is used to record the encrypted image. The decryption is the reverse of the encryption process using conjugate phase masks [1, 5, 6]. (b) The computer-generated photon 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 it performs 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 integrated circuit. All ICs have information written on them similar to a barcode. In [7], 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 three-dimensional (3D) display. In [8], a 3D authentication technique was introduced by combining a 3D imaging technique known as integral imaging with the 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.

Generally speaking, 3D integral imaging requires multiple two-dimensional (2D) perspectives of a scene known as elemental images (EI). Transferring the images from one party to another in a secure method can be difficult. In [10], 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 the DRPE. The encrypted RGB images were then stored in multiple quick-response (QR) codes. Knowing the decryption keys to the 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 [5, 6] 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 photon counting regime. Photon counting may be mathematically modelled using a Poisson distribution under certain assumptions [for example, see G. W. Goodman, Statistical Optics, 1985]. 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 (see [11]). 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 attacks if their encryption keys are not continuously updated. By applying quantum imaging to the system, this security risk can be mitigated. As shown in Fig. 1, when the double-random-phase encryption was 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 nano-particles [9] into an object is also a topic of interest. These nano-particles 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 nano-particles into objects is needed. Nano-particles 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 the 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 quick response (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 (e.g. [12]). 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 and Funding Information
We wish to acknowledge Honeywell for its support.

References

[1] P. Refregier and Bahram Javidi. "Optical image encryption based on input plane and Fourier plane random encoding." *Optics Letters* 20.7 (1995): 767-769.

[2] B. Javidi and J. Horner. "Optical pattern recognition for validation and security verification." *Optical engineering* 33.6 (1994): 1752-1756.

[3] O. Matoba and B. Javidi. "Encrypted optical memory system using three-dimensional keys in the Fresnel domain." *Optics Letters* 24.11 (1999): 762-764.

[4] W. Chen, B. Javidi, and X. Chen. "Advances in optical security systems." *Advances in Optics and Photonics* 6.2 (2014): 120-155.

[5] Pérez-Cabré, Elisabet, Myungjin Cho, and Bahram Javidi. "Information authentication using photon-counting double-random-phase encrypted images."*Optics letters* 36.1 (2011): 22-24.

[6] A. Markman and B. Javidi. "Full-phase photon-counting double-random-phase encryption." *JOSA A* 31.2 (2014): 394-403.

[7] A. Markman, B. Javidi, and M. Tehranipoor. "Photon-counting security tagging and verification using optically encoded QR codes." *Photonics Journal, IEEE* 6.1 (2014): 1-9.

[8] C. Myungjin and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," Optics Letters, 38, 3198-3201 (2013).

[9] A. Carnicer, A. Hassanfiroozi, P. Latorre-Carmona, Y. Huang, and B. Javidi, "Security authentication using phase-encoded nanoparticle structures and polarized light." *Optics letters* 40.2 (2015): 135-138.

[10] A. Markman, J. Wang, and Bahram Javidi. "Three-dimensional integral imaging displays using a quick-response encoded elemental image array." *Optica* 1.5 (2014): 332-335.

[11] Narravula, Hayat, Javidi, "Information theoretic approach for assessing image fidelity in photon-counting arrays," *Optics Express*, 18, 2449 (2010)

[12] O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan, B. Javidi, "Optical Techniques for Information Security," *Proc. IEEE Journal*, 97, 1128-1148 (2009)

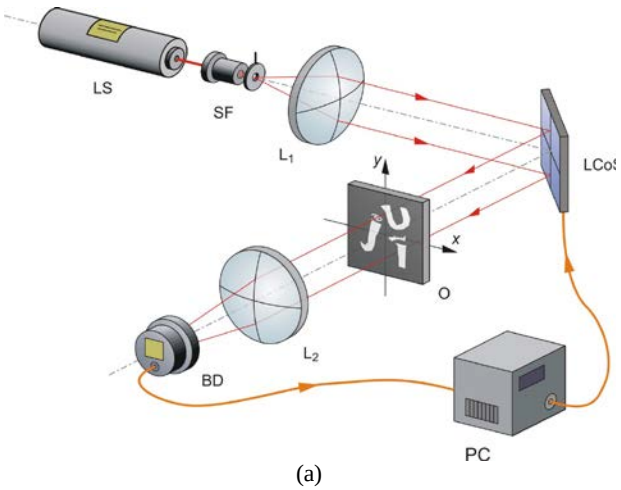
16. Optical encryption by computational ghost imaging - Enrique Tajahuerce and Jesús Lancis

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 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 [2]. In this section we focus on the application of computational ghost imaging (CGI) to encryption.

Computational imaging with single-pixel detectors enables to obtain spatial information of an object by sampling the scene with a set of microstructured light patterns [3]. A simple bucked detector records the signal associated to 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 [4]. The reference one measures the intensity distribution of the light illuminating the object, while the second 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 [5].

Image encryption with CGI is a cryptography technique with a modified symmetric key [6]. The idea is outlined in Figure 1(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, it is possible to recover the image of the object. The bottom pictures in Figure 1 show an example of encryption. Figure 1(b) is the image to be encrypted, (c) the decrypted image, and (c) an attempt of decryption with a wrong key. The outline of the optical encryption methods is depicted in Figure 2. Several encryption techniques based on this idea have recently been reported [7,8].



(a)

(b) (c) (d)

Figure 1 – Optical encryption by using computational ghost imaging.

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 focus 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 [9]. 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. 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 been already proposed both in CGI and optical encryption by CGI [10]. Another approach to

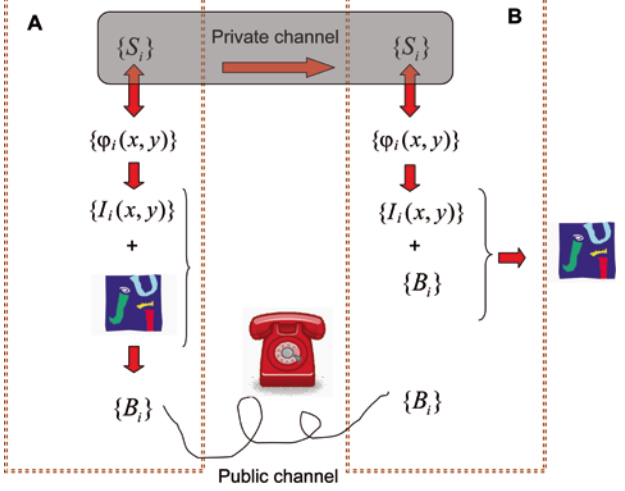


Figure 2 – Outline of the optical encryption system. The transmitter (A) and the receiver (B) share a secret key {Si} generating the phase distributions $\varphi_i(x,y)$ in the SLM (LCoS) in Figure 1. The information is encrypted on a vector containing the intensity values {Bi} detected by the single-pixel detector (BD) in Figure 1.

reduce the acquisition time is by employing faster spatial light modulators 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 developing systems 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 technique, the main advance to increase security in encryption by CGI will arise by developing non symmetric keys. 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 believe also that encryption by CGI will benefit from general advances in quantum imaging [4]. 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, 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 any other single-pixel imaging technique, will benefit from the development of faster spatial light modulators. 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 MEMs based diffractive SLMs, which are able to work at hundreds of kHz but in linear array configurations.

Advances on 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 spatial light modulators even with low light levels. Besides, by using multidimensional detectors, able to measure different optical parameters such as polarization, phase, or spectral content, 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.

References

[1] Ph. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. 20, 767-769 (1995).

[2] Y. Frauel, T.J. Naughton, O. Matoba, E. Tajahuerce, B. Javidi, Three-dimensional imaging and processing using computational holographic imaging, Proc. IEEE 94, 636-653 (2006)

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

[4] A. Gatti, E. Brambilla, and L. A. Lugiato, "Quantum Imaging," Progress in Opt., Vol. 51, pp. 251 (2008).

[5] Y. Bromberg, O. Katz, and Y. Silberberg, “Ghost imaging with a single detector,” Phys. Rev. A, Vol. 79, 053840 (2009).
[6] P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis “Optical encryption based on computational ghost imaging”, Opt. Lett. 35, 2391-2393 (2010)
[7] M. Tanha, R. Kheradmand, and S. Ahmadi-Kandjani, “Gray-scale and color optical encryption based on computational ghost imaging”, App. Phys. Lett. 101, 101108 (2012)
[8] W. Chen and X. Chen, “Ghost imaging for three-dimensional optical security”, App. Phys. Lett. 103, 221106 (2013).
[9] L.J. Kong, Y. Li, S.X. Qian, S.M. Li, C. Tu, and H.T. Wang, “Encryption of ghost imaging”, Phys. Rev. A, 88, 013852 (2013).
[10] S. Zhao, L. Wang, W. Liang, W. Cheng, and L. Gong, “High performance optical encryption based on computational ghost imaging with QR code and compressive sensing technique”, Opt. Comm. 353, 90–95 (2015).

Acknowledgments and Funding Information

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).