Roadmap on Optics and Photonics for Security and Encryption

Bahram Javidi, Artur Carnicer, Kavan Ahmadi, Yasuhiro Awatsuji, Wen Chen, Thierry Fournel, Patrice Genevet, Jingying Guo, Wenqi He, Mathieu Hébert, et al.

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 8 June 2025, accepted 1 August 2025, date of publication 8 August 2025, date of current version 14 August 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3597226

PERSPECTIVE

Roadmap on Optics and Photonics for Security and Encryption

BAHRAM JAVIDI[1], (Fellow, IEEE), ARTUR CARNICER[2], KAVAN AHMADI[2], YASUHIRO AWATSUJI[3], WEN CHEN[4,5], (Senior Member, IEEE), THIERRY FOURNEL[6], PATRICE GENEVET[7], JINGYING GUO[8], WENQI HE[9], MATHIEU HÉBERT[6], ALOKE JANA[7], EDMUND Y. LAM[10], (Fellow, IEEE), GUI-LU LONG[11,12], (Member, IEEE), OSAMU MATOBA[13], (Member, IEEE), ZHAOKE MI[14], INKYU MOON[15], NAVEEN K. NISHCHAL[16], DONG PAN[11], (Member, IEEE), XIANG PENG[9], PEPIJN W. H. PINKSE[17], (Member, IEEE), YISHI SHI[14,18], GUOHAI SITU[8], ADRIAN STERN[19], XIAOGANG WANG[20], TIAN XIA[21], YIN XIAO[4], XIE ZHENWEI[21], AND SHUO ZHU[10]

[1]Electrical and Computer Engineering Department, University of Connecticut, Storrs, CT 06269, USA
[2]Departament de Física Aplicada, Universitat de Barcelona (UB), 08028 Barcelona, Spain
[3]Faculty of Electrical Engineering and Electronics, Kyoto Institute of Technology, Kyoto 606-8585, Japan
[4]Department of Electrical and Electronic Engineering, The Hong Kong Polytechnic University, Hong Kong
[5]Photonics Research Institute, The Hong Kong Polytechnic University, Hong Kong
[6]Laboratoire Hubert Curien, UMR 5516, Univ. Lyon/UJM, CNRS, Institut d'Optique Graduate School, 42023 Saint-Étienne, France
[7]Department of Physics, Colorado School of Mines, Golden, CO 80401, USA
[8]Wang Zhijiang Laser Innovation Center, Shanghai Institute of Optics and Fine Mechanics, Chinese Academy of Sciences, Shanghai 201800, China
[9]College of Physics and Optoelectronic Engineering, Shenzhen University, Shenzhen 518060, China
[10]Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong
[11]Beijing Academy of Quantum Information Sciences, Beijing 100193, China
[12]State Key Laboratory of Low-Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, China
[13]Center of Optical Scattering Image Science, Kobe University, Kobe 657-8501, Japan
[14]Center for Materials Science and Optoelectronics Engineering, University of Chinese Academy of Sciences, Beijing 100049, China
[15]Department of Robotics and Mechatronics Engineering, DGIST, Daegu 42988, South Korea
[16]Department of Physics, Indian Institute of Technology Patna, Patna, Bihar 801106, India
[17]MESA+ Institute, University of Twente, 7500 AE Enschede, The Netherlands
[18]Aerospace Information Research Institute, Chinese Academy of Sciences, Beijing 100094, China
[19]School of ECE, Ben Gurion University of the Negev, Be'er Sheva 8410501, Israel
[20]Department of Applied Physics, Zhejiang University of Science and Technology, Hangzhou 310023, China
[21]Nanophotonics Research Centre, Institute of Microscale Optoelectronics, State Key Laboratory of Radio Frequency Heterogeneous Integration, Shenzhen University, Shenzhen 518060, China

Corresponding authors: Bahram Javidi (bahram.javidi@uconn.edu) and Artur Carnicer (artur.carnicer@ub.edu)

ABSTRACT In 1994, Javidi and Horner published a paper in Optical Engineering that highlighted the ability of free space optical systems to manipulate sensitive data for authentication purposes. The underlying idea was effective yet surprisingly simple: an optical nonlinear joint transform using a random phase mask in both the input and the reference could produce a correlation peak to indicate whether the input object is authentic or not. This seminal paper fueled the development of this new discipline. After three decades, optical encryption and security have matured into a field that plays a central role in the development of photonics techniques. While the pioneering work was mainly focused on the field of optical information processing, nowadays, a broad spectrum of disciplines are contributing to developing security solutions, including nanotechnology, materials science, quantum information, and deep learning, just to cite a few. The present roadmap paper gathers 28 leading authors in the field from 21 academic institutions across nine different countries. It is organized into 17 sections which discuss the present and future challenges, state-of-the-art technology, and real-world solutions to address the security challenges facing our society.

The associate editor coordinating the review of this manuscript and approving it for publication was Derek Abbott.

INDEX TERMS Computational neuromorphic imaging, compressive imaging and deep learning, integrated photonics, metasurfaces, optical security and encryption, physical unclonable functions and random number generators, ptychography, quantum secure direct communication, scattering media and speckle, structured light: polarization and orbital angular momentum.

I. INTRODUCTION

Many of the critical components, functions, tools, and assets in the world that impact our daily activities are information based. Healthcare, manufacturing, transportation, commerce, finance, defense and security, etc. are heavily dependent on reliable transmission, storage, and processing of information. Thus, while securing and authenticating information are critical for proper and reliable functioning of these very important activities, we continue to face great challenges to counter attacks and hacking of databases of banks, energy resources, healthcare, government agencies, public institutions, etc. The attackers have become increasingly sophisticated and effective in overcoming the security barriers to penetrate the databases or gain unauthorized access to critical systems and do damage. It is a reminder that the arms race between hackers and information protectors is on-going and perhaps never ending. The attacks are mainly conducted digitally which makes the case for employing physical phenomenon such as optics and photonics to counter the hacking attempts. Optics and photonics possess many degrees of freedom. The electromagnetic nature of optical waveforms allows access and manipulation of amplitude, phase, polarization, and wavelength which are beneficial for information security. The emerging fields of quantum imaging and meta materials have provided additional areas of research and development in optical security.

In 2024, we celebrated 30 years since the inception of work in Optical Encryption and Security. This is an opportune moment to recognize those who made early contributions to the advancement of this field. In 1994, Javidi and Horner published the paper on optical security and authentication [1]. The paper proposed to use a single input plane random phase encoding of biometrics or other primary objects for security and authentication. That summer in 1994, Javidi was hosted by Refregier in his Lab and they published the follow up paper in 1995 extending the concept to optical encryption by using an additional random phase key in the frequency plane [2]. These publications generated interest in using free space optics for information security and led to various cross disciplinary collaborations and research activities. A joint collaboration with Peyghambarian's group resulted in introducing an all polymeric optical pattern recognition system for security verification [3] followed by introducing an all phase encoded key and biometrics for authentication [4], Fourier plane phase encoding for authentication [5], and a review paper on this subject [6].

In 1997-1999, two promising young scientists from Japan, Matoba and Nomura, and another brilliant scientist from Spain, Tajahuerce, made excellent contributions to novel concepts in optical security. Matoba reported how the optical 2D phase keys can be extended to three dimensional keys in the Fresnel domain [7], or by using multiple wavelengths to increase the complexity of the encryption keys [8], and introducing multidimensional optical keys for security systems [9]. Nomura reported using digital holography in information security [10], polarization encoding for optical security [11], and optical encryption using binary key codes [12]. Tajahuerce demonstrated encrypting three dimensional information with digital holography [13], and optical security and encryption with totally incoherent light [14]. Matoba demonstrated secure real-time displays by optical retrieval of encrypted digital holograms [15], [16]. Watermarking using optical encryption was reported [17], [18] through the work by Kishk, and remote authentication of objects was reported in [19].

The research in optical encryption and security has substantially evolved since these early years. While the research in early years was mainly focused on optical signal processing, the authors in this manuscript illustrate the cross disciplinary nature of the current research in the field. The sections presented in this manuscript illustrate the depth and breadth of a vast array of activities related to optical encryption, security, and authentication. Cross disciplinary nature of current activities spans from deep learning, computational neuromorphic imaging, meta surfaces, nano technologies, structured vector beams, combatting adversarial attacks in deep learning, visual cryptography, ptychography, orbital angular momentum, spirally polarized beams, narrow optical spectral linewidth fingerprints, nanostructured materials, physical unclonable functions, and multidimensional optical encryption on a chip, for high-capacity and ultra-compact encryption systems.

Overview of Contributions: This document presents a comprehensive description of present advancements in optical security and encryption, authored by leading experts in the field. The document comprises 16 sections that cover a diverse range of topics, displaying the potential of these technologies in data protection.

Pan and Long (section II) highlight the progress in quantum-secure protocols for both free space and wired networks. Zhu and Lam (section III) introduce computational neuromorphic imaging as a novel approach to address encryption challenges. Nishchal (section IV) emphasizes the potential of structured vector beams in optical encryption. Xiao and Chen (section V) explore the robustness of converting unidimensional signals into 2D signals for secure free-space optical transmission. Wang (section VI) emphasizes the importance of integrating deep learning methods to strengthen optical crypto systems against sophisticated attacks. He and Peng (section VII) propose a highly secure key storage method using scattering media, ensuring that digital keys cannot be retrieved. Moon's work on double

random phase encoding (section VIII) demonstrates the efficacy of optical systems in achieving perfect forward secrecy for image cryptography. Shi and Mi (section IX) discuss recent advancements in invisible visual cryptography, speckle-based watermarking and ptychography encryption, offering new techniques for encrypting multiple color images. Xia and Xie (section X) expand on the capabilities of Orbital Angular Momentum (OAM) metasurfaces holography, introducing multidimensional optical field steering for enhanced encryption. Ahmadi and Carnicer (section XI) present a method for visual cryptography using highly focused spirally polarized beams and deep learning, ensuring robust decryption through convolutional neural networks. Pinkse (section XII) explores the use of narrow optical spectral linewidth fingerprints in integrated photonics for anti-counterfeiting and remote identification. Jana and Genevet (section XIII) address the challenges of classical optical encryption that can be addressed with disordered metasurfaces in combination with deep learning. Carnicer and Javidi (section XIV) highlight the significance of optical authentication using nanostructured materials and polarized light, to ensure secure and reliable authentication. Fournel and Hébert (section XV) focus on physical authentication using True Repeatable Random Number Generators and Physical Unclonable Functions, emphasizing uniqueness and unpredictability of patterns and fingerprint for secure authentication. Situ (section XVI) introduces the concept of multidimensional optical encryption on a chip, leveraging metasurfaces for high-capacity and ultra-compact encryption systems. Stern and Javidi (section XVII) propose using optical compressive imaging to safeguard deep neural networks against adversarial attacks, presenting a robust defense strategy. Finally, Matoba and Awatsuji (section XVIII) discuss the application of optical encryption techniques to multidimensional physical data, enhancing traditional methods with the physical properties of light for long-term data recordings.

II. QUANTUM SECURE DIRECT COMMUNICATION AND NETWORKING

A. COMMUNICATION TOWARDS POST-QUANTUM SECURITY

As quantum computing advances towards maturity, it poses a formidable threat to the security of traditional encryption systems, necessitating a transition towards new encryption techniques and algorithms that can withstand attacks from quantum computers. This paradigm shift heralds the dawn of the post-quantum era, where two primary strategies can be utilized for achieving secure communication: post-quantum cryptography and quantum communication. Post-quantum cryptography rests upon mathematical problems that are currently deemed intractable for quantum computers, offering the advantages of being lightweight and readily adaptable to various platforms. In contrast, quantum communication leverages the fundamental principles of quantum physics to provide an information-theoretic security that is mathematically provable. Among the various quantum communication protocols, quantum secure direct communication (QSDC), first proposed by Long and Liu in 2000 [20], stands as a paradigmatic example. QSDC directly employs quantum states as the carriers of information to enable secure communication between two distant users [21], [22], [23] with unique features such as detecting eavesdroppers, compatible with existing network infrastructures, simplifying the confidential communication process, and covert transmission. These attributes position QSDC as a promising candidate for securing future communication networks against the looming threat of quantum computing [24]. The secure communication model of QSDC is shown in Figure 1, where the authenticated classical channel is used for necessary eavesdropping detection steps, and any information to be transmitted does not pass through the classical channel.

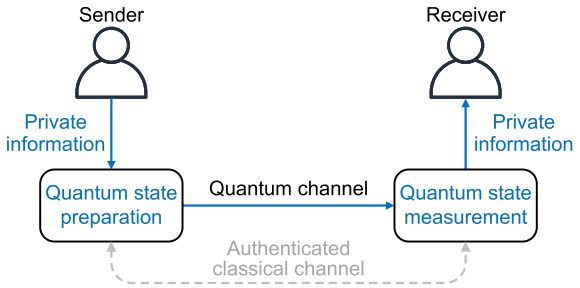


FIGURE 1. The basic model of QSDC.

B. DEVELOPMENT AND APPLICATION

QSDC has evolved through four distinct phases since its inception: the conceptualization phase (2000-2005), the protocol development phase (2006-2015), the principle demonstration phase (2016-2018), and the practical advancement phase (2019 onwards). In the first and second phases, QSDC protocols and QSDC-based cryptographic protocols using various quantum states were constructed. In the third phase, QSDC was experimentally demonstrated, and began to move towards practicality and application in the fourth phase.

To demonstrate the secure and reliable transmission of confidential information using quantum states in noisy and eavesdropping environments, the frequency was used to encode information and verified the feasibility of the DL04 QSDC protocol. Meanwhile, the correlation and non-locality of entanglement were also confirmed for the transmission of confidential information.

When quantum states encoding the information are transmitted in a quantum channel, they are prone to losses and noise, posing challenges to the reliability of information transmission. The forward error correction code in classical communication can address this issue, but it requires extremely low-rate channel coding to recover secret information from a small number of received signals. In 2019, significant milestones were achieved in the areas of quantum channel coding, information-theoretic security performance

evaluation, and designing a stable communication system, culminating in the successful demonstration of 50 bps QSDC over a 1.5 km fiber channel. The current farthest point-to-point communication distance has reached 100 kilometers, marking a milestone that enables practical intercity applications.

Free-space QSDC boasts both flexibility and mobility, capable of transcending the constraints imposed by geographical terrain and communication environments. Among the current viable strategies for achieving global QSDC, satellite-based one-hop relay holds significant promise. The DL04 QSDC protocol has already demonstrated successful free-space communication, and ongoing efforts are refining protocols that are even more suited for satellite-to-ground QSDC. These advancements underscore the potential to harness the unique attributes of free-space QSDC for establishing a global quantum communication network, paving the way for secure, efficient, and ubiquitous quantum communication in the near future [25].

Long-distance quantum-secure communication and large-scale quantum Internets rely ultimately on quantum repeaters, practical quantum repeaters pose a formidable challenge. While quantum key distribution employs trusted repeaters to extend communication distances and user scales, the security of keys remains vulnerable at the relay nodes, necessitating heightened security concerns at these classical intermediary points. In response, the concept of secure repeater [24] has emerged as a solution. Here, the terminal sender encrypts messages using post-quantum cryptography and subsequently employs QSDC for hop-by-hop relay transmission of the ciphertext until it reaches the terminal receiver, who then decrypts it using keys in post-quantum cryptography. This secure repeater paradigm leverages QSDC to ensure reliable and secure information transmission over noisy and potentially eavesdropped channels, while post-quantum cryptography safeguards information at the relay nodes, offering a dual layer of protection that addresses current limitations in quantum communication network security. Furthermore, the integration of entanglement distribution techniques and entangled QSDC protocols enables the establishment of multi-user networks devoid of trusted relay nodes. The demonstrated performance of 1 kbps over 40 km suggests feasibility for metropolitan-scale applications. Figure 2 summarizes the representative QSDC experiments and their achieved communication performance.

The gradual maturation of QSDC has enabled the initiation of applied research endeavors. This communication paradigm can be harnessed for various applications, including the transmission of financial privacy information and reliable monitoring of hazardous materials. Furthermore, integrating QSDC into 5G or 6G networks as a security enabler can ensure the secure transmission of critical information, thereby infusing these networks with a robust security foundation. Furthermore, QSDC can bolster the security of blockchain networks. We propose a QSDC application roadmap that maintains the existing encryption systems at the upper layers

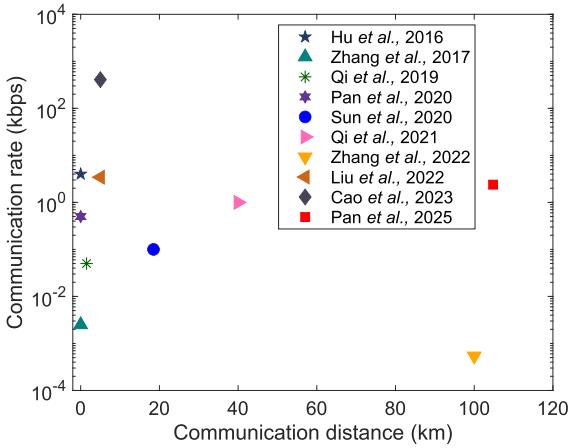


FIGURE 2. The representative QSDC experiments and their achieved communication performance. These representative experiments are summarized in [24], [26]. Note that if the communication distance is not available, we have set the communication distance to 0.

of classical networks while leveraging QSDC as a device for transmitting encrypted messages [25]. This approach undoubtedly provides a dual-layer protection mechanism for information transmission, enhancing the overall security posture of communication systems.

C. FUTURE PROSPECTS

With the proliferation and maturation of quantum technologies, the communication distance and rate of QSDC will be further enhanced, propelling its various deployment applications with greater momentum. In the future, it is imperative to realize the integration of terrestrial and satellite-based quantum networks into a global quantum network, aimed at providing a myriad of QSDC application services [27]. Moreover, the development of quantum network control and management that enable these application services is crucial. Given that QSDC is essentially a secure transmission method, by synergizing the strengths of both classical encryption and QSDC, we can forge a robust secure communication ecosystem that is resilient against emerging threats and adept at catering to the diverse requirements of modern society.

III. SECURITY ENHANCEMENT WITH COMPUTATIONAL NEUROMORPHIC IMAGING

A. STATUS

Information security and encryption have become increasingly vital challenges in both private and commercial information databases in modern society. Optical encryption offers attractive properties with its parallel, high-speed transmission, and low-power consumption encryption features. It is an emerging technique for security and encryption, science the first optical encryption scheme has been proposed and demonstrated via a double random phase encoding model [2]. Optics and photonics processing implementations are cost-efficient yet powerful in information security, image encryption, and data authentication [28]. Numerous impressive implementations of optical encryption systems

showcase the promising properties of utilizing optics and photonics to ensure information security and safety.

However, recent advances in optical encryption methods have primarily focused on the complexity of experimental setups, which rely on advanced optoelectronic devices. A critical issue in most existing optical encryption techniques is that the dimensions (i.e. data format) of the ciphertexts are identical to those of the plaintexts, potentially leading to a cracking process with similar plaintext-ciphertext forms. Consequently, conventional optical systems encode information using light signals, and the plaintext-ciphertext form remains consistent with a frame-based camera, which may increase the risk of the system being cracked. Moreover, traditional intensity images are redundant and temporally sparse. Therefore, adopting a different data dimension between plaintexts and ciphertexts could be a promising approach to address information security concerns.

B. CURRENT AND FUTURE CHALLENGES

Currently, bio-inspired event cameras have been designed to closely resemble the human visual system, making them promising platforms for computational imaging and computer vision applications [29]. Consequently, it is desirable to enhance and transform the encryption strategy and ciphertext storage formats using the bio-inspired sensing framework. Computational imaging is a classical paradigm that combines the optical system and algorithms, which is embedded in optical encryption improvement. Meanwhile, with event cameras on the horizon as the new medium of information sensing, many vision and imaging tasks are carried out with these new bio-inspired sensors. Computational neuromorphic imaging (CNI) is an emerging technique that combines optics, event cameras, and computational models [30].

Event stream data is known for its exceptional capacity to record changeable information asynchronously and has its own data characteristics. Inspired by recent advances in the CNI paradigm and speckle correlography, a neuromorphic encryption technique is proposed to make the images optically encrypted into event-stream ciphertext. As illustrated in Figure. 3, the speckle correlography modulation and events recorded with the neuromorphic devices realize the encryption process. The detailed forward processes are depicted in the blue dashed box. The origin information modulated with an optical modulation process and the generation of corresponding event-stream ciphertext are simultaneously achieved using the neuromorphic encryption system [31]. Meanwhile, the privacy of event-stream data can be enhanced with obfuscation, which further improves the security level and protects the vital information [32].

Despite recent advances with the CNI paradigm, the challenges in implementing CNI techniques for security applications can be briefly summarized as follows: (1) Integrating CNI-informed security solutions into existing optical systems poses technical difficulties. (2) Ensuring the robustness and reliability of CNI-informed security systems

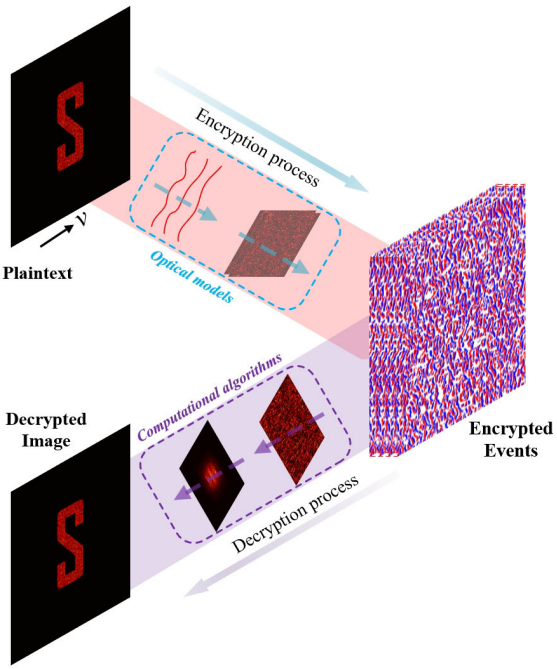


FIGURE 3. Schematic illustration of the neuromorphic encryption and decryption process.

under various environmental conditions and potential attacks is crucial for real-world deployment. (3) The specialized optical components and event generation conditions required for CNI-informed security solutions can be costly, limiting their accessibility. (4) The lack of industry-wide standards and protocols for the integration of CNI-informed security solutions may hinder their widespread adoption and interoperability. To address these challenges, continued research, development, and collaboration between academia, industry, and regulatory bodies will be essential for the widespread implementation of CNI-informed security solutions in the future.

C. ADVANCES IN SCIENCE AND TECHNOLOGY TO MEET CHALLENGES

As with various optical applications, the primary advancement in enhancing information security through the CNI technique will emerge from developing nonsymmetric data formats and specialized keys. By harnessing the advantages of the CNI paradigm, several key advances can be explored to address the challenges associated with security applications. Despite the promising strides made, challenges persist in scaling and integrating neuromorphic encryption into broader applications. We outline two promising aspects to address these challenges and further enhance security with optics and photonics. On the one hand, incorporating optics and photonics systems can enable the miniaturization and cost-efficient integration of CNI-informed security components. Advances in integrated photonics may improve the scalability, reliability, and low redundancy of CNI-informed security solutions Advances in integrated optical schemes

may improve the scalability, reliability, and low redundancy of CNI-informed security solutions [33], e.g., lensless system for further compact solution, metasurface for the enhanced and flexible scheme, and compressed coding for spatiotemporal improvement. On the other hand, combining machine learning can facilitate more efficient plaintext encryption and ciphertext decryption within CNI-informed schemes. Machine learning-powered algorithms can enhance the accuracy, speed, and flexibility of CNI-informed security solutions, potentially addressing the challenges related to scalability and user acceptance. However, learning methods with encryption also have problems to address, e.g., integration challenges, confidentiality risks, and generalization capability. By leveraging these proposed advancements, the research community can work towards overcoming existing challenges and accelerating the adoption of CNI-informed security solutions across various domains.

D. CONCLUDING REMARKS

With the field of event-based techniques rapidly evolving, CNI-enhanced security and encryption will play an increasingly vital role in future applications. As the scientific community anticipates further developments, the CNI-informed method might set a new benchmark in encryption methodologies, emphasizing the transformative power of interdisciplinary research in advancing image security and optical encryption. The neuromorphic design can be readily extended to multimodal information processing, paving the way for optical image encryption and leading to a vast spectrum of applications in security. Discussions and workshops addressing these challenges are expected to shed light on future applications for CNI-informed security and encryption enhancement.

IV. STRUCTURED LIGHT BEAMS FOR INFORMATION SECURITY

In the present digital era, information security is a prime concern in all areas including optical communication. This has led to the development of various cryptosystems employing digital, quantum, and optical protocols. Optical cryptography deals with the manipulation of light's amplitude, phase, spatial frequency, wavelength, polarization, and orbital angular momentum (OAM). The double random phase encoding technique pioneered by Refregier and Javidi paved the way for image/data encryption in optics [2]. Over the years, the method has been extended to different architectures and various optical domain encoding [34]. Phase encoding approaches offer high security but involves complex interferometric set-up for precise wavefront control and measurement. This leads to complexity and quality degradation in practical implementation. In cryptosystems based on polarization distribution, which deals with intensity measurements (Stoke's parameters), similar issue occurs.

To overcome the quality reconstruction issue, of late, structured light beams have been introduced to cryptography [35]. In this case, amplitude, phase, and polarization

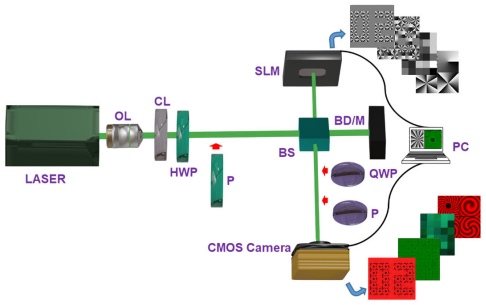


FIGURE 4. Schematic of the experimental set-up. OL: objective lens, CL: collimating lens, HWP: half wave plate, QWP: quarter wave plate, P: polarizer, BS: beam splitter, BD: beam dump, M: mirror, PC: personal computer, CMOS: complementary metal-oxide semiconductor.

of the light beam are engineered in various ways to meet specific requirements. The light shaping techniques offer benefits like robust encoding, greatly enhance the capacity, and show robustness up to the moderate levels of atmospheric turbulence [36]. It has additional flexibility that generation of structured light is possible with a partially coherent source such as light-emitting diode. This not only makes the set-up simple but optimizes cost and removes the inherent speckle problems. Light beams having spiral phase fronts are termed as vortex beams. The phase of such beams contains the term $\exp(il\varphi)$, where l and φ denote topological charge (TC) and azimuthal angle, respectively. Each photon of the beam carries an OAM of amount $l\hbar$. Due to the helical phase front, intensity in the middle of the beam is zero, which is known as a vortex. An encryption system based on an array of vortex beams has been developed where each pixel of the image is first mapped to an integer number and then encoded into the light beam in the form of an array of vortices having TC values identical as the integer numbers [37]. The approach is associated with an interferometric set-up to accurately identify the TC values for successful decryption. To avoid the involved complexity, binary image encryption scheme has been reported, where the presence of a vortex indicates a low-value pixel and absence of a vortex represents a high-value pixel [36]. The developed architecture allows image authentication also using an array of vortices with exclusive-OR operation.

Figure 4 shows the schematic diagram of a generic experimental set-up for the encryption-decryption scheme using different structured light beams. Here, the phase of a light beam is modulated using a phase-only spatial light modulator (SLM) to generate a scalar light beam. For the generation of a vector light beam, additional equipment like a polarizer and wave plates are used appropriately. A light beam having different polarization distributions at different points in the transverse plane is called a vector beam. In a vector beam-based encryption technique, first, an image is converted to a phase-only value using a phase retrieval algorithm and then a random phase function is combined to encrypt the data/image. Finally, the encrypted data is encoded into the form of vector light beams exploiting the property of

polarization. Further enhancement of the security has been achieved by extending the idea into an optical asymmetric approach [38]. To overcome the multiple intensity recordings, a single-shot intensity recording-based image encryption has been reported, where the image is converted into binary data and then encoded into the light beam using binary polarization states. Here, randomly selected regions of the transverse plane are encoded using polarization switch states to enhance the security. In polarization switch encoding, some regions of the transverse plane are encoded with the logic that high-intensity states present '1' and low-intensity states represent '0', and the rest of the regions are encoded following the reverse logic. Recently, a scheme has been developed demonstrating multiple images encoding onto two spatially separated polarization components of light [39]. Here, the information is encoded into an array of C-point polarization singularity, generated through the superposition of optical vortices having different magnitude, each modulated into orthogonal components. The manipulation within two orthogonal polarization components is demonstrated through non-interferometric method which simplifies vector beam generation.

The inherent properties of structured light beams like self-healing and orthogonality increase the quality and capacity of data, still there are several challenges like the efficient generation of high quality structured light beams with simple and economical set-up and efficient detection of such beams. For example, spiral phase plate can generate structured light beams with high conversion efficiency but has limitation with the efficient manufacturing technique. Similarly, the switch speed of liquid crystal SLM often limits its use in real-time applications, though advancements are anticipated as the technology matures. Recently, nanofabrication technology has enabled the generation of these beams using ultrathin optical devices like metasurfaces. Thus, further research can be focused towards the development of good quality devices for the efficient generation and detection of structured light beams. This will enable development of practical optical cryptosystems.

V. PHYSICALLY-SECURED FREE-SPACE OPTICAL DATA TRANSMISSION THROUGH SCATTERING MEDIA

Free-space optical communication has gained considerable attention due to its characteristics, e.g., efficient power usage, high capacity and resistance to electromagnetic interference etc. However, challenges are associated with optically transmitting data in free space. One major issue is the complexity of achieving high-fidelity data transmission, when light waves pass through scattering media. In addition, noise in the channel degrades quality of the received signals, as another challenge to overcome. Recent research advance [40], [41], [42], [43] has demonstrated that converting a signal into 2D amplitude-only patterns can enable high-fidelity transmission through scattering media. The process is shown in Fig. 5, and the methods are developed to realize the transformation, e.g., zero-frequency replacement. The generated amplitude-only patterns act as information carriers in free space, and are sequentially embedded into a SLM. However, refresh rate of the SLM imposes a limitation on the speed of data transmission. To address this limit, it is possible to design and adopt micro-electromechanical systems and phased array photonic integrated circuits.

In the context of the developed free-space optical communication with single-pixel detection, it is well recognized that it is crucial to address the issue of data security. Traditional security strategies are usually designed and applied before optical transmission, and these methods are not ideal for inherently insecure optical channels. Physical layer security emerges as a promising alternative, offering unbreakable and quantifiable secrecy. It has been illustrated that scaling factors in optical channels can be used as physical keys [44], [45]. The scaling factors can be flexibly controlled by using optical devices at the transmitter, e.g., variable beam attenuator (VBA) and SLM. The VBA adjusts intensity of light waves, and SLM can display various modulation patterns, creating dynamic conditions for data transmission. In addition, other strategies are also developed for flexibly controlling scaling factors [46], [47]. The physically-secured data remain robust even in complex environments in the developed free-space optical communication systems.

Optical waves that propagate through scattering media are detected, as ciphertext. Without security keys (i.e., scaling factors), it is impossible to recover original signal from the detected light intensities. When correct scaling factors are applied, the transmitted signal can be decoded. Although a scattering environment is considered, the usage of physically and dynamically-generated scaling factors as keys still enables a realization of physically-secured and high-fidelity free-space optical data transmission.

In the future, integrating nano/micro-electromechanical systems or phased array photonic integrated circuits into free-space optical communication can be considered as an opportunity. Nano/micro-electromechanical systems or phased array photonic integrated circuits have additional advantages, e.g., high refresh rates, increased efficiency and the ability to manipulate light in a novel way. These characteristics make them a promising component for free-space optical communication. It is possible to optimize the transmission in order to develop compact and robust free-space optical communication. An avenue could be opened for next-generation secure and high-fidelity free-space optical communication.

VI. SPECKLE-BASED OPTICAL ENCRYPTION WITH DEEP LEARNING

A. STATUS

With the rapid progress of network technology and the extensive information exchange, the demand for hardware solutions that can offer superior protection for sensitive data exhibits a consistent upward trend. Despite the prevalent utilization of software-based encryption systems to enhance data security, their efficacy might be constrained by factors

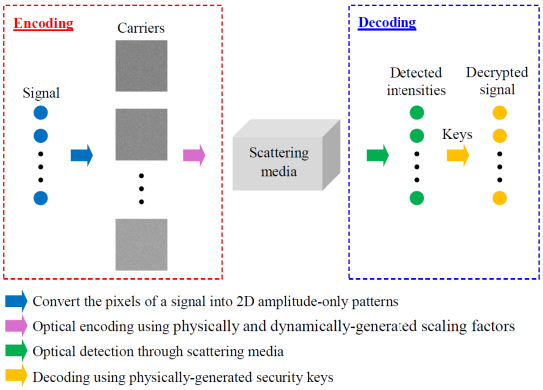


FIGURE 5. A schematic for physically secured optical data transmission through scattering media in free space using single pixel detection.

such as key length and computing power. In this context, the advent of the double random phase encoding technique based on the optical 4-f system holds great significance, indicating that the degrees of freedom including amplitude, phase, polarization, and so on, could potentially be utilized for optical information security processing.

In recent years, deep learning (DL) techniques, which have offered top-quality solutions in various computational imaging domains over the past few years, have also been utilized in the field of optical encryption. Figure 6 depicts a flowchart of the decryption process of a holographic and speckle encryption method based on DL [48]. The synthetic computer-generated hologram (CGH), created by combining two CGHs, one termed "secret CGH" and the other referred to as "cover CGH", is multiplied by the decryption key to produce a speckle pattern, which is then inputted to the pre-trained deep neural network to output the secret image. When the synthetic CGH is illuminated by a laser without decryption, the cover image is displayed to confuse the attacker and offer a means for matching the synthetic CGH and the decryption key pair.

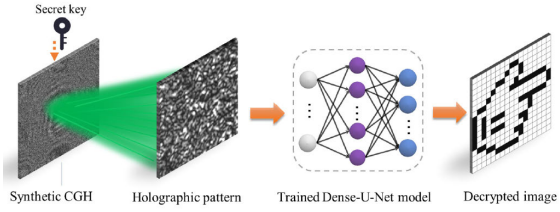


FIGURE 6. Schematic of speckle pattern decryption using deep learning.

Optical security and encryption have also been put forward via the combination of DL with random binary masks made of polyethylene terephthalate [49], single-pixel imaging [50], Digital Micromirror Device (DMD) based complex amplitude coding [51], two-channel detection [52], and binary hologram [53], allowing for more efficient security encryption of the data in comparison with conventional approaches. The experimental results demonstrate that the networks employed in those speckle-based optical encryption schemes can be successfully applied as optically encoded image processors.

B. CURRENT AND FUTURE CHALLENGES

On the one hand, traditional optical encryption techniques inherit the benefits of optical information processing; on the other hand, these techniques themselves also possess some inevitable issues. For instance, the systems have extremely high alignment requirements for the optical path; the decryption process is vulnerable to additional noise during transmission; in a relatively complex setting, information is readily lost during transmission, greatly impacting the decryption effect, and so forth. Hence, addressing these issues is one of the crucial points in the research of optical security. DL is one of the solutions; however, currently, the majority of encryption methods dependent on DL still require extensive training datasets and considerable training time.

Additionally, the attacks confronted by optical security systems are increasingly diversifying and becoming more sophisticated. In recent years, DL has been employed to carry out attack tests on numerous traditional optical security systems and has achieved success in breaking them. Although these tests currently mostly adopt an "end-to-end" approach driven by large quantities of training data, with the rapid development of DL technology, it is foreseeable that optical information security will face an increasing number of challenges. Nevertheless, different attack approaches not only evaluate the security of encryption systems but also offer fresh viewpoints for creating novel optical image encryption systems. It would be extremely beneficial to develop more practical and secure optical image encryption schemes that can resist DL-based attacks [48]. However, when neural network models pre-trained by a series of known plaintext-ciphertext pairs is utilized for decryption, all the physical secret keys become useless for most of reported optical encryption systems, and the security of those systems consequently relies too heavily on the network models.

C. ADVANCES IN SCIENCE AND TECHNOLOGY TO MEET CHALLENGES

Constructing new encryption frameworks and deeply integrating deep learning with computational imaging techniques can circumvent the abovementioned situations [54], offering additional levels of security to DL-assisted optical cryptosystems. Figure 7 depicts the flowchart that demonstrates a new computational imaging encryption incorporating a DL-assisted steganographic and holographic authentication approach. The refinement process is crucial for optimizing the physics-driven network model, enabling it to achieve a balance between successful non-secret image reconstruction and protecting the confidentiality of the hidden image. This method encrypts and authenticates images effectively by combining direct and indirect imaging methods. Direct imaging techniques permit rapid acquisition of image information, while indirect imaging techniques reconstruct images via

computational algorithms. In terms of security, this method has multiple features. Concerning eavesdropping attacks, the system utilizes encrypted transmission of CGH; even if attackers intercept the majority of holographic data, they are unable to obtain the complete keys or the original image. Regarding tampering attacks, the system is highly sensitive to binarization thresholds; for example, a mere change of 0.002 in threshold values can lead to a substantial decrease in decryption quality, and any tampering with key parameters will result in decryption failure. When it comes to data interception or loss attacks, the system can recover valid information despite partial ciphertext loss, retaining the integrity and recognizability of decrypted images.

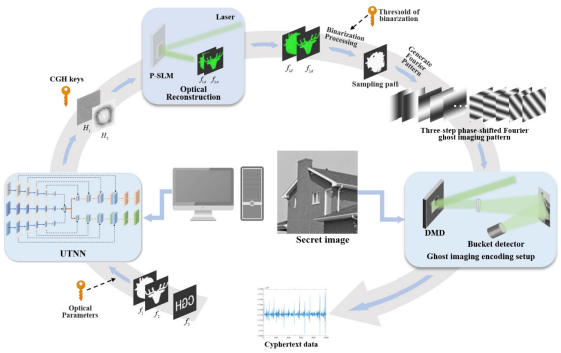


FIGURE 7. Computational imaging encryption with a DL-assisted steganographic and holographic authentication strategy.

D. CONCLUDING REMARKS

The domain of optical image encryption has progressively ascended along the ''S-curve'' in tandem with innovative concepts, counter-suggestions, cryptanalysis, and improvements. These recently undertaken studies have demonstrated that DL possesses tremendous potential in enhancing the security and efficiency of optical encryption systems. It is expected that discussions regarding challenges may provide some valuable insights for future research endeavors on speckle-based encryption with deep learning.

VII. A HIGHLY SECURE KEY STORAGE METHOD BY USING OF SCATTERING MEDIA

A. INTRODUCTION

As B. Schneier famously said, ''the essence of cryptography is turning a long password into a short secret key,'' emphasizing the importance of managing and securely storing these keys [55]. Traditional digital keys, typically stored in the memory of a computer, are vulnerable to attacks, as malicious actors can easily steal or copy them. The most dangerous thing is that the victims are often unaware that their keys have been compromised. In 2002, Pappu et al. introduced the concept of the Physical Unclonable Function (PUF), which leverages the random distribution of microparticles in scattering media to serve as high-security, unclonable physical tokens [56]. However, while effective for identity authentication, this approach has limitations in protecting those already-existing digital keys from being copied. To securely storing these keys, the primary motivation of our recent work [57] is to establish a one-to-one mapping between traditional digital keys and physically unclonable scattering media, creating an Unclonable Equivalent Key (UEK).

B. METHODOLOGY

The proposed method builds upon the modified focusing-oriented Wavefront Shaping (WS) technique to securely store digital keys. In this scheme, any digital key is first encoded into a binary multi-point pattern, which is then linked to scattering media through WS algorithm. By modulating the Input Wavefront Distribution (IWD) using SLM, a mapping relationship between the digital key and the scattering media is established. The scattering media, composed of microparticles that form a unique, unclonable structure, serves as a UEK, while the IWD can either be kept private or public. An attacker, even with knowledge of the IWD, would be unable to reconstruct the key. This is due to the lack of a proper mathematical model to describe the complex physical processes involved when light passes through scattering media, particularly when the input and output fields exceed the optical memory effect's range.

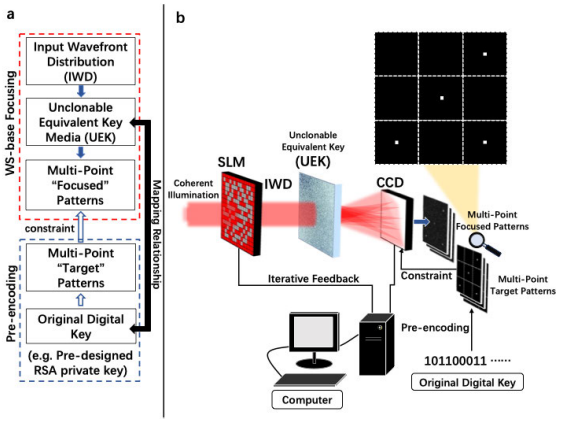


FIGURE 8. Illustration of the methodology: (a) pre-encoding and WS-based Focusing, (b) a potential optoelectronic setup.

C. EXPERIMENTS

A 450 nm laser source was used, with the beam passing through a multi-layer scattering medium (A focused light beam sheds onto two-layer ground glasses with 220-grit for each and is collected by a 20× objective lens). The modulated laser beam generates specific output patterns that correspond to the stored digital keys. The experimental results confirmed that through the WS technique, the digital key could be successfully mapped into an output light field based on the scattering media, achieving a high signal-to-background ratio (SBR).

D. CHALLENGES

To apply the laboratory-based scheme to any practical application, we must face the issue of large-scale fabrication.

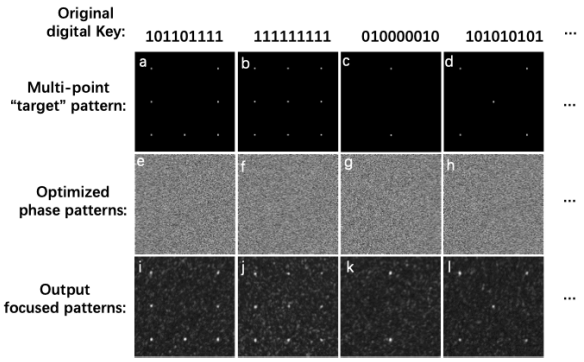


FIGURE 9. Key extraction experimental results on the condition of two-layer ground glasses: (a-d) multi-point "target" patterns related to the original digital key. (e-h) the optimized phase patterns, say IWD, obtained by the modified WS-based focusing process. (i-l) the corresponding output-focused patterns.

It's relatively lucky that all that is required is an extremely low-cost scattering medium (e.g., ground glass) and an iterative algorithm. Though the process is not easy due to the nature of hybrid opto-electronic modulating, the cost can be low. Furthermore, in the area of encryption, how to balance the sensitivity (security-level) and the robustness (easy-to-use) always matters a lot. It can be imagined that even a tiny misalignment of any an involved component here will have a heavy influence on the key extraction. To address this, we can further introduce an alignment mechanism, e.g. a 3-axis stage and alignment marks on the medium. This approach, along with a reference-based usage protocol, will simplify the alignment process and enhance the system's practicality. Noted that the protocol mainly involves selecting a specific reference region within the encoded pattern to guide the alignment.

E. CONCLUSION

Unlike traditional optical encryption methods that use scattering media to disrupt the input light beam and obscure the information, the proposed method leverages the unique, unclonable properties of the scattering medium itself for key storage and extraction. With the aid of alignment mechanisms and usage protocols, our approach resists reverse-engineering attacks and ensures secure key storage and retrieval, even with minor occlusions or misalignments. Notably, the proposed concept of UEK could, in principle, replace any digital easy-to-cloneable bit string (e.g., an already existing private key) in an unclonable manner, and it's totally different than the traditional optical scattering PUF, which only serves as an authentication identity token.

VIII. ROBUST AND PRACTICAL IMAGE CRYPTOGRAPHY VIA DOUBLE RANDOM PHASE ENCODING

Optical image encryption techniques based on Fourier optics has been studied extensively since the double random phase encoding (DRPE) scheme was first proposed in [2]. The DRPE technique encrypts images by phase-encoding using the random phase-only mask in both the input and Fourier planes in 4f optical system. In the field of the image security, since DRPE, optical cryptosystems are attracting more attention due to their inherent high-speed parallel processing and large key space [58]. Thereafter, various optical encryption schemes and applications has been proposed, which are based on the fractional Fourier transform, Fresnel transform, gyrator transform, phase-truncated Fourier transforms, digital holography, and so on [7], [58], [59]. In DRPE, optical images can be represented in the form of complex sinusoidal waveforms, which implies that values on pixels of the image can be parallelized on a page basis rather than on a pixel basis. In contrast, the conventional digital block cipher algorithms such as AES and RSA [60] is designed to be optimized only for text-based datasets, structured datasets or bit stream. Many fields including public health care and biomedicine, deal with a patient's private information such as biomedical images. Huge amounts of private images should be securely and quickly protected as personal information. Therefore, it is necessary to develop a practical security system that can store and reconstruct such information safely and rapidly. Recent studies showed that the DRPE-based optical cryptosystems can efficiently encrypt and multiplex multiple holograms employing the phase-encoding multiplexing method [61]. In the schemes, multiple holograms are separately encrypted by applying the DRPE technique and then they are phase encoded and superimposed with sets of binary phase masks, which are generated from Hadamard matrices (see Fig. 10). The Hadamard matrix is used because it has binary elements and therefore allows us to change the phase of the hologram in a simpler way. Consequently, this approach allows that many groups of holograms or vast amounts of private images can be encrypted and decrypted by using a many of different sets of binary phase masks.

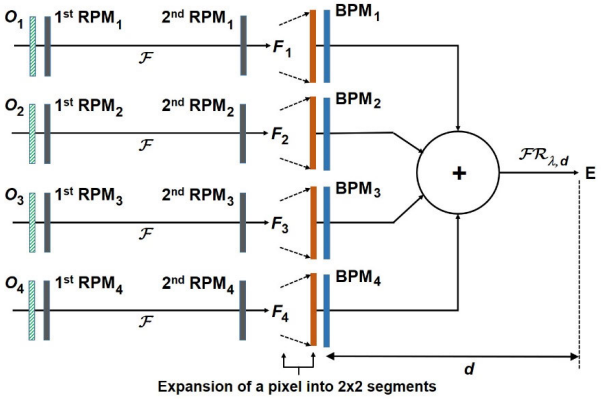


FIGURE 10. Schematic setup for multiple-hologram or multiple-image encryption process [61].

The current digital cryptosystems with the key exchange protocol based on the Diffie-Hellman (DH) scheme can guarantee perfect forward secrecy (PFS). The PFS is an encryption scheme which can provide temporary session key exchanges between client and server. Whenever every new session is initiated by a user, PFS allows to provide a unique

session key between client and server for data encryption that is only used during the session. Therefore, even though one of the session keys is leaked, the secret key information for encryption within any other session can be preserved from any future attacks. However, the key exchange algorithm is designed optimally only for encoding small datasets, such as text and speech sets, and cannot quickly process large datasets such as optical images. Recently, the DRPE-based studies showed that optical cryptosystems can also ensure the PFS using complex sinusoidal waveform versions of the DH key exchange algorithm for robust image cryptography [62]. To establish PFS in the image encryption-decryption schemes based on DRPE, they introduced the optical version of the DH schemes to use transitory secret exponents between two parties. These secret exponents are permanently eliminated as soon as the generated session key is completed. This means during the encryption new session keys are constantly generated by the optical DH schemes with new secret exponents for each connection between two parties. Therefore, the exposure of a single session key will not affect the encrypted images with another one. This is due to that the generated session key with the latest secret exponent are never stored and reused, which allows to implement forward secrecy to its full benefits and makes it more difficult for an attacker to find the session key or the secret exponents of the two users by manipulating their complex sinusoidal waveforms due to the factoring problem and the phase periodicity (phase modulus 2π). Furthermore, the concepts suggest an efficient image encryption-decryption scheme under the objective of significantly improving the security of the DRPE-based cryptosystems.

In the near future, it is required to develop the DRPE-based cryptosystems to efficiently, rapidly store, retrieve, and manage huge amounts of 3D images such as hologram using much larger order Hadamard matrices. The optical cryptosystems must consider perfect forward secrecy. The key to implementing Perfect Forward Secrecy (PFS) in the optical domain lies in leveraging the physical properties of light—such as phase, polarization, and interference patterns—to perform the mathematical operations equivalent to those used in traditional cryptographic protocols. We anticipate that implementing PFS in optical systems—via an optical adaptation of the Diffie-Hellman key exchange—will become a next frontier in optical cryptography, with the potential to redefine secure high-speed optical communications. In addition, it is needed to practically and securely search for, remove, and add desired encrypted images on a cloud system or database. Future DRPE-based security systems must meet critical requirements for image storage, secure access control, retrieval mechanisms, integrity verification, and resistance to adversarial attacks.

IX. INVISIBLE VISUAL CRYPTOGRAPHY AND PTYCHOGRAPHY ENCRYPTION

In the field of information security, digital encryption methods have been widely adopted. However, with the continuous advancement and enhancement of computer technology, digital encryption faces significant challenges. Single digital encryption techniques are no longer sufficient to meet the demands for information security. As a branch of information security research, non-traditional cryptography based on optical principles and technologies has played a crucial role and has become one of the current research hotspots. It is well known that light possesses various properties such as wavelength, amplitude, phase, and polarization. These attributes make light a multi-dimensional information carrier, providing multiple options for encryption degrees of freedom and offering high levels of confidentiality in optical encryption systems. Figure 11 illustrates three types of optical encryption schemes: invisible visual encoding, speckle hiding, and ptychography encryption encoding.

A. INVISIBLE VISUAL CRYPTOGRAPHY CODING

In 1994, Moni Naor and Adi Shamir first proposed the visual cryptography scheme. This scheme encodes a secret image into two visual keys. By overlaying the two visual keys, the secret information can be recovered. In 2017, we introduced the integration of visual cryptography into optical image encryption, combining visual cryptography with optical methods, and proposed the concept of invisible visual cryptography [63]. In this scheme, a phase recovery algorithm is used to convert the visual cryptography-encoded keys into invisible phase information, resulting in pure-phase diffractive optical elements (DOE). During decryption, light waves are used to illuminate the two DOEs to obtain the visual keys, which are then combined to reveal the secret information. Compared to traditional visual cryptography schemes, this approach offers enhanced visual key concealment and represents a close integration of digital cryptography and optical encryption. We have also explored using holographic optical elements and metasurface holograms as carriers for phase keys. Holographic optical elements are phase keys manufactured through holographic exposure of photopolymers. Metasurface holograms utilize artificial atomic monolayers to encode phase key information. Both of these schemes use laser beams to separately illuminate the two phases key carriers to obtain the visual keys, which are then combined to retrieve the secret information.

In traditional visual cryptography schemes, the visual keys are generally meaningless shared images. Building on the concept of invisible visual cryptography, we have proposed an enhanced optical hiding scheme for visual cryptography [64]. This scheme allows for the decomposition of a secret image into multiple meaningful images, which are then hidden within diffractive optical elements. For hiding color images, we divide the color image into red, green, and blue channels. Each channel is decomposed into multiple meaningful shared images, which are then concealed within phase keys. In traditional visual cryptography schemes, if an attacker tampers with the secret information, it is challenging to determine whether the

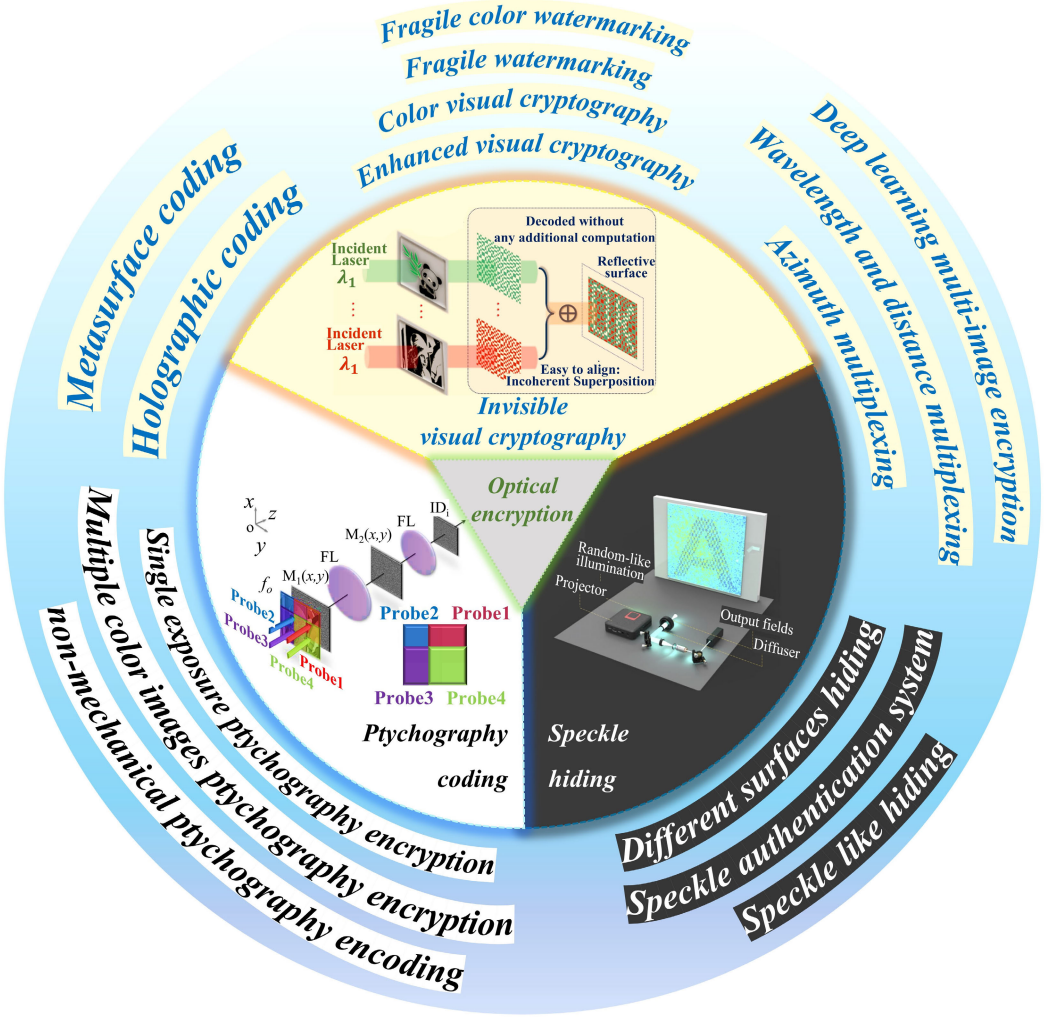


FIGURE 11. Invisible visual encoding, speckle hiding, and ptychography encryption encoding.

extracted secret information remains secure. To address this issue, we proposed optical fragile watermarking schemes based on visual cryptography combined with QR codes, as well as optical color fragile watermarking based on pixel non-expansion visual cryptography. A series of simulation attack experiments has demonstrated that these schemes exhibit good fragility. They can sensitively detect image tampering under various types of attacks.

The information capacity of optical encryption has always been a key focus for researchers. Our research group has made significant efforts to enhance the capacity for encrypting multiple images securely. We have employed various multiplexing schemes to achieve this. We were the first to introduce azimuthal multiplexing into optical hiding [65]. In this approach, visual keys are concealed within cascaded phase plates with different azimuthal states. During extraction, different information segments can be retrieved by rotating the pure phase plates to specific azimuthal angles. Additionally, we implemented both diffraction distance and wavelength multiplexing, hiding the visual keys of secret images within two phase keys. This approach also enables the encryption of multiple images. However, due to the diversity and irrelevance of multi-image hidden information, it is challenging to ensure both the quality and quantity of the extracted secret images simultaneously. To address this issue, we proposed a phase linkage system based on a physics-driven neural network (Multi-dimension Information Integration using Highway network, MIHNet) to improve optical multi-image hiding methods. MIHNet is a physics-driven deep neural network designed to generate phase keys. The generated phase keys can independently reproduce high-quality hidden images in the Fresnel domain.

B. SPECKLE HIDING

Traditional visual keys are often specially designed pixel blocks, which can easily alert attackers. In 2020, we proposed an optical watermarking scheme that uses natural speckle patterns instead of visual keys [66]. Natural speckle, as a naturally occurring physical key, has significant randomness,

making it less likely to attract the attention of attackers. Using natural speckle as a substitute for visual keys enhances security. In the encryption process, secret information is embedded into natural speckle patterns. A grayscale rearrangement algorithm is then used to generate a quasi-random watermark. During decryption, the watermark is projected onto the natural speckle pattern as illumination. These are combined incoherently to extract the secret information directly through visual perception. We subsequently optimized the algorithm for embedding secret information into natural speckle, allowing a greater variety of speckle-like patterns to serve as carriers for the keys [67]. This optimization also improves the clarity of the decrypted secret information. Building on speckle visual cryptography, we were the first to combine speckle visual cryptography with QR codes to design an authentication system for user identification. In this system, QR code images containing user authentication information are hidden within speckle images using the speckle visual cryptography method, and the speckle images are then printed on physical documents.

C. PTYCHOGRAPHY ENCRYPTION CODING

The introduction of double-random phase encoding in 1995 marked the beginning of optical encryption research. This technique employs a 4F system with two random phase plates placed on the input and spectral planes to encrypt an image, resulting in ciphertext that resembles white noise on the output plane. In 2013, building on double-random phase encoding, our research group was the first to apply ptychography imaging schemes to optical encryption [68]. In this method, a probe scans the image to be encrypted, ultimately producing multiple ciphertexts. Due to the characteristics of ptychography imaging, this scheme can encrypt complex amplitude images, significantly enhancing the security of the encryption system. Subsequently, we explored using single-exposure ptychography imaging systems to encrypt multiple images, with security primarily ensured by imperceptibility and extensive scrambling algorithms. To further improve the security of multi-image encryption, in 2021, we proposed a ptychography encoding method for encrypting multiple images and color images [69]. This method inserts phase keys into the planes of multiple encrypted images and uses multilayered encoding and double-random phase encoding to convert images into ciphertext. Additionally, we utilized non-mechanical ptychography imaging to hide optical information. The core of this method includes non-mechanical ptychography encoding (NPE) based on spatial light modulators and a decoding algorithm based on pure phase rapid response codes (PQR). NPE completely eliminates errors introduced by diffraction image scanning, while the PQR constrained decoding algorithm can extract high-quality information from a small number of embedded diffraction images.

D. OUTLOOK

In the information age, the demand for optical encryption is growing, leading to increasing attention towards optical encryption. The future development of optical encryption will undoubtedly be multidimensional. Although our current focus is mainly on the amplitude and phase information of encryption systems, there are other important informational dimensions in optics, such as polarization, frequency, pulse width, and mode field. The next step will be to explore how to integrate these additional dimensions with optical encryption schemes to achieve more diverse and multidimensional information hiding. For instance, information carriers vary at different wavelengths. Ultraviolet or infrared light can be used to achieve further invisible encryption technologies. Additionally, current mainstream visual encryption schemes mainly target two-dimensional images. However, light field control technology allows us to precisely manipulate light fields in three-dimensional space. Therefore, future research will also include an in-depth exploration of visual encryption schemes, aiming to design new three-dimensional visual encryption schemes that can be integrated with three-dimensional light field control, thereby enabling the concealment and protection of three-dimensional information. This will further expand the application fields of optical encryption technology and bring more possibilities to the field of information security.

X. ADVANCED MULTIDIMENSIONAL OPTICAL FIELD STEERING FOR OPTICAL ENCRYPTION

A. STATUS

Research on optical image encryption began in the 1970s, initially focusing on leveraging optical systems to enhance data security through image processing and transformation. Early techniques primarily utilized optical modulation methods for encoding images, though these approaches were mostly experimental and not widely adopted. A significant advancement occurred in 1995 when Refregier and Javidi introduced the double-phase random encoding method, which employs random phase encoding in both the input and Fourier planes [2]. Traditional optical systems generally rely on phase modulation via light propagation through a medium, such as phase-type spatial light modulators. However, these systems face challenges including low resolution, large pixel sizes, and limited field of view. In contrast, metasurfaces modulate phase through strong interactions between their structures and light, often at a sub-wavelength scale. This capability enables metasurfaces to achieve high resolution, ultra-thin profiles, and exceptional properties, marking a new era in planar optics for optical devices. Additionally, metasurfaces can modulate amplitude, polarization, wave vector, and frequency, facilitating the development of high-capacity, multi-channel holographic encryption systems. Nonetheless, recent advancements in these areas are approaching their theoretical limits.

B. CURRENT AND FUTURE CHALLENGES

OAM provides a novel dimension for information transmission, akin to amplitude, frequency, and phase. Defined by its helical phase, which produces vortex beams, OAM encodes information through variations in the helical topological charge. This capability opens new avenues in optical communication and information processing, with significant potential for advancements in optical holography, encryption, and signal processing. In 2019, Ren et al. introduced OAM holography for high-security encryption, encoding information across different OAM channels to create a multiplexed hologram with 10-bit OAM encoding [70]. Subsequently, Fang et al. extended OAM-multiplexing meta-holograms for high-security applications, achieving a 10-bit OAM-multiplexed hologram that encoded Arabic numerals 0 to 9 by illuminating ten high-order OAM modes with topological charge numbers ranging from -50 to 50 [71]. To represent letters A to Z, they used two-digit Arabic numerals from 01 to 26. Despite these advancements, the encryption dimensions of conventional vortex beams limit the scope of standard OAM holography.

To enhance encryption dimensions, new vortex beam designs are needed. Integrating spin angular momentum (SAM) with OAM-multiplexed holography and manipulating full-polarization vectors remain underexplored. A key challenge is the lack of a practical mechanism to modulate both OAM and SAM eigenstates simultaneously. While cylindrical vector beams (CVBs) represent another vector light field, research into OAM holography based on CVBs is limited. Standard coherent OAM holography struggles to preserve OAM properties in densely sampled high-resolution images due to interference, imposing a fundamental resolution limit of $\gamma \leq 1$ for a given OAM channel number and limiting the potential of OAM holographic multiplexing. Additionally, OAM-multiplexing holography is prone to multiplexing crosstalk during image reconstruction, particularly affecting OAM beams with small helical mode index intervals.

C. SOLUTIONS TO THE PROBLEM

To enhance encryption dimensions, an ellipse-like beam is employed to achieve OAM multiplexed holography. This approach allows for the independent manipulation of three factors in the ellipse-like beam: topological charge, power index, and radial shift parameter [72]. By modulating both OAM and SAM eigenstates, angular momentum holography can synergistically utilize these two fundamental dimensions as information carriers through a single-layer, non-interleaved metasurface [73]. This design enables spatial modulation of the waveform by independently controlling and overlaying the two spin eigenstates in each operation channel. An angular momentum meta-hologram can reconstruct two distinct sets of holographic images—spin-orbital locked and spin-superimposed—resulting in multi-dimensional and multi-channel holography dictated by the incident angular momentum.

To incorporate CVB as an additional dimension in encryption, we propose a method that utilizes a parity Hall metasurface to separate the radial and azimuthal orthogonal degenerate states of a CVB with the same order [74]. This approach utilizes the relationship between mode field diameter and CVB order to apply intensity proportions as distribution probabilities for meta-atoms, thereby improving metasurface utilization and demultiplexing efficiency. A CVB-multiplexed holographic metasurface was designed to encode various images into CVB channels of different orders for effective holographic storage.

To preserve OAM properties in densely sampled high-resolution images, a model for multiplexed crosstalk in OAM holography is proposed. This model includes a method to achieve an almost crosstalk-free pseudo-incoherent scenario by adjusting γ [75]. By temporally multiplexing coherent light, the method approximates a pseudo-incoherent environment, effectively mitigating multiplexed crosstalk and achieving high-quality super-resolution. Image quality is assessed using structural similarity index measurements and variation coefficients. This approach facilitates high-quality, high-resolution, and high-capacity OAM multiplexed holographic reconstruction.

D. CONCLUDING REMARKS

Orbital angular momentum has emerged as a major area of research in information encryption. OAM metasurface holography offers the potential to create an almost infinite number of channels, each with independent modes, thereby greatly expanding information capacity. Beyond traditional spiral phase encryption, OAM holography utilizes additional dimensions, such as novel vortex light and polarization, to further enhance encryption capabilities. Additionally, the ability to achieve a crosstalk-free pseudo-incoherent scenario facilitates the production of high-quality super-resolution images. Consequently, OAM holography holds significant promise for advancing applications in 3D displays, secure information transmission, and sophisticated encryption technologies.

XI. VISUAL CRYPTOGRAPHY USING HIGHLY FOCUSED SPIRALLY POLARIZED BEAMS AND DEEP LEARNING

Encryption methods based on optical systems leverage the properties of light propagation. Polarization is one of the most valuable attributes of the electromagnetic field in security applications due to its ease of manipulation and measurement. Beams can exhibit random polarization, where the field direction changes unpredictably from one point to another. Conversely, it is relatively straightforward to generate beams with non-uniform polarization but well-defined symmetry profiles, such as radial, azimuthal, or spiral. The properties of the electromagnetic field in the focal domain of a high numerical-aperture microscope lens differ significantly from those in a paraxial system. While weakly focused beams can be accurately described using Fresnel formalism, the Richards-Wolf equation should be used to explain the field

near the focus. Even though paraxial beams are purely transverse, focused beams may exhibit a strong electric field component in the direction of propagation (longitudinal component, E_z). The presence of this longitudinal component is a consequence of Gauss's Theorem and can also occur in paraxial beams. However, in paraxial beams, the energy associated with E_z, which depends on the numerical aperture of the focusing system, can be neglected [76]. It is relatively straightforward to encode information in E_z, making it a proposed medium for encrypted data. Since separating the longitudinal component from the transverse components is challenging, the encoded information appears mixed with the transverse components, adding an extra layer of complexity [77].

A. VISUAL ENCRYPTION WITH FOCUSED FIELDS

Exclusive-OR (XOR) visual encryption (VE) is a popular cryptographic technique proposed by Naor and Shamir in 1994 [78]. Although originally intended for sharing digital images among multiple recipients, recent studies have reported optical implementations of this technique. Today, VE is an active research area, with contributions involving not only conventional optics techniques but also meta-surfaces and deep learning (see, for instance, ref. [79]). A VE system based on focused beams is outlined in Fig. 12 [80]. We demonstrated the feasibility of the technique using 10-bit Unicode characters, but it can be easily extended to arbitrary-length codes. Considering the inherent circular symmetry of optical systems, both characters are independently encoded as binary masks using a suitable method derived from [81] and displayed on a liquid crystal device (LCD). The characters are subsequently propagated through an optical system capable of producing and analyzing the polarization state of the corresponding focused beam. A collimated polarized laser beam illuminates the LCD displaying the encoded character. Then, a vortex retarder VR in combination with the polarizer LP2 produces a tunable spirally polarized beam. Relay lenses L2 and L3 project the beam onto the entrance pupil of a high-numerical-aperture microscope lens MO1. Finally, six polarimetric images (the same ones used to determine the Stokes parameters) can be recorded on the camera (CCD) with the help of a quarter wave plate QWP2 and polarizer LP3. This polarimetric set can be shared among up to six recipients.

The original character is retrieved from the polarimetric set by interrogating a convolutional neural network (CNN). The training dataset is generated by simulating the propagation of light through the optical system and calculating the corresponding polarimetric set. Provided the system is properly trained, the character is retrieved from the experimental set. This procedure is repeated for each subsequent character. Finally, both decoded characters are XOR-combined to decrypt the message.

The complete polarimetric set is utilized to retrieve the corresponding character. This process involves querying the CNN that was trained in an earlier stage. The training dataset was created by simulating light propagation through the optical system and calculating the corresponding six polarimetric images for all possible 10-bit characters. This interrogation procedure is performed twice, once for each polarimetric set, and the two recovered characters are then XOR-combined to decrypt the message. It is important to note that the state of polarization of the input beam completely influences the decryption process, as the entire training set depends on this property. Therefore, a different CNN should be trained for every possible state of polarization of the input beam, and the correct identification of the character relies on the use of the suitable CNN.

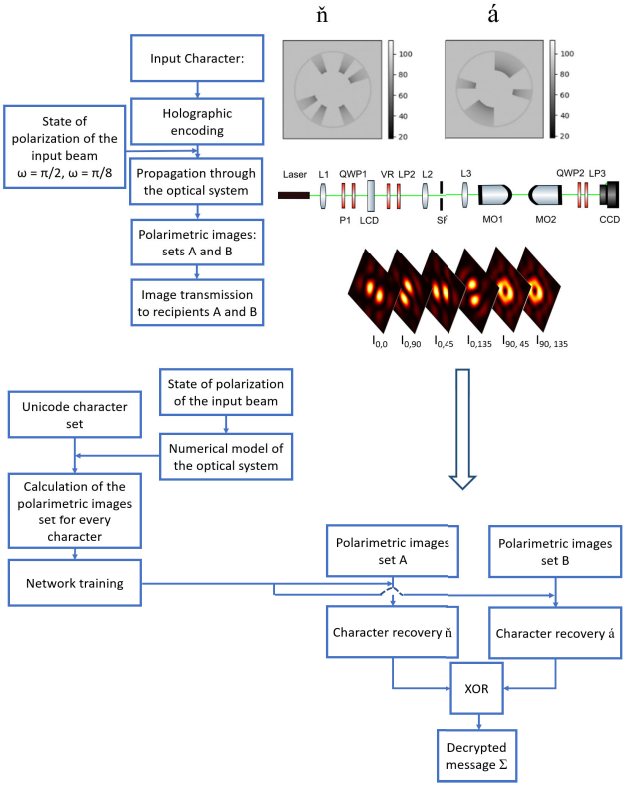


FIGURE 12. Outline of the Visual encryption technique using spirally polarized highly focused beams (adapted from [80]).

B. HARDWARE AND SCALABILITY CHALLENGES

The practical implementation of the optical encryption system involves hardware and scalability considerations due to the complexity of the setup and the use of CNNs. This setup integrates several devices that must be carefully aligned and stabilized; any slight misalignment, vibration, or drift due to mechanical perturbations or environmental changes can alter the resulting polarimetric intensity pattern, thereby degrading the accuracy of the CNN decoding. Moreover, the input polarization state must be stable and reproducible: since the encryption scheme relies on a specific state of polarization, any deviation in this state would require recalibration or retraining of the CNN to maintain accurate decoding. Consequently, high-quality optical components

and strict calibration procedures are needed to minimize aberrations and ensure consistent polarization, resulting in reliable and repeatable operations.

In terms of scalability, the current convolutional neural network (CNN) is tied to a specific optical configuration and training set. This means that (i) changes in the optical parameters, (ii) modifications to the encoding function, or (iii) the need to accommodate even a larger number of codes (> 10 bit) require the generation of a new training set, which increases classification complexity and results in longer training times. Furthermore, it will be necessary to develop enhanced CNN models that can tolerate minor hardware variations.

Note that the real-time implementation of the decryption system may be limited by the need to acquire up to six polarized images for each encrypted symbol. This limitation could be mitigated by integrating certain optical components, such as polarization cameras, capable of capturing all required channels in a single shot or faster spatial light modulators. Addressing these practical hardware issues and scalability considerations will be crucial for transitioning this polarization-based encryption technique from a laboratory demonstration to a deployable secure encryption system.

XII. NARROW OPTICAL SPECTRAL LINEWIDTH FINGERPRINTS FROM INTEGRATED PHOTONICS

Narrow optical spectral features are rare. We give an overview of natural and artificial systems exhibiting narrowband spectral features and argue that because of this rarity, integrated photonic circuits are excellent authentication tools.

Anticounterfeiting marks commonly employ advanced photonic structures, such as holograms, to create optical impressions that are difficult to replicate. These marks are relatively straightforward to fabricate and are typically identical across applications like IDs and bank cards. Visual inspection is required to verify their presence and integrity, necessitating close proximity to the anticounterfeiting marks.

By contrast, tags like barcodes in supermarkets serve a different purpose: identifying objects through machine-readable labels that do not necessarily require the protection of label integrity or copy resistance. These visual tags, like anticounterfeiting marks, also require proximity for inspection. However, if the readout relies on spectral properties rather than spatial ones, single-spatial-mode readout becomes feasible, enabling distant readout via a telescope or optical fiber. This concept is recognized, for instance, in the work on satellite license plates [82], where a combination of retroreflectors and spectral filters is used to create a passive tag suitable for satellite identification.

Photonic Integrated Circuits (PICs) offer the capability to engineer complex spectral signatures [83]. The cited example involves a network of ring resonators which produce spectral features with linewidths on the order of a few GHz using low-Q resonators. The commercial SiN PIC platform, utilized in this case, has also been shown to produce much higher-Q resonators with spectral linewidths in the MHz range [84]. Although other mature platforms, such as silicon-on-insulator (SOI), exist, SiN combines low optical losses with a relatively small feature size, making it an ideal candidate for these applications.

One might consider other optical systems that exhibit complex spectra with narrowband features. However, we argue that naturally occurring materials with such spectral characteristics are rare and, when they do exist, their features are typically weak. Identifying a system with a complex, fingerprint-like spectrum and sharp spectral features is an exceedingly challenging task. Our own survey, presented in the accompanying table, reveals that few materials or systems known for narrowband behavior approach these criteria. Notably, color centers in diamond and carbides come closest, but even these are limited in strength.

In hindsight, the challenge becomes clear: achieving narrow spectral features requires high Q factors, which necessitate either long-lived (and consequently weak) emitters or long optical path lengths in low-loss materials. For instance, the volume hologram filter achieves a linewidth as narrow as 6 GHz but requires a thickness of 8 mm. PICs, by contrast, allow the folding of very long optical path lengths into a compact footprint, typically by using high-Q resonators. Ref. [83] shows that such PICs share unclonability properties with PUFs.

The primary challenge that remains before PICs can be used as tags or unique keys lies in developing practical readout methods. Coupling PICs to single-mode fibers or optical telescopes is relatively straightforward. However, creating small PICs that can be read from a distance may require advanced solutions such as optical phased-array antennas or integrated photonic retroreflectors [85]. Spectral readout can be performed with a calibrated fast-scanning narrow-linewidth laser and recording the reflection or the transmission, if accessible. The entire spectrum does not need to be measured, a random spectral window can be chosen. Alternatively, Fourier-transform techniques can be used to obtain spectral data faster. The obtained spectrum should be compared with a public database of known spectral fingerprints to obtain a unique digital identifier of the tag or key. We conclude that PICs are ideally suited for the creation of optical spectral fingerprint tags or hardware tokens, which are exceptionally difficult to replicate using alternative methods.

XIII. METASURFACE-ASSISTED OPTICAL SECURITY AND ENCRYPTION

A. STATUS

With the rapid advancement of information technology, securing information has become a vital task, especially with the growing threats to data privacy and security. Traditional cryptographic techniques based on some mathematical algorithms are increasingly vulnerable to advances in computational power. Optical security and encryption offer a powerful approach to protecting sensitive information

TABLE 1. An overview of narrow spectral-feature systems and materials.

Material	Remark	Linewidth
Rhodamine 6G dye	Widely used in dye lasers	50 nm ≈ 35 THz
Rare-earth doped glass [86]	Inhomogeneous broadening	3 THz
Polymethine dyes (Organic Dye)	Relatively small homogeneous broadening	10 - 100 GHz
Narrow-band Interference filters [87]		100 GHz
Lyot filter	Using a thick birefringent material	0.05nm ≈35 GHz
Volume holographic filters [88]	Thickness limited. In this example, 8 mm	0.01nm ≈ 6 GHz
Metamaterials [89]	Relatively new development	0.01nm ≈ 6 GHz
Atomic gases	Doppler broadening	0.2 - 1 GHz
Color Centers in Diamond or Carbide	Spin transition lines used for qubit systems	10 - 100 MHz

by leveraging the inherent properties of electromagnetic beams and various optical systems. Unlike the traditional cryptography method based on mathematical algorithms, optical encryption utilizes photon's abundant degrees of freedom (DoFs) to encode information securely. However, conventional optical encryption systems often rely on a complex arrangement of optical components, leading to bulky setups. Moreover, traditional optical elements offer limited control over the optical field, leaving the full potential of light's multi-dimensional DoFs untapped. Metasurfaces (MS), two-dimensional artificial structures consisting of subwavelength light-modulating unit cells, have demonstrated a remarkable ability to structure multi-dimensional optical fields. This makes them a promising solution for compact optical encryption systems. In recent studies on optical encryption using metasurfaces, information is encoded directly into the metasurface structures, which serve as physical carriers. These methods can be broadly classified into three categories. (1) DoFs space: This strategy involves utilizing single or multiplexing multiple DoFs of light, such as polarization, frequency, incident angle, nonlinear effects, OAM, and higher-dimensional Poincare beams; (2) Spatiotemporal space: In this approach, tunable modulation is achieved through external stimuli, such as chemical reactions, changes in the surrounding medium, mechanical actuation, electrical gating, and phase transition materials; (3) Algorithm space: This category includes techniques like computational approaches with single-pixel imaging (SPI), vector visual cryptography, code division multiplexing, and secret sharing with cascaded metasurfaces [90]. Researchers have demonstrated highly secured optical encryption strategies using spin-orbital-locked and spin-superimposed holographic images, which employ angular momentum holography technique on a single-layer, non-interleaved metasurface [73]. Additionally, hierarchical encryption schemes have been developed, integrating both direct and indirect observation channels. These systems could incorporate tunable materials to achieve a dual/multi-channel metasurface based on polarization and angular multiplexing. A large-capacity secured optical encryption strategy has also been proposed using multi-channel, high-dimensional Poincaré beams generated through cascaded metasurfaces [91]. By cascading two arrayed metasurfaces, more beam properties can be independently engineered, significantly expanding both the key space and encoding possibilities. Thus, the introduction of metasurfaces into optical encryption technology has paved the way for highly secure encryption schemes, primarily by combining the DoFs space with the algorithm space.

B. CHALLENGES

Nanophotonic technology could address a range of challenges currently faced by classical optical encryption schemes. One of the primary issues is the sensitivity of optical systems to alignment and environmental factors, such as noise and interference, which can significantly degrade the quality of encrypted signals. Wafer level, vertical stacking of metasurfaces allows for precise alignment, and precise vertical integration. Additionally, the security of existing encryption strategies is not absolute and highly dependent on the complexity and number of encryption keys. While increasing the number of keys can enhance encryption security, managing and securely distributing encryption keys poses a challenge, particularly when keys are shared through classical communication channels or via verification codes. These classical methods are often vulnerable to tampering and lack the protection offered by the no-cloning theorem, which safeguards entangled photons in quantum communication. Scalability is also a concern, as current optical encryption technologies are not yet fully optimized for large-scale real-life applications. Further encryption dimensionality can be accessed using active metasurfaces, however, achieving pixel-level real-time modulation for dynamic arbitrary wavefront steering in optical frequencies remains a hurdle. Furthermore, these systems are susceptible to physical attacks, such as tampering with optical components, which can compromise the security of the data. Lastly, the absence of standardized protocols in optical encryption makes it difficult to integrate these technologies into existing security frameworks, leading to inconsistencies in performance and security across different implementations.

C. ADVANCES VIA LEARNING-BASED OPTICAL ENCRYPTION STRATEGY

The above-discussed limitations of securing data through a classical communication channel can be relaxed using innovative learning-based optical encryption methodologies. Artificial intelligence, especially through the use of deep neural networks (DNN), consisting of multiple layers of

interconnected neurons, has emerged as a powerful tool for decrypting sensitive data through a learning-based mechanism. One key advantage is that the associated database faces minimal risk of leakage, as it can be promptly deleted after the training process is complete. The decryption relies solely on the trained network, without needing access to the original database. As a result, the database remains protected and inaccessible to users. Based on this principle, recently, researchers have proposed a highly-secured learning-based optical encryption method using disordered metasurface (DM) [92]. In this encryption system, plaintext/image optical information is first combined with a QR phase code (acting as a security key) to create a secure input as shown in Fig.13 a). The inputs are then transmitted through the disordered metasurface, generating speckle intensity patterns (ciphertext) that contain both the encrypted input information and the security key. Decryption only occurs when users are providing the correct combination of security key, ciphertext, and polarization to a previously trained neural network. To ensure a high level of security and prevent unauthorized access, only the receivers should have access to the decoding neural network. To decrypt the speckle patterns, multiple neural networks P(i)/P(j)-DMNet are trained, each corresponding to specific polarization states P(i)/P(j) and input data. These networks learn to accurately decipher the plaintexts/images only when the speckles and security key match, ensuring that unauthorized access is prevented even if the ciphertext is obtained. The proposed encryption system based on disordered metasurfaces provides ultra-stable and secure encryption, suitable for real-world applications. Combining multiple polarization channels and a double-secure encryption method, it addresses the limitations of conventional scattering-based systems, offering enhanced security and robustness.

D. FUTURE PERSPECTIVES

The implementation of optical encryption using metasurfaces faces several challenges associated with large-scale manufacturing and their integration into compact embedded electronic systems. However, a key advantage is the compatibility of metasurface fabrication with conventional CMOS chip manufacturing processes, which supports scalable production. In addition, their inherently planar configuration facilitates co-integration with electronics. The potential to cascade multiple metasurface layers in a compact architecture, as reported in the context of the so-called diffractive neural networks, may further enhance the encoding capacity and information density, thus offering a path toward scalable and efficient metasurface-based photonic systems. In parallel, optical encryption using entangled photons offers immense potential for revolutionizing data security. Optical encryption using entangled photons offers immense potential for revolutionizing data security. Entangled photons, safeguarded by the no-cloning theorem, are inherently resistant to unauthorized interception. As recently proposed, MS provides an ideal platform for generating multichannel, high-dimensional

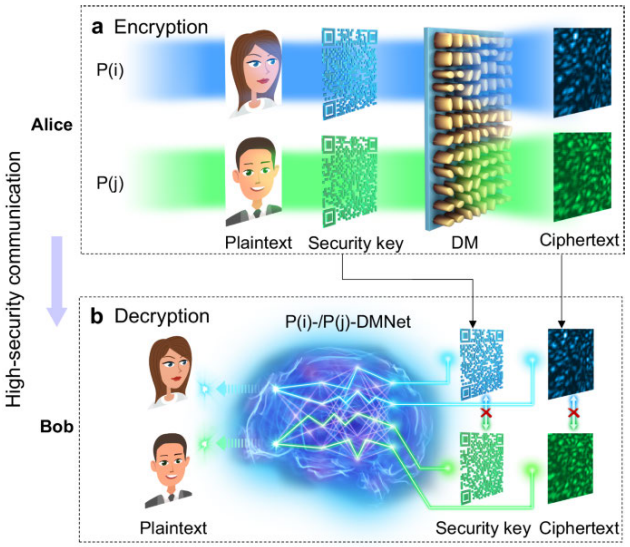


FIGURE 13. Schematic representation of learning-based optical encryption system. a) Secure data encryption via spin-multiplexing disordered metasurface and b) Learning-based decryption process with two spin-dependent deep neural networks (DNN). Figure reproduced with permission from ref. [92], Nature Publishing Group.

entangled photons, overcoming the limitations of traditional nonlinear materials [93]. By relaxing momentum conservation in spontaneous parametric down-conversion (SPDC) processes, MS enables the generation of SPDC photons with arbitrary frequencies and directions. Additionally, all-dielectric MS facilitates multiphoton quantum interference and state reconstruction [94]. The fusion of entangled photon-generated ciphertext (in the form of speckle patterns or any arbitrary spatial mode mixing) with a DNN-based decryption process further enhances the security manifold, thus, paving a groundbreaking pathway toward unbreakable communication technologies. In addition, the arbitrary light modulation properties of metasurfaces can be extended to entangled photons wavefront engineering, reaching levels of innovation far beyond the simple beam splitters used for quantum optics experiments [95], which would eventually offer new prospects for achieving structured entangled multiphoton fields, including higher-dimensional encoding through OAM modes and arbitrary polarization-based quantum entanglement. This increases the keyspace and complexity, making metasurface-based optical encryption exponentially harder to break, while also providing tamper detection through the sensitivity of entangled states to disturbances, ensuring innovative, robust, and more secure communication.

XIV. OPTICAL AUTHENTICATION USING NANOSTRUCTRED MATERIALS AND POLARIZED LIGHT

Since the publication of the seminal papers in optical security and cryptography [1], [2], researchers have focused on the development and improvement of encryption techniques or performing cryptanalysis against common attacks. Comparatively, little work has been done regarding optically

authenticating both the sender and the message. In contrast, digital signatures play a critical role in electronic communications, as they provide (i) a way to trust the identity of the sender and (ii) that the message has not been tampered with during transmission. Note that signing a message does not add anything to the encryption process, but it ensures that the sender is who they claim to be. It is possible to transfer this concept to the physical realm: under certain assumptions, a distinctive, unique, and non-clonable signature can be assigned to a specific physical device [96]. Various strategies have been developed to assign signatures to the materials that support the message to be transmitted, which can be analyzed and processed by optical methods. Unlike their digital counterparts, an optical signature is not based on mathematical methods related to asymmetric cryptography and private and public key pairs. In the problems we are considering, secure unclonable ID tags are generated by the light that interacts with the device where the message is encoded, e.g.: the physical configuration of the nanoparticles within the material is responsible for generating a unique optical signature. There are various materials with suitable properties able to generate optical signatures that can be authenticated. Among them, we highlight devices containing metallic nanoparticles [97], or those that have been manufactured using thin-film metal deposition techniques [98]. We have also created optical codes with a 3D printer using a special wire made of polylactic acid (PLA) combined with metal powder. Interestingly, these 3D-printed codes behave similarly to those fabricated using the nanoparticle structures mentioned above, but they have been made with much simpler and affordable equipment [99]. Very often, an extra layer of complexity is added to the design of an optical code. When light passes through a diffuser, the phase of the wavefront is randomly modified at every point. Phase encoding is a common technique in information optics because after propagation, the beam generates a speckle-like distribution. [97], [98], [100]. With advances in material science, diffusers may be replaced with specially fabricated metamaterials. A particularly useful scenario was described in [101]: The sale and consumption of counterfeit pharmaceutical products outside the regulated supply chain can pose a significant public health risk. A feasible way to circumvent this fraudulent activity is to optically tag the product by adding gold nanoparticles in the pill coating. Polarimetric techniques are so precise that they can even distinguish pills with varying concentrations of gold nanoparticles. This technique might provide patients with the assurance that the product they are acquiring has not been tampered with.

When the code is illuminated with a polarized beam, a unique speckle distribution is generated. Then, the reflected light is analyzed using conventional polarization analysis methods by estimating the Stokes vector of the reflected light recorded with a camera, and assessing the characterization of the Mueller matrix of the sample. Given the statistical nature of the speckle distribution, basic statistical characteristics can be estimated such as mean, variance, skewness, kurtosis, entropy, and the gray scale histogram. This information is used to train classical machine learning classifiers. Depending on the problem, k-nearest neighbors, support vector machines, and random forests have been used. However, deep learning algorithms may be used as well. Principal component analysis might be required to reduce the dimensionality of the problem for computational efficiency. To allow the classifier to be successfully and reliably trained, it may be necessary to generate a sufficient volume of data to produce training, test, and validation sets. With the popularization of convolutional neural networks, these methods could gain robustness, as they do not depend on the selected features, although it might be necessary to generate even larger training sets.

XV. AUTHENTICATION VIA TRUE REPEATABLE RANDOM NUMBER GENERATORS AND OPTICAL SCATTERING PUFS

Physical authentication allows a material element or, whenever appropriate, the element holder, to be cryptographically identified by physical probing. Material elements which are subject to uncontrolled variations inherent to their fabrication process, are intended to be the site of a physical phenomenon when interacting with the probe. Probing different elements produce unique patterns captured by a sensor then processed in order to extract robust fingerprints, some feature vectors serving as identifiers. In optical authentication, material elements represent complex photonic structures without any microelectronic circuitry, and dedicated probe systems are lighting equipments. The more straightforward, the more efficient. Elements must be easy to fabricate and use, authentication patterns easy to produce. *Easy to fabricate, use and produce* requires material elements made from inexpensive components according to a standard fabrication process, and light source with mount should be integrable. Fingerprinting with the whole opto-digital chain must be fast.

Uniqueness and *unpredictibility* of patterns and fingerprints are required for authentication. The fabrication process is expected to produce random fluctuations in the material structure, leading to a large number of light signals when probing, very different from each other. For this purpose, light-matter interaction has to provide highly uncorrelated patterns when sampling the state space of the physical process, and high entropy when extracting fingerprints. Information compression by capturing 1D or 2D patterns from 3D random media at a certain scale is the first step in the fingerprinting process. In addition, the source of information that the physical process constitutes together with the light probe needs to be stable over time and external conditions: *reliability* is essential for a successful implementation. In the end, any design will be supported by heuristic arguments explaining its ability to satisfy at least uniqueness, unpredictability, and reliability, together with resistance to some attacks. These arguments are derived from signal or image formation models. These preliminar requirements have

to be confirmed by implementing the whole fingerprinting process, and measuring false acceptance and false reject rates from actual samples. Some complementary properties may be required by the application for the authentication protocol.

We will focus here on two challenge-response protocols devoted to the authentication of 3D microstructures via 2D imaging patterns resulting from light scattering. These protocols rely on *unclonability*: it must be hard to clone any of the material elements produced by the implemented fabrication process even by using the most avanced fabrication technologies (e.g. nanoduplication). At some scales, the elements correspond to disordered media in different states $\mathbf{x}$ issued from a random variable $\mathbf{X}$ which represents their fabrication process. A given material element in state $\mathbf{x}$ will be here authenticated in two different frameworks: either from a single challenge-response pair (CRP) or from numerous ones in different lighting conditions.

A. TRUE REPEATABLE RANDOM NUMBER GENERATORS

A symmetric challenge-response protocol can be implemented without digital key exchange, typically for authenticating a paper document transmitted by Bob to Alice. This can be achieved by coding texture captured from the light scattered by such a strongly diffusing structure, usually in incoherent regime. For this purpose, a bitstream serving as encryption key $\mathbf{k}(\mathbf{x})$ is extracted from material element $\mathbf{x}$ to be currently authenticated, first by Bob for further deciphering, then by Alice (the trusted receiver of the element) for ciphering a n-bit nonce sent on-line by Bob (the verifier). If the element is authentic, the encryption key is the right one. This requires an extraction of pure random bits from the material element, and the ability to re-extract with high probability the same bits from the same element at any later time. Such a True Random Number Generator (TRNG) has been implemented via an adaptative image source coding delivering sparse and dispersed binary sequences where each bit represents either the positive or the negative, non-standard contribution of a locally strong eigenmode or equivalent [102]. Let us note that probabilistic repeatability is specific in the field of TRNGs, and that the so-called TR*epeatable*RNGs were coined in the goal to extract bits of information anchored in physical random structures. A few random bits per mm^2 can be extracted on average from a standard paper sheet. A truncation of the extracted sequences to n bits gives random binary vectors usable as random fingerprints. This approach eliminates the need to store an identifier in comparison with fiberfingerprinting [103], a biometric approach combined with digital signature, where a fingerprint is first extracted, then printed (in machine-readable format) together with data and their digital signature for later off-line verification.

In this framework, we can consider a layer of diffusing medium with heterogenous structure at the microscopic scale, whose macroscopic transmittance varies randomly according to the position ξ over the surface. The area imaged in one pixel of the image is assumed much larger that the thickness of the layer, which prevents considering the lateral flux exchanges between adjacent areas, and thus allows using an optical model based on the two-flux theory. According to this theory, the flux transfers that occur in the area around each position can be represented by a flux transfer matrix of the form [104]

$$T[\mathbf{x}] = \frac{1}{\tau}\begin{pmatrix} 1 & -\rho \\ \rho & \tau^2 - \rho^2 \end{pmatrix} \tag{1}$$

where ρ and τ denote the reflectance and the transmittance of the layer, related to the absorption and scattering coefficients of the material and a layer thickness of reference, e.g., the average layer thickness. A change of layer thickness or concentration in scattering elements, as it happens in a paper sheet where the sheet thickness is higher or the fibers are denser in some place, results in a change of optical thickness γ and a new flux transfer matrix simply given by $T[\mathbf{x}]^\gamma$. The transmittance as captured by the sensor in each position ξ is thus given by

$$\tau(\mathbf{x}, \xi) = \frac{1}{\left(T[\mathbf{x}]^{\gamma(\xi)}\right)_{11}} \tag{2}$$

Such a non linear image formation which reflects the inhomogeneities of any random microstructure $\mathbf{x}$ is highly stable as long as normal conditions of use are maintained. A Gaussian distribution is obtained for output intensity in the case of normal diffusion. This reflects a large number of independent scattering events in volume. The standard deviation gives a unit for a patch-based analysis approach which leads to key $\mathbf{k}(\mathbf{x})$ after coding as described.

B. OPTICAL SCATTERING PUFS

When physical authentication concerns a communication token, material element $\mathbf{x}$ is encapsulated to be probed on demand in response to one of a large number of challenges. In optical imaging, light-matter interaction is expected to deliver many highly uncorrelated patterns by varying probe state, and some lighting parameters θ. Outputs are unpredictable fingerprints $f(\mathbf{x}, \theta)$ algorithmically derived from the patterns. A set of CRPs $(\theta_\mathbf{i}, \mathbf{f}(\mathbf{x}, \theta_\mathbf{i}))$ precommitted by Bob (the verifier) from *function* $f(\mathbf{x}, \cdot)$, can be each used one time with the aim of authenticating material element $\mathbf{x}$: the more valid responses to challenges, the more confident in Alice's identity. Any valid response must remain unpredictable knowing a subset of valid pairs coming from the same element and potentially eavesdropped. Three other properties are required to get an *authentication* PUF. First, the function must have a *high sensitivity to probe state changes* (in addition to a high sensitivity to material element) in order to prevent from finding collisions knowing a set of CRPs, and to ensure tamper-resistance. Another property refers to the absence of a polynomial complexity algorithm and machine learning model (e.g. a generative model) able to computationally generate a pattern so a response corresponding to a given probe state (challenge)

knowing a fine description of the current material element. The *hard to simulate* property makes the presence of the material element necessary. The last property is *immutability*, required to ensure that each fingerprint is irreversibly altered if tampered with.

As reported in the seminal work by Pappu et al. [105] in which the concept was introduced under the name of *Physical One-Way Functions*, coherent multiple scattering is a physical phenomenon well-suited to design functions checking the properties of a PUF. Its various implementations are now known as Optical Scattering PUFs (OS-PUFs). In particular, the coherent illumination of a disordered medium composed of randomly distributed scatterers in a transparent substrate (e.g. glass spheres with an average diameter of 500 μm, distributed in epoxy) allows a high sensitivity when changing the probe state, typically the incidence angle of a laser beam. This results from a random phase along the wavefront emerging from the medium after the waves diffracted by the scatterers at random positions interfere constructively or destructively with each other. A speckle figure is then formed in the image sensor plane. Rotating the incident beam by a very small angle shifts the speckle pattern in the image plane until a new speckle pattern appears uncorrelated with the previous one. The angle necessary to obtain two (highly) uncorrelated speckle patterns is typically a ten of microradians. When assuming material element $\mathbf{x}$ as a linear medium and focusing on input-output relationship, light transport can be described by a $2N \times 2N$ complex-valued transmission matrix $\overline{\mathbf{T}}_{\mathbf{x}}$ where N corresponds to the number of independent ingoing and outgoing modes (discriminative incidence angles). It is given by $N = \frac{2\pi A {n_e}^2}{\lambda^2}$ where n_e is the effective refractive index of the medium, λ is the incident wavelength, and A is the illumination area. Note that in practice, a more efficient variable probing is performed by using a laser beam at normal incidence with a DMD or a LCD screen: the probe space is defined by the set of $N_r \times N_c$ bitmaps displayable on the matrix light source. However efficient phase-retrieval based techniques can be used for measuring transmission matrix $\overline{\mathbf{T}}_{\mathbf{x}}$, and some numerical methods are in a position to efficiently recover it from an accessible number of CRPs. In this context, the hard to simulate property is not verified. To make the problem harder, OS-PUFs assume coherent multiple scattering in a weak non-linear regime: the mean free path is considered much greater than wavelength λ plus an enhanced backscattering length. The resulting distributed non-linearity aimed to force an attacker to collect an unreasonable huge number of pairs, towards an order of magnitude close to $2^{N_r \times N_c}$ so much more than only $N_r \times N_c$ single lighting pixel activations in linear regime.

The first manufactured integrated version, made with a linear scattering structure, was successfully attacked by machine learning algorithms in [106]. The attack assumes that the adversary has access to speckle patterns during the training phase. In reply to modeling attacks, many efforts were deployed to develop highly non-linear optical materials and increase the dimensionality of the challenge-response space, as in [107]. Learnability of OS-PUFs was only addressed in depth very recently in [108], on the basis on the Probably Approximately Correct framework: in the case of a weakly non-linear dielectric medium, such a PUF can be efficiently learnt to arbitrary precision with arbitrarily high probability, given a number of CRPs polynomially bounded based on the number of pixels in both the matrix light source and the image plane.

C. CONCLUDING REMARKS AND FUTURE DIRECTIONS

Whereas TRRNGs are today in use for authenticating manufactured goods [109], implementing all the properties that define an authentication OS-PUF in a miniaturized system is still challenging. Addressing silicon compounds such as metasurfaces with quantum dots compatible with standard manufacturing [110], opens up routes of photonic authentication for Si chips, an alternative to electronic PUFs. Learning complex scattering structures efficiently with a tractable amount of real CRPs is another feature direction. Physics-informed machine learning can help in this task and afterwards improve design.

XVI. TOWARDS MULTI-DIMENSIONAL OPTICAL ENCRYPTION ON A CHIP

A. STATUS

Optical information processing systems, characterized by their high-speed and parallel processing capabilities, are particularly well-suited for applications in information encryption and security. Traditionally, this is achieved by strategically positioning multiple random phase masks along distinct planes parallel to the optical axis within the system. Upon illumination of a plaintext image with a coherent laser beam, a ciphertext image exhibiting a noise-like pattern is generated at the output plane. This phenomenon arises due to the interaction of each spatial frequency component of the wavefront with a series of stochastic perturbations as it propagates through the system.

B. CURRENT AND FUTURE CHALLENGES

In the past three decades, the field has witnessed three primary developmental trajectories. First, the simple optical Fourier transform system employed in the early study by Réfrégier and Javidi [2] have been extended to linear canonical transform systems including fractional Fourier and Fresnel transforms [111] and gyrator transform [112]. Second, the introduction of new imaging modality such as computational ghost imaging [113]. And finally, research has expanded to include the encoding of light field attributes beyond phase, such as polarization states [35]. These advancements are aimed at bolstering the security of optical encryption systems.

However, the linear nature of these systems poses significant security vulnerabilities [114]. The ciphertext image, when represented as a two-dimensional array, can

be formulated as a system of linear equations relative to the input plaintext image. Despite the complexity, these equations are deterministic and, in theory, reversible given a sufficient number of equations. This reversibility implies that an adversary with knowledge of the system parameters could potentially decrypt the ciphertext [115]. In addition, traditional optical encryption systems often use bulky optical components, which have low robustness and limited capacity for encrypted information. It is essential to find more compact, stable, and efficient encryption devices.

C. ADVANCES IN SCIENCE AND TECHNOLOGY TO MEET CHALLENGES

On-chip integrated metasurfaces offer possibilities to meet the aforementioned challenges. First, photonic chips provide a compact and stable platform that enhances the stability of decryption systems. Second, on-chip systems based on metasurfaces possess the ability to control multidimensional optical fields, which helps increase the information capacity of optical encryption. Finally, Metasurfaces can enhance the nonlinear effects of materials, enable dynamic encryption and break the attacker's linear assumptions about the encryption process. Taking dielectric materials as an example, on-chip integrated metasurfaces can be created by growing or etching structures with subwavelength resolution on traditional waveguides [116]. By modifying the duty cycle of the structure, the spatial distribution of the effective refractive index can be customized to achieve specific functions. Gradient metasurfaces can be designed to realize mode conversions within the waveguide, such as polarization evolution, signal routing, and optical nonlinear effects. They can also achieve mode conversions between waveguides and free space, such as efficient coupling, on-chip holography, and structured light generation.

Because the metasurface unit structures operate on subwavelength scales, they can be used to change polarization states by modifying anisotropic responses. Arbitrary Stokes parameter transformations can be implemented with the help of geometric phase, propagation phase, and resonance phase. The geometric phase can also be used to control the spin angular momentum. Arranging vortex phases in space can generate orbital angular momentum, and by modifying the geometric configuration and structural parameters, frequency selection and dispersion control can be achieved. Overall, on-chip integrated metasurfaces exhibit flexible multidimensional optical field control capabilities [117].

Silicon and lithium niobate are two common on-chip materials, both of which exhibit nonlinear effects. Through external excitation, dynamic beam control can be realized. However, their nonlinear responses to external excitation are very weak, for instance, the refractive index change caused by lithium niobate's electro-optic effect is typically around 10^{-4}. Achieving large phase shifts usually requires sufficiently long waveguides, which increases the device's size. One characteristic of metasurfaces is their ability to flexibly control the quality factor of resonance, ranging from tens to tens of thousands. This is very beneficial in addressing this issue. By designing structures with high quality factors, the optical field can be localized in a small region [118], enhancing the interaction between light and lithium niobate, thereby amplifying the electro-optic effect while balancing modulation efficiency and compactness. Besides silicon and lithium niobate, other tunable materials such as phase-change materials can also be integrated to achieve richer control effects. The dynamic modulation capability are beneficial for building high security encryption systems.

D. CONCLUDING REMARKS

In this chapter, we introduced the challenges faced by traditional optical encryption, including security issues caused by linear encryption, information capacity limitations due to low-dimensional optical field control, and stability problems in bulky systems. By incorporating metasurfaces into photonic chips, leveraging their resonance-enhanced nonlinear effects and multidimensional optical field control capabilities, a promising platform is provided for constructing highly secure, high-capacity, and ultra-compact optical encryption systems.

XVII. ENCRYPTION BY OPTICAL COMPRESSIVE IMAGING FOR SAFEGUARDING DEEP NEURAL NETWORKS

A. THE ADVERSARIAL-ATTACK ARM RACE ON DEEP NEURAL NETWORKS

DNNs have become a ubiquitous enabling technology for an extremely wide range of applications. Unfortunately, most DL architectures are vulnerable to Adversarial Attacks (AA), which involve making small perturbations to images to cause the DL algorithm to fail. Even though numerous defense algorithms have been developed to address the threat of adversarial attacks, all existing defenses are in the software domain, which facilitates developing counter-attacks, known as adaptive attacks. As a result, an ongoing arms race between DNN designers and attackers has emerged.

This arms race can be stopped or mitigated by employing optical encryption to secure data before it is presented to a DNN system. We have introduced such a defense strategy in [119] where we used optical Compressive Imaging (CI) [120] for encryption. The ability of CI to block AA in computer vision was further validated in a recent comprehensive study [121]. The study found that a digitally implemented compressive sensing model enhances the security of computer vision systems, provided that the adversary does not have access to the CI model. The optical implementation of CI meets this requirement by serving as a hardware encryption process [4], which effectively prevents the adversary from gaining access to the CI model (see Section C), thereby protecting the Deep Neural Network (DNN) from adaptive attacks.

B. BLOCKING ADVERSARIAL ATTACKS WITH OPTICAL COMPRESSIVE SENSING

Compressive Imaging (CI) [122] is an image acquisition theory that allows for the sensing and reconstruction of an N-dimensional signal, $\mathbf{f} \in \mathbb{R}^N$, using only $M < N$ measurements, $\mathbf{g} \in \mathbb{R}^M$, through a linear sensing process $\mathbf{g} = \Phi\mathbf{f}$. The sensing matrix $\Phi \in \mathbb{R}^{M\times N}$ represents the randomized sampling of $\mathbf{f}$ [122]. While CI was originally developed for signal acquisition, it can also be employed for image encryption [28]. In this context, the input $\mathbf{f}$ represents the plaintext, the output $\mathbf{g}$ represents the ciphertext, and the compression process functions as the encryption algorithm, with the random matrix Φ serving as a symmetric encryption key. To defend against AAs, CI can be combined with a DNN in the two configurations depicted in Fig 14. Both schemes replace the standard camera with a CI for capturing the image provided for the DNN.

The scheme in Fig. 14(a) follows a conventional CI acquisition-and-reconstruction process followed by the DNN, which performs a desired task (e.g., classification, detection, detection, segmentation, etc.). Then, the input signal is reconstructed by one of the iterative algorithms available in the CI literature [120] or by one of the recent DL reconstruction methods [123]. Finally, the threatened DNN processes the reconstructed signal. The CI process acts as a pre-filtering of the DNN's input and, along with the reconstruction algorithm, removes the adversarial perturbations applied on $\mathbf{f}$. From a cryptographic point of view, CI encrypts the image with Φ operating as a symmetric key, shared between the compressive imager and the reconstruction algorithm through a secure channel. Without the knowledge of Φ the adversary cannot develop an adaptive attack.

With the scheme shown in Fig. 14(b), the CI process offers defense from adversarial attacks by concealing the sensing matrix Φ from the attacker. However, unlike traditional CS (Fig. 14(a)) the signal $\widehat{f}$ is not reconstructed before the application of the DNN. Instead, the DNN is applied directly to the CI data. The DNN needs to be trained on labeled data generated by the specific CI matrix used. The CI encryption conceals the gradients from an adversary, preventing potential attacks. Even if the attacker fully knows the targeted DNN, without access to Φ, it will be extremely challenging, if not impossible, to devise efficient attacks.

We have demonstrated the defense using the method depicted in Fig. 14(a) in [119]. We implemented CI using a single-pixel camera setup that utilized a scrambled Hadamard transform at a compression rate of 20:1. The CI method has effectively defended a ResNet101 classifier from physical attacks on real-world objects. In a separate study [124], we also demonstrated the effectiveness of compressive 3D imaging in defending deep learning models against attacks on point clouds, such as those generated by LiDARs. Our simulations revealed that CI was able to evade 89% of Carlini-Wagner adaptive targeted attacks on a PointNet++ classifier.

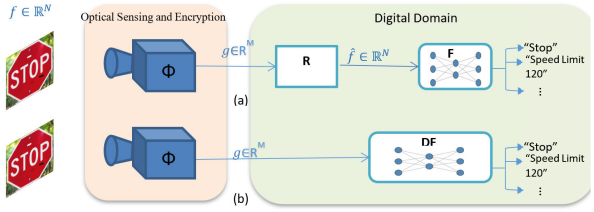


FIGURE 14. Two schemes that use optical CI for defending a DNN, F, from physical world adversarial attacks on the object, f. R represents the reconstruction algorithm, and DF is DNN trained to perform tasks applied directly to CI data. An adversary may have complete knowledge of the targeted DNN model. However, he does not have access to the exact structure of the CI matrix, Φ, which serves as an encryption key.

C. SECURITY OF THE OVERALL SYSTEM

For a common image size, N, the key space spanned by all possible random keys is extremely large, providing practical computational secrecy. However, due to the linearity of the CI process, it may be vulnerable to attacks from a malicious eavesdropper that gains access to input-output pairs. In such a case the eavesdropper may apply a known-plaintext attack (KPA) or a chosen-plaintext attack (CPA) [4] to infer the key Φ. In practice, since CI is applied on high-dimensional data (images having a large number of pixels, N), it has a noteworthy level of security against KPA, but it may be vulnerable to CPA if the eavesdropper can apply interrogations of the CI system. Fortunately, owing to the optical (hardware) compressive imaging, applying such attacks requires an enormous effort since it involves generating exact physical plaintexts, properly placing them in front of the imager, capturing the output, and repeating this process N times (where N is the number of image pixels). Furthermore, as a countermeasure against CPA, the key can be varied periodically.

In summary, optical CI provides efficient defense against AAs. While it may not surpass software-based defense methods in terms of performance, it does deliver competitive results. Most importantly, it provides resilience against adaptive attacks, presenting a unique solution to the persistent issue of the arms race between attackers and software-defense practitioners. Future work direction would be to develop fast optical CI systems with dynamic sensing matrices capability.

XVIII. OPTICAL ENCRYPTION TECHNIQUES FOR MULTI-DIMENSIONAL PHYSICAL DATA

Optical encryption techniques [81] can encrypt image data using physically real diffusers such as phase modulation, and thus can enhance the strength of encryption in a way that strengthens computer-based encryption techniques such as RSA or DES. In particular, the double random phase encryption technique can use various physical information of light waves, such as two random phase masks [125], their positions [7], wavelengths, and polarizations [126], and thus has the advantage of multidimensionality in the information required for data decryption. The optical data

encryption can be used in the voice recording [127], [128]. Here we will review our optical encryption techniques and their applications to optical data storage and optical voice recording.

Optical data storage is one of the most promising data storage systems, especially for cold data. Compared to other data storage systems such as HDD (hard disc drive), SSD (solid-state drive), and tape drive, optical data storage has strong advantages such as long-term storage of more than 30 years, resistance to magnetic noise, compatibility to reading devices. However, storage capacity and recording/reading speed are two major problems. Optical encryption techniques can enhance the usage of optical data storage because the physical data encryption as well as software data encryption can be used simultaneously. It enhances security levels from attacks. Holographic optical memory can record page data as encoding amplitude, phase, and polarization for increasing the data amount, in a volume medium. We have proposed optical encryption techniques such as double random phase encryption in Fresnel domain [7], polarization encoding for holographic data storage. Especially, double random phase encryption in Fresnel domain opened new research directions to increase the total number of keys. Polarization is also important physical parameter of optical wave.

Digital holography is one of the recording methods of hologram in a digital image sensor and then original data can be reconstructed in a computer by calculating the optical wave propagation by extracting the optical wave from the hologram. We have proposed an optical sound imaging technique based on digital holography called optical microphone [127]. Sound wave modulates the refractive-index of the air and then phase modulated light wave caused by the refractive-index change by sound wave can be recorded as digital holograms. To capture the propagation behavior, frame rate of the image sensor should be fast due to sampling theorem. Voice data is one of the biometric data of living human. Therefore, human voice is also important to identify the personal correctly. We have proposed the voice encryption techniques based on digital holography [127], [128]. In recorded hologram process, double random phase encryption technique and its improved techniques can be applied. Even after the recording, recorded holograms can be also encrypted by optical encryption.

Various physical information possessed by light waves can be used to raise the level of encryption. This can provide a strong encryption technique for the encryption of biometric information that cannot be rewritten. In order for physical encryption and coding to play an important role in the digital information society, it is necessary to conduct research on the construction of systems that can implement practical use.

XIX. FINAL REMARKS

This Roadmap paper comprises 17 sections to provide an overview of current research in optical security. Each section is prepared by one or two experts in the field. The author of each section describes the progress, potential, vision, and challenges in a particular application of optical security. This includes computational neuromorphic imaging, compressive imaging, deep learning, integrated photonics, metasurfaces, orbital angular momentum, physical unclonable functions, polarization, ptychography, quantum secure direct communication, random number generators, scattering media, speckle, and structured light. As in any overview paper of this nature, it is not possible to describe and represent all the possible applications, approaches, and activities in the broad field of optical security. Thus, we apologize in advance if we have ignored any relevant work. There are many other noteworthy activities by researchers in this field that we were not able to cover in this overview road map article [28], [129], [130], [131], [132], [133].

CONTRIBUTION STATEMENT

Section II: Dong Pan and Gui-Lu Long.
Section III: Shuo Zhu and Edmund Y. Lam.
Section IV: Naveen K. Nishchal.
Section V: Yin Xiao and Wen Chen.
Section VI: Xiaogang Wang.
Section VII: Wenqi He and Xiang Peng.
Section VIII: Inkyu Moon.
Section IX: Yishi Shi and Zhaoke Mi.
Section X: Tian Xia and Zhenwei Xie.
Section XI: Kavan Ahmadi and Artur Carnicer.
Section XII: Pepijn W. H. Pinkse.
Section XIII: Aloke Jana and Patrice Genevet.
Section XIV: Artur Carnicer and Bahram Javidi.
Section XV: Thierry Fournel and Mathieu Hébert.
Section XVI: Guohai Situ and Jingying Guo.
Section XVII: Adrian Stern and Bahram Javidi.
Section XVIII: Osamu Matoba and Yasuhiro Awatsuji.

Bahram Javidi and Artur Carnicer coordinated the organization of the paper and prepared the Abstract, the Introduction, and the Final remarks. All authors reviewed the manuscript.

ACRONYMS

AA: Adversarial Attacks.
CGH: Computer-Generated Hologram.
CNI: Computational Neuromorphic Imaging.
CNN: Convolutional Neural Network.
CPA: Chosen-Plaintext Attack (CPA).
CVB: Cylindrical vector beams.
DH: Diffie-Hellman.
CI: Compressive Imaging.
DL: Deep Learning.
DM: Disordered Metasurface.
DMD: Digital Micromirror Device.
DNN: Deep Neural Network.
DOE: Diffractive Optical Elements.
DoF: Degrees of Freedom.
DRPE: Double Random Phase Encoding.
HDD: Hard Disc Drive.
IWD: Input Wavefront Distribution.

KPA: Known-Plaintext attack.
LCD: Liquid Crystal Device.
MIHNet: Multi-dimension Information Integration using Highway Network.
MS: Metasurface.
NPE: Non-mechanical Ptychography Encoding.
OAM: Orbital Angular Momentum.
PFS: Perfect Forward Secrecy.
PIC: Photonic Integrated Circuits.
PLA: Polylactic Acid:]
PQR: Phase Rapid Response Codes.
PUF: Physical Unclonable Function.
QSDC: Quantum Secure Direct Communication.
SAM: Spin Angular Momentum.
SBR: Signal-to-Background Ratio.
SSD: Solid-State Drive.
SLM: Spatial Light Modulator.
SPDC: Spontaneous Parametric Down-conversion.
SPI: Single-pixel imaging.
TC: Topological Charge.
TRNG: True Random Number Generator.
TRRNG: True Repeatable Random Number Generators.
UEK: Unclonable Equivalent Key.
VBA: Variable Beam Attenuator.
VE: Visual Encryption.
WS: Wavefront Shaping.

DECLARATION OF COMPETING INTERESTS

The authors declare no competing interests.

REFERENCES

[1] J. L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.*, vol. 33, no. 6, pp. 1752–1756, Jun. 1994.

[2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, 1995.

[3] B. L. Volodin, B. Kippelen, K. Meerholz, B. Javidi, and N. Peyghambarian, "A polymeric optical pattern-recognition system for security verification," *Nature*, vol. 383, no. 6595, pp. 58–60, Sep. 1996.

[4] B. Javidi, "Fully phase encoded key and biometrics for security verification," *Opt. Eng.*, vol. 36, no. 3, pp. 935–942, Mar. 1997.

[5] B. Javidi and E. Ahouzi, "Optical security system using Fourier plane phase encoding," *Appl. Opt.*, vol. 37, pp. 6247–6255, Apr. 1998.

[6] B. Javidi, "Securing information with optical technologies," *Phys. Today*, vol. 50, no. 3, pp. 27–32, Mar. 1997.

[7] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Opt. Lett.*, vol. 24, no. 11, pp. 762–764, 1999.

[8] O. Matoba and B. Javidi, "Encrypted optical storage with wavelength key and random codes," *Appl. Opt.*, vol. 38, no. 32, pp. 6785–6790, 1999.

[9] O. Matoba and B. Javidi, "Encrypted optical memory systems based on multidimensional keys for secure data storage and communications," *IEEE Circuits Devices Mag.*, vol. 16, no. 5, pp. 8–15, May 2000.

[10] T. Nomura and B. Javidi, "Information security using digital holography," *Opt. Lett.*, vol. 25, no. 1, pp. 28–30, 2000.

[11] T. Nomura, "Polarization encoding for optical security systems," *Opt. Eng.*, vol. 39, no. 9, pp. 2439–2443, Sep. 2000.

[12] T. Nomura and B. Javidi, "Optical encryption system using a binary key code," *Appl. Opt.*, vol. 39, pp. 4783–4787, Mar. 2000.

[13] E. Tajahuerce and B. Javidi, "Encrypting three dimensional information with digital holography," *Appl. Opt.*, vol. 39, no. 35, pp. 6595–6601, 2000.

[14] E. Tajahuerce, J. Lancis, B. Javidi, and P. Andrés, "Optical security and encryption with totally incoherent light," *Opt. Lett.*, vol. 26, no. 10, pp. 678–681, 2001.

[15] O. Matoba and B. Javidi, "Optical retrieval of encrypted digital holograms for secure real-time display," *Opt. Lett.*, vol. 27, no. 5, pp. 321–323, 2002.

[16] O. Matoba and B. Javidi, "Secure three-dimensional data transmission and display," *Appl. Opt.*, vol. 43, no. 11, pp. 2285–2291, 2004.

[17] S. Kishk and B. Javidi, "Distortion tolerant image recognition receiver by use of a multiple hypothesis method," *Appl. Opt.*, vol. 41, pp. 2149–2157, Feb. 2002.

[18] S. Kishk and B. Javidi, "3D object watermarking by a 3D hidden object," *Opt. Exp.*, vol. 11, no. 8, pp. 874–888, 2003.

[19] B. Javidi, "Real-time remote identification and verification of objects using optical ID tags," *Opt. Eng.*, vol. 42, no. 8, p. 2346, 2003.

[20] G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 3, Feb. 2002, Art. no. 032302.

[21] K. Wen, F.-G. Deng, and G. Lu Long, "Reusable vernam cipher with quantum media," 2007, *arXiv:0711.1632*.

[22] C. H. Bennett, G. Brassard, and S. Breidbart, "Quantum cryptography II: How to re-use a one-time pad safely even if P=NP," *Nat. Comput.*, vol. 13, pp. 453–458, Oct. 2014.

[23] F.-G. Deng and G. L. Long, "Repeatable classical one-time-pad cryptosystem with quantum mechanics," 2019, *arXiv:1902.04218*.

[24] D. Pan, G.-L. Long, L. Yin, Y.-B. Sheng, D. Ruan, S. X. Ng, J. Lu, and L. Hanzo, "The evolution of quantum secure direct communication: On the road to the Qinternet," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 3, pp. 1898–1949, Feb. 2024.

[25] D. Pan, X.-T. Song, and G.-L. Long, "Free-space quantum secure direct communication: Basics, progress, and outlook," *Adv. Devices Instrum.*, vol. 4, Jan. 2023, Art. no. 0004.

[26] D. Pan, Y.-C. Liu, P. Niu, H. Zhang, F. Zhang, M. Wang, X.-T. Song, X. Chen, C. Zheng, and G.-L. Long, "Simultaneous transmission of information and key exchange using the same photonic quantum states," *Sci. Adv.*, vol. 11, no. 8, Feb. 2025, Art. no. eadt4627.

[27] Y.-C. Liu, Y.-B. Cheng, X.-B. Pan, Z.-Z. Sun, D. Pan, and G.-L. Long, "Quantum integrated sensing and communication via entanglement," *Phys. Rev. Appl.*, vol. 22, no. 3, Sep. 2024, Art. no. 034051.

[28] B. Javidi et al., "Roadmap on optical security," *J. Opt.*, vol. 18, no. 8, 2016, Art. no. 083001.

[29] G. Gallego, T. Delbrück, G. Orchard, C. Bartolozzi, B. Taba, A. Censi, S. Leutenegger, A. J. Davison, J. Conradt, K. Daniilidis, and D. Scaramuzza, "Event-based vision: A survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 44, no. 1, pp. 154–180, Jan. 2022.

[30] S. Zhu, C. Wang, H. Liu, P. Zhang, and E. Y. Lam, "Computational neuromorphic imaging: Principles and applications," *Proc. SPIE*, vol. 12857, pp. 4–10, Mar. 2024.

[31] S. Zhu, C. Wang, J. Huang, P. Zhang, J. Han, and E. Y. Lam, "Neuromorphic encryption: Combining speckle correlography and event data for enhanced security," *Adv. Photon. Nexus*, vol. 3, no. 5, Jul. 2024, Art. no. 056002.

[32] P. Zhang, S. Zhu, and E. Y. Lam, "Event encryption: Rethinking privacy exposure for neuromorphic imaging," *Neuromorph. Comput. Eng.*, vol. 4, Jun. 2024, Art. no. 014002.

[33] S. Zhu, Z. Ge, C. Wang, J. Han, and E. Y. Lam, "Efficient non-line-of-sight tracking with computational neuromorphic imaging," *Opt. Lett.*, vol. 49, no. 13, pp. 3584–3587, 2024.

[34] N. K. Nishchal, *Optical Cryptosystems*. Bristol, U.K.: IOP Publishing, 2019.

[35] X. Li, T.-H. Lan, C.-H. Tien, and M. Gu, "Three-dimensional orientation-unlimited polarization encryption by a single optically configured vectorial beam," *Nature Commun.*, vol. 3, no. 1, Aug. 2012, Art. no. 998.

[36] A. Shikder, S. K. Rao, P. Kumar, and N. K. Nishchal, "Binary image encryption with a QR code-encoded optical beam having an array of vortices," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 41, no. 3, pp. A73–A82, 2024.

[37] P. Kumar, N. K. Nishchal, and A. AlFalou, "Controllable optical vortex array for image encoding," *IEEE Photon. Technol. Lett.*, vol. 34, no. 10, pp. 521–524, May 15, 2022.

[38] S. K. Rao and N. K. Nishchal, "Optical asymmetric cryptosystem for multiple image encryption through vector field encoding," *Appl. Phys. B, Lasers Opt.*, vol. 129, no. 11, Nov. 2023, Art. no. 170.

[39] M. Baliyan and N. K. Nishchal, "Optical cryptography with C-point vector beams," *Opt. Lasers Eng.*, vol. 180, Sep. 2024, Art. no. 108337.
[40] Y. Xiao, L. Zhou, and W. Chen, "Wavefront control through multi-layer scattering media using single-pixel detector for high-PSNR optical transmission," *Opt. Lasers Eng.*, vol. 139, Apr. 2021, Art. no. 106453.
[41] Y. Xiao and W. Chen, "High-fidelity optical transmission around the corner," *IEEE Photon. Technol. Lett.*, vol. 33, no. 1, pp. 3–6, Jan. 15, 2021.
[42] Y. Xiao, L. Zhou, and W. Chen, "High-fidelity ghost diffraction and transmission in free space through scattering media," *Appl. Phys. Lett.*, vol. 118, no. 10, Mar. 2021, Art. no. 104001.
[43] Y. Xiao, L. Zhou, Z. Pan, Y. Cao, M. Yang, and W. Chen, "Analog ghost hidden in 2D random binary patterns for free-space optical data transmission," *Opt. Lasers Eng.*, vol. 150, Mar. 2022, Art. no. 106880.
[44] Y. Xiao, L. Zhou, Z. Pan, Y. Cao, and W. Chen, "Physically-enhanced ghost encoding," *Opt. Lett.*, vol. 47, no. 2, pp. 433–436, 2022.
[45] Y. Xiao, L. Zhou, Z. Pan, Y. Cao, and W. Chen, "Physically-secured high-fidelity free-space optical data transmission through scattering media using dynamic scaling factors," *Opt. Exp.*, vol. 30, no. 5, pp. 8186–8198, 2022.
[46] Y. Cao, Y. Xiao, and W. Chen, "Securing 2D information carriers over dynamic and turbulent media in a free-space optical channel," *Opt. Lett.*, vol. 48, no. 13, pp. 3491–3494, 2023.
[47] Y. Cao, Y. Xiao, Z. Pan, L. Zhou, and W. Chen, "Physically-secured ghost diffraction and transmission," *IEEE Photon. Technol. Lett.*, vol. 34, no. 22, pp. 1238–1241, Nov. 14, 2022.
[48] X. Wang, W. Wang, H. Wei, B. Xu, and C. Dai, "Holographic and speckle encryption using deep learning," *Opt. Lett.*, vol. 46, no. 23, pp. 5794–5797, 2021.
[49] X. Wang, H. Wei, M. Jin, B. Xu, and J. Chen, "Experimental optical encryption based on random mask encoding and deep learning," *Opt. Exp.*, vol. 30, no. 7, pp. 11165–11173, 2022.
[50] S. Lin, X. Wang, A. Zhu, J. Xue, and B. Xu, "Steganographic optical image encryption based on single-pixel imaging and an untrained neural network," *Opt. Exp.*, vol. 30, no. 20, pp. 36144–36154, 2022.
[51] L. Zhang, S. Lin, Q. Zhou, J. Xue, B. Xu, and X. Wang, "Speckle-based optical encryption with complex-amplitude coding and deep learning," *Opt. Exp.*, vol. 31, no. 21, pp. 35293–35304, 2023.
[52] Q. Zhou, X. Wang, M. Jin, L. Zhang, and B. Xu, "Optical image encryption based on two-channel detection and deep learning," *Opt. Lasers Eng.*, vol. 162, Mar. 2023, Art. no. 107415.
[53] J. Xue, X. Wang, Q. Zhou, L. Zhang, and M. Yao, "Deep-learning-assisted optical steganographic encryption via ghost encoding and binary hologram," *Opt. Lasers Eng.*, vol. 172, Jan. 2024, Art. no. 107891.
[54] X. Wang, Q. Zhou, L. Zhang, J. Xue, B. Xu, X. Yu, S. Wang, and Z. Zhang, "Computational imaging encryption with a steganographic and holographic authentication strategy," *Laser Photon. Rev.*, vol. 18, no. 6, Jun. 2024, Art. no. 2300820.
[55] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Hoboken, NJ, USA: Wiley, 2000.
[56] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.
[57] Z. Chen, J. Chen, J. Chen, J. Cai, T. Huang, D. Lu, X. Peng, and W. He, "Highly-secure scattering-media-based key storage," *Opt. Lasers Eng.*, vol. 184, Jan. 2025, Art. no. 108613.
[58] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," *Adv. Opt. Photon.*, vol. 6, no. 2, pp. 120–155, 2014.
[59] B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Opt. Lett.*, vol. 28, no. 4, pp. 269–271, 2003.
[60] M. Stamp, *Information Security: Principles and Practice*. Hoboken, NJ, USA: Wiley, 2011.
[61] Y. Kim, M. Sim, and I. Moon, "Secure storage and retrieval schemes for multiple encrypted digital holograms with orthogonal phase encoding multiplexing," *Opt. Exp.*, vol. 27, no. 16, pp. 22147–22160, 2019.
[62] I. Moon, Y. Kim, S. Gholami, and O. Jeong, "Double random phase encoding schemes with perfect forward secrecy for robust image cryptography," *OSA Continuum*, vol. 4, no. 8, pp. 2245–2259, 2021.
[63] Y.-S. Shi and X.-B. Yang, "Invisible visual cryptography," *Chin. Phys. Lett.*, vol. 34, no. 11, Nov. 2017, Art. no. 114204.
[64] T. Yu, D.-Y. Yang, R. Ma, Y.-P. Zhu, and Y.-S. Shi, "Enhanced-visual-cryptography-based optical information hiding system," *Acta Phys. Sinica*, vol. 69, no. 14, 2020, Art. no. 144202.
[65] W. Lv, X. Sun, D. Yang, Y. Zhu, Y. Tao, and Y. Shi, "Optical multiple information hiding via azimuth multiplexing," *Opt. Lasers Eng.*, vol. 141, Jun. 2021, Art. no. 106574.
[66] X. Sun, S. Zhang, R. Ma, Y. Tao, Y. Zhu, D. Yang, and Y. Shi, "Natural speckle-based watermarking with random-like illuminated decoding," *Opt. Exp.*, vol. 28, no. 21, pp. 31832–31843, 2020.
[67] Z. Mi, Y. Zhu, Y. Zhu, T. Zhang, Z. Huang, F. Wu, C. Ke, S. Ge, L. Rong, and Y. Shi, "Optical information hiding for different surface images," *Appl. Opt.*, vol. 63, no. 9, pp. 2324–2330, 2024.
[68] Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang, and H. Li, "Optical image encryption via ptychography," *Opt. Lett.*, vol. 38, no. 9, pp. 1425–1427, 2013.
[69] J. Zhang, D. Yang, R. Ma, and Y. Shi, "Multi-image and color image encryption via multi-slice ptychographic encoding," *Opt. Commun.*, vol. 485, Apr. 2021, Art. no. 126762.
[70] H. Ren, G. Briere, X. Fang, P. Ni, R. Sawant, S. Héron, S. Chenot, S. Vézian, B. Damilano, V. Brändli, S. A. Maier, and P. Genevet, "Metasurface orbital angular momentum holography," *Nature Commun.*, vol. 10, no. 1, Jul. 2019, Art. no. 2986.
[71] X. Fang, H. Ren, and M. Gu, "Orbital angular momentum holography for high-security encryption," *Nature Photon.*, vol. 14, no. 2, pp. 102–108, Feb. 2020.
[72] T. Xia, Z. Xie, and X. Yuan, "Ellipse-like orbital angular momentum multiplexed holography and efficient decryption utilizing a composite ellipse-like lens," *Laser Photon. Rev.*, vol. 18, no. 2, Feb. 2024, Art. no. 2300759.
[73] H. Yang, P. He, K. Ou, Y. Hu, Y. Jiang, X. Ou, H. Jia, Z. Xie, X. Yuan, and H. Duan, "Angular momentum holography via a minimalist metasurface for optical nested encryption," *Light, Sci. Appl.*, vol. 12, no. 1, Mar. 2023, Art. no. 79.
[74] C. Zhou, W. Liang, Z. Xie, J. Ma, H. Yang, X. Yang, Y. Hu, H. Duan, and X. Yuan, "Optical vectorial-mode parity Hall effect: A case study with cylindrical vector beams," *Nature Commun.*, vol. 15, no. 1, May 2024, Art. no. 4022.
[75] Z. Shi, Z. Wan, Z. Zhan, K. Liu, Q. Liu, and X. Fu, "Super-resolution orbital angular momentum holography," *Nature Commun.*, vol. 14, no. 1, Apr. 2023, Art. no. 1869.
[76] A. Carnicer, I. Juvells, D. Maluenda, R. Martínez-Herrero, and P. M. Mejías, "On the longitudinal component of paraxial fields," *Eur. J. Phys.*, vol. 33, no. 5, pp. 1235–1247, Sep. 2012.
[77] A. Carnicer, I. Juvells, B. Javidi, and R. Martínez-Herrero, "Optical encryption in the longitudinal domain of focused fields," *Opt. Exp.*, vol. 24, no. 7, pp. 6793–6801, 2016.
[78] M. Naor and A. Shamir, "Visual cryptography," in *Proc. Adv. Cryptol. Workshop Theory Appl. Cryptograph. Techn.*, 1995, pp. 1–12.
[79] F. Zhang, Y. Guo, M. Pu, L. Chen, M. Xu, M. Liao, L. Li, X. Li, X. Ma, and X. Luo, "Meta-optics empowered vector visual cryptography for high security and rapid decryption," *Nature Commun.*, vol. 14, no. 1, Apr. 2023, Art. no. 1946.
[80] K. Ahmadi and A. Carnicer, "Optical visual encryption using focused beams and convolutional neural networks," *Opt. Lasers Eng.*, vol. 161, Feb. 2023, Art. no. 107321.
[81] O. Matoba, T. Nomura, E. Pérez–Cabré, M. S. Millán, and B. Javidi, "Optical techniques for information security," *Proc. IEEE*, vol. 97, no. 6, pp. 1128–1148, 2009.
[82] F. Silvestri, G. Castro do Amaral, B. Perlingeiro Correa, D. Bakker, L. Feenstra, E. Di Iorio, and I. Ferrario, "Satellite license plate: System modelling and first ground-to-ground tests," in *Proc. 2nd NEO Debris Detection Conf.*, 2023, p. 92.
[83] L. van der Hoeven, M. C. Velsink, D. Stellinga, and P. W. H. Pinkse, "Ring resonator networks as physical unclonable keys," in *Proc. Optica Adv. Photon. Congr.*, 2022, pp. 1–2.
[84] X. Ji, S. Roberts, M. Corato-Zanarella, and M. Lipson, "Methods to achieve ultra-high quality factor silicon nitride resonators," *APL Photon.*, vol. 6, no. 7, Jul. 2021, Art. no. 071101.
[85] K. Van Acoleyen, D. C. O'Brien, F. Payne, W. Bogaerts, and R. Baets, "Optical retroreflective marker fabricated on silicon-on-insulator," *IEEE Photon. J.*, vol. 3, no. 5, pp. 789–798, Oct. 2011.
[86] R. M. MacFarlane and R. M. Shelby, "Homogeneous line broadening of optical transitions of ions and molecules in glasses," *J. Lumin.*, vol. 36, nos. 4–5, pp. 179–207, Jan. 1987.

[87] R. Faber, K. Zhang, and A. Zoeller, "Design and manufacturing of WDM narrow-band interference filters," *Proc. SPIE*, vol. 4094, pp. 58–64, Oct. 2000.

[88] G. A. Rakuljic and V. Leyva, "Volume holographic narrow-band optical filter," *Opt. Lett.*, vol. 18, no. 6, pp. 459–461, 1993.

[89] L. Huang, R. Jin, C. Zhou, G. Li, L. Xu, A. Overvig, F. Deng, X. Chen, W. Lu, A. Alù, and A. E. Miroshnichenko, "Ultrahigh-Q guided mode resonances in an all-dielectric metasurface," *Nature Commun.*, vol. 14, no. 1, Jun. 2023, Art. no. 3433.

[90] H. Yang, K. Ou, H. Wan, Y. Hu, Z. Wei, H. Jia, X. Cheng, N. Liu, and H. Duan, "Metasurface-empowered optical cryptography," *Mater. Today*, vol. 67, pp. 424–445, Jul. 2023.

[91] J. Ji, C. Chen, J. Sun, X. Ye, Z. Wang, J. Li, J. Wang, W. Song, C. Huang, K. Qiu, S. Zhu, and T. Li, "High-dimensional Poincaré beams generated through cascaded metasurfaces for high-security optical encryption," *PhotoniX*, vol. 5, no. 1, Apr. 2024, Art. no. 13.

[92] Z. Yu, H. Li, W. Zhao, P.-S. Huang, Y.-T. Lin, J. Yao, W. Li, Q. Zhao, P. C. Wu, B. Li, P. Genevet, Q. Song, and P. Lai, "High-security learning-based optical encryption assisted by disordered metasurface," *Nature Commun.*, vol. 15, no. 1, Mar. 2024.

[93] L. Li, Z. Liu, X. Ren, S. Wang, V.-C. Su, M.-K. Chen, C. H. Chu, H. Y. Kuo, B. Liu, W. Zang, G. Guo, L. Zhang, Z. Wang, S. Zhu, and D. P. Tsai, "Metalens-array–based high-dimensional and multiphoton quantum source," *Science*, vol. 368, no. 6498, pp. 1487–1490, Jun. 2020.

[94] K. Wang, J. G. Titchener, S. S. Kruk, L. Xu, H.-P. Chung, M. Parry, I. I. Kravchenko, Y.-H. Chen, A. S. Solntsev, Y. S. Kivshar, D. N. Neshev, and A. A. Sukhorukov, "Quantum metasurface for multiphoton interference and state reconstruction," *Science*, vol. 361, no. 6407, pp. 1104–1108, Sep. 2018.

[95] Z. Gao, Z. Su, Q. Song, P. Genevet, and K. E. Dorfman, "Metasurface for complete measurement of polarization bell state," *Nanophotonics*, vol. 12, no. 3, pp. 569–577, Feb. 2023.

[96] A. Carnicer and B. Javidi, "Optical security and authentication using nanoscale and thin-film structures," *Adv. Opt. Photon.*, vol. 9, no. 2, pp. 218–256, 2017.

[97] A. Carnicer, A. Hassanfiroozi, P. Latorre-Carmona, Y.-P. Huang, and B. Javidi, "Security authentication using phase-encoded nanoparticle structures and polarized light," *Opt. Lett.*, vol. 40, no. 2, pp. 135–138, 2015.

[98] A. Carnicer, O. Arteaga, E. Pascual, A. Canillas, S. Vallmitjana, B. Javidi, and E. Bertran, "Optical security verification by synthesizing thin films with unique polarimetric signatures," *Opt. Lett.*, vol. 40, no. 22, pp. 5399–5402, 2015.

[99] K. Ahmadi, P. Latorre-Carmona, B. Javidi, and A. Carnicer, "Polarimetric identification of 3D-printed nano particle encoded optical codes," *IEEE Photon. J.*, vol. 12, no. 3, pp. 1–10, Jun. 2020.

[100] A. Markman, A. Carnicer, and B. Javidi, "Security authentication with a three-dimensional optical phase code using random forest classifier," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 33, no. 6, pp. 1160–1165, 2016.

[101] A. Carnicer, O. Arteaga, J. M. Suñé-Negre, and B. Javidi, "Authentication of gold nanoparticle encoded pharmaceutical tablets using polarimetric signatures," *Opt. Lett.*, vol. 41, no. 19, pp. 4507–4510, 2016.

[102] T. Fournel, Y. Boutant, J. A. Benediktsson, B. Javidi, and K. S. Gudmundsson, "Designing a dictionary for true repeatable random number generation," *AIP Conf. Proc.*, vol. 949, no. 1, pp. 91–98, 2007.

[103] J. R. Smith and A. V. Sutherland, "Microstructure based indicia," in *Proc. 2nd Workshop Autom. Identificat. Adv. Technol.*, 1999, pp. 79–83.

[104] M. Hebert, *Optical Models for Material Appearance*. Les Ulis, France: EDP Sciences, 2022.

[105] Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Sci.*, vol. 3, no. 2, pp. 81–91, 2020.

[106] U. Rührmair, C. Hilgers, S. Urban, A. Weiershäuser, E. Dinter, B. Forster, and C. Jirauschek, "Optical PUFs reloaded," *Cryptol. ePrint Arch.*, vol. 2013, pp. 1–18, Mar. 2013.

[107] R. Hui, F. Chen, M. Li, and J. Zhang, "Non-linear optical scattering PUF: Enhancing security against modeling attacks for authentication systems," *Opt. Exp.*, vol. 31, no. 24, pp. 40646–40657, 2023.

[108] A. Albright, B. Gelfand, and M. Dixon, "Learnability of optical physical unclonable functions through the lens of learning with errors," *IEEE Trans. Inf. Forensics Security*, vol. 20, pp. 886–897, 2025.

[109] Y. Boutant, T. Fournel, and J. M. Becker, "Method for extracting random signatures from a material element and method for generating a decomposition base to implement the extraction method," U.S. Patent 8 989 500 B2, 2005.

[110] K. Wang, J. Shi, W. Lai, Q. He, J. Xu, Z. Ni, X. Liu, X. Pi, and D. Yang, "All-silicon multidimensionally-encoded optical physical unclonable functions for integrated circuit anti-counterfeiting," *Nature Commun.*, vol. 15, no. 1, Apr. 2024, Art. no. 3203.

[111] G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Opt. Lett.*, vol. 29, no. 14, pp. 1584–1586, 2004.

[112] J. A. Rodrigo, T. Alieva, and M. L. Calvo, "Applications of gyrator transform for image processing," *Opt. Commun.*, vol. 278, no. 2, pp. 279–284, Oct. 2007.

[113] P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, "Optical encryption based on computational ghost imaging," *Opt. Lett.*, vol. 35, no. 14, pp. 2391–2393, 2010.

[114] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," *Opt. Exp.*, vol. 15, no. 16, pp. 10253–10265, 2007.

[115] J. Hou and G. Situ, "Image encryption using spatial nonlinear optics," *eLight*, vol. 2, no. 1, pp. 1–18, Dec. 2022.

[116] Y. Meng, Y. Chen, L. Lu, Y. Ding, A. Cusano, J. A. Fan, Q. Hu, K. Wang, Z. Xie, Z. Liu, Y. Yang, Q. Liu, M. Gong, Q. Xiao, S. Sun, M. Zhang, X. Yuan, and X. Ni, "Optical meta-waveguides for integrated photonics and beyond," *Light Sci. Appl.*, vol. 10, no. 1, 2021, Art. no. 235.

[117] S. Wan, K. Qu, Y. Shi, Z. Li, Z. Wang, C. Dai, J. Tang, and Z. Li, "Multidimensional encryption by chip-integrated metasurfaces," *ACS Nano*, vol. 18, no. 28, pp. 18693–18700, Jul. 2024.

[118] C. U. Hail, M. Foley, R. Sokhoyan, L. Michaeli, and H. A. Atwater, "High quality factor metasurfaces for two-dimensional wavefront manipulation," *Nature Commun.*, vol. 14, no. 1, Dec. 2023, Art. no. 8476.

[119] V. Kravets, B. Javidi, and A. Stern, "Optical compressive imaging for defending deep learning from adversarial attacks," *Opt. Lett.*, vol. 46, pp. 1951–1954, Mar. 2021.

[120] E. C. Marques, N. Maciel, L. Naviner, H. Cai, and J. Yang, "A review of sparse recovery algorithms," *IEEE Access*, vol. 7, pp. 1300–1322, 2019.

[121] Y. Cheng, B. Zhou, Y. Chen, Y.-C. Chen, X. Ji, and W. Xu, "Evaluating compressive sensing on the security of computer vision systems," *ACM Trans. Sensor Netw.*, vol. 20, no. 3, pp. 1–24, May 2024.

[122] A. Stern, *Optical Compressive Imaging*. Boca Raton, FL, USA: CRC Press, 2017.

[123] A. Stern, S. Kandalaft, O. Lowte, and V. Kravets, "A comparison of deep learning-based compressive imaging methods from a practitioner's perspective," *Proc. SPIE*, vol. 13036, Jun. 2024, Art. no. 1303603.

[124] V. Kravets, B. Javidi, and A. Stern, "Compressive imaging for thwarting adversarial attacks on 3D point cloud classifiers," *Opt. Exp.*, vol. 29, no. 26, pp. 42726–42737, 2021.

[125] X. Tan, O. Matoba, T. Shimura, K. Kuroda, and B. Javidi, "Secure optical storage that uses fully phase encryption," *Appl. Opt.*, vol. 39, no. 35, pp. 6689–6694, 2000.

[126] O. Matoba and B. Javidi, "Secure holographic memory by double random polarization encryption," *Appl. Opt.*, vol. 43, no. 14, pp. 2915–2919, 2004.

[127] S. K. Rajput and O. Matoba, "Optical voice encryption based on digital holography," *Opt. Lett.*, vol. 42, no. 22, pp. 4619–4622, 2017.

[128] S. K. Rajput, S. Notte, T. Inoue, R. Yamaguchi, R. Todo, Y. Kumon, K. Nishio, O. Matoba, and Y. Awatsuji, "Optical voice security scheme for anticounterfeiting," *Opt. Lasers Eng.*, vol. 173, Feb. 2024, Art. no. 107892.

[129] X. Zhan, X. Chang, D. Li, R. Yan, Y. Zhang, and L. Bian, "Scattering-induced entropy boost for highly-compressed optical sensing and encryption," 2022, *arXiv:2301.06084*.

[130] Q. Zhao, H. Li, Z. Yu, C. M. Woo, T. Zhong, S. Cheng, Y. Zheng, H. Liu, J. Tian, and P. Lai, "Speckle-based optical cryptosystem and its application for human face recognition via deep learning," *Adv. Sci.*, vol. 9, no. 25, Sep. 2022, Art. no. 2202407.

[131] L. Bian, X. Chang, S. Jiang, L. Yang, X. Zhan, S. Liu, D. Li, R. Yan, Z. Gao, and J. Zhang, "Large-scale scattering-augmented optical encryption," *Nature Commun.*, vol. 15, no. 1, Nov. 2024, Art. no. 9807.

[132] H. Singh, "Cryptanalysis of a double-image symmetric optical cryptosystem utilizing devil's vortex Fresnel array and the linear canonical transform," *J. Modern Opt.*, vol. 71, nos. 19–21, pp. 700–715, Dec. 2024.

[133] H. Singh, "Double-phase image encryption using interference concept, devil's fractional vortex Fresnel lens phase masks, and the gyrator transform," *Optik*, vol. 327, Aug. 2025, Art. no. 172289.

BAHRAM JAVIDI (Fellow, IEEE) received the M.S. and Ph.D. degrees from The Pennsylvania State University. He is currently the Board of Trustees Distinguished Professor and the SNET Endowed Chair of the University of Connecticut. He has more than 1200 publications, including more than 540 peer-reviewed journal articles, and more than 520 conference proceedings. He is a strong believer in international scientific exchange and collaboration, and has co-authored publications with more than 300 different students, scientists, and engineers from around the world. His research interests include a broad range of transformative imaging approaches using optics and photonics, and he has made seminal contributions to passive and active multi-dimensional imaging from nano to micro and macro scales. His research has been recognized by honors and awards, including The Optica Society Emmett Leith Medal, in 2021; the Optica C. E. K. Mees Medal, in 2019; the IEEE Photonics Society William Streifer Scientific Achievement Award, in 2019; the Optica Joseph Fraunhofer Award, in 2018; and the European Physical Society Prize for Applied Aspects of Quantum Electronics and Optics, in 2015. He was awarded the IEEE Donald G. Fink Paper Prize, in 2008; the John Simon Guggenheim Foundation Fellow Award, in 2008; the Alexander von Humboldt Foundation Prize, in 2007; the SPIE Technology Achievement Award, in 2008; and the SPIE Dennis Gabor Award in Diffractive Wave Technologies, in 2005.

ARTUR CARNICER was born in Barcelona, in 1965. He received the Licentiate and Ph.D. degrees in physics from Universitat de Barcelona (UB), in 1989 and 1993, respectively. He is currently a Full Professor of optics with the Applied Physics Department, UB. His research interests include highly focused electromagnetic fields, optics for information security, and 3D integral imaging. He is a Senior Member of Optica and SPIE, and a member of the Catalan Physical Society and the Spanish Optical Society (SedOPTICA).

KAVAN AHMADI received the B.S. degree in physics and the M.S. degree in electro-optical engineering-laser, in 2009 and 2013, respectively, and the Ph.D. degree (cum laude) in physics from Universitat de Barcelona (UB), Spain, in 2023. In 2019, he was awarded a Predoctoral Scholarship at UB, where he was a Personal Investigator and contributed to a research and development project with the Wavefront Engineering Group, Department of Applied Physics, UB. He has contributed to cutting-edge research in wavefront engineering, Fourier optics, digital holography, and applications of machine learning for optics. Currently, he is a Substitute Professor with the Department of Applied Physics, UB, where he mentors students in the Optics Laboratory. He has authored and co-authored several peer-reviewed book chapters, journal articles, and conference papers, showcasing advancements in optical encryption and focused electromagnetic field estimation. His research interests include optical encoding, computational imaging, and interdisciplinary applications of machine learning in optics.

YASUHIRO AWATSUJI received the B.Eng., M.Eng., and D.Eng. degrees in applied physics from Osaka University, in 1992, 1994, and 1997, respectively. He was a Research Associate with the Division of Information and Production Science, Kyoto Institute of Technology, from 1997 to 2005. He was an Associate Professor with the Department of Electronics and Information Science, Kyoto Institute of Technology, in 2005. Also, he was a Researcher with the Precursory Research for Embryonic Science and Technology (PRESTO), Japan Science and Technology Agency, from 2005 to 2009. He was an Associate Professor with the Division of Electronics, Graduate School of Science and Technology, from 2005 to 2014. He has been a Professor with the Division of Electronics, Graduate School of Science and Technology, Kyoto Institute of Technology, since 2014. His research interest includes information optics with emphasis on holography. He is also interested in three-dimensional imaging, three-dimensional measurement, quantitative phase imaging, microscopy, visualization of invisible objects, high-speed imaging, ultrafast imaging, and optical information processing. He is a Senior Member of Optica and the International Society for Optics and Photonics (SPIE). Also, he is a member of Japan Society of Applied Physics and the Optical Society of Japan.

WEN CHEN (Senior Member, IEEE) received the Ph.D. degree from the National University of Singapore. He conducted extensive research as a Research Associate, in 2010, and as a Research Fellow, from 2011 to 2015, with the National University of Singapore. He was a Visiting Scholar with Harvard University, in 2013. He joined The Hong Kong Polytechnic University as an Assistant Professor, in December 2015. Since July 2021, he has been an Associate Professor with the Department of Electrical and Electronic Engineering and Photonics Research Institute, The Hong Kong Polytechnic University. He has authored or co-authored more than 160 international journal and conference papers on his field of specialization. He is listed among the top 2% of the world's most highly cited scientists by Stanford University. His research interests include computational optics, information photonics, optical imaging, optical encoding, optical sensing, free-space optical data transmission, deep learning in optics, and photonics. He serves as an Associate Editor for several academic journals *Optics and Lasers in Engineering* and *Optics Express*.

THIERRY FOURNEL received the Licentiate degree in mathematics and the Ph.D. degree in image processing and analysis from the University of Saint-Etienne (UJM), in 1985 and 1991, respectively. Currently, he is a Full Professor with UJM, teaching applied information theory and deep learning principles in the local branch of Institut d'Optique Graduate School. His research work focuses on visual cryptography and paper document authentication, both taught in the optics-image-vision-multimedia master's program. His research interests include image formation and image spaces, visual interpretability, and cryptographic primitives. He elaborated original concepts in image-based security as a True Repeatable Random Generator, in 2007, secret image and color sharing, in 2012, and Cauchy-Glass patterns for visual authentication, in 2018. He heads the Image Science and Computer Vision team within the Laboratoire Hubert Curien (UMR 5516).

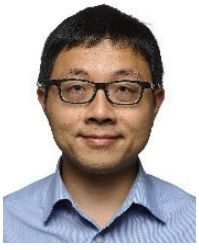
PATRICE GENEVET received the Ph.D. degree from Université d'Azur, France, in 2009, on localized spatial solitons in semiconductor lasers and amplifiers. He is currently a Professor of physics with Colorado School of Mines. From 2009 to 2014, he spent five years as a Research Fellow with the Capasso Group (SEAS, Harvard University) in collaboration with Prof. M. O. Scully (Texas A&M University), where he developed the concept of Metasurfaces. In 2014, he obtained the position of a Senior Research Scientist with A*STAR, Singapore. In 2015, he joined CNRS as a Chargé de Recherche. He receives several awards, including the ERC Starting Grant 2015, the 2017 Aim-Cotton Price from the French Physical Society, the 2019 ERC Proof of Concept, and the 2021 Fabry-De Gramont Price from the French Optical Society. Since 2018, he has been named annually among the Top 1% Highly Cited Researchers by Clarivate. He owns eight patents, more than 125 publications, an H factor of 56, and more than 29300 citations (Google Scholar). His research activities concern the development of optical metamaterials, passive and active metasurfaces, and their applications and integration in optoelectronic devices.

JINGYING GUO received the B.S. degree from Shandong University, China, in 2015, and the Ph.D. degree from Shanghai Institute of Optics and Fine Mechanics, Chinese Academy of Sciences, China, in 2021. From 2021 to 2023, he was a Postdoctoral Researcher with Shanghai Institute of Optics and Fine Mechanics, Chinese Academy of Sciences. Since 2024, he has been an Associate Researcher with Shanghai Institute of Optics and Fine Mechanics, Chinese Academy of Sciences. His research interests include metasurfaces, computational imaging, and deep learning.

WENQI HE was born in Hubei, China, in 1984. He received the B.S. degree in optoelectronic information engineering from South China Normal University, in 2007, and the M.S. degree in physical electronics and the Ph.D. degree in optical engineering from Shenzhen University, in 2010 and 2012, respectively. He has been an Associate Professor with the College of Physics and Optical Engineering, Shenzhen University, since 2019. He has authored more than 60 articles in peer-reviewed professional journals and more than ten inventions. His research interests include computational optical imaging, optical encryption, and computer vision.

MATHIEU HÉBERT received the Ph.D. degree from École Polytechnique Fédérale de Lausanne (EPFL), in 2006. He is currently a Full Professor with the Institut d'Optique-Graduate School, Laboratoire Hubert Curien, CNRS, and the University Jean Monnet of Saint-Etienne. Since 2019, he has been the Director of the research grouping APPAMAT' of CNRS on material appearance sciences. His research activity is focused on optical models for appearance in various application domains, such as printing, manufacturing, and health and beauty.

ALOKE JANA was born in Kolkata, in 1999. He received the B.S. and M.S. degrees from Indian Institute of Science Education and Research (IISER) Kolkata, India. Currently, he is pursuing the Ph.D. degree with the Department of Physics, Colorado School of Mines, USA. Prior to this, he was a Visiting Research Student with the Physical Research Laboratory (PRL), India. His research interests include topological photonics, metamaterials, and spin-orbit interactions of light.



EDMUND Y. LAM (Fellow, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering from Stanford University. He was a Visiting Associate Professor with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology. He is currently a Professor of electrical and electronic engineering and the Associate Dean of the Graduate School, The University of Hong Kong, Hong Kong. He also serves as the Computer Engineering Program Director and the Research Program Coordinator of the AI Chip Center for Emerging Smart Systems. His research interests include computational imaging algorithms, systems, and applications. He is a fellow of Optica, SPIE, IS&T, IOP, and HKIE, and a Founding Member of Hong Kong Young Academy of Sciences.

GUI-LU LONG (Member, IEEE) received the B.S. degree from Shandong University, in 1982, and the Ph.D. degree from Tsinghua University, in 1987. Since then, he has been with Tsinghua University. From 1989 to 1993, he was a Research Fellow with the University of Sussex, U.K. He is currently a Professor with Tsinghua University. Notably among his various contributions, he proposed the theory of quantum secure direct communications, in 2000, which is one of the three major quantum secure communication theories; constructed a quantum exact search algorithm, sometimes called the Grover-Long algorithm; and established the linear combination unitaries (LCU) paradigm, which is widely used in quantum algorithm designs. He published more than 400 articles in refereed international journals. His research interests include quantum communication and computing, and optical microcavity. He is a fellow of IoP, U.K., and APS, U.S. He served as the President of the Associations of Asian Pacific Physical Societies, from 2017 to 2019, and the Vice-Chair of C13 of IUPAP, from 2015 to 2017.

OSAMU MATOBA (Member, IEEE) received the Ph.D. degree in applied physics from Osaka University, Osaka, Japan, in 1996.

He was a Research Associate with the Institute of Industrial Science, The University of Tokyo, from 1996 to 2002. From 2002 to 2009, he was an Associate Professor with the Department of Computer Science and Systems Engineering, Kobe University. He is currently a Professor with the Center of Optical Scattering Image Science (OaSIS), Kobe University. He has published more than 150 technical articles in major peer-reviewed journals. His research interests include optical sensing, including digital holography, computational imaging, imaging through scattering medium, three-dimensional imaging in neuroscience, and biology. He is a fellow of SPIE and Optica, and a member of the Optical Society of Japan (OSJ) and Japan Society of Applied Physics (JSAP). He received the 2008 IEEE Donald G. Fink Prize Paper Award.

ZHAOKE MI was born in 1999. He received the master's degree from Hebei University of Engineering, in 2024. He is currently a Research Assistant with the Institute of Optoelectronics, University of Chinese Academy of Sciences. He participated in the construction of a microscopic holographic imaging device and measured special optical devices. His main research interests include optical encryption, optical computational imaging, and detection.

INKYU MOON received the B.S. degree in electronics engineering from Sungkyunkwan University, South Korea, in 1996, and the Ph.D. degree in electrical and computer engineering from the University of Connecticut, USA, in 2007. From 2009 to 2017, he was a Faculty Member with the Department of Computer Engineering, Chosun University, South Korea. He joined DGIST, South Korea, in 2017. He is currently a Full Professor with the Department of Robotics and Mechatronics Engineering. With more than 100 publications in journals, conferences, and as invited papers. His research interests include digital holography, biomedical imaging, and optical information processing. He is a Senior Member of Optica.

NAVEEN K. NISHCHAL received the Ph.D. degree in physics from IIT Delhi, in 2005.

He has been a Faculty Member with the Department of Physics, Indian Institute of Technology (IIT) Patna, since 2008. He was with the Instruments Research and Development Establishment, Dehradun, as a Scientist C, from 2004 to 2007. Further, he was with IIT Guwahati as an Assistant Professor with the Physics Department, from 2007 to 2008. He has been a Researcher with Oulu Southern Institute, University of Oulu, Finland. He has authored the book *Optical Cryptosystems* published by IOP Publishing, in 2019. He has authored 107 international journal articles and 275 papers in various conferences. He received the India Top Cited Author Award-2019 as the author of one of the top 1% most-cited papers in physics published throughout by IOP Publishing, U.K., from 2016 to 2018. His research interests include optical information processing, optical cryptography, digital holography and transport of intensity, optical pattern recognition, and structured light. He is a Senior Member of OPTICA and SPIE. He received the Dinabandhu Sahu Memorial Award from Indian Association of Physics Teachers, in 2022. He is an Associate Editor of *Optical Engineering* (SPIE) and *Optics Continuum* (OPTICA).

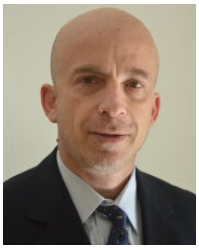
DONG PAN (Member, IEEE) received the B.S. degree from Northwest University, Xi'an, China, in 2016, and the Ph.D. degree from Tsinghua University, Beijing, in 2021. From 2018 to 2019, he was a Visiting Student with the University of Southampton, Southampton, U.K. He is currently an Assistant Research Scientist with Beijing Academy of Quantum Information Sciences. Starting in 2024, he began as a Standing Committee Member of China Materials Library for the Materials and Devices Scientists Committee. His current research interests include quantum communications and quantum networks.

XIANG PENG was born in Tianjin, China, in 1950. He received the B.S., M.S., and Ph.D. degrees in optical engineering from Tianjin University, in 1981, 1984, and 1989, respectively. From 1985 to 1986, he was a Visiting Scholar with the University of Houston, USA. From 1990 to 1992, he was awarded a Fellowship by the Alexander von Humboldt Foundation. Since 1984, he has been with Tianjin University as an Assistant Professor and was an Associate Professor, in 1992, and a Full Professor, in 1998. He joined Shenzhen University, in January 2003, and retired there, in 2021. Currently, he is a Principal Scientist with Anhua Company Ltd., Shenzhen, China. He has more than 200 publications in refereed journals and more than 40 inventions. His current research interests include optical imaging, metrology, and optical security.

PEPIJN W. H. PINKSE (Member, IEEE) was born in 1970. He received the Ph.D. degree in (quantum) optical studies of spin-polarized atomic hydrogen from the University of Amsterdam, in 1997, and the Habilitation degree from TU Munich, in 2008. Thereafter, in Germany, he performed seminal cavity QED experiments with the University of Konstanz and the Max Planck Institute for Quantum Optics (MPQ). Here, he also pioneered new ways of cooling and trapping ultracold molecules in a project he initiated, in 2002. In 2009, he moved to the University of Twente, The Netherlands. Here, he pioneered together with Boris Skoric and Allard Mosk, quantum-secure authentication (QSA), the quantum-secure readout of a multiple scattering key as a so-called Physical Unclonable Function (PUF). He is currently the Chair of the Adaptive Quantum Optics Group and the Director of the Center for Quantum Nanotechnology Twente (QUANT). He is combining ideas from quantum optics with 3D nanofabricated scattering media, multimode fibers, and complex integrated photonic circuits.

YISHI SHI was born in 1981. He is currently the Head of the Optical Engineering Teaching and Research Department, University of Chinese Academy of Sciences, the Director of the Optical Image and Intelligent Vision Laboratory, and a Visiting Researcher with the Institute of Aerospace Information Research, Chinese Academy of Sciences. He mainly engaged in research in the fields of optoelectronic information and artificial intelligence. He has published more than 80 articles as the corresponding author, including 14 top journal articles, with three articles cited more than 100 times. He serves as a Standing Committee Member of the Specialized Committee on Holography and Optical Information of the Chinese Optical Society, a Thematic Expert of the Defense Science and Technology Innovation Special Zone under the Central Military Commission, and a member of the Technical Committee on Optical Measurement Standardization of China. He is a reviewer for more than 20 SCI journals, including American Optical Society series journals, IEEE optical journals, Elsevier optics journals, British Physical Society optical journals, and journals of the series of the Physical Society of China and the Optical Society of China.

GUOHAI SITU received the B.S. degree from Nankai University, in 2001, and the D.S. degree from the Chinese Academy of Sciences, in 2006. He is currently the Director of Shanghai Institute of Laser Technology, and an Adjunct Professor with Shanghai Institute of Optics and Fine Mechanics, Chinese Academy of Sciences. His focus is on imaging through optically thick scattering media, computational ghost imaging, and phase imaging. To date, he has published 100 articles in leading journals. His research interest includes a broad spectrum of deep-learning-based computational optical imaging. He is a fellow of Optica and a Distinguished Young Scholar Recipient (NSFC). He also serves on the Editorial Boards of *Advanced Photonics* and *Advanced Photonics Nexus*.



ADRIAN STERN received the Ph.D. degree in electrical engineering from Ben Gurion University of the Negev, in 2003. Currently, he is a Full Professor with the School of Electrical and Computer Engineering, Ben Gurion University of the Negev. He has held a visiting scholar position with MIT and the University of Connecticut (UConn). He has published more than 225 journal and conference papers, and book chapters. He is the editor of the first book on optical compressive imaging. His current research interests include computational imaging systems, spectral imaging, physics-informed deep learning, and 3D imaging. He has served on the editorial boards of multiple journals and is an elected fellow member of both SPIE and OSA.

XIAOGANG WANG received the B.S., M.S., and Ph.D. degrees from Zhejiang University, in 2001, 2006, and 2013, respectively. He is currently a Professor with Zhejiang University of Science and Technology. From 2014 to 2015, he was a Visiting Scholar with the Department of Electrical and Computer Engineering, National University of Singapore. He has been granted four research funds from the National Natural Science Foundation of China (NSFC). He has published about 100 articles in refereed international journals. His research interests include optical security, computational imaging, and beam propagation. He was selected as a member of the "151 talent Program of Zhejiang Province," in 2015. He was honored with the Second Prize of the Natural Science Award of the Ministry of Education of China (as a Core Member), in 2012.

TIAN XIA is currently a Postdoctoral Researcher with the Institute of Microscale Optoelectronics, Shenzhen University. His research interests include zone plate, beam control, holography, and metasurface.

YIN XIAO received the Ph.D. degree from The Hong Kong Polytechnic University, in 2020. He is currently a Research Assistant Professor with the Department of Electrical and Electronic Engineering, The Hong Kong Polytechnic University. His current research interests include optical imaging, free-space optical data transmission, information photonics, and artificial intelligence in photonics.

XIE ZHENWEI is currently an Associate Professor with the Institute of Microscale Optoelectronics, Shenzhen University. He has made notable advancements in the field of optical angular momentum. He has developed innovative mechanisms for generating, multiplexing, and demultiplexing optical vortices, introduced the novel optical vector mode parity Hall effect, and predicted optical Bloch skyrmions. His research has been featured in prestigious journals, including *Nature Communications*, *Light: Science and Applications*, *Advanced Photonics*, *Applied Physics Reviews*, *ACS Photonics*, *Laser and Photonics Reviews*, *Photonics Research*, *Applied Physics Letters*, and *Optics Letters*. He has published more than 90 SCI articles, garnered 5 053 citations, and holds an H-index of 34. Nine of his articles have received Top Download awards, two have been recognized as ESI Highly Cited Papers, and six have been selected as featured articles or covers. He has won the Second Prize in Shenzhen Natural Science and has led numerous research projects, including those funded by the National Natural Science Foundation, Guangdong Province, Shenzhen Peacock Plan, and key initiatives with Huawei and other major organizations. He is also listed among the world's Top 2% Scientists, for 2021, 2022, and 2023.

SHUO ZHU received the Ph.D. degree from Nanjing University of Science and Technology, in 2023. He is currently a Postdoctoral Fellow with the Department of Electrical and Electronic Engineering, The University of Hong Kong. His research interests include computational neuromorphic imaging and its optical applications.