



Optical encryption using joint transform correlators: opto-digital implementations

John Fredy Barrera-Ramírez and Alejandro Velez-Zea

*Grupo de Óptica y Fotónica, Instituto de Física, Facultad de Ciencias Exactas y Naturales,
Universidad de Antioquia UdeA, Calle 70 No. 52-21, Medellín, Colombia*

In memory of Professor Gallieno Denardo, ICTP Italy

This paper presents a comprehensive review of experimentally validated opto-digital joint transform correlator (JTC) cryptosystems, classified according to the transform domain in which they operate: Fourier, Fresnel (free-space), and fractional. Particular attention is given to implementations that incorporate the suppression of non-significant terms, multiplexing strategies, and the use of physical random phase masks, all of which are essential in realistic optical cryptosystems. The review additionally examines single-arm JTC configurations, which do not use an external reference arm to record the encryption key, leading to compact and secure architectures with reduced setup complexity. Overall, this review consolidates the main advances in opto-digital JTC encryption and highlights the experimental trends that define current and emerging cryptosystem designs. © Anita Publications. All rights reserved.

doi: [10.54955/AJP.35.1-3.2026.77-102](https://doi.org/10.54955/AJP.35.1-3.2026.77-102)

Keywords: Experimental optical encryption, Joint transform correlator, Double random phase encoding, Opto-digital cryptosystems, Reference-free cryptosystem.

1 Introduction

The study of the physical properties of light has experienced remarkable progress in recent decades, leading to technological innovations that have enhanced the quality of life in modern society. Advances in light-based technologies have had a profound impact on communication, renewable energy, lighting, health, imaging, and security. Among these areas, information protection has become particularly relevant, as the exponential growth in the exchange of private data demands stronger and more efficient encryption systems. However, many digital encryption systems once considered invulnerable have been compromised, which has stimulated the search for alternative approaches, including optical encryption. In this context, the field of optical information processing enables the manipulation and protection of data, offering high-speed parallel processing and incorporating physical parameters that can be used to increase security [1-8].

Over the last three decades, optical encryption has been recognized as a promising alternative for data protection at the physical layer. The seminal double random phase encoding (DRPE) scheme proposed by Refregier and Javidi in 1995 introduced a powerful framework for optical security: an input image is transformed into a stationary noise-like pattern through the combined action of two statistically independent random phase masks located at different planes of a 4f optical processor [9]. The first experimental demonstration by Javidi et al. confirmed that DRPE could be physically implemented, thus

Corresponding author

e mail: john.barrera@udea.edu.co (John Fredy Barrera-Ramírez)

validating the feasibility of optical encryption beyond numerical simulation [10]. Subsequent experimental developments explored different physical mechanisms and multiplexing strategies. Early implementations using photorefractive crystals demonstrated phase-conjugate encryption and holographic key storage [11], showing the potential of nonlinear media for secure optical encoding. Additional contributions reported multiple-image encryption based on aperture modulation [12], polarization multiplexing [13], lateral-shift-based key modulation [14], and undercover multiplexing [15]. These experiments demonstrated that DRPE-based systems can provide multiple-image protection although their practical implementation is limited by the number of optical elements involved and the stringent alignment requirements needed for stable operation.

As an alternative to the classical 4f encryption system, Nomura and Javidi introduced a joint transform correlator (JTC) encryption architecture based on the DRPE technique in 1999 [16]. In this JTC cryptosystem, the object to be encrypted and the key are placed side by side in the input plane, and the resulting joint power spectrum (JPS) is recorded at the Fourier plane using a single lens in a 2f configuration. In this scheme, one random phase mask corresponds to the security key, while the other is placed in direct contact with the object to be encrypted. This architecture eliminates the need for a reference arm to obtain the encrypted data, uses only one lens, and reduces the alignment requirements compared with 4f systems. Early implementations based on photorefractive crystals demonstrated secure optical data storage using random phase key codes [17], and were followed by experimental color encryption in a JTC configuration [18], color image encryption employing a joint fractional Fourier transform correlator [19], and multiplexing of encrypted data by means of fractal masks [20].

Extending the crystal-based demonstrations of the JTC encrypting system, research rapidly expanded toward opto-digital implementations in which the JPS is recorded with CCD (charge-coupled device) or CMOS (complementary metal–oxide–semiconductor) sensors and processed numerically. Early opto-digital realizations explored phase-shifting interferometry to improve the accuracy of JPS recording [21] and demonstrated high-fidelity recovery of multiple encrypted data through the suppression of undesired terms [22]. Subsequent developments further confirmed the feasibility of encoding complex information in joint-transform architectures, including three-dimensional configurations [23] and optimized random-phase strategies for improved image quality [24]. Additional contributions demonstrated the multiplexing of encrypted movies and dynamic sequences under a JTC arrangement [25], as well as the incorporation of reference-wave-assisted architectures to improve reconstruction fidelity [26]. Multiplexing approaches based on key rotations [27] and sub-sample synthesis for enhanced decrypted quality [28] were also reported, together with the first demonstrations of multiplane optical encryption using phase-only holography [29] and full complex modulation [30].

Further research demonstrated the use of color holographic movie encryption under JTC configurations [31], random-reference-beam enhancement to increase robustness [32], and cryptographic salting to reinforce the security of DRPE-derived schemes in opto-digital systems [33]. A set of experimental studies addressed grayscale optical encryption [34], speckle-noise suppression [35], and noise-free QR-code data recovery [36], followed by scrambling-based noise reduction strategies [37] and the introduction of customized data containers tailored to opto-digital encryption setups [38]. Complementary efforts focused on efficient data-volume handling in experimentally encrypted information [39], optimization of QR-code multiplexing for noise-free character retrieval [40], and general protocols for opto-digital packaging, modulation, and multi-image encryption [41–43].

Several contributions explored lateral-shift multiplexing with modified random masks [44], optical asymmetric cryptosystems based on binary phase modulation [45], and the use of complex-encoded key masks for improved system flexibility [46]. Parallel-encryption strategies for multichannel imaging [47] and JTC systems employing spiral-phase masks [48], topological-charge multiplexing [49], and nonlinear

joint-transform correlation [50] were also investigated. These experiments further confirmed the versatility and maturity of opto-digital JTC encryption in the Fourier domain, even as their implementation complexity varies depending on the type of key modulation, phase encoding, or multiplexing strategy employed.

Additional enhancements included cropping-assisted JTC encryption architectures [51], QR-code-based multi-image JTC systems [52], binary-encoded encryption configurations for grayscale data [53], hybrid optical–digital correlator approaches for security tasks [54], and early demonstrations of Fourier-plane JTC encryption techniques based on phase-term suppression [55]. Collectively, these results further confirmed the maturity, versatility, and robustness of opto-digital JTC encryption in the Fourier domain.

In parallel, the research community also explored extensions of the JTC architecture to other propagation domains. These Fresnel-based configurations, implemented either as joint Fresnel correlators (JFC) or as joint free-space (JFS) cryptosystems, introduced free-space propagation as an additional physical mechanism that enhances encryption flexibility and increases the number of available security parameters. A first step in this direction was the proposal of a JFC architecture employing double optical wedges, which enabled precise control of the effective Fresnel transform order and broadened the range of correlation operations that could be implemented experimentally [56]. The JTC concept was then extended to a joint free-space cryptosystem that used a spatial light modulator (SLM) and a digital camera, demonstrating that high-quality encryption and decryption could be achieved directly under Fresnel propagation conditions [57]. Further work reported an optical image encryption scheme based on a JFC with double optical wedges, confirming that Fresnel-domain JTC architectures are effective for security applications and demonstrating that the introduction of an extra key parameter enhances resistance to attacks and enlarges the key space [58]. A subsequent contribution introduced a noiseless Fresnel JTC encryption configuration that combined a complex secret key with a JFC employing a Billet split lens, significantly improving reconstruction fidelity and robustness [59]. Advancing this line of work, an experimental study of JFC-based optical image encryption consolidated these advances by implementing a fully opto-digital Fresnel-domain cryptosystem and characterizing its performance under realistic conditions [60]. More recently, experimental research demonstrated the use of phase modulation induced by thermal-lens effects to implement a Fresnel-domain JTC cryptosystem, using controlled sample displacements to generate distinct keys and enabling an undercover protocol with decoy data [61]. Collectively, these results established that JTC-based encryption is not restricted to the Fourier domain and that Fresnel propagation provides additional degrees of freedom that can be precisely tuned in experimental opto-digital systems.

A further generalization led to the fractional JTC encrypting system, in which the fractional Fourier transform replaces the classical Fourier transform and the fractional order acts as an additional encryption parameter that expands the key space and enables multiuser and container-based protocols. The first experimental demonstrations of the fractional JTC encrypting system included color-image implementations, thus validating the feasibility of fractional-domain optical security systems using a refractive crystal as a recording medium [19]. Subsequent progress introduced fractional JTC architectures combined with digital holography, demonstrating that phase retrieval and holographic recording could be integrated to improve encryption accuracy [62]. Follow-up work expanded these ideas through iterative partial-phase encoding under a joint fractional correlator using phase-shifting digital holography, demonstrating enhanced control over the fractional domain [63]. The fractional framework was further applied to multiuser and container-based cryptographic protocols, enabling noise-free decryption for multiple authorized users sharing the same encoded dataset [64]. An important development was the first focus-tunable fractional optical cryptosystem, in which an electrically tunable lens enabled fast and stable adjustment of the fractional order, greatly improving the flexibility of laboratory implementations [65]. More recently, a unified fractional-based description of free-space and single-lens processors demonstrated accurate fractional-order decryption for

both numerically and experimentally encrypted data, consolidating the role of the fractional Fourier transform as a practical tool for opto-digital JTC cryptosystems [66]. In combination, these advances show that the fractional domain provides a versatile extension of the JTC architecture, offering tunable parameters that substantially enhance security, flexibility, and multiuser operation.

More recently [67-71], research has focused on reference-free or single-arm JTC cryptosystems, which eliminate the external interferometric arm traditionally used for key recording and thereby simplify the optical architecture. An important early step was the introduction of a master-key generation protocol that avoided the need for an external reference wave in an experimental JTC encrypting architecture, enabling more compact and stable configurations [67]. This line of work was further advanced by the demonstration of a high-performance compact optical cryptosystem without a reference arm, which confirmed that single-arm arrangements can achieve efficient encryption and robust decryption under laboratory conditions [68]. Based on this architecture, a secure selective recovery protocol was proposed for multiple optically encrypted data, enabling flexible access control to specific elements within a multiplexed dataset while preserving the integrity of the remaining information [69]. More recent contributions have shown that non-interferometric key recording can be directly implemented in JTC cryptosystems, removing the need for interference-based registration and enhancing robustness to environmental perturbations [70]. The latest developments employ ptychographic key retrieval in experimental JTC architectures, demonstrating that computational phase-retrieval strategies can recover high-quality keys from intensity-only measurements and further reduce system complexity [71]. Overall, these single-arm JTC implementations represent the current trend toward miniaturized, robust, and low-cost opto-digital encryption systems, making them particularly attractive for real-world secure imaging and authentication tasks.

Beyond JTC-based systems, recent contributions demonstrate that optical encryption is expanding toward complex-media and novel device physics [72-75]. For instance, the use of random scattering media in encryption schemes augments security by expanding the key space and providing robustness against model-based inversion attacks [72]. Additionally, sparse point-spread-function strategies enable multi-image optical encryption with compressed optical signatures and controllable cross-talk in low-SNR environments [73]. Moreover, statistically stationary random-light illumination further increases security by decorrelating the plaintext from accessible field statistics, effectively suppressing information leakage channels [74]. Furthermore, a photo-thermoelectric detector couples optical images to output voltages through photon-induced thermal distribution, providing an encryption scheme compatible with integrated circuits for secure multi-waveband communication [75].

In parallel, metasurface-based holography has also advanced significantly, beginning with addressable metasurfaces for dynamic holography and optical information encryption [76]. Subsequent developments demonstrated holographic color prints with combined phase-and-amplitude control for enhanced optical security [77]. Later, reprogrammable meta-holograms allowed dynamic key rotation and flexible update of encrypted channels [78], while cascaded metasurface holography enabled optical secret sharing protocols with selective access [79]. Further contributions introduced metasurface-based keys for computational imaging encryption [80], metasurface-empowered optical cryptography with multifunctional wavefront control [81], and visual cryptography systems using meta-optics enable rapid decryption without compromising security [82]. More recently, metasurface-enabled optical encryption and steganography demonstrated enhanced information-security capacities with complex and multichannel meta-operators [83]. Another significant development is the enhancement of optical encryption at the physical layer through a learning-based decryption method, where a system utilizing a spin-multiplexing disordered metasurface generates high-security and multi-channel optical encryption via data-driven training [84].

Finally, multiplane experimental encryption using phase-only holography [29] and full-complex modulation [30] has extended volumetric capacity, enabling the simultaneous encryption of multiple

objects on distinct planes. Together, these advances outline a broader trend toward physical-layer security that integrates wavefront manipulation, complex scattering media, and programmable meta-optics with computational methods.

In this context, this paper presents a comprehensive review of experimentally demonstrated opto-digital JTC cryptosystems, classified according to the transform domain in which they operate: Fourier, Fresnel (free-space), and fractional. Special emphasis is placed on practical implementations that include the filtering of non-relevant terms, multiplexing protocols, and the use of ground-glass diffusers as random phase masks. The paper also analyzes compact JTC systems without a reference arm, which constitute the most promising direction for the next generation of compact JTC systems. Throughout this paper, these configurations are referred to as the Fourier JTC encrypting system (also called the conventional JTC cryptosystem), the Fresnel JTC encrypting system (or Fresnel JTC cryptosystem), the fractional JTC encrypting system (or fractional JTC cryptosystem), and the single-arm JTC encrypting system (or single-arm JTC cryptosystem).

2 Opto-digital Fourier JTC cryptosystem

The joint transform correlator encrypting system, introduced by Nomura and Javidi in 2000 [16], offers several practical advantages over the classical 4f DRPE system. In this Fourier JTC encrypting system, the object and the key are placed side by side in a single input plane using the DRPE technique, and the resulting joint power spectrum is recorded with a CCD or CMOS sensor. This configuration eliminates the need for a reference arm to obtain the encrypted data, reduces alignment sensitivity, and simplifies the optical setup while preserving the security mechanisms of DRPE. This compact configuration enables direct acquisition of an intensity-only encrypted object that can be digitally filtered, repositioned, and processed with high flexibility. As demonstrated in numerous experimental studies, these advantages established the conventional JTC encrypting system as a robust and accessible platform for opto-digital optical encryption, and as the natural starting point for analyzing the principles and performance of modern JTC-based cryptosystems.

2.1 Description of the Fourier JTC cryptosystem

The description of the JTC encrypting system in the Fourier configuration is presented in this section, and a schematic of the corresponding setup is depicted in Fig 1. In the Fourier JTC cryptosystem, the input plane contains the object to be encrypted $o(x, y)$ multiplied by a random phase mask $r(x, y)$, and a second random phase mask $k(x, y)$ that acts as the encryption key. In the experimental implementation, the object and the window delimiting the key region, usually known as key window, are displayed on an SLM, while the random phase masks are generated by placing a ground-glass diffuser in direct contact with the SLM [27]. Therefore, the input plane is expressed as,

$$i(x, y) = g((x, y) \otimes \delta(x-a, y) + k(x, y) \otimes \delta(x+a, y)) \quad (1)$$

where $g((x, y) = o(x, y) \cdot r(x, y)$, the symbol $\otimes$ denotes the convolution, $\delta(\cdot)$ is the Dirac delta function, and $2a$ is the distance between the object and the encryption key.

This input plane is illuminated by a plane wave, and the Fourier transform (FT) of the resulting field is obtained in the camera plane by placing a positive lens between the input and the detector. The intensity registered by the camera, the joint power spectrum (JPS), is given by,

$$J(v, w) = |i(v, w)|^2 = |G(v, w)|^2 + |K(v, w)|^2 + G(v, w)K^*(v, w)e^{-4i\pi av} + G^*(v, w)K(v, w)e^{4i\pi av}, \quad (2)$$

where (v, w) are the frequency coordinates, $G(v, w)$ and $K(v, w)$ are the Fourier transforms (FTs) of $g(x, y)$ and $k(x, y)$, respectively, and $*$ indicates the complex conjugate operator. The last two terms contain the encrypted information, while the remaining terms convey extra information that may constitute a vulnerability in the

cryptosystem [85]. To eliminate this issue, the unwanted terms are filtered as follows: A FT is applied to the JPS to spatially separate its components. Subsequently, the extra terms are removed, retaining only one of the last two terms. An inverse Fourier transform (IFT) is then applied to the selected term, and the result is defined as the encrypted data [86].

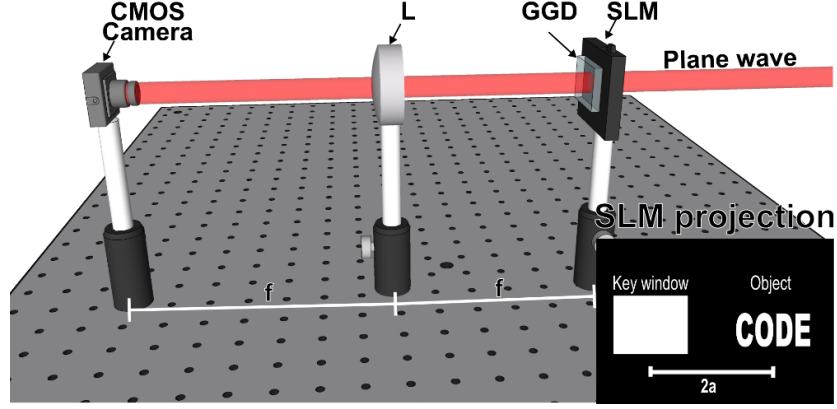


Fig 1. Basic experimental scheme of a Fourier JTC encryption system. L: lens, f: focal length of the lens, GGD: ground-glass diffuser, SLM: spatial light modulator, and 2a: separation between the object and the key window.

By retaining the third term of the JPS, the encrypted object is given by,

$$E(v, w) = G(v, w)K^*(v, w). \quad (3)$$

The next step in the encryption process is the experimental recording of the key information. To this end, an interferometric arrangement is implemented, in which one arm contains the JTC encrypting architecture displaying only the key window, while the second arm introduces a reference plane wave, as shown in Fig 2. The detected intensity distribution at the camera plane is,

$$L(v, w) = |P(v, w)|^2 + |K(v, w)|^2 + P(v, w)K^*(v, w)e^{2i\pi\lambda(\alpha v + \beta w)} + P^*(v, w)K(v, w)e^{-2i\pi\lambda(\alpha v + \beta w)}, \quad (4)$$

where α and β are the incidence angles of the plane wave on the camera, λ is the wavelength of the illumination source, and $P(v, w)$ denotes the reference plane wave. By applying a filtering procedure analogous to that used to obtain the encrypted object in Eq (3), the information of the encryption key $K(v, w)$ is then finally obtained [28].

Then, the decryption process proceeds by multiplying the encrypted data by the FT of the encryption key $K(v, w)$, and applying the IFT to the resulting product.

$$d(x, y) = g(x, y) \otimes k^*(x, y) \otimes k(x, y), \quad (5)$$

where $\otimes$ denotes the convolution operator. The self-correlation $k^*(x, y) \otimes k(x, y)$ can be approximated as a Dirac delta by applying the broadband noise approximation [87]. As a result, the decrypted object is,

$$d(x, y) = g(x, y) \otimes \delta(x, y) = g(x, y) = o(x, y) \cdot r(x, y), \quad (6)$$

Therefore, the decrypted intensity, $|d(x, y)|^2 = |o(x, y)|^2$, retrieves the original object intensity.

In experimentally implemented DRPE-based cryptosystems, including JTC architectures, the decrypted object typically exhibits speckle noise due to the use of two random phase masks. A practical and highly effective opto-digital solution is to embed the information into a robust binary container prior to encryption [36]. In practice, encoding the message as a QR code before optical encryption generates a binary representation with intrinsic redundancy and error-correction properties, which provide tolerance to the speckle noise characteristic of decrypted data in DRPE-based cryptosystems. After optical decryption, a

simple block-processing stage restores the QR structure, enabling the original message to be recovered with perfect fidelity, even though the decrypted QR pattern still exhibits speckle arising from the encryption–decryption process. This opto-digital, container-based strategy provides an experimentally validated method to overcome the degradation inherent to physical optical encryption systems.

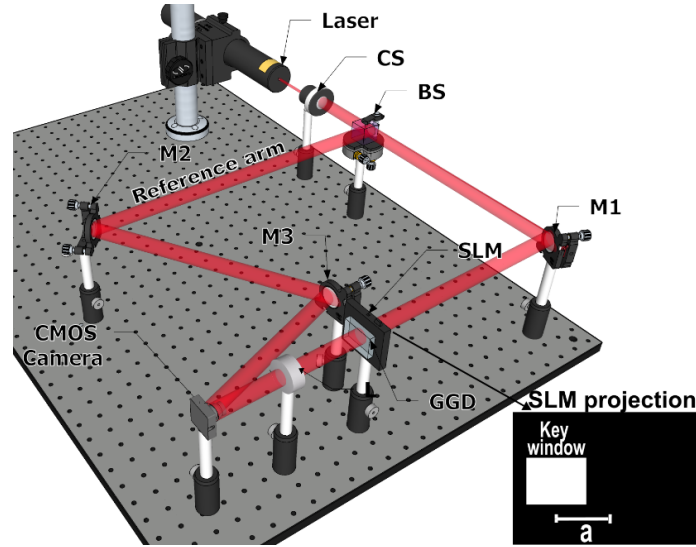


Fig 2. Basic experimental scheme used to record the Fourier hologram of the encryption key. L: lens, GGD: ground-glass diffuser, CS: collimation system, BS: beam splitter, M: mirror, and SLM: spatial light modulator.

Figure 3 illustrates the experimental performance of the Fourier-domain JTC encrypting system when QR codes are used as information containers [36]. In **Fig 3(a)**, the input image to be encrypted is shown together with its corresponding QR-encoded representation in **Fig 3(b)**, which serves as a robust information container. The encrypted QR pattern is presented in **Fig 3(c)** and exhibits the speckle-like distribution characteristic of DRPE-based JTC encryption. After decryption, the QR structure in **Fig 3(d)** contains speckle noise that locally distorts the cell distribution. A subsequent digital block-processing step removes these distortions, resulting in the clean binary code displayed in **Fig 3(e)**, which is correctly decoded as shown in **Fig 3(f)**. These experimental results confirm that embedding the information into a QR container prior to optical encryption enables reliable, noise-free information recovery under realistic JTC operating conditions, even when the optically decrypted patterns remain affected by speckle.

2.2 Experimental opto-digital Fourier-domain JTC implementations

A broad range of experimental works has explored different aspects of Fourier-domain JTC encryption, including key recording, noise suppression, multiplexing strategies, grayscale and three-dimensional information handling, QR-code protection, and security-enhanced protocols. The following overview presents the contributions and highlights the experimental configurations used in the reported studies, emphasizing their practical advantages.

Early contributions to JTC-based encryption addressed fundamental limitations of the architecture while demonstrating progressively more capable optical and opto-digital implementations. For instance, an initial study showed that the autocorrelation structure of a Fourier-plane JTC can be used advantageously by compensating the phase distortions introduced in the shifted input distributions, enabling successful reconstruction through binary-phase CGHs (computer-generated holograms) and CCD detection despite the sensitivity of the system to pixel-dependent phase artifacts [55]. A subsequent analysis compared the

performance of fully optical and hybrid JTC processors for security verification, incorporating an optically addressed liquid-crystal modulator and evaluating peak-to-noise ratios and correlation efficiency for different phase-mask strategies. The results highlighted the high sensitivity of purely optical configurations and the robustness of hybrid architectures at the expense of additional complexity [54].

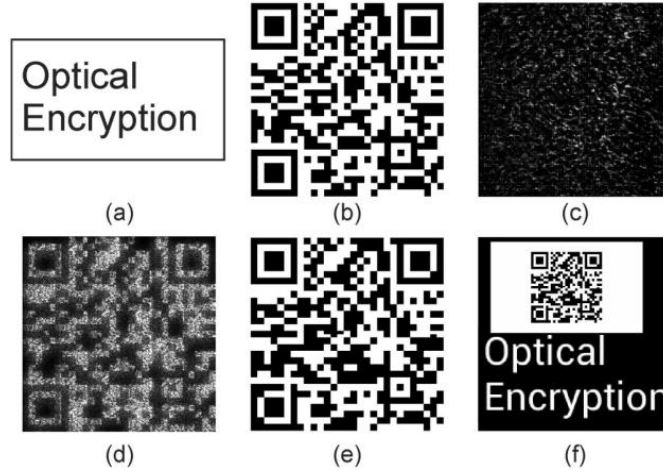


Fig 3. (a) Input message and (b) its respective QR code, (c) encrypted QR code, (d) decrypted QR code, (e) decrypted QR code after block processing, and (f) recovered information after reading (e). Experimental results reproduced from Ref [36] with permission from © Optica Publishing Group.

As the investigation moved forward, later work combined DRPE with three-step phase-shifting interferometry to record the encrypted field and the key as Fresnel holograms using a phase-only LCTV, a strategy that relaxes alignment constraints and enables stable opto-digital decryption while requiring precise phase-shift control during acquisition [21]. In a further development, a practical implementation of complex-valued key masks was achieved by cascading two twisted-nematic SLMs operating in amplitude and phase modes and by developing a modified iterative Fourier transform algorithm that adapts the mask to the restricted complex-modulation range of real devices, demonstrating successful optical decryption and key-shift invariance despite the inherent limitations of commercial SLM modules [46].

Further research focused on incorporating a filtering process and studying the invariance properties of the JTC architecture. An experimental JTC-based encryption scheme using a digital holographic configuration in a Mach–Zehnder interferometer, with a JTC in one arm and a reference wave in the other, was introduced. The noise influence caused by intensity saturation during image capture was analyzed to design a filtering process that reduces the information to be handled and increases the speed of the overall procedure [26]. An experimental study demonstrated that the intrinsic invariance to lateral shifts in a conventional JTC encrypting architecture prevents diffuser-shift multiplexing, because all encrypted images are recovered regardless of the diffuser position. A modified random-mask arrangement was then proposed, in which the diffuser is placed in a separate plane so that its Fourier-transformed speckle pattern acts as the encryption mask, and controlled lateral shifts enable the encryption and selective recovery of multiple images [44].

The following development was the introduction of opto-digital strategies to improve decryption quality and control noise. Noise suppression was subsequently addressed through an opto-digital approach that records the joint power spectrum optically and applies digital filtering to remove undesired correlation terms, enabling the decryption of encrypted and multiplexed images with high fidelity [22]. Further work implemented an experimental multiplexing procedure in which successive in-plane rotations of the encrypting diffuser generate different encoding keys, enabling the storage and selective recovery of multiple encrypted

objects within the same JTC architecture by combining optical recording with virtual-optics filtering and repositioning steps [27]. In addition, an opto-digital protocol was developed to synthesize encrypted sub-samples of an image, combining optical recording of the joint power spectrum with digital recombination of the encrypted segments to improve the quality of the decrypted image while preserving compatibility with the JTC architecture [28].

As the scope of the JTC expanded toward dynamic information and multiplexing, an experimental contribution [25] demonstrated the multiplexing of encrypted movies. In this method, each frame of a dynamic scene was encrypted using the same encryption key in the JTC arm. The encrypted data for each frame was then assigned to specific coordinates in the Fourier domain, preventing overlap in the output plane. All processed frames were combined into a single multiplexed package. Decryption involved multiplying this package by the Fourier transform of the correct key and applying an inverse Fourier transform, after which the correctly positioned frames were extracted and synchronized to display the movie. The approach was also extended to multiplex several movies, each accessible only with its corresponding key [25]. A related contribution proposed a solution to multiple data handling by separately processing each object, applying a packaging operation to generate a single information unit that is encrypted with a random phase mask, and allowing the end user to recover the objects in separate locations by multiplying by the conjugate mask and performing a Fourier transform [42]. Another study presented an experimental JTC encryption protocol in which each input character is displayed as a single frame to build a multiplexed keyboard, allowing text of unlimited length to be handled with double-key security by combining an optical key with a selection-position key [43].

A new direction in this field explored QR-code containers and opto-digital packaging strategies. An experimental scheme was reported in which the message is first encoded as a QR code and then optically encrypted in a JTC architecture, so that the binary QR representation with redundancy and error-correction enables noise-free recovery of the original information after decryption and a simple block-based postprocessing stage, even though the decrypted QR pattern still exhibits speckle [36]. A complementary contribution reported experimental scrambling and noise reduction applied to the optical encryption of QR codes, combining JTC-based encryption with scrambling procedures that enhance security while reducing residual noise in the decrypted QR code [37]. Another contribution reported an experimental opto-digital protocol in which each data element is optically processed in a 2f system with a random phase mask, digitally filtered to remove non relevant terms, and theta modulated with a grating that assigns a distinct spatial position. All modulated elements are combined into a single package, which is then encrypted by multiplication with a random phase mask, enabling simultaneous recovery of all data without superposition by an authorized user [41].

Subsequent work consolidated these packaging and recovery strategies into noise-free protocols. A JTC-based scheme was presented in which each character of a message is converted into a QR code, divided into portions, processed through a 2f digital-holography technique, and combined into a single package that can be recovered without speckle noise and correctly decoded after binarization. The encrypted package can also be multiplied by a digital diffuser, allowing opto-digital encryption while maintaining the noiseless retrieval of QR codes [40].

The next phase expanded the scope of the JTC cryptosystem to three-dimensional information, specialized containers, and efficient data-volume management. A three-dimensional JTC cryptosystem was introduced, encrypting 3D information using a second 3D object as a key. The decryption is performed virtually through numerical propagation, which reconstructs the depth information and confirms the viability of protecting volumetric objects [23]. Improved decryption quality was obtained by embedding the information into a customized data container specifically designed to increase noise tolerance and to allow the optical encryption of larger amounts of information under practical recording conditions. This tailored

container structure overcomes the limitations of conventional QR-based containers, providing enhanced robustness to speckle noise in coherent optical encryption [38]. An optical approach for efficiently managing multiple encrypted data was also demonstrated, combining optical filtering and optical scaling to reduce the amount of experimental data while preserving correct decryption [39]. The method defines an efficiency factor that determines the achievable data reduction, with experiments reporting volume reductions up to 94.24% without degrading the reconstructed information [39].

Following these developments, the research focus progressively shifted toward robustness and security enhancement. A procedure for enhancing the security of DRPE schemes was presented by incorporating cryptographic salting into the JTC architecture, increasing sensitivity to variations in the encryption process and improving robustness against different types of attacks, as demonstrated by numerical simulations and optical experiments [33]. An experimental optical encryption method for grayscale information was also introduced, showing that grayscale scenes can be optically encrypted and correctly recovered with good visual quality, including the reconstruction of a grayscale video that confirms the feasibility of the approach under practical conditions [34]. A deterministic speckle-noise reduction procedure was then proposed, modifying the encrypted distribution to reduce the speckle present in the decrypted images, with experiments showing clear visual improvement without altering the image content [35]. A parallel multi-channel encryption strategy was further developed, allowing several images to be encrypted simultaneously within a JTC configuration and recovered independently, demonstrating efficient multi-image handling in a parallel optical architecture [47].

The structure of the key masks and the assignment of multiple access levels were subsequently studied. An optimized encryption method using optimized random phases was reported, where phase masks are designed to produce nearly phase-only encrypted data, reducing random correlation noise and improving decryption quality, as confirmed by numerical and experimental results [24]. Additional experimental research analyzed a JTC encryption system based on a spiral phase mask, exploring how its characteristics influence the encrypted data and providing experimental results that describe the behavior of this configuration under different conditions [48]. Finally, a topological-charge multiplexing scheme was demonstrated for JTC multiple-image encryption, showing that different topological charges allow distinct images to be encrypted and decrypted independently, enabling multi-image processing and multi-level authorization within a single optical system [49].

Another line of work addressed real-time operation and decryption-quality improvements in opto-digital configurations. Secure real-time generation and display of color holographic movies was demonstrated, showing that dynamic color information can be produced and visualized continuously within an opto-digital configuration. The system enables real-time color holographic movie generation and provides experimental validation of its operation under practical conditions, confirming the feasibility of continuous secure display of color holographic content [31]. A random reference beam cryptosystem was reported to obtain improved decryption quality, incorporating a random reference beam into the optical encryption scheme and providing numerical and experimental results that demonstrate the behavior of the proposed configuration [32]. A joint-transform correlator multiple-image encryption system based on a quick-response code key was presented, where a QR code is used as the key in the optical encryption process, and experimental results show correct encryption and decryption of multiple images within the proposed architecture [52]. Additionally, a JTC encryption system based on binary encoding for grayscale images was investigated. This method converts the grayscale input into a binary image prior to optical encryption, improving the decrypted image quality. Experimental validation confirmed the effectiveness of binary encoding for high-fidelity grayscale encryption in a JTC architecture [53].

Further contributions investigated schemes aimed at improving encryption performance and security. An experimental three-step JTC optoelectronic setup in which the input plane is fully encoded in phase

by a phase-only SLM was presented, providing enhanced control over the phase information and enabling high-quality optical reconstructions [50]. Another proposal was a security-enhanced JTC optical cryptosystem that employs a cropping operation as a defensive mechanism. The method allows up to 10% of the ciphertext to be cropped prior to transmission while preserving decryption quality and resisting multiple attacks, using a low-complexity and easily operable process [51]. Additionally, an asymmetric JTC cryptosystem was introduced that combines binary phase modulation with an image superposition–subtraction operation to construct a one-way trapdoor function, establishing an asymmetric optical encryption architecture. The system employs a structured spiral phase mask as the key, whose parameters are secured using the RSA algorithm, thus improving key distribution and management and aligning the scheme with public-key cryptographic principles [45].

More recently, the evolution of this research line has consolidated the use of full complex modulation in experimental JTC cryptosystems. An encryption method achieving full complex modulation was demonstrated using a single phase-only SLM. The technique encodes complex-valued input planes for a JTC cryptosystem into phase-only holograms, enabling independent control over the phase and amplitude of both the cryptographic keys and the objects. The capabilities of the method were validated by generating optimized random phase masks and experimentally encrypting various grayscale and binary objects. Numerical simulations and experimental results confirmed that this full complex modulation approach, combined with optimized masks, enhances the quality of the decrypted objects [30]. Extending this approach, a scheme to encrypt multiplane scenes using full complex modulation was demonstrated. The work reports the experimental encryption of a multiplane scene composed of up to nine different two-dimensional objects placed at different distances along the optical axis. Additionally, it demonstrates that binary amplitude encoding is superior to double-phase encoding, producing comparable or higher quality, particularly in the experimental case, and allowing the encryption of larger scenes [29].

Taken together, these experimental contributions demonstrate that Fourier-domain JTC cryptosystems can be implemented with a wide variety of opto-digital configurations. On one hand, compact architectures offer accessibility and are well suited for multiplexed encryption, though they often require post-processing to control noise. In contrast, more elaborate architectures incorporating complex-encoded keys, spiral or topological-phase masks, asymmetric or salting protocols, and full complex modulation add extra security parameters, enable three-dimensional and multiplane scenes to be encrypted, and improve decrypted quality, at the cost of complexity and more alignment and stability constraints. This progression from simple to sophisticated implementations summarizes the evolution of Fourier-domain JTC encryption and sets the conceptual foundation for its extension into the Fresnel and fractional domains, which are examined in the following sections.

3 Opto-digital Fresnel JTC cryptosystem

The JTC cryptosystem can be reconfigured to operate in the Fresnel domain instead of the conventional Fourier domain. This system enables optical encryption under free-space propagation, provides additional flexibility, and expands the available security parameters beyond those found in traditional Fourier-domain implementations. Unlike the $2f$ arrangement, where the encrypted data is recorded at the Fourier plane using a lens, Fresnel-based JTC configurations operate through a controlled propagation distance. The resulting architecture preserves the compactness and recording simplicity of the Fourier-based JTC encrypting system while introducing new experimental degrees of freedom associated with propagation distance, space–bandwidth matching, and the size and recording position of the joint Fresnel power distribution.

3.1 Description of the Fresnel JTC cryptosystem

The Fresnel JTC encrypting system follows the same conceptual framework described in the Fourier-domain configuration but replaces the lens-based Fourier transform with a free-space propagation stage of

distance z . In particular, the input plane has the same configuration as in the Fourier JTC cryptosystem, with the object and the key arranged side by side and multiplied by their corresponding random phase masks, as defined in Eq (1). Since in this configuration there is no lens that performs an optical Fourier transform of the input plane, the pattern registered by the CMOS camera corresponds directly to the free-space propagation of the input plane transmittance.

A schematic representation of the opto-digital Fresnel JTC cryptosystem is shown in Fig 4. At a propagation distance z from the input plane, the complex field $U_z(u, v)$ reaches the CMOS sensor, and its recorded intensity is known as the joint Fresnel power distribution (JFPD) [57]:

$$J_z(u, v) = |U_z(u, v)|^2 = |G_z(u, v)|^2 + |K_z(u, v)|^2 + G_z(u, v)K_z^*(u, v)e^{-4i\pi zu} + G_z^*(u, v)K_z(u, v)e^{4i\pi zu}, \quad (7)$$

where $G_z(u, v)$ and $K_z(u, v)$ are the Fresnel transforms of $g(x, y)$ and $k(x, y)$ at propagation distance z , and $u = x/\lambda z$ and $v = y/\lambda z$ are the coordinates in the Fresnel plane. To obtain the encrypted object and the information associated with the security key, the Fresnel JTC cryptosystem follows a procedure analogous to that used in the Fourier JTC cryptosystem described in Section 2.1. The detailed opto-digital implementation of this process is described in Ref [57].

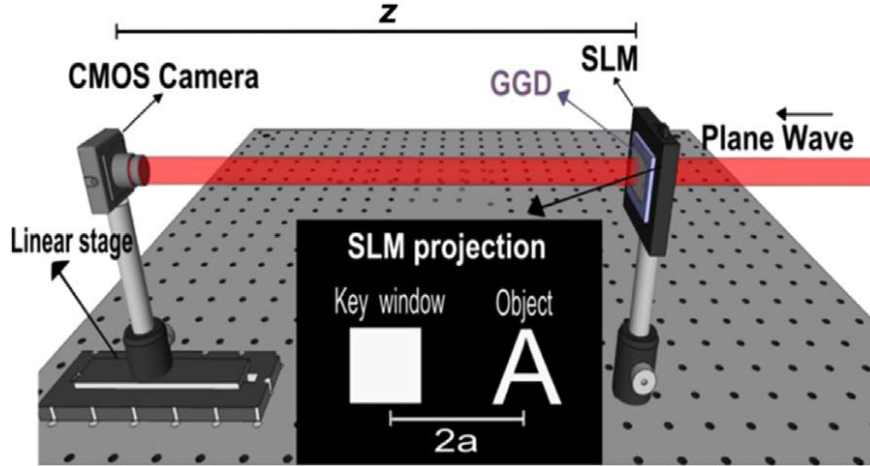


Fig 4. Basic experimental scheme of the Fresnel JTC cryptosystem. SLM: spatial light modulator, GGD: ground-glass diffuser, and z : propagation distance. Scheme reproduced from Ref [57] with permission from Elsevier.

Figure 5 summarizes the main features of the Fresnel-domain cryptosystem [57]. The input object is shown in Fig 5(a), while Fig 5(b) displays the experimentally recorded JFPD, which exhibits the speckle-like structure produced by the diffuser and the free-space propagation. Under the correct Fresnel-domain key, the original information is recovered (Fig 5(c)), with a speckle level comparable to that observed in other optical cryptosystems. In contrast, the use of an incorrect key leads to the noise-like output shown in Fig 5(d), where the encrypted information remains completely hidden and no recognizable features can be recovered, confirming the security of the method.

Compared with the Fourier-domain architecture, the Fresnel JTC introduces the propagation distance z as an additional physical security parameter, so that deviations from the correct value produce a mismatch during decryption and reinforce protection against brute-force attacks. At the same time, eliminating the Fourier lens simplifies the optical arrangement and removes lens-induced aberrations, focal-length restrictions, and some alignment constraints, leading to a more experimentally accessible setup.

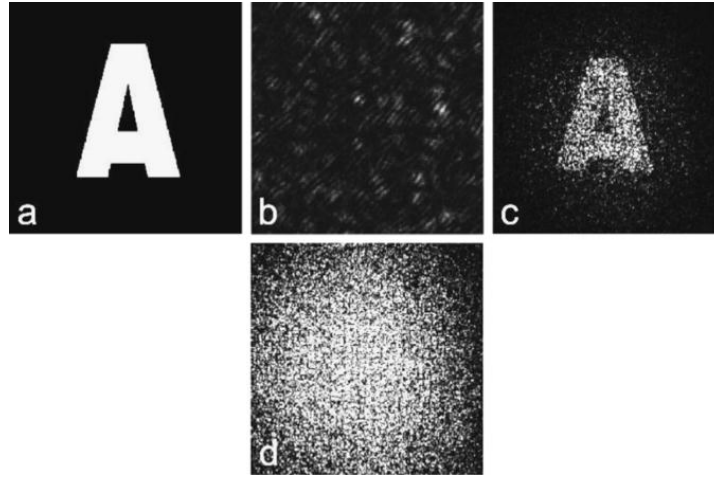


Fig 5. (a) Original object, (b) JFPD of (a), (c) decrypted object with the correct key, and (d) decrypted object with an incorrect key. Experimental results reproduced from Ref [57] with permission from Elsevier.

3.2 Experimental Fresnel-domain implementations

This section summarizes the experimental developments carried out within the Fresnel-domain JTC framework, outlining the configurations adopted, the strategies used for recording and processing, and the practical behavior observed in implementations.

In an initial Fresnel-domain implementation, a joint Fresnel transform correlator based on double optical wedges is presented, where the classical wedge interference device replaces the discrete linear phase mask and achieves continuous linear phase modulation with high precision. This correlator is space-variant and, compared with a conventional JTC, produces a sharper correlation peak, a reduced zero-order term, and a more uniform joint Fresnel power spectrum. The optical configuration has a simple structure and is easy to perform experimentally with common optical elements [56]. In a related Fresnel-domain configuration, a joint free-space cryptosystem is evaluated as a function of the object–camera and key–camera distances, revealing gradual degradation of the recovered object as the object–camera distance increases and a significant tolerance to axial displacements of the key. Experimental results demonstrate the validity and applicability of the cryptosystem and show that the decrypting protocol is simple while keeping standard security characteristics, with a structure that is simpler than others because it does not require lenses [57].

In a subsequent wedge-based Fresnel configuration, another optical cryptosystem based on a joint Fresnel transform correlator with double optical wedges is proposed, in which the encrypted image is real-valued and thus easier to record and transmit, and the encryption process does not require strict alignment of optical elements or the generation of the complex conjugate of the key. The decrypted image quality is improved because the original encrypted image is divided by the Fresnel transform power distribution of the key mask to obtain a recovered image with significantly reduced noise. The nonlinearity of the encryption process and the introduction of an extra key parameter enhance the security of the system against attacks and enlarge the key space [58]. Extending the Fresnel-domain approach, a noiseless optical cryptosystem based on a joint Fresnel transform correlator with a Billet split lens is designed, where the adjustable split width controls the size and recording position of the joint Fresnel power distribution. The object to be encrypted is converted into a QR code to avoid noise effects, and a complex secret key composed of a QR-code filter and a spiral phase mask is introduced to facilitate transmission and preservation. A successful decryption

requires the correct QR filter and correct spiral phase, due to the high sensitivity of the complex secret key to these components [59].

Following these developments, an experimental study investigated an encryption system based on a joint Fresnel transform correlator, analyzing factors affecting decrypted image quality and implementing denoising operations to reduce noise effectively. The research identified that the mismatch between the space-bandwidth product of the joint image and the experimental system degrades the decrypted quality. By optimizing the random phase mask and the key mask through an iterative algorithm, the decrypted image quality was improved. The optimized phase masks do not weaken the resistance of the ciphertext to occlusion, while the space-bandwidth of the system limits the amount of information that can be encrypted [60]. In a more recent contribution, an experimental study implemented a Fresnel JTC cryptosystem by employing phase modulation generated through the thermal-lens effect. Controlled axial displacements of the sample were used to modify the phase of the illumination beam, resulting in the generation of two distinct encryption keys. This feature enabled an undercover protocol in which a target object and a decoy object were encrypted with different keys and multiplexed into a single package. Access to the decoy information is possible with its corresponding key, whereas recovery of the target object requires both the correct key and knowledge of the specific undercover decryption procedure [61].

The contributions reviewed demonstrate that the Fresnel JTC encrypting system can be implemented with double optical wedges, lensless free-space propagation, and joint Fresnel correlators that incorporate Billet split lenses, complex secret keys, and the photothermal effect. The reported results indicate that these arrangements generate real-valued encrypted distributions and joint Fresnel power patterns with sharper correlation spots and smaller zero-order terms, and that decrypted quality is mainly determined by propagation distance, wedge geometry, split width, phase-mask design, and the space-bandwidth match between the encrypted data and the recording system. These contributions also reveal that denoising procedures, additional key parameters, and optimized random phase and key masks improve the behavior of encrypted and decrypted information without reducing resistance to occlusion or axial misalignment, confirming the experimental feasibility of Fresnel-domain JTC cryptosystems. Beyond the Fresnel JTC cryptosystem, several studies indicate that introducing fractional Fourier transforms into the JTC framework provides additional flexibility for encryption and enables new configurations that are examined in the next section.

4 Opto-digital Fractional JTC cryptosystem

The fractional JTC encrypting system extends the capabilities of the Fourier and Fresnel JTC architectures by introducing the fractional Fourier transform (FrFT) as the optical operation governing the propagation of the input field. Instead of relying on a physical Fourier lens or free-space propagation, the system employs a tunable fractional order α that determines an intermediate transform domain between the Fourier and Fresnel representations. This additional degree of freedom expands the key space and reinforces security by associating the encryption and decryption processes with a specific fractional order. As in the previous sections, the input plane preserves the same configuration defined in Eq (1), with the object and the key arranged side by side and multiplied by their corresponding phase masks.

4.1 Description of the Fractional JTC cryptosystem

The fractional joint transform correlator (FrJTC) extends the JTC encryption framework by incorporating the fractional Fourier transform (FrFT) as the transform that generates the encrypted data. As in the Fourier and Fresnel domain architectures, the input plane contains the object window and the key window, both displayed on an SLM and illuminated through a ground-glass diffuser to provide the two random phase masks required for encryption. A schematic representation of this opto-digital fractional architecture is shown in Fig 6.

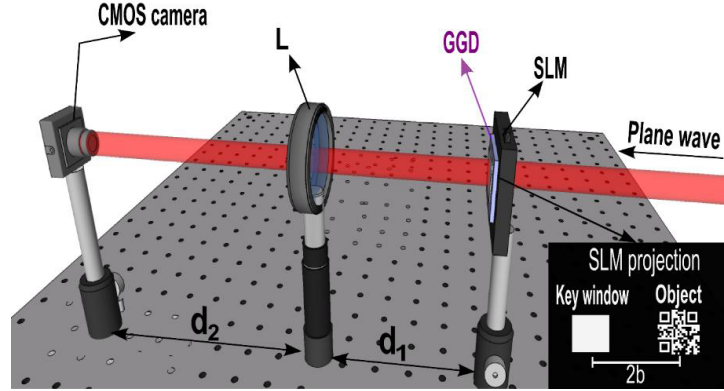


Fig 6. Basic experimental scheme of the fractional JTC cryptosystem. L: lens, GGD: ground-glass diffuser, SLM: spatial light modulator, d_1 : input plane-lens distance, d_2 : lens-output plane distance, and $2b$: separation between the object and key window. Scheme reproduced from Ref [64] with permission from Elsevier.

This arrangement reproduces the standard JTC input configuration used throughout this review. The input plane of the FrJTC system can be expressed as [64],

$$e(x, y) = \tau_{b, \alpha}\{g(x, y)\} + \tau_{-b, \alpha}\{k(x, y)\} \quad (8)$$

here $\tau_{b, \alpha}\{\}$ is the translation fractional Fourier operator and α is the fractional order [88,89]. The translation fractional Fourier operator of order α shifts the object and key window while preserving their fractional-domain structure. In the optical setup of the FrJTC, the combination of the free space propagation between the input plane and the lens, the quadratic phase introduced by the lens, and the free space propagation from the lens to the output plane results in a fractional Fourier transform of order α . When $\alpha = \pi/2$, the system corresponds to the classical Fourier JTC encrypting configuration. In this context, the value of α is determined by the distances d_1 and d_2 between the SLM, the lens, and the CMOS sensor, as well as by the lens focal length f . In particular, the fractional order satisfies

$$\alpha = \arccos\left(\frac{[(d_1 - f)(d_2 - f)]^{1/2}}{f}\right) \quad (9)$$

which establishes the precise optical configuration required to achieve the desired fractional plane.

At the CMOS detector, the system records the joint fractional Fourier power distribution (JFrPD), defined as the intensity of the fractional Fourier transform of the input field,

$$J_\alpha(\xi, \eta) = |e(\xi, \eta)|^2 = |G_\alpha(\xi, \eta)|^2 + |K_\alpha(\xi, \eta)|^2 + G_\alpha(\xi, \eta)K_\alpha^*(\xi, \eta)e^{-4i\pi b\xi\text{csc}(\alpha)} + G_\alpha^*(\xi, \eta)K_\alpha(\xi, \eta)e^{4i\pi b\xi\text{csc}(\alpha)}, \quad (10)$$

here $G_\alpha(\xi, \eta)$ and $K_\alpha(\xi, \eta)$ are the fractional Fourier transforms of order α of $g(x, y)$ and $k(x, y)$ respectively, and $\text{csc}(\cdot)$ is the cosecant trigonometric function. To obtain the encrypted object and the data associated with the security key, the fractional JTC architecture follows a procedure that parallels the strategy employed in the Fourier-domain JTC described in Section 2.1. In this case, the fractional joint power spectrum is digitally captured and processed to extract both the encrypted information and the corresponding encryption key. The complete opto-digital implementation of this encryption-decryption protocol, including the generation and manipulation of the fractional-order domains involved, is thoroughly detailed in Ref [64].

In addition to the security parameters inherent to the JTC architecture, the fractional order α acts as an extra encryption key. Only the correct value of α reproduces the precise propagation that defines the joint fractional power distribution; a deviation leads to a noise-like decrypted field.

Figure 7 illustrates the operation of the fractional-domain JTC cryptosystem [64]. The original object is shown in Fig 7(a), while Fig 7(b) displays the experimentally recorded joint fractional power distribution (JFrPD) for a specific fractional order. The encrypted data obtained is presented in Fig 7(c). Decryption with an incorrect key, either by using a wrong fractional order or an unauthorized user-specific configuration, produces the noise-like pattern in Fig 7(d), where the data remains encrypted, thus evidencing the security of the scheme. The object is decrypted only when the correct key parameters, including the proper fractional order, are used (Fig 7(e)). These results demonstrate that fractional order constitutes a highly sensitive security parameter.

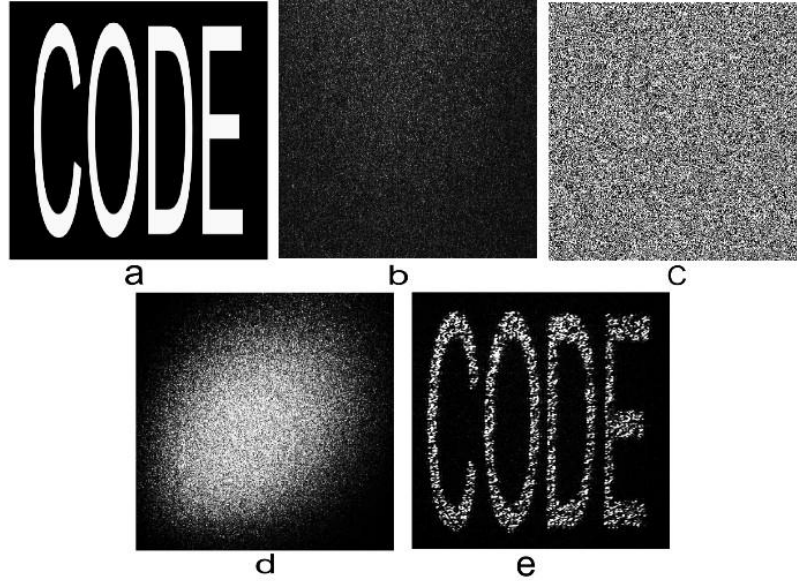


Fig 7. (a) Original object, (b) JFrPD of (a), (c) encrypted data, (d) decrypted data with an incorrect key, and (e) properly decoded data. Experimental results reproduced from Ref [64] with permission from Elsevier.

4.2 Experimental Fractional-domain implementations

This section reviews the experimental contributions related to fractional-domain JTC architectures, describing the implementations used to operate with tunable fractional orders and examining the practical behavior of these systems under different encryption and decryption conditions.

A hybrid encryption scheme that combines a JTC with a joint fractional transform correlator is proposed. The system holographically generates an additional random phase mask used as a master key by means of a Mach–Zehnder interferometer containing a JTC arm, and the fractional order acts as an additional security parameter while the interferometric operation is required only once during the master-key generation, which relaxes stability and alignment requirements. Experimental results verify the feasibility of the proposal and include an application to multiple-image encryption using a multiplexing technique [63]. In a related fractional-domain implementation, an encryption scheme that uses iterative partial random phase encoding in a joint fractional transform correlator is described. This implementation uses a two-step phase-shifting interferometry to retrieve the encrypted image from only two interference intensity distributions. The fractional-domain architecture alleviates alignment constraints and removes the need for beam splitting in holographic recording, while the two-step phase-shifting interferometry procedure suppresses disturbances from DC and conjugate terms in the output. A set of random binary masks is incorporated as additional

keys to restrict the encoding area of the random phase masks, ensuring that only selected pixel regions are subjected to phase encoding while the remaining data are preserved [63].

In another study, an experimental contribution reports a fractional JTC cryptosystem in which the robustness of the scheme is evaluated as a function of the fractional order. The protocol demonstrates noise-free information recovery when QR codes are used as information containers and shows that multiple encrypted data associated with different fractional orders can be handled in a multiuser scenario [64]. A different approach uses an electrically focus-tunable lens to control the fractional order in a fractional Fourier JTC encrypting system. Numerical simulations and experimental results evaluate encryption and decryption for different focal lengths and demonstrate a multiplexing method that exploits the tunability of the lens to validate the flexibility of the cryptosystem [65].

Finally, an opto-digital fractional Fourier-based description is introduced for the decryption of experimental JTC cryptosystems implemented with free-space propagation and a single-lens processor. Decryption using implementations based on the convolution method and the Fresnel transform method shows excellent agreement with inverse propagation, and the analysis of fractional-order variations and random occlusion confirms that the fractional order acts as an additional encryption parameter [66].

The experimental studies reviewed in this subsection demonstrate the versatility and growing maturity of fractional-domain JTC encryption. Different strategies have been proposed to control the fractional order, including interferometric master-key generation, digital holography combined with iterative partial phase encoding, diffuser-based implementations, and electronically tunable lenses. These approaches expand the range of experimental configurations available for fractional encryption, enabling noise-free reconstruction, multiuser operation, tunable encryption parameters, and accurate decryption in both free-space and single-lens architectures. In combination, these contributions establish the fractional-domain JTC as a flexible and experimentally viable platform for optical encryption. In parallel to these developments in the fractional domain, a complementary research direction focused on simplifying the optical arrangement by eliminating the reference arm and enabling compact single-arm configurations for key recording and data protection.

5 Single-arm JTC cryptosystem

The evolution of JTC encryption has therefore led to a research line focused on compact architectures and reference-free key recording, which has produced single-arm implementations with greater practicality in experimental environments. The single-arm JTC encrypting system is a compact optical encryption architecture in which both the encrypted data and the security key are recorded without the need for a physical reference arm. This approach eliminates several alignment and stability requirements present in conventional interferometric systems while preserving the essential characteristics of Fresnel-domain JTC encryption. In this section, we review key-registering strategies for high-performance single-arm JTC cryptosystems, including master-key generation, reference-free recording, selective recovery, and non-interferometric key retrieval [67-71].

5.1 Description of the single-arm JTC cryptosystem

Figure 8 shows the optical architecture of the compact single-arm JTC cryptosystem in the Fresnel domain. The procedure to obtain the encrypted object is the same as that described in Section 3.1.

The information of the encryption key is required for the recovery process. In general, an off-axis holographic system is implemented for the experimental recording of the security key (see Section 2.1). Figure 9(b) shows the experimental arrangement of a conventional Fresnel JTC cryptosystem used to record the information of the decryption key; this scheme includes an off-axis arm that enables the holographic recording [57]. In this configuration, the key information is obtained from the interference between the

Fresnel transform of the key and a plane wave provided by the reference arm, which is used exclusively during key recording and is blocked during the encryption step.

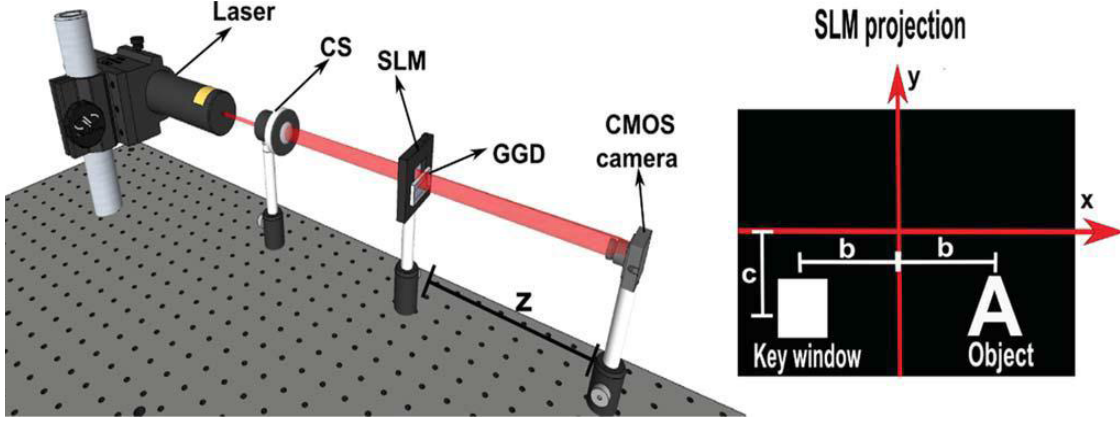


Fig 8. Basic experimental scheme of single-arm JTC cryptosystem. CS: collimation system; SLM: spatial light modulator; GGD: ground-glass diffuser, $2b$: separation between the object and key window, and z : distance between the SLM and the CMOS camera. Scheme reproduced from Ref [68] with permission from © IOP Publishing.

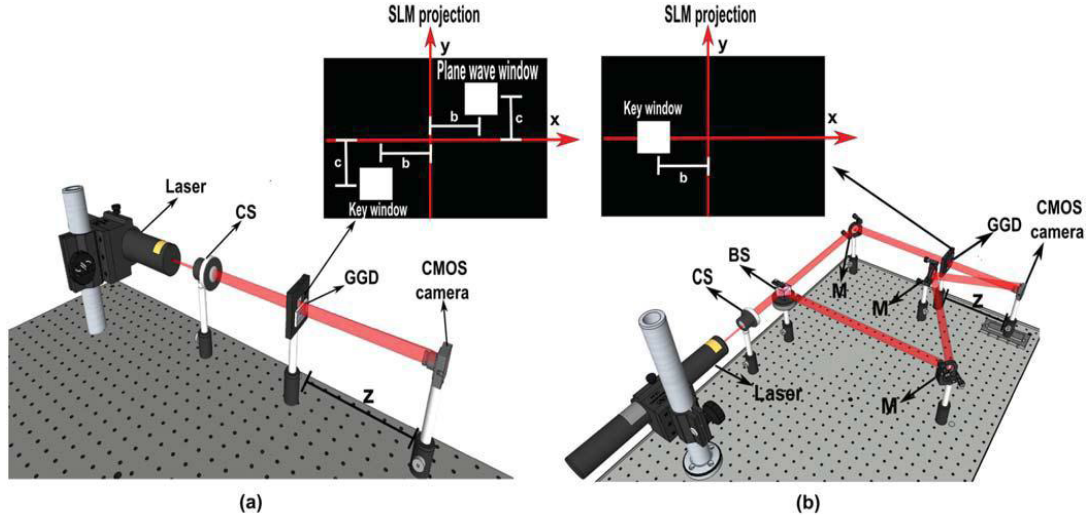


Fig 9. Basic experimental setup used for registering the encryption key in a: (a) compact optical cryptosystem and (b) conventional Fresnel JTC cryptosystem. CS: collimation system; SLM: spatial light modulator; BS: beam splitter; GGD: ground-glass diffuser, and z : distance between SLM and the CMOS camera. Scheme reproduced from Ref [68] with permission from © IOP Publishing.

On the other hand, Fig 9(a) presents the experimental setup used to register the key information in the single-arm JFS cryptosystem [68]. In this configuration, instead of including a separate reference arm to record the encryption-key information, an empty window is projected onto the region of the SLM that is not in contact with the diffuser, providing a plane wave window. When the key and plane-wave windows are projected on the SLM, the input plane is

$$i_s(x, y) = w(x, y) \otimes \delta(x - b, y - c) + k(x, y) \otimes \delta(x + b, y + c) \quad (11)$$

here $w(x, y)$ represents the plane wave window, and c is the separation along the y-axis between plane wave window and the center of the SLM. Therefore, the recorded hologram in the camera detector is

$$J_{zr}(u, v) = |W_z(u, v)|^2 + |K_z(u, v)|^2 + W_z(u, v)K_z^*(u, v)e^{(-4i\pi(bu+cv))} + W_z^*(u, v)K_z(u, v)e^{(4i\pi(bu+cv))}, \quad (12)$$

where $W_z(u, v)$ is the Fresnel transform of $w(x, y)$. The intensity terms $|W_z(u, v)|^2$ and $|K_z(u, v)|^2$ are recorded separately and subtracted from Eq (12), resulting in an expression with only the two cross-terms. After an FT of the result and retaining the desired term, the inverse Fourier transform leads to the Fresnel-domain key

$$K_z(u, v). \quad (13)$$

The decryption process is performed by multiplying the encrypted data by the recovered Fresnel-domain key and then applying an inverse Fresnel transform to obtain the decrypted object.

Figure 10 compares the performance of the single-arm JTC cryptosystem with that of a conventional Fresnel JTC cryptosystem under identical operating conditions [68]. Figures 10(a-c) correspond to the decrypted objects obtained with the single-arm configuration, whereas Figs 10(d-f) show the results recovered using the reference-arm cryptosystem. For the three representative objects tested, both configurations provide comparable reconstruction quality when the correct key and propagation parameters are used, indicating that the removal of the reference arm does not compromise the encryption–decryption process. In addition, any mismatch in the decryption key or propagation conditions leaves the data in an encrypted, noise-like state, so that no recognizable information can be retrieved, which further highlights the security of both architectures. These qualitative observations agree with the correlation-coefficient analysis, confirming that the single-arm JTC cryptosystem maintains reconstruction fidelity while significantly reducing optical complexity [68].

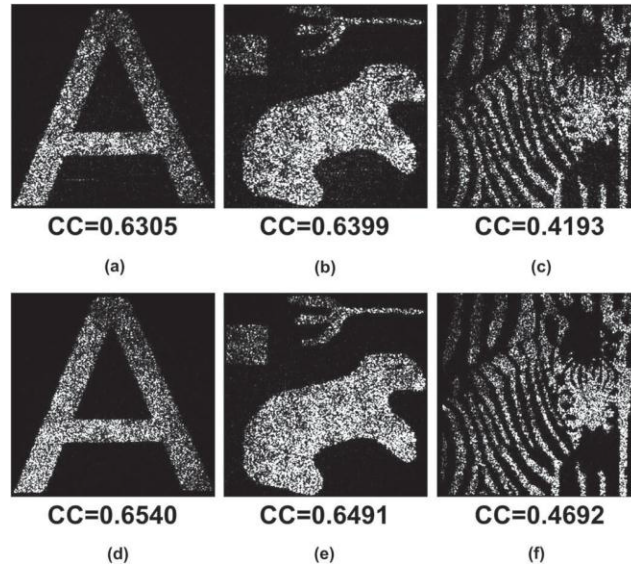


Fig 10. (a-c) Decryption results using the single-arm JTC cryptosystem; (d-f) decryption results with the Fresnel JTC cryptosystem. Experimental results reproduced from Ref [68] with permission from © IOP Publishing.

Accordingly, in the single-arm cryptosystem the same experimental configuration is used to record both the encrypted data and the security-key information, and only the SLM projection is changed (see Figs 8 and 9(a)). As a consequence, the single-arm JFS cryptosystem exhibits a more compact architecture than the conventional JFS cryptosystem, since it requires only a collimated light source, an SLM, and a recording

medium. This reduces the possible sources of aberrations, relaxes the stability and alignment requirements of the arrangement, simplifies the operation of the encrypting system, and additionally lowers the overall cost of the experimental setup.

5.2 Experimental single-arm JTC cryptosystem implementations

A series of experimental contributions have investigated different aspects of single-arm JTC cryptosystems, including a master-key strategy, compact implementations without a physical reference arm, multiple encrypted data recording, and iterative key-retrieval procedures. In what follows, we summarize the main results of these works and discuss the experimental configurations they employ, emphasizing their advantages in the context of opto-digital JTC encryption.

An experimental master-key generation protocol is implemented in a Fourier-domain JTC cryptosystem to avoid the use of a reference wave during the encryption stage. In an initial step, a random phase mask is holographically recorded in an interferometric arrangement to obtain the Fourier transform of a master key, which is stored as a hologram. Once the master key has been generated, subsequent encryptions are carried out in a conventional JTC architecture without a physical reference arm, where the master key is used together with the encoding key, so that both are required for successful decryption and the overall security of the protocol is enhanced [67].

In another study, a compact single-arm optical cryptosystem is implemented in which both the encrypted data and the security key are recorded without a reference arm, thus reducing the size and complexity of the setup [68]. The system operates as a Fresnel-domain joint transform architecture that uses an SLM in contact with a ground-glass diffuser together with a plane-wave window on the diffuser-free region of the SLM. Its performance is assessed by encrypting and decrypting different inputs, by testing robustness against noise and data loss, and by encoding the data to be encrypted by means of a customized data container for optical security, achieving a 97% reduction in the data volume of the encrypted information while allowing noise-free recovery.

In the same single-arm free-space framework, a secure selective recovery protocol for multiple optically encrypted data is implemented, in which each encrypted object is sampled with an orthogonal random binary mask and all sampled data are multiplexed into a single package. Selective access is achieved by multiplying the multiplexed data with the corresponding mask and applying the standard decryption process, so that each object is recovered without crosstalk, whereas an unauthorized user only observes the overlap of all encrypted information. The protocol is experimentally validated by encrypting an optical keyboard and testing its performance under occlusion, random noise, and holographic projection for selective reconstruction [69].

In a further step toward reference-free operation, an opto-digital cryptosystem based on JTC architecture is implemented to record the key without a reference beam, phase-shifting techniques, or an additional window in the input plane. Only two intensity recordings are required: the intensity of the key Fourier transform and the JPS between the key and an arbitrary object in contact with a random phase mask. These data, together with the known input amplitudes, are used in a modified Gerchberg–Saxton algorithm that recovers the phase of the encryption key, as confirmed by numerical simulations and optical experiments [70].

Finally, a ptychographic key-retrieval method is implemented in an experimental JTC cryptosystem to record the key without using a reference beam, phase-shifting methods, or an additional window in the input plane. In this approach, the key is illuminated with different probes, and its phase is reconstructed from the probe information and the corresponding cryptosystem outputs by means of a ptychographic algorithm. Two probes are sufficient to obtain a key that enables successful decryption, whereas additional probes improve the accuracy of the recovered key and the quality of the decrypted objects. The decrypted

objects obtained with the ptychographic key exhibit a quality comparable to those recovered with the key recorded using a reference arm [71].

Overall, these works delineate a clear progression from interferometric JTC architectures with master-key management [67] toward compact single-arm cryptosystems that record both the encrypted data and the key without an external reference arm and can multiplex multiple protected objects in a single package [68,69], and finally to key-recording schemes based on iterative phase retrieval and ptychographic reconstruction [70,71]. These systems provide simple and compact arrangements while enabling selective access and flexible key management, although iterative and ptychographic reconstruction require additional computational processing. This balance between optical compactness, robustness, and numerical complexity characterizes the current generation of single-arm JTC cryptosystems, consolidating these approaches as experimentally viable alternatives that complement the developments reported for Fourier, Fresnel, and fractional-domain architectures. In particular, the analysis of compact JTC configurations operating without reference arms highlights these single-arm schemes as especially attractive candidates for future optical encryption platforms [67-71].

The adaptability of the joint transform correlator cryptosystem is evidenced by its successful implementation across multiple transform domains and its capacity to process a wide range of information. By incorporating distinct physical parameters, JTC-based systems achieve enhanced security and functionality. A clear evolution toward more compact architectures has reduced operational constraints while preserving robust performance, positioning these opto-digital cryptosystems as practical and versatile solutions for protecting information.

6 Conclusions and discussion

This review presents a comprehensive analysis of experimentally demonstrated opto-digital joint transform correlator (JTC) cryptosystems implemented in the Fourier, Fresnel, fractional, and single-arm configurations. The accumulated evidence from more than two decades of research confirms that the JTC architecture constitutes one of the most versatile and experimentally accessible platforms for optical encryption. Its ability to operate with compact optical systems and incorporate physical parameters as security keys has enabled a broad spectrum of encryption strategies that extend far beyond the classical double random phase encoding framework. Fourier-domain JTC implementations have matured into robust opto-digital architectures capable of supporting multiplexed data containers, grayscale and color information, dynamic sequences, multi-plane objects, and real random-phase masks. These systems benefit from simple setups, often requiring only a lens, a diffuser, an SLM, and a camera, while numerical post-processing provides flexible control over filtering and reconstruction. Nonetheless, their performance critically depends on controlling random-correlation noise, managing the spatial distribution of encrypted terms, and ensuring high-quality registration of the key, particularly when interferometric recording is required. Fresnel-domain JTC architectures broaden the operational space by eliminating the Fourier lens and introducing the propagation distance as an additional physical parameter. This Fresnel-domain configuration enhances the key space, relaxes optical constraints associated with lens aberrations, and enables propagation-dependent multiplexing and color-sensitive encryption. However, the Fresnel domain exhibits more speckle noise and greater sensitivity to alignment and sampling conditions, which must be carefully analyzed when designing experimental implementations.

Fractional-domain JTC cryptosystems further extend these capabilities by incorporating the fractional Fourier transform as a tunable operator. The fractional order acts simultaneously as a geometric parameter and a security key, enabling multiuser operation, and fine control over noise sensitivity. Experimental implementations using digital holography, thermal lenses, and electrically tunable lenses demonstrate that FrFT-based systems can be implemented with excellent reconstruction quality while offering fast

reconfigurability and enhanced security. Some of the main challenges are the precise calibration of the fractional order, numerical sampling requirements, and the increased computational requirements associated with iterative schemes.

A significant trend identified in this review is the evolution toward single-arm JTC cryptosystems, which represent a major step toward compact, low-cost encryption systems with relaxed alignment and stability requirements. By recording both the encrypted object and the key without a physical reference arm, these architectures reduce optical complexity while maintaining high decryption quality. Recent developments integrating iterative algorithms and ptychographic reconstruction confirm that high-quality complex keys can be recovered even in the absence of a reference arm. These approaches consolidate single-arm architectures as experimentally viable alternatives that complement the developments reported for Fourier, Fresnel, and fractional-domain JTC cryptosystems.

Overall, the experimental results discussed in this review demonstrate that JTC-based optical encryption remains a vibrant and rapidly evolving area of research. The combination of compact architectures, tunable physical parameters, and powerful opto-digital processing provides a unique framework for secure information handling across a wide range of applications. Continued progress in optical devices and architectures, computational phase retrieval, and wavefront-control technologies is expected to lead to increasingly robust, scalable, and portable optical cryptosystems, positioning JTC-based architectures as central components of next-generation physical-layer security solutions.

Acknowledgments

Comité para el Desarrollo de la Investigación—CODI (Universidad de Antioquia—UdeA, Colombia).

References

1. Matoba O, Nomura T, Perez-Cabre E, Millan M S, Javidi B, Optical techniques for information security, *Proc IEEE*, 97(2009)1128–1148.
2. Alfalou A, Brosseau C, Optical image compression and encryption methods, *Adv Opt Photon*, 1(2009)589–636.
3. Graydon O, Quick response codes, *Nat Photon*, 7(2013)343; doi.org/10.1038/nphoton.2013.127.
4. Barrera-Ramírez J F, Tebaldi M, Torroba R, Experimental double random phase encoding technique under a joint transform correlator architecture, *Asian J Phys*, 22(2013)135–152.
5. Situ G, Zhang J, Advances in optical security systems, *Adv Opt Photon*, 6(2014)120–155.
6. Zhang Y, Wang X, A review of optical image encryption techniques, *Opt Laser Technol*, 57(2014)327–342.
7. Javidi B, Carnicer A, Yamaguchi M, Nomura T, Pérez-Cabré E, Millán M S, Nishchal N K, Torroba R, Barrera-Ramírez J F, He W, Peng X, Stern A, Rivenson Y, Alfalou A, Brosseau C, Guo C, Sheridan J T, Situ G, Naruse M, Matsumoto T, Juvells I, Tajahuerce E, Lancis E, Chen W, Chen X, W H Pinkse P, Mosk A P, Markman A, Roadmap on optical security, *J Opt*, 18(2016)083001; doi.org/10.1088/2040-8978/18/8/083001.
8. Carnicer A, Javidi B, Optical security and authentication using nanoscale and thin-film structures, *Adv Opt Photon*, 9(2017)218–256.
9. Refregier F, Javidi B, Optical image encryption based on input plane and Fourier plane random encoding, *Opt Lett*, 20(1995)767–769.
10. Javidi B, Zhang G, Li J, Experimental demonstration of the random phase encoding technique for image encryption and security verification, *Opt Eng*, 35(1996)2506–2512.
11. Unnikrishnan G, Joseph J, Singh K, Optical encryption using phase conjugation in a photorefractive crystal, *Appl Opt*, 31(1998)8181–8186.
12. Barrera-Ramírez J F, Henao R, Tebaldi M, Torroba R, Bolognini N, Multiple image encryption using an aperture-modulated optical system, *Opt Commun*, 261(2006)29–33.
13. Barrera-Ramírez J F, Henao R, Tebaldi M, Torroba R, Bolognini N, Multiplexing encrypted data by using polarized light, *Opt Commun*, 260(2006)109–112.

14. Barrera-Ramírez J F, Henao R, Tebaldi M, Torroba R, Bolognini N, Multiplexing encryption–decryption via lateral shifting of a random phase mask, *Opt Commun*, 259(2006)532–536.
15. Barrera-Ramírez J F, Henao R, Tebaldi M, Torroba R, Bolognini N, Code retrieval via undercover multiplexing, *Optik*, 119(2008)139–142.
16. Nomura T, Javidi B, Optical encryption using a joint transform correlator architecture, *Opt Eng*, 39(2000)2031–2035.
17. Nomura T, Mikan S, Morimoto Y, Javidi B, Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator, *Appl Opt*, 42(2003)1508–1514.
18. Tebaldi M, Horrillo S, Pérez-Cabré E, Millán M S, Amaya D, Torroba R, Bolognini N, Experimental color encryption in a joint transform correlator architecture, *J Phys Conf Ser*, 274(2011)012054; doi.org/10.1088/1742-6596/274/1/012054.
19. Lu D, Jin W, Color image encryption based on joint fractional Fourier transform correlator, *Opt Eng*, 50(2011)068201; doi.org/10.1117/1.3590724.
20. Barrera-Ramírez J F, Tebaldi M, Amaya D, Furlan W D, Monsoriu J A, Bolognini N, Torroba R, Multiplexing of encrypted data using fractal masks, *Opt Lett*, 37(2012)2895–2897.
21. La Mela C, Iemmi C, Optical encryption using phase-shifting interferometry in a joint transform correlator, *Opt Lett*, 31(2006)2562–2564.
22. Henao R, Rueda E, Barrera-Ramírez J F, Torroba R, Noise-free recovery of optodigital encrypted and multiplexed images, *Opt Lett*, 35(2010)333–335.
23. Velez-Zea A, Barrera-Ramírez J F, Torroba R, Three-dimensional joint transform correlator cryptosystem, *Opt Lett*, 41(2016)599–602.
24. Velez-Zea A, Barrera-Ramírez J F, Torroba R, Optimized random phase encryption, *Opt Lett*, 43(2018)3558–3561.
25. Barrera-Ramírez J F, Tebaldi M, Ríos C, Rueda E, Bolognini N, Torroba R, Experimental multiplexing of encrypted movies using a JTC architecture, *Opt Express*, 20(2012)3388–3393.
26. Rueda E, Barrera-Ramírez J F, Henao R, Torroba R, Optical encryption with a reference wave in a joint transform correlator architecture, *Opt Commun*, 282(2009)3243–3249.
27. Rueda E, Ríos C, Barrera-Ramírez J F, Henao R, Torroba R, Experimental multiplexing approach via code key rotations under a joint transform correlator scheme, *Opt Commun*, 284(2011)2500–2504.
28. Barrera-Ramírez J F, Rueda E, Ríos C, Tebaldi M, Bolognini N, Torroba R, Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality, *Opt Commun*, 284(2011)4350–4355.
29. González-Moncada J A, Velez-Zea A, Barrera-Ramírez J F, Multiplane experimental optical data encryption using phase-only holography, *Opt Laser Eng*, 188(2025)108900; doi.org/10.1016/j.optlaseng.2025.108900.
30. González-Moncada J A, Velez-Zea A, Barrera-Ramírez J F, Experimental optical encryption with full complex modulation, *Appl Opt*, 63(2024)4182–4191.
31. Velez-Zea A, Barrera-Ramírez J F, Torroba R, Secure real-time generation and display of color holographic movies, *Opt Laser Eng*, 122(2019)239–244.
32. Jaramillo A, Barrera-Ramírez J F, Montoya S, Mira-Agudelo A, Velez-Zea A, Torroba R, Improved decryption quality with a random reference beam cryptosystem, *Opt Laser Eng*, 112(2019)119–127.
33. Velez-Zea A, Barrera-Ramírez J F, Torroba R, Cryptographic salting for security enhancement of double random phase encryption schemes, *J Opt*, 19(2017)105703; doi.org/10.1088/2040-8986/aa8738.
34. Velez-Zea A, Barrera-Ramírez J F, Torroba R, Experimental optical encryption of grayscale information, *Appl Opt*, 56(2017)5883–5889.
35. Velez-Zea A, Barrera-Ramírez J F, Torroba R, Innovative speckle noise reduction procedure in optical encryption, *J Opt*, 19(2017)055704; doi.org/10.1088/2040-8986/aa6526.
36. Barrera-Ramírez J F, Mira-Agudelo A, Torroba R, Experimental QR code optical encryption: noise-free data recovering, *Opt Lett*, 39(2014)3074–3077.
37. Barrera-Ramírez J F, Velez-Zea A, Torroba R, Experimental scrambling and noise reduction applied to the optical encryption of QR codes, *Opt Express*, 22(2014)20268–20277.
38. Velez-Zea A, Barrera-Ramírez J F, Torroba R, Customized data container for improved performance in optical cryptosystems, *J Opt*, 18(2016)125702; doi.org/10.1088/2040-8978/18/12/125702.

39. Trejos S, Barrera-Ramírez J F, Velez-Zea A, Tebaldi M, Torroba R, Optical approach for the efficient data volume handling in experimentally encrypted data, *J Opt*, 18(2016)065702; doi.org/10.1088/2040-8978/18/6/065702.
40. Trejos S, Barrera-Ramírez J F, Torroba R, Optimized and secure technique for multiplexing QR code images of single characters: Application to noiseless messages retrieval, *J Opt*, 17(2015)085702; doi.org/10.1088/2040-8978/17/8/085702.
41. Trejos S, Barrera-Ramírez J F, Tebaldi M, Torroba R, Experimental optodigital processing of multiple data via modulation, packaging, and encryption, *J Opt*, 16(2014)055402; doi.org/10.1088/2040-8978/16/5/055402.
42. Barrera-Ramírez J F, Trejos S, Tebaldi M, Torroba R, Experimental protocol for packaging and encrypting multiple data, *J Opt*, 15(2013)055406; doi.org/10.1088/2040-8978/15/5/055406.
43. Barrera-Ramírez J F, Velez-Zea A, Torroba R, Experimental multiplexing protocol to encrypt messages of any length, *J Opt*, 15(2013)055404; doi.org/10.1088/2040-8978/15/5/055404.
44. Rueda E, Barrera-Ramírez J F, Henao R, Torroba R, Lateral shift multiplexing with a modified random mask in a JTC encrypting architecture, *Opt Eng*, 48(2009)027006; doi.org/10.1117/1.3080753.
45. Liu Y, Shen X, Zhou B, Liu J, Cai J, Liu X, Cheng Y, Optical asymmetric JTC cryptosystem based on binary phase modulation and image superposition–subtraction operation, *Appl Opt*, 61(2022)8711–8729.
46. Chen C L, Lin L C, Cheng C J, Design and implementation of an optical joint transform encryption system using complex-encoded key mask, *Opt Eng*, 47(2008)068201; doi.org/10.1117/1.2943269.
47. Liu J, Bai T, Shen X, Dou S, Lin C, Cai J, Parallel encryption for multi-channel images based on an optical joint transform correlator, *Opt Commun*, 396(2017)174–184.
48. Chen Q, Shen X, Experimental research on JTC encryption system based on spiral phase mask and its characteristics, *Opt Commun*, 427(2018)123–131.
49. Chen Q, Shen X, Dou S, Lin C, Wang L, Topological charge number multiplexing for JTC multiple-image encryption, *Opt Commun*, 412(2018)155–160.
50. Vilardy J M, Millán M S, Pérez-Cabrè E, Experimental optical encryption scheme for the double random phase encoding using a nonlinear joint transform correlator, *Optik*, 217(2020)164653; doi.org/10.1016/j.ijleo.2020.164653.
51. Chen Q, Shen X, Cheng Y, Lin C, Liu Y, Zhou B, A security-enhanced joint transform correlator optical encryption system with cropping operation, *Optik*, 245(2021)167654; doi.org/10.1016/j.ijleo.2021.167654.
52. Chen Q, Shen X, Cheng Y, Huang F, Lin C, Liu H X, Joint-transform Correlator Multiple-image Encryption System Based on Quick-response Code Key, *Curr Opt Photon*, 3(2019)320–328.
53. Peng K, Shen X, Huang F, He X, A Joint Transform Correlator Encryption System Based on Binary Encoding for Grayscale Images, *Curr Opt Photon*, 3(2019)548–554.
54. Muravsky L I, Kulynych Y P, Maksymenko O P, Voronyak T I, Pogan I Y, Vladimirov F L, Kostyukevych S A, Fitio V M, Performance of optical and hybrid joint transform correlators for tasks of optical security, *Semicond Phys Quantum Electron Optoelectron*, 5(2002)222–230.
55. Park S-J, Kim J-Y, Bae J-K, Kim S-J, Fourier-plane encryption technique based on removing the effect of phase terms in a joint transform correlator, *Opt Rev*, 8(2001)413–415.
56. Shen X, Liu X, Yin J, Lu X, Kong D, Lin C, Joint Fresnel transform correlator based on double optical wedges, *Opt Commun*, 339(2015)243–246.
57. Barrera-Ramírez J F, Jaramillo A, Velez-Zea A, Torroba R, Experimental analysis of a joint free space cryptosystem, *Opt Laser Eng*, 83(2016)126–130.
58. Shen X, Dou S, Lei M, Chen Y, Optical image encryption based on a joint Fresnel transform correlator with double optical wedges, *Appl Opt*, 55(2016)8513–8522.
59. Li S, Shen X, Zhou B, Wang L, Noiseless optical encryption based on a complex secret key and a joint Fresnel transform correlator with a Billet split lens, *Appl Opt*, 57(2018)6503–6509.
60. Dou S, Shen X, Zhou B, Wang L, Lin C, Experimental research on optical image encryption system based on joint Fresnel transform correlator, *Opt Laser Technol*, 112(2019)56–64.
61. Jaramillo-Orsorio A, Velez-Zea A, Cabrera H, Niemela J, Barrera-Ramírez J F, Torroba R, Optical encryption using phase modulation generated by thermal lens effect, *J Opt*, 24(2022)025702; doi.org/10.1088/2040-8986/ac4412.

62. Wang Q, Guo Q, Lei L, Zhou J, Optical image encryption based on joint fractional transform correlator architecture and digital holography, *Opt Eng*, 52(2013)048201; doi.org/10.1117/1.OE.52.4.048201.
63. Wang Q, Guo Q, Lei L, Zhou J, Iterative partial phase encoding based on joint fractional Fourier transform correlator adopting phase-shifting digital holography, *Opt Commun*, 313(2014)1–8.
64. Jaramillo A, Barrera-Ramírez J F, Velez-Zea A, Torroba R, Fractional optical cryptographic protocol for data containers in a noise-free multiuser environment, *Opt Laser Eng*, 102(2018)119–125.
65. Jaramillo-Osorio J A, Torres-Sepúlveda W, Velez-Zea A, Mira-Agudelo A, Barrera-Ramírez J F, Torroba R, Focus-tunable experimental optical cryptosystem, *Opt Laser Technol*, 148(2022)107689; doi.org/10.1016/j.optlastec.2021.107689.
66. Vargas-Castrillón C, Velez-Zea A, Barrera-Ramírez J F, Application of the fractional Fourier transform for decryption in experimental optical cryptosystems, *J Opt*, 26(2024)055601; doi.org/10.1088/2040-8986/ad2eda.
67. Rueda E, Ríos C, Barrera-Ramírez J F, Torroba R, Master key generation to avoid the use of an external reference wave in an experimental JTC encrypting architecture, *Appl Opt*, 51(2012)1822–1827.
68. Jaramillo A, Barrera-Ramírez J F, Montoya S, Mira-Agudelo A, Velez-Zea A, Torroba R, High performance compact optical cryptosystem without reference arm, *J Opt*, 22(2020)035702; doi.org/10.1088/2040-8986/ab68f0.
69. Jaramillo A, Velez-Zea A, Mira-Agudelo A, Barrera-Ramírez J F, Torroba R, Secure selective recovery protocol for multiple optically encrypted data, *Opt Laser Eng*, 137(2020)106383; doi.org/10.1016/j.optlaseng.2020.106383.
70. Vargas-Castrillón C, Velez-Zea A, Barrera-Ramírez J F, Non-interferometric key recording applied to a joint transform cryptosystem, *Opt Lett*, 48(2023)672–675.
71. Vargas-Castrillón C, Velez-Zea A, Barrera-Ramírez J F, Ptychographic key retrieval in an experimental joint transform correlator cryptosystem, *Opt Eng*, 64(2025)018105; doi.org/10.1117/1.OE.64.1.018105.
72. Bian L, Chang X, Jiang S, Yang L, Zhan X, Liu S, Li D, Yan R, Gao Z, Zhang J, Large-scale scattering-augmented optical encryption, *Nat Commun*, 15(2024)9807; doi.org/10.1038/s41467-024-54168-3.
73. Xu N, Qi D, Cheng L, Pan Z, Zhou C, Lin W, Ma H, Yao Y, Shen Y, Deng L, Sun Z, Zhang S, Sparse point spread function-based multi-image optical encryption, *Commun Phys*, 8(2025)184; doi.org/10.1038/s42005-025-02105-1.
74. Lin S, Zhu X, Shen Y, Wang F, Chen X, Gbur G, Cai Y, Yu J, Statistically stationary random light for high-security encryption, *Optica*, 12(2025)1261–1268.
75. Qiu M, Chen J, Chai X, Cheng Z, Yao M, Wen Y, He J, Yang Z, Wang Q, Optical image encryption with photo-thermoelectric device, *Opt Express*, 33(2025)29689–29700.
76. Li J, Kamin S, Zheng G, Neubrech F, Zhang S, Liu N, Addressable metasurfaces for dynamic holography and optical information encryption, *Sci Adv*, 4(2018)eaar6768; doi.org/10.1126/sciadv.aar6768.
77. Lim K T P, Liu H, Liu Y, Yang J K W, Holographic colour prints for enhanced optical security by combined phase and amplitude control, *Nat Commun*, 10(2019)25; doi.org/10.1038/s41467-018-07808-4.
78. Qu G, Yang W, Song Q, Liu Y, Qiu C W, Han J, Tsai D P, Xiao S, Reprogrammable meta-hologram for optical encryption, *Nat Commun*, 11(2020)5484; doi.org/10.1038/s41467-020-19312-9.
79. Georgi P, Wei Q, Sain B, Schlickriede C, Wang Y, Huang L, Zentgraf T, Optical secret sharing with cascaded metasurface holography, *Sci Adv*, 7(2021)eabf9718; doi.org/10.1126/sciadv.abf9718.
80. Zheng P, Dai Q, Li Z, Ye Z, Xiong J, Liu H C, Zheng G, Zhang S, Metasurface-based key for computational imaging encryption, *Sci Adv*, 7(2021)eabg0363; doi.org/10.1126/sciadv.abg0363.
81. Yang H, Ou K, Wan H, Hu Y, Wei Z, Jia H, Cheng X, Liu N, Duan H, Metasurface-empowered optical cryptography, *Mater Today*, 67(2023)424–445.
82. Zhang F, Guo Y, Pu M, Chen L, Xu M, Liao M, Li L, Li X, Ma X, Luo X, Meta-optics empowered vector visual cryptography for high security and rapid decryption, *Nat Commun*, 14(2023)1946; doi.org/10.1038/s41467-023-37510-z.
83. Xing W, Bu C, Zhang Xi, Choi D Y, Li Y, Yue W, Cheng J, Li Z, Chen S, Gao S, Metasurface-enabled optical encryption and steganography with enhanced information security, *Nanophotonics*, 14(2025)1391–1403.
84. Yu Z, Li H, Zhao W, Huang P S, Lin Y T, Yao J, Li W, Zhao Q, Chieh-Wu P, Li B, Genevet P, Song Q, Lai P, High-security learning-based optical encryption assisted by disordered metasurface, *Nat Commun*, 15(2024)2607; doi.org/10.1038/s41467-024-46946-w.

85. Zhang C, Liao M, He W, Peng X, Ciphertext-only attack on a joint transform correlator encryption system, *Opt Express*, 21(2013)28523–28530.
86. CuChe E, Marquet P, Depeursinge C, Spatial filtering for zero-order and twin-image elimination in digital off-axis holography, *Appl Opt*, 39(2000)4070–4075.
87. Goodman J W, *Speckle phenomena in optics: theory and applications*, (SPIE Press, Bellingham), 2013.
88. Torres R, Pellat-Finet P, Torres Y, Fractional convolution, fractional correlation and their translation invariance properties, *Signal Process*, 90(2010)1976–1984.
89. Lohmann A, Mendlovic D, Fractional joint transform correlator, *Appl Opt*, 36(1997)7402–7407.

[Received: 20.12.2025; revised recd: 29.03.2026; accepted: 30.03.2026]



John Fredy Barrera-Ramírez received his B.Sc. degree in Physics, M.Sc. degree in Physics, and Ph.D. degree in Physics from the University of Antioquia (Medellín, Colombia). Since 2006, he has been with the Institute of Physics at the University of Antioquia, where he is currently a Full Professor and Coordinator of the Optics and Photonics Group. He received the international ICO/ICTP Gallieno Denardo Award, jointly conferred by the International Commission for Optics (ICO) and the International Centre for Theoretical Physics (ICTP), Trieste, Italy. He was also selected as a Future Leader at the Science and Technology in Society (STS) Forum in Kyoto, Japan. In addition, he served as a Young TWAS Affiliate of The World Academy of Sciences (TWAS), and as both Junior Associate and Regular Associate of ICTP. Professor Barrera is an OPTICA Senior Member and an SPIE Senior Member. He was included among the “30 scientists under 40” highlighted by LatinAmericanScience.org, and his research has been showcased in prestigious scientific platforms and sections, including the Nature Photonics Research Highlights, IOPselect, OPTICA’s Spotlight on Optics, and the Highlights section of the Journal of Optics. His work has also been featured in the TWAS Annual Report and the article “Roadmap on Optical Security” published in the Journal of Optics. In addition, his publications have appeared several times among the most downloaded articles in OPTICA journals.



Alejandro Velez-Zea obtained his degree in Physics from the University of Antioquia and a Ph.D. in Physics from the Universidad Nacional de La Plata (Argentina), where he conducted his research at the Centro de Investigaciones Ópticas de La Plata. He subsequently completed postdoctoral fellowships at this research center and at the Grupo de Optica y Fotonica of the Universidad de Antioquia. He is currently an Associate Professor at the Institute of Physics of the Universidad de Antioquia, where he teaches experimental physics and conducts research in computer-generated holography and holographic display systems. He is the author of 60 publications in international journals, which have received more than 960 citations. His work has been recognized with distinctions including the OPTICA Global Challenge 2023 award, recognition as a Distinguished Graduate of the Ph.D. in Physics program at the Universidad Nacional de La Plata, selection of one of his articles as a “Spotlight on Optics” by OPTICA Publishing, two honorable mentions in the Alejandro Ángel Escobar Awards, and the Highest-Impact Research Award granted by the Mayor’s Office of Medellín (on two occasions), among others.