

RESEARCH ARTICLE

Metasurface-Based Optical Fractional Fourier Transform: Implementation and Applications

Jiaqi Yu^{1,2} | Shuhan Guo² | Junjie Zhan² | Yifan Shao² | Yubo Wang² | Dingke Wan² | Rui Chen² | Pankaj K. Choudhury² | Gang Bao^{1,3} | Yungui Ma² 

¹School of Mathematical Sciences, Zhejiang University, Hangzhou, Zhejiang, China | ²State Key Lab of Extreme Optical Technology and Instrumentation Centre For Optical and Electromagnetic Research, College of Optical Science and Engineering, International Research Center for Advanced Photonics, Zhejiang University, Hangzhou, Zhejiang, China | ³Center for Interdisciplinary Applied Mathematics, Zhejiang University, Hangzhou, Zhejiang, China

Correspondence: Gang Bao (baog@zju.edu.cn) | Yungui Ma (yungui@zju.edu.cn)

Received: 21 November 2025 | **Revised:** 14 June 2026 | **Accepted:** 15 June 2026

Keywords: fractional Fourier transform | fractional Fourier optics | optical metasurface | image encryption

ABSTRACT

The fractional Fourier transform (FrFT), a generalization of the classical Fourier transform (FT) with a fractional-order parameter, enables flexible tuning between time and frequency domains, making it a powerful tool in signal processing. However, its utility in optics is constrained by the lack of compact, efficient analog implementation platforms, limiting progress in optical information processing. Herein, a compact analog optical FrFT system based on metasurface phase planes able to realize accurate analog FrFT computation is presented. Building on this platform, and leveraging FrFT's unique advantages of tunable fractional orders and independent time-frequency domains, two novel image encryption algorithms are developed: a single-image scheme integrated with Arnold transform for enhanced scrambling, and a dual-image scheme enabled by iterative computation for parallel data processing. Comprehensive numerical calculations, optical simulations, and physical experiments validate the robustness and reliability of the proposed system and algorithms. Notably, the tunable fractional order of FrFT provides a large encryption key space and high key sensitivity, significantly boosting encryption security. This work establishes a versatile analog optical FrFT platform and two high-security encryption schemes, offering a new paradigm for advancing optical information processing, paving the way toward developing practical optical cryptosystems.

1 | Introduction

Fourier optics, based on the Fourier transform (FT), is a frequency-domain analytical approach that simplifies the design, performance optimization, and diffraction analysis of optical systems [1]. It can be used to describe phenomena such as wave propagation, reflection, refraction, and focusing, determining its potency in optical imaging [2–6], holography [7–13], and optical computing [14–19]. However, the limitation of conventional FT to a single time-frequency domain imposes constraints on

frequency-domain operations, particularly for complex spectral scenarios. To overcome this, the fractional Fourier transform (FrFT), an extension and generalization of the classical FT, was proposed. Its promising applications were initially reported in signal processing [20–24] and quantum mechanics [25–27]. Later, Almeida established the standardized form of the FrFT and demonstrated its mathematical properties [28]. Owing to its ability to operate across multiple domains and unique time-frequency transformation capabilities, the FrFT is indispensable in time-frequency filtering [29–31], optical imaging and encryp-

Jiaqi Yu and Shuhan Guo contributed equally to this work.

© 2026 Wiley-VCH GmbH

tion [32–37], and quantum signal processing [38–40]. Particularly in optical image encryption [41–43], the FrFT's tunable order and unique rotational property in the time-frequency plane provide encryption algorithms with a vast key space and strong sensitivity to order variations. Moreover, recent studies have demonstrated that integrating FrFT-based encryption with chaotic algorithms and machine learning techniques can significantly enhance security [44, 45]. However, these advanced algorithms are predominantly realized digitally. This digital paradigm not only exposes ciphertext to interception and replication during network transmission but also faces computational bottlenecks, hindering real-time processing of large-scale data. In contrast, an analog optical FrFT implementation offers a superior alternative by leveraging the intrinsic properties of light. It promises computation at the speed of light and processes entire 2D datasets in a single shot. Crucially, it elevates security beyond the digital realm: encryption keys become physical parameters of the optical system (e.g., lens focal length f , propagation distance z), and the ciphertext is a physical wavefront encoded on a device, significantly increasing the difficulty of digital copying and brute-force attacks. The development of a compact, accurate, and physically robust optical system [46, 47] for analog FrFT computation is therefore a critical step toward next-generation, high-security optical information processing. By performing the transform in parallel as light propagates through passive optical elements, it intrinsically achieves near-zero latency and vastly superior energy efficiency, making it particularly advantageous for real-time, high-throughput applications.

In this work, we present a compact optical system employing metasurface-based phase planes to perform analog computation of FrFT. First, we prove the system's capability to accurately simulate FrFT computation both theoretically and experimentally. Then, leveraging the extensive order space and unique time-frequency transformation properties of the FrFT, we develop two encryption algorithms: a single-image scheme combining the FrFT computation with the Arnold transform, and a dual-image scheme using iterative computation to encode two grayscale images into a single complex amplitude ciphertext, using the FrFT order as the decryption key. This physical method of loading ciphertext and performing decryption avoids risks associated with internet transmission, simultaneously benefiting from the speed and energy efficiency of optical computation. Experimental results demonstrate strong order sensitivity, i.e., small parameter changes lead to significant differences in decryption outcomes. The algorithms exhibit strong robustness, accurately decrypting complex 256-level grayscale images while preserving fine details.

2 | Results

2.1 | Optical Implementation of Analog FrFT Computation

The formula for the α th order FrFT applied to a two-dimensional input function U_{in} defined in the original $z(x,y)$ plane is

$$g(u, v) = F^\alpha [U_{\text{in}}(x, y)] = C_\alpha \iint_{-\infty}^{\infty} K(x, y; u, v) U_{\text{in}}(x, y) dx dy \quad (1)$$

where g represents the output function in the new $w(u,v)$ plane after operation, and the kernel function K and constant C_α are, respectively, written as

$$K(x, y; u, v) = \exp \left(i\pi \frac{u^2 + x^2 + v^2 + y^2}{\tan \Phi_\alpha} \right) \exp \left(-i2\pi \frac{xu + yv}{\sin \Phi_\alpha} \right) \quad (2)$$

$$C_\alpha = \exp \left[-\frac{i\pi}{2} \text{sgn}(\sin \Phi_\alpha) + i\Phi_\alpha \right] |\csc \Phi_\alpha| \quad (3)$$

Here, the term $\Phi_\alpha = \alpha\pi/2$ is a key variable that defines the transform operation with order α , and also, the coordinate correspondence between the original and transformed spaces. $\alpha = 1$ reduces FrFT to conventional FT, characterized by an orthogonal space-momentum domain, when analyzing spatially distributed signals. When $\alpha \neq 1$, the corresponding FrFT domain can be obtained by rotating the orthogonal z - w domain of the FT around the plane axis by an angle Φ_α . Thus, Equation (1) performs a mathematical transform in the z - w complex domain, rather than merely along the real axis in the $z(x,y)$ plane (as is the case for conventional FT). By varying Φ_α , an infinite number of $U_{\text{in}} \rightarrow g$ mappings can be obtained, thereby providing greater selectivity for processing a complex signal, which is vital for image encryption.

Then, we introduce the metasurface-based optical system for performing the analog computation of FrFT. Section S1 provides more details regarding the mathematical process. As Figure 1 illustrates, a collimated laser beam of wavelength λ is incident on the front metasurface (FM) to generate the input function $U_{\text{in}}(x, y)$, and then modulated by passing through an intermediate phase mask (PM), defined by the transmission function $t(\zeta, \eta)$, positioned at a distance z . Ultimately, the propagating light field is projected onto an output imaging screen (IS) placed at the same distance z from the PM. Based on Fresnel diffraction theory, the transmitted field immediately behind PM with a local coordinate (ζ, η) can be expressed as [48]

$$U_{\text{PM}}(\zeta, \eta) = \frac{e^{ik_0 z}}{i\lambda z} t(\zeta, \eta) \iint_{-\infty}^{\infty} U_{\text{in}}(x, y) \cdot \exp \left[\frac{i\pi}{\lambda z} \left((\zeta - x)^2 + (\eta - y)^2 \right) \right] dx dy \quad (4)$$

In the above, $k_0 = 2\pi/\lambda$ is the wavevector in vacuum. As Section S1 addresses, by taking $t(\zeta, \eta) = \exp[i\pi/\lambda \cdot a(\zeta^2 + \eta^2)]$ as a Fourier lens and applying the Gaussian integration [49], the field distribution on the output plane with a local coordinate (u, v) is

$$U_{\text{out}}(u, v) = -\frac{ie^{i2k_0 z}}{\lambda z (2 - z/f)} \iint_{-\infty}^{\infty} U_{\text{in}}(x, y) \cdot \exp \left[\frac{i\pi}{\lambda z} \left(\frac{1 - z/f}{2 - z/f} \right) (x^2 + u^2 + y^2 + v^2) \right] \cdot \exp \left[-\frac{i2\pi}{\lambda z (2 - z/f)} (xu + yv) \right] dx dy \quad (5)$$

where $f = -1/a$ is the focal length of the middle PM lens. We see that Equation (5) will exactly replicate Equation (1) by taking the

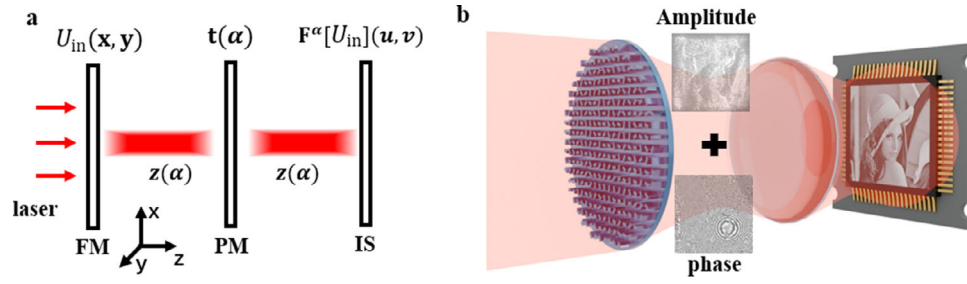


FIGURE 1 | Schematics of the optical FrFT and its application in image encryption. (a) The optical system for an α -order FrFT consists of a front metasurface (FM) at the input plane, a middle phase mask (PM), and a back imaging screen (IS) at the output plane. The FM generates the input function $U_{in}(x, y)$ under the incidence of a laser beam. (b) Schematic of the image encryption scheme based on the aforementioned optical system. The complex amplitude ciphertext is encoded onto the front metasurface; the decrypted image can be observed at the output plane by irradiating the system with a collimated laser beam of the target wavelength.

following coefficient correspondence relationships:

$$\frac{P_{\text{math}}^2}{\sin\Phi_\alpha} = \frac{P_{\text{opt}}^2}{\lambda z(2 - z/f)} \quad (6)$$

$$\frac{P_{\text{math}}^2}{\tan\Phi_\alpha} = \frac{P_{\text{opt}}^2}{\lambda z} \left(\frac{1 - z/f}{2 - z/f} \right) \quad (7)$$

Here, the coefficients P_{math} ($= N^{-1/2}$, with N representing the sampling number [50]) and P_{opt} denote the mesh period for discretizing the continuous coordinates of Equation (1) (mathematical target) and Equation (5) (optical analogue), respectively. From Equations (6) and (7), the focal length f of the middle phase lens and the spacing z can be determined once the fractional order α , operating wavelength λ , sampling number N and optical period P_{opt} are known. In other words, the optical system for FrFT is more customizable than that of the conventional FT, making it more sensitive to manufacturing and system errors. These characteristics, in turn, endow it with significant application advantages in the field of encrypted imaging.

In Section S2 and Figure S1a,b, we validate the above optical FrFT framework using the standard “Lena” and “Cameraman” images as target, taking their $-\alpha$ -th order FrFT as the original inputs. We compare the α -th order FrFT results obtained via numerical computation and scalar diffraction methods using Equation (5), confirming their consistency, and thus, demonstrating the accuracy of FrFT simulation. Our analysis reveals that the peak signal-to-noise ratio (PSNR) as a metric of image quality degrades rapidly with order deviation. The “Lena” image, which contains more grayscale levels and complex details, shows higher sensitivity to order variations. Only ± 0.05 order shift causes the PSNR to decrease by ~ 15 dB, making the image entirely unrecognizable.

2.2 | FrFT for Optical Image Encryption

The availability of a continuous fractional order and independence between domains makes the FrFT especially well-suited for image encryption. We first present a single-image encryption algorithm combining the FrFT with the Arnold transform, a widely used digital image encryption technique [51]. The

encryption process begins with Arnold transform

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \quad (8)$$

where (x, y) and (x', y') represent pixel coordinates before and after transformation, respectively. The transformed image undergoes FrFT computation to produce the ciphertext $I_{\text{en}} = F^{-\alpha}(I')$. Decryption applies an inverse FrFT $I_{\text{de}} = F^{\alpha}(I_{\text{en}})$ followed by an inverse Arnold transform

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \quad (9)$$

Using our FrFT optical implementation, we can also replace the digital FrFT computation in decryption. In Figure S1c, we show the decrypted result for “Lena” image with $\alpha = 0.4$, confirming the effectiveness of the proposed method. After undergoing the FrFT and Arnold scrambling, the images become unrecognizable, with the intermediate decryption results remaining obscured until the final step. Figure S1d compares the histogram distributions of the original images and their corresponding ciphertexts, revealing completely distinct grayscale distributions with low correlation—this prevents information extraction from the ciphertexts. Additionally, the extensive order space of FrFT enables “one-image-one-code” encryption, thereby ensuring high security.

Next, we propose a dual-image encryption scheme that encrypts two grayscale images into a single ciphertext image. This is followed by the design of distinct optical systems corresponding to two decryption fractional orders for reconstructing the original images. The specific encryption orders, unique optical element parameters, and intrinsic properties of the FrFT itself collectively ensure the security of the encryption method. The workflow of this method is outlined as follows: Let I_1 and I_2 denote two 2D grayscale images, and h represents the corresponding ciphertext image. Additionally, φ_1 , φ_2 and φ are three phase functions defined over $[0, 2\pi]$. The iterative encryption algorithm [52] using FrFT needs to satisfy the equation

$$h \exp(i\varphi) = F^{-\alpha}[I_1 \exp(i\varphi_1)] = F^{-\beta}[I_2 \exp(i\varphi_2)] \quad (10)$$

Algorithm 1 | Dual image Encryption Algorithm

Require: Input I_1, I_2, α, β
Initialize $\varphi_1 \leftarrow 0$
Initialize $\varphi_2 \leftarrow 0$
For $MSE > threshold$ **do**
 $\varphi_2^k = \text{angel}\{F^{\beta-\alpha}\{I_1 \exp(i\varphi_1^k)\}\}$
 $I_2^k = \text{amplitude}\{F^{\beta-\alpha}\{I_1 \exp(i\varphi_1^k)\}\}$
 $MSE = [I_2^k - I_2]^2 / (N \times N)$
 $\varphi_1^{k+1} = \text{angel}\{F^{\alpha-\beta}\{I_2 \exp(i\varphi_2^k)\}\}$
End for
Return φ_1, φ_2
Calculate h, φ

Here, α and β represent the specific encryption orders that are pre-determined. Then, an iterative phase retrieval algorithm is utilized to obtain the precise ciphertext amplitude h and ciphertext phase φ (Algorithm 1 provides the detailed procedure). Specifically, we employed a Gerchberg-Saxton-like algorithm, which shares the core principle of iteratively enforcing known amplitude constraints across different domains while allowing the phase to evolve. As detailed in Algorithm 1, for any two given grayscale images acting as target amplitudes I_1 and I_2 , the algorithm starts with a random phase φ for the ciphertext field h . In each iteration, the fields in the two decryption domains are calculated via the FrFT of orders α and β . It then replaces the calculated amplitudes with the target amplitudes I_1 and I_2 , respectively, while retaining the calculated phases (φ_1 and φ_2). These updated fields are subsequently inverse-transformed back to the ciphertext domain, and their combination is utilized to update the ciphertext phase φ for the next iteration. This deterministic process ensures full reproducibility and continues iterating until the Mean Squared Error (MSE) between the calculated and target amplitudes falls below 10^{-3} , which typically converges within 40–50 iterations. For a 512×512 image, the total computation time is approximately 3–4 min on a personal computer (Intel Core i7-12700H, 16 GB RAM), with the cost dominated by the two FrFT operations per iteration.

Lastly, the decryption process is carried out by applying the FrFT to the ciphertext, i.e.,

$$I_1 = \text{amplitude}\{F^\alpha[h \exp(i\varphi)]\} \quad (11)$$

$$I_2 = \text{amplitude}\{F^\beta[h \exp(i\varphi)]\} \quad (12)$$

As Figure 1b shows, we use the complex amplitude $h \exp(i\varphi)$ as the ciphertext after iterative convergence. By passing it through two different optical systems with individual (z, f) pairs, two distinct decrypted images can be obtained on their own imaging plane (according to the orders α and β). Figure 2a presents the original images, and the decrypted images obtained through numerical and optical scalar diffraction calculations in the dual-image encryption algorithm. Good agreement between these results validates the optical system defined by Equations (6) and (7) implementing the FrFT computation. The discrepancies between the decrypted and original images mainly arise from convergence errors during the encryption iteration (Equation 10). Consequently, a moderate PSNR (e.g., 19.8 dB for ‘OPT’) repre-

sents a theoretical upper limit for this dual-image multiplexing algorithm. However, rather than absolute fidelity, the crucial metric for image encryption is the sharp contrast between a clearly recognizable image for authorized users and complete noise for unauthorized access, which our results robustly demonstrate.

We also quantitatively evaluated the sensitivity of the encryption method to the key (i.e., the order) using PSNR. In addition to the two-letter images discussed above, we calculated the PSNR of the decryption images for three different types of encrypted images under the same key set (combinedly $\alpha = 0.46$ and $\beta = 0.63$). These typical images include English letters such as ‘ZJU,’ ‘OPT,’ and ‘MATH’ Chinese text written as ‘qiu shi zhi guang’ numbers like ‘120’ and a more complex image resembling an eagle labeled ‘qiu shi eagle,’ with smaller feature sizes and increasing levels of detail. As Figure 2b shows, the PSNR curves vary among the encrypted image types. A smaller minimum feature size and higher resolution of the original image lead to a smaller full width at half maximum (FWHM) in the corresponding PSNR curve, reflecting higher key sensitivity and increased difficulty in decryption. The smallest FWHM observed is ~ 0.04 , which indicates that a deviation of only ± 0.02 orders is permissible. For subsequent optical experiments, we incorporated specific experimental parameters into the numerical simulations to obtain PSNR curves under the conditions of wavelength $\lambda = 1064$ nm, equivalent optical period $P_{\text{opt}} = 9.34$ μm , and the image resolution of 512×512 . As Figure 2c shows, the solid line represents the PSNR curve of the decrypted result obtained via mathematical calculations, while the dashed line represents the PSNR curve of the decrypted result obtained via optical scalar diffraction. The figure clearly shows that the two curves match well, demonstrating that the decryption results obtained via optical simulation of the FrFT possess the same strong-order sensitivity as those derived from numerical computations. For the target order $\alpha = 0.46$, when the implementation order deviates from 0.46 to 0.42 or 0.5, the decrypted result becomes unclear. Similarly, for the target order $\beta = 0.63$, setting the implementation order to 0.6 or 0.67 also reduces decryption accuracy. To further assess possible structural information under incorrect decryption orders, we calculated the NCC and SSIM between the original and decrypted images, with detailed definitions and analysis provided in Section S7. As shown in Figure S4, both metrics exhibit high values near the correct orders, while deviations from the correct orders lead to reduced correlation and structural similarity. Together with the representative decrypted images, these results indicate that the incorrectly decrypted outputs do not stably reproduce the original letter structures, although weak similarity may remain for small order deviations. This clearly demonstrates high key sensitivity of the method implemented and indicates that, in the case of an unknown key, an attacker would need to design and fabricate a considerable number of optical components, resulting in substantial time and financial costs.

Additionally, we examined the effects of varying the optical system parameters f and z , which depend on the key. As Figure 2d shows, each contour line of the same color represents the same PSNR value, illustrating how these parameters affect the image quality. From the PSNR value displayed in the figure, we can observe that, when f or z deviates from the correct value by 5%, the decryption result becomes blurred, and the accurate result

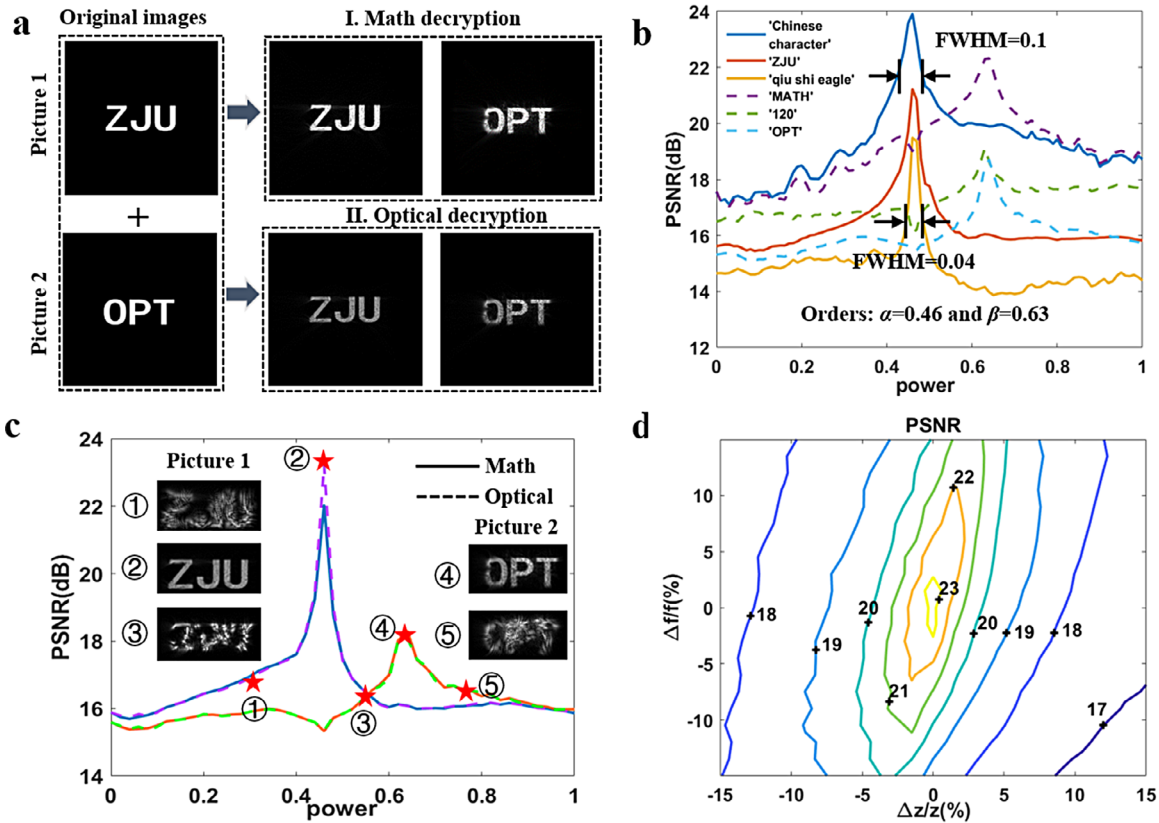


FIGURE 2 | FrFT-based optical encryption and robustness analysis. (a) Original image, numerically decrypted image, and scalar diffraction decrypted image of dual-image (patterns of ZJU and OPT) encryption algorithm. (b) Effect of the decryption order on the PSNR of different image patterns. (c) Comparison of numerical decryption and scalar diffraction decryption for the 'ZJU' and 'OPT' images. (d) Effect of the two optical parameters (z, f) on the PSNR of the decryption images.

can no longer be identified. This demonstrates that the method exhibits high sensitivity not only to the system parameters, but also to the precise alignment of the optical components, thereby greatly increasing the difficulty of decryption.

2.3 | Experimental Implementation

To explicitly illustrate how the physical profiles of the metasurfaces are mathematically derived from the target FrFT orders, we present the Metasurface Profile Design Workflow in Section S7. For the basic FrFT calculation (Figure 3a), the system consists of two metasurfaces. MS1 simultaneously modulates both amplitude and phase, which are designed to exactly match the complex amplitude of the $-\alpha$ order FrFT of the target image. MS2 is a phase-only metasurface encoding a standard lens phase. Crucially, the focal length f of this lens is directly determined by the target operational order α through Equations (6) and (7) thereby establishing a deterministic link between the FrFT order and the metasurface phase profile. Conversely, for the encryption setup (Figure 3c), a single complex-amplitude metasurface is employed as the ciphertext carrier. Its amplitude h and phase ϕ are directly extracted from the outputs of Algorithm 1. Because the iterative computation within Algorithm 1 fundamentally relies on the predefined encryption fractional orders (α_1 and α_2), the physical structure of the encrypted metasurface is intrinsically bound to these specific keys.

Here, Figure 3a,b illustrate the optical setup and experimental results. With the operating wavelength of 1064 nm, fractional order $\alpha = 0.3$, equivalent optical period $P_{\text{opt}} = 1.48 \mu\text{m}$, and 512×512 image resolution, Equations (6) and (7) provides the focal length $f = 2080 \mu\text{m}$ and spacing $z = 226 \mu\text{m}$. The experimental results confirm that our single-phase-plane design accurately performs the FrFT computation at the target order, yielding images with high clarity and computational precision.

Meanwhile, based on the numerical simulations described above, we designed the optical setup for dual-image decryption, as Figure 3c depicts. Upon entering the system, the incident light is first attenuated, then passes through an aperture, and is converted into the x -polarized light by a linear polarizer. The processed light then passes through a beam expander before interacting with the metasurface sample. After undergoing optical periodic matching, the encoded output light is then magnified by a microscope system. Finally, the focused light converges onto the imaging plane at a predetermined location, completing the decryption process via a lens with a specific focal length.

Figure 3d shows the amplitude and phase maps corresponding to the ciphertext of target images. We employed a metasurface composed of silicon pillars acting as half-wave plates to generate the amplitude and phase of the ciphertext, with detailed structural parameters as in Figure 3e. The metasurface's performance hinges on its precise geometry. It features 810 nm-tall amorphous

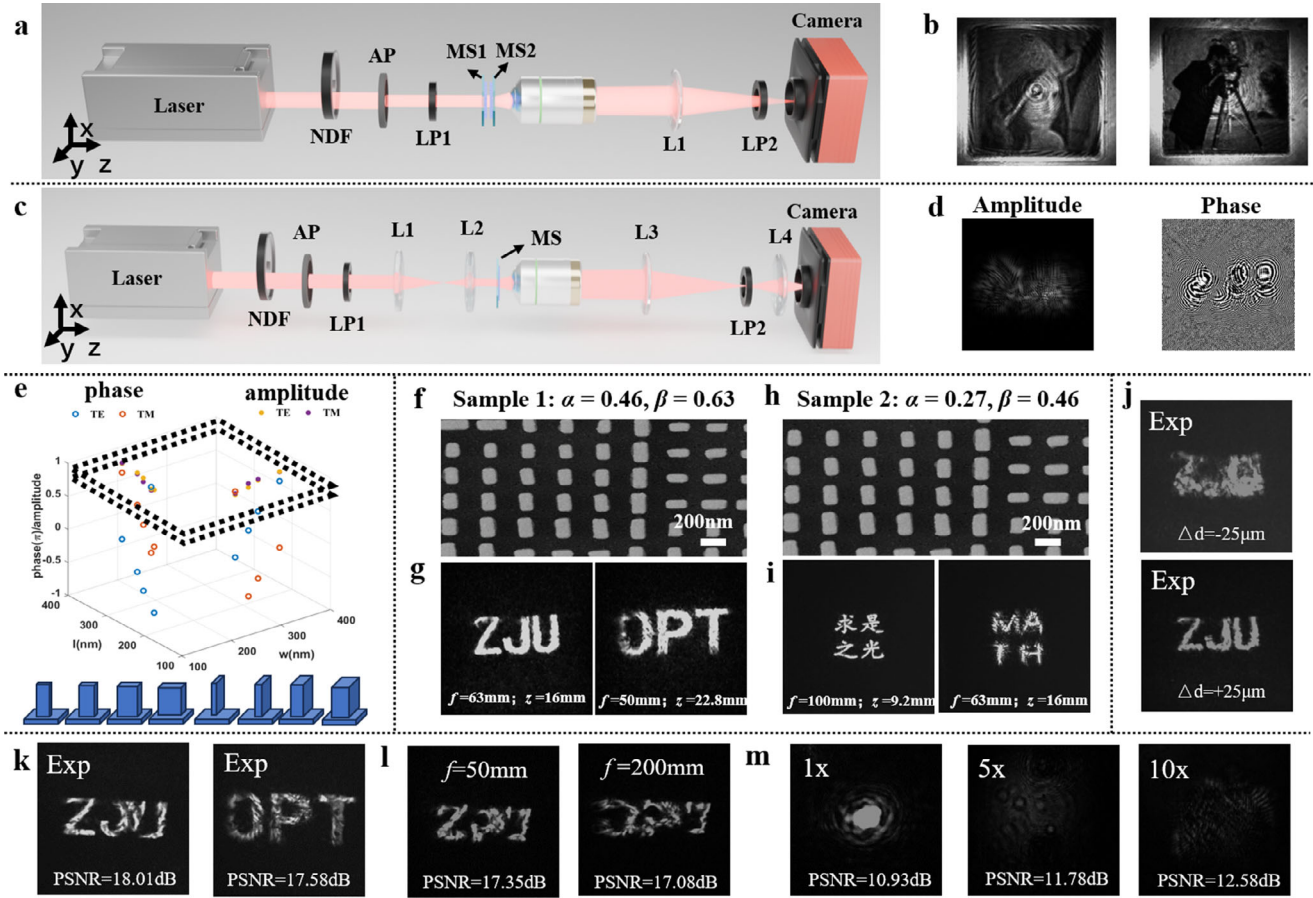


FIGURE 3 | Setup and measurement results. (a) Schematic diagram of the optical system used in the FrFT calculation. (NDF: neutral density filters; AP: aperture; LP: linear polarizer; MS: metasurface; L: lens) (b) Experimental result of the FrFT calculation. (c) Schematic diagram of the optical system used in the decryption process. (d) Ciphertext amplitude and phase of encrypted images. (e) Transmission amplitude and phase corresponding to the 8 types of meta-atom cells schematically drawn below, which have been utilized in our metasurfaces. (f,g) SEM image and optical decryption results for Sample 1. (h,i) SEM image and optical decryption results for Sample 2. The keys (α and β) and corresponding optical system parameters (f and z) for each pattern is given in (f)–(i). (j) Effect of the distance on the decryption results (k) Effect of ciphertext noise on the decryption results (l) Effect of the focal length f on the decryption results (m) Effect of different magnification levels on the decryption results.

silicon nanopillars on a fused silica substrate, a height optimized for full 2π phase coverage at the 1064 nm wavelength. The side lengths of these square pillars, arranged in a 467 nm-period lattice, vary from 120 nm to 360 nm to encode the complex amplitude of the ciphertext at the pixel level. Fabrication via EBL and ICP etching achieves a tight dimensional tolerance of ± 5 –10 nm, which is critical for minimizing phase errors and ensuring clearly recognizable decryption. The blue and orange dots represent the phase responses of the structures under the transverse electric (TE) and transverse magnetic (TM) modes, respectively, with their absolute difference concentrated around π and spanning the full range from 0 to 2π . The yellow and purple dots inside the black dashed box indicate the amplitudes under the TE and TM modes, which are similar and both exceed 0.9. This characteristic allows the required amplitude to be tailored through rotational adjustments, enabling the design of customized complex amplitude profiles. We show below the specific structural designs, with detailed parameters in Section S3. By leveraging the inherent properties of half-wave plates, we initially produced light polarized in the x -direction using a linear polarizer. Subsequently, a second linear polarizer, aligned in the y -direction, was strategically put before the FrFT lens.

This arrangement ensured that the complex amplitude emerging from the second polarizer accurately represents the intended ciphertext information. Since the metasurface has a period of 467 nm and comprises 512×512 structures, beam expansion was necessary to cover the entire metasurface with the incident light. To meet the optical periodicity requirements, we used a microscope with a 20 $\times$ magnification factor and a numerical aperture (NA) of 0.4. This setup provided sufficient magnification to align the actual optical system parameters with those from the numerical simulations.

We designed two sets of ciphertexts corresponding to different patterns, with the SEM images of the metasurface shown in Figure 3f,h, and the experimental decryption results shown in Figure 3g,i. According to numerical simulations, the first set of parameters was determined as $\alpha = 0.46$ and $\beta = 0.63$. From Equations (6) and (7) we calculated $f_1 = 63.6$ mm, $z_1 = 16$ mm; $f_2 = 50$ mm, $z_2 = 22.8$ mm. Experimental results demonstrate that the ‘ZJU’ and ‘OPT’ patterns in the first set are successfully decrypted at their designated positions. This clearly illustrates the feasibility of simulating the optical system-based FrFT encryption algorithm via an optical system, achieving ideal decryption

results. In the second set, we chose more detailed Chinese characters “qiu shi zhi guang” and the “MATH” pattern as the target images for encryption. We selected the orders $\alpha = 0.27$ and $\beta = 0.46$, and calculated $f_1 = 100$ mm, $z_1 = 9.2$ mm; $f_2 = 63.6$ mm, $z_2 = 16$ mm. Similarly, we obtained good decryption results. However, both sets of decrypted images exhibit some degree of blurring and edge artifacts, attributed to errors in the iterative algorithm and imperfections arising during sample fabrication.

As our numerical simulations demonstrated, the robustness of the FrFT-based encryption algorithm was further validated through optical experiments. We first evaluated the effect of positional shifts in the optical system by adjusting the microscope's objective lens with a 75 μ m range (Section S4 provides detailed images). As Figure 3j shows, an axial displacement of just 25 μ m causes severe image degradation, exhibiting a PSNR drop of 3–5 dB. While Equations (6) and (7) predict a theoretical drop of merely 0.05 dB based purely on the equivalent fractional order mismatch, this discrepancy does not invalidate our model. This theoretical estimate also explains why some decrypted patterns, particularly under positive axial shifts, can still retain recognizable structural contours. Rather, the experimental observation represents a superposition of the mathematical order deviation, defocus, and direction-dependent aberrations introduced by the magnified imaging system. Specifically, defocus-induced wavefront errors and quantization errors dominate the degradation, impacting image quality far more profoundly than the purely mathematical mismatch alone. These results highlight the high sensitivity of the decryption process to positional variations in the optical setup.

Additionally, we performed attack simulations on the ciphertext by adding phase noise at the pixel level. As Figure 3k exhibits, despite the introduced phase noise reducing the clarity of the decrypted patterns, the final recognition of the decrypted results remained unaffected, suggesting that random ciphertext-level perturbations alone are insufficient to compromise the optical decryption process. Recognizing that manufacturing imperfections are unavoidable, we analyzed the system's robustness against manufacturing errors. Our simulations show that typical fabrication tolerances (± 5 –10 nm) result in only a minor decryption quality loss (~ 0.5 dB PSNR drop), preserving fine details. However, larger errors (> 25 nm) lead to a significant performance degradation (> 3 dB PSNR drop). This confirms the system is robust enough for practical implementation, yet ultimate fidelity hinges on the precision of the nanofabrication process. To assess the effect of variations in the focal length of lens, we used a system with a fixed focal length of 63 mm. We utilized common laboratory lenses with focal lengths of 50 mm and 200 mm for testing. The experimental results in Figure 3l clearly show that only the lens with the designed focal length achieved accurate decryption, while the others failed. As previously mentioned, the matching of optical periods plays a crucial role in the experiments, serving as a bridge between theory and experiment. We tested objective lenses at different magnifications (i.e., different equivalent optical periods), namely no magnification, 5 $\times$, and 10 $\times$; as Figure 3m illustrates, none produced successful decryption. Only a 20 $\times$ magnification provides accurate results where the optical parameters were properly matched.

In the following, we apply our encryption method to two well-known images, namely the “Lena” and “Baboon” images, that feature a wide range of pixel-level details and exhibit significant grayscale variations across different regions, making them substantially more complex than those used in previous experiments. Figure 4a presents the original images, the numerically decrypted results, and the decrypted images obtained via scalar diffraction. We used a new set of keys, namely $\alpha = 0.25$ and $\beta = 0.58$, and simulated the optical decryption process using scalar diffraction, yielding promising outcomes. As Figure 4b depicts, both decrypted images contain rich details, which also ensures key sensitivity. With an FWHM as low as 0.02, even a slight deviation leads to a significant change in the PSNR. Similarly, Figure 4c illustrates the decryption process and the correlation between the two optical parameters (z, f). From the figure, it is evident that, when the variable z deviates from its accurate value by 3%, the decryption result immediately becomes blurred. To better preserve the details of both images during decryption, we reduced the magnification and NA of the microscope system. Specifically, we used a 10 $\times$ magnification with an NA of 0.25, and employed a method of small-period filling with a large-period structure, where a 3×3 superlattice unit served as a large supercell. Corresponding to the keys α and β , we have $f_1 = 250$ mm, $z_1 = 18.48$ mm; $f_2 = 120$ mm, $z_2 = 46$ mm. Figure 4d shows the experimental decryption image. As illustrated, the decryption results are also satisfactory, with fine details across different regions well-restored and grayscale variations clearly preserved. This demonstrates that the proposed fractional-order Fourier optical system effectively simulates the mathematical process and that our optical encryption method delivers reliable performance for images featuring small-scale details, complex structures, and multiple grayscale levels.

3 | Discussion

The advantages of our method over traditional computer-based decryption lie in the transmission of ciphertext via physical media, which effectively prevents attacks, such as duplication, interception, or tampering over the internet. Moreover, the encryption key is not simply a set of numerical values but is embedded within the optical system parameters, adding complexity to the decryption process. Compared with conventional FT-based optical encryption [53–59], the FrFT-based approach provides a set of usable fractional orders rather than a single fixed Fourier domain at $\alpha = 1$. Moreover, the FrFT order is relatively independent of other light-field modulation degrees of freedom used in metasurface cryptosystems, such as wavelength, OAM, structural color, spatial displacement, and multichannel holography, and can in principle be further multiplexed with them. A concise comparison with conventional FT optics and representative metasurface-based cryptosystems is provided in Table S5 in the Section S9. In parallel, the hybrid digital-quantum paradigm has emerged [60–62]. It leverages Quantum Key Distribution (QKD) to secure keys for digital algorithms. Our all-optical analog approach, however, performs encryption as a physical process, where keys (α, f, z) are embedded in the hardware and the ciphertext is a physical metasurface. Thus, while their strength is securing the digital key, ours is securing the entire physical process, making the two approaches complementary.

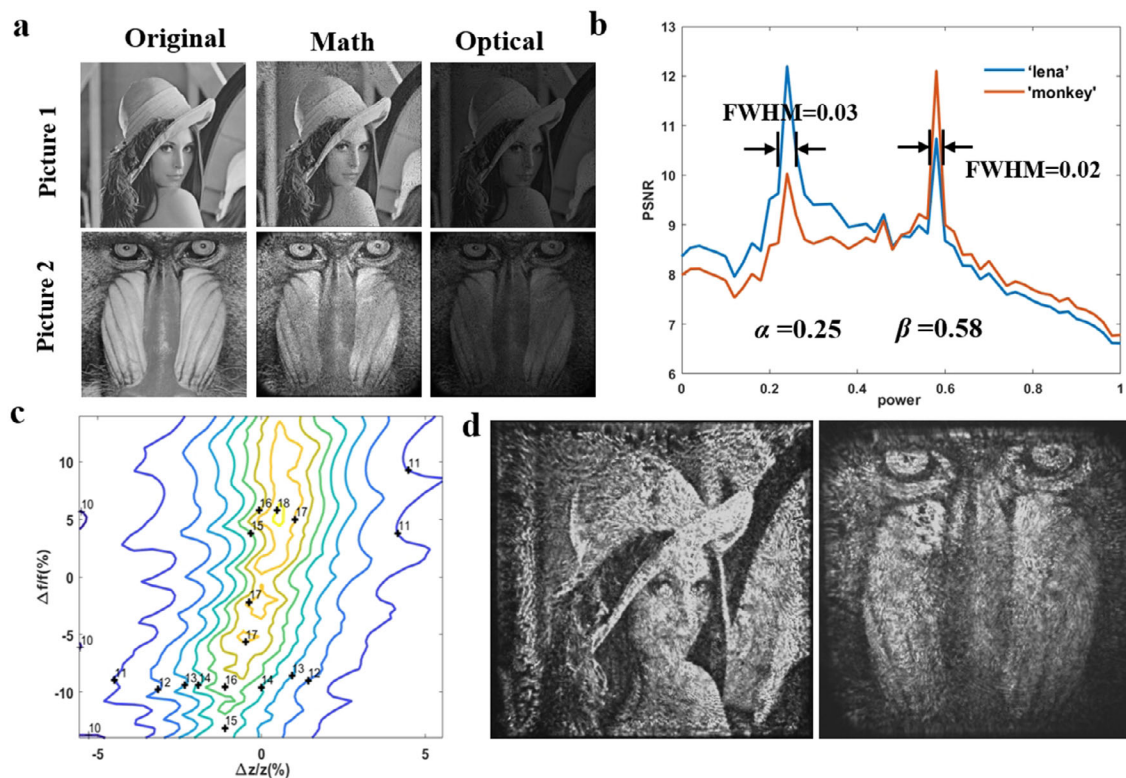


FIGURE 4 | Dual multiple-grayscale-levels image decryption results. (a) Original "Lena" and "Baboon" images together with their decryption results by both numerically computation and the scalar diffraction theory. (b) Relationship curve between PSNR of the two images and the decryption order. (c) Effect of the two optical parameters (z, f) on the decryption results. (d) Experimental decryption results. For these figures, the encryption keys are set by $\alpha = 0.25$ and $\beta = 0.58$.

The system's security against physical attacks is multi-layered. First, reverse-engineering the acquired metasurface, for example through SEM imaging, would mainly reveal partial geometric information of the ciphertext carrier, while the material dispersion, polarization response, fabrication-induced deviations, and actual optical transfer characteristics cannot be fully determined from SEM images alone. More importantly, an intercepted or even replicated ciphertext metasurface is still insufficient for reliable decryption without the matched optical decryption conditions. Therefore, the security of the proposed system originates not only from the physical ciphertext itself, but also from its coupling with the specific FrFT optical decryption path.

The robustness against a brute-force attack is substantial, although the practically usable key space should be regarded as a finite effective key space rather than an infinite continuous one. This effective key space is constrained by the ciphertext-dependent complex-amplitude distribution, meta-atom discretization, fabrication tolerance, and alignment precision. Nevertheless, the high key sensitivity, together with the requirement that each valid key corresponds to a specific set of optical parameters, still makes exhaustive physical trials highly demanding in practice.

This method is highly sensitive to its parameters. Even a slight change in the fractional order of encryption alters both the ciphertext content and the optical system parameters, causing a significant drop in decryption accuracy when using the original setup. The physical limitation of this approach stems from the fact that encrypted images with different feature sizes produce

distinct distributions in the fractional frequency domain. Constraints due to the NA of the microscope components, spectral information in the fractional domain is truncated, preventing successful decryption of extremely high-frequency details.

The pronounced sensitivity of our system to its parameters (f, z) presents a fundamental trade-off: it underpins cryptographic strength but demands extreme precision. We have quantitatively established the system's tolerance limits, demonstrating that a mere 5% deviation in f or z (Figure 2d) or a 25 μm lateral misalignment (Figure 3j) causes a catastrophic loss of image fidelity. To resolve this trade-off, we experimentally implemented a practical calibration strategy. Before decrypting target ciphertexts, an authorized user performs a one-time pre-alignment using a standard test pattern. By fine-tuning the optical setup (e.g., using precision translation stages to adjust lateral alignment and distance z) to maximize the output clarity, manufacturing and assembly tolerances are actively compensated. The clearly recognizable experimental results presented in Figures 3 and 4 directly validate this strategy. They prove that initial macroscopic mechanical errors can be practically corrected to meet the strict sub-micrometer requirements, robustly locking in the optimal configuration and perfectly reconciling high cryptographic sensitivity with operational reliability.

The errors in the proposed method mainly arise from four factors –(i) during metasurface fabrication, the geometric parameters (length and width) of the square silicon columns inevitably deviate from their theoretical design due to processing limitations. Given that measuring all $N = 262144$ unit cells via scanning

electron microscopy (SEM) is technically prohibitive, and the error sources in EBL and ICP etching (e.g., proximity effects, resist thickness variation) are highly complex and spatially dependent, it is difficult to extract a global statistical distribution. Thus, following the precedent in most reported metasurface literature, the fabrication tolerance is provided as a maximum deviation range of $\pm 5\text{--}10$ nm. Within this specific range, the geometric deviations alter the electromagnetic resonance conditions of the individual nanopillars, directly linking to the induced phase and amplitude fluctuations at the ciphertext plane. (ii) there are micrometer-level deviations in the distances between various optical components in the optical system, affecting the decryption results; (iii) the iterative phase retrieval algorithm inherently incurs convergence errors, causing discrepancies between the decrypted image and the original plaintext; (iv) the intensity inhomogeneity of the incident beam. In practice, the light beam is not a perfect plane wave after expansion, which can cause slight brightness variations in the decrypted image. However, since our decryption process is predominantly sensitive to phase rather than intensity, this non-uniformity has a negligible impact on the accuracy and recognizability of the final decrypted result. These factors combinedly account for the unavoidable differences observed in the final decryption outcomes.

Looking forward, this work opens several promising avenues for future development. Firstly, the method can be extended to color image encryption by independently processing the R, G, and B channels, potentially using unique fractional orders as keys for each channel to enhance security. Secondly, dynamic or video encryption could be realized by replacing the static metasurface with a programmable spatial light modulator (SLM), enabling real-time ciphertext display and optical decryption. Thirdly, scalability to higher resolutions presents a key future challenge, which will require overcoming significant hurdles in computational efficiency for iterative algorithms, large-area nanofabrication, and the design of high-numerical-aperture (NA) optical systems to preserve fine image details.

The introduction of FrFT has greatly increased the flexibility of time-frequency domain transformations. For a given signal, spectral information across different fractional Fourier domains displays unique characteristics, allowing desired outcomes to be achieved through mathematical operations in these domains. Additionally, image encryption algorithms based on all-optical frameworks and FrFT represent a technological innovation in the field of image encryption, introducing physical system encryption as an alternative to traditional digital signal encryption. Looking forward, encryption security will be further improved through second-order encryption methods based on FrFT and multi-channel encryption techniques for RGB. At the same time, the multi-dimensional fractional domain transformations enabled by fractional Fourier optics will pave the way for novel approaches in multi-dimensional optical field manipulation as well as time-frequency signal transformation and filtering.

4 | Conclusions

The aforementioned results indicate that the numerical calculations and optical experiments demonstrate that the system accurately computes the FrFT. Based on this, two image encryp-

tion methods have been developed: one encrypts a single image with Arnold transform, and the other encodes two grayscale images into a complex amplitude ciphertext, using the FrFT order as the decryption key. To enable all-optical decryption, a polarization-conversion metasurface has been designed to jointly control amplitude and phase, serving as the ciphertext carrier. This allows the optical system to perform FrFT and decrypt the images. Experimental results show clear decrypted images, particularly for “Lena” and “Baboon,” indicating effective grayscale restoration and validating both the encryption algorithm and optical platform. Key-related optical parameters, including lens focal length and element distances, have been tested via simulations and experiments, confirming high sensitivity to keys and substantially increasing decryption difficulty. The obtained results indicate advancement in optical encryption and establish a new paradigm for applying fractional Fourier optics in secure communications and information processing.

Author Contributions

Y. Ma conceived the initial idea. J. Yu, S. Guo, and J. Zhan performed the numerical simulations of the designed metasurface. S. Guo fabricated the metasurface. J. Yu, S. Guo, Y. Shao, and Y. Wang conducted the optical measurements. J. Yu, R. Chen, and D. Wan analysed the data. G. Bao, Pankaj K. Choudhury, and Y. Ma provided theoretical advice. All authors contributed to the writing of the paper and contributed to the discussion and analysis. G. Bao and Y. Ma guided the entire project.

Acknowledgements

This work is sponsored by the National Key Research and Development Program of China (2023YFA1009100), the Key Project of Joint Funds for Regional Innovation and Development (U21A20425), the Joint Funds of the National Natural Science Foundation of China (U24A20313), Natural Science Foundation of Zhejiang Province LDT23F05014F05, National Natural Science Foundation of China (62475234 and 62405268), National Key Research and Development Program of China (2024YFA1012600), and Fundamental Research Funds for the Central University (2021FZZX001-07).

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Statement

I certify that this manuscript is original and has not been published and will not be submitted elsewhere for publication while being considered by Laser & Photonics Reviews. No data have been fabricated or manipulated (including images) to support our conclusions. No data, text, or theories by others are presented as if they were our own. The submission has been received explicitly from all co-authors. And authors whose names appear on the submission have contributed sufficiently to the scientific work and therefore share collective responsibility and accountability for the results.

Data Availability Statement

The data that support the findings of this study are available in the supplementary material of this article.

References

1. J. W. Goodman, *Introduction to Fourier Optics*, 4th ed. (The McGRAW-Hill Companies, Inc., 2017).

2. A. Zaidi, N. A. Rubin, M. L. Meretska, et al., "Metasurface-Enabled Single-Shot and Complete Mueller Matrix Imaging," *Nature Photonics* 18 (2024): 704–712.
3. Z. Shen, F. Zhao, C. Jin, S. Wang, L. Cao, and Y. Yang, "Monocular Metasurface Camera for Passive Single-Shot 4D Imaging," *Nature Communications* 14 (2023): 1035–1038, <https://doi.org/10.1038/s41467-023-36812-6>.
4. R. Chen, Y. Shao, Y. Zhou, et al., "A Semisolid Micromechanical Beam Steering System Based on Micrometa-Lens Arrays," *Nano Letters* 22 (2022): 1595–1603, <https://doi.org/10.1021/acs.nanolett.1c04493>.
5. Y. Zhang, P. Lin, P. Huo, et al., "Dielectric Metasurface for Synchronously Spiral Phase Contrast and Bright-Field Imaging," *Nano Letters* 23 (2023): 2991–2997, <https://doi.org/10.1021/acs.nanolett.3c00388>.
6. Y. Hu, Y. Jiang, Y. Zhang, et al., "Achromatic Full Stokes Polarimetry Metasurface for Full-Color Polarization Imaging in the Visible Range," *Nano Letters* 24 (2024): 13018–13026.
7. M. Gopakumar, G.-Y. Lee, S. Choi, et al., "Full-Colour 3D Holographic Augmented-Reality Displays with Metasurface Waveguides," *Nature* 629 (2024): 791–797, <https://doi.org/10.1038/s41586-024-07386-0>.
8. S. So, J. Kim, T. Badloe, et al., "Multicolor and 3D Holography Generated by Inverse-Designed Single-Cell Metasurfaces," *Advanced Materials* 35 (2023): 2208520, <https://doi.org/10.1002/adma.202208520>.
9. Y. Yin, Q. Jiang, H. Wang, et al., "Multi-Dimensional Multiplexed Metasurface Holography by Inverse Design," *Advanced Materials* 36 (2024): 2312303.
10. J. Kim, J.-H. Im, S. So, et al., "Dynamic Hyperspectral Holography Enabled by Inverse-Designed Metasurfaces with Oblique Helicoidal Cholesterics," *Advanced Materials* 36 (2024): 2311785.
11. Z. Yu, X. Gao, J. Yao, et al., "Spin-Orbit-Locking Vectorial Metasurface Holography," *Advanced Materials* 37 (2024): 2415142.
12. S. Guo, Y. Shao, J. Zhan, et al., "Polarization-Controlled Metasurface for Simultaneous Holographic Display and Three-Dimensional Depth Perception," *Nanophotonics* 14 (2025): 197–207, <https://doi.org/10.1515/nanoph-2024-0509>.
13. S. Guo, Y. Shao, J. Zhan, et al., "Multifunctional Metasurface: Holography and Spot Cloud Projection," *Advanced Optical Materials* 12 (2024): 202401235.
14. X. Liang, Z. Zhou, Z. Li, et al., "All-Optical Multiplexed Meta-Differentiator for Tri-Mode Surface Morphology Observation," *Advanced Materials* 35 (2023): 2301505, <https://doi.org/10.1002/adma.202301505>.
15. I. Tanriover, S. A. Dereshgi, and K. Aydin, "Metasurface Enabled Broadband all Optical Edge Detection in Visible Frequencies," *Nature Communications* 14 (2023): 6484–6488, <https://doi.org/10.1038/s41467-023-42271-w>.
16. C. Zhou, Y. Wang, and L. Huang, "All-Optical Analog Differential Operation and Information Processing Empowered by Meta-Devices," *Nanophotonics* 14 (2025): 1021–1044, <https://doi.org/10.1515/nanoph-2024-0540>.
17. A. Cordaro, B. Edwards, V. Nikkhah, A. Alù, N. Engheta, and A. Polman, "Solving Integral Equations in Free Space with Inverse-Designed Ultrathin Optical Metagratings," *Nature Nanotechnology* 18 (2023): 365–372, <https://doi.org/10.1038/s41565-022-01297-9>.
18. C. Zhou, Y. Wang, and L. Huang, "All-Optical Analog Differential Operation and Information Processing Empowered by Meta-Devices," *Nanophotonics* 14 (2025): 1021–1044, <https://doi.org/10.1515/nanoph-2024-0540>.
19. Y. Zhou, J. Zhan, Z. Xu, et al., "Electromagnetic Spatiotemporal Differentiation Meta-Devices," *Laser & Photonics Reviews* 17 (2023): 2300182.
20. S.-C. Pei, M.-H. Yeh, and T.-L. Luo, "Fractional Fourier Series Expansion for Finite Signals and Dual Extension to Discrete-Time Fractional Fourier Transform," *IEEE Transactions on Signal Processing* 47 (1999): 2883–2888.
21. T. Erseghe, P. Kraniuskauskas, and G. Carioraro, "Unified Fractional Fourier Transform and Sampling Theorem," *IEEE Transactions on Signal Processing* 47 (1999): 3419–3423, <https://doi.org/10.1109/78.806089>.
22. L. J. Stanković, T. Alieva, and M. J. Bastiaans, "Time-Frequency Signal Analysis Based on the Windowed Fractional Fourier Transform," *Signal Processing* 83 (2003): 2459–2468, [https://doi.org/10.1016/S0165-1684\(03\)00197-X](https://doi.org/10.1016/S0165-1684(03)00197-X).
23. M.-H. Yeh, "Angular Decompositions for the Discrete Fractional Signal Transforms," *Signal Processing* 85 (2005): 537–547, <https://doi.org/10.1016/j.sigpro.2004.11.001>.
24. E. Sejdić, I. Djurović, and L. J. Stanković, "Fractional Fourier Transform as a Signal Processing Tool: an Overview of Recent Developments," *Signal Processing* 91 (2011): 1351–1369.
25. V. Namias, "The Fractional Order Fourier Transform and Its Application to Quantum Mechanics," *IMA Journal of Applied Mathematics* 25 (1980): 241–265, <https://doi.org/10.1093/imamat/25.3.241>.
26. M. A. Man'ko, "Fractional Fourier Transform in Information Processing, Tomography of Optical Signal, and Green Function of Harmonic Oscillator," *Journal of Russian Laser Research* 20 (1999): 226–238, <https://doi.org/10.1007/BF02508542>.
27. S. Abe and J. T. Sheridan, "Random Fractional Fourier Transform: Stochastic Perturbations along the Axis of Propagation," *Journal of the Optical Society of America A* 16 (1999): 1986–1991, <https://doi.org/10.1364/JOSAA.16.001986>.
28. L. B. Almeida, "The Fractional Fourier Transform and Time-frequency Representations," *IEEE Transactions on Signal Processing* 42 (1994): 3084–3091, <https://doi.org/10.1109/78.330368>.
29. R. Torres and E. Torres, "Fractional Fourier Analysis of Random Signals and the Notion of /Spl Alpha/-Stationarity of the Wigner-Ville Distribution," *IEEE Transactions on Signal Processing* 61 (2013): 1555–1560, <https://doi.org/10.1109/TSP.2012.2236834>.
30. J. Shi, J. Zheng, X. Liu, W. Xiang, and Q. Zhang, "Novel Short-Time Fractional Fourier Transform: Theory, Implementation, and Applications," *IEEE Transactions on Signal Processing* 68 (2020): 3280–3295, <https://doi.org/10.1109/TSP.2020.2992865>.
31. T. Alikasifoglu, B. Kartal, and A. Koç, "Wiener Filtering in Joint Time-Vertex Fractional Fourier Domains," *IEEE Signal Processing Letters* 31 (2024): 1319–1323.
32. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical Encryption by Double-Random Phase Encoding in the Fractional Fourier Domain," *Optics Letters* 25 (2000): 887–889, <https://doi.org/10.1364/OL.25.000887>.
33. B. Hennelly and J. T. Sheridan, "Optical Image Encryption by Random Shifting in Fractional Fourier Domains," *Optics Letters* 28 (2003): 269–271, <https://doi.org/10.1364/OL.28.000269>.
34. Z. Liu and S. Liu, "Double Image Encryption Based on Iterative Fractional Fourier Transform," *Optics Communications* 275 (2007): 324–329, <https://doi.org/10.1016/j.optcom.2007.03.039>.
35. N. Zhou, Y. Wang, L. Gong, H. He, and J. Wu, "Novel Single-Channel Color Image Encryption Algorithm Based on Chaos and Fractional Fourier Transform," *Optics Communications* 284 (2011): 2789–2796, <https://doi.org/10.1016/j.optcom.2011.02.066>.
36. Z. Fu, Y. Lin, D. Yang, and S. Yang, "Fractional Fourier Transforms Meet Riesz Potentials and Image Processing," *SIAM Journal on Imaging Sciences* 17 (2024): 476–500.
37. H. M. Ozaktas, M. Kutay-Alper, and Z. Zalevsky, "The Fractional Fourier Transform: with Applications in Optics and Signal Processing," in *2001 European Control Conference (ECC)* (Scitech Book News, 2001).
38. S. P. Walborn, D. S. Lemelle, D. S. Tasca, and P. H. Souto Ribeiro, "Schemes for Quantum Key Distribution with Higher-Order Alphabets Using Single-Photon Fractional Fourier Optics," *Physical Review A* 77 (2008): 62323, <https://doi.org/10.1103/PhysRevA.77.062323>.

39. T. Zhao, T. Yang, and Y. Chi, "Quantum Weighted Fractional Fourier Transform," *Mathematics* 10 (2022): 1896.
40. K. Zhang, L.-L. Li, P.-P. Yu, Y. Zhou, D. W. Guo, and H.-Y. Fan, "Quantum Entangled Fractional Fourier Transform Based on the IWOP Technique," *Chinese Physics B* 32 (2023): 040302, <https://doi.org/10.1088/1674-1056/ac7e32>.
41. Z. Liu and S. Liu, "Random Fractional Fourier Transform," *Optics Letters* 32 (2007): 2088–2090, <https://doi.org/10.1364/OL.32.002088>.
42. L. Sui and B. Gao, "Single-Channel Color Image Encryption Based on Iterative Fractional Fourier Transform and Chaos," *Optics & Laser Technology* 48 (2013): 117–127, <https://doi.org/10.1016/j.optlastec.2012.10.016>.
43. H. Chen, Z. Liu, C. Tanougast, and J. Ding, "Optical Hyperspectral Image Cryptosystem Based on Affine Transform and Fractional Fourier Transform," *Applied Sciences* 9 (2019): 330.
44. I. S. Samanta, P. K. Rout, and S. Mishra, "An Optimal Extreme Learning-based Classification Method for Power Quality Events Using Fractional Fourier Transform," *Neural Computing and Applications* 33 (2021): 4979–4995, <https://doi.org/10.1007/s00521-020-05282-y>.
45. E. Koç and A. Koç, "Fractional Fourier Transform in Time Series Prediction," *IEEE Signal Processing Letters* 29 (2022): 2542–2546.
46. J. García, D. Mas, and R. G. Dorsch, "Fractional-Fourier-transform Calculation through the Fast-Fourier-Transform Algorithm," *Applied Optics* 35 (1996): 7013–7018.
47. J. M. Vildary, Y. Torres, M. S. Millán, and E. Pérez-Cabré, "Generalized Formulation of an Encryption System Based on a Joint Transform Correlator and Fractional Fourier Transform," *Journal of Optics* 16 (2014): 125405–125418, <https://doi.org/10.1088/2040-8978/16/12/125405>.
48. E. A. Saleh, Bahaa, and M. C. Teich, *Fundamentals of Photonics* (Wiley, 2019).
49. G. B. Arfken, *Mathematical Methods for Physicists* (Academic Press Inc., 2012).
50. A. Bultheel and H. E. M. Sulbaran, "Computation of the Fractional Fourier Transform," *Applied and Computational Harmonic Analysis* 16 (2004): 182–202, <https://doi.org/10.1016/j.acha.2004.02.001>.
51. V. I. Arnold and A. Avez, *Ergodic Problems of Classical Mechanics* (Benjamin, 1968).
52. X. Sui, Z. He, D. Chu, et al., "Non-Convex Optimization for Inverse Problem Solving in Computer-Generated Holography," *Light: science & applications* 13 (2024): 158–181.
53. R. Zhao, B. Sain, Q. Wei, et al., "Multichannel Vectorial Holographic Display and Encryption," *Light: Science & Applications* 7 (2018): 95–104.
54. G. Qu, W. Yang, Q. Song, et al., "Reprogrammable Meta-Hologram for Optical Encryption," *Nature Communications* 11 (2020): 5484, <https://doi.org/10.1038/s41467-020-19312-9>.
55. Z. Li, X. Kong, J. Zhang, et al., "Cryptography Metasurface for One-Time-Pad Encryption and Massive Data Storage," *Laser & Photonics Reviews* 16 (2022): 2200113.
56. L. Wang, T. Wang, R. Yan, et al., "Color Printing and Encryption with Polarization-Switchable Structural Colors on all-Dielectric Metasurfaces," *Nano Letters* 23 (2023): 5581–5587.
57. Z. Yu, H. Li, W. Zhao, et al., "High-Security Learning-Based Optical Encryption Assisted by Disordered Metasurface," *Nature Communications* 15 (2024): 2607, <https://doi.org/10.1038/s41467-024-46946-w>.
58. H. Yang, P. He, K. Ou, et al., "Angular Momentum Holography via a Minimalist Metasurface for Optical Nested Encryption," *Light: Science & Applications* 12 (2023): 79–90.
59. F. Zhang, Y. Guo, M. Pu, et al., "Meta-Optics Empowered Vector Visual Cryptography for High Security and Rapid Decryption," *Nature Communications* 14 (2023): 1946, <https://doi.org/10.1038/s41467-023-37510-z>.
60. B. Mallick, P. Parida, C. Nayak, M. K. Panda, B. Prasad, and G. Sahu, "Quantum Image Encryption Scheme Using DPS Protocol Based on 3D Non-Equilateral Arnold Transform and URUK Chaotic Map," *Optics Communications* 592 (2025): 132240, <https://doi.org/10.1016/j.optcom.2025.132240>.
61. B. Mallick, P. Parida, C. Nayak, et al., "Multi-Channel Multi-Protocol Quantum Key Distribution System for Secure Image Transmission in Healthcare," *IEEE Access* 13 (2025): 62476–62505.
62. B. Mallick, P. Parida, C. Nayak, et al., "Secure Real-Time Transmission of Multi-Spectral Satellite Images Inducing a 6D Hyper-chaotic System and BB84 QKD Protocol," *Alexandria Engineering Journal* 122 (2025): 364–384, <https://doi.org/10.1016/j.aej.2025.02.113>.

Supporting Information

Additional supporting information can be found online in the Supporting Information section.

Supporting File: lpor71470-sup-0001-SuppMat.pdf.