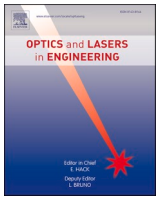
Optics and Lasers in Engineering 188 (2025) 108900

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

journal homepage: www.elsevier.com/locate/optlaseng



Multiplane experimental optical data encryption using phase only holography

Juan Andrés González-Moncada *, Alejandro Velez-Zea, John Fredy Barrera-Ramírez

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

ARTICLE INFO

Keywords:
Encryption
Multiplane
Complex modulation
Optimization
Computer generated hologram

ABSTRACT

In this paper, we demonstrate a scheme to encrypt multiplane scenes using an experimental joint transform correlator cryptosystem capable of full complex modulation, implemented with a single phase-only spatial light modulator. We use two different encoding algorithms to achieve full complex modulation of the input plane of the joint transform correlator cryptosystem, enabling the encryption of any complex optical field using arbitrary complex-valued encryption keys. Using the capabilities of this proposal, we demonstrate, for the first time to our knowledge, the experimental optical encryption of a multiplane scene composed of up to nine different 2D objects placed at different distances along the optical axis. This scheme is implemented using both double-phase encoding and binary amplitude encoding, and the performance with both encoding approaches is compared both numerically and experimentally. We show that binary amplitude encoding is superior to double-phase encoding, producing results with comparable or higher quality, particularly in the experimental case, and allowing the encryption of larger scenes than what is possible using double-phase encoding.

1. Introduction

The ability to accurately control optical light fields has become the cornerstone of many important applications, ranging from metrology [1,2], microscopy [3,4] and optical trapping [5,6], to optogenetics [7,8] and holographic displays with ever increasing resolution [9,10], viewing angle [11,12], and generation speed [13]. Two key factors have enabled these applications: first, the increased availability of high resolution spatial light modulators (SLMs), capable of controlling the phase or amplitude of an incoming optical field, and secondly, the rapid improvements in computer generated holography (CGH), which enables encoding a target complex light distribution into a phase-only or amplitude-only function that can be used in conjunction with SLMs.

As the applications of CGH combined with SLMs for optical field control become increasingly common, there is a growing need for methods to process the associated holographic content efficiently and securely. This has led to renewed interest in optical methods for holographic data compression [14] and optical encryption [15]. Optical encryption methods have been the subject of intense research since Refrieger & Javidi proposed the double random phase encoding scheme (DRPE) in 1995 [16]. Optical encryption methods include visual cryptography, where images are decomposed into shares that reveal the original information when superposed [17]. In general, visual cryptography techniques face challenges such as limited contrast, pixel expansion, and memory complexity. However, these methods have the advantages of not requiring complex algorithms and providing high security, as a fixed minimum number of shares is necessary to recover the original image [18]. These characteristics make visual cryptography appealing in high-security applications, and variants tailored for specific purposes have been proposed [19].

Single-pixel imaging is another optical encryption technique in which objects are illuminated with structured light patterns, and the light from the entire scene is registered using a single-pixel detector [20,21]. The detector signals act as the ciphered text, while the corresponding light patterns act as encryption keys. The original scene can be recovered from a reduced number of measurements using optimization algorithms, provided that the structured light patterns, which serve as encryption keys, are known. This technique achieves both compression and encryption of the original images. Variants of this method, such as computational ghost imaging, have been proposed to address limitations, including the complexity of key management [22,23].

While most research focused on optical encryption as an alternative to conventional digital encryption methods to secure any type of data, the inherent optical nature of these schemes make them specially well

* Corresponding author.
E-mail address: juan.gonzalezm1@udea.edu.co (J.A. González-Moncada).

https://doi.org/10.1016/j.optlaseng.2025.108900
Received 19 November 2024; Received in revised form 27 January 2025; Accepted 19 February 2025

suited for encryption of holographic content. For this purpose, optical encryption methods like DRPE that use coherent light sources are necessary; however, optical encryption based on DRPE faces significant challenges [15]. First, the encryption-decryption process introduces noise and degradation, which may affect the integrity of the data to be processed. This degradation is mainly caused by the use of random phase masks (RPMs) as encryption keys [24]. Significant efforts have been made to minimize this degradation by using alternative architectures [25–27], optimizing the random phases used for encryption [28,29], modifying the input data, or using noise resistant data containers [30–33], however, these noise reduction methods increase the complexity of the encryption system or add additional processing steps, which may not be desirable.

The second challenge is related to the security of the DRPE. Since Javidi's initial proposal, a variety of attacks have been demonstrated against these systems [34–38], leading to the subsequent modifications aimed to protect against these attacks. Similarly to the case of noise reduction, these proposals use a variety of approaches, such as modification of the encryption keys [39–41] or addition of new types of keys [42,43], alternative methodologies for identifying authorized users [44], introducing new transformation domains between the input and output plane of the DRPE [40,45–48], using nonlinear operations such as phase and amplitude truncation [49], or scrambling of inputs and keys [50,51], and cryptographic methods like salting [52] and steganography [53], to name a few. These proposals, while achieving their goal of increasing the DRPE security in many cases, usually introduce operations that require complex light modulation, which is difficult to achieve in experimental implementations. For these reasons, most of these proposals are limited to numerical implementations.

This leads to the third challenge: achieving an experimental optical implementation capable of processing a variety of inputs. The original DRPE system was based on a 4F architecture and was initially proposed to encrypt amplitude-only inputs. Furthermore, the encrypted data was a complex-valued function, which required holographic techniques for adequate recording and storage. Later, Javidi proposed implementing DRPE with a joint transform correlator (JTC) architecture [54]. In this implementation, the encrypted data is encoded into an intensity function, eliminating the need for its holographic recording; however, the input was still intended to be an amplitude-only function. Subsequent proposals analyzed the effectiveness of optical implementations of DRPE to encode phase-only inputs. Nevertheless, most optical implementations of DRPE are limited to processing either phase-only or amplitude-only inputs. This limitation poses a significant challenge when working with optical field control systems, such as those used in holographic displays, since the information to be encoded is in general a complex-valued function

This limitation means that most of the proposals to reduce the noise and increase the security of DRPE have only been implemented in numerical simulations or virtual systems. These methods utilize complex-valued inputs or keys, requiring light modulation setups that are difficult to implement. Even when these methods can be implemented, they are usually limited to encrypting simple objects [55–60] or rely on multiple SLMs, making them both costly and impractical in many scenarios.

In the case of encryption of holographic data for optical field control applications, it is highly desirable to enable the encryption and the projection of decrypted fields using a single SLM, without the introduction of additional elements. To achieve this, we recently proposed a method that utilizes the double-phase hologram generation method [61], enabling full complex control of the input plane of a JTC cryptosystem that a single phase-only SLM [62]. This method enabled both the experimental encryption of complex inputs and the use of arbitrary computer-generated complex-valued keys, significantly expanding the capabilities of conventional DRPE schemes. However, despite the capabilities of this system, the use of double-phase hologram generation imposes a significant limitation on the size of the objects to be processed for a given SLM. Although this approach has the potential to encrypt any complex field, its demonstration has been limited to individual 2D amplitude inputs.

To overcome these limitations, we now propose a methodology based on the binary amplitude encoding (BAE) hologram generation [63,64] and multiplane hologram generation with the global Gerchberg-Saxton algorithm [65,66]. Multiplane holograms are of particular interest because, unlike common 3D CGH, they can present fully independent information at different depth planes with minimal crosstalk, which can lead to improved security and multiuser applications in optical encryption schemes. Furthermore, despite the need for advanced optimization methods to eliminate interplane crosstalk, these holograms effectively demonstrate the flexibility of an encryption scheme capable of processing fully complex-valued input scenes. Our proposed method can encrypt arbitrary 3D light distributions and is demonstrated with a multiplane scene composed of multiple 2D objects placed at different distances along the same optical axis. Furthermore, we show that, compared to our previous approach, BAE enables the encryption of larger objects with improved quality. Additionally, we implement random phase optimization to achieve noise reduction in the decrypted 3D scenes. Numerical and experimental results confirm the effectiveness of this approach.

2. Joint transform correlator cryptosystem

As a starting point for the methods detailed in this work, we will explain the basic scheme of a JTC cryptosystem and the associated limitations. This is a DRPE architecture that reduces alignment requirements by placing the object and the encryption key on the same plane [54], as seen in Fig. 1.

The input plane of this system contains both the object and the encryption key, and is given by

$$\boldsymbol{u}(\boldsymbol{x},\boldsymbol{y}) = \boldsymbol{c}(\boldsymbol{x}+\boldsymbol{b},\boldsymbol{y}) + \boldsymbol{k}(\boldsymbol{x}-\boldsymbol{b},\boldsymbol{y}), \tag{1}$$

where $k(x,y)$ is an RPM that will be the encryption key, $c(x,y)$ is the object to be encrypted $o(x,y)$ multiplied by a second RPM $r(x,y)$, and $2b$ is the separation between the center of both functions. In an experimental implementation, both RPMs are provided by a ground glass diffuser, as shown in Fig. 1. 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 camera. The intensity registered by the camera is called joint power spectrum (JPS) and it is given by

$$\begin{aligned} |\boldsymbol{U}(\boldsymbol{v},\boldsymbol{w})|^2 \quad = \quad & |\boldsymbol{C}(\boldsymbol{v},\boldsymbol{w})|^2 + |\boldsymbol{K}(\boldsymbol{v},\boldsymbol{w})|^2 + \boldsymbol{C}(\boldsymbol{v},\boldsymbol{w})\boldsymbol{K}^*(\boldsymbol{v},\boldsymbol{w})\boldsymbol{e}^{-4i\pi b v} \\ & + \boldsymbol{C}^*(\boldsymbol{v},\boldsymbol{w})\boldsymbol{K}(\boldsymbol{v},\boldsymbol{w})\boldsymbol{e}^{4i\pi b v}, \end{aligned} \tag{2}$$

where (v,w) are the frequency coordinates, $C(v,w)$ and $K(v,w)$ are the FT of $c(x,y)$ and $k(x,y)$, respectively, and * indicates the complex conjugate operator. The decryption can be accomplished using either of the last two terms, while the remaining terms in the JPS convey extra infor-

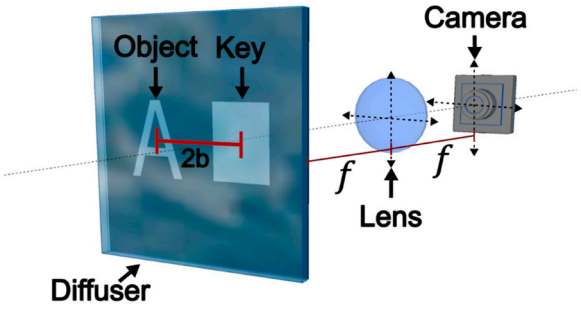


Fig. 1. Basic JTC encryption scheme. 2b: separation between key and object, *f*: focal length of the lens.

mation that may constitute a vulnerability in the cryptosystem [67]. To eliminate this issue, the extra terms are filtered as follows: the terms of the JPS are spatially separated by taking its FT and the extra terms are then filtered, retaining only one of the last two terms. Then, an inverse Fourier transform (IFT) of the selected term is performed and the result is defined as the encrypted data [68].

In this study, we retain the third term of the JPS, so the encrypted object is given by

$$\boldsymbol{E}(\boldsymbol{v},\boldsymbol{w}) = \boldsymbol{C}(\boldsymbol{v},\boldsymbol{w})\boldsymbol{K}^{*}(\boldsymbol{v},\boldsymbol{w}). \tag{3}$$

The decryption process consists of multiplying the encrypted data by the FT of the encryption key $K(v,w)$, that must be known beforehand and taking the IFT of the product. By applying the convolution theorem, the result is

$$\boldsymbol{d}(\boldsymbol{x},\boldsymbol{y}) = \boldsymbol{c}(\boldsymbol{x},\boldsymbol{y}) \otimes \boldsymbol{k}^{*}(\boldsymbol{x},\boldsymbol{y}) \otimes \boldsymbol{k}(\boldsymbol{x},\boldsymbol{y}), \tag{4}$$

where $\otimes$ denotes the convolution operator. In particular, $k^{*}(x,y) \otimes k(x,y)$ represents the self-correlation of the key $k(x, y)$, which is a random function. This self-correlation can be approximated as a Dirac delta by applying the broadband noise approximation [69]. The decrypted object is then

$$\boldsymbol{d}(\boldsymbol{x},\boldsymbol{y}) = \boldsymbol{c}(\boldsymbol{x},\boldsymbol{y}) \otimes \boldsymbol{\delta}(\boldsymbol{x},\boldsymbol{y}) = \boldsymbol{c}(\boldsymbol{x},\boldsymbol{y}), \tag{5}$$

so that the original object can be recovered by extracting it from $c(x,y)$.

3. Phase mask optimization

Despite the equivalence indicated by equation 5, numerical and experimental tests show that the recovered object is degraded with respect to the original one [30,32,51]. It is well known that optical systems that employ coherent light sources inherently suffer from degradation due to speckle noise. However, in this case, multiple studies have shown that most of the resulting degradation in JPS cryptosystems can be avoided, as it is caused by low intensity noise present in the self-correlation of the key, which is not accounted for in equation 4 [70]. This low intensity noise, known as random correlation noise (RCN) is neglected by the broadband noise approximation. This degradation is one of the main limitations of the JTC cryptosystem, but it can be mitigated by employing RPMs optimized to minimize the RCN.

To achieve this, we must explore the self-correlation of $k(x,y)$ found in equation 4. This self-correlation is exactly equal to a Dirac delta in two cases: when the RPM is infinite in extension or when its FT has constant amplitude across the entire plane, in which case it is a phase-only function. While the first case is impossible to achieve in an experimental setup, an approximation to the second one is possible by generating RPMs whose FT closely approximates a phase-only function. We can achieve this using phase retrieval algorithms, such as the Gerchberg-Saxton (GS) algorithm [71]. Phase retrieval algorithms generate the phase distribution of a complex field with a known amplitude and a target amplitude distribution in its FT. To reduce the RCN, we require a key RPM, placed on its respective position of the input plane, whose FT produces a field with nearly constant amplitude. Fig. 2 shows the flowchart of an iteration of the GS algorithm given these amplitude constraints.

Previous reports have analyzed the effects of employing keys optimized with the GS algorithm on decryption quality [29]. These reports found that the GS algorithm preserves the random nature of the key while increasing the decryption quality in an asymptotic manner. This means that the quality of the decrypted objects continuously increases with the number of GS iterations applied to optimize the key, but the rate of improvement decreases as the number of iterations increases.

4. Multiplane hologram generation

The GS algorithm previously shown is one of the many algorithms used in the field of CGH. CGH allows the projection of optical fields that have not been previously experimentally recorded, and combined with adequate SLM devices, enable precise control of optical fields, allowing reproduction of 3D intensity distributions. One application of CGH that has been of considerable interest in the last few years are multiplane holograms [72–74]. Multiplane holograms encode the optical field corresponding to a scene composed of several objects located at different distances along the same axis, one behind the other, as illustrated in Fig. 3. In the context of optical encryption, multiplane holography would facilitate the encryption of multiple 2D objects in a single step into one encrypted object. Then, the different objects would be recovered, one behind the other, without crosstalk, by propagating the decrypted field at specific distances. This capability significantly increases the usefulness and flexibility of optical encryption schemes.

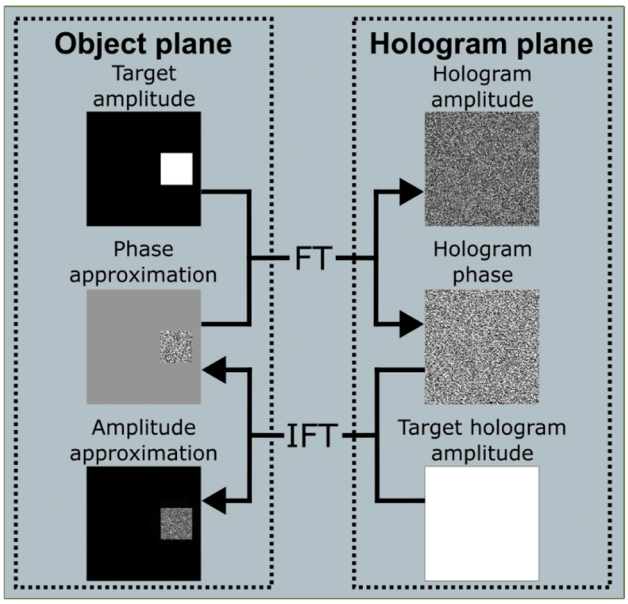


Fig. 2. Flowchart of GS algorithm. FT: Fourier transform, IFT: inverse Fourier transform.

Since most efficient SLM devices are phase-only, most research in multiplane holography has focused on generating phase-only multiplane holograms. One of the most straightforward methods for generating these types of holograms is by applying the global Gerchberg-Saxton (GGS) algorithm [65]. This is an extension of the GS algorithm that allows for the enforcement of amplitude constraints at multiple planes as the optical field propagates through space. Numerically, free-space propagation over a distance z is achieved using the Fresnel transform (FrT). Fig. 4 shows the flowchart of an iteration of the GGS algorithm.

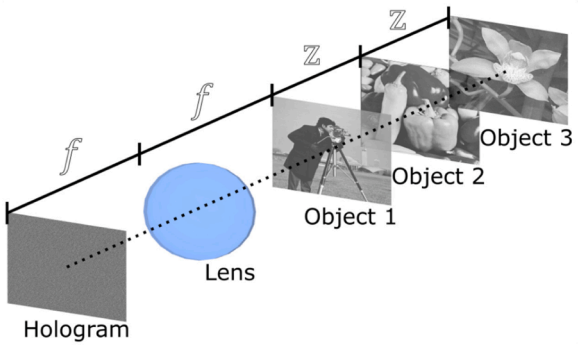


Fig. 3. Multiplane hologram. The first object is produced on the hologram Fourier plane and the subsequent objects are produced after propagating through free space. f: lens focal length, z: propagation distance.

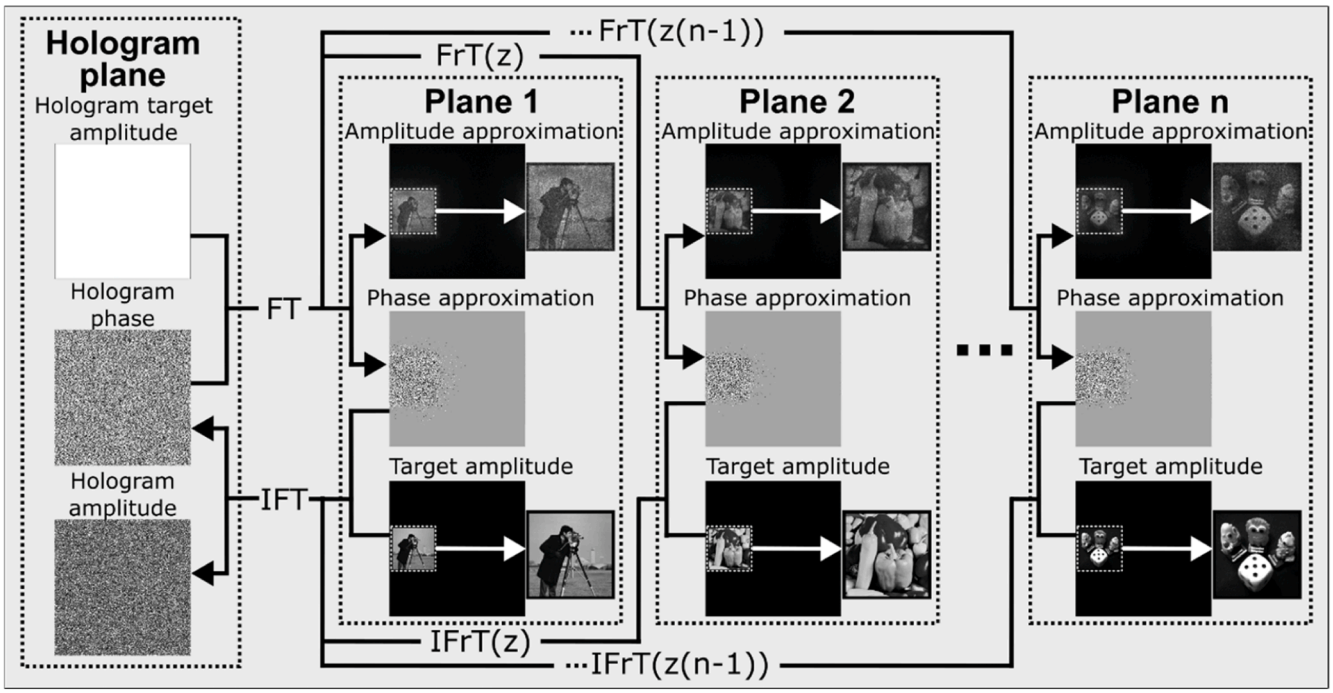


Fig. 4. Flowchart of GGS algorithm. FT: Fourier transform, IFT: inverse Fourier transform, FrT: Fresnel transform, IFrT: inverse Fresnel transform, n: number of objects in the multiplane scene, z: axial distance between planes.

GGS algorithms are generally defined to consider only planes connected through free space propagation, but we modified the implemented algorithm in accordance with the JTC so that the first plane is achieved using a FT, while the subsequent planes are obtained through free-space propagation.

The GGS algorithm, like the GS, is an iterative process. To show its behavior, we evaluate the reconstruction quality according to the number of GGS iterations applied by measuring the correlation coefficient (CC) between the reconstructions and the original images. The correlation coefficient between two images, A and B, is defined as

$$\mathrm{CC} = \frac{\sum_m \sum_n \left(\boldsymbol{A}_{m,n} - \overline{\boldsymbol{A}}\right)\left(\boldsymbol{B}_{m,n} - \overline{\boldsymbol{B}}\right)}{\sqrt{\left(\sum_m \sum_n \left(\boldsymbol{A}_{m,n} - \overline{\boldsymbol{A}}\right)^2\right)\left(\sum_m \sum_n \left(\boldsymbol{B}_{m,n} - \overline{\boldsymbol{B}}\right)^2\right)}}, \tag{6}$$

where m and n indicate their respective pixels, and $\overline{A}$ and $\overline{B}$ are the average values of the pixels in each image. Given this definition, the CC takes values between 0 and 1, where a higher value indicates better reconstructions. Fig. 5 shows the calculated CC for reconstructions obtained from a multiplane hologram generated using the GGS algorithm. The holograms generated had a size 2160 × 2160 pixels, a pixel size of 3.76 μm, and produced 4 objects with a size of 320 × 320 pixels axially separated by a distance of 6.38 mm when illuminated by a beam with a wavelength of 532 nm. The observed asymptotic behavior is consistent with the results obtained in previous studies [65].

As can be seen from these results, the GGS shows a rapid improvement in the quality of the reconstructed objects for each plane during the initial 20 iterations. However, the increase in quality becomes significantly slower with additional iterations. In this case, 4 different 2D objects could be encoded into a single phase-only hologram with adequate quality with 100 iterations. Achieving a noticeable increase in

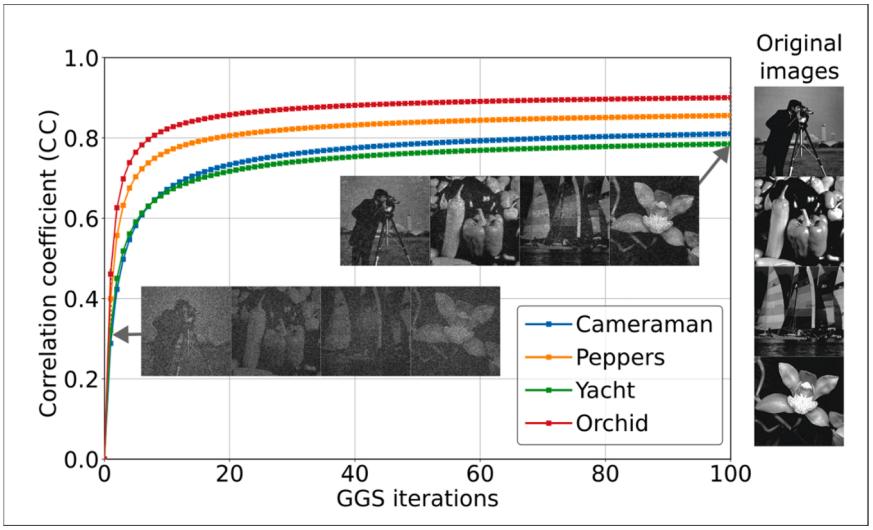


Fig. 5. Reconstruction correlation coefficient as a function of the number of GGS iterations applied to generate the multiplane hologram.

quality beyond this result can be expected to require many additional iterations, resulting in increased computation time. However, additional improvements could be made using alternative multiplane hologram generation algorithms that implement stochastic gradient descent [75] and mixed constraints [76], reducing the number of objects in the multiplane scene, or by decreasing the size of the objects.

5. Holographic encoding of the joint transform correlator input plane

Now, we turn our attention to the primary goal of our contribution: demonstrating an experimentally viable optical encryption method capable of processing multiplane optical fields with minimal degradation. This encryption scheme is capable of simultaneously encoding information of multiplane scenes into a single encrypted data. To achieve this, we propose combining the phase-only multiplane hologram, obtained using the GGS algorithm, and the nearly phase-only optimized key hologram, obtained using the GS algorithm. This combination defines a new hologram that results in a JTC input plane capable of encrypting multiplane scenes using a key optimized to minimize degradation. However, even though both the key and multiplane scene are contained in phase-only holograms, their combination is no longer phase-only, but rather a complex-valued hologram that cannot be directly projected in an experimental setup using a single SLM. As a result, the study of multiplane scene encryption must be limited to numerical simulations or require extremely precise arrangements of multiple SLMs, which significantly decreases the flexibility of the resulting system. One way to address this issue consists of using hologram encoding algorithms.

Hologram encoding algorithms usually receive complex holograms and generate new phase-only or other types of holograms with equivalent information. Fig. 6 shows a protocol to encode a complex-valued JTC input plane with a multiplane scene and a GS optimized key into a single phase-only hologram. In a previous study, we have shown the effectiveness of using a similar protocol to achieve complex modulation in experimental JTC cryptosystems. However, this study was limited to the use of the double-phase encoding (DPE) algorithm to encrypt single 2D objects [62].

The standard DPE algorithm generates a phase-only hologram whose FT is equivalent to the FT of the original complex hologram [61]. It works by defining an array of 2×2 phase-only pixels, called macropixels, for each pixel of the complex hologram. Each complex pixel $c_{nm} = |c_{nm}|e^{i\theta_{nm}}$ of size $2\alpha \times 2\beta$ is codified by its corresponding macropixel, composed of four phase-only pixels of size $\alpha \times \beta$. These phase-only pixels are arranged in a checkerboard pattern and take values given by

$$\begin{aligned} \phi_{nm}^{(1)} &= \theta_{nm} + \cos^{-1}\left(|c_{nm}|\right) \\ \phi_{nm}^{(2)} &= \theta_{nm} - \cos^{-1}\left(|c_{nm}|\right), \end{aligned} \tag{7}$$

where $|c_{nm}|$ is normalized over the complex hologram. The use of macropixels limits the size of the complex input plane that can be codified using this technique.

Recently, a new encoding algorithm called amplitude encoding (BAE) was proposed [63,64]. This algorithm also produces a phase-only hologram whose FT is equivalent to the FT of the original complex hologram. This approach has not yet been explored in the context of optical encryption and has characteristics that could be beneficial for these systems. In particular, BAE does not use macropixel arrangements, eliminating the main drawback of the DPE. The BAE algorithm runs as follows: First, a mask is generated by binarizing the amplitude of the original complex into a_{on} and a_{off} pixels. This binarization process is performed using dithering algorithms such as Floyd-Steinberg dithering. Then, the values of the phase-only hologram are determined based on the mask, where pixels corresponding to a_{on} will retain the phases of the original complex hologram. Meanwhile, the pixels corresponding to a_{off} will alternate its values between 0 and π, so that adjacent pixels will

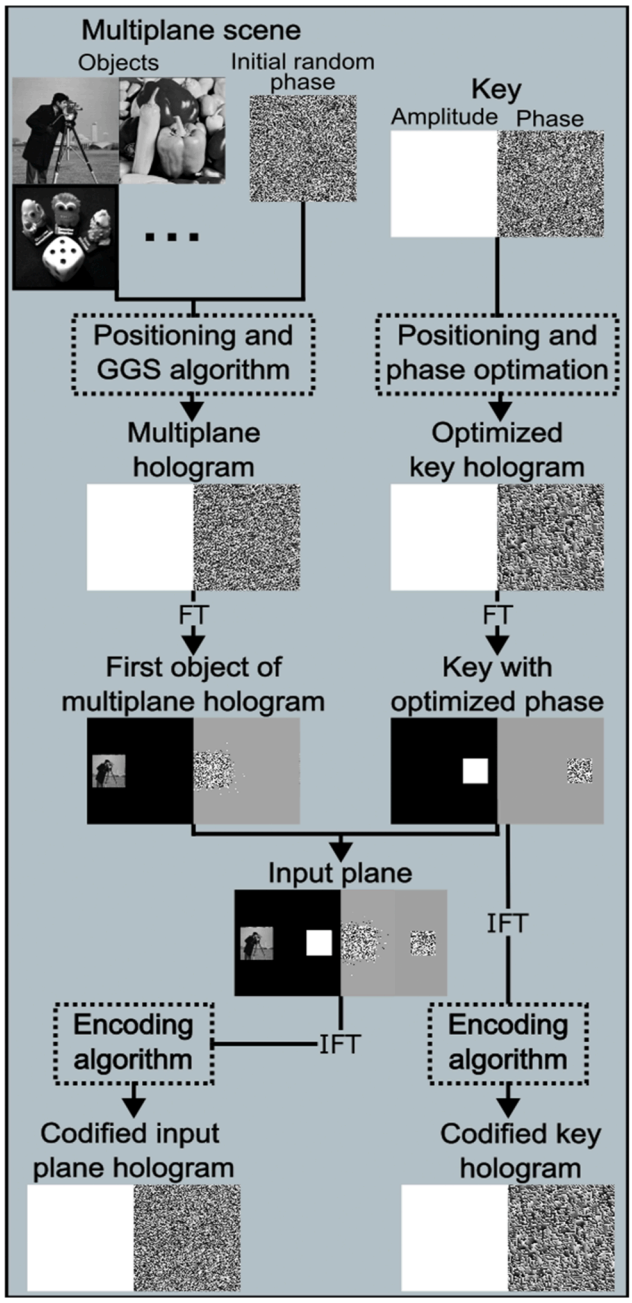


Fig. 6. Input plane hologram generation method. FT: Fourier transform, IFT: inverse Fourier transform.

cancel each other through destructive interference. This phase assignation is expressed as

$$\phi_{nm} = \begin{cases} \theta_{nm}, & \text{for } a_{nm} = a_{\text{on}} \\ \theta_{nm}^{(\text{alt})}, & \text{for } a_{nm} = a_{\text{off}} \end{cases}, \tag{8}$$

where $\theta_{nm}^{(\text{alt})}$ is defined as

$$\boldsymbol{\theta}_{\boldsymbol{nm}}^{(\text{alt})} = \begin{cases} 0, & \text{if previous } \boldsymbol{\theta}_{\boldsymbol{nm}}^{(\text{alt})} \text{ is } \pi \\ \pi, & \text{if previous } \boldsymbol{\theta}_{\boldsymbol{nm}}^{(\text{alt})} \text{ is } 0 \end{cases}. \tag{9}$$

The tradeoff of this method is the introduction of noise in the reconstruction plane. The location of this noise depends on the raster scan direction of the alternating substitution. In this study, we used vertical raster scan, as it was found to be less prone to signal and noise

superposition. Comparisons between both algorithms showed that DPE had similar or superior fidelity to BAE, but lower light efficiency and effective resolution due to the use of macropixel arrangements. In the context of encryption, both BAE and DPE can be used as encoding algorithms in the input plane hologram generation method shown in Fig. 5.

6. Multiplane scene encryption

Both the DPE and BAE algorithms produce a phase-only hologram, whose FT results in the desired complex-valued JTC input plane, needed to encrypt a multiplane scene using an optimized key. However, the FT of this input plane is a phase-only function by construction, which means that the digital camera of the optical setup can't properly register the JPS. To address this situation, it is important to note that the input plane produced by the phase-only holograms presents additional features because of the encoding process. In the case of DPE, there are replicas of the input plane centered at $\left[\pm p\frac{1}{2\alpha}, \pm q\frac{1}{2\beta}\right]$, where $p, q = \ldots, -2, -1, 0, 1, 2, \ldots$ represent the diffraction order. In the case of BAE, noise artifacts arise along the vertical borders of the input plane due to the vertical raster scan [64]. These additional features can be removed by placing a spatial filter on the input plane, ensuring that the JPS is no longer a phase-only function. As a result, the digital camera can properly register the JPS from the filtered input plane, and the JTC encryption process can continue as usual. Ultimately, the JTC with complex modulation, achieved using encoding algorithms, includes a SLM positioned so that the input plane is generated on its FT plane, precisely where the filter is located. The optical setup can be found in Fig. 7. To reiterate, the codified phase-only hologram is projected using the SLM, and the resulting field propagates through free space. A positive lens is placed to ensure that the JTC input plane, which includes the multiplane scene, is formed at the focal length of the lens. The artifacts produced by the encoding algorithms are removed using a spatial filter, and the filtered input plane, containing the multiplane scene, can be encrypted using a conventional JTC.

7. Numerical results

To test this proposal, we generated codified input plane holograms and codified key holograms using the protocol shown in Fig. 6. We then used numerical simulations to generate the JTC input plane, apply filtering, and then obtain the corresponding encrypted object (equation 3). To perform the decryption of this data, the encrypted object is multiplied by the FT of the encryption key and the IFT of the product produces the decrypted field, which corresponds to the complex field of the first object in the multiplane scene. Afterwards, subsequent propagations of this field enable the reconstruction of the other objects, as shown in Fig. 8.

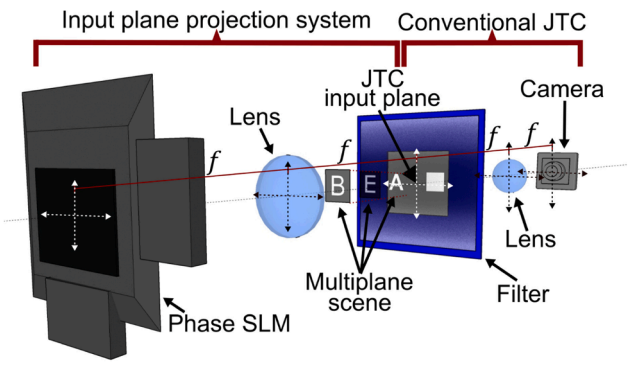


Fig. 7. JTC with complex modulation. SLM: spatial light modulator, *f*: lens focal length, JTC: joint transform correlator.

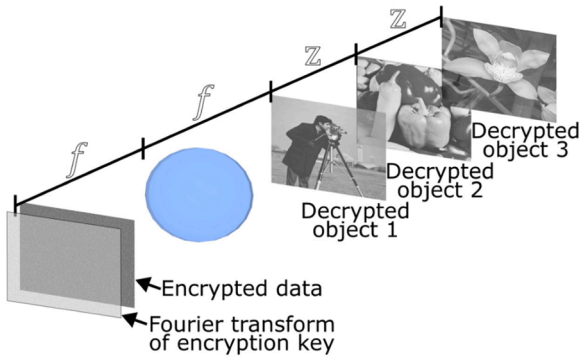


Fig. 8. Decrypted multiplane hologram. The first object is recovered on the focal plane of the lens, and the subsequent objects are reconstructed after propagating through free space. *f*: lens focal length, z: propagation distance.

The codified holograms had a size of 2160 × 2160 pixels, with a pixel size of 3.74 μm. The object and the key on the input plane had a size of 320 × 320 pixels and were separated a distance of $2b = 720$ pixels. Given the size restrictions imposed by the DPE algorithm, these values were chosen so that the input plane could be codified using both DPE and BAE algorithms, enabling a direct comparison of their performances. Considering the asymptotic behavior of the GS algorithm, we decided to use optimized keys in all cases, generated using 100 iterations of the algorithm. The numerical algorithms considered an illumination wavelength of 532 nm, and the multiplane scene to be encrypted was composed of 4 different 2D objects separated by an axial distance of 6.38 nm. The phase optimization and the generation of the multiplane holograms took approximately 0.6 s and 6.4 s seconds, respectively. These algorithms were executed using a NVIDIA GeForce RTX 4090.

Fig. 9 shows the results obtained using the proposed method to encrypt and decrypt multiplane holograms generated using 1 and 100 iterations of the GGS algorithm and codified using both the BAE and DPE algorithms. Above each decrypted image there is a specific section zoomed in for better visualization and below each reconstruction is the correlation coefficient between them and the corresponding original image. The results show that using 100 iterations of the GS algorithm and 100 iterations of the GGS algorithm is sufficient to generate a multiplane hologram that allows JTC encryption and decryption of the multiplane scene with acceptable quality.

The objects on each plane were satisfactorily recovered when using the correct key and the corresponding propagation distance. The results obtained using the BAE and DPE algorithms are similar, the latter produces a higher CC for the first plane but a lower value for the subsequent planes. Overall, BAE produces a higher mean CC across all planes. The object recovered on the first plane presents the best quality and the CC tends to decrease as the propagation distance for the decrypted field increases. Lastly, the objects recovered on each plane show no obvious signs of the presence of the other objects, suggesting the possibility of introducing the propagation distance as a security parameter to recover each object and for use in steganographic schemes [53,77,78]. This capability could be used in tandem with system modifications that address JTC cryptosystem vulnerabilities to further increase system security.

To analyze the effectiveness of the propagation distance as a security parameter, we calculated the CC between the original objects and the recovered field when propagated over different distances. Fig. 10 shows the results of this test using BAE, along with the reconstruction obtained at distances differing from the correct ones by approximately 2 mm. As expected, the correctly decrypted field produces the first object, the next object is recovered after propagating the field in the plane of the first object 6.38 mm, and the propagation distance must be increased by 6.38 mm to recover each subsequent object. The correct propagation distance for each reconstruction is indicated by the maximum values of the CC for

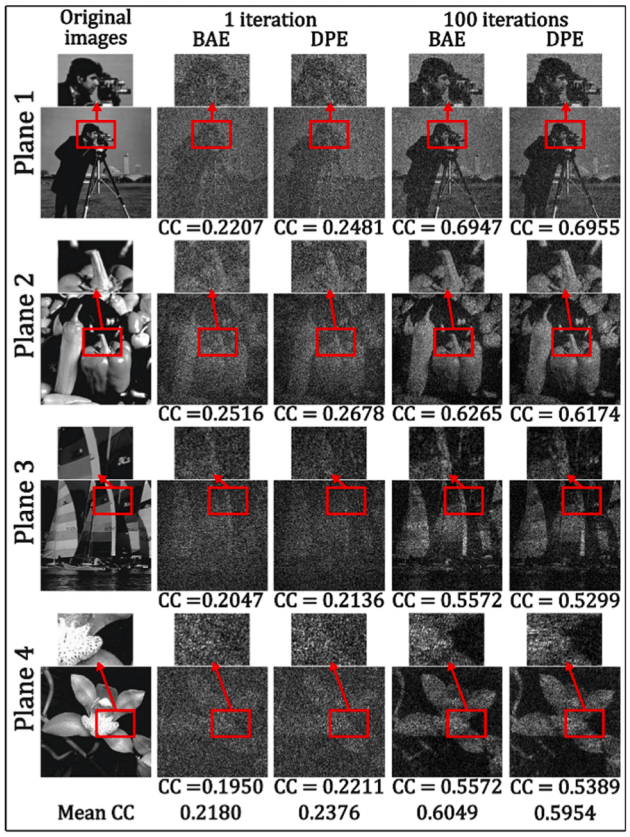


Fig. 9. Numerical results after JTC encryption-decryption of four-object multiplane holograms obtained using different numbers of GGS iterations and codified using different encoding algorithms. Below each column are the average CC values for all planes. BAE: binary amplitude encoding, DPE: double-phase encoding, CC: correlation coefficient.

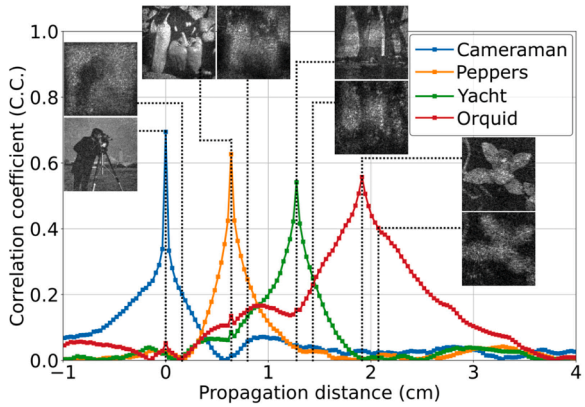


Fig. 10. Correlation coefficient between the decrypted BAE multiplane hologram and the original objects as a function of the propagation distance.

each image obtained at those distances. Deviating from the correct value by approximately 2 mm results in a defocused object with no indication of the presence of the others. The behavior is the same when using DPE as the encoding algorithm. These tests support the idea of strengthening system security and flexibility by using the propagation distance as an additional security parameter.

To test the maximum number of objects that can be simultaneously encrypted with this proposal, we encrypted and decrypted a multiplane hologram with 9 objects codified into it using the same object size, key size, and separation. Generating holograms with this increased number of planes took approximately 14.4 s.

Fig. 11 shows the results of this test. As in the previous case, the object recovered in the first plane has the best quality, with a decreasing trend in quality for objects located in more distant planes. The latter objects are not distinguishable when using a hologram generated with a single iteration of the GGS algorithm, and only become discernible after 100 iterations, albeit with a considerable amount of noise.

When considering the case with 100 iterations of the GGS algorithm, using BAE as the encoding algorithm results in decrypted objects with higher intensity compared to using DPE. As a result, the objects obtained with BAE present an overall higher CC, though some noise regions also show higher intensity when using BAE. Overall, both BAE and DPE provide similar results as encoding algorithms, although BAE generally produces a slightly higher CC.

Finally, the proposed method was also tested by encrypting multiplane holograms containing a variable number of objects. These holograms were generated using the same parameters specified for the test shown in Fig. 11. Specifically, 100 iterations of the GS algorithm and the GGS algorithm were employed to generate optimized keys and multiplane holograms of size 2160×2160 pixels, with a pixel size of 3.76 μm. The objects had a size of 320×320 pixels and were axially separated by a distance of 6.38 mm when illuminated by a beam with a wavelength of 532 nm. The results of this test are shown in Fig. 12.

This test was then repeated using BAE instead of DPE, obtaining the results shown in Fig. 13.

These results indicate that increasing the number of planes in the multiplane scene reduces the average reconstruction quality across all planes, as evidenced by the decreasing average correlation coefficient values across all planes. The decryption quality is particularly low for the planes that require longer propagation distances for recovery. However, despite this trend, BAE presents higher average quality, as measured by the CC, across all cases, ranging from 2 to 9 independent planes.

Based on these results, and considering the decreasing quality of the generated multiplane holograms as more objects are encoded, the proposed method allows for the simultaneous encryption of up to approximately 9 objects. Improved results could be achieved by using a significantly higher number of GGS iterations during hologram generation or by employing alternative phase retrieval algorithms; however, these options would increase computation time accordingly. Alternatively, deep learning techniques could be investigated to achieve superior results while maintaining or even reducing computational requirements.

8. Experimental results

To further support our proposal, we also conduct experimental tests using the setup shown in Fig. 14. This setup is an interferometric arrangement, where one arm has the proposed JTC encrypting system with complex modulation shown in Fig. 7, and the other arm provides a reference beam, which is only used to record the encryption key and is not needed for the encryption process. The phase-only codified hologram of the JTC input plane is projected using a GAEA-2, which has a maximum resolution of 4160×2464 pixels and a pixel size of 3.74 μm. The input plane is reconstructed by performing the optical FT of the SLM plane with a positive lens with a focal length of 20 cm. A spatial filter in this plane removes higher diffraction orders and the DC term. Subsequently, a second positive lens with a focal length of 15 cm performs an additional optical FT of this input plane, ensures that the intensity recording in the camera plane corresponds to the JPS between the scene to be encrypted and the optimized key. The camera used is a U3–3800CP-C-HQ digital camera with a resolution of 5536×3692 and a pixel size of 2.4 μm.

Once the JPS is recorded, the next step is to record the information of the phase-only encoded optimized key. For this purpose, the phase-only encoded optimized key is projected onto the SLM. The optimized key is

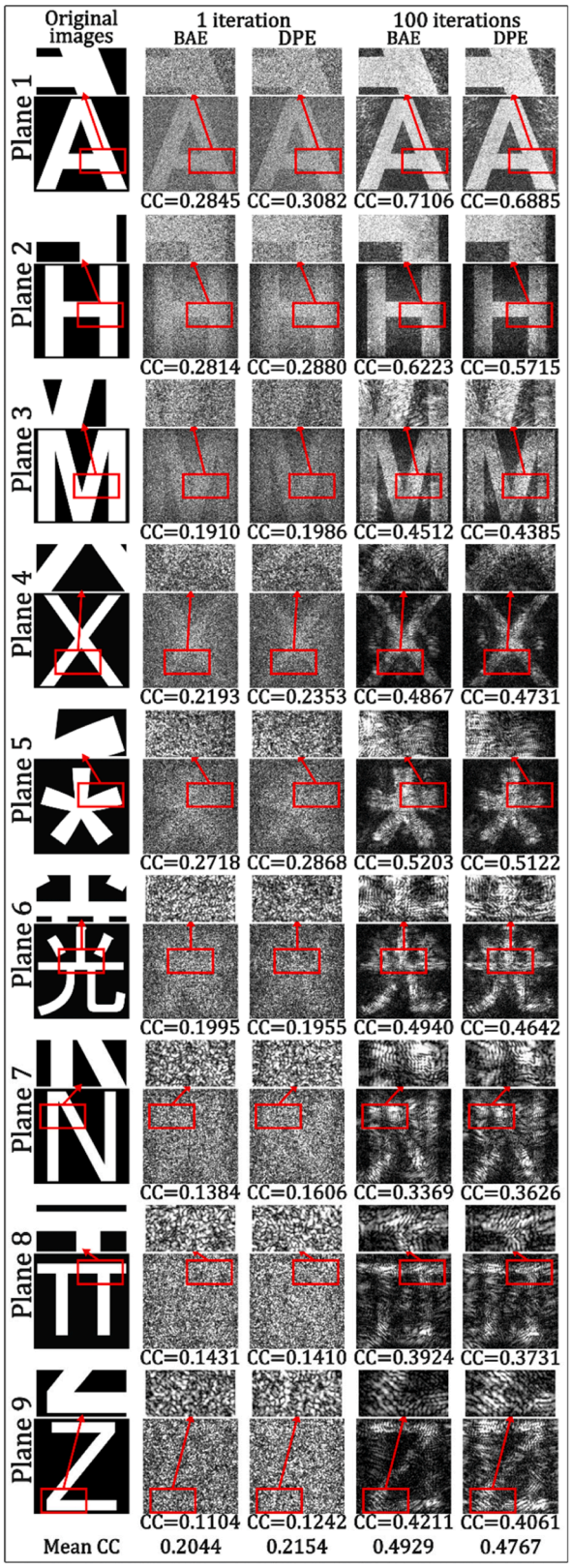


Fig. 11. Numerical results after JTC encryption-decryption of nine-object multiplane holograms obtained using different numbers of GGS iterations and codified using different encoding algorithms. Below each column are the average CC values for all planes. BAE: binary amplitude encoding, DPE: double-phase encoding, CC: correlation coefficient.

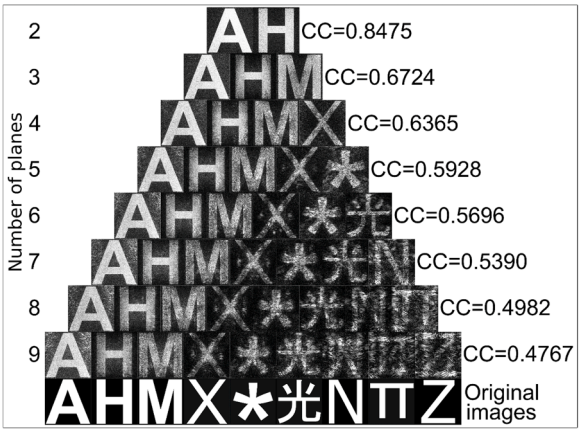


Fig. 12. Numerical results after JTC encryption-decryption of multiplane holograms containing different numbers of objects, codified with double phase encoding. The average correlation coefficient (CC) value for each case is displayed to the right of each row.

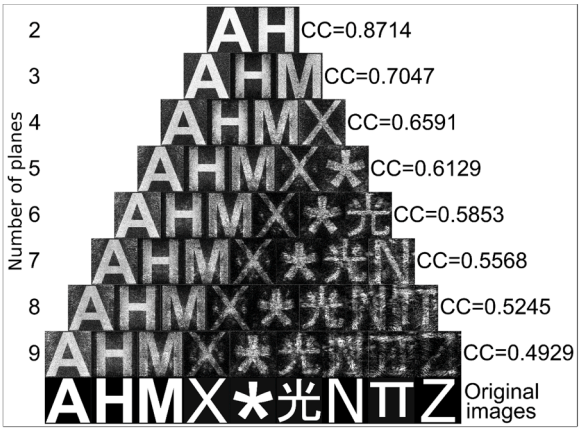


Fig. 13. Numerical results after JTC encryption-decryption of multiplane holograms containing different numbers of objects, codified with binary amplitude encoding. The average correlation coefficient (CC) value for each case is displayed to the right of each row.

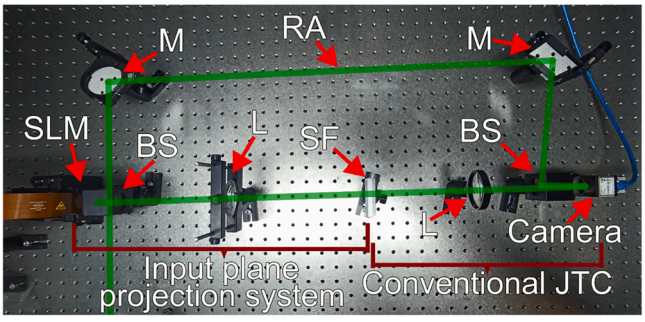


Fig. 14. Experimental setup. SLM: spatial light modulator, BS: beam splitter, M: mirror, SF: spatial filter, L: lens, RA: reference arm.

reconstructed at the same position as the JTC input plane by the lens with 20 cm of focal length. In this reconstruction plane, a spatial filter eliminates all higher diffraction orders and the DC term. The second lens, with a focal length of 15 cm, then performs its optical Fourier transform. The interference between the reference beam and the Fourier transform of the optimized key is recorded by the camera as an intensity pattern, representing the Fourier hologram of the optimized key. The

key information is then extracted from this hologram and subsequently used for decryption

The experimental setup was used to reproduce the previous tests. The codified holograms generated for the experimental tests had a size of 3840 × 2160 pixels.

Fig. 15 shows the experimental results when encrypting and decrypting nine-object multiplane holograms generated using 1 and 100 iterations of the GGS algorithm. Once again, each multiplane scene was encrypted using a key optimized with 100 iterations of the GS algorithm. Though the overall quality is inferior compared to the numerical simulations, the same behavior is observed. There is noticeable improvement when increasing the GGS iterations, as even the first objects are not clearly discernible when using a multiplane hologram generated with a single iteration of the GGS algorithm. The first object presents the best reconstruction quality and there is a decreasing trend for the subsequent objects. Compared to the holograms codified using DPE, the ones generated using BAE produce reconstructions with higher contrast compared to the background noise and a higher CC.

The BAE algorithm produced noticeable better results in experimental tests compared with DPE, in contrast to the numerical simulation where the difference was much smaller. This effect is believed to be due to the higher light efficiency produced by the holograms codified using the BAE algorithm compared to DPE [64], which results in brighter objects that are better differentiated from the background noise.

The results thus far indicate that BAE produces better results compared to DPE. In addition, BAE avoids one of DPE main drawbacks, as it does not limit the maximum size of the input plane that can be codified. To highlight this critical difference, we increased the object size from 320 × 320 to 420 × 420 pixels and performed numerical and experimental tests encrypting a multiplane hologram with 6 objects codified within it. This object size, along with the previous parameters, results in an input field extending that's too large to be codified into a 3840 × 2160 hologram using DPE [61]; however, the codification can be achieved using BAE [64]. The results of these tests are shown in Fig. 16. The trend from previous tests is maintained, achieving good reconstruction quality despite the larger size of the target objects in each plane. These results demonstrate that BAE allows codification, and consequently, encryption-decryption under conditions that were not possible with DPE.

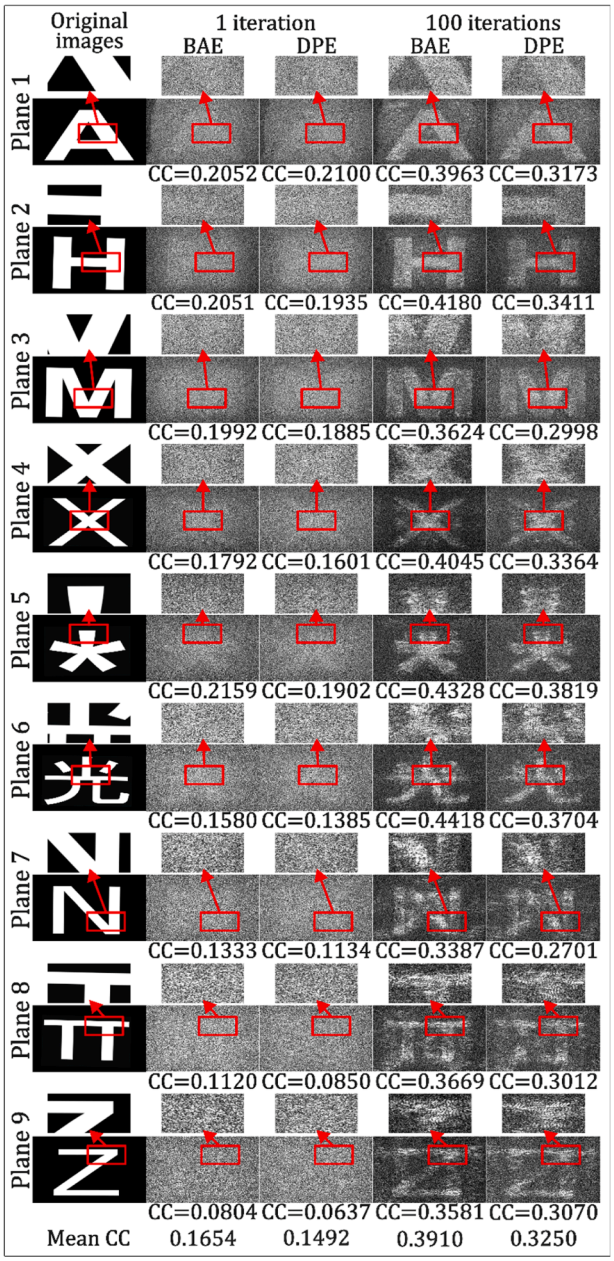


Fig. 15. Experimental results after JTC encryption-decryption of nine-object multiplane holograms obtained using different numbers of GGS iterations and codified with different encoding algorithms. Below each column are the average CC values for all planes. BAE: binary amplitude encoding, DPE: double-phase encoding, CC: correlation coefficient.

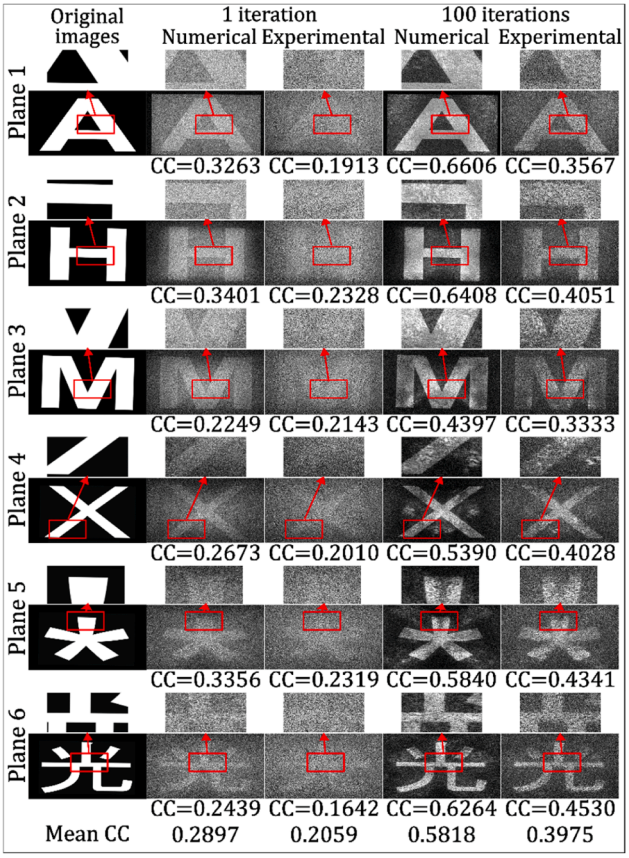


Fig. 16. Numerical and experimental results after JTC encryption-decryption of six-object multiplane holograms with larger objects obtained using different numbers of GGS iterations and codified with binary amplitude encoding. Below each column are the average CC values for all planes. CC: correlation coefficient.

9. Conclusions

We proposed a technique that uses computer generated holography encoding algorithms to enable fully complex modulation and control of the input plane of a JTC cryptosystem. The technique allowed us, for the first time to our knowledge, to use an experimental JTC DRPE cryptosystem to encrypt multiplane scenes. In doing so, we achieved simultaneous encryption of up to 9 different 2D objects, resulting in a single encrypted object. Each object is recovered only when using the correct encryption key and propagation distance, showing no obvious signs of the presence of the other objects. This behavior suggests the possibility of using multiplane schemes to increase the security of the cryptosystem.

Additionally, we compared the effects of using BAE and DPE as the encoding algorithm used in our proposal. Overall, BAE produced better results compared to DPE. BAE demonstrated a minor improvement in numerical tests but showed clear advantages in quality and capabilities when used in the experimental cryptosystem. This difference is thought to be due to the higher light efficiency of BAE compared to DPE. Additionally, BAE lifted the restriction on the maximum size of the input plane, allowing the encryption of objects with larger dimensions than was possible using DPE, thus increasing the versatility of the encryption scheme.

The results validate the capacity of the proposed scheme to encrypt arbitrary complex optical fields, within the resolution restrictions of the encoding algorithm used. This same approach could be extended to 3D scenes, objects with extended depth, or any combination of holographic scenes, enabling unparalleled flexibility to process holographic data with an experimental DRPE scheme. Further enhancements to the proposed technique could be achieved by exploring other phase retrieval algorithms, multiplane hologram generation algorithms, encoding algorithms, and different types of encryption keys that take advantage of the full complex modulation of this approach.

CRediT authorship contribution statement

Juan Andrés González-Moncada: Writing – original draft, Visualization, Software, Methodology, Investigation, Formal analysis, Conceptualization. **Alejandro Velez-Zea:** Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Methodology, Investigation, Funding acquisition, Formal analysis, Conceptualization. **John Fredy Barrera-Ramírez:** Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Methodology, Investigation, Funding acquisition, Formal analysis, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appear ed to influence the work reported in this paper.

Acknowledgment

Comité para el Desarrollo de la Investigación—CODI (Universidad de Antioquia—UdeA, Colombia); Sistema General de Regalías de Colombia (BPIN 2020000100464), OPTICA Foundation global challenge prize 2023.

Data availability

Data will be made available on request.

References

[1] Hu Y, Chen Q, Feng S, Zuo C. Microscopic fringe projection profilometry: a review. Opt Lasers Eng 2020;135:106192.
[2] Kim J, Jeon P, Lee H, Kim DY. High-frequency sinusoidal structured light generation with the anti-blaze condition of a digital micromirror device. Opt Lasers Eng 2024;176:108053.
[3] Ren YX, De Lu R, Gong L. Tailoring light with a digital micromirror device. Ann Phys 2015;527:447–70.
[4] Aguilar A, García-Márquez J, Landgrave JEA. Super-resolution with a complex-amplitude pupil mask encoded in the first diffraction order of a phase grating. Opt Lasers Eng 2020;134:106247.
[5] Abacousnac J, Grier DG. Dexterous holographic trapping of dark-seeking particles with Zernike holograms. Opt Express 2022;30:23568–78.
[6] Grier DG. A revolution in optical manipulation. Nature 2003;424:810–6.
[7] Shymkiv Y, Yuste R. Aberration-free holographic microscope for simultaneous imaging and stimulation of neuronal populations. Opt Express 2023;31:33461–74.
[8] Junge S, Schmieder F, Sasse P, Czarske J, Torres-Mapa ML, Heisterkamp A. Holographic optogenetic stimulation with calcium imaging as an all optical tool for cardiac electrophysiology. J Biophotonics 2022;15:1–14.
[9] Gopakumar M, Lee GY, Choi S, Chao B, Peng Y, Kim J, Wetzstein G. Full-colour 3D holographic augmented-reality displays with metasurface waveguides. Nature 2024;629:791–7.
[10] Liu K, Wu J, He Z, Cao L. 4K-DMDNet: diffraction model-driven network for 4K computer-generated holography. Opto-Electronic Adv 2023;6:220135.
[11] Kukolowicz R, Kozacki T, Chlipala M, Idicula MS, Martinez-Carranza J, Finke W, Gerej I. Digital holographic content manipulation for wide-angle holographic near-eye displays. Opt Express 2024;32:14565–81.
[12] Tseng E, Kuo G, Baek SH, Matsuda N, Maimone A, Schiffers F, Chakravarthula P, Fu Q, Heidrich W, Lanman D, Heide F. Neural étendue expander for ultra-wide-angle high-fidelity holographic display. Nat Commun 2024;15:1–8.
[13] Chang C, Ding X, Wang D, Ren Z, Dai B, Wang Q, Zhuang S, Zhang D. Split Lohmann computer holography: fast generation of 3D hologram in single-step diffraction calculation. Adv Photonics Nexus 2024;3:1–13.
[14] Blinder D, Ahar A, Bettens S, Birnbaum T, Symeonidou A, Ottevaere H, Schretter C, Schelkens P. Signal processing challenges for digital holographic video display systems. Signal Process Image Commun 2019;70:114–30.
[15] Javidi B, Carnicer A, Yamaguchi M, Nomura T, Pérez-Cabré E, Millán MS, Nishchal NK, Torroba R, Barrera-Ramírez JF, He W, Peng X, Stern A, Rivenson Y, Alfalou A, Brosseau C, Guo C, Sheridan JT, Situ G, Naruse M, Matsumoto T, Juvells I, Tajahuerce E, Lancis J, Chen W, Chen X, Pinkse PWH, Mosk AP, Markman A. Roadmap on optical security. J Opt 2016;18:083001.
[16] Refregier P, Javidi B. Optical image encryption based on input plane and fourier plane random encoding. Opt Lett 1995;20:767–9.
[17] Ibrahim DR, Sen J, Abdullah R. An overview of visual cryptography techniques. Multimed Tools Appl 2021;80:31927–52.
[18] Francis N, Thomas AL. Exploring recent advances in random grid visual cryptography algorithms. J Supercomput 2024;80:23205–24.
[19] Bachiphale PM, Zulpe NS. A comprehensive review of visual cryptography for enhancing high - security applications. Multimed Tools Appl 2024.
[20] Zhang C, Han B, He W, Peng X, Xu C. A novel compressive optical encryption via single-pixel imaging novel compressive optical encryption via single-pixel imaging. IEEE Photonics J 2019;11:1–8.
[21] C. Zhang, W. He, B. Han, M. Liao, D. Lu, X. Peng, and C. Xu, "Compressive optical steganography via single-pixel imaging," 27, 13469–78 (2019).
[22] Sui L, Pang Z, Cheng Y, Cheng Y, Xiao Z, Tian A, Qian K, Anand A. An optical image encryption based on computational ghost imaging with sparse reconstruction. Opt Lasers Eng 2021;143:106627.
[23] Xu C, Li D, Guo K, Yin Z, Guo Z. Computational ghost imaging with key-patterns for image encryption. Opt Commun 2023;537:129190.
[24] Javidi B, Towghi N, Maghzi N, Verrall SC. Error-reduction techniques and error analysis for fully phase- and amplitude-based encryption. Appl Opt 2000;39:4117–30.
[25] Vilardy JM, Torres Y, Millán MS, Pérez-Cabré E. Generalized formulation of an encryption system based on a joint transform correlator and fractional fourier transform. J Opt 2014;16:125405.
[26] Chang KM, Chen C, Wang J, Wang QH. Improved single-random-phase holographic encryption using double-phase method. Opt Commun 2019;443:19–25.
[27] Yu X, Chen H, Xiao J, Sun Y, Li X, Wang K. Incoherent optical image encryption based on coded aperture correlation holography. Opt Commun 2022;510:127889.
[28] Girija R, Singh H. Symmetric cryptosystem based on chaos structured phase masks and equal modulus decomposition using fractional fourier transform. 3D Res 2018;9:42.
[29] Velez-Zea A, Barrera-Ramírez JF, Torroba R. Optimized random phase encryption. Opt Lett 2018;43:3558–61.
[30] Velez-Zea A, Barrera-Ramírez JF, Torroba R. Customized data container for improved performance in optical cryptosystems. J Opt 2016;18:125702.
[31] Barrera-Ramírez JF, Mira-Agudelo A, Torroba R. Optical encryption and QR codes: secure and noise-free information retrieval. Opt Express 2013;21:5373–8.
[32] Barrera-Ramírez JF, Mira-Agudelo A, Torroba R. Experimental QR code optical encryption: noise-free data recovering. Opt Lett 2014;39:3074–7.
[33] Jaramillo-Osorio A, Barrera-Ramírez JF, Mira-Agudelo A, Velez-Zea A, Torroba R. High performance compact optical cryptosystem without reference arm. J Opt 2020;22:035702.
[34] Qin W, Peng X, Meng X. Cryptanalysis of optical encryption schemes based on joint transform correlator architecture. Opt Eng 2011;50:028201.
[35] Liao M, He W, Lu D, Peng X. Ciphertext-only attack on optical cryptosystem with spatially incoherent illumination: from the view of imaging through scattering medium. Sci Rep 2017;7:1–9.

[36] Barrera-Ramírez JF, Vargas-Castrillón C, Tebaldi M, Torroba R, Bolognini N. Known-plaintext attack on a joint transform correlator encrypting system. Opt Lett 2010;35:3553–5.
[37] Frauel Y, Castro A, Naughton TJ, Javidi B. Resistance of the double random phase encryption against various attacks. Opt Express 2007;15:10253–65.
[38] Barrera-Ramírez JF, Vargas-Castrillón C, Tebaldi M, Torroba R. Chosen-plaintext attack on a joint transform correlator encrypting system. Opt Commun 2010;283:3917–21.
[39] Huang Z-J, Cheng S, Gong L-H, Zhou N-R. Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform. Opt Lasers Eng 2020;124:105821.
[40] Singh H, Yadav AK, Vashisth S, Singh K. Fully phase image encryption using double random-structured phase masks in gyrator domain. Appl Opt 2014;53:6472–81.
[41] Singh H. Devil's vortex Fresnel lens phase masks on an asymmetric cryptosystem based on phase-truncation in gyrator wavelet transform domain. Opt Lasers Eng 2016;81:125–39.
[42] Tao S, Tang C, Shen Y, Lei Z. Optical image encryption based on biometric keys and singular value decomposition. Appl Opt 2020;59:2422–30.
[43] Jaramillo-Osorio A, Velez-Zea A, Mira-Agudelo A, Barrera-Ramírez JF, Torroba R. Secure selective recovery protocol for multiple optically encrypted data. Opt Lasers Eng 2021;137:106383.
[44] Abookasis D, Arazi O, Rosen J, Javidi B. Security optical systems based on a joint transform correlator with significant output images. Opt Eng 2001;40:1584–9.
[45] Vilardy JM, Millán MS, Pérez-Cabré E. Nonlinear optical security system based on a joint transform correlator in the Fresnel domain. Appl Opt 2014;53:1674–82.
[46] Rajput SK, Matoba O. Security-enhanced optical voice encryption in various domains and comparative analysis. Appl Opt 2019;58:3013–22.
[47] Mehra I, Nishchal NK. Optical asymmetric image encryption using gyrator wavelet transform. Opt Commun 2015;354:344–52.
[48] Rajput SK, Nishchal NK. Image encryption and authentication verification using fractional nonconventional joint transform correlator. Opt Lasers Eng 2012;50:1474–83.
[49] Mehra I, Rajput SK, Nishchal NK. Cryptanalysis of an image encryption scheme based on joint transform correlator with amplitude- and phase- truncation approach. Opt Lasers Eng 2014;52:167–73.
[50] Liu S, Guo C, Sheridan JT. A review of optical image encryption techniques. Opt Laser Technol 2014;57:327–42.
[51] Barrera-Ramírez JF, Velez-Zea A, Torroba R. Experimental scrambling and noise reduction applied to the optical encryption of QR codes. Opt Express 2014;22:20268–77.
[52] Velez-Zea A, Barrera-Ramírez JF, Torroba R. Cryptographic salting for security enhancement of double random phase encryption schemes. J Opt 2017;19:105703.
[53] Jiao S, Zhou C, Shi Y, Zou W, Li X. Review on optical image hiding and watermarking techniques. Opt Laser Technol 2019;109:370–80.
[54] Nomura T, Javidi B. Optical encryption using a joint transform correlator architecture. Opt Eng 2000;39:2031–5.
[55] Wang X, Chen W, Mei S, Chen X. Optically secured information retrieval using two authenticated phase-only masks. Nat Publ Gr 2015;5:15668.
[56] Chen Q, Shen X, Lin C, Wang H. Experimental research on JTC encryption system based on spiral phase mask and its characteristics. Opt Commun 2018;427:123–31.
[57] Vilardy JM, Millán MS, Pérez-Cabré E. Experimental optical encryption scheme for the double random phase encoding using a nonlinear joint transform correlator. Optik (Stuttg) 2020;217:164653.
[58] Liu Y, Shen X, Liu J, Peng K. Optical asymmetric JTC cryptosystem based on multiplication-division operation and RSA algorithm. Opt Laser Technol 2023;160:109042.
[59] 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 2019;112:56–64.
[60] Hoon Kwak C, Kim GYeup, Javidi B. Volume holographic optical encryption and decryption in photorefractive LiNbO ? : fe crystal. Opt Commun 2019;437:95–103.
[61] Arrizón V. Improved double-phase computer-generated holograms implemented with phase-modulation devices. Opt Lett 2002;27:595–7.
[62] González-Moncada JA, Velez-Zea A, Barrera-Ramírez JF. Experimental optical encryption with full complex modulation. Appl Opt 2024;63:4182–91.
[63] Shimobaba T, Takahashi T, Yamamoto Y, Hoshi I, Shiraki A, Kakue T, Ito T. Simple complex amplitude encoding of a phase-only hologram using binarized amplitude. J Opt 2020;22:045703.
[64] Shimobaba T, Wang F, Starobrat J, Kowalczyk A, Suszek J, Ito T. Comparison of double-phase hologram and binary amplitude encoding: holographic projection and vortex beam generation. Appl Opt 2023;62:7471–9.
[65] Velez-Zea A, Torroba R. Mixed constraint in global and sequential hologram generation. Appl Opt 2021;60:1888–95.
[66] Piestun R, Spektor B, Shamir J. Wave fields in three dimensions: analysis and synthesis. J Opt Soc Am A 1996;13:1837–47.
[67] Zhang C, Liao M, He W, Peng X. Ciphertext-only attack on a joint transform correlator encryption system. Opt Express 2013;21:28523–30.
[68] Cuche E, Marquet P, Depeursinge C. Spatial filtering for zero-order and twin-image elimination in digital off-axis holography. Appl Opt 2000;39:4070–5.
[69] Goodman JW. Speckle phenomena in optics: theory and applications. 2nd ed. SPIE Press; 2013.
[70] Velez-Zea A, Barrera-Ramírez JF, Torroba R. Innovative speckle noise reduction procedure in optical encryption. J Opt 2017;19:55704.
[71] Gerchberg RW, Saxton WO. A practical algorithm for the determination of phase from image and diffraction plane pictures. Optik (Stuttg) 1972;35:237–46.
[72] Velez-Zea A, Barrera-Ramírez JF. Double phase computer generated on-axis multiplane holograms. Opt Lasers Eng 2023;169:107681.
[73] Velez-Zea A, Barrera-Ramírez JF, Torroba R. Improved phase hologram generation of multiple 3D objects. Appl Opt 2022;61:3230–9.
[74] Makowski M, Sypek M, Kolodziejczyk A, Mikula G, Suszek J. Iterative design of multiplane holograms: experiments and applications. Opt Eng 2007;46:045802.
[75] Wang Z, Chen T, Chen Q, Tu K, Feng Q, Lv G, Wang A, Ming H. Reducing crosstalk of a multi-plane holographic display by the time-multiplexing stochastic gradient descent. Opt Express 2023;31:7413–24.
[76] Wang J, Wang J, Zhou J, Zhang Y, Wu Y. Crosstalk-free for multi-plane holographic display using double-constraint stochastic gradient descent. Opt Express 2023;31:31142–57.
[77] Liang C, Huang T, Dai Q, Li Z, Yu S. A single-sized metasurface for image steganography and multi-key information encryption. Engineering 2024;41:61–70.
[78] T. Shimobaba, S. Oshima, T. Kakue, and T. Ito, "Image quality enhancement of embedded holograms in holographic information hiding using deep neural networks," arXiv Prepr. arXiv2112.11246. (2021).