Hindawi
International Journal of Optics
Volume 2022, Article ID 6298010, 20 pages
https://doi.org/10.1155/2022/6298010

Research Article

Single-Pixel Compressive Digital Holographic Encryption System Based on Circular Harmonic Key and Parallel Phase Shifting Digital Holography

B. Lokesh Reddy and Anith Nelleri

School of Electronics Engineering, Vellore Institute of Technology (VIT), Chennai 600127, Tamil Nadu, India

Correspondence should be addressed to Anith Nelleri; anith.nelleri@vit.ac.in

Received 28 January 2022; Accepted 12 May 2022; Published 14 July 2022

Academic Editor: Wei Liu

An encryption system that combines compressive sensing (CS) and two-step parallel phase shifting digital holography (PPSDH) using double random phase encoding (DRPE) is presented in this paper. The two-step PPSDH is a linear inline holographic scheme and is much suitable for encrypting the 2D/3D information in a single exposure. The distribution of random phase mask (RPM) in the DRPE is implemented using circular harmonic key which increases the security of the encryption process. In this system, the keys used to encrypt are spatial positions of the planes, wavelength, and rotation of the circular harmonics in RPMs, and CS acts as an additional key that makes the system more secure than the conventional optical encryption methods. At the transmission end, two-step PPSDH is applied to encrypt the object information in single hologram. The digital mirror device (DMD) is placed between the object and a single-pixel detector for acquiring fewer hologram measurements. At the receiver end, the single digital hologram is numerically recovered by using a CS optimization problem. The original complex object field is decrypted from the CS recovered holograms by the inversion of two-step PPSDH process with the help of the correct keys. The numerical simulations are presented for complex 2D and 3D objects to test the feasibility of the proposed encryption and decryption system. The proposed method carried out intensity and phase reconstruction of the original object field using single-pixel compressive imaging. The computer simulation results demonstrated that the encrypted information is highly secured with the rotation of the circular harmonic key. The sensitivity of the decrypted intensity and phase images is also studied with variations of the encrypted keys. The obtained results show that the proposed encryption scheme is feasible and has better security performance and robustness.

1. Introduction

Digital holography [1–7] is a promising technique to sense and retrieve 3D object information such as amplitude and phase of the object. The optically generated and digitally sensed holograms are numerically reconstructed to obtain 3D object features. The sensed digital hologram is a real-valued digital image. The retrieved 3D information from the digital hologram is a 2D complex image that contains 3D information of the object in the form of intensity and phase. Thus, the existing 2D image processing algorithms can adapt to process 3D information from 2D digital complex images. The optically generated and digitally sensed holograms are numerically reconstructed to obtain the 3D object features. The sensed digital hologram is a real-valued digital image. Digital holography has been widely used in many applications in the areas of phase contrast imaging [8, 9], 3D microscopy [10, 11], 3D object recognition [6, 12], information security [13, 14], surface shape measurement [15–17], interferometry [18, 19], etc.

The optoelectronic and computational imagining concepts involved in digital holography enable us to sense the compressed holographic data by digital sensors. Later on, it can be reconstructed with good accuracy using computational techniques. The compressive sensing (CS) techniques [20–25] can adapt well to digital holography as the process

involves the detection of holographic data in the transform domain. This opens up new avenues for combining compressive data sensing with information security or encryption. Thus, the sensing and computing modalities of digital holography have complemented the CS framework. It has emerged as a secured CS 3D information system with a high data transmission rate and less storage space. The CS [20–25] is a paradigm shift in signal sampling theory that deals with reconstruction of the original signal from fewer samples than those of the Nyquist sampling rate. CS is an iterative procedure to reconstruct the original signal from the incomplete linear measurements by exploiting the sparsity of the signal. In the CS theory, the most commonly used sparse representations of the signal are FFT, DCT, Wavelet, etc. and help in accurate reconstruction of the original signal. CS framework is applied in holographic encryption for sampling and compression in order to reduce the hologram acquisition data and electronic data-processing load at sensors.

In conventional digital holographic encryption/decryption methods, the encrypted information is transmitted at the Nyquist sampling rate. The sender and receiver use a secret key to decrypt the encrypted information. The transmission of hologram requires a large amount of data storage, but the transmission channel bandwidth is limited. Traditionally, holographic encryption methods are implemented based on double random phase encoding (DRPE) [26–31], joint transform correlator (JTC) [32, 33], and ghost imaging (GI) [34], along with the encryptions based on the Fresnel domain [27, 29, 35, 36], Fourier domain, or fractional Fourier domain [37–40]. The CS based encryption methods have the additional advantage that the encryption depends on the measurement matrix (sampling mask) used for the sensing process which will enhance the security level and act as an additional key, which is not used in the conventional optical encryption systems. CS can be implemented in the optical domain using a digital micromirror device (DMD) and a single-pixel detector [41]. A DMD device is a reflective spatial light modulator introduced by Texas instruments that contain many micromirrors. The light incident on the DMD is modulated with the sampling matrix, and then a single-pixel detector records the measurements depending on the orientation of the mirrors [41, 42]. A single-pixel detector sequentially measures the light field that is reflected from the DMD device. The sensed information of a single-pixel detector ($K \ll M$ measurements) is converted from analog to digital information using A/D convertor, and it transmits K random linear measurements of the object under recording. The encrypted information is numerically reconstructed using the CS optimization algorithm [20–25] from fewer measurements. A single-pixel detector can reduce the size and complexity of the sensor at the transmitting end.

In recent years, CS-based optical encryption methods have been increasing the demand for many optical information processing applications [41–53]. The idea of the single-pixel imaging was first proposed by Duarte et al. [41]. Bromberg et al. [43] have demonstrated a real-time pseudo-thermal GI using a combination of the DMD and single-pixel detector. Di et al. [44] have proposed multiple image encryption based on single-pixel compressive holography to encrypt the holograms. The decryption process of each image was carried out using total variation minimization problem. Clemente et al. [45] have adapted a phase shifting digital holography (PSDH) technique with a single-pixel detector to demonstrate the compressive holographic encryption. This method has experimentally reconstructed the amplitude of the ophthalmic lens by retaining only 20% of the hologram pixels. Li et al. [46, 47] have numerically presented a compressive optical image encryption method for inline PSDH by adopting the single-pixel imaging. In this work, the phase shifted digital holograms were acquired using single-pixel detector. In the reconstruction process, the encrypted holograms were reconstructed by retaining various hologram measurements (such as 60%, 80%, and 90%). Finally, the intensity of the original object wavefield was decrypted from the reconstructed holograms by the inversion of PSDH process. Leihong et al. [48] have experimentally presented compressive ghost imaging encryption based on PSDH. The simulation results have shown that the CS scheme improved the security and reconstruction quality of the intensity image. Wang et al. [49] have presented single-pixel compressive holographic encryption by modifying the Mach–Zehnder interferometer setup for multiple-3D-object imaging based on multiple interferences. The numerical simulation results have shown the accurate reconstruction of original 3D object intensity information from encrypted hologram measurements. It has been demonstrated that the cryptosystem provides high encryption capacity and robustness with multiple interferences. Recently, Du et al. [50] have proposed an efficient CS based optical image encryption system using single-pixel imaging. In this method, the input image is encrypted using one random phase mask (RPM) with various recording distances as one-dimensional vector key. It has been numerically presented that the one RPM key at different recording distances minimized the key storage requirement of data transmission and also enhanced the robustness of the encryption system. The encryption systems [44–50] were proposed based on inline schemes such as four-step, three-step, or two-step PSDH. Moreover, the phase reconstruction of the encrypted object field is not presented in the single-pixel compressive holography. The strength of digital holography is the ability to reconstruct the phase information and has great applications in 3D imaging of moving objects. Although the phase reconstruction is accurate in classical PSDH, it is not suitable for moving objects because it involves multiple exposures. On the other hand, to acquire instantaneous 3D image of object wavefield, parallel phase shifting digital holography (PPSDH) [54–56] was proposed. The PPSDH is a single exposure scheme that can be used for imaging moving objects or static objects. In the present work, single-pixel compressive imaging is demonstrated based on PPSDH and circular harmonic keys in DRPE scheme for improving the security level and storage efficiency of holographic data.

The encrypted hologram measurements can be realized with much less criteria than those of the Nyquist sampling.

In this paper, a CS based encryption method to encrypt the complex object information by using linear two-step PPSDH and a circular harmonic key in DRPE is demonstrated. The holographic encryption system is implemented using a phase-only key with the random spatial distribution of circular harmonics in the Fresnel domain to improve the system security performance. The single-pixel compressive imaging is adapted with two-step PPSDH for compression of the encrypted holograms in the optical domain. During the encryption process, the two RPMs, the measurement matrix, the distance, and the wavelength of Fresnel transform are encryption keys. Compared with the traditional encryption scheme, the transmitted information can be significantly reduced with single-shot exposure method, and the circular harmonic key is associated with RPM, which improves the security of the system. In the proposed system, the quality of reconstructed hologram is guaranteed with much less rate than that of the Nyquist sampling. The proposed system is validated using computer simulations to show the proof of the concept. The robustness and key space security of the proposed encryption system have been verified with minimal pixel detection. The CS reconstruction framework was implemented using the Total Variation Minimization by Augmented Lagrangian and Alternating Direction Algorithm (TVAL3) [24]. The efficacy of the proposed cryptosystem has been analyzed using various performance metrics, and also the key space security and robustness of our method have been examined.

2. Proposed Encryption and Decryption Scheme Using a Circular Harmonic Key in DRPE

The schematic representation of the optical encryption arrangement of DRPE using the circular harmonic key in the Fresnel domain is shown in Figure 1(a). In this method, the RPM is expressed in terms of polar coordinates using a circular harmonic key [57, 58] to enhance the security of the optical system. To obtain the circular harmonic key, the Cartesian coordinates (x, y) are converted to the polar coordinates (ρ, φ) using $x = \rho\cos\varphi$ and $y = \rho\sin\varphi$. Thus, the RPM key can be expressed in the Fresnel domain as

$$P(\rho, \varphi) = \exp[i\Phi(\rho, \varphi)], \tag{1}$$

where Φ contains the distribution of random values. The key can be decomposed into circular harmonics [56] with the position (ρ, φ) as the center, which is expressed as follows:

$$\Phi(\rho\cos\varphi, \rho\sin\varphi) = \Phi(\rho, \varphi) = \sum_{m=-\infty}^{\infty} \Phi_m(\rho)\exp[im\varphi], \tag{2}$$

where m is the order of circular harmonics and $\Phi_m(\rho)$ can be calculated as follows:

$$\Phi_m(\rho) = \frac{1}{2\pi}\int_0^{2\pi} \Phi(\rho, \varphi)\exp[im\varphi]\mathrm{d}\varphi. \tag{3}$$

Now, the RPM using a circular harmonic key in the Fresnel domain is defined as follows:

$$P_m(\rho, \varphi) = \exp[i\Re\{\Phi_m(\rho, \varphi)\}], \tag{4}$$

where $\Re$ is the real part of $\Phi_m(\rho, \varphi)$; Φ_m contains the distribution of random values and polar coordinates $\rho = \sqrt{x^2 + y^2}$. The circular harmonic given in (4) is rotation-symmetric, and $\Phi_m(\rho)$ highly depends on the position (ρ, φ). Now, the first RPM_1 is expressed as follows:

$$P_m(\rho_1, \varphi_1) = \exp[i\Re\{\Phi_m(\rho_1, \varphi_1)\}] = \mathrm{RPM}_1, \tag{5}$$

and similarly, the second RPM_2 can be expressed as follows:

$$Q_m(\rho_2, \varphi_2) = \exp[i\Re\{\Phi_m(\rho_2, \varphi_2)\}] = \mathrm{RPM}_2. \tag{6}$$

The inclusion of circular harmonic function [57, 58] in the random phase masks imparts additional degrees of freedom of encoding such as order of harmonics (m), radius (ρ_1, ρ_2), and rotation angle (φ_1, φ_2) to strengthen the security level of the encryption system. Therefore, the proposed encryption scheme with keys in polar coordinates is a solution to the problem of variance in the decryption process. The degree of rotation angle and the order of the circular harmonic key in the RPMs increase the complexity of DRPE process, thus breaking the keys.

The encryption process involves three different planes, i.e., the input plane, the intermediate Fresnel transform plane, and the output plane. The optical system is illuminated with a plane wave of wavelength λ, and the encrypted complex object information is obtained at the output plane in the Fresnel domain. The object $O(x_i, y_i)$ which is located in the input plane (x_i, y_i) is bonded with RPM_1. When the plane wave propagates through the system, the random phase mask distribution $P_m(\rho_1, \varphi_1)$ gets multiplied by $O(x_i, y_i)$ which results in primary random phase encoding. The propagation of this field to the plane at a distance d_1 from the input plane and the resulting complex Fresnel field is denoted by $U(x', y')$ as given in (7). At distance d_1, the field $U(x', y')$ gets multiplied by the second random phase mask $Q_m(\rho_2, \varphi_2)$ resulting in second random phase encoding in the Fresnel plane. This field is further propagated to the output plane by a distance d_2 to obtain the Fresnel encrypted field $G(x_0, y_0)$ as given in (8). The free space propagation corresponding to each plane is modeled by a Fresnel transform with the corresponding distance.

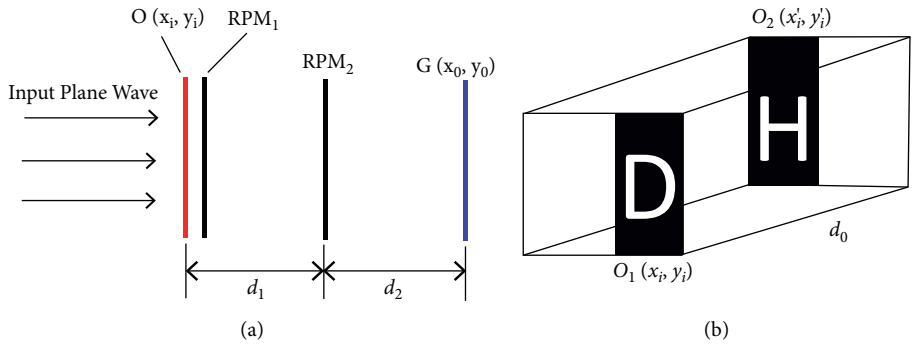


FIGURE 1: (a) Schematic setup of the DRPE in Fresnel domain illustrating the principle of the encryption system: $O(x_i, y_i)$ is a 2D complex object; RPM_1 and RPM_2, are random phase masks; $G(x_0, y_0)$ is the DRPE information obtained after the two phase masks; d_1 and d_2 are distances between the planes. (b) 3D complex object used in the simulation: $O_1(x_i, y_i)$ is an object at plane 1; $O_2(x_i', y_i')$ is an object at plane 2; d_0 is the distance between the two planes.

$$U(x', y'; d_1) = \frac{e^{ikd_1}}{i\lambda d_1} \iint O(x_i, y_i) P_m(\rho_1, \varphi_1) \exp \frac{i\pi}{\lambda d_1} \left[(x' - x_i)^2 + (y' - y_i)^2 \right] \mathrm{d}x\mathrm{d}y, \tag{7}$$

$$G(x_0, y_0; d_2) = \frac{e^{ikd_2}}{i\lambda d_2} \iint U(x', y') Q_m(\rho_2, \varphi_2) \exp \frac{i\pi}{\lambda d_2} \left[(x_0 - x')^2 + (y_0 - y')^2 \right] \mathrm{d}x\mathrm{d}y. \tag{8}$$

For simplicity, (7) and (8) can be written as follows:

$$G(x_0, y_0) = \mathcal{F}rT_{\lambda, d_2} \left\{ Q_m(\rho_2, \varphi_2) \cdot \mathcal{F}rT_{\lambda, d_1} \{ O(x_i, y_i) \cdot P_m(\rho_1, \varphi_1) \} \right\}. \tag{9}$$

Now, decryption process can be expressed as follows:

$$O(x_i, y_i) = \mathcal{F}rT^{-1}_{\lambda, d_1} \left\{ \mathcal{F}rT^{-1}_{\lambda, d_2} \{ G(x_0, y_0) \cdot Q^*_m(\rho_2, \varphi_2) \} P^*_m(\rho_1, \varphi_1) \right\}, \tag{10}$$

where $\mathcal{F}rT$ is forward Fresnel transform and $\mathcal{F}rT^{-1}$ is inverse Fresnel transform. The decryption process is the same as the encryption shown in (10), but in the reverse direction with complex conjugate of the random phase masks and inverse Fresnel transforms. The Fresnel transform is inverted using the correct keys to obtain the original complex object information.

The 3D complex object used in the encryption system is shown in Figure 1(b). The 3D object construction can be considered as the integration of different sections of complex planes with certain features separated by a small distance d_0 which is analogous to the depth information of the object. Computationally, this is realized by combining the front and back plane with features as shown in Figure 1(b) using the Fresnel transform between the planes corresponding to a distance d_0. Then, 3D object optical encryption process can be expressed as follows:

$$G(x_0, y_0) = \mathcal{F}rT_{\lambda, d_2} \left\{ Q_m(\rho_2, \varphi_2) \cdot \mathcal{F}rT_{\lambda, d_1} \left\{ P_m(\rho_1, \varphi_1) \cdot O_2(x_i', y_i') \cdot \mathcal{F}rT_{\lambda, d_0} \{ O_1(x_i, y_i) \} \right\} \right\}. \tag{11}$$

Similarly, the 3D complex object decryption process is given in the following equations:

$$O_2(x_i', y_i') = \mathcal{F}rT^{-1}_{\lambda,d_1}\left\{\mathcal{F}rT^{-1}_{\lambda,d_2}\{G(x_0, y_0)\}.Q^*_m(\rho_2, \varphi_2)\right\} \cdot P^*_m(\rho_1, \varphi_1), \tag{12}$$

$$O_1(x_i, y_i) = \mathcal{F}rT^{-1}_{\lambda,d_0}\{O_2(x_i', y_i')\}, \tag{13}$$

where d_0 is the distance between two planes, and $O_1(x_i, y_i)$ and $O_2(x_i', y_i')$ are the decrypted 3D object fields at the front and back plane, respectively. Two important features have to be considered for optical encryption techniques. Firstly, the encrypted field must be resistant to attacks, and secondly, the end user has to decrypt the information without any difficulty at the receiver end. An authentic user with the knowledge of RPMs and their circular harmonic key distributions can only decrypt the encrypted information. Thus, circular harmonics improve the security of the optical encryption and decryption process. In this method, the decryption procedure significantly increases the key space security with the operating wavelength, and the spatial positions of the phase mask between the adjacent planes are additional keys for the robust decryption.

The proposed optical encryption system consists of a single-pixel compressive holographic imaging system based on two-step PPSDH that encrypts the complex object information using DRPE and circular harmonic keys. Figure 2 shows the schematic of the proposed optical setup using Mach–Zehnder interferometric recording geometry. The light beam from the laser is divided into two parts using a polarizing beam splitter (PBS). The half wave plates are used to control the intensity and polarization of the interfering light beams. In the object arm, the complex object information is encrypted using DRPE in the Fresnel domain using two RPMs and circular harmonic keys. A phase array device PSLM is used in the reference wave arm to give the required phase shifts to the reference wave in an interleaved manner as mentioned in Section 3. The interference field formed by the encrypted and reference beams is sampled using a DMD by modulating it with a chosen measurement matrix (i.e., sampling mask) for a specific sample ratio. The output of the DMD is coupled to a single-pixel photodetector using a convex lens. Thus, the incomplete measurements of the encrypted single digital Fresnel hologram on the photodetector are obtained. The mathematical model of the proposed encryption and decryption using PPSDH and single-pixel compressive imaging is presented in Section 3.

3. Two-Step PPSDH Approach for Proposed Encryption and Decryption Using Single-Pixel Compressive Imaging

In this section, we present mathematical framework for numerical demonstration of single-pixel digital holographic scheme based on two-step PPSDH and DRPE, in which the random phase masks use circular harmonic key in the Fresnel domain. The flow diagram of the proposed encryption and decryption procedure is shown in Figure 3. The optical encryption technique uses DRPE in the Fresnel domain based on circular harmonic key as explained in Section 2. Let us consider that the input object field $O(x_i, y_i)$ of size $M \times N$ to be encrypted is multiplied by RPM_1. Then, Fresnel transform is performed through propagation distance d_1 and a complex Fresnel field is obtained as described in the following equation:

$$U(x', y') = \mathcal{F}rT_{\lambda,d_1}\{O(x_i, y_i) \cdot \mathrm{RPM}_1\}, \tag{14}$$

where $\mathcal{F}rT$ represents Fresnel transform. $U(x', y')$ field is obtained after RPM1 is multiplied by RPM2. Then, another Fresnel transform is performed, and the obtained encrypted Fresnel field in the DMD plane can be expressed as in the following equation:

$$G(x_0, y_0) = \mathcal{F}rT_{\lambda,d_2}\{U(x', y').\mathrm{RPM}_2\}. \tag{15}$$

Here, RPM_1 and RPM_2 are two independent random phase masks. Now, linear two-step PPSDH [54, 55, 58, 59] is applied for obtaining single-shot inline hologram on the DMD plane, in which a phase array device such as spatial light modulator is used to give phase shifts to the reference wave in an interleaved manner with a periodic phase of $\theta = \{0, -\pi/2\}$. The complex encrypted field $G(x_0, y_0)$ is interfered by the reference wave $R_\theta(x_0, y_0)$. The single-shot inline hologram $H_\theta(x_0, y_0)$ generated on the DMD plane can be expressed as follows:

$$H_\theta(x_0, y_0) = \left|G(x_0, y_0) + R_\theta(x_0, y_0)\right|^2, \tag{16}$$

where

$$R_\theta(x_0, y_0) = \left\{\frac{R_0(x_0, y_0) \text{ when } (x, y) = (\text{even}, \text{even})}{R_{-(\pi/2)}(x_0, y_0) \text{ when } (x, y) = (\text{odd}, \text{even})}\right\}, \quad \text{For}, x_0, y_0 = 0 \text{ to } N - 1. \tag{17}$$

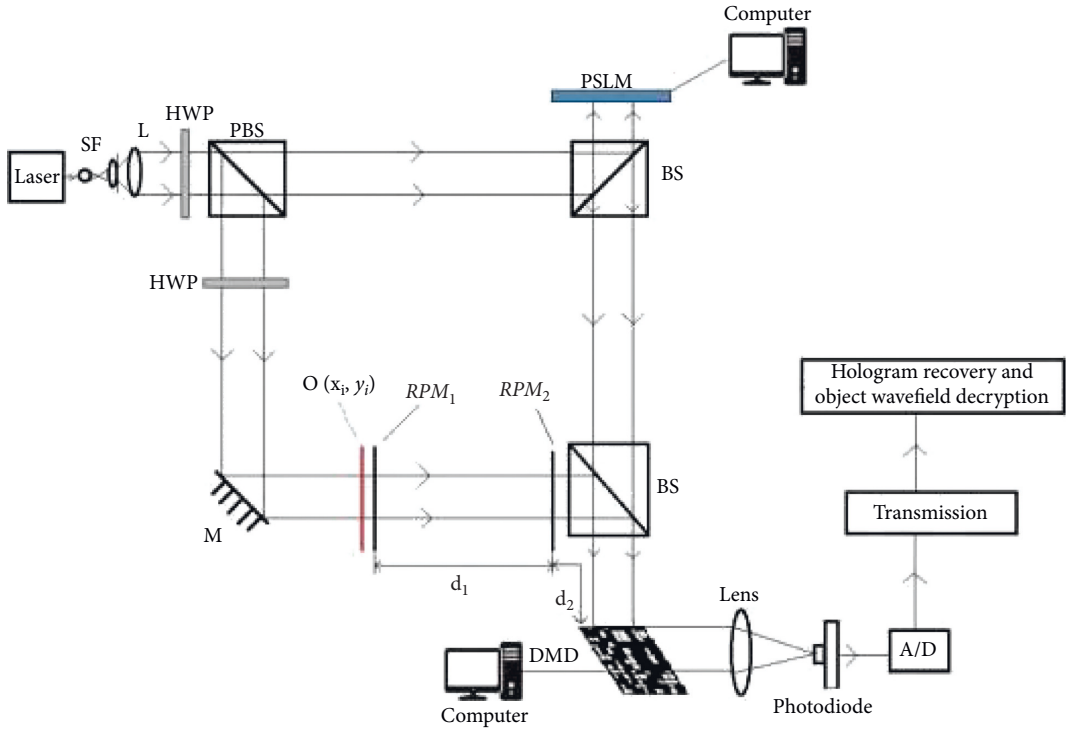


FIGURE 2: Schematic setup of PPSDH and single-pixel compressive imaging for encryption and decryption. SF: spatial filtering, L: collimation lens, PBS: polarizing beam splitter, HWP: half wave plate, M: mirror, RPM: random phase mask, PSLM: phase-only spatial light modulator, BS: beam splitter, DMD: digital micromirror device.

Therefore, the digital hologram on the DMD plane is governed by the following equation:

$$H_\theta(x_0, y_0) = \left\{ \frac{H_0(x_0, y_0; 0) \text{ when } (x, y) = (\text{even, even})}{H_{-(\pi/2)}(x_0, y_0; -(\pi/2)) \text{ when } (x, y) = (\text{odd, even})} \right\}, \quad \text{For, } x_0, y_0 = 0 \text{ to } N - 1. \tag{18}$$

Now, the measurement matrix Ψ in the DMD is modulated with single-shot hologram $H_\theta(x_0, y_0)$. The random measurement matrix is generated numerically using pseudorandom generator sequences of 0 and 1. Then, the modulated light field reflected from a DMD is measured by a single-pixel detector through M computations of the measurement matrix, and $M \times 1$ linear measurements Y are obtained. The output of the single-pixel detector [41, 59] can be numerically obtained by computing the inner product of the interference filed H_θ and the M computations of the random measurement matrix Ψ with various sample ratios in the DMD plane:

$$Y = \Psi \cdot H_\theta, \tag{19}$$

where $Y \in R^{M\times 1}$ is incomplete measurement data, $\Psi \in R^{M\times N}$ is random vector generated in the DMD, and $H_\theta \in R^{N\times 1}$ is interference filed on the DMD plane.The encrypted incomplete linear measurements are transmitted through the channel and are decrypted at the receiver end. Both sender and receiver share secret keys to decrypt the encrypted information. In the encryption process, the linear measurements $K \ll M$ samples with K nonzero entries are considered less than the Nyquist sampling rate. In the decryption process, first the CS framework is used to recover the original single-shot hologram H_θ from incomplete measurements Y by solving optimization problem [24].

$$\tilde{H}_\theta = \underbrace{\min}_{H_\theta} \sum_{i=1}^{N^2} \left\| D_i H_\theta \right\|_1 \text{ subject to } Y = \Psi \cdot H_\theta, \tag{20}$$

where D_i denotes discrete gradient of the vector H_θ at position i. Here, $\tilde{H}_\theta$ denotes the recovered single-shot hologram using CS method. Now, the individual phase shift holograms $\tilde{H}_0(x_0, y_0)$ and $\tilde{H}_{-(\pi/2)}(x_0, y_0)$ are separated from single hologram with periodic loss of pixels, and then the separated holograms' values of the vacant pixels are interpolated to obtain the new guess values. The complex Fresnel field $G(x_0, y_0)$ on the DMD plane is obtained using Meng's two-step PSDH formula [43, 60] as given in (21)–(24) and then inverts the encryption process to reconstruct the original object field.

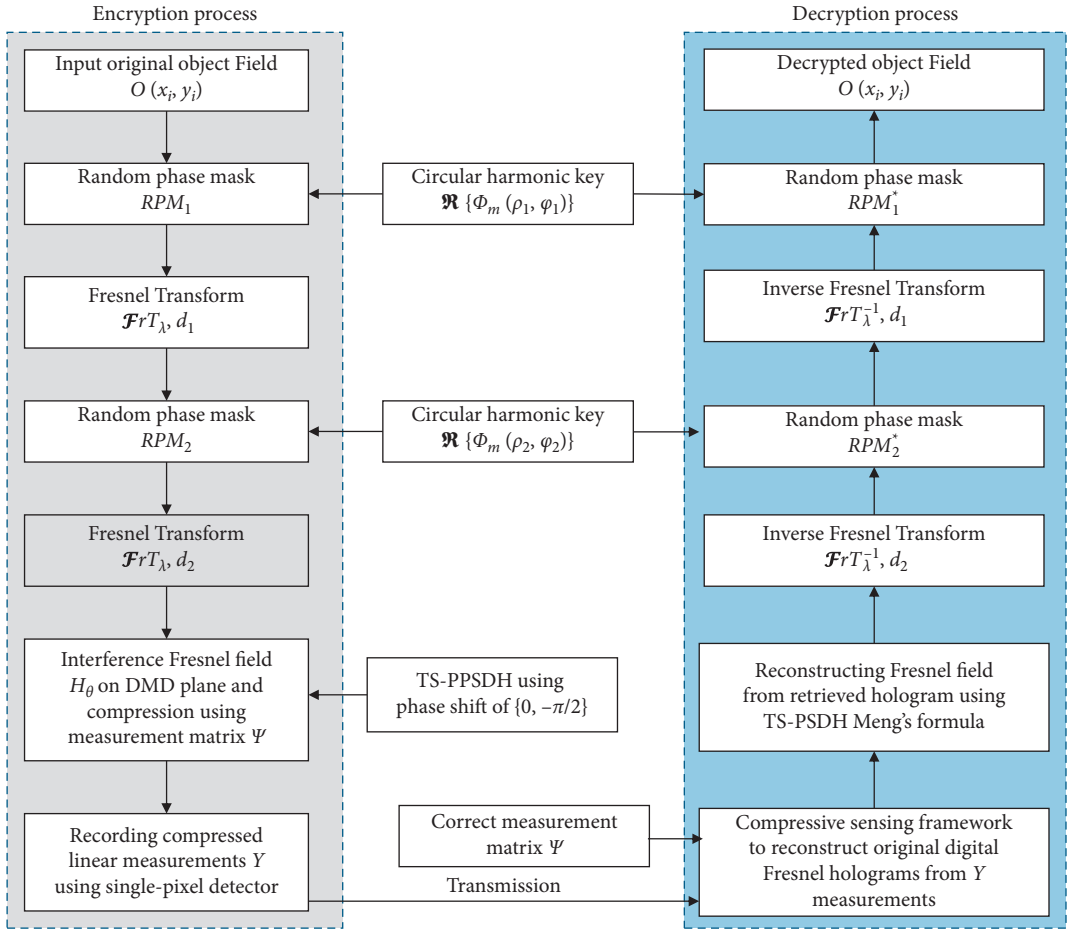


Figure 3: Flowchart of compressive digital holographic encryption and decryption system.

$$G(x_0, y_0) = \frac{\{\tilde{H}_0(x_0, y_0) - a(x_0, y_0)\} - i\{\tilde{H}_{-(\pi/2)}(x_0, y_0) - a(x_0, y_0)\}}{2A_r}, \tag{21}$$

where

$$a(x_0, y_0) = 0.5 * \left\{v - \left(v^2 - 2w\right)^{0.5}\right\}, \tag{22}$$

$$v = \tilde{H}_0(x_0, y_0) + \tilde{H}_{-(\pi/2)}(x_0, y_0) + 2A_r^2, \tag{23}$$

$$w = \tilde{H}_0(x_0, y_0)^2 + \tilde{H}_{-(\pi/2)}(x_0, y_0)^2 + 4A_r^2. \tag{24}$$

The retrieved complex field $G(x_0, y_0)$ is inverse Fresnel propagated by a distance d_2 and multiplied by conjugate of RPM_2 to obtain original field $U(x', y')$:

$$U(x', y') = \mathcal{F}rT_{\lambda, d_2}^{-1}\{G(x_0, y_0)\} \cdot \mathrm{RPM}_2^*. \tag{25}$$

To reconstruct the original encrypted object filed, $U(x', y')$ is inverse-Fresnel-transformed by the distance d_1 and then multiplied by the conjugate phase of the RPM_1.

$$O(x_i, y_i) = \mathcal{F}rT_{\lambda, d_1}^{-1}\{U(x', y')\} \cdot \mathrm{RPM}_1^*. \tag{26}$$

The sample ratio of the measurement matrix is calculated using the formula $(C/L)^*100$, where C is the sample size of compression and L is the size of the original object M^*N. We reduced the sample ratio parameter "C" to study the performance of the hologram compression. The higher the sample size "C," the higher the image quality. To measure the quality of the decrypted complex images, we calculated mean square error (MSE) and relative error (RE) between the original object image and decrypted image, expressed as follows:

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{x_i=1}^{M} \sum_{y_i=1}^{N} \left[\tilde{O}(x_i, y_i) - O(x_i, y_i)^2\right], \tag{27}$$

$$\mathrm{RE} = \frac{\sum_{x_i=1}^{M} \sum_{y_i=1}^{N} \left|\left|\tilde{O}(x_i, y_i)\right| - \left|O(x_i, y_i)\right|\right|^2}{\sum_{x_i=1}^{M} \sum_{y_i=1}^{N} \left|O(x_i, y_i)\right|^2}, \tag{28}$$

where M and N are the size of the original object, $\widetilde{O}(x_i, y_i)$ is the decrypted complex object wave with compression, and $O(x_i, y_i)$ is the original complex object wave. It can be seen from encryption and decryption system that five keys are used: RPM keys with angles φ_2 and φ_2, distance between two adjacent planes d_1 and d_2, measurement matrix Ψ, and wavelength λ, and the radii of circular harmonic ρ_1 and ρ_2 values stored in the encryption process act as the additional keys in the decryption process. Thus, the proposed system improves the security of the encryption effectively. In the proposed technique, the two-step PPSDH and circular harmonic key in DRPE are combined to improve the reconstruction accuracy and security performance of the decrypted information. The main idea of the digital holographic technique integrated with the single-pixel detector and CS theory is to obtain both the intensity and phase information of a complex 2D or 3D scene under recording.

4. Simulation Experiments and Discussion

To verify the proposed scheme, two numerical simulations were conducted. The parameters used in the simulations were the wavelength $\lambda = 632.8$ nm; the order of circular harmonic key $m = 2$; the rotation angles and radii of the two circular harmonic keys: $\varphi_1 = 3^\circ$, $\varphi_2 = 6^\circ$ and $\rho_1 = 6.38$, $\rho_2 = 8.29$; and the distance between two adjacent planes is $d_1 = d_2 = 40$ mm from the DMD plane.

4.1. 2D Complex Object Encryption and Decryption Results. A binary 2D complex object field "E" of size 64×64 was used in the simulation. The intensity of the 2D object was taken as 0.5, and the corresponding phase was considered as e^{1j}. In order to visualize the quality of the phase in the reconstruction process, we have chosen constant phase value in the object function. The original complex object field is encrypted using (9) in the proposed system. The original intensity and the phase of the input complex object field are shown in Figures 4(a) and 4(b), respectively. The circular harmonic key of order $m = 2$ was used in the random phase mask as shown in Figure 4(c). The encrypted Fresnel field at the DMD plane was produced by using Fresnel transform equations (7)-(8). The measurement matrix Ψ was used in the simulation with random sequences of 0 and 1. The encrypted complex Fresnel field from the object path was interfered with the retarded reference wave to obtain the interference filed and then modulated with the measurement matrix. The simulated single-shot inline digital Fresnel hologram on DMD plane is shown in Figure 4(d).

At the receiver end, the compressed single-shot digital hologram is recovered with correct Ψ matrix by solving the unconstrained CS optimization equation as given in (20). The recovered digital holograms from 50% measurements after interpolation are shown in Figures 4(e) and 4(f). The complex Fresnel field was retrieved from the recovered digital holograms using (21)–(24) and inverted the DRPE process as specified in (10). When one of RPM_2 is incorrect, the decrypted intensity and phase distribution are shown in Figures 5(a) and 5(b), respectively. A small change in the decryption distance $d_1 = 41$ mm used in the reconstruction process results in noisy intensity and phase distribution as shown in Figures 5(c) and 5(d). Figures 5(e) and 5(f) show the intensity and phase of the incorrect measurement matrix which is replaced with the original matrix Ψ. The decrypted simulation results with correct keys are shown in Figures 6 and 7.

4.2. 3D Complex Object Encryption and Decryption Simulation Results. The encryption and decryption simulation procedure of the 3D complex object is explained in Section 2. To simulate the 3D complex object, we have considered two transparent objects, "D" and "H," made of binary images. The light propagates through the first object plane and obtains the features of the first complex object "D." Then, the obtained features of first object plane are propagated through a distance of $d_0 = 5$ mm using Fresnel propagation (Fresnel transform) and obtain another complex object features "H" in the second plane. Therefore, finally the 3D complex object information is obtained immediately after the second plane which contains depth information of the objects. The intensity and complex phase of the two objects are taken as 1.0 and e^{1j}, respectively. The simulation process of DRPE and compression of the interferograms are carried out as explained in Section 4.1. Finally, the 3D complex object scene at two different sections can be reconstructed back with single digital hologram using CS algorithm and then invert the two-step PPSDH process with original keys.

The decrypted results with incorrect keys are shown in Figure 8. The intensity and phase distribution of 3D complex object scene are decrypted at first plane with one of the incorrect RPM_2 keys. The decrypted intensity and phase distribution are shown in Figures 8(a) and 8(b). Figures 8(c) and 8(d) shows the intensity and phase distribution of incorrect distance key, $d_1 = 41$ mm, was used for decrypting the complex object at first plane. When an incorrect Ψ is replaced with measurement matrix, the intensity and phase distribution of 3D object scene decrypted at first plane are shown in Figures 8(e) and8(f).

4.3. Compressive Ratio Performance. Figure 6 shows the relationship between MSE and sample ratio of the decrypted intensity and phase images for different sample ratios. From Figure 6, it can be seen that when the compression ratio is less than 30% measurements than its intensity, phase reconstruction accuracy is feasible for both the simulations, as shown in Figures 7(a)–7(c) and Figures 9(a) and 9(b). Its corresponding phase images are shown in Figures 10(a)–10(c) and Figures 11(a) and 11(b). When the sample ratio is between 30% and 40% measurements, then the decrypted intensity and phase images' accuracy is acceptable, as shown in Figures 7(c), 10(c), 9(c) and 9(d), and 11(c) and 11(d), respectively.

When the sample ratio is greater than 40% measurements, then the intensity and phase reconstruction quality is

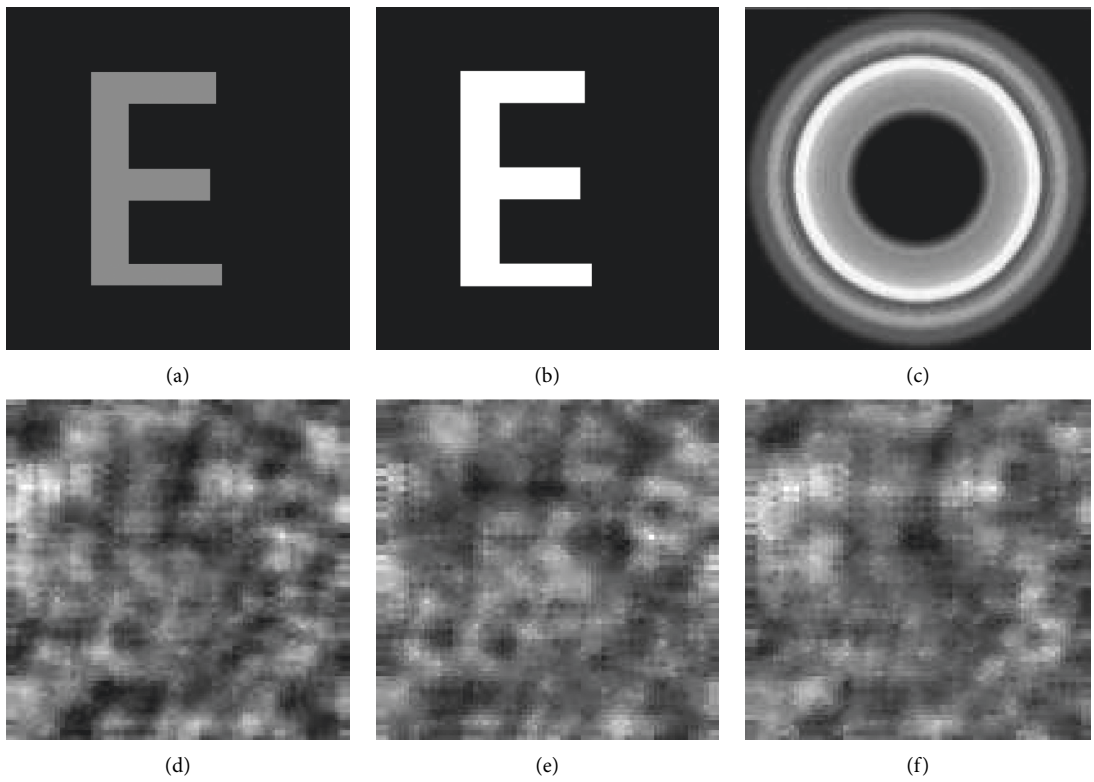


Figure 4: Simulation results based on the proposed encryption system: (a) intensity and (b) the corresponding phase of Figure 4(a), (c) one of the circular harmonic keys $P_m(\rho_1, \varphi_1)$ of order $m = 2$ and $\varphi_1 = 3^\circ$, (d) simulated two-step PPSDH on DMD plane, (e) recovered $\widetilde{H}_0$ digital hologram, and (f) recovered $\widetilde{H}_{-(\pi/2)}$ digital hologram after interpolation from $64 \times 64 \times 50\%$ measurements using CS framework.

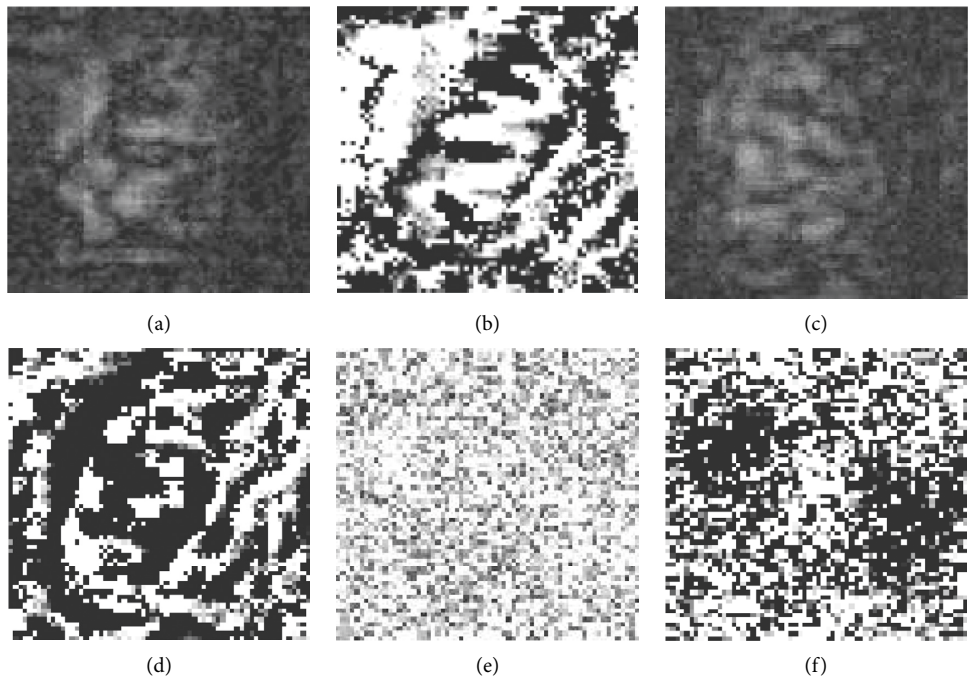


Figure 5: Decryption results using incorrect keys with $64 \times 64 \times 50\%$ measurements: (a) reconstructed intensity distribution when one of RPM_2 is wrong and (b) the corresponding phase, (c) reconstructed intensity distribution when one of the d_1 decryption distances is wrong and (d) the corresponding phase, and (e) reconstructed intensity distribution when the measurement matrix Ψ is incorrect and (f) the corresponding phase.

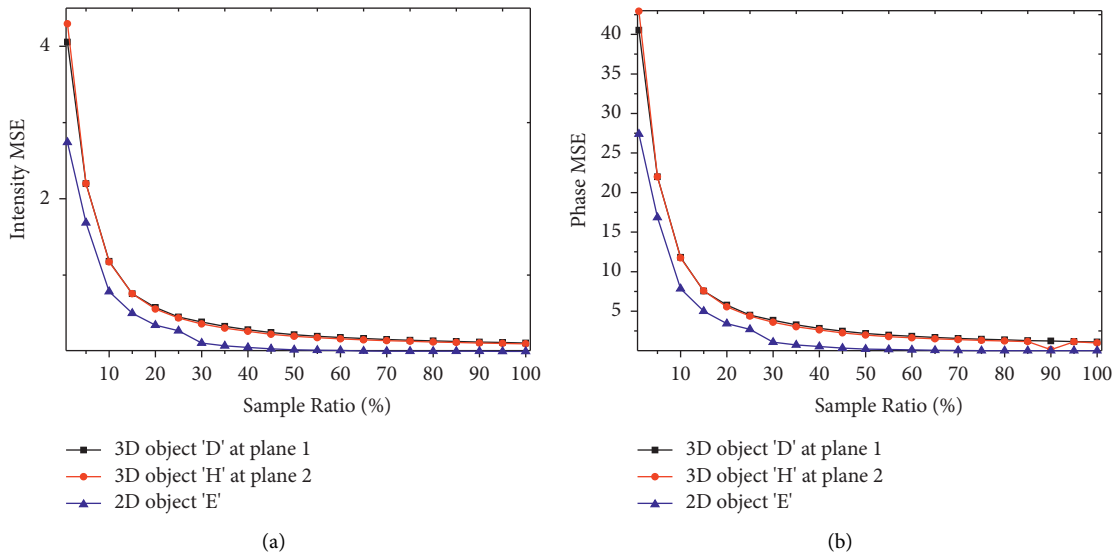


Figure 6: Performance of sample ratio versus MSE between decrypted and original complex wave: (a) MSE of intensity deviation; (b) MSE of phase deviation.

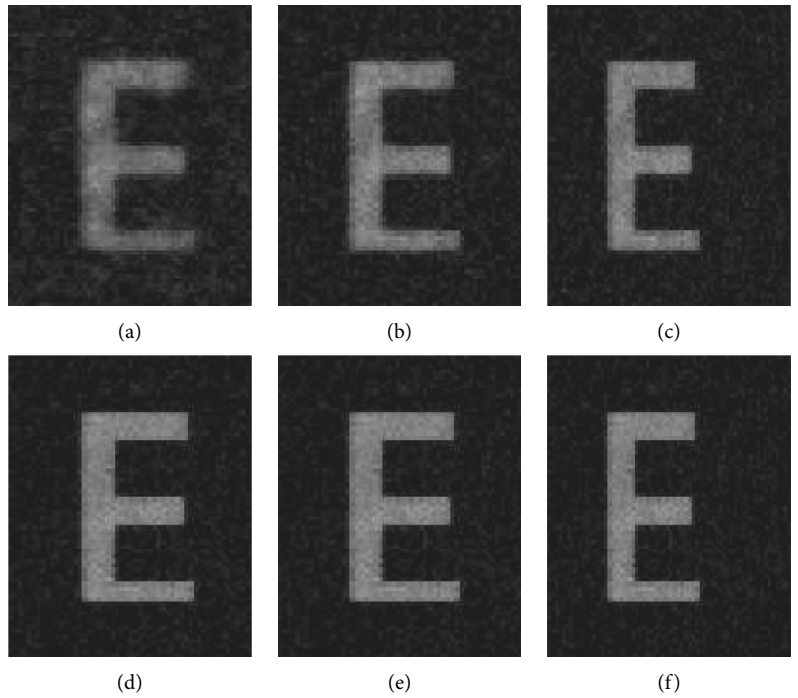
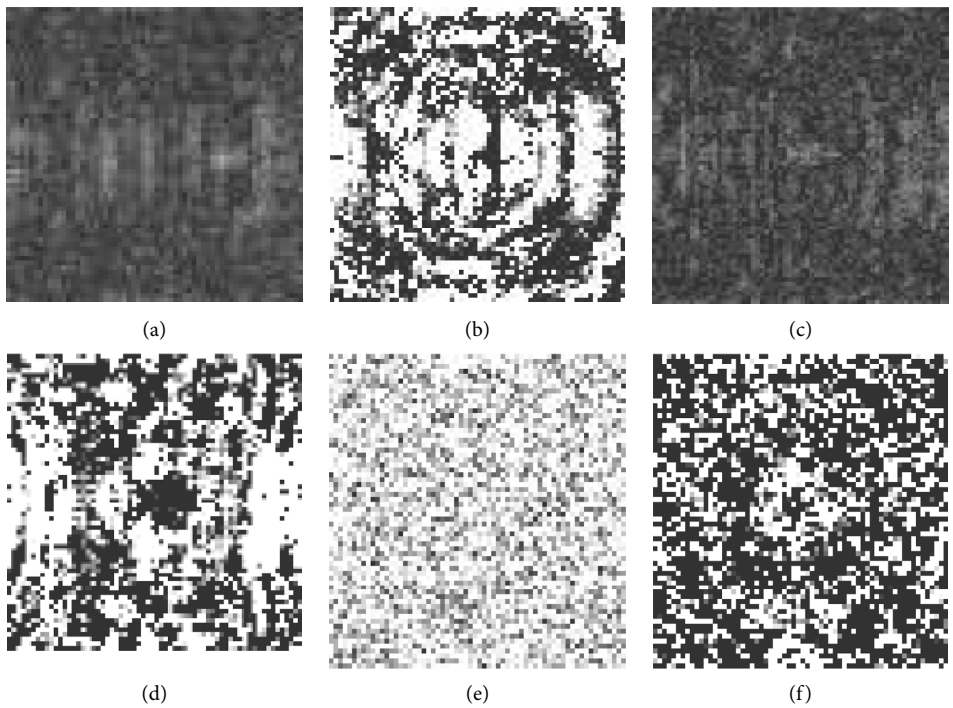


Figure 7: Intensity distribution of the decrypted 2D object using correct keys: (a) $64 \times 64 \times 5\%$ measurements; (b) $64 \times 64 \times 10\%$ measurements; (c) $64 \times 64 \times 15\%$ measurements; (d) $64 \times 64 \times 35\%$ measurements; (e) $64 \times 64 \times 45\%$ measurements; (f) $64 \times 64 \times 65\%$ measurements.

similar to the original image, as shown in Figures 7(e) and 7(f), 10(e) and 10(f), 9(e) and 9(f), and 11(e) and 11(f), respectively. Figures 7–11 show the decrypted intensity and phase distribution of both 2D and 3D object simulation cases from various sample ratios. If the correct keys such as wavelength, propagation distance, RPMs, and measurement matrix are used, then the decrypted intensity and phase images for both 2D and 3D simulation cases are shown in Figures 7–11. If the different wrong keys are used in the decryption process, the quality of the decrypted intensity and phase images are affected and fail to reconstruct the originalobject wavefield as shown in Figures 12–18.

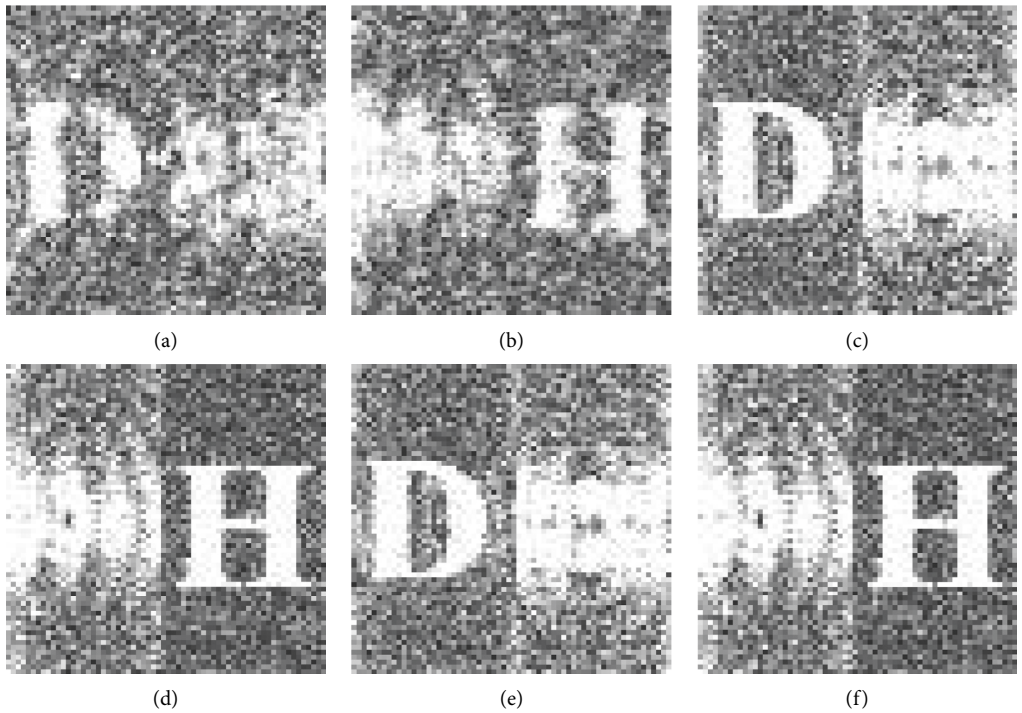
4.4. Key Space Security and Sensitivity Analysis. Figures 12–18 show the sensitivity of the keys with a small deviation δ when the correct keys fail to decrypt the original



(a) (b) (c)

(d) (e) (f)

Figure 8: Decrypted simulation results: (a) intensity information when one of the circular harmonic keys, RPM_2, is wrong and (b) the corresponding phase; (c) intensity information when one of the d_1 distances is wrong and (d) the corresponding phase; (e) intensity information when the measurement matrix Ψ is incorrect and (f) the corresponding phase.



(a) (b) (c)

(d) (e) (f)

Figure 9: Intensity of the decrypted 3D object scene using correct keys: (a) reconstructed at first plane with $64 \times 64 \times 8\%$ measurements; (b) reconstructed at second plane with $64 \times 64 \times 8\%$ measurements; (c) reconstructed at first plane with $64 \times 64 \times 25\%$ measurements; (d) reconstructed at second plane with $64 \times 64 \times 25\%$ measurements; (e) reconstructed at first plane with $64 \times 64 \times 65\%$ measurements; (f) reconstructed at second plane with $64 \times 64 \times 65\%$ measurements.

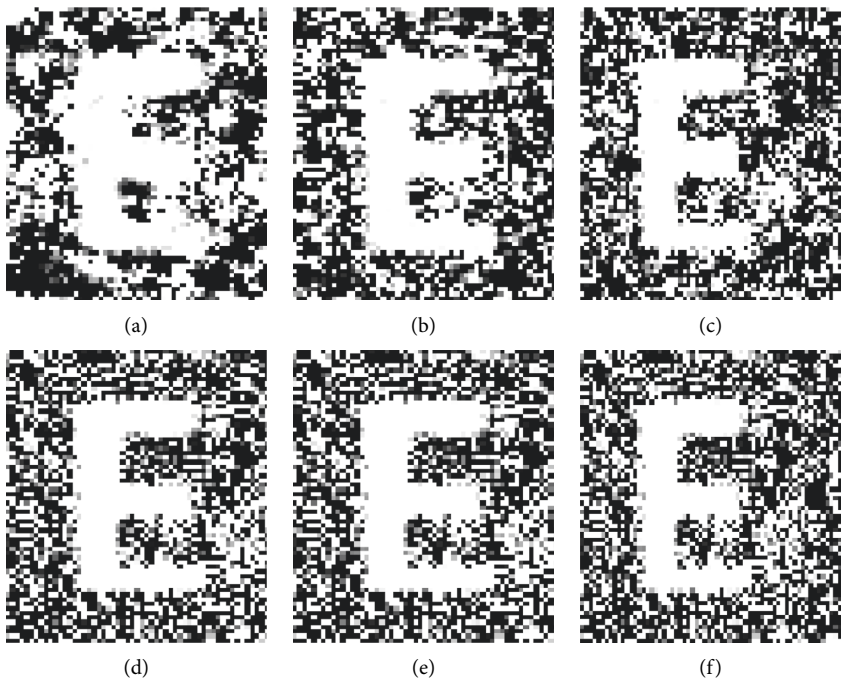


Figure 10: Phase distribution of the decrypted 2D object using correct keys: (a) $64 \times 64 \times 5\%$ measurements; (b) $64 \times 64 \times 10\%$ measurements; (c) $64 \times 64 \times 15\%$ measurements; (d) $64 \times 64 \times 35\%$ measurements; (e) $64 \times 64 \times 45\%$ measurements; (f) $64 \times 64 \times 65\%$ measurements.

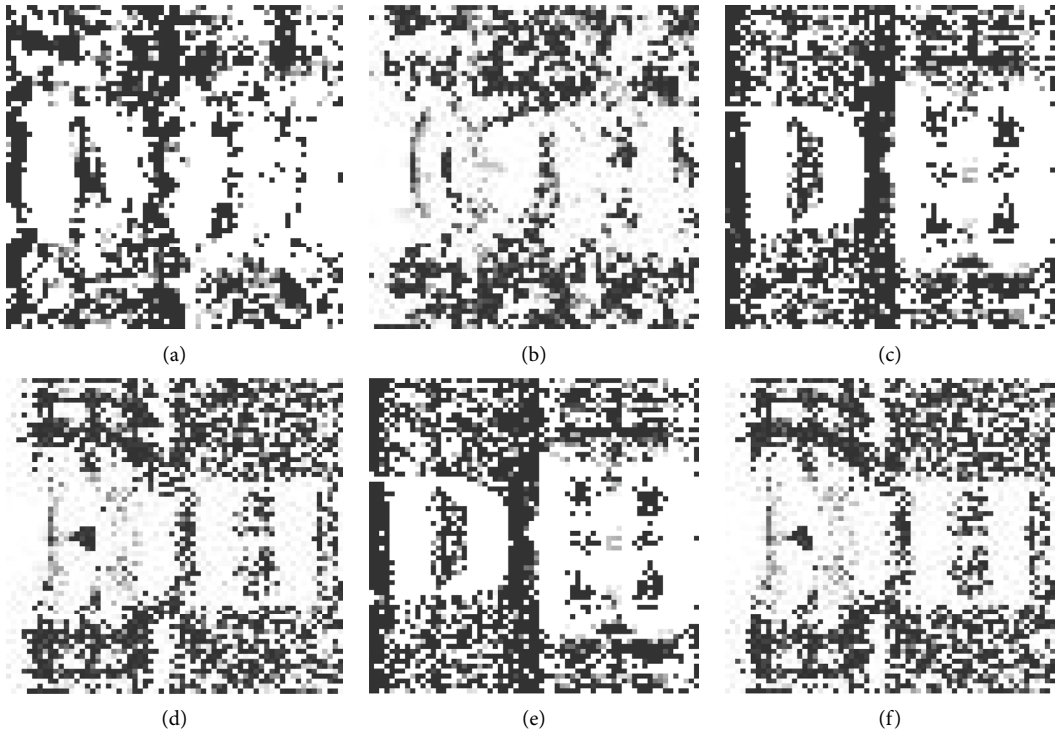


Figure 11: Phase distribution of the decrypted 3D object using correct keys: (a) reconstructed at first plane with $64 \times 64 \times 8\%$ measurements; (b) reconstructed at second plane with $64 \times 64 \times 8\%$ measurements; (c) reconstructed at first plane with $64 \times 64 \times 25\%$ measurements; (d) reconstructed at second plane with $64 \times 64 \times 25\%$ measurements; (e) reconstructed at first plane with $64 \times 64 \times 65\%$ measurements; (f) reconstructed at second plane with $64 \times 64 \times 65\%$ measurements.

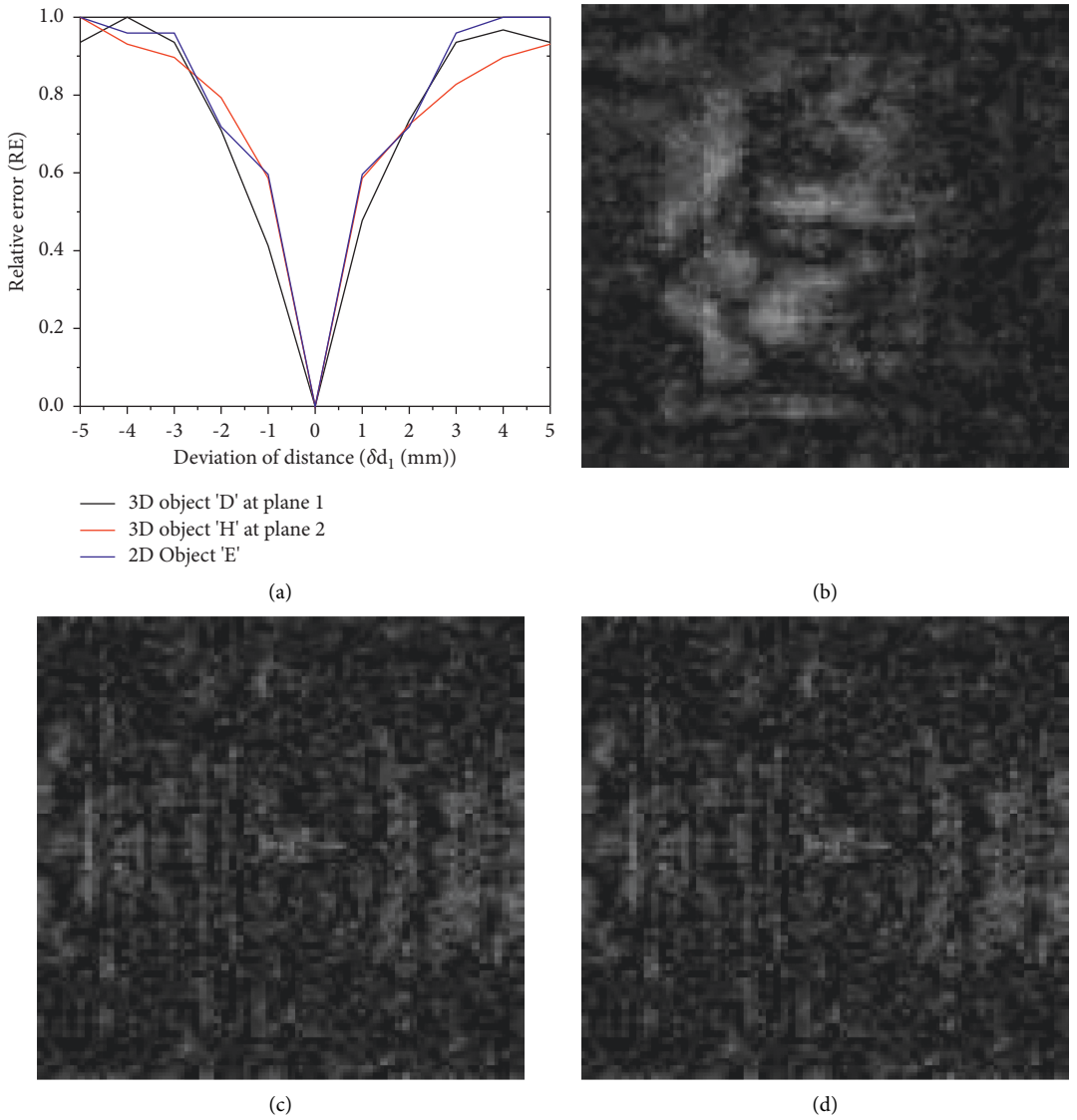


FIGURE 12: Decrypted results with incorrect d_1 distances: (a) the RE plot corresponding to the deviation of distance; (b) reconstructed 2D object with wrong distance d_1 = 41 mm; (c), (d) reconstructed 3D object wave with wrong distance d_1 = 41 mm at first plane and second plane, respectively.

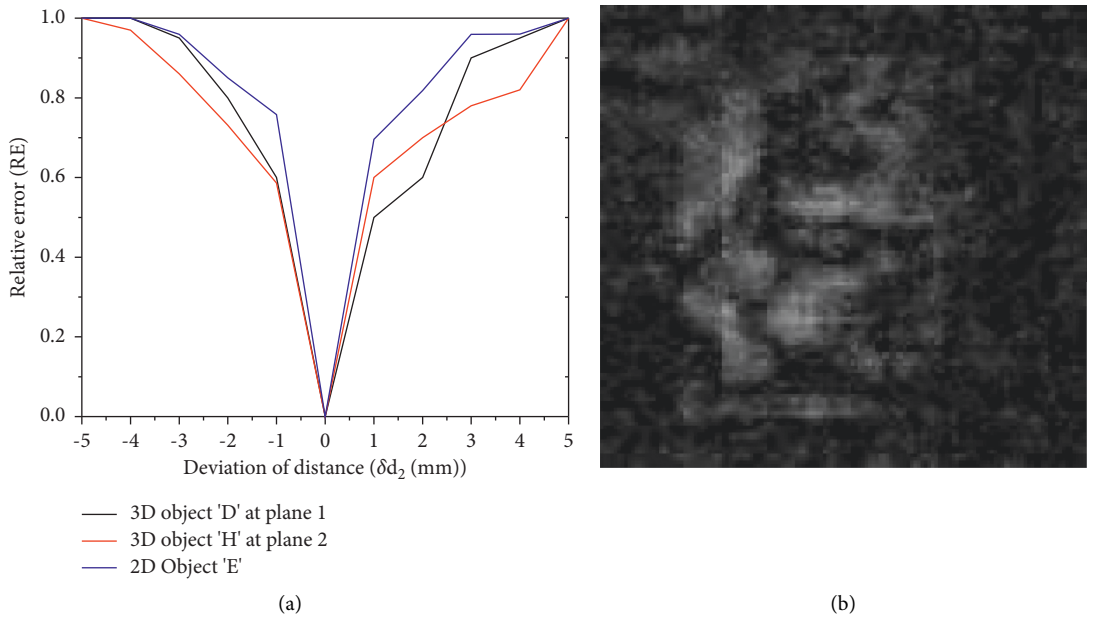
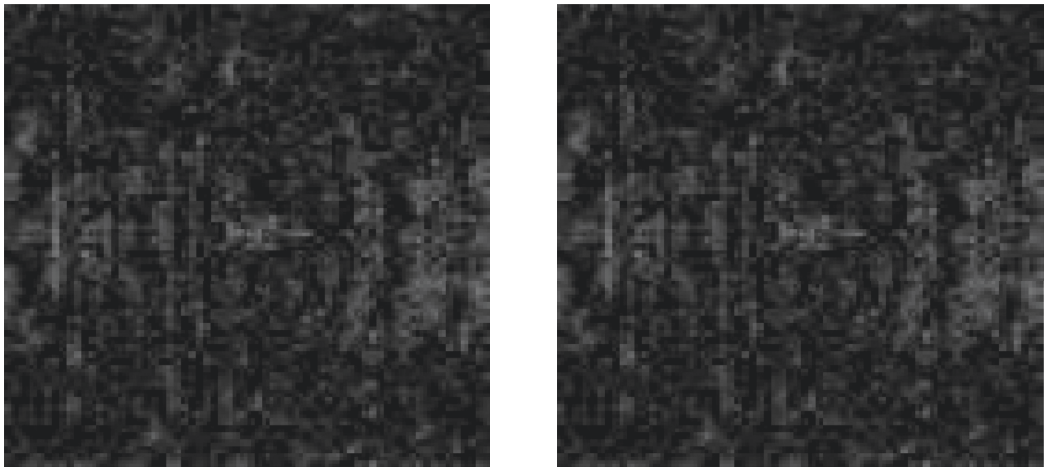
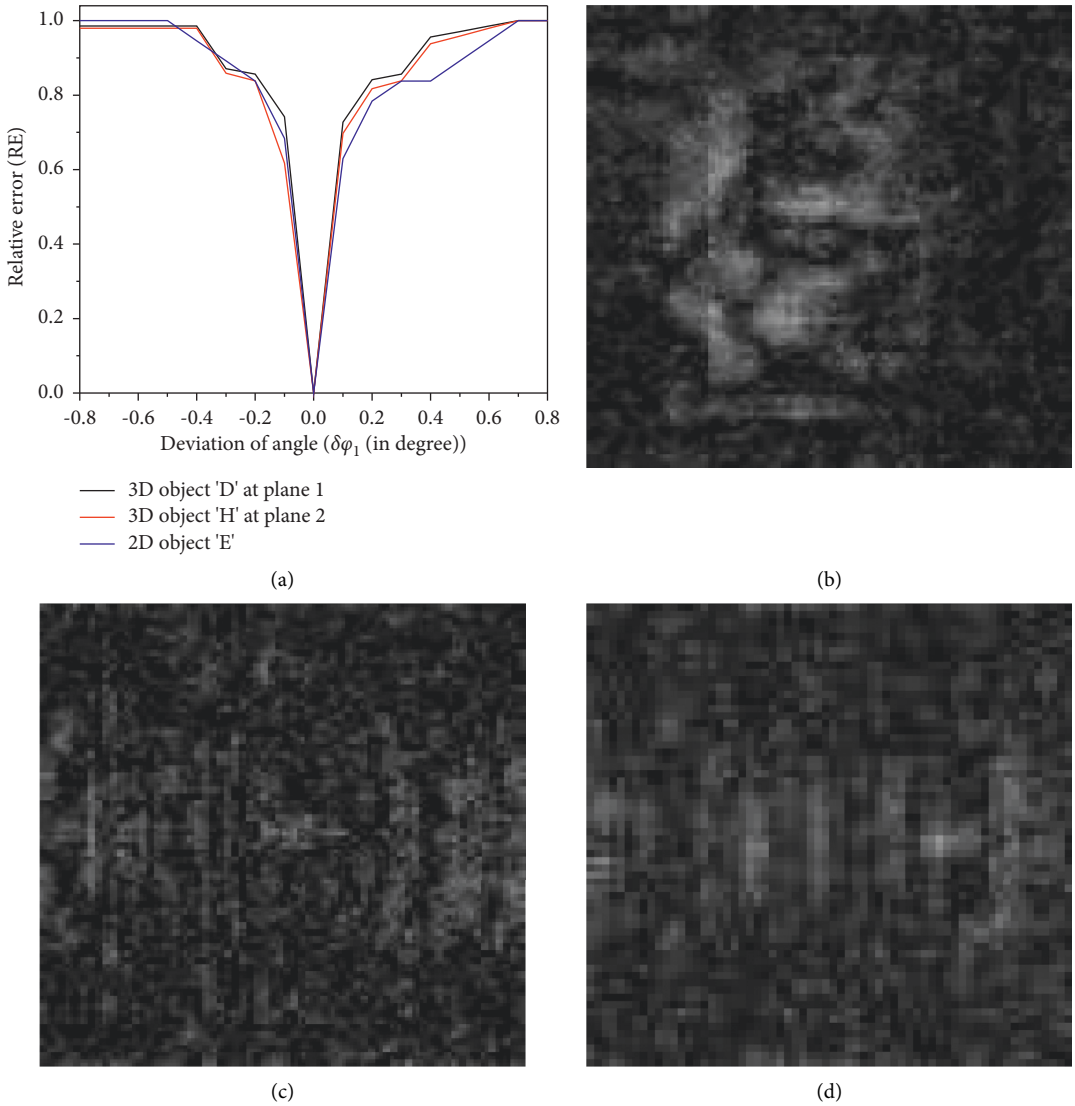


FIGURE 13: Continued.



(c) (d)

Figure 13: Decrypted results with incorrect d_2 distances: (a) the RE plot corresponding to the deviation of distance; (b) reconstructed 2D object with wrong distance $d_2 = 41$ mm; (c), (d) reconstructed 3D object wave with wrong distance $d_2 = 41$ mm at first plane and second plane, respectively.



(a) (b)

(c) (d)

Figure 14: Decrypted results with wrong angle of $p_m(\rho_1, \varphi_1)$: (a) the RE plot corresponding to the deviation of distance; (b) reconstructed 2D object with wrong angle $\varphi_1 = 3.1^\circ$; (c), (d) reconstructed 3D object with wrong angle $\varphi_1 = 3.1^\circ$ at first plane and second plane, respectively.

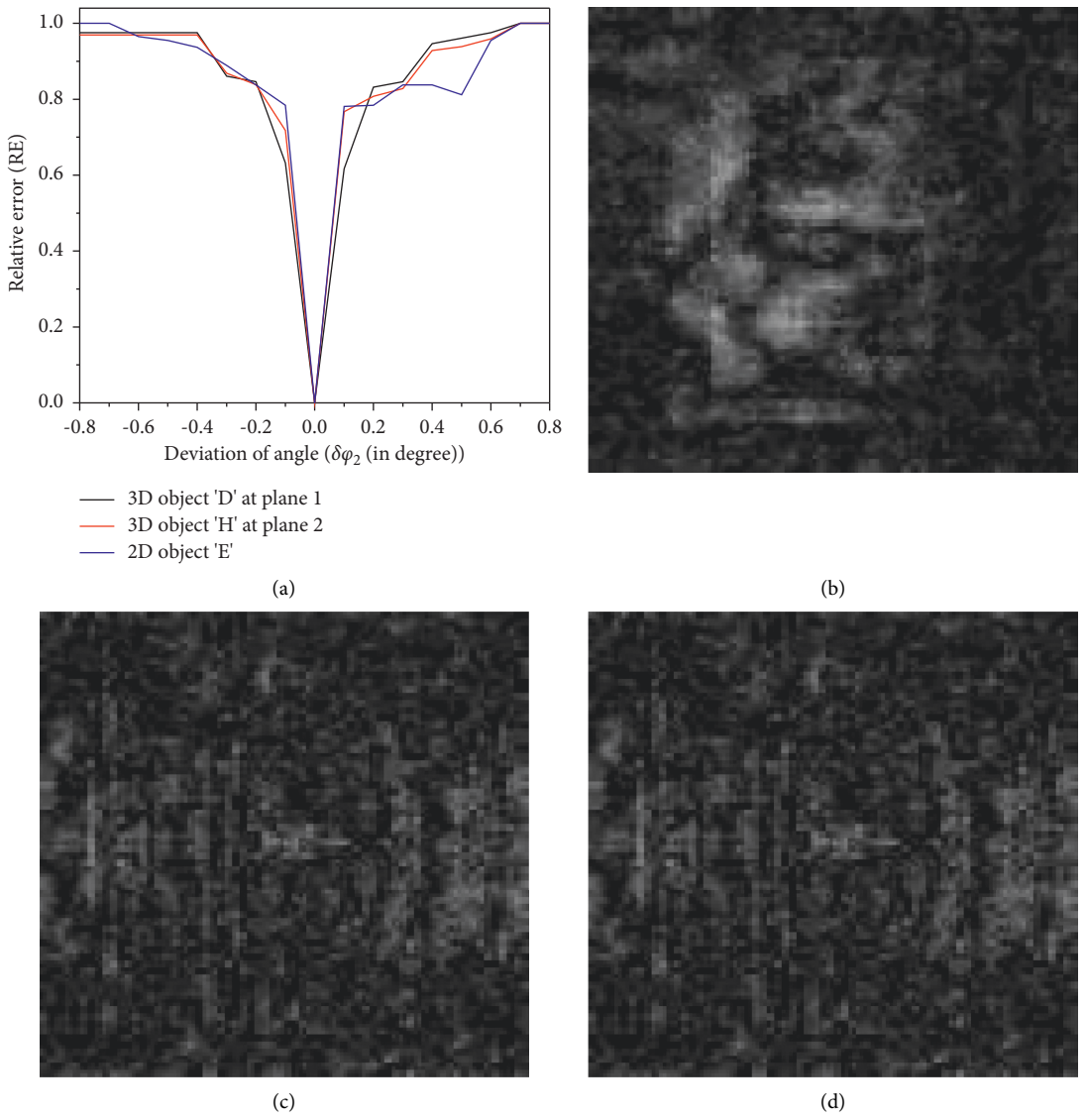


Figure 15: Decrypted results with wrong angle of $Q_m(\rho_2, \varphi_2)$: (a) the RE plot corresponding to the deviation of angle; (b) reconstructed 2D object with wrong angle $\varphi_2 = 6.1^\circ$; (c), (d) reconstructed 3D object with wrong angle $\varphi_2 = 6.1^\circ$ at first plane and second plane, respectively.

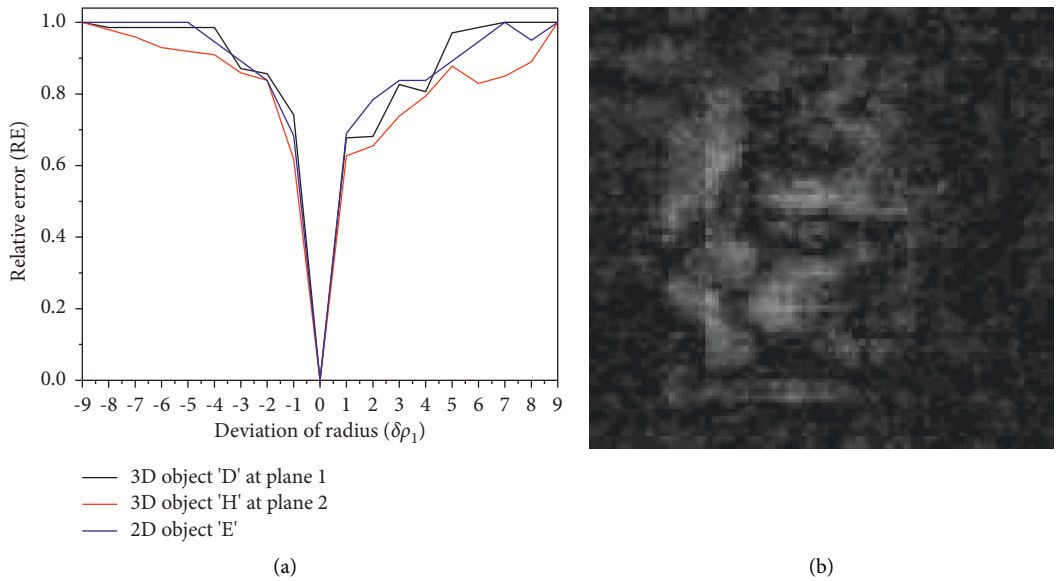
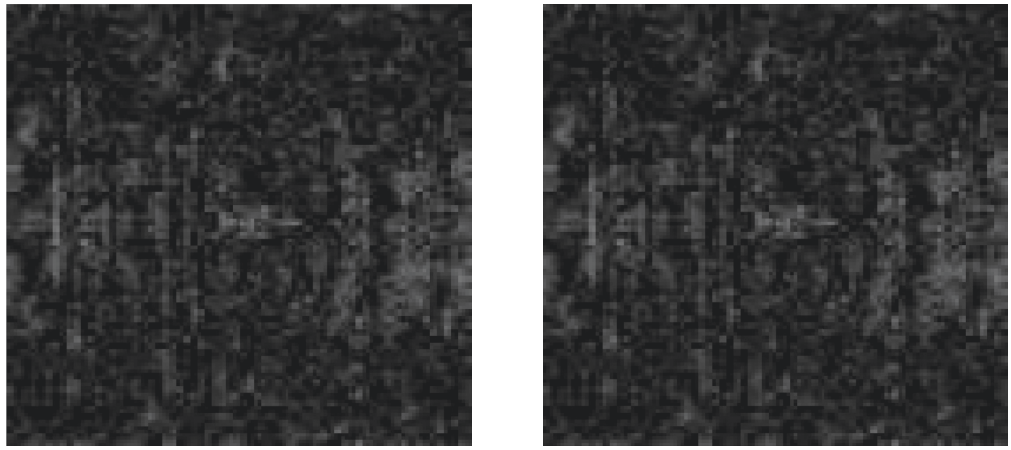
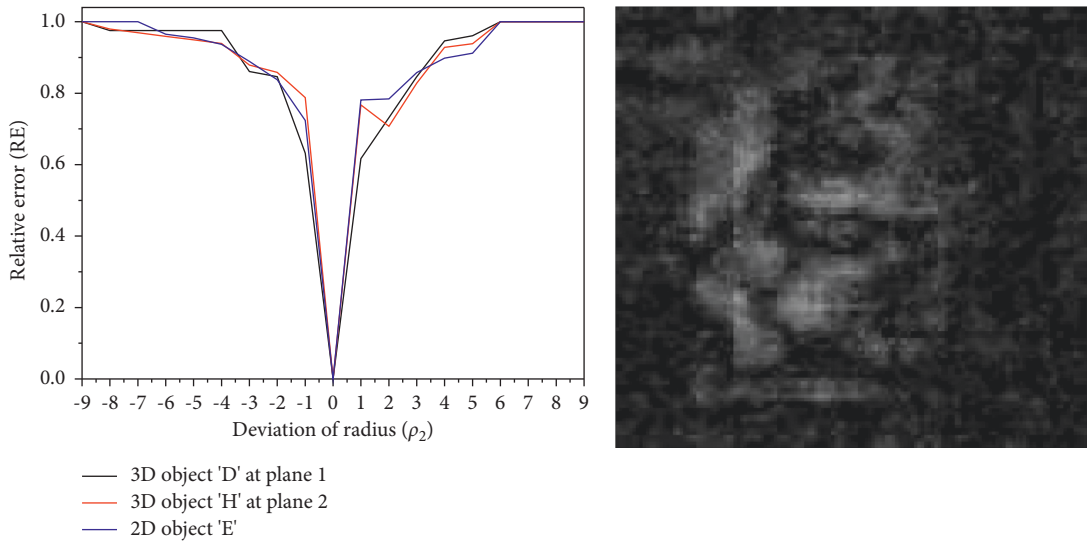


Figure 16: Continued.

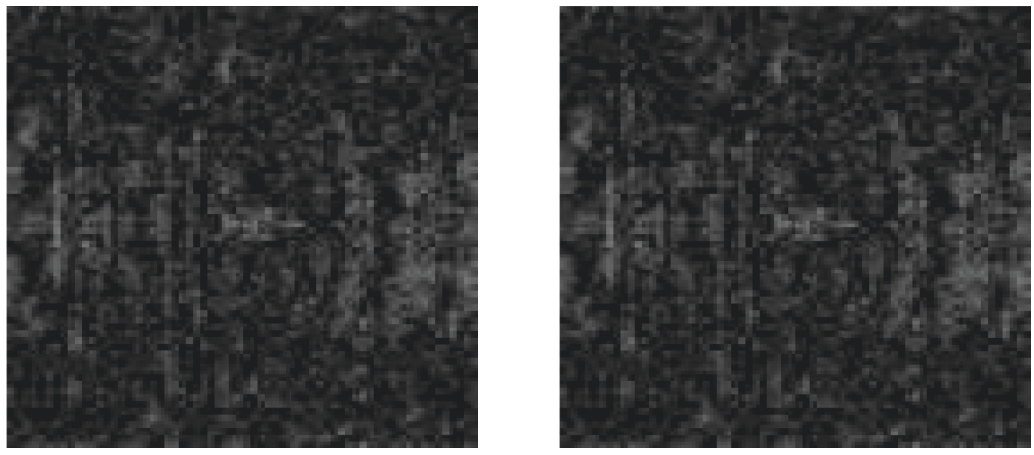


(c) (d)

Figure 16: Decrypted results with incorrect radius of $P_m(\rho_1, \varphi_1)$: (a) the RE plot corresponding to the deviation of radius; (b) reconstructed 2D object with incorrect radius $\rho_1 = 7.38$; (c), (d) reconstructed 3D object with incorrect radius $\rho_1 = 7.38$ at first plane and second plane, respectively.



(a) (b)



(c) (d)

Figure 17: Decrypted results with wrong radius of $Q_m(\rho_2, \varphi_2)$: (a) the RE plot corresponding to the deviation of radius; (b) reconstructed 2D object with incorrect radius $\rho_2 = 9.29$; (c), (d) reconstructed 3D object with incorrect radius $\rho_2 = 9.29$ at first plane and second plane, respectively.

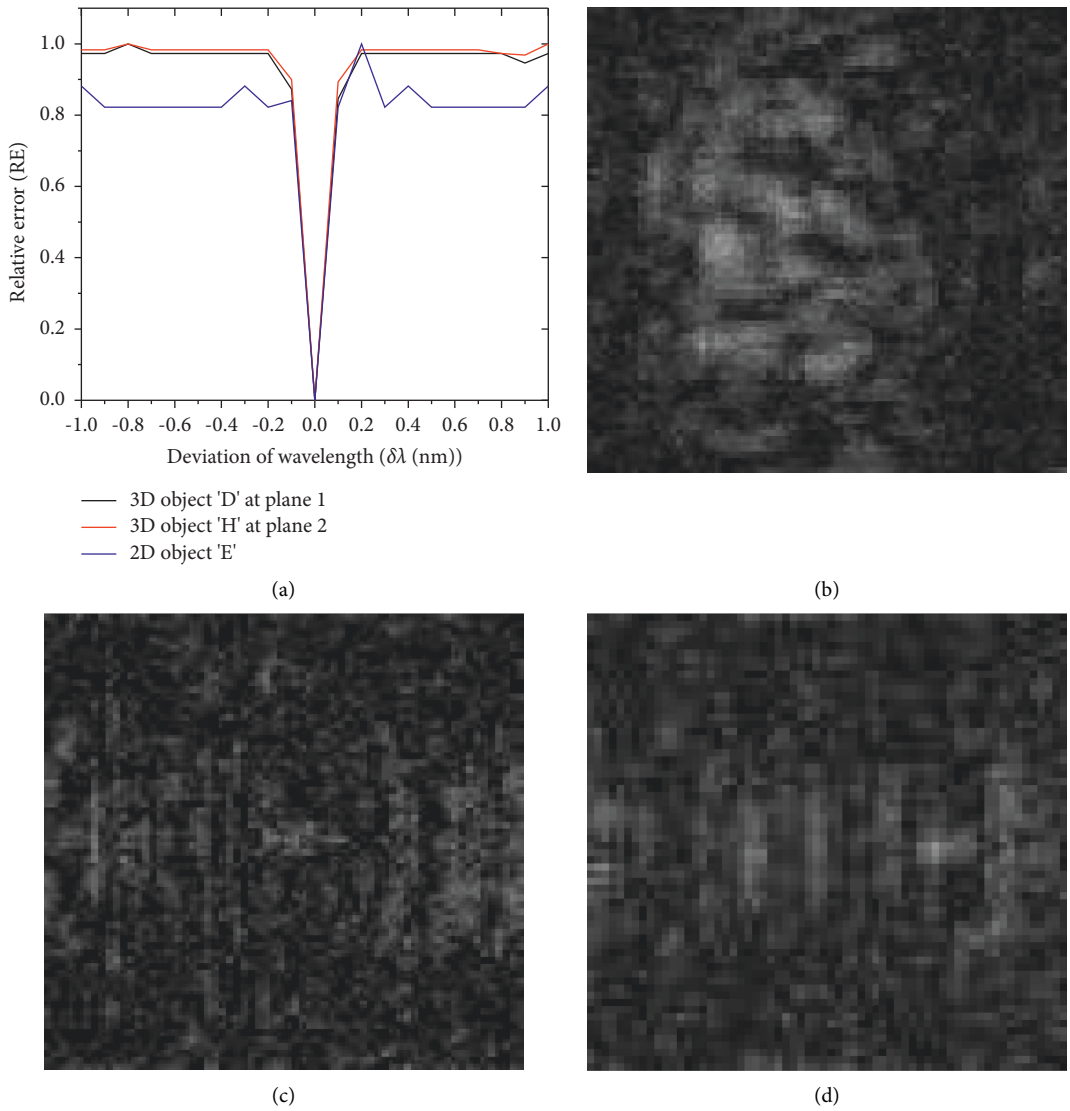


FIGURE 18: Decrypted results with wrong wavelength: (a) the RE plot corresponding to the deviation of wavelength; (b) reconstructed 2D object with wrong wavelength $\lambda = 632.81$ nm; (c), (d) reconstructed 3D complex object with wavelength $\lambda = 632.81$ nm at first plane and second plane, respectively.

complex object and completely looks like a noisy image. It can be seen that the RE plot value reaches minimum only when the decrypted keys are the same as the encrypted keys; otherwise, the RE value is maximum. The quality of the decrypted complex object is high when RE value is minimum; otherwise, it appears like a noisy image. Figures 12–18 show the RE plot of the decrypted complex object with deviation in the decrypted keys for both 2D and 3D simulation cases.

From Figures 12 and 13, it can be observed that the RE plot decreases to zero sharply only when the decrypted distance is the same as the simulation recording distance. Figures 12(b) and 13(b) show that the decrypted 2D complex object looks like a noisy image when a wrong distance key, $d_1 = d_2 = 41$ mm, is used. On the other hand, Figures 12(c), 12(d), 13(c), and 13(d) show the decrypted complex object of the 3D object with wrong distance key, $d_1 = d_2 = 41$ mm, at first plane and second plane, respectively.

It can be seen from Figures 14 and 15 that the RE plot value decreases to zero sharply with a small variation in the angle of $\pm 0.1^\circ$ for both simulation cases. When the wrong angle of the RPM_1 key $\varphi_1 = 3.1^\circ$ is used instead of the correct key value 3°, the decrypted results are shown in Figure 14. Similarly, when the wrong angle of another RPM_2 key $\varphi_2 = 6.1^\circ$ is used to decrypt the complex object for both the simulation cases, it fails to reconstruct original object wave as shown in Figure 15.

It can be seen from Figures 16 and 17 that the RE plot value decreases to zero sharply with a small variation in the radius of ± 1.0 for both 2D and 3D simulation cases. The decrypted results for the incorrect radius of the RPM_1 key when $\rho_1 = 7.38$ are shown in Figure 16. Similarly, the wrong radius of the other mask RPM_2 key, when $\rho_2 = 9.29$, was used for decryption, and it failed to reconstruct the original object wave, as shown in Figure 17.

The sensitivity of the recording wavelength was also studied. The wrong wavelength of $\lambda = 632.81$ nm was used, and its corresponding decrypted complex object result is shown in Figure 18. Here, it can be seen that the RE plot of the wavelength decreases to zero sharply with a small deviation of ±0.01 nm as shown in Figure 18(a). From the above results, it can be concluded that the proposed compressive digital Fresnel holographic encryption system is sensitive to the small variations in the decrypted keys such as measurement matrix, distance, wavelength, and rotation of the RPM using circular harmonic key. Therefore, the increase in the sensitivity of the keys results in the difficulty of duplicating the keys in the decryption process.

5. Conclusion

In this paper, an efficient 2D and 3D information security system is proposed using single-pixel compressive digital holography. The proposed system combines CS and digital holography for complex data encryption using minimal pixel detection. The hologram encryption process uses a DRPE scheme in the Fresnel domain using circular harmonic key, and this scheme enhances the security performance of the decryption process with the variation of the rotation key as presented in the simulation results. In addition, the measurement matrix and other digital holographic secret keys make the system more secure than the conventional method. The two-step PPSDH technique and CS based system are combined to improve the resolution of the reconstructed images. Due to the single-pixel imaging and PPSDH, the 3D information transmission and data storage are effectively reduced. The numerical simulation results show that the proposed cryptosystem has capability to decrypt the intensity and phase information of the object wave accurately from highly compressed digital Fresnel hologram. To quantify the reconstructed complex images, MSE and RE are analyzed for different compression ratios and different key attacks. A small deviation in the decrypted key leads to a considerable increase in the RE value and thus failure to reconstruct the original object information. It is verified from the results that the encryption system has high security and robustness and can be used in many information security applications.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by Science and Engineering Research Board (SERB), Department of Science and Technology, Government of India, under the sanction order no. CRG/2018/003906.

References

[1] U. Schnars and W. Jueptner, *Digital Holography*, Springer, Berlin, Germany, 2005.

[2] U. Schnars and W. Jüptner, "Direct recording of holograms by a CCD target and numerical reconstruction," *Applied Optics*, vol. 33, no. 2, pp. 179–181, 1994.

[3] P. Picart and J. Leval, "General theoretical formulation of image formation in digital Fresnel holography," *Journal of the Optical Society of America*, vol. 25, no. 7, pp. 1744–1761, 2008.

[4] J. W. Goodman, *Introduction to Fourier Optics*, Roberts and Company Publishers, Greenwood, CO, USA, 2005.

[5] A. Nelleri, J. Joseph, and K. Singh, "Recognition and classification of three-dimensional phase objects by digital Fresnel holography," *Applied Optics*, vol. 45, no. 17, pp. 4046–4053, 2006.

[6] A. Nelleri, U. Gopinathan, J. Joseph, and K. Singh, "Three-dimensional object recognition from digital Fresnel hologram by wavelet matched filtering," *Optics Communications*, vol. 259, no. 2, pp. 499–506, 2006.

[7] Y. Zhang, Y. Zhu, and E. Y. Lam, "Holographic 3D particle reconstruction using a one-stage network," *Applied Optics*, vol. 61, no. 5, pp. B111–B120, 2022.

[8] T. Tahara, Y. Kozawa, A. Matsuda, and R. Oi, "Quantitative phase imaging with single-path phase-shifting digital holography using a light-emitting diode," *OSA Continuum*, vol. 4, no. 11, pp. 2918–2927, 2021.

[9] N. Hai and J. Rosen, "Single-plane and multiplane quantitative phase imaging by self-reference on-axis holography with a phase-shifting method," *Optics Express*, vol. 29, no. 15, pp. 24210–24225, 2021.

[10] V. F. Rad, A. Babaei-Ghazvini, R. Jamali, I. Shahabi-Ghahfarrokhi, and A.-R. Moradi, "Digital holographic microscopy for real-time investigation of 3D microstructural dynamics of starch-kefiran-based nanocomposite," *Applied Optics*, vol. 60, no. 16, pp. 4706–4715, 2021.

[11] M. Panahi, R. Jamali, V. F. Rad, M. Khorasani, A. Darudi, and A. R. Moradi, "3D monitoring of the surface slippage effect on micro-particle sedimentation by digital holographic microscopy," *Scientific Reports*, vol. 11, no. 1, pp. 1–11, 2021.

[12] B. Javidi and D. Kim, "Three-dimensional-object recognition by use of single-exposure on-axis digital holography," *Optics Letters*, vol. 30, no. 3, pp. 236–238, 2005.

[13] B. Javidi, *Optical and Digital Techniques for Information Security*, Springer Science & Business Media, Berlin, Germany, 2005.

[14] A. Nelleri, J. Joseph, and K. Singh, "Lensless complex data encoding for digital holographic whole information security," *Optical Engineering*, vol. 47, no. 11, Article ID 115801, 2008.

[15] N. Yoshikawa and T. Miyake, "Omnidirectional 3D shape measurement using image outlines reconstructed from gabor digital holography," https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4075081.

[16] B. Lokesh Reddy, P. Ramachandran, and A. Nelleri, "Compressive complex wave retrieval from a single off-axis digital Fresnel hologram for quantitative phase imaging and microlens characterization," *Optics Communications*, vol. 478, Article ID 126371, 2021.

[17] L. R. Bodi, P. Ramachandran, and A. Nelleri, "Optimal Fresnelet sparsification for compressive complex wave

retrieval from an off-axis digital Fresnel hologram," *Optical Engineering*, vol. 60, no. 7, Article ID 073102, 2021.

[18] V. S. V. Allaparthi, A. Vishnoi, and G. Rajshekhar, "Phase derivative estimation in digital holographic interferometry using deep," *Applied Optics*, vol. 4, 2022.

[19] K. S. Vengala, N. Paluru, and R. K. S. Subrahmanyam Gorthi, "3D deformation measurement in digital holographic interferometry using a multitask deep learning architecture," *Journal of the Optical Society of America A*, vol. 39, no. 1, pp. 167–176, 2022.

[20] E. J. Candès, "Compressive sampling," in *Proceedings of the International Congress of Mathematicians*, Madrid, Spain, 2006, https://doi.org/10.4171/022-3/69.

[21] D. L. Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[22] E. Candès and J. Romberg, "Sparsity and incoherence in compressive sampling," *Inverse Problems*, vol. 23, no. 3, 2007.

[23] E. J. Candes and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Processing Magazine*, vol. 25, no. 2, 2008.

[24] L. I. Chengbo, W. Yin, and Z. Yin, "TV minimization by augmented Lagrangian and alternating direction algorithms," 2009, https://www.caam.rice.edu/%7Eoptimization/L1/TVAL3/v.beta/User_Guide_beta2.4.pdf.

[25] J. M. Bioucas-Dias and M. A. T. Figueiredo, "A new TWIST: two-step iterative shrinkage/thresholding algorithms for image restoration," *IEEE Transactions on Image Processing*, vol. 16, no. 12, pp. 2992–3004, 2007.

[26] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Optics Letters*, vol. 25, no. 12, pp. 887–889, 2000.

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

[28] D. S. Monaghan, G. Situ, U. Gopinathan, T. J. Naughton, and J. T. Sheridan, "Role of phase key in the double random phase encoding technique: an error analysis," *Applied Optics*, vol. 47, no. 21, pp. 3808–3816, 2008.

[29] A. Nelleri, J. Joseph, and K. Singh, "Error analysis for a lensless in-line digital holographic complex information security system based on double random phase encoding," *Optics and Lasers in Engineering*, vol. 47, 2009.

[30] S. K. Rajput and N. K. Nishchal, "Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform," *Applied Optics*, vol. 52, no. 4, pp. 871–878, 2013.

[31] G. Li, W. Yang, D. Li, and G. Situ, "Cyphertext-only attack on the double random-phase encryption: experimental demonstration," *Optics Express*, vol. 25, no. 8, pp. 8690–8697, 2017.

[32] J. Li, T. Zheng, Q.-Z Liu, and R. Li, "Double-image encryption on joint transform correlator using two-step-only quadrature phase-shifting digital holography," *Optics Communications*, vol. 285, no. 7, pp. 1704–1709, 2012.

[33] D. Kumar and N. K. Nishchal, "Digital holography based three-dimensional object recognition using binary differential joint transform correlator," in *Proceedings of the 12th International Conference on Fiber Optics and Photonics*, Washington, DC, USA, 2014.

[34] P. Clemente, V. Durán, E. Tajahuerce, V. Torres-Company, R. Martínez-Cuenca, and J. Lancis, *Digital Holography by Ghost Imaging*, Optica Publishing Group, Washington, DC, USA, 2011.

[35] A. Nelleri, "Digital Fresnel field encryption for three-dimensional information security," *Optical Engineering*, vol. 46, no. 4, Article ID 045801, 2007.

[36] S. K. Rajput and N. K. Nishchal, "Fresnel domain nonlinear optical image encryption scheme based on Gerchberg-Saxton phase-retrieval algorithm," *Applied Optics*, vol. 53, no. 3, pp. 418–425, 2014.

[37] B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Optics Letters*, vol. 28, no. 4, pp. 269–271, 2003.

[38] N. K. Nishchal, J. Joseph, and K. Singh, "Securing information using fractional Fourier transform in digital holography," *Optics Communications*, vol. 235, no. 4–6, pp. 253–259, 2004.

[39] N. K. Nishchal, J. Joseph, and K. Singh, "Fully phase-based encryption using fractional order Fourier domain random phase encoding: error analysis," *Optical Engineering*, vol. 43, no. 10, p. 2266, 2004.

[40] S. K. Rajput and N. K. Nishchal, "Image encryption based on interference that uses fractional Fourier domain asymmetric keys," *Applied Optics*, vol. 51, no. 10, pp. 1446–1452, 2012.

[41] M. F. Duarte, M. A. Davenport, D. Takhar et al., "Single-pixel imaging via compressive sampling," *IEEE Signal Processing Magazine*, vol. 25, no. 2, pp. 83–91, 2008.

[42] M. N. Kulakov, R. S. Starikov, and P. A. Cheremkhin, "Objects reconstruction by compressive sensing from single-pixel registrations using DMD," *KNE Energy*, vol. 3, no. 3, pp. 509–522, 2018.

[43] Y. Bromberg, O. Katz, and Y. Silberberg, "Ghost imaging with a single detector," *Physical Review*, vol. 79, no. 5, Article ID 053840, 2009.

[44] H. Di, K. Zheng, X. Zhang et al., "Multiple-image encryption by compressive holography," *Applied Optics*, vol. 51, no. 7, pp. 1000–1009, 2012.

[45] P. Clemente, V. Durán, E. Tajahuerce, P. Andrés, V. Climent, and J. Lancis, "Compressive holography with a single-pixel detector," *Optics Letters*, vol. 38, no. 14, pp. 2524–2527, 2013.

[46] J. Li, J. Sheng Li, Y. Yang Pan, and R. Li, "Compressive optical image encryption," *Scientific Reports*, vol. 5, no. 1, Article ID 10374, 2015.

[47] L. Jun, B. Jia, X. Dai et al., "Compressive optical image encryption using phase-shifting interferometry on a joint transform correlator," *Optica Applicata*, vol. 47, 2017.

[48] Z. Leihong, X. Rui, Z. Dawei, and C. Jian, "Optical encryption based on the algorithm of compressive ghost imaging and phase-shifting digital holography," *Ukrainian Journal of Physical Optics*, vol. 19, no. 3, pp. 179–190, 2018.

[49] Y. Wang, Q. Liu, J. Wang, and Q.-H. Wang, "Optical encryption of multiple three-dimensional objects based on multiple interferences and single-pixel digital holography," *Chinese Physics B*, vol. 27, no. 3, Article ID 034202, 2018.

[50] J. Du, Y. Xiong, C. Wu, and C. Quan, "Optical image encryption with high efficiency based on variable-distance ghost imaging," *Optik*, vol. 252, Article ID 168484, 2021.

[51] P. Zheng, Q. Dai, Z. Li et al., "Metasurface-based key for computational imaging encryption," *Science Advances*, vol. 7, no. 21, Article ID eabg0363, 2021.

[52] S. Jiao, J. Feng, Y. Gao, T. Lei, and X. Yuan, "Visual cryptography in single-pixel imaging," *Optics Express*, vol. 28, no. 5, pp. 7301–7313, 2020.

[53] C. Zhang, B. Han, W. He, X. Peng, and C. Xu, "A novel compressive optical encryption via single-pixel imaging," *IEEE Photonics Journal*, vol. 11, no. 4, pp. 1–8, 2019.

[54] Y. Awatsuji, M. Sasada, and T. Kubota, "Parallel quasi-phase-shifting digital holography," *Applied Physics Letters*, vol. 85, no. 6, pp. 1069–1071, 2004.

[55] Y. Awatsuji, T. Tahara, A. Kaneko et al., "Parallel two-step phase-shifting digital holography," *Applied Optics*, vol. 47, no. 19, pp. D183–D189, 2008.
[56] T. Tahara, K. Ito, T. Kakue et al., "Parallel phase-shifting digital holographic microscopy," *Biomedical Optics Express*, vol. 1, no. 2, pp. 610–616, 2010.
[57] J. E. Rueda-Parada and J. Enrique, "Encryption using circular harmonic key," *Dyna*, vol. 82, no. 190, pp. 70–73, 2015.
[58] Q. Wang, Q. Guo, L. Lei, and J. Zhou, "Optical interference-based image encryption using circular harmonic expansion and spherical illumination in gyrator transform domain," *Optics Communications*, vol. 346, pp. 124–132, 2015.
[59] B. Lokesh Reddy and A. Nelleri, "Complex object wave retrieval using single-pixel compressive imaging of an off-axis Fresnel hologram," *Journal of Modern Optics*, vol. 69, no. 10, pp. 541–553, 2022.
[60] P. Ramachandran, Z. C. Alex, and A. Nelleri, "Phase reconstruction using compressive two-step parallel phase-shifting digital holography," *Optical Engineering*, vol. 57, no. 4, Article ID 043105, 2018.