

Optical image watermarking based on orbital angular momentum holography

Jialong Zhu(朱家龙), Jiaying Ji(季佳滢), Le Wang(王乐), and Shengmei Zhao(赵生妹)

Citation: Chin. Phys. B, 2024, 33 (**12**): 124202. DOI: 10.1088/1674-1056/ad8cbd
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Interface state-based bound states in continuum and below-continuum-resonance modes with high-*Q* factors in the rotational periodic system

Jialing Yang(杨嘉玲), Aoqian Shi(史奥芊), Yuchen Peng(彭宇宸), Peng Peng(彭鹏), and Jianjun Liu(刘建军)
Chin. Phys. B, 2024, 33 (**8**): 084206. DOI: 10.1088/1674-1056/ad4630

Optimization of extreme ultraviolet vortex beam based on high harmonic generation

Bo Xiao(肖礴), Yi-Wen Zhao(赵逸文), Fang-Jing Cheng(程方晶), Ge-Wen Wang(王革文), Wei Jiang(姜威), Yi-Chen Wang(王一琛), Jie Hu(胡杰), Hong-Jing Liang(梁红静), and Ri Ma(马日)
Chin. Phys. B, 2024, 33 (**5**): 054209. DOI: 10.1088/1674-1056/ad2bf0

Effectively modulating spatial vortex four-wave mixing in a diamond atomic system

Nuo Ba(巴诺), Ming-Qi Jiang(姜明奇), Jin-You Fei(费金友), Dan Wang(王丹), Hai-Lin Jiang(蒋海林), Lei Wang(王磊), and Hai-Hua Wang(王海华)
Chin. Phys. B, 2024, 33 (**4**): 044202. DOI: 10.1088/1674-1056/ad0771

Generation of orbital angular momentum hologram using a modified U-net

Zhi-Gang Zheng(郑志刚), Fei-Fei Han(韩菲菲), Le Wang(王乐), and Sheng-Mei Zhao(赵生妹)
Chin. Phys. B, 2024, 33 (**3**): 034207. DOI: 10.1088/1674-1056/ad12aa

Properties of focused Laguerre-Gaussian beam propagating in anisotropic ocean turbulence

Xinguang Wang(王新光), Yangbin Ma(马洋斌), Qiujie Yuan(袁邱杰), Wei Chen(陈伟), Le Wang(王乐), and Shengmei Zhao(赵生妹)
Chin. Phys. B, 2024, 33 (**2**): 024208. DOI: 10.1088/1674-1056/ad053c

---

Optical image watermarking based on orbital angular momentum holography

Jialong Zhu(朱家龙)[1,2,†], Jiaying Ji(季佳滢)[1], Le Wang(王乐)[1], and Shengmei Zhao(赵生妹)[1,3,‡]

[1] *Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*
[2] *School of Information Engineering, Suqian University, Suqian* 223800, *China*
[3] *National Laboratory of Solid State Microstructures, Nanjing University, Nanjing* 210093, *China*

(Received 31 August 2024; revised manuscript received 21 October 2024; accepted manuscript online 30 October 2024)

We propose an optical image watermarking scheme based on orbital angular momentum (OAM) holography. Multiple topological charges (TCs, l) of OAM, as multiple cryptographic sub-keys, are embedded into the host image along with the watermark information. Moreover, the Arnold transformation is employed to further enhance the security and the scrambling time (m) is also served as another cryptographic key. The watermark image is embedded into the host image by using the discrete wavelet transformation (DWT) and singular value decomposition (SVD) methods. Importantly, the interference image is utilized to further enhance security. The imperceptibility of our proposed method is analyzed by using the peak signal-to-noise ratio (PSNR) and the histogram of the watermarked host image. To demonstrate robustness, a series of attack tests, including Gaussian noise, Poisson noise, salt-and-pepper noise, JPEG compression, Gaussian low-pass filtering, cropping, and rotation, are conducted. The experimental results show that our proposed method has advanced security, imperceptibility, and robustness, making it a promising option for optical image watermarking applications.

Keywords: optical image watermarking, orbital angular momentum, holography, discrete wavelet transformation

PACS: 42.40.Jv, 42.30.–d

DOI: 10.1088/1674-1056/ad8cbd

1. Introduction

With the development of digital images, videos, and multimedia assets, the vulnerability of digital content to unauthorized copying, distribution, tampering, and piracy has increased significantly. The security and privacy of these digital information can be enhanced by integrating chaotic systems,[1–3] machine learning,[4] complex algorithms,[5–9] and optical encryption technologies.[10–12] In recent years, optical encryption technology has been developed rapidly in response to the growing prevalence of these digital information security issues. Among these optical encryption techniques, optical image watermarking techniques have gained increasing attention due to two significant potential advantages.[13] Firstly, optical systems can facilitate high-speed parallel optical information processing to handle large volumes of data.[14] Secondly, optical watermarking can be directly applied to physical objects, whether two-dimensional (2D) case[15] or three-dimensional (3D) case.[16]

Holographic watermarking is a highly regarded technique in the field of optical image watermarking.[10–12] This technique leverages the principles of holography, a method for capturing and reconstructing the watermarking information from light interference patterns. These watermarks are often challenging to detect or remove without the appropriate decryption keys and provide a high level of security and robustness against various attacks. The advantage of holographic watermarking lies in its ability to combine security and imperceptibility effectively.

Some physical dimensions within an optical system, including wavelength, amplitude, phase, distance, and polarization, can be utilized as the cryptographic keys to enhance the security of holographic watermarking. For example, Chen *et al*. proposed the utilization of pure phase-only masks and wavelength as cryptographic keys to ensure robust information security.[17] Jiao *et al*. suggested that complex amplitudes can be employed as cryptographic keys to conceal data.[18] Chen *et al*. also proposed the use of a double random-phase for hiding information.[19] Sui *et al*. implemented a watermarking scheme based on computational ghost imaging that uses both the wavelength and the propagation distance as the key.[20] Guo *et al*. introduced the idea of arbitrary polarization encoding in full-color holography to enhance security and capability.[21]

Orbital angular momentum (OAM), described by the expression $\exp(\mathrm{i}l\theta)$ with θ representing the azimuthal angle and l denoting the topological charge (TC), is regarded as an independent physical dimension utilized in holography, including optical multiplexed displays,[22,23] optical storage,[24,25] optical communication,[26,27] optical sensors,[28,29] and so on. However, the utilization of OAM's TC as the cryptographic key to enhance the security of holographic watermarking, especially multiple keys simultaneously embedded in one host

[†]Corresponding author. E-mail: zjl@squ.edu.cn
[‡]Corresponding author. E-mail: zhaosm@njupt.edu.cn

© 2024 Chinese Physical Society and IOP Publishing Ltd

image, has been far less discussed and reported.

In this paper, we propose an optical image watermarking method based on orbital angular momentum holography. The watermark image is converted into a watermark hologram and then combined with an OAM hologram to create an OAM-watermark hologram. Here, multiple TCs and scrambling times are served as the cryptographic keys at the same time. To further enhance security, an Arnold transformation algorithm is performed on the OAM-watermark hologram, resulting in the creation of a cryptographic OAM hologram. Here, multiple TCs and scrambling times are served as the cryptographic keys simultaneously to improve security. The cryptographic OAM hologram is embedded into the host image using the discrete wavelet transformation (DWT) and singular value decomposition (SVD) methods. In the watermark recovery process, the cryptographic OAM hologram is extracted from the watermarked host image using the same DWT and SVD methods. The cryptographic OAM hologram is restored to the OAM-watermark hologram by the anti-Arnold transformation method. The watermark image can be reconstructed by illuminating the OAM-watermark hologram with the inverse OAM beam.

2. Principle and method

The principle of optical image watermarking based on OAM holography is illustrated in Fig. 1, which comprises four main components: the watermark preprocessing process, depicted as in Fig. 1(a); the watermark embedding system, shown in Fig. 1(b); the OAM-watermark hologram recovery system, illustrated in Fig. 1(c); and the optical reconstruction method, presented in Fig. 1(d). The watermark preprocessing process and the watermark embedding system are completed by the encryption side, while the OAM-watermark hologram recovery system and the optical reconstruction method are completed by the decryption side.

2.1. Watermark preprocessing

In the watermark preprocessing process (Fig. 1(a)), the original watermark $w(x,y)$ (for example, "NUPT") is first sampled into K point watermarks $s_i(x,y)$ $(i=1,\ldots,K)$ by multiple sub-sampling arrays, which can be described as

$$\begin{aligned} s_1(x,y) &= w(x,y)\times \mathrm{Comb}_1(x,y),\\ s_2(x,y) &= w(x,y)\times \mathrm{Comb}_2(x,y),\\ &\vdots = \vdots,\\ s_K(x,y) &= w(x,y)\times \mathrm{Comb}_K(x,y), \end{aligned} \tag{1}$$

where (x,y) and $\mathrm{Comb}(x,y)$ represent the Cartesian coordinates and a Dirac periodic array, respectively. K point watermarks are converted into K watermark holograms $(W_i(u,v)$, for $i=1,\ldots,K)$, by employing either the computer-generated hologram (CGH) method[30] or the neural network-based method,[31] which can be expressed as

$$\begin{aligned} W_1(u,v) &= \sum_{x=1}^{M}\sum_{y=1}^{M} s_1(x,y)\exp[-\mathrm{i}2\pi(xu+yv)],\\ W_2(u,v) &= \sum_{x=1}^{M}\sum_{y=1}^{M} s_2(x,y)\exp[-\mathrm{i}2\pi(xu+yv)],\\ &\vdots = \vdots,\\ W_K(u,v) &= \sum_{x=1}^{M}\sum_{y=1}^{M} s_K(x,y)\exp[-\mathrm{i}2\pi(xu+yv)], \end{aligned} \tag{2}$$

where (u,v) and $M\times M$ are the spatial frequencies of (x,y) and the size of the watermark hologram, respectively. Then, the K sub-OAM watermark holograms are created by superposing K sub-watermark holograms $(W_k(u,v))$ with distinct OAM TC values. For instance, for $K=4$ in the example, $l_1=2$, $l_2=4$, $l_3=6$, and $l_4=8$ are applied for the four sub-watermarks 'N', 'U', 'P', and 'T'. Finally, all sub-OAM watermark holograms are multiplexed to generate a single OAM watermark hologram, which can be given by

$$I_{\mathrm{O}}(u,v)=\sum_{k=1}^{K=4} W_k(u,v)\exp(\mathrm{i}l_k\theta), \tag{3}$$

where all l_k can be served as the cryptographic key, Key_1, which is composed by $l_1,\ldots,l_K$.

2.2. Watermark embedding system

In the watermark embedding system (Fig. 1(b)), the OAM-watermark hologram is firstly scrambled by using Arnold transformation,[32] where the transformation matrix (A) can be given as

$$A=\begin{bmatrix}1 & d\\ c & cd+1\end{bmatrix}. \tag{4}$$

Here, c and d can be freely specified. The information at each pixel in the OAM-watermark hologram $(I_{\mathrm{O}}(u_0,v_0))$ is scrambled m times to obtain the cryptographic OAM hologram $(I_{\mathrm{W}}(u_m,v_m))$, which can be represented as

$$\begin{bmatrix}u_m\\ v_m\end{bmatrix}=A^m\begin{bmatrix}u_0\\ v_0\end{bmatrix}\bmod(M), \tag{5}$$

where m is the scrambling times in the Arnold transformation. It depends on the size $(M\times M)$ of the hologram and can serve as another cryptographic key (Key_2). (u_0,v_0) represents the pixel coordinates on the OAM-watermark hologram $(I_{\mathrm{O}}(u_0,v_0))$. (u_m,v_m) represents the pixel coordinates on the cryptographic OAM hologram $(I_{\mathrm{W}}(u_m,v_m))$. $\mathrm{mod}(\cdot)$ represents the modulo operation.

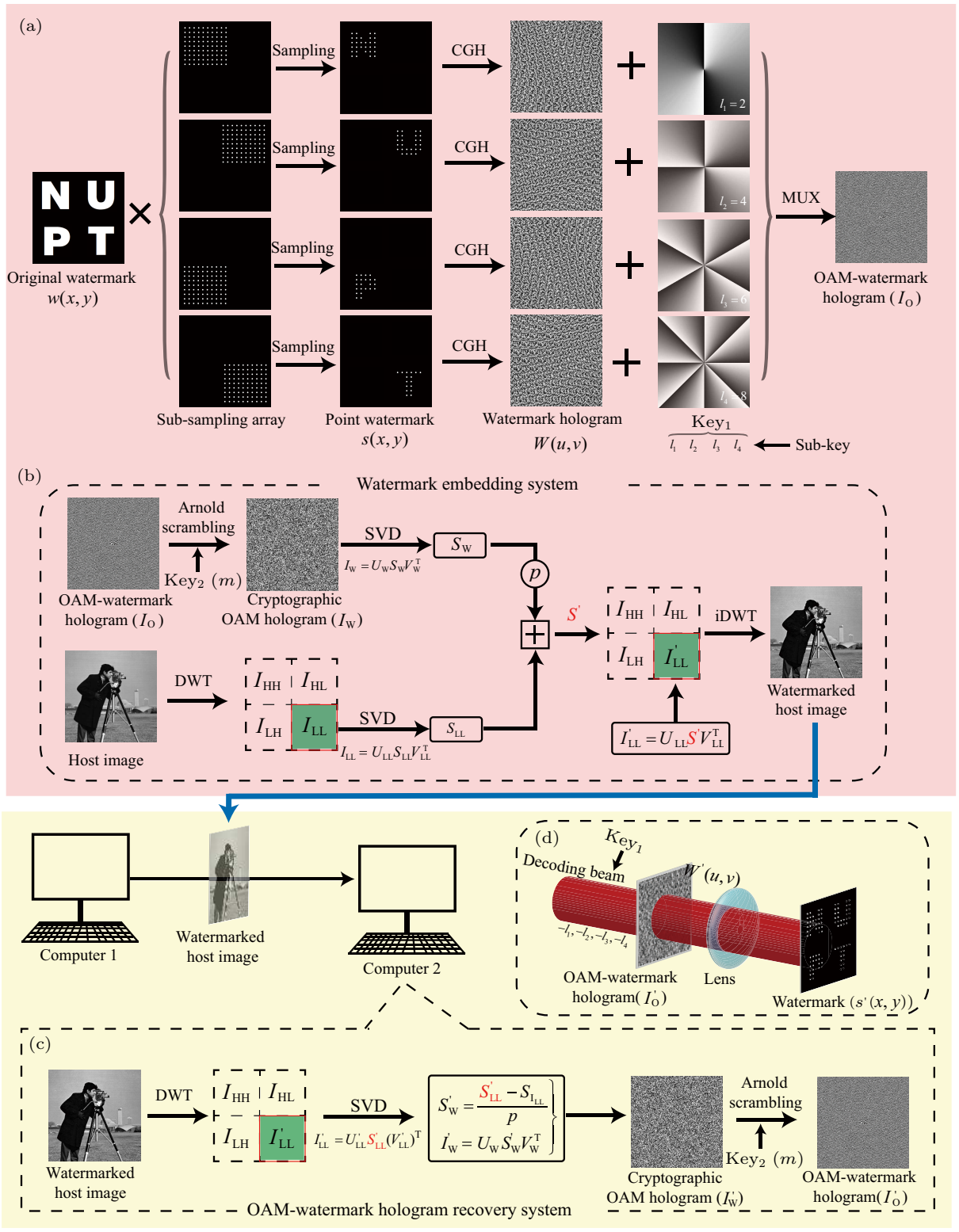


Fig. 1. The schematic configuration of optical image watermarking based on OAM holography. (a) The watermark preprocessing process. (b) The watermark embedding system. (c) OAM-watermark hologram recovery system. (d) The optical reconstruction method.

On the other hand, the host image ("cameraman") is decomposed into four non-overlapping subbands by discrete wavelet transform (DWT): the low-frequency component (I_{LL}), the horizontal component (I_{LH}), the vertical component (I_{HL}), and the diagonal component (I_{HH}). In the proposed watermarking scheme, the cryptographic OAM hologram is embedded within the low-frequency component (I_{LL}) of the host image. This component is selected because it encompasses the primary intensity content, ensuring that the watermark is less susceptible to image manipulations like compression and noise. Embedding in this component also helps maintain the watermark's visibility and integrity.[5] For enhancing the robustness of the watermark, the low-frequency component (I_{LL}) and the cryptographic OAM hologram (I_W) are both decom-

posed using the SVD method, respectively. The results can be described as

$$\begin{aligned} I_{\mathrm{W}} &= U_{\mathrm{W}} S_{\mathrm{W}} V_{\mathrm{W}}^{\mathrm{T}}, \\ I_{\mathrm{LL}} &= U_{\mathrm{LL}} S_{\mathrm{LL}} V_{\mathrm{LL}}^{\mathrm{T}}, \end{aligned} \tag{6}$$

where U_{W} and U_{LL} represent the left singular matrices. V_{W} and V_{LL} represent the right singular matrices. S_{W} and S_{LL} represent the singular value matrices. Then, the singular value matrix (S_{W}) corresponding to the cryptographic OAM hologram is added to the singular value matrix (S_{LL}) of the low-frequency component with embedding level (p, $p > 0$) resulting in a new singular value matrix (S'), which can be expressed as

$$S' = S_{\mathrm{LL}} + pS_{\mathrm{W}}, \tag{7}$$

where p represents the embedding level, which affects the imperceptibility of the watermark. For an excessively smaller p, the amount of the embedded watermark information is not enough for the watermark extraction. The original singular value matrix (S_{LL}) is replaced with the new singular value matrix (S') to obtain the new low-frequency component (I'_{LL}), which can be described as

$$I'_{\mathrm{LL}} = U_{\mathrm{LL}} S' V_{\mathrm{LL}}^{\mathrm{T}}. \tag{8}$$

Finally, the original low-frequency component (I_{LL}) is replaced with the new low-frequency component (I'_{W}), and all four components are transformed into the watermarked host image using the inverse discrete wavelet transform (iDWT).

2.3. Watermark recovery system

The watermarked host image is transmitted from the encryptor (using computer 1) to the decryptor (using computer 2) via network transmission. Figure 1(c) shows the OAM-watermark hologram recovery system. In the OAM-watermark hologram recovery system, the DWT is employed to decompose the watermarked host image into four non-overlapping subbands: the low-frequency component (I'_{LL}), the horizontal component (I'_{LH}), the vertical component (I'_{HL}), and the diagonal component (I'_{HH}). The low-frequency component (I'_{LL}) is further decomposed using the SVD method, as

$$I'_{\mathrm{LL}} = U'_{\mathrm{LL}} S'_{\mathrm{LL}} (V'_{\mathrm{LL}})^{\mathrm{T}}. \tag{9}$$

According to Eq. (7), the singular value matrix of the cryptographic OAM hologram can be obtained as

$$\begin{aligned} S'_{\mathrm{W}} &= \frac{S'_{\mathrm{LL}} - S_{\mathrm{LL}}}{p}, \\ I'_{\mathrm{W}} &= U_{\mathrm{W}} S'_{\mathrm{W}} V_{\mathrm{W}}^{\mathrm{T}}, \end{aligned} \tag{10}$$

where S'_{W} and I'_{W} represent the singular value matrix of the cryptographic OAM hologram and the recovery-cryptographic OAM hologram, respectively. Then, the OAM-watermark hologram ($I'_{\mathrm{O}}(u_0, v_0)$) is obtained from the recovery-cryptographic OAM hologram ($I'_{\mathrm{W}}(u_m, v_m)$) using the anti-Arnold transformation algorithm with decryption key ($\mathrm{Key}_2 = m$), which can be given by

$$\begin{bmatrix} u_0 \\ v_0 \end{bmatrix} = \begin{bmatrix} cd+1 & -c \\ -d & 1 \end{bmatrix}^m \begin{bmatrix} u_m \\ v_m \end{bmatrix} \bmod (M), \tag{11}$$

where (u_0, v_0) represents the pixel coordinates of the OAM watermark hologram ($I'_{\mathrm{O}}(u_0, v_0)$).

2.4. Optical reconstruction method

The optical reconstruction method (Fig. 1(d)) is employed to transform the OAM watermark hologram into the watermark image. Firstly, the key beam with the inverse OAM beam (multiple sub-keys, $\mathrm{Key}_1 = -l_1, -l_2, -l_3, \ldots, -l_K$) is used to illuminate the OAM watermark hologram, which can be described as

$$\begin{aligned} W'(u,v) &= I'_{\mathrm{O}}(u,v)[\exp(-\mathrm{i}l_1\theta) \\ &\quad + \exp(-\mathrm{i}l_2\theta) + \cdots + \exp(-\mathrm{i}l_K\theta)] \\ &= W'_1(u,v) + W'_2(u,v) + \cdots + W'_K(u,v), \end{aligned} \tag{12}$$

where the OAM mode in the OAM watermark hologram is converted to Gaussian mode. Then, the frequency domain ($W'(u,v)$) is tranformed into spatial domain ($s'(x,y)$) by the inverse Fourier transform (iFT). Hence, the watermark information is recovered through the Fourier lens, which can be given by

$$\begin{aligned} s'(x,y) &= \mathrm{iFT}(W'(u,v)) \\ &= s'_1(x,y) + s'_2(x,y) + \cdots + s'_K(x,y), \end{aligned} \tag{13}$$

where $s'(x,y)$ and $\mathrm{iFT}(\cdot)$ represent the recovery sampling watermark image and the inverse Fourier transform, respectively. According to Eq. (13), the matching of all multiple sub-keys is required for decrypting the complete watermark image.

3. Experimental results

To validate the proposed OAM-watermarking method, a proof-of-principle experiment is conducted. Figure 2 illustrates the experimental decryption process, where figures 2(a) and 2(b) represent the optical setup and its experimental results. Firstly, the Key_2 is used to obtain the right OAM-watermark hologram by the anti-Arnold transformation algorithm in the decryptor. Then, Computer 2 transmits the OAM hologram with K (here, four) Sub-keys to the spatial light modulator (SLM1, Holoeye PLUTO-2) for the generation of the key beam. Concurrently, Computer 2 dispatches the recovery OAM watermark hologram to SLM2.

In the optical setup (Fig. 2(a)), a laser operating at a wavelength of 633 nm is employed, and its intensity is adjustable using a variable neutral density filter (NDF). A half-wave plate (HWP) is utilized to align the beam's polarization direction

with SLM1, responsible for generating the OAM beam. SLM2 is used for imprinting the OAM watermark hologram. The OAM beam is directed onto SLM2 via a beam splitter (BS1). The beam reflected from BS2 of SLM2 is subjected to Fourier transformation using a lens with a focal length of 150 mm. Finally, the captured results are captured by a charge-coupled device (CCD). The size of the original host image and the watermark image are both 800×800 pixels ($M = 800$). It should be noted that if there is a long distance between SLM1 and SLM2, it becomes necessary to use an additional lens to control the size of the OAM beam generated by SLM1. Furthermore, precisely aligning the OAM beam with the center of SLM2 is crucial for achieving optimal reconstruction results.

The reconstruction watermarks are displayed in Fig. 2(b). When the scrambling times ($\text{Key}_2 = m$) are employed, the correct OAM-watermark hologram can be achieved. When the matched decoding beam, which contains four sub-keys ($\text{Key}_1 = -l_1, -l_2, -l_3, -l_4$), illuminates the OAM-watermark hologram, the captured result is shown as a Gaussian mode (solid point array) in four sub-watermarks. The point array is used to filter out the Gaussian mode. The reconstruction watermark is turned out by multiplying the captured result with the point array. However, there is no output from the reconstruction, when the Gaussian beam with no correct OAM mode is utilized as the decoding beam. If the unmatched decoding beam carrying a single or two sub-keys ($\text{Key}_1 = -l_4$, or $\text{Key}_1 = -l_1, -l_4$), only the corresponding sub-watermarks are transformed into Gaussian points, while the other sub-watermarks still in OAM mode, which they can not appear after the filtering. It is worth noting that the partial watermark information is meaningless for the watermarking. In addition, if the scrambling times (Key_2) do not match, the correct OAM-watermark hologram cannot be achieved, leading to an incorrect recovery watermark. Therefore, a sequence of TC (l) values and the scrambling times (m) are utilized as cryptographic keys (Key_1 and Key_2) in the proposed watermarking scheme. The four sub-keys in Key_1 resemble a secret sharing scheme, which provides greater security compared to using a single cryptographic key.

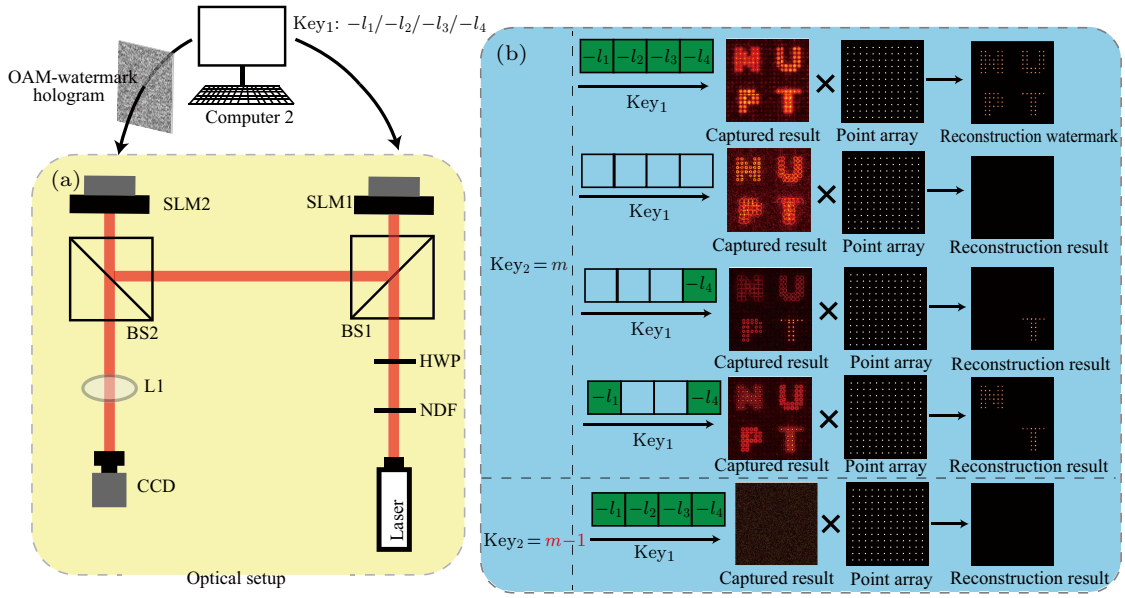


Fig. 2. The experimental decryption process: (a) the optical setup, (b) the experimental results with different key beam ($\text{Key}_1 = 0$ and -2) and the scrambling time ($\text{Key}_2 = m$ and $m - 1$).

4. Discussion

4.1. Security

To further enhance security, we propose adding the interference image to conceal the watermark information, as shown in Fig. 3. Figure 3(a) illustrates the processes of adding the interference image. Figure 3(b) shows a comparison of the captured results without and with the interference image. Firstly, the interference image complements the four sub-watermarks. The interference hologram is obtained using the same steps as for a single sub-watermark with the interference image, with a TC value of 5 ($l = 5$). Then, the interference hologram and the OAM-watermark hologram are multiplexed to generate the Mux-watermark hologram. Finally, the Mux-watermark hologram is embedded into the host image using the same method as the OAM-watermark hologram.

The specific steps for multiplexing (MUX) include: Both the OAM-watermark hologram and the interference hologram undergo Fourier transformations (FT). The Fourier-transformed results are then added together. This added result is subjected to an inverse Fourier transform (iFT). From the outcome of this inverse Fourier transform, the phase-only hologram is extracted using the angle algorithm to create the Mux-watermark hologram.

When the watermarked host image with the OAM-

watermark hologram is reconstructed using a single sub-key (such as $l = -8$), the corresponding sub-watermark appears as Gaussian points and can be successfully reconstructed (Fig. 3(b)). However, other ring-shaped light spots may reveal the sub-watermark information. For the watermarked host image with the Mux-watermark hologram reconstructed using the same sub-key ($l = -8$), the corresponding sub-watermark is similarly displayed as Gaussian points and is successfully reconstructed. Importantly, the additional ring-shaped light spots from the interference image effectively mask the ring-shaped light spots of the sub-watermarks, thereby enhancing security. Therefore, our proposed method can further enhance security by utilizing the interference image.

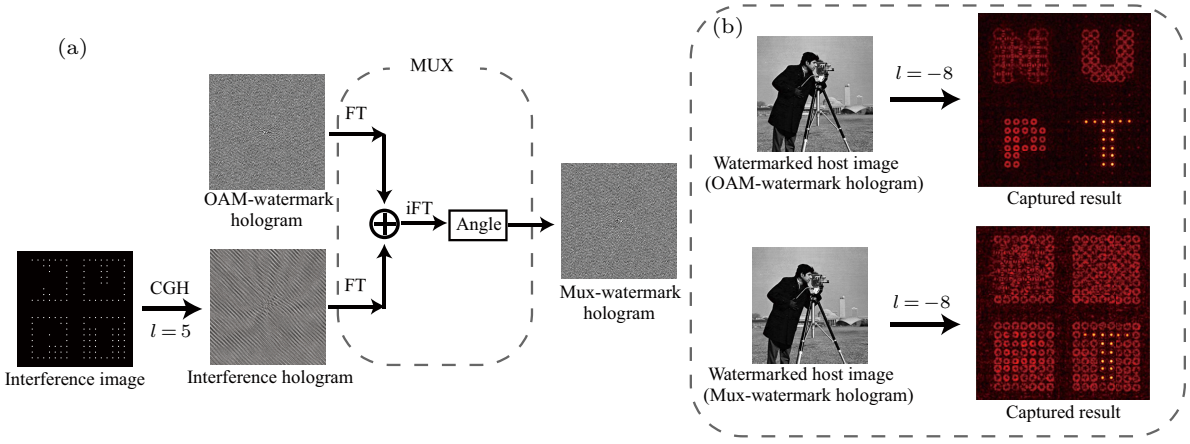


Fig. 3. (a) The processes of adding the interference image. (b) The comparison of the captured results without and with the interfering image.

4.2. Imperceptibility

To evaluate the imperceptibility of our watermarking method, the peak signal-to-noise ratio (PSNR) and the histogram are employed. The PSNR measures the degree of similarity between the watermarked host image and the original host image. It assists in assessing whether the watermarking process affects the visual quality as perceived by human observers. The higher PSNR value indicates better imperceptibility and improved visual quality. The PSNR is defined as[33]

$$\begin{aligned} \mathrm{PSNR} &= 10\lg\left(\frac{(2^n-1)^2}{\mathrm{MSE}}\right), \\ \mathrm{MSE} &= \frac{1}{M\times M}\sum_{x=1}^{M}\sum_{y=1}^{M}[f(x,y)-f'(x,y)]^2, \end{aligned} \tag{14}$$

where n and MSE represent the bit depth of the host image (here $n = 8$) and the mean square error. $f(x,y)$ and $f'(x,y)$ represent the intensity value of the original host image and the watermarked host image, respectively.

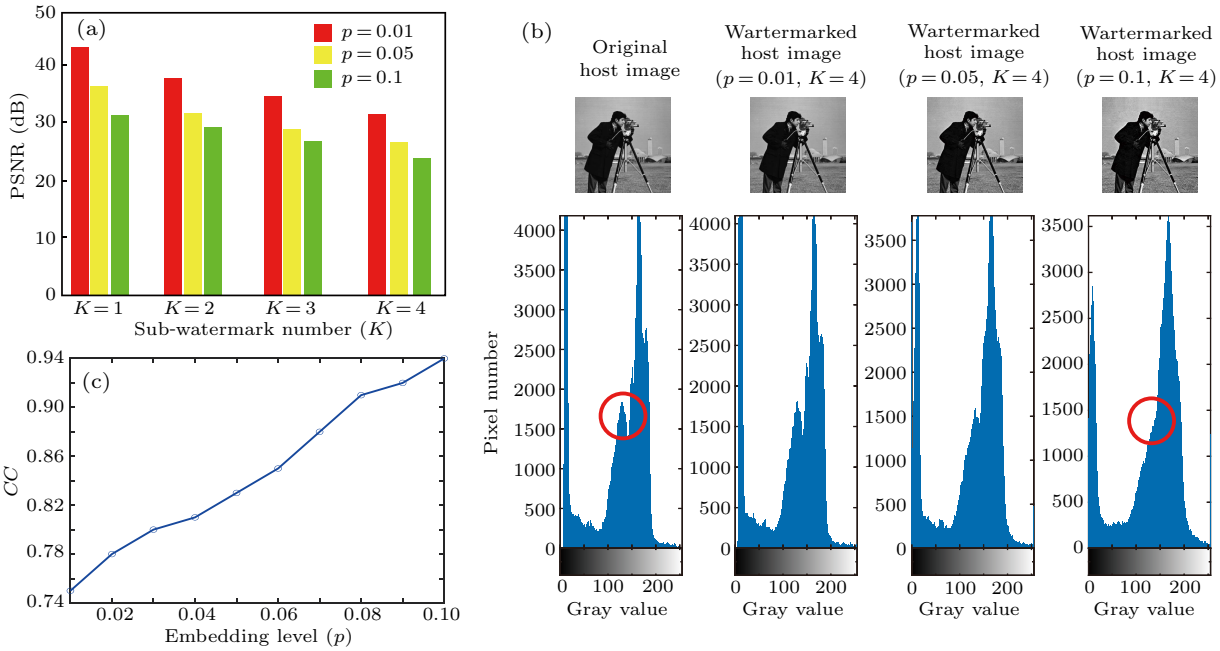


Fig. 4. (a) The PSNR with different embedding levels (p), and the sub-watermark number (K). (b) Histograms of the original host image and different watermarked host images. (c) The correlation coefficient (CC) with different embedding levels.

In addition, the correlation coefficient (CC) is also introduced to compare the similarity between the reconstructed watermark image ($s'(x,y)$) and the original watermark image ($s(x,y)$). The CC between the two images is defined as[34]

$$CC = \frac{E\{[s-E(s)]-[s'-E(s')]\}}{\sigma_s \sigma_{s'}}, \tag{15}$$

where s and s' represent the original watermark image and the reconstructed watermark image respectively, σ is the standard deviation of the corresponding image. $E\{\cdot\}$ represents the expected value operator.

The PSNR of the watermarked host image is analyzed under different embedding levels (p), and the sub-watermark number (K), as shown in Fig. 4(a). Generally, PSNR beyond 30 dB is considered to be of good imperceptibility. From the results, it is evident that provided the embedding level and sub-watermark number are not excessively high, the PSNR consistently exceeds 30 dB. When the sub-watermark number is 4 ($K = 4$), the watermarked host images with different embedding levels ($p = 0.01, 0.05$, and 0.1) and their histograms are shown in Fig. 4(b). The histograms of the watermarked host images with $p = 0.01$ and $p = 0.05$ are similar to the original host image. However, the histograms of the watermarked host image with $p = 0.1$ have a slight difference from the original host image. The intensity distribution of the pixels and the areas within the red circles exhibit noticeable differences. It should be noted that a smaller embedding level leads to a higher PSNR but a lower CC, as illustrated in Fig. 4(c). Thus, based on these data, our proposed image watermarking scheme can achieve good imperceptibility through the embedding level and the sub-watermark number.

4.3. Robustness

Additionally, to quantitatively assess the robustness, a series of attack tests on the watermarked host image is conducted by employing various methods, including the noise attacks (Gaussian noise, Poisson noise, salt-pepper noise), JPEG compression, Gaussian low-pass filtering, cropping, and rotation. The embedding level is 0.05 ($p = 0.05$) and the sub-watermark number is 1 ($K = 1$). The test results of the attacked watermarked host images, the reconstruction watermarks, and their CC are shown in Fig. 5. The results indicate that the proposed watermarking scheme exhibits high robustness against JPEG compression attacks, Poisson noise, and Gaussian low pass, with all CC exceeding 0.95 ($CC > 0.95$). In the case of salt-pepper noise, with a noise density of 0.1, its correlation coefficient (CC) is 0.9203 ($CC = 0.9203$). Regarding cropping, when the cropped area constitutes 5.5% of the host image area,

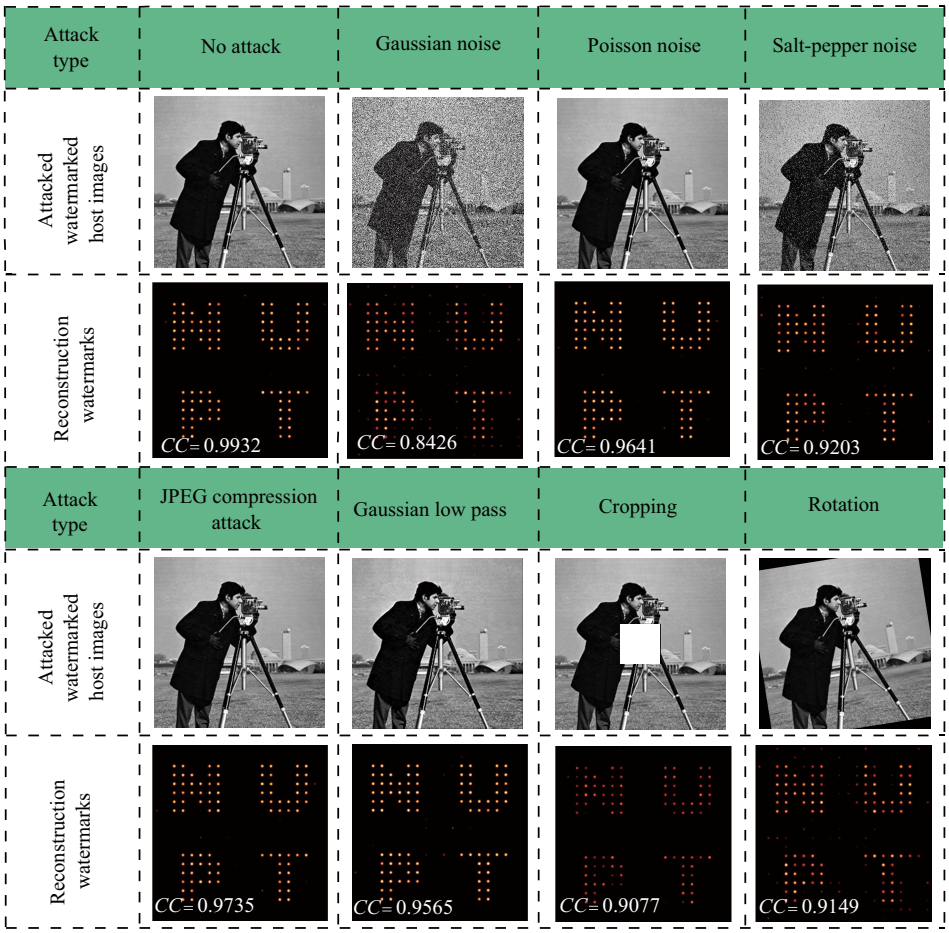


Fig. 5. The experimental results of different attack tests, including Gaussian noise, Poisson noise, salt-pepper noise, JPEG compression attacks, Gaussian low-pass filtering, cropping, and rotation.

its *CC* is 0.9077 ($CC = 0.9077$), and cropping weakens the intensity of the reconstructed watermark. For rotation, at an angle of 10 degrees (10°), its *CC* is 0.9149 ($CC = 0.9149$). In the case of Gaussian noise, under a variance of 0.03, its *CC* is 0.8426 ($CC = 0.8426$), and the watermark information retrieval becomes unfeasible when the variance exceeds 0.05. It is relatively weaker against Gaussian noise because Gaussian noise introduces a continuous and evenly distributed perturbation into the image data. On the whole, the proposed image watermarking scheme is robust against most attacks, but less against Gaussian noise.

4.4. Comparison analysis

We compared the effects of embedding the cryptographic OAM hologram into different components of the host image (I_{LL}, I_{LH}, I_{HL}, and I_{HH}). The number of sub-watermarks is 4 ($K = 4$), and the embedding level is 0.05 ($p = 0.05$). The experimental results with various embedding components are shown in Fig. 6. From the histogram results, embedding the cryptographic OAM hologram into the low-frequency components exhibits better consistency with the original host image. (particularly at the four positions marked with red circles). Based on the histogram and *CC* results, embedding the cryptographic OAM hologram into the low-frequency components is the optimal choice.

On the other hand, we compared our proposed OAM-image watermarking scheme with several recent and representative image encryption schemes in terms of correlation coefficients (*CC*) and peak signal-to-noise ratio (PSNR). The results of these comparisons are summarized in Tables 1 and 2, respectively.

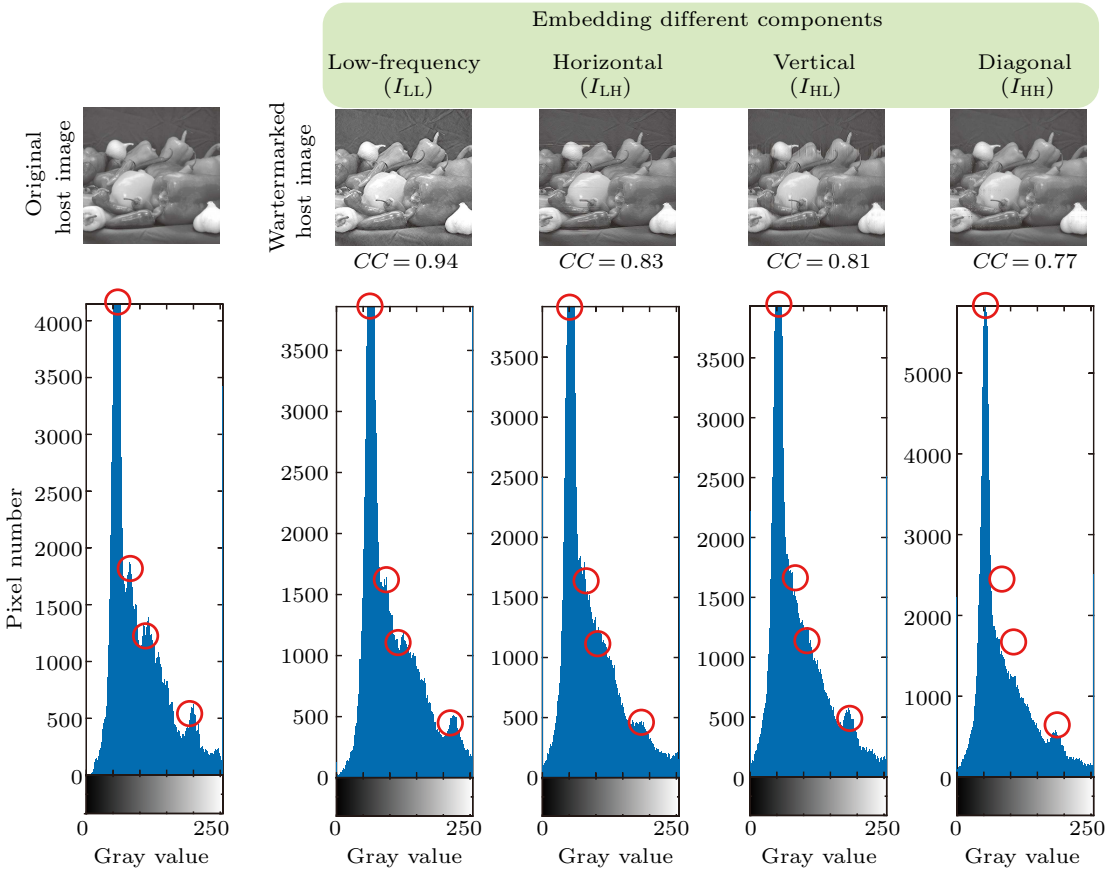


Fig. 6. Histogram and *CC* experimental results for embedding the cryptographic OAM hologram into different components.

Table 1. Comparison of *CC* values between the proposed scheme and other schemes[5–7] under various attacks.

Attacks	Ref. [5]	Ref. [6]	Ref. [7]	Proposed scheme
Gaussian noise	0.9845	0.9852	0.9917	0.8426
Poisson noise	0.9761	0.9793	0.9913	0.9641
Salt-pepper noise	0.9856	0.9864	0.9883	0.9203
JPEG compression	0.9892	0.9920	0.9965	0.9735
Gaussian lowpass filtering	0.9856	0.9854	0.9877	0.9565
Cropping	0.9235	0.9734	0.9759	0.9077
Rotation	0.9847	0.9725	0.9938	0.9149

Table 2. Comparison of PSNR values between the proposed scheme and other schemes.[5–7]

Schemes	Ref. [5]	Ref. [6]	Ref. [7]	Proposed scheme
PSNR	56.14 dB	57.28 dB	56.63 dB	56.45 dB

As shown in Tables 1 and 2, the *CC* values of our method under each type of attack demonstrate a disparity when compared to the other three methods, particularly in response to the Gaussian noise attack. In addition, regarding the PSNR values, our method exhibits comparable performance with no

significant disparities observed when contrasted with the three established methods. The primary reason for this disparity is that the other three methods employ computational techniques to restore watermarked images, whereas our method requires optical means for image restoration. The watermark results are captured by a CCD camera, and speckle noise in the optical path significantly impacts the quality of watermark recovery. Although our method demonstrates lower *CC* values, the combination of algorithmic and optical experimental approaches adds complexity to the watermark reconstruction process, thereby enhancing its security.

5. Conclusion

In conclusion, we have developed an optical image watermarking scheme utilizing OAM holography, in which a sequence of topological charge (TC) values (l) and scrambling times (m) function as cryptographic keys to secure watermark information. Our experimental results demonstrate that the watermark image can be accurately reconstructed using matched keys. Enhanced security is achieved by employing the correct combination of four TC values and scrambling times. Moreover, we optimized the imperceptibility of the watermark by fine-tuning the embedding depth and the number of sub-watermarks. Attack tests further validated the robustness of our scheme and its ability to recover after various disruptions. This work presents a viable method for protecting sensitive data across different sectors, potentially advancing the field of information security.

For future work, we aim to explore the integration of quantum cryptography principles to further enhance security measures. Additionally, we plan to conduct cross-media watermarking tests to evaluate the scheme's efficacy in diverse digital formats, extending its applicability. Finally, testing under more aggressive attack scenarios will be crucial to ensure that the watermarking scheme can withstand evolving cyber threats, thereby contributing to its practical implementation in real-world applications.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant No. 62375140), the Natural Science Foundation of Suqian, Jiangsu Province, China (Grant No. S202108), the Open Research Fund of the National Laboratory of Solid State Microstructures (Grant No. M36055), and the Postgraduate Research & Practice Innovation Program of Jiangsu Province, China (Grant No. KYCX21-0745).

References

[1] Feng X F, Jiang M R, Zhang H and Wang C P 2024 *Journal of the Franklin Institute* **361** 319
[2] Zhou N R, Tong L J and Zou W P 2023 *Signal Processing* **211** 109107
[3] Ye G D, Wu H S, Liu M and Huang X L 2023 *Chaos, Solitons & Fractals* **171** 113469
[4] Rieyan S A, News M R K, Rahman A M, Khan S A, Zaarif S T J, Alam M G R, Hassan M M, Lanni M and Fortino G 2024 *Information Fusion* **102** 102004
[5] Zhou N R, Hu L L, Huang Z W, Wang M M and Luo G S 2024 *Expert Systems with Applications* **238** 122052
[6] Gong L H and Luo H X 2023 *Optics & Laser Technology* **167** 109665
[7] Liang Q and Zhu C X 2023 *Optics & Laser Technology* **160** 109033
[8] Sui L S, Zhang X, Huang C T, Tian A L and Anand Krishna A 2019 *Optics and Lasers in Engineering* **113** 29
[9] Sui L S, Xin M T and Tian A L 2013 *Opt. Lett.* **38** 1996
[10] Takai N and Mifune Y 2002 *Appl. Opt.* **41** 865
[11] Kishk S and Javidi B 2003 *Opt. Lett.* **28** 167
[12] Zhao N X, Li Z L, Zhu G D, Li J X, Deng L G, Dai Q, Zhang W G, He Z X and Zheng G X 2022 *Opt. Express* **30** 37554
[13] Jiao S M, Zhou C Y, Shi Y S, Zou W B and Li X 2019 *Optics & Laser Technology* **109** 370
[14] Shao W D, Huang D M, Li H Y, Deng L, Yang Q, Dai X X, Liu D M and Cheng M F 2023 *Journal of Lightwave Technology* **41** 4941
[15] Ye Z Y, Qiu P H, Wang H B, Xiong J and Wang K G 2019 *Opt. Express* **27** 36505
[16] Xiao D, Li X W, Wang D, Wang Y and Wang Q H 2019 *Opt. Commun.* **453** 124340
[17] Chen Y Y, Wang J H, Lin C C and Hwang H E 2013 *Appl. Opt.* **52** 5247
[18] Jiao S M, Zhang D F, Zhang C L, Gao Y, Lei T and Yuan X C 2021 *Optics and Lasers in Engineering* **138** 106455
[19] Chen Y Y, Zhou X, Xiao Y L, Yuan S and Wu X L 2010 *Optics & Laser Technology* **42** 617
[20] Sui L S, Cheng Y, Tian A L and Anand Krishna A 2018 *Optics and Lasers in Engineering* **107** 38
[21] Guo X Y, Zhong J Z, Li B J, Qi S X, Li Y, Li P, Wen D D, Liu S, Wei B Y and Zhao J L 2022 *Adv. Mater.* **34** 2103192
[22] Fang X Y, Ren H R and Gu M 2020 *Nat. Photon.* **14** 102
[23] Ren H R, Fang X Y, Jang J, Bürger J, Rho J and Maier S A 2020 *Nat. Nanotechnol.* **15** 948
[24] Zhu J L, Wang L and Zhao S M 2022 *IEEE Photon. Technol. Lett.* **35** 179
[25] Olaleye T M, Ribeiro P A and Raposo M 2023 *Photonics* **10** 664
[26] Trichili A, Rosales-Guzmán C, Dudley A, Ndagano B, Ben Salem A, Zghal M and Forbes A 2016 *Sci. Rep.* **6** 27674
[27] Zhou H Q, Wang Y T, Li X, Xu Z T, Li X W and Huang L L 2021 *Appl. Phys. Lett.* **119** 044104
[28] Zhu J L, Wang L, Ji J Y and Zhao S M 2022 *Appl. Phys. Lett.* **120** 251104
[29] Dong J T, Tian Z P, Wang S, Xie L Y, Li Y Y and Zhao E X 2023 *Opt. Lett.* **48** 2018
[30] Pi D P, Liu J and Wang Y T 2022 *Light: Science & Applications* **11** 231
[31] Meng W J, Pi D P, Li B L, Luan H T, Gu M and Fang X Y 2024 *Laser & Photonics Reviews* **18** 2301258
[32] Elayan M A and Ahmad M O 2016 *International Conference on Image and Signal Processing*, May 7 2016, p. 317
[33] Wang S Q, Meng X F, Yin Y K, Wang Y R, Yang X L, Zhang X, Peng X, He W Q, Dong G Y and Chen H Y 2019 *Optics and Lasers in Engineering* **114** 76
[34] Qu G, Meng X F, Yang X L, Wu H Z, Wang P W, He W Q and Chen H Y 2021 *Optics and Lasers in Engineering* **137** 106376