Multi-dimensional multiplexing optical secret sharing framework with cascaded liquid crystal holograms

Keyao Li, Yiming Wang, Dapu Pi, Baoli Li, Haitao Luan, Xinyuan Fang, Peng Chen, Yanqing Lu and Min Gu

https://doi.org/10.29026/oea.2024.230121

Received: 25 July 2023; Accepted: 10 November 2023; Published online: 25 January 2024

Related articles

100 Hertz frame-rate switching three-dimensional orbital angular momentum multiplexing holography via cross convolution
Weijia Meng, Yilin Hua, Ke Cheng, Baoli Li, Tingting Liu, Qinyu Chen, Haitao Luan, Min Gu, Xinyuan Fang

Flat multifunctional liquid crystal elements through multi-dimensional information multiplexing
Dongliang Tang, Zhenglong Shao, Xin Xie, Yingjie Zhou, Xiaohu Zhang, Fan Fan, Shuangchun Wen

Metasurface-based nanoprinting: principle, design and advances
Rao Fu, Kuixian Chen, Zile Li, Shaohua Yu, Guoxing Zheng

4K-DMDNet: diffraction model-driven network for 4K computer-generated holography
Kexuan Liu, Jiachen Wu, Zehao He, Liangcai Cao

More related article in Opto-Electronic Journals Group website

http://www.oejournal.org/oea
Multi-dimensional multiplexing optical secret sharing framework with cascaded liquid crystal holograms

Keyao Li¹,²†, Yiming Wang³†, Dapu Pi¹, Baoli Li¹, Haitao Luan¹, Xinyuan Fang¹*, Peng Chen³*, Yanqing Lu³ and Min Gu¹

Secret sharing is a promising technology for information encryption by splitting the secret information into different shares. However, the traditional scheme suffers from information leakage in decryption process since the amount of available information channels is limited. Herein, we propose and demonstrate an optical secret sharing framework based on the multi-dimensional multiplexing liquid crystal (LC) holograms. The LC holograms are used as spatially separated shares to carry secret images. The polarization of the incident light and the distance between different shares are served as secret keys, which can significantly improve the information security and capacity. Besides, the decryption condition is also restricted by the applied external voltage due to the variant diffraction efficiency, which further increases the information security. In implementation, an artificial neural network (ANN) model is developed to carefully design the phase distribution of each LC hologram. With the advantage of high security, high capacity and simple configuration, our optical secret sharing framework has great potentials in optical encryption and dynamic holographic display.

Keywords: holographic encryption; optical secret sharing; cascaded liquid crystal hologram; multi-dimensional multiplexing


Introduction

Secret sharing distributes the secret image to different shareholders and decodes the secret images by conjoining sufficient shares together. It is considered as a trustworthy cryptographic method and has been widely used in the fields of privacy protection and intellectual property rights¹,². Due to the parallel information processing ability and multi-dimensional multiplexing capability, optical encryption has attracted more attention in the last decade³−¹⁹. As an essential security element, optical holography, where the secret images are embedded into the pre-encoded phase-only holograms, is an effective way to realize optical secret sharing²⁰−²⁷. Nevertheless, the bulky optical components and limited modulation ability hinder optical holography to build up a compact and multifunctional secret sharing system²⁸. To break these constraints, the development of light-weight and high-efficiency optical components is highly desirable. In this work, we introduce an optical secret sharing framework based on liquid crystal (LC) holograms, which can be controlled by external electric fields. With the help of an artificial neural network (ANN) model, we can carefully design the phase distribution of each LC hologram. This framework demonstrates excellent performance in information security, capacity, and configuration simplicity.
bottlenecks, cascaded metasurface has further been used for secret sharing. In this method, the secret information can only be decrypted when the metasurfaces are accurately combined, thus ensuring the security of the secret sharing system. However, owing to the inherent limitations of metasurface, it is difficult to create secret sharing platforms massively with merit of dynamic tunability.

Due to the multi-dimensional modulation capacity, voltage sensitivity and high diffraction efficiency, liquid crystals (LCs) with anisotropic molecule architectures have evolved as a promising candidate for information encryption. For example, LC holograms based on chirality invertible superstructures have been proposed to enable a high-dimensional multiplexing information encryption platform. However, so far, constrained by traditional algorithm, most LC holographic devices are one-layer configuration, which only allow for the access to different information channels, but not the physical segmenting of these information channels among different shareholders. In this context, cascaded LC holograms provide the possibility for the physical separation of the secret information and have great potential for creating a multi-dimensional multiplexing, dynamic adjustable and high diffraction efficiency secret sharing platform.

In this work, we experimentally demonstrate a hybrid-multiplexing LC optical secret sharing framework. The secret information is decomposed and dispensed into two co-constrained LC holograms, each of which can reconstruct an authentication image in the specific location. Moreover, when these two LC holograms are stacked together, six independent new holographic images can be decrypted with different secret keys, including polarization of the incident light and the distance between the cascaded LC holograms. We utilize the ANN to complete the inverse design of the sophisticated multi-confined and cascaded multilayer issues. This cascaded LC scheme breaks the limitations of traditional optical secret sharing, and blazes a trail in broad areas of optical visual cryptography, dynamic holographic display, and ultra-high-capacity information storage.

Design principle
The optical secret sharing framework based on the cascaded LC holograms is illustrated in Fig. 1(a). By optimizing the corresponding phase distribution of each LC hologram through ANN method, the incident light with specific polarization state is modulated by the cascaded LC scheme breaks the limitations of traditional optical secret sharing, and blazes a trail in broad areas of optical visual cryptography, dynamic holographic display, and ultra-high-capacity information storage.

![Fig. 1 | Illustration diagram of the multi-dimensional multiplexing optical secret sharing framework based on the cascaded LC holograms. (a) A neural network is adapted to inversely design the phase distribution of the LC holograms and the secret images can be decrypted when the circular polarization light illuminates on the distance-adjustable cascaded LC holograms with appropriate external voltage. (b) The different secret keys and the corresponding decrypted holographic images.](image-url)
LC holograms and the secret information is decrypted at the predetermined distance. The LC element consists of two indium-tin-oxide glass outside, two photoalignment layers inside and one nematic LC layer in the middle. The modulation function of the LC can be changed by setting different external voltages, as displayed in the zoom-in view in Fig. 1(a). If the incident light is left circular polarization (LCP), and only the LC hologram 1 is in the ‘on’ state ($U_{on}$), the authentication image ‘2’ will be decrypted at the predetermined location and recorded by the charge-coupled device (CCD). In this situation, the incident light is modulated only by LC hologram 1 and equivalent to directly passing through LC hologram 2 without phase modulation. When the working state of the two LC holograms is inverse, the authentication image ‘4’ will be decrypted at the same position. Keeping the position of LC hologram 1 unchanged and moving the LC hologram 2, six secret images will be decrypted when the corresponding polarized light and distance are used as the secret keys, as shown in Fig. 1(b). Specifically, the polarization state of incident light includes LCP and right circular polarization (RCP). In addition, the initial distance between the cascaded LC holograms is $d_1=4$ cm, and the moving step length of the LC hologram 2 along the axial direction is 1.5 cm ($d_2=5.5$ cm, $d_3=7$ cm). The peak signal-to-noise ratio (PSNR) is adopted to evaluate the quality of the holographic reconstructed images. To obtain the value range of the distance with good effectiveness, the relationship of the average PSNR of the two circular-polarization-multiplexing images with the distance has been firstly analyzed (Fig. S1). In this way, the optical secret sharing framework with cascaded LC holograms can reconstruct eight different holographic images containing two authentication images and six secret images.

According to the above-mentioned approach, we structure a neural network with multi-dimensional and co-constrained input fields as shown in Fig. 2. The polarization states of the incident light, the imposed external voltage and the moving distance between the two LC holograms are presumed as the input parameters. The angular spectrum diffraction theory builds up the full connection of all layers. The forward propagation model of the wavefronts in the free space after modulated by the layers can be described as

$$E(x, y) = F^{-1}\{F[\phi_s(x, y)] \cdot H_d(u, v)\}, \quad (1)$$

where $F$ and $F^{-1}$ denote the Fourier transform and the inverse Fourier transform, respectively. $E_s(x, y)$ represents the product of input field $O(x_0, y_0)$ and the transmission coefficient of the neurons $g(\phi_s)$. The transfer function $H_d(u, v)$ is expressed as

$$H_d(u, v) = \exp\left[ikd\sqrt{1 - \lambda^2u^2 - \lambda^2v^2}\right], \quad (2)$$

**Fig. 2** Design principle of multi-dimensional multiplexing optical holographic secret sharing framework. The polarization states of the incident light, the imposed external voltage and the moving distance between the two LC holograms are the input parameters of the ANN model. The difference between the reconstructed images and the ideal images is defined as the loss function. Through the back-propagation optimization process, the phase distributions of the two LC holograms are calculated.
where \( u \) and \( v \) are spatial frequencies, and \( k = \frac{2\pi}{\lambda} \) is the wave number. The distance between the cascaded LC holograms is \( d = d_0 + n\Delta d \), where \( d_0 \) is the initial distance between the cascaded LC holograms and \( \Delta d \) is the moving step length. According to the above framework, different input fields can be mapped to the corresponding secret image in the output plane by using the error back-propagation algorithm to update the learnable parameters \( g(\phi_s) \). The aim of the error back-propagation algorithm is to minimize the loss function (mean squared error, MSE) between the actual and ideal output intensity distribution. The phase distribution of the LC holograms can be obtained when the loss function gradient with regard to phase distribution converges. Owing to the spin-orbital interplay of light in anisotropic medium, the consecutive phase modulation in LC through PB phase is feasible. In practice, all LC unit-cells possess orientation angle in the plane as well as out of plane, called LC director. The Pancharatnam–Berry (PB) phase modulation is twofold of the orientation angle in-plane of each unit-cell. In this way, different in-plane orientation angles ranged in \((-90^\circ, 90^\circ)\) can correspondingly realize the PB phase modulation of \((0, 2\pi)\).

**Results and discussion**

Through the effective and convenient network, the design of the multi-multiplexing optical holographic secret sharing framework based on the cascaded LC holograms can be accomplished. We verify the performance and practicality of the proposed secret sharing framework using the experimental equipment displayed in Fig. 3(a). In order to import and transmit the expected circular polarization state of the incident light, a linear polarizer (OPPF1-VIS, JCOPTIX, China) and a quarter-wave plate (TWP20Q, JCOPTIX, China) are placed in front of as well as behind the cascaded LC holograms as circular polarizer and analyzer. Two LC holograms are laid on two three-dimensional translation stages. The grayscale images in the top-left and bottom-right corner are the simulated phase distribution of share 1 and share 2. The reddish-brown images in the zoom-in view are the corresponding polarized micrograph of the fabricated LC holograms. Q-wave plate, quarter-wave plate. (b) The diffraction efficiency of the LC holograms with different external voltage.

---

**Fig. 3** | The experimental setup and the diffraction efficiency of the LC holograms. (a) Optical setup for multi-multiplexing optical holographic secret sharing framework. The grayscale images in the top-left and bottom-right corner are the simulated phase distribution of share 1 and share 2. The reddish-brown images in the zoom-in view are the corresponding polarized micrograph of the fabricated LC holograms. Q-wave plate, quarter-wave plate. (b) The diffraction efficiency of the LC holograms with different external voltage.
stages to achieve the precise alignment and moving step length, meanwhile the initial distance between the two LC holograms is set as 4 cm. All the decrypted holographic images are collected by a CCD in the same imaging plane and the wavelength of the illumination light is 633 nm (HNL20L, Thorlabs, America). Each LC hologram has an effective size of 2.12 mm×2.12 mm and contains 768×768 pixels. The zoom-in view of Fig. 3(a) individually shows the simulated phase distribution and the polarized micrograph of the fabricated LC hologram samples.

In implementation, the anisotropy will alter when an external electric field is imposed to change the LC director from in-plane to out-of-plane. The variation of anisotropic refractive index bestowed the LC director with the ability of electrically adjustable phase retardation. Therefore, the diffraction efficiency can be dynamically controlled by imposing different external voltages. The tendencies of the diffraction efficiency versus voltage for two LC holograms at working wavelength of 633 nm are depicted in Fig. 3(b), respectively. The optimum on-state voltage for LC hologram 1 and LC hologram 2 is 5.4 V and 5.8 V respectively, and the corresponding diffraction efficiency can reach 61.5% and 62.4%. Nevertheless, the two LC holograms are off-state when the voltages are set as 3.6 V and 3.8 V, respectively. Here, the efficiency, or polarization conversion efficiency, at the activation voltage is determined by the diffraction efficiency of the phase pattern and the transmittance of the LC device. As such, the quality of holographic images from single LC hologram can be improved after selecting the appropriate polarization states. However, for secret sharing, the noise cannot be separated thoroughly from the final secret images through polarization filtering because the polarization states remain unchanged in the processes. Benefitting from the sensitivity of external voltage stimuli, LC holograms acquire the dynamic modulation ability, which provides the possibility to unlock information without detaching any shares and enables the optical secret sharing platform more compact and stable. According to above characteristics, we can conveniently acquire the authentication information and the secret images through the optical secret sharing framework by user-friendly adjusting the external voltage.

Numerous encoding information can transmit in different users with high security through the optical secret sharing framework as displayed in Fig. 4. In the optical secret sharing framework, different secrets are shared and customized keys are assigned to two different users. By using the identity keys, user 1 and user 2 can acquire the authentication images ‘2’ and ‘4’, as shown in Fig. 4(a). Utilizing different operator keys from other information recipient, i.e., the different polarization states and separation distance of two LC samples, the operator images including multiplication (×), division (÷), exponentiation (∧), integer rounding (%), calculating residue (//) and radical sign (√), can be experimentally reconstructed as shown in Fig. 4(b). Combining the authentication

![Fig. 4](https://example.com/fig4.png)
images with the operator images to carry out the second decryption, the eventual secret information is worked out. Here, the spatial position of the LC holograms along the propagation direction was adopted as the pre-negotiated calculation order of the secrets in our proposed scheme. The PSNR of experimental results in Fig. 4(b) can be calculated as 16.11 dB (‘2’), 16.77 dB (‘4’), 15.51 dB (‘x’), 15.8 dB (‘+’), 15.06 dB (‘\(\wedge\)’), 13.58 dB (‘%’), 14.62 dB (‘/’), and 13.91 dB (‘\(\sqrt{-}\)’), which are close to the theoretical results in Fig. 2. To explain the insufficient image quality, the optimization process in our scheme can mathematically be seen as a multiple loss optimization problem, wherein the loss function is constrained by all the mean square error (MSE) for reconstructing multiple images (Supplementary Section 1). As such, the increase of the multiplexing images results in more MSE terms in loss functions, which can be physically interpreted as the noises (or crosstalk) which results in the decrease of the PSNR values (Fig. S2). Without losing generality, to analyze the pixel match problem, we have evaluated the effect of displacement in the x direction between two holograms as shown in the Fig. S3. To analyze the distance sensitivity, some deviation along the light propagation direction (\(\Delta d\)) has been added on the original location (Fig. S4). The deviation of the fast axis of the first QWP results in the elliptically-polarized incident beams. Here, the secret images reconstructed by different elliptically-polarized beams are given in Fig. S5 to illustrate the robustness.

The proposed multi-dimensional multiplexing optical secret sharing framework allows for the simultaneous and ultra-high security transmission of multiple messages, which overcomes the drawbacks of traditional holographic encryption methods and has lots of superiorities than earlier solutions. Firstly, the secret images are hidden into different shares (LC holograms) and the terminal secret images can only be decrypted through the cascaded shares. Even if one of the shares is stolen, the secret image cannot be retrieved and only the authentication image as camouflage will be revealed, which greatly improves the security of the secret sharing platform. The crack difficulty of the framework was also analyzed when one hologram is fixed and the effective pixel number of the other hologram is ranging (Supplementary Section 2, Fig. S6). Secondly, the multi-dimensional multiplexing technique increases the complexity of secret key, which enhances the security and information capacity. Notably, the multiplexing information channels for encryption can be further increased by incorporating more secret shares (Supplementary Section 3, Fig. S7). Also, it is possible to utilize the linear polarization states to increase the information channels of this holographic secret sharing scheme. (Supplementary Section 4, Fig. S8). Thirdly, owing to the electrical adjustable ability of the LC device, the security of the proposed secret sharing framework can be further improved. The imposed external voltage can be mapped independently to the different secret shares, which sets more stringent conditions to decrypt the secret information and reduces the possibility of information disclosure. Notably, in comparison to the holographic secret schemes with metasurface holograms\(^{29}\), the unique advantages of LC devices, such as high diffraction efficiency, controllable efficiency, and low manufacturing cost, is more suitable for such secret sharing scheme with cascaded diffractive holograms. Considering current advanced technology in LC display industry, the mass manufacturing of this secret sharing platform could be feasible as well.

**Conclusions**

In this work, we propose and experimentally demonstrate the multi-dimensional multiplexing optical secret sharing framework with cascaded LC holograms. We create a dependable and practical neural network of error back-propagation based on the angular spectrum diffraction theory to design the framework. The multi-dimensional inputs of our network in the encryption process, such as polarization of light, distance between the LC holograms and the applied external electrical voltage, enhance the security of the secret information. The two authentication images and six operator images can be respectively decrypted if all the secret keys are correct, and the final secret information will be revealed through the second decoding. The full-fledged manufacturing technology of LC devices allows our proposal to be more practicable and versatile. Therefore, with merits of convenient design, extensive fabrication and outstanding security, the multi-dimensional multiplexing optical secret sharing framework has great potential to be used in information storage, dynamic display, and multi-functional optical information processing.

**References**

2. Blakley GR. Safeguarding cryptographic keys. In 1979 Interna-
### Acknowledgements

We would like to acknowledge the support from the National Natural Science Foundation of China (No. 62005164, 62122507, 62175101, and 62005166), the Shanghai Natural Science Foundation (23ZR1443700), Shanghai Education Development Foundation and Science Foundation of China (No. 62005164, 62222507, and 62175101). The support from the National Natural Science Foundation of China (No. 62322040, 62375101, and 62527808) is also acknowledged. The support of CAST Young Elite Scientists Sponsorship Program by CAST (No. 20220042, Science and Technology on Managing Requirements Knowledge 313–318 (IEEE, 1979); http://doi.org/10.1109/MARK.1979.8817296.


ology Commission of Shanghai Municipality (Grant No. 21DZ1100500), the Shanghai Municipal Science and Technology Major Project, and the Shanghai Frontiers Science Center Program (2021–2025 No. 20).

**Author contributions**

X. Y Fang proposed the original idea and conceived the experiment. K. Y. Li performed the experiment, assisted by B. L. Li and H. T. Luan. Y. M. Wang and P. Chen fabricated the sample and carried out the microimaging. D. P Pi and K. Y. Li wrote the original manuscript, revised by X. Y. Fang and P. Chen. M. Gu, Y. Q. Lu, P. Chen and X. Y. Fang provided the resource support, funding acquisition and supervised the project.

**Competing interests**

The authors declare no competing financial interests.

**Supplementary information**

Supplementary information for this paper is available. https://doi.org/10.29026/oea.2024.230121