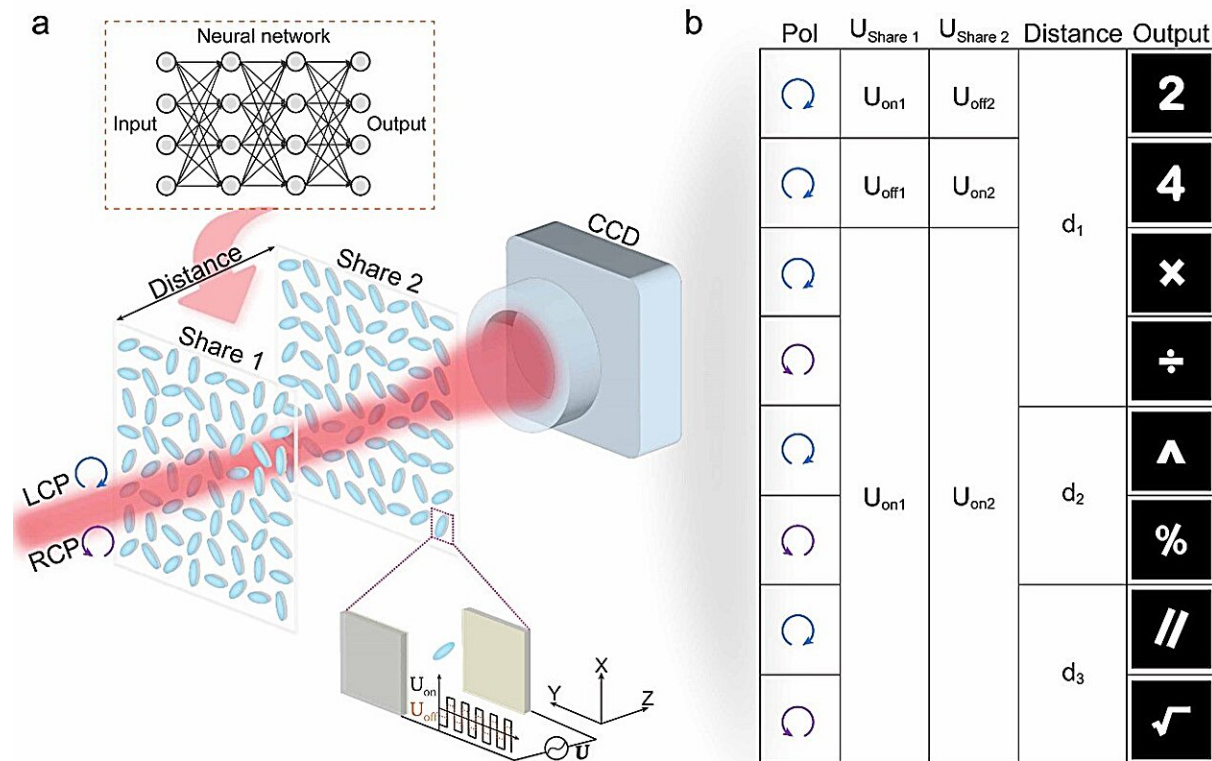# Multi-dimensional multiplexing optical secret-sharing framework with cascaded liquid crystal holograms

February 6 2024

The schematic diagram of multi-dimensional multiplexing optical secret sharing framework with cascaded liquid crystal holograms. Credit: *Opto-Electronic Advances* (2024). DOI: 10.29026/oea.2024.230121

Information security has become particularly crucial under the background of the big data era. Optical secret-sharing schemes encrypt information and physically divide it into different shares. Information can only be decrypted by cascading a sufficient number of shares.

These schemes can be widely applied to information encryption and anti-counterfeiting due to high security and rapid information processing capabilities.

Holography is a significant method for optical encryption, and it can also realize holographic multiplexing by using different physical dimensions of light as independent information channels. The metasurface holographic multiplexing technology meets the urgent needs for miniaturization and integration of optical systems.

However, there are significant challenges in building a cascaded optical secret-sharing platform with dynamic tunability and high diffraction efficiency, limited by precise manufacturing requirements and inherent physical properties of materials.

For the realization of low-cost, convenient, high-efficiency, and high-capacity cascaded optical secret sharing schemes, anisotropic structured liquid crystal optoelectronic materials with high diffraction efficiency and voltage-tunable switch features provide a novel approach.

The authors of an article published in *Opto-Electronic Advances* propose a multi-dimensional multiplexing optical secret-sharing framework with cascaded liquid crystal holograms. In this framework, the polarization state of the incident light and the distance between the liquid crystal holograms are used as the decryption keys of encrypted information.

An error back-propagation neural network with angular spectrum diffraction theory was created, accomplishing the inverse design of

complex multi-constraint and multi-layer cascading problems. The multi-dimensional inputs in the encryption process of the network, such as the polarization state of the incident light, the external voltage applied to the cascaded liquid crystal shares and their distances, significantly enhance the security of the secret information. This allows for the ultra-secure transmission of multiple information channels simultaneously, overcoming the limitations of traditional holographic encryption methods.

First, the secret image is hidden in different shares (individual liquid crystal holograms) and can only be decrypted through cascading the shares. Even if one of the shares is stolen, it is impossible to retrieve the final secret information and only an authentication image will be displayed, greatly enhancing the security of the secret-sharing platform.

Second, the multi-dimensional multiplexing technique increases the complexity of the secret keys, enhancing both information security and capacity. Furthermore, the encryption information channels can be further increased by adding more secret shares and utilizing linear polarization state multiplexing. Interestingly, the flexible electric tuning capability of liquid crystal devices effectively heightens the security of the proposed secret-sharing framework. The externally applied voltage can be independently mapped to different secret shares, setting more stringent conditions for information decryption and significantly reducing the possibility of information leakage.

The multiplexing of eight images by controlling the polarization state of the incident light was experimentally demonstrated, the distance between the shares, and applying different voltage states externally to the liquid crystal layers.

In this scheme, the secret information is decomposed and distributed into two mutually constrained liquid crystal holograms. When these two

liquid crystal holograms are cascaded together, it is only necessary to adjust the external applied voltage (U_{on}, U_{off}) of each liquid crystal share, so that each individual [hologram](link) can reconstruct an authentication image (number 2 or 4) at a specific position.

Furthermore, under high modulation efficiency voltage (U_{on}) for each liquid crystal share, six independent operation images (mathematical symbols) can be decrypted using different secret keys, which include the polarization of the incident light and the distance between the cascaded liquid crystal holograms.

The final encrypted information can be obtained through secondary decoding by performing mathematical operations displayed by different operation images between the authentication images. The mature manufacturing technology of liquid crystal components makes this framework more practical and multifunctional.

With its convenient design, low-cost manufacturing, and ultra-high security, this multi-dimensional multiplexing optical secret sharing scheme has great potential in applications of ultra-high capacity information storage, dynamic holographic display, and multifunctional optical information processing.