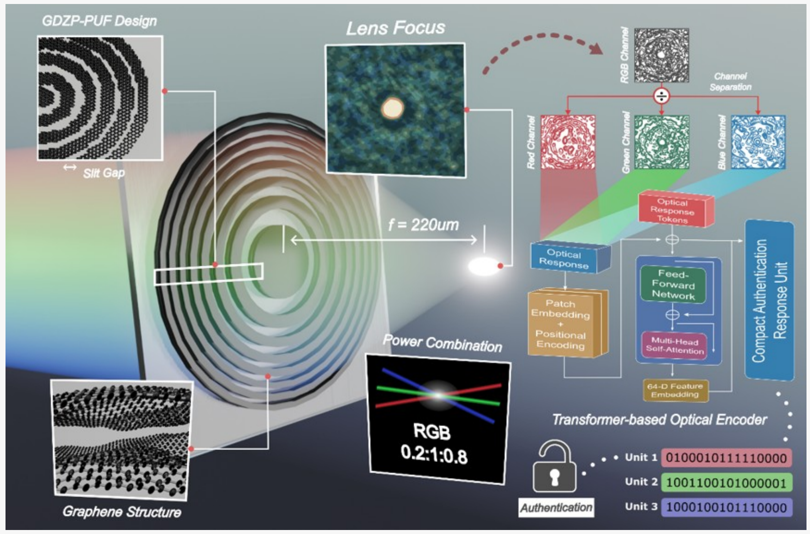
New Graphene Diffraction Technology Enables Spectrally Programmable Optical Authentication

Multi-color light challenges and AI analysis transform graphene diffraction patterns into compact binary security responses

CHENGDU, SICHUAN, CHINA, September 14, 2026 /EINPresswire.com/ -- As electronic devices become increasingly connected, hardware authentication must move beyond stored digital secrets that can be copied or emulated. Researchers developed a graphene-based optical physical unclonable function that uses different combinations of red, green, and blue light as programmable challenges. A transformer-based model converts the resulting diffraction patterns into compact binary response units, demonstrating a route toward spectrally programmable optical authentication for future hardware security in connected devices and edge systems.



Conceptual overview of the GDZP-ViT optical PUF system

Group photo of the research team at Yonsei University

Modern electronic systems depend on reliable ways to confirm that a device is genuine. Conventional security methods often rely on stored digital keys or software-based credentials. These approaches are powerful, but they can become vulnerable if the stored information is copied, leaked, or reproduced by an attacker. Physical unclonable functions, or PUFs, offer a different strategy: instead of storing a secret, they use tiny and unavoidable manufacturing variations in a physical object to generate a unique response.

Optical PUFs use light to read these physical variations. When light interacts with a complex material or optical structure, the resulting pattern can be extremely difficult to reproduce exactly. However, many optical PUFs produce analog images or speckle patterns that are not straightforward to convert into short, stable, and verifiable digital responses. This has limited their practical use in authentication systems.

The research team addressed this challenge using graphene diffractive zone plates. A diffractive zone plate is an ultrathin optical element that focuses light through interference rather than through the curved surfaces used in conventional lenses. Because diffraction depends strongly on wavelength, the same graphene zone plate responds differently when illuminated with different combinations of red, green, and blue light. The study was made available online on July 22, 2026, in the journal Opto-Electronic Advances.

In the proposed system, the color composition of the incident light acts as an optical challenge. The graphene diffractive zone plate then produces a wavelength-dependent focal and interference pattern, which serves as the physical response. These patterns contain information from both the designed Fresnel-zone geometry and small fabrication-induced variations in the multilayer graphene structure.

To make the optical response usable for authentication, the researchers used a vision transformer model to analyze the captured diffraction images. The model converts each high-dimensional RGB diffraction pattern into a compact numerical representation. Stable components of this representation are then selected and converted into binary response units that can be compared using standard authentication metrics.

This approach turns a complex optical image into a repeatable digital response while preserving the physical uniqueness and challenge dependence of the optical system. Rather than relying on a single fixed image, the platform can generate different responses under different spectral challenges. In this way, the work demonstrates a spectrally programmable diffractive optical PUF that bridges physical optics, graphene nanomaterials, and artificial intelligence-based readout.

This study contributes to the broader effort to build security functions directly into physical hardware. As artificial intelligence, edge computing, and connected devices become more widespread, authentication cannot rely only on software credentials or stored digital secrets. Hardware-level identifiers that are difficult to copy or predict can provide an additional layer of trust for future electronic systems.

The proposed platform is important because it combines two properties that are rarely achieved together in optical PUFs. First, the graphene diffractive zone plate provides a physically complex optical response shaped by fabrication-induced local heterogeneity. Second, the response can be reconfigured by changing the RGB spectral challenge without mechanically moving the device or scanning the beam position. This enables a fixed optical geometry to support multiple challenge-response states.

Another significance of the work lies in the conversion of analog optical patterns into compact binary response units. Optical systems naturally generate rich images, but practical authentication protocols require stable digital outputs that can be compared, stored, and verified. By using a vision transformer to extract global diffraction features and selecting reliable embedding dimensions for binarization, the team demonstrates a pathway from optical complexity to authentication-oriented digital responses.

The approach may be useful for future optical security tags, anti-counterfeiting technologies, chip or package authentication, and hardware roots of trust. In such applications, the optical structure would act as a physical layer that is difficult to clone, while the spectral challenge sequence would provide a programmable way to interrogate the device.

The work should be understood as a proof-of-concept demonstration rather than a finalized manufacturing platform. The current graphene transfer and focused-ion-beam patterning process was used to accurately define the diffractive structures and validate the principle. Future implementations may explore scalable fabrication routes, integrated optical readers, and chip- or package-level authentication modules.

More broadly, the study shows how nanophotonic hardware and learning-based analysis can work together in security systems. Instead of treating artificial intelligence only as a classifier, the model is used to stabilize and interpret physically meaningful optical responses. This combination may inspire new forms of programmable optical authentication, secure photonic hardware, and adaptive physical security systems.

Reference
Title of original paper: Spectrally encoded diffractive optical unclonable functions using graphene zone plates
Journal: Opto-Electronic Advances
DOI: https://doi.org/10.29026/oea.2026.260076

About Prof. Seong Chan Jun’s group from Yonsei University
Prof. Seong Chan Jun's group focuses on the integration of nanomaterials, optics, and artificial intelligence to develop functional photonic systems for sensing, diagnostics, and security.

The group has extensive experience in graphene-based optical devices, diffractive optics, optical molecular sensing, and machine-learning-assisted analysis of complex optical responses. In this work, these research directions were extended toward optical hardware security by using graphene diffractive zone plates as spectrally programmable physical authentication elements.

The group is exploring applications in non-contact sensing, biomedical diagnostics, optical security systems, and intelligent photonic devices. Their long-term goal is to develop compact optical platforms for complex real-world environments.

Siyi Ma
Email: oej_publishing@ioe.ac.cn Expert Contact Prof. Seong
email us here
