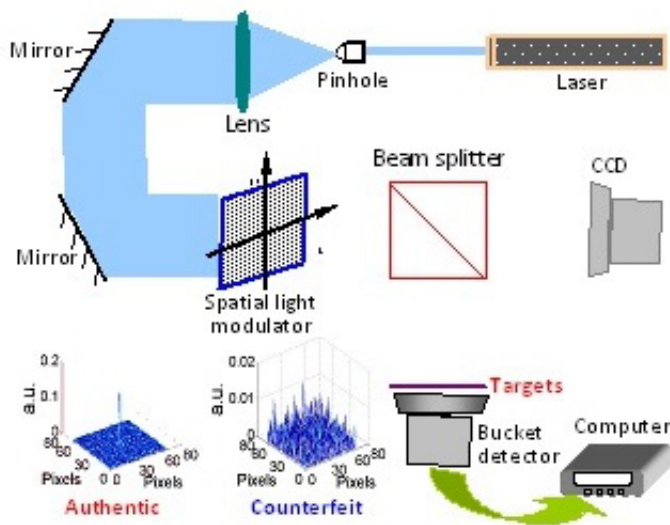


New, enhanced security of data storage and transmission via optical 'marked ghost imaging' technology

June 24 2014



A schematic illustration of marked ghost imaging. Credit: W. Chen and X. Chen/NUS

"Ghost imaging" sounds like the spooky stuff of frivolous fiction, but it's an established technique for reconstructing hi-res images of objects partly obscured by clouds or smoke. Now a group of researchers at the National University of Singapore (NUS) is applying the same idea in reverse to securing stored or shared electronic data.

Described in the journal *Applied Physics Letters*, from AIP Publishing, the work establishes "marked ghost imaging" technology as a new type of multi-layer verification protocol for [data storage](#) or transmission.

By "ghosting up" data, the scientists can hide the contents of electronic communications from hackers, deconstructing it into multiple foggy files that make no sense on their own and can only be reconstructed by someone who has the right decoder key (technically called a "reference intensity sequence").

"The sender can send out a huge number of different reference intensity sequences—only one is authentic, and others are counterfeit—for confusing the attackers," said Wen Chen, an NUS professor who led the work with co-author Xudong Chen.

"This novel method based on ghost imaging can dramatically enhance system security, and it may be straightforward to apply it to other optical security systems," Chen added.

How the Technology Works

Information security has become one of the most important social and academic topics in recent years as massive increases in data storage have coincided with rapidly developing modern technologies for accessing that data virtually anywhere. Imaging technology has attracted more and more attention in computer security circles because of its promise to enhance the security of data storage or transmission, which is what led Chen and colleagues to develop their marked ghost [imaging technology](#) based on traditional optical ghost imaging.

Traditional ghost imaging uses digital cameras to detect light bouncing directly off of an object as well as light that does not directly bounce from the object to the detector. It allows solid images of objects to be

reconstructed by shining light into a beamsplitter and separating it into two correlated beams—one directed at the object and the other, reference arm directed at the camera lens. When these two beams are correlated, they create a silhouette image of the object.

Chen and colleagues report that they can do the same thing either virtually, using software, or physically, by altering the optics of the data transmission. Their technology allows them to create highly-sparse reference intensity patterns that act as security keys and lowly-sparse intensity patterns of the object as ciphertexts, the information being decoded. To decode object data, the reference-arm patterns are then processed to 'rebuild' one new reference intensity sequence. This is crucial because requiring only one rebuilt intensity sequence doesn't increase the system's complexity, while allowing multiple marks (the keys) to be hidden.

Future research includes analysis of the upper limit of keys that can be embedded without increasing the system's complexity and developing greater robustness of the system against attacks.

More information: "Marked ghost imaging" Wen Chen and Xudong Chen. *Applied Physics Letters*, June 24, 2014.

[scitation.aip.org/content/aip/ ... 25/10.1063/1.4879843](https://scitation.aip.org/content/aip/.../25/10.1063/1.4879843)

Provided by American Institute of Physics

Citation: New, enhanced security of data storage and transmission via optical 'marked ghost imaging' technology (2014, June 24) retrieved 19 April 2024 from <https://phys.org/news/2014-06-storage-transmission-optical-ghost-imaging.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private

study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.