Optical holography makes information simpler to secure, more difficult to decrypt

February 19 2007

Retrieved image in the optical holography method, reconstructed from interferograms with the exact phase keys. Credit: Xiaogang Wang, et al.

As business done over the Internet is becoming almost conventional these days—more banks becoming virtual, more companies going global—information security is something most people take for granted on a daily basis. However, with computer crime at an all-time high in the past few months, scientists working on the latest security technologies have a job where many consumers' trust is at stake.

The methods behind various encryption techniques have roots in the manipulations of basic components of science. For digital holography, for example, the focus is light, and how scientists can slightly shift the phases of light waves in order to make information disappear completely—and then bring the data back by knowing the correct "keys," the phase codes and phase masks.

Scientists Xiaogang Wang, a physicist from Zhejiang Forestry University, and Yixiang Chen, an electrical engineer from the Zhejiang University of Media and Communications, have recently designed a new type of digital holography for information security that both simplifies the security process and increases the data transmission efficiency.

"We obtain two interferograms by using two-step phase shifting digital holography, and then encrypt them into phase codes in fractional Fourier domain which can be transmitted in the conventional communication channel," the scientists report in their paper in *Journal of Optics A: Pure and Applied Optics*.

While many ideas for securing information become difficult to implement in the real world, Wang and Chen designed their method to overcome many of the practical challenges faced by encryption techniques in general. Building on a method using phase-shifting interferometry, which measures the deviations of optical surfaces (Kim, 2004), Wang and Chen's method is based on a two-step process that doesn't require expensive optical hardware.

"Actually, it is very difficult for most [encryption methods] to be applied in the real world because of the complexity and location precision of their optical hardware, the lack of compact and low-cost optoelectronics devices and the difficulty in optical alignment," the scientists explain. "Digital optics techniques are reasonable solutions to those problems with the rapid development of computer and internet techniques."

To encrypt an image, the scientists first made 3D holograms of an object, which is done by shining a light beam on the object and comparing the returned light with a reference light beam. This form of information, called an "interferogram," then gets digitally encrypted into a phase code based on the frequencies of different wave phases (the fractional Fourier domain), which is done by a computer-generated random phase mask.

The mask divides a single incoming beam into two beams, creating an interference pattern where the beams overlap. In Wang and Chen's method, two interferograms are digitally encrypted as two phase masks, which can transmit data but require the correct keys for decryption.

A receiver can digitally decrypt the data using two retrieval keys: the phase codes (containing information on wave frequency) and phase masks. Along with these, the scientists also used phase shifts as an additional retrieval key, although this key was less sensitive to accuracy. After performing calculations with these keys, a receiver can reconstruct the data. Without the exact keys, however, attempts at reconstruction result in white noise.

"With this technique, the efficiency of data transmission is considerably raised because there is no need for complex and expensive optical hardware and no difficulty in optical alignment in the encryption and decryption processes," the scientists explain.

Citation: Wang, Xiaogang, and Chen, Yixiang. "Securing information using digital optics." *J. Opt. A: Pure Appl. Opt.* 9 (2007) 152-155.