Enhanced holographic encryption using a phase-modulated plane wave

Joewono Widjaja

Illuminating a random phase mask inserted in front of an input image with a uniform plane wave improves the quality of decrypted images without degrading security.

Holography—using laser light to record and reconstruct 3D images—is also a very useful method for transmitting images securely. A hologram of an object image is essentially an encryption of an object wave (i.e., a light wave diffracted from the object image) using a reference, or uniform, wave as a key. Because holography preserves the state of the object wave as it passes a certain point, referred to as the wave’s phase, security can be even further improved by encoding this information as well. Almost all credit cards and passports contain embossed holograms for protecting against counterfeit. But the object image can easily be reconstructed by illuminating the hologram using the same reference wave. Hence, the security of the holographic encryption is poor. Security can be improved by randomizing the phase of the object wave using a phase mask (i.e., a ground glass screen) placed behind the object image.

Figure 1 shows a Mach-Zehnder interferometer (a device for implementing holographic encryption) in which one arm carries an object wave of the input image, $f$, while the other carries a reference wave. To encode random phase information, the object wave is first propagated through free space of distance $z_1$. Following modulation by a random phase mask, $P$, the randomized object wave propagates through the second free space of distance $z_2 - z_1$ toward a recording plane. Thus, this process involves convolutions (encodings) of the object wave with two impulse responses (encoders determined by the propagation distance). An interference pattern of the resultant wave distribution and the reference wave whose phase is shifted by a phase retarder is recorded by a CCD sensor, a process known as phase-shifting holography. To decrypt the image, the wave distribution corresponding to the object wave at the recording plane is reconstructed from the holograms, again, using the phase-shifting technique. The real image, which is the conjugate (reverse) of the object wave, is retrieved by performing a reverse propagation of the field distribution from the recording plane back to the input plane.

However, this method has several drawbacks related to the limited resolution of the CCD sensor. The first is that, due to an aliasing problem, the free-space impulse response of the encryption differs from that of the reversed propagation in the decryption. When the two different impulse responses are convolved, the output is an undesired array of sinc, i.e., a bipolar pulse. The second problem is that the quality of the decrypted images

Continued on next page
depends on separation of the input and the mask. Because the sinc function has a bipolar amplitude, multiple random patterns are produced that distort the reconstructed object image. This distortion is greatest when the mask is located in the middle of the recording distance, because the amplitude of the resultant convolution is maximum.

The first drawback can be addressed by subtracting a reconstructed wavefront obtained from phase-shifting holograms of the same mask recorded without the input image from the decrypted image.\(^1\) To obviate the second problem, we have been working on a new method of holographic encryption by swapping the positions of the mask and the input image.\(^2\) We use the same phase-shifting holography for the encryption-decryption process. The separation distance between the mask and the input image becomes \(z_1\), while the input and the recording plane is \(z_2\).

In our new approach, the field distribution at the recording plane is given by \(\{(P \otimes h_{z_1}) f \} \otimes h_{z_2}\), where \(\otimes\) and \(h_z\) are the convolution operation and the free-space impulse response with distance \(z\), respectively. After this field distribution is reconstructed from the holograms, its conjugate is propagated from the recording plane back to the input plane, yielding \((P^* \otimes h_{z_1}^*) f^*\). The conjugate of the object wave \(f^*\) is separated from the convolution by taking the logarithm of its absolute value \(\log |(P^* \otimes h_{z_1}^*) f^*| = \log |(P^* \otimes h_{z_1}^*)| + \log |f^*|\). The first term on the right-hand side represents noise that corresponds to the diffracted field of the mask, while the second term is associated with the input image. Since both the mask and the impulse response are known, the noise can be numerically eliminated. Consequently, the aliasing error due to the undersampled impulse response disappears completely. Finally, we obtain the image information by solving for \(|f^*|\).

We verified the feasibility of our new method by encrypting fingerprint patterns. Figure 2 plots the peak signal-to-noise ratio (PSNR) of the decrypted fingerprints as a function of \(z_1\). The PSNRs we obtained using the conventional and the new methods are represented by circle and cross symbols, respectively. The quality of the images decrypted using our approach is generally higher and more stable. The fluctuation in PSNR caused by the overlapping of multiple fingerprints and the dip at distance \(2z_1 = z_2\) does not occur. The results show that high-quality image encryption can be implemented without having to locate a suitable mask position. As a next step, we plan to apply the method to encrypting biometric information.

**Author Information**

Joewono Widjaja
Suranaree University of Technology
Nakhon Ratchasima, Thailand

Joewono Widjaja is currently a professor at the Institute of Science, Suranaree University of Technology. In 2008 he received the International Commission for Optics’ Galileo Galilei Award. His research focuses on optical information processing.

**References**