Encryption based on CGH decoding and XOR operation

Tien Viet Vu [a], Nguyen Noi Bai [a], Nam Kim [a], Seok-Hee Jeon [b], and Sangkeun Gil [c]

[a]Department of Information and Communication Engineering, Chungbuk National University

[b]Department of Electronic Engineering, Incheon University

[c]Department of Electronic Engineering, Suwon University

There has been considerable effort to develop optical encryption schemes: Javidi and co-workers [1] have been responsible for proposing the use of phase masks to scramble and encrypt amplitude information. More recently, this system architecture was modified by the replacement of the amplitude information at the input with phase-encoded information.[2]

The problem with these systems is that they use information encoded in both amplitude and phase regimes, hence often requiring the fabrication of complex optical masks. Mogensen and Gluckstad [3] proposed an alternative approach based on the direct mapping of an encrypted phase mask and a decrypting phase key, resulting in the decryption of information completely within a phase-only domain. However, their system uses a phase-contrast filter with an 4-f setup to convert decrypted phase information into amplitude image which can be captured by intensity-sensitive devices. In this paper we propose an alternative decryption scheme which is simpler and is more easily realized than that of Mogensen et al.

The schematic diagram of the binary phase-only decryption and the phase-contrast visualization proposed by Mogensen et al. is shown in Fig. 1. A plane-polarized wave front illuminates an encrypted mask, which consists of a random array of binary phase-shifting pixels with relative phase shifts of 0 and π. The binary information was electronically scrambled with a random binary pattern, and then this scrambled information was used to generate the encrypted mask. The decrypting key reverses the scrambling operation in the optical domain and results in the decrypted phase-only information. The role of the phase-contrast filter and the imaging 4f setup is to generate an intensity pattern at the output that corresponding to the decrypted phase information encoded in the wave front.

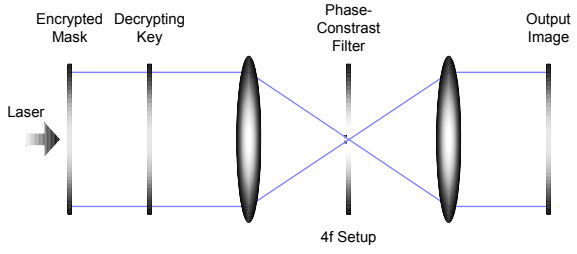

Figure 1. Generic system architecture for the decryption operation and phase-contrast filter.

In our approach, the encrypted mask was produced as follows. First we generate a CGH of the input image needed to be encrypted. The CGH has uniform amplitude and phase elements with relative phase shifts of 0 and π. We use an optimization algorithm such as stimulated annealing to generate a CGH which properly encoded the original image in Fourier domain. Second, the CGH was electronically scrambled with a random phase-only pattern. Finally, the scrambled information was fabricated to produce the encrypted mask. The result of each step is demonstrated in Fig. 2.

Figure 2. Production of encrypted mask. (a) original amplitude image, (b) CGH, (c) encrypted mask.

Our decryption scheme is shown in Fig. 3. The decrypting key reverses the scrambling operation in the optical domain and results in the decrypted phase-only information. We Fourier transform this information by a Fourier lens to produce the decrypted amplitude image in the back focal plane.

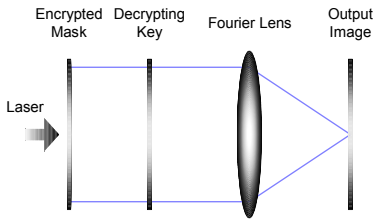

Figure 3. Decryption diagram with Fourier lens.

Acknowledgement

This research was supported by the Ministry of Information & Communications, Korea, under the information Technology Research Center (ITRC) Support Program. and by the Regional Research Centers Program of the Ministry of Education & Human Resources Development in Korea

References

[1] P. Refregier and B. Javidi, " Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett., vol. 20, pp. 767-769, 1995.

[2] N. Towghi, B. Javidi, and Z. Luo, " Fully phase encrypted image processor," JOSA, vol. 16, pp. 1915-1927, 1999.

[3] P. C. Mogensen and J. Gluckstad, " Phase-only optical encryption," Opt. Lett., vol. 25, pp. 566-568, 2000.