OPTICAL PROCESSING SYSTEMS FOR ENCRYPTION, SECURITY VERIFICATION, AND ANTICOUNTERFEITING

Bahram Javidi

University of Connecticut, U-157
Electrical and Systems Engineering Department
260 Glenbrook Road
Storrs, Connecticut 06269-2157
Tel. 203-486-2867 Fax 203-486-1273 email: bahram@eng2.uconn.edu

The recent development of commercially available, low-cost optoelectronic devices, components, and systems and their increased technical performance suggest that optical processing systems and devices have significant potential for encryption, security, verification, and anticounterfeiting applications.These systems can combat fraud which is a serious problem facing many banks, businesses, and consumers. Counterfeit parts such as computer chips, machine tools, etc. are arriving on our shores in great numbers. With the rapid advances in computers, CCD technology, image processing hardware and software, printers, scanners, and copiers, it is simple to reproduce pictures, logos, symbols, money bills, or patterns. Presently, credit cards and passports use holograms for security which are inspected by human eye and can be easily reproduced.

We present a number of new all optical encoding methods that can perform high speed encryption of high volume of data such as images in parallel into complex phase/ amplitude patterns .[1] These techniques can be used for encryption, anti-counterfeiting, security verification of credit cards, passports, and other IDs so that they cannot easily be reproduced. Complex phase/amplitude patterns that cannot be seen and cannot be copied by an intensity sensitive detector such as a CCD camera are employed to encode the data.

The decryption/reconstruction can be performed in parallel and is both fault tolerant and robust to noise. These techniques allow encoding of information in a way which is difficult to decode if one does not know a ``key'' but very easy if one knows that key.

One method is to permanently and irretrievably bond a 2-D phase mask to a primary identification amplitude pattern such as a fingerprint, a picture of a face, or a signature. Both the phase mask and the primary pattern are identifiable in an optical processor or correlator.[2] The phase portion of the pattern consists of a 2-D phase mask with large dimensions to make it difficult to determine the contents of the mask. With the high resolution of the commercially available optical films and materials, M(x,y) can be of the order of a million pixels, and yet the mask size will be only a few millimeter square.

The verification system that reads the card could be one of several coherent optical

processors architectures. This system provides the flexibility of allowing a "code of the day", or whatever time interval is appropriate, by inserting a card containing another authorized reference phase mask in the input. For even more security, the primary pattern could itself be phase encoded. This would have the effect that the combined pattern would be completely invisible to the eye or to any other detector using conventional light sources. This technique would have an additional security value, in that anyone wanting to counterfeit the card, would not even be able to easily determine what type of a primary pattern they would have to produce on the card.

1. P. Refregier and B. Javidi, Optical Image Encryption using Input and Fourier Plane Random Phase Encoding," Journal of Optics Letters, vol. 20, pp. 767-769, April 1, 1995.

2. B. Javidi, and J. L. Horner, "Optical Pattern Recognition for Validation and Security Verification," Journal of Optical Engineering, vol. 33, no. 6, June 1994.