NAG10-191

FINAL REPORT

Optical Verification Laboratory Demonstration System For High-Security Identification Cards

Submitted to:
NASA

Care of:
Ms. Lynn E. Rafford
Grant Officer
OP-ESO
NASA
KSC, FL 32899

Submitted by:

The University of Connecticut

Principal Investigator:
Professor Bahram Javidi
University of Connecticut
Department of Electrical Engineering, U-157
260 Glenbrook Rd.
Storrs, Connecticut 06269-2157
Tel. (860) 486-2867; Fax (860) 486-2447
e-mail: bahram@engr.uconn.edu

NASA FINAL REPORT

Optical Verification Laboratory Demonstration System For High-Security Identification Cards

by

Bahram Javidi

Document fraud including unauthorized duplication of identification cards and credit cards is a serious problem facing the government, banks, businesses, and consumers. In addition, counterfeit products such as computer chips, and compact discs, 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 becoming increasingly easy to reproduce pictures, logos, symbols, paper currency, or patterns. These problems have stimulated an interest in research, development and publications in security technology. Some ID cards, credit cards and passports currently use holograms as a security measure to thwart copying. The holograms are inspected by the human eye. In theory, the hologram cannot be reproduced by an unauthorized person using commercially-available optical components; in practice, however, technology has advanced to the point where the holographic image can be acquired from a credit card—photographed or captured with by a CCD camera—and a new hologram synthesized using commercially- available optical components or hologram-producing equipment. Therefore, a pattern that can be read by a conventional light source and a CCD camera can be reproduced.

An optical security and anti-copying device that provides significant security improvements over existing security technology was demonstrated. The system can be applied for security verification of credit cards, passports, and other IDs so that they cannot easily be reproduced. We have used a new scheme of complex phase/amplitude patterns that cannot be seen and cannot be copied by an intensity-sensitive detector such as a CCD camera. A random phase mask is bonded to a primary identification pattern which could also be phase encoded. The pattern could be a fingerprint, a picture of a face, or a signature. The proposed optical processing device is designed to identify both the random phase mask and the primary pattern [1-3]. We have demonstrated experimentally an optical processor for security verification of objects, products, and persons. This demonstration is very important to encourage industries to consider the proposed system for research and development.

The optical security and anti-counterfeiting device can be manufactured into a compact, low cost, reliable security system. The system can be used to secure identification cards, and access to sensitive sites. In addition, it can secure credit and ATM cards, thereby significantly reducing their fraudulent use and sparing the banking industry potentially billions of dollars. The system could be applied to U.S. and state government documents so that they cannot be easily forged. A conservative list might include passports, driver's licenses, social security cards, medical insurance ID's, and ID cards for restricted access facilities. The system would significantly reduce fraudulent claims to social service agencies by preventing forgery of government identification papers and cards, thereby saving the government billions of dollars.

The basic concept behind the security system is to permanently and irretrievably bond a phase mask to a primary identification pattern such as a fingerprint, a picture of a face, or a signature so that they cannot easily be reproduced or copied by an intensity-sensitive detector such as a CCD camera [1]. Both the random phase mask and the primary pattern are identifiable in an optical correlator [1-3]. An object or primary pattern whose authenticity is to be verified, consisting of an amplitude or phase primary pattern to which a random phase mask has been bonded, is placed in the input plane of the correlator. Coherent light illuminates the complex mask, extracting the signal. The correlation between the phase-encoded signal on the card and the reference phase mask is performed. The output correlation between the input mask pattern and the reference mask function is detected by the detector. The intensity of the correlation determines the degree of similarity between the input mask and the mask stored in the filter to verify the authenticity of the input phase mask on the card. If the reference mask matches or has a high degree of correlation with the input phase mask, a high intensity spot will be detected, and if the intensity exceeds a predetermined level, an authenticity verification signal is produced. If the input phase mask is a counterfeit, the intensity of the correlation spot will be below the threshold established at the output. The processor used to verify the input mask can also be used to verify the primary pattern such as a fingerprint or a picture.

A nonlinear joint transform correlator (JTC) [3] was used for verifying the phase codes. A low cost compact architecture based on the nonlinear JTC was designed to implement the optical system. In choosing the optoelectronic correlator, attention was given to performance in terms of discrimination and noise robustness, cost, compactness, reliability, and relative ease of updating the codes. Experiments were

performed to illustrate the system performance in terms of noise, discrimination, and system robustness. The JTC architecture [3] is attractive for implementing this optical validation system because the alignment of the filter in the Fourier plane of the frequency plane correlator can be critical. The JTC architecture makes it very easy to rapidly update or change the master code, or to write an individual code quickly, or to display the primary pattern. The joint power spectrum is nonlinearly transformed with respect to a threshold function. The threshold function can be determined to optimize the performance of the nonlinear JTC with respect to a given performance criterion such as maximizing the peak intensity of the first order correlation term, or reducing the on-axis autocorrelation terms to produce a higher correlation peak to sidelobe ratio. For JTCs, the reference function is displayed alongside the input scene in the input plane and can be easily updated in real-time using optical or optoelectronic input-output devices called spatial light modulators. As a result, the need for filter computation is eliminated and pattern recognition can be performed in parallel and with high speed using all optical techniques.

References

1. Javidi and J. Horner, "Optical Pattern Recognition System for Security Verification," Optical Engineering, vol 33, no. 6, June 1994.
2. B. Javidi, "Encrypting Information with Optical Technologies," Physics Today, vol. 50, no. 3, March 1997.
3. Javidi, "Nonlinear Joint Transform Correlators," chapter of the book, Real-time Optical Information Processing, edited by B. Javidi and J. L. Horner, Academic Press, 1994.