Securing Information with Optical Technologies

The next generation of data security systems may thwart counterfeiters and eavesdroppers by employing new systems and devices based on optical information processing.

Bahram Javidi

Data security has become part of our everyday lives. For even the most banal transactions, a secure piece of identification—a passport, password, bank card, credit card, personal identification number or driver's permit—is often required. As those proofs of identity have become increasingly necessary in our complex world, they have also increased the opportunities for deception. Each year, US business spends many billions of dollars on information fraud, including forged credit cards. Many of those losses are passed onto the consumer. Each year, tens of millions of dollars in counterfeit US notes are seized worldwide. And counterfeit manufactured goods, such as computer chips and machine tools, are arriving on our shores in greater numbers than ever.

Although the public is largely unaware of it, an "arms race" is going on between the developers of data security systems and counterfeiters. The race is escalating as the technology for perpetrating information fraud becomes increasingly common. Because of rapid technological advances in computers, charge-coupled devices (CCDs), printers, scanners, copiers and image-processing hardware and software, it has become possible to produce authentic-looking counterfeits of portraits, logos, symbols, money bills and other complex patterns.

Even the anticounterfeiting techniques that represent a high state of the art have become more vulnerable. For nearly a decade, the holograms on credit cards and passports have been difficult for counterfeiters to reproduce. These days, however, a CCD camera can be used to capture a holographic pattern, and a skilled holographer can make a duplicate that could pass casual inspection by the average person.

Electronic communications and data stored on computers are under a similar threat. Conversations on line and cellular telephones can be intercepted or tapped, and unsecured channels of communication on the Internet are easy to breach. As advanced high-speed computers, able to reduce the time required to decipher an encoded message, become more available, even highly sophisticated encryption techniques can become increasingly vulnerable.

But the lives of counterfeiters and eavesdroppers can be made more difficult, and many technologies are being explored and developed to that end. As one example, for the past few years, my colleagues and I have explored various ways of using commercially available optical systems, devices and materials to reduce problems in data security and encryption.[1–5] (See figure 1.) I believe that the techniques of optical information processing presented here could play an important part in stemming the tide of information fraud. For now, however, the jury is still out.

Bahram Javidi *(bahram@eng2.uconn.edu) is a professor of electrical and systems engineering at the University of Connecticut in Storrs.*

Advantages of optical techniques

There are good reasons to consider using the new optical information processing techniques for protecting data and biometrics (fingerprints and facial features) against tampering.[1–9] Unlike most computers, optical devices have an inherent capability for parallel processing; every pixel of a two-dimensional image can be both relayed and processed at the same time.[10–12] Electronic computers, though, are mostly limited to serial processing; the ones and zeros denoting the presence or absence of a pixel have to be processed one bit at a time. So, when there is a large volume of information to be processed, parallel processing offers enormous advantages. Custom-made optical hardware available today can process a two-dimensional array of data (such as an image on a film transparency), consisting of hundreds of thousands of pixels, at several hundred frames per second (where each array constitutes a frame). That rate is at least an order of magnitude higher than that of electronic counterparts.

Besides their rapid transmission of information, optical processors offer certain other advantages when it comes to security.[1–5] Information can be hidden in any of several dimensions—such as the phase, wavelength, spatial frequency or polarization of the light. An intensity-sensitive device such as a CCD camera cannot copy all of those dimensions (phase, for example). It is possible to tuck away an optically based message in only one small section of a two-dimensional array, a strategem that forces unauthorized users to find the message's position before they can begin to decode it. Further, an 8-bit optical system can give each pixel gray-scale qualities with (for example) as many as 256 discrete shades, rather than merely the ones and zeros encoded in an electronic security processor. Finally, before an unauthorized user can even begin the laborious process of decoding an image, he has to gain access to the sophisticated and expensive optoelectronic devices and systems he needs to process the information. Taken together, then, all of these properties may substantially increase the number of mathematical possibilities the would-be code breaker must consider when

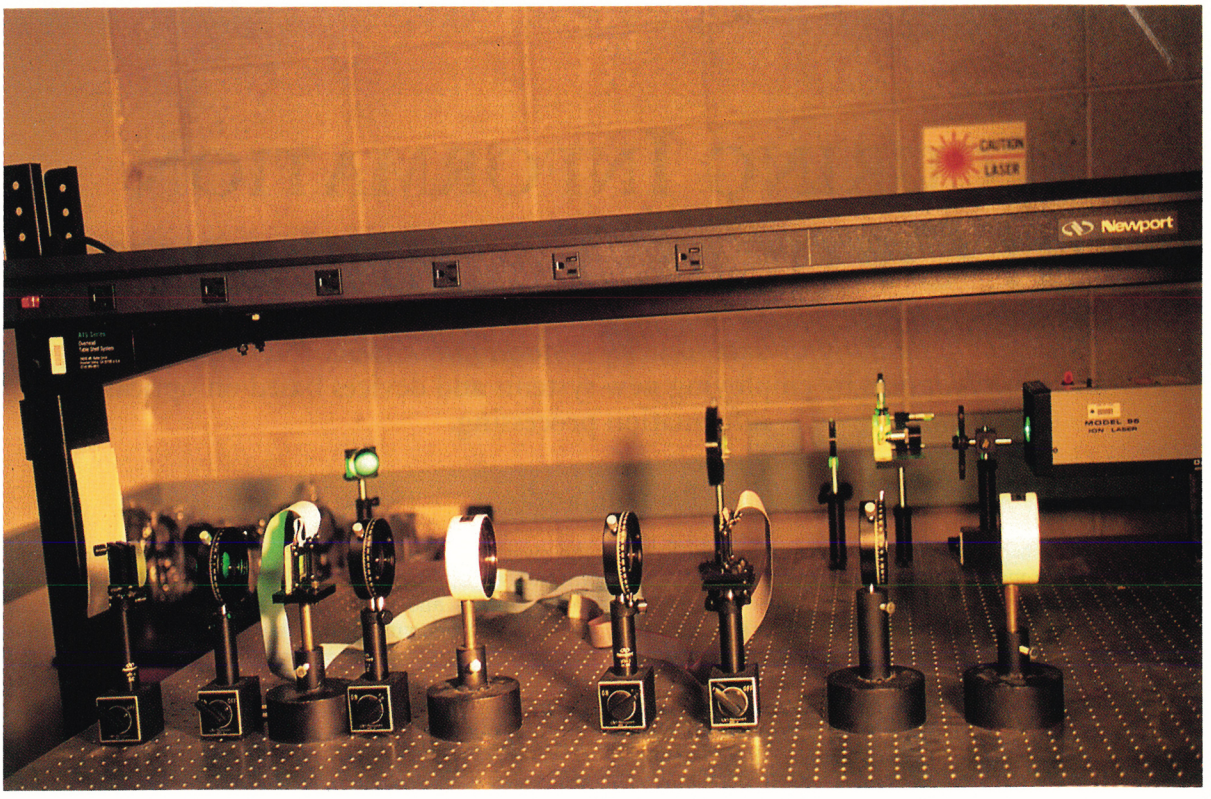

FIGURE 1. OPTICAL SECURITY SYSTEMS can be constructed in the laboratory from commercially available components, such as lasers, mirrors, lenses, detectors and so on. The system shown here was designed for encrypting and decrypting data.

faced with these new optical encryption techniques.

Consider a typical optical system for processing information. It will consist of a light source, a data (or input) plane, lenses, mirrors, beam splitters, detectors, display devices and (depending on its use) perhaps other, more sophisticated optical components, such as spatial light modulators (see the box on page 30).[10–12] The components can be arranged in various configurations to suit the type of data processing desired. The following scenario describes some of the basic processes in an optical system.

Information from a two-dimensional image (say, a picture of a face on a film transparency) is illuminated by a coherent light source, such as an expanded laser beam. After passing through the film, the light passes through a converging lens that introduces a delay, or phase shift, to the incident wavefront by an amount proportional to the thickness of the lens, the index of refraction of the lens and the wavelength of the illuminating light. The light is distributed at the back focal plane of the lens according to the spatial frequencies that were present in the original image. Low-frequency components of the image (in our example, the larger parts of the face, such as the forehead) pass through the lens on axis and so lie near the center of the back focal plane. The high-frequency components (the smaller parts of the image, such as the eyebrows and the lips) fall near the periphery of the back focal plane. The distribution pattern is comparable to far-field (or Fraunhofer) diffraction, in which the far-field image is a superposition of the far-field light patterns generated by the pixels in the input image. More important, the spatial distribution of the frequency components in the back focal plane can be described mathematically as the Fourier transform of the input image. Thus, the back focal plane is also called the Fourier plane (see figure 2). If we place yet another lens behind the Fourier plane of the first lens, the distribution of light at the back focal plane of the second lens is the double Fourier transform of the image in the input plane.

The Fourier transform capability of a converging lens is a crucial property of optical information processors because it allows further manipulation of the optical data in the spatial frequency domain. For example, we might introduce a spatial filter, such as an opaque spot, into the Fourier plane. When placed in the center of the Fourier plane, such a spot would block the low spatial frequencies of the input image, while permitting high spatial frequencies (the fine details) to continue through the system. This filter would generate a high-pass filtered version of the input image.

More sophisticated types of image processing can be achieved by using more complex spatial filters in the Fourier plane. Consider an input image $g(x,y)$ and a filter $h(x,y)$, where the x-y plane represents the input plane. A Fourier transform of the filter $h(x,y)$ produces the complex spatial filter $H(\alpha,\beta)$, where the α-β plane is the Fourier plane. If we insert this complex spatial filter into the Fourier plane and place a second converging lens behind it, the light pattern in the back focal plane of the second lens will be equivalent to the input image $g(x,y)$ filtered by $h(x,y)$—or the convolution of the input image $g(x,y)$ with the filter $h(x,y)$.[10,11]

Introducing task-specific spatial filters into the Fourier plane enables us to undertake several signal processing operations, including pattern recognition, image encoding and image manipulation. The pattern-recognition capability becomes important if we want to compare an authentic image (which can be stored within the

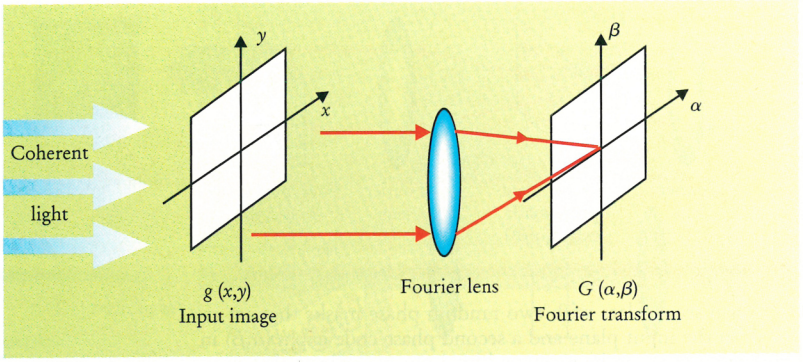

FIGURE 2. FOURIER TRANSFORMATION of an input image by a converging lens is a fundamental principle of optical processing. Here, a coherent light source (such as a laser beam) illuminates an image $g(x,y)$ in the data plane. The light distribution on the back focal plane of the lens is a Fourier transform $G(\alpha,\beta)$ that represents the spatial frequencies of the input image. A spatial filter placed in this Fourier plane can selectively pass or manipulate the amplitude and phase of the desired spatial frequencies.

optical processor) to an unknown image presented in the input plane: The optical processor must find a degree of similarity between the two objects. In World War II, a similar problem confronted military scientists attempting to extract the radar signals of enemy planes from background noise. The wartime scientists discovered that a specific signal mired in white noise could be detected by using a filter that was merely an inverted version of the signal itself in the time domain.

In the Fourier domain, that "matched filter" is equivalent to the Fourier transform of the original image in which the amplitude of the signal is the same but the phase is reversed.[12–14] If the correct image is presented at the input plane, there will be a total phase cancellation between the input and the matched filter in the Fourier plane. All the values of light that pass through the filter will be detected as positive real numbers, and a CCD or other intensity-detecting device will produce a large, well-defined verification signal. If the input image does not correspond to the matched filter, the differences in the phases will produce some complex values of light, which do not add constructively, and no strong verification signal will be produced.

The same principles are put to use in another method of optical correlation: the nonlinear joint transform correlator. It makes a spatial filter unnecessary and produces much better pattern-recognition performance.[10,12] In this method the images to be correlated are presented together in the input plane, and their combined (or joint) Fourier transform is produced in the focal plane behind the first converging lens. If the joint Fourier transform is recorded on photosensitive film, for example, and a second Fourier transform is taken, the two objects can be correlated in the second Fourier plane. The main advantage of the joint transform correlator is that both the unknown input image and the reference image are Fourier transformed simultaneously, so that the interference between the transforms is achieved in a single step. As a result, the reference and input images can be updated easily on a display device, and the correlation between them can be obtained in real time.

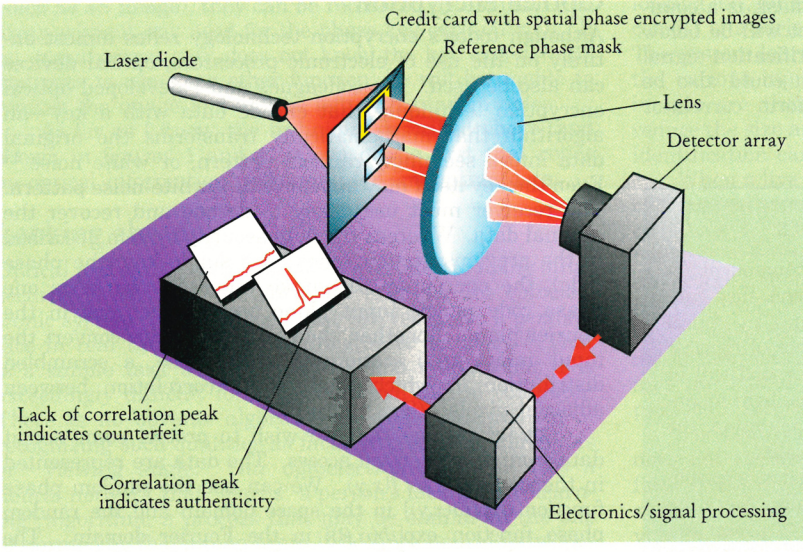

FIGURE 3. SPATIAL PHASE MASKS modify the phase of incident waveforms from a coherent light source. On a credit card, the phase mask would cover information that identified the bearer, such as a portrait, fingerprint, signature or account number. The mask is compared to a reference phase mask, which can be bonded to another part of the card. When the two phase masks are presented together in the input plane, a converging lens produces their joint Fourier transform and the similarities between the masks are determined by a nonlinear joint transform correlator. For even greater security, the portrait or fingerprint on the card may itself be phase encoded and compared to a live input image of the cardholder's face or fingerprint.

Phase encoding for security

Consider an optical security technique that would exploit the ability of optical processors to detect the phase of an incident waveform. One approach would be to permanently bond a phase mask to an authentic item, such as a document or article of merchandise. The phase mask could be a sheet of transparent plastic with areas of both high and low optical density (or different indexes of refraction). Since the passage of light is delayed according to the optical density of a material, a coherent light source (such as a laser beam) that illuminates the phase mask would be encoded with a distinct phase pattern. The pattern in the mask, known only to the authorized producer of the item, could not be seen with the naked eye or a microscope—and it could not be copied by photographic film or a CCD camera.[1,4,5] The phase mask might also be bonded to a fingerprint or a portrait, for use on an identification card. Attempts to separate the phase mask from the original image would destroy the mask.

Such a phase mask can be repre-

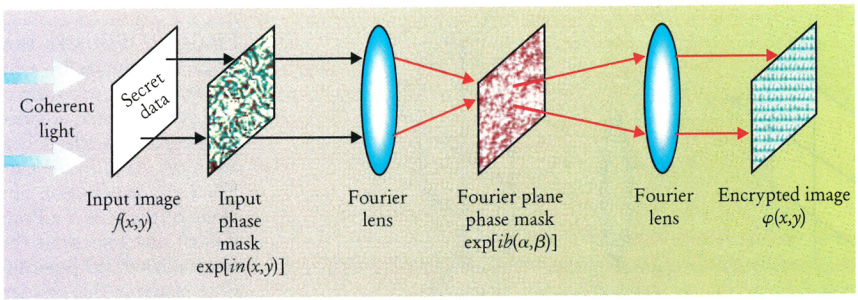

FIGURE 4. OPTICAL ENCRYPTION can secure data with two random phase masks that act as "keys"—one phase code $\exp[in(x,y)]$ in the input plane and a second phase code $\exp[ib(\alpha,\beta)]$ in the Fourier plane. The encrypted data $\varphi(x,y)$ can be recovered by a reverse process that uses the decoding masks $\exp[-in(x,y)]$ and $\exp[-ib(\alpha,\beta)]$.

sented mathematically by the function $\exp[iM(x,y)]$, where $M(x,y)$ is a real function. The high resolution of commercially available optical films and materials currently permits the mask to be only a few millimeters square, yet contain about one million pixels. An image $g(x,y)$, such as a fingerprint on an identification card, with a phase mask bonded to it has a composite input signal:

$$s(x,y) = g(x,y)\exp[iM(x,y)] \qquad (1)$$

The processor has an *a priori* knowledge of the mask $\exp[iM(x,y)]$ in the form of a spatial filter positioned in the Fourier plane of the optical correlator. The correlation between the pattern of the phase mask and the filter can be detected by a CCD image sensor. The intensity of the correlation determines the degree of similarity between the input mask and the mask stored in the filter. If the input phase mask matches the spatial filter, the CCD sensor will detect a high-intensity spot and then produce a verification signal. If the input phase mask is a counterfeit, the intensity of the correlation spot will be below some predetermined threshold and no verification signal will be produced. Such a security system could also be configured with a nonlinear joint transform correlator (figure 3).

Spatial Light Modulators

Spatial light modulators are the principal components in many optical processing systems. In general, they convert an electrical or optical input signal into an optical output. They can be likened to a single piece of reusable photographic film that can be written on (or updated) in real time. One commonly encountered spatial light modulator is the display panel in a liquid crystal television; the panel converts an electrical signal into an image.

An optical input for a spatial light modulator is usually an image whose light amplitude varies spatially. Since the output light distribution (amplitude or spatial phase) is a function of the input amplitude, the device can serve as a spatial filter as well as a display device. When a spatial light modulator is placed at the Fourier plane, the filter functions can be modified in real time by an electrical signal, which redistributes the pattern of pixels on the display. In this way, the spatial frequencies in the original input image can be manipulated as they pass through the spatial light modulator.

The real-time capabilities of spatial light modulators allows users to change the spatial filters at will, to create a security system with "keys" that can be changed at any time.

If there is no original image and only the phase mask $\exp[iM(x,y)]$ is used for verification, $g(x,y)$ will be a constant. If the original image needs to be verified, the processor will have an *a priori* knowledge of the image pattern $g(x,y)$. In such a case, both the phase mask and the original image are verified.

For even more security, the original image could itself be phase encoded,[1,5] generating the composite input image

$$s(x,y) = \exp[ig(x,y)]\exp[iM(x,y)]\,. \qquad (2)$$

The combined pattern would be completely invisible to the eye or to any other detector using conventional light sources. Unauthorized users would have difficulty determining whether the original image was a face, a fingerprint or some other image. Even if an unauthorized user did obtain the original image, he would still have to unscramble the random phase pattern of the mask.

Optical encryption

Although today's encryption technology relies almost entirely on the use of electronic processors, optical devices can also be used. My colleagues and I developed optical encryption techniques that encode data with a key—an algorithm that mathematically transforms the original data into a seemingly random pattern, or white noise.[2,4] Even the key itself may appear to be a white-noise pattern. The receiver must use a key to decode and recover the original data. Whereas the data security system described in the previous section relies on a single key (the phase code), the encryption technique relies on two keys: one phase code in the input plane and another one in the Fourier plane. Together, the two phase codes convert the input image into stationary white noise, a scrambled distribution in which there is no correlation between adjacent pixels. (See figure 4).

Let us assume that we wish to protect some secret data from unauthorized access. The data are represented in the x-y plane as $f(x,y)$. We can use the random phase function $\exp[in(x,y)]$ in the space domain and the random phase function $\exp[ib(\alpha,\beta)]$ in the Fourier domain. The encrypted version of the secret data can be represented as

$$\varphi(x,y) = f(x,y)\exp[in(x,y)] * \mu(x,y) \qquad (3)$$

where $\mu(x,y)$ is the inverse Fourier transform of $\exp[ib(\alpha,\beta)]$, and $*$ denotes the convolution operation.

To decrypt the secret data, the Fourier transform of $\varphi(x,y)$ is multiplied by the decoding mask $\exp[-ib(\alpha,\beta)]$, which serves as the key and cancels the encoding phase mask. The original data can then be recovered in the spatial domain by multiplying by the second phase mask $\exp[-in(x,y)]$. If the original data are real and positive

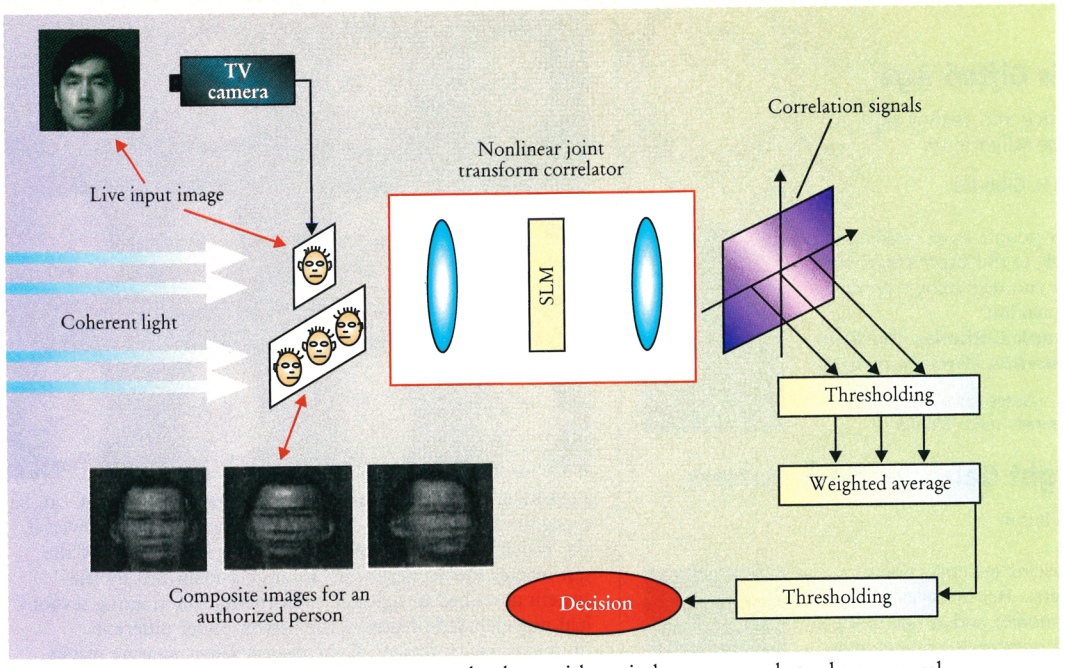

FIGURE 5. REAL-TIME FACIAL RECOGNITION can be done with optical processors that rely on neural network–based learning algorithms. A nonlinear joint transform correlator performs a joint Fourier transform on a live input image and on each of a set of composite images of an authorized individual (which may be stored on an identification card, eliminating the need to store large amounts of data in the processor's memory). The interference pattern produced by the joint Fourier transform is further processed to obtain the degree of correlation between the input image and each composite image. The correlation signals are then thresholded, weighted and summed. If the weighted average of the signals exceeds another predetermined threshold, the system will verify the authenticity of the input image.

(such as an image), they can be recovered by using a CCD array, without any need for the phase key $\exp[-iM(x,y)]$. If an unauthorized user does not know the key $\exp[-ib(\alpha,\beta)]$ and tries to use some other function, he will be unable to recover the image and will be left with random noise.

As far as I know, the technique described above (and shown in figures 1 and 4) is one of the first that relies on optical information processing for encrypting data.

Looking ahead

Optical processing methods can be extended to many other security needs.[3,6,8,9] Recently, for example, an optoelectronic system was developed that can recognize a person's face in real time with a high degree of accuracy.[3,6] That is a simple task for the human visual system, but it is exceedingly difficult for a conventional digital computer. There is no obvious algorithm to solve the problem of recognizing such qualities as facial expressions, hairstyles or viewing angle. Our optoelectronic system uses a neural network that "learns" a person's face with a "learning" algorithm, a process that may be similar to the one performed by the human brain.[15,16] Since neural networks are parallel systems requiring large and dense interconnections between neurons, optical information processors are a natural choice for solving such problems.

A general idea of the optoelectronic process can be obtained from a brief description of the system design.[3] (See figure 5.) The system is trained with a few hundred images, captured by a CCD, of a single individual presenting various facial expressions and profiles. As the system gathers the input images, it adds them together to form various composite images. One composite image might correspond to a series of input images of a person looking left, for example, whereas another composite might consist of a series in which the individual is looking right. The system learns by modifying the composite images as the various input images are presented. The composite images are then stored in the system's memory or (to reduce the size and complexity of the system) on a personal identification card carried by each user.

When a live CCD image of a person's face is presented to a trained system, a nonlinear joint transform correlator compares it to the composite images. The correlation between the input and the composites must exceed a certain threshold before it is relayed. The correlations are then weighted and averaged to produce an output. If the average correlations exceed a predetermined threshold, it indicates a good match between the live CCD image and the stored composite images, and the system will produce a strong verification signal.

The beauty of the technique is that the neural network does not require complete knowledge of the individual's face; it merely relies on the training data. Indeed, the system recognizes individuals wearing glasses and individuals under various illuminations—even when such images were not included in the training (figure 6). Already a robust, compact system can be easily constructed with commercially available optoelectronic devices, without the need for filters or holograms.[3] If implemented, the method would be the first widespread use of neural-networks hardware in a commercial system.

For the near future, it seems likely that optical information technology will be exploited by high-end users, such as governments or industries that need to protect valuable data, before it makes its way into widespread commercial devices. Although several companies are now

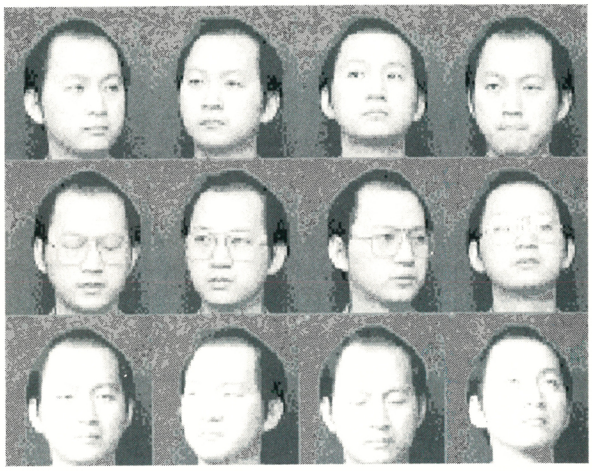

FIGURE 6. VARIOUS IMAGES OF AN INDIVIDUAL'S FACE can be recognized by a neural network–based optical system, even if the system was not trained with the test images. All of the test images shown here were accurately identified by the system described in figure 5, even though the training sessions had not included images of the person under different illuminations or images of the person when wearing glasses.

building prototype devices that can perform some of the processing described above, there is still a need for R&D in this young field before industry will be able to manufacture compact and low-cost optical systems on a large scale.

I hope that this work will stimulate other scientists to consider how developments in their own fields—whether materials science, mathematics, computing or optics—might improve the designs of optical security and encryption systems. Someday, perhaps, optical processing systems will be in common use for data security.

I greatly appreciate the help of Guanshen Zhang, Arnaud Sergent and Jian Li in the preparation of this manuscript. I am also grateful to the USAF Rome Lab at Hanscom Air Force Base and the National Science Foundation for their support.

References

1. B. Javidi, J. L. Horner, Opt. Eng. **33**, 1752 (1994).
2. P. Refregier, B. Javidi, Opt. Lett. **20**, 767 (1995).
3. B. Javidi, J. Li, Q. Tang, Appl. Opt. **34**, 3950 (1995).
4. B. Javidi, G. Zhang, J. Li, Opt. Eng. **35**, 2506 (1996).
5. B. Javidi, A. Sergent, G. Zhang, Opt. Eng. **36**, (1997), in press.
6. H. S. Li, Y. Qiao, D. Psaltis, Appl. Opt. **32**, 5026 (1993).
7. R. L. Van Reneese, ed., *Optical Document Security*, Artech House, Boston (1994).
8. K. H. Fielding, J. L. Horner, C. K. Makekau, Opt. Eng. **30**, 1958 (1991).
9. H. Rajenbach, Proc. SPIE **2237**, 322 (1994).
10. J. W. Goodman, *Introduction to Fourier Optics*, McGraw-Hill, New York (1968).
11. B. E. A. Saleh, M. Teich, *Fundamentals of Photonics*, Wiley, New York (1991).
12. B. Javidi, J. L. Horner, eds., *Real-Time Optical Information Processing*, Academic Press, New York (1994).
13. A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, 3rd ed., McGraw-Hill, New York (1991).
14. R. O. Duda, P. E. Hart, *Pattern Classification and Scene Analysis*, Wiley, New York (1973).
15. R. Lippmann, IEEE-ASSP Magazine, April 1987, p. 4.
16. Y. S. Abu-Mostafa, D. Psaltis, Sci. Am. **256**(3), 88 (1987). ■