Journal of the Optical Society of Korea, Vol. 4, No. 1, March 2000, pp. 19-22

Optical Encryption System using a Computer Generated Hologram

Jong-Yun Kim, Se-Joon Park, and Soo-Joong Kim

Dept. of Electronic Engineering, Kyungpook National University, Taegu 702-701, KOREA
E-mail : yuni@palgong.knu.ac.kr

Jang-Keun Bae

Dept. of Electronic & Information, Kumi college, Kyungpook, 780-711, KOREA

Yang-Hoi Doh

Dept. of Electronic Engineering, Cheju National University, Cheju, 690-756, KOREA

Cheol-Su Kim

School of Computer & Electronic Engineering, Kyongju University, Kyungpook 780-712, KOREA

(Received August 25, 1999)

A new image encoding and identification scheme is proposed for security verification by using a CGH(computer generated hologram), random phase mask, and a correlation technique. The encrypted image, which is attached to the security product, is made by multiplying a QP-CGH(quadratic phase CGI) with a random phase function. The random phase function plays a key role when the encrypted image is decrypted. The encrypted image can be optically recovered by a 2-f imaging system and automatically verified for personal identification by a 4-f correlation system. Simulation results show the proposed method can be used for both the reconstruction of an original image and the recognition of an encrypted image.

I. INTRODUCTION

Credit card fraud is a serious and widespread problem facing many banks, businesses, and consumers. In addition, counterfeit parts, such as computer chips, machine tools, etc., are becoming ever more prolific with the rapid advances in computers, CCD technology, image processing hardware and software, printers, scanners, and copiers for producing logos, symbols, money bills, or patterns. Presently, credit cards and passports use holograms for security as they can be inspected by human eye. In theory, a hologram cannot be reproduced by an unauthorized person using commercially available optical components. In practice, however, a holographic pattern can be easily acquired from a credit card(photographed or captured by a CCD camera) and then a new hologram is synthesized for the counterfeit. Recently, various optical-processing systems have been proposed for encryption, security systems, and the anti-counterfeiting and verification of biometrics. [1–6]

In this paper, a new image encoding and identification scheme for security applications is proposed using a CGH(computer generated hologram), random phase mask, and an optical correlation technique. The original image consists of a pure image and an identification number. The original image is encoded by bonding a random phase mask to a QP-CGH(quadratic phase-CGH) of it. The QP-CGH is made by using an SA(simulated annealing) algorithm [7] which has the advantage that it provides a low probability of a local minimum. The original image can be reconstructed by inverse Fourier transforming the encrypted image which is multiplied with the complex conjugate of the phase mask while encoding. The information of the random phase mask plays a key role when the encrypted image is decrypted. As the encoded image is a phase-only pattern, it is invisible under ordinary light and has the advantage that a simple intensity detector is unable to copy its image. Even if the information of the original image is known, the security image can not be reproduced because the random phase in-

formation has a high entropy. The authenticity and personal identification of the card can be easily verified using a low-power laser source since the encoded image has a high optical efficiency. Computer simulation results are provided to verify usefulness of the proposed method for optical security applications.

II. ENCODING METHOD

The encoded image is made by attaching a random phase mask to a QP-CGH for use in security products such as credit cards, passports. An SA algorithm is used when making the CGH to reduce the noise due to inevitable quantization error. Quadratic phases, that is 0, $\pi/2$, π,and $3\pi/2$, are used to remove the conjugate image of the original image that is generated due to a binary phase. This method provides good reconstruction of the low frequency part of the image. The SA algorithm finds the optimal solution using an iterative technique along with many variable parameters. It avoids the local minimum in an iteration process, conditionally permitting the temporary increase of the cost function.

The encoded image is phase-only function, therefore, it cannot be seen and cannot be copied by an intensity detector such as a CCD camera or a copier, etc. The random phase mask used as a device to verify the authenticity plays a key role when the encrypted image is decrypted. It is well known that the random noise, that leads to a large number of different realizations, maximizes entropy and is obtained with uniformly distributed noise with statistical independency. So the contents of the phase mask cannot be determined by light intensity detectors, and it is also extremely complicated to recover the encrypted image by blind deconvolution. Consequently, the encoded phase mask provides a double security. Also a phase-only characteristic of the encoded image, in theory, leads to no optical energy loss and delivers a very high optical efficiency enabling the use of a low power light source.

The original image is composed of a pure image and an identification number image. The former presents a personality such as a face, fingerprint or signature, and the latter is a serial number such as a PIN(personal identification number) or an office number. The former is for establishing the authenticity of the card, and the latter is for personal identification. Fig. 1 shows the encoding process. The Fig. 1(a) is the original image to be encoded, 1(b) is its phase hologram, 1(c) is random phase mask, and 1(d) is final encoded image.

III. OPTICAL METHOD FOR DECODING & IDENTIFICATION

The verification system that constructs the original image and identification can be one of several optical processor architectures. In Fig. 2, the upper part illustrates a 2-f imaging system for decoding the encoded image, and the lower part illustrates a 4-f correlation system for establishing the authenticity of the card and personal identification from the reconstructed image. The encoded image, whose authenticity is to be verified, consisting of a phase hologram pattern to which a phase mask has been bonded, is placed in the input plane P1 of the processor. And the phase key, which is the complex conjugate of the phase function during encoding, is superposed in the input plane. Random phase function of the encoded image is offset by the

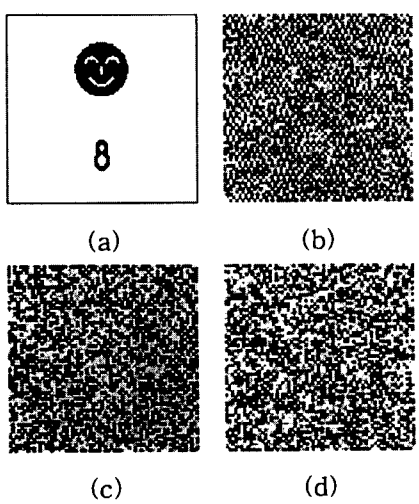

FIG. 1. Generating the encoded image. (a) original image (b) phase hologram (c) phase mask (d) encoded image

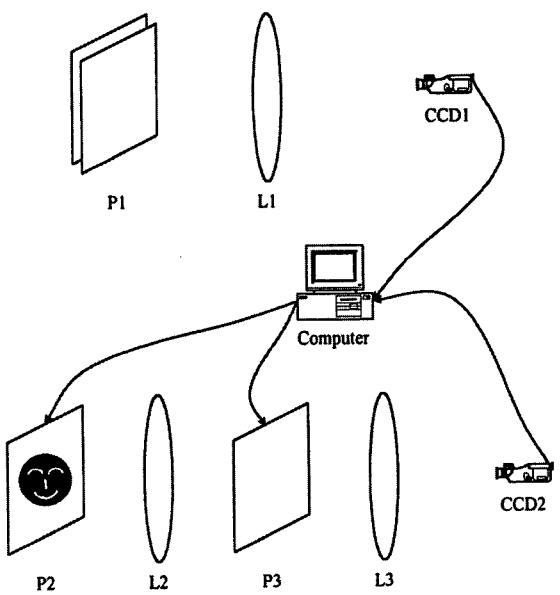

FIG. 2. Image reconstruction and verification.

phase key. So only the hologram of the original image seems to be in the input plane. They are Fourier transformed by lens L1. Thus the original image is reconstructed in the plane of CCD1, and digitally split into a pure image part and a number part. These parts are then used as the inputs(in the plane P2) of optical correlators, and an optical spatial filter is positioned in the Fourier plane P3. The final correlation results are obtained in the plane of CCD2. The authentication of the card and personal identification can then be performed. This system can be implemented in real time using spatial light modulators.

The spatial filters used in this paper were a conventional matched filter for the authenticity of the card, and a MMACE(multiplexed minimum average correlation energy) filter [8] for personal identification. The authenticity of the card can be recognized by correlating the matched filter with the pure image, and the personal identification can be recognized by correlating the recognition filter with the extracted alphanumeric image.

An MMACE filter is a synthetic filter generated in the frequency plane by multiplexing several filters in only one filter plane. It is capable of controlling the correlation peaks in the correlation plane and minimizing sidelobes. In this paper, 4 MACE filters are multiplexed by using a spatial frequency modulation of the phase component in the Fourier domain. Hence the correlation distribution plane of the MMACE filter is divided into 4 subplanes. If the correlation results were coded, it would be possible to discriminate a maximum of 15 different images. The code having all 0's('0000') is excluded because it has no information. Each MACE filter for the recognition of the identification number is

$$\mathbf{H}_i = \mathbf{D}^{-1}\mathbf{F}[\mathbf{F}^{+}\mathbf{D}^{-1}\mathbf{F}]^{-1}\mathbf{u}_i, \qquad i = 1,2,3,4 \quad (1)$$

where matrix $\mathbf{D}$ is the average spectrum of alphanumeric training images in each MACE filter. $\mathbf{F}$, a row vector representing the training images, is

$$\mathbf{F} = [\mathbf{F_1}\ \mathbf{F_2}\ \cdots\ \mathbf{F_{15}}] \quad (2)$$

and the constraint vectors are

$$\begin{aligned} \mathbf{u_1} &= [\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,] \\ \mathbf{u_2} &= [\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,0\,1\,1\,1\,] \\ \mathbf{u_3} &= [\,0\,1\,0\,1\,0\,1\,0\,0\,0\,1\,1\,1\,0\,0\,1\,] \\ \mathbf{u_4} &= [\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,] \end{aligned} \quad (3)$$

The element of the constraint vectors is set to '1' in the image to be recognized,'0' in the image to be rejected. The transfer function of the MMACE filter, which multiplexes 4MACE filters, is

$$H(\alpha,\beta) = \sum_{i=1}^{4} H_i(\alpha,\beta)exp[-j2\pi(a_i\alpha + b_i\beta)] \quad (4)$$

where a_i, b_i represent the amounts of displacement of each correlation result. When the center of the output correlation plane is coordinated (0,0), a_i has the (+) sign in the case of shifting the correlation results to the left and has the (−) sign in the case of shifting to the right. For b_i, similarly, the (+) sign corresponds to upwards and the (−) sign corresponds to downwards. Thus 4 subplanes constitute the output plane in the order of left-up, right-up, left-down, and right-down. Using the constraint vectors of 4 subplanes, 15 codes are assigned to 10 numeric and 5 alphabet characters as shown in table 1. The correlation results between the alphanumeric image and the MMACE filter is compared with an appropriate threshold value. Four correlation subplane results with each MACE filter are searched in the order of the above, and one of the codes in table 1 is obtained. With reference to the codes, the alphanumeric character can be recognized.

IV. COMPUTER SIMULATIONS

The validity of the proposed method for security application is investigated using the original image of Fig. 1(a), where the upper image is the pure image for authenticity and the lower image is the PIN for verification. The encoded image(Fig. 1(d)) is multiplied by the phase key and inverse Fourier transformed to form the reconstructed image(Fig. 3). When the phase key, which is wrong, is used in the decryption process, reconstructed image is shown in Fig. 3(b). Fig. 4(a) shows the split pure image used for verifying the authenticity of the card, and 4(b),the result of correlation

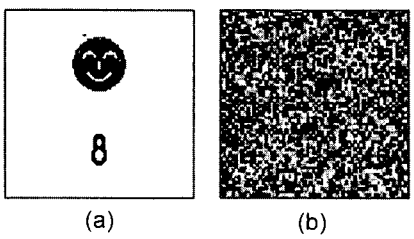

FIG. 3. Reconstructed image. (a) with correct phase key (b) with wrong phase key

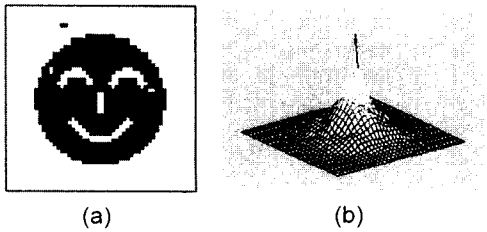

FIG. 4. Verifying the authenticity of the card. (a) pure image, (b) correlation result

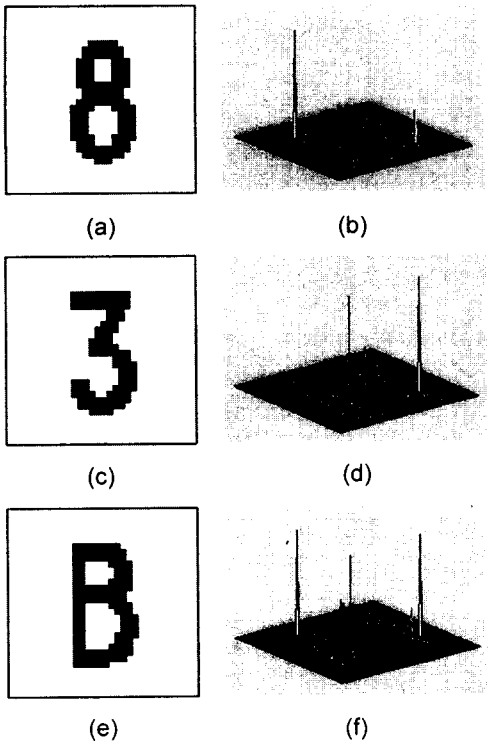

FIG. 5. Recognition of the identification number. (a) number image, (b) correlation result of (a), (c) number image, (d) correlation result of (c), (e) number image, (f) correlation result of (e)

TABLE 1. Code table for personal identification.

	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E
Sub-P1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
Sub-P2	0	0	0	1	1	1	1	0	0	1	0	0	1	1	1
Sub-P3	0	1	1	0	0	1	1	0	0	1	1	1	0	0	1
Sub-P4	1	0	1	0	1	0	1	0	1	1	0	1	0	1	0

with matched filter, shows the card is authentic.

Fig. 5(a) shows the split alphanumeric image for identification verification, and 5(b), the result of correlation with the MMACE filter, shows the 4 subplanes output. This is thresholded by an optimal threshold value where the value is the lowest correlation intensity of a true image to discriminate similar false images. In this simulation it is at 80% of the maximum correlation peak. Accordingly '1' is assigned to the value larger than threshold and '0' to the smaller value. In Fig. 5(b), 4 subplanes show the code of '1000' and this code represents the number'8' with reference to table 1. And Fig. 5(c), 5(e) show other alphanumeric input images and Fig. 5(d), 5(f) illustrate their correlation images with the same correlation filter. We can obtain the code of '0011', '1011' from Fig. 5(d), 5(f) and recognize the number '3' and the letter'B'. It is clear from these figures that the proposed method can be used for verifying the authenticity and identification number.

V. CONCLUSION

In this paper, a new security scheme was proposed using optical correlation. The original image is encoded by multiplexing a CGH and random phase, then it is reconstructed using a phase key, which is a complex conjugate of the phase function used during the encoding process, and a Fourier transform lens. The result is split into a pure image and identification number image, thereafter, the process of authentication and identity verification is performed using acorrelator. The proposed encoded image, which is phase-only, is invisible in ordinary light, therefore, an intensity sensitive detector is unable to reproduce it. Plus it provides a high optical efficiency and the use of a low power laser source. The random mask provides a double security because it has many different realizations, and the encoded image provides not only authentication, but also personal identification of the card. Computer simulations confirmed the feasibility of the proposed system.

ACKNOWLEDGMENTS

This research was supported by University Research Program sponsored by Ministry of Information & Communication in South Korea.

REFERENCES

[1] B. Javidi and J. L. Horner, Opt. Eng. **33**, 1752 (1994).
[2] P. Refregier and B. Javidi, Opt. Lett. **20**, 767 (1995).
[3] B. Javidi, Optics & Photonics News, 28 (1997).
[4] R. K. Wang, I. A. Watson, and C. Chatwin, Opt. Eng. **35**, 2464 (1996).
[5] B. Javidi, proc. SPIE **3386**, 14 (1998).
[6] T. Nomura, SPIE's Newsletter, **4** (1998).
[7] C. S. Kim, D. H. Kim, J. W. Kim, J. K. Bae, and S. J. Kim, Journal of IEEK. **32-A**, 111 (1995)
[8] J. W. Kim, C. S. Kim, J. K. Bae, Y. H. Doh, and S. J. Kim, Journal of KICS **19**, 2364 (1994).