濟州大學校 産業技術硏究所 論文集, 第10卷, 1號, pp.147-152, 1999. 6
Cheju Nat'l Univ. Res. Insti. Ind. Tech. Jour., Vol.10, No.1 pp.147-152, 1999. 6

Image encryption and identification for security verification

Jong-Yun Kim*, Yang-Hoi Doh** and Soo-Joong Kim*

신원보증을 위한 영상 암호화와 신분증명

김종윤*·도양회**·김수중*

ABSTRACT

A new image encoding and identification scheme is proposed for security verification by using a CGH(computer generated hologram), random phase mask, and correlation technique. The encrypted image, which is attached to the security product, is made by multiplying QP-CGH(quadratic phase CGH) 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.

Key Words : Image encryption, security verification, phase key

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 the 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

* School of Electronic & Electrical Eng., Kyungpook Nat'l Univ.
경북대학교 공과대학 전자전기공학부
** Faculty of Electrical & Electronic Eng., Res. Insti. Ind. Tech., Cheju Nat'l Univ.
제주대학교 공과대학 전기전자공학부, 산업기술연구소

acquired from a credit card (photographed or captured by a CCD camera) and then a new hologram synthesized for counterfeit. Recently, various optical processing systems have been proposed for encryption, security systems, and the anti-counterfeiting and verification of biometrics[1,6].

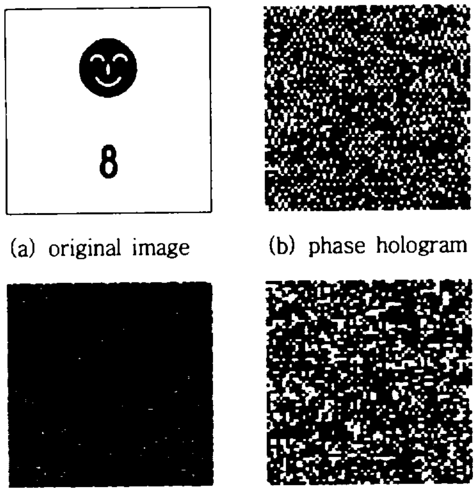
In this paper, a new image encoding and identification scheme for security applications is proposed using a CGH(computer generated hologram), random phase mask, and optical correlation technique. The original image consists of a pure image and identification number. The original image is encoded by bonding a random phase mask to a QP-CGH(quadratic phase-CGH) of it. QP-CGH is made using SA(simulated annealing) algorithm[7] which has the advantage that it provides a low probability of local minimum. The original image can be reconstructed by inverse Fourier transforming the encrypted image which is multiplied by 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 information has a high entropy. The authenticity and personal identification of the card can be easily verified using a low-power laser source since 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. The low frequency part of the image is well reconstructed using this method. The SA algorithm finds the optimal solution using an iterative technique along with many variable parameters. This 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 the largest number of different realizations, maximizes entropy and is obtained with uniformly distributed noise with statistically independent realization. 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.



(a) original image (b) phase hologram

(c) phase mask (d) encoded image

Fig. 1 Generating the 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 complex conjugate of the phase function during encoding, is superposed in the input plane. So only the hologram of the original image seems to be in the input plane. Thus the original image is reconstructed by the CCD camera in the plane of CCD1, and digitally split into a pure image part and a number part. The parts are then used as the inputs(in the plane P2) of the optical correlators, and an optical spatial filter is positioned in the Fourier plane of the frequency plane P3. The final correlation results are obtained in the plane of CCD2. The authenticity of the card and personal identification can then be performed. This system can be implemented in real time using spatial light modulators.

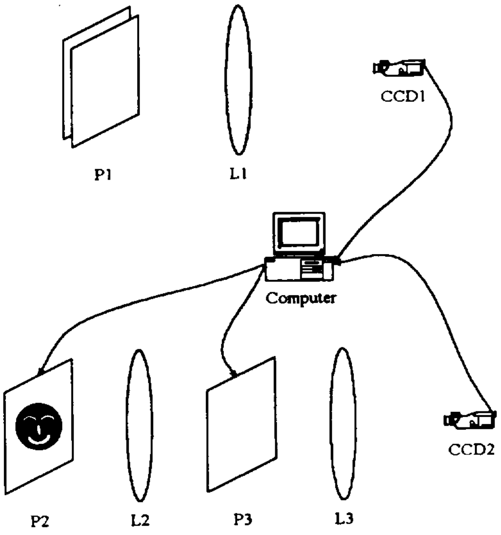


Fig. 2 Image reconstruction and verification

In this paper, the spatial filters used 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 able to control the correlation peaks in the correlation plane and minimize sidelobes. In this paper, 4 MACE filters are multiplexed by using a spatial frequency modulation of 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 excepted because it has no information. Each MACE filter for the recognition of the identification number is

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

where matrix D is the average spectrum of alphanumeric training images in each MACE filter. F, a row vector, represents the training images, is

$$\mathbf{F} = [\mathbf{F}_1\ \mathbf{F}_2 \cdots \mathbf{F}_{15}] \tag{2}$$

and the constraint vectors are

$$\begin{aligned}\mathbf{u}_1 &= [0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1]\\ \mathbf{u}_2 &= [0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1]\\ \mathbf{u}_3 &= [0\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1]\\ \mathbf{u}_4 &= [1\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0]\end{aligned} \tag{3}$$

The element of the constraint vectors is supposed to '1' in the image to be recognize, '0' in the image to be reject. The MMACE filter, which multiplexes 4 MACE filters, is

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

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 a (+) sign in the case of shifting the correlation results to the left or upwards, and has a (−) sign in the case of shifting to the right or 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 thresholded with an appropriate threshold value. 4 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.

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	1	0	1	1	1	0	0	1	0	0	1	1	1
Sub-P3	0	1	0	1	0	1	0	0	0	1	1	1	0	0	1
Sub-P4	1	0	0	1	1	0	0	0	1	1	0	1	0	1	0

IV. Computer Simulations

The validity of the proposed method for security application is investigated using 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). Fig. 4(a) shows the split pure image used for verifying the authenticity of the card, and 4(b), the result of correlation with matched filter, shows the card is authentic.

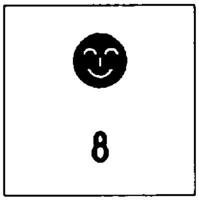


Fig. 3 Reconstructed image

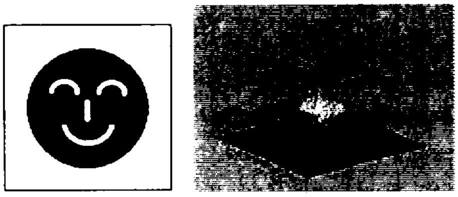
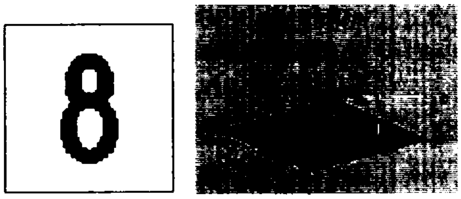

(a) (b)

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

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 optimal threshold value where the value is the lowest correlation intensity of 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 value and '0' to the value smaller. In Fig. 5(b), 4 subplanes show the code of '1000' and this code represents the number '8' with reference to table 1. It is clear from these figures that the proposed method can be used for verifying the authenticity and identification number.



(a) (b)

Fig. 5 Recognition of the identification number
(a) alphanumeric image,
(b) correlation result

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 in the encoding, and Fourier transform lens. The result is split into a pure image and identification number image, thereafter, the process of the authenticating the card and identity verification is performed using a correlator. 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 the low power laser source. The random

mask provides a double security because it has many different realizations. And the encoded image provides not only the checking the authority but also personal identification of the card. Computer simulations confirmed the possibility of the proposed system.

요 약

컴퓨터형성 홀로그램과 무작위 위상 마스크, 광상관 기술을 이용하여 신원보증을 위한 새로운 영상 암호화와 신분증명 체계를 제안하였다. 보안제품에 부착되는 암호화된 영상은 4진 위상 컴퓨터형성 홀로그램에 무작위 위상 함수를 곱하여 제작하였다. 무작위 위상 함수는 암호화된 영상을 복원할 때 핵심적인 역할을 한다. 암호화된 영상은 2-f 영상복원 시스템을 이용하여 복원하고, 4-f 상관 시스템을 이용하여 개인의 신원증명을 위한 확인작업을 자동적으로 수행한다. 제안된 방법을 원래의 영상을 복원하고 암호화된 영상을 인식하는데 사용할 수 있음을 시뮬레이션 결과를 통하여 보였다.

References

1) B. Javidi and J. L. Horner, 1994. Optical pattern recognition for validation and security verification, *Opt. Eng.*, vol. 33, no. 6, pp. 1752-1756.

2) P. Refregier and B. Javidi, 1995, Optical image encryption based on input plane and Fourier plane, *Optics Letters*, vol. 20, no. 7, pp. 767-769.

3) B. Javidi, 1997, Optical Informaion Processing for Encryption and Security Systems, *Optics & Photonics News*, pp. 28-33.

4) R. K. Wang, I. A. Watson, and C. Chatwin, 1996, Random phase encoding for optical security, *Opt. Eng.*, vol. 35, no. 9, pp. 2464-2469.

5) B. Javidi, 1998, Optical spatial filtering for image encryption and security systems, *Proc. of SPIE*, vol. 3386, pp. 14-23.

6) T. Nomura, 1998, Encryption using joint-transform correlator architecture for robust alignment, *SPIE's Newsletter*, p. 4.

7) C. S. Kim, D. H. Kim, J. W. Kim, J. K. Bae, and S. J. Kim, 1995, Synthesis of binary phase computer generated hologram by using an efficient simulated annealing algorithm, *Journal of IEEK*, vol. 32-A, no. 2, pp. 111-118.

8) J. W. Kim, C. S. Kim, J. K. Bae, Y. H. Doh, and S. J. Kim, 1994, Synthesis of multiplexed MACE filter for optical Korean character recognition, *Journal of KICS*, vol. 19, no. 12, pp. 2364-2375.