1999 年度 大韓電子工學會 夏季綜合學術大會 論文集 第 22 卷 第 1 號 99/6

CGH와 위상 마스크를 이용한 영상 보안 및 개인 인증

°김종윤* 박세준* 김종찬** 김철수*** 조웅호**** 김수중*

* 경북대학교 전자공학과

** 경북전문대학 전자과

*** 경주대학교 컴퓨터전자공학부

**** 대구공업대학 전자계산과

Image Security and Personal Identification using CGH and Phase Mask

°Jong-Yun Kim* Se-Joon Park* Jong-Chan Kim** Cheol-Su Kim***

Woong-Ho Cho**** Soo-Joong Kim*

* Dept. of Electronics Eng., Kyungpook Nat'l Univ.

** Dept. of Electronics, Kyungpook Tech. College

*** School of Computer & Electronics, Kyongju Univ.

**** Dept. of Computer Science, Taegu Tech. College

E-mail : yuni@palgong.kyungpook.ac.kr

Abstract

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

Ⅰ. 서 론

최근 컴퓨터의 프린터 기술의 발달로 인해 신용카드, 주민등록증, 여권, 지폐 등의 위조가 심각한 사회문제로 대두되고 있다. 그래서 근래에는 보다 발전된 형태로 신용카드와 여권 등에 홀로그램이 위조방지용으로 널리 이용되고 있으며 이것은 이론적으로는 복제될 수 없지만 실제 경우 홀로그램 패턴이 광세기 패턴이므로 CCD와 같은 기존의 광검출기로 쉽게 검출되어 새로운 홀로그램의 합성과 복제가 가능하게 한다. 따라서 어떠한 경우에도 ID 카드 위조나 복제를 근본적으로 차단할 수 있는 새로운 접근 방법에 대한 연구가 계속되고 있으며, 최근에는 CCD 카메라와 같은 기존의 광세기 검출기로는 볼 수도 복제될 수도 없는 복소함수 형태의 랜덤위상 패턴을 사용하는 새로운 광학적 보안 기법이 제시되고 있다[1-4].

본 논문에서는 CGH(computer generated hologram), 랜덤 위상 마스크, 그리고 광상관 기법을 이용하여 영상을 암호화하고 개인 인증하는 방법을 제시하였다. 국소해에 빠질 우려가 적은 SA(simulated annealing) 알고리듬[5]을 사용하여 만든 QPH(qudratic phase hologram)에 랜덤 위상 함수를 마스크로 붙여 영상을 암호화한다. 이 영상은 신용카드, 운전면허증 등의 보안제품에 스티커 형태로 붙여서 사용할 수 있다. 이렇게 암호화한 영상은 위상패턴으므로 단순한 광세기 검출기로는 복사할 수 없는 장점을 가지고 있다. 그리고 원영상에 대한 정보를 알고 있다 하더라도 마스크의 정보가 랜덤하기 때문에 암호영상을 제작하기는 마찬가지로 어렵다. 원영상은 순수영상과 고유번호로 이루어져 있으며 이는 암호화한 영상에 암호영상 제작시 사용한 위상 마스크의 복소공액을 곱한 후 푸리에 변환하여 재생된다. 이들과 광상관 필터와의 상관결과로

카드의 진위여부 및 분리인식을 할 수 있다. 암호화된 영상은 위상함수이므로 이론적으로는 광에너지 손실이 없고 높은 광효율을 제공하며 낮은 출력의 광원을 사용할 수 있다.

간단한 입력을 사용한 컴퓨터 시뮬레이션을 통하여 제안한 보안시스템의 성능을 확인하였다.

Ⅱ. 암호영상 생성

CGH 제작시 피할 수 없는 양자화 오차로 인한 재생영상에서의 잡음을 줄이기 위해 SA 알고리듬을 이용한 홀로그램을 사용하였다. 이진 홀로그램 재생시 발생하는 공액 이미지를 없애기 위해 위상홀로그램을 0, $\pi/2$, π, $3\pi/2$로 4진화하였으며 이 방법은 저주파 성분의 영상도 손실없이 재생된다. 반복적인 기법을 통해 최적의 해를 찾아가는 SA알고리듬에서는 사용되는 변수들이 많고, 이 변수에 대한 값들의 선택이 최적해를 찾는 데 중요한 역할을 한다. 그리고 이는 비용함수의 일시적 증가를 조건부 수용함으로써 반복과정 중의 국소(local minimum) 최적해에서 벗어날 수 있다. 이렇게 만든 위상 홀로그램에 랜덤 위상 마스크를 붙인 영상이 최종 암호영상이 된다. 이렇게 만들어진 암호영상은 신용카드, 여권 등의 제품에 붙여서 사용될 수 있다.

이 때 사용한 랜덤 위상 함수는 암호화된 영상이 복원될 때 중요한 역할을 한다. 암호화된 영상은 위상함수이므로 CCD 카메라나 복사기와 같은 단순한 광세기 검출기로는 복사할 수 없다. 그리고 랜덤 잡음은 엔트로피를 극대화시키고 통계적으로 독립적인 구현을 가진 균일하게 분포된 잡음으로부터 얻어진다. 위상 마스크의 내용 또한 빛세기 검출기로는 결정되어지기 힘드므로 이에 대한 정보 없이는 원영상의 재생이 불가능하다.

암호화된 영상은 전체적으로 위상함수이므로 이론적으로는 광에너지 손실이 없고 높은 광효율을 제공하며 낮은 출력의 광원을 사용할 수 있다. 암호화된 영상은 얼굴, 지문, 사인 등 개인의 특징을 나타내는 것과 주민등록번호, 사원번호 등의 일련번호의 조합으로 이루어져 있다. 전자는 카드의 진위를 구별하기 위한 것이고, 후자는 개인 인증을 위한 것이다. 영상 암호화 과정은 그림 1에서와 같다. 그림 1(a)는 암호화할 원영상, 1(b)는 이의 위상홀로그램, 1(c)는 랜덤 위상 마스크, 1(d)는 최종 암호영상이다.

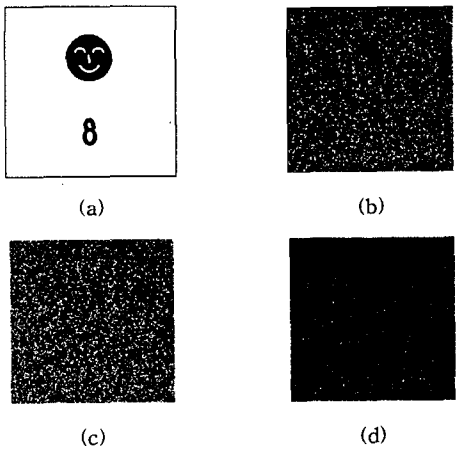


그림 1. 암호영상의 생성
(a) 원영상 (b) 위상 홀로그램
(c) 위상 마스크 (d) 암호 영상

Ⅲ. 영상복원 및 개별 인식

암호영상을 복원하고 분류 인식하기 위한 시스템의 구성도는 그림 2와 같다. 그림 2에서 윗부분의 2-f 시스템은 암호영상을 복원하기 위한 것이고, 아랫부분은 재생영상으로부터 카드 진위 여부 및 개인 식별을 위한 것이다. 암호영상은 위상마스크와 푸리에 렌즈로 이루어진 2-f 시스템을 이용하여 암호화된 영상을 광학적으로 복원한다. 이때 위상키는 암호화할 때에 사용한 위상키의 공액복소함수이다.

재생된 영상은 CCD 카메라로 받아 디지틀적으로 순수영상 부분과 번호부분으로 나눈 후 광상관기의 입력으로 사용된다. 본 논문에서는 광상관필터로서 카드

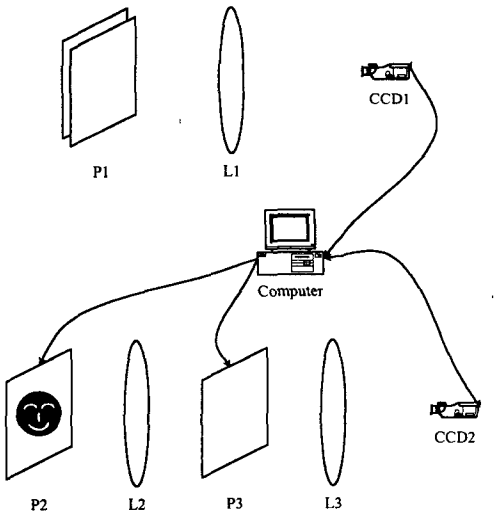


그림 2. 영상 복원 및 개인 인증

진위를 위해서는 정합필터를, 개별인식을 위해서는 예리한 상관첨두치와적은 부엽을 가지는 MMACE (multiplexed minimun average correaltion energy) filter를 사용하였다[6]. 정합 필터와 추출된 순수영상과의 상관첨두치의 유무로 카드의 진위를 구별할 수 있고, 번호 영상과 인식필터와의 상관결과로 고유번호를 분리인식할 수 있다.

MMACE 필터는 출력상관 평면상에서 상관첨두치를 임의로 제어함과 동시에 부엽의 크기를 최소화하여 예리한 상관첨두치를 가지는 MACE 필터와 하나의 필터평면에 여러 개의 필터함수를 중첩시키는 다중화 기법을 이용하는 주파수 평면에서 생성되는 합성필터이다. 본 논문에서는 네 개의 MACE 필터를 한 평면에 합성하였으며, 이때 필터의 크기는 각 MACE 필터와 입력영상과의 상관결과가 중첩되지 않고 입력영상 크기의 네배로 하였다. 그리고 네 개의 MACE 필터는 상·하·좌·우로 공간이동시켜 하나의 필터에 합성하였다. 따라서 상관평면에는 입력영상과 네 개의 MACE 필터와의 상관결과가 네 개의 부평면에 나뉘어져 나타난다. 이 상관결과를 4bit로 부호화하면 최대 15개의 영상을 분리인식할 수 있다. 이때 모든 코드가 0, 즉 부평면에서 상관첨두치가 없는 것은 제외된다. 각 고유번호를 인식하기 위한 부평면의 MACE 필터들은

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

와 같이 구할 수 있다. 여기서 D행렬은 각 MACE 필터합성에 사용된 고유번호 학습영상의 평균 스펙트럼을 의미하고, F는 필터합성시 사용된 지역명 학습영상을 나타내며

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

로 표현되는 행벡터이다. 그리고 제한 벡터는

$$\begin{aligned}\mathbf{u}_1 &= [000000011111111]\\ \mathbf{u}_2 &= [001011100100111]\\ \mathbf{u}_3 &= [010101000111001]\\ \mathbf{u}_4 &= [100110001101010]\end{aligned} \qquad (3)$$

로 하였다. 제한 벡터의 원소는 인식하고자 하는 영상에는 1을, 분리하고자 하는 영상에는 0을 부여하였다. 앞에서 만들어진 숫자와 일부 영문자를 인식하기 위한 MACE 필터들을 다중화 기법을 이용하여 하나의 필터로 중첩시킨 MMACE 필터함수는

$$H(\xi,\eta) = \sum_{i=1}^{4} H_i(\xi,\eta)\times\exp[-j2\pi(a_i\xi+b_i\eta)] \qquad (4)$$

와 같이 표현된다. 이때 상관결과의 분리정도를 결정하는 a_i와 b_i의 값은 출력상관평면의 중앙화소를 (0,0)이라 할 때 상관결과를 좌측과 상단으로 이동시킬 경우는 (+)값을, 우측과 하단으로 이동시킬 경우는 (-)값을 가진다.

표 1. 개인 인증을 위한 코드표

	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E
subp Ⅰ	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1
subp Ⅱ	0	0	1	0	1	1	1	0	0	1	0	0	1	1	1
subp Ⅲ	0	1	0	1	0	1	0	0	0	1	1	1	0	0	1
subp Ⅳ	1	0	0	1	1	0	0	0	1	1	0	1	0	1	0

그림 2에서 평면 P1, P2, P3 및 CCD 카메라는 렌즈 L1, L2, L3의 전후 초점면에 있으며 평면 P1에는 암호영상 및 위상키가, P2에는 순수영상 또는 고유번호 영상이 위치한다. 먼저 평면 P1에서는 암호영상과 위상키가 직렬로 연결되어 영상의 곱으로 구현된다. 여기서 위상키는 암호영상을 해독하는 데 핵심적인 부분으로 암호시 붙여진 위상함수와 공액복소 형태이다. 그래서 이 마스크와 위상함수는 서로 상쇄되고 마치 평면 P1에는 위상 홀로그램만 있는 것처럼 된다. CCD1에는 P1의 위상 홀로그램만이 푸리에 변환되어 원영상이 재생되고 컴퓨터로 이를 이진화하고 순수영상 및 고유번호 영상으로 나눈 후 차례로 광상관기의 입력면 P2에 올린다. 입력의 푸리에 변환 영상과 광상관필터는 P3면에서 서로 곱해진 후 렌즈 L3에 의해 다시 푸리에 변환되어 CCD2면에는 입력영상과 필터와의 상관결과가 출력된다. 이를 적절하게 문턱화하여 카드의 진위여부 및 개인 인증을 수행할 수 있다. LCD(liquid crystal device)를 이용하면 평면 P1, P2, P3에 각 영상을 기록하면 실시간적으로도 구현이 가능하다.

재생된 고유번호 영상의 인식과정은 다음과 같다. 먼저 입력영상을 푸리에 변환시켜 MMACE 필터와 곱하여 상관을 취한 후 적절한 값으로 문턱화한 후 상관세기를 4개의 부평면 중 좌상의 부평면부터 우상, 좌하, 우하의 순으로 검색한다. 만약 좌상의 부평면에서 모든 화소를 검색하여 상관첨두치를 찾게 되면 다른 부평면의 동일 위치에서의 상관치를 검사하여 인식코드를 획득한다. 만약 좌상의 부평면에서 코드가 획득되지 않으면 우상, 좌하, 우하의 부평면에서 동일한 방법으로 코드를 획득한다. 그리고 컴퓨터에 기억된 표 1의 코드표와 비교하여 해당 숫자 및 영문자를 인식한다.

Ⅳ. 컴퓨터 모의실험

컴퓨터 시뮬레이션에 사용한 입력영상은 그림 1(a)에서와 같다. 여기서 상단의 이미지는 카드의 진위를 구별하기 위한 순수영상이고, 하단의 이미지는 개인

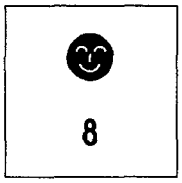


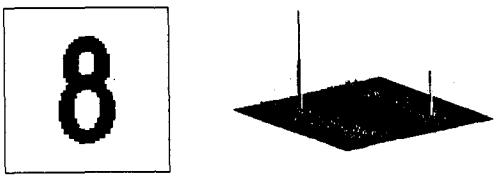
그림 3. 재생 영상

인증을 위한 고유번호 영상이다. 이는 각각 광상관기의 입력으로 들어간다. 암호영상을 위상 키와 푸리에 렌즈로 복원한 재생영상은 그림 3과 같다.

재생영상 중 분리된 순수 이미지 영상은 그림 4(a)와 같고 정합필터와의 상관결과는 그림 4(b)와 같다. 또한 개인식별을 위하여 분리된 숫자 영상은 그림 5(a)와 같고 MMACE필터와의 상관결과는 그림 5(b)와 같고 이들을 문턱화한다. 이때 최적의 문턱치값은 유사영상을 분리할 수 있는 최소의 상관세기로 본 논문에서는 그 값을 최고 상관치의 80%로 하여 문턱값보다 큰 값은 '1'로, 작은 값은 '0'으로 설정하였다. 그림 5(b)에서 '8'자의 위치에서 획득할 수 있는 코드가 '1000'이므로 표 1의 코드와 비교해 보면 숫자 '8'을 인식할 수 있음을 알았다.

(a) (b)

그림 4. 카드 진위 판별
(a) 순수 영상 (b) 상관결과



(a) (b)

그림 5. 고유번호 인식
(a) 고유 번호 영상 (b) 상관결과

V. 결 론

본 논문에서는 광상관을 이용하여 영상의 보안 및 인증을 위한 새로운 방법을 제안하였다. CGH와 위상함수를 이용하여 영상을 암호화한다. 암호영상을 만들 때 사용한 위상함수가 암호영상을 재생할 때에 핵심역할을 한다. 원영상은 암호영상 제작 시 사용한 위상함수의 복소함수값을 가진 위상키와 푸리에 렌즈를 이용하여 재생하고, 이를 순수영상과 고유번호로 나눈 후 광상관기를 통해 암호영상의 진위여부 및 개인인증을 할 수 있다. 제안한 방법으로 제작한 암호영상은 위상패턴으로 광세기 검출기로 복제가 불가능할 뿐만 아니라 높은 광효율은 제공하여 저출력 광원 사용이 가능하게 한다. 또한 이 방법은 랜덤한 위상 마스크를 사용함으로써 복제를 더욱 어렵게 하였고 원영상 복원 후 카드의 진위 여부 뿐만 아니라 개별 인식을 할 수 있는 장점을 제공한다. 제안한 방법으로 간단한 입력을 사용하여 영상 복원 및 영상의 진위 유무, 분리인식 가능함을 확인하였다. 선명하고 깨끗한 그레이 영상 재생을 위한 홀로그램과 분리 인식할 데이터의 선정이 앞으로 연구해야될 과제이다.

참고문헌

[1] B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification", vol. 33, no. 6, pp. 1752-1756, 1994. 6.

[2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane", Optics Letters, vol. 20, no. 7, pp. 767-769, 1995. 1.

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

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

[5] 김철수, 김동호, 김정우, 배장근, 이재곤, 김수중, "효율적인 Simulated Annealing 알고리듬을 이용한 이진 위상 컴퓨터형성 홀로그램의 합성", 대한전자공학회 논문지, vol. 32-A, no. 2, 1995. 2.

[6] 김정우, 김철수, 배장근, 도양회, 김수중, "인쇄체 한글의 광학적 인식을 위한 다중 MACE 필터의 합성", 한국통신학회 논문지, vol. 19, no. 12, pp. 2364-2375, 1994. 12.