《연구논문》 Hankook Kwanghak Hoeji, Volume 14, Number 4, August 2003

개인신원정보 보호를 위한 광 보호 시스템

윤종수

에스케이테크

㉾ 472-905 경기도 남양주시 와부읍 월문리 820-2

도양회†

제주대학교 전기전자공학부, 첨단기술연구소

㉾ 690-756 제주도 제주시 아라동 1

(2002년 12월 9일 받음, 2003년 6월 2일 수정본 받음)

개인의 신원정보 보호를 위하여 새로운 광 정보보호 시스템을 제안하였다. 개인 신원정보의 확인과 인증을 위하여 얼굴영상과 개인식별번호로 구성된 신원정보를 사용하였다. 영상 암호화는 4-f 광상관기의 입력과 푸리에영역에서 랜덤위상패턴을 사용하는 위상암호화 기술을 사용하였다. 그렇지만 암호화된 영상을 복원하는 과정에서 개인의 신원정보가 유출될 가능성이 있다. 이에 대처하기 위하여 신원확인 과정에서 영상을 복원하지 않고 암호화된 영상을 그대로 사용하였다. 암호화된 개인식별번호는 제안된 MMACE_p 필터를 사용하여 분류·인식하였고, 개인정보의 인증은 OWMF를 사용하여 얼굴영상의 상관치를 구하여 확인하였다. 제안된 MMACE_p 필터는 10개의 암호화된 숫자를 한꺼번에 인식할 수 있도록 4개의 MACE_p 필터를 다중화하여 합성하였고, OWMF는 얼굴영상의 분리인식 능력과 SNR을 향상시킬 수 있도록 하였다. 컴퓨터 시뮤레이션을 통하여 제안된 정보보호기술이 개인신원정보 보호에 적용될 수 있음을 보였다.

주제어 : optical security, encryption, MACE filter, correlation.

I. 서 론

정보사회가 발전함에 따라 주민등록증, 여권, 면허증, 출입증 등의 개인의 신원을 증명할 수 있는 신분증과 각종 신용카드의 사용이 급격히 증가하고 있다. 그러나 프린터, 스캐너, 복사기, 컴퓨터 관련 장치들과 소프트웨어 기술의 발달로 복제기술이 나날이 향상됨에 따라 신분증과 신용카드 등의 위조가 용이해지고 있으며 이는 심각한 사회문제가 되고 있다. 또한 주민등록번호, 신용카드번호 등은 단순히 번호의 유출만으로도 개인의 신용정보를 불법으로 이용당할 수 있어 이에 대한 대책이 시급하다. 이런 문제를 해결하기 위한 방법으로 신용카드와 신분증 등에 엠보싱 홀로그램을 부착하여 사용하고 있으나, 이것도 광세기 검출기를 이용하면 마스터 홀로그램의 합성 및 대량복제가 가능하여 불법사용을 막을 수 없다. 그래서 단순하면서도 광의 장점을 이용할 수 있고, 어떠한 경우에도 신분증과 카드의 위조, 복제나 불법사용을 근본적으로 차단할 수 있는 새로운 방법에 대한 연구가 계속되고 있다.[1,2]

그렇지만 기존의 광학적 영상암호화 방법들은 개인의 신분을 인증하기 위하여 암호화된 영상을 복원하여 사용한다.[3-5] 예를 들면, 복원한 얼굴영상과 신분증을 제시한 사람의 얼굴을 육안으로 확인하거나 복원한 얼굴영상을 데이터베이스에 있는 본인의 얼굴정보와 서로 비교하거나, 또는 복원한 개인식별번호(personal identification number, PIN) 영상을 이용하여 신분증을 제시한 사람의 식별번호를 질의응답 하는 등과 같이 복원영상을 이용하는 경우이다. 그러나 개인식별번호를 복원하는 경우에는 번호가 유출될 소지가 있어 신용카드나 비밀취급인가증 등의 비밀코드처럼 보안을 요하는 곳에서 사용하기에는 부적합하다. 따라서 암호화된 영상을 복원하더라도 개인의 신원정보를 육안으로 식별할 수 없도록 하거나, 암호화된 영상을 복원하는 과정 없이 인식시스템에서만 신원을 확인하도록 할 필요가 있다.

본 연구에서는 개인의 신원정보 보호를 위하여 새로운 광 정보보호 시스템을 제안하였다. 제안한 시스템은 개인식별번호와 얼굴영상으로 구성된 신원정보영상을 암호화하여 위상홀로그램 형태로 신분증에 부착시키고, 이를 사용할 때에는 홀로그램 패턴을 광학적으로 해독하여 개인인증을 하는 방법이다. 신원정보영상의 암호화는 Towghi 등이 제안한 위상암호화 방법[5]을 기본으로 하여 공간영역과 공간주파수영역에서 랜덤위상패턴을 사용하여 이중으로 암호화한다. 암호화된 신분증의 인증은 일차적으로 제안된 MMACE_p(multiplexed MACE_phase encrypted) 필터를 사용하여 개인식별번호를 분류·인식하고, 개인의 신원을 확인한다. 개인의 신원이 확인되면 광웨이브릿 정합필터[6](optical wavelet matched filter, OWMF)를 이용하여 복원된 얼굴영상과 데이터베이스에 저장된 얼굴정보와의 1:1 광상관(optical correlation)을 수행하며, 이를 통하여 신분증 소지자의 진위여부를 판별한다. 특히 개인식별번호를 인식할 때에는 번호를 복원하지 않고 암호화된 상태에서 인식하도록 하여 신원정보의 유출을 막을 수 있도록 하였다. 또한 인

†E-mail: yhdoh@cheju.ac.kr

식된 개인식별번호를 이용하여 얼굴정보를 1:1 광상관을 취하므로 인증속도가 빠르고, 신원확인을 이중으로 하므로 부정사용의 가능성을 현저히 줄일 수 있다. 따라서 제안된 시스템은 각종 금융거래, 신용거래, 보안통제 등의 폭넓은 분야에서 안전하면서도 신속하게 업무를 처리할 수 있는 이점을 제공하리라 기대된다.

II. 개인신원정보의 암호화

2.1. 얼굴영상의 위상암호화 방법

신원정보영상 중에서 개인식별번호는 보안이 된 상태에서 인식할 수 있도록 하지만, 얼굴영상은 복원하여 신분증 소지자의 실물과 비교하여야 하므로 Towghi 등의 방법[5]을 사용한다. Towghi 등이 제안한 영상의 위상암호화는 공간영역과 공간주파수영역에서 이중으로 암호화할 수 있는 4-f 광상관기를 기본 시스템으로 하고 있다. 이는 정규화된 입력영상을 위상패턴으로 변환한 후, 공간영역에서 랜덤위상패턴을 곱하여 암호화하고, 이의 푸리에 변환된 결과를 공간주파수영역에서 또 다른 랜덤위상패턴을 곱하여 이중으로 암호화한다.

암호화하고자 하는 정규화된 입력영상을 $f(x, y)$라 하면, 위상패턴으로 변환된 입력영상 신호 $c(x, y)$는

$$c(x, y)=exp[j\pi f(x, y)] \tag{1}$$

처럼 표현되고, 위상의 범위는 구간 $[0, \pi]$의 값을 갖는다. 공간영역과 공간주파수영역에서 사용하는 랜덤위상패턴 $g(x, y)$와 $Q(u, v)$는 구간 [0, 1]에서 균일한 확률분포를 갖는 서로 독립인 랜덤 백색잡음(uniformly distributed random noise) $p(x, y)$와 $b(u, v)$를 각각 위상패턴으로 변환하여 얻으며

$$\begin{aligned} g(x, y)&=\exp[j2\pi p(x, y)] \\ Q(u, v)&=\exp[j2\pi b(u, v)] \end{aligned} \tag{2}$$

와 같이 표현된다.

입력영상 $f(x, y)$의 위상암호화 과정은 먼저, 위상패턴으로 변환된 입력영상 $c(x, y)$를 공간영역에서 랜덤위상패턴 $g(x, y)$와 곱하고, 이의 푸리에 변환된 결과를 공간주파수영역에서 랜덤위상패턴 $Q(u, v)$와 곱한다. 이렇게 공간주파수영역에서 얻은 결과를 역 푸리에 변환하면 암호화된 영상 $\varphi_f(x, y)$를 얻는다. 이 과정을 수식으로 표현하면

$$\begin{aligned} \varphi_f(x, y)&=\mathcal{F}^{-1}[\mathcal{F}\{c(x, y)g(x, y)\}Q(u, v)] \\ &=\{c(x, y)g(x, y)\}\otimes q(x, y) \\ &=\{\exp[j\ \pi f(x, y)]\ \exp[j\ 2\pi p(x, y)]\}\otimes q(x, y) \end{aligned} \tag{3}$$

와 같다. 여기서 $\mathcal{F}\{\cdot\}$는 푸리에 변환 연산자, $\mathcal{F}^{-1}\{\cdot\}$은 역 푸리에 변환 연산자, $\otimes$는 콘볼루션(convolution) 연산자이고, $q(x, y)$는 전달함수 $Q(u, v)=\exp[j2\pi b(u, v)]$의 임펄스 응답이다.

암호화된 영상의 복원 과정은 암호화의 역 과정으로 암호화 과정에서 사용된 랜덤위상패턴 $g(x, y)$와 $Q(u, v)$의 복소공액을 이용하여 이루어진다. 먼저, 암호화된 영상 $\varphi_f(x, y)$를 푸리에 변환한 후, 공간주파수영역에서 $Q^*(u, v)$를 곱한 후, 공간영역에서 $g^*(x, y)$를 곱하면 위상패턴으로 변환된 입력영상 신호 $c(x, y)$를 얻는다. 이 과정을 수식으로 표현하면

$$\begin{aligned} c(x, y)&=[\mathcal{F}^{-1}[\mathcal{F}\{\varphi_f(x, y)\}\times Q^*(u, v)]]\times g^*(x, y) \\ &=\{c(x, y)g(x, y)\}\otimes q(x, y) \\ &=c(x, y)=\exp[j\ \pi f(x, y)] \end{aligned} \tag{4}$$

와 같다. 여기서 원래의 입력영상 $f(x, y)$의 복원은 $c(x, y)=\exp[j\pi f(x, y)]$의 위상성분을 검출한 후 π로 나눠주면 된다.

이러한 영상의 위상암호화[그림 1(a)]와 복원[그림 1(b)]은 4-f 광 상관시스템을 사용하여 광학적으로 구현이 가능하다. 그림 1(a)에서 공간영역인 광상관기의 입력평면에 위상패턴으로 변환된 입력영상 $c(x, y)=\exp[j\pi f(x, y)]$와 랜덤위상패턴 $g(x, y)=\exp[j2\pi p(x, y)]$를 설치하고 코히어런트 광을 비추면 공간주파수영역인 푸리에평면에서 $\{c(x, y)\times g(x, y)\}$의 푸리에 변환을 얻는다. 이는 주파수평면에 설치되어 있는 랜덤위상패턴인 $Q(u, v)=\exp[j2\pi b(u, v)]$와 곱해지며, 주파수평면에서 곱해진 결과는 역 푸리에 변환되어 출력평면에서 $\{c(x, y)\times g(x, y)\}$와 $q(x, y)$의 콘볼루션 결과로 암호화된 영상 $\varphi_f(x, y)$를 얻을 수 있다.

암호화된 영상의 복원은 그림 1(b)에서 보이는 것과 같이 암호화 과정과 유사한 구조를 가진다. 암호화된 영상 $\varphi_f(x, y)$를 입력평면에 설치하고 코히어런트 광을 비추면 공간주파수영역에서 암호화된 영상의 푸리에 변환을 얻는다. 이는 암호화 과정에서 사용된 주파수영역 랜덤위상패턴의 복소공액 $Q^*(u, v)=\exp[-j2\pi b(u, v)]$와 주파수영역에서 곱해지고, 주파수평면에서 곱해진 결과는 역 푸리에 변환되어 출력평면에 $\{c(x, y)\times g(x, y)\}$로 나타난다. 이때 출력평면에 공간영역 랜덤위상패턴의 복소공액 $g^*(x, y)=\exp[-j2\pi p(x, y)]$를 설치하면 위상패턴으로 변환된 입력영상 $c(x, y)=\exp[j\pi f(x, y)]$를 얻을 수 있으며, 여기서 위상성분을 검출하여 π로 나누면 입력영상 $f(x, y)$를 얻

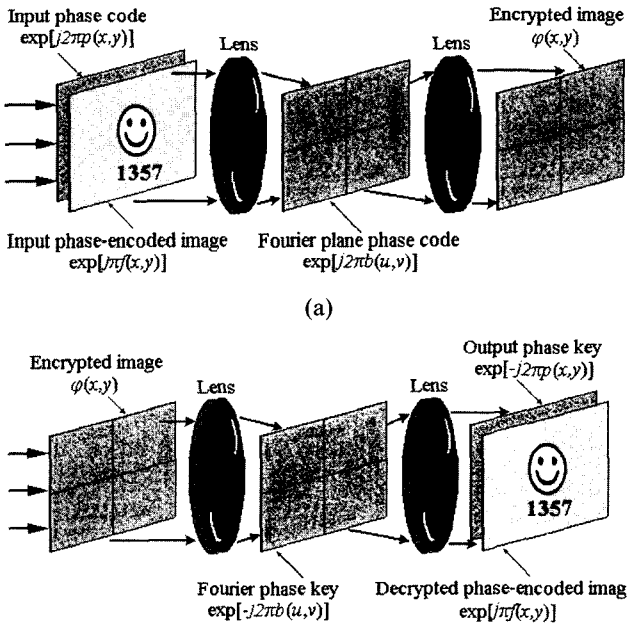

그림 1. (a) 영상의 위상 암호화와 (b) 복원을 위한 광 상관기.

을 수 있다. 즉, 암호화된 영상을 복원하기 위해서는 공간영역에서의 랜덤위상패턴 $g(x, y)$와 공간주파수영역에서의 랜덤위상패턴 $Q(u, v)$를 알고 있어야 가능하므로 이들은 암호화된 영상을 복원하기 위한 핵심적인 암호키 역할을 하게 된다.

2.2. 개인식별번호의 위상암호화 방법

제안한 개인식별번호의 암호화 방법은 비밀코드처럼 보안을 요하는 경우나 개인의 신원정보가 타인에게 보여져서는 안 될 경우에 암호화된 신원정보를 복원하는 과정 없이 인식시스템에서 신원확인이 이루어지도록 하기 위한 것이다. 개인식별번호를 구성하는 각각의 숫자영상을 $f_i(x, y)$라 하고, 각각의 숫자영상에 대응하는 서로 독립인 백색잡음을 $p_i(x, y)$라 하면, 공간영역에서 위상암호화한 각각의 학습영상 $t_i(x, y)$는

$$t_i(x, y) = \exp[j\pi f_i(x, y)]\exp[j2\pi p_i(x, y)], \quad i=0, 1, \ldots, 9 \quad (5)$$

와 같이 정의할 수 있다. 이렇게 암호화된 각각의 숫자영상은 공간영역에서 암호화된 개인식별번호영상 $t(x, y)$를 구성한다. 공간영역에서 암호화된 영상 $t(x, y)$는 다시 공간주파수영역에서 랜덤위상패턴 $Q(u, v) = \exp[j2\pi b(u, v)]$에 의해서 이중으로 암호화된다. 이중으로 암호화된 개인식별번호 영상 $\varphi_t(x, y)$는

$$\begin{aligned}\varphi_t(x, y) &= \mathcal{F}^{-1}[T(u, v)Q(u, v)] \\ &= t(x, y) \otimes q(x, y)\end{aligned} \quad (6)$$

와 같다. 여기서 $T(u, v)$는 암호화된 영상 $t(x, y)$의 푸리에 변환된 결과이다.

개인식별번호 영상의 위상암호화도 그림 1(a)의 4-f 광 상관 시스템을 사용하여 광학적으로 구현할 수 있다. 그림 1(a)에서 공간영역인 광상관기의 입력평면에는 공간영역에서 암호화된 숫자영상 $t_i(x, y)$의 조합으로 구성된 $t(x, y)$를 설치한다. 이는 푸리에 변환되어 공간주파수영역에 나타나며 주파수평면에 설치되어 있는 랜덤위상패턴 $Q(u, v) = \exp[j2\pi b(u, v)]$와 곱해진다. 주파수평면에서 곱해진 결과는 역 푸리에 변환되어 출력평면에서 $t(x, y)$와 $q(x, y)$의 콘볼루션 결과로 암호화된 개인식별번호 영상 $\varphi_t(x, y)$를 얻을 수 있다.

암호화된 상태에서 개인식별번호를 인식하기 위해서는 공간영역에서 암호화된 숫자영상 $t_i(x, y)$를 학습영상으로 하여 필터를 설계한 후, 주파수영역의 암호키 $Q^*(u, v) = \exp[-j2\pi b(u, v)]$를 사용하여 인식할 수 있다. 이와 같이 숫자영상을 공간영역에서 위상암호화하여 학습영상으로 만들게 되면, 학습영상은 단순한 숫자영상보다 더 많은 정보를 포함하게 되어 학습영상들의 유사성을 감소시킬 수 있으므로 분리인식 능력을 향상시킬 수 있다. 또한 암호화된 영상으로부터 개인식별번호를 인식하기 위해서는 암호화 과정에서 사용되는 랜덤위상패턴들을 모두 알고 있어야만 가능하므로 비밀코드 및 개인정보 보호에 더욱 유용하게 사용될 수 있다.

III. 개인의 신분인증

3.1. 개인식별번호의 분류 · 인식

제안한 개인의 신분인증 방법은 먼저, 개인식별번호를 분류 · 인식하여 신원을 파악한 후, 그 사람의 얼굴정보와 복원한 얼굴영상을 서로 비교함으로써 이루어진다. 개인식별번호를 분류 · 인식하기 위해서 제안된 MMACE_p(multiplexed MACE_phase encrypted) 필터는 위상암호화된 학습영상들을 MACE(mininum average correlation energy) 방식으로 합성한 후 이를 다중화하여 만든다. MMACE_p 필터의 설계는 먼저 복원된 학습영상을 인식대상으로 하는 MMACE(multiplexed MACE) 필터[7]의 설계과정을 이해하면 쉽게 접근할 수 있으며, MMACE_p 필터의 성능도 역시 MMACE 필터와 비교하여 보이는 것이 좋다.

MMACE 필터는 MACE 필터들을 공간주파수영역에서 변조하여 다중화 하는 방법을 이용한다. 본 연구에서는 숫자 '0'~'9'를 효과적으로 분류 · 인식하기 위하여 4개의 MACE 필터를 다중화 하였으며, 다중화된 상관결과는 코드로 만들어 4개의 부평면에 나누어 표시하였다. 개인식별번호를 인식하기 위한 4개의 MACE 필터는

$$\mathbf{H}_{\mathrm{MACE},i} = \mathbf{D}^{-1}\mathbf{F}\,[\mathbf{F}^{+}\mathbf{D}^{-1}\mathbf{F}]^{-1}\,\mathbf{u}_i, \quad i = 1, 2, 3, 4 \quad (7)$$

와 같다. 여기서 '+' 기호는 복소공액전치(complex conjugate transpose)변환을 나타내고, 행렬 D는 숫자 '0'~'9' 영상의 평균 에너지 스펙트럼을 나타내며, F는 푸리에 변환된 학습영상('0'~'9' 숫자영상)들을 행벡터

$$\mathbf{F} = [\mathbf{F}_0\ \mathbf{F}_1\ \cdots\ \mathbf{F}_9] \quad (8)$$

로 표현한 것이다.

제한벡터 $\mathbf{u}_i$는 벡터 원소 값을 조정하여 각각의 부평면에서 상관첨두치를 원하는 비율로 제한해 줄 수 있는데, 각각의 부평면에서 인식하고자 하는 학습영상에 대해서는 원소 값을 '1'로 두어 최대 상관첨두치가 나타나도록 하고, 인식하지 않는 학습영상에 대해서는 원소 값을 '0'으로 두어 상관첨두치가 나타나지 않도록 한다. 이를 코드화하면 인식대상으로 하는 학습영상('0'~'9' 숫자영상)들을 특정코드와 1:1 대응시킬 수 있다. 여기서 코드 값은 임의로 설정할 수 있으며 4개의 필터를 다중화한 경우에는 코드값이 모두 '0'인 경우를 제외하고 최대 15개의 서로 다른 코드를 사용할 수 있으므로 기호나 특수문자 등을 포함하여 최대 15개의 서로 다른 숫자나 문자를 분리인식 할 수 있다. 코드값이 모두 '0'인 상태의 코드를 제외한 이유는 입력평면에 영상정보가 존재하지 않거나, 필터를 합성할 때에 사용된 학습영상에 포함되지 않는 숫자나 문자가 입력되는 경우에도 모두 '0'의 값을 갖는 코드를 발생시켜서 오인식의 가능성이 있기 때문이다. 표 1은 '0'~'9' 숫자영상들의 조합으로 생성되는 개인식별번호를 인식하기 위하여 본 연구에서 사용한 코드표이며, 이에 해당하는 제한벡터 $\mathbf{u}_i$는

$$\begin{aligned}\mathbf{u}_1 &= [1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1] \\ \mathbf{u}_2 &= [1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0] \\ \mathbf{u}_3 &= [0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0] \\ \mathbf{u}_4 &= [0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1]\end{aligned} \quad (9)$$

와 같다. 예를 들어 숫자 '6'이 입력되면 제한벡터 $\mathbf{u}_1$은 부평면1에서 상관첨두치가 나타나지 않도록 하여 '0'의 코드를 발

표 1. 개인식별번호의 분류 · 인식을 위한 코드표

	0	1	2	3	4	5	6	7	8	9
Sub-P1	1	0	0	0	0	0	0	0	1	1
Sub-P2	1	0	0	0	1	1	1	1	0	0
Sub-P3	0	0	1	1	0	0	1	1	0	0
Sub-P4	0	1	0	1	0	1	0	1	0	1

생시키고, 제한벡터 $\mathbf{u}_2$는 부평면2에서 최대상관첨두치가 나타나도록 하여 '1'의 코드를 발생시킨다. 마찬가지로 부평면3과 부평면4에서는 제한벡터 $\mathbf{u}_3$과 $\mathbf{u}_4$는 각각 '1'과 '0'의 코드를 발생시킨다. 이 결과를 조합하면 '0110'의 코드가 되어 숫자 '6'을 인식하게 되는 것이다.

4개의 MACE 필터를 공간주파수영역에서 변조하여 다중화한 MMACE 필터는

$$H_{MMACE}(u,v)=\sum_{i=1}^{4} H^{*}_{MACE,i}(u,v)\ \exp[-j2\pi(m_i u+n_i v)] \quad (10)$$

와 같다. 여기서 m_i와 n_i는 4개의 상관결과를 출력상관평면에서 겹치지 않도록 하기 위한 공간이동계수로서 각각 상관결과의 좌우이동과 상하이동을 나타낸다. 결과적으로 4개의 MACE 필터가 다중화된 MMACE 필터와 개인식별번호 영상의 상관결과는 4개의 부평면으로 나누어져서 서로 독립적으로 위치하게 되며, 이를 경계값처리를 한 후 표 1의 코드표와 비교하여 개인식별번호를 인식하게 된다.

한편, 제안한 영상암호화 방법을 사용하여 암호화된 개인식별번호 영상을 복원하는 과정 없이 분류 · 인식할 수 있는 MMACE_p 필터는 공간영역에서 숫자영상 대신에 위상암호화된 학습영상 $t_i(x,y)$들을 MACE 방법으로 합성하는 것으로부터 시작한다. 위상암호화된 영상을 인식하기 위한 MACE_p 필터는

$$\mathbf{H}_{MACE\_p,i}=\mathbf{D}_T^{-1}\mathbf{T}[\mathbf{T}^{+}\mathbf{D}_T^{-1}\mathbf{T}]^{-1}\mathbf{u}_i \quad (11)$$

와 같다. 여기서 $\mathbf{D}_T$는 공간영역에서 위상암호화된 학습영상들의 평균 에너지 스펙트럼이고, $\mathbf{T}$는 행벡터로 암호화된 학습영상의 푸리에 변환이다. 여기에 사용된 제한벡터 $\mathbf{u}_i$는 식 (9)와 같고, 개인식별번호를 분류·인식하기 위한 코드표도 표 1과 같게 설정하였다. 이들 MACE_p 필터들을 다중화 방법을 이용하여 합성한 MMACE_p 필터는

$$H_{MMACE\_p}(u,v)=\left[\sum_{i=1}^{4} H^{*}_{MACE\_p,i}(u,v)\,exp[-j2\pi(m_i u+n_i v)]Q^{*}(u,v)\right] \quad (12)$$

와 같다. 여기서 $Q^{*}(u,v)=\exp[-j2\pi b(u,v)]$는 공간주파수영역의 암호화과정에서 사용되었던 랜덤위상패턴의 복소공액성분인 암호키이다. 이는 MMACE_p 필터의 경우 암호화된 영상을 복원하지 않고 인식하도록 하기 때문에 필터에 암호키의 정보를 포함시킨 것이다.

개인식별번호의 인식을 위한 광시스템은 그림 1과 같은 4-f 광상관기를 사용한다. 입력평면에는 암호화된 개인식별번호영상을 설치하고 공간주파수영역에 제안한 MMACE_p 필터를 설치하면, 출력평면에서 코드화된 상관분포를 얻을 수 있고, 이를 통해 개인식별번호를 인식할 수 있다.

3.2. 얼굴영상 인식

MMACE_p 필터로 개인식별번호를 분류 · 인식하여 신원을 파악한 후에는 그 사람에 대한 개인인증 과정을 거치도록 하였다. 개인인증을 위한 인식시스템은 잡음이 존재하는 환경에서도 비슷한 얼굴을 구별하여 인식할 수 있도록 변별력이 뛰어나야 한다. 웨이브릿 변환은 대역통과특성을 가지고 있어 영상의 경계선정보를 잘 나타낼 수 있고 특징점 추출에 효과적이다. 따라서 본 연구에서는 웨이브릿 변환을 이용하여 얼굴영상의 특징점을 추출한 후, 추출한 얼굴정보를 광웨이브릿정합필터(optical wavelet matched filter, OWMF) 형태로 데이터베이스에 보관하고, 복원한 얼굴영상과 1:1 광상관을 취함으로써 개인 인증을 할 수 있도록 하였다.

얼굴영상을 $f(x,y)$ 라면 OWMF는

$$W_f(u,v)=F(u,v)^{*}\left|H_a(u,v)\right|^2 \quad (13)$$

와 같다. 여기서 $H_a(u,v)$는 푸리에변환된 웨이브릿 함수로서 본 연구에서는 다음과 같이 정의되는 Mexican-hat 웨이브릿 함수를 사용하였다.

$$H_a(u,v)=4\pi^2 a^2(u^2+v^2)\exp[-2\pi^2 a^2(u^2+v^2)] \quad (14)$$

여기서 a는 축척모수(scaling parameter)로서 그 값은 영상의 특징과 용도에 따라 적절하게 선정하여야 한다.

웨이브릿 함수는 웨이브릿 축척모수의 변화에 따라 대역폭의 크기와 그 중심이 변하는 대역통과필터 특성을 갖게 된다. 대개의 경우 웨이브릿 변환된 영상은 경계선 정보가 강조된 영상으로 웨이브릿 축척모수의 크기와 웨이브릿 함수의 종류에 따라 경계선 강조 효과가 다르다. 그러므로 웨이브릿 변환을 이용하면 각 개인의 얼굴영상에서 특징점을 추출할 수 있으며 잡음이 존재하는 영상에서 잡음의 영향을 최소화 할 수 있다.

얼굴영상의 인식을 위한 광시스템은 그림 1과 같은 4-f 광상관기를 사용한다. 입력평면에는 복원된 얼굴영상을 설치하고 공간주파수영역에 제안한 OWMF를 설치하면, 출력평면에서 상관분포를 얻을 수 있고, 이를 통해 얼굴영상을 인식할 수 있다.

IV. 컴퓨터 시뮬레이션 결과 및 고찰

주민등록증, 운전면허증, 신용카드, 여권, 비밀취급인가증 등 개인의 신원을 증명할 수 있는 신분증의 종류는 여러 가지가 있다. 신분증에 부착되는 신원정보도 얼굴이나 지문, 주민등록번호, 서명(signature), 인장(seal) 등 다양하다. 본 연구에서는 개인신원정보 영상으로 신분증에 부착된 얼굴사진을 스캔한 영상(96×128, gray-scale 영상)과 개인이 갖는 고유한 개인식별번호(220×32, 이진영상)를 임의로 정하여 사용하였다. 제안한 신분인증 시스템은 개인식별번호 영상으로부터 식별번호를 분류 · 인식하여 개인의 신원을 파악한 후, 그 사람의 얼굴정

보와 복원한 얼굴영상을 서로 비교하여 최종적으로 개인의 신분을 인증하게 된다.

4.1. 개인식별번호의 분류 · 인식

개인식별번호의 분류·인식은 제안된 MMACE_p 필터를 사용하며, MMACE 필터를 사용한 경우와 비교하여 제안된 방식이 더욱 효과적임을 보여주고자 한다. 그림 2는 이진영상으로 표현된 220×32 화소의 개인식별번호를 MMACE 필터와 MMACE_p 필터를 사용하여 분류 · 인식할 수 있음을 보여주는 것으로 암호화된 개인식별번호 영상에 잡음이 첨가되지 않은 경우이다. 그림 2(a)는 암호화된 개인식별번호 영상을 복원한 것으로 '0'~'9'의 숫자를 모두 포함하고 있으며, 잡음이 첨가되어 있지 않은 경우이므로 입력영상과 동일하게 나타난다. 그림 2(b)는 그림 2(a)의 개인식별번호를 암호화된 상태에서 분류 · 인식하기 위하여 공간영역에서 암호화된 영상으로, 위상패턴을 256 gray-scale 영상으로 표현한 것이다. 그림 2(c)는 그림 2(a)의 복원영상과 MMACE 필터와의 상관결과로서, 각 부평면들을 440×64 화소의 평면에 겹치지 않게 나타내었다. 그림 2(d)는 그림 2(b)의 암호화된 영상과 제안한 MMACE_p 필터와의 상관결과로서 MMACE 필터의 경우보다 잡음이 적어 인식능력이 향상됨을 확인할 수 있다.

이때 필터의 인식능력은 다음과 같이 정의되는 신호대잡음비(signal-to-noise ratio, SNR)로 평가할 수 있다.

$$\mathrm{SNR}=10\log\frac{r_{max}}{N_{rms}}[\mathrm{dB}] \tag{15}$$

여기서 r_{max}는 상관평면에서 최대상관치이며, N_{rms}는 최대상관치의 50% 이하 신호들의 실효치이다. SNR은 부엽의 크기와 연관이 되어 SNR이 작은 값일 때는 부엽의 크기가 크고, 큰 값이면 부엽의 크기가 작고 예리한 상관첨두치가 나타남을 의미한다. 여기서 MMACE 필터의 경우는 19.6dB이고, MMACE_p 필터의 경우는 21.4dB로서 MMACE_p 필터의 경우가 더 우수함을 알 수 있다.

그림 2의 (e)와 (f)는 각각 그림 2(c)와 (d)의 상관결과를 최대상관치의 50%로 경계값 처리한 후, 4개의 부평면을 분리해서 나타낸 이진영상으로 경계값보다 큰 값은 모두 '1'의 값으로 할당하여 흰 점으로 나타냈다. 여기서 각각의 부평면의 같은 위치에서 출력되는 값을 표 1에서 주어진 코드표와 비교하면 개인식별번호를 정확하게 분류 · 인식할 수 있다. 여기서 4개의 흰 원으로 표시한 위치를 예로 들어 관찰해 보면, 두 필터 모두 각각의 부평면으로부터 '0110'이라는 코드값을 얻고, 이를 코드표와 비교하면 숫자 '6'이라고 인식하게 된다. 나머지 위치에서도 같은 방식으로 살펴보면 다른 숫자들에 대해서도 오인식이 없이 정확하게 인식하고 있음을 확인할 수 있다. 즉, 암호화된 개인식별번호 영상에 잡음이 첨가되지 않은 경우에는 상관출력평면에서 MMACE_p 경우의 SNR이

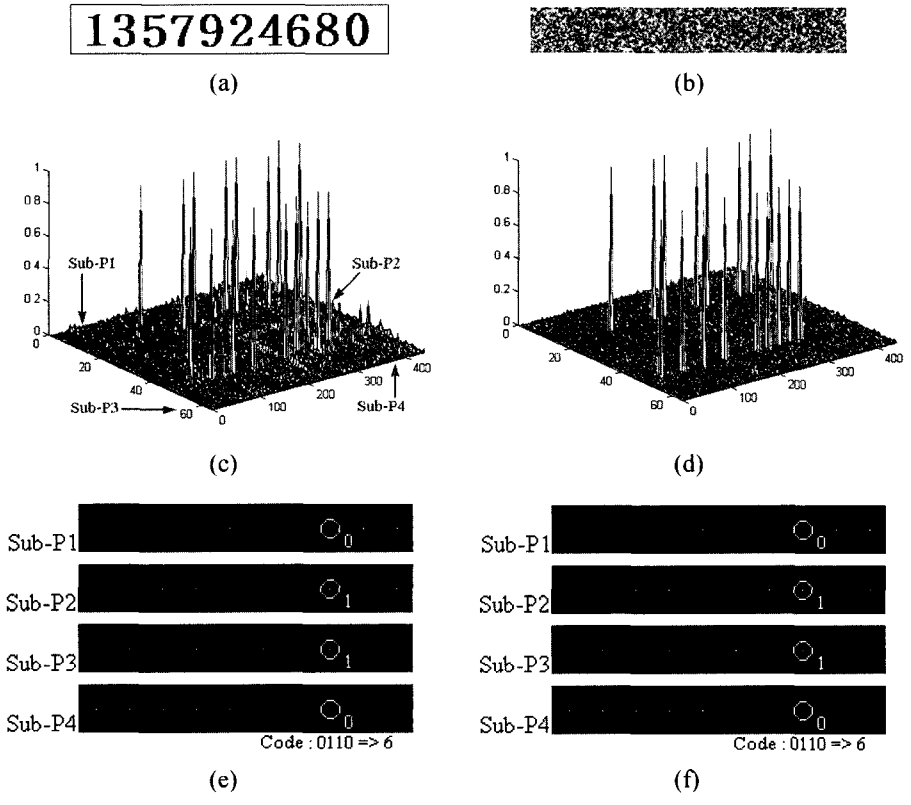

그림 2. 개인식별번호의 인식(잡음이 없는 경우): (a) 복원영상(입력영상과 동일), (b) 암호화된 영상, (c) 복원영상과 MMACE 필터의 상관결과, (d) 암호화된 영상과 MMACE_p 필터의 상관결과, (e) (c)를 문턱화한 결과, (f) (d)를 문턱화한 결과.

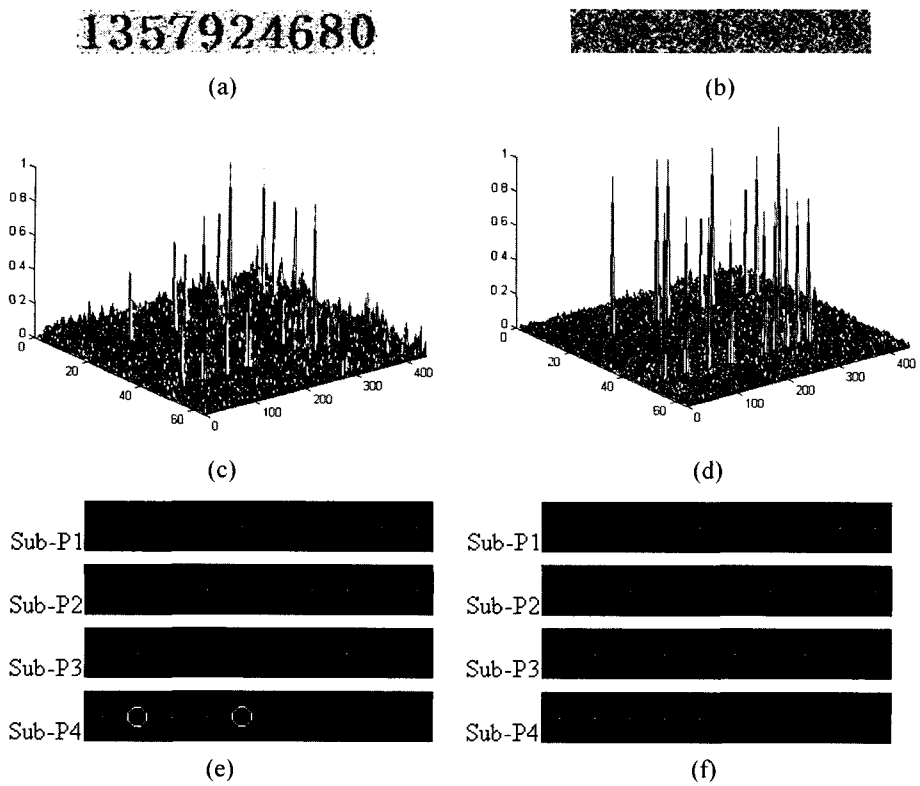

그림 3. 개인식별번호의 인식(표준편차 $\sigma=1$인 잡음이 더해진 경우): (a) 복원영상, (b) 암호화된 영상, (c) 복원영상과 MMACE 필터의 상관결과, (d) 암호화된 영상과 MMACE_p 필터의 상관결과, (e) (c)를 문턱화한 결과, (f) (d)를 문턱화한 결과.

MMACE 경우보다 높아 우수한 특성을 나타내지만 경계값처리를 하면 동일한 출력을 보여 여기서는 그 차이를 말할 수 없다.

그림 3은 암호화된 영상에 백색잡음이 첨가된 경우로서 MMACE_p 필터의 우수성을 분명하게 보여주기 위한 것이다. 그림 3(a)와 (b)는 표준편차 $\sigma=1$인 백색잡음이 더해졌을 때 복원한 영상과 복원되기 전의 암호화된 영상으로 상당량의 재생손실이 발생한 것을 보여주고 있다. 영상을 암호화하고 복원하는 과정에서 발생하는 재생손실은 평균제곱에러(mean squared error, MSE)를 사용하여 표현할 수 있다. 원래의 입력영상을 $f(x,y)$, 복원영상을 $f_r'(x,y)$라면, 영상 암호화 및 복원 과정에서 발생하는 에러 MSE는

$$MSE(|f_r'|)=E\left\{\frac{1}{N\times M}\sum_{x=1}^{N}\sum_{y=1}^{M}[\|f(x,y)|-|f_r'(x,y)\|^2]\right\} \qquad (16)$$

와 같이 정의된다.[5] 여기서 입력영상과 복원영상은 구간 [0,1]의 값을 갖는 N×M 화소의 영상이고, $E\{\cdot\}$는 평균을 의미한다. 그림 3의 경우 재생손실(MSE)은 0.0756 이었다.

그림 3(c)는 MMACE 필터를 사용하여 얻은 상관결과로 상관첨두치들이 많이 감소하고 잡음이 증가한 것을 관찰할 수 있다. 반면에 그림 3(d)의 제안한 MMACE_p 필터를 사용하여 얻은 상관결과는 그림 3(c)와 비교하여 상관첨두치들이 아주 안정되어 있으며 잡음도 적은 것을 알 수 있다. 개인식별번호를 분류·인식하기 위하여 그림 3(c)와 (d)의 상관결과를 경계값처리한 그림 3(e)와 (f)를 관찰해 보면, 부평면 4의 결과가 서로 일치하지 않는 것을 확인할 수 있다. 그림 3(f)의 MMACE_p 필터의 경우는 부평면 4에 '11111 00000'의 정확한 코드를 생성하고 있지만 그림 3(e)의 MMACE 필터의 경우는 '10110 00000'의 부정확한 코드를 생성하고 있다. 즉, MMACE 필터의 경우 잡음의 영향으로 상관첨두치의 값이 낮아져서 코드 '1'로 인식해야 할 부분에서 코드 '0'으로 인식하는 부분이 생기는 것을 알 수 있다. 결국 MMACE 필터의 경우에는 숫자 '3'을 '2'로, 숫자 '9'를 '8'로 오인식하고 있지만 MMACE_p 필터의 경우에는 오인식이 없이 모든 숫자를 정확하게 인식하고 있음을 알 수 있다.

그림 4는 암호화된 영상에 첨가된 백색잡음의 영향에 따른 필터의 성능변화를 보이기 위한 것으로써, 잡음의 표준편차의 변화에 대한 상관출력의 SNR 변화를 나타내었다. 잡음의 표준편차가 증가함에 따라 MMACE 필터와 MMACE_p 필터 모두 SNR이 감소하는 것을 볼 수 있지만 제안한 MMACE_p 필터의 경우가 MMACE 필터의 경우보다 SNR이 높아서 상대적으로 우수한 성능을 가지고 있음을 확인할 수 있다. MMACE 필터를 사용하여 개인식별번호를 분류·인식할 경우는 백색잡음의 표준편차 $\sigma=0.85$ 이상일 때부터 오인식이 발생한 반면, 제안한 MMACE_p 필터를 사용한 경우는 백색잡음의 표준편차 $\sigma=1.75$ 이상일 때부터 오인식이 발생하였다. 여기서 오인식이 발생하는 시점의 SNR이 다른 이유는 SNR은 최대상관치와 최대상관치의 50%이하 신호들의 실효치의 비로 정의되었고, 오인식의 기준은 최대상관치의 50%로 경

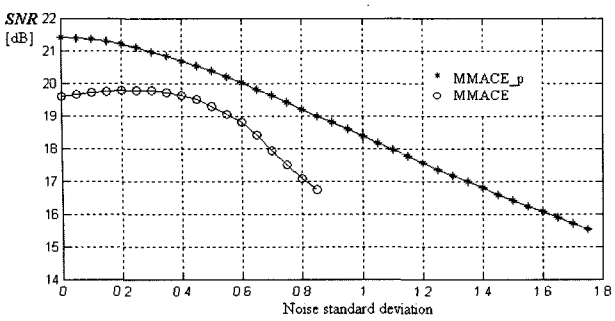

그림 4. 잡음의 표준편차의 변화에 대한 상관출력의 SNR 변화.

계값 처리한 결과를 기준으로 생성한 '1'과 '0'의 코드를 사용하였기 때문이다.

결국 그림 4의 결과는 제안한 MMACE_p 필터가 SNR이 높고 오인식의 가능성이 낮아 MMACE 필터보다 우수한 인식성능을 가지고 있음을 나타내고 있다. 이러한 이유는 단순한 숫자영상을 합성하는 MMACE 필터에 비해 공간영역에서 위상암호화된 학습영상을 합성하는 MMACE_p 필터가 더 많은 정보를 포함하고 있기 때문이다. 그러므로 주민등록번호나 비밀코드와 같이 숫자나 문자의 조합으로 구성되는 개인신원정보는 제안한 영상암호화 방법을 사용하여 암호화한 후 신분증에 부착시키고, 개인의 신분을 인증하는 과정에서는 암호화된 영상을 복원하지 않은 상태에서 신원정보를 인식할 수 있도록 하는 것이 더 효과적임을 알 수 있다.

4.2. 개인 인증

개인 인증은 개인식별번호 인식을 통하여 일차적으로 신원이 파악된 개인의 얼굴정보와 복원한 얼굴영상과의 상관을 통하여 이루어진다. 그림 5(a)는 개인인증을 위한 얼굴영상들로서, 왼쪽부터 순서대로 기준영상, 시험영상1, 시험영상2, 시험영상3, 시험영상4로 사용하였다. 그림 5(b)는 데이터베이스에 OWMF 형태로 저장된 얼굴정보의 임펄스응답으로서, 그림 5(a)의 얼굴영상들을 웨이브릿 변환한 결과이다. 여기서 웨이브릿 변환할 때 축척모수 a는 1로 두었으며 얼굴영상의 경계선 정보를 강조하고 있음을 확인할 수 있다. 그림 5(c)는 암호화된 영상을 복원하면서 잡음에 오염된 경우 인증 가능여부를 검증하기 위하여 사용된 오염된 기준영상의 복원영상들이다. 제일 왼쪽은 잡음이 없는 경우이고, 그 다음부터는 암호화된 영상에 백색잡음이 더해진 경우이다. 여기서 백색잡음의 표준편차(σ)는 각각 0.3, 0.5, 0.7, 1이며, 이때 복원영상에 발생한 재생손

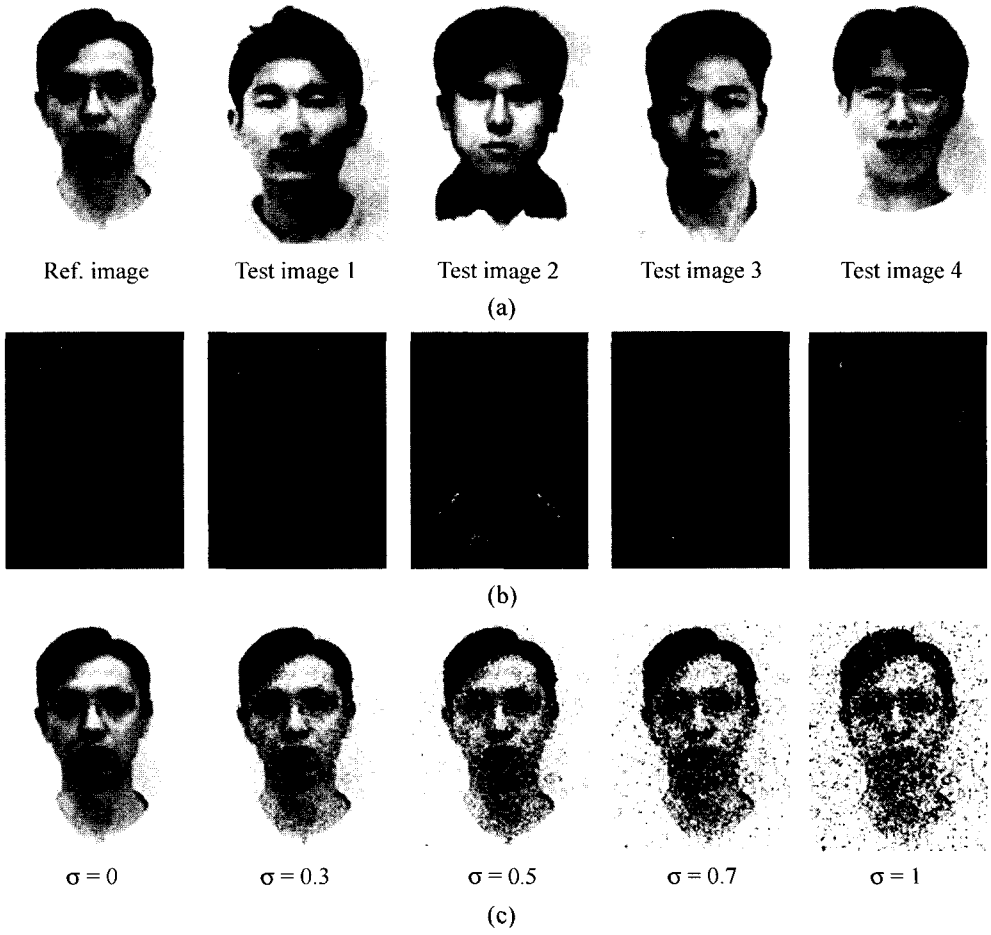

그림 5. 개인 인증을 위한 얼굴영상: (a) 기준영상과 시험영상들, (b) 웨이브릿 변환된 기준영상과 시험영상들, (c) 잡음에 오염된 기준영상의 복원영상.

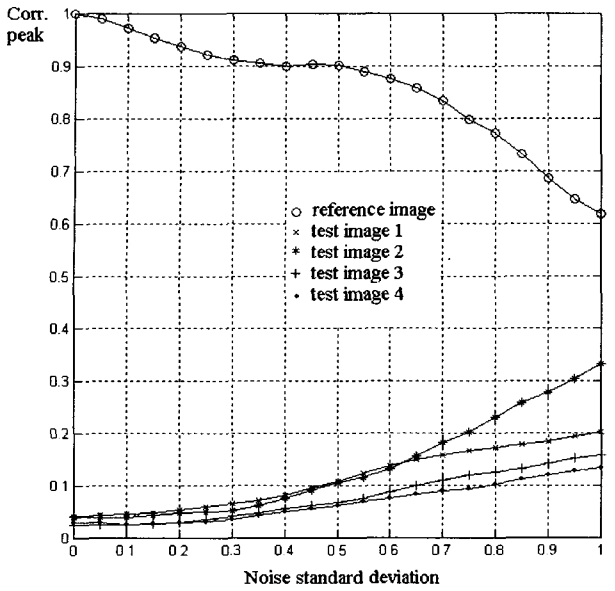

그림 6. 기준영상에 첨가된 백색잡음의 양에 따른 각 얼굴영상들의 상관첨두치의 변화.

실(MSE)은 각각 0.0043, 0.0126, 0.0269, 0.0520 이었다.

그림 6은 복원된 기준영상과 데이터베이스에 OWMF 형태로 저장되어 있는 얼굴영상정보들(기준영상, 시험영상 1, 시험영상 2, 시험영상 3, 시험영상 4)과의 상관첨두치의 변화를 암호화된 기준영상에 첨가된 백색잡음의 정도에 따라 나타내었다. 상관첨두치의 크기는 잡음 없이 복원된 기준영상과 저장되어 있는 기준영상정보와의 상관첨두치를 기준으로 정규화하였다. 복원된 기준영상과 저장되어 있는 기준영상의 상관첨두치가 크다는 것은 복원된 기준영상을 정확하게 인식할 확률이 높다는 것을 의미하고, 복원된 기준영상과 저장되어 있는 시험영상들의 상관첨두치가 크다는 것은 상대적으로 오인식할 확률이 높다는 것을 의미한다.

그림 6의 결과를 분석해 보면 백색잡음의 표준편차가 커짐에 따라 복원된 기준영상과 저장되어 있는 기준영상의 상관첨두치는 감소하는 반면, 복원된 기준영상과 저장되어 있는 시험영상들의 상관첨두치는 오히려 증가하여 오인식할 확률이 높아지고 있음을 알 수 있다. 여기서 기준영상을 정확히 인식하기 위한 상관첨두치의 최소값을 잡음이 없는 경우의 70%로 하고, 시험영상을 오인식하지 않을 상관첨두치의 최대값을 30%로 하면 인식과 오인식사이의 여유가 40%가 되어 인증의 신뢰성을 높일 수 있다. 본 연구에서 사용한 얼굴영상에 대해서는 백색잡음의 표준편차 σ가 0.85 이하일 때, 이 조건을 잘 만족시켜 오인식이 없이 안정적으로 인식할 수 있었다.

V. 결 론

본 연구에서는 개인의 신원정보 보호를 위하여 새로운 광정보보호 시스템을 제안하였다. 제안한 시스템은 개인식별번호와 얼굴영상으로 구성된 신원정보영상을 공간영역과 공간주파수영역에서 랜덤위상패턴을 사용하여 이중으로 암호화하여 위상홀로그램 형태로 신분증에 부착시킨 후, 이를 광학적으로 해독하여 개인인증을 하도록 하였다. 암호화된 신분증의 인증은 일차적으로 개인식별번호를 분류·인식하여 개인의 신원을 확인한 후, 복원된 얼굴영상과 데이터베이스에 저장된 얼굴정보와의 1:1 광상관을 통하여 신분증의 진위여부를 판별하였다.

개인식별번호를 효과적으로 분류·인식하기 위하여 각각의 숫자영상을 공간영역에서 서로 다른 랜덤위상으로 암호화하여 학습영상으로 만들었다. 이는 단순한 숫자영상을 합성하는 MMACE 필터에 비해 공간영역에서 위상암호화된 학습영상을 합성하는 MMACE_p 필터가 더 많은 정보를 포함하고 있어 분리인식 능력을 향상시킬 수 있었기 때문이다. 또한 번호를 복원하지 않고 암호화된 상태에서 인식하여 신원정보의 유출을 막을 수 있었다. MMACE_p 필터로 개인식별번호를 분류·인식하여 신원을 파악한 후에는 OWMF 형태로 데이터베이스에 보관되어 있는 그 사람의 얼굴정보와 복원한 얼굴영상을 서로 비교하여 그 사람에 대한 개인인증을 확증하도록 하였다. 이는 영상의 특징점 추출에 효과적인 웨이브릿 변환을 이용하여 잡음이 존재하는 환경에서도 비슷한 얼굴을 구별하여 인식할 수 있도록 한 것이다.

제안된 광 정보보호 시스템의 타당성을 확인하기 위하여 숫자영상과 얼굴영상에 대한 컴퓨터 시뮬레이션을 수행하였다. 제안된 시스템은 개인식별번호를 암호화된 상태에서 인식하여 신원정보의 유출을 막을 수 있을 뿐만 아니라 1:1 광상관을 통하여 얼굴정보를 인증하므로 인증속도가 빠르고, 신원확인을 이중으로 하므로 부정사용의 가능성을 현저히 줄일 수 있었다. 따라서 제안된 시스템은 각종 금융거래, 신용거래, 보안통제 등의 폭넓은 분야에서 안전하면서도 신속하게 업무를 처리할 수 있는 이점을 제공하리라 기대된다.

감사의 글

이 논문은 2002년도 제주대학교 발전기금 학술연구비(첨단기술연구소)에 의해 연구되었습니다.

참고문헌

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

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

[3] 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.

[4] L. G. Neto, "Implementation of image encryption using the phase-contrast technique," *Proc. of SPIE.*, vol. 3386, pp. 284-290.

[5] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," *Journal of Optical Society of America*, Vol. 16, No. 8, pp. 1915-1927, 1999.

[6] Roberge, D. and Y. Sheng, "Optical wavelet matched filter,"

Appl. Opt. vol. 33, no. 23, pp. 5287-5293, 1994.
[7] J. W. Kim, C. S. Kim, J. K. Bae, Y. H. Doh, and S. J. Kim, "Synthesis of multiplexed MACE filter for optical Korean character recognition," *Journal of KICS*, Vol. 19, No. 12. pp. 2364-2375, 1994.

Optical security system for protection of personal identification information

Jong-Soo Yoon
SK Tech Co., KyungKi 472-905, KOREA

Yang-Hoi Doh†
Department of Electrical and Electronic Engineering, Research Institute of Advanced Technology, Cheju National University, Cheju 690-756, KOREA
†*E-mail: yhdoh@cheju.ac.kr*

(Received December 9, 2002, Revised manuscript June 2, 2003)

A new optical security system for the protection of personal identification information is proposed. Personal identification information consisting of a pure face image and an identification number is used for verification and authentication. Image encryption is performed by a fully phase image encryption technique with two random phase masks located in the input and the Fourier plane of 4-f correlator. The personal information, however, can be leaked out in the decryption process. To cope with this possibility, the encrypted image itself is used in the identification process. An encrypted personal identification number is discriminated and recognized by using the proposed MMACE_p (multiplexed MACE_p) filter, and then authenticity of the personal information is verified by correlation of the face image using the optical wavelet matched filter (OWMF). MMACE_p filter is a synthetic filter with four MACE_p (minimum average correlation energy_phase encrypted) filters multiplexed in one filter plane to recognize 10 different encrypted-numbers at a time. OWMF can improve discrimination capability and SNR (signal to noise ratio). Computer simulations confirmed that the proposed security technique can be applied to the protection of personal identification information.

OCIS Codes : 100.4550. 100.5010. 100. 3010.