碩士學位論文

身分證 僞造防止를 위한 映像暗號化와 個人 認證

濟州大學校 大學院
電氣電子工學科

尹 鍾 壽

2000 年 12 月

身分證 僞造防止를 위한
映像暗號化와 個人 認證

指導敎授 都 良 會

尹 鍾 壽

이 論文을 工學 碩士學位 論文으로 提出함

2000年 12月

尹鍾壽의 工學 碩士學位 論文을 認准함

審査委員長 金 敬 杓

委 員 [illegible]

委 員 都 良 會

濟州大學校 大學院

2000年 12月

Image encryption and identification for anti-counterfeiting of ID card

Jong-Soo Yoon
(Supervised by professor Yang-Hoi Doh)

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Engineering

Department of Electrical and Electronic Engineering
GRADUATE SCHOOL
CHEJU NATIONAL UNIVERSITY

2000. 12.

목 차

Summary

As we enter the 21st century in a world of increasing automation and technology in the areas of financial transactions, licensing, and entry to secure areas, it becomes increasingly important to positively identify individuals. The problems with fraud and counterfeiting continue, with the increase in the digital technology and improvements in low-cost devices such as color printers. So there is a significant demand for fast reliable identification of people and verification of cards and IDs.

In this paper, a new optical security system is proposed. This system not only encrypts the original image into a random-noise-like image but also decrypts the encrypted image and identifies by using 4-f optical correlation system. The encrypted image is made by a fully phase image encryption technique that two random phase masks located in the input and the Fourier plane of 4-f correlator. This encrypted image can be decrypted only when the corresponding phase codes are used for decryption. Personal information, however, can be known because encrypted image is decrypted. Therefore I propose, in this paper, modified fully phase image encryption technique that the encrypted image is used for verifying the identity without decrypting of the encrypted image. In personal identification process, identity is verified from PIN(personal identification number) by using MMACE or MMACE_p filter. And then authenticity of the card is verified by using OWMF(optical wavelet matched filter). MMACE and MMACE_p filter are synthetic filter that four MACE(minimum average correlation energy) filters are multiplexed in one filter plane to recognize the 10 different identification numbers. Computer simulation results show a good performance of the proposed optical security technique.

Ⅰ. 서 론

컴퓨터와 정보통신의 발달로 사회는 점점 복잡해지고 급속한 정보교류가 필요하게 되었다. 또한 초고속 정보망과 이동전화 보급의 확대는 사람의 생활반경을 점점 넓히고 있다. 특히 인터넷쇼핑과 홈쇼핑 같은 전자상거래에 신용카드를 이용하여 원격지에서 물건의 구매가 가능해지고 있으며, 텔레뱅킹을 이용한 금융거래 서비스가 보편화되고 있다. 이러한 멀티미디어 정보사회에서는 개인의 정보와 신용이 중요시되고, 여권이나 신용카드와 같은 개인의 신원을 증명할 수 있는 신분증의 사용이 증가할 것이다. 그러나 프린터, 스캐너, 복사기, 컴퓨터 관련 장치들과 각종 소프트웨어 기술의 발달로 복제기술이 향상됨에 따라 신용카드나 여권, 지폐 등의 위조가 심각한 사회문제가 되고 있다. 이런 문제를 해결하기 위해서 현재는 엠보싱 홀로그램이 부착된 각종 신용카드와 여권이 사용되고 있으나, 이것도 광세기 검출기를 이용하면 마스터 홀로그램의 합성 및 대량 복제가 가능하다. 그래서 단순하면서도 광의 장점을 이용할 수 있고, 어떠한 경우에도 카드의 위조나 복제를 근본적으로 차단할 수 있는 새로운 방법에 대한 연구가 계속되고 있다.

기존의 광학적 영상암호화 방법들은 암호화된 영상이 복원되는 경우로 개인의 신분을 인증하기 위하여 복원영상이 필요한 경우에 사용된다. 예를 들면, 복원한 얼굴영상과 신분증을 제시한 사람의 얼굴을 육안으로 확인하거나 복원한 얼굴영상을 데이터베이스에 있는 본인의 얼굴정보와 서로 비교하거나, 또는 복원한 개인식별번호 영상을 이용하여 신분증을 제시한 사람의 식별번호를 질의응답 하는 등과 같이 복원영상이 이용되는 경우이다. 그러나 이 경우 암호화된 개인신원정보 영상을 복원하므로 인해 개인의 신원정보가 유출될 소지가 있어 신용카드나 비밀취급인가증 등의 비밀코드처럼 보안을 요하는 곳에 사용하기에는 부적합하다. 그러므로 암호화된 영상을 복원하더라도 개인의 신원정보를 육안으로 식별할 수 없도록 하거나, 암호화된 영상을 복원하는 과정 없이 인식시스템에서만 신원을 확인할 수 있도록 해야 한다(Refregier 등 1995), (Neto, 1998), (Towghi 등 1999).

모든 인식시스템이 그러하듯이, 주어진 인식환경에 적절하면서도 처리시간이 크게 요구되지 않아야 좋은 인식시스템이라 할 수 있다. 광상관 필터를 이용하여 개인 인증을 하기 위해서 인식필터는 다음과 같은 특성을 갖는 것이 바람직하다. 즉, 비슷한 얼굴일 경우에 발생하는 부엽(sidelobe)의 크기를 감소시킬 수 있도록 변별력이 뛰어나야 되고, 개인식별번호(personal identification number) 영상처럼 숫자로 근접하게 구성된 영상으로부터 식별번호를 구별 인식해야 되고, 잡음이 존재하는 경우에도 무관하게 인식할 수 있어야 하며, 인식시스템의 규모는 가능한 한 작으면서 실시간으로 인식할 수 있어야 한다. 앞에서 언급한 특성을 대체적으로 만족하는 기존의 광 상관필터에는 MACE(minimum average correlation energy) 필터와 웨이브릿 변환을 이용한 광 웨이브릿 정합필터(optical wavelet matched filter, OWMF), MMACE(multiplexed MACE) 필터 등이 있다(Mahalanobis 등 1987), (Roberge 등 1993), (Kim 등 1994). MACE 필터는 공간주파수 영역에서 평균 상관에너지를 최소로 하여 예리한 상관첨두치를 얻을 수 있고, 부엽의 효과가 작어 우수한 변별력을 갖는다. 그러나 숫자로 구성되는 개인식별번호 영상으로부터 식별번호를 분류·인식하기 위해서는 10개의 MACE 필터가 필요하게 되고 정합횟수도 많아지게 된다. 한편, 비슷한 얼굴을 분리인식하기 위해서는 얼굴영상의 특징점(feature)을 효과적으로 추출할 수 있어야 하고, 변별력이 뛰어나야 한다. Mallat(1989)에 의해 웨이브릿 변환이 발표된 후, 웨이브릿 변환을 이용한 영상신호처리가 활발히 연구되고 있는데, 웨이브릿 함수는 그 종류 및 웨이브릿 축척모수(wavelet scale parameter)에 따라 대역의 중심주파수와 대역폭이 달라지므로 영상의 특징점 추출이 용이하다.

본 논문에서는 개인의 신원정보 보호를 위한 새로운 영상암호화 방법과 광 정보보호 시스템을 제안하였다. 제안한 시스템은 개인의 신원정보 영상을 공간영역과 공간주파수영역에서 이중으로 암호화한 후, 위상홀로그램 형태로 신분증에 부착시킴으로써 기존의 카드 위조 및 복제에 따른 사고를 예방할 수 있을 뿐만 아니라 육안으로는 암호화된 개인의 신원정보 영상을 식별이 불가능하여 개인의 신원정보 보호도 가능하다. 또한 암호화된 신분증을 사용할 때는 신분증의 진위 여

부 판별과 개인의 신분을 인증하는 과정을 거치도록 하였는데, 암호화된 영상이 복원되어 개인의 신원정보가 타인에게 보여져도 문제가 되지 않는 경우나 복원한 영상을 이용하여 육안으로도 신분확인이 필요한 경우는 기존의 Towghi 등이 제안한 영상의 위상암호화 방법을 사용하여 개인의 신원정보를 암호화하였다. 반면, 비밀코드처럼 보안을 요하는 경우나 개인의 신원정보가 타인에게 보여져서는 안 될 경우는 Towghi 등이 제안한 위상암호화 방법을 수정하여 복원영상 없이 인식 시스템에서 신원확인이 이루어지도록 하였다.

암호화된 신분증을 사용할 때 이루어지는 개인의 신분인증은 먼저 개인식별번호를 분류·인식하여 개인의 신원을 파악한 후, 데이터베이스에 등록된 그 사람의 얼굴정보와 복원한 얼굴영상을 서로 비교하여 이루어지도록 하였다. 개인 인증 시스템의 규모와 정합횟수를 줄이기 위해 하나의 필터평면에 4개의 MACE 필터를 다중화 시키는 MMACE 필터로 사용하여 복원한 개인식별번호 영상으로부터 식별번호를 효과적으로 분류·인식하여 개인의 신원을 파악할 수 있도록 하였다. 반면, 암호화된 개인식별번호 영상을 복원하지 않고도 식별번호를 분류·인식할 수 있도록 하기 위하여 MMACE_p 필터를 제안하였다. MMACE_p 필터는 공간영역에서 위상암호화된 숫자영상을 합성한 필터로 단순히 숫자영상을 합성하는 MMACE 필터보다 더 많은 정보를 포함하게 되어 신호대잡음비와 인식률을 향상시킬 수 있다. 그리고 데이터베이스에 저장되는 얼굴정보는 OWMF의 임펄스응답을 의미하며, 잡음이 존재하는 환경에서도 비슷한 얼굴을 구별 인식할 수 있도록 웨이브릿 변환을 이용하여 얼굴영상의 특징점들을 추출하였다.

제안한 시스템은 간단하면서도 기존의 카드 위조 및 복제에 따른 사고를 예방할 수 있고, 개인의 신분인증 과정을 거치므로 현금자동입출금(ATM)기기, 금융거래, 출입통제, 기타 보안통제 등과 같은 폭넓은 분야에서 보다 안전하게 업무를 자동적으로 처리할 수 있는 이점을 제공하리라 기대된다. 컴퓨터 시뮬레이션을 통해 제안한 영상암호화 및 보안 방법이 개인정보 보호 및 인증시스템에 유용함을 확인하였다.

Ⅱ. 광상관 필터

개인의 신원정보 보호를 위해서 신분증에 부착되는 신원정보영상을 암호화 및 복원하고, 개인의 신분을 인증하는 일련의 과정들이 4-f 광 상관시스템에서 이루어지는 방법을 제안하였다. 홀로그램 형태로 신분증에 부착되는 신원정보영상은 공간영역(space domain)과 공간주파수영역(spatial frequency domain)에서 이중으로 암호화된 복소(complex) 위상영상이므로 복제가 거의 불가능할 뿐만 아니라 육안으로는 식별할 수 없으므로 개인정보 보호에도 유용하다.

개인의 신분인증은 광상관 필터를 사용하여 이루어지는데, 광을 이용한 신호처리는 렌즈를 기본으로 하는 광학시스템의 2차원적 푸리에 변환 능력을 이용하여 2차원 영상의 인식 및 분류에 유리한 기능을 제공한다(Vander Lugt, 1964). 광신호는 각기 상호작용이 없이 독립적이고 병렬적으로 전파될 수 있어 2차원 신호를 광속으로 처리하는 고속 병렬처리 특성을 갖고 있으며, 꾸준한 광소자들의 개발로 인해 초고속 신호처리가 가능해지고 있다. 이러한 광 신호처리의 장점을 이용한 광상관 필터의 종류로는 고전적 정합필터(classical matched filter, CMF), 위상성분만 포함하는 위상필터(phase only filter, POF), 공간영역에서 학습영상들을 합성하는 SDF(synthetic discriminant function) 필터, 공간주파수영역에서 학습영상들을 합성하는 MACE 필터, 웨이브릿 변환을 이용한 OWMF 등이 있다.

1. 공간정합필터

임의의 신호에 섞여 있는 특정 신호만을 찾고자 할 때 유용하게 사용되는 정합필터는 패턴 인식에서도 중요한 역할을 한다. 선형 공간불변 필터(linear space-invariant filter)의 임펄스 응답 $h(x,y)$가 특정신호 $s(x,y)$에 정합되었다고 할 때

$h(x,y)$는

$$h(x,y) = s^*(-x,-y) \tag{1}$$

를 만족하고, 임의의 입력신호 $f(x,y)$가 특정신호 $s(x,y)$와 정합되는 정도를 측정하기 위해 이 필터에 $f(x,y)$가 입력될 때 상관출력 $o(x,y)$는

$$\begin{aligned} o(x,y) &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(\xi,\eta)h(x-\xi,y-\eta)d\xi d\eta \\ &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(\xi,\eta)s^*(\xi-x,\eta-y)d\xi d\eta \end{aligned} \tag{2}$$

이 된다. 이 식을 공간주파수영역으로 나타내면

$$\begin{aligned} O(u,v) &= F(u,v)H(u,v) \\ &= F(u,v)S^*(u,v) \end{aligned} \tag{3}$$

이 된다. 여기서 공간주파수영역의 함수 $O(u,v)$, $F(u,v)$, $H(u,v)$ 및 $S(u,v)$는 각각 공간영역의 함수 $o(x,y)$, $f(x,y)$, $h(x,y)$ 및 $s(x,y)$의 푸리에 변환이다. 따라서 상관영역에서의 출력 $o(x,y)$는

$$o(x,y) = \mathcal{F}^{-1}[F(u,v)H(u,v)] \tag{4}$$

이 된다. 이러한 일련의 상관작용을 광학적으로 실현하기 위한 기본적인 광 상관기의 구성은 그림 1과 같으며, Vander Lugt가 처음으로 홀로그램방식을 이용한 광학시스템으로 정합필터를 구현하였다.

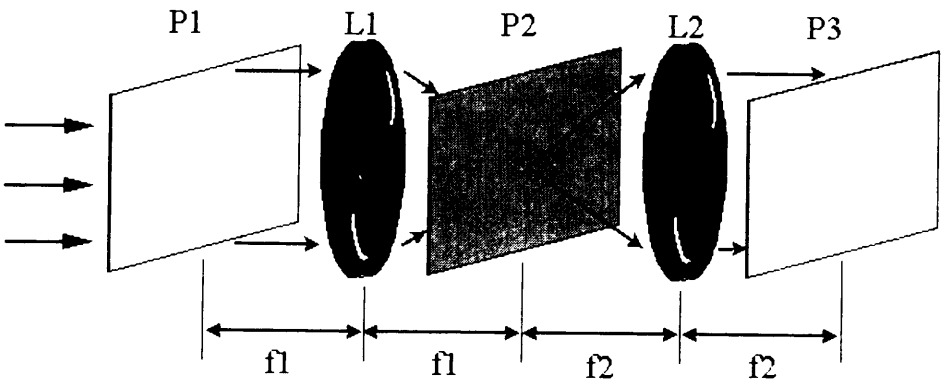


Fig. 1. Schematic diagram of Vander Lugt optical correlator.

그림에서 P1은 입력평면, P2는 공간주파수평면, 그리고 P3은 상관출력평면으로 볼록렌즈 L1 및 L2의 전후 초점면에 각각 위치하게 된다. 볼록렌즈 L1의 전 초점면인 P1 평면에 입력신호 $f(x,y)$가 설치되고 코히어런트(coherent)한 평면파(plane wave)가 입사되면 광의 회절특성과 렌즈의 위상 변환 특성에 의해 렌즈 L1의 후 초점면인 P2 평면에는 $f(x,y)$의 푸리에 변환된 신호 $F(u,v)$가 출력된다. 한편 P2 평면에 인식하고자 하는 특정신호 $s(x,y)$의 푸리에 변환된 함수의 공액 복소함수 $S^*(u,v)$, 즉, 광상관 필터 $H(u,v)$를 설치하면 렌즈 L2의 후 초점면 P3 평면에는 $F(u,v)$와 $H(u,v)$가 곱해진 함수의 푸리에 변환된 결과가 출력되며, 이는 입력신호 $f(x,y)$와 특정신호 $s(x,y)$의 상관결과인 $o(x,y)$가 된다.

이 때 광 상관기의 특성은 신호대잡음비(signal-to-noise ratio, SNR) 등으로 평가할 수 있는데, 다음과 같이 정의된다(Yang 등 1992).

$$\mathrm{SNR} = 10\log\frac{r_{max}}{N_{rms}} \quad [\mathrm{dB}] \tag{5}$$

r_{max} : 최대상관치, N_{rms} : 최대상관치의 50% 이하 신호들의 실효치

SNR은 상관 분포에서 최대상관치와 잡음의 비로써, 이는 부엽의 크기와 연관이 되어 SNR이 작은 값일 때는 부엽의 크기가 크고, 큰 값이면 부엽의 크기가 작고 예리한 상관첨두치가 나타남을 의미한다.

CMF의 전달함수는 인식대상이 되는 기준함수 $f(x,y)$를 푸리에 변환한 후, 공간주파수영역에서 진폭성분과 위상성분으로 분리하여 위상성분의 복소공액을 취하여 얻은 것으로

$$H_{\mathrm{CMF}}(u,v) = |F(u,v)|\exp[-j\varphi(u,v)] \tag{6}$$

와 같이 나타낼 수 있다. CMF는 입력의 위치정보를 보존하는 특성을 갖고 있기 때문에 입력의 변위에 비례해서 상관영역에서의 변위가 나타나므로, 입력영상 내에서 각 집단의 위치가 중요한 역할을 하는 대상의 인식에 유용하다. 그러나 진폭정보와 위상정보를 함께 갖는 필터는 일반적으로 공간주파수영역에서 고주파 성분의 에너지가 급격하게 감쇠하므로 입력영상의 경계선 정보가 많이 상실된다. 따라서 상관첨두치가 작을 뿐만 아니라 부엽의 크기가 커서 비슷한 모양의 입력을 구별 인식하지 못한다. 이는 주로 높은 주파수영역에서의 에너지 감쇠에 기인하므로 이를 보상해 줄 필요가 있다.

공간주파수영역에서 위상정보는 진폭정보보다 더 중요한 요소가 되며, 위상정보만 포함하는 POF의 전달함수는

$$H_{\mathrm{POF}}(u,v) = \exp[-j\varphi(u,v)] \tag{7}$$

로 쓸 수 있다(Horner 등 1984). 즉, POF는 CMF에 $1/|F(u,v)|$이 곱해진 형태로 $1/|F(u,v)|$는 고역통과 필터의 특성을 나타낸다. 이는 높은 공간주파수영역에서의 에너지 감쇠를 보상해주므로 입력영상의 경계선 정보를 강조하게 된다. 따라서 상관첨두치가 매우 크고 예리하며, 부엽의 크기도 작아서 비슷한 모양의 근접한 입력영상 인식에 매우 유용하게 적용될 수 있다. 그러나 인식하고자 하는 영상의 왜

곡에 대해서는 민감한 결과를 가지므로 개인 인증을 위한 인식시스템에 사용하기에는 부적합하다. 이러한 단점을 보상하기 위하여 Casasent(1984)는 학습영상들을 공간영역에서 선형 조합하여 합성한 SDF 필터를 제안하였다. SDF 필터는 크기나 회전과 같은 왜곡에 무관한 상관 특성을 얻을 수 있으나, 학습영상들의 에너지 분포에 따라 상관첨두치가 달라지고, 무시 못할 부엽이 발생하므로 숫자로 근접하게 구성되는 개인식별번호의 인식 및 비슷한 얼굴을 구별 인식해야 하는 개인 인증을 위한 인식시스템에는 부적절하다.

MACE 필터는 SDF 필터와는 달리 학습영상들의 선형조합을 공간주파수영역에서 수행하고 필터계수를 Lagrange 승수를 이용하여 출력 상관 평면상에서의 상관첨두치를 임의로 제어함과 동시에 부엽의 크기가 최소화되도록 합성한 최적의 선형조합 필터이다. 이렇게 합성된 MACE 필터는 전처리과정이 필요없고, 그 성능이 아주 뛰어나 숫자로 근접하게 구성되는 개인식별번호 인식에 적합하다. 한편, 웨이브릿 변환은 대역통과특성을 가지고 있어 영상의 경계선정보를 잘 나타낼 수 있고 특징점 추출에 효과적이다. 웨이브릿 변환을 광학적으로 구현하는 것을 광 웨이브릿 변환이라 하며, 웨이브릿 변환을 이용하는 OWMF는 전처리과정 없이도 입력영상에 웨이브릿 변환 효과를 줄 수 있으므로 기존의 정합필터에 비해 변별력과 SNR을 개선할 수 있다.

2. MMACE 필터

개인의 신분을 확인하기 위한 인식시스템은 규모가 가능한 한 작으면서도 숫자로 근접하게 구성된 개인식별번호를 신속하게 분류·인식할 수 있어야 한다. MACE 필터는 출력상관평면에서의 상관첨두치를 임의로 제어함과 동시에 부엽의 크기가 최소화되도록 합성한 최적의 선형조합 필터이다. 그러나 숫자로 구성되는 개인식별번호 영상으로부터 식별번호를 분류·인식하기 위해서는 10개의 MACE

필터가 필요하게 되고 정합횟수도 많아지게 된다. 따라서 개인 인증 시스템의 규모와 정합횟수를 줄이기 위해 하나의 필터평면에 4개의 MACE 필터를 다중화 시키는 MMACE 필터로 개인식별번호를 효과적으로 분류·인식하여 개인의 신원을 파악할 수 있는 방법을 제안하였다. 4개의 MACE 필터들의 위상을 공간주파수 변조한 다음 하나의 필터에 합성하는 MMACE 필터는

$$H_{\mathrm{MMACE}}(u,v) = \sum_{i=1}^{4} H^{*}_{\mathrm{MACE},i}(u,v)\exp[-j2\pi(a_i u + b_i v)] \tag{8}$$

와 같다. 여기서 a_i와 b_i는 상관결과의 분리정도를 정해주기 위한 변수로써, a_i와 b_i의 설정에 의해서 상관결과가 중첩되지 않게 합성할 수 있다.

여기에 사용된 MACE 필터의 합성원리는 다음과 같다. 학습영상의 수를 N_T라 할 때, i번째 학습영상인 $f_i(x,y)$와 필터의 임펄스응답 함수 $h(x,y)$에 의한 출력상관 함수 및 상관에너지는

$$o_i(x,y) = f_i(x,y) \bigstar h(x,y) \tag{9}$$

$$\begin{aligned} E_i &= \sum_{x=1}^{d}\sum_{y=1}^{d} |o_i(x,y)|^2 \\ &= \sum_{u=1}^{d}\sum_{v=1}^{d} |H(u,v)|^2 |F_i(u,v)|^2 \\ &= \sum_{u=1}^{d}\sum_{v=1}^{d} |H(u,v)|^2 D_i(u,v) \end{aligned} \tag{10}$$

와 같다. 여기서 ★는 상관자(correlation operator)이며, 이 식에서 $F_i(u,v)$ 및 $H(u,v)$를 각각 열벡터 $\mathbf{F}_i$와 $\mathbf{H}$로 표현하고, 학습영상들을 벡터행렬 표기법으로

$$\mathbf{F} = [\,\mathbf{F}_1\ \mathbf{F}_2\ \mathbf{F}_3\ \cdots\ \mathbf{F}_{N_T}\,] \tag{11}$$

라 한다면 식 (10)은

$$\mathbf{E}_i = \mathbf{H}^+ \mathbf{D}_i \mathbf{H} \tag{12}$$

로 표현된다. 여기서 +는 복소공액전치(complex conjugate transpose) 변환을 나타내고, $\mathbf{D}_i$는 i번째 학습영상의 에너지 스펙트럼을 갖는 대각행렬이다. 그리고 백터표기법에 의한 학습영상들과 필터와의 출력상관 첨두치는

$$\mathbf{F}^+ \mathbf{H} = \mathbf{u} \tag{13}$$

로 나타나며, 여기서 제한백터 $\mathbf{u}$는 상관첨두치를 원하는 비율로 제한하는 역할을 한다. 그리고 평균상관에너지는

$$E_{av} = \mathbf{H}^+ \mathbf{D} \mathbf{H} \tag{14}$$

로 주어진다. 여기서 $\mathbf{D}$는 모든 학습영상들의 평균 에너지 스펙트럼을 갖는 대각행렬이다. 출력상관평면에서 원하는 상관첨두치를 갖고 부엽을 최소화하기 위해서는 식 (13)의 제한조건을 만족하면서, 식 (14)의 평균 상관에너지를 최소화하는 필터함수 $\mathbf{H}$를 구하면 된다. MACE 필터는 Lagrange 승수법을 이용하여 구한 최적의 선형조합 필터로, 필터함수 $\mathbf{H}_{\mathbf{MACE}}$는

$$\mathbf{H}_{\mathbf{MACE}} = \mathbf{D}^{-1}\mathbf{F}[\mathbf{F}^+ \mathbf{D}^{-1}\mathbf{F}]^{-1}\mathbf{u} \tag{15}$$

와 같다. 이렇게 합성된 MACE 필터는 전처리과정이 필요 없고, 부엽의 효과가 적어 우수한 변별력을 갖는다.

3. OWMF

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

웨이브릿 변환은 다해상도 영상분해 및 영상압축에 많이 이용되며, 광을 이용한 웨이브릿 변환도 많이 연구되어 Sheng 등(1993)에 의해 광학적 패턴인식 분야에 적용되기 시작하였다. 웨이브릿 변환을 광학적으로 구현하는 것을 광 웨이브릿 변환이라 하며, 임의의 영상 $f(x,y)$의 광 웨이브릿 변환 $w_f(a,x,y)$는

$$w_f(a,x,y) = f(x,y) \star h_a(x,y) \tag{16}$$

와 같이 정의된다. 여기서 a는 웨이브릿 축척모수로 양의 값을 가지며, $h_a(x,y)$는 등방성인 딸웨이브릿(daugther wavelet) 함수로 모웨이브릿(mother wavelet) 함수의 축척(scale)으로부터 얻을 수 있다. 함수 $h_a(x,y)$는

$$h_a(x,y) = \frac{1}{a} h\left(\frac{x}{a}, \frac{y}{a}\right) \tag{17}$$

와 같고, 식 (16)과 같이 표현된 웨이브릿 변환을 공간주파수영역에서 나타내면

$$W_f(u,v) = F(u,v)\ H^*_a(u,v) \tag{18}$$

와 같다. 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. 이의 효과를 높이는 것은 영상의 적절한 특징점 추출을 의미하며 이는 패턴인식에 중요한 영향을 미치므로 영상에 따른 적절한 웨이브릿 함수와 웨이브릿 축척모수의 선정이 중요하다. 광을 이용한 패턴인식에 주로 사용되고 있는 웨이브릿 함수로는 Haar, Morlet 및 Mexican-hat 웨이브릿 함수 등이 있다(Marr and Hildreth, 1980), (Martinet 등 1987), (Sheng 등 1992), (Yang 등 1992), (Szu 등 1992), (Burns 등 1992), (이 등 1995).

OWMF는 기준영상의 복소공액에 푸리에 변환된 웨이브릿 함수의 제곱을 곱한 것으로, 입력영상의 웨이브릿 변환을 위한 웨이브릿 함수를 포함하고 있어 전처리 과정 없이도 입력영상에 웨이브릿 변환 효과를 가지며 광 상관기에 적용하여 패턴인식에 이용할 수 있다. 입력영상을 $f(x,y)$라 하고 기준영상을 $r(x,y)$라고 할 때 공간주파수영역에서의 입력영상과 기준영상과의 상관은

$$\begin{aligned} O(u,v) &= W_f(u,v)\ W^*_r(u,v) \\ &= F(u,v)\ R^*(u,v)\,|H_a(u,v)|^2 \end{aligned} \tag{19}$$

로 주어진다. 여기서 $F(u,v)$를 제외한 항은

$$H_{\mathrm{OWMF}}(u,v) = R^*(u,v)\,|H_a(u,v)|^2 \tag{20}$$

와 같으며, $H_{\mathrm{OWMF}}(u,v)$를 OWMF라 한다. 출력상관평면에서의 결과는 식 (20)을 역 푸리에 변환한 것으로

$$
\begin{aligned}
o(x,y) &= \mathcal{F}^{-1}\{O(u,v)\} \\
&= \mathcal{F}^{-1}\{W_1(u,v)\} \star \mathcal{F}^{-1}\{W_2(u,v)\}
\end{aligned}
\tag{21}
$$

와 같다. 이 식으로부터 OWMF에 의한 상관은 웨이브릿 변환된 영상간의 상관과 같음을 알 수 있다. 따라서 OWMF는 기존의 정합필터에 비해 변별력과 SNR을 개선할 수 있어 비슷한 얼굴영상의 구별 인식에 유용하게 사용될 수 있다.

Ⅲ. 개인신원정보의 암호화와 복원

개인의 신원정보 보호를 위해서 본 논문에서 제안한 방법은 암호화된 신원정보 영상을 홀로그램 형태로 신분증에 부착시키고, 신분증을 사용할 때에는 암호화된 홀로그램 패턴을 광학적으로 해독하여 실제 정보와 비교함으로써 개인 인증을 하는 방법이다. 개인신원정보 영상의 암호화는 공간영역과 공간주파수영역에서 이중으로 이루어지며, 암호화된 영상은 복소 위상영상으로 복제가 거의 불가능하고 육안으로는 식별할 수 없게 된다.

기존의 광학적 영상암호화 방법들을 살펴보면, Refregier 등(1995)은 4-f 광 상관시스템을 이용하여 입력평면과 주파수평면에 랜덤위상패턴을 사용하여 영상을 암호화하고, 동일한 시스템을 이용하여 원래의 입력영상을 복원하는 방법을 제안하였다. 이 방법은 기존의 영상암호화 방법 중 응용가능성이 가장 높고 많이 연구되어지고 있다. 그러나 암호화된 영상에 잡음이 있는 경우에는 복원영상의 재생손실이 비교적 크다. Neto(1998)는 4-f 광 상관시스템의 주파수평면에 중심이 유전체로 코팅된 유리판을 사용하고, 입력영상을 진폭값에 비례하는 위상값으로 바꾸어 랜덤위상패턴과 함께 암호화하고, 영상을 복원할 때는 암호화과정에 사용된 랜덤위상패턴의 복소공액 값을 가진 패턴을 입력평면에 사용하는 위상-세기(phase-contrast) 방법을 제안하였다. 이 방법 역시 세기에 비례하는 위상값의 근사식에 대한 에러가 복원영상의 왜곡으로 나타난다. Han 등(1999)은 256 그레이 레벨을 갖는 입력영상을 각 비트 평면으로 나누어 8개의 이진영상들을 얻은 후 이들을 각각 암호키와 XOR 연산을 수행함으로써 영상을 암호화하는 방법을 제시하였다. 그러나 이 방법은 영상을 이진 비트 평면 영상으로 변환해야 하기 때문에 시스템이 복잡하고 그 크기가 커지게 된다. 한편, Towghi 등이 제안한 영상의 위상암호화 방법은 4-f 광 상관시스템에서 이루어지기 때문에 시스템이 간단하고, Refregier 등이 제안한 영상암호화 방법과 XOR 연산에 의한 영상암호화 방법에 비해 재생손실이 적다는 장점을 가지고 있다(Towghi 등 1999), (Javidi 등 1999).

위의 방법들을 사용하여 개인의 신원정보 영상을 암호화한다면, 개인의 신분을 인증하기 위해서는 암호화된 영상을 복원하는 과정을 거친 후, 복원한 영상을 직접 육안으로 확인하거나 데이터베이스에 보관된 정보와 서로 비교해야 한다. 그러나 이 경우 암호화된 개인신원정보 영상을 복원하므로 인해 개인의 신원정보가 유출될 소지가 있어 신용카드나 비밀취급인가증 등의 비밀코드처럼 보안을 요하는 곳에 사용하기에는 부적합하다. 그러므로 암호화된 영상을 복원하더라도 개인의 신원정보를 육안으로 식별할 수 없도록 하거나, 암호화된 영상을 복원하는 과정 없이 인식시스템에서만 신원을 확인할 수 있도록 해야 한다.

따라서 본 논문에서는 암호화된 영상이 복원되어 개인의 신원정보가 타인에게 보여져도 문제가 되지 않는 경우나 복원영상을 이용하여 육안으로도 신분확인이 필요한 경우는 Towghi 등이 제안한 영상의 위상암호화 방법을 사용하여 신원정보영상을 암호화하였다. 반면, 비밀코드처럼 보안을 요하는 경우나 개인의 신원정보가 타인에게 보여져서는 안될 경우는 위상암호화 방법을 수정하여 복원영상 없이 인식시스템에서 신원확인이 이루어지도록 하였다.

1. 영상의 위상암호화 방법

Towghi 등이 제안한 영상의 위상암호화는 정규화된 입력영상을 위상패턴으로 변환 후, 공간영역에서 랜덤위상패턴을 사용하여 암호화하고, 다시 공간주파수영역에서 또 다른 랜덤위상패턴을 사용하여 암호화한다. 암호화하고자 하는 입력영상을 $f(x,y)$라 하면, 입력영상이 위상패턴으로 변환된 신호 $c(x,y)$는

$$c(x,y) = \exp[j\pi f(x,y)] \tag{22}$$

처럼 표현되고, 위상의 범위는 구간 $[0,\pi]$의 값을 갖는다. 그리고 $p(x,y)$와 $b(u,v)$는

구간 [0,1]에서 균일한 확률분포를 갖는 서로 독립인 랜덤한 잡음(uniformly distributed random noise)이며, 각각 위상패턴으로 변환된 신호 $q(x,y)$, $H(u,v)$는

$$q(x,y) = \exp[j2\pi p(x,y)]$$
$$H(u,v) = \exp[j2\pi b(u,v)] \tag{23}$$

와 같이 표현된다. 여기서 $q(x,y)$는 공간영역에서의 랜덤위상패턴을 의미하고, $H(u,v)$는 공간주파수영역에서의 랜덤위상패턴을 의미한다.

입력영상의 위상암호화 과정은 먼저, 위상패턴으로 변환된 입력영상인 $c(x,y)$와 공간영역에서의 랜덤위상패턴인 $q(x,y)$가 곱해지고, 푸리에 변환된 후 공간주파수영역에서의 랜덤위상패턴인 $H(u,v)$와 곱해진다. 마지막으로 암호화된 영상은 역푸리에 변환을 통해 얻어진다. 암호화된 영상 $\varphi_p(x,y)$는

$$\begin{aligned}\varphi_p(x,y) &= \mathcal{F}^{-1}[\mathcal{F}\{c(x,y)q(x,y)\}H(u,v)] \\ &= \{c(x,y)\ q(x,y)\} \otimes h(x,y) \\ &= \{\exp[j\pi f(x,y)]\ \exp[j2\pi p(x,y)]\} \otimes h(x,y)\end{aligned} \tag{24}$$

와 같다. 여기서 $\otimes$는 콘볼루션(convolution) 연산자이고, $h(x,y)$는 전달함수 $H(u,v)=\exp[j2\pi b(u,v)]$의 임펄스 응답이다.

암호화된 영상의 복원 과정은 암호화의 역 과정으로, 암호화된 영상 $\varphi_p(x,y)$가 푸리에 변환된 후, 암호화 과정에서 사용된 랜덤위상패턴인 $q(x,y)$와 $H(u,v)$의 복소공액을 이용하여 이루어진다. 먼저, 공간주파수영역에서 $H^*(u,v)$가 곱해진 후, 공간영역에서 $q^*(x,y)$가 곱해진다. 입력영상이 위상패턴으로 변환된 신호 $c(x,y)$는

$$
\begin{aligned}
c(x,y) &= [\mathcal{F}^{-1}[\mathcal{F}\{\varphi_p(x,y)\}\times H^*(u,v)]]\times q^*(x,y) \\
&= [c(x,y)q(x,y)]\times q^*(x,y) \\
&= c(x,y) = \exp[j\pi f(x,y)]
\end{aligned} \tag{25}
$$

와 같이 복원된다. 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 위상암호화 방법은 그림 2와 그림 3처럼 4-f 광 상관시스템을 사용하여 광학적으로 구현이 가능하다. 그림 2에서 입력평면에 위상패턴으로 변환된 입력영상 $c(x,y)$와 첫번째 랜덤위상패턴인 $q(x,y)$를 설치하고, 주파수평면에 두번째 랜덤위상패턴인 $H(u,v)$를 설치하면, 출력평면에서는 곱 $\{c(x,y)\times q(x,y)\}$와 $h(x,y)$와의 콘볼루션 결과로 암호화된 영상을 얻을 수 있다. 암호화된 영상을 복원하는 과정은 그림 3처럼 암호화된 영상 $\varphi_p(x,y)$를 입력평면에 설치하고, 주파수평면에는 암호화 과정에서 사용된 두번째 랜덤위상패턴의 복소공액 $H^*(u,v)$을 설치하며, 출력평면에 첫번째 랜덤위상패턴의 복소공액 $q^*(x,y)$를 설치하면, 위상패턴으로 변환된 입력영상 $c(x,y)=\exp[j\pi f(x,y)]$를 얻을 수 있다. 암호화된 영상을 복원하기 위해서는 공간영역에서의 랜덤위상패턴인 $q(x,y)$와 공간주파수영역에서의 랜덤위상패턴인 $H(u,v)$를 알고 있어야 가능하므로, 두개의 랜덤위상패턴은 엔트로피(entropy)를 극대화하는 효과를 갖으며, 암호화된 영상을 복원하기 위한 핵심적인 암호키 역할을 하게 된다.

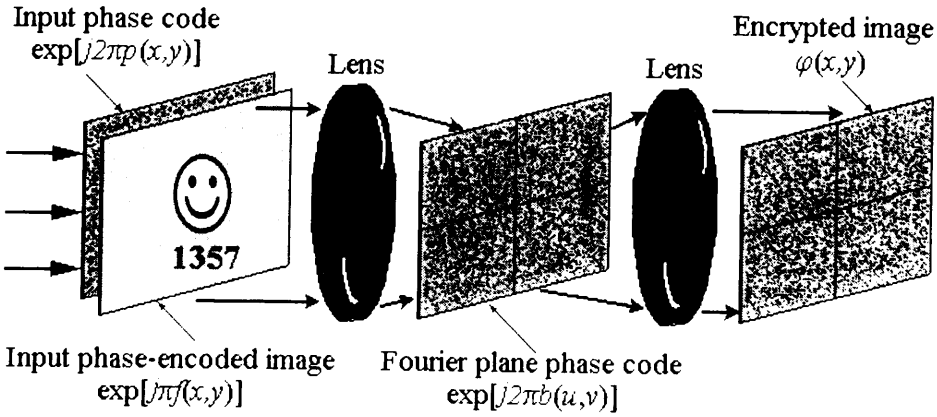


Fig. 2. Optical implementation of the fully phase encryption method.

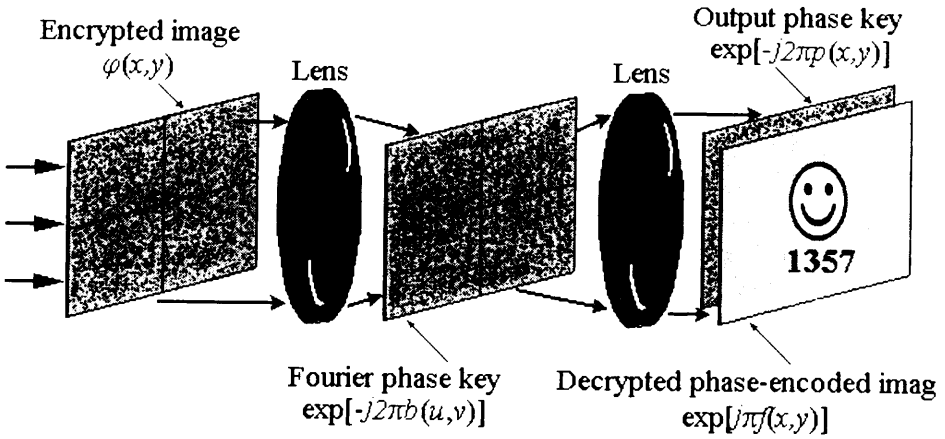


Fig. 3. Optical implementation of the image reconstruction method.

한편, 암호화된 영상 $\varphi_p(x,y)$에 잡음 $n(x,y)$이 더해진 영상을 $\varphi'_p(x,y)$라 하면

$$\begin{aligned}\varphi'_p(x,y) &= [\{c(x,y)q(x,y)\}\otimes h(x,y)] + n(x,y) \\ &= [\exp[j\pi f(x,y) + j2\pi p(x,y)]\otimes h(x,y)] + n(x,y)\end{aligned} \tag{26}$$

와 같이 표현되고, 복원되는 영상은 잡음 $n(x,y)$이 더해졌기 때문에 더 이상 위상 성분만을 갖는 함수가 아니다. 복원되는 영상은

$$A(x,y)\exp[j\pi f_p'(x,y)] = \exp[j\pi f(x,y)] + n_0(x,y) \tag{27}$$

와 같으며, 여기서 $A(x,y)\geq 0$ 인 값이고, $n_0(x,y)$는 복소잡음(complex noise)으로

$$\begin{aligned}n_0(x,y) &= \mathcal{F}^{-1}[\mathcal{F}[\,n(x,y)\,]\times H^*(u,v)\,]\times r^*(x,y) \\ &= \mathcal{F}^{-1}[\mathcal{F}[\,n(x,y)\,]\times\exp[-j2\pi b(u,v)]]\times\exp[-j2\pi p(x,y)]\end{aligned} \tag{28}$$

와 같다. 최종적인 영상복원은 식 (27)에서 위상성분을 검출해야 한다. 만약 잡음이 존재하지 않으면 $A(x,y)=1$, $f_p'(x,y)=f(x,y)$가 되어

$$A(x,y)\exp[j\pi f_p'(x,y)] = \exp[j\pi f(x,y)] \tag{29}$$

처럼 표현되고, 위상의 범위는 구간 $[0,\pi]$의 값을 갖게 된다. 그러나 잡음이 존재할 경우에 위상의 범위는 구간 $[0,2\pi]$의 값을 갖게 되므로 3사분면(third quadrants)과 4사분면의 위상을 음의 위상으로 표현해 줄 필요가 있다. 예를 들어, $A(x,y)\exp[j4\pi/3]$의 위상은 $-2\pi/3$로 표현하고, $A(x,y)\exp[-j\pi/2]$의 위상은 $-\pi/2$로 된다. 표기를 간략하게 하기 위해서 복소수 z의 위상을 $Arg(z)$라고 표현하면, 원래의 입력영상

이 구간 [0,1]의 값이므로, 최종적인 복원영상은 위상성분의 값을 절대치(absolute value)화 하면 된다. 그러므로 복원영상은

$$|f_p'(x,y)| = |Arg\{A(x,y)\exp[j\pi f_p'(x,y)]\}/\pi| \tag{30}$$

처럼 표현되고, 구간 [0,1]의 값을 갖게 된다.

영상을 암호화하고 복원하는 과정에서 재생손실이 발생할 경우 복원영상의 재생손실을 계산하기 위해서 평균제곱에러(mean squared error, MSE)를 사용하였다. 원래의 입력 영상 $f(x,y)$가 N×M 화소를 갖는다면, 영상 암호화 및 복원 과정에서 발생하는 재생손실 MSE는

$$MSE(|f_p|) = E\left\{\frac{1}{N\times M}\sum_{x=1}^{N}\sum_{y=1}^{M}[\|f(x,y)| - |f_p'(x,y)\|^2]\right\} \tag{31}$$

와 같다. 여기서 $|f_p'(x,y)|$는 식 (30)과 같으며, $E\{\cdot\}$는 평균을 의미한다. 이상에서 살펴본 영상의 위상암호화 방법은 다른 방법에 비해 시스템이 단순하며 재생손실이 적은 특징을 가지고 있다.

2. 제안한 영상암호화 방법

본 논문에서 제안한 영상암호화 방법은 영상의 위상암호화 방법을 수정한 것으로, 비밀코드처럼 보안을 요하는 경우나 개인의 신원정보가 타인에게 보여져서는 안 될 경우, 또는 암호화된 영상을 복원하는 과정 없이 인식시스템에서 신원확인이 이루어지도록 하기 위해서 제안되었으며, 비밀코드나 주민등록번호처럼 단순히 숫자나 문자의 조합으로 구성되는 영상을 암호화하기 위한 방법이다.

비밀코드의 용도로 사용될 개인식별번호 영상을 암호화하기 위해서는 숫자영상이 '0'~'9'까지 10개가 필요하게 되므로, 숫자 '1', '2', …, '9', '0'의 영상을 각각 $f_1(x,y)$, $f_2(x,y)$, …, $f_{10}(x,y)$라 하고, 각각의 숫자영상에 대응하는 잡음(uniformly distributed random noise)을 $p_1(x,y)$, $p_2(x,y)$, …, $p_{10}(x,y)$라 하면, 각각의 숫자영상들이 공간영역에서 위상암호화된 학습영상 $t_1(x,y)$, $t_2(x,y)$, …, $t_{10}(x,y)$는

$$\begin{aligned} t_1(x,y) &= \exp[j\pi f_1(x,y)]\exp[j2\pi p_1(x,y)] \\ t_2(x,y) &= \exp[j\pi f_2(x,y)]\exp[j2\pi p_2(x,y)] \\ &\vdots \\ t_{10}(x,y) &= \exp[j\pi f_{10}(x,y)]\exp[j2\pi p_{10}(x,y)] \end{aligned} \tag{32}$$

와 같이 정의할 수 있다. 예를 들어 비밀코드가 '1357'이라면, 위상암호화된 학습영상의 조합으로 구성되는 입력영상 $t(x,y)$는 그림 4와 같이 표현할 수 있다. 이렇게 구성된 입력영상 $t(x,y)$는 다시 공간주파수영역에서 랜덤위상패턴인 $H(u,v)$에 의해서 이중으로 암호화된다. 암호화된 개인식별번호 영상 $\varphi_p(x,y)$는

$$\begin{aligned} \varphi_p(x,y) &= \mathcal{F}^{-1}[\, T(u,v)H(u,v)\,] \\ &= t(x,y) \otimes h(x,y) \end{aligned} \tag{33}$$

와 같다. 여기서 $h(x,y)$는 전달함수 $H(u,v)=\exp[j2\pi b(u,v)]$의 임펄스 응답이다.

$t_1(x,y)$	$t_3(x,y)$	$t_5(x,y)$	$t_7(x,y)$

Fig. 4. The input image is made by combining phase encrypted training images.

이와 같이 숫자나 문자 영상을 위상변환하여 학습영상으로 만들게 되면, 학습영상은 단순한 숫자나 문자 영상보다 더 많은 정보를 포함하게 된다. 즉, 숫자 '1', '2', …, '9', '0'을 인식하기 위하여 각각의 숫자영상들을 위상변환하여 학습영상으로 만들어 합성한 필터는 단순히 숫자영상 자체를 학습영상으로 하여 합성한 필터보다 학습영상들의 유사성을 감소시킬 수 있으므로 분리인식 능력을 향상시킬 수 있다. 예를 들어, 숫자 '1', '5', '8'은 인식하고, '4', '6', '9'는 분리할 경우, 단순히 숫자영상들을 합성한 필터는 숫자 '1'과 '4', '5'와 '6', '8'과 '9'의 유사성으로 인하여 숫자 '4', '6', '9'영상과의 상관출력 결과에서 작지만 원하지 않는 상관첨두치들이 나타나게 된다. 그러나 숫자영상들을 위상변환하게 되면 이러한 유사성을 최소화할 수 있어 상관출력 결과에서 SNR을 높이는 효과를 얻을 수 있다. 또한 암호화된 영상으로부터 개인식별번호를 인식하기 위해서는 암호화 과정에서 사용되는 랜덤위상패턴들을 알고 있어야만 가능하므로 비밀키 및 개인정보 보호에 유용하게 사용될 수 있다.

Ⅳ. 개인의 신분인증

본 논문에서는 신분증을 이용한 개인의 신분인증 방법을 두 가지로 제안하였다. 첫번째 방법은 먼저 암호화된 신원정보영상을 복원한 후, 복원영상을 이용하여 개인의 신분을 인증하는 방법이다. 이러한 방법은 복원한 얼굴영상과 신분증을 제시한 사람의 얼굴을 육안으로 확인하거나, 복원한 얼굴영상을 데이터베이스에 있는 본인의 얼굴정보와 비교하거나, 또는 복원한 개인식별번호 영상을 이용하여 신분증을 제시한 사람의 식별번호를 질의응답하는 등의 용도로써 이용될 수 있다. 두 번째 방법은 복원과정 없이 암호화된 신원정보영상을 이용하여 개인의 신분을 인증하는 방법으로, 비밀코드처럼 보안을 요하는 경우에 비밀코드는 육안으로 식별할 수 없고, 단지 인식시스템에서만 인식해야 될 경우이다.

개인의 신원정보보호 및 신분인증 시스템의 블럭도는 그림 5와 같다. 입력영상은 얼굴영상과 개인식별번호 영상으로 이루어지고, 이 입력영상이 랜덤위상패턴에 의해서 암호화되어 홀로그램 형태로 신분증에 부착된다. 그리고 신분증을 이용한 개인의 신분인증은 먼저, 개인식별번호를 인식하여 그 사람의 신원을 파악하게 된다. 여기서 개인식별번호의 인식은 암호화된 개인식별번호 영상을 복원하여 MMACE 필터로 분류·인식하는 방법과 암호화된 영상을 복원하는 과정 없이 MMACE_p 필터로 분류·인식하는 방법을 제안하였다. 개인식별번호로부터 그 사람의 신원을 파악한 후에는 데이터베이스에 저장된 본인의 얼굴정보와 암호키를 사용하여 복원한 얼굴영상과의 상관을 통하여 개인 인증을 하는 방법을 제안하였다. 여기서 데이터베이스에 저장된 얼굴정보는 OWMF의 임펄스응답을 의미하며, 웨이브릿 변환을 이용하여 얼굴영상의 특징점들을 추출하게 된다. 제안한 방법은 데이터베이스에 저장된 본인의 얼굴정보와 복원한 얼굴영상과의 1:1 광상관을 취하므로 인증 속도가 빠르고, 신원확인을 이중으로 하므로 오인식의 발생을 방지할 수 있다는 장점이 있다.

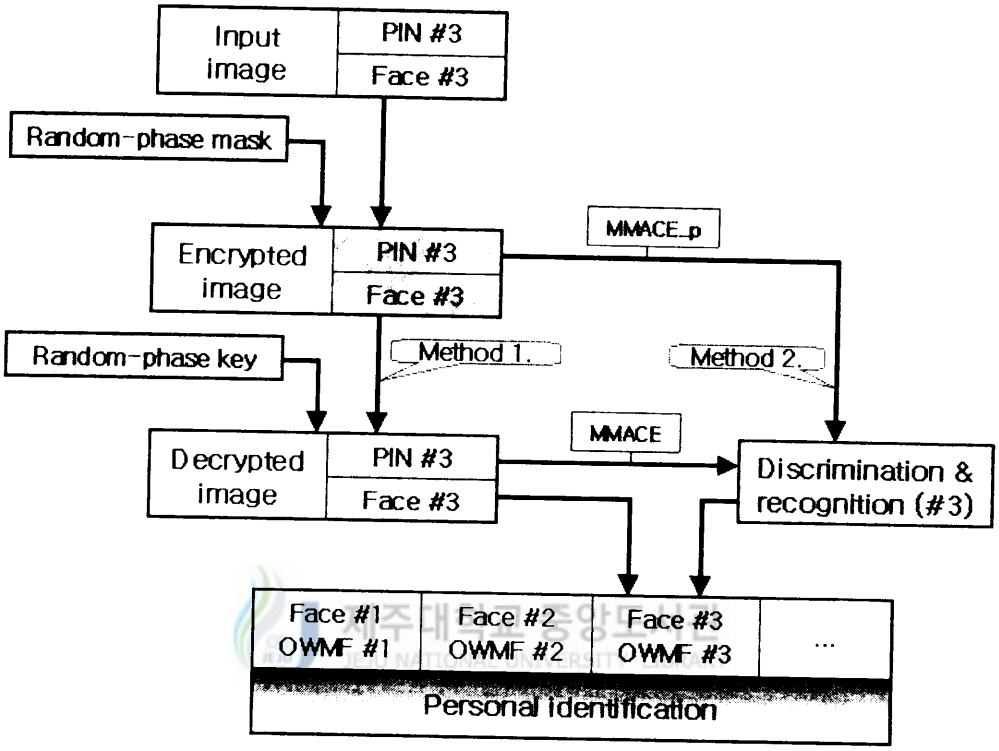


Fig. 5. The block diagram of verifying system.

1. 개인식별번호의 분류·인식

본 논문에서 제안한 방법인 신분증을 이용한 개인의 신분인증은 먼저, 개인식별번호를 분류·인식하여 신원을 파악한 후, 그 사람의 얼굴정보와 복원한 얼굴영상을 서로 비교함으로써 이루어진다. 개인식별번호를 분류·인식하기 위해서 사용되는 MMACE 필터는 MACE 필터들의 위상을 공간주파수 변조하여 합성하는 다중화 방법을 이용한다. 본 논문에서는 숫자 '0'~'9'를 효과적으로 분류·인식하기 위하여 4개의 MACE 필터를 다중화 하였다. 그러므로 상관결과는 4개의 부평면으로

나눠지고, 만약 상관결과를 코드화한다면 기호나 특수문자 등을 포함하여 최대 15개의 서로 다른 숫자나 문자를 분리인식 할 수 있다. 개인식별번호를 인식하기 위한 4개의 MACE 필터는

$$\mathbf{H}_{\mathrm{MACE},i} = \mathbf{D}^{-1}\mathbf{F}[\mathbf{F}^{+}\mathbf{D}^{-1}\mathbf{F}]^{-1}\mathbf{u}_{i}, \qquad i=1,2,3,4 \tag{34}$$

와 같다. 여기서 행렬 **D**는 숫자 '0'~'9' 영상의 평균 에너지 스펙트럼이고, **F**는 푸리에 변환된 학습영상('0'~'9' 숫자영상)들을 행벡터로 표현한 것이다.

$$\mathbf{F} = [\mathbf{F}_1\ \mathbf{F}_2\ \ldots\ \mathbf{F}_{10}] \tag{35}$$

그리고 제한벡터는

$$\begin{aligned}
\mathbf{u}_1 &= [0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1] \\
\mathbf{u}_2 &= [0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1] \\
\mathbf{u}_3 &= [0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 0] \\
\mathbf{u}_4 &= [1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0]
\end{aligned} \tag{36}$$

와 같이 코드화하였다. 여기서 제한벡터의 원소가 '1'이라는 것은 필터를 합성할 때 사용된 학습영상을 인식하는 것을, '0'이라는 것은 분리하는 것을 의미한다. 그리므로 다중화 방법을 이용하여 합성한 MMACE 필터는

$$H_{\mathrm{MMACE}}(u,v) = \sum_{i=1}^{4} H^{*}_{\mathrm{MACE},i}(u,v)\exp[-i2\pi(a_i u + b_i v)] \tag{37}$$

와 같다. 여기서 상관결과의 분리정도를 결정하는 a_i와 b_i의 값은 출력상관평면의 중앙화소를 (0,0)이라 할 때, a_i는 상관결과를 좌측으로 이동시킬 경우 양의 값을,

우측으로 이동시킬 경우는 음의 값을 사용하였으며, b_i는 상관결과를 상단으로 이동시킬 경우는 양의 값을, 하단으로 이동시킬 경우는 음의 값을 사용하였다. 이때 4개의 부평면에서의 상관결과가 서로 겹치지 않고 독립적으로 나타나도록 하기 위해 a와 b는 출력상관평면 크기의 '1/4'로 채택하였다. 따라서 4개의 MACE 필터가 다중화 된 MMACE 필터와 입력과의 상관결과는 그림 6과 같이 독립적으로 위치하게 된다.

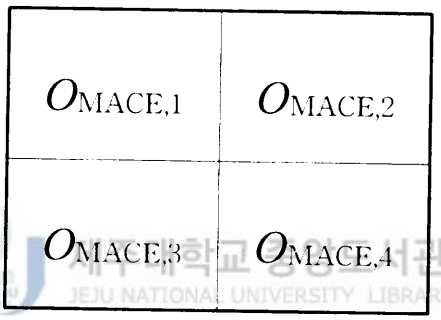


Fig. 6. Positions of correlation result.

개인식별번호 영상과 MMACE 필터와의 상관결과는 경계값처리 후, 4개의 부평면으로 나눠지며, 개인식별번호를 분류·인식하기 위한 코드표는 표 1과 같다. 표 1의 코드값은 임의로 설정한 것으로 코드표에서 모두 '0'인 상태의 코드를 제외하였는데, 이는 입력영상에 숫자가 없거나 필터합성시 사용된 학습영상이 존재하지 않는 숫자나 문자가 입력되는 경우 모두 '0'의 값을 갖는 코드가 발생하여 오인식이 될 수 있다. 이 문제점을 없애기 위하여 모두 '0'인 상태의 코드를 코드표에서 제외하였다.

Table 1. Code table for personal identification number.

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

한편, 제안한 영상암호화 방법을 사용하여 암호화한 개인식별번호 영상으로부터 식별번호를 분류·인식하기 위해서는 필터자체에 암호키(암호화 과정에서 사용된 랜덤위상패턴의 복소공액)를 포함하고 있어야만 가능하다. 암호화된 개인식별번호 영상을 복원하는 과정 없이 분류·인식할 수 있는 필터 $H_{\mathrm{MMACE_P}}$는

$$H_{\mathrm{MMACE\_P}}(u,v) = H_{\mathrm{MMACE1}}(u,v) \times H^{*}(u,v)$$
$$= \left[\sum_{i=1}^{L} H^{*}_{\mathrm{MACE\_P},i}(u,v) \exp[-j2\pi(a_i u + b_i v)] \right] \times H^{*}(u,v) \tag{38}$$

와 같다. 여기서 $H_{\mathrm{MACE_P}}$는 식 (32)에 나타낸 바와 같이 공간영역에서 위상암호화된 학습영상 $t_1(x,y)$, $t_2(x,y)$, …, $t_{10}(x,y)$들을 MACE 방법으로 합성한 필터로

$$\mathbf{H}_{\mathrm{MACE\_P},i} = \mathbf{D}_{\mathbf{T}}^{-1}\mathbf{T}[\mathbf{T}^{+}\mathbf{D}_{\mathbf{T}}^{-1}\mathbf{T}]^{-1}\mathbf{u}_i \tag{39}$$

와 같다. 여기서 $\mathbf{D_T}$는 공간영역에서 위상암호화된 학습영상들의 평균 에너지 스펙트럼이고, $\mathbf{T}$는 행벡터로 푸리에 변환된 학습영상이다. 여기에 사용된 제한벡터 $\mathbf{u}_i$는 식 (36)과 같고, 개인식별번호를 분류·인식하기 위한 코드표도 표 1과 같게 설정하였다.

2. 개인 인증

신분증을 이용한 개인의 신분인증은 개인식별번호를 분류·인식하여 그 사람의 신원을 파악한 후, 데이터베이스에 저장된 본인의 얼굴정보와 복원한 얼굴영상과의 상관결과로써 개인 인증을 할 수 있도록 제안하였다. 데이터베이스에 저장된 얼굴정보는 OWMF의 임펄스응답을 의미하며, 신분증에 부착될 얼굴사진을 웨이브릿 변환하여 얼굴영상의 특징점들을 추출하게 된다. OWMF는 얼굴영상을 $f(x,y)$ 라면

$$G_{\mathrm{OWMF}}(u,v) = F(u,v)^{*}\,|H_a(u,v)|^2 \tag{40}$$

와 같다. 여기서 $H_a(u,v)$는 푸리에 변환된 웨이브릿 함수로, 광을 이용한 패턴인식에서 주로 사용되는 웨이브릿 함수는 Harr, Morlet 및 Mexican-hat 등이 있으며, 본 논문에서는 얼굴영상의 특징점을 추출하기 위해 Maxican-hat 웨이브릿 함수를 사용하였다. 본 논문에 사용된 Mexican-hat 웨이브릿 함수는 등방성 Gauss 함수 $g_a(x,y)=\exp[-(x^2+y^2)/2a^2]$를 2차 미분한 함수로

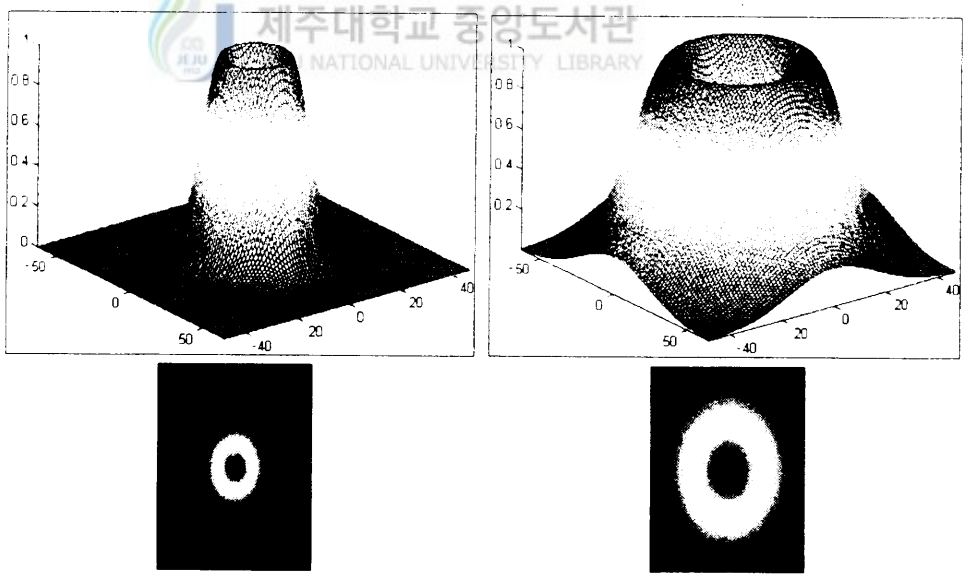
$$\begin{aligned} h_a(x,y) &= \nabla^2 g_a(x,y) \\ &= \frac{1}{a^2}\left[\frac{x^2+y^2}{a^2}-2\right]\exp\left(-\frac{x^2+y^2}{2a^2}\right) \end{aligned} \tag{41}$$

와 같고, 공간주파수영역에서의 Mexican-hat 웨이브릿 함수는

$$H_a(u,v) = 4\pi^2 a^2(u^2+v^2)\exp[-2\pi^2 a^2(u^2+v^2)] \tag{42}$$

이다. 여기서 축척모수 a의 값은 영상의 종류 및 적용하고자 하는 경우에 따라 적절하게 선정해야 하는데, 본 논문에서는 축척모수가 a=1일 때 얼굴영상들의 특징점을 추출하는데 효과적이였다.

그림 7은 본 논문에 사용된 Mexican-hat 웨이브릿 함수를 공간주파수영역에서 보여주고 있는데 그림 7(a)는 축척모수 a=2일 때, 그림 7(b)는 축척모수 a=1일 때이다. 그리고 아래 부분 그림은 대역통과 특성을 단면적으로 나타낸 것으로, 그림 7(a)는 저주파 영역과 중간 주파수를 통과시키고 있으며, 그림 7(b)는 중간 주파수와 고주파 영역을 통과시키는 것을 보여주고 있다. 그러므로 웨이브릿 변환을 이용하면 각 개인의 얼굴영상에서 특징점들을 추출할 수 있어 잡음이 존재하는 영상에 대해서도 잡음의 영향을 최소화 할 수 있다.



(a) (b)

Fig. 7. Mexican-hat wavelet function in the frequency domain: (a) a=2, (b) a=1.

V. 컴퓨터 시뮬레이션 결과 및 고찰

1. 개인신원정보의 암호화와 복원

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 논문에서는 개인신원정보 영상으로 주민등록증에 부착된 얼굴사진을 스캔한 영상(96×128, gray-scale 영상)과 개인이 갖는 고유한 개인식별번호(220×32, 이진영상)를 임의로 정하여 사용하였다.

그림 8과 그림 9는 개인의 신원정보인 개인식별번호 영상과 얼굴영상을 암호화하고 복원하는 과정을 나타낸 것으로, 암호화된 영상은 복소(complex) 영상이므로 그림 8(b)와 9(b)는 각각 그림 8(a)의 개인식별번호 영상과 그림 9(a)의 얼굴영상을 암호화된 영상의 크기성분을, 그림 8(c)와 9(c)는 암호화된 영상의 위상성분을 256 gray-scale 영상으로 표현한 것이다. 그림에서 확인할 수 있듯이 암호화된 영상은 입력영상의 어떠한 정보도 나타내지 않고 마치 랜덤한 잡음처럼 보이게 된다. 이렇게 암호화된 영상이 복소 위상홀로그램 형태로 신분증에 부착되어 개인의 신원정보를 보호하고 신분증의 위조를 방지하는 역할을 한다. 그림 8(d)와 9(d)는 암호화된 영상을 복원한 것으로 원래의 입력영상을 그대로 복원하고 있음을 알 수 있다. 그림 8(e)와 9(e)는 암호화된 영상에 평균이 '0'이고, 표준편차가 σ=0.5인 백색잡음(white gaussian noise)이 더해졌을 경우에 복원한 영상이며, 실제 복원되는 신호는 256 gray-level 이상을 갖지만, 220×32×256의 해상도를 갖는 영상으로 표현하였다. 그림에서 확인할 수 있듯이 복원영상 전 영역에 걸쳐 잡음이 발생하며, 이 때 발생한 재생손실은 각각 MSE=0.0154, MSE=0.0126이다. 개인의 신분을 인증하기 위한 인식시스템에서는 이와 같이 암호화된 영상을 복원하는 과정에서

재생손실이 발생하더라도 인식할 수 있어야 한다. 그림 8(f)는 공간주파수영역에서의 암호키가 틀릴 경우, 그림 9(f)는 공간영역에서의 암호키가 틀릴 경우 복원되는 영상으로, 부정확한 암호키를 사용하여 암호화된 영상을 복원하면 원래의 입력영상을 재생할 수 없음을 확인할 수 있다. 그러므로 개인신원정보 영상을 암호화하는 과정에서 사용된 두 개의 랜덤위상패턴은 엔트로피를 극대화하는 효과를 갖으며, 암호화된 영상을 복원하는 과정에서 핵심적인 역할을 하게 된다.

그림 10은 본 논문에서 사용한 얼굴영상과 개인식별번호 영상에 대하여 암호화된 영상에 백색잡음이 더해졌을 경우에 발생하는 재생손실인 MSE를 알아보기 위한 것으로 표준편차 σ가 증가함에 따라 MSE도 증가하는 것을 알 수 있다. 이때 사용된 평균값은 모두 '0'이다. 개인의 신분을 인증하기 위한 인식시스템은 이와 같이 암호화된 영상을 복원하는 과정에서 재생손실이 발생하더라도 무관하게 인식할 수 있어야 한다.

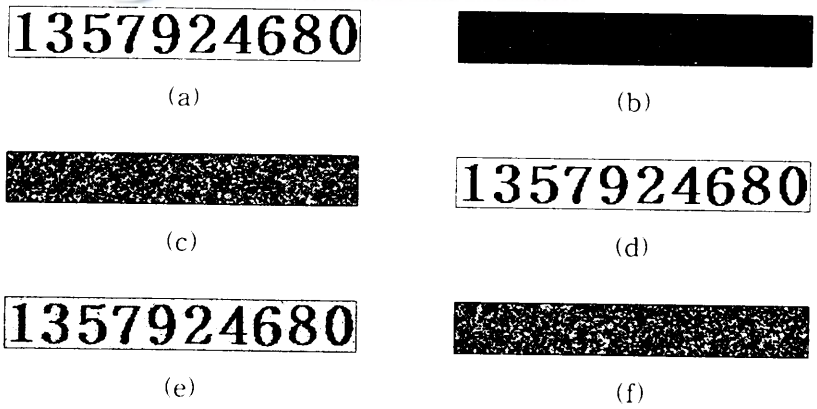
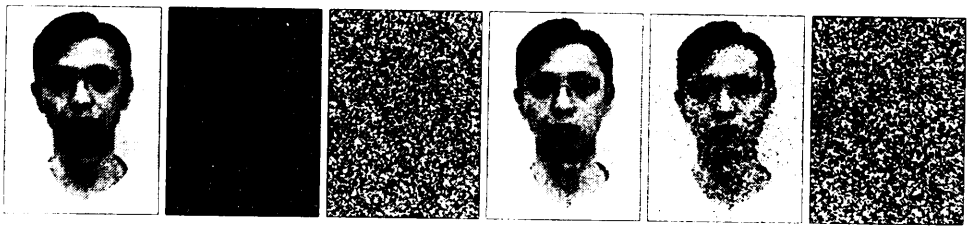


Fig. 8. Phase encryption and decryption for a binary image:
(a) original binary image, (b) magnitude of the encrypted image,
(c) phase of the encrypted image, (d) recovered image,
(e) recovered image in additive white gaussian noise(σ=0.5,MSE=0.0154),
(f) reconstructed image from a different random phase key in the frequency domain.



(a) (b) (c) (d) (e) (f)

Fig. 9. Encryption and decryption for a gray-scale image:
(a) original gray-scale image, (b) magnitude of the encrypted image,
(b) magnitude of the encrypted image, (d) recovered image,
(e) recovered image in additive white gaussian noise(σ=0.5,*MSE* 0.0126),
(f) reconstructed image from a different random phase key in the space domian.

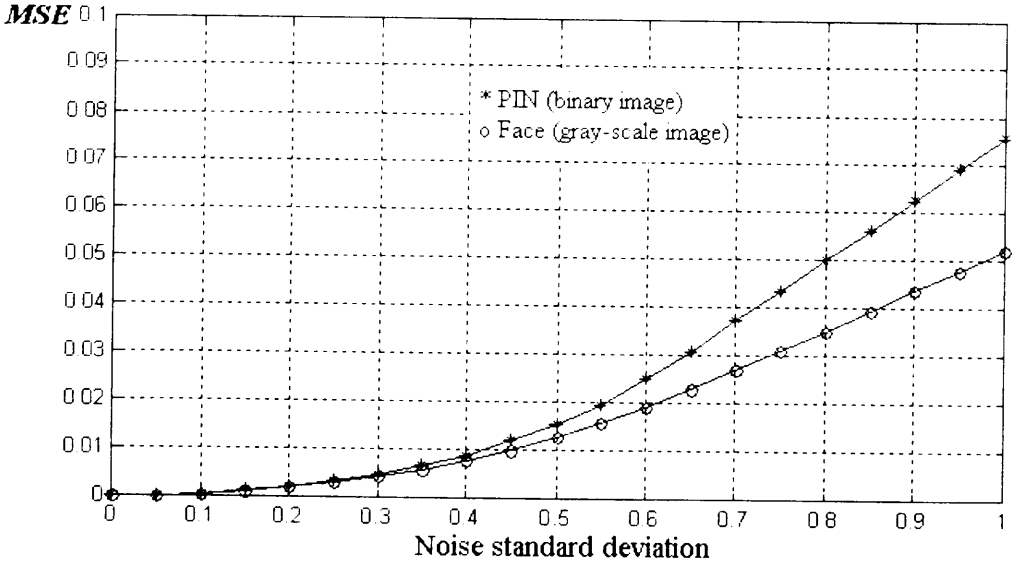


Fig. 10. *MSE* versus standard deviation in the prese of additive white gaussian noise.

2. 개인식별번호의 분류 · 인식

제안한 신분인증 시스템은 먼저, 개인식별번호 영상으로부터 식별번호를 분류 · 인식하여 개인의 신원을 파악한 후, 그 사람의 얼굴정보와 복원한 얼굴영상을 서로 비교하게 된다. 그림 11은 MMACE 필터와 MMACE_p 필터를 사용하여 개인식별번호를 효과적으로 분류 · 인식할 수 있음을 보여준다. 그림 11(a)는 암호화된 개인식별번호 영상을 복원한 영상으로 220×32 화소를 갖는 이진영상이다. 그림 11(b)는 복원과정 없이 식별번호를 분류 · 인식하기 위하여 제안한 암호화방법을 사용하여 암호화한 개인식별번호 영상의 위상패턴을 256 gray-scale 영상으로 표현한 것이다. 여기서 비밀코드에 해당하는 식별번호는 그림 11(a)와 동일하다. 그림 11(c)는 복원영상인 그림 11(a)와 MMACE 필터와의 상관결과로써, 440×64평면으로 그림에서 제1부평면은 좌 · 상 부분에 위치하고, 제2부평면은 우 · 상, 제3부평면은 좌 · 하, 제4부평면은 우 · 하 부분에 각각 위치하여 상관출력 결과가 서로 중첩없이 나타나는 것을 확인할 수 있다. 그림 11(d)는 암호화된 개인식별번호 영상과 제안한 MMACE_p 필터와의 상관결과로써 SNR이 향상됨을 확인할 수 있다. 여기서 SNR은 상관평면에서 최대상관치와 최대상관치의 50%이하 상관치들의 실효치의 비로 그림 11(c)에서의 SNR은 19.6이고, 그림 11(d)에서의 SNR은 21.4로 나타났다. 그림 11의 (e)와 (f)는 각각 그림 11(c)와 11(d)의 상관결과를 최대상관치의 50%로 경계값처리 후, 4개의 부평면으로 나타낸 이진영상이며 경계값보다 큰 값은 모두 '1'의 값으로 할당하여 동일한 값으로 나타냈다. 그림에서 흰 점의 위치에서 출력 값이 '1'이 됨을 의미하며, 각 부평면에서 같은 위치의 출력 값을 확인함으로써 개인식별번호를 효과적으로 분류 · 인식할 수 있다. 예를 들어, 그림 11(e)의 4개의 흰 원을 표시한 것처럼 각 부평면에서 같은 위치의 출력으로부터 '0110'이라는 코드값을 얻고, 표 1의 코드표와 비교하여 숫자 '6'이라고 인식하게 된다. 나머지 숫자들에 대해서도 같은 방식으로 살펴보면 오인식이 없이 모두 정확하게 인식하고 있음을 확인할 수 있다. 이와 같이 제안한 방법을 사용하면 숫자

로 복잡하게 구성되는 개인식별번호를 한번의 광상관만으로도 효과적으로 분류·인식할 수 있다.

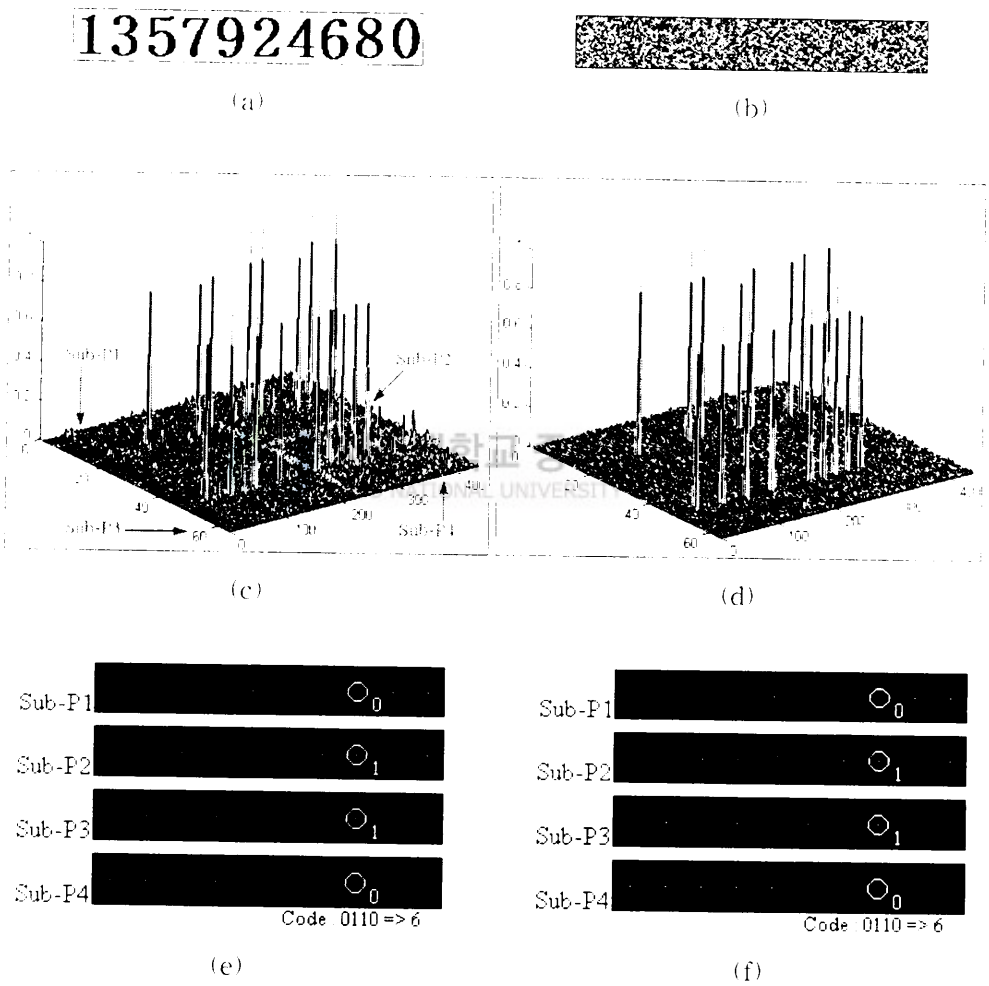


Fig. 11. Recognition of the personal identification number:
(a) recovered binary image, (b) encrypted image,
(c) correlation (a) with MMACE, (d) correlation (b) with MMACE_p,
(e) thresholded image of the (c), (f) thresholded image of the (d).

그림 12는 암호화된 영상에 백색잡음이 더해졌을 경우에도 개인식별번호를 분류·인식할 수 있음을 보여준다. 그림 12(a)는 암호화된 개인식별번호 영상에 표준편차 σ=0.5인 백색잡음이 더해졌을 때 복원한 신호를 220×32×256의 해상도를 갖는 영상으로 표현한 것이며, 이때의 재생손실은 MSE=0.0154이다. 그림 12(b)는 제안한 암호화방법을 사용하여 암호화한 개인식별번호 영상에 그림 12(a)에서 사용했던 표준편차 σ=0.5인 백색잡음이 더해진 영상의 위상패턴을 256 gray-scale 영상으로 표현한 것이다. 그림 12(c)는 복원한 영상과 MMACE 필터와의 상관결과로 SNR은 19.3이고, 그림 12(d)는 잡음이 더해진 암호화된 영상과 MMACE_p 필터와의 상관결과로 그림 12(c)와 비교하여 상관첨두치들이 아주 안정된 결과를 나타내고 있으며 SNR은 20.4로 잡음이 존재하는 환경에서도 SNR이 높게 나타났다. 그림 12의 (e)와 (f)는 각각 그림 12(c)와 12(d)의 상관결과를 경계값처리한 결과로써, 그림 11의 (e) 및 (f)와 동일한 결과를 갖는다. 그러므로 제안한 방법은 어느 정도의 잡음이 존재하는 환경에서도 개인식별번호를 효과적으로 분류·인식할 수 있음을 확인할 수 있다.

그림 13은 잡음이 존재할 경우, MMACE 필터에서는 인식하지 못하지만, 제안한 MMACE_p 필터를 사용하여 인식할 수 있음을 확인하기 위한 것이다. 그림 13(a)는 표준편차 σ=1인 백색잡음이 더해졌을 때 복원한 영상으로 재생손실은 MSE=0.0756이고, 그림 13(b)는 암호화된 영상에 그림 13(a)에서와 같은 백색잡음이 더해진 영상의 위상패턴이다. 그림 13(c)는 MMACE 필터를 사용하여 얻은 상관결과로 상관첨두치들이 많이 감소하고 있다. 그러나 MMACE_p 필터를 사용하여 얻은 상관결과인 그림 13(d)는 그림 13(c)와 비교하여 상관첨두치들이 아주 안정된 결과를 나타내고 있다. 그림 13의 (e)와 (f)는 각각 그림 13(c)와 13(d)의 상관결과를 경계값처리한 결과로써, 그림 13(e)에서 보는 바와 같이 표준편차 σ=1인 백색잡음이 더해졌을 때 숫자 '3'을 '2'로, 숫자 '9'를 '8'로 인식하는 오인식이 발생하고 있다. 그러나 그림 13(f)는 그림 11의 (e) 및 (f)와 동일한 결과로 오인식이 없이 모두 정확하게 인식하고 있어 제안한 MMACE_p 필터가 잡음이 존재하는 환경에서 SNR과 인식률이 증가함을 확인할 수 있다.

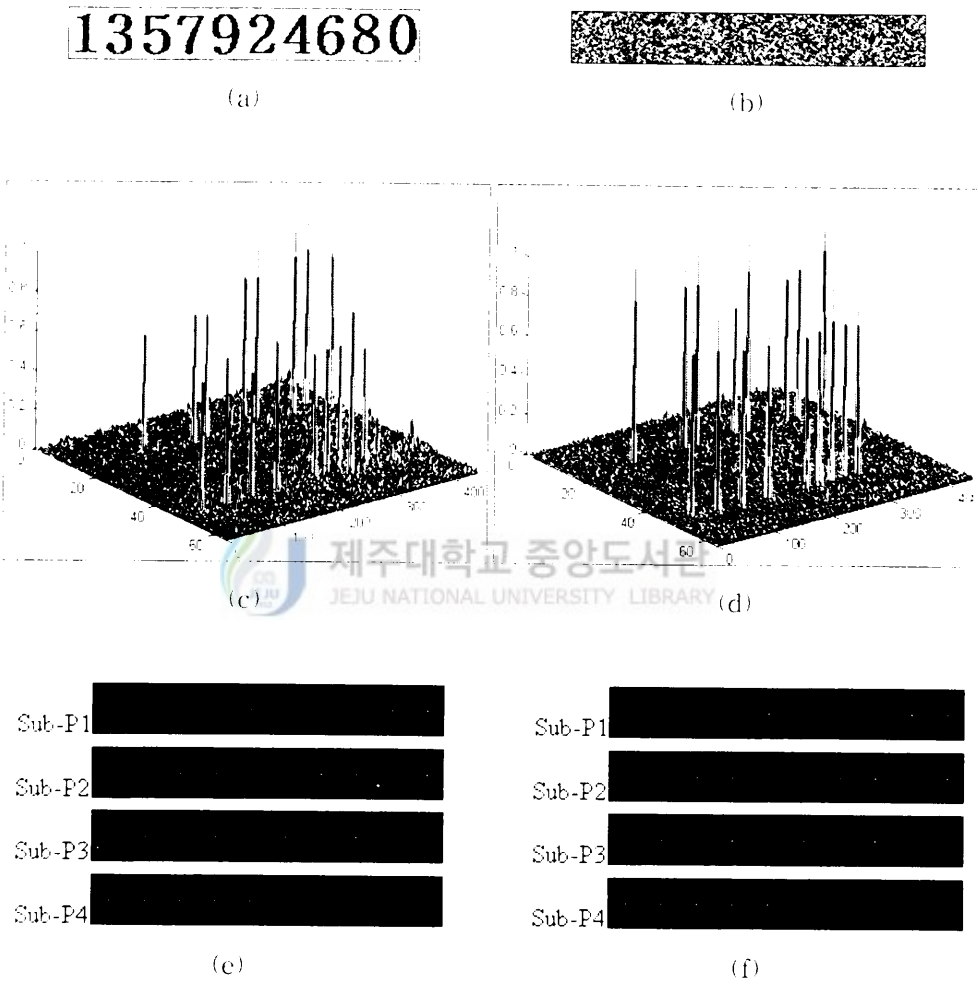


Fig. 12. Recognition of the personal identification number in additive white gaussian noise (σ=0.5):
(a) recovered binary image(MSE=0.0154), (b) encrypted image with noise, (c) correlation (a) with MMACE, (d) correlation (b) with MMACE_p, (e) thresholded image of the (c), (f) thresholded image of the (d).

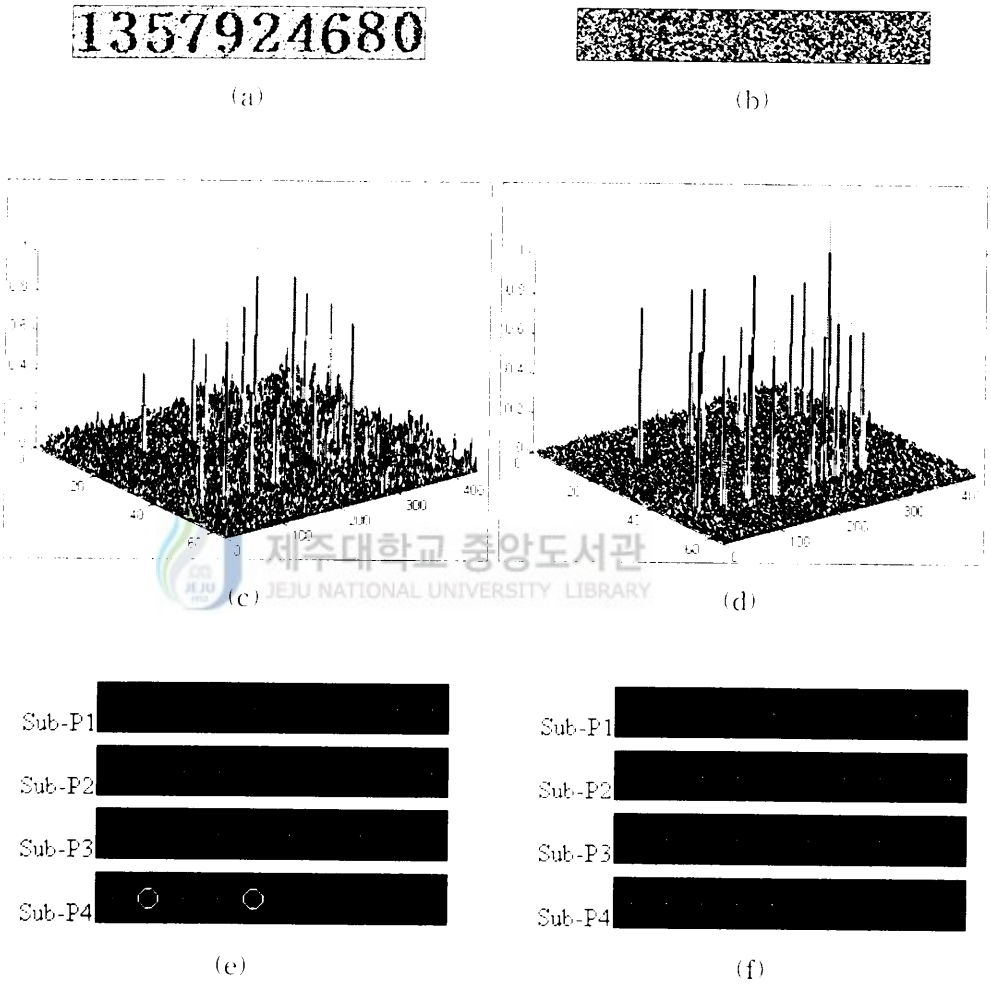


Fig. 13. Recognition of the personal identification number in additive white gaussian noise (σ=1.0):
(a) recovered binary image(MSE=0.0756), (b) encrypted image with noise, (b) correlation (a) with MMACE, (d) correlation (b) with MMACE_p, (e) thresholded image of the (b), (f) thresholded image of the (d).

그림 14는 잡음의 영향에 따른 SNR를 나타낸 것으로써, 잡음이 존재하는 환경에서도 제안한 MMACE_p필터가 다소 우수한 성능을 가지고 있음을 확인할 수 있다. MMACE 필터를 사용하여 개인식별번호를 분류·인식할 경우는 표준편차 σ=0.85 이상인 백색잡음일 때부터 오인식이 발생하였다. 반면, 제안한 MMACE_p 필터를 사용할 경우는 표준편차 σ=1.75 이상인 백색잡음일 때부터 오인식이 발생하였다. 이 결과는 시뮬레이션에 사용된 숫자영상과 백색잡음의 패턴에 따라서 약간의 차이는 있겠으나, 제안한 MMACE_p 필터가 MMACE 필터보다 인식률과 SNR에서 다소 우수한 성능을 가지고 있음을 나타내는 것이다. 이러한 이유는 단순한 숫자영상을 합성하는 MMACE 필터에 비해 공간영역에서 위상암호화된 학습영상을 합성하는 MMACE_p 필터가 보다 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 않고 인식시스템에서 신원을 확인할 수 있도록 하는 것이 더 효과적임을 알 수 있다.

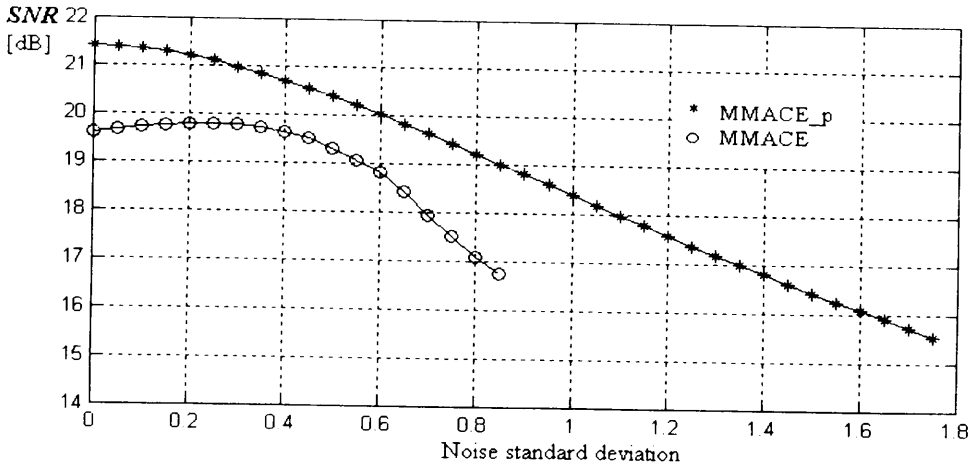


Fig. 14. SNR versus standard deviation in the presence of additive white gaussian noise.

3. 개인 인증

본 논문에서 제안한 개인 인증은 먼저 개인식별번호를 분류·인식하여 개인의 신원을 파악한 후, 그 사람의 얼굴정보와 복원한 영상과의 상관을 통하여 이루어진다. 여기서 얼굴정보는 OWMF의 임펄스응답을 의미하며, 웨이브릿 변환을 이용하여 얼굴영상의 특징점을 추출한 후 데이터베이스에 보관되어진다. 예를 들어, 어떤 사람의 얼굴영상을 웨이브릿 변환하여 얻은 영상의 특징점을 얼굴정보 'OWMF1'이라 하고, 복원한 얼굴영상을 'Face1'이라 한다면, 개인 인증은 얼굴정보(OWMF1)와 복원영상(Face1)과의 상관결과로써 이루어진다. 그리고 다른 사람의 얼굴영상(시험영상)을 광 웨이브릿 변환하여 얻은 영상의 특징점을 얼굴정보 'OWMF2'라 하면, 복원한 얼굴영상(Face1)과 다른 사람의 얼굴정보(OWMF2)와의 상관결과에서는 분리·인식이 이루어져야 오인식이 발생하지 않게 된다.

그림 15(a)는 각 개인의 얼굴영상들로, 제일 왼쪽의 그림이 기준영상이고, 그 다음부터 시험영상1, 시험영상2, 시험영상3, 시험영상4로 사용하였다. 그림 15(b)는 각각의 얼굴영상들을 웨이브릿 변환한 결과로 얼굴영상의 경계선 부분을 강조하고 있음을 확인할 수 있다. 이렇게 추출되는 영상의 특징점들을 얼굴정보로써 데이터베이스에 저장하게 되는 것이다. 그림 15(c)는 암호화된 기준영상을 복원한 영상들로, 제일 왼쪽의 그림이 잡음이 없을 경우이고, 그 다음부터 암호화된 영상에 표준편차가 각각 σ=0.3, σ=0.5, σ=0.7 σ=1인 백색잡음이 더해진 영상을 복원한 영상이며, 이때 발생한 재생손실은 각각 MSE=0.0043, MSE=0.0126, MSE=0.0269, MSE=0.0520이다.

그림 16은 기준영상에 대한 상관결과로써, 여기서 상관결과들은 기준영상의 얼굴정보(OWMF)와 기준영상(reference image)과의 상관첨두치로 정규화하였다. 그림 16(a)는 기준영상의 얼굴정보와 기준영상과의 자기상관결과로써 상관첨두치는 '1'이다. 그림 16의 (b)와 (c), (d), (e), (f)는 기준영상의 얼굴정보(OWMF)와 복원한 얼굴영상들과의 상관결과로 그림 16(b)는 암호화된 기준영상에 잡음이 없을 때

복원한 얼굴영상에 대한 상관결과로써 상관침투치는 '1'이다. 그림 16의 (c)와 (d), (e), (f)는 기준영상의 얼굴정보(OWMF)와 암호화된 기준영상에 표준편차가 각각 σ=0.3, σ=0.5, σ=0.7, σ=1인 백색잡음이 더해졌을 때 복원한 얼굴영상들과의 상관결과로써, 이 때의 상관침투치들은 각각 '0.912', '0.902', '0.834', '0.617'로 모두 예리한 상관침투치가 존재하며, 암호화된 영상을 복원하는 과정에서 어느 정도의 재생손실이 발생하더라도 인식할 수 있음을 확인할 수 있다.

그림 17은 오인식의 발생을 시험하기 위한 것으로써, 그림 17의 (a)와 (b), (c), (d)는 각각 시험영상의 얼굴정보들(OWMF1, OWMF2, OWMF3, OWMF4)과 암호화된 기준영상에 잡음이 없을 때 복원한 얼굴영상과의 상관결과를 나타낸 것으로, 모두 예리한 상관침투치가 존재하지 않으므로 분리·인식이 이루어지고 있음을 확인할 수 있다. 그림 17의 (e)와 (f), (g), (h)는 시험영상의 얼굴정보들과 암호화된 기준영상에 서로 다른 백색잡음이 더해졌을 때 복원한 얼굴영상들과의 상관결과로써, 그림 17(e)는 시험영상1의 얼굴정보(OWMF1)와 암호화된 기준영상에 표준편차 σ=0.3인 백색잡음이 더해졌을 때 복원한 얼굴영상과의 상관결과로 상관침투치는 '0.066'이고, 그림 17(f)는 시험영상2의 얼굴정보(OWMF2)와 암호화된 기준영상에 표준편차 σ=0.5인 백색잡음이 더해졌을 때 복원한 얼굴영상과의 상관결과로 상관침투치는 '0.106'이다. 그림 17(g)는 시험영상3의 얼굴정보(OWMF3)와 암호화된 기준영상에 표준편차 σ=0.7인 백색잡음이 더해졌을 때 복원한 얼굴영상과의 상관결과로 상관침투치는 '0.110'이고, 그림 17(h)는 시험영상4의 얼굴정보(OWMF4)와 암호화된 기준영상에 표준편차 σ=1인 백색잡음이 더해졌을 때 복원한 얼굴영상과의 상관결과로 상관침투치는 '0.136'으로써, 잡음이 존재하는 환경에서도 모두 예리한 상관침투치가 존재하지 않고 분리·인식이 이루어져 오인식이 발생하지 않음을 확인할 수 있다.

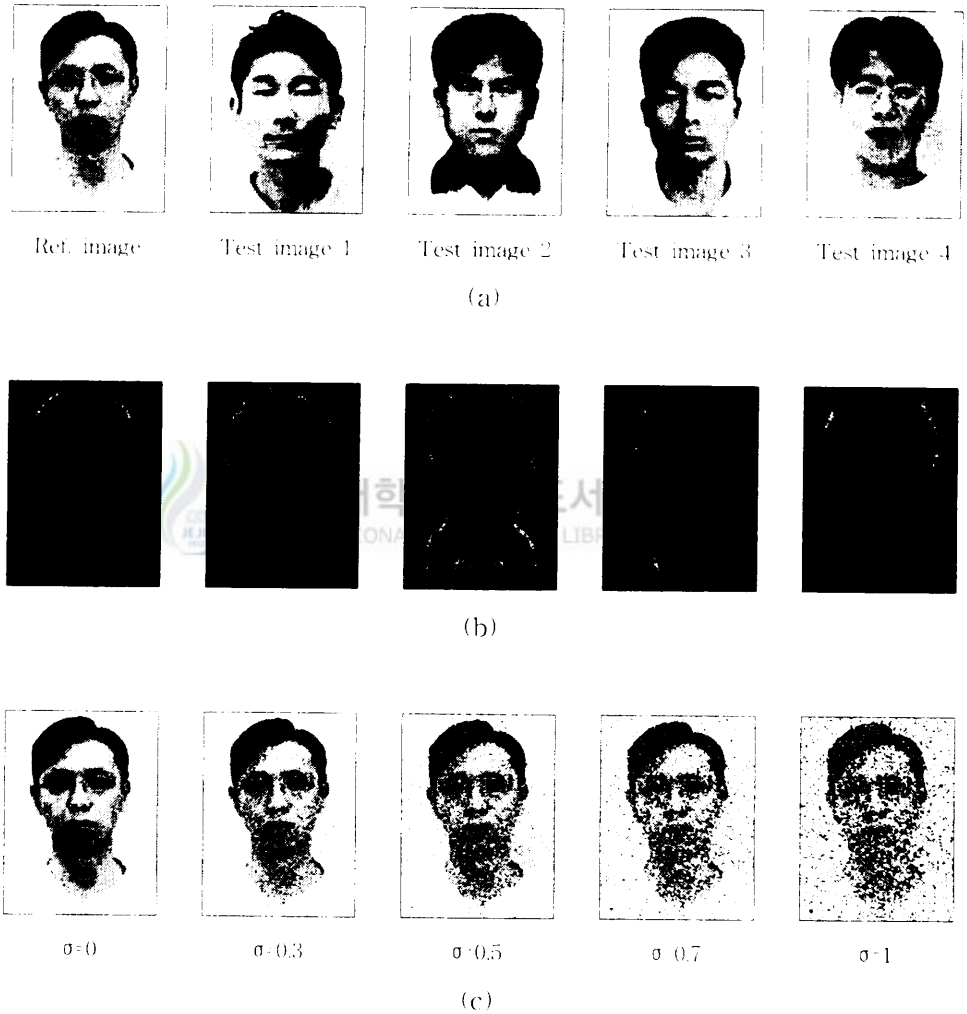
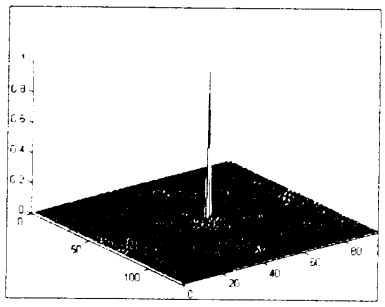
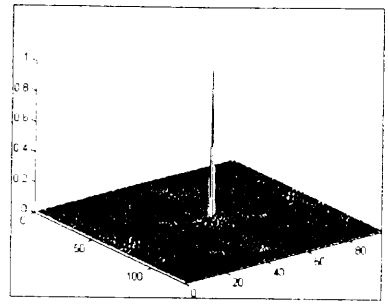


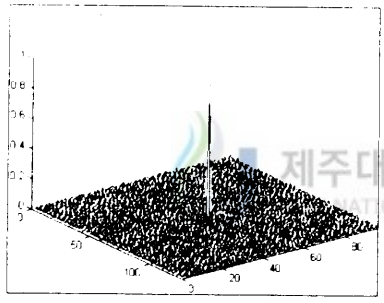
Fig. 15. The Data for verifying the authenticity of the ID card:
(a) original face images,
(b) wavelet transform of the original face images,
(c) recovered image from the encrypted image with white noise.



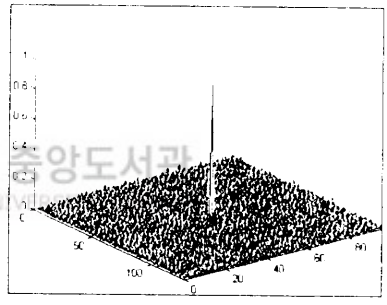
(a) auto-correlation



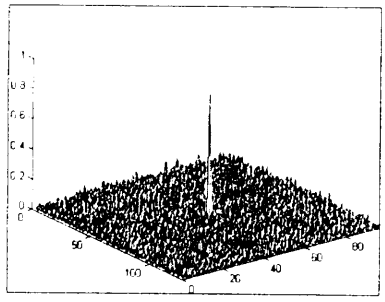
(b) σ=0



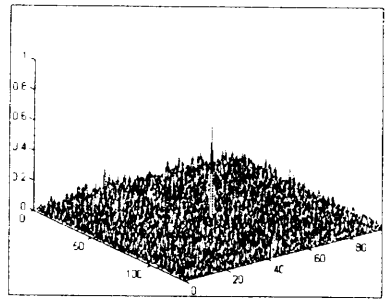
(c) σ=0.3



(d) σ=0.5



(e) σ=0.7

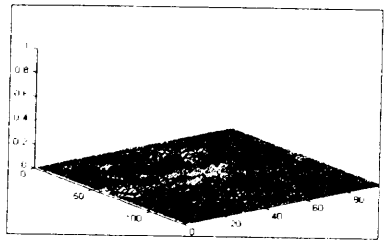


(f) σ=1

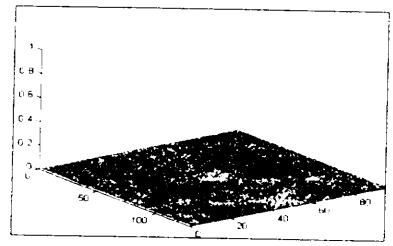
Fig. 16. Correlation results of the reference image:

(a) correlation the OWMF with the reference image,

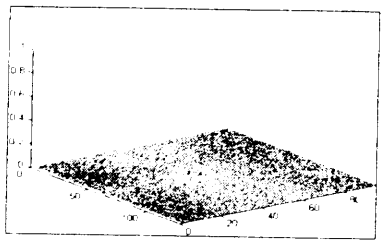
(b), (c), (d), (e), (f) correlatoin the OWMF with the decrypted images.



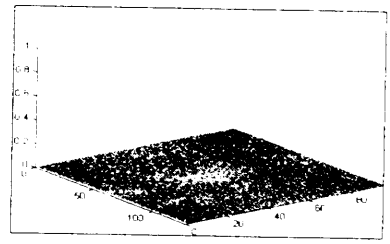
(a) OWMF1



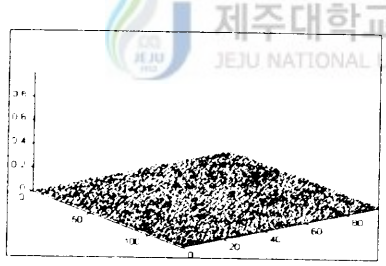
(b) OWMF2



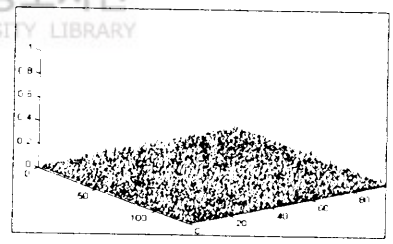
(c) OWMF3



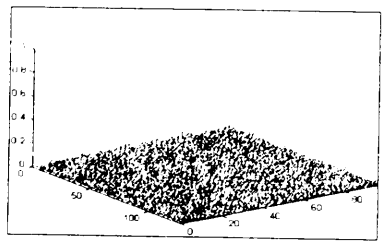
(d) OWMF4



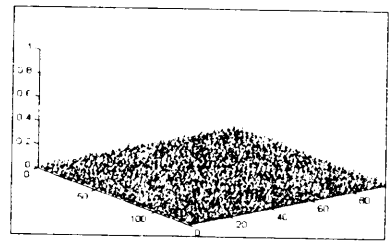
(e) OWMF1, σ=0.3



(f) OWMF2, σ=0.5



(g) OWMF3, σ=0.7



(h) OWMF4, σ=1

Fig. 17. Correlation results of the test images with decryted image:
(a), (b), (c), (d) correlation OWMFs with decrypted image without noise,
(e), (f), (g), (h) correlation OWMFs with decrypted image in additive noise.

그림 18은 백색잡음의 표준편차 σ의 변화에 따른 상관첨두치의 변화를 나타낸 것으로 기준영상에 대하여 상관첨두치가 크다는 것은 인식할 확률이 높다는 것을, 시험영상들에 대하여 상관첨두치가 크다는 것은 오인식할 확률이 높다는 것을 의미한다. 본 논문에서 사용한 얼굴영상에 대해서는 표준편차 σ=0.85인 백색잡음일 때, 기준영상에 대한 상관첨두치는 '0.732'이며, 시험영상1, 시험영상2, 시험영상3, 시험영상4에 대한 상관첨두치는 각각 '0.179', '0.259', '0.132', '0.111'로 나타났는데, 이 경우 경계값을 0.7정도로 하면 표준편차 σ=0~0.85인 경우에 대해서 오인식이 없이 모두 안정적으로 인식할 수 있었다.

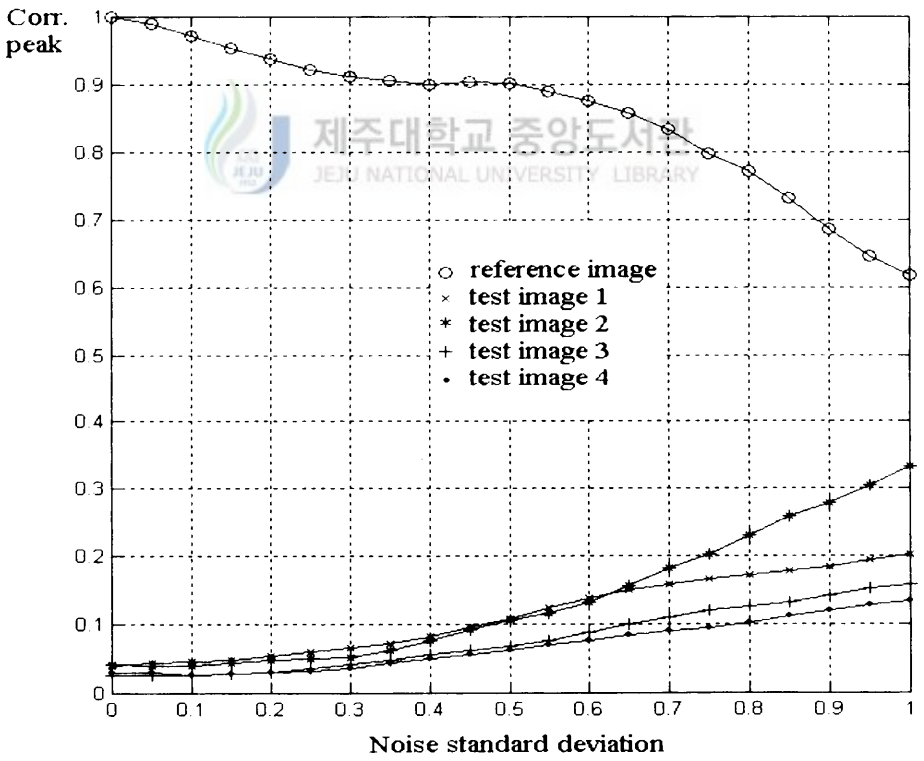


Fig. 18. Correlation peak value versus standard deviation in the presence of additive white gaussian noise.

Ⅵ. 결 론

개인의 신원정보 보호를 위해 본 논문에서 제안한 방법은, 암호화된 신원정보영상을 홀로그램 형태로 신분증에 부착하고, 신분증을 사용할 때에는 암호화된 홀로그램 패턴을 광학적으로 해독하여 실제 정보와 비교함으로써 개인 인증을 하는 방법이다. 개인식별번호 영상과 얼굴영상의 암호화는 공간영역과 공간주파수영역에서 랜덤위상패턴을 사용하여 이중으로 이루어진다. 특히 개인식별번호처럼 개인의 신원정보가 단순히 숫자나 문자의 조합으로 구성되는 경우에는 제안한 영상암호화 방법을 사용하여 암호화한다면, 암호화된 개인의 신원정보 영상을 복원하는 과정이 필요 없게 되어 개인의 신원정보 보호에도 유용하게 사용될 수 있다.

신분증을 이용한 개인의 신분인증은 먼저 개인식별번호를 분류·인식하여 개인의 신원을 파악한 후, 그 사람의 얼굴정보와 복원한 얼굴영상과의 광상관을 취하여 이루어진다. MMACE 필터와 MMACE_p 필터를 사용하여 식별번호를 효과적으로 분류·인식할 수 있음을 확인할 수 있었다. 제안한 MMACE_p 필터는 공간영역에서 위상암호화된 학습영상들을 합성한 필터로, 단순한 숫자영상을 합성하는 MMACE 필터보다 안정된 상관첨두치를 나타내며 SNR이 향상되었다. 그러므로 주민등록번호나 비밀코드처럼 단순히 숫자나 문자의 조합으로 구성되는 개인의 신원정보는 제안한 영상암호화 방법을 사용하여 암호화한 후 신분증에 부착시키고, 개인의 신분을 인증하는 과정에서는 암호화된 영상을 복원하지 않고 인식시스템에서 신원확인이 이루어지도록 하는 것이 더 효과적임을 확인할 수 있었다. 개인식별번호를 분류·인식하여 신원을 파악한 후에는 그 사람의 얼굴정보와 복원한 얼굴영상을 서로 비교하게 되는데, OWMF는 얼굴영상의 특징점들을 추출하는 효과를 가지고 있어 변별력이 뛰어나고, 잡음이 존재하는 환경에서도 오인식은 발생하지 않았다. 제안한 방법으로 개인의 신원정보 보호는 물론, 개인의 신분을 인증할 수 있음을 시뮬레이션 결과를 통하여 확인하였다.

참고문헌

Anderson, C. S. and R. C. Anderson, 1987, "Comparison of phase-only and classical matched filter scale sensitivity," *Opt. Eng.*, vol. 26, no. 3, pp. 276-280.

Burns, T. J., K. H. Fielding, S. K. Rogers, S. D. Pinski and D. W. Ruck, 1992, "Optical Harr wavelet transform," *Opt. Eng.*, vol. 31, no. 9, pp. 1852-1858.

Casasent, D., 1984, "Unified synthetic discriminant function computational formulation," *Appl. Opt.*, vol. 23, no. 10, pp. 1620-1627.

Casasent, D., G. Ravichandran, 1992, "Advanced distortion invariant minimum average correlation energy (MACE) filters," *Appl. Opt.*, vol. 31, no. 8, pp. 1109-1116.

Casasent, D., W. Chang, 1986, "Correlation synthetic discriminant function," *Appl. Opt.*, vol. 25, no. 14, pp. 2343-2350.

노 양희, 1998, "한글문자 인식을 위한 양자화 위상 SDF 필터," *경북대학교 박사 학위 논문*.

Han, J. W., C. S. Park, D. H. Ryu, and E. S. Kim, 1999, "Optical image encryption based on XOR operations," *Opt. Eng.*, vol. 38, no. 1, pp. 47-54.

Horner, J. L. and J. R. Leger, 1985, "Pattern recognition with binary phase-only filter," *Appl. Opt.*, vol. 24, no. 5, pp.609-611.

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

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

Javidi, B., 1998, "Optical Spatial Filtering For Image Encryption and Security Systems," *SPIE*, vol. 3386, pp. 14-23.

Javidi, B., A. Sergent, G. Zhang, L. Guilbert, 1997, "Fault tolerance properties of a double phase encoding encryption technique," *Opt. Eng.*, vol. 36, no. 4, pp. 992-998.

Javidi, B., A. Sergent, 1997, "Fully phase encoded key and biometrics for security verification," *Opt. Eng.*, vol. 36, no. 3, pp. 935-942.

Javidi, B., E. Ahouzi, 1998, "Perfomance of double phase encoding encryption technique using binarized encrypted images," *Opt. Eng.*, vol. 32, no. 2, pp. 565-569.

Javidi, B., E. Tajahuerce, 2000, "Three-dimensinal object recognition by use of digital holography," *Optics Letters*, vol. 25, no. 9, pp. 610-612.

Javidi, B., G. Zhang, and J. Li, 1997, "Encrypted optical memory using double-random phase encoding," *Appl. Opt.*, vol. 36, no. 5, pp. 1054-1058.

Javidi, B., L. Bernard, and N. Towghi, 1999, "Noise performance of double-phase encryption compared to XOR encryption," *Optical Engineering*, vol. 38, no.1, pp. 9-19.

Javidi, B., T. Nomura, 2000, "Securing information by use of digital holography," *Optics Letters*, vol. 25, no. 1, pp. 28-30.

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

김 정우, 1995, "인쇄체 한글의 왜곡불변 인식을 위한 광상관필터," *경북대학교 박사학위 논문*.

Kim, J. Y., S. J. Park, S. J. Kim, 2000, "Optical Encryption System using a Computer Generated Hologram," *Journal of the Optical Society of Korea*, vol. 4, no. 1, pp. 19-22.

이 하운, 김 정우, 김 수중, 1995, "광웨이브릿 fSDF 필터를 이용한 회전불변 지문 인식," *한국통신학회 논문지*, 제20권 7호, pp. 1822-1833.

이 하윤, 1997, "크기와 회전에 무관한 패턴인식을 위한 광 웨이브릿 상관필터," *경북대학교 박사학위 논문*.

Martinet, R. K., J. Morlet and A. Grossmann, 1987, "Analysis of sound patterns through wavelet transform," *Int. J. Patt. Rec. Artificial Intell*, vol. 1, no. 2, pp. 237-302.

Mahalanobis, A., B. V. K. Kumar, and D. Casasent, 1987, "Minimum average correlation energy filter," *Appl. Opt.* vol. 26, no. 17, pp. 3633-3640.

Mallat, S. G., 1989, "A theory for multiresolution signal decomposition: the wavelet representation," *IEEE, Trans. Pattern Anal. Machine Intell.*, 32, pp. 674-693.

Marr, D. and E. Hildreth, 1980, "Theory of edge detection," *Proc. R. Lond.*, B 207, pp. 187-217.

Neto, L. G. 1998, "Implementation of image encryption using the phase-contrast technique," *Proc. of SPIE.*, vol. 3386, pp. 284-290.

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

Roberge, D. and Y. Sheng, 1994, " Optical composite wavelet matched filters," *SPIE*, vol. 2242, Wavelet Applications, pp. 584-591.

Roberge, D. and Y. Sheng, 1994, "Optical wavelet matched filter," *Appl. Opt.* vol. 33, no. 23, pp. 5287-5293.

Sheng, Y., D. Roberge and H. H. Szu, 1992, "Optical wavelet transform," *Opt. Eng.*, vol. 31, no. 9, pp. 1840-1845.

Sheng, Y., D. Roberge, H. Szu, and T. Lu, 1993, "Optical wavelet matched filters for shift-invariant pattern recognition," *Optics Letters*, vol. 18, no.4, pp. 299-301, 1993.

Szu, H. H., Y. Sheng and J. Chen, 1992, "The wavelet transform as a bank of the matched filter," *Appl. Opt.*, vol. 31, pp. 3267-3277.

Tajahuerce, E., O. Matoba, S. C. Verrall, and B. Javidi, 2000, "Optoelectronic information encryption with phase-shifting interferometry," *Appl. Opt.* vol. 39, no. 14, pp. 2313-2320.

Towghi, N., B. Javidi, and Z. Luo, 1999, "Fully phase encrypted image processor," *Optical Society of America*, vol. 16, no. 8, pp. 1915-1927.

Vander Lugt, A., 1964, "Signal detection by complex signal filtering," *IEEE Trans. Infor. Theory*, vol. IT-10, pp. 139-145.

Wang, R. K., I. A. Watson, and C. Chatwin, 1996, "Random phase encoding for optical security," *Optical Engineering*, vol. 35, no. 9, pp. 2464-2469.

Weber, D., J. Trollnger, 1999, "Novel implementation of nonlinear joint transform correlators in optical security and validation," *Opt. Eng.*, vol. 38, no. 1, pp. 62-68.

Yang, S., H. H. Szu, Y. Sheng, H. J. Caulfield, 1992, "Optical Haar wavelet transform of binary image," *Opt. Eng.*, vol. 31, no. 9, pp. 1846-1851.