論文96-33A-12-15

홀로그래픽 영상 암호화 및 디코딩 기법

(Holographic Image Encryption and Decoding Scheme)

楊 勳 其 *, 鄭 大 燮 **, 金 恩 洙 **

(Hoon-Gee Yang, Dae-Sub Jung, and Eun-Soo Kim)

요 약

본 논문에서는 백색잡음을 이용해서 개인의 신상 정보를 나타내는 원영상을 암호화하고 암호화된 영상을 광학적으로 디코딩하는 새로운 보안 인증 기법을 제시한다. 제시된 방법은 홀로그래피의 기록 및 복원과정을 이용하는 것으로서 암호화 과정은 광학적인 방법외에도 FFT루틴을 이용해서 간단히 디지틀적으로 처리할 수 있다. 특히 디지틀적 방법으로 암호화시키면 복원시킬 때 잡음성분을 원영상으로부터 분리시키는데 도움을 준다. 이와 같이 하여 얻어진 인코딩된 결과는 원영상 및 백색잡음 영상을 통과한 두 광파의 간섭패턴 분포와 유사하게 된다. 실시간적으로 수행될 수 있는 디코딩 과정은 암호키에 해당하는 백색잡음 영상을 통과한 빛을 암호카드에 조사하므로서 광학적으로 원영상을 복원시키게 된다. 암호영상 및 암호키에 사용할 데이터는 위상형 데이터 뿐만 아니라 실수 형태의 데이터를 사용할 수 있음을 수학적으로 증명하였으며 증명된 결과가 시뮬레이션 결과와 일치함을 보인다.

Abstract

This paper presents a new security verification technique based on an image encryption by a white noise image that serves as an encryption key. In the proposed method that resembles holographic process, the encryption process is executed digitally using FFT routine which gives chances for separating corruptive noise from reconstructed primary image. The encoded image thus obtained is regarded as an interference pattern caused by two lightwaves transmitted through the primary image and the white noise image. The decoding process is executed optically and in real-time fashion where lightwave transmitted through the white noise image illuminates the encrypted card. We analytically prove that real-type data as well as phase-type data can be used for both an encoded image and an

Ⅰ. 서 론

일반적으로 여권, 신용카드, 각종 ID 카드등의 위조 여부를 확인하기 위한 수단으로 사진, 얼굴, 지문 등이 사용되고 있으나 최근, 컴퓨터, 영상처리 및 프린터 기술들의 발달과 더불어 각종 카드 등의 위조가 고도로 정교하게 이루어짐에 따라 현대 신용 사회에서 심각한 사회문제로 대두되고 있다.

근래에는 보다 발전된 형태로 신용카드와 여권 등에 홀로그램이 널리 이용되고 있으나 이것은 사람의 눈에 의해 검색되는 것으로 이론적으로는 복제될 수 없지만 실제 경우 홀로그램 패턴이 광세기 패턴으로 CCD와 같은 기존의 광검출기로 쉽게 검출되어 새로운 홀로그램의 합성과 복제가 가능하게 된다. 따라서, 어떠한 경우에도 ID 카드 위조나 복제를 근본적으로 차단할 수 있는 새로운 접근 방법에 대한 많은 연구가 이루어지

* 正會員, 光云大學校 電波工學科 新技術研究所
(Dept. of Radio Science & Eng., Institute of New Technology, Kwangwoon Univ.)
** 正會員, 光云大學校 電子工學科 新技術研究所
(Dept. of Electronic Eng., Institute of New Technology, Kwangwoon Univ.)

接受日字: 1996年4月18日, 수정완료일: 1996年12月9日

고 있으며, 최근에는 CCD와 같은 기존의 광세기 검출기로는 볼 수도 복제될 수도 없는 복소함수 형태의 랜덤위상 패턴을 사용하는 새로운 광학적 보안 기법이 제시되고 있다.

Refregier는 원래의 영상(primary image)에 두 가지 랜덤 위상 마스크로 영상을 암호화하는 새로운 영상 암호화 기법을 제시하였다. 즉, 두 랜덤 마스크중 하나는 입력 평면에, 다른 하나는 공간 주파수 평면에 위치해서 궁극적으로 원영상이 stationary 백색잡음 형태로 변환되며,[1,2] 디코더(암호해독) 시스템에서는 암호카드 영상을 광학적으로 퓨리에 변환한 후, 변환된 값에 암호키에 해당하는 랜덤 위상 마스크의 공액 복소값을 곱하게 된다. 그리고, 그 결과를 광학적으로 다시 역퓨리에 변환하여 검출기가 위치해 있는 평면에서 원영상을 복구하게 된다. 그러나, 이 방법은 암호화된 영상이 복소수값을 가지므로 카드를 제작하기 어려울 뿐 아니라, 디코더에는 복소값을 나타낼 수 있는 실시간 공간 광 변조기(SLM : spatial light modulator)가 요구된다는 점등이 문제점으로 제시되고 있다.

한편, Javidi는 원영상 위에 랜덤 위상 마스크를 접착시키므로써 암호화하는 단순한 방법을 제시하였다. 디코더에서는 암호카드와 랜덤 위상 마스크에 해당하는 기준영상을 JFT(joint Fourier transform)시키고, JTPS(joint transform power spectrum)을 검출한 후, 이것을 다시 역퓨리에 변환시키게 된다[3,4]. 따라서, 카드의 진위는 상관 첨두값을 검사하므로써 판정할 수 있는데 이 방법은 Refregier의 방법에 비해 시스템 정렬(alignment)에 그다지 민감하지 않기 때문에 디코더의 제작이 용이한 장점을 갖지만 데이터에 손상을 주지 않으면서 교묘하게 위상 마스크를 떼어 내면, 카드를 위조할 수 있다는 심각한 단점을 지니고 있다.

따라서, 본 논문에서는 카드 위조를 근본적으로 차단하고 실질적으로 구현이 가능한 접근방법으로 원영상을 실수값으로 암호화시킬 수 있고, 더우기 암호키로 실수값 패턴을 이용할 수 있는 새로운 홀로그래픽 영상 암호화 및 디코딩 기법을 제시하고자 한다. 2.1절에서는 홀로그래픽 영상 암호화 및 디코딩 방법에 대한 이론적 분석을 기술하고, 2.2절에서는 위조방지를 근본적으로 막기위한 랜덤 위상 함수의 사용에 대해 서술한다. 2.3절에서는 구현을 위한 데이터 변환 방법 및 그 효과를 분석하고 3장에서는 시뮬레이션 결과를 제시하고자 한다.

Ⅱ. 제안된 방법의 이론적 분석

1. 영상 암호화 및 디코딩 이론

1) 영상 암호화 기법

개인 신원에 대한 정보를 담고 있는 원영상을 $f(x,y)$라고 하자. 이 영상은 암호화된 후 최종 출력 평면에서 암호키에 의해 재생될 영상으로 검출기로 포착될 수 있도록 충분히 작아야 한다. $g(x,y)$는 실수 함수로서 $f(x,y)$를 인코딩할 뿐만 아니라 $f(x,y)$를 복원 즉, 암호 카드를 해독하는 암호키 역할을 하는 함수를 나타낸다. 이러한 두 영상이 주어졌을 때, 암호화된 영상 $H(u,v)$ 는

$$H(u,v) = F(u,v)G^*(u,v)\exp[-j(d_1+d_2)v] + F^*(u,v)G(u,v)\exp[j(d_1+d_2)v] \quad (1)$$

와 같이 디지틀적으로 계산할 수 있다. 여기서, d_1와 d_2는 임의로 선택할 수 있는 상수이고, *는 공액복소수를, u,v는 공간 주파수를 나타내며 $F(u,v)$와 $G(u,v)$는 $f(x,y)$와 $g(x,y)$의 퓨리에 변환을 각각 나타낸다. 식(1)에서 우변에 있는 두 항은 서로 공액관계에 있으므로 $H(u,v)$는 실수 함수가 된다. 참고로 함수 $H(u,v)$는 그림 1과 같은 광 JTC(joint transform correlator) 시스템의 입력 평면상의 좌표 $(0.,d_1)$와 $(0.,d_2)$에 $f(x,y)$와 $g(x,y)$를 각각 위치시키고 평면파를 조사하여 JFT(Joint Fourier Transform)함으로써 광학적으로도 얻을 수 있다.

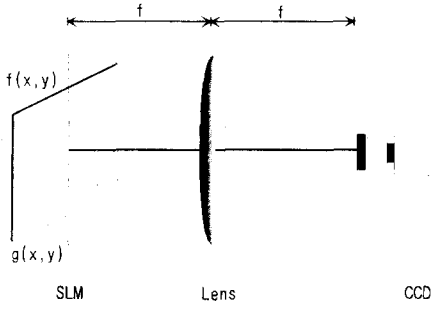


그림 1. 광 JFT 시스템
Fig. 1. Optical Joint Fourier Transform system.

이때, CCD에 검출된 JTPS는 $|F(u,v)|^2+|G(u,v)|^2+H(u,v)$와 같이 주어지며, $|F(u,v)|^2$와 $|G(u,v)|^2$는 광전자적으로 JTPS에서 간단히 제거될 수 있다[5]. 하지만 식(1)에 의해서 얻어진 $H(u,v)$는 해독할 수

있는 여지가 있으므로 (2.2 절에서 설명했음.) 랜덤위상 함수를 곱하여야 한다. 이 과정은 본 논문에서 제시된 바와 같이 디지틀적으로는 간단히 처리되지만 광학적으로는 위상 마스크를 이용해야 하므로 참고문헌 [3] 에서 제시한 Javidi 방법 보다 개선된 점이 없다.

2) 암호해독(디코딩) 기법

암호화된 영상 $H(u,v)$에서 원영상 $f(x,y)$를 복원하는 암호해독(디코더) 시스템은 그림2과 같이 구성할 수 있으며 이는 일반적인 퓨리에 홀로그램의 복원 시스템과 유사함을 알 수 있다.

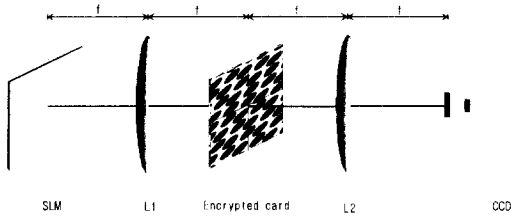


그림 2. 디코딩 시스템
Fig. 2. Decoding system.

그림2에서 암호키 역할을 하는 $g(x,y)$가 SLM상의 $(0.,d_2)$에 위치해 있다고 하자. 이때, 함수 $g(x,y)$는 렌즈 L_1에 의해 퓨리에 변환되어 $G(u,v)\exp[-jd_2v]$으로 주어지며, 암호화된 ID 카드 함수 $H(u,v)$와 곱해진 후 렌즈 L_2에 의해 다시 역퓨리에 변환된다. 이때, 역퓨리에 변환된 출력 함수는

$$p(x,y) = f(x,y-d_1)\circledast g(-x,-y)\circledast g(x,y) + f(-x,-y)\circledast g(x,y)\circledast g(x,y)\circledast\delta(x,y+d_1-2d_2) \quad (2)$$

와 같이 표현할 수 있다. 식(2)에서 ⊛는 콘볼루션(convolution)을 나타내며, $G^*(u,v)$의 역퓨리에 변환은 $g^*(-x,-y)$이나 $g(x,y)$는 실수 함수이므로 공액표시(*)는 생략하였다. 암호키인 $g(x,y)$에 가장 이상적인 패턴은 자기상관함수 $g(x,y)\circledast g(-x,-y)$가 임펄스 함수 $\delta(x,y)$에 가장 가깝도록 하는 함수로서 만약, 자기상관함수가 $\delta(x,y)$라면 식(2)의 오른쪽의 첫번째 항은 $f(x,y-d_1)$이 될 것이다.

따라서, $g(x,y)$가 백색잡음인 경우 서로 다른 위치에서 표본화된 임의의 두 값은 완전히 상관관계가 없게 되므로 암호키 함수로서 가장 적당하다고 말할 수 있다. $g(x,y)$가 백색잡음인 경우 식(2)의 오른쪽의 두 번째 항에서 $g(x,y)\circledast g(x,y)$는 결과적으로 균일하게 분포된 또다른 백색잡음이 되며, 이 함수는 기저대역 필터의 역할을 하는 $f(-x,-y)$를 통과하면서 smoothing 된다. 또한, $g(x,y)$ 함수의 유한한 개구를 고려한다면 잡음성분은 $(0.,-d_1+2d_2)$에 중심을 두고 비교적 균일하게 퍼지게 되며, 이 잡음은 d_1과 d_2 값을 적당히 선택하므로서 원영상으로 부터 분리될 수 있다. 따라서, 이 잡음성분이 적당히 분리되면, 출력 평면상의 좌표 $(0.,d_1)$에 위치한 검출기의 중심에서 원영상을 검출하게 된다.

2. 원영상의 랜덤위상 코딩

원영상 $f(x,y)$는 실수 함수이고, 암호키 $g(x,y)$는 균일하게 분포된 백색잡음으로 주어진 경우 $g(x,y)$에 관한 부분적인 정보는 예측이 불가능하나 $f(x,y)$는 개인신원에 관한 정보이므로 부분적인 진폭 정보는 우연히 예측할 수 있다. 우선, 이 부분적인 진폭정보로부터 암호키 해독, 더 나아가 ID 카드의 복제가 가능한지를 조사해 보자. 고려할 수 있는 방법으로 이종연상루프(hetero-associative loop)을 생각할 수 있다[16]. $f_1(x,y)$이 부분적 진폭패턴을 나타낸다고 가정하자. 이때 $f_1(x,y)$의 퓨리에 변화인 $F_1(u,v)$를 계산하고, $F_1(u,v)$에 $H(u,v)$를 곱한 후, $F_1(u,v)H(u,v)$의 역퓨리에 변환을 실행하여 보자. 그 결과는

$$p_1(x,y) = IFT[F(u,v)F_1(u,v)G^*(u,v)]\circledast\delta(x,y-(d_1-d_2)) + IFT[F^*(u,v)F_1(u,v)G(u,v)]\circledast\delta(x,y+(d_1-d_2)) \quad (3)$$

와 같이 표현할 수 있으며 여기서, IFT는 역퓨리에 변환을 나타내고 있다. 식(3)의 우변 첫 번째 항은 잡음성분을 나타내고 둘째 항은 $f_1(x,y)$가 우연히 $f(x,y)$이라면, $g(x,y+d_1-d_2)$로 주어지게 된다. 그러나, $f_1(x,y)$는 부분적인 진폭이므로 $f(x,y)$는

$$f(x,y) = f_1(x,y) + f_2(x,y) \quad (4)$$

처럼 표현할 수 있으며 여기서, $f_2(x,y)$는 원영상에서 부분 정보를 뺀 나머지 패턴이다. 식(4)를 이용하여 식(3)의 우변 둘째 항을 정리하면

$$IFT[F_1^*(u,v)F_1(u,v)G(u,v)]\circledast\delta(x,y+(d_1-d_2)) + IFT[F_2^*(u,v)F_1(u,v)G(u,v)]\circledast\delta(x,y+(d_1-d_2)) \quad (5)$$

이 된다. 식(5)의 첫째 항은 $g(x,y+d_1-d_2)$이고, 둘째

항은 잡음 형태를 갖게 된다. 따라서, 원영상 $f(x,y)$만큼은 안돼도 부분적인 영상정보 $f_1(x,y)$를 통해 암호키 $g(x,y)$를 연상 유추하는데 이용될 수 있음을 알 수 있다. 즉, $f_1(x,y)$를 이용해서 $p_1(x,y)$를 구한 후 $p_1(x,y)$의 진폭을 적당히 thresholding 하므로서 $g(x,y)$와 유사한 암호키인 $g_1(x,y)$를 얻을 수 있고, 다시 $g_1(x,y)$를 이용해서 2.1절에서 서술한 디코딩 과정을 따르면, $f_1(x,y)$보다 $f(x,y)$에 가까운 또다른 부분적 진폭패턴을 복원할 수 있다. 결과적으로, 위에서 언급한 과정을 이종연상 루프를 통해 반복 수행하게 되면 연상 메모리 기능에 의해 원영상 $f(x,y)$뿐만 아니라 $g(x,y)$도 구할 수 있으며, $f(x,y)$를 불법의 다른 영상으로 대치시키고 $g(x,y)$를 이용하므로서 위조 카드의 제작이 가능해지게 된다. 따라서, 앞에서 기술한 암호해독 및 위조 가능성에 대한 문제점을 근본적으로 해결할 수 있는 방법으로 랜덤 위상 함수 $\exp[j\phi(x,y)]$가 곱해진 원영상을 사용할 수 있다. 그러므로 이 함수가 $f_r(x,y)$라 하면, $f_r(x,y)$는 $f_r(x,y)=f(x,y)\exp[j\phi(x,y)]$로 정의될 수 있다. 그러므로 이 경우, 암호화된 영상 $H(u,v)$는

$$H(u,v)=F_r(u,v)G^*(u,v)\exp[-j(d_1-d_2)v] + F_r^*(u,v)G(u,v)\exp[j(d_1-d_2)v] \quad (6)$$

와 같이 표현되는데 여전히 실수 함수로 주어짐을 알 수 있다. 그러나, $f_r(x,y)$에 관한 부분적 정보는 원영상을 그대로 사용하는 경우와 달리 랜덤 위상 함수 코딩 때문에 결코 예측할 수 없으므로 아무리 이종연상 루프를 $f_r(x,y)$에 적용한다 하더라도, $g(x,y)$ 및 $f(x,y)$는 결코 추정할 수 없게 된다.

3. 데이터 변형

일반적으로, 식(1)에 따라 계산된 $H(u,v)$ 함수를 ID 카드 제작에 직접 이용하는 경우, 비록 $H(u,v)$가 실수 함수이지만, 반드시 양의 실수 함수인 것만은 아니므로 제작상 어려움이 따르게 된다. 이러한 문제점을 해결하기 위한 2가지 접근 방법을 제시하고자 한다. 먼저, 첫번째 방법으로, $H(u,v)$에 일정한 정수 a를 더해 줌으로써 $H(u,v)$의 값을 양수화 할 수 있다. 결과적인 암호 영상 $H_a(u,v)$는

$$H_a(u,v)=H(u,v)+a \quad (7)$$

와 같이 주어질 수 있으며, 이 경우 디코더 출력함수는

$$p_a(x,y)=p(x,y)+a\times g(x,y+d_2) \quad (8)$$

이 된다. 식(8)의 우변 둘째항의 바이어스로 인한 잡음은 $(0.,-d_2)$에 위치하게 되므로, $f(x,y)$가 복원되는 영역에서 분리될 수 있다. 그러나, a값이 큰 경우 대부분의 에너지는 $f(x,y)$를 복원하는데 기여하지 못하고 잡음으로 소모됨으로써 복원영상의 컨트라스크가 저하될 수 있다. 두 번째 방법은 $H(u,v)$를 위상 형으로 변형시키는 방법으로서 $H(u,v)>0$일때 $\exp[j0]$로, $H(u,v)<0$일 때 $\exp[j\pi]$로 각각 코딩하여, 위상타입의 매질로 ID 카드를 제조할 수 있다. $H(u,v)$는 $\exp[j0]$와 $\exp[j\pi]$로 코딩하는 대신 $\exp[j\pi/2]$와 $\exp[-j\pi/2]$ 혹은 $\exp[-j\pi/2]$와 $\exp[j\pi/2]$로 코딩될 수도 있으며, 만약 $\exp[j\pi/2]$와 $\exp[-j\pi/2]$로 코딩된다면, 양자화 잡음이 없는 경우 디코더 출력함수는 $jp(x,y)$로 주어짐으로 광 세기 함수는 $p(x,y)$와 같게 된다.

ID 카드 제작을 위한 $H(u,v)$ 데이터의 변형 이외에, 암호키 $g(x,y)$를 SLM에 표현할 수 있는 데이터형태로의 변형도 요구되는데, 앞에서 언급한 바와 같이 양의 실수 혹은 위상 타입으로 암호키를 만들 수 있다. 양의 실수 함수로 만드는 경우 일정한 상수 b를 더하게 되면 SLM에 표현될 암호키 함수 형태는

$$g(x,y-d_2)+b\times rect(\alpha x,\alpha(y-d_2)) \quad (9)$$

로 주어진다.

여기서, α는 $rect(\cdot)$ 함수의 크기가 암호키의 크기와 동일하도록 만드는 스케일 계수를 나타낸다. 이 경우 디코더에 도달한 출력함수 $p_b(x,y)$는

$$p_b(x,y)=p(x,y)+b\times f(x,y)\otimes g(-x,-y)\otimes rect(\alpha x,\alpha(y+d_1-2d_2)) + b\times f(-x,-y)\otimes g(x,y)\otimes rect(\alpha x,\alpha(y-d_1)) \quad (10)$$

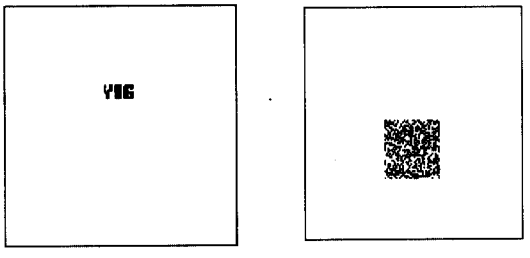
와 같이 주어지며, 식(10)을 살펴보면 상수 b는 $(0.,d_1)$과 $(0.,-d_1+2d_2)$에 중심을 둔 두가지의 잡음을 야기시킴을 알 수 있다.

Ⅲ장에서는 암호영상 및 암호키를 양의 실수와 위상 형태로 표현했을 때의 암호해독 과정에 대한 각각의 시뮬레이션 결과를 제시하였다.

Ⅲ. 시뮬레이션

본 논문에서는 원영상의 디지틀적 계산에 의한 암호화 과정과 광학적 디코딩 과정을 시뮬레이션 하였다. 원영

상은 128×128 크기를 갖는 "YHG" 글씨 이다. 그림 3(a)는 원영상 함수가 512×512 null 어레이에 위치해 있는 경우의 진폭 분포를 나타내고 있다. 암호키에 해당하는 백색잡음은 128×128 크기를 갖고 1과 -1이 랜덤하게 분포된 함수로서 그림3(b)에 나타내었다. 암호키의 진폭값은 모두 1로서 같지만 디스플레이를 위해서 그림3(b)에서는 1과 -1을 그레이 레벨 0과 255로 각각 나타내었다. $F(u,v)\exp[-jd_1v]$를 구하기 위해 512×512 어레이내의 특정 위치 $(0.,d_1)$에 $f(x,y)$를 위치시킨 후, 512×512 어레이에 대한 2차원 FFT(Fast Fourier Transform)를 취하였다. $G(u,v)\exp[-jd_2v]$도 유사하게 계산할 수 있으며, (u,v) 평면상의 두 2차원 함수를 이용해서 $H(u,v)$를 계산하였다. 본 시뮬레이션에서는 d_1은 어레이내의 64개의 표본 간격에 해당하는 거리라 가정했으며, d_2는 $-d_1$과 같게 하였다. 2.3절에서 언급했듯이 $H(u,v)$는 실질적인 구현을 위해 양의 실수형과 위상형으로 데이터를 변형하였다. 그림4(a) 와 그림4(b)는 양의 실수값과 위상 값으로 각각 표현된 $H(u,v)$의 분포를 보여주고 있다.

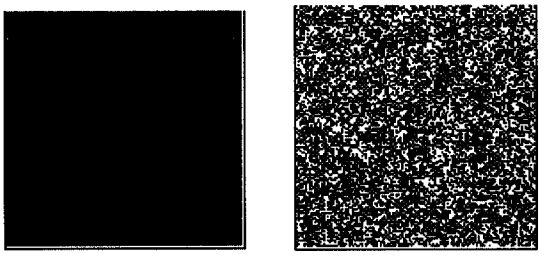


(a) (b)

그림 3. (a) 암호화 시킬 원영상
(b) 기준 영상

Fig. 3. (a) Primary image to be encoded
(b) Reference image.

위상 형태의 데이터는 그림 3(b)에서 처럼 두개의 그레이 레벨 0과 255로 나타내었다. 암호키 $g(x,y)$는 +1과 -1로 구성된 2진 위상 함수이기 때문에 이미 위상형태를 취하고 있다고 말할 수 있다. 양의 실수형으로의 데이터 수정은 +1만 전체 데이터에 더하므로서 간단히 얻을 수 있다. 그림 5는 위상형 데이터로 영상 및 암호키를 코딩한 경우 디코딩된 복원영상을 나타내고 있다.



(a) (b)

그림 4. (a) 양의 실수값으로 암호화된 영상
(b) 위상타입으로 암호화된 영상

Fig. 4. (a) Encoded image in positive real type
(b) Encoded image in phase-only type

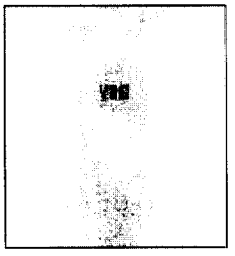


그림 5. 위상형의 암호영상 및 암호키를 사용하여 복원된 원영상

Fig. 5. Reconstructed image using phase-only type encoded image and encryption key

여기서, 원영상 성분은 $(0.,d_1)$에서 복원되었으며, 식 (2)의 둘 째항 때문에 생기는 간섭잡음은 $(0.,-d_1+2d_2)$과 일치하는 위치에 중심을 두고 있다. 그림6는 양의 실수로 영상을 코딩하고, 암호키를 위상타입의 데이터를 사용했을 때 디코딩된 결과를 나타낸 것이다.

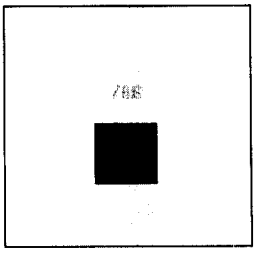


그림 6. 양의 실수형태의 암호영상과 위상형의 암호키로 복원된 원영상

Fig. 6. Reconstructed original image using real-positive type encoded image and phase-only type encryption key.

식(8)에서 예상했듯이, 사각형 형태의 간섭잡음이 $(0., d_2)$을 중심으로 해서 발생함을 볼 수 있다. 그림6에서 잡음이 까맣게 나온 이유는 $g(x,y)$의 진폭이 균일하게 1이기 때문이다. 그림7은 암호키가 0과 2로 구성된 양의 실수함수이며, 영상이 위상 타입으로 인코딩된 경우에 복원된 영상이다.

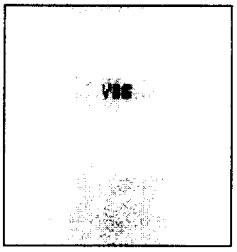


그림 7. 위상형의 암호영상과 양의 실수형태의 암호키로 복원된 원영상
Fig. 7. Reconstructed image using phase-only type encoded image and real-positive type encryption key.

여기서는 $f(x,y)$이외에 두개의 간섭 성분이 존재하게 되며, 이것은 2.3절에서 분석됐듯이, 하나의 성분은 원영상 성분이 복원되는 위치와 일치하는 $(0., d_1)$에 중심을 두고 다른 하나는 $(0., -d_1+2d_2)$에 위치하여 나타난다. 그림8에서 보여준 영상은 영상 및 암호키를 모두 양의 실수 형태로 코딩하였을 때 복원된 결과이다.

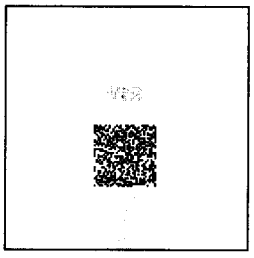


그림 8. 양의 실수형태의 암호영상 및 암호키를 사용하여 복원된 영상
Fig. 8. Reconstructed image using real-positive type encoded image and encryption key.

그림에서 식(8)의 a에 의해 생긴 사각형 형태의 잡음과 식(9)의 b로 인한 두개의 간섭 성분을 볼 수 있다. 이 경우 대부분 에너지가 잡음 성분을 출력시키는데 소모되므로, $f(x,y)$의 광 세기는 아주 낮게 나타난다. 그림9에서는 암호영상 및 암호키가 위상타입으로 코딩되어 있고 SLM이 원래의 위치에서 (Δ_x, Δ_y)만큼 비껴나서 있을 때 디코딩된 결과를 제시하였다. 복원영상의 선명도는 같지만 원래 복원 위치에서 $(-\Delta_x, -\Delta_y)$만큼 비껴나서 출력되었다. 만약 카드가 $(0., d_1)$에서 (Δ_x, Δ_y) 만큼 비껴 나서 입력되었다면 $(-\Delta_x, -\Delta_y)$ 만큼 이동하여 원영상이 복원되는 것이 아니라 blur 된다. 그 이유는 암호카드와 암호키가 주파수 평면에서 곱해지기 때문이며 그러므로 암호 영상과 암호키 사이에 이동 불변 복원특성은 보장할 수 없다.

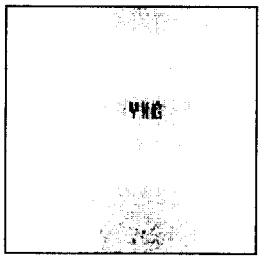


그림 9. 정렬이 정확히 안되었을 때 복원된 영상
Fig. 9. Reconstructed image in case of out-of-alignment.

Ⅳ. 결 론

본 논문에서는 FFT 루틴을 이용해서 디지틀적으로 영상을 암호화하는 방법 및 암호화할 때 사용했던 백색 잡음 형태의 암호키를 이용해서 실시간적으로 원영상을 복원시키는 디코딩 방법을 제시하였다. 디지틀적으로 암호화를 할 때는 두개의 파라미터 값을 적당히 선택하므로써, 원영상에서 간섭잡음을 분리해 낼 수 있었다. 제시된 방법은 원영상에 랜덤 위상 함수를 곱하므로서, 이종연상 루프등을 이용하여도 암호 영상을 실질적으로 디코딩할 수 없게 하였다. 양의 실수 혹은 위상 형태를 갖는 데이터를 이용해서 암호 영상이나 암호키를 표현할 수 있게 하여 실질적인 구현 가능 방법을 제시하였다. 시뮬레이션 결과, 암호 영상에 사용된 데이터가 양의 실수인 경우, 간섭잡음이 복원 영상보다 더 지배적이다. 만약 양의 실수 데이터가 암호 영상과 암호키 모두에 사용된다면, 비록 간섭잡음의 분리가 가능하더라도 원영상을 복원하는데 기여하는 광세기는 현저하게 작아진다. 반면, 암호 영상과 암호키에 위상 타입의 데이터를 사용해서 얻은 복원 영상은 가장 좋

은 결과는 보여 주었다.

참 고 문 헌

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding", Opt. Lett., vol.20, pp.767-769, 1995.

[2] M. H. Hayes, J. S. .Lim and A. V. Oppenheim, "Signal reconstruction from phase or magnitude", IEEE Trans. ASSP, vol.28, pp.672-680, 1980.

[3] B. Javidi and J. L. Honer, "Optical pattern recognition for validation and security verification", Opt. Eng., vol.33, pp.1752-1756, 1994.

[4] B. Javidi, "Nonlinear joint power spectrum based optical correlation", Appl. Opt., vol.28, pp.2358-2367, 1989.

[5] Sang-Yi Yi, Eun-Soo Kim and Hoon-Gee Yang, "A BPEJTC-based Segmentation for a Nonstationary Image.", Opt. Comm., vol.123, pp.716-724, 1996.

[6] Eun-Soo Kim, Seung-Hyun Lee and Woo-Sang Lee," Optical implementation of a holographic heteroassociative memory system", Jpn. J. Appl. Phys., vol.29, pp.1304-1306, 1990.

저 자 소 개

楊 勳 其(正會員) 第 33卷 第 1號 參照
현재 광운대학교 전파공학과 조교수

金 恩 洙(正會員) 第 33卷 第 10號 參照
현재 광운대학교 전자공학과 교수

鄭 大 燮(正會員)
1970년 1월 29일생. 1995년 8월 서울산업대학교 전자공학과 졸업(공학사). 1995년 9월 ~ 현재 광운대학교 전자공학과 석사과정. 주관심분야는 컴퓨터 비젼, 패턴인식, 영상코딩