論文2003-40SD-9-5

가상위상영상을 이용한 잡음 및 변이에 강한 암호화 시스템

(Shift and Noise Tolerance Encryption System using a Phase-Based Virtual Image)

徐 東 煥 *, 金 秀 重 *

(Dong-Hoan Seo and Soo-Joong Kim)

요 약

본 논문에서는 위상 변조된 가상 영상을 이용하여 암호화 수준을 향상시키고 퓨리에 영역에서 잡음이나 변이에 강한 복호화 방법을 제안하였다. 암호화된 영상은 원 영상이 아닌 위상 변조된 가상 영상과 무작위 위상 영상을 곱하여 퓨리에 변환하여 만든다. 따라서 허가되지 않은 사용자가 암호화된 영상을 분석함으로써 있을 수 있는 복제 가능성을 원 영상의 어떤 정보도 포함하지 않은 가상 영상을 사용함으로써 배제할 수 있다. 복호화 과정은 암호화된 영상과 제안한 위상 대응 규칙으로 만들어진 퓨리에 복호화 키를 간섭시킨 후 퓨리에 역변환하여 간단히 원 영상을 재생하고 컴퓨터 모의 실험을 통하여 제안한 방법의 암호화된 영상과 복호화 키 영상에 잡음이나 영상의 절단, 변이가 발생하더라도 원 영상의 복원이 가능함을 확인하였다.

Abstract

In this paper, we propose an improved image encryption and the shift-tolerance method in the Fourier space using a virtual phase image. The encrypted image is obtained by the Fourier transform of the product of a phase-encoded virtual image, not an original image, and a random phase image. Therefore, even if unauthorized users analyze the encrypted image, we can prevent the possibility of counterfeiting from unauthorized people using virtual image which dose not contain any information from the original image. The decryption technique is simply performed by inverse Fourier transform of the interference pattern between the encrypted image and the Fourier decrypting key, made of proposed phase assignment rule, in frequency domain. We demonstrate the robustness to noise, to data loss and shift of the encrypted image or the Fourier decryption key in the proposed technique.

Keyword : optical security, interferometer, phase image

Ⅰ. 서 론

현대 사회가 정보화 사회로 발전해 감에 따라 각종 정보공유의 필요성이 커져 가고 있으며 이를 위한 여러 가지 수단이 연구되어 온 반면 한편에서는 허가되지 않은 개인이나 그룹의 불법적인 접근이나 사용으로부터 특정 정보를 보호하기 위한 수많은 보안 체계와 암호 체계들이 제안되고 구현되어 왔다. 최근에는 광학

* 正會員, 慶北大學校 電子電氣컴퓨터學部
(School of Electronical Engineering & Computer Science, Kyungpook Nat'l Univ.)

※ 본 연구는 정보통신부 기초기술연구지원사업(과제번호 : C1-2002-012-0-3) 지원으로 수행되었음.
接受日字:2002年12月18日, 수정완료일:2003年9月1日

기술을 이용한 보안 시스템에 관한 연구가 활발히 진행되고 있는데 이는 광의 병렬성과 고속성을 충분히 이용할 뿐만 아니라 위상 정보와 세기 정보를 동시에 광학 매질에 기록할 수 있으므로 사람의 눈이나 세기 검출기로는 위상정보를 추출하는 것이 불가능하여 위조나 복제를 근본적으로 차단할 수 있다는 특성에 기인한다. 이러한 광 암호화 시스템들은 주로 4-f 광 상관기(correlator)나 간섭계를 이용하여 입력평면에 세기 정보를 가지는 원 영상을 백색잡음 형태를 가지는 복소함수로 암호화한 후 동일한 시스템을 이용하여 복호화 한다[1-5]. 이를 이용한 대표적인 방법은 이중 무작위 위상 부호화 방법(double random phase encoding)으로 이는 4-f 광 상관기를 이용하여 입력 평면과 퓨리에 평면에 두개의 랜덤 위상 마스크를 두어 영상을 암호화하고, 영상의 복원은 랜덤 위상의 복소 공액값을 가진 마스크를 퓨리에 평면에 놓아 동일한 시스템을 이용하여 원 영상을 복원하게 된다. 이 방법은 정확한 복소 공액값을 가지는 위상 카드제작의 어려움과 광축 정렬의 문제점이 있고 이를 해결하기 위해 광축 정렬이 필요 없는 결합 변환 상관기(joint transform correlator ; JTC)를 이용한 방법[6-8]과 광굴절 매질을 이용하여 공액 복소빔을 이용한 방법[9] 등이 제안되었다. 또한 앞서 제안한 방법에서 암호화된 영상이 여러 형태의 외부 영향에 얼마나 강한 방법인가를 확인하였다[10, 11]. 이 방법들은 여러 잡음이나 암호화된 영상의 절단에는 강하지만 무작위 위상 특성에 의해 복호화키가 한 픽셀만 이동되더라도 원 영상을 재생할 수 없는 단점이 있다. 이를 해결하기 위한 방법으로 복호화 키의 픽셀 이동이 발생하더라도 원 영상이 재생되는 방법[12]이 제안되었으나 이 방법은 복호화키의 이동에 따른 암호화키의 절단이 동반되어서 원 영상이 재생되므로 원 영상의 재생 시 암호화키의 절단이 필요하고 그에 따른 원 영상의 해상도가 낮아지는 단점을 가진다. 최근에는 세기정보 암호화 수준을 향상시키기 위하여 입력평면에 위상정보를 가지는 원 영상을 이용하여 암호화하는 방법[13-17]들이 제안되었으며 이 중 Mogensen 등[15, 16]은 위상 정보를 암호화한 후 일반화된 위상 세기 방법(generalized phase-contrast technique)을 이용하여 간단히 원 영상을 복원할 수 있는 방법이 제안하였다. 이 방법은 공간 영역에서 암호화 및 복호화가 이루어지므로 광학적 시스템에서 암호화키의 한 픽셀의 이동만 생기더라도 원 영상을 재생할 수 없어 정확한 광축 정렬의 어려움을 가진다. 또한 앞서 제안된 방법들의 가장 큰 단점 중에 하나는 암호화키와 복호화키가 동일하므로 만약 허가되지 않은 사용자가 암호화된 영상을 분석하여 암호화키를 파악함으로써 복원 영상을 예측할 수 있는 문제점이 있다. 이 문제점을 해결하기 위해 반복적인 알고리즘을 이용하여 가상 세기 영상을 이용한 방법[18]이 제안되었으나 이 또한 4-f 광 상관기를 이용하므로 여전히 광축 정렬의 어려움을 가지고 원 영상을 재생하기 위한 시간소모가 많은 단점이 있다.

본 논문에서는 위상 변조된 원 영상의 정보를 세 개의 위상 변조된 영상 즉 가상 영상, 무작위 영상, 복호화키 영상에 각각 배분시키고 위상 변조된 가상 영상과 무작위 영상을 이용하여 암호화함으로써 암호화키인 무작위 영상을 분석 및 파악함으로써 있을 수 있는 복제 가능성을 배제시켜 암호화 수준을 향상시켰고 퓨리에 영역에서 암호화된 영상과 복호화 키 영상의 변이가 발생하더라도 원 영상이 복원됨을 제안하였다. 암호화된 영상은 원 영상의 어떤 정보도 포함하지 않은 위상 변조된 가상 영상과 컴퓨터로 발생시킨 무작위 위상 영상을 곱하여 퓨리에 변환하여 만든다. 따라서 허가되지 않은 사용자가 암호화된 영상을 분석하더라도 가상 영상을 원 영상으로 오인하게 되므로 복호화키의 정보 없이는 결코 원 영상의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하다는 장점을 가진다. 또한 시스템 내부에 항상 존재하는 복호화키의 정보가 유출되더라도 제안한 위상 대응 규칙에 의해 복호화 키의 암호화 수준을 향상시켰다. 복호화 과정은 암호화된 영상과 퓨리에 복호화 키를 간섭시킨 후 퓨리에 역변환하여 간단히 원 영상을 재생한다. 컴퓨터 모의 실험을 통하여 제안한 암호화 방법이 잡음이나 암호화된 영상이 절단되었을 경우 영상의 복원이 가능함을 확인하였고 기존의 시스템은 암호화 영상과 복호키의 상대적인 위치가 서로 정확히 주어져야 하는데 비하여 제안한 방법은 이러한 변이에 대하여 강한 특성이 있음을 검증하였다.

Ⅱ. 제안한 암호화 및 복호화 과정

원 영상 $f(x, y)$, 암호화할 가상 영상 $v(x, y)$, 무작위 영상 $r(x, y)$, 복호화키 영상 $d(x, y)$라고 하면 위상 변조된 원 영상 $f_p(x, y)$는 제안한 암호화 방법에서

$$f_p(x,y)=\exp[j\pi f(x,y)]$$
$$=\exp\{j\pi[v(x,y)+2r(x,y)-d(x,y)]\} \quad (1)$$

로 표현된다. 먼저 암호화할 가상 영상 $v(x,y)$와 컴퓨터로 발생시킨 무작위영상 $r(x,y)$을 각각 위상 변조하고 위상 변조된 각각의 영상 $v_p(x,y)$, $r_p(x,y)$는

$$v_p(x,y)=\exp[j\pi v(x,y)],\ r_p(x,y)=\exp[j2\pi r(x,y)] \quad (2)$$

와 같이 표현되며 여기서 변조된 영상의 위상 값은 [0, π]사이이고 그 세기는 '1'이므로 $|v_p(x,y)|^2=|r_p(x,y)|^2=1$로 주어진다. 두 위상 변조된 영상을 곱한 영상을 $e(x,y)$라 두면

$$e(x,y)=v_p(x,y)r_p(x,y)$$
$$=\exp\{j\pi[v(x,y)+2r(x,y)]\} \quad (3)$$

와 같고 원 영상과 무작위 영상의 선형적인 합임을 알 수 있고 이를 퓨리에 변환하여 암호화된 영상 $E(u, v)$로 사용한다. 이때 만약 허가되지 않은 개인이나 그룹이 암호화된 영상을 퓨리에 변환이나 위상 측정 방법 등으로 분석하더라도 가상영상을 원 영상으로 오인하게 되므로 정확한 복호화키 없이는 결코 원 영상의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하다는 장점을 가진다. 또한 본 논문에서 시스템 내부에 존재하는 복호화키 영상을 분석함으로써 있을 수 있는 복제 가능성을 배제하기 위하여 제안한 위상 대응 규칙에 의해 복호화키 영상 $\exp\{j\pi d(x, y)\}$를 만든다. 먼저 복호화키 영상을 재생하기 위하여 위상성분들의 단순한 가감법에 의해

$$\exp[j\pi d_A(x,y)]=\exp\{j\pi[v(x,y)+2r(x,y)-f(x,y)]\} \quad (4)$$

와 같이 표현할 수 있으며 여기에서 $\exp\{j\pi d_A(x, y)\}$를 복호화키를 만들기 위한 산술 연산키라고 가정하고 아래첨자 'A'는 산술연산을 표현한다. 만약 이 산술 연산키를 복호화키로 사용한다면 위상성분들의 산술적인 연산에 의해 원 영상의 정보가 복호화 키에 포함되어 있어서 복호화 시스템이 불법적인 사용자에 의해 분석이 용이하게 된다. 따라서 제안한 위상 대응 규칙을 이용하여 복호화키를 만드는 방법은

$$\exp[j\pi f(x,y)]=\exp\{j\pi[f(x,y)\pm 2n]\}$$
$$\exp[j\pi d_A(x,y)]=\exp\{j\pi[d_{A(x,y)}\pm 2n]\} \quad (5)$$

의 원리를 이용하며 여기에서 n은 정수이다. 즉 산술 연산키 $\exp\{j\pi d_A(x, y)\}$의 위상 값은 [$-\pi$, 3π]사이이므로 이를 [0, 2π]사이 값으로 위상 랩핑(phase wrapping)시킨다. 따라서 복호화키 $\exp\{j\pi d(x, y)\}$는

$$\exp[j\pi d(x,y)]=\begin{cases}\exp\{j\pi[d_A(x,y)+2]\}, & -1\le d_A(x,y)<0\\ \exp\{j\pi[d_A(x,y)]\}, & 0\le d_A(x,y)<2\\ \exp\{j\pi[d_A(x,y)-2]\}, & 2\le d_A(x,y)<3\end{cases} \quad (6)$$

에 의해 만들어지고 이를 퓨리에 변환하여 시스템에서 사용하는 퓨리에 복호화키 $D(u, v)$로 사용한다. 복호화를 위한 실험 구성도는 <그림 1>과 같으며 암호화된 영상

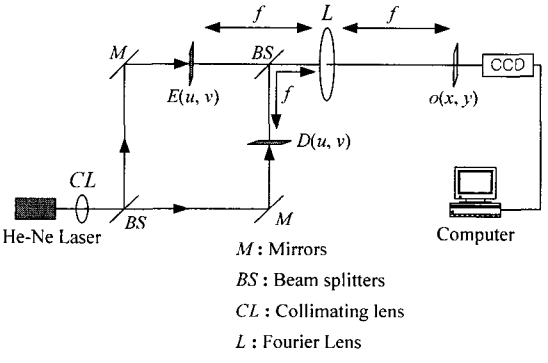


그림 1. 영상 복원을 위한 간섭계 시스템
Fig. 1. The interferometer system used for image decryption.

$E(u, v)$와 복호화키 $D(u, v)$는 간섭계의 퓨리에 영역에 각각 놓여지며, BS에 의해 합쳐진 영상 $O(u, v)$는

$$O(u,v)=E(u,v)+D(u,v) \quad (7)$$

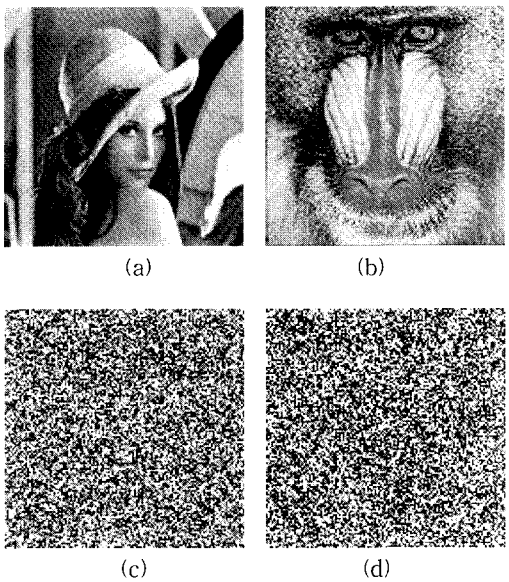
와 같으며 이 합쳐진 영상은 퓨리에 렌즈 L에 의해 퓨리에 역변환되고 그에 따른 CCD에 나타나는 세기함수는

$$|o(x,y)|^2=|e(x,y)|^2+|d_p(x,y)|^2$$
$$+e(x,y)d_p^*(x,y)+e^*(x,y)d_p(x,y)$$
$$=1+1+\exp[j\pi f(x,y)]+\exp[-j\pi f(x,y)]$$
$$=2+2\cos[\pi f(x,y)] \quad (8)$$

와 같으며 여기서 $f(x, y) = v(x, y) \cdot r(x, y) - d(x, y)$ 이다. 식 (8)에서 원 영상이 이진 영상이면 정확히 원 영상의 반전된 영상이 복원되지만 그레이 영상에서는 식 (8)의 여현 함수의 비선형성에 의해 영상의 왜곡이 발생함을 알 수 있으나 이는 컴퓨터의 후처리를 통하여 간단히 복원 가능하다.

Ⅲ. 컴퓨터 모의실험 및 고찰

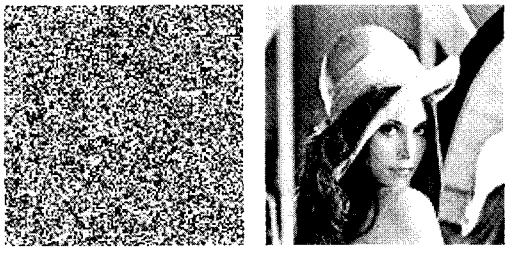
본 논문에서는 제안한 암호화 및 복호화 방법이 외부 영향에 강한 특성이 있음을 컴퓨터 모의실험을 통하여 확인하였다. <그림 2>는 컴퓨터 모의실험을 위하여 나타낸 영상들로 그레이 값을 가지며 그 화소수는 128×128이다. <그림 2(a)>는 복원할 원 영상 $f(x, y)$로 'Lena'를 사용하였고 <그림 2(b)>와 <그림 2(c)>는 각각 암호화될 가상 영상 $v(x, y)$로 'Baboon' 영상과 컴퓨터로 발생시킨 무작위 영상 $r(x, y)$이며 이들을 각각 [0, 1]사이의 값으로 정규화 시켜 위상 변조하여 서로 곱한 후 퓨리에 변환한 암호화된 영상을 <그림 2(d)>에 나타내었으며 이는 가상 영상과는 전혀 관계없는 무작위 패턴으로 나타남을 확인할 수 있다. 여기서 암호화된 영상은 눈으로 볼 수 없는 복소 함수이므로 편의를 위해서 세기 패턴으로 나타내었다. 또한 만약 허가되지 않은 사용자가 암호화키를 분석하더라도 가상 영상을 원 영상으로 오인하게 되므로 복제 가능성을 배제할 수 있다. <그림 3>은 외부의 영향이나 잡음이 없을 경우로서 <그림 3(a)>는 복원 영상을 얻기 위해 제안한 위상 대응 규칙으로 만든 올바른 복호화키의 퓨리에 변환된 영상이며 <그림 3(b)>는 이에 대응되는 복원 영상의 반전 영상이다. 여기에서 그레이 영상을 재생함으로써 식 (6)의 여현 함수의 비선형성에 의해 원 영상의 왜곡이 발생하는데 <그림 3(b)>에서 이는 보상하지 않았지만 후처리를 통하여 보상할 수 있다. 하지만 이때 실질적인 광 실험을 위해서 <그림 2(d)>와 <그림 3(a)>는 복소값을 표시할 수 있는 SLM과 같은 광학 소자가 필요하지만 현재의 SLM의 기술은 크기 변조 혹은 위상 변조에 대한 성분만을 기록할 수 있으므로 이 복소 영상들을 정확히 표시하기가 어렵다[19]. 따라서 현재 복소값을 표현하는 대표적인 기술로 홀로그래픽 필름이나 컴퓨터 형성 홀로그램(computer generated hologram, CGH)[20]을 이용하여 기록하지만 이 또한 공간대역폭제한과 양자화 손실로 인한 영상의 해상도가 떨어지는 단점을 가진다.



(a) (b) (c) (d)

그림 2. 암호화 및 복호화를 위해 사용된 (a) 원 영상, (b) 가상 영상, (c) 무작위 영상, (d) 암호화된 영상

Fig. 2. Images used for encryption and decryption: (a) original image, (b) virtual image, (c) random image, and (d) encrypted image.



(a) (b)

그림 3. (a) 퓨리에 복호화 키와 (b) 반전된 복원 영상의 모의실험 결과

Fig. 3. Simulation results: (a) Fourier decrypting key and (b) the inversion of the reconstructed image.

1. 위상 잡음에 의한 영향

간섭계를 이용한 암호화 시스템은 진동이나 외부 교란으로 인해 위상 지연이 발생할 수 있으므로 실험구성이 정밀해야 하고 특히 위상 암호화 시스템은 세기 암호화 시스템보다 암호화 수준은 향상되지만 잡음이

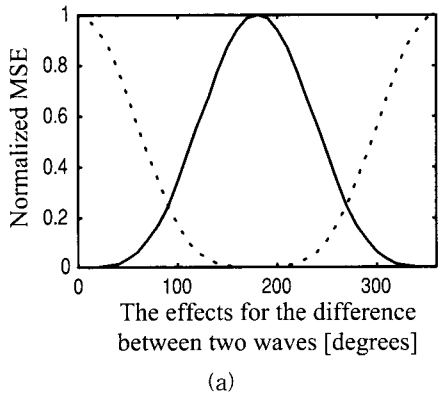
나 위상 마스크의 흠집 등에 민감하여 영상의 왜곡이 발생할 수 있다. 따라서 암호화된 영상 $E(u, v)$나 퓨리에 복호화키 $D(u, v)$의 암호화 및 복호화 과정에서 발생할 수 있는 잡음 $N(u, v)$와 복호화 과정에서 간섭계의 두 경로 차로 인한 위상차를 고려하면 식 (8)은

$$|o(x,y)|^2 = 2 + 2n_a(x,y)\cos[\pi(f(x,y) + n_p(x,y)\} + n_w(x,y)] \quad (9)$$

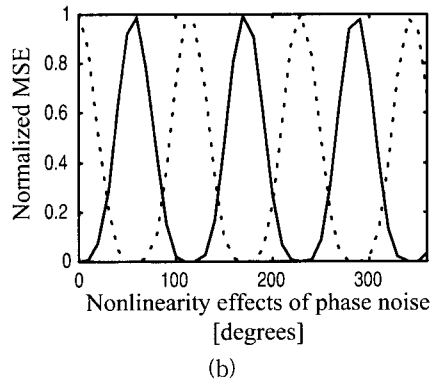
이 되고 여기서 $n_w(x, y)$는 간섭계의 두 파 사이의 위상차이고 $n(x, y)$는 잡음 $N(u, v)$의 퓨리에 역변환이며 $n(x,y) = n_a(x,y)\exp[j\pi n_p(x,y)]$로 표현한다. n_a와 n_p는 각각 암호화된 영상이나 퓨리에 복호화키에서 나타날 수 있는 먼지나 흠집에 의한 크기 잡음과 위상 잡음이다. 여기서 n_a는 실제 시스템에서 중요한 문제지만 위상 암호화 시스템에서는 크기 성분을 보통 '1'로 둔다[13]. <그림 4(a)>와 <그림 4(b)>는 각각 두 파의 위상차 (n_w)가 있을 경우와 위상 잡음 (n_p) 있을 경우를 분리하여 복원 영상의 평균제곱오차 (mean square error ; MSE)를 나타내었다. 여기에서 사용된 평균제곱오차의 표준[13]은

$$\mathrm{MSE} = E\left\{ \frac{1}{N \times M} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} [\,|\,|f_o(x,y)| - |f_d(x,y)|\,|^2] \right\} \quad (10)$$

이며 여기서 $f_o(x, y)$와 $f_d(x, y)$는 각각 원 영상과 복원 영상이며 $N \times M$은 각 영상의 픽셀 수이며 $E(\ )$는 평균값을 나타낸다. <그림 4>에서 점선과 실선은 각각 복원 영상과 그것의 반전 영상이 위상차가 발생할 경우의 평균제곱오차를 나타낸 것으로 컴퓨터로 복원 영상과 그것의 반전 영상을 모두 얻는다면 원 영상의 정보를 얻을 수 있음을 알 수 있다. 그러나 <그림 4(a)>에서 90°와 270°, <그림 4(b)>에서 1/2 rad부터 1 rad간격으로 점선과 실선이 만나는 교점에선 정확한 복호화키를 사용하더라도 복원 영상과 반전영상으로 원 영상의 정보를 알 수 없음을 나타낸다.



(a)



(b)

그림 4. 위상차로 인한 평균 제곱 오차. (a) 두 파의 위상차가 있을 경우, (b) 위상 잡음이 있을 경우

Fig. 4. Mean squared errors when the phase error is due to (a) the phase difference between the two waves, (b) the phase noise, respectively.

2. 암호화된 영상의 절단이나 변이에 대한 영향

제안한 암호화 시스템의 외부 영향에 대한 성능을 평가하기 위해 먼저 암호화된 영상을 임의로 절단하여 그에 대응하는 복원 영상을 분석하였다. 수식적인 표현을 간단히 하기 위해 1차원으로 표현하고 암호화된 영상의 일부분이 복호화에 사용된다면 절단된 암호화 영상 $E_b(u)$는

$$E_b(u) = E(u)\,\mathrm{rect}\left(\frac{u}{\Omega}\right) \quad (11)$$

와 같으며 여기에서 Ω 는 직각 동공 함수(rectangular pupil function)의 너비이다. 따라서 식 (11)의 복원을 위한 퓨리에 변환은

$$\begin{aligned} e_b(x) &= e(x) * \Omega \sin c(\Omega x) \\ &= \sum_{n=0}^{N-1} e(n)\Omega \sin c[\Omega(x-n)] \end{aligned} \quad (12)$$

여기에서 $*$ 는 상승적분 연산자이고 N은 공간영역에서의 표본화 개수이며 암호화된 영상의 너비를 1로 정규화시켜 $\Omega \le 1$로 표현하였다. 퓨리에 복호화키 $D(u)$를 퓨리에 역변환하고 식 (12)와 합쳐진 영상은

$$o_h(x) = \sum_{n=0}^{N-1} e(n)\Omega \sin c[\Omega(x-n)] + d(x) \quad (13)$$

와 같다. 따라서 CCD에 나타나는 복원영상은

$$\begin{aligned} |o_h(x)|^2 &= \left| \sum_{n=0}^{N-1} e(n)\Omega \sin c[\Omega(x-n)] \right|^2 + |d(x)|^2 \\ &+ \sum_{n=0}^{N-1} e^*(n)\Omega \sin c[\Omega(x-n)]d(x) \\ &+ \sum_{n=0}^{N-1} e(n)\Omega \sin c[\Omega(x-n)]d^*(x) \\ &= \begin{cases} \Omega^2 + 1 + 2\Omega\cos[\pi f(x)], & x = n \\ \sum_{n=0}^{N-1} r(x,n), & x \neq n \end{cases} \end{aligned} \quad (14)$$

로 표현되며 여기에서 $r(x, n)$은 $x = n$을 제외한 나머지 세기 성분을 나타내며 출력평면에 균일하게 분포된 무작위 함수로 나타난다. 식 (14)에서 Ω에 의해 복원영상의 해상도가 떨어지지만 암호화된 영상의 일부분이 절단되더라도 원 영상이 복원됨을 알 수 있다. <그림 5(a)>와 <그림 5(c)>는 각각 암호화된 영상 <그림 2(d)>를 각각 25%와 75% u축으로 절단하였을 경우와 이를 복호화를 위한 실험 구성도의 정확한 위치에 두었을 때 그에 대응되는 복원 영상을 각각 <그림 5(b)>와 <그림 5(d)>에 나타내었고 <그림 5(e)>는 암호화된 영상을 u축을 따라 절단한 경우의 평균제곱오차이다. 여기서 암호화된 영상의 절단되는 픽셀의 위치 정보가 변하더라도 복원 영상의 해상도에는 영향을 미치지 않고 퓨리에 복호화키가 절단되더라도 동일한 해상도를 가짐을 여러 실험을 통해서 확인하였다. <그림 5(d)>에서 암호화된 영상의 75%가 절단되더라도 원 영상의 정보를 얻을 수 있음을 알 수 있다.

또한 암호화된 영상이나 퓨리에 복호화키가 복호화를 위한 실험 구성도의 정확한 위치로부터 u축으로 변이가 발생할 경우 식 (7)은

$$O(u,v) = E(u-u_0, v-v_0) + D(u,v) \quad (15)$$

로 표현되며 여기서 u_0는 ku/(N+1)이며 v_0는 $k_v/(N+1)$이고 N은 암호화된 영상의 픽셀 수이며 k_u와 k_v는 각각 u축과 v축을 따라 이동된 픽셀 값이다. 이 합쳐진 영상은 퓨리에 렌즈 L에 의해 퓨리에 역변환되고 그에 따른 CCD에 나타나는 세기함수는

$$\begin{aligned} |o(x,y)|^2 &= 1 + 1 + \exp[j\pi f(x,y)]\exp(j2\pi u_0 x)\exp(j2\pi v_0 y) \\ &+ \exp[-j\pi f(x,y)]\exp(-j2\pi u_0 x)\exp(-j2\pi v_0 y) \\ &= 2 + 2\cos[\pi f(x,y) + 2\pi u_0 x + 2\pi v_0 y] \end{aligned} \quad (16)$$

로 표현된다. <그림 6(a)~(d)>는 퓨리에 영역에서 암호화된 영상이 정확한 위치에서 각각 (u, v)축을 따라 (a) (2, 0), (b) (2, 1), (c) (2, 2), (d) (1, 4) 픽셀만큼 변이가 생겼을 경우에 재생된 영상들이다. 여기서 복원

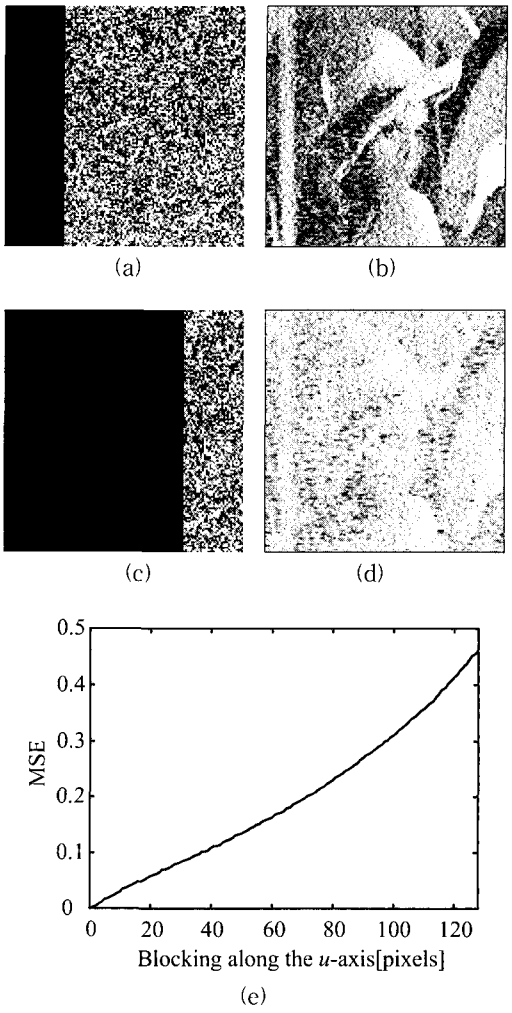


그림 5. u축을 따라 암호화된 영상이 각각 (a) 25%와 (c) 75% 절단되었을 때 그에 대응하여 복원된 영상 (b)와 (d); (e) u축을 따라 절단되었을 경우의 복원 영상의 평균제곱오차

Fig. 5. The occluded encrypted images of (a) 25% and (c) 75% along the u axis and the corresponding reconstructed images (b) and (d), respectively; (e) the MSEs for the reconstructed images.

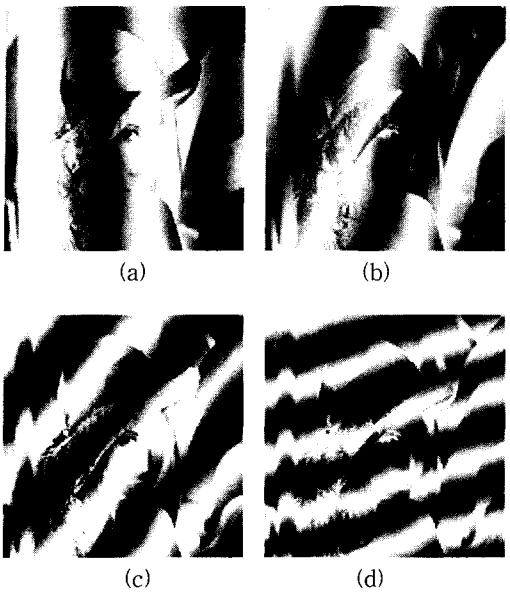


그림 6. 퓨리에 영역에서 암호화된 영상이 정확한 위치에서 (a) (2, 0), (b) (2, 1), (c) (2, 2), (d) (1, 4) 픽셀만큼 변이가 생겼을 경우에 재생된 영상

Fig. 6. The decrypted results when the encrypted image is shifted for (a) (2, 0), (b) (2, 1), (c) (2, 2), and (d) (1, 4) pixels from the matching position in Fourier space, respectively.

영상의 전 영역에 여현 함수의 위상 성분 $2\pi u_0 x$와 $2\pi v_0 y$에 의하여 줄무늬가 발생하고 이 재생된 영상의 줄무늬 개수는 식 (16)을 통하여 암호화된 영상의 이동된 전체 픽셀 값과 동일함을 알 수 있고 또한 줄무늬의 기울기는 $\tan^{1}(u/v)$이다. 따라서 재생된 영상을 통하여 암호화된 영상의 변이 정도를 알 수 있음으로 컴퓨터의 후처리를 통하여 보완할 수 있다.

Ⅳ. 결 론

본 논문에서는 가상 위상 영상을 이용하여 암호화 수준을 향상시키고 잡음이나 인위적인 외부의 영향에 강한 복호화 방법을 제안하였다. 제안한 암호화 방법은 원 영상의 어떤 정보도 포함하지 않은 가상 영상을 이용함으로써 허가되지 않은 개인이나 그룹이 암호화된 영상을 다양한 위상 측정 방법이나 퓨리에 변환 등으로 분석하더라도 그들은 가상 영상을 원 영상으로 오인하게 됨으로 어떠한 경우에도 원 영상을 복호화할 수 없는 장점을 가지며 위상 랩핑 방법을 이용하여 시스템에 존재하는 복호화키의 암호화 수준을 향상시켰으며 복호화 과정에서 암호화된 영상이나 퓨리에 복호화키 영상이 절단되더라도 원 영상의 정보를 가지고 있으며 또한 잡음이나 변이가 발생하더라도 그에 따른 문제를 분석하고 그 해결 방법을 제안하였다.

참 고 문 헌

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

[2] R. K. Wang, I. A. Watson, and C. Chatwin, "Random phase encoding for optical security," Opt. Eng., vol. 35, pp. 2464-2469, 1996.

[3] 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.

[4] B. Javidi, G. Zhang, and Jian Li, "Experimental demonstration of the random phase encoding technique for image encryption and security verification," Opt. Eng., vol. 35, pp. 2506-2512, 1996.

[5] B. Javidi and E. Ahouzi, "Optical security system with Fourier plane encoding," Appl. Opt., vol. 37, pp. 6247-6255, 1998.

[6] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng., vol. 39, pp. 2031-2035, 2000.

[7] T. Nomura and B. Javidi, "Optical encryption system with a binary key code," Appl. Opt., vol. 39, pp. 4783-4787, 2000.

[8] M. Yamazaki and J. Ohtsubo, "Optimization of encrypted holograms in optical security systems," Opt. Eng., vol. 40, pp. 132-137, 2001.

[9] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption system that uses phase conjugation in a photorefractive crystal," Appl. Opt., vol. 37, pp. 8181-8186, 1998.

[10] B. Javidi, A. Sergent, G. Zhang, and L. Guibert,

"Fault tolerance properties of a double phase encoding encryption technique," Opt. Eng. vol. 36, pp. 992-998, 1997.

[11] B. Javidi, A. Sergent, and E. Ahouzi, "Performance of double phase encoding encryption technique using binarized encrypted images," Opt. Eng., vol. 37, pp. 565-570, 1998.

[12] B. Wang, C. C. Sun, W. C. Su, and A. E. T. Chiou, "Shift-tolerance property of an optical double-random phase-encoding encryption system," Appl. Opt., vol. 39, pp. 4788-4793, 2000.

[13] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," J. Opt. Soc. Am. A, vol. 16, pp. 1915-1927, 1999.

[14] X. Tan, O. Matoba, T. Shinura, K. Kuroda, and B. Javidi, "Secure optical storage that uses fully phase encryption," Appl. Opt., vol. 39, pp. 6689-6694, 2000.

[15] P. C. Mogensen and J. Gluckstad, "Phase-only optical encryption," Opt. Lett., vol. 25, pp. 566-568, 2000.

[16] P. C. Mogensen and J. Glückstad, "Phase-only optical decryption of a fixed mask," Appl. Opt., vol. 40, pp. 1226-1235, 2001.

[17] J. Ohtsubo and A. Fujimoto, "Practical image encryption and decryption by phase-coding technique for optical security systems," Appl. Opt., vol. 41, pp. 4848-4855, 2002.

[18] H. T. Chang, "Image encryption using separable amplitude-based virtual image and iteratively retrieved phase information," Opt. Eng., vol. 40, pp. 2165-2171, 2001.

[19] L. G. Neto, D. Roberge, and Y. Sheng, "Full-range, continuous, complex modulation by the use of two coupled-mode liquid-crystal televisions," Appl. Opt., vol. 35, pp. 4567-4576, 1996.

[20] C. Iemmi, S. Ledesma, J. Campos, and M. Villarreal, "Gray-level computer-generated hologram filters for multiple-object correlation," Appl. Opt., vol. 39, pp. 1233-1240, 2000.

저 자 소 개

徐 東 煥(正會員) 第38卷 SD編 第11號 參照
현재 : 경북대학교 대학원 전자공학과 박사과정 재학중

金 秀 重(正會員) 第33卷 B編 第7號 參照
현재 : 경북대학교 전자전기공학부 정교수