論文2003-40SD-7-6

결합 변환 상관기를 이용한 잡음 및 변이에 강한 암호화 시스템

(Shift and Noise Tolerance Encryption System Using a Joint Transform Correlator)

徐 東 煥 *, 金 秀 重 *

(Dong-Hoan Seo and Soo-Joong Kim)

요 약

본 논문에서는 가상 위상 영상과 정확한 광축 정렬이 필요 없는 결합 변환 상관기를 이용하여 잡음이나 변이에 강한 복호화 방법을 제안하였다. 암호화된 영상은 원 영상을 속이기 위한 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. 결합 변환 상관기를 이용한 제안한 복호화 방법이 암호화된 영상에 잡음이나 절단, 변이에 대해서 강한 특성을 가짐을 확인하였다.

Abstract

In this paper, we propose the shift and noise tolerance method using a virtual phase image and a joint transform correlator (JTC) architecture that can alleviate the need for an accurate optical axis alignment. An encrypted image is obtained by the Fourier transform of the product of a phase-encoded virtual image to camouflage the original one 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. We demonstrate the robustness to noise, to data loss and to shift of the encrypted image using a JTC in the proposed decryption technique.

Keyword : optical security, joint transform correlator, phase image

Ⅰ. 서 론

광학적 보안 시스템은 세기정보와 위상정보를 동시에 광학 매질에 기록할 수 있으므로 사람의 눈이나 기존의 세기검출기로는 추출이 불가능하고 무작위 특성에 의해서 원래의 패턴을 복제나 위조하기가 어렵다는 특성을 가진다. 현재 사용되는 광 보안 시스템은 주로 4-f 광 상관시스템[1-4]이나 간섭계 구조[5]를 이용하여 원 영상을 재생하게 되는데, 이때 암호화에 사용된 무작위 위상마스크에 의해서 주로 진위 여부를 판정하게 된다. 이 중 4-f 광 상관시스템은 광축 정렬 문제와 암호화할 때 사용한 위상마스크의 복소공액 마스크를 제작해야 하는 어려움이 있으며, 간섭계를 이용한 시스템은 정밀한 실험구성을 필요로 하며 외부 교란에 많은

* 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.)

接受日字:2002年12月18日, 수정완료일:2003年6月10日

영향을 받는다는 단점이 있다. 이에 여러 형태의 외부 영향이나 잡음에 얼마나 강한가를 이중 무작위 위상 부호화(double random phase encoding) 방법[6, 7]을 이용하여 제안하였는데 이 방법들은 여러 잡음이나 암호화된 영상의 절단에는 강하지만 무작위 위상 특성에 의해 복호화키가 한 픽셀만 이동하더라도 원 영상을 재생할 수 없는 단점이 있다. 이를 해결하기 위하여 위 방법을 이용하여 복호화 키의 픽셀 이동이 발생하더라도 원 영상이 재생되는 방법[8]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[9-13]들이 제안되었으며 이 중 Mogensen 등[11, 12]은 위상 정보를 암호화한 후 일반화된 위상 세기 방법(generalized phase-contrast technique)을 이용하여 간단히 원 영상을 복원할 수 있는 방법이 제안되었다. 이 방법은 공간 영역에서 암호화 및 복호화가 이루어지므로 광학적 시스템에서 암호화키의 한 픽셀의 이동만 생기더라도 원 영상을 재생할 수 없어 정확한 광축 정렬이 필요하다. 이에 반하여 결합변환상관기(JTC: joint transform correlator)는 광축 정렬이 필요 없고 외부교란에도 거의 영향을 받지 않는 장점이 있다. 그러나 JTC는 그 구조적인 특성 때문에 출력 평면에 큰 세기의 자기상관 성분이 나타나는데, 이는 JTC를 광 상관 시스템이나 광 보안 시스템에 이용하기 어렵게 만드는 주된 원인이 된다. 최근 JTC를 이용한 광학적 암호화 방법[14-16]이 제안되었는데 이 방법은 JTC의 주파수 스펙트럼(JPS : joint power spectrum)을 암호화된 영상으로 기록하여 사용하고, 4-f 상관시스템을 이용하여 복호화한다. 그러나 이 방법은 기록된 암호화 패턴이 실수함수이므로 세기검출기로 복사가 가능하고, 복호화시 4-f 상관기를 이용하므로 광축 정렬의 어려움이 존재하며 기록된 JPS에 존재하는 자기상관성분을 제거하여야 하는 문제점을 가지고 있다. 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. 이를 해결하기 위해 반복적인 알고리즘을 이용하여 가상 세기 영상을 이용한 방법[17]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 영상을 이용하여 암호화함으로써 암호화키인 무작위 영상을 분석 및 파악함으로써 있을 수 있는 복제 가능성을 배제시켰고 JTC의 가장 큰 문제점인 자기상관성분을 이용하여 원 영상을 복원할 수 있는 방법과 제안한 방법이 잡음이나 변이, 절단에 강한 특성을 가짐을 확인하였다. 제안한 방법은 원 영상의 어떤 정보도 포함하지 않는 가상 위상 영상과 무작위 위상 영상의 곱을 퓨리에 변환하여 암호화된 영상으로 사용하여 허가되지 않은 사람들이 이 암호화된 영상을 분석함으로써 있을 수 있는 복제 가능성을 배제할 수 있으므로 복호화 키의 정보 없이는 결코 원 영상의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하다는 장점을 가지며 퓨리에 변환된 위상 영상들을 JTC의 주파수 평면에 두어 퓨리에 변환하여 원 영상을 재생함으로 JTC의 문제점인 자기상관성분을 이용하여 복호화되는 장점을 가진다. 제안한 JTC 구조에서 발생하는 위상성분의 영향에 대한 분석의 타당성을 검증하고 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 JTC를 이용한 복호화 방법

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

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

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

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

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

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

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 다양한 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. 본 논문에서 제안한 위상 대응 규칙에 의한 복호키 영상을 만드는 방법은

$$\begin{aligned} d_p(x,y) &= \exp[j\pi d(x,y)] \\ &= \exp\{j\pi[v(x,y)+r(x,y)-f(x,y)]\} \end{aligned} \quad (4)$$

와 같이 표현되며 이를 퓨리에 변환하여 복호화키 $D(u, v)$로 사용한다. 복호화를 위한 JTC 구성도는 <그림 1>과 같다. 여기에서 암호화된 영상 $E(u, v)$는 <그림 1>의 결합

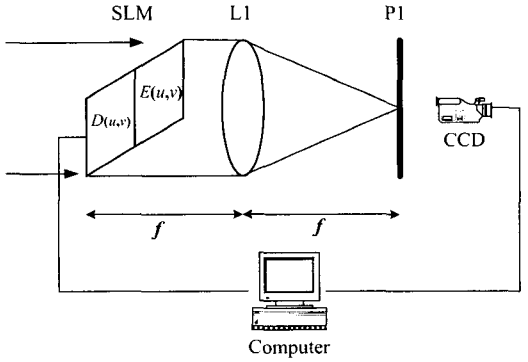

그림 1. 결합 변환 상관기를 이용한 복호화 시스템
Fig. 1. Decryption system using joint transform correlator.

입력 평면의 우반 평면에, 복호화키 $D(u, v)$는 좌반 평면에 각각 놓여지며, 결합입력평면 $P(u, v)$는

$$P(u,v) = E(u-u_0,v) + D(u+u_0,v) \quad (5)$$

와 같다. 본 논문에서 암호화된 영상은 주파수 영역이므로 각각의 영상이 JTC의 결합입력 평면에 놓여지게 되면 원래의 중심에 대해서 $\pm u_0$만큼 이동된 결과를 가져온다. 따라서 결합평면은 렌즈 L1에 의해서 푸리에 역변환 되어지며 이는

$$p(x,y)=e(x,y)\exp(j2\pi u_0x)+d_p(x,y)\exp(-j2\pi u_0x) \quad (6)$$

로 주어진다. 여기서 $\exp(j2\pi u_0x)$는 주파수영역에서 중심의 이동에 의해 생기는 출력평면에서의 위상성분이다. 출력평면 P1에 놓인 CCD 카메라에 의해서 검출되어지는 세기함수는

$$\begin{aligned} |p(x,y)|^2 = {} & |e(x,y)|^2+|d_p(x,y)|^2+e(x,y)d_p^*(x,y) \\ & \exp(j4\pi u_0x)+e^*(x,y)\,d_p(x,y)\exp(-j4\pi u_0x) \\ = {} & 1+1+\exp[j\pi f(x,y)]\exp(j4\pi u_0x) \\ & +\exp[-j\pi f(x,y)]\exp(-j4\pi u_0x) \\ = {} & 2+2\cos[\pi f(x,y)+4\pi u_0x] \end{aligned} \quad (7)$$

와 같다. 식 (7)에서 위상 성분 $4\pi u_0x$를 고려하기 위해 표본화된 영상의 주파수 영역과 공간영역의 관계를 살펴보면

$$\begin{aligned} &\Delta d=\frac{1}{2f_{x0}}, \quad x=k\Delta d=k\frac{L}{N_x} \\ &u=k\frac{1}{\Delta d}=k\frac{N_x}{L}, \quad k=0,1,\ldots\ldots,N_x-1 \end{aligned} \quad (8)$$

로 주어지며 편의상 x축과 u축만 표시하였다. 여기서 Δd는 표본화 간격, f_{x0}는 영상의 x축의 최고 주파수, L은 x축으로의 영상의 길이, k는 화소번호이며 N_x는 표본화 개수이다. 따라서 <그림 1>에서 각 입력영상의 중심인 $(\pm u_0, 0)$는 전체 결합입력평면의 중심에서 $\pm$ 1/4되는 지점만큼 이동되므로 위의 값을 식 (7)에 대입하여 정리하면

$$\begin{aligned} |p(x,y)|^2 &= 2+2\cos[\pi f(x,y)+k_x] \\ &= \begin{cases} 2+2\cos[\pi f(x,y)], & k_x=2n \\ 2-2\cos[\pi f(x,y)], & k_x=2n-1 \end{cases} \end{aligned} \quad (9)$$

와 같으며 여기서 n은 정수이며 k_x는 x축으로의 화소번호이다. 식 (9)에서 JTC의 문제점인 자기상관성분이

원 영상 재생에 필요한 성분이 됨을 알 수 있고 또한 컴퓨터의 후처리를 통하여 즉 x축 방향의 홀수 화소를 제거하여 영상을 재생하면 x축으로 반으로 줄어든 명암이 반전된 원 영상이 재생되고 반면에 짝수 화소를 제거하면 반으로 줄어든 원 영상이 재생됨을 알 수 있으나 재생 영상의 크기가 반으로 줄어드는 단점을 가진다. 따라서 본 논문에서는 복호화 과정에서 생기는 위상 성분의 영향을 제거하기 위하여 제안한 암호화 과정에서 $e(x, y)$와 $d_p(x, y)$에 위상 성분 $\exp(j2\pi u_0 x)$와 $\exp(-j2\pi u_0 x)$를 각각 곱한 후 퓨리에 변환하여 암호화된 영상과 퓨리에 복호화키로 사용한다. 그러므로 식 (7)에서의 위상 성분 $4\pi u_0 x$ 는 $8\pi u_0 x$가 되어 식 (9)는

$$\begin{aligned} |p(x, y)|^2 &= 2 + 2\cos[\pi f(x, y) + 2\pi k_x] \\ &= 2 + 2\cos[\pi f(x, y)] \end{aligned} \tag{10}$$

와 같으며 여기서 위상 성분은 x축을 따라 π의 짝수 배가 되므로 여현 함수에서 무시할 수 있다. 식 (10)에서 JTC 출력 평면에 나타나는 영상은 반전된 원 영상이 복원됨을 알 수 있으며 또한 복원 영상이 이진 영상이면 정확히 원 영상이 복원되지만 그레이 영상으로 확장하면 식 (10)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.

1. 암호화 과정에서 위상 성분을 곱하지 않은 경우

<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 'Elaine'를 사용하였고 <그림 2(b)>와 <그림 2(c)>는 각각 암호화될 가상 영상 $v(x, y)$로 'Lena' 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 나타내었고 또한 암호화 과정에서 위상 성분 $\exp(j2\pi u_0 x)$를 곱하지 않은

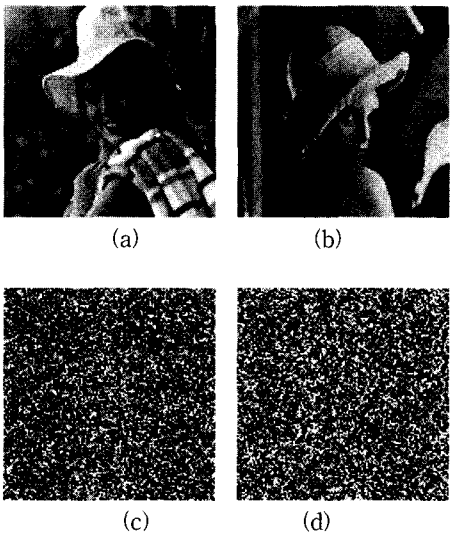

그림 2. 암호화 및 복호화를 위해 사용된 (a) 원 영상, (b) 가상 영상, (c) 무작위 영상, (d) 암호화된 영상

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

경우이다. <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 이 또한 위상 성분 $\exp(-j2\pi u_0 x)$를 곱하지 않은 경우이며 <그림 3(b)>는 <그림 2(d)>와 <그림 3(a)>를 결합입력평면에 각각 두고 퓨리에 역변환하여 CCD에 나타나는 영상으로 위상성분에 의해 복원 영상이 왜곡됨을 알 수 있다. <그림 3(c)>와 <그림 3(d)>는 컴퓨터 후처리를 통하여 위상 성분의 영향을 제거한 영상들로써 <그림 3(c)>는 x축 방향의 홀수 화소를 제거한 영상으로 x축으로 크기가 반으로 줄어든 명암이 반전된 원 영상이 재생되고 반면에 <그림 3(d)>는 x축 방향의 짝수 화소를 제거한 영상으로 크기가 반으로 줄어든 원 영상이 재생됨을 알 수 있다. 여기에서 그레이 영상을 재생함으로써 식 (9)의 여현 함수의 비선형성에 의해 원 영상의 왜곡이 발생하는데 <그림 3>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[18]. 따라서 현재 복소값을 표현하는 대표적인 기술로 홀로그래픽 필름이나 컴퓨터 형성 홀로그램(computer generated hologram, CGH)[19]을 이용하여 기록하지만 이 또한 공간대역폭제한과 양자화 손실로 인한 영상의 해상도가 떨어지는 단점을 가진다.

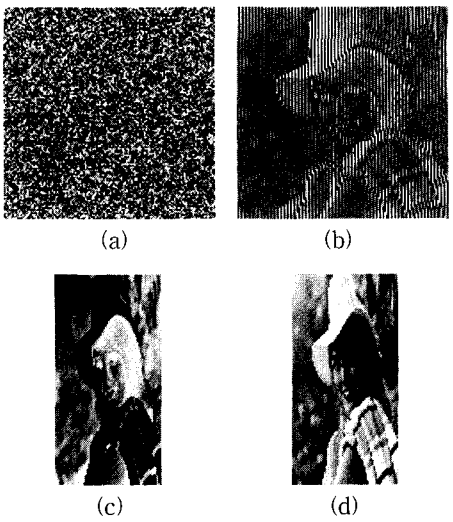

그림 3. 모의 실험 결과 : (a) 퓨리에 복호화 키, (b) 복원 영상, (c) <그림 3(b)>의 영상에서 x축의 홀수 화소를 제거시킨 영상, (b) <그림 3(b)>의 영상에서 x축의 짝수 화소를 제거시킨 영상

Fig. 3. Simulation results : (a) Fourier decrying key (b) reconstructed image (c) reconstructed image when odd pixels are removed in Fig. 3(b) (d) reconstructed image when even pixels are removed in Fig. 3(b).

2. 암호화 과정에서 위상 성분을 곱한 경우

복호화 과정에서 생기는 위상 성분의 영향을 제거하기 위하여 제안한 암호화 과정에서 $e(x, y)$와 $d_p(x, y)$에 위상 성분 $\exp(j2\pi u_0 x)$와 $\exp(-j2\pi u_0 x)$를 각각 곱한 후 퓨리에 변환하여 결합입력평면에 영상을 두고 재생할 경우는 <그림 4>에 나타내었다. <그림 4(a)>와 <그림 4(b)>는 복호화 과정에서 생기는 위상 성분의 영향을 제거하기 위하여 제안한 암호화 과정에서 $e(x, y)$와 $d_p(x, y)$에 위상 성분 $\exp(j2\pi u_0 x)$와 $\exp(-j2\pi u_0 x)$를 각각 곱한 후 퓨리에 변환한 영상이고 <그림 4(c)>와 <그림 4(d)>는 그에 따른 복원된 영상과 그것의 반전 영상이다. 식 (10)에서처럼 JTC 출력평면에 나타나는 복원 영상은 크기의 변화가 없는 반전된 원 영상이 복원됨을 알 수 있다.

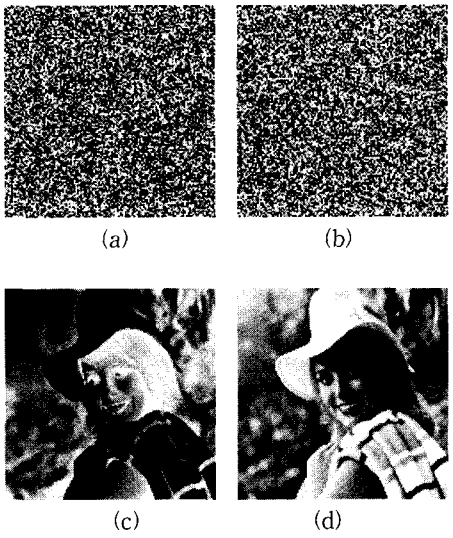

그림 4. 암호화 과정에서 위상 성분을 곱한 경우의 (a) 암호화된 영상, (b) 퓨리에 복호화 키, (c) 복원 영상, (d) 반전된 복원 영상

Fig. 4. (a) Encrypted image, (b) Fourier decrying key, (c) reconstructed image (c) the inversion of reconstructed image in case of multiplying phase terms in encryption process.

3. 위상 잡음에 의한 영향

위상 암호화 시스템은 세기 암호화 시스템보다 암호화 수준은 향상되지만 잡음이나 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 $N(u, v)$로 인한 위상차를 고려하면 식 (10)은

$$|p(x,y)|^2 = 2 + 2n_a(x,y)\cos[\pi\{f(x,y) + n_p(x,y)\}] \quad (11)$$

이 되고 여기서 $n(x,y) = n_a(x,y)\exp[j\pi n_p(x,y)]$로 표현되며 잡음 $N(u, v)$의 퓨리에 역변환이다. 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[9].

<그림 5(a)>는 위상 잡음 (n_p) 있을 경우 복원 영상의 평균제곱오차 (mean square error ; MSE)를 나타내었다. 여기에서 사용된 평균제곱오차의 표준[9]은

$$\mathrm{MSE} = E\left\{ \frac{1}{N\times M} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} [\,|\,|f_o(x,y)| - |f_d(x,y)|\,|^2] \right\} \quad (12)$$

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 5>에서 점선과 실선은 각각 복원 영상과 그것의 반전 영상이 위상 잡음이 발생할 경우의 평균제곱오차를 나타낸 것으로 컴퓨터로 복원 영상과 그것의 반전 영상을 모두 얻는다면 원 영상의 정보를 얻을 수 있음을 알 수 있다. 그러나 <그림 5>에서 1/2 rad부터 1 rad간격으로 점선과 실선이 만나는 교점에선 정확한 복호화키를 사용하더라도 복원 영상과 반전영상으로 원 영상의 정보를 알 수 없음을 나타낸다.

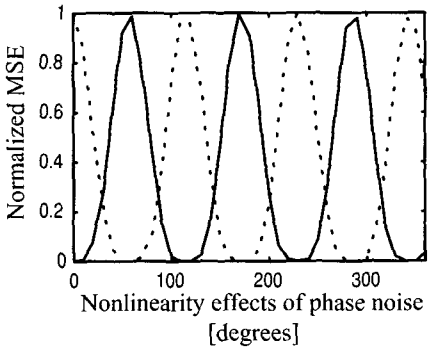

그림 5. 위상 잡음으로 인한 평균 제곱 오차
Fig. 5. Mean squared errors due to the phase noise.

4. 암호화된 영상의 절단이나 변이에 대한 영향

<그림 6>은 제안한 암호화 시스템이 외부 영향에 대한 성능을 평가하기 위해 암호화된 영상을 임의로 절단하여 그에 대응하는 복원 영상을 표현하였다. <그림 6(a)>, <그림 6(c)>, 와 <그림 6(e)>는 각각 암호화된 영상 <그림 4(a)>를 각각 25%, 50%와 75% u축으로 절단하였을 경우와 이를 복호화를 위한 실험 구성도의 정확한 위치에 두었을 때 그에 대응되는 복원 영상을 각각 <그림 6(b)>, <그림 6(d)>와 <그림 6(f)>에 나타내었다. 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 6(f)>에서 암호화된 영상의 75%가 절단되더라도 원 영상의 정보를 얻을 수 있음을 알 수 있다.

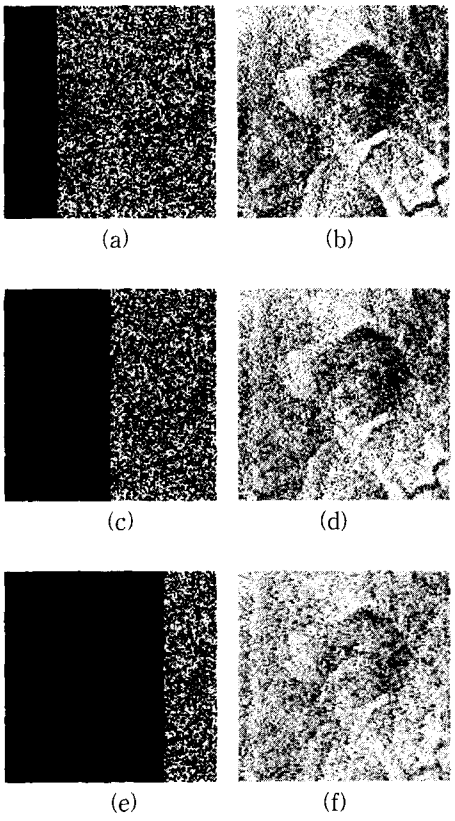

그림 6. u축을 따라 암호화된 영상이 각각 (a) 25%, (c) 50%, (e) 75% 절단되었을 때 그에 대응하여 복원된 영상 (b), (d), (f)
Fig. 6. The occluded encrypted images of (a) 25%, (c) 50%, and (e) 75% along the u-axis and the corresponding reconstructed images (b), (d), and (f), respectively.

또한 암호화된 영상이나 퓨리에 복호화키가 복호화를 위한 실험 구성도의 정확한 위치로부터 u축을 따라 변이가 발생할 경우 식 (5)는

$$P(u,v) = E[u-(u_0+a),v] + D(u+u_0,v) \quad (13)$$

로 표현되며 여기서 a는 $k/(N+k)$이며 N은 암호화된 영상의 픽셀 수이며 k는 u축을 따라 이동된 픽셀 값이다. 이때 식 (13)은 퓨리에 렌즈 $L1$에 의해 퓨리에 역변환되어 CCD에 나타나는 세기함수는

$$|o(x,y)|^2 = 1+1+\exp[j\pi f(x,y)]\exp(j2\pi\alpha x) + \exp[-j\pi f(x,y)]\exp(-j2\pi\alpha x) \quad (14)$$
$$= 2+2\cos[\pi f(x,y)+2\pi\alpha x]$$

로 표현된다. <그림 7(a), (b), (c)>와 <그림 7(d)>는 퓨리에 영역에서 암호화된 영상이 정확한 위치에서 각각 u축을 따라 1, 3, 5, 7 픽셀만큼 변이가 생겼을 경우에 재생된 영상들이다. 여기서 복원 영상의 전 영역에 여현 함수의 위상 성분에 의하여 줄무늬가 발생하고 이 재생된 영상의 줄무늬 개수와 암호화된 영상의 이동된 픽셀 값이 동일함을 알 수 있다. 따라서 재생된 영상을 통하여 암호화된 영상의 변이 정도를 알 수 있음으로 컴퓨터의 후처리를 통하여 보완할 수 있다. 또한 제안한 암호화 방법은 u축 뿐만 아니라 v축과 u-v축에 대한 이동에 대해서도 동일한 특성을 가진다.

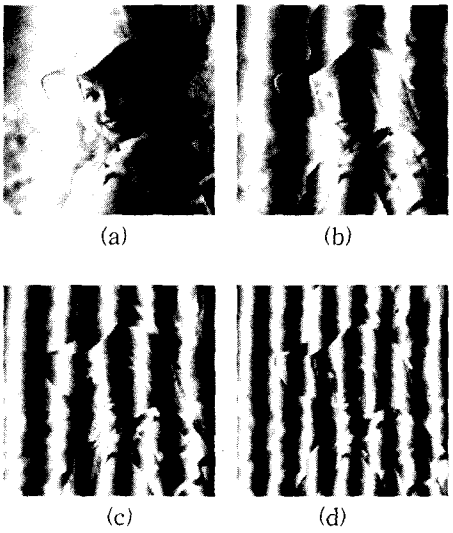

그림 7. 퓨리에 영역에서 암호화된 영상이 정확한 위치에서 각각 u축을 따라 (a) 1, (b) 3, (c) 5, (d) 7 픽셀만큼 변이가 생겼을 경우에 재생된 영상

Fig. 7. The decrypted results when the encrypted image is shifted for (a) one, (b) three, (c) five, and (d) seven pixels from the matching position in Fourier space, respectively.

Ⅳ. 결 론

본 논문에서는 가상 위상 영상과 JTC의 가장 큰 문제점인 자기상관성분을 이용하여 원 영상을 복원할 수 있는 방법과 제안한 방법이 잡음이나 변이, 절단에 강한 특성을 가짐을 확인하였다. 제안한 방법은 가상 위상 영상과 무작위 위상 영상의 곱을 퓨리에 변환하여 암호화된 영상으로 사용하므로 허가되지 않은 사람들이 이 암호화된 영상을 분석함으로써 있을 수 있는 복제 가능성을 배제하였으며 퓨리에 변환된 위상 영상들을 JTC의 주파수 평면에 두어 퓨리에 역변환하여 원 영상을 재생함으로 JTC의 문제점인 자기상관성분을 이용하여 복호화되는 장점을 가진다. 하지만 제안한 복호화 방법은 전통적인 JTC구조의 퓨리에 역변환하는 한 과정만 이용하므로 위상성분의 영향이 발생한다. 따라서 본 논문에서는 검증실험을 통하여 위상성분의 영향을 확인하고 그 제거 방법으로 암호화 과정에서 동일한 위상 성분을 미리 곱하여 이를 퓨리에 변환하여 결합입력평면에 둠으로써 해결하였고 결합 변환 상관기를 이용한 제안한 복호화 방법이 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] 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.

[7] 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.

[8] 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.

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

[10] 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.

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

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

[13] 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.

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

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

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

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

[18] 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.

[19] C. lemmi, 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