

가상 영상을 이용한 주파수 영역에서의 광학적 암호화 및 복호화 방법

서동환[†] · 조규보 · 박세준 · 김수중

경북대학교 전자전기컴퓨터학부

Ⓣ 701-702 대구광역시 북구 산격동 1370

김정우

동양대학교 전자공학과

Ⓣ 750-711 경북 영주시 풍기읍 교촌동 1

노덕수

경일대학교 전자정보공학과

Ⓣ 712-701 경북 경산시 하양읍 부호리 33

(2002년 12월 2일 받음, 2003년 4월 7일 수정본 받음)

본 논문에서는 위상 변조된 가상 영상과 결합변환상관기를 이용하여 암호화 및 복호화 수준을 향상시키는 방법을 제안하였다. 원 영상은 주파수 영역에서 가상 위상 영상과 무작위 위상 영상의 곱을 푸리에 변환하여 만든 암호화 영상과 제안한 위상 대응 규칙으로 만든 푸리에 복호화 키를 푸리에 변환하여 출력 평면에서 간단히 복원된다. 제안한 방법은 암호화된 영상을 허가되지 않은 사람들이 분석함으로써 있을 수 있는 복제 가능성을 원 영상의 어떤 정보도 포함하지 않은 가상 영상을 사용함으로써 배제할 수 있다. 또한 위상 변조된 영상의 자기상관성분의 세기는 1이므로 원 영상은 이 자기상관성분을 이용하여 재생되므로 결합변환상관기의 가장 큰 문제점인 자기상관성분을 제거해야 하는 문제를 해결할 수 있다. 하지만 위상 암호화 방법은 잡음이나 흠집에 민감하여 복원영상의 왜곡이 발생할 수 있으므로 본 논문에서는 이 문제를 분석하고 해결책을 제시하였다. 검증 실험을 통하여 분석의 타당성을 확인하고 제안한 암호화 방법이 광 암호화 시스템에 적용 가능성을 확인하였다.

주제어 : joint transform correlator, fourier hologram, interference.

I. 서 론

광학적 보안 시스템은 무작위 위상을 발생시켜 원 영상을 암호화 한 후 위상 마스크, 컴퓨터 형성 홀로그래프(CGH: computer generated hologram) 또는 공간 광 변조기(SLM: spatial light modulator)에 기록을 한다. 이렇게 암호화된 영상은 세기정보와 위상정보가 동시에 기록되므로 사람의 눈이나 기존의 세기검출기로는 추출이 불가능하고 무작위 특성에 의해서 원래의 패턴을 역추적하기가 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 광축정렬 문제와 암호화할 때 사용한 위상마스크의 복소공액 마스크를 제작해야 하는 어려움이 있으며, 간섭계를 이용한 시스템은 정밀한 실험구성을 필요로 하며 외부 교란에 많은 영향을 받는다는 단점이 있다. 이에 반하여 결합변환상관기(JTC: joint transform correlator)^[7]는 광축정렬이 필요 없고 외부교란에도 거의 영향을 받지 않는 장점이 있다. 그러나 JTC는 그 구조적인 특성 때문에 출력 평면에 큰 세기의 자기상관성분이 나

타하는데, 이는 JTC를 광 상관 시스템이나 광 보안 시스템에 이용하기 어렵게 만드는 주 원인이 된다. 최근 JTC를 이용한 광학적 암호화 방법^[8]이 제안되었는데 이는 JTC의 주파수 스펙트럼(JPS: joint power spectrum)을 암호화된 영상으로 기록하여 사용하고, 4-f 상관시스템을 이용하여 복호화 한다. 따라서 이 방법은 기록된 암호화 패턴이 실수함수이므로 세기검출기로 복사가 가능하고, 복호화시 4-f 상관기를 이용하므로 광축정렬의 어려움이 존재한다. 또한 기록된 JPS에 존재하는 자기상관성분을 제거하여야 하는 문제점을 가지고 있다. 자기상관성분을 제거하는 가장 대표적인 방법은 디지털 감산연산을 수행하여 제거하는 것인데^[9] 이는 JTC의 입력평면을 구성하기 전에 각각의 입력영상들의 파워스펙트럼을 미리 CCD 카메라로 획득하여 컴퓨터에 저장한 후 JPS에서 빼주는 과정을 거치므로 실시간 처리에 문제로 작용한다. 최근에는 세기정보 암호화 수준을 향상시키기 위하여 입력평면에 위상정보를 가지는 원 영상을 이용하여 암호화하는 방법^[10,11]들이 제안되었으며 이 중 Mogensen 등^[12,13]은 위상 정보를 암호화한 후 일반화된 위상 세기 방법(generalized phase-contrast technique)을 이용하여 간단히 원 영상을 복원할 수 있으나 복호화 과정에서 위상 세기 필터(phase-contrast filter)와 4-f 시스템을 이용하므로 광축정렬의 어려움을 가진다. 앞서 제안된 방법들의 가장 큰 단점 중에 하나는 만약 허가되지 않은 사용자가 암호

[†]E-mail: dhseo@palgong.knu.ac.kr

화된 영상을 분석하여 암호화 키를 파악함으로써 복원 영상을 역 추적할 수 있는 문제점이 있다. 이를 해결하기 위해 반복적인 알고리즘을 이용하여 가상 세기영상을 이용한 방법¹⁴⁾이 제안되었으나 이 또한 광축정렬의 어려움을 가지고 원 영상을 재생하기 위한 시간소모가 많다.

본 논문에서는 가상 위상 영상과 JTC의 자기상관성분을 이용하여 원 영상을 복원할 수 있는 암호화 방법을 제안하였다. 제안한 방법은 먼저 원 영상의 정보가 없는 가상 위상 영상과 무작위 위상 영상의 곱을 푸리에 변환하여 암호화된 영상으로 사용하므로 허가되지 않은 개인이나 그룹이 암호화된 영상을 분석하더라도 가상 영상을 원 영상으로 오인하게 된다. 따라서 복호화 키의 정보 없이는 결코 원 영상의 정보를 확인할 수 없게 됨으로써 보다 높은 정보 보호가 가능하다는 장점을 가진다. 푸리에 변환된 위상 영상들을 JTC의 주파수 평면에 두어 푸리에 변환하여 원 영상을 재생함으로써 기존의 JTC를 이용한 광학적 암호화 방법에서 자기상관성분을 제거하여야 하는 문제점을 해결하고 이를 이용하여 복호화되는 장점을 가진다 하지만 위상 암호화 시스템은 잡음이나 흠집 등에 민감하므로 이에 대한 분석을 통하여 해결책을 제시하였다. 검증 실험을 통하여 JTC 구조에서 발생하는 위상성분의 영향에 대한 분석의 타당성을 검증하고 제안한 암호화 방법이 광 암호화 시스템에 적용 가능함을 확인하였다.

II. 전통적인 JTC

전통적인 JTC의 시스템 블럭도는 그림 1과 같다. 여기에서 SLM은 입력영상이 올라가는 결합입력평면(joint input plane)을, 렌즈 L1은 푸리에 변환렌즈를, P1은 출력평면을 나타내며, f 는 렌즈의 초점 거리이다. 그림 1에서 $r(x, y)$ 는 중심이 $(-x_0, 0)$ 에 배치되는 기준영상이고 $h(x, y)$ 는 중심이 $(x_0, 0)$ 에 배치되는 입력영상이다. 이는

$$e(x, y) = h(x - x_0, y) + r(x + x_0, y) \tag{1}$$

로 주어지며, 결합입력평면은 L1에 의해서 푸리에 변환되는데 이는

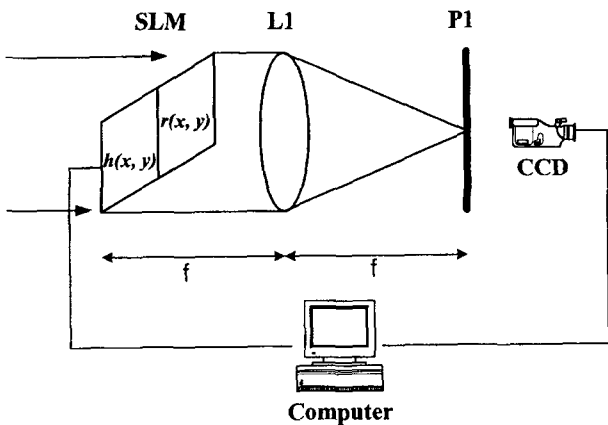


그림 1. 전통적인 결합변환상관기.

$$E(u, v) = H(u, v)\exp(-j2\pi x_0 u) + R(u, v)\exp(j2\pi x_0 u) \tag{2}$$

와 같이 표현되고, 출력평면 P1에 놓인 세기 검출기(intensity detector) 출력단의 광세기 함수는

$$\begin{aligned} |E(u, v)|^2 &= |H(u, v)|^2 + |R(u, v)|^2 \\ &+ H(u, v)R^*(u, v)\exp(-j4\pi x_0 u) \\ &+ H^*(u, v)R(u, v)\exp(j4\pi x_0 u) \end{aligned} \tag{3}$$

와 같이 표현된다. CCD로 검출된 광세기 함수는 다시 SLM으로 올려지게 되며, L1에 의해서 푸리에 역변환된다. 이때 출력 상관평면에서의 광분포 함수는

$$\begin{aligned} g(x, y) &= h \star h + r \star r + h \star r \star \delta(x + 2x_0, y) + r \star h \star \delta(x - 2x_0, y) \end{aligned} \tag{4}$$

와 같다. 여기서 \star 는 상관자를, $*$ 는 상승자를 뜻한다. 식 (1)에서 결합입력평면에 놓여진 각각의 영상은 공간영역에서 원래의 중심에 대해 $\pm x_0$ 만큼 이동한 결과가 되며 이는 주파수 영역에서 식 (2)의 위상성분 $\exp(j2\pi x_0 u)$ 으로 나타나게 된다. 식 (3)과 식 (4)에서 앞의 두 항은 각각의 입력영상의 자기상관 성분이며, 뒤의 두 항은 각 입력영상간의 상호상관성분이다. 자기상관의 세기는 상호상관의 세기에 비해 아주 크므로 광상관 시스템에서는 오인식을 유발시키며, 광 보안 시스템에서는 원 영상의 복원을 어렵게 만든다.

III. 제안한 암호화 방법 및 JTC를 이용한 복호화

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

$$\begin{aligned} f_p(x, y) &= \exp[j\pi f(x, y)] \\ &= \exp\{j\pi[v(x, y) + r(x, y) - d(x, y)]\} \end{aligned} \tag{5}$$

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

$$v_p(x, y) = \exp[j\pi v(x, y)], \quad r_p(x, y) = \exp[j\pi r(x, y)] \tag{6}$$

와 같이 표현되며 여기서 변조된 영상의 위상 값은 $[0, \pi]$ 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

$$\begin{aligned} e(x, y) &= v_p(x, y)r_p(x, y) \\ &= \exp\{j\pi[v(x, y) + r(x, y)]\} \end{aligned} \tag{7}$$

와 같고 원 영상과 무작위 영상의 선형적인 합임을 알 수 있고 이를 푸리에 변환하여 암호화된 영상 $E(u, v)$ 로 사용한다. 이때 만약 허가되지 않은 개인이나 그룹이 암호화된 영상을 푸리에 변환이나 위상 측정 방법 등으로 분석하더라도 가상영

상을 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 복호키영상을 만드는 방법은

$$d_p(x, y) = \exp[j\pi d(x, y)] \\ = \exp\{j\pi[v(x, y) + r(x, y) - f(x, y)]\} \quad (8)$$

와 같이 표현되며 이를 푸리에 변환하여 복호화키 $D(u, v)$ 로 사용한다.

복호화에 사용되는 JTC 구성도는 그림 1과 동일하나 입력 평면을 공간 영역이 아닌 주파수 영역으로 표현한다. 암호화된 영상 $E(u, v)$ 는 그림 1의 결합입력평면의 우반 평면에, 복호화키 $D(u, v)$ 는 좌반평면에 각각 놓여지며, 결합입력평면 $J(u, v)$ 는

$$J(u, v) = E(u - u_0, v) + D(u + u_0, v) \quad (9)$$

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. 결합평면은 렌즈 L1에 의해서 푸리에 역변환 되어지며 이는

$$j(x, y) = e(x, y)\exp(j2\pi u_0 x) + d_p(x, y)\exp(-j2\pi u_0 x) \quad (10)$$

로 주어진다. 여기서 $\exp(j2\pi u_0 x)$ 는 주파수 영역에서 중심의 이동에 의해 생기는 출력평면에서의 위상성분이다. 출력평면 PI에 놓인 CCD 카메라에 의해서 검출되어지는 세기함수는

$$|j(x, y)|^2 = |e(x, y)|^2 + |d_p(x, y)|^2 \\ + e(x, y)d_p^*(x, y)\exp(j4\pi u_0 x) \\ + e^*(x, y)d_p(x, y)\exp(-j4\pi u_0 x) \quad (11) \\ = 1 + 1 + \exp[j\pi f(x, y)] \exp(j4\pi u_0 x) \\ + \exp[-j\pi f(x, y)] \exp(-j4\pi u_0 x) \\ = 2 + 2\cos[\pi f(x, y) + 4\pi u_0 x]$$

와 같다. 식 (11)에서 위상 성분 $4\pi u_0 x$ 를 고려하기 위해 표본화된 영상의 주파수 영역과 공간영역의 관계를 살펴보면

$$\Delta d = \frac{1}{2f_{x0}}, \quad x = k\Delta d = k\frac{L}{N_x} \\ u = k\frac{1}{\Delta d} = k\frac{N_x}{L}, \quad k = 0, 1, \dots, N_x - 1 \quad (12)$$

로 주어지며 여기에서 편의상 x 축과 u 축만 표시하였다. 여기서 Δd 는 표본화 간격, f_{x0} 는 영상의 x 축의 최고 주파수, L 은 x 축으로의 영상의 길이, k 는 화소번호이며 N_x 는 표본화 개수이다. 그림 1에서 각 입력영상의 중심인 $(\pm u_0, 0)$ 는 중심에서 $1/2$ 되는 지점만큼 이동되므로 위의 값을 식 (11)에 대입하여 정리하면

$$|j(x, y)|^2 = 2 + 2\cos[\pi f(x, y) + 2k_x] \\ = 2 + 2\cos[\pi f(x, y)] \quad (13)$$

와 같으며 여기서 k_x 는 x 축으로의 화소 번호이므로 복원영상에 영향을 미치지 않는다. 식 (13)에서 복원 영상이 이진 영상이면 정확히 원 영상이 복원되지만 그레이 영상으로 확장하면 식 (13)의 여현 함수의 비선형성에 의해 영상의 왜곡이 발생함을 알 수 있으며 이를 해결하기 위해서는 컴퓨터의 후처리가 동반되어야 하는 단점을 가지고 있다. 또한 위상 암호화 방법은 암호화 과정에서의 위상차나 계속적인 사용으로 인한 흠집 등의 문제로 인한 복원 영상의 왜곡이 발생할 수 있다. 따라서 본 논문에서는 이러한 문제들이 발생하더라도 컴퓨터로 원 영상과 반전 영상의 정보를 함께 얻는다면 원 영상의 정보를 인식할 수 있음을 컴퓨터 모의 실험을 통하여 확인하였다.

IV. 검증 실험

그림 2는 컴퓨터 모의실험을 위하여 제작된 영상들로 그 화소수는 128×128 이다. 그림 2(a)는 복원할 원 영상 $f(x, y)$ 로 그레이 값을 가지는 'Elaine'를 사용하였고 그림 2(b)와 (c)는 각각 암호화된 가상 영상 $v(x, y)$ 와 컴퓨터로 발생시킨 무작위 영상 $r(x, y)$ 이며 이들을 각각 $[0, 1]$ 사이의 값으로 정규화시켜 위상 변조하여 서로 곱한 후 푸리에 변환한 암호화된 영상을 그림 2(d)에 나타내었으며 이는 가상 영상과는 전혀 관계 없는 무작위 패턴으로 나타남을 확인할 수 있다. 또한 만약 허가되지 않은 사람들이 암호화키를 분석하더라도 가상 영상을 원 영상으로 오인하게 되므로 복제 가능성을 배제할 수 있다. 그림 3(a)와 (b)는 각각 복원 영상을 얻기 위해 제안한 위상 대응 규칙으로 만든 올바른 복호화키의 푸리에 변환된

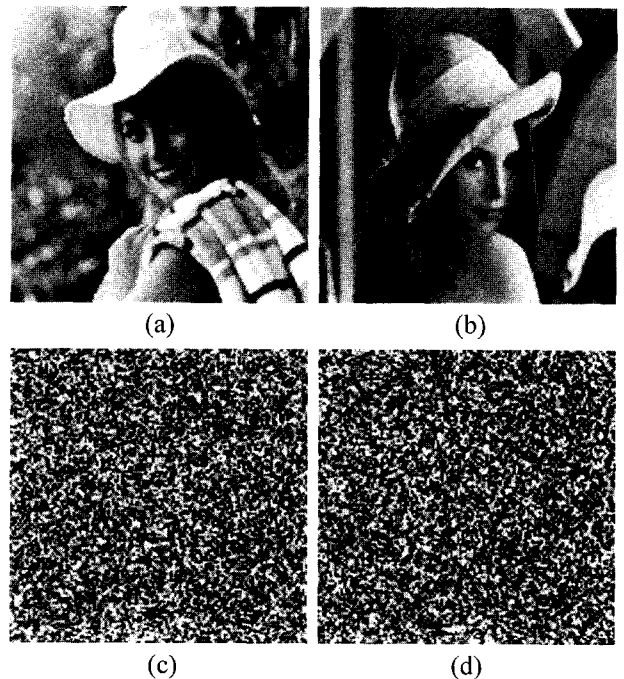


그림 2. 컴퓨터 모의실험에 사용된 영상. (a) 원 영상, (b) 가상 영상, (c) 무작위 영상, (d) 암호화된 영상.

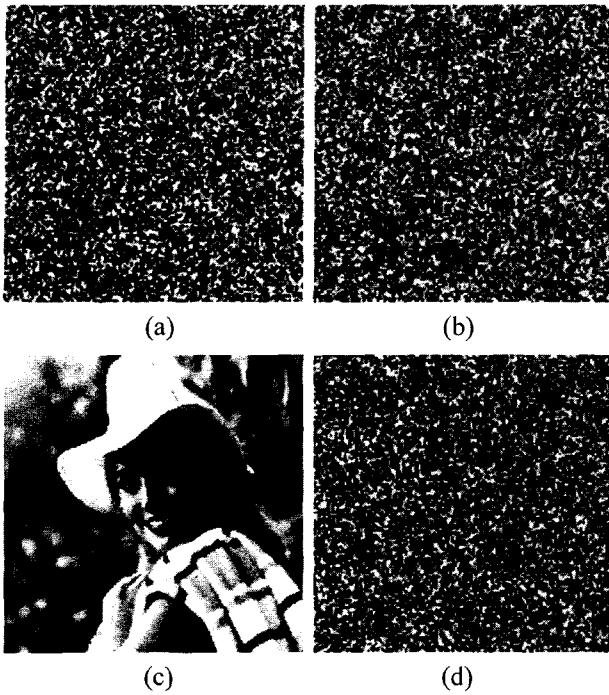


그림 3. 컴퓨터 모의실험 결과. (a) 올바른 푸리에 복호화키, (b) 거짓 푸리에 복호화키, (c) 올바른 푸리에 복호화키로 재생된 영상, (d) 거짓 푸리에 복호화키로 재생된 영상.

영상과 컴퓨터를 통해 만든 거짓 키이며 그림 3(c)와 (d)는 이에 각각 대응되는 복원 영상들로서 거짓 키로는 영상이 재생되지 않음을 확인할 수 있으나 그림 3(c)에서 그레이 영상을 재생함으로써 식 (13)의 여현 함수의 비선형성에 의해 원 영상의 왜곡이 발생하는데 그림 3(c)에서 이는 보상하지 않았지만 후처리를 통하여 보상을 할 수 있다. 그러나 실제 위상 암호화 시스템은 세기 암호화 시스템보다 암호화 수준은 향상되지만 잡음이나 위상 마스크의 흠집 등에 민감하여 영상의 왜곡이 발생할 수 있다. 따라서 암호화된 영상이나 푸리에 복호화키의 암호화 과정에서의 위상차나 계속적인 사용으로 인한 흠집 등의 문제로 인한 복원 영상의 왜곡이 발생할 수 있으므로 이로 인한 영상왜곡의 특성을 고려하면 식 (13)은

$$|j(x, y)|^2 = 2 + 2n_a(x, y)\cos[\pi\{f(x, y) + n_p(x, y)\}] \quad (14)$$

이 되고 여기서 잡음 $n(x, y) = n_a(x, y)\exp[j\pi n_p(x, y)]$ 이고 n_a 와 n_p 는 각각 복원 영상에서 나타날 수 있는 먼지나 흠집에 의한 크기 잡음과 위상 잡음이다. 여기서 n_a 는 실제 시스템에서 중요한 문제지만 위상 암호화 시스템에서는 크기 성분을 보통 '1'로 둔다.¹¹⁾ 그림 4는 위상 잡음(n_p)이 있을 경우 복원 영상과 그것의 반전 영상의 평균제곱오차(mean square error; MSE)를 나타내었다. 여기에서 사용된 평균제곱오차의 표준¹¹⁾은

$$MSE = E \left\{ \frac{1}{N \times M} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} [|f_o(x, y)| - |f_d(x, y)|]^2 \right\} \quad (15)$$

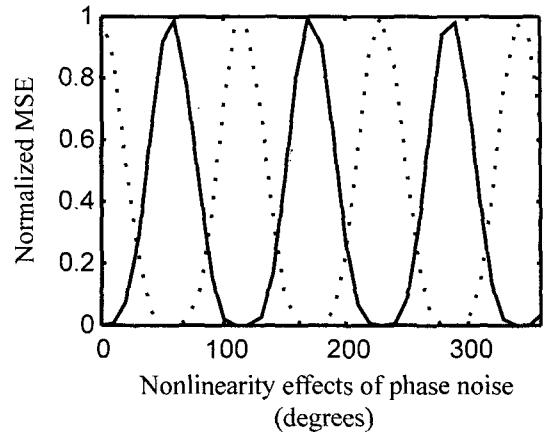


그림 4. 복원 영상의 위상 잡음으로 인한 평균 제곱 오차.

이며 여기서 $f_o(x, y)$ 와 $f_d(x, y)$ 는 각각 원 영상과 복원 영상이고 $N \times M$ 은 원 영상의 픽셀 수이며 $E\{\cdot\}$ 는 평균값이다. 그림 4에서 점선은 복원 영상이 위상차가 발생할 경우 원 영상과의 정규화 평균제곱오차를 표현하고 실선은 위상차가 발생한 복원 영상의 반전 영상과 원 영상과의 정규화된 평균제곱오차를 표현한 것이며 이는 컴퓨터로 복원 영상과 그것의 반전 영상을 모두 얻는다면 원 영상의 복원이 가능함을 나타낸다. 그러나 그림 4에서 1/2 rad부터 1 rad 간격으로 점선과 실선이 만나는 교점에서 정확한 복호화키를 사용하더라도 복원 영상과 반전영상으로 원 영상의 정보를 알 수 없음을 나타낸다.

VI. 결 론

본 논문에서는 가상 위상 영상과 JTC의 자기상관성분을 이용하여 원 영상을 복원하는 암호화 방법을 제안하였다. 가상 위상 영상과 무작위 위상 영상의 곱을 푸리에 변환하여 암호화된 영상으로 사용하므로 허가되지 않은 사람들이 이 암호화된 영상을 분석함으로써 있을 수 있는 복제 가능성을 배제할 수 있으며 JTC를 이용하여 암호화된 영상을 복호화하면 출력에 나타나는 암호화된 영상과 키 코드 영상은 위상 변조된 영상이므로 이들의 자기상관 성분의 세기는 1이 되며 원 영상은 이 자기상관성분을 이용하여 재생된다. 따라서 JTC의 가장 큰 문제점인 자기상관성분을 제거해야 하는 문제를 해결할 수 있다. 하지만 제안한 암호화 방법은 전통적인 JTC 구조의 푸리에 역변환하는 한 과정만 이용하므로 위상성분의 영향이 발생하므로 본 논문에서는 이 문제를 분석하고 해결방법을 제안하였다. 검증 실험을 통하여 위상성분의 영향을 확인하고 그 제거 방법의 타당성을 검증하여 암호화 방법이 광 암호화 시스템에 적용 가능성을 확인하였다.

감사의 글

본 연구는 정보통신부 기초기술연구지원사업(과제번호 : C1-2002-012-0-3) 지원으로 수행되었음.

참고문헌

- [1] B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.*, vol. 33, no. 6, pp. 1752-1756, 1994.
- [2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767-769, 1995.
- [3] 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, no. 9, pp. 2506-2512, 1996.
- [4] L. G. Neto, "Implementation of Image Encryption using the Phase-Contrast Technique," *Proc. SPIE*, vol. 3386, pp. 284-290, 1998.
- [5] B. Javidi and E. Ahouzi, "Optical security system with Fourier plane encoding," *Appl. Opt.*, vol. 37, no. 26, pp. 6247-6255, 1998.
- [6] J. Y. Kim, S. J. Park, C. S. Kim, J. K. Bae, and S. J. Kim, "Optical image encryption using interferometry-based phase masks," *Electron. Lett.*, vol. 36, no. 10, pp. 874-875, 2000.
- [7] C. S. Weaver and J. W. Goodman, "Technique for optically convolving two functions," *Appl. Opt.*, vol. 5, pp. 1248-1249, 1966.
- [8] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," *Opt. Eng.*, vol. 39, No. 8, pp. 2031-2035, 2000.
- [9] C. J. Kuo, "Joint transform correlation improved by means of the frequency selective technique," *Opt. Eng.*, vol. 33, no. 2, pp. 522-527, 1994.
- [10] X. Tan, O. Matoba, T. Shinura, K. Kuroda, and B. Javidi, "Secure optical storage that uses fully phase encryption," *Appl. Opt.*, vol. 39, no. 35, pp. 6689-6694, 2000.
- [11] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," *J. Opt. Soc. Am. A*, vol. 16, no. 8, pp. 1915-1927, 1999.
- [12] P. C. Mogensen and J. Glückstad, "Phase-only optical encryption," *Opt. Lett.*, vol. 25, no. 8, pp. 566-568, 2000.
- [13] P. C. Mogensen and J. Glückstad, "Phase-only optical decryption of a fixed mask," *Appl. opt.*, vol. 40, no. 8, pp. 1226-1235, 2001.
- [14] Hsuan T. Chang, "Image encryption using separable amplitude-based virtual image and iteratively retrieved phase information," *Opt. Eng.*, vol. 40, no. 10, pp. 2165-2171, 2001.

Optical encryption and decryption technique using virtual image in frequency domain

Dong-Hoan Seo[†], Kyu-Bo Cho, Se-Joon Park, and Soo-Joong Kim

School of Electrical Engineering & Computer Science, Kyungpook National University, Daegu 702-701, KOREA

[†]E-mail: dhseo@palgong.knu.ac.kr

Jeong-Woo Kim

Department of Electronic, Dongyang University, Youngju 750-711, KOREA

Duck-Soo Noh

Department of Electronic & Information Engineering, Kyungil University, Daegu 712-701, KOREA

(Received December 2, 2002, Revised manuscript April 17, 2003)

In this paper, we propose an improved image encryption and decryption method using a virtual image and a joint transform correlator (JTC). The encrypted image is obtained by the Fourier transform of the product of a virtual-phase image and a random-phase image, and a Fourier transform of the decrypting key generated by the proposed phase assignment rule is used as the Fourier decrypting key. Based on the solution, the original image is reconstructed using JTC in the frequency-domain. The proposed method using a virtual image, which does not contain any information from the original image, prevents the possibility of counterfeiting by unauthorized people. And also the auto-correlation terms, which are the drawback of a JTC system, contribute to reconstructing the original image rather than to disturbing its identification. But because phase-only encryptions are sensitive to noise and scratches, phase errors can be generated in fabricating the encrypted image or the Fourier decrypting key so the errors that are responsible for degradation of the quality of the reconstructed image are analyzed and the solution is demonstrated. Computer simulations show the solution, and the proposed method is very useful for JTC architecture.

OCIS Codes : 100.1160, 100.4550.