《연구논문》 Hankook Kwanghak Hoeji, Volume 14, Number 6, December 2003

시각 암호화와 가상 위상영상을 이용한 광 암호화 시스템

김인식 · 서동환† · 신창목 · 조규보 · 김수중

경북대학교 전자전기컴퓨터학부

㉾ 701-702 대구광역시 북구 산격동 1370

노덕수

경일대학교 전자정보공학과

㉾ 712-701 경북 경산시 하양읍 부호리 33번지

(2003년 8월 12일 받음, 2003년 11월 10일 수정본 받음)

광을 이용하여 암호화를 하는 경우는 위조 및 복제의 방지를 위하여 세기성분보다는 위상성분을 이용하여 주로 암호화를 하고 있다. 그러나 위상정보를 검출할 수 있는 장비가 개발된다면 정보를 유출 당할 수 있는 위험이 있다. 이러한 위험을 줄이기 위해 본 논문에서는 가상 위상영상을 이용하고 또한 정보를 다수가 공유할 수 있도록 시각 암호화(visual cryptography) 방법을 이용하여 정보를 보다 안전하게 보관하고 공유하는 시스템을 제안하였다.

주제어 : visual cryptography, phase image, image encryption, interferometer.

I. 서 론

현대사회에서 정보산업이 발전함에 따라 단체나 개인의 각종 정보공유의 필요성이 커져 가고 있으며 이에 비례하여 정보보호의 중요성이 커지고 있다. 또한 CCD 카메라, 복사기, 스캐너 등과 같은 하드웨어와 함께 각종 소프트웨어 기술의 발달로 인해 개인의 신원이나 화폐 등의 복제기술의 수준이 높아져 국내외적으로 이로 인한 피해가 늘어나고 있는 실정이다. 따라서 개인이나 단체의 정보에 대한 불법적인 접근이나 사용으로부터 이를 보호하려는 수많은 보안 체계들이 제안되고 구현되어 왔고 컴퓨터, 디지털 및 광학 기술들을 이용하여 위조 및 복제를 방지하기 위한 연구도 활발히 이루어지고 있다.[1-8] 또한 다수의 회사나 주요 국가기관, 일반가정 등에서는 정보로의 접근이나 불법적인 침입을 제한하기 위해 비밀번호나 생물학적 특징을 이용한보안 시스템을 사용하여 기밀 정보의 보호 및 유출방지를 유지하고 있는 경우가 늘어나고 있다. 이와 달리 중요한 정보를 안전하게 관리하기 위해서 정보를 여러 개로 분산하여 이를 허가된 사용자에게만 배포하여 이들의 합의 없이는 그 정보를 결코 확인 할 수 없게 만드는 방안에 대해서도 다양한 연구가 이루어져 왔다. 이의 가장 대표적인 방식이 비밀 정보로서 영상을 이용하여 복잡한 암호학적 연산 없이도 비밀을 복원할 수 있는 시각 암호화(visual cryptography)이다.[9,10] 이 방식으로 분산된 비밀영상은 랜덤한 암호 영상들로 이들을 미리 허락된 사용자들에게 나누어주어 이 영상들이 한자리에 모이지 않는 한 원 영상을 확인하는 것은 불가능하여 안전성이 유지된다.

본 논문에서는 원 영상을 가상 영상(virtual image)과 랜덤 영상을 이용하여 키 영상으로 분리하고 분리한 영상들을 위상변조(phase modulation)를 하여 CCD나 복사기 같은 광 세기 검출기로는 위상의 분포 패턴을 확인할 수 없도록 하였다. 따라서 위상정보가 검출된다 할지라도 원 영상이 분리되어 있어 찾기 힘들도록 하였다. 위상변조된 키 영상은 복호시에 사용하는 위상 키 영상으로 사용하였다. 또한 합이 1이 되는 가상 복소 영상(virtual complex image)들을 이용하여 위상변조된 가상 위상 영상과 랜덤 영상을 숨겼고 이를 푸리에 변환(Fourier transform)영역에서 암호화하였고 이들을 허가된 사용자들에게 나누어주는 카드로 사용하였다. 따라서 정당한 사용자가 아닌 사람이 이 카드를 훔치더라도 그 카드에는 원 정보를 전혀 가지지 않는 복소 영상과 가상 위상 영상과 랜덤 영상만 있기 때문에 정보가 유출될 염려가 사라지게 된다. 복호화는 마흐-젠더 간섭계(Mach-Zehnder interferometer)의 광 경로가 동일한 지점에 이 카드들을 놓아 간섭시키고 푸리에 렌즈를 통하여 역 변환을 수행한 후 키 영상과 곱을 수행하고 참조파(reference beam)를 사용하여 간섭한 후 CCD로 검출함으로써 원 영상을 복원해 낼 수 있다. 이렇게 재생된 영상은 이론적으로 여현함수의 비선형성 때문에 약간의 차이는 있으나 시각적으로는 크게 차이를 느끼지 못한다. 컴퓨터 시뮬레이션을 통하여 제안한 시각 암호화와 가상 위상영상을 이용한 광 암호화 시스템의 유용성을 확인하였다.

II. 시각 암호화와 가상 위상영상을 이용한 암호화 및 복호화 과정

2.1. 시각 암호화 기법

중요한 정보를 안전하게 관리하기 위해서 정보를 여러 개로 분산하여 임의의 개수 이상이 결합되면 비밀정보에 접근할 수

†E-mail: dhseo@palgong.knu.ac.kr

있지만, 그 미만이 결합되면 결코 비밀정보에 접근할 수 없는 비밀 관리 체계인 (k, n)문턱치 비밀 분산법이 Shamir[8]에 의해 제안된 이후, 비밀정보로서 영상을 이용하여 복잡한 암호학적 연산 없이도 비밀을 복원할 수 있는 시각암호화가 Naor와 Shamir[9]에 의해 제안되었다. 이 방식에 의해 분산된 비밀영상은 슬라이드와 같은 물리적 중첩이 가능한 곳에 인쇄되는 경우를 가정한다. (k, n)비밀 분산법에서처럼 그룹 내 n명에게 배포된 슬라이드 중 임의의 k명 이상의 슬라이드를 겹치면 비밀영상을 복원할 수 있지만, k-1명 이하의 슬라이드를 겹치는 경우에는 비밀영상을 복원할 수 없어 안정성이 유지된다.

2.2. 시각 암호화와 가상 위상영상을 이용한 암호화 과정

원 영상 $f(x, y)$을 시각 암호화 방법을 기초로 하여 가상 영상 $v(x, y)$와 랜덤 영상 $r_1(x, y)$, 키 영상 $r_2(x, y)$로 분리하면

$$r_2(x, y)=f(x, y)-\{v(x, y)+2r_1(x, y)\} \tag{1}$$

와 같이 된다. 분리된 영상들을 각각 위상변조시켜 위상 가상 영상과 위상 랜덤 영상의 곱을 수행하고 위상 키 영상은 복호시에 사용하는 키로서 사용하게 된다.

$$p_{vr_1}=\exp[j\pi\{v(x, y)+2r_1(x, y)\}]$$
$$p_{vr_2}=\exp\{j\pi r_2(x, y)\} \tag{2}$$

합이 1이 되는 복소 영상 $A_i(x, y)\exp\{j\pi\phi_i(x, y)\}$을 선택하면

$$\sum_{i=1}^{N}A_i(x, y)\exp\{j\pi\phi_i(x, y)\}=C(x, y)=1 \tag{3}$$

와 같이 되고 이 각각의 복소 영상에 식 (2)의 p_{vr_1}을 곱하면

$$\begin{aligned}&A_1(x, y)\exp\{j\pi\phi_1(x, y)\}p_{vr_1}\\&\quad=A_1(x, y)\exp[j\pi\{v(x, y)+2r_1(x, y)+\phi_1(x, y)\}]\\&A_2(x, y)\exp\{j\pi\phi_2(x, y)\}p_{vr_1}\\&\quad=A_2(x, y)\exp[j\pi\{v(x, y)+2r_1(x, y)+\phi_2(x, y)\}]\\&\qquad\cdots\\&A_N(x, y)\exp\{j\pi\phi_N(x, y)\}p_{vr_1}\\&\quad=A_N(x, y)\exp[j\pi\{v(x, y)+2r_1(x, y)+\phi_N(x, y)\}]\end{aligned} \tag{4}$$

와 같이 되어 위상 가상 영상과 랜덤 영상이 복소 영상에 숨겨지는 효과를 가지게 된다. 식 (4)에 만들어진 영상들을 각각 푸리에 변환을 수행하면

$$\begin{aligned}&H_1(u, v)=\mathcal{F}[A_1(x, y)\exp\{j\pi\phi_1(x, y)\}p_{vr_1}]\\&H_2(u, v)=\mathcal{F}[A_2(x, y)\exp\{j\pi\phi_2(x, y)\}p_{vr_1}]\\&\qquad\cdots\\&H_N(u, v)=\mathcal{F}[A_N(x, y)\exp\{j\pi\phi_N(x, y)\}p_{vr_1}]\end{aligned} \tag{5}$$

와 같이 되고 이 $H_i(u, v)(i=1, 2, 3, \cdots, N)$을 미리 허락된 사용자들에게 나누어주는 카드로서 사용한다. 여기서 $\mathcal{F}$는 푸리에 변환을 나타낸다.

2.3. 복호화 과정

복호화는 나누어진 카드들이 모두 한자리에 모였을 때 Mach-Zehnder 간섭계를 이용하여 이루어진다. 각 카드들은 간섭계의 경로 상에 렌즈의 초점거리에 맞추어 위치시켜 광학적인 합을 수행한 후 푸리에 변환을 수행하고 이것을 다시 위상키 카드와 곱을 수행한 후 참조파와 간섭에 의해 복호 영상을 얻는다. 암호화된 카드들이 간섭계의 정렬 오차로 인해 각각 다른 방향으로 이동되어 중첩되었을 경우 이동된 성분들은 푸리에 변화 후 위상함수로 나타나며, 이 위상함수들은 복원시 합이 1이 되어야 할 각각의 복소 영상들에 곱해져 암호화된 카드에 사용된 복소 영상을 임의의 복소 영상으로 변화시킨다. 그러므로 세기패턴으로 관측되는 영상은 임의의 값을 가지는 코사인 함수와 원 영상의 정보를 가지는 코사인 함수의 곱으로 인해 잡음형태로 나타나며, 세기패턴에 원 영상의 정보가 있다하더라도 원 영상의 정보를 재생할 수가 없다. 만약 암호화된 각 카드들이 모두 동일한 값의 오차로 정렬되어 중첩된다면, 오차의 값은 CCD평면에서 일정한 줄무늬로 나타나므로 오차를 보정할 수 있다.[11]

그림 1은 카드가 4개일 때 복호화에 사용된 Mach-Zehnder 간섭계의 구성도이다. 암호화된 카드들을 그림 1의 간섭계에 사용할 경우, 거울 2, 3, 4 후의 카드들은 beam splitter를 지나면서 영상이 좌우가 바뀌게 되므로 거울 2, 3, 4 경로에 해당하는 암호화된 카드들은 각각 좌우를 바꾼 상태로 간섭계에 사용한다. 먼저 간섭계를 경로 상에 놓이게 되는 카드들의 합을 수행하면 결과는

$$H(u, v)=H_1(u, v)+H_2(u, v)+\ldots+H_N(u, v) \tag{6}$$

와 같이된다. 만약 서로 다른 경로의 beam splitter를 통과한 암호화된 카드들의 크기가 다르게 중첩될 경우, 화소 대 화소의 간섭결과는 원 영상 복원의 정보가 아닌, 임의의 값으로 바뀌므로 카드들의 합은 임의의 잡음 형태로 나타난다. 그러므로, 간섭계에 놓인 카드들의 각 경로에 있는 이미지 렌즈(Imaging lens)들을 조절하여 중첩되는 카드들의 크기가 동일하게 한 후 푸리에 렌즈를 통해 역 푸리에 변환을 하게 되면

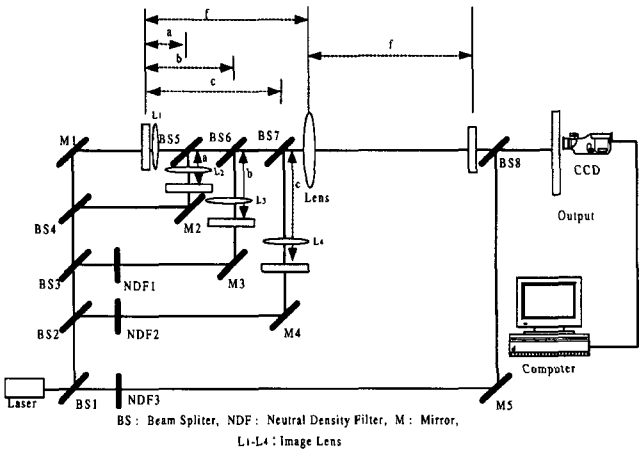

그림 1. 카드가 4개 일때 영상 복원 시스템.

$$h(x,y)=\mathcal{F}^{-1}[H(u,v)]$$
$$=[A_1(x,y)\exp\{j\pi\phi_1(x,y)\}+A_2(x,y)\exp\{j\pi\phi_2(x,y)\}$$
$$+\cdots+A_N(x,y)\exp\{j\pi\phi_1(x,y)\}]$$
$$\times\exp[j\pi v(x,y)+2r_1(x,y)\}]$$
$$=\exp[j\pi\{v(x,y)+2r_1(x,y)\}] \quad (7)$$

이 된다. $\mathcal{F}^{-1}$는 역푸리에 변환을 나타내며 복소 영상의 합이 1이 된다. 여기에 위상 키 카드를 곱해주게 되면

$$h(x,y)\exp\{j\pi\ r_2(x,y)\}$$
$$=\exp[j\pi\{v(x,y)+2r_1(x,y)+r_2(x,y)\}]$$
$$=\exp\{j\pi v(x,y)\} \quad (8)$$

이 되어 위상 성분에 원 정보가 나타남을 알 수 있다. 참조파(reference beam) $R(x,y)$와의 간섭을 세기 $I(x,y)$로 나타내면

$$I(x,y)=|R(x,y)+R(x,y)\,\mathcal{F}^{-1}[H(u,v)]\exp\{j\pi r_2(x,y)\}|^2$$
$$=|R(x,y)+R(x,y)h(x,y)\exp\{j\pi r_2(x,y)\}|^2$$
$$=|R(x,y)|^2|1+\exp\{j\pi f(x,y)\}|^2$$
$$=1+1+\exp\{j\pi f(x,y)\}+\exp\{-j\pi f(x,y)\}$$
$$=2+2\cos\{\pi f(x,y)\} \quad (9)$$

이 되어 반전된 영상을 얻을 수 있다. 반전된 영상은 결국 키 영상들의 합인 복소 영상 함수 $H(u,v)$의 역푸리에 변환 영상에 위상키 카드를 곱한 결과와 참조파와의 간섭으로 구해지므로, 복소 영상 함수 $H(u,v)$는 복호화 과정에서 원 정보 재생시 필요한 시스템의 전달함수의 역할을 한다. 여기서 $R(x,y)=\exp(j\Phi)$이며, Φ는 간섭계 경로에 의한 위상차이다. 원 영상과 비교하면 여현함수의 비선형 특성 때문에 약간의 차이는 있으나 인간의 시각으로 구별하기는 어렵다.

III. 컴퓨터 모의 실험과 고찰

3.1. 컴퓨터 시뮬레이션

컴퓨터 시뮬레이션에 사용한 영상들은 128×128 그레이 영상이며 가상 복소 영상은 4개를 사용하였고 랜덤 영상은 컴퓨터 프로그램에서 제공하는 랜덤 발생기를 이용하였고, 그림 1의 복호 시스템을 기초로 하여 간섭계의 각 광 경로에서 경로길이가 일정하다는 가정에서 시뮬레이션을 실행하였다. 그림 2(a)는 원 영상을 나타내고, 그림 2(b)~(c)는 가상 영상, 랜덤 영상, 키 영상을 각각 나타내고 있고 이 영상들의 합이 원 영상이 된다. 그림 2의 영상들을 각각 위상변조하여 위상 가상 영상과 위상 랜덤 영상은 곱을 수행하고 위상 키 영상은 복호화 시에 사용하는 키로서 사용한다. 그림 3은 가상 복소 영상들의 진폭 영상들로 각각 3(a)는 $A_1(x,y)$, (b)는 $A_2(x,y)$, (c)는 $A_3(x,y)$, (d)는 $A_4(x,y)$를 나타내고 있다. 이 복소 영상들의 합은 1이 되도록 하였다. 위상변조된 영상의 곱을 가상 복소 영상에 곱을 수행하여 푸리에 변환한 카드들의 영상은 그림 4에서와 같다. 그림 5는 재생된 영상 5(a)와 그의 반전된 영상 5(b)를 보여주고 있다. 여현 함수의 비선형성으로 인하여 원 영상과 비교하면 약간의 차이는 있으나 원 영상이 잘 복원됨을 알 수 있다.

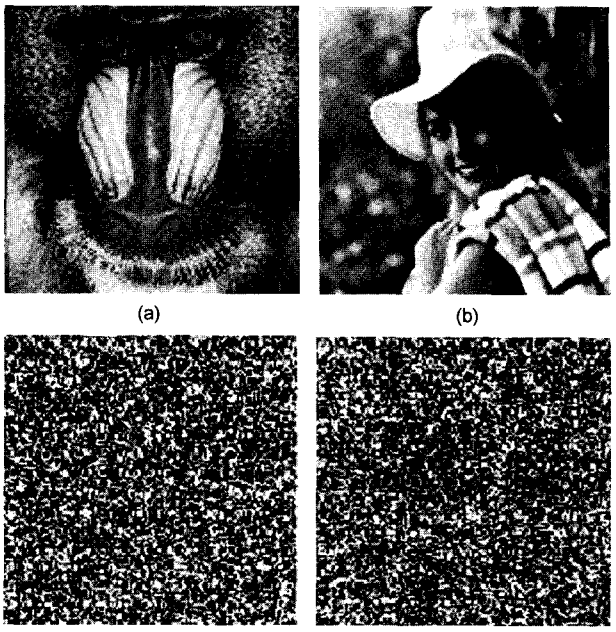

그림 2. 원 영상과 위상변조에 사용된 영상. (a)원 영상, (b)가상 영상, (c)랜덤 영상, (d) 키 영상.

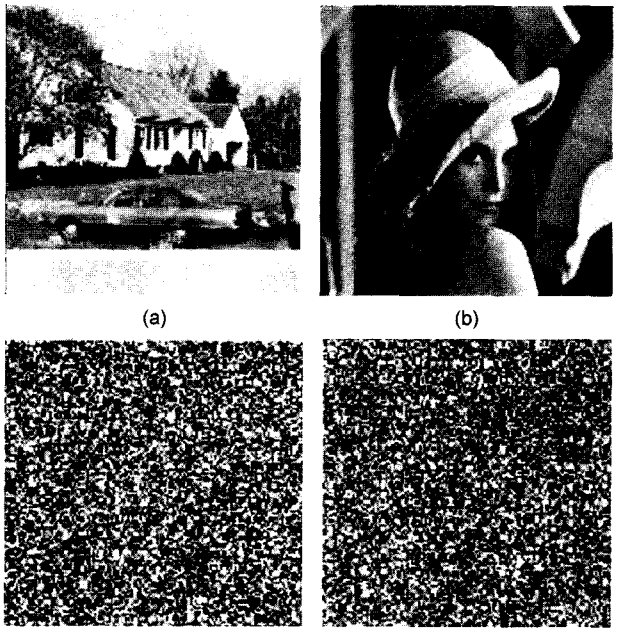

그림 3. 복소 영상의 가상 진폭 영상.

3.2. 컴퓨터 시뮬레이션에 관한 고찰

(1) 거짓 카드를 사용한 경우

모든 카드들이 한자리에 모여야만 복호화가 가능하다 하지만 이 모인 카드 중에 거짓 카드 $H_{diff}(u,v)$가 있을 경우

$$H(u,v)=H_1(u,v)+H_2(u,v)+H_3(u,v)+H_{diff}(u,v) \quad (10)$$

와 같이 되고, 복호화 과정을 전개하면 식 (10)이 역 푸리에 변환되어 위상 키 카드가 곱해질 경우

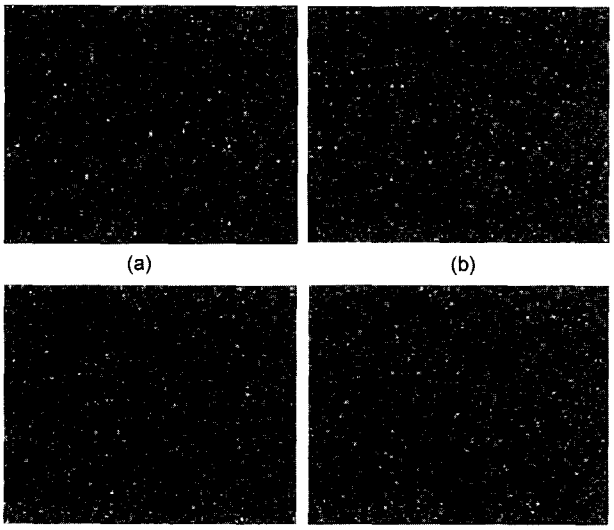

그림 4. 그림 2(b)와 (c)의 위상변조된 영상들이 곱해진 후 그림 3의 가상 복소 영상들에 곱해져 푸리에 변환된 카드 영상.

그림 5. Mach-Zehnder 간섭계를 이용하여 재생된 영상. (a) 재생된 영상, (b) 반전시킨 영상.

$$h(x,y)\exp\{j\pi r_2\}=[A_1(x,y)\exp\{j\pi\phi_1(x,y)\}+A_2(x,y)\exp\{j\pi\phi_1(x,y)\}+A_3(x,y)\times\exp\{j\pi\phi_3(x,y)\}]\exp\{j\pi f(x,y)\}+A_{diff}(x,y)exp\{j\pi r_2(x,y)\} \quad (11)$$

가 되고 최종 세기를 구하면

$$I(x,y)=\left|1+h(x,y)\exp\{j\pi r_2(x,y)\}\right|^2$$
$$=\left|1+S\ \exp\{j\pi f(x,y)\}+A_{diff}(x,y)\exp\{j\pi r_2(x,y)\}\right|^2$$
$$=1+|S|^2+\left|A_{diff}(x,y)\right|^2+S\ \exp\{j\pi f(x,y)\}+S^*\exp\{-j\pi f(x,y)\}+A_{diff}(x,y)\exp\{j\pi\ r_2(x,y)\}+A^*_{diff}(x,y)\exp\{-j\pi r_2(x,y)\}+S^*A_{diff}(x,y)\times\exp[j\pi\{r_2(x,y)-f(x,y)\}]+S\ A^*_{diff}(x,y)\times\exp[-j\pi\{r_2(x,y)-f(x,y)\}] \quad (12)$$

가 된다. 단, $S=A_1(x,y)\exp\{j\pi\phi_1(x,y)\}+A_2(x,y)\exp\{j\pi\phi_2(x,y)\}+A_3(x,y)\times\exp\{j\pi\phi_3(x,y)\}$이다. *는 켤레 복소수를 의미하고 복소 영상의 합이 1을 갖지 않고 어떤 영상으로 남아 있어서

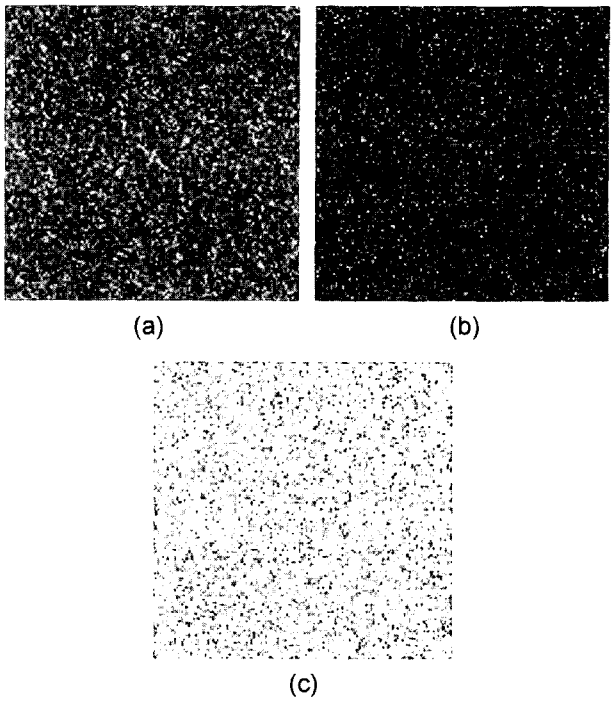

그림 6. 거짓 카드를 사용했을 경우. (a)거짓 카드, (b)재생 영상, (c) 반전 영상.

원 영상을 재생할 수 없음을 알 수 있다. 그림 6은 거짓 카드가 사용되었을 때의 시뮬레이션 결과를 보여 주고 있다.

(2) 카드에 잡음이 섞였을 경우

카드를 사용할 경우 각 카드에 잡음이 섞여질 수도 있는데 이 경우 식을 유도해 보면

$$H(u,v)=\{H_1(u,v)+N_1(u,v)\}+\{H_2(u,v)+N_2(u,v)\}+\{H_1(u,v)+N_3(u,v)\}+\{H_4(u,v)+N_4(u,v)\}=H_1(u,v)+H_2(u,v)+H_3(u,v)+H_4(u,v)+N(u,v) \quad (13)$$

와 같다. 여기서 $N(u,v)=N_1(u,v)+N_2(u,v)+N_3(u,v)+N_4(u,v)$이다. 역 푸리에 변환되어 위상 키 카드가 곱해지면

$$h(x,y)=\exp\{j\pi\ r_2(x,y)\}=[A_1(x,y)\exp\{j\pi\phi_1(x,y)\}+A_2(x,y)\exp\{j\pi\phi_2(x,y)\}+A_3(x,y)\exp\{j\pi\phi_3(x,y)\}+A_4(x,y)\exp\{j\pi\phi_4(x,y)\}]\times\exp\{j\pi f(x,y)\}+n(x,y)exp\{j\pi r_2(x,y)\}=\exp\{j\pi f(x,y)\}+n(x,y)\exp\{j\pi r_2(x,y)\} \quad (15)$$

와 같고 $n(x,y)=\mathcal{F}^{-1}[N(u,v)]$이다. 최종 세기를 구하면

$$I(x,y)=\left|1+h(x,y)\exp\{j\pi\ r_2(x,y)\}\right|^2=\left|1+\exp\{j\pi f(x,y)\}+n(x,y)\exp\{j\pi r_2(x,y)\}\right|^2=2+|n(x,y)|^2+2\cos\{\pi f(x,y)\}+n(x,y)\exp\{j\pi r_2(x,y)\}+n^*(x,y)\exp\{-j\pi r_2(x,y)\}+n^*(x,y)\times\exp[j\pi\{f(x,y)-r_2(x,y)\}]+n(x,y)\exp[j\pi\{r_2(x,y)-f(x,y)\}] \quad (15)$$

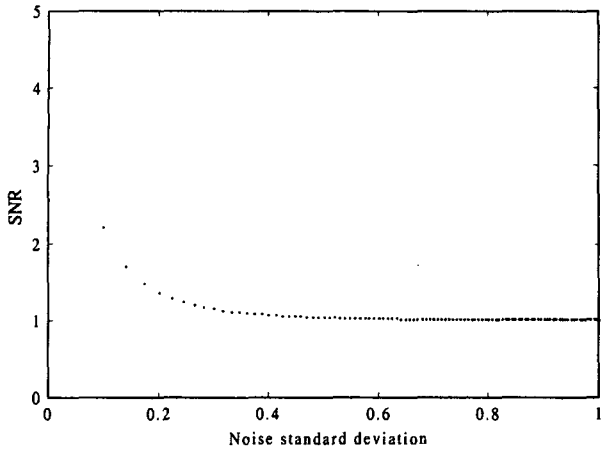

그림 7. 백색 가우스 잡음이 첨가 되었을 경우의 신호 대 잡음비.

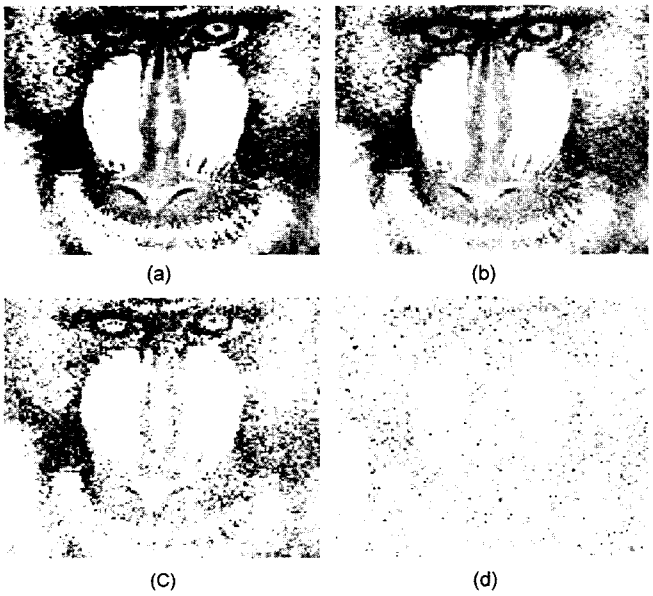

그림 8. 표준편차에 따른 재생 영상. (a) $\sigma=0.02$, (b) $\sigma=0.05$, (c) $\sigma=0.1$, (d) $\sigma=0.3$.

와 같다. 신호 대 잡음비(Signal-to-Noise Ratio)를 구해 보았다. 잡음은 평균이 0이고 표준편차가 σ인 백색 가우스 잡음을 사용하였고 $M\times N$의 영상인 경우 신호 대 잡음비의 식은 다음의 수식을 사용하였다.

$$\mathrm{SNR}=\sqrt{\frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}|I(x,y)|^2}{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}|I(x,y)-I(x,y)|^2}} \tag{16}$$

그림 7는 카드에 백색 가우스 잡음이 섞인 경우의 신호 대 잡음비를 보여 주고 있다. 가우스 잡음의 표준편차에 따른 SNR의 변화는 $\sigma=0.02$일 때 10.14, $\sigma=0.05$일 때 4.10, $\sigma=0.1$일 때 2.213, $\sigma=0.3$일 때 1.15로 σ가 커질수록 급격하게 떨어짐을 알 수 있다. σ가 0.3 이하의 경우는 육안으로 식별하기가 어려웠다. 그림 8는 SNR에 따른 재생영상의 반전 영상을 보여 주고 있다.

VI. 결 론

위상변조만을 이용하는 기존의 광 암호화 시스템의 경우에는 암호화된 영상의 위상정보를 추출 당하면 원 영상이 드러날 수 있는 위험이 있다.이러한 위험을 줄이기 위해 본 논문에서는.시각 암호화 방법과 가상 위상 영상을 이용하여 영상을 암호화하고 Mach-Zehnder 간섭계와 세기 검출기를 이용하여 원 영상을 재생하는 방법을 제안하였다. 원 영상은 가상영상들을 가지고 분리하고 위상변조한 다음 합이 1이 되는 복소 영상들을 각각 곱해 주어 푸리에 변환함으로써 암호화를 하게 된다. 복호는 암호화된 카드들이 Mach-Zehnder 간섭계의 각 경로에 올려져 합을 이루고 푸리에 변환된 후 위상 키 카드와 곱해져서 수행되며, 복원된 영상은 최종적으로 CCD를 통해 세기패턴으로 구한다. 암호화된 카드는 가상 위상 영상들과 복소 영상의 푸리에 변환만이 존재하기 때문에 원 영상에 대한 정보를 갖고 있지 않다. 원 영상은 분리되어 위상성분으로 존재하지만 원 영상의 복원이 가능함을 수식적으로 증명하였고 컴퓨터 시뮬레이션을 통하여 확인하였다. 또한 거짓카드를 사용할 경우 영상재생이 불가능하고 백색 가우스 잡음이 섞여 있는 경우 SNR을 살펴봄으로써 이 시스템의 잡음정도를 알 수 있다. 광학적 실험을 수행할 경우 암호화된 복소 카드들의 정보를 재생하는 있는 광학적 소자가 필요하다. 일반적으로 복소 정보는 두 개의 SLM(spatial light modulator)을 적절히 이용하여 표현할 수 있으나, 현재의 SLM의 기술적 한계로 인해 위상값을 원하는 값으로 조절하는데 어려움이 있어 복소 영상을 표현하는 면에서 광학적 실험의 한계가 있다. 복소 영상값을 정확히 재생할 수 있는 SLM이나 광학소자가 개발된다면, 광학적 실험이 가능할 것이다.

제안한 시스템은 모든 카드들이 한 곳에 모여야 복호가 가능하므로, 정보의 공동소유 및 정보보호 분야에 적용할 수 있다.

참고문헌

[1] B. Javidi and J. L. Honor, "Optical pattern recognition for validation and security verification," *Opt. Eng.*, vol. 33, no. 6, pp. 1752-176, 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] F. T. S. Yu, S. Jutamulia, and D. A. Gergory, "Real-time liquid TV XOR- and XNOR-gate binary image subtraction technique," *Appl. Opt.*, vol. 26, no. 14, pp. 2738-2742, 1987.

[4] J. Rodolfo, H. Rajbenbach, and J. Huignard, "Performance of a photorefractive joint transform correlator for fingerprint identification," *Opt. Eng.*, vol. 34, no. 4, pp. 1166-1171, 1995.

[5] J. Y. Kim, S. J. Park, C. S. Kim, J. G. Bae, and S. J. Kim,

"Optical image encryption using interferometry-based phase mask," *Elec. Lett.*, vol. 36, pp. 874-875, 2000.
[6] P. Stepien, R. Gajda, and T. Szoplik, "Distributed kinoforms in optical security applications," *Opt. Eng.*, vol. 35, no. 9, pp. 2453-2458, 1996.
[7] L. G. Neto, "Implementation of image encryption using the phase-contrast technique," *Proc. SPIE.*, vol. 3386, pp. 284-290, 1998.
[8] D. H. Seo and S. J. Kim, "Image encrypiton using phase-based virtual image and interferometer," *JOSK*, vol. 6, no. 4, pp. 156-160, 2002.
[9] A. Shamir, "How to share a secret," *Comm. of ACM*, vol. 22, pp. 612-613, 1979.
[10] M. Naor and A. Shamir, "Visual cryptography," *Advanced in Cryptography Eurocrypt94*, vol. 950, no. 7, pp. 1-12, 1995.
[11] D. H. Seo and S. J. Kim, "Shift-tolerance property of optical security system using phase-based virtual Image," *Opt. Rev.*, vol. 10, no. 4, pp 1-4, 2003.

Optical encryption system using visual cryptography and virtual phase images

In-Sik Kim, Dong-Hoan Seo†, Chang-Mok Shin, Kyu-Bo Cho, and Soo-Joong Kim
School of Electrical Engineering & Computer Science, Kyungpook National University, Daegu 702-701, KOREA
†*E-mail: dhseo@palgong.knu.ac.kr*

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

(Received August 12, 2003, Revised manuscript November 10, 2003)

We propose an encryption method using visual cryptography and virtual phase images. In the encryption process, the original image is shared by virtual images and the decryption key image. We multiply the virtual phase images with each complex image, which has the constant value of its sum after performing the phase modulation of the virtual images and the decryption key. The encryption cards are made by Fourier transforming the multiplied images. It is possible to protect information about the original image because the cards do not have any information from the original image. To reconstruct the original image, all the encryption cards are placed on each path of a Mach-Zehnder interferometer and then the lights passing through them are summed. Since the summed image is inverse Fourier transformed by a Fourier lens, the phase image is multiplied with the decryption key and the output image is obtained in the form of intensity on the CCD plane. Computer simulations show a good performance of the proposed optical security system.

OCIS Codes : 100.1160, 120.3180, 120.5060.