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

무작위 분할 영상과 결합변환 광 상관기를 이용한 암호화 시스템

최상규 · 서동환† · 신창목 · 김수중

경북대학교 전자전기컴퓨터학부

㉾ 701-702 대구광역시 북구 산격동 1370

배장근

구미 1대학 전자정보과

㉾ 730-711 경북 구미시 부곡동 407

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

본 논문에서는 키 영상과 암호화 영상의 암호화 수준을 동등하게 하기 위해서 분할 영상을 제작하여 결합변환 상관기의 주파수 영역을 이용한 광 암호화 시스템을 제안하였다. 제안한 암호화 과정은 원 영상의 반조 영상을 만들고 이를 시각 암호화를 이용하여 두 개로 나누어 분할 영상으로 만든다. 두 개의 분할 영상 각각 위상변조 한 후 위상변조된 무작위 영상을 곱하고, 이들을 각각 푸리에 변환하여 두 개의 최종 암호화 영상을 얻는다. 그 두 암호화 영상 중에 하나를 복호화 키로 사용하여 진위 여부를 판별하게 된다. 제안한 방법에 의해 제작된 암호화 영상은 1차로 시각 암호화를 이용하여 암호화시키고 2차로 위상변조된 무작위 영상을 곱해서 암호화하므로 복제와 위조를 통한 위상정보의 유출에도 원 영상의 복원을 막을 수 있으며, 원 영상 재생에 결합변환 상관기의 주파수 영역을 이용하기 때문에 시스템 구성이 간단하며 두 암호화 영상 중에 특정한 영상을 복호화 키로 쓰지 않아도 된다. 본 논문에서는 컴퓨터 모의 실험을 통해 제안한 방법의 타당성을 확인하였으며 잡음에 대한 영향을 분석하였다.

주제어 : Phase encoding, Random divided image, Joint transform correlator.

I. 서 론

현대 사회는 정보를 기반으로 하는 산업의 발전으로 개인의 정보와 신용이 더욱 더 중요시되고 여권, 신용카드, 은행카드 등의 개인 신분증의 사용이 늘어나고 있다. 그러나 컴퓨터 관련 장비들과 소프트웨어 기술의 발달로 인해 화폐뿐만 아니라 여러 이미지 패턴들의 복제가 쉽게 이루어지고 있으며, 위조 기술이 고도화되고 완벽해짐에 따라 어떠한 경우에도 개인 정보보호뿐만 아니라 위조나 복제를 근본적으로 차단할 수 있는 새로운 접근 방법에 관한 연구가 이루어지고 있다. 이러한 연구들 중에서 광을 이용한 암호화 시스템들이 많이 제안되고 있다. 광 암호화 시스템은 광의 고속성과 병렬성을 이용할 수 있어서, 고속으로 대용량의 정보를 처리하는데 적합하다. 또한 기존의 디지털 영상처리 시스템들은 영상 신호의 명암 즉 세기를 검출해서 대량 복제와 위조가 가능한 반면에 광 암호화 시스템은 영상 신호를 위상 정보로 기록할 수 있기 때문에 인간의 시각이나 세기 검출기로는 위조가 불가능한 장점을 가지고 있다. 그래서 최근에는 위상정보를 이용한 광 암호화 시스템이 많이 제안되고 있다.[1-6]

본 논문에서는 복호화 키와 암호화 영상의 수준을 동등하게 하기 위해서 분할 영상을 제작하여 결합변환 상관기의 주파수 영역에서의 광 암호화 시스템을 제안하였다. 제안한 방법에서는 원 영상을 시각 암호화(visual cryptography)를 이용하여 두 부분으로 분할하여 암호화하는 방법에 적용하였다. 또 반조 영상을 사용하여 그레이 레벨을 가지는 원 영상의 해상도와 유사하게 하여 이진 영상에만 적용되던 암호화를 그레이 영상에도 적용이 가능하게 하였으며, 키로 사용된 무작위 영상을 해독당하더라도 원 영상의 분할 영상만이 재생되므로 정보 유출을 막을 수 있게 하였다. 암호화 과정은 원 영상의 반조 영상을 만들고 이를 시각 암호화를 이용하여 두 개로 나누어 분할 영상으로 만든다. 두 개의 분할 영상 각각 위상변조한 후 위상변조된 무작위 영상을 곱하고, 이들을 각각 푸리에 변환하여 두 개의 최종 암호화 영상을 얻는다. 제안한 방법에 의해 제작된 암호화 영상은 1차로 시각 암호화를 이용하여 암호화시키고 2차로 위상변조된 무작위 영상을 곱해서 암호화하여 복제와 위조를 통한 위상정보의 유출에도 원 영상의 복원을 막을 수 있게 하였다. 또 결합변환 상관기의 주파수 영역을 이용하기 때문에 시스템 구성이 간단하며 두 암호화 영상 중에 특정한 영상을 복호화 키로 쓰지 않아도 된다. 본 논문에서는 컴퓨터 모의 실험 및 이에 대한 고찰을 통해 제안한 방법의 타당성을 확인하였으며 잡음에 대한 영향을 분석하였다.

II. 시각 암호화와 결합변환 상관기

2.1. 시각 암호화

Shamir는 접근 권한이 동등한 회원으로 구성된 그룹에 적용하기 위한 평등한 비밀 분산법인 임계치 방법(thresholding scheme)[7]과 그 응용 형태인 시각 암호화[8]를 제안하였다. 근

†E-mail: dhseo@palgong.knu.ac.kr

본적인 시각 암호화는 두 장의 투명한 용지에 원 영상을 분산하여 구성하는 것으로 간단히 구현할 수 있다. 이때 한 장을 암호 영상으로 선택하면 나머지 한 장이 키 영상이 된다. 복호는 더욱 간단하다. 암호 영상과 키 영상을 중첩시키면 원 영상이 나타난다. 이와 같이 시각 암호화는 별도의 복호 알고리듬을 수행하지 않고 단순히 인간의 시각으로 복호할 수 있으므로 암호에 대한 지식이나 이를 수행하기 위한 장치 없이도 간단히 사용할 수 있는 장점이 있다. 그러나 영상을 암호화하기 위해 원 영상을 이루는 화소들을 각각 여러 개의 부화소(subpixels)로 나누어야 하며 이로 인해 복호화된 영상의 해상도가 저하된다.

2.2. 결합변환 상관기

결합변환 상관기[9]는 광축정렬 문제를 해결할 수 있는 광 상관 시스템이며 이는 입력영상과 기준영상을 결합변환 상관기의 결합입력평면에 동시에 올리기 때문에 가능하다. 결합변환 상관기의 시스템 구성도는 그림 1과 같다. 그림 1에서 공간광 변조기(spatial light modulator; SLM)는 입력영상이 올라가는 결합입력평면을, L은 푸리에 변환렌즈를, P는 출력평면을 나타내며, f는 렌즈의 초점거리이다. 또한 $r(x, y)$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 L에 의해서 푸리에 변환되는데 이는

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

와 같이 표현되고, 출력평면 P에 놓인 세기 검출기(intensity detector)에 나타나는 출력단의 광세기 함수의 결합 파워스펙트럼(joint power spectrum)은

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

와 같이 표현된다. 식 (2)와 (3)에서 나타나는 위상 성분은 입력영상과 기준영상의 중심이 결합입력평면에서는 원래의 중심에 비해 $\pm x_0$만큼 이동하였기 때문에 나타나는 위상 성분이다. CCD로 검출된 광 세기 함수는 컴퓨터를 통하여 다시 공간광 변조기로 올려지게 되며, 렌즈 L에 의해서 역푸리에 변환된다. 이때 출력상관평면에서의 광 분포함수는

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

와 같다. 여기서 ★는 상관자(correlation)를, *는 상승자(convolution)를 뜻한다. 식 (4)의 앞의 두 항은 각각의 입력영상의 자기상관 성분이며, 뒤의 두 항은 각 입력영상간의 상호상관 성분이다. 결합변환 상관기는 4-f 광 상관기 구조[9]의 광축정렬 문제를 해결할 수 있으며 외부교란이나 진동에도 강한

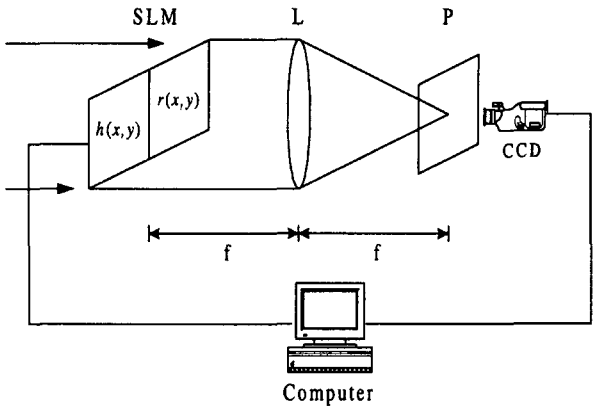

그림 1. 전통적인 결합변환 상관기.

구조를 지니며 간단한 구조를 가지고 있다. 또한 현재 널리 사용되는 공간 광 변조기 등의 광학적 장비 또는 디지털 장비와도 직접적인 결합이 용이하므로 실시간 처리에 보다 적합하다.

III. 제안한 암호화 및 복호화 방법

3.1. 무작위 분할 영상을 이용한 암호화

암호화 과정은 먼저 암호화할 원 영상의 반조 영상을 구한 후 이를 시각 암호화를 이용하여 두 부분으로 분할하게 된다. 여기에서는 위상 성분을 이용하여 암호화하기 때문에 두 영상의 화소를 XOR의 관계를 가지도록 분할하면 된다. 그리고 반조 영상은 이진 영상이므로 분할 영상들 또한 이진 영상이 된다. 이때 원 영상의 반조 영상을 $f(x, y)$라 두고 분할된 두 개의 영상을 각각 $f_1(x, y)$, $f_2(x, y)$라 한다면

$$f(x, y) = f_1(x, y) \oplus f_2(x, y) \tag{5}$$

와 같다. 단 ⊕는 XOR 연산이다. 그 다음으로는 두 분할 영상 $f_1(x, y)$, $f_2(x, y)$, 그리고 암호화하기 위해 컴퓨터에서 발생한 무작위 영상 $r(x, y)$를 위상변조한다. 위상변조된 각각의 영상 $f_{p1}(x, y)$, $f_{p2}(x, y)$, $r_p(x, y)$,는

$$\begin{aligned}f_{p1}(x, y) &= \exp[j\pi f_1(x, y)] \\ f_{p2}(x, y) &= \exp[j\pi f_2(x, y)] \\ f_p(x, y) &= \exp[j2\pi r(x, y)]\end{aligned} \tag{6}$$

와 같이 표현된다. 여기서 위상 변조된 분할 영상과 무작위 영상의 세기는 1이므로 $|f_{p1}(x, y)|^2 = |f_{p2}(x, y)|^2 = |r_p(x, y)|^2 = 1$이다. 위상변조된 분할 영상 $f_{p1}(x, y)$, $f_{p2}(x, y)$를 위상변조된 무작위 영상 $r_p(x, y)$와 각각 곱한 암호화 영상을 $e_1(x, y)$, $e_2(x, y)$라 두면

$$\begin{aligned}e_1(x, y) &= f_{p1}(x, y)\, r_p(x, y) = \exp[j\pi\{f_1(x, y) + 2r(x, y)\}] \\ e_2(x, y) &= f_{p2}(x, y)\, r_p(x, y) = \exp[j\pi\{f_2(x, y) + 2r(x, y)\}]\end{aligned} \tag{7}$$

와 같다. 이때 암호화된 위상영상 $e_1(x, y)$과 $e_2(x, y)$를 각각 푸리에 변환한 영상을 $E_1(u, v)$, $E_2(u, v)$라 두면

$$\begin{aligned}E_1(u, v) &= \Im\{e_1(x, y)\} \\ E_2(u, v) &= \Im\{e_2(x, y)\}\end{aligned} \tag{8}$$

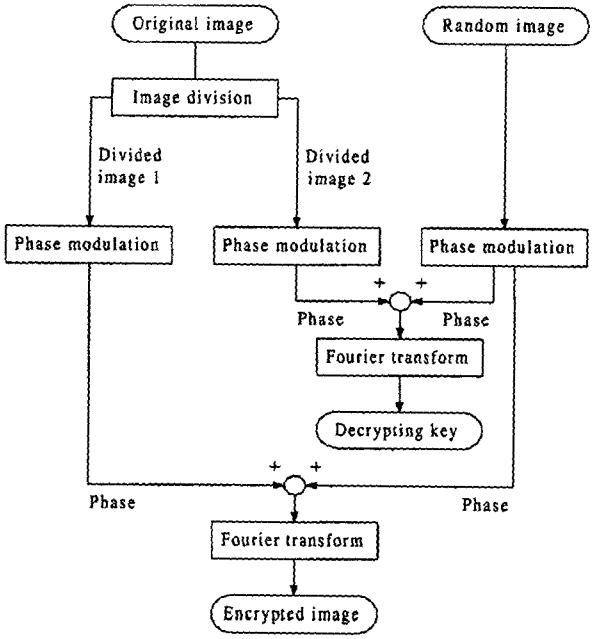

그림 2. 암호화 과정의 블록선도.

와 같다. 본 논문에서는 $E_1(u, v)$을 최종 암호화된 영상으로 사용하고 $E_2(u, v)$를 원 영상을 복원하기 위한 복호화 키로 사용하게 된다. 제안한 암호화 과정을 그림 4에 블록선도로 나타내었다.

3.2. 결합변환 상관기를 이용한 복호화

제안한 복호화 시스템은 그림 3과 같다. 암호화된 영상 $E_1(u, v)$는 그림 3의 결합입력평면의 우반 평면에, 복호화 키 $E_2(u, v)$는 좌반 평면에 놓여진다. 본 논문에서 암호화된 영상과 복호화 키 영상은 주파수 영역이고 각각의 영상들이 결합입력평면에 나란히 놓여지게 되므로 원래의 중심에 대해서 $(\pm u_0, 0)$만큼 이동하게 된다. 따라서 결합입력평면 $E(u, v)$는

$$E(u, v) = E_1(u - u_0, v) + E_2(u + u_0, v) \tag{9}$$

와 같고 결합입력평면은 렌즈 L에 의하여 역푸리에 변환되면

$$e(x, y) = e_1(x, y)\exp(j2\pi u_0 x) + e_2(x, y)\exp(-j2\pi u_0 x) \tag{10}$$

으로 나타난다. 여기서 $\exp(\pm j2\pi u_0 x)$성분은 주파수 영역에서 중심 이동에 의해 생기는 위상 성분을 나타낸다. 출력평면에 놓인 CCD 카메라에 의해서 검출되는 광 세기함수는

$$\begin{aligned}|e(x, y)|^2 &= |e_1(x, y)\exp(j2\pi u_0 x) + e_2(x, y)\exp(-j2\pi u_0 x)|^2 \\ &= |e_1(x, y)^2 + e_2(x, y)|^2 \\ &+ e_1(x, y)\, e_2^*(x, y)\exp(j4\pi u_0 x) \\ &+ e_1^*(x, y)\, e_2(x, y)\exp(-j4\pi u_0 x) \\ &= 2 + \exp[j\pi\{f_1(x, y) - f_2(x, y)\}]\exp(j4\pi u_0 x) \\ &+ \exp[-j\pi\{f_1(x, y) - f_2(x, y)\}]\exp(-j4\pi u_0 x) \\ &= 2 + 2\cos[\pi\{f_1(x, y) - f_2(x, y)\} + 4\pi u_0 x]\end{aligned} \tag{11}$$

와 같다. 여기서 식 (11)에서 재생된 영상에 영향을 미치는 u_0는 결합입력평면의 중심에서 암호화된 영상과 복호화 키 영상의 각각의 중심의 위치를 나타내며 이의 영향이 없다고 가정한다면

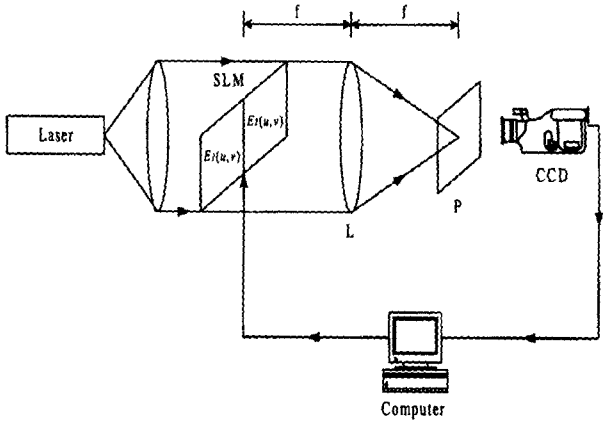

그림 3. 제안한 복호화 시스템.

$$\begin{aligned}|e(x, y)|^2 &= 2 + 2\cos[\pi\{f_1(x, y) - f_2(x, y)\}] \\ &= \begin{cases} 4, & f_1(x, y) - f_2(x, y) = 0 \\ 0, & f_1(x, y) - f_2(x, y) = \pm 1 \end{cases}\end{aligned} \tag{12}$$

와 같이 나타난다. 즉 두 분할 영상의 화소 값이 같을 때는 4가 나오고 다른 화소 값을 가지면 0이 나오게 되므로 XOR 연산을 만족하게 되므로 반조 영상이 여현(cosine) 함수의 형태로 반전된 영상이 복원된다.

3.3. 위상 성분의 영향에 따른 복원된 값의 변화

결합입력평면에 올라가는 두 영상의 중심의 위치인 u_0의 값에 따라 복원된 값이 달라지게 되므로 위상 성분을 고려해야 한다. 표본화된 주파수 영역과 공간 영역의 관계[10]는

$$\begin{aligned}&\Delta d = \frac{1}{2f_{x0}} \\ &x = k\Delta d = k\frac{L}{N_x} \\ &u = k\frac{1}{\Delta d} = k\frac{N_x}{L},\ k = 0, 1, \ldots, N_x - 1\end{aligned} \tag{13}$$

으로 주어지며 편의상 x축과 u축만 표시하였다. 여기서 Δd는 표본화 간격, f_{x0}는 영상의 x축 최고 주파수, L은 x축의 영상 길이, k는 화소번호이며는 표본화 개수이다.

그림 3에서 암호화 영상과 복호화 키의 중심이 $(\pm u_0, 0)$에 있다면 이는 각각의 중심 u_0가 복호화 시스템의 주파수 영역의 결합입력평면의인 지점에 위치하는 것과 같은 의미를 가진다. 식 (13)에서 f_{x0}는 $1/2\Delta d$이므로 암호화 영상과 복호화 영상의 중심좌표 u_0는 $1/4\Delta d$이다. 따라서 식 (13)을 식 (11)에 대입하여 정리하면

$$\begin{aligned}|e(x, y)|^2 &= 2 + 2\cos[\pi\{f_1(x, y) - f_2(x, y)\} + 4\pi u_0 x] \\ &= 2 + 2\cos\left[\pi\{f_1(x, y) - f_2(x, y)\} + 4\pi\left(\frac{1}{4\Delta d}\right)(k_x\Delta d)\right] \\ &= 2 + 2\cos[\pi\{f_1(x, y) - f_2(x, y)\} + \pi k_x] \\ &= \begin{cases} 2 + 2\cos[\pi\{f_1(x, y) - f_2(x, y)\}], & k_x = 2n \\ 2 - 2\cos[\pi\{f_1(x, y) - f_2(x, y)\}], & k_x = 2n + 1 \end{cases}\end{aligned} \tag{14}$$

와 같으며 여기서 n은 정수이고, k_x는 x축으로의 화소 번호이다. 식 (14)에서 결합변환 상관기의 자기상관 성분을 이용하여 복호화 됨을 알 수 있으나 화소번호에 따라 복호화 영상이 달라짐을 알 수 있다. 그러므로 컴퓨터 후처리를 통해 x축 방향으로 홀수화소를 반전시켜 복호화하면 반조 영상의 명암이 반전된 영상이 재생되며 x축 방향으로 짝수화소를 반전시켜 복호화하면 반조 영상이 재생된다.

이 때 시스템 내성적인 측면에서 만약 충분치 못한 크기의 렌즈를 사용하여 결합입력평면을 푸리에 변환할 경우 암호화 영상 및 키 영상의 일부분이 잘려나간 상태로 푸리에 변환된다. 하지만, 암호화 영상과 키 영상의 정보는 주파수 평면상에서 넓게 퍼진(spread spectrum) 상태로 되어있기 때문에 일부분이 잘려나가는 불완전한 역푸리에 변환이 되더라도 잡음이 섞인 원 영상이 재생되는데 이는 결합입력평면에 직각 동공함수(rectangular pupil function)를 곱하여 역푸리에 변환된 형태와 유사하므로 CCD 평면에서는 sinc 함수 성분이 발생하여 복원 영상의 전 배경 영역에 잡음 형태로 영향을 미치게 된다.[11]

IV. 컴퓨터 모의 실험 결과 및 고찰

4.1. 컴퓨터 모의 실험 결과

본 논문에서는 컴퓨터 모의 실험을 수행하기 위해 제작한 영상들을 그림 4에 나타내었다. 그림 4(a)는 원 영상인 256×256 크기를 가지는 'Elaine' 영상이며, 그림 4(b)는 원 영상의 반조 영상이고, 그림 4(c)는 그림 4(b)를 시각 암호화에 의해 분할한 첫 번째 분할 영상이며, 그림 4(d)는 두 번째 분할 영상이며, 그림 4(e)는 분할 영상을 암호화하기 위해 컴퓨터로 생성한 무작위 영상이다. 암호화 영상을 만들기 위해서는 첫 번째 분할 영상과 두 번째 분할 영상은 이진 값이므로 0과 1의 값으로 위상변조하고, 무작위 영상은 0과 1사이의 값으로 정규화(Normalization)시켜 위상변조하고 각각을 서로 곱하여 푸리에 변환한다. 그림 4(f)는 첫 번째 분할 영상을 암호화하여 푸리에 변환한 영상을 나타내며 그림 4(g)는 두 번째 분할 영상을 암호화하여 푸리에 변환한 올바른 복호화 키를 나타내며 그림 4(h)는 컴퓨터로 임의로 만든 거짓 복호화 키이다. 그림 4의 영상을 사용하여 컴퓨터 모의 실험한 결과를 그림 5

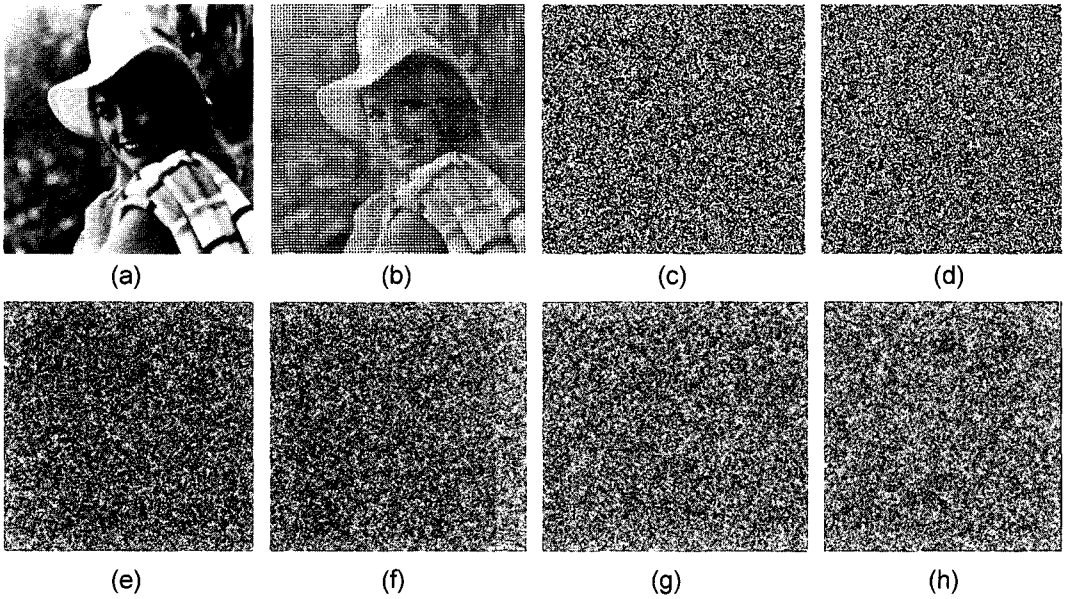

그림 4. 컴퓨터 모의 실험에 사용한 영상 (a) 원 영상, (b) (a)의 반조 영상, (c) (b)의 첫 번째 분할 영상, (d) (b)의 두 번째 분할 영상 (e) 무작위 영상, (f) 암호화된 푸리에 영상, (g) 올바른 푸리에 복호화 키 (h) 잘못된 푸리에 복호화 키.

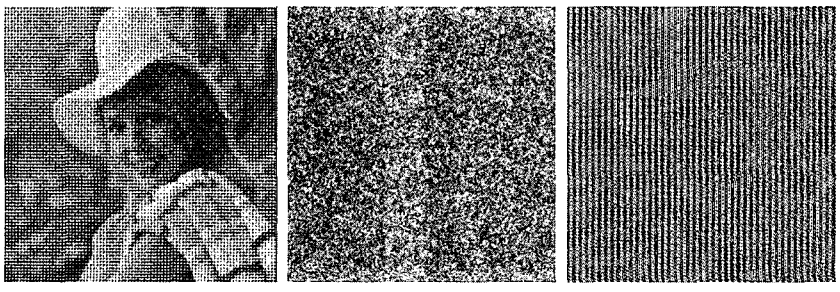

그림 5. 컴퓨터 모의 실험 결과 (a) 그림 4(g)에 의해 복호화된 영상, (b) 그림 4(h)에 의해 복호화된 영상 (c) (a)의 x축으로 짝수 화소를 반전시킨 영상.

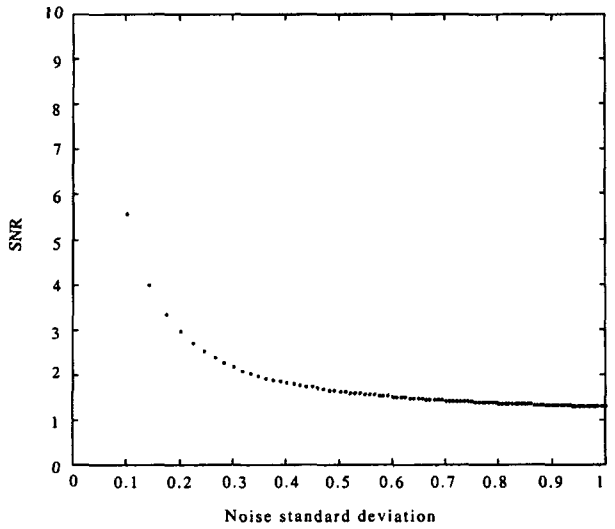

그림 6. 가우스 잡음에 대한 복호화 영상의 신호 대 잡음비.

에 나타내었다. 그림 5(a)는 올바른 키 영상을 사용하여 복호화 한 영상을 나타내며 그림 5(b)는 거짓 키 영상을 사용하여 복호화 한 영상을 나타낸다. 명확하게 거짓 키 영상으로는 원래의 영상을 복원할 수 없음을 확인 할 수 있었다. 또한 올바른 키에 의해 복호화된 영상은 위상성분의 영향이 일정하게 나타나기 때문에 화소값에 따른 줄무늬를 가진 영상이 재생되므로 원 영상과 상이함을 알 수 있다. 따라서 원 영상으로 복원하기 위해서는 위상성분의 영향에 따른 화소값을 적절히 보상해야 하는데, 이를 위해 컴퓨터 후처리를 하였다. 그 방법은 특정 화소를 반전시켜 복호화한 것이며 이를 그림 5(c)에 나타내었으며 이는 위상성분의 영향을 받은 x축으로 짝수 화소를 반전시킨 영상으로 원래의 영상과 같음을 알 수 있다. 그러므로 제안한 방법을 이용하여 복호화된 영상은 컴퓨터 후처리를 통하여 원래의 영상이 정확히 재생됨을 알 수 있다. 따라서 본 논문에서 제안한 방법은 반조 영상을 사용하여 복호화하므로 이진 영상이지만 그레이 영상의 효과를 가질 수 있도록 복원이 가능함을 알 수 있다.

4.2. 잡음의 영향에 대한 고찰

실제로 암호화 영상과 복호화 키 제작을 위해 광학적 리소그라피(lithography)를 이용하여 제작시 위상 마스크 두께에 따른 잡음이 발생할 수 있다. 따라서 암호화된 푸리에 영상이나 푸리에 복호화 키에 잡음이 발생되었을 때 복호화 영상의 신호 대 잡음비(signal-to-noise ratio; SNR)를 살펴볼 필요가 있다. 만일 복호화 키에 잡음이 섞인 경우를 가정한다면

$$E(u,v)=E_1(u-u_0,v)+E_2(u+u_0,v)+N(u+u_0,v) \tag{15}$$

와 같다. 단 $N(u,v)$는 평균이 0이고 표준편차가 σ인 가우스 잡음이다. 역푸리에 변환하여 CCD에 검출되는 성분은

$$\begin{aligned}|e(x,y)|^2 &=2+n(x,y)^2+\cos[\pi\{f_1(x,y)-f_2(x,y)\}+4\pi u_0 x]\\ &+n^*(x,y)\exp[j\pi\{f_1(x,y)+2r(x,y)\}]\exp(j4\pi u_0 x)\\ &+n(x,y)\exp[-j\pi\{f_1(x,y)+2r(x,y)\}]\exp(-j4\pi u_0 x)\\ &+n^*(x,y)\exp[j\pi\{f_2(x,y)+2r(x,y)\}]\\ &+n(x,y)\exp[-j\pi\{f_2(x,y)+2r(x,y)\}]\end{aligned} \tag{16}$$

와 같으며 $n(x,y)=\mathfrak{I}^{-1}\{N(u,v)\}$ 이다. 여기서는 복호화 영상의 신호 대 잡음비를 구하였다. 잡음이 없을 때의 복호화 영상을 $I(x,y)$라고 하고 잡음이 존재 할 때의 복호화 영상을 $I'(x,y)$라고 할 때 두 영상의 평균 제곱(mean square) 신호 대 잡음비를 사용하였다. 두 영상의 크기가 $M\times N$일 때 복호화 영상의 신호 대 잡음비는

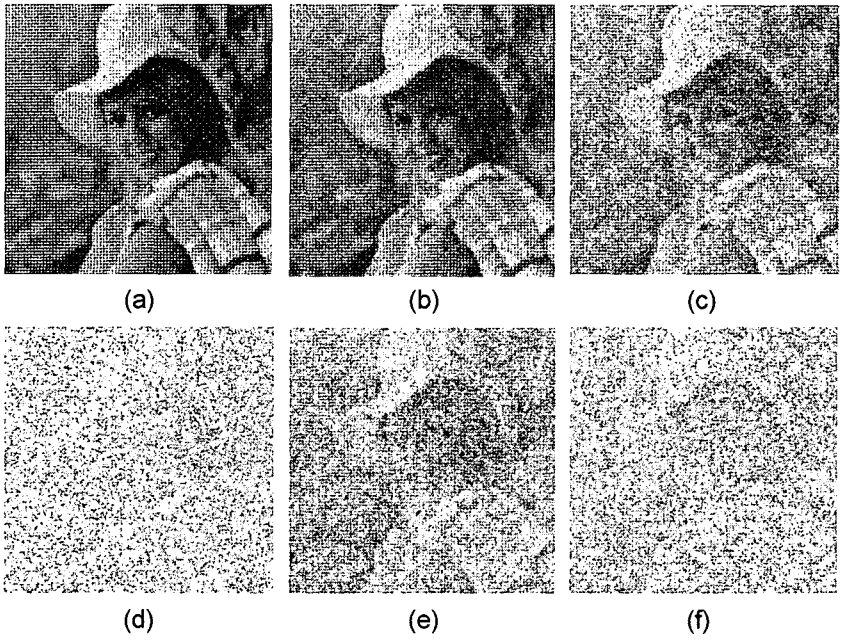

그림 7. 가우스 잡음의 표준편차에 따른 복호화 영상 (a) $\sigma=0.1$, (b) $\sigma=0.2$, (c) $\sigma=0.3$, (d) $\sigma=0.4$, (e) $\sigma=0.5$, (f) $\sigma=0.6$.

$$SNR=\left\{\frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}I'(x,y)^2}{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[I'(x,y)-I(x,y)]^2}\right\}^{\frac{1}{2}} \quad (17)$$

과 같다.

그림 6은 식 (17)을 이용하여 복호화된 영상에 가우스 잡음이 첨가되었을 때 잡음의 표준편차에 따른 신호 대 잡음비를 나타내었다. 가우스 잡음의 표준편차가 커지면 잡음이 영상에 넓은 범위로 영향을 끼치게 되므로 결과가 좋지 않다. 그러므로 가우스 잡음의 표준편차가 커질수록 결합변환 상관기를 이용하여 복호화된 영상의 신호 대 잡음비가 점점 떨어짐을 알 수 있다. 그림 7은 복호화 키에 가우스 잡음이 들어갔을 때 잡음의 표준편차에 따른 제안한 시스템에 의해 복호화된 영상을 나타내었다. 신호 대 잡음비가 2보다 클 때를 나타낸 가우스 잡음의 표준편차가 0.3까지의 경우인 그림 7(a), 그림 7(b), 그림 7(c)를 살펴보면 복호화 영상을 식별하는 것이 쉬우나, 신호 대 잡음비가 2보다 작을 때를 나타낸 표준편차가 0.4보다 큰 경우인 그림 7(d), 그림 7(e), 그림 7(f)를 살펴보면 복호화 영상을 식별하기 어려움을 알 수 있다.

V. 결 론

본 논문에서는 원 영상의 반조 영상을 만든 후 이를 시각 암호화를 이용하여 두 개의 분할 영상으로 나누고 각각 위상변조한 후 위상변조된 무작위 영상을 곱하여 암호화한 후에 푸리에 변환을 거쳐 결합변환 상관기의 결합입력평면에 올려서 역푸리에 변환을 하여 영상을 복원하는 방법을 제안하였다. 그리고 이를 수행하기 위해 컴퓨터 모의 실험을 하여 결과를 얻었다. 본 논문은 기존의 방법과 비교할 때 원 영상의 분할 영상을 사용하므로 암호화에 사용한 무작위 성분을 알더라도 원 영상이 가진 정보를 알 수 없게 하였으며 암호화된 영상과 복호화 키 각각에 원 영상의 정보를 모두 포함하지 않으므로 키가 고정적이지 않다는 장점을 가지게 되며 반조 영상을 도입하여 그레이 레벨의 영상에 대해서도 구현이 가능하게 하였다. 앞으로 광학 장비의 성능이 개선되고 다중위상을 정확히 표현할 수 있는 공간 광 변조기와 광 식각 기술이 더 발전한다면 정보 보호 시스템과 광학적 인증 시스템에 실질적으로 활용할 수 있을 것이다.

참고문헌

[1] 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.

[2] L. G. Neto, "Optical implementation of image encryption using random phase encoding," *Opt. Eng.*, vol. 35, no. 9, pp. 2459-2463, 1996.

[3] J. Y. Kim, S. J. Park, C. S. Kim, J. G. Bae, and S. J. Kim, "Optical image encryption using interferometry-based phase masks," *Elec. Lett.*, vol. 36, no. 10, pp. 874-875, 2000.

[4] R. K. Wang, I. A. Watson, and C. Chatwin, "Random phase encoding for optical security," *Opt. Eng.*, vol. 35, no. 9, pp. 2464-2469, 1996.

[5] 박세준, "결합변환 상관기의 여현 위상특성을 이용한 광 암호화 방법," 경북대학교 박사학위 논문, 2001.

[6] 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.

[7] A. Shamir, "How to share a secret," *Comm. of ACM*, vol. 22, pp. 612-613, 1979.

[8] M. Naor and A. Shamir, "Visual cryptography," *Advanced in Cryptography Eurocrypt 94*, vol. 950, no. 7, pp. 1-12, 1995.

[9] J. W. Goodman, Introduction to Fourier Optics, (McGraw-Hill, San Francisco, USA, 2nd edition, 1996), Chapter 8.

[10] S. J. Park, J. Y. Kim, J. K. Bae, and S. J. Kim, "Fourier-plane encryption technique based on removing the effect of phase terms in a joint transform correlator," *Opt. Rev.*, vol. 8, no. 6, pp. 413-415, 2001.

[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 random divided image and joint transform correlator

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

Jang-Keun Bae
School of Electronic information, Kumi college, Kyungpook 730-711, KOREA

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

We proposed the optical system using two divided halftone images to hide the original image and a joint transform correlator. The encryption procedure is performed by the Fourier transform of the product of each divided image by visual cryptography and the same random image which is generated by computer processing. As a result, we can obtain two Fourier divided images which are used as the encrypted image and the decrypting key, respectively. In the decryption procedure, both the encrypted image and the decrypting key are located on the joint input plane. Then the original image is reconstructed on a CCD camera which is located in the output plane. An autocorrelation term of joint transform correlator contributes to decrypt the original image. To demonstrate the efficiency of the proposed system, computer simulations and noise analysis are performed. The result show that the proposed system is a very useful optical certification system.

OCIS Codes : 100.1160, 120.3180, 120.5060.