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

위상 변조 Exclusive-OR 연산을 이용한 광학적 암호화 방법

신창목† · 서동환 · 김수중
경북대학교 전자전기컴퓨터학부
㉾ 701-702 대구광역시 북구 산격동 1370

(2003년 6월 18일 받음, 2003년 10월 17일 수정본 받음)

본 논문에서는 XOR 연산을 위상 변조하여 만든 위상 변조 XOR(phase-encoded exclusive-OR) 연산이라는 개념을 기본으로 그레이 영상을 암호화 한 새로운 광 암호화 방법을 제안하였다. 그레이 원 영상을 이진 영상들의 합으로 분리한 후 각각의 이진 영상들을 이진 무작위 영상들과 위상변조 XOR 연산 방법을 이용해 암호화하고, 이를 위상 변조하여 암호화된 데이터를 만들었다. 그리고 복호화에 필요한 키 데이터는 암호화 시 사용한 무작위 이진 영상들로 만든 무작위 그레이 영상을 위상 변조하여 구하였다. 암호화된 데이터는 위상 변조로 인한 비선형성과 비가시적 특성을 가지므로 기본적으로 높은 정보보호의 특성이 있으나, 여기에 위상정보 자체를 암호화함으로써 보다 높은 수준의 정보 보호를 가능하게 하였다. 또한, 복호화 과정은 암호화 데이터와 키 데이터의 단순 곱과 기준파와 간섭을 이용하므로, 원 영상 복원 시 간단한 위상 시각화 시스템(phase-visualization system)으로 구현할 수 있다. 컴퓨터 시뮬레이션을 통해 제안한 방법의 구현 가능성과 타당성을 확인하였다.

주제어 : optical encryption, interferometer, random phase.

I. 서 론

최근에 광의 병렬성에 따른 빠른 처리 특성을 이용한 광학적 암호화 이론[1-7]들이 주목되고 있다. 그 결과 여러 가지 광학적 암호화 방법들이 제안되어 왔으며 대표적인 예로 4-f 광상관기(correlator)나 간섭계(interferometer) 구조를 이용해 원 영상을 백색잡음 형태를 가지는 복소 영상으로 암호화한 후 동일한 시스템으로 복호화하는 방법들이 있다.[1,2] 이러한 암호화방법은 암호화하고자 하는 정보의 종류에 따라 즉, 원 영상의 세기 정보를 바로 암호화하는 크기 기반 암호화 방법(amplitude-based encryption)[1]과 세기정보를 위상정보로 변조한 후 암호화하는 위상 기반 암호화 방법(phase-based encryption)[2]으로 나눌 수 있다. 위상 기반 암호화 방법은 크기 기반 암호화 방법에 비해 잡음에 영향을 덜 받으며, 위상 변조된 정보의 비 선형적 위상함수 특성에 의해 더 높은 암호화 수준을 가지며, 또한 위상 성분만을 암호화에 사용함으로 기록이나 저장이 더욱 쉽고 간단하다.[2] 이상적인 경우 위상정보는 보이지 않는 특성에 의해 일반 세기 검출기로 복사를 하거나 해석할 수 없지만, 간섭 방법(interferometric technique)이나 일반적인 위상 세기 방법(generalized phase contrast technique)[6]등을 적용하면 암호화된 위상 정보를 유추하거나 추출해낼 수 있다. 그러므로, 불법 사용자가 위상정보를 추출하여도 해석하기 힘들도록 위상 정보를 암호화 할 필요가 있으며, 복호화는 키 정보를 소유한 자에 의해 간단하게 복호화되어야 한다.

광 암호화에 사용되는 방법 중에서 XOR연산을 이용한 방법[3,4]이 있으며, 크기 기반 암호화 방법이라 할 수 있는 Han 등[3]이 제안한 방법과 위상 기반 암호화 방법이라 할 수 있는 Kim등[4]이 제안한 방법이 있다. Han등은 LCD(Liquid crystal device)와 LA(lenslet arrary)에 의한 편광(polarization)을 이용하여 그레이 영상을 이진수의 비트 수만큼 나눈 이진 영상들을 XOR 연산 암호화함으로써 암호화된 이진 정보를 가진 각 사용자에 대한 인증이 가능한 방법을 제안하였다. 위 방법으로 암호화 수행 시 암호화된 8개의 이진 영상들은 각각 암호화 키에 의해 광학적으로 구해지지만, 암호화된 그레이 영상은 이진 영상들을 디지털적으로 후처리해야만 구해진다. 이 때 암호화된 그레이 영상은 다시 8개의 암호화된 이진 영상으로 쉽게 나누어지므로, 불법 사용자가 각각의 암호화된 이진 영상을 통해 원 영상의 정보를 추정하거나 접근할 수 있다. 또한 복호화 과정에서 최종 그레이 영상을 얻기 위해서 복호화된 이진 영상을 합치는 디지털 후처리 과정이 필요하다. Kim 등은 두 이진 위상 영상간의 광학적 간섭을 이용한 XOR 암호화 방법을 제안하였는데, 이 방법은 구현이 간단하지만, 이진 위상간의 간섭을 이용하므로 그레이 영상의 암호화에는 한계점을 가지고 있다.

본 논문에서는 그레이 원 영상에 대해 디지털적인 phase-encoded XOR 연산기반의 암호화 방법을 제안하여 암호화 영상을 만들고 이를 위상 부호화 하여 광학적 복호화 시스템으로 원 영상을 복원할 수 있는 광학적 위상 암호화 영상과 키 영상을 구현하였다.

그레이 영상을 이진 영상들의 합으로 분리한 후 각각의 이진 영상들을 위상 변조된 임의의 이진 영상들과 위상 변조 XOR 연산을 이용해 암호화하고, 원 영상 복원에 필요한 그레이 값들을 곱하여 각각 더함으로써 암호화 영상과 키 영상을 만들고, 두 영상들을 다시 한번 위상 변조시켜 암호화 데이터와 키 데이터를 만드는 암호화 방법을 제안하였다. 제안한 방법은 암호화 데이터가 무작위 위상정보를 가지도록 암호화함

†E-mail: neo_minstrel@daum.net

으로써 단순한 위상정보의 추출만으로 원 영상 정보가 유출되지 않도록 하여 높은 암호화 수준이 되도록 하였고, 암호화된 데이터나 키 데이터 모두 XOR 연산을 기본으로 암호화함으로써 두 데이터의 곱과 기준파의 간섭으로 원 영상이 간단히 복원되도록 하였다. 따라서 본 논문에서는 높은 암호화 수준과 간단한 복호화 시스템을 가진 광 암호화 방법을 제안하였으며, 이러한 방법의 적합성과 구현가능성을 컴퓨터 시뮬레이션을 통하여 확인하였다.

II. 제안한 그레이 영상 암호화 방법

우선, 최대 그레이 크기 n을 가지는 영상 $O_n(x,y)$이 있다고 가정할 때 이를 n개의 이진영상들의 합으로 표현 할 수 있으며

$$O_n(x,y)=1\cdot b_1(x,y)+2\cdot b_2(x,y)+\ldots+n\cdot b_n(x,y) \tag{1}$$

와 같다. 여기서 b_1, b_2, b_3, $\cdots$, b_n은 0 또는 1의 값을 갖는 이진 영상을 나타낸다. 나누어진 이진 영상들, 즉 슬라이드 영상들을 각각 무작위 이진영상들 r_1, r_2, r_3, $\cdots$, r_n과 XOR 연산을 하여 암호화된 새로운 이진영상 e_1, e_2, e_3, $\cdots$, e_n을 만들 수 있으며, 이 때 n번째 암호화된 이진 영상은

$$e_n=b_n\oplus r_n \tag{2}$$

로 나타낸다. 위 식 (2)에서 기호 $\oplus$는 XOR 연산자를 의미한다. 만약 암호화된 이진 영상들과 임의 이진영상들을 위상 변조한 후 b_n을 구하면,

$$b_n(x,y)=\frac{1}{2}\left|[\exp(j\pi e_n)-\exp(j\pi r_n)]\right| \tag{3}$$

와 같이 표현되며, 원 영상으로부터 나누어진 이진영상 b_n을 구할 수 있다. 이때 사용되는 위상 변조 XOR 연산규칙은 표 1과 같다.

즉, b_n이 1이고 r_n이 0이라고 가정한다면, $\exp(j\pi r_n)$은 1이 되므로 $\exp(j\pi e_n)$은 −1로 결정되며 두 값 $\exp(j\pi e_n)$, $\exp(j\pi r_n)$의 차는 −2로써, 절대값을 취한 후 2로 나누면 b_n의 값이 된다. 따라서 원 영상 $O_n(x,y)$을 표 1의 연산규칙으로 나타나면

$$\begin{aligned}O_n(x,y)=\frac{1}{2}\{&1\cdot\left|\exp(j\pi e_1)-\exp(j\pi e_1)\right|+\\&2\cdot\left|\exp(j\pi e_2)-\exp(j\pi r_2)\right|+\\&3\cdot\left|\exp(j\pi e_3)-\exp(j\pi r_3)\right|\ldots+\\&n\cdot\left|\exp(j\pi e_n)-\exp(j\pi r_n)\right|\}\end{aligned}$$

표 1. XOR 연산과 제안한 위상 변조 XOR 연산

Binary images			Phase-encoded images		
XOR			Phase encoded XOR		
b_n	e_n	r_n	$\exp(j\pi e_n)$	$\exp(j\pi r_n)$	$\lvert\exp(j\pi e_n)-\exp(j\pi r_n)\rvert/2=b_n$
0	0	0	1	1	0
	1	1	−1	−1	0
1	0	1	1	−1	1
	1	0	−1	1	1

$$\begin{aligned}=\frac{1}{2}|\{&1\cdot[\exp(j\pi e_1)-\exp(j\pi e_1)]+\\&2\cdot[\exp(j\pi e_2)-\exp(j\pi r_2)]+\\&3\cdot[\exp(j\pi e_3)-\exp(j\pi r_3)]\ldots+\\&n\cdot[\exp(j\pi e_n)-\exp(j\pi r_n)]\}|\end{aligned} \tag{4}$$

와 같다. 위 식 (4)에서 전체에 절대값 기호를 두어도 등식이 성립하는 것은 각 레벨에 해당하는 슬라이드 영상의 화소들, 즉 1의 값으로 나타나는 화소들은 서로 중첩되지 않고 독립적인 위치를 유지하므로 슬라이드 영상간의 연산 결과는 절대값 기호의 우선 순위에 영향을 받지 않기 때문이다.

식 (4)에서 위상 변조되어 암호화한 이진 영상들 $\exp(j\pi e_1)$, $\exp(j\pi e_2)$, $\cdots$, $\exp(j\pi e_n)$과 위상 변조한 이진 무작위 영상들 $\exp(j\pi r_1)$, $\exp(j\pi r_2)$, $\cdots$, $\exp(j\pi r_n)$을 각각 나눈 후, 더하여 구한 암호화 영상 $E(x,y)$와 키 영상 $K(x,y)$은

$$\begin{aligned}E(x,y)&=\frac{1}{2}[1\cdot\exp(j\pi e_1)+2\cdot\exp(j\pi e_2)+\ldots+n\cdot\exp(j\pi e_n)]\\K(x,y)&=-\frac{1}{2}[1\cdot\exp(j\pi r_1)+2\cdot\exp(j\pi r_2)+\ldots+n\cdot\exp(j\pi k_n)]\end{aligned} \tag{5}$$

와 같이 표현할 수 있다. 암호화 영상과 키 영상을 한번 더 위상 부호화 하여

$$\begin{aligned}\tilde{E}(x,y)&=\exp[j\pi E(x,y)/n]\\\tilde{K}(x,y)&=\exp[j\pi K(x,y)/n]\end{aligned} \tag{6}$$

과 같이 최종 암호화 데이터 $\tilde{E}(x,y)$와 키 데이터 $\tilde{K}(x,y)$를 구한다. 암호화 영상과 키 영상을 위상 부호화 하기 전에 먼저 원 영상 $O_n(x,y)$의 최대 그레이 값 n으로 두 영상을 나누는 과정이 필요하며 이는 암호화 영상 $E(x,y)$와 키 영상 $K(x,y)$를 [0, (n+1)/2*π]의 범위로 위상 부호화 하여, 복호화 영상의 위상값이 $[0,\pi]$ 범위에서 재생되도록 함으로써, 복호화 영상의 화소값들은 최대값을 1로 정규화하여 위상 변조한 원 영상의 반전 영상 화소값들과 동일하게 된다. 암호화 데이터와 키 데이터의 위상성분은 위상 부호화 XOR 연산에 의해 $[0,2\pi]$내에 임의로 존재하므로 위상 정보를 안다고 해도 두 개의 위상 성분을 결합하지 않고서는 원 영상을 복원할 수가 없다.

만약 키 없이 암호화 영상을 분석하여 원 영상을 복호화하고자하는 경우, 예를 들어 암호화 영상이 64×64이고 최대 그레이 레벨값인 n이 256이라고 한다면, 한 화소의 값을 찾는데 256번의 연산이 소요되므로, 전체의 영상값을 찾는데는 $256^{64}\times256^{64}\approx1.78\times10^{308}$번의 수학적 연산이 필요하다. 또한, 암호화된 영상은 XOR된 이진 영상들의 합에 의해 원 영상의 화소정보가 임의로 바뀐 그레이 영상이기 때문에 암호화된 영상만으로는 원 영상을 복원이 거의 불가능하므로, 암호화된 영상은 매우 높은 암호화 수준을 유지한다.

III. 4×4 크기의 그레이 영상에 대한 암호화 및 복호화

4×4 크기의 최대 그레이 레벨 값이 3인 원 영상(O_3)을 식 (1)처럼 각각의 그레이 값에 해당하는 슬라이드 이진 영상(b_3,

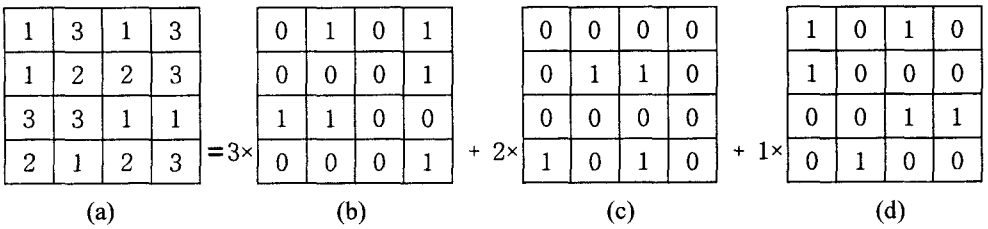


그림 1. 원 영상의 슬라이드 영상화. (a) 원 영상 O_3, (b) 슬라이드 영상 b_3, (c) 슬라이드 영상 b_2, (d) 슬라이드 영상 b_1.

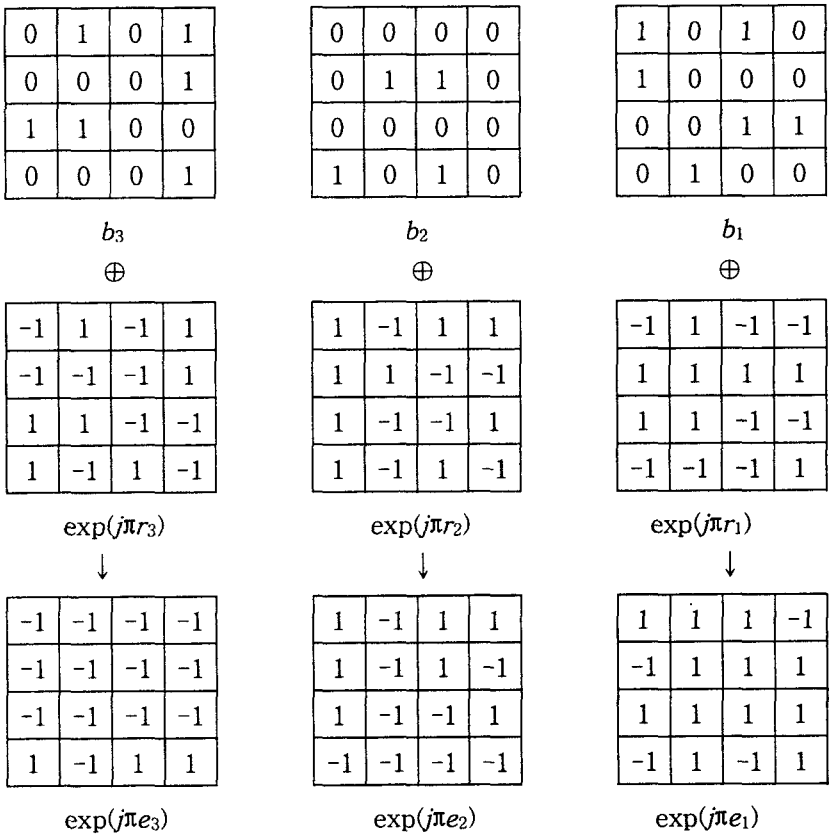


그림 2. 표 1의 위상 변조 XOR 규칙을 이용한 슬라이드 영상의 암호화.

b_2, b_1)으로 나누어 표현하면 그림 1과 같다.

각 레벨에 해당하는 슬라이드 영상의 화소들, 즉, 1의 값을 가지는 화소들은 그림 1과 같이 서로 만나거나 중첩되지 않고 독립적인 위치를 가진다. 위의 슬라이드 영상들을 1 또는 −1 값만 가지도록 위상 변조된 3개의 다른 무작위 이진 영상들 $\exp(j\pi r_3)$, $\exp(j\pi r_2)$, $\exp(j\pi r_1)$과 표 1의 위상 변조 XOR 방법으로 암호화하는 과정은 그림 2와 같고, 암호화된 이진 결과 영상들은 $\exp(j\pi e_3)$, $\exp(j\pi e_2)$, $\exp(j\pi e_1)$으로 표현된다.

암호화된 이진 결과영상들과 위상 변조된 무작위 이진 영상들에 식 (5)를 적용하여 암호화 영상 $E(x, y)$와 키 영상 $K(x, y)$를 만드는 과정은 그림 3과 같다.

위의 암호화 영상과 키 영상을 식 (6)과 같이 위상 부호화 했을 경우, 광학적인 복호화에 사용되는 최종 암호화 데이터 $\tilde{E}(x, y)$ 와 키 데이터 $\tilde{K}(x, y)$ 가 구해진다. 원 영상의 복호화는 암호화 영상과 키 영상의 합에 절대값을 취할 경우, 그림 4와 같이 원 영상(O_3)이 되는 원리를 이용한다.

광학적 복호화 수행시 암호화 데이터와 키 데이터를 간섭계의 경로에 나란히 두면, 두 영상간의 곱에 의한 위상성분은 암호화 영상과 키 영상간의 합이 된다. 위상성분의 합 그 자체로는 원 영상의 정보가 되지는 못하지만, 코사인 함수의 우함수적 특성으로 인해 자동적으로 위상 성분에 절대값 기호가 취해짐으로 원 영상의 정보가 복원이 되며, 원 영상의 정보는 코사인 함수에 의해 반전되어 CCD에 나타난다.

IV. 간섭계를 사용한 복호화

복호화 영상은 위상 시각화 시스템으로 간단하게 구할 수 있다. 본 논문에서는 위상 시각화 시스템으로 그림 1과 같은 마흐젠더 간섭계[7]를 이용해 복호화 과정을 수행하였다.

간섭계의 한쪽 경로에 그림 1과 같이 암호화 데이터와 키 데이터를 일렬로 놓고, 다른 경로에 기준 파를 간섭시켰을 때 CCD 평면에서 관찰되는 복호화 영상은

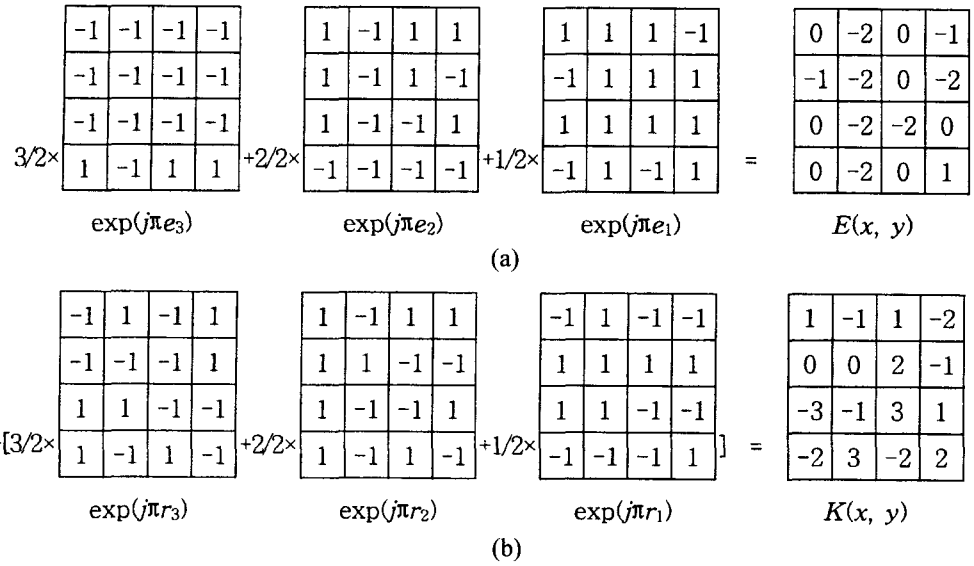


그림 3. 암호화 영상과 키 영상 제작. (a) 암호화 영상, (b) 키 영상.

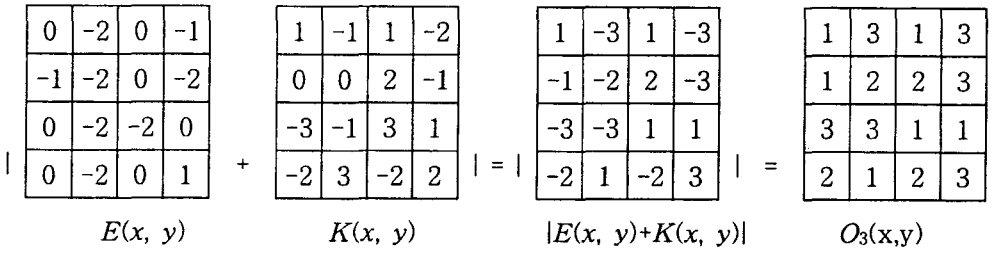


그림 4. 암호화 영상과 키 영상을 이용한 원 영상의 복원 원리.

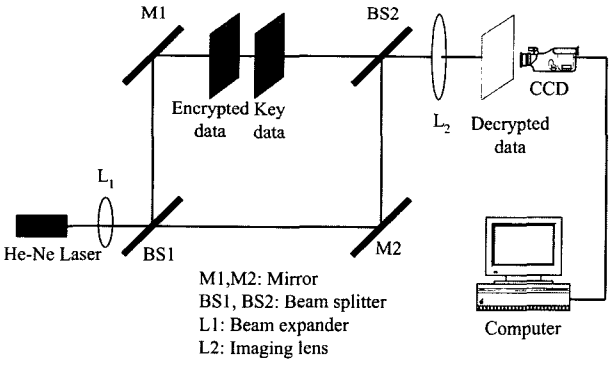


그림 5. 영상 복호화를 위한 마흐젠더 간섭계.

$$
\begin{aligned}
&O_{CCD}(x,y)\\
&=\left|R(x,y)+R(x,y)\tilde{E}(x,y)\tilde{K}(x,y)\right|^2\\
&=|R(x,y)|^2\left|1+\exp[j\pi(E(x,y))/n]\exp[j\pi K(x,y)/n]\right|^2\\
&=|R(x,y)|^2\{2+2\cos[\pi E(x,y)/n+\pi K(x,y)/n]\}\\
&=|R(x,y)|^2\left\{2+2\cos\left[\frac{\pi}{n}|E(x,y)+K(x,y)|\right]\right\}\\
&=|R(x,y)|^2\left\{2+2\cos\left[\frac{\pi}{n}O_n(x,y)\right]\right\} \qquad (7)
\end{aligned}
$$

과 같이 표현되며, 여기서 $R(x,y)$는 기준파를 의미한다. 기준파의 크기와 위상성분의 표현은

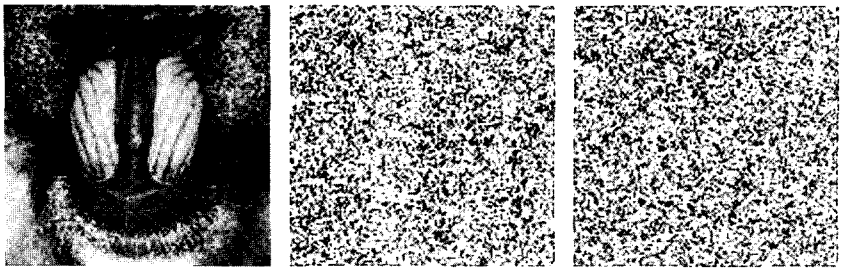
$$
\begin{aligned}
&R(x,y)=E\exp(j\theta)\\
&|R(x,y)|=|E\exp(j\theta)|^2=|E|^2 \qquad (8)
\end{aligned}
$$

과 같다.

식 (7)에서 n으로 각각 나눈 암호화 영상 $E(x,y)$와 키 영상 $K(x,y)$의 합은 그 자체로 원 영상의 정보는 아니지만, 위상 부호화한 영상을 CCD로 관측할 때 발생하는 코사인 함수의 우함수적 특성으로 인해 절대값 기호가 그 합에 취해짐으로 정규화된 원 영상이 된다. 정규화된 원 영상은 위상 부호화 시 $\exp(j\pi)$ 함수로 위상 부호화 되었기 때문에 코사인 함수의 $[0,\pi]$ 구간내에서만 그 값이 존재하며, 이 구간 내에서는 정규화된 원 영상이 코사인 함수 출력과 반비례적인 일대일 관계로 표현되므로, 정규화된 원 영상의 반전영상이 CCD평면에서 비선형적인 특성으로 나타난다. 반전영상을 컴퓨터로 후처리(post processing)하여 최종 복호화 영상을 얻을 수 있다.

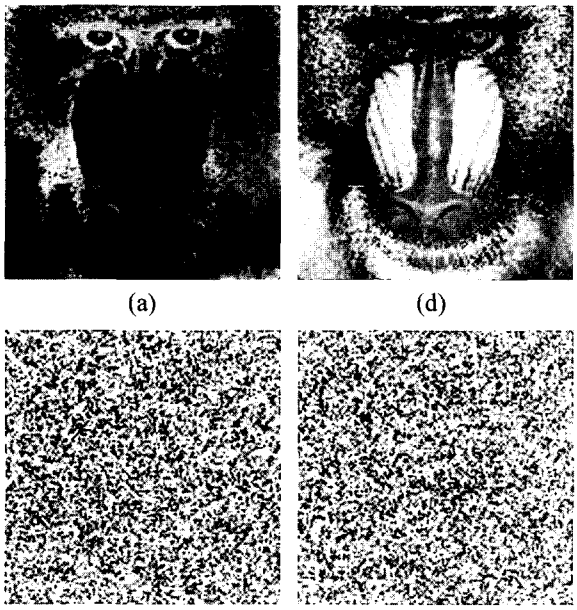
V. 컴퓨터 모의 실험

그림 6(a)는 128×128 화소수와 최대 그레이 값 220을 가지는 Baboon영상이며 이를 컴퓨터 모의 실험의 원 영상으로



(a) (b) (c)

그림 6. 컴퓨터 모의실험 영상. (a) 원 영상, (b) 암호화 데이터, (c)키 데이터.



(a) (d)

(c) (d)

그림 7. 컴퓨터 모의실험 영상. (a) CCD 평면에서의 복호화 영상, (b) 3(a)의 후처리 후 영상, (c)거짓 키 영상, (d) 거짓 키로 재생된 영상.

사용하여 암호화된 데이터와 키 데이터를 생성하였다. 암호화된 데이터와 키 데이터는 $[0, 2\pi]$ 범위의 위상 영상으로 눈으로 보이지 않기 때문에 편의를 위해 그레이 값 [0, 255]로 대응시켜 그림 6(b)와 그림 6(c) 같이 나타내었다.

그림 6(b)와 그림 6(c)를 마흐젠더 간섭계의 한 경로에 두고 나머지 경로에는 기준파를 두어 간섭시켜 CCD평면에 나타난 결과 영상이 그림 7(a)이다. 그림 7(a)는 원 영상의 반전영상이므로 컴퓨터를 이용한 후처리 과정으로 최종 복호화 영상 그림 7(b)를 얻을 수 있다. 그림 7(c)와 같은 임의의 거짓 키 영상을 사용하여 복호화한 결과는 그림 7(d)이며 원 정보가 복호화 되지 않음을 확인할 수 있다.

만약 암호화 데이터와 키 데이터의 화소 사이즈를 작게 하여 제작한 경우, 두 영상간의 간격이 조금이라도 있으면 두 영상간의 위상이 제대로 간섭되었다할지라도 회절 현상에 의해 출력평면에서 재생된 이미지의 효율은 상당히 떨어진다.[7] 그러므로, 두 영상간의 픽셀을 정확히 일치시켜 완전히 포갠 후(superimposed) 간섭시켰을 경우에는 암호화 데이터와 키

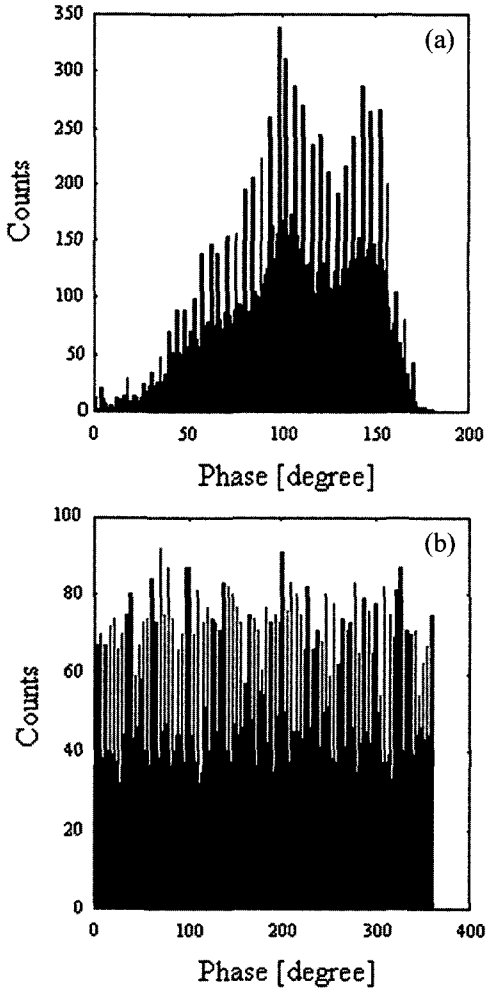


그림 8. 히스토그램. (a) 위상 변조한 원 영상의 위상성분 히스토그램 (b) 암호화 데이터의 위상성분 히스토그램.

데이터의 픽셀 사이즈를 작게 하여 제작한다할지라도 회절효과의 영향을 거의 받지 않고 원 영상을 재생할 수 있다. 또한 포갠 영상들과 CCD와의 거리가 멀어지면 회절 문제가 발생할 수 있으므로, CCD를 기준파와 간섭된 평면에 밀착시켜 거리차가 최소화시키면 회절 현상을 줄일 수 있다.

최대값을 1로 정규화하여 위상 변조한 원 영상과 암호화 데이터의 위상 분포를 히스토그램으로 비교해 보았다. 그림 8(a)는 원 영상의 위상성분에 대한 히스토그램 분포이고, 그림 8(b)

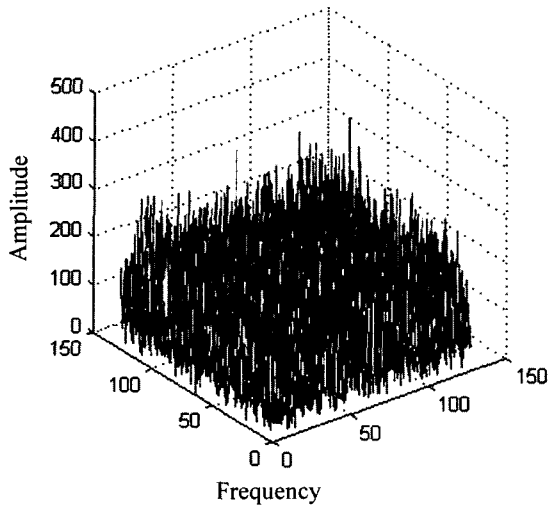


그림 9. 3차원 주파수 평면에서의 암호화 데이터 성분.

는 암호화 데이터의 위상성분에 대한 히스토그램 분포이다. 원 영상의 위상성분들이 특정한 분포를 가지는 반면 암호화된 영상의 위상성분은 0°에서 360° 사이의 고른 분포를 가진 잡음 형태로 분포함을 알 수 있다.

또한 암호화 데이터가 푸리에 영역에서 특정한 주파수 성분으로 분석되는지 확인하기 위해 암호화 데이터의 주파수 성분 분포를 그림 9와 같이 3차원으로 표현하였으며, 이를 통해 암호화 데이터의 주파수 분포가 전 영역에 고르게 나타남을 알 수 있다.

따라서 제안한 암호화 방법으로 암호화된 영상 정보는 공간 영역이나 주파수 영역에서 임의적인 잡음 형태의 분포를 가지므로 암호화된 영상 정보만으로는 원 영상의 정보를 쉽게 유추하거나 해석할 수 없다.

VI. 결 론

본 논문에서는 위상 변조 XOR 연산이라는 방법을 토대로 그레이 영상에 대한 새로운 암호화 방법을 제안하였다. 그레이 원 영상을 위상 변조 XOR에 연산을 이용하여 암호화 영상을 만들고 이를 위상 변조시킴으로써 위상 변조 영상의 특성상 세기 검출기로 그 정보를 쉽게 복사하거나 알아낼 수 가 없다는 특징과, 설사 그 정보가 유출된다할 지라도 암호화된 데이터의 위상정보들은 서로 독립적인 XOR연산의 결과이기 때문에 키 데이터의 위상정보 없이는 원 영상의 복호화 할 수는 없다는 장점을 이용하여 보다 높은 정보보호를 가능케 하였다. 또한, 영상 복원시 간섭의 원리를 이용하여 암호화 데이터와 키 데이터를 일렬로 나열하여 기준파와 간섭시키므로써, 간단한 시스템으로 복호화 구현이 가능하도록 하였다. 마지막으로 시뮬레이션을 통해 제안한 암호화 방법의 적합성과 구현 가능성을 검증해보았다.

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] N. Towghi, B. Javidi, and Z. Luo. "Fully phase encrypted image processor," *J. Opt. Soc. Am.* A, vol. 16, no. 8, pp. 1915-19272, 1999.

[3] J. W. Han, C. S Park, D. H. Ryu, and E. S. Kim, "Optical image encryption based on XOR operations," *Opt. Eng.* vol. 38, no. 1, pp. 47-54, 1999.

[4] 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, no. 10, pp. 874-875, 2000.

[5] P. C. Mogensen and J. Gluckstad, "Phase-only optical encryption," Opt. Lett., vol. 25, no. 8, pp. 566-568, 2000.

[6] P. C. Mogeansen and J. Gluckstad, "Phase-only optical decryption of a fixed mask," *Appl. opt.*, vol. 40, no. 8, pp. 1226-1235, 2001.

[7] D. H. Seo and S. J. Kim. "Interferometric phase-only optical encryption system that uses a reference wave," *Opt. Lett.*, vol. 28, no. 5, pp. 304-306, 2003.

Optical security scheme using phase-encoded XOR operations

Chang-Mok Shin†, Dong-Hoan Seo, and Soo-Joong Kim
School of Electrical Engineering & Computer Science, Kyungpook National University, Daegu 702-701, KOREA
†E-mail: neo_minstrel@daum.net

(Received June 18, 2003, Revised manuscript October 17, 2003)

In this paper, we have proposed a full phase encryption scheme based on phase-encoded XOR operation. The proposed scheme encrypts a gray-level image by slicing an original image and combining with XORed images which resulted from phase-encoded XOR operations between sliced images and phase-encoded binary random images. Then we produce an encrypted image by combining only XORed images and a key image by only phase-encoded binary random images. The encrypted image and key image are converted into encrypted data and key data by a phase-encoding method. The merits are that the proposed encryption scheme can basically fulfill a high-level encryption using a full phase encryption scheme which has nonlinear and invisible characteristics. The scheme also improves security by encrypting the phase information before full phase encryption. The decryption system based on the principle of interference between a reference wave and a direct pixel-to-pixel mapping image of encrypted data with key data can be simply implemented using a phase-visualization system. Simulation results indicate that our proposed encryption scheme is effective and simple for a gray-scale image and optical decryption system.

OCIS Codes : 100.1160, 120.3180, 120.5060.