《연구논문》 Hankook Kwanghak Hoeji, Volume 16, Number 4, August 2005

푸리에 영역에서의 위상 변조 Exclusive-OR 연산을 이용한 단일 경로 위상 암호화 시스템

신창목 · 조규보† · 김수중

경북대학교 전자전기컴퓨터학부

㉾ 701-702 대구광역시 북구 산격동 1370

노덕수

경일대학교 전자정보통신공학부

㉾ 712-701 경산북도 경산시 하양읍 부호리 33번지

(2005년 6월 3일 받음, 2005년 7월 14일 수정본 받음)

본 논문에서는 원 영상을 푸리변환한 후 위상 변조 XOR 연산으로 암호함으로써 정보의 손실에 강하며 한 개의 광 경로만으로 간단히 복호화 할 수 있는 위상 암호화 시스템을 제안하였다. 영 삽입된(zero-padded) 원 영상에 무작위 위상 영상을 곱하여 푸리에 변환된 데이터 값을 키 데이터와 위상 변조 XOR 연산으로 암호화한다. 이렇게 생성된 암호화 데이터와 키 데이터를 최종적으로 위상 변조하여 위상 암호화 영상과 위상 키 영상을 만든다. 위상 변조된 암호화 영상과 키 영상은 비가시성과 비선형성으로 인해 높은 정보보호의 특성이 있으며 또한, 푸리에 영역의 암호화로 인해 절단에 의한 정보의 손실에도 영상을 복호화 할 수 있다. 복호화 과정은 암호화 영상과 키 영상의 단순곱을 푸리에 변환한 후 영차 성분(zero-order component)을 공간 필터링함으로써 간단히 구현할 수 있으며, 복호화 시스템은 2-f 구조의 단일 경로의 구조를 바탕으로 하므로 부피가 상대적으로 작을 뿐만 아니라 외부 충격이나 기온 변화와 같은 환경적인 영향을 받지 않고 복호화를 수행할 수 있다. 제안한 암호화 과정과 복호화 시스템의 구현 가능성 및 타당성을 컴퓨터 모의실험을 통해 확인하였다.

주제어 : Optical encryption, Fourier plane, Phase-only image.

I. 서 론

최근 몇 년 동안 광의 고유한 특성인 빠른 연산능력과 병렬성을 기반으로 한 다양한 암호화 시스템들이 제안되어 왔다.[1-10] 이 중 크기 정보와 위상 정보를 함께 부호화 하는 크기 기반 암호화 시스템(amplitude-based encryption system)은 여러 가지 이론 및 실험적 결과들에 의해 암호화에 적합한 방법임이 증명되고 연구되었다.[1,2] 그러나 크기 기반 암호화 시스템은 복소 정보를 표현할 수 있는 마스크나 소자의 제작 한계로 인해 실제 시스템 구현에 제약이 따른다. 이러한 제작상의 어려움을 극복하고 좀 더 암호화 수준을 높이기 위해 여러 암호화 이론들과 결합된 위상 기반 암호화 시스템들(phase-based encryption system)이 제안되고 있다.[3-8] 일반적으로 위상 기반 암호화 시스템은 잡음이 있을 경우나 대역폭이 제한된 환경에서 크기 기반 암호화 시스템보다 더 효율적이고 우수한 구현 결과들을 보여주며, 비가시적인 특성과 비선형성으로 인해 보다 높은 암호화 수준을 유지한다.[3]

위상 기반 암호화 시스템에서 복호화할 정보의 표현을 위해선 출력평면에서 위상 정보를 세기 정보로의 변환 과정이 필요하며, 이를 위해 4-f 구조의 위상 대조차 여파기(phase-contrast filter)를 사용하여 위상정보를 진폭 정보로 변환함으로써 원 영상을 복호화하는 방법[5,6]이나 마흐젠더 간섭계의 구조를 이용하여 복호화하는 방법[7] 등이 제안되었다. 마흐젠더 간섭계에 의한 복호화 방법은 광 정렬 및 화소 대 화소 정합(mapping) 문제를 어느 정도 해결했으나 두 개의 경로를 가지는 간섭계의 기본적인 특성으로 인해 기계적인 충격이나, 진동 그리고 온도 변화와 같은 환경적인 요소에 민감하다는 단점이 있다. 반면에 위상 대조차 여파기에 의한 복호화 구조는 외부적 진동과 교란에 강하다는 장점을 가지고 있지만 출력 평면에서 원하는 세기 영상을 얻기 위해서는 여파기 내부의 핀홀(pinhole)을 광 파장의 위상에 따라 세심하게 조절하고 설계하여야 한다.

본 논문에서는 푸리에 영역에서 영상을 위상 변조 XOR 연산[10]으로 암호화함으로써 간단한 단일 경로 2-f 구조로 복호화가 가능한 위상 암호화 시스템을 제안하였다. 암호화 과정은 영 삽입된 원 영상을 무작위 위상 영상과 곱하여 푸리에 변환하고, 푸리에 변환된 데이터값 중 실수 값들만 취한 후 이를 무작위 키 데이터와 위상 변조 XOR하여 암호화 한다. 암호화된 데이터와 키 데이터는 백색잡음의 가우시안 분포 특성을 가지며 이를 위상 변조하여 최종 암호화 영상과 키 영상을 생성한다. 복호화시 암호화 영상과 키 영상을 나란히 두고 이에 빛을 통과 시킨 후 렌즈를 이용해 푸리에 변환하고 이를 공간필터로 영차 성분을 제거한 후 CCD로 검출함으로써 간단히 원하는 복호화 세기 패턴을 얻을 수 있다. 제안한 복호화 시스템은 복호화 과정에서 기준파 없이 위상 시

† E-mail: ckb10040@ee.knu.ac.kr

각화(phase visualization)를 수행하므로 기존의 마흐젠더 시스템에 비해 기계적 진동이나 떨림에 의한 영향을 덜 받을 뿐만 아니라 암호화 영상과 키 영상의 곱의 수행 시 두 영상을 간단히 포개어 빛을 통과시킴으로써 광 축 문제와 화소 대 화소 정합 문제를 최소화 할 수 있다. 비록 제안한 시스템이 위상 대조차 여파기를 사용한 시스템처럼 필터를 필요로 하지만, 제안한 복호화 시스템 내의 필터는 단순히 영차 성분만을 제거하는 공간 필터로써의 역할을 2-f 구조의 출력 평면에서 수행하므로 기존의 복호화 시스템에 비해 더 간단하고 부피 또한 줄어든 장점을 가진다.

II. 푸리에 영역의 영상 암호화 과정

원 영상을 $f(x, y)$라 한다면 여기에 영 삽입(zero-padding)하여 무작위 위상 영상과 곱한후 푸리에 변환하면

$$F(u, v) = \mathrm{FT}\{ f_z(x, y) \ \exp[\, jn(x, y)]\} \tag{1}$$

와 같다. 여기서 $f_z(x, y)$는 영 삽입된 원 영상, $n(x, y)$는 $[0, 2\pi]$의 분포를 가지는 백색잡음 영상을 나타내며, FT{ · }는 푸리에 변환 연산자이다.

영 삽입된 원 영상을 푸리에 변환했을 경우 푸리에 변환된 영상의 실수값만을 역푸리에 변화하여 원 영상 정보의 복원이 가능하므로, $F(u, v)$의 실수값만을 취한 영상 $F_{real}(u, v)$를 구한다. 그레이 값을 가지는 $F_{real}(u, v)$를 위상 변조 XOR 방법으로 암호화하기 위해 우선 $F_{real}(u, v)$의 최소값이 0이상의 값을 가지도록 $F_{real}(u, v)$의 데이터값들에 최소값을 빼면,

$$F^{+}_{real}(u, v) = F_{real}(u, v) - F_{\min} \tag{2}$$

이 되며, 이 때 F_{min}은 $F_{real}(u, v)$의 최소값을, $F^{+}_{real}(u, v)$는 0 이상의 실수값을 가지는 영상을 나타낸다. $F^{+}_{real}(u, v)$는 다양한 그레이 값을 가지는 화소들로 이루어져 있으며 최소 그레이 화소값 m, 최대 그레이 화소값 n을 가진다고 할 때, 이를 동일한 화소값으로 그룹화한 이진 영상들의 합으로 표현할 수 있다.[10]

$$F^{+}_{real}(u, v) = mF_m(u, v) + (m+1)F_{m+1}(u, v) + \ldots + nF_n(u, v) \tag{3}$$

여기서 F_m, F_{m+1}, ..., F_n은 0 또는 1의 값을 가지는 이진 영상이다. 이렇게 나누어진 이진 영상 즉 슬라이드 영상들을 각각 1이나 -1의 값을 가지는 무작위 이진 영상들 r_m, r_{m+1}, ⋯, r_n과 표 1에서의 위상 변조 XOR 연산을 수행하여 암호화된 새로운 이진영상 e_m, e_{m+1}, ⋯, e_n을 생성하며, 이 때 그레이 값이 k인 슬라이드 영상 F_k를 암호화된 영상 e_k와 r_k로 표현하면

$$F_k(u, v) = s_k(u, v)[e_k(u, v) - r_k(u, v)] \tag{4}$$

와 같다.

표 1에서 g_k와 h_k는 일반적인 XOR연산 수행시의 무작위 이진 영상과 XOR된 영상을 나타낸다. 식 (4)에서 $S_k(u, v)$는 $F_k(u, v)$의 정확한 부호 복원의 역할을 하며 1이나 -1의 값을 가지는 백색잡음 분포의 이진 영상이다. 따라서 식 (4)를 이용하여 $F^{+}_{real}(u, v)$를 나타내면

$$\begin{aligned} F^{+}_{real}(u, v) = {} & mF_m + (m+1)F_{m+1} + \ldots + nF_n \\ = {} & 1/2[ms_m(e_m - r_m) + (m+1)s_{m+1}(e_{m+1} - r_{m+1}) \\ & + \ldots + ns_n n(e_n - r_n)] \end{aligned} \tag{5}$$

와 같다. 식 (5)에서 각각의 $s(u, v)$들에 존재하는 -1 화소값들은 고유한 위치에 존재하여 서로 영향을 주지 않으므로

$$\begin{aligned} & F^{+}_{real}(u, v) \\ & = 1/2[ms_m(e_m - r_m) + (m+1)s_{m+1}(e_{m+1} - r_{m+1}) + \ldots \\ & \quad + ns_n n(e_n - r_n)] \\ & = 1/2(s_m \times s_{m+1} \times \ldots \times s_n)[m(e_m - r_m) + (m+1)(e_{m+1} - r_{m+1}) \\ & \quad + \ldots + n(e_n - r_n)] \\ & = 1/2S[m(e_m - r_m) + (m+1)(e_{m+1} - r_{m+1}) + \ldots + n(e_n - r_n)] \end{aligned} \tag{6}$$

로 나타낼 수 있다. 이 때 $S = s_m \times s_{m+1} \times \ldots \times s_n$ 를 의미한다. 식 (6)으로부터 암호화한 이진 영상들 e_n, e_{m+1}, ⋯, e_n과 무작위 이진 영상들 r_m, r_{m+1}, ⋯, r_n을 각각 다른 화소값 대로 분리한 후 더하여 구한 암호화 데이터 $E(u, v)$와 키 영상 $K(u, v)$는

$$\begin{aligned} E(u, v) &= 1/2S[me_m + (m+1)e_{m+1} + \ldots + ne_n] \\ K(u, v) &= 1/2S[mr_m + (m+1)r_{m+1} + \ldots + nr_n] \end{aligned} \tag{7}$$

과 같이 표현할 수 있다. 암호화 데이터와 키 데이터를 위상 부호화 하여

$$\begin{aligned} \tilde{E} &= \exp[\, j\pi E(u, v)/nC] \\ \tilde{K} &= \exp[\, j\pi K(u, v)/nC] \end{aligned} \tag{8}$$

와 같이 최종 암호화 영상 $\tilde{E}$와 키 영상 $\tilde{K}$를 생성한다. 여

표 1. XOR 연산과 위상 변조 XOR 연산.

XOR ($b_k \oplus g_k = h_k$)			Phase encoded XOR ($b_k \oplus r_k = e_k$)		s_k $=\exp\{j\pi[(e_k - r_k)/2 - b_k]/2\}$	$b_k = 1/2 s_k(e_k - r_k)$
b_k	g_k	h_k	r_k	e_k		
0	0	0	1	1	1	0
	1	1	-1	-1	1	
1	0	1	1	-1	-1	1
	1	0	-1	1	1	

기서 F^{+}_{rea}의 최대 그레이 화소값 n은 복호화 영상의 위상 정보가 [0, π] 구간내에 존재하도록 정규화하는 역할을 하며, 양수 C는 암호화 영상과 키 영상의 위상 범위를 적절히 줄여 복호화 영상의 시각적 퀄러티(visual quality)를 조절한다.

III. 4×4 크기의 그레이 영상에 대한 암호화 및 복호화의 예

4×4 크기의 최대 그레이 레벨 값이 5인 영상(F)를 암호화하고자 할 경우 우선 식 (3)처럼 각각의 그레이 값에 해당하는 슬라이드 이진 영상(b_1, b_2, b_5)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 -1의 다른 무작위 이진 영상들 r_1, r_2, r_5와 표 1의 위상 변조 XOR 방법으로 암호화하는 과정은 그림 2와 같고, XOR된 이진 영상들은 e_1, e_2, e_5로 표현된다.

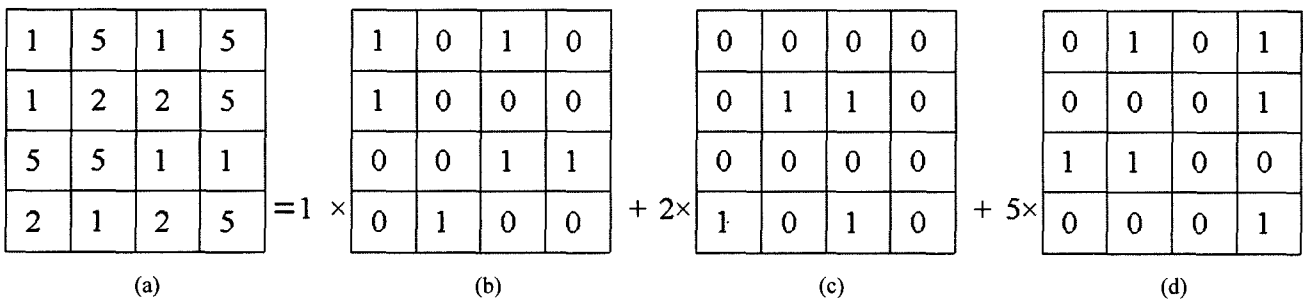


그림 1. 영상의 슬라이드 이진화. (a) 영상 F, (b) 슬라이드 영상 b1, (c) 슬라이드 영상 b2, (d) 슬라이드 영상 b5.

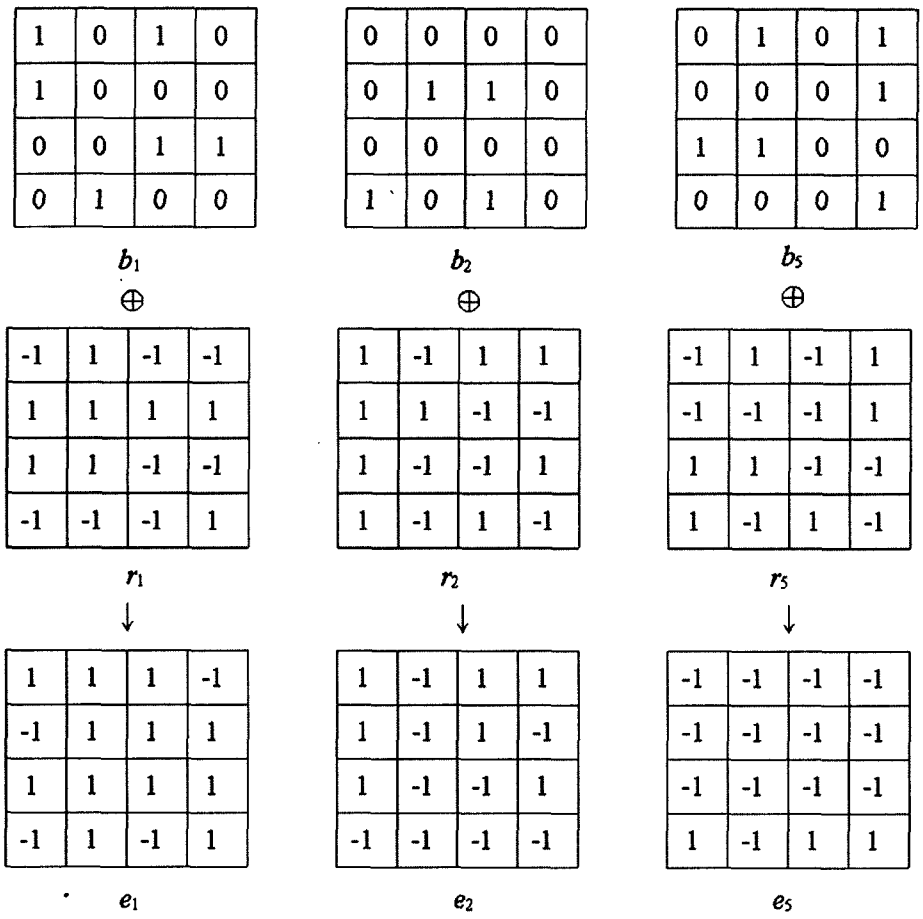


그림 2. 표 1의 위상 변조 XOR 규칙을 이용한 슬라이드 영상의 XOR 암호화.

이 때 슬라이드 영상 복원시 필요한 이진 영상 s_1, s_2, s_5는 표 1에 의해 그림 3과 같이 표현된다.

그림 3에서 같이 슬라이드 영상 복원시 영향을 미치는 s_5, s_2, s_1내의 -1 화소값들은 고유한 위치에 존재하여 영향을 주지 않으므로, 식 (6)에서와 같이 서로 곱하여 하나의 영상으로 대체하면 그림 4와 같이 나타난다.

XOR된 이진 영상들과 무작위 이진 영상들에 식 (7)를 적용하여 암호화 데이터 $E(u, v)$와 키 데이터 $K(u, v)$를 만드는 과정은 그림 5와 같다.

위의 암호화 영상과 키 영상을 식 (8)과 같이 위상 부호화

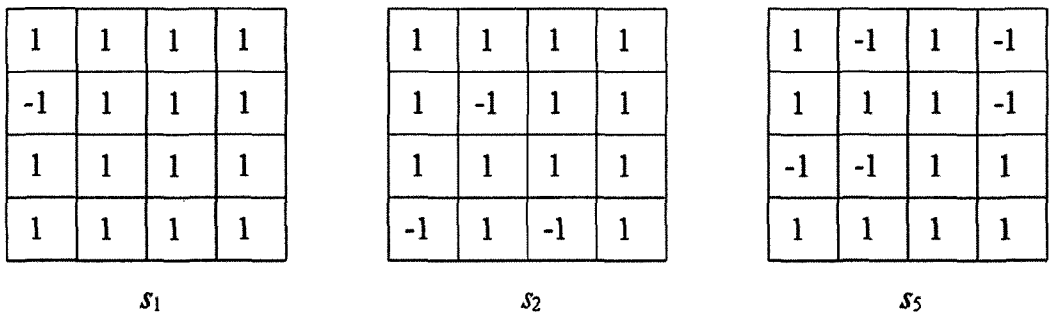


그림 3. 슬라이드 영상 복원시 필요한 이진 부호 영상.

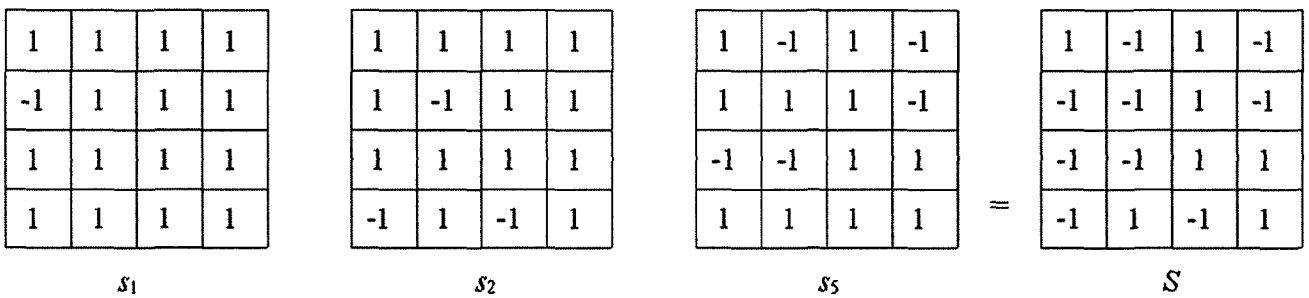
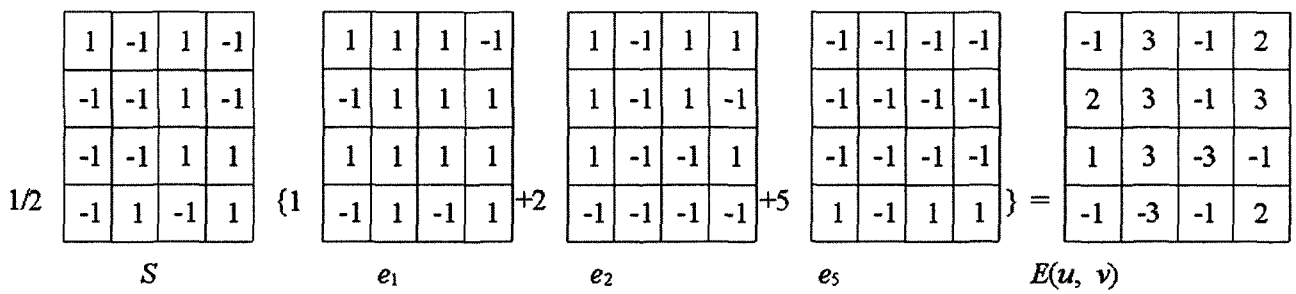
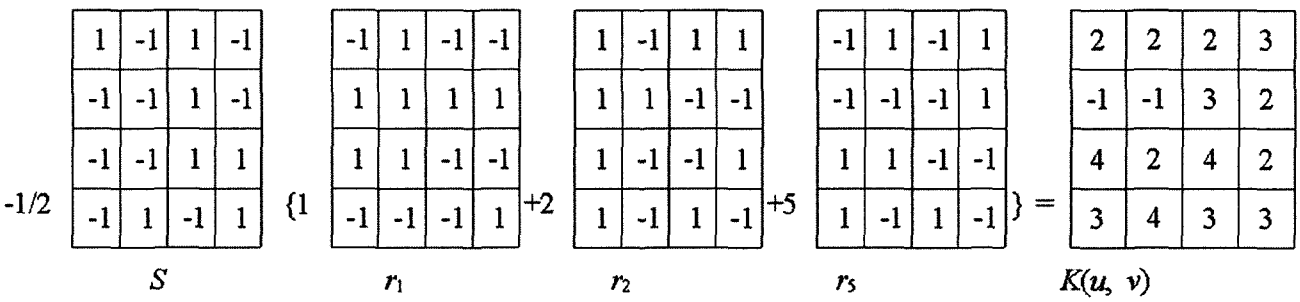


그림 4. 이진 부호 영상들의 간략화.



(a)



(b)

그림 5. 암호화 데이터와 키 데이터 제작. (a) 암호화 데이터, (b) 키 데이터.

했을 경우, 광학적인 복호화에 사용되는 최종 암호화 영상 $\hat{E}(u,v)$ 와 키 영상 $\hat{K}(u,v)$가 구해진다. 영상의 복호화는 암호화 영상과 키 영상의 곱을 통해 위상 성분의 합이 구해짐으로써 그림 6에서처럼 영상 F가 되는 원리로 수행된다.

복원된 영상 F는 푸리에 평면상에 복원된 영상이며 이를 푸리에 변환하고 공간 필터링하며 원 영상의 정보를 복호화할 수 있다.

IV. 단일 경로 시스템에 의한 복호화 과정

원 영상의 정보를 복호화하기 위해 암호화 영상 $\hat{E}(u,v)$와 키 영상 $\hat{K}(u,v)$를 그림 7의 입력으로 사용한다.

입력파 $R(u,v)$의 크기성분을 R, 위상성분을 $\exp(j\theta)$라 했을 때 푸리에 렌즈 L_2를 통과하기 전 암호화 영상과 키 영상을 통과한 신호는

$$\begin{aligned} R(u,v)\,\hat{E}(u,v)\,\hat{K}(u,v) &= R(u,v)\ \exp(j\pi E/nC)\ \exp(j\pi K/nC) \\ &= R(u,v)\ \exp[j\pi(E+K)/nC] \\ &= R\ \exp(j\theta)\ \exp(j\pi F^{+}_{real}/nC) \end{aligned} \tag{9}$$

와 같다. 만약, 위상 부호화시 C 값을 크게 했다면 식 (9)는

$$R\ \exp(j\theta)\ \exp(j\pi F^{+}_{real}/nC) \approx R\ \exp(j\theta)(1+j\pi F^{+}_{real}/nC) \tag{10}$$

와 같이 근사화되며, 이 신호는 렌즈 L_2를 통과한 후

$$\begin{aligned} &FT\{R\ \exp(j\theta)(1+j\pi F^{+}_{real}/nC)\} \\ &= FT\{R\ \exp(j\theta)+R\ \exp(j\theta)j\pi[F_{real}(u,v)-F_{min}]/nC\} \\ &= \delta(x,y)\ R\ \exp(j\theta)(1-j\pi F_{min}/nC) \\ &\quad + j\pi R\ \exp(j\theta)/nC\ \ FT\{F_{real}(u,v)\} \end{aligned} \tag{11}$$

로 푸리에 변환되어 나타난다. 식 (11)의 첫 번째 성분인 $\delta(x,y)R\ \exp(j\theta)(1-j\pi F_{min}/nC)$는 영차 위치에만 존재하므로 영차 성분을 차단하는 공간 필터를 통과시켜 억제할 수 있다. 이때 일정한 해상도(resolution)의 입력이 제안한 시스템에 사용될 경우엔 공간 필터의 차단영역 크기를 영상 크기에 따라 조절할 필요가 없으나, 해상도가 각각 다른 영상을 시스템의 입력으로 사용할 경우에 화소 즉 픽셀의 크기 자체가 달라지므로 이에 따라 공간 필터의 차단영역 크기를 조절할 필요가 있다. 따라서 공간 필터의 영차성분차단에 따른 최종 CCD 평면에 나타나는 신호는

$$\begin{aligned} O_{CCD}(x,y) &= |j\pi R\ \exp(j\theta)\,FT\{F_{real}(u,v)\}/nC|^2 \\ &= |j\pi R\ \exp(j\theta)/nC\ 0.5[f_z'(x,y)]\ \exp[jn'(x,y)]|^2 \\ &= (0.5\pi R/nC)^2[f_z'(x,y)]^2 \end{aligned} \tag{12}$$

이다. 여기서 $\exp[jn'(x,y)]$는 $FT\{\exp[jn(x,y)]\}$의 실수값에 대한 푸리에 변환 영상이며 $f_z'(x,y)$는 $F_{real}(u,v)$를 푸리에 변환했을 경우 출력평면에 나타나는 우 함수 특성의 실수(real and even) 영상이다. CCD 평면상에서 얻어진 $f_z'(x,y)$에는 원 영상 정보가 영차 위치를 중심으로 대칭적으로 존재하므로 이중 하나의 영역을 선택하고 선택한 영상에서 $0.5\pi R/nC$의 값을 보상하는 컴퓨터 후처리(post-processing) 통해 최종 복호화 영상을 얻을 수 있다.

V. 컴퓨터 모의 실험 및 분석

그림 8(a)는 128×128 화소 크기의 Lena영상을 원 영상으로 하여 영 삽입한 257×257 화소 크기의 영상이며, 이를 이용하여 암호화 영상과 키 영상을 생성하였다. 그림 8(b)는 영 삽입된 원 영상에 무작위 위상 영상을 곱하여 푸리에 변환한 후 최소값의 레벨을 0으로 한 실수 영상이다. 그림 8(b)의 영상을 그림 8(d)의 키 영상과 위상변조 XOR 연산 수행한 후 위상 부호화 과정을 거쳐 구한 최종 암호화 영상은 그림 8(c)로 나타내었으며 이 때 암호화 영상과 키 영상의 위상값들은 실제 눈에 보이지 않으므로 편의상 그레이 값 범위의 [0;255]로 대응시켜 표현하였다.

그림 8(c)와 그림 8(d)를 그림 1의 단일 경로 복호화 시스템의 입력으로 하여 CCD평면에 재생한 영상이 그림 9(a)이며, 그림 9(b)와 같이 거짓 키 영상으로 복호화할 경우 그림 9(c)와 같이 원 정보가 복호화 되지 않는다.

특정 요소나 환경의 변화가 복호화 영상 복원에 미치는 영향은 *MSE*(mean square error)이나 *PSNR*(peak signal to noise ratio)을 사용하여 분석가능하다. 제안한 암호화 방법에서 복호화 영상의 시각적 퀄러티(visual quality)는 C 값에 따라 식 (10)의 근사화가 어느 정도 되느냐에 큰 영향을 받으므로, C 값에 따른 복호화 영상의 시각적 특성을 좀 더 쉽고 직접적으로 나타내기 위해 *PSNR*(peak signal to noise ratio)값으로 분석하였다.[11,12]

-1	3	-1	2		2	2	2	3		1	5	1	5
2	3	-1	3		-1	-1	3	2		1	2	2	5
1	3	-3	-1		4	2	4	2		5	5	1	1
-1	-3	-1	2		3	4	3	3		2	1	2	5
E(u, v)					*K(u, v)*					*F*			

그림 6. 위상 성분의 암호화 데이터와 키 데이터를 이용한 영상의 복원 원리.

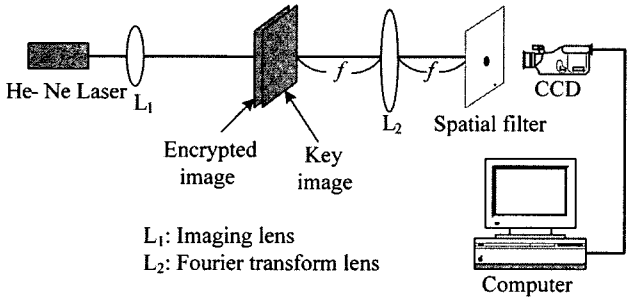
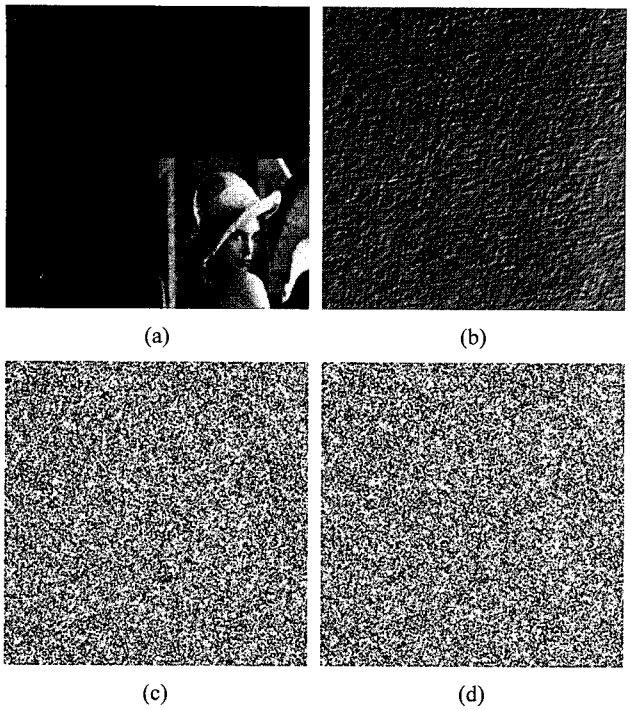
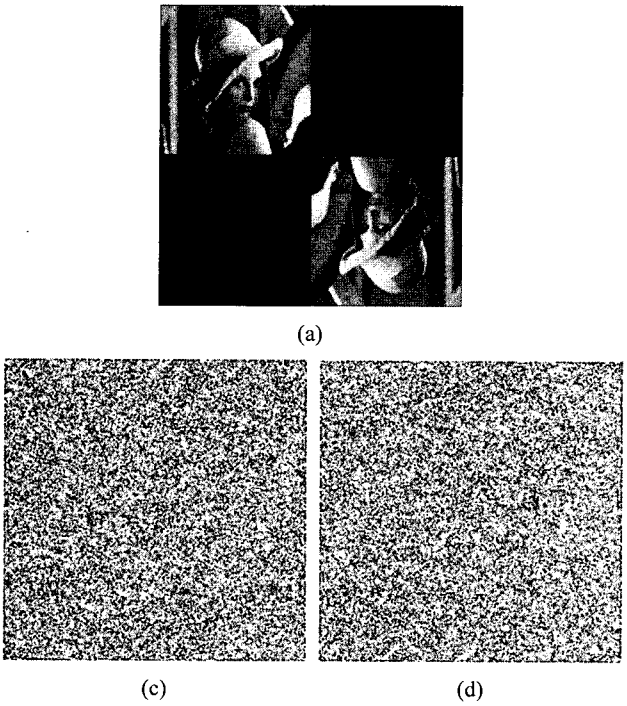


그림 7. 영상 복호화를 위한 단일 경로 시스템.



(a) (b) (c) (d)

그림 8. 컴퓨터 모의실험 영상. (a) 영 삽입된 원 영상, (b) 영상 (a)의 푸리에 변환 실수 영상, (c) 암호화 영상 (d) 키 영상.



(a) (c) (d)

그림 9. 컴퓨터 모의 실험 영상. (a) 복호화 영상, (b) 거짓 키 영상, (c) 거짓 키로 재생된 영상.

$$PSNR = 20\ \log\left(\frac{2^{n_{bit}}-1}{\left\{\frac{1}{NM}\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}\left[\|f_o(x,y)|-|f_o'(x,y)\|^2\right]\right\}^{1/2}}\right) \quad (13)$$

여기서 $f_o(x, y)$과 $f_o'(x, y)$는 원 영상과 C 값의 증가에 따른 복호화 영상을 각각 나타내며, $N\times M$은 원 영상의 화소수, n_{bit}는 화소를 표현하는 비트 수를 의미한다.

그림 10과 같이 복호화 영상의 *PSNR*은 C 값의 따라 비선형적으로 비례하며 C 값이 [0;20] 구간 안에서 *PSNR*이 급격하게 증가함을 알 수 있다. 또한 더 큰 *PSNR*을 위해 C 값을 계속 증가시킨다 할지라도 그림 4에서 나타나듯 *PSNR*은 그 증가폭이 둔화되어 나타난다. 이는 C 값을 크게 하여 암호화 데이터를 위상 부호화 했을 경우 복호화 영상의 시각적 퀄러티는 눈에 띄게 향상되지 않으며, 오히려 위상 부호화시 위상 범위를 줄여 실제 광소자로의 위상값 구현시 정밀한 위상 표현의 어려움을 초래하게 된다. 그림 10에서 C 값이 '1.2''일 때 괜찮은 시각적 퀄러티(acceptable visual qaulity)의 복호화 영상(≈20 dB)의 영상이, C 값이 '3.1' 일 때 높은 시각적 퀄러티(good visual quality)의 복호화 영상(≈30 dB)이 구해지며 이를 통해 C 값을 크게 하지 않고도, 즉 위상의 범위를 작은 값으로 줄이지 않아도 만족할 만한 복호화 영상이 나타남을 알 수 있다. 그림 3(a)는 위상 부호화시 C 값을 10으로 하였을 때의 복호화 영상이며 이 영상의 *PSNR*은 '42.23' dB이다.

제안한 암호화 방법은 기존의 공간 영역의 암호화 방법과는 달리 푸리에 영역의 암호화로 인해 암호화 영상의 정보가 손실되었을 경우에도 원 영상의 복호화가 가능하다. 그림 11(a), (b), (c)는 암호화 영상을 각각 25%, 50%, 75% 절단했을 때의 영상들이며, 그림 11(d), (e), (f)는 이를 이용해 CCD 평면의 복호화 영상들이다.

절단에 따른 원 영상 복원의 수치적인 값은 그림 6과 같이 원 영상과 복호화 영상간의 상관 효율(correlation efficiency, CE)로 나타내었다.

$$CE = \frac{COV(f, f')}{S_f S_{f'}} \quad (14)$$

여기서 $COV(f, f')$은 원 영상 f와 복호화 영상 f'간의 공분

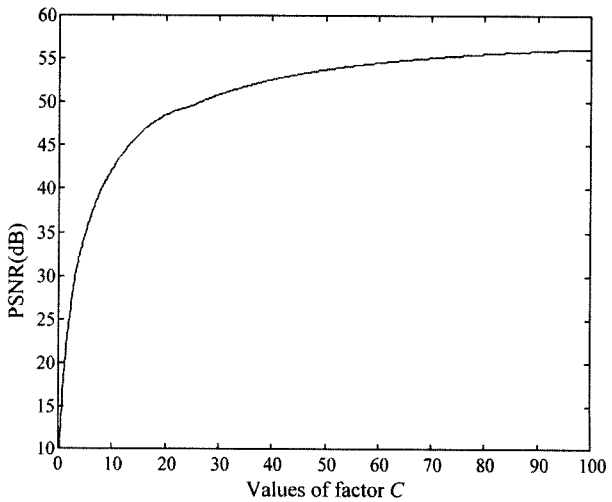


그림 10. C 값의 따른 복호화 영상의 PSNR.

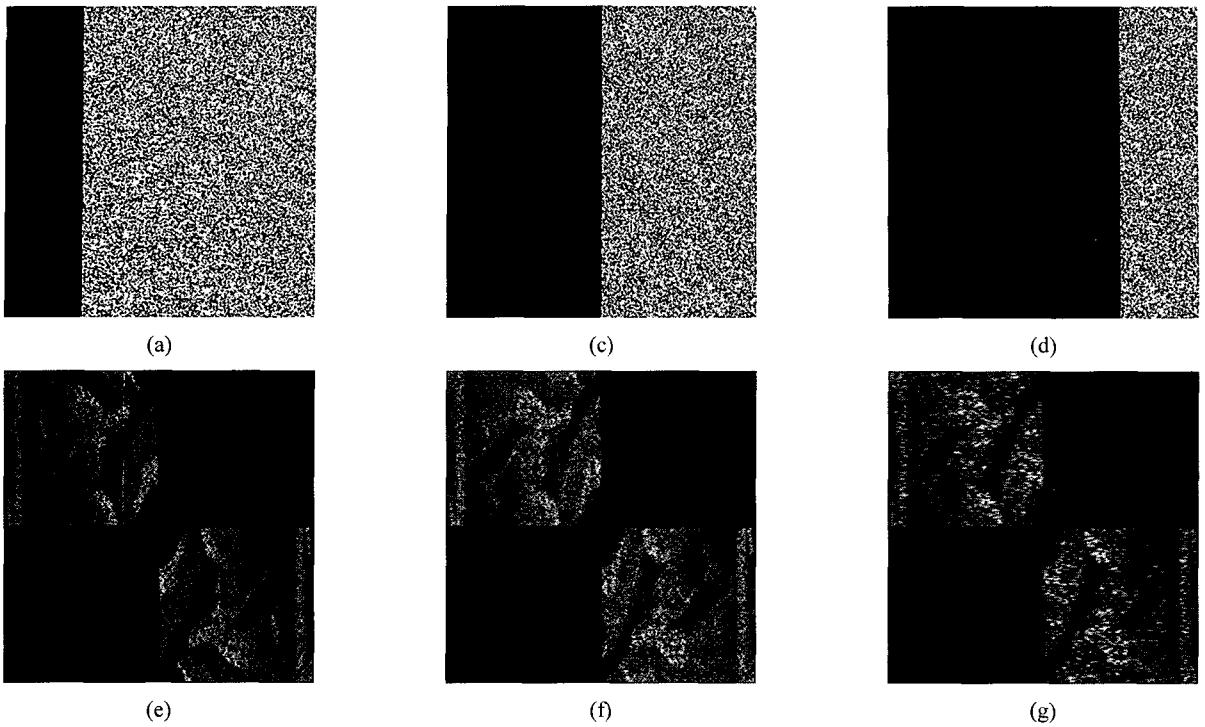


그림 11. 절단된 암호화 영상들과 CCD 평면상의 복호화 영상들: a) 25% 절단, (b) 50% 절단, (c) 75% 절단, (d) (a)에 의해 재생 된 영상, (e) (b)에 의해 재생된 영상, (f) (c)에 의해 재생된 영상.

산(covariance)을 의미하며, S_f와 $S_{f'}$은 두 영상 f와 f'의 표준 편차를 나타낸다. 푸리에 영역에서 생성된 암호화 영상의 절단에 따른 상관효율 값들과 기존의 공간 영역에서 생성된 암호화 영상의 절단에 따른 상관효율 값들을 식 (14)로 각각 구하고 이를 그림 12로 나타내어 복호화 영상의 복원 정도를 서로 비교하였다. 그림 12에서 실선은 푸리에 영역의 암호화 영상이 절단되는 비율에 따른 상관효율을, 점선은 공간 영역의 암호화 영상이 절단되는 비율에 따른 상관효율을 의미한다. 전체적으로 실선이 점선보다 위쪽에 위치하고 있으며 이는 제안한 푸리에 영역에서의 암호화 방법이 기존의 제안되었던 공간 영역에서의 위상 변조 XOR 암호화 방법에 비해 암호화 정보가 절단되었을 경우 더 좋은 재생 효율을 가짐을 보여준다.

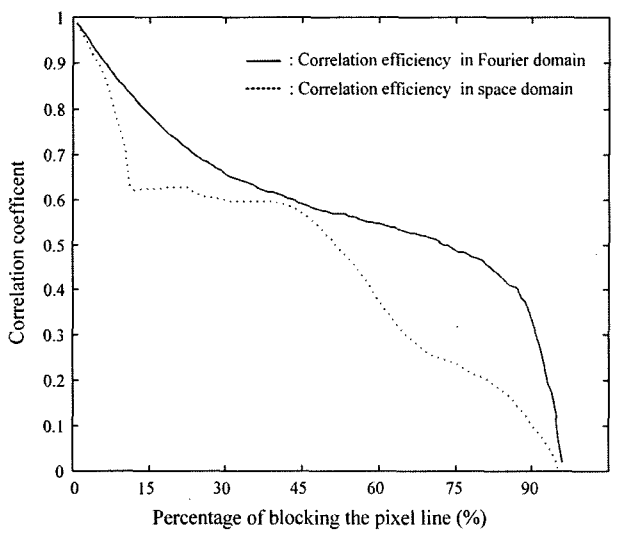


그림 12. 절단에 따른 원 영상과 복호화 영상의 상관 효율.

VI. 결 론

본 논문에서는 영 삽입된 원 영상을 푸리에 영역으로 변환하고 이를 위상 변조 XOR 연산으로 암호화함으로써 2-f 구조의 단일 경로 시스템으로 복호화 할 수 있는 암호화 시스템을 제안하였다. 푸리에 영역의 위상변조 XOR 암호화를 수행하여 암호화시 위상 그레이 정보의 암호화 영상을 생성하여 높은 정보 보안성을 확보하였고 더불어 정보 손실에도 강한 장점을 가지게 하였다. 또한 복호화 과정시 외부 진동이나 교란에 강한 단일 경로의 복호화 시스템을 통해 수행하여 간단히 복호화 정보를 시각화하였다. 컴퓨터 모의실험을 통해 복호화시 근사화로 인해 발생하는 복호화 영상의 시각적 퀄러티와 정보 손실에 대한 특성을 수치적으로 분석하였고, 제안한 암호화 과정 및 복호화 시스템의 구현 가능성과 타당성을 확인하였다. 마지막으로 현재 사용되는 광학장비의 성능개선과 그레이 위상 정보를 정확하게 표현할 수 있는 SLM과 위상 마스크의 식각 기술 향상이 이루어진다면 제안

한 방법의 효율적인 광 실험 구현이 가능할 것이라 생각된다.

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] 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.

[3] 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.

[4] 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, 6689-6694, 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.

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

[9] G. Situ and J. Zhang, "A lensless optical security system based on computer-generated phase only masks," *Opt. Commu*, vol. 232, 115-122, 2004.

[10] 신창목, 서동환, 김수중, "위상 변조 Exclusive-OR 연산을 이용한 광학적 암호화 방법," *한국광학회지*, 제 14권, 6호, 623-629, 2003.

[11] VG. R. Fowles, *Introduction to Modern Optics*(Dover Publications, New York, 2nd Ed., 1975.)

[12] T. J. Naughton, Y. Frauel, B. Javidi, and E. Tajahuerce, "Compression of digital holograms for three-dimensional object reconstruction and recognition," *Applied Optics*, vol. 41, no. 20, pp. 4124-4132, July, 2002.

Single Path Phase-only Security System using Phase-encoded XOR Operations in Fourier Plane

Chang-Mok Shin, Kyu-Bo Cho† and Soo-Joong Kim

chool of Electrical Engineering & Computer Science, Kyungpook National University, Daegu 702-701, Korea

†*E-mail: chb10040@ee.knu.ac.kr*

Duck-Soo Noh

School of Electronic Information & Communication Engineering., Kyungil University Kyungsan 712-701, Korea

(Received June 3, 2005, Revised manuscript July 14, 2005)

Phase-only encryption scheme using exclusive-OR rules in Fourier plane and a single path decryption system are presented. A zero-padded original image, multiplied by a random phase image, is Fourier transformed and its real-valued data is encrypted with key data by using XOR rules. A decryption is simply performed based on 2-*f* setup with spatial filter by Fourier transform for multiplying phase-only encrypted data by phase-only key data, which are obtained by phase-encoding process, and spatial filtering for zero-order elimination in inverse-Fourier plane. Since the encryption process is peformed in Fourier plane, proposed encryption scheme is more tolerant to loss of key information by scratching or cutting than previous XOR encryption method in space domain. Compare with previous phase-visualization systems, due to the simple architecture without a reference wave, our system is basically robust to mechanical vibrations and fluctuations. Numerical simulations have confirmed the proposed technique as high-level encryption and simple decryption architecture.

OCIS Codes : 070.2590, 100.1160, 110.5100, 120.5060.