논문 2005-42SD-6-5

다중 위상 분할과 위상 랩핑 방법을 이용한 광 암호화 시스템

(Optical security system using multi-phase separation and phase-wrapping method)

신 창 목*, 김 수 중**, 서 동 환***

(Chang Mok Shin, Soo Joong Kim, and Dong Hoan Seo)

요 약

본 논문에서는 exclusive-OR 연산을 기반으로 암호화된 그레이 영상에 위상 랩핑(phase-wrapping)과 다중 위상 분할(multi-phase separation)방법을 적용하여 광학적 복호화가 용이하도록 한 광 암호화 시스템을 제안하였다. 암호화시 그레이 영상을 이진 영상들의 합으로 분리한 후 각각의 이진영상을 이진 무작위 영상과 변형된 XOR(modified XOR) 연산을 수행하고, 연산된 이진 영상들과 이진 무작위 영상들을 따로 결합한 후 이를 위상 부호화하여 암호화 영상과 키 영상을 만든다. 복호화시 암호화 영상과 키 영상의 위상 정보를 광소자로 구현할 경우 제어 가능한 위상 범위의 현실적 한계로 인해 그레이 정보 복원에 제약이 따른다. 따라서 위상 랩핑(phase-wrapping) 방법으로 암호화 영상과 키 영상의 위상 범위를 줄이고, 다중 위상 분할(multi-phase separation)로 이 영상들을 낮은 레벨의 위상영상들로 분할함으로써, 위상범위가 제한된 광소자로도 그레이 영상의 복호화가 가능하도록 하였다. 복호화는 암호화 영상과 키 영상의 곱을 기준파와 간섭시켜 간단히 구현하며, 컴퓨터 모의 실험을 이용해 제안한 방법의 타당성과 복호화시 위상 범위의 제한에 따른 영향을 분석하였다.

Abstract

In this paper, we proposed an optical security system based on a gray-image exclusive-OR encryption using multi-phase separation and phase-wrapping method. For encryption, a gray image is sliced into binary images, which have the same pixel value, and these images are encrypted by modified XOR rules with binary random images. The XORed images and the binary images respectively combined and converted into full phase images, called an encrypted image and a key image. For decryption, when the encrypted image and key image are used as inputs on optical elements, practically due to limited controllability of phase range in optical elements, the original gray image cannot be efficiently reconstructed by these optical elements. Therefore, by decreasing the phase ranges of the encrypted image and key image using a phase-wrapping method and separating these images into low-level phase images using multi-phase separation , the gray image can be reconstructed by optical elements which have limited control range. The decrytion process is simply implemented by interfering a multiplication result of encrypted image and key image with reference light. The validity of proposed scheme is verified and the effects, which are caused by phase limitation in decryption process, is analyzed by using computer simulations.

Keywords: 광 암호화(optical security), 위상 랩핑(phase-wrapping), 다중 위상 분할(multi-phase separation)

I. 서 론

최근에 정보의 암호화를 위한 광학적 시스템이 광의 병렬성과 고속성에 따른 특성으로 인해 많이 연구되어 지고 있다[1-12]. 광 암호화 시스템은 다양한 부호화 방법을 이용하여 정보를 암호화하며, 원 영상의 세기 정보를 부호화하는 크기 기반 암호화(amplitude-based encryption)방법, 세기 정보를 위상 정보로 변조하는 위상 기반 암호화(fully phase-based encryption)방법, 그리고 세기 정보를 빛의 편광상태로 부호화하는 편광 암호화(polarization encryption) 방법 등을 주로 이용한다[1-4].

* 정회원, ** 평생회원, 경북대학교 전자전기컴퓨터공학부
(Optical Signal Processing Lab, School of Electrical Engineering and Computer Science, Kyungpook Nat'l University)
*** 정회원, 한국해양대학교 전기전자공학부
(Division of Electrical and Electronics Engineering, Korea Maritime University)
접수일자 : 2004년11월21일, 수정완료일 : 2005년5월4일

위상 기반 암호화 방법은 크기 기반 암호화 방법에 비해 잡음에 영향을 덜 받으며, 위상 정보만을 이용하기 때문에 기록이나 저장이 용이하다[2]. 또한, 위상정보는 시각적으로 투명하므로 위조자가 세기 검출기로 쉽게 암호화 정보를 복사할 수 없으며, 암호화된 위상 정보를 전기적으로 위상을 조절할 수 있는 공간 광 변조기(spatial light modulator; SLM)와 같은 광소자로 구현할 경우 실시간 암호화나 복호화가 가능하다. 그러나 위상 기반 암호화 시스템의 효율적인 구현을 위해선 광소자들의 위상 표현 정확도나 위상 범위 등이 고려되어야하며, 위상 기반 암호화 방법만으로 시스템을 구현할 경우 간섭 기교(interferemetic technique)와 같은 정밀한 방법으로 암호화된 위상 정보의 추출 및 해석이 이루어질 수도 있으므로 효과적인 암호화 알고리즘과 결합을 통해 암호화 수준을 높일 필요가 있다[9]. 이러한 효과적인 암호화 알고리즘 중에는 광 exclusive-OR (XOR) 알고리즘이 있다[4,7-8]. Han 등은 광 XOR 알고리즘을 바탕으로 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[8]. 위 방법으로 암호화된 그레이 영상은 광학적 구현 시 디지털적으로 다시 이진 영상들로 나누어야 하는 과정이 필요하고, 암호화된 그레이 영상 또한 8개의 암호화된 이진 영상으로 쉽게 나누어지므로, 불법 사용자가 각각의 암호화된 이진 영상을 통해 원 영상의 정보를 추정하거나 접근할 수 기회를 가질 수 있다.

본 논문에서는 변형된 XOR 연산(modified XOR operation)을 기반으로 하여 그레이 영상을 암호화하고, 위상 랩핑 (phase-wrapping)과 다중 위상 분할 (multi-phase separation)방법을 암호화된 영상에 적용함으로써 높은 암호화 수준을 유지할 뿐만 아니라 위상 조절 범위가 제한된 광소자로도 그레이 영상의 복원이 가능한 광 암호화 시스템을 제안하였다.

그레이 영상의 암호화를 위해 우선 그레이 영상을 동일한 화소값을 가지는 이진 영상들로 나눈 후 서로 다른 이진 무작위 영상들과 변형된 XOR 연산을 수행하여 암호화된 이진 영상을 생성한다. 이 때 이진 무작위 영상들을 서로 독립적인 백색잡음이라고 한다면, 변형된 XOR연산에 의해 암호화된 이진 영상들 또한 독립적인 백색잡음의 분포를 가지므로, 암호화된 이진 영상들과 이진 무작위 영상들을 각각 따로 분리해 결합하면 중심극한 정리(central limit theorem)에 의해 가우시안 분포의 암호화 데이터와 키 데이터를 얻을 수 있다. 이 데이터들을 위상 변조하여 광학적 복호화에 쓰이는 최종 암호화 영상과 키 영상을 생성한다. 그러나 그레이 영상 복원을 위해 그레이 값의 범위를 가지는 암호화 데이터와 키 데이터를 위상 부호할 경우 광소자의 현실적인 위상 표현 한계 때문에 광학적 구현에 장애가 된다. 그러므로 위상 변조 전 위상 랩핑(phase-wrapping)을 이용해 데이터들의 값의 범위를 줄이고, 위상 부호화된 영상에 다중 위상 분할(multi-phase separation)을 적용하여 위상 조절 범위가 제한된 광소자로도 그레이 영상의 복원이 가능하도록 하였다.

복호화는 암호화 영상과 키 영상의 단순 곱에 기준파를 간섭시켜 구현하며, 원 영상 복원 시 간단한 위상 시각화 시스템(phase-visualization system)인 마흐 젠더(Mach-Zehnder)간섭계로 구현하였다[12]. 제안한 암호화 시스템의 타당성 및 복호화시 위상 범위의 제한에 따른 영향을 컴퓨터 모의실험을 통해 확인하고 분석하였다.

Ⅱ. 암호화 과정

1. 그레이 영상의 분리

그레이 영상의 화소들은 매우 다양한 값의 분포를 가지며, 이러한 다양한 값 중 동일한 값들을 하나의 영상으로 분리하여 이진영상으로 나타낼 경우 그레이 영상을 그림 1의 예와 같이 이진 영상의 합으로 표현할 수 있다.

그러므로 최소 그레이 화소값 m과 최대 그레이 화소값 n을 가지는 원 영상 $O_{m,n}(x, y)$을 이진 영상으로 표현하면

$$O_{m,n}(x,y) = mb_m(x,y) + (m+1)b_{m+1}(x,y) + \cdots + (n-1)b_{n-1}(x,y) + nb_n(x,y) \quad (1)$$

와 같다. 여기서 b_m, b_{m+1}, ⋯, b_{n-1}, b_n은 0 또는 1의 값을 갖는 이진 영상들 즉 슬라이드 영상들을, m, m+1,⋯, n-1, n은 원 영상의 그레이 화소값을 나타낸다.

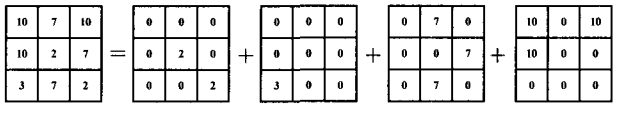

그림 1. 3×3 그레이 영상의 이진 분리.
Fig. 1. Binary slice of 3×3 gray image.

2. 변형된 XOR 연산에 의한 영상 암호화

나누어진 슬라이드 영상들 b_m, b_{m+1}, ⋯, b_{n-1}, b_n을 각각 -1과 1의 값을 가지는 이진 무작위 영상들 r_m, r_{m+1}, ⋯, r_{n-1}, r_n과 변형된 XOR 연산을 하여 새로운 이진 암호화 영상 e_m, e_{m+1},⋯, e_{n-1}, e_n 을 만들 수 있으므로 임의의 화소값 k를 가지는 슬라이드 영상을 이진 무작위 영상과 이진 암호화 영상으로 구하면

$$b_k(x,y)=\frac{1}{2}|e_k(x,y)-r_k(x,y)| \tag{2}$$

이 되고, 이 때 사용되는 변형된 XOR 연산규칙은 표 1과 같다.

표 1에서 p_k 와 q_k는 0과 1을 가지는 이진 무작위 영상과 XOR된 영상을 각각 나타내며, 기호 ⊕는 XOR연산을 의미한다. 식 (2)를 이용하여 원 영상 $O_{m,n}$를 표현하면

$$\begin{aligned} &O_{m,n}\\ &=1/2\{m|e_m-r_m|+(m+1)|e_{m+1}-r_{m+1}|+\\ &\quad\cdots+(n-1)|e_{n-1}-r_{n-1}|+n|e_n-r_n|\} \end{aligned} \tag{3}$$

과 같다. 그림 1과 같이 서로 다른 슬라이드 영상의 화소값들은 대수적 연산 시 서로 겹치거나 영향을 주지 않으므로 식 (3)에서 각각의 절대값 기호를 전체 절대값 기호로 대신하여

$$\begin{aligned} &O_{m,n}\\ &=1/2|m(e_m-r_m)+(m+1)(e_{m+1}-r_{m+1})+\\ &\quad\cdots+(n-1)(e_{n-1}-r_{n-1})+n(e_n-r_n)| \end{aligned} \tag{4}$$

로 나타낼 수 있다.

식 (4)에서 이진 암호화 영상들 e_m, e_{m+1},⋯, e_{n-1}, e_n과 이진 무작위 영상들 r_m, r_{m+1}, ⋯, r_{n-1}, r_n을 분리한 후 각각 더하여 구한 그레이 값의 암호화 데이터 $E(x, y)$와 키 데이터 $K(x, y)$는

표 1. XOR 연산 규칙들과 변형된 XOR 연산 규칙들.
Table 1. XOR rules and modified XOR rules.

XOR 연산 ($b_k \oplus p_k = q_k$)			변형된 XOR 연산 ($b_k \oplus r_k = e_k$)			슬라이드 영상 b_k 의 수식적 복원
b_k	p_k	q_k	b_k	r_k	e_k	$b_k = \lvert e_k - r_k\rvert/2$
0	0	0	0	1	1	0
0	1	1	0	-1	-1	0
1	0	1	1	1	-1	1
1	1	0	1	-1	1	1

$$\begin{aligned} E(x,y)&=\frac{1}{2}[me_m+(m+1)e_{m+1}+\cdots+ne_n]\\ K(x,y)&=-\frac{1}{2}[mr_m+(m+1)r_{m+1}+\cdots+nr_n] \end{aligned} \tag{5}$$

와 같다. $E(x, y)$와 $K(x, y)$는 가우시안 백색잡음 분포의 특성을 가지고 있으므로 XOR연산을 기본으로 암호화 되었다 할지라도 키 데이터 없이 암호화 데이터만으로는 원 영상의 정보를 얻는 것이 거의 불가능하다.

3. 위상 부호화와 위상 랩핑

광학적 구현을 위해 암호화 데이터 $E(x, y)$와 키 데이터 $K(x, y)$를 위상 부호화하여

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

과 같이 암호화 영상 $\mathcal{E}(x, y)$와 키 영상 $\mathcal{K}(x, y)$를 구한다. 이 때 $1/n$은 원 영상을 정규화하여 $[0; \pi]$ 범위에서 나타나게 하는 역할을 한다. 암호화 영상과 키 영상을 그대로 광학적으로 구현할 경우 광소자의 위상조절범위의 현실적 한계 때문에 암호화 영상과 키 영상의 위상값이 제대로 표현되지 않으므로, 그레이 원 영상의 복원이 어렵다. 그러므로 위상 랩핑 방법을 이용해 위상 부호화된 영상들의 위상값의 범위를 줄여줌으로써 광소자의 위상 표현 제약에 따르는 문제점을 다소 해결할 수 있다.

제안한 위상 랩핑 방법은 기본적으로 위상 함수의 주기적 특성을 이용하며 위상 함수의 주기적 특성을 수식적으로 나타내면

$$\exp[j\pi f(x,y)]=\exp\{j[\pi f(x,y)+2\pi]\} \tag{7}$$

와 같다. 여기서 $f(x, y)$는 1로 정규화된 임의의 영상을 나타낸다. 위상 랩핑 과정은 다음과 같다.

원 영상 정보는 암호화 영상$\tilde{E}(x,y)$과 키 영상 $\tilde{K}(x,y)$의 곱에 의해 나타나므로

$$\begin{aligned} &\tilde{E}(x,y)\times\tilde{K}(x,y)\\ &=\exp(j\pi\frac{E}{n}+j\pi\frac{K}{n})\\ &=\exp(j\pi\{IN[\frac{E}{n}]+DE[\frac{E}{n}]+\\ &\qquad IN[\frac{K}{n}]+DE[\frac{K}{n}]) \end{aligned} \tag{8}$$

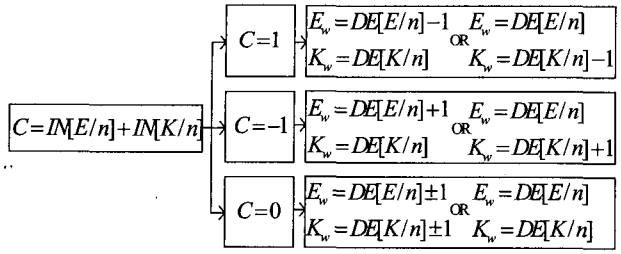

그림 2. 위상 랩핑 규칙의 블록 다이어그램.
Fig. 2. The block diagram of the phase-wrapping rules.

로 표현되며, 여기서 $IN[\cdot]$와 $DE[\cdot]$는 각각 입력 정보의 정수부분과 소수부분을 나타내는 함수이다. 곱에 의한 위상 정보는 $1/n$의 정규화로 인해 $[-\pi, \pi]$ 범위 내에서만 존재하므로 $IN[E/n]$와 $IN[K/n]$의 합은 '-1', '0' 그리고 '1'의 세 가지 경우밖에 없다. 따라서 식 (8)의 위상값에 -2π나 2π를 더하면

$$\begin{aligned}&\tilde{E}(x,y)\times\tilde{K}(x,y)\\&=\exp\left(j\pi\left\{IN[\frac{E}{n}]+DE[\frac{E}{n}]+\right.\right.\\&\qquad\left.\left.IN[\frac{K}{n}]+DE[\frac{K}{n}]\mp j2\pi\right)\right\}\qquad(9)\\&=\exp\left(j\pi\left\{\pm1+DE[\frac{E}{n}]+DE[\frac{K}{n}]\mp2\pi\right\}\right)\\&=\exp\left(j\pi\left\{\mp1+DE[\frac{E}{n}]+DE[\frac{K}{n}]\right\}\right)\end{aligned}$$

와 같이 $IN[E/n]$와 $IN[K/n]$항이 제거된다. 식 (9)로부터 원 영상은 '-1', '0', 그리고 '1'의 세 가지 정수와 암호화 데이터 및 키 데이터의 소수부분의 합으로도 복원할 수 있다. 그러므로 그림 2와 같은 위상 랩핑 규칙을 이용해 데이터들의 소수부분에 정수 '-1'이나 '1'을 더하여 정수 범위가 줄어든 암호화 데이터 $E_w(x, y)$와 키 데이터 $K_w(x, y)$를 구하고 이를 다시 위상 부호화하여

$$\begin{aligned}\tilde{E}_w(x,y)&=\exp\left[j\pi E_w(x,y)\right]\\\tilde{K}_w(x,y)&=\exp\left[j\pi K_w(x,y)\right]\end{aligned}\qquad(10)$$

과 같이 최종 위상 랩핑된 암호화 영상 $\tilde{E}_w(x,y)$와 키 영상 $\tilde{K}_w(x,y)$를 생성한다.

4. 다중 위상 분할

위상 범위가 줄어든 $\tilde{E}_w(x,y)$와 $\tilde{K}_w(x,y)$를 각각 하나의 광소자로 구현할 경우 영상의 위상값들은 광소자의 위상 조절 범위내에서 정확하게 표현되어져야하지만 현실적으로 위상 레벨이 제한된 하나의 광소자로는 $\tilde{E}_w(x,y)$나 $\tilde{K}_w(x,y)$의 위상 범위를 균등하게 나타내기 어렵다. 또한 영상의 위상 레벨을 광소자의 제한된 위상레벨로 양자화(quantization)하여 낮출 경우 하나의 광소자로 위상 표현은 가능하나 양자화로 인한 정보 손실로 복호화시 그레이 정보 복원이 힘들다.

따라서 영상의 위상 레벨을 그레이 정보의 복원이 가능한 만큼 양자화한 후 이를 다시 여러 위상 영상으로 나누어 표현하는 다중 위상 분할을 수행함으로써 위상 레벨이 제한된 광소자들로 그레이 정보를 복호화 할 수 있다.

$$\begin{aligned}&\exp(j\pi f_{q_1,q_2,\cdots,q_n})\\&\quad n\text{ 레벨 양자화}\\&=\exp(j\pi f^{(1)}_{q_1,\cdots,q_k})\times\ \exp(j\pi f^{(2)}_{q_{k+1},\cdots,q_{2k}})\times\qquad(11)\\&\quad k\text{ 레벨 양자화}\qquad k\text{ 레벨 양자화}\\&\cdots\ \times\exp(j\pi f^{(L)}_{q_{k-n-1},\cdots,q_n})\\&\qquad k\text{ 레벨 양자화}\end{aligned}$$

위 식 (11)은 n 레벨로 양자화한 위상 영상을 k레벨의 위상 영상들로 L개 수 만큼 다중 위상 분할한 것을 나타내며 이 때 $\sum_1^L k$ 는 n과 같다. 다중 위상 분할에서 생성되는 새로운 위상 영상의 수는 광소자의 위상 레벨에 반비례하는데 이는 광소자의 위상 레벨이 낮을 경우 위상 영상의 수를 늘여 낮은 위상 레벨을 보완함으로써 원 영상을 복원하기 위함이다. 제안한 암호화 알고리즘은 화소 대 화소의 일대일 대응을 이용하므로 최종 암호화 영상 $\tilde{E}_w(x,y)$와 키 영상 $\tilde{K}_w(x,y)$의 위상값을 각각 다른 레벨로 양자화하여도 원 영상 복호화가 가능하다. 그러므로 이러한 양자화 특성과 다중 위상 분할을 이용하여 사용자에게는 낮은 레벨로 양자화한 하나의 암호화 영상을 할당하고 시스템 내에는 높은 레벨로 양자화한 후 다중 위상 분할한 낮은 레벨의 여러 키 영상들을 둠으로써 낮은 위상 레벨의 광소자로도 그레이 정보의 복호화가 가능한 효율적인 광 암호화 시스템을 구현할 수 있다.

III. 복호화 과정

복호화 기법 중 위상 영상을 세기 영상으로 변환하는 방법에는 여러 가지가 있으며, 본 논문에서는 그 중 그림 3과 같이 간섭의 원리를 바탕으로 한 마흐젠더(Mach-Zehnder)간섭계로 영상을 복호화 하였다.

간섭계의 한쪽 경로에 그림 3과 같이 암호화 영상과

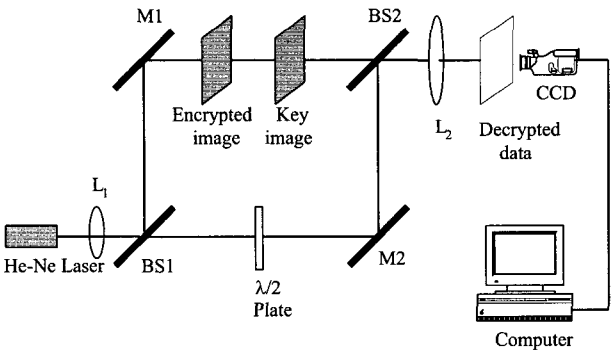

그림 3. 영상 복호화를 위한 마흐젠더 간섭계: M1, M2 거울; BS1, BS2 분광기, L1 줄맞춤 렌즈, L2 초점 렌즈

Fig. 3. Mach-Zehnder interferometer for image decryption: M1, M2, mirrors; BS1, BS2, beam splitters; L1, collimating lens; L2, imaging lens.

키 영상을 직렬로 놓고, 다른 경로에 λ/2 위상 지연판을 통과한 기준 파와 간섭시켰을 때 *CCD* 평면에서 관찰되는 복호화 영상은

$$\begin{aligned} & O_{CCD}(x,y) \\ & = |R(x,y)\exp(j\pi) + R(x,y)\times \\ & \quad E_w(x,y)\ K_w(x,y)|^2 \\ & = |R(x,y)\exp(j\pi)|^2\ |1+\exp(-j\pi)\times \\ & \quad E_w(x,y)\ K_w(x,y)\ |^2 \\ & = |R(x,y)\exp(j\pi)|^2|1-\exp(-j\pi)\times \\ & \quad \exp[j\pi E_w(x,y)]\exp[j\pi K_w(x,y)]|^2 \\ & = |R(x,y)|^2\{2-2\cos[\pi E_w(x,y)+\pi K_w(x,y)]\} \end{aligned} \tag{12}$$

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

$$\begin{aligned} & R(x,y) = E\ \exp(j\theta) \\ & |R(x,y)| = |E\exp(j\theta)|^2 = |E|^2 \end{aligned} \tag{13}$$

과 같다. 식 (12)에서 코사인의 성분 $E_w(x, y)+K_w(x, y)$는 정규화된 원 영상이므로 CCD의 출력영상은 코사인 함수에 의해 비선형 특성으로 나타난다. 비선형 영상에 $\cos^{-1}$함수 등의 컴퓨터 후처리(post-processing)를 수행하면 최종 복호화 영상을 얻을 수 있다.

Ⅳ. 컴퓨터 모의 실험 및 분석

암호화를 위해 그림 4(a)와 같이 최소 화소값 26, 최대 화소값 238인 256×256 화소크기의 'Lena'영상을 원 영상으로 사용하였다. 그림 4(b)와 4(c)는 각각 식 (5)의 의해 위상 랩핑을 거치지 않고 생성된 암호화 데이터와 키 데이터이며, 이를 위상 부호화한 후 식 (12)에 의해 복호화한 영상은 그림 4(d)와 같다. 그림 4(e)는 비선형 특성의 그림 4(d)를 컴퓨터 후처리한 후 구한 최종 복호화 영상이다. 암호화 데이터와 키 데이터는 균일한 백색잡음 분포의 이진·무작위 영상들의 결합으로 생성되므로 그림 5와 같이 가우시안 백색 잡음 분포 특성을 나타낸다.

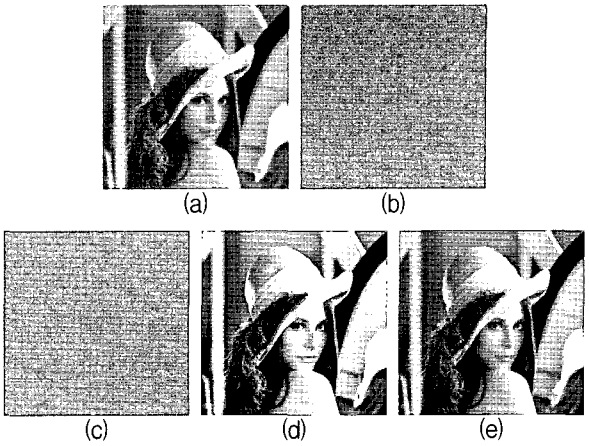

그림 4. 컴퓨터 모의 실험 영상: (a) 원 영상, (b) 암호화 데이터, (c) 키 데이터 (d) CCD 평면 복호화영상 (e) 후처리 복호화 영상

Fig. 4. Computer simulation images: (a) original image, (b) encrypted data, (c) key data, (d) decrypted image on CCD plane (e) decrypted image by post-processing

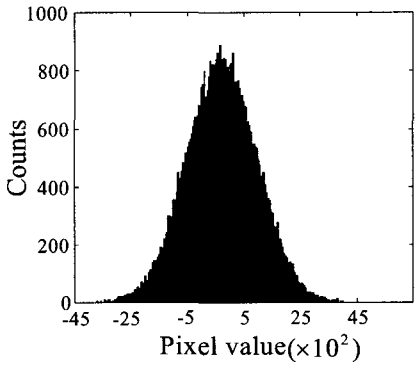

그림 5. 암호화 데이터의 히스토그램

Fig. 5. Histogram of encrypted data.

그림 5에서 암호화 데이터 및 키 데이터는 대략 [-4400; 4100]의 범위의 값을 가지며 이를 위상 랩핑하여 n값을 곱한 경우 [-470; 470] 범위의 데이터들인 그림 6(a)와 (b)와 같이 나타난다. 그러므로 위상 랩핑을

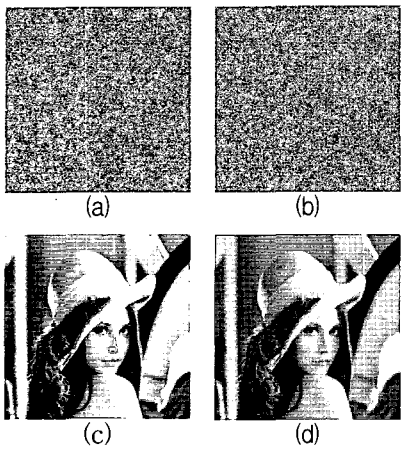

그림 6. 위상 랩핑 후의 영상들: (a) 암호화 데이터, (b) 키 데이터, (c) CCD 평면 복호화 영상, (d) 후처리 복호화 영상

Fig. 6. Phase-wrapped images: (a) encrypted data, (b) key data, (c) decrypted image on CCD plane, (e) decrypted image by post-processing

수행할 경우 기존 데이터의 범위를 약 1/10 정도 줄일 수 있다. 위상 랩핑된 암호화 데이터와 키 데이터를 위상 부호화하여 복호화한 영상은 그림 6 (c)와 (d)와 같다.

그림 4와 6의 복호화 영상 비교를 통해 위상 랩핑 방법은 복호화된 영상의 질을 거의 변화시키지 않고 데이터의 범위를 줄여줌을 확인할 수 있다.

광학적 복호화를 위해 데이터를 실시간으로 위상 부호화할 경우 즉 예를 들어 SLM등으로 위상을 제어한다면 그림 4(b)와 (c)는 14 비트 즉 16384 레벨의 위상이 필요한 반면, 그림 6(a)와 (b)는 '10' 비트 즉 1024 레벨의 위상만으로 그레이 영상을 복원할 수 있다. 그러나 위상 랩핑을 통해 위상 레벨을 줄였다 할지라도 현실적으로 단일 회절 소자로 제어 가능한 위상 레벨은 최대 약 64 레벨정도이므로 실제 위상 구현을 위해선 데이터들의 값에 대한 양자화가 필요하다[10].

데이터들의 값을 균일 양자화(uniform quantization) 했을 경우 복원되는 영상의 시각적 퀄러티(visual quality)는 *PSNR*(peak signal to noise ratio)을 이용해 정량적 지표로 나타내었다.

$$PSNR = 20 \log_{10} \left\{ \frac{2^n - 1}{\sqrt{\frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \| f_o(x,y) | - | f_o'(x,y) \|^2}} \right\} \quad (14)$$

여기서 $f_o(x, y)$는 데이터를 양자화하지 않은 경우의 복호화 영상을, $f_o'(x, y)$는 양자화 했을 경우의 복호화 영상이다. M과 N은 재생된 영상의 픽셀 크기이며, n은 $f_o(x, y)$의 한 화소 비트수를 나타낸다.

암호화 데이터와 키 데이터를 다양한 값으로 양자화 했을 경우 위상 랩핑의 적용에 따라 달라지는 *PSNR*값은 표 2와 같다.

표 2로부터 데이터를 위상 랩핑한 후 양자화 할 경우 16레벨에서도 괜찮은 시각적 퀄러티(acceptable visual quality)의 복호화 영상(≈20 dB)을 얻을 수 있으며, 64 레벨 정도에서는 높은 시각적 퀄러티를 가진 영상(≧

표 2. 양자화시 위상 랩핑 유무에 의한 PSNR 비교

Table 2 The comparison of PSNR values, according to whether applying phase-wrapping method or not, in different quantization.

양자화 레벨(Q)	후처리 복호화 영상의 *PSNR* (dB)	
	위상 랩핑 전	위상 랩핑 후
4	5.85	7.40
8	5.99	14.06
16	6.29	19.51
32	6.97	24.73
64	8.62	31.73
128	17.83	37.34
256	23.92	43.11
512	29.94	47.33

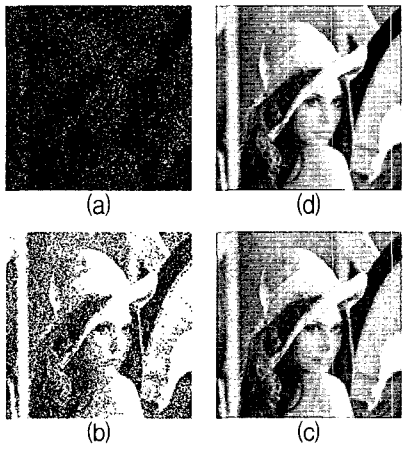

그림 7. 양자화 레벨 Q에 따른 복호화 영상들:
(a) 위상랩핑 전 Q가 16일 때 복호화 영상,
(b) 위상랩핑 전 Q가 64일 때 복호화 영상,
(c) 위상랩핑 후 Q가 16일 때 복호화 영상,
(d) 위상랩핑 후 Q가 64 일 때 복호화 영상

Fig. 7. Decrypted images according to different quantization levels: (a) decrypted image with Q=16 before phase wrapping (b) decrypted image with Q=64 before phase wrapping, (c) decrypted image with Q=16 after phase wrapping, (d) decrypted image with Q=64 after phase wrapping.

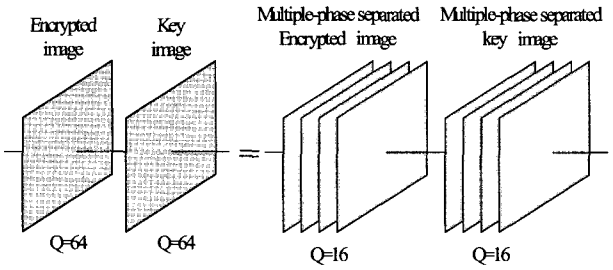

그림 8. Q가 64인 암호화 영상과 키 영상의 다중 위상 분할

Fig. 8. Multi-phase separation of encrypted image andkey image with Q=64.

30dB)의 복호화가 가능함을 알 수 있다. 이에 대한 영상들은 그림 7로 나타내었다.

위상 랩핑 후 양자화하여 위상 부호화한 영상에 다중 위상 분할을 적용하면 낮은 레벨의 영상들의 결합으로 시각적 퀄러티를 높인 복호화 영상을 얻을 수 있다. 예를 들어 그림 8과 같이 64레벨로 양자화한 암호화 영상과 키 영상을 각각 16레벨로 다중 위상 분할할 경우 각각 4개씩의 낮은 레벨의 위상 영상을 일렬로 나열함으로써 64레벨의 *PSNR*을 가진 복호화 영상을 간단히 얻을 수 있다. 그러나 실제 위상 영상의 간섭 시 암호화 영상과 분할된 키 영상의 화소 사이즈를 작게 하여 제작한 경우, 영상간의 간격이 조금이라도 있으면 두 영상간의 위상이 제대로 간섭되었다할지라도 회절 현상에 의해 출력평면에서 재생된 이미지의 효율은 상당히 떨어진다. 그러므로 영상간의 픽셀을 정확히 일치시켜 완전히 포갠 후(superimposed) 간섭시켰을 경우에는 암호화 영상과 분할된 키 영상의 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.

암호화 영상과 키 영상을 다르게 양자화 했을 경우에도 영상이 복호화되므로 암호화 영상은 낮을 레벨의 하나의 영상으로 양자화하고 키 영상은 낮은 레벨을 가지는 여러 개의 키로 다중 위상 분할하면 효율적인 시스템 구현이 가능하다.

그림 9는 4 레벨, 8 레벨, 16 레벨로 각각 양자화한 하나의 암호화 영상을 4 레벨, 8 레벨, 16 레벨로 각각 양자화한 다중 위상 분할 키 영상으로 복호화 했을 때, 다중 위상 분할 키 영상 수의 증가에 따라 변화하는 *PSNR*값을 나타낸 것이다.

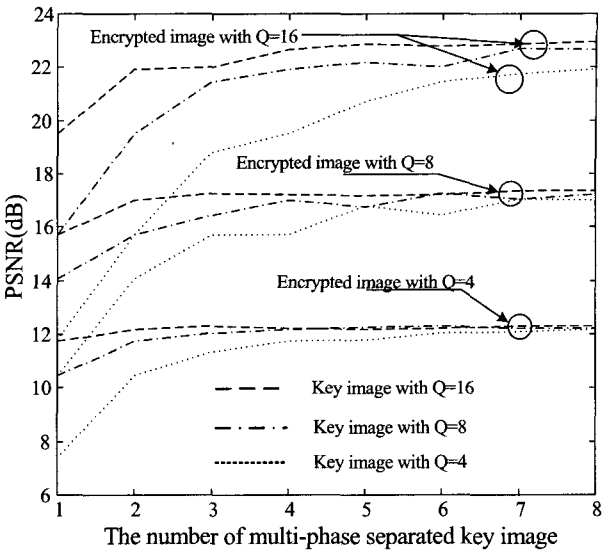

그림 9. 다중 위상 분할 키 영상 수 변화에 의한 PSNR

Fig. 9. PSNR values according to the number of multi-phase separated key image.

그림 9로부터 암호화 영상의 양자화 레벨이 높을수록 복호화 영상의 *PSNR*값은 다중 위상 분할된 키 영상의 수에 민감하게 좌우되며, 암호화 영상의 양자화 레벨이 고정되어 있으므로, 키 영상의 수를 늘여서 *PSNR*값을 높이는 데는 한계가 있음을 알 수 있다. 따라서 원하는 *PSNR*값을 효율적으로 얻기 위해선 소자의 위상 한계 레벨에 따라 다중 위상 분할 영상의 수를 적절히 고려하여 위상 레벨과 분할 영상 수를 고려해야 함을 알 수 있다.

Ⅳ. 결 론

본 논문에서는 간단한 XOR 연산과 대수식을 결합하여 그레이 영상을 암호화하고 암호화 영상에 위상 랩핑 방법과 다중 위상 분할을 적용하여 위상 레벨의 한계가 있는 소자로 그레이 영상의 복원이 가능한 광 암호화 시스템을 제안하였다. 암호화된 영상은 기본적으로 위상 영상이므로 세기 검출기로 쉽게 복제가 불가능 할 뿐만 아니라 위상값을 추출한다할지라도 키 영상의 정보 없이는 복원이 거의 불가능하므로 높은 암호화 수준을 유지한다. 현실적으로 위상 조절의 한계가 있는 소자로 그레이 영상을 복호화하기 위해 암호화 영상과 키 영상의 양자화를 통한 복원 영상의 PSNR을 분석하여 제안한 위상 랩핑 방법의 타당성을 확인하였고, 키 영상의 다중 위상 분할 시 키 영상의 수에 따라 달라지는 PSNR값을 비교 분석하여 보다 효율적 시스템 구현방

법을 제안하였다. 마지막으로 컴퓨터 모의실험과 통하여 제안한 암호화 방법이 광 암호화 시스템에 적용 가능함을 확인하였다. 현재 사용되는 광학장비의 성능개선과 위상 조절 레벨의 향상을 위한 고성능 SLM이나 위상 마스크의 식각 기술 개발이 이루어진다면 제안한 암호화 방법의 성능을 향상시킬 수 있을 뿐만 아니라 효율적인 광 실험의 구현도 가능할 것이라 생각된다.

참 고 문 헌

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, no. 7, pp. 767-769, April, 1995.

[2] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," *J. Opt. Soc. Am. A*, vol. 16, no. 8, pp. 1915-1927, August, 1999.

[3] B. Javidi and T. Nomura, "Polarization encoding for optical security systems," *Optical. Engineering*, vol. 39, no. 9, pp. 2439-2442, September, 2000.

[4] C. J. Cheng and M. L. Chen, "Polarization encoding for optical encryption using twisted nematic liquid crystal spatial light modulators," *Optics Communications*, vol. 237, pp. 45-52, July, 2004.

[5] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Optics Letters*, vol. 24, no. 11, pp. 762-764, June, 1999.

[6] N. K. Nishcal, J. Joseph, and K. Singh, "Securing information using fractinal Fourier transform in digital holography," *Optics Communications*, vol. 235. pp. 253-259, May, 2004.

[7] J. Y. Kim, S. J. Park, C. S. Kim, J. G. Bae, and S. J. Kim, "Optical image encryption using interferometry-based phase mask," *Electron Letters*, vol. 36, no. 10, pp. 874-875, June, 2000.

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

[9] P. C. Mogensen and J. Glückstad, "Phase-only optical encryption," *Optics Letters*, vol. 25, no. 8, pp. 566-568, April, 2000.

[10] H. T. Chang, W. C. Lu, and C. J. Kuo, "Multiple-phase retrieval for optical security systems by use of random-phase encoding," *Applied Optics*, vol. 41, no. 23, August, 2002.

[11] P. C. Mogensen and J. Glückstad, "Phase-only decryption of a fixed mask," *Applied Optics*, vol. 40, no. 8, pp. 1226-1235, March, 2001.

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

저 자 소 개

신 창 목(정회원)

제41권 SD편 6호 참조

서 동 환(정회원)

제41권 SD편 6호 참조

김 수 중(평생회원)

제40권 SD편 9호 참조