논문 2011-06-22

실수값 복원키를 이용한 광 영상 은닉 기술

(Optical Image Hiding Technique using Real-Valued Decoding Key)

조 규 보, 서 동 환*, 최 은 창
(Kyu-Bo Cho, Dong-Hoan Seo, Eun-chang Choi)

Abstract : In this paper, an optical image hiding technique using real-valued decoding key is proposed. In the embedding process, a each zero-padded original image placed in a quadrants on an input plane is multiplied by a statistically independent random phase pattern and is Fourier transformed. An encoded image is obtained by taking the real-valued data from the Fourier transformed image. And then a phase-encoded pattern, used as a hidden image and a decoding key, is generated by the use of multiple phase wrapping from the encoded images. A transmitted image is made from the linear superposition of the weighted hidden images and a cover image. In reconstruction process, the mirror reconstructed images can be obtained at two quadrants by the inverse-Fourier transform of the product of the transmitted image and the decoding key. Computer simulation and optical experiment are demonstrated in order to confirm the proposed technique.

Keywords : Image hiding, Real-valued decoding key, Phase wrapping rule

1. 서 론

최근 광 정보보호에 관한 연구가 활발하게 진행되어 왔으며 이는 광의 병렬성과 고속성을 충분히 이용할 수 있는 장점 및 세기정보와 위상정보를 동시에 광학 매질에 기록할 수 있으므로 사람의 눈이나 기존의 세기검출기로는 추출이 불가능하고 무작위 특성에 의해서 원래의 패턴을 복제나 위조하기가 어렵다는 특성을 가진다. 일반적으로 사용되어 왔던 광 정보보호 시스템은 주로 4-f 광 상관시스템 [1-4]이나 간섭계 구조 [5]를 이용하여 원 영상을 재생하게 되는데, 이때 암호화에 사용된 무작위 위상마스크에 의해서 주로 진위 여부를 판정하게 된다. 이 중 4-f 광 상관시스템은 광축 정렬 문제와 암호화할 때 사용한 위상마스크의 복소공액 마스크를 제작해야 하는 어려움이 있으며, 간섭계를 이용한 시스템은 정밀한 실험구성을 필요로 하며 외란에 많은 영향을 받는다는 단점이 있다. 이에 여러 형태의 외부 영향이나 잡음에 얼마나 강한가를 이중 무작위 위상 부호화(double random phase encoding) 기술 [6-7]을 이용하여 제안하였는데 이 기술들은 여러 잡음이나 암호화된 영상의 절단에는 강하지만 광학적 시스템이 가지는 배열의 문제인 화소 대 화소 대응을 정밀하게 하지 않으면 복원영상을 얻을 수가 없다. 이를 해결하기 위하여 위 기술을 이용하여 복원키의 픽셀 이동이 발생하더라도 원 영상이 재생되는 기술 [8]이 제안되었으나 이 기술은 복원키의 이동에 따른 암호화키의 절단이 동반되어서 원 영상이 재생되므로 원 영상의 재생 시 암호화키의 절단이 필요하고 그에 따른 원 영상의 해상도가 낮아지는 단점을 가진다. 다른 기술로는 세기정보 암호화 수준을 향상시키기 위하여 입력평면에 위상정보를 가지는 원 영상을 이용하여 암호화하는 기술 [9]들이 제안되었다. 이 기술은 공간 영역에서 암호화 및 복원이 이루어지므로 광학적 시스템에서 정밀한 화소 대 화소의 대응이 없다면 원영상을 재생할 수 없으므로 정확한 광축 정렬이 필요하다 [10]. 또한 앞서 제안된 기술들의

* 교신저자(Corresponding Author)
논문접수 : 2011. 01. 31., 수정일 : 2011. 02. 23., 채택확정 : 2011. 03. 21.
서동환 : 한국해양대학교 전기전자공학부
조규보, 최은창 : 한국전자통신연구원

가장 큰 단점 중에 하나는 암호화키와 복원키가 동일하므로 만약 허가되지 않은 사용자가 암호화된 영상을 분석하여 암호화키를 파악함으로써 복원 영상을 예측할 수 있는 문제점이 있다.

본 논문에서는 본 논문에서는 실수값 복원키와 위상래핑방법 [10]을 이용하여 향상된 암호화 수준을 가지는 영상 은닉 기술을 제안하고자 한다. 은닉해야 될 푸리에 변환된 제로패딩 원영상을 제작하고 위의 과정에서 제작된 영상에 위상래핑기술을 적용하여 은닉 영상과 복원키를 제작하고, 만들어진 은닉 영상을 커버영상과 일차 선형 변환을 시켜서 배포 영상을 제작한다. 복원 과정에서는 제작된 배포영상과 복원키를 변환하여 출력 평면에서 간단히 복원된다. 제안된 기술은 위상래핑 방법의 비선형성을 이용하여 복원키와 은닉영상을 생성시키므로 비인가 사용자들에 의해 패턴이 해킹 당하지 않도록 하였고, 원영상의 정보를 복원 과정에서 직접사용하지 않으므로 원영상과 간섭계 등을 이용하여 복원영상을 추출하는 방법에 비해 높은 수준의 정보 보호가 가능하도록 하였다. 또한 위상 정보를 이용하는 광학적 시스템에 비해 제안 된 기술의 은닉영상 임베딩 과정에서 사용되는 모든 패턴들이 정실수값을 가지므로, 다양한 영상 전송 시스템에 적용될 수 있다는 장점을 지닌다.

Ⅱ. 본 론

1. 배포영상 생성 과정

$o_z(x,y)$와 $\exp[jn(x,y)]$는 각각 입력평면의 한사분면에 위치하고 있는 제로패딩 된 원영상과 무작위 위상 영상이며, $n(x,y)$는 $[0,2\pi]$구간에서 균일하게 분포된 백색 신호라고 했을 때 먼저 아래 수식과 같이 서로 곱하여 푸리에 변환 시켜 아래와 같은 수식을 얻는다.

$$O(\zeta,\eta)=\Im\{O_z(x,y)\exp[jn(x,y)]\}, \qquad (1)$$

이 영상의 실수부를 취하고, [-1, 1]구간에서 정규분포를 취하여 $E(\zeta,\eta)$를 얻는 후 이 영상으로부터 위상래핑기술을 이용하여 두 개의 위상변조영상을 얻어낸다. 무작위 위상변조패턴 $\exp[j2\pi r_{1h}(\zeta,\eta)]$는 산술적인 연산을 통해 아래의 수식에서 주어지는 것과 같이 얻을 수가 있다.

$$\exp[j2\pi r_{1h}(\zeta,\eta)]=\exp[j2\pi\{E(\zeta,\eta)+r_d(\zeta,\eta)\}] \qquad (2)$$

여기에서 $r_d(\zeta,\eta)$는 복원키를 만드는데 사용되며 [0,1]구간에서 무작위 분포된다. 아래 수식(7)과 같은 위상래핑기술 규칙에 의해 $r_{1h}(\zeta,\eta)$로부터 $r_h(\zeta,\eta)$를 생성할 수 있다.

$$\exp[j2\pi r_h] = \begin{cases}\exp\{j2\pi[r_{1h}(\zeta,\eta)+1]\}, -1\le r_{1h}<0\\ \exp\{j2\pi[r_{1h}(\zeta,\eta)]+0\}, 0\le r_{1h}<1\\ \exp\{j2\pi[r_{1h}(\zeta,\eta)]-1\}, 1\le r_{1h}<2\end{cases} \qquad (3)$$

위의 수식을 이용하여 $\exp[j2\pi r_{1h}]$을 위상래핑규칙을 이용하여 $\exp[j2\pi r_h]$이 생성되며 이는 $[0,2\pi]$구간에서 위상래핑 된다. 위상래핑기술을 적용하는 이유는 연산이 비선형적이므로 보안의 수준을 높이는 역할을 하기 때문에 인가되지 않은 사용자가 위상변조 된 영상을 분석하기 어렵게 한다는 장점을 가지고 있다. 또한 실제적인 통신시스템에 사용될 수 있도록 정 실수값을 얻어 낼 수 있도록 고안되었다.

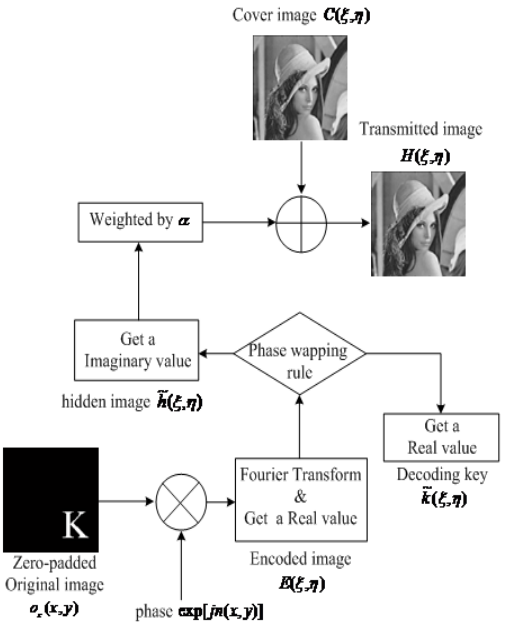


그림 1. 배포영상 생성 과정

Fig. 1. Block diagram for the process of generating transmission image

영상에 임베딩 될 은닉영상을 $\tilde{h}(\zeta,\eta)$, 복원키를

$\tilde{k}(\zeta,\eta)$라고 하면 아래 수식(8)과 같은 기술로 생성할 수 있다.

$$\tilde{h}(\zeta,\eta) = \mathrm{Im}\{\exp[j2\pi r_h(\zeta,\eta)/K]\} = \sin[2\pi r_h(\zeta,\eta)/K] \quad (4)$$
$$\tilde{k}(\zeta,\eta) = \mathrm{Re}\{\exp[j2\pi r_d(\zeta,\eta)/K]\} = \cos[2\pi r_d(\zeta,\eta)/K]$$

위의 수식에 의해 생성되고 [0,1]구간에서 정규화된 은닉영상$\tilde{h}(\zeta,\eta)$와 커버영상 $C(\zeta,\eta)$을 일차선형 변환 시켜서 다음 수식(9)와 같은 배포영상을 생성한다.

$$H(\zeta,\eta) = \alpha\tilde{h}(\zeta,\eta) + C(\zeta,\eta) \quad (5)$$

배포영상 생성과정의 블록 다이어그램은 그림 1과 같다.

2. 복원 과정

원영상을 복원하기 위해서는 배포영상을 복원키와 직접 곱하고 역 푸리에 변환을 수행한다. 복원키와 배포영상의 곱은 수식(10)과 같이 주어진다.

$$\begin{aligned}&\tilde{k}(\zeta,\eta)H(\zeta,\eta) \quad (6)\\ &= \cos[2\pi r_d(\zeta,\eta)/K]\{\alpha\sin[2\pi r_h(\zeta,\eta)/K] + C(\zeta,\eta)\}\\ &= (\alpha/2)\sin[2\pi\{r_h(\zeta,\eta) - r_d(\zeta,\eta)\}/K]\\ &+ C(\zeta,\eta)\cos[2\pi r_d(\zeta,\eta)/K]\\ &+ (\alpha/2)\sin[2\pi\{r_h(\zeta,\eta) + r_d(\zeta,\eta)\}/K]\end{aligned}$$

Taylor series 전개를 이용하여 우변 첫째 항을 다음과 같이 표현 할 수 있다.

$$\begin{aligned}&(\alpha/2)\sin[2\pi\{r_h(\zeta,\eta) - r_d(\zeta,\eta)\}/K] \quad (7)\\ &= (\alpha/2)\sin[2\pi E(\zeta,\eta)/K]\\ &= (\alpha/2)\{2\pi E(\zeta,\eta)/K - [2\pi E(\zeta,\eta)/K]^3/3! - \cdots\}\\ &= (\alpha\pi/K)E(\zeta,\eta), \text{for } 2\pi E(\zeta,\eta) << K.\end{aligned}$$

$2\pi E(\zeta,\eta) << K$에 대해서, 식(11)의 K는 위의 식(11)의 세 번째 항의 위상의 dynamic range를 낮추고, 식(12)와 같은 수식을 이끌어낼 수 있도록 하였다. 위의 식 (12)의 역푸리에 변환은 다음과 같다.

$$\begin{aligned}&\Im^{-1}\{\tilde{k}(\zeta,\eta)H(\zeta,\eta)\} \quad (8)\\ &= \Im^{-1}\{(\alpha\pi/2)E(\zeta,\eta)\}\\ &+ \Im^{-1}(\alpha/2)\sin[2\pi\{r_k(\zeta,\eta) + r_d(\zeta,\eta)/K\}]\\ &+ \Im^{-1}\{C(\zeta,\eta)\cos[2\pi r_d(\zeta,\eta)/K]\}\\ &= e'(x,y) + r'(x,y) + C'(x,y)\end{aligned}$$

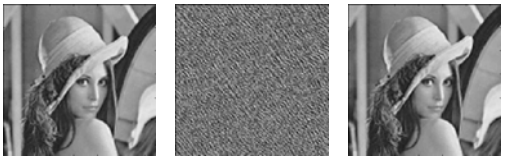
간략하게 표현하기 위해, 위의 수식(13)처럼 표현 하였으며, CCD 출력 평면에서 나타나는 복원영상에 대한 수식은 아래와 같다.

$$\begin{aligned}&R_{CCD}(x,y) \quad (9)\\ &= |e'(x,y) + r'(x,y) + C'(x,y)|^2\\ &\approx |e'(x,y) + r'(x,y)|^2\\ &= |e'(x,y)|^2 + e'(x,y)r'(x,y)^* + e'(x,y)^*r'(x,y)\\ &\quad + |r'(x,y)|^2\\ &= (\alpha\pi/2k)^2[o_z'(x,y)]^2 + e'(x,y)r'(x,y)^*\\ &\quad + e'(x,y)^*r'(x,y) + |r'(x,y)|^2\end{aligned}$$

식(14)에서 $C'(x,y)$는 실험과정에서 공간필터를 이용하거나 통과시키는 기술을 통해 제거되어지며, $o_z'(x,y)$는 $\mathrm{Re}[\Im\{o_z(x,y)\}]$를 역푸리에 변환한 결과로써, real even 복원패턴을 가진다. 위의 수식(14)에서 $e'(x,y)r'(x,y)^* + e'(x,y)^*r'(x,y)$와 $|r'(x,y)|^2$항은 거의 화이트노이즈처럼 복원영상보다 매우 작은 의사-난수의 형태로 출력평면 전체에 분산되게 되어 출력평면에는 복원영상이 두드러지게 나타난다. 위의 수식에서 K값은 위에서 언급했듯이 식(14)의 결과식 중 첫 번째 항의 세기 레벨을 향상시키고, 위상의 dynamic range를 조절하는 역할을 하여 전체적으로 지수항의 크기를 감쇄시켜서 식이 근사화 될 수 있도록 한다. 아래 그림3은 제안된 복원과정의 블록다이어그램을 나타낸다.

3. 모의실험

제안된 영상은닉 기술의 성능을 알아보기 위해서 컴퓨터 모의실험을 실행 하였다. 그림 3(a)에서 64×64 크기의 “K"영상을 제로 패딩하여 129×129 이미지로 제작하였으며, 그림3(b)와 3(c)는 제로패딩 된 영상을 푸리에 변환 시킨 후 실수값을 취한 영상과 이를 다시 역푸리에 변환하여 복원 시 2개 사분면에 대칭적으로 나타나는 복원영상을 보여주고 있다.

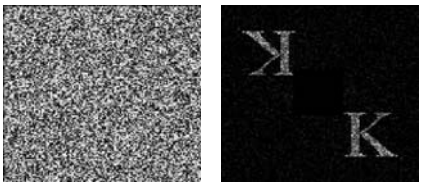


(a) (b) (c)

그림 2. 배포영상 생성과정에서 사용되는 영상: (a) 커버영상, (b) 은닉영상, (c) 배포영상

Fig. 2. Images used in the process of generating the transmission image: (a) cover image, (b) hidden image, (c) transmitted image

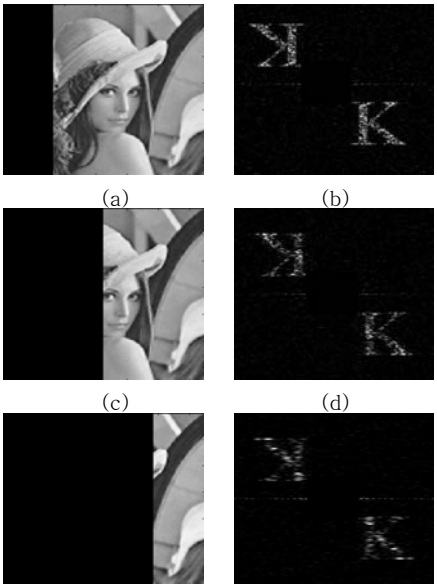
그림 4(a), 4(b), 그리고 4(c)는 커버영상, 은닉영상, 그리고 배포영상을 각각 나타낸 것이며, α와 K는 각각 0.02 와 20으로 고정하여 모의실험을 하였다.



(a) (b)

그림 3. 복원과 과정에서 사용된 영상들: (a) 음수값이 없는 복원키, (b)복원 영상

Fig. 3. Images used in the reconstruction process in simulations: (a) decoding key with non-negative value, (b) reconstructed image



(a) (b) (c) (d) (e) (f)

그림 6. 절단된 배포영상과 복원된 원영상: (a) 25% 절단된 배포영상, (b) 복원된 원영상, (c) 50% 절단된 배포영상, (d) 복원된 원영상, (e) 75% 절단된 배포영상, (f) 복원된 원영상

Fig. 6. Truncated transmitted images and reconstructed images: (a) 25% blocked transmitted image, (b) reconstructed image of (a), (c) 50% blocked transmitted image, (d) reconstructed image of (c), (e) 75% blocked transmitted image, (f) reconstructed image of (e)

그림 5(a)와 5(b)는 복원 키와 복원된 원영상을 나타낸 것이다. 제안된 기술이 절단에 대해 강한 특성을 가지는지를 확인하기 위해 배포영상을 적당한 비율로 절단하여 원 영상을 재생하는 모의실험을 수행하였다. 그림 6(a), 6(c), 6(e)는 배포영상을 25%, 50%, 75% 절단한 영상이며, 이 영상들에 대해 재생된 원영상은 6(b), 6(d), 6(f)와 같다. 재생된 영상은 그림 5(b)에 비해 잡음이 많이 가해졌지만 시각적으로 구분이 가능하므로 절단에 대해 강인함을 확인 할 수 있다.

표 1. 배포영상의 절단에 따른 PSNR값의 변화

Table 1. Variation of the value of PSNR for truncating transmitted image

truncation	25	50	75
PSNR(dB)	30.14	27.67	23.98

재생 된 원영상의 식별 가능정도를 알아보기 위해 PSNR 값을 측정한 결과를 표 1에서 나타내었다. 절단된 픽셀의 수가 증가할수록 PSNR값은 낮아지고, 복원된 원영상의 잡음이 증가하고 영상의 질이 많이 떨어지지만 원래의 영상의 형태대로 식별이 가능함을 하여 절단에 대해 제안된 시스템이 강인한 특성을 가짐을 알 수 있다.

4. 광실험

제안된 시스템 구현을 위한 광실험도는 그림 7과 같고, 배포영상을 생성하는 과정은 컴퓨터에서 수치 해석적으로 수행하고, 원영상의 복원은 광학적으로 수행되어진다. 실험에 사용된 광원은 선형 편광 된 파장이 514nm인 He-Ne레이저이고, LCD는 해상도 800×600의 HoloEye 사의 LC 2002 패널로 구동회로를 사용했으며, PULNiX사의 TM-1320-15CL CCD를 사용하여 추출된 영상을 기록하였다. L1 및 L2는 렌즈, SF는 Beam Expander로 사용되는 Spatial Filter를 나타낸다. 위상변조 특성을 가지는 두 개의 LC SLM에 배포영상과 복원을 위한 복원 키를 각각 올린 후 정확히 화소 대 화소 매칭을 한 후 레이저 광을 투과시킨 후 L2렌즈에 의해 푸리에 변환 시킨 후 CCD 평면에서 원영상을 재생한다. 강한 세기를 가지는 DC 성분이 나타나는 출력평면의 가운데 부분에 공간차단 필터를 위치시켜 재생되는 영상의 가시성이 좋도록 하였다. 실험에서 절단된 부분이 증가할수록

재생영상의 해상도가 떨어지지만 인식 불가능한 정도가 아니므로 어느 정도 절단에 대해 강인한 특성을 가진다.

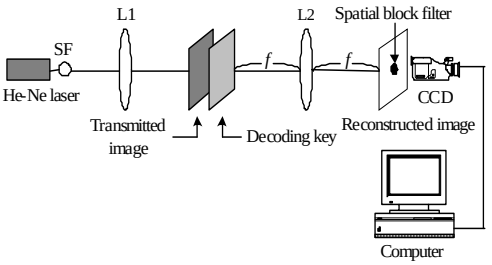


그림 7. 광실험
Fig. 7. Optical experiment

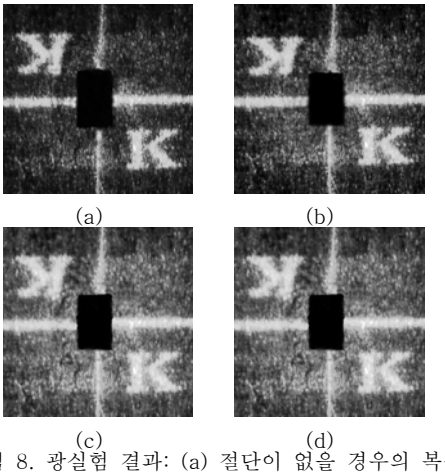


그림 8. 광실험 결과: (a) 절단이 없을 경우의 복원 영상, (b) 25% 절단한 경우의 복원 영상, (c) 50% 절단한 경우의 복원 영상, (d) 75% 절단한 경우의 복원 영상

Fig. 8. Results of optical experiment: (a) reconstructed image with non-truncated transmitted image, (b) reconstructed image with 25% truncated image, (c) reconstructed image with 50% truncated image, (d) reconstructed image with 75% truncated image

IV. 결 론

제안된 기술은 실수값을 가지는 복원키와 위상래핑기술의 비선형성을 이용하여 복원키와 은닉영상을 생성시키므로 허가되지 않은 사용자들에 의한 사용을 방지 할 수 있으며, 원영상 정보를 복원 과정에서 직접 사용하지 않으므로 보다 높은 정보보호가 가능하도록 하였다. 제안된 기술의 장점은 위상래핑기술의 비선형성을 이용하여 복원키와 은닉영상을 생성시키므로 허가되지 않은 사용자들에 의해 위의 패턴들을 확인할 수 없도록 하였으며, 원영상의 정보를 복원과정에서 직접 사용하지 않으므로 보다 높은 정보보호가 가능하도록 하였다. 그리고 기존의 복소수 기반의 광학적 시스템에 비해 제안된 기술의 은닉영상 삽입 과정에서 사용되는 모든 패턴들이 정 실수 값을 가지므로, 제안된 시스템이 인터넷 등 다양한 영상 전송 시스템에 적용 될 수 있다. 또한 제안된 기술은 직렬로 배열되는 간단한 광학적 구조를 가지므로 기존의 간섭계 등을 이용한 광학적 시스템이 가지는 배열의 문제를 해결하므로 화소 대 화소 대응을 용이하게 하여 복원 영상의 해상도를 높일 수 있다. 또한 복원 된 영상의 가시성에 영향을 미치는 요소와 데이터 손실에 따른 견실성을 검증하여 제안된 기술이 광영상 은닉 시스템에 적용 가능함을 확인한 결과 배포 영상이 절단 등의 데이터 손상에 대해 내구성이 있음을 확인하였다.

참고문헌

[1] B. Javidi and J. L. Horner, “Optical pattern recognition for validation and security verification”, Opt. Eng., Vol.33, pp. 1752-1756, 1994.

[2] R. K. Wang, I. A. Watson, and C. Chatwin, “Random phase encoding for optical security”, Opt. Eng., Vol.35, pp. 2464-2469, 1996.

[3] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding”, Opt. Lett., Vol.20, pp. 767-769, 1995.

[4] 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, pp. 2506-2512, 1996.

[5] B. Javidi and E. Ahouzi, “Optical security system with Fourier plane encoding”, Appl. Opt., Vol.37, pp. 6247-6255, 1998.

[6] B. Javidi, A. Sergent, G. Zhang, and L. Guibert, "Fault tolerance properties of a double phase encoding encryption technique", Opt. Eng. Vol.36, pp. 992-998, 1997.
[7] B. Javidi, A. Sergent, and E. Ahouzi, "Performance of double phase encoding encryption technique using binarized encrypted images", Opt. Eng., Vol.37, pp. 565-570, 1998.
[8] B. Wang, C. C. Sun, W. C. Su, and A. E. T. Chiou, "Shift-tolerance property of an optical double-random phase-encoding encryption system", Appl. Opt., Vol.39, pp. 4788-4793, 2000.
[9] J. Ohtsubo and A. Fujimoto, "Practical image encryption and decryption by phase-coding technique for optical security systems", Appl. Opt., Vol.41, pp. 4848-4855, 2002.
[10] A. Loussert, A. Alfalou, R. El Sawada, and A. Alkholidi, "Enhanced System for image's compression and encryption by addition of biometric characteristics", IJSEIA, Vol.2, No.2, pp. 111-118, 2007.
[11] C. M. Shin, D. H. Seo, and S. J. Kim, "Optical security system using multi-phase separation and phase-wrapping technique", Journal of IEEK, Vol.42, No.6, pp.31-38, 2005.

저 자 소 개

조 규 보 (Kyu-Bo Cho)

1999년 : 경북대학교 전자공학과 학사.
2001년 : 경북대학교 전자공학과 석사.
2008년 : 경북대학교 전자공학과 박사.
현재, 한국전자통신연구원 선임기술원.
관심분야 : 광 정보보호, 3D 디지털 홀로그래피, 신재생에너지(태양광 & 2차 전지).
Email : daniel.cho@etri.re.kr

서 동 환 (Dong-Hoan Seo)

1996년 : 경북대학교 전자공학과 학사.
1999년 : 경북대학교 전자공학과 석사.
2003년 : 경북대학교 전자공학과 박사.
현재, 한국해양대학교 전기전자공학부 부교수.
관심분야 : 신호처리, 수중통신, 데이터통신, 영상통신, 전기시스템.
Email : dhseo@hhu.ac.kr

최 은 창 (Eun-chang Choi)

1990년 : 경북대학교 전자공학과 학사.
1992년 : 경북대학교 전자공학과 석사.
2006년 : 경북대학교 전자공학과 박사.
현재, 한국전자통신연구원 IT융합기술팀장.
관심분야 : WPAN, 무선 홈네트워크, u-컴퓨팅, IT융합기술.
Email : ecchoi@etri.re.kr