광자 계수 이중 랜덤 위상 암호화 영상 정보 인증에 대한 검토

조 명 진*

1. 서 론

최근 디지털 콘텐츠의 제작과 교류가 활발히 이루어져 고부가가치 산업으로 성장하고 있다. 특히, 영상의 광학적 암호화 기술에 대하여 연구가 활발히 진행되고 있다 [1-7]. 하지만, 디지털 콘텐츠는 불법복제에 취약하고 보안의 문제를 가지고 있다. 이러한 문제들을 해결하기 위하여 다양한 기술들이 연구 개발 되고 있는데, 그 중의 하나가 암호화 기법이다. 암호화 기법은 송신자와 수신자 간의 약속된 키 (key) 정보를 사용하여 정보를 암호화 하고 복호화 한다. 여기서, 어떤 외부의 공격자가 이 키를 도용하게 되면 암호화된 정보는 더 이상 보안성을 가지지 못하게 된다. 또한, 양질의 디지털 콘텐츠를 불법복제 하여 유통하게 되는 경우가 발생하여 산업에 막대한 피해를 끼치게 된다. 일반적으로 디지털 콘텐츠는 복제하는 것이 매우 쉽다. 이러한 디지털 콘텐츠의 정보적 가치를 보호하기 위해, 숨겨진 암호 코드 (워터 마크와 같은)를 추가할 필요성이 제기되고 있다. 기존의 암호화 기법들은 여전히 키 정보에 의존하게 되는 형식을 취하고 있기 때문에, 이러한 키 정보를 보다 보안성이 뛰어나게 만드는 연구가 중요해지고 있다. 원 영상 (Primary image)와 함께 전송되는 노이즈와 같은 랜덤 분포를 생성하기 위하여 많은 알고리즘이 개발되고 있다 [1-7]. 이러한 기술들은 전송되는 정보를 보호하는데 있어서 매우 유용하다. 가장 광범위하게 사용되는 알고리즘 중의 하나인 이중 랜덤 위상 암호화 기술 (Double- random phase encryption: DRPE)은 [2] 키(key) 정보의 갱신 없이 정보를 복호화 (decryption)하고자 할 때 침입자의 공격에 대하여 매우 취약하다 [8,9]. 이러한 문제점들을 해결하기 위하여, 광학적 암호화 기술에 광자 계수 이미징 방법 (Photon counting imaging) [10-12, 14-22]을 적용하여 보다 강력한 정보 보호 능력을 가지는 방법이 제안되었다. [18]. 광자 계수 이미징 방법은 다양한 분야에 적용되고 있다. 이 기술은 광자의 수가 지극히 제한된 환경에서 물체를 인식하고 검출하는 것이 가능하기 때문에, 국방산업과 같은 분야에 적용될 수 있다. 또한, 광자 단위로 이미징을 하는 것이 가능하기 때문에, 의료산업과 같은 분야에서도 쓰여진다. 이러한, 광장 계수 이미징 시스템의 특성으로 인해, 정보의 암호화 기술에서도 많은 장점을 가지고 있다. 특히, 광자 계수 이미징 시스템에서, 영상은 들어오는 광자의 기대 수 (expected number)를

※ 교신저자(Corresponding Author) : 조명진, 주소 : 경기도 안성시 중앙로 327, 전화: 031)670-5298, FAX: 031)670-5199, E-mail : mjcho@hknu.ac.kr
* 한경대학교 전기전자제어공학과

제어함으로써 제한된 수의 광자를 가질 수 있다 [12]. 이를 통해, 암호화된 정보의 정보 보호 능력을 조절하는 것이 가능하다.

본 논문에서는 제한된 광자 수를 가지는 이중 랜덤 위상 암호화 기술에 대해 검토한다. 이 방법에서는 제한된 광자 수를 가지는 암호화 영상을 사용하여 복호화를 한다. 이와 같이 복호화된 영상은 침입자가 쉽게 식별하지 못한다. 이 영상들은 시각적으로 식별 가능한 것이 아니라 광학적 상관 필터 (correlation filter)를 사용하여 식별가능하다. 이것은 향상된 정보 보호 능력을 제공하고 공격에 보다 효율적이다.

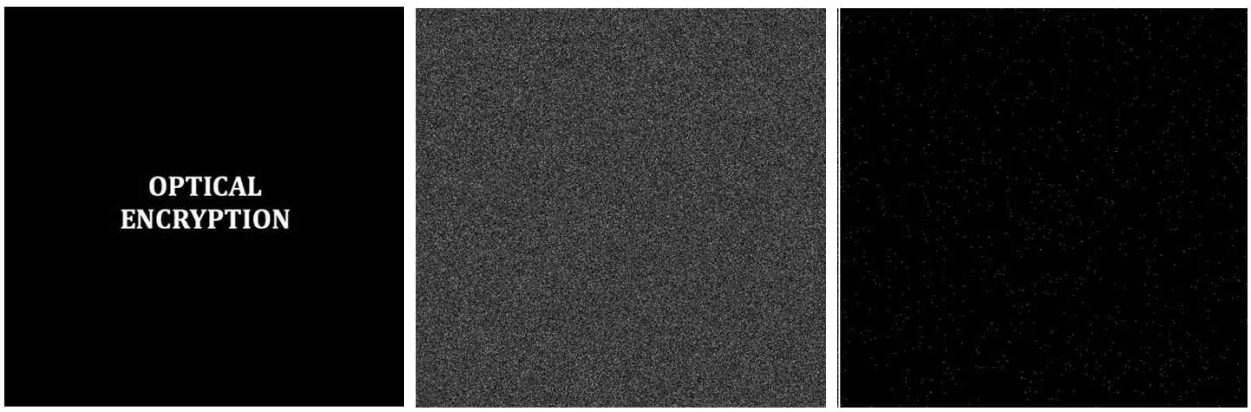
2. 이중 랜덤 위상 암호화 (Double-random-phase encryption: DRPE)

이중 랜덤 위상 암호화 [2]에 대해 설명해 보자. 단순화하기 위해 영상 $f(x)$[그림 1(a)]는 1차원 표기법을 사용하여 표기한다. 두 랜덤 노이즈 $n(x)$, $b(\mu)$는 [0, 1]의 구간을 갖는 균일 분포 (Uniform distribution)이라고 가정한다. 좌표 (x), (μ)는 공간과 주파수 영역을 의미한다. 우선, 영상 $f(x)$에 위상 마스크 (Phase mask) $\exp[i2\pi n(x)]$를 곱한다. 그리고 나서, 그 결과물을 함수 $h(x)$로 컨볼루션 (Convolution)한다. 여기서 함수 $h(x)$의 푸리에 변환 (Fourier transform)은 $\mathrm{FT}\{h(x)\} = \exp[i2\pi b(\mu)]$이다. 최종적으로 암호화된 영상 $\psi(x)$ 는 다음과 같이 정의된 복소 함수 (complex-valued function)가 된다.

$$\Psi(x) = \{f(x)\exp[i2\pi n(x)]\} * h(x) \qquad (1)$$

여기서 $*$는 컨볼루션을 의미한다. 복소 크기를 갖는 암호화된 영상 $\psi(x)$는 크기 (Amplitude) $|\Psi(x)|$와 위상 정보 (Phase information) $\Phi_\psi(x)$를 가지기 때문에 $\Psi(x) = |\Psi(x)|\exp[i\Phi_\psi(x)]$ 같이 쓰여질 수 있다. 일반적으로, 암호화 함수는 그림 1(a)로부터 얻어진 암호화 신호의 크기 분포를 보여주는 그림 1(b)에 나타나 있는 것처럼, 콘텐츠를 숨기기 위해 잡음과 같은 모습을 가진다.

이중 랜덤 위상 암호화 알고리즘의 제안으로 인해, 이 알고리즘에 기반 하여 다양한 논문들이 발표되고 있고 특히 광학적 정보보호 분야에 적용되고 있다. 이중 랜덤 위상 암호화 기술은 광학 시스템에 적용될 때 숨겨진 정보를 찾기 위하여 정확히 알고 있어야 하는 몇몇 비선형 효과와 부가된 실험 파라미터들(광학적 저장 매질, 위치, 빛



(a) (b) (c)

그림 1. (a) 영상 $f(x)$, (b) 함수 $|\Psi(x)|$, (c) $N_p = 10^3$을 가지는 함수 $|\Psi_{ph}(x)|$.

의 파장과 편광)을 자주 포함하기 때문에 보다 나은 정보보호를 수행할 수 있다. 하지만, 이중 랜덤 위상 암호화 기술은 이산적으로 수행될 수 있는 암호화 알고리즘으로 보여질 수 있다. 이것은 brute force attack에 대처하는 능력이 있지만, 알려지고 선택된 암호문의 원문과 암호문 공격에는 취약하다 [8, 9, 28]. 이러한 이유로, 최근 몇 년동안 광학적 암호화 절차의 정보보호 능력을 증가시키는 새로운 방법들이 제안되고 있다. 그 중에, 이중 랜덤 암호화 기술과 광자 계수 이미징 기술이 혼합된 방법이 제안되었다 [23].

3. 광자 계수 이미징 기술을 사용한 제한된 광자 수를 가지는 이중 랜덤 위상 암호화 영상

광자 계수 이미징 시스템에서, 영상은 전체 영상에서 입사하는 광자의 기대 수 (expected number)를 조절함으로써 제한된 광자 수를 가질 수 있다 [2, 12, 23-25]. 따라서, 일반적으로 광자 수가 제한되는 영상은 원 영상보다 더 작은 정보를 가진다.

광자수가 제한되어 있는 암호화 영상을 생성하기 위해 전체 영상에서 광자의 수 N_p를 제어하는 광자 계수 이미징 기술이 사용된다. 픽셀 j에서 l_j 광자가 계수되는 확률은 다음 식과 같이 포아송 분포 (Poisson distribution)으로 나타낼 수 있다 [12,13].

$$P_d(l_j;\lambda_j)=\frac{|\lambda_j|^{l_j}e^{-\lambda_j}}{l_j!},\quad l_j=0,1,2,\ldots, \tag{2}$$

여기서 l_j는 픽셀 j에서 검출된 광자의 수이고 포아송 파라미터 λ_j는 픽셀 j에서 정규화된 조도 (normalized irradiance) 다시 말해 $\sum_{j=1}^{M}x_j=1$인 x_j와 함께 $\lambda_j=N_p x_j$로 주어진다. 여기서 M은 영상에서 픽셀의 전체 수와 같다. 광자수가 제한되는 영상은 원 영상에서의 물체 모양을 보기가 매우 어렵다. 광자 수가 증가함에 따라 원 영상에서의 물체 모양을 서서히 나타난다. 광자 계수 이미징 기술은 많은 분야와 다양한 대역폭에 적용되고 있다 [10, 11, 12, 15, 26, 27]. 또한 광자 수가 제한되는 분포를 사용한 2차원 영상 인식 증명되었다 [10, 11]. 3차원 물체의 인식에 관한 광자 계수 이미징 방식은 최근 연구가 진행되고 있다 [12, 15].

광자 계수 이미징 방법은 복소의 값을 갖는 암호화된 분포 $\Psi(x)$에 적용될 수 있다. 광자 수가 제한된 크기 데이터 $|\Psi_{ph}(x)|$는 정규화된 크기 분포 $|\Psi(x_j)|/\sum_{j=1}^{M}|\Psi(x_j)|$에 위에서 언급한 절차를 적용함으로써 생성된다. 최소한 하나의 광자 계수를 갖는 픽셀이 광자 계수가 제한되는 암호화된 함수 $\Psi_{ph}(x)$에서 다루어진다. 오직 이러한 픽셀들만 복호화를 위한 크기와 위상에 대한 정보를 포함한다. 그림 1(c)는 그림 1(b)와 관련있는 광자 계수가 제한되는 암호화된 함수의 크기를 나타낸다. 여기서 전체 광자의 수는 $N_p=10^3$이고 픽셀당 최대 광자의 수는 2이다.

식 1에서 설명한 이중 랜덤 위상 암호화 기술에 따라 정보를 복호화하기 위해 암호화된 함수 $\Psi_{ph}(x)$는 우선 푸리에 변환되고 그것에 복호화 키 $\exp[-i2\pi b(\mu)]$를 곱한다. 이리하여, 함수 $f_{ph}(x)\exp[i2\pi n(x)]$가 얻어진다. 원래 영상 $f(x)$가 실수이면서 양수인 함수라고 한다면 CCD (Charge-Coupled Device) 카메라와 같은 크기에 민감한 장치는 광자 계수가 제한된 복호화된 영상 $f_{ph}(x)$를 얻을 것이다. 그림 2(a)는 그림 1(c)의 희박한 암호화된 분포로부터 얻어진 복화된 영상을 보여준다. 전달하고자 하는 영상 [그림 1(a)]에 포함되어 있는 문자들은 복호화된 영상 [그림 2(a)]

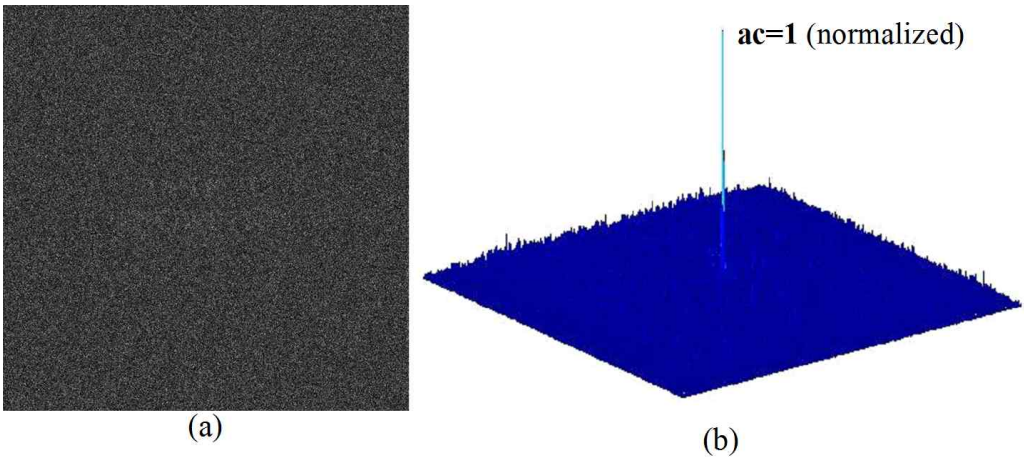


그림 2. (a) 영상 $f_{ph}(x)$, (b) $k=0.3$에 대한 상관 평면.

의 노이즈 배경에서 식별하기가 어렵다.

4. 실험 결과

복원된 신호 $f_{ph}(x)$를 인증하기 위해, 이것을 참조 영상으로 쓰이는 원래 영상 $f(x)$와 비선형 상관 (Nonlinear correlation)에 의해 비교한다 [14]. 하지만, 많은 다른 인식 방법들이 쓰여져도 된다 [15-17]. 비교되는 신호들은 푸리에 변환되고, 비선형적으로 수정되고, 주파수 영역에서 곱해진다. 이러한 곱을 역 푸리에 변환 (Inverse Fourier Transform)함으로써 두 신호 사이의 비선형 상관 $c(x)$는 다음과 같이 구해진다 [14].

$$c(x)=IFT\left\{|F_{ph}(\mu)F(\mu)|^{k}\exp\left[i\left(\Phi_{F_{ph}}(\mu)-\Phi_{F}(\mu)\right)\right]\right\} \tag{3}$$

여기서 대문자는 함수를 푸리에 변환한 것이고 소문자는 함수를 나타낸다.

kth-law 프로세서에서 파라미터 k는 적용된 비선형성의 강도를 정의하고 프로세서의 성능 정도를 결정한다 [14]. 광자 계수 이미징을 사용한 이중 랜덤 위상 암호화 기술에 최적화된 k 파라미터 값을 얻기 위해 컴퓨터 시뮬레이션을 수행하였다. 상관 출력의 평가는 peak-to-correlation (PCE)과 식별율 (discrimination ratio: DR)을 척도로 고려하여 수행하였다 [16]. 최대 크기 피크 값과 출력 면의 전체 에너지 사이의 비로 정의되는 PCE 파라미터는 보통 출력 상관 피크의 날카로운 정도와 높이를 가리킨다. DR은 상관 출력의 최대 피크 값 (maximum peak value of the correlation output: cc)과 참조 타깃의 최대 자기 상관 피크 값 (maximum autocorrelation peak value of the reference target: ac) 사이의 비와 연관되어 있다. 이것은 작은 차이를 식별하는 것에 대한 시스템의 능력에 대해 말해준다.

그림 3은 함수 $f_{ph}(x)$와 $f(x)$가 상관에 의해 비교될 때, 다양한 k 값에 대한 기대 광자 수 N_p와 PCE의 그래프를 나타낸다. N_p가 10^7보다 작을 때, PCE 값은 특별히 광자 수에 따라 급격히 감소한다. k의 중간 값인 $k\in[0.2,0.4]$는 작은 광자 수 (10^5 이하)에 대해 최적의 PCE 값을 가진다. 우리는 적절하게 좋은 DR을 가지는 날카롭고 강한 상관 피크를 제공하는 k=0.3을 선택한다. 그림 2(b)에 나타나 있는 출력 상관 평면은 $f_{ph}(x)$와 $f(x)$를 비교할 때 얻어진다. 날카로운 피크는 잡음 배경 위에 나타난다. 비교를 쉽게 하기 위해 최대 상관

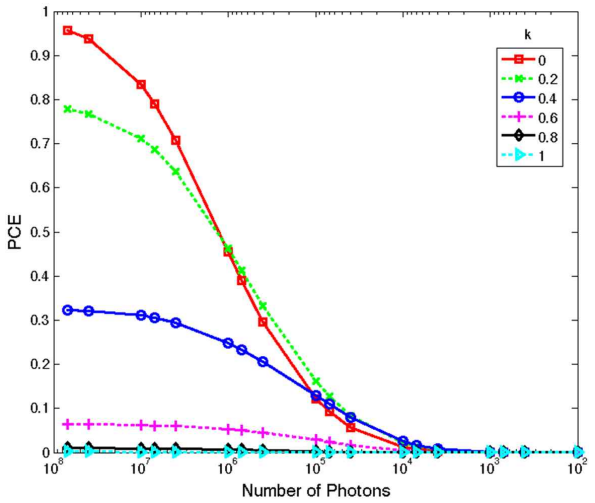


그림 3. 다양한 비선형성 (k)에 대한 광자의 수 (N_p) 변화에 따른 PCE 값.

값은 1로 설정한다.

광자 계수 이미징을 이용한 이중 랜덤 위상 암호화 기술의 구별 능력을 시험하기 위해, 다른 문자 영상 $g(x)$ [그림 4(a)]를 식 (1)을 사용하여 암호화하고 식 (2)와 N_p=10^3을 사용하여 광자 계수가 제한된 암호화 영상을 계산하고, 이 영상으로부터 적절한 키를 사용하여 그림 4(b)와 같은 복화화된 영상 $g_{ph}(x)$를 얻는다. 복호화된 영상 $g_{ph}(x)$는 원래 문자를 구별하기 어렵게 만드는 잡음현상을 가지는 그림 2(b)에 나타나 있는 $f_{ph}(x)$와 매우 유사하다. 영상 $g_{ph}(x)$는 또한 인증을 검증하기 위해 비선형 상관 [식 (3)]을 통해 원 영상

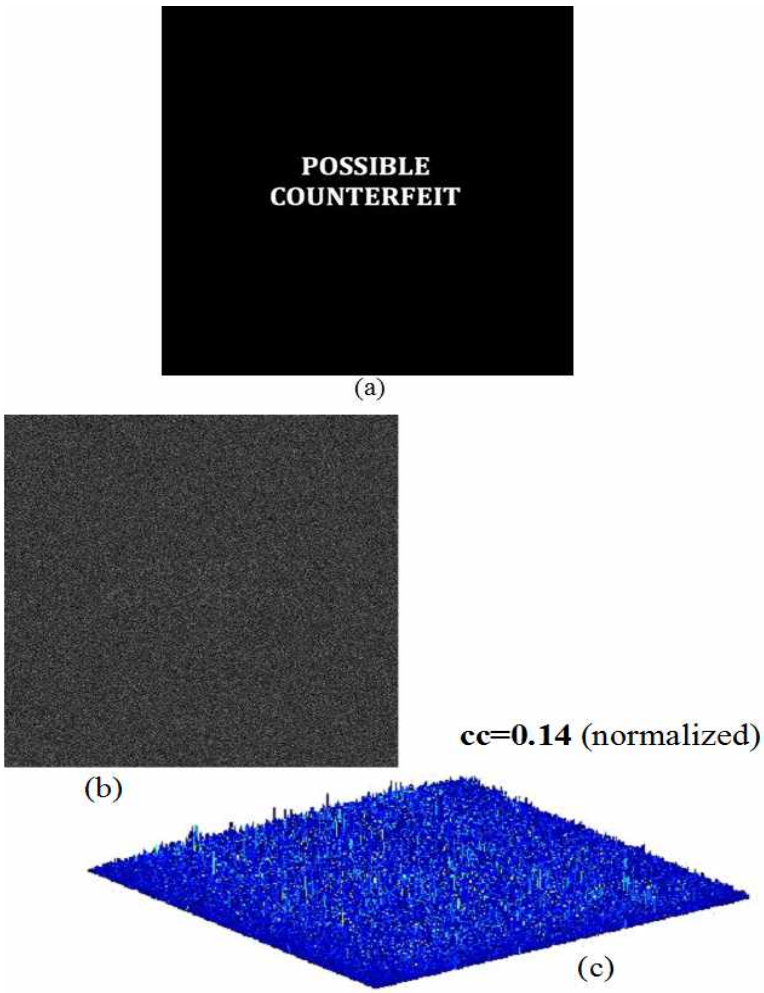


그림 4. (a) 영상 $g(x)$, (b) $N_p = 10^3$에 대한 영상 $g_{ph}(x)$, (c) $k = 0.3$에 대한 상관 평면.

과 비교된다. 그림 4(c)는 해당하는 상관 평면을 나타낸다. 이 경우, 어떠한 두드러진 상관 피크가 없이 오직 잡음 배경만이 얻어진다. 상관 평면의 최대 정규화된 세기 값은 0.14이다. 한편으로 이 결과는 광자 수가 제한된 암호화 함수로부터 복호화된 정보를 인증하는 것이 가능하다는 것을 증명하는 것이고, 반면에 다른 유사한 영상으로부터 구별할 수 있다는 것을 증명하는 것이다.

5. 결 론

본 논문에서는 광자 계수 영상과 이중 랜덤 위상 암호화 기술을 혼합한 새로운 영상 암호화 기법을 설명하였다. 희박한 암호화된 분포를 생성하고 복호화된 영상은 바로 시각적인 검사에 의해서는 인식될 수 없다. 암호화 처리에서 줄어든 광자 수를 사용하여 비선형 상관에 의해 암호화된 정보의 인증이 증명된다. 이 절차는 복호화된 정보가 시각적인 인식이 더 어려워지도록 만드는 잡음과 같은 모양을 가진다는 측면에서 공격자로부터 이중 랜덤 위상 암호화 기술의 취약성을 극복할 수 있게 한다.

참 고 문 헌

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

[2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Optics Letters, Vol. 20, pp. 767-769, 1995.

[3] D. Weber and J. Trolinger, "Novel implementation of nonlinear joint transform correlators in optical security and validation," Optical Engineering, Vol. 38, pp. 62-68, 1999.

[4] X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, and K. Kuroda, "Secure optical memory system with polarization encryption," Applied Optics, Vol. 40, pp. 2310-2315, 2001.

[5] T. Nomura, K. Uota, and Y. Morimoto, "Hybrid encryption of a 3-D object using a digital holographic technique," Optical Engineering, Vol. 43, pp. 2228-2232, 2004.

[6] B. Javidi, Ed. *Optical and digital techniques for information security*, Springer, New York, 2005.

[7] O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan, and B. Javidi, "Optical techniques for information security," Proceedings of the IEEE, Vol. 97, pp. 1128-1148, 2009.

[8] A. Carnicer, M. Montes-Usategui, S. Arcos, I. Juvells, "Vulnerability to chosen-cypertext attacks of optical encryption schemes based on double random phase keys," Optics Letters, Vol. 30, pp. 1444-1446, 2005.

[9] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Optics Express, Vol. 15, pp. 10253-10265, 2007.

[10] E. A. Watson, G. M. Morris, "Imaging thermal objects with photon-counting detector," Applied Optics, Vol. 31, pp. 4751-4757, 1990.

[11] G. M. Morris, "Scene matching using photon-limited images," Journal of Optical Society of America A, Vol. 1, pp. 482-488, 1984.

[12] S. Yeom, B. Javidi, E. Watson, "Photon counting passive 3D image sensing for automatic target recognition," Optics Express, Vol. 13, pp. 9310-9330, 2005.

[13] J. W. Goodman, *Statistical optics*, Wiley, New York, 2000.

[14] J. Jung, M. Cho, D. K. Dey, and B. Javidi, "Three-dimensional photon counting integral imaging using Bayesian estimation," Optics Letters, Vol. 35, No. 11, pp. 1825-1827, 2010.

[15] M. Cho, A. Mahalanobis, and B. Javidi, "3D passive photon counting automatic target rec-

ognition using advanced correlation filters," Optics Letters, Vol. 36, No. 6, pp. 861-863, 2011.

[16] I. Moon and B. Javidi, "Three dimensional imaging and recognition using truncated photon counting model and parametric maximum likelihood estimator," Optics Express, Vol. 17, No. 18, pp. 15709-15715, 2009.

[17] D. Aloni, A. Stern, and B. Javidi, "Three-dimensional photon counting integral imaging reconstruction using penalized maximum likelihood expectation maximization," Optics Express, Vol. 19, No. 20, pp. 19681-19687, 2011.

[18] M. Daneshpanah, B. Javidi, and E. Watson, "Three dimensional object recognition with photon counting imagery in the presence of noise," Optics Express, Vol. 18, No. 25, pp. 26450-26460, 2010.

[19] C.-G. Lee, I. Moon, and B. Javidi, "Photon-counting three-dimensional integral imaging with compression of elemental images," Journal of Optical Society of America A, Vol. 29, No. 6, pp. 854-860, 2012.

[20] X. Xiao and B. Javidi, "3D photon counting integral imaging with unknown sensor positions," Journal of Optical Society of America A, Vol. 29, No. 5, pp. 767-771, 2012.

[21] M. Cho and B. Javidi, "Three-dimensional photon counting integral imaging using moving array lens technique," Optics Letters, Vol. 37, No. 9, pp. 1487-1489, 2012.

[22] I. Moon and B. Javidi, "Three-dimensional recognition of photon-starved events using computational integral imaging and statistical sampling," Optics Letters, Vol. 34, No. 6, pp. 731-733, 2009.

[23] E. Perez-Cabre, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Optics Letters, Vol. 36, pp. 22-24, 2011.

[24] M. S. Millan, E. Perez-Cabre, and B. Javidi, "Multifactor authentication reinforces optical security," Optics Letters, Vol. 31, pp. 721-723, 2006.

[25] E. Perez-Cabre, M. S. Millan, and B. Javidi, "Near infrared multifactor identification tags," Optics Express, Vol. 15, pp. 15615-15627, 2007.

[26] M. Guillaume, P. Melon, P. Refregier, and A. Llebaria, "Maximum-likelihood estimation of an astronomical image from a sequence at low photon levels," Journal of Optical Society of America A, Vol. 15, pp. 2841-2848, 1998.

[27] B. Tavakoli, B. Javidi, and E. Watson, "Three-dimensional visualization by photon counting computational integral imaging," Optics Express, Vol. 16 pp. 4426-4436, 2008.

[28] M. S. Millan and E. Perez-Cabre, *Optical data encryption Optical and Digital Image Processing. Fundamentals and Applications* Ed G. Cristobal, P. Schelkens, and H. Thienpont (Weinheim: Wiley-VCH), 2011.

조 명 진

- 1997년 ~ 2003년 : 부경대학교 전자정보통신공학과 학사
- 2003년 ~ 2005년 : 부경대학교 정보통신공학과 석사
- 2005년 ~ 2007년 : 삼성전자 DM총괄 VD사업부 선행개발그룹 선임연구원
- 2007년 ~ 2011년 : Electrical and Computer Engineering, University of Connecticut 석사, 박사
- 2012년 ~ 2012년 8월 : University of Connecticut, Adjunct Faculty
- 2012년 9월 ~ 현재 : 국립한경대학교 전기전자제어공학과 조교수
- 관심분야: 3차원 디스플레이 시스템, 3차원 영상 시스템, 3차원 물체 추적 및 인식, 3차원 수중 영상 시스템, 3차원 의료영상 시스템