

이진 위상 홀로그램을 이용한 간섭성 영상 암호화 및 복원

Interferometric Image Encryption and Decryption using Binary Phase Hologram

김종윤
경동대학교 정보통신공학부 교수

Jong-Yun Kim
Professor, School of IT Eng., Kyungdong University

김정우
동양대학교 전자공학과 교수

Jeong-Woo Kim
Professor, Dept. of Electronic Eng., Dongyang University

중심어 : 광보안, 이진 위상 홀로그램, 간섭

요약

본 논문에서는 이진 위상 홀로그램과 간섭원리를 이용하여 기존의 광 암호화 방법보다 암호영상 마스크를 제작하기는 쉽고 암호 해독은 어려운 영상 암호 기법과 복원 및 인증 시스템을 제안하였다. 제안한 암호화 방법은 원영상의 홀로그램을 암호화하므로 원영상을 이중으로 암호화한다. 또한 암호화된 위상패턴을 위상카드로 제작할 경우 광세기 검출기로 볼 수 없을 뿐만 아니라 복제할 수도 없어서 개인 정보보호 및 인증시스템에 매우 유용하게 사용될 수 있다.

Abstract

In this paper, we propose the new optical security technique using two phase holograms based on interferometer. The encoded random phase image does not have any information on the original image. Without knowing the key mask, one cannot decode the encrypted image and regenerate the original image. And the use of two phase-only images in the proposed security system leads to maximum optical efficiency (100% in theory). Also they cannot be detected by an intensity detector such as a CCD camera. Computer simulations and optical experiments show performance of the proposed methods.

1. 서론

컴퓨터와 통신의 발달로 개인의 정보와 신용이 중요시됨에 따라 여권, 신용카드 등과 같은 각종 신분증을 많이 이용함에 따라 프린터, 스캐너, 또는 복사기 등을 이용한 이들의 복제가 늘고 있다. 이를 억제하기 위해 디지털 및 광학적 위조 방지 시스템에 대한 연구가 활발하다. 현재 엠보싱(embossed) 홀로그램이 부착된 각종 신용카드와 여권이 사용되고 있으나 이는 광세기 검출기를 이용하면 마스터 홀로그램 합성 및 대량복제가 가능하다. 따라서 암호키 패턴을 사용하여 영상을 복소 영상 또는 순수 위상영상으로 암호화하여 세기 검출기로는 복제가 불가능한 방법이 주로 연구된다.[1-5]

본 논문에서는 이진 위상 홀로그램과 간섭원리를 이용하여 기존의 광 암호화 방법보다 암호영상 마스크를 제작하기는 쉽고 암호 해독은 어려운 영상 암호화와 복원 방법을 제안하였다. 영상 암호화를 위해 먼저 SA(simulated

annealing) 알고리즘을 이용하여 원영상의 이진 위상 홀로그램을 구한다.[6] 그리고, 원영상을 복원하기 위한 시스템에서 암호키 역할을 하는 기준영상을 얻는다. 이때 기준영상은 암호화할 원영상의 정보를 아는 사람도 원영상을 복원할 수 없도록 무작위 잡음 발생기로부터 얻는다. 0 또는 π 의 위상값으로 구성된 홀로그램과 기준영상으로부터 원영상의 암호영상을 얻기 위해 기준영상과 암호영상의 위상차가 위상 홀로그램의 동일한 위상값에 대응되도록 암호규칙을 제안하였다. 즉 위상 홀로그램의 한 지점에서의 위상값이 0일 때, 기준영상의 동일한 지점에서의 위상값이 0이면 암호영상의 위상값은 π 가 되고, π 이면 암호영상의 위상값은 0이 되게 한다. 이렇게 암호화된 영상은 이진 위상값으로 이루어져 있어 마스크를 쉽게 제작할 수 있으나 CCD 카메라나 복사기와 같은 세기 검출기로는 측정이 불가능하다. 또한 원영상의 정보를 알고 있어도 기준영상의 다양성과 SA 알고리즘을 이용한 홀로그램의 무규칙성에 의해 암호영상 생성이 기존의 암호화 방법보다 어렵다. 암호

영상으로부터 원영상을 복원할 제안한 영상복원 시스템은 Mach-Zehnder 간섭계[7], 푸리에 렌즈, CCD 카메라, 그리고 SLM (spatial light modulator) 등으로 구성하였다. 간섭계는 암호영상과 기준영상의 간섭 홀로그램 영상을 구하기 위한 것이고, SLM과 렌즈는 각각 간섭영상을 위상 패턴으로 변조하고 푸리에 변환하기 위해 사용된다. 암호영상으로부터 원영상을 재생할 때에는 암호키 역할을 하는 기준영상과 암호영상을 제안한 영상복원시스템의 두 경로 중 위상차가 같은 위치에 각각 놓는다. 이들의 간섭영상은 CCD 카메라에 의해 검출되어 SLM과 렌즈에 의해 위상 변조와 푸리에 변환을 거쳐 푸리에 렌즈의 후초점면에 원영상으로 재생된다. 재생된 원영상은 직접 육안으로 확인 가능하고, 광상관시스템[8]을 이용하여 카드 진위 여부 및 개인인증이 가능하다. 컴퓨터 시뮬레이션과 광실험을 통해 제안한 영상 암호화 및 보안 방법이 개인 정보보호 및 인증 시스템에 유용함을 확인하였다.

II. CGH와 간섭을 기초로 한 영상 암호화

본 논문에서는 원영상의 홀로그램을 두 개의 랜덤 위상 홀로그램으로 나누어 하나는 기준영상으로 사용하고 나머지 하나는 원영상의 암호영상으로 사용하여 원영상을 암호화하였다. 이 때 두 위상 홀로그램의 간섭영상이 원영상의 홀로그램의 세기변조영상이 되도록 표 1에서 제안한 영상 암호규칙에 따라 홀로그램의 셀의 값을 각각 구한다. 즉 두 파의 경로차가 동일한 광경로를 가지는 두 지점에 위상값 0과 π 로 이루어진 기준영상과 암호영상에 대한 위상 마스크를 각각 놓아서 이들의 합성파가 세기변조영상을 표현할 수 있게 하였다. 제안한 영상 암호 방법의 주요 개념을 간단히 나타내면 그림 1에서와 같다.

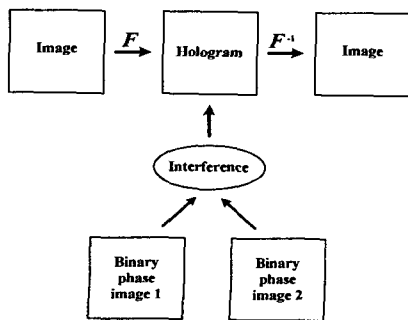


그림 1. 제안한 영상 암호화 방법의 주요 개념

표 1. 제안한 영상 암호 규칙

Hologram image	Reference image	Encrypted image
0	0	π
	π	0
π	0	0
	π	π

원영상의 암호영상을 구하는 블록도는 그림 2와 같다. 먼저 원영상의 홀로그램을 구한다. 이 때 기존의 광 영상 암호화 방법에서 필요한 복소 정함 패턴이나 다중 값 위상 영상 제작의 어려움을 해소하기 위해 이진 위상 홀로그램을 원영상의 푸리에 변환 영상으로 사용하였다. 그리고 CGH(computer generated hologram) 제작시 피할 수 없는 양자화 오차로 인한 재생영상에서의 잡음을 줄이기 위해 SA(simulated annealing) 알고리즘을 사용하였다. 이는 비용함수의 일시적 증가를 조건부 수용함으로써 비용함수가 반복과정 중의 국소(local minimum) 최적해에서 벗어날 수 있는 장점을 가지고 있다. 원영상의 홀로그램을 사용함으로써 이중암호화 효과를 가진다.

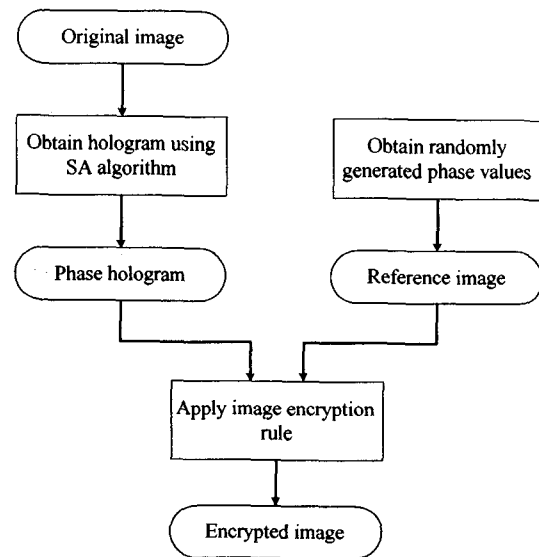


그림 2. 영상 암호기법의 블록도

그리고 기준영상은 랜덤 잡음 발생기를 사용해서 구한 후 원영상의 푸리에 영상에 따라 암호영상을 생성할 수 있다. 이 때 영상의 각 셀들은 표 1의 암호규칙을 참조하여 구하

고, 이들은 0과 π 로 구성된 위상 마스크로 제작할 수 있다. 제안한 방법을 이용하면 하나의 기준영상에 대해 암호화하고자 하는 원영상에 따라 암호영상은 다른 위상 마스크로 제작되어 개인 인증시스템에도 응용 가능하다. 그리고, 기준영상과 원영상에 대한 위상 카드는 일반 유리판을 화학적 식각을 통해 만들거나 각 화소의 위상을 제어하는 광리소그래피를 이용하여 제작할 수 있다.

III. 광학적 영상 복호화

암호화된 두 개의 위상 카드로 원영상을 복원하기 위해 제안한 광학적 보안 시스템의 영상 복원 구성도는 그림 3에서와 같고, 이는 Mach-Zehnder 간섭계, 푸리에 렌즈, SLM 등으로 이루어져 있다. 이때 HeNe 레이저와 같은 가간섭성 광원을 사용하여야 하며, 광원은 빔분할기에 의해 두 개의 경로로 나누어지고 빔분할기에 의해 다시 합쳐진다. 두 경로 중 하나에 기준영상을 두고 이의 암호영상을 경로차가 같은 다른 하나의 경로에 두면 Diffuser의 위치에서는 이들의 간섭영상을 얻을 수 있고, 이를 SLM를 이용하여 위상패턴으로 변조 후 렌즈 L을 이용하여 푸리에 변환하면 원영상을 복원할 수 있다.

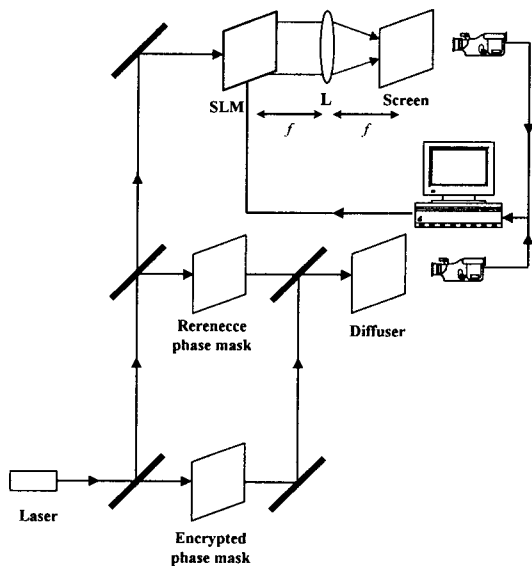


그림 3. 제안한 광 영상 복원 시스템의 구성도

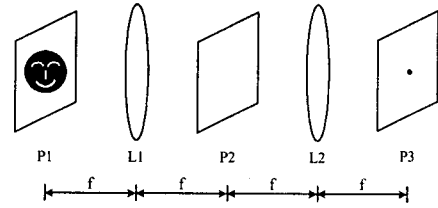


그림 4. 4f 광상관기를 사용한 암호영상의 진위여부 확인 및 개인인증 시스템 구조도

복원된 영상은 그림 4와 같은 4f 광상관기의 입력으로 사용하고, 주파수 평면에는 원영상의 푸리에 홀로그램 등을 배치하면 암호영상의 진위여부 자동 인식 및 개인 인증을 구현할 수 있다.

IV. 실험

1. 컴퓨터 모의실험

컴퓨터 모의 실험에서는 그림 5에서와 같은 영상과 마름모영상을 원영상으로 사용하였고, 이의 이진 위상 홀로그램은 그림 6에서와 같다. 그리고 랜덤 기준영상이 그림 7(a)와 같을 때, 표 1의 암호규칙을 참조하여 구한 암호 영상은 그림 7(b)와 7(c)와 같다. 여기서 그림 6과 7에서의 영상은 위상패턴을 나타낸 것이며, 영상을 이루는 밝은 셀은 위상값 π 를 나타내고 어두운 셀은 위상값 0을 나타낸다.

컴퓨터 모의실험을 통해 얻은 그림 7에서의 기준영상과 암호영상들의 간섭영상을 그림 8에서와 같다. 이 영상들의 패턴은 그림 6에서와 같으나 실제로는 세기 영상이므로 이들로부터 홀로그램을 얻기 위해서는 SLM 등을 이용한 위상 변조 과정이 필요하다.

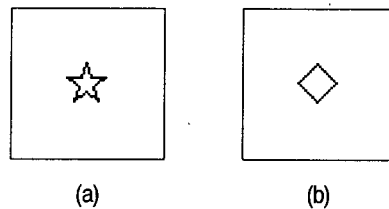


그림 5. 컴퓨터 모의실험에서 사용한 원영상들

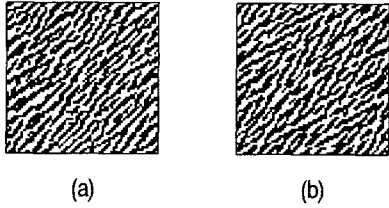


그림 6. SA 알고리즘을 사용하여 구한 그림 5의 이진 위상 홀로그램

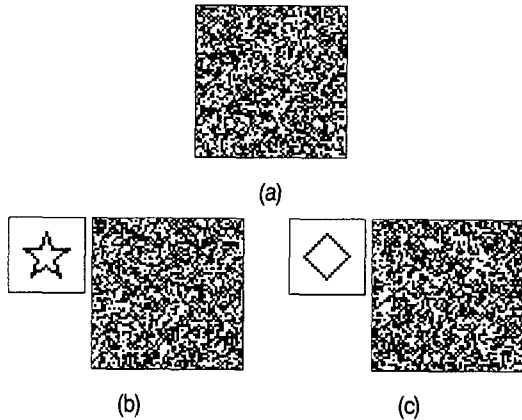


그림 7. (a) 기준 영상과 (b), (c) 그림 5에서의 원영상들에 대한 암호영상

그림 8에서의 간섭영상들을 푸리에 변환하여 얻은 복원 영상은 그림 9에서와 같고 원영상이 제대로 복원되었음을 알 수 있다. 이 때 이진 홀로그램의 특성 때문에 영상이 대칭으로 복원되는 것을 알 수 있다. 영상 복원시 기준영상이나 암호영상이 달라지면 영상이 복원되지 않는다. 예를 들어 그림 10(a)는 기준영상이 다른 경우이고 10(b)는 암호영상이 다른 경우의 복원영상이다.

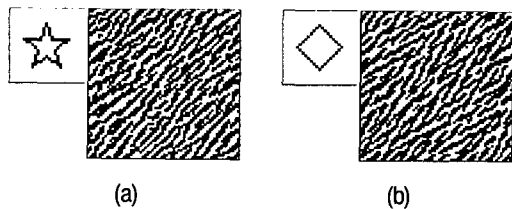


그림 8. 그림 7에서의 기준영상과 암호영상들의 간섭영상

그림 9에서 복원된 영상을 별영상을 필터로 사용한 광상 관기의 입력에 위치하여 얻은 상관결과는 그림 11에서와 같다. 그림 11의 상관결과를 내장된 문턱값으로 문턱화하여 상관첨두치의 존재유무로 개인 인증 및 암호영상의 진위여 부를 판별 가능하다.

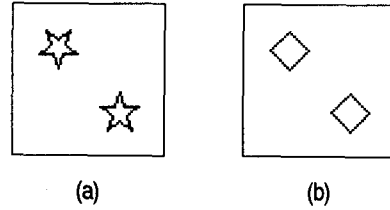


그림 9. 그림 8에서의 간섭영상을 푸리에 변환하여 얻은 복원영상

2. 광실험

제안한 광영상복원 및 인증 시스템의 타당성을 확인하기 위한 광실험은 세 부분으로 나누어 시행하였다.

먼저 두 위상영상의 간섭영상이 세기영상으로 출력되는 지 확인하기 위해 그림 12와 같이 Mach-Zehnder 간섭계를 구성하여 실험하였다. 간섭영상이 그림 13의 영상이 되도록 그림 14에서와 같이 두 이진영상으로 나눈다. 그림 14의 위상값을 가진 위상 홀로그램을 제작하기 위해서는 식각 과정이 필요할 데 이 때 사용되는 마스크 영상은 그림 15에서와 같고, 최종식각된 위상 홀로그램은 그림 16에서와 같이 육안으로는 패턴 식별이 불가능하다.

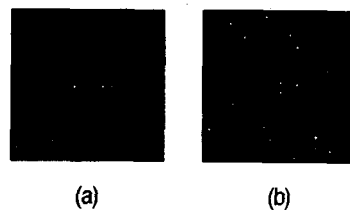


그림 10. (a) 기준영상이나 (b) 암호영상이 바뀌었을 때의 복원영상

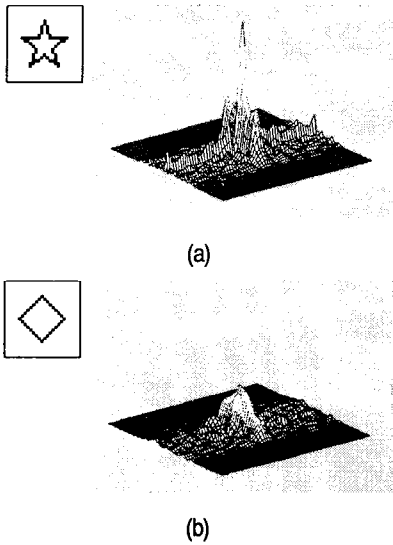


그림 11. 그림 5(a)의 영상과 그림 9의 복원영상과의 상관결과

그림 16의 위상 마스크를 그림 12에서의 간섭계의 두 경로에 두었을 때의 간섭영상은 그림 17과 같다. 재생영상에서 간섭 실험시 진동, 소음 등으로 인한 주위 잡음을 확인할 수 있다.

이진 위상 홀로그램을 푸리에 변환하여 원영상을 얻기 위한 광실험 구성도는 그림 18에서와 같다. 그림 8(a)의 별 영상의 간섭영상을 위상으로 바꾸어 복원한 영상은 그림 19에서와 같다. 이때 간섭영상의 밝은 부분은 위상을 π 로, 어두운 부분은 위상을 0으로 바꾸었다.

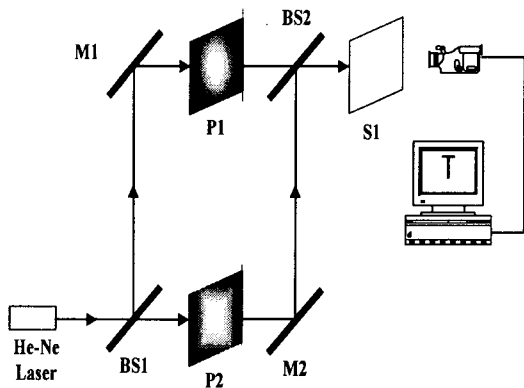


그림 12. 두 이진 위상 마스크의 간섭영상을 얻기 위한 광 실험 구성도

복원영상에서 DC 부분을 제거하기 위해 SF(spatial filter)를 사용하였다. 그림 19에서 별모양이 대각선 방향으로 쌍으로 생기는 것은 푸리에 홀로그램을 이진으로 양자화함으로 인한 것이다. 따라서 제안한 시스템을 사용하여 암호영상으로부터 원영상을 복원할 수 있음을 알 수 있다.

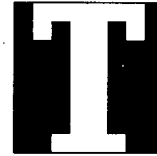


그림 13. 간섭실험을 확인하기 위한 원영상

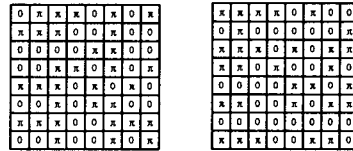


그림 14. 그림 13의 간섭영상을 얻기 위해 임의로 나눈 두 위상영상의 위상값

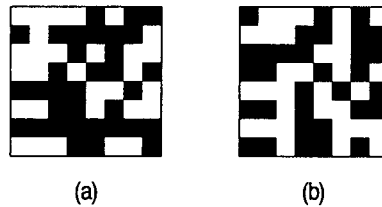


그림 15. 그림 14의 위상값들을 유리식각으로 구하기 위해 사용한 마스크 패턴

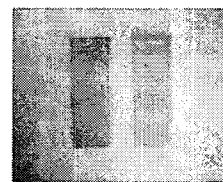


그림 16. 이진 위상 마스크

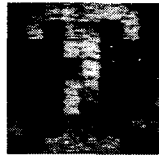


그림 17. 그림 16에서의 두 이진 위상 마스크의 간섭 패턴

복원한 영상에서 암호영상의 진위여부 및 개인인증을 확인하기 위한 광상관시스템은 그림 20에서와 같다. 그림 5(a)의 별영상과 이의 정합필터와의 광상관결과는 그림 21에서와 같다. 상관평면의 중심에 상관침두치가 있음을 확인할 수 있다. 이를 문턱화하면 침두치의 유무로 진위여부를 확인할 가능하다.

세 가지의 광실험을 통하여 제안한 광 암호 및 복원 시스템의 타당성을 확인하였다.

V. 결론

본 논문에서는 두 개의 위상 홀로그램, Mach-Zehnder 간섭계, SLM, 광상관기 등을 이용하여 이진 원영상을 랜덤한 기준영상에 대한 이진위상 암호영상으로 암호화하는 새로운 광학적 영상 암호화 방법, 영상 복원 및 인증 시스템을 제안하였다.

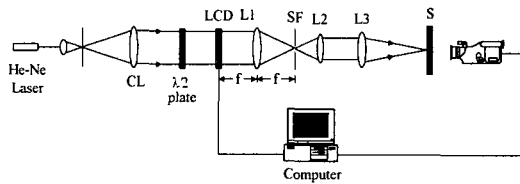


그림 18. 이진 위상 홀로그램으로부터 원영상을 얻기 위한 광실험 구성도



그림 19. 위상 홀로그램을 푸리에 변환하여 얻은 복원영상

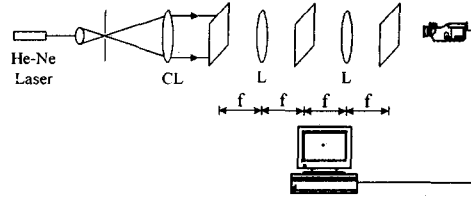


그림 20. 진위여부 및 개인인증을 위한 광실험 구성도

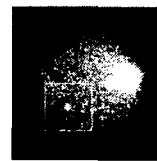


그림 21. 별영상과 이의 정합필터와의 광상관결과

0과 π 의 위상값을 가지는 랜덤한 기준영상과 파의 간섭 원리를 기초로 제안한 암호 규칙에 따라 암호 영상을 생성할 수 있었다. 이때 암호영상과 기준영상은 원영상의 홀로그램영상을 기준으로 제작하였기 때문에 원영상을 이중으로 암호화한다. 그리고 기준 영상과 암호 영상을 경로차가 같은 마흐-젠더 간섭계의 두 개의 경로에 각각 놓아서 이들을 통과하는 두 빛의 간섭 패턴을 푸리에 변환함으로써 원영상을 복원했다. 복원한 영상은 암호영상의 진위여부 및 개인인증에 사용할 수 있고, 제안한 영상암호화 및 복원시스템은 카드형태로 제작되어 개인 인증이나 정보보호에 응용가능하다.

참고 문헌

- [1] B. Javidi and J. L. Homer, "Optical Pattern Recognition for Validation and Security Verification," *Optical Engineering*, Vol. 33, No. 6, pp. 1752-1756, June, 1994.
- [2] L. G. Neto, "Implementation of Image Encryption using the Phase-contrast Technique," *Proceedings of SPIE*, Vol.3386, pp. 284-290, Apr. 1998.
- [3] R. K. Wang, I. A. Watson, and C. Chatwin, "Random Phase Encoding for Optical Security," *Optical*

- Engineering*, Vol.35, No.9, pp. 2464-2469, Sep. 1996.
- [4] J. W. Han, D. H. Ryu, D. S. Park, and E. S. Kim, "Optical Image Encryption Based on XOR Operations," *Optical Engineering*, Vol.38, No.1, pp. 47-54, Jan. 1999.
- [5] J.-Y. Kim, S.-J. Park, C.-S. Kim, J.-G. Bae, and S.-J. Kim, "Optical Image Encryption using Interferometry-based Phase Masks," *Electronic Letters*, Vol.36, No.10, pp. 874-875, May. 2000.
- [6] C.-S. Kim, J.-W. Kim, J.-K. Bae, and S.-J. Kim, "Real time Optical Image Generation using Phase Grating with Simulated Annealing Algorithm," *Journal of IEEK*, Vol. 33-B, No.6, pp. 149-155, June. 1996.
- [7] E. Hecht, *Optics*, 2nd Ed., Addison-Wesley, Ch.9, 1987.
- [8] A. Mahalanobis, B. V. K. Kumar, and D. Casasent, "Minimum Average Correlation Energy Filters," *Applied Optics*, Vol.26, No.17, pp. 3633-3640, Sep. 1987.

김 종 윤(Jong-Yun Kim)

정회원



1995년 2월 : 경북대학교 전자공학과
졸업(공학사)
1997년 2월 : 경북대학교 전자공학과
졸업(공학석사)
2001년 2월 : 경북대학교 전자공학과
졸업(공학박사)
2001년 3월 ~ 현재 : 경동대학교 정

보통신공학부 교수

<관심분야> : 콘텐츠 보호, 교육·IT 콘텐츠

김 정 우(Jeong-Woo Kim)

정회원



1987년 2월 : 경북대학교 전자공학과
졸업(공학사)
1989년 2월 : 경북대학교 전자공학과
졸업(공학석사)
1995년 8월 : 경북대학교 전자공학과
졸업(공학박사)
1996년 3월 ~ 현재 : 동양대학교 전

자공학과 교수

<관심분야> : 콘텐츠 보호, 패턴 인식