한국산업정보학회논문지 제13권 제3호(2008. 9)

이진위상 컴퓨터형성홀로그램과 다중 XOR 연산을 이용한 영상 암호화의 개선

(An Improvement of Image Encryption using Binary Phase Computer Generated Hologram and Multi XOR Operations)

김 철 수*
(Cheol-Su Kim)

요 약 본 논문에서는 이진위상 컴퓨터형성홀로그램(binary phase computer generated hologram; BPCGH)과 다중 XOR 연산을 이용하여 영상의 암호화를 개선시키는 방법을 제안하고자 한다. 먼저 암호화를 위해 원영상을 재생할 수 있는 BPCGH를 반복 알고리듬을 이용하여 설계하며, 이를 암호화할 영상으로 간주하여 랜덤하게 발생시킨 위상 키 영상과의 XOR 연산을 통해 암호화한다. 암호화된 영상을 다시 XOR 연산을 통해 여러 개의 슬라이드 영상으로 나눔으로써 암호화를 개선시킨다. 홀로그램의 복호화 과정은 암호화된 슬라이드 영상과 암호화시에 사용된 무작위 위상 키 영상을 직렬 정합시킨 후, 기준파와의 간섭에 의해 수행된다. 그리고 복호화된 홀로그램 영상은 위상 변조한 후, 역푸리에 변환하여 최종적으로 구한다. 그리고 슬라이드 영상의 패턴을 적절히 바꾸어 주면 다양한 형태의 복호화된 BPCGH 영상을 생성할 수 있다. 제안된 암호화 방법은 암호화시에 사용된 무작위 키 영상 정보가 없으면 원영상이 전혀 복원 되지 않고, 암호화된 슬라이드 영상을 달리함에 따라 복원되는 홀로그램의 패턴을 다양하게 얻을 수 있으므로 차별화된 인증 시스템에 활용할 수 있다.

핵심주제어 : 이진위상 컴퓨터형성홀로그램, XOR 연산, 슬라이드 영상, 인증 시스템

Abstract In this paper, we proposed an improvement technique of image encryption using binary phase computer generated hologram(BPCGH) and multi exclusive-OR(XOR) operations. For the encryption process, a BPCGH that reconstructs the origial image is designed, using an iterative algorithm, and the resulting hologram is regarded as the image to be encrypted. The BPCGH is encrypted through the exclusive-OR operation with the random generated phase key image. Then the encrypted image is divided into several slide images using XOR operations. So, the performance of encryption for the image is improved. For the decryption process, we cascade the encrypted slide images and phase key image and interfere with reference wave. Then decrypted hologram image is transformed into phase information. Finally, the origianl image is recovered by an inverse Fourier transformation of the phase information. If the slide images are changed, we can get various decrypted BPCGH images. In the proposed security system, without a random generated key image, the original image can not be recovered. And we recover another hologram pattern according to the slide images, so it can be used in the differentiated authorization system.

Key Words : binary phase computer generated hologram, exclusive-OR operation, slide image, authorization system

* 경주대학교 컴퓨터멀티미디어공학부

1. 서 론

사회구조가 복잡해지고, 지식 정보화 사회로 접어들면서 정보보호 및 관리에 대한 중요성이 높아지고 있으며, 이에 대한 연구가 활발히 진행되고 있다. 정보를 보호하기 위한 방법에는 4f 광상관기를 이용하여 입력 평면과 푸리에 평면에 랜덤위상 마스크를 사용하여 영상을 암호화하는 방법에 대한 연구[1-4], 원영상을 bit-plane으로 각각 나누어 암호화 키와 XOR 연산을 수행함으로써 영상을 암호화하는 방법[5], 영상 암호화를 위한 위상 마스크 제작에 phase-contrast 기술과 랜덤 위상을 이용하는 방법[6] 등 이 있으며, 중요한 정보를 안전하게 관리하기 위해서 정보를 여러 개로 분산시킨 후 임의의 개수 이상이 모여야 비밀정보에 접근할 수 있는 (k,n) 문턱치 비밀 분산법 및 시각 비밀 분산법 등[7-9]이 있다. 최근에는 이와 같은 방식들에 근거하여 정보보호 및 관리를 더 강화할 수 있는 방법에 대해 진행이 되고 있는 추세이다. 그러나 정보보호 및 관리가 강화될수록 그 방법이 복잡해지고, 구현을 위한 비용이 많이 소요된다. 본 논문에서는 BPCGH와 다중 XOR 연산 기법을 이용하여 영상정보의 암호화를 강화하는 새로운 방법을 제안하고자 한다. 먼저 원영상에 대한 BPCGH를 반복 알고리듬을 이용하여 설계한 후, 이를 암호화할 영상으로 간주하였다. 그리고 설계된 BPCGH를 랜덤하게 발생시킨 이진위상 영상과 키 위상 영상으로 나눈다. 랜덤 이진위상 영상은 다시 n 개의 랜덤 이진위상을 가지는 슬라이드 영상으로 나눈다. 즉 BPCGH가 $n+1$ 개의 랜덤 이진위상 영상으로 나누어지고, 복원이 되려면 위의 모든 영상 정보들이 있어야 가능하다. 이 과정에서 이루어지는 연산은 XOR연산이며, 이는 간섭계를 이용하면 광학적으로 구현이 가능하다.

제안된 방법은 원영상이 아닌 원영상에 대한 BPCGH를 이용하므로, 명암도영상(gray image)도 쉽게 암호화가 가능하고, 슬라이드 영상의 적절한 조합을 통해 다양한 형태의 컴퓨터형성홀로그램을 복호화할 수 있는 장점이 있기 때문에 정보의 공동소유를 통한 보안강화 및 차별화된 인증 시스템 구현 등에 응용할 수 있을 것으로 기대된다.

2. 제안한 광 암호화 방법

2-1. BPCGH의 설계

1948년 Gabor에 의해 제시된 홀로그램은[10] 물체에 의해 산란된 파면의 크기와 위상정보를 기준파와 간섭을 통하여 세기의 형태로 기록한 것이며, 이를 통하여 물체의 영상 정보를 충실히 재현할 수 있다. 특히 CGH는 회절이론에 의한 수학적인 연산을 통해 이상적인 간섭 파면을 계산하여 기록한 것이다. 연속정보의 CGH 제작은 기록소자의 해상도 제한, 정보의 저장 및 전송에서 많은 문제점이 있으므로 정보의 이진화가 요구된다. 그러나 연속정보를 이진화하면 정보의 손실이 발생하고, 영상 재생시 양자화 잡음으로 나타난다. 이를 해결하는 여러 방법들 중 최적의 해를 구할 수 있는 방법이 SA(simulated annealing)알고리듬이다.[11-12]

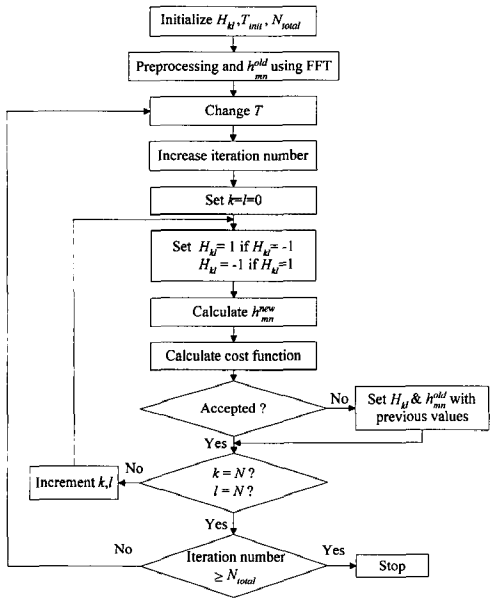
통계열역학에서 비롯된 SA 알고리듬은 복잡한 최적 해를 풀기 위한 반복적인 알고리듬으로써 국소 최적 해에서 벗어날 수 있는 반면 많은 반복과정을 수행해야 하므로 시간이 많이 소요된다. 본 논문에서는 SA 알고리듬을 이용하여 암호화할 원영상에 대한 최적의 BPCGH를 설계하였다. 원영상 함수 $h(x,y)$는 SA 알고리듬을 통해 설계된 BPCGH, 즉 $H(u,v)$를 푸리에 변환하므로써 얻을 수 있다. 각 함수는 $N\times N$화소들로 구성되어 있으며, 이들의 이산적인 표현은

$$h_{mn}=\frac{1}{N^2}\sum_{k=-N/2}^{N/2-1}\sum_{l=-N/2}^{N/2-1}\times H_{kl}\exp\left(j2\pi\left(\frac{km}{N}+\frac{\ln}{N}\right)\right) \quad (1)$$

와 같다. 여기서 H_{kl}는 $H(u,v)$의 (k,l)번째 표본화 값이며, h_{mn}는 $h(x,y)$의 (m,n)번째 표본화 값이다. 원영상 생성을 위해 SA 알고리듬에서 사용된 비용함수를 제한된 영역 내에서 목표영상과 재생된 영상 사이의 평균자승오차 E로 정의하였다.

$$E = \frac{1}{AB} \sum_{m=m_0}^{m_o+A-1} \sum_{n=n_0}^{n_o+B-1} \times \left| \left| f'_{mn} \right|^2 - \left| h_{mn} \right|^2 \right|^2 \quad (2)$$

여기서 A와 B는 각각 목표영상의 가로 및 세로의 크기를 나타내며, $f_{mn}{}'$는 목표영상의 전체 에너지를 나타낸다. 이 비용함수는 제한된 영역 내에서 목표영상을 찾아가도록 함으로써 관심영역 밖의 배경잡음을 줄여 더욱 높은 효율을 가질 수 있게 한다. BPCGH의 최적설계를 위한 SA 알고리듬의 순서도는 그림 1과 같다.



(그림 1) BPCGH의 최적설계를 위한 SA 알고리듬의 순서도

알고리듬의 수행과정은 H_{kl}의 초기값을 '1', 또는 '-1'로 무작위 선택하고, 비용함수 E^{old}를 계산한 후, 이로부터 SA 알고리듬에 사용되는 초기 온도 T_{init}, 냉각속도 D_t, 그리고 반복횟수 N를 결정한다. H_{kl}의 한 화소를 1에서 -1로 또는 -1에서 1로 바꾼 후 비용함수를 새로이 계산한다. 만약 바꾼 화소 값에 의해 새로이 계산된 비용함수가 감소하면 그 변화를 무조건 받아들이고, 그렇지 않으면 무조건 배척하는 것이 아니라 다음과 같은 확률을 도입하여 조건적으로 받아들인다.

$$P(\Delta E) = \exp(-\Delta E / T_n), \quad T_n = (D_t)^n T_{init} \quad (3)$$

여기서 P는 수용 확률을 나타내고, ΔE는 비용함수의 변화량을 나타낸다. 그리고 T_n는 n번째 반복과정에서의 온도를 나타내는 매개 변수이다. 위의 과정이 모든 화소에 대하여 반복 수행된다. 홀로그램을 구성하는 모든 화소들이 선택되면 한 번의 반복 과정이 끝나게 되고, 위에서 설명한 일련의 과정을 반복 횟수만큼 수행하게 된다.

2-2. 영상 암호화 및 복호화

본 논문에서 제안한 암호화 방법은 원래의 영상을 암호화 하는 것이 아니라 원영상의 홀로그램 정보를 암호화 시키는 것이다. 홀로그램은 그 정보의 일부를 손실하여도 원영상을 복원할 수 있는 특성이 있으므로 정보의 전송과정에서 생길 수 있는 각종 잡음 등에 상당히 둔감하다. 먼저 원영상 정보를 손실없이 재생할 수 있는 BPCGH를 SA 알고리듬으로 설계한 후, 무작위로 발생시킨 이진 위상을 구하고, 이를 암호화 및 복호화에 필요한 키 영상으로 하며, 다음 식으로 표현하였다.

$$K(x,y) = \exp[j\pi r(x,y)] \quad (4)$$

여기서 $r(x,y)$는 무작위로 발생시켜서 구한 이진영상이다. 즉 무작위로 발생시킨 이진영상을 위상 변조하면 키 영상이 생성되는 것이다. 키 영상은 무작위로 발생시킨 영상이므로 원영상 및 홀로그램에 대한 정보가 전혀 없다고 할 수 있으며, 순수한 위상값 만을 가지므로 그 세기는 '1'이 된다. 암호 영상은 홀로그램 영상과 키 영상과의 XOR연산을 통해 구하며, 다음 식으로 표현된다.

$$e(x,y) = h(x,y) \oplus r(x,y), \quad E(x,y) = \exp[j\pi e(x,y)] \quad (5)$$

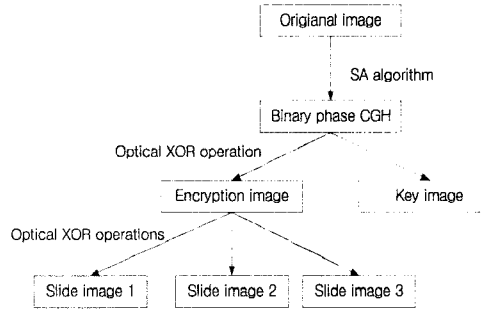
여기서 $h(x,y)$는 SA 알고리듬으로 설계된 홀로그램 함수의 이진영상이며, 첨자 $\oplus$는 XOR 연산자이다.

암호 영상 $e(x,y)$는 n개의 랜덤 이진 슬라이드 영상인 $e_1(x,y)$, $e_2(x,y)$, $\cdots$, $e_n(x,y)$로 나눈 후,

아래 식을 만족하도록 한다.

$$e(x,y) = e_1(x,y) \oplus e_2(x,y) \oplus \cdots \oplus e_n(x,y) \quad (6)$$

이 방법은 n 개의 슬라이드 영상을 XOR연산 해야만 원영상의 BPCGH 정보를 얻을 수 있다. 이와 같은 XOR연산은 LCD와 같은 공간광변조 특성이 있는 광소자를 이용하면 실시간으로 쉽게 처리할 수 있으며, 제안한 암호화 방법을 도식으로 표현하면 그림 2와 같다.



(그림 2) 제안한 암호화 방법

복호화 과정은 간섭의 원리를 이용하며, 먼저 암호화된 n 개의 슬라이드 영상과 키 영상을 간섭계의 한 경로에 직렬로 정합시킨다. 이를 수식으로 표현하면 다음과 같다.

$$\begin{aligned} m(x,y) &= E(x,y)K(x,y) \\ &= \exp[j\pi h(x,y)] \end{aligned} \quad (7)$$

또 다른 경로에는 기준파만 조사시키며, 이로부터 구해지는 간섭계 출력면에서의 세기는

$$\begin{aligned} I(x,y) &= |R(x,y) + R(x,y)m(x,y)|^2 \\ &= |R(x,y)|^2 |1 + \exp[j\pi h(x,y)]|^2 \end{aligned} \quad (8)$$

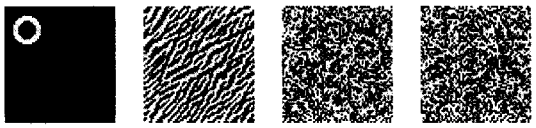
여기서 기준파는 $R(x,y) = E\exp(j\psi)$로 표현되며, E는 파의 크기, ψ는 초기위상을 나타낸다. 기준파의 세기는 $|E|^2$ 이고, 홀로그램 함수 $h(x,y)$는 '0' 또는 '1'의 값만을 가지므로 최종 간섭세기는

$$I(x,y) = |E|^2 \begin{cases} 4, & \text{for } h(x,y) = 0 \\ 0, & \text{for } h(x,y) = 1 \end{cases} \quad (9)$$

이 된다. 즉 복원하고자 하는 홀로그램 함수 $h(x,y)$의 반전 함수가 생성된다. 그러나 이진 홀로그램 함수는 그 함수가 지니고 있는 정보인 '0'과 '1'의 값이 서로 바뀌어도 재생영상이 같은 특징이 있다. 이와 같은 간섭세기를 다시 한번 위상변조한 후, 역푸리에 변환하면 원영상이 재생된다.

3. 컴퓨터 시뮬레이션 결과 및 고찰

본 논문에서 제안한 암호화 및 복호화 방법에 의한 결과를 검증하기 위해 컴퓨터 시뮬레이션을 하였으며, 이를 구현할 수 있는 광 실험 구성도를 제안하였다. 그림 3은 컴퓨터 모의실험에 사용된 이진 문자영상과 이에 대한 암호화 결과를 나타낸다.



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

(그림 3) 이진영상에 대한 홀로그램 및 암호화 결과 (a) 원영상, (b) BPCGH, (c) 키 영상, (d) 암호화된 영상

그림 3(b), (c) 및 (d)에서 검은 화소 부분은 위상이 'π', 흰 화소 부분은 '0'을 나타낸다. 그림 3(d)의 암호화된 영상은 식 (5)에서처럼 홀로그램 함수와 키 영상에 의해 결정된다. 암호화된 영상은 다시 XOR 연산에 의해 n 개의 슬라이드 영상으로 다시 나뉘어지고, n 명의 사람에게 각각 배정된다. 본 논문에서는 3개의 슬라이드 영상으로 나누었으며, 이를 그림 4에 나타내었다.

(a) (b) (c)

(그림 4) 암호화된 영상에 대한 각 슬라이드 영상 (a) 슬라이드 영상 1, (b) 슬라이드 영상 2, (c) 슬라이드 영상 3

영상의 복호화를 위해서는 마흐-젠더 간섭계의 한 쪽 경로에 n개의 슬라이드 영상과 키 영상을 직렬로 정합시킨 후, 다른 경로에는 광 경로가 동일한 기준파를 조사시켜 간섭시킨다. 이때 간섭패턴은 그림 3(b)의 홀로그램 영상이 생성되는 것이 아니라 식 (9)에 의해 홀로그램의 반전 영상이 생성된다. 이를 다시 위상 변조하여 역푸리에 변환하면 원영상이 생성된다. 이때 BPCGH는 그 위상값이 서로 바뀌어도 재생되는 영상은 동일한 특징이 있으므로 반전된 홀로그램 영상을 그대로 이용할 수 있다. 그림 5는 컴퓨터 시뮬레이션 결과를 보여주며, 모든 슬라이드 영상과 정확한 키 영상을 사용하였을 때에만 원래의 영상 정보를 복호화할 수 있음을 알 수 있다.

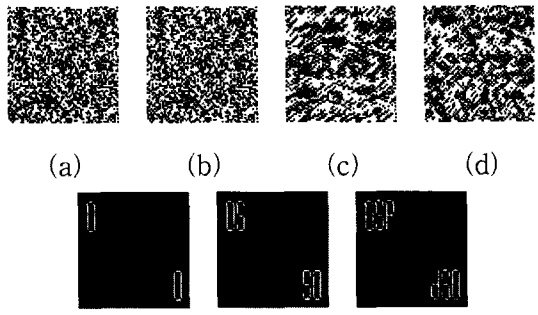
(a) (b) (c) (d)

(그림 5) 컴퓨터 시뮬레이션을 통한 복호화된 이진영상 (a) 슬라이드 영상을 모두 사용했을 때, (b) 슬라이드 영상 1이 없을 때, (c) 슬라이드 영상 1, 2가 없을 때, (d) 틀린 키 영상을 사용했을 때

제안한 방법에서는 암호화된 영상을 다시 XOR 연산을 통해 이진위상을 갖는 여러 개의 슬라이드 영상을 쉽게 생성할 수 있으므로 암호화를 보다 강화할 수 있고, 슬라이드 영상을 적절히 조합하면 다양한 형태의 원영상을 복호화할 수 있으므로, 차별화된 인증 시스템에 응용이 가능하리라 예상된다.

그림 6은 슬라이드 영상의 적절한 조합에 따른 다양한 복호화 영상을 보여주는 시뮬레이션 결과이다.

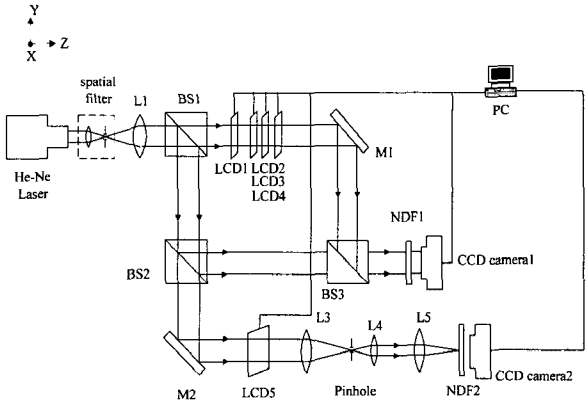
제안한 방법을 광학적으로 구현하기 위한 시스템 구성도는 그림 7과 같다. 키 영상 정보 및 3개의 슬라이드 영상 정보를 간섭계내의 한 경로에 위치한 LCD1, LCD2, LCD3, LCD4에 위상 변조하여 올린 후, 기준파와 간섭을 시키면 간섭패턴이 BS3 뒤에 나타나고, 이를 광 검출기인 CCD에서 획득하도록 구성하였다. 이 간섭세기를 다시 LCD5에 위상 변조하여 입력시키면 L3, L4, L5의 조합에 의해 푸리에 변환이 되어 원래의 영상이 최종적으로 복원된다.



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

(e) (f) (g)

(그림 6) 슬라이드 영상의 조합에 따른 복호화 영상 (a) 키 영상, (b) 슬라이드 영상 1, (c) 슬라이드 영상 2, (d) 슬라이드 영상 3, (e) 슬라이드 영상 1만을 사용했을 때, (f) 슬라이드 영상 1과 2를 사용했을 때, (g) 슬라이드 영상 1, 2 및 3을 모두 사용했을 때



L: lens M : mirror
BS1 : beam splitter (50 : 50)
BS2 : beam splitter (65 : 35)
NDF : neutral density filter
PC : personal computer
LCD1 : key image
LCD2,3,4 : slide images
LCD5 : binary phase hologram

(그림 7) 제안한 광학적 복호화 시스템

제안된 방법은 이진영상뿐만 아니라 명암도영상의 암호화에도 그대로 적용할 수 있다. 명암도 영상을 생성할 수 있는 BPCGH만 설계되면 암호화 및 복호화 과정은 이진영상일 경우와 동일하게 적용할 수 있다.

만약 이진위상이 아닌 다중위상 컴퓨터형성홀로그램을 설계하여 이용한다면 이진위상으로 인해 생기는 역상을 제거할 수 있어 출력 대역폭을 넓게 활용하고, 재생되는 영상의 효율 또한 개선시킬 수 있을 것이다. 그리고 슬라이드 영상의 정보를 적절히 제어하고, 조합하면 서로 다른 원영상을 재생할 수가 있어 그 응용성이 다양할 것으로 기대된다.

4. 결 론

본 논문에서는 BPCGH와 다중 XOR 연산을 이용하여 영상을 암호화 및 복호화하는 방법을 제안하였고, 이를 광학적으로 구현할 수 있는 시스템을 제안하였다. 암호화 과정에서는 원영상의 BPCGH을 설계하고, 이를 암호화 영상으로 활용하였다. 먼저 무작위로 발생시킨 이진위상 키 영상을 생성시키고, 홀로그램과 키 영상으로부터 암호화된 영상을 생성하였다. 암호화된 영상을 다시 n개의 슬라이드 영상으로 나누어 보안을 강화하였다. 복호화 과정은 마흐-젠더 간섭계의 한 경로에 암호화된 슬라이드 영상과 키 영상을 직렬로 정합시켜 배치시키고, 기준파와의 간섭을 통해 간섭무늬를 얻었다. 이를 위상 변조한 후, 다시 역푸리에 변환하여 원영상을 얻을 수 있었다. 제안된 방법은 원래의 영상을 암호화하는 것이 아니라 원영상의 홀로그램 정보를 암호화함으로써 기존의 방법에 비해 암호화 및 복호화 과정이 간단하고, 암호화된 슬라이드 영상 정보의 적절한 제어 및 조합을 통해 서로 다른 BPCGH를 생성할 수 있고, 이를 통해 다양한 형태의 원영상을 복원할 수 있으므로 차별화된 접근통제 제어분야에 활용할 수 있을 것으로 기대된다.

참 고 문 헌

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 32, no. 7, pp. 767- 769, 1995

[2] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Opt. Lett.*, vol. 30, no. 13, pp. 1644-1646, July, 2005.

[3] X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," *Opt. Lett.*, vol. 31, no. 22, pp. 3261-3263, Nov., 2006.

[4] X. C. Cheng, L. Z. Cai, Y. R. Wang, X. F. Meng, H. Zhang, X. F. Xu, X. X. Shen, and G. Y. Dong, "Security enhancement of double- random phase encryption by amplitude modulation," *Opt. Lett.*, vol. 33, no. 14, pp. 1575-1577, July, 2008.

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

[6] L. G. Neto, "Implementation of image encryption using the phase-contrast technique," *Proceedings of SPIE*, vol. 3386, pp. 284-290, 1998.

[7] A. Shamir, "How to share a secret," *Communications of ACM*, vol. 22, pp. 12-613, 1979.

[8] M. Naor and A. Shamir, "Visual cryptography," *Advanced in Cryptography Eurocrypt94.*, vol. 950, no.7, pp. 1-12, 1995.

[9] C. Blundo, A. D. Santis, and M. Naor, "Visual cryptography for grey level images," *Info. Proc. Lett.*, vol. 75, pp. 255-259, 2000.

[10] J. W. Goodman, *Introduction to Fourier*

Optics, Chapter 8, McGraw-Hill, New York, 2nd Ed., 1996.
[11] C. S. Kim, D. H. 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. 32-A, pp. 149-155, June, 1995.
[12] C. J. Cheng, L. C. Lin, C. M. Wang, and C. L. Chen, "Optical Joint Transform Encryption Using Binary Phase Difference Key Msk," *Opt. Rev.*, vol. 12, no. 5, pp. 367-371, 2005.

김 철 수 (Cheol-Su Kim)

- 종신회원
- 1989년 2월: 경북대학교 전자공학과(공학사)
- 1991년 2월: 경북대학교 대학원 전자공학과 (공학석사)
- 1997년 2월: 경북대학교 대학원 전자공학과 (공학박사)
- 1995년 3월~1998년 2월: 김천대학 전자통신과
- 1998년 3월~현재: 경주대학교 컴퓨터멀티미디어공학부 부교수
- 2008년 3월~현재: 미국 코네티컷대학교 전자및컴퓨터공학과 방문교수
- 관심분야 : 광통신, 정보보호, 광디스플레이, 광메모리 등