

# SA 알고리즘과 광 상관 시스템을 이용한 영상 암호화 및 복호화

김철수<sup>†</sup>, 조창섭<sup>\*\*</sup>

## 요 약

본 논문에서는 SA(simulated annealing) 알고리즘에 기반한 4-f 광 상관 시스템을 이용하여 실제적인 영상 보안 시스템을 제안하였다. 반복적인 SA 알고리즘을 이용하여 이진 위상 성분을 갖는 암호화된 영상과 키 영상을 얻고, 4-f 광 상관 시스템을 이용하여 암호화된 영상과 키 영상과의 상관을 통해 복호화된 영상이 구해진다. 제안된 방법에서는 암호화된 영상 및 키 영상이 이진 위상 성분으로 구성되므로 광 보안 시스템을 구현하기 쉬운 장점이 있다. 그리고 만약 암호화된 영상을 암호화 시스템내에서 고정시키고, 키 영상 정보만을 달리하면 서로 다른 영상을 복호화할 수 있으므로 차별화된 인증시스템에 응용할 수 있는 장점도 있다. 컴퓨터 시뮬레이션 결과는 두 영상(암호화 및 키 영상)의 이진 위상 성분에도 불구하고, 복호화영상이 생성됨을 보여준다.

## Image Encryption and Decryption Using SA Algorithm and Optical Correlator System

Cheol Su Kim<sup>†</sup>, Chang Sop Cho<sup>\*\*</sup>

## ABSTRACT

In this paper, a practical image security system using SA algorithm and 4-f optical correlator system is proposed. The encrypted image and key image with binary phase components are generated using an iterative SA algorithm. a decrypted image is found through the correlation of the encrypted and key images using 4-f optical correlator system. The encrypted and key images are consisted of binary phase components. So, it is easy to implement the optical security system using the proposed technique. And if we fix the encrypted image in the optical security system and change the key images, we get different images, so it is possible to apply to the distinguished authorization system using different key images. Computer simulations show that despite the binary phase components of the two images(encrypted and key image), decrypted images are generated.

**Key words:** Simulated annealing algorithm(시뮬레이티드 어닐링 알고리즘), correlator(상관기), encryption(암호화), decryption(복호화)

## 1. 서 론

현대 정보화 사회에서는 컴퓨터 시스템 및 통신

시스템의 결합으로 시공간을 초월하여 엄청난 양의 정보교환이 신속히 이루어지고 다양한 형태의 서비스 환경이 창출되어 사회 전반에 걸쳐 빠르게 확산됨에 따라 경제, 사회 등 전 분야에 큰 변화를 일으키고 있다. 이러한 사회는 우리생활을 보다 편리하게 만들어 주고 있지만 때로는 정보의 유출로 인한 막대한 피해를 주기도 하여서 정보보호가 매우 중요한 문제로 대두된다. 특히 정보의 공유와 개방을 목표로 개발된 인터넷으로 인해 통신선로를 통한 정보에의 불

※ 교신저자(Corresponding Author) : 김철수, 주소 : 경북 경주시 효현동 산 42-1(780-712), 전화 : 054)770-5178, FAX : 054)748-2895, E-mail : kimcs@gyeongju.ac.kr

접수일 : 2003년 3월 31일, 완료일 : 2003년 8월 8일

<sup>†</sup> 정회원, 경주대학교 컴퓨터멀티미디어공학부 조교수

<sup>\*\*</sup> 준회원, 경북대학교 대학원 전자공학과 박사과정

(E-mail : fourier38@hanmail.net)

법 침입이 새로운 사회적·법적 문제로 대두되고 있다. 또한 정보화 진전에 따라 개인의 정보와 신용이 중요시되고, 인터넷을 통한 상품구매, 의료비 결재를 위한 스마트 카드 보급계획, 여권, 신용카드, 은행카드 등과 같은 개인의 신원을 증명할 수 있는 신분증의 사용이 늘어나고 있다. 그러나 프린터, 스캐너, 복사기, 컴퓨터 관련 장치들과 각종 소프트웨어 기술의 발달로 인해 화폐, 각종 신용카드뿐만 아니라 컴퓨터 칩과 같은 제조품의 위조 및 복제기술의 수준이 높아져 국내외적으로 이로 인한 피해액이 연간 수십 억 달러에 이르고 있는 실정이다. 이에 따라 최첨단 컴퓨터, 디지털 및 광학 기술들을 이용하여 위조 방지 시스템에 관한 연구가 전세계적으로 활발히 이루어지고 있지만 위조 및 복제 기술을 훨씬 능가하는 완벽한 보안시스템은 개발되지 않고 있다. 그러므로 위조나 복제에 대한 방지 기술은 반드시 연구, 개발되어야 한다.

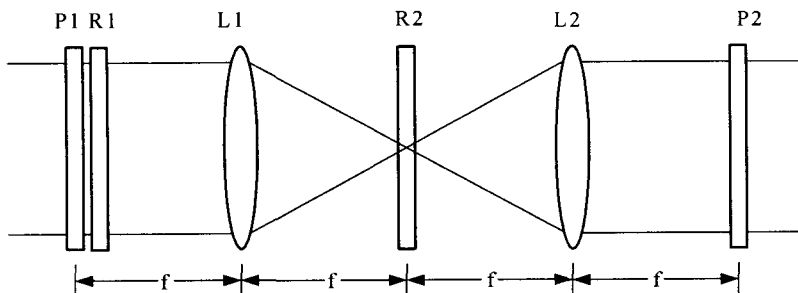
광은 고유의 병렬성과 고속성을 가지므로 많은 양의 정보를 처리할 수 있고, 정보를 표현할 수 있는 방법이 다양하여 기존의 광 세기 검출기를 이용하더라도 복제할 수 없는 특징이 있으므로 개인의 신원을 인증하는 보안시스템 구현에 많이 이용되고 있다.

광을 이용한 기존의 암호화 및 복호화 시스템에는 Refregier 등이 제안한 두 개의 랜덤 위상 마스크를 이용하는 방법[1], Mach-Zehnder 간섭계를 이용하는 방법[2], 그리고 결합 변환 상관기(JTC; joint transform correlator)를 이용하는 방법[3] 등이 있으며, 최근에는 실제로 구현하여 상용화할 수 있는 방향으로 많은 연구가 진행되고 있는 추세이다.

본 논문에서는 실제 광 보안 시스템의 구현을 위해 광 상관 시스템과 SA 알고리즘을 이용하여 이진(binary) 및 명암도(gray) 영상의 암호화 및 키 영상 정보를 이진 값으로 생성하는 방법을 제안하였으며, 컴퓨터 시뮬레이션을 통해 그 타당성을 확인하였다.

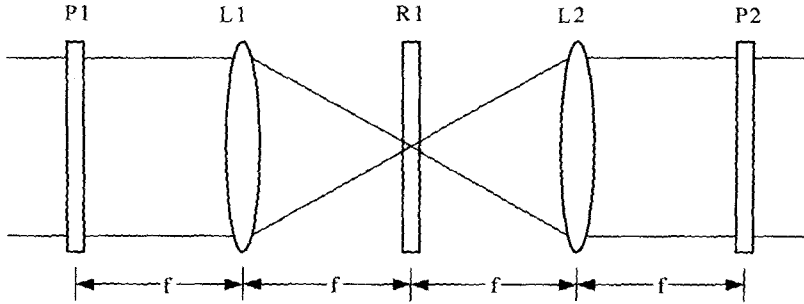
## 2. 기존의 광학적 영상 암호화 및 복호화 방법

기존의 광학적 영상 암호화 방법 중 가장 널리 연구되고 있는 방법으로는 Refregier가 제안한 4-f 광 상관 시스템을 이용하여 입력 평면과 푸리에 평면에 랜덤위상 마스크를 사용하여 영상을 암호화하는 방법이다. 즉, 그림 1, 2와 같이 두 랜덤 마스크중 하나는 입력 평면에, 다른 하나는 공간 주파수 평면에 위치해서 궁극적으로 목표영상(target image)이 stationary 백색잡음(white noise)형태로 변환되며, 복원 시스템에서는 암호화된 영상을 광학적으로 푸리에(Fourier) 변환한 후, 변환된 값에 암호키에 해당하는 랜덤 위상 마스크의 공액 복소 값을 곱하게 된다. 그리고 그 결과를 광학적으로 다시 역푸리에 변환하여 검출기가 위치해 있는 평면에서 목표영상을 복구하게 된다. 그러나 이 방법은 암호화된 영상이 복소수 값을 가지므로 카드를 제작하기 어려울 뿐 아니라 복소수 값을 나타낼 수 있는 실시간 공간 광 변조기(SLM; spatial light modulator)가 요구되는 문제점이 있다. 한편, Javidi는 더 단순한 방법으로 목표영상 위에 랜덤 위상 마스크를 접착시킴으로써 영상을 암호화하고 그 위상 마스크의 푸리에 변환된 영상의



P1 : Input image  
 R1, R2 : Phase mask  
 P2 : Encrypted image  
 L1, L2 : Fourier lens

그림 1. Refregier가 제안한 영상 암호화 시스템



P1 : Encrypted image  
 R1 : Key card  
 P2 : Decrypted image

그림 2. Refregier가 제안한 영상 복호화 시스템

공액 복소 값을 푸리에 평면에서 곱하고 역푸리에 변환해서 영상을 복원하는 방법[4]을 제시하였다. 심각한 단점은 영상에 부착된 위상 마스크를 영상에 손상을 주지 않으면서 교묘하게 떼어 내면, 카드의 위조가 가능해 진다는 것이다.

국내에서도 광학적으로 영상 암호화 및 복원 기법에 대한 연구가 일부에서 진행되고 있는데, 그중 하나가 홀로그래피 기법을 이용하여 영상 정보를 암호화하고 복원할 수 있는 방법이다[5]. 이 방법에서는 기존의 방법과 큰 차이가 없으며, 방법 과정에 디지털 처리가 들어가고, 복원시 영상 주변에 많은 잡음이 생성되는 단점이 있다. 이외에도 XOR 연산을 이용하는 방법과 phase-contrast 기술을 이용한 방법 등이 광학적 영상 암호화에 사용되었다.

Han은 목표영상을 bit-plane으로 각각 나누어 암호화 키와 XOR 연산을 수행함으로써 영상을 암호화하는 방법[6]을 제시하였다. 그러나 이 방법은 시스템이 복잡하고 영상을 bit-plane으로 변환하기 위해 디지털적인 처리가 필요하므로 광학적 장치만으로는 구현이 불가능한 단점이 있다.

그리고, Neto는 영상 암호화를 위한 위상 마스크 제작에 phase-contrast 기술과 랜덤 위상을 이용하였다. 암호화할 입력 영상을 위상 정보로 변환하고, 다시 랜덤 발생시킨 위상 정보와 더한 후 이를 감광 매질에 기록하였고, 복원할 때에는 랜덤 위상 정보의 복소 공액을 곱한 후, phase-contrast 기술을 이용하여 원래의 영상을 복원하였다[7]. 이 방법은 암호화 시 반복적인 알고리즘을 사용하지 않으므로 시간은 단축되지만 phase-contrast 기술 적용할 때 세기에

비례하는 위상값의 근사식에 대한 예러가 복원영상의 왜곡으로 나타나게 된다.

### 3. 제안한 영상 보안 시스템

#### 3.1 SA 알고리즘

SA 알고리즘은 통계열역학에서 사용된 최적화 방법으로, 반복 과정을 이용하여 온도 감소에 따른 에너지가 최소가 되는 것을 구하는 알고리즘으로 방문 판매원 문제(traveling salesmen problem)등의 조합 최적화(combination optimization)문제를 해결할 수 있다.

본 논문에서 SA알고리즘은 랜덤하게 출발한 공간 영역과 주파수 영역에 있는 두 이진 위상 영상의 상관 결과가 반복과정을 통해 목표영상(target image)에 수렴하도록 하는 주파수 영역의 이진 위상 영상 정보를 구하기 위해 이용되었다. 즉 목표영상과 반복 과정에서 생성된 두 이진 위상 영상의 상관결과와의 평균자승오차인 비용함수(cost function)가 최소가 되도록 하기 위해 SA 알고리즘에 사용되는 매개변수를 비용함수의 평균변화량을 통해 선택하였다[8].

SA 알고리즘이 가지는 특징은 초기 반복 과정 중 에서 냉각 속도에 따른 비용함수의 일시적 증가로 인해 발생할 수 있는 국소 최적해(local minimum)문제를 식 (1)과 같은 볼츠만 확률 분포식(Boltzman probability distribution)을 이용한 조건부 수용을 통해 해결 할 수 있다는 점이다.

$$T_n = (D)^n T_{mi}, \quad P(\Delta e) = \exp\left(-\frac{\Delta e}{T_n}\right) \quad (1)$$

식 (1)에서  $T_{ini}$ 는 초기 온도,  $T_n$ 는  $n$  번째 반복과정에서의 온도,  $D_t$ 는 냉각 속도,  $\mathcal{L}e$ 는 비용함수의 평균 변화량을 나타낸다. SA 알고리즘에서는 0~1 사이의 무작위 확률보다  $P(\mathcal{L}e)$ 가 클 경우에 수렴하는데, 탐색 초기에는  $T_n$ 이  $\mathcal{L}e$ 보다 상대적으로 큰 값을 가지므로, 1에 가까운 확률 값을 가지도록 하여 국소 최적해를 벗어나도록 설계하였다.

3.2 SA 알고리즘을 이용한 영상 암호화 및 복호화

기존의 광학적 암호화 시스템에서의 문제점은 여러 방법을 통해 암호화된 영상과 암호화된 영상을 해독할 때 사용되는 키 영상 정보가 복소 값 또는 연속하는 실수값을 가진다는 것과 이를 정확하게 표현할 수 있는 장치의 개발에 어려움이 있다. 본 연구에서는 이진 및 명암도 영상을 암호화하고, 해독에 필요한 키 영상 정보를 랜덤한 이진값으로 표현하여 실제 보안 시스템의 구현이 가능하도록 하기 위해 4-f 광 상관 시스템과 SA 알고리즘을 이용하였다.

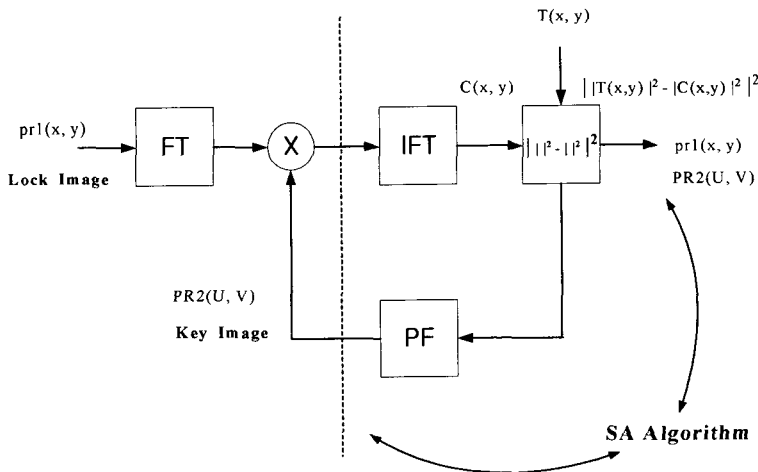
영상의 암호화 및 복호화 과정을 설명하는 블록도는 그림 3과 같다. 먼저 영상의 암호화를 위해 '1' ( $e^{j0}$ )과 '-1' ( $e^{j\pi}$ )로 구성되는 이진 위상 랜덤 패턴함수를 공간영역과 주파수영역에서 생성하고, 이를  $pr1(x, y)$  및  $PR2(U, V)$ 라 한다. 여기서  $x, y$ 는 공간 영역의 좌표이고,  $U, V$ 는 주파수영역의 좌표를 의미

한다.  $pr1(x, y)$ 를 그림 3과 같은 4-f 상관 시스템의 입력평면(R1)에 두고,  $PR2(U, V)$ 를 필터평면(R2)에 두면 두 함수의 상관 결과가 출력평면(P2)에 나타난다. 이를  $C(x, y)$ 라 하고, 암호화할 목표영상  $T(x, y)$ 와의 평균자승오차를 통해 비용함수를 구하며, 다음 식으로 표현한다.

$$E = \frac{1}{AB} \sum_{m=m_0}^{m_0+A-1} \sum_{n=n_0}^{n_0+B-1} ||T_{mn}|^2 - |C_{mn}|^2|^2 \quad (2)$$

여기서  $A$ 와  $B$ 는 각각 목표영상의 가로 및 세로의 크기를 나타내며,  $m_0$ 와  $n_0$ 는 목표영상이 시작되는 공간 위치를 나타낸다. 그리고  $T_{mn}$ 은 목표영상의 표본화 값을 나타내며,  $C_{mn}$ 은 두 이진 위상 영상의 상관 결과의 표본 값을 나타낸다.

이 비용함수는 제한된 영역내에서 목표영상을 찾아가도록 함으로써 관심영역 밖의 배경잡음을 줄여 더욱 높은 효율을 가질 수 있게 하는데, 이를 위해 필터평면의 이진 위상 랜덤함수  $PR2(U, V)$ 의 각 화소값이 '1'이면 '-1'로 '-1'이면 '1'로 변환 후 다시 비용함수를 구한 후 비용함수가 변환전의 값에 비해 감소하면 변환을 받아들이고, 증가하더라도 불쓰만 확률분포에 근거하여 조건부 수용을 하는 SA 알고리즘을 이용한다. 이와 같은 과정을 필터정보의 모든 화소에 대해 반복수행하고, 다시 반복횟수 만큼 수행



FT : Fourier transform  
 IFT : Inverse Fourier transform  
 PF : Phase flipping of each pixel in the key image

그림 3. 제안된 방법의 블록도

하면 목표영상에 가까운 상관 값을 구할 수 있다. 이때  $pr1(x, y)$ 를 목표영상의 암호화된 영상,  $PR2(U, V)$ 를 암호화된 영상의 해독에 필요한 키 영상으로 한다. 두 영상정보는 랜덤한 이진 값이므로 구현하기 쉬울 뿐 만 아니라 목표영상에 대한 정보가 전혀 포함되어 있지 않다. 그리고 목표영상이 바뀌게 되면 입력평면의 이진 위상 랜덤함수  $pr1(x, y)$ 와, 필터평면의 이진 위상 랜덤함수  $PR2(U, V)$ 를 새로이 발생시키고, 위의 과정을 되풀이하여 목표영상의 암호화된 영상 및 키 영상을 구할 수 있다. 또한 입력평면의  $pr1(x, y)$ 를 고정시키고, 필터평면의  $PR2(U, V)$ 만을 변화시켜가면서 위의 과정을 되풀이하더라도 새로운 목표영상의 키 영상을 구할 수 있다. 즉 목표영상 이 바뀌더라도 입력평면의  $pr1(x, y)$ 는 변하지 않고,  $PR2(U, V)$ 함수만을 변화시켜서 원하는 목표영상의 키 영상을 구할 수 있다는 것이다. 이와 같은 성질을 적용하면 차별화된 인증 시스템구현에도 활용할 수 있을 것으로 기대된다. 그림 3의 블록도 내에서 사용된 SA 알고리즘의 흐름도는 그림 4와 같다.

영상의 암호화 과정은 SA 알고리즘이 사용되므로 암호화과정에 소요되는 시간이 길지만, 암호화된 영

상의 복호화 과정은 암호화된 영상  $pr1(x,y)$ 와 키 영상  $PR2(U,V)$ 의 광학적인 상관을 통해 수행되므로 빛의 속도로 처리할 수 있으며, 복호화 과정에 사용되는 두 영상 정보가 이진 위상 값을 가지므로 간단히 설계할 수 있어 실제 구현도 가능하다.

#### 4. 컴퓨터 시뮬레이션 결과

본 논문에서 제안한 이중 암호화/복호화 방법에 의한 결과를 검증하기 위해 네 종류의 영상에 대해 컴퓨터 시뮬레이션 하였다. 시뮬레이션에 사용된 목표영상은 이진 문자(text) 영상, Lena 영상의 눈 부분만을 취한 명암도 영상, 그리고 크기가 다른 이진 캐릭터(character) 두 영상이며, 이를 그림 5에 나타내었다.

목표영상은  $64 \times 64$  전체 크기내에서 이진 문자 영상은  $22 \times 7$ , 명암도 영상은  $15 \times 15$ , 이진 캐릭터 영상은 각각  $18 \times 36$ ,  $18 \times 18$ 의 실제 크기를 가진다. 그림 5의 목표영상에 대해 제안된 방법인 그림 3의 블록도에 의해 생성된 최종 암호화된 영상, 키 영상, 그리고 4-f 광 상관 시스템을 이용하여 얻은 두 영상의 상관 결과인 복호화된 영상을 그림 6, 7, 8, 및 9에 나타내었다. 암호화된 영상과 키 영상은 이진 위상값을 가지며, 두 영상에서 흰 부분은 ' $\pi$ '위상을 검은 부분은

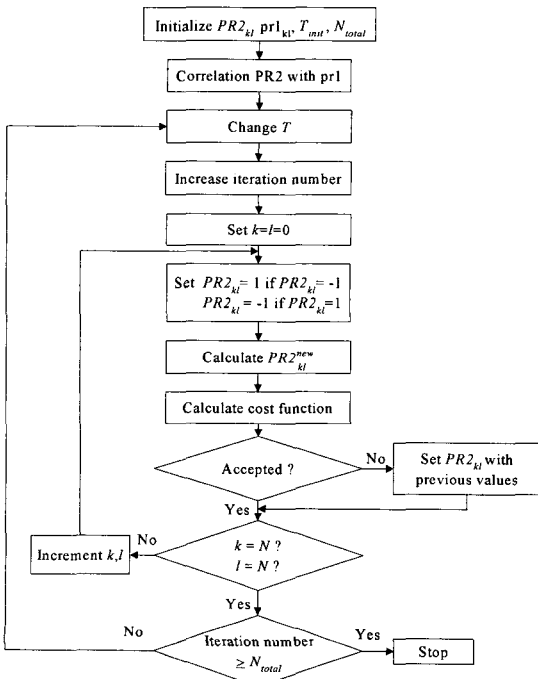


그림 4. 영상 암호화 및 복호화에 사용되는 SA 알고리즘의 흐름도

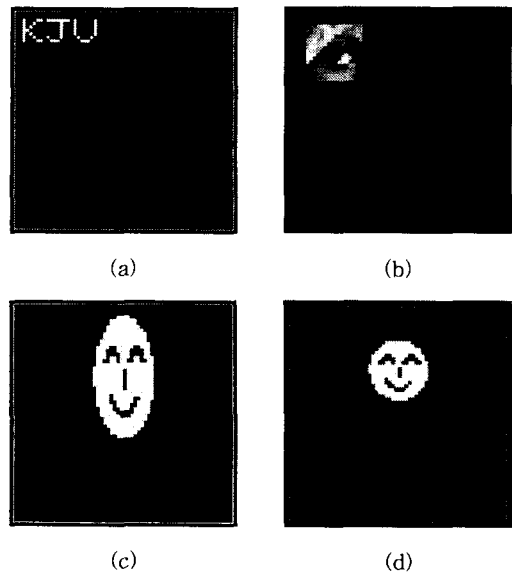
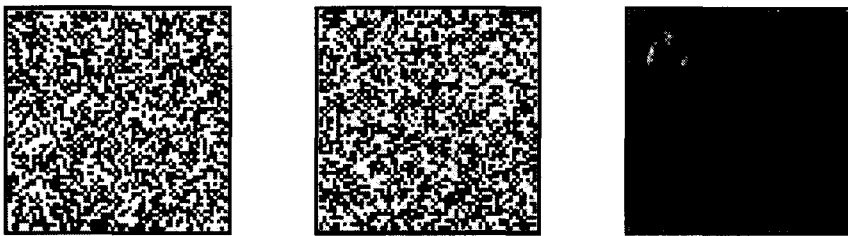


그림 5. 목표영상 (a) 이진 문자 영상 (b) 명암도 영상 (c) 이진 캐릭터 영상(대) (d) 이진 캐릭터 영상(소)



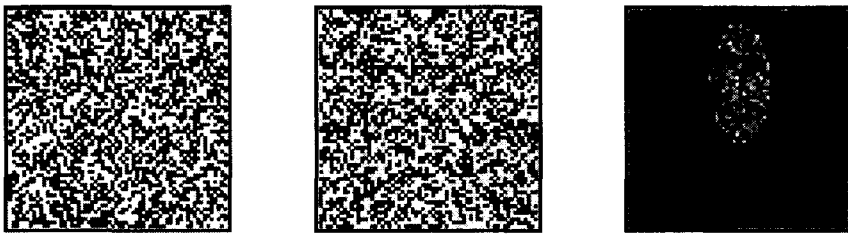
(a) (b) (c)

그림 6. 이진 문자 영상에 대한 컴퓨터 시뮬레이션 결과 (a) 암호화된 영상 (b) 키 영상 (c) 복호화된 영상



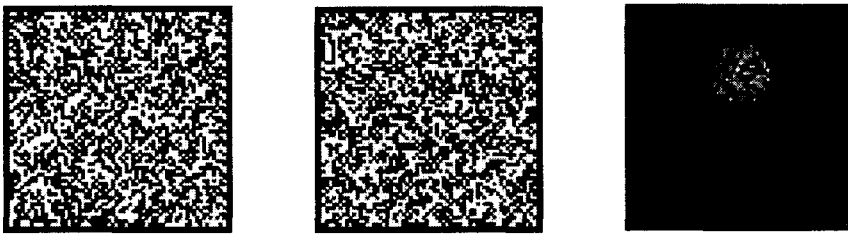
(a) (b) (c)

그림 7. 명암도 영상에 대한 컴퓨터 시뮬레이션 결과 (a) 암호화된 영상 (b) 키 영상 (c) 복호화된 영상



(a) (b) (c)

그림 8. 이진 캐릭터 영상(대)에 대한 컴퓨터 시뮬레이션 결과 (a) 암호화된 영상 (b) 키 영상 (c) 복호화된 영상



(a) (b) (c)

그림 9. 이진 캐릭터 영상(소)에 대한 컴퓨터 시뮬레이션 결과 (a) 암호화된 영상 (b) 키 영상 (c) 복호화된 영상

‘0’위상을 나타낸다.

그림 6, 7, 8 및 9에 나타난 영상들을 잘 살펴보면 각 영상들에 대한 암호화된 영상 정보가 모두 동일하고, 키 영상 정보만 다르다는 것을 알 수 있다. 즉 키 정보만 달리하면 서로 다른 영상 정보를 복호화

할 수 있다는 것이다. 이와 같은 성질은 기존의 영상 보안 시스템에서는 볼 수 없는 특징으로써 키 정보에 등급을 부여하면 차별화된 인증 시스템에 활용이 가능하리라 생각된다. 그리고 복호화된 영상 정보는 많은 반복과정을 거쳤지만 두 개의 이진 위상 정보를

상관함으로써 구한 결과이므로 원래의 영상과 똑 같을 수는 없고, 다만 SA 알고리즘에서 적절한 매개변수의 선정을 통해 그 효율을 높일 수 있다. 복호화된 영상의 객관적인 평가를 위해 도입된 평가수식인 복원율(RE; reconstruction efficiency)은 다음과 같다.

$$RE = \sum_{m=n_0}^{m_0+A-1} \sum_{n=n_0}^{n_0+B-1} \frac{|C_{mn}|^2}{|T_{mn}|^2} \times 100 \% \quad (11)$$

여기서  $m_0, n_0$ 는 실제 영상의 시작 위치를 나타내고,  $A, B$ 는 실제 영상의 가로 및 세로 크기를 나타낸다. 그리고  $T_{mn}$ 과  $C_{mn}$ 는 목표영상 및 복호화된 영상의 표본 값을 나타내며, 목표영상에 가까울수록 복원율은 '1'의 값을 가진다. 본 논문의 SA 알고리즘에서 사용된 각 영상들에 대한 변수 값들은 비용함수의 평균변화량을 통해 결정하였고, 복호화된 영상들의 복원율을 표 1에 나타내었다.

표 1에서 제시된 변수들을 사용하여 컴퓨터 시뮬레이션 한 결과 명암도 영상인 Lena 영상의 경우 약 4시간 정도 소요되었으며, 반복횟수의 증가에 따른 비용함수 값의 감소 변화를 그림 10에 나타내었다. 만약 목표영상 내의 실제 영상의 크기가 커지면 시간은 더 많이 소요된다.

시뮬레이션 결과인 영상의 복원율과 비용함수의 수렴과정을 살펴보면 복호화된 영상들이 목표영상과 차이가 많이 남을 볼 수 있는데, 이는 암호화된 영상 및 키 영상 정보가 이진 값을 가지기 때문에 복원된 영상이 목표영상에 수렴하지 못해서 나온 결과이다. 만약 이들 두 영상들의 정보를 다중 또는 연속적인 값으로 만들면 복호화된 영상의 복원율을 높일 수 있다. 그리고 그림 8, 9의 컴퓨터 시뮬레이션 결과와 표 1의 결과에서 볼 수 있는 것처럼 전체 입력 영상의 크기에서 실제 영상이 차지하는 부분을 작게 하면 즉 자유도(degree of freedom)를 높이면 복호화되는 영상 정보의 효율을 높일 수도 있다.

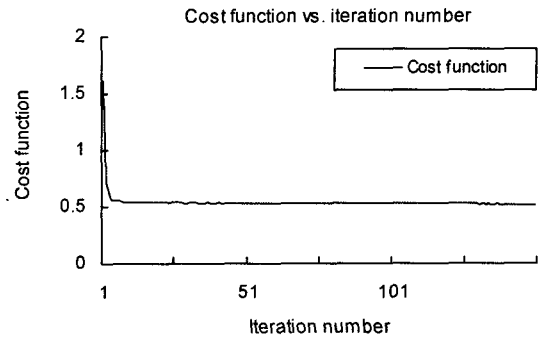


그림 10. 반복횟수의 증가에 따른 비용함수의 변화( $D_t=0.91, T_{init}=5.0$ )

만약 암호화할 때 사용된 키 정보가 아닌 다른 랜덤한 이진 위상 키 정보를 사용하게 되면 그림 11에서 볼 수 있는 것처럼 목표영상이 전혀 복호화되지 않고 잡음형태의 결과만 나타내고 있다.

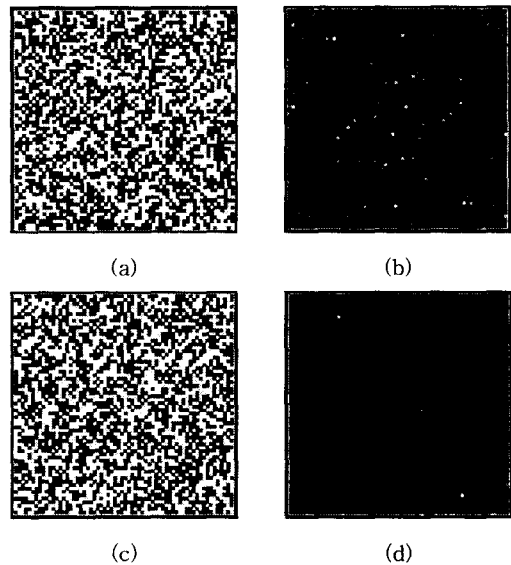


그림 11. 잘못된 키 영상 정보를 사용했을 때 복호화된 영상 (a) 이진 문자 영상의 잘못된 키 영상 (b) 그림 11(a)에 의해 복호화된 영상 (c) 명암도 영상의 잘못된 키 영상 (d) 그림 11(c)에 의해 복호화된 영상

표 1. 냉각속도, 초기온도 및 반복횟수의 변화에 따른 복호화된 영상들의 복원율

Images	Variables	Iteration number (N)	Cooling speed ( $D_t$ )	Initial temp. ( $T_{init}$ )	Reconstruction efficiency (%) (RE)
text image		150	0.94	7.0	31.8
gray image		150	0.91	5.0	39.4
character image(large)		150	0.93	10.0	41.4
character image(small)		150	0.93	5.0	48.7

## 5. 결 론

본 논문에서는 4-f 광 상관 시스템과 SA 알고리즘을 이용하여 영상의 암호화 및 복호화 방법을 제안하였으며, 컴퓨터 시뮬레이션을 통해 제안된 방법의 구현 가능성을 확인하였다. 제안된 방법에서는 암호화된 영상과 키 정보가 각각 이진 위상 성분으로 표현되어 실제 구현이 쉬우며, 암호화된 정보를 시스템내에 고정시키고, 키 영상 정보만을 달리하면 복호화되는 영상이 다르게 나타나므로 인증을 차별화하는 분야에서 활용이 가능할 것으로 예상된다. 그러나 4-f 광 상관 시스템을 사용하므로 광축 정렬문제가 존재하고, 이진 위상 정보만으로 표현되므로 복호화된 영상 정보가 목표영상과 똑 같지 않다는 단점도 있다. 그러나 이와 같은 문제는 문턱치를 설정하여 유사정도를 판단한다면 실제 구현상에서는 문제가 되지 않을 것이다.

## 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. 32, no. 7, pp. 767-769, 1995.

[2] 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, 2000.

[3] J. Ohtsubo and A. Fujimoto "Practical image encryption and decryption by phase-coding technique for optical security systems" *Applied Optics*, vol. 41, no. 23, pp. 4848-4855, 2002.

[4] B. Javidi and J. L. Honer, "Optical pattern recognition for validation and security verification", *Optical Engineering*, vol.33, no. 6, pp. 1752-1756, 1994.

[5] 양훈기, 정대섭, 김은수, "홀로그래픽 영상 암호화 및 디코딩 기법", *대한전자공학회 논문지*, 제 33권 12호, pp. 97-103, 1996.

[6] 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, 1999.

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

[8] 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.

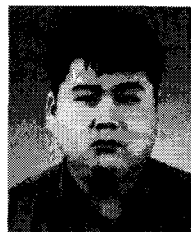


김 철 수

1989년 2월 경북대학교 전자공학과 졸업  
 1991년 2월 경북대학교 전자공학과 석사  
 1997년 2월 경북대학교 전자공학과 박사

1998년 3월 ~ 현재 경주대학교 컴퓨터멀티미디어공학부 조교수

관심분야 : 광신호처리, 홀로그래픽 광 메모리 기술, 3차원 영상 표현, 광암호화, 워터마킹 등



조 창 섭

2001년 2월 경주대학교 정보통신공학과 졸업

2003년 2월 경주대학교 컴퓨터전자공학과 석사

2003년 3월 ~ 현재 경북대학교 대학원 전자공학과 박사과정

관심분야 : 광신호처리, 컴퓨터형성홀로그램, 광암호화