

# 집적영상 및 랜덤 픽셀-스크램블링 기법을 이용한 새로운 광 영상 암호화

정회원 박 영 일\*, 종신회원 김 석 태\*\*°, 김 은 수\*

## Novel Optical Image Encryption using Integral Imaging and Random Pixel-scrambling Schemes

Yong-Ri Piao\* *Regular Member*, Seok-Tae Kim\*\*°, Eun-Soo Kim\* *Lifelong Members*

### 요 약

본 논문에서는 집적영상(integral imaging) 및 랜덤 픽셀-스크램블링(random pixel-scrambling) 기법을 이용한 새로운 광 영상 암호화(optical image encryption) 방법을 제안하였다. 즉, 제안된 방법의 부호화 과정에서는 먼저 입력영상을 여러 개의 작은 크기의 블록으로 나누어 픽셀-스크램블링을 한 다음 집적 영상 기술을 이용하여 요소 영상(elemental image)을 생성하고 이 영상의 안정성을 위하여 2차 픽셀-스크램블링을 수행하여 최종 암호화된 영상을 얻게 된다. 그리고 복호화 과정에서는 암호화된 영상에 광학적인 집적 영상 복원 기법과 역 픽셀-스크램블링 방법을 사용하여 최종적으로 원 영상을 복원하게 된다. 새로이 제안된 광 영상 암호화 기법의 잡음 첨가 및 크로핑과 같은 데이터 손실에 대한 강인성을 실험을 통해 분석하고 그 결과를 제시하였다.

**Key Words** : Optical image encryption, Integral imaging, Elemental images, Random pixel-scrambling

### ABSTRACT

In this paper, optical image encryption using integral imaging and pixel-scrambling technologies is proposed. In the encryption process, we use pixel scrambling to change the order of subsections into which the cover image is divided, and the utilize the integral imaging scheme to obtain the elemental image from the scrambled image. In order to achieve higher security, we reuse pixel scrambling to the elemental image. In the decryption process, we employ optical integral imaging reconstruction technique and inverse pixel scrambling method. Computer simulation results prove the feasibility of the proposed method and robustness against data loss and noise.

### I. 서 론

초고속 광대역 통신망과 인터넷의 발달은 대용량의 정보교환이 신속히 이루어지고 다양한 형태의 멀티미디어 서비스의 환경이 사회 전반에 걸쳐 큰 변화를 일으키고 있다. 그러나 네트워크 개인정보

유출, 불법 복제 및 악용 문제에 대해서 우려하면서 정보 보안에 대한 관심이 매우 높아지고 있다. 하지만 현재 사용하는 디지털 암호화 방법은 하드웨어 기술과 소프트웨어 기술의 급격한 발달로 인해 위조 및 복제가 고도로 정교하게 이루어지고 있으며 보안성에 한계를 갖고 있다. 이러한 문제를 방지하

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업 (IITA-2009-C1090-0902-0018)으로 연구결과가 수행되었습니다.

\* 광운대학교 차세대 3D 디스플레이 연구센터 (eskim@kw.ac.kr)

\*\* 부경대학교 전자컴퓨터정보통신공학부 (setakim@pknu.ac.kr, ° : 교신저자)

논문번호 : KICS2008-11-484, 접수일자 : 2008년 11월 3일, 최종논문접수일자 : 2009년 4월 5일

기 위해 광 정보 처리 시스템을 이용한 광학적 암호화 기법에 대한 연구가 활발히 진행되고 있다.

기존의 광 암호화 시스템은 무작위 위상마스크를 사용하여 원 영상을 암호화하며 이렇게 암호화된 영상은 전통적인 상관 시스템이나 간섭계 시스템을 이용하여 원 영상을 재생하게 되는데, 이런 무작위 위상마스크를 부착하거나 위상패턴으로 제조된 신용카드나 신분증은 복제나 위조를 방지할 수 있는 효과적인 대안이 될 수 있다. 가장 잘 알려진 광학적 영상 암호화 방법으로는 Javidi 그룹에서 제안한 원 영상에 랜덤 위상 마스크를 접촉시킴으로써 영상을 암호화하고 그 위상 마스크의 푸리에 변환된 영상의 공액 복소 값을 푸리에 평면에서 곱하고 역 푸리에 변환해서 영상을 복원하는 방법이다<sup>11</sup>. 그러나 이 방법은 영상에 부착된 위상 마스크를 영상에 손상을 주지 않으면서 교묘하게 떼어내면, 영상의 위조가 가능해진다는 심각한 단점이 있다. 한편, Refregier<sup>12</sup>는 광상관기를 이용하여 입력 평면과 푸리에 평면에 랜덤위상 마스크를 사용하여 영상을 암호화 하는 방법을 제안하였다. 즉, 두 랜덤 마스크중 하나는 입력 평면에, 다른 하나는 공간 주파수 평면에 위치해서 원 영상이 백색잡음 형태로 변환되며, 복원 시스템에서는 암호화된 영상을 광학적으로 푸리에 변환 한 후 랜덤 위상 마스크의 공액 복소값을 곱하게 된다. 그러나 이 방법은 암호화키로 복소 공액의 위상 함수를 사용하므로 정밀한 마스크 키가 필요하고 복소수 값을 나타낼 수 있는 고가의 장비가 요구 될 뿐만 아니라 또한 복호화 된 영상에 잡음이 심한 단점이 있다.

따라서, 최근에는 암호화된 정보의 강건성 및 용이한 구현을 실현하기 위하여 랜덤 픽셀-스크램블링(random pixel-scrambling) 기법을 적용한 새로운 광 정보보호 시스템을 구현하는 많은 연구들이 진행되고 있다<sup>3-5</sup>. 즉, Zhao<sup>13</sup> 등은 랜덤 픽셀 스크램블링을 진행한 입력영상에 위상 마스크를 접촉시킨 후 fractional 푸리에 영역으로 변환하여 암호화 하는 방법을 제안하였고, Meng<sup>14</sup> 등은 입력 영상을 랜덤 픽셀 스크램블링 진행한 후 프레넬 변환(Fresnel transform)을 이용하여 암호화 하는 방법을 제안하였다. 또한, Wang<sup>15</sup> 등은 랜덤 픽셀-스크램블링을 진행한 입력 영상을 이진 푸리에 변환을 이용한 컴퓨터 생성 홀로그램 (BFT CGH)으로 생성하여 암호화 하는 방법을 제안하였다. 그러나, 이러한 방법들에서는 스크램블링된 영상을 암호화하기 위한 광학적 구현 방법들이 진폭과 위상의 복소함수를 사용

하기 때문에 실제 광학적 구현에 사용할 경우 위상 정보를 진폭 정보로 변환해야 진위 여부를 판별할 수 있거나 외부 교란에 민감하고 복원 시에 영상 주변에 많은 잡음이 생성되는 문제점 등을 가지게 된다.

본 논문에서는 홀로그램 암호화와 같이 고가의 광학적 장비와 복잡한 광학적 구현이 필요하지 않고, 또한 홀로그램의 데이터 중복(redundant data)과 분산 메모리(distributed memory) 특성을 동시에 가지는 3D display 기술 중의 하나인 집적 영상(integral imaging)<sup>[6-8]</sup> 기술 기반의 랜덤 픽셀-스크램블링 기법을 이용한 영상 암호화 방법을 처음으로 제안하고자 한다. 제안된 기법에서는 먼저 입력 영상을 임의의 블록으로 나누어 랜덤 픽셀 스크램블링을 수행하고, 집적 영상 기술에서 영상 픽업(pickup) 알고리즘을 이용하여 요소 영상(elemental images)을 생성하게 된다. 이때 얻어진 요소 영상은 위상 정보 없이 진폭 정보만을 포함하게 한다. 그리고 이 요소 영상의 안정성 향상을 위하여 2차 랜덤 픽셀-스크램블링을 수행하여 최종 암호화된 영상을 얻고, 다음으로 암호화 된 영상에 잡음을 첨가하고 크로핑(cropping) 공격을 한 후, 집적 영상 복원 기법과 역 픽셀-스크램블링 방법으로 원 영상을 최종적으로 복원하게 된다.

본 논문에서는 새로이 제안된 광 암호화 방법에 대한 컴퓨터 모의실험을 수행하고 그 실험결과를 분석하고자 한다. 이를 위해, 2장에서는 새로운 광 영상 암호화 적용을 위한 집적 영상 기술의 원리를 설명하고 3장에서는 2장의 분석결과를 기반으로 집적 영상 및 픽셀-스크램블링 기술을 이용한 새로운 광 영상 암호화 기법을 제안한다. 그리고 4장에서는 제안된 암호화 기법의 실험 및 결과분석을 하고 5장에서 그 결론을 맺는다.

## II. 집적영상의 원리

최근 차세대 3D 디스플레이 기술로 고려되는 집적영상 기법이 활발하게 연구되고 있다<sup>9-15</sup>. 이 방식의 원리는 이미 1908년에 처음 제안되었고 하드웨어적인 한계로 그동안 큰 발전이 없었으나 최근 LCD, HDTV와 같은 디스플레이 장치 및 CCD와 같은 고 해상도의 영상장치 개발로 다시 큰 주목을 받고 있으며 지금까지 집적영상의 연구는 집적영상 기술 자체의 성능향상에 중점을 두고 있다. 이러한 원인으로 집적 영상 기술을 다른 분야에 응용한 예는 아직까지 없었으며 본 논문에서 처음으로 집적

영상 기반의 압축화 방법을 시도하고자 한다.

집적 영상의 주요특징은 첫째로 데이터를 획득함에 있어서 렌즈배열(혹은 핀홀 배열) 하나와 CCD 카메라만 필요하다는 광학적 구현이 용이한 장점이 있다. 둘째로, 홀로그램을 이용한 압축화 시스템은 광학적 구조가 복잡하기에 정밀한 조작을 필요로 하며 외부교란 등에 민감한 단점을 가지고 있는 반면에 집적영상 기술은 시스템 구현이 간단하기에 외부교란 등 잡음에 강인한 장점을 가지고 있다. 셋째로 렌즈배열 (혹은 핀홀배열)을 통하여 얻은 요소 영상의 집합은 원 데이터의 중복된 정보를 가지며, 또한 일부분 요소영상의 데이터가 손실할 경우에 기타 요소영상에 동일한 데이터가 중복하여 기록되어 있기 때문에 나머지 데이터를 가지고 원 데이터를 회복할 수 있는 장점이 있다. 마지막으로 요소영상은 렌즈배열(혹은 핀홀 배열)을 통하여 획득하기 때문에 부동한 시야각에서 얻어진 데이터를 갖고 있기 때문에 분산 메모리 특성을 가지고 있기 때문에 데이터 압축화에 적합하다고 할 수 있다. 그 외 집적영상은 입체영상을 관측하는데 안경과 같은 기타 도구가 필요치 않으며 2D 디스플레이와 호환성이 뛰어나며 고해상도 CCD를 통한 실시간 전송이 가능해지면 3DTV등에 응용도 가능할 것으로 전망되고 있다.

집적 영상 기술은 그림 1과 같이 픽업과 디스플레이 두 가지 부분으로 구성되어 있다. 그림 1(a)의 픽업 부분에서는 3차원 물체의 정보를 렌즈 배열과 CCD를 이용하여 요소 영상형태로 픽업 기록된다. 여기서, 픽업된 요소 영상은 각각의 작은 렌즈를 통

하여 렌즈 배열의 개수와 같은 수의 작은 물체영상이 CCD 카메라에 투영되어 기록된 것이다. 이와는 달리 디스플레이 부분에서는 얻어진 요소 영상을 이용하여 광학적인 방법과 컴퓨터적인 방법으로 3D 영상을 복원할 수 있다. 그림 1(b)는 광학적으로 3D 영상을 복원 하는 방법을 보여주고 있다. 즉, 얻어진 요소 영상을 디스플레이 장치에 표시하고 역으로 렌즈 배열을 통과하여 3D 영상을 원 위치와 동일한 위치에서 재생하게 된다. 이에 반해 그림 1(c)은 3D 영상 재생을 나타낸 것으로 컴퓨터적 집적영상 복원 (computational integral imaging reconstruction: CIIR) 이라고 한다. 이 방법은 광학적 복원 방법을 컴퓨터적으로 모델링하여 각 거리별로 평면 영상을 재생하는 방법으로 원 물체가 놓인 거리에서 재생된 영상은 선명히 나타나고 다른 거리에서는 흐려지는 특성을 가지고 있다.

보다 자세한 이해를 위해서 집적 영상의 픽업과 정과 컴퓨터 복원과정에 대해서 설명한다.

### 2.1 픽업 방법

집적 영상 기술에서 요소 영상의 픽업 원리는 그림 2와 같다. 여기서는 그림 1(a)의 렌즈 배열에서 k번째 렌즈릿에 의해 픽업되는 요소 영상을 E라고 하고, 이때 3D 물체를 O 라고 하자. 그러면 CCD 에 기록되는 k번째 요소 영상은 다음과 같이 표현할 수 있다.

$$E(x_k, y_k, -g) = O\left(\frac{x_k g}{-z}, \frac{y_k g}{-z}, z\right) \quad (1)$$

여기서  $x_k, y_k$ 는 k번째 렌즈에서 볼 수 있는 영상의 픽셀을 나타내고 g는 3D 물체와 렌즈배열 사이 거리, z는 렌즈배열과 픽업 평면 사이 거리를 나타낸다. 따라서 전체 요소 영상을 얻기 위해서는 모든 렌즈릿에 대해서 식(1)의 과정을 동일하게 반복한다. 그림 2(b)는 3D 물체와 계산되어진 요소영상의 예를 보여준다.

### 2.2 CIIR 방법

집적 영상 기술에서 3D 영상은 광학적으로 또는 컴퓨터적으로 복원이 가능한데 그림 3은 컴퓨터적 복원 방법인 CIIR 방법을 나타낸 것이다. 여기서,  $h_{pq}(x, y, z)$ 를 크기가  $s_x, s_y$ 이고 (p, q)에 위치한 요소 영상  $E_{pq}$ 가 렌즈배열을 역으로 통과하여 재생된 영상이라고 가정하면 재생한 영상  $h_{pq}(x, y, z)$ 는

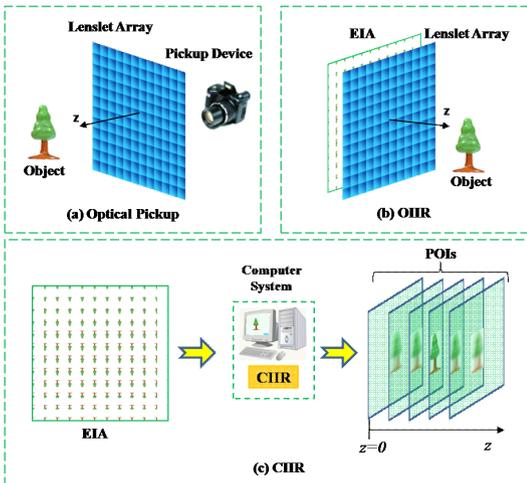


그림 1. 집적 영상 기술의 원리: (a) 픽업 (b) 디스플레이 (c) CIIR

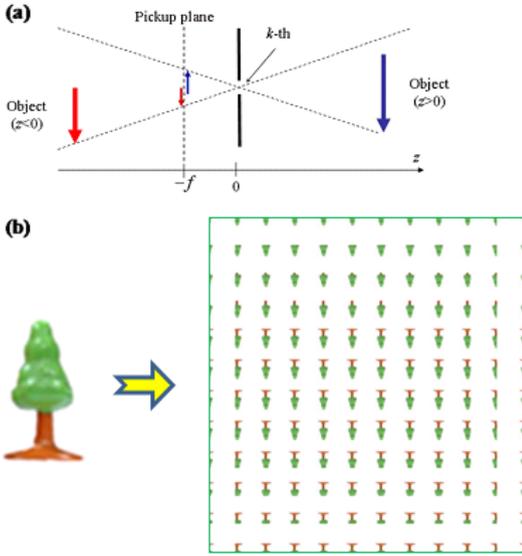


그림 2. (a) 집적 영상 기술의 픽업 원리 (b) 요소영상의 예  
식 (2)과 같이 표현할 수 있다.

$$h_{pq}(x, y, z) = \frac{E_{pq} \left[ -\frac{x}{M} + \left(1 + \frac{1}{M}\right) s_x p - \frac{y}{M} + \left(1 + \frac{1}{M}\right) s_y p \right]}{M^2}$$

$$\text{for } \begin{cases} s_x(p - M/2) \leq x \leq s_x(p + M/2) \\ s_y(p - M/2) \leq y \leq s_y(p + M/2) \end{cases}, \quad M = g/L$$

(2)

여기서  $M$ 은 영상 확대비율로서 3D 물체와 렌즈 배열 사이 거리  $g$ 와 렌즈배열과 재생 평면 사이 거리  $L$ 의 비를 나타내게 된다.  $(p, q)$ 에 위치한 요소

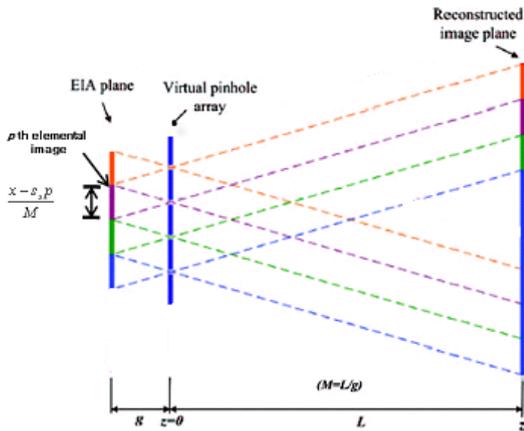


그림 3. 집적 영상 기술의 컴퓨터적 복원 원리

영상  $E_{pq}$ 로부터 재생한 영상  $h_{pq}(x, y, z)$  들은 식 (3) 을 이용하여 재생평면  $(x, y, z)$ 에서 원 3D 영상  $h(x, y, z)$ 을 재생할 수 있다.

$$h(x, y, z) = \sum_{p=0}^{m-1} \sum_{q=0}^{n-1} h_{pq}(x, y, z) \quad (3)$$

여기서  $m, n$  는 요소영상 배열의 크기를 나타낸다.

### III. 새로이 제안된 광 영상 암호화 기법

본 논문에서는 집적 영상 방식과 랜덤 픽셀-스크램블링 기술을 이용한 새로운 광 영상 암호화 기법을 제안하였다. 본 논문에서 새로이 제안된 기법의 광 영상 암호화 및 복호화 과정은 그림 4와 그림5에 각각 나타내었다.

#### 3.1 암호화 과정

먼저 암호화 과정은 그림 4에서 보이듯이 암호화하고자 하는 입력 영상  $f(x, y)$ 를  $8 \times 8$  블록으로 분할한 다음 랜덤비트 시퀀스(random bit sequence)를 생성하여  $8 \times 8$  블록 단위로 랜덤 픽셀-스크램블링(PS1)을 진행한 영상  $f'(x, y)$ 를 얻는다. 여기에서 생성된 랜덤 비트 시퀀스는 암호화 된 영상을 복호화할 때에 첫 번째 키(key1)로 사용된다. 그림 5는  $3 \times 3$  크기의 블록을 랜덤 픽셀-스크램블링한 결과 영상의 예를 보여준 것이다.

다음으로  $f'(x, y)$ 를 그림 2에서 설명한 집적 영상 기술의 픽업 과정으로 요소 영상을 획득한다. 그러나 광학적으로 요소 영상을 획득할 경우 렌즈 배열에 의한 많은 오류가 발생하기 때문에 컴퓨터적 픽업 과정(IP)을 사용한다. 즉  $f'(x, y)$  영상을 임의의 거리  $z$ 에 위치시키고 렌즈 배열에 대해서 기하 광학적 레이(ray) 해석을 통하여 요소 영상을 획득한

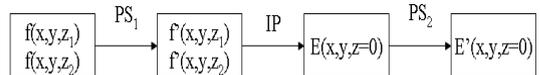


그림 4. 광 영상 암호화 과정

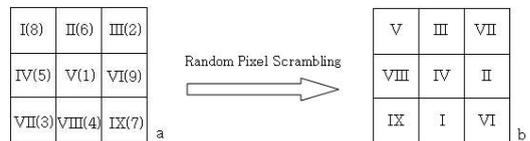


그림 5. 정 방향 랜덤 픽셀-스크램블링 방법

다. 이때 컴퓨터적으로 생성된 요소 영상을  $E(x,y)$ 로 나타낸다.

마지막으로 요소 영상  $E(x,y)$ 의 안전성 향상을 위하여 다시 랜덤 픽셀-스크램블링 (PS2)을 수행하여 최종 암호화된 영상  $E'(x,y)$ 를 얻는다. 여기서 생성된 랜덤 비트 시퀀스는 복호화 할 때에 두 번째 키(key2)로 사용된다.

### 3.2 복호화 과정

한편 새로이 제안된 광 영상 암호화 방법의 복호화 과정은 그림 6에서 보이듯이 암호화된 영상  $E'(x,y)$ 를 두 번째 암호화 키(key2)로 역 랜덤 픽셀-스크램블링(IPS2)을 수행하여 복호화된 요소 영상  $E(x,y)$ 를 먼저 얻는다. 그림 7은 3×3 크기의 블록에 대한 역 방향 랜덤 픽셀-스크램블링 과정의 예를 보여준 것이다.

다음으로 복호화된 요소영상  $E(x,y)$ 를 그림 3의 집적영상의 컴퓨터적 디스플레이 시스템을 이용하여 z 거리에서 CCD를 이용하여 3D 영상을 복원한다. 이때 복원되는 영상은 암호화 과정에서 사용한 z 값과 일치할 경우에 영상이 정상적으로 복원되고 다른 경우에서 영상이 제대로 복원되지 않는다. 따라서 z 값은 암호화의 중요한 키로써 사용되어질 수 있다. 다음으로 컴퓨터적 디스플레이 시스템에서 얻는 영상  $h(x,y)$ 에 대해서 첫 번째 암호화 키(key1)를 사용하여 역 랜덤 픽셀-스크램블링 과정을 수행하여 최종 복호화된 영상  $h'(x,y)$ 을 얻게 된다.

## IV. 실험결과

### 4.1 실험 조건

본 논문에서 제안하는 암호화 방법의 유용함을 보이기 위해서 컴퓨터 모의실험을 수행하였다. 실험에 사용하는 영상은 그림 8(a)에 보인 것과 같이 256×256 픽셀을 가지는 2진 영상이다. 첫 번째 랜

덤 픽셀-스크램블 과정에서는 8×8 블록 단위로 픽셀 스크램블을 하였고 두 번째 랜덤 픽셀-스크램블 과정에서는 256×256 크기로 픽업된 요소 영상에 대하여 픽셀-스크램블을 수행하였다. 그리고 요소 영상의 픽업 과정에서는 핀홀 배열을 16×16개로 가정하였고, 실험 영상과 핀홀 배열 간의 간격은 12 mm로 하였으며, 핀홀 배열은 z=0 mm 에 위치하였다. 그리고 요소 영상과 핀홀 배열 간격은 3 mm로 하였고 핀홀 간의 간격은 1.08mm로 가정하여 컴퓨터 픽업을 수행하였다.

### 4.2 실험 결과 및 안정성 분석

그림 8(a)의 실험 영상에 대해서 암호화 과정별로 나타난 영상을 그림 8(b)~(d)에 각각 나타내었다. 그림 8(b)은 1차 랜덤 픽셀-스크램블링 영상, 그림 8(c)은 컴퓨터 픽업 과정으로 얻어진 요소 영상, 그림 8(d)은 2차 랜덤 픽셀-스크램블링 후 최종 암호

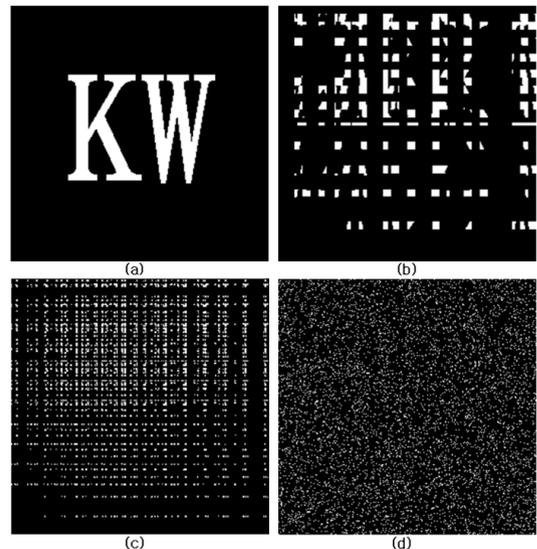


그림 8. 암호화 과정 : (a) 입력 영상, (b) 픽셀-스크램블링, (c) 요소 영상, (d) 픽셀-스크램블링 후 암호화된 영상

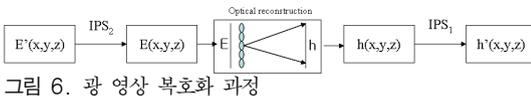


그림 6. 광 영상 복호화 과정

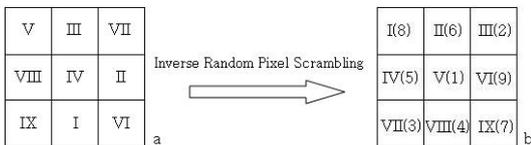


그림 7. 역 방향 랜덤 픽셀 스크램블링 방법

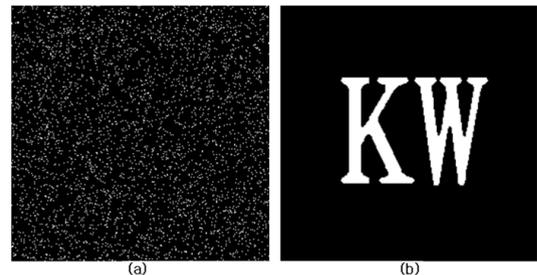


그림 9. 복호화 과정: (a) 잘못된 암호화기로 복원한 영상, (b) 정확한 암호화기로 복원한 영상

화 된 영상을 나타내고 있다. 그림 8(d)에서 볼 수 있듯이 제안한 방법의 암호화 영상을 원 영상과 비교하면 최종 암호화된 영상은 잡음 패턴과 같이 나타내면서 픽셀간의 상관성이 없음을 알 수 있다.

그림 9는 그림 8(d)의 암호화된 영상에 대해서 그림 5의 복호화 과정에 따라 잘못된 암호화키와 정확한 암호화키를 이용하여 복원한 실험결과를 보여준다. 그림 9(a)는 잘못된 암호화키로 복원된 영상을 나타내고 있으며 그림 9(b)는 정확한 암호화키로 복원한 원 영상을 나타내고 있다. 그림 9의 결과에서 알 수 있듯이 제안방법은 암호화키에 민감하며 오직 정확한 암호화키를 사용한 경우에만 원 영상을 복원할 수 있으며 잘못 된 암호화키를 사용한 경우에 원 영상은 복원할 수 없을 뿐만 아니라 노이즈와 같이 원 영상과 아무 상관없는 데이터를 얻는다는 것을 알 수 있다.

### 4.3 실험 결과 및 강인성 분석

본 논문에서 제안하는 광 암호화 방법의 강인성을 검증하기 위하여 그림 8(d)의 암호화된 영상에 크로핑과 가우시안 잡음 첨가를 진행하여 정확한 키로 복원하는 실험을 수행하였다.

그림 10(a)~(c)는 25%, 55%, 85%를 크로핑 공격을 한 암호화 영상을 나타내고 그림 10(d)~(f)는 복원한 영상을 나타낸 것이다. 그림 10에서 볼 수 있듯이 암호화 된 영상의 85%가 손실 되었을 경우에도 암호화키로 원 영상을 복원 할 수 있을 뿐만 아니라 복원 영상에서 원 영상의 모습이 선명하게 잘 나타난다는 것을 알 수 있다. 그림 11은 85% 크로핑 공격에 대한 제안방법과 BFT CGH<sup>[5]</sup>, 픽셀-스크램블링 등 기존방법과의 비교를 나타내고 있다. 그림 11(d)~(f)의 복원 영상에서 볼 수 있듯이 제안 방법은 복원한 영상이 다른 방법에 비하여 선명하게 나타나며 표 1에서 제안방법의 PSNR값은 17.1139dB로 나타나 기존 방법에 비해 크로핑과 같은 데이터 손실에 더 강인하다는 것을 증명할 수 있다.

그림 12(a)는 암호화된 영상에 Mean=0이고 Variance가 0.1, 0.3, 0.5인 가우시안 잡음을 첨가한 암호화 영상을 나타내고 그림 12(b)는 암호화키로 복원한 영상을 각각 나타낸 것이다. 그림 12에서 볼 수 있듯이 본 논문에서 제안한 방법은 가우시안 잡음을 첨가에도 원 영상을 복원할 수 있을 뿐만 아니라 광학적인 빛의 산란 등의 특성으로 인해 영상 전체에 분포된 잡음이 다른 방법에 비해 제안 방법의 복원 영상에서 일정하게 제거된 것을 그림 13(d)에서 확

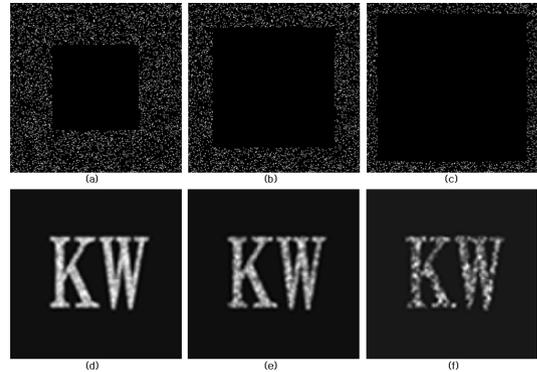


그림 10. 크로핑 공격 후 복호된 영상: (a)~(c) 25%,55%, 85% 크로핑 한 암호화 영상, (d)~(f) (a),(b),(c)에 대한 복원영상

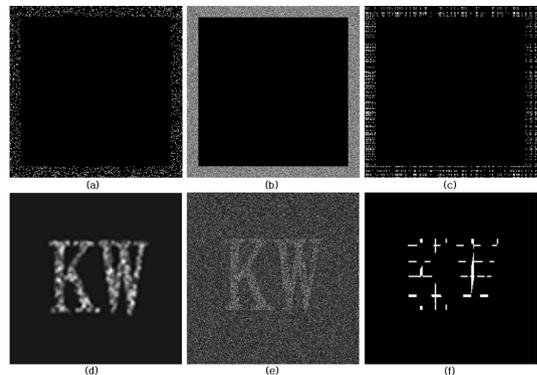


그림 11. 85% 크로핑 공격에 대한 다른 방법과의 비교: (a) 제안방법, (b) BFT CGH 방법, (c) 픽셀-스크램블링 방법, (d)~(f) (a),(b),(c)에 대한 복원영상

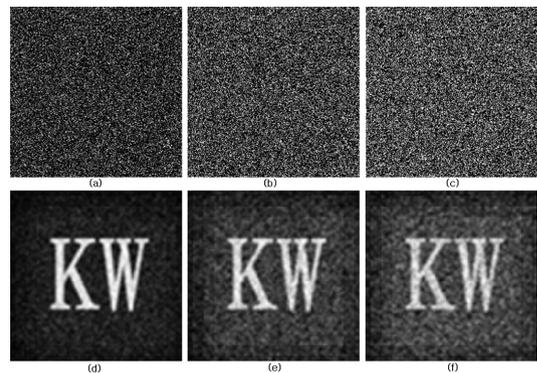


그림 12. 가우시안 잡음 첨가 후 복원된 영상: (a)~(c) Mean이 0이고 Variance가 각각 0.1, 0.3, 0.5 인 가우시안 잡음을 첨가한 암호화된 영상, (d)~(f) (a),(b),(c)에 대한 복원영상

인할 수 있다. 표 2의 PSNR값의 비교결과에서도 제안방법은 기존 방법에 비해 잡음에 대한 강인성을 검증할 수 있었다.

표 1. 85% 크로핑 공격에 대한 복원영상들의 PSNR 비교

	PS method	BFT CGH method	Proposed method
PSNR	5.5780 dB	9.4449 dB	17.1139 dB

표 2. Mean이 0이고 Variance가 0.4인 가우시안 잡음 첨가에 대한 복원영상들의 PSNR 비교

	RPS method	BFT CGH method	Proposed method
PSNR	7.4242 dB	9.2800 dB	15.9126 dB

4.4 실험 결과 및 유용성 분석

또한 본 논문에서의 제안방법이 다중 영상 암호화에도 가능함을 보이기 위해 그림 14(a)와 (b)에 나타난 256×256 픽셀을 가지는 그레이 영상으로 4.1절의 동일한 실험조건에서 추가적으로 실험을 수행하였다. tree와 cow 두 영상을 각각 렌즈베열로부터 12mm와 30mm인 곳에 위치하고 요소영상을 픽업하고 암호화를 진행하였으며 암호화된 영상을 그림 15(a)에 나타내고 있다. 그림 15(b)는 역 방향 랜덤 픽셀-스크램블링을 한 후 회복한 tree와 cow의 요소영상을 나타내고, 두 물체가 원래 위치한 z=12mm, z=30mm인 거리에서 회복한 tree와 cow 두 영상을 그림 15(c)와 (d)에 나타내고 있다. 그림 15(c)와 (d)에서 볼 수 있듯이 집적영상 기술을 암호화에 적용하였기 때문에 비록 암호화 과정에 cow의 머리 부분이 tree에 의해 가려져 있었지만 복원된 cow 영상에 머리 부분의 가려진 원 데이터까지 회복된다는 것을 검증할 수 있다. 때문에 집적영상 기술을 암호화에 적용하면 통신 중에 일부분 데이터가 손실되거나 수정되었을 경우에도 그 부분의 데이터가 복원되는 장점을 가지고 있기 때문에 데이터 통신에서 유용하다는 것을 알 수 있다.

V. 결 론

본 논문에서는 최근 3D 영상 기술에서 새로운 방식으로 알려진 집적 영상 기술에서 요소 영상을 획득하는 방법과 랜덤 픽셀-스크램블링 기술을 이용한 새로운 광 영상 암호화 방법을 제안하였다. 제안된 기법에서는 픽셀간의 상관성을 제거하기 위하여 먼저 입력영상을 여러 개의 작은 사이즈의 블록으로 나누어 랜덤 픽셀-스크램블링을 하였다. 다음 3D 집적 영상에서 광 영상 픽업방법을 이용하여 요소 영상을 생성하고, 마지막으로 요소 영상의 안정성 향상을 위하여 랜덤 픽셀-스크램블링을 수행하여 최종적으로 광 암호화된 영상을 얻었다. 암호화 된 영상에 가우시안 잡음 첨가와 크로핑 공격을 한 후

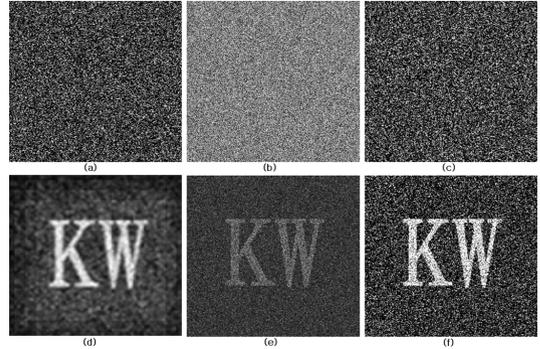


그림 13. Mean이 0이고 Variance가 0.4인 가우시안 잡음 첨가에 대한 다른 방법과의 비교: (a) 제안방법, (b) BFT CGH 방법, (c) 픽셀-스크램블링 방법, (d)-(f) (a),(b),(c)에 대한 복원영상



그림 14. (a) Tree 영상, (b) Cow 영상

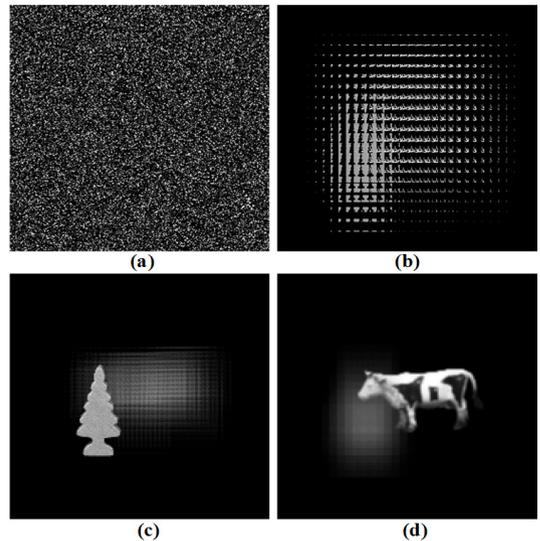


그림 15. (a) 암호화된 영상, (b) 요소영상, (c) z=12mm에서 복원한 tree 영상, (d) z=30mm에서 복원한 cow 영상

광학적 집적 영상 복원 기법과 역 픽셀-스크램블링 방법으로 복원한 실험결과를 분석함으로써 본 논문에서 새로이 제안한 영광영상 암호화 기법의 유용성과 공격에 대한 강인성을 증명하였다.

참 고 문 헌

[1] B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.*, Vol. 33, No. 6, pp. 1752-1756, 1994.

[2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and fourier plane random encoding," *Opt. Lett.*, Vol. 20, No. 7, pp. 767-769, 1995.

[3] Jianlin Zhao, Hongqiang Lu, Xiaoshan song, Jifeng Li and Yanhua Ma, "Optical image encryption based on multistage fractional Fourier transforms and pixel scrambling technique," *Opt. Comm.* 249, pp. 493-499, 2005.

[4] X. F. Meng, L. Z. Cai, X. L. Yang, X. X. Shen and G. Y. Dong, "Information security system by iterative multiple-phase retrieval and pixel random permutation," *Appl. Opt.*, Vol. 45, pp. 3289-3297, 2006.

[5] Y. Y. Wang, Y. R. Wang, Y. Wang, H. J. Li and W. J. Sun, "Optical image encryption based on binary Fourier transform computer-generated hologram and pixel scrambling technology," *Opt. and Lasers in Engineering* 45, pp. 761-765, 2007.

[6] J. -S. Jang and B. Javidi, "Improved viewing resolution of 3D integral imaging with non-stationary micro-optics," *Opt. Lett.*, Vol. 27, pp. 324-326, 2002.

[7] R. Martinez-Cuenca, A. Pons, G. Saavedra, M. Martinez-Corral and B. Javidi, "Optically-corrected elemental images for undistorted integral image-display," *Opt. Express* 14, pp. 9657-9663, 2006.

[8] D. H. Shin and H. Yoo, "Image quality enhancement in 3D computational integral imaging by use of interpolation methods," *Optics Express* 15, pp. 12039-12049, 2007.

[9] S. A. Benton, ed., *Selected Papers on Three-Dimensional Displays* (SPIE Optical Engineering Press, Bellingham, WA, 2001).

[10] T. Okoshi, "Three-dimensional display," *Proc. IEEE* 68, pp. 548-564, 1980.

[11] A. R. L. Travis, "The display of Three-dimensional video images," *Proc. of IEEE* 85,

pp. 1817-1832, 1997.

[12] D. H. McMahon and H. J. Caulfield, "A technique for producing wide-angle holographic displays," *Appl. Opt.* 9, pp. 91-96, 1970.

[13] G. Lippmann, "La photographie integrale," *Comptes-Rendus Academie des Sciences* 146, pp. 446-451, 1908.

[14] F. Okano, H. Hoshino, J. Arai, and I. Yuyama, "Real-time pickup method for a three-dimensional image based on integral photography," *Appl. Opt.* 36, pp. 1598-1603, 1997.

[15] S.-W. Min, B. Javidi, and B. Lee, "Enhanced three-dimensional integral imaging system by use of double display devices," *Appl. Opt.* 42, pp. 4186-4195, 2003.

박 영 일 (Yong-Ri Piao)

정회원



2003년 8월 JiLin University  
통신공학과, 공학사  
2005년 8월 부경대학교 정보통신공학과, 공학석사  
2008년 8월 부경대학교 정보통신공학과, 공학박사  
2008년 9월~현재 광운대학교 차

세대 3차원 디스플레이 연구센터, 연구교수  
<관심분야> 영상처리, 암호화, 집적영상 디스플레이, Cellular automata.

김 석 태 (Seok-Tae Kim)

종신회원



1983년 8월 광운대학교 전자공학과, 공학사  
1988년 8월 Kyoto Institute of Technology, 전자공학과, 공학석사  
1991년 8월 Osaka대학교 통신공학과, 공학박사

1999년 Univ. of Washington, USA, 방문교수  
2006년 Simon Fraser Univ., Canada, 방문교수  
1991년~현재 부경대학교 전자컴퓨터정보통신공학부 재직, 교수  
<관심분야> 영상처리, 패턴인식, 워터마킹, Cellular automata.

김 은 수 (Eun-Soo Kim)

종신회원

한국통신학회지 Vol. 24, No. 9A 참조