

집적 영상 방식과 랜덤 픽셀 스크램블링 기술을 이용한 3D 영상 암호화

박영일¹ · 김석태^{2*} · 김은수¹

¹광운대학교 · ²부경대학교

3D image encryption using integral imaging scheme and pixel-scrambling technology

Yongri Piao¹ · Seok-Tae Kim^{2*} · Eun-Soo Kim¹

¹ Kwangwoon University · ² Pukyong National University

*E-mail : setakim@pknu.ac.kr

요 약

본 논문에서는 집적 영상 (integral imaging) 방식과 픽셀 스크램블링 (pixel scrambling) 기술을 이용한 광 영상 암호화 (optical image encryption) 방법을 제안한다. 제안한 방법의 부호화 과정에서는 먼저 입력영상을 여러 개의 작은 사이즈의 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 얻는다. 그리고 복호화 과정에서는 암호화된 영상에 광학적인 집적 영상 복원 기법과 역 픽셀 스크램블링 방법을 사용하여 원 영상을 복원한다. 제안하는 광 암호화 방법에 대해서 크로핑과 같은 데이터 손실 및 노이즈에 대한 컴퓨터 적으로 모의실험을 수행하여 강인성과 유용성을 보였다.

키워드

3D image encryption, Random pixel scrambling, Elemental image, Security

I. 서 론

최근 컴퓨터 및 인터넷 기술의 비약적인 발전으로 디지털 데이터의 안정성 보장과 불법적인 내용 조작을 동시에 막을 수 있는 암호화 방법이 활발히 연구되고 있다. 기존의 암호화 방법들은 주파수 영역에서는 DCT와 DWT[1-2]를 이용하여 연구되고 있고 공간 영역에서 Chaotic sequence[3-4]를 이용한 암호화 연구가 주류를 차지하고 있다.

또한 랜덤 위상 변조[5-6]방식과 fractional Fourier transform[7-9]를 기반으로 하여 픽셀 스크램블링을 광학시스템에 적용하여 암호화 하는 광학적 기술로 데이터 암호화하는 연구가 주목을 받고 있다.

본 논문에서는 최근 3D 영상 기술에서 새로운 방식으로 알려진 집적 영상 (integral imaging) [10-12]기술과 랜덤 픽셀 스크램블링 (random pixel scrambling)을 이용한 광 영상 암호화 방법을 새로이 제안한다. 제안하는 방법은 먼저 입력영상을 임의의 블록으로 나누어 랜덤 픽셀 스크램블링을 수행하고 집적 영상 기술에서 영상

픽업(pickup) 알고리즘을 이용하여 요소 영상을 생성한다. 그리고 이 요소 영상의 안정성 향상을 위하여 2차 랜덤 픽셀 스크램블링을 수행하여 최종 암호화된 영상을 얻는다. 다음으로 암호화 된 영상에 노이즈첨가와 크로핑(cropping) 공격을 첨가한 후 광학적 집적 영상 복원 기법과 역 픽셀 스크램블링 방법으로 원 영상을 복원한다. 제안하는 광 암호화 방법에 대해서 기초적인 컴퓨터 모의실험을 수행하고 실험결과를 보고한다.

II. 집적 영상의 원리

집적 영상 기술은 1908년에 처음 제안되었으며 하드웨어적인 한계로 그동안 큰 발전이 없었으나 최근에 LCD, HDTV와 같은 디스플레이 장치 및 CCD와 같은 고 해상도의 영상장치 개발로 다시 큰 주목을 받고 있으며 연구가 활발히 진행되고 있다. 이 방식의 주요한 특징은 구조가 간단하고 입체영상을 관측하는데 안경과 같은 기타 도구가 필요하지 않으며 2D 디스플레이와 호환성이 뛰어나고 해상도 CCD를 통한 실시간 전송이 가능해

지만 3DTV등에 응용이 가능할 것으로 예상된다. 집적 영상 기술은 그림 1과 같이 픽업과 디스플레이 두 가지 부분으로 나눌 수 있다. 그림 1(a)의 픽업 부분에서는 3차원 물체의 정보를 렌즈 배열과 CCD를 이용하여 요소 영상을 기록한다. 픽업된 요소 영상은 각각의 작은 렌즈를 통하여 렌즈 배열의 개수와 같은 작은 영상이 CCD 카메라에 투영되어 기록된 것이다. 이와는 달리 그림 1(b)의 디스플레이 부분에서는 얻어진 요소 영상을 디스플레이 장치에 표시하고 렌즈 배열을 사용하여 3D 영상을 원 위치와 동일하게 재생할 수 있다.

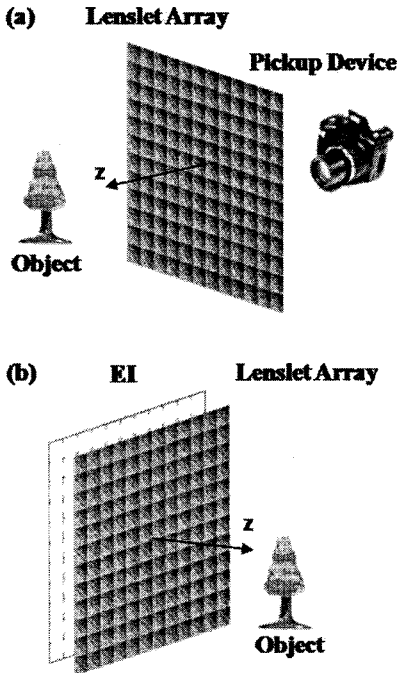


그림 1. 집적 영상 기술 (a) 픽업 (b) 디스플레이

III. 제안하는 광 영상 암호화 방법

본 논문에서는 집적 영상 방식과 랜덤 픽셀 스크램블링 기술을 이용한 새로운 광 영상 암호화 방법을 제안한다. 본 논문에서 제안하는 방법의 암호화 및 복호화 과정을 그림 2와 그림 3에 각각 나타내었다.

3.1 암호화 과정

먼저 암호화 과정은 그림 2에서 보이듯이 암호화 하고자 하는 입력 영상 $f(x,y)$ 를 8×8 블록으로 분할한 다음 랜덤비트 시퀀스를 생성하여 8×8 블록 단위로 랜덤 픽셀 스크램블링(PS1)을 진행한 영상 $f'(x,y)$ 를 얻는다. 여기에서 생성된 랜

덤 비트 시퀀스는 암호화 된 영상을 복호화 할 때에 첫 번째 키(key 1)로 사용된다. 그림 4는 3×3 사이즈의 블록을 랜덤 픽셀 스크램블링한 결과 영상을 보여주는 예이다.

다음으로 $f'(x,y)$ 를 그림 1(a)에서 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 해석을 통하여 요소 영상을 획득한다 [12]. 이때 컴퓨터적으로 생성된 요소 영상을 $E(x,y)$ 로 나타낸다.

그리고 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.

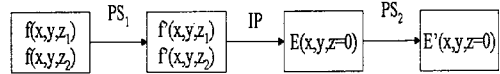


그림 2. 광 암호화 과정

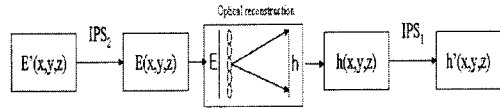


그림 3. 광 복호화 과정

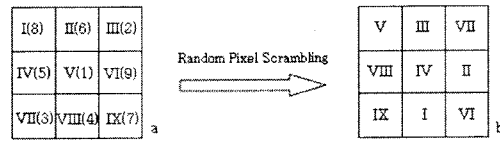


그림 4. 정 방향 랜덤 픽셀 스크램블링 방법

3.2 복호화 과정

한편 제안하는 광 암호화 방법의 복호화 과정은 그림 3에서 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 5는 3×3 사이즈의 블록에 대한 역 방향 랜덤 픽셀 스크램블링 과정의 예를 보여준다.

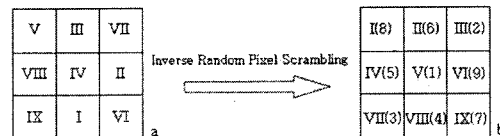


그림 5. 역 방향 랜덤 픽셀 스크램블링 방법

다음으로 복호화된 요소 영상 $f(x,y)$ 를 그림 1(b)의 집적 영상의 광학적 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 이 z 값 또한 암호화의 중요한 키로써 사용되어질 수 있다. 다음으로 이 광학적 디스플레이 시스템을 통하여 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

본 논문에서 제안하는 광 암호화 방법의 유용함을 보이기 위해서 컴퓨터 모의실험을 수행하였다. 실험에 사용하는 영상은 그림 6(a)에 보인 256×256 픽셀을 가지는 2진 영상이다. 첫 번째 랜덤 픽셀 스크램블 과정에서는 8×8 블록 단위로 픽셀 스크램블을 하였고 두 번째 랜덤 픽셀 스크램블 과정에서는 256×256 사이즈로 픽업된 요소 영상에 대하여 픽셀 스크램블을 수행하였다. 그리고 요소 영상의 픽업 과정에서는 렌즈 배열을 16×16개로 가정하였고, 실험 영상과 핀홀 배열 간의 간격은 12 mm로 하였으며, 핀홀 배열은 $z=0$ mm 의 위치시켰다. 그리고 요소 영상과 핀홀의 배열 간격은 3 mm로 하였고 핀홀 간의 간격은 1.08mm로 가정하여 컴퓨터 픽업을 수행하였다.

그림 6(a)의 실험 영상에 대해서 암호화 과정별로 나타난 영상을 그림 6(b)-(d)에 각각 나타내었다. 그림 6(b)는 1차 랜덤 픽셀 스크램블링 영상, 그림 6(c)는 컴퓨터 픽업 과정으로 얻어진 요소 영상, 그림 6(d)는 2차 랜덤 픽셀 스크램블링 후 최종 암호화된 영상을 나타내고 있다. 그림 6(d)에서 볼 수 있듯이 제안한 방법의 암호화 영상을 원 영상과 비교하면 암호화된 영상은 노이즈 패턴과 같이 보이면서 픽셀간의 상관성이 없음을 알 수 있다.

그림 7은 그림 6(d)의 암호화된 영상에 대해서 그림 3의 복호화 과정과 정확한 암호키를 이용하여 복호화한 후의 결과를 보여준다. 이때 집적 영상의 광학적 디스플레이 과정을 컴퓨터 적으로 모델링하였다. 그림 7(b)의 결과에서 정확한 암호키를 사용하였지만, 컴퓨터 복원과정에서 다수의 오류가 발생함을 확인하였으며, 이는 컴퓨터 복원 과정에 의해서 나타나는 오류로써 집적 영상의 복원 과정의 알고리즘을 향상한다면 원 영상을 얻을 수 있다.

한편 본 논문에서 제안하는 광 암호화 방법의 강인성과 유용성을 검증하기 위하여 그림 6(d)의 암호화된 영상에 가우시안 노이즈 첨가와 크로핑을 진행하여 정확한 키로 복원하는 실험을 추가적으로 수행하였다. 그림 8은 암호화된 영상에 50%의 크로핑 한 후 복원한 영상을 나타내고 그림 9는 암호화된 영상에 Mean=0, Variance=0.5인 가

우시안 노이즈를 첨가한 후 복원한 영상을 나타낸다. 그림 8과 그림 9에서 볼 수 있듯이 본 논문에서 제안한 방법은 가우시안 노이즈 첨가 공격에도 원 영상을 복원할 수 있을 뿐만 아니라 암호화된 영상의 50%가 크로핑 되었을 경우에도 원 영상을 복원 할 수 있어 제안 방법의 강인성과 유용성을 검증할 수 있다.

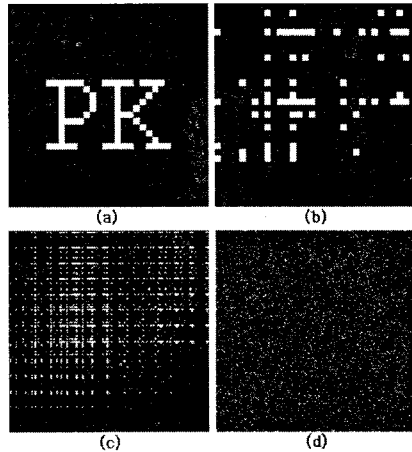


그림 6. 암호화 과정 (a) 입력영상 (b) 랜덤 픽셀 스크램블링 (c) 요소 영상 (d) 랜덤 픽셀 스크램블링 후 암호화된 영상

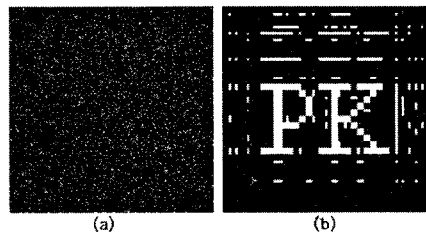


그림 7. 복호화 과정 (a) 암호화된 영상 (b) 정확한 암호화키(key)로 복호화된 영상

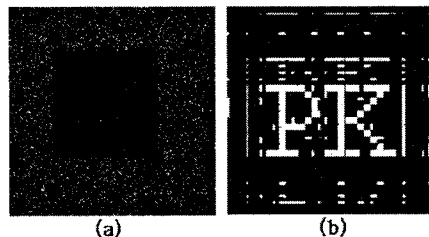


그림 8. 크로핑 공격 후 복호화 과정 (a) 50% 크로핑 공격 후 암호화된 영상 (b) 정확한 암호화키(key)로 복호화된 영상

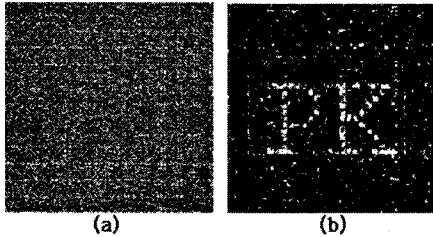


그림 9. 가우시안 노이즈 첨가 후 복호화 과정 (a) 가우시안 노이즈 첨가된 암호화영상 (b) 정확한 암호화키(key)로 복호화 된 영상

V. 결론

본 논문에서는 최근 3D 영상 기술에서 새로운 방식으로 알려진 집적 영상 기술에서 요소 영상을 획득하는 방법과 랜덤 픽셀 스크램블링 기술을 이용한 광 영상 암호화 방법을 제안하였다. 제안 방법은 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 생성하였다. 마지막으로 요소 영상의 안정성 향상을 위하여 랜덤 픽셀 스크램블링을 재 수행하여 최종 광 암호화된 영상을 얻었다. 암호화 된 영상에 노이즈첨가와 크로핑 공격을 첨가한 후 광학적 집적 영상 복원 기법과 역픽셀 스크램블링 방법으로 복호 화한 실험결과와 분석을 통하여 제안한 방법의 유용성과 공격에 대한 강인성을 증명하였다.

Acknowledgements

본 연구는 지식경제부 및 정보통신 연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(IITA-2008-C1090-0801-0018).

참고문헌

- [1] 박영일, 김석태, "선형계수확장 기반의 새로운 웨이블릿 워터마킹", 한국통신학회 논문지, Vol. 32, pp. 16-22, 2006.
- [2] 박영일, 김석태, "웨이블릿 기반의 자기참조 기법을 이용한 블라인드 워터마킹", 한국통신학회 논문지, Vol. 33, No. 1, pp. 62-67, 2008.
- [3] Xiaojun Tong and Minggen Cui, "Image encryption with compound chaotic sequence cipher shifting dynamically", Image and Vision Computing, Vol. 26, pp. 843-850, 2008.
- [4] Di Xiao, Xiaofeng Liao and Pengcheng Wei, "Analysis and improvement of a chaos-based image encryption algorithm", Chaos, Solitons & Fractals, 2007.
- [5] Wang RK and Chatwin C., "Random phase encoding for optical security", Optics Engineering, Vol. 35, pp. 2464-2469, 1996.
- [6] Situ G and Zhang J, "Image hiding with computer-generated phase codes for optical authentication", Optics Communication, Vol. 245, pp.55-65, 2005.
- [7] Hennelly B and Sheridan JT, "Optical image encryption by random shifting in fractional Fourier domains", Optics Letter, Vol. 28, pp. 269-271, 2003.
- [8] Zhao J, Lu H, Song X, Li J and Ma Y, "Optical image encryption based on multistage fractional Fourier transforms and pixel scrambling technique", Optics Communication, Vol. 249, pp.493-499, 2005.
- [9] Narendra Singh and Aloka Sinha, "Optical image encryption using fractional Fourier transform and chaos", Optics and Lasers in Engineering, Vol. 46, pp. 117-123, 2008.
- [10] J. -S. Jang and B. Javidi, "Improved viewing resolution of 3D integral imaging with nonstationary micro-optics", Optics Letter, Vol. 27, pp. 324-326, 2002.
- [11] R. Martinez-Cuenca, A. Pons, G. Saavedra, M. Martinez-Corral and B. Javidi, "Optically-corrected elemental images for undistorted Integral image display", Optics Express 14, pp. 9657-9663, 2006.
- [12] 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.