부분 홀로그램의 이중 프레넬 변환을 이용한 암호화 알고리즘

*이윤혁 김동욱 서영호
광운대학교 전자재료공학과
*winner9100@kw.ac.kr

Encryption Algorithm using Dual Fresnel Transform of Partial Hologram

*Lee, Yoon-Hyuk Kim, Dong-Wook Seo, Young-Ho
Dept. of Electronic Materials Eng., Kwangwoon University

요약

홀로그램 콘텐츠의 정보보안을 위한 암호화 방법을 제안한다. 제안하는 암호화 기법은 실시간 처리를 위해 부분 홀로그램에 대하여 편향치를 더하고, 이중 프레넬 변환을 수행하여 에너지가 집중된 DC 영역을 획득한다. 이때 집중된 영역이 암호화 영역으로 적은 데이터를 이용하여 고효율의 암호화를 수행한다. 제안한 기법은 기존 연구보다 변환하는 크기를 줄이기 때문에 같은 효율로 고속의 암호화를 수행할 수 있다. 1,024×1,024 크기의 홀로그램을 32×32 부분홀로그램으로 구성하여 적용할 경우 약 18배 빠르게 처리할 수 있다.

1. 서론

디지털 홀로그램은 실제 공간상에 객체가 재현되는 영상 시스템으로 제작부터 서비스과정까지 많은 비용이 소모되는 고가의 콘텐츠이다. 따라서 홀로그램 콘텐츠는 서비스 분야에 따라 다르겠지만 정보보호수단이 필요하다. 기존의 영상 시스템의 정보보호 기술로는 저작권을 주장하기 위한 워터마킹 기법과 허용된 사용자에게만 공개하는 암호화 기법 등 다양한 기술들이 존재한다. 홀로그램 영상은 주파수 및 중복성 등 여러 특성이 기존의 영상 시스템과 상당한 차이가 있기 때문에 기존 영상 시스템에서 사용한 정보보호 기술을 홀로그램에 적용하기 어렵다. 따라서 홀로그램을 위한 정보보호 기술이 연구되어 왔다[1]. [1]에서 제안한 홀로그램 암호화 기법은 프레넬 변환에서 입력의 공간주파수에 따른 퍼짐 특성[2]을 이용하여 홀로그램 정보를 집중시키고, 이 데이터를 암호화를 수행하는 기법으로 매우 적은 양을 암호화하여도 전체 데이터를 암호화 할 수 있다. [1]의 방법은 홀로그램 전체 데이터에 대하여 이중 프레넬 변환을 수행하기 때문에 프레넬 변환을 처리하기 위한 시간이 많이 소모되기 때문에 적은 데이터를 암호화하여도 실시간 처리가 어려운 단점이 있다. 본 논문에서는 앞서 설명한 단점을 해결하기 위해 부분 홀로그램으로 나누고, 이중 프레넬 변환을 이용한 암호화 기법을 제안한다.

2. 제안하는 암호화 방법

그림 1은 제안하는 암호화/복호화 기법으로 먼저 홀로그램을 N개의 부분 홀로그램을 나누고, 각 홀로그램에 편향을 더한 뒤 이중 프레넬 변환을 수행하고, 집중된 영역을 추출하여 블록암호화[3] 알고리즘을 이용하여 암호화/복호화를 수행한 뒤 역과정을 통하여 홀로그램을

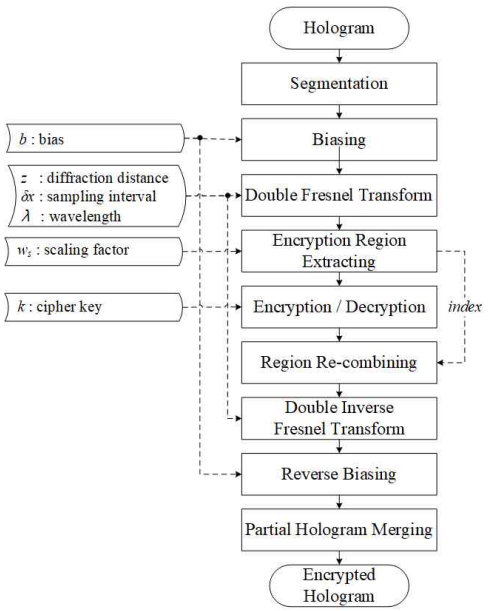


그림 1. 홀로그램 암호화/복호화 알고리즘.
Figure 1. Hologram encryption/decryption algorithm.

획득한다. 그림 2는 부분 홀로그램 하나를 암호화 하는 과정을 나타내었는데 부분 홀로그램에 특정 편향을 더하고 프레넬 변환을 수행결과 가운데에 높은 에너지를 갖고, 공간주파수가 낮은 DC영역이 생기게 된다. 공간주파수가 낮은 데이터를 프레넬 변환을 수행할 경우 퍼짐정도가 낮은 특성[2]으로 인하여 변환 결과 영상에서는 집중되는데 1차 프레넬 변환에서 생긴 DC영역은 2차 프레넬 변환을 통하여 매우 집중된다. 집중된 영역이 암호화 영역으로 전체 영상에 비하여 매우 작다.

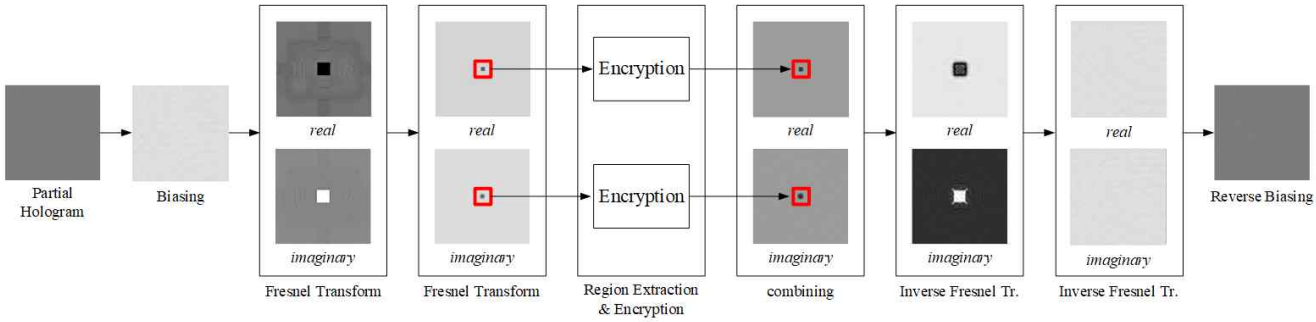
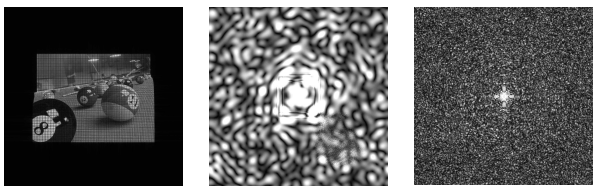


그림 2. 부분 홀로그램 암호화 과정의 예

Figure 2. Example of partial hologram encryption procedure

3. 실험결과

제안한 암호화 기법은 C/C++과 CUDA 라이브러리를 이용하여 구현하였고, 구현 환경은 Intel I-7 3770 CPU와 16GB의 메모리를 가지는 호스트 시스템과 서브시스템으로 GTX 680 그래픽 처리장치(Graphic Processing Unit, GPU)를 이용하였다. 그림 3은 기존 연구[1]와 제안한 방법으로 암호화를 수행한 홀로그램을 재생한 결과이다. 그림 3(a)은 원본 홀로그램의 복원 결과이고 그림 3(b)와 (c)는 각각 기존연구[1]와 제안한 방법으로 암호화를 수행한 뒤 복원한 결과이다. 암호화한 데이터의 비율은 각각 전체 홀로그램 데이터 대비 0.005%, 0.006%으로 매우 적은 데이터만 암호화를 수행한 결과로 NCC값은 둘 다 0.01이하로 두 방법의 성능은 유사하다.



(a) (b) (c)

그림 3. (a)원본의 복원결과; 암호화된 홀로그램의 복원 결과 (b)기존 연구, (c)제안한 방법

Figure 3. (a)Reconstruction results of original hologram; reconstruction result from (b) previous method, (c) propose method.

표 1은 이전 연구[1]와 제안한 방법을 이용하여 홀로그램의 암호화 수행시간을 나타냈다. 사용한 홀로그램은 1,024×1,024 크기의 홀로그램을 이용하였고, 이중 프레넬 변환에 사용한 파라미터는 모두 동일하게 하였다. 부분 홀로그램의 크기를 작게 할수록 암호화 수행시간은 감소하며 크기가 32×32일 경우 기존 방법에 비하여 약 18배정도 시간을 단축하는 것을 확인 할 수 있다.

표 1. 암호화 수행시간의 비교

Table 1. Encryption time comparison

Partial Hologram Size	Encryption Time[s]		
	Previous Method	Proposed Method	Ratio
1,024 × 1,024	1.488	1.492	0.99
512 × 512		0.812	1.83
256 × 256		0.448	3.32
128 × 128		0.256	5.81
64 × 64		0.144	10.35
32 × 32		0.081	18.44

4. 결론

본 논문에서는 제안하는 암호화 기법은 기존 연구[1]에서 사용한 이중 프레넬 변환을 이용한 기법을 부분 홀로그램에 적용하여 동일한 암호화 성능에도 불구하고 처리속도는 최대 18배까지 증가시킬 수 있다. 실험 결과 32×32 부분홀로그램에 적용 하였을 경우 약 12fps로 실시간 처리에는 못 미치지만 GPU의 성능을 높일 경우 실시간 처리가 가능 할 것으로 사료된다.

감사의 글

이 논문은 2018 년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2018R1D1A1B07043220)

참고문헌

[1] Y. H. Lee, Y. H. Seo, D. W. Kim, “Digital Hologram Encryption Algorithm using Fresnel Diffraction”, Journal of Broadcast Engineering, 20(6), 807-817.(2015)

[2] D. P. Kelly, “Numerical calculation of the Fresnel transform”, Journal of the Optical Society of America A 31(4), 755-764(2014)

[3] J. H. Kim, Y. H. Seo, D. W. Kim, “Area Efficient FPGA Implementation of Block Cipher Algorithm SEED”, Journal of KIISE, JOK, 7(4), 372-381(2008)