

이산 웨이블릿 패킷 변환을 이용한 디지털 홀로그램의 암호화

종신회원 서영호*, 정회원 최현준**, 종신회원 김동욱**

Digital Hologram Encryption using Discrete Wavelet Packet Transform

Young-Ho Seo* *Lifelong Member*, Hyun-Jun Choi** *Regular Member*,
Dong-Wook Kim** *Lifelong Member*

요약

본 논문에서는 이산 웨이블릿 패킷 변환을 이용하여 디지털 홀로그램의 중요 성분을 추적하고 암호화하는 새로운 방법을 제안한다. 공간과 주파수 영역에서 디지털 홀로그램의 특성을 분석하여 디지털 홀로그램을 다루는데 필요한 정보를 얻는다. 얻어진 정보들을 종합하여 웨이블릿 변환과 부대역의 패킷화를 이용한 암호화 방법을 제안한다. 웨이블릿 변환의 레벨과 에너지 값을 선택함으로써 다양한 강도로 암호화가 가능하다. 암호화 효과를 수치 및 시각적으로 분석하여 최적의 파라미터를 제시한다. 따라서 별도의 분석과정 없이 본 논문에서 제시된 파라미터를 이용하여 효율적으로 암호화를 수행할 수 있다. 실험결과를 살펴보면 전체 데이터 중에서 단지 0.032%의 데이터만을 암호화하더라도 객체를 분간할 수 없다. 부대역의 패킷화 정보와 암호화 시 이용한 키를 전체 암호키로 이용할 수 있다.

Key Words : Digital hologram, Fringe pattern, Encryption, 3 dimensional image, DWPT

ABSTRACT

In this paper, we propose a new method which estimates and encrypts significant component of digital hologram using discrete wavelet packet transform (DWPT). After analyzing the characteristics of digital hologram in spatial and frequency domain, the required information for ciphering digital hologram was extracted. Based on this information an ciphering method was proposed with wavelet transform and packetization of subbands. The proposed algorithm can encrypt digital hologram in various robust from selecting transform-level and energy threshold. From analyzing the encryption effect numerically and visually, the optimized parameter for encryption is presented. Without additional analyzing process, one can encrypt efficiently digital hologram using the proposed parameter. Although only 0.032% among total data is encrypted, the reconstructed object dose not identified. The paketization information of subbands and the cipher key can be used for the entire secret key.

I. 서론

최근 영상과 비디오 콘텐츠에 대한 사용이 급속히

증가하면서 데이터의 안전한 전송을 위해 여러 암호화 알고리즘들이 개발되었고, 몇몇 알고리즘들은 국제 및 국내 표준으로 선정되어 널리 사용되고 있다.

※ 본 연구는 한국과학재단 특정기초연구(R01-2006-000-10199-0)지원으로 수행되었음.

* 광운대학교 교양학부 IT전공(yhseo@kw.ac.kr), **광운대학교 전자재료공학과 ({hjchoi, dwkim}@kw.ac.kr)

논문번호 : KICS2008-01-008, 접수일자 : 2008년 1월 4일, 최종논문접수일자 : 2008년 9월 30일

특히, 영상과 비디오 같은 멀티미디어 매체는 데이터 양이 방대해서 전체 데이터를 암호화 하는데 많은 비용과 시간이 소요된다. 이러한 이유로 인해서 암호화 하는 양을 줄이는 연구들이 진행되어 왔다.

디지털 홀로그램은 두 가지 방법으로 생성이 가능하다. 첫 번째는 홀로그래픽 아날로그 필름에 기록했던 간섭패턴(혹은 프린지 패턴)을 CCD(charge coupled device) 카메라를 이용하여 디지털 데이터로 기록하는 방법이다. 두 번째는 컴퓨터 생성 홀로그램(computer generated hologram, CGH) 기법^[1]이다. 생성한 디지털 홀로그램은 수신단의 공간 광변조기(spatial light modulator, SLM)에 디스플레이한 후 레이저광을 조사함으로써 공간상에서 3차원 영상을 재생한다^[2]. 광학 장비들은 고가이고 영상의 획득이나 디스플레이를 위한 취급에도 상당한 노력이 필요하며, CGH 역시 복잡한 연산을 통해서만 홀로그램을 얻을 수 있다. 따라서 이런 고급 콘텐츠인 홀로그램의 저작권을 보호할 필요성이 크게 대두되고 있다^[3,4].

광학적으로 암호화를 시도하는 대상은 크게 2차원 영상과 3차원 객체로 나누어진다. 광학을 이용하여 2차원 영상을 암호화하는 최근 연구에는 확장된 fractional Fourier transform (FRT)과 디지털 홀로그래피 기술을 이용하여 광학 영상을 암호화한 방법이 있다^[5]. 확장된 FRT는 두 번 사용되고, 두 FRT 사이에 랜덤 위상 마스크를 삽입한다. 또한 Lensless Fresnel transform hologram에 기초한 확장 다중화 기법을 이용하여 컬러 영상을 암호화하는 방법도 제안되었다^[6]. 가장 최근에는 이진 Fourier 변환 방식의 CGH와 화소 변환 기법을 이용하여 영상을 암호화하는 방법도 제안되었다. 암호화된 영상은 이진 영상이기 때문에 잡음과 왜곡에 강인하다^[7]. 또한 암호화를 이용하여 3차원 객체를 보호하고자 하는 연구도 활발히 이루어져 왔다. 반사파 혹은 참조파의 경로에 위상 마스크를 삽입하여 3차원 객체를 위상 변이 디지털 홀로그램으로 암호화하는 연구가 수행되었다^[8]. 또한 컴퓨터로 생성된 랜덤한 위상기를 이용하여 3차원 객체의 프레넬 회절을 임의의 평면으로 전파시킴으로써 암호화하는 연구도 제안되었다^[9]. 광학 신호처리 분야의 선두 연구그룹으로 평가받고 있는 미국의 Javid 교수팀은 위상 이동 디지털 홀로그래피 방식을 이용하여 CCD 카메라로 획득한 프린지 패턴을 랜덤 위상 마스크로 암호화 하는 방식을 제안하고 암호화된 데이터를 프레넬 영역에서 무손실 부호화 기법을

이용하여 압축하였다. 이 방법은 백색잡음으로 암호화를 수행하기 때문에 암호화 효율은 높아지지만 암호화기로 복소 공역의 위상 함수를 사용하므로 정밀한 마스크 키가 필요하다는 특징을 갖는다^[10]. 이산 여현 변환(discrete cosine transform, DCT)을 이용하여 주파수로 변환한 후에 DC 값을 암호화한 방식과 Mallat-tree 방식의 이산 웨이블릿 변환(discrete wavelet transform, DWT)을 이용한 후에 일부 부대역을 암호화한 연구도 수행되었다^[11].

이처럼 최근 연구되는 대부분의 광학 보안관련 연구는 광학적인 특성들을 이용한 보안 인증 시스템분야로 편중되어 있다. 본 논문에서는 고가의 광학장비나 복잡한 연산을 통해서만 얻을 수 있는 디지털 홀로그램 콘텐츠의 보안을 위한 효율적이고 강력한 암호화 기법을 제안한다. 디지털 홀로그램을 공간 영역과 주파수 영역에서 특성을 분석하고, 이를 기반으로 효율적인 암호화 기법을 제안한다.

본 논문의 구성은 다음과 같다. II장에서는 암호화 방식을 결정하고 정당성을 보여주기 위해 디지털 홀로그램을 공간영역과 주파수 영역에서 분석한다. III장에서는 II장의 분석결과를 기반으로 암호화 기법을 제안한다. IV장에서는 제안한 암호화 기법을 디지털 홀로그램에 적용하고 다양한 각도로 분석한다. 마지막으로 V장에서 결론을 맺는다.

II. 홀로그램의 변환과 특성

2.1 이산 웨이블릿 변환과 리프팅 기법

DWT는 DCT와 같이 시간영역의 신호를 주파수 영역의 계수로 변환한다. 그러나 푸리에 변환을 기반으로 하는 도구들과 달리 주파수 영역에서 신호가 갖는 주파수 성분뿐만 아니라 위치에 따른 주파수 성분의 정보까지 얻을 수 있다. 또한 영상을 블록으로 분할하지 않고 원 영상을 그대로 처리함으로써 블록효과를 제거할 수 있다. DWT를 기반으로 영상을 압축할 경우에 다양한 압축률을 얻기 쉬우며, 전체영상에 대해 주파수 대역별로 분리하므로 비트스트림이 잡음에 강인하다. 부대역의 구조를 활용하면 일부분 전송된 정보로 전체영상을 복원할 수 있는 장점을 갖는다. 현재 디지털 시네마를 위한 압축도구인 JPEG2000의 기본 주파수 변환도구로 사용되고 있다^[12].

DWT를 연산하는 방법은 크게 컨벌루션 필터링 방법과 리프팅 방법이 있다. 리프팅은 컨벌루션 필터링을 변형 및 개선하여 연산의 속도와 메모리의

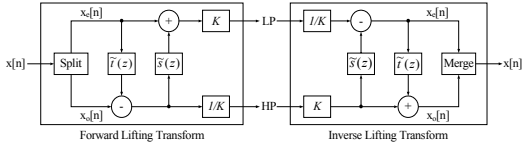


그림 1. 팩토링을 이용한 정방향역방향 리프팅
Fig. 1. Forward/inverse lifting using factoring

사용효율을 높인 방법이다. 본 논문에서는 리프팅을 이용하여 DWT를 수행하고자 한다¹³⁾. 리프팅 방식의 기본적인 원리는 웨이블릿 필터의 다상 행렬을 삼각 행렬과 대각 행렬로 인수분해하는 것이다. 그림 1에 일반적인 리프팅 과정을 나타내고 있는데, 리프팅을 이용한 웨이블릿 변환은 분할, 결합, 예측, 갱신, 및 조정의 네 단계로 구성된다¹⁴⁾.

2 dimensional(2D) DWT는 열과 행방향으로 1D DWT를 각각 독립적으로 연산하여 수행된다. 2차원 데이터, 즉 영상에 대해 2D DWT를 수행하면 각기 다른 주파수 특성을 갖는 4개의 영역이 생성된다. 이 영역을 부대역이라고 하고 일반적으로 주파수 특성에 따라서 LL, LH, HL, 및 HH 영역으로 표시한다. 4개의 부대역은 열과 행방향으로 다운 샘플링 되었기 때문에 4개의 부대역을 합한 크기는 원영상의 크기와 동일하다. 1-레벨 DWT에 의해 생성된 부대역의 구조를 그림 2(a)에 표시하였다.

처음으로 생성된 4개의 부대역 중에서 가장 저주파 부대역인 LL 부대역에 대해 2D DWT를 적용한다. 이러한 방식으로 주파수를 분할하는 방식을 Mallat-tree 방식이라고 한다. Mallat-tree 방식으로 L-레벨만큼 2D DWT를 수행하면 (3L+1)개의 부대역이 생성된다¹²⁾. 4개의 부대역 중에서 필요에 따라 임의의 부대역을 선택하여 DWT를 수행하는 방식을 이산 웨이블릿 패킷 변환(discrete wavelet packet transform, DWPT)이라 한다¹⁵⁾. 패킷화된 DWT 부대역의 구조를 그림 2(b)에 표시하였다.

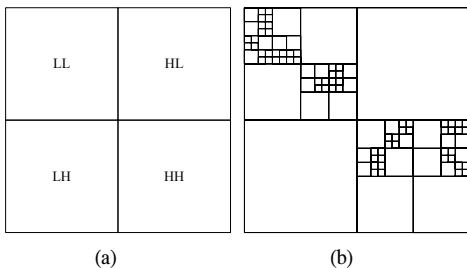


그림 2. DWT에 의한 부대역의 생성 (a) 1 레벨 (b) 5 레벨의 예
Fig. 2. Subband structure example by DWT (a) 1 level (b) 5 level

2.2 홀로그래프의 특성

본 절에서는 다양한 영상처리 기법을 이용하여 디지털 홀로그래프를 분석하고 특성을 파악한다. 분석된 디지털 홀로그래프의 특성으로부터 디지털홀로그래프를 암호화하기 위한 기본 아이디어를 얻는다.

2.2.1 표본화

일반적인 영상의 경우에 sample 혹은 pixel 단위로 subsampling 과정을 거치고 다시 원래의 영상과 동일한 공간적인 해상도를 취할 경우에 원영상에서 고주파가 제거된 형태의 blurring 영상이 생성된다. 하지만 그림 3(b)와 같이 디지털 홀로그래프 자체에 대해 subsampling 과정을 수행하게 되면 원영상 혹은 원객체의 정보가 거의 소실한다. 이런 결과로부터 디지털 홀로그래프를 구성하는 인접성분들 간의 상관도는 거의 없고 각각이 독립적인 정보를 표현한다는 것을 알 수 있다. 또한 디지털 홀로그래프에 대해 subsampling을 블록 단위로 수행한 결과를 그림 3(c) 및 (d)에 나타냈는데, 각각 128×128 및 64×64 블록 단위로 subsampling을 수행한 후 복원한 결과이다. 블록 단위가 클수록 원객체와 더 가까운 형태를 가진다. 이러한 결과는 홀로그래프내의 특정 국부영역은 전체 객체에 대한 정보를 모두 가지고, 선택된 영역의 크기가 커질수록 복원결과가 우수하다는 것을 보여준다. 그림 3의 (b)는 (c) 및 (d)와 동일한 데이터 량을 subsampling하였지만 복원 결과는 전혀 다르다는 것으로 확인할 수 있다.

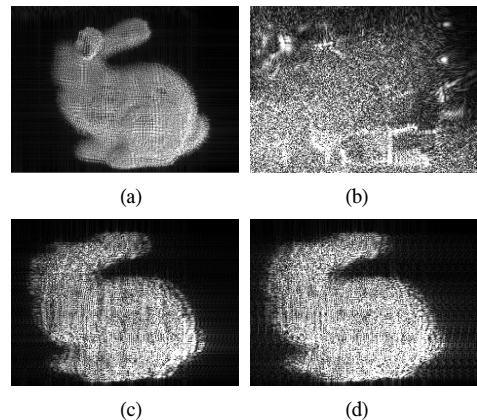


그림 3. 디지털 홀로그래프의 subsampling 후 복원 결과 (a) 원 객체, (b) 1-pixel 단위, (c) 128×128 블록 단위, (d) 64×64 블록 단위의 subsampling
Fig. 3. Image example after subsampling digital hologram (a) original 3D object, reconstructed object after sub-sampling by a unit of (b) one pixel, (c) 64×64 block, (d) 128×128 block

2.2.2 국부화 (localization)

디지털 홀로그래프의 국부영역의 특성은 일정 크기로 디지털 홀로그래프를 분할한 뒤 복원한 결과를 관찰하여 확인할 수 있다. 그림 4(a)와 같이 중심을 기준으로 분할한 후 그림 4(b)와 같이 스케일링된 결과를 얻는다. 이러한 결과는 2차원 영상과는 전혀 다른 광학적인 특성이다. 또한 디지털 홀로그래프의 국부영역에서는 그 영역에서 바라본 전체 객체의 정보가 모두 포함된다. 그림 5에 이러한 특성을 나타냈다. 전체 홀로그래프를 분할한 후 각 세그먼트를 복원하면 다른 각도에서 바라본 3차원 객체가 나타난다.

국부적 영역의 독립적 특성은 다시점 영상과 유사하게 처리될 수 있는 가능성을 준다. 즉, 디지털 홀로그래프는 분할된 후 분할된 영역은 개별적으로 다루어 질 수 있고, 각 영역들이 그림 5와 같이 유사한 정보를 포함하고 있다면 정보들 간의 상관성 혹은 중복성을 이용하여 처리될 수 있다¹⁶⁾.

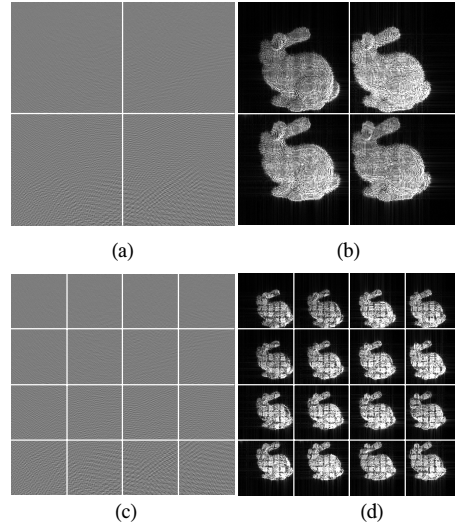


그림 5. 전체 홀로그래프의 국부적 복원 결과 (a) 512×512 크기 (b) 256×256 크기
Fig. 5. Reconstructed objects in local regions, (a) 512×512 size, (b) 256×256 size

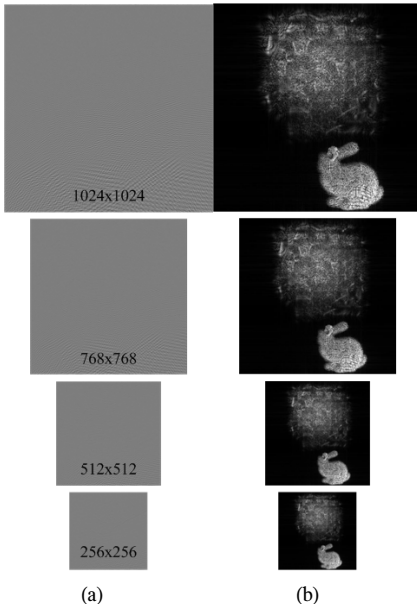


그림 4. Fringe 패턴의 분할을 통한 디지털 홀로그래프의 스케일링 (a) 중심을 기준으로 분할된 fringe 패턴 (b) 분할된 fringe 패턴을 이용한 역 CGH 결과
Fig. 4. Scaling examples using cropping digital hologram (a) cropped holograms, (b) reconstructed objects

2.2.3 주파수

그림 1, 4, 및 5에서 볼 수 있듯이 디지털 홀로그래프는 시각적으로 잡음과 유사한 형태이고, 주파수 특성도 2차원 영상과 다르다. 그림 6에 DWPT를 이용하여 주파수 영역으로 변환한 후에 계수들의

LLLL	LLHL	HLLL	HLHL	LLLL	LLHL	HLLL	HLHL
50.998%	0.084%	0.001%	0.019%	89.788%	0.825%	0.062%	0.863%
2.837%	3.239%	0.019%	1.324%	0.498%	1.380%	0.126%	1.595%
LHLL	LHHL	HHLL	HHHL	LHLL	LHHL	HHLL	HHHL
0.983%	2.294%	0.011%	1.241%	0.031%	0.072%	0.015%	0.132%
LHLH	LHHH	HHLH	HHHH	LHLH	LHHH	HHLH	HHHH
9.505%	17.581%	0.089%	9.777%	0.494%	1.495%	0.206%	2.419%

그림 6. 주파수 영역에서 계수의 평균 에너지 (a) 디지털 홀로그래프 (b) 자연 영상
Fig. 6. Average coefficient energy in frequency domains (a) digital hologram (b) natural image

평균 에너지를 나타냈다. 그림 6(a)의 디지털 홀로그래프를 그림 6(b)의 2차원 자연 영상과 비교할 때 최저주파수 계수 및 영역에서 가장 큰 에너지를 보이는 것은 유사하지만 고주파 성분의 에너지가 증가하는 경향성은 전혀 다르다.

2.2.4 디지털 홀로그래프 이산 웨이블릿 변환

앞 절들에서 보인 결과들을 살펴보면 다음과 같은 두 가지 큰 특징을 확인할 수 있다. 첫 번째는 디지털 홀로그래프는 국부 영역이 전체 객체에 대한 정보를 갖고 있다는 것이다. 두 번째는 일반적인 영상과 다른 주파수 특성을 갖는다는 것이다. 이러한 특징으로부터 다음과 같이 결론을 내릴 수 있다.

디지털 홀로그래프는 국부 영역이 전체 객체의 정보를 모두 포함하고 있기 때문에 영역을 나누어서 압축하는 것보다는 전체 홀로그래프를 대상으로 압

호화를 수행하는 것이 적합하다. 즉, 2차원 데이터를 쪼개서 변환하는 DCT보다 전체 2차원 정보를 처리하는 DWT가 더욱 적합하다. 물론 전체 2차원 데이터에 대해 DCT를 적용할 수 있지만 전역 DCT는 주파수 분할 특성과 에너지 집중도가 좋지 않다. 또한 전역 DCT는 연산량이 너무 방대하여 실제로 사용하기는 어렵다. 따라서 DWT가 가장 적합한 것으로 판단할 수 있다. 디지털 홀로그래ムの 주파수 특성은 일반 영상의 주파수 특성과 매우 다르기 때문에 일반 영상에 적용하는 것과 다른 방식으로 DWT를 적용해야 한다. 즉, DWT를 적용하는데 있어서 디지털 홀로그래ム에 특화된 부대역 구조가 필요하다.

III. 디지털 홀로그래ムの 암호화 기법

본 장에서는 디지털 홀로그래ム을 위한 암호화 및 복호화 기법을 제안한다. 먼저 전체적인 과정을 소개하고, 다음으로 암호화 및 복호화 알고리즘을 설명한다. 그리고 암호화 과정을 위한 부대역 선택 알고리즘을 소개한다.

3.1 개요

홀로그래ム을 암호화하기 위한 기존의 알고리즘들은 홀로그래ム에 적응적이지 않다는 단점을 갖는다. 적응성이 없을 경우에는 알고리즘을 적용하는데 속도는 빠르지만 최적화는 되지 않는다. 속도와 최적화는 서로 상보적인 관계로 볼 수 있다. 디지털 홀로그래ムの 어느 주파수 성분을 암호화 하였다면 역과정을 거친 후에 해당 주파수 성분을 공격할 여지가 있다. 이러한 취약성을 해결하기 위해서는 역과정을 추적하기 어려워야 하고 주파수 성분을 예측하기 어려워야 한다. 제안하고자 하는 알고리즘은 이러한 문제들을 적절히 해결하고 효율적으로 암호화를 시도하고자 한다.

디지털 홀로그래ム은 자연 영상과 전혀 다른 주파수 특성을 갖기 때문에 mallot-tree 방식의 DWT가 적당하지 않다. 즉 부대역을 패킷화하여 디지털 홀로그래ム에 특화된 부대역 구조로부터 추출된 주파수 성분을 암호화해야 한다. 이러한 부대역 구조는 암호화된 주파수를 예측하기 어렵게 하고 역과정을 이용한 공격이 어렵다. 디지털 홀로그래ム에 따라서 각각의 부대역에 대해 적응적으로 DWT를 수행하고 그 기준은 에너지의 중요도에 의존한다. 시각적인 인지도는 정보가 갖는 에너지의 량에 비례하기

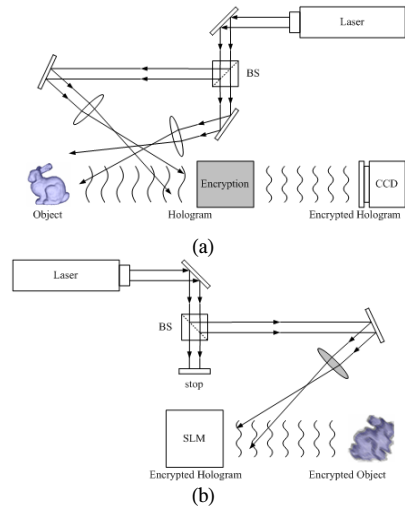


그림 7. 디지털 홀로그래ム 암호화의 개념도
Fig. 7. Graphical concept of digital hologram encryption

때문에 가능하면 에너지가 높은 주파수 대역을 은닉하여 암호화 효율을 높여야 한다.

제안하고자 하는 암호화 과정을 그림 7에 쉽게 나타내었다. 반사파와 참조파의 위상차에 암호화 알고리즘을 적용하여 암호화된 회절 패턴, 즉 디지털 홀로그래ム을 획득하고 저장한다. 이 과정을 그림 7(a)에 나타냈다. 디지털 홀로그래ム은 암호화된 상태로 저장 및 전송된다. 만일 복호화 과정을 거치지 않고 재생하고자 한다면 그림 7(b)와 같이 왜곡된 객체를 관찰하게 된다.

3.2 제안한 암호화 알고리즘

본제안한 암호화 알고리즘을 그림 1에 흐름도를 이용하여 나타내었다. 디지털 홀로그래ム을 4개의 부대역으로 변환하고, 4개의 부대역에 대해 각각 다시 DWT를 수행한다. 부대역 들의 에너지 분포를 탐색하고, 다시 DWT를 수행할 부대역을 선정한다. 이러한 과정을 Selection Map과 Priority Map에 기록하여 탐색과정을 저장한다. Selection Map은 선택된 부대역에 대한 정보를 보유하고, Priority Map은 동일한 레벨에서 선택된 부대역들 중 어느 부대역이 암호화 우선순위가 높은지를 보유하고 있다. 이러한 과정은 선택된 부대역들의 총 에너지값이 임계치(E_{TH})보다 클 때까지 계속 진행된다. DWT 레벨의 임계치(L_{TH})가 높아질수록 각 부대역의 크기와 에너지가 작아지기 때문에 에너지 임계치를 만족시키기 위해 선택되는 부대역의 개수는 증가하고 정밀하게 에너지 합계를 조절할 수 있다. 최종적으로 선택된

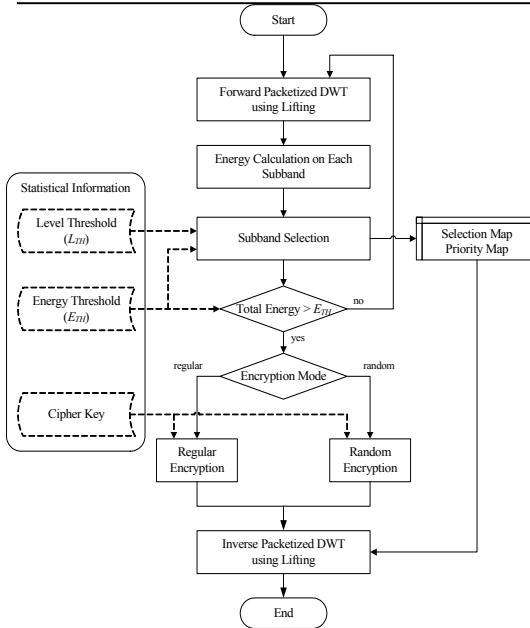


그림 8. 홀로그램 암호화 절차
Fig. 8. Hologram encryption procedure

부대역들은 블록 암호화 알고리즘을 이용하여 암호화한 후에 역 PDWT를 수행하여 암호화된 디지털 홀로그램을 생성한다.

암호화 과정에서 생성된 Selection Map, Priority Map, 그리고 블록 암호화 알고리즘의 cipher key를 합쳐서 전체 secret key가 된다. 이 secret key는 허가받은 사용자에게만 전달된다.

제안한 알고리즘으로부터 아래와 같이 디지털 홀로그램의 암호화를 위한 다양한 정보화 솔루션을 제시할 수 있다.

- 암호화 효과의 판단을 위한 임계치 검출
- 영상을 구성하는 주파수들 중에서 시각적으로 큰 영향을 미치는 성분의 검출
- 영상을 구성하는 주파수들 중에서 에너지가 큰 성분의 검출
- 디지털 홀로그램의 암호화를 위한 최적화된 부대역의 구조와 주파수 성분의 제시
- 디지털 홀로그램의 암호화를 위한 솔루션 제시

그림 9에는 디지털 홀로그램을 복호화하는 절차를 나타내었다. 복호화 절차는 암호화 절차의 역과정이고 암호화 시 사용하였던 cipher key를 그대로 사용하고, 암호화 과정에서 추출했던 Selection Map과 Priority Map을 이용한다.

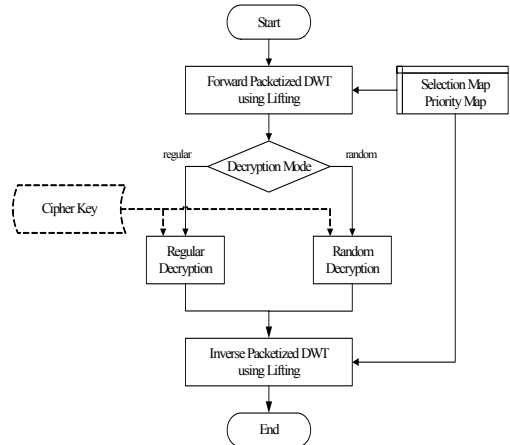


그림 9. 홀로그램 복호화 절차
Fig. 9. Hologram decryption procedure

3.3 부대역 선택

제안한 디지털 홀로그램의 암호화 알고리즘에서 부대역을 선택하는 방법은 그림 10의 순서로 수행한다. 에너지 집중도가 높은 부대역을 추적하는 경우에 동일한 에너지를 갖는 부대역이 존재한다면 (L, LH, HL, HH)의 순서로 우선 순위를 결정한다. L_{TH} 에 의해 증가한 부대역에 대한 정보를 업데이트한 후에 L_{TH} 에 따라서 생성되는 부대역들의 순서를 추적하여 Priority Map을 위한 Priority flag를 생성한다. 그리고 E_{TH} 에 따라 부대역을 선택하고, Selection Map을 위해 Selection flag를 생성한다.

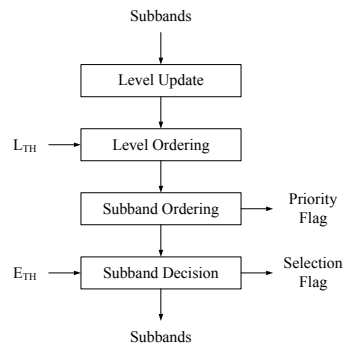


그림 10. 부대역 선택 절차
Fig. 10. Subband selection procedure

IV. 실험 및 결과

본 장에서는 제안한 암호화 기법을 이용하여 디지털 홀로그램을 암호화하고, 암호화 효과를 살펴본다. DWPT를 이용하여 디지털 홀로그램을 암호화할 경우에 최적의 부대역과 에너지 조합을 제시한다.

4.1 실험방법

제안한 암호화 기법을 몇 가지 디지털 홀로그램에 적용하고, 암호화 결과를 확인하였다. 먼저, 컴퓨터 생성 홀로그램(computer generated hologram, CGH) 방법을 이용하여 3차원 객체의 디지털 홀로그램을 생성한다. 다음으로 순방향 DWPT를 이용하여 생성된 디지털 홀로그램을 주파수 영역의 계수로 변환하고, 앞 절에서 설명한 방법으로 부대역을 선택한다. 선택된 부대역의 계수들을 블록 암호화 알고리즘을 이용하여 암호화한다. 역방향 PDWT를 거쳐서 암호화된 디지털 홀로그램이 생성된다. 최종적으로 역 CGH 과정을 거쳐서 암호화된 3차원 객체가 생성된다. 실험 절차를 그림 11에 나타내었다. 암호화된 결과는 peak noise-to-signal ratio (PSNR)과 normalized correlation (NC)를 이용하여 수치적으로 확인한다. 또한 수치적인 통계와 함께 시각적인 판단을 통해서 결과를 판단한다. PSNR과 NC는 식 (1)과 (2)에 정의하였다.

$$PSNR(dB) = 10 \log_{10} \frac{255^2}{\frac{1}{XY} \sum_{x,y} (I_{x,y} - I'_{x,y})^2} \quad (1)$$

$$NC = \frac{\sum_{i=1}^N I_i I'_{eff}}{\sum_{i=1}^N I_i^2} \quad (2)$$

본 실험에서는 DWPT 과정 이후에 생성된 부대역 계수를 모두 암호화하지 않고 계수의 최상위 비트만을 암호화한다. 최상위 비트만을 암호화해도 전체 비트를 암호화한 것과 효과가 거의 유사하였다.

그림 11의 암호화 방법을 이용하여 암호화를 수행한 예를 그림 12에 나타내었다. 그림 12의 예는 $L_{TH} = 5$ 이고 $E_{TH} = 20$ 의 경우이다. $E_{TH} = 20$ 이지만 실제로 암호화된 에너지의 양은 17.3%이고, PSNR은 10.15dB이다. 암호화된 부대역의 크기는 0.39%이고, 최상위 비트 평면만을 암호화했기 때문에 암호화된 양은 0.0488%이다. 그림 12(a)는 3차원 객체로부터 생성된 디지털 홀로그램이고, 그림 12(b)는 선택된 부대역을 표시한 것이다. 그림 12(c)는 암호화된 디지털 홀로그램이고, 그림 12(d)는 복원된 객체이다. 그림 3(a)와 그림 12(d)를 비교하면 암호화된 정도를 확인할 수 있다. 전체 데이터 중에서 0.0488%만을 암호화했음에도 불구하고 원래의 객체를 알아보기 어려울 만큼 암호화효과가 우수하다는 것을 확인할 수 있다.

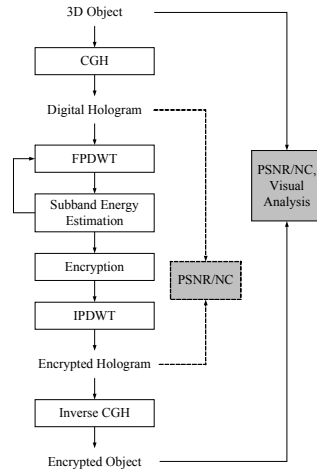


그림 11. 실험 절차
Fig. 11. Experiment procedure

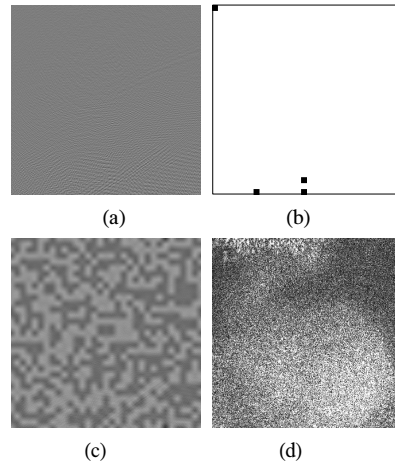


그림 12. 암호화 실험 과정 (5-레벨, 에너지 20%) (a) 디지털 홀로그램 (b) 선택된 부대역 (c) 암호화된 홀로그램 (d) 복원된 객체
Fig. 12. Encryption procedure (5-level, energy 20%) (a) digital hologram (b) selected subbands (c) encrypted hologram (d) reconstructed object

E_{TH} 와 L_{TH} 의 값을 조절하여 다양한 암호화 방법이 가능하다. 그림 13은 $L_{TH} = 4$ 인 경우에 E_{TH} 에 따라 선택된 부대역들을 나타낸다. 모든 경우에 대해서 최저 주파수 대역은 반드시 포함시킨다. 최저 주파수 대역은 에너지의 양에 상관없이 전체 디지털 홀로그램의 평균 주파수를 나타내므로 암호화 시 포함시킨다.

다음 절부터 암호화 결과들과 효과를 살펴보는는데, 그림 11에 나타낸 것과 같이 디지털 홀로그램과 3차원 객체에 대해서 각각의 NC, PSNR, 그리고 시각적인 분석을 시도한다.

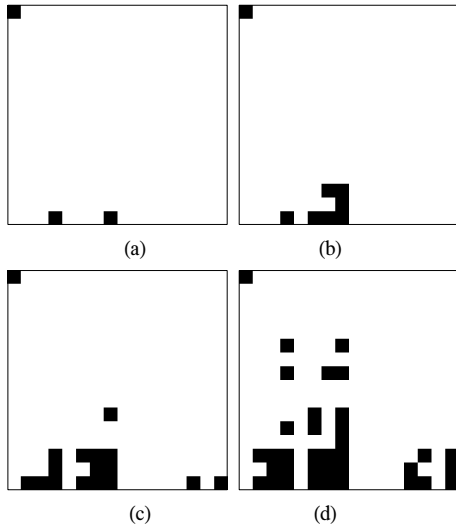


그림 13. E_{TH} 값에 의한 선택된 부대역 (a) 20 (b) 40 (c) 60 (d) 80
 Fig. 13. the selected subbands according to E_{TH} (a) 20 (b) 40 (c) 60 (d) 80

4.2 암호화 효과

4.2.1 디지털 홀로그램

먼저 디지털 홀로그램 자체의 암호화 효과를 살펴본다. CGH에 의해서 생성된 디지털 홀로그램과 암호화 이후의 홀로그램의 NC 및 PSNR을 측정하여 그림 14에 그래프로 정리하였다. 그림 14(a)는 NC에 대한 그래프이고 그림 14(b)는 PSNR에 대한 그래프이다. 레벨(L_{TH})과 에너지(E_{TH})를 변화시키면서 다양한 조건을 실험하였다. 결과를 살펴보면 NC와 PSNR 값이 L_{TH} 과 E_{TH} 에 대해 경향성을 갖지 않는다는 것을 확인할 수 있다. NC는 거의 0.72 이하의 값을 갖고, PSNR은 9dB 이하의 값을 갖기 때문에 이미 경향성을 갖는 범위를 벗어난 것으로 볼 수 있다.

4.2.2 3차원 객체

디지털 홀로그램과 마찬가지로 3차원 객체에 대해서도 암호화 효과를 살펴본다. 원래의 3차원 객체와 암호화된 3차원 객체 사이의 NC와 PSNR 결과를 그림 15에 나타냈다. 먼저 그림 15(a)의 NC 결과를 살펴보면 암호화에 포함된 E_{TH} 가 증가할수록 NC는 감소하는 것을 확인할 수 있다. 전체적으로 살펴보면, L_{TH} 이 증가할수록 NC가 더욱 작다. 즉, PDWT를 이용하여 주파수를 세분화할수록 암호화 효과는 좋다는 것을 알 수 있다. 그림 15(b)는 3차원 객체의 PSNR 결과이고, 경향성을 찾기 어렵다.

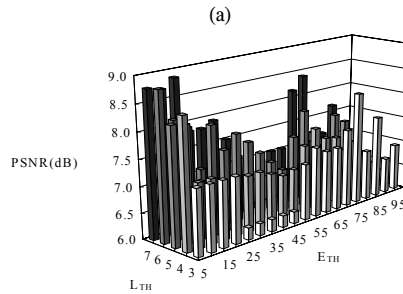
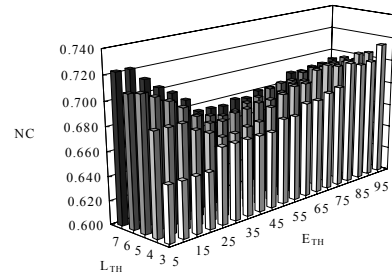


그림 14. 디지털 홀로그램의 암호화 결과 (a) PSNR (b) NC
 Fig. 14. Encryption result of digital hologram (a) PSNR (b) NC

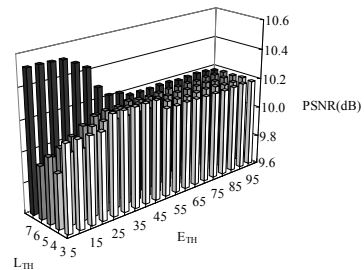
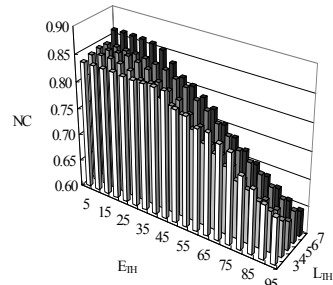


그림 15. 객체의 암호화 결과 (a) NC (b) PSNR
 Fig. 15. Encryption result of object (a) NC (b) PSNR

레벨 L_{TH} 과 에너지 E_{TH} 에 따른 암호화 영역의 비율을 그림 16에 보였다. 동일한 E_{TH} 라면 L_{TH} 가 클수록 암호화 영역은 작다. 즉, 작은 부대역만을 암호화할지라도 유사한 에너지를 만족시킬 수 있다는 의미이다. PDWT의 레벨이 증가하면 주파수를

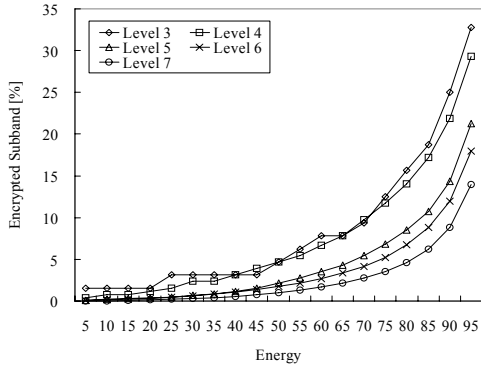


그림 16. 암호화 영역의 비율에 대한 그래프
Fig. 16. Graph for ratio of encrypted region

표 1. 레벨에 따른 MSB의 위치
Table 1. position of MSB for level

L_{TH}	MSB
2	9
3	10
4	11
5	12
6	12
7	13

더욱 세분화할 수 있고, 중요 주파수 영역을 찾는 것이 더욱 정밀해진다. L_{TH} 에 따른 최상위 비트 위치를 표 1에 나타냈다. 암호화된 데이터의 값은 그

림 16의 결과를 표 1로 나누어야 한다.

NC와 PSNR 결과들을 종합적으로 살펴보면 수치적인 결과들만 가지고는 암호화 효과를 정확하게 판단하기 어렵다는

결론을 낼 수 있다. 따라서 수치적인 결과들과 함께 시각적인 관찰을 통해서 암호화 효과를 판단하고자 한다.

4.3 시각적 판단

4.3.1 3차원 객체의 암호화 효과

그림 12와 같이 디지털 홀로그램을 시각적으로 관찰하는 것으로 암호화 효과를 판단하기는 어렵다. 시각적으로 암호화 효과를 판단하기 위해서는 디지털 홀로그램보다 역 CGH를 거쳐 복원된 3차원 객체를 확인해야 한다.

그림 17에 3차원 객체의 암호화 결과를 나타내었다. L_{TH} 는 6이고 E_{TH} 는 5에서 40까지 변화시켰다. 5에서 40까지의 E_{TH} 에 대한 결과를 보인 것은 이 영역에서 객체를 식별할 수 없게 되기 때문이다. 객체를 식별할 수 없는 지점의 E_{TH} 는 L_{TH} 에 따라서 달라진다.

그림 18에는 다양한 객체들에 대한 암호화 결과를 나타내었다. 그림 17과 마찬가지로 L_{TH} 는 6이다. 그림 18(j)는 광학적으로 캡처한 디지털 홀로그램을 암호화하고 복원한 결과이고, 나머지 그림들은 CGH를 통해서 생성된 디지털 홀로그램을 암호화하고 복원한 결과이다.

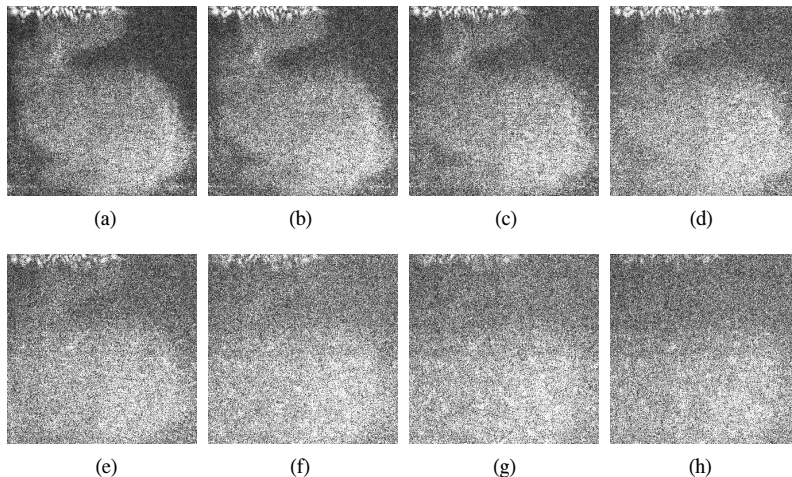


그림 17. 에너지량에 따른 복원된 객체의 암호화 효과 (a) 5 (b) 10 (c) 15 (d) 20 (e) 25 (f) 30 (g) 35 (h) 40
Fig. 17. Encryption effect of the reconstructed object according to energy (a) 5 (b) 10 (c) 15 (d) 20 (e) 25 (f) 30 (g) 35 (h) 40

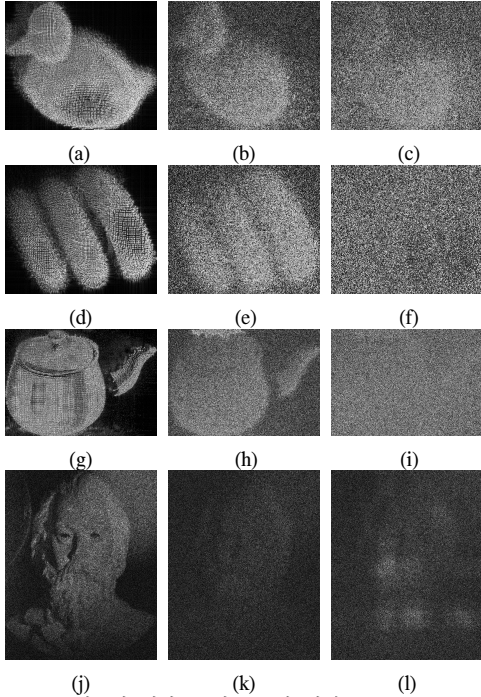


그림 18. 암호화 결과. 오리 (a) 원 객체 (b) $E_{TH} = 15$ (c) $E_{TH} = 30$, 스프링 (d) 원 객체 (e) $E_{TH} = 15$ (f) $E_{TH} = 30$, 주전자 (g) 원 객체 (h) $E_{TH} = 5$ (i) $E_{TH} = 10$, 브라함 (j) 원 객체 (k) $E_{TH} = 10$ (l) $E_{TH} = 30$

Fig. 18. Visual example of the encrypted and reconstructed objects. Duck (a) original object (b) $E_{TH} = 15$ (c) $E_{TH} = 30$, spring (d) original object (e) $E_{TH} = 15$ (f) $E_{TH} = 30$, teapot (g) original object (h) $E_{TH} = 5$ (i) $E_{TH} = 10$, Brahm (j) original object (k) $E_{TH} = 10$ (l) $E_{TH} = 30$

4.3.2 암호화 효율

암호화된 3차원 객체를 시각적으로 관찰하면서 L_{TH} 별로 3차원 객체를 분별할 수 없는 E_{TH} 를 선정하였다. 선택된 E_{TH} 에서 암호화 영역의 비율을 표 2에 정리하였다. 표 2의 값들은 그림 15의 실험 결과로부터 추출한 값이다. 표 2는 수치적인 암호화 결과와 시각적인 판단을 종합한 결과에 해당한다. 표 2를 살펴보면 L_{TH} 이 증가하면 객체를 분별할 수 없는 E_{TH} 는 증가하고, 암호화된 영역의 비율은 감소한다. 즉, 주파수를 세분화시키면 작은 영역만을 암호화한다 할지라도 더 많은 에너지가 암호화되어 암호화 효율은 높아진다. 표 2의 암호화 효율은 식 (3)으로 정의된다. 레벨 7의 결과를 살펴보면 전체 데이터의 0.032%만을 암호화하여도 객체가 완전히 은닉된다. 레벨 6의 경우는 0.053%를 암호화 하였을 때 객체가 분간할 수 없게 된다.

표 2. 암호화 효율의 분석 및 비교

Table 2. Analysis and comparison of encryption efficiency

Item	L_{TH}				
	3	4	5	6	7
E_{TH}	20	25	30	30	35
Ratio of Encrypted Region (%)	1.563	1.563	0.684	0.635	0.415
Ratio of Encrypted Data (%)	0.156	0.142	0.056	0.053	0.032
Efficiency	128	176	523	567	1096
Efficiency Ratio (%)	11.7	16.1	48.0	51.7	100.0

$$Efficiency = \frac{Ratio\ of\ Encrypted\ Data}{E_{TH}} \quad (3)$$

표 2에서 L_{TH} 가 7인 경우는 L_{TH} 가 6인 경우보다 암호화 효율이 거의 2배가 높다. L_{TH} 가 5와 6은 거의 유사하고 L_{TH} 가 5인 경우는 4인 경우보다 2.5배 정도 높다. 표 2에서 L_{TH} 에 대한 E_{TH} 의 값은 암호화를 위한 최적의 부대역 조합으로 해석할 수도 있다. 최적화된 부대역 조합을 그림 19에 나타냈다.

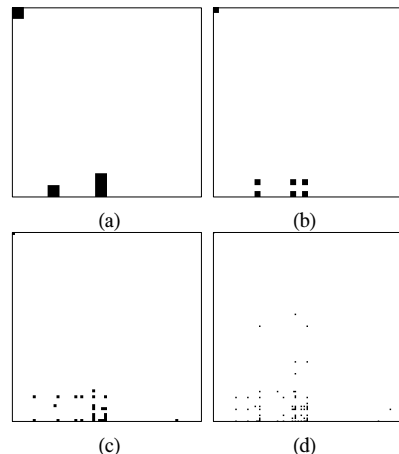


그림 19. 암호화를 위한 부대역 조합 (a) $L_{TH} = 4$, $E_{TH} = 25$ (b) $L_{TH} = 5$, $E_{TH} = 30$ (c) $L_{TH} = 6$, $E_{TH} = 30$ (d) $L_{TH} = 7$, $E_{TH} = 35$

Fig. 19. Subband combination for encryption (a) $L_{TH} = 4$, $E_{TH} = 25$ (b) $L_{TH} = 5$, $E_{TH} = 30$ (c) $L_{TH} = 6$, $E_{TH} = 30$ (d) $L_{TH} = 7$, $E_{TH} = 35$

4.4 결과 비교

이번 절에서는 디지털 신호처리 방식으로 홀로그래램을 암호화한 두 논문과 제안한 기법을 비교하고자 한다. 먼저, Wang^[7]의 논문에서 제안한 알고리

즘은 비교적 단순하게 Fourier 변환 방식으로 얻어진 디지털 홀로그래프를 화소 단위로 scrambling한 것이다. 홀로그래프를 직접 scrambling하기 때문에 시각적으로 판단되는 암호화 효과는 scrambling한 화소의 개수와 비례한다. 전체 홀로그래프를 모두 암호화하기 위해서는 전체 데이터의 100%를 암호화해야 한다. 앞서 설명한 바와 같이, 본 논문에서 제안한 방식은 전체 데이터 중에서 0.032%의 데이터만을 암호화하여도 전체 홀로그래프가 암호화되는 효과를 얻는다. 그러나 암호화를 시키기 위한 0.032%의 핵심 데이터를 찾기 위해 DWPT를 수행하는 과정이 추가적으로 요구된다. 암호화의 강인성을 고려하면 scrambling으로 수행된 암호화 방식은 원래의 데이터가 암호화된 결과에 고스란히 남아 있으므로 공격에 취약하다.

다음으로 Kim^[11]의 결과와 비교하고자 한다. 두 연구의 결과를 energy의 비교해보면, [11]에서는 홀로그래프가 갖는 에너지 중에서 90%의 에너지를 암호화해야지만 충분한 암호화 효과를 얻을 수 있는 반면에 본 논문에서는 30%의 에너지만을 암호화하여도 충분한 암호화 효과를 얻을 수 있다. 이는 본 논문에서 제안한 방식이 시각적으로 중요한 성분, 즉 암호화 효과를 최대화 시킬 수 있는 요소를 더욱 효율적으로 찾을 수 있다는 것이다. 또한 암호화 비율도 그 만큼 비례하여 감소하게 되는데 [11]에서 90%의 에너지를 포함하는 암호화의 경우에 25%의 데이터를 암호화하게 되는 반면에 제안한 방식은 0.032%만을 암호화한다. 만일 90%의 에너지를 암호화할 경우라 할지라도 level=7의 DWPT를 적용하면 전체 데이터에서 8.795%만을 암호화하기 때문에 알고리즘의 효율성은 훨씬 뛰어나다.

V. 결 론

본 논문에서는 디지털 홀로그래프를 공간 및 주파수 영역에서 분석하여 부표본화(subsampling), 국부화, 그리고 주파수의 에너지 분포 등에 대한 특성을 보였다. 이러한 특성으로부터 디지털 홀로그래프를 암호화하는데 전역변환이 적합하다는 것과 일반영상과 다르게 주파수를 분해해야 한다는 것을 알 수 있었다. 따라서 이산 웨이블릿 변환을 패킷화하여 홀로그래프의 주파수 성분을 분해하고, 이들 주파수에서 중요한 주파수 성분을 추적하였다. 중요한 주파수, 즉 많은 에너지를 갖는 주파수 성분을 선택하고 암호화하여 디지털 홀로그래프를 암호화하였다. 암호화

효과는 수치 및 시각적으로 확인하였다. 디지털 홀로그래프와 복원된 객체의 NC와 PSNR을 수치적으로 확인했을 경우에 상관성을 정의하기 어려웠다. 그러나 시각적인 특성과 암호화량을 분석하여 DWPT 레벨과 에너지 량 사이의 관계를 규명할 수 있었다. 또한 암호화를 위한 최적의 부대역 구조를 제시할 수 있었다. DWPT 레벨이 증가할수록 암호화량에 대한 암호화 효율은 높아진다. 그러나 연산량이 증가하므로 응용분야에 따라서 레벨과 에너지량, 그리고 암호화 강도를 적절하게 선택해서 사용해야 한다. 7레벨의 경우에 전체 데이터 중에서 0.032%의 데이터만을 암호화한다 할지라도 복원된 객체를 시각적으로 확인하기 어려웠다. 본 논문에서 제안한 디지털 홀로그래프의 암호화 기법과 분석결과는 추후 이 분야를 연구하는 연구자에게 좋은 지표가 될 것으로 기대한다.

참 고 문 헌

- [1] B. R. Brown and A. W. Lohmann, "Computer-generated Binary Holograms," IBM Journal of research and Development, Vol.13, No.2, pp.160-168, March 1969.
- [2] B. Javidi and F. Okano, "Three Dimensional Television, Video, and Display Technologies," Springer Verlag Berlin. March 2002.
- [3] P. Hariharan, "Basics of Holography," Cambridge University Press, 2002.
- [4] H. Yosikawa, "Digital holographic signal processing," Proc. TAO First International Symposium on Three Dimensional Image Communication Technologies, 1993.
- [5] X. Wang, D. Zhao, and L. Chen, "Image encryption based on extended fractional Fourier transform and digital holography technique," Optics Communication, Vol.260, pp.449-453, 2006.
- [6] L. Chen and D. Zhao, "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms," Optics Express, Vol.14, No.19, Sept. 2006.
- [7] 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,” Optics and Lasers Eng., Vol.45, pp.761-765, 2007.

[8] E. Tajahuerce and B. Javidi, “Encryption three-dimensional information with digital holography,” Appl. Opt. Vol.39, pp.6595-6601, Dec. 2000.

[9] H. Kim, D.-H. Kim, and Y. H. Lee, “Encryption of digital hologram of 3-D object by virtual optics,” Optics Express, Vol.12, No.20, pp.4912-4921, Oct. 2004.

[10] T. J. Naughton and B. Javidi, “Compression of encrypted three-dimensional objects using digital holography,” Opt. Eng., Vol.43, No.10, pp.2233-2238, Oct. 2004.

[11] D.-W. Kim, H.-J. Choi, Y.-G. Choi, J.-S. Yoo, and Y.-H. Seo, “Information hiding for digital holograms by electronic partial encryption methods,” Optics communication, Vol.277, Issue 2, pp.277~287, Sept. 2007.

[12] R. M. Rao, A. S. Bopardikar, and T. Boros, “Wavelet transforms, introduction to theory and application,” Prentice Hall PTR, 1st edition, Sept. 1998

[13] W. Sweldens, “The lifting scheme: A new philosophy in biorthogonal wavelet constructions,” in *Proc. SPIE*, Vol.2569, 1995, pp.68-79.

[14] I. Daubechies and W. Sweldens, “Factoring wavelet transforms into lifting schemes,” *J. Fourier Anal. Appl.*, Vol.4, pp.247-269, 1998.

[15] Z. Xiong, K. Ramchandran, M. T. Orchard, “Wavelet Packet Image Coding Using Space-Frequency Quantization,” *IEEE Trans. on Image Processing*, Vol.7, No.6, pp.892-898, June 1998.

[16] Y.-H. Seo, H.-J. Choi, and D.-W. Kim, “Lossy Coding Technique for Digital Holographic Signal”, *SPIE Optical Engineering*, Vol.45, No.6, pp.065802-1~065802-10, Jun. 2006.

서 영 호 (Young-Ho Seo)

중신회원



1999년 2월 광운대학교 전자재료 공학과 졸업(공학사)
 2001년 2월 광운대학교 일반대학원 졸업(공학석사).
 2000년 3월~2001년 12월 인티스 닷컴(주) 연구원.
 2004년 8월 광운대학교 일반대학원 졸업(공학박사)

2003년 6월~2004년 6월 한국전기연구원 연구원
 2004년 12월~2005년 8월 유한대학 연구교수
 2005년 9월~2008년 2월 한성대학교 조교수
 2008년 3월~현재 광운대학교 조교수
 <관심분야> 2D/3D 영상 및 비디오 처리, 디지털 홀로그래, SoC 설계, 워터마킹/암호화
 e-mail : yhseo@hansung.ac.kr

최 현 준 (Hyun-Jun Choi)

정회원



2003년 2월 광운대학교 전자재료공학과(공학사)
 2005년 2월 광운대학교 전자재료공학과(공학석사)
 2005년 3월~현재 광운대학교 전자재료공학과 박사과정

<관심분야> Image Processing, 디지털 홀로그래, 디지털 콘텐츠 보안, FPGA/ASIC 설계

김 동 욱 (Dong-Wook Kim)

중신회원



1983년 2월 한양대학교 전자공학과 졸업(공학사).
 1985년 2월 한양대학교 대학원 졸업(공학석사).
 1991년 9월 Georgia공과대학 전기공학과 졸업(공학박사).

1992년 3월~현재 광운대학교 전자재료공학과 정교수. 광운대학교 신기술 연구소 연구원.
 2000년 3월~2001년 12월 인티스닷컴(주) 연구원.
 <관심분야> 디지털 VLSI Testability, VLSI CAD, DSP 설계, Wireless Communication