

## Fresnelet transform을 이용한 디지털 홀로그램 워터마킹

\*구자명 \*서영호 \*김동욱

\*광운대학교

\*dwkim@kw.ac.kr

## Digital Holographic Watermarking using Fresnelet Transform

\*Koo, Ja-Myung \*Seo, Young-Ho \*Kim, Dong-Wook

\*Kwangwoon Univ.

## 요약

본 논문에서는 3차원 입체 비디오 기술의 최종목표인 디지털 홀로그램 영상의 소유권 보호를 위한 디지털 워터마킹 알고리즘을 제안한다. 제안한 워터마킹 알고리즘은 디지털 홀로그램의 Fresnelet 변환 영역에서 악의적인 공격들에 대해 강한 내성을 가지는 계수 정보들을 이용하여 워터마킹 정보를 추출하여 사용한다. 제안한 알고리즘으로 압축 등의 공격을 수행하여 본 워터마킹 알고리즘의 강인성을 검증하였다. 실험 결과 제안한 디지털 홀로그램 워터마킹 알고리즘은 대부분의 공격들에 대해 매우 강한 내성을 보였다.

## 1. 서론

홀로그램 비디오는 원래의 3차원 입체상을 공간상에 정확히 재현할 수 있는 가장 이상적인 입체 시각 시스템이며, 3차원 입체 비디오처리 기술의 최종목표는 결국에는 완전하게 입체를 구현한 홀로그램 서비스인 것이다.

홀로그래피는 1940년대 초에 제안된 이후 3차원 정보를 기록할 수 있다는 특징 때문에 많은 관심을 끌었다. 그리고 1966년 이후 많은 연구자들이 컴퓨터에 의한 홀로그램(computer-generated hologram, CGH)의 제작을 연구해 오고 있다[1][2].

인터넷 등 정보통신망의 급속한 발전 및 보급에 따라 소유권자의 동의 없이 디지털 콘텐츠들의 불법적 사용이 확산되면서 불법적 복제 및 위/변조를 방지하고 소유권을 효과적으로 보호하기 위한 디지털 워터마킹(Digital Watermarking) 기술은 지적재산권을 보호하는 기술로서 가장 각광받고 있으며, 현재 많은 연구와 실제적 응용으로의 접근이 이루어지고 있다[3][4]. 디지털 홀로그램은 2차원 정보이기는 하지만 3차원 정보를 포함하고 있는 초고부가가치의 콘텐츠이므로 소유권자의 소유권 보호가 디지털 홀로그램의 배포, 유통, 방송 등에 매우 중요한 요소가 될 것으로 전망된다.

본 논문에서는 CGH 기법으로 생성한 디지털 홀로그램의 소유권 보호를 위한 워터마킹 알고리즘을 제안한다. 제안한 알고리즘은 Fresnelet 변환 공간에서 각 부대역의 정보를 워터마크 정보로 사용하는 방법이다. 이 방법의 성능을 평가하기 위하여 압축 등의 공격을 수행하여 본 알고리즘의 강인성을 검증한다.

## 2. Fresnelet 변환

Fresnelet 변환은 디지털 홀로그램에 대하여 2D기반의 영상처리 기법을 사용하기 위해 홀로그램을 Fresnel변환과 Wavelet 변환을 이용하여 만들어진 알고리즘이다.

Fresnel 변환은 식 1과 같이 입력으로부터 거리  $z$ 에 회절 현상을 나타낼 수 있다[5].

$$g(s) = Ff(x), \quad F = \frac{\Delta s}{\sqrt{\lambda z}} U W V \quad (1)$$

$$U = \text{diag}[u_x] u_x = \exp\left[\frac{j\pi}{\lambda z}(x \Delta x)^2\right]$$

$$V = \text{diag}[v_s] v_s = \exp\left[\frac{j\pi}{\lambda z}(s \Delta s)^2\right]$$

$$W = [w_{xs}] w_{xs} = \exp\left[-\frac{j2\pi}{\lambda z}(x \Delta x)(s \Delta s)\right]$$

$f(x)$ 는 입력이고  $g(s)$ 는 출력이다.  $\lambda$ 는 광원의 파장이고  $\Delta x$ 와  $\Delta s$ 는 입력과 출력의 화소의 크기이다.

식 1의 Fresnel 변환 필터  $F$ 를 식 2와 같이 각각 저대역 필터( $F_0$ )와 고대역 필터( $F_1$ )를 만들어 Fresnelet 변환을 할 수 있다. 식 3은 역 Fresnelet 변환을 위한 필터이다.  $L$ 과  $H$ 는 Wavelet변환의 각각 저대역 필터와 고대역 필터이다[6].

$$F_0 = \frac{\Delta s}{\sqrt{\lambda z}} L U W V, \quad F_1 = \frac{\Delta s}{\sqrt{\lambda z}} H U W V \quad (2)$$

$$F_0^* = \frac{\Delta x}{\sqrt{\lambda z}} V^* W^* U^* L^t, \quad F_1^* = \frac{\Delta x}{\sqrt{\lambda z}} V^* W^* U^* H^t \quad (3)$$

그림 1은 홀로그램의 회절 영상에 Wavelet 변환을 적용하였다.

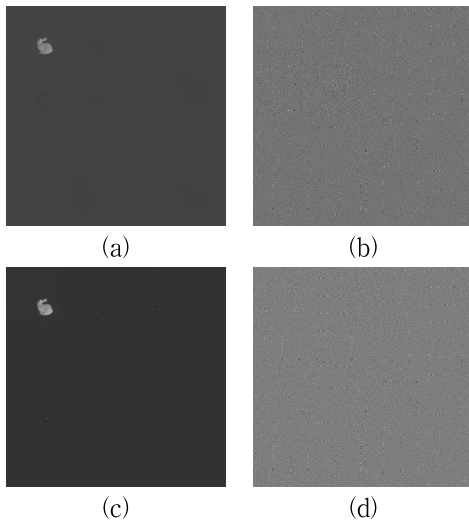


그림 1. Fresnelet 변환된 부대역 영상: Mallat-tree Fresnelet; (a) 크기, (b) 위상, Quad-tree Fresnelet; (c) 크기, (d) 위상.

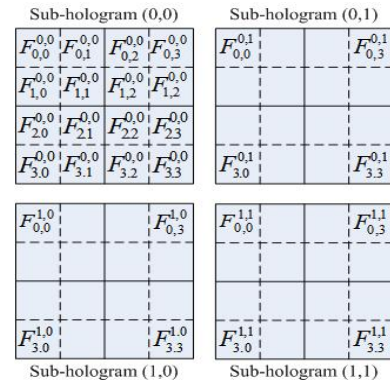


그림 3 4개로 분할된 각 홀로그램의 2-level Fresnelet 변환

$$AD_{i,j} = \frac{1}{m \times n} \sum_{h=1}^m \sum_{w=1}^n D_{i,j}^{h,w} \quad (2)$$

그 다음  $AD_{i,j}$  를  $k$ -bit 양자화(quantization  $QAD_{i,j}$ )하여 그것을 워터마크 정보로 사용한다. 이렇게 모든 부대역에 대해 동일한 방법으로 워터마크를 추출하여 비트스트림으로 나타내면 식 (3)과 같다.

$$W = QAD_{1,1}, QAD_{1,2}, \dots, QAD_{1,2^n}, \dots, QAD_{2^n,1}, \dots, QAD_{2^n,2^n} \quad (3)$$

### 3. 제안한 워터마킹 알고리즘

그림 2는 제안하는 워터마킹 방법의 전체 흐름도를 나타내고 있다.

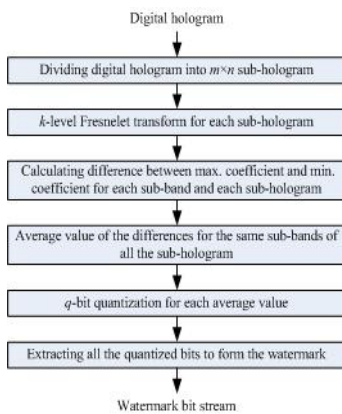


그림 2. 전체 워터마킹 알고리즘

먼저, 보호하고자 하는 디지털 홀로그램을 원하는 수( $m \times n$ )만큼 분할을 한 다음 그림 3와 같이 분할된 각 홀로그램을 Fresnelet 변환을 한다.

그 다음 각 부대역의 최고, 최저 계수들의 차이( $D_{i,j}^{h,w}$ )를 구한 다음, 각 부분 동일 위치에 있는 홀로그램의 차이 값 평균을 식 (2)와 같이 구한다.

### 4. 실험 및 결과

그림 4은 디지털 홀로그램 워터마킹의 강인성을 평가하는 흐름도를 나타낸다.

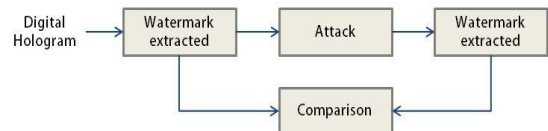


그림 4. 강인성 평가 방법

그림 5은 디지털 홀로그램을 공격하여 홀로그램을 Fresnel 변환을 이용하여 회절한 영상이다. 원본에 비해 가우시안 블러링 공격을 가한 영상이 가장 나쁜 화질을 보였으며, 샤프닝 공격 후의 영상이 가장 원본과 유사해 보였다.

표 1은 공격 후 원본 영상과의 화질 및 추출한 워터마크 bit stream의 공격에 따른 오차율을 구한 것이다.

오차율에서 볼 수 있듯이 본 논문에서 제안한 디지털 홀로그램 보호를 위한 워터마킹 알고리즘이 예상되는 다양한 공격들에 대해 상당히 높은 수준의 내성을 가지고 있음을 확인 할 수 있다.

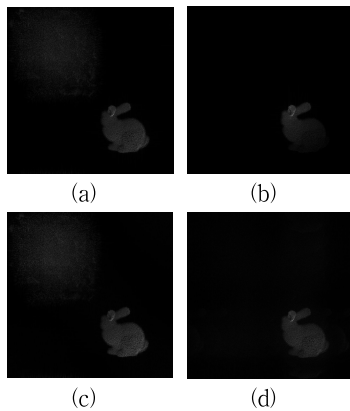


그림 5. 공격당한 회절 영상: (a) 원본, (b) 가우시안 블러링, (c) 샤프닝, (d) JPEG 압축

[2] J. K. Chung and M. H. Tsai, Three-Dimensional Holographic Imaging, John Wiley & Sons, Inc., 2002.  
 [3] Watermarker Community (<http://mad.sarang.net>), 2004.  
 [4] K.Tanaka, Y. Nakamura and K.Matsui, "Embedding Secret Information into a Dithered Multilevel Image", Proceeding of 1990 IEEE Military Communications Conference, pp. 216-220, 1990.  
 [5] U. Schnar and W. Jueptner, Digital Holography, Springer, Berlin, Germany, 2005.  
 [6] M. Nazeer and D.-G. Kim, "An Efficient Data Hiding Technique in Frequency domain by using Fresnelet basis", WCE 2012, London, U.K, 2012.

표 1 공격에 대한 영상 화질 및 오차율

Attacks		Image quality(dB)	Error ratio of extracted watermark(%)
Original hologram	Blurring (Gaussian)	31.3	1.3
	Sharpening	35.2	0.4
	JPEG quality 12	51.5	0
	JPEG quality 0	30.9	2.2
Cropped hologram	Blurring (Gaussian)	32.6	3.3
	Sharpening	38	1.4
	JPEG quality 12	49.7	0
	JPEG quality 0	30.7	3.3

## 5. 결론

본 논문에서는 디지털 홀로그램을 Fresnelet 변환한 후 어느 공격에도 강인성을 갖는 워터마킹 정보를 찾는 방법을 제안하였다. 제안한 알고리즘을 적용한 후 총 4 단계의 공격을 수행하여 워터마킹 알고리즘의 강인성을 검증하였다. 실험 결과 공격에 따른 제안한 알고리즘의 오차율이 최대 2.2%까지 나타나는 것을 확인하였다.

## 감사의 글

이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2010-0026245).

## 참고문헌

[1] T. Motoki, H. Isono, and I. Yuyama, "Present Status of Three-Dimensional Television Research," Proc. IEEE 83(7): 1009-1021(July 1995).