프레넬 변환을 이용한 암호화 알고리즘

*이윤혁 *서영호 *김동욱

광운대학교

*winner9100@kw.ac.kr

Encryption Algorithm using Fresnel Transform

*Lee, Yoon-Hyuk *Seo, Young-Ho *Kim, Dong-Wook

Kwangwoon University

요약

최근 고 해상도의 콘텐츠의 보급이 늘어나는데 이에 따라 암호화를 위한 계산 량과 시간이 증가하였다. 본 논문은 고 해상도의 콘텐츠에서 많은 양의 암호화 계산과 시간을 줄이기 위해 프레넬 변환을 이용한 암호화 방법을 제안하였다. 프레넬 변환을 통하여 획득한 회절 영상은 거리에 따라 가운데로 집중되는 특성을 가지는데, 고 해상도의 영상을 먼 거리에서의 회절 영상을 획득하여 가운데의 집중된 영역에 암호화를 수행하여 암호화 영역을 줄여 계산 량을 줄일 수 있다. 본 논문에서 제안하는 암호화 알고리즘을 구현하여 10m의 거리일 때 0.004%의 데이터만 암호화 하여 모든 데이터를 숨길 수 있다.

1. 서론

최근 고 해상도의 콘텐츠의 보급이 늘어나고, 이에 따른 콘텐츠의 보호를 위한 암호화 알고리즘이 연구되고 있다. 그러나 고 해상도의 영상을 암호화하기 위해서는 많은 양의 계산과 시간이 필요하다[1]. 본 논문에서는 앞서 설명한 문제를 해결하기 위해 프레넬 변환을 수행하여 거리에 따른 회절 영상의 집중 현상을 이용하여 적은 량의 데이터를 암호화하여 데이터를 보호할 수 있는 알고리즘을 제안한다. 2장에서는 프레넬 변환의 회절 영상의 집중 현상을 설명하고, 3장에서는 제안하는 알고리즘을 설명하고, 마지막으로 결과를 보인다.

2. 프레넬 변환

식 1은 프레넬 변환을 위한 식으로 $X(x,y,z)$는 $E(u,v,0)$로부터 거리 z만큼 떨어진 회절 평면의 x,y좌표의 회절 값이고 λ는 파장이고, p_x,p_y,p_u,p_v는 각각 x,y,u,v에 해당하는 화소의 크기 이다[2].

$$X(x,y,z) = e^{j\frac{\pi}{\lambda z}\{(xp_x)^2+(yp_y)^2\}} \sum E(u,v,0) e^{j\frac{-2\pi}{\lambda z}\{xp_x up_u + yp_y vp_v\}} e^{j\frac{\pi}{\lambda z}\{(up_u)^2+(vp_v)^2\}} \quad (1)$$

p_x,p_y는 $p_x=(\lambda z)/(p_u N)$, $p_y=(\lambda z)/(p_v M)$의 관계식을 가지는데 N,M은 입력 영상의 해상도 이다. 즉, p_x,p_y는 거리에 따라 비례하여 커진다. 즉, 입출력의 해상도가 같을 경우 회절 평면의 실제 크기는 거리에 비례하여 커진다. 그러나 2D영상과 같이 평면 입력의 경우 거리와 관계없이 회절 평면에 나타나는 회절 영상의 실제 크기는 일정하다. 따라서 그림 1과 같이 상대적으로 거리에 따라 회절 영상이 가운데로 집중되는 현상이 생긴다[1].

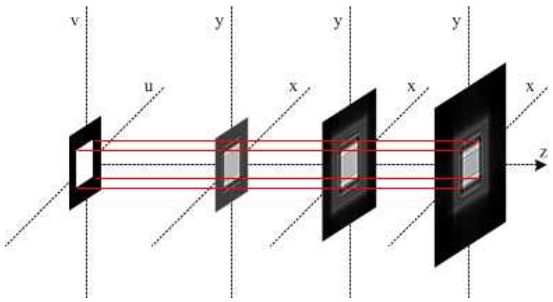

그림 1. 거리에 따른 회절 영상

3. 프레넬 변환을 이용한 암호화 방법

앞 장에서 설명한 프레넬 변환의 특성을 이용하여 암호화 방법을 그림 2에 나타내었다. 식 1에서 프레넬 변환은 복소수의 연산을 통하여 계산을 하는데, 입력 영상은 실수만 존재하기 때문에 복소수를 위하여 가로 방향으로 1/2 다운 샘플링을 통하여 짝수 열은 실수, 홀수 열은 허수로 재배치를 수행한다. 다음으로 회절 영상을 만들기 위해 프레넬 변환을 수행 하는데, 가로방향으로 1/2 다운 샘플링을 하였기 때문에 가로 방향의 화소의 크기는 2배로 하여 입력의 실제 크기를 맞추어 준다. 프레넬 변환을 수행 후 가운데로 집중된 영역을 찾기 위해 식 2를 통하여 암호화 영역의 크기를 구하여 암호화를 수행한다. 식 2에서

n,m은 암호화 영역의 가로 세로 해상도이다. w_x,w_y는 가중치 계수이다.

$$n = w_x \frac{(p_u N)^2}{\lambda z}, m = w_y \frac{(p_v M)^2}{\lambda z} \quad (2)$$

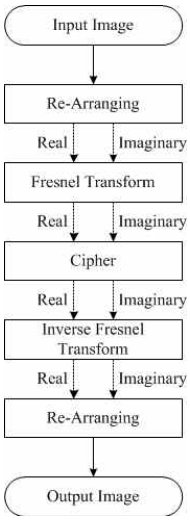

그림 2. 프레넬 변환을 이용한 암호화 알고리즘

4. 실험 결과

그림 3은 가중치를 1로 하고, 거리를 0.5, 1, 5, 10m로 변화 시켰을 때 암호화한 영상이다. 표 1은 각 결과의 집중된 회절 영상의 크기(암호화 영역)와 암호화 율을 나타냈다. 거리가 증가 할수록 암호화 율은 줄지만 데이터 숨김 정도가 낮아지는 결과를 확인했다.

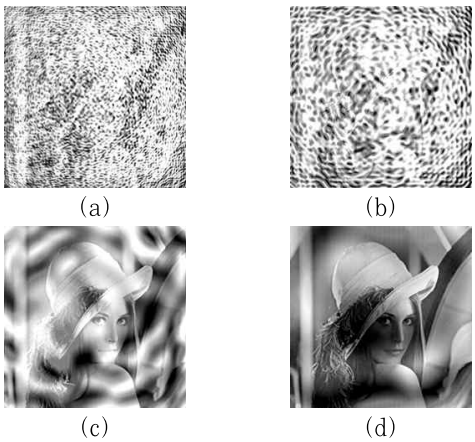

그림 3. 가중치 1일 때의 암호화 결과 (a)0.5m, (b)1m, (c)5m, (d)10m

표 1. 가중치 1일 때의 암호화 율

거리(m)	0.5	1	5	10
암호화 크기	89×89	44×44	8×8	4×4
암호화 율(%)	0.378	0.092	0.003	0.0007

그림 4는 암호화 율을 0.004% (암호화 영역의 크기, 10×10)으로 하여 암호화를 수행한 영상이다. 10m일 때 가중치를 1로 하였을 때의 집중된 회절 영상의 크기(4×4)보다 약 2.5배 정도 크게 암호화를 수행하여 데이터를 숨길 수 있다.

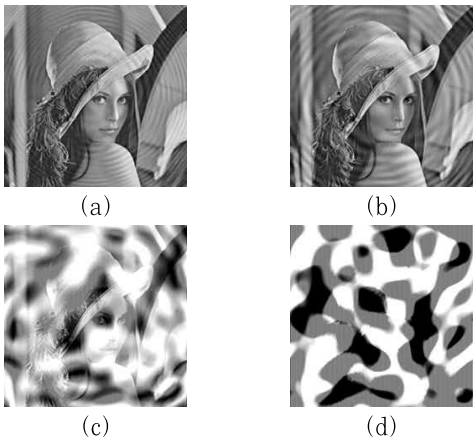

그림 4. 가중치 1일 때의 암호화 결과 (a)0.5m, (b)1m, (c)5m, (d)10m

5. 결론

본 논문에서 프레넬 변환을 거리에 따라 회절 영상의 집중되는 현상을 이용하여 암호화 영역을 줄여 암호화를 하는 방법을 제안 하였다. 10m의 거리에서 0.004%의 데이터만 암호화 하여 수행하여도 데이터를 모두 보호할 수 있다. 이는 더 높은 해상도의 콘텐츠도 적은 계산량으로 암호화 할 수 있다.

감사의 글

이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2013R1A1A2057798).

참고 문헌

[1] http://en.wikipedia.org/wiki/Fresnel_diffraction

[2] Y.-H. Lee, H.-J. Choi, Y.-H. Seo, D.-W. Kim, “Digital Hologram Watermarking with the Fresnel Diffraction Model”, 3DSA, May 2014.