주파수 공간에서 Peak Constellation을 활용한 비가시성 워터마크의 설계 및 평가

이창민[1], 김재국[1], 박경준, 최완주, 이상화[2], 조남익

서울대학교 전기·정보공학부 뉴미디어통신공동연구소, ㈜마크애니

dochi@snu.ac.kr, jaeguk@snu.ac.kr, kjpark@markany.com, wjchoi1@markany.com,

lsh529@snu.ac.kr, nicho@snu.ac.kr

([1]공동 1저자, [2]교신저자)

Design and Evaluation of Invisible Watermark using Peak Constellation in Frequency Domain

Lee Changmin[1], Kim Jae Guk[1], Kyung Jun Park, Wan Joo Choi, Lee Sang Hwa[2],

Cho Nam Ik

INMC, Dept. of Electrical and Computer Engineering, Seoul National University

MarkAny Inc.

요 약

본 논문은 영상의 주파수 영역에서 constellation 구조를 갖는 워터마크 패턴의 설계를 제안 및 평가를 수행한다. 주파수 영역에서 정의된 constellation의 위치에 peak의 유무의 판단을 통하여 0과 1을 구분하며, 이렇게 생성된 peak constellation 구조에 대해 역퓨리에 변환을 수행하면 고주파 특성을 지닌 noise 이미지가 된다. 이를 이미지에 적절히 삽입하는 것을 통하여 비가시적 워터마킹을 구현하였으며, 이를 실제 이미지에 적용하여 비가시성 부분에서는 SSIM 0.998 수준의 성능과 최대 224비트의 메시지를 전달 가능한 것을 확인하였다. 또한 54비트의 peak constellation 구조에 대하여 BER 0.002 수준의 오류율을 보이는데 성공하였다.

Ⅰ. 서 론

생성형 AI 기술이 발달함에 따라, 영상의 출처 및 소유권 판별에 대한 기술의 수요가 증가하고 있다. 일반적으로 영상이나 문서에 대한 권리를 보호하기 위해 사용되는 방법이 저작권자를 특정할 수 있는 이미지나 글귀를 희미하게 삽입하는 워터마킹 기법이며, 특히 디지털 이미지의 워터마킹에 대해서는 저작권, 군, 포렌식과 같은 다양한 분야에서의 수요가 존재한다[1].

워터마킹 기법은 크게 spatial domain, frequency domain에서의 워터마킹으로 분류가 되며[2], 또한 워터마크가 가시적이냐 비가시적이냐로 구분이 된다[3]. 일반적으로 주파수 공간에서의 워터마킹이 여러 가지 기하학적 공격에 대해서 강건함을 보이며[4], 이에 본 논문은 비가시적인 주파수 공간에서 비가시적 워터마크에 대한 연구를 진행하였다.

본 논문에서는 비가시적인 워터마크의 구현을 위하여 FFT를 활용한 주파수 공간에서의 peak constellation 구조의 설계에 대해서 다루며, peak constellation 구조의 성능에 대하여 논한다.

Ⅱ. Peak Constellation 구조의 설계

본 논문에서 설계한 비가시성 워터마크는 다음과 같은 특징을 가지도록 하였다.

1) 영상에 특징적으로 보이지 않는 noise 구조
2) 반복된 패턴을 삽입하여 영상의 일부를 통하여 추출 가능
3) 삽입된 메시지의 내용과 관계 없이 유지되는 비가시성
4) 주파수 영역에서의 규칙성을 가져 constellation 구조를 파악 가능
5) 크롭, 리사이징과 같은 다양한 종류의 공격을 받은 이후 추출 가능

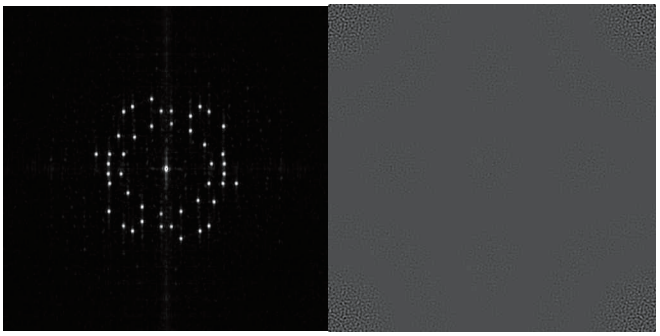

그림 1. 주파수 domain의 Peak (왼쪽)과 이를 기반으로 생성된 noisy한 이미지(오른쪽)

이러한 특징들을 위하여, 그림 1과 같이 패턴 이미지의 512x512 pixel에 대응되는 FFT domain에 peak를 삽입하여 이를 바탕으로 512x512 크기의 noisy한 패턴을 생성하였다. 일반적인 이미지에 대하여 FFT 수행시, 대부분 이미지의 특성들은 저주파 영역에 형성되기에, 해당 신호와 겹치지 않게 하기 위하여 고주파 영역에 peak를 삽입하였다. 또한 resizing, warping과 같은 공격에 강건하도록 몇 개의 궤도를 설정하여 궤도를 따라 peak를 추정할 수 있도록 하였다. 그림 1에 보이는 것은 3개의 궤도를 지닌 constellation 구조이며, constellation 위에 peak를 놓는 구조를 이후 peak constellation 구조라 정의한다. 이렇게 정의된 동심원의 peak constellation 구조는 warping, resizing에 대해서도 어느정도 구조를 유지하여 메시지를 추출가능할 수 있도록 한다.

미리 정의해둔 constellation의 peak 위치를 통하여, 해당 위치에 peak가

존재하지 않으면 0, 존재한다면 1로 인식하여, 이를 통하여 peak constellation에 담긴 메시지를 복호화 하면 비가시성 워터마크에 담긴 메시지를 복원 가능하도록 하였다.

Ⅲ. Peak Constellation에 대한 실험

본 단락에서는 앞서 제시한 peak constellation 구조의 성능에 대해서 평가를 진행한다. 비가시성 워터마크의 주요 성능으로 얼마나 잘 안보이는지, 얼마나 많은 메시지를 손실없이 담을 수 있는지를 논하며, 본 논문에서는 이 두가지 성능에 대해서 논할 것이다. 모든 실험은 주파수영역에서 메시지에 대응되는 peak를 심고 512x512 크기의 패턴 이미지를 생성후, 이를 1024x1024 크기의 이미지에 블렌딩 한 후, 이를 재추출하는 과정을 거쳐 진행하였다.

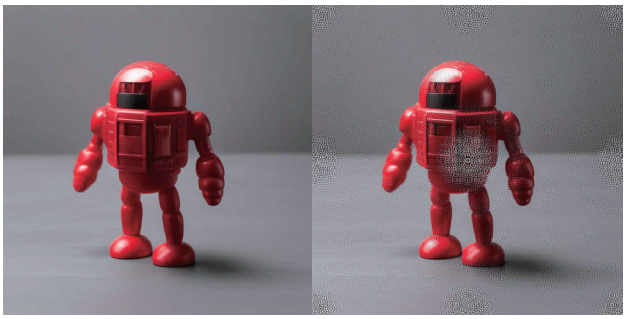

그림 2. 워터마크를 삽입 전 이미지 (왼쪽)과 삽입 후 이미지 (오른쪽)

그림 2는 워터마크 삽입 전 이미지와 실험에서 진행한 비가시성 워터마크가 삽입된 이미지 간의 SSIM 값은 담긴 메시지와 무관하게 0.998 수준이며, 본 논문에서는 이해를 돕기 위하여 가시성을 높여 어떤 식으로 비가시성 워터마킹이 삽입되었는지를 보였다.

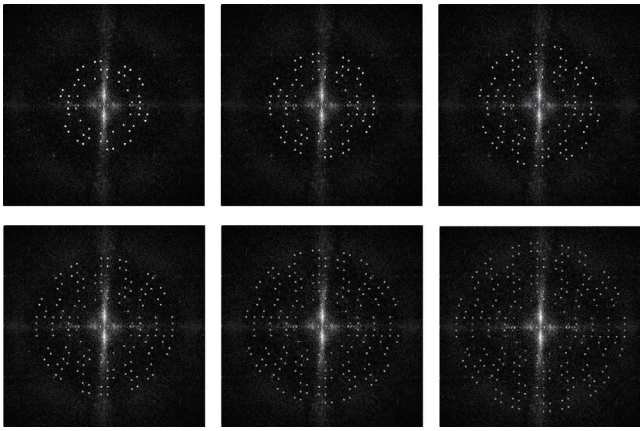

그림 3. 다양한 궤도(3~8)의 개수에 따른 peak 추출 결과

그림 3은 앞에서 보인 그림 2의 대해서 다양한 궤도의 개수에 대하여 패턴 이미지를 생성한 후 이를 fft domain으로 다시 추출한 결과이다. 궤도 3개의 constellation 구조부터 궤도 8개의 constellation 구조까지 메세지를 담도록 실험을 하였으며, 궤도 3개의 경우 54비트, 8개의 경우 224 비트의 메시지를 담았다.

위 그림으로부터 peak의 추출에 대해서는 궤도의 개수가 늘어나도 어느 정도 육안으로 추출이 되는 것을 확인 가능하나, 궤도 수가 늘어남에 따라 peak의 수가 증가할수록 이미지에서 보이는 peak 하나의 해상도가 서서히 떨어지는 현상을 보여주고 있다.

Ⅳ. 결론

본 논문에서는 비가시성 워터마크의 방법론으로써 주파수 도메인에서의 peak constellation의 설계 및 성능에 대해서 연구를 수행하였으며, SSIM 0.998 수준의 원본 영상과 거의 비슷한 수준의 비가시성과, 최대 224비트의 메시지를 추출하는데 성공하였으며, 54bit의 peak constellation 구조에 대해서 임의의 400장의 이미지에 대하여 메시지 검출을 진행하여 BER(Bit Error Rate) 0.002 수준의 오류율을 보이는데 성공하였다.

그러나 그림 4에서 보이는 것처럼 궤도 수에 따른 비트 수 증가가 아닌, 메세지의 peak 개수 자체가 늘어나면 peak 자체의 해상도가 떨어지는 현상이 있어, 이를 위하여 안정적으로 메시지의 검출이 가능한 최대 비트 수에 대한 연구나, 후처리에 대한 추가적인 연구가 필요할 것으로 사료된다.

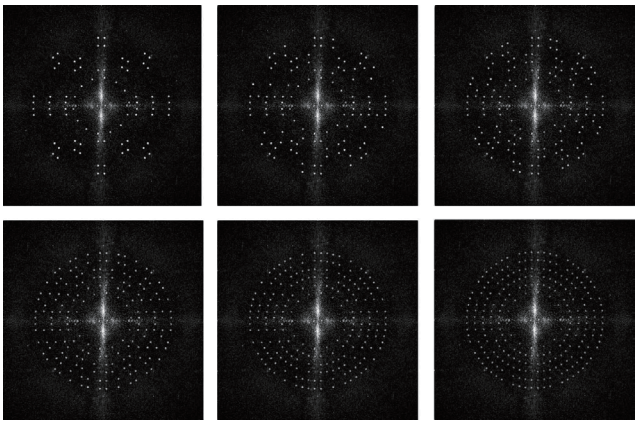

그림 4. peak 개수 증가에 따른 peak 추출 결과

ACKNOWLEDGMENT

본 논문은 과학기술정보통신부 정보통신산업진흥원의 2024년도 AI반도체 응용실증 지원사업의 지원을 받아 수행됨. (과제명: 생성형 AI 콘텐츠 진위 여부 판별을 위한 국산 NPU AI 반도체 기반 고속 Invisible Watermarking 서비스 실증, 주관기관: ㈜마크애니).

참 고 문 헌

[1] Hosny, Khalid M., et al. "Digital image watermarking using deep learning: A survey." Computer Science Review 53 (2024): 100662.

[2] S. Gaur, V. Barthwal, An extensive analysis of digital image watermarking techniques, Int. J. Intell. Syst. Appl. Eng. 12 (1) (2024) 121 - 145.

[3] Zainol, Zurinahni, et al. "Hybrid SVD-based image watermarking schemes: a review." IEEE Access 9 (2021): 32931-32968.

[4] Sharma, Sunpreet, et al. "A review of image watermarking for identity protection and verification." Multimedia Tools and Applications 83.11 (2024): 31829-31891.