Generative Adversarial Network를 이용한 디지털 워터마킹 방법

*이재은 서영호 김동욱

광운대학교

*jelee@kw.ac.kr

Digital Watermarking Method using Generative Adversarial Network

*Lee, Jae-Eun Seo, Young-Ho Kim, Dong-Wook

Kwangwoon University

요약

본 논문에서는 GAN(Generative Adversarial Network)을 이용한 디지털 워터마크 삽입 및 추출 방법을 제안한다. 호스트 영상의 데이터 셋은 128×128 크기의 흑백 영상인 BOssBase 데이터 셋을 사용하고, 워터마크 영상은 8×8 크기의 이진 영상을 사용한다. 네트워크는 호스트 영상에 워터마크를 삽입하는 삽입기와 워터마크가 삽입된 영상에서 워터마크를 추출하는 추출기로 구성된다. 강인성을 위해 삽입기가 생성한 영상에 공격 시뮬레이션을 수행한 다음에 워터마크를 추출한다. 그 결과, PSNR은 31.47dB가 나왔고, 공격에 강인한 워터마크를 추출할 수 있다.

1. 서론

최근, 영상의 무분별한 공급으로 인한 지적재산권 보호기술이 필수적이다. 지적재산권 보호기술로 가장 유망한 기술은 워터마킹(watermarking) 기술이다[1].

따라서, 본 논문에서는 요즘 컴퓨터 비전에서 뛰어난 결과를 내어 주목받고 있는 딥 러닝을 기반으로 디지털 워터마크를 삽입하고 추출하는 방법을 제안한다. BOssBase 데이터 셋을 사용하고, GAN 구조를 이용하여 네트워크를 구성한다. 강인성을 측정하기 위해, 공격에 대한 강도를 조절하여 시험한 뒤 결과를 비교, 분석한다.

2. 제안하는 방법

스테가노그래피 데이터 셋인 흑백 영상의 BOssBase 10,000장을 128×128 크기로 조절하여 호스트 영상의 훈련 데이터로 사용한다. 워터마크 영상은 8×8의 이진 영상을 사용한다.

네트워크의 구조는 GAN 구조를 이용한 삽입기와, 추출기로 구성되며 Fig. 1에 나타낸다. 8×8 크기의 워터마크 영상을 4개의 컨볼루션 계층을 수행하여 128×128로 만든다. 그 다음, 업샘플링한 워터마크 영상과 호스트 영상을 붙이고, 5개의 컨볼루션 계층을 수행하여 워터마크가 삽입된 영상을 만든다. 삽입기가 만든 영상을 공격 시뮬레이션을 수행하고 추출기의 입력으로 사용하여 공격에 대한 강인성을 갖도록 한다. 추출기는 4개의 컨볼루션 계층을 수행하여 8×8 크기의 워터마크를 추출한다. 활성화 함수는 영상을 출력하는 층에서만 tanh 함수를 사용하고 그 외에는 모두 ReLU 함수를 사용한다.

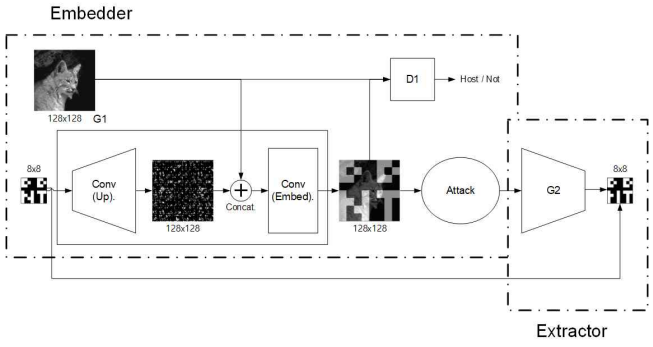

Fig. 1. Architecture of Embedder and Extractor

3. 실험 결과

시험 데이터는 49장의 표준 데이터 셋을 128×128로 조절하여 사용한다. 삽입기가 생성한 워터마크가 삽입된 영상과 호스트 영상의 PSNR을 측정하여 평균한 결과가 31.47dB이다. 결과 영상은 Fig. 2에 나타낸다. 그 다음, 워터마크가 삽입된 영상에 공격을 수행하여 추출기로 워터마크를 추출한 결과를 Fig. 3에 나타낸다.

Fig. 2. Samples of host image and watermark embedded image. First row: Host image, and second row: watermark embedded image

	No attack	Gaussian filtering (3×3)	Salt and pepper (p=0.01)	Gaussian additive noise (p=0.01)
NC	0.9840	0.8840	0.9776	0.9588

Table. 1. NC result of extracted watermark according to attack

4. 결론

본 논문은 딥 러닝을 사용하여 디지털 워터마크를 삽입 및 추출 할 수 있는 가능성을 증명하였고 추후에는 기존 알고리즘보다 더 강인한 네트워크를 설계할 수 있을 것이라 기대한다.

감사의 글

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2019R1F1A1054552)

참고문헌

[1] Ingemar J. Cox, et al., “Digital Watermarking and Steganography”, Elsevier, 2008.