

웹 빅데이터를 활용한 앙상블 딥러닝 기반 불법 복제품 판독 자동화 시스템

이찬재 · 정성호 (넷코아테크 미래기술전략연구실), 운영 (홍익대학교)

목 차	1. 서 론
	2. 선행 연구
	3. 방법론
	4. 실험 결과
	5. 결 론

1. 서 론

디자인이란, 주어진 목적을 달성하기 위해 창작자가 여러 조형요소를 합리적이고 유기적으로 구성한 일련의 창작 활동을 의미하며, 이를 통한 결과물을 포함한다. 이러한 디자인은 디자인 출원을 통해 저작권, 디자인권에 따라 법적인 보호를 받을 수 있다. 그런데 이 디자인을 불법적으로 정교하게 모방할 경우 일반인은 진품과 가품에 대해 전문지식 없이 구별하기가 쉽지 않다. 또한 국내 외적으로 불법적인 위조 및 복제품들이 늘어나고 있고, 이에 따라 정당한 권리를 가진 생산자와 소비자가 피해를 입는 사례가 증가하고 있으며, [1]의 OECD 보고서에 따르면 연간 피해액이 5천억 달러에 이른다고 한다. 이러한 피해를 방지하고자 세관에서는 해외로부터 들어온 물건의 불법 모방 여부를 파악하고 불법 복제가 의심되는 경우 다양한 각도에서 물건을 촬영하여 이를 디자인 저작권

자에게 통보한다. 그러나 이러한 일련의 판독 과정은 서로 다른 특성을 가진 디자인권이 계속해서 추가(출원)되고 시간이 지나면 삭제(소멸)되는 디자인권의 독특한 특성 때문에 자동화 과정을 구축하기 어렵다. 현재 판독해야하는 물건에 대한 교육을 받은 판독권자가 직접 물품을 하나씩 검사하고 있으나, 하루에도 수 없이 많은 물건이 들어오기 때문에 물건들을 직접 전수 조사하기에는 어려움이 있다.

따라서 본 연구에서는 [2]에서 제안된 것과 같이 다수의 물품에 대해 분해 및 파괴 검사를 행하지 않고 검사 물품의 특정 디자인권 침해 여부를 판단하는 인공지능 기반 자동 판독 시스템의 접근 방법에 기반하여 용도에 따라 기존의 합성 신경망 기반의 오토인코더 대신 웹 빅데이터를 활용한 앙상블 딥러닝 모델을 제안하고자 한다. 앙상블 모델은 총 2단계로 구축되어 있으며, 1단계는 UP-DETR[3]과 YOLOv4[4]를 결합한 앙상블 모

델로 현물 이미지로부터 가장 유사한 3개의 디자인 등록번호를 추출하는 단계이다. 2단계는 현물 이미지와 함께 특정 물건의 도면이 제시된 경우에 도면에 대해 학습한 Resnet[5] 모델을 결합하여 현물과 도면의 유사도를 측정하고 이를 제공하는 단계이다. 판독 시스템의 목표는 기존의 시스템과 같이 대상 물건의 외형을 기준으로 디자인권을 파악하는 것을 목표로 한다. 이 시스템을 통해 수작업 판독 시스템을 자동화하여 물건이 진품일 경우 해당하는 디자인권을 파악하고, 불법 복제품일 경우 웹 기반 REST API를 활용하여 크롤링 및 스크랩을 통해 수집된 웹 빅데이터를 사용해 수집된 저작권 정보를 토대로 진품의 디자인권을 찾아 디자인 저작권자에게 전달할 수 있도록 하는 자동화 서비스를 개발하여 제공함으로써 생산자 및 소비자의 정당한 권리를 보호하고자 한다.

2. 선행 연구

불법 복제품 여부 판별을 위해서 가장 기본적으로 사용되는 주요 특징은 가시적인 물건의 특성으로, 물건의 이미지를 촬영하여 판독 할 수 있다. 판별 작업을 자동화하기 위해서는 현물 이미지에 존재하는 특정 패턴을 추론 할 수 있어야 하는데, 이는 컴퓨터 비전 분야의 알고리즘을 통해 해결 할 수 있다. 특히 물건의 특정 패턴을 학습하여 디자인권 침해 여부를 판독하기 위해서는 [3-5]에서 제시된 것과 같은 대표적으로 우수한 예측 성능을 기록한 컴퓨터 비전 분야의 알고리즘들을 적용하여 문제를 해결 할 수 있다.

기술이 발전하면서 복제품들은 보다 정교하게 진화하고 있지만, 불법 복제품 판독 분야는 발전은 매우 더딘 상황이다. [6,7]에서는 위조지폐 판독을 위해, [8]은 로고에 대한 위조 및 복제 감지를

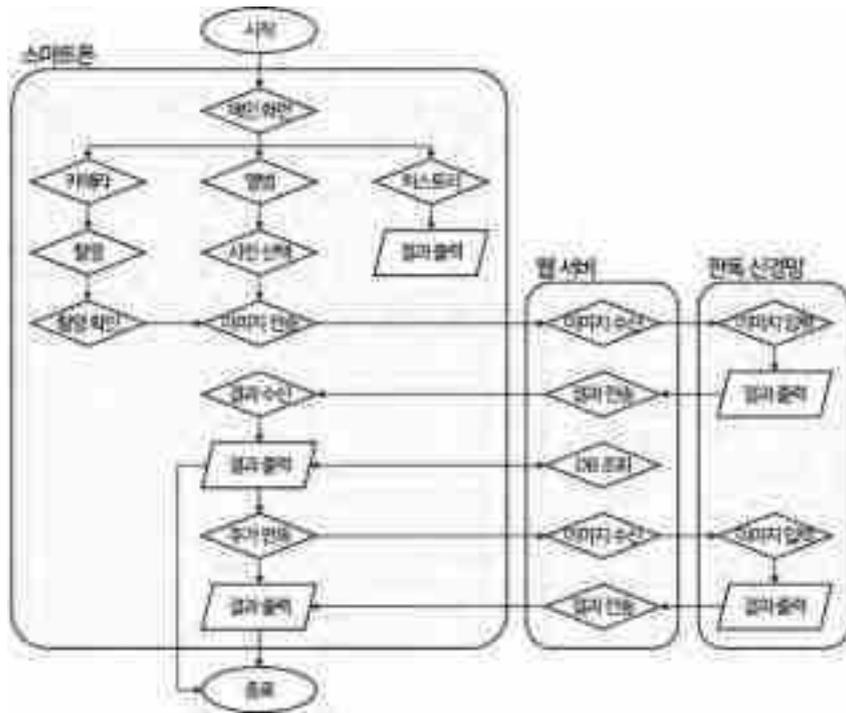
위해 컴퓨터 비전 인공지능 모델이 제안되었으며, 이와 같이 비슷한 분야에서 사용된 유사 선행 연구들이 존재한다. 그러나 [6-8]에서 알 수 있듯 여전히 한정된 분야에서 한정된 물건에 대해서만 연구되어지고 있다. 또한 이와 관련된 각 회사가 가진 판독 기술들은 공개 시 무수한 위조품들이 보다 쉽게 만들어질 수 있으므로 해당 기술을 가진 기업들은 위조 감지 시스템을 공개하지 않고, 대부분 폐쇄적으로 구축하여 서비스를 제공하고 있다. 따라서 관련 분야의 선행 연구가 많이 공유되지 않아 참고가 어렵다.

3. 방법론

[6-8]에서 제시된 선행 연구들의 판독 시스템은 한정된 물건에 대해서만 진행 되었지만, 본 연구에서는 여러 회사의 다양한 물건에 대해서 동시에 판독이 가능한 통합 자동 판독 시스템을 구축하고자 한다. 판독 시스템의 핵심 기능인 판독 신경망은 단계적으로 학습하여 부분적으로 물건의 추가 및 변경이 가능하고, 여러 종류의 물건 판독 시 최적의 임계치를 적용한 단계적인 직렬연결 방법으로 결과를 출력하므로, 정확히 물건의 디자인권을 검출해 낼 수 있을 것으로 기대한다. 3장에서는 판독 시스템의 기본적인 구조와 앙상블 딥러닝 신경망에 대해 설명한다.

3.1 판독 시스템

전반적인 판독 시스템의 구조는 (그림 1)과 같다. (그림 1)을 보면 스마트폰을 통해 촬영 또는 앨범의 사진 선택을 통해 이미지를 서버로 전송하는 동시에 제안된 신경망을 통해 판독을 시작하고 출력된 결과를 앱으로 전달한다. 또한 과거의 결과 내역도 다시 볼 수 있다. 판독 신경망은 인공지능



(그림 1) 판독 시스템의 구조

능을 통해 1단계 결과로 대상 물품의 외형과 가장 일치하는 Top-3 디자인 등록번호를 출력하며, 출력된 결과를 다시 웹서버를 통해 스마트폰에 전달한다. 스마트폰은 수신된 결과를 바탕으로 웹서버의 DB를 조회하여 추가적인 정보를 받아 온다. 이 때의 DB는 특허정보검색서비스(키프리스)[9]로부터 디자인권에 명시된 정보들을 찾아 서버의 DB에 저장된 것으로, 필요시 관리자가 추가 및 변경이 가능하며, 이 정보들을 디자인 등록번호와 같이 출력 한다. 1단계 판독 후 특정 디자인권의 도면들과 유사도를 측정하고 싶은 경우 추가적인 2단계 판독을 진행 할 수 있다. 스마트폰에서 촬영된 이미지와 특정 디자인권의 도면들을 웹서버를 통해 판독 신경망에 전달하면 판독 신경망은 추가적인 판독을 진행하여 이에 대한 결과를 제공한다. (그림 1)의 판독 시스템 구조는 대략적인 흐름을 설명하기 위해 작성된 것으로 실제로는 이보다 다

양한 기능들이 있으나 주요 흐름만을 표시한 것이다. 본 연구에서는 이러한 판독 시스템의 핵심 기능인 판독 신경망에 대하여 보다 자세히 설명하고자 한다.

3.2 판독 신경망

판독 신경망은 2단계로 구성되어 있다. 1단계는 현물 이미지로부터 해당하는 Top-N개의 디자인 등록번호 및 유사도를 추출하는 단계로, 본 연구에서는 Top-3까지의 디자인 등록번호를 추출하였으나, 이는 사용자의 요구에 따라 언제든지 변경될 수 있다. 2단계는 특정 디자인 등록번호를 가진 도면 이미지를 현물 이미지와 같이 입력받아 도면과 현물 이미지와의 유사도를 측정하는 단계이다. 유사도는 0 ~ 1 사이의 정규화된 실수 값으로, 1에 가까울수록 해당 디자인권의 디자인이 판독하고

자 하는 이미지와 유사하다는 뜻이고, 0에 가까울 수록 무관하다는 뜻이다.

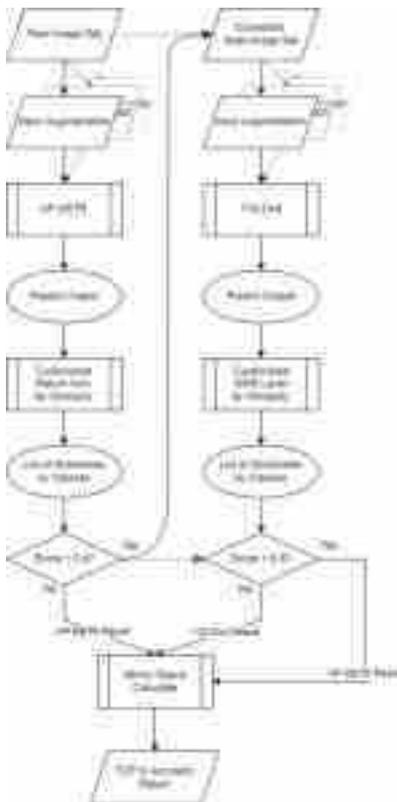
3.2.1 판독 신경망 1단계 모델

판독 신경망 1단계 모델은 다음과 같은 순서로 작동하며 전반적인 흐름은 (그림 2)와 같이 나타낼 수 있고, 다음 7단계의 순서로 작동된다.

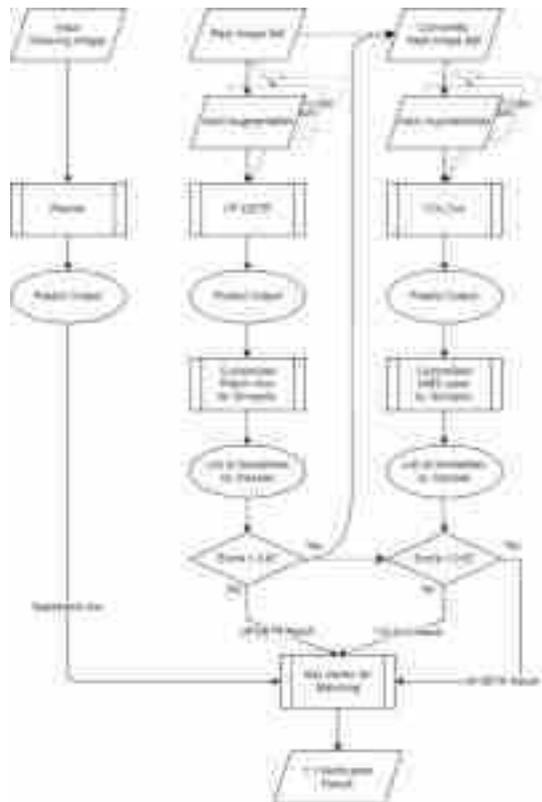
1. 판독 신경망은 판독하고자 하는 실제 이미지 데이터를 1 ~ n개 입력받는다.
2. 입력받은 이미지를 이미지 증강 기술(Input Augmentation)을 통해 입력 이미지 자체를 증강하여 메인 신경망에 전달한다. 본 연구에 사용된 추론 모델의 입력 이미지 증강 기술은 필수로 적용해야 하는 것은 아니며, 내부 실험적

으로 예측 성능의 증가가 있어 방향을 0도, 90도, 180도, 270도씩 돌려 입력 이미지들을 4배 증강하여 사용했다.

3. 메인 신경망은 Unknown 클래스를 포함하는 정확도가 매우 높은 신경망을 사용한다. Unknown 클래스는 배경과 같이 학습할 필요가 없거나 주요 특징이 아닌 부분에 대해 해당 이미지를 모르는 클래스(Unknown Class)의 물건으로 분류하도록 하는 것으로, 학습 클래스에 대해서 해당 클래스의 특징만을 잘 학습할 수 있도록 도와주고, 학습할 필요가 없는 특징은 Unknown 클래스로 예측되게 학습함으로써 클래스를 보다 잘 구별 할 수 있도록 돕는다. 또한 모델의 출력 부분에서 Softmax를 거친 이



(그림 2) 판독 신경망 1단계 모델



(그림 3) 판독 신경망 2단계 모델

후 Unknown 클래스를 제외하여 최종적인 결과를 출력한다. 따라서 기본적으로 Unknown 클래스가 포함된 신경망은 클래스의 합이 1이 아니다. Unknown 클래스는 개별 바운딩 박스에 대해서 학습하지 않은 클래스는 어느 다른 클래스를 가리키지 않게 함으로써 단계적인 신경망 구축 시에 핵심적으로 작동 할 수 있게 한다. 본 연구에서는 Unknown 클래스를 지원하면서도 정확도가 높은 신경망 중에서 특히 우수한 성능을 입증한 객체 탐지 분야의 UP-DETR[3] 신경망을 메인 신경망으로 사용했다.

이 신경망은 DETR(DEtection TRansformer) [10] 신경망을 기반으로 하여 개선된 신경망으로, DETR에 Random Query Patch 기능을 추가한 것이다. DETR 모델은 Backbone을 통해 기본적인 이미지의 특징을 추출하고, 이를 Positional Encoding을 통해 V, K, Q의 형태로 입력의 형태를 바꾸어 Encoder- Decoder Block에 입력으로 사용하는 Attention 기반의 Transformer 모델이다. Random Query Patch는 이미지의 Patch를 무작위로 자른 후 이를 Transformer의 Decoder 부분에 Query Q로 사용하는 것으로, DETR 신경망보다 더 빠르게 수렴이 가능하고 더 높은 정확도를 가졌다. 모델의 학습 과정에서 이미지 증강 기술을 사용하였는데, 이미지의 크기, 각도, 색상, 조도를 일정 범위 내에서 무작위로 변화시키거나, 이미지의 일부를 가리는 등의 기술을 적용했다. 이를 통해 이미지의 일부만 보이거나, 지나치게 어둡거나 혹은 밝아 판독하기 어려운 상황에서도 감지가 가능하도록 하였다. 파라미터는 예측 결과의 클래스 수를 판독하고자 하는 클래스의 수로 변경하고, 200 Epoch 만큼 학습을 진행하였으며, 과적합(Overfitting)을 방지하기

위해 검증 데이터를 기준으로 가장 학습 결과가 높게 나타난 모델을 실험에 사용하였다. 그 외에는 모델의 원래 성능을 정확하게 비교하기 위해 기본 옵션을 적용하였다.

4. 이를 통해 학습된 신경망의 출력을 제안된 유사도 추출 함수를 통해 각 클래스에 대한 유사도를 출력한다. 입력 이미지에 실제로 여러 개의 서로 다른 물건이 입력될 수 있으므로, 유사도 추출 함수는 다음과 같은 수식으로 구성되어 저촉될 수 있는 모든 디자인권 등록번호의 유사도를 출력하였다.

$$Y = \{c_1, \dots, c_n\} \tag{1}$$

$$c_i = \max(X_{I \times B \times C_i}) \tag{2}$$

유사도 함수의 입력으로 사용되는 신경망의 출력 데이터 세트는 3차원 행렬의 형태이며, 그 Shape은 [증강된 이미지(I)의 수, 바운딩 박스(B)의 수, 클래스(C)의 수]와 같이 구성된다. 수식 1의 Y는 유사도 함수의 최종적인 출력 결과를 의미하며, Y의 요소인 c_i 는 수식 2를 통해 계산된다. 수식2의 c_i 는 C_i 차원의 모든 I와 모든 B의 값들 중 최댓값을 출력한다. 이 수식을 통해 해당 이미지에서 검출될 수 있는 모든 디자인권에 대한 최대 유사도를 출력한다.

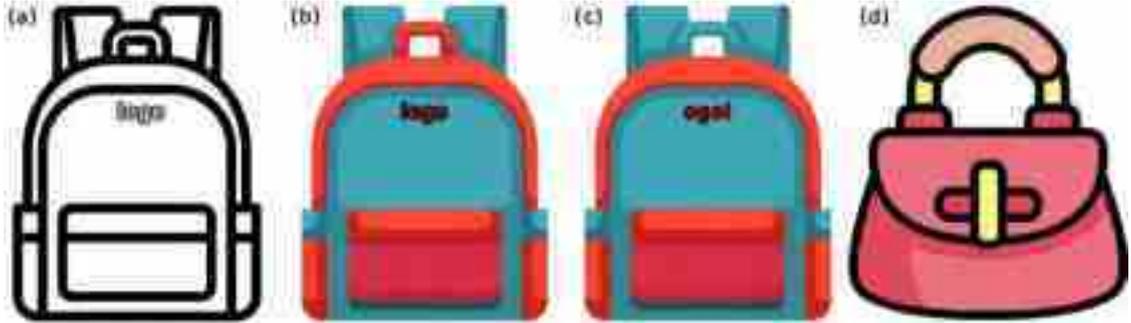
5. 이를 통해 출력된 각 클래스에 대한 유사도를 정렬하고, 가장 높은 Top-1 클래스의 유사도가 하한 임계 0.67보다 낮을 경우, 메인 모델은 기 학습된 디자인 등록번호와 유사하지 않은 것으로 판단한다. 이 때 하한 임계는 실험에 의해 결정된 것으로 4.2.1장의 실험 결과를 통해 결정되었다. 반대로 Top-1 유사도가 하한 임계보다 크거나 같다면 기 학습된 디자인권의 디자인과 유사한 것으로 판단하고 Top-N개의 유사 등

- 록번호와 같이 1단계 모델의 결과로 출력한다.
6. 메인 모델의 Top-1 유사도가 하한 임계를 넘지 못하면, 서브 모델에 대해서 1 ~ 5 번째에서 제시된 순서대로 동일하게 진행한다. 서브 모델은 물건의 수가 언제든 변경될 수 있기 때문에 유사시에 빠르게 학습 될 수 있으면서 정확도가 높은 모델로 선정했다. 여러 분야에서 입증된 YOLOv4[4] 모델은 정확도가 높으면서 빠르게 학습 될 수 있으며, 대표적인 Real-Time Object Detector로 사용될 정도로 모델이 가볍다. 이 모델은 제한된 환경에서 메인 모델과 함께 직/병렬로 연산해도 메모리 문제(Out-of-Memory) 등이 없어 서브 모델로 선정했다. YOLOv4는 제품의 시스템에서 빠른 동작 속도를 확보하기 위해서 연산량 BFLOP(Billion Floating Point Operations)을 줄이기보다는 병렬적으로 최적화된 연산을 가능하게 하는 것을 목표로 개량된 모델이다. 또한 학습 과정에서 1개의 GPU만으로도 높은 정확도와 함께 빠른 학습이 가능한 모델이라는 특징이 있다. 메인 모델에서와 같이 이미지 증강 기술을 적용하였으며, 파라미터도 마찬가지로 판독하고자 하는 클래스 수로 변경하였고, 250 Epoch 만큼 학습을 진행하였다. 이 모델 또한 학습 과정에서 과적합을 방지하기 위해 검증 데이터를 기준으로 가장 학습 결과가 높게 나타난 모델을 실험에 사용했으며, 모델의 원래 성능과 비교하기 위해 기본 옵션을 적용하였다.
 7. 6번째 순서 진행 후 서브 모델의 유사도 추출 함수를 통해 출력된 각 클래스에 대한 유사도를 정렬하고, 가장 높은 Top-1 클래스의 유사도가 만약 하한 임계 0.67보다 낮을 경우 서브 모델은 기 학습된 디자인 등록번호와 유사하지 않은 것으로 판단한다. 따라서 이 때는 다시 신

뢰도가 보다 높은 메인 모델의 결과를 최종적으로 출력한다. 반대로 서브 모델에서 하한 임계보다 Top-1 유사도의 값이 크거나 같을 경우, 기 학습된 디자인권의 디자인과 유사한 것으로 판단하고, Top-N개의 유사 등록번호와 같이 1단계 모델의 결과로 최종 출력한다. 이때의 하한 임계는 메인 모델의 하한 임계와 마찬가지로 실험에 의해 결정된 것으로, 4.2.2장의 실험 결과를 통해 결정되었다.

본 연구에서는 메인 모델과 서브 모델을 구축하여 앙상블을 통해 빠르면서도 정확한 예측을 진행하고자 했다. 2개 이상의 모델을 사용하는 앙상블 모델은 [11]에서 제시된 것처럼 다양한 방법이 있으며, 보통 여러 개의 약한 모델을 생성하고 그 예측을 결합함으로써 보다 정확한 최종 예측을 도출하는 기법이다. 특히 앙상블 방법 중 [12] 등에서 언급된 Voting은 서로 다른 알고리즘을 가진 모델을 병렬(독립적)로 결합하고, 투표를 통해 결과 값을 도출하는 방법이다. 기본적인 Voting은 모든 모델의 결과를 출력하고 이어 붙인 행렬에서 클래스에 따른 평균 혹은 가장 많이 선출된 클래스를 결과로 도출하는 방식이다. 하지만 이 경우 모든 입력에 대해 모든 모델의 결과를 출력해야만 하는 단점이 있기 때문에, 본 연구에서는 임계치를 통한 앙상블 방법을 제안하고자 하며, 메인 모델의 정확도를 최대한 보장하면서 서브 모델이 제한적으로 작동 할 수 있도록 하여 메인 모델의 정확도를 개선시키고자 했다. 또한 메인 모델에서 충분히 높은 신뢰도(유사도)를 가진다면 굳이 모든 서브 모델의 결과를 계산 할 필요가 없으므로 연산 속도가 보다 빠르다는 장점이 있다.

(그림 4)를 보면, (a)는 도면 이미지, (b)는 도면과 일치하는 진품의 현물 이미지라고 하고, (c)는 (b)를 모방한 불법 복제품이고, (d)는 (a)의 디자인



(그림 4) 판독 신경망 입력 이미지들의 예시. (a)~(d)는 다음과 같다. (a)는 도면 이미지, (b)는 도면과 일치하는 현물 이미지, (c)는 불법 복제품, (d)는 무관한 이미지

권과는 전혀 다른 무관한 물건이라고 할 때, 판독 신경망 1단계 모델은 (b) 물건에 대해 학습을 했으므로 입력 이미지로 (b)가 들어올 경우 1에 가까운 유사도와 함께 (b)에 해당하는 디자인 등록번호를 먼저 출력한다. 판독하고자 하는 입력 이미지로 불법 복제품인 (c)를 받을 경우 신경망은 (b)의 디자인 등록번호와 함께 비교적 1과 가까운 유사도를 출력한다. 이를 통해 불법 복제품이 어떠한 기 학습된 디자인권을 가진 물건과 유사한지를 검출할 수 있다. 만약 (d)와 같은 이미지가 주어진다면, (d)는 (b)나 (c)가 유사하다고 나타나는 디자인권과는 전혀 다른 이미지이기 때문에, 해당 클래스의 유사도는 0과 가깝게 출력된다. 만약 별도의 유사한 기 학습된 디자인권 정보가 없다면, 저축된 디자인권이 없다고 판단한다. 본 연구의 신경망은 이러한 방법을 통해 (c)와 같은 물건을 빠르게 감지할 수 있고, (d)와 같이 검사하지 않아도 되는 물건은 빠르게 선별할 수 있다. 이를 통해 불법 복제품인지 아닌지를 판독하는 전문가가 자동 판독 시스템의 정보를 토대로 보다 빠르게 디자인권 소유자의 정보를 찾을 수 있다.

3.2.2 판독 신경망 2단계 모델

판독 신경망의 2단계 모델은 도면의 클래스를

추출하는 과정과 1단계 모델의 결과와 매칭하여 최종 유사도를 측정하는 과정이 추가된 방법이다. 세관에서 특정 도면과 해당 물건 간의 유사도 측정을 위해 사용할 수 있으며, 유사도가 1에 근접하면 도면과 실제 이미지가 같은 디자인 등록번호를 갖거나 정교하게 제작된 불법 복제품이라는 의미이다. 반대로 유사도가 0에 가깝게 나타난다면 이는 도면과 현물 이미지가 서로 다른 디자인 등록번호를 갖거나 전혀 다른 물건이라는 의미를 가진다. 단, 이 때의 유사도는 법적인 관점에서 효력이 있는 절대적인 수치는 아니며, 특정 어느 도면이 가리키는 디자인 등록번호와 해당 물건이 어느 정도 일치하는지를 확인하기 위한 용도이다. 1단계 모델은 Top-N에 대해서만 알 수 있지만, 2단계 모델은 특정한 물건과의 유사도를 비교할 수 있다. 이 신경망 모델의 순서는 다음과 같이 3단계의 순서로 작동하며, 전반적인 흐름은 (그림 3)과 같이 나타낼 수 있다.

1. 도면 이미지를 입력받고 이에 해당하는 디자인 등록번호를 추출한다. 이는 가볍고 단순한 모델로도 충분히 학습이 가능하여 본 연구에서는 Resnet50[5] 신경망을 사용했다. 실험에 사용된 Resnet 신경망은 이미지 분류에 자주 쓰이는 합성곱 신경망 모델로 2015년에 이미 우수한 성능을 보이며 다양한 분야에서 사용되고

있다. 본 연구에서는 기 학습된 Resnet 모델의 Fine Tuning된 모델로부터 전이 학습을 통해 빠르게 학습을 진행했다.

2. 앞서 도면 이미지와 함께 입력받은 현물 이미지를 판독 신경망 1단계 모델의 전 과정인 1 ~ 7의 과정을 동일하게 진행한다.
3. 2번째 순서에서 추출된 유사도 리스트에 대해서 1번째 순서에서 출력된 디자인 등록번호와 매칭되는 유사도를 최종 출력한다. 4.3.1장의 실험 결과에서 이와 관련된 실험을 진행하였다. 실험 결과는 도면과 이미지가 일치 시 예측 정확도 평균은 0.9714로 나타났고, 도면과 이미지가 불일치 시 예측 정확도 평균은 0.0003으로 나타났다.

앞선 (그림 4)를 다시 보면, (a)와 (b) 혹은 (a)와 (c)가 쌍으로 주어졌을 때는 유사도가 1과 가깝게 나타날 것이고, (a)와 (d)가 쌍으로 주어진 경우는 유사도가 0에 가깝게 나타날 것이다. 본 연구의 시스템은 이러한 방법을 통해 특정한 도면 혹은 특정한 디자인권에 대해서 어느 정도의 유사도를 가지는지를 검출 할 수 있다.

4. 실험 결과

이 장에서는 제안된 판독 시스템의 판독 신경망에 대한 실험을 진행한다. 먼저 실험 환경에 대한 설명과 판독 신경망 1단계에서 메인 모델과 서버 모델의 적정 임계에 대한 실험을 먼저 진행한다. 이후 앙상블 전의 개별 모델과의 비교를 통해 제안된 앙상블 모델의 성능을 비교한다. 마지막으로 앙상블 2단계 모델의 일치 유사도 평균 및 불일치 유사도 평균을 측정한다. 이와 함께 각 실험에서 실험에 따른 결과를 설명하고자 한다.

4.1 실험 환경 설정

실험에는 직접 수집한 총 123,480장의 84개 물건에 대한 이미지와 해당 물건과 일치하는 도면 이미지 671장을 사용하여 학습을 진행했다. 실제 이미지 사진은 각 물건마다 학습 데이터로 1,242장씩, 검증 데이터로 138장씩 9 : 1 비율로 나누어 사용했다. 학습 및 검증과는 다르게 별도로 구성된 테스트 데이터는 90장씩 별도로 수집하여 사용했다. 각 데이터는 다양한 조건에 의해 촬영되었는데, 여러 각도, 장소나 배경, 조도, 가림의 정도(최대 절반), 비닐 랩을 통한 포장 유무 등의 조건을 추가하여 데이터를 수집했다. 이를 통해 물건을 알아보기 어려운 각도, 어두운(혹은 밝은) 조도, 어질러진 환경, 비닐로 포장된 상태, 물건의 반이 가려져 어떠한 물건인지 알아보기 어려운 상황에서도 감지가 정상적으로 진행될 수 있도록 하였다. 또한 84종의 물건은 손톱깎이, 가위, 립스틱, 화장품, 이어폰, 응원봉, 인형, 헤어드라이어, 청소기, 자동차 헤드램프, 자동차 휠, 자동차 범퍼에 이르기까지 다양한 크기의 사물에 대해 유사한 다른 물건들을 포함하여 완구문구, 이미용품, 의류, 스포츠용품, 생활가전, IT, 자동차 등의 여러 분야의 물건들로 선정하였다.

도면 데이터는 클래스마다 6~14장의 이미지를 사용했는데, 이는 키프리스 플러스[9]에서 공개하는 데이터로 간단한 회원가입 후 웹기반 REST API를 활용하여 크롤링 및 스크랩을 통해 빠르게 수집 할 수 있다. 먼저 API Key를 요청하여 Key를 받고, Query에 해당 Key 정보를 같이 입력하여 REST API를 통해 크롤링 및 스크랩 방법으로 수집 할 수 있다. 키프리스 플러스 홈페이지에서 디자인 버튼을 누르거나 [메인 > 데이터 목록 > 분류 체계별 > 국내 IP데이터 > 한국공보 > 디자인] 탭에 들어간 후, 디자인 공보 탭 안의 서지정보

탭을 살펴보면 서지상세정보(공공데이터 포털 연계), 한국분류, 국제분류, 형태분류 등의 특허에 대한 다양한 정보들을 출원번호(applicationNumber)를 입력하면 제공받을 수 있다. 분류 정보는 디자인 분류코드 이력 탭에서도 똑같이 출원번호를 통해 조회 할 수 있으며, 디자인 도면의 경우 디자인 공보 탭의 도면/전문 탭 안에 디자인 육면도 탭에서 마찬가지로 출원번호를 입력하면 도면 이미지가 제공되는 http 링크를 통해 제공한다. 해당 링크를 크롤링하여 도면 이미지를 받을 수 있다. 상기 나열한 정보를 제외하고도 다양한 정보를 스크랩할 수 있으나 본 연구에서는 도면 이미지 정보를 학습에 사용하였다.

학습 환경은 다음과 같으며 먼저 학습에 사용된 장비는 Dell EMC DSS 8440으로, 인텔 제온 골드 6248 2.5G 20Core/40Thread CPU가 2개 탑재되어 총 40Core 80Thread로 구성되어 있으며, 16GB RDIMM 3200MT/s RAM이 16개 탑재되어 총 256GB로 구성되어 있고, NVIDIA Tesla V100 32G GPU가 6개 탑재되어 총 192GB의 VRAM으로 구성되었다. 해당 장비에 Ubuntu 18.04.5 LTS 운영체제에서 Docker Container를 통해 학습을 진행하였으며, CUDA 11.4 버전, PyTorch 1.6.0 버전, Torchvision 0.6.0 버전의 라이브러리를 베이스로 학습을 진행하였다.

실험 환경은 다음과 같으며 실험에 사용된 장비는 AMD Ryzen7 3800X CPU 8Core/16Thread CPU 1개와 32GB DDR4 2666MHz(PC4-21300) RAM 2개, NVIDIA 2080 Super 8GB GPU 1개로 구성된 장비에 운영체제와 학습 환경 및 라이브러리는 학습 환경과 동일하게 구성하여 진행했다. 위 실험 환경은 내부 테스트를 위한 실험 환경이다. 실제 서비스가 제공된 환경은 이보다 성능이 낮은 장비로, 인텔 i7-9750H 2.60GHz CPU 1개와 16 GB RAM 1개, NVIDIA T1000 D6

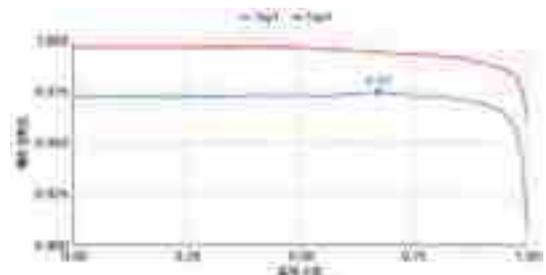
4GB GPU 1개로 구성된 노트북 장비에서 운영체제는 동일하지만 학습 환경은 Container 환경이 아닌 기본 작업 환경에서 위와 동일한 라이브러리를 설치하여 제공하였다.

4.2 앙상블 1단계 모델

4.2.1 메인 모델의 적정 하한 임계

앞서 3.2.1장 판독 신경망 1단계 모델에서 메인 모델의 유사도 출력 함수로부터 Top-1 클래스의 유사도를 하한 임계에 따라 앙상블 모델을 단계적으로 구현하였다. 이 과정에서 유사도의 적정 하한 임계는 다음 실험 결과를 통해 결정되었다.

실험 결과는 (그림 5)와 같이 나타났으며 임계 수준은 0.00에서 1.00까지 0.01단위로 테스트하였다. 임계 수준이 0.00이라 함은 모든 예측 결과를 메인 모델의 결과로만 출력하는 것이고, 1.00이라 함은 모든 예측 결과를 서브 모델의 결과로만 출력하는 것으로 전체 모델에서 서브 모델의 영향력에 따른 정확도로 해석할 수 있다. 임계 수준에 따른 예측 결과를 살펴보면 유사도 Top-1을 기준으로 가장 정확도가 높은 임계 수준은 0.67일 때로 나타났으며, 이 때의 예측 정확도는 0.9749(97.49%)로 나타났다. Top-3의 경우 오히려 임계가 증가할수록 다소 정확도가 떨어지는 추세를 보이고 있지만, 전반적인 추세는 Top-1의 추세와 비슷하게



(그림 5) Main Model 하한 임계에 따른 정확도 비교

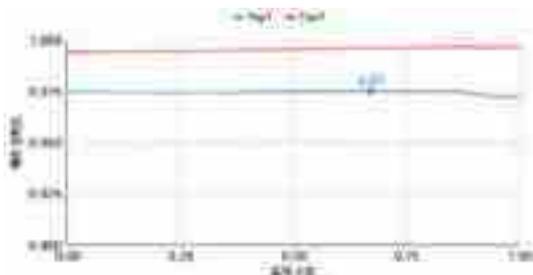
나타나고 있다. 위 실험 결과를 바탕으로 앙상블 모델의 메인 모델 하한 임계는 0.67로 설정하였다.

4.2.2 서브 모델의 적정 하한 임계

앞서 3.2.1장 판독 신경망 1단계 모델에서 서브 모델의 유사도 출력 함수로부터 Top-1 클래스의 유사도를 하한 임계에 따라 앙상블 모델을 단계적으로 구현하였다. 이 과정에서 유사도의 적정 하한 임계는 다음 실험 결과를 통해 결정되었다.

실험 결과는 (그림 6)과 같이 나타났으며 예측 정확도의 범위와 임계 수준의 범위는 모두 위 실험과 동일하다. 또한 이 임계 수준은 4.2.1 실험에서 가장 예측 결과가 높게 나타난 메인 모델의 하한 임계가 0.67로 설정된 상황에서 서브 모델의 하한 임계를 측정하는 것으로, 위 실험과는 반대로 임계 수준이 0.00이라 함은 서브 모델의 예측이 진행되었을 때 모든 예측 결과를 서브 모델의 결과로만 출력하는 것이고, 1.00이라 함은 모든 예측 결과를 메인 모델의 결과로만 출력하는 것이다. 임계 수준에 따른 앙상블 모델의 예측 결과를 살펴보면 유사도 Top-1을 기준으로 가장 정확도가 높은 임계 수준은 메인 모델의 임계와 마찬가지로 0.67일 때로 나타났으며, 이 때의 예측 정확도는 0.9755(97.55%)로 나타났다. 위 실험 결과를 바탕으로 서브 모델의 하한 임계 또한 0.67로 설정하였다.

4.2.1장과 4.2.2장의 실험 결과에 따른 하한 임



(그림 6) Sub Model 하한 임계에 따른 정확도 비교

계는 실험에 의해 결정된 것이지만, 다른 데이터셋을 사용하거나 혹은 다른 메인 모델과 서브 모델로 모델을 변경 할 경우 그에 따라 적정한 값으로 재설정해야 하며, 위 실험 결과에 따른 수치는 대략적인 가이드를 위해 사용 될 수 있다.

4.2.3 앙상블 모델과 선행 모델 비교

〈표 1〉의 실험 결과를 살펴보면 개별 모델보다 앙상블 모델이 Top-1 정확도가 높게 나타나고 있다. 이를 통해 하나의 단일 모델보다 단계적 앙상블 모델을 통해서 예측 성능의 개선이 이루어지고 있음을 알 수 있다. 또한 서브 모델은 예측 성능이 메인 모델에 비해 현저하게 낮게 나타나고 있음에도 불구하고, 앙상블을 통해 예측 성능의 개선 효과를 보여주고 있다. 앙상블 모델에 사용된 메인 모델과 서브 모델은 언제든지 사용자가 원하는 모델로 변경 될 수 있으며, 서브 모델의 경우 단계적으로 여러 모델을 결합 할 수 있다. 또한 이 단계적 결합의 주요 장점은 크게 3가지이다.

첫째, 메인 모델과 같은 클래스의 데이터로 서브 모델을 학습하여 앙상블 시 예측 정확도의 개선을 일으킬 수 있다.

둘째, 서로 다른 클래스를 학습하여 결합 할 수 있다. 즉, 메인 모델은 높은 정확도를 가지지만 학습에 걸리는 Cost가 높으므로, 자주 변하지 않는 클래스에 대해 학습하여 높은 신뢰도를 바탕으로 정기 업데이트를 통해 일정한 주기를 가지고 클래스의 수 변화에 대해 대응 할 수 있고, 서브 모델은

〈표 1〉 기본 모델과 앙상블 모델의 예측 결과 비교

학습 모델	UP-DETR	YOLOv4	앙상블 모델
Top-1 예측 정확도	0.9725	0.9045	0.9755
Top-3 예측 정확도	0.9967	0.9603	0.9964

비교적 낮은 정확도를 가지지만 학습에 걸리는 Cost가 낮으므로, 자주 변하는 클래스에 대해 학습하여 비정기 업데이트를 통해 수시로 긴급하게 업데이트가 가능하므로 클래스의 수가 계속해서 변하는 상황에서 정기/비정기 업데이트를 통해 하나의 서비스로 제공될 가능성이 있다.

셋째, 단독 신경망이 수용 할 수 있는 클래스 수의 한계를 넘어(1,000개 이상의 클래스) 전체 클래스를 단독 신경망 하나로 모두 학습하여 커버 할 수 없는 상황에 다다르면 본 연구의 양상블 모델로 메인 모델을 순차적으로 적용하여 보다 많은 수의 클래스에 대해서도 대응 할 수 있다는 가능성이 있다.

예측 정확도가 개선된 Top-1과는 다르게 Top-3 예측 정확도는 UP-DETR 개별 모델보다 0.0003% 정도 낮게 나타난 것을 볼 수 있다. 실제 테스트 데이터셋에서 0.0003%는 이미지 1~2장 정도에 해당하므로 데이터셋의 크기가 충분하지 않아 나타날 수 있는 예측 오차 정도로 판단된다. 이는 (그림 5)와 (그림 6)에서 나타난 바와 같이 양상블 모델의 Top-3 예측 정확도는 Top-1의 예측 정확도와 비슷한 추세를 가지기 때문에, 충분한 데이터셋에서 Top-1 예측 정확도가 개선되면 Top-3의 예측 정확도도 개선될 수 있을 것으로 기대한다. 실험에 보다 많은 클래스의 물건을 예측에 사용하고자 하였지만, 데이터를 직접 수집해야 하여 수집 과정에 한계가 있어 더욱 많은 클래스의 물건을 학습하지 못해 나타난 한계점은 추후 후속 연구를 통해 개선해 나가고자 한다.

4.3 양상블 2단계 모델

4.3.1 일치 유사도 평균 및 불일치 유사도 평균

판독 신경망 2단계 모델은 도면으로부터 디자

〈표 2〉 양상블 2단계 모델의 유사도

학습 모델	양상블 2단계 모델
도면과 이미지가 일치하는 경우의 예측 정확도 평균	0.9714
도면과 이미지가 불일치하는 경우의 예측 정확도 평균	0.0003

인 등록번호를 추출하여 해당 등록번호와 매칭되는 1단계 모델의 클래스 유사도를 출력하는데, 이때의 유사도에 대한 실험 결과를 살펴보면 표 2와 같다. 표 2의 결과를 통해 기 학습한 디자인권에 대한 디자인 특징이 나타날 경우, 1에 가까운 수치를 출력하고, 기 학습한 디자인권에 대한 디자인 특징이 나타나지 않을 경우, 0에 가까운 수치를 출력하는 것을 알 수 있다. 이는 메인 모델인 UP-DETR이 Unknown 클래스를 포함하여 학습함으로써 클래스의 특징에 따라 학습한 클래스를 정확히 분류하고 모르는 클래스는 Unknown 클래스로 잘 분류하고 있다는 의미로 판단된다. 그러나 학습 품목 중 디자인이 비슷하게 생겼지만 별도의 디자인권 등록번호를 가지는 경우에 메인과 서브 모델에 나누어 배치할 경우 메인 모델에서 학습된 특징에 기반하여 학습한 물건 중 하나로 분류가 될 수 있으므로, 실제로 유사하게 생긴 물건은 하나의 모델에서 학습 할 수 있도록 하는 것을 권장한다.

5. 결 론

불법 복제품은 보다 정교해지고 있고, 이에 따른 피해는 점차 증가하고 있다. 또한 세관에서는 이러한 불법 복제품을 판독하기 위해 전문적인 교육을 받은 사람이 직접 검사를 진행하고 있지만, 이를 모두 직접 판독하기에는 어려움이 많다. 본 연구에서는 불법 복제품을 판독하는 과정에서 보다 빠르게 검사를 진행 할 수 있도록 비파괴 검사

시스템인 불법 복제품 판독 자동화 시스템을 제안 하며, 이를 통해 생산자 및 소비자의 정당한 권리를 보호하고자 하였다.

불법 복제품 판독 시스템의 핵심 기술인 판독 신경망을 인공지능 알고리즘으로 총 2단계의 앙상블 모델을 제안한다. 1단계 모델은 검사하고자 하는 물건 이미지를 입력으로 받아 해당 물건이라 판단하는 디자인 등록번호와 유사도에 대해서 N 개 출력하고, 2단계 모델은 특정한 도면과 해당 물건의 유사도를 출력한다. 1단계 모델은 학습한 디자인권에 대해 Top-1으로 정확히 예측 할 확률 (예측 정확도, 유사도)는 97.55%이며, Top-3로 정확히 예측 할 확률은 99.64%로, 학습한 디자인권 정보에 대해 비교적 정확한 검출이 가능하다. 또한 이 모델은 메인 모델과 서브 모델로 구성된 앙상블 모델로, 메인 모델과 같은 클래스의 데이터로 서브 모델을 학습하여 결합 할 경우 예측 정확도를 개선 할 수 있으며, Unknown 클래스를 통해 각 모델들이 서로 다른 클래스의 데이터를 학습하여도 결합 할 수 있다는 가능성을 통해 클래스의 수가 계속해서 변하는 환경에서도 사용이 가능 할 것으로 기대한다. 그리고 단독 신경망이 수용 할 수 있는 한계 클래스의 수를 넘어(1,000개 이상의 클래스) 단독 신경망으로 전체 클래스를 모두 학습하여 커버 할 수 없는 상황에서도 여러 메인 모델, 여러 서브 모델로 단계적으로 앙상블 모델을 구축하면 다수의 클래스에 대해서도 학습이 가능 할 것으로 기대한다. 또한, 해당 시스템은 공개된 빅데이터를 웹에서 크롤링하여 활용한다. 크롤링을 통해서 수집된 데이터를 통해 정확도의 개선 등에 있어서 도움이 되었으며, 크롤링을 통한 학습 데이터의 확보 없이는 본 시스템이 개발, 운영 되기는 어렵다.

이후 연구는 보다 많은 메인 모델과 서브 모델을 결합하거나, 서로 다른 클래스를 학습한 모델

들을 결합하여 예측 정확도의 개선 혹은 수많은 클래스에 대해 예측 할 수 있도록 하는 가능성을 확인하기 위한 연구를 진행하고자 한다. 하지만 본 연구에서 직접적으로 다른 클래스를 학습한 모델과 결합하지는 않았기 때문에 이는 후속 연구를 통해 개선하여 구체적인 방법론을 제시하고자 한다. 또한 많은 클래스를 학습하는 환경에서도 이러한 Unknown 클래스를 추가하여 이종 모델의 앙상블을 통한 결합으로 정확도의 개선이 가능한지 또한 후속 연구를 통해 개선하여 구체적인 방법론을 제시하고자 한다.

참 고 문 헌

- [1] Organisation for Economic Co-operation and Development, & Kazimierczak, M. (2016). Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact. OECD Publishing.
- [2] Kim, J. G., Seo J. Y., Lee C. J., Jo S. M., Kim S. M., Yoon S. M. & Yoon Y.. (2022). Detecting Design Infringement Using Multi-Modal Visual Data and Auto Encoder based on Convolutional Neural Network. Journal of Computer Science and Engineering, 49(2), (137-144).
- [3] Dai, Z., Cai, B., Lin, Y., & Chen, J. (2021). Up-detr: Unsupervised pre-training for object detection with transformers. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 1601-1610).
- [4] Bochkovskiy, A., Wang, C. Y., & Liao, H. Y. M. (2020). Yolov4: Optimal speed and accuracy of object detection. arXiv preprint arXiv:2004.10934.
- [5] He, K., Zhang, X., Ren, S., & Sun, J.

(2016). Deep residual learning for image recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 770-778).

[6] Kumar, S. N., Singal, G., Sirikonda, S., & Nethravathi, R. (2020, December). A novel approach for detection of counterfeit Indian currency notes using deep convolutional neural network. In IOP Conference Series: Materials Science and Engineering (Vol. 981, No. 2, p. 022018). IOP Publishing.

[7] Lee, S. H., & Lee, H. Y. (2018). Counterfeit bill detection algorithm using deep learning. Int. J. Appl. Eng. Res, 13, 304-310.

[8] Daoud, E., Vu, D., Nguyen, H., & Gaedke, M. (2020). ENHANCING FAKE PRODUCT DETECTION USING DEEP LEARNING OBJECT DETECTION MODELS. IADIS International Journal on Computer Science & Information Systems, 15(1).

[9] <https://plus.kipris.or.kr/>

[10] Carion, N., Massa, F., Synnaeve, G., Usunier, N., Kirillov, A., & Zagoruyko, S. (2020, August). End-to-end object detection with transformers. In European conference on computer vision (pp. 213-229). Springer, Cham.

[11] Zhang, C., & Ma, Y. (Eds.). (2012). Ensemble machine learning: methods and applications. Springer Science & Business Media.

[12] Zhou, Z. H. (2012). Ensemble methods: foundations and algorithms. CRC press.

저 자 약 력



이 찬 재

이메일 : arisel117@gmail.com

- 2019년 홍익대학교 도시공학전공 (학사)
- 2021년 홍익대학교 인공지능·빅데이터전공 (석사)
- 2021년~현재 넷코아테크 미래기술전략연구소 연구원
- 관심분야: 머신러닝, 빅데이터, 컴퓨터 비전, 네트워크, 대형 그래프, 스마트시티



정 성 호

이메일 : wjdtjdgh2005@gmail.com

- 2021년 인천대학교 수학과 (학사)
- 2021년~현재 넷코아테크 미래기술전략연구소 연구원
- 관심분야: 머신러닝, 빅데이터, 컴퓨터 비전



윤 영

이메일 : young.yoon@hongik.ac.kr

- 2003년 University of Texas at Austin 컴퓨터과학과 (학사)
- 2006년 University of Texas at Austin 컴퓨터과학과 (석사)
- 2012년 University of Toronto 컴퓨터공학과 (박사)
- 2015년~현재 홍익대학교 컴퓨터공학과 조교수
- 관심분야: 분산컴퓨팅, 미들웨어, 인공지능