DenseNet 을 통한 얼굴 스푸핑 탐지 기술

김소의 [1], 유수경 [1], 이의철 [1,*]
[1] 상명대학교 휴먼지능정보공학전공
soeui291@gmail.com, tnrud7495@gmail.com
*Corresponding author: eclee@smu.ac.kr

Face spoofing detection using DenseNet

So-Eui Kim, Su-Gyeong Yu, Eui Chul Lee
Dept. of Human Centered Artificial Intelligence, Sangmyung University

요 약

얼굴을 이용한 신원인식 방법은 높은 사용 편의성과 보편성 때문에 다양한 분야에서 활용되고 있다. 그러나 타인의 얼굴 사진이나 테블릿 PC 를 통한 얼굴 동영상 재생과 같은 손쉬운 방법을 통한 얼굴 스푸핑 공격 사례가 다수 보고되고 있다. 하지만 기존의 영상의 텍스처 특징을 활용한 방법은 영상의 초점 상태에 취약하고 기계학습에 사용된 데이터에 의존적이다. 따라서 보다 강력한 스푸핑 탐지 기술이 필요하다. 본 연구에서는 다양한 각도와 거리 편차 요소를 포함하는 자체 구축 DB 와 DenseNet 을 활용한 딥러닝 기반의 위조 얼굴 검출 기술을 연구했다.

1. 서론

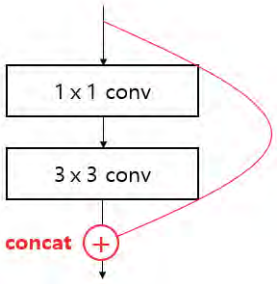
오늘날 생체 인식은 보다 안정적이게 발전했다. 여러 생체 인식 방법 중 얼굴 인식 시스템은 편리하며 거부감이 낮은 방법 중 하나이다. 하지만 지난 몇 년간 스푸핑 공격과 같은 생체 인식 시스템의 잠재적 취약점이 다수 보고됐다 [1]. 따라서 얼굴 인식의 안전성을 보장하기 위해 보다 정확한 얼굴 인식 시스템 개발이 요구되고 있다.

기존의 연구에서는 LBP, DCT, SVM 을 이용해 얼굴 스푸핑 공격을 탐지했다 [2]. 이러한 방식들은 고수준 특징인 질감을 기반으로 한다 [3]. 그러나 질감 정보는 영상의 초점, 해상도에 따라 유의미한 동작을 하지 못할 수 있다. 또 기존의 연구에서 사용된 대부분의 공개 DB 들은 거리, 각도 편차에 대한 정보가 담겨있지 않다.

본 논문에서는 이러한 문제점을 해결하고자 CNN 기반의 신경망 모델인 DenseNet-121 을 통한 얼굴 스푸핑 공격 탐지 기술을 연구했다. 연구에 사용한 DB 는 거리, 각도와 같은 차별화된 특성을 가지는 PR-FASD 이다 [4].

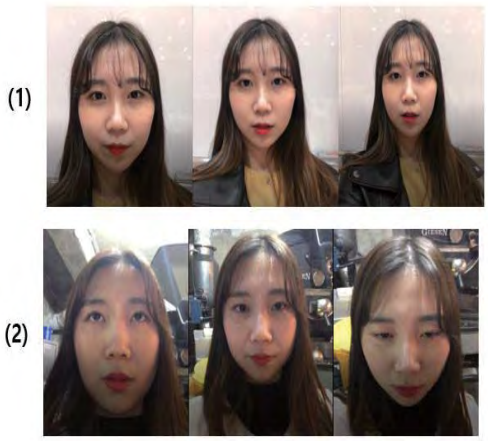
2. 본론

기존에 사용되던 기계학습 모델에서는 사람이 구현한 프로그램에 의해 추출된 특징을 이용하여 학습하였다. 반면 DenseNet-121 은 신경망 모델 중 하나로 입력 데이터의 특징을 스스로 추출하고 학습한다. 이때, Densely connection 을 기반으로 하여 layer 의 feature map 을 계속해서 다음 layer 의 입력과 Concatenation 한다. 즉, concatenation 연산을 이용해 이전 layer 의 정보가 다음 layer 의 출력에 연결됨으로써 최초의 정보가 마지막까지 반영되는 것이다. 이를 통해 기존의 신경망모델에서 나타났던 degradation 문제와 Vanishing-gradient 문제를 개선했다[5]. (그림 1)은 Densnet-121 모델의 구조를 나타낸다.



(그림 1) DenseNet-121 신경망 모델 방식.

연구에 사용한 DB 는 고정되지 않은 배경과 조명, 3 가지의 거리(near, halfway, distant), 그리고 3 가지의 각도(bottom, middle, top)라는 차별화된 특성을 가지는 PR-FASD 이다. 이 DB 에는 30 명(남성: 19 여성: 11)의 실제 얼굴 영상과 스푸핑 공격 방지를 위한 인쇄된 사진과 재생 비디오를 촬영한 가짜 얼굴 영상이 있다. PR-FASD 의 예시는 (그림 2)에서 볼 수 있다.



(그림 2) PR-FASD 얼굴 이미지 예시 (1): 3 가지 거리, (2): 3 가지 각도.

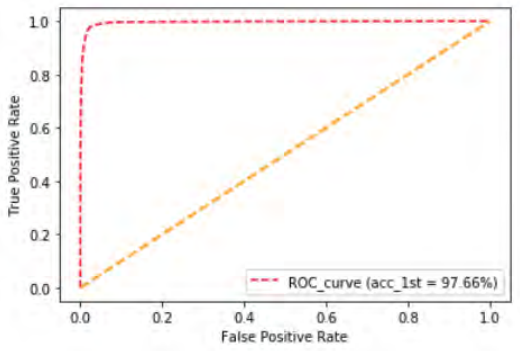
3. 실험 및 결과

본 논문에서는 PR-FASD 데이터베이스를 학습, 검증, 테스트 데이터로 이용하였다. 신경망 모델인 Densnet-121 의 입력으로 들어온 얼굴 이미지는 7×7 크기의 convolution filter 64 개를 사용하여 학습되었으며, 이 과정에서 1×1 및 3×3 convolution filter 로 이루어진 Dense Block 은 총 4 개로 구성되어졌다. 각각의 feature map 의 depth 는 128, 256, 512, 1024 으로 2 배씩 증가하였으며, 이때 stride=2, epoch=100 으로 지정하였다. 학습과정에서 Binary cross entropy 를 손실함수로, 확률적 경사 하강법을 최적화함수로 사용하였으며 learning rate 은 0.001 이였다. 또한, 과적합 등의 문제를 방지하기 위해 학습과정에서 검증데이터를 추가적으로 이용하였다.

얼굴 스푸핑 공격 검출 성능 결과 확인 지표로 Half Total Error Rate(HTER)과 정확도를 사용하였다. HTER 은 값이 작을수록 성능이 좋은 것으로 오분류의 비율 만을 이용한 값이다. Equal error rate(EER)은 False Rejection Rate(FRR)과 False Acceptance Rate(FAR) 값의 동일한 비율을 말하며 값이 낮을수록 좋은 성능을 나타낸다. 최종 학습된 모델을 사용하여 테스트 얼굴데이터를 분류한 결과로 HTER, EER 은 각각 2.34, 2.85 로 아래 <표 1>과 같다. 얻어진 결과는 Receiver Operating Characteristic(ROC) 곡선을 이용하여 시각화 되었다. ROC 곡선은 False Positive Rate(FPR)과 True Positive Rate(TPR)을 각각 x, y 축으로 놓은 그래프로 ROC 곡선의 밑면적인 Area Under the Curve(AUC)의 넓이가 넓을수록 분류 모델의 성능이 좋음을 나타낸다. 분류성능에 대한 ROC 곡선은 (그림 3)에서 볼 수 있다. 결과적으로 PR-FASD 를 이용한 위조 얼굴 검출에 대한 Densenet-121 의 분류 정확도는 97.66%로 매우 뛰어났다. 비교를 위해 추가적으로 수행한 SVM 모델의 정확도는 92.26%로 비교적 저조한 성능을 보였다. Densnet-121 모델은 concatenation 을 통해 이미지의 저수준 특징을 깊은 layer 까지 보존 가능한 구조를 가지고 있다. 이는 고수준 특징만 사용되고 나머지는 버려졌던 기존 모델들과는 다르게, 저수준 특징까지도 분류 과정에 사용한다. 따라서 기존 방식보다 위조 얼굴 검출에 있어서 유효성을 가진다고 할 수 있다.

<표 1> DenseNet-121 분류 성능 결과

구 분	HTER	EER
PR-FASD	2.34	2.85



(그림 3) DenseNet-121 모델의 ROC 곡선.

추후, Densenet-121 과 더불어 이진 분류를 위해 유용하게 이용되는 신경망 모델인 Resnset-18 을 이용한 위조 얼굴 분류 검출을 할 예정이다. 또한 두 모델의 결과 비교를 통해 이미지의 저수준 특징 반영이 위조 얼굴 검출 성능에 유효한 영향을 미치는가에 대한 연구를 진행할 계획이다.

참고문헌

[1] Biggio, B., Akhtar, Z., Fumera, G., Marcialis, G. L., & Roli, F. Security evaluation of biometric authentication systems under real spoofing attacks. IET biometrics, 1(1), 11-24, 2012.

[2] TIAN, Ye; XIANG, Shijun. Detection of video-based face spoofing using LBP and multiscale DCT. In: International Workshop on Digital Watermarking. Springer, Cham, 16-28, 2016.

[3] MÄÄTTÄ, Jukka; HADID, Abdenour; PIETIKÄINEN, Matti. Face spoofing detection from single images using micro-texture analysis. In: 2011 international joint conference on Biometrics (IJCB). IEEE, p. 1-7, 2011.

[4] BOK, Jin Yeong; SUH, Kun Ha; LEE, Eui Chul. Verifying the Effectiveness of New Face Spoofing DB with Capture Angle and Distance. Electronics, 9.4: 661, 2020.

[5] HUANG, Gao, et al. Densely connected convolutional networks. In: Proceedings of the IEEE conference on computer vision and pattern recognition, 4700-4708, 2017.