# StyleGAN2-ADA로 증강한 데이터를 이용한 사용자 인증

오유진*, 임세진**, 서화정*†

*한성대학교 (대학생)

**한성대학교 (대학원생)

*† 한성대학교 (교수)

# User authentication using data augmented with StyleGAN2-ADA

Yu-Jin Oh* ,Se-Jin Lim** ,Hwa-Jeong Seo*†

*Hansung University(student)

**Hansung University(Graduate student)

*† Hansung University(Professor)

**요 약**

인공지능 모델은 대량의 데이터 셋을 요구한다. 사용자 얼굴 인식을 통해 인증을 수행하는 모델의 경우 한 사람당 이미지를 대량으로 수집해야 한다. 이를 사람이 일일이 하는 것은 쉽지 않다. 본 논문에서 제안하는 것은 이를 StyleGAN2-ADA를 이용해 데이터를 증강하고 증강된 데이터로 사용자 인증을 하는 시스템이다. 한 사람의 이미지를 pre-trained된 StyleGAN2-ADA를 이용하여 머리색, 표정 등을 다양한 스타일로 바꾸어 데이터를 증강한다. 증강된 데이터로 FaceNet을 학습하고 학습된 FaceNet을 통해 사용자 얼굴을 인증한다.

## I. 서론

대부분의 인공지능 모델은 적은 데이터 셋으로 학습하면 과적합이 발생하거나 매우 낮은 정확도가 나와 수만에서 수십만 장 정도의 대량의 데이터 셋을 요구한다. 그러나 구할 수 있는 데이터 셋에는 한계가 있다. 만약 사용자 얼굴 인증을 할 때, 한 사람의 이미지를 수집할 경우 여러 장 촬영해야 한다. 이마저도 같은 모습으로만 촬영한다면 그 이미지에 대한 과적합이 발생하여 다른 구도, 여러 모습의 이미지가 필요하다. 이러한 이유로 사람이 데이터 셋을 일일이 만들고 증강하는 것은 다소 어렵다. 현재 rotation, crop 등 여러 증강 기법이 있지만, 본 논문에서는 이를 헤어스타일, 악세사리 착용 여부 등 사람의 스타일을 바꾸어주는 StyleGAN2-ADA을 데이터 증강에 사용한다. 이를 통해 데이터를 증강하고 증강된 데이터로 사용자 인증을 하는 얼굴 인식 시스템을 제안한다.

## II. 관련 연구

### 2.1. 생성적 적대 신경망 (Generative Adversarial Network, GAN) [1]

생성적 적대 신경망은 정답이 주어지지 않은 상태에서 데이터의 특징을 스스로 학습하는 알고리즘인 비지도 학습으로, 생성 모델(Generator)과 분류 모델(Discriminator)로 구성되어있다. 생성 모델은 분류 모델을 속이기 위한 가짜 이미지를 생성하고 분류 모델은 주어진 이미지의 진위를 판별하는 모델로 두 모델의 경쟁을 통해 생성 모델은 판별모델의 확률값이 0.5에 해당하는 진짜와 매우 유사한 가짜 이미지를 생성한다. 이러한 GAN을 활용한 데

이터 증대, 이미지 복원 등의 연구가 진행되고 있으며 의료 산업이나 제약산업 등 여러 분야에서도 활용되고 있다.

### 2.2 StyleGAN

StyleGAN은 2018년 NVDIA 연구원이 개발한 모델로 생성 모델의 구조를 Style transfer에 기반하여 만든 모델이다[2]. 생성 모델의 각 레이어에 스타일 정보를 더하는 방식으로 이미지를 생성한다. 그러나 StyleGAN은 물방울 무늬 노이즈가 생기는 droplet artifacts와 얼굴 전반적인 스타일이 변화하는 것이 아닌 얼굴 특정 부분이 고정된 위치를 갖는 phase artifacts가 흔히 발견된다는 단점이 있다. StyleGAN2는 이 단점을 개선했다. 생성 모델의 정규화(normalization)를 변경하여 droplet artifact 문제를 해결하고 저해상도부터 학습하여 고해상도로 높여가는 progressive growth를 제거하여 phase artifacts 문제를 해결하였다[3].

#### 2.2.1 StyleGAN2-ADA [4]

생성적 적대 신경망은 적은 데이터로 학습을 하면 판별모델이 과적합 된다는 한계점이 있다. 판별모델이 과적합 되면 생성 모델 또한 발산한다. 과적합 문제를 해결하기 위해서는 rotation, noise 추가 등 기존 데이터 증강과 같은 해결법이 있지만 이러한 방식도 생성적 적대 신경망 기반 모델에서 적용하면 증강누출(augmentation leaking)이 생긴다. 증강누출을 해결하기 위해 StyleGAN2-ADA는 Adaptive Discriminator Augmentation 알고리즘을 사용한다. Adaptive Discriminator Augmentation(ADA)은 증강된 데이터만 사용하여 판별모델과 생성 모델을 학습시키고 과적합 정도에 따라 증강확률을 동적으로 조절하여 증강누출이 생기지 않는다. 이로 인해 과적합 되는 것을 막아 적은 데이터로도 학습이 가능하다.

### 2.3. FaceNet [5]

FaceNet은 google에서 개발한 얼굴 인식 시스템이다. 얼굴 이미지를 각각 128차원으로 임베딩하고 유클리드 공간에서 이미지 간의 거리에 따라 분류하는 모델이다. 얼굴 이미지에서 특징값을 구해, 값들 간의 거리를 통해 이미지를 식별한다. 같은 인물일수록 이미지 간의 거리가 가깝고 다른 인물이면 거리가 멀다. FaceNet은 Triplet 손실함수를 사용하여 특징을 학습하는 Metric을 학습한다.

## III. 시스템 제안

본 논문에서는 StyleGAN2-ADA를 이용하여 사용자 얼굴 이미지를 증강하고 증강한 이미지를 얼굴 식별에 활용하는 사용자 인증 시스템을 제안한다. 사람은 시간에 따라 헤어 스타일이나, 표정, 악세사리 착용 여부 등 스타일이 바뀌는데 이 점에 착안하여 StyleGAN2-ADA를 이용하여 데이터를 증강한다.

### 3.1 시스템 구조

아래 그림 1은 시스템 구조이다. 해당 시스템은 StyleGAN2-ADA를 거쳐 사용자 얼굴의 이미지를 다양한 스타일 데이터로 증강하는 단계, 증강된 데이터로 FaceNet을 학습시키는 단계, 학습된 FaceNet으로 사용자를 식별하는 단계로 구성된다.

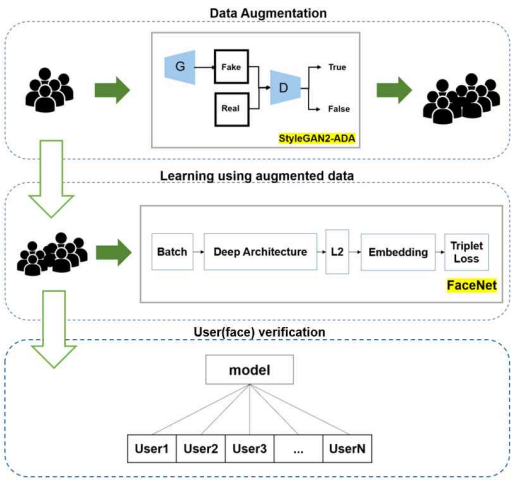


그림 1 . 사용자 인증 절차

각 단계에 대해서 더 자세히 설명한다. 먼저

데이터 증강 단계에서는 StyleGAN2-ADA를 사용한다. StyleGAN2-ADA는 생성 모델을 Style transfer에 기반하여 구성하였고 ADA알고리즘으로 수천 장의 적은 데이터로도 학습할 수 있다. 이 StyleGAN2-ADA를 이용하면 사용자의 머리색, 안경 유무, 입술 색 등을 바꾸어 다양한 스타일의 이미지를 얻을 수 있다. 먼저 여러 스타일의 데이터 셋을 수집하여 StyleGAN2-ADA를 학습시킨다. 학습된 모델에 사용자 얼굴 이미지를 입력하게 되면 그림 2와 같이 사용자의 스타일이 변화된 데이터를 얻게 된다. 그 중 성별이나 전체적인 스타일을 바꾸는 것이 아닌 미세한 부분을 바꾸기 위해 색상적인 측면이나 가장 세밀한 부분을 담당하는 fine Style을 적용한다. 이러한 방식으로 데이터를 증강하고 증강된 데이터로 FaceNet을 학습시킨다. 학습된 FaceNet을 사용하여 사용자의 얼굴을 식별하게 된다.

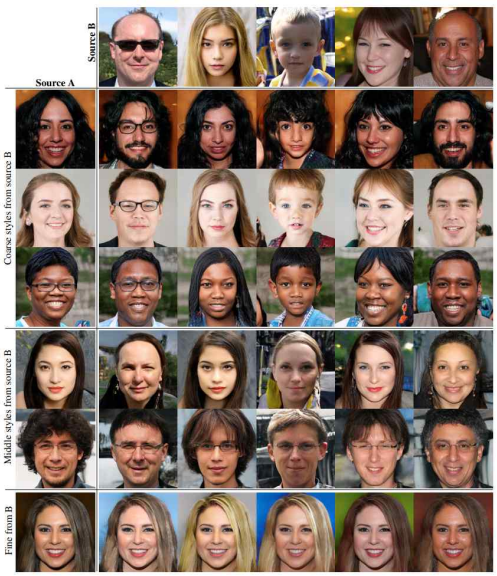


그림 2. 다양한 Style의 이미지[2]

### 3.2 시스템 동작

사용자 인증 절차는 그림 3과 같다. 사용자는 자신의 얼굴 이미지를 등록한다. 등록된 이미지는 제안된 모델을 통해 다양한 스타일 이미지로 증강되고 FaceNet을 학습시킨다. 이러한 절차를 거쳐 최종적으로 사용자가 등록된다. 사용자는 학습된 FaceNet을 통해 본인을 인증한다. 전체 사용자 중 해당하는 사용자 이름이 있을 경우 본인 인증이 완료되고, 해당하는 사용자가 없을 경우 처음으로 돌아가 얼굴을 새로 등록하게 된다.

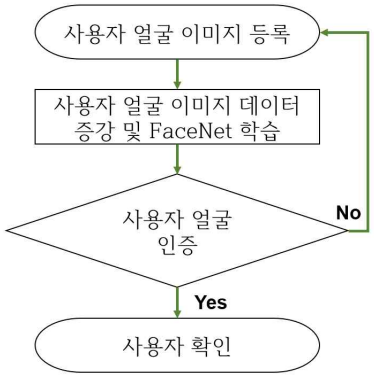


그림 3. 사용자 인증 절차

## IV. 결론

본 논문에서는 StyleGAN2-ADA를 이용한 데이터 증강과 증강한 데이터로 학습시킨 FaceNet으로 사용자 인증 시스템을 제안하였다. 사람마다 시간에 따라 다양한 스타일의 모습을 갖게 되는데 이를 매번 촬영하여 데이터를 수집하는 대신 StyleGAN2-ADA를 통해 해결하였다. StyleGAN2-ADA를 활용하여 사용자 인증에 필요한 이미지 데이터양을 충분히 수집하는데 소요되는 시간 및 비용적인 측면에서의 효율성을 높이고 부족한 데이터 한계를 극복할 수 있다. 향후 시스템 구현을 통해 시험에서 사람의 도움 없이 본인 확인과 안면 인식 도어락 등 사용자 인증이 필요한 다양한 분야에서 사용될 수 있을 것으로 기대할 수 있다.

## V. Acknowledgement

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services, 100%).

## [참고문헌]


[1] Goodfellow, Ian J., et al. "Generative Adversarial Nets." stat 1050 (2014): 10.

[2] Karras, Tero, Samuli Laine, and Timo Aila. "A style-based generator architecture for generative adversarial networks." Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2019.

[3]Karras, Tero, et al. "Analyzing and improving the image quality of stylegan." Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2020. URL: https://www.gartner.com/doc/2487216/definition-threat-in-telligence

[4] Karras, Tero, et al. "Training generative adversarial networks with limited data." Advances in Neural Information Processing Systems 33 (2020): 12104-12114.

[5] Schroff, Florian, Dmitry Kalenichenko, and James Philbin. "Facenet: A unified embedding for face recognition and clustering." Proceedings of the IEEE conference on computer vision and pattern recognition. 2015.