산업융합연구 제17권 제3호 pp. 23-29, 2019
ISSN 2635-8875 / e-ISSN 2672-0124
https://doi.org/10.22678/JIC.2019.17.3.023

사용자 인증을 위한 딥러닝 기반 얼굴인식 기술 동향

문형진[1], 김계희[2*]
[1]성결대학교 정보통신공학과 교수, [2]경남과학기술대학교 컴퓨터 메카트로닉스 공학과

A Survey on Deep Learning based Face Recognition for User Authentication

Hyung-Jin Mun[1], Gea-Hee Kim[2*]
[1]Professor, Dept. of Information & Communication Engineering, Sungkyul University
[2]Researcher, Dept. of Computer Science & Engineering, Gyeongnam National University of Science and Technology

요 약 차이가 나는 물체를 구별하는 물체인식과 달리, 얼굴인식은 유사한 패턴을 가진 얼굴의 Identity를 구별한다. 이에 따라 LBP, HOG, Gabor과 같은 특징 추출 알고리즘이 딥러닝 기반으로 대체되고 있다. 딥 러닝 기술을 활용하여 머신러닝으로 얼굴을 식별할 수 있는 기술이 발전하면서 다양한 분야에서 얼굴인식 기술이 활용되고 있다. 특히, 금융거래 외에도 사용자 식별이 필요한 다양한 오프라인 환경에서 활용되어 세밀하고 개인에 적합한 서비스가 제공될 수 있다. 얼굴 인식 기술은 스마트 미러와 같은 장치를 통해 손쉽게 사용자 인증을 하고, 식별이 된 사용자에게 서비스를 제공할 수 있는 기술로 발전할 수 있다. 본 논문에서는 사용자 인증의 다양한 기법 중에서 얼굴인식 기술에 대한 조사 및 파이썬으로 작성된 얼굴인식 사례 소스 분석과 얼굴인식 기술을 활용한 다양한 서비스의 가능성을 제시하고자 한다.

키워드 : 얼굴인식, 사용자인증, 딥러닝, 인증, 다중 인증

Abstract Object recognition distinguish objects which are different from each other. But Face recognition distinguishes Identity of Faces with Similar Patterns. Feature extraction algorithm such as LBP, HOG, Gabor is being replaced with Deep Learning. As the technology that identify individual face with machine learning using Deep Learning Technology is developing, The Face Recognition Technology is being used in various field. In particular, the technology can provide individual and detailed service by being used in various offline environments requiring user identification, such as Smart Mirror. Face Recognition Technology can be developed as the technology that authenticate user easily by device like Smart Mirror and provide service authenticated user.

In this paper, we present investigation about Face Recognition among various techniques for user authentication and analysis of Python source case of Face recognition and possibility of various service using Face Recognition Technology.

Key Words : Face Recognition, User Authentication, Deep Learning, Authentication, Multi-Factor Authentication

1. 서론

4차 산업혁명시대가 도래하면서 기반 기술인 인공지능, 사물인터넷 등의 발달은 더 많은 사용자 인증이 요구되어 지고 있다. 보안 서비스로서 사용자 인

*Corresponding Author : 김계희(jenni7@naver.com)
Received August 21, 2019 Revised September 17, 2019
Accepted September 20, 2019 Published September 30, 2019

증은 비대면 시스템에서 상대방의 신원을 확인할 수 있는 수단으로 ID/PS 기반의 인증이 보편적으로 사용되고 있었지만 안전성과 편리성이라는 측면에서 생체인증기술이 최근 이슈가 되고 있다. 하지만 생체인증 기술이 안전한 인증을 담보하지 않기 때문에 이중인증(Multi-Factor Authentication)의 하나의 요소로 활용되고 있다[1, 2]. 하지만 딥러닝 기술을 통해 생체인증의 False negative 나 False positive 문제를 해결하여 추가적인 인증수단의 요구없이 인증이 가능해지고 있다. 생체인식은 생체 정보 즉 지문, 홍채, 손등 정맥, 망막, 손글씨, 얼굴, 음성 등을 사용하여 개인 식별을 의미한다. 최근 스마트 폰에 사용자 식별을 위해 생체인식 기술은 지문이나 얼굴인식 등이 활용된다.

최근 얼굴인식을 이용한 생체인식 기술들이 사용자 편리성면에서 탁월한 인식 기술로 활용되고 있다. 얼굴인식은 다른 생체인식보다 사용자로 하여금 일정한 동작을 요구하지도 않고, 비접촉으로 쉽게 확인할 수 있기 때문이다. 경쟁력이 있는 얼굴인식기술은 다양한 분야에서 활용이 가능하다[3].

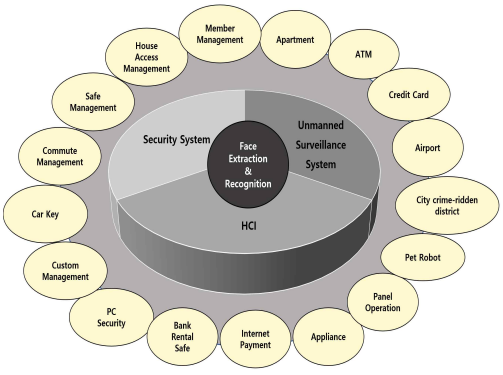


Fig. 1. Area of Face recognition Applications[3]

얼굴인식 기술은 카메라를 통해서 영상들을 입력받으면 영상을 시스템의 데이터베이스에 있는 정보와 비교하여 구별하는 기술이다. 초기의 얼굴인식 기술은 출입통제 시스템이나 접근 권한을 제어하는 수준에 활용되었지만 미국의 911 테러 이후 출입국 보안 관리 및 공공장소에서 CCTV 카메라를 활용하여 감시하고, 분석하는 연구가 진행되고 있다[4, 5].

본 논문은 사용자 인증 기법으로 딥러닝기반의 얼굴인식 기술 분석을 하고자 한다. 다음 장에서는 관련 연구를 소개하고, 3장에서는 얼굴인식 기술을 살펴보고, 4장에서는 얼굴인식 기술 사례 분석 및 논의를 하고, 5장에서는 결론 및 향후 연구를 기술한다.

2. 관련 연구

2.1 사용자 인증

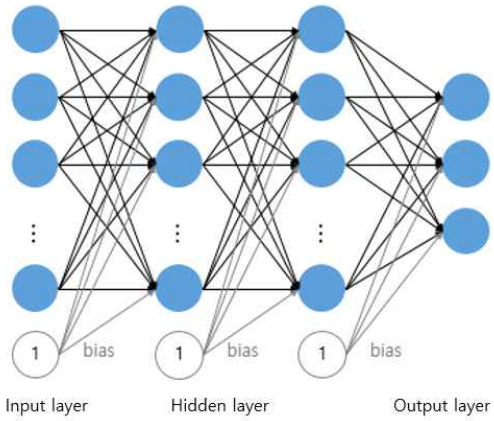
사용자 인증은 시스템에 접속한 사용자를 식별하는 보안 서비스로서 개인 맞춤형 서비스를 제공하기 위해 시스템에서는 등록된 사용자인지, 서비스를 제공받을 권한이 있는 지를 확인하는 절차이다. 대부분의 시스템에서는 편리성 때문에 사용자 인증에 아이디를 이용하여 인증을 실시한다. 최근 스마트 폰에 다양한 하드웨어가 내장되어 지문인증, 홍채인증, 얼굴인식 등 다양한 생체인증정보를 통해 사용자 인증을 실시한다[6].

생체인증을 통한 사용자 인증하는 과정에서 오탐(False Positive)과 미탐(False Negative)가 존재하기 때문에 하는 다중 인증을 요구한다. 다중 인증은 하나의 인증 수단으로 사용자 인증을 하는 것이 아니라 추가적인 인증수단을 적용하여 임계치를 넘을 경우 인증을 완료한다. 아이디로 1차 인증한 후 2차 인증으로 생체인증이나 사용자의 글 쓰는 패턴 등으로 사용자을 식별할 수 있다[7].

2.2 딥러닝

딥러닝은 여러 비선형 변환기법의 조합으로 높은 수준의 추상화를 시도하는 기계학습 알고리즘으로 사람의 사고방식을 컴퓨터에 적용한 기계학습의 한 분야이다. 즉, 딥러닝은 주어진 문제를 해결하기 위해 사람의 개입 없이 데이터를 통해 컴퓨터가 패턴인식 또는 특징적 학습을 하여 스스로 문제를 해결할 수 있는 기계학습 기술이다. 인간의 뇌가 뉴런들 간의 연결이 깊은 구조를 가진 것처럼 입력과 출력 사이에 여러 개의 레이어를 연결하여 진보된 학습과 추론에 대한 인공신경망 기법을 적용한 기술이다[8].

딥러닝 학습은 입력 값을 통해 모델을 학습하는 과정으로 피드포워드 과정과 백 프로파케이션 과정의 반복을 통해 출력 값과의 오차를 줄이는 방식으로 학습을 수행한다(Fig. 2).



(출처 : https://wikidocs.net/24958)

Fig. 2. Architecture of Deep Learning Model

딥러닝 기술은 인터넷 환경에서 다양한 접근이나 동작을 학습하여 비정상적인 접근 및 악성코드의 동작을 탐지할 수 있어 보안 분야에서도 활용이 가능한 기술이다[9].

복잡한 문제 해결을 위해 딥러닝 솔루션을 쉽게 구축할 수 있는 프레임워크가 다양해지고 있다. 구글에서 2015년에 개발하여 오픈소스로 공개한 텐서플로우, 최초의 딥러닝 라이브러리 중 하나이며, 파이썬 기반으로 CPU, GPU의 수치계산에 유용한 Theano, 효율적인 신경망 구축을 단순화한 인터페이스인 Keras 는 TensorFlow와 Theano 에서도 동작되도록 구성되었다.

표현과 속도, 모듈성에 초점을 두고 BVCL에서 개발된 Caffe는 CNN 모델링이나 이미지 처리문제에 효과적이다. Lua 기반으로 페이스북, 트위터, 구들 등에서 사용하고 개발된 Torch 는 유연성이 좋고, 모델 제작과정에 효과적이다. 그 외에도 자바로 개발한 Deep Learning 4j 과 R, 파이썬, Julia 와 같은 언어를 지원하는 MxNet, 딥러닝 모델 교육을 위한 오픈 소스 CNTK 등이 있다.

2.3 얼굴인식 검증 데이터셋

딥러닝 기반 얼굴인식 기술을 검증하기 위해 대용량 데이터셋이 요구된다. 네이버 개발자 센터는 Clova 플랫폼 서비스 제공하는데 이는 얼굴인식을 통해 유명인을 찾거나 얼굴의 윤곽과 눈, 코, 입, 표정을 제공하고 있다[10]. 카카오 Vision API는 이미지 내부의 콘텐츠를 분석하여 얼굴 검출, 상품 검출 등을 판별할 수 있는 API를 제공하고 있다[11]. MS Azure는 사람 얼굴 감지, 감정 인식, 유사 얼굴 검색 및 유사한 이미지 그룹화 등 서비스를 제공하고 있다[12].

Table 1. Big DataSet for Face recognition[13]

Dataset	Image	Face	Source
MegaFace	1,027,060	690,572	Flickr
MegaFace2	4,753,320	672,057	Flickr
CASIA WebFace	494,414	10,575	Celebrity Search
LFW	13,233	5,749	Yahoo News
FaceScrub	106,863	530	Celebrity Search
YouTube Faces	3,425(V*)	1,595	YouTube
CelebFaces	202,599	10,177	Celebrity Search
DeepFace	4,400,000	4,000	Internal
FaceNet	500,000,000	10M	Internal
IJB-A	5,712 2,085(V*)	500	Internal
IJB-B	67,000 7,000(V*)	1,845	Internal
IJB-C	138,000 11,000(V*)	3,531	Internal
VGGFace	2,600,000	2,622	Google & YouTube
VGGFace2	3,310,000	9,131	Google & YouTube

*v : video

3. 얼굴인식 기술

얼굴인식 기술은 사전에 입력된 여러 이미지 등 영상에서 얼굴 영역 추출하는 단계, 각 이미지에서 추출된 얼굴 영역에서 특징 추출하는 단계, 새로운 이미지와의 매칭을 통한 식별하는 단계, 즉 3개 단계를 통해 이미지로부터 사용자를 식별하는 기술이다[3, 13, 14]. Fig. 3는 훈련과 테스트로 병행 처리하는 과정으로 주어진 이미지를 가지고 얼굴인식 과정을 구체적인 단계를 나타내고 있다. 사전에 여

러 얼굴이미지를 입력받아 학습을 시키고, 사용자 식별을 위해 새로운 이미지를 학습된 모델을 활용하여 테스트를 통해 사용자를 식별하는 과정을 보여주고 있다.

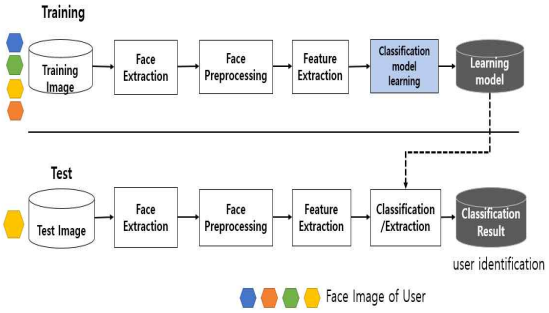


Fig. 3. Pipeline of Face recognition

3.1 얼굴 영역 추출 단계

입력 영상에서 얼굴 부분만을 검출하는 단계로 개인의 얼굴이 고정된 모양을 갖지 않기 때문에 다양한 변형이 가능하여 얼굴 영역추출에 어려움이 있다. 얼굴 템플릿에 기반하여 얼굴 영역을 추출화는 방법과 눈, 코, 입과 같은 얼굴 요소의 위치를 기반으로 특징 벡터를 계산하여 얼굴 부분을 추출하는 방법이 있다.

-템플릿을 이용한 얼굴 영역 추출은 얼굴 모델을 학습을 시켜 입력 영상이 모델에 부합하는 수준에 따라 판별한다. 템플릿을 이용하면 얼굴과 얼굴이 아닌 영상을 구별할 수도 있다.

-얼굴 요소간의 위치 벡터를 계산하여 얼굴을 축출할 수 있다.

3.2 특징 추출 단계

얼굴 영상으로부터 식별을 효율적으로 높이기 위해 얼굴 구성 요소인 눈, 코, 입을 찾아 특징(Feature) 추출한다. 고차원 신호를 차원을 낮추어 통계적 방법으로 특징 추출하는 방법(PCA)와 선형 판별 분석 방법(LDA)이 있다. 이 방법은 계산 속도가 빠르고 모델이 저장된 DB의 크기가 크지 않아도 되는 장점이 있다.

3.3 매칭을 이용한 식별 단계

특징 벡터값을 DB에 저장하고, 등록된 특징 벡터값과 비교하여 식별한다. 즉, 얼굴의 특징 벡터를 최근접 분류기를 이용하여 얼굴을 인식한다. 최근에는 SVM 기법을 이용하여 얼굴의 작은 영역에서 요소만 추출한 후 특징 벡터로 활용하여 인식한다.

4. 얼굴인식 소스 분석 및 논의

구글의 FaceNet, 페이스북 DeepFace가 대표적인 얼굴인식기술이다. 카메라를 통해 개인의 얼굴을 찍고, Face API가 제공되는 서버에 전달이 되고, HOG를 통해 얼굴을 인식하고, 재배치하고 128개의 벡터를 추출하고, SVM으로 분류하여 얼굴을 인식하는 기술이다.

4.1 프로그램 소스 분석

Fig. 4 는 길지 않은 파이썬 소스를 실행하여 주어진 사진과 비교하는 얼굴 인식하는 프로그램이다. 얼굴 인식하는 프로그램은 3개의 단계로 사용자를 식별한다.

- step 1. Fig. 4(a)는 사전에 주어진 사진이다. 여기에서는 영화 매트릭스의 배우 사진을 등록한다. 배우 사진으로 부터 각각 얼굴 영역을 찾는다.
- step 2. Fig. 4(b)는 찾은 얼굴 영역에서 랜드 마크를 찾은 후 얼굴을 인코딩한 후 사전에 등록된 사용자 이미지의 벡터를 저장하고, 사용자를 식별하는 구현 코드이다. 사전에 등록된 배우의 이름을 부여하고, 모델을 학습한다. 새로운 사진을 입력하여 그 사진이 누구인지를 판정할 수 있다.
- step 3. Fig. 4(c)는 딥러닝 학습 모델에서 새로운 사진이 누구인지 식별한 결과를 보여준다. 마지막 사진은 사전에 등록되지 않는 사용자라서 unknown 으로 표시된다.

(a) Input Image of Actor' Face

```
import cv2, dlib
import numpy as np
import matplotlib.pyplot as plt
import matplotlib.patches as patches
import matplotlib.patheffects as path_effects

detector = dlib.get_frontal_face_detector()
sp = dlib.shape_predictor('models/shape_predictor
_68_face_landmarks.dat')
facerec = dlib.face_recognition_model_v1('models/
dlib_face_recognition_resnet_model_v1.dat')

def find_faces(img): ~~#Define the Fuunction
def encode_faces(img, shapes): ~~#Function
~~

for name, img_path in img_paths.items():
 img_bgr = cv2.imread(img_path)
 img_rgb=cv2.cvtColor(img_bgr, cv2.COLOR_BGR2RGB)
  _, img_shapes, _ = find_faces(img_rgb)
  descs[name]=encode_faces(img_rgb, img_shapes)[0]

np.save('img/descs.npy', descs)
```

```
#target image
img_bgr = cv2.imread('img/target.jpg')
img_rgb=cv2.cvtColor(img_bgr, cv2.COLOR_BGR2RGB)

rects, shapes, _ = find_faces(img_rgb)
descriptors=encode_faces(img_rgb, shapes)

fig, ax = plt.subplots(1, figsize=(20, 20))
ax.imshow(img_rgb)

for i, desc in enumerate(descriptors):
  found = False
    for name, saved_desc in descs.items():
      ~~~
        if dist < 0.6:
            found = True
            ~~~
            break
    if not found:
      ~~~
```

(b) Source of Python[15]

(c) Result of Actor' Face recognition(target.jpg)

Fig. 4. Program Source of Face recognition[15]

4.2 논의 및 사례연구

얼굴인식 기술의 중요성이 부각되면서 1985년 부터 특허가 출원되어 연평균 약 18%씩 성장하고 있다. Table 2은 최근 2018년까지의 얼굴인식 세부분야별, 기간별 출원특허 비율을 나타낸 것이다[13].

Table 2. Ratio Change for Face Technology Patent

Fields	Total	~2010	2011~15	2016~18
Face Detection	41%	55%	27%	24%
Feature Extraction	20%	18%	19%	16%
Face Classification	28%	20%	36%	45%
Emotion Recognition	5%	2%	9%	13%
etc	7%	6%	8%	3%

얼굴인식 기술을 이용하여 활용할 수 있는 분야는 다양하게 존재한다. 헤어샵이나 헬스장, 음식점 등 소규모 고객을 가지는 다양한 상점에서 회원카드를 기반으로 포인트나 다른 서비스를 제공하는 시대에서 스마트 미러 등을 활용하여 고객을 확인하고, 고객 맞춤형 서비스를 제공하는 시대가 도래하고 있다. 이처럼 얼굴인식 기술은 실생활에서 다양하게 활용될 수 있다.

5. 결론

최근 이슈가 되고 있는 인공지능 기술 중에서 딥러닝 기술이 부각이 되고 있다. 특히, 개인별 서비스를 제공하기 위해 인증이 요구되는 시점에서 생체인증 서비스가 다양해지고 있다. 생체인증 중에 편리성 등으로 얼굴인식이 사용자 인증에 활용 가능성이 높

아지고 있다.

본 논문은 얼굴인식 기술의 중요성을 강조하고, 얼굴인식 기술의 발전 및 활용분야를 조사하고, 얼굴인식 기술의 단계별 과정과 적용가능성을 설명하고 있다. 특히 인터넷에서 제공되고 있는 실제 소스을 분석하고, 사용자 인증 기술로 가능성을 알아보았다.

향후 연구로는 고객을 대상으로 개인별로 고객 맞춤별로 서비스가 필요한 산업체에서 얼굴인식 기술을 이용하여 쉽게 빠르게 고객을 식별할 수 있는 스마트 미러 등의 제품 개발이 필요하다. 얼굴 뿐만 아니라 모션인식을 새로운 인증 기술로 활용할 수 있도록 추가적인 연구가 필요하다.

REFERENCES

[1] H. J. Mun. (2019). A Study on the User Identification and Authentication in the Smart Mirror in Private. Journal of Convergence for Information Technology, 9(7), 100-105.
DOI : 10.22156/CS4SMB.2019.9.7.100

[2] H. J. Mun. (2018). Biometric Information and OTP based on Authentication Mechanism using Blockchain. *Journal of Convergence for Information Technology*, 8(3), 85-90.
DOI : 10.22156/CS4SMB.2018.8.3.085

[3] H. J. Moon, S. H. Kim (2013). Face Recognition : A Survey. *Korea Information Processing Society Review*, 20(3), 14-23.

[4] T. Horiuchi, T. Hada (2013). A complementary study for the evaluation of face recognition technology. 2013 47th International Carnahan Conference on Security Technology (ICCST), pp. 1-5.

[5] S. Xie, S. Shan, X. Chen & J. Chen (2010). Fusing Local Patterns of Gabor Magnitude and Phase for Face Recognition. *IEEE Transactions on Image Processing,* 19(5), 1349-1361.

[6] Y. C. Hwang, H. J. Mun, J. W. Lee. (2015). Face Recognition System Technologies for Authentication System - A Survey. *Journal of Convergence for Information Technology,* 5(3), 9-13.

[7] J. Shin, Z. Liu, C. M. Kim & H. J. Mun. (2018). Writer identification using intra-stroke and inter-stroke information for security enhancements in P2P systems. *Peer-to-Peer Networking and Applications,* 11(6), 1166-1175.
DOI : 10.1007/s12083-017-0606-0

[8] H. S. Choi, Y. H. Cho. (2019). Analysis of Security Problems of Deep Learning Technology. *Journal of the Korea Convergence Society*, 10(5), 9-16.
DOI : 10.15207/JKCS.2019.10.5.009

[9] ETRI. (2016). Trends on Distributed Frameworks for Deep Learning, *Electronics and Telecommunications Trends*, 31(3), 131-141. https://ettrends.etri.re.kr/ettrends/159/0905002137/0905002137.html

[10] Naver. https://developers.naver.com/products/clova/face/

[11 Kakao. https://vision-api.kakao.com/

[12] Microsoft. https://azure.microsoft.com/ko-kr/services/cognitive-services/face/

[13] H. I. Kim, J. Y. Moon & J. Y. Park. (2018). Research Trends for Deep Learning-Based High-Performance Face Recognition Technology, Electronics and Telecommunications Trends, 33(4), 43-53.
DOI : 10.22648/ETRI.2018.J.330405

[14] S. H. Lee. (2018). A Method for Determining

Face Recognition Suitability of Face Image. *JKAIS*,19(11), 295-302.

[15] Github. https://github.com/kairess/simple_face_recognition

문형진(Hyung Jin Mun) [종신회원]

- 2008년 2월 : 충북대학교 전자계산학과(이학박사)
- 2017년 3월 ~ 현재 : 성결대학교 정보통신공학과 조교수

- 관심분야 : 사용자 인증, 딥러닝, 빅데이터분석
- E-Mail : jinmun@gmail.com

김계희(Gea Hee Kim) [정회원]

- 2013년 8월 : 한국방송통신대학교 정보과학과(이학석사)
- 2017년 2월 : 경남과학기술대학교 컴퓨터공학과(공학박사)
- 2018년 ~현재 : ㈜ E-Core HRD 연구원

- 관심분야 : Vanet, IoT, 무선네트워크, 인공지능(AI)
- E-Mail : jenni7@naver.com