개인정보 보호를 위한 위치정보 마스킹 시스템

오희주, 김상대

순천향대학교 의료IT공학과

ohj5018@sch.ac.kr, sdkim.mie@sch.ac.kr

Location information masking system for personal information protection

Huiju Oh, Sangdae Kim

Dept of Medical IT Engineering, Soonchunhyang University

요 약

일상에서의 사진을 SNS에 공유할 때 사용자의 위치를 파악할 수 있는 특정한 정보가 포함되기도 한다. 이는 스토킹 같은 범죄에 이용될 수 있다. 이러한 문제를 해결하기 위해 본 연구에서는 광학문자인식(OCR)을 활용하여 이미지에 특정한 정보가 포함된 부분을 자동으로 마스킹해주는 시스템을 제안한다. 이는 이미지에 사용자의 위치를 파악할 수 있는 텍스트와 같은 정보가 인식되면 그 정보만 마스킹한 후 사용자에게 반환해 주어 사용자의 위치를 보호할 수 있다.

I. 서론

이동전화를 사용하는 사람들의 수가 증가하면서 이에 따라 SNS(Social Network Service) 사용자 수 또한 함께 증가하고 있다. 사람들은 여행지나 일상의 모습을 촬영하고 인스타그램, 페이스북 등 SNS에 촬영한 사진을 공유하고 있다.[1]

일상에서의 얼굴이나 풍경 등 다양한 사진들을 촬영할 경우 사용자의 위치를 확인할 수 있는 특정 정보가 같이 포함되기도 한다. 이때 이러한 정보가 들어간 이미지는 촬영한 곳의 장소를 알아내는 범죄에 이용될 수 있다. 2019년 일본에서는 한 남성이 여성 아이돌 가수의 얼굴 사진 속 눈동자를 보고, 사용자의 위치를 알아낸 뒤 직접 찾아가는 사례가 있었다.[2] 이렇게 이미지만으로도 스토킹 행위를 당할 수 있으며, SNS가 활발해지면서 접근하거나 따라다니는 행위의 스토킹 피해는 더욱 늘어나고 있다.[3] 또한 더 나아가 주거침입으로 이어지기도 한다.

따라서 본 논문에서는 사용자의 위치정보를 기반으로 하는 스토킹 범죄를 예방하기 위해 사용자의 위치정보를 가려주는 시스템을 만들고자 한다. 이 시스템은 사용자가 촬영한 사진 속에 사용자의 위치를 알 수 있는 특정한 정보가 포함되면 광학 문자 인식(OCR) 시스템을 사용하여 그 정보만 지워준 후 사용자에게 반환해 준다.

이로써 사용자는 안전하게 사진을 업로드하고, 스토킹을 예방할 수 있으며, 스토킹뿐만 아니라 강도나 주거 침입에도 예방할 수 있다.

II. 위치정보 보호 시스템

본 장에서는 오픈소스인 Tesseract OCR을 사용하여 이미지 속 사용자의 위치를 추측할 수 있는 정보를 마스킹해주는 시스템을 제안한다.

II-1. 기존 연구

본 절에서는 사용된 기술 및 기술의 동작 과정에 관해 설명한다.

본 기술은 광학문자인식(Optical Character Recognition, OCR)을 사용하였는데, 이는 텍스트 이미지를 기계가 읽을 수 있는 텍스트 포맷으로 변환해 주는 기술이다. [그림1]을 통해 OCR의 동작 과정을 보면 먼저 PRE PROCESSING (전처리)에서 Raw Image에 대한 이진화, 잡음 제거, 왜곡 감지 단계를 거친다. 다음으로 SEGMENTATION(세분화)이 진행되어 이미지를 선 또는 문자로 분해하고 FEATURE EXTRACTION(특징 추출) 과정을 진행한다. 마지막으로 높은 정확도로 문자를 classifier(분류)하고, POST PROCESSING(후처리) 단계를 거쳐 결과를 나타낸다.[4]

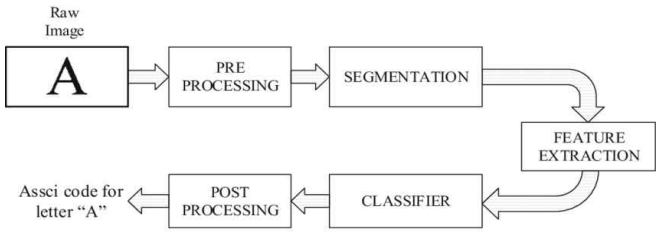

그림 1. Structure of OCR system[4]

Tesseract는 구글에서 지원하는 오픈소스 OCR의 엔진으로, 본 연구에 적용한 Tesseract는 LSTM(신경망) 기반을 적용하여 더욱 인식률을 높였다.

II-2. 시스템 동작 과정

본 절에서는 제안한 시스템에 관한 결과를 나타낸다. 원본 사진에서도 결과가 잘 나오지만, 마스킹 된 부분을 자세하게 보여주기 위해 텍스트가 있는 부분만 선별하여 제시한다.

그림 2. 사용자가 촬영한 사진

그림 3. 마스킹 기법이 적용된 사진

본 연구에서는 Python을 기반으로 한 웹 사이트 개발과 Flask를 활용하여 사용자가 촬영한 사진을 웹 사이트에 업로드한 후, 특정 정보가 마스킹 처리된 사진을 반환받을 수 있는 기능을 구현하였다. 사용자 인터페이스의 구현을 위해, 웹 표준기술인 HTML, CSS, JavaScript를 활용하였다. 구현한 웹 사이트에 [그림 2]와 같은 사진을 업로드하면, Tesseract OCR 시스템을 통해 자동으로 이미지 속의 텍스트를 인식하는 기술을 활용하였다. 이 과정을 통해 식별된 텍스트를 마스킹하기 위해, 각 문자의 좌표와 크기를 파악하여 문자가 위치한 부분만을 마스킹하는 알고리즘을 적용하였다. 이러한 마스킹 기법을 사용함으로써, 사용자의 위치를 알 수 있는 정보를 선택적으로 숨기면서도, 원본 이미지는 그대로 유지하는 데에 중점을 두었다. 이와 같은 기술은 사용자가 웹 사이트에 사진을 업로드할 때마다 자동으로 실행되며, 이 과정을 거친 후 마스킹 처리된 사진을 사용자에게 반환한다. 반환된 사진은 [그림 3]에서 확인할 수 있듯이, 사용자의 민감한 정보를 효과적으로 보호하는 데에 큰 도움을 준다.

III. 결론 및 향후 연구

사람들이 일상에서 촬영한 사진을 SNS에 공유한다. 이때 이미지 속에 사용자의 위치를 알 수 있는 정보가 포함되기도 한다.

따라서 본 논문에서는 사용자의 위치정보가 포함된 이미지가 공유되었을 때 발생할 수 있는 범죄를 예방하기 위해 위치정보를 보호하는 시스템을 제안한다. 이미지 속에 텍스트가 포함되면 그 텍스트로 정보를 파악할 수 있게 되므로, Tesseract OCR을 사용하여 이미지 속 텍스트를 인식한다. 이후 인식한 텍스트의 크기에 맞춰 텍스트를 가릴 수 있도록 마스킹하여 정보를 가려준다. 하지만, LSTM 기반을 적용하였음에도 불구하고 한글 인식률이 낮다는 문제점이 있다. 또한 이미지의 화질에 따라서도 인식률의 차이가 보였다.

향후, OCR이 한글 인식률을 높일 수 있도록 학습 방안에 관해 연구할 것이며, 이미지의 화질을 모두 일정하게 만들 수 있다면 효과적으로 시스템을 이용할 수 있을 것으로 사료된다.

ACKNOWLEDGMENT

본 연구는 2024년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업의 연구 결과로 수행되었음(2021-0-01399)

참 고 문 헌

[1] KISDI 2023년 한국미디어패널조사 주요 결과, https://www.kisdi.re.kr/report/view.do?key=m2101113025790&arrMasterId=4333447&masterId=4333447&artId=1168536#none

[2] 정진영 기자, '눈동자에 비친 경치'로 집 유추…아이돌 성추행한 日남성 붙잡혀, 국민일보, https://www.kmib.co.kr/article/view.asp?arcid=0013803089

[3] KOSIS, 여성가족부,「여성폭력실태조사」, 2021, 2024.02.22, 평생 스토킹 피해 유형(중복응답), https://kosis.kr/statHtml/statHtml.do?orgId=154&tblId=DT_154023_22AA020200&conn_path=I2

[4] Heidarysafa, Mojtaba & Reed, James & Kowsari, Kamran & Leviton, April & Warren, Janet & Brown, Donald. (2020). From Videos to URLs: A Multi-Browser Guide to Extract User's Behavior with Optical Character Recognition. 10.1007/978-3-030-17795-9_37.