응시자 행동로그와 영상데이터 분석을 통한 온라인 시험 부정행위 방지 시스템 구현

최성환, 김용범, 안세진, 서동만
대구가톨릭대학교 컴퓨터소프트웨어학부
dute7570@cu.ac.kr, mach2320@cu.ac.kr, asj0423@cu.ac.kr, sarum@cu.ac.kr

A Development of a Cheating Detection System based on behavior logs and video data analysis

Sung-Hwan Choi, Yong-Bum Kim, Se-Jin Ahn, Dongmahn Seo
School of Computer Software, Daegu Catholic University

요 약

코로나19 대유행으로 비대면 교육이 보편화되어 온라인 학습과 시험이 교육기관에서 일반화되고 있다. 이러한 급격한 변화로 교육의 공정성 문제와 온라인 시험의 부정행위 문제가 대두되고 있다. 온라인 시험은 대면 시험과는 달리 시험 감독관이 부정행위를 적발하기 어렵기 때문에 응시자의 다양한 환경을 고려하여 정확하게 부정행위를 판별하는 방법이 필요하다. 본 연구에서는 온라인 시험환경에서 응시자의 행동 데이터와 영상데이터를 분석하여 부정행위를 감독관에게 추천하는 시스템을 제안한다. 제안 시스템의 구현을 통해 온라인 시험 환경에서 부정행위를 탐지 기능을 확인한다.

1. 서론

코로나 19 대유행으로 인해 온라인 수업과 온라인 시험 등을 활용하는 비대면 교육환경이 보편화되었다. 이러한 온라인 교육 환경의 증가는 기존 대면교육과 다른 다양한 문제들이 발생하고 있다. 다양한 문제점 중에서도 온라인 시험의 공정성이 가장 큰 문제로 대두되고 있다. 공정해야 할 온라인 시험에서 개개인의 감독과 관리가 쉽지 않은 상황을 이용한 다양한 부정행위가 빈번하게 발생하고 있다.[1]

온라인 시험 부정행위는 크게 응시자 인증 부정행위와 시험 중 부정행위로 나눌 수 있다. 응시자 인증 부정행위의 경우 시험 시작 시점에 실제 응시자의 신원을 확인하여 응시자 명단과 대조하는 것으로 방지가 가능하다.

온라인 시험은 시공간의 제약 없이 대규모 인원이 동시에 시험을 치를 수 있다는 장점이 있다. 그러나 부정행위 검출이 어렵다는 이유로 시험 결과에 대한 신뢰도가 낮아 종종 공정성 시비 발생하여 제한적으로 적용되고 있다.

본 논문에서는 온라인 시험 환경에서 사용자의 행동 데이터와 영상 데이터 분석을 통한 부정행위 방지 시스템을 제안한다. 제안하는 시스템은 응시자의 키보드와 마우스의 입력 데이터와 카메라로 촬영한 응시자 영상을 분석하여 부정행위로 의심되는 상황을 저장하여 시험 감독관이 부정행위를 파악할 수 있도록 한다. 제안 시스템의 구현과 실험을 통해 온라인 시험 환경에서 부정행위를 탐지할 수 있음을 확인하였다. 본 시스템의 부정행위 탐지 기능은 온라인 응시자의 부정행위 시도를 미연에 방지하는 효과는 물론 공정성이 매우 중요한 입학시험과 입사시험, 자격증시험, 직무능력 평가 등 다양한 분야에서 활용될 수 있다. 본 논문의 2 장에서는 관련 연구들을 살펴보고, 3 장에서는 연구 방법에 대해 소개하고, 4 장에서 연구 결과, 마지막 5 장에서 결론을 기술한다.

2. 관련 연구

온라인 시험 환경에서의 부정행위를 방지하기 위해 다양한 시도가 이루어져 오고 있다. 현재 온라인 시험환경에서 수집할 수 있는 응시자 데이터는 비인가 SW 실행 데이터, 얼굴 인식 데이터, 마우스 및 키보드 입력 데이터 가능하다.

2.1 얼굴 인식 방식

온라인 시험 전 응시자의 얼굴을 Haar cascade 알고리즘[2]을 통해 얼굴을 인식하며, 기존에 촬영하여 저장해둔 응시자의 얼굴과 일치하면, 시험방에 접속할 수 있다. 시험 응시 중에도 얼굴이 일치하지 않다고 판단 시, 로그에 기록이 남도록

한다. Haarcascade 는 영상의 명암을 통해 오브젝트를 검출하는 알고리즘이다. 오브젝트 특징이 직사각형 영역으로 구성되어 있기 때문에 적분 이미지로 최적화했을 때 대채로 자원 대비 성능이 높다. 영역 간 밝기 차이를 이용한 특성 덕분에 그림자가 많고 밝기 차이가 많은 얼굴을 인식하는 데에 적합하므로 본 연구에서는 이 알고리즘을 사용한다.

2.2 특수키 인식 방식

온라인 시험 도중 부정행위를 하는 응시자의 키보드 패턴을 파악하여 시험을 치르는 도중에 사용되어 지지 않는 입력 값들을 특수 키 입력으로 확인하고 부정행위를 잡아 낼 수 있다. 키보드 모듈을 사용하여 응시자의 시험 도중 부정행위 가능성이 있는 입력 값들을 감지할 수 있다. 시험 도중 응시자가 특수 키를 입력하면 로그에 기록을 저장하고, 즉시 감독관에게 알림을 보낸다. 특정한 키의 입력을 탐지함으로써 응시자의 부정행위를 막아 낼 수 있다는 장점이 있다.

2.3 차단프로그램 관리

시험 감독관이 시험 방 생성과정에서 시험 중 차단할 응용프로그램을 선택한다. 예를 들어, 크롬, 마이크로소프트 엣지, 사파리 등의 웹 프라우저나, 카카오톡 등과 같은 매신저 프로그램, 메모장, PDF 뷰어 등의 프로그램, 계산기 등이다. 운영체제의 프로세스 제어 명령어를 이용하여 응시자가 시험 도중 차단 프로그램 리스트 내의 프로그램을 실행하더라도 강제 종료하여 부정행위를 방지할 수 있다.

3. 연구방법

3-1. 동작 원리

제안 시스템은 크게 응시자용 프로그램과 감독관용 프로그램으로 구성된다. 응시자용 프로그램은 시험 입장 시 응시자 본인의 학번과 시험번호를 통한 본인 인증과 얼굴 인식의 2 단계 과정으로 응시자 인증 부정행위를 방지한다. 감독관이 시험을 생성할 때 영문(대소문자 구분)과 숫자로 구성된 15 자리의 무작위의 시험번호가 생성된다. 얼굴인식 시스템은 사전에 등록한 사진과 카메라 화면의 얼굴을 비교하여 본인 여부 확인을 진행하고 동일한 것이 파악되면 시험 입장이 가능하다. 응시자의 좌석 이탈 여부 파악이 가능하다. 응시자가 10 초 이상 자리를 이탈하면 5 초 단위로 계산하여 기록된다. 키보드의 경우 복사, 붙여넣기, 윈도우 키 등 시험에 필요 없는 기능을 사용할 시 입력값을 기록한다. 감독관용 프로그램은 모든 응시자의 컴퓨터 화면과 얼굴을 확인하며 감독 할 수 있다.

3-2. 구조

응시자용은 응용프로그램으로, 감독관용은 웹으로 구현하였다.

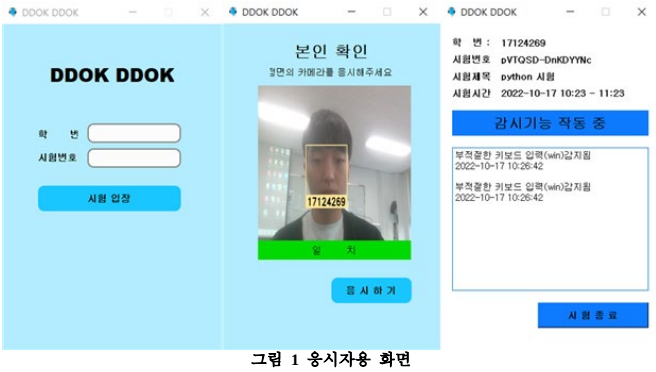

그림 1 응시자용 화면

먼저 응시자용 프로그램은 학번과 시험번호 입력을 하여 시험 입장을 해야 하고 본인확인(얼굴 인식)을 통하여 입장한다. 입장 시 '시험 대기 중'이 표시되고 감독관이 시험 버튼을 클릭 시 '감시 기능 작동 중'이란 글귀로 바뀌게 되면서 시험을 치른다. 그 아래에 본인의 부정행위 기록이 부정행위 시간과 함께 표시된다. 시험 종료 버튼을 통하여 프로그램을 빠져나올 수 있다.

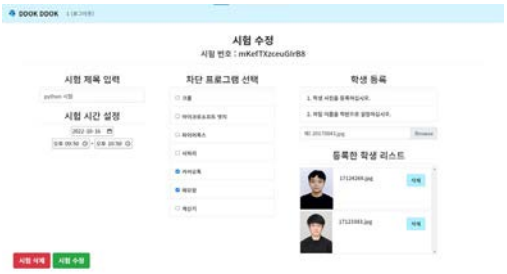

그림 2 감독관용 화면

감독관용 웹 페이지는 로그인을 할 수 있는 화면을 시작으로 로그인과 회원가입이 있다. 회원가입을 하고 로그인하면 메뉴 화면으로 넘어가는데 '시험 생성', '시험수정', '시험 입장' 메뉴로 나뉘어 있다. 먼저 '시험 생성' 메뉴를 클릭 시 시험번호, 시험 제목, 시험 시간, 차단 프로그램 선택, 학생 등록이 있다. 학생 등록에는 응시자의 학번과 사진을 저장하여야 한다. 사진은 앞서 말한 얼굴인식에 사용이 되고 응시자 입력 시 아래에 학생 리스트에 등록이 된다. 시험 수정 메뉴는 생성이 된 기록을 가지고 시험 생성 화면으로 넘어가서 수정할 수 있게 된다. 시험 입장 메뉴 클릭하고 시험 버튼을 클릭하면 학생의 응시 화면을 확인할 수 있다. 부정행위 적발이 되면 빨간색으로 표시가 되고 응시자 화면 클릭 시 실시간으로 로그를 조회할 수 있다. 카메라로 탐지되는 경우 당시의 사진과 함께 로그에 기록이 된다. 이후에도 언제든지 기록 열람이 가능하다.

3-3. 시스템 구현

얼굴인식 시스템은 OpenCV 와 python 의 face_recognition[3]를 활용한다. 본인 확인 시 얼굴과 사진 속 얼굴이 동일하다면 '일치'와 함께 학번과 응시하기 버튼이 활성화되고 동일하지 않다면 '불일치'와 응시하기 버튼이 비활성화된다. 응시 도중 본인이 아닌 사람이 탐지가 되면 '응시 대상자가 아닌 타인 감지'라는 글귀와 함께 기록된다. 인원 파악의 경우 '00 명이 감지 되었습니다'라고 기록이 되고, 사람

이 존재하지 않는다면 '아무도 없음'과 존재하는 시간이 길어지면 나타날 때까지의 시간을 계산하여 '00초 동안 감지 되지 않음'으로 보여준다.
키보드 탐지 기능은 특수적인 키가 입력되었을 때 기록된다. 프로그램이 차단 또는 키보드 감시 프로그램은 thread 를 만들어 탐지하고 프로그램이 실행하거나 실행 중이라면 운영체제의 kill() 함수를 사용하여 지정한 프로그램 혹은 웹을 자동으로 종료한다.

3. 연구 결과

그림 3 부정행위 탐지 화면

응시자의 행동 중 부정행위로 탐지되는 행동이 발견되면 감독관에게 붉은색 화면이 1 초간 깜빡인다.

그림 4 학생 세부 정보(학생 화면 및 부정행위 로그 리스트)

응시자의 화면을 클릭하게 된다면 자세한 로그와 함께 응시자 화면을 감독 가능하다.

그림 5

그림 6

[그림 5]는 올바른 응시자가 탐지되었을 때 상황이며, [그림 6]은 응시자 외 제 3 자가 탐지되었을 때의 부정행위가 탐지된 상황이다. 이로써 사전에 타인이 시험을 응시하는 경우를 사전에 차단할 수 있다.

시험을 응시하는 도중 자리를 비우게 된다면, n 초 동안 감지되지 않았다는 문구가 감독관에게 정상적으로 전달되는 화면이다.

그림 7

그림 8

[그림 7]은 특수 키 입력 부정행위 감지 시 감독관에게 로그 전송 화면, [그림 8]은 응시자용 프로그램의 부정행위 감지 시 로그 출력 화면이다.

시험도중 정리된 파일의 검색 부정행위를 하는 경우를 잡아 낼 수 있다. 응시자가 응시도중 특수한 키를 입력한 경우 감독관에게 부정행위 알림이 가며, 로그가 정상적으로 감독관에게 남게 된 사진이다.

그림 9 시험 결과 화면

시험이 끝나고 난 뒤의 화면. 감독관은 이 화면에서 응시가 끝난 시험의 로그와 결과를 찾아 볼 수 있다.

5. 결 론

본 연구에서는 기존 온라인 시험 환경에서 부정행위를 탐지하는 시스템을 제안한다. 제안하는 시스템은 얼굴 인식 데이터와 특수 키 입력 데이터, 차단프로그램 데이터를 활용하여 온라인 시험에서의 부정행위를 탐지하여 시험 감독관에게 통보한다. 구현된 제안 시스템은 응시자 인증 부정행위와 시험 중 부정행위를 방지할 수 있음을 확인하였다.

이 시스템의 몇가지 한계점이 있다. 영상 범위 밖에서 이루어지는 부정행위를 탐지하지 못하는 점, 특수키 사용이 부정행위를 입증하기 까지는 어렵다는 점, 차단 프로그램에 등록되지 않은 프로그램을 사용한다면 사전에 막기가 힘들다는 점, 마지막으로 제안하는 시스템 기능을 위해 프로그램을 우회할 수 있는 가능성이 존재한다.

향후에는 딥러닝을 통한 응시자 얼굴인식 정확도 향상과 응시 환경의 소리 데이터 기반의 부정행위 탐지 기능을 연구할 계획이다. 이와 더불어 온라인 환경에서 발생할 수 있는 다양한 부정행위 유형을 분석하여 보다 공정한 온라인 시험 환경에 관한 연구를 지속할 예정이다.

Acknowledgement 본 논문은 과학기술정보통신부 및 정보통신기획평가원에서 주관하여 진행하는 'SW 중심대학사업'의 결과물입니다. (2019-0-01056)

참고문헌

[1]인하대 뿐인가..건국대에선 온라인시험 동시접속 기록 '발칵', https://v.daum.net/v/20200602060104123 , (2020. 6. 2)

[2] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001, 2001, pp. I-I, doi: 10.1109/CVPR.2001.990517.

[3] OpenCV ,https://pyimagesearch.com/2018/09/24/opencv-face-recognition/