

# 인공 지능 기술을 활용한 기만 탐지 기법에 대한 최신 동향 연구

이지혜, 조영호(교신저자)

국방대학교 관리대학원 국방과학학과 컴퓨터공학과/사이버전 협동전공

e-mail: c16530@gmail.com, youngho@kndu.ac.kr

## A Study of Research Trends on Deception Detection Techniques using Artificial Intelligence Technology

Jihye Lee, Youngho Cho

Dept. of Defense Science (Computer Engineering and Cyberwarfare Major),  
Korea National Defense University

### 요 약

기만(Deception)은 단순한 속임수를 뜻하며 인간의 삶에 빈번하게 발생하지만 범죄에 사용되어 개인의 인생에 심각한 영향을 주기도 한다. 범죄적 속임수를 뜻하는 사기(Fraud)나 거짓말(Lying)도 기만(Deception)에 포함된다. 기만 행위 간 발생하는 행동 및 생리적 변화를 단서(Cue)로 정의하여 적극적으로 증거중심적으로 특정 커뮤니케이션의 진실 전달 여부를 추론하는 과정을 기만 탐지라고 한다. 기만 탐지를 위해 기존에는 심리적·행동적 단서를 기반으로 각종 기계(거짓말 탐지기, 기능적 자기공명영상)를 사용한 기만 탐지와 같은 방법이 사용되어 왔지만, 최근에는 인공지능 기술을 접목하여 기만행위를 정확히 탐지하기 위한 노력이 지속되고 있다. 국내 연구는 해외 연구에 비해 양도 부족하고, 연구가 이루어지지 않는 분야도 있으며, 질적으로도 보완할 필요가 있다. 따라서, 본 연구는 국내의 문헌 연구를 통해 기만 탐지 기법을 단서와 인공지능 기술 중 머신러닝과 딥러닝을 기준으로 분류 및 목록화하여 소개하여 기만 탐지 기법에 대한 충분한 이해를 목표로 수행되었다.

### 1. 서론

미국 서던 캘리포니아 대학교의 제리슨 심리학 교수에 의하면 우리가 매일 나누는 대화 중에서 3분의 1이 거짓말이라고 한다. 이렇듯 거짓말은 우리의 주변에서 빈번하게 일어나는 일이며, 진실과 거짓을 알고 싶어 하는 욕구도 인간의 역사와 함께 계속 되어 왔다. 특히, 법률 분야에서 진실과 거짓은 개인의 인생을 결정지을 수도 있기 때문에 법 집행기관은 진위 여부 판단을 위해 다양한 접근을 해왔으며, 현장에서는 거짓말 탐지기(Polygraph), 행동 분석, 진술 분석, 음성강세분석(Vocal Stress Analysis, VSA), 안면열영상분석(Thermal Imaging of the Face), 뇌지문분석(Brain Fingerprinting), 기능적 자기공명영상(fMRI) 등을 활용하고 있다.

최근 딥러닝, 머신 러닝의 인공지능 기술을 활용한 연구는 기만 탐지 영역에서도 적용되고 있다. 해외에서는 기만탐지에 인공지능 기술을 다양하게 접목하기 위한 노력이 있어왔다.[1, 2]. 하지만 국내에서는 인공지능 기술보다는 거짓말 탐지기와 같은 기계적 기만 탐지, 행동에 기반을 둔 심리적인 기만 탐지에 대한 연구가 더 많이 진행되었고, 인공지능 기술은 금융 분야의 이상 거래탐지 시스템(Fraud Detection System)에 주로 적용되었으며, 기만 탐지 분야에 대한 동향 연구는 찾아보기 어렵다.

본 연구는 방대한 문헌 연구를 통해 기만 탐지 기법을 단서와 인공지능 기술 중 머신러닝과 딥러닝을 기준으로 분류 및 목록화하여 소개함으로써 기만 탐지기법에 대한 최신 연구동향의 이해를 목표로 수행되었다. 이를 위해, 2장에서는 단서를 기반으로 기만 탐지 기법들을 분류하며, 3장에서는 인공지능 기술과 기만 탐지 기법들에 대해 살펴보고, 4장에서는 국내외 연구 사례를 목록화하여 제시한 후 5장에서 결론을 맺는다.

### 2. 단서 기반 기만 탐지 기법의 분류

#### 2.1 기만과 기만 탐지의 개념

세계 최대의 온라인 정신 건강 및 행동 사이트인 Psychology Today 홈페이지에서는 기만(Deception)을 사실이 아닌 정보를 사람들이 이 믿도록 부추기는 (크든 작든, 잔인하든 친절하든 관계 없는) 행위로 정의한다. 이와 유사한 미국 국제개발처 감찰관실 홈페이지에서 사기(Fraud)는 금전적 또는 개인적 이익을 얻기 위한 부당하거나 범죄적인 속임수로 정의하고 있다. 본 연구에서는 사기(Fraud) 또한 기만(Deception)에 포함된 것으로 본다.

또한, 기만 탐지(Deception Detection)란 특정한 커뮤니케이션이 진실을 전달하는지 여부를 결정하는 행위로, 기만자의 행동 및 생리적 변화를 관찰하여 기만 여부를 판단하는 적극적이고 증거 중심적인 추론 과정으로 정의한다[3].

#### 2.2 단서 기반 기만 탐지 기법

기만행위에 대한 이론적 근거 중 단서 누출(Cue Leakage) 이론에서는 속임수가 무엇인지에 대한 단서를 기만자가 누설한다고 한다[4]. 이를 바탕으로 연구된 [5]에서 단서(Cue)는 속임수를 나타낸다고 여겨지는 관찰되고 측정될 수 있는 지표 또는 변수로 정의하였다.

[2]에서는 다양한 연구에 대한 문헌적 검토를 통해 데이터 유형에는 텍스트, 비디오, 오디오, EEG-P300 신호 등이 있으며, 이를 기반으로 기만 탐지의 단서는 언어적 단서, 비언어적 단서, 하이브리드 단서로 구분한다. 본 연구에서도 동일한 개념을 사용한다.

##### 2.2.1 언어 단서 기반 기만 탐지 방법

기만자의 말에 미치는 영향을 분석하는 방법으로, 텍스트 기반과 음성 기반으로 구분된다. 텍스트 기반은 문장, 기호 및 단어와

같은 표면 세부 사항에 초점을 맞추고, 음성 기반은 표면 뿐만 아니라 내부 의미 구조의 특징에도 초점을 맞추며, 음성 흐름에 포함된 기만은 식별이 쉽지 않다.

2.2.2 비언어 단서 기반 탐지 방법

기만자가 말하고 행동하는 방식에 미치는 영향을 분석하는 방법으로, 신경학적, 시각적 또는 음성적(vocal)인 지표인 얼굴, 제스처, 시선, 미세한 표현 등에 대하여 뇌파 신호 관찰, 비디오 분석 등을 통해 기만의 징후를 감지한다.

2.3.1 하이브리드 단서 기반 탐지 방법

근래의 연구들은 언어 혹은 비언어 단서가 융합된 하이브리드 방식으로 융합하여 사용되는데, 이는 언어와 비언어 요소 모두가 기만 판단에 중요한 단서를 제공하기 때문이다.

3. 인공지능 기술과 기만 탐지 기법

3.1 머신 러닝(Machine Learning)

머신 러닝은 컴퓨터가 데이터로부터 학습하고 명시적으로 프로그래밍하지 않고도 작업을 수행하는 기술로, 크게 지도 학습과 비지도 학습으로 구분되는데, 기만 탐지에서는 지도 학습이 주로 사용되었다. [1]에 의하면, 기만 탐지에 가장 많이 사용된 알고리즘은 Neural networks(NN), Support Vector Machines(SVM), Logistic Regression(LR), K-Nearest Neighbor, Decision Trees(KNN)의 순이다.

3.2 딥 러닝(Deep Learning)

딥러닝은 머신러닝에 포함된 개념으로, 지식을 계층적 구조로 표현하는데 인공 신경망에 별도로 훈련된 은닉층을 쌓아 학습하는 방식으로, [2]에 의하면, 심리학, 컴퓨터 과학, 언어학 및 범죄학을 포함한 여러 분야에서 딥러닝 기술을 활용하여 신뢰할 만한 기만 탐지 도구를 구축하기 위해 노력해 왔다.

4. 기만 탐지 관련 문헌 연구

4.1 해외 연구

본 연구에서는 [1], [2]에서 조사된 연구를 기준으로 성능 지표가 75% 이상이거나, 지표가 75%에 못 미치더라도 의미 있는 연구 총 57개를 분석한 후 대표적인 연구들을 <표 1>에 제시하였다.

<표 1> 인공지능 기술별 해외 기만 탐지 기법 분류

		머신 러닝	딥 러닝
언어	텍스트	[6]	[7]
	음성	[8]	[9]
비언어	얼굴	[10]	[11]
	눈	[12]	-
	뇌파	[13]	[14]
	비지도	[15]	-
하이브리드		[16]	[17]

4.1.1 머신 러닝을 활용한 기만 탐지

1) 언어 단서 기반 기만 탐지

텍스트를 이용한 머신 러닝 기만 탐지는 다음과 같다.

Feng 등[6]은 제품 리뷰부터 에세이라는 다양한 도메인의 4개의 서로 다른 데이터셋을 대상으로, 확률적 문맥 자유 문법(PCFG: Probabilistic Context Free Grammar) 구문 분석 트리와 SVM을 사용하여 기존 연구의 최고 결과를 개선하여 91.2%의 정확도와 14%의 오류 감소를 달성하였다.

음성을 이용한 머신 러닝 기만 탐지는 다음과 같다.

Nasri 등[8]은 ReLiDDB (ReGIM-Lab Lie Detection DataBase)라는 데이터 베이스를 구축 후, 자동 음성 처리에 일반적으로 사용되는 MFCC(Mel Frequency Cepstral Coefficient)를 기반으로 하여, 음향 매개변수가 거짓말 탐지에 유용한지 조사하였다. 분류과정에서 SVM을 사용했으며, 음성 오디오의 거짓 혹은 진실 탐지 정확도는 각각 88.23% 및 84.52% 였다.

2) 비언어 단서 기반 기만 탐지

얼굴을 단서를 사용한 머신러닝 기만 탐지는 Avola 등[10]의 연구가 대표적인데, 인터뷰 대상이 포함된 비디오 프레임에서 얼굴 AU(Action Unit)을 추출하고, SVM, RF를 통해 진실 혹은 속임수로 분류하며, 정확도 76.84%를 달성하였다.

단서로 눈을 사용한 Labibah 등[12]은 눈 추적과 동공 직경 변화를 통해 Wavelet Transform to Gabor Image Processing 프로세스를 사용한 후, 거짓 여부를 Decision Tree(DT)를 통해 분류하였으며, 정밀도는 97%, 회수율은 94%를 보였다.

기만 탐지 과정에 뇌파 중 하나인 P300(뇌파 중 베타파 범주에 속하며 자극 관련성 평가, 의사 결정 및 맥락 업데이트의 인지 처리와 관련)을 추출하여 사용할 수 있는데, Gao 등[13]은 독립 성분 분석(ICA)을 사용한 모델로, P300 성분을 자동으로 인식한 후 Pz 전극에서 P300을 재구성하는 알고리즘이며, SVM으로 시간, 주파수 영역의 특징을 추출하였으며, 82.45%의 정확도를 보였다.

Mathur 등[15]은 고위험군 레이블을 사용하지 않고 비디오에서 고위험군 속임수를 탐지하는 최초의 멀티모달 비지도 전층 학습 접근법인 하위 공간 정렬(Subspace Alignment: SA) 접근법을 제안하였고, 이는 고위험군 기만(예: 범법행과정의 기만)의 실제 데이터 부족 문제를 해결하였다. 최고의 비지도 SA 모델(75% AUC, 74% 정확도)은 SA가 없는 모델을 능가하고, 인간의 능력을 능가하는 성능을 발휘한다고 주장하였다.

3) 하이브리드 기만 기만 탐지

하이브리드 머신 러닝 기만 탐지 중 대표적인 것은 Nidhi 등[16]의 연구이다. 50명의 피험자의 생리학적 특징(혈압, 심박수 및 호흡수)과 음성 특징(기본 주파수, 제로 교차율, 프레임 기능 및 에너지)을 사용하고, 인공 신경망(Artificial Neural Network: ANN)과 SVM이 사용하여 분류한다. ANN 모델의 정확도는 93.33%, SVM 모델의 정확도는 100%이다.

4.1.2 딥 러닝을 활용한 기만 탐지

1) 언어 단서 기반 기만 탐지

텍스트를 이용한 딥 러닝 기만 탐지는 다음과 같다.

Barsever 등[7]의 연구가 있으며, Ott 코퍼스 데이터 셋에 대해 사전 훈련된 BERT(Bidirectional Encoder Representations from Transformers) 모델 사용하여 69개의 진실한 문장과 148개의 기만적인 문장을 식별했으며, 93.6%의 정확도에 도달하였다.

음성을 이용한 딥 러닝 기만 탐지는 다음과 같다.

Xie 등[9]은 원본 음성의 시간 정보를 보존하여 음성 길이에 따라 차원이 동적으로 변하는 프레임 수준의 음향 특징을 추출한 후 양방향 LSTM (Bidirectional Long Short-Term Memory)와 프레임 수준 음향 기능을 결합한 방법이 제안되었다. 사용된 데이터 셋은 Columbia-SRI-Colorado 코퍼스로 평균 정확도는 70.3%에 도달하여 비접촉 모드로 이전 작업보다 향상된 성과를 보

였다. 또한 컨볼루션 연산을 사용하여 시간-주파수 혼합 데이터를 발굴하였다.

2) 비언어 단서 기반 기만 탐지

얼굴 단서를 활용한 딥러닝 기만 탐지는 Karimi 등[11]이 대표적인데, 기만적인 비디오를 자동으로 정확하게 탐지할 수 있는 중단 간 프레임워크를 제안하였다. 제안 모델은 자동 기능 추출, 시각 단서 제공, 분류의 과정을 거치며, 시각 및 음성 모드에서 자동 기능 추출을 위해 CNN을, 전체 기능 시퀀스 조사에 LSTM을 사용한다. 데이터 셋으로는 실제 법원 재판의 비디오를 사용하였고, 제시된 모델은 음성 모드에서 74.16%, 시각 모드에서 75%, 음성과 시각 모드에서 84.16%의 정확성을 보였다.

뇌파(P300) 단서에 대한 기만탐지는 Amber 등[14]에 의하여 이루어졌으며, 30명의 피험자들의 P300 신호들(유죄와 무죄로 구분된)을 분류 문제에 효과적인 CNN(Convolutional Neural Network)의 접근 방식을 적용하여 99.6%의 높은 정확도를 달성했다.

3) 하이브리드 기반 기만 탐지

하이브리드 딥 러닝 기만 탐지는 Gogate 등[17]의 연구가 대표적인데, 시각적 및 텍스트 단서와 함께 처음으로 오디오 단서를 통합하여 자동화된 속임수 탐지를 위한 새로운 딥 러닝 기반 다중 모드 융합을 제시하였다. 시각적 특징 추출에 3D-CNN, 텍스트 기능 추출에 텍스트-CNN, 음향 특징 추출에 가장 널리 사용되는 오픈소스 소프트웨어인 openSMILE을 사용하였으며, 융합 방법에는 빠른(기능 수준) 융합, 늦은(의사결정 수준) 융합을 사용하였다. 정확도 96.42%, 정밀도 96%, 민감도는 95%의 성과를 보였다.

4.2 국내 연구

논문 검색 과정에서 주제 관련된 논문을 총 16개 확인하였으며, 대표적인 연구들은 <표2>에 제시하였다.

<표 2> 인공지능 기술별 국내 기만 탐지 기법 분류

		머신 러닝	딥 러닝
언어	텍스트	[18]	[19]
	음성	[20]	[21]
비언어	얼굴	[22]	없음
	눈	[23]	
하이브리드		없음	

4.2.1 머신 러닝을 활용한 기만 탐지

1) 언어 단서 기반 기만 탐지

텍스트를 이용한 머신 러닝 기만 탐지는 이승훈 등[18]의 연구가 대표적이며, 크라우드 펀딩 사기 프로젝트에 대해 공개적인 것이 없기 때문에, Kickscammed.com, Reddit, 페이스북의 그룹 중 하나인 ‘Crowdfunding Projects that Never Delivered’, 그리고 구글 검색을 통해 사기 프로젝트를 찾아내어 데이터 셋을 수집 한 후 필터링하였다. 프로젝트의 기본정보, 제작자 정보, 사회적 정보, 개체명 인식, 시간적, 공간적 단어, 글의 가독성 등의 기능 추출 후 RF와 LR을 사용하여 분류하였는데 RF를 통해서 84.46%의 정확도를 보였다.

음성을 이용한 머신 러닝 기만 탐지는 최진경의 연구[20]가 있다. 72명으로부터 각각 1,440개의 진실과 거짓 데이터(총 2,880개)를 확보한 후 음성, 열화상, 영상의 단서를 상관 클러

스터링, 차분진화 DT, SVM을 사용하였으며, DT는 71.6%, SVM은 72.1%의 정확도를 보였다.

2) 비언어 단서 기반 기만 탐지

김명수 등[19]의 연구는 얼굴을 단서로 사용한 연구로, 거짓말로 인해 변화된 얼굴 온도를 측정하였다. 16명의 피험자에게 거짓말을 유도하는 실험(참은 실거주지에 대한 1분 묘사, 거짓은 실험 시작 전 암기한 거짓 거주지 묘사)을 진행 후 피험자별 상관분석 결과 참 판별 정확도는 43.8%이며, 거짓 판별 정확도는 62.5%였다. 이 연구는 얼굴을 단서로 연구를 하였지만 인공지능 기술을 활용하지 않았다.

이연실 등[23]의 연구는 눈을 단서로 사용하였으며, 실험참가자를 유죄(25명)와 무죄(27명) 집단으로 나눠 모의범죄를 수행한 후, 비교질문검사를 실시하여 동공크기 및 응시횟수와 응시시간을 측정한다. 상태 불안에 대한 자기 보고식 검사 결과, 검사 전에는 유죄집단과 무죄집단의 상태불안에 차이가 없지만 검사 후 유죄집단과 무죄집단의 상태불안에 유의미한 차이가 있었으며 무죄집단에 비해 유죄집단의 상태불안이 유의미하게 높았다. 유죄집단과 무죄집단의 관련질문과 비교질문에 대한 동공크기 변화량을 비교하였을 때, 유죄 집단이 관련질문에서 확연하게 큰 동공크기의 증가를 보여 집단 간 동공크기 변화량의 차이가 통계적으로 유의미함을 알 수 있다.

4.2.2 딥 러닝을 활용한 기만 탐지

1) 언어 단서 기반 기만 탐지

텍스트를 이용한 딥 러닝 기만 탐지는 신준호[19]의 연구가 대표적이다. 대검찰청으로부터 아동 성범죄 피해자와의 대면조사 녹취록을 제공받아 수사과정에서 사용하는 진술분석 기법인 CBCA(Criteria Based Content Analysis)의 준거를 기존 모델보다 더 잘 분류하기 위해, 강건하게 최적화된 BERT(RoBERTa), 데이터 증강(문장 내 노이즈 추가, 문장 내 일부 단어 변경, 단어 임베딩 변경)을 사용한다. 제안 모델은 기존 모델보다 높은 F1 스코어를 달성(0.754)하였다.

음성을 이용한 딥 러닝 기만 탐지는 김영명[21]의 연구가 있으며, 71명의 사람으로부터 얻은 참 1,420건, 거짓 1,420건의 ‘아니요’ 음성 데이터로부터 openSMILE 특징점 집합 활용하여 시계열 특징점을 6,373개 추출하였다. 분류과정에 사용한 모델은 SVM, DNN, LSTM, Bi-LSTM을 사용하였으며, 각각의 정확도는 63.25%, 52.54%, 59.88%, 70.09%의 정확도를 달성하였다.

5. 결론

본 연구는 머신러닝 기술을 사용한 기만 탐지 기법들의 연구 동향에 대해 국내 최초로 수행한 연구로, 국내 연구 동향을 분석한 결과 다음과 같은 제한사항이 있었다.

첫째, 국내 연구는 해외 연구에 비해, 어떤 인공 기술에 관해서든 어떤 단서에 관해서든 연구의 양(quantity)이 부족하다. 해외 논문의 경우에 구글 스콜라에서 학술검색에서 “deception or fraud detection”, “machine or deep learning”의 키워드를 조합해서 두 영역을 만족하는 논문들이 수 백개 확인된다. 국내 논문은 구글 스콜라, DBpia에서 “사기 혹은 기만 탐지”와 “머신러닝 혹

은 딥러닝"을 동시에 넣으면 두 영역을 만족하는 논문은 10건 이하로 검색되었다.

둘째, 국내 연구는 연구가 되지 않은 영역(하이브리드 단서, 비언어 단서 딥러닝 분야)이 식별되었으며, 전체적으로 연구의 질(quality) 역시 향상해야 한다.

기만 탐지 분야는 참과 거짓의 정확한 판단을 통해 공정한 법 집행을 가능하게 하므로 매우 중요한 연구 분야이다. 따라서, 이 분야의 연구의 양과 질을 향상시키기 위해 연구자들의 노력과 관심이 필요하다.

#### 참고문헌

- [1] Constâncio, Alex Sebastião, et al. "Deception detection with machine learning: A systematic review and statistical analysis," Plos one Vol.18, No.2, 2023
- [2] Alaskar, Haya, et al. "Intelligent techniques for deception detection: a survey and critical study." Soft Computing, pp.1-20, 2022.
- [3] Levine, Timothy R. "Truth-default theory (TDI) a theory of human deception and deception detection," Journal of Language and Social Psychology, pp. 378-392, Vol 33, No.4, 2014
- [4] Waxer and Peter H. "Nonverbal cues for anxiety: An examination of emotional leakage," Journal of Abnormal Psychology, Vol.86, No.3, pp.306 - 314, 1977
- [5] Fuller, Christie M., David P. Biro, and Dursun Delen. "Exploration of feature selection and advanced classification models for high-stakes deception detection," Proceedings of the 41st Annual Hawaii International Conference on System Sciences. IEEE, 2008.
- [6] Feng, Song, Ritwik Banerjee, and Yejin Choi. "Syntactic stylometry for deception detection," Proceedings of the 50th Annual Meeting of the Association for Computational Linguistics, Vol.2, 2012.
- [7] Barsever, Dan, Sameer Singh, and Emre Neftci. "Building a better lie detector with BERT: The difference between truth and lies," 2020 International Joint Conference on Neural Networks (IJCNN). IEEE, 2020.
- [8] Nasri, Hanen, Wael Ouarda, and Adel M. Alimi. "ReLiDSS: Novel lie detection system from speech signal," 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp.1-8, 2016.
- [9] Xie, Yue, et al. "Convolutional bidirectional long short-term memory for deception detection with acoustic features," IEEE Access Vol.6, pp.76527-76534, 2018
- [10] Avola, Danilo, et al. "Automatic deception detection in rgb videos using facial action units," Proceedings of the 13th International Conference on Distributed Smart Cameras, pp.1-6, 2019.
- [11] Karimi, Hanid, Jiliang Tang, and Yanen Li. "Toward end-to-end deception detection in videos," 2018 IEEE International Conference on Big Data (Big Data), pp.1278-1283, 2018
- [12] Labibah, Zuhrah, Muhammad Nasrun, and Casi Setianingsih. "Lie detector with the analysis of the change of diameter pupil and the eye movement use method gabor wavelet transform and decision tree," International Conference on Internet of Things and Intelligence System (IOTAIS), IEEE, pp.214-220, 2018
- [13] J. Gao, Y. Yang, W. Wei and N. Rao, "A New Lie Detection Method based on Small-number of P300 Responses," proc. International Conference on Biomedical Engineering and Biotechnology, pp.662-665, 2012.
- [14] Amber, Faryal, et al. "P300 based deception detection using convolutional neural network," 2019 2nd International Conference on Communication, Computing and Digital systems (C-CODE). IEEE, pp.201-204, 2019.
- [15] Mathur, Leena, and Maja J. Mataric. "Unsupervised audio-visual subspace alignment for high-stakes deception detection," ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp.2255-2259, 2021.
- [16] Srivastava Nidhi, and Sipi Dubey. "Deception detection using artificial neural network and support vector machine," 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA). IEEE, pp.1205-1208, 2018.
- [17] Gogate, Mandar, Ahsan Adeel, and Amir Hussain. "Deep learning driven multimodal fusion for automated deception detection," Symposium series on computational intelligence (SSCI). IEEE, pp.1-6, 2017.
- [18] 이승훈, and 김현철. "크라우드펀딩에서의 사기 프로젝트 탐지: 캠페인의 프로필 정보와 언어적 특성을 활용하여," 한국컴퓨터정보학회논문지, 23권 3호, 55-62쪽, 2018
- [19] 신준호, "데이터 증강을 이용한 CBCA 준거 기반 진술 분류," 국내석사학위논문, 명지대학교 대학원, 2023. 서울
- [20] 최진경. "상관 클러스터링과 차분진화를 사용한 머신러닝 기반 개인화된 음성 거짓말 탐지 알고리즘," Diss. 한양대학교, 2022.
- [21] 김영명. "양방향성 장단기 기억 기술 순환신경망 모델 기반 음성 거짓말 탐지 알고리즘 개발," Diss. 한양대학교, 2020.
- [22] 김명수, 김주영, 남보름, 최진경, and 김인영. "열 영상 얼굴 감지를 이용한 비접촉식 거짓말탐지 온도 신호 상관분석," 대한전자공학회 학술대회, 1481-1482쪽, 2020
- [23] 이연실, 이상현, 방철, 최훈, 김석찬, and 이장한. "안구운동 추적 장비를 통한 거짓말자의 동공크기 및 안구운동 연구," 한국심리학회지: 사회 및 성격 30권 2호, 63-76쪽, 2016