

딥보이스로 제작된 음성 탐지 시스템

Researching speech detection systems made with DeepVoice

팀 명	비상구
지도교수	유승재, 김민수
팀 원	최 수 민 (팀장) 박 우 경 이 하 영 정 진 호 홍 준 희

2025. 11. 4

중부대학교 미래융합공학부 정보보호학전공

목 차

1. 서론
 - 1.1 연구 배경
 - 1.2 연구 필요성
 - 1.3 연구 목적 및 주제선정
2. 관련 연구
 - 2.1 딥페이크(DeepFake)
 - 2.2 딥보이스(DeepVoice)
 - 2.3 학습 알고리즘
3. 본론
 - 3.1 시스템 구성
 - 3.2 피처 선정
 - 3.3 애플리케이션 개발
4. 결론
 - 4.1 결론 및 기대효과
 - 4.2 향후 계획
5. 참고 자료
6. 별첨
 - 6.1 발표 PPT
 - 6.2 소스 코드

1. 서론 (14pt)

1.1 연구 배경 (12pt)

오늘날 인공지능 기술이 발전하면서 디지털 미디어의 신뢰성을 위협하는 딥페이크기술이 부(DeepFake) 상하고 있다. 딥페이크를 활용하여 실제와 구분하기 어려운 조작된 동영상 오디오이미지 등 다양한 딥페이크 유형이 존재한다.

공격자는 딥페이크로 제작한 딥보이스를 이용하여 금융 기관 및 수사 기관과 같은 국가 기관을 사칭해 조직적으로 범죄를 진행하고 성별연령에 관계 없이, 금융 피해가 지속적으로 증가하고 있다.

본 연구에서는 오디오와 관련된 딥페이크 유형을 중점으로 발생하는 보이스피싱 범죄 피해 예방에 도[2] 움을 제공하고자 머신러닝 및 딥러닝을 활용, (ML) (DL)하여 딥보이스로 제작된 음성 탐지 시스템을 제안하고자 한다.

1.2 연구 필요성

경찰청 자료에 의하면, 2021~2023년까지는 총 피해액과 1인당 피해액이 완만하게 감소하는 추세를 보인다. 그러나 2024년에 두 지표가 동시에 급증하였다. 특히 1인당 피해액이 큰 폭으로 상승했다는 점은, 단순 다량발송형 스팸보다 정교한 표적형 사기가 늘었을 가능성을 시사한다.

또한 2024년에는 딥보이스(음성 합성/변환) 기술이 뚜렷한 발전 추세를 보이며, 수 초 내외의 짧은 음성 샘플만으로도 화자 특성(음색·운율·억양) 복제가 가능해졌고, 실시간 대화형 음성 에이전트가 확산되면서 합성음의 자연스러움·반응속도·잡음 내성이 크게 향상됐다. 상용 API와 공개 모델의 등장으로 접근성과 배포 용이성도 높아져, 실시간 통화 환경에서 설득력 높은 사칭이 이루어지기 쉬운 환경이 조성되었다. Fig. 1.은 경찰청에서 조사한 보이스피싱 피해 자료이다.



Fig. 1. 경찰청 보이스피싱 피해 현황 및 추이

1.3 연구 목적 및 주제선정 이유

2024년 들어 딥보이스(음성 합성·변환) 기술이 고도화되면서 수 초 분량의 음성만으로 화자의 음색·운율을 설득력 있게 복제할 수 있게 되었다. 그 결과, 기사 사례(Fig. 2.)와 같이 가족·지인 사칭을 통해 “긴급 송금”, “사고·병원”, “폭행·협박” 등을 명분으로 금전을 요구하거나 압박하는 범죄가 급증하고 있다. 특히 통화·음성메시지는 ‘목소리’ 자체를 신뢰하는 매체이므로, 짧은 검증 없이 즉시 의사결정이 발생해 건당 피해액이 커지는 경향을 보인다. 이러한 환경 변화는 기존의 번호 차단·계좌 모니터링 중심 대응만으로는 충분하지 않음을 보여준다.

이러한 이유로 가족·지인 단위의 소규모 환경에서 딥보이스로 제작된 음성 탐지 시스템을 제안한다.



Fig. 2. 가족·지인을 사칭한 딥보이스 보이스피싱 사례

2. 관련 연구

2.1 딥페이크 (DeepFake)

DeepFake는 Deep Learning과 Fake의 합성어로, 대규모 데이터와 신경망을 활용해 현실에 존재하지 않거나 실제로 일어나지 않은 장면을 이미지·영상·음성 형태로 그럴듯하게 합성하는 기술을 의미한다. 생성 모델(예: GAN, 변분오토인코더, 확산모델 등)은 원본 데이터의 통계적 특성을 학습해 얼굴 교체(face swap), 표정·입 모양 재현(lip-sync), 목소리 모사(voice cloning) 등을 가능하게 한다. Fig. 3.는 이러한 DeepFake 기술의 전형적인 사례를 보여주며, 인간이 육안으로 구분하기 어려울 만큼 고해상도·고현실감을 달성한다.

이 같은 기술은 영화·게임·접근성 향상 등 긍정적 활용 가능성을 지니지만, 허위 정보 유포, 명예훼손, 금융 사기와 같은 위험을 동반한다. 특히 합성물이 짧은 시간에 대량 생성되고, SNS·메신저를 통해 고속 확산된다는 점이 대응을 어렵게 만든다.

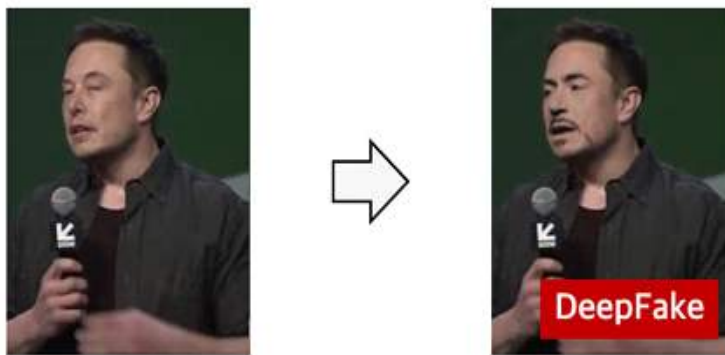


Fig. 3. DeepFake 기술 예시

2.2 딥보이스 (DeepVoice)

DeepFake의 세부 영역 중에서도 음성 합성(딥보이스)은 사회적 파급력이 가장 즉각적이다. 그 이유는 통화·음성메시지처럼 신뢰를 전제로 하는 매체에서 곧바로 사용될 수 있고, 단 몇 초~수십 초의 샘플만으로도 화자의 목소리 특징(포먼트, 프로소디, 억양)을 학습해 실시간에 가까운 합성이 가능하기 때문이다. 또한 영상의 경우 프레임 단위의 시각적 위변조 흔적(경계부 노이즈, 조명 불일치 등)을 탐지하는 도구가 비교적 보급되어 있는 반면, 음성은 통신 환경에 따른 잡음·코덱 압축이 흔적을 덮어버려 탐지가 더 어렵다.

따라서 본 연구는 DeepFake 중에서도 음성 기반 위협(DeepVoice)에 초점을 맞추어, 실제 피해가 급증하는 보이스피싱 시나리오에서의 탐지·차단 방안을 탐구한다.

DeepVoice는 화자의 음색·발음·운율을 학습해 목소리를 고충실도로 복제하거나 임의의 텍스트를 해당 화자의 음성으로 합성하는 기술을 일컫는다. 상용 음성비서(예: Bixby, Siri, Google Assistant, Alexa)에서 발전해 온 TTS(Text-to-Speech)·VC(Voice Conversion) 모델이 기술적 기반을 제공하며, 최근에는 짧은 음성 샘플만으로도 특정

화자를 설득력 있게 모사한다. 이러한 기술은 접근성 향상(실어증 환자 맞춤 음성 복원 등) 같은 긍정적 응용이 가능하지만, 동시에 가족·지인 사칭형 보이스피싱, 기업 내 임원 사칭을 통한 송금 지시 등 고위험 사회공학 공격에 악용되고 있다.

2.3 학습 알고리즘

실제 보이스와 딥보이스 간의 뚜렷한 피처를 선정할수록 모델의 정확도를 향상시킬 수 있다. 본 연구에서는 머신러닝과 딥러닝을 융합하여 모델 학습에 이용하고, RandomForest와 DNN을 이용하여 음성 데이터를 학습한다.

직접 피처를 선정하여 모델을 생성하는 과정에는 머신러닝이 적합하고, 음성의 크기가 크고 복잡한 형태의 파일을 학습하기에는 딥러닝이 적합하여 두 알고리즘을 이용해 모델을 학습시켜야 한다. 정적으로 선정된 피처 데이터는 DNN의 앙상블 학습 과정에 효과적인 결과를 나타낸다. Fig. 4.는 학습 알고리즘을 선정한 이유를 설명한다.

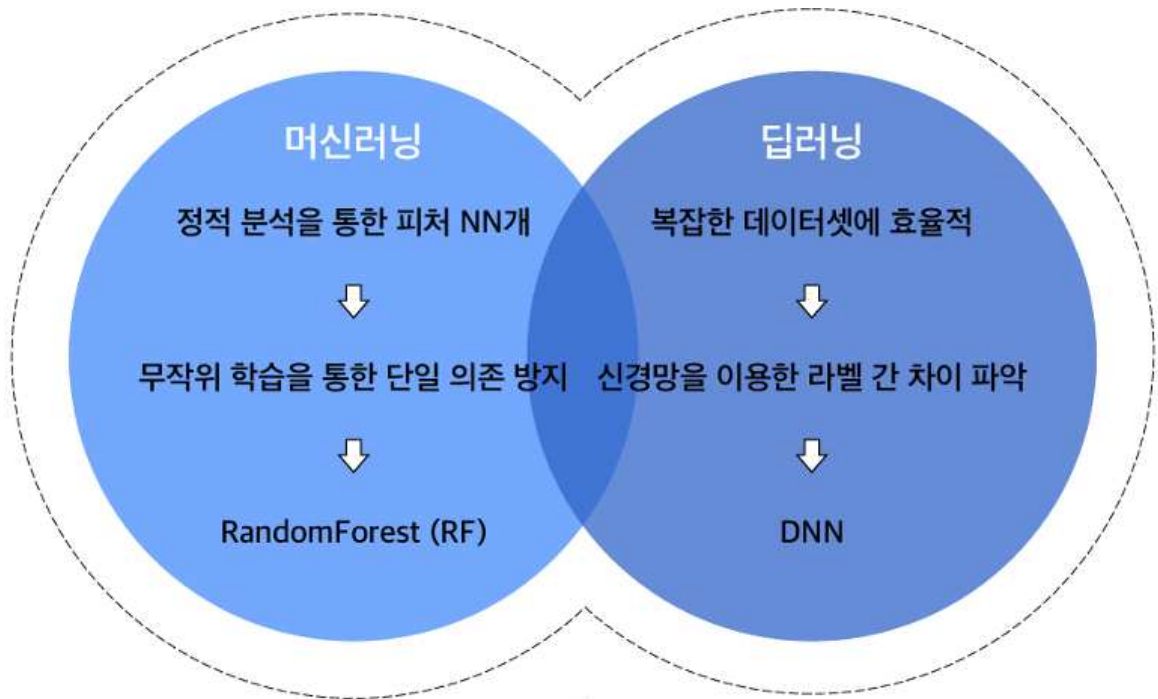


Fig. 4. 학습 알고리즘 선정

3. 프로젝트 내용

3.1 시스템 구성

본 프로젝트의 구성은 Fig. 5와 같다. 프로젝트는 크게 7단계로 나누어 동작한다.

우선 5초 분량의 사용자의 음성을 5개 녹음한다(1). 녹음된 음성은 사용자 음성 학습 인공지능 학습에 사용되고(2), 해당 인공지능은 통화 과정에서 실시간으로 사용자의 음성을 추출하여 데이터베이스에 저장한다(3). 데이터베이스에 저장된 사용자의 음성을 가지고 딥보이스 제작 인공지능을 활용하여 딥보이스를 생성한다(4). 딥보이스 또한 데이터베이스에 저장된다(5).

그렇게 저장된 사용자의 음성과 딥보이스 음성은 딥보이스를 구분하는 인공지능 학습에 사용된다(6). 딥보이스 구분 인공지능은 통화 중 딥보이스를 탐지하고 탐지 즉시 사용자에게 알림을 보내어 딥보이스 유무를 알린다(7).

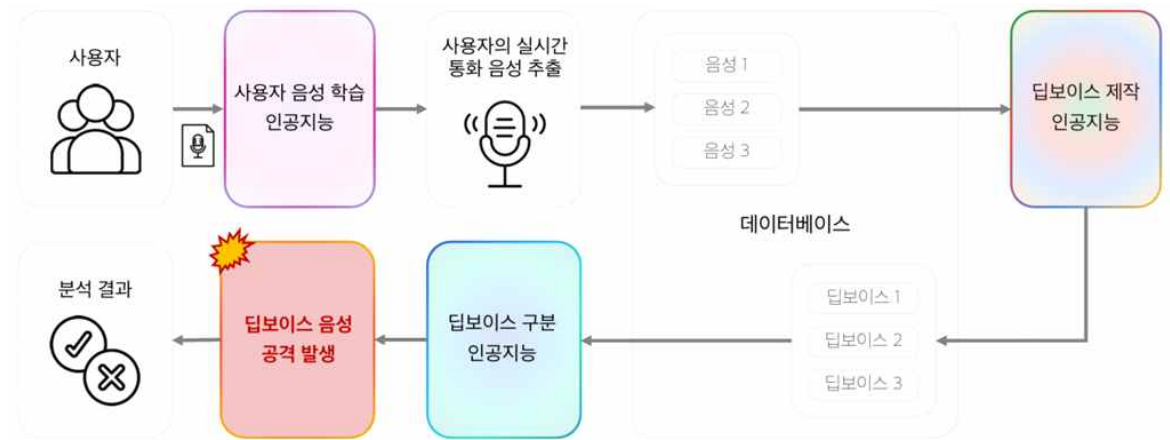


Fig. 5. 시스템 구성도(FlowChart)

3.2 피쳐 선정

인공지능을 학습하기 위해서는 먼저 피쳐를 선정하는 것이 중요하다. 어떤 피쳐를 선정하느냐에 따라 모델의 성능이 크게 달라지기 때문에 피쳐 선정에 오랜 시간을 사용해야 한다. 딥보이스는 음성을 기반으로 한 기술이기 때문에 피쳐 선정 또한 음성과 관련된 피쳐로 선정하였다. 딥보이스와 목소리의 파장, 주파수 등에서 차이를 발견하여 다음과 같이 12개의 피쳐를 선정하였다.

인공지능 학습에 사용된 피쳐는 다음과 같다. MFCC, Chroma, Tonnetz, Zero-Crossing Rate, Spectral Centroid, Spectral Rolloff, Spectral Flatness, RMS Energy, Harmonic/Percussive, Tempo, Spectral Bandwidth, Spectral Contrast

피쳐에 대한 설명은 다음과 같다.

MFCC는 음성의 스펙트럼 에너지 분포를 저차원 공간에 나타내어 음색과 발음 특성을 나타낸다. Fig. 6와 같이 실제 음성(원본)은 각 프레임(시간) 별로 MFCC값이 다양한 폭

(-400~200 이상) 고르게 분포하며, 특정 프레임에서는 짙은 빨간색(고값), 다른 프레임에서는 파란색(저값)을 자주 넘나드는 것을 특징으로 한다. 구체적으로 일부 음소·무성음·자음 구간에서 MFCC가 순간적으로 낮게 떨어지며 파란색으로 뚜렷하게 특정값이 드러나고 발음이 선명하게 구분된다. 반면 딥보이스는 오렌지색(중간값 부근)이 많이 분포하며, 시간 축에 따라 원본 대비 더 균일한 MFCC 특징값을 보이고, 전반적으로 단조로운 패턴이 다수 존재함을 확인할 수 있다.

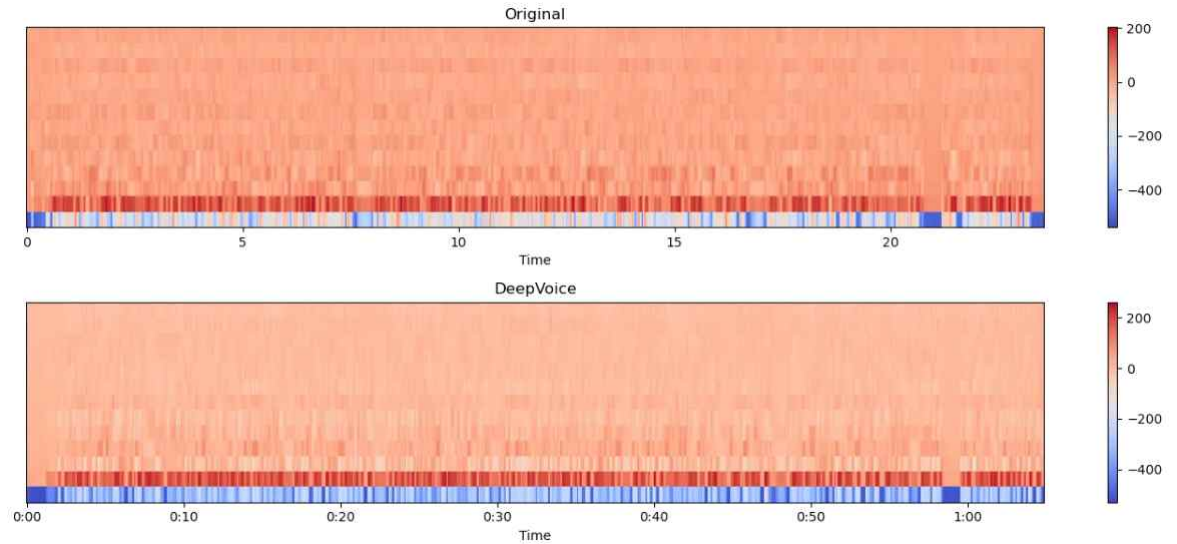


Fig. 6. MFCC

RMS Energy는 오디오 신호의 짧은 구간(프레임) 내 진폭(amplitude)의 제곱 평균 제곱근으로, 해당 구간의 전반적인 소리 크기(loudness) 또는 강도를 나타낸다. RMS Energy의 시각적 변화를 관찰하면 발화의 강약 변화, 즉 다이내믹 레인지(dynamic range)를 파악할 수 있다.

Fig. 7.과 같이 실제 음성은 0.05 근처에 낮은 값부터 0.3에 근접하는 높은 값까지 넓은 범위에 걸쳐 에너지가 분포하며, 시간에 따라 부드럽고 자연스러운 변화를 보인다. 이는 모음 구간에서 소리가 커지고 자음 구간에서 작아지는 등 자연스러운 발화의 강약 조절이 잘 이루어지고 있음을 의미한다.

반면 딥보이스는 원본보다 프레임 수가 훨씬 많이 나타나는데, 이는 합성 과정에서 프레임 추출 설정이 더 촘촘하게 이루어졌을 가능성을 나타낸다.

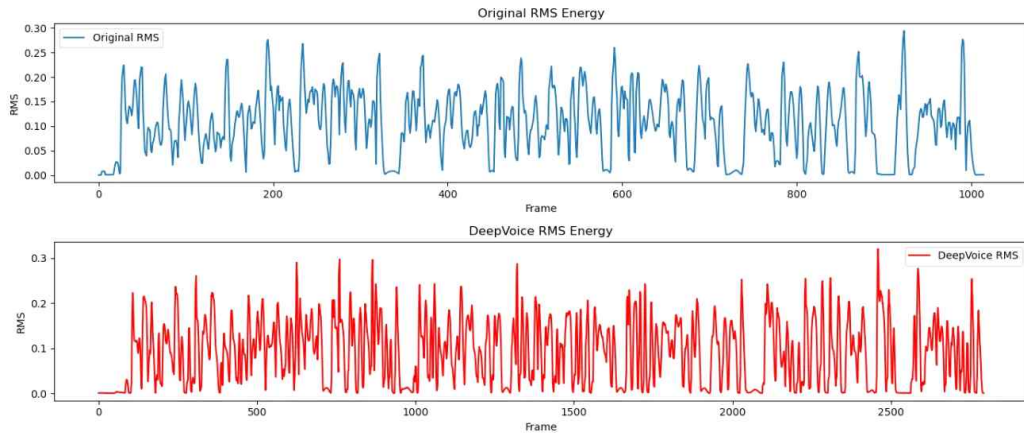


Fig. 7. RMS Energy

Zero-Crossing Rate(ZCR)은 오디오 신호의 파형이 시간 축(0점)을 교차하는 비율을 측정한 값으로, 신호의 포함된 고주파 성분의 양을 직접적으로 나타내는 지표이다. 일반적으로 목소리의 진동으로 생성되는 유성음은 저주파수 대역에 에너지가 집중되어 ZCR이 낮게 나타나고, 공기의 마찰이나 파열로 생성되는 무성음은 고주파수 대역의 에너지가 많은 ZCR이 높게 나타난다.

Fig. 8.과 같이 실제 음성은 ZCR이 대략 0.0에서 0.2 사이를 오르내리며, 파열음이나 마찰음과 같은 특정 무성은 구간에서 순간적으로 높아지는 자연스러운 패턴을 보인다. 반면 딥보이스는 특정 구간에서 ZCR이 짧은 간격으로 매우 높게 급상승하는 모습이 자주 관찰된다. 이는 유성음으로 발생되어야 할 구간에서 불필요한 노이즈나 고주파 아티팩트가 포함되어 유성음과 무성음 간의 전환이 부자연스럽게 처리되었음을 나타낸다.

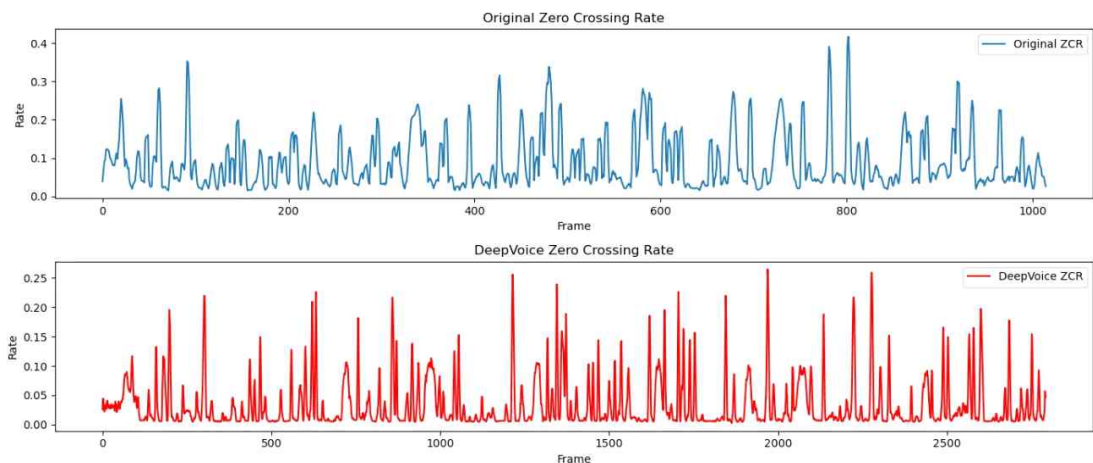


Fig. 8. Zero-Crossing Rate

Chroma는 12음계(반음)에 해당하는 12개의 파치 클래스(pitch class)로 사상(mapping)하여 표현하는 12차원의 특징 벡터이다.

Fig. 9.와 같이 원본 음성은 짧은 시간(약 0-25초) 동안 다양한 색상 변화가 나타난다. 특정 반음대에 에너지가 집중되지 않고, 여러 반음대에 걸쳐 에너지가 동적으로 분포하

는 경향이 보인다.

반면 딥보이스는 상대적으로 긴 시간(약 1분 이상) 동안 색상 변화 패턴이 단조롭고 반복적이다. 특정 반응대에서 짙은 빨간색(고에너지) 구간이 길게 유지되거나, 전반적으로 유사한 패턴이 지속되는 모습을 보인다.

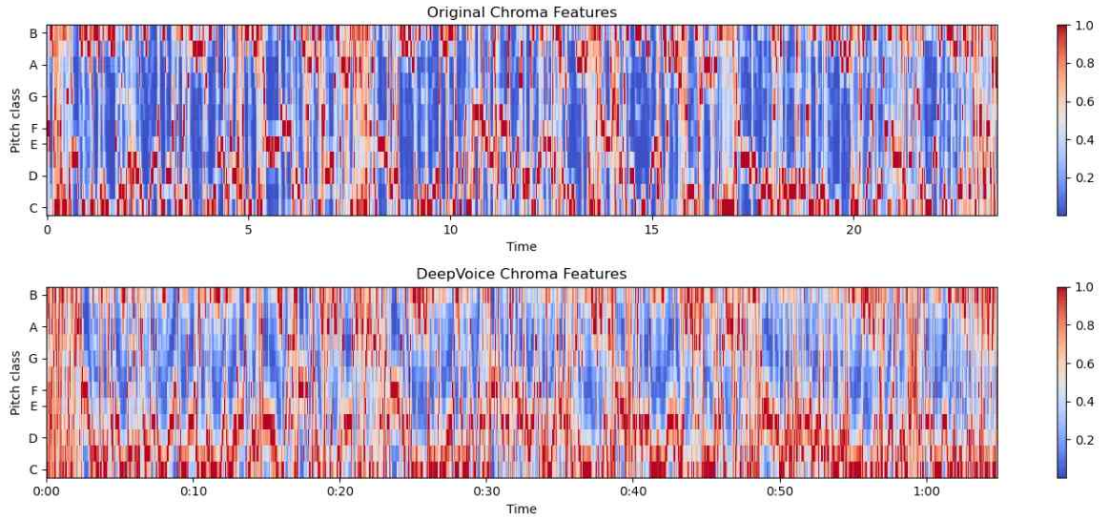


Fig. 9. Chroma 12음계

Spectral Contrast는 주파수 스펙트럼 내에서 국소적인 피크(peak, 에너지가 높은 부분)와 밸리(valley, 에너지가 낮은 부분) 간의 에너지 차이를 측정하는 지표이다.

Fig. 10.과 같이 원본 음성은 각 주파수 대역(세로축)에 걸쳐 밝은색과 어두운색 구간이 동적으로 교차하며 나타난다. 반면 딥보이스의 그래프는 시간 축을 따라 원본 대비 훨씬 균일하고 변화가 적은 패턴을 보인다

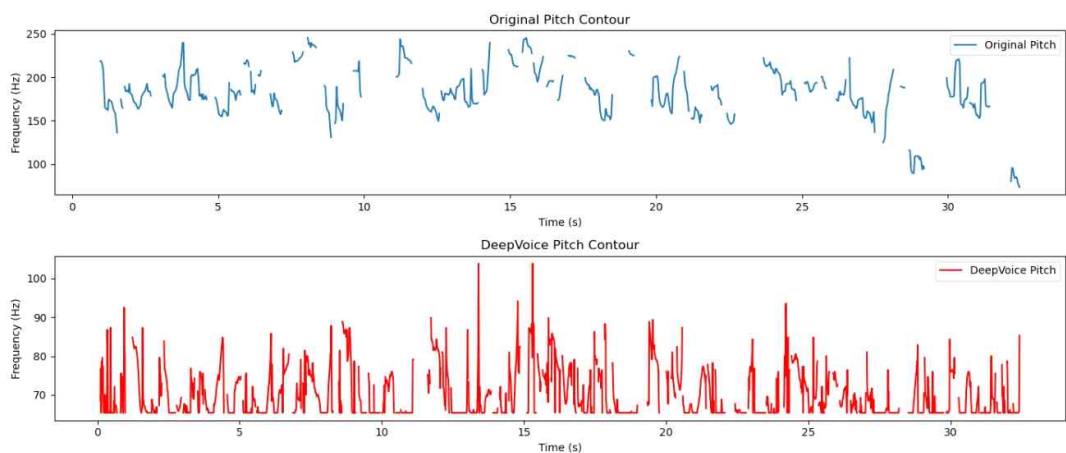


Fig. 10. Spectral Contrast

이 외 피쳐들에 대한 설명은 다음과 같다.

Tonnetz(6차원)은 조화(하모닉) 관계 임베딩으로 음악 지향 피쳐지만, 음성의 조화적 패턴·공명 차이를 간접적으로 반영한다.

Spectral Centroid는 스펙트럼의 “무게중심” 주파수로 값이 높을수록 밝고 날카로운 음색을 나타낸다

Spectral Rolloff는 누적 스펙트럼 에너지의 일정 비율(85~95%)에 도달하는 주파수·고주파 에너지 비중을 나타내는 지표이다

Spectral Bandwidth는 스펙트럼 퍼짐 정도를 나타낸다. 대역폭/분산을 나타내 음색의 퍼짐·거침과 연관된다.

Spectral Flatness는 스펙트럼이 얼마나 평탄한지를 나타낸다 값이 높을수록 노이즈/거친음성일 가능성을 보여준다

Tempo는 비트 추적 기반 추정 템포를 의미한다. 음성에서는 말속도/리듬성의 대략적 지표를 나타낸다.

3.3 애플리케이션 개발

본 프로젝트의 목적은 가족 혹은 가까운 지인 대상의 딥보이스 보이스피싱을 방지하기 위한 시스템을 개발하는 것을 목표하였다. 이걸 구현하기 위해 직접 전화 통화 환경에서 모델이 정상적으로 동작할 수 있는지 확인하기 위해 전화 애플리케이션 개발을 목표로 하였다.

앱에 대한 기능은 다음과 같다.

Fig. 11.은 메인화면 페이지로 “시작하기” 버튼을 누르면 다음 음성 녹음 페이지로 넘어간다.

Fig. 12.는 인공지능 모델을 학습하기 위한 사용자의 음성 데이터 셋을 수집하는 과정이다. 해당 페이지는 5초 분량의 문장 5개를 띄어주고 사용자는 시간에 문장에 맞게 녹음을 수행한다. 녹음된 파일은 데이터베이스에 저장된다.

Fig. 13.은 모델을 생성하는 페이지로 Fig. 14.에서 “모델 생성/업데이트” 버튼을 누르면 모델을 생성할 수 있다. 해당 모델은 딥보이스를 탐지하는 모델로 기존에 사용자에게 녹음 받은 음성 파일로 딥보이스 음성을 생성하여 원본 음성 5개, 딥보이스 음성 5개로 모델을 생성한다.

Fig. 14.는 전화 페이지로 상대방과 전화 통화를 할 수 있는 페이지이다.

Fig. 15.는 전화 통화 중에 딥보이스 음성이 탐지가 되었을 때 사용자에게 보여지는 경고 문구이다.



Fig. 11. 메인 화면

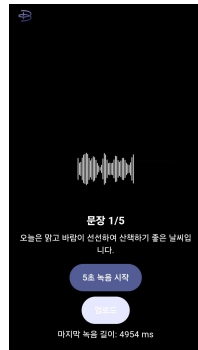


Fig. 12. 음성 녹음



Fig. 13. 모델 생성

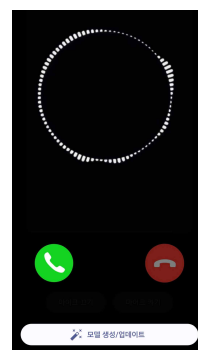


Fig. 14. 전화 기능

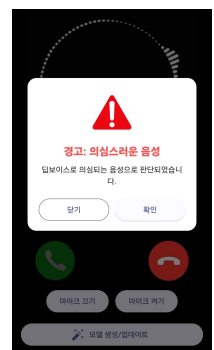


Fig. 15. 탐지 알림

4. 결론

4.1 결론 및 기대효과

결론적으로 만든 모델은 사용자의 실제 음성 5개, 딥보이스 음성 5개를 학습하였다. 그리하여 최종적으로 모델에 대한 테스트를 한 결과 992개의 음성 테스트 데이터셋을 기반으로 98.8%로 상당히 높은 정확도를 보였다.

하지만 본 프로젝트는 가족 또는 지인을 대상으로 지도학습을 적용하였다. 그렇기에 모델 학습에 사용되지 않은 사람의 음성에 대해서는 비교적 낮은 정확도를 보였으나, 딥보이스 음성에 경우 잘 탐지하는 모습을 보여준 반면 실제 음성에 경우 정확도가 떨어진 모습을 보였다.



학습에 사용되지 않은 사람의 딥보이스 음성이라 할지라도 정확하게 탐지하는 모습에서 향후 사람과 딥보이스 음성에 대한 탐지로 발전시킬 가능성을 보여준다.

본 프로젝트의 기대효과는 다음과 같다.

1. 보이스피싱, 금융 피해 대응, 음성 저작권 보호, 신분 도용 및 명예 훼손 방지
2. 시스템 운영의 효율적 자원 활용, 새로운 보안 인프라 구축
3. API 제공을 통한 연계 가능성, 음성 기반 증거 분석 활용 제공

4.2 향후 계획

지금까지는 가족 간의 딥보이스 보이스피싱 탐지에 중점을 두고 프로젝트를 진행하였다. 그렇기에 비지도 학습보다는 지도 학습을 통해 모델에 학습된 사용자의 음성만 효과적으로 탐지하도록 만들었다.

하지만 가족 간의 딥보이스 보이스피싱은 다른 사람의 딥보이스는 탐지하지 못한다는 한계점이 존재한다. 분명 딥보이스를 활용한 보이스피싱 또한 가족에 한정되지 않고 다양한 방법으로 발전해가며 피싱 범죄를 일으킨다.

향후 지도 학습을 비지도 학습 알고리즘을 사용하여 가족에 한정되어 있지 않고, 사람과 기계음의 차이를 탐지하여 어떠한 사람이라고 딥보이스 음성에 대해서는 탐지할 수 있도록 할 계획이다.

5. 참고 자료

- (1) Reshma Sunil, Partima Mer, Anjali Diwan, Rajesh Mahadeva, Anuj Sharma, “Exploring autonomous methods for deepfake detection: A detailed survey on techniques and evaluation”, Heliyon, Vol.11, No.3, ‘2025.02.15.
- (2) Soowoon Kim, Sungtaek Lee, “Development of Voice Phishing Damage Prevention Service Misusing Deep Voice”, The Journal of Korean Intitute of Communications and Information Sciences, Vol.47, No.10, 1677–1685, ‘22.10.
- Harsh Chotaliya, Mohammed Adil Khatri, Shubham Kanojiya, Mandar Bivalkar, (3)“DeepFake Detetection Techniques using Deep Neural Networks(DNN)”, IEEE Xplore, ‘24.03.
- (4)Tushar Kapoor, Abhi Gaur, Tushar Rajora, Yogya Prashar, Jyoti Parashar, “Deepfake Audio Detection System”, iJRASET, ‘24.05.07.
- (5)Run Wang, Felix Juefei–Xu, Yihao Huang, Qing Guo, Xiaofei Xie, Lei Ma, Yang Liu, “DeepSonar:Towards Effective and Robust Detection of AI–Synthesized Fake Voice”, arXiv:2005.13770, ‘20.08.15.

6. 별첨

6.1 소개 자료

2025 정보보호학과 졸업작품 전시회

비상구

딥보이스 음성 탐지 시스템 연구

SUMMARY

인공지능 기술이 급속하게 발전하면서 디지털 미디어의 신뢰성을 저하시키는 딥페이크(DeepFake) 기술을 통해, 다양한 유형의 공격 기법이 늘어나고 있다. 음성과 관련된 딥페이크 유형을 중점으로 DeepVoice를 탐지하는 시스템을 제안한다.

머신러닝(RF)과 딥러닝(DNN)을 결합하여, 실제 음성과 딥보이스 간 특징을 효과적으로 학습시켜 모델 정확도를 향상시켰다. 이를 기반으로 딥페이크와 관련된 사이버 보안 피해로부터 안전한 환경을 조성하는 데 도움을 제공할 수 있을 것이라고 기대한다.

FLOWCHART

```
graph LR; User[사용자] --> Training[사용자 음성 학습 인공지능]; Training --> Extraction[사용자의 실시간 통화 음성 추출]; Extraction --> Samples[음성 1, 음성 2, 음성 3]; Samples --> Detection[딥보이스 제작 인공지능]; Detection --> DB[(데이터베이스)]; DB --> Classification[딥보이스 구분 인공지능]; Classification --> Attack[딥보이스 음성 공격 발생]; Attack --> Result[분석 결과];
```

The flowchart illustrates the system's workflow. It begins with a user providing voice data for training an AI model. This model is then used to extract real-time voice from the user's calls. These extracted voice samples are fed into a detection AI model. The detection model's output is stored in a database, which is then used by a classification AI model to distinguish between real and deepfake voices. If a deepfake voice is detected, an attack is triggered, leading to a final analysis result.

2025 정보보호학과 졸업작품 전시회

EXPECTATION

①

사이버 범죄

보이스피싱, 금융 피해 대응

음성 관련 저작권 보호

신분 도용 및 명예 훼손 방지

②

이용률에 따른 정확도 향상

시스템 운영의 효율적인 자원 활용

새로운 보안 인프라 구축

인공지능 학습 시스템 신뢰도 향상

③

기술의 폭넓은 활용

API 제공을 통한 연계 가능

음성 기반 증거 분석 활용 제공

다양한 산업 분야의 가능성

APP UI



현재 사용자의 음성을 학습 중입니다.

이제부터 새로운 음성을 학습할 수 있습니다.

MEMBER



최수민



박우경



이하영

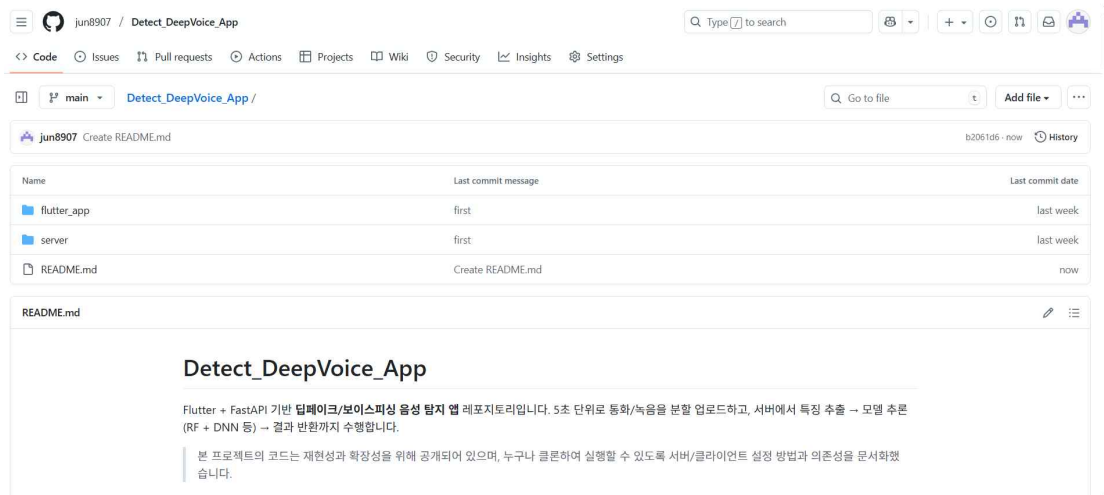


정진호

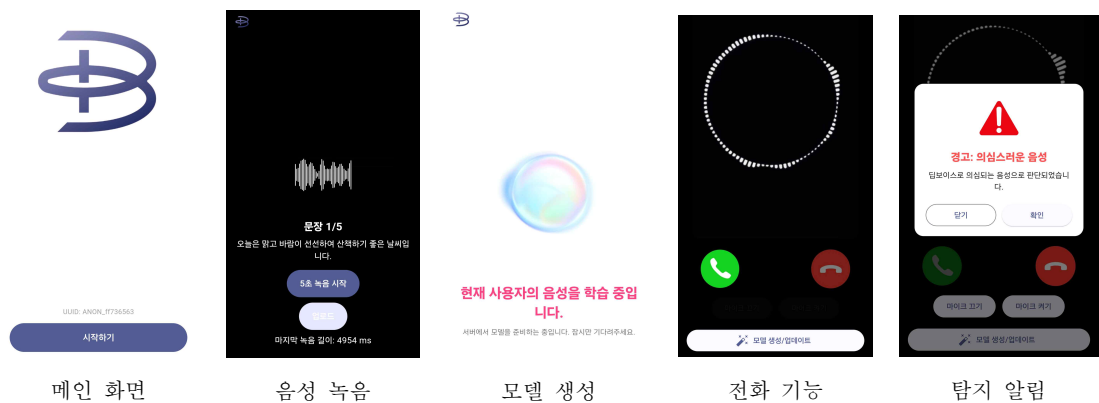


홍준희

6.2 프로젝트 소개



본 프로젝트는 산출물의 개방성과 재사용성을 최우선 가치로 삼았다. 이에 따라 전체 소스 코드를 GitHub 공개 저장소(https://github.com/jun8907/Detect_DeepVoice_App)에 업로드하여 공유하였고, README를 통해 설치·실행 방법, 데이터 준비 절차, 모델 학습/평가 스크립트 사용법을 상세히 문서화하였다. 또한 라이선스와 기여 가이드라인을 명시하여 외부 기여와 2차 활용이 원활히 이루어지도록 하였다.



시연 영상은 다음과 같이 구성되어 있다. 메인 화면 -> 음성 녹음 -> 모델 생성 -> 전화 기능 -> 탐지 알림 순으로 진행되며, 각 단계에 대한 설명은 3.3장을 참고(https://drive.google.com/file/d/1UxE1a1Qz_j73Wmymdo190cJKeZxwWxZw/view?usp=sharing)

6.3 팀 소개



최수민

팀장 최 수 민 (Su-min Choi)

2020 3월~현재 : 중부대학교 정보보호학전공 4학년 재학

맡은 역할 : PM, 피처 분석

<관심 분야> 인공지능, 정보보호



박우경

팀원 박 우 경 (Wu-kyung Park)

2020 3월~현재 : 중부대학교 정보보호학전공 4학년 재학

맡은 역할 : 피처 분석, 머신러닝

<관심 분야> 인공지능, 정보보호



이하영

팀원 이 하 영 (Ha-young Lee)

2020 3월~현재 : 중부대학교 정보보호학전공 4학년 재학

맡은 역할 : 피처 분석, 자료 조사

<관심 분야> 보안컨설팅, 정보보호



정진호

팀원 정 진 호 (Jin-ho Jung)

2020 3월~현재 : 중부대학교 정보보호학전공 4학년 재학

맡은 역할 : 인공지능 모델 학습, 논문 작성

<관심 분야> 인공지능(머신러닝), 정보보호



홍준희

팀원 홍 준 희 (Jun-hee Hong)

2022 3월~현재 : 중부대학교 정보보호학전공 4학년 재학

맡은 역할 : 애플리케이션 개발, 서버 구축

<관심 분야> 디지털포렌식, 정보보호

6.4 발표 자료