© 2017 IJSRSET | Volume 3 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Anti-Spoofing for Text Independent Speaker Verification

[1]Dr. SaravananV, [2]Vetri K P, [3]Udhaya Moorthy MK, [4]Aravind D

[1]Associate Professor, Department of ECE, Jeppiaar SRR Engineering College. Chennai, Tamil Nadu, India
[2,3,4] UG scholars, Department of ECE, Jeppiaar SRR Engineering College., Chennai, Tamil Nadu, India

ABSTRACT

This paper describes the scientific study of vulnerability of automatic speaker verification to various vary of spoofing attacks. We start with radical analysis of the spoofing effects of five speech syntheses and eight voice conversion system and also the vulnerability of three speaker verification system under those attacks. Then we introduce variety of countermeasures to prevent the spoofing attacks from the each noted and unknown attackers. Known attacker's square measure spoofing system those output was used to train the countermeasures, whereas associate unknown assailant is a spoofing system whose output offers to the countermeasures during coaching. Finally we describe benchmark automatic system against human performance on each speaker verification and spoofing deduction task. The main objective of the proposed method is to protect from the spoofing attack for text independent speaker verification.

Keywords : MATLAB, Automatic Speaker Verification (ASV).

I. INTRODUCTION

The main function of automatic speaker verification (ASV), sometimes described as type of voice biometrics, is to accept or reject a claimed identity based on a speech sample. The main two types of the ASV system: text-dependent and text-independent. Text-dependent ASV assumes constrained word content and is normally used in authentication applications because it can deliver the high accuracy required. Text-independent ASV does not place constraints on word content, and is normally used in surveillance applications. For example, in call-center applications, a caller's identity can be verified at the time of course of a natural conversation without forcing the caller to speak a specific passphrase. Moreover, as such a verification process usually tasks place under remote scenarios without any face-to-face contact, a spoofing attack – an attempt to manipulate a verification result by mimicking a target speaker's voice in person or by using computer-based techniques such as voice conversion or speech synthesis – is a fundamental concern. Hence, in this work, we focus on spoofing and anti-spoofing for text-independent ASV.

II. METHODS AND MATERIAL

A. Existing System

This paper describes the first version of a speaker verification spoofing and anti-spoofing database, named SAS corpus. The corpus includes nine spoofing techniques, two of which are speech synthesis, and seven are voice conversion. We design two protocols, one is used for standard speaker verification evaluation, and the other for spoofing materials. Hence, they allow the speech synthesis community to produce spoofing materials incrementally without knowledge of speaker verification spoofing and anti-spoofing. To provide a set of preliminary results, we conducted speaker verification experiments using two state-of-the-art systems. Without any anti-spoofing techniques, the two systems are extremely vulnerable to the spoofing attacks implemented in our SAS corpus.

B. Problem and Drawbacks

In the existing methods, even though ASV systems achieve very good speaker verification performance, they are extremely vulnerable to spoofing attacks. Even the simplest VC-C1 spoofing attack, which only changes the spectral slope of the source speaker, considerably increases the False Alarm Rate (FAR). The more sophisticated attacks using speech synthesis or voice conversion lead to FARs as high as 99.11%.

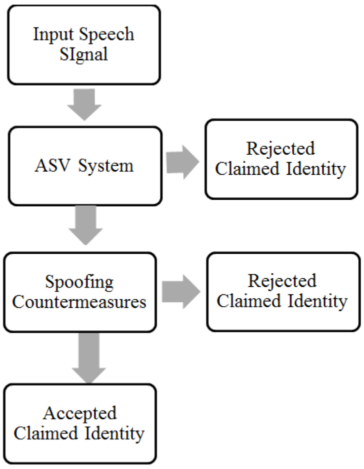
In existence a particular spoofing type (speech synthesis or voice conversion) and often just one variant (algorithm) of that type, then designs and evaluates a countermeasure for that specific, known attack.

Previous studies have been unable to conduct a broader evaluation because of the lack of a standard, publicly-available spoofing database that contains a variety of spoofing attacks.

C. Proposed System

This paper, we present a systematic study of the vulnerability of automatic speaker verification to a diverse range of spoofing attacks. We begin with a thorough analysis of the spoofing effects and attacks of five speech synthesis and eight voice conversion systems, and the vulnerability of three speaker verification systems under those attacks. We then introduce a many number of countermeasures to prevent spoofing attacks from both known and unknown attackers. Known attackers are spoofing systems whose output was used to train the countermeasures, while an unknown attacker is a spoofing system whose output was not available to the countermeasures during training. Finally, we benchmark automatic systems against human performance on both speaker verification and spoofing detection tasks.

D. Overall Diagram


Input Speech SIgnal
ASV System
Rejected Claimed Identity
Spoofing Countermeasures
Rejected Claimed Identity
Accepted Claimed Identity

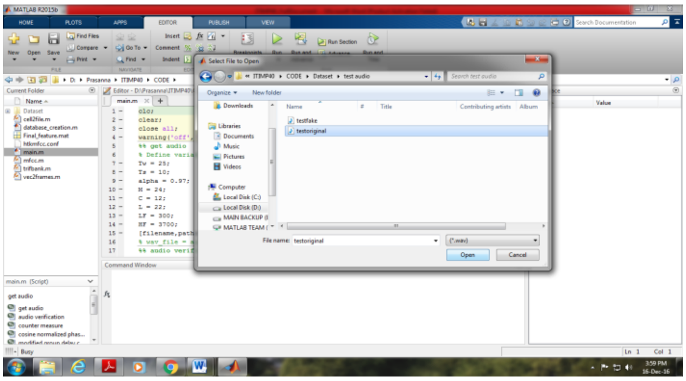
E. Technique Explanation

This paper, each study assumes a specific spoofing type (speech synthesis or voice conversion) and often just one variant (algorithm) of that type, then designs and find out a countermeasure for that particular, known attack. However, in practice it may not be possible to know the exact type of spoofing attack and therefore evaluations of ASV systems and countermeasures under a broad set of spoofing types are desirable. Most, if not all, previous studies have been unable to run a broader evaluation because of the lack of a standard, publicly-available spoofing database that contains a variety of spoofing attacks. To address this problem, we have previously developed a spoofing and anti-spoofing (SAS) database including both speech synthesis and voice conversion spoofing attacks. This database includes spoofing speech from two different speech synthesis systems and seven different voice conversion systems.

III. RESULTS AND DISCUSSION

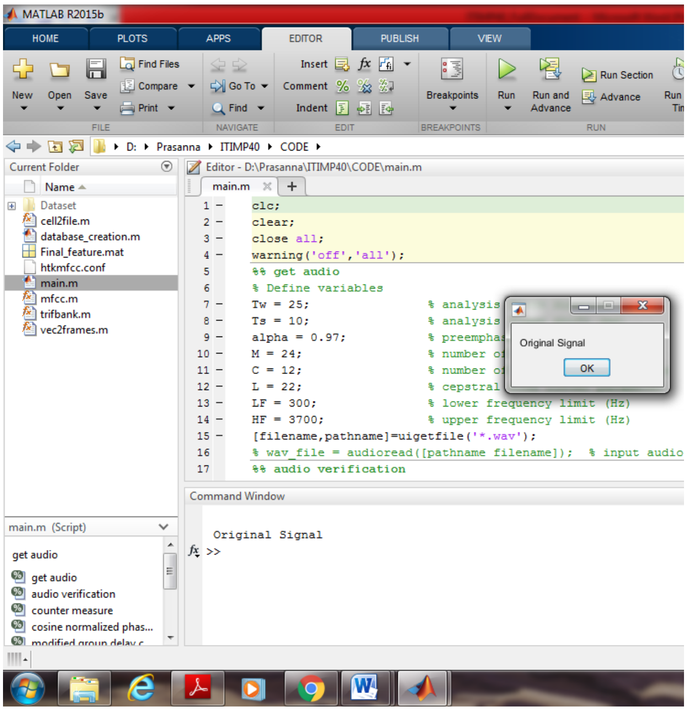
This work, when reporting the false acceptance rates (FARs) and the false rejection rates (FRRs) for a particular spoofing algorithm, the decision threshold is set to achieve the EER operating point for that spoofing algorithm. The ASV systems achieve excellent verification performance. In general, our project suggest that it is easier to spoof male speakers than female speakers in the sense that the FARs for the various spoofing attacks for female speakers are generally lower than that for male speakers.

INPUT FILE:



```
clc;
clear;
close all;
warning('off',
%% get audio
% Define varia
Tw = 25;
Ts = 10;
alpha = 0.97;
M = 24;
C = 12;
L = 22;
LF = 300;
HF = 3700;
[filename,path
% wav_file = a
%% audio verif
```

OUTPUT:



```
clc;
clear;
close all;
warning('off','all');
%% get audio
% Define variables
Tw = 25;                    % analysis
Ts = 10;                    % analysis
alpha = 0.97;               % preempha
M = 24;                     % number o
C = 12;                     % number o
L = 22;                     % cepstral
LF = 300;                   % lower frequency limit (Hz)
HF = 3700;                  % upper frequency limit (Hz)
[filename,pathname]=uigetfile('*.wav');
% wav_file = audioread([pathname filename]);  % input audio
%% audio verification
```

```
Original Signal
>>
```

It mainly uses

- ✓ Forensics and piracy deterrence
- ✓ Surveillance applications
- ✓ Authentication
- ✓ Content filtering

IV. CONCLUSION AND FUTURE WORK

All existing literature surveys that we awareness of in the areas of ASV spoofing and anti-spoofing, report results for just one or two spoofing algorithms, and generally assumes prior knowledge of the spoofing algorithms in order to implement matching countermeasures. As we discussed in, the lack of a large-scale, strong dataset and protocol was a fundamental barrier to progress in this area. We believe that this situation is now rectified, by our release of the standard dataset SAS, combined with the benchmark results presented in this paper.

In future work, to make the system suitable for many other voice authentication applications, spoofing countermeasures for text-dependent ASV must also be developed.

V. REFERENCES

[1]. Z. Wu et al., "SAS: A speaker verification spoofing database containing diverse attacks," in Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP), 2015.

[2]. M. Wester, Z. Wu, and J. Yamagishi, "Human vs machine spoofing detection on wideband and narrowband data," in Proc. Interspeech, 2015.

[3]. P. Golden, "Voice biometrics–The Asia Pacific experience," Biom. Technol. Today, vol. 2012, no. 4, pp. 10–11, 2012.

[4]. M. Khitrov, "Talking passwords: Voice biometrics for data access and security," Biom. Technol. Today, vol. 2013, no. 2, pp. 9–11, 2013.

[5]. B. Beranek, "Voice biometrics: Success stories, success factors and what's next," Biom. Technol. Today, vol. 2013, no. 7, pp. 9–11, 2013.