Replay Attack and Anti-Spoofing for Automatic Speaker Verification

- Lantian Li, Yixiang Chen, Dong Wang, Thomas Fang Zheng

Name : Jay Shah

Student ID : 201501071

Abstract:

Use of voice as important input interface for portable devices and that increasing use of audio interfaces can be mainly attributed to the success of speech recognition technologies. Speech is principle and most inherent form of communication among humans. Because of this fact that speech is primary form of personal identification and it varies person to person. So, people generally have no problem accepting it as biometric. Among various biometric authentication Automatic Speaker Verification (ASV) using speech signal is interesting and useful topic and this is widely use in biometric authentication. This is very useful because speech signals are easily collectable and makes ASV suitable for wide range of applications and speech interface is easy to use and less intrusive. With this advancements come the risk of criminal threats where they are reportedly trying to access sensitive information using voice spoofing techniques. Among all of them replay attacks are real challenge for voice biometrics. For practical scenario of Automatic Speaker Verification (ASV) systems, replay attack poses a true risk. By replaying a pre-recorded speech signal of the genuine speaker, ASV systems tend to be easily fooled. So, there is need of an effective replay detection method. Over-fitting problem caused by variability factors in speech signal is major difficulty in replay detection. An F-ratio probing tool is proposed and three variability factors are investigated using this tool: speaker identity, speech content and playback & recording device. In paper's analysis shows that device is the most influential factor that contributes the highest over-fitting risk. So, there is a frequency warping approach to alleviate the over-fitting problem.