Spoofing Attacks to Voice Verification Systems Using Statistical Speech Synthesis

Dr. Cenk Demiroğlu
Özyeğin University

Abstrac

Speaker verification systems have made tremendous progress in the last decade. The text-dependent speaker verification problem is considered as solved. Indeed, those systems are deployed in commercial applications in many companies around the world. For example, in Turkey, companies such as Turkcell and Avea are using those systems in their call centers. Recent text-independent systems that can authenticate the customers without any specific vocal password are also performing well enough for many applications. Although those systems are much harder to train and expensive to deploy, their commercial applications are beginning to take root especially in the developed countries.

Even though the speaker verification systems perform well, one of their critical weaknesses is their susceptibility to spoofing attacks. That weakness has not been studied as much in the literature. In this talk, I will introduce the state-of-the-art speaker verification system developed at the Ozyegin University speech lab. After discussing the theory behind that system, latest results on benchmark tests will be presented. Then, I will talk about rapid speaker adaptation systems that we developed in the lab for statistical text-to-speech synthesis (TTS) in addition to making a short introduction to statistical TTS. Finally, our attempts to attack on the speaker verification system with our rapid adaptation methods will be presented.

Biography

He obtained an undergraduate degree in Electrical and Electronic Engineering at Bogazici University in 1999 and a PhD from Georgia Institute of Technology in 2005. After PhD, he has worked at the R&D groups of three small companies in USA for five years. He played lead role in the development of a large-vocabulary speech recognition system for three years and the development of an embedded text-to-speech synthesis system for one year.He joined Ozyegin University as an assistant professor at 2009. Dr Demiroglu's research and consulting activities are focused on speech recognition, speech synthesis, speaker verification, speech analysis, and medical applications of the speech processing field.