The 2017 Conference on Computational Linguistics and Speech Processing
ROCLING 2017, pp. 114-115

基於鑑別式自編碼解碼器之錄音回放攻擊偵測系統

A Replay Spoofing Detection System Based on Discriminative Autoencoders

呂滇鼎 Yu-Ding Lu 曹昱 Yu Tsao
中央研究院資訊創新科技研究中心
Research Center for Information Technology Innovation
Academia Sinica

李鴻欣 Hung-Shin Lee 王新民 Hsin-Min Wang
中央研究院資訊科學研究所
Institute of Information Science
Academia Sinica

摘要

在此論文中，我們提出了一個基於鑑別式自編碼解碼器的神經網路模型，對語者辨識系統的錄音回放攻擊進行自動偵測，也就是判斷語者辨識系統所收到的音訊內容是屬於真實的人聲或是由錄音機所回放出來的人聲。在語者辨識領域中，以人為的聲音造假對語者辨識系統進行的攻擊稱之為欺騙攻擊（Spoofing Attack）。有鑑於深度類神經網路模型已被廣泛應用在語音處理相關問題，我們期望能夠應用相關模型在此類問題上。在所提出的鑑別式自編碼解碼器模型中，我們利用模型的中間層來達到特徵抽取的目的，並且提出新的損失函數，使得中間層的特徵將依照資料的標記結果做分群，因此新的特徵將具有能鑑別真偽人聲的資訊，最後再利用餘弦相似度來計算所抽取的特徵與真實的人聲相近與否，得到偵測的結果。我們採用 2017 Automatic Speaker Verification Spoofing and Countermeasures

Challenge（ASVspoof-2017）所提供的資料庫進行測試，所提出的系統在開發數據集上得到了很好的成效，與官方所提供的測試方法相比，其準確度約有 42 % 的相對進步幅度。

關鍵字：語者辨識，語者辨識攻擊，回放攻擊偵測，鑑別式自編碼解碼器，深度類神經網路