УДК 004.934

РАЗДЕЛЬНАЯ КАЛИБРОВКА ПО УСЛОВИЯМ В ЗАДАЧЕ ГОЛОСОВОГО АНТИСПУФИНГА

Самородова М.Э. (университет ИТМО)
Научный руководитель – **Чирковский А.Д.** (ООО «ЦРТ»)

Аннотация. В данной работе исследуется влияние акустических условий, таких как реверберация, на работу системы обнаружения атак повторного воспроизведения при голосовой аутентификации. В качестве подхода по уменьшению влияния внешних условий рассматривается раздельная калибровка по условиям. Актуальность работы обусловлена тем, что в настоящее время слабо исследованы способы адаптации модели антиспуфинга под разные акустические условия.

Введение. За последние годы достигнут значительный прогресс в изучении биометрии лица и голоса. Благодаря успешному использованию глубоких нейронных сетей, работающих с большими объемами данных, современные системы распознавания лиц и голоса способны эффективно справляться с внутриклассовой и межклассовой вариативностью. Кроме того, в настоящее время всё большее распространение получает способ передачи информации посредством речевых сообщений (телефонные сети, интернет-телефония), поэтому повышается интерес к интерфейсам, использующим речь для взаимодействия между пользователем и информационной системой. Также системы голосовой биометрии отличаются от других систем низкой стоимостью внедрения: многие устройства ежедневного пользования (смартфоны, персональные компьютеры) по умолчанию оснащены микрофонами. Всё это делает область голосовой биометрии не только перспективным направлением исследований, но и востребованной технологией в коммерческой среде. Однако широкое распространение этих систем вызвало опасения по поводу безопасности их использования.

Системы верификации по голосу (ASV) могут достигать высокой точности при взаимодействии с мошенниками, которые не прилагают никаких усилий, чтобы замаскировать свой голос и сделать его похожим на целевого говорящего. Однако эти системы уязвимы к более сложным спуфинг-атакам. Под спуфинг-атакой подразумевается попытка обмануть злоумышленником систему верификации личности, посредством представления поддельного или скопированного биометрического образца или путем умышленного изменения собственных биометрических характеристик. Эта проблема вызвала высокий уровень интереса в исследовательском сообществе биометрии.

Спуфинг-атаки могут осуществляться по логическому и физическому каналу. При этом второй способ, то есть физический доступ, более вероятен, поскольку он не требует специальных технических знаний и осуществляется посредством повторного воспроизведения записи целевого диктора. Таким образом, в более реалистичной ситуации злоумышленник будет совершать именно такого рода атаку. Внешние условия атаки могут негативно сказываться на работе системы антиспуфинга и ухудшать качество всей системы верификации, что недопустимо в приложения безопасности, например, таких как доступ к банковским счетам.

Основная часть. Спуфинг-атаки повторного воспроизведения содержат реверберацию помещений, в которых были сделаны записи. Влияние реверберации может негативно сказываться на работе системы антиспуфинга: в некоторых условиях ухудшается общее качество системы, в зависимости от условий также может меняться и порог принятия решения. Вследствие чего система антиспуфинга теряет робастность и не может показывать

одинаковую производительность при различных внешних условиях. Одним из подходов к решению данной проблемы может являться раздельная калибровка по условиям.

Система антиспуфинга является бинарным классификаторов, который делит входные данные на два класса: живая речь (класс genuine) и спуфинг-атака (класс spoof). При этом откалиброванным классификатором является вероятностный классификатор, для которого выходные данные могут быть напрямую интерпретированы как уровень достоверности принадлежности к классу. То есть калибровка системы — это процесс улучшения модели таким образом, чтобы распределение и поведение прогнозируемой вероятности были аналогичны распределению и поведению вероятности, наблюдаемых в обучающих данных.

Таким образом, при делении реверберации по квантилям можно осуществить калибровку систему по условиям, приблизив общий порог FA-FR кривых на известных данных к 0.5 и настроив частные пороги по квантилям реверберации в районе 0.5, сохранив при этом распределение оценок модели на всём диапазоне от 0 до 1.

Выводы. Откалиброванная по условиям система может обладать большей робастностью и в меньшей степени зависит от внешних условий. При этом нетрудно перечислить широкий спектр отраслей, требующих быстрой, надёжной и удобной аутентификации пользователей: доступ к персональному компьютеру или смартфону, доступ к электронной почте, банковские операции, открытие дверей, контроль доступа в помещения, запуск двигателя автомобиля, пересечение государственных границ, а также любое взаимодействие с государственными органами, требующее верификации.