

УДК 378.147:340

**ИССЛЕДОВАНИЕ ТЕХНОЛОГИИ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ
ИНФОРМАЦИОННЫХ СИСТЕМ МЕТОДАМИ ГОЛОСОВОЙ БИОМЕТРИИ****Алпатова А.Е., Терещенко Т.М.**

Восточноукраинский национальный университет им. В.И.Даля

Кафедра компьютерных наук

Аннотация

Алпатова А., Терещенко Т.М. Исследование технологии аутентификации пользователей информационных систем методами голосовой биометрии. Рассмотрены основные способы идентификации личности методами голосовой биометрии. Выделены преимущества и недостатки таких систем. Приведена сравнительная характеристика с другими биометрическими системами.

Общая постановка проблемы

Последнее время появляется все большая необходимость в защите информационных систем. Наиболее надежный метод защиты информации - использование биометрических систем. Голос – такая же неотъемлемая черта человека, как и его лицо или отпечатки пальцев. Распознавание пользователей по голосу весьма удобно и требует от них минимум усилий.

Распознавание голоса - это технология, которая позволяет использовать голос в качестве идентификационного устройства.

Применения технологии распознавания голоса, используемые на протяжении долгого времени, предполагали произнесение каждого слова отдельно. Это позволяло машине определить, где кончается одно слово и где начинается другое. Такие применения технологии распознавания голоса все еще встречаются для управления компьютерными системами.

Исследование

Идентификация по голосу основана на анализе уникальных характеристик речи, обусловленных анатомическими особенностями (размер и форма горла и рта, строение голосовых связок) и приобретенными привычками (громкость, манера, скорость речи).

Идентификация по голосу происходит по следующей схеме: система сравнивает образец голоса, представленного в цифровой форме, с так называемым «голосовым отпечатком», хранящимся в базе данных. «Голосовой отпечаток» - это цифровое изображение уникальных характеристик голоса. Процесс занесения данных в базу данных занимает несколько минут. Система предлагает ответить на несколько вопросов. Ответы являются идентификационными фразами, которые позднее будут использоваться для идентификации человека. Для каждого вопроса пользователь произносит ответ четыре раза. Ответ должен состоять как минимум из трех слогов и длиться больше секунды для того, чтобы создать "голосовой отпечаток". Записанные ответы накладывают друг на друга и убирают посторонний шум. Полученные фразы система сравнивает с ранее сохраненным «голосовым отпечатком».

Человек произносит две или три идентификационные фразы. Если две произнесенные фразы проходят биометрический тест, личность человека идентифицируется. Если одна из этих фраз не принимается, система обращается к третьей произнесенной фразе, и если она принимается системой, то личность пользователя также идентифицируется. Если система не уверена в правильности идентификации пользователя после трех произнесенных

идентификационных фраз, она отказывает пользователю в доступе и отправляет к оператору, или связь просто прерывается.

Существует два типа систем голосовой биометрии:

Текстозависимые

Текстнезависимые

Текстозависимые применяются в системах контроля доступа: для верификации необходимо произнести парольную фразу, которая сравнивается с хранящимися в системе эталонами произнесения для каждого зарегистрированного пользователя. Недостатком таких систем является то, что парольную фразу трудно сохранить в тайне. Современные средства акустического прослушивания (радиожучки и другие подслушивающие устройства) позволяют достаточно успешно осуществлять несанкционированное копирование парольной фразы. Данный недостаток отсутствует в текстнезависимых системах.

Текстнезависимые системы используются, как правило, при решении полицейских задач: скрытая идентификация, криминалистическая идентификация, фоноучеты. Для верификации или идентификации в таких системах может использоваться практически любой фрагмент свободной звучащей речи достаточной длины. Недостатком является то что в таких системах понижается надежность и скорость распознавания.

Первичные параметры речевого сигнала должны обладать следующими свойствами (Рис. 1)

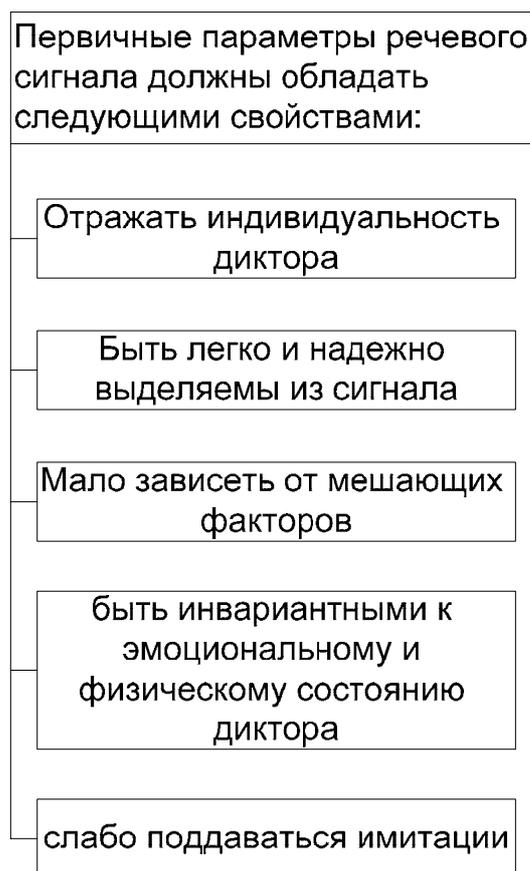


Рисунок 1 – Первичные параметры речевого сигнала

В сравнении с другими биометрическими системами голосовая имеет преимущество по цене и достаточный уровень надежности (Таблица 1). Важно отметить, что только 2% лиц не смогли зарегистрироваться в системе верификации по голосу, в то время как доля отказов

в регистрации для «отпечатка пальцев» составила 4%, а по радужной оболочке глаза - уже 7%.

Таблица 1

Сравнительная характеристика биометрических систем

Биометрическая система Параметры	Отпечаток пальца	Голос	Радужная оболочка	Лицо
Ошибка регистрации	4%	2%	7%	~0%
Номинальное значение вероятности «допуска чужого»	2.5%	0.75%	6%	4%
Номинальное значение вероятности «отвержения своего»	0.1%	0.75%	0.001%	10%
Стоимость системы	Высокая	Низкая	Очень высокая	Высокая

Основными проблемами, стоящими на пути развития систем распознавания речи являются:

1. Большие объемы словарей
2. Шаблоны непрерывной речи
3. Различные акценты и произношения

Объемы словарей определяют степень сложности, требования к вычислительной мощности и надежность систем распознавания голоса. Система может приспособиться к непрерывному потоку речи, но есть еще и строгие семантические правила, которым необходимо следовать, чтобы система смогла понять семантику комбинаций слов в предложениях. Необходимо продолжать основательные исследования, только это позволит «справиться» с такими характеристиками речи, как морфология, акценты, высота звука, скорость, громкость, сливающиеся слова, контекст, артикуляция, лингвистическая информация, синонимы и т. д. Ожидается, что основным направлением развития станет моделирование языков для использования в системах распознавания речи.

Так же существует проблема отделения речевого сигнала от шумового фона. Запись голосового сигнала должна происходить в условиях минимального шумового фона.

Недостатками технологий распознавания личности по голосу, является:

1. Голос, в отличие от папиллярных узоров пальцев или ладоней, меняется с возрастом. Таким образом, клиентам придется периодически обновлять хранящийся в системе эталон речи.

2. На голос оказывает влияние физическое и эмоциональное состояние человека в момент речевого акта. Так, например, система может не узнать по голосу человека, если он находится в состоянии алкогольного опьянения или у него во рту жевательная резинка, или у него отдышка после тяжелой физической работы.

3. Надежность работы системы в значительной степени зависит от качества канала передачи речевого сигнала к системе идентификации, в частности, от таких его характеристик, как частотный диапазон, уровень нелинейных искажений, отношение сигнал/шум, неравномерность частотной характеристики. Наивысшая надежность работы обеспечивается в том случае, когда эталон голоса клиента и его запрос поступают по одному и тому же каналу, например телефонному.

Вывод

В настоящее время получены определенные результаты по синтезу систем идентификации голоса, которые показывают достаточно точную идентификацию и верификацию дикторов. Однако вопрос о создании прецизионных (особо точных) систем идентификации по голосу остается открытым. В связи с этим возникает ряд задач, таких, как исследование точности, устойчивости и разрешающей способности первичных параметров, расширение поля признаков, а также автоматический лингвистический анализ речи.

Список литературы

1. Женило В.Р. Компьютерная фоноскопия. М.: Типография Академии МВД России, 1995, 208 с.
2. Кухарев Г.А. Биометрические системы: Методы и средства идентификации личности человека. – Спб.: Политехника, 2001. – 240 с.
3. Рамишвили Г.С. Автоматическое опознавание говорящего по голосу. - М.: Радио и связь, 1981.-224 с.
4. Сердюков В.Д. Опознавание речевых сигналов на фоне мешающих факторов. Тбилиси, Наука:1987,142 с.
5. <http://www.osp.ru>
6. <http://identityandauthentication.com>