УДК 621.391

© Зиновьев В.Н., Кравцов М.С.
Zinoviev V., Kravtsov M.

АЛГОРИТМЫ ГОЛОСОВОЙ ВЕРИФИКАЦИИ

ALGORITHMS OF VOICE VERIFICATION

Аннотация. *В статье приведен алгоритм формирования голосового отпечатка и алгоритм распознавания. Описанные алгоритмы отличаются повышенной точностью, надёжностью и безопасностью. Также описана система защиты от подмены голоса на основе парольных фраз.*

Annotation. *The algorithm of formation of a voice print and algorithm of recognition is given in article. The described algorithms differ the increased accuracy, reliability and safety. The system of protection against voice substitution on the basis of password phrases is also described.*

Ключевые слова. *Биометрия, голос, верификация, алгоритм.*

Key words. *Biometrics, voice, verification, algorithm.*

Исследование проблемы контроля доступа к различным ресурсам на данный момент занимает значительное место в современной науки. В основу решения данного вопроса положены биометрические технологии. Биометрия предполагает систему распознавания людей по одной или более физических или поведенческих черт[1]. В области информационных технологий биометрические данные используются в качестве формы управления идентификаторами доступа и контроля доступа[1]. В качестве биометрических признаков могут использоваться как уникальные признаки, полученные с рождения, например: ДНК, отпечатки пальцев, радужная оболочка глаза; так и характеристики, приобретённые со временем или же способные меняться с возрастом или внешним воздействием, например: почерк, голос или походка[1]. Широкое распространение данных технологий связано с развитием и удешевлением средств вычислительной техники.

Системы распознавания по голосу имеют ряд преимуществ перед системами, использующими для распознавания другие черты. Самым весомым преимуществом является, отсутствие необходимости применения дополнительного оборудования, так как устройства записи звука на данный момент присутствуют практически в каждом устройстве, начиная от телефона, заканчивая персональным компьютером. Также стоит отметить, что голос является практически неотчуждаемым от его носителя. Но существующие алгоритмы верификации на данный момент являются не точными и имеют большую ошибку первого рода FRR.

Верификация — это подтверждение соответствия конечного продукта предопределённым эталонным требованиям[2]. Таким образом, в процессе верификации мы получаем эталон, с которым впоследствии происходит сравнение. В связи с этим процесс верификации условно можно разделить на два этапа. Первый этап заключается в формировании голосового отпечатка. Второй этап представляет собой непосредственно процесс верификации, т.е. сравнения голоса субъекта доступа с записанным эталоном. Практически все существующие системы верификации имеют одинаковый алгоритм получения голосового отпечатка и алгоритм сравнения. Примерный алгоритм формирования голосового отпечатка существующих систем верификации представлен на рис. 1.

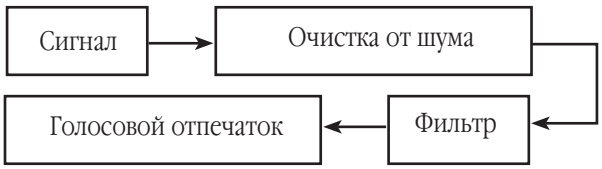

Рис. 1. Алгоритм верификации

Зиновьев Вячеслав Николаевич – доктор технических наук, профессор, профессор кафедры ИТУС, ГБОУВПО «Финансово-технологическая академия», тел. (495)543-36-76;
Кравцов Михаил Сергеевич – аспирант, кафедра ИТУС, ГБОУВПО «Финансово-технологическая академия».

Zinoviev Vyacheslav – doctor of technical sciences, professor, professor of department ITUS, SEIHPE "Financial and technology academy", tel. (495) 543-36-76;
Kravtsov Michael– a graduate student of department ITUS, SEIHPE "Financial and technology academy".

В основе данного алгоритма лежит фильтр, представляющий собой метод получения ключевых характеристик, на основе которых и происходит дальнейшее сравнение[3]. На данный момент большинство исследований направлено на совершенствование существующих и получение новых методов распознавания. Наиболее распространёнными методами являются метод кепстрального преобразования спектра речевых сигналов, метод опорных векторов и метод аппроксимации плотности вероятности в пространстве признаков взвешенной смесью нормальных распределений[4].

Авторами предлагается изменить сам алгоритм формирования голосового отпечатка. Пример алгоритма приведен на рис. 2.

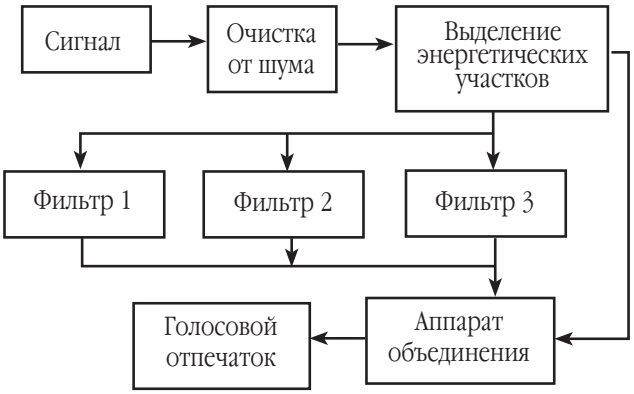

Рис. 2. Предлагаемый алгоритм получения голосового отпечатка

Поступивший сигнал очищается от шума, затем происходит выделение энергетических участков, далее происходит фильтрация и получение ключевых характеристик, потом происходит объединение полученных данных и формирование на их основе голосового отпечатка. В предложенном алгоритме добавлен блок выделения энергетических участков и аппарат объединения, также предлагается использовать несколько фильтров с различными существующими методами распознавания. При этом голосовой отпечаток будет состоять не только из ключевых характеристик, но и из набора энергетических участков и списка фильтров, пример голосового отпечатка приведен на рис. 3.

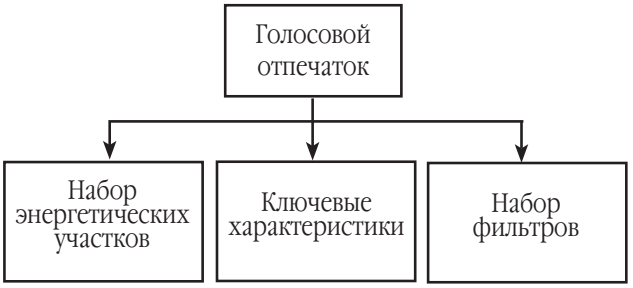

Рис. 3. Голосовой отпечаток

На основании полученного голосового отпечатка строится алгоритм распознавания. Структура алгоритма приведена на рис. 4.

Процесс распознавания состоит из следующей последовательности: поступивший сигнал очищается от

Рис. 4. Предлагаемый алгоритм сравнения

шума, затем происходит проверка заданной парольной фразы, далее сравнение с полученным ранее голосовым отпечатком и в конце принятие решения о соответствии.

Авторами также предложена система защиты от подмены голосового сигнала с помощью звукозаписывающих устройств, с применением парольных фраз. Данная система основана на выделение энергетических участков при этом выбираются наиболее энергетически мощные звуки, так как они менее зависимы от шумов и искажений. В основном это гласные и звонкие согласные, произношение которых хорошо отражает работу голосовых связок и речевого тракта. Эти звуки обязательно имеют ярко выраженную неравномерность спектральной характеристики и именно в них выражена индивидуальная особенность мышечной активности речевого тракта личности[5]. Формируется база данных, состоящая из фраз с определённым набором гласных и согласных, при анализе которых можно получить одинаковый набор энергетических участков, из которых в последующем и будут выделены ключевые характеристики. Помимо этого, для дополнительной защиты от принуждения субъекта доступа к произношению парольной фразы предусмотрено дополнительное слово, при произношении которого происходит блокировка системы.

Предлагаемый алгоритм позволит снизить ошибку первого рода FRR из-за выделения большего количества ключевых характеристик. За счет этого увеличивается точность и надёжность распознавания. Также благодаря предлагаемой системе парольных фраз повышается безопасность верификации, так как подмена голоса субъекта доступа становится невозможна.

Литература

1. Болл Р. М., Коннел Дж. Х., Панканти Ш., Ратха Н. К., Сеньор Э. У., Руководство по биометрии. — М.:Техносфера, 2007, 368с.

2. Синицын С. В., Налютин Н. Ю. Верификация программного обеспечения. — М.:БИНОМ, 2008, 368с.

3. Репалов С.А., Разработка математических моделей и робастных алгоритмов идентификации дикторов по их речи: дис. ... канд. физ.-мат.наук: 05.13.18 / Репалов Сергей Анатольевич. — Ростов-на-Дону, 2003, 140с.

4. Сорокин В.Н., Вьюгин В.В., Тананыкин А.А.. Распознавание личности по голосу: аналитический обзор // Информационные технологии в технических и социально-экономических системах. – Москва, 2012, 30с.

5. Боршевников А. Е. Надежность схем биометрической идентификации, с использованием генерации ключевых последовательностей [Текст] / А. Е. Боршевников // Технические науки: традиции и инновации: материалы междунар. заоч. науч. конф. (г. Челябинск, январь 2012 г.). — Челябинск: Два комсомольца, 2012. — С. 6-8.

6. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – Санкт-Петербург: Наука и Техника, 2004, 284с.

Материал поступил в редакцию 19. 04. 2013 г.