ПРОГРАММНЫЙ МОДУЛЬ ВЕРИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ПО ГОЛОСУ: ВОПРОСЫ НАДЕЖНОСТИ И КАЧЕСТВА

О.Б. Зельманский

Белорусский государственный университет информатики и радиоэлектроники,
кафедра защиты информации
П. Бровки, 6, г. Минск, 220013, Беларусь
телефон: + (37529) 3900914; e-mail: 7650772@rambler.ru

Рассматривается метод реализации программного модуля верификации пользователя по голосу на основе объединения алгоритмов детектирования речи и верификации диктора. Предлагается использование личного кода, настраиваемого порога верификации, системы контрольных фраз, повторной верификация в течение сеанса доступа, повторного произнесение контрольной фразы, с целью повышения надежности и качества программных средств, использующих рассматриваемый модуль.

Ключевые слова – аудио сигнал, верификация, детектирование, речь.

1 ВВЕДЕНИЕ

Сегодня в сфере защиты информации большой популярностью пользуются биометрические методы верификации пользователя. Основу этих методов составляет процесс определения уникальных индивидуальных особенностей человека. Наиболее распространенным является использование отпечатков пальцев, рисунка радужной оболочки глаза, черт лица. Однако, для построения алгоритмов обработки указанных особенностей необходимо использовать специальные средства ввода информации, а именно сканеры отпечатков пальцев и видеокамеры. Следует отметить, что данные устройства сложнее и дороже, чем микрофон. Кроме того, для обработки рисунка радужной оболочки глаза или отпечатков пальцев требуется значительно больше вычислительных ресурсов, чем для обработки аудио сигнала. Таким образом, биометрическая верификация пользователя по голосу является более дешевой и не требовательной к ресурсам вычислительной техники. Принимая во внимание возможность удаленной верификации по голосу, используя средства мобильной и радиосвязи, можно сказать, что разработка алгоритмов верификации на основе голоса и их реализация в виде отдельных программных модулей представляется весьма актуальной. Готовые программные модули верификации пользователя по голосу благодаря невысоким требованиям к вычислительной технике, а так же надежности и быстродействию лежащих в их основе алгоритмов можно встраивать в любые программные средства, в которых необходимо реализовать контроль доступа к информации.

2 ОПИСАНИЕ МЕТОДА

С целью повышения надежности, а так же сокращения количества операций при обработке аудио сигнала непосредственно перед верификацией пользователя необходимо осуществлять детектирование речи [1], а именно выделить из аудио сигнала только речевые фрагменты. Таким образом, значения классификационных параметров, определяющиеся индивидуальными особенностями голоса, будут рассчитываться только для речевых участков, что в свою очередь снизит загруженность вычислительной техники и повысит качество программного средства. При этом для детектирования речи и верификации по голосу возможно использование общего массива значений классификационных параметров сигнала [2], к которым можно отнести параметры, как во временной области, так и в частотной [3].

Наиболее важным этапом верификации пользователя является принятие решения об индивидуальности говорящего. Для этого рассчитанные на речевых фрагментов аудио сигнала значения классификационных параметров сравниваются с эталонными значениями, сформированными в процессе регистрации пользователя. Соответственно, в случае если разница между рассчитанными и эталонными значениями параметров не превышает установленного допустимого порога, называемого порогом верификации, верифицируемому диктору доступ разрешается. Порог верификации определяется исходя из соотношения между ошибками первого и второго рода. К ошибкам первого рода относится принятие злоумышленника за легального пользователя, к ошибкам второго рода относится отказ зарегистрированному пользователю в доступе. В случае, когда требуется максимальная степень защиты, т.е. нельзя пропустить постороннее лицо, необходимо минимизировать ошибки первого рода, при этом максимизировав ошибки второго. В результате легальному пользователю, возможно, придется несколько раз проходить процедуру верификации, в виду того, что увеличится вероятность отказа ему в доступе. Если же необходимо обеспечить беспрепятственный доступ пользователя с первого произнесения пароля, следует минимизировать ошибки второго рода, за счет максимизации ошибок первого рода, принимая во внимание тот факт, что вероятность проникновения злоумышленника возрастает. Таким образом, имеется возможность настраивать про-

граммный модуль верификации по голосу в зависимость от решаемых задач и области применения программного средства.

Тем не менее, наряду с голосовыми параметрами необходимо использование дополнительных параметров, позволяющих повысить надежность программного средства, например уникального личного кода. То есть сначала требуется ввести код, чтобы пройти первый этап верификации, а затем соответствующую этому коду парольную фразу. Целесообразно чтобы эта фраза была ответом на вопрос, задаваемый ЭВМ. С целью повышения стойкости программы к действиям злоумышленника предлагается использовать систему ответов на один и тот же вопрос. Для полного доступа необходимым будет ответ, который логически не связан с вопросом. Если будет произнесен другой ответ, то либо это злоумышленник, либо, в случае если контрольная фраза имеет логическую связь с вопросом, пользователь, который находится под угрозой насилия со стороны злоумышленника. В последнем случае система может предоставить ограниченный доступ к информации и при этом оповестить соответствующую службу. Важно также обеспечить секретность эталонных значений классификационных параметров, вычисленных для контрольных фраз. Для этой цели создается база данных, в которой предусмотрено шифрование информации.

Известным приемом является использование злоумышленником записей голоса пользователя системы [4]. Для того, чтобы избежать возможности использования таких записей, в ходе верификации предлагается несколько раз повторить одну и ту же фразу. Так как человек не может совершенно одинаково дважды произнести одну фразу, то в случае если рассчитанные для этой фразы значения классификационных параметров окажутся одинаковыми, можно сделать вывод об использовании записи голоса пользователя.

Еще одним методом несанкционированного доступа к информации является подмена пользователя после процедуры верификации. В связи с этим возможно использование повторной верификации в течение сеанса доступа. Кроме того, все неудачные попытки пройти процесс верификации должны протоколироваться, речевые участки, анализируемые при этом, сохраняться в отдельный файл для последующего расследования.

3 РЕАЛИЗАЦИЯ

Для программной реализации рассматриваемой системы верификации пользователя по голосу целесообразным представляется использование объектно-ориентированного языка программирования C++. Это обусловлено возможностью разработки C++ классов, выполняющих соответствующие функции. Первоначально необходимо использовать объект класса, выполняющий предварительную подготовку и фильтрацию входного аудио сигнала, его разбиение на временные окна, выделение классификационных параметров сигнала. Далее выполняются функции следующего класса по детектированию речи и формированию речевых участков анализируемого сигнала. После этого запускаются функции объекта класса, в задачи которого входит непосредственная верификация пользователя.

Так же имеется возможность разработки и использования библиотек C++ классов. Например, удобным является создание специальной библиотеки, содержащей классы для работы с аудио устройствами ЭВМ, а так же для обработки входного и выходного аудио сигналов. Подобная библиотека динамически подключается к приложению по мере необходимости использования ее классов, что увеличивает быстродействие приложения. Кроме того, для выполнения стандартных операций над анализируемым сигналом можно использовать стандартные библиотеки функций. Так для вычисления быстрого дискретного преобразования Фурье применяется готовая библиотека, что позволяет избежать ошибок, возникающих при реализации известных и уже реализованных алгоритмов.

4 ВЫВОДЫ

Таким образом, реализация в программном модуле верификации пользователя по голосу рассмотренных механизмов противодействия злоумышленнику обеспечивает высокое качество и надежность программного средства, в котором используется данный модуль.

ЛИТЕРАТУРА

[1] Зельманский, О.Б. Программное средство верификации диктора по голосу: системное проектирование / О.Б. Зельманский // Сборник материалов VII Белорусско-российской научно-технической конференции Технические средства защиты информации. – 2009. – С. 40.

[2] Зельманский, О.Б. Автоматическая верификация диктора по голосу с предварительным детектированием речи / О.Б. Зельманский // Сборник материалов XIII международной научно-технической конференции Современные средства связи. – 2009. – С. 145.

[3] Речевые интерфейсы ЭВС : Учебно-методическое пособие / А.А.Петровский [и др.]. – Минск : БГУИР, 2004. - 51 с.

[4] Каганов, А.Ш. Об использовании относительных просодических и спектральных характеристик в задаче криминалистической идентификации личности по звучащей речи / А.Ш. Каганов // Информационные технологии процессуального доказывания - Москва, 2002. - с. 42-47.