УДК 004.93

Т.Ю. Дорошенко, Е.Ю. Костюченко

Система аутентификации на основе динамики рукописной подписи

Реализованы программное обеспечение и база данных для проведения исследования идентификации пользователя по рукописной подписи, проставляемой при помощи графического планшета. Собрана база подписей для проведения исследования. Сформированы и выделены параметры для проведения аутентификации. Полученные результаты позволяют осуществить реализацию системы для идентификации пользователя по подписи на основе комбинированного подхода, использующего аппараты математической статистики и искусственных нейронных сетей.

Ключевые слова: аутентификация пользователей, динамическая рукописная подпись, графический планшет.

Постановка задачи. Среди систем аутентификации большими перспективами в настоящее время обладают биометрические системы, основанные на поведенческой (динамической) характеристике человека и учитывающие особенности, характерные для подсознательных движений человека в процессе воспроизведения какого-либо действия. К таким методам относится аутентификация по рукописному/клавиатурному почерку, голосу и др. В этом случае дорогостоящее оборудование не является неотъемлемой частью системы, невозможен обход системы за счет изготовления муляжей, а сам способ привычен для человека и не вызывает отторжения. Принципиально важным преимуществом динамических биометрических систем контроля доступа является возможность для личности сохранять в тайне свой биометрический образ (парольную фразу), что на 4–6 десятичных порядков повышает степень защиты, предоставляемой динамическими БСКД относительно статических [1–3].

Разрабатываемое программное обеспечение представляет собой прототип системы аутентификации компьютерной системы по динамике подписи пользователя на графическом планшете. Цель работы – повышение надежности традиционной парольной защиты за счет использования многофакторной аутентификации на основе анализа динамики проставления подписи, проводимого с использованием аппаратов математической статистики и искусственных нейронных сетей.

Основой аутентификации личности по почерку и динамике написания контрольных фраз (подписи) являются уникальность и стабильность динамики этого процесса для каждого человека, характеристики которой могут быть измерены, переведены в цифровой вид и подвергнуты компьютерной обработке. Таким образом, при аутентификации для сравнения выбирается не продукт письма, а сам процесс.

Биометрическую аутентификацию по подписи можно разделить на следующие этапы:

– предъявление пользователем биометрического образа – ввод пароля (подписи) на графическом планшете;

– оцифровка входных электрических сигналов – измерение заданных биометрических параметров в предъявленном образе;

– нормализация входных сигналов, приводящая их к некоторому эталонному значению;

– сохранение в базе данных системы биометрического эталона идентифицируемой личности – построение шаблона (или профиля) пользователя;

– обучение системы;

– сравнение предъявляемого пользователем профиля с сохраненными;

– предсказание уровня ошибок первого и второго рода для полученного биометрического профиля, принятие решения.

Программное обеспечение для съема образа подписи. Важным этапом решения задачи подтверждения подлинности динамической подписи являются получение, анализ и хранение динамических характеристик (первичных параметров) подписей, проставляемых на графическом планшете. В связи с этим создан программный модуль для съема образа подписи.

Основные задачи, решаемые модулем:

– фиксация перемещений пера относительно чувствительной зоны планшета и перехват потока входных данных;

– динамическая отрисовка подписи на специальной панели в режиме реального времени;

– нормализация первичных параметров подписи;

– сохранение нормализованных первичных параметров подписи в базе данных.

Для обеспечения корректного функционирования системы съема подписи с множеством графических планшетов, представленных на рынке, а также для получения всех данных, которые позволяет снимать аппаратное обеспечение, использован стандартизированный программный интерфейс для графических планшетов, датчиков трехмерного положения и других указывающих устройств в Windows – WinTab.

Алгоритм снятия подписи:

1) при вызове функции подписи – открытие контекста устройства ввода, передающего данные в цифровой форме непосредственно к приложению, без подготовки курсора;

2) каждый раз при возникновении события «Приход пакета» (каждые 5 мс, если перо находится в области действия планшета) вызвать обработчик событий, выполнить пункты 3–8;

3) получение серийного номера пакета, вызвавшего событие;

4) получение пакета с серийным номером пакета, вызвавшего событие;

5) нормализация данных пакета;

6) сохранение пакета в массив WintabPacket;

7) изображение точки на специальной панели;

8) при вызове функции сохранения подписи – закрытие контекста устройства ввода, увеличение счетчика массива.

По серийному номеру пакета извлекаются требуемые показатели: координаты положения пера, сила давления пера на поверхность планшета, угол пера по часовой стрелке и угол наклона пера относительно поверхности графического планшета, время снятия показателей.

Анализ снятых первичных характеристик показал, что в некоторых пакетах некорректно устанавливается штамп времени. Об этой же погрешности говорится и в статье П.С. Ложникова, А.В. Еременко [4]. Рассмотрим суть проблемы на примере используемого дигитайзера WACOM Intuos 3, имеющего частоту дискретизации, равную 200 Гц. Это означает, что когда перо находится в области чувствительности дигитайзера, все поступающие от него пакеты должны иметь штамп времени, кратный 5 мс. Однако в единичных случаях наблюдается отклонение этого значения (в отдельных случаях даже нарушается порядок следования пакетов по штампу времени). При этом можно заметить, что ошибка появляется именно в проставлении штампа – все остальные снимаемые характеристики не имеют скачков. Решено пренебречь данным параметром и при вычислении скоростей на отрезках дискретизации использовать заданную производителем частоту дискретизации, равную 5 мс; для упорядочивания пакетов использовать идентификатор пакета pktID.

Еще одной ошибкой (уже аппаратной части графического планшета) является периодическое одновременное (в одном пакете) проставление значений, больших, чем нуль, для параметров давления и координаты положения кончика пера над планшетом по оси Z. Это буквально бы значило, что перо не касается планшета, но оказывает на него давление, что невозможно.

Также особое внимание уделено искажениям, вызванным невозможностью точного воспроизведения подписи одним человеком. К таким искажениям относятся:

– изменение геометрических размеров подписи;

– нестабильность времени воспроизведения подписи;

– изменение угла наклона подписи относительно системы координат.

Используемые алгоритмы для компенсации изменений описаны в автореферате диссертации [5].

При нормализации подписей перед их сохранением в базу данных решаются следующие задачи:

1) удаление нулевых (по параметру давления) значений пакетов в начале и в конце подписи, что предотвращает хранение «мусора» в базе данных, которое впоследствии может снизить информативность сигналов;

2) исправление ошибки «координата Z – давление»;

3) поворот подписи таким образом, чтобы она располагалась параллельно оси абсцисс;

4) нормализация по размеру.

Интерфейс главного окна программы и внешний вид проставляемой подписи для проведения исследования представлены на рис. 1.

Рис. 1. Интерфейс главного окна программы

Реализованный модуль работает под операционной системой Windows, выполнен с использованием среды разработки Microsoft Visual Studio 2010, языка программирования C# и платформы .NET, MySQL Connector, библиотеки WintabDN. Шаблоны для работы с библиотекой WintabDN взяты с электронного ресурса [6].

Формирование вектора биометрических параметров. Точность работы системы аутентификации зависит от размера пространства первичных и вторичных характеристик подписи. Количество первичных характеристик зависит от возможностей аппаратной составляющей системы и определяется количеством степеней свободы, которое описывает число квазинепрерывных характеристик взаимного положения планшета и пера.

Для формирования вектора биометрических параметров (вторичных характеристик) первичные параметры часто подвергаются преобразованию путем вычисления линейных функционалов по полной реализации подписи или по ее фрагментам. Распространенным методом получения вектора биометрических параметров является вычисление дискретного преобразования Фурье с последующим выделением амплитуд гармоник [9, 10].

Таким образом, для получения вторичных характеристик выполняется следующий алгоритм:

1) удаление постоянной составляющей из спектра;
2) увеличение количества точек для получения гладкой кривой;
3) быстрое преобразование Фурье для спектров каждого из параметров;
4) выделение первых семи гармоник – получение амплитуд и частот для каждой гармоники от каждого первичного параметра;
5) нормализация вторичных характеристик по амплитуде максимальной гармоники;
6) проведение статистического анализа, отсев подписей с грубыми отклонениями от среднего значения более чем на 3σ.

База данных для хранения параметров динамической подписи. Для обеспечения хранения характеристик эталонных подписей в одном месте и возможности удобного доступа к ним выполнено инфологическое проектирование и реализована база данных в СУБД MySQL [7]. База данных размещена на сервере кафедры КИБЭВС (93.91.166.75:3306).

Таблицы базы данных и атрибуты:

– пользователи: идентификатор пользователя (PK), фамилия, имя, отчество, дата рождения;

– подписи: идентификатор подписи (PK), идентификатор пользователя (FK), дата и время проставления подписи (проставляется в момент сохранения подписи по времени на сервере), комментарий;

– пакеты: идентификатор подписи (FK, PK), серийный номер пакета (PK), трехмерные координаты *X*, *Y*, *Z* кончика пера относительно планшета, сила нажатия (давление) пера на планшет, угол наклона пера относительно планшета и угол пера по часовой стрелке, временной штамп;

– нормализованные пакеты: идентификатор подписи (FK, PK), серийный номер пакета (PK), нормализованные трехмерные координаты *X*, *Y*, *Z* кончика пера относительно планшета, сила нажатия (давление) пера на планшет, угол наклона пера относительно планшета и нормализованный угол пера по часовой стрелке;

– названия параметров: идентификатор параметра (PK), имя параметра, описание параметра;

– значения параметров: идентификатор подписи (FK, PK), идентификатор параметра (FK, PK), номер гармоники (PK), значение амплитуды гармоники, значение частоты гармоники.

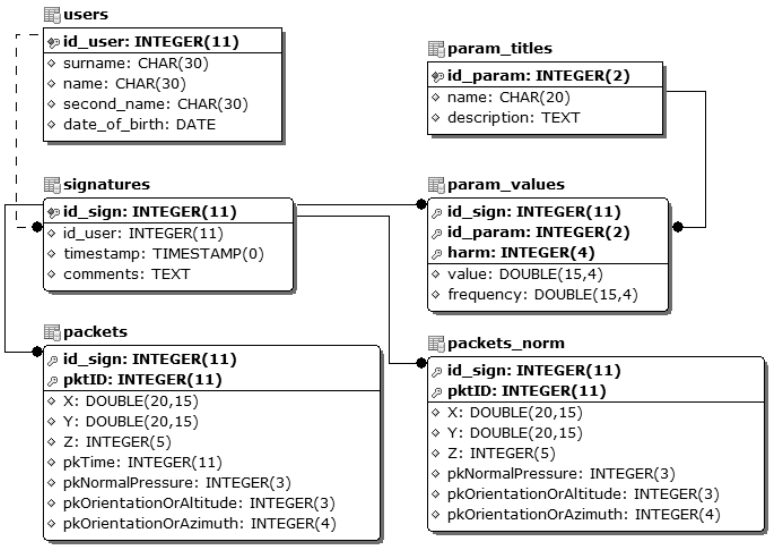

Рис. 2. Концептуальная модель данных

Концептуальная модель данных представлена на рис. 2.

Предоставленные на уровне СУБД права доступа к базе данных: администраторам – полный доступ, пользователям – только INSERT.

Планирование эксперимента. В качестве основных характеристик любой биометрической системы принимают ошибки первого (FAR) и второго (FRR) рода. Первое число характеризует вероятность ложного совпадения биометрических характеристик двух людей, а второе – вероятность отказа доступа человеку, имеющему допуск. Таким образом, встает задача предварительной оценки точности определения ошибок первого и второго рода при идентификации пользователей по динамической подписи.

Из теории вероятностей доверительный интервал для оценки неизвестных вероятностей может быть построен по следующей формуле [8]:

$$p = \frac{n}{t^2 + n}\left(\omega + \frac{t^2}{2n} \pm t\sqrt{\frac{\omega(1-\omega)}{n} + \frac{t^2}{4n^2}}\right). \quad (1)$$

Здесь параметр t определяется уровнем доверительной вероятности на основе функции Лапласа. При уровне доверительной вероятности 0,95 параметр t = 1,96. Кроме того можно воспользоваться методом, изложенным в [12].

Предварительная оценка частоты ошибок первого и второго рода может быть найдена исходя из анализа ошибок аналогов и составляет $\omega_1 = 0{,}01$ для ошибок первого рода и $\omega_2 = 0{,}01$ для ошибок второго рода.

Количество экспериментов по идентификации определяется объемом базы подписей и предварительно составляет 1300 экспериментов по оценке ошибок первого рода и 11700 экспериментов по оценке ошибок второго рода. На настоящий момент в базе содержится 1203 подписи, число ненулевых точек подписи составляет 600–1000.

Подставляя эти данные в формулы, получаем предварительные границы доверительных интервалов для ошибок первого и второго рода: $p_1 \in [0{,}006;\ 0{,}017]$ и $p_2 \in [0{,}008;\ 0{,}012]$. Эти значения позволяют определять вероятность ошибок первого и второго рода с точностью до 0,0055 и 0,002 соответственно. Данный расчет является прикидочным, поскольку самих оцениваемых вероятностей пока нет, однако порядок оценки точности этих значений не изменится.

Заключение. В ходе проделанной работы были получены следующие результаты:

1. Реализован модуль для снятия образа динамической подписи, проставляемой на графическом планшете.
2. Собрана база подписей 12 пользователей суммарным объемом более 1200 подписей.
3. Получены вторичные характеристики для каждой подписи.
4. Получены предварительные оценки, позволяющие спрогнозировать порядок размаха доверительного интервала вероятностей ошибок первого и второго рода при дальнейшем эксперименте, а по сути – точность получаемых оценок вероятностей ошибок.

Следующим этапом исследования является получение оценки информативности параметров для задачи идентификации на основе метода накопленных частот [10], реализованного ранее и адаптированного для возможности идентификации нескольких пользователей, а также с применением подхода оценки информативности параметров при решении задач с использованием искусственных нейронных сетей [11].

Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУР на 2014 год (проект № 1220).

Литература

1. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: ПГУ, 2000. – 188 с.
2. Брюхомицкий Ю.А. Параметрический метод биометрической аутентификации пользователей информационных систем // Информационное противодействие угрозам терроризма. – 2003. – № 1. – С. 42–48.
3. Костюченко Е.Ю. Идентификация по биометрическим параметрам при использовании аппарата нейронных сетей / Е.Ю. Костюченко, Р.В. Мещеряков // Нейрокомпьютеры: разработка, применение. – 2007. – № 7. – С. 39–50.
4. Ложников П.С. Идентификация личности по рукописным паролям / П.С. Ложников, А.В. Еременко // Мир измерений. – 2009. – № 4 (98). – С. 11–17.
5. Сорокин И. А. Формирование системы признаков для идентификации личности по динамике воспроизведения подписи: автореф. дис. ... канд. техн. наук: 05.13.01. – Пенза, 2005. – 22 с.
6. WintabDN-шаблоны [Электронный ресурс]. – Режим доступа: http://sourceforge.net/projects/wintabdn, свободный (дата обращения: 10.02.2014).
7. Кузнецов М.В. MySQL 5 / М.В. Кузнецов, И.В. Симдянов. – СПб.: БХВ-Петербург, 2006. – 1024 с.
8. Гмурман В.Е. Теория вероятностей и математическая статистика: учеб. пособие для вузов. – М.: Высшая школа, 2004. – 479 с.
9. Ложников П.С. Разработка метода идентификации личности по динамике написания слов: автореф. дис. ... канд. техн. наук: 05.13.01. – Омск, 2004. – 22 с.
10. Еременко А.В. Повышение надежности аутентификации пользователей компьютерных систем по динамике написания пароле: автореф. дис. ... канд. техн. наук: 05.13.19. – Омск, 2011. – 20 с.
11. Костюченко Е.Ю. Критерии информативности при обработке биометрических сигналов при помощи нейронных сетей / Е.Ю. Костюченко, Р.В. Мещеряков, А.Ю. Крайнов // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 118–120.
12. Архипов В.А. Технология поиска при решении задач прикладной математики / В.А. Архипов, С.С. Бондарчук, И.Г. Боровской, А.А. Шелупанов // Вычислительные технологии. – 1995. – Т. 4, № 10. – С. 51–62.

Дорошенко Татьяна Юрьевна
Инженер каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: 8-923-408-31-47
Эл. почта: tankem@mail.ru

Костюченко Евгений Юрьевич
Канд. техн. наук, доцент каф. КИБЭВС ТУСУРа
Тел.: 8-923-444-42-24
Эл. почта: key@keva.tusur.ru

Doroshenko T.Y., Kostyuchenko E.Y.

The authentication system based on dynamic handwritten signature

Implemented software and database for the research of user identification, based on handwritten signature, stamped with a tablet. Base of signatures collected for a future research. Formed and isolated characteristics for authentication. The obtained results allow produce the implementations of the system for identify the user by their signatures. Process of identification will be based on combination of approaches using mathematical statistics and artificial neural networks.

Keywords: user authentication, dynamic handwritten signature, graphically tablet.