УДК 681.3

Н.П.Орищенко

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПОСРЕДСТВОМ РУКОПИСНОЙ ПОДПИСИ

Воронежский институт высоких технологий

В статье рассматриваются проблемы, связанные с аутентификацией пользователей на основе их подписей. Отмечены основные методы распознавания таких объектов. Приведена структура модуля для распознавания рукописной подписи.

Ключевые слова: аутентификация, подпись, распознавание, система, алгоритм, метод.

В настоящее время многие направления деятельности в значительной мере направлены на развитие систем обработки и распознавания изображений.

Но, до сих пор при решении задач в этой области возникает ряд сложных проблем. Распознавание изображений находит широкое применение в различных областях – распознавание лиц, объектов, символов, автомобильных номеров, дактилоскопия и других. В этот круг задач так же можно включить распознавание рукописных подписей с целью идентификации их владельца. Данная задача является актуальной и нерешенной.

Рукописные подписи имеют достаточно сложную структуру и мелкую детализацию, всё это представляет большую сложность для решения данной задачи математическими методами и требует больших вычислительных затрат.

Методы распознавания подписи разделяются на два типа по способу получения данных:

Статический метод предполагает, что человек расписывается на бумаге, изображение сканируется или фотографируется, а далее биометрическая система анализирует полученное изображение. Часто этот метод называют «off-line» методом. Статический метод дает меньше информации по сравнению с динамическим методом, так как известны лишь координаты точек.

Динамический метод предполагает, что человек расписывается в графическом планшете, который считывает подпись в режиме реального времени.

Этот метод называют также «on-line» методом. Динамическая информация может содержать в себе следующие характеристики:

- пространственная координата конца пера x(t);
- пространственная координата конца пера y(t);
- давление конца пера на планшет;

- угол движения пера;
- наклон пера.

Сиометрическая идентификация личностей включает в себя несколько этапов. Последовательность действий может выглядеть приблизительно таким образом:

1. Производится считывание биометрических данных пользователей.
2. На основе того, что идет обращение к локальным или внешним базам данных, по заранее сформированным шаблонам с признаками пользователя, происходит установление его личности.
3. Для обращения к базам данных происходит установление списка прав и обязанностей пользователей.
4. Принимают решения, которые зависят от конкретных задач.

Основные задачи, которые решаются с привлечением биометрических систем для проведения процессов идентификации (аутентификации), могут использоваться для:

- определения прав по физическому доступу – для охранных систем: дверной замок или блокировка запуска автомобиля, или пропуск на территорию производственных организаций;
- определения прав по виртуальному доступу – для терминалов в компьютерных или банковских сетях, для систем, связанных с удаленным доступам к ресурсам;
- учета и контроля – в государственных (например, в системах, связанных с контролем, охраной и допуском) или частных (например, в системах, связанных с маркетинговыми исследованиями) организациях.

Основным преимуществом биометрических систем является интерфейсная простота их взаимодействия с клиентом. Поэтому в качестве одного из перспективных направлений для сферы информационной безопасности в течение последнего времени стала биометрическая идентификация (аутентификация). Но при этом, как можно иногда выяснить, далеко не все специалисты имеют полное понятие о биометрии. Вероятно, основной проблемой биометрии является вопрос ее надежности.

Понятие надежности, как правило, разделяют на три большие области. Первую из них регулярно обсуждают сами производители биометрического оборудования.

Речь идет о вероятностном характере производимой биометрическими устройствами идентификации.

Поскольку условия сканирования каждый раз несколько отличаются, а сканируемые части тела или поведенческие рефлексы клиента также не вполне постоянны, можно говорить не о точном совпадении измерения с шаблоном (как это происходит, например, при сравнении с эталоном

вводимого в компьютер пароля), а лишь о величине вероятностной меры правильного отождествления.

Поэтому все биометрические устройства характеризуются параметрами: «вероятность непризнания своего» (то есть вероятность не идентифицировать зарегистрированного пользователя системы) и «вероятность признания своим чужого» (то есть вероятность неверного отождествления постороннего с кем-то из легальных пользователей). Именно эти характеристики биометрических систем и будут рассмотрены ниже в статье.

Речь идет о защищенности систем от сознательного обмана, о способах симулировать объект биометрического сканирования.

Известны способы обмана биометрических систем, которые контролируют доступ на основе отпечатков пальцев. Например, японский криптограф Цутому Мацумото и группа его студентов в Университете Иокогамы (отнюдь не профессионалов-взломщиков) наглядно показали, как с помощью простейшего инвентаря и материалов можно обмануть практически любую из таких систем. Японские студенты проверили 12 коммерческих сканирующих устройств. Каждое из них смогли обмануть, в среднем в четырех случаях из пяти. Специалистам в области биометрии все эти факты были давно известны, однако результаты подобных исследований сознательно замалчиваются.

Выход из положения не является простым, он требует привлечения более сложных в использовании и более дорогих методов биометрии (а лучше – многофункциональную аутентификацию), что сразу ставит под удар саму идею повсеместного распространения биометрических технологий. Приемлемого решения на данный момент можно добиться комбинированной проверкой – считыванием нескольких параметров, например отпечатка пальца и голоса, использованием биометрического контроля вместе со смарткартами и т.п.

Наконец, третьим аспектом проблемы надежности является вопрос сохранности собранной биометрической информации. Для большинства биометрических систем существуют уязвимости по взлому вследствие перехватов, сохранений и последующих воспроизведений данных.

Возможности осуществления, зависят от способов передачи биометрической информации по сетям.

Но в качестве недостатка можно отметить то, что, в биокоде в отличие от безличных кодов-паролей, практически всегда есть намного больше информации, чем это требуется устройству для проверки доступа.

Даже рисунок радужной оболочки глаза, не говоря уж о ДНК- коде, может сообщить специалисту важную информацию о состоянии индивидуума, его врожденных или приобретенных свойствах, в том числе болезнях.

А такая информация, очевидно, является слишком интимной, чтобы давать доступ к ней не только своему лечащему врачу. Возможные злоупотребления очевидны каждому – от проведения дискриминирующих действий при процессах приема на работу до осуществления прямого шантажирования.

Среди систем аутентификации большими перспективами в настоящее время обладают биометрические системы, основанные на поведенческой характеристике человека и учитывающие особенности, характерные для подсознательных движений людей в процессах воспроизведения определенных действий.

К таким методам относится аутентификация по рукописному 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 можно назвать возможности для личностей по сохранению в тайне своих биометрических образов.

Основным достоинством аутентификации пользователей по их биометрическим признакам является:

- трудность фальсификации этих признаков;
- высокая достоверность аутентификации из-за уникальности этих признаков;
- неотделимость биометрических признаков от личности пользователя.

Общим недостатком средств аутентификации пользователей по биометрическим признакам является их более высокая стоимость, что обусловлено необходимостью приобретения дополнительных аппаратных средств.

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
- проведение предсказания уровней ошибок первого и второго рода по полученным биометрическим профилям, принятие решения

Важным этапом решения такой задачи, как подтверждение 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.

На рис.1 приведены основные блоки, входящие в структуру модуля.

Рис. 1 Структура модуля для распознавания рукописной 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.

ЛИТЕРАТУРА

1. Рожкова А.А. Проблемы, связанные с распознаванием речи / Международный студенческий научный вестник. 2015. № 3-3. С. 379.
2. Москальчук Ю.И. Возможности систем управления на предприятиях / Международный студенческий научный вестник. 2015. № 3-3. С. 374-375.
3. Чопоров О.Н., Чупеев А.Н., Брегеда С.Ю. Методы анализа значимости показателей при классификационном и прогностическом моделировании / Вестник Воронежского государственного технического университета. 2008. Т. 4. № 9. С. 92-94.
4. Секушина С.А. Информационные технологии в компании / Международный студенческий научный вестник. 2015. № 3-3. С. 380-381.
5. Луканова О.Г.О развитии информационных технологий на предприятии / Международный студенческий научный вестник. 2015. № 3-3. С. 370.
6. Кулдилова А.А. Компоненты инноваций в организациях / Международный студенческий научный вестник. 2015. № 3-3. С. 368-369.
7. Чопоров О.Н., Наумов Н.В., Куташова Л.А., Агарков А.И. Методы предварительной обработки информации при системном анализе и моделировании медицинских систем / Врач-аспирант. 2012. Т. 55. № 6.2. С. 382-390.
8. Жвелия Л.Р. Характеристики информационных систем управления / Международный студенческий научный вестник. 2015. № 3-3. С. 364-365.
9. Жвелия Л.Р. Применение информационных технологий на предприятии / Международный студенческий научный вестник. 2015. № 3-3. С. 364.
10. Дешина А.Е., Ушкин И.А., Чопоров О.Н. Интегральная оценка общего риска при синтезе иткс на основе параметров риска ее компонентов / Информация и безопасность. 2013. Т. 16. № 4. С. 510-513.
11. Гордиевская К.Ю. Проблемы, касающиеся биометрической идентификации / Международный студенческий научный вестник. 2015. № 3-3. С. 363.

12. Пахомова А.С., Чопоров О.Н., Разинкин К.А. Целенаправленные угрозы компьютерного шпионажа: признаки, принципы и технологии реализации / Информация и безопасность. 2013. Т. 16. № 2. С. 211-214.
13. Львович Я.Е. Многоальтернативная оптимизация: теория и приложения / Воронеж, издательство "Кварта", 2006. 415 с.
14. Львович Я.Е. Принятие решений в экспертно-виртуальной среде / Воронежский ин-т высоких технологий, Российский новый ун-т, Воронежский филиал. Воронеж, 2010. 139 с.
15. Преображенский Ю.П. Оценка эффективности применения системы интеллектуальной поддержки принятия решений / Вестник Воронежского института высоких технологий. 2009. № 5. С. 116-119.
16. http://old.computerra.ru/2002/445/18034/.
17. Мозговой А.А. Проблемы существующих методик оптического распознавания рукописного текста / Вестник Воронежского государственного технического университета. 2012. Т. 8. № 7-1. С. 22-25.
18. Мозговой А.А. Распознавание рукописных текстовых символов, вводимых в мобильные устройства / Вестник Воронежского института высоких технологий. 2011. № 8. С. 48-50.
19. Мозговой А.А. Методика синтеза словаря для задачи автоматического распознавания рукописных слов / Телекоммуникации. 2014. № 5. С. 3-4.
20. Мозговой А.А. Проблемы применения скрытых марковских моделей при распознавании рукописного текста / В мире научных открытий. 2013. № 6 (42). С. 186-198.
21. Мозговой А.А. Предварительная обработка изображений символов с целью улучшения качества последующей скелетизации (утонения) / Вестник Воронежского института высоких технологий. 2013. № 10. С. 156-160.
22. Мозговой А.А. Проблемы извлечения рукописных слов из сканированного изображения / Моделирование, оптимизация и информационные технологии. 2013. № 1. С. 14.
23. Мозговой А.А. Преобразование Хафа в задачах автоматического распознавания рукописного текста / Вестник Воронежского института высоких технологий. 2012. № 9. С. 62-64.

N.P. Orischenko

THE USER AUTHENTICATION IN THE INFORMATION SYSTEM BY MEANS OF A HANDWRITTEN SIGNATURE

Voronezh Institute of High Technologies

The paper discusses the problems associated with users authentication on the basis of their signatures. The basic methods of recognition of such objects are pointed out. The structure of the module for recognition of a handwritten signature is given.

Keywords: authentication, signature, recognition, system, algorithm, method.