УДК 625.8

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЖЕЛЕЗНОДОРОЖНЫХ ОБЪЕКТОВ НА ОСНОВЕ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ПО РУКОПИСНОМУ ПОЧЕРКУ ЧЕЛОВЕКА

С. Е. ПАВЛЮЧИК, С. Н. БЕЛАН
Государственный университет инфраструктуры и технологий, г. Киев, Украина

Постановка проблемы. Тенденция развития современного общества тесно связана с ростом информационных ресурсов, информационных технологий. К тому же огромное количество информации ограниченного доступа переносится, хранится и обрабатывается в информационных системах железнодорожного транспорта, что формирует потребность в обеспечении их информационной защищенности. Вопросы информационной безопасности на современном этапе рассматриваются как приоритетные. Существующие на сегодняшний день средства и методы защиты информации в автоматизированных системах достаточно разнообразны, что отражает многообразие способов и средств возможных несанкционированных действий. Защита информации в информационных системах обеспечивается созданием комплексной системы защиты, одной из главных составляющих которой являются методы защиты от несанкционированного доступа к объектам железнодорожного транспорта. Проблема аутентификации пользователя компьютерной системы со времени появления мультипользовательских систем стала весьма актуальной. Особое место в этой теме занимают биометрические методы, основанные на уникальности биометрической информации, носителем которой является человек [1–3]. Существуют различные биометрические характеристики, которые делятся на статические и динамические. Наиболее точную идентификацию личности дают методы, совмещающие несколько биометрических характеристик, особенно статических и динамических (например, статическое изображение подписи и ее динамическое формирование).

Цель работы. Повышение эффективности методов биометрической идентификации и аутентификации для повышения надежности средств защиты информации в автоматизированных системах на железной дороге с помощью анализа статических изображений и динамики рукописного почерка.

Суть работы. Описан метод биометрический идентификации по изображению рукописного почерка и по динамике его написания.

Для этого фиксируют изображение подписи на бумажном носителе или на специальном планшете, с выхода которого получают кодовую последовательность, описывающую данное изображение. Для сохранения подписи используются специальные ручки или восприимчивые к давлению поверхности. Шаблон создается в зависимости от необходимого уровня защиты. Как правило, количество эталонов, формируемое в режиме обучения, не меньше десяти.

Первоначально полученное изображение утоньшают, т. е. получают его остов и считывают координаты черных пикселей, которые принадлежат изображению подписи. Обычно выделяют два способа обработки данных подписи:

– анализ самой подписи, то есть используется просто система совпадения двух картинок;

– анализ динамических характеристик написания, то есть для аутентификации строится свертка, в которую входит информация по подписи, временными и статистическими характеристикам.

Анализ самой подписи сильно подвержен ошибкам, так как является неточным, а также существует возможность подмены подписи злоумышленником. Так как подпись не может быть всегда одинаковой, этот метод дает большой процент ошибок. В результате этот способ используется в местах, где точность результата не столь важна или процесс аутентификации контролируется. Передвижение пера может осуществляться вдоль одной прямой, по плоскости или в трехмерном пространстве, точность аутентификации растет с увеличением количества осей.

В данном способе важна временна́я характеристика, указывающая на период, потраченный на введение определенной части подписи. Большинство систем аутентификации по рукописному почерку останавливаются на зависимости перемещения пера от времени.

Кроме того, используют и комбинированную (мультимодальную) биометрическую систему аутентификации. В этом случае соединяются несколько типов биометрических технологий, которые

позволяют одновременно учитывать различные характеристики человека. Такой способ является более надежным с точки зрения возможности подделки. Имея графический планшет, можно получить двухмерное или трехмерное (если учитывать давление) изображение подписи. Давление определяют с помощью специальных поверхностей, фиксируют силу нажатия пера во время рукописного ввода. Обработка характерных значений наклона пера производится с помощью сложных подсчетов матрицы коэффициентов двумерного дискретного косинусного преобразования. Все планшеты опрашиваются с конечной частотой, а процесс формирования человеком подписи занимает обычно около 1–2 секунд, потому на одну подпись приходится всего 100–200 точек, по которым ее можно анализировать. Но если пользователь расписывается световым пером, кодируются не только координаты кончика пера, но и сила нажатия (давление) пера на планшет, угол наклона пера по планшету и угол пера по часовой стрелке.

Порядок работы систем динамической аутентификации: преобразование неэлектрических величин (координат конца пера, звуковые давления) в электрические сигналы; оцифровка входных электрических сигналов; масштабирование амплитуд входных сигналов, которое приводит их к некоторому эталонному значению; приведение сигналов к единому масштабу времени; вычисление вектора (матрицы) контролируемых биометрических параметров; определение режимом работы системы совокупности операций, осуществляемых с уже сложившимся вектором параметров.

В данной системе аутентификации по динамическим характеристикам подписи входными параметрами являются зависимости координат конца пера $X(t)$, $Y(t)$, $Z(t)$ от времени в системе координат графического планшета. Планшет может конвертировать эти аналоговые величины в цифровую форму. Данный подход позволяет перейти от анализа изображения к более простому анализу траектории, который ведется по всем трем зависимостям. При попытке обвода подписи динамические характеристики будут явно отличаться от оригинальных. Считанные координаты в качестве эталонных заносят в блок хранения эталонов и придают им идентификатор личности. В режиме идентификации получают подпись идентифицируемого и сравнивают с полученными эталонами.

После получения остова изображения приступают к расчету графических характеристик подписи. Используется матрица расстояний как основная графическая характеристика. Распознается образ и образ-эталон, которые, как правило, отличаются друг от друга масштабом, поворотом и смещением. Сравнение нового образа с эталоном происходит за одну итерацию сразу после вычисления его инварианта. В работе также остов выделяется с помощью клеточных технологий на основе клеточных автоматов с ортогональным покрытием. Для анализа предложенного метода было проведено исследование, которое позволило подтвердить надежность функционирования. Для этого были использованы несколько ключевых фраз, сформированных различными пользователями. Также использовалась программа, реализующая данный метод.

Вывод. Метод биометрической аутентификации личности по рукописному почерку позволяет осуществлять реализацию системы для идентификации пользователя по подписи на основе комбинированного подхода, используя аппараты математической статистики. Данный метод приемлем на объектах железнодорожного транспорта в подразделениях, где работают с оперативной и конфиденциальной информацией и т. д. Идентификацию по подписи нельзя использовать везде, в частности, этот метод не подходит для ограничения доступа в помещение или для доступа в компьютерные сети. Основное преимущество подписи по сравнению с использованием, например, дактилоскопии в том, что это распространенный и признанный способ подтверждения своей личности.

Список литературы

1 **Иванов, А. И.** Биометрическая идентификация личности по динамике подсознательных движений / А. И. Иванов. – Пенза : Изд-во Пенз. гос. ун-та, 2000. – 188 с.

2 **Болл, Р.** Руководство по биометрии / Р. Болл, Дж. Коннел. – М. : Техносфера, 2007.

3 **Лапина, Т. И.** Способ биометрической аутентификации пользователя по рукописному почерку в системах контроля доступа / Т. И. Лапина, В. А. Милых, Д. В. Лапин // Информационно-измерительные и управляющие системы. – 2011. – № 9:11. – С. 40–43.