УДК 343.982.3

П.А. ФИЛОНЕНКО

АНАЛИЗ ИНФОРМАЦИОННЫХ ПРИЗНАКОВ ОТПЕЧАТКОВ ПАЛЬЦЕВ И СКАНИРУЮЩИХ УСТРОЙСТВ

Введение

В наше время пароли, персональные идентификационные номера и специальные идентификационные карточки стали жизненной необходимостью. Таким образом, человек должен хранить в своей памяти огромное количество различных комбинаций цифр и букв.

Чтобы облегчить участь современного человека, компании, специализирующиеся на производстве компьютеров, начали заниматься разработкой биометрических технологий. Биометрия – эта наука, изучающая возможности использования различных характеристик человеческого тела (будь то отпечатки пальцев или уникальные свойства человеческого зрачка или голоса) для идентификации каждого конкретного человека. Пользуясь биометрическими технологиями, человек никогда не сможет забыть необходимый ему пароль или код, поскольку его большой палец, голос или зрачок глаза всегда находятся с ним [1].

Отпечаток пальца образует так называемые папиллярные линии на гребешковых выступах кожи, разделенных бороздками. Из этих линий складываются сложные узоры (дуговые, петлевые и завитковые), которые обладают свойствами индивидуальности и неповторимости, что позволяет абсолютно надежно идентифицировать личность. Хотя процент отказа в доступе уполномоченных пользователей составляет около трех процентов ошибочного доступа – меньше одного к миллиону. Преимущества доступа по отпечатку пальца – простота использования, удобство и надежность. Весь процесс идентификации занимает мало времени и не требует усилий от тех, кто использует данную систему доступа [2]. Исследования также показали, что использование отпечатка пальца для идентификации личности является наиболее удобным из всех биометрических методов. Вероятность ошибки при идентификации пользователя намного меньше в сравнении с другими биометрическими методами [3]. Кроме того, устройство идентификации по отпечатку пальца не требует много места на клавиатуре или в механизме.

В каждом отпечатке пальца можно определить два типа признаков – глобальные и локальные.

Глобальный признак отпечатка пальца

Глобальные признаки – те, которые можно увидеть невооружённым глазом (рис. 1) [4]:

- Папиллярный узор. Область образа – выделенный фрагмент отпечатка, в котором локализованы все признаки.
- Ядро – пункт, локализованный в середине отпечатка или некоторой выделенной области.
- Пункт "дельта" – начальная точка. Место, в котором происходит разделение или соединение бороздок папиллярных линий, либо очень короткая бороздка (может доходить до точки).
- Тип линии – две наибольшие линии, которые начинаются как параллельные, а затем расходятся и огибают всю область образа.
- Счётчик линий – число линий на области образа, либо между ядром и пунктом "дельта".

На рис. 1 представлены следующие типы узоров. С 1 по 4 – узоры типа «петля» (левая, правая, центральная, двойная), 5 и 6 – узоры типа «дельта» или «дуга» (простая и острая), 7 и 8 – узоры типа «спираль» (центральная и смешанная))

Метод на основе глобальных признаков.

Выполняется обнаружение глобальных признаков (ядро, дельта). Количество этих признаков и их взаимное расположение позволяет классифицировать тип узора. Окончательное

распознавание выполняется на основе локальных признаков (число сравнений получается н несколько порядков ниже для большой базы данных).

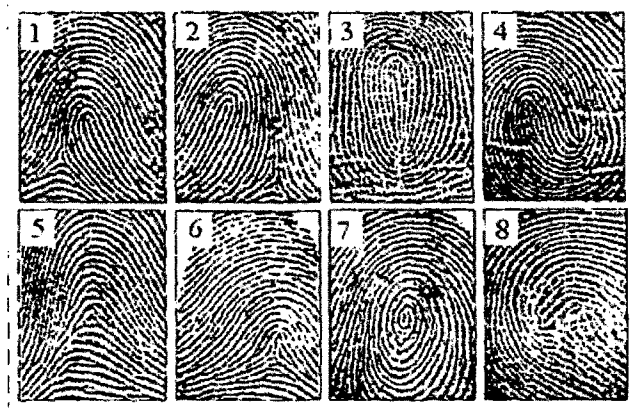

Рис.1

Локальный признак отпечатка пальца

Другой тип признаков – локальные. Их называют минуциями – уникальные для каждог отпечатка признаки, определяющие пункты изменения структуры папиллярных лини (окончание, раздвоение, разрыв и т.д.), ориентацию папиллярных линий и координаты в эти пунктах. Каждый отпечаток содержит до 70 минуций (рис. 2).

Рис. 2

На рис. 2 представлен отпечаток пальца на котором отмечены следующие признаки: две линии – "тип линии"; то, что между ними – может выступать в качестве области образа, не обычно берётся вся площадь отпечатка; окружность слева – пункт "дельта"; окружность ниже – ядро; квадратими выделены некоторые минуции. Папиллярный узор – левая петля.

Практика показывает, что отпечатки пальцев разных людей могут иметь одинаковые глобальные признаки, но совершенно невозможно наличие одинаковых микроузоров минуций. Поэтому глобальные признаки используют для разделения базы данных на классы и на этапе аутентификации. На втором этапе распознавания используют уже локальные признаки.

Для использования локальных признаков прибегают к этапам сравнения двух отпечатков:

- Этап 1. Улучшение качества исходного изображения отпечатка. Увеличивается резкость границ папиллярных линий.
- Этап 2. Вычисление поля ориентации папиллярных линий отпечатка. Изображение разбивается на квадратные блоки, со стороной больше 4 пикселей и по градиентам яркости вычисляется угол t ориентации линий для фрагмента отпечатка.
- Этап 3. Бинаризация изображения отпечатка. Приведение к чёрно-белому изображению (1 bit) пороговой обработкой.

– Этап 4. Утончение линий изображения отпечатка. Утончение производится до тех пор, пока линии не будут шириной 1 пиксель (рис. 3).

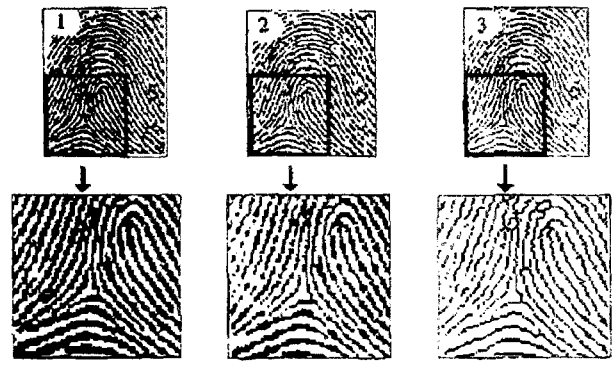

Рис. 3

– Этап 5. Выделение минуций. Изображение разбивается на блоки 9x9 пикселей. После этого подсчитывается число чёрных (ненулевых) пикселей, находящихся вокруг центра. Пиксель в центре считается минуцией, если он сам ненулевой, и соседних ненулевых пикселей один (минуция "окончание") или два (минуция "раздвоение") (рисунок 4).

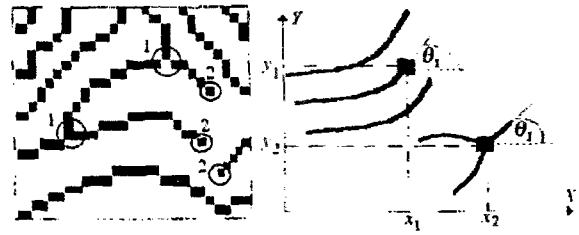

Рис. 4

Координаты обнаруженных минуций и их углы ориентации записываются в вектор:

$$W(p) = [(x_1, y_1, t_1), (x_2, y_2, t_2) \ldots (x_p, y_p, t_p)],$$

где p – число минуций. При регистрации пользователей этот вектор считается эталоном и записывается в базу данных. При распознавании вектор определяет текущий отпечаток (что вполне логично).

– Этап 6. Сопоставление минуций. Два отпечатка одного пальца будут отличаться друг от друга поворотом, смещением, изменением масштаба и/или площадью соприкосновения в зависимости от того, как пользователь прикладывает палец к сканеру. Поэтому нельзя сказать, принадлежит ли отпечаток человеку или нет на основании простого их сравнения (векторы эталона и текущего отпечатка могут отличаться по длине, содержать несоответствующие минуции и т.д.). Из-за этого процесс сопоставления должен быть реализован для каждой минуции отдельно.

Этапы сравнения:

– Регистрация данных.

– Поиск пар соответствующих минуций.

– Оценка соответствия отпечатков.

При регистрации определяются параметры аффинных преобразований (угол поворота, масштаб и сдвиг), при которых некоторая минуция из одного вектора соответствует некоторой минуции из второго.

При поиске для каждой минуции нужно перебрать до 30 значений поворота (от -15 градусов до +15), 500 значений сдвига (от -250 пкс. до +250 пкс. хотя, конечно, границы выбирают и поменьше) и 10 значений масштаба (от 0,5 до 1,5 с шагом 0,1). Итого до 150 000 ша-

гов для каждой из 70 возможных минуций. (На практике, все возможные варианты не перебираются – после подбора нужных значений для одной минуции их же пытаются подставить и к другим минуциям, иначе было бы возможно сопоставить практически любые отпечатки друг другу).

Оценка соответствия отпечатков выполняется по формуле

$$K = (D * D * 100\%)/(p * q),$$

где D – количество совпавших минуций, p – количество минуций эталона, q – количество минуций идентифицируемого отпечатка). В случае, если результат превышает 65%, отпечатки считаются идентичными (порог может быть понижен выставлением другого уровня бдительности).

Если выполнялась аутентификация, то на этом всё и заканчивается. Для идентификации необходимо повторить этот процесс для всех отпечатков хранящихся в базе данных, затем выбирается пользователь, у которого наибольший уровень соответствия (разумеется, его результат должен быть выше порога 65%).

Анализ существующих сканеров отечатка пальца

Устройства считывания отпечатков пальцев сейчас находят различные применения. Их устанавливают на ноутбуки, в мыши, клавиатуры, флеш накопителя, а также применяют в виде отдельных внешних устройств и терминалов, продающихся в комплекте с системами AFIS (Automated fingerprint identification systems – системы автоматизированной идентификации отпечатков пальцев).

Несмотря на внешние различия, все сканеры можно разделить на несколько основных видов (см. таблицу):

- оптические;
- полупроводниковые (меняют свойства в местах контакта);
- ультразвуковые (ультразвук возвращается через различные промежутки времени, отражаясь от бороздок или линий).

Сканеры отпечатков пальцев прошли действительно долгий путь к улучшению. Современные системы оснащены различными датчиками (температуры, силы нажатия и т. п.), которые повышают степень защиты от подделок. С каждым днем системы становятся все более удобными и компактными. Большинство компаний производят готовые системы, которые оснащены всем необходимым, включая программное обеспечение. Интеграторам в этой области просто нет необходимости собирать систему самостоятельно, поскольку это невыгодно и займет больше времени и сил, чем купить готовую и уже недорогую при этом систему, тем более выбор будет действительно широк.

Стандарты для использования отпечатков пальцев

Сейчас в основном используются стандарты ANSI и ФБР США. В них определены следующие требования к образу отпечатка:

- каждый образ представляется в формате несжатого TIF;
- образ должен иметь разрешение не ниже 500 dpi;
- образ должен быть полутоновым с 256 уровнями яркости;
- максимальный угол поворота отпечатка от вертикали не более 15 градусов;
- основные типы минуций – окончание и раздвоение.

Обычно в базе данных хранят более одного образа, что позволяет улучшить качество распознавания. Образы могут отличаться друг от друга сдвигом и поворотом. Масштаб не меняется, так как все отпечатки получают с одного устройства.

На сегодняшний день разработаны и приняты международные стандарты, которые облегчают решение поставленной задачи[6]:

- ISO/IEC 7816-11. Personal Verification Through Biometric Methods.
- ISO/IEC 19794-2. Finger Minutiae Data.

ISO/IEC 19794-4. Finger Image Data.

Разновидность технологии	Сущность	Достоинства	Недостатки
Оптическая (на отражение)	Для захвата оптического изображения отпечатка пальца используется CMOS или CCD матрица	-	Трудность различения живого пальца и его имитации; чувствительность к загрязнениям.
Оптическая (на просвет)	Кончик пальца освещается со стороны ногтя. Прошедший через палец свет попадает на линзу датчика и далее на оптический сенсор, анализирующий характеристики поглощения света живыми тканями. Этот способ разработан компанией Mitsubishi Electric Corp.	Высокая надежность считывания и устойчивость к обману; не требуется контакт пальца с поверхностью датчика	Сложность изготовления
Емкостная	Кончик пальца помещается напротив массива элементов, чувствительных к емкости. Различия в диэлектрике между гребнем (в основном вода) и впадиной (воздух) позволяют их идентифицировать и построить образ отпечатка.	Один из наиболее популярных методов вследствие его надежности и низкой стоимости	Уязвимость от электростатического разряда (ESD); возможность обмана искусственным кончиком пальца.
Радио	Кончик пальца возбуждается радиоволной низкой интенсивности. В этом случае он действует как передатчик, а различие расстояний между гребнями и впадинами может быть обнаружено массивом соответственно настроенных антенн. Необходимо, чтобы кончик пальца контактировал с областью излучения датчика (по его периферии).	Поскольку анализируются физиологические свойства кожи, очень сложно обмануть такой датчик искусственным пальцем.	Неустойчивая работа при плохом контакте пальца с передающим кольцом, которое может стать некомфортно горячим
Давление	Массив чувствительных к давлению пикселей на основе пьезоэлектрических элементов преобразует давление гребней пальца в электрические импульсы.	-	Низкая чувствительность, срабатывание от имитации пальца, повреждение при чрезмерном давлении
MEMS	Кончик пальца анализируется множеством микроэлектромеханических элементов.	-	Высокая вероятность ошибки; возможность обмана имитацией;
Тепловая	Использование пироэлектрического материала для преобразования различия температуры в напряжение. Тепловой датчик на основе массива элементов из такого материала измеряет разницу температур между элементом под гребнем и элементом под впадиной кончика пальца.	Устойчивость к электростатическому разряду; отсутствие какого-либо воздействия на палец; работа в широком диапазоне температур; невозможность обмана с помощью имитации пальца.	Тепловой образ на датчике сохраняется короткое время ~0,1 *с*, поскольку при касании датчика быстро наступает тепловое равновесие

BioAPI является стандартом BioAPI Consortium, разработанным специально для унификации программных интерфейсов программного обеспечения разработчиков биометрических устройств. На данный момент принятым за основу стандартом является версия стандарта 1. которая вышла в марте 2001 года и была реализована под Windows. Пока ещё не вышла е версия под платформы Unix (Linux), но, насколько можно судить по сообщениями BioA Consortium, разработка ведётся давно и уже был период бета-тестирования среди члено консорциума. Согласно статистике сайта консорциума, более 90 биометрических производителей уже заявили о совместимости своих продуктов и решений со стандартом BioAPI.

CBEFF (Common Biometric Exchange File Format) – единый формат представления биометрических данных, который предлагается для замены биометрических форматов, используемых производителями различных сегментов биометрического рынка в своём оборудовании и программном обеспечении. При создании CBEFF были учтены все возможные аспекты его применения, в том числе криптография, многофакторная биометрическая идентификация и интеграция с карточными системами идентификации.

AAMVA Fingerprint Minutiae Format/National Standard for the Driver License/Identificatio Card DL/ID-2000, американский стандарт на формат представления, хранения и передачи отпечатков пальцев для водительских прав. Совместим со спецификациями BioAPI и стандартом CBEFF.

ANSI/NIST-ITL 1-2000 Fingerprint Standard Revision – американский стандарт, определяющий общий формат представления и передачи данных по отпечаткам пальцев, лицу, нательным шрамам и татуировкам для использования в правоохранительных органах США.

Выводы

Анализ информационных признаков является неотъемлемой частью системы идентификации личности по отпечаткам пальцев, предназначенной для обнаружения сходства между двумя изображениями отпечатка пальца. В результате распознавания можно установить личность человека, приложившего палец, что может использоваться при входе в систему. Посредством глобальных и локальных признаков удается значительно понизить уровень влияния смещения и переноса отпечатка пальцев, а также шумов и искажений в изображении. Большое количество разработанных и введенных в действие стандартов дает возможность дальше изучать и применять на практике биометрическую характеристику человека, а именно – отпечатки пальцев.

Список литературы 1. *Биометрические* технологии – альтернатива персональным идентификационным номерам и паролям. Точка доступа: http://www.k2kapital.com/archives/research/rs20000508.html 2. *Alonso-Fernandez. F.* Combining Multiple Matchers for fingerprint verification: a case study in BioSecure Network of Excellence / F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, H. Fronthaler, K. Kollreider, J. Bigun // Annals of Telecommunications, Multimodal Biometrics. – Mallorca, Spain. – 2007. – P. 357-379. 3. *Завгородний В.И.* Комплексная защита информации в компьютерных системах : учеб. пособие. – М. Логос, 2001. – 264 с. 4. *Bazen, A.* Segmentation of fingerprint images / A. Bazen, S. Gerez Proc.Workshop on Circuits Systems and Signal Processing. – Basel: T&Y. – 2001. – P. 276–280. 5. *Biometric* Standards Activity. Точка доступа: http://www.biometrics.org/standards.php.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 11.07.201