УДК 519.7

ОМРИ КАРИМ

ПОСТРОЕНМЕ АЛГОРИТМА РАСПОЗНАВАНИЯ ОТПЕЧАТКОВ ПАЛЬЦЕВ ДЛЯ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

Разрабатывается алгоритм системы контроля доступа на основе отпечатков пальцев. Многолетний опыт применения и интенсивные разработки метода идентификации по отпечаткам пальцев привели к тому, что в настоящее время он рассматривается как наиболее надежный способ идентификации личности. Анализируются существующие методы распознавания и разрабатывается структурная схема системы контроля доступа на основе отпечатков пальцев.

1. Введение

За последние годы интерес к биометрической идентификации значительно вырос, так как с развитием современных технологий появилась возможность быстрого и точного определения уникальных физиологических данных человека. Такого рода идентификация нашла широкое применение в современных биометрических системах контроля и управления доступом (СКУД), которые обладают рядом существенных преимуществ перед традиционными СКУД, основанными на использовании идентификационных ключей (магнитных карт, электронных ключей и пр.) [1, 2]. Перечислим главные преимущества биометрических СКУД:

– исключается возможность несанкционированного использования ключей;

– обеспечивается высокая степень защиты от имитации;

– отпадает необходимость обязательного ношения ключей;

– исключается влияние человеческого фактора (потеря или порча ключа, забывчивость, передача ключей третьим лицам и т.п.);

– отсутствуют затраты на изготовление новых ключей, замену или восстановление существующих.

Наибольшее распространение в биометрических СКУД получил дактилоскопический метод (анализ отпечатков пальцев), который уже длительное время успешно используется в криминалистике. Выбор именно этого метода является разумным компромиссом между требованиями по достаточной надёжности, экономичности и скорости идентификации.

Дактилоскопический метод идентификации базируется на том, что не существует людей с одинаковыми отпечатками пальцев (даже у близнецов они различны), а папиллярный узор, сформировавшись на эмбриональном уровне, не меняется с возрастом и восстанавливается после кожных повреждений. Кожа человека имеет определённые температурные и

электрические характеристики, поэтому дактилоскопические данные могут быть получены не только оптическим, но и термическим и ёмкостным способами или на основе различных сочетаний этих трёх способов. Такое разнообразие способов реализации делает дактилоскопический метод идентификации более доступным, универсальным и актуальным [3, 4].

Целью исследования является разработка алгоритма распознавания на базе известных методов сканирования отпечатков пальцев для систем контроля доступа. Для достижения поставленной цели необходимо решить следующие задачи:

- проанализировать аналогичные автоматизированные системы контроля доступа;
- определить основные подходы к построению подобного рода систем;
- провести анализ существующих методов распознавания личности по отпечаткам пальцев.

2. Анализ методов идентификации по отпечаткам пальцев

Идентификация по отпечаткам пальцев – на сегодня самая распространенная биометрическая технология. По данным International Biometric Group, доля систем распознавания по отпечаткам пальцев составляет 52% от всех используемых в мире биометрических систем.

Во второй половине XX века в связи с появлением новых технических возможностей распознавание по отпечаткам пальцев начало выходить за рамки использования только в криминалистике и нашло свое применение в самых различных областях информационных технологий; в первую очередь такими областями стали:

– системы управления доступом;
– информационная безопасность (доступ в сеть, вход на ПК);
– учет рабочего времени и регистрация посетителей;
– системы голосования;
– проведение электронных платежей;
– аутентификация на Web-ресурсах;
– различные социальные проекты, где требуется идентификация людей (благотворительные акции и т. д.);
– проекты гражданской идентификации (пересечение государственных границ, выдача виз на посещение страны и т.п.).

В автоматизированном распознавании отпечатков пальцев, в отличие от традиционной дактилоскопии, возникает гораздо меньше проблем, связанных с различными внешними факторами, влияющими на сам процесс распознавания.

Качество получаемого со сканера изображения папиллярного узора пальца является одним из основных критериев, от которого зависит избираемый алгоритм формирования свертки отпечатка пальца и в конечном итоге идентификации человека.

В настоящее время выделяют три класса алгоритмов сравнения отпечатков пальцев:

1. Корреляционное сравнение – два изображения отпечатка пальца накладываются друг на друга и подсчитывается корреляция (по уровню интенсивности) между соответствующими пикселями, вычисленная для различных выравниваний изображений относительно друг друга (например, путем различных смещений и вращений). По соответствующему коэффициенту принимается решение об идентичности отпечатков.

Вследствие сложности и длительности работы данного алгоритма, особенно при решении задач идентификации (сравнение «один-ко-многим») – системы, построенные с его использованием, сейчас практически не используются.

2. Сравнение по особым точкам – по одному или нескольким изображениям отпечатков пальцев со сканера формируется шаблон, представляющий собой двухмерную поверхность, на которой выделены конечные точки и точки ветвления. При сравнении – на отсканированном изображении отпечатка также выделяются эти точки, их карта сравнивается с шаблоном и по количеству совпавших точек принимается решение по идентичности отпечатков.

В работе алгоритмов данного класса также используются механизмы корреляционного сравнения, но при сравнении положения каждой из предположительно соответствующих друг другу точек (рис. 1).

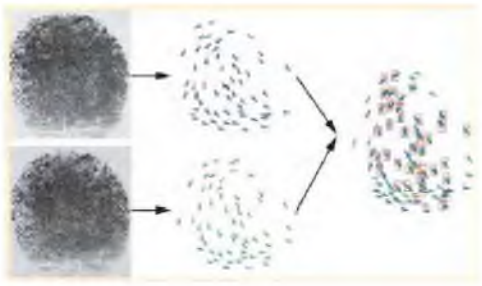


Рис. 1. Сравнение двух отпечатков пальцев по особым точкам

В силу простоты реализации и скорости работы – алгоритмы данного класса являются наиболее распространенными. Единственным существенным недостатком данного метода сравнения являются достаточно высокие требования к качеству получаемого изображения (около 500 dpi).

3. Сравнение по узору – в данном алгоритме сравнения используются непосредственно особенности строения папиллярного узора на поверхности пальцев. Полученное со сканера изображение отпечатка пальца разбивается на множество мелких ячеек, как показано на рис. 2 (размер ячеек зависит от требуемой точности).

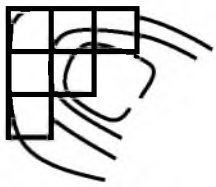


Рис. 2. Разбитие папиллярного рисунка на ячейки

Кроме этого, существует еще ряд методов распознавания отпечатков пальцев.

Метод выявления ключевых точек. Каждый отпечаток пальца состоит из определенного количества борозд и полосок. Полосы – это приподнятые части кожного покрова, борозды – впалые части. Полосы составляют так называемые ключевые точки: края полос (там, где полосы заканчиваются) и раздвоения – там, где они разветвляются (рис. 3).

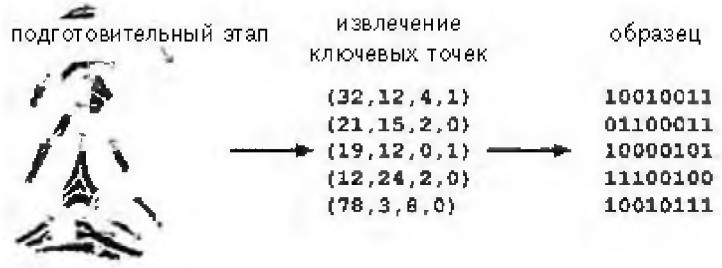


Рис. 3. Регистрация отпечатка по набору ключевых точек

Во время регистрации ключевые точки располагаются в определенном месте, а их расположение относительно друг друга и их направление регистрируются. На основе этих данных создается образец (шаблон) – информация, которая впоследствии будет использована для удостоверения личности пользователя.

Запатентованный метод сопоставления узоров Precise Biometrics во время регистрации отпечатка определяет наличие упомянутых выше дополнительных характеристик. Небольшие участки отпечатка и расстояние между ними извлекаются из общей картины с целью максимально увеличить количество уникальной информации. Наиболее значимы участки вокруг ключевых точек и участки с небольшим радиусом изгиба. Основная структура и уникальные комбинации полос также являются ценными данными.

Метод Precise BioMatch использует как методы выделения ключевых точек, так и алгоритмы сопоставления узоров. Объединение двух разных технологий позволяет Precise BioMatch более эффективно работать с различными типами изображений, даже с отпечат-

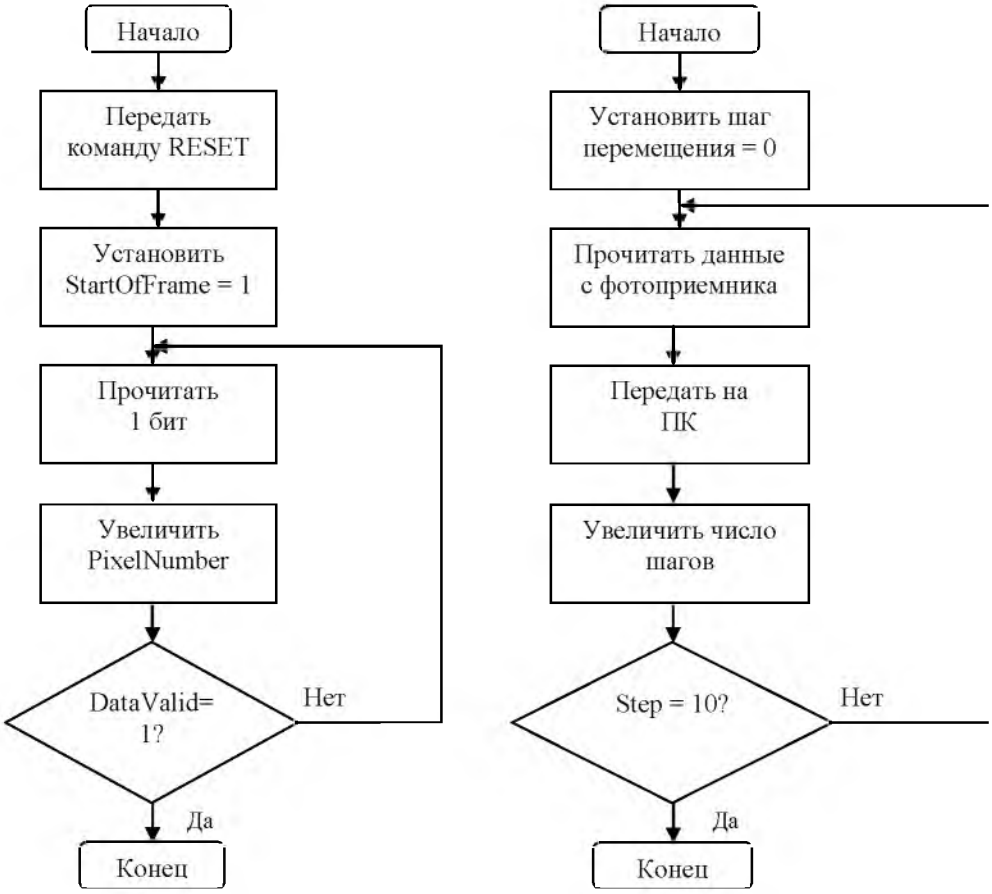
ками низкого качества. Например, отпечаток пальца с несколькими ключевыми точками или отпечатки с размытым рисунком могут помешать пользователю при регистрации, однако смешанная технология, используемая алгоритмом Precise BioMatch, в данном случае будет иметь преимущество.

3. Алгоритм сканирования отпечатка пальца

Рассмотрим алгоритм считывания данных с фотодатчика (рис. 4, а).

При получении изображения мы работаем с регистром PixelData, который расположен по адресу 0x48.

Как видно из рис. 5, данный регистр состоит из двух системных бит (SOF и DataValid) и шести бит Pixel Data.



а б

Рис. 4. Алгоритм считывания изображения (а) и алгоритм сканирования отпечатка пальца (б)

Bit	7	6	5	4	3	2	1	0
Field	SOF	Data_Valid	PD_5	PD_4	PD_3	PD_2	PD_1	PD_0

Рис. 5. Регистр PixelData

Бит SOF (StartOfFrame) принимает значение «1» после процедуры инициализации. Бит DataValid переходит в единичное состояние после считывания последнего бита изображения. Шесть бит данных кодируют значение яркости текущего пикселя по шкале от 0 до 63. При этом минимальное значение равно 0, а максимальное – 63.

Для считывания изображения, которое находится под фотодатчиком ADNS-2610, необходимо выполнить следующие операции:

– произвести процедуру инициализации;
– установить бит SOF (StartOfFrame) в состояние «1»;
– прочитать значение яркости для первого бита изображения;
– увеличить счетчик пикселей на 1;
– проверить состояние бита DataValid. Если оно равно 1, то операцию чтения можно прекратить. Если нет, то выполнить чтение следующего бита изображения.

На рис. 6 показан пример полученного изображения.

Для сканирования полного отпечатка пальца необходимо перемещение фотодатчика как по оси x, так и по оси *y*. Для этого необходимо разрабатывать сложный механизм перемещения, что существенно удорожит данную конструкцию.

Рис. 6. Пример полученного изображения

Проведенные экспериментальные исследования показали, что при небольшом количестве хранимых изображений отпечатков пальцев (до 32) можно отказаться от перемещения датчика по одной из осей и сканировать только узкую полоску, шириной 5 мм. При этом полученного рисунка будет достаточно для однозначной идентификации личности.

При обработке наборов признаков происходит определение степени согласования каждого эталона набора с изображением отпечатка. Полученные вследствие этого данные суммируются с учетом весовых коэффициентов и запоминаются для дальнейшего использования. После обработки всех наборов эталонов происходит поиск наибольшей величины степени согласования. По номеру этого набора находится описание распознаваемого изображения.

В случае, если максимальная вероятность не превышает 50%, то изображение считается не распознанным. Тогда можно перейти в режим обучения для классификации подобного изображения. В режиме обучения новые изображения отпечатков пальцев сканируются, описываются и присваиваются определенному сотруднику. После этого полученные данные заносятся в базу данных.

4. Выводы

В результате исследования был разработан новый алгоритм сканирования отпечатка пальца.

Научная и практическая значимость. На основе синтеза известных методов распознавания отпечатков пальцев получен надежный алгоритм распознавания и управления системой контроля доступа, реализуемый на базе ПК.

Список литературы: **1.** *Андрианов В.И., Соколов А.В.* Охранные системы для дома и офиса. СПб.: БХВ-Петербург; Арлит. 2002. 304 с. **2.** *Магауенов Р.Г.* Системы охранной сигнализации: основы теории и принципы построения: Учебное пособие. М.: Горячая линия – Телеком, 2004. 367 с. **3.** *Горелик А.Л., Скрипник В.А.* Методы распознавания. М.: Высшая школа, 1984. **4.** FBI Integrated Automated Fingerprint Identification System (IAFIS), USA Federal Bureau of Investigation, Web: http://www.fbi.gov/hq/cjisd/iafis/iafisbuilds.htm

Поступила в редколлегию 15.12.2008

Омри Карим, студент гр. ПЗАСм-08-1, кафедра программного обеспечения ЭВМ, ХНУРЭ. Научные интересы: методы распознавания, искусственный интеллект. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 702-14-46.