УДК 519.254

В.В. Старовойтов

БИОМЕТРИЧЕСКИЕ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА ПО ОТПЕЧАТКАМ ПАЛЬЦЕВ

Рассматриваются особенности построения биометрических систем контроля доступа людей в определенные помещения. Детально описываются основные алгоритмы обработки и анализа отпечатков пальцев для этих целей. Представляются схемы построения трех вариантов системы контроля доступа.

Введение

Организация системы контроля и управления доступом (СКУД) – это совокупность программно-аппаратных технических средств, целью которых является регулирование входа людей на заданную территорию или доступа к определенным информационным ресурсам. В свою очередь, управление доступом – это разграничение прав доступа, т. е. определение кого, в какое время и на какую территорию (к каким ресурсам) допускать.

Средства СКУД по функциональному назначению подразделяют на следующие группы:

– устройства (преграждающие, управляемые, исполнительные, считывающие);

– идентификаторы;

– средства управления в составе аппаратных устройств и программных средств.

Устройства первой группы представляют собой механические препятствия типа дверей, ворот, турникетов и т. п. и далее в данной работе рассматриваться не будут.

По виду используемых признаков идентификаторы можно разделить на механические средства (карточки, жетоны), пароли и биометрические данные (отпечаток пальца, изображение лица и т. п.). В отличие от бумажных и пластиковых идентификаторов (паспорта, водительских прав) или пароля биометрические характеристики нельзя забыть или потерять, подделать их также достаточно трудно. По оценкам зарубежных специалистов, более 85 % установленных в США средств биометрического контроля доступа предназначались для защиты машинных залов ЭВМ, хранилищ ценной информации, исследовательских центров, военных установок и учреждений. Таким образом, в ближайшем будущем все СКУД будут использовать биометрические данные человека для определения прав его доступа в определенные помещения или к информационным ресурсам.

Главное преимущество биометрической идентификации заключается в том, что идентифицируется конкретный человек, а не отчуждаемый носитель (карта, жетон и т. п.) или пароль. Биометрический идентификатор нельзя забыть, украсть или передать. Современные средства биометрической идентификации обладают развитыми средствами определения муляжей. Таким образом, можно утверждать, что при использовании биометрии отпадает и проблема предъявления поддельных идентификаторов. Вместе с тем не следует противопоставлять различные методы и средства идентификации друг другу. Наиболее эффективно комплексное применение разных технологий, например биометрических средств и смарт-карт. В этом случае цифровую модель идентификатора (например, отпечатка пальца) можно хранить в защищенной памяти смарт-карты и при распознавании пользователя сравнивать модель отпечатка, хранимую в памяти смарт-карты, с моделью отпечатка, предъявляемого в данный момент. При таком подходе биометрическая идентификация дополняется «имущественной» (необходимостью предъявить материальный носитель).

1. Отпечатки пальцев как идентификатор личности

Идентификации человека по отпечаткам пальцев в настоящее время является лидером среди биометрических технологий. Это достаточно точная, дружественная к пользователю и экономичная технология для применения в области идентификации. Данной технологией

в США пользуются, например, ФБР, Секретная служба, Агентство национальной безопасности, министерства финансов и обороны и другие организации.

Преимущества доступа по отпечаткам пальцев – простота использования, удобство и надежность. Критический обзор статистических моделей отпечатков в различных системах идентификации приведен в статье [1]. Современные системы распознавания нельзя обмануть отрубленными пальцами (можно измерить физические параметры кожи, температуру, пульс) и муляжами [2].

Алгоритмы распознавания отпечатков пальцев делятся на два класса [3]: распознавание по отдельным деталям (характерным точкам) и по рельефу всей поверхности пальца. В первом случае устройство анализирует участки, уникальные для конкретного отпечатка, и определяет их взаимное расположение. Во втором случае обрабатывается изображение всего отпечатка. В современных системах часто используется комбинация этих двух способов, что позволяет повысить достоверность идентификации. Регистрация отпечатка пальца человека на оптическом сканере занимает немного времени. Крошечная CCD-камера делает снимок отпечатка пальца. Затем полученное изображение преобразуется в уникальный шаблон отпечатка. Этот шаблон шифруется и записывается в базу данных для аутентификации пользователей.

На сегодняшний день использование отпечатка пальца для идентификации личности – самый удобный для пользователя из всех биометрических методов. Качество распознавания отпечатка и возможность его правильной обработки алгоритмом существенно зависят от состояния поверхности пальца, его положения относительно сканирующего элемента, чистоты пальца и окна сканера, а также от ряда других условий.

Папиллярные узоры формируются совокупностью выступов и впадин на коже. Они различается даже у близнецов. На каждом отпечатке пальца можно определить два типа признаков: глобальные и локальные. Глобальные признаки – это те, которые можно увидеть невооруженным глазом:

– узор типа «петля» (левая, правая, центральная, двойная);

– узор типа «дельта», или «дуга» (простая и острая), – зона, где выступ разветвляется на три линии, которые затем сходятся в одной точке;

– узор типа «спираль» (центральная и смешанная).

Локальные признаки, или минуции, подробно описаны в ГОСТ Р ИСО/МЭК 19794-2:2005 «Информационные технологии. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка» [4]. Он определяет следующие понятия локальных признаков отпечатков пальцев:

1. Папиллярные гребни – это гребни кожи ладонной поверхности кистей и пальцев рук, непосредственно контактирующие с поверхностью при соприкосновении. Уникальный рельеф, образованный папиллярными гребнями на пальце, формирует отпечатки пальцев. На рис. 1 гребни показаны темными полосами, а впадины – светлыми.

а) *б)* *в)*

Рис. 1. Примеры основных типов глобальных признаков отпечатков пальцев: *а)* дуга; *б)* петля; *в)* завиток

2. Контрольные точки (минуции) – точки нарушения непрерывности гребней, которые могут иметь вид окончания, разделения гребней или иметь более сложную составную форму. ГОСТ [4] определяет два основных типа минуций (рис. 2):

бифуркация (раздвоение) гребня – точка, соответствующая области, в которой отпечаток гребня разделяется на два гребня;

окончание гребня – точка, соответствующая области, в которой отпечаток гребня заканчивается или начинается.

Идентификация по отпечаткам пальцев – наиболее распространенная и развитая биометрическая технология. Ее используют до 60 % биометрических систем.

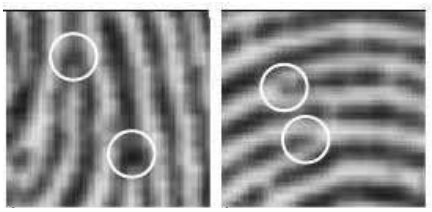


Рис. 2. Примеры окончания и бифуркации (раздвоения) гребня

2. Устройства сканирования отпечатков пальцев

Сканеры последних поколений надежны, компактны и доступны по цене. Для снятия отпечатка и дальнейшего распознавания образца используются три основные технологии: оптическая, полупроводниковая и ультразвуковая.

По соотношению «цена – качество» одними из лучших сканеров отпечатка пальца являются сканеры BioLink U-Match 3.5. Они относятся к устройствам первого типа. Эти сканеры применяются сотрудниками коммерческих компаний и государственных структур более чем в 50 странах мира.

3. Улучшение изображения отпечатка пальца

Отпечатки, полученные стационарно (например, в милиции) под контролем специалиста, обычно имеют хорошее качество и являются информационно-избыточными, т. е. содержат более чем достаточное количество индивидуальных признаков (рис. 3). Алгоритмы обработки и сравнения таких отпечатков достаточно хорошо проработаны (см., например, [3]).

Рис. 3. Отпечатки хорошего качества

Отпечатки, получаемые непосредственно пользователем на пунктах контроля доступа (в спешке, при частично испачканных пальцах или полях сканера), могут привести к получению недостаточно качественного изображения (рис. 4). В связи с этим становится актуальной задача повышения качества изображения и выделения зоны (т. е. сегментации) с четко прослеживаемыми гребнями для надежного выделения минуций и последующего распознавания.

Рис. 4. Пример недостаточно качественного изображения отпечатка

Один из современных подходов к построению модели отпечатков плохого качества описан в работе [5], однако до его применения необходимо выполнить сегментацию области отпечатка и повысить качество изображения.

Алгоритм сегментации и улучшения изображения отпечатка пальца состоит из следующих шагов:

Шаг 1. Нормализация изображения. Выполнить нормализацию исходного изображения отпечатка пальца, чтобы после преобразования оно имело заданные среднее значение и среднеквадратичное отклонение.

Шаг 2. Вычисление локальной ориентации. Вычислить ориентационное изображение из нормализованного изображения отпечатка пальца.

Шаг 3. Оценка локальной частоты хребтов. Вычислить матрицу частот на базе нормализованного и ориентационного изображений.

Шаг 4. Сегментация отпечатка. Построить маску отпечатка путем разбиения нормализованного изображения на блоки и выполнения классификации каждого блока, разделив их на содержащие хребты отпечатки и не содержащие. Затем маску сгладить с помощью морфологических фильтров.

Шаг 5. Фильтрация нормализованного изображения. Применить набор фильтров (Габора или подобных), настроенных на локальную ориентацию выступов и частоту выступов, к пикселам хребтов и впадин в нормализованном изображении для получения улучшенного изображения отпечатка пальца. Для построения шаблона отпечатка использовать часть изображения, которое получено после фильтрации изображения, попавшего в маску, построенную на шаге 4.

Опишем перечисленные шаги более детально.

Нормализация изображения. Пусть $I(i, j)$ обозначает полутоновое значение (уровень яркости) пиксела (i, j); M и VAR – среднее значение и среднеквадратическое отклонение изображения I соответственно; $G(i, j)$ – нормализованное полутоновое значение пиксела (i, j). Нормализованное изображение G (рис. 5) вычисляется по формуле

$$G(i, j) = \begin{cases} M_0 + \sqrt{\dfrac{VAR_0 (I(i, j) - M)^2}{VAR}}, & \text{если } I(i, j) > M; \\ M_0 - \sqrt{\dfrac{VAR_0 (I(i, j) - M)^2}{VAR}} & \text{в противном случае,} \end{cases}$$

где M_0 и VAR_0 – заданные значения среднего и среднеквадратического отклонения соответственно.

а) *б)*

Рис. 5. Результат нормализации изображения отпечатка: *а)* исходное изображение *I*; *б)* нормализованное изображение *G* ($M_0 = 100$, $VAR_0 = 100$)

Вычисление локальной ориентации. Ориентационное изображение передает важные свойства отпечатков пальцев и определяет постоянные координаты для выступов и впадин в локальном соседстве.

Пусть *G* – нормализованное изображение. Для вычисления локальной ориентации к нормальному изображению применяются следующие действия:

– разделить *G* на блоки размером $w \times w$ (например, 16 × 16);

– вычислить градиенты $dx(i, j)$ и $dy(i, j)$ в каждом пикселе (i, j);

– оценить локальную ориентацию в каждом блоке относительно центрального пиксела (i, j):

$$V_x(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2d_x(u,v)d_y(u,v);$$

$$V_y(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} \left(d_x^2(u,v)d_y^2(u,v)\right);$$

$$\theta(i, j) = \frac{1}{2}\tan^{-1}\left(\frac{V_y(i, j)}{V_x(i, j)}\right),$$

где $\theta(i, j)$ – оценка методом наименьших квадратов локальной ориентации выступа в блоке, расположенном симметрично относительно пиксела (i, j). Она представляет направление, которое является ортогональным к доминантному направлению спектра Фурье в окне размерности w x w (рис. 6).

Рис. 6. Пример ориентационного поля: показано белыми стрелками для параметров $w = 16$ и $w_\phi = 5$

Вследствие шума, искажения структур выступов, впадин и других деталей на входном изображении рассчитанная локальная ориентация выступа $\theta(i, j)$ не всегда корректна. Так как локальная ориентация выступа изменяется медленно в соседних блоках, где нет особых точек, применяем низкочастотный фильтр для ее корректировки. Чтобы выполнить низкочастотную фильтрацию, ориентационное изображение необходимо преобразовать в непрерывное векторное поле:

$$\Phi_x(i, j) = \cos(2\theta(i, j));$$

$$\Phi_y(i, j) = \sin(2\theta(i, j)),$$

где $\hat{O}_x$ и $\hat{O}_y$ – компоненты *x* и *y* векторного поля соответственно.

Полученное поле подвергается низкочастотной фильтрации следующим образом:

$$\Phi'_x(i, j) = \sum_{u=-w_\Phi/2}^{w_\Phi/2} \sum_{v=-w_\Phi/2}^{w_\Phi/2} W(u,v)\Phi_x(i - uw, j - vw);$$

$$\Phi'_y(i, j) = \sum_{u=-w_\Phi/2}^{w_\Phi/2} \sum_{v=-w_\Phi/2}^{w_\Phi/2} W(u,v)\Phi_y(i - uw, j - vw),$$

где W – двухмерный низкочастотный фильтр и $w_\Phi \times w_\Phi$ определяет размер фильтра. Операция сглаживания выполняется в блоках, размер фильтра равен 5 x 5.

Локальная ориентация выступа в пикселе (i, j) вычисляется по формуле

$$O(i, j) = \frac{1}{2}\tan^{-1}\left(\frac{\hat{O}'_y(i, j)}{\hat{O}'_x(i, j)}\right).$$

Оценка локальной частоты хребтов. Если минуции не обнаружены локально, уровни яркости вдоль гребней могу быть смоделированы как синусоидальная волна вдоль нормали к ориентации хребта (рис. 7).

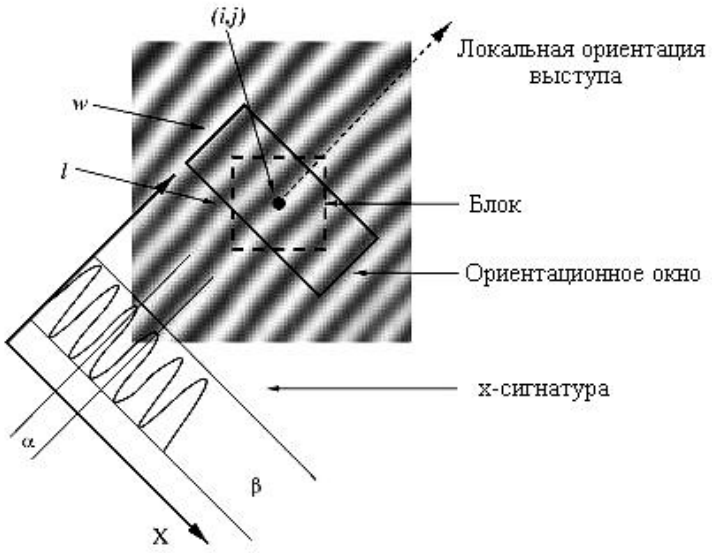


Рис. 7. Ориентационное окно и *x*-сигнатура

Локальная частота выступов – это важное свойство, присущее изображению отпечатка пальца. Пусть G – нормализованное изображение, а O – ориентационное. Тогда для оценки локальной частоты выступов необходимо:

– разделить G на блоки размером $w \times w$ (16 × 16);

– для каждого блока, центрированного в пикселе (i, j), вычислить ориентационное окно размером $l \times w$ (32 × 16), которое определяется в координатной системе выступа;

– для каждого блока, центрированного в пикселе (i, j), вычислить x-сигнатуру $X[0]$, $X[1]$, ..., $X[l-1]$ выступов и впадин в пределах ориентационного окна:

$$X\left[k\right] = \frac{1}{w}\sum_{d=0}^{w-1} G(u,v),\ k = 0,\ 1,\ ...,\ l-1;$$

$$u = i + \left(d - \frac{w}{2}\right)\cos O(i,j) + \left(k - \frac{l}{2}\right)\sin O(i,j);$$

$$v = j + \left(d - \frac{w}{2}\right)\sin O(i,j) + \left(\frac{l}{2} - k\right)\cos O(i,j).$$

Если не обнаружено особых точек в ориентационном окне, x-сигнатура формирует дискретную синусоидально очерченную волну, которая имеет такую же частоту, как выступы и впадины в ориентационном окне. Поэтому частота выступов и впадин может быть оценена из x-сигнатуры. Пусть $T(i, j)$ – среднее число пикселов между двумя следующими друг за другом вершинами в x-сигнатуре, тогда частота Ω вычисляется как $\Omega = 1 / T(i, j)$.

Если не обнаружено следующих друг за другом вершин из x-сигнатуры, частота устанавливается в значение –1, чтобы отличить ее от действительных частотных значений.

Для изображения отпечатка пальца, отсканированного с постоянным разрешением, значение частоты выступов и впадин в локальном соседстве лежит в определенном диапазоне. Для изображения, отсканированного с разрешением 500 dpi, этот диапазон равен $\left[\frac{1}{4} \div \frac{1}{21}\right]$.

Блоки, в которых детали или особые точки обнаружены, но выступы и впадины испорчены или искажены, не формируют четкую синусоидально очерченную волну. Частотные значения для этих блоков должны быть интерполированы по частотам соседних блоков, которые имеют хорошо определяемую частоту. Для каждого блока, расположенного симметрично относительно (i, j):

$$\Omega'(i,j) = \begin{cases} \Omega(i,j), \text{ если } \Omega(i,j) \neq -1; \\ \dfrac{\sum_{u=-w_\Omega/2}^{w_\Omega/2}\sum_{v=-w_\Omega/2}^{w_\Omega/2} W_g(u,v)\mu\left(\Omega\left(i-uw, j-vw\right)\right)}{\sum_{u=-w_\Omega/2}^{w_\Omega/2}\sum_{v=-w_\Omega/2}^{w_\Omega/2} W_g(u,v)\delta\left(\Omega\left(i-uw, j-vw\right)+1\right)} \text{ в противном случае,} \end{cases}$$

где $$\mu(x) = \begin{cases} 0, \text{ если } x \leq 0, \\ x \text{ в противном случае;} \end{cases}$$

$$\delta(x) = \begin{cases} 0, \text{ если } x \leq 0, \\ 1 \text{ в противном случае;} \end{cases}$$

Wg – дискретное ядро Гаусса со средней величиной 0 и изменением 9; $W_\Omega = 7$ – размер ядра.

Если существует по хотя бы один блок с частотным значением –1, необходимо поменять местами Ω и Ω' и повторить предыдущие вычисления еще раз.

Расстояние между выступами локально меняется медленно, поэтому низкочастотный фильтр может быть использован для сглаживания полученных значений:

$$F(i, j) = \sum_{u=-w_{\Omega/2}}^{w_{l/2}} \sum_{v=-w_{\Omega/2}}^{w_{l/2}} W_l(u,v)\Omega'(i - uw, j - vw),$$

где W_l – двухмерный низкочастотный фильтр с модульным интегралом; $W_l = 7$ – размер фильтра.

Сегментация отпечатка. Изображение разбивается на блоки размером $W_l \times W_l$, в каждом блоке вычисляется среднеквадратичное отклонение std_{ij}. Эмпирически выбирается порог T. Блоки, в которых $std_{ij} > T$, считаются содержащими хребты. Остальные блоки считаются неинформативными. Строится бинарная маска информативности блоков. Полученная маска подвергается фильтрации морфологической операцией замыкания для сглаживания краев.

Фильтрация нормализованного изображения. Очертания параллельных хребтов и впадин с хорошо определяемой частотой и ориентацией на изображении отпечатка пальца содержат полезную информацию, которая помогает устранить нежелательные шумы. Для этого используется полосовой фильтр, который настраивается на соответствующую частоту и ориентацию. Он может эффективно удалять нежелательные шумы и сохранять достоверные структуры хребтов и впадин. Фильтры Габора дают оптимальное решение этой задачи как в пространственной, так и в частотной областях, поэтому их целесообразно использовать как полосовые фильтры.

Фильтр Габора описывается формулой

$$h(x, y : \varphi, f) = \exp\left\{-\frac{1}{2}\left[\frac{x_\varphi^2}{\delta_x^2} + \frac{y_\varphi^2}{\delta_y^2}\right]\right\}\cos(2\pi f x_\varphi),$$

$$x_\varphi = x\cos\varphi + y\sin\varphi,$$

$$y_\varphi = x\sin\varphi + y\cos\varphi,$$

где φ – ориентация фильтра Габора; f – частота синусоидальной плоскостной волны; δ_x и δ_y – пространственные константы огибающей Гаусса вдоль осей x и y соответственно. Модуляционно-передаточная функция фильтра Габора определяется выражением

$$H(u, v : \varphi, f) = 2\pi\delta_x\delta_y \exp\left\{-\frac{1}{2}\left[\frac{(u_\varphi - u_0)^2}{\delta_u^2} + \frac{(v_\varphi - v_0)^2}{\delta_v^2}\right]\right\} + 2\pi\delta_x\delta_y \exp\left\{-\frac{1}{2}\left[\frac{(u_\varphi + u_0)^2}{\delta_u^2} + \frac{(v_\varphi + v_0)^2}{\delta_v^2}\right]\right\},$$

$$u_\varphi = u\cos\varphi + v\sin\varphi,$$

$$v_\varphi = -u\sin\varphi + v\cos\varphi,$$

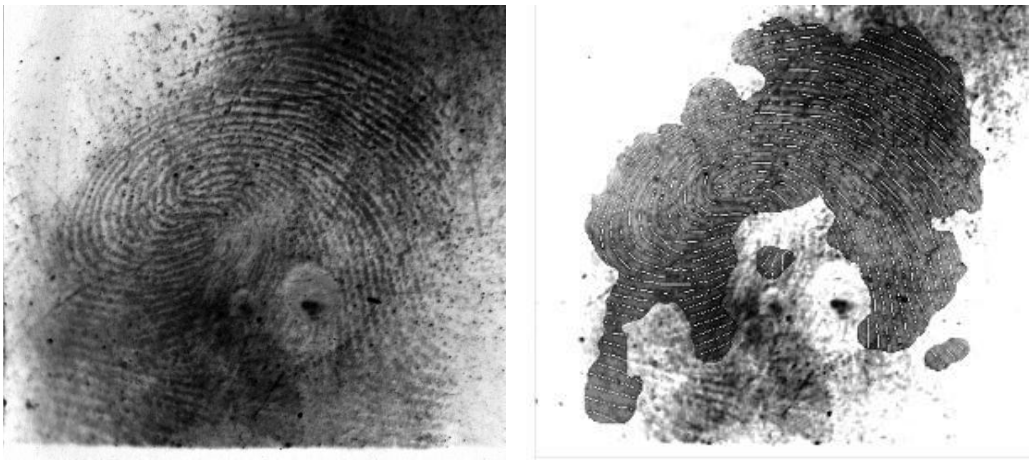
$$u_0 = \frac{2\pi\cos\varphi}{f},$$

$$v_0 = \frac{2\pi\sin\varphi}{f},$$

где $\delta_u = 1/2\pi\delta_x$ и $\delta_v = 1/2\pi\delta_y$.

Для применения фильтров Габора к изображению задаются три параметра: частота синусоидальной плоскостной волны f, направление фильтра, среднеквадратичные отклонения огибающей (оболочки) Гаусса δ_x и δ_y.

Частотная характеристика фильтра *f* определяется локальной частотой хребтов, а направление – локальной ориентацией выступа. Выбор значений δ_x и δ_y содержит компромисс. Чем больше эти значения, тем фильтры более устойчивы к шумам, но при этом возрастает вероятность того, что фильтры будут создавать ложные выступы и впадины. С другой стороны, чем меньше значения δ_x и δ_y, тем менее вероятно, что фильтры будут создавать ложные выступы и впадины; следовательно, они будут менее эффективны в устранении шумов. Значения δ_x и δ_y выбраны равными 4,0 на основе экспериментов.



а) *б)*

Рис. 8. Построение улучшенного изображения: *а)* исходное изображение низкого качества; *б)* улучшенное изображение с выделенной областью, содержащей хребты (показана темным, центральные линии хребтов показаны белым)

Пусть *G* – нормализованное изображение отпечатка пальца, *O* – ориентационное изображение, *F* – частотное изображение, а *R* – восстанавливающая маска. Тогда улучшенное изображение *E* (рис. 8) вычисляется по формуле

$$\mathrm{E}(i,j)=\begin{cases}255, \text{ если } R(i,j)=0;\\ \sum\limits_{u=-w_g/2}^{w_g/2}\sum\limits_{v=-w_g/2}^{w_g/2} h\big(u,v:O(i,j),F(i,j)\big)G(i-u,j-v) \text{ в противном случае,}\end{cases}$$

где w_g = 11 и определяет размер фильтров Габора.

Дополнительную информацию по этому вопросу можно найти в работах В.Ю. Гудкова [6].

4. Сравнение отпечатков по найденным локальным признакам

Алгоритм сравнения отпечатков по локальным признакам состоит из следующих шагов:

Шаг 1. Улучшение качества исходного изображения отпечатка. Повысить резкость папиллярных линий (хребтов) в найденной маске.

Шаг 2. Бинаризация изображения отпечатка. Преобразовать изображение к черно-белому представлению пороговой обработкой.

Шаг 3. Утончение линий изображения отпечатка. Выполнить утончение бинарного изображения до получения линий шириной 1 пиксел.

Шаг 4. Выделение минуций. Изображение разбить на блоки (например, 9x9 пикселов). Анализируя окрестности каждого пиксела, выделить окончания и раздвоения хребтов (рис. 9).

Рис. 9. Пример выделения минуций

Координаты обнаруженных минуций и их углы ориентации записать 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.

Шаг 5. 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 процесс сопоставления выполняется для разных пар минуций (рис. 10). При поиске для каждой минуции перебирают до 30 значений поворота (от −15 до +15°), 500 значений сдвига (от −250 до +250 пикселов) и 10 значений масштаба (от 0,5 до 1,5 с шагом 0,1), т. е. до 150 000 вариантов для каждой из 70 возможных минуций.

Шаг 6. Принятие решения о совпадении отпечатков. Оценка совпадения отпечатков выполняется по формуле $K = \dfrac{D^2}{pq} \cdot 100\,\%$, где D – количество совпавших минуций; p – количество минуций шаблона, хранящегося в базе; q – количество минуций предъявленного отпечатка. Если K превышает 65 %, отпечатки считаются идентичными. Для более высокого уровня защиты от незарегистрированного пользователя порог может быть повышен.

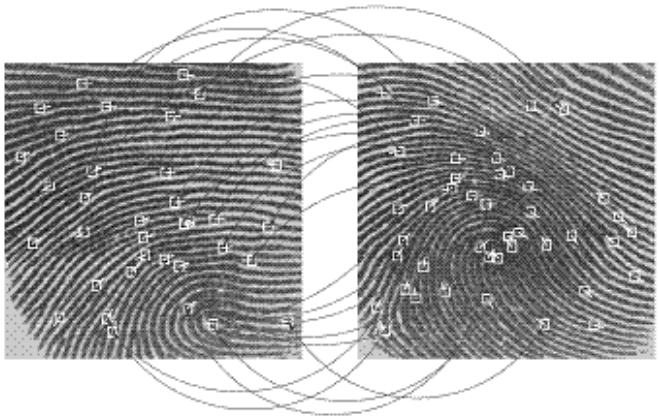


Рис. 10. Пример сравнения одинаковых точек на двух отпечатках

Более подробно о точности результатов сравнения отпечатков пальцев 13 разными способами можно прочитать в статье [7].

5. Организация системы биометрического контроля доступа

Ниже описаны три схемы реализации биометрических систем под конкретные применения, в каждой из них на одного пользователя можно зарегистрировать до 10 отпечатков пальцев, причем в базу данных записываются только шаблоны отпечатков. Далее пользователю присваиваются пра-

ва доступа на конкретные точки прохода, при этом шаблоны отпечатков в кодированном виде передаются по линии связи в контроллер биометрического терминала и хранятся в нем независимо от компьютера. Кратко опишем схемы построения систем контроля доступа [8].

5.1. Схема автономного биометрического терминала для контроля доступа в помещение

Автономный биометрический терминал (биометрический замок) управляет точкой прохода (дверью) без подключения к компьютеру (рис. 11). Устройство представляет собой контроллер и считывающий сенсор отпечатков пальцев в едином корпусе. Для открытия двери пользователь прикладывает палец к сканеру отпечатков пальцев. После положительного сравнения отпечатка пальца с хранящимися в базе шаблонами устройство открывает замок. Для выхода используется кнопка выхода (как в домофонной системе).

Дополнительно может быть подключена сирена для оповещения о взломе устройства. Это самый простой вариант применения биометрических технологий по отпечатку пальца для доступа в помещение. Применяется для реализации СКУД на одной точке прохода или в нескольких точках с независимым программированием оборудования. Преимуществом биометрического замка является автономное питание от встроенных пальчиковых батареек.

Рис. 11. Пример автономного биометрического терминала для контроля доступа в помещение

5.2. Схема сетевого биометрического терминала для контроля доступа в помещение

Сетевой терминал доступа может подключаться к компьютеру по сетевым интерфейсам RS485, Ethernet (рис. 12). Сравнение отпечатков пальцев может производиться как в самом терминале, так и на сервере с помощью режима серверной идентификации. При сравнении отпечатков пальцев на сервере могут создаваться практически не ограниченные по размеру базы данных шаблонов отпечатков. Сетевые терминалы используются для создания распределенных сетевых систем контроля доступа. На компьютер устанавливается программное обеспечение, которое управляет одновременно большим количеством терминалов. К нему может подключаться usb-сканер отпечатков пальцев для регистрации отпечатка пальца пользователя в системе. Шаблоны отпечатков разрешенных пользователей можно загрузить во все терминалы в сети.

Рис. 12. Пример сетевого биометрического терминала для контроля доступа в помещение

5.3. Схема сетевого биометрического терминала для контроля доступа к информационным ресурсам

На рис. 13 представлен один из вариантов сетевой распределенной системы с разграничением прав доступа пользователей. Она открыта для интеграции с устройствами других производителей и при необходимости может наращиваться. Организация сети строится с использованием интерфейса RS485 и выделенных линий связи Ethernet либо сотовых сетей формата GSM. Биометрические терминалы объединяются в магистраль RS485 (до 255 шт.).

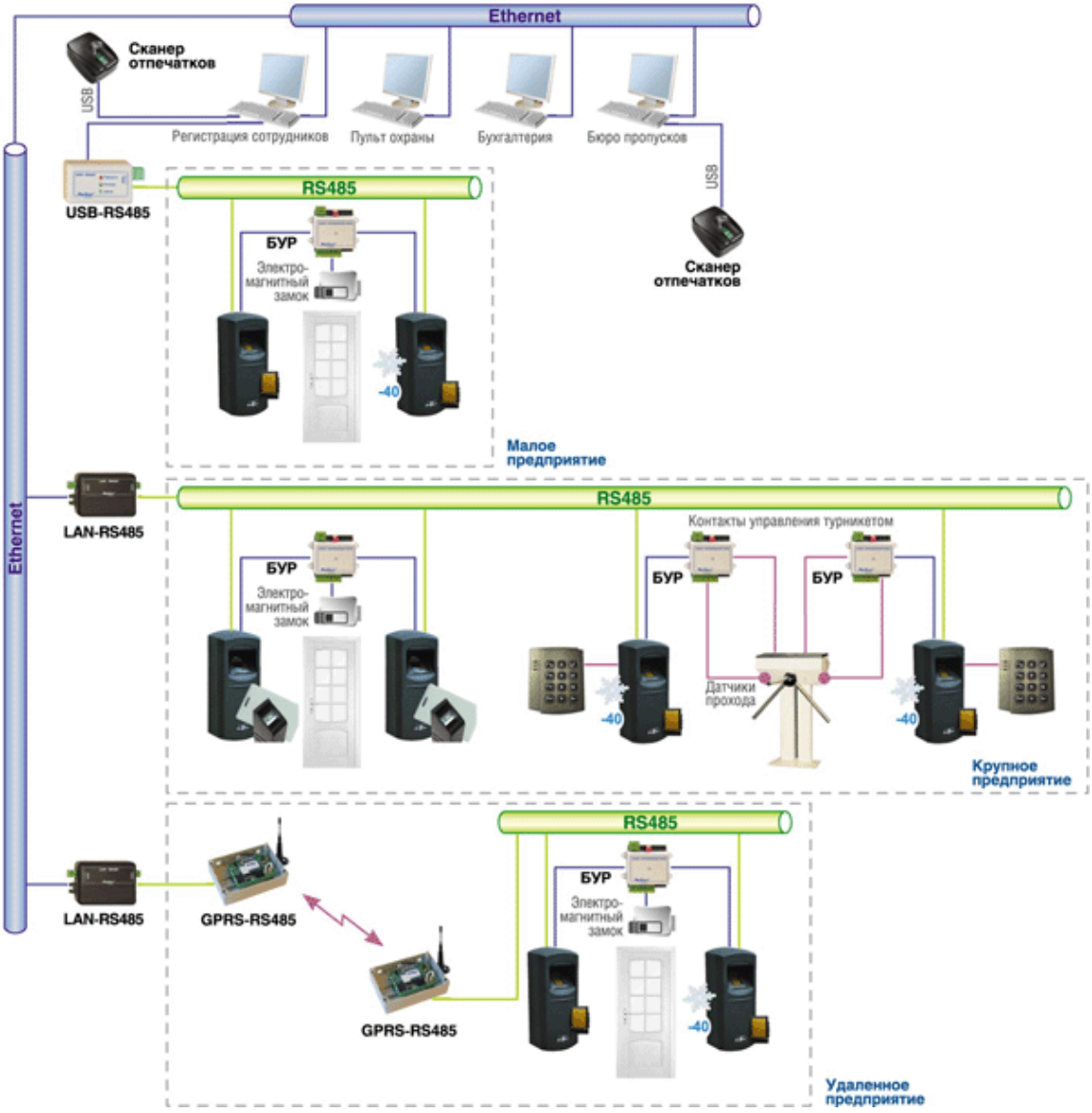


Рис. 13. Пример сетевого биометрического терминала для контроля доступа к информационным ресурсам

Заключение

Сегодня использование отпечатков пальцев при идентификации личности – наиболее простой и комфортный для пользователя биометрический метод доступа. Поэтому для организации системы контроля и управления доступом людей на заданную территорию или к определенным информационным ресурсам предлагается использовать биометрическую технологию на основе признаков, извлеченных из отпечатков пальцев. Биометрические системы подобного типа все чаще используются для различных практических приложений, однако детальные описания алгоритмов и особенности построения подобных систем в литературе отсутствуют.

В статье описаны ключевые алгоритмы обработки и анализа изображений отпечатка пальца различного качества, представлены схемы трех вариантов организации биометрической системы контроля доступа в помещение и к информационным ресурсам. Приведены ссылки на ключевые работы по биометрической идентификации с использованием отпечатков пальцев.

Список литературы

1. Modern statistical models for forensic fingerprint examinations: A critical review / J. Abraham [et al.] // Forensic Science International. – 2013. – Vol. 232, no. 1–3. – P. 131–150.

2. Ларин, П.З. Обведем вокруг пальца? Обман биометрических систем доступа, использующих дактилоскопическую идентификацию личности / П.З. Ларин, Е.И. Ревер // Информационная безопасность. – 2004. – № 3. – С. 24–27.

3. Handbook of fingerprint recognition / D. Maltoni [et al.]. – N.Y. : Springer-Verlag, 2009. – 494 p.

4. Информационные технологии. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка : ГОСТ Р ИСО/МЭК 19794-2:2005. – Введ. 29.12.05. – М. : Федеральное агентство по техническому регулированию и метрологии, 2005. – 42 с.

5. Muñoz-Briseño, A. Fingerprint indexing with bad quality areas / A. Muñoz-Briseño, A. Gago-Alonso, J. Hernández-Palancar // Expert Systems with Applications. – 2013. – Vol. 40. – P. 1839–1846.

6. Гудков, В.Ю. Математические модели и методы обработки цифровых дактилоскопических изображений : автореф. дис. … д-ра физ.-мат. наук : 05.13.18 / В.Ю. Гудков ; Челябинский гос. ун-т. – Челябинск, 2010. – 40 с.

7. Haber, R.N. Experimental results of fingerprint comparison validity and reliability : A review and critical analysis / R.N. Haber, L. Haber // Science and Justice, 2014. – Vol. 54. – P. 375–389.

8. Схемы монтажа биометрических терминалов контроля доступа [Электронный ресурс]. – Режим доступа : http://fingerprint.com.ua/article/schaccessterminal.html. – Дата доступа : 15.01.2015.

Поступила 14.01.2015

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова, 6
e-mail: valerys@newman.bas-net.by

V.V. Starovoitov

BIOMETRIC ACCESS CONTROL SYSTEMS BASED ON FINGERPRINTS

Features of biometric access control system design for control people's access to certain facilities are described. Basic algorithms for fingerprint processing and analysis are given in details. Construction schemes of three variants of an access control system are presented.