ЗАЩИЩЕННАЯ БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ В СИСТЕМАХ КОНТРОЛЯ ДОСТУПА. I. Математические модели и алгоритмы

Protected Biometrical Identification in Accept Control System I. Mathematical models and algorithms

Ключевые слова: биометрическая идентификация – biometrical identification; технология – technology; алгоритмы – algorithms; защищенность – security; достоверность – trustworthiness.

Рассматриваются математические модели и алгоритмы традиционной и новой – защищенной технологии биометрической идентификации в системах контроля доступа.

Mathematical models and algorithms of Traditional and New – Protected Biometrical Identification in Accept Control System are considered.

ЛОВЦОВ / LOVTSOV D.
Дмитрий Анатольевич
(dal-1206@mail.ru)
заслуженный деятель науки РФ,
доктор технических наук, профессор,
заместитель по научной работе директора Института точной механики и вычислительной техники им. С.А. Лебедева Российской академии наук, Москва

КНЯЗЕВ / KNYAZEV K.
Кирилл Владимирович
(dal@ipmce.ru)
аспирант Института точной механики и вычислительной техники им. С.А. Лебедева Российской академии наук, Москва

В автоматизированных системах контроля легитимности доступа и полномочий субъектов (персонала, клиентов, пассажиров, пользователей и др.) актуальной остается проблема обеспечения *защищенности* хранимых в информационных базах эталонных персональных данных, регулярно подвергающихся несанкционированным атакам по традиционным и нетрадиционным (скрытым) информационным каналам [1] с целью их выявления.

Совершенствование технологий распознавания (идентификации и аутентификации), реализуемых в современных системах контроля доступа (СКД), связано, главным образом, с обеспечением его *достоверности* при ограничениях на *оперативность* и *ресурсоемкость* и обеспечении *защищенности* хранимых эталонных данных. Требование к СКД по *достоверности* идентификации заключается в том, чтобы система крайне редко отказывала бы в доступе легитимным субъектам и, в то же время, практически полностью исключала бы несанкционированное проникновение. В этом отношении наиболее эффективны биометрические технологии распознавания, использующие сравнение физиологических или психологических особенностей субъектов с их эталонными биометрическими характеристиками (отпечатки пальцев, геометрия рук, фонограммы голосов и др.), хранящимися в информационной базе СКД в электронно-цифровой форме, поскольку, *во-первых*, в отличие от паролей и карточек «биометрическую информацию» нельзя забыть или потерять (если только вместе с ее носителем), а, *во-вторых*, для предъявления такой информации требуется физическое присутствие ее носителя, т.е. самого субъекта. *Защищенность* хранимых эталонных данных предполагает практическую невозможность восстановления с их помощью реальных физиологических или психологических особенностей субъектов.

Исторически, в частности, в рамках криминалистики более основательно (примерно за 100 лет) разработана технология биометрической идентификации (ТБИ) на основе анализа отпечатков пальцев. Отпечаток пальца образует так называемые папиллярные линии на гребешковых выступах кожи, разделенных бороздками. Из этих линий складываются сложные узоры (дуговые, петлевые, завитковые), которые обладают свойствами индивидуальности и неповторимости, что позволяет достаточно верно идентифицировать личность. Хотя доля отказа в доступе уполномоченным субъектам на практике составляет около 3%, доля ошибочного доступа – меньше одного к миллиону [2].

Преимуществами технологии доступа по отпечатку пальца являются также оперативность, простота

использования и удобство. Весь процесс биометрической идентификации занимает немного времени (10 – 20 с) и не требует особых усилий. Вероятность ошибки идентификации намного меньше в сравнении с другими биометрическими технологиями. Кроме того, устройства идентификации по отпечатку пальца являются, как правило, малогабаритными [2].

Имеющийся (полученный) образ отпечатка пальца («биометрический образец» [3]) – это растр, который можно *описать особым образом*, основываясь на строении папиллярного узора. Выявив структуру отпечатка его можно сравнить с другими отпечатками и выявить те, которые являются аналогичными или же заключить, что отпечатки различны.

Дактилоскопическая (от греч. *daktilos* – палец) идентификация имеет и свои *недостатки*. Так, приблизительно у 1 – 2% людей отпечатки пальцев имеют плохое качество [2]. Люди, занятые физическим трудом, получают во время работы многочисленные мелкие травмы, верхний слой кожи рук может быть поврежден, что создает определённые трудности при сравнении отпечатков. Отпечаток может также деформироваться при большой влажности и под воздействием ряда других внешних факторов. В связи с этим выполнение жестких требований по оперативности (производительности) работы алгоритмов, характерных для общегражданских приложений, в настоящее время остается трудноразрешимой задачей.

В целом, дактилоскопическая ТБИ включает, как правило, пять алгоритмических модулей [3]:

1. Модуль снятия отпечатка *B* пальца, на выходе которого – данные *E* отпечатка пальца субъекта (битовое отображение графического объекта).

2. Модуль обработки изображения *E* (улучшение качества исходного изображения отпечатка; вычисление поля ориентации папиллярных линий; «бинаризация» – переход к двум цветам изображения отпечатка; утончение папиллярных линий на бинарном изображении), на выходе которого – определённое изображение *C*.

3. Модуль извлечения особенностей *f*, в котором из полученных данных *C* извлекают набор особенностей *f*(*C*). Набор *f*(*C*) показывает, в частности, положение и ориентацию «завитка» и др., его обычно получают после нескольких шагов обработки данных *C*. Значение количества минуций (от лат. *minutia* – метка или «ключевая точка», характеризующая окончание и бифуркацию – раздвоение папиллярных линий) зависит от алгоритма их извлечения. Изображение *C* имеет, как правило, разрешение 500 *dpi* (*dots per inch*), размер 250x250 пикселей (255 градаций серого).

4. Сопоставляющий модуль (функция μ сравнения), в котором извлеченные данные *f*(*C*), т.е. *f*(*B*), могут быть сопоставлены с эталонными *f*(*A*).

5. Модуль принятия решения, где личность субъекта принимается или отвергается в зависимости от решающего условия: если $\mu\{f(B), f(A)\} > \alpha$ (где α – параметр безопасности) – субъект действительно тот, за кого себя выдает, иначе – нет.

Известно несколько вариантов сравнения отпечатков пальцев: корреляционное сравнение, *сравнение по особым точкам*, сравнение по узору, сопоставление по шаблону, сравнение на основе графов и др. [4]. Причем наиболее целесообразным вариантом распознавания отпечатка пальца представляется сравнение по особым точкам вследствие достаточно высокой достоверности, оперативности и простоты реализации. Соответствующий алгоритм включает четыре шага:

Шаг 1. Обработка входного изображения. Изображение, получаемое со сканера, изначально непригодно для выделения особых точек, поэтому его необходимо преобразовать к удобному виду. Для этого его нужно отфильтровать, чтобы убрать так называемые «шумы» и мелкие дефекты. Затем необходимо привести бинарное (двухцветное) изображение к его «скелету», в котором толщина всех линий – 1 *пиксель*, т.е. «стянуть» линии в центр, не делая при этом разрывов.

Шаг 2. Поиск минуций [5]. Изображение разбивается на блоки размера [3x3] пикселов. После этого подсчитывается число «черных» (ненулевых) пикселов, находящихся вокруг центра (причем пиксел в центре считается минуцией, если он сам ненулевой), и соседних ненулевых пикселов – один (минуция «окончание») или три (минуция «бифуркация»). Подсчёт числа черных пикселов вокруг текущего пиксела основан на анализе 8-элементных блоков смежных пикселов.

Шаг 3. Получение математического представления отпечатка. *Координаты* обнаруженных минуций и их *углы ориентации* записываются в вектор *B*. Элементами этих векторов являются минуции, каждая из которых представлена своими координатами (*x, y*) и углом $\theta \in [0, 2\pi]$ направления. При этом входная информация точечных образов принимает следующий вид:

$$B_{[N\times 3]} = (b_1, b_2, b_3, \dots, b_N),\ \ b_j = \left(x_{b_j}, y_{b_j}, \theta_{b_j}\right), j = \overline{1,N}$$

где N – число минуций.

Шаг 4. Сравнение полученного представления с эталоном из информационной базы [6]. Пусть *A* – вектор («точечный образ») отпечатка-эталона:

$$A_{[N\times 3]} = (a_1, a_2, a_3, \dots, a_N),\ \ a_i = \left(x_{a_i}, y_{a_i}, \theta_{a_i}\right), i = \overline{1,N}$$

где N – число минуций.

Так как в процессе снятия отпечатка палец мог быть повернут на угол $\Delta\theta$ и сдвинут на расстo-

яние Δl, минуции $b_j \in B$, $a_i \in A$ считаются совпадающими, если выполняются следующие пороговые условия:

$$L(b_i, a_i) = \sqrt{(x_{b_i} - x_{a_i})^2 + (y_{b_i} - y_{a_i})^2} \le L^0$$

$$J(b_i, a_i) = \min\left(\left|\theta_{b_i} - \theta_{a_i}\right|, 2\pi - \left|\theta_{b_i} - \theta_{a_i}\right|\right) \le J^0$$

где L^0, J^0 – заданные значения порогов различимости сдвигов и углов.

При сравнении нужно перебрать до 30 значений угла χ «поворота» (от -15° до $+15^\circ$). «Поворот» выполняется путем умножения матрицы поворота на вектор-столбец, описывающий вращаемую точку:

$$\begin{vmatrix} x'_{b_j} \\ y'_{b_j} \end{vmatrix} = \begin{Vmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{Vmatrix} \cdot \begin{vmatrix} x_{b_j} \\ y_{b_j} \end{vmatrix}$$

После поворота координаты и их углы ориентации будут следующими:

$$B'_k = \left(b_{k_1}, b_{k_2}, b_{k_3}, \dots, b_{k_N}\right),$$

$$b'_{kj} = \left(x'_{kb_j}, y'_{kb_j}, \theta'_{kb_j}\right), j = \overline{1, N}, k = \overline{1, K}$$

Пусть $H_{ik}(b_i, a_i, L^0, J^0)$ – функция-индикатор совпадения минуций $b_i' \in B$ и $a_i \in A$:

$$H_{ik}(b_i, a_i, L^0, J^0) = \begin{cases} 1, \text{если } L(b_i, a_i) \le L^0 \text{ и } J(b_i, a_i) \le J^0 \\ 0, \text{в противном случае} \end{cases}$$

а принятие решения осуществляется по следующему продукционному правилу:

$$R_{ik}(b_i, a_i, L^0, J^0) = \begin{cases} 1, \text{если } \sum_{ik} H_{ik} \ge H^0 \\ 0, \text{в противном случае} \end{cases}, \quad H^0 = \beta N,$$

где H^0 – значение порога достаточного количества совпадений минуций; β – коэффициент сопряжения [7].

Тогда традиционная задача сравнения точечных образов отпечатков примет вид:

$$D(w^*) = \max_{\{w\}}, T(w^*) \le \tau^0, Q(w^*) \le Q^0$$

где $w^* = < L^{0*}, J^{0*}, H^{0*} >$ – оптимальный набор пороговых параметров.

Данный способ сравнения имеет довольно высокую достоверность и оперативность, но низкую защищенность вследствие возможности однозначного восстановления образов отпечатков пальцев по хранимой в информационной базе СКД биометрической информации в виде декартовых координат и углов ориентации минуций.

Для обеспечения *защищенности* дактилоскопической ТБИ представляется необходимым таким образом изменить хранимую в информационной базе биометрическую информацию A, чтобы исключить саму возможность восстановления исходных персональных биометрических данных B, т.е. обеспечить семантическую их независимость и, соответственно, равенство нулю количества $I\{A(w^*), B\} = 0$ взаимной информации [8].

Для этого предлагается представлять отпечаток пальца не в виде вектора, а в виде следующей матрицы [9]:

$$B_{[m \times m]} = \left\| d'_{ij} \right\|, i = \overline{1, M}, j = \overline{1, M},$$

$$\begin{cases} B_1 = (d'_{11}, d'_{12}, d'_{13}, \dots, d'_{1M}) \\ B_M = (d'_{M1}, d'_{M2}, d'_{M3}, \dots, d'_{MM}) \end{cases}$$

где d_{ij} – расстояние между i-й и j-й минуциями.

В отличие от традиционного способа здесь исключены углы ориентации минуций, поэтому минуции $B_j^0 \in B$ и $A_i^0 \in A$ считаются совпадающими, если выполняется следующее пороговое условие различимости сдвигов:

$$L(d_{ij}, d'_{ij}) \le L^0$$

Кроме того, можно повысить и достоверность ТБИ, дополнительно применив на *втором* шаге (поиск минуций) алгоритм устранения ложных минуций (что незначительно снижает оперативность).

Аналогично предыдущему способу при сравнении также нужно перебрать до 30 значений угла χ поворота (от -15° до $+15^\circ$), но в отличие от координат, расстояния между минуциями меняться не будут, а будет меняться лишь последовательность расстояний:

$$B_1 = (d'_{11}, d'_{1M}, d'_{1M-1}, \dots, d'_{12})$$

$$B_M = (d'_{M1}, d'_{M4}, d'_{M5}, \dots, d'_{MM})$$

Так как $d_{11}, d_{22}, \dots, d_{MM}$ (расстояния от точки до самой себя) равны нулю, а $d_{12} = d_{21}, \dots, d_{M-1, M} = d_{M, M-1}$ (взаимные расстояния между точками), получим симметричную матрицу B с нулевыми значениями на главной диагонали.

Пусть $H(d_{ij}, d'_{ij}, L^0)$ – функция-индикатор совпадения минуций $b_j' \in B$ и $a_i \in A$:

$$H_i(d_{ij}, d'_{ij}, L^0) = \begin{cases} 1, \text{если } B_n(L^0) \equiv A \\ 0, \text{в противном случае} \end{cases}$$

Тогда принятие решения при сравнении точечных образов отпечатков будет осуществляться по следующему продукционному правилу:

$$R_i(d_{ij}, d'_{ij}, L^0) = \begin{cases} 1, \sum_i H_i \geq H^0 \\ 0, \text{в противном случае} \end{cases}, \quad H^0 = \beta N.$$

Отсюда, математическую постановку задачи защищенной биометрической идентификации в СКД в условиях информационного соперничества на основе рассмотренного способа сравнения точечных образов можно представить как требование максимизировать достоверность (D) идентификации при ограничениях на *оперативность* (T) и *ресурсоемкость* (Q) и обеспечении *защищенности* ($I\{A, B\} = 0$) хранимых эталонных данных A, т. е. в следующем виде:

$$D(w^*) = \max_{\{w\}} , T(w^*) \leq \tau^0, Q(w^*) \leq Q^0,$$

$$I[A(w^*), B_k] = 0, k = 1,2,3, \dots, w^* =< d_{ij}^*, L^{0^*}, H^{0^*} >$$

Задача в данной постановке является сложной многопараметрической многоэтапной оптимизационной задачей оперативного стохастического программирования, методов решения которой в настоящее время не существует. Особенностью данного типа задач является, в частности, то, что ее надо решать каждый раз заново, учитывая сложившуюся ситуацию (ситуационное описание СКД). Логическая декомпозиция сформулированной задачи выявила следующие частные прикладные подзадачи (относительно простые) и соответствующие последовательно выполняемые *алгоритмы* [9]:

– алгоритм обеспечения контрастности (характеристика, определяемая через яркость) изображения, основанный на последовательном применении известных методов линейной растяжки гистограммы, ее нормализации и эквализации [10] и позволяющий получить более резкие и чёткие границы папиллярных линий отпечатка пальца;

– алгоритм «бинаризации», обеспечивающий преобразование изображения отпечатка пальца к двухцветному – черно-белому изображению;

– алгоритм «скелетизации», обеспечивающий утончение линий изображения отпечатка пальца до ширины в 1 *пиксель*;

– алгоритм выделения минуций, обеспечивающий обнаружение локальных признаков, определяющих пункты изменения структуры папиллярных линий (окончание, бифуркация, разрыв и др.), ориентацию папиллярных линий и координаты этих пунктов, необходимых для дальнейшего процесса идентификации;

– алгоритм удаления ложных минуций, обеспечивающий удаление с изображения отпечатка пальца «контрольных» точек, возникших как результат обработки изображения (обеспечения контрастности, бинаризации, скелетизации), т.е. не являющихся истинными минуциями;

– алгоритм сравнения отпечатков пальцев, обеспечивающий сопоставление минуций предварительно обработанного изображения отпечатка пальца и «биометрического образца», хранящегося в базе данных и знаний (БДЗ) СКД.

В целом, разработанный комплекс алгоритмов из состава информационно-математического обеспечения (ИМО) СКД отличается от традиционных тем, что позволяет:

- достичь максимальной резкости границ папиллярных линий отпечатка пальца благодаря последовательному применению трех лучших методов улучшения контрастности изображения;

- получить рациональный порог бинаризации, а также избавиться, благодаря использованию логической фильтрации трех видов, от ошибок (небольшие выступы и впадины по длине линий, маленькие отростки и «хвосты», пустоты), которые возникают после бинаризации изображения отпечатка пальца;

- удалять ложные минуции с изображения отпечатка пальца (особенность соответствующего оригинального алгоритма заключается в том, что он позволяет удалить *максимальное* количество ложных минуций, практически обеспечивая, тем самым, наличие только реальных минуций);

- осуществлять сравнение отпечатков пальцев и «образцов» на основе численного сравнения соответствующих конструктивных матриц.

Литература

1. *Ловцов Д. А.* Информационная безопасность эргасистем: нетрадиционные угрозы, методы, модели // Информация и Космос. – 2009. – № 4. – С. 100 – 105.
2. *Торвальд Ю.* Сто лет криминалистики. – М.: Прогресс, 1974. – 440.
3. ГОСТ Р ИСО/МЭК 19794-2 –2005. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Ч. 2. Данные изображения отпечатка пальца – контрольные точки. – М.: Стандарты, 2006. – 38 с.
4. Http://ru.wikipedia.org/wiki – Дактилоскопия.
5. *Pokhriyal A., Merit S. L.* Minutiae Extraction using Rotation Invariant Thinning // International Journal of Engineering Science and Technology. – Vol. 2(7). – 2010. P. 3225 – 3235.
6. Abbad K., Assem N., Tairi H., Aarab A. Fingerprint Matching Relying on Mi-nutiae Hough Clusters // ICGST – GVIP Journal. – Vol. 10. – 2010.
7. *Рыканов А.С.* Анализ методов распознавания отпечатков пальца // Системи обробки інформації. – 2010. – Вип. 6 (87). – С. 167– 170.
8. *Князев В. В., Ловцов Д. А.* Ситуационное планирование защищённой переработки формализованной информации в АСУ // Вопросы защиты информации. – 1996. – № 3. – С. 23 – 28.
9. *Князев К. В.* Способ биометрической идентификации // Труды конф. XII Междунар. форума «Высокие технологии XXI в.» (18 – 21 апреля 2011 г.) / РФРВТ. – М.: Изд-во «ЛКИ», 2011. – С. 502 – 503.
10. Http://cv-dev.ru – Выравнивание гистограммы яркости.