УДК 004.932.2

АЛГОРИТМЫ РЕГИСТРАЦИИ И ВЕРИФИКАЦИИ БИОМЕТРИЧЕСКОЙ ИНФОРМАЦИИ ДЛЯ СИСТЕМ ПРИНЯТИЯ РЕШЕНИЯ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНЫХ КАРТОЧНЫХ УСТРОЙСТВ

Степанов А.Ю.

Национальный исследовательский университет «МИЭТ», Москва, e-mail: 2x2z5@mail.ru

Аутентификация пользователя информационной системы по биометрическим параметрам является надежным и удобным способом разграничения доступа**.** В настоящее время наибольшее распространение получили биометрические системы, использующие отпечатки пальцев. Системы, основанные на технологии Match-On-Card (MoC), имеют высокую защищенность, так как отпечатки пальцев хранятся не в централизованной базе данных, а на высокозащищенных интеллектуальных карточных устройствах (смарт-картах). В данной статье рассмотрены основные концепции построения биометрических систем и предложены быстрые алгоритмы регистрации и верификации отпечатков пальцев для систем принятия решения на основе интеллектуальных карточных устройств. Рассмотрена и решена проблема сравнения отпечатков пальцев на высокозащищенном интеллектуальном карточном устройстве (смарт-карте). Предложенные алгоритмы регистрации и верификации отпечатков пальцев предъявляют низкие требования к производительности вычислительных устройств. Хранение эталона отпечатка пальца требует от 1100 до 1900 байт. Время верификации отпечатков пальцев не превышает двух секунд, значения FAR и FRR равны 0,00452 и 2,23 % соответственно, что лучше существующих аналогов.

Ключевые слова: биометрия, отпечатки пальцев, смарт-карта, Match-On-Card

ENROLLMENT AND VERIFICATION BIOMETRIC ALGORITHMS FOR SMART-CARDS

Stepanov A.Yu.

National Research University of Electronic Technology, Moscow, e-mail: 2x2z5@mail.ru

User authentication via biometrics is a reliable and convenient way for access control. Fingerprint biometric systems are the most widely used for today. Systems based on Match-On-Card (MoC) technology have the highest security because fingerprints are stored in a highly secure smart card. There is no central database of user fingerprints. In this paper we propose registration and verification algorithms of biometric data with low performance requirements and memory use. The developed algorithms are based on the analysis of minutiae of fingerprints. Registration algorithm uses information about the mutual location of minutiae to accelerate the verification process. In result, a fingerprint template size is from 1100 to 1900 bytes and the fingerprint verification process takes about of two seconds. FAR less than 0,01 % and FRR is about 2 %. The proposed algorithms do not consider effects of other minutiae characteristics (such as type and quality) of fingerprint verification process. This research does not cover investigation of the ability to store multiple fingerprint templates on the smart card and this may be the result of further investigation.

Keywords: biometrics, fingerprint, smart card, Match-On-Card

С развитием информационных технологий биометрию стали применять во многих областях человеческой деятельности. Биометрические системы защиты информации обладают значительными преимуществами перед традиционными системами, так как однозначно идентифицируют человека. Среди преимуществ биометрических систем выделяют легкость предъявления биометрических данных (отпечаток пальцев или радужной оболочки глаза), неотчуждаемость биометрических характеристик, а также легкость встраивания в системы многофакторной аутентификации. Наибольшее распространение в настоящее время получили системы, которые в качестве биометрической информации используют отпечатки пальцев [1].

В настоящее время существует несколько концепций построения биометрических систем. Отличаются они местом хранения и сравнения отпечатков пальцев.

– Концепция Match-On-Server. В данном подходе ОП хранятся и сопоставляются на централизованном сервере. Сервер сравнивает отпечатки и выдает разрешение на дальнейшее действие. Недостатками данной концепции являются необходимость гарантировать постоянный доступ к серверу, а также обеспечение высоких требований безопасности.

– Концепция Match-On-PC. В данном подходе ОП хранятся на компьютерах пользователей. Сравнение отпечатка-кандидата с эталоном также происходит на компьютере пользователя.

– Концепция Match-On-Card. В данном подходе хранение и сравнение отпечатков пальцев происходит на интеллектуальном карточном устройстве (далее смарт-карта).

Безопасное хранение отпечатков пальцев является важной задачей, так как в отличие от приватных ключей их сложно изменить, если отпечаток пальца будет украден. Биометрические системы, основанные на концепции Match-On-Card (рис. 1), обладают рядом преимуществ перед остальными, а именно: на смарт-карте не хранится изображение отпечатка пальца, а только шаблон отпечатка пальца, который практически невозможно преобразовать обратно в изображение [2]; шаблон отпечатка пальца никогда не возвращается, верификация происходит на смарт-карте, а следовательно, нет необходимости строить централизованное хранилище эталонов отпечатков пальцев пользователей системы.

Вычислительные возможности смарт-карт несоизмеримо малы по сравнению с персональными компьютерами. Поэтому при разработке новых алгоритмов сравнения отпечатков пальцев особое внимание следует уделять скорости сравнения отпечатков пальцев, размерам памяти, необходимой для проведения вычислений и для хранения эталонов отпечатков пальцев.

Алгоритмы регистрации и верификации не используют изображения отпечатков пальцев, а работают с их шаблонами, сформированными в формате стандарта ISO/IEC 19794-2 [4]. Шаблон отпечатка пальца представляет собой набор особых точек, который является математическим представлением изображения отпечатка пальца. Каждая точка характеризуется тремя параметрами: координаты местоположения внутри изображения отпечатка пальца, тип особой точки (точка обрыва и точка разветвления (рис. 2, а) и ориентация хребта θ (в градусах), на котором была найдена точка (рис. 2, б и в).

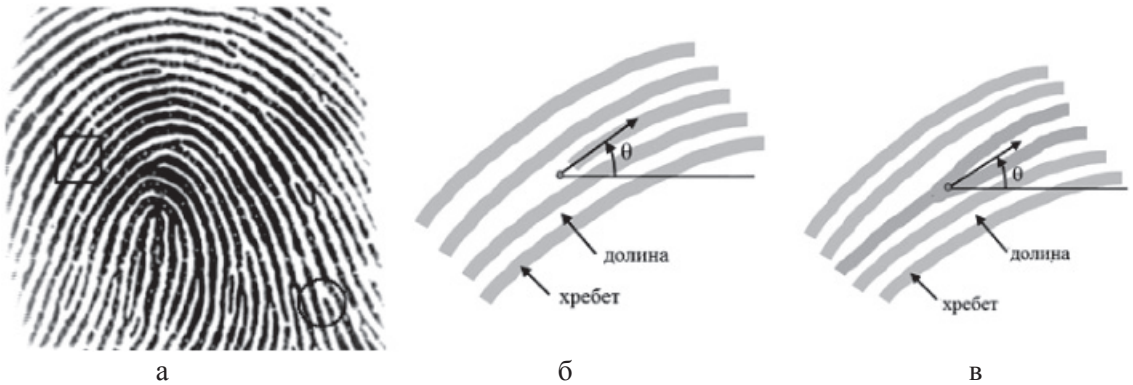
В качестве показателей эффективности алгоритмов регистрации и верификации используются следующие параметры:

– вероятность ложного принятия решения (False Accept Rate, FAR) – вероятность того, что система некорректно сравнит шаблоны разных отпечатков пальцев;

– вероятность ложного отказа (False Reject Rate, FRR) – вероятность того, что система не сопоставит шаблоны отпечатков пальцев, принадлежащих одному и тому же пальцу;

– размер шаблона-эталона отпечатка пальца, который хранится на смарт-карте.

Рис. 1. Распределение задач в системе Match-on-Card



а б в

Рис. 2. Особые точки:
а – точка обрыва выделена кругом, точка разветвления выделена квадратом;
б – расположение и угол ориентации точки обрыва;
в – расположение и угол ориентации точки разветвления

На основании указанных параметров можно проводить сравнения существующих современных алгоритмов. В статье [1] приводится алгоритм верификации отпечатков пальцев для Java Card. Алгоритм имеет асимметричное время сравнения отпечатков пальцев, которое составляет от 0,3 (для сопоставимых отпечатков) до 8 (для несопоставимых) секунд. Авторы приводят следующие параметры эффективности алгоритмов: FAR составляет около 0,1 % и FRR – около 6 %. В статье [3] описан алгоритм аутентификации для системы Match-On-Card на основе отпечатков пальцев. В предложенном алгоритме сравниваются отпечатки пальцев, представленных в формате [4], с помощью матрицы аффинных преобразований (трансляций и поворотов), размер которой составляет от 512 байт до 32 Кбайт. Время сравнения отпечатков пальцев составляет от 66 до 303 миллисекунд, которое достигается благодаря дополнительному аппаратному модулю. Показатели эффективности алгоритмов (FAR и FRR) в статье [3] явно не указываются.

Существующие решения не совсем подходят для реализации на смарт-карте, так как предъявляются относительно высокие требования к производительности вычислительного устройства и к размерам памяти. В данной статье предлагаются алгоритмы регистрации и верификации шаблонов отпечатков пальцев с низкими требованиями к производительности и памяти вычислительных устройств.

Целью работы является разработка методик и алгоритмов обработки биометрической информации для систем принятия решения в составе интеллектуальных карточных устройств с малыми вычислительными ресурсами для решения задач идентификации и верификации личности.

Алгоритм регистрации отпечатков пальцев

В данной статье предлагается алгоритм регистрации шаблонов отпечатков пальцев, представленных в формате ISO 19794-2 [4], который является математическим представлением информации об особых точках отпечатка пальца. Извлечение данных об особых точках и формирование шаблона производится внешним программным обеспечением и не рассматривается в данной статье.

Для описания алгоритма регистрации отпечатков пальцев введем некоторые обозначения. Пусть изображению отпечатка пальца A функцией вычисления шаблона f поставлен в соответствие шаблон $T = f(A)$ в виде множества (1):

$$T = \{m_i\}; \quad (1)$$

$$m_i = \{x_i, y_i, \theta_i\}, \quad (2)$$

где $i \in I = 1...n$; n – количество особых точек; m_i – особые точки отпечатка пальца (2), а x_i, y_i – координаты особых точек; θ_i – углы направлений особых точек (рис. 2, б и в).

Регистрация шаблона сводится к поиску группы $G = \{(m_i, C_i)\}$, где C_i – центральная область, которая представляет собой информацию о взаимном расположении центральной точки и соседних особых точек. Центральные области вычисляются на основе особых точек. Каждая особая точка m_i из шаблона T принимается в качестве центральной особой точки. Для этих точек строится центральная область C_i по формулам (3)–(7).

$$C_i = \{t_i\}, \quad (3)$$

$$t_i = \left\{ d_{ij}, \alpha_{ij}, \Delta\theta_{ij} \mid d_{ij} < k_1 \right\}, \quad i, j \in 1...n; \quad (4)$$

$$d_{ij} = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2}; \quad (5)$$

$$\Delta\theta_{ij} = \theta_i - \theta_j; \quad (6)$$

$$\alpha_{ij} = \theta_i - \operatorname{arctg}\left(x_i - x_j, y_i - y_j\right), \quad (7)$$

где центральные области C_i представлены в виде множества связей t_i; t_i характеризует взаимное расположение центральной особой точки m_i и соседней особой точки m_j; d_{ij} – расстояние между особыми точками; k_1 характеризует порог приемлемого расстояния; $\Delta\alpha_{ij}$ – угол поворота направления центральной особой точки до направления прямой, соединяющей эту точку с соседней; $\Delta\theta_{ij}$ – разность углов направлений особых точек (рис. 3).

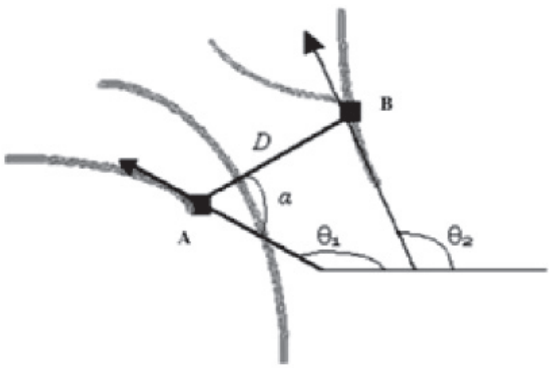


Рис. 3. Расстояния и углы между двумя особыми точками

Для добавления центральных областей C_i вместе с соответствующими им особыми точками m_i в группу G необходимо соблюдение выполнения равенства (8):

$$\left|C_i\right| = k_2, \quad i \in I = 1...n, \tag{8}$$

где k_2 характеризует порог минимального количества связей.

Количество элементов в группе G ограничено двумя параметрами k_3 и k_4, что показано неравенством

$$k_3 \le \left|G\right| \le k_4, \tag{9}$$

где k_3, k_4 – пороги, характеризующие минимальное и максимальное (соответственно) количество центральных областей в зарегистрированном шаблоне отпечатка пальца.

Если неравенство (9) не выполняется, то шаблон не регистрируется. Особенность данного алгоритма заключается в том, что шаблон отпечатков пальцев в процессе регистрации преобразуется к внутреннему представлению, что позволяет ускорить процесс верификации отпечатков пальцев, так как информация о взаимном расположении особых точек шаблона-эталона отпечатка пальца заранее вычисляется данным алгоритмом и сохраняется в энергонезависимой памяти устройства.

Алгоритм верификации отпечатков пальцев

Аналогично алгоритму регистрации, алгоритм верификации отпечатков пальцев работает с шаблонами отпечатков пальцев, представленными в формате ISO 19794-2 [3]. Решение о степени сходства двух шаблонов отпечатков пальцев лежит в диапазоне 0–100 % (чем больше %, тем выше совпадение).

Введем некоторые обозначения. Пусть каждому изображению отпечатка пальца A_1 и A_2 функцией вычисления шаблона f поставлены в соответствие шаблоны $T_1 = f(A_1)$ и $T_2 = f(A_2)$ в виде множеств (10) и (11)

$$T_1 = \{m_i\};\ m_i = \{x_i, y_i, \theta_i\}; \tag{10}$$

$$T_2 = \{m_j\};\ m_j = \{x_j, y_j, \theta_j\}. \tag{11}$$

Предполагается, что шаблон T_1 зарегистрирован на смарт-карте по алгоритму, схема которого представлена на рис. 4, поэтому для него существует группа $G_1 = \{(m_i, C_i)\}$, где $i \in I$, количество элементов в которой ограниченно неравенством (9).

Для шаблона T_2 происходит формирование центральных областей согласно формулам (3)–(7) и находится группа G_2, которая соответствует выражению (12).

$$G_2 = \{(m_j, C_j)\}, j \in 1...r; \tag{12}$$

$$k_5 \le r \le k_6, \tag{13}$$

где r – количество центральных областей для шаблона T_2 и ограничено неравенством (13); k_5 и k_6 – пороги, ограничивающие количество связей в центральной области C_j.

В процессе верификации каждая центральная область зарегистрированного шаблона $(m_i, C_i) \in G_1$ сравнивается с каждой центральной областью шаблона верифицируемого отпечатка пальца $(m_j, C_j) \in G_2$, $i \in I$, $j \in J$. Для этого находится группа L, которая описывается равенством (14) и отображает наилучшие сопоставления связей двух сравниваемых центральных областей. Размер группы L ограничен неравенством (15).

$$L = \{l_a\},\ a \in I; \tag{14}$$

$$1 \le \left|L\right| \le k_7, \tag{15}$$

где l_a отображает степень различия связей центральных областей и представляет собой расстояние Хэмминга связей центральных областей, а порог k_7 ограничивает размер группы L. Каждый элемент l_r вычисляется согласно формуле (16) и удовлетворяет неравенству (17) при условии, что выполняются неравенства (18)–(20).

$$l_a = \Delta d_{ij} + \Delta\alpha_{ij} + \Delta\theta_{ij}; \tag{16}$$

$$l_a < k_{11}; \tag{17}$$

$$\Delta d_{ij} < k_8; \tag{18}$$

$$\Delta\alpha_{ij} < k_9; \tag{19}$$

$$\Delta\theta_{ij} < k_{10}, \tag{20}$$

где $\Delta d_{ij} = \left|d_i - d_j\right|$ – разница между расстояниями связей, $\Delta\alpha_{ij} = \left|\alpha_i - \alpha_j\right|$ – разница между углами α связей, $\Delta\theta_{ij} = \left|\theta_i - \theta_j\right|$ – разница между углами θ связей, для $i \in 1...\left|C_i\right|$, $j \in 1...\left|C_j\right|$; k_8–k_{11} – пороги, ограничивающие Δd_{ij}, $\Delta\alpha_{ij}$, $\Delta\theta_{ij}$, l_a, и обозначают допустимые отклонения при сравнении связей.

Степень расхождения сравниваемых центральных областей определяется группой N согласно равенству (21), каждый элемент которой вычисляется согласно формуле (23) и удовлетворяет неравенству (24). Размер группы N ограничен неравенством (22).

$$N = \{n_i\}, \quad i \in I; \tag{21}$$

$$1 \le \left|N\right| \le k_{12}; \tag{22}$$

$$n_i = \frac{\sum_{i=1}^{|L|} l_i}{|L|}; \quad (23)$$

$$n_i < k_{13}, \quad (24)$$

где n_i отражает среднее отклонение по всем связям сравниваемых центральных областей, k_{12} – порог, ограничивающий максимальный размер группы N; k_{13} – порог, характеризующий допустимое отклонение n_i.

Степень сходства двух шаблонов отпечатков пальца рассчитывается по формулам.

$$S(T_1, T_2) = 100 - 100 \cdot \frac{W}{k_{11} + 1}, \quad (25)$$

где

$$H = \frac{\sum_{n=1}^{|N|} n_i}{|N|}; \quad (26)$$

$$k'_{14} = \frac{(100 - k_{14}) \cdot (k_{11} + 1)}{100}; \quad (27)$$

$$W = \begin{cases} k'_{14}, & \text{если } |N| \geq k_{12} \text{ и } H < k'_{14}; \\ k_{11} + 1, & \text{если } |N| \geq k_{12} \text{ и } H \geq k'_{14}; \\ k_{11} + 1, & \text{если } |N| < k_{12}, \end{cases} \quad (28)$$

где H – среднее отклонение сопоставимых центральных областей; W и k'_{14} – порог, характеризующий допустимое отклонение центральных областей; k_{14} – порог принятия решения о сходстве отпечатков пальцев.

$$S(T_1, T_2) \geq k_{14}. \quad (29)$$

Шаблоны отпечатков пальцев T_1 и T_2 сопоставимы, если неравенство (29) выполняется.

Заключение

В данной статье рассмотрены основные концепции построения биометрических систем и предложены быстрые алгоритмы регистрации и верификации отпечатков пальцев для систем принятия решения на основе интеллектуальных карточных устройств. Системы, основанные на концепции Match-On-Card, являются более защищенными по сравнению с системами, основанными на других концепциях. Ключевым элементом систем Match-On-Card является высокозащищенное интеллектуальное карточное устройство (смарт-карта). В данной статье рассмотрена и решена проблема сравнения отпечатков пальцев на высокозащищенном интеллектуальном карточном устройстве (смарт-карте).

Предложенные алгоритмы регистрации и верификации отпечатков пальцев предъявляют низкие требования к производительности вычислительных устройств, поэтому предназначены для внедрения на смарт-карты. Хранение эталона отпечатка пальца требует от 1100 до 1900 байт. Время верификации отпечатков пальцев не превышает двух секунд, значения FAR и FRR равны 0,00452 и 2,23 % соответственно, что в несколько раз лучше существующих аналогов [1–3]. Предложенные алгоритмы не учитывают влияния других характеристик особых точек на процесс сравнения отпечатков пальцев и возможность хранения нескольких эталонов шаблонов отпечатков пальцев на смарт-карте, что может быть результатом дальнейшего исследования.

Список литературы/References

1. Stefano Bistarelli, Francesco Santini и Anna Vaccarelli. An Asymmetric Fingerprint Matching Algorithm for JavaCard // Pattern Analysis & Applications. – 2006. – P. 359–376.

2. A. Ross, J. Shah and A.K. Jain. From Template to Image: Reconstructing Fingerprints From Minutiae Points // IEEE Trans. Pattern Anal. Mach. Intell. – 2007. – Vol. 29, № 4 – P. 544–560.

3. Taoufik Chouta, Jean-Luc Danger, Laurent Sauvage, Tarik Graba. A small and high-performance coprocessor for fingerprint match-on-card // IEEE Xplore. – 2012. – P. 915–922.

4. ISO/IEC 19794-2 Biometrics – Biometric Data Interchange Formats – Part 2: Finger Minutiae Data // ISO/IEC JTC 1/SC 37. – 2004. – № 464.

5. Pankanti, Sharath. On the Individuality of Fingerprints // IEEE Transactions On Pattern Analysis and Machine Intelligence. – 2002. – T. 24.

6. Kaur, Manvjeet, и др. Fingerprint Verification System using Minutiae Extraction Technique // International Journal of Computer, Electrical, Automation, Control and Information Engineering – 2008. – T. 22 – P. 3405–3411.