УДК 004.056
DOI: 10.33764/2618-981X-2019-6-2-61-65

ОСОБЕННОСТИ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ, ИСПОЛЬЗУЮЩИХ БИОМЕТРИЧЕСКУЮ ИДЕНТИФИКАЦИЮ ПО ЛИЦУ

Глеб Андреевич Акилин
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, тел. (965)829-79-15, e-mail: akilin-ap@yandex.ru

Евгений Владимирович Грицкевич
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент кафедры информационной безопасности, тел. (383)343-91-11, e-mail: gricew@mail.ru

Рассматриваются особенности имитационного моделирования систем идентификации личности по лицу человека. Анализируется общая схема работы биометрической системы идентификации.

Ключевые слова: информационная безопасность, оптотехника, биометрия, идентификация по лицу.

FEATURES OF SIMULATION MODELING OF INFORMATION SYSTEMS USING BIOMETRIC IDENTIFICATION BY FACE

Gleb A. Akilin
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone: (965)829-79-15, e-mail: akilin-ap@yandex.ru

Evgeny V. Gritskevich
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Department of Information Security, phone: (383)343-91-11, e-mail: gricew@mail.ru

The features of simulation modeling of identification systems based on a person's face are considered. General working scheme of biometric identification system is analyzed.

Key words: information security, optotechnics, biometry, face identification.

Введение

Увеличение потока информации, а также ресурсов и капиталов различного вида приводит к необходимости усовершенствования систем защиты. Остро стоит вопрос определения личности и допуска данной личности куда-либо, т. е. вопрос идентификации и аутентификации [1, 2]. Ранее данные вопросы решались исключительно с применением персонала, отвечающего за проверку личностных идентифицирующих признаков. Данный метод не является эффективным, в основном, по причинам высокой стоимости процедуры проверки и создания препятствий в организации работы защищаемого процесса. Не исключа-

ется вероятность сговора персонала и проверяемого субъекта или ошибок персонала по причине утомления.

Современная компьютерная техника позволяет перевести процедуру проверки личности в режим автоматической обработки изображений с использованием различной биометрической информации, относящейся к проверяемому субъекту. Появились программно-технические комплексы, ориентированные на биометрическую идентификацию и аутентификацию человека. Такие системы, во многом, рассчитаны на использование технологий искусственного интеллекта и нейросетей. Эти системы требуют тщательной настройки под конкретную задачу и обрабатываемый материал. Причем, чем меньше ошибок возникает при работе системы, тем более жесткие требования предъявляются к условиям ее работы.

Облегчение задачи подбора правильных параметров выбранного режима работы биометрической идентифицирующей системы возможно с использованием имитационной компьютерной модели, позволяющей прогнозировать поведение анализируемой системы в различных условиях ее эксплуатации. Далее рассматриваются вопросы, связанные с виртуальным моделированием информационных систем, использующих биометрическую идентификацию по лицу [3, 4].

Методы биометрической идентификации

Итак, объектом исследования в данной работе является биометрическая идентификация/аутентификация личности, предметом – подраздел, отвечающий за работу с изображением лица человека. Исторически, метод опознавания лица появился первым и с тех пор применяется повсеместно. Человек сам, без каких либо приборов, апеллируя лишь к своим органам чувств и опыту, может с достаточно большой уверенностью узнавать других людей и различные иные объекты живой и неживой природы. Применяемые при этом на подсознательном уровне методы могут быть различными: определение по изображению лица, по силуэту и характеру походки, по запаху, звукам речи и т. п. [5, 6].

При практической реализации методов технической биометрии данные способы также использовались. В особенной степени это относилось к органам зрения человека, поэтому большинство эксплуатируемых систем являются оптотехническими по своей элементной базе и схемным решениям [7, 8].

Биометрическая идентификация по лицу использует индивидуальные особенности строения и формы лица. Человек различает достаточно большой спектр видов и форм отдельных частей лица. Данный метод применяется, в частности, при составлении фотокомбинированных портретов (фотороботов) и словесных портретов. Суть обоих методов состоит в использовании комбинаций стандартных, шаблонных частей лица. Недостатками данного подхода являются низкая точность и сложность реализации.

Современная биометрическая идентификация по лицу использует метод, основывающийся на определении нескольких идентификационных точек лица

и их координат. Идентификационная точка – это место расположения или граница определенного объекта на лице. Примером могут являться уголки губ, мочки ушей, центр носа и так далее. Более подробно расположение таких точек показано на рис. 1.

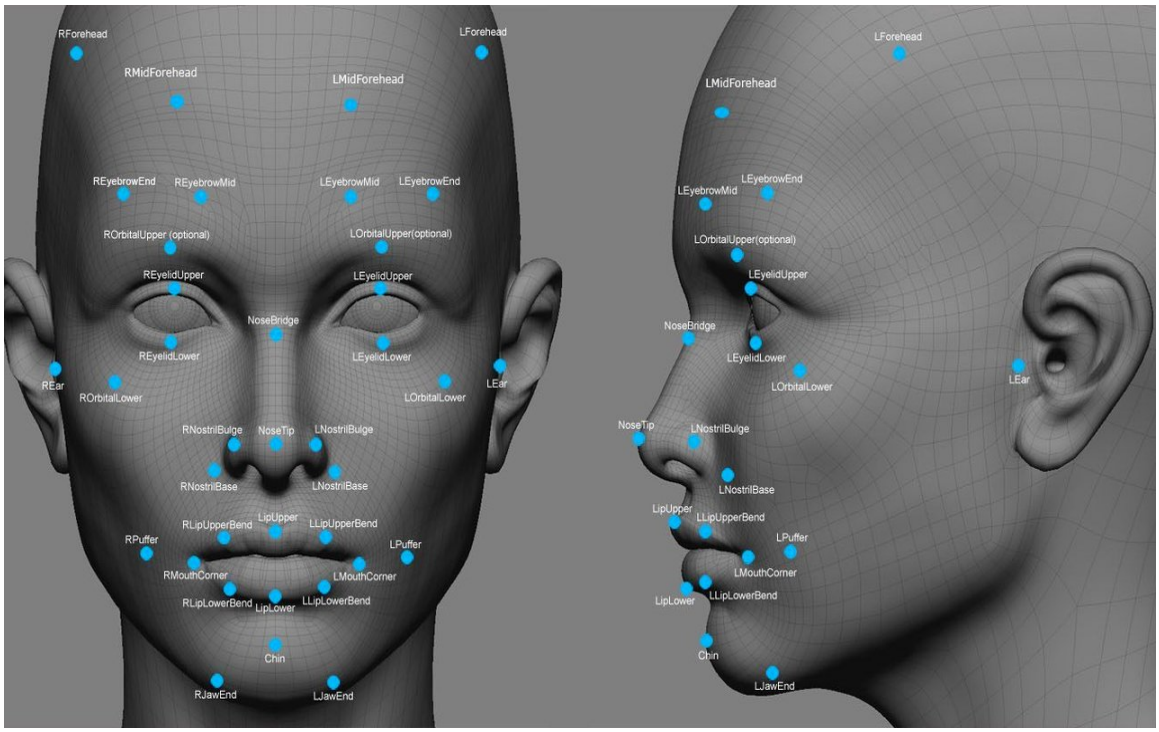

Рис. 1. Расположение идентификационных точек на лице

Задача нахождения точек с общими у различных людей признаками при использовании современных нейросетевых технологий выполняется с малым количеством ошибок [9, 10]. Зная координаты точек, можно получить индивидуальный числовой вектор, называемый вектором контролируемых параметров. На рис. 2 показана условная схема общего алгоритма решения задачи идентификации.

Для случая, когда используется обработка изображения лица, можно конкретизировать приведенный на рис. 2 алгоритм, представив его нижеперечисленными шагами:

1) в систему тем или иным техническим способом вводится изображение лица (возможно, его термограммы) в двумерном или трехмерном форматах;

2) в изображении детектируются контрольные точки идентификации, расположение которых является строго индивидуальным;

3) вычисляется ключ на основе данных точек;

4) производится сравнение ключа с эталонными образцами для выявления совпадения.

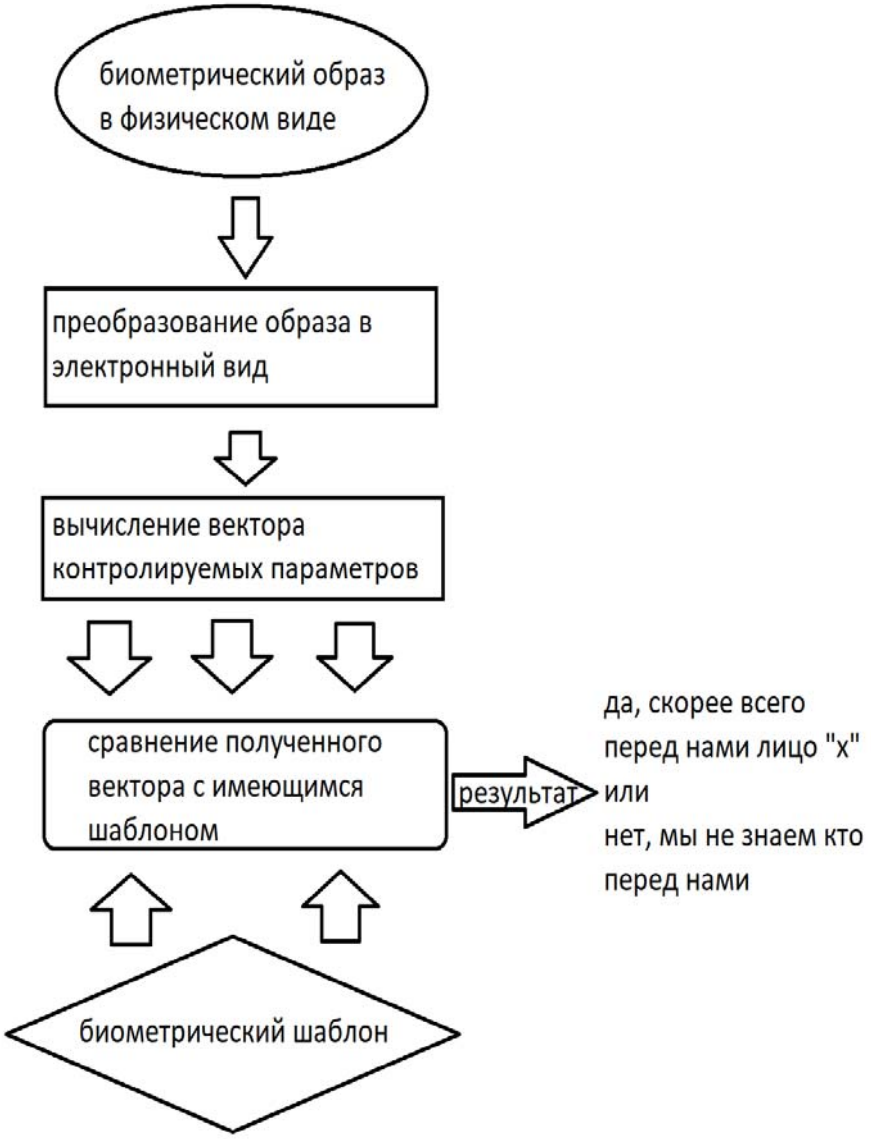

Рис. 2. Алгоритм решения задачи идентификации

Каждый из шагов алгоритма реализуется в виде отдельной программы, или функционально обособленной части основной программы. Информация передается от одного программного модуля к другому по мере возникновения необходимости ее обработки различными способами. Очевидно, что при этом требуется настройка каждого отдельного компонента программно-технического комплекса.

Заключение

Практическая реализация биометрической идентификации по лицу включает несколько этапов. Это, в свою очередь, требует четкой согласованности при работе различных компонентов программно-технического комплекса и тщательной настройки этих компонентов между собой. Имитационная ком-

пьютерная модель создает возможность для проведения такого согласования в виртуальном пространстве, что позволяет существенно сэкономить средства и время, затрачиваемые на настройку системы при ее эксплуатации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Фейс-контроль: риски и перспективы внедрения биометрии в Новосибирске [Электронный ресурс]. – Режим доступа: https://nsk.rbc.ru/nsk/30/03/2019/5c9dfaa99a7947aa27eae88f?from=from_main.

2. Нейросетевая модель распознавания рукописных символов в системах биометрической идентификации и аутентификации / Катасев А. С., Катасева Д. В., Кирпичников А. П., Гумерова Р. И. // Вестник Казанского технологического университета. – 2016. – Т. 19, № 4. – С. 122–126.

3. Кухарев Г. А., Каменская Е. И., Матвеев Ю. Н. Методы обработки и распознавания изображений лиц в задачах биометрии. – СПб. : Политехника, 2013. – 388 с.

4. Кухарев Г. А. Биометрические системы: Методы и средства идентификации личности человека. – СПб. : Политехника, 2001. – 240 с.

5. Handbook of biometrics / A. K. Jain, P. Flynn, A. A. Ross. – Springer, 2008. – 565 p.

6. Аюпова А. Р., Ахатов Р. Р. Биометрический паспорт: зло или добро // Здоровый образ жизни как условие устойчивого развития государства. Сборник материалов Всероссийской научно-практической конференции. – Уфа : Башкирский госуд. ун-т, 2017. – С. 35–38.

7. Соколов Ю. Н. Электронный паспорт в уголовном судопроизводстве // Евразийский юридический журнал. – 2017. – № 4 (107). – С. 265–267.

8. Фахреева Д. Р., Фахреев Н. Н. Биометрический документ как элемент противодействия коррупции // Наука, техника и образование. – 2016. – № 3 (21). – С. 208–209.

9. Волкова С. С., Матвеев Ю. Н. Применение сверточных нейронных сетей для решения задачи противодействия атаке спуфинга в системах лицевой биометрии // Научно-технический вестник информационных технологий, механики и оптики. – 2017. – Т. 17, № 4. – С. 702–710.

10. Кумов В. С., Самородов А. В. Разработка и исследование метода оценки ракурса по координатам контрольных точек 2D изображения лица // Наука и образование: научное издание МГТУ им. Н. Э. Баумана. – 2016. – № 1. – С. 78–89.