УДК 621.391

Б.Ф. БАДАЛЯН, М.С. МАРГАРЯН, Д.О. МОСОЯН

БИОМЕДИЦИНСКИЕ МЕТОДЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Рассматриваются эффективные и перспективные методы биометрической аутентификации личности, основанные на анализе таких физиологических биомедицинских показателей, как сигналы электрокардиограммы и кардиоритм. Проанализированы критерии эффективности систем биометрической аутентификации. Разработана компьютерная модель детектирования основных информационных характеристик сигнала электрокардиограммы в среде MATLAB R2019a.

Ключевые слова: аутентификация, биометрические параметры, ложный доступ, электрокардиограмма (ЭКГ), комплекс QRS, сердечный ритм.

Введение. Процедуры идентификации и аутентификации применяются для разграничения доступа случайных или незаконных субъектов (процессы или пользователи) информационных систем и сетей к определенным ресурсам. Существует множество различных методов аутентификации, которые основаны на знании некоторой секретной информации (пароль, персональный идентификационный код (PIN -Personal Identification Number)), владении некоторым уникальным признаком (магнитные карты, смарт-карты, биометрические характеристики пользователей), а также расположении в определенном месте (использование координат навигационного приемника или конкретного IP-адреса в сети, конфигурации региональных параметров программного обеспечения и т.д.).

Наиболее распространенными, простыми и привычными являются парольные методы аутентификации, основанные на конфиденциальных идентификаторах пользователей. В подобных системах недопустимо хранение паролей пользователей в «чистом» виде в базе данных системы, поскольку в случае компрометирования базы данных украденные пароли могут быть применены для доступа к учетным записям пользователей на других сервисах при использовании ими одинаковых паролей. Кроме того, пароль не должен быть слишком длинным, постоянным, одинаковым для разных сервисов и учетных записей, содержать легко доступную личную информацию [1]. Рекомендуется для генерации и надежного хранения паролей использовать специальные безопасные программные менеджеры паролей.

Биометрическая аутентификация основана на измерении уникальных физиологических характеристик человека. Методы биометрической аутенти-

фикации делятся на статические и динамические (поведенческие). Статические методы основаны на таких физиологических биометрических параметрах, как отпечатки пальцев, геометрия лица или руки, сетчатка или радужная оболочка глаза, ДНК и т.д. Динамические методы основаны на поведенческих особенностях людей (голос, подпись, клавиатурный почерк).

Основная часть. На этапе регистрации биометрические параметры пользователя фиксируются с помощью специального датчика, значимая информация извлекается и в качестве шаблона сохраняется в базе данных наряду с другими такими идентификаторами, как имя учетной записи или PIN-код. Для аутентификации пользователь предъявляет датчику определенный биометрический параметр. Система считывает биометрические показатели, выделяет определенные черты (запрос на аутентификацию) и с помощью алгоритма сопоставления сравнивает их с шаблонами, зарегистрированными в базе данных [2]. Если степень схожести между шаблоном и запросом превышает заранее заданный определенный порог, то происходит положительная аутентификация.

Эффективность биометрической аутентификационной системы с точки зрения пользователей характеризуется ошибками ложного доступа FAR (False Acceptance Rate) и ложного отказа доступа FRR (False Rejection Rate) [3]. Первая характеристика является вероятностью ложного совпадения биометрических параметров двух пользователей (типичные значения FAR составляют порядка 0.01%). Ложный отказ возникает, когда система не подтверждает личность законного пользователя (типичные значения FRR составляют проядка 1%).

Человеческий организм уникален не только по таким внешним признакам, как отпечатки пальцев, сетчатка глаза или походка. Уникальным является также сердечный ритм каждого человека, который зависит от формы сердца, его размеров и положения в теле. С точки зрения биометрической аутентификации, проверка по сердцу — уникальная в своём роде. В отличие от остальных биометрических параметров, сердце гораздо сложнее отделить от организма жертвы, здесь отсутствует возможность столь лёгкой подделки, как при распознавании по лицу или голосу.

Частота сердечного ритма, измеряемая в ударах минуту, может быть легко оценена подсчетом хорошо различимых волн на электрокардиограмме (ЭКГ), которая также является уникальным биомедицинским параметром каждого человека. Форма волн ЭКГ изменяется под действием сердечно-сосудистых заболеваний и патологий (ишемия и инфаркт миокарда), а следовательно, такой биометрический показатель можно применять не только для диагностики различных нарушений ритмической активности, но и для аутентификации пользователей.

Основными информационными характеристиками сигнала ЭКГ являются зубец P, QRS-комплекс и зубец T, которые вызваны деполяризацией предсердий, деполяризацией желудочков и реполяризацией желудочков соответственно (рис.1).

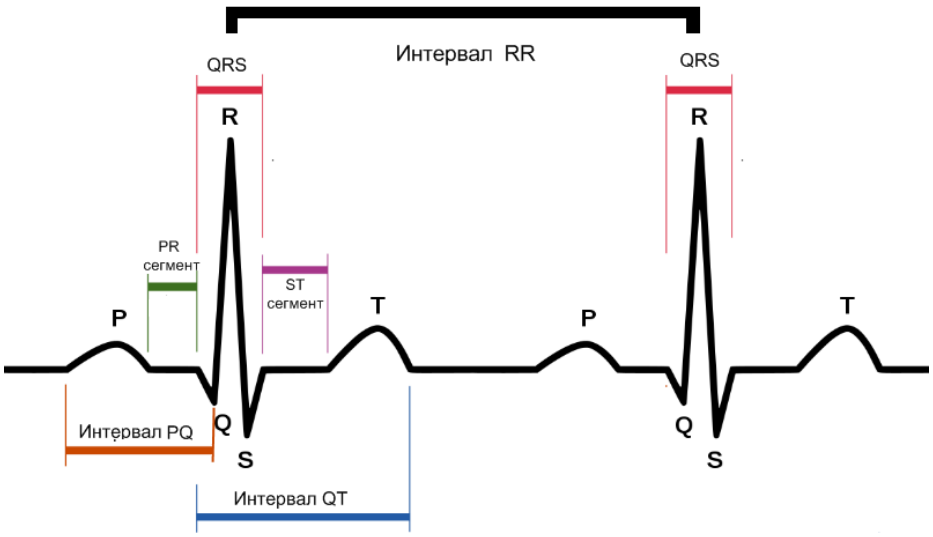

Рис. 1. Стандартный сигнал ЭКГ

Промежуток времени от начала зубца P до начала комплекса QRS называется интервалом PQ и указывает на время, необходимое для прохождения потенциала действия через предсердия и артриовентикулярный (AB) узел. Сразу после того, как сердечный импульс выходит из AB узла, почти одновременное сокращение всей мускулатуры желудочков приводит к появлению комплекса QRS [4]. Зубец R — это самая крупная отметка на ЭКГ, так как мышечные клетки желудочков многочисленны и деполяризуются почти одновременно.

За комплексом QRS следует сегмент ST. Когда клетки желудочков начинают реполяризироваться, еще раз появляется напряжение на поверхности тела, и на ЭКГ фиксируется зубец T. Зубец T шире и не такой высокий, как зубец R, так как реполяризация желудочков менее синхронизирована, чем деполяризация. К моменту завершения зубца T все клетки сердца находятся в состоянии покоя [5].

По выраженности высокочастотных или низкочастотных колебаний R-R интервалов можно судить о различных патологиях вариабельности сердечного ритма, что также используется при кардиобиометрическом методе

аутентификации. Для реализации метода биометрической аутентификации можно использовать также специальный низкоуровневый допплеровский радар, который позволяет каждые 8 секунд определять форму, размер и ритм сердца человека. В дальнейшем он следит в непрерывном режиме — и сразу реагирует на смену сердца перед сканером. Аутентификация не зависит от состояния сердца в текущий момент времени. Кроме того, уникальные особенности, отличающие кардиоритм каждого человека, не изменяются, если скорость биения сердца увеличивается, к примеру, после интенсивных физических нагрузок.

С помощью пакета расширения DSP System Toolbox системы MATLAB R2019a была разработана модель обнаружения комплекса QRS и оценки сердечного ритма пользователя (рис. 2).

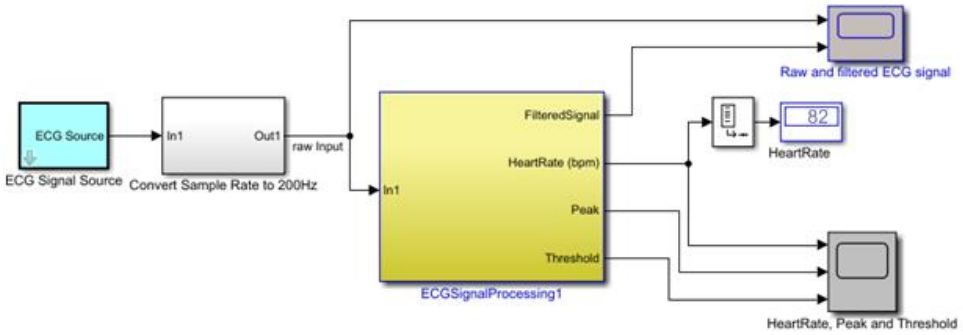

Рис. 2. Модель обнаружения комплекса QRS

Алгоритм обнаружения в реальном времени комплекса QRS разработан в предположении, что частота дискретизации входного сигнала ЭКГ всегда составляет 200 *Гц* (или 200 *выборок / с*). Однако реальные данные ЭКГ могут иметь разные частоты дискретизации в диапазоне от 200 *Гц* до 1000 *Гц*, например, 360 *Гц* в этом примере. Для возможности анализа сигналов ЭКГ с различными частотами используется блок преобразования частоты дискретизации в 200 *Гц*.

Блок обнаружения комплекса QRS обнаруживает пики отфильтрованного сигнала ЭКГ в режиме реального времени, как показано на рис.3. Обнаруженный пик классифицируется как комплекс QRS или шум, в зависимости от того, находится ли он выше установленного порогового значения или нет, как показано на рис. 4.

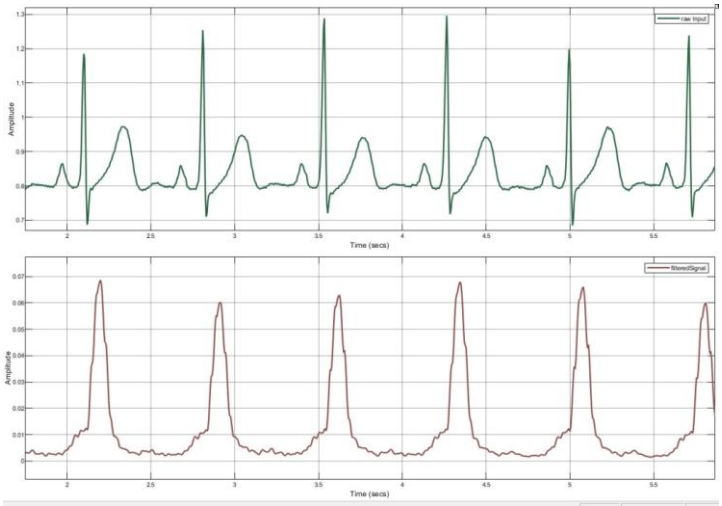

Рис. 3. Фрагмент комплекса QRS и сигнала ЭКГ после фильтрации

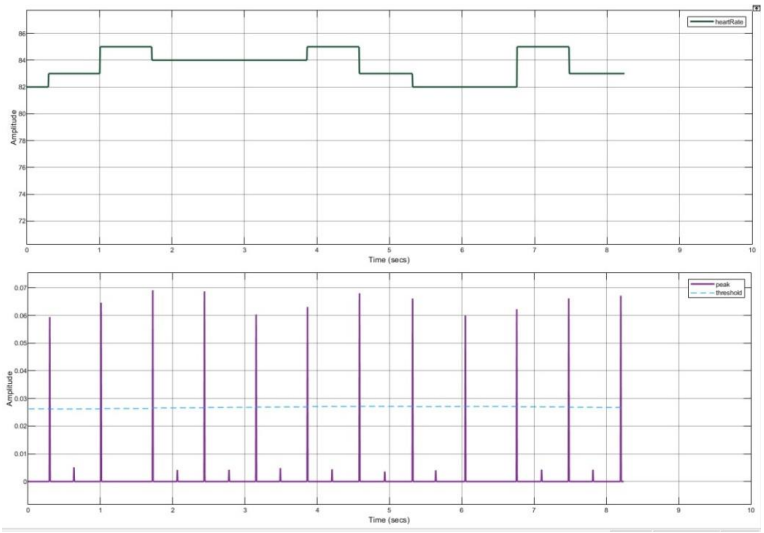

Рис. 4. Мониторинг сердечного ритма и порог обнаружения комплекса QRS

Заключение. Предложенный метод идентификации личности по сердечному ритму и ЭКГ отличается простотой и относительно низкой стоимостью реализации. Миниатюризация устройства позволит интегрировать его в современные фитнес-браслеты или смарт-часы, а наличие технологии Bluetooth гарантирует оперативную и безошибочную передачу результатов измерения системе аутентификации. При этом результаты исследований биомедицинского метода биометрической аутентификации указывают на более худшие показатели FAR и FRR, чем остальные методы (1% FAR при значении FRR в 6%).

Однако метод обладает достаточной достоверностью для осуществления повседневных задач аутентификации. Кроме того, в будущем возможно создание и повсеместное использование базы данных отпечатков сердец всех граждан, что позволит почти безошибочно распознавать личность любого человека.

СПИСОК ЛИТЕРАТУРЫ

1. **Карпухин Е.О.** Технологии и методы защиты инфокоммуникационных систем и сетей: Учебное пособие для вузов.- М.: Горячая линия-Телеком, 2020.-120 с.
2. **Бадалян Б.Ф., Гомцян О.А.** Применение вейвлетов в системах биометрической идентификации // Вестник НПУА: Сборник научных статей.-Ереван, 2016.-Часть 1.- С.361-367.
3. **Дшхунян В.Л., Шаньгин В.Ф.** Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты.-М.:ООО «Издательство АСТ»: Издательство «НТ Пресс», 2004.- 695 с.
4. **Кубланов В.С., Борисов В.И., Долганов А.Ю**. Анализ биомедицинских сигналов в среде MATLAB: Учебное пособие.- Екатеринбург: Изд-во Урал.ун-та, 2016.- 120 с.
5. **Рангайян Р.М.** Анализ биомедицинских сигналов. Практический подход / Пер. с англ.; Под ред. А.П. Немиренко.- М.: ФИЗМАТЛИТ, 2007.- 440 с.

Բ.Ֆ. ԲԱԴԱԼՅԱՆ, Մ.Ս. ՄԱՐԳԱՐՅԱՆ, Դ.Հ. ՄՈՍՈՅԱՆ

ԿԵՆՍԱՉԱՓԱԿԱՆ ՆՈՒՅՆԱԿԱՆԱՑՄԱՆ ԿԵՆՍԱԲԺՇԿԱԿԱՆ ՄԵԹՈԴՆԵՐ

Դիտարկված են անձի կենսաչափական նույնականացման արդյունավետ և հեռանկարային մեթոդներ, որոնք հիմնված են այնպիսի ֆիզիոլոգիական կենսաչափական ցուցանիշների վերլուծության վրա, ինչպիսիք են էլեկտրասրտագրի ազդանշանները և սրտի ռիթմը: Վերլուծված են կենսաչափական նույնականացման համակարգերի արդյունավետության չափանիշները: MATLAB 2019a միջավայրում մշակվել է էլեկտրասրտագրի ազդանշանի հիմնական տեղեկատվական բնութագրերի դետեկտման համակարգչային մոդել:

Առանցքային բառեր. նույնականացում, կենսաչափական պարամետրեր, կեղծ մուտք, ԷՍԳ, QRS-համալիր, սրտի ռիթմ:

B.F. BADALYAN, M.S. MARGARYAN, D.H. MOSOYAN

BIOMEDICAL METHODS OF BIOMETRIC AUTHENTICATION

Effective and promising methods of biometric personality authentication based on the analysis of physiological biomedical indicators such as electrocardiogram signals and cardiac rhythm are considered. The criteria for the effectiveness of biometric authentication systems are analyzed. A computer model for detecting the main information characteristics of an electrocardiogram signal in the MATLAB R2019a environment has been developed.

Keywords: authentication, biometric parameters, false acceptance, ECG, QRS complex, heart rate.