



Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»



12th April 2018, Astana

**ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ**

**Студенттер мен жас ғалымдардың
«Ғылым және білім - 2018»
атты XIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ
XIII Международной научной конференции
студентов и молодых ученых
«Наука и образование - 2018»**

**PROCEEDINGS
of the XIII International Scientific Conference
for students and young scholars
«Science and education - 2018»**

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58

Ғ 96

Ғ 96

«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: <http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/>, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докторанттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

©Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2018

передает сигналы биометрии на сервер или верификатор биометрических данных. Временная метка клиентов и SPV-сервера является одним из примеров ответа на вызов, инициированный сервером SPV. Ответы, полученные от клиентов, используются для определения того, является ли получение сигнала биометрического сигнала синхронным, и сохраняются ли сигналы биометрии в течение, по меньшей мере, продолжительности времени, указанного политикой. Сервер SPV, основанный на результатах обработки валидатором ответа, координатором синхронизации и верификатором биометрии, затем удостоверяет (при необходимости) завершение многосторонней авторизации, запрошенную инициатором на клиенте.

Координатор синхронизации: синхронность реализуется и гарантируется с помощью протокола, управляемого сервером SPV. Время для проверки синхронности измеряется с помощью достаточно точных часов и не требует знания абсолютного времени, например, универсального скоординированного времени (UTC); сервер Trusted Time Server, настроенный на UTC, может быть использован для подтверждения того, что транзакция не только синхронно произошла между несколькими сторонами, но и транзакция также произошла в определенный абсолютный момент времени. Сервер Trusted Time Server может стать частью Координатора по синхронизации, или это может быть услуга третьей стороны.

Координатор политики: координатор политики содержит параметры политики, такие как задержка синхронизации, время сохранения, требуемый уровень безопасности, количество сторон, подлежащих аутентификации, и т.д.

В этой статье описывается новая система и метод многопартийной аутентификации. Процесс многопартийной аутентификации использует синхронные и постоянные сигналы биометрии, полученные от сторон транзакции на основе политики, для утверждения запроса транзакции. Сигналы биометрии предпочтительно выражаются в виде сжатых видеосигналов, имеющих статистически вставленные данные ответа на вызов.

Список использованных источников

1. Adolphs, R., D. Tranel, H. Damsio, and A.R. Damasio. Impaired recognition of emotion in facial expressions following bilateral damage to the human amygdala., 2014 // 440-450 с.
2. S. Narayanan. 2004. Analysis of emotion recognition using facial expressions, speech and multimodal information., 2008 // 331-338 с.
3. Ekman, P., W.V. Friesen, V. Wallace, and P. Ellsworth. Emotion in the human face: Guidelines for research and an integration of findings. Oxford: Pergamon, 1998 // 201-218 с.

УДК 004.934

ВОЗМОЖНОСТИ БИОМЕТРИИ ДЛЯ АУТЕНТИФИКАЦИИ В БЕСПРОВОДНЫХ УСТРОЙСТВАХ

Абдиманов Абзал Асырханович

Магистрант Евразийского национального университета им. Л.Н. Гумилева
Научный руководитель – Ш. Сеилов

Надежная аутентификация личностей становится важной проблемой в контекстах электронного голосования, мобильной коммерции, контроля доступа и контроля пользовательского интерфейса. Традиционные системы аутентификации, например на основе PIN кода или пароля, имеют проблемы, связанные с безопасностью. Биометрические системы аутентификации используют физиологические и поведенческие черты человека, которые способны отличить авторизованного человека от мошенника. В этой статье рассмотрены биометрические технологии и ограничения беспроводных устройств, которые определяют осуществимость и производительность системы аутентификации. Даны короткие оценки самых распространенных биометрических систем.

Биометрический подход к проблеме аутентификации человека заключается в использовании определенного физического признака. Наиболее известные физиологические характеристики включают, например, лицо, отпечаток пальца, рисунок радужной оболочки и ручную геометрию. Есть также много биометрических признаков, которые основаны на поведении человека, например, голос, подпись, динамика нажатия клавиш и распознавание походки. Биометрическая аутентификация, обычно называемая биометрической проверкой, относится к индивидуальному сопоставлению шаблонов, полученных из биометрических образцов.

Результатом аутентификации является вероятность принятия самозванца и отказ от подлинной идентичности. Это отличается от таких подходов, как использование PIN-кодов и паролей, которые могут обеспечить точный результат: да/нет. Однако эти традиционные методы не могут установить, был ли код или пароль выполнен легитимным или самозванным лицом. Еще одно преимущество биометрических черт состоит в том, что их нельзя забыть, и их не так легко или нельзя передать другому человеку. В традиционных подходах к аутентификации люди имеют значительное количество кодов для запоминания для разных целей, и эти коды часто плохо создаются и управляются [1].

В настоящее время основными движущими силами прогресса биометрических технологий являются быстро развивающиеся сенсорные технологии, улучшающиеся алгоритмы и растущая вычислительная мощность в вычислительных платформах. Одновременно ряд приложений требуют надежной и простой в использовании функции аутентификации. Когда для проверки заявленной личности применяется биометрическая аутентификация, конечной целью будет повышение безопасности в целевом приложении. Более того, удобство использования будет тесно связанным и важным фактором, который часто определяет окончательный этап успеха и фактический уровень безопасности.

Возможность использования разных биометрических черт человека

Биометрические характеристики могут оцениваться в соответствии со следующими основными классификаторами:

- Универсальность: у всех людей должна быть уникальная характеристика.
- Уникальность: никакие два человека не должны быть одинаковыми на основе выбранной характеристики.
- Постоянство: характеристика не должна меняться с течением времени.
- Коллективность: характеристика должна быть количественно измеримой.

Для технологически ориентированной оценки может быть указан разнообразный набор важных факторов. Во-первых, технологическая зрелость, масштабируемость и удобство использования могут рассматриваться как фундаментальные проблемы. Основными факторами, касающимися сенсорных технологий, являются принцип физического восприятия, энергопотребление, размер датчика и надежность. Объем вычислительных ресурсов, необходимых для технологий алгоритмов и программного обеспечения, является существенным. Другие примечательные элементы включают размер представления (шаблона) биометрических данных и проблемы хранения данных, проблемы безопасности и конфиденциальности, а также производительность с точки зрения статистических коэффициентов ошибок. Эти факторы содержат широкие технологические области. Например, получение изображения отпечатка пальца может основываться на принципах оптического, термического, емкостного, электронного поля или определения давления. Кроме того, датчик отпечатков пальцев может быть реализован с использованием плоских и линейных моделей. Нажатие пальца на поверхность датчика или подметание его по поверхности влияет на, например, эргономичность, размер датчика и надежность, функции изображения и обработку данных. Кроме того, стоимость является основным фактором, определяющим любое решение в беспроводных устройствах [2].

Наиболее общие биометрические характеристики кратко поясняются ниже. В Таблицах 1 и 2 представлены важные аспекты квалификации определенного подхода и указаны проблемы, которые имеют отношение к использованию беспроводной сети. Стоит

отметить, что некоторые наиболее удобные и приемлемые биометрические подходы могут быть не очень точными, и наоборот. Другими словами, биометрия с «сильным» методическим способом может быть трудным в использовании.

Отпечатки пальцев: распознавание отпечатков пальцев является одним из самых зрелых, приемлемых и простых в использовании биометрических подходов, применяет информацию, доступную каждому кончику пальца. Вкратце, представления отпечатков пальцев основаны главным образом на хребтах плавника (профили серой шкалы, рисунки гребня) и черты, извлеченные из хребтов (*minutiae*). Скорость распознавания в настоящее время приемлема для многих приложений и является конкурентоспособной с традиционными методами аутентификации (PIN-код и парольные запросы). Кроме того, экспериментально было показано, что даже идентичные близнецы, имеющие близкую генетическую связь, могут идентифицироваться своими отпечатками пальцев. Важное качество изображения из-за характеристик популяции и факторов окружающей среды, очевидно, представляет собой проблему. Еще одним императивным аспектом может быть неконтролируемая среда использования, которая затрагивает все биометрические подходы (Таблицы 1 и 2), особенно когда используются беспроводные приложения.

Лицо: лицо широко признается биометрической чертой, главным образом из-за его общности. Кроме того, получение изображений лица является относительно простой и непродуманной задачей. Существует два основных подхода к распознаванию лиц: первый подход – преобразование, состоящие из представления изображения лица с набором ортонормированных базисных векторов, например собственных; второй метод, основан на презентациях атрибутов, которые извлекают из лиц такие атрибуты, как нос, глаза и т.д. Также рассматриваются геометрические свойства извлеченных атрибутов. Сложные условия визуализации часто являются основными трудностями при распознавании лиц (Таблица 1), что дополнительно подчеркивается при использовании беспроводной сети. В последнее время камеры успешно интегрируются в мобильные устройства, обеспечивая новую возможность использования лицевой биометрии.

Радужная оболочка: радужная оболочка человеческого глаза представляет собой узор текстуры, который, как утверждается, является уникальной особенностью для каждого человека и глаз. Приобретение изображения радужной оболочки требует сотрудничества от предмета, поскольку изображение радужной оболочки должно располагаться в центре области формирования изображения, и изображение должно располагаться на некотором расстоянии от фокальной плоскости камеры. При существующих технологиях особенности текстуры кольцевой радужной оболочки извлекаются в вектор-инвариантным положением с постоянной длиной. Предлагаемый подход позволяет очень точно и быстро распознавать человека. Однако, независимо от его явных преимуществ, биометрические данные на основе радужной оболочки можно рассматривать как менее приемлемый и технически требовательный подход, например, для беспроводных приложений (Таблица 1).

Таблица 1 – Общие физиологические характеристики с их атрибутами для биометрической аутентификации

Физиологические характеристики	Преимущества	Недостатки
Лицо	- Естественная и общая характеристика. - Бесконтактное получение изображений. - Камеры интегрируются во многие системы.	- Нарушение точности, например, из-за изменения внешнего вида лица. - Условия изображения являются критическими. - Использование беспроводной сети требует дополнительных требований к методам визуализации.

Отпечаток пальцев	- Исторически зрелый подход. - Расширенные технологии распознавания и алгоритмов. - Значительно простое использование изображений.	- Криминологическая история может вызвать проблемы приемлемости. - Качество отпечатков пальцев варьируется в зависимости от населения. - При использовании в беспроводной сети примечание о недостаточном надзоре заслуживает внимания.
Радужная оболочка	- Черты радужной оболочки уникальны и стабильны. - Получение изображения без физического контакта. - Высокая точность в FAR.	- Требование условий визуализации. - Потенциально менее приемлемый из-за неудобной работы.
Спектральная биометрия	- Основано на измерении света, рассеянного кожей. - Маленький и простой в использовании датчик. - Простая обработка данных.	- Будучи новым подходом, уникальность и постоянство этого способа идентификации еще изучается.

Голос: Несмотря на то, что голос является очень естественной характеристикой человека и признан годным для биометрической аутентификации, он не очень точен для аутентификации по нескольким причинам (Таблица 2). Когда рассматривается проверка верификации, существуют два основных подхода к аутентификации: текстовый подход, основанный на фиксированной фразе, и текстовый подход, использующий нефиксированные фразы. Более того, еще более сложный подход заключается в применении методов, не зависящих от языка. Сильным атрибутом голосовой биометрии является то, что требуемый датчик и, следовательно, фактические биометрические данные в настоящее время предоставляются мобильными телефонами [3].

Таблица 2 – Общие поведенческие характеристики с их атрибутами для биометрической аутентификации

Поведенческие характеристики	Преимущества	Недостатки
Голос	- Обычно доступно в системах связи. - Необходимые устройства существуют, например, на мобильных телефонах. - Возможен интерактивный протокол аутентификации.	- Состояние предмета и окружающей среды оказывает сильное влияние на производительность. - Менее приемлемый в общественных местах.
Подпись	- Длинная история и приемлемая. - Независимо от родного языка. - Динамические функции улучшают производительность.	- Естественная изменчивость подписей. - Постоянство является спорным, поскольку человек может изменить свою подпись.
Динамика нажатия клавиш	- Доступно в компьютерных средах.	- Зависит от клавиатуры и эмоций человека. - Менее приемлемо, если клавиатура постоянно контролируется.

Биометрические технологии постоянно продвигаются к коммерческой реализации в беспроводных устройствах. В этой статье был указан ряд биометрических технологий и ограничений на основе параметров беспроводной сети, которые определяют возможность и эффективность функции аутентификации. Защита различных персональных данных, открытие заблокированных пользовательских интерфейсов, мобильная торговля и контроль доступа могут быть приложениями, которые будут полезны при проверке на основе биометрических данных. При тщательном проектировании и внедрении преимущество возникает в основном за счет увеличения удобства и совместной безопасности [4].

Список использованных источников

1. Данилов Б.С. Основы биометрии / КомпьютерПресс. 2014 – № 2. С. 45-52.
2. Иванов А. И. Нейросетевые алгоритмы биометрической идентификации личности / А. И. Иванов. – М.: Радиотехника, 2004. – 56 с.
3. Цылин Д. Аутентификация личности // Электроника: наука, технология, бизнес. – 2008. – № 5. – 10-12 с.
4. Гниненко В. Биометрические черты и их характеристики // Нальчик: Звезда, 2016. – 200 с.

ӘОЖ 621.391.037.3

ЖҮЛҮ ЭЛЕКТР СТАНСАСЫНЫҢ ЖҰМЫСЫН ARDUINO МК НОБАЙЛАУ

Ақжүніс Ініят, Сатыбалды Асқар

Л.Н. Гумилев атындағы ЕҰУ РЭТ-39/1, РЭТ-49/1 топтарының студенттері.

Ғылыми жетекшісі - РЭТ кафедрасының профессоры Әубәкір Д. Ә.

Кіріспе.

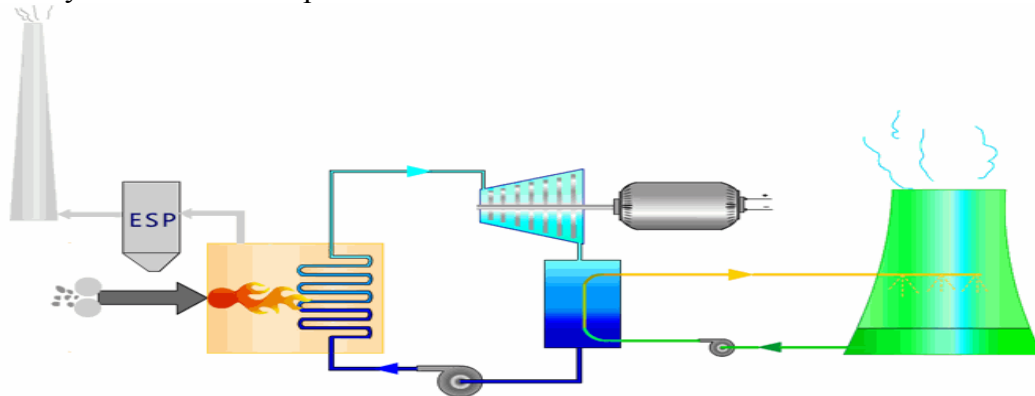
Электр стансасы – қандай да бір энергияны электрліге айналдыруда қызмет ететін энергетикалық құрылғы.

Электр стансасының түрі ең алдымен энерготасымалдаушысының түрімен анықталады. Органикалық отынды (көмір, мұнай, газ және т.б.) жағуда бөлінетін жылу энергиясы қолданылатын жылу электр стансалары (ЖЭС) кең қолданыс тапты.

1 ЖЭС Негізгі жұмыс істеу қағидасы

ЖЭС-да отынның жылуымен суды қайнатып, одан шыққан жоғары қысымды бумен генераторға жалғанған жапырақты дөңгелектерді айналдырып электр қуатын шығарады.

Булар үлкен моржаның сүзгісінен өтіп қайта суға айналып, суыған соң насос арқылы ысыту құбырларына қайта жіберіліп отырды сөйтіп барлық процес қайталана береді де электр қуаты тоқтаусыз алынып отырады.



Сурет 1 – ЖЭС құрылымының жалпы сызбасы