



Қазақ технология және бизнес университеті
Казакский университет технологии и бизнеса
Kazakh university of technology and business

№ 3 (2020)

ҚазТБУ Хабаршысы

Вестник КазУТБ

Vestnik KazUTB



ISSN (Print) 2708 - 4132

ISSN (Online) 2663 - 1830

Қазақ технология және бизнес университеті
Kazakh University of Technology and Business
Казахский университет технологии и бизнеса

ҚазТБУ ХАБАРШЫСЫ
VESTNIK KazUTB
ВЕСТНИК КазУТБ

№ 3 (2020)

Жылына 4 рет шығады

Published 4 times a year

Выходит 4 раза в год

Нұр-Сұлтан, 2020

Nur-Sultan, 2020

Нур-Султан, 2020

Главный редактор: Ж.З.Уразбаев

д.т.н., профессор Президент-ректор АО «КазУТБ»

Заместитель главного редактора: Н. Г.Джумамухамбетов

д.ф.-м.н, профессор

Редакционная коллегия:

Кулажанов К.С. д.х.н., профессор, академик НАН РК (Казахстан)

Надиров Н.К. д.х.н., профессор, академик НАН РК (Казахстан)

Мансуров З.А. д.х.н., профессор, академик НАН РК (Казахстан)

Фазылов С.Д. д.х.н., профессор, академик НАН РК (Казахстан)

Кулажанов Т.К. д.х.н., профессор, академик НАН РК (Казахстан)

Изтаев А.И. д.т.н., профессор, академик НАН РК (Казахстан)

Нурахметов Б.К. д.т.н., профессор (Казахстан)

Шеров Т.К. д.т.н., профессор (Казахстан)

Рубен М.П. доктор философии (PhD) (Испания)

Жилисбаева Р.О. д.т.н., профессор (Казахстан)

Какимов А.К. д.т.н., профессор (Казахстан)

Узаков Я.М. д.т.н., профессор (Казахстан)

Додаев К.О. д.т.н., профессор (Узбекистан)

Кузнецов О.Л. д.т.н., профессор (Россия)

Маткаримов Б.Т. д.т.н., профессор (Казахстан)

Боранбаев С.Н. д.т.н., профессор (Казахстан)

Пешков В. доктор философии (PhD), (Бельгия)

Мымрин В.А. д.т.н., профессор (Бразилия)

Мухамедиев Б.М. д.э.н., профессор (Казахстан)

Смагулова Ш.А. д.т.н., профессор (Казахстан)

Искакова Ж.Б. к.х.н., асс. профессор (Казахстан)

Ответственный секретарь, к.ф.-м.н. М.К. Оспанова

Собственник: АО «Казахский университет технологии и бизнеса».

Регистрация: Министерство информации и коммуникаций Республики Казахстан.

Комитет Информации. Дата и номер первичной постановки на учет: №14139-Ж от 07.02.2014.

Вторичная постановка на учет: 11.02.2020 - № KZ46VPY00020253.

Периодичность: Ежеквартально. ISSN: 2708- 4132, ISSN (Online): 2663-1830.

Тематическая направленность: Информационно-коммуникационные и химические технологии, Производственные и обрабатывающие отрасли Экономика, бизнес и услуги.

Адрес редакции: 010000, г.Нур - Султан, Есильский район, ул.Кайыма Мухамедханова,

37 «А», тел.:(7172) 27-92-30 (134), e-mail: journal.vestnik.kazutb@mail.ru

© Казахский университет технологии и бизнеса

МАЗМҰНЫ \ CONTENTS \ СОДЕРЖАНИЕ

Ақпараттық-коммуникациялық және химиялық технология

Information and communication and chemical technologies

Информационно-коммуникационные и химические технологии

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Мазаков Т.Ж., Джомартова Ш.А., Турсынбай А.Т., Жакып Б.М. АНАЛИТИЧЕСКОЕ РЕШЕНИЕ ОБРАТНОЙ ЗАДАЧИ ФАРМАКОКИНЕТИКИ МЕТОДАМИ КОМПЬЮТЕРНОЙ АЛГЕБРЫ И ДИХОТОМИИ | 8-19 |
| Джомартова Ш.А., Байрбекова Г.С., Шорманов Т.С., Зиятбекова Г.З., Элиасқар М.С., Мазакова А.Т. МНОГОПАРАМЕТРИЧЕСКАЯ АВТОМАТИЗИРОВАННАЯ СИСТЕМА БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ | 20-35 |
| Нургалиев Н.У., Колпек А. ИССЛЕДОВАНИЕ КИНЕТИКИ ТЕРМИЧЕСКОЙ ДЕСТРУКЦИИ УГЛЯ МЕСТОРОЖДЕНИЯ БОРЛЫ | 36-42 |
| Жалмаханбетова Р.И., Мухитдинова М.И., Жұмағалиева Ж.Ж. ХЛОР АТОМЫ БАР ТАБИҒИ СЕСКВИТЕРПЕНДІ ЛАКТОНДАР(шолу) | 43-50 |

УДК 51-76; 004.8

**Ш.А. Джомартова^{1,2}, Г.С. Байрбекова², Т.С. Шорманов²,
Г.З. Зиятбекова^{1,2}, М.С. Элиасқар^{1,2}, А.Т. Мазакова²**

(¹Институт информационных и вычислительных технологий КН МОН РК, Казахстан, Алматы,

²Казахский национальный университет имени аль-Фараби,

Казахстан, Алматы, tmazakov@mail.ru)

МНОГОПАРАМЕТРИЧЕСКАЯ АВТОМАТИЗИРОВАННАЯ СИСТЕМА БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ

Аннотация. Статья посвящена разработке системы биометрической идентификации человека по лицу, отпечаткам пальца и голосу. В качестве информативных признаков биометрической идентификации человека по лицу использованы двумерные и трехмерные характеристики лица человека, учитывающие площадь и объем. Для учета таких явлений, как сдвиг портрета, разный масштаб фотографий и наклон идентифицируемого лица, разработан сложный алгоритм идентификации. Для биометрической идентификации человека по отпечаткам пальцев использован сканер FPM10A и микроконтроллер Arduino. Идентификационные признаки основаны на анализе строения папиллярных узоров на пальца: тип и вид папиллярного узора; направление и крутизна потоков папиллярных линий; строение центрального рисунка узора; строение дельты; количество папиллярных линий между центром и дельтой и множество других признаков.

Другой тип признаков – локальные. Их также называют минуциями (особенностями или особыми точками) – уникальные признаки присущие только конкретному отпечатку, определяющие пункты изменения структуры папиллярных линий (окончание, раздвоение, разрыв и т. д.), ориентацию папиллярных линий и координаты в этих пунктах. Каждый отпечаток может содержать до 70 и более минуций. Для биометрической идентификации человека по голосу использованы алгоритмы MFCC и PLP для цифровой обработки и анализа аудиозаписей. Для акустического анализа речи применены различные алгоритмы: скрытые марковские модели, модель смеси гауссовских распределений. Получен результат определения тональности речи и содержательности речи для целей идентификации по голосу. На СУБД Visual FoxPro разработана «Многопараметрическая автоматизированная система биометрической идентификации личности».

Ключевые слова: защита информации, двухмерное и трехмерное изображение, идентификация, папиллярные узоры, характеристика голоса, человеческая речь, акустическое моделирование.

**Sh.A. Jomartova^{1,2}, G.S. Bayrbekova², T.S. Shormanov²,
G.Z. Ziyatbekova^{1,2}, M.S. Aliaskar^{1,2}, A.T. Mazakova²**

(¹RSE Institute of Information and Computational Technologies MES RK CS, Almaty, Kazakhstan,

²Al-Farabi Kazakh National University, Almaty, Kazakhstan. jomartova@mail.ru)

MULTIPARAMETER AUTOMATED SYSTEM FOR BIOMETRIC IDENTIFICATION OF A PERSON

Abstract. The article is devoted to the development of a system for biometric identification of a person by face, fingerprints and voice. As informative signs of biometric identification of a person by face, two-dimensional and three-dimensional characteristics of a person's face were used, taking into account the area and volume. A sophisticated identification algorithm has been developed to take into account such phenomena as portrait shift, different photo scales and the tilt of the identified person. For biometric identification of a person by fingerprints, an FPM10A scanner and an Arduino microcontroller were used. Identification signs are based on the analysis of the structure of papillary patterns on the finger: type and type of papillary pattern; direction and steepness of streams of papillary lines; the structure of the central pattern of the pattern; delta structure; the number of papillary lines between the center and the delta and many other signs.

Another type of signs is local. They are also called minutiae (features or special points) - unique features inherent only in a particular imprint, determining the points of change in the structure of papillary lines (ending, bifurcation, break, etc.), the orientation of the papillary lines and coordinates at these points. Each print can contain up to 70 or more minutes. For biometric identification of a person by voice, the MFCC and PLP algorithms are used for digital processing and analysis of audio recordings. Various algorithms are used for acoustic analysis of speech: hidden Markov models, a model of a mixture of Gaussian distributions. The result of determining the tone of speech and the content of speech for the purposes of identification by voice is obtained. The "Multiparameter automated system of biometric identification of a person" has been developed on the Visual FoxPro DBMS.

Key words: information security, two-dimensional and three-dimensional image, identification, papillary patterns, voice characteristics, human speech, acoustic modeling.

Ш.А. Джомартова^{1,2}, Г.С. Байрбекова², Т.С. Шорманов²,
Г.З. Зиятбекова^{1,2}, М.С. Әлиасқар^{1,2}, А.Т. Мазакова²

(¹Қазақстан Республикасының Білім және Ғылым Министрлігі Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан,

²Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан, jomartova@mail.ru)

АДАМДЫ БИОМЕТРИЯЛЫҚ СӘЙКЕСТЕНДІРУДІҢ КӨППАРАМЕТРЛІ АВТОМАТТАНДЫРЫЛҒАН ЖҮЙЕСІ

Аңдатпа. Мақала адамды бет, саусақ іздері мен дауысы бойынша биометриялық сәйкестендіру жүйесін жасауға арналған. Адамның бет-әлпетінің екі өлшемді және үш өлшемді сипаттамалары, ауданы мен көлемін ескере отырып, тұлғаны биометриялық сәйкестендірудің ақпараттық белгілері ретінде қолданылады. Портреттің ауысуы, әртүрлі фотосуреттер және сәйкестендірілген адамның еңкеюі сияқты құбылыстарды ескеретін күрделі сәйкестендіру алгоритмі жасалған. Саусақ іздері бойынша адамды биометриялық сәйкестендіру үшін FPM10A сканері және Arduino микроконтроллері қолданылды. Сәйкестендіру белгілері саусақтағы папиллярлы өрнектердің құрылымын талдауға негізделген: папиллярлық өрнектің түрі мен түрі; папиллярлық сызықтар ағындарының бағыты және тік болуы; өрнектің орталық өрнегінің құрылымын; атырау құрылымы; орталық пен дельта арасындағы папиллярлық сызықтардың саны және көптеген басқа белгілер.

Белгілердің тағы бір түрі - жергілікті. Оларды ерекшеліктері немесе арнайы нүктелеріне қарай минуция деп те атайды. Папиллярлық сызықтар құрылымының өзгеру нүктелерін анықтайтын (аяқталу, екі сызықты болуы, үзіліс және т.б.), сондай-ақ, папиллярлық сызықтар мен осы нүктелердегі координаттардың бағдарын анықтайтын, нақты ізге ғана тән ерекше белгілері болады. Саусақ іздерінің әр басылымы 70 немесе одан да көп минуцияны қамтуы мүмкін. Адамды дауысы бойынша биометриялық сәйкестендіруге, сонымен қатар цифрлық өңдеу мен аудиожазбаларды талдау үшін MFCC және PLP алгоритмдері қолданылады. Сөйлеудің акустикалық талдауы үшін әр түрлі алгоритмдер қолданылады: жасырын Марков модельдері, Гаусс үлестірімдері қоспасының моделі. Дауыспен сәйкестендіру мақсатында сөйлеу тонын және сөйлеу мазмұнын анықтаудың нәтижелері алынды. Visual FoxPro ДҚБЖ-да «Адамды биометриялық сәйкестендірудің көппараметрлі автоматтандырылған жүйесі» жасалды.

Түйін сөздер: ақпараттық қауіпсіздік, екі өлшемді және үш өлшемді сурет, сәйкестендіру, папиллярлық өрнектер, дауыстық сипаттама, адамның сөйлеуі, акустикалық модельдеу.

Введение. Проблема защиты информации и информационной безопасности является одним из важнейших аспектов развития современного общества. В настоящее время решение этой проблемы в области разработки и эксплуатации информационных систем различного назначения связано с разработкой всевозможных требований к обеспечению их безопасности и созданием программно-аппаратных средств от несанкционированного доступа [1-3].

Автоматическое распознавание человека для установления личности имеет большое количество приложений в различных областях. Проблемы общественной безопасности, потребность в удаленной аутентификации, развитие человеко-машинных интерфейсов вызывает повышенный интерес к данной технологии [4-5].

Все более широкое применение находят в системах контроля доступа к рабочим местам, мобильным устройствам, локальным и глобальным информационным ресурсам методы биометрической идентификации личности. Так как для реализации систем не требуется специализированная техника, а биометрический признак нельзя потерять, забыть или передать, наиболее перспективными являются системы, принцип работы которых основан на распознавании лица человека [6].

В Указе Президента Республики Казахстан от 10 октября 2006 года N 199 «О Концепции информационной безопасности Республики Казахстан» отмечено: «Анализ современного состояния информационной безопасности

в Казахстане показывает, что ее уровень в настоящее время не соответствует потребностям человека, общества и государства» и в качестве основной цели обеспечения информационной безопасности указано: «создание и укрепление национальной системы защиты информации, в том числе в государственных информационных ресурсах».

31 января 2017 г. Президент Республики Казахстан Нурсултан Абишевич Назарбаев обратился к казахстанцам с посланием «Третья модернизация Казахстана: глобальная конкурентоспособность». В этом обращении отмечена необходимость разработки и принятия программы «Цифровой Казахстан». В связи с этим по поручению Н.А. Назарбаева в целях обеспечения информационной безопасности общества и государства в сфере информатизации и связи, а также защиты неприкосновенности частной жизни граждан при использовании ими информационно-коммуникационных технологий разработана Концепция «Киберщит Казахстана». В ней отмечено, что особого внимания требуют вопросы подготовки кадров в вузах Казахстана по информационной безопасности и разработки отечественных средств защиты информации.

Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают 100 % идентификацию. На данный момент в биометрических системах для аутентификации пользователя успешно используются следующие биометрические характеристики: радужная оболочка глаза, отпечаток пальца, отпечаток

Белгілердің тағы бір түрі - жергілікті. Оларды ерекшеліктері немесе арнайы нүктелеріне қарай минуция деп те атайды. Папиллярлық сызықтар құрылымының өзгеру нүктелерін анықтайтын (аяқталу, екі сызықты болуы, үзіліс және т.б.), сондай-ақ, папиллярлық сызықтар мен осы нүктелердегі координаттардың бағдарын анықтайтын, нақты ізге ғана тән ерекше белгілері болады. Саусақ іздерінің әр басылымы 70 немесе одан да көп минуцияны қамтуы мүмкін. Адамды дауысы бойынша биометриялық сәйкестендіруге, сонымен қатар цифрлық өңдеу мен аудиожазбаларды талдау үшін MFCC және PLP алгоритмдері қолданылады. Сөйлеудің акустикалық талдауы үшін әр түрлі алгоритмдер қолданылады: жасырын Марков модельдері, Гаусс үлестірімдері қоспасының моделі. Дауыспен сәйкестендіру мақсатында сөйлеу тонын және сөйлеу мазмұнын анықтаудың нәтижелері алынды. Visual FoxPro ДҚБЖ-да «Адамды биометриялық сәйкестендірудің көппараметрлі автоматтандырылған жүйесі» жасалды.

Түйін сөздер: ақпараттық қауіпсіздік, екі өлшемді және үш өлшемді сурет, сәйкестендіру, папиллярлық өрнектер, дауыстық сипаттама, адамның сөйлеуі, акустикалық модельдеу.

Введение. Проблема защиты информации и информационной безопасности является одним из важнейших аспектов развития современного общества. В настоящее время решение этой проблемы в области разработки и эксплуатации информационных систем различного назначения связано с разработкой всевозможных требований к обеспечению их безопасности и созданием программно-аппаратных средств от несанкционированного доступа [1-3].

Автоматическое распознавание человека для установления личности имеет большое количество приложений в различных областях. Проблемы общественной безопасности, потребность в удаленной аутентификации, развитие человеко-машинных интерфейсов вызывает повышенный интерес к данной технологии [4-5].

Все более широкое применение находят в системах контроля доступа к рабочим местам, мобильным устройствам, локальным и глобальным информационным ресурсам методы биометрической идентификации личности. Так как для реализации систем не требуется специализированная техника, а биометрический признак нельзя потерять, забыть или передать, наиболее перспективными являются системы, принцип работы которых основан на распознавании лица человека [6].

В Указе Президента Республики Казахстан от 10 октября 2006 года N 199 «О Концепции информационной безопасности Республики Казахстан» отмечено: «Анализ современного состояния информационной безопасности

в Казахстане показывает, что ее уровень в настоящее время не соответствует потребностям человека, общества и государства» и в качестве основной цели обеспечения информационной безопасности указано: «создание и укрепление национальной системы защиты информации, в том числе в государственных информационных ресурсах».

31 января 2017 г. Президент Республики Казахстан Нурсултан Абишевич Назарбаев обратился к казахстанцам с посланием «Третья модернизация Казахстана: глобальная конкурентоспособность». В этом обращении отмечена необходимость разработки и принятия программы «Цифровой Казахстан». В связи с этим по поручению Н.А. Назарбаева в целях обеспечения информационной безопасности общества и государства в сфере информатизации и связи, а также защиты неприкосновенности частной жизни граждан при использовании ими информационно-коммуникационных технологий разработана Концепция «Киберщит Казахстана». В ней отмечено, что особого внимания требуют вопросы подготовки кадров в вузах Казахстана по информационной безопасности и разработки отечественных средств защиты информации.

Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают 100 % идентификацию. На данный момент в биометрических системах для аутентификации пользователя успешно используются следующие биометрические характеристики: радужная оболочка глаза, отпечаток пальца, отпечаток

ладони, сосудистые рисунки, геометрия лица, отпечаток голоса, подпись, сравнение ДНК, которые обладают свойствами, без которых невозможно их практическое применение [7 - 9]:

Всеобщность: каждый человек имеет биометрические характеристики.

Уникальность: не существует двух людей, обладающих полностью одинаковыми биометрическими характеристиками.

Постоянство: биометрические характеристики должны быть стабильны во времени.

Измеряемость: биометрические характеристики должны быть измеряемы каким-либо физическим считывающим устройством.

Также очень важным свойством является приемлемость. Оно менее всего связано с каким-либо определенным биометрическим параметром, однако без его учета нельзя создать полную картину эффективности использования биометрических систем. Комбинация всех перечисленных выше свойств определяет эффективность биометрических систем аутентификации. Основные биометрические характеристики, а также виды их реализации приведены в таблице 1 [10].

В настоящее время не существует биометрических параметров, которые сочетали бы в себе все эти свойства одновременно, особенно если учитывать приемлемость. Поэтому, становится актуальным применение многопараметрической биометрической аутентификации.

Таблица 1– Биометрические характеристики

| Биометрическая характеристика | Регистрирующее устройство | Образец | Исследуемые черты |
|-------------------------------|---------------------------|-------------------------------|--------------------------------------------------------------------------------------------|
| Отпечаток пальца | Сканер | Изображение отпечатка пальцев | Расположение и направление гребешковых выступов и разветвлений на отпечатке пальцев и т.п. |
| Геометрия лица | Видеокамера, фотоаппарат | Изображение лица | Относительное расположение и форма носа и т.п. |
| Голос | Микрофон, телефон | запись голоса | Частота и модуляция голосового образа |

Методы. Как было сказано выше, задача биометрической идентификации личности по лицу, отпечаткам пальца и голосу относятся к одной из задач, решаемых при помощи алгоритмов обработки данных.

Обсуждение. Для программной реализации АС «Биометрическая система защиты информации» выбрана СУБД Visual FoxPro.

Visual FoxPro – это Система Управления Реляционными Базами Данных, основанная на объектно-ориентированном, визуально программируемом языке программирования. Начиная с девятой версии Visual FoxPro поставляется набор классов GDIPlus и MCI.

В GDIPlus поддерживается работа как с растровыми (BMP, GIF, PNG и т.д.), так и с векторными (WMF, EMF)

изображениями. Графический интерфейс устройств (GDIPlus) позволяет разрабатываемым приложениям использовать графику и форматированный текст, для вывода на экран монитора или печати на принтере [11].

Основным свойством GDIPlus для ее использования при программной реализации АРМ «Биометрическая система защиты информации» является следующее:

- возможность загрузки и сохранения изображений из файла, из поля таблицы или переменной;
- возможность получения информации об изображении (определение размера раstra, разрешения раstra, графического формата);
- возможность осуществления ряда операций над изображением (поворот и отражение, отсечение прямоугольного фрагмента, изменение размера изображения, интерполяция);
- возможность самостоятельного рисования в окне формы;
- возможность печати изображений на принтере.

С помощью MCI можно записывать, воспроизводить звуковые и видеофайлы различных форматов. MCI при необходимости использует различные кодеки для

кодирования и декодирования «сжатых» файлов, таких как MP3, WMA или AVI. Управление мультимедийными устройствами и файлами в MCI отличается чрезвычайной простотой. Интерфейс MCI поддерживает 46 команд, таких как открытие файла (OPEN), запуск процесса воспроизведения файла (PLAY), приостановка воспроизведения файла (PAUSE), завершение воспроизведения (CLOSE), получение информации о текущем состоянии процесса воспроизведения (STATUS), позиционирование внутри файла (SEEK), управление воспроизведением звука (SETAUDIO), управление воспроизведением видео (SETVIDEO) и др. На базе СУБД Visual FoxPro 9 реализована интерфейсная часть, включающая следующие режимы: 1) биологические характеристики, 2) параметры характеристик, 3) исходные базы данных, 4) настройка базы данных, 5) простая идентификация, 6) сложная идентификация, 7) классификация [12].

После вызова АРМ появляется главный экран программы, представленный на рисунке 1.

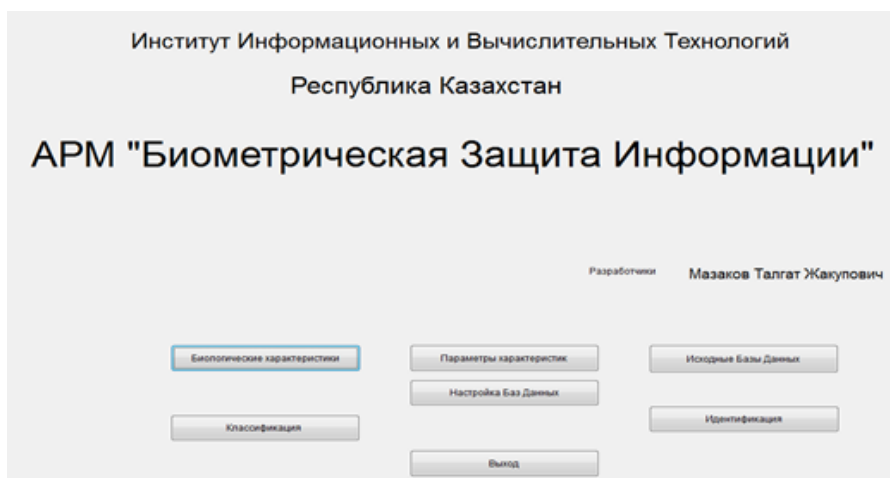


Рис. 1 – Главный экран АРМ

На данный момент в качестве биологической характеристики включены «видеобраз лица», «отпечаток пальца» и «голос».

Режим – «исходные базы данных». В качестве исходных данных для изображений могут быть использованы портреты в следующих графических форматах: bmp, gif, jpeg, tiff и png.

Для режима «видеобраз лица» основной информацией является объемная 3d-модель, представленная как регулярная матрица высот.

В таблице IsxDan.dbf поля имеют следующие назначения: Kodxar – код биометрической характеристики; koddan – код исходного изображения лица;

namdan – имя файла, содержащего изображение лица;
 kla – номер класса, к которому принадлежит изображение
 (вычисляется в режиме «классификация»)

Для параметров характеристик введены следующие типы:
 1 - координата точки; 2 - расстояние (число); 3 - площадь; 4 -
 объем.

В дальнейшем по мере введения новых биометрических характеристик будут вводиться новые типы.

Режим – «классификация». В программе реализована классификация по одному или нескольким параметрам. В данном случае задача классификации состоит в упрощении матрицы данных, слишком обширной для непосредственного анализа человеком. Не существует единственно «правильной» классификации какого-либо набора данных.

Различные численные стратегии обычно приводят к совершенно разным результатам.

Следовательно, необходима помощь консультанта по численным методам для характеристики имеющихся типов классификации, и дело специалиста – выбрать тип, который ему подходит.

Результаты. Основной алгоритм. Начальные действия во всех агломеративных системах одинаковы. Для n индивидов вычисляются все $n(n-1)/2$ мер различия и пара индивидов с наименьшей мерой объединяется в одну группу. Необходимо затем определить подходящую меру различия между этой группой и остальными $n-1$ индивидами, а на более поздних стадиях, очевидно, будет необходимо определить меру между индивидом и группой любого объема, а также между любыми двумя группами. На каждом шаге классификации осуществляется объединение (между двумя индивидами, между индивидами и группой или между двумя группами), для которой мера различия минимальна среди всех оставшихся к данному шагу. Мера должна быть такой, чтобы индивид мог рассматриваться как группа из одного элемента. Стратегия объединения определяется именно мерой различия между группами. Всего в процессе алгоритма вычисляется $(n-1)$ мер. В [13] показано, что d_{ij} - меры обычно могут рассматриваться с позиции одной линейной модели. Пусть имеются две группы i и j с n_i и n_j элементами соответственно;

мера различия между этими группами обозначается d_{ij}
 Допустим, что d_{ij} – минимальная мера из всех оставшихся, так что i и j объединяются и образуют новую группу h с $n_h = n_i + n_j$ элементами. Рассмотрим некоторую другую группу k с n_k элементами. Перед объединением известны значения $d_{hi}, d_{hj}, d_{ij}, n_h, n_i$ и n_j . Положим

$$d_{hk} = \alpha_i d_{hi} + \alpha_j d_{hj} + \beta d_{ij} + \gamma |d_{hi} - d_{hj}| \quad (1)$$

где параметры $\alpha_i, \alpha_j, \beta$ и γ определяют сущность стратегии.

Гибкая стратегия применима для любой меры различия и определяется четырьмя ограничениями: $\alpha_i + \alpha_j + \beta = 1,$

$\alpha_i = \alpha_j, \beta < 1, \gamma = 0.$ Стратегия монотонна, и ее свойства полностью зависят от β . Если $\beta = -0,25$

то стратегия сохраняет метрику пространства. Если принимает положительные значения, то стратегия сжимает пространство, а если

отрицательная, то растягивает. В программе использовала значение $\beta = -0,25$, как рекомендованное для практики.

В программе реализованы различные алгоритмы классификации, так называемые стратегии объединения (агломеративные системы): гибкая стратегия, стратегия ближайшего соседа, стратегия дальнего соседа, стратегия группового среднего, центроидная стратегия, стратегия на сумме квадратов.

«Видеобраз лица»

Для характеристики «видеобраз лица» определены ряд параметров, представляющих собой:

- 1) точку - координаты зрачков глаз, переносицы, кончика носа,
- 2) расстояние – между глазами, между переносицей и кончиком носа, основанием носа,
- 3) периметр - треугольника (зрачки глаз и кончик носа), треугольника (переносица и основание носа),
- 4) площадь – изолинии глазниц, изолинии носа,
- 5) объем – глазниц, носа.

В качестве исходных данных для «видеобраза лица» используется объемная 3d-модель, представленная как регулярная матрица высот [14- 15].

Алгоритмы обработки информационных параметров для идентификации человека по лицу:

1. Координаты центра зрачка левого глаза - (P1x, P1y): определяются из графического файла с фотографией человека;

2. Координаты центра зрачка правого глаза - (P2x, P2y): определяются из графического файла с фотографией человека;

3. Расстояние между зрачками - P3: вычисляются через данные (P1x, P1y) и (P2x, P2y);

4. Глубина левой глазницы - P4: определяются из файла с 3D-данными лица человека;

5. Площадь первой изолинии левой глазницы - P5: вычисляются файла с 3d-данными лица человека путем аппроксимации изолинии эллипсом;

6. Площадь второй изолинии левой глазницы - P6: вычисляются файла с 3d-данными лица человека путем аппроксимации изолинии эллипсом;

7. Площадь третьей изолинии левой глазницы - P7: вычисляются файла с 3d-данными лица человека путем аппроксимации изолинии эллипсом;

8. Объем левой глазницы - P8: вычисляются через данные P5, P6, P7 и расстояние (шаг) между изолиниями;

9. Глубина правой глазницы - P9: вычисляется аналогично параметру P4;

10. Площадь первой изолинии правой глазницы – P10: вычисляется аналогично параметру P5;

11. Площадь второй изолинии правой глазницы – P11: вычисляется аналогично параметру P6;

12. Площадь третьей изолинии правой глазницы – P12: вычисляется аналогично параметру P7;

13. Объем правой глазницы – P13: вычисляется аналогично параметру P8;

14. Координаты кончика носа – (P14x, P14y): определяются из графического файла с фотографией человека;

15. Координаты левого основания носа – (P15x, P15y): определяются из графического файла с фотографией человека;

16. Координаты правого основания носа – (P16x, P16y): определяются из графического файла с фотографией человека;

17. Высота кончика носа – P17: определяются из файла с 3d-данными лица человека;

18. Высота переносицы – P18: определяются из файла с 3d-данными лица человека;

19. Площадь первой изолинии левой носа – P19: вычисляются файла с 3d-данными лица человека путем аппроксимации изолинии трапецией;

20. Площадь второй изолинии левой носа – P20: вычисляются файла с 3d-данными лица человека путем аппроксимации изолинии трапецией;

21. Площадь третьей изолинии левой носа – P21: вычисляются файла с 3d-данными лица человека путем аппроксимации изолинии трапецией;

22. Объем носа – P22: вычисляются через данные P19, P20, P21 и расстояние (шаг) между изолиниями;

23. Периметр треугольника «нос-глаза» – P23: вычисляются через данные (P1x, P1y), (P2x, P2y) и (P14x, P14y);

24. Площадь треугольника «нос-глаза» – P24: вычисляются через данные (P1x, P1y), (P2x, P2y) и (P14x, P14y) по формуле Герона;

25. Отношение «Расстояние между зрачками»/«Расстояние между переносицей и основанием носа» – P25: вычисляются через данные (P1x, P1y), (P2x, P2y) и (P14x, P14y).

Лицо сканируется при помощи 3d сканера от компании HP Intel RealSense SR 300, установленный на ноутбуке HP Pavilion и имеющий ПО Camera Explorer SDK (рисунок 2). После редактирования изображение лица импортируется в формате PLY (ASCII) или в формате XYZ. В формате XYZ сохраняются лишь координаты точек в виде текстового файла, который с легкостью можно открыть в любом текстовом редакторе и обрабатывать в программных расчетах.

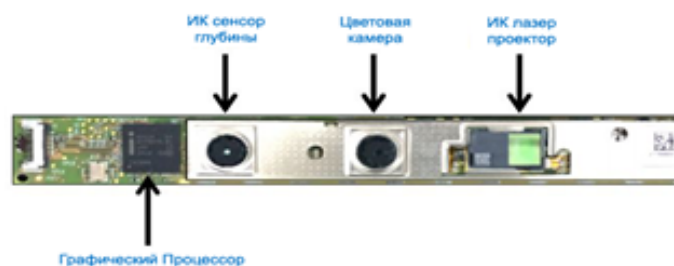


Рис. 2 – Общий вид 3D-сканирующего ноутбука

Алгоритм построения матрицы высот базируется на методе интерполяции поверхностей. В нем неравномерно распределенные точки в трехмерном пространстве интерполируются непрерывной функцией двух независимых переменных. Для построения регулярной матрицы высот выполняются следующие этапы: формирование опорных узлов, вычисление матрицы ближайших точек и матрицы расстояний, интерполяция узлов, корректировка матрицы высот.

Ввиду того, что данные в формате PLY представлены поточечно координатами (x, y, z) разработана программа линейной интерполяции, которая строит регулярную матрицу высот на основе кубической интерполяции.

«Отпечаток пальца»

Системы, основанные на дактилоскопии, сравнивают полученный отпечаток памяти с другими отпечатками, которые хранятся в базах системы или же с отпечатком конкретного человека, способ сравнения также зависит от сферы применения данной технологии [16 - 17].

Для создания блока биометрической системы идентификации человека по отпечаткам пальцев

использован модуль FPM10A с библиотекой Adafruit Arduino [18].

На рисунке 3 представлены элементы блока получения снимка и идентификации отпечатков пальцев. Указанный блок реализован на основе контроллера Arduino UNO.

Arduino – это устройство на основе микроконтроллера ATmega 328 [19]. В его состав входит все необходимое для удобной работы с микроконтроллером: 14 цифровых входов/выходов (из них 6 могут использоваться в качестве ШИМ-выходов), 6 аналоговых входов, кварцевый резонатор на 16 МГц, разъем USB, разъем питания, разъем для внутрисхемного программирования (ICSP) и кнопка сброса.

Оптический сканер отпечатков пальцев - модуль, который можно использовать совместно с Arduino и другими микроконтроллерами [20]. Способен сохранять в памяти отпечатки пальцев (1000 отпечатков) с дальнейшим их идентифицированием. Используется в местах строгой секретности, как своего рода паролевый ключ доступа, основанный на сканировании и сверки отпечатков пальцев с базой данных.



Рис. 3 – Сканер отпечатков пальцев: 1 – FPM10A оптический сканер отпечатков пальцев; 2 – Arduino UNO; 3 – провода для подключение сканера к Arduino; 4 – USB кабель для Arduino

При использовании датчика отпечатка пальцев есть два основных этапа. Сначала записываются данные в память сенсора, то есть присваивается уникальный ID каждому отпечатку, который будет использован для сравнения в дальнейшем. После записи данных, можно переходить к «поиску», сравнивая текущее изображение отпечатка с теми,

которые записаны в памяти датчика.

С помощью программы SFGDemo и ArduinoIDE загружаются новые отпечатки пальцев, присваивая каждому из них новый ID#. Все загруженные изображения отпечатков пальцев зашифрованы (рисунок 4).

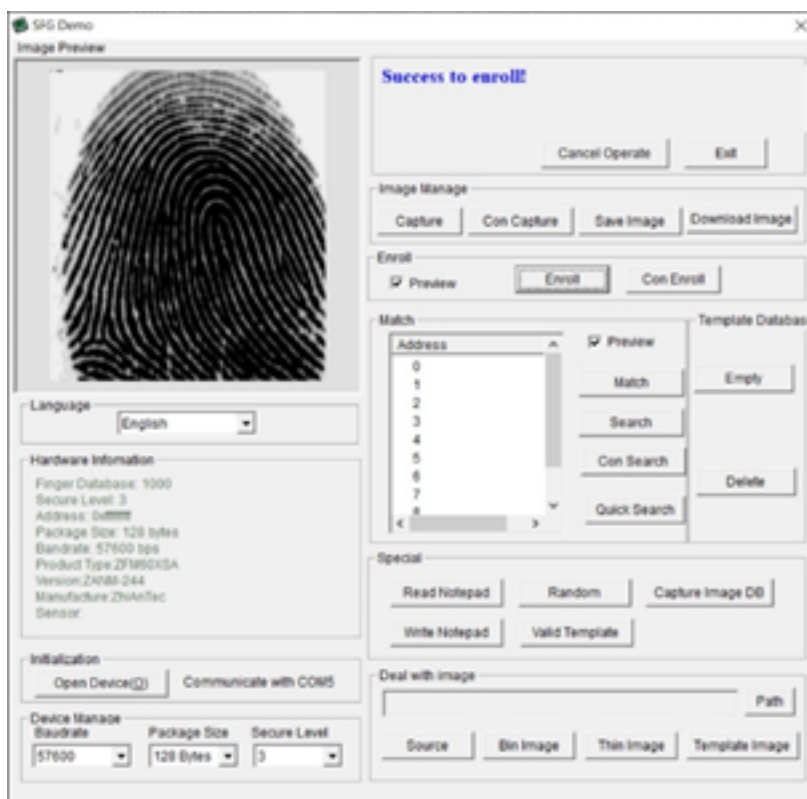


Рис. 4 –Загрузка отпечаток пальцев в базу

На рисунке 5 можно увидеть процент совпадения. Отпечатки пальцев, не совпадающие с отпечатками пальцев, хранящимися в базе, игнорируются сканнером.

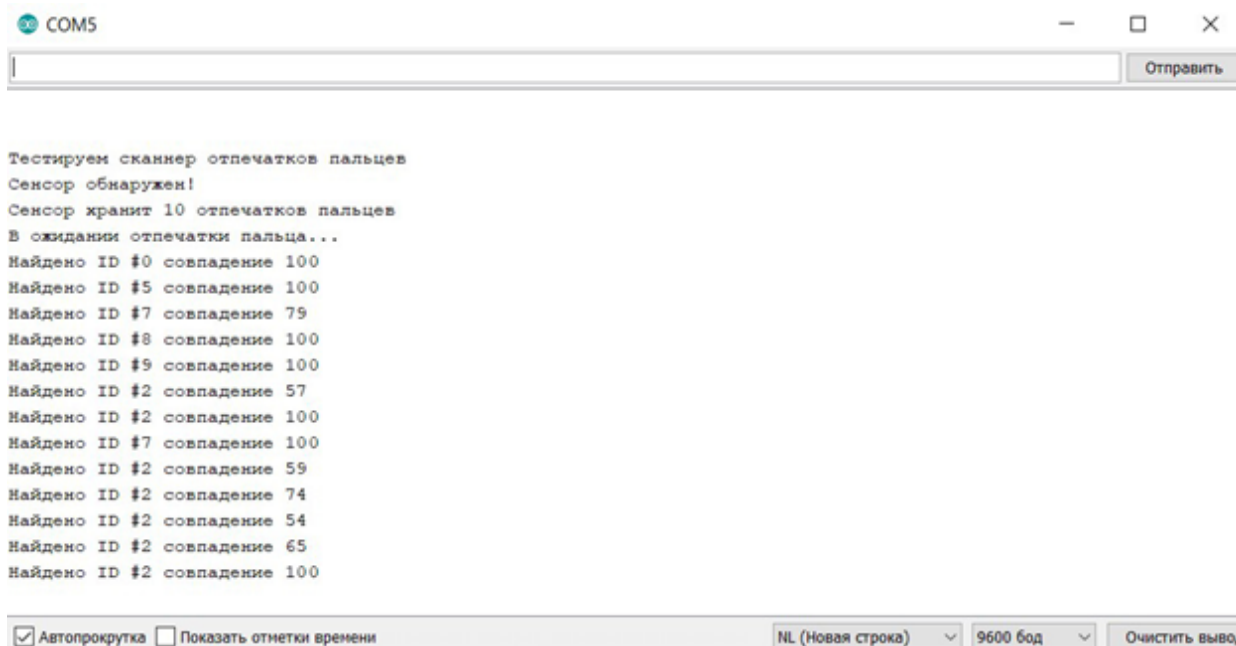


Рис. 5 – Распознавание отпечатков пальцев

Идентификационные признаки строения папиллярных узоров на пальцах принято подразделять на глобальные и локальные признаки [21].

К глобальным относят признаки, которые можно увидеть невооружённым глазом. К таким признакам относятся: тип и вид папиллярного узора; направление и крутизна потоков папиллярных линий; строение центрального рисунка узора; строение дельты; количество папиллярных линий между центром и дельтой и множество других признаков.

Другой тип признаков — локальные. Их также называют минуциями (особенностями или особыми точками) — уникальные признаки присущие только конкретному отпечатку, определяющие пункты изменения структуры папиллярных линий (окончание, раздвоение, разрыв и т. д.), ориентацию папиллярных линий и координаты в этих пунктах. Каждый отпечаток может содержать до 70 и более минуций.

В данном исследовании использованы несколько видов дескрипторов: SIFT, SURF и ORB [22]. По результатам проведенного анализа эффективности и скорости методик и алгоритмов биометрической идентификации лиц можно сделать следующие выводы.

Использование подхода на основании выделения ключевых точек на изображении для проведения биометрической идентификации по отпечаткам пальцев, позволяет создать на ее базе программную систему для быстрого распознавания отпечатков и последующую поиска.

Алгоритмы SURF/SIFT имеют лучшие классифицирующие способности при решении бытовых задачи поиска на текстурированных изображениях. Оба алгоритма более требовательны к аппаратной части и больше подходят для других задач компьютерного зрения, также оба алгоритма запатентованы и имеют запрета на коммерческое использование, без согласия правообладателя. Для задач идентификации по отпечаткам пальцев, они имеют «избыточную мощности».

Алгоритм ORB имеет более высокую скорость работы в сравнение с вышеуказанными алгоритмами методиками SIFT/SURF, и больше подходит для задач биометрической идентификации по отпечаткам пальцев. Дескрипторы алгоритма ORB это бинарные дескрипторы и проверка на

совпадение для таких дескрипторов, это сумма расстояний Хэмминга для каждого байта дескриптора. Применение данного алгоритма больше подходит для задач поиска по не полному отпечатку пальца.

«Голос»

Одним из параметров биометрической идентификации личности является голосу, но голос человека может меняться в зависимости от возраста, эмоционального состояния, здоровья или других факторов, что делает процесс идентификации более сложным к реализации. Технология идентификации по голосу применяется в самых различных сферах защиты информации, систем контроля доступа, криминалистике и других сферах.

Устная речь человека представляет собой упорядоченную систему акустических сигналов, которые воспринимаются как звуковой образ, в устной речи человека отражаются его индивидуальные признаки и особенности. Индивидуальность голоса является следствием формой и размерами ротовой и носовой полости горла и органов дыхания. Таким образом физические характеристики звуков – частота, длительность, интенсивность – у каждого человека строго индивидуальны. Акустическая характеристика голоса относительно устойчива во времени и остается индивидуальной даже при патологических изменениях органов речи. Задача идентификации по голосу состоит в выделении из входного аудиопотока именно человеческую речь, ее классификация и распознавание.

Поскольку, человеческий голос, это сумма множества отдельных частот, создаваемых голосовыми связками, то можно выделить несколько признаков, которые можно наблюдать и проанализировать в речи каждого человека:

- Вокальность речи (громкость, темп, стабильность – физические компоненты);
- Тональность речи (интонация – психологические компоненты);
- Содержательность речи (словарный запас конкретной личности).

Громкость – это субъективная мера ощущения, связанная с воздействием на органы слуха звуковых колебаний и зависящая от амплитуды и частоты данных колебаний.

Темп речи – это субъективная мера, связанная со скорости произношения тех или иных отрезков речи во времени. Темп может быть связан с содержанием, обычно наиболее важные слова произносятся медленнее. Громкость и темп речи индивидуальны для каждого человека.

Человек обладает определенным словарным запасом, это запас определяется его социальными и психическими окружением. Сформировавшиеся в юности примерно к двадцати годам особенности речи, голоса, интонации, а также манера говорить, сохраняются в течение всей жизни и обладают комплексом определенных, только им присущих признаков [23].

Проанализировав отдельные элементы речи можно определить индивидуальную манеру речи человека. Также одной из важнейших характеристик системы голосовой идентификации является скорость (быстродействие) идентификации личности.

Между идентификационными признаками голоса одного и того же человека, полученные в разное время и в разном эмоциональном состоянии, имеются определенные зависимости, которые необходимо установить.

Различие в тембрах разных голосов описывается разными частотными спектрами. Математическим аппаратом для анализа частотного спектра является преобразование Фурье, как способ описать сложную звуковую волну спектрограммой. При расчете спектрограммы второго порядка, выявляются гармоники, которые называются «кепстр», они не удобны для анализа, поскольку дублируют информацию, пример такой гармоники, равномерный фоновый шум или музыка в песне.

Учитывая особенностей слуха человека, а именно его нелинейная природа по отношению к восприятию звуковых частот. Для данной задачи используется преобразование из шкалы Герц в мел-шкалу (мел-психофизическая единица высоты звука) ниже указана формула для перехода между частотой (Гц) и высотой звука в мелах

$$m = 1127 * \ln(1 + f/700) \quad (2)$$

на вычисление спектра применяется набор из M фильтров шкалы мел, обычно M=20 или M=24, обычно, чем больше фильтров, тем выше точность, при этом фильтры смещаются в те частоты, в которых больше всего в аудиозаписи:

$$x_i = \sum_{k=0}^{N-1} |X_k| * H_i(f_k), i = 1..M \quad (3)$$

Фильтр шкалы мел H имеет треугольный вид, пример такого фильтра показан ниже (рисунок 5).

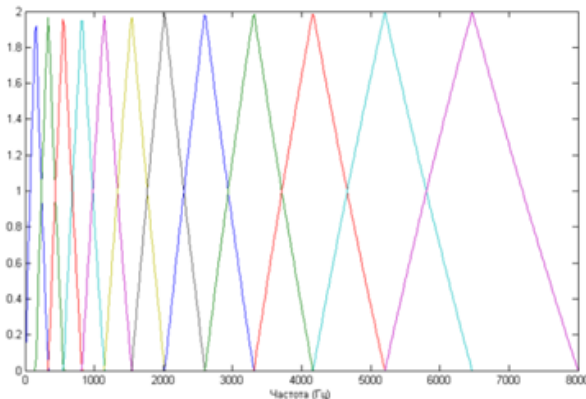


Рис.5 – Пример Мел-фильтра

Для акустического анализа речи также применяются самые различные алгоритмы, наиболее распространенными являются скрытые марковские модели (СММ или НММ в английской версии), а также модель смеси гауссовских распределений (СГР или GMM в английской версии), в последние годы активно применяются нейронные сети [24].

Акустическое моделирование с помощью скрытой марковской модели позволяет определить содержательность речи и предсказать слова, которые будут использованы для идентификации, что в свою очередь позволяет повысить точность идентификации. Недостатком данного подхода является необходимость подготовки языковой модели, а для этого необходимо собрать большую обучающую выборку аудиозаписей, которую необходимо предварительно «разметить» и оцифровать. Данный подход означает, что необходимо получить записи все возможных звуков для базы данных слов.

Режим– «идентификация». В данном режиме для вводимых данных о человеке (изображения лица, пальца или звукового файла), которого необходимо идентифицировать, вычисляется степень соответствия его с каждым из данных, внесенных в таблицу IsxDan.dbf.

Выводы. Разработана АРМ «Биометрическая система защиты информации». Определены структуры таблиц базы данных и их взаимосвязь. На основе предварительной

классификации объектов ускорен поиск заданного человека в исходной базе. На основе применения методов многокритериальной оптимизации для каждого класса вычисляются свои коэффициенты, позволяющие ранжировать критерии по важности. Исследованы свойства предложенного математического алгоритма.

В алгоритме распознавания человека впервые учтены такие параметры как объем носа, объем глазницы и др. трехмерные характеристики. Для ускорения идентификации все данные, находящиеся в исходной базе данных, предварительно классифицируются.

Для учета таких явлений, как сдвиг портрета, разный масштаб фотографий и наклон идентифицируемого лица, разработан сложный алгоритм идентификации.

Проведенные на модельной задаче численные исследования показали эффективность распознавания человека при изменении масштаба фотографии.

На базе микроконтроллера Arduino и сканера FPM10A разработана система распознавания предназначена для хранения данных, дальнейшей ее обработки, идентификации и отображении снимков отпечатков пальцев.

В качестве идентификационные признаков выбрана

структура строения папиллярных узоров на пальцах. Получен результат совпадении отпечатков пальцев с различным вращением через сканер. Перспективной областью является поиск по не полному отпечатку пальца, поскольку часто на практике имеется только часть отпечатка пальцев для проведения поиска совпадений.

Экспериментальное исследование биометрической идентификации по отпечаткам пальцев, созданной на основе дескрипторов SIFT, SURF и ORB, показало, что разработанная программная система обладает инвариантностью к поворотам изображения. Способна работать в большом диапазоне изменении освещения до 50-70% от уровня освещения на изображении, а также обладает инвариантностью к изменению масштаба и незначительным искажениям.

В системе отработаны три алгоритма по анализу аудиозаписей для решения задачи проведения биометрической идентификации по голосу.

Работа выполнена за счет средств грантового финансирования научных исследований на 2018-2020 годы по проекту AP05131027 «Разработка биометрических методов и средств защиты информации».

Литература

1. Бузов Г.А., Практическое руководство по выявлению специальных технических средств несанкционированного получения информации. – М.: Горячая линия – Телеком.- 2010. – 240 с.
2. Грибунин В.Г., Комплексная система защиты информации на предприятии. – М.: Изд-во «Академия».- 2009. – 416 с.
3. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. – Санкт-Петербург: НИУ ИТМО.- 2012. – 416 с.
4. Болл Р.М., Коннел Дж.Х., Панканти Ш., Ратха Н.К., Сеньор Э.У., Руководство по биометрии. – М.: Техносфера.- 2007. – 368 с.
5. Традиционные методы биометрической аутентификации и идентификации / В.М. Колешко, Е.А. Воробей, П.М. Азизов, А.А. Худницкий, С.А. Снигерев. – Минск: БНТУ.- 2009. – 107 с.
6. Афанасьев А.А., Веденьев Л.Т., Воронцов А.А., Газизова Э.Р., Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. – М.: Горячая линия – Телеком.- 2012. – 550 с.
7. S. Crihalmeanu, A. Ross., Multispectral sclera patterns for ocular biometric recognition, Pattern Recognition Lett.-33 (2012) - pp.1860–1869.

8. Технические средства и методы защиты информации /Под ред. Зайцева А.П. – М.: Изд-во «Машиностроение».- 2009. – 508 с.
9. Шаньгин В.Ф., Комплексная защита информации в корпоративных системах. – М.: ИД «Форум».- 2012. – 592 с.
10. Кухарев Г.А., Каменская Е.И., Матвеев Ю.Н., Щеголева Н.Л., Методы обработки и распознавания изображений лиц в задачах биометрии. – М.: Политехника.- 2013. – 416 с.
11. Клепинин В.Б., Агафонова Т.П. Visual FoxPro 9.0. Наиболее полное руководство. - СПб.: БХВ-Петербург.-2007. – 1216 с.
12. Джомартова Ш.А., Исимов Н.Т., Байрбекова Г.С., Зиятбекова Г.З., Абдразак Ж., Идентификация личности на основе 2D- и 3D-изображений // Вестник Национальной инженерной академии Республики Казахстан.- 2018. – № 2(68). – С.16-20.
13. Айвазян С.А., Бухшбергер В.М., Енюков И.С., Мешалкин Л.Д., Прикладная статистика. Классификация и снижение размерности. – М.: Финансы и статистика.- 1989. – 607 с.
14. Джомартова Ш.А., Мазаков Т.Ж., Мазакова А.Т., Автоматизированная система поиска кольцевых структур // Вестник национальной инженерной академии Республики Казахстан.- 2016. – № 1(59). – С. 59-64.
15. Костюк Ю.Л., Фукс А.Л., Визуально гладкая аппроксимация однозначной поверхности, заданной нерегулярным набором точек // Труды Международной научно-практической конференции. Геоинформатика. – Томск: Изд-во Томского университета.- 2000. С. 41–45.
16. Задорожный В.В. Идентификация по отпечаткам пальцев // PC Magazine / Russian Edition. - 2004. – № 1. – С. 5.
17. Ларина Е.А., Глушко А.А. Сканирующие методы получения отпечатков пальцев // Молодой ученый.- 2016. – №27. – С. 97-107.
18. Петин В.А. Проекты с использованием контроллера Arduino. - СПб.: БХВ-Петербург.- 2016. – 464 с.
19. Бокселл Дж., Изучаем Arduino. 65 проектов своими руками. – СПб.: Питер.- 2017. – 400 с.
20. Белов А.В., Arduino. От азов программирования до создания практических устройств. – СПб.: НиТ, 2018. – 480 с.
21. Tan and B. Bhanu, "Robust fingerprint identification" in International Conference on Image Processing 2002. – Vol. 1. – IEEE, 2002. – pp. 1–277.
22. Ethan Rublee, Vincent Rabaud, Kurt Konolige, Gary Bradski: «ORB: an efficient alternative to SIFT or SURF», Computer Vision (ICCV), IEEE International Conference on. IEEE. pp. 2011.- pp.2564–2571.
23. Россинская Е.Р., Профессия - эксперт (Введение в юридическую специальность). – М.: Юрист.- 1999. – 192 с.
24. Dzmitry Bahdanau, Kyunghyun Cho, and Yoshua Bengio., Neural machine translation by jointly learning to align and translate. CoRR, abs/1409.0473.- 2014.

References

1. Buzov G.A., A Practical guide to identifying special technical means of unauthorized obtaining of information. - М.: Hot line – Telecom.- 2010. - 240 p.
2. Gribunin V. G., Complex system of information protection at the enterprise. – М.: publishing house "Academy".- 2009. – 416 p.

3. Katrin Y. F., Razumovsky, A. V., Spivak A. I., Protection of information by technical means. – Saint Petersburg: ITMO national research University, 2012. – 416 p.
4. ball R. M., Connel J. H., Pankanti S., Ratha N. K., Senior E. U., Guide to biometrics. – M.: Technosphere.- 2007. – 368 p.
5. Traditional methods of biometric authentication and identification / V. M. Koleshko, E. A. Vorobey, P. M. Azizov, A. A. Khudnitsky, S. A. Snigerev. – Minsk: BNTU.- 2009. – 107 p.
6. Afanasyev A. A., Vedenev L. T., Vorontsov A. A., Gazizova E. R., Authentication. Theory and practice of providing secure access to information resources. – Moscow: Hotline – Telecom.- 2012. – 550 p.
7. S. Crihalmeanu, A. Ross., Multispectral sclera patterns for ocular biometric recognition, Pattern Recognition Lett.-33 (2012) - pp.1860–1869.
8. Technical means and methods of information protection /Ed. Zaitseva A. P. – M.: publishing house "mechanical engineering".- 2009. – 508 p.
9. Shang'in V. F., Complex information protection in corporate systems, Moscow: Forum publishing house.- 2012.- 592 p.
10. Kukharev G. A., Kamenskaya E. I., Matveev Yu. N., Shchegoleva N. L. methods of processing and recognition of face images in biometrics problems. – Moscow: Polytechnic.- 2013. – 416 p.
11. Klepinin V. B., Agafonova T. P., Visual FoxPro 9.0. the Most complete guide. - SPb.: BHV-Petersburg.-2007. – 1216 p.
12. Dzhomartova Sh. A., Yessimov N. T., Baibekova G. S., Ziyatbekova G. Z., Abdrazak Zh., Identification of a person based on 2D and 3D images // Bulletin of the National engineering Academy of the Republic of Kazakhstan.- 2018. – № 2(68). – pp. 16-20.
13. Ayvazyan S. A., Bukhshberger V. M., Enyukov I. S., Meshalkin L. D., Applied statistics. Classification and reduction of dimension. – M.: Finance and statistics.- 1989. – 607 p.
14. Dzhomartova sh. a., Mazakov T. Zh., Mazakova A. T., Automated search System for ring structures // Bulletin of the national engineering Academy of the Republic of Kazakhstan.- 2016. – № 1(59). – Pp. 59-64.
15. Kostyuk Yu. L., Fuchs A. L., Visually smooth approximation of a unique surface given by an irregular set of points // Proceedings of the International scientific and practical conference. Geoinformatics. – Tomsk: Tomsk University publishing house.- 2000. P. 41-45.
16. ZADOROZHNY V. V., Identification by fingerprints // PC Magazine / Russian Edition. - 2004. – No. 1. – С. 5.
17. Larina E. A., Glushko A. A., Scanning methods for obtaining fingerprints // Young scientist.- 2016. – No. 27. – Pp. 97-107.
18. Petin V. A., Projects using the Arduino controller. - SPb.: BHV-Petersburg.- 2016. – 464 p.
19. Boxell J., Learning Arduino. 65 projects with your own hands. – SPb.: Piter.- 2017. – 400 p.
20. Belov A.V., Arduino. From the basics of programming to the creation of practical devices. – St. Petersburg: NIT, 2018. – 480 p.
21. Tan and B. Bhanu, "Robust fingerprint identification" in International Conference on Image Processing 2002. – Vol. 1. – IEEE, 2002. – pp. 1–277.

22. Ethan Rublee, Vincent Rabaud, Kurt Konolige, Gary Bradski: «ORB: an efficient alternative to SIFT or SURF», Computer Vision (ICCV), IEEE International Conference on. IEEE. pp. 2011.- pp.2564–2571.
23. Rossinskaya E. R., Profession - expert (Introduction to the legal specialty). – М.: Lawyer.- 1999. – 192 p.
24. Dzmitry Bahdanau, Kyunghyun Cho, and Yoshua Bengio., Neural machine translation by jointly learning to align and translate. CoRR, abs/1409.0473.- 2014.

Сведения об авторах

Джомартова Шолпан Абдразаковна – доктор технических наук, профессор КазНУ имени аль-Фараби;

Байрбекова Ғазиза Серікқызы – доктор PhD;

Шорманов Тимур Серікханович – PhD докторант КазНУ имени аль-Фараби;

Зиятбекова Гулзат Зиятбекқызы – PhD докторант КазНУ имени аль-Фараби;

Әлиасқар М.С. – PhD докторант КазНУ имени аль-Фараби;

Мазакова Айгерим Талгатовна – магистрант КазНУ имени аль-Фараби.

j