Список литературы

1. Бухштаб А. А. Теория чисел – М: Наука, 1975 г.
2. Айерленд К. Классическое введение в современную теорию чисел. М: Мир, 1987.
3. Акушинский И. Л., Юдицкий Д. И. Машинная арифметика в остаточных классах. – М. Советское радио, 1968.
4. Червяков Н. И. Применение системы остаточных классов в цифровых системах обработки и передачи информации. – Ставрополь: СВВиУС, 1984.

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АРМ «БИОМЕТРИЧЕСКАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ»

Байрбекова Г.С., Мазаков Т.Ж., Джомартова Ш.А.

Институт информационных и вычислительных технологий КН МОН РК,
Казахский национальный университет имени аль-Фараби,
e-mail: zika_3086@mail.ru, tmazakov@mail.ru, jomart63@gmail.com

Аннотация

В настоящее время одним из самых перспективных направлений в системах контроля доступа становится использование биометрических данных человека. Для реализации биометрической системы защиты информации рассмотрена подсистема типа АРМ «Биометрическая система защиты информации». Основным требованием к системе программирования АРМ является возможность работы с графическими и звуковыми файлами. Разработана инфологическая модель АРМ «Биометрическая система защиты информации». Определены структуры таблиц базы данных и их взаимосвязь. На базе СУБД VisualFoxPro 9 реализована интерфейсная часть, в качестве биологической характеристики включен «видеообраз лица». Для характеристики «видеообраз лица» определены ряд параметров: в частности «расстояние между зрачками глаз», «площади выпуклых или вогнутых частей лица». Для получения количественных значений параметров характеристик разработан алгоритм вычисления «площади выпуклых или вогнутых частей лица», основанный на построении и анализе триангуляции.

Защита любого объекта включает несколько рубежей, число которых зависит от уровня режимности объекта. При этом во всех случаях важным рубежом является система контроля и управления доступом (СКУД) на объект. Хорошо организованная, с использованием современных технических средств, СКУД позволяет решать целый ряд задач, таких как противодействие промышленному шпионажу, защита конфиденциальной информации, учет рабочего времени, контроль прихода и ухода сотрудников. При реализации конкретных СКУД используются различные способы и реализующие их устройства для идентификации и аутентификации личности [1].

СКУД — один из наиболее развитых сегментов рынка безопасности как в России, так и за рубежом. По данным ряда экспертов, ежегодный прирост рынка СКУД составляет более 25 %. Число специалистов, работающих в сфере технических систем безопасности, превышает 500 тыс. человек [2].

Индустрия безопасности сегодня развивается сильными шагами. Это связано с ростом мировой экономики, а также с подъемом в отдельных отраслях, проявляющих интерес такого рода системам. Примерами таких отраслей могут служить розничная торговля, транспортная сфера, строительство [3].

СКУД — совокупность программно-технических и организационно-методических средств, с помощью которых решаются задачи контроля и управления помещением предприятия, а также оперативный контроль передвижения персонала и временем его нахождения на территории предприятия [4, 5].

Системы контроля доступа сегодня очень динамично развиваются. Предъявление высоких требований к надежности, простоте управления, легкости обслуживания, экономичности в работе и удешевлению базовой стоимости при увеличении функционала СКУД привело к появлению программно-модульных систем, которые обеспечивают гибкость при построении архитектуры каждого конкретного решения[12]. При этом тенденция к созданию интегрированных систем, позволяющих в рамках СКУД объединять охранно-пожарные сигнализации, системы охранного теленаблюдения (CCTV) и обеспечивать диспетчеризацию контролируемых сооружений, привела к созданию действующих комплексных автоматизированных систем безопасности объектов [11]. Сейчас применительно даже к малым объектам можно смело говорить о комплексных системах безопасности и управления[13].

Перспективность и преимущества биометрических технологий создают впечатление однозначности и вседоступности [10]. Однако все не так просто, как кажется на первый взгляд. Грамотная разработка подразумевает большие затраты сил и средств, которые не каждое предприятие сочтет целесообразными[7].

Сегмент СКУД сегодня прочно занят дактилоскопическими считывателями [9,15], которые просты в эксплуатации, недороги и многократно апробированы. Несмотря на их недостатки и достоинства других технологий, практика внедрения говорит за себя — пока это лидирующая технология [23].

В настоящее время одним из самых перспективных направлений в системах контроля доступа становится использование биометрических данных человека. Такой способ аутентификации очень удобен. Однако биометрия находится в самом начале длинного пути, и существует ряд проблем, связанных с относительной новизной данной технологии[16].

На данный момент в биометрических системах для аутентификации пользователя успешно реализованы следующие характеристики: радужная оболочка глаза, отпечаток пальца, отпечаток ладони, сосудистые рисунки [14], геометрия лица, отпечаток голоса, подпись, сравнение ДНК [6, 8].

Для реализации биометрической системы защиты информации рассмотрим подсистему типа АРМ «Биометрическая система защиты информации». Основным требованием к системе программирования АРМ является возможность работы с графическими и звуковыми файлами. Система программирования должна обеспечивать работу со следующими графическими форматами[19]:

Формат BMP (*битовый массив, BitMaP*) – это системный формат операционной системы Windows. В Windows API (набор функций ядра системы) предусмотрены готовые средства для его загрузки, сохранения, отображения и выполнения других стандартных операций по работе с изображениями [18].

структуру цифрового изображения, представленного в виде двумерного массива пикселей, которому предпослана некоторая «шапка» (header), содержащая размеры массива и другую служебную информацию. После загрузки файла в формате BMP сразу обеспечивается доступ к пикселям по их координатам (*x*,*y*). Эти два фактора (простая структура и системная поддержка ОС Windows) делают данный формат крайне привлекательным для использования его в практических задачах на начальных этапах изучения машинного зрения [17].

Формат PCX – исторически первый стандарт представления растровой графики на персональных компьютерах IBM PC. Этот формат изначально применялся в программе Paintbrush фирмы ZSoft и впоследствии был преобразован фирмой Microsoft в WindowsPaintbrush. Формат PCX удобен для хранения искусственных изображений, в которых присутствуют значительные области однородных цветов, и плохо приспособлен для хранения «естественных» изображений, полученных различными устройствами ввода. В связи с этим область применения данного формата в последние годы сокращается, хотя файлы в формате PCX по-прежнему во множестве можно встретить в различных многолетних архивах цифровых изображений.

Разработанный компанией CompuServe формат *GIF*(*GraphicsInterchangeFormat*) был задуман как формат межплатформенного обмена графическими данными. Предназначенный для пересылки файл не может иметь большого объема, поэтому в формате GIF пиксель изображения не кодируется количеством бит более 8. Кроме того, этот формат использует рассмотренный выше алгоритм сжатия данных LZW. Еще одной важной особенностью данного формата является то, что формат GIF позволяет сохранять в одном файле два и более изображений. Существует даже понятие «анимированный GIF»: один из режимов визуализации файла формата GIF предполагает последовательное отображение хранящихся в файле картинок, что создает эффект короткого мультфильма. Такие файлы нашли широкое применение в мультимедийных интернет - приложениях.

В настоящее время формат GIF широко распространен благодаря своей относительной компактности и возможностям «анимации» с использованием текста. Однако в области обработки и анализа изображений эти достоинства не играют определяющей роли.

Формат TIFF (*TaggedImageFileFormat*, формат файлов изображения, снабженных «тегами», то есть метками-дескрипторами) был изначально создан для хранения изображений и серий изображений, оцифрованных с помощью оптических сканеров. По структуре это один из самых сложных и многовариантных форматов хранения изображений. Файлы формата TIFF имеют расширение .tiff или .tif. Каждый файл начинается заголовком изображения (ImageFileHeader, IFH). Важнейший элемент этого заголовка – каталог файлов изображений (ImageFileDirectory, IFD), служащий указателем на информативные структуры данных. IFD представляет собой таблицу для идентификации одной или нескольких порций данных переменной длины, называемых *тегами*. Теги, в свою очередь, хранят информацию об изображениях. В спецификации TIFF определено более 70 различных типов тегов. Такой формат на самом деле представляет собой достаточно гибкое и пространное описание изображения, написанное на специальном языке, основу которого составляют слова-теги, а синтаксис определяется стандартом TIFF.

типов тегов. Файл TIFF может содержать несколько изображений, каждому из которых сопутствуют собственный IFD и набор тегов. Растровые данные в каждом из изображений могут сжиматься с использованием любого из нескольких методов, в число которых входят RLE, LZW и несколько других.

Сложность и гибкость данного формата является, с одной стороны, его достоинством, с другой – порождает целый ряд проблем. Основная из них связана с *совместимостью*. Во-первых, формат столь обширен и трудоемок в реализации, что лишь немногие пакеты, работающие с изображениями, обеспечивают возможность правильного считывания всех существующих модификаций файлов TIFF. Если же в одной программе реализовано одно подмножество формата, а в другой – другое, то велика вероятность того, что файл, сохраненный в одном пакете, не будет корректно прочитан в другом. Во-вторых, предусмотренная для разработчиков оригинального прикладного ПО возможность создавать свои специализированные расширения формата TIFF, добавляя новые теги, чревата тем, что изображения, созданные такими системами будут неверно или не полностью считываться стандартными пакетами, игнорирующими неизвестные им новые теги.

Тем не менее, несмотря на существование указанных проблем, формат TIFF стал «де-факто» стандартом в области хранения и передачи сканерных изображений. Он также активно используется и в области создания приложений машинного зрения.

Формат JPEG был создан в результате работы объединенной группы экспертов в области фотографии JPEG (JointPhotographicExpertsGroup). Он был задуман и разработан как новый международный стандарт сжатия цветных изображений. Группа JPEG взяла на себя задачу разработки общеупотребительного стандарта сжатия с тем, чтобы удовлетворить нуждам большинства возможных устройств и приложений, которые испытывают необходимость в сжатии изображений с высокими степенями сжатия. Эта задача была блестяще решена, и в настоящее время формат JPEG является основным стандартом ввода, хранения и передачи изображений, получаемых от цифровых фотоаппаратов, бытовых видеокамер, web-камерами множества других бытовых и специализированных устройств. При этом формат JPEG действительно одновременно обеспечивает хорошее визуальное качество изображений и высокую степень сжатия данных за счет использования специального алгоритма сжатия, относящегося к классу алгоритмов сжатия с потерями информации. Формат JPEG - достаточно сложный и гибкий формат. Он обеспечивает возможность сжатия/восстановления изображений в четырех различных режимах работы.

Формат PNG (*portablenetworkgraphics*, сокращение произносится по-английски) — растровый формат хранения графической информации, использующий сжатие без потерь.

Формат PNG спроектирован для замены устаревшего и более простого формата GIF, а также, в некоторой степени, для замены значительно более сложного формата TIFF.

Формат PNG позиционируется, прежде всего, для использования в Интернете и редактирования графики.

Формат PNG хранит графическую информацию в сжатом виде. Причём это сжатие производится без потерь, в отличие, например, от JPEG с потерями.

Для программной реализации АРМ «Биометрическая система защиты информации» выбрана СУБД VisualVoxPro.

на объектно-ориентированном, визуально программируемом языке программирования. Начиная с девятой версии VisualVoxPro поставляется набор классов GDIPlus и MCI.

В GDIPlus поддерживается работа как с растровыми (BMP, GIF, PNGи 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 [20].

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 растра, разрешения растра, 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.

В настоящее время на рынке предлагается ряд готовых систем и технологий биометрической идентификации и аутентификации личности.

Система ZNFace компании ZN VisionTechnologies AG – сочетает в себе новейшие компьютерные разработки с системой контроля доступа, основанной на автоматическом распознавании лиц. ZN-камера делает снимок человека, стоящего на рубеже контроля, и проверяет его в считанные доли секунды. Специально разработанный модуль оптического фильтра и функция контроля за живым лицом предотвращает любую попытку обмана путем применения фотографий или масок.

Компьютеризованная база фотоданных ZN-Phantomas – может автоматически сравнивать и идентифицировать лица. Для сравнения годится фотография, фоторобот, рисунок или кадр, полученный при видеосъемке. ZN-Phantomas проводит поиск среди сохраненных в памяти изображений, используя систему распознавания лиц, созданную по образу работы человеческого мозга на базе технологии органического видения. Скорость работы системы позволяет просматривать 10 тыс. изображений за три минуты. Система может работать со всеми SQL-базами данных, использующими ODBC-протокол (Oracle, Sybase SQL, DB2, Informix).

Система FaceIT компании Identix – осуществляет распознавание людей при попадании изображения лица в поле зрения видеокамеры высокого разрешения. Разработки фирмы финансируются госдепартаментом США. Данная система проходит апробацию в аэропортах США. В прессе появлялись сообщения, результаты тестирования нельзя назвать удовлетворительными, однако контракт с фирмой продолжен и теперь акцент переносится на идентификацию по фотографиям. Госдепартамент США собирается обязать гостей США иметь фото установленного образца, дабы облегчить распознавательным программам работу.

Из систем, разработанных в России и СНГ, можно рассмотреть продукцию фирмы AsiaSoftware. Фирма предлагает FRS SDK – комплект разработчика, предназначенный для построения информационно-поисковых систем, связанных с распознаванием лиц, и ряд систем идентификации по изображениям лиц. Система базируется на алгоритмах распознавания и сравнения изображений. Основой этих алгоритмов является модифицированный метод анализа принципиальных компонент, заключающийся в вычислении максимально декореллированных коэффициентов, характеризующих входные образы человеческих лиц. На вход системы подается оцифрованное видеоизображение. Специальные алгоритмы определяют наличие изображения лица человека, выделяют его, определяют точное расположение зрачков, производят позиционирование и масштабирование. После этого происходит автоматическое кодирование выделенного изображения лица человека с целью определения основных характерных признаков. Размер полученного массива признаков составляет примерно 300 байт.

На базе СУБД VisualFoxPro 9 реализована интерфейсная часть, включающая следующие режимы: 1) биологические характеристики, 2) параметры характеристик, 3) исходные базы данных, 4) настройка базы данных, 5) классификация, 6) идентификация.

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

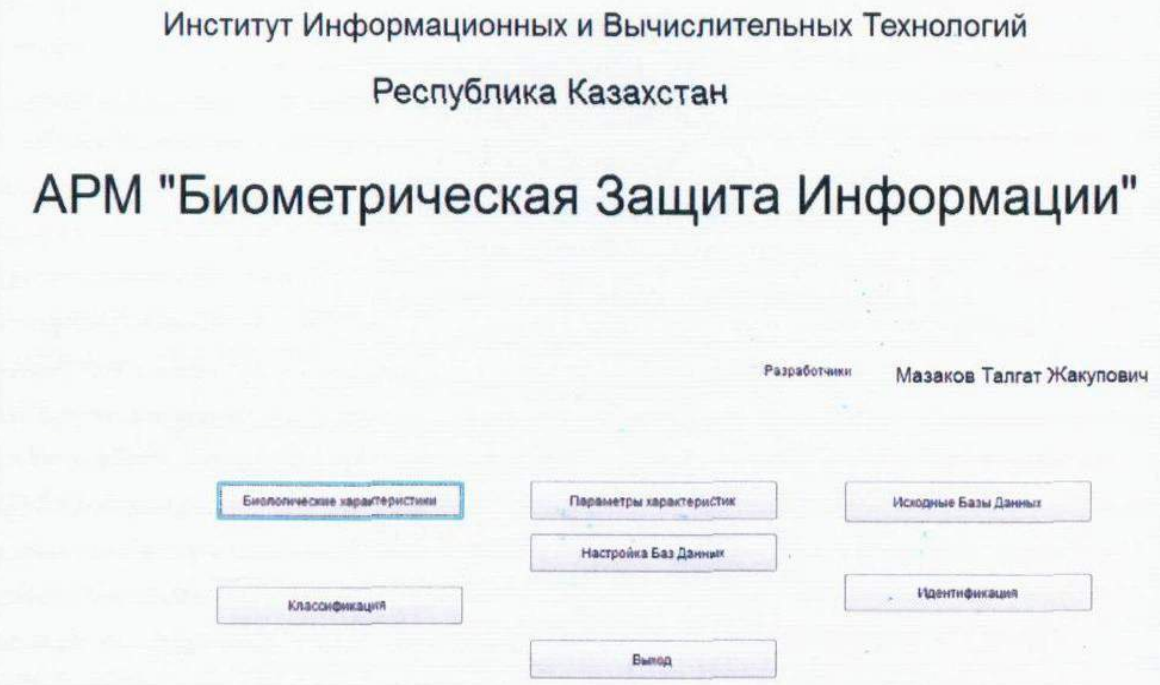

Рис.1. Главный экран АРМ

(структура представлена на рисунке 2), ParXar.dbf (структура представлена на рисунке3), IsxDan.dbf (структура представлена на рисунке 4).

Режим – «биологические характеристики». На данный момент в качестве биологической характеристики включен «видеообраз лица». В дальнейшем планируется работать со следующими биологическими характеристиками: «термограмма лица», «отпечаток пальца», «геометрия руки», «голос» и др.

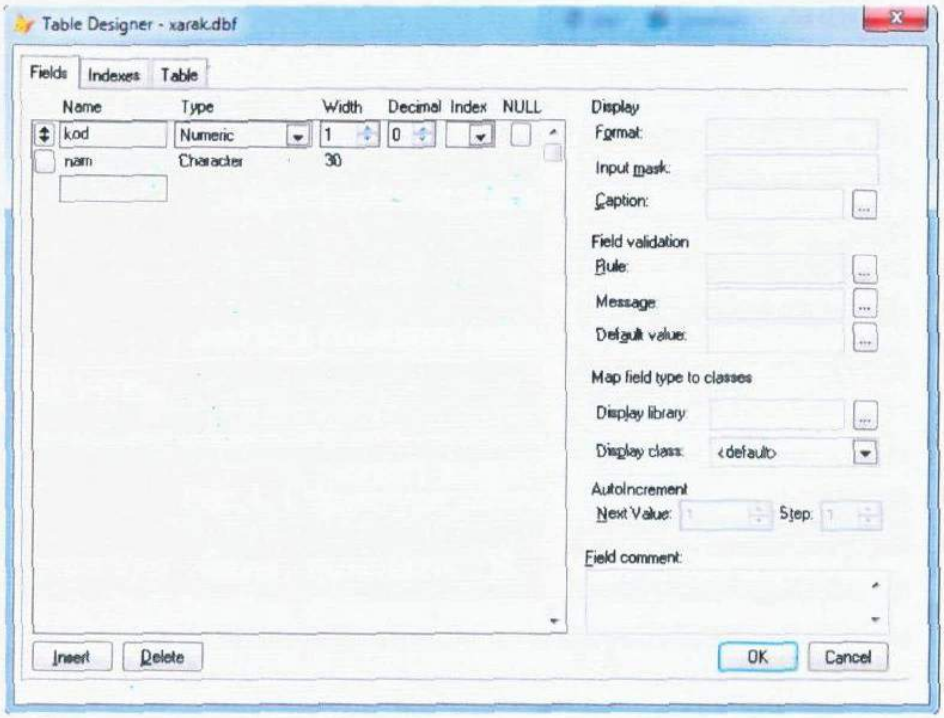

Рис.2. Структура таблицы Xarak.dbf

Для проведения экспериментов в таблицу Xarak.dbf введена одна запись со следующими значениями полей:

kod=1,

nam=«видеообраз лица».

Режим – «параметры характеристик». Для характеристики «видеообраз лица» определены ряд параметров: в частности «расстояние между зрачками глаз», «площади выпуклых или вогнутых частей лица».

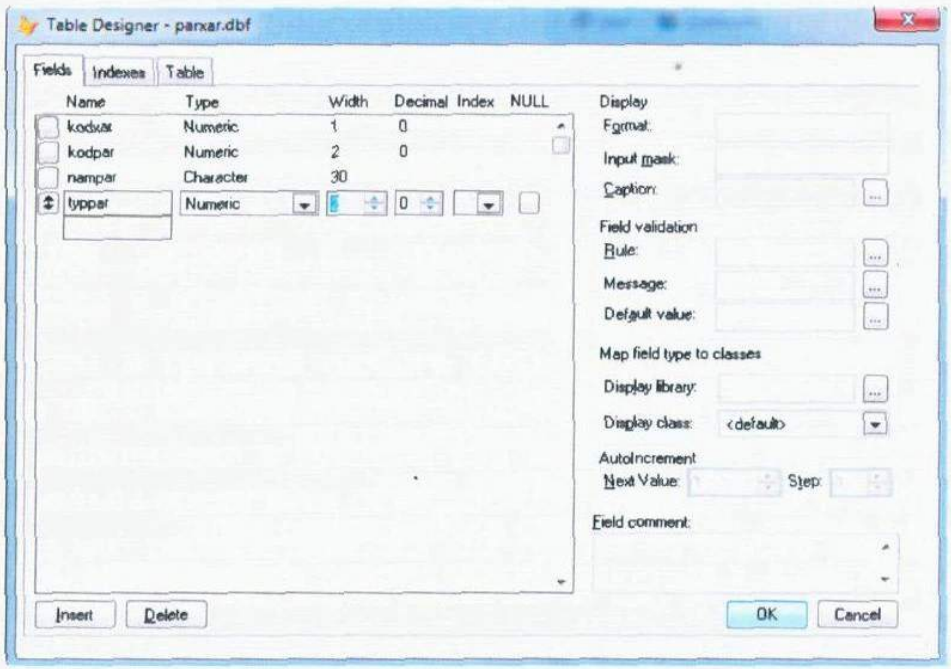

Рис.3. Структура таблицы ParXar.dbf

Для параметров характеристик введены следующие типы:

1 - точка на плоскости (2 координаты);

2 - точка в пространстве (3 координаты);

3 - расстояние (число);

4- многоугольник на плоскости;

5 – изолиния определенного уровня объемной модели.

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

Для проведения экспериментов в таблицу ParXar.dbf введены несколько записей со следующими значениями полей:

1) kodxar=1,kodpar=1,
nampar=«координаты центра зрачка левого глаза»,
typpar=1;

2) kodxar=1,kodpar=1,
nampar=«координаты центра зрачка правого глаза»,
typpar=1;

3) kodxar=1,kodpar=1,
nampar=«расстояние между зрачками глаз»,
typpar=3;

4) kodxar=1,kodpar=1,
nampar=«площадь левой глазницы на первом уровне»,
typpar=5;

5) kodxar=1,kodpar=1,
nampar=«площадь левой глазницына втором уровне»,
typpar=5;

6) kodxar=1,kodpar=1,
nampar=«площадь правой глазницына первом уровне»,
typpar=5;

7) kodxar=1,kodpar=1,
nampar=«площадь правой глазницы на втором уровне»,
typpar=6;

8) kodxar=1,kodpar=1,
nampar=«площадь носа на первом уровне»,
typpar=5;

9) kodxar=1,kodpar=1,
nampar=«площадь носа на втором уровне»,
typpar=5.

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

В таблице IsxDan.dbf поля имеют следующие назначения:

kodxar – код биометрической характеристики;

koddan–код исходного изображения лица;

namdan–имя файла, содержащего изображение лица;

klas– номер класса, к которому принадлежит изображение (вычисляется в режиме «классификация»).

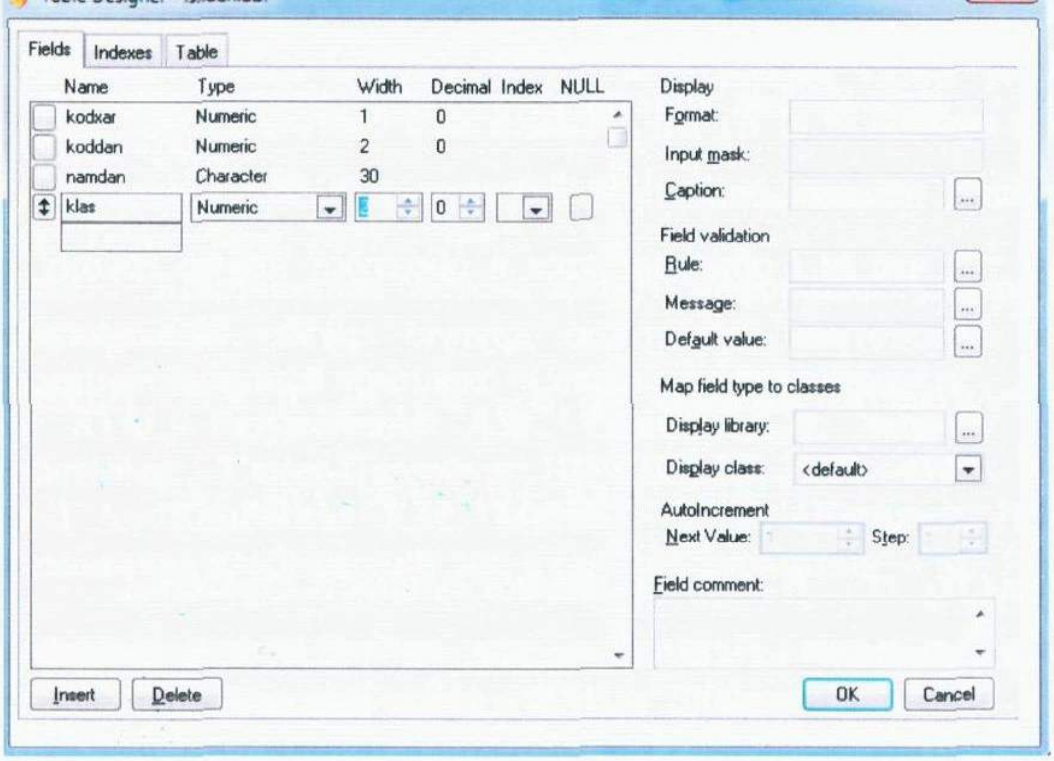

Рис.4. Структура таблицы IsxDan.dbf

Режим – «настройка базы данных». В данном режиме в зависимости от структуры таблиц Xarak.dbfиParXar.dbf в автоматическом режиме создается структура таблицы RezDan.dbf. В дальнейшем в соответствии с типом параметров вычисляются численные характеристики каждого изображения. Для вычисления значений параметров, имеющих тип typpar=5, на основе метода триангуляции [22] строится поверхность лица человека и для некоторых линий уровня строится соответствующая изолиния и вычисляется площадь фигуры, ограниченная этой изолинией.

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.

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 $n-2$ 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.

меры обычно могут рассматриваться с позиции одной линейной модели. Пусть имеются две группы iи jс 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 iи j объединяются и образуют новую группу kс $n_k = n_i + n_j$ элементами. Рассмотрим некоторую другую группу hс n_h элементами. Перед объединением известны значения $d_{hi}, d_{hj}, d_{ij}, n_h, n_i$ и n_j. Положим

$$d_{hk} = \alpha_i d_{hi} + \alpha_j d_{hj} + \beta d_{ij} + \gamma \left| d_{hi} - d_{hj} \right|$$

где параметры α_i, α_j, β 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 $\beta = 0$, то стратегия сохраняет метрику пространства. Если β 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) [25]: гибкая стратегия, стратегия ближайшего соседа, стратегия дальнего соседа, стратегия группового среднего, центроидная стратегия, стратегия на сумме квадратов.

Режим – «идентификация». В данном режиме для вводимого изображения лица, которое необходимо идентифицировать, вычисляется степень соответствия его с каждым из изображений [26], внесенных в таблицу IsxDan.dbf.

Заключение. Разработана инфологическая модель АРМ «Биометрическая система защиты информации». Определены структуры таблиц базы данных и их взаимосвязь.

На базе СУБД VisualFoxPro 9 реализована интерфейсная часть, включающая следующие режимы: 1) биологические характеристики, 2) параметры характеристик, 3) исходные базы данных, 4) настройка базы данных, 5) классификация, 6) идентификация.

На данный момент в качестве биологической характеристики включен «видеообраз лица». В дальнейшем планируется работать со следующими биологическими характеристиками: «термограмма лица», «отпечаток пальца», «геометрия руки», «голос» и др [24].

Для характеристики «видеообраз лица» определены ряд параметров: в частности «расстояние между зрачками глаз», «площади выпуклых или вогнутых частей лица». В качестве исходных данных для «видеообраза лица» могут быть использованы портреты в следующих графических форматах: bmp, gif, jpeg, tiff и png.

Для получения количественных значений параметров характеристик разработан алгоритм вычисления «площади выпуклых или вогнутых частей лица», основанный на построении и анализе триангуляции.

Список использованной литературы

1. Бузов Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации. – М.: Горячая линия – Телеком, 2010. -240с.
2. Болл Р.М., КоннелДж.Х., Панканти Ш., Ратха Н.К., Сеньор Э.У. Руководство по биометрии. – М.: Техносфера, 2007. – 368 с.
3. Грибунин В.Г. Комплексная система защиты информации на предприятии. – М.: Изд-во «Академия», 2009. – 416с.
4. Программно-аппаратный комплекс «Секрет» //www.okbsapr.ru
5. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. – Санкт-Петербург: НИУ ИТМО, 2012. –416 с.
6. 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.
7. Гудков В.Ю.,Боков М.В. Скоростная обработка изображения отпечатка пальца //Труды института системного анализа РАН. – 2009г. - № 45.
8. Фан НгокХоанг, СпицынВ.Г. Алгоритмы для классификации отпечатков пальца на основе применения фильтра Габора, вейвлет-преобразования и многослойной нейронной сети //Известия Томского политехнического университета. – 2012г. - № 5.
9. Maltoni D., Maio D., Jain A.K., Prabhakar S. Handbook of fingerprint recognition. -N.Y.: Springer, 2003. – 348 p.
10. Соколов А.В. Шпионские штучки. Новое и лучшее. – СПб: Изд-во «Полигон», 2000. – 256 с.
11. Технические средства и методы защиты информации /Под ред. Зайцева А.П. -М.: Изд-во «Машиностроение», 2009. – 508 с.
12. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. -М.: ИД «Форум», 20120. – 592 с.
13. Жуковский В.В., СайС.В. Способ улучшения изображения отпечатка пальца//Вестник ТОГУ. – 2009г. - № 4.
14. Javier R. Movellan (Ed) Tutorial on Gabor Filters.2008.http://mplab.ucsd.edu/tutorials/gabor.pdf (датаобращения: 20.06.2014).
15. Asker M. Bazen, Sabih H. Gerez. Systematic methods for the computation of the directional fields and singular points of fingerprint //IEEE Transactions on pattern analysis and machine intelligence. – 2002 - № 7.
16. Jie Zhou, JinweiGu, David Zhang.Topological Structure and Orientation Field//Department of Computing, the Hong Kong Polytechnic University, Kowloon, Hong Kong
17. BaseGroupLabs, технологии анализа данных. URL: http://www.basegroup.ru/, Логистическая регрессия и ROC-анализ - математический аппарат, http://www.basegroup.ru/library/analysis/regression/logistic/ (дата обращения 20.06.2014)
18. Гонсалес Р. Цифровая обработка изображений. М., 2005
19. Визильтер Ю.В., Желтов С.Ю., Князь В.А., Ходарев А.Н., Моржин А.В. Обработка и анализ цифровых изображений с примерами на LabVIEWIMAQVision. – М.: ДМК Пресс, 2007. – 464 с.
20. Клепинин В.Б., Агафонова Т.П. VisualFoxPro 9.0. Наиболее полное руководство. - СПб.: БХВ-Петербург, 2007. – 1216с.
21. Lance G.N., Williams W.T. Note on the Classification of Multilevel Data. – Comput.J., 1967, 9, P.381-382.

– Томск: Изд-во Томского университетаЮ 2996.э – 168 с.

23. Байрбекова Г.С. О тенденции и развитии современных биометрически технологий //Вестник, серия физико-математические науки, №1(49), 2015 стр. 198-202

24. Байрбекова Г.С. О необходимости подсистемы аутентификации разграничения доступа для АИС //Сборник статей по материалам XXII Международной заочной научно-практической конференции «Научная дискуссия вопросы математики, физики, химии, биологии»(№ 11 (21). - М.: Изд «Международный центр науки и образования», 2014. – стр. 35-40

25. Байрбекова Г.С., Мазаков Т.Ж. О некоторых проблемах обеспечения информационной безопасности и управления доступом //Мат.науч.конф.ИИВТ МОН РК «Современные проблемы информатики и вычислительных технологий»,Алматы 2015 стр. 34-38

26. Джомартова Ш.А. Мазаков Т.Ж., Жайдарова А.М. Система обеспечения безопасности АИС «Демография». - М.: Сборник научных трудов «Евразийское научное объединение», № 7, 2015, часть 1, с.4-7.

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ И БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В ТРАНСГРАНИЧНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Бегимбаева Е.Е.

Институт информационных и вычислительных технологий КН МОН РК, Казахстан, e-mail: enlik_89@mail.ru

Аннотация. *В статье рассматриваются проблемы правового регулирования информации в трансграничном информационном пространстве и ее безопасность. Рассмотрено понятие - социальная инженерия. Описаны методы защиты от воздействия социальной инженерий.*

Динамика развития информационных технологий в социально-экономическом государстве предъявляет повышенные требования к решению вопросов информационной безопасности. Традиционные методы правового регулирования и общественного контроля, действие норм права в пространстве и времени, а также проблема юрисдикции требуют определенной корректировки в современных условиях существования информационного пространства.

Поскольку информация представляет собой стратегический национальный ресурс, в геополитической конкуренции развитых стран мира борьба за удержание информационного превосходства занимает значимое место. С началом глобализации эффективность национальных систем обеспечения информационной безопасности оказалась решающим фактором в политике любого субъекта геополитического соперничества, а неэффективность ведет к крупномасштабным конфликтам, последствия которых могут вызвать дезорганизацию государственного управления, угрозу национальной безопасности.