УДК 681.3.069

Д.В. Александрович, А.Л. Ерохин

Харьковский национальный университет радиоэлектроники, Харьков

ИССЛЕДОВАНИЕ МОДЕЛЕЙ И МЕТОДОВ БИОМЕТРИЧЕСКОГО КОНТРОЛЯ ПОСЕЩАЕМОСТИ

В статье рассматривается классификация моделей и методов биометрического контроля посещаемости. Выполнен анализ различных методов аутентификации человека: верификация и идентификация, а также технологий аутентификации: по отпечаткам пальцев, по рисунку радужной оболочки, по лицу (2D и 3D распознавание), по венам рук, по сетчатке глаза, по геометриш рук.

Ключевые слова: *биометрия, верификация, идентификация, распознавание.*

Введение и постановка задачи

Биометрический контроль посещаемости – автоматизированный метод, с помощью которого путем проверки (исследования) уникальных физиологических особенностей или поведенческих характеристик человека осуществляется идентификация личности [1].

В отличие от пароля или персонального идентификационного номера (ПИН), биометрическая характеристика не может быть забыта, потеряна, или украдена. Поскольку биометрические характеристики каждой отдельной личности уникальны, они могут использоваться для предотвращения воровства или мошенничества. Это могут быть как уникальные признаки, полученные им с рождения, например: ДНК, отпечатки пальцев, радужная оболочка глаза; так и характеристики, приобретенные со временем или же способные меняться с возрастом или внешним воздействием, например: почерк, голос или походка.

Учитывая сказанное выше, становится актуальным исследование методов биометрического контроля посещаемости, которые позволят эффективно работать на объектах с разным количеством сотрудников и требованиями безопасности. Это позволить подобрать оптимальный тип биометрического контроля посещаемости без потерь времени.

1. Исследование и анализ методов распознавания личности

Любая аутентификация человека строится на трех традиционных принципах:

- по собственности: к собственности может относиться пропуск, пластиковая карта, ключ или общегражданские документы.

- по знаниям: к знаниям относятся пароли, коды или информация (например, девичья фамилия матери);

- по биометрическим характеристикам: эти три принципа могут использоваться как по отдельности, так и в группах. Эта методология и порождает два основных направления биометрии: верификацию и идентификацию.

Верификацией называется подтверждение личности человека через биометрический признак, где первичная аутентификация прошла по одному из первых двух методов, указанных выше. Верификация подразумевает значительно большую надежность системы. Вероятность того, что система пропустит нарушителя, не применяющего средства преодоления равна FAR используемого биометрического метода. Даже для самых слабых биометрических систем эта вероятность ничтожно мала. Основными минусами верификации являются два пункта. Первый — человеку требуется носить с собой документ или помнить пароль системы. Всегда существует проблема потери или забывания информации. Так же верификация принципиально невозможна для скрытной аутентификации.

Работу системы доступа, основанной на биометрической верификации можно представить следующим способом (рис. 1).

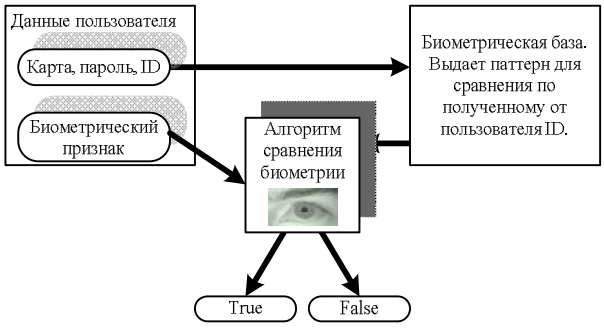

Рис. 1. Работа системы, основанной на биометрической верификации

Биометрической идентификацией называется такое использование биометрического признака, при котором не требуется дополнительной информации. Поиск объекта осуществляется по всей базе данных и не требует предварительного ключа (рис. 2). Понятно, что основным минусом этого является то, что чем больше человек в базе, тем больше вероятность ложного доступа произвольного человека.

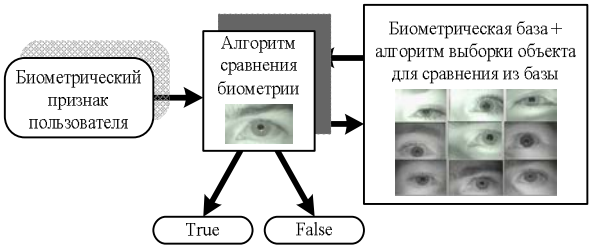

Рис. 2. Работа системы,
основанной на биометрической идентификации

Например, системы по пальцам дают возможность содержать базу не более 300 человек, по глазам не более 3000. Плюс идентификации – все ключи всегда будут с вами, не нужно ни паролей, ни карточек.

2. Исследование рабочих характеристик биометрических систем

Существуют различные характеристики, позволяющие сравнивать биометрические системы. Наиболее часто используемые для сравнения показатели эффективности биометрических систем:

коэффициент ложного отказа доступа (FRR): вероятность того, что система биометрической идентификации не признает подлинность отпечатка пальца, зарегистрированного в ней пользователя

коэффициент ложного пропуска (FAR): вероятность того, что система биометрической идентификации по ошибке признает подлинность отпечатка пальца пользователя, не зарегистрированного в системе

В качестве двух основных характеристик любой биометрической системы можно принять ошибки первого и второго рода. В теории радиолокации их обычно называют «ложная тревога» или «пропуск цели», а в биометрии наиболее устоявшиеся понятия — FAR (False Acceptance Rate) и FRR(False Rejection Rate). Первое число характеризует вероятность ложного совпадения биометрических характеристик двух людей. Второе – вероятность отказа доступа человеку, имеющего допуск. Система тем лучше, чем меньше значение FRR при одинаковых значениях FAR. Иногда используется, и сравнительная характеристика EER, определяющая точку в которой графики FRR и FAR пересекаются. Но она далеко не всегда репрезентативна.

Можно отметить следующее: если в характеристиках системы не даны FAR и FRR по открытым биометрическим базам — то что бы производители не заявляли о ее характеристиках, эта система скорее всего недееспособна или сильно слабее конкурентов.

Но не только FAR и FRR определяют качество биометрической системы. Если бы это было только так, то лидирующей технологией было бы распознавание людей по ДНК, для которой FAR и FRR стремятся к нулю. Очевидно, что эта технология неприменима на сегодняшнем этапе развития человечества. Было выработано несколько эмпирических характеристик, позволяющих оценить качество системы. Устойчивость к подделке – это эмпирическая характеристика, обобщающая то, насколько легко обмануть биометрический идентификатор. Устойчивость к окружающей среде – характеристика, эмпирически оценивающая устойчивость работы системы при различных внешних условиях, таких как изменение освещения или температуры помещения. Простота использования показывает насколько сложно воспользоваться биометрическим сканером, возможна ли идентификация «на ходу». Важной характеристикой является «Скорость работы», и «Стоимость системы». Не стоит забывать и то, что биометрическая характеристика человека может изменяться со временем, так что если она неустойчива – это существенный минус.

Основными методами, использующими статические биометрические характеристики человека, являются идентификация по папиллярному рисунку на пальцах, радужной оболочке, геометрии лица, сетчатке глаза, рисунку вен руки, геометрии рук. Также существует семейство методов, использующих динамические характеристики: идентификация по голосу, динамике рукописного подчерка, сердечному ритму, походке. На рис. 3 представлено распределение биометрического рынка пару лет назад.

В каждом втором источнике эти данные колеблются на 15-20 процентов, так что это всего лишь оценочное представление. Под понятием «геометрия руки» скрываются два разных метода.

В данной статье рассмотрены статические характеристики. Из динамических характеристик на сегодняшний момент только распознавание по голосу имеет хоть какую-то статистическую значимость (сравнимую с худшими статическими алгоритмами FAR~0.1%, FRR~6%), но лишь в идеальных условиях.

Чтобы ощутить вероятности FAR и FRR, можно оценить, как часто будут возникать ложные совпадения, если установить систему идентификации на проходной организации с численностью персонала N человек. Вероятность ложного совпадения полученного сканером отпечатка пальца для базы данных из N отпечатков равна FAR·N.

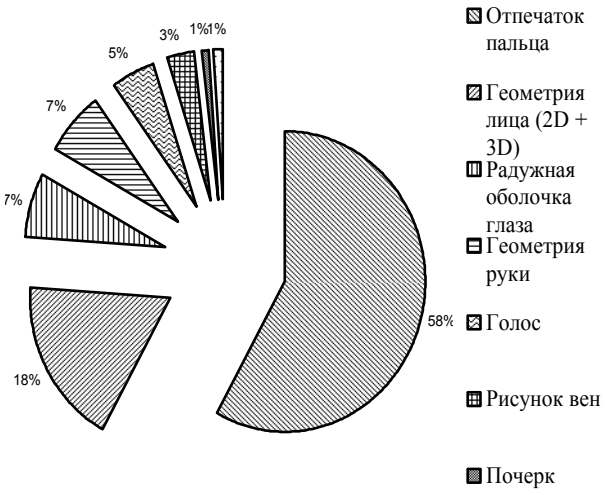

Рис. 3. Распределение биометрического рынка.

И каждый день через пункт контроля доступа проходит тоже порядка N человек. Тогда вероятность ошибки за рабочий день FAR·(N·N). В зависимости от целей, системы идентификации вероятность ошибки за единицу времени может сильно варьироваться, но если принять допустимым одну ошибку в течение рабочего дня, то:

$$\mathrm{FAR} \times \mathrm{N}^2 \approx 1, \Rightarrow \mathrm{N} \approx \sqrt{\frac{1}{\mathrm{FAR}}} \qquad (1)$$

Тогда получим, что стабильная работа системы идентификации при FAR=0.1% =0.001 возможна при численности персонала N≈30.

Самыми статистически надежными и устойчивыми к подделке системами доступа являются системы допуска по радужной оболочке и по венам рук. Системы биометрической идентификации можно комбинировать, достигая астрономических точностей. Самыми дешевыми и простыми в использовании, но обладающими хорошей статистикой, являются системы допуска по пальцам. Допуск по 2D лицу удобен и дешев, но имеет ограниченную область применений из-за плохих статистических показателей. Для радужной оболочки можно увеличить точность системы практически квадратично, без потерь для времени, если усложнить систему, сделав ее на два глаза. Для дактилоскопического метода — путем комбинирования нескольких пальцев, и распознаванию по венам, путем комбинирования двух рук, но такое улучшение возможно только при увеличении времени, затрачиваемого при работе с человеком.

Рассмотрим характеристики каждой из систем (табл. 1). Расставим оценки в каждой графе. Чем ближе оценка к 10, тем лучше система в этом отношении. Также рассмотрим соотношение FAR и FRR для этих систем. Это соотношение определяет эффективность системы и широту ее использования (табл. 2).

Таблица 1

Характеристики систем, работающих по разным биометрическим технологиям

Биометрическая технология	Устойчивость к подделке	Устойчивость к окружающей среде	Простота использования	Стоимость	Скорость	Стабильность признака во времени
Радужная оболочка	10	9	8	7	10	10
Дактилоскопия	6	10	9	10	10	9
Лицо: 2D 3D	 4 9	 6 8	 6 10	 10 5	 10 7	 8 10
Вены руки	10	7	9	7	8	7
Сетчатка	10	10	6	3	6	9

Таблица 2

Соотношение рабочих характеристик биометрических систем

Биометрическая технология	FAR = 0,1%	FAR = 0,01%	FAR = 0,001%	FAR = 0,0001%	FAR = 0,00001%
Радужная оболочка (FRR)	0,07%	0,07%	0,12%	0,15%	0,16%
Дактилоскопия (FRR)	0,3%	0,4%	0,6%	0,9%	-
Лицо(FRR): 2D 3D	2,5%	5% ~0,1%	6%	9%	-

Обобщив результаты для методов, можно сказать, что для средних и больших объектов, а также для объектов с максимальным требованием в безопасности следует использовать радужную оболочку в качестве биометрического доступа и, возможно, распознавание по венам рук. Для объектов с количеством персонала до нескольких сотен человек оптимальным будет доступ по отпечаткам пальцев. Системы распознавания по 2D изображению лица весьма специфические. Они могут потребоваться в случаях, когда распознавание требует отсутствия физического контакта, но поставить систему контроля по радужной оболочке невозможно. Например, при необходимости идентификации человека без его участия, скрытой камерой, или камерой наружного обнаружения, но возможно это лишь при малом количестве субъектов в базе и небольшом потоке людей, снимаемых камерой.

Остановимся подробнее на внутренних аспектах работы современных биометрических систем распознавания по отпечаткам пальцев, на том, с чего

начинается их работа и что является ядром любой такой системы. Рассмотрим методы получения отпечатка пальца в электронном виде и методы сравнения отпечатков пальцев.

Получение электронного представления отпечатков пальцев с хорошо различимым папиллярным узором — достаточно сложная задача. Поскольку отпечаток пальца слишком мал, для получения его качественного изображения приходится использовать достаточно изощренные методы.

В автоматизированных системах используют всего два типа деталей узора папиллярных линий для идентификации (особых точек):

- конечные точки – точки, в которых «отчетливо» заканчиваются папиллярные линии;

- точки ветвления – определяются как точки, в которых папиллярные линии раздваиваются.

Алгоритм верификации состоит из 4-х шагов.

Первый – обработка входного изображения. Изображение, получаемое со сканера, изначально непригодно для выделения особых точек, поэтому его необходимо преобразовать к удобному нам виду. Для этого его нужно бинаризировать, затем привести бинарное изображение к его скелету, в котором толщина всех линий – 1 пиксель, т.е. стянуть линии в центр, не делая при этом разрывов.

Второй – поиск ключевых точек. В нашем случае это конечные точки, ветвления и ядро, поэтому: находим центральную точку отпечатка пальца, т.е. точку наибольшей кривизны папиллярного узора; принимаем центральную точку за начало координат; определяем радиус относительно начала координат, в котором будем искать особые точки, что необходимо для уменьшения или расширения зоны поиска особых точек в зависимости от необходимой точности распознания; находим ветвления и конечные точки в заданном радиусе и вычисляем их координаты.

Третий – получение математического представления отпечатка. Чтобы система могла просто оперировать с образами отпечатков, необходимо создать математическое представление образа. В частности, достаточно удобно работать с матрицами. Принимая найденные точки за вершины графа, можно построить полный, ненаправленный взвешенный граф.

Четвертый – сравнение полученного представления с шаблоном из базы. В силу простоты реализации математического представления отпечатка пальца операция сравнения образов сводится к сравнению матриц одинаковых размерностей, что в свою очередь не требует больших вычислительных ресурсов и увеличивает быстродействие системы в целом.

3. Алгоритм верификации изображения отпечатка пальца

Алгоритм верификации отпечатка пальца состоит из следующих этапов:

- бинаризация полученного изображения;
- скелетизация изображения;
- выделение точек;
- сравнение точек.

Скелетизация широко используется во многих задачах обработки изображений, например, распознавание символов, обработка картографических изображений и технических чертежей.

Особенность скелетов объектов состоит в том, что они сохраняют информацию о топологической структуре объекта и сокращают объем памяти, необходимой для их хранения.

Существуют разнообразные методы получения скелета символа, отличные друг от друга:

1. Метод Щепина.
2. Скелетизация с применением шаблонов.
3. Волновой метод
4. Скелетизация по алгоритму Зонга-Суня.

В результате исследования был выбран шаблонный метод, который требует всего один обход изображения. Для снижения уровня неточностей используется часть шаблонов из второго набора.

Шаблоны соответствуют матрице 3*3, где центральный элемент является текущим пикселем в обходе изображения. На рис. 4 представлены два набора шаблонов. Серым цветом на них обозначены пиксели, цвет которых не имеет значения.

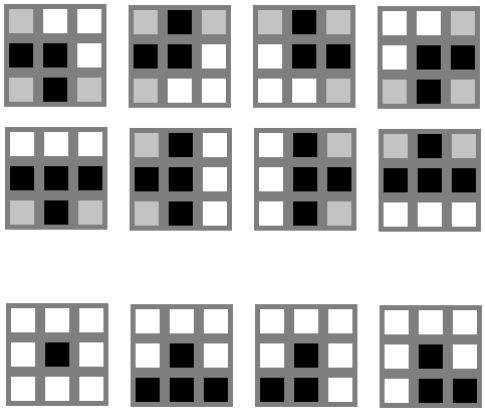

Рис. 4. Шаблоны для скелетизации.

Восемь первых шаблонов, являются основной частью. Четыре снизу для устранения «шума», причем эти четыре так же могут быть повернуты на 90, 180 и 270 градусов, и ищутся вторым обходом изображения.

Если алгоритм наталкивается на шаблон, то центральный пиксель окрашивается в белый цвет (не принадлежит скелету). Обход продолжается, пока остаются возможности удаления.

В настоящее время выделяют три класса алгоритмов сравнения отпечатков пальцев:

- корелляционное сравнение;
- сравнение по ключевым точкам;
- сравнение по узору.

Сравнение по особым точкам – это наиболее целесообразный подход к распознанию отпечатка пальца, поскольку он довольно прост в реализации и показывает достаточно высокое быстродействие и точность, потому именно этот алгоритм я выбрала для реализации.

4. Описание разработанной системы

На вход алгоритма подается изображение отпечатка пальца, полученное со сканера. Его размеры в среднем составляют 300x434 пикселя. В первую очередь необходимо отфильтровать изображение и привести его к бинарному виду.

Далее изображение отпечатка пальца подвергается скелетизации. Работа процедуры заключается в последовательном симметричном удалении граничных точек объектов до тех пор, пока не будут получены линии толщиной в один элемент, которые и называются скелетами исходных объектов.

Всего для выделения «скелета» требуется не более L/2 циклов, где L – максимальная толщина линии в преобразуемом объекте.

Ключевым моментом алгоритма скелетизации является быстрый поиск на изображениях элементов объектов, окрестность которых совпадает с одним из заданных структурных шаблонов.

В полученном описании скелета производится огрубляющая предобработка, состоящая в удалении коротких линий и объединении близких триад.

После подготовки изображения переходим к поиску ключевых точек. Принимая найденные точки за вершины графа, можно построить полный, ненаправленный взвешенный граф, который представим в виде матрицы. Алгоритм обработки изображения отпечатка пальца представлен на рис. 5.

Сравнение полученного представления с шаблоном из базы сводится к сравнению матриц одинаковых размерностей. На рис. 6 представлен алгоритм верификации отпечатка пальца.

Преимущества предлагаемого алгоритма позволяют: классифицировать отпечаток пальца не по одному, а по двум признакам (размерность матрицы и вес графа), повышая ее точность; варьировать количество классов по каждому признаку и задавать диапазон изменения величин внутри класса; контролировать распределение отпечатков пальцев по классам, добиваясь их равномерного распределения; увеличивать скорость сравнения, поскольку сравниваются матрицы; повышать точность сравнения за счет увеличения области поиска особых точек.

В качестве языка программирования для реализации программного модуля был выбран Python. Помимо самого Python, также использовалась PIL (Python Imaging Library), для разбора картинки на пиксели. Приведем программную реализацию функции бинаризции:

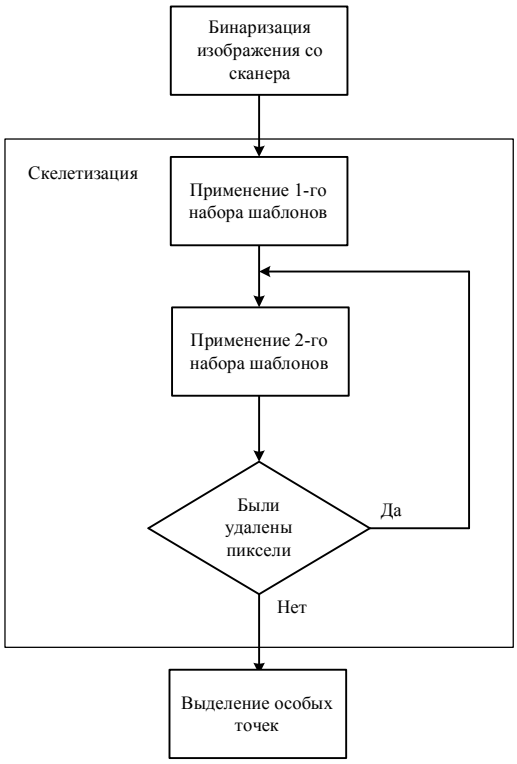

Рис. 5. Алгоритм обработки изображения отпечатка пальца

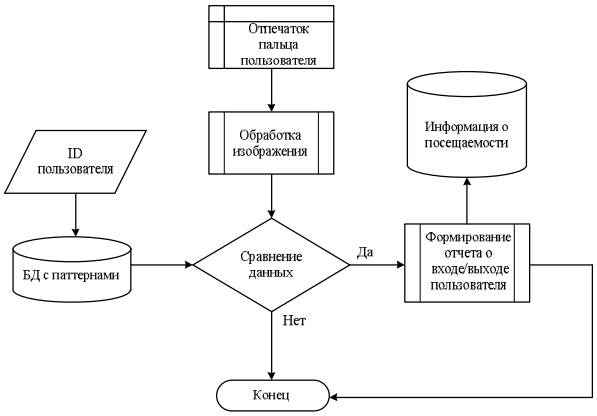

Рис. 6. Алгоритм верификации отпечатка пальца

```
def binary(img):
    bImg=[ ]
    for i in range(img.size[0]):
        tmp=[ ]
        for j in range(img.size[1]):
            t=img.getpixel((i,j))
            p=t[0]*0.3+t[1]*0.59+t[2]*0.11
            if p>128:
                p=1
            else:
                p=0
            tmp.append(p)
        bImg.append(tmp)
    return bImg
```

Приведем программную реализацию выделения особых точек. Если в окрестности из восьми точек, есть только одна черная, то это конечная точка. Если же их две, то это просто точка линии, три — точка ветвления:

```
#подсчет количества черных в окрестности
def checkThisPoint(img, x, y):     c=0
   for i in range(x-1,x+2):
      for j in range(y-1,y+2):
         if img[i][j]==0:
            c+=1
   return c-1
#формирова-
ние списков точек ветвления и конечных
def findCheckPoint(img):
   x=len(img)
   y=len(img[0])
   branchPoint=[ ]
   endPoint=[ ]
   for i in range(x):
      for j in range(y):
         if img[i][j]==0:
            t=checkThisPoint(img, i, j)
            if t==1:
               endPoint.append((i,j))
            if t==3:
               branchPoint.append((i,j))
   return (branchPoint, endPoint)
```

Приведем программную реализацию сравнения точек. Простой поиск точки, которая попадает в окрестность 30*30 и является точкой того же типа.

```
#вход: кортеж точек эталона и кортеж проверяемого;
#выход (совпало, всего)
def matchingPoint(r, v):
   all=0
   match=0
   for i in v[0]:
      x=range(i[0]-15,i[0]+15)
      y=range(i[1]-15,i[1]+15)
      all+=1
      for j in r[0]:
         if j[0] in x and j[1] in y:
            match+=1
            break
   for i in v[1]:
      x=range(i[0]-15,i[0]+15)
      y=range(i[1]-15,i[1]+15)
      all+=1
      for j in r[1]:
         if j[0] in x and j[1] in y:
            match+=1
            break
    return (match,all)
```

Выводы

На основе обзора и анализа современных алгоритмов распознания отпечатка пальца было разработано формальное описание быстрого и надежного алгоритма распознания, на выходе которого формируется матрица с суммой элементов, равной весу графа, и размерностью, равной количеству вершин графа.

Преимущества алгоритма позволяют: классифицировать отпечаток пальца не по одному, а по двум признакам (размерность матрицы и вес графа), повышая ее точность; варьировать количество классов по каждому признаку и задавать диапазон изменения величин внутри класса; контролировать распределение отпечатков пальцев по классам, добиваясь их равномерного распределения; увеличивать скорость сравнения, поскольку сравниваются матрицы; повышать точность сравнения за счет увеличения области поиска особых точек.

В данной реализации акцент делался на простоте и наглядности кода. Возможно, дополнить ее несколькими проверками, например, смотреть углы вхождения линий в особые точки. При проверке откидывать пары уже найденных, для тех случаев, когда в окрестность попадает много точек одного типа.

Список литературы

1. Last updated: Biometrics Overview May 19, 2014 В. Задорожный http://www.nist.gov/itl/biometrics/index.cfm.

2. Задорожный В. Обзор биометрических технологий [Электронный ресурс] / В. Задорожный. – Режим доступа:. http://www.bre.ru/security/20234.html.

3. The Biometric Consortium [Электронный ресурс]. – Режим доступа:http://www.biometrics.org.

4. Common Biometric Exchange File Format (CBEFF), January 2001, USA National Institute of Standards and Technology (NIST). [Электронный ресурс]. – Режим доступа:http://www.nist.gov.

5. Fingerprints & Other Biometrics [Электронный ресурс]. – Режим доступа: http://www.fbi.gov/about-us/cjis/fingerprints_biometrics.

Поступила в редколлегию 23.06.2014

Рецензент: д-р техн. наук, проф. И.П. Захаров, Харьковский национальный университет радиоэлектроники, Харьков.

ДОСЛІДЖЕННЯ МОДЕЛЕЙ І МЕТОДІВ БІОМЕТРИЧНОГО КОНТРОЛЮ ВІДВІДУВАНОСТІ

Д.В. Александрович, А.Л. Єрохін

У статті розглядається класифікація моделей і методів біометричного контролю відвідуваності. Виконано- аналіз різних методів аутентифікації людини: верифікація і ідентифікація, а також технологій аутентифікації: за відбитками пальців, по малюнку веселкової оболонки, по обличчю (2D і 3D розпізнавання), по венах рук, по сітківці ока, з геометрії рук.

Ключові слова: *біометрія, верифікація, ідентифікація, розпізнавання.*

RESEARCH MODELS AND METHODS OF BIOMETRIC CONTROL TRAFFIC

D.V. Aleksandrovych, A.L. Yerokhin

Different authentication methods of a person are analyzed: verification and identification and authentication technologies: by fingerprints, by the pattern of the iris, by a face (2D and 3D recognition), by the veins of hands, by the retina, by the geometry of hands. The advantages and disadvantages of each technology are listed in the article. In conclusion comparative characteristics of biometric systems of monitoring attendance, working on different technologies and recommendations for the selection of technologies for enterprises with different number of employees and safety requirements are presented.

Keywords: *biometrics, verification, identification, recognition.*