УДК 004.93

ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ ПО ДВУМЕРНЫМ ОПТИЧЕСКИМ ОБРАЗАМ ОТПЕЧАТКОВ ПАЛЬЦЕВ

© 2010 Д.И. Трифонов

Самарский государственный университет

Поступила в редакцию 11.01.2010

В статье описывается метод идентификации личности по двумерным оптическим образам отпечатков пальцев человека, основанный на их обработке с помощью аппарата фрактальной геометрии.
Ключевые слова: биометрия, отпечаток пальца, фрактал, идентификация.

1. ВВЕДЕНИЕ

В настоящее время биометрические методы идентификации личности становятся все более и более актуальной технологией распознавания личности. Преимущество биометрических систем идентификации, по сравнению с традиционными подходами, заключается в том, что идентифицируется не внешний предмет, принадлежащий человеку, а сам человек.

Наибольшее распространение получили технологии идентификации личности по отпечаткам пальцев, в основе которого лежит уникальность для каждого человека рисунка папиллярных узоров [1].

В настоящее время существует несколько алгоритмов идентификации личности по отпечаткам пальцев. В данной работе предложен новый метод идентификации личности по фрактальной размерности двумерных образов отпечатков пальцев. Его суть заключается в том, что изображение отпечатка пальца, полученного оптическими методами, представляется в виде фрактального множества, для которого вычисляется его числовая характеристика – фрактальная размерность. Этот параметр и будет являться той уникальной характеристикой, по которой будет происходить сравнение.

Возможность применения теории фракталов для биометрической идентификации личности – то нововведение, которое предложено, опробовано в работе и описано в данной статье.

2. ТЕОРИЯ

В основе метода распознавания личности лежит компьютерный алгоритм вычисления размерности Минковского для изображений, полученных оптическим путем. Алгоритм опирается на следующее соотношение аппарата фрактальной геометрии:

$$\log N(\xi) = \log c - d \log \xi, \qquad (1)$$

где $N(\xi)$ – минимальное число шаров радиуса ξ, необходимых для покрытия компактного множества A,

d - любое неотрицательное вещественное число.

Как легко заметить, зависимость $\log N(\xi)$ от $\log \xi$ – прямая с угловым коэффициентом d. Для определения неизвестных параметров c и d необходимо оценить N(x) [2].

Процедура вычисления фрактальной размерности d двумерного образа отпечатка происходит следующим образом:

Вход: S (бинарная квадратная матрица фрактала), p (размер S)

Выход: d (оценка размерности Минковского)

Инициализация:

Lmax = наибольшее целое < p/10 (максимальный размер клетки)

Шаги:

For L = 1 to Lmax

N(L) = 0

B = наибольшее целое ≤ p/L

for i = 1 to B

for j = 1to B

$$\text{cnt} = \sum_{k=(i-1)L+1}^{iL} \left(\sum_{h=(j-1)L+1}^{jL} S(k,h) \right) //$$

число точек в клетке

if cnt >0, N(L) =N(L)+1, end if

end for

for L to Lmax

$$\xi_L = \log(L)$$

$$\eta_L = \log(N(L))$$

end for

Найти МНК-прямую по точкам (ξ_L, η_L), L = 1, ..., Lmax

размерность d = модуль углового коэффициента МНК-прямой [3].

Трифонов Денис Иванович, аспирант кафедры безопасности информационных систем.
E-mail: denstarrr@gmail.com

Данный алгоритм оценки фрактальной размерности будет применен для нахождения дробной размерности изображения отпечатка пальца, а полученный результат для распознавания личности.

3. ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА

Практическая реализация алгоритма распознавания личности заключалась в создании специальной биометрической системы, все фазы работы которой можно представить в виде следующей блок-схемы:

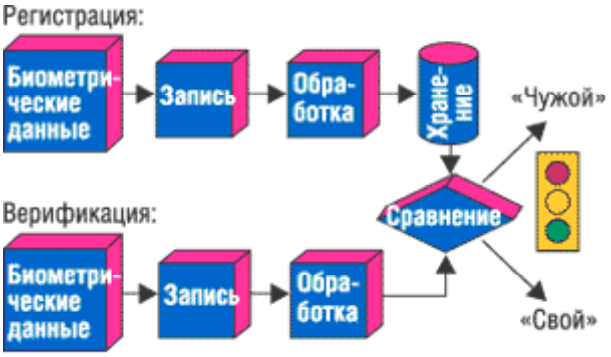

Рис. 1. Блок-схема биометрической системы

Модель процесса идентификации, реализованная в данной работе, также включает в себя все стадии, указанные на блок-схеме.

Регистрация пользователей. Процесс регистрации подразумевает под собой следующее: пользователь фиксирует значение какого-либо параметра отпечатка пальца в специальной базе данных, в которой будут храниться значения характеристик всех других пользователей. Зафиксированное значение биохарактеристики называется эталоном или шаблонным значением.

В данной работе исходными данными являются двумерные плоские изображения отпечатков пальцев человека. Их получение осуществлялось с помощью оптического сканера Futronic FS - 80. Данный этап является одним из самых важных в работе, т.к. качество полученных отпечатков пальцев напрямую влияет на точность дальнейшей идентификации личности.

Для получения исходных данных использовались FTIR-сканеры [FTIR, Frustrated Total Internal Reflection] – оптические контактные сканеры, основанные на измерении различий в полном внутреннем отражении подсвечиваемых внешним источником участков кожи на границе соприкосновения пальца с поверхностью предметного стекла сканера (чаще всего призмы). Считывание получившегося изображения производится ПЗС или КМОП фотоприемными устройствами [4].

Используемый в работе сканер представляет собой модуль для захвата и передачи на ПК образа отпечатка пальца. Уникальная технология, использующая прецизионную CMOS матрицу, позволяет получать изображения отпечатка пальца с высоким качеством. Сканер FS-80 может применяться в любых приложениях, где требуется эффективная и достоверная идентификация человека.

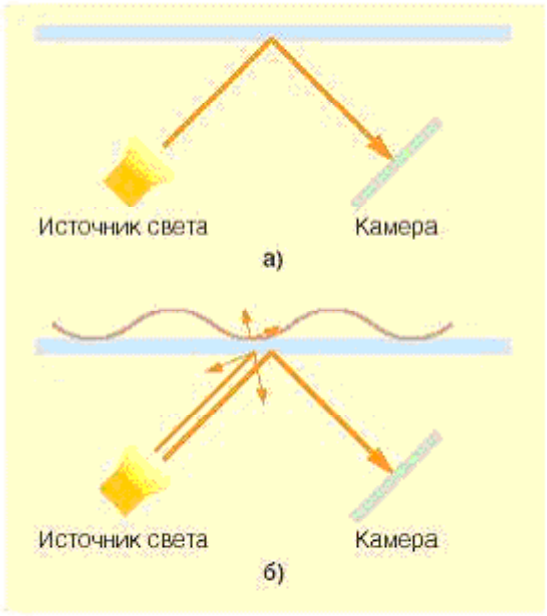

Рис. 2. Принцип действия FTIR- сканеров

В сканер FS-80 встроена специальная электронная схема, LFD (Live Finger Detection), позволяющая отличить живой палец от муляжа [5].

Рис. 3. Оптический сканер Futronic FS-80

Для получения значения эталона, по которому будет происходить идентификация, снимается несколько изображений отпечатка пальца. Для каждого из вычисляется значение фрактальной размерности образа отпечатка пальца и по формуле (2) находится их среднее арифметическое:

$$Dcp=(D1+D2+...+Dn)/n, \quad (2)$$

где Dcp – среднее значение фрактальной размерности;

D1..Dn - значения размерности 1-го...n-го ОП;

n - общее число ОП.

При этом следует отметить, чем больше вариантов одного и того же пальца сделано, тем точнее будет среднее арифметическое. Полученный результат и есть эталон, и все дальнейшие сравнения будут происходить с ним.

Следует учитывать, что получить абсолютно одинаковое значение одного и того же отпечатка пальца практически невозможно. Это объясняется тем, что состояние поверхности пальца может меняться под действием внешних факторов: грязь, царапины, порезы, смещения и растяжения кожи, различная сила нажатия, сухость и влажность кожи.

Исходя из этого было введено понятие среднего отклонения ΔDcp - диапазон значений, в пределах которого значения отпечатков пальцев могут отличаться от эталона. Параметр ΔDcp определяется по формуле (3):

$$\Delta Dcp=(|D1-Dcp|+|D2-Dcp|+...+|Dn-Dcp|)/n, \quad (3)$$

где ΔDcp – отклонение от среднего значения.

В табл. 1 параметры Dcp и ΔDcp отражены более детально.

Следующим этапом распознавания личности является аутентификация и верификация пользователей Аутентификация - это процесс, в рамках которого выполняется проверка личности пользователя и устанавливается, что пользователь именно тот человек, за которого себя выдает [6].

В разрабатываемой системе аутентификация происходит следующим образом. Зарегистрированный ранее пользователь указывает логин - запись в базе данных, соответствующая конкретному пользователю. После этого он должен предъявить нечто, что может подтвердить подлинность субъекта. В данном случае в качестве такого “паспорта” выступает отпечаток пальца.

Сканированное изображение отпечатка обрабатывается и по алгоритму Минковского для него вычисляется значение фрактальной размерности. Полученный результат сравнивается со значением, которое хранится в базе данных и соответствует зарегистрированному шаблону того пользователя, в качестве которого субъект себя заявляет. Описанная процедура реализована в специальной программе по распознаванию личности. Ее интерфейс представлен на рис. 4.

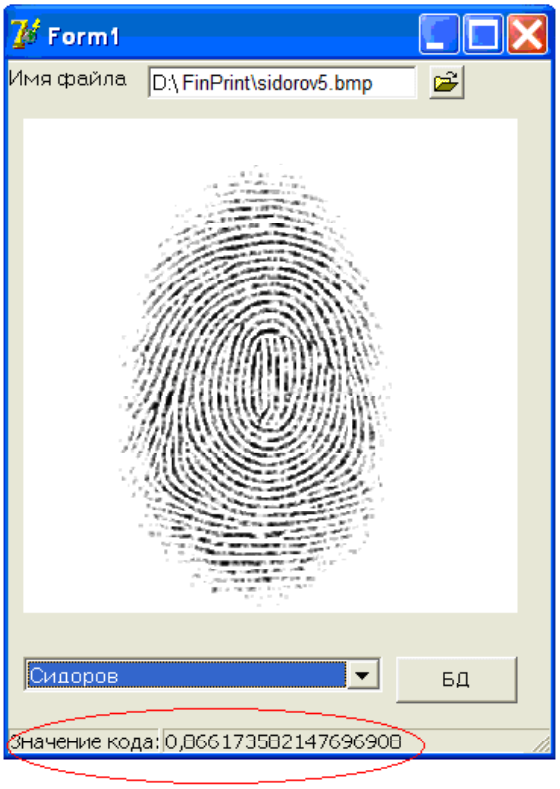

Рис. 4. Интерфейс программы

В разрабатываемой системе доступа рассматривается два варианта развития событий. Если полученное значение фрактальной размерности

Таблица 1. Результаты значений размерности отпечатков пальцев

Варианты отпечатка пальца					
Значение фрактальной размерности	1,5564	1,5529	1,5567	1,5574	1,5569
Среднее значение размерности $D_Ф$	1,5561				
Среднее отклонение $\Delta D_Ф$	0,0062				

схоже со значением эталона в пределах допустимых значений, то система воспринимает пользователя как "своего". Аутентификация проходит успешно, пользователь получает доступ к системе в соответствии с назначенными ему правами. Если же разница между полученным значением размерности и эталонным значением превышает установленное допустимое отклонение, то система распознает субъект как "чужого". Соответственно пользователю будет отказано в доступе к системе.

Возможность обоих вариантов зависит от строгости политики безопасности. Если администратор установит слишком строгие правила политики безопасности, а именно низкий уровень допустимого отклонения Δ Dcp, то отказ в доступе может получить как злоумышленник, так и легальный пользователь. Следовательно, возникнет ошибка первого рода FRR (False Reject rate) – "ложный отказ", "недопустить своего". Напротив, если установить слишком большое значение Δ Dcp , то злоумышленник, у которого схожи отпечатки пальцев с отпечатками легального пользователя, может получить доступ, т.е возникнет ошибка второго рода FAR (False Acceptance Rate) – что означает "ложный допуск", "пропустить чужого".

Дальнейшая реализация системы заключалась в ряде испытаний на базе реальных отпечатках пальцев людей. Согласно проведенному исследованию, для разрабатываемой системы эти параметры составили:

FAR – 0,001 %

FRR – 0,0001 %

Данные показатели означают, что возможность допуска чужого составляет 1 случай из тысячи, возможность не допустить своего - 1 из 10 тысяч.

Сопоставив полученные результаты, можно сделать вывод, что разрабатываемая система идентификации личности по двумерным образам отпечатков пальцев может выступать в качестве реальной биометрической системы контроля доступа, удовлетворяющей всем требованиям безопасности. Следует отметить – лежащий в основе метод обработки оптических изображений, базирующийся на математическом для распознавания личности по отпечаткам пальцев, но и по другим изображениям биометрических характеристик человека - рисунка вен кисти руки, сетчатка глаза, геометрии формы лица.

Особую благодарность за помощь и содействие в подготовке работы хотелось бы выразить научному руководителю – доктору физико-математических наук, профессору СамГУ Горохову Александру Викторовичу.

СПИСОК ЛИТЕРАТУРЫ

1. *Венедов М.А.* Политика России в области биометрии. Статьи, репортажи, интервью. URL: http://www.biometrics.ru (дата обращения 11.02.2009).
2. *Морозов А.В.* Введение в теорию фракталов. М.: Парус, 1996. С. 24-29.
3. *Кроновер Р.М.* Фракталы и хаос в динамических системах. Основы теории. М.: Постмаркет, 2000. С. 127-137.
4. Основные типы сканеров отпечатков пальцев и принципы их работы . URL: http://www.biolink.ru (дата обращения 4.02.2009)
5. Futronic в ногу с временем - технология "Live finger detection". URL: http://www.biometricacs.com (дата обращения 4.02.2009)
6. *Шелупанов А.А., Зайцев А.П., Мещеряков Р.В.* Основы защиты информации. Томск: В-Спектр, 2009. С. 67 - 72.
7. Руководство по биометрии / *Р. М. Болл, Дж. Х. Коннел, Ш. Панканти, Н. К. Ратха, Э. У. Сеньор*. М.: Техносфера, 2007.

PERSON IDENTIFICATION BY TWO-DIMENSION FINGERPRINT OPTICAL IMAGES

© 2010 D.I. Trifonov

Samara State University

In this article we described person identification method by two-dimension human fingerprint optical images, based on their treatment by means of mathematical fractal geometry.

Key words: biometry, fingerprint, fractal, identification.

Denis Trifonov, Graduate Student of information system security department. E-mail: denstarrr@gmail.com