

УДК 004.93

Д.И. Трифонов

Идентификация личности по фрактальной размерности отпечатков пальцев и системы контроля и управления доступом

Представленная статья посвящена новому методу распознавания личности, основанному на определении уникального идентификатора – фрактальной размерности отпечатков пальцев человека. Предложенный метод может быть использован в качестве основы для построения биометрических систем контроля и управления доступом (СКУД). Дано описание метода, его теоретическое обоснование, рассмотрен алгоритм его работы, преимущества и недостатки.

Ключевые слова: биометрия, отпечаток пальца, фрактал, фрактальная размерность, идентификация и аутентификация личности, СКУД.

В настоящее время биометрические методы идентификации личности становятся все более и более актуальной технологией. Их растущая популярность обусловлена рядом преимуществ по сравнению с обычными способами идентификации. Преимущество биометрических систем идентификации, по сравнению с традиционными подходами, заключается в том, что идентифицируется не внешний предмет, принадлежащий человеку, а собственно сам человек. Обобщенно технологии распознавания личности, основанные на особенностях физиологии и анатомии человека, его поведения и привычек называются биометрическими [1].

В настоящее время наибольшее распространение получили устройства и методы идентификации личности по отпечатку пальца. В их основе лежит уникальность рисунка папиллярных узоров пальцев каждого человека. На данный момент существует несколько алгоритмов идентификации личности по отпечаткам пальцев. Как правило, их принцип основывается на сравнении отпечатков по их уникальным элементам – точкам ветвления и слияния папиллярных линий, ширине гребней и впадин и т.д. (рис. 1). Все они обладают определенными преимуществами и определенными недостатками.

Метод идентификации личности, описываемый в данной работе, качественно отличается от существующих. Его особенность заключается в новой интерпретации теории фракталов и хаоса – использовании математического аппарата данных разделов науки в технологиях защиты информации. Нововведение заключается в создании эффективного алгоритма распознавания личности, основанного на вычислении новой характеристики – размерности фрактального множества, в качестве которого выступает реальный отпечаток пальца человека.

Рассмотрим описание алгоритма более подробно. Компьютерные алгоритмы вычисления размерности Минковского обычно опираются на соотношение:

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

где $N(\xi)$ – минимальное число шаров радиуса ξ , необходимых для покрытия компактного множества A ; d – любое неотрицательное вещественное число; c – любое положительное натуральное число.

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



Рис. 1. Основные типы контрольных точек отпечатка пальца

Компьютерный алгоритм оценки фрактальной размерности представлен ниже:

Назначение: проводит оценку размерности плоского фрактала.

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

Выход: d (оценка размерности Минковского).

Инициализация:

L_{\max} = наибольшее целое $< p/10$ (максимальный размер клетки).

Шаги:

```

For  $L = 1$  to  $L_{\max}$ 
     $N(L) = 0$ 
     $B =$  наибольшее целое  $\leq p/L$ 
    for  $i = 1$  to  $B$ 
        for  $j = 1$  to  $B$ 
             $cmt = \sum_{k=(i-1)L+1}^{iL} \left( \sum_{h=(j-1)L+1}^{jL} S(k, h) \right)$  // число точек в клетке
            if  $cmt > 0$ ,  $N(L) = N(L) + 1$ , end if
        end for
    end for
end for
for  $L$  to  $L_{\max}$ 
     $\xi_L = \log(L)$ 
     $\eta_L = \log(N(L))$ 
end for

```

Найти МНК-прямую по точкам (ξ_L, η_L) , $L = 1, \dots, L_{\max}$, размерность d = модуль углового коэффициента МНК-прямой [3].

Данный алгоритм показывает, что численная оценка размерности Минковского может применяться для распознавания образов и вполне приемлема для того, чтобы отличать отпечатки пальцев одного типа от отпечатков другого типа. Таким образом, данный алгоритм оценки фрактальной размерности будет применен для нахождения дробной размерности изображения отпечатка пальца, а полученный результат – для распознавания личности.

Программная реализация алгоритма идентификации личности заключалась в создании такой системы, которая могла бы соответствовать и удовлетворять всем требованиям реальной системы контроля и управления доступом (СКУД), т.е. она должна включать в себя все процедуры и операции, которые осуществляет СКУД при распознавании личности. Логически все фазы процесса идентификации можно представить в виде следующей блок-схемы, изображенной на рис. 2.

Регистрация:

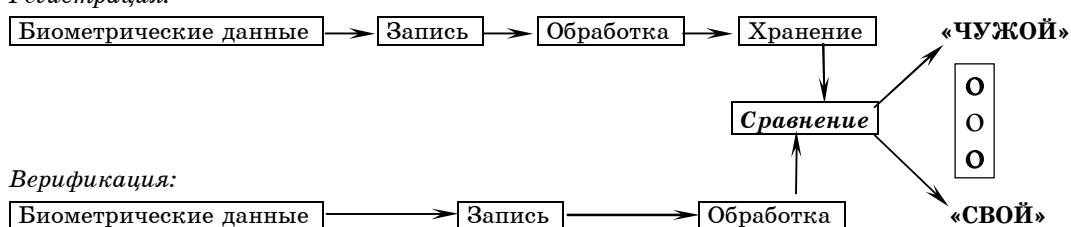


Рис. 2. Блок-схема биометрической системы

Модель процесса идентификации, реализованная в данной работе, также включает в себя все стадии, указанные на блок-схеме. Более подробное описание каждого этапа представлено далее.

Регистрация пользователей. Для того чтобы система могла идентифицировать пользователя, его необходимо зарегистрировать, т.е. указать какой-либо идентификатор, с которым будет ассоциироваться только этот пользователь и никто другой. Процесс регистрации подразумевает под собой следующее: пользователь фиксирует значение какой-либо своей биометрической характеристики (в нашем случае отпечатка пальца) в специальной базе данных. Зафиксированное значение характеристики называется эталоном, или шаблонным значением.

На данном этапе работы было проведено тестирование на искусственных отпечатках пальцев, сгенерированных программой *SFinGe 2.0* [4]. Отпечатки пальцев, созданные ею, практически не отличаются от натуральных отпечатков пальцев.

Для получения эталона делается несколько снимков отпечатка пальца, по которому будет происходить идентификация. Затем вычисляется значение каждого снимка отпечатка пальца (ОП) и по формуле (2) находится их среднее арифметическое:

$$D_{\text{ср}} = (D_1 + D_2 + \dots + D_n)/n, \quad (2)$$

где $D_{\text{ср}}$ – среднее значение фрактальной размерности; D_1, \dots, D_n – значения размерности 1-го, ..., n -го ОП соответственно; n – общее число ОП.

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.

Результаты оценки значений размерности отпечатков пальцев

Варианты отпечатка пальца					
Значение фрактальной размерности	1,5564	1,5529	1,5567	1,5574	1,5569
Среднее значение размерности $D_{\text{ср}}$				1,5561	
Среднее отклонение $\Delta D_{\text{ср}}$				0,0062	

Однако существует следующая проблема. Дело в том, 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. Кроме того, при сканировании ОП возможны различные смещения и растяжения кожи, нажатие может происходить с разной силой, сухость и влажность кожи также влияют на значение размерности отпечатка пальца. Следовательно, при каждом сканировании одного и того же пальца значение ОП будет всегда немного отличаться.

Чтобы идентификация произошла успешно, необходимо оставить какой-либо минимальный промежуток, в который будут попадать следующие значения одного и того же ОП. Для этого по формуле (3) вычисляется среднее отклонение, т.е. определяется диапазон значений, в пределах которого значения отпечатков пальцев могут отличаться от эталона:

$$\Delta D_{\text{ср}} = (|D_1 - D_{\text{ср}}| + |D_2 - D_{\text{ср}}| + \dots + |D_n - D_{\text{ср}}|)/n, \quad (3)$$

где $\Delta D_{\text{ср}}$ – отклонение от среднего значения.

После того как каждый пользователь будет зарегистрирован, при любом следующем обращении к системе будет происходить распознавание личности, т.е. идентификация.

Следующим этапом распознавания личности является аутентификация пользователей. Аутентификация – это процесс, в рамках которого выполняется проверка личности пользователя, компьютера или сети и который фактически подтверждает, что пользователь именно тот человек, за которого себя выдает. Вообще аутентификация индивидов возможна при представлении информации, хранящейся в разной форме, которая могла бы подтвердить подлинность субъекта. Аутентификация позволяет обоснованно и достоверно разграничить права доступа к информации, находящейся в общем пользовании.

В нашем случае аутентификация происходит следующим образом. Предположим, зарегистрированный ранее пользователь хочет войти в систему. Выбрав из выпадающего списка зарегистрированных пользователей свой логин (в данном случае он является фамилией субъекта), пользователь должен предъявить нечто, что может подтвердить подлинность субъекта. В данном случае в качестве такого «паспорта» выступает отпечаток пальца.

Далее пользователь с помощью сканера снимает изображение отпечатка пальца. Полученное изображение обрабатывается системой и получается некое число, которое характеризует данный отпечаток, – фрактальная размерность ОП. Полученный результат сравнивается со значением, которое хранится в базе данных и соответствует зарегистрированному шаблону того пользователя, в качестве которого заявляет себя субъект.

Далее возможны два варианта. Если полученное значение фрактальной размерности схоже со значением эталона в пределах допустимых значений, то система воспринимает

пользователя как «своего». Аутентификация проходит успешно и 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 администрирования данной системы доступа. Это значит, что если администратор установит слишком строгие правила политики безопасности, а именно низкий уровень допустимого отклонения $\Delta D_{\text{ср}}$, 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 $\Delta D_{\text{ср}}$, 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», «возможность пропустить чужого». Следует отметить, что ошибка второго рода более критична, чем первого. Если доступ получит нелегальный пользователь, то ущерб может быть намного больше, чем от ошибки *FRR*. Ошибка «ложный отказ» легко устранима повторным сканированием отпечатка пальца.

Согласно проведенному исследованию, для разрабатываемой системы эти параметры составили: *FAR* – 0,001, *FRR* – 0,0001%. Данные цифры означают буквально следующее – для показателя *FAR* «пропустить чужого» из тысячи процедур идентификации возможен один случай, когда ошибочно будет опознан незарегистрированный пользователь, соответственно для *FRR* «не допустить своего» из десяти тысяч возможен один случай, когда легитимный пользователь не будет опознан. В работе было выполнено тестирование алгоритма идентификации личности по фрактальной размерности отпечатков пальцев на искусственных ОП. Полученные результаты дали основание полагать, что данный алгоритм применим для распознавания личности и построения реальных СКУД.

Преимущества реализуемого метода распознавания личности заключаются в следующем. Безопасность – сама идея идентификации личности по фрактальной размерности отпечатков пальцев существенно отличается от существующих алгоритмов. Для каждого отпечатка пальца вычисляется его фрактальная размерность – математическая величина, которая уникальна для каждого отпечатка пальца. Соответственно все дальнейшие операции происходят именно с этой характеристикой. Данное условие существенно повышает безопасность системы, так как по фрактальной размерности нельзя выполнить обратное преобразование и, следовательно, невозможно восстановить структуру и рисунок отпечатка.

Размер хранимых данных – в этом компоненте реализованная система фрактальной идентификации личности сильно выигрывает. Это связано с тем, что в базе данных регистрируется не сам отпечаток пальца, и даже не его контрольные точки, а непосредственно числовые характеристики – фрактальные размерности, которые занимают наименьший, по сравнению с другими системами, объем.

Результаты и выводы – в данной статье представлено описание нового метода идентификации личности по фрактальной размерности отпечатков пальцев. В частности рассказывается об этапах реализации данного метода на практике, его тестировании с использованием базы отпечатков пальцев, и делается заключение о возможности применения данного метода в качестве реальной системы распознавания личности. Руководствуясь основными принципами построения систем биометрической идентификации, была программно реализована система распознавания личности, которая может послужить основой для реально действующей СКУД.

Литература

1. Венедов М.А. Политика России в области биометрии [Электронный ресурс]. – Режим доступа: http://www.electronics.ru/pdf/6_2000/, свободный (дата обращения: 24.05.2010).
2. Морозов А.В. Введение в теорию фракталов. – М.: Парус, 1996. – 160 с.
3. Кроновер Р.М. Фракталы и хаос в динамических системах. Основы теории. – М.: Постмаркет, 2000. – С. 127–137.
4. Программа для генерации искусственных отпечатков пальцев [Электронный ресурс]. – Режим доступа: <http://bias.csr.unibo.it/research/biolab/sfinge.html/>, свободный (дата обращения: 24.05.2010).

Трифонов Денис Иванович

Аспирант каф. безопасности информационных систем
Самарского государственного университета, г. Самара.
Тел.: 8-927-722-83-12;
Эл. адрес: trifonovdi@gmail.com

D.I. Trifonov

Person identification by fractal dimension fingerprints and control access systems

Article is devoted to new method person recognition, based on fractal dimension human fingerprints. Method, theoretic base, algorithm, advantages and disadvantages describes in this paper. This method can be used as base for creation real Access control system (ACS).

Keywords: Biometry, fingerprint, fractal, fractal dimension, person identification, authentication, ACS.
