



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: 2004128951/09, 22.09.2004

(24) Дата начала отсчета срока действия патента:
22.09.2004

(43) Дата публикации заявки: 10.03.2006

(45) Опубликовано: 27.10.2006 Бюл. № 30

(56) Список документов, цитированных в отчете о
поиске: RU 2148274 C1, 17.08.2000. RU 2199943
C1, 10.03.2003. RU 2195020 C1, 11.01.2000. EP
1085454 A2, 21.03.2001. US 6181808 B1,
30.01.2001. US 6175641 B1, 16.01.2001. US
5719950 A, 17.02.1998.

Адрес для переписки:

194223, Санкт-Петербург, пр-кт М. Тореза, 68,
ОАО "ЦНИИ "Электрон", ген. директору И.С.
Васильеву

(72) Автор(ы):

Васильев Иван Сергеевич (RU),
Кафтанов Виталий Сергеевич (RU),
Минкин Виктор Альбертович (RU),
Штам Александр Ильич (RU),
Рацис Панос (CY),
Рыкашевский Ханс (FR)

(73) Патентообладатель(и):

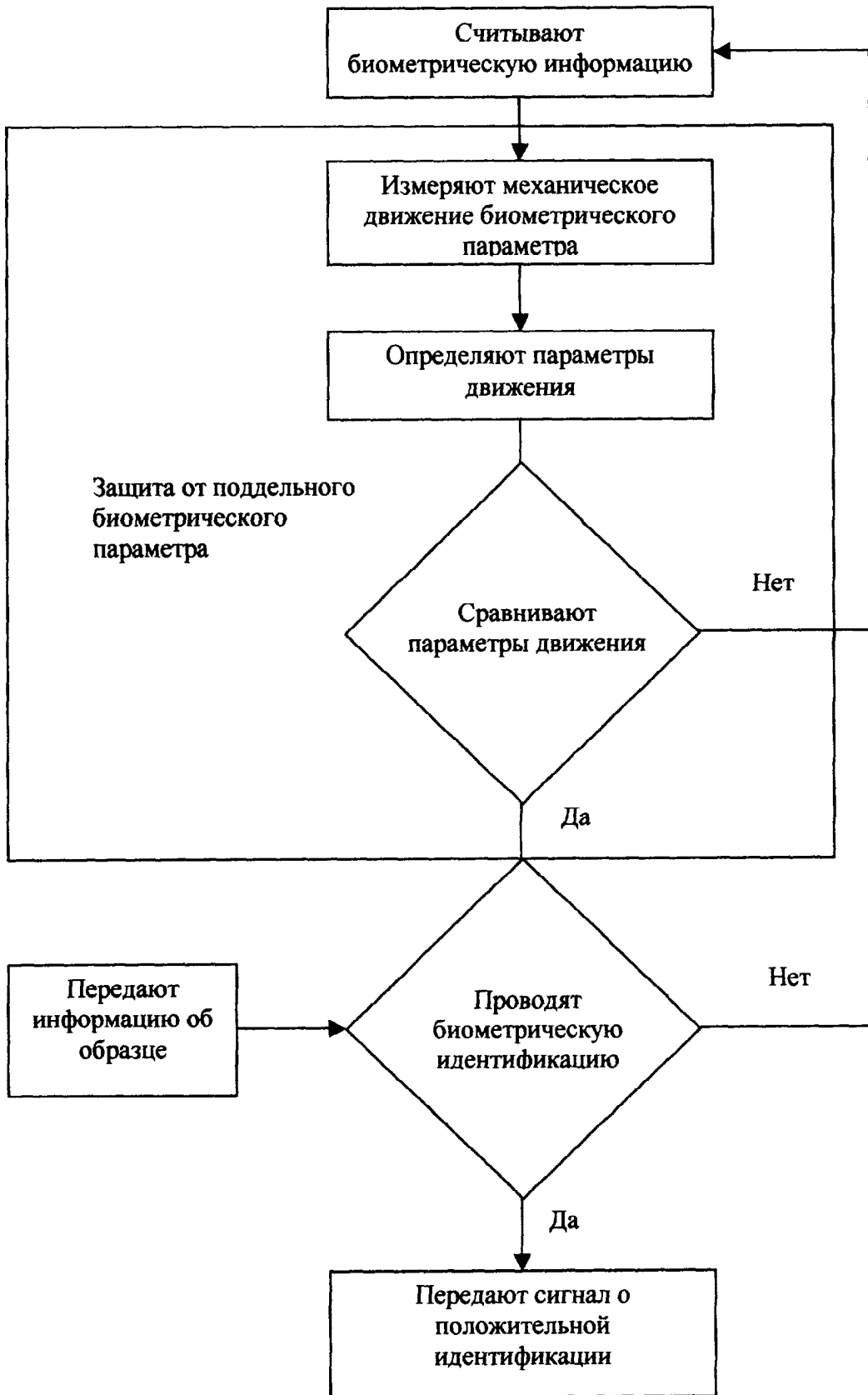
ОАО "Центральный научно-исследовательский
институт "Электрон" (RU),
Рацис Панос (CY),
Рыкашевский Ханс (FR)

(54) СПОСОБ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

(57) Реферат:

Изобретение относится к биометрии. Его использование для защиты от поддельных биометрических параметров в системах контроля доступа и паспортных системах позволяет получить технический результат в виде повышения надежности биометрической идентификации. Способ включает в себя считывание информации о биометрической характеристике пользователя, сравнение полученной информации с образцом и защиту от поддельной статической биометрической характеристики. Технический результат достигается благодаря тому, что для защиты от

поддельной биометрической характеристики измеряют изменение во времени статической биометрической характеристики, определяют параметры изменения статической биометрической характеристики и отвергают вводимую статическую биометрическую характеристику как поддельную при отклонении указанных параметров от установленной нормы. В качестве статической биометрической характеристики используют отпечаток пальца, а изменение во времени при снятии отпечатка пальца определяют по временной зависимости площади контактной поверхности отпечатка пальца. 3 з.п. ф-лы, 5 ил.





FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(51) Int. Cl.
G06K 9/62 (2006.01)
A61B 5/117 (2006.01)

(12) **ABSTRACT OF INVENTION**

(21), (22) Application: **2004128951/09, 22.09.2004**

(24) Effective date for property rights: **22.09.2004**

(43) Application published: **10.03.2006**

(45) Date of publication: **27.10.2006 Bull. 30**

Mail address:
**194223, Sankt-Peterburg, pr-kt M. Toreza, 68,
OAO "TsNII "Ehlektron", gen. direktoru I.S. Vasil'evu**

(72) Inventor(s):
**Vasil'ev Ivan Sergeevich (RU),
Kaftanov Vitalij Sergeevich (RU),
Minkin Viktor Al'bertovich (RU),
Shtam Aleksandr Il'ich (RU),
Ratsis Panos (CY),
Rykashevskij Khans (FR)**

(73) Proprietor(s):
**OAO "Tsentral'nyj nauchno-issledovatel'skij
institut "Ehlektron" (RU),
Ratsis Panos (CY),
Rykashevskij Khans (FR)**

(54) **METHOD FOR BIOMETRIC IDENTIFICATION**

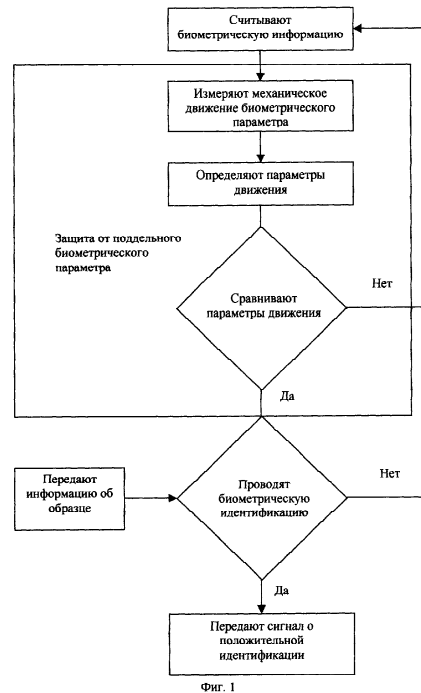
(57) Abstract:

FIELD: biometry.

SUBSTANCE: method includes reading information about biometric characteristic of user, comparing received information to sample and protection from fake static biometric characteristic. Technological result is achieved due to fact, that for protection from fake biometric characteristic, alternation of static biometric characteristic in time is measured, parameters of alternation of static biometric characteristic are determined and input static biometric characteristic is refused as fake if aforementioned parameters deviate from set norm. As static biometric characteristic, fingerprint is used, and alternation in time during reading of fingerprint is determined by temporal dependence of area of contact surface of fingerprint.

EFFECT: increased reliability of biometrical identification when used for protection from fake biometric parameters in access control and passport systems.

4 cl, 6 dwg



Фиг. 1

RU 2 286 599 C2

RU 2 286 599 C2

Изобретение относится к области биометрии и может быть использовано для защиты от поддельных биометрических параметров в системах контроля доступа и паспортных системах.

5 Глобальное развитие биометрических систем создает естественные предпосылки для разработки систем и методов фальсификации биометрических параметров, а также
разработки систем и методов по защите от фальсификации при биометрической
идентификации. Условно все методы защиты от поддельных или фальсифицированных
биометрических параметров можно разделить на статические и динамические. К
10 статическим методам защиты следует отнести дополнительно определяемое мгновенное значение определенной физической величины, которое должно быть присуще реальному биометрическому параметру и отсутствовать у фальсифицированного. Примером такой защиты может быть определение электрического сопротивления кожи пальца или руки для дактилоскопических сенсоров и систем [1, 2] с помощью специальной системы электродов, а также для идентификации по форме ладони [3].

15 Другим примером статической дополнительной защиты является измерение температуры объекта и других физиологических параметров, присущих человеку, что используется как в контактных биометрических системах идентификации, например дактилоскопических [4], так и в бесконтактных, например системах распознавания по лицу или сетчатке глаза. Дополнительно измеряемая физическая величина позволяет в
20 некоторых случаях отвергать поддельные биометрические носители, однако если эта физическая величина является известной, то возможно ее использование и в фальсифицированном биометрическом параметре. Для фальсификации, например, электрического сопротивления кожи достаточно изготовить фальшивый отпечаток пальца из электропроводящего силикона, имеющего электрическое сопротивление, аналогичное
25 сопротивлению кожи пальца. Для фальсификации температурной защиты достаточно изготовить фальсифицированный носитель из материала с хорошей теплопроводностью, тогда выявить подделку статическим методом практически невозможно. Кроме того, введение измерения дополнительного параметра требует создания дополнительных аппаратных средств, например системы электродов на дактилоскопическом сенсоре для
30 измерения электрического сопротивления кожи или температурного датчика для измерения температуры тела. Это приводит к удорожанию и усложнению системы биометрической идентификации и снижает надежность работы.

Таким образом, статические методы защиты от поддельных биометрических носителей не обеспечивают реального выявления поддельных носителей, т.к. основаны на измерении
35 дополнительных статических параметров, лишь частично отражающих свойства живых объектов.

Другим возможным способом статической защиты при биометрической идентификации является детальный анализ формы вводимого биометрического параметра. Действительно, подделка обычно сделана менее качественно, чем оригинал, который
40 содержит огромное количество мелких деталей, не передающихся при изготовлении подделки. Например, для отпечатка пальца это могут быть поры на коже (пороскопия) или форма края папиллярной линии (эджескопия), которые существенно отличаются на оригинале и подделке. Однако для детального анализа формы биометрического параметра необходимо, прежде всего, иметь высокую разрешающую способность сканера. Для
45 уверенной идентификации по особым точкам отпечатка пальца достаточно иметь разрешающую способность сканера 500 dpi (при площади $\sim 1,5 \text{ см}^2$), а для анализа формы желательнее иметь разрешающую способность более 1500 dpi. Такая высокая разрешающая способность существенно затрудняет работу системы в режиме реального времени, увеличивает стоимость системы и, в конечном счете, не дает гарантии защиты,
50 потому что возможно изготовить фальшивый биометрический носитель с учетом повышенной разрешающей способности.

Известные динамические способы защиты от подделок основаны на анализе изменения во времени основного или дополнительного биометрического параметра.

Наиболее известным биометрическим параметром, характеризующим реального человека, является его пульс и пульсовые волны, вызываемые сокращением сердечной мышцы.

Известен способ, устройство регистрации пульсовой волны и биометрическая система 5 идентификации, позволяющие выявлять фальшивые носители дактилоскопической информации за счет эффекта объемного пульса, наблюдаемого в кончиках пальца, т.е. синхронных пульсовых волн, фиксируемых в различных точках и областях одного объекта. Указанный способ включает считывание информации о биометрическом параметре 10 пользователя - регистрацию пульсовой волны путем освещения кровенесущей ткани, преобразование светового потока, обусловленного рассеянием на кровенесущей ткани, в электрический сигнал с помощью оптоэлектронного преобразователя, обработку полученной пульсовой волны с помощью нескольких фоточувствительных областей, 15 расположенных на находящихся рядом местах кровенесущей ткани, сравнение полученной информации с образцом и защиту от поддельного биометрического параметра с помощью информации об объемном пульсе.

Данный способ биометрической идентификации взят нами за прототип [5]. Способ 20 позволяет успешно выявлять фальшивые носители дактилоскопического изображения при наличии у человека нормального периферийного пульса в кончиках пальцев. Однако известно, что при некоторых заболеваниях периферийный пульс у человека может практически отсутствовать, также происходит существенное уменьшение периферийного 25 пульса, связанное с уменьшением размеров микрокапилляров, например при охлаждении организма или когда человек нервничает. Данное свойство существенно ограничивает применение данного способа для выявления поддельных дактилоскопических носителей информации. Кроме того, данный способ защиты применим только для систем, 30 работающих в проходящем через объект свете, а указанные системы составляют незначительную часть биометрического рынка.

Предлагаемый способ решает задачу повышения надежности системы биометрической 35 идентификации путем уменьшения ошибок при выявлении поддельных биометрических носителей.

Достигается это тем, что в известном способе биометрической идентификации, 40 включающем считывание (ввод) информации о биометрическом параметре пользователя, сравнение полученной информации с образцом и защиту от поддельного биометрического параметра, защиту от поддельного биометрического параметра осуществляют измеряя механическое движение (перемещение) данного биометрического параметра, выявляют 45 параметры движения, присущие биометрическому параметру, и отвергают вводимый биометрический параметр как поддельный при отклонении указанного параметра от установленной нормы.

В другом варианте способа в качестве биометрического параметра используют 50 отпечаток пальца, а механическое движение отпечатка пальца измеряют по временной зависимости площади контактной поверхности отпечатка пальца.

Отличием является также то, что площадь контактной поверхности отпечатка пальца определяют используя параметры плотности распределения сигнала биометрического носителя, например ширину среднеквадратического отклонения.

В следующем варианте способа механическое движение биометрического параметра 45 измеряют, используя временную зависимость интегрального значения, например центра тяжести данного биометрического параметра.

Известно, что пульсовая волна, перемещаясь внутри кровеносных сосудов человека, 50 изменяет кровенаполнение, а значит, и прозрачность кровеносных сосудов внутри организма человека [5]. Также известно, что в соответствии с третьим законом Ньютона для замкнутой системы должен выполняться закон сохранения импульса, т.е. внутреннее движение должно вызывать внешнее перемещение. Конечно, человеческий организм представляет собой достаточно сложную систему, весьма далекую от классической механики и динамики, однако многие ученые предполагают, что именно фрактальная

динамика и является одной из основных характеристик высокоразвитых организмов [6].

Наложение множества процессов мышечной, мозговой, электрической активности, одновременно происходящих на различных уровнях, должно, по логике, приводить к смазыванию каждого из перечисленных процессов и создавать сложности для их

5 отдельного восстановления из хаоса механического движения. Действительно, достаточно тяжело поверить, что можно выявить, например, пульсовую составляющую в доле микрон на фоне скорости перемещения частей тела человека в несколько см/с. Однако с помощью относительно несложной математики авторам удалось устойчиво выявить механическое перемещение пальца, синхронное с пульсовой волной при установке пальца в

10 многоэлементный матричный дактилоскопический сенсор.

Кожа человека представляет собой сложную многослойную структуру [7], механические свойства которой достаточно сложно подделать, т.к. поверхностный слой кожи состоит из отдельных ороговевших клеток, а практически все подделки изготавливают из монолитного материала. Пальцы человека обладают определенной упругостью, которая обычно

15 существенно различна для людей, занимающихся физическим или умственным трудом. При этом была отмечена определенная закономерность: при установке на контактную поверхность пальцы, которые условно можно назвать жесткими, совершают большее перемещение по горизонтальной оси, а пальцы, которые условно можно назвать мягкими, совершают большее перемещение по вертикальной оси, причем амплитуда, частота и фаза этих перемещений синхронизированы с прохождением пульсовой волны в теле человека. Авторам удалось установить, что данный эффект наблюдается и при

20 практическом отсутствии периферийного пульса в кончиках пальцев, т.е. когда прозрачность пальцев практически не изменяется из-за сужения микрокапилляров. Наблюдаемое явление существенно уменьшает возможность изготовления не выявляемых фальшивых носителей биометрической и, прежде всего, дактилоскопической информации, т.к. копирование свойств эластичности кожи в дополнение ко всем другим параметрам представляет собой трудноразрешимую задачу.

Предлагаемый способ биометрической идентификации особенно важен для применения в составе биометрической паспортной системы, стоимость которой может составлять

30 несколько миллиардов долларов, а стоимость средств, затраченных на изготовление фальшивого биометрического параметра, может не превышать всего 100 долларов США [8]. При этом если паспортная система не способна выявить поддельный носитель биометрической информации, то все средства на нее будут затрачены впустую, если паспортная система не оснащена надежной системой защиты от поддельных

35 биометрических носителей.

Естественно, что возможно наблюдение не только пульсовой кривой, но и ее вариабельности, например, используя метод фрактальной динамики [6]. При этом, конечно, увеличивается и время измерения (до 30 с) [6], но вероятность пропуска поддельного носителя становится ниже, что может быть существенным для особо охраняемых объектов.

На фиг.1 приведена структурная схема предлагаемого способа биометрической идентификации.

На фиг.2 приведены графики пульсовых волн, полученные одновременно для реального пальца с ярко выраженным периферийным пульсом:

- 45 а) при измерении временной зависимости "прозрачности" пальца;
 б) при измерении временной зависимости среднеквадратического отклонения (СКО);
 в) при измерении временной зависимости математического центра тяжести.

На фиг.3 приведены графики пульсовых волн для практически отсутствующего периферийного пульса:

- 50 а) на реальном пальце при измерении временной зависимости "прозрачности" пальца;
 б) на реальном пальце при измерении временной зависимости СКО;
 в) на реальном пальце при измерении временной зависимости математического центра тяжести.

На фиг.4 приведены графики пульсовых волн для фальсифицированного биометрического параметра, установленного на реальный палец:

- a) при измерении временной зависимости "прозрачности" пальца;
- b) при измерении временной зависимости СКО;

5 c) при измерении временной зависимости математического центра тяжести.

На фиг.5 приведены плотность распределения сигнала с дактилоскопического сканера в момент прохождения пульсовой волны через палец (a) и в обычном состоянии (b).

Приведем пример конкретного выполнения способа при использовании дактилоскопического сканера, основанного на принципе получения дактилоскопического изображения в проходящем через палец свете [9, 10, 11].

10 считывание информации о биометрическом параметре пользователя осуществляют, устанавливая палец пользователя в дактилоскопический сканер DC21P [12], подсоединенный к персональному компьютеру Samsung P30, через параллельный порт, работающий в режиме EPP. Информация об образце, т.е. оригинальном отпечатке, была
15 заранее занесена в базу данных, а также на пластиковую карту (паспорт) пользователя [12]. Программа DC Test Pulse, загруженная на персональный компьютер, первоначально осуществляет сравнение сканируемого отпечатка с отпечатком, хранящимся в базе данных (с образцом), а затем осуществляет проверку подлинности вводимого биометрического параметра, выявляя совпадение частотных составляющих пульсовых волн с помощью
20 быстрого Фурье - преобразования для пульсовых кривых, полученных различными методами расчета и с различных участков отпечатка пальца. Результаты измерений выводятся программной биометрической идентификации на экран PC и на внешнее управляющее устройство. Проверку подлинности и сравнение параметров движения осуществляют, анализируя получаемый спектр основных частот за 5 секунд. Естественно, что отсутствие
25 пульсовых перемещений или их вариабельность более определенного порога в 20% формирует сигнал "Нет" при сравнении параметров движения, и система возвращается к новому циклу считывания биометрической информации. В случае совпадения частотных параметров механического движения и объемного пульса проверка подлинности считается осуществленной положительно и полученное дактилоскопическое изображение сравнивают
30 с образцом, после чего делают вывод о результате идентификации. В противном случае, когда отсутствует механическое движение отпечатка или его вариабельность превышает 20%, биометрический параметр отвергается как поддельный и система возвращается к первоначальному считыванию и дает предупредительный звуковой сигнал. Частота считывания дактилоскопических изображений для сканера DC21P составляет 50 кадров/с,
35 что вполне достаточно для уверенной регистрации пульса, а мощность компьютера P1600M достаточна для проведения регистрации пульсовых волн и идентификации пользователя в режиме реального времени.

Поясним пульсовые кривые, приведенные на фиг 2. Из фиг.2 следует, что у
40 большинства людей при наличии четкого периферийного пульса можно наблюдать пульсовые волны не только по изменению прозрачности внутри пальца, но и по движению пальца по вертикали и горизонтали. Это заключение достаточно важно, т.к. позволяет фиксировать пульсовую волну не только с помощью дактилоскопического сканера, просвечивающего палец, что уже было известно ранее [5], но и с помощью любых других дактилоскопических сканеров (оптических, емкостных), имеющих достаточное
45 быстродействие (не менее 50 f/s) и разрешающую способность.

На фиг.3 приведены пульсовые кривые для человека, имеющего слабый периферийный пульс. Исследования показали, что в нормальных условиях примерно 5-10% людей имеет такую картину, а при охлаждении или стрессе этот процент увеличивается. Приведенные кривые показывают, что пульсовые волны при механическом перемещении пальца менее
50 чувствительны к периферийному пульсу, чем изменение прозрачности, а значит, более надежно характеризуют живой палец.

На фиг.4 приведены пульсовые кривые для наиболее сложного, с точки зрения выявления подделки, фальшивого пальца, когда на реальный палец установлена

прозрачная силиконовая тонкая прокладка с чужим трехмерным (рельефным) отпечатком пальца. Из фиг.4 следует, что такой фальшивый дактилоскопический носитель приводит практически к исчезновению пульсаций, связанных с механическим перемещением.

Вероятно, это происходит из-за существенной разницы в эластичности и механико-инерционных свойств реального пальца и фальшивого дактилоскопического носителя.

Таким образом, отсутствие механического пульса в пальце может свидетельствовать о наличии фальшивого дактилоскопического носителя и давать сигнал о возможной фальсификации системы, что особенно важно для паспортной технологии, в которой необходимо уверенно различать изображение отпечатка пальца на документе от живого пальца.

На фиг.5 показано изменение плотности распределения сигнала отпечатка пальца при прохождении пульсовой волны, когда палец плотнее прижимается к контактной поверхности (Фиг.5а) и ширина распределения и СКО существенно уменьшаются по сравнению с моментом времени, когда плотность крови в пальце уменьшается (Фиг.5б).

Так как СКО является интегральной и относительной характеристикой, то оказалось, что временная зависимость СКО мало чувствительна к шумам и артефактам и хорошо передают параметры пульса. Возможно использование и других математических характеристик, отражающих ширину распределения или расстояния между модами (максимумами распределений) для получения пульсовой зависимости.

Естественно, что приведенная в описании реализация способа биометрической идентификации не ограничивает возможные применения предлагаемого изобретения, которые могут быть значительно шире и определяться уровнем развития техники.

В качестве примера биометрической технологии в данном описании была использована дактилоскопическая технология, как наиболее распространенная и имеющая лучшие характеристики. Естественно, возможно применение предлагаемого метода и для защиты других биометрических параметров, связанных с движением тела человека, например идентификации по лицу или радужной оболочке глаза.

Применение данного изобретения возможно и в комплексе с другими способами защиты от поддельных биометрических параметров, что должно обеспечить надежность биометрической системы в соответствии с требованиями рынка и заказчиков.

Литература

1. RU п.2218084, МКИ А 61 В 5/117, опубл. 10.12.2003.
2. US п.6175641, МКИ А 61 В 5/117 В, опубл. 16.01.2001.
3. US п.6181808, МКИ G 06 К 9/00, опубл. 30.01.2001.
4. US п.5719950, МКИ G 06 К 9/00, опубл. 17.02.1998.
5. RU п.2199943, МКИ А 61 В 5/02, опубл. 10.03.2001. (Прототип).
6. Вассерман Е.А., Карташев Н.К., Полонников Р.И. "Фрактальная динамика электрической активности мозга", С.Петербург, Наука, 2004 г.
7. Кожа (Строение, функция, общая патология и терапия). / Под ред. Фролова Е.П., Москва, Медицина, 1982 г.
8. T.Matsumoto, H.Matsumoto, K.Yamada, S.Hoshino "Fingers on Fingerprint systems". Proceedings of SPIE, vol.4677, January, 2002.
9. RU п.2031625, МКИ А 61 В 5/117, опубл. 27.03.95 г.
10. US п.6668071, МКИ G 06 К 9/00, опубл. 23.12.2003.
11. RU п.2195020, МКИ G 06 К 5/00, 19/00, G 07 F 7/10, опубл. 20.12.2002 г.
12. www.elsvs.ru 06.2004.

Формула изобретения

1. Способ биометрической идентификации, включающий считывание информации о биометрической характеристике пользователя, сравнение полученной информации с образцом и защиту от поддельной статической биометрической характеристики, отличающийся тем, что для защиты от поддельной биометрической характеристики измеряют изменение во времени статической биометрической характеристики, определяют

параметры изменения статической биометрической характеристики и отвергают вводимую статическую биометрическую характеристику как поддельную при отклонении указанных параметров от установленной нормы.

5 2. Способ по п.1, отличающийся тем, что в качестве статической биометрической характеристики используют отпечаток пальца, а изменение во времени при снятии отпечатка пальца определяют по временной зависимости площади контактной поверхности отпечатка пальца.

3. Способ по п.2, отличающийся тем, что площадь контактной поверхности отпечатка пальца определяют, используя параметры плотности распределения сигнала биометрической характеристики, например ширину среднеквадратического отклонения.

10 4. Способ по п.1, отличающийся тем, что изменение по времени статической биометрической характеристики измеряют, используя временную зависимость интегрального значения, например центра тяжести данной биометрической характеристики.

15

20

25

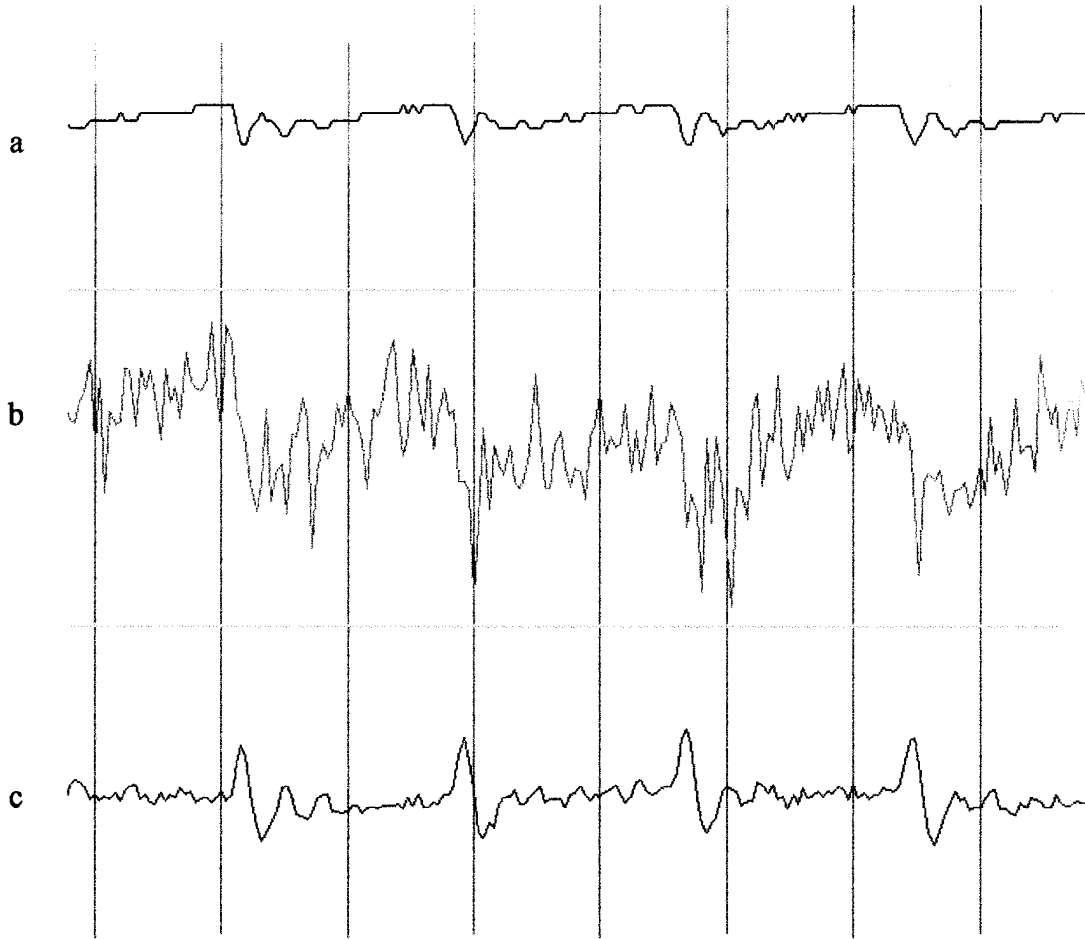
30

35

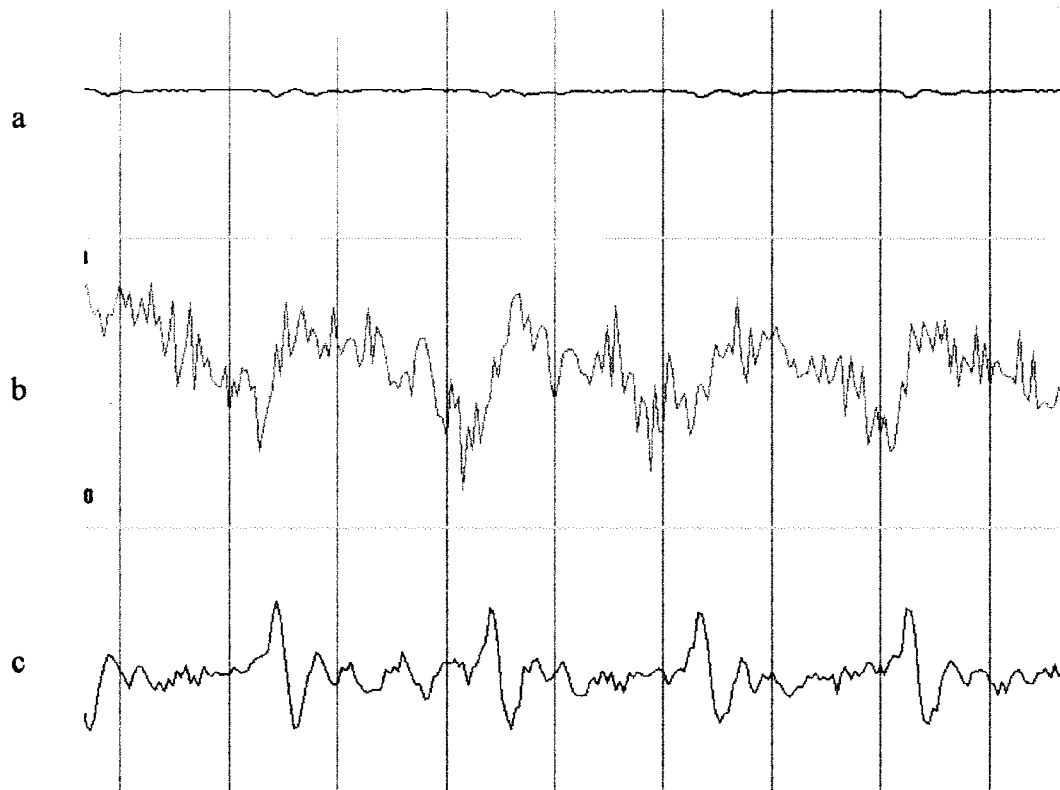
40

45

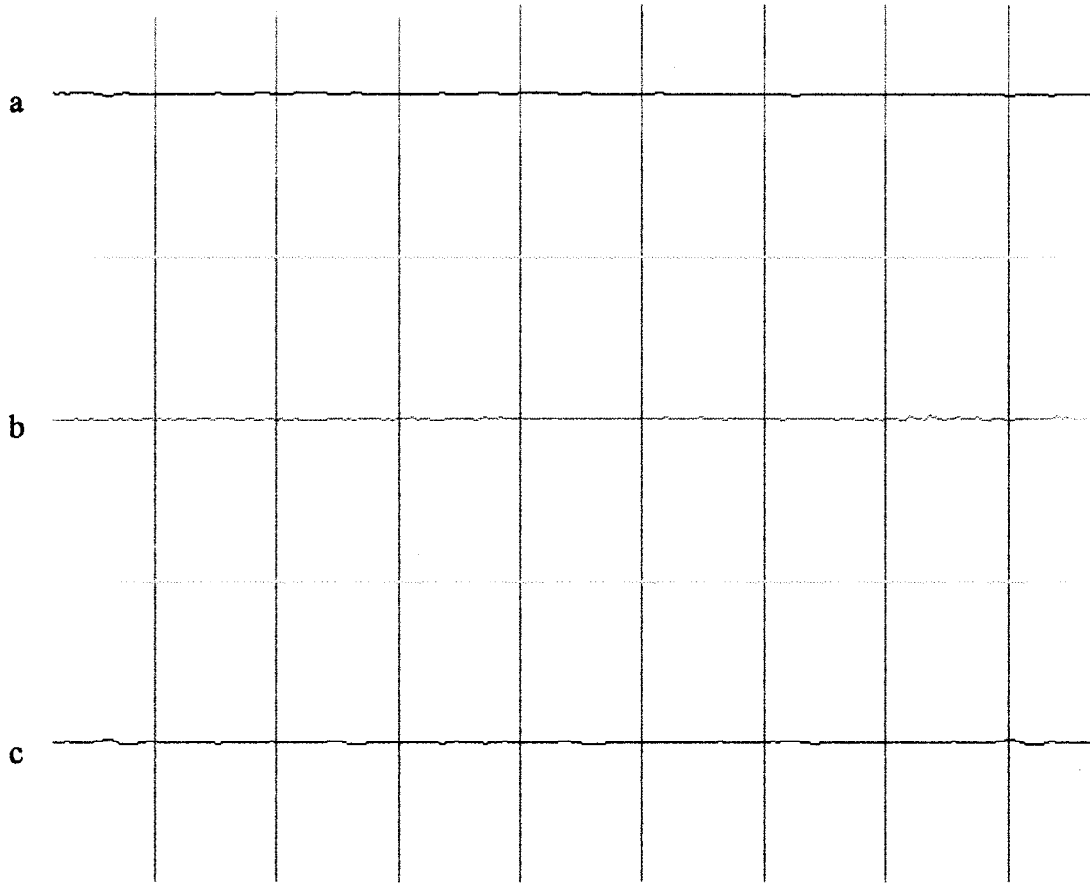
50



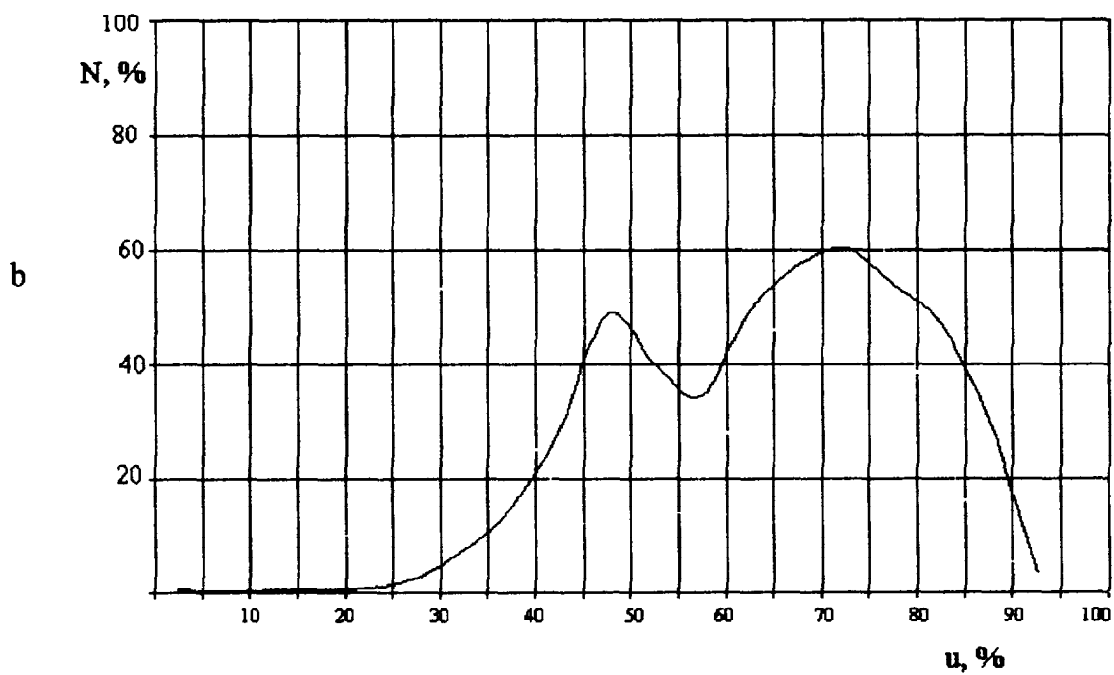
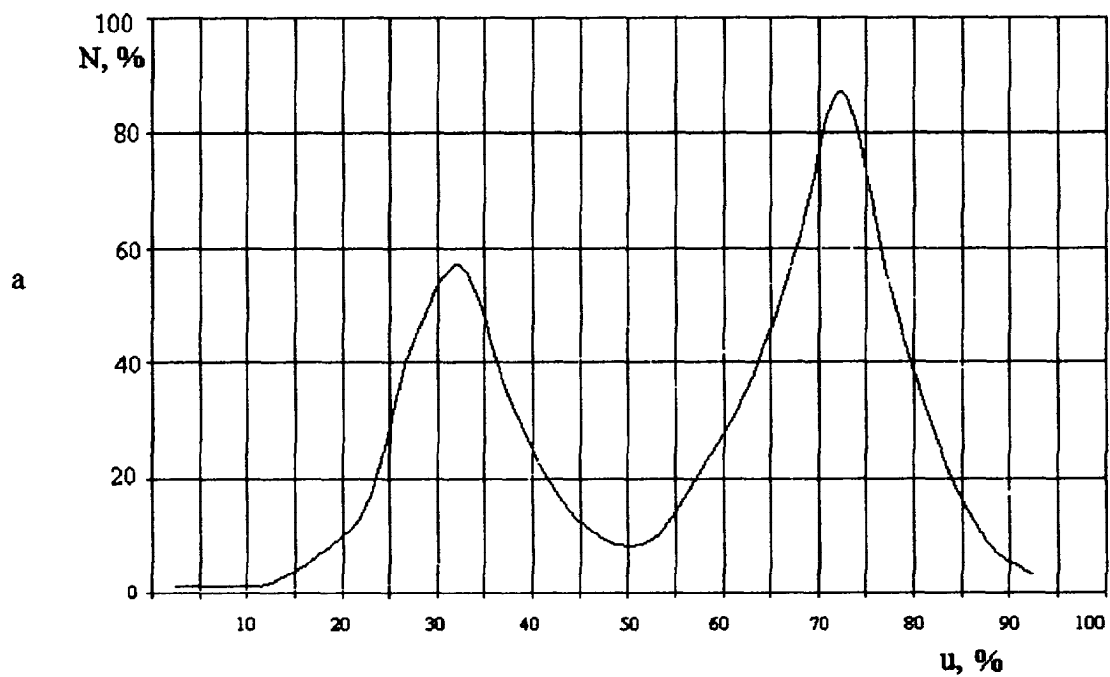
фиг. 2



фиг. 3



фиг. 4



фиг. 5