РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 459 252** (13) **C1**

(51) МПК
G06K 9/62 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2011134510/08, 17.08.2011**

(24) Дата начала отсчета срока действия патента:
17.08.2011

Приоритет(ы):
(22) Дата подачи заявки: **17.08.2011**

(45) Опубликовано: **20.08.2012** Бюл. № **23**

(56) Список документов, цитированных в отчете о поиске: **RU 2008111525 A, 27.09.2009. RU 2148274 C1, 27.04.2000. RU 83152 U1, 20.05.2009. US 5995953 A1, 30.11.1999. US 6950538 B2, 27.09.2005. EP 1221127 B1, 06.05.2009.**

Адрес для переписки:
644119, г.Омск, Бульвар Зеленый, 8, кв.7, П.С. Ложникову

(72) Автор(ы):
Ложников Павел Сергеевич (RU),
Перевальский Виктор Александрович (RU),
Патронов Константин Сергеевич (RU)

(73) Патентообладатель(и):
Общество с ограниченной ответственностью "Научно-технический центр "КАСИБ" (RU)

(54) СИСТЕМА И СПОСОБ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ЭВМ (ВАРИАНТЫ)

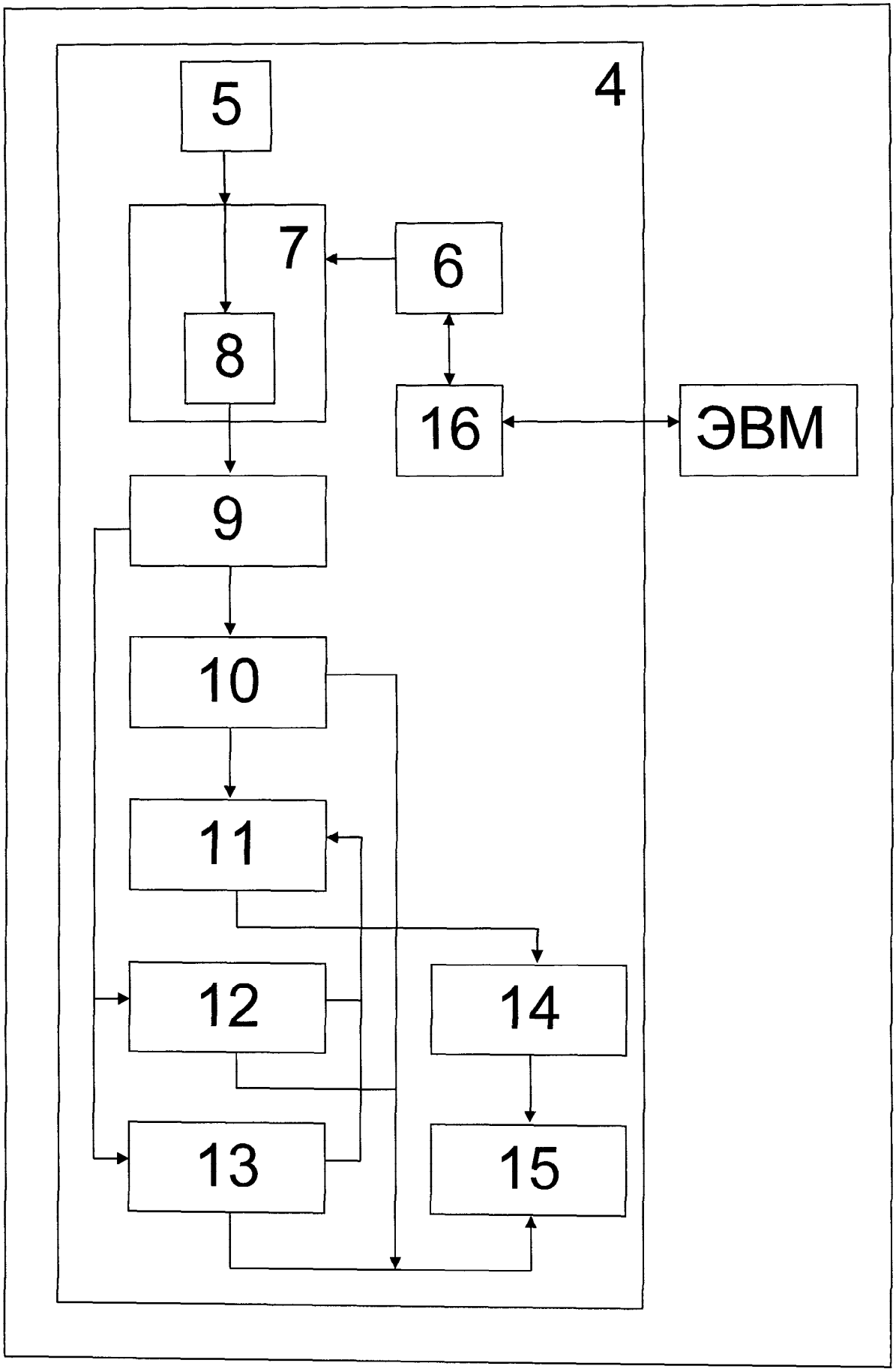
(57) Реферат:

Изобретение относится к средствам считывания и идентификации информации, которые могут использоваться для контроля подлинности информации и могут использоваться в области безопасности, государственных учреждениях и банках. Технический результат заключается в обеспечении надежной идентификации при увеличенном количестве зарегистрированных пользователей в базе данных. Такой результат достигается тем, что в системе идентификации пользователей ЭВМ, содержащей носитель информации и устройство считывания информации, включающее первый модуль, выполненный в виде корпуса и пишущего элемента, и второй модуль, содержащий сенсорное устройство и контроллер, согласно изобретению во второй модуль, выполненный герметизированным на печатной плате, дополнительно введен процессор обработки, включающий аналого-цифровой преобразователь, блок повышения качества входных данных, блок интегральных преобразований, блок математических ожиданий, дисперсии, блок коэффициентов корреляции, блок временного интервала, блок эталона, блок принятия решения, и USB интерфейс, сенсорное устройство выполнено в виде акселерометра, причем выход акселерометра соединен со входом процессора обработки, выход которого соединен со входом контроллера, выход которого соединен с USB интерфейсом и далее USB портом с ЭВМ, фиксирующим информацию, при этом питание акселерометра, процессора обработки и процессора осуществляется от ЭВМ через USB порт. 3 н. и 6 з.п. ф-лы, 6 ил.

RU 2459252 C1

RU 2459252 C1

RU 2459252 C1



Фиг. 2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 459 252** (13) **C1**

(51) Int. Cl.
G06K 9/62 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2011134510/08, 17.08.2011**

(24) Effective date for property rights:
17.08.2011

Priority:
(22) Date of filing: **17.08.2011**

(45) Date of publication: **20.08.2012 Bull. 23**

Mail address:
644119, g.Omsk, Bul'var Zelenyj, 8, kv.7, P.S. Lozhnikovu

(72) Inventor(s):
Lozhnikov Pavel Sergeevich (RU),
Pereval'skij Viktor Aleksandrovich (RU),
Patronov Konstantin Sergeevich (RU)

(73) Proprietor(s):
Obshchestvo s ogranichennoj otvetstvennost'ju "Nauchno-tekhnicheskij tsentr "KASIB" (RU)

(54) SYSTEM AND METHOD OF IDENTIFYING COMPUTER USERS (VERSIONS)

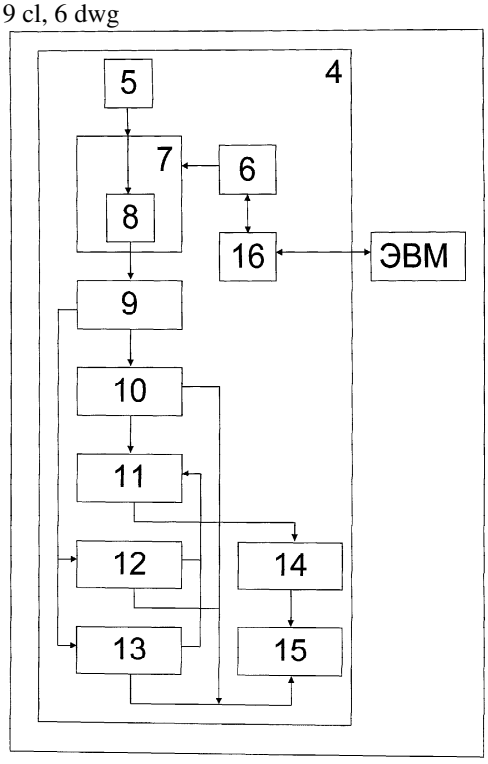
(57) Abstract:

FIELD: information technology.

SUBSTANCE: in the system of identifying computer users, having a data medium and a data reader, having a first module which is in form of a housing and writing element, and a second module having a sensor device and a controller, according to the invention, the second module, which is sealed on a printed-circuit board, further includes a processing processor, having an analogue-to-digital converter, a unit for improving quality of input data, an integral transformation unit, a unit for mathematical expectation, dispersion, a correlation coefficient unit, a time interval unit, a reference unit, a decision unit and a USB interface; the sensor device is in form of an accelerometer whose output is connected to the input of the processing processor, whose output is connected to the input of the controller, whose output is connected to the USB interface and further by a USB port to the computer which stores the information, wherein the accelerometer, the processing processor and the processor are powered from the computer through the USB port.

EFFECT: providing reliable identification with more registered users in the database.

9 cl, 6 dwg



Фиг. 2

RU 2459252 C1

RU 2459252 C1

Изобретение относится к средствам считывания и идентификации информации, которые могут использоваться для контроля подлинности информации и могут использоваться в области безопасности, государственных учреждениях и банках.

Наиболее близкой к предлагаемому устройству является система идентификации объектов, содержащая носитель информации, размещаемый на идентифицируемом объекте, устройство считывания информации, корпус которого выполнен в виде ручки, контроллер видеосенсора, запоминающие устройства, блок усилителей [1].

Недостатком системы-прототипа также является узкая область применения и невысокие функциональные возможности.

Наиболее близким к предлагаемому способу является способ идентификации личности по особенностям подписи [2]. По этому способу первичные данные о динамике воспроизведения рукописного слова получают с помощью графического планшета в виде трех функций времени: изменения положения светового пера в плоскости планшета X(t) и Y(t), а также в виде изменения давления кончика пера на чувствительную к нажатию поверхность планшета P(t). Сущность заявленного изобретения заключается в том, что вводят в вычислитель преобразованные в цифровую форму колебания пера, воспроизводящего подпись идентифицируемой личности, и его давление на графический планшет с последующим определением начала и конца подписи идентифицируемой личности, фрагментируют упомянутую подпись, масштабируют каждый фрагмент этой подписи, вычисляют дифференциальные и интегральные параметры фрагментов упомянутой подписи, а также вычисляют временные интервалы фрагментов этой подписи. При необходимости идентификации личности решение принимают путем сравнения упомянутых вычисленных параметров и временных интервалов с их эталонными значениями, после определения упомянутых дифференциальных и интегральных параметров осуществляют повторное масштабирование упомянутых вычисленных параметров и временных интервалов, минимизируя среднее отклонение упомянутых вычисленных параметров и временных интервалов от их эталонных значений, дополнительно вычисляют коэффициенты корреляции этих вычисленных параметров и временных интервалов, а также вычисляют оценки указанных коэффициентов корреляции, при упомянутом принятии решения сравнивают эти оценки коэффициентов корреляции с их эталонными значениями. Решение об идентификации личности принимается искусственной нейронной сетью с предварительным ее обучением как на примерах образцов подписи идентифицируемой личности, так и на примерах попыток подделки, получаемых путем искажения упомянутых эталонных значений. Этот способ использует максимальный объем информации, который суммируется из общего числа контролируемых параметров и привлекаемых вторичных контролируемых параметров, получаемых из первичных параметров. Благодаря решению компенсировать плохое качество исходных параметров их количеством, основным достоинством прототипа является повышение достоверности идентификации личности по особенностям почерка.

Недостатком способа-прототипа является получение дополнительных параметров за счет разделения подписи на сегменты по признаку отрыва пера и вычисления дополнительных параметров динамики ввода на найденных участках подписи. Другими словами, количество выбираемых для идентификации параметров зависит от результата разбиения подписи на фрагменты. Приводятся оптимистические расчеты для подписи, в процессе воспроизведения которой автор совершил 7 отрывов пера от поверхности планшета. Большинство авторов реже делают прерывания при

написании пароля или не делают их вообще. Если для подписи с 7 сегментами вычисляется порядка 600 параметров (для одной функции), то для случая ввода подписи с одним временным интервалом (ввод подписи без отрывов пера) число параметров снизится до 15 (причем последние 10 являются производными от первых пяти, следовательно, несут в себе меньше информации о динамике подписи). В таком свете событий многократного увеличения числа параметров не происходит, рассчитывать на высокие значения вероятности идентификации не приходится. Еще один недостаток в данном способе - точность определения количества сегментов в подписи и их продолжительности, что является необходимым условием для корректного масштабирования реализации подписи к эталону. Алгоритм определения фрагментов подписи по отрыву пера подвержен ошибкам работы ввиду неоднозначного воспроизведения индивидуумами подписей (пользователи по-разному совершают отрывы пера при разных попытках ввода подписи). Получаемые значения параметров для неправильно найденных фрагментов будут значительно отличаться от эталонных. Несмотря на высокие вероятностные характеристики последнего метода, все рассмотренные выше способы обладают одним существенным недостатком. Недостаток проявляется в том, что при расширении базы данных биометрических эталонов, т.е. при обучении биометрической системы распознавать новых пользователей и достижении некоторого критического числа зарегистрированных пользователей в системе, резко падает вероятность того, что на выходе решающего правила окажется верный результат распознавания. Это происходит из-за особенности работы метода распознавания в режиме идентификации, когда вероятность ложного распознавания (ошибка второго рода) увеличивается пропорционально количеству человек в базе данных системы при той же чувствительности (ошибке первого рода). Причина отмеченного явления заключается в размытии «собственной области» объекта в пространстве признаков, получение высоких значений вероятностей правильной идентификации из представленного списка лиц не представляется возможным. Режим идентификации имеет ряд преимуществ перед верификацией - он удобнее в использовании (от пользователя не требуется ввода идентификатора) и характеризуется меньшим временем прохода. Если число сотрудников больше критического значения, использование биометрических методов в режиме идентификации становится ненадежным.

Задачей изобретения является разработка системы и способа идентификации пользователя ЭВМ по особенностям динамики воспроизведения рукописных паролей, обеспечивающих надежную и удобную идентификацию человека на уровне прототипа при увеличенном количестве зарегистрированных пользователей в базе данных в несколько раз по сравнению с аналогами.

Поставленная задача достигается тем, что в системе идентификации пользователей ЭВМ, содержащей носитель информации и устройство считывания информации, включающее первый модуль, выполненный в виде корпуса и пишущего элемента, и второй модуль, содержащий сенсорное устройство и контроллер, согласно изобретению во второй модуль, выполненный герметизированным на печатной плате, дополнительно введен процессор обработки, включающий аналого-цифровой преобразователь, блок повышения качества входных данных, блок интегральных преобразований, блок математических ожиданий, дисперсии, блок коэффициентов корреляции, блок временного интервала, блок эталона, блок принятия решения, и USB интерфейс, сенсорное устройство выполнено в виде акселерометра, причем выход

акселерометра соединен со входом процессора обработки, выход которого соединен со входом контроллера, выход которого соединен с USB интерфейсом и далее USB портом с ЭВМ, фиксирующим информацию, при этом питание акселерометра, процессора обработки и процессора осуществляется от ЭВМ через USB порт. Второй модуль устройства считывания может быть выполнен в резиновом корпусе, размещенном в виде насадки на корпусе первого модуля либо размещенном внутри корпуса первого модуля и расположенном последовательно за пишущим элементом. Первый модель может быть выполнен в виде ручки либо в виде карандаша с полым корпусом.

Поставленная задача достигается также тем, что в способе идентификации пользователей ЭВМ, заключающемся во введении оцифрованных данных о динамических параметрах колебаний пера при воспроизведении подписи в процессор обработки, определении начала и конца фрагментов введенной подписи, масштабировании каждого фрагмента подписи, определении параметров масштабированных фрагментов, принятии решения по идентификации личности, согласно изобретению масштабированию подвергают один пример подписи (пароля) относительно рассматриваемого эталона, в блоке интегральных преобразований осуществляют вычисление интегралов Фурье для преобразованных функций, одновременно вычисляя продолжительность нормированных сигналов, в качестве параметров используют плотности вероятностей найденных коэффициентов корреляции, в блоке вычисления математических моментов производят оценку информативности каждого параметра, далее в блоке интегральных преобразований, блоке вычисления временного интервала и блоке вычисления коэффициентов корреляции вычисляют контролируемые параметры по одной реализации подписи, при этом решение принимают на последнем шаге процесса идентификации параметров с порогом параметров принятия решения, а при отсутствии параметров с финальной вероятностью выше установленного порога формируют сообщение о необходимости повторного ввода подписи.

Технический результат достигается тем, что в системе используется сенсорное устройство в виде пьезоэлектрического акселерометра и процессор обработки, включающий аналого-цифровой преобразователь, блок повышения качества входных данных, блок интегральных параметров, блок математических ожиданий, дисперсии, блок коэффициентов корреляции, блок временного интервала, блок эталона, блок принятия решения и позволяющий использовать дополнительную систему признаков, применять процедуры повышения качества биометрических данных, кроме того, идентификацию пользователя проводить по усовершенствованному алгоритму распознавания, полученному в результате развития классической стратегии Байеса, в котором предусмотрена обработка исключительных случаев.

Предлагаемый способ основан на том, что для прохождения процедуры идентификации подписант воспроизводит специальной ручкой либо карандашом рукописное слово-пароль. Параллельно с этим происходит преобразование в цифровую форму колебания пера на плоскости, давление, оказываемое кончиком пера на плоскость, изменения наклона пера к плоскости, а также вращения пера относительно своей вертикальной оси с последующим определением начала и конца подписи идентифицируемой личности, выполняется масштабирование подписи через нахождение коэффициентов корреляции выходных сигналов о движениях пера. В качестве параметров идентифицируемого лица используют плотности вероятностей найденных коэффициентов корреляции, определяют моменты отрыва пера,

обрабатывают подпись, удаляя из траекторий поступивших от сенсорного устройства сигналов фрагменты, соответствующие участкам отрыва пера от поверхности (или интервалам нулевого давления), найденные участки траектории подписи последовательно соединяют между собой для получения непрерывных траекторий сигналов по времени, выполняют другой вариант масштабирования каждой функции этой подписи, вычисляют интегральные параметры по полным реализациям упомянутых функций, временной интервал воспроизведения пароля, принимают идентификационное решение сравнением вычисленных упомянутых параметров с их эталонными значениями, используя вероятностный метод распознавания, основанный на усовершенствованной стратегии распознавания Байеса, полученные на последнем шаге вероятности гипотез сравнивают с порогом распознавания, а при отсутствии гипотезы с финальной вероятностью выше установленного порога формируется сообщение на экране монитора о необходимости повторного ввода подписи.

Сущность изобретения заключается в том, что пользователь предъявляет на вход распознающего устройства образец подписи (пароля), одновременно в вычислителе происходит регистрация колебаний пера по времени X(t), Y(t), P(t), T(t), R(t). При этом возможны следующие виды трансформации траектории сигнала (по сравнению с другими попытками ввода подписи идентифицируемой личностью): пропуск участка отрыва пера от поверхности графического планшета, вставка участка, либо изменение его продолжительности. Отличительной особенностью предложенного способа является операция масштабирования подписи через нахождение коэффициентов корреляции выходных сигналов о движениях пера и использование в качестве основной системы параметров идентифицируемого лица плотностей вероятностей найденных коэффициентов корреляции. Упомянутые коэффициенты корреляции между выходными функциями движений пера и их производными дают оценки похожести формы измеряемых кривых, а стабильность этих оценок обеспечивается тем, что формы функций имеют подобный вид для реализации пароля подписанта. Установлено, что наряду с признаками, несущими информацию о динамике движения пера в каждом из измерений, коэффициенты корреляции являются информативными признаками и позволяют оценивать динамику формируемых кривых в совокупности, то, каким образом изменения одной функции приводят к изменениям в остальных. Эти признаки индивидуальны для пользователей и остаются стабильными на протяжении долгого времени.

Второй отличительной особенностью предложенного способа является использование процедуры повышения качества входных данных, согласно которой устраняют различия между реализациями подписи в траекториях сигналов с последующим их масштабированием. С целью устранения неоднозначностей при воспроизведении подписи, выполняют предварительную обработку, удаляя из траекторий поступивших от сенсорного устройства сигналов фрагменты, соответствующие участкам отрыва пера от поверхности, траектории измеряемых функций в эти моменты времени характеризуются широкой вариативностью, и динамика изменения функций носит неопределенный (случайный) характер. После применения к сигналам упомянутой процедуры найденные участки траектории подписи последовательно соединяют между собой («склеивают») для получения непрерывных траекторий сигналов по времени. На основе полученных функций строится расширенное пространство признаков.

Координаты x и y, определяющие положение пера на плоскости, изменяются во времени в пределах $x \in 0; x_{max}$, $y \in 0; y_{max}$, где x_{max} и y_{max} - количество разрешаемых

пикселей по соответствующим осям планшета. Далее от функций X(t), Y(t) переходят к функциям мгновенной скорости по оси x и оси y соответственно, используя соотношения:

$$\upsilon_{xi} = \frac{x_{i+1} - x_i}{\Delta t}; \upsilon_{yi} = \frac{y_{i+1} - y_i}{\Delta t},$$

где x_i, y_i - координаты пера в момент времени $i\Delta t$; $i=0, 1, 2, \ldots, T_n/\Delta t$; T_n - время, затрачиваемое на подпись; Δt - период взятия отсчетов. Последние две характеристики необходимы для защиты от попытки обвода полученного злоумышленником экземпляра парольного слова, написанного автором. Измеряемые величины: давление кончика пера на чувствительную к нажатию поверхность планшета P(t), угол наклона T(t) и вращение пера R(t), используются в абсолютном виде без вычисления мгновенной скорости на отрезках дискретизации. Решение объясняется тем, что вероятный злоумышленник, наблюдая за процессом написания парольного слова автором, не сможет фиксировать моменты изменения давления, угла наклона и поворота пера. При попытке обвода подписи нарушителем включается механизм зрительной корректировки, происходит существенное падение скорости выполнения действий, то же справедливо и для признаков, описанных ранее (функции мгновенной скорости по оси OX и оси OY). Нарушитель субъективно не ощущает падения собственной скорости в режиме обвода оригинала. Перейти в режим подсознательного воспроизведения нарушитель просто физически не может без длительной процедуры обучения.

Динамика написания заученного слова обладает определенной изменчивостью. Даже два раза подряд невозможно одинаково с точностью до пикселя и миллисекунды написать пароль. Возникают отклонения по траектории колебания пера, продолжительности и скорости написания рукописного слова. Введенные K рукописных пароля (в разное время) отличаются длительностью написания и характером кривой. К отличительной части предложенного способа относится процедура нейтрализации амплитудно-временных различий кривых. Во время ввода рукописного слова активируются пиксели, соответствующие текущему положению светового пера на планшете, и одновременно заполняются пять массивов: координата x активированного пикселя, координата y активированного пикселя, давление кончика пера на поверхность планшета в точке активированного пикселя, угол наклона пера к плоскости графического планшета в точке активированного пикселя, вращение пера относительно своей вертикальной оси в точке активированного пикселя.

Для устранения амплитудно-временных различий кривых выполняют прямое разложение функций в ряд Фурье, одновременно вычисляют амплитуду и частоту для первых G гармоник. На следующем шаге частоты гармоник масштабируемой функции заменяют частотами соответствующих гармоник, полученных для функции, к которой производится масштабирование, выполняют нормирование по амплитуде спектра масштабируемой функции путем деления квадрата амплитуды каждой гармоники на энергию исходного сигнала. Далее выполняют обратное преобразование Фурье для G гармоник с измененными характеристиками. Для дискретного случая энергия рассчитывается по формуле:

$$E_s = \sum_{i=1}^{N} A_i^2,$$

где N - количество отсчетов в сигнале, A_i - амплитуда сигнала на i-м отсчете.

На следующем этапе вычисляют интегральные характеристики для масштабированных сигналов в форме линейных функционалов Фурье, определяя амплитуды первых G гармонических составляющих. При этом находят (N-m-1) интегральных параметров, которые вместе с m измеренными коэффициентами корреляции между упомянутыми функциями и их производными и нормированным в результате исключения провалов давления пера временем воспроизведения пароля образуют N анализируемых далее данных V, где V - вектор признаков или набор параметров исходного сигнала, отражающих свойство объекта, важное для распознавания. Для принятия решения об отнесении заявляемой подписи к одному из зарегистрированных эталонов применяется вероятностный метод распознавания с критерием риска принятия решения Байеса. При этом, если выбранная мера близости данного объекта (представленного в виде вектора признаков V) и некоторого класса (представленного в виде эталонного описания) превышает меру близости этого объекта со всеми остальными классами и превышает некоторое заранее заданное число P, то принимается решение о принадлежности неизвестного объекта к данному классу. Если мера близости не превышает пороговое значение P ни для какого класса, то принимается решение о том, что в базе данных системы распознавания не существует класса, к которому принадлежит распознаваемый объект, т.е. принимается решение «Чужой», а на экран монитора выводится сообщение о необходимости повторного ввода подписи (пароля). Для сохранения надежности идентификации на уровне прототипа при увеличении количества распознаваемых пользователей в несколько раз алгоритм принятия решения дополнен операцией, описание которой приводится ниже.

Отличительная особенность предложенного способа заключается в нахождении наиболее вероятной гипотезы на этапе идентификации личности с помощью модифицированной формулы гипотез Байеса (1). Суть модификации заключается в использовании способа связывания промежуточных оценок параметров и их корректировании. На очередном шаге расчета вероятностей байесовых гипотез априорными вероятностями гипотез считаются вероятности гипотез, вычисленные на предыдущем шаге. После получения финальных вероятностей производится их корректировка по формуле (2).

$$P_j(H_i|A) = \frac{P_{j-1}(H_i|A) \times P(A|H_i)}{\sum_{j=1}^{n} P_{j-1}(H_i|A) \times P(A|H_i)} \quad (1)$$

Решение принимается на последнем шаге в пользу той гипотезы, финальная вероятность которой превысила установленный порог принятия решения. Условные вероятности на шаге A для каждой гипотезы определяются по нормальному закону распределения:

$$P(A|H_i) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-M)^2}{2\sigma^2}},$$

где M и σ - математическое ожидание и среднее квадратичное отклонение очередного проверяемого признака i-го эталона.

Изменения стандартного алгоритма продиктованы выявленными в нем недостатками. При использовании в задачах идентификации биометрических образов классической формулы Байеса возможны сбои, которые способны привести к ошибке принятия решения (ошибке распознавания). Часто на очередном шаге работы

стратегии Байеса вероятность некоторой гипотезы становится близкой по значению к единице, а вероятности оставшихся гипотез в сумме дают околонулевое значение, несмотря на то что на предыдущем шаге одна из этих гипотез имела высокую вероятность и являлась правильным решением. С целью ослабления влияния некачественных биометрических признаков на интегральный результат идентификации, стандартный алгоритм дополнен блоком корректировки финальных вероятностей гипотез, реализующим ограничение приращения вероятностей гипотез на промежуточных шагах идентификации путем их умножения на корректирующий множитель 1/n с последующим суммированием вероятностей каждой гипотезы в отдельности по формуле (2). Величина 1/n определяется тем, что вероятность гипотезы может изменяться в пределах от 0 до 1, n - количество используемых для идентификации параметров. Таким образом, за один шаг идентификации вероятность не может измениться более чем на 1/n.

$$P_j(H_i|A) = P_{j-1}(H_i|A) + \frac{1}{n} * (P_j(H_i|A) - P_{j-1}(H_i|A)), \quad (2)$$

где n - количество используемых для идентификации параметров.

На фиг.1 представлена предложенная система идентификации пользователей ЭВМ. Система содержит объект носитель информации (не показан) и устройство считывания информации, включающее первый модуль 1, выполненный в виде корпуса 2 и пишущего элемента 3, и второй модуль 4, содержащий сенсорное устройство 5 и контроллер 6. На фиг.2 представлен второй модуль 4, выполненный герметизированным на печатной плате, процессор обработки 7, включающий аналого-цифровой преобразователь 8, блок повышения качества входных данных 9, блок интегральных преобразований 10, блок вычисления математических ожиданий и дисперсии 11, блок вычисления коэффициентов корреляции 12, блок вычисления временных интервалов 13, блок эталонов 14, блок принятия решения 15, и USB интерфейс 16. На фиг.3 представлен вариант, в котором второй модуль 4, выполненный в резиновом корпусе, размещен в виде насадки на корпусе первого модуля 1.

Система идентификации пользователей ЭВМ для выполнения предложенного способа имеет объект носитель информации (не показан) и устройство считывания информации, включающее первый модуль 1, выполненный в виде корпуса 2 и пишущего элемента 3, и второй модуль 4, содержащий сенсорное устройство 5, в качестве которого используется пьезоэлектрический интегральный трехосевой акселерометр ADXL, выходы которого соединены с процессором обработки 7 и соответственно со входами аналого-цифрового преобразователя 8, выход которого параллельно соединен со входами блока повышения качества входных биометрических данных 9, в котором совмещены процедуры обработки траекторий регистрируемых сигналов и их масштабирования и блока вычисления коэффициентов корреляций 12. Выход блока 9 параллельно соединен со входами блока интегральных преобразований 10, блока вычисления временных интервалов 13. В свою очередь выход блока интегральных преобразований 10 соединен со входом блока вычисления математических ожиданий и дисперсий 11. Выход блока вычисления математических ожиданий и дисперсий 11 соединен со входом блока эталонов 14. Выход блока вычисления коэффициентов корреляций 12 соединен со входом блока вычисления математических ожиданий и дисперсий 11. Выход блока временного интервала 13 соединен со входом блока вычисления математических ожиданий и дисперсий 11. Выход блока эталонов 14 соединен со входом блока принятия решения 15. Кроме

того, выход блока интегральных преобразований 10 подключен ко входу блока принятия решения 15.

В общем случае при реализации предложенных системы и способа система с блок-схемой фиг.1 работает следующим образом. Пользователь воспроизводит слово пароль устройством считывания информации. При этом устройство считывания информации с помощью сенсорного устройства 5 преобразует колебания пера в электрические сигналы Y(t), X(t), P(t), T(t), R(t), которые преобразуются в цифровую форму аналого-цифровым преобразователем 8. В блоке 12 вычисляются коэффициенты корреляции между функциями и их производными. В блоке повышения качества входных данных 9 траектории сигналов подвергаются обработке, исключающей из подписи неинформативные участки. Фиг.4 демонстрирует результат обработки траекторий измеряемых сигналов X(t), Y(t), P(t) на примере двух реализаций 4а, 4б одной подписи. На вертикальной оси графика фиг.4 отложены отсчеты положения пера в координатах, на горизонтальной оси отложены соответствующие отсчеты времени. На верхней координатной плоскости графика изображен вид траекторий функций после применения предложенной процедуры обработки сигналов, на нижней координатной плоскости - исходный вид траекторий сигналов. Алгоритм работы процедуры масштабирования в блоке 9 зависит от режима, в котором находится устройство: в режиме обучения биометрической системы масштабированию подвергаются n реализаций подписи (слова), поступивших на вход от пользователя, кривые колебания пера приводятся к единому масштабу амплитуд и времени. На фиг.5,а приведены кривые скорости изменения колебания пера по оси OX и оси OY при воспроизведении пароля. На вертикальной оси графика фиг.5 отложены отсчеты скорости изменения положения пера в пиксель/сек, на горизонтальной оси отложены соответствующие отсчеты времени. На фиг.5,б представлен результат масштабирования функций скорости изменения положения пера по оси OX и оси OY (фиг.5а) соответственно по предложенному выше способу. При переходе устройства в режим идентификации в блоке 9 масштабированию подвергается один пример подписи (пароля) введенного рукописного слова относительно рассматриваемого эталона перед его проверкой решающим правилом. Далее преобразованные функции поступают в блок интегральных преобразований 10, который осуществляет вычисление интегралов Фурье для полных реализаций рассматриваемых функций, учитываются амплитуды и фазы первых 6 гармонических составляющих. Одновременно вычисляют продолжительность нормированных сигналов. При обучении устройства полученные данные после преобразования блоками 5, 8, 9, 10, 12, 13 усредняются блоком вычисления математических ожиданий и дисперсий 11, производится оценка информативности каждого параметра, собранные таким образом данные о пользователе запоминаются в блоке эталонов 14.

После обучения, в режиме идентификации личности рассматриваемое устройство работает аналогично, с той лишь разницей, что блок 11 не работает, а блоки 10, 12, 13 вычисляют контролируемые параметры по одной реализации подписи. Кроме того, работает блок принятия решения 15, вычисляющий меру близости поступивших данных к эталонным по формулам (1, 2). Решение "Свой" принимается на последнем шаге процесса идентификации при сравнении финальных вероятностей гипотез с порогом принятия решения, при отсутствии гипотезы с финальной вероятностью выше установленного порога принимается решение "Чужой" и формируется сообщение на экране монитора о необходимости повторного ввода подписи.

Системы идентификации по известным причинам уступают верификационным по

количеству возможных зарегистрированных пользователей. Без данного ограничения невозможно сохранять приемлемый уровень ошибок первого и второго рода. Предложенная модификация формулы Байеса имеет двойственный характер и сочетает в себе свойства идентификационной и верификационной процедур, что позволяет снизить указанное ограничение в несколько раз. С одной стороны, упомянутое решение предусматривает оценку степени совпадения подписи идентифицируемой личности с каждым из эталонов в базе, с другой стороны, получение суммарной величины откорректированных промежуточных вероятностей и принятие идентификационного решения относительно гипотезы, получившей на последнем шаге идентификации наибольшую вероятность путем ее сравнения с порогом распознавания.

В частном случае реализация предлагаемого способа может выглядеть следующим образом, проиллюстрированным на фиг.6. Каждому пользователю на предприятии, имеющему доступ к защищаемым информационным ресурсам, ставится в соответствие уникальный код, хранящийся в памяти микросхемы указателя, такое решение позволяет проводить двухфакторную аутентификацию пользователя и снижает процессорное время, затрачиваемое на исполнение алгоритма идентификации в блоке 15. Пользователь, перемещаясь вдоль контролируемой зоны на предприятии, может получить доступ к защищаемым информационным ресурсам только после воспроизведения рукописного пароля с помощью устройства считывания информации.

Использование новой операции в блоке принятия решения 15 позволяет увеличить количество эталонов зарегистрированных пользователей с сохранением надежности идентификации на уровне прототипа. Сохранение вероятных характеристик идентификации личности на заданном уровне по предложенному способу обусловлено несколькими причинами.

1. В сравнении с прототипом используется процедура повышения качества входных данных, исключающая из предъявленных реализаций подписи неинформативные участки. На втором этапе выполняют масштабирование обработанных функций по времени и нормирование по амплитуде. Результатом применения процедуры является повышение стабильности контролируемых параметров.

2. В сравнении с прототипом для поиска наиболее вероятной гипотезы используется модифицированная формула Байеса, в которой априорными вероятностями гипотез на очередном шаге идентификации считаются вероятности гипотез, вычисленные на предыдущем шаге. Такое решение позволяет интегрально оценить контролируемые параметры для всех гипотез. Приращение вероятности идентификации на очередном шаге ограничивается, что защищает от ошибок принятия решения, связанных с плохим качеством контролируемых параметров.

3. В сравнении с прототипом используется новый подход к формированию системы параметров, позволяющих оценить динамику совокупности движений подписанта при воспроизведении им подписи.

4. В сравнении с прототипом производится определение информативности каждого параметра перед его сохранением в базу данных, что позволяет в дальнейшем затрачивать минимум процессорного времени на вычисления по двум алгоритмам распознавания.

5. В сравнении с прототипом, использующим с целью повышения достоверности идентификации личности по особенностям почерка привлечение вторичных контролируемых параметров, получаемых из первичных параметров, увеличено количество основных параметров, обладающих большей значимостью, по сравнению

с вторичными.

Имеющиеся данные статистических испытаний позволяют оценить вероятности ошибок идентификации личности на уровне 0,005 при увеличении размера базы данных зарегистрированных пользователей в несколько раз.

Литература

1. Патент РФ №83152, G06K 7/10, опубл. 22.01.2009 г.

2. Патент РФ №2148274, G06K 9/22, G06K 9/62, G06F 15/18, опубл. 27.04.2000 г.

Формула изобретения

1. Система идентификации пользователей ЭВМ, содержащая носитель информации и устройство считывания информации, включающее первый модуль, выполненный в виде корпуса и пишущего элемента, и второй модуль, содержащий сенсорное устройство и контроллер, отличающаяся тем, что во второй модуль, выполненный герметизированным на печатной плате, дополнительно введен процессор обработки, включающий аналого-цифровой преобразователь, блок повышения качества входных данных, блок интегральных преобразований, блок математических ожиданий, дисперсии, блок коэффициентов корреляции, блок временного интервала, блок эталона, блок принятия решения, и USB-интерфейс, сенсорное устройство выполнено в виде акселерометра, причем выход акселерометра соединен со входом процессора обработки, выход которого соединен со входом контроллера, выход которого соединен с USB-интерфейсом и далее USB-портом с ЭВМ, фиксирующим информацию, при этом питание акселерометра, процессора обработки и процессора осуществляется от ЭВМ через USB-порт.

2. Система идентификации пользователей ЭВМ по п.1, отличающаяся тем, что второй модуль, выполненный в резиновом корпусе, размещен в виде насадки на корпусе первого модуля.

3. Система идентификации пользователей ЭВМ по п.1, отличающаяся тем, что второй модуль размещен внутри корпуса первого модуля и расположен последовательно за пишущим элементом.

4. Система идентификации пользователей ЭВМ по п.1, отличающаяся тем, что первый модуль выполнен в виде ручки.

5. Система идентификации пользователей ЭВМ по п.1, отличающаяся тем, что первый модуль выполнен в виде карандаша с полым корпусом.

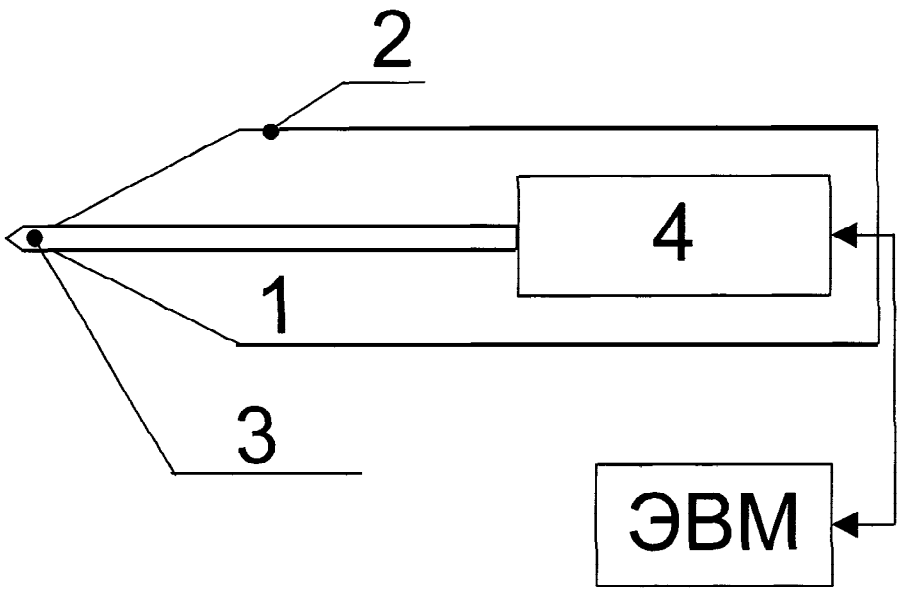
6. Система идентификации пользователей ЭВМ, содержащая носитель информации и устройство считывания информации, включающее первый модуль, выполненный в виде корпуса и пишущего элемента, и второй модуль, содержащий сенсорное устройство и контроллер, отличающаяся тем, что во второй модуль, выполненный герметизированным на печатной плате, дополнительно введен процессор обработки, включающий аналого-цифровой преобразователь, блок повышения качества входных данных, блок интегральных преобразований, блок математических ожиданий, дисперсии, блок коэффициентов корреляции, блок временного интервала, блок эталона, блок принятия решения, и радиомодуль, изготовленный по технологии Bluetooth, сенсорное устройство выполнено в виде акселерометра, причем выход акселерометра соединен со входом процессора обработки, выход которого соединен со входом контроллера, выход которого соединен с радиомодулем, при этом питание акселерометра, процессора обработки и контроллера осуществляется от источника питания, размещенного во втором модуле.

7. Система идентификации пользователей ЭВМ по п.6, отличающаяся тем, что

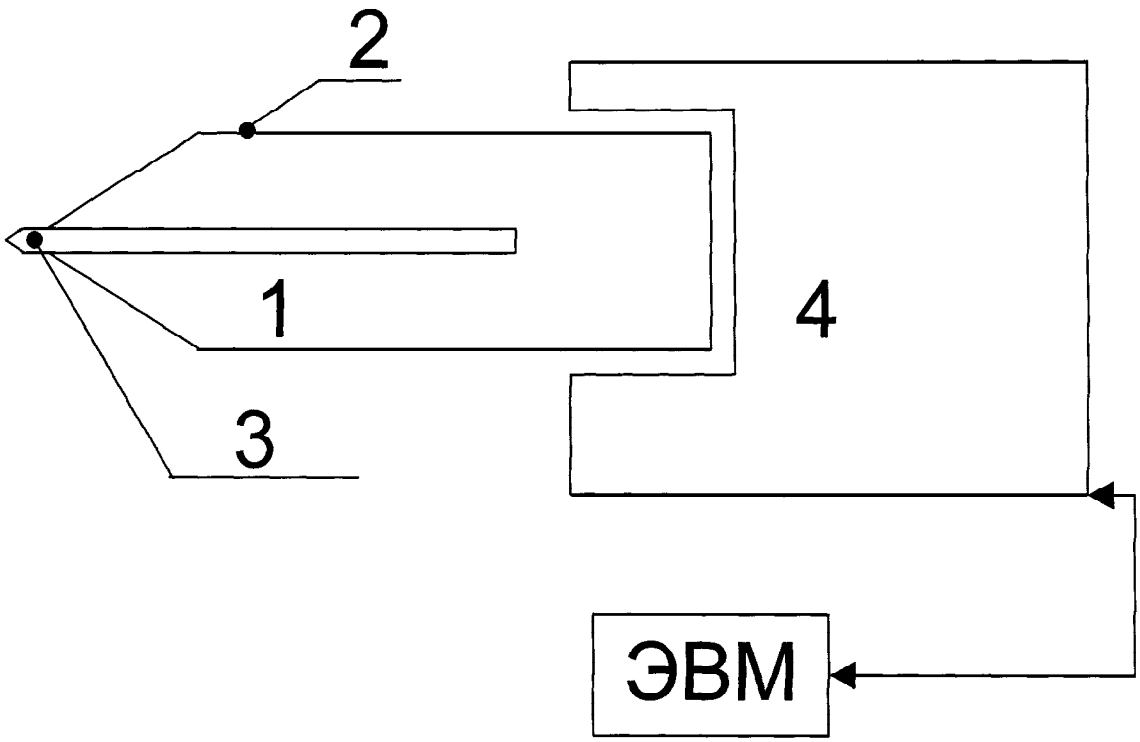
первый модуль выполнен в виде ручки.

8. Система идентификации пользователей ЭВМ по п.6, отличающаяся тем, что первый модуль выполнен в виде карандаша с полым корпусом.

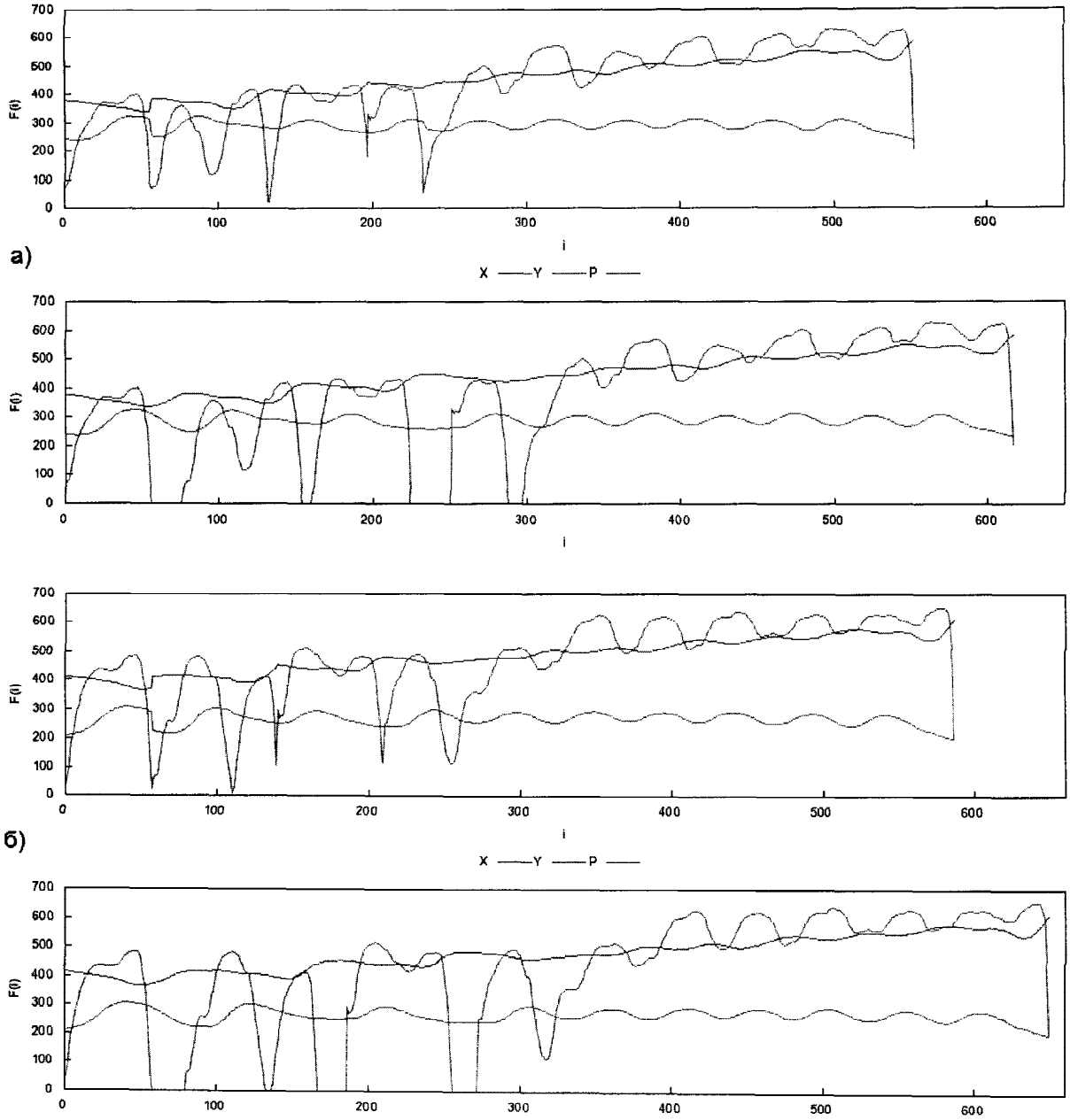
9. Способ идентификации пользователей ЭВМ, заключающийся во введении оцифрованных данных о динамических параметрах колебаний пера при воспроизведении подписи в процессор обработки, определении начала и конца фрагментов введенной подписи, масштабировании каждого фрагмента подписи, определении параметров масштабированных фрагментов, принятии решения по идентификации личности, отличающийся тем, что масштабированию подвергают один пример подписи (пароля) относительно рассматриваемого эталона, в блоке интегральных преобразований осуществляют вычисление интегралов Фурье для преобразованных функций, одновременно вычисляя продолжительность нормированных сигналов, в качестве параметров используют плотности вероятностей найденных коэффициентов корреляции, в блоке вычисления математических моментов производят оценку информативности каждого параметра, далее в блоке интегральных преобразований, блоке вычисления временного интервала и блоке вычисления коэффициентов корреляции вычисляют контролируемые параметры по одной реализации подписи, при этом решение принимают на последнем шаге процесса идентификации параметров с порогом параметров принятия решения, а при отсутствии параметров с финальной вероятностью выше установленного порога формируют сообщение о необходимости повторного ввода подписи.



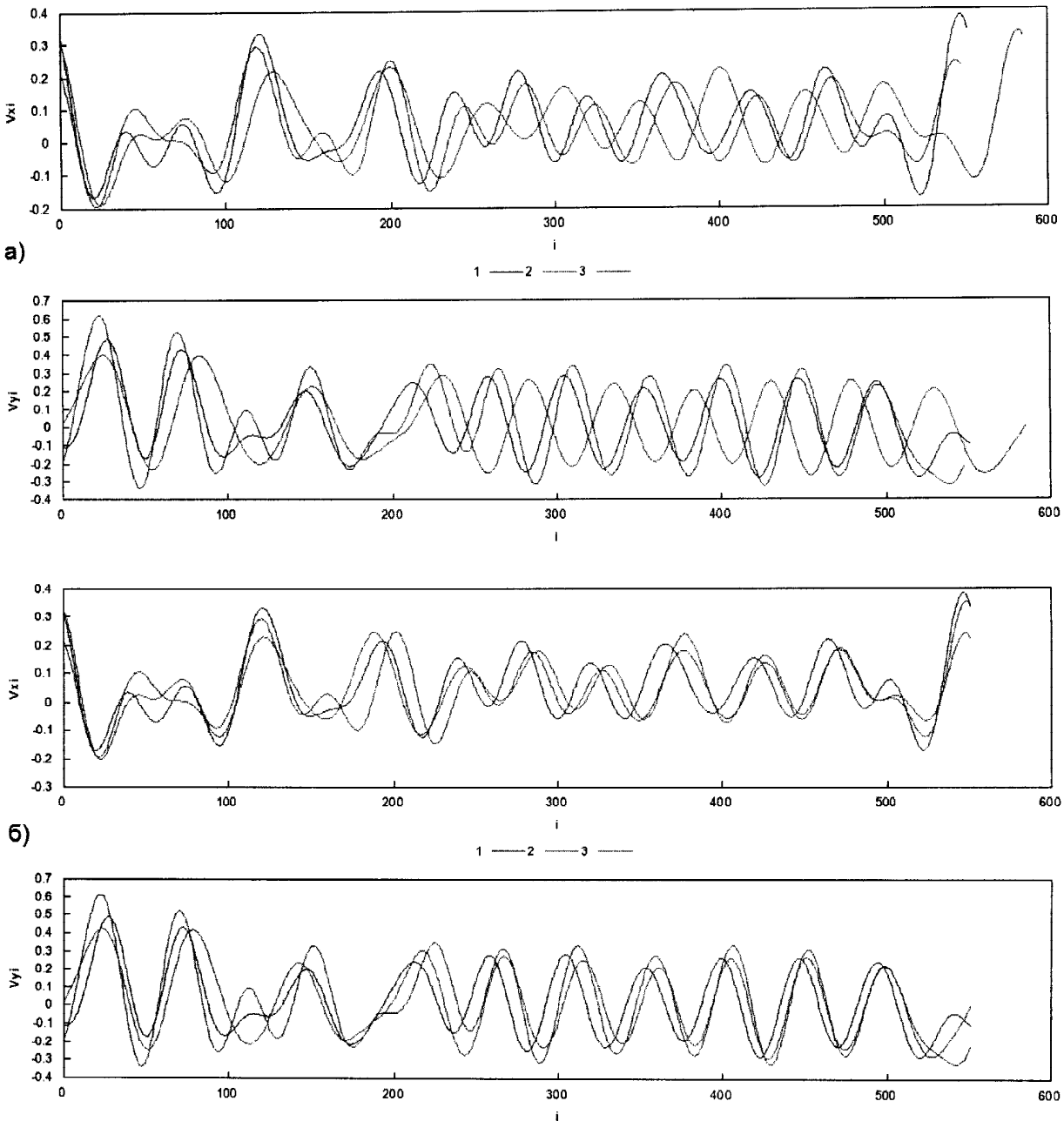
Фиг. 1



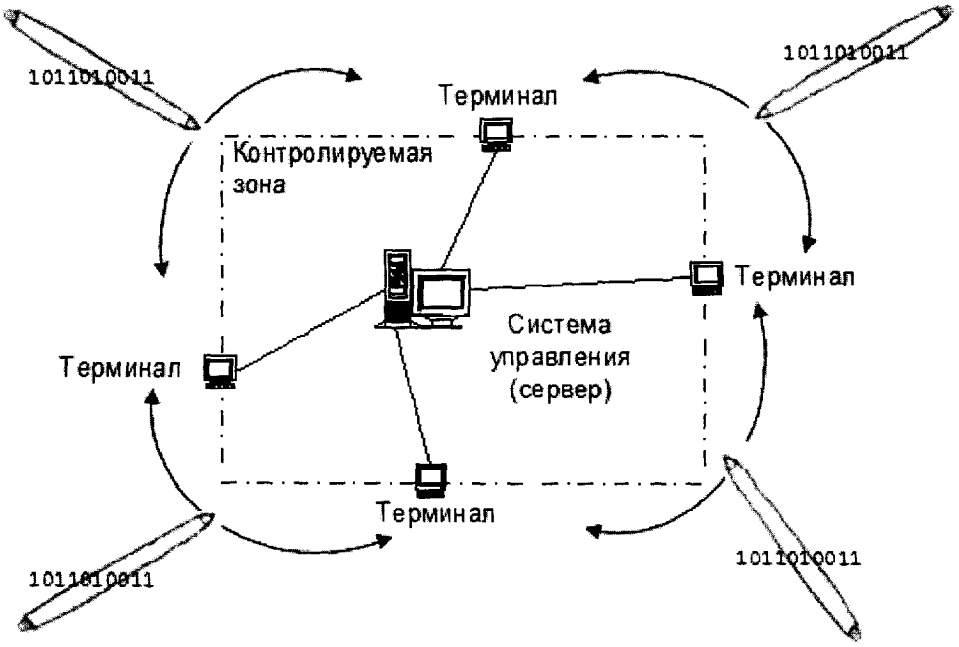
Фиг. 3



Фиг. 4



Фиг. 5


1011010011
1011010011
Терминал
Контролируемая зона
Терминал
Система управления (сервер)
Терминал
Терминал
1011010011
1011010011

Фиг. 6