(19) Евразийское патентное ведомство

(11) 042866 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.03.30

(21) Номер заявки
202290286

(22) Дата подачи заявки
2022.02.10

(51) Int. Cl. ***G06F 21/32*** (2006.01)
G06F 7/02 (2006.01)
G06V 40/00 (2006.01)

(54) СПОСОБ И СИСТЕМА АВТОМАТИЗИРОВАННОГО ОПРЕДЕЛЕНИЯ ПОРОГА ИДЕНТИФИКАЦИИ ДЛЯ БИОМЕТРИЧЕСКИХ ОБРАЗЦОВ В СИСТЕМЕ КОНТРОЛЯ ДОСТУПА

(31) **2021131450**
(32) **2021.10.27**
(33) **RU**
(43) **2023.03.24**

(71)(73) Заявитель и патентовладелец:
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" (ПАО СБЕРБАНК) (RU)

(72) Изобретатель:
Бабин Александр Павлович (RU)

(74) Представитель:
Герасин Б.В. (RU)

(56) US-B2-8190540
US-A1-20150146941
US-A1-20140157384
RU-C1-2742040
RU-C2-2286599

(57) Настоящее изобретение, в общем, относится к области вычислительной обработки данных, а в частности, к способам определения порога идентификации для биометрических образцов в системе контроля доступа. Техническим результатом, достигающимся при решении вышеуказанной технической проблемы, является повышение точности определения порога идентификации для биометрических образцов в системе контроля доступа. Компьютерно-реализуемый способ определения порога идентификации для биометрических образцов в системе контроля доступа, выполняемый с помощью по меньшей мере одного процессора и содержащий этапы, на которых: получают ретроспективные данные, отбирают данные идентификации образцов за выбранный период времени, определяют количество идентификаций n и количество зарегистрированных биометрических шаблонов N за выбранный период времени, определяют для данных идентификаций информацию о по меньше мере двух скоринговых баллах TOP-1 и TOP-2; формируют гистограмму, состоящую из m элементов ($T1_i$), формируют гистограмму, состоящую из m элементов ($T2_i$), определяют для каждой точки гистограмм сумму значений всех элементов гистограммы, начиная с текущего, определяют значение FAR_i (вероятность ложного допуска при аутентификации, на основе полученных значений FAR_i на предыдущем этапе, рассчитывают значение $FPIR_i$ (вероятность ложноположительной идентификации), определяют порог идентификации для биометрических образцов, и назначают полученный порог идентификации для по меньшей мере одного биометрического сенсора.

042866 B1

042866 B1

Область техники

Настоящее техническое решение, в общем, относится к области вычислительной обработки данных, а в частности, к способам определения порога идентификации для биометрических образцов в системе контроля доступа.

Уровень техники

В соответствии с ГОСТ Р ИСО/МЭК 19795-1-2007 Национального Стандарта Российской Федерации "Идентификация биометрическая" для определения ошибки второго рода биометрической верификации (FAR) при высоких скорбаллах (более 95% от максимума) лицевой биометрии с точностью +/-30% для доверительной вероятности 90% нужно по крайней мере 3e10 (30 событий для FAR 1e-9) независимых сравнений или 6e10 добровольцев. Этим же ГОСТ допускается альтернативный метод перекрестного сравнения, но данный метод не гарантирует статистическую независимость, что уменьшает доверительную вероятность для обеспечения требуемого уровня FAR по сравнению с тем же числом независимых испытаний. Но даже в этом случае для FAR 1e-9 потребуется более 245000 добровольцев (размеченных шаблонов, т.е. шаблонов принадлежавшим разным людям), а для FAR 1e-10 потребуется уже более 775000 размеченных шаблонов. Учитывая, что это персональные данные, их сложно получить для исследований. Усугубляет проблему и тот факт, что люди при идентификации используют различные устройства, поэтому для того, чтобы результат исследования был не только статистически значимым, но и соответствовал реальности, устройства для сбора образцов должны соответствовать реально применяющимся устройствам и их частоте использования.

Из уровня техники известен способ определения порога идентификации для биометрических образцов, раскрытый в патенте US 8190540 B2.

В данном способе для определения порога идентификации для биометрических образцов, используются образцы содержащие персональные данные пользователей, что снижает безопасность данного способа.

Недостатком существующих решений в данной области техники является низкая точность определения порога идентификации для биометрических образцов.

Сущность технического решения

Заявленное техническое решение предлагает новый подход в области определения порога идентификации для биометрических образцов в системе контроля доступа.

Решаемой технической проблемой или технической задачей является создание нового способа и системы определения порога идентификации для биометрических образцов в системе контроля доступа.

Основным техническим результатом, достигающимся при решении вышеуказанной технической проблемы, является повышение точности определения порога идентификации для биометрических образцов в системе контроля доступа.

Дополнительным техническим результатом, достигающимся при решении вышеуказанной технической проблемы, является повышение безопасности определения порога идентификации для биометрических образов в системе контроля доступа за счет использования логов с информацией о результатах реальных идентификаций не содержащих персональные данные пользователей.

Заявленные результаты достигаются за счет компьютерно-реализуемого способа автоматизированного определения порога идентификации для биометрических образцов в системе контроля доступа, выполняемый с помощью по меньшей мере одного процессора и содержащий этапы, на которых:

a) получают ретроспективные данные, содержащие сведения о результатах сравнения биометрических образцов, проходящих идентификацию, с зарегистрированными биометрическими шаблонами, при которых результат имеет наивысший скоринговый балл;

b) отбирают данные идентификации образцов за выбранный период времени, в ходе которого количество зарегистрированных биометрических шаблонов изменялось не более чем на 1% за выбранный период времени;

c) определяют количество идентификаций n и количество зарегистрированных биометрических шаблонов N за выбранный период времени;

d) определяют для данных идентификации, полученных на этапе b) информацию о поменьше мере двух скоринговых баллов TOP-1 и TOP-2, где TOP-1 максимальное значение скорингового балла идентификации, TOP-2 -следующее за TOP-1 значение скорингового балла, при этом значения TOP-1 и TOP-2 выше порога аутентификации;

e) формируют гистограмму, состоящую из m элементов ($T1_i$), распределения скорингового балла TOP-1 идентификаций на диапазоне от порога аутентификации до максимально возможного скорингового балла;

f) формируют гистограмму, состоящую из m элементов ($T2_i$), распределения скорингового балла TOP-2 идентификаций на диапазоне от порога аутентификации до максимально возможного скорингового балла;

g) определяют для каждой точки гистограмм сумму значений всех элементов гистограммы начиная с текущего, получая новые гистограммы из m элементов;

h) определяют значение FAR_i (вероятность ложного допуска при аутентификации) с помощью системы уравнений, используя данные, полученные на этапах c, g;

i) на основе полученных значений FAR_i на предыдущем этапе, рассчитывают значение $FPIR_i$ (вероятность ложноположительной идентификации) по формуле:

$$FPIR_i = 1 - (1 - far_i)^N$$

j) и на основе полученных значений $FPIR_i$ определяют порог идентификации для биометрических образцов, и

k) назначают полученный порог идентификации для по меньшей мере одного биометрического сенсора.

Также заявленные технические результаты достигаются за счет системы определения порога идентификации для биометрических образцов в системе контроля доступа, содержащая:

по меньшей мере один процессор;

по меньшей мере одну память, соединенную с процессором, которая содержит машиночитаемые инструкции, которые при их выполнении по меньшей мере одним процессором обеспечивает выполнение заявленного способа.

Описание чертежей

Признаки и преимущества настоящего изобретения станут очевидными из приводимого ниже подробного описания изобретения и прилагаемых чертежей, на которых:

фиг. 1 иллюстрирует общую схему заявленного способа;

фиг. 2 иллюстрирует пример общего вида вычислительной системы, которая обеспечивает реализацию заявленного решения.

Осуществление изобретения

На сегодняшний день биометрические системы уже привычны каждому и активно участвуют в нашей жизни. Сканеры отпечатков пальцев, встроенные в смартфоны, технологии распознавания лиц и прочие инструменты постепенно приходят на замену традиционным методам идентификации и все чаще проникают в крупные бизнесы, такие как банковское обслуживание и розничная торговля (ритейл). Биометрические системы имеют ряд преимуществ в сравнении с традиционными методами, так как приспособлены под идентификацию личности без возможности передачи ключа и во многом являются более удобными с точки зрения пользователя. Однако, чем более активно ведется внедрение такого вида систем, тем более остро встает вопрос обеспечения информационной безопасности.

Биометрическая идентификация - это процесс сравнения и определения сходства между данными человека и его биометрическим "шаблоном". Биометрия позволяет идентифицировать и провести верификацию человека на основе набора специфических и уникальных черт, присущих ему от рождения. Этот метод распознавания принято считать одним из самых надежных, так как в отличие от стандартных логина и пароля биометрическими данными гораздо сложнее несанкционированно воспользоваться.

Биометрическая идентификация может проводиться: по отпечатку пальца, по лицу, по радужной оболочке глаза, по геометрии рук, по термограмме лица, по ДНК, на основе акустических характеристик уха, по рисунку вен и т.д. не ограничиваясь. Распознавание отпечатков пальцев является одним из первых биометрических методов. Он основан на определении структуры линий на подушечках пальцев рук, иначе - папиллярных узоров. После считывания сканером уникальный рисунок трансформируется в цифровой биометрический шаблон, при помощи которого система определяет, кто перед ней находится.

Идентификация по рисунку вен на пальцах/руках является усовершенствованной версией предыдущего метода идентификации. Взломать алгоритм его работы значительно труднее, чем при другом биометрическом сканировании, поскольку вены находятся глубоко под кожей. Инфракрасные лучи проходят через поверхность кожи, где они поглощаются венозной кровью. Специальная камера фиксирует изображение, оцифровывает данные, а затем либо сохраняет их, либо использует для подтверждения личности.

Определение геометрии руки относится к измерению таких характеристик, как длина и ширина пальцев, их кривизна и относительное расположение. На данный момент этот метод является устаревшим и уже почти не используется, хотя когда-то был доминирующим вариантом биометрической идентификации. Современные достижения в области программного обеспечения для распознавания отпечатков пальцев и лиц затмили его актуальность. Существует также тип биометрических методов распознавания рисунка ладони, получивший название "дактилоскопия.

Идентификация по радужной оболочке. Радужная оболочка, или цветная часть глаза, состоит из толстых нитевидных мышц. Эти мышцы помогают формировать зрачок, чтобы контролировать количество света, попадающего в глаз. Измеряя уникальные складки и характеристики этих мышц, инструменты биометрической верификации могут подтвердить личность с невероятной точностью. Технологии динамического сканирования (например, сканирование того, как человек моргает) добавляют дополнительный уровень точности и безопасности.

Проверка сетчатки позволяет отсканировать капилляры глубоко внутри глаза с помощью камер ближнего инфракрасного диапазона. Получившееся изображение сначала предварительно обрабатывается для улучшения его качества, а затем преобразовывается в биометрический шаблон для регистрации

нового пользователя и для последующей сверки с эталоном во время попыток распознавания пользователя.

Технология распознавания лиц, безусловно, является одной из первых форм биометрических систем идентификации. Программное обеспечение такого рода измеряет геометрию лица, включая расстояние между глазами и от подбородка до лба (и это лишь некоторые из параметров). После сбора данных усовершенствованный алгоритм преобразует их в зашифрованный код, иначе - подпись (сигнатуру) лица. Идентификация по форме ушной раковины, в отличие от многих других биометрических методов, для которых требуются специальные камеры, данный вид идентификации измеряет акустику уха с помощью специальных наушников и неслышимых звуковых волн. Микрофон внутри каждого наушника измеряет то, каким образом звуковые волны отражаются от ушной раковины и расходятся в разных направлениях в зависимости от изгибов слухового прохода. Цифровая копия формы уха преобразуется в биометрический шаблон для дальнейшего использования. Технология распознавания голоса попадает в сферы и физиологических, и поведенческих биометрических данных. С физиологической точки зрения такие системы распознают форму голосового тракта человека, включая нос, рот и гортань, определяют производимый звук. С поведенческой точки зрения они фиксируют то, как человек что-то говорит - вариации движений, тон, темп, акцент и т.д., что также является уникальным для каждого человека.

Термограмма - это представление инфракрасной энергии в виде изображения распределения температуры. Биометрическая термография лица фиксирует тепловые узоры, вызванные движением крови под кожей. Поскольку кровеносные сосуды каждого человека неповторимы, соответствующие термограммы также уникальны даже среди однояйцевых близнецов, что делает этот метод биометрической верификации даже более точным, чем традиционное распознавание лиц.

ДНК издавна использовалась в качестве метода идентификации. Кроме того, это единственная форма биометрии, которая может отслеживать семейные связи. Сопоставление ДНК особенно ценно при работе с пропавшими без вести, выявлении жертв катастроф и потенциальной торговли людьми. Кроме того, помимо отпечатков пальцев, ДНК - единственный биометрический объект, который невозможно непреднамеренно "забыть". ДНК, собранная из волос, слюны и т.д., содержит последовательности коротких тандемных повторов (англ. short tandem repeat sequences, STR). С их помощью можно однозначно подтвердить личность, сравнивая их с другими STR в базе данных.

Вышеперечисленные методы идентификации содержат персональную информацию о пользователях, что осложняет доступ к таким данным для исследований. Усугубляет ситуацию и тот факт, что пользователи при идентификации используют различные устройства, поэтому для того, чтобы результат исследования был не только статистически значимым, но и соответствовал реальности, устройства для сбора образцов должны ответствовать реально применяющимся устройствам и их частоте использования.

Биометрическая информация, как и любая другая, уязвима. Банки, больницы и любые другие учреждения то и дело подвергаются хакерским атакам, и часть информации попадает в руки злоумышленников. Но одно дело, если это стандартные логин и пароль, а другое - если речь идет о биометрических данных. Ведь пароль можно сменить, а палец или радужку глаза - нет. В последнем случае при компрометации данных злоумышленник получает доступ ко всем активам с биометрической верификацией.

Заявленное техническое решение предлагает способ определения порога идентификации для биометрических образцов (ошибки второго рода биометрической верификации (FAR) и идентификации (FPIR) непосредственно на ПРОМ данных, используя не сами биометрические образцы, а логи с информацией о результатах реальных идентификаций.

Данные логи не содержат персональную информацию пользователей, что повышает безопасность определения порога идентификации для биометрических образов в системе контроля доступа.

В логах нет информации ни о FAR (false accept rate - ошибка второго рода при верификации для интересующего скорбалла), ни о FRR (false reject rate - ошибка первого рода при верификации для интересующего скорбалла), неизвестно и какое количество пользователей, которые проходили процесс идентификации, были зарегистрированы в системе. Но можно собрать статистику результатов идентификации для того или иного скорбалла (скоринговый балл - число, как правило от 0 до 1 (или от 0 до 100), которое характеризует степень похожести двух образцов. Где 0 - абсолютно не похож, 1 (или 100) - полное совпадение). При этом можно рассмотреть результаты идентификации как для лучшего кандидата (наиболее похожий шаблон среди зарегистрированных), так и для следующего кандидата, игнорируя лучшего.

Как показано на фиг. 1, заявленный способ определения порога идентификации для биометрических образцов в системе контроля доступа (100), содержит ряд последовательных этапов, выполняемых с помощью по меньшей мере одного процессора.

На этапе (101) получают ретроспективные данные, содержащие сведения о результатах сравнения биометрических образцов, проходящих идентификацию, с зарегистрированными биометрическими шаблонами, при которых результат имеет наивысший скоринговый балл.

На данном этапе выполняется обработка исторических данных о результатах идентификаций, например, получаемые из логов идентификации за заданный временной промежуток (день, неделя, месяц и т.п.). При каждой идентификации биометрический образец каждого человека, например, изображения

лица или сетчатки глаза, сравнивают со всеми биометрическими ранее зарегистрированными шаблонами. В результате этих сравнений получают значения скоринговых баллов, и максимальный из них или несколько максимальных (в данном случае используют два максимальных значения) являются результатом идентификации.

На этапе (102) выполняется отбор данных идентификации биометрических образцов за выбранный период времени, в ходе которого количество зарегистрированных биометрических шаблонов изменялось не более чем на 1% за выбранный период времени.

Осуществляется определение периода времени, за который исследуются ретроспективные данные по идентификациям, и выполняется их отбор (фильтрация) за выбранный период.

На этапе (103) осуществляется определение количества идентификаций n и количества зарегистрированных биометрических шаблонов N за выбранный период времени.

Для этого определяется количество идентификаций (n), выполненных за выбранный период, а также количество биометрических шаблонов (N), зарегистрированных в системе. Так как количество биометрических шаблонов за выбранный период могло меняться, то в качестве значения количества шаблонов (N) может приниматься среднее арифметическое количества шаблонов на начало и конец временного периода.

Например, n=25000, N=10,000,000.

На этапе (104) для данных идентификации полученных на этапе (102) определяют информацию о поменьше мере двух скоринговых баллов TOP-1 и TOP-2, где TOP-1 максимальное значение скорингового балла идентификации, TOP-2 - следующее за TOP-1 значение скорингового балла, при этом значения TOP-1 и TOP-2 выше порога аутентификации.

На данном этапе анализируется результат каждой идентификации, выбранной на этапе (102), впоследствии выполняется определение для каждой идентификации двух значений - максимальный скоринговый балл сравнения образца со всеми образцами, зарегистрированными в системе (TOP-1), и второй по величине результат сравнения (TOP-2).

Например, при идентификации были получены следующие скоринговые баллы: 98, 95, 93, 92... (записаны в порядке убывания). Для такой идентификации определяют только два значения: 98 и 95.

Важно отметить, что при формировании списка скорбаллов при идентификации может быть наложено условие на минимальное значение скорбалла. Эта граница (минимальное значение скорбалла, ниже которого результаты сравнения не принимаются во внимание) будет являться порогом аутентификации.

Например, если минимально интересующее значение скорбалла 80, а в результате идентификации были получены значения скорбаллов 83, 78, 77..., то в качестве результата идентификации определяется только значение 83. В качестве TOP-1 и TOP-2 такой идентификации определяют пару 83 и <80 (значение меньше 80). Если в результате идентификации все сравнения были ниже порога аутентификации, например, 75, 73, 70..., то определяется, что не было зафиксировано ни одного скорбалла выше требуемого порога и результатом такой идентификации является пустое множество. В качестве TOP-1 и TOP-2 такой идентификации определяют пару <80 и <80 (здесь 80 - порог аутентификации).

На этапе (105) выполняется формирование гистограммы, состоящей из m элементов ($T1_i$), распределения скорингового балла TOP-1 идентификаций на диапазоне от порога аутентификации до максимально возможного скорингового балла. На данном этапе весь диапазон скорбаллов от порога аутентификации до максимально возможного значения (точного совпадения двух образцов) делится на m частей (чем больше m, тем больше точек можно получить на графике). Например, диапазон от 80 до 100 можно поделить на 20 равных частей: 80-81, 81-82, ... 99-100. Определяется, какое количество значений TOP-1, полученных на этапе (104), попадает в каждый диапазон. Формируется гистограмма для значений TOP-1. Например,

<80	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99
7000	200	180	140	135	145	120	110	90	120	125	145	205	210	275	530	580	900	1540	3150	9100

На этапе (106) осуществляется формирование гистограммы, состоящей из m элементов ($T2_i$), распределения скорингового балла TOP-2 идентификаций на диапазоне от порога аутентификации до максимально возможного скорингового балла. На данном этапе для тех же диапазонов, полученных на этапе (105), выполняют аналогичные действия для скорбаллов TOP-2, и впоследствии формируется гистограмма для значений TOP-2. Например,

<80	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99
23000	440	350	270	240	190	160	105	80	55	35	23	20	13	8	5	4	2	0	0	0

На этапе (107) выполняется определение для каждой точки гистограмм сумм значений всех элементов гистограммы начиная с текущего, получая новые гистограммы из m элементов ($R1_i$ и $R2_i$)

$$R1_i = \sum_{j=i}^{m} T1_j$$

$$R2_i = \sum_{j=i}^{m} T2_j$$

На данном этапе для каждой точки гистограмм, полученных на этапах (105) и (106), выполняется расчет сумм значений на гистограмме, начиная с текущего до максимального скорбалла.

score	<80	80	81	82	83	84	85	86	87	88	89
R1	25000	18000	17800	17620	17480	17345	17200	17080	16970	16880	16760
R2	25000	2000	1560	1210	940	700	510	350	245	165	110

score	90	91	92	93	94	95	96	97	98	99
R1	16635	16490	16285	16075	15800	15270	14690	13790	12250	9100
R2	75	52	32	19	11	6	2	0	0	0

На этапе (108) рассчитывается значение FAR_i (вероятность ложного допуска при аутентификации) с помощью данных, полученных на этапах (103), (107), по следующей формуле:

$$\begin{cases} \begin{cases} 1-(1-far_i)^N - \frac{\left(1-\frac{R1_i}{n*q}\right)*N*far_i}{1-far_i} = \frac{R2_i}{n*q} \\ y_i = 1 - \frac{1-R1_i/(n*q)}{(1-far_i)^N} \end{cases} \\ y_i \geq 0 \\ q \to max \\ q \in [R1_1/n; 1] \\ y_1 \geq \max\limits_{1<i<m} y_i \end{cases}$$

На данном этапе для каждой пары значений двух рядов, полученных на этапе (107), находящихся на одинаковых позициях ($R1_i$ и $R2_i$) и для известного значения количества зарегистрированных шаблонов (N) и идентификаций за период (n), определяется значение FAR_i (вероятность ложного допуска при аутентификации), принимая q=1. Для приведенных выше данных получают:

score	80	81	82	83	84	85	86	87	88	89
FAR	1.21e-08	9.36e-09	7.23e-09	5.60e-09	4.16e-09	3.03e-09	2.08e-09	1.46e-09	9.85e-10	6.60e-10
y	0.6840	0.6837	0.6827	0.6819	0.6808	0.6784	0.6765	0.6741	0.6720	0.6682

score	90	91	92	93	94	95	96	97	98	99
FAR	4.52e-10	3.16e-10	1.97e-10	1.18e-10	6.97e-11	3.93e-11	1.36e-11	0	0	0
y	0.6639	0.6585	0.6507	0.6426	0.6317	0.6106	0.5875	0.5516	0.49	0.364

Как видно из таблицы, значение "y" для скорбалла 80 имеет максимальное значение, т.е. выполняется условие выхода из цикла поиска решения.

$$y_1 \geq \max_{1<i<m} y_i.$$

Если это условие не выполняется, то значение q уменьшается на 0.01 и вычисления этапа (108) повторяют с новым значением q.

На этапе (109) на основе полученных значений FAR_i на предыдущем этапе (108), рассчитывают значение $FPIR_i$ (вероятность ложноположительной идентификации) по формуле

$$FPIR_i = 1 - (1 - far_i)^{N^*}$$

На данном этапе рассчитывают значение $FPIR_i$ по приведенной выше формуле. Здесь N* - количество зарегистрированных шаблонов в системе, для которой требуется установить порог идентификации.

В качестве примера рассчитаем FPIR для 10 миллионов зарегистрированных биометрических шаблонов.

score	80	81	82	83	84	85	86	87	88	89
FPIR	0.1138	0.0894	0.0697	0.0544	0.0407	0.0299	0.0206	0.0145	0.0098	0.0066

score	90	91	92	93	94	95	96	97	98	99
FPIR	0.0045	0.0032	0.0020	0.0012	0.000696	0.000393	0.000136	0.0	0.0	0.0

На этапе (110) на основе полученных значений $FPIR_i$ определяется порог идентификации для биометрических образцов.

На данном этапе имея в качестве настраиваемого параметра значение FPIR, и получив таблицу, построенную на этапе (109), выполняется определение значения скорбалла, которое следует установить в качестве порога идентификации для интересующего количества зарегистрированных шаблонов. Для этого по требуемому значению FPIR устанавливается соответствующее ему значение скорбалла. Например, если требуемое значение FPIR равно 0.0005, то в качестве порога идентификации устанавливается скорбалл 94.65.

Если требуемое значение FPIR больше максимального значения FPIR в таблице, то в качестве порога идентификации используют порог аутентификации (в данном примере 80).

На этапе (111) полученный порог идентификации назначается для по меньшей мере одного биометрического сенсора. Это позволяет контролировать ошибку FPIR реально работающей системы на заданном уровне. Например, если где-то изменились условия или оборудование идентификации или изменилась нейросеть распознавания, то описанный выше подход может позволить системе идентификации оперативно отреагировать на произошедшие изменения, и не допустить неконтролируемого роста ошибки FPIR (доли ложных допусков незарегистрированных в системе пользователей). На фиг. 2 представлен пример общего вида вычислительной системы (300), которая обеспечивает реализацию заявленного способа или является частью компьютерной системы, например, сервером, персональным компьютером, частью вычислительного кластера, обрабатывающим необходимые данные для осуществления заявленного технического решения.

В общем случае, система (300) содержит объединенные общей шиной информационного обмена один или несколько процессоров (301), средства памяти, такие как ОЗУ (302) и ПЗУ (303), интерфейсы ввода/вывода (304), устройства ввода/вывода (1105), и устройство для сетевого взаимодействия (306).

Процессор (301) (или несколько процессоров, многоядерный процессор и т.п.) может выбираться из ассортимента устройств, широко применяемых в настоящее время, например, таких производителей, как: Intel™, AMD™, Apple™, Samsung Exynos™, MediaTEK™, Qualcomm Snapdragon™ и т.п. Под процессором или одним из используемых процессоров в системе (300) также необходимо учитывать графический процессор, например, GPU NVIDIA или Graphcore, тип которых также является пригодным для полного или частичного выполнения способа, а также может применяться для обучения и применения моделей машинного обучения в различных информационных системах.

ОЗУ (302) представляет собой оперативную память и предназначено для хранения исполняемых процессором (301) машиночитаемых инструкций для выполнение необходимых операций по логической обработке данных. ОЗУ (302), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.). При этом в качестве ОЗУ (302) может выступать доступный объем памяти графической карты или графического процессора.

ПЗУ (303) представляет собой одно или более устройств постоянного хранения данных, например, жесткий диск (HDD), твердотельный накопитель данных (SSD), флэш-память (EEPROM, NAND и т.п.), оптические носители информации (CD-R/RW, DVD-R/RW, BlueRay Disc, MD) и др.

Для организации работы компонентов системы (300) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (304). Выбор соответствующих интерфейсов зависит от конкретного исполнения вычислительного устройства, которые могут представлять собой, не ограничиваясь: PCI, AGP, PS/2, IrDa, FireWire, LPT, COM, SATA, IDE, Lightning, USB (2.0, 3.0, 3.1, micro, mini, type C), TRS/Audio jack (2.5, 3.5, 6.35), HDMI, DVI, VGA, Display Port, RJ45, RS232 и т.п. Для обеспечения взаимодействия пользователя с вычислительной системой (300) применяются различные средства (305) В/В информации, например, клавиатура, дисплей (монитор), сенсорный дисплей, тачпад, джойстик, манипулятор мышь, световое перо, стилус, сенсорная панель, трекбол, динамики, микрофон, средства дополненной реальности, оптические сенсоры, планшет, световые индикаторы, проектор, камера, средства биометрической идентификации (сканер сетчатки глаза, сканер отпечатков пальцев, модуль распознавания голоса) и т.п.

Средство сетевого взаимодействия (306) обеспечивает передачу данных посредством внутренней или внешней вычислительной сети, например, Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (306) может использоваться, но не ограничиваться: Ethernet карта, GSM модем, GPRS модем, LTE модем, 5G модем, модуль спутниковой связи, NFC модуль, Bluetooth и/или BLE модуль, Wi-Fi модуль и др. Представленные материалы заявки раскрывают предпочтительные примеры реализации технического решения и не должны трактоваться как ограничивающие иные, частные примеры его воплощения, не выходящие за пределы испрашиваемой правовой охраны, которые являются очевидными для специалистов соответствующей области техники.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Компьютерно-реализуемый способ автоматизированного определения порога идентификации для биометрических образцов в системе контроля доступа, выполняемый с помощью по меньшей мере одного процессора и содержащий этапы, на которых:

a) получают ретроспективные данные, содержащие сведения о результатах сравнения биометрических образцов, проходящих идентификацию, с зарегистрированными биометрическими шаблонами, при которых результат имеет наивысший скоринговый балл;

b) отбирают данные идентификации образцов за выбранный период времени, в ходе которого количество зарегистрированных биометрических шаблонов изменялось не более чем на 1% за выбранный период времени;

c) определяют количество идентификаций n и количество зарегистрированных биометрических шаблонов N за выбранный период времени;

d) определяют для данных идентификации, полученных на этапе b) информацию о по меньше мере двух скоринговых баллов TOP-1 и TOP-2, где TOP-1 - максимальное значение скорингового балла идентификации, TOP-2 - следующее за TOP-1 значение скорингового балла, при этом значения TOP-1 и TOP-2 выше порога аутентификации;

e) формируют гистограмму, состоящую из m элементов ($T1_i$), распределения скорингового балла TOP-1 идентификаций на диапазоне от порога аутентификации до максимально возможного скорингового балла;

f) формируют гистограмму, состоящую из m элементов ($T2_i$), распределения скорингового балла TOP-2 идентификаций на диапазоне от порога аутентификации до максимально возможного скорингового балла;

g) определяют для каждой точки гистограмм сумму значений всех элементов гистограммы начиная с текущего, получая новые гистограммы из m элементов;

h) определяют значение FAR_i (вероятность ложного допуска при аутентификации) на основании данных, полученных на этапах c) и g);

i) на основе полученных значений FAR_i на предыдущем этапе, рассчитывают значение $FPIR_i$ (вероятность ложноположительной идентификации) по формуле

$$FPIR_i = 1 - (1 - far_i)^N$$

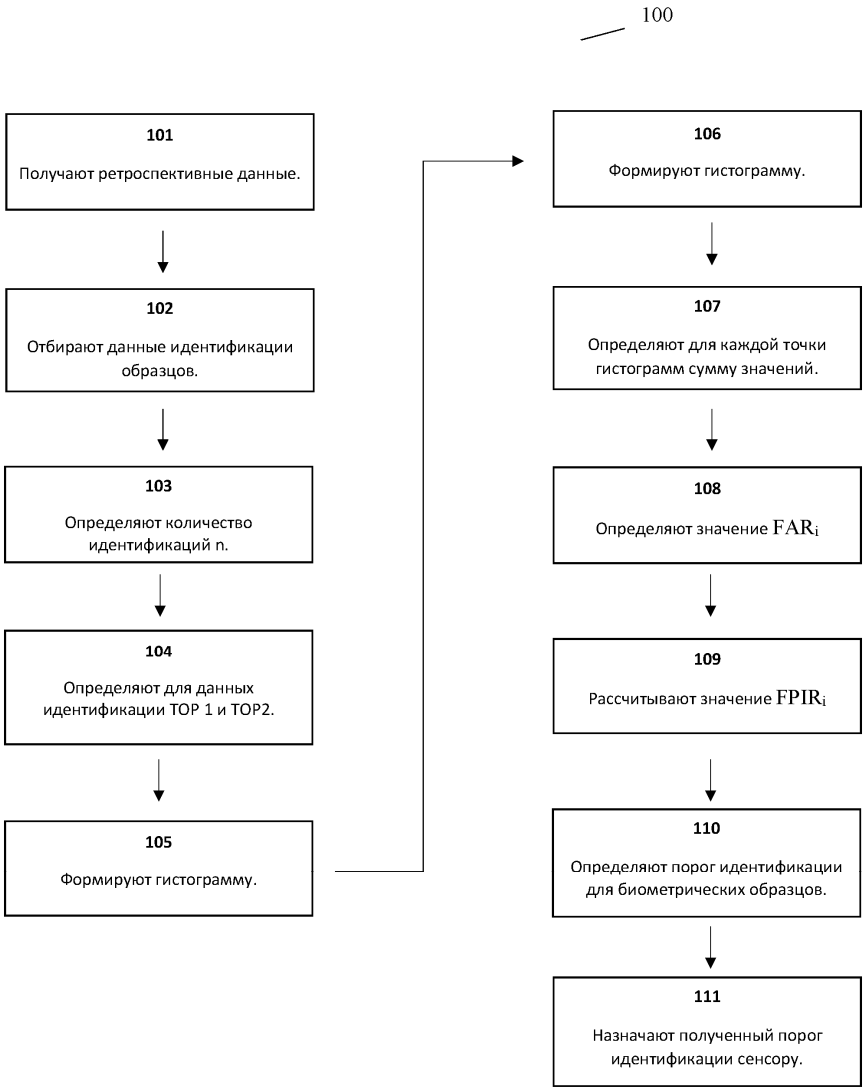
j) на основе полученных значений $FPIR_i$ определяют порог идентификации для биометрических образцов, и

k) назначают полученный порог идентификации для по меньшей мере одного биометрического сенсора.

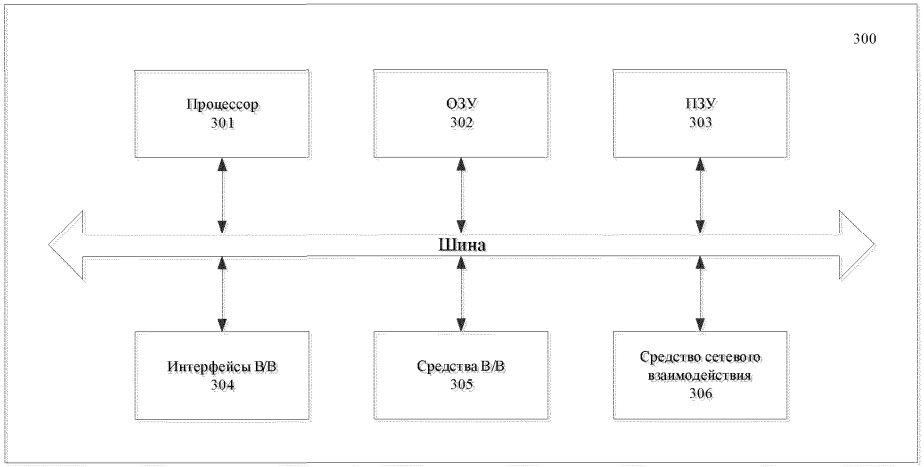
2. Система автоматизированного определения порога идентификации для биометрических образцов в системе контроля доступа, содержащая:

по меньшей мере один процессор;

по меньшей мере одну память, соединенную с процессором, которая содержит машиночитаемые инструкции, которые при их выполнении по меньшей мере одним процессором обеспечивает выполнение способа по п.1.


100
101
Получают ретроспективные данные.
102
Отбирают данные идентификации образцов.
103
Определяют количество идентификаций n.
104
Определяют для данных идентификации TOP 1 и TOP2.
105
Формируют гистограмму.
106
Формируют гистограмму.
107
Определяют для каждой точки гистограмм сумму значений.
108
Определяют значение FAR_i
109
Рассчитывают значение $FPIR_i$
110
Определяют порог идентификации для биометрических образцов.
111
Назначают полученный порог идентификации сенсору.

Фиг. 1


300
Процессор
301
ОЗУ
302
ПЗУ
303
Шина
Интерфейсы В/В
304
Средства В/В
305
Средство сетевого взаимодействия
306

Фиг. 2