(19) Евразийское патентное ведомство

(11) 018562 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2013.08.30

(21) Номер заявки
201071381

(22) Дата подачи заявки
2009.04.29

(51) Int. Cl. ***G06K 19/07*** (2006.01)
G06K 19/077 (2006.01)

(54) ПРОПУСКНОЙ ДОКУМЕНТ И ПРОПУСКНАЯ СИСТЕМА

(31) **0810807.8; 0818272.7**
(32) **2008.06.12; 2008.10.06**
(33) **GB**
(43) **2011.08.30**
(86) **PCT/GB2009/001093**
(87) **WO 2009/150394 2009.12.17**

(71)(73) Заявитель и патентовладелец:
ДЕ ЛА РЮ ИНТЕРНЕШНЛ ЛИМИТЕД (GB)

(72) Изобретатель:
Грин Стефен Банистер (GB)

(74) Представитель:
Хмара М.В. (RU)

(56) DE-A1-102005062827
US-A1-2007159338
US-A1-2004233042
US-A1-2002044096
WO-A-0211061
US-A1-2007164866
US-A1-2005218215
US-A1-2003173408
WO-A1-02054784
US-A1-2007252001

(57) Разработан пропускной документ, содержащий первую RFID-метку, считываемую только в пределах первого расстояния, и вторую RFID-метку, считываемую в пределах второго расстояния, причем первая RFID-метка содержит данные, относящиеся к владельцу пропускного документа и идентификационный код, а вторая RFID-метка содержит идентичный или взаимосвязанный идентификационный код, при этом второе расстояние превышает первое расстояние. Разработаны также способ и система для контроля доступа в определенную область. Каждый человек, желающий получить указанный доступ, имеет детектируемый уникальный идентификатор. Способ включает детектирование в первом пункте уникального идентификатора человека, находящегося в этом пункте; использование детектированного уникального идентификатора для извлечения информации, относящейся к указанному человеку, из одной или более внешних баз данных; передачу извлеченной информации во второй пункт, удаленный от первого пункта, и использование извлеченной информации во втором пункте для принятия решения о предоставлении доступа человеку, имеющему уникальный идентификатор.

018562 B1

018562 B1

Область техники

Изобретение относится к пропускным документам и системам, в частности к паспортам и идентификационным картам, но может быть применено к документам любого другого типа. Изобретение относится также к способам контроля доступа в определенную область, преимущественно при иммиграционном контроле.

Предшествующий уровень техники

Известен метод повышения степени защиты документа путем включения в него бесконтактной памяти данных в виде метки радиочастотной идентификации (Radio Frequency Identification, далее - RFID). Обычно RFID-метка программируется во время изготовления документа с внесением в нее данных, относящихся к владельцу документа. Это не только делает документ более сложным для подделывания или модифицирования, но также облегчает проверку его действительности, поскольку она может быть проведена до некоторой степени автоматически.

Традиционно RFID-метки, встраиваемые в паспорта, являются высокочастотными (HF) RFID-метками, работающими на частоте 13,56 МГц. HF RFID-метки являются предпочтительными, поскольку они могут хранить приемлемый объем данных и могут считываться только с короткого расстояния. Это расстояние предпочтительно составляет менее 1 м, но может быть увеличено до 1,5 м и даже при использовании мощного считывателя доведено максимум примерно до 3 м. Ограниченность области, в пределах которой может быть опрошена RFID-метка, является гарантией сохранения конфиденциальности данных, записанных на чипе. В качестве дополнительной защиты данных на чипе документ может быть снабжен электромагнитным экраном, таким как слой металлической сетки, которая предотвращает считывание с чипа, например, пока паспорт не будет раскрыт.

Сущность изобретения

Желательно улучшить защищенность пропускных документов, насколько это возможно, т.е. затруднить подделывание документа и облегчить обнаружение подделок. Желательно, кроме того, ускорить проверку таких документов.

В соответствии с первым аспектом изобретения пропускной документ содержит первую RFID-метку, считываемую только в пределах первого расстояния, и вторую RFID-метку, считываемую в пределах второго расстояния, причем первая RFID-метка содержит данные, относящиеся к владельцу пропускного документа, и идентификационный код, а вторая RFID-метка содержит идентичный или взаимосвязанный идентификационный код. При этом второе расстояние превышает первое расстояние.

Создание документа с двумя RFID-метками, имеющими взаимосвязанные коды, улучшает качество защиты, поскольку удаление или подмену любой из меток будет легко обнаружить. Кроме того, применение RFID-метки с увеличенной дальностью действия не ухудшает качество защиты, т.к. она несет только идентификационный код, а не какие-либо персональные данные. Идентификационные коды, содержащиеся в первой и второй RFID-метках, могут быть идентичными или только взаимосвязанными, например через базу данных, связывающую идентификационный код каждой первой RFID-метки с определенным идентификационным кодом второй RFID-метки. Альтернативно, любой из двух идентификационных кодов может содержать весь другой код или его часть.

Желательное первое расстояние включает максимальное расстояние считывания от первой RFID-метки, лежащее в интервале от 0 до около 3 м, предпочтительно в интервале от 0 до около 1 м. Первая RFID-метка не может считываться при превышении указанного максимального расстояния считывания, но может считываться в любой точке зоны, задаваемой максимальным расстоянием считывания (например, от непосредственной близости к первой RFID-метке до максимального расстояния).

Желательное второе расстояние включает максимальное расстояние считывания от второй RFID-метки, превышающее 1 м, предпочтительно превышающее 3 м, особо предпочтительно превышающее 10 м. Как было отмечено, максимальное расстояние считывания для второй RFID-метки больше, чем для первой. Вторая RFID-метка может считываться в любой точке зоны, задаваемой максимальным расстоянием считывания.

В предпочтительном варианте идентификационный код идентифицирует вторую RFID-метку, причем идентичный идентификационный код запрограммирован в первой RFID-метке. Альтернативно, идентификационный код идентифицирует первую RFID-метку, причем идентичный идентификационный код запрограммирован во второй RFID-метке.

Желательно, чтобы данные, содержащиеся в первой RFID-метке, включали относящиеся к владельцу персональные и/или биометрические данные, предпочтительно данные по отпечаткам пальцев, шаблоны радужной оболочки и/или данные опознавания по лицу.

Первая RFID-метка предпочтительно содержит высокочастотный (HF) RFID-чип, а вторая RFID-метка содержит ультравысокочастотный (UHF) RFID-чип. В некоторых вариантах HF RFID-чип функционирует в частотном диапазоне 3-29 МГц, предпочтительно 13-14 МГц, особо предпочтительно у 13,56 МГц, а UHF RFID-чип функционирует в частотном диапазоне 433-950 МГц, предпочтительно 860-870 МГц.

В некоторых предпочтительных вариантах первая и вторая RFID-метки интегрированы в один чип.

Вторая RFID-метка предпочтительно не содержит данных, относящихся к владельцу документа.

Для использования в изобретении пассивные RFID-метки предпочтительнее, чем активные. Пассивные RFID-метки в качестве источника питания используют только считыватель и не требуют наличия батареек или аналогичных элементов. Пассивные UHF RFID-метки в типичном варианте могут считываться с расстояния до 10 м, в изготовлении они дешевле, чем активные или полупассивные RFID-метки.

Однако активные или полупассивные RFID-метки также приемлемы для изобретения. Активные и полупассивные RFID-метки используют внутренние батарейки для питания своих контуров. Активная метка использует свою батарейку также для посылки радиоволн на считыватель, тогда как полупассивная метка для осуществления передачи использует энергию, получаемую от считывателя. Поскольку такие метки содержат больше электроники, чем пассивные RFID-метки, они более дорогие. Активные и полупассивные UHF RFID метки обычно резервируются для применений, требующих считывания документа с больших расстояний; при этом они обычно излучают на высоких частотах, 850-950 МГц, так что могут считываться с расстояний 30 м или более.

Первый аспект изобретения дополнительно охватывает пропускную систему (систему обеспечения безопасности), содержащую множество пропускных документов вышеописанного типа, причем идентификационный код каждого документа присвоен только этому документу. Система содержит также первый считыватель, выполненный с возможностью считывать данные с первых RFID-меток; второй считыватель, выполненный с возможностью считывать данные со вторых RFID-меток; базу данных, содержащую записи данных со сведениями по каждому владельцу пропускного документа и с соответствующим идентификационным кодом, и процессор, выполненный с возможностью в случае распознавания идентификационного кода первым или вторым считывателем извлекать из базы данных соответствующую запись данных.

Первый и второй считыватели на практике могут быть объединены в единый модуль, сконфигурированный с возможностью считывания и первой, и второй RFID-меток.

Желательно, чтобы процессор был дополнительно подключен по меньшей мере к одной внешней базе данных и выполнен с возможностью извлекать записи, соответствующие владельцу идентифицированного пропускного документа, по меньшей мере из одной внешней базы данных.

Согласно второму аспекту изобретения создана биометрическая контрольная система, содержащая

считыватель RFID-метки для считывания данных с пропускного документа, имеющего по меньшей мере одну RFID-метку, причем единственная или каждая RFID-метка содержит идентификационный код, идентифицирующий пропускной документ;

по меньшей мере один входной биометрический модуль для тестирования биометрических характеристик владельца пропускного документа;

базу данных, содержащую записи данных со сведениями по каждому владельцу пропускного документа и с соответствующим ему идентификационным кодом; и

процессор, выполненный с возможностью в случае распознавания идентификационного кода извлекать соответствующую ему запись данных и сравнивать выходные данные от указанного биометрического модуля с биометрическими данными в извлеченной записи данных, чтобы удостовериться в том, что владелец пропуска соответствует записи данных по владельцу пропускного документа.

Благодаря выявлению профиля владельца документа система может проводить парное сравнение входных биометрических данных человека с хранящимися данными для этого человека, чтобы определить, имеется ли совпадение между ними. Такое сравнение требует существенно меньшей вычислительной мощности, чем сравнение указанных входных биометрических данных со всеми записями данных, чтобы идентифицировать владельца (т.е. сравнение одного комплекта данных с N комплектами). Как следствие, процесс проверки ускоряется.

Считыватель RFID-метки выполнен с возможностью считывания RFID-метки с расстояния от RFID-метки более 1 м, предпочтительно более 3 м, особо предпочтительно более 10 м. Желательно, чтобы считыватель RFID-метки был считывателем ультравысокочастотной (UHF) RFID-метки, а каждая RFID-метка была UHF RFID-меткой.

Входной биометрический модуль (входные биометрические модули) выполнен (выполнены) с возможностью сканировать радужную оболочку владельца, и/или его отпечаток пальца (отпечатки пальцев), и/или производить опознавание по лицу.

В предпочтительном варианте считыватель RFID-метки расположен на расстоянии от входного биометрического модуля (входных биометрических модулей). Это позволяет извлекать профиль владельца до того, как он подойдет к входному биометрическому модулю. Желательно, чтобы считыватель RFID-метки находился на входе в зону проверки, содержащую входной биометрический модуль (входные биометрические модули).

Одна из проблем, с которой сталкиваются многие системы иммиграционного контроля, состоит в необходимости ускорения проверки каждого пассажира и, тем самым, ускорения прохождения потока пассажиров. Действительно, часто наблюдаются длинные очереди в аэропортах, пассажирских морских портах и в других местах, в которых паспорт или другой пропускной документ каждого человека изучается и сопоставляется с записями данных.

Согласно третьему аспекту изобретения создан способ контроля доступа в определенную область в

условиях, когда каждый человек, желающий получить указанный доступ, имеет детектируемый уникальный идентификатор. Данный способ включает

детектирование в первом пункте, через который разрешено проходить всем людям, желающим получить доступ в указанную область уникального идентификатора человека, находящегося в первом пункте;

использование детектированного уникального идентификатора для извлечения информации, относящейся к указанному человеку, из одной или более внешних баз данных;

передачу извлеченной информации во второй пункт, удаленный от первого пункта; и

использование извлеченной информации во втором пункте, когда в нем находится указанный человек, для принятия решения о предоставлении ему доступа в указанную область.

Благодаря детектированию уникального идентификатора, такого, например, как номер паспорта или номер чипа, в первом пункте и его использованию для извлечения информации, такой как профиль владельца документа, из внешних баз данных (например, баз данных, которые ведутся независимо от системы иммиграционного контроля) можно получить данные о каждом владельце документа (т.е. о человеке, которому соответствует уникальный идентификатор) без необходимости предъявления владельцем своего пропускного документа инспектору. При этом можно будет принять решение (например, разрешить ли владельцу вход) во втором пункте без необходимости останавливать владельца на длительный период, в течение которого производится проверка записей. Тем самым будет значительно повышена производительность проверки. Данный способ можно использовать, например, в аэропортах, или в других транспортных терминалах, или на границах между странами.

Первый пункт желательно расположить так, чтобы он перекрывал зону, через которую проходят все люди, желающие войти в контролируемую область (например, люди, входящие в аэропорт с самолета). Второй пункт может быть расположен на расстоянии от первого на маршруте, по которому следуют люди. Например, второй пункт может находиться в аэропорте, аналогично традиционному пункту паспортного контроля, на некотором расстоянии от первого пункта вдоль указанного маршрута, непосредственно перед или за залом, в котором выдается багаж. Расстояние между пунктами предпочтительно является достаточно большим, чтобы людям, движущимся от первого пункта ко второму, требовалось на это, по меньшей мере, заданное минимальное время. Это время должно быть достаточным для извлечения релевантных данных и их передачи во второй пункт. На практике это время предпочтительно составляет менее 60 с, более предпочтительно менее 30 с.

Однако система может быть реализована и при существенно большем удалении одного пункта от другого. Например, первый пункт может соответствовать выходу на посадку в аэропорте, в котором производится детектирование уникальных идентификаторов пассажиров, проходящих на посадку в самолет. Вторым пунктом в этом случае может быть аэропорт назначения.

Извлеченные данные могут передаваться во второй пункт непосредственно (например, в необработанном виде), в форме оповещения или сообщения или иным образом, например по электронной почте. Однако способ предпочтительно включает введение извлеченной информации во временную базу данных по тому человеку (тем людям), чей уникальный идентификатор был детектирован. В этом случае извлеченная информация передается во второй пункт посредством обращения к временной базе данных. Информацию, переданную таким способом, можно быстро просмотреть, поскольку она уже сгруппирована и сохранена локально; кроме того, минимизируются требования по объему памяти данных во втором пункте, и освобождается полоса связи. Поступление детектированного уникального идентификатора во второй пункт может быть использовано для запуска выведения нужных данных из временной базы данных, так что объем команд, вводимых оператором, сводится к минимуму.

При получении необходимой информации по каждому пассажиру системе могут быть доступны любые подходящие базы данных. В дополнение к внешним базам могут быть опрошены одна или более "локальных" баз данных (например, интегрированных в систему иммиграционного контроля). Внешние базы данных предпочтительно включают одну или более из следующих баз: базу данных паспортной службы (ПС), содержащую персональную информацию о владельцах паспортов (например, граждан Великобритании); базу данных по потерям и кражам со сведениями о потерянных и украденных уникальных идентификаторах; базу данных, содержащую национальный стоп-лист со сведениями о людях, представляющих интерес, и соответствующих им уникальных идентификаторах, а также базу данных предварительной информации о пассажирах со сведениями о людях, которые, как можно ожидать, стремятся получить доступ в определенную область.

Во многих случаях по меньшей мере одна из внешних баз данных будет содержать биографические данные, по меньшей мере, некоторых людей, включая имя человека, его адрес, место и дату рождения, возраст и т.д.

В особо предпочтительном варианте одна или более внешних баз данных содержат биометрические данные, по меньшей мере, некоторых из людей. Биометрические данные содержат данные по одному или более отпечатков пальцев, данные по радужной оболочке (радужке) и данные опознавания по лицу (предпочтительно включающие фотографию человека). Биометрические данные являются особенно полезными, поскольку позволяют провести сопоставление владельца паспорта и его владельца по сведени-

ям баз данных автоматически, т.е. быстрее и точнее по сравнению с оператором.

Следовательно, если одна или более внешних баз данных содержат биометрические данные, соответствующие детектированному уникальному идентификатору, эти биометрические данные желательно включить в извлеченную информацию, передаваемую во второй пункт.

В некоторых вариантах может представляться желательным одновременно получить всю информацию, ассоциированную с уникальным идентификатором, из всех доступных баз данных и сделать всю эту информацию доступной во втором пункте. Однако во многих случаях предпочтительно свести объем передаваемой информации к минимуму, чтобы уменьшить ширину полосы связи и емкость памяти для временной базы данных или для второго пункта. В связи с этим целесообразно, чтобы операция использования детектированного уникального идентификатора для извлечения информации, относящейся к указанному человеку из одной или более внешних баз данных, включала

проведение поиска, по меньшей мере, в некоторых из внешних баз данных с целью извлечения первой информации, относящейся к указанному человеку;

принятие решения, основываясь на первой информации, о целесообразности предоставления указанному человеку доступа в контролируемую область, и в случае положительного решения проведение поиска, по меньшей мере, в некоторых из внешних баз данных с целью извлечения второй информации, относящейся к указанному человеку.

При этом первую и вторую информацию передают во второй пункт. В этом случае вторую информацию требуется извлекать, только если первая информация поддерживает допуск человека в контролируемую область.

Вторая информация предпочтительно содержит биометрические данные. В типичной ситуации она будет использоваться, только если извлеченная первая информация указывает, что конкретному человеку следует разрешить вход в определенную область. Действительно, при любом другом результате владелец должен будет получить помощь от представителя пограничной службы, не обращаясь к автоматической биометрической контрольной системе.

Каждый пассажир может быть направлен в один и тот же второй пункт (в котором может иметься множество стоек), где извлеченная информация используется, чтобы определить, проверка в каком объеме необходима, чтобы разрешить владельцу доступ в указанную область. Например, во втором пункте могут иметься аппарат для биометрического контроля и представитель службы, которые способны провести проверку и принять решение. Однако при этом работа с пассажирами все же будет вестись в последовательном режиме, что может привести к образованию очереди из-за людей, чьи извлеченные данные создали проблемы. В связи с этим предпочтительно организовать параллельную работу с различными категориями пассажиров. Поэтому, после того как информация была извлечена, способ дополнительно предусматривает выбор, основываясь на извлеченной информации, одного или более из множества вторых пунктов и направление носителя уникального идентификатора к выбранному второму пункту (выбранным вторым пунктам).

В зависимости от извлеченной информации владельцы идентификаторов могут быть направлены к различным средствам для проведения операции принятия окончательного решения: например, если выявлены проблемы с профилем владельца, он может быть направлен за помощью к представителю, осуществляющему контроль за посадкой. Если же по информации из базы (баз) данных никаких проблем не выявлено, владельца можно направить по более быстрому, автоматизированному маршруту, например к пункту биометрического контроля. Это дополнительно повысит пропускную способность.

Как было упомянуто, метод, по которому принимается решение во втором пункте, сделан зависящим от извлеченной информации. Однако в общем случае предпочтительно, чтобы операция использования извлеченной информации для принятия решения о предоставлении человеку, имеющему уникальный идентификатор, доступа в указанную область, включала определение того, указывает ли извлеченная информация, что человеку, соответствующему уникальному идентификатору, следует предоставить доступ в определенную область. Если да, нужно определить, является ли человек, имеющий уникальный идентификатор, человеком, соответствующим указанному идентификатору по данным внешней базы данных (внешних баз данных).

В одном предпочтительном варианте проведение проверки включает сравнение идентификационного документа, предъявленного человеком, имеющим уникальный идентификатор, с самим человеком, причем идентификационный документ предпочтительно включает уникальный идентификатор.

В другом предпочтительном варианте, если извлеченная информация включает биометрические данные, проведение проверки включает сравнение человека, имеющего уникальный идентификатор, по меньшей мере, с некоторыми извлеченными биометрическими данными, ассоциированными с уникальным идентификатором во внешней базе данных (внешних базах данных). Проверка в этом случае предпочтительно включает анализ одного или более отпечатков пальцев, анализ радужной оболочки или опознавание по лицу. Такая проверка предпочтительно проводится биометрической контрольной системой по второму аспекту изобретения.

При этом желательно, чтобы были доступны несколько или все названные методы проверки и чтобы соответствующий метод выбирался для каждого человека в зависимости от извлеченной информации.

В особо предпочтительном варианте каждый уникальный идентификатор, связанный с пропускным документом, выполненным согласно первому аспекту изобретения, предпочтительно имеет вид второй RFID-метки. Однако в других вариантах уникальный идентификатор может предоставляться отдельно от идентификационного документа, например вместе с картой, выдаваемой при регистрации на рейс, картой частого пассажира или даже с багажным ярлыком. При применении уникального идентификатора использование RFID-метки с большим радиусом действия (UHF RFID-метки) особенно эффективно, поскольку, как это было описано ранее, в этом случае идентификатор может считываться с относительно больших расстояний, не создавая неудобств для владельцев, в частности без необходимости останавливать их. При этом права личности не нарушаются, поскольку персональные данные владельцев доступны только персоналу, имеющему доступ к базе данных (базам данных).

Использование описанных документов обеспечивает возможность включения в способ иммиграционного контроля операции аутентификации документа. В связи с этим операция использования извлеченной информации для принятия решения о предоставлении человеку, имеющему уникальный идентификатор, доступа в указанную область, предпочтительно включает определение аутентичности пропускного документа опрашиванием первой RFID-метки и проверку соответствия (например, совпадения или согласованности) содержащегося в ней идентификационного кода уникальному идентификатору (которым может являться идентификационный код второй RFID-метки). Это позволяет сделать проверку аутентичности автоматической, причем она может применяться вместо или параллельно с другими методами, такими как визуальный анализ элементов защиты на документе, например, таких как голограммы, оптически переменные краски, ультрафиолетовые или инфракрасные элементы.

Согласно третьему аспекту изобретения создана система для контроля доступа в определенную область, содержащая

детектор, выполненный с возможностью детектировать уникальный идентификатор, имеющийся у человека, находящегося в первом пункте, через который разрешен проход всем людям, желающим получить доступ в определенную область, причем уникальный идентификатор соответствует определенному человеку;

контроллер, выполненный с возможностью принимать детектированный уникальный идентификатор от детектора, извлекать информацию, относящуюся к указанному человеку, которому соответствует детектированный уникальный идентификатор, из одной или более внешних баз данных и передавать извлеченную информацию во второй пункт, удаленный от первого пункта, и по меньшей мере один терминал во втором пункте, выполненный с возможностью обеспечения принятия на основе извлеченной информации решения о предоставлении человеку, который находится во втором пункте и имеет уникальный идентификатор, доступа в указанную область.

Детектор предпочтительно содержит радиочастотную антенну, выполненную с возможностью считывания RFID-меток, предпочтительно UHF RFID-меток, для детектирования записанных в них уникальных идентификаторов.

Система предпочтительно содержит также временную базу данных, причем контроллер выполнен с возможностью хранения извлеченной информации в указанной базе, а по меньшей мере один терминал во втором пункте выполнен с возможностью доступа к временной базе данных.

По меньшей мере один терминал предпочтительно содержит компьютер и монитор для отображения по меньшей мере части извлеченной информации или контрольный биометрический модуль.

В особо предпочтительном варианте по меньшей мере один терминал содержит второй детектор, выполненный с возможностью детектировать уникальный идентификатор, имеющийся у человека во втором пункте, и выполнен с возможностью идентифицировать извлеченную информацию, соответствующую уникальному идентификатору, детектированному вторым детектором.

Система может содержать также множество терминалов во втором пункте и дополнительно направляющее средство, выполненное с возможностью направлять каждого человека к выбранному терминалу или к выбранному подмножеству множества терминалов, основываясь на извлеченной информации, соответствующей уникальному идентификатору, имеющемуся у человека.

Направляющее средство предпочтительно содержит третий детектор, выполненный с возможностью детектировать уникальный идентификатор, имеющийся у человека, находящегося вблизи направляющего средства, и выполнено с возможностью идентифицировать извлеченную информацию, соответствующую уникальному идентификатору, детектированному третьим детектором. Направляющее средство может дополнительно содержать выходной модуль, выполненный с возможностью направлять каждого человека, выдавая указание на выбранный терминал или на выбранное подмножество множества терминалов.

Краткое описание чертежей

Далее со ссылками на прилагаемые чертежи будут описаны примеры пропускных документов, систем и способов согласно изобретению.

На фиг. 1 схематично представлена система для контроля доступа;

на фиг. 2 показан пропускной документ, пригодный для использования в системе по фиг. 1;

на фиг. 3 схематично показано направляющее устройство, пригодное для использования в системе

по фиг. 1;

на фиг. 4 схематично показан терминал биометрического контроля, пригодный для использования в системе по фиг. 1;

на фиг. 5 представлена блок-схема способа контроля доступа;

на фиг. 6 представлена блок-схема, иллюстрирующая шаги способа по фиг. 5.

Сведения, подтверждающие возможность осуществления изобретения

Дальнейшее описание будет сфокусировано на использовании пропускных документов, систем и способов в иммиграционных сценариях, т.е. в процессе контроля доступа в страну, реализуемом, например, в аэропорту, в морском порту или в другом транспортном узле. Однако должно быть понятно, что изобретение в равной степени применимо к контролю доступа и в любую другую область, когда представляется желательным предотвратить доступ в нее некоторым людям или, наоборот, разрешить доступ только определенным людям. Другими примерами являются офисы, производственные предприятия, школьные и университетские кампусы, зрелищные мероприятия и т.д.

На фиг. 1 показаны люди P, приближающиеся к контролируемой области R. Каждый человек P несет (имеет с собой) уникальный идентификатор, который может быть детектирован системой 10 иммиграционного контроля. Эта система содержит контроллер 11, сконфигурированный для получения сигналов от детектора 15, выполненного с возможностью перекрывать первый пункт 1. Как будет подробно описано далее, детектор 15 способен детектировать уникальные идентификаторы, имеющиеся у людей P, находящихся в первом пункте 1, и передавать детектированные уникальные идентификаторы контроллеру 11.

Контроллер 11 связан с одной или более внешних баз 14a, 14b и 14c данных. Внешние базы данных (например, база 14a) могут быть практически доступны через сетевое соединение или любое иное средство 16 обмена данными, включая Интернет, интранет, телефонную сеть общего пользования и сети беспроводной связи.

Любая внешняя база данных, содержащая информацию, релевантную для решения, следует или нет разрешить людям доступ в указанную область, может быть доступна через контроллер 11. Под "внешними базами данных" понимаются базы данных, которые ведутся, по существу, независимо от рассматриваемой системы иммиграционного контроля, например правительственными или правоохранительными органами или другими системами иммиграционного контроля (например, находящимися в других аэропортах).

Применительно к системам иммиграционного контроля контроллер 11 может иметь доступ к таким базам данных, как ведущаяся британским правительством база данных ПС (со сведениями обо всех владельцах паспортов в Великобритании), база Интерпола по потерям и кражам, один или более национальных стоп-листов, Индексированный список подозреваемых по Великобритании и база данных конфиденциальных сведений Министерства иностранных дел США. Может обеспечиваться также доступ к базам данных, содержащим информацию, предоставленную другими системами иммиграционного контроля. По меньшей мере в одной, но, возможно, в каждой базе данных информация, касающаяся определенного человека, ассоциирована с принадлежащим ему уникальным идентификатором.

Контроллер 11 выполнен с возможностью извлекать, основываясь на уникальных идентификаторах, детектируемых детектором 15, информацию из одной или более баз 14 данных. На практике эта операция может включать использование каждого детектированного уникального идентификатора для формирования запроса к каждой выбранной базе данных. Альтернативно, сначала может быть опрошена одна база данных (как правило, база данных ПС или ее эквивалент за пределами Великобритании), чтобы идентифицировать человека, соответствующего уникальному идентификатору. Извлеченная информация (например, фамилия человека) может затем использоваться для проведения поисков определенного типа в одной или более других баз данных. Затем результаты этих поисков могут быть переданы обратно в базу данных ПС, чтобы можно было принять решение о предоставлении доступа данному человеку. В качестве опции могут быть извлечены также дополнительные данные из локальных (внутренних) баз 12 данных, например, содержащих записи, хранящиеся в самой системе 10 иммиграционного контроля.

Сгруппированные извлеченные данные делаются доступными по меньшей мере одному второму пункту 2. Данный пункт находится на некотором расстоянии от первого пункта 1 по направлению движения людей P к контролируемой области R. В типичной системе иммиграционного контроля первый пункт может находиться, например, в аэропорту, у входа для прибывших пассажиров, а второй пункт - в зоне паспортного контроля, непосредственно перед зоной выдачи багажа. Второй пункт, как правило, снабжен одним или более терминалов, выполненных с возможностью использования извлеченной информации. В системе по фиг. 1 во втором пункте 2 имеются три таких терминала 40, 50a и 50b. Первый терминал 40 снабжен компьютером (например, персональным) с монитором, которым может пользоваться любой работник пограничной службы. Второй и третий терминалы 50a и 50b содержат аппарат для биометрического контроля, который будет описан далее. Все терминалы используются для принятия, основываясь на извлеченной информации, решения о том, следует ли разрешить человеку P вход в контролируемую область R.

Извлеченная информация может быть передана во второй пункт различными способами. В одном

варианте информация может быть передана на один или более терминалов (или на все терминалы) в форме сообщения, например электронной почты, или другой последовательности данных. Если можно установить, на каком из терминалов будет производиться проверка, сообщение может быть отправлено только на этот терминал (или на соответствующее подмножество терминалов). Альтернативно, отправка может быть неселективной. Однако в предпочтительном варианте извлеченная информация хранится контроллером 11 в локальной временной базе 13 данных. Термин "временная" в контексте изобретения означает, что содержимое данной базы данных относится к людям, уникальные идентификаторы которых были детектированы, например к людям, которые вошли в данную систему иммиграционного контроля (в отличие от баз данных с информацией, относящейся к людям вообще). Как правило, для каждого детектированного уникального идентификатора создается запись, с которой ассоциируется любая соответствующая извлеченная информация. В зависимости от характера и объема извлеченной информации может оказаться необязательным или нежелательным включение в указанную запись всей извлеченной информации. Запись может содержать также сведения о решении, принятом контроллером 11 на основе извлеченной информации, например слово "СТОП", если по сведениям из одной или более баз данных выявлена проблема, или "В ПОРЯДКЕ", если никаких проблем не выявлено.

Каждый терминал 40, 50a и 50b может обратиться к временной базе 13 данных, чтобы извлечь соответствующую запись данных по мере подхода каждого человека P ко второму пункту 2. Это извлечение можно производить вручную (например, вводом имени человека). Однако терминал предпочтительно снабжен детектором, который считывает уникальный идентификатор, имеющийся у человека, приближающегося к терминалу, и процессором, который формулирует соответствующий запрос к временной базе 13 данных, чтобы извлечь релевантные данные.

После этого во втором пункте 2 может быть принято решение, следует ли разрешить человеку, имеющему указанный уникальный идентификатор, доступ в область R. Это решение может, например, целиком основываться на извлеченной информации, так, если извлечено сообщение "В ПОРЯДКЕ", человек может быть сразу пропущен в контролируемую область. Однако для повышения безопасности принятие решения предпочтительно включает проведение проверки, действительно ли человек, имеющий уникальный идентификатор, является именно тем человеком, которому этот идентификатор соответствует по сведениям баз данных. Как будет подробно описано далее, режим проведения проверки зависит от того, какая информация была извлечена. Дополнительное улучшение может состоять в проверке аутентичности уникального идентификатора.

Уникальный идентификатор может быть присвоен каждому человеку P различным образом. Предпочтительно, чтобы этот идентификатор мог детектироваться дистанционно, без необходимости останавливать человека. Для этой цели особенно удобным вариантом являются RFID-метки, хотя применимы и другие технологии, включая применение одно- и двумерных штрих-кодов. Особенно эффективными представляются ультравысокочастотные (UHF) RFID-метки с учетом того, что они могут опрашиваться считывателем с большого расстояния. Такие метки могут быть встроены в документ, например в карту, выдаваемую пассажиру при регистрации на рейс, или в карту частого пассажира. Альтернативно, ярлыки, несущие RFID-метки, могут прикрепляться к посадочным талонам. Пример особо предпочтительного пропускного документа 20, содержащего уникальный идентификатор и пригодного для системы по фиг. 1 (и имеющего также другие применения), представлен на фиг. 2. Он будет подробно описан далее.

В некоторых вариантах каждый человек P может двигаться от первого пункта прямо ко второму пункту и при наличии более одного терминала может самостоятельно выбрать один из них или быть направленным к определенному терминалу в соответствии с такими критериями, как национальность, страна отправления и т.д. Такой вариант особенно удобен, если система предусматривает, что все люди P подвергаются одному и тому же варианту проверки независимо от характера извлеченной информации, например, служащий, осуществляющий контроль, проводит каждую проверку (такую, на которую рассчитан терминал 40 по фиг. 1), используя извлеченную информацию. Однако, как уже отмечалось, желательно реализовать более чем один способ проведения проверки в зависимости от типа извлеченной информации. Например, если были переданы биометрические данные, проверка может быть проведена посредством аппарата для биометрического контроля (АБК), т.е. на терминале 50a или 50b. При неполучении таких данных может потребоваться проверка, проводимая представителем пограничной службы. Кроме того, каждый из терминалов 40, 50a и 50b может быть пригоден для различных типов проверки. Например, аппараты для биометрического контроля терминалов 50a, 50b могут быть пригодны для получения через них доступа к извлеченным данным, как это осуществляется через компьютер 40. Альтернативно, оборудование, требуемое для осуществления биометрического контроля, может быть встроено в компьютеризованный терминал 40.

В этом варианте люди P могут подходить к любому терминалу во втором пункте, где будет проведена соответствующая проверка, чтобы решить, может ли быть разрешен доступ в область R конкретному человеку P. Однако поскольку некоторые формы проверки занимают больше времени, чем другие, эта схема может привести к излишним очередям. Поэтому в особо предпочтительном варианте система 10 дополнительно содержит направляющее устройство 30, установленное в третьем пункте 3, на пути между первым пунктом 1 и вторым пунктом 2. Направляющее устройство 30 направляет каждого человека P

к одному из терминалов 40, 50a или 50b (или к подмножеству терминалов), основываясь на извлеченной информации, соответствующей уникальному идентификатору направляемого человека. Например, люди, по которым были извлечены биометрические данные, могут быть направлены к терминалу 50a или 50b биометрического контроля для ускоренной проверки, тогда как люди, по которым биометрические данные недоступны, могут быть направлены к представителю пограничной службы на терминале 40. Это позволит сократить очереди благодаря "быстрому пропусканию" части людей с применением ускоренных процедур проверки, тогда как представитель пограничной службы может заниматься только теми людьми, данные по которым требуют дополнительного изучения (или по которым информация в базах данных отсутствует).

Пример направляющего устройства 30 показан на фиг. 3. Устройство 30 содержит процессор 31, связывающийся с контроллером 11 или с временной базой 13 данных, и выходное устройство, такое как дисплей 32 для выдачи указания человеку P о том, к которому из терминалов 40, 50a и 50b (именуемых в совокупности множеством вторых пунктов) он должен обратиться. Устройство 30 может идентифицировать приближающего человека P различными способами. Предпочтительно оно содержит считыватель 33, выполненный с возможностью считывать уникальный идентификатор человека аналогично детектору 15. Например, считыватель 33 может быть считывателем RFID-метки. Однако антенна этого считывателя может быть менее мощной, чем у детектора 15, так что уникальный идентификатор детектируется, только когда человек вплотную приблизится к устройству (например, менее чем на 1 м) или даже только когда он прикоснется своим уникальным идентификатором к устройству 30. Детектированный уникальный идентификатор используется процессором 31, чтобы получить (предпочтительно через временную базу 13 данных) доступ к релевантным данным, извлеченным контроллером 11. Основываясь на извлеченных данных, процессор 31 решает, к которому из терминалов (или вторых пунктов) должен быть направлен человек, соответствующий уникальному идентификатору. После этого процессор выдает соответствующее указание. Альтернативно, решение может приниматься контроллером 11 и включаться в данные, получаемые процессором 31. Указания могут выдаваться направляющим устройством 30 также (или только) в звуковой форме. Таким образом, каждый человек, движущийся от первого пункта, может предъявить свой уникальный идентификатор устройству 30, чтобы быть направленным к соответствующему терминалу и далее следовать для проведения проверки именно к этому терминалу. В результате минимизируются очереди. В типичном варианте следует установить множество устройств 30 вблизи третьего пункта, чтобы одновременно направлять многих людей P.

Пример выполнения терминала 50a или 50b биометрического контроля представлен на фиг. 4. В типичном варианте он содержит процессор 51, выполненный с возможностью связываться с контроллером 11 и/или с временной базой 13 данных, выходное устройство, такое как дисплей 52, и входной биометрический модуль 54. Данный модуль 54 содержит входное средство, пригодное для проведения требуемого биометрического измерения. Например, этот модуль может содержать сканер отпечатка пальца или радужной оболочки или камеру для опознавания по лицу. Терминал может быть снабжен входными средствами различных типов; например, любой терминал можно сделать способным проводить как сканирование радужной оболочки, так и сопоставление отпечатков пальцев. Имеется также средство (такое как детектор 53) для детектирования уникального идентификатора человека. Как и в случае направляющего устройства 30, можно использовать детектор 53 любого типа, соответствующего характеру используемых уникальных идентификаторов. В рассматриваемом варианте им может быть UHF RFID-считыватель, мощность которого отрегулирована с целью детектирования только уникальных идентификаторов, находящихся в непосредственной близости от терминала 50. Детектированный уникальный идентификатор используется процессором 51 для извлечения (предпочтительно через временную базу 13 данных) соответствующих данных, сгруппированных контроллером 11. Как правило, к входному (контрольному) биометрическому модулю 54 будут направляться только люди, биометрические данные которых имеются в извлеченной информации, так что процессор 51 будет способен провести прямое (парное) сравнение данных, полученных им от контрольного биометрического модуля 54 (например, отпечатка пальца или результата сканирования радужной оболочки), и аналогичных данных, содержащихся в соответствующей записи данных. Такое прямое сравнение можно произвести значительно быстрее, чем намного более сложное и, соответственно, медленное сравнение одного результата проверки с N (большим количеством) результатов поиска биометрических данных по всем базам данных для неопределенного круга людей. В результате возрастают и производительность, и защищенность. Возможность прямого сравнения двух комплектов данных улучшает также надежность опознавания по лицу.

На фиг. 5 и 6 приведены блок-схемы способа, иллюстрирующие операции, входящие в вариант процесса иммиграционного контроля. Фиг. 5 дает общее представление о данном процессе. Каждый человек P имеет с собой уникальный идентификатор (УИ), встроенный в документ 20 типа паспорта, карты 20', которая может быть выдана ПС, или карты 20" частого пассажира, которая также может содержать номер паспорта ее владельца. По желанию, можно использовать и любой иной вариант обладания уникальным идентификатором. В данном примере уникальным идентификатором служит код, содержащийся в RFID-метке, предпочтительно в UHF RFID-метке, который может быть считан с относительно большого расстояния. Так, в первом пункте 1, соответствующем, например, месту выхода из самолета,

т.е. зоне перехода от самолета к пункту контроля, детектор, такой как считыватель UHF-чипа, сканирует паспорт 20 человека с расстояния нескольких футов, считывая уникальный идентификатор, записанный в чипе. Поскольку UHF-чип не содержит никаких персональных данных, эта операция не создает никаких проблем, связанных с защитой прав личности.

Затем уникальный идентификатор используют для получения данных (как это было описано выше) от внешней базы 14 данных (внешних баз данных, БД), например от главной государственной базы паспортных данных (например, БД ПС Великобритании), данные в которую должны были быть записаны при выдаче паспорта. За время, которое требуется человеку, чтобы добраться из первого пункта до второго пункта 2, такого как пункт иммиграционного контроля, можно, используя данные, найденные в государственной базе 14 паспортных данных, провести также несколько дополнительных поисков в других внешних базах данных (например, в БД Интерпола). Любые собранные при этом данные будут храниться локально, во временной БД, так что они будут доступны представителю иммиграционной службы до того, как путешественник подойдет к пункту иммиграционного контроля. Дополнительное время на поиск позволяет провести более тщательную проверку в аспекте безопасности, а также ускоренный пропуск граждан данной страны, поскольку представитель иммиграционного контроля будет располагать всей имеющейся релевантной информацией до того, как путешественник появится в пункте иммиграционного контроля.

В предпочтительных вариантах имеется также опция быстрого прохождения иммиграционного контроля. По результатам сканирования UHF-чипа в промежуточном третьем пункте 3 на пути к пункту иммиграционного контроля люди, которые были предварительно признаны системой не требующими детального паспортного контроля, могут быть направлены по отдельному коридору, в котором представителям иммиграционного контроля достаточно провести только беглую проверку (например, только визуальную инспекцию документа). Лицам, не имеющим UHF-чипа в своих паспортах или отмеченным системой как имевшие какие-то проблемы на предварительной стадии, необходимо будет пройти стандартную, более тщательную процедуру иммиграционного контроля. Таким образом, данный вариант, по существу, соответствует опережающему иммиграционному контролю, существенно сокращающему затраты времени на прохождение иммиграционного контроля гражданами данной страны с одновременным повышением надежности контроля.

На фиг. 6 описанный процесс проиллюстрирован более подробно. На шаге S100 уникальный идентификатор человека детектируется в первом пункте 1. На шагах S102 и S104 контроллер 11 принимает детектированный уникальный идентификатор и использует его для поиска данных в различных внешних базах 14 данных. На шаге S106 контроллер определяет, были ли идентифицированы какие-либо проблемы в извлеченных данных. Если да, на шаге S107 некоторые или все извлеченные данные записываются во временную базу 13 данных, предпочтительно с выделением причины для отказа или дальнейшего выяснения. Если нет, на шаге S108 контроллер определяет, имеются ли в извлеченных данных биометрические данные, или указывает, что биометрические данные доступны. Если нет, на шаге S109 некоторые или все извлеченные данные записываются во временную базу 13 данных, предпочтительно с указанием, что данный человек прошел проверку. Если биометрические данные доступны, на шаге S110 они извлекаются (если уже не были извлечены на шаге S104), а на шаге S112 извлеченные данные (включая биометрические данные) записываются во временную базу 13 данных, предпочтительно с указанием на успешно пройденную проверку.

В данном примере людей P, приближающихся ко второму пункту 2, направляют к одному из терминалов 40a, 40b, 50a, 50b или 50c в зависимости от извлеченных данных. Эта операция производится в третьем пункте 3, например, посредством устройства 30, описанного выше. На шаге S300 делается попытка детектировать уникальный идентификатор, имеющийся у человека, находящегося в третьем пункте 3. Если этот идентификатор не детектируется, человека направляют к стандартному контрольному терминалу 40a, обслуживаемому представителем иммиграционной службы, поскольку система не имеет никакой дополнительной информации. Если уникальный идентификатор детектируется, на шаге S302 он используется для поиска соответствующей извлеченной информации во временной базе 13 данных. Если идентифицированы какие-то проблемы, запись рассматривается как негативная, и человека также направляют к стандартному контрольному терминалу 40a. Если никаких проблем в данных не выявлено, на шаге S304 определяется, имеются ли биометрические данные (либо составляющие часть извлеченных данных, либо доступные системе иным путем, например использованием ключа к данным с целью извлечь биометрическую информацию из другой базы данных). В данном примере эта операция включает до трех проверок, чтобы определить, имеется ли по данному человеку шаблон отпечатков пальцев, шаблон лица или шаблон радужной оболочки (радужки). При этом эти шаги могут выполняться в любом порядке и не ограничиваться приведенными выше вариантами. При первой проверке (шаг S304a) определяют, имеется ли шаблон отпечатков пальцев. Если да, человека можно направить к терминалу 50a биометрического контроля по отпечаткам пальцев. Если нет, на шаге S304b определяют, имеется ли шаблон лица. Если да, человека можно направить к терминалу 50c биометрического контроля по шаблону лица. Если нет, на шаге S304c определяют, имеется ли шаблон радужки. Если да, человека можно направить к терминалу 50b биометрического контроля по радужке. Если нет, это будет соответствовать в

данном примере отсутствию доступных биометрических данных, так что человека направят к другому стандартному контрольному терминалу 40b, где может быть проведен беглый осмотр, чтобы убедиться, что фотография на паспорте соответствует его предъявителю.

Когда человек P подходит во втором пункте 2 к назначенному ему терминалу, производится требуемая проверка. В типичном случае она включает проверку того, что человек, имеющий уникальный идентификатор, - это именно тот человек, которому данный идентификатор присвоен в базах данных. Однако в системах, требующих не столь высокого уровня безопасности, эта операция может не требоваться, а решение может приниматься только на основе извлеченных данных.

В рассматриваемом примере, если человека направляют к стандартному контрольному терминалу, такому как 40a или 40b, обслуживаемому представителем соответствующей службы, уровень проводимой проверки будет зависеть от того, какие данные были извлечены, и от наличия каких-либо проблем идентификации. К терминалу 40a будут подходить люди, по которым нет записей данных или выявленных проблем. Паспортная документация таких людей будет требовать тщательного анализа паспорта на шаге S200, занимающего не менее 10 с на человека. По людям, подходящим к терминалу 40b, будут иметься записи данных "пропустить", так что в этом случае требуется только беглая проверка (занимающая около 2 с на человека), чтобы убедиться, на шаге S204, что предъявитель паспорта соответствует изображенному на паспортной фотографии.

Люди, подходящие к терминалу 50a биометрического контроля, проходят на шаге S202 автоматическую проверку путем сопоставления их отпечатка пальца (отпечатков пальцев) с соответствующими записями данных. При приближении к терминалу 50a детектируется уникальный идентификатор (шаг S202a), после чего из временной базы 13 данных извлекают соответствующие биометрические данные (шаг S202b). Затем проводится прямое (парное) сопоставление извлеченных и реальных биометрических данных. Аналогичный процесс имеет место и на терминале 50b биометрического контроля, на котором производят сканирование радужной оболочки для сравнения (на шаге S208) результатов с записями данных. Как правило, записи по радужным оболочкам хранятся в отдельной базе данных. Поэтому детектированный (на шаге S208a) уникальный идентификатор человека используют для получения доступа к временной базе 13 данных, чтобы получить из нее (на шаге S208b) нужные данные, включая ключ, который можно использовать для поиска биометрических данных в базе данных по радужной оболочке (шаг S208c). Затем производят парное сравнение результатов сканирования с записями данных. На терминале 50c, использующем опознавание по лицу, делается снимок владельца паспорта, который сравнивают с извлеченными данными для опознавания по лицу (шаг S206). И в этом случае уникальный идентификатор, имеющийся у владельца паспорта, детектируется (шаг S206a) и используется для извлечения соответствующих данных опознавания по лицу (шаг S206b), которые затем могут быть использованы для проведения парного сравнения.

Следует отметить, что в зависимости от конкретного приложения первый, второй и (по желанию) третий пункты могут быть сконфигурированы во многих различных вариантах. Одна из проблем, связанных с авиарейсами, состоит в том, чтобы гарантировать, чтобы определенный человек попал в соответствующий самолет. Хотя существует много различных предложений, направленных на улучшение данной операции с помощью биометрических данных, в варианте согласно изобретению предлагается считывать уникальный идентификатор человека (например, записанный в паспорт с UHF RFID-меткой) при регистрации на рейс (в первом пункте) и снова считывать его у пункта выхода на посадку (во втором пункте). В этом случае внешняя база данных может содержать списки ожидаемых пассажиров, так что окончательное решение о допуске на посадку может просто предусматривать проверку соответствия каждого детектируемого уникального идентификатора идентификатору в списке. Использование UHF RFID-чипа существенно упростит данную процедуру, причем без возникновения проблем, связанных с защитой данных. При этом такой вариант позволяет придать существующим паспортам соответствующую функциональность, поскольку авиакомпания может прикреплять к ним соответствующие UHF RFID-ярлыки при регистрации и передавать данные об этом государственным паспортным системам и другим внешним базам данных.

Другим аспектом, связанным с безопасностью систем типа описанных выше, является аутентичность самих уникальных идентификаторов. Как было упомянуто выше, эти идентификаторы встраиваются в документы, такие как паспорта. Далее будет описан особо эффективный пропускной документ, предназначенный для использования в описанной выше системе иммиграционного контроля (и в других системах, где аутентичность документа является важным фактором).

Пример такого документа 20 представлен на фиг. 2. Его идея состоит в совмещении HF RFID-чипа (типа предназначенного для паспортов и рассчитанного на короткое расстояние, КР), UHF RFID-чипа (рассчитанного на большое расстояние, БР) и соответствующих антенн в одном пропускном документе, таком как паспорт или идентификационная карта.

Высокочастотные (HF) RFID-метки работают в частотном диапазоне 3-29 МГц, более предпочтительно 13-14 МГц и особо предпочтительно 13,56 МГц. В зависимости от конструкции чипа (особенно от размера антенны) и мощности считывателя расстояние, с которого возможно считывание данных с чипа, не превышает примерно 3 м. Типичное значение максимального расстояния, считающееся приемлемым,

составляет 1 м. В некоторых случаях может оказаться желательным ограничить его еще сильнее, до нескольких сантиметров или даже до прямого контакта со считывателем.

Ультравысокочастотные (UHF) RFID-метки работают в частотном диапазоне 433-950 МГц, особо предпочтительно 860-870 МГц. UHF-метки обеспечивают увеличенные расстояния считывания, примерно до 10 м (при типичных значениях около 3 м, также зависящих от конструкции чипа), и высокие скорости считывания.

В рассматриваемом примере документ 20 - это документ типа брошюры с передней обложкой 21, задней обложкой 22 и страницами 23. Первая и вторая RFID-метки в типичном варианте могут быть интегрированы в или на одну или обе обложки. Например, в варианте по фиг. 2 HF RFID-метка 25 (для короткого расстояния) и UHF RFID-метка 26 (для увеличенного расстояния) находятся на задней обложке 22 брошюры, вместе с соответствующими антеннами 25a и 26a. В других вариантах одна метка может быть на передней обложке, а другая на задней.

Комбинация HF-метки 25 и UHF-метки 26 придает документу 20 дополнительную функциональность и защищенность. Например, HF-чип 25 для электронного паспорта (е-паспорта) может содержать сведения об UHF-чипе 26 (и/или наоборот), так что наличие UHF-чипа, встроенного в переднюю обложку е-паспорта, может служить доказательством того, что подмена чипа (чипов) паспорта не имела места.

UHF-чипы, такие как метка 26, способны содержать только очень малый объем данных (обычно только единственный код, такой как уникальный идентификатор). В отличие от этого, е-паспортный HF-чип 25 может содержать десятки килобайт данных. UHF-метки лучше подходят для считывания с больших расстояний и поэтому могут быть более удобными и менее опасными для владельца считываемого документа в отношении нарушения конфиденциальности. Поскольку в UHF-чипе не содержится никаких данных, с ним, в отличие от е-паспортных чипов, не возникает никаких серьезных вопросов в отношении гражданских свобод/прав личности. UHF-чипы относительно недороги (их стоимость составляет обычно всего несколько центов США) по сравнению HF-чипами е-паспортного типа. В общем случае, чипы по обеим технологиям могут применяться в непосредственной близости друг от друга, сохраняя функциональность обеих технологий.

Комбинирование двух технологий в одном документе 20 дает много преимуществ.

В типичном случае в е-паспортном HF-чипе 25 имеется участок, именуемый "Datagroup 13", способный содержать данные, которые не требуются согласно спецификации Международной организации гражданской авиации. В одном варианте изобретения этот участок может содержать идентификационный код в форме данных об UHF-чипе. Альтернативно, в UHF-чипе может быть запрограммирован идентификационный код в виде числа, соответствующего уникальному идентификатору чипа, записанному в HF-чипе, или данным, запрограммированным в участке "Datagroup 13". В случае использования такой методологии удаление или замена чипа становится легко обнаруживаемой, что обеспечивает более высокий уровень защищенности паспорта.

Идентификационные коды в двух RFID-метках необязательно должны быть идентичными; вместо этого они могут быть взаимосвязанными, например через базу данных или соответствующий алгоритм.

Наличие UHF-чипа создает и другие, дополнительные выгоды. Например, контроль и учет паспортов в процессе их изготовления является трудным и дорогостоящим процессом из-за наличия большого количества производственных стадий и коррекции, которая часто оказывается необходимой. Наличие в паспорте UHF-чипа сделало бы этот процесс намного проще и надежнее, обеспечив возможность отслеживания каждого документа на протяжении всего процесса, с соответствующим повышением эффективности и снижением затрат. Применение UHF-чипа облегчает отслеживание паспорта, поскольку этот чип может считываться с большого расстояния, так что мониторинг паспортов становится возможным при их изготовлении на предприятии, при упаковке в коробки, при доставке на место, где паспорта будут персонализированы, при персонализации паспортов и при выдаче паспорта заявителю. Внутри самого предприятия паспорт может отслеживаться и идентифицироваться при переносе с одного производственного участка на другой.

Одна специфичная трудность, как правило, возникающая в процессе изготовления паспорта, состоит в том, что для идентификации каждого паспорта оператору необходимо открыть его и изучить содержащуюся в нем информацию (такую как номер паспорта или имя его владельца). Это действие является неудобным и снижающим производительность. Применение UHF-чипа решает эту проблему, поскольку паспорт может быть идентифицирован автоматически соответствующим считывателем, когда он попадает в диапазон действия считывателя. Оператору больше не будет нужно открывать документ; кроме того, отпадает вероятность ошибки в отношении пользователя. Применительно к е-паспортам (например, к паспортам, содержащим также HF RFID-чип, хранящий персональные данные) эти возможности станут еще более важными в связи с их существенно более высокой ценой по сравнению с обычными паспортами. Хотя наличие HF RFID-чипа и UHF RFID-чипа в качестве непременных принадлежностей паспорта является предпочтительным, обычный е-паспорт или даже стандартный паспорт без RFID-чипа может быть сделан "отслеживаемым" путем прикрепления к нему UHF RFID-чипа на время изготовления и/или персонализации. По желанию, этот чип может быть удален на более поздней стадии. Например, UHF-чип может содержаться в ярлыке, который прикрепляется к паспорту, а затем снимается.

В случае, когда UHF и HF функциональности должны быть перманентными свойствами паспорта, оба чипа могут быть объединены в единственный чип. Это сократит общие затраты на воплощение обеих технологий в одном документе, одновременно придав паспорту дополнительную функциональность. Такое решение обеспечит дополнительный уровень аутентификации, как это описано выше, и сделает документ "отслеживаемым".

С учетом рассмотренных факторов представляется предпочтительным использовать пропускной документ 20 в вышеописанной системе иммиграционного контроля как источник уникальных идентификаторов. UHF RFID-чип 26 идеально подходит для хранения уникального идентификационного кода, который может детектироваться соответствующим UHF RFID-считывателем. При этом проверка, производимая во втором пункте, может включать проверку аутентичности документа путем считывания данных как с UHF-чипа 26, так и с HF-чипа 25 и проведения сравнения. Например, если оба чипа 25, 26 запрограммированы с включением одного и того же уникального идентификатора, сравнение кодов каждого из них позволит проверить, не был ли подменен один из чипов. Аналогично, если оба чипа 25 и 26 снабжены взаимосвязанными кодами, проверка может состоять в использовании соответствующих баз данных или алгоритма, чтобы определить, является ли взаимосвязь между чипами правильной, чтобы детектировать возможную подмену любого из них.

Таким образом, терминал (терминалы) во втором пункте 2 может (могут) содержать аутентифицирующий аппарат, снабженный считывателем (считывателями) для опрашивания первой и второй RFID-меток, и процессорные средства для проведения сравнения данных, извлеченных из каждой метки. Может оказаться достаточным использование единственного RFID-считывателя, если его можно сконфигурировать для чтения RFID-меток обоих типов, например, если он может работать на обеих нужных частотах. Альтернативно, можно использовать два специализированных считывателя. Аутентифицирующий аппарат может быть интегрирован с терминалами 50a, 50b, 50c биометрического контроля и со стандартными контрольными терминалами 40a, 40b или являться отдельным модулем.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Пропускной документ, содержащий первую метку радиочастотной идентификации (RFID-метку), считываемую только в пределах первого расстояния, и вторую RFID-метку, считываемую в пределах второго расстояния, причем первая RFID-метка содержит данные, относящиеся к владельцу пропускного документа и идентификационный код, а вторая RFID-метка содержит идентичный или связанный идентификационный код, причем второе расстояние превышает первое расстояние.

2. Документ по п.1, отличающийся тем, что первое расстояние включает максимальное расстояние считывания от первой RFID-метки, лежащее в интервале от 0 до около 3 м, предпочтительно в интервале от 0 до около 1 м.

3. Документ по п.1 или 2, отличающийся тем, что второе расстояние включает максимальное расстояние считывания от второй RFID-метки, превышающее 1 м, предпочтительно превышающее 3 м, особо предпочтительно превышающее 10 м.

4. Документ по любому из предыдущих пунктов, отличающийся тем, что указанный идентификационный код идентифицирует вторую RFID-метку, причем идентичный идентификационный код запрограммирован в первой RFID-метке.

5. Документ по любому из пп.1-3, отличающийся тем, что указанный идентификационный код идентифицирует первую RFID-метку, причем идентичный идентификационный код запрограммирован во второй RFID-метке.

6. Документ по любому из предыдущих пунктов, отличающийся тем, что данные, содержащиеся в первой RFID-метке, включают относящиеся к владельцу персональные и/или биометрические данные, предпочтительно данные по отпечаткам пальцев, шаблон (шаблоны) радужной оболочки и/или данные опознавания по лицу.

7. Документ по любому из предыдущих пунктов, отличающийся тем, что первая RFID-метка содержит высокочастотный (HF) RFID-чип, а вторая RFID-метка содержит ультравысокочастотный (UHF) RFID-чип.

8. Документ по п.7, отличающийся тем, что HF RFID-чип функционирует в частотном диапазоне 3-29 МГц, предпочтительно 13-14 МГц, особо предпочтительно 13,56 МГц.

9. Документ по п.7 или 8, отличающийся тем, что UHF RFID-чип функционирует в частотном диапазоне 433-950 МГц, предпочтительно 860-870 МГц.

10. Документ по любому из предыдущих пунктов, отличающийся тем, что первая и вторая RFID-метки интегрированы в один чип.

11. Документ по любому из предыдущих пунктов, отличающийся тем, что пропускной документ является паспортом.

12. Пропускная система, содержащая

множество пропускных документов, выполненных согласно любому из предыдущих пунктов, причем идентификационный код каждого документа уникален;

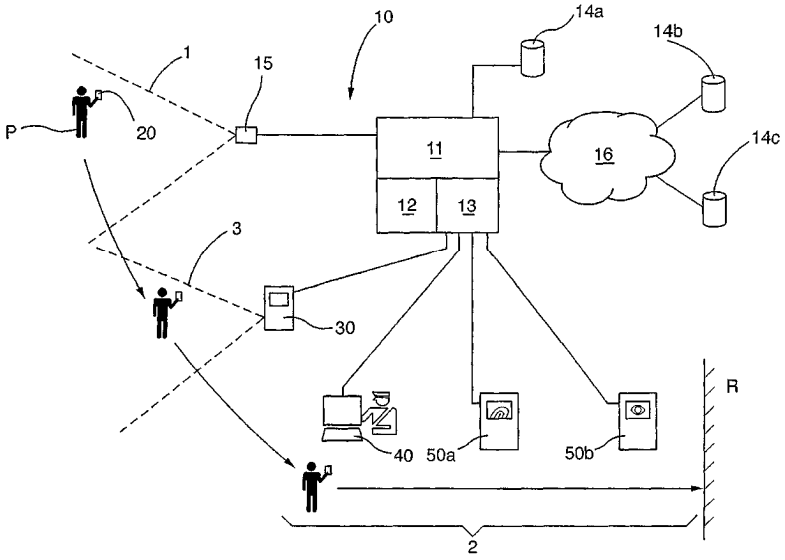
первый считыватель, выполненный с возможностью считывать данные с первых RFID-меток;

второй считыватель, выполненный с возможностью считывать данные со вторых RFID-меток;

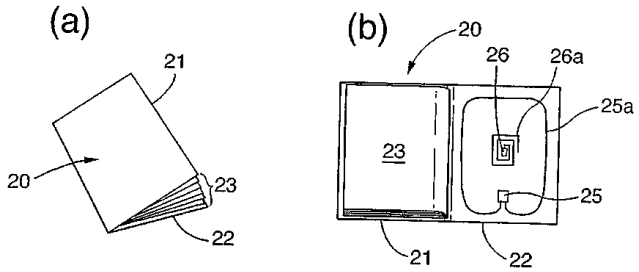
базу данных, содержащую записи данных по каждому пропускному документу, с указанием соответствующего ему идентификационного кода и сведений о владельце указанного документа; и

процессор, выполненный с возможностью в случае распознавания идентификационного кода первым или вторым считывателем извлекать из базы данных соответствующую запись данных.

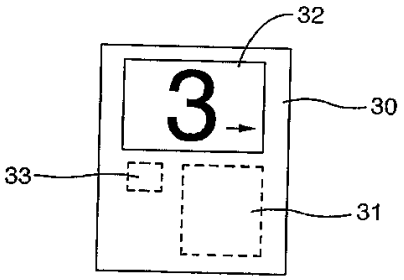
13. Система по п.12, отличающаяся тем, что процессор дополнительно подключен по меньшей мере к одной внешней базе данных и выполнен с возможностью извлекать записи, соответствующие владельцу идентифицированного пропускного документа, по меньшей мере из одной внешней базы данных.



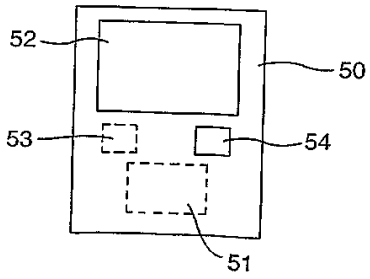
Фиг. 1



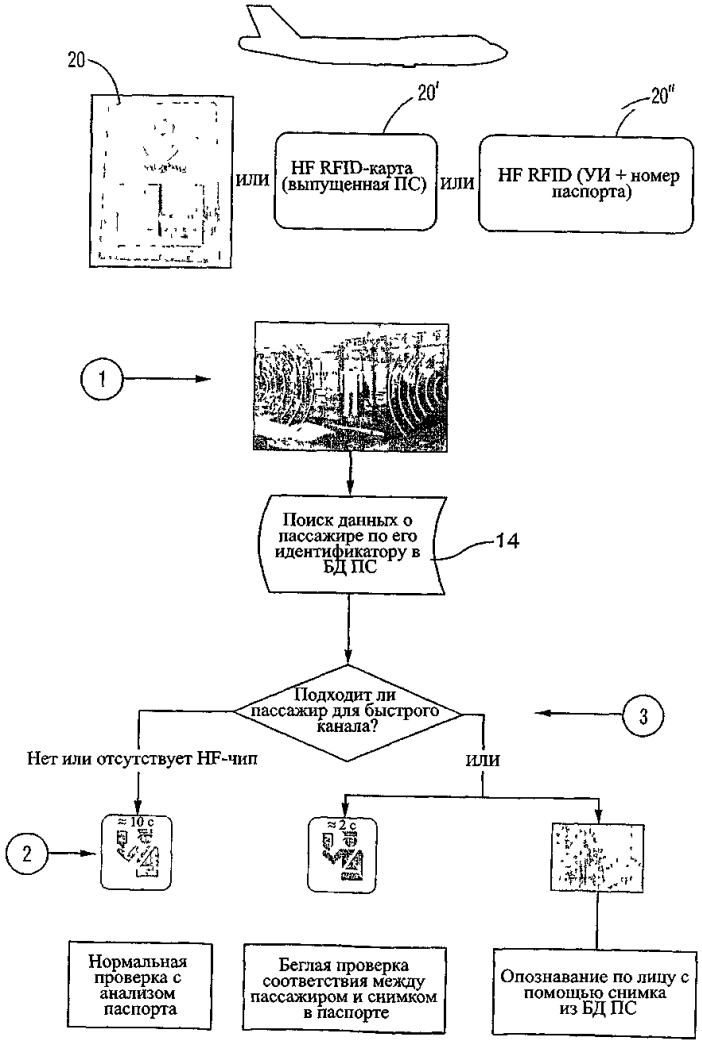
Фиг. 2



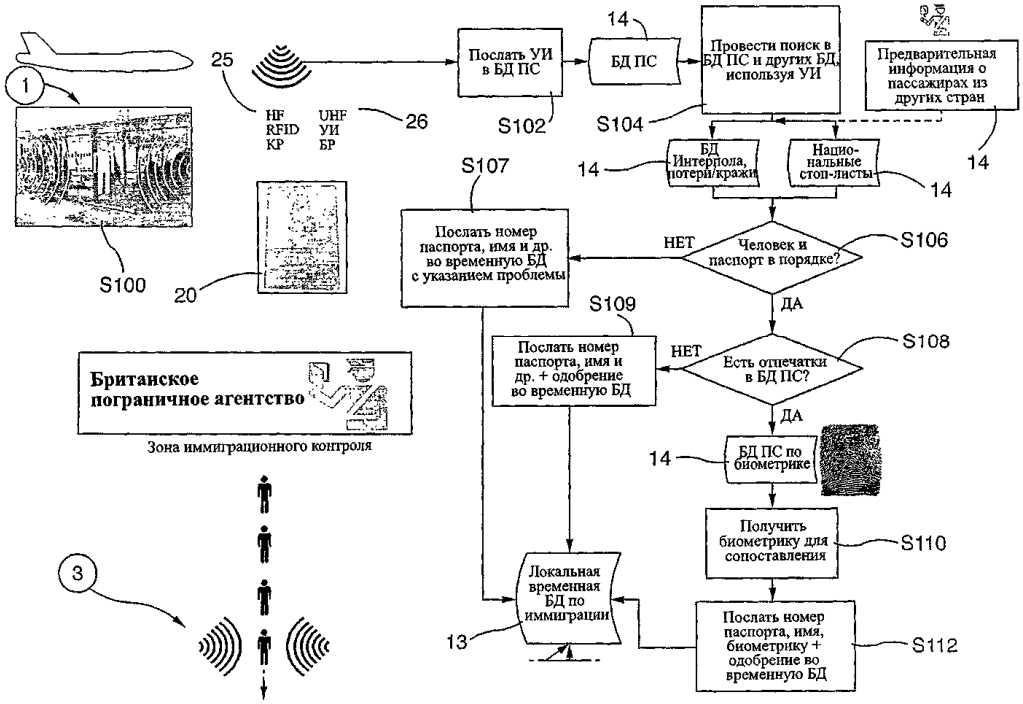
Фиг. 3


52
50
53
54
51

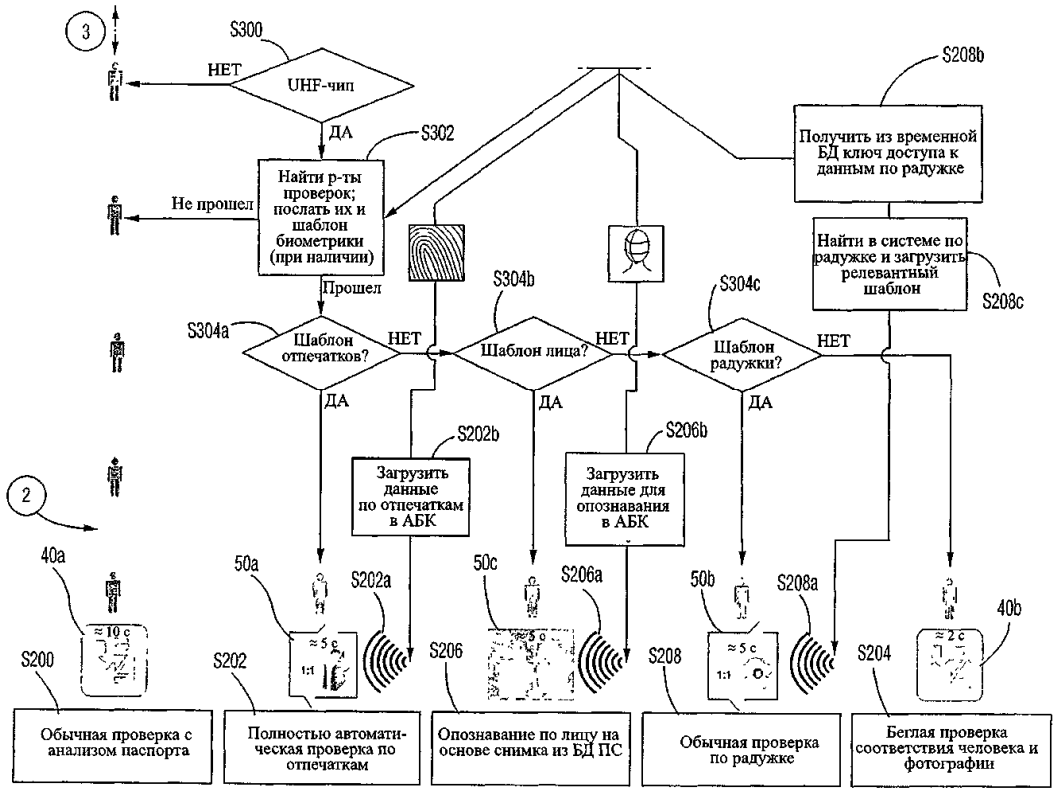
Фиг. 4


20
20'
20''
HF RFID-карта (выпущенная ПС)
ИЛИ
ИЛИ
HF RFID (УИ + номер паспорта)
1
Поиск данных о пассажире по его идентификатору в БД ПС
14
Подходит ли пассажир для быстрого канала?
3
Нет или отсутствует HF-чип
ИЛИ
2
≈ 10 с
≈ 2 с
Нормальная проверка с анализом паспорта
Беглая проверка соответствия между пассажиром и снимком в паспорте
Опознавание по лицу с помощью снимка из БД ПС

Фиг. 5



Фиг. 6



Продолжение фиг. 6