(19) Евразийское патентное ведомство

(11) 041862 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.12.09

(21) Номер заявки
201792126

(22) Дата подачи заявки
2016.09.20

(51) Int. Cl. ***B42D 25/305*** (2014.01)
G06Q 10/10 (2012.01)
B42D 25/24 (2014.01)

(54) УДАЛЕННОЕ ПРОСТАВЛЕНИЕ ОТМЕТОК В ЗАЩИЩЕННОМ ДОКУМЕНТЕ

(31) **15186661.3**
(32) **2015.09.24**
(33) **EP**
(43) **2018.08.31**
(86) **PCT/EP2016/072259**
(87) **WO 2017/050739 2017.03.30**

(71)(73) Заявитель и патентовладелец:
СИКПА ХОЛДИНГ СА (CH)

(72) Изобретатель:
Талверди Мехди (CA)

(74) Представитель:
Абильманова К.С. (KZ)

(56) US-A1-2015143535
WO-A1-2013067092
US-B1-7958147

(57) Система для удаленного проставления отметок в защищенном документе, содержащая интерфейс, выполненный с возможностью приема графических данных об отсканированном изображении защищенного документа от оборудования на участке и по сети; хранилище данных, выполненное с возможностью хранения записи данных, содержащей указанные принятые данные об изображении и дополнительные данные в отношении владельца отсканированного защищенного документа; модуль обработки графических данных, выполненный с возможностью наложения изображения отметки на изображение защищенного документа, а также выполненный с возможностью генерирования дополнительных графических данных об отсканированном изображении защищенного документа с отметкой; и модуль обеспечения доступа, выполненный с возможностью предоставления доступа к указанным дополнительным графическим данным.

041862 B1

041862 B1

041862 B1

Область техники

Настоящее изобретение относится к системам, единицам и способам для удаленного проставления отметок в паспорте и защищенном документе. В частности, настоящее изобретение относится к проставлению отметок в паспортах в качестве примера защищенного документа с соответствующими штампами, метками, визами и т.п.

Уровень техники

В большинстве стран принято, что лиц проверяют на приграничных контрольно-пропускных пунктах при въезде в страну или выезде из нее. Различные правила и законы устанавливают, разрешен ли лицам въезд или отказано ли во въезде (или выезде). Общепринятым средством является выдача виз, которые дают лицу право на въезд в страну на определенный ограниченный период (например, 30 или 90 дней и т.д.) или без ограничений. Как правило, лицо предъявляет свой паспорт на приграничном контрольно-пропускном пункте при въезде в страну, и официальное лицо проверяет состояние визы. Если въезд может быть разрешен, в паспорт ставится официальный штамп или метка, указывающая на въезд (возможно, вместе с местом въезда и датой) или сама по себе представляет визу. После покидания страны в паспорт ставится еще одна метка, так что паспорт может быть проверен для определения того, истекло ли разрешенное время, или исчерпано ли разрешенное количество въездов (повторных въездов) в страну.

Недостаток штампов и меток или, в целом, отметки, проставляемой в паспорта и другие защищенные документы, заключается в том, что место и качество отметки в документе может в большой степени варьироваться. В частности, может быть проставлен штамп (мокрая печать) плохого качества, что негативно влияет на различимость отметки, или отметка создает помеху для уже существующих отметок, что, соответственно, влияет на их различимость. Кроме того, положение соответствующих отметок (например, штампа о въезде и штампа о выезде) может не быть хорошо определено, так что официальные лица вынуждены просмотреть весь паспорт, чтобы найти штамп о въезде и чтобы найти подходящее место для штампа о выезде. Это занимает время, и сотрудник контрольно-пропускного пункта может обслужить только ограниченное количество лиц за отведенное время. Кроме того, защищенные документы, такие как паспорта, имеют только ограниченное пространство, доступное для отметок, так что нерациональное использование доступного пространства может повлечь необходимость в выдаче нового паспорта перед простановкой еще одной визы.

В то же время электронные системы для выдачи и проверки подлинности защищенных документов, таких как паспорта, идентификационные карты, визы, водительские права и т.п., в настоящее время являются общепринятой практикой в большинстве стран мира. Такие системы, как правило, содержат центральные репозитории данных, которые соединены с оборудованием и терминалами на участке посредством надежно защищенных, закрытых протоколов и каналов передачи данных. Как правило, оборудование на участке содержит терминалы ввода данных, сканеры, принтеры и т.п.

Как правило, уполномоченный персонал использует такие системы, например, на приграничных (иммиграционных) контрольно-пропускных пунктах, правительственных служебных помещениях, аэропортах и мобильных контрольно-пропускных пунктах, являющихся частью общих патрулей полиции. В частности, уполномоченный персонал может проверить защищенный документ у владельца на участке путем запроса персональных данных из защищенного документа посредством получения доступа к указанным специальным центральным репозиториям данных. Система может предоставлять результат анализа на терминал на участке, так что персонал может предпринимать соответствующее действие, например разрешить проверенному лицу пройти контрольно-пропускной пункт, задержать проверенное лицо, удостоверить проверенное лицо путем проставления штампа или метки на предъявленный защищенный документ. Например, сотрудник может направить запрос системе в отношении того, являются ли предъявленный паспорт и виза подлинными, и, соответственно, извлечь информацию о том, должна ли быть проставлена отметка в паспорте, а также может ли лицо пройти контрольно-пропускной пункт и въехать в страну или нет.

В публикации US 7314162 раскрыт способ и система для оповещения об использовании идентификационного документа путем сохранения в базе данных и оповещения владельца идентификационного документа случаев, при которых водительские права, паспорт или другие идентификационные документы государственного образца, принадлежащие этому лицу, представлены в форме идентификационных данных, тем самым упрощая раннее уведомление о хищении персональных данных.

Кроме того, в публикации US 7503488 раскрыт способ оценки риска фальсификации перед выдачей заявителю водительских прав на основе относительной вероятности фальсификации, связанной, по имеющимся сведениям, с конкретной комбинацией дополнительных идентификационных документов (например, свидетельством о рождении, паспортом, студенческим билетом и т.д.), представленных заявителем при его подаче на водительские права.

Таким образом, целью настоящего изобретения является создание системы для удаленного проставления отметок в паспорте и защищенном документе, что делает эффективным использование существующей инфраструктуры, т.е. оборудования на участке, центральной обработки данных и репозиториев, а также сетей, по которым они соединены. В частности, целью настоящего изобретения является ре-

шение проблематичного и неудовлетворительного проставления отметок в паспортах и защищенных документах.

Раскрытие сущности изобретения

Решение вышеуказанных проблем и недостатков известных замыслов обеспечивается за счет объекта изобретения по независимым пунктам формулы изобретения. Дополнительные предпочтительные варианты реализации описаны в зависимых пунктах формулы изобретения.

В соответствии с вариантом реализации настоящего изобретения предложена система для удаленного проставления отметок в защищенном документе, содержащая интерфейс, выполненный с возможностью приема графических данных об отсканированном изображении защищенного документа от оборудования на участке и по сети; хранилище данных, выполненное с возможностью сохранения записи данных, содержащей указанные принятые данные об изображении и дополнительные данные в отношении владельца отсканированного защищенного документа; модуль обработки графических данных, выполненный с возможностью наложения изображения отметки на изображение защищенного документа, а также выполненный с возможностью генерирования дополнительных графических данных об отсканированном изображении защищенного документа с отметкой; и модуль обеспечения доступа, выполненный с возможностью предоставления доступа к указанным дополнительным графическим данным.

В соответствии с вариантом реализации настоящего изобретения предложен способ удаленного проставления отметок в защищенном документе, включающий этап приема графических данных об отсканированном изображении защищенного документа от оборудования на участке и по сети; этап сохранения записи данных, содержащей указанные принятые данные об изображении и дополнительные данные в отношении владельца отсканированного защищенного документа; этап наложения изображения отметки на изображение защищенного документа, а также генерирования дополнительных графических данных об отсканированном изображении защищенного документа с отметкой; и этап предоставления доступа к указанным дополнительным графическим данным.

В целом, в вариантах реализации сеть может представлять собой проводную или беспроводную сеть или их комбинацию. Кроме того, указанные данные могут сопровождаться данными о голосе, биометрическими данными, данными биологического анализа, такими как образец крови, профиль ДНК или наблюдения и т.д. Кроме того, модуль аналитических операций может быть выполнен с возможностью сопоставления записи данных с архивными данными в репозитории или данными о данных (метаданными).

Краткое описание чертежей

Далее будут описаны варианты реализации настоящего изобретения, которые представлены для улучшенного понимания изобретательских замыслов, но которые не следует рассматривать в качестве ограничения изобретения, со ссылкой на фигуры, на которых

фиг. 1A показывает схематический вид обычного приграничного контрольно-пропускного пункта с электронным оборудованием для анализа защищенного документа;

фиг. 1B - схематический вид защищенного документа с отметками, например паспорта с визами, штампами и метками;

фиг. 2 - схематический вид применения системы для удаленного проставления отметок в паспорте и защищенном документе в соответствии с вариантом реализации настоящего изобретения;

фиг. 3 - схематический вид серверной единицы для удаленного проставления отметок в защищенном документе в соответствии еще с одним вариантом реализации настоящего изобретения;

фиг. 4 - схематический вид общего варианта реализации устройства серверной единицы для удаленного проставления отметок в защищенном документе; и

фиг. 5 - блок-схему общего варианта реализации способа работы в соответствии с вариантом реализации настоящего изобретения.

Осуществление изобретения

На фиг. 1A показан схематический вид обычного приграничного контрольно-пропускного пункта с электронным оборудованием для анализа защищенного документа. В частности, показан контрольно-пропускной пункт 30 в качестве части охранного оборудования на участке 1. В целом, термин "участок" относится ко всем местам, в которых распространено соответствующее оборудование и компоненты. Таким образом, данное оборудование на участке содержит компоненты, такие как терминал для ввода данных, терминалы с дисплеем, сканеры, принтеры и т.п. В показанном примере, контрольно-пропускной пункт 30 обеспечивает сотруднику 19 службы безопасности возможность работы, например, с терминалом 11 с дисплеем и сканером 12. При обычном сценарии лицо предъявляет защищенный документ сотруднику 19. Следовательно, предполагается, что лицо является владельцем защищенного документа и выполняется анализ и проверка правильности владения и/или соответствующей подлинности предъявленного защищенного документа.

Более конкретно, лицо предъявляет защищенный документ сотруднику 19, который, в свою очередь, может использовать сканер 12 для сканирования защищенного документа или его частей. Как правило, сканер 12 использует технологии обработки данных для извлечения информации в отношении лица (или владельца предъявленного защищенного документа), такой как имя, дата рождения и/или номер

защищенного документа в формате биографических или биометрических данных, таком как RFID-контент и т.д. В целом, любой из следующих элементов данных может представлять собой так называемые дополнительные данные в отношении лица/владельца/собственника защищенного документа: фамилию, имя, дату и место рождения, страну гражданства, место и страну проживания, номер документа, тип идентификационного документа, дату выдачи документа, место выдачи документа, биометрические данные владельца, данные об изображении или графические данные в отношении лица, отпечатков пальцев или других физических характеристик владельца документа и т.п.

Сразу после того, как сканер 12 сгенерировал такую информацию в отношении лица, данная информация может быть передана по защищенному каналу связи в центральный репозиторий 120 некоторого типа (не показан). Данный репозиторий, вероятно, представляет собой сервер или ресурсы центра хранения данных, частную сеть и/или облачную инфраструктуру, которые размещены и выполнены с возможностью анализа принятой информации в отношении проверки подлинности. Например, репозиторий может хранить данные в отношении того, имеет ли лицо право на въезд в данную страну или нет. Предполагая, что показанный контрольно-пропускной пункт 30 расположен перед выходом на посадку или безопасно соединен электронным образом (по проводной или беспроводной связи) с системой аэропорта, репозиторий может хранить данные, указывающие на то, правомерно ли лицо въехало в страну и покидает ли лицо страну в разрешенный срок действия визы. Например,репозиторий может информировать сотрудника 19 через терминал 11 с дисплеем о том, что лицо, предъявившее свой паспорт на контрольно-пропускном пункте 30, пребывало в стране дольше, чем разрешено его/ее соответствующей визой. В свою очередь, сотрудник 19 может управлять турникетом 13 для обеспечения возможности задержания лица. Само собой, сотрудник 19 также может управлять турникетом 13 для пропуска лица, если ответ от репозитория 120 указывает на то, что все в порядке.

В целом, в обычных электронных системах для анализа защищенного документа, как правило, используется участок 1 с распространенным оборудованием и центральные ресурсы некоторого типа, расположенные в одном или более центральных местах для сохранения и анализа данных. Канал может быть реализован посредством специально предназначенной линии передачи сигналов или может представлять собой некоторый тип защищенной связи по существующим сетям передачи данных, таким как интернет (например, VPN-соединение, туннели и т.д.). Данные обычные системы обладают недостатком, заключающимся в затрудненном добавлении или изменении компонентов оборудования 10 на участке.

На фиг. 1В показан схематический вид защищенного документа с отметками, например паспорта с визами, штампами и метками. В частности, показан открытый разворот паспорта в качестве примера защищенного документа 40. Как правило, в паспорте может содержаться идентификационная информация некоторого типа, такая как номер 41 паспорта. Владелец паспорта (лицо) мог подаваться на получение визы в необходимую страну, которая была выдана и соответствующим образом проставлена в паспорт 40 в виде визовой метки 42 некоторого типа. В свою очередь, данная визовая метка может содержать соответствующую идентификационную информацию и защитные признаки, такие как фотография, голограммы и т.п.

Как показано, в паспорт 40 могут быть проставлены дополнительные отметки в форме метки 43 и штампы 44, 45 и 46. Как уже указано, проставление штампов и меток может обладать различными недостатками. В частности, метка 43 может быть проставлена таким образом, что она закрывает часть ранее проставленного штампа 44. Таким образом, это может существенно повлиять на различимость штампа 44. Подобным образом, штамп 45 может быть проставлен неправильно, так что на паспорте 40 отображается только его часть. Еще одним, но не окончательным, примером является плохое качество проставленного штампа 46, что также существенно влияет на различимость. Последнее может быть результатом слишком малого количества краски или прикладываемого давления при проставлении штампа 46 в паспорт 40. Более того, штамп 46 ставят повторно таким образом, что на различимость других отметок в паспорте может быть оказано существенно влияние.

На фиг. 2 показан схематический вид применения системы для удаленного проставления отметок в паспорте и защищенном документе в соответствии с вариантом реализации настоящего изобретения. Соответствующая система 20 предусмотрена в некотором центральном месте 2 в таком смысле, что она может быть удаленной относительно различных средств на участке 1, в котором распространено оборудование для сканирования, печати, ввода/вывода данных и т.д. В целом, система 20 обеспечивает удаленное проставление отметок в защищенных документах и, таким образом, содержит интерфейс 21, выполненный с возможностью приема данных 111 об изображении отсканированного защищенного документа от оборудования на участке 1 и по сети 110. Таким образом, интерфейс 21 может принимать графические данные от любого типа сканера и источника данных на участке 1. В целом, графические данные являются данными отсканированного изображения защищенного документа в том смысле, что защищенный документ отсканирован таким образом, чтобы сгенерировать цифровое изображение в форме указанных графических данных. Таким образом, указанные графические данные могут определять значения цвета или яркости пикселов, из которых может быть составлено изображение.

Система 20 не полагается и даже не требует специализированных и особых форматов данных, а наоборот, выполнена с возможностью приема и обработки графических данных об изображении, принятых

по сети любого типа, такой как сеть Интернет, интранет, мобильные устройства и другие средства сетевой передачи данных, такие как спутники. Как следствие, для сканирования защищенного документа и генерирования соответствующих данных об изображении может быть использовано любое подходящее оборудование для сканирования. Таким образом, указанное оборудование для сканирования может содержать сканеры 12 уже существующего специально предназначенного оборудования 10 на участке, которое используется соответствующим органом/учреждением. Например, оборудование 10 на участке может быть сторонним оборудованием, предоставленным органу/учреждению вместе со специализированным центральным репозиторием, как описано и разъяснено более подробно в отношении фиг. 1. Подобным образом, оборудование для сканирования также может содержать отдельные или автономные компоненты, не являющиеся частью какого-либо специального оборудования 10 на участке, такого как сканер 12', или не зависящие от него. Кроме того, предполагается любой другой источник данных для генерирования и направления данных об изображении или цифровых данных отсканированного защищенного документа по сети 110 на интерфейс 21 системы. Система 20 дополнительно содержит хранилище 22 данных, выполненное с возможностью хранения записи данных, содержащей принятые данные об изображении и дополнительные данные в отношении владельца отсканированного защищенного документа.

В вариантах реализации настоящего изобретения предусмотрена обработка графических данных для наложения изображения отметки на изобращение защищенного документа. В соответствии с настоящим вариантом реализации система 20 содержит модуль 23 обработки графических данных, который извлекает графические данные об отсканированном изображении защищенного документа из хранилища 22 данных. Модуль 23 обработки графических данных выполнен с возможностью наложения изображения 49 отметки на изображение защищенного документа. Кроме того, модуль 23 обработки графических данных выполнен с возможностью генерирования так называемых дополнительных графических данных об отсканированном изображении защищенного документа с отметкой. Эти дополнительные графические данные могут быть также сохранены в хранилище 22 данных или в другом специальном хранилище данных. Иными словами, получают виртуальное проставление отметок в защищенном документе. Система 20 дополнительно содержит модуль 24 обеспечения доступа, выполненный с возможностью предоставления доступа к дополнительным графическим данным, которые могут храниться в хранилище 22 данных или в другом специальном хранилище данных. Благодаря модулю 24 обеспечения доступа официальные лица или другой уполномоченный персонал могут сделать запрос на осмотр 112 виртуального защищенного документа.

В целом, варианты реализации настоящего изобретения обеспечивают возможность проставления отметки в защищенном документе с хорошо определенным и проконтролированным качеством с соблюдением подобным образом хорошо определенных правил и требований. В частности, отметка может быть наложена на изображение защищенного документа в подходящем положении с использованием подходящих цветов и/или вариаций контраста. Как следствие, дополнительные графические данные обеспечивают отметку на изображении защищенного документа, которая проставляется в правильном положении с хорошо определенным заданным качеством, что, в свою очередь, может решить указанные проблемы, связанные с плохим качеством воспроизведения, плохой различимостью, эффективным использованием доступного пространства, эффективным использованием времени осмотра и т.п.

Вышеописанный вариант реализации настоящего изобретения может дополнительно обеспечивать преимущество, заключающееся в том, что оборудование, используемое на участке 1, может быть более независимым от любой централизованной единицы, в целом отвечающей за анализ данных, связанных с защищенными документами. Система 20 в соответствии с данным вариантом реализации может интегрироваться в любое существующее оборудование на участке так, что вместе с системой 20 могут работать базовые функционалы, такие как сканирование, печать, отображение информации и механическая операция, такая как открытие выхода на посадку и т.п. В частности, использование данных об изображении отсканированного защищенного документа обеспечивает возможность виртуального использования любого подходящего оборудования для сканирования на участке и использования обычной инфраструктуры сети передачи данных.

На фиг. 3 показан схематический вид серверной единицы для удаленного проставления отметок на защищенном документе, в соответствии еще с одним вариантом реализации настоящего изобретения. В данном варианте реализации функционалы системы интегрированы в серверную единицу, т.е. в форме приложения, запущенного на некотором типе ресурсов обработки (сервере, специальном аппаратном обеспечении, части центра хранения данных). Подобно системе, описанной в отношении фиг. 2, серверная единица 20' содержит интерфейс 21, выполненный с возможностью приема данных 111 об изображении отсканированного защищенного документа от оборудования 10 на участке и по сети 110. Серверная единица 20' дополнительно содержит хранилище 22 данных, выполненное с возможностью хранения записи данных, содержащей указанные принятые данные об изображении и дополнительные данные в отношении владельца отсканированного защищенного документа. Кроме того, серверная единица 20' содержит модуль 23' обработки графических данных, выполненный с возможностью наложения изображения отметки на изображение защищенного документа. Кроме того, модуль 23' обработки графических

данных выполнен с возможностью генерирования дополнительных графических данных об отсканированном изображении защищенного документа с отметкой. Эти дополнительные графические данные могут быть также сохранены в хранилище 22' данных или в другом внешнем хранилище данных. Помимо этого, серверная единица 20' содержит модуль 24 обеспечения доступа, выполненный с возможностью предоставления доступа к дополнительным графическим данным.

В данном варианте реализации интерфейс 21' реализован в виде сервера приложений, который может обеспечивать закрытое облачное оперативное управление устройством считывания, сканером, принтером и/или интегрированным устройством считывания/сканером/принтером, вне зависимости от того, что может быть установлено на участке. Сервер 21' приложений может обеспечивать другие административные функции, тем самым устраняя трудности при интегрировании любого сканера/устройства считывания/принтера в существующие сторонние электронные системы. Хранилище 22' данных может быть реализовано в виде модуля сбора данных, выполненного с возможностью сбора и сохранения всех необходимых в базе данных. Тип данных, которые могут быть сохранены, может быть ограничен или сужен национальным законодательством (например, законами о неприкосновенности). Однако сохраненные данные могут быть в форме записей данных, которые могут быть связаны с каждым случаем использования или выбранными случаями использования защищенного документа или ценного изделия (паспорта).

Запись данных может включать любое из следующего: (i) данные об изображении защищенного документа, отсканированного устройством считывания/сканером или интегрированным устройством, в том числе множество отсканированных изображений при множестве длин волн электромагнитного излучения, ультразвуковые отсканированные изображения (например, жидкостей, представляющих собой часть защищенного документа или ценных изделий), рентгеновские отсканированные изображения, лазерные отсканированные изображения и т.д.; (ii) идентификационные данные защищенного документа, такие как номер паспорта, изображение(я) или другие идентификационные данные паспорта и его содержания, в том числе места в паспорте с любыми предыдущими официальными штампами (например, визами) в данном конкретном паспорте; (iii) биометрические и/или биографические данные собственника или владельца документа или изделия, такие как отпечатки пальцев, отсканированные изображения глаза, отсканированные изображения лица, отсканированные изображения тела, данные инфракрасного термодатчика, аудиовизуальные записи и т.д.; (iv) дата, время и место каждого случая использования или выбранных случаев использования документа/изделия, в том числе, например, при каждом сканировании паспорта на объекте сканирования паспорта, таком как объект пересечения государственной границы (контрольно-пропускной пункт), транспортный узел, такой как в аэропортах, корабельные доки и железнодорожные станции, или в банках, гостиницах и т.д., или при каждом сканировании ценного изделия на объекте сканирования; (v) записи звука, изображения или видеовзаимодействий между собственниками документа/изделия и сотрудниками (персоналом) на объекте сканирования паспорта или другие записи, относящиеся к использованию документа/изделия, связанные мультимедийные метаданные (например, количество записанных кадров, частотные сигнатуры голоса или другие записанные данные) и метрики, вычисленные из таких мультимедийных метаданных (которые, например, могут быть зашифрованы и использованы для дополнения существующих технологий по борьбе с несанкционированным доступом); (vi) видеоданные, показывающие лиц, использующих паспорт или другое ценное изделие; (vii) туристическая информация, связанная с собственником или владельцем ценного изделия, например информация о прибытии и/или пункте назначения, такая как номер авиарейса, связанный с паспортом, сканируемым в аэропорту или на другом объекте сканирования паспорта; (viii) медицинская информация (например, состояние здоровья, подверженность инфекционным заболеваниям в прошлом, медицинские отчеты и т.д., связанные с собственником паспорта, лицом (например, беглецом), присутствующим на официальном объекте по сбору данных, или владельцем ценного изделия; (ix) соответствующая документация, такая как отсканированное изображение таможенных форм, отсканированные изображения вторичных документов идентификации, примечания, сделанные вовлеченными сотрудниками, и т.д.; (x) личность ответственного сотрудника, оперирующего с паспортом или другим ценным изделием, как, например, место, где сотрудник идентифицирован, например, по отпечатку пальца с помощью соответствующего оборудования, если оно установлено, или по другим биометрическим данным; и (xi) RFID-контент, причем в паспорте, этикетке или бирке (например, прикрепленной к объекту) или ценном изделии установлен RFID-чип и отсканирован на объекте сканирования (паспорта). База данных также может хранить информацию в отношении визы, въезде в страну, выезде из страны, таможенной форме, отметках о пересечении границы, штампы в паспорте или другие официальные штампы для использования при центральном (т.е. удаленном) управлении сканером, устройством считывания, принтером и/или интегрированным устройством, вне зависимости от того, что может быть установлено.

Сервер 20' может необязательно содержать модуль 23A аналитических операций, выполненный с возможностью анализа записей данных, хранящихся в хранилище 22 данных, а также с возможностью генерирования соответствующего результата анализа. Например, принятые данные 111 об изображении анализируют на идентификационные или защитные признаки, поскольку такие признаки являются общепринятыми элементами современных защищенных документов. В частности, модуль 23A аналитических операций может считывать такие идентификационные или защитные метки, связанные с дополни-

тельными данными, которые хранятся с соответствующей записью данных. Например, идентификационная метка может обеспечивать идентификацию конкретного лица, являющегося владельцем визы. В соответствии с данным примером, после этого, дополнительные данные могут указывать на допустимый регион или период, в котором и в течение которого лицо может пребывать. Если модулем 23 аналитических операций обнаружено несоответствие, может быть выдан соответствующий маркер модулю 24' обеспечения доступа. В свою очередь, модуль 24' обеспечения доступа может сгенерировать и выдать уведомление на основе результата анализа, взятого в модуле 23А аналитических операций. С помощью уведомления сотрудник на участке 1 может быть уведомлен о результате анализа, взятого в серверной единице 20' удаленным образом.

Модуль 23А аналитических операций может быть специально выполнен с возможностью анализа данных, хранящихся в базе данных, для определения в режиме реального времени потенциально неправомерного использования паспорта или другого ценного изделия, такого как когда собственником паспорта предпринимается попытка въезда в страну или выезда из нее без соответствующего въезда или выезда в прошлом, или когда собственник ценного изделия проявляет выразительные манеры поведения, такие как взволнованность. В целом, такой анализ может называться проверками правдоподобия и/или проверкой любой поступающей информации, связанной с событием (например, попыткой пересечения государственной границы), на соответствие одному или более заранее определенным правилам. Например, правило может определять то, что данному лицу требуется въехать в страну, и оно должно быть зарегистрировано соответствующим образом перед тем, как будет замечена попытка выезда из страны. В одном варианте реализации модуль 23А аналитических операций выполнен с возможностью определения того, наложена ли отметка модулем 23' графической обработки или нет. Кроме того, модуль 23А аналитических операций может быть выполнен с возможностью определения места в пределах защищенного документа, в котором наложено изображение отметки.

Кроме того, модуль 23А аналитических операций также может выполнять мониторинг внешних баз 220 данных, например, Интерпола, Европола, национальных баз криминальных данных и других баз данных, для идентификации интересующих лиц, предпринимающих попытку использования паспорта на объекте сканирования паспорта или другого ценного изделия на объекте сканирования. Кроме того, модуль 23' аналитических операций может выполнять мониторинг ограничения продолжительности пребывания для выдачи сигнала тревоги, если срок пребывания собственника паспорта "превышен" (например, не выехал из страны до даты истечения срока своей визы) или срок его пребывания "недостаточен" (например, не находился на протяжении достаточного времени в стране для получения права на специальный иммиграционный статус).

Помимо модуля 24' обеспечения доступа может быть реализован модуль 24А сигнала тревоги в качестве специального модуля сигнала тревоги, выполненного с возможностью выдачи сигнала тревоги ответственному сотруднику или другому официальному лицу, когда документ/изделие (например, паспорт или другое ценное изделие), отсканированный сотрудником, был отмечен модулем 23А аналитических операций как связанный с неправомерным использованием или вызывающий иное сомнение. Сигналы тревоги также могут быть сгенерированы при несанкционированном доступе или обнаружении другого физического повреждения серверной единицы 20' или ее модуля. Для этой цели может быть обеспечен датчик 25 (например, температуры, давления, вибрации, местоположения и т.д.), выполненный с возможностью обнаружения несанкционированного доступа. Сигналы тревоги или, более конкретно, уведомление, может быть выдано ответственному сотруднику или другому официальному лицу посредством модуля защищенной связи (который описан ниже) и/или по электронной почте, через текстовое и/или голосовое сообщение (например, на мобильный телефон) и т.д. Сигналы тревоги могут быть предоставлены любому официальному органу по всему миру в рамках закона в целях превентивной безопасности.

Может быть предусмотрен модуль 26 сетевой защиты, выполненный с возможностью защиты серверной единицы 20' от внешних атак, исходящих из сети Интернет. Модуль сетевой защиты также может содержать вышеуказанные датчики 25, подходящие для осуществления мониторинга физического несанкционированного доступа, вмешательства или другого повреждения компонентов аппаратного обеспечения специального назначения. Таким образом, модуль 26 может называться модулем сетевой защиты и защиты от несанкционированного доступа.

Модуль 27 защищенной связи может быть предусмотрен для шифрования связей между серверной единицей 20' и электронными системами вовлеченных национальных правительств, их органов, коммерческих предприятий или других потребителей, т.е. оборудования на участке, с использованием технологий шифрования в соответствии с предпочтениями потребителя и требованиями законодательства. Таким образом, модуль 27 защищенной связи может упрощать связи между серверной единицей 20' и клиентскими компьютерами, в том числе сканерами, устройствами считывания, принтерами и/или интегрированными устройствами, например, на объектах сканирования паспорта. Модуль 27 защищенной связи может быть выполнен с возможностью связи с клиентскими компьютерами в пределах каждой страны по специфической для страны VPN (Virtual Private Network - виртуальная частная сеть). В некоторых вариантах реализации может быть использована отдельная VPN для каждого объекта сканирования (паспор-

та). Специфические для страны связи упрощают обмен информацией между странами (в рамках законодательства обеих стран) посредством серверной единицы, несмотря на несовместимость между соответствующими относящимися к паспортам электронными системами различных стран.

В более общем смысле модуль 27 защищенной связи может быть выполнен с возможностью упрощения обмена информацией между обслуживаемыми потребителями, несмотря на несовместимости между их соответствующими системами путем приема данных от первого обслуживаемого потребителя, согласно первому протоколу передачи данных, с последующей передачей данных от серверной единицы второму обслуживаемому потребителю, согласно второму протоколу передачи данных, причем первый и второй протоколы передачи данных не обязательно совместимы друг с другом. Любое количество модулей серверной единицы 20' может быть интегрировано в индивидуально настроенный "блок черного ящика" и любой предоставленный модуль может быть серийно произведен в качестве автономного блока, подходящего для интегрирования с существующими сторонними электронными системами.

На фиг. 4 показан схематический вид общего варианта реализации устройства серверной единицы для анализа защищенного документа. В целом, серверная единица 20 может представлять собой любую единицу, обеспечивающую ресурсы 211 обработки (например, блок обработки, совокупность блоков обработки, ЦП, часть центра хранения/обработки данных и т.д.), ресурсы 212 памяти (запоминающее устройство, база данных, часть хранения данных) и средства 213 связи. Благодаря последнему единица 20 может поддерживать связь с сетью 110 передачи данных. Ресурсы 212 памяти могут хранить код, который предоставляет инструкции ресурсам 211 обработки во время работы для воплощения любого варианта реализации настоящего изобретения. В частности, ресурсы 212 памяти могут хранить код, который предоставляет инструкции ресурсам 211 обработки во время работы для реализации интерфейса для приема данных об изображении отсканированного защищенного документа по сети 110. Кроме того, хранилище данных может быть реализовано так, чтобы оно было выполнено с возможностью хранения записи данных, содержащей принятые данные об изображении и дополнительные данные в отношении владельца отсканированного защищенного документа.

В соответствии с настоящим вариантом реализации ресурсы 212 памяти хранят код, который предоставляет инструкции ресурсам 211 обработки во время работы для реализации модуля обработки графических данных, выполненного с возможностью наложения изображения отметки на изображение защищенного документа, а также с возможностью генерирования дополнительных графических данных об отсканированном изображении защищенного документа с отметкой, и модуля обеспечения доступа, выполненного с возможностью предоставления доступа к указанным дополнительным графическим данным.

На фиг. 5 показана блок-схема общего варианта реализации способа работы, в соответствии с вариантом реализации настоящего изобретения. Данный вариант реализации способа описан в контексте иллюстративного сценария в отношении паспортного контроля и проверки подлинности. В данном сценарии предполагается первый этап S51 (СКАНИРОВАНИЕ ЗАЩИЩЕННОГО ДОКУМЕНТА), заключающийся в сканировании защищенного документа (или ценного изделия) для генерирования соответствующих данных об изображении. Таким образом, даже в странах, в которых не используется конкретный сканер/устройство считывания/принтер, паспорта все равно сканируют с помощью соответствующего оборудования на участке на въездах в страну и/или выезде из нее с использованием существующих объектов (оборудования) сканирования паспорта в этой стране. После этого система может связаться, например, по специфической для страны VPN и по защищенной зашифрованной связи с существующими объектами сканирования паспорта для сбора и сохранения информации, связанной с каждым случаем использования паспорта. Более конкретно, на этапе S52 (ПРИЕМ ДАННЫХ ОБ ИЗОБРАЖЕНИИ) сервер или система для удаленного проставления отметок в защищенном документе принимает данные об изображении по сети.

На этапе S53 (НАЛОЖЕНИЕ ОТМЕТКИ) система выполняет обработку графических данных для наложения изображения отметки на изображение защищенного документа и выполнена с возможностью генерирования дополнительных графических данных об отсканированном изображении защищенного документа с отметкой. На этапе S54 (ПРЕДОСТАВЛЕНИЕ ДОСТУПА) предоставляют доступ к сгенерированным дополнительным графическим данным.

Вариант реализации способа может дополнительно включать этап анализа принятых данных об изображении для определения того, должна ли быть наложена и, возможно, где, отметка на изображение отсканированного защищенного документа или нет. В частности, для обнаружения любых возможных нарушений могут использоваться уже указанные механизмы (правдоподобие, соответствие правилам и т.п.). Если нарушения не обнаружены или случай использования предъявленного защищенного документа (например, паспорта) не вызывает иные подозрения, может быть сгенерирована отметка в виде "виртуального" (т.е. хранимого в цифровом формате) официального штампа, который может представлять собой, например, штамп о въезде и/или выезде, который хранится в модуле базы данных, так что к нему имеется доступ у ответственного сотрудника и, следовательно, у официальных лиц на других объектах сканирования паспорта в пределах законодательства каждой страны из пары (т.е. страны, в которой данные были собраны, и страны, в которой к ним получают доступ). В некоторых вариантах реализации си-

стема может информировать в режиме реального времени ответственного сотрудника или другое официальное лицо, отсканировавшего паспорт, в котором находятся предшествующие официальные штампы (например, визы). Например, когда собственник паспорта выезжает из страны, варианты реализации настоящего изобретения могут проинформировать ответственного сотрудника о номере страницы, на которой находится соответствующий предшествующий штамп о въезде.

Несмотря на то, что были описаны подробные варианты реализации, они служат лишь для обеспечения улучшенного понимания настоящего изобретения, определенного независимыми пунктами формулы изобретения, и их не следует рассматривать в качестве ограничения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система для анализа отсканированного изображения защищенного документа, чтобы определить, следует ли проставлять на отсканированном изображении защищенного документа соответствующую виртуальную отметку в виде штампа, метки или визы, и проставления отметки в случае положительного результата анализа, содержащая

интерфейс, выполненный с возможностью приема графических данных, представляющих собой отсканированное изображение защищенного документа, от оборудования на участке и по сети;

хранилище данных, выполненное с возможностью хранения указанных принятых графических данных и дополнительных данных в отношении владельца отсканированного защищенного документа, при этом дополнительные данные в отношении владельца отсканированного защищенного документа содержат по меньшей мере одно из следующего: фамилия и имя владельца; дата и место рождения владельца; страна гражданства владельца; место и страна проживания владельца; номер документа; тип идентификационного документа; дата выдачи документа; место выдачи документа; биометрические данные владельца; допустимый регион или период, в котором и в течение которого владелец может пребывать;

модуль обработки графических данных, выполненный с возможностью наложения изображения отметки на отсканированное изображение защищенного документа, а также выполненный с возможностью генерирования графических данных, представляющих собой отсканированное изображение защищенного документа с наложенным изображением отметки;

модуль аналитических операций, выполненный с возможностью анализа принятых графических данных, представляющих собой отсканированное изображение защищенного документа, и генерирования результата анализа, при этом анализ принятых графических данных включает определение того, накладывать ли изображение отметки на отсканированное изображение защищенного документа модулем обработки графических данных или нет, при этом принятые графические данные, представляющие собой отсканированное изображение защищенного документа, анализируются на идентификационные или защитные признаки, для идентификации соответствующих дополнительных данных, которые хранятся в хранилище данных, и определяется на основании идентифицированных соответствующих дополнительных данных, разрешено ли для данного защищенного документа наложение изображения отметки на отсканированное изображение защищенного документа модулем обработки графических данных;

модуль обеспечения доступа, выполненный с возможностью предоставления доступа уполномоченному персоналу к указанным графическим данным, представляющим собой отсканированное изображение защищенного документа с наложенным изображением отметки, для осмотра этих данных, и дополнительно выполненный с возможностью генерирования и выдачи уведомления на основе результата анализа, взятого в модуле аналитических операций, для уведомления уполномоченного персонала о том, следует ли уполномоченному персоналу инициировать наложение изображения отметки на отсканированное изображение защищенного документа модулем обработки графических данных; и

датчик, выполненный с возможностью обнаружения несанкционированного доступа к системе, при этом указанный датчик представляет собой любой из датчика температуры, датчика давления, датчика вибрации и/или датчика местоположения.

2. Система по п.1, в которой модуль анализа дополнительно выполнен с возможностью определения того, где отметка наложена модулем обработки графических данных.

3. Система по п.1 или 2, которая дополнительно содержит модуль сетевой защиты, выполненный с возможностью защиты системы от сетевых атак и/или физических атак на аппаратное обеспечение системы.

4. Система по любому из пп.1-3, которая дополнительно содержит модуль защищенной связи, выполненный с возможностью обеспечения защищенной передачи указанных данных об изображении и/или указанного уведомления.

5. Система по любому из пп.1-4, которая выполнена с возможностью связи с внешней базой данных.

6. Система по любому из пп.1-5, которая является удаленной относительно оборудования, которое выполняет сканирование защищенного документа для генерирования указанных данных об изображении.

7. Система по п.6, в которой доступ к указанным дополнительным графическим данным предостав-

ляется в место, в котором был отсканирован защищенный документ.

8. Способ анализа отсканированного изображения защищенного документа, чтобы определить, следует ли проставлять на отсканированном изображении защищенного документа соответствующую виртуальную отметку в виде штампа, метки или визы, и проставления отметки в случае положительного результата анализа, включающий этапы

приема посредством интерфейса графических данных, представляющих собой отсканированное изображение защищенного документа, от оборудования на участке и по сети,

сохранения в хранилище данных указанных принятых графических данных и дополнительных данных в отношении владельца отсканированного защищенного документа, при этом дополнительные данные в отношении владельца отсканированного защищенного документа содержат по меньшей мере одно из следующего: фамилия и имя владельца; дата и место рождения владельца; страна гражданства владельца; место и страна проживания владельца; номер документа; тип идентификационного документа; дата выдачи документа; место выдачи документа; биометрические данные владельца; допустимый регион или период, в котором и в течение которого владелец может пребывать,

посредством модуля обработки графических данных, наложения изображения отметки на отсканированное изображение защищенного документа, а также генерирования графических данных, представляющих собой отсканированное изображение защищенного документа с наложенным изображением отметки,

посредством модуля обеспечения доступа, предоставления доступа уполномоченному персоналу к указанным графическим данным, представляющим собой отсканированное изображение защищенного документа с наложенным изображением отметки, для осмотра этих данных;

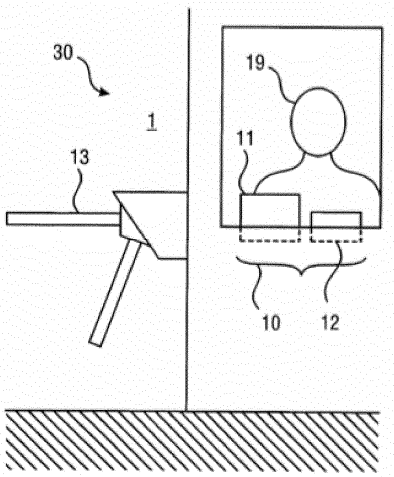
при этом способ дополнительно включает перед наложением изображения отметки на отсканированное изображение защищенного документа

посредством модуля аналитических операций анализ принятых графических данных, представляющих собой отсканированное изображение защищенного документа, и генерирование результата анализа, при этом анализ принятых графических данных включает определение того, накладывать ли изображение отметки на отсканированное изображение защищенного документа или нет, при этом принятые графические данные, представляющие собой отсканированное изображение защищенного документа, анализируются на идентификационные или защитные признаки, для идентификации соответствующих дополнительных данных, которые хранятся в хранилище данных, и определяется на основании идентифицированных соответствующих дополнительных данных, разрешено ли для данного защищенного документа наложение изображения отметки на отсканированное изображение защищенного документа модулем обработки графических данных, и

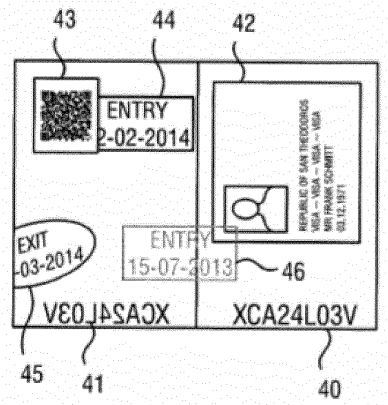
посредством модуля доступа генерирование и выдачу уведомления на основе результата анализа, проведенного в модуле аналитических операций, для уведомления уполномоченного персонала о том, следует ли уполномоченному персоналу инициировать наложение изображения отметки на отсканированное изображение защищенного документа модулем обработки графических данных; и

способ дополнительно включает обнаружение несанкционированного доступа к системе при помощи датчика, при этом указанный датчик представляет собой любой из датчика температуры, датчика давления, датчика вибрации и/или датчика местоположения.

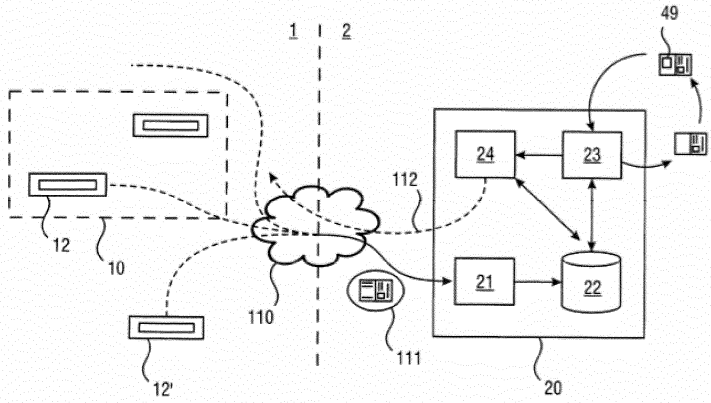
9. Способ по п.8, который дополнительно включает этап сканирования указанного защищенного документа оборудованием на участке и генерирования данных об изображении отсканированного защищенного документа, а также этап передачи данных об изображении по сети системе для анализа.



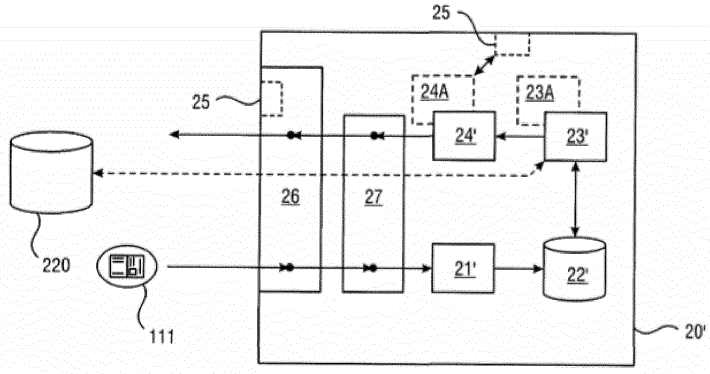
Фиг. 1А



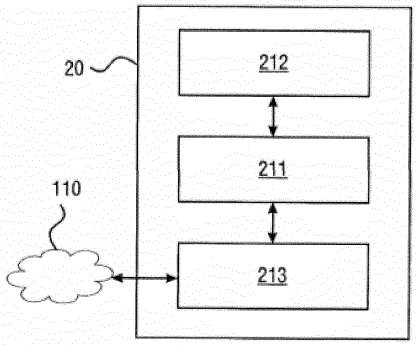
Фиг. 1B



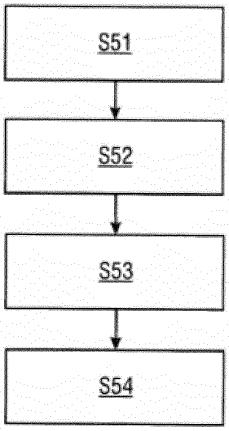
Фиг. 2



Фиг. 3



Фиг. 4



Фиг. 5