(19) Евразийское патентное ведомство

(11) 043799 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.06.26

(21) Номер заявки
201792127

(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) УДАЛЕННАЯ ПЕЧАТЬ ОТМЕТОК НА ЗАЩИЩЕННОМ ДОКУМЕНТЕ

(31) **15186696.9**
(32) **2015.09.24**
(33) **EP**
(43) **2018.08.31**
(86) **PCT/EP2016/072257**
(87) **WO 2017/050737 2017.03.30**

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

(72) Изобретатель:
Талверди Мехди (CA)

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

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

(57) Система для удаленной печати отметок на защищенном документе, содержащая интерфейс, выполненный с возможностью приема запроса на информацию в отношении отметки, подлежащей печати на защищенном документе, от оборудования на участке и по сети; модуль генерирования отметки, выполненный с возможностью генерирования данных, определяющих отметку, подлежащую печати на защищенном документе; модуль удаленного управления принтером, выполненный с возможностью управления печатающим оборудованием удаленно относительно системы для печати отметки на защищенном документе.

043799 B1

043799 B1

Область техники

Настоящее изобретение относится к системам, единицам и способам удаленной печати отметок на защищенном документе. В частности, настоящее изобретение относится к удаленному 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 то, 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, проставляемых 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 сказывается на различимости 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 проставлением еще одной визы.

Иными словами, официальные штампы (например, визовые штампы, штампы о въезде, штампы о выезде, таможенная форма) изредка неправильно ставятся в соответствующий защищенный документ (например, паспорта со штампами, проставленными в неправильной секции паспорта, такой как в пределах машиночитаемой зоны). Кроме того, официальные штампы изредка могут быть проставлены ненадлежащим образом (например, с указанием неправильной даты или времени, проставлены неравномерно, так что они размазаны или содержат неразличимые части) или в паспорт изредка ставят неправильный тип штампа (например, рабочая виза, студенческая виза и т.д.) либо официальный штамп (например, виза) может быть выдан ненадлежащим образом (например, проставлен в паспорт при том, что собственник паспорта в действительности не претендовал на выбранный официальный штамп). В дополнение к вышеуказанному, физические мокрые печати легко поддаются копированию или подделыванию иным образом.

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 указанных 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, проставить штамп или метку на предъявленном защищенном документе и т.д. 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. Кроме того, общепринятым является то, что оборудование на участке обеспечивает самоприклеивающиеся метки, например, с двумерным штрих-кодом и другими признаками, так что сотрудник может просто распечатать такую метку и проставить ее в паспорте.

В публикации US 7314162 раскрыт способ и система для оповещения об использовании идентификационного документа путем сохранения в базе данных и оповещения владельцу 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 удаленной печати отметок на защищенных документах, что делает, с одной стороны, эффективным использование существующей инфраструктуры (т.е. оборудования на участке, центральной обработки данных и репозиториев, а также сетей, по которым они соединены), а с другой стороны, является в достаточной степени защищенной и надежной, так что она может быть использована применительно к защищенным документам, таким как паспорта. В частности, целью настоящего изобретения является решение проблематичного и неудовлетворительного проставления отметок в паспортах и защищенных документах.

В дополнение к вышеуказанному, может быть желательным реагирование на хищение, копирование и/или подделывание официального штампа (например, визы) страны путем быстрой замены всех официальных штампов страны новыми штампами, имеющими новый внешний вид. Однако в случае физических мокрых печатей, обновление официального штампа включает физическую замену множества таких физических штампов, находящихся во множестве объектов приграничного контроля на государственной границе, в посольствах по всему миру и других объектах, использующих такие штампы, что занимает время и является дорогим, тем самым замедляя возможность быстрого обновления страной своих официальных штампов.

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 удаленной печати отметок на защищенном документе, содержащая интерфейс, выполненный с возможностью приема запроса на информацию в отношении отметки, подлежащей печати на защищенном документе, от оборудования на участке и по сети; модуль генерирования отметки, выполненный с возможностью генерирования данных, определяющих отметку, подлежащую печати на защищенном документе; модуль удаленного управления принтером, выполненный с возможностью управления печатающим оборудованием удаленно относительно системы для печати отметки на защищенном документе.

В соответствии с вариантом реализации настоящего изобретения предложен способ удаленной печати отметки на защищенном документе, включающий этап приема запроса на информацию в отношении отметки, подлежащей печати на защищенном документе, от оборудования на участке и по сети; этап генерирования данных, определяющих отметку, подлежащую печати на защищенном документе; этап удаленного управления печатающим оборудованием удаленно относительно системы для печати отметки на защищенном документе.

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.

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

Фиг. 1B показывает схематический вид защищенного документа с отметками, например, паспорта с визами, штампами и метками.

Фиг. 2 показывает схематический вид применения системы для удаленной печати отметок на защищенных документах, в соответствии с вариантом реализации настоящего изобретения.

Фиг. 3 показывает схематический вид серверной единицы для удаленной печати отметок на защищенных документах, в соответствии еще с одним вариантом реализации настоящего изобретения.

Фиг. 4 показывает схематический вид общего варианта реализации устройства серверной единицы для удаленной печати отметок на защищенных документах.

Фиг. 5 показывает 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 и для печати. 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 любой тип

терминала для ввода данных, камеры, 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 11с дисплеем и сканером/принтером 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.

Подобным образом если контрольно-пропускной пункт 30 является частью приграничного пункта пропуска, сотрудник 19 проверяет, может ли лицо, предъявляющее защищенный документ, въехать в страну и состояние визы какого типа следует проверить. Общепринято, что после разрешения на въезд в страну, сотрудник генерирует и проставляет визовую метку или штамп в предъявленном паспорте. В решениях, известных из уровня техники, предусмотрены мокрые печати или печать самонаклеивающихся меток, которые соответствующим образом проставляются на подходящее свободное пространство защищенного документа (например, паспорта).

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 сеть 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 податься 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 фотографии, 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 только 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 удаленной печати отметок на защищенных документах, таких как паспорта, 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 удаленную печать отметок на защищенных документах и, таким образом, содержит интерфейс 21, выполненный с возможностью приема запроса на информацию 111 от оборудования на участке 1 и по сети 110. Данный тип информации может содержать любые подходящие данные для вызова защищенного запроса на удаленную печать отметки. В частности, запрос на информацию 111 может содержать информацию для идентификации предъявленного паспорта и/или его собственника, информацию о типе запрошенной отметки, информацию о свойствах отметки (например, продолжительность разрешенного пребывания, отображаемая на отметке) и т.п. Подобным образом запрос может быть вызван путем приема данных 111 об изображении отсканированного защищенного документа. 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.

Таким образом, 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 спутник. 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 или принтеры 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 также может содержать отдельные или автономные компоненты, не являющиеся частью какого-либо специального оборудования 10 на участке, такие как сканер, принтер или интегрированное устройство 12', или не зависящие от него. Кроме того, предполагается любой другой источник данных для генерирования и направления запроса на информацию 111 в отношении защищенного документа по сети 110 на интерфейс 21 системы. Система 20 дополнительно содержит хранилище 22 данных, выполненное с возможностью хранения записи данных в отношении запроса на информацию. В случае, если предусмотрены эти данные об изображении отсканированного защищенного документа, запись данных может в значительной степени содержать принятые данные об изображении и дополнительные данные в отношении владельца отсканированного защищенного документа.

Система 20 дополнительно содержит модуль 25 генерирования отметки, который выполнен с возможностью выдачи данных, определяющих отметку, подлежащую печати на защищенном документе. Для этой цели, модуль 25 генерирования отметки также может использовать емкость хранилища 22 данных или также может в значительной степени получать доступ к отдельному специальному хранилищу данных. Для генерирования отметки, модуль 25 генерирования отметки может полагаться на разделение на постоянную и динамическую части отметки. Более конкретно, модуль 25 генерирования отметки может составлять отметку таким образом, что постоянная часть применима к нескольким отметкам, тогда как динамическая часть может зависеть от конкретного запроса на отметку. Например, постоянная часть может содержать всю информацию и элементы графического исполнения визовой отметки необходимой страны. Следовательно, динамическая часть может быть сгенерирована конкретно для отметки, подлежащей печати на необходимом защищенном документе, для отображения информации, такой как дата въезда, разрешенная продолжительность, место въезда, серийный номер, любой другой код защищенного признака и т.п.

В системе 20 может быть предусмотрен необязательный модуль 23 обработки графических данных/аналитических операций. Данный модуль 23 может быть выполнен с возможностью анализа принятого запроса на информацию в отношении генерирования соответствующего результата анализа. Таким образом, система может быть выполнена с возможностью осуществления проверки правдоподобия или соответствия правилу в ответ на принятый запрос на информацию. Например, запрос на информацию может содержать информацию, которая идентифицирует лицо, желающее въехать в данную страну, а результат анализа может указывать на то, разрешен ли лицу доступ или нет. Подобным образом результат анализа может указывать на то, действительно ли запрошенная отметка должна быть напечатана на

удаленном защищенном документе. Таким образом, модуль 23 может быть выполнен с возможностью предоставления команд модулю 24 удаленного управления принтером соответствующим образом.

Указанный модуль 24 управления принтером, содержащийся в системе 20, выполнен с возможностью удаленного управления печатающим оборудованием на участке 1 для печати отметки на защищенном документе удаленным образом. Более конкретно, модуль 24 управления принтером устанавливает канал 112 управления с соответствующим печатающим оборудованием на участке, таким как устройство 12', которое в настоящем примере представляет собой интегрированное устройство, выполненное как с возможностью сканирования предъявленного защищенного документа, так и с возможностью печати на данном документе. В соответствии с конкретным вариантом реализации настоящего изобретения модуль 24 управления принтером управляет удаленным печатающим оборудованием 12' для печати отметки, предотвращая возможность несанкционированного воспроизведения отметки. Например, модуль 24 управления принтером может предоставлять команды на печать удаленному печатающему оборудованию 12' в некоторой прерывистой последовательности, где последующая часть отметки передается от модуля 24 управления принтером только после получения соответствующей обратной связи о том, что предыдущая последовательность была напечатана на защищенном документе. Такой последовательный подход может затруднить перехват потока управляющих данных для незаконного воспроизведения отметки.

В соответствии с еще одним вариантом реализации настоящего изобретения модуль 23 в дополнение к анализу или в качестве альтернативы ему может выполнять обработку графических данных для наложения изображения отметки на изображение защищенного документа. В соответствии с настоящим вариантом реализации система 20 содержит модуль 23, который извлекает графические данные об отсканированном изображении защищенного документа из хранилища 22 данных.

Также модуль 23 может быть выполнен с возможностью последующего наложения изображения 49 отметки, предоставленного модулем 25, на изображение защищенного документа. Таким образом, модуль 23 может генерировать так называемые дополнительные графические данные 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, что преимущественно может отражать текущую отметку, напечатанную на защищенном документе. Таким образом, доступ к этим дополнительным графическим данным может обеспечить уполномоченному персоналу возможность проверки наличия отметки, напечатанной на предъявленном защищенном документе. Например, уполномоченный персонал может определить несоответствие, если внешний вид отметки, напечатанной на защищенном документе, не соответствует внешнему виду дополнительных графических данных.

В целом варианты реализации настоящего изобретения обеспечивают возможность печати отметки в защищенном документе с хорошо определенным и проконтролированным качеством с соблюдением подобным образом хорошо определенных правил и требований. В частности, отметка может быть напечатана на защищенном документе в подходящем положении с использованием подходящих цветов и/или вариаций контраста. В частности, хранилище 22 данных может хранить, или система 20 может получить из внешнего источника данных, данные, которые отражают положения отметок, напечатанных на конкретном защищенном документе в прошлом. Путем запроса и оценки таких данных, представляется возможным определение местоположения для печати отметки на защищенном документе более эффективным образом. В частности, положение отметки о выезде из страны может быть выбрано так, чтобы находиться вблизи местоположения отметки о въезде в страну. Это может обеспечить возможность легкой и быстрой обработки на контрольно-пропускных пунктах. Кроме того, ограниченное пространство защищенного документа может быть использовано более эффективно, так что в нем может располагаться большее количество отметок, предотвращая, при этом, влияние одной отметки на внешний вид и/или различимость другой отметки.

На фиг. 3 показан схематический вид серверной единицы для удаленной печати отметок, 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 запроса на информацию 111 от оборудования 10 на участке и по сети 110. Серверная единица 20' дополнительно содержит хранилище 22 данных, выполненное с возможностью хранения записи данных, содержащей любые принятые данные об изображении и дополнительные данные в отношении владельца отсканированного защищенного документа и любой принятый запрос.

Кроме того, серверная единица 20' может содержать необязательный модуль 23' аналитических операций и/или необязательный модуль 23A обработки графических данных, выполненный с возможностью оценки принятого запроса и генерирования соответствующего результата анализа, а также, соответственно, наложения изображения отметки на изображение защищенного документа. Кроме того, модуль 23A обработки графических данных выполнен с возможностью генерирования дополнительных графических дан-

ных 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, отсканированном 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 видео взаимодействий 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.

Необязательный модуль 23' аналитических операций может быть выполнен с возможностью анализа записей данных, хранящихся в хранилище 22 данных, а также с возможностью генерирования соот-

ветствующего результата анализа. В частности, модуль 23A аналитических операций может считывать идентификационные или защитные метки, связанные с дополнительными 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 или может быть выдано уведомление на основе результата анализа, взятого в модуле 23A аналитических операций. Посредством уведомления сотрудник на участке 1 может быть уведомлен о результате анализа, взятого в серверной единице 20' удаленным образом.

Модуль 23' 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 23A аналитических операций выполнен с возможностью определения того, наложена ли отметка модулем 23' графической обработки или нет. Кроме того, модуль 23A аналитических операций может быть выполнен с возможностью определения места в пределах защищенного документа, в котором наложено изображение отметки.

Кроме того, модуль 23' 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). Модуль 24' управления принтером как и в других вариантах реализации выполнен с возможностью управления удаленным принтером 12 для печати отметки, предоставленной модулем 25' генерирования отметки, на защищенном документе на участке.

Кроме того, модуль 24A сигнала тревоги может быть реализован 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 23' 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 26 (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 27 сетевой защиты, выполненный с возможностью защиты серверной единицы 20' от внешних атак, исходящих из сети Интернет. Модуль сетевой защиты также может содержать вышеуказанные датчики 26, подходящие для осуществления мониторинга физического несанкционированного доступа, вмешательства или другого повреждения компонентов аппаратного обеспечения специального назначения. Таким образом, модуль 27 может называться модулем сетевой защиты и защиты от несанкционированного доступа.

Модуль 28 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 28 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 28 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 вари-

антах реализации может быть использована отдельная VPN для каждого объекта сканирования (паспорта). 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 28 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, выполненного с возможностью запроса информации в отношении отметки, подлежащей печати на защищенном документе, от оборудования на участке и по сети. В соответствии с настоящим вариантом реализации ресурсы 212 памяти хранят код, который предоставляет инструкции ресурсам 211 обработки во время работы также для реализации модуля генерирования отметки, выполненного с возможностью генерирования данных, определяющих отметку, подлежащую печати на защищенном документе, и модуля удаленного управления принтером, выполненного с возможностью управления печатающим оборудованием удаленно относительно системы для печати отметки на защищенном документе.

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 (прием запроса на информацию), заключающийся в приеме запроса на информацию в отношении отметки, подлежащей печати на защищенном документе, от оборудования на участке и по сети. На этапе S52 (генерирование данных об отметке) генерируют данные, определяющие отметку, подлежащую печати на защищенном документе. Кроме того, на этапе S53 (удаленное управление принтером) управляют печатающим оборудованием, удаленным относительно системы, для печати отметки на защищенном документе.

Для соответствующих реализаций могут быть использованы доступные устройства считывания, сканеры и принтеры и/или интегрированные устройства для осуществления печати и/или сканирования паспорта. Изначально система может выполнять аналитические операции в режиме реального времени при каждом сканировании паспорта на объекте сканирования паспорта для определения того, совпадает ли количество и хронологический порядок въездов и выездов для проверки того, является ли собственник паспорта лицом, интересующим официальных лиц в стране, в которой был отсканирован паспорт собственника, и/или для определения того, является ли поведение собственника паспорта примечательным (например, подозрительным). Если случай использования паспорта отмечен как вызывающий сомнение, система может выдать сигнал тревоги ответственному сотруднику или другим официальным лицам, в соответствии с национальным законодательством и протоколами.

На основе собранных и переданных в систему данных может быть определен необходимый тип официального штампа (например, рабочая виза, студенческая виза и т.д.) надежным и централизованным образом. После этого система может сообщить ответственному сотруднику, работающему с оборудованием на участке (устройством считывания/принтером), заранее определенную информацию для предоставления указаний сотруднику в отношении процедур для опроса собственника паспорта. Сообщенная информация может содержать предлагаемые вопросы, которые могут содержать выбранные случайным образом вопросы, перечень пунктов для учета сотрудником перед утверждением проставления штампа, другую соответствующую информацию о порядке работы и любые их комбинации.

Если паспорт пригоден для проставления штампа, система извлекает из базы данных соответствующий шаблон официального штампа (постоянную часть) и его динамическую часть и контент (т.е. значения полей в шаблоне) и централизованным образом (т.е. удаленно) управляет принтером для печати официального штампа на паспорте (или другом защищенном или официальном документе) в соответствии с правилами в отношении расположения официального штампа для конкретной страны. В вариантах

официальный штамп может быть напечатан в случайном месте, в случайном месте в пределах конкретных границ или в месте, выбранном задействованным сотрудником (при условии того, что система определяет то, что такое место удовлетворяет правилам в отношении расположения для конкретной страны). Официальный штамп (отметка) может содержать зашифрованные данные, содержащие динамическим образом зашифрованные данные, для уровня безопасности, который недостижим физическими мокрыми печатями. Кроме того, система может управлять оборудованием на участке для печати любого количества официальных штампов, в том числе любого количества шаблонов официального штампа, несмотря на то что наиболее распространенным является один шаблон (а иногда два шаблона).

Таким образом, способ работы может дополнительно включать этап анализа любых принятых данных об изображении для определения того, должна ли быть напечатана и, возможно, где отметка на защищенном документе 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 система может быть информировать в режиме реального времени ответственного сотрудника или другого официального лица, 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.

В целом каждый шаблон отметки (официального штампа) может иметь любое подходящее художественное оформление и исполнение, в том числе конкретный цвет, затенение и тип краски (например, выбор набора картриджей или набора резервуаров для краски), используемое при печати официального штампа. Кроме того, может быть предусмотрено любое количество полей шаблона, в том числе поля шаблона, связанные с положением (например, вертикальное, горизонтальное, под конкретным углом) официального штампа на паспорте; дополнительный текст (например, наименование места, ограничения в передвижении, другие сообщения и т.д.), подлежащий динамическому включению; легко читаемые человеком и/или машиночитаемые коды (например, штрих-коды) для включения зашифрованных данных (например, идентификационных данных штампа, биометрических данных сотрудника или собственника паспорта или других идентификационных данных, зашифрованных данных, зашифрованных форм данных любого другого поля и т.д.; другие поля; и любую их комбинацию.

Подробный перечень возможных полей шаблона, из которого может быть выбрано любое количество полей шаблона для воплощения варианта реализации настоящего изобретения, может быть следующим:

1) ШТАМП_НАПРАВЛЕНИЕ=0;
2) ШТАМП_НАИМЕНОВАНИЕ_АЭРОПОРТА=1;
3) ШТАМП_НОМЕР_АЭРОПОРТА=2;
4) ШТАМП_ИМЯ_СОТРУДНИКА=3;
5) СОТРУДНИК_НОМЕР=4;
6) ВЫХОД НА ПОСАДКУСЕКЦИЯ=5;
7) ВЫХОД НА ПОСАДКУ_НОМЕР=6;
8) ВЪЕЗД_ДАТА=7;
9) ВЪЕЗД_ВРЕМЯ=8;
10) ВЫЕЗД_ДАТА=9;
11) ВЫЕЗД_ВРЕМЯ=10;
12) ДЛИТЕЛЬНОСТЬ=11;
13) ДОКУМЕНТ_ТИП=12;
14) ДОКУМЕНТ_ПОДТИП=13;
15) ДОКУМЕНТ_НОМЕР=14;
16) ДОКУМЕНТ_СТРАНА_ВЫДАЧИ=15;
17) ПАССАЖИР_ФАМИЛИЯ=16;
18) ПАССАЖИР_ИМЯ=17;
19) ПАССАЖИР_ГРАЖДАНСТВО=18;
20) ПАССАЖИР_ДАТА_РОЖДЕНИЯ=19;
21) ПАССАЖИР_ПОЛ=20;
22) ПАССАЖИР_МЕСТОРОЖДЕНИЯ=21;
23) ДОКУМЕНТ_ДАТА_ВЫДАЧИ=22;
24) ДОКУМЕНТ_МЕСТО_ВЫДАЧИ=23;

25) ДОКУМЕНТ_СРОК _ДЕЙСТВИЯ=24;
26) ПАССАЖИР_ИДЕНТИФИКАЦИОННЫЙ_КОД=25;
27) ПОЕЗДКА_ЦЕЛЬ=26;
28) ШТАМП_ИДЕНТИФИКАЦИОННЫЙ_НОМЕР=27.

Еще в одном варианте реализации настоящего изобретения система выполнена с возможностью осуществления следующего режима работы. Система принимает ввод пользователя, предоставляющий модифицированные или иные новые данные шаблона, определяет страну, к которой относятся новые данные шаблона, передает новые данные шаблона каждому элементу оборудования на участке в этой стране, отправляет сообщение сотрудникам на участке о том, что доступно обновление. Когда любые устройства из оборудования на участке затем перезапускаются или иным образом обновляются, новые данные шаблона заменяют данные шаблона, которые использовались перед этим. Распространение нового шаблона на каждый элемент оборудования на участке в этой стране может включать в себя распространение нового шаблона, например, на объектах приграничного контроля на государственной границе, в посольствах по всему миру, полицейских органах или других органах по всему миру.

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 удаленной физической печати соответствующих виртуально сгенерированных штампа, метки или визы на уже существующем физическом защищенном документе, таком как паспорт, выполненная с возможностью связи с внешней базой данных и содержащая

интерфейс, выполненный с возможностью приема запроса на информацию в отношении соответствующих виртуально сгенерированных штампа, метки или визы, подлежащих физической печати на уже существующем физическом защищенном документе, от оборудования на участке и по сети;

модуль генерирования отметки, выполненный с возможностью генерирования данных, определяющих соответствующие виртуально сгенерированные штамп, метку или визу, подлежащие физической печати на уже существующем физическом защищенном документе, при этом сгенерированные данные состоят из шаблонной части, включающей общую информацию и элементы графического исполнения, применимые ко всем виртуально сгенерированным штампам, меткам или визам, и динамической части, включающей информацию, специально сгенерированную для конкретных виртуально сгенерированных штампа, метки или визы;

модуль удаленного управления принтером, выполненный с возможностью управления печатающим оборудованием удаленно относительно системы для физической печати соответствующих виртуально сгенерированных штампа, метки или визы на уже существующем физическом защищенном документе;

модуль аналитических операций, выполненный с возможностью анализа принятых графических данных об изображении уже существующего физического защищенного документа, а также с возможностью генерирования результата анализа и определения того, должны ли быть физически напечатаны соответствующие виртуально сгенерированные штамп, метка или виза на уже существующем физическом защищенном документе или нет;

модуль защищенной связи, выполненный с возможностью обеспечения уведомления на основании результата анализа,

отличающаяся тем, что модуль аналитических операций дополнительно выполнен с возможностью определения в режиме реального времени неправомерного использования физического защищенного документа путем мониторинга баз криминальных данных для идентификации интересующих лиц, предпринимающих попытку использования физического защищенного документа, и/или проверки любой поступающей информации, связанной с использованием физического защищенного документа, на соответствие одному или более заранее определенным правилам.

2. Система по п.1, в которой модуль удаленного управления принтером выполнен с возможностью последовательной передачи частей данных команды на печать, а также выполнен с возможностью ожидания подтверждения перед передачей следующей части.

3. Система по п.1, в которой шаблонная часть хранится в центральном месте и система выполнена с возможностью централизованного обновления указанной шаблонной части.

4. Система по п.1, в которой модуль аналитических операций дополнительно выполнен с возможностью определения того, где соответствующие виртуально сгенерированные штамп, метка или виза должны быть физически напечатаны на уже существующем физическом защищенном документе.

5. Система по любому из пп.1-4, которая дополнительно содержит датчик, выполненный с возможностью обнаружения несанкционированного доступа к системе.

6. Система по п.5, в которой указанный датчик представляет собой любой из датчика температуры, датчика давления, датчика вибрации и/или датчика местоположения.

7. Система по любому из пп.1-6, которая дополнительно содержит модуль сетевой защиты, выпол-

ненный с возможностью защиты системы от сетевых атак и/или физических атак на аппаратное обеспечение системы.

8. Система по любому из пп.1-7, в которой модуль защищенной связи дополнительно выполнен с возможностью обеспечения защищенной передачи данных об изображении.

9. Система по любому из пп.1-8, которая является удаленной относительно оборудования, которое выполняет физическую печать соответствующих виртуально сгенерированных штампа, метки или визы на уже существующем физическом защищенном документе.

10. Способ удаленной физической печати соответствующих виртуально сгенерированных штампа, метки или визы на уже существующем физическом защищенном документе, таком как паспорт, включающий

этап приема запроса на информацию в отношении соответствующих виртуально сгенерированных штампа, метки или визы, подлежащих физической печати на уже существующем физическом защищенном документе, от оборудования на участке и по сети;

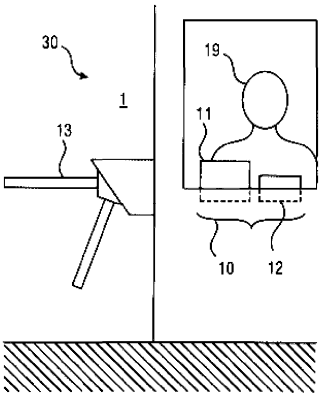
этап анализа принятых графических данных об изображении уже существующего физического защищенного документа, а также генерирования результата анализа и определения того, должны ли быть физически напечатаны соответствующие виртуально сгенерированные штамп, метка или виза на уже существующем физическом защищенном документе или нет;

этап определения в режиме реального времени неправомерного использования физического защищенного документа путем мониторинга баз криминальных данных для идентификации интересующих лиц, предпринимающих попытку использования физического защищенного документа, и/или проверки любой поступающей информации, связанной с использованием физического защищенного документа, на соответствие одному или более заранее определенным правилам;

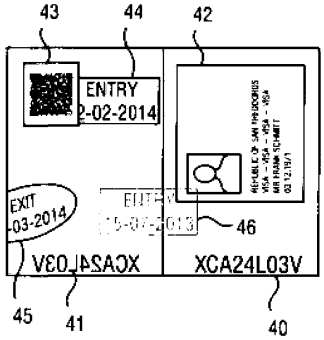
этап обеспечения уведомления на основании результата анализа;

этап генерирования данных, определяющих соответствующие виртуально сгенерированные штамп, метку или визу, подлежащие физической печати на уже существующем физическом защищенном документе, при этом сгенерированные данные состоят из шаблонной части, включающей общую информацию и элементы графического исполнения, применимые ко всем виртуально сгенерированным штампам, меткам или визам, и динамической части, включающей информацию, специально сгенерированную для конкретных виртуально сгенерированных штампа, метки или визы;

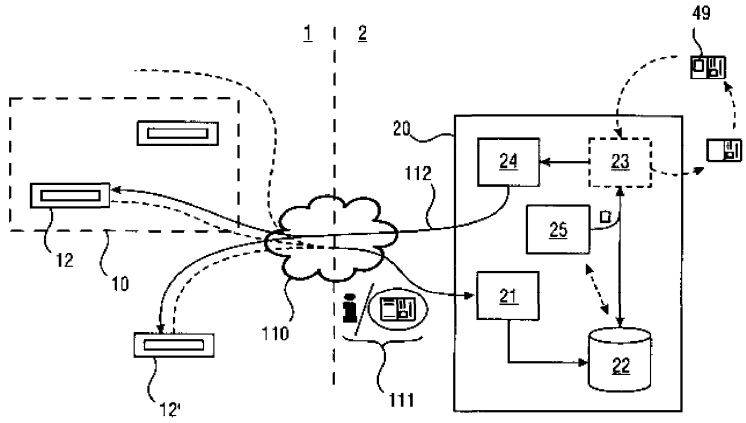
этап удаленного управления печатающим оборудованием удаленно относительно системы для физической печати соответствующих виртуально сгенерированных штампа, метки или визы на уже существующем физическом защищенном документе.



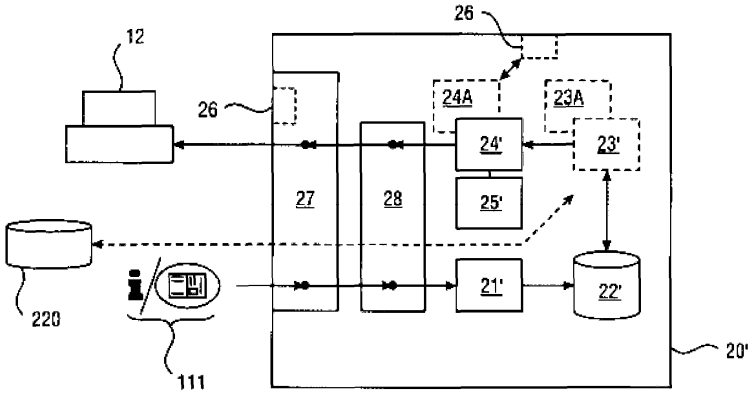
Фиг. 1A



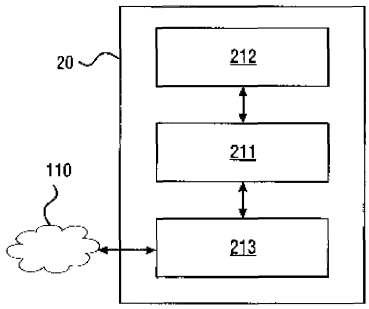
Фиг. 1B



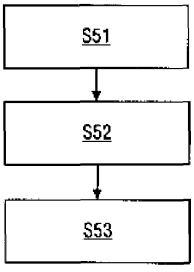
Фиг. 2



Фиг. 3



Фиг. 4



Фиг. 5