РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 676 231** (13) **C2**

(51) МПК
H04L 9/32 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 9/3226 *(2006.01);* ***H04L 9/3228*** *(2006.01);* ***H04L 9/38*** *(2006.01);* ***G06F 21/36*** *(2006.01);* ***G09C 5/00*** *(2006.01);* ***H04L 63/08*** *(2006.01);* ***H04L 63/083*** *(2006.01)*

(21)(22) Заявка: **2016100178, 13.06.2014**

(24) Дата начала отсчета срока действия патента:
13.06.2014

Дата регистрации:
26.12.2018

Приоритет(ы):
(30) Конвенционный приоритет:
13.06.2013 US 61/834,765

(43) Дата публикации заявки: **18.07.2017** Бюл. № **20**

(45) Опубликовано: **26.12.2018** Бюл. № **36**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **13.01.2016**

(86) Заявка PCT:
US 2014/042386 (13.06.2014)

(87) Публикация заявки PCT:
WO 2015/030903 (05.03.2015)

Адрес для переписки:
129090, Москва, ул. Б.Спасская, 25, строение 3, ООО "Юридическая фирма Городисский и Партнеры"

(72) Автор(ы):
АИССИ, Селим (US),
КГИЛ, Таехо (US),
ГАДДАМ, Аджит (US)

(73) Патентообладатель(и):
ВИЗА ИНТЕРНЭШНЛ СЕРВИС АССОСИЭЙШН (US)

(56) Список документов, цитированных в отчете о поиске: **US 2004/230843 A1, 18.11.2004. US 2008/263361 A1, 23.10.2008. GB 2478924 A, 28.09.2011. US 2008/0244700 A1, 02.10.2008. US 2013/0138968 A1, 30.05.2013. US 2013/0139238 A1, 30.05.2013. RU 2483476 C2, 27.05.2013.**

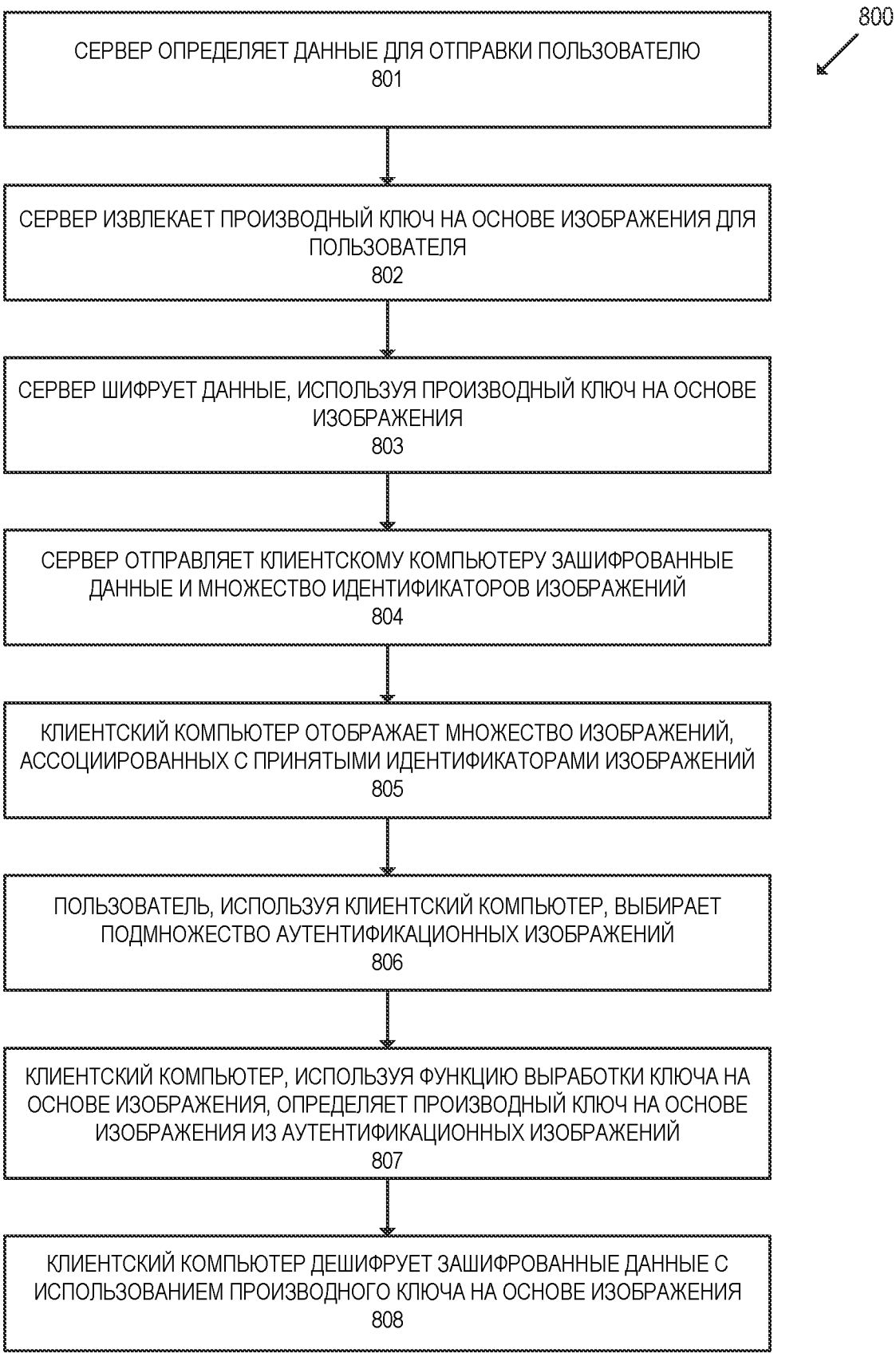
(54) ФУНКЦИЯ ВЫРАБОТКИ КЛЮЧА НА ОСНОВЕ ИЗОБРАЖЕНИЯ

(57) Реферат:

Изобретение относится к области формирования и использования производного ключа на основе изображения. Технический результат заключается в обеспечении защищенной передачи данных. В различных вариантах осуществления изобретения производный ключ на основе изображения может использоваться для упрощения аутентификации пользователей и шифрования данных. Для некоторых вариантов осуществления раскрывается способ, содержащий определение производного ключа на основе изображения, причем производный ключ на основе изображения формируется из выборки аутентификационных изображений, выбранной пользователем, шифрование данных с использованием производного ключа на основе изображения и передачу зашифрованных данных. 3 н. и 17 з.п. ф-лы, 13 ил.

RU 2676231 C2

RU 2676231 C2



ФИГ.8

RU 2676231 C2

RU 2676231 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 676 231** (13) **C2**

(51) Int. Cl.
H04L 9/32 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 9/3226 *(2006.01);* ***H04L 9/3228*** *(2006.01);* ***H04L 9/38*** *(2006.01);* ***G06F 21/36*** *(2006.01);* ***G09C 5/00*** *(2006.01);* ***H04L 63/08*** *(2006.01);* ***H04L 63/083*** *(2006.01)*

(21)(22) Application: **2016100178, 13.06.2014**

(24) Effective date for property rights:
13.06.2014

Registration date:
26.12.2018

Priority:
(30) Convention priority:
13.06.2013 US 61/834,765

(43) Application published: **18.07.2017** Bull. № **20**

(45) Date of publication: **26.12.2018** Bull. № **36**

(85) Commencement of national phase: **13.01.2016**

(86) PCT application:
US 2014/042386 (13.06.2014)

(87) PCT publication:
WO 2015/030903 (05.03.2015)

Mail address:
129090, Moskva, ul. B.Spasskaya, 25, stroenie 3, OOO "Yuridicheskaya firma Gorodisskij i Partnery"

(72) Inventor(s):
AISSI, Selim (US),
KGIL, Taekho (US),
GADDAM, Adzhit (US)

(73) Proprietor(s):
VIZA INTERNESHNL SERVIS ASSOSIEJSHN (US)

(54) IMAGE BASED KEY DERIVATION FUNCTION

(57) Abstract:

FIELD: data processing.

SUBSTANCE: invention relates to the field of generating and using an image-based derived key. In various embodiments of the invention, an image-based derived key can be used to facilitate user authentication and data encryption. For some embodiments, a method is disclosed comprising determining an image-based derived key, wherein the image-based derived key is generated from a selection of authentication images chosen by the user, encrypting data using the image-based derived key and transmitting the encrypted data.

EFFECT: secure data transfer.

20 cl, 13 dwg

RU 2676231 C2

RU 2676231 C2

ФИГ.8

RU 2676231 C2

RU 2676231 C2

ПЕРЕКРЕСТНЫЕ ССЫЛКИ НА РОДСТВЕННЫЕ ЗАЯВКИ

[0001] Настоящая заявка является обычной заявкой и испрашивает приоритет по предварительной заявке США № 61/834765, поданной 13 июня 2013 г. (номер дела поверенного № 79900-876181 (595US01)), все содержание которой во всех отношениях включается в этот документ посредством ссылки.

УРОВЕНЬ ТЕХНИКИ ИЗОБРЕТЕНИЯ

[0002] Обеспечение хорошо защищенной передачи данных является давней задачей в области компьютерной безопасности. Пароли являются широко применяемой методикой для аутентификации пользователей, при помощи которой пользователь может вводить последовательность алфавитных, цифровых или других знаков. Пароль можно сравнивать непосредственно с паролем на сервере либо хешировать и сравнивать с хэшем, сохраненным на сервере. Как только пароль проверен, можно устанавливать ключ шифрования между пользователем и сервером. Однако типичные выбранные пользователями пароли часто обладают низкой энтропией: они содержат мало знаков и распространенные шаблоны. Таким образом, для взлома паролей можно использовать атаки методом подбора, например атаки на основе универсальных графических процессоров (GPGPU). В некоторых случаях можно задавать требования к минимальной длине пароля и сложности, чтобы заставить пользователей выбирать сложные пароли. Однако увеличение сложности пароля увеличивает трудность пользователя в запоминании пароля, что может приводить к другим источникам уязвимости (например, записывание пользователем пароля в блокнот или сохранение его в электронном документе).

[0003] Варианты осуществления настоящего изобретения решают эти и другие проблемы по отдельности и вместе.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

[0004] Варианты осуществления изобретения относятся к способам формирования и использования производного ключа на основе изображения. В различных вариантах осуществления производный ключ на основе изображения может использоваться для упрощения аутентификации пользователей и шифрования данных.

[0005] Один вариант осуществления раскрывает способ, содержащий определение производного ключа на основе изображения, причем производный ключ на основе изображения формируется из выборки аутентификационных изображений, выбранной пользователем, шифрование данных с использованием производного ключа на основе изображения и передачу зашифрованных данных.

[0006] Один вариант осуществления изобретения раскрывает сервер. Сервер содержит процессор и долговременный компьютерно-читаемый носитель информации, содержащий исполняемый процессором код для реализации способа, содержащего определение производного ключа на основе изображения, причем производный ключ на основе изображения формируется из выборки аутентификационных изображений, выбранной пользователем, шифрование данных с использованием производного ключа на основе изображения и передачу зашифрованных данных.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0007] Фиг. 1 показывает систему, которая может использоваться с вариантами осуществления изобретения.

[0008] Фиг. 2 показывает пример клиентского компьютера в соответствии с некоторыми вариантами осуществления.

[0009] Фиг. 3 показывает пример сервера в соответствии с некоторыми вариантами осуществления.

[0010] Фиг. 4 показывает способ для регистрации производного ключа на основе изображения, ассоциированного с пользователем, в соответствии с некоторыми вариантами осуществления.

[0011] Фиг. 5 показывает альтернативный способ регистрации, который может использоваться с некоторыми вариантами осуществления изобретения.

[0012] Фиг. 6 показывает пример сетки, иллюстрирующей девять изображений, которые могут быть приняты от сервера и отображены клиентским компьютером, в соответствии с некоторыми вариантами осуществления.

[0013] Фиг. 7 показывает блок-схему функции выработки ключа на основе изображения (IBKDF) в соответствии с некоторыми вариантами осуществления.

[0014] Фиг. 8 показывает способ отправки зашифрованных данных от сервера к клиентскому компьютеру с использованием производного ключа на основе изображения в соответствии с некоторыми вариантами осуществления.

[0015] Фиг. 9 показывает аналогичный способ отправки зашифрованных данных от клиентского компьютера к серверу в соответствии с некоторыми вариантами осуществления.

[0016] Фиг. 10 показывает способ для аутентификации пользователя с использованием производного ключа на основе изображения в соответствии с некоторыми вариантами осуществления.

[0017] Фиг. 11 показывает систему, используемую для проведения платежа в соответствии с вариантом осуществления изобретения.

[0018] Фиг. 12 показывает пример платежного устройства в виде карты в соответствии с некоторыми вариантами осуществления.

[0019] Фиг. 13 показывает блок-схему компьютера в соответствии с некоторыми вариантами осуществления.

ПОДРОБНОЕ ОПИСАНИЕ ИЗОБРЕТЕНИЯ

[0020] Варианты осуществления изобретения относятся к способам формирования и использования производного ключа на основе изображения. В различных вариантах осуществления производный ключ на основе изображения может использоваться для упрощения аутентификации пользователей и шифрования данных.

[0021] В некоторых вариантах осуществления пользователь может выбирать подмножество изображений из множества представленных пользователю изображений. Выборка аутентификационных изображений от пользователя может использоваться для формирования производного ключа на основе изображения, используя функцию выработки ключа на основе изображения. Производный ключ на основе изображения может использоваться клиентским компьютером для шифрования отправляемых серверу данных или дешифрования принимаемых от сервера данных. К тому же производный ключ на основе изображения может использоваться сервером для шифрования отправляемых пользователю данных или дешифрования принимаемых от пользователя данных. Кроме того, производный ключ на основе изображения может использоваться для аутентификации пользователя путем сравнения ключа с предыдущим ключом, сохраненным для пользователя.

[0022] Перед дальнейшим описанием вариантов осуществления изобретения описание некоторых терминов может помочь в понимании вариантов осуществления изобретения.

[0023] "Изображение" может включать в себя любое электронное представление визуальных данных, например изображение, пиктограмму, чертеж или другое представление. Изображение может использоваться для отображения, например, двумерной сетки пикселей. Изображение может храниться в любом подходящем

формате, например в электронных форматах файлов JPEG, GIF, BMP и PNG. "Аутентификационное изображение" может включать в себя любое изображение, которое может использоваться для аутентификации пользователей. Например, сервер может хранить множество аутентификационных изображений, которые могут выбираться пользователем.

[0024] "Ключ шифрования" может включать в себя любой элемент данных или другую порцию информации, действующую для шифрования данных (например, открытого текста) в зашифрованный текст. "Ключ дешифрования" может включать в себя любой элемент данных или другую порцию информации, действующую для дешифрования зашифрованного текста в исходные данные (например, открытый текст). В некоторых вариантах осуществления ключ шифрования и ключ дешифрования может быть одним и тем же ключом (например, в системе с симметричным ключом). В таких случаях ключ шифрования может использоваться для дешифрования зашифрованного текста. В других вариантах осуществления ключи шифрования и дешифрования могут отличаться (например, в системе с асимметричным ключом).

[0025] "Функция выработки ключа" может включать в себя любую функцию, используемую для определения одного или нескольких ключей шифрования или дешифрования. Как правило, функция выработки ключа в качестве входа может принимать некое входное значение и использовать входное значение для формирования ключа. В некоторых случаях функция выработки ключа также может использовать значение соли (случайное число-модификатор), число итераций, коэффициент нагрузки и/или любой другой подходящий параметр. Функции выработки ключа можно реализовать любым подходящим образом, например, используя криптографическую хэш-функцию. Одним примером функции выработки ключа является функция 2 выработки ключа на основе пароля (PBKDF2, которая задана в RFC 2898).

[0026] "Функция выработки ключа на основе изображения" (IBKDF) может включать в себя любую функцию выработки ключа, в которой входное значение формируется из множества изображений. Изображения, используемые в качестве входа, могут определяться любым подходящим образом, например с помощью выбранного пользователем подмножества. В качестве входа может использоваться любой подходящий аспект изображения. Например, в некоторых случаях идентификатор изображения или метаданные изображения, ассоциированные с изображением, могут использоваться в качестве входа в IBKDF. В некоторых случаях к изображению может применяться хэш или другая функция, и результирующее значение может использоваться в качестве входа в IBKDF. В некоторых случаях данные, содержащие само изображение, могут использоваться в качестве входа в IBKDF.

[0027] "Производный ключ на основе изображения" может включать в себя любой криптографический ключ, сформированный с использованием функции выработки ключа на основе изображения. Производный ключ на основе изображения может иметь любой подходящий тип (например, симметричный или асимметричный) и длину.

[0028] Варианты осуществления изобретения обеспечивают преимущество установления защищенной связи с пользователем по способу, который надежнее, нежели подходы на основе пароля. Независимо от криптографической стойкости методик, используемых при аутентификации, шифровании и дешифровании, такие методики в конечном счете могут полагаться на предоставление пользователем информации, доказывающей его идентичность. Если предоставленная пользователем информация слишком простая, то она может быть уязвима к атакам методом подбора. В подходах к аутентификации пользователей на основе пароля пользователь обязан выбирать

пароль, содержащий алфавитные, цифровые или другие знаки, и воспроизводить пароль каждый раз, когда нужно аутентифицировать пользователя. Однако выбор и запоминание пароля с высокой энтропией – пароля, который имеет большую сложность, например, меняющееся применение заглавных букв и использование символов и других специальных знаков – часто является трудным для пользователей. В отличие от этого изображение, по своему характеру носителя, может содержать значительно больше энтропии, чем знак. Поскольку люди могут легче запоминать короткую последовательность изображений, нежели длинную и очень сложную последовательность знаков, пользователю легче использовать для аутентификации подмножество изображений с высокой энтропией, нежели алфавитно-цифровой пароль. Таким образом, варианты осуществления изобретения обеспечивают формирование ключей с высокой энтропией и их использование для защищенной связи без обременения пользователей. Это повышает безопасность и препятствует атакам методом подбора или атакам по радужным таблицам.

[0029] К тому же варианты осуществления изобретения обеспечивают преимущество установления защищенной связи, не требуя отдельного процесса аутентификации. В одном способе защищенной передачи данных можно сначала выполнить процесс аутентификации, и если аутентификация успешна, то можно установить сеансовый ключ шифрования между использующим клиентский компьютер пользователем и сервером. Как правило, такой процесс включал бы в себя (1) отправку клиентским компьютером аутентификационной информации (например, пароля) серверу, (2) проверку пароля сервером, (3) установление сеансового ключа клиентским компьютером и сервером, (4) отправку сервером данных, зашифрованных с использованием сеансового ключа, пользователю и (5) дешифрование пользователем зашифрованных данных с использованием сеансового ключа. Варианты осуществления изобретения могут усовершенствовать этот процесс путем сворачивания аутентификации и передачи данных в один этап, выполняемый каждым из сервера и пользователя. В частности, в соответствии с некоторыми вариантами осуществления сервер может отправлять клиентскому компьютеру данные, зашифрованные с использованием производного ключа на основе изображения, ранее определенного пользователем. Тогда клиентский компьютер может восстанавливать производный ключ на основе изображения с использованием подмножества аутентификационных изображений, указанного пользователем. Восстановленный производный ключ может использоваться для дешифрования данных. Таким образом, варианты осуществления позволяют надежно передавать данные с использованием одного сообщения, тогда как процесс последовательной аутентификации и передачи данных может требовать обмена несколькими сообщениями между сервером и клиентским компьютером. Это может быть особенно полезно в ситуациях, причем доступ к сети ненадежен или имеет большую задержку.

[0030] К тому же варианты осуществления изобретения обеспечивают преимущество создания большей безопасности на мобильных устройствах и других устройствах с ограниченными возможностями ввода. Например, ввод длинного и сложного пароля с использованием емкостной клавиатуры на мобильном телефоне может занимать много времени и приводить к ошибкам пользователя. В отличие от этого варианты осуществления изобретения предусматривают выбор пользователем подмножества аутентификационных изображений путем выбора изображений из сетки изображений. Поскольку каждое изображение обладает большей энтропией, нежели один знак, отображенные пользователю изображения можно сделать больше, и соответственно

их легче выбирать пальцем, пером или другом устройством ввода, нежели отдельными клавишами, отображенными на емкостной клавиатуре. Таким образом, варианты осуществления изобретения могут улучшить взаимодействие с пользователем по сравнению с аутентификацией на основе пароля.

[0031] Вышеприведенные примеры выделяют только некоторые преимущества использования производного ключа на основе изображения в соответствии с вариантами осуществления изобретения.

I. СИСТЕМЫ

[0032] Фиг. 1 показывает систему 100 в соответствии с вариантом осуществления изобретения. Система 100 содержит пользователя 101, который может взаимодействовать с клиентским компьютером 102. Клиентский компьютер 102 может быть подключен к серверу 104 с использованием сети 103 связи. Сеть 103 связи может быть любой подходящей компьютерной сетью, например проводной или беспроводной сетью. Сервер 104 может быть подключен к базе 106 данных пользователей, которая может хранить различные данные, связанные с пользователем 101 и/или другими пользователями, и к базе 105 данных изображений, которая может хранить различные данные, связанные с изображениями, например файлы изображений, метаданные изображений и идентификаторы изображений.

[0033] Кроме того, хотя термины "клиентский компьютер" и "сервер" для простоты объяснения в некоторых вариантах осуществления используются для описания потока информации между двумя вычислительными устройствами, следует принять во внимание, что варианты осуществления не ограничиваются отношениями "клиентский компьютер-сервер". Например, в некоторых вариантах осуществления описанные в этом документе методики также могут использоваться для упрощения одноранговой связи между двумя или более вычислительными устройствами. Таким образом, в некоторых вариантах осуществления клиентский компьютер 102 и сервер 104 могут обладать одинаковыми или аналогичными возможностями и/или функциональными возможностями, и их можно реализовать с помощью одинаковых или аналогичных компонентов. Кроме того, одно вычислительное устройство в некоторых случаях может действовать как клиентский компьютер, а в других случаях может действовать как сервер в зависимости от того, как вычислительное устройство взаимодействует с другим вычислительным устройством.

[0034] Фиг. 2 показывает пример клиентского компьютера 102 в соответствии с одним вариантом осуществления изобретения. Клиентский компьютер 102 может включать в себя любое подходящее вычислительное устройство, например настольный или переносной компьютер, планшет, смартфон или другое мобильное устройство. Клиентский компьютер 102 может содержать множество модулей, например модуль 102(A) клиентских приложений, модуль 102(B) пользовательского ввода, модуль 102 (C) выработки ключа, модуль 102(D) шифрования, модуль 102(E) хранения изображений и сетевой интерфейс 102(F). Каждый из модулей 102(A)-(F) можно реализовать с использованием любого сочетания аппаратных средств и программного обеспечения компьютера, например процессоров и компьютерно-читаемых носителей.

[0035] Модуль 102(A) клиентских приложений может конфигурироваться для выполнения одного или нескольких клиентских приложений. Клиентское приложение может включать в себя любое приложение, программное обеспечение или иной исполняемый файл. В некоторых вариантах осуществления клиентское приложение может конфигурироваться для приема от сервера множества изображений и отображения пользователю множества аутентификационных изображений. Клиентское приложение

может определять выбранное пользователем подмножество аутентификационных изображений. Клиентское приложение также может инициировать шифрование или дешифрование данных с использованием производного ключа на основе изображения, сформированного из выборки аутентификационных изображений. Клиентское приложение может взаимодействовать с любым из модулей 102(B)-(F).

[0036] Модуль 102(B) пользовательского ввода может конфигурироваться для обработки пользовательского ввода от одного или нескольких устройств пользовательского ввода, например клавиатур, мышей, сенсорных экранов и т. п. Пользовательский ввод может использоваться для определения, например, какие из множества аутентификационных изображений выбираются пользователем. Например, если аутентификационные изображения отображаются в сетке, то модуль 102(B) пользовательского ввода может использоваться для определения одного или нескольких указанных пользователем местоположений в сетке и соответствующих указанным местоположениям изображений.

[0037] Модуль 102(C) выработки ключа может конфигурироваться для выработки производных ключей на основе изображений, используя функцию выработки ключа на основе изображения (IBKDF). В некоторых вариантах осуществления функция выработки ключа на основе изображения, используемая модулем выработки ключа, в качестве входа может принимать выбранное пользователем множество изображений. В качестве входа может использоваться любой подходящий аспект изображения. Например, в некоторых случаях идентификатор изображения или метаданные изображения, ассоциированные с изображением, могут использоваться в качестве входа в IBKDF. В некоторых случаях к изображению может применяться хэш или другая функция, и результирующее значение может использоваться в качестве входа в IBKDF. В некоторых случаях в качестве входа в IBKDF можно использовать часть или все данные изображения (например, свойства пикселей у некоторых или всех пикселей на изображении) у самого изображения. В некоторых вариантах осуществления вход в IBKDF может включать в себя сочетание этих вариантов. В некоторых вариантах осуществления модуль 102(C) выработки ключа можно полностью или частично реализовать в специализированных аппаратных средствах, например, с использованием аппаратного модуля безопасности (HSM), доверенного платформенного модуля (TPM) или защищенного элемента (SE).

[0038] Модуль 102(D) шифрования может конфигурироваться для шифрования и дешифрования данных с использованием криптографических ключей. В различных вариантах осуществления модуль 102(D) шифрования может конфигурироваться для шифрования и дешифрования данных с использованием симметричных ключей (например, AES, TDES, Blowfish и т. п.) или асимметричных ключей (например, RSA и ECC) любой подходящей длины. В некоторых вариантах осуществления модуль 102(D) шифрования можно полностью или частично реализовать в специализированных аппаратных средствах, например, с использованием аппаратного модуля безопасности (HSM), доверенного платформенного модуля (TPM) или защищенного элемента (SE). Как правило, модуль 102(D) шифрования будет использовать производный ключ на основе изображения, чтобы шифровать данные для отправки серверу 104 или дешифровать принятые от сервера 104 данные.

[0039] Модуль 102(E) хранения изображений может конфигурироваться для хранения множества изображений. В некоторых вариантах осуществления множество изображений может включать в себя подмножество аутентификационных изображений, выбранное пользователем, а также множество других аутентификационных изображений. В

различных вариантах осуществления модуль 102(E) хранения изображений может принимать изображения по сети (например, от сервера), с другого носителя информации (например, переносного носителя информации) или непосредственно с камеры (например, камеры, подключенной к клиентскому компьютеру 102 или являющейся его частью).

[0040] Сетевой интерфейс 102(F) может включать в себя любое программное обеспечение и/или аппаратные средства, сконфигурированные для осуществления связи с компьютерной сетью. Сетевой интерфейс 102(F) может включать в себя любой подходящий проводной или беспроводной интерфейс, например Ethernet, WiFi, Bluetooth, NFC и т. п. Сетевой интерфейс 102(F) может использоваться для подключения клиентского компьютера 102 к любой локальной сети (LAN) или глобальной сети (WAN).

[0041] Фиг. 3 показывает пример сервера 104 в соответствии с одним вариантом осуществления изобретения. Сервер обычно является мощным компьютером или кластером компьютеров. Например, сервер может быть крупным мэйнфреймом, кластером миникомпьютеров или группой серверов, функционирующих как одно целое. В одном примере сервер может быть сервером баз данных, соединенным с веб-сервером. Сервер 104 может содержать множество модулей, например модуль 104(A) регистрации пользователей, модуль 104(B) аутентификации пользователей, модуль 104(C) выработки ключа, модуль 104(D) шифрования, модуль 104(E) выбора изображений и сетевой интерфейс 104(F). Каждый из модулей 104(A)-(F) можно реализовать с использованием любого сочетания аппаратных средств и программного обеспечения компьютера, например процессоров и компьютерно-читаемых носителей. К тому же сервер 104 может быть соединен с базой 105 данных изображений и/или базой 106 данных пользователей.

[0042] Модуль 104(A) регистрации пользователей может конфигурироваться для регистрации пользователей на сервере 104. Регистрация пользователя может содержать, например, отправку клиентскому компьютеру множества аутентификационных изображений, прием от клиентского компьютера подмножества аутентификационных изображений, выбранного пользователем 101, и сохранение подмножества выбранных изображений в записи базы данных, ассоциированной с пользователем 101 (например, в базе 106 данных пользователей). Модуль 104(A) регистрации пользователей также может конфигурироваться для приема другой информации, относящейся к пользователю 101, например личной информации, платежной информации или любой другой подходящей информации.

[0043] Модуль 104(B) аутентификации пользователей может конфигурироваться для аутентификации пользователей. Как правило, модуль 104(B) аутентификации пользователей может аутентифицировать пользователей, ранее зарегистрированных на сервере 104. Аутентификация пользователя может содержать, например, прием подмножества аутентификационных изображений, выбранного пользователем 101, формирование производного ключа на основе изображения с использованием подмножества аутентификационных изображений и функции выработки ключа на основе изображения и сравнение производного ключа на основе изображения с ключом, сохраненным ранее для пользователя 101 (например, в базе 106 данных пользователей).

[0044] Модуль 104(C) выработки ключа может конфигурироваться для выработки производных ключей на основе изображений, используя функцию выработки ключа на основе изображения (IBKDF). В некоторых вариантах осуществления функция выработки ключа на основе изображения, используемая модулем выработки ключа, в

качестве входа может принимать выбранное пользователем множество изображений. В качестве входа может использоваться любой подходящий аспект изображения. Например, в некоторых случаях идентификатор изображения или метаданные изображения, ассоциированные с изображением, могут использоваться в качестве входа в IBKDF. В некоторых случаях к изображению может применяться хэш или другая функция, и результирующее значение может использоваться в качестве входа в IBKDF. В некоторых случаях в качестве входа в IBKDF можно использовать часть или все данные изображения (например, свойства пикселей у некоторых или всех пикселей на изображении) у самого изображения. В некоторых вариантах осуществления вход в IBKDF может включать в себя сочетание этих вариантов. В некоторых вариантах осуществления модуль 104(C) выработки ключа можно полностью или частично реализовать в специализированных аппаратных средствах, например, с использованием аппаратного модуля безопасности (HSM), доверенного платформенного модуля (TPM) или защищенного элемента (SE).

[0045] Модуль 104(D) шифрования может конфигурироваться для шифрования и дешифрования данных с использованием криптографических ключей. В различных вариантах осуществления модуль 104(D) шифрования может конфигурироваться для шифрования и дешифрования данных с использованием симметричных ключей (например, AES, TDES, Blowfish и т. п.) или асимметричных ключей (например, RSA и ECC) любой подходящей длины. В некоторых вариантах осуществления модуль 104(D) шифрования можно полностью или частично реализовать в специализированных аппаратных средствах, например, с использованием аппаратного модуля безопасности (HSM), доверенного платформенного модуля (TPM) или защищенного элемента (SE). Как правило, модуль 104(D) шифрования будет использовать производный ключ на основе изображения, чтобы либо шифровать данные для отправки клиентскому компьютеру 102, либо дешифровать принятые от клиентского компьютера 102 данные.

[0046] Модуль 104(D) выбора изображений может конфигурироваться для определения изображений для отправки клиентскому компьютеру 102 в процессе регистрации, аутентификации или шифрования. Изображения могут выбираться любым подходящим образом. Например, в некоторых вариантах осуществления изображения могут выбираться случайно, в некоторых вариантах осуществления выбранные изображения могут соответствовать некой теме или категории, выбранной пользователем. Например, если пользователь 101 выбрал категорию изображений, соответствующую "водным объектам", то модуль 104(D) выбора изображений может извлекать только изображения, включающие в себя озера, океаны, реки или другие водные объекты. В некоторых вариантах осуществления для способов шифрования или аутентификации может выбираться множество изображений, содержащее выборку аутентификационных изображений от пользователя, а также может выбираться случайное подмножество других изображений.

[0047] Сетевой интерфейс 104(F) может включать в себя любое программное обеспечение и/или аппаратные средства, сконфигурированные для осуществления связи с компьютерной сетью. Сетевой интерфейс 104(F) может включать в себя любой подходящий проводной или беспроводной интерфейс, например Ethernet, WiFi, Bluetooth, NFC и т. п. Сетевой интерфейс 104(F) может использоваться для подключения клиентского компьютера 102 к любой локальной сети (LAN) или глобальной сети (WAN).

[0048] База 105 данных изображений может хранить множество изображений. Изображения могут быть общедоступными изображениями (например, фотографиями

из банка фотографий) или личными изображениями (например, изображениями, взятыми из личного репозитория пользователя). В некоторых вариантах осуществления база 105 данных изображений может хранить данные изображений (например, файлы изображений) самих изображений. В других вариантах осуществления база 105 данных изображений может хранить относящиеся к изображениям метаданные, например идентификатор изображения, хэш изображения и т. п., без хранения фактических изображений.

[0049] База 106 данных пользователей может хранить информацию о множестве пользователей. База 106 данных пользователей может содержать, например, идентификатор пользователя для каждого из пользователей, производный ключ на основе изображения для пользователей и хэш или другой защищенный индикатор выбранного пользователем подмножества аутентификационных изображений. В некоторых вариантах осуществления, если пользователь выбрал тему или категорию для аутентификационных изображений, то эту тему или категорию также можно сохранить в базе 106 данных пользователей.

II. СПОСОБЫ РЕГИСТРАЦИИ

[0050] Фиг. 4 показывает способ 400 для регистрации производного ключа на основе изображения, ассоциированного с пользователем 101. Как правило, способ 400 может выполняться перед защищенной связью между клиентским компьютером 102 и сервером 104, как описано в способах 800 и 900, и перед способом аутентификации, например способом 1000. Например, в одном варианте осуществления способ 400 может выполняться, когда пользователь создает учетную запись на сервере 104.

[0051] На этапе 401 сервер 104 предоставляет клиентскому компьютеру 102 множество аутентификационных изображений. Множество аутентификационных изображений может выбираться сервером 104 с использованием модуля 105(E) выбора изображений и может содержать любой подходящий набор изображений (например, набор изображений, сохраненный в базе 105 данных изображений). В некоторых вариантах осуществления пользователь 101 может выбирать категорию или тему для набора изображений, например водные объекты, президенты Соединенных Штатов и т. п. В других вариантах осуществления изображения могут выбираться случайно из всех хранимых сервером 104 изображений.

[0052] На этапе 402 клиентский компьютер 1022 отображает пользователю 101 множество аутентификационных изображений. Множество изображений может отображаться в любом подходящем формате. В некоторых вариантах осуществления клиентский компьютер 102 может отображать аутентификационные изображения в сетке, чтобы каждая клетка в сетке была разным изображением. В других вариантах осуществления клиентский компьютер 102 может единовременно отображать одно из множества изображений, но позволять пользователю рекурсивно просматривать множество изображений (например, используя кнопку). В еще одних вариантах осуществления клиентский компьютер 102 может проводить показ слайдов из множества изображений.

[0053] Фиг. 6 показывает пример сетки 600, иллюстрирующей девять изображений, которые могут быть приняты от сервера 104 и отображены клиентским компьютером 102. Как показано на фиг. 6, сетка 600 может включать в себя изображения здания, мужчины в костюме, футболиста, машины, ребенка, самолета, баскетболиста, мужчины, фотографирующего другого мужчину, и дома. Хотя показанные в сетке 600 изображения являются набросками, варианты осуществления изобретения могут использовать цветные изображения (например, фотографии), полутоновые изображения, анимации

или любые другие подходящие визуальные представления.

[0054] На этапе 403 пользователь 101 выбирает подмножество аутентификационных изображений из множества изображений. Выбранное пользователем 101 подмножество изображений может включать в себя одно изображение либо может включать в себя несколько изображений. К тому же подмножество может быть неупорядоченным (то есть не важен порядок, в котором выбираются изображения) либо упорядоченным (то есть фиксируются изображения и порядок, в котором они выбираются). Пользователь 101 может выбирать подмножество аутентификационных изображений любым подходящим образом. Например, если пользователь 101 использует мобильное устройство с емкостным сенсорным экраном, то пользователь 101 может касаться изображений для их выбора. Если пользователь 101 использует настольный или переносной компьютер с клавиатурой и мышью, то пользователь 101 может щелкать кнопкой на изображениях для их выбора. Один или несколько элементов в клиентском компьютере 102, например модуль 102(A) клиентских приложений и/или модуль 102(B) пользовательского ввода, может фиксировать выборку от пользователя 101.

[0055] Сетка 600 показывает три выбранных пользователем 101 изображения: футболиста, баскетболиста и дома, которые указаны, например, выделенной границей изображения.

[0056] На этапе 404 клиентский компьютер 102 отправляет серверу 104 подмножество аутентификационных изображений, выбранное пользователем 101. В некоторых вариантах осуществления сервер 104 можно отправлять сами выбранные изображения. Например, клиентский компьютер 102 может отправлять серверу 104 множество файлов изображений (например, файлы JPG, PNG или BMP).

[0057] В других вариантах осуществления серверу 104 можно отправлять координаты строки и столбца у выбранных изображений в сетке изображений. Например, для показанной в сетке 600 выборки соответствующими координатами могут быть [(1, 3), (3, 1), (3,3)]. Координата (1, 3) указывает первую строку и третий столбец, указывая изображение футболиста. Координата (3, 1) указывает третью строку и первый столбец, указывая изображение баскетболиста. Координаты (3,3) указывают третью строку и третий столбец, указывая изображение дома. Таким образом, список координат [(1, 3), (3, 1), (3,3)] может использоваться для указания выбранного подмножества аутентифицированных изображений, отправленных серверу 104.

[0058] В других вариантах осуществления можно передавать уникальные идентификаторы, соответствующие каждому выбранному изображению. В одном примере сервер 104 может вести базу данных из 1000 изображений, пронумерованных от 0 до 999. Например, изображение футболиста может иметь номер 523, изображение баскетболиста может иметь номер 135, а изображение дома может иметь номер 878. Таким образом, серверу 104 может передаваться сочетание уникальных идентификаторов 523135878 для указания секретной выборки изображений.

[0059] В еще одних вариантах осуществления серверу 104 можно отправлять значения хэшей выбранных изображений. Значения хэшей можно вычислять, например, путем выполнения некой хэш-функции над изображением.

[0060] На этапе 405 сервер 104 определяет производный ключ на основе изображения из выбранных пользователем 101 изображений и функции выработки ключа на основе изображения. "Функция выработки ключа на основе изображения" (IBKDF) может включать в себя любую функцию выработки ключа, в которой входное значение формируется из множества изображений. В качестве входа может использоваться любой подходящий аспект изображения. Например, в некоторых случаях идентификатор

изображения или метаданные изображения, ассоциированные с изображением, могут использоваться в качестве входа в IBKDF. В некоторых случаях к изображению может применяться хэш или другая функция, и результирующее значение может использоваться в качестве входа в IBKDF. В некоторых случаях в качестве входа в IBKDF можно использовать часть или все данные изображения (например, свойства пикселей у некоторых или всех пикселей на изображении) у самого изображения. В некоторых вариантах осуществления вход в IBKDF может включать в себя сочетание этих вариантов. IBKDF в качестве входа также может принимать некоторое количество других параметров, например, значение соли (например, число или строку), число итераций или коэффициент нагрузки и нужную длину ключа. Один пример IBKDF, которая может использоваться в некоторых вариантах осуществления изобретения, показан на фиг. 7.

[0061] На этапе 406 сервер 104 сохраняет производный ключ на основе изображения в базе 106 данных пользователей. Как правило, производный ключ на основе изображения ассоциируется с записью в базе 106 данных пользователей, соответствующей пользователю 101. К тому же в некоторых вариантах осуществления хэши и/или идентификаторы изображений, соответствующие выбранным аутентификационным изображениям, также можно хранить в базе 106 данных пользователей.

[0062] Следует отметить, что хотя способ 400 описывает один возможный способ регистрации, варианты осуществления изобретения не ограничиваются упомянутым способом. Например, фиг. 5 показывает альтернативный способ 500 регистрации, который может использоваться с некоторыми вариантами осуществления изобретения. Этапы 501-503 способа 500 соответственно аналогичны этапам 401-403 способа 400. Однако, тогда как на этапе 404 способа 400 клиентский компьютер 102 отправляет серверу 104 подмножество выбранных аутентификационных изображений, на этапе 504 способа 500 клиентский компьютер 102 определяет производный ключ на основе изображения из выбранных аутентификационных изображений с использованием функции выработки ключа на основе изображения. Затем на этапе 505 клиентский компьютер 104 отправляет серверу 104 производный ключ на основе изображения, а на этапе 506 сервер сохраняет производный ключ на основе изображения в базе 506 данных пользователей. Таким образом, в способе 500 производный ключ на основе изображения вырабатывает клиентский компьютер 102, а не сервер 104.

[0063] К тому же, хотя способы 400 и 500 включают в себя соответственно этапы 401 и 501, упоминающие сервер 104, предоставляющий множество изображений клиентскому компьютеру 102 в некоторых вариантах осуществления, такие этапы выполнять не нужно. Например, в некоторых вариантах осуществления выбранные клиентским компьютером 102 изображения могут сохраняться клиентским компьютером 102 заранее (например, в модуле 102(E) хранения изображений). Например, пользователь 101 может выбирать изображения, снятые ранее камерой, присоединенной к клиентскому компьютеру 102. В таких случаях серверу 104 не нужно хранить изображения в базе 105 данных изображений.

III. СПОСОБЫ ВЫРАБОТКИ КЛЮЧА

[0064] Фиг. 7 показывает блок-схему 700 функции выработки ключа на основе изображения (IBKDF) в соответствии с одним вариантом осуществления изобретения. Как показано на фиг. 7, IBKDF включает в себя некоторое количество параметров, например значение изображения (I), длину ключа (Klen), значение соли (S) и число итераций (C). Результатом IBKDF является итоговый ключ (K).

[0065] Значение изображения (I) может представлять числовое значение, ассоциированное с выборкой аутентификационных изображений. В некоторых вариантах осуществления значение изображения может формироваться путем объединения идентификаторов для каждого выбранного изображения. Для показанной в сетке 600 выборки в одном варианте осуществления изображение футболиста может иметь номер 523, баскетболист может иметь номер 135, а дом может иметь номер 878. Таким образом, в качестве входа в IBKDF может использоваться значение изображения, равное 523135878. В некоторых вариантах осуществления значение изображения может отправляться клиентским компьютером 102 серверу 104. В других вариантах осуществления значение изображения может вычисляться сервером 104 с использованием данных, отправленных клиентским компьютером 102. Например, если выбранные изображения идентифицировались клиентским компьютером 102 в формате строка-столбец, то сервер 104 может обращаться к сетке изображений для определения идентификаторов для каждого сообщения.

[0066] Соль (S) может быть случайными или алгоритмически сформированными данными. Например, в некоторых вариантах осуществления для формирования значения соли может использоваться утвержденный FIPS 149-2 генератор случайных двоичных последовательностей. В некоторых вариантах осуществления соль может быть специфичной для пользователя. Например, соль может включать в себя идентификатор пользователя для пользователя 101.

[0067] Число итераций (C) может включать в себя количество повторений функции IBKDF, которое нужно выполнить для формирования итогового ключа. Например, число итераций можно увеличивать для препятствия атакам методом подбора или атакам по радужным таблицам на сформированные IBKDF. В различных вариантах осуществления число итераций можно регулировать на основе нужного компромисса между скоростью вычисления производного ключа и безопасностью.

[0068] Длина ключа (Klen) может быть параметром, используемым для задания длины сформированного ключа. В некоторых вариантах осуществления большая длина ключа может указывать более защищенный ключ, но может требовать дополнительной обработки для его формирования.

[0069] Как только определяются все параметры для IBKDF, формируется производный ключ на основе изображения. IBKDF может использовать любой подходящий алгоритм формирования ключа. Например, может использоваться стандарт PBKDF2 (функция 2 выработки ключа на основе пароля). Результатом IBKDF является итоговый ключ (K) на основе выбранного подмножества аутентификационных изображений.

IV. СПОСОБЫ ШИФРОВАНИЯ ДАННЫХ

[0070] Фиг. 8 показывает способ 800 отправки зашифрованных данных от сервера 104 к клиентскому компьютеру 102 с использованием производного ключа на основе изображения. Как правило, способ 800 может выполняться после того, как ассоциированный с клиентским компьютером 102 пользователь зарегистрировался на сервере 104 (например, в соответствии со способами 400 или 500).

[0071] На этапе 801 сервер 104 определяет данные для отправки пользователю 101. В некоторых вариантах осуществления данные могут быть конфиденциальными по своей сути, так что было бы нежелательно отправлять данные открытым текстом (то есть незашифрованными). Например, данные могут включать в себя личную информацию или платежную информацию. Однако вместе с описанными в этом документе методиками могут использоваться любые подходящие данные (например, конфиденциальные, неконфиденциальные или их сочетание).

[0072] На этапе 802 сервер 104 извлекает производный ключ на основе изображения для пользователя 101. Как правило, производный ключ на основе изображения хранится в базе 106 данных пользователей или на другом носителе информации. В некоторых вариантах осуществления производный ключ на основе изображения можно извлечь с использованием предоставленного пользователем 101 идентификатора, например имени пользователя или ID пользователя.

[0073] На этапе 803 сервер 104 шифрует определенные на этапе 801 данные, используя извлеченный производный ключ на основе изображения. Сервер 104 может использовать, например, модуль 104(D) шифрования.

[0074] На этапе 804 сервер 104 отправляет клиентскому компьютеру 102 зашифрованные данные и множество идентификаторов изображений. Множество идентификаторов изображений может указывать клиентскому компьютеру 102, какие аутентификационные изображения отображать пользователю 101. В некоторых вариантах осуществления множество идентификаторов изображений может включать в себя идентификаторы, указывающие подмножество аутентификационных изображений, выбранное пользователем, а также множество идентификаторов, указывающих другие изображения. Таким образом, пользователю 101 будет представлено несколько изображений, лишь некоторые из которых являются частью подмножества, ранее выбранного пользователем 101.

[0075] На этапе 805 клиентский компьютер 102 отображает множество изображений, ассоциированных с принятыми идентификаторами изображений. Например, пользователю можно опять отобразить сетку 600, или пользователю можно отобразить другую сетку изображений, включающую в себя футболиста, баскетболиста и дом.

[0076] На этапе 806 пользователь 101, используя клиентский компьютер 102, выбирает подмножество аутентификационных изображений. Как описано для этапа 403 из способа 400 регистрации, выбранное пользователем 101 подмножество изображений может включать в себя одно изображение либо может включать в себя несколько изображений. К тому же подмножество может быть неупорядоченным или упорядоченным и может выбираться любым подходящим образом.

[0077] На этапе 807 клиентский компьютер 102, используя функцию выработки ключа на основе изображения, определяет производный ключ на основе изображения из аутентификационных изображений. В различных вариантах осуществления для формирования производного ключа на основе изображения могут использоваться идентификаторы изображений, хэши изображений или сами изображения.

[0078] На этапе 808 клиентский компьютер 102 дешифрует зашифрованные данные с использованием производного ключа на основе изображения.

[0079] В одном примерном варианте использования в соответствии со способом 800, на этапе 803 сервер 104 шифрует банковскую выписку для пользователя 101, используя пользовательский производный ключ на основе изображения. На этапе 804 сервер 104 отправляет клиентскому компьютеру 102 зашифрованную выписку вместе с множеством идентификаторов изображений. На этапе 805 клиентский компьютер 102 отображает аутентификационные изображения, соответствующие принятым идентификаторам изображений. На этапе 806 пользователь 101 выбирает подмножество аутентификационных изображений. Затем на этапах 807 и 808 клиентский компьютер 102 соответственно извлекает и дешифрует банковскую выписку с использованием выбранного подмножества аутентификационных изображений. Таким образом, сервер 104 надежно передает клиентскому компьютеру 102 банковскую выписку пользователя.

[0080] Фиг. 9 показывает аналогичный способ 900 отправки зашифрованных данных

от клиентского компьютера 102 к серверу 104. Как правило, способ 900 может выполняться после того, как ассоциированный с клиентским компьютером 102 пользователь зарегистрировался на сервере 104 (например, в соответствии со способами 400 или 500).

[0081] На этапе 901 клиентский компьютер 102 определяет данные для отправки серверу 104. Как правило, данные могут быть конфиденциальными по своей сути, так что было бы нежелательно отправлять данные открытым текстом (то есть незашифрованными). Например, данные могут включать в себя личную информацию или платежную информацию. Однако вместе с описанными в этом документе методиками могут использоваться любые подходящие данные (например, конфиденциальные, неконфиденциальные или их сочетание).

[0082] На этапе 902 клиентский компьютер 104 отображает пользователю множество изображений. Отображаемые изображения могут определяться с использованием принятой от сервера 104 информации (например, идентификаторов изображений) либо могут определяться клиентским компьютером 102. Например, пользователю можно опять отобразить сетку 600, или пользователю можно отобразить другую сетку изображений, включающую в себя футболиста, баскетболиста и дом.

[0083] На этапе 903 пользователь 101 выбирает подмножество аутентификационных изображений из множества изображений. Выбранное пользователем 101 подмножество изображений может включать в себя одно изображение либо может включать в себя несколько изображений. К тому же подмножество может быть неупорядоченным или упорядоченным и может выбираться любым подходящим образом.

[0084] На этапе 904 клиентский компьютер 102, используя функцию выработки ключа на основе изображения, формирует производный ключ на основе изображения из подмножества аутентификационных изображений.

[0085] На этапе 905 клиентский компьютер 102 шифрует определенные на этапе 901 данные, используя производный ключ на основе изображения.

[0086] На этапе 906 клиентский компьютер 102 отправляет серверу 104 зашифрованные данные и идентификатор пользователя. Идентификатор пользователя может включать в себя любой идентификатор, подходящий для идентификации пользователя. Например, идентификатор пользователя может включать в себя имя пользователя или ID пользователя.

[0087] На этапе 907 сервер 104, используя идентификатор пользователя, определяет производный ключ на основе изображения, ассоциированный с пользователем. Например, в некоторых вариантах осуществления принятый идентификатор пользователя может использоваться для извлечения производного ключа на основе изображения из базы 106 данных пользователей.

[0088] На этапе 908 сервер 104 использует производный ключ на основе изображения для пользователя, чтобы дешифровать зашифрованные данные.

[0089] В одном примерном варианте использования в соответствии со способом 900, на этапе 901 пользователь 101 вводит в клиентский компьютер 102 имя пользователя и номер кредитной карты. На этапе 902 клиентский компьютер 102 отображает пользователю 101 множество аутентификационных изображений. Пользователь 101 на этапе 903 выбирает подмножество аутентификационных изображений, которые используются на этапе 904 для формирования производного ключа на основе изображения. На этапе 905 клиентский компьютер 102 шифрует номер кредитной карты пользователя и на этапе 906 отправляет серверу 104 зашифрованный номер карты вместе с именем пользователя. На этапе 907 сервер 104 извлекает ассоциированный с

пользователем 101 производный ключ на основе изображения, используя принятое имя пользователя, и на этапе 908 дешифрует зашифрованный номер кредитной карты, используя производный ключ на основе изображения. Таким образом, пользователь 101 надежно передает серверу 104 информацию о своей кредитной карте.

[0090] Следует отметить, что хотя способы 800 и 900 описывают возможные способы шифрования данных, варианты осуществления изобретения не ограничиваются перечисленными способами. Например, хотя отправка идентификаторов изображений вместо изображений, как упомянуто на этапе 804, обладает преимуществом минимизации передачи данных, в некоторых вариантах осуществления сами изображения могут передаваться повторно. Такие варианты осуществления могут быть особенно полезны, если клиентское устройство не хранит изображения локально. В качестве альтернативы в некоторых вариантах осуществления сервер 104 может не отправлять клиентскому компьютеру 102 изображения или идентификаторы изображений на этапе 804. В некоторых таких вариантах осуществления клиентский компьютер 102 может сам хранить множество изображений и определять, какие изображения представлять пользователю 101. В таких вариантах осуществления возможность дешифровать незашифрованные данные может зависеть как от пользователя 101, знающего правильную выборку аутентификационных изображений, так и от клиентского компьютера 102, имеющего изображения.

V. СПОСОБЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ

[0091] Фиг. 10 показывает способ 1000 для аутентификации пользователя 101 с использованием производного ключа на основе изображения. Как правило, способ 1000 может выполняться после того, как ассоциированный с клиентским компьютером 102 пользователь зарегистрировался на сервере 104 (например, в соответствии со способами 400 или 500).

[0092] На этапе 1001 клиентский компьютер 102 отправляет серверу 104 идентификатор пользователя. Идентификатор пользователя может быть любыми данными, подходящими для идентификации пользователя 101. Например, идентификатор пользователя может содержать имя пользователя, адрес электронной почты или номер счета для пользователя 101.

[0093] На этапе 1002 сервер 104 отправляет клиентскому компьютеру 102 множество идентификаторов изображений, причем множество идентификаторов изображений включает в себя ранее выбранное пользователем 101 подмножество аутентификационных изображений. Как правило, множество отправленных идентификаторов изображений должно быть достаточно большим, чтобы случайное угадывание секретной выборки изображений было маловероятным, но не настолько большим, чтобы требовать от пользователя 101 просматривать чрезмерное количество изображений для идентификации секретных изображений. Например, если имеется три секретных изображения для пользователя 101, то на этапе 1002 можно отправить всего 20 идентификаторов изображений.

[0094] На этапе 1003 клиентский компьютер 102 отображает аутентификационные изображения, соответствующие принятым идентификаторам изображений. На этапе 1004 пользователь 101 выбирает подмножество отображенных аутентификационных изображений. На этапе 1005 клиентский компьютер 102 отправляет серверу секретную выборку изображений.

[0095] На этапе 1006 сервер 104 восстанавливает производный ключ на основе изображения, используя принятое подмножество аутентификационных изображений. Как правило, восстановление производного ключа на основе изображения может

выполняться с использованием способа, аналогичного описанному на этапе 405 в способе 400.

[0096] На этапе 1007 сервер 104 сравнивает восстановленный производный ключ с производным ключом, сохраненным для пользователя 101 в базе 106 данных пользователей. Если восстановленный производный ключ и сохраненный производный ключ совпадают, то на этапе 1008 пользователя аутентифицируют. В противном случае пользователя 101 не аутентифицируют.

[0097] В одном примере пользователь 101, ранее зарегистрированный для веб-сайта с использованием способа 400, выбирает в качестве подмножества изображения футболиста, баскетболиста и дома, показанные в сетке 600. На этапе 1001 пользователь отправляет серверу 104 свое имя пользователя. На этапе 1002 сервер 104 отправляет пользователю 101 20 идентификаторов изображений, включая идентификаторы, соответствующие трем изображениям в ранее выбранном подмножестве. На этапе 1003 клиентский компьютер 102 отображает изображения пользователю 101. На этапе 1004 пользователь 101 выбирает подмножество аутентификационных изображений, а на этапе 1005 клиентский компьютер 102 отправляет их серверу 104. На этапах 1006 и 1007 сервер 104 восстанавливает производный ключ на основе изображения и сравнивает его с ключом, ранее сохраненным в базе 105 данных пользователей. Если они совпадают, то на этапе 1008 пользователя аутентифицируют.

[0098] Следует понимать, что фиг. 10 предназначена для описания, а не ограничения. Например, вместо сервера 104, отправляющего клиентскому компьютеру 102 множество изображений, как описано на этапе 1002, пользователь 101 может выбирать изображения, локально сохраненные в клиентском компьютере 102. В таких вариантах осуществления возможность аутентифицировать пользователя может зависеть как от знания секретной выборки изображений, так и от наличия секретных изображений в клиентском компьютере 102. Кроме того, в некоторых вариантах осуществления пользователь может формировать производный ключ на основе изображения и отправлять его серверу 104 для аутентификации, не заставляя сервер 104 восстанавливать производный ключ на основе изображения.

VI. ПЛАТЕЖНЫЕ СИСТЕМЫ

[0099] Фиг. 11 показывает систему, используемую для проведения платежа в соответствии с вариантом осуществления изобретения. Система включает в себя пользователя (не показан), который может управлять переносным пользовательским устройством 1101. Пользователь может использовать переносное пользовательское устройство 1101 для проведения покупок на устройстве 1102 доступа, подключенном к компьютеру 1103 торговца. Компьютер 1103 торговца может быть подключен к компьютеру 1104 эквайера. Компьютер 1104 эквайера может быть подключен к компьютеру 1106 эмитента посредством сети 1105 обработки платежей.

[0100] При использовании в данном документе "эмитент" обычно может относиться к хозяйствующему субъекту (например, банку), который ведет финансовые счета для пользователя и может выдавать пользователю реквизиты платежа, сохраненные на переносном бытовом приборе 101, например сотовом телефоне, смарт-карте, планшете или переносном компьютере. "Торговец" обычно является субъектом, который принимает участие в транзакциях и может продавать товары или услуги. "Эквайер" обычно является хозяйствующим субъектом (например, коммерческим банком), у которого есть деловые отношения с конкретным торговцем или другим субъектом. Некоторые субъекты могут выполнять функции эмитента и эквайера. Некоторые варианты осуществления могут включать в себя такие единые эмитенты-эквайеры.

Каждый из субъектов (например, компьютер 1103 торговца, компьютер 1104 эквайера, сеть 1105 обработки платежей и компьютер 1106 эмитента) может содержать один или несколько компьютеров для осуществления связи или выполнения одной или нескольких функций, описанных в этом документе.

[0101] Сеть 1105 обработки платежей может включать в себя подсистемы, сети и операции обработки данных, используемые для поддержки и оказания услуг центров сертификации, услуг авторизации, услуг аннулированных банковских карточек и расчетно-кассовых услуг. Примерная сеть обработки платежей может включать в себя VisaNet™. Сети обработки платежей, такие как VisaNet™, способны обрабатывать транзакции по кредитным картам, транзакции по дебетовым картам, транзакции электронных кошельков и другие типы коммерческих транзакций. VisaNet™, в частности, включает в себя систему VIP (система комплексных платежей Visa), которая обрабатывает запросы авторизации, и систему Base II, которая оказывает расчетно-кассовые услуги. В некоторых вариантах осуществления сеть 1105 обработки платежей может проводить транзакции практически в реальном масштабе времени.

[0102] Сеть 1105 обработки платежей может включать в себя один или несколько серверов. Сервер обычно является мощным компьютером или кластером компьютеров. Например, сервер может быть крупным мэйнфреймом, кластером миникомпьютеров или группой серверов, функционирующих как одно целое. В одном примере сервер может быть сервером баз данных, соединенным с веб-сервером. Сеть 1105 обработки платежей может использовать любую подходящую проводную или беспроводную сеть, включая Интернет.

[0103] В типичной покупке пользователь приобретает товар или услугу у торговца 1103 с использованием переносного бытового прибора 1101 (например, мобильного телефона). Переносной бытовой прибор 1101 пользователя может взаимодействовать с устройством 1102 доступа у торговца, ассоциированным с компьютером 1103 торговца. Например, пользователь может поднести переносной бытовой прибор 1101 к датчику NFC в устройстве 1102 доступа. В качестве альтернативы пользователь может электронно указывать торговцу подробности платежа, например, используя электронный кошелек или в сетевой транзакции.

[0104] Устройством 1102 доступа формируется запрос авторизации, а затем перенаправляется компьютеру 1104 эквайера. Как правило, запрос авторизации включает в себя поле для номера основного счета (PAN), ассоциированного с переносным бытовым прибором 1101. После приема запроса авторизации этот запрос авторизации отправляется в сеть 1105 обработки платежей. Затем сеть 1105 обработки платежей перенаправляет запрос авторизации соответствующему компьютеру 1106 эмитента, ассоциированному с эмитентом счета пользователя. Включенный в запрос авторизации PAN может использоваться для направления сообщения подходящему компьютеру 1106 эмитента.

[0105] "Запрос авторизации" может быть электронным сообщением, которое отправляется в сеть обработки платежей и/или эмитенту платежной карты, чтобы запросить авторизацию для транзакции. Запрос авторизации в соответствии с некоторыми вариантами осуществления может соответствовать ISO 8583, который является стандартом для систем, которые обмениваются информацией об электронных транзакциях, ассоциированных с платежом, выполненным пользователем с использованием платежного устройства (например, мобильного устройства) или платежного счета. Запрос авторизации может включать в себя идентификатор счета эмитента, который может ассоциироваться с платежным устройством или платежным

счетом. Запрос авторизации также может содержать дополнительные элементы данных, соответствующие "идентификационной информации", только в качестве примера включающие в себя: служебный код, CVV (проверочное значение карты), dCVV (динамическое проверочное значение карты), дата истечения срока и т. п. Запрос авторизации также может содержать "информацию о транзакции", например, любую информацию, ассоциированную с текущей транзакцией, например сумму транзакции, идентификатор торговца, местоположение торговца и т. п., а также любую другую информацию, которая может использоваться при определении, следует ли идентифицировать и/или авторизовать транзакцию. Запрос авторизации также может включать в себя другую информацию, например информацию, которая идентифицирует устройство доступа, которое формировало запрос авторизации, информацию о местоположении устройства доступа и т. п.

[0106] После того, как компьютер 1106 эмитента принимает запрос авторизации, компьютер 1106 эмитента возвращает ответ авторизации в сеть 1105 обработки платежей для указания, авторизована ли текущая транзакция (или не авторизована). Затем сеть 1105 обработки платежей перенаправляет ответ авторизации обратно к эквайеру 1104. Затем эквайер 1104 возвращает ответ компьютеру 1103 торговца. В некоторых вариантах осуществления, например когда в сети 1105 обработки платежей срабатывает критерий мошенничества, сеть 1105 обработки платежей может отклонить транзакцию, ранее авторизованную компьютером 1106 эмитента.

[0107] "Ответ авторизации" может быть электронным сообщением-ответом на запрос авторизации, сформированным финансовым учреждением-эмитентом или сетью обработки платежей. Ответ авторизации только в качестве примера может включать в себя один или несколько следующих индикаторов состояния: одобрение -- транзакция была одобрена; отказ -- транзакция не была одобрена; или Звонок в контактный центр -- ответ, ожидающий больше информации; торговец должен позвонить по бесплатному номеру телефона авторизации. Ответ авторизации также может включать в себя код авторизации, который может быть кодом, который выпустивший кредитную карту банк возвращает в ответ на запрос авторизации в электронном сообщении (либо напрямую, либо через сеть обработки платежей) устройству доступа торговца (например, POS-оборудованию), который указывает одобрение транзакции. Код может служить в качестве подтверждения авторизации. Как отмечалось выше, в некоторых вариантах осуществления сеть обработки платежей может формировать или перенаправлять торговцу ответ авторизации.

[0108] После того, как компьютер 1103 торговца принимает ответ авторизации, устройство доступа в компьютере 1103 торговца может предоставить ответ авторизации для пользователя. Ответ может отображаться бесконтактным устройством доступа либо может быть напечатан на кассовом чеке. С другой стороны, если транзакция является сетевой транзакцией, то торговец может предоставить веб-страницу или другое указание ответа авторизации.

[0109] В конце дня сеть 1105 обработки платежей может проводить обычный расчетно-кассовый процесс. Кассовый процесс является процессом обмена финансовыми подробностями между эквайером и эмитентом для упрощения проводки по платежному счету пользователя и сверки состояния расчетов пользователя. Однако следует отметить, что варианты осуществления изобретения не ограничиваются одним процессом расчетов.

[0110] Варианты осуществления изобретения могут использоваться в соответствии с системой из фиг. 11 любым подходящим образом. Например, в некоторых вариантах осуществления пользователь 101 может подключаться к компьютеру 1103 торговца с

использованием клиентского компьютера 102. Например, компьютер 1103 торговца может управлять веб-сайтом электронной коммерции. Чтобы создать учетную запись в компьютере 1103 торговца, пользователь 101 может сначала зарегистрироваться в компьютере 1103 торговца, используя клиентский компьютер 102 в соответствии со способом 400 или способом 500. Когда пользователь позже входит в компьютер 1103 торговца, может выполняться способ 1000 аутентификации. Когда пользователь 101 проводит платеж за товары или услуги у торговца, могут выполняться способы 800 и/или 900 защищенной связи. Например, пользователь 101 может отправлять компьютеру 1103 торговца платежную информацию в соответствии со способом 900. Аналогичным образом торговец может отправлять пользователю 101 счет-фактуру или кассовый чек в соответствии со способом 800. В этих способах компьютер 1103 торговца может играть роль сервера 104, а компьютер пользователя может играть роль клиентского компьютера 102. В более общем смысле описанные выше способы могут использоваться для связи и аутентификации между любыми субъектами в системе из фиг. 11.

VII. КОМПЬЮТЕРЫ

[0111] Фиг. 12 показывает пример платежного устройства 101” в виде карты. Как показано, платежное устройство 101” содержит пластмассовую подложку 101(m). В некоторых вариантах осуществления бесконтактный элемент 101(o) для сопряжения с устройством 102 доступа может находиться на пластмассовой подложке 101(m) или встраиваться в нее. На карте может быть напечатана или выбита информация 101(p) о пользователе, например номер счета, дата истечения срока и/или имя пользователя. На пластмассовой подложке 101(m) также может находиться магнитная полоса 101(n). В некоторых вариантах осуществления платежное устройство 101" может содержать микропроцессор и/или микросхемы памяти с сохраненными в них пользовательскими данными.

[0112] Как отмечено выше и показано на фиг. 12, платежное устройство 101” может включать в себя магнитную полосу 101(n) и бесконтактный элемент 101(o). В некоторых вариантах осуществления в платежном устройстве 101” могут присутствовать магнитная полоса 101(n) и бесконтактный элемент 101(o). В некоторых вариантах осуществления в платежном устройстве 101” может присутствовать либо магнитная полоса 101(n), либо бесконтактный элемент 101(o).

[0113] Фиг. 13 – высокоуровневая блок-схема компьютерной системы, которая может использоваться для реализации любого из описанных выше субъектов или компонентов. Показанные на фиг. 13 подсистемы взаимосвязаны посредством системной шины 1375. Дополнительные подсистемы включают в себя принтер 1303, клавиатуру 1306, несъемный диск 1307 и монитор 1309, которые соединяются с адаптером 1304 дисплея. Периферия и устройства ввода/вывода (I/O), которые соединяются с контроллером 1300 I/O, могут подключаться к компьютерной системе с помощью любого количества средств, известных в данной области техники, например последовательного порта. Например, последовательный порт 1305 или внешний интерфейс 1308 может использоваться для подключения компьютера к глобальной сети, такой как Интернет, устройству ввода типа "мышь" или сканеру. Межсоединение посредством системной шины 1375 позволяет центральному процессору 1302 осуществлять связь с каждой подсистемой и управлять исполнением инструкций из системной памяти 1301 или с несъемного диска 1307, а также обменом информацией между подсистемами. Системная память 1301 и/или несъемный диск может олицетворять компьютерно-читаемый носитель.

[0114] Как описано, патентоспособная услуга может включать в себя реализацию

одной или нескольких функций, процессов, операций или этапов способа. В некоторых вариантах осуществления функции, процессы, операции или этапы способа можно реализовать как результат исполнения набора инструкций или программного кода с помощью соответствующим образом запрограммированного вычислительного устройства, микропроцессора, процессора данных или т. п. Набор инструкций или программный код можно хранить в памяти или в другом виде элемента хранения данных, к которому обращается вычислительное устройство, микропроцессор и т. п. В других вариантах осуществления функции, процессы, операции или этапы способа можно реализовать с помощью микропрограммного обеспечения или специализированного процессора, интегральной схемы и т. п.

[0115] Следует понимать, что настоящее изобретение, которое описано выше, можно модульно или комплексно реализовать в виде управляющей логики с использованием компьютерного программного обеспечения. На основе раскрытия изобретения и предоставленных в этом документе идей средний специалист в данной области техники узнает и примет во внимание другие пути и/или способы реализации настоящего изобретения с использованием аппаратных средств и сочетания аппаратных средств и программного обеспечения.

[0116] Любой (любую) из компонентов или функций программного обеспечения, описанных в этой заявке, можно реализовать в виде программного кода для исполнения процессором с использованием любого подходящего языка программирования, например Java, C++ или Perl, использующего, например, традиционные или объектно-ориентированные методики. Программный код можно хранить в виде последовательности инструкций или команд на компьютерно-читаемом носителе, например в оперативном запоминающем устройстве (RAM), долговременном запоминающем устройстве (ROM), на магнитном носителе, например жестком диске или гибком диске, либо оптическом носителе, например CD-ROM. Любой такой компьютерно-читаемый носитель может постоянно находиться на одном вычислительном устройстве или внутри него и может присутствовать на разных вычислительных устройствах или внутри них в системе или сети.

[0117] Хотя некоторые примерные варианты осуществления подробно описаны и показаны на прилагаемых чертежах, нужно понимать, что такие варианты осуществления являются всего лишь пояснительными и не предназначены для ограничения широкого изобретения, и что это изобретение не должно ограничиваться показанными и описанными конкретными компоновками и конструкциями, поскольку у специалистов в данной области техники могут возникнуть различные другие модификации.

[0118] Использование в данном документе формы единственного числа имеет целью означать "по меньшей мере один", если явным образом не указано иное.

(57) Формула изобретения

1. Компьютер, содержащий:

процессор; и

долговременный компьютерно-читаемый носитель, содержащий исполняемый процессором код для реализации способа, содержащего:

определение производного ключа на основе изображения с использованием функции выработки ключа на основе изображения, причем производный ключ на основе изображения формируется из выборки аутентификационных изображений, выбранной пользователем, и при этом функция выработки ключа на основе изображения в качестве

входных параметров принимает значение изображения, которое представляет числовое значение, ассоциированное с выборкой аутентификационных изображений, значение длины ключа, которое задает длину производного ключа на основе изображения, число итераций, которое представляет количество повторений функции выработки ключа на основе изображения, которое нужно выполнить для формирования производного ключа на основе изображения, и значение соли, которое включает в себя идентификатор пользователя, идентифицирующий пользователя;

шифрование данных с использованием производного ключа на основе изображения; и

передачу зашифрованных данных.

2. Компьютер по п. 1, в котором способ дополнительно содержит:

отображение множества изображений, причем выборка аутентификационных изображений является подмножеством множества отображенных изображений.

3. Компьютер по п. 2, в котором способ дополнительно содержит:

прием клиентским компьютером множества идентификаторов изображений, причем идентификаторы изображений идентифицируют множество изображений для отображения клиентским компьютером.

4. Компьютер по п. 2, в котором множество изображений случайно размещается в сетке, отображенной с использованием клиентского компьютера.

5. Компьютер по п. 1, в котором серверу передаются зашифрованные данные, причем сервер определяет производный ключ на основе изображения, и при этом производный ключ на основе изображения используется сервером для дешифрования зашифрованных данных.

6. Компьютер по п. 5, в котором способ содержит:

отправку серверу производного ключа на основе изображения, причем производный ключ на основе изображения используется для дешифрования зашифрованных данных.

7. Компьютер по п. 1, в котором способ дополнительно содержит:

предоставление клиентскому компьютеру множества идентификаторов изображений, причем идентификаторы изображений идентифицируют множество изображений для отображения клиентским компьютером, и при этом выборка аутентификационных изображений является подмножеством множества изображений.

8. Компьютер по п. 1, в котором клиентскому компьютеру передаются зашифрованные данные, причем клиентский компьютер определяет производный ключ на основе изображения, и при этом производный ключ на основе изображения используется клиентским компьютером для дешифрования зашифрованных данных.

9. Компьютер по п. 1, в котором способ содержит:

прием от клиентского компьютера выборки аутентификационных изображений, выбранной пользователем, причем клиентскому компьютеру отправляются зашифрованные данные.

10. Система, содержащая:

компьютер по п. 1; и

сервер, содержащий:

второй процессор; и

второй долговременный компьютерно-читаемый носитель, содержащий исполняемый вторым процессором код для реализации второго способа, содержащего:

прием от компьютера зашифрованных данных;

определение производного ключа на основе изображения, ассоциированного с зашифрованными данными; и

дешифрование зашифрованных данных с использованием производного ключа на основе изображения.

11. Реализуемый компьютером способ, содержащий этапы, на которых:

определяют с помощью процессора производный ключ на основе изображения с использованием функции выработки ключа на основе изображения, причем производный ключ на основе изображения формируется из выборки аутентификационных изображений, выбранной пользователем, и при этом функция выработки ключа на основе изображения в качестве входных параметров принимает значение изображения, которое представляет числовое значение, ассоциированное с выборкой аутентификационных изображений, значение длины ключа, которое задает длину производного ключа на основе изображения, число итераций, которое представляет количество повторений функции выработки ключа на основе изображения, которое нужно выполнить для формирования производного ключа на основе изображения, и значение соли, которое включает в себя идентификатор пользователя, идентифицирующий пользователя;

шифруют данные с помощью процессора, используя производный ключ на основе изображения; и

передают зашифрованные данные с помощью процессора.

12. Способ по п. 11, дополнительно содержащий этап, на котором:

отображают множество изображений, причем выборка аутентификационных изображений является подмножеством множества отображенных изображений.

13. Способ по п. 11, дополнительно содержащий этап, на котором:

принимают множество идентификаторов изображений с помощью процессора клиентского компьютера, причем идентификаторы изображений идентифицируют множество изображений для отображения клиентским компьютером.

14. Способ по п. 12, в котором множество изображений случайно размещается в сетке, отображенной с использованием клиентского компьютера.

15. Способ по п. 11, в котором серверу передаются зашифрованные данные, причем сервер определяет производный ключ на основе изображения, и при этом производный ключ на основе изображения используется сервером для дешифрования зашифрованных данных.

16. Способ по п. 15, дополнительно содержащий этап, на котором:

отправляют серверу выборку аутентификационных изображений с помощью процессора, причем выборка аутентификационных изображений используется сервером для определения производного ключа на основе изображения.

17. Способ по п. 15, причем способ содержит этап, на котором:

отправляют серверу с помощью процессора производный ключ на основе изображения, причем производный ключ на основе изображения используется для дешифрования зашифрованных данных.

18. Способ по п. 11, дополнительно содержащий этап, на котором:

предоставляют клиентскому компьютеру с помощью процессора множество идентификаторов изображений, причем идентификаторы изображений идентифицируют множество изображений для отображения клиентским компьютером, и при этом выборка аутентификационных изображений является подмножеством множества изображений.

19. Способ по п. 11, в котором клиентскому компьютеру передаются зашифрованные данные, в котором клиентский компьютер определяет производный ключ на основе изображения, и при этом производный ключ на основе изображения используется

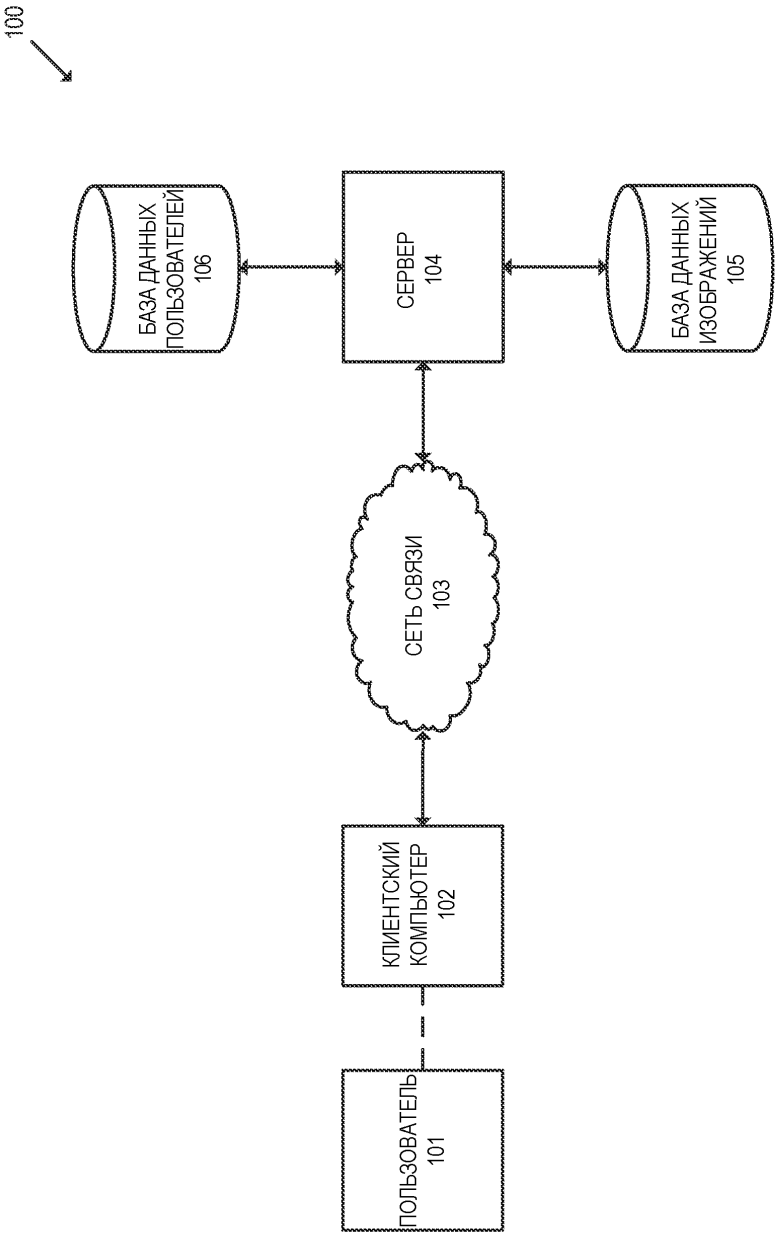
клиентским компьютером для дешифрования зашифрованных данных.

20. Способ по п. 11, дополнительно содержащий этап, на котором:

принимают от клиентского компьютера с помощью процессора выборку аутентификационных изображений, выбранную пользователем, причем клиентскому компьютеру отправляются зашифрованные данные.

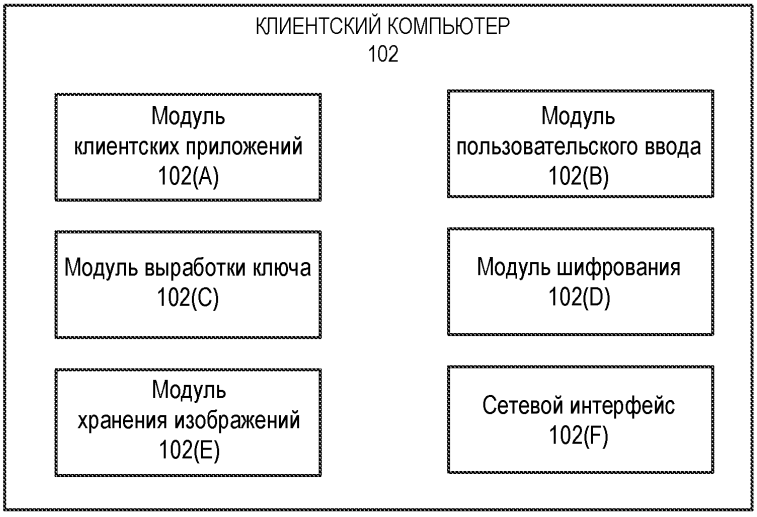
1

530810



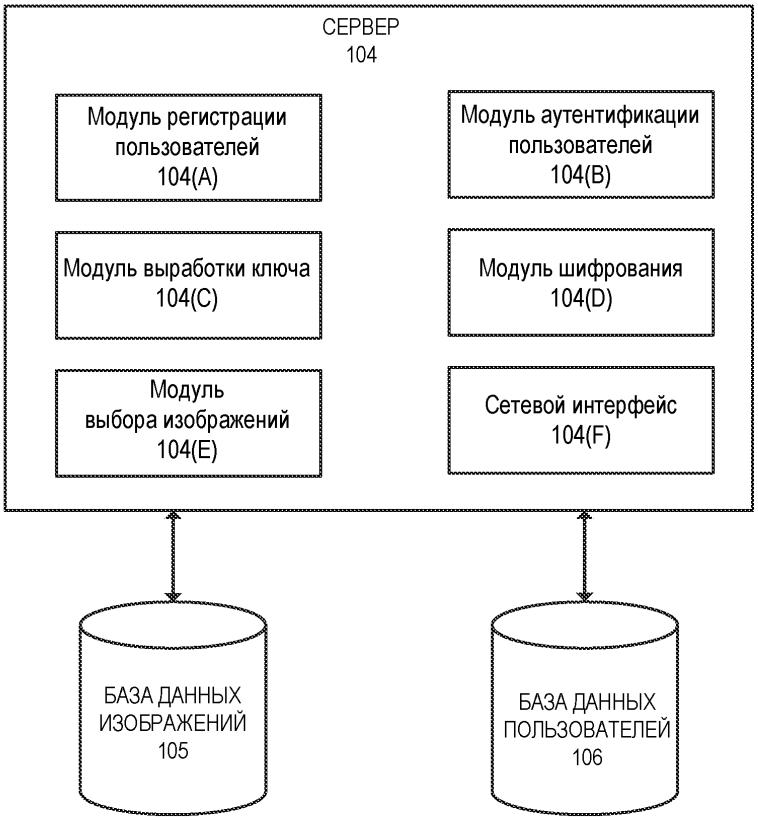
ФИГ.1

2


КЛИЕНТСКИЙ КОМПЬЮТЕР
102
Модуль клиентских приложений 102(A)
Модуль пользовательского ввода 102(B)
Модуль выработки ключа 102(C)
Модуль шифрования 102(D)
Модуль хранения изображений 102(E)
Сетевой интерфейс 102(F)

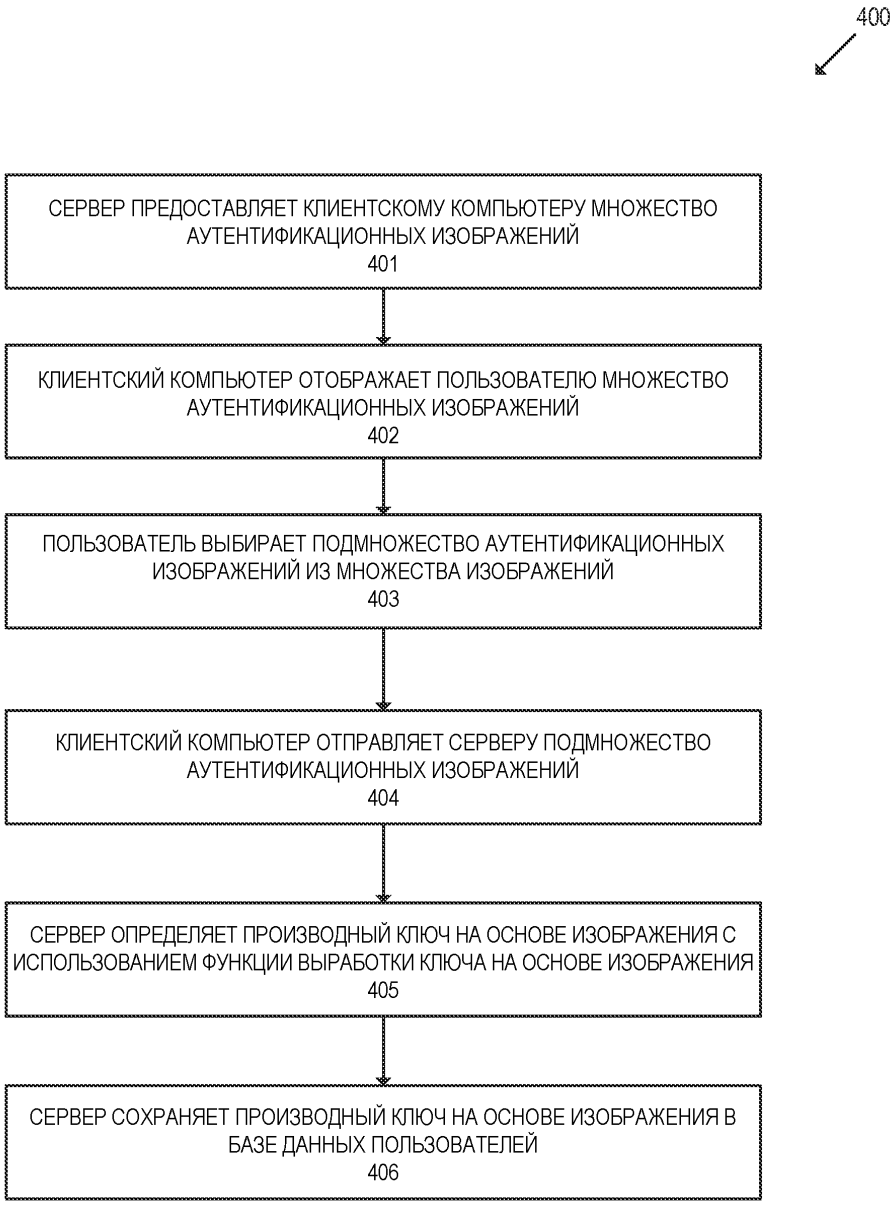
ФИГ.2

3


СЕРВЕР
104
Модуль регистрации пользователей 104(A)
Модуль аутентификации пользователей 104(B)
Модуль выработки ключа 104(C)
Модуль шифрования 104(D)
Модуль выбора изображений 104(E)
Сетевой интерфейс 104(F)
БАЗА ДАННЫХ ИЗОБРАЖЕНИЙ 105
БАЗА ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ 106

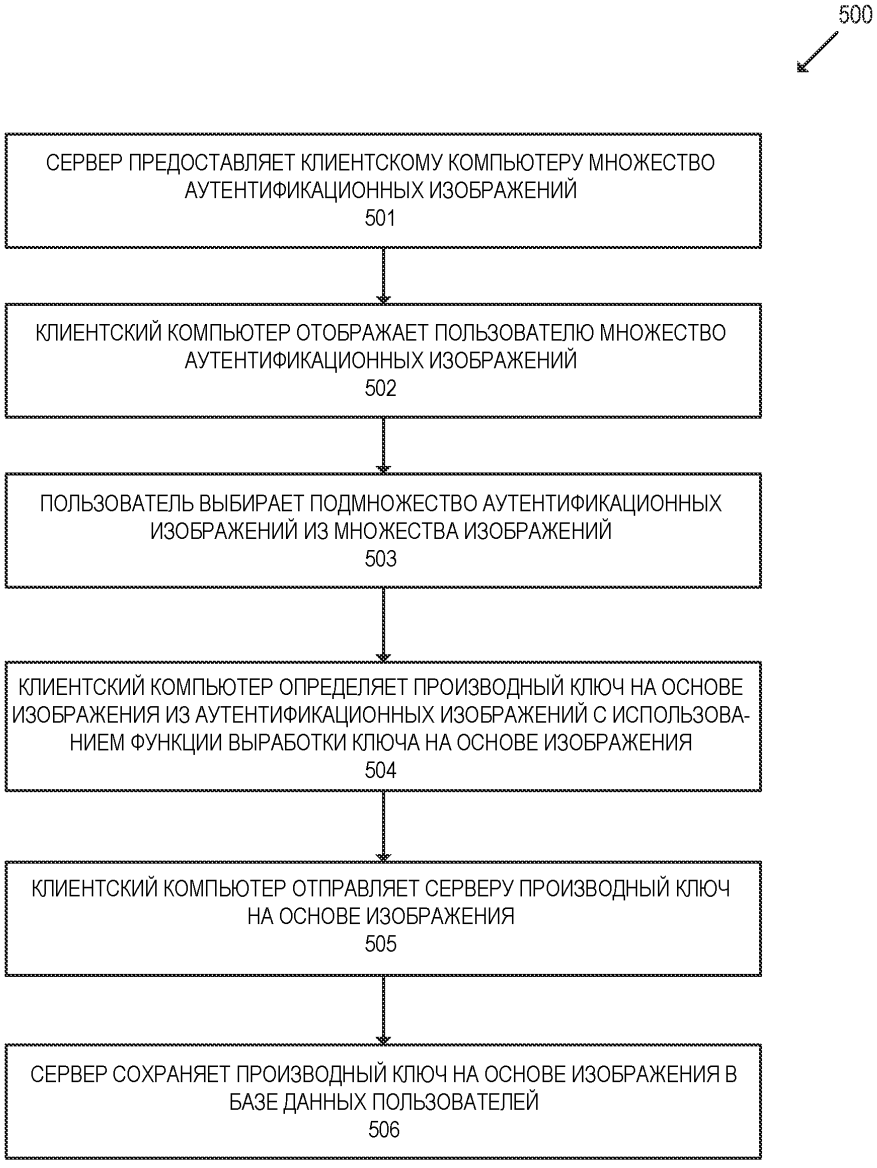
ФИГ.3

4


400
СЕРВЕР ПРЕДОСТАВЛЯЕТ КЛИЕНТСКОМУ КОМПЬЮТЕРУ МНОЖЕСТВО АУТЕНТИФИКАЦИОННЫХ ИЗОБРАЖЕНИЙ
401
КЛИЕНТСКИЙ КОМПЬЮТЕР ОТОБРАЖАЕТ ПОЛЬЗОВАТЕЛЮ МНОЖЕСТВО АУТЕНТИФИКАЦИОННЫХ ИЗОБРАЖЕНИЙ
402
ПОЛЬЗОВАТЕЛЬ ВЫБИРАЕТ ПОДМНОЖЕСТВО АУТЕНТИФИКАЦИОННЫХ ИЗОБРАЖЕНИЙ ИЗ МНОЖЕСТВА ИЗОБРАЖЕНИЙ
403
КЛИЕНТСКИЙ КОМПЬЮТЕР ОТПРАВЛЯЕТ СЕРВЕРУ ПОДМНОЖЕСТВО АУТЕНТИФИКАЦИОННЫХ ИЗОБРАЖЕНИЙ
404
СЕРВЕР ОПРЕДЕЛЯЕТ ПРОИЗВОДНЫЙ КЛЮЧ НА ОСНОВЕ ИЗОБРАЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ ФУНКЦИИ ВЫРАБОТКИ КЛЮЧА НА ОСНОВЕ ИЗОБРАЖЕНИЯ
405
СЕРВЕР СОХРАНЯЕТ ПРОИЗВОДНЫЙ КЛЮЧ НА ОСНОВЕ ИЗОБРАЖЕНИЯ В БАЗЕ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ
406

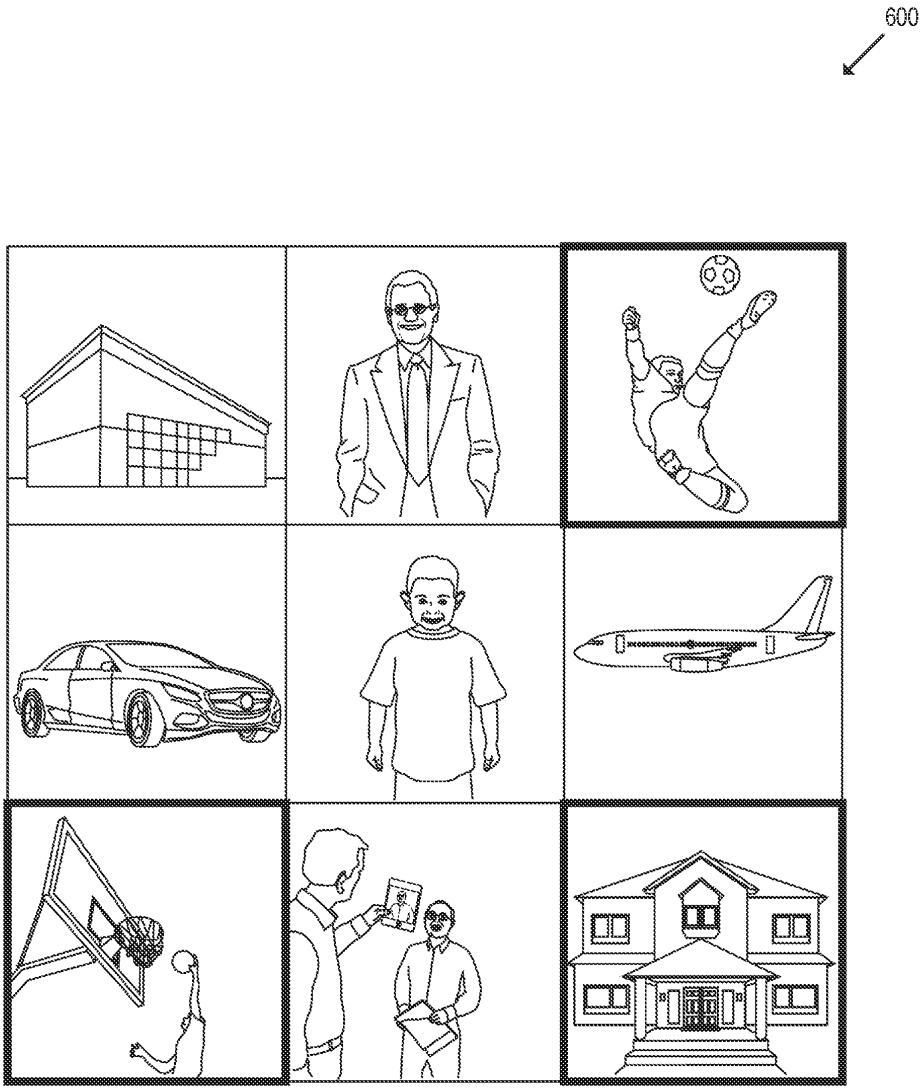
ФИГ.4

5


500
СЕРВЕР ПРЕДОСТАВЛЯЕТ КЛИЕНТСКОМУ КОМПЬЮТЕРУ МНОЖЕСТВО АУТЕНТИФИКАЦИОННЫХ ИЗОБРАЖЕНИЙ
501
КЛИЕНТСКИЙ КОМПЬЮТЕР ОТОБРАЖАЕТ ПОЛЬЗОВАТЕЛЮ МНОЖЕСТВО АУТЕНТИФИКАЦИОННЫХ ИЗОБРАЖЕНИЙ
502
ПОЛЬЗОВАТЕЛЬ ВЫБИРАЕТ ПОДМНОЖЕСТВО АУТЕНТИФИКАЦИОННЫХ ИЗОБРАЖЕНИЙ ИЗ МНОЖЕСТВА ИЗОБРАЖЕНИЙ
503
КЛИЕНТСКИЙ КОМПЬЮТЕР ОПРЕДЕЛЯЕТ ПРОИЗВОДНЫЙ КЛЮЧ НА ОСНОВЕ ИЗОБРАЖЕНИЯ ИЗ АУТЕНТИФИКАЦИОННЫХ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ФУНКЦИИ ВЫРАБОТКИ КЛЮЧА НА ОСНОВЕ ИЗОБРАЖЕНИЯ
504
КЛИЕНТСКИЙ КОМПЬЮТЕР ОТПРАВЛЯЕТ СЕРВЕРУ ПРОИЗВОДНЫЙ КЛЮЧ НА ОСНОВЕ ИЗОБРАЖЕНИЯ
505
СЕРВЕР СОХРАНЯЕТ ПРОИЗВОДНЫЙ КЛЮЧ НА ОСНОВЕ ИЗОБРАЖЕНИЯ В БАЗЕ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ
506

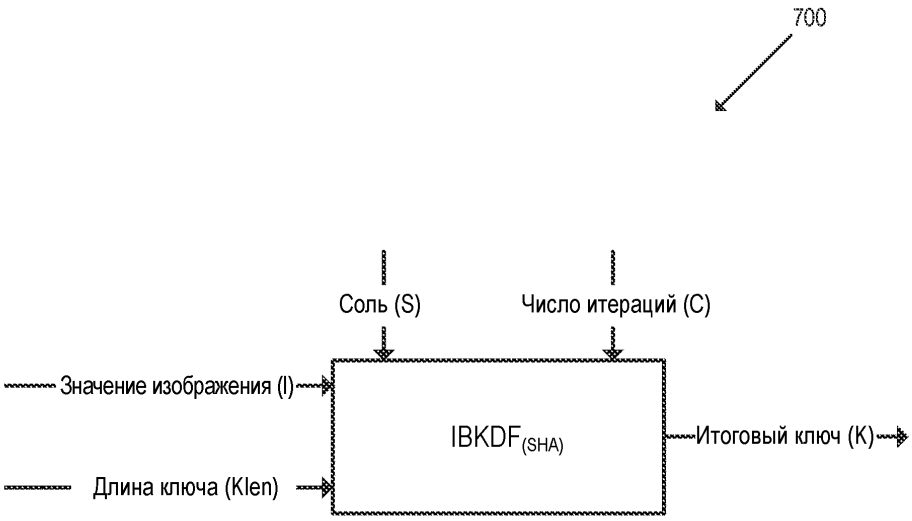
ФИГ.5

6

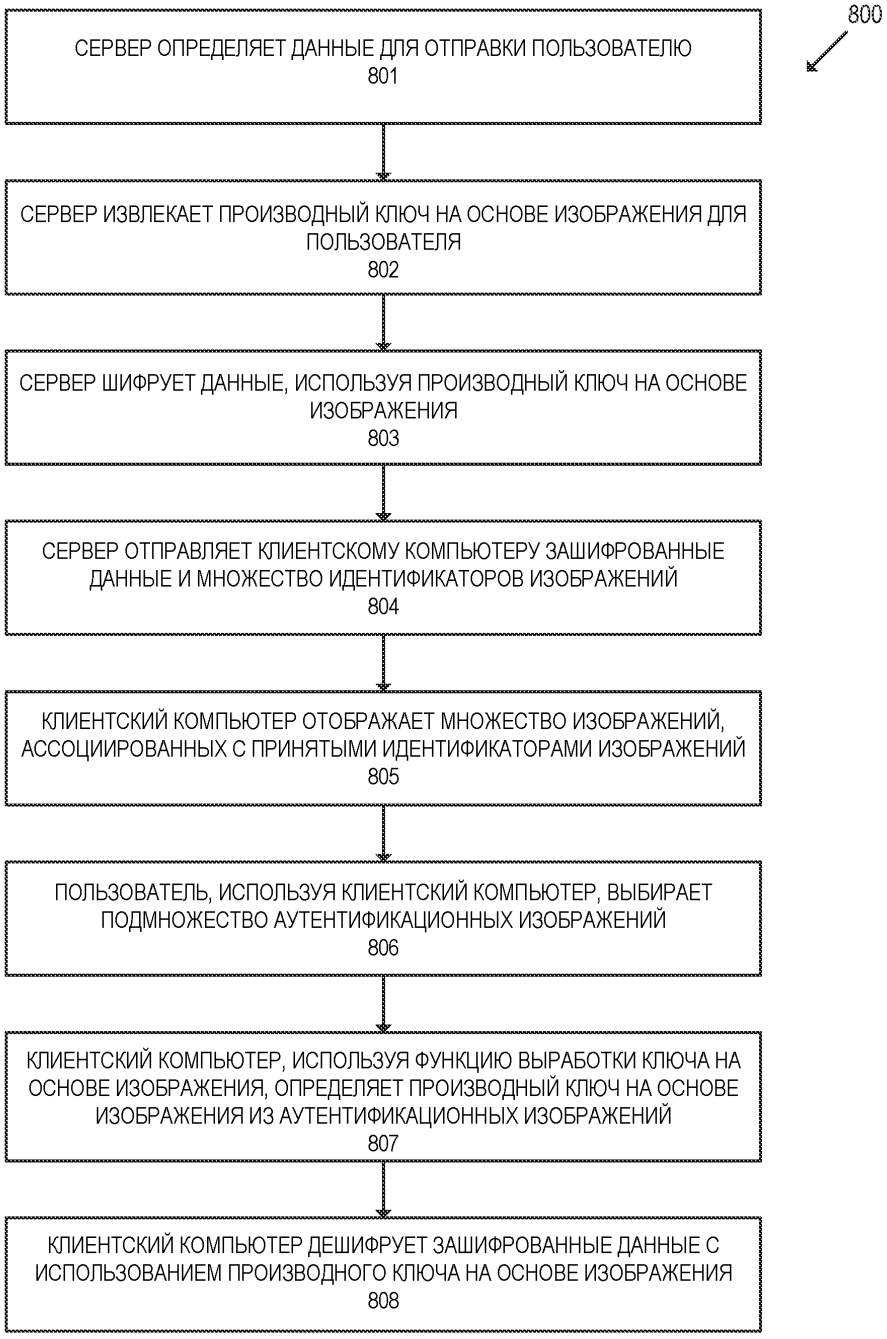


ФИГ.6

7

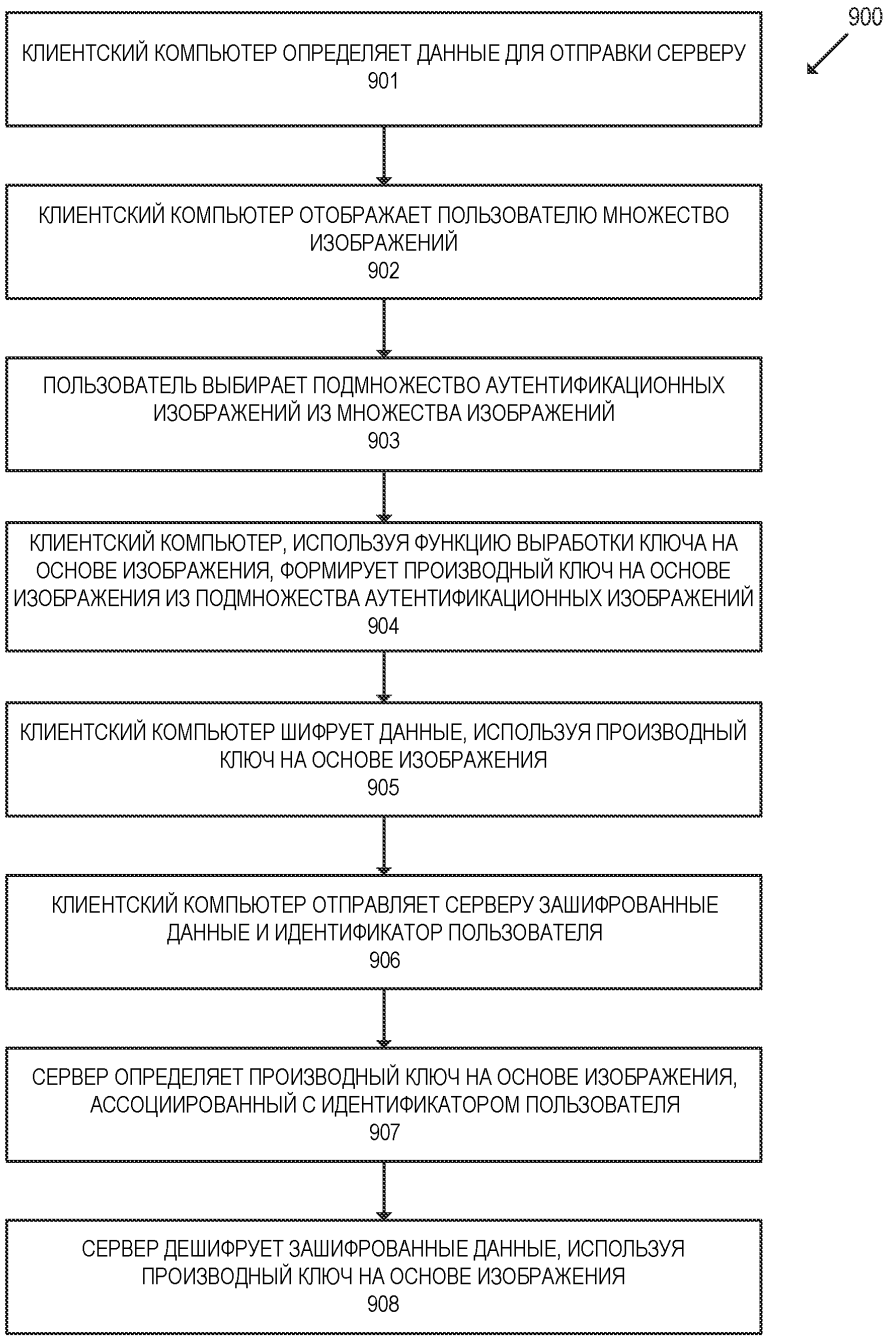

700
Соль (S)
Число итераций (C)
Значение изображения (I)
IBKDF(SHA)
Итоговый ключ (K)
Длина ключа (Klen)

ФИГ.7


800
СЕРВЕР ОПРЕДЕЛЯЕТ ДАННЫЕ ДЛЯ ОТПРАВКИ ПОЛЬЗОВАТЕЛЮ
801
СЕРВЕР ИЗВЛЕКАЕТ ПРОИЗВОДНЫЙ КЛЮЧ НА ОСНОВЕ ИЗОБРАЖЕНИЯ ДЛЯ ПОЛЬЗОВАТЕЛЯ
802
СЕРВЕР ШИФРУЕТ ДАННЫЕ, ИСПОЛЬЗУЯ ПРОИЗВОДНЫЙ КЛЮЧ НА ОСНОВЕ ИЗОБРАЖЕНИЯ
803
СЕРВЕР ОТПРАВЛЯЕТ КЛИЕНТСКОМУ КОМПЬЮТЕРУ ЗАШИФРОВАННЫЕ ДАННЫЕ И МНОЖЕСТВО ИДЕНТИФИКАТОРОВ ИЗОБРАЖЕНИЙ
804
КЛИЕНТСКИЙ КОМПЬЮТЕР ОТОБРАЖАЕТ МНОЖЕСТВО ИЗОБРАЖЕНИЙ, АССОЦИИРОВАННЫХ С ПРИНЯТЫМИ ИДЕНТИФИКАТОРАМИ ИЗОБРАЖЕНИЙ
805
ПОЛЬЗОВАТЕЛЬ, ИСПОЛЬЗУЯ КЛИЕНТСКИЙ КОМПЬЮТЕР, ВЫБИРАЕТ ПОДМНОЖЕСТВО АУТЕНТИФИКАЦИОННЫХ ИЗОБРАЖЕНИЙ
806
КЛИЕНТСКИЙ КОМПЬЮТЕР, ИСПОЛЬЗУЯ ФУНКЦИЮ ВЫРАБОТКИ КЛЮЧА НА ОСНОВЕ ИЗОБРАЖЕНИЯ, ОПРЕДЕЛЯЕТ ПРОИЗВОДНЫЙ КЛЮЧ НА ОСНОВЕ ИЗОБРАЖЕНИЯ ИЗ АУТЕНТИФИКАЦИОННЫХ ИЗОБРАЖЕНИЙ
807
КЛИЕНТСКИЙ КОМПЬЮТЕР ДЕШИФРУЕТ ЗАШИФРОВАННЫЕ ДАННЫЕ С ИСПОЛЬЗОВАНИЕМ ПРОИЗВОДНОГО КЛЮЧА НА ОСНОВЕ ИЗОБРАЖЕНИЯ
808

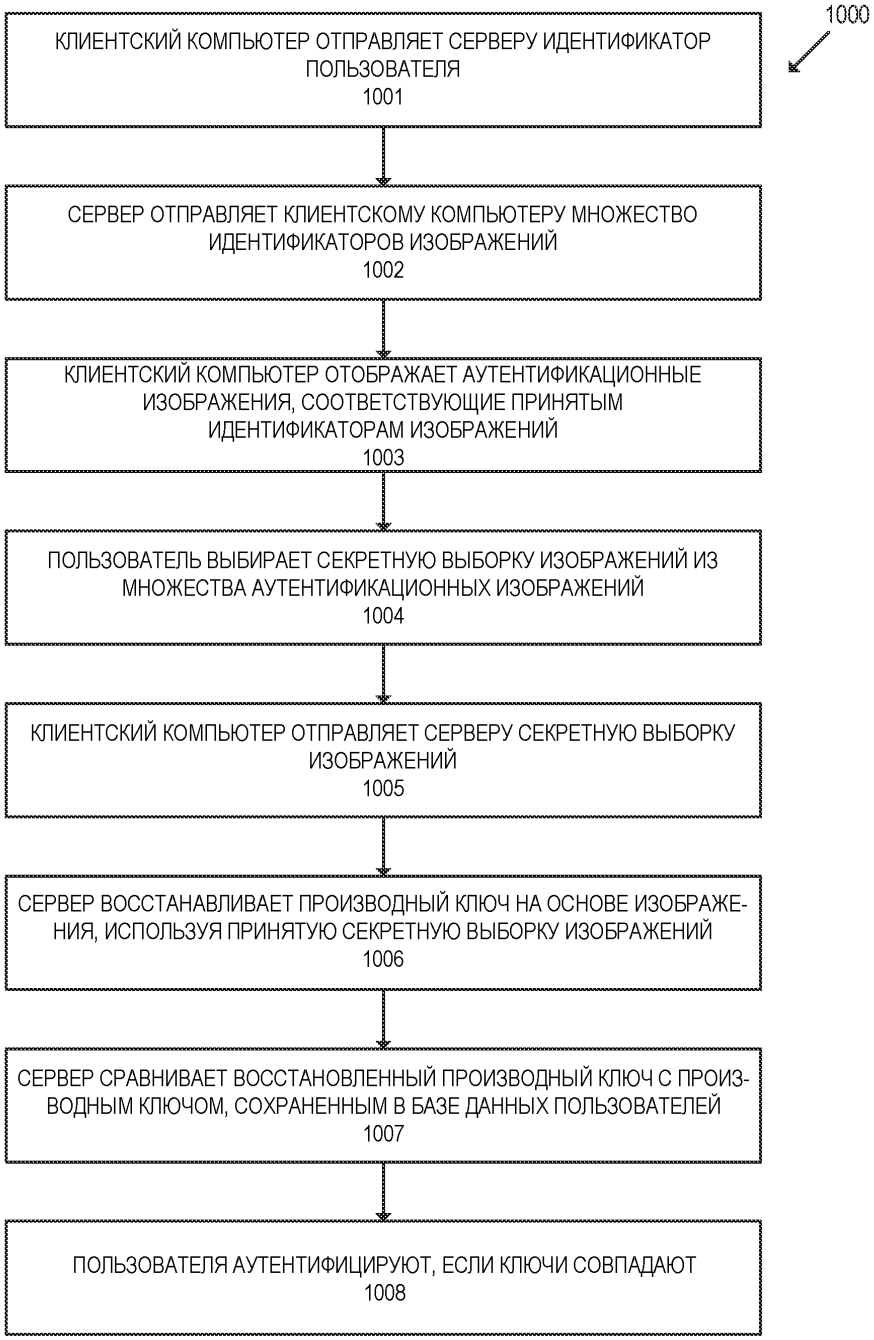
ФИГ.8

9


900
КЛИЕНТСКИЙ КОМПЬЮТЕР ОПРЕДЕЛЯЕТ ДАННЫЕ ДЛЯ ОТПРАВКИ СЕРВЕРУ
901
КЛИЕНТСКИЙ КОМПЬЮТЕР ОТОБРАЖАЕТ ПОЛЬЗОВАТЕЛЮ МНОЖЕСТВО ИЗОБРАЖЕНИЙ
902
ПОЛЬЗОВАТЕЛЬ ВЫБИРАЕТ ПОДМНОЖЕСТВО АУТЕНТИФИКАЦИОННЫХ ИЗОБРАЖЕНИЙ ИЗ МНОЖЕСТВА ИЗОБРАЖЕНИЙ
903
КЛИЕНТСКИЙ КОМПЬЮТЕР, ИСПОЛЬЗУЯ ФУНКЦИЮ ВЫРАБОТКИ КЛЮЧА НА ОСНОВЕ ИЗОБРАЖЕНИЯ, ФОРМИРУЕТ ПРОИЗВОДНЫЙ КЛЮЧ НА ОСНОВЕ ИЗОБРАЖЕНИЯ ИЗ ПОДМНОЖЕСТВА АУТЕНТИФИКАЦИОННЫХ ИЗОБРАЖЕНИЙ
904
КЛИЕНТСКИЙ КОМПЬЮТЕР ШИФРУЕТ ДАННЫЕ, ИСПОЛЬЗУЯ ПРОИЗВОДНЫЙ КЛЮЧ НА ОСНОВЕ ИЗОБРАЖЕНИЯ
905
КЛИЕНТСКИЙ КОМПЬЮТЕР ОТПРАВЛЯЕТ СЕРВЕРУ ЗАШИФРОВАННЫЕ ДАННЫЕ И ИДЕНТИФИКАТОР ПОЛЬЗОВАТЕЛЯ
906
СЕРВЕР ОПРЕДЕЛЯЕТ ПРОИЗВОДНЫЙ КЛЮЧ НА ОСНОВЕ ИЗОБРАЖЕНИЯ, АССОЦИИРОВАННЫЙ С ИДЕНТИФИКАТОРОМ ПОЛЬЗОВАТЕЛЯ
907
СЕРВЕР ДЕШИФРУЕТ ЗАШИФРОВАННЫЕ ДАННЫЕ, ИСПОЛЬЗУЯ ПРОИЗВОДНЫЙ КЛЮЧ НА ОСНОВЕ ИЗОБРАЖЕНИЯ
908

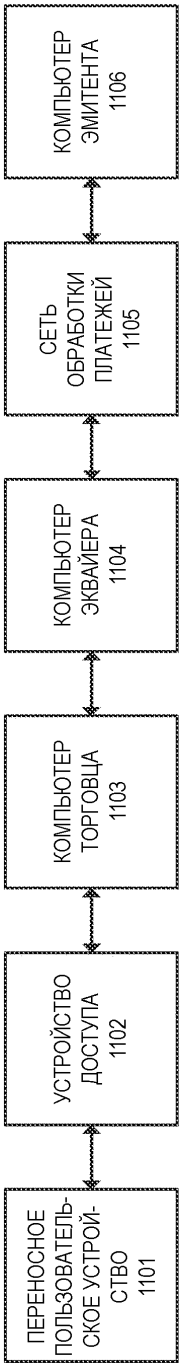
ФИГ.9

10

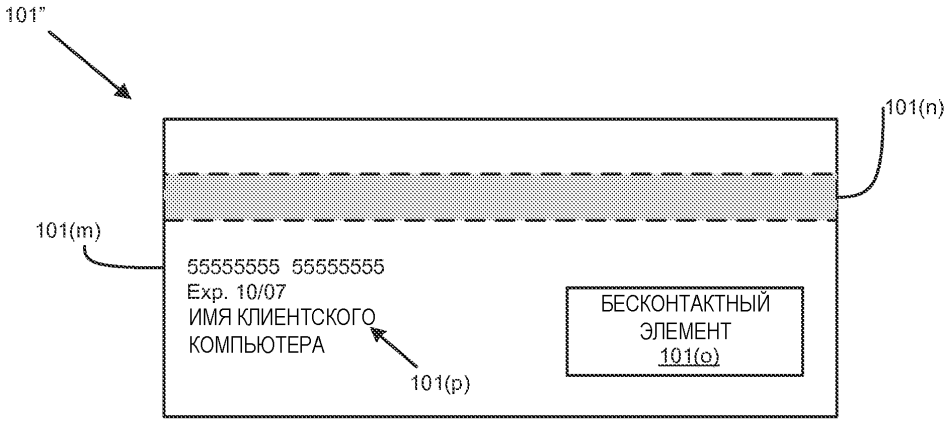

1000
КЛИЕНТСКИЙ КОМПЬЮТЕР ОТПРАВЛЯЕТ СЕРВЕРУ ИДЕНТИФИКАТОР ПОЛЬЗОВАТЕЛЯ
1001
СЕРВЕР ОТПРАВЛЯЕТ КЛИЕНТСКОМУ КОМПЬЮТЕРУ МНОЖЕСТВО ИДЕНТИФИКАТОРОВ ИЗОБРАЖЕНИЙ
1002
КЛИЕНТСКИЙ КОМПЬЮТЕР ОТОБРАЖАЕТ АУТЕНТИФИКАЦИОННЫЕ ИЗОБРАЖЕНИЯ, СООТВЕТСТВУЮЩИЕ ПРИНЯТЫМ ИДЕНТИФИКАТОРАМ ИЗОБРАЖЕНИЙ
1003
ПОЛЬЗОВАТЕЛЬ ВЫБИРАЕТ СЕКРЕТНУЮ ВЫБОРКУ ИЗОБРАЖЕНИЙ ИЗ МНОЖЕСТВА АУТЕНТИФИКАЦИОННЫХ ИЗОБРАЖЕНИЙ
1004
КЛИЕНТСКИЙ КОМПЬЮТЕР ОТПРАВЛЯЕТ СЕРВЕРУ СЕКРЕТНУЮ ВЫБОРКУ ИЗОБРАЖЕНИЙ
1005
СЕРВЕР ВОССТАНАВЛИВАЕТ ПРОИЗВОДНЫЙ КЛЮЧ НА ОСНОВЕ ИЗОБРАЖЕНИЯ, ИСПОЛЬЗУЯ ПРИНЯТУЮ СЕКРЕТНУЮ ВЫБОРКУ ИЗОБРАЖЕНИЙ
1006
СЕРВЕР СРАВНИВАЕТ ВОССТАНОВЛЕННЫЙ ПРОИЗВОДНЫЙ КЛЮЧ С ПРОИЗВОДНЫМ КЛЮЧОМ, СОХРАНЕННЫМ В БАЗЕ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ
1007
ПОЛЬЗОВАТЕЛЯ АУТЕНТИФИЦИРУЮТ, ЕСЛИ КЛЮЧИ СОВПАДАЮТ
1008

ФИГ.10

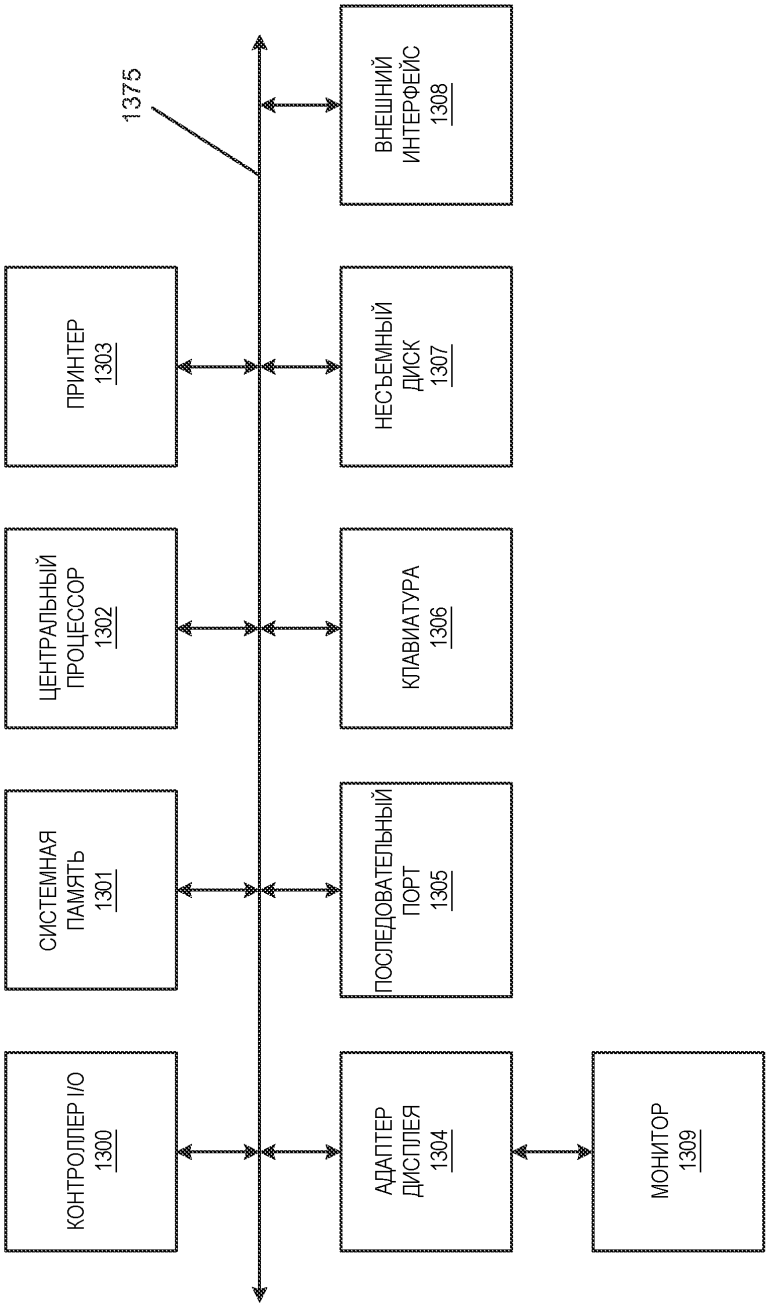
11


ПЕРЕНОСНОЕ ПОЛЬЗОВАТЕЛЬСКОЕ УСТРОЙСТВО 1101
УСТРОЙСТВО ДОСТУПА 1102
КОМПЬЮТЕР ТОРГОВЦА 1103
КОМПЬЮТЕР ЭКВАЙЕРА 1104
СЕТЬ ОБРАБОТКИ ПЛАТЕЖЕЙ 1105
КОМПЬЮТЕР ЭМИТЕНТА 1106

ФИГ.11


101"
101(n)
101(m)
55555555 55555555
Exp. 10/07
ИМЯ КЛИЕНТСКОГО
КОМПЬЮТЕРА
101(p)
БЕСКОНТАКТНЫЙ
ЭЛЕМЕНТ
101(o)

ФИГ.12


1375
ВНЕШНИЙ ИНТЕРФЕЙС 1308
НЕСЪЕМНЫЙ ДИСК 1307
КЛАВИАТУРА 1306
ПОСЛЕДОВАТЕЛЬНЫЙ ПОРТ 1305
АДАПТЕР ДИСПЛЕЯ 1304
МОНИТОР 1309
ПРИНТЕР 1303
ЦЕНТРАЛЬНЫЙ ПРОЦЕССОР 1302
СИСТЕМНАЯ ПАМЯТЬ 1301
КОНТРОЛЛЕР I/O 1300

ФИГ.13