РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 386 168** (13) **C2**

(51) МПК
G06K 5/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2005104394/09, 17.02.2005**

(24) Дата начала отсчета срока действия патента:
17.02.2005

(30) Конвенционный приоритет:
17.03.2004 US 10/802,981

(43) Дата публикации заявки: **27.07.2006**

(45) Опубликовано: **10.04.2010** Бюл. № **10**

(56) Список документов, цитированных в отчете о поиске: **RU 2088971 C1, 27.08.1997. CA 2595621 A1, 26,08.2000. US 4820912 A, 11.04.1989. EP 1173001 A2, 16.01.2002. US 6332030 B1, 18.12.2001. ФРИТЧ В. Применение микропроцессоров в системах управления. - М.: Мир, 1984, с.60-70.**

Адрес для переписки:
129090, Москва, ул. Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Автор(ы):
КИРОВСКИ Дарко (US)

(73) Патентообладатель(и):
МАЙКРОСОФТ КОРПОРЕЙШН (US)

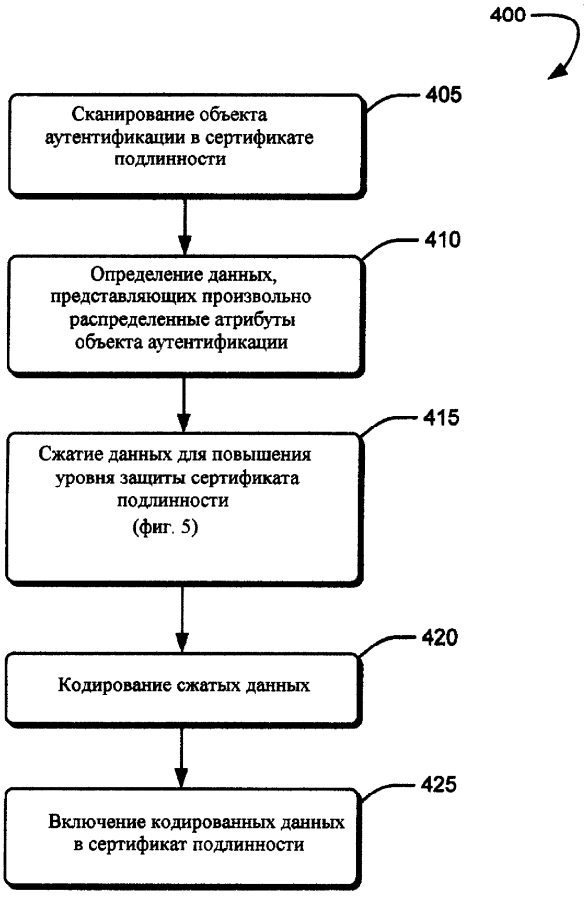
RU 2386168 C2

RU 2386168 C2

(54) СИСТЕМА И СПОСОБ КОДИРОВАНИЯ ПРОИЗВОЛЬНО РАСПРЕДЕЛЕННЫХ ПРИЗНАКОВ В ОБЪЕКТЕ

(57) Реферат:

Системы и способы относятся к области кодирования произвольно распределенных признаков в объекте. Техническим результатом является снижение стоимости изготовления объектов с повышенной защищенностью данных. В изобретении определяют произвольно распределенные признаки объекта, сжимают и кодируют с помощью подписи. Создают ярлык, содержащий объект аутентификации и кодированные данные. Данные можно сжимать, определяя функцию плотности вероятности, связанную с объектом аутентификации. Векторы, связанные с произвольно распределенными атрибутами, определяют на основании, по меньшей мере частично, функции плотности вероятности. Векторы кодируют с использованием алгоритма арифметического кодирования. 5 н. и 24 з.п. ф-лы, 14 ил., 4 табл.



Фиг. 4

RU 2386168 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 386 168** (13) **C2**

(51) Int. Cl.
G06K 5/00 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2005104394/09, 17.02.2005**

(24) Effective date for property rights:
17.02.2005

(30) Priority:
17.03.2004 US 10/802,981

(43) Application published: **27.07.2006**

(45) Date of publication: **10.04.2010 Bull. 10**

Mail address:
129090, Moskva, ul. B.Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. Ju.D.Kuznetsovu, reg.№ 595

(72) Inventor(s):
KIROVSKI Darko (US)

(73) Proprietor(s):
MAJKROSOFT KORPOREJShN (US)

RU 2386168 C2

(54) SYSTEM AND METHOD FOR CODING OF RANDOMLY DISTRIBUTED CRITERIA IN OBJECT

(57) Abstract:

FIELD: information technologies.

SUBSTANCE: in invention they identify randomly distributed criteria of object, compress them and code them with the help of signature. Label is created, which contains object of authentication and coded data. Data may be compressed thus identifying function of probability density related to object of authentication. Vectors related to randomly distributed attributes are identified on the basis of at least partially probability density function. Vectors are coded with application of arithmetical coding algorithm.

EFFECT: reduced cost of objects manufacturing with high extent of data protection.

29 cl, 14 dwg, 4 tbl

Фиг. 4

RU 2386168 C2

Область техники, к которой относится изобретение

Описанные здесь системы и способы, в целом, относятся к ярлыкам, защищенным от подделки и/или защищенным от незаконного изменения, и, в частности, для использования произвольно распределенных признаков объекта (внедренных или собственных) для ограничения несанкционированных попыток подделки или подлога с помощью ярлыка.

Уровень техники

Подделка и незаконное изменение ярлыков стоят торговцам и товаропроизводителям миллиардов долларов ежегодной потери прибыли и потери потребителей. С распространением компьютерной технологии изготовление ярлыков, похожих на оригинальное изделие, упростилось. Например, можно использовать сканер для сканирования изображения оригинального ярлыка с высоким разрешением, после чего можно неоднократно воспроизводить его с минимальными затратами. Кроме того, купоны можно сканировать, изменять (например, в сторону увеличения ценности), повторно печатать и погашать.

В последние годы использовались различные технологии, чтобы остановить поток подделок и подлогов. Один из способов защиты ярлыков состоит во внедрении в них штрих-кодов. Штрих-код обычно представляет собой машиносчитываемый код, напечатанный на ярлыке. Используя сканер штрих-кодов, можно быстро считывать и аутентифицировать штрих-код. Одна проблема современных ярлыков, снабженных штрих-кодом, состоит в том, что один и тот же ярлык можно использовать на различных изделиях.

Другое современное решение состоит в проверке сканированного штрих-кода с помощью защитных данных, хранящихся в базе данных (например, в системе пункта продаж (ПП)). Однако это решение требует включения новейших данных от продавца или производителя. Такое решение требует оперативного и тесного взаимодействия нескольких организаций. Кроме того, такое решение ограничивает гибкость его реализации и не всегда осуществимо.

Однако эти технологии страдают общим недостатком, который заключается в том, что сканируемые ярлыки физически идентичны для данного изделия. Соответственно, хотя процесс производства для создания законных ярлыков может быть весьма изощренным, фальсификатору не потребуется много времени, чтобы найти способ обойти защиту. Скопировав один раз ярлык, его можно тиражировать (например, создав мастер-копию, которую можно дублировать с малыми затратами). Даже если ярлык занесен в черный список в базе данных после данного количества применений, не гарантируется, что ярлыки, которые были сканированы до этого, действительно являются оригинальными ярлыками.

Соответственно, современные решения не могут обеспечивать ярлыки, которые относительно трудно скопировать и недорого производить.

Раскрытие изобретения

Описанные здесь системы и способы направлены на кодирование произвольно распределенных признаков в объекте. Согласно одному аспекту, определяют произвольно распределенные признаки в объекте аутентификации. Данные, представляющие произвольно распределенные признаки, сжимают и кодируют с помощью подписи. Создают ярлык, содержащий объект аутентификации и кодированные данные.

Согласно другому аспекту, данные сжимают, определяя функцию плотности вероятности, связанную с объектом аутентификации. Векторы, связанные с

произвольно распределенными атрибутами, определяют на основании, по меньшей мере частично, функции плотности вероятности. Векторы кодируют с использованием алгоритма арифметического кодирования.

Краткое описание чертежей

Фиг.1 - пример объекта аутентификации для использования в качестве части ярлыка, например, сертификата подлинности.

Фиг.2 - схема, демонстрирующая пример системы сертификатов подлинности и иллюстративные процедуры, реализуемые системой для выдачи проверки сертификата подлинности.

Фиг.3А - схема иллюстративной системы сканирования для восприятия произвольно распределенных признаков объекта аутентификации, связанного с сертификатом подлинности.

Фиг.3В - вид сверху объекта аутентификации, показанного на фиг.3А.

Фиг.4 - логическая блок-схема иллюстративного процесса, который можно использовать для создания сертификата подлинности.

Фиг.5 - логическая блок-схема иллюстративного процесса, который можно использовать для сжатия данных, которые представляют произвольно распределенные атрибуты объекта аутентификации.

Фиг.6 - графическое представление областей, которые соответствуют четырем различным зонам в иллюстративном объекте аутентификации.

Фиг.7 - графическое представление девятнадцати разных зон иллюстративного объекта аутентификации.

Фиг.8 - график иллюстративной функции плотности вероятности для квадратного объекта аутентификации.

Фиг.9 - графическое представление областей в объекте аутентификации.

Фиг.10 - графическое представление, иллюстрирующее, как арифметический кодер кодирует строку "aba".

Фиг.11 - пример экземпляра объекта аутентификации, показанного с помощью узлов.

Фиг.12 - графическое представление сертификата подлинности, предназначенного для оптимизации эффективности затрат.

Фиг.13 - схема иллюстративного вычислительного устройства, которое можно полностью или частично реализовать посредством описанных систем и способов.

Осуществление изобретения

I. Введение

Описанные здесь системы и способы направлены на кодирование информации о произвольно распределенных признаках объекта, используемого в качестве ярлыка. Ярлыки могут включать в себя средства идентификации любого типа, присоединяемые к изделию или встраиваемые в него. Ярлык, который можно аутентифицировать, называется здесь сертификатом подлинности. Объект с произвольно распределенными признаками, используемый в сертификате подлинности, называется здесь объектом аутентификации. Чтобы обеспечить самоаутентификацию, сертификат подлинности может включать в себя как объект аутентификации, так и информацию о произвольно распределенных признаках. Метод сжатия можно использовать для увеличения объема информации о произвольно распределенных признаках, которую можно кодировать и включать в сертификат подлинности. Согласно одному вычислению, стоимость горячей штамповки сертификата подлинности экспоненциально возрастает пропорционально повышению

степени сжатия информации. Это существенное увеличение стоимости горячей штамповки обеспечивает надежный сертификат подлинности, который относительно дешево изготовить, но трудно фальсифицировать.

На фиг.1 показан пример объекта 100 аутентификации для использования как части ярлыка, например, сертификата подлинности. Для эффективного использования в сертификате подлинности объект 100 аутентификации обычно содержит произвольно распределенные признаки, которые являются уникальными и которые трудно копировать. Пример объекта 100 аутентификации, показанный на фиг.1, является частью сертификата подлинности на основе волокон и содержит волокна 110, внедренные в объект произвольным образом. Волокна 110 выступают в качестве произвольно распределенных признаков объекта 100 аутентификации. Волокна 110 могут быть включены в объект 100 аутентификации любыми средствами. Например, волокна 110 можно распылять на объект 100 аутентификации. Волокна 110 можно также внедрять в объект 100 аутентификации в процессе изготовления. Согласно одному варианту осуществления, волокна 110 являются оптическими волокнами, способными пропускать свет между своими концами. Таким образом, облучая светом определенную зону 120 объекта 100 аутентификации, освещают концы волокон 131-133, по меньшей мере, один конец которых находится в освещенной зоне.

Согласно фиг.1, объект 100 аутентификации содержит к произвольно распределенных волокон. Объект 100 аутентификации можно сканировать с разрешением L×L пикселей. Каждое волокно имеет фиксированную длину R. Хотя иллюстративный объект 100 аутентификации, показанный на фиг.1, содержит волокна, следует понимать, что в сертификате подлинности аналогично можно использовать объекты аутентификации с другими произвольно распределенными признаками.

Произвольно распределенные признаки объекта 100 аутентификации можно использовать в сертификате подлинности для защиты доказательства подлинности произвольного объекта, например изделия. Например, определенные труднодублируемые данные вокруг произвольно распределенных признаков сертификата подлинности могут быть оцифрованы, подписаны личным ключом блока издания, и подпись может быть отпечатана на сертификате подлинности в машиносчитываемом виде для подтверждения подлинности изготовленного экземпляра. Каждый экземпляр сертификата подлинности связан с объектом, подлинность которого хочет проверить блок издания. Согласно одному варианту осуществления, проверка подлинности производится, осуществляется путем извлечения подписанных данных (данных о произвольно распределенных признаках) с использованием общего ключа блока издания и проверки совпадения извлеченных данных с данными соответствующего экземпляра сертификата подлинности. Чтобы подделать защищенные объекты, противнику необходимо по выбору: (i) вычислить личный ключ блока издания, (ii) разработать процесс изготовления, который может точно дублировать уже подписанный экземпляр сертификата подлинности, и (iii) завладеть подписанными экземплярами сертификата подлинности. С этой точки зрения сертификат подлинности можно использовать для защиты изделий, ценность которых, в целом, не превышает стоимость горячей штамповки одного экземпляра сертификата подлинности, включая накопленное развитие успешного процесса соперничающего изготовления.

Цель системы сертификата подлинности состоит в том, чтобы гарантировать подлинность изделий или определенной информации, связанной с изделием. Сфера

применения очень широка, от борьбы с пиратством программного обеспечения и мультимедиа (например, DVD, CD) до негорячештампованных купонов и разработки оборудования, защищенного от подделки. Например, создание чипа, защищенного от подделки, требует покрытия его корпуса сертификатом подлинности. Перед каждым использованием следует проверить целостность сертификата подлинности, чтобы проверить подлинность защищенной микросхемы.

Ниже будут рассмотрены иллюстративные аппаратные платформы для недорогого, но эффективного считывания произвольно распределенных признаков сертификата подлинности на основе волокон. Аппаратные платформы могут включать в себя штрих-код. Поскольку емкость штрих-кода для недорогих устройств считывания ограничивается примерно 3 кбитами, сообщение, подписанное личным ключом, ограничивается той же длиной. Кроме того, поскольку одной из целей сертификата подлинности является максимизация усилий противника, нацеленных на горячую штамповку конкретного экземпляра и сертификата подлинности, будет рассмотрена проблема, связанная с сохранением в подписанном сообщении фиксированной длины как можно большего объема информации об уникальных и произвольно распределенных признаках сертификата подлинности на основе волокон. Будет предоставлен пример аналитической модели сертификата подлинности на основе волокон. Затем в нижеследующем рассмотрении проблема сжатия множества точек будет также формализована и будет показано, что оптимальное сжатие позиций волокон в экземпляре сертификата подлинности является NP-полной задачей. Для эвристического решения этой задачи будет обеспечен алгоритм, который значительно повышает отношения сжатия по сравнению с традиционными методами сжатия.

II. Издание и проверка сертификата подлинности

На фиг.2 показана схема, демонстрирующая иллюстративную систему 200 сертификата подлинности и иллюстративные процедуры, используемые системой для издания и проверки сертификата подлинности. Система 200 сертификата подлинности включает в себя сертификат 210 подлинности, блок 320 издания и блок 250 проверки. Согласно фиг.2, сертификат 210 подлинности может содержать объект 100 аутентификации, показанный на фиг.1, штрих-код 213 и текст 215.

Информация, которую нужно защищать на сертификате подлинности, включает в себя: (a) представление труднодублируемых произвольно распределенных признаков объекта 100 аутентификации и (b) связанные с ним произвольные текстовые данные. Сначала произвольно распределенные признаки объекта 100 аутентификации, например позиции волокон, сканируют с использованием аппаратного устройства. Ниже со ссылкой на фиг.3 мы подробно рассмотрим, как собирают и представляют эту информацию.

В целях рассмотрения предположим, что результирующая информация f является случайной строкой из n_F битов. Параметр n_F является фиксированным и равен $n_F = k \cdot n_{RSA}$, $k \in N$, где n_{RSA} - это длина общего ключа RSA (например, $n_{RSA} = 1024$), и k обычно задано как $k \in [1,3]$. При данном n_F собрание f данных 231, представляющее произвольно распределенные признаки объекта 100 аутентификации, может статистически максимизировать расстояние между двумя различными экземплярами сертификата подлинности. Эта задача непосредственно сводится к минимизированному правдоподобию ложного отрицательного результата и ложного положительного результата на этапе проверки.

Текстовые данные f являются произвольной строкой символов, которая зависит от приложения (например, срока годности, гарантии производителя). Текстовые данные

извлекаются из текста 215, напечатанного на сертификате 210 подлинности, как показано на фиг.2.

Текстовые данные можно хэшировать с использованием криптографически защищенного алгоритма 237 хэширования, например SHA1. Выход хэш-функции обозначается как сообщение t, состоящее из n_T битов. Блок 230 издания создает сообщение m, которое может быть подписано RSA. Например, сообщения f и t сливаются в сообщение m длиной $n_M = n_F$ с использованием обратимого оператора $\otimes$, который гарантирует, что каждый бит из m зависит от всех битов из f и t. Этот этап может максимизировать число битов, которыми нужно манипулировать в данных 231, а также в тексте 215 для создания определенного сообщения m. Примером такого оператора является симметричное шифрование $m = t \otimes f = E_t(f)$ для f с использованием t или определенного подмножества битов из t в качестве ключа. Сообщение m подписывается подписью 235 RSA с использованием личного ключа 233 блока 230 издания. Каждые n_{RSA} битов из m подписываются по отдельности. Результирующая подпись s имеет $n_S = n_M = n_F$ битов. Это сообщение кодируется и печатается как штрих-код 213 (например, штрих-код по стандарту PDF417) на сертификате 210 подлинности.

Проверка сертификата 210 подлинности производится в несколько этапов. Блок 250 проверки сначала сканирует отпечатанные компоненты: текст 215 и штрих-код 213. Штрих-код 213 декодируют в первоначально отпечатанную подпись s. Текст 215 сканируют и хэшируют для создания сообщения t. Заметим, что для этой задачи не требуется общий процесс оптического распознавания символов (OCR), поскольку шрифт, используемый для печати текста, известен блоку 250 проверки и оптимизирован для усовершенствованного OCR. Для успешной проверки сертификата подлинности текст 215 и штрих-код 213 должны быть считаны без ошибок; современные технологии сканирования позволяют легко выполнить эту задачу.

Блок 250 проверки осуществляет проверку 255 подписи RSA на s с использованием общего ключа 253 блока издания и получает подписанное сообщение m. Затем блок 250 проверки может вычислить $f=m(\otimes)^{-1}t$. В примере использования шифрования в качестве $\otimes$ это достигается дешифрованием $f=E_t^{-1}(m)$. Затем блок 250 проверки сканирует данные 251, представляющие произвольно распределенные признаки в объекте 100 аутентификации, и создает их представление f'. Блок 250 проверки сравнивает f' с извлеченным f. Блоку 250 проверки нужно определить величину корреляции между двумя множествами данных: одним - присоединенным к сертификату, и другим - используемым для создания подписи на сертификате подлинности. На блоке 259 принятия решения, если уровень подобия двух множеств данных превосходит некоторый порог, то блок 250 проверки объявляет, что этот сертификат 210 подлинности подлинный, и наоборот.

На фиг.3А показана схема иллюстративной системы 300 сканирования для восприятия произвольно распределенных признаков объекта 310 аутентификации, связанных с сертификатом подлинности. Система 300 сканирования содержит оптический датчик 322 и источник 324 света. Оптический датчик 322 способен сканировать объект 310 аутентификации и может содержать матрицу устройств с зарядовой связью (ПЗС) с конкретным разрешением. Согласно одному варианту осуществления, оптический датчик 322 имеет разрешение 128×128 пикселей. Источник 324 света способен обеспечивать свет определенной длины волны для освещения зоны аутентификации объекта 310. Источник 324 света может включать в

себя, например, светодиод (СИД). Согласно фиг.3А, один конец волокна 326 объекта 310 аутентификации освещается источником 324 света. Свет проходит к другому концу волокна 326 и воспринимается оптическим датчиком 322.

На фиг.3В показан вид сверху объекта 310 аутентификации, показанного на фиг.3А. В ходе работы система 300 сканирования делит объект 310 аутентификации на зоны, например зоны 311-314. Согласно фиг.3В, источник 324 света системы 300 сканирования излучает свет на зону 314, тогда как зоны 311-313 изолированы от источника 324 света. Благодаря освещению зоны 314 оптический датчик 322 может определить местоположение концевых точек в зонах 311-313 объекта 310 аутентификации. Таким образом, считывание произвольно распределенных признаков в объекте 310 аутентификации включает в себя четыре цифровых изображения, которые содержат четыре разных множеств точек. Каждое множество точек связано с конкретной зоной и определяется путем освещения этой зоны.

Возможно, что развитие технологии, например нанотехнологии, позволяет с помощью электронного устройства декодировать произвольно распределенные признаки из сертификата подлинности и создать световую картину, соответствующую этим признакам. Такое устройство может иметь возможность осуществлять горячую штамповку сертификата подлинности. Согласно одному варианту осуществления, система 300 сканирования может иметь возможность препятствовать этому способу горячей штамповки путем изменения длины волны (т.е. цвета) света, используемого источником 324 света. Например, длину волны света можно случайным образом выбирать каждый раз при сканировании объекта аутентификации системой 300 сканирования. Оптический датчик 322 может иметь возможность обнаруживать длину волны света, излучаемого волокнами объекта аутентификации, и определять, соответствует ли эта длина волны длине волны света, излучаемой источником 324 света. Если длины волны излученного и обнаруженного света не совпадают, то сертификат подлинности, скорее всего, является поддельным.

На фиг.4 показана логическая блок-схема иллюстративного процесса 400, который можно использовать для создания сертификата подлинности. В блоке 405 сканируют объект аутентификации в сертификате подлинности. Объект аутентификации можно сканировать с использованием системы 300, показанной на фиг.3А.

В блоке 410 определяют данные, представляющие произвольно распределенные атрибуты объекта аутентификации. В объекте аутентификации на основе волокон данные могут включать в себя позиции концевых точек освещенных волокон, например концевых точек, показанных на фиг.3В.

В блоке 415 данные сжимают, чтобы повысить уровень защиты сертификата подлинности. Сжатие данных будет подробно рассмотрено со ссылкой на фиг.5. В общих чертах можно определить путь для сжатия части данных, представляющих произвольно распределенные атрибуты объекта аутентификации.

В блоке 420 кодируют сжатые данные. Например, сжатые данные можно подписывать с использованием личного ключа 233, показанного на фиг.2. В блоке 425 кодированные данные включают в сертификат подлинности. Например, кодированные данные можно напечатать в сертификат подлинности в виде штрих-кода, например штрих-кода 213, показанного на фиг.2.

На фиг.5 показана логическая блок-схема иллюстративного процесса 500, который можно использовать для сжатия данных, которые представляют произвольно распределенные атрибуты объекта аутентификации. В целях рассмотрения процесс 500 будет описан применительно к сертификату подлинности на основе волокон. Однако

процесс 500 можно применять к сертификату подлинности любого типа.

В блоке 505 определяют функцию плотности вероятности, связанную с объектом аутентификации. Функция плотности вероятности будет рассмотрена в разделе III-A. Функция плотности вероятности показана в уравнении 11. На фиг.8 показано графическое представление иллюстративной функции плотности вероятности. В общих чертах функция плотности вероятности выражает вероятность того, что единица произвольно распределенных атрибутов находится в определенном месте объекта аутентификации. Применительно к сертификату подлинности на основе волокон функция распределения вероятности может выражать вероятность того, что конкретная точка в зоне объекта аутентификации освещена. Функцию плотности вероятности также можно использовать для вычисления количества волокон, освещаемых в конкретной зоне.

В блоке 510 определяют векторы, связанные с произвольно распределенными атрибутами. Применительно к сертификату подлинности на основе волокон используются двухточечные векторы, и это будет рассмотрено в разделе IV-A. В частности, уравнение 16 можно использовать для вычисления двухточечных векторов для выражения произвольно распределенных атрибутов в сертификате подлинности на основе волокон.

В блоке 515 векторы кодируют с использованием алгоритма арифметического кодирования. Алгоритм арифметического кодирования будет рассмотрен в разделе IV-A. Иллюстративный алгоритм показан в таблице 2.

В блоке 520 определяют путь для сжатия части векторов в фиксированном объеме данных. Способ вычисления пути рассмотрен в разделе IV-B. Иллюстративный путь можно вычислить с использованием уравнения 20. В блоке 525 возвращают путь сжатых данных, выражающий часть произвольно распределенных атрибутов.

III. Модель сертификата подлинности

В этом разделе рассматривается аналитическая модель сертификата подлинности на основе волокон. Смоделированы два признака сертификата подлинности S. Исходя из того, что освещена конкретная зона S_i сертификата подлинности, вычисляют функцию плотности вероятности освещения конкретной точки в $S\text{-}S_i$. Кроме того, исходя из того, что в S находится K волокон, вычисляют ожидаемое количество волокон, освещаемых в $S\text{-}S_i$.

A. Распределение освещенных концевых точек волокон

Объект (L,R,K) аутентификации моделируется как квадрат со стороной L единиц и K волокнами фиксированной длины $R \leq L/2$, произвольно разбросанных по объекту. Из этой модели можно вывести другие варианты модели, например объект с переменной длиной волокна или объект произвольной формы. Объекты аутентификации располагаются в положительном квадранте двухмерной прямоугольной системы координат, как показано на фиг.1. Кроме того, объект аутентификации делят на четыре равных квадрата $S=\{S_1,S_2,S_3,S_4\}$. Затем каждый из них используют для записи трехмерной структуры волокон, как описано выше со ссылкой на фиг. 3A и 3B. Затем волокно обозначают как упорядоченную пару $f=\{A,B\}$ точек $A,B \subset S$, причем расстояние между ними $\|A-B\|=R$.

Определение 1. Распределение освещенных концевых точек волокон

Пусть один из квадратов S_i освещен, тогда функция плотности вероятности (ФПВ) $\varphi(i,Q(x,y))$ определяется для любой точки $Q(x,y) \subset S\text{-}S_i$ через вероятность $\xi(i,P)$ того,

что область $P \subset S\text{-}S_i$ содержит освещенную концевую точку A волокна f={A,B} при условии, что другая концевая точка B располагается в освещенной зоне S_i. Более формально для любой $P \subset S - S_i$

$$\xi(i,P)=Pr[A \subset P | f=\{A,B\} \subset S, B \subset S_i] = \iint_{Q(x,y) \subset P} \varphi(i, Q(x,y))dxdy \qquad (6)$$

Предположим, что бросание волокна f={A,B} в объект аутентификации состоит из двух зависимых событий: (i) первая концевая точка A попадает в объект аутентификации, и (ii) вторая концевая точка B достигает объекта аутентификации. Хотя A может попасть в любое место СП (сертификата подлинности), позиция B зависит от местоположения A. Концевая точка B должна попасть на часть периметра круга с центром в A и радиусом R и содержащегося в объекте аутентификации. В оставшейся части этой подобласти функцию $\varphi(i,Q(x,y))$ аналитически вычисляют на основании анализа событий (i-ii). Для краткости для случая, когда освещена зона S_1, вычисляется только $\varphi(1,Q(x,y))$. $\varphi(1,Q(x,y))$ вычисляется в два этапа.

Определение 2. Ограничение периметра

Во-первых, для данной точки $A \subset S$ определяют функцию $\rho(A)$, которая выражает длину части периметра (дуги) круга с центром в A и радиусом R, который целиком заключен в объекте S аутентификации. В объекте аутентификации имеется четыре разных зоны (обозначенные P1-P4 на фиг.6), где $\rho(A)$ однородно вычисляется.

На фиг.6 изображено графическое представление областей P1-P4, соответствующих четырем различным зонам в иллюстративном объекте 600 аутентификации. Для каждой точки в определенной области Px вычисляют функцию ограничения периметра с использованием замкнутой аналитической формы, характерной для этой области, с использованием уравнений 7-10, которые рассмотрены ниже.

Область P1

Это центральная область объекта аутентификации, где для любой точки $Q \subset P1$ окружность радиуса R с центром в Q не пересекается ни с какими сторонами объекта аутентификации. Границы области заданы следующим образом: $R \le x \le L\text{-}R$, $R \le y \le L\text{-}R$.

$$\rho(Q(x,y))=2R\pi. \qquad (7)$$

Область P2

Имеется четыре разных зоны P2, где окружность радиуса R с центром в любой точке $Q \subset P2$ дважды пересекается с одной и той же стороной объекта аутентификации. Для краткости рассмотрим только следующий случай:

$R \le x \le L\text{-}R$, $0 \le y < R$. Уравнения для трех других зон можно вычислить симметрично.

$$\rho(Q(x,y)) = R\left[\pi + 2\arcsin\left(\frac{y}{R}\right)\right] \qquad (8)$$

Область P3

Имеется четыре разных зоны P3, где окружность радиуса R с центром в любой точке $Q \subset P3$ дважды пересекается с двумя разными сторонами объекта аутентификации. Рассмотрим только следующий случай: $0 \le x < R$, $0 \le y < R$, $x^2 + y^2 \ge R^2$.

$$\rho(Q(x,y)) = 2R\left[\pi - \arccos\left(\frac{x}{R}\right) - \arccos\left(\frac{y}{R}\right)\right] \qquad (9)$$

Область P4

Имеется четыре разных зоны P3, где окружность радиуса R с центром в любой точке Q ⊂ P4 по одному разу пересекается с двумя краями СП. Рассмотрим только следующий случай: $x^2 + y^2 < R^2$.

$$\rho(Q(x,y)) = 2R\left[\pi + \arccos\left(\frac{x}{R}\right) + \arccos\left(\frac{y}{R}\right)\right] \quad (10)$$

Во всех уравнениях 8-10 фактическая φ(1,Q(x,y)) вычисляется исходя из того, что освещенная концевая точка A волокна f={A,B} находится в позиции A=Q(x,y), только если B находится на части(ях) окружности C(Q,R) с центром в Q(x,y) с диаметром R и содержащейся в S_1.

Лемма 3. Зависимость φ(i,Q(x,y)) от ρ(Q(x,y)).

Используя функцию ρ(Q(x,y)), вычисляют ФПВ φ(i,Q(x, y)) с использованием следующего интеграла:

$$\varphi(i,Q(x,y)) = \int_{C(Q,R)\subset S_i} \frac{\alpha R d\vartheta}{\rho(Q(x+R\cos\vartheta, R\sin\vartheta))} \quad (11)$$

где ϑ описывает периметр C(Q,R)⊂S и α является константой, так что:

$$\iint_{Q(x,y)\subset S_i} \varphi(i,Q(x,y))dxdy = 1 \quad (12)$$

Точка Q⊂S-S_i может быть освещена только благодаря волокну f={Q,B}, так что B⊂S_i. Отсюда следует, что B расположена где-то на периметре круга C(Q, R), содержащегося в S_i. Для данного волокна f={A,B} вероятность того, что A лежит на конкретной бесконечно малой дуге длиной dl⊂S, равна dl/ρ(B). Следовательно:

$$\varphi(i,Q) = area\,(S - S_i)^{-1} \int_{C(Q,R)\subset S_i} \frac{4Rdld\,\vartheta}{\rho(B(Q,R,\vartheta)\subset dl} \quad (13)$$

где функция area(S-S_i) вычисляет площадь под S-S_i. Таким образом, ФПВ φ(1,Q(x,y)) в точке Q⊂S-S_1 пропорциональна интегралу от величины, обратной ρ(•), по C(Q,R)⊂S_1.

На фиг.7 показано графическое представление девятнадцати различных зон иллюстративного объекта 700 аутентификации, которые имеют характерные аналитические формулы в качестве решения интеграла, приведенного в уравнении 11. Для простоты φ(1,Q(x,y)) приблизительно решается с использованием простого численного расчета. Результаты приведены на фиг.8.

На фиг.8 показан график иллюстративной функции плотности вероятности для квадратного объекта аутентификации с параметрами L=64 и R=28, дискретизированной в единичных точках. На фиг.8 показано, что вероятность того, что концевая точка волокна лежит в определенной малой области P⊂S-S_i, значительно изменяется в зависимости от конкретного положения P в S-S_i. Используя информацию об изменении φ(i,Q(x,y)) в пределах S-S_i, можно значительно усовершенствовать алгоритмы сжатия подмножества точек, что представлено в разделе IV. Изготовление объекта аутентификации, характеризуемого φ(i,Q(x,y))=const по всей области S-S_i, является нетривиальной задачей, вероятно, столь же сложной, как и горячая штамповка оригинального объекта аутентификации.

Таблица 1

Область	Границы	$\psi(1,Q(x,y))$
T0	$0 \le x \le L/2-R, \quad 0 \le y \le L/2-R$	0
T1	$x^2+(y-L/2)^2 < R^2,$ $0 \le x \le L/2-R,$ $L/2-R < y \le L/2$	$R\left[\arcsin\left(\frac{x}{R}\right)+\arccos\left(\frac{L/2-y}{R}\right)\right]$
T2	$x^2+(y-L/2)^2 \ge R^2,$ $0 \le x \le L/2-R,$ $L/2-R < y \le L/2$	$2R\arccos\left(\frac{L/2-y}{R}\right)$
T3	$x^2+(y-L/2)^2 \ge R^2,$ $(x-L/2)^2+y^2 \ge R^2,$ $(x-L/2)^2+(y-L/2)^2 \ge R^2$	$2R\left[\arccos\left(\frac{L/2-y}{R}\right)+\arccos\left(\frac{L/2-x}{R}\right)\right]$
T4	$x^2+(y-L/2)^2 < R^2,$ $(x-L/2)^2+y^2 < R^2,$ $(x-L/2)^2+(y-L/2)^2 \ge R^2$	$R\left[\arcsin\left(\frac{x}{R}\right)+\arcsin\left(\frac{y}{R}\right)\right]$ $R\left[\arccos\left(\frac{L/2-y}{R}\right)+\arccos\left(\frac{L/2-x}{R}\right)\right]+$
T5	$x^2+(y-L/2)^2 < R^2,$ $(x-L/2)^2+y^2 < R^2,$ $(x-L/2)^2+(y-L/2)^2 < R^2$	$R\left[\frac{\pi}{2}+\arcsin\left(\frac{x}{R}\right)+\arcsin\left(\frac{y}{R}\right)\right]$
T6	$x^2+(y-L/2)^2 < R^2,$ $(x-L/2)^2+y^2 \ge R^2,$ $(x-L/2)^2+(y-L/2)^2 \ge R^2,$ $L/2-R < x \le L/2$	$R\left[\arcsin\left(\frac{x}{R}\right)+\arccos\left(\frac{L/2-y}{R}\right)\right]+$ $2R\arccos\left(\frac{L/2-x}{R}\right)$
T7	$x^2+(y-L/2)^2 < R^2,$ $(x-L/2)^2+y^2 \ge R^2,$ $(x-L/2)^2+(y-L/2)^2 < R^2$	$R\left[\frac{\pi}{2}+\arcsin\left(\frac{x}{R}\right)+\arccos\left(\frac{L/2-x}{R}\right)\right]$
T8	$x^2+(y-L/2)^2 \ge R^2,$ $(x-L/2)^2+y^2 \ge R^2,$ $(x-L/2)^2+(y-L/2)^2 < R^2$	$R\left[\frac{\pi}{2}+\arccos\left(\frac{L/2-y}{R}\right)+\arccos\left(\frac{L/2-x}{R}\right)\right]$

B. Отношение освещенности концевых точек волокна

Определение 3. Отношение освещенности концевых точек волокна

Для объекта аутентификации (L,R,K) и его освещенной зоны S_i отношение освещенности λ определяется как вероятность того, что волокно f={A,B} легло так, что одна из его концевых точек находится в $B \subset S\text{-}S_i$, при том условии, что другая его концевая точка находится в $A \subset S_i$:

$$\lambda = Pr[B \subset S\text{-}S_i | f=\{A,B\}, A \subset S_i] \qquad (14)$$

Определение 4. Возможно освещенная дуга

Для любой точки $A \subset S_i$ определяют функцию $\psi(i,A(x,y))$, которая измеряет длину части периметра C(A,R), содержащегося в $S\text{-}S_i$.

На фиг.9 показано графическое представление областей T0-T8, где $\psi(i,Q(x,y))$ вычисляется с использованием характерных замкнутых аналитических форм. $\psi(i,Q(x,y))$ аналитически вычисляют на основании анализа событий (i-ii) из раздела III-A. По аналогии с разделом III-A вычисление производится только в случае, когда зона S_i освещена. В СП имеется девять различных зон (обозначенных T0-T8 на фиг.9), где $\psi(1,Q)$ вычисляется однородно. Аналитические замкнутые формы для $\psi(1,Q)$, зависящие от местоположения Q в S_i, приведены в таблице 1.

Лемма 4. Зависимость $\psi(1,Q(x,y))$, $\rho(Q(x,y))$ и λ.

Отношение освещенности, определенное в определении 3, можно вычислить следующим образом:

$$\lambda = \int_{Q(x,y)\subset S_i} \frac{\psi(i,Q(x,y))}{\rho(Q(x,y))} dxdy \qquad (15)$$

Круг с центром в точке $A \subset S$ и радиусом R обозначен C(A,R). Для каждой точки $Q \subset S_i$ вероятность того, что другая концевая точка B волокна $f=\{Q,B\}$ лежит в $S\text{-}S_i$, равна отношению длин частей периметра C(Q,R), содержащихся в $S\text{-}S_i$ и S соответственно. Интегрируя это отношение по всем точкам в S_i, получаем уравнение 15.

С учетом того, что объект аутентификации (L,R,K) с использованием λ вычислен путем численной аппроксимации уравнения 15 и замкнутых форм для $\psi(1,Q)$ и таблицы 1, можно вычислить ожидаемое число освещенных точек в $S\text{-}S_i$, когда S_i освещена как $\lambda K/2$. Например, для объекта аутентификации (64,28,100) результирующее $\lambda \approx 0.74$, и это значит, что в среднем число освещенных концевых точек в случае, когда S_i освещена, составляет примерно $0.74 \times 50 = 37$.

IV. Сжатие подмножества точек в СП

Цель системы сертификата подлинности состоит в том, чтобы задача изготовления (т.е. горячей штамповки) конкретного экземпляра объекта аутентификации была как можно труднее. Эта цель количественно выражается в необходимости записи позиций как можно большего количества волокон объекта аутентификации. В иллюстративном алгоритме сжатия количество зон объекта аутентификации равно четырем; поэтому для каждой зоны S_i четверть $n_M/4$ битов подписанного сообщения m выделяется для сохранения как можно большего количества концевых точек волокон, освещенных в $S\text{-}S_i$, когда свет падает на S_i. Заметим, что в общем случае не все освещенные точки нужно сохранять; кодировать с использованием $n_M/4$ битов можно только наибольшее подмножество этих точек.

В этом разделе мы опишем механизм, способный кодировать расстояние между двумя освещенными точками в объекте аутентификации. Механизм основан на арифметическом кодировании. Затем мы формализуем задачу сжатия как можно большего количества концевых точек с использованием постоянного числа битов. Наконец, мы покажем, что эта задача является NP-полной, и представим конструктивную эвристику в качестве субоптимального решения.

A. Кодирование двухточечных векторов

В этом подразделе мы опишем, как вектор, заданный своими начальной и конечной

точками, кодируется с использованием количества битов, близкого к минимальному. Дополнительное ограничение состоит в том, что точки в рассматриваемой области появляются в соответствии с данной ФПВ.

1) Арифметическое кодирование

Арифметический кодер (АК) преобразует входной поток произвольной длины в единичное рациональное число в [0,1}. Главная сила АК в том, что он может сжимать как угодно близко к энтропии. Ниже мы покажем, как слово "aba" кодируется с использованием алфавита с неизвестной ФПВ появления символов.

На фиг.10 показано графическое представление примера того, как арифметический кодер кодирует строку "aba" с использованием алфавита L={a,b} с неизвестной ФПВ появления символов. Пример показан на фиг.10.

Первоначально диапазон АК сбрасывают на [0,1} и каждому символу в L назначают равную вероятность появления Pr[a]=Pr[b]=1/2. Таким образом, АК делит свой диапазон на два поддиапазона [0,0.5} и [0.5,1}, каждый из которых представляет "b" и "a" соответственно. Символ “a” кодируется сужением диапазона АК до диапазона, соответствующего этому символу, т.е. [0.5,1}. Кроме того, АК обновляет счетчик появления символа “a” и повторно вычисляет Pr[a]=2/3 и Pr[b]=1/3. В следующей итерации, согласно обновленным Pr[a], Pr[b], АК делит свой диапазон на [0.5,0.6667} и [0.6667,1}, каждый из которых представляет "b" и "a" соответственно. При следующем появлении "b" АК сужает свой диапазон до соответствующего [0.5,0.6667}, обновляет Pr[a]=Pr[b]=2/4 и делит новый диапазон на [0.5,0.5833} и [0.5833,0.6667}, каждый из которых представляет "b" и "a" соответственно. Поскольку последним символом является "a", АК кодирует этот символ, выбирая в качестве выходного значения любое число в [0.5833,0.6667}. Выбирая число, которое кодируется минимальным числом битов (в нашем примере, цифр), 0.6, АК создает свое окончательное выходное значение. Декодер воспринимает длину сообщения либо явно в заголовке сжатого сообщения, либо в особом символе “конец файла”.

АК итеративно сужает свой рабочий диапазон вплоть до момента, когда его диапазон становится таким, что старшие цифры верхней и нижней границ оказываются одинаковыми. Тогда старшую цифру можно передавать. Этот процесс, именуемый перенормировкой, позволяет сжимать файлы любой длины на арифметических модулях ограниченной точности. Усовершенствования в работе классического АК сосредоточены на: использовании заранее вычисленных аппроксимаций арифметических расчетов, замене деления и умножения сдвигом и сложением.

АК кодирует последовательность входящих символов $s=s_1,s_2,...$ с использованием количества битов, равного энтропии источника, $H(s) = -\sum_{s_i} \Pr[s_i]\log_2(\Pr[s_i])$.

Поэтому для полубесконечного потока независимых и одинаково распределенных символов на компьютере с арифметикой бесконечной точности АК является оптимальным энтропийным кодером.

Арифметическое кодирование двухточечного вектора с минимальным расстоянием

Пусть свет падает на один из квадрантов S_i объекта аутентификации (L,R,K). Затем предположим, что объект аутентификации разделен на сетку из L×L единичных квадратов U=u(i,j), i=1...L, j=1...L, где каждый u(i,j) покрывает квадратную область в x∈{i-1,i], y∈{j-1,j]. Единичные области моделируют пиксели цифрового сканирования объекта аутентификации. Разрешение сканирования равно L×L. Затем главную точку единицы u(x,y) задают как точку Q_u с координатами (x,y).

Лемма 5. Вероятность освещения единицы.

Если предположить, что имеется κ волокон, имеющих в точности одну концевую точку в $S\text{-}S_i$, вероятность того, что единичная область $u(x,y)\subset S\text{-}S_i$ содержит, по меньшей мере, одну освещенную концевую точку волокна, равна:

$$r(u)=Pr[(\exists f=\{A,B\}\in F)A\subset u,B\subset S_i]=1-[1-\xi(i,u)]^{\kappa} \quad (16)$$

и

$$\tau(u)=Pr[(\exists f=\{A,B\}\in F)A\subset u,B\subset S_i]=1-Pr[(\neg\exists c\in F)A\subset u,B\subset S_i]=1-\{1-Pr[A\subset u,B\subset S,|f=\{A,B\}]\}^{\kappa}$$

Из уравнения 7 выводится уравнение 16. В разделе III-B вычисляется ожидание для κ, равное $E[\kappa]=\lambda K/2$.

Задача I. Двойное векторное кодирование для СП

При том условии, что единица $u\subset S\text{-}S_i$ содержит освещенную концевую точку волокна, задача состоит в том, чтобы кодировать с использованием как можно меньшего числа битов местоположения двух других освещенных единиц v_1 и v_2 относительно единицы u. Дополнительное ограничение состоит в том, что среди всех освещенных единиц в $S\text{-}S_i$ главные точки v_1 и v_2, Q_1 и Q_2 соответственно располагаются на двух кратчайших расстояниях в евклидовом смысле от главной точки u, Q_u. Правило приоритетов установлено таким образом, что если множество единиц V, $|V|>1$ находится на одном и том же расстоянии по отношению к u, то та из них, которая имеет наибольшую вероятность освещения: $\text{argmax}_{v\in V}(\tau(v))$, кодируется первой.

Таблица 2

Алгоритм A1

Задать U как список всех единичных областей в $S\text{-}S_i\text{-}u$.

Список всех помеченных единиц, $M(u)$, задан как $M(u)=\varnothing$.

делать

Найти все единичные области $V=\arg\min_{v\in U}\|Q_v-Q_u\|$

делать

Найти единичную область $w=\text{argmax}_{v\in V}\,\xi(1,v)$

Задать диапазон АК для w равным $\gamma(w,u)$ (см. уравнения 17, 18)

Множество узлов перед w равно $M_w(u)=M(u)$.

$M(u)=M(w)\cup w$, $V=V\text{-}w$, $U=U\text{-}w$.

пока $V\neq\varnothing$

пока $U\neq\varnothing$

Кодирование вектора от единицы к единице производится с использованием АК, который использует алгоритм A1 для назначения соответствующего диапазона на интервале кодирования каждому символу кодирования, т.е. каждой единице $v \subset S\text{-}S_i$, отличной от исходной единицы u. Для каждой единицы v алгоритм A1 назначает диапазон, равный вероятности того, что v является одной из двух ближайших освещенных единиц относительно исходной единицы u. Эта вероятность обозначается как $p(v|u)$. В случае, когда ожидается, что $\kappa >> 1$ единиц освещены в $S\text{-}S_i$, $p(v|u)$ можно вычислить следующим образом:

$$p(v|u) = \tau(v) \prod_{w \subset M_v(u)} [1 - \tau(w)] + \sum_{w \subset M_v(u)} \tau(v)\tau(w) \prod_{z \subset M_v(u), z \neq w} [1 - \tau(z)] \quad (17)$$

где множество единиц $M_v(u)$ вычисляется, как в алгоритме 1. Для каждой единицы v алгоритм A1 назначает диапазон $\gamma(y,v)$, используемый АК для кодирования, с тем условием, что u уже закодирована. Этот диапазон равен:

$$\gamma(v,u) = \frac{p(v|u)}{\sum_{w \subset S - S_i} p(w|u)} \quad (18)$$

Таким образом, две ближайших освещенных единицы кодируются конструкцией почти оптимально (например, кодирование оптимально на процессоре с арифметикой бесконечной точности), поскольку последовательность символов кодируется с использованием числа битов, приблизительно равного энтропии источника:

$$H(u) = -\sum_{v \subset S - S_i} \gamma(v,u) \log_2[\gamma(v,u)] \quad (19)$$

Двойное векторное кодирование используется как примитив для кодирования подмножества точек во всем алгоритме сжатия, представленном в разделе IV-B. Хотя алгоритм кодирования близок к оптимальному для множества предположений, представленных в разделе IV-A.2, то же самое множество ограничений не пригодно для задачи сжатия в целом, поэтому в разделе IV-B рассматривается внутренняя оптимальность использования арифметического кодирования в диапазоне выделения через A1.

B. Сжатие подмножества точек

Рассмотрим модель задачи оптимизации для сжатия позиций как можно большего количества освещенных единичных областей с использованием фиксированного числа битов. Рассмотрим следующий ориентированный полный граф со взвешенными ребрами. Для каждой освещенной единицы $u \subset S\text{-}S_i$ создается узел n_u. Ориентированное ребро $e(u,v)$ от узла n_u к узлу n_v взвешено оптимальной длиной кодового слова, которое кодирует вектор, указывающий на v, $\omega(e(u,v)) = -\log_2[\gamma(v,u)]$, как в уравнении 19, при том условии, что u уже закодирована. Обозначим этот граф как $G(N,E,\Omega)$, где N, E и Ω представляют множество узлов, ориентированных ребер и соответствующих весовых коэффициентов соответственно.

Задача 2. Сжатие подмножества точек (СПТ)

ДАНО: ориентированный, полный и взвешенный граф $G(N,E)$ с неотрицательной вершинной функцией $Q: E \rightarrow R$, положительное целое $l_{min} \in Z^+$, положительное

действительное число $\Lambda \in R^+$.

ВОПРОС: существует ли подмножество из $l > l_{min}$ узлов $N^* \subset N$ с путем через них, т.е. перестановка $<n^*_{\pi(1)},...,n^*_{\pi(l)}>$, так что сумма весовых коэффициентов вдоль пути равна:

$$\sum_{i=1}^{l-1} \omega\left(e\left(n^*_{\pi(i)}, n^*_{\pi(j+l)}\right)\right) < \Lambda \qquad (20)$$

Задача 2 моделирует задачу оптимизации для сжатия как можно большего количества (т.е. l) концевых точек волокна в объекте аутентификации с использованием фиксированного хранилища (т.е. A). Эта задача является NP-полной, поскольку можно показать, что асимметричную задачу коммивояжера, АЗК, можно свести к СПТ, $АЗК \leq_m^p СПТ$ путем двоичного поиска по A. В остальной части этого раздела представлена конструктивная эвристика A2, нацеленная на решение этой задачи. Главное конструктивное требование для эвристики состоит в высокой производительности во время выполнения, поскольку каждый сертификат подлинности нужно подписывать отдельно на производственной линии.

Во-первых, мера расстояния между двумя узлами в N не подчиняется неравенству треугольника для всех узлов. Интуитивно, процедура кодирования из раздела IV-A кодирует векторы в S-S_i с использованием количества битов, пропорционального вероятности того, что определенная единица является одной из двух ближайших освещенных точек. Поэтому единицы, более далекие от исходного узла, кодируются значительно более длинными кодовыми словами, поскольку они, скорее всего, не появляются, из-за чего быстрые переходы к этим узлам в решении являются крайне нежелательными.

Теорема 2. Мера ω расстояния не всегда удовлетворяет неравенству треугольника: $\omega(e(u, v)) + \omega(e(v, w) \geq \omega(u, w)$.

Для простоты предположим, что $(\forall u \subset S\text{-}S_i)$, $t=\tau(u)=const$, тогда u, v, и w располагаются вдоль одной линии в S-S_i. Эвклидовы расстояния $||y-v||$, $||v-w||$, и $||y-w||$ равны a, b, и $a+b$ соответственно. Из неравенства треугольника следует, что $f(u,v,w)=\log_2[\gamma(w,u)]-\log_2[\gamma(v,u)]-\log_2[\gamma(w,v)]\geq 0$. Из уравнений 17 и 18 можно вывести:

$$f(a,b,t) = 2ab\pi \log_2(1-t) + \log_2 \frac{t}{1-t} - \log_2 \frac{(1-t)^2 + (a^2+b^2)\pi t(1-t) + a^4b^4\pi^2t^2}{1+\left[(a+b)^2\pi - 1\right]t} \qquad (21)$$

и показать, что для $ab\pi t>>1$ неравенство треугольника не выполняется, т.е. $f(a,b,t)<0$.

Наилучший алгоритм для АЗК, где выполняется неравенство треугольника, дает решения самое большее в $\log(|N|)$ раз хуже оптимального. Альтернативно, насколько известно авторам, алгоритмы аппроксимации для вариантов АЗК, где не выполняется неравенство треугольника, не были разработаны. В общем случае при произвольной метрической функции расстояния ω задача АЗК является NPO-полной, т.е. не существует хорошего алгоритма аппроксимации, если не $P=NP$. С другой стороны, алгоритмы аппроксимации для вариантов ЗК, которые удовлетворяют расширенной версии неравенства треугольника: $\mu(\omega(e(u,v))+\omega(e(v,w)))\geq\omega(u,w)$, $\mu>1$, могут быть решены с результатом, в худшем случае, в $(3\mu+1)\mu/2$ хуже оптимального решения. Метрика расстояний ω не подчиняется этому ограничению, поэтому эвристика для задачи 2 разработана без гарантии на худший случай. Можно разместить экземпляр объекта аутентификации, который нельзя удовлетворительно сжать. Вероятность

этого события должна быть мала, менее одного на миллион.

Таблица 3

Алгоритм A2

КОНСТРУКТИВНАЯ ФАЗА

Множество ребер $E' = \{argmin_e(\omega(a,b),\omega(b,a)) \mid (\forall a,b) \subset N\}$

Множество подпутей P выбирают как множество кратчайших K ребер в E', так что $\sum_{i=1}^{K} \omega(e_i) \leq \Lambda$ сортируются по ω.

Обозначим вес кратчайшего ребра в E как ω_{min},

для каждого пути $p_i \subset P$, $i = 1..K\text{-}1$

для каждого пути $p_j \subset P$, $j = i+1..K$

если p_i и p_j имеют общий начальный-конечный узел

Связать p_i и p_j как $p_i = p_i|p_j$.

Удалить p_j из P.

Обозначим начальный и конечный узлы пути $p_i \subset P$ как s_i и d_i.

Соответственно

для каждого пути $p_i \subset P$, $i = 1..K$

Найти кратчайшие пути $q(i,j)$ от s_i к любому d_j, $j \neq i$.

Пока $|P| < \max P$

$$(p_i, p_j) = \arg\min_{q(i,j)} \sum_{e \subset \{p_i | q(i,j) | p_j\}} \frac{\omega(e)}{|\{p_i \mid q(i,j) \mid p_j\}|}$$

Присоединить $p_i = p_i|q(i,j)|p_j$ и удалить p_j из P.

Найти исчерпывающе присоединение $p_h = p_1|\ldots|p_{maxP}$, так что

$$M(p_h)\left\{\sum_{e \subset P_h} \omega(e) < \Lambda \quad \text{и} \quad |p_h| \quad \text{максимально}\right\}$$

reroute(p_h)

reroute(p_h)

$p_{лучш} = p_h$

для каждого ребра $e(s_i,d_i) \subset p_h$, $i = 1,\ldots,|p_h|\text{-}1$

для каждой пары узлов $(d_i, s_j) \subset p_h, j = i+2,\ldots,|p_h|\text{-}1$.

Найти кратчайший путь $q(i,j)$ через узлы в $N\text{-}p_h$.

если путь $e_1,\ldots,e_i|q(i,j)e_j,\ldots,e_{|p_h|}$ имеет лучшую

метрику $M(p_h)$, чем $p_{лучш}$, **то** $p_{лучш} = p_h$.

ЖАДНОЕ ИТЕРАТИВНОЕ УСОВЕРШЕНСТВОВАНИЕ

повторить I раз

Стянуть p_h, так что $\sum_{e \subset p_h} \omega(e) \leq \rho\Lambda$, где ρ – коэффициент стягивания, произвольно выбранный из $\rho \in \{0.4, 0.8\}$.

Обозначим узлы n_0 и n_1 как первый и последний узел в p_h.

пока $\sum_{e \subset p_h} \omega(e) \leq \Lambda$

Среди ребер, которые имеют n_0 или n_1 в качестве конечного или начального узла соответственно.

Присоединить e к p_h.

reroute(p_h)

Предпосылкой использования метрики расстояний ω из раздела IV-A является предположение, что хорошее решение обеспечивает прохождение через каждый узел на своем маршруте через два ближайших соседних узла. Поэтому в рамках задачи 2 используемая метрика является оптимальной, только если наилучшее найденное решение удовлетворяет этому свойству. Если конечное решение не имеет этого свойства, оптимальность кодирования единичного вектора зависит от распределения весовых коэффициентов ребер в решении.

Разработанная эвристика A2 имеет две стадии: конструктивную фазу и фазу итеративного усовершенствования. Конструктивная фаза подчиняется жадной эвристике, которая строит первоначальное решение. Сначала A2 идентифицирует множество доминирующих ребер E′. Для каждой пары ребер *e(u,v), e(v,u)* между узлами *u, v,* A2 выбирает только более короткое из двух и сохраняет его в E′. Затем создается множество P из первоначальных подпутей путем сортировки ребер в E′ и выбора K кратчайших ребер, для которых сумма весовых коэффициентов как можно ближе к Λ. Первый и последний узел в пути p_i обозначаются как s_i и d_i соответственно. На следующем этапе A2 присоединяет подпути из P итеративно в порядке возрастания их весовых коэффициентов: в любой точке пара кратчайших подпутей p_i, p_j, имеющих общий начальный-конечный узел $d_i=s_j$, связывается, пока не будут созданы все возможные соединения. В маловероятном случае, когда $|P|=1$, находится оптимальное решение, и поиск останавливается. В противном случае все однореберные подпути удаляются из P. Затем с использованием алгоритма Дейкстры A2 находит все кратчайшие пути между каждым конечным хвостом d_i каждого подпути p_i в P и начальными хвостами всех остальных подпутей s_j, $i=1...|P|$, $i\neq j$. Кратчайшие пути обходятся через узлы, не принадлежащие P. Кратчайший путь между s_i и d_j обозначается как $q(i,j)$. На другом жадном этапе A2 сортирует все сочленения $p_i/q(i,j)/p_j$ по их отношению вес/счетчик узлов. В порядке возрастания этой метрики A2 продолжает присоединять подпути в P через узлы в *N-P*, пока суммарное количество оставшихся путей не станет равным |P|=maxP (обычно maxP=9). Оставшиеся пути присоединяются с использованием точного алгоритма, который находит путь p_h с оптимальной метрикой: максимальной мощностью и суммой весов, меньшей A. На конечном этапе процедура повторного обхода просматривает все узлы в P и, используя алгоритм Дейстры, пытается найти кратчайшие пути к другим узлам в P через оставшиеся узлы в E. Та же процедура также пытается найти лучший конечный хвост, чем тот, который существует в p_h. Для каждого повторного обхода A2 проверяет, имеет ли новый повторный обход лучшую метрику, чем текущий, наилучший путь p_h. На фиг.11 показан пример экземпляра объекта аутентификации (512,0.4·512,256), в котором имеется $\kappa=88$ узлов. A2 возвратил путь, показанный жирными линиями. Путь таков, что его сумма весовых коэффициентов меньше $\Lambda = 512$. Для документирования пути используется 12.11 битов на точку.

На фазе итеративного усовершенствования мы несколько раз повторяем следующий цикл. На первом этапе A2 стягивает наилучший найденный к настоящему моменту путь $p_{лучш}$ в p_h, так что $|p_h|$ максимален, и сумма весовых коэффициентов вдоль p_h меньше доли $\rho\Lambda$. Параметр стягивания ρ произвольно выбирают в каждой итерации в $\rho \in \{0.4,0.8\}$. Узлы n_0 и n_l обозначены как первый и последний узел в p_h. Хотя сумма весовых коэффициентов в p_h меньше Λ, среди ребер, которые имеют n_0 или n_l в качестве конечного или начального узла соответственно, находим ребро e с минимальным весом присоединяем его к p_h. Когда новый путь-кандидат p_h создан, его принимают как наилучшее решение, если его метрика лучше метрики наилучшего пути, созданного до сих пор. На последнем этапе цикла итеративного усовершенствования A2 осуществляет вышеописанную процедуру повторного обхода.

Для приспособления времени прогона A2 для конкретного класса объектов аутентификации (L,R,K) в пределах одной секунды цикл усовершенствования

повторяется I = {100,10000} раз. В целом, сложность A2 в наихудшем случае составляет $O(|M|^3 \log|M)$, когда кратчайшие пути с множественными источниками вычисляются посредством алгоритма Дейкстры. В реализации, которая использует алгоритм Флойда-Варшалла для вычисления всех пар кратчайших путей, сложность A2 можно снизить до $O(|N|^3)$. Хотя граф изначально полон, удаляя ребра с высокими весовыми коэффициентами, мы создаем разреженный граф, где алгоритм Джонсона для кратчайших путей всех пар дает $O(|N|^2 \log|N|+|N||E|)$.

V. Эмпирическая оценка

В этом разделе показано, как параметры объекта аутентификации (L,R,K) влияют на производительность алгоритма A.2. На фиг.11 показано решение для одного варианта этой задачи, объекта аутентификации (512,0.4·512,256). Сетка сканирования до L=512 ячеек сканирования. На чертеже описан случай, когда освещен нижний левый квадрант объекта аутентификации. Граф $G(N,E)$, построенный с использованием соответствующих освещенных концевых точек волокна, показан линиями средней толщины. Показаны только десять кратчайших ребер, начинающихся с каждого из к = 88 узлов графа. Результирующий путь, показанный на чертеже с использованием толстых линий, состоит из 41 точек. Сумма весовых коэффициентов вдоль ребер пути меньше лимита хранилища: A = 512 бит. Путь сжимается с использованием 12.11 битов на концевую точку волокна (б/ктв). Сохранение данных без сжатия потребовало бы 41·18=738 битов, что дает коэффициент сжатия 0.61. Коэффициент сжатия определяется как отношение размера сжатого сообщения к размеру исходного сообщения.

VI. Цель проектирования для системы СП

Целью разработчика сертификата подлинности является максимизация стоимости горячей штамповки ζ_f с использованием ограниченной стоимости изготовления ζ_m. На ζ_m может влиять несколько параметров. Для краткости и простоты рассмотри три параметра:

суммарная длина волокна $RK \leq \Phi$,

допуск сканирования ζ и

хранилище штрих-кода Λ.

Производительность системы оптимизируется путем ограничения количества попыток, доступных противнику, для точного позиционирования достаточного подмножества подписанных концевых точек волокна (раздел VI-A) и выбора параметров системы $\{R_*,K_*\}$, так что ожидаемая стоимость горячей штамповки $\zeta_f(A2)$ достигает максимума (раздел VI-B).

A. Ограничение количества вражеских попыток

Рассмотрим схему сжатия C, которая сохраняет G из к освещенных концевых точек волокна в хранилище, ограниченном по Λ. В общем случае при горячей штамповке сертификата подлинности противник может использовать все к волокон для размещения, по меньшей мере, $G\zeta$ из них точно в их соответствующих местах. Стоимость горячей штамповки сертификата подлинности в общем случае зависит от количества доступных попыток. Здесь предложена методика для уменьшения количества вражеских попыток K_T путем обнаружения аномального поведения волокон вокруг подписанных концевых точек волокна в ходе проверки.

Таблица 4

Алгоритм A3

ИЗДАНИЕ ЭКЗЕМПЛЯРА СП
Сканировать множество N из κ точек, освещаемых, когда свет падает на S_i с использованием Λ битов, сжатие подмножества $P \subset N$ с $G=\|P\| \leq \kappa$.
Найти подмножество единиц $U \subset S\text{-}S_i$, так что $(\forall u_i \in U)(\forall p_j \in P) min(\|u_i - p_j\|) < \varepsilon_1$.
$\varepsilon_2=\|N \cap U\|-G$, $K_T=G+\varepsilon_2$.
Подписать P, ε_2 и соответствующую информацию (см. раздел 2).
ПРОВЕРКА ЭКЗЕМПЛЯРА СП
Найти подмножество единиц $U \subset S\text{-}S_i$, так что
$(\forall u_i \in U)(\forall p_j \in P) \min(\|u_i - p_j\|) < \varepsilon_1$.
Сканировать множество N' из к' точек, освещаемых, когда свет падает на S_i
если $\|N' \cap U\| > K_T$, **то** экземпляр СП непригоден,
иначе если $\|N' \cap P\| > G\zeta$, **то** экземпляр СП пригоден,
иначе СП непригоден.

Блоки издания и проверки сертификата подлинности повторяют свои части алгоритма A3 для каждого квадранта S_i объекта аутентификации. Блок издания первоначально сканирует экземпляр объекта аутентификации и собирает информацию о множестве точек N, освещаемых, когда S_i освещен. Затем, используя имеющиеся Λ битов, он сжимает наибольшее подмножество $P \subset N$, $|P|=G$, возвращенное A2. Затем A3 находит подмножество $U \subset S\text{-}S_i$, такое, что эвклидово расстояние между каждой единицей $u_i \in U$ и ближайшей к ней единицей $p_j \in P$ не превышает ε_1. Подмножество U единиц представляет ε_1-окрестность P. Затем блок издания подсчитывает количество K_T точек в N, которые принадлежат U. Поскольку K_T должно быть больше G, чтобы предотвратить ложные отрицательные результаты, блок издания сохраняет помимо P разность $\varepsilon_2 = K_T - G$ в сообщении m, которое позднее подписывается с использованием личного ключа блока издания (см. раздел II). Используя общий ключ блока издания, блок проверки извлекает из присоединенной подписи сжатое подмножество P точек и ε_2 и воссоздает соответствующую ε_1-окрестность U. Затем блок проверки сканирует экземпляр объекта аутентификации на предмет множества освещенных волокон N', когда S_i освещен. Он объявляет, что экземпляр подлинный, проверяя, что количество общих точек в U и N' не больше $G+\varepsilon_2$ и что количество общих точек в N' и P не меньше $G\zeta$.

Благодаря сохранению ε_2 в подписи противнику приходится использовать не более $K_T = G + \varepsilon_2$ попыток позиционирования волокон в ε_1-окрестности P. Целью противника является размещение, по меньшей мере, $G\zeta$ концевых точек волокна из P точно, следовательно, противник может позволить себе $G(1 - \zeta) + \varepsilon_2$ неправильных размещений, находящихся в ε_1-окрестности P в процессе горячей штамповки.

Ожидается, что каждая попытка, нацеленная на точку p_i, в случае неудачи заканчивается в ε_1-окрестности p_i. Увеличивая ε_1, блок проверки может идентифицировать возможные неправильные размещения в более обширной окрестности; однако это также увеличивает ожидание для ε_2-значения, которое разработчик сертификата подлинности желает сохранять как можно меньшим.

Ниже показана эмпирическая методология проектирования, которая принимает данное ε_1=const, а затем добивается максимизации главной цели ζ_f(A2) с точки зрения нескольких параметров сертификата подлинности.

B. Проектирование системы СП

Задача 3. Цель проектирования для системы СП

Для данных алгоритма сжатия A2, фиксированного $RK \le \Phi$, ζ, ε_1 и Λ, среза $\{R_*, K_*\}$ имеющегося волокна, которое максимизирует:

$$\{R_*, K_*\} = \arg \max_{\{R,K \mid RK \le \Phi\}} \zeta_f(A2, R, K) \qquad (22)$$

где ζ_f является стоимостью горячей штамповки экземпляра СП.

На фиг.12 показано графическое представление конструкции сертификата подлинности для оптимизированных эффективностей стоимости. По оси абсцисс отложена длина R волокна относительно L, а по оси ординат показано количество волокон L. Полоска иллюстрирует логарифм стоимости горячей штамповки $\log_{10}(\zeta_f(A2,R,K))$ с лимитом ограничения Λ = 512 битов и набором фиксированных параметров: ζ =0.9, ε_1 = 8 и v = 0.8. На чертеже также показано качество решений для всех срезов волокна фиксированной длины $RK = \Phi$ = 100L.

Можно использовать простую эмпирическую методику, которая ищет наилучший срез волокна $\{R_*, K_*\}$. Процедура поиска показана на фиг.12. По оси абсцисс и ординат отложены значения R и K соответственно. Полоска обозначает ожидаемый логарифм стоимости горячей штамповки экземпляра сертификата подлинности, $\log_{10}(\zeta_f(A2,R,K))$.

Стоимость дана в отношении R и K и для фиксированного набора параметров: Λ=512, ζ=0.9, ε_1=8 и v=0.8. Диаграмма на фиг.12 вычислена эмпирически. A2 применяется к 500 произвольно сгенерированным экземплярам сертификата подлинности (512,R,K) с каждой комбинацией из $R=\{0.05L, 0.10L, ..., 0.45L\}$ и K={80, 96, .., 192, 256, 384, 512, 768 ,1024}. Ожидаемая производительность сжатия для каждой точки в оставшейся части пространства $\{R, K\}$ получена интерполяцией эмпирических результатов. Согласно фиг.12, наилучший срез волокна можно получить в окрестности $K_* \approx 900$ и $R_* \approx 0.1$L. Этот результат говорит о том, что для выбранной среды проектирования крестообразный сертификат подлинности является наилучшей опцией. Заметим, что тщательный выбор среза волокна привел к повышению на порядок величины стоимости горячей штамповки в отношении произвольно выбранной точки на $RK = \Phi$. Эмпирические принципы, используемые в этом примере, можно применить к поиску набора параметров, близких к оптимальным, для разных сред и производственных ограничений сертификата подлинности.

На фиг.13 показано иллюстративное вычислительное устройство 1300, которое можно полностью или частично реализовать в описанных системах. Вычислительное устройство 1300 является всего лишь одним примером вычислительной системы и не предполагает никакого ограничения объема использования или функциональных возможностей изобретения.

Вычислительное устройство 1300 можно реализовать посредством многих других сред или конфигураций вычислительной системы общего или специального назначения. Примеры общеизвестных вычислительных систем, сред и/или конфигураций, которые могут быть пригодны для использования, включают в себя, но не только, персональные компьютеры, компьютеры-серверы, тонкие клиенты, толстые клиенты, карманные или портативные устройства, многопроцессорные системы, системы на основе микропроцессора, телевизионные приставки, программируемую бытовую электронику, сетевые ПК, миникомпьютеры, универсальные компьютеры, игровые приставки, распределенные вычислительные среды, которые могут включать в себя любые из вышеописанных систем или устройств, и т.д.

Компоненты вычислительного устройства 1300 могут включать в себя, но не только, процессор 1302 (например, любой из микропроцессоров, контроллеров и т.п.), системную память 1304, устройства 1306 ввода, устройства 1308 вывода и сетевые устройства 1310.

Вычислительное устройство 1300 обычно включает в себя разнообразные компьютерно-считываемые носители. Такие носители могут представлять собой любые имеющиеся носители, к которым может осуществлять доступ вычислительное устройство 1300, и включают в себя энергозависимые и энергонезависимые носители, сменные и стационарные носители. Системная память 1304 включает в себя компьютерно-считываемый носитель в виде оперативной памяти (ОЗУ) и/или энергонезависимой памяти, например постоянной памяти (ПЗУ). Базовая система ввода/вывода (BIOS), содержащая основные процедуры, которые помогают переносить информацию между элементами вычислительного устройства 1300, например, при запуске, хранится в системной памяти 1304. Системная память 1304 обычно содержит данные и/или программные модули, непосредственно доступные процессору 1302 и/или в данный момент обрабатываемые им.

Системная память 1304 также включает в себя другие сменные/стационарные, энергозависимые/энергонезависимые компьютерные носители информации. Например, это может быть жесткий диск для считывания со стационарного, энергонезависимого носителя и записи на него; это может быть привод магнитных дисков для считывания со сменного, энергонезависимого носителя (например, “флоппи-диска”) и записи на него; и привод оптических дисков для считывания со стационарного, энергонезависимого носителя и/или записи на него, например CD-ROM, DVD или другой тип оптического носителя.

Приводы и соответствующие компьютерно-считываемые носители обеспечивают энергонезависимое хранение компьютерно-считываемых команд, структур данных, программных модулей и других данных для вычислительного устройства 1300. Очевидно, что для реализации иллюстративного вычислительного устройства 1300 также можно использовать другие типы компьютерно-считываемых носителей, на которых могут храниться данные, к которым вычислительное устройство 1300 может осуществлять доступ, например магнитные кассеты или другие магнитные запоминающие устройства, карты флэш-памяти, CD-ROM, цифровые универсальные диски (DVD) или другие оптические запоминающие устройства, блоки оперативной памяти (ОЗУ), блоки постоянной памяти (ПЗУ), электрически стираемые программируемые постоянные запоминающие устройства (ЭСППЗУ) и т.п. В системной памяти 1304 может храниться любое количество программных модулей, например операционная система 1320, прикладные программы 1328 и данные 1332.

Вычислительное устройство 1300 может включать в себя различные компьютерно-считываемые носители, которые называются средами передачи данных. Среды передачи данных обычно реализуют компьютерно-считываемые команды, структуры данных, программные модули или другие данные в сигнале, модулированном данными, например несущей волне или другом транспортном механизме, и включают в себя любые среды доставки информации. Термин “сигнал, модулированный данными” означает сигнал, одна или несколько характеристик которого изменяется таким образом, чтобы кодировать информацию в сигнале. В порядке примера или ограничения среды передачи данных включают в себя проводные среды, например проводную сеть или прямое проводное соединение, и беспроводные среды, например акустические, радио, инфракрасные и другие беспроводные среды. В состав компьютерно-считываемых носителей входят комбинации любых из вышеописанных.

Пользователь может вводить команды и информацию в вычислительное устройство 1300 через устройства 1306 ввода, например клавиатуру и указательное устройство (например, “мышь”). Другие устройства 1306 ввода могут включать в себя микрофон, джойстик, игровую панель, контроллер, спутниковую антенну, последовательный порт, сканер, сенсорный экран, сенсорные панели, кнопочные панели и/или т.п. Устройства 1308 вывода могут включать в себя монитор на основе ЭЛТ, экран ЖКД, громкоговорители, принтеры и т.п.

Вычислительное устройство 1300 может включать в себя сетевые устройства 1310 для подключения к компьютерным сетям, например локальной сети (ЛС), глобальной сети (ГС) и т.п.

Хотя изобретение было описано применительно к структурным особенностям и/или этапам способа, следует понимать, что изобретение, охарактеризованное в прилагаемой формуле изобретения, не ограничивается конкретными описанными признаками или этапами. Напротив, конкретные признаки и этапы раскрыты как предпочтительные формы реализации заявленного изобретения.

Формула изобретения

1. Способ кодирования произвольно распределенных признаков в объекте, содержащий этапы, на которых

определяют произвольно распределенные признаки в объекте,

определяют функцию плотности вероятности, связанную с объектом,

сжимают данные, представляющие произвольно распределенные признаки, при этом сжатие основано частично на функции плотности вероятности,

кодируют сжатые данные с помощью подписи, и

создают ярлык, содержащий объект и кодированные данные;

определяют векторы, связанные с произвольно распределенными признаками, основываясь, по меньшей мере, частично на функции плотности вероятности; и

кодируют векторы с использованием алгоритма арифметического кодирования, при этом алгоритм арифметического кодирования содержит:

Задать U как список всех единичных областей в $S\text{-}S_i\text{-}u$.

Список всех помеченных единиц, M(u), задан как $M(u)=\varnothing$

делать

Найти все единичные области $V=\operatorname{argmin}_{v \subset U} \|Q_v - Q_u\|$

делать

Найти единичную область $w=\operatorname{argmax}_{v \in V} \xi(l,v)$

Задать диапазон АК для w равным γ(w,u) (см. уравнения 17, 18)

Множество узлов перед w равно $M_w(u)=M(u)$

$M(u)=M(u)\cup w$, $V=V-w$, $U=U-w$.

пока $V\neq\varnothing$

пока $U\neq\varnothing$

при этом S означает зону сертификата подлинности объекта, S_i означает конкретную область сертификата подлинности объекта, ξ(l,v) означает вероятность того, что зона содержит освещенные концевые точки волокна, АК означает арифметический кодер, который преобразует входной поток произвольной длины в одно рациональное число в пределах [0,1}, u означает единичный квадрат, U означает единичные квадраты, Q означает главную точку единицы, v означает освещенную единицу относительно u, argmax означает правило приоритетов, установленное таким образом, что освещенная единица, которая имеет наибольшую вероятность освещения кодируется первой, M означает набор единиц, и γ(w,u) означает рабочий диапазон, используемый АК для кодирования w.

2. Способ по п.1, в котором при кодировании векторов с использованием алгоритма арифметического кодирования определяют путь для соединения части векторов в фиксированном объеме данных.

3. Способ по п.1, в котором произвольно распределенные признаки представляют собой волокна, произвольно размещенные в объекте.

4. Способ по п.3, в котором функция плотности вероятности представляет вероятность того, что волокна в конкретной области освещены источником света.

5. Способ по п.3, в котором функцию плотности вероятности выводят на основании, по меньшей мере, частично длины волокон.

6. Способ по п.3, в котором каждый вектор представляет концевые точки двух волокон.

7. Способ по п.1, в котором данные кодируют с помощью личного ключа.

8. Способ по п.1, в котором ярлык представляет собой сертификат подлинности, способный к самоаутентификации, и объект представляет собой объект аутентификации, входящий в состав сертификата подлинности.

9. Способ по п.1, в котором кодированные данные включают в ярлык в качестве штрих-кода.

10. Способ по п.1, дополнительно содержащий этапы, на которых

определяют текстовые данные, содержащие строку символов,

хэшируют текстовые данные посредством алгоритма,

шифруют сжатые данные с использованием хэшированных текстовых данных и включают текстовые данные в ярлык.

11. Способ по п.10, в котором алгоритм представляет собой криптографически защищенный алгоритм хэширования.

12. Способ по п.10, в котором алгоритм представляет собой криптографический алгоритм SHA1.

13. Одно или несколько компьютерно-считываемых запоминающих устройств для хранения команд, выполняемых процессором для осуществления способа по п.1.

14. Система для кодирования произвольно распределенных признаков в объекте, содержащая

блок издания, сконфигурированный с возможностью определять произвольно распределенные признаки в объекте аутентификации и сжимать данные, представляющие произвольно распределенные признаки, содержащие волокна, при

этом блок издания также сконфигурирован с возможностью кодирования сжатых данных с помощью подписи и создания ярлыка, содержащего объект аутентификации и кодированные данные,

при этом блок издания также сконфигурирован с возможностью определения функции плотности вероятности, связанной с объектом аутентификации, причем функция плотности вероятности определена как вероятность нахождения второго конца волокна в данном местоположении с неосвещенной областью, когда первый конец волокна расположен в освещенной области объекта аутентификации, определения векторов, связанных с произвольно распределенными признаками, основываясь, по меньшей мере, частично на функции плотности вероятности, и кодирования части векторов в виде пути с применением алгоритма арифметического кодирования, содержащего

Задать U как список всех единичных областей в $S\text{-}S_i\text{-}u$.

Список всех помеченных единиц, M(u), задан как $M(u)=\varnothing$

делать

Найти все единичные области $V=\operatorname{argmin}_{v \subset U} \|Q_v - Q_u\|$

делать

Найти единичную область $w=\operatorname{argmax}_{v \in V} \xi(l,v)$

Задать диапазон АК для w равным $\gamma(w,u)$ (см. уравнения 17, 18)

Множество узлов перед w равно $M_w(u)=M(u)$

$M(u)=M(u) \cup w$, $V=V-w$, $U=U-w$.

пока $V \neq \varnothing$

пока $U \neq \varnothing$,

при этом S означает зону сертификата подлинности объекта, S_i означает конкретную зону сертификата подлинности объекта, $\xi(l,v)$ означает вероятность того, что зона содержит освещенные концевые точки волокон, АК означает арифметический кодер, который преобразует входной поток произвольной длины в единичное рациональное число в [0,1}, u означает единичный квадрат, U означает единичные квадраты, Q означает главную точку единицы, v означает освещенную единицу относительно u, argmax означает правило приоритетов, установленное таким образом, что освещенная единица, которая имеет наибольшую вероятность освещения, кодируется первой, M означает набор единиц и $\gamma(w,u)$ означает рабочий диапазон, используемый АК для кодирования w.

15. Система по п.14, в которой блок издания также обеспечивает кодирование сжатых данных с помощью личного ключа.

16. Система по п.14, в которой блок издания также обеспечивает включение в ярлык штрих-кода с кодированными данными.

17. Система по п.14, в которой блок издания также обеспечивает определение текстовых данных, содержащих строку символов, и хэширование текстовых данных с помощью алгоритма.

18. Система по п.17, в которой блок издания также обеспечивает шифрование сжатых данных с использованием хэшированных текстовых данных и включение текстовых данных в ярлык.

19. Система по п.14, дополнительно содержащая блок проверки, способный декодировать данные, представляющие произвольно распределенные признаки в ярлыке, и аутентифицировать ярлык путем сравнения декодированных данных с данными действительных произвольно распределенных признаков, определенных из

объекта аутентификации.

20. Аутентификационный ярлык, содержащий

объект аутентификации, содержащий произвольно распределенные признаки, и

кодированную информацию, связанную с объектом аутентификации, причем информация закодирована с помощью подписи и содержит сжатые данные, представляющие произвольно распределенные признаки в объекте аутентификации, при этом данные в кодированной информации сжаты путем

определения функции плотности вероятности, связанной с объектом аутентификации,

определения векторов, связанных с произвольно распределенными атрибутами, на основании, по меньшей мере, частично функции плотности вероятности, и

кодирования векторов с использованием алгоритма арифметического кодирования,

при этом ярлык допускает самоаутентификацию путем сравнения сжатых данных в кодированной информации и данных, представляющих произвольно распределенные признаки, полученных путем анализа объекта аутентификации, при этом

сжатые данные получают путем:

определения векторов, связанных с произвольно распределенными признаками, основываясь, по меньшей мере, частично на функции плотности вероятности; и

кодирования векторов с применением алгоритма арифметического кодирования, содержащего

Задать U как список всех единичных областей в S-S_i-u.

Список всех помеченных единиц, M(u), задан как $M(u)=\varnothing$

делать

Найти все единичные области $V=\operatorname{argmin}_{v \subset U} \|Q_v - Q_u\|$

делать

Найти единичную область $w=\operatorname{argmax}_{v \in V} \xi(l,v)$

Задать диапазон АК для w равным $\gamma(w,u)$ (см. уравнения 17, 18)

Множество узлов перед w равно $M_w(u)=M(u)$

$M(u)=M(u) \cup w$, $V=V-w$, $U=U-w$.

пока $V \neq \varnothing$

пока $U \neq \varnothing$,

при этом S означает зону сертификата подлинности объекта, S_i означает конкретную зону сертификата подлинности объекта, $\xi(l,v)$ означает вероятность того, что зона содержит освещенные концевые точки волокон, АК означает арифметический кодер, который преобразует входной поток произвольной длины в единичное рациональное число в [0,1}, u означает единичный квадрат, U означает единичные квадраты, Q означает главную точку единицы, v означает освещенную единицу относительно u, argmax означает правило приоритетов, установленное таким образом, что освещенная единица, которая имеет наибольшую вероятность освещения, кодируется первой, M означает набор единиц и $\gamma(w, u)$ означает рабочий диапазон, используемый АК кодирования w.

21. Ярлык по п.20, в котором кодированная информация включена в ярлык в качестве штрих-кода.

22. Ярлык по п.20, в котором кодированная информация закодирована с помощью личного ключа.

23. Ярлык по п.20, который также содержит текстовые данные, содержащие строку символов, причем сжатые данные зашифрованы с использованием текстовых данных.

24. Ярлык по п.23, в котором сжатые данные зашифрованы путем хэширования текстовых данных посредством алгоритма и шифрования сжатых данных с использованием хэшированных текстовых данных.

25. Устройство для создания ярлыка, содержащее

средство определения произвольно распределенных признаков в объекте аутентификации;

средство определения функции плотности вероятности, связанной с объектом аутентификации, при этом функция плотности вероятности определяет вероятность точки, содержащей освещенный второй конец волокна и обусловленной местоположением первого конца волокна в освещенной области;

средство сжатия данных, представляющих произвольно распределенные признаки, при этом сжатие основано частично на функции плотности вероятности;

средство кодирования сжатых данных с помощью подписи;

средство создания ярлыка, содержащего объект аутентификации и кодированные данные;

средство определения векторов, связанных с произвольно распределенными признаками, основываясь, по меньшей мере, частично на функции плотности вероятности; и

средство кодирования векторов с применением алгоритма арифметического кодирования, содержащего:

Задать U как список всех единичных областей в $S\text{-}S_i\text{-}u$.

Список всех помеченных единиц, M(u), задан как $M(u)=\varnothing$

делать

Найти все единичные области $V=\operatorname{argmin}_{v \subset U} \|Q_v - Q_u\|$

делать

Найти единичную область $w=\operatorname{argmax}_{v \in V} \xi(l,v)$

Задать диапазон АК для w равным $\gamma(w,u)$ (см. уравнения 17, 18

Множество узлов перед w равно $M_w(u)=M(u)$

$M(u)=M(u) \cup w$, $V=V-w$, $U=U-w$.

пока $V \neq \varnothing$

пока $U \neq \varnothing$,

при этом S означает зону сертификата подлинности объекта, S_i означает конкретную зону сертификата подлинности объекта, $\xi(l,v)$ означает вероятность того, что зона содержит освещенные концевые точки волокон, АК означает арифметический кодер, который преобразует входной поток произвольной длины в единичное рациональное число в [0,1}, u означает единичный квадрат, U означает единичные квадраты, Q означает главную точку единицы, v означает освещенную единицу относительно u, argmax означает правило приоритетов, установленное таким образом, что освещенная единица, которая имеет наибольшую вероятность освещения, кодируется первой, M означает набор единиц и $\gamma(w, u)$ означает рабочий диапазон, используемый АК для кодирования w.

26. Устройство по п.25, дополнительно содержащее средство включения волокон в объект аутентификации в качестве произвольно распределенных признаков.

27. Устройство по п.25, дополнительно содержащее средство определения векторов, связанных с произвольно распределенными признаками, на основании, по меньшей мере, частично функции плотности вероятности и

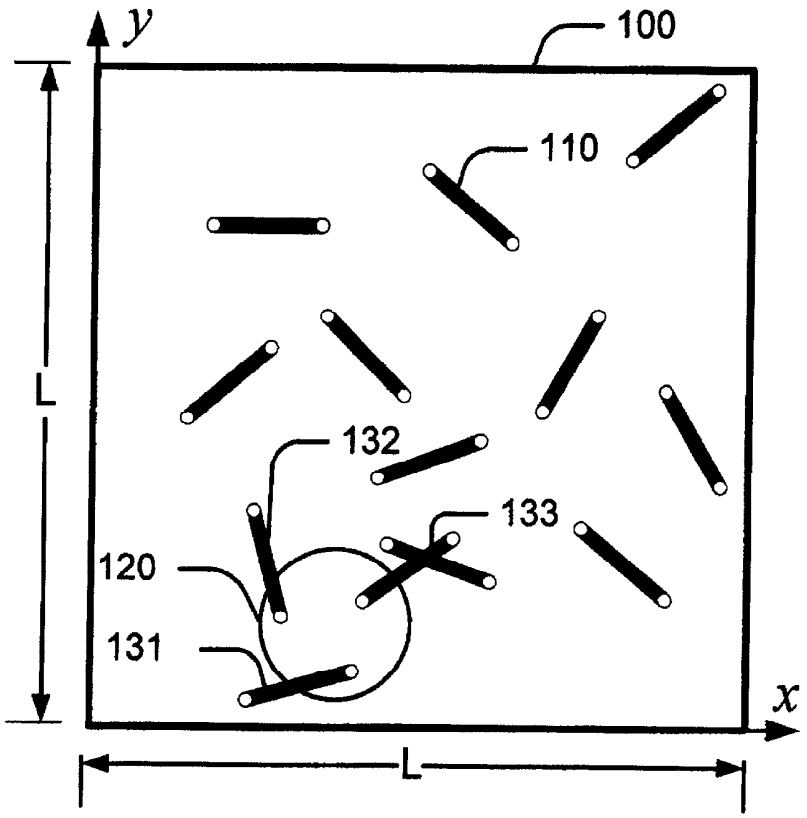
средство кодирования векторов с использованием алгоритма арифметического

кодирования.

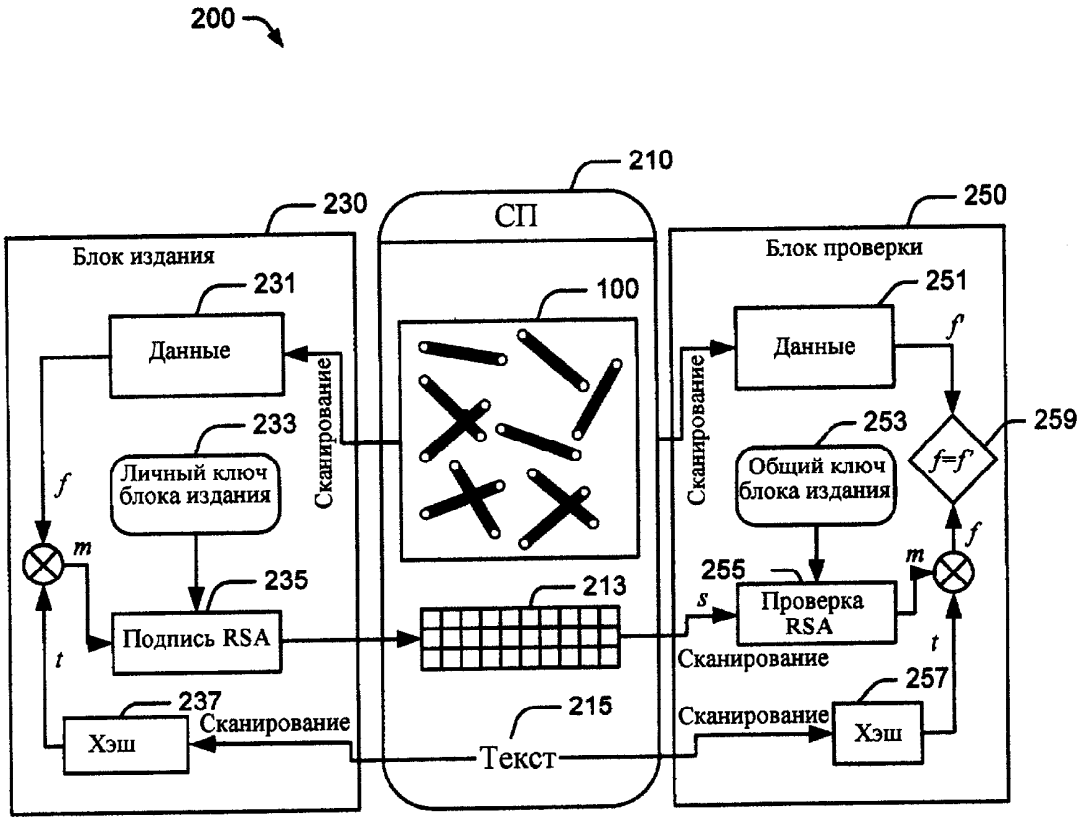
28. Устройство по п.25, дополнительно содержащее средство определения текстовых данных, содержащих строку символов, средство хэширования текстовых данных посредством алгоритма, средство шифрования сжатых данных с использованием хэшированных текстовых данных и

средство включения текстовых данных в ярлык.

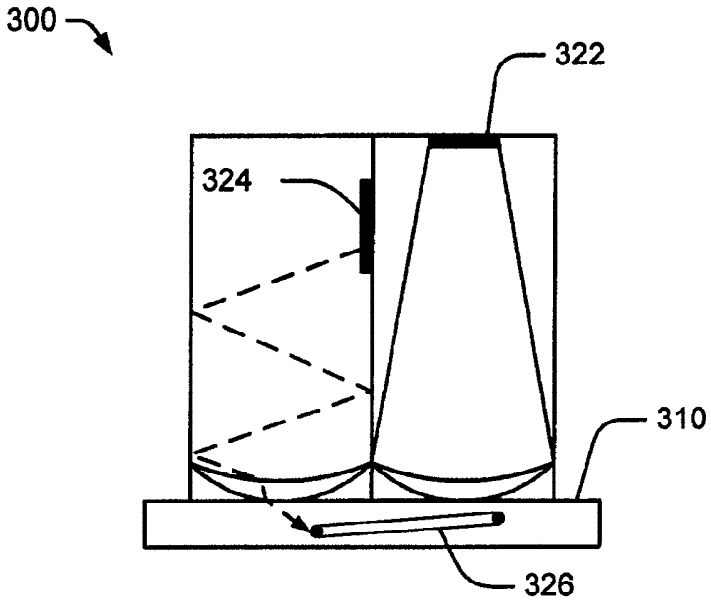
29. Устройство по п.25, дополнительно содержащее средство аутентификации ярлыка путем сравнения кодированных данных с данными, связанными с произвольно распределенными признаками в объекте аутентификации.


y
100
110
L
132
133
120
131
x
L

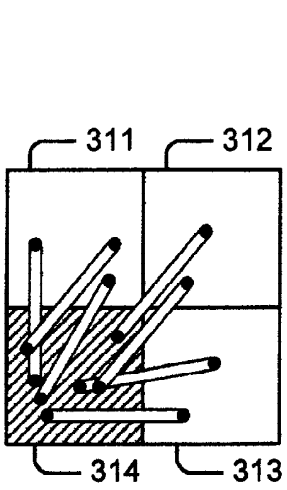
Фиг. 1


200
210
СП
230
Блок издания
231
Данные
233
Личный ключ блока издания
f
m
235
Подпись RSA
t
237
Хэш
Сканирование
100
213
215
Текст
Сканирование
250
Блок проверки
251
Данные
f
253
Общий ключ блока издания
259
f=f'
Сканирование
255
s
Проверка RSA
Сканирование
m
f
t
257
Сканирование
Хэш

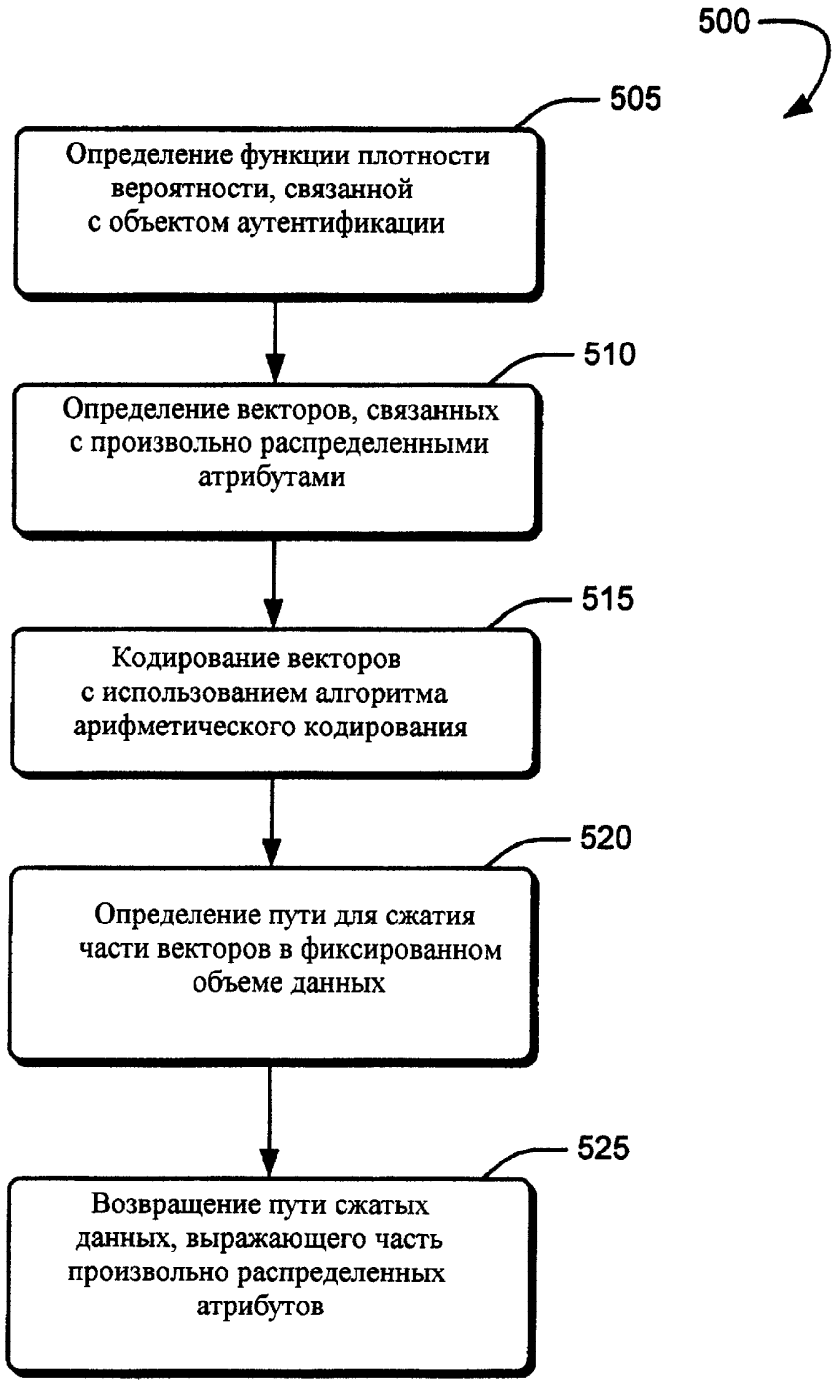
Фиг. 2



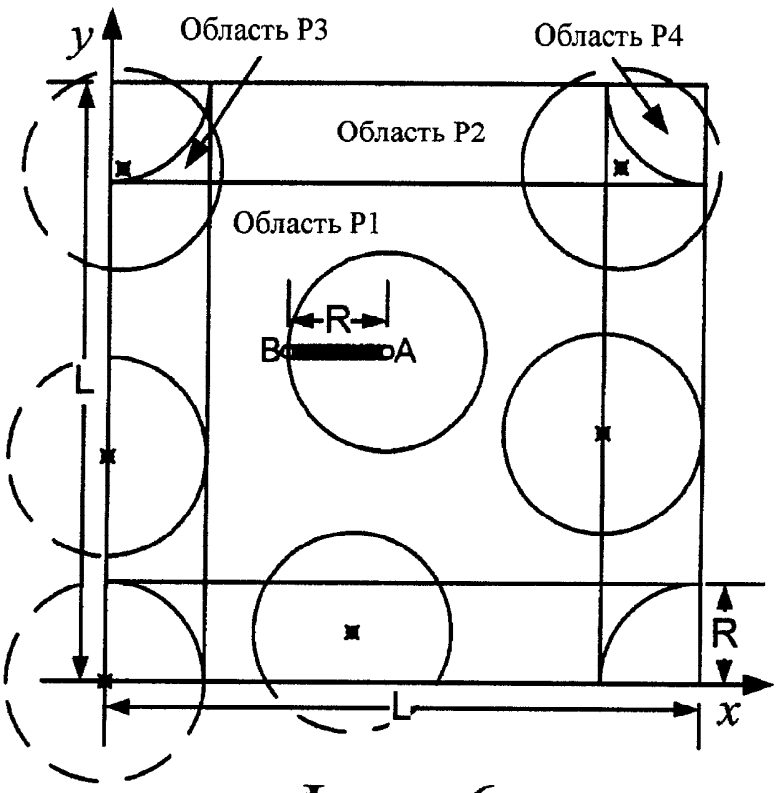
Фиг. 3A



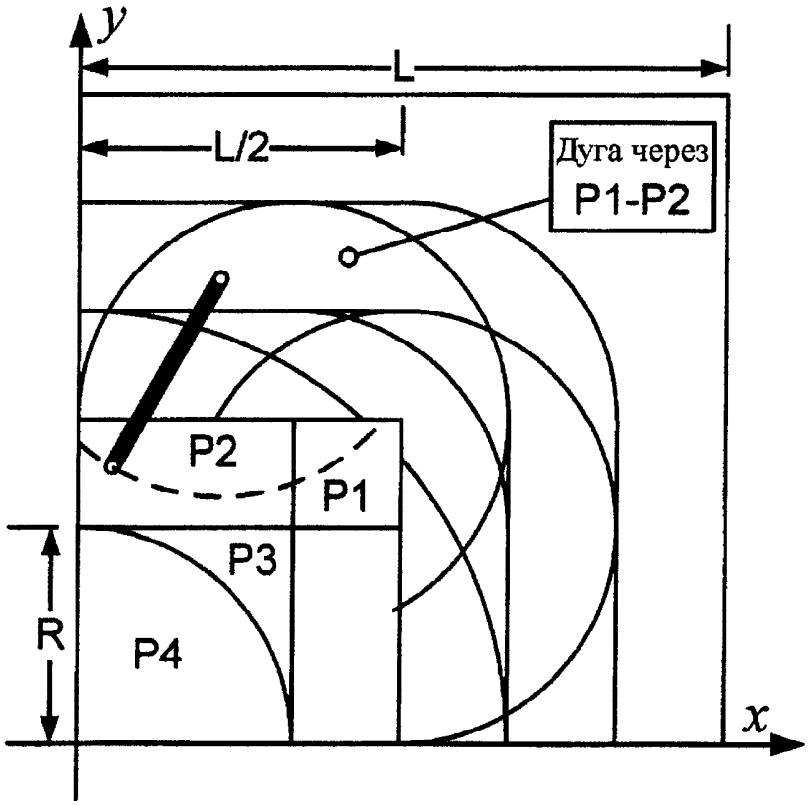
Фиг. 3B


500
505
Определение функции плотности вероятности, связанной с объектом аутентификации
510
Определение векторов, связанных с произвольно распределенными атрибутами
515
Кодирование векторов с использованием алгоритма арифметического кодирования
520
Определение пути для сжатия части векторов в фиксированном объеме данных
525
Возвращение пути сжатых данных, выражающего часть произвольно распределенных атрибутов

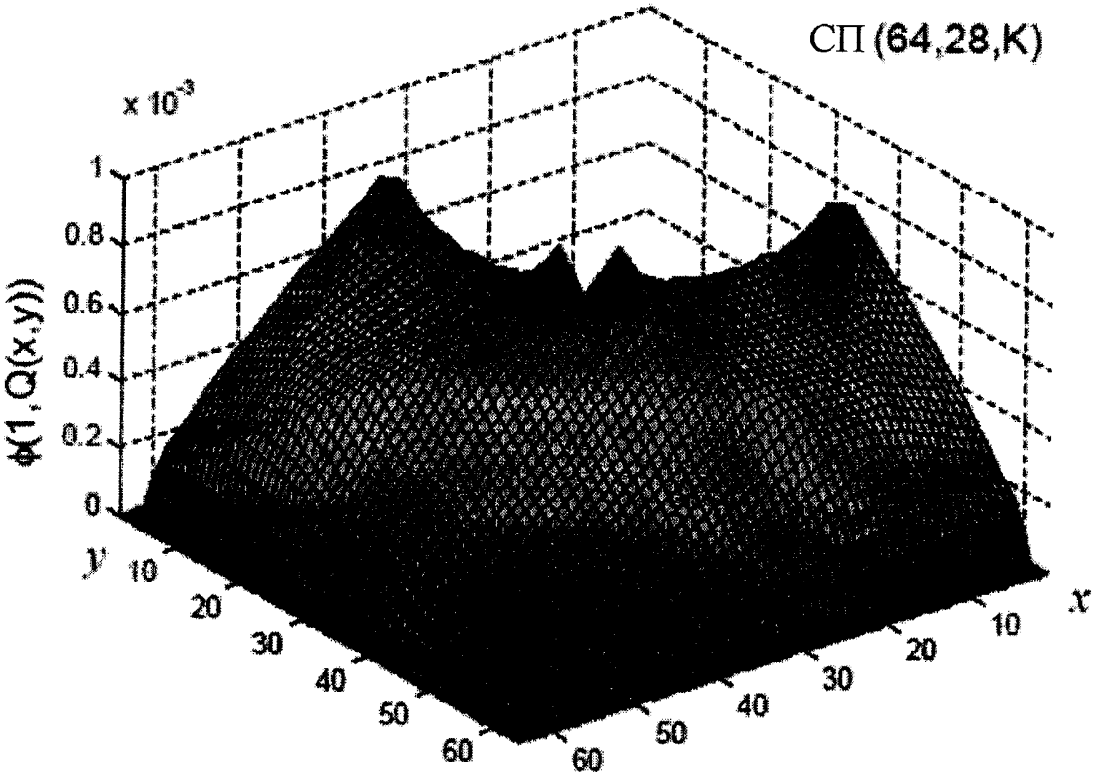
Фиг. 5



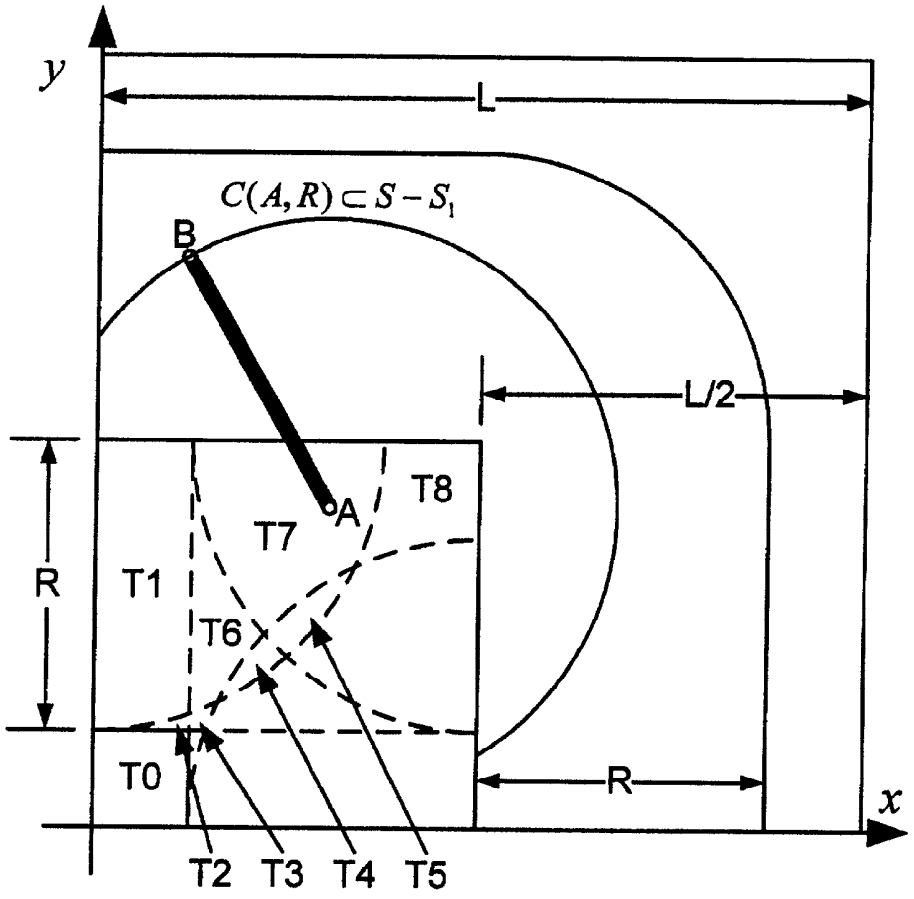
Фиг. 6


y
L
L/2
Дуга через
P1-P2
P2
P1
P3
R
P4
x

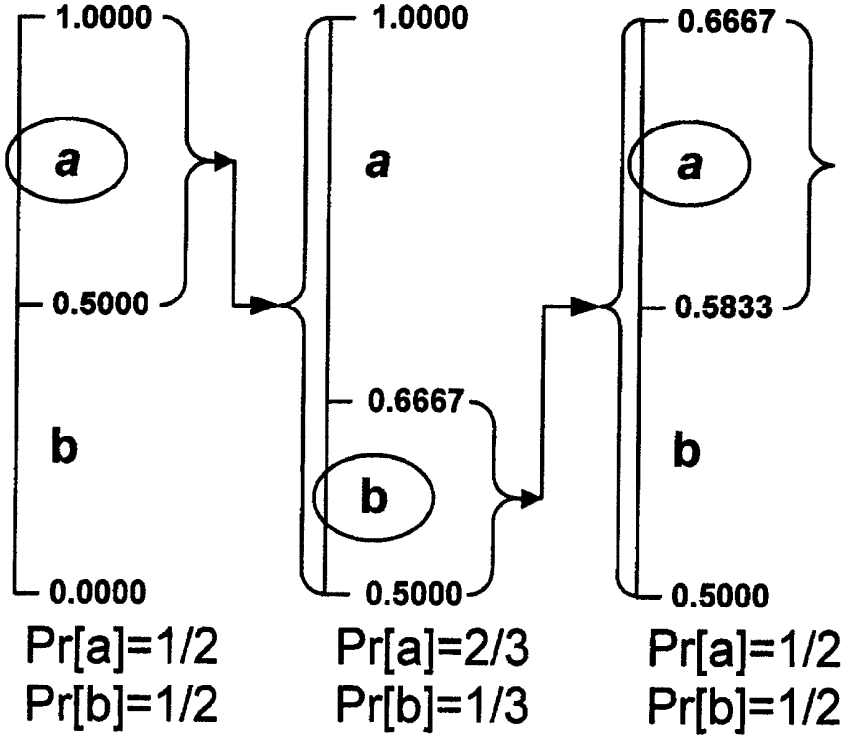
Фиг. 7


СП (64,28,K)
x 10^-3
1
0.8
0.6
0.4
0.2
0
Φ(1,Q(x,y))
y
10
20
30
40
50
60
x
10
20
30
40
50
60

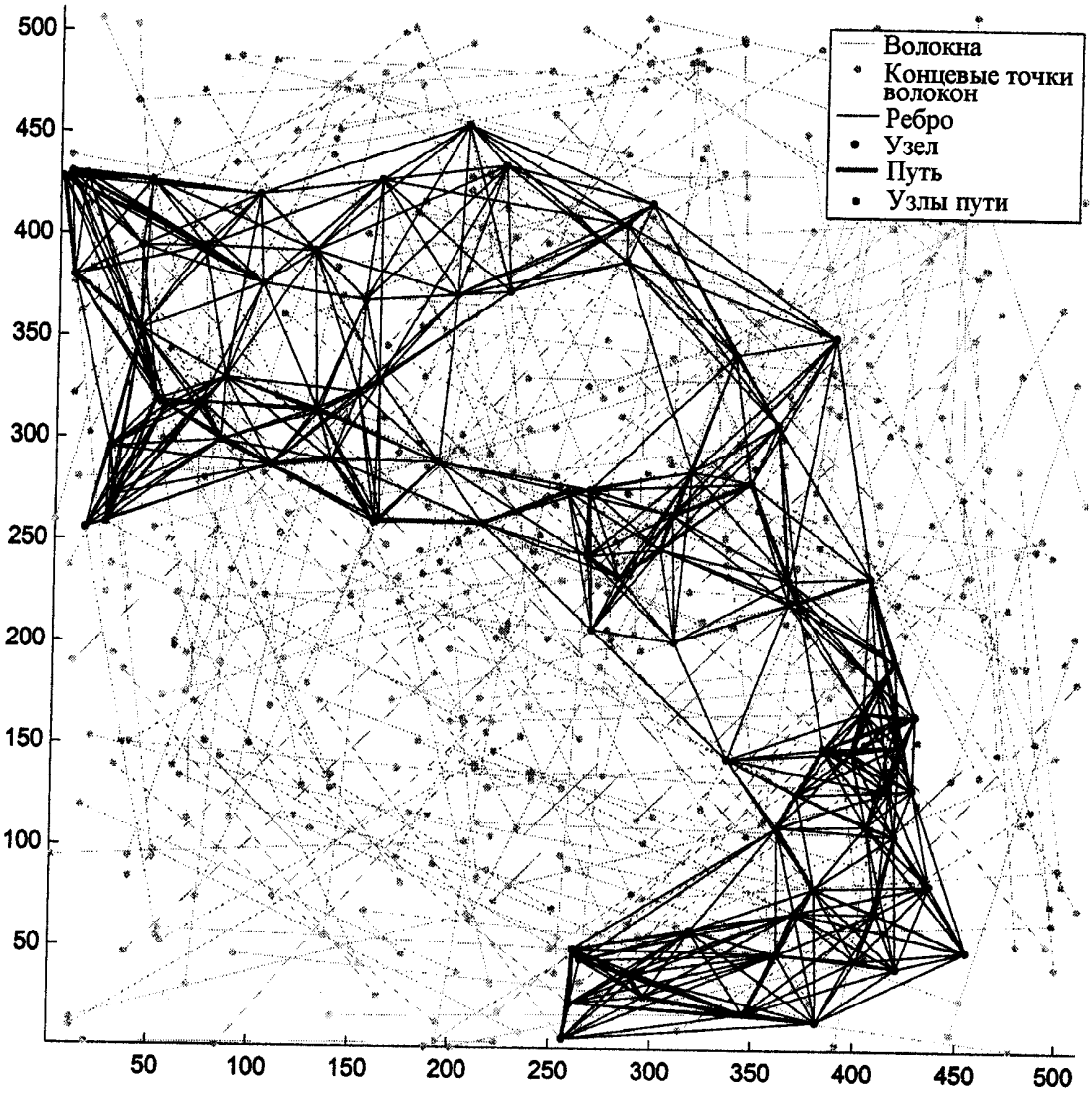
Фиг. 8


y
L
C(A,R) ⊂ S − S1
B
A
L/2
R
T1
T2
T3
T4
T5
T6
T7
T8
T0
R
x

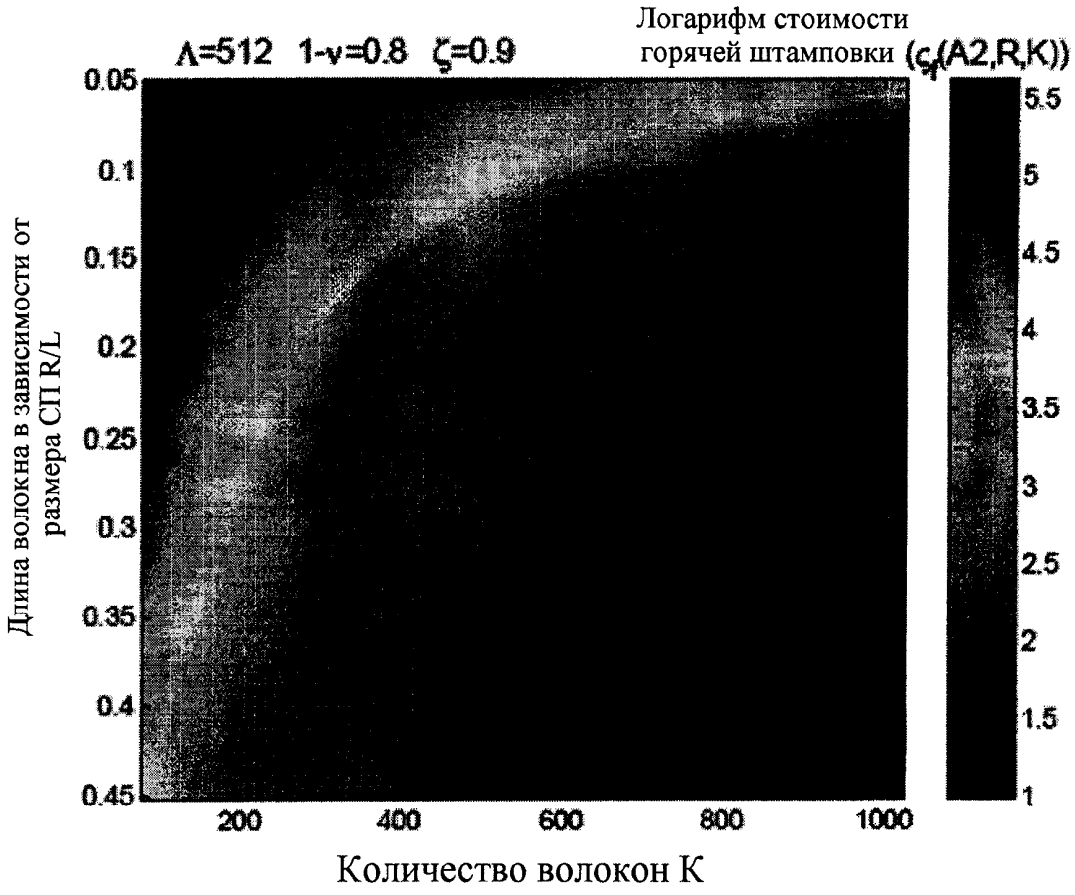
Фиг. 9


1.0000
a
0.5000
b
0.0000
Pr[a]=1/2
Pr[b]=1/2
1.0000
a
0.6667
b
0.5000
Pr[a]=2/3
Pr[b]=1/3
0.6667
a
0.5833
b
0.5000
Pr[a]=1/2
Pr[b]=1/2

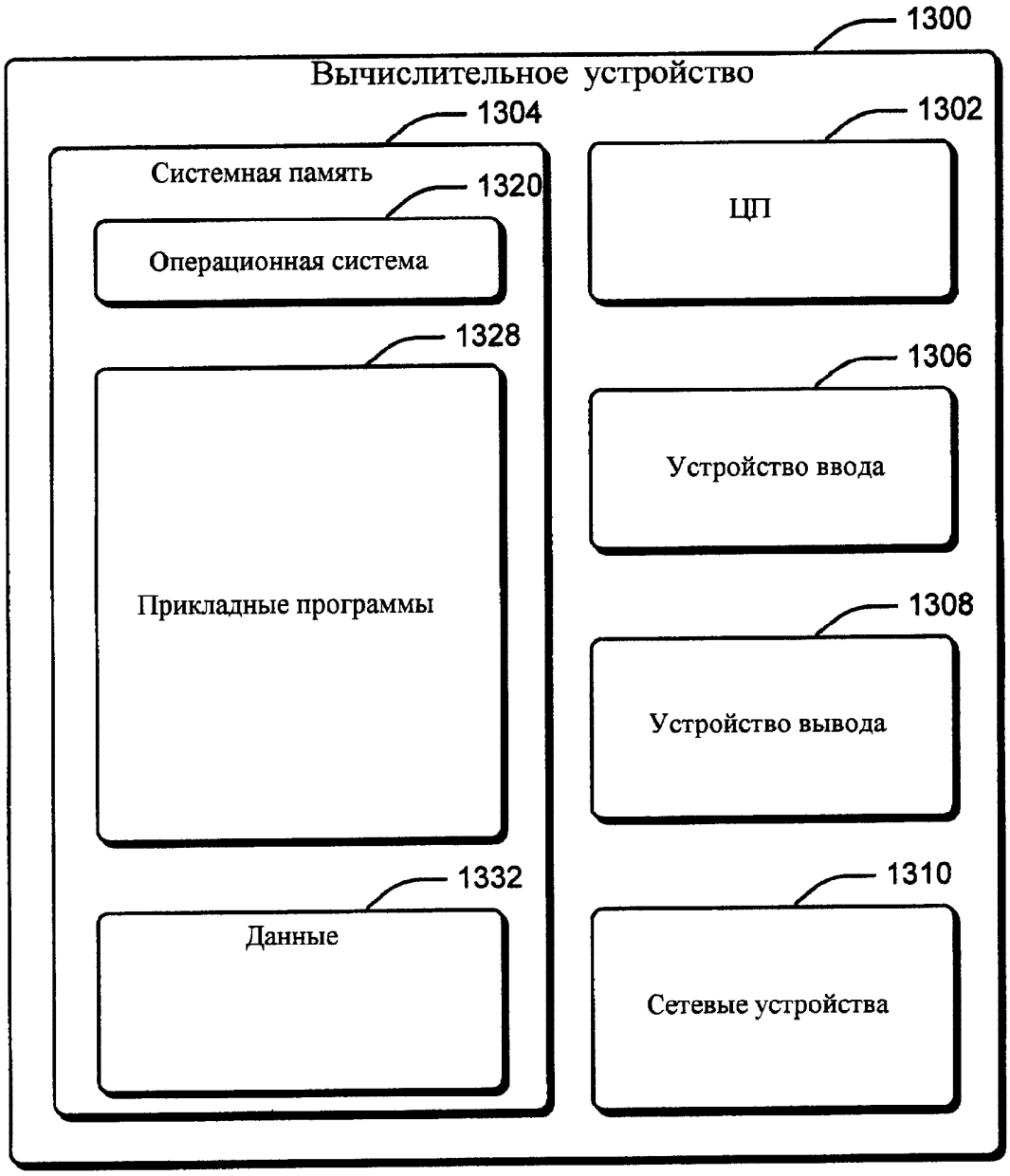
Фиг. 10


Волокна
Концевые точки волокон
Ребро
Узел
Путь
Узлы пути
500
450
400
350
300
250
200
150
100
50
50
100
150
200
250
300
350
400
450
500

Фиг. 11


Λ=512 1-ν=0.8 ζ=0.9
Логарифм стоимости горячей штамповки (ζ1(A2,R,K))
Длина волокна в зависимости от размера СП R/L
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4
0.45
200
400
600
800
1000
5.5
5
4.5
4
3.5
3
2.5
2
1.5
1
Количество волокон K

Фиг. 12


1300
Вычислительное устройство
1304
Системная память
1320
Операционная система
1328
Прикладные программы
1332
Данные
1302
ЦП
1306
Устройство ввода
1308
Устройство вывода
1310
Сетевые устройства

Фиг. 13