



(12) 发明专利

(10) 授权公告号 CN 1670761 B

(45) 授权公告日 2012.03.14

(21) 申请号 200510009491.7

US 5974150 A, 1999.10.26, 摘要, 说明书第

(22) 申请日 2005.02.16

11栏第15—33行, 第12栏第50—62行, 第13栏第39—60行, 第16栏第25—45行.

(30) 优先权数据

10/802,981 2004.03.17 US

WO 91/19614 A1, 1991.12.26, 全文.

(73) 专利权人 微软公司

审查员 张广平

地址 美国华盛顿州

(72) 发明人 D·基洛弗斯基

(74) 专利代理机构 上海专利商标事务所有限公司 31100

代理人 张政权

(51) Int. Cl.

G06K 17/00 (2006.01)

G09C 1/00 (2006.01)

H03M 7/30 (2006.01)

(56) 对比文件

DE 10204870 A1, 2003.08.14, 全文.

WO 99/17486 A1, 1999.04.08, 全文.

EP 0889448 A2, 1999.01.07, 全文.

WO 01/43086 A1, 2001.06.14, 全文.

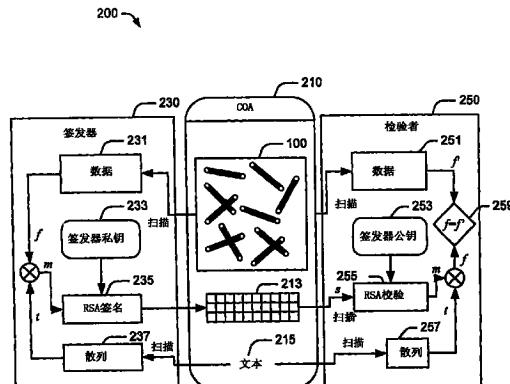
权利要求书 3 页 说明书 18 页 附图 11 页

(54) 发明名称

用来编码对象中随机分布特征的系统和方法

(57) 摘要

所述系统和方法涉及编码对象中的随机分布特征。确定验证对象中的随机分布特征。表示随机分布特征的数据被压缩，并用签名进行编码。标签被创建，并包括验证对象和经编码数据。该数据可通过确定关联于该验证对象的概率密度函数来压缩。与随机分布属性相关联的向量是至少部分地基于概率密度函数被确定的。使用算术编码算法编码该向量。



1. 一种用于创建标签的方法,其特征在于,包括:

扫描验证证书中的验证对象;

确定所述验证对象中的表示随机分布特征的数据;

通过:

确定关联于所述对象的概率密度函数,

确定表示随机分布属性的向量,

使用算术编码算法来编码向量,

确定用于在固定量数据中压缩部分向量的路径,以及

返回表示部分随机分布属性的经压缩数据的路径,

来压缩表示所述随机分布特征的数据,其中所述随机分布特征是随机位于所述对象内的纤维,所述概率密度函数表示在特定区域内的纤维被光源照亮的概率;

用签名编码经压缩的数据;以及

创建包括所述对象和经编码的数据的标签,

其中所述纤维是能够在端点之间传送光线的光学纤维。

2. 如权利要求1所述的方法,其特征在于,所述概率密度函数至少部分地基于所述纤维的长度来推导。

3. 如权利要求1所述的方法,其特征在于,经压缩的数据用私钥进行编码。

4. 如权利要求1所述的方法,其特征在于,所述标签是被配置为自校验的验证证书,并且所述对象是包括在验证证书中的验证对象。

5. 如权利要求1所述的方法,其特征在于,被编码的经压缩数据作为条形码被包括在标签中。

6. 如权利要求1所述的方法,其特征在于,还包括:

确定包括字符串的文本数据,其中所述文本数据包括在所述标签中;

用密码学安全散列算法散列所述文本数据;以及

使用所述经散列的文本数据对所述经压缩的数据加密。

7. 如权利要求6所述的方法,其特征在于,所述密码学安全散列算法是SHA1密码学算法。

8. 一种用于创建标签的系统,其特征在于,包括

一签发器,被配置成用以确定验证对象中的随机分布特征并通过:

确定关联于所述验证对象的概率密度函数,

确定表示随机分布属性的向量,

使用算术编码算法来编码向量,

确定用于在固定量数据中压缩部分向量的路径,以及

返回表示部分随机分布属性的经压缩数据的路径,

来压缩表示所述随机分布特征的数据,其中所述随机分布特征是随机位于所述验证对象内的纤维,所述概率密度函数表示在特定区域内的纤维被光源照亮的概率,所述签发器还被配置成以签名编码经压缩的数据,并创建包括所述验证对象和经编码的数据的标签,

其中所述纤维是能够在端点之间传送光线的光学纤维。

9. 如权利要求8所述的系统,其特征在于,所述签发器还被配置成用私钥编码经压缩

的数据。

10. 如权利要求 8 所述的系统,其特征在于,所述签发器还被配置成把带有被编码的经压缩数据的条形码包括在所述标签中。

11. 如权利要求 8 所述的系统,其特征在于,所述签发器还被配置成确定包括字符串的文本数据,并用算法散列所述文本数据,其中所述文本数据包括在所述标签中。

12. 如权利要求 11 所述的系统,其特征在于,所述签发器还被配置成使用所述经散列的文本数据对所述经压缩的数据加密。

13. 如权利要求 8 所述的系统,其特征在于,还包括:

一校验器,被配置成解码所述标签中表示所述随机分布特征的数据,并通过比较经解码数据与从所述验证对象确定的有效随机分布特征的数据,来验证所述标签。

14. 一种标签,其特征在于,包括:

一验证对象,其包括随机分布特征;以及

关联于所述验证对象的经编码的信息,所述信息用签名进行编码并包括表示所述验证对象中随机分布特征的经压缩数据,

其中所述标签是通过对所述经编码的信息中的经压缩数据与经分析所述验证对象获取的表示随机分布特征的数据进行比较而自校验的;

其中通过:

确定关联于所述验证对象的概率密度函数,

确定表示随机分布属性的向量,

使用算术编码算法来编码向量,

确定用于在固定量数据中压缩部分向量的路径,以及

返回表示部分随机分布属性的经压缩数据的路径,

来压缩表示所述随机分布特征的数据,表示所述随机分布特征的数据被压缩并用签名编码,其中所述随机分布特征是随机位于所述验证对象内的纤维,所述概率密度函数表示在特定区域内的纤维被光源照亮的概率,

其中所述纤维是能够在端点之间传送光线的光学纤维。

15. 如权利要求 14 所述的标签,其特征在于,经编码的信息作为条形码被包括在所述标签中。

16. 如权利要求 14 所述的标签,其特征在于,经编码的信息用私钥进行编码。

17. 如权利要求 14 所述的标签,其特征在于,还包括:

包括字符串的文本数据,其中使用所述文本数据对所述经压缩数据加密。

18. 如权利要求 17 所述的标签,其特征在于,经压缩数据被如下加密:

用密码学安全散列算法散列所述文本数据;以及

使用经散列的文本数据对所述经压缩数据加密。

19. 一种用于创建标签的装置,其特征在于,包括:

用以确定验证对象中的随机分布特征的装置;

用以通过:

确定关联于所述对象的概率密度函数,

确定表示随机分布属性的向量,

使用算术编码算法来编码向量，
确定用于在固定量数据中压缩部分向量的路径，以及
返回表示部分随机分布属性的经压缩数据的路径，
来压缩表示所述随机分布特征的数据的装置，其中所述随机分布特征是随机位于所述对象内的纤维，所述概率密度函数表示在特定区域内的纤维被光源照亮的概率；

用来以签名编码所述数据的装置；以及
用以创建包括所述验证对象和经编码的数据的标签的装置，
其中所述纤维是能够在端点之间传送光线的光学纤维。

20. 如权利要求 19 所示的装置，其特征在于，还包括把纤维加入所述验证对象作为随机分布特征的装置。

21. 如权利要求 19 所示的装置，其特征在于，还包括：

一装置，用以确定包括字符串的文本数据，其中所述文本数据被包括在所述标签中；
一装置，用以用密码学安全散列算法散列所述文本数据；以及
一装置，用以使用所述经散列的文本数据对经压缩的数据加密。

22. 如权利要求 19 所示的装置，其特征在于，还包括：

一装置，用以通过对经编码数据与所述验证对象中关联于所述随机分布特征的数据进行比较来验证所述标签。

用来编码对象中随机分布特征的系统和方法

技术领域

[0001] 本文所述的系统和方法一般涉及防伪和 / 或防篡改标签，尤其涉及利用对象的随机分布特征（无论嵌入的或自然固有的）来限制对伪造和 / 或篡改标签的未经授权尝试。

背景技术

[0002] 标签的伪造和篡改使产品销售商和产品制造商在损失收入和损失客户方面每年花费数十亿美元。随着计算机技术的迅速成长，产生象真品的标签已变得越来越容易。例如，可利用扫描仪来扫描真标签的高分辨率图像，然后以最少成本重复再生产。还有，礼券也可以被扫描、更改（例如改为有更大面值）、重复印制、并兑换。

[0003] 近年来已利用各种技术来制止伪造和篡改的泛滥成灾。一种保护标签的方法是通过加入条形码。条形码通常是印在标签上的机器可读码。使用条形码扫描仪，可快速读取并验证带有条形码的标签。当前条形码标签的一个问题是在各个产品上要使用相同的标签。

[0004] 当前的另一方案是使经扫描条形码对照存储在数据库中的安全数据（例如电子收款机系统 POS 系统）进行检查。然而，这个方案需要加入来自销售商或制造商的最近数据。这种方案需要多方的及时并紧密合作。还有，这种方案限制了其实现的灵活性，且并非总是可行的。

[0005] 然而，这些技术有一个通病；即，对于给定产品所扫描的标签物理上是相同的。因此，尽管产生合理标签的制造过程是高度复杂的，但对于伪造者而言要确定产生伪造合格品的方法通常却并不需要很长时间。而且，一旦标签被成功复制了一次，它就可以重复再生产了（例如建立低成本可复制的主副本）。即使在使用若干次后秘密地将标签列于数据库中，也不能保证先扫描的标签确实是真标签。

[0006] 因此，当前方案不能提供较难复制且可较便宜生产的标签。

发明内容

[0007] 本文所述的系统和方法涉及编码对象中的随机分布特征。在一方面中，确定验证对象中的随机分布特征。代表随机分布特征的数据被压缩并用签名编码。标签产生，并且它包括验证对象和经编码数据。

[0008] 在另一方面中，通过确定关联于验证对象的概率密度函数来压缩数据。关联于随机分布属性的向量至少部分地基于概率密度函数来确定。使用算术编码算法来对向量进行编码。

附图说明

[0009] 图 1 显示用作标签一部分的示例验证对象，诸如验证证书。

[0010] 图 2 是示出验证系统的示例证书，以及由该系统采用的用以签发并校验验证证书的示例过程的示意图。

[0011] 图 3A 是示例扫描系统的示意图，该系统用以捕捉关联于验证证书的验证对象的

随机分布特征。

- [0012] 图 3B 是图 3A 中所示验证对象的顶视图。
- [0013] 图 4 是可用以创建验证证书的示例过程流程图。
- [0014] 图 5 是可用以压缩代表验证对象随机分布属性的数据的示例过程流程图。
- [0015] 图 6 是对应于示例验证对象四个不同区域的区域图形表示。
- [0016] 图 7 是示例验证对象上十九个不同区域的图形表示。
- [0017] 图 8 是正方形验证对象的概率密度函数的示例图形。
- [0018] 图 9 是验证对象中区域的图形表示。
- [0019] 图 10 是算术编码器如何编码字符串“aba”的示例的图形表示。
- [0020] 图 11 是用节点显示的验证对象实例的示例。
- [0021] 图 12 是为优化成本效率而设计的验证证书的图形表示。
- [0022] 图 13 示出了所述系统和方法可全部或部分实现的示例计算设备。

具体实施方式

[0023] I. 导言

[0024] 在此所述的系统和方法涉及有关在标签中使用的对象随机方法特征的编码信息。标签可包括任何类型的附于或包括在产品上的识别手段。被配置用以验证的标签在此称为验证证书。在验证证书中使用的带有随机分布特征的对象在此称为验证对象。为了使能自校验，验证证书可包括验证对象和关于随机分布特征的信息。可使用压缩方法来增加可编码并包括在验证证书中的关于随机分布特征的信息量。根据一示例计算，伪造验证证书的成本与压缩该信息上的改进成指数比例增加。这种伪造成本上的实质性增加导致了一种制造相对便宜但却难以伪造的可靠验证证书。

[0025] 图 1 显示了用作部分标签的示例验证对象 100，诸如验证证书。为了有效地在验证证书中使用，验证对象 100 通常包含唯一而且难以复制的随机分布特征。图 1 中所示的示例验证对象 100 是基于纤维验证证书的一部分，并包含以随机方式嵌入对象中的纤维 110。纤维 110 作为验证对象 100 的随机分布特征。纤维 110 可以任何方法加入验证对象 100。例如，可把纤维 110 喷在验证对象 100 上。也可在制造过程中把纤维 110 嵌到验证对象 100 中。在一实施例中，纤维 110 是能够在端点之间传送光线的光学纤维。因而，通过在验证对象 100 的某区域 120 上照光，至少有一端在点亮区域内的纤维 131-133 的端点被照亮。

[0026] 图 1 中，验证对象 100 包括 κ 个随机分布纤维。以 $L \times L$ 象素的分辨率扫描验证对象 100。每根纤维有固定长度为 R 。尽管图 1 中的示例验证对象 100 包含纤维，可以理解，也可以相似方式在验证证书中使用带有其它随机分布特征的验证对象。

[0027] 验证对象 100 的随机分布特征可在验证证书中使用，以保护诸如产品的随机对象验证的证据。例如，某些有关验证证书随机分布特征的难以复制的数据可被数字化、用签发器 (issuer) 的私钥签名、并且签名以机器可读形式印在验证证书上以便校验产品是真的。验证证书的每个实例都与签发器想要证明其真实性的对象相关联。在一实施例中，验证的校验通过使用签发器公钥提取经签名数据（关于随机分布特征的数据），并校验提取数据与验证证书的相关联实例数据相匹配来完成。为了伪造被保护对象，对手需要：(i) 算出签发器私钥，(ii) 设计可准确复制验证证书的已签名实例的制造过程，或者 (iii) 验证证书

的不当签名实例。从这个角度而言,验证证书可被用来保护其值大约不超过伪造单个验证证书实例(包括成功的对抗性制造过程累积开发)的成本的产品。

[0028] 验证证书系统的目标是确保产品或关联于产品的某些信息的验证。其应用的集是众多并广泛的,范围从软件和介质(例如DVD、CD)的防盗版,到不可伪造礼券和防篡改硬件的设计。例如,制造防篡改芯片将需要在其包装上覆盖一个验证证书。在每次使用前,应当校验验证证书的完整性,以便校验被保护硅片的真实性。

[0029] 下面,将讨论用以便宜但有效地读出基于纤维验证证书的随机分布特征的实例硬件平台。硬件平台可包括条形码。由于对于低成本读取器条形码的容量限制为约3k比特,由私钥签名的消息也被限制为同样长度。还有,由于验证证书系统的目标之一是使打算伪造验证证书特定实例的对手要花费的精力最多,将讨论关联于在固定长度的经签名消息中存储尽可能多的关于基于纤维验证证书的唯一且随机分布特征的信息的困难。将提供用于基于纤维验证证书的示例分析模型。然后,以下的讨论也将正式提出点集压缩问题,并显示验证证书实例中纤维位置的优化压缩是NP-完全问题。为了探索式地解决该问题,将提供一种对常规压缩方法的压缩比例上有极大改进的算法。

[0030] II. 签发并校验验证证书

[0031] 图2是示出验证系统200的示例证书,以及由该系统采用的用以签发并校验验证证书的示例过程的示意图。验证系统200的证书包括验证证书210、签发器230以及验证者250。如图2所示,验证证书210可包括图1中的验证对象、条形码213和文本215。

[0032] 在验证证书上需要保护的信息包括:(a)验证对象100难以复制的随机分布特征的表示以及(b)任意相关联文本数据。开始,使用硬件设备扫描诸如纤维位置的验证对象100的随机分布特征。如何收集并表示该信息的细节将结合图3如下进行讨论。

[0033] 为了进行讨论,假设结果信息f是 n_F 个比特的随机字符串。参数 n_F 是固定的,并等于 $n_F = k * n_{RSA}$, $k \in N$,其中 n_{RSA} 是RSA公钥的长度(例如, $n_{RSA} = 1024$),且k通常设定为 $k \in [1, 3]$ 。给定一固定 n_F ,代表验证对象100随机分布特征的数据231的摘要f可使任何两个不同验证证书实例之间的距离统计地为最大。在验证步骤中该目标直接转化为假阴性和假阳性的最小可能性。

[0034] 文本数据t是取决于应用(例如,过期日期、制造商保证)的任意字符串。文本数据源自如图2所示印在验证证书210上的文本215。

[0035] 可使用一种诸如SHA1的密码学安全散列算法237来使文本数据形成散列。散列函数的输出被表示为有 n_T 比特的消息t。签发器230创建可通过RSA签名的消息m。例如,使用确保m的每个比特都取决于f和t二者的所有比特的可逆运算符 \otimes ,消息f和t被合并成长度为 $n_M = n_F$ 的消息m。这个步骤可使需要在用以创建某消息m的数据231以及文本215中进行操作的比特数达最多。这种运算符的示例是使用t或者来自t的比特子集为密钥的对f的对称加密 $m = t \otimes f \equiv E_t(f)$ 。使用签发器230的私钥233用RSA签名235对消息m进行签名。结果签名s有 $n_S = n_M = n_F$ 比特。该消息被编码并在验证证书210上印制为条形码213(诸如遵照PDF417标准的条形码)。

[0036] 验证证书210的校验包括若干步骤。开始校验器扫描印制组件:文本215和条形码213。条形码213被解码为原始印制签名s。文本215被扫描并形成散列以便创建消息t。注意对该任务而言不需要一般光学字符识别(OCR),因为用以印制该文本的字体为校验

器 250 已知，并为改进 OCR 优化。为了验证证书的成功校验，需无错误地读取文本 215 和条形码 213；这是用现代扫描技术就可轻松完成的任务。

[0037] 校验器 250 使用签发器的公钥 253 来执行 s 上的 RSA 签名校验 255，并获取经签名消息 m。然后检验者 250 计算 $f = m(\otimes)^{-1}t$ 。在使用加密为 \otimes 的示例中，这可通过解密 $f = E_t^{-1}(m)$ 来完成。接着，检验者 250 扫描表示验证对象 100 中随机分布特征的数据 251，并创建其表现 f'。检验者 250 比较 f' 和经提取 f。检验者 250 需要对两组数据之间的相互关系进行量化：附于证书上的数据和用以创建验证证书上签名的数据。在判定框 259，如果两组数据的相似度超过了某阈值，检验者 250 宣布验证证书 210 是真的，反之亦然。

[0038] 图 3A 是示例扫描系统 300 的示意图，该系统用以捕捉关联于验证证书的验证对象 310 的随机分布特征。扫描系统 300 包括光学扫描仪 322 和光源 324。光学传感器 322 被配置用以扫描验证对象 310，并可包括特定分辨率的电荷耦合装置 (CCD) 矩阵。在一实施例中，光学传感器 322 的分辨率为 128×128 象素。光源 324 被配置用以提供有特定波长的光，以照亮验证对象 310 的区域。电源 324 可包括例如发光二极管。如图 3A 所示，验证对象 310 中纤维 326 的一端被光源 324 照亮。光线传送到纤维 326 的另一端，并被光学传感器 322 所检测。

[0039] 图 3B 是图 3A 中验证对象 310 的顶视图。操作中，扫描系统 300 将验证对象 310 分成诸如 311-314 的多个区域。如图 3B 所示，扫描系统 300 的光源 324 照在区域 314 上，而区域 311-313 从光源 324 隔离。通过照亮区域 314，验证对象 310 在区域 311-313 中的端点位置可由光学传感器 322 确定。因而，验证对象 310 中随机分布特征的读取包括包含四个不同点集的四个数字化图像。每个点集与一个特定区域相关联，且通过照亮该区域来确定。

[0040] 可以想像，诸如纳米技术 (nanotechnology) 的技术进步可使电子装置能够解码来自验证证书的随机分布特征，并创建对应于这些特征的光图案。这种装置可能能够伪造验证证书。在一实施例中，扫描系统 300 可配置成通过改变光源 324 使用的光线波长（例如颜色）来防止这种伪造方法。例如，每次由扫描系统 300 扫描验证对象时，随机选择光线的波长。光学传感器 322 可被配置成检测由验证对象中纤维发出的光线波长，并确定该波长是否对应于光源 324 发出的光线波长。如果发出的波长与检测的波长不匹配，则验证证书可能是伪造品。

[0041] 图 4 是用以创建验证证书的示例过程 400 的流程图。在方框 405，扫描验证证书中的验证对象。可使用图 3A 中的扫描系统 300 来扫描验证对象。

[0042] 在方框 410，确定表示验证对象随机分布特征的数据。在基于纤维的验证对象中，数据可包括诸如图 3B 所示端点的被照亮纤维端点的位置。

[0043] 在方框 415，压缩数据以提高验证证书的安全度。数据压缩将结合图 5 进行详述。简言之，可确定用以压缩表示验证对象中随机分布属性的一部分数据的路径。

[0044] 在方框 420，编码经压缩的数据。例如，经压缩的数据可使用图 2 中私钥 233 进行签名。在方框 425，经编码的数据被加入验证证书。例如，经编码数据可在印制证书上印成诸如图 2 中条形码 213 的条形码。

[0045] 图 5 是示例过程 500 的流程图，该过程可用以压缩表示验证对象随机分布属性的数据。为了进行讨论，过程 500 将在基于纤维验证证书的上下文中进行描述。然而，过程

500 可应用于任何类型的验证证书。

[0046] 在方框 505, 确定关联于验证对象的概率密度函数。概率密度函数将在小节 III-A 中讨论。示例概率密度函数如等式 11 所示。示例概率密度函数的图形表示在图 8 中示出。简言之, 概率密度函数表示在验证对象的某位置发现一个随机分布属性单元的可能性。在基于纤维验证证书的上下文中, 概率密度函数可表示在验证对象区域中一特定点被照亮的概率。也可使用概率密度函数来计算在特定区域中一共有多少纤维将被照亮。

[0047] 在方框 510, 确定关联于随机分布属性的向量。在基于纤维验证证书的上下文中, 使用点对点向量并在小节 IV-A 中讨论。特别地, 等式 16 被用来计算点对点向量以表示基于纤维验证证书中的随机分布属性。

[0048] 在方框 515, 使用算术编码算法来编码向量。算术编码算法将在小节 IV-A 中讨论。示例算法在表格 2 中显示。

[0049] 在方框 520, 确定用于在固定量数据中压缩部分向量的路径。用以计算路径的方法在小节 IV-B 中讨论。可使用等式 20 来计算示例路径。在方框 525, 返回表示部分随机分布属性的经压缩数据的路径。

[0050] III. 验证证书模型

[0051] 在本小节中, 讨论基于纤维验证证书的分析模型。模拟了验证证书 S 的两个特征。假设照亮了验证证书的特定区域 S_i , 计算在 $S-S_i$ 中特定点被照亮的概率密度函数。同样, 假设在 S 中有 K 根纤维, 可计算在 $S-S_i$ 中被照亮纤维的预期数量。

[0052] A. 被照亮纤维端点的分布

[0053] 验证对象 (L, R, K) 被模拟为边长为 L 单元的正方形, 其上随机抛掷有固定长度为 $R \leq L/2$ 的 K 根纤维。诸如可变纤维长度或随意形状验证对象的其它模型变量, 可从该模型推理。验证对象位于图 1 所示 2D 笛卡尔坐标系统的正象限中。另外, 验证对象被分成四个相等的正方形 $S = \{S_1, S_2, S_3, S_4\}$ 。每个都被用来记录结合图 3A 和 3B 所述的 3D 纤维结构。然后, 纤维被表示为点 $A, B \subset S$ 的多元组 $f = \{A, B\}$, 从而它们间的距离为 $\|A-B\| = R$ 。

[0054] 定义 1. 被照亮纤维端点的分布。假设一个正方形 S_i 被照亮, 对任意点 $Q(x, y) \subset S-S_i$ 通过任何区域 $P \subset S-S_i$ 包含纤维 $f = \{A, B\}$ 的被照亮纤维端点 A 的概率 $\xi(i, P)$ 来定义概率密度函数 (pdf) $\varphi(i, Q(x, y))$, 以其它端点 B 位于被照亮区域 S_i 的事实为条件。更正式地, 对于任何 $P \subset S-S_i$:

$$[0055] \quad \xi(i, P) = P_r[A \subset P | f = \{A, B\} \subset S, B \subset S_i]$$

[0056]

$$= \iint_{Q(x,y) \subset P} \varphi(i, Q(x, y)) dx dy \quad (6)$$

[0057] 假设把纤维 $f = \{A, B\}$ 掷入验证对象包括两个相关联事件 : (i) 第一端点 A 落于验证对象上以及 (ii) 第二端点 B 碰到验证对象。尽管 A 可以落在 COA 上的任意地方, B 的位置却取决于 A 的位置。端点 B 必须落于以 A 为中心半径为 R 且包含在验证对象中圆的部分圆周内。在本小节的剩余部分, 函数 $\varphi(i, Q(x, y))$ 基于对事件 (i-ii) 的分析进行分析计算。为简便起见, 当区域 S_i 被点亮时仅计算 $\varphi(i, Q(x, y))$ 。 $\varphi(i, Q(x, y))$ 分两步进行计算。

[0058] 定义 2. 圆周容纳 (Perimeter Containment)。首先, 对于给定点 A $\subset S$, 定义测量以 A 为圆心半径为 R 被整个验证对象 S 包围的圆的部分圆周 (弧) 长度的容纳函数 $\rho(A)$ 。在验证对象中有四个 $\rho(A)$ 同一计算的不同区域 (在图 6 中标记为 P1 到 P4)。

[0059] 图 6 是对应于示例验证对象 600 中四个不同区域的区域 P1-P4 的图形表示。对于某区域 P_x 的每个点, 以对该区域独特的封闭分析形式使用如下讨论的等式 7-10 来计算圆周容纳函数。

[0060] 区域 P1。这是圆周对象的中心区域, 对于任意点 Q $\subset P_1$, 以 Q 为圆心半径为 R 的圆与验证对象的任何边界不相交。该区域由 $R \leq x \leq L-R, R \leq y \leq L-R$ 定界。

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

[0062] 区域 P2。有四个不同 P2 区域, 在以任意点 Q $\subset P_2$ 为圆心半径为 R 的圆与验证对象的一个边界正好相交两次。为了简便, 仅考虑以下区域: $R \leq x \leq L-R, 0 \leq y < R$ 。可对称计算其它三个区域的等式。

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

[0064] 区域 P3。有四个不同 P3 区域, 在以任意点 Q $\subset P_3$ 为圆心半径为 R 的圆与验证对象的两个不同边界相交两次。为了简便, 仅考虑以下区域: $0 \leq x < R, 0 \leq y < R, x^2+y^2 \geq R^2$ 。

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

[0066] 区域 P4。有四个不同 P4 区域, 在以任意点 Q $\subset P_4$ 为圆心半径为 R 的圆与 COA 的两个边界相交一次。仅考虑以下区域: $x^2+y^2 < R^2$ 。

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

[0068] 在所有的等式 8-10 中, 仅考虑在 $(0, \pi/2)$ 中函数 $\arcsin(\cdot)$ 和 $\arccos(\cdot)$ 的返回值。

[0069] 在第二个步骤, 仅当 B 位于以 Q(x, y) 为圆心半径为 R 并被包含于 S_1 的圆 C(Q, R) 的部分上时, 基于纤维 $f = \{A, B\}$ 的被照亮端点 A 在位置 A = Q(x, y) 上的事实计算有效的 $\varphi(i, Q(x, y))$ 。

[0070] 引理 3. $\varphi(i, Q(x, y))$ 源于 $\rho(Q(x, y))$ 的相关性。使用函数 $\rho(Q(x, y))$, 用以下积分计算 pdf $\varphi(i, Q(x, y))$:

[0071]

$$\varphi(i, Q(x, y)) = \int_{C(Q, R) \subset S_1} \frac{\alpha R d\theta}{\rho(Q(x + R \cos \theta, y + R \sin \theta))} \quad (11)$$

[0072] 其中 θ 在 $C(Q, R) \subset S$ 的圆周上递进, 而且 α 是常量从而:

[0073]

$$\iint_{Q(x, y) \subset S - S_1} \varphi(i, Q(x, y)) dx dy = 1. \quad (12)$$

[0074] 仅因为纤维 $f = \{Q, B\}$ 点 $Q \subset S-S_i$ 可被照亮, 从而 $B \subset S_i$ 。这隐含了 B 位于由 S_i 包含的圆 $C(Q, R)$ 的圆周上的某处。对于某给定纤维 $f = \{A, B\}$, A 落在长度为 $d\ell \subset S$ 的特定无限小圆弧上的概率等于 $d\ell/e(B)$ 。因此:

[0075]

$$\varphi(i, Q) = \text{area}(S-S_i)^{-1} \int_{C(Q, R) \subset S_i} \frac{4Rd\ell d\theta}{e(B(Q, R, \theta) \subset C)d\ell}, \quad (13)$$

[0076] 其中函数 $\text{area}(S-S_i)$ 计算在 $S-S_i$ 下的区域。因而, 在点 $Q \subset S-S_i$ 上的 pdf $\varphi(1, Q(x, y))$ 与 $\rho(\cdot)$ 在 $C(Q, R) \subset S_i$ 上值的倒数的积分成比例。

[0077] 图 7 是示例验证对象 700 上十九个不同区域的图形表示, 该对象有独特的分析公式作为等式 11 中确定的积分的解式。为了简便, 使用简单的数字计算近似解答 $\varphi(1, Q(x, y))$ 。结果在图 8 中示出。

[0078] 图 8 是带有从单元点上采集的参数 $L = 64$ 以及 $R = 28$ 的正方形验证对象的示例概率密度函数的曲线图。图 8 显示了纤维端点落在某小区域 $P \subset S-S_i$ 的可能性取决于 P 在 $S-S_i$ 中的特定位置而有极大的变化。通过使用关于 $\varphi(i, Q(x, y))$ 在整个 $S-S_i$ 中变化的信息, 可大大改进点子集压缩算法, 如小节 IV 中所示。在整个区域 $S-S_i$ 上制造验证对象使 $\varphi(i, Q(x, y)) = \text{常量}$ 不是一个琐碎的任务而已, 可能会和伪造原始验证对象一样困难。

[0079]

Area	Bounds	$\varphi(1, Q(x, y))$
T0	$0 \leq x \leq L/2 - R, 0 \leq y \leq L/2 - R$	0
T1	$x^2 + (y - L/2)^2 < R^2, 0 \leq x \leq L/2 - R, L/2 - R < y \leq L/2$	$R \left[\arcsin\left(\frac{x}{R}\right) + \arccos\left(\frac{L/2-y}{R}\right) \right]$
T2	$x^2 + (y - L/2)^2 \geq R^2, 0 \leq x \leq L/2 - R, L/2 - R < y \leq L/2$	$2R \arccos\left(\frac{L/2-y}{R}\right)$
T3	$x^2 + (y - L/2)^2 \geq R^2, (x - L/2)^2 + y^2 \geq R^2, (x - L/2)^2 + (y - L/2)^2 \geq R^2$	$2R \left[\arccos\left(\frac{L/2-y}{R}\right) + \arccos\left(\frac{L/2-x}{R}\right) \right]$
T4	$x^2 + (y - L/2)^2 < R^2, (x - L/2)^2 + y^2 < R^2, (x - L/2)^2 + (y - L/2)^2 \geq R^2$	$R \left[\arcsin\left(\frac{x}{R}\right) + \arcsin\left(\frac{y}{R}\right) \right] + R \left[\arccos\left(\frac{L/2-y}{R}\right) + \arccos\left(\frac{L/2-x}{R}\right) \right] +$
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	$x^2 + (y - L/2)^2 < R^2, (x - L/2)^2 + y^2 \geq R^2$	$R \left[\arcsin\left(\frac{x}{R}\right) + \arccos\left(\frac{L/2-y}{R}\right) \right] + 2R \arccos\left(\frac{L/2-x}{R}\right)$

[0080]

	$(x - L/2)^2 + (y - L/2)^2 \geq R^2,$ $L/2 - R < x \leq L/2$	
T7	$x^2 + (y - L/2)^2 < R^2,$ $(x - L/2)^2 + y^2 \geq R^2,$ $(x - L/2)^2 + (y - L/2)^2 < R^2$	$R \left[\frac{\pi}{2} + \arcsin\left(\frac{x}{R}\right) + \arccos\left(\frac{L/2-x}{R}\right) \right]$
T8	$x^2 + (y - L/2)^2 \geq R^2,$ $(x - L/2)^2 + y^2 \geq R^2,$ $(x - L/2)^2 + (y - L/2)^2 < R^2$	$R \left[\frac{\pi}{2} + \arccos\left(\frac{L/2-y}{R}\right) + \arccos\left(\frac{L/2-x}{R}\right) \right]$

[0081] 表格 1(注解 :area- 区域, bounds- 边界)

[0082] B. 纤维端点的照亮比例

[0083] 定义 3. 纤维端点的照亮比例。对于验证对象 (L, R, K) 及其照亮区域 S_i , 照亮比例 λ 被定义为纤维 $f = \{A, B\}$ 落在对象上使得其端点之一在 $B \subset S-S_i$ 中的概率, 其中以其它端点在 $A \subset S_i$ 的事实为条件 :

[0084] $\lambda = \Pr[B \subset S-S_i | f = \{A, B\}, A \subset S_i]. \quad (14)$

[0085] 定义 4. 可能照亮圆弧。对于任意点 $A \subset S_i$, 函数 $\varphi(i, A(x, y))$ 被定义为测量包含于 $S-S_i$ 内 $C(A, R)$ 的边界部分的长度的函数。

[0086] 图 9 是区域 T0-T8 的图形表示, 使用独特的封闭分析形式来计算 $\varphi(i, Q(x, y))$ 函数。 $\varphi(i, Q(x, y))$ 基于小节 III-A 上对事件 (i-ii) 的分析进行分析计算。类似于小节 III-A, 仅在区域 S_i 被点亮的情形进行计算。在 COA 中有九个不同区域 (图 9 中标记为 T0 到 T8), 其中 $\varphi(1, Q)$ 同一计算。取决于 Q 在 S_i 中的位置对 $\varphi(1, Q)$ 的分析封闭形式在表格 1 中给出。

[0087] 引理 4. $\varphi(1, Q(x, y))$ 、 $\rho(Q(x, y))$ 和 λ 的相关性。如定义 3 中定义的照亮系数 (illumination ratio) 可如下计算 :

$$[0088] \lambda = \int_{Q(x,y) \subset S_i} \frac{\varphi(i, Q(x, y))}{\rho(Q(x, y))} dx dy. \quad (15)$$

[0089] 以点 $A \subset S$ 为中心的半径为 R 的圆被表示为 $C(A, R)$ 。对于每个点 $Q \subset S_i$, 纤维 $f = \{Q, B\}$ 的另一端点 B 落于 $S-S_i$ 内的可能性, 等于 $C(Q, R)$ 分别被 $S-S_i$ 和 S 包含的圆周长度的比例。通过将该比例对 S_i 中所有点积分, 可获得等式 15。

[0090] 给定使用 λ 由数字近似等式 15 和来自表格 1 的 $\varphi(1, Q)$ 封闭形式计算的验证对象 (L, R, K) , 可计算当 S_i 被照亮为 $\lambda K/2$ 时 $S-S_i$ 中被照亮点的预期数量。例如, 对于验证对象 (64, 28, 100) 结果 $\lambda \approx 0.74$, 其含义是在 S_i 被照亮的情形中被照亮的端点数量平均约为 $0.74 \cdot 50 = 37$ 。

[0091] IV. COA 中点子集的压缩

[0092] 验证证书系统的目标是确保制造 (即伪造) 特定验证对象实例的任务尽可能地困难。该目标被量化为对记录验证对象尽可能多纤维的位置的需求。在示例压缩算法中, 验证对象的区域数等于 4; 因此, 对于每个区域 S_i , 经签名消息 m 中的 $1/4$ 比特数 $n_m/4$ 被用以

存储尽可能多的一旦照亮了 S_i , $S-S_i$ 中被照亮的纤维端点。注意一般而言, 不需要存储所有的被照亮端点; 仅需要使用 $n_w/4$ 比特数编码的这些点的最大子集。

[0093] 在本小节中, 描述了一种机制, 其被配置为用以编码验证对象中两个照亮点之间的距离。该机制基于算术编码。然后, 形式化使用固定比特数来压缩尽可能多纤维端点的问题。最后, 讨论将显示该问题是 NP- 完全问题, 并提供一种建设性试探法作为次优方案。

[0094] A. 编码点对点向量

[0095] 在本分节中, 描述了如何使用接近最少的比特数来编码由其起点和终点定义的向量。附加限制是被考虑区域中的点根据给定 pdf 出现。

[0096] 1) 算术编码

[0097] 算术编码器 (AC) 把任意长度的输入流转换成 $[0, 1]$ 中的单一有理数。AC 的主要优点是它能接近熵 (entropy) 地任意压缩。以下的讨论显示如果给定带有未知 pdf 符号出现的字母表, 如何对字 “aba” 进行编码。

[0098] 图 10 是如果给定带有未知 pdf 符号出现的字母表 $L = \{a, b\}$, 算术编码器如何编码字符串 “aba”的示例的图形表示。示例如图 10 所示。开始时, AC 的范围被重设为 $[0, 1]$, 且 L 中每个符号都有相等的出现可能性 $Pr[a] = Pr[b] = 1/2$ 。因而, AC 将其范围分成二个子范围 $[0, 0.5]$ 和 $[0.5, 1]$, 每个分别代表 “b” 和 “a”。通过把 AC 的范围限制成对应于该符号即 $[0.5, 1]$ 的范围, 对符号 a 进行编码。另外, AC 为符号 “a”的出现更新计数器, 并重新计算 $P_r[a] = 2/3$ 以及 $P_r[b] = 1/3$ 。在下一次迭代中, 根据已更新 $P_r[a]$ 和 $P_r[b]$, AC 将其范围分成 $[0.5, 0.6667]$ 以及 $[0.6667, 1]$, 每个分别代表 “b” 和 “a”。当下次 “b” 到达时, AC 将其范围减到相应的 $[0.5, 0.6667]$, 更新 $P_r[a]P_r[b] = 2/4$, 并将该新范围分成 $[0.5, 0.5833]$ 以及 $[0.5833, 0.6667]$, 每个分别代表 “b” 和 “a”。由于最终的符号为 “a”, AC 通过选择 $[0.5833, 0.6667]$ 中的任意数作为输出来编码该符号。通过选择用最少比特数编码的数字 (我们示例中的数字), 0.6, AC 创建其最终输出。解码器由明显在经压缩消息首部或通过专用的 “end-of-file” 符号知道消息长度。

[0099] AC 迭代地减少其操作范围直到某一点, 当其范围中上边界和下边界的主要数字相等。然后, 传送主要数字。称为 “重正化” (renormalization) 的该过程可用限定精度算术单元进行任何长度的文件压缩。传统 AC 的性能改进集中在: 使用预先计算的算术运算近似值, 将用移位和加法替换除法和乘法。

[0100] 使用等于源熵 $H(s) = -\sum_s Pr[s_i] \log_2(Pr[s_i])$ 的比特数, AC 编码一个序列的输入符号 $s = s_1, s_2, \dots$ 。因此, 对于不相关并同一分布符号的半无限流, 在带有无限精度算法的计算机上, AC 是最佳的熵编码器。

[0101] 2. 最短距离点对点向量的算术编码

[0102] 给定一个验证对象 (L, R, K) , 假设光线照在其四分体之一 S_i 。然后, 我们假设验证对象被分割成 $L \times L$ 单元方块的网格 $U = u(i, j) i = 1 \dots L, j = 1 \dots L$, 其中每个 $u(i, j)$ 覆盖 $x \in [i-1, i], y \in [j-1, j]$ 中的方形区域。单元区域模拟验证对象数字化扫描的象素。扫描分辨率等于 $L \times L$ 。然后, 单元 $u(x, y)$ 的主要点被定义为坐标为 (x, y) 的点 Q_u 。

[0103] 引理 5. 单元照亮可能性。假设有 k 根纤维的只有一个端点在 $S-S_i$ 中, 任何单元区域 $u(x, y) \subset S-S_i$ 包含至少一个被照亮纤维端点的概率等于:

$$[0104] \tau(u) = \Pr[\{\exists f = \{A, B\} \in F) A \subset u, B \subset S_i\}] \quad (16)$$

[0105] $= 1 - [1 - \xi(i, u)]^k.$

[0106] 以及

[0107] $\tau(u) = \Pr[(\exists f = \{A, B\} \in F) A \subset u, B \subset S_i] = 1 - \Pr[(\neg \exists c \in F) A \subset$

[0108] $u, B \subset S_i] = 1 - (1 - \Pr[A \subset u, B \subset S_i | f = \{A, B\}])^k$

[0109] 由等式 7 可得出等式 16。在小节 III-B 中, 计算出 k 的期望值为 $E[k] = \lambda K/2$ 。

[0110] 问题 1. 对 COA 的双向量编码。以单元 $U \subset S-S_i$ 包含一被照亮纤维端点的事实为条件, 目标是要使用尽可能少的比特数来编码相对于单元 u 的另两个被照亮单元 v_1 和 v_2 的位置。附加限制是在 $S-S_i$ 的所有被照亮单元中, 分别为 Q_1 和 Q_2 的 v_1 和 v_2 主要点位于离 u 主要点 Q_u 的两个欧几里得几何 (Euclidean) 最短距离上。优先规则设置为如果一组单元 V , $|V| > 1$ 位于相对于 u 的相同距离上, 最有可能照亮的那个单元 $\text{argmax}_v \subset V(\tau(v))$ 被首先编码。

[0111]

设定 U 是 $S-S_i-u$ 中所有单元区域的列表。
 所有经标记单元的列表 $M(u)$ 被设定为 $M(u) = \emptyset$ 。
 do
 找出所有的单元区域 $V = \text{argmin}_{v \in V} \|Q_v \cdots Q_u\|$ 。
 do
 找出单元区域 $w = \text{argmax}_{v \in V} \xi(1, v)$ 。
 设定 w 的 AC 范围为 $\gamma(w, u)$ (参见等式 17, 18)。
 排列在 w 之前节点组是 $M_w(u) = M(u)$ 。
 $M(u) = M(u) \cup w$, $V = V-w$, $U = U-w$ 。
 while $V \neq \emptyset$
 while $U \neq \emptyset$

[0112]

表格 2. 算法 A1

[0113] 使用 AC 完成单元对单元向量的编码, 其中使用算法 A1 在每个编码符号 (即不同于源单元 u 的每个单元 $v \subset S-S_i$) 编码间隔上分配的相应范围。对于每个单元 v , 算法 A1 分配了等于 v 是相对源单元 u 两个最近被照亮单元之一的概率的范围。该概率表示为 $p(v|u)$ 。在当 $k >> 1$ 预期在 $S-S_i$ 中单元被照亮时, 可如下计算 $p(v|u)$:

[0114] $p(v|u) = \tau(v) \prod_{w \in M_v(u)} [1 - \tau(w)] + \quad (17)$

[0115] $\sum_{w \in M_v(u)} \tau(v) \tau(w) \prod_{z \in M_v(u), z \neq w} [1 - \tau(z)],$

[0116] 其中单元组 $M_v(u)$ 以算法 A1 进行计算。对于每个单元 v , 以已编码 u 的事实为条件, 算法 A1 分配由 AC 使用的范围 $\gamma(v, u)$ 以编码 v 。该范围等于 :

[0117] $\gamma(v, u) = \frac{p(v|u)}{\sum_{w \in S-S_i} p(w|u)}. \quad (18)$

[0118] 因而, 两个最近的被照亮单元由接近最优的构建进行编码 (例如在带有无限精度

算法的处理器上编码最优),因为使用约等于源熵的若干比特来编码一系列符号:

$$[0119] \quad H(u) = - \sum_{v \in S-S_i} \gamma(v, u) \log_2 [\gamma(v, u)]. \quad (19)$$

[0120] 双向量编码被用作基元(primitive),以小节IV-B中给出的整体压缩算法来编码点子集。尽管该编码算法对于小节IV-A.2中给出的那组假设而言是接近最优的,但是相同的限制组并不对整体压缩目标有效。因此,通过A1使用带有范围分配的算法编码的固有最优化在小节IV-B中讨论。

[0121] B. 点子集的压缩

[0122] 模拟了使用固定比特数来压缩尽可能多被照亮单元区域位置的最优化问题。考虑以下带有权重边界的有向完全图形。对于每个被照亮单元 $u \subset S-S_i$, 创建节点 n_u 。从节点 n_u 到节点 n_v 的有向边界 $e(u, v)$ 用编码指向 v (如等式19中 $\omega(e(u, v)) = -\log_2[\gamma(v, u)]$) 向量的编码字最优长度被赋以权重,假设 u 已被编码的事实为条件。将此图表示为 $G(N, E, \Omega)$,其中 N, E, Ω 分别表示节点组、有向边界、以及相应的权重。

[0123] 问题2. 点子集的压缩(CPS)。

[0124] 实例:有向、完全、且带有权重的图形 $G(N, E)$,其具有非负顶点函数 $\Omega : E \rightarrow R$ 、正整数 $l_{min} \in Z^+$ 、正实数 $\Lambda \in R^+$ 。

[0125] 问题:有没有这样的 $l > l_{min}$ 节点子集 $N^* \subset N$,其具有穿过节点的路径即排列 $\langle n_{\pi(1)}^*, \dots, n_{\pi(f)}^* \rangle$,使得沿路径的权重和为:

$$[0126] \quad \sum_{i=1}^{l-1} \omega(e(n_{\pi(i)}^*, n_{\pi(i+1)}^*)) < \Lambda. \quad (20)$$

[0127] 问题2模拟了使用固定存储(例如 Λ)来压缩验证对象中尽可能多(例如1)纤维端点的最优化问题。该问题是NP完全的,因为它证明通过对 Λ 的二进制检索非对称流动推销员问题(ATSP)可被简化为CPS, $ATSP \leq_p CPS$ 。在本小节的剩余部分,给出了针对解决该问题的有效建设性试探法A2。试探法的先决设计要求是快速的运行时性能,因为每个验证证书必须在生产线上单独签名。

[0128] 首先, N 中两节点间的距离测量不遵从所有节点的三角不等式。直观地,小节IV-A中的编码过程使用与某单元是两个最近的被照亮单元之一的可能性成比例的若干比特来对 $S-S_i$ 中的向量进行编码。因此,由于离源节点较远的单元不太可能出现,就以长得多的编码字对它们编码,这使在方案路线中到这些节点的捷径变得极为不合需要。

[0129] 定理2. 距离测量 ω 一般不遵从三角不等式:

$$[0130] \quad \omega(e(u, v)) + \omega(e(v, w)) \geq \omega(u, w)$$

[0131] 为简便起见,假设 ($\forall u \subset S-S_i$) $r = \tau(u) =$ 常量,则 u, v 和 w 都位于 $S-S_i$ 中的同一线条上。欧几里得距离 $\|u-v\|$, $\|v-w\|$ 和 $\|u-w\|$ 分别是 a, b 和 $a+b$ 。三角不等式隐含了 $f(u, v, w) = \log_2[\gamma(w, u)] - \log_2[\gamma(v, u)] - \log_2[\gamma(w, v)] \geq 0$ 。从等式17和18,可计算出以下等式:

$$[0132] \quad f(a, b, t) = 2ab\pi \log_2(1-t) + \log_2 \frac{t}{1-t} - \quad (21)$$

$$[0133] \quad -\log_2 \frac{(1-t)^2 + (a^2 + b^2)\pi t(1-t) + a^4 b^4 \pi^2 t^2}{1 + [(a+b)^2 \pi - 1]t},$$

[0134] 且显示对于 $ab\pi 1 >> 1$, 三角不等式不成立, 即 $f(a, b, t) < 0$ 。

[0135] 三角不等式成立的 ATSP 最佳近似算法, 所产生的方案最多比最优方案差 $\log(|N|)$ 倍。或者, 就作者所知, 还未开发出三角不等式不成立的 ATSP 变式的近似算法。通常, 当距离度量函数 ω 任意时, ATSP 问题是 NPO 完全的, 即除非 $P = NP$ 才会有好的近似算法。另一方面, 可解决 TSP 变式的满足三角不等式比例版本

[0136] $\mu(\omega(e(u, v)) + \omega(e(v, w))) \geq \omega(u, w)$, $\mu > 1$ 的近似算法, 其最坏结果是比最优方案差 $(3\mu + 1)\mu/2$ 倍。距离度量 ω 不遵从该限制, 因此, 问题 2 的试探法无最差情形保证地进行开发。另外, 我们追求试探法的尽可能好的平均性能, 而不是最差情形保证。可去除不能满意压缩的验证对象实例。这种事件的可能性应当是很小, 少于百万分之一。

[0137]

建设性阶段

边界组为 $E' = \{\text{argmin}_{(a,b)} (\omega(a,b), \omega(b,a)) \mid (\forall a, b) \subset N\}$ 。

子路径组 P 被选为按 ω 排序的 E' s.t. $\sum_{e \in P} \omega(e) \leq \Lambda$ 中最短 K 个边界的组。

将 E 中最短边界的权重表示为 ω_{\min} 。

for 每个路径 $p_i \subset P, i = 1..K - 1$

for 每个路径 $p_j \subset P, j = i + 1..K$

if p_i 和 p_j 有同一个源-目标节点

连接 p_i 和 p_j 为 $p_i = p_i \cup p_j$

从 P 中去除 p_j

将路径 $p_i \subset P$ 的源和目标节点分别表示为 s_i 和 d_i

for 每个路径 $p_i \subset P, i = 1..K$

找出所有从 s_i 到任何 $d_j, j \neq i$ 的最短路径 $q(i,j)$

while $|P| < \max P$

$$(p_i, p_j) = \text{argmin}_{q(i,j)} \sum_{e \in \{p_i \cup q(i,j) \cup p_j\}} \frac{\omega(e)}{|(p_i \cup q(i,j) \cup p_j)|}$$

连接 $p_i = p_i \cup q(i,j) \cup p_j$ 并从 P 去除 p_j

穷举地找出连接 $p_h = p_1 \cup \dots \cup p_{\max P}$ s.t.

$$M(p_h) \{ \sum_{e \in p_h} \omega(e) < \Lambda \text{ 且 } |p_h| \text{ 为最大值} \}$$

reroute(P_h) (重找路线)

reroute(P_h)

$P_{best} = P_h$

for 每个边界 $e(s_i, d_i) \subset p_h, i = 1, \dots, |p_h| - 1$

for 每个节点对 $(d_i, s_j) \subset p_h, j = i + 2, \dots, |p_h| - 1$

找出经 $N - p_h$ 中节点的最短路径 $q(i,j)$

if 路径 $e_1, \dots, e_i \mid q(i,j) \mid e_j, \dots, e_{|p_h|}$ 有比 P_{best} 更好的度量 $M(p_h)$

then $P_{best} = P_h$

贪婪迭代改进

repeat (重复) 1 次

收缩 P_h 使得 $\sum_{e \in P_h} \omega(e) \leq \rho \Lambda$, 其中 ρ 是从 $\rho \in \{0.4, 0.8\}$ 中随机选取的收缩因子。

将节点 n_0 和 n_1 表示为 P_h 的第一个和最后一个节点。

while $\sum_{e \in P_h} \omega(e) \leq \Lambda$

在具有 n_0 和 n_1 分别作为目标或源的边界中, 找出带有最小权重的边界 e 。

将 e 连接到 P_h 。

reroute(P_h)

[0139]

表格 3. 算法 A2

[0140] 使用来自小节 IV-A 的距离度量之后的基本原理, 是基于这样的假设: 好的方案经由两个最近邻节点成功遍历路径上的每个节点。因此, 在问题 2 的范围内, 仅当最佳方案被发现满足该属性时所使用度量才是最佳的。如果最终方案并无此属性, 编码单个向量的最优性取决于方案中边界权重的分布。

[0141] 已开发的试探法 A2 有两个步骤: 建设性阶段和迭代改进阶段。建设性阶段遵从建立初始方案的贪婪试探法。开始时, A2 标识一组优势边界 E' 。对于节点 u, v 之间的每对边界 $e(u, v), e(v, u)$, A2 仅选择两者中较短边界并将之存储在 E' 中。然后通过对 E' 中的边界排序并选择其权重和尽可能接近 Λ 的最短前 K 个边界, 创建一组初始子路径 P 。路径 P_h 中的第一个和最后一个节点被分别表示为 s_i 和 d_i 。在下一步骤中, A2 以权重的递增顺序来迭代地连接来自 P 的子路径: 在任何点上, 直到建立了所有可能连接, 才连接具有共同源 - 目标节点 $d_i = s_j$ 的最短子路径对 p_i, p_j 。在 $|P| = 1$ 的不太可能的情形中, 找到了最佳方案并停止搜索。否则, 从 P 中去除所有单边界子路径。然后, 使用 Dijkstra 算法, A2 找出 P 中每个子路径 p_i 的每个目标端点 d_i 和所有其它子路径 $s_j, i = 1 \dots |P|, i \neq j$ 的源端点之间的所有最短路径。经由不在 P 中的节点, 定出最短路径路线。 s_i 和 d_j 之间的最短路径表示为 $q(i, j)$ 。在另一贪婪步骤中, A2 根据其权重 / 节点计数比例来排序所有的连接 $p, |q(i, j)| P_i$ 。以该度量的递增顺序, A2 继续经由 $N-P$ 中的节点连接 P 中子路径, 直到剩余路径的总数为 $|P| = \max P$ (通常 $\max P = 9$)。使用找出带有最佳度量 (最大基数和权重之和小于 Λ) 路径 p_h 的精确算法来连接这些剩余路径。在最后步骤中, 重定路径过程浏览了所有 P 中的节点, 并使用 Dijkstra 算法尝试找出经由 E 中剩余节点到 P 中其它节点的最短路径。相同的过程还尝试找出比 p_h 中存在的更好结束端点。对于每个重定路径, A2 检查新的重定路径是否比当前的最佳路径 p_h 有更好的度量。

[0142] 图 11 是验证对象实例的示例, 被示为具有 $\kappa = 88$ 个节点的 $(512, 0.4 \cdot 512, 256)$ 。A2 返回用粗线表示路径。该路径的权重和比 $\Lambda = 512$ 小。为了记录该路径, 使用 12.11 比特 / 点。

[0143] 在迭代改进阶段中, 我们重复以下循环若干次。在第一步中, A2 把当前发现的最佳路径 P_{best} 收缩为 p_h , 从而 $|p_h|$ 是最大值且沿 p_h 的权重和小于 $\rho \Lambda$ 的一小部分。收缩参数 ρ 是在每次迭代中在 $\rho \in \{0.4, 0.8\}$ 范围内随机选取的。节点 n_0 和 n_1 被表示为 p_h 中的第一个和最后一个节点。虽然 p_h 上权重和小于 Λ , 在把 n_0 或 n_1 分别作为目标或源的边界之中, 我们发现带有最小权重的边界 e 并把其连接到 p_h 。当创建了新的候选路径 p_h 时, 如果其度量比迄今为止所创建的最佳度量更好, 则将其采用为最佳方案。在迭代改进循环

的最后一步时, A2 执行前述的重定路径过程。

[0144] 为了使 A2 对于特定验证对象 (L, R, K) 类的运行时在一秒之内, 改进循环重复 $I = \{100, 10000\}$ 次。一般而言, 当通过 Dijkstra 算法计算多源最短路径时, A2 的最差次数复杂性为 $O(|N|^3 \log |N|)$ 。在使用 Floyd-Warshall 算法来计算所有成对最短路径的实现中, A2 的复杂性可降为 $O(|N|^3)$ 。尽管图形原来是完全的, 通过去除具有高权重的边界, 我们还是创建了稀疏图形, 其中用于计算所有成对最短路径的 Johnson 算法产生了 $O(|N|^2 \log |N| + |N||E|)$ 。

[0145] V. 经验估算

[0146] 本小节中的讨论示出验证对象 (L, R, K) 参数如何影响算法 A2 的执行。图 11 示出了对问题单个实例 – 验证对象 (512, 0.4 • 512, 256) 的方案。扫描对准 $L = 512$ 的扫描单元网格。该图示出了当验证对象的左下四分体被照亮时的情形。使用相应被照亮纤维端点建立的图形 $G(N, E)$ 用中等粗线示出。仅示出了从图中每个 $\kappa = 88$ 节点开始的最短的前十个边界。在图中用粗线示出的结果路径包括四十一个节点。沿路径边界的权重和小于存储限制: $\Lambda = 512$ 比特。使用 12.11 比特 / 纤维端点 (b/fep) 压缩了该路径。不经压缩存储该数据需要 $41 \cdot 18 = 738$ 比特, 因而压缩比为 0.61。压缩比被定义为经压缩消息尺寸与原消息尺寸的比例。

[0147] VI. COA 系统的设计目标

[0148] 验证证书设计者的目标是使用有限制造成本 ζ_m 使伪造成本 ζ_f 最高。若干参数可影响 ζ_m 。为简便起见, 讨论三个参数:

[0149] 纤维总长度 $RK \leq \Phi$,

[0150] 扫描误差 ζ , 以及

[0151] 条形码存储 Λ 。

[0152] 通过限制对手可进行的对经签名纤维端点足够的分组精确定位的试验次数 (小节 VI-A) 并选取系统参数 { R, K } , 来最优化系统性能, 从而使预期伪造成本 $\zeta_f(A2)$ 达最高 (小节 VI-B)。

[0153] A. 限制对手试验次数

[0154] 考虑把 κ 个被照亮纤维端点中的 G 个存储在限定为 Λ 的存储器中。一般而言, 当伪造验证证书时, 对手可使用所有 κ 根纤维来尝试把其中至少 $G \zeta$ 根精确置入相应位置。伪造验证证书的成本大部分取决于可进行试验的次数。在这里, 提出了一种通过检测在验证期间经签名纤维端点周围纤维的非正常分布, 以减少对手试验次数 K_T 的技术。

签发 COA 实例

扫描当灯光照在 S_i 上时被照亮的 κ 个点的组 N 。

使用 Λ 个比特来压缩分组 $P \subset N$, 其中 $G = |P| \leq \kappa$ 。

找出单元分组 $U \subset S-S_i$, 从而

$$(\forall u_i \in U) (\forall p_j \in P) \min(\|u_i - p_j\|) < \varepsilon_1.$$

$$\varepsilon_1 = |N \cap U| - G, K_T = G + \varepsilon_2.$$

签名 P , ε_2 以及相关联信息 (参见小节 2)。

校验 COA 实例

从签名中提取 P , ε_2 。

找出单元分组 $U \subset S-S_i$, 从而

$$(\forall u_i \in U) (\forall p_j \in P) \min(\|u_i - p_j\|) < \varepsilon_1.$$

扫描当灯光照在 S_i 上时被照亮的 κ' 个点的组 N' 。

if $|N' \cap U| > K$, then COA 实例无效,

elseif $|N' \cap P| \geq G \zeta$ then COA 实例有效,

else COA 实例无效。

[0155] 表格 4. 算法 A3

[0156] 验证证书的签发器和校验器对每个验证对象四分体 S_i 重复算法 A3 的各自部分。开始时签发器扫描验证对象实例，并收集有关灯光照在 S_i 上时所照亮的点组 N 的信息。然后，使用可用的 Λ 个比特，它压缩由 A2 返回的最大分组 $P \subset N$, $|P| = G$ 。然后，A3 找出分组 $U \subset S-S_i$, 从而每个单元 $u_i \in U$ 与其最近单元 $p_j \in P$ 之间的欧几里得距离最大为 ε_1 。单元分组 U 表示 P 的 ε_1 邻域。然后，签发器计算存在于 U 的 N 中点数 K_T 。因为, K_T 不得不比 G 大以防止假阴性，签发器存储了消息 m 中后来用签发器私钥签名 (参见小节 II) 的差值 $\varepsilon_2 = K_T - G$ 以及 P 。使用签发器的公钥，校验器从所附签名中提取经压缩点分组 P 和 ε_2 ，并重建相应的 ε_1 邻域 U 。然后，校验器为了灯光照在 S_i 上时所照亮的纤维组 N' 对验证对象进行扫描。通过检查 U 和 N' 中的共同点数至多为 $G + \varepsilon_2$ ，而 N' 和 P 中的共同点数至少为 $G \zeta$ ，它宣布该实例是真的。

[0157] 通过把 ε_2 存储在签名中，对手被强迫使用最多 $K_T = G + \varepsilon_2$ 次在 P 的 ε_1 邻域中定位纤维的试验。对手的目标是精确放置来自 P 的至少 $G \zeta$ 个纤维端点，因此对手可忍受在伪造过程中在 P 的 ε_1 邻域中 $G(1 - \zeta) + \varepsilon_2$ 次错误放置。预期目标为点 P_i 的每次试验，如果成功最终该点位于 P_i 的 ε_1 邻域中。通过增大 ε_1 ，校验器可在较大的邻域范围标识可能的错误放置；然而，这也可能增大验证证书设计者想要保持尽可能小值的 ε_2 期望值。

[0158] 以下显示了一种经验设计方法，其采用给定 $\varepsilon_1 = \text{常数}$ ，并从若干验证证书参数的角度追求使主要目标 $\zeta_j(A2)$ 的最大化。

[0159] B. 设计一种 COA 系统

[0160] 问题 3. COA 系统的设计目标。对于给定压缩算法 A2、给定的 $RK \leq \Phi$ 、 ζ 、 ε_1 和 Λ ，找出使以下等式最大化的可用纤维的一个分段 (cut) $\{R_*, K_*\}$ ：

$$\{R_*, K_*\} = \arg \max_{(R, K) | RK \leq \Phi} \zeta_f(A2, R, K), \quad (22)$$

[0162] 其中 ζ_f 是伪造 COA 实例的成本。

[0163] 图 12 是为最佳成本效力设计的验证证书的图形表示。横坐标相对于 L 量化纤维长度 R, 而纵坐标示出了纤维数 K。显示条示出伪造 log- 成本为 $\log_{10}(\zeta_f(A2, R, K))$, 其中限制极限 $A = 512$ 比特且一组固定参数为: $\zeta = 0.9$, $\varepsilon_1 = 8$ 和 $v = 0.8$ 。该图还示出了为固定长度纤维 $RK = \Phi = 100L$ 的所有分段而获取的方案质量。

[0164] 可使用一种简单的搜索最佳纤维分段 $\{R_*, K_*\}$ 的经验技术。使用图 12 示出搜索过程。横坐标和纵坐标分别表示 R 和 K 的值。显示条表示伪造验证证书实例的期望 log- 成本 $\log_{10}(\zeta_f(.42, R, K))$ 。该成本相对于 R、K、以及固定参数组 $A = 512$, $\zeta = 0.9$ 和 $v = 0.8$ 给出。图 12 中图表是经验计算的。A2 应用于随着 $R = \{0.05L, 0.10L, \dots, 0.45L\}$ 和 $K = \{80, 96, \dots, 192, 256, 384, 512, 768, 1024\}$ 的每个组合而随机生成的 500 个验证证书 (512, R, K) 实例。 $\{R, K\}$ 空间剩余部分中每个点的预期压缩性能是通过内插 (interpolating) 经验结果来获取的。从图 12, 可在邻域 $k_* \approx 900$ 和 $R_* \approx 0.1L$ 中找到最佳纤维分段。该结果指出了这样一个事实, 即对于选定设计环境十字形验证证书是最佳选项。注意纤维分段的审慎选择可导致相对于 $RK = \Phi$ 上随机选定点而在伪造成本上成数量级的改进。可应用在此例中使用的经验原理, 以针对不同的验证证书环境和制造限制搜索接近最佳的参数组。

[0165] 图 13 阐述了所述系统和方法可在其中全部或部分实现的示例计算装置 1300。计算装置 1300 仅是计算系统的一个示例, 并非旨在提出对本发明使用范围或功能性的任何限制。

[0166] 计算装置 1300 也可在很多其它通用或专用计算系统环境或配置中实现。适于使用的众所周知的计算系统、环境、和 / 或配置的示例包括, 但不限于, 个人计算机、服务器计算机、瘦客户机、厚客户机、手持式或膝上型设备、多处理器系统、基于微处理器的系统、置顶盒、可编程电器消费品、网络 PC、迷你计算机、大型机、游戏控制台、包括任一种以上系统或设备的分布式计算环境、等等。

[0167] 计算装置 1300 的组件可包括, 但不限于, 处理器 1302 (例如任何微处理器、控制器等等)、系统存储器 1304、输入装置 1306、输出装置 1308 以及网络装置 1310。

[0168] 计算装置 1300 通常包括各种计算机可读介质。计算机可读介质可以是能被计算装置 1300 访问的任何可用介质, 并包括易失和非易失介质、可移动和不可移动介质。系统存储器 1304 包括诸如随机存取存储器 RAM 的易失存储器和 / 或诸如只读存储器 ROM 的非易失存储器形式的计算机可读介质。包含有助于计算装置 1300 如起动时在元件间传送信息的基本例程的基本输入 / 输出系统 BIOS 通常存储在系统存储器 1304 中。系统存储器 1304 通常包含可被处理器 1302 立即访问和 / 或现时操作的数据和 / 或程序模块。

[0169] 系统存储器 1304 还可包括其它可移动 / 不可移动、易失 / 非易失计算机存储介质。作为示例, 可包括硬盘驱动器用来读取和写入不可移动、非易失磁性介质; 磁盘驱动器用来读取和写入可移动、非易失磁盘 (例如“软盘”); 以及光盘驱动器用来读取和写入可移动、非易失光盘, 诸如 CD-ROM、DVD 或其它类型的光学介质。

[0170] 盘驱动器及其相关联的计算机可读介质为计算装置 1300 提供计算机可读指令、数据结构、程序模块、和其它数据的非易失存储。可以理解, 其它类型的计算装置 1300 可访问的可存储数据的计算机可读介质, 如磁带或其它磁性存储设备、闪存卡、CD-ROM、数字化多功能光盘 (DVD) 或其它光学存储设备、随机存取存储器 (RAM)、只读存储器 (ROM)、电子可擦可编程只读存储器 (EEPROM) 等等, 也可被用来实现示例性计算装置 1300。任何数量的程

序模块可被存储在系统存储器 1304 中，包括作为示例，操作系统 1320、应用程序 1328、以及数据 1332。

[0171] 计算装置 1300 可包括各种标识为通信介质的计算机可读介质。通信介质通常包含计算机可读指令、数据结构、程序模块、或其它已调制数据信号形式的数据，诸如载波或其它传送机制，且包含任何信息传递介质。术语“已调制数据信号”意指用将信息编码到信号中的方式设置或改变其一个或多个特征的信号。作为示例，而非限制，通讯介质包括诸如有线网络或有线直接连接的有线介质，和诸如声学、射频、红外线和其它无线介质的无线介质。所有以上内容的组合也应包含在“计算机可读介质”范围之内。

[0172] 用户可通过诸如键盘和定位装置（如“鼠标”）的输入装置 1306 向计算装置 1300 输入指令和信息。其它输入装置 1306 可包括话筒、游戏杆、游戏垫、控制器、卫星接收器、串行端口、扫描仪、触摸屏、触摸垫、键板、和 / 或等等。输出装置 1308 可包括 CRT 监视器、LCD 屏幕、扬声器、打印机等等。

[0173] 计算装置 1300 可包括用来连接到诸如局域网 (LAN)、广域网 (WAN) 等等的计算机网络的网络装置 1310。

[0174] 尽管本发明已用结构化特征和 / 或方法论步骤的专用语言作了说明，但可以理解的是在所附权利要求书中定义的本发明无须受限于所述特定特征或步骤。相反，特定特征和步骤是以实现所要求保护的本发明的示例性形式被揭示的。

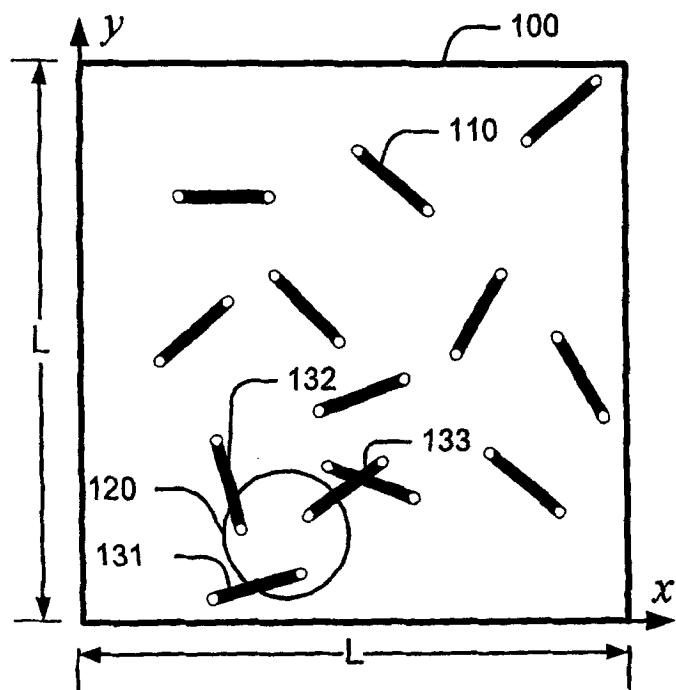


图 1

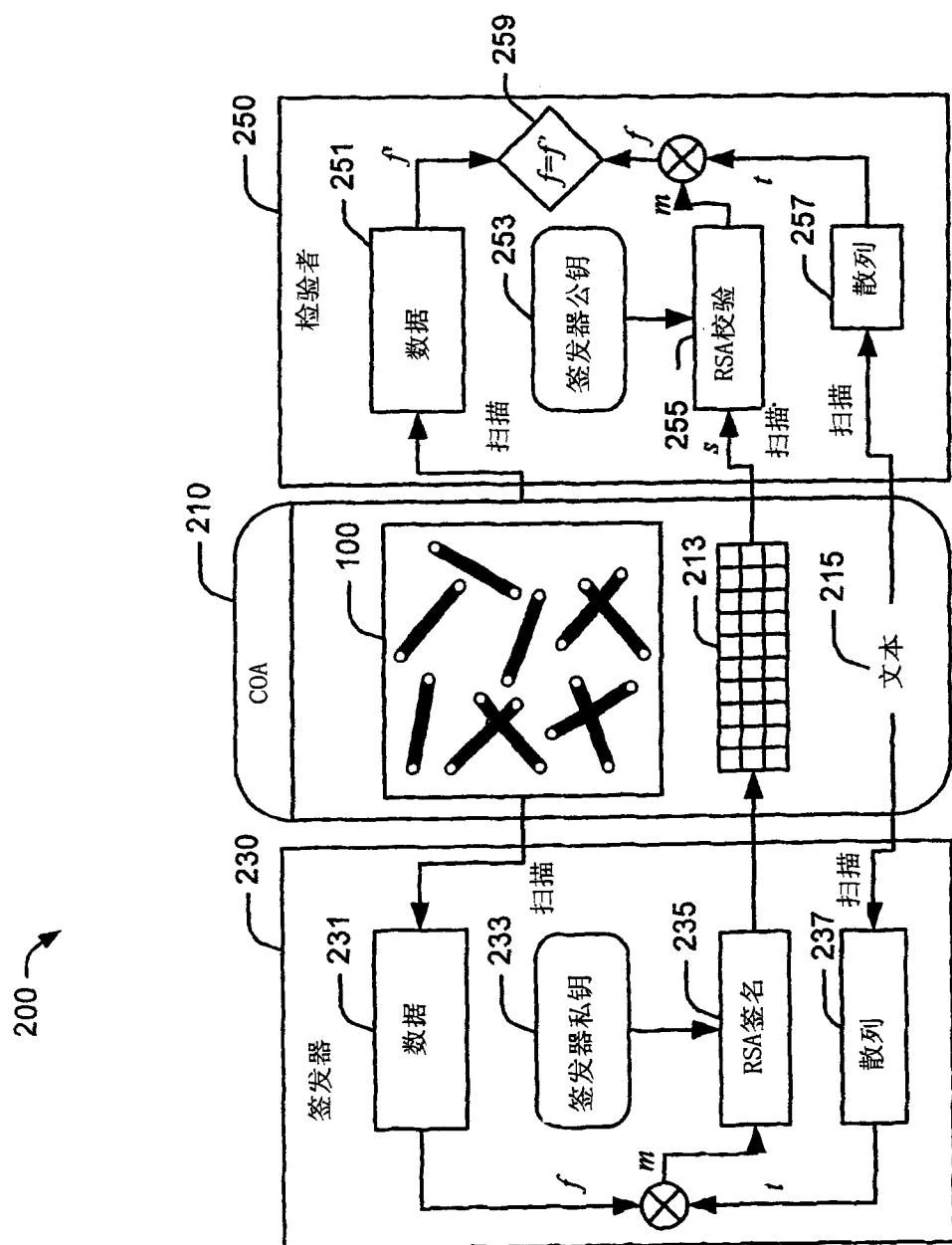


图 2

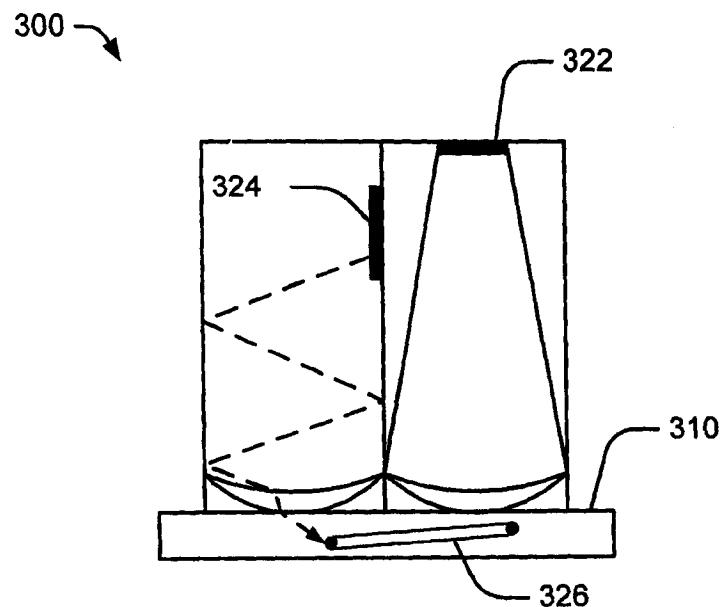


图 3A

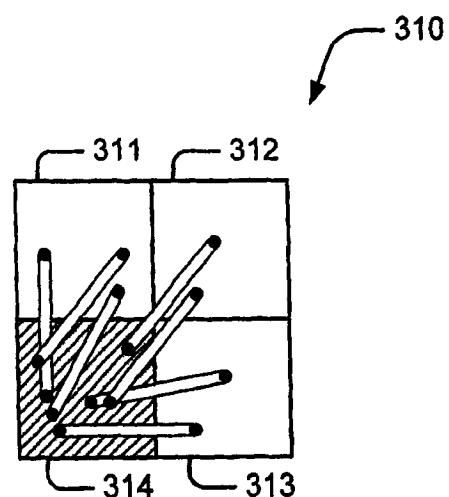


图 3B

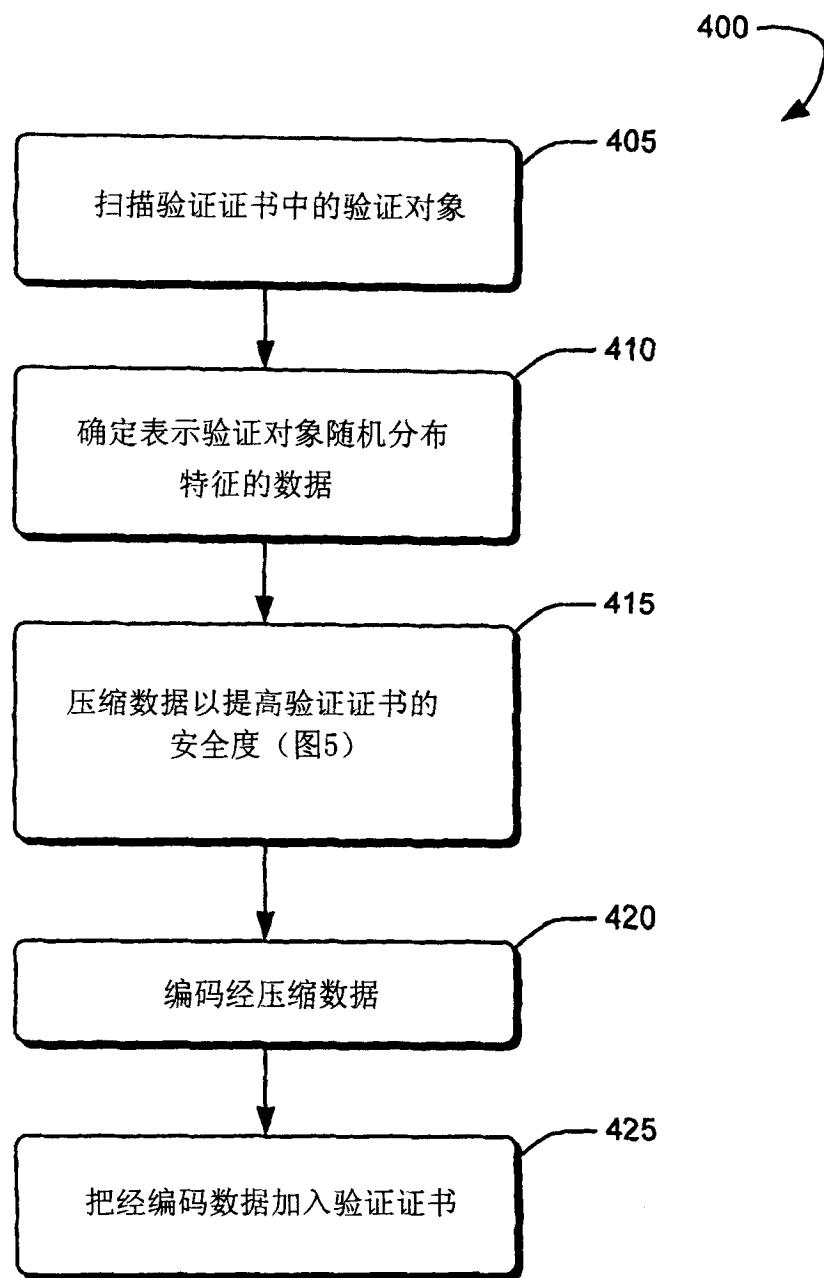


图 4

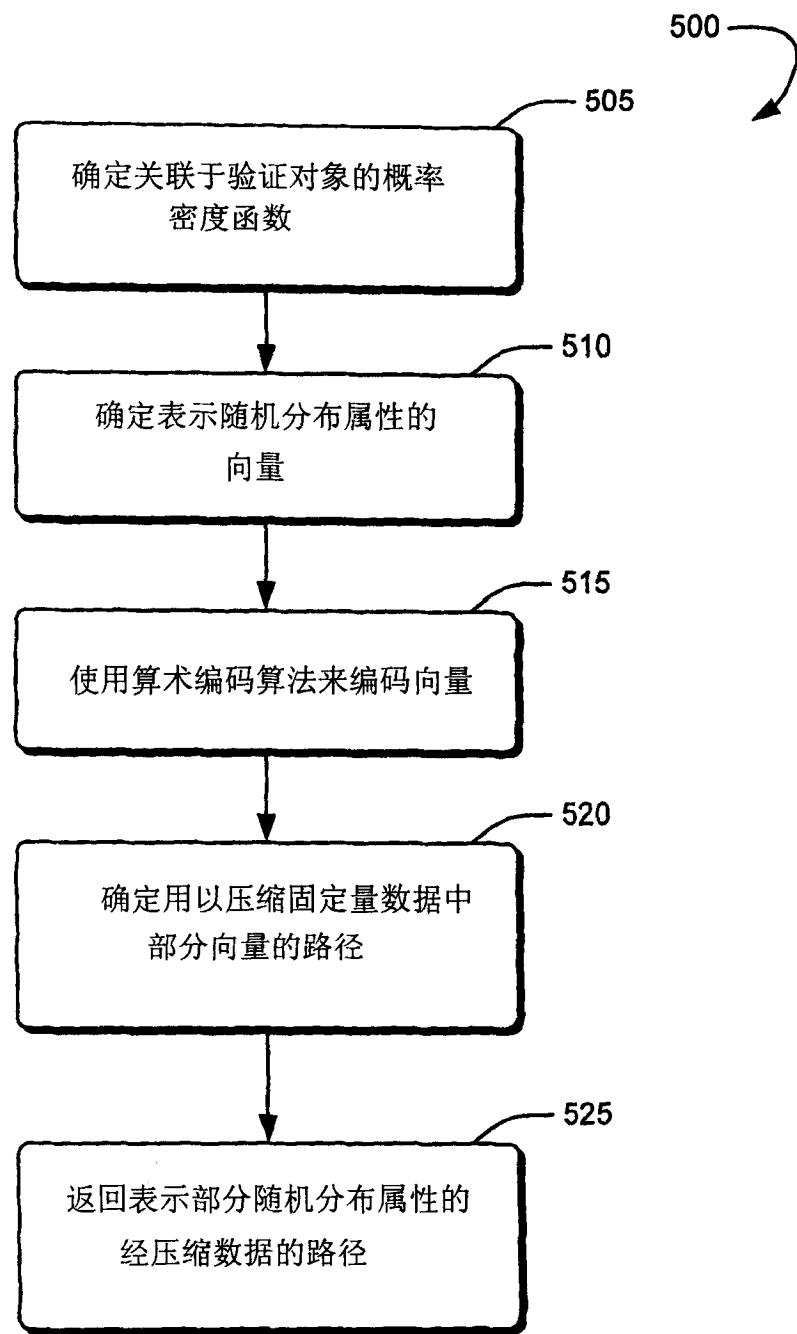


图 5

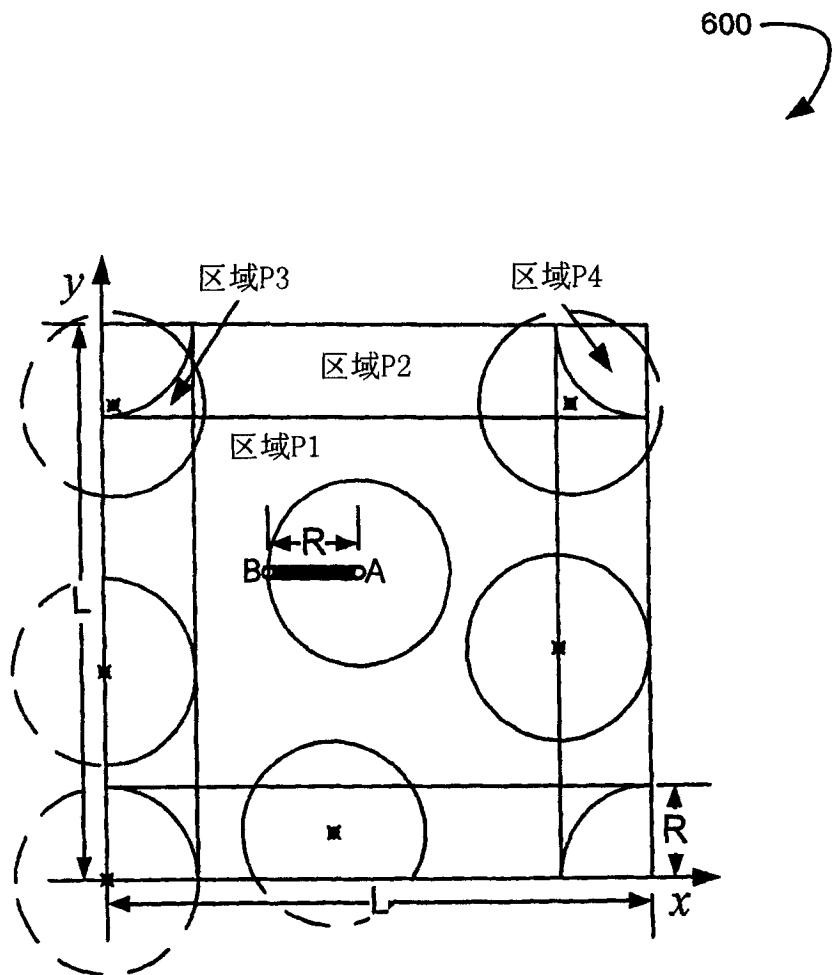


图 6

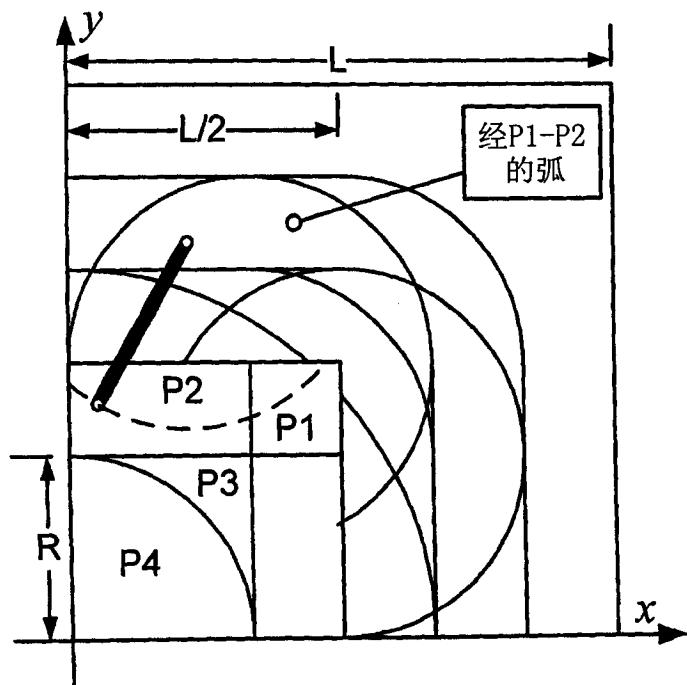


图 7

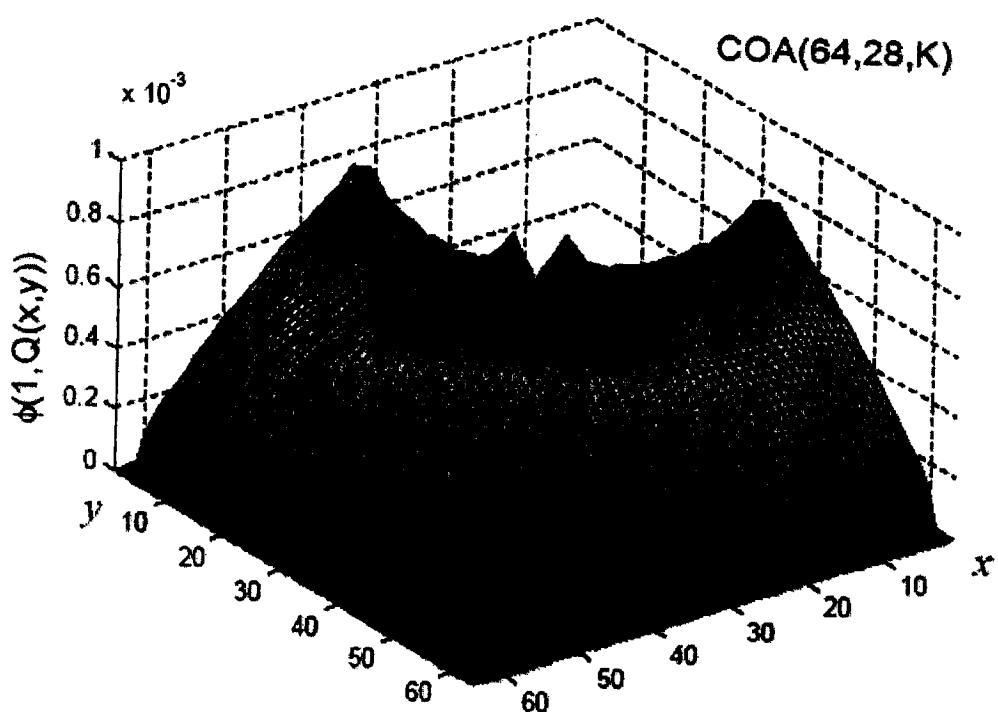


图 8

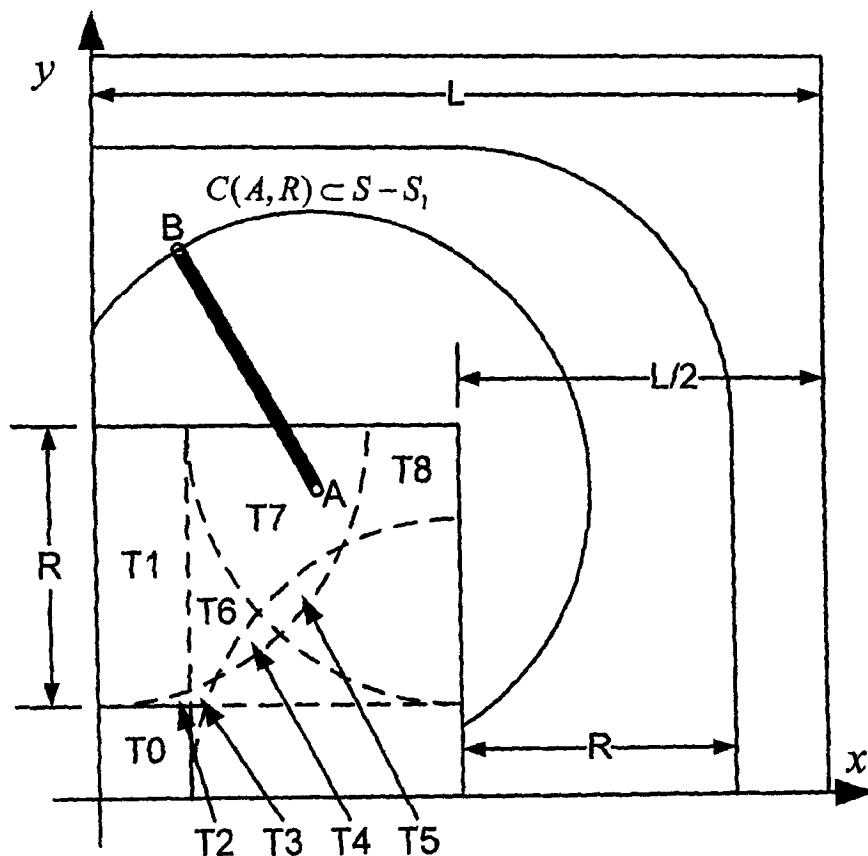


图 9

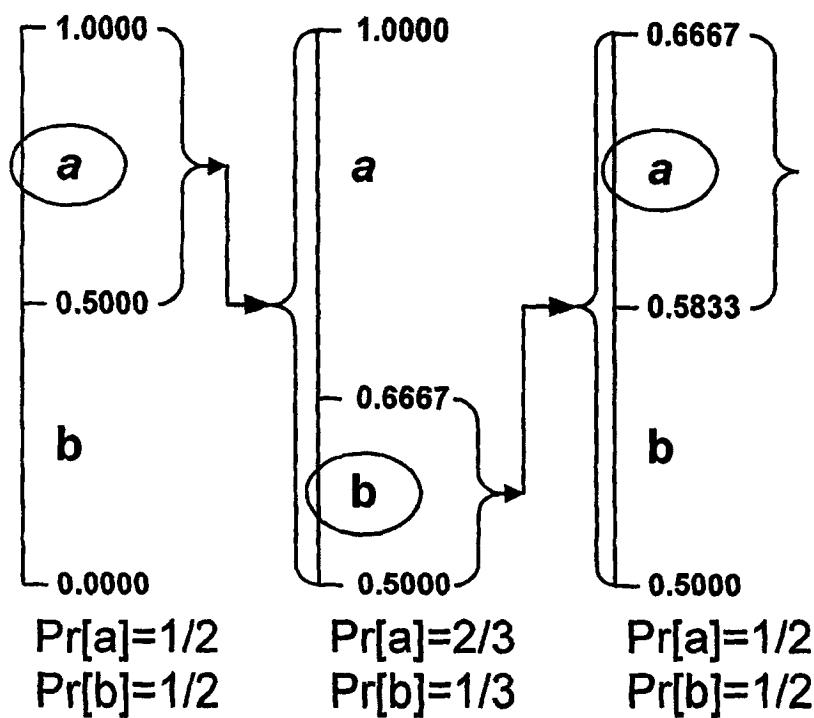


图 10

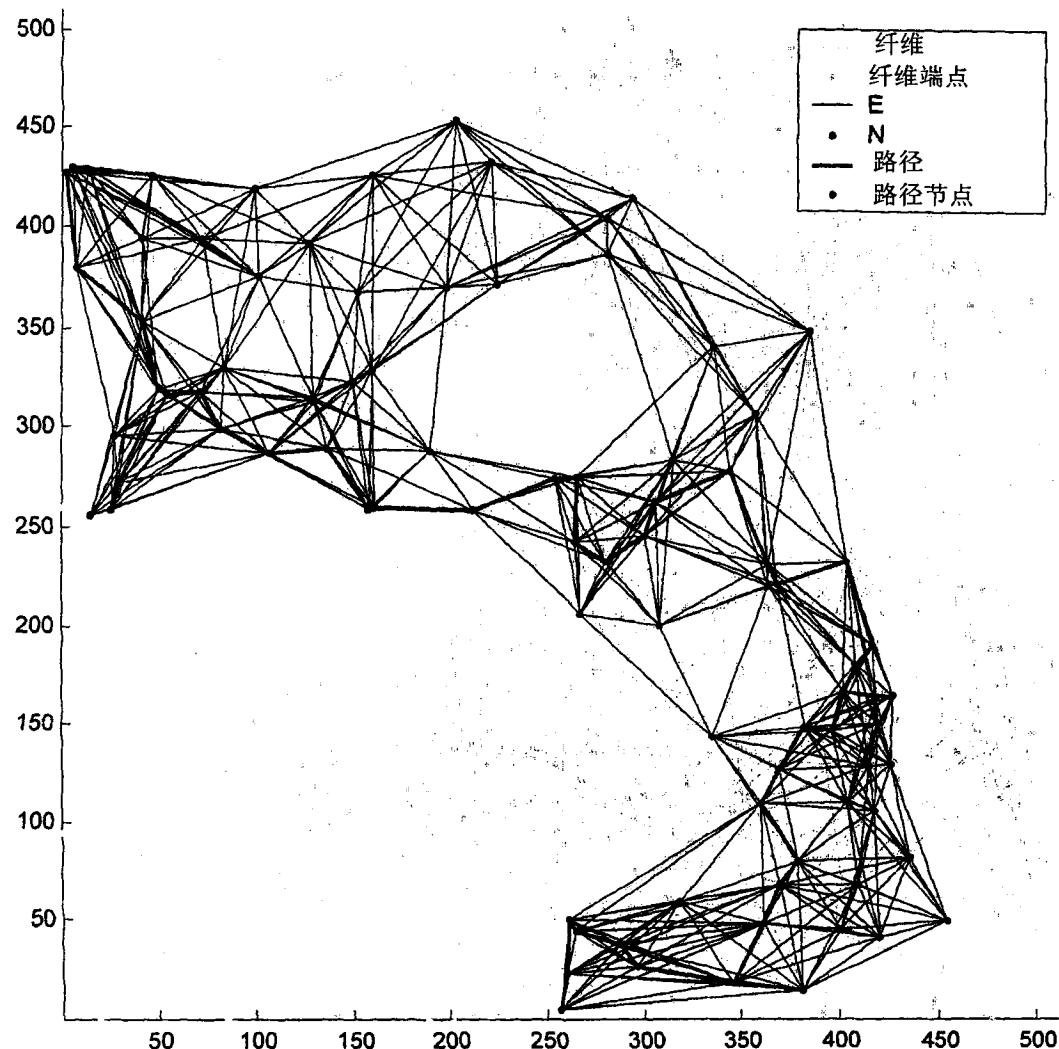


图 11

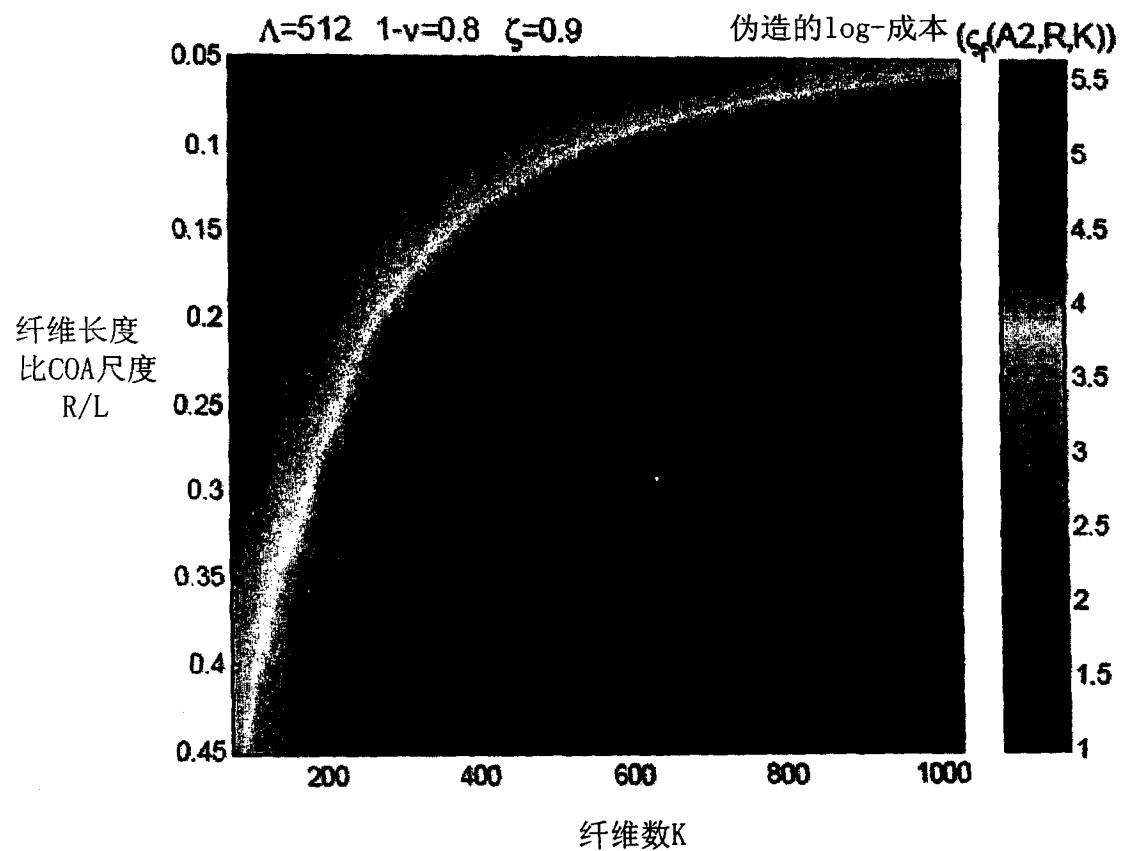


图 12

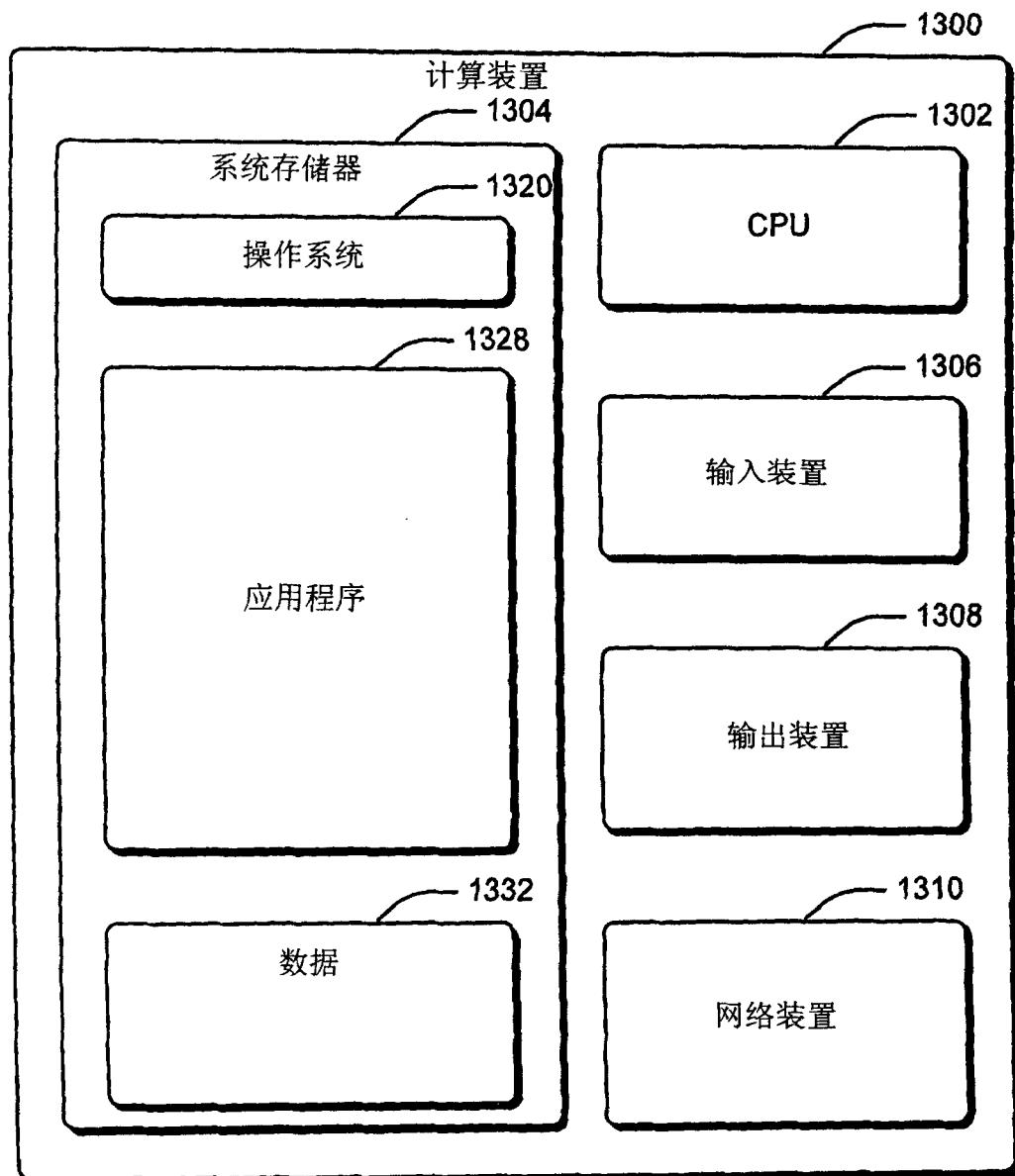


图 13