计算机科学2002Vol. 29№. 12

数字指纹协议的研究与发展

Research and Development of Digital Fingerprinting Protocol

颜 浩 陈克非

(上海交通大学计算机科学与工程系 上海200030)

Abstract With the development of e-commerce, digital product has been the main format of multimedia product on the Internet. At the same time, the problem of copyright protection has gained much attention. Because of the character to be copied easily, the software products such as JPEG or GIF images, applications and documents are being copied illegally every day. This does harm to the merchants' benefit. The goal of digital fingerprinting protocol is to study a method based on cryptography to trace the source of illegal copy, which in certain conditions can be applied in all kinds of software product. The basic idea of digital fingerprinting, like the fingerprint of human being, is to embed an unique "fingerprint" into each copy of the product sent to the buyer. When finding the illegal copy, the merchant can trace the source of it, who maybe is a dishonest buyer called traitor, accuse the traitor. So the merchant can protect his copyright. This paper introduces the history of digital fingerprinting protocol and discusses some of the important protocol schemes.

Keywords Fingerprinting protocol, Copyright protection, Secure 2-party computation, Bit commitment

一、引言

随着电子商务的发展,以无形的数字格式作为多媒体产品的发布形式将成为 Internet 上的主流方式。但由于软件产品的易拷贝性,对软件产品(如 JPEG、GIF 图像,应用程序,各种文档等)的盗版就变得异常容易。从目前的技术研究来说,在开放环境下要严格防止非法使用者的侵权拷贝是不太可行的。主要的研究方向集中在如何有效地追查非法拷贝源,即发布商能够追查到这一份产品拷贝的原始购买者以向这个非法盗版者提起诉讼(正版购买者应保护自己的产品拷贝不被其他人盗取)。这一类相关技术中比较主要的有数字水印技术、数字指纹协议体系等。

数字水印技术研究主要关注一个算法在数字产品(主要针对数字图像)中如何嵌入一串信息(水印)并能够完整地检测恢复。这一信息可以是发布商的名称,也可以是任意的有特定意义的 BIT 串。水印嵌入的要求是不可见性、鲁棒性,还要求能抵抗一定的主动攻击。

仅有水印嵌入检测算法是不足以实现版权的保护,我们需要一个完整的保护协议来规范商家和购买者之间的交易行为。既要保护商家的版权不受侵害,也要保护诚实的购买者的合法权益,因此,人们提出了数字指纹协议的概念。

数字指纹协议有比较大的适应性,在一定的前提下可以应用于各种类型的软件产品(图像、文档等)。其基本思想是类似人类手指指纹的作用,在分发给每个软件产品购买者的产品拷贝中加入唯一的"指纹",当产品生产者发现侵权行为后,通过这一"指纹"来跟踪产品非法拷贝的源头,对盗版者进行指控,从而达到版权保护和威慑的作用。

用指纹协议来进行版权保护的思想最早是由 Neal R. Wagner 在1983年所提出的[1],后人在此基础上从不同的方面提出了各种实际的方案。1994年 Chor 等提出了可以应用于付费电视广播系统中的 Traitor-tracing 协议[2],是指纹协议研究中的一个重要里程碑,以后的众多协议研究都沿用了其中的数学思想。1995年 Boneh 等提出了另一种指纹协议[3],主要解决标记--"指纹"分发问题,这个协议可以和数字水印技术结合起来,从而在更多的应用环境中使用。1996年 Pfitzmann 等提出了非对称的指纹协议的概念和基本协议体系[4],如同加密体系从对称模式发展到分对称模式一样,从另一个安全角度将指纹协议带入了一个新的研究方向。在此之后,人们又不断提出了新的指纹协议体系,如匿名指纹协议[5]、门限 Traitor-tracing 协议[6]等。本文将对一些典型的指纹协议作基本的介绍和分析,并对数字指纹协议未来的研究发展方向和应用前景进行展望。

二、基本 Traitor-tracing 指纹协议的体系结构

Traitor-tracing 协议是由 Benny Chor 等于1994提出的,在详细描述这个协议之前举一个典型的应用例子。在付费电视广播系统中,发行商(Data supplier)向他的所有合法用户广播加密的电视节目,如对每一个节目块(Block)使用不同的对称加密密钥,为了使合法用户能够解密所有节目块,发行商给每个合法用户分发一个唯一的个人密钥(为了能和非对称密码方案中的私钥 private key 加以区别,我们在这里使用个人密钥这个词),用户使用他的个人密钥解密出节目块中的对称加密密钥,从而解密出节目块中的内容。这个个人密钥就可以理解为指纹协议中的"指纹"。

这里有几个假设,任何用户都需要使用一个有效的个人密钥来获取节目的内容,而不能直接把节目的明文广播给非法的用户(这个做法可能是经济代价上不可行的);发行商不可能用每个合法用户的个人密钥直接加密节目或者说向每个合法用户广播完全不同的加密节目内容,因为这样广播代价太大而不可行;节目必须被分成许许多多的小块(Block),每个块使用不同的对称密钥加密(每个对称密钥本身的大小相对于 Block 的大小可以忽略),如果节目使用同一密钥加密,则一个合法用户只要用他的个人密钥解密出对称密钥发给一个非法用户则后者可以一直解密所有的节目。所以任何盗版者只能把自己的个人密钥发给非法用户使用或通过几个共谋盗版者之间通过比较他们各自的个人密钥来拼出一个不同的合法个人密钥发布。

颜 浩 硕士研究生,研究方向:信息安全、秘密学、网络安全。陈克非 博士,教授,博士生导师,研究方向:信息安全、秘密学、网络安全。

考虑安全性，当某个想发布盗版的合法用户 Alice (Traitor)把他的个人密钥非法告诉一个非法用户 Bob(pirate user)，使 Bob 也能够解密出各个节目块中的内容，从而构成侵权行为。当发行商发现 Bob 的侵权行为后，他可以得到 Bob 所使用的个人密钥，发现这个密钥的原始所有者，从而抓到盗版源头 Alice，达到保护版权的目的。在后面的描述中将说明 Traitor-tracing 协议如何保证在 Traitor 共谋的情况下，发行商也可以至少追查出一个共谋盗版者，或者说这个概率是很大的。

更一般地，我们把 Traitor-tracing 描述成如下协议模型：

协议中可能的角色：

· 数据发布者(Data supplier 或 Merchant，下文中都使用后者)：提供数字产品的商家。

·合法用户(User 或 Buyer，下文中都是用后者)：购买数据发布者产品的正版用户。

·盗版者(Traitor)：向非法用户提供个人密钥(指纹)的一个合法用户。

·共谋者(Traitors)：一组通过比较各自个人密钥进行侵权活动的盗版者。

·非法使用者(Pirate user)：使用 traitors 提供的个人密钥获得发布者产品的非正版用户。

·仲裁者(Judge)：仲裁 merchant 对 traitor(s)的诉讼。

协议中的对象：

·商品(Item)：数据发布者出售的一个产品(如一部电影)，合法用户的一个个人密钥在一个同一个商品中都是有效的，每个 Item 被分成多个会话数据块。

·会话密钥(Session key)：对称密码体制的密钥(如流密码中的密钥)。

·会话数据块(Session block)：数据发布者向外广播(公布)的一段产品数据，每个会话数据块包含两部分：

·加密块(Cipher block)：由会话密钥加密的有效数据(明文)，每个会话数据块中使用的会话密钥都不相同；

·使能块(Enabling block)：用分段并且对称加密的方法保存对应加密块使用的会话密钥。

·个人密钥(Personal key)：每个合法用户用来解密会话密钥的一个密钥集合。

协议参数：

coll_size：协议可以保证安全的最大的共谋者的个数；

L：会话密钥的分段个数，个人密钥的集合大小；

b：一个任意字母表的大小，如字母表为{1,2,3,…,b}；

N：Buyer 的最大数量；

协议可以简略地描述成如下的过程(图1)。可分成四个子协议。

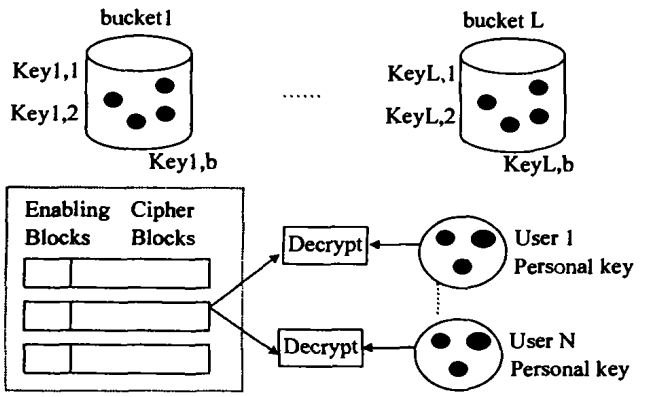

图1

密钥初始化子协议　由 Merchant 执行。对于一个 Item，Merchant 随机选择 L 个对称密钥集合，每个集合有 b 个密钥，每个集合可以形象地比作一个密钥桶(Bucket)，这 L * b 个对称密钥可以按字母顺序表示为 $key_{L,b}$。对于这个 Item 中每个会话数据块，选择一个会话密钥 S。

密钥指纹子协议　对每个 Buyer，Merchant 统一随机选择一个长为 L 的码字，其中每一位都是字母表{1,2,3,…,b}中的某个字母。这样一个码字就和 L 个密钥桶中 L 个密钥对应起来，这 L 个密钥构成一个 Buyer 的 Personal key。如码字为{7,3,4,…,9}，Personal key＝{可 $key_{1,7}$，$key_{2,3}$，$key_{3,4}$，…，$key_{L,9}$}。Merchant 保存每个 Buyer 的 Personal key，把 personal key 发给对应的 Buyer，personal key 对其他人是保密的。(码字的可能空间为 $b^L \gg N$)

会话发送子协议　Merchant 广播(发布)Item 中每个会话数据块，每个会话数据块中 cipher block 使用这个块对应的 session key 加密。session key 被等长地分成 L 段 $S_1 \cdots S_i \cdots S_L$，其中第 i 段使用第 i 个密钥桶中的 b 个密钥进行加密(i＝1,…,L)。这 L * b 个加密值按次序排列构成这个会话数据块的 Enabling block，随加密块一起发送。每个 Buyer 收到一个会话数据块后，使用自己的 personal key 从 Enabling block 中解密出对应的 S_1，…S_L，组成完整的 session key S，从而解密出对应加密块中的有效数据。

盗版跟踪子协议　对一组 coll_size 个共谋 traitors 来说，为了使一个 pirate user 可以成功解密所有 session block 中的数据，他们必须提供一个有效的 personal key。首先他们不会提供其中单个人的 personal key，否则 Merchant 直接从检测出的这个 personal key 查到 traitor，那么他们就要对 L 段中每个 S_i，从他们的 coll_size 个 personal key 中对应的 coll_size 个 $key_{i,j}$ 中选择一个作为解密 S_i 的密钥，使最终共谋产生的 personal key 是有效的，但是和 traitors 中的任意一个 personal key 都不同，来阻止追查。但是，该协议通过如下算法使 merchant 仍能确定其中的一个 traitor：当事后查到了一个 pirate user，merchant 可以得到一个该 pirate user 使用的 personal key K(实际是每个密钥桶中对应一个 $key_{i,j}$)。对于这个 K 中 L 个 $key_{i,j}$(i＝{1,…,L})，merchant 对每个其 personal key 中对应位置等于 $key_{i,j}$ 的 Buyer 作一次标记，如 K＝{$key_{1,7}$，$key_{2,3}$，$key_{3,4}$，…，$key_{L,9}$}，某个 Buyer 的 personal key ＝{$key_{1,7}$，$key_{2,8}$，$key_{3,4}$，…，$key_{L,6}$}(假设…位置中的对应 key 都不相同)，则这个 Buyer 被标记两次(第1、3两个密钥桶)。最后被标记次数最多的 Buyer 就被认为是 traitors 之一。(实际上这个 Buyer 至少被标记 L/coll_size 次，并且共谋所伪造的 personal key 等于一个合法 Buyer 的 personal key 的概率根据参数设置是可忽略的，以保证共谋不能陷害一个诚实的 Buyer，这个算法的证明以及共谋不可陷害的证明在文[2]中进行了详细的证明)。

三、非对称 Traitor-tracing 协议

Pfitzmann 等将非对称的概念应用于 Trait-tracing 协议，以改善协议的安全性和公平性。简单来说，在基本的 Trait-tracing 协议中，Merchant 和 Buyer 都知道卖给 Buyer 的个人密钥(Personal key)，那么在发现盗版提起诉讼时，Buyer 完全可以声称 Merchant 发现的 Personal key 是 Merchant 的一个不诚实的员工所流传出去的，从而使仲裁无法确认谁是 traitor(对称性)。

非对称的概念就是要使标识 Buyer 的"指纹"只有 Buyer 自己知道(自己选择生成其个人密钥的码字),而 Merchant 在商品交易时不知道,但可以确认。在 tracing 时 Merchant 可以得到足够的证据(Proof)来指认相关的 traitor。

非对称的概念也被用于基于码字安全的指纹协议中。

非对称 Traitor-tracing 协议的基础仍基于上文简述的基本 Traitor-tracing 协议,包括参与的角色和对象。为了实现非对称性,我们需要增加三个密码学体系:一个公钥签名模式、一个承诺模式和一个安全2-party 计算。在这里我们不讨论这些模式的概念和实现,假设都已存在。

协议参数:

σ:一个适当的概率参数以表示安全的系数;

coll_size:协议可以保证安全的最大的共谋者的个数;

L:会话密钥的分段个数,个人密钥的集合大小(这里我们选定 $L=64*coll\_size*(\sigma+\log_2(N))$);

b:一个任意字母表的大小,如字母表为{1,2,3,…,b}(这里我们选定 $b=48*coll\_size$);

N:Buyer 的最大数量。

协议分成六个子协议:

Buyer 签名密钥生成　每个购买者(Buyer)生成一对签名模式使用的公私钥(sk_B,pk_B)并公布其 pk_B。

密钥初始化子协议　和基本(对称)协议中的对应子协议相同,merchant 选择 L 个密钥桶(Bucket),每个桶有 b 个对称密钥。

密钥指纹子协议　Buyer 选择一个长为 L 的码字 $word_B$(这一步在基本协议中是由 merchant 完成的)。Buyer 对 $word_B$ 生成一个承诺 com_B,并把这个承诺发送给 merchant。用来揭示承诺的信息称为 $open_B$。Buyer 使用自己的签名私钥 sk_B 对如下消息进行签名:$msg_B=(text, com_B)$,生成 sig_B。其中 text 是一个字符串,只要足以说明签名消息的含义。Merchant 使用 pk_B 验证 sig_B 是对 msg_B 的一个有效的签名。

接下来执行安全2-party 计算:

输入:
Buyer:$word_B$ 和 $open_B$
Merchant:在密钥初始化子协议中生成的 L * b 个对称密钥,一个随机选择的大小为 L/2的集合 Set_B({1,…,L}的子集),com_B

计算:
验证 $open_B$ 可以打开承诺 com_B,否则协议失败
验证 Set_B 的大小最多为 L/2个元素
$word_B$ 中符号对应集合 Set_B 中元素的位置组成的有序符号集称为 $halfword\_trace_B$,其余部分称为 $halfword\_evid_B$

输出:
Buyer:由 $word_B$ 对应生成的个人密钥(Personal key)
Merchant:$halfword\_trace_B$(这样 Merchant 只知道 $word_B$ 中的一半符号而不能猜出整个 $word_B$,仍符合我们的非对称性)
这样在执行完安全2-party 计算后 Merchant 得到的交易记录 $record_M=(id_B, text, com_B, sig_B, Set_B, halfword\_trace_B)$,Buyer 得到的交易记录 $recordB=(text, word_B, open_B)$。

会话发送子协议　和基本协议中对应的子协议相同。

盗版跟踪子协议　如同基本协议中一样,Merchant 发现一个 pirate user,得到一个个人密钥,也就相当于找到一个长为 L 的码字 $word_{found}$,他搜索所有交易记录中的(Set_B, $halfword\_trace_B$),找到一个记录,其 $halfword\_trace_B$ 和 $word_{found}$ 至少有 L/(4 * coll_size)个对应位置上符号是相同的。他取出 $msg_B=(text, com_B)$和 sig_B 准备向仲裁者控告此 Buyer。

仲裁子协议　Merchant 组成的证据为 $proof=(msg_B, sig_B, word_{accuse})$,其中 $word_{accuse}$ 长为 L 的码字,码字中对应 Set_B 中元素的位置上由 $halfword\_trace_B$ 中的对应符号组成,码字中其他位置的符号由 $word_{found}$ 中的对应位置符号组成。

Buyer 提供 $open_B$。

仲裁者首先验证 sig_B 签名的有效性和承诺的有效性(揭示 $word_B$)。

然后验证 $word_{accuse}$ 和 $word_B$ 是否至少在 L/2+L/(16 * coll_size)个对应位置上的符号相同,成立则指控成功,否则 Buyer 即可否认指控。

为了使 $word_B$ 始终对 Merchant 保密,可以用零知识证明来给出 $word_B$。

四、其他主要的指纹协议

上面介绍的两个协议是典型的对称和非对称的数字指纹协议,除了这些以外,对称性的数字指纹协议还有如基于码字(标记)安全的指纹协议[3],与这个协议相对应的非对称协议[4,7,8],以及现在研究比较多的匿名数字指纹协议等[5,9]。其他和这方面研究相关的论文有文[10~20]。下面简单介绍一下这些协议的概念。

(1)基于码字(标记)安全的指纹协议

这种指纹协议主要考虑如何构造一种安全的码字(码字是嵌入在如图像之类的软件产品中的),来防止多人的共谋攻击。其中应用了纠错码的许多方法。协议本身并没有规定码字是如何嵌入产品的,但提出了一个 Marking Assumption 来限制嵌入方法的功能。这个协议可以和比较强的数字水印嵌入算法一同工作来保证产品的安全性。

(2)非对称的基于码字安全的指纹协议

如同非对称的 Traitor-tracing 协议,为了保证 Buyer 的安全性,把非对称的概念也引入了码字安全的指纹协议。其构造类似于非对称的 Traitor-tracing 协议。

(3)匿名指纹协议

这是对指纹协议在非对称以后的一大改进,其目的是保持 Buyer 在进行交易时能不对 Merchant 泄露其真实身份,就如同我们平时在商店购买商品时不需要对售货员出示身份证一样。但是,在发现产品被非法散播时仍需能检测出盗版的 Traitor。匿名指纹协议中引入了一个注册中心的角色(RC),Buyer 使用在注册中心登记的身份而不是其真实身份同 Merchant 进行交易(这里的身份可能就是某种数字签名体系中的公钥),只要 Buyer 是诚实的,Merchant 就不会从指纹协议的过程中知道 Buyer 的身份,否则在有 RC 参与的子协议中进行仲裁。

五、对主要数字指纹协议的分析和展望

从指纹协议的发展来看,早期的对称性的数字指纹协议提出了基本的指纹协议体系结构,奠定了数学基础,是后来所有协议的基石,这些协议研究的重点是使用类似纠错码或其他方法来构造唯一的"指纹",并使用概率论的工具来证明协议的安全性,它们主要关心的安全问题是防止 N 个人的共谋攻击,这类协议中最具有代表性和可行性的就是前面重点介绍的基本 Traitor-tracing 协议,它不依赖其他技术的研究发展情况,协议的提出就是针对广播加密节目问题的,使其应用性非常强。而基于码字安全的指纹协议适应性比较强,它不指定"指纹"嵌入方法,只要满足它所要求的 Marking Assumption,但是如数字水印等相关信息隐藏方法还不能从理论上证明足够的鲁棒性,所以这种指纹协议在应用上会有比较大的障碍。对称性数字指纹协议的缺点,我们总结为这两条,一是考虑的安全因素不够多,仅仅针对共谋攻击,这也是以后非对称协议提出的原因之一;二是随着共谋者 N 的增加,协议

执行需要的数据量会大大增加，系统假设的N不能太大，就这一点来说，如何在保证安全性的条件下降低协议的复杂性是一个重要的研究方向，这很大一部分依赖于纠错码技术的发展。

非对称数字指纹协议的提出使指纹协议的研究迈上了一个新的台阶，只有购买者自己知道"指纹"的内容，避免了因双方都保有"指纹"从而无法仲裁的问题，既保证了盗版者的不可抵赖性，又保证了诚实的购买者不会被不诚实的商家或其工作人员所陷害。由于非对称数字指纹协议使用了安全两方计算等密码学技术，从执行效率来说会很大程度依赖于这些技术的效率，因此选择合适的相关技术方案是非对称指纹协议在应用时需要研究的问题。

而匿名协议则是目前的研究热点，使指纹协议更贴近于现实中的商品交易过程。匿名性已经成为继非对称性之后对数字指纹协议的基本安全要求。由于安全要求的增加，指纹协议使用的密码技术也随之增加，使协议的复杂性更是大大增加，这很不利于实际应用，我们认为如何简化数字指纹协议，提出技术依赖性比较小，执行速度快的匿名协议是使数字指纹协议实用化的一个重要的研究方向。

结论 数字指纹协议为解决电子交易中的盗版问题提出了可行的密码学体系，从各种安全性角度解决了不同的安全问题。数字指纹协议的提出，使数字产品的无形交易过程变得更安全可靠。越来越多的数学密码学工具被用来实现更安全的非对称性和匿名性。数字指纹协议有着广阔的应用前景，从数字图像、数字电影电视节目、数字音乐，到应用程序、数字文档，各种数字产品的交易都可以和数字指纹协议结合起来以保证产品版权的安全性。因此，除了理论的研究，如何将指纹协议结合到各种现实的电子交易应用系统中去也是非常需要解决的问题，毕竟理论研究的目的是为了现实的应用。

参考文献

1 Wagner N R. Fingerprinting; 1983 Symposium on Security and Privacy, IEEE, Oakland, California, 18～22

2 Chor B, Fiat A, Naor M. Tracing Traitors; Crypto '94, LNCS 839, Springer-Verlag, Berlin, 1994. 257～270

3 Boneh D, Shaw J. Collusion-Secure Fingerprinting for Digital Data; Crypto'95, LNCS 963, Springer-Verlag, Berlin, 1995. 452～465

4 Pfitzmann B, Schunter M. Asymmetric Fingerprinting; Eurocrypt'96, LNCS 1070, Springer-Verlag, Berlin, 1996. 84～95

5 Pfitzmann B, Waidner M. Anonymous Fingerprinting; Eurocrypt'97, LNCS1233, Springer-Verlag, Berlin, 1997. 88～102

6 Naor M, Pinkas B. Threshold Traitor Tracing; Crypto'98, LNCS 1462, Springer-Verlag, Berlin, 1998. 502～517

7 Pfitzmann B, Waidner M. Asymmetric Fingerprinting for Larger Collusions; accepted for 4th ACM Conference on Computer and Communications Security, 1997

8 Biehl I, Meyer B. Protocols for Collusion-Secure Asymmetric Fingerprint-ing; STACS 97, LNCS 1200, Springer-Verlag, Berlin, 1997. 399～412

9 Domingo-Ferrer J. Anonymous Fingerprinting of Electronic Information with Automatic Identification of Redistributors; Electronics Letters 34/13, 1998. 1303～1304

10 Blakley G R, Meadows C, Purdy G B. Fingerprinting Long Forgiving Messages; Crypto'85, LNCS 218, Springer-Verlag, Berlin, 1986. 180～189

11 Garonni G. Assuring Ownership Rights for Digital Images. In: Proc. VIS '95; Vieweg, Wiesbaden, 1995. 251～263

12 Canetti R. Studies in secure multiparty computation and applications: [Ph. D. dissertation]. MIT, 1999

13 Cox I J, Kilian J, Leighton T, et al. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 1997, 6(12): 1673～1687

14 Fiat A, Naor M. Broadcast Encryption; Crypto'93, LNCS 773, Springer-Verlag, Berlin, 1994. 480～491

15 Lai X, Massey J. Hash functions based on block ciphers, Eurocrypt'92, Springer-Veralg, 1992. 55～70

16 Ostrovsky R. An efficient software protection scheme; Crypto '89, LNCS 435, Springer-Verlag, Heidelberg, 1990. 610～611

17 Petitlas F A P, Anderson R J, Kuhn M G. Information hiding-A survey. Proc. of the IEEE, 1999, 87(7): 1062～1078

18 Roe M. Performance of block ciphers and hash functions-one year later, FSE'94. In: Proc. of Second Intl. Workshop on Fast Software Encryption, Springer-Verlag, 1994. 359～362

19 Salvail L. Quantum bit commitment from a physical assumption, Crypto'98, Springe-Veralg, Berlin, 1998. 338～353

20 Yao A C. Protocols for secure computations, 23rd STOC. In: Proc. of the IEEE 23rd Annual Symposium on the Foundation of Computer Science, 1982. 160～164

（上接第159页）

参考文献

1 叶俊勇，汪同庆，杨波，等. 皮鞋内腔CT测量仪的扫描运动控制系统. 重庆大学学报，2001，24(6)：108～112

2 程正兴. 小波分析算法与应用. 西安交通大学出版社，1998. 31～40

3 Mallat S. A theory for multiresolution signal decomposition: the wavelet representation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1989, 11(7): 674～693

4 Mallat S. Multifrequency channel decompositions of images and wavelet models. IEEE transactions on Acoustic. Speech and Signal Processing, 1989, 37(12): 2091～2110

5 Mandelbrot B B. The Fractal Geometry of Nature. New York: Freeman, 1983

6 Pentland A P. Fractal-Based Description of Nature Scenes. IEEE Trans. Pattern Anal. Mach. Intell., 1984, 6 (6): 661～674

7 Peleg S, Naor J, Hartley R, Avnir D. Multiple Resolution Texture Analysis and Classification. IEEE Trans. Pattern Anal. Mach. Intell., 1984, 6 (4): 518～523

8 Keller J M, Chen S, Keller J M. Texture Description and Segmentation Through Fractal Geometry. Computer Vision Graphics Image Processing, 1989, 45: 150～166

9 Sarkar N, Chaudhuri B B. An Efficient Approach to Estimate Fractal Dimension of Textural Images. Pattern Recognition, 1992, 25(9): 1035～1041

10 Jin X C, et al. A Practical Method for Estimating Fractal Dimension. Pattern Recognition Letters, 1995, 16: 457～464

11 应字铮，石青云. 实数域上的盒数计算与分形维数估计. 模式识别与人工智能，1997，10(4)：357～361