先 为防止多个购买者合谋伪造一个忠实购买者的指纹从而对其陷害 必须保证叛逆者识别协议不能跟踪到忠诚购买者 即使出现跟踪错误 在审判阶段应能够纠正错误 在扩频指纹中 由于指纹序列彼此独立、正交 在没有忠诚者指纹信息情况下 通常进行伪造的概率 虚警概率 要比去除指纹概率 漏警概率 小得多 即便合谋者能够以一定概率伪造指纹 : 由于指纹. : 与 : 无关 能够伪造. : 的概率将更小 因此只要指纹码字随机强且足够长 容忍性大 即便多于合谋尺寸 多个购买者合谋陷害的概率仍是可忽略的

如果发行商 E 对购买者 : 进行陷害 或者 E 知道 : 的密钥 18: 或者能够伪造出 : 拷贝 I :″中的指纹 显然如果密码系统是安全的 那么只有 : 知道自己的密钥 E 是无法解密出 / 颁发的指纹 如果 E 要伪造指纹 虽然指纹 : 是可以任意伪造的 但是伪造. : 必须保证它能够与 / 和 : 共同生成的. : 之间的相关检测大于阈值 * 由于 E 只有. : 的加密指纹序列 : . :′ 根据密码系统的安全性 E 不可能猜测出指纹信息 即使根据同态性质进行指纹的相关检测 也无法得到相关检测结果 从而保证忠实购买者的安全 此外 发行商和某个购买者合谋可以获得指纹序列 但无法对 / 已经存储的购买者签名 1+). : 进行伪造和修改 由于 / 对每个购买者分配的指纹是唯一性、不可重复的 发行商无法再次使用指纹 也不能用它对其他购买者进行陷害

, V Ž ª Ÿ

要实现购买者的不可否认性 就要求在购买者拷贝中必须含有只有该购买者才能提供的秘密信息 而发行商只有发现盗版拷贝时才能获得这些信息并将其作为法律证据 在所提出的协议中 每个参与方分别持有部分秘密! 购买者 : 具有保密字符串 1*5+): 及其杂凑值 * ?* 并用 * ?* 修改证据指纹. : 指纹中心 / 具有原始指纹. : 发行商 E 具有秘密置换 4 及身份指纹 : 从而保证单独一方不能伪造嵌入指纹及其相关证据 假设发行商 E 发现了一个非法拷贝 I 并从指纹 : 中成功跟踪到购买者 : 以及提取到指纹. : 如果仲裁人 能证明 / 记录的原始指纹. : 与. : 的相似性 根据购买者不可陷害性质 : 的唯一性指纹是几乎无法由其他人 发行商或多个叛逆者合谋 生成的 因此可判定 : 是有罪的 同时 由于指纹. :′ 含有 : 的秘密信息 * ?* / 和 E 所保留的签名 1+). : 1+). / 和 1+). E 也在密码安全上保证了. : 的完整性和有效性 此外 : 可以为自己辩护 通过公开自己的秘密 1*5+): 可以重建所有数据 并与 : 的真实拷贝进行对比 排除其他协议参与者作弊的可能

, V Ë © Ÿ # a ‹ Ÿ

不可感知性是为保证多媒体作品质量和价值而提出的特殊要求 在本文提出的方案中 发行商 E 依照 视觉或听觉 感知掩蔽模型计算出感知权重 再根据式中加法同态性质 将指纹按照感知权重进行放缩 从而实现指纹感知嵌入 感知嵌入不仅提高作品质量 而且可以提高指纹跟踪检测概率和鲁棒性 同时权重缩放改变了指纹取值和分布 使得指纹安全性被增强

不用于传统方案由购买者预先申请指纹 所提出方案的扩频指纹序列是在协议执行中申请的 发行商 E 可以根据多媒体作品的实际情况 如指纹长度 要求指纹中心 / 按照参数 4' 5 3 1 构造指纹序列 提高了指纹在应用中的适应性

Œ , ‘

根据不可陷害性的分析 发行商 E 或者多个购买者合谋都无法进行欺骗 假设指纹中心 / 的忠实性 审判协议在没有购买者 : 参与情况下 E 从非法拷贝提取的指纹信息. : 与 / 提供的原指纹信息. : 进行相关检测获得的结果足以完成对购买者的审判 与其他协议需要购买者 : 直接或间接提供指纹相比 如果 : 将指纹及其相关信息遗忘 将无法进行相关检测 整个审判也将无法进行 同时 协议允许购买者向仲裁者 提供自己的秘密信息 对整个购买过程进行检查 防止不忠诚现象发生

9 ²

本文在扩频指纹编码基础上 根据扩频指纹特点和安全性要求 提出了一种定点小数表示方法并结合加法同态密码系统 给出了一种对购买者透明的非对称指纹方案 实现了透明购买、不可感知、缺席审判等特性 与其他指纹方案相比较 所提出的算法更具实用性和安全性 本文为实现公平电子交易以及数字指纹提供了一条新思路 对知识产权保护及其他相关领域在理论和实践上都具有一定的现实意义

• I Ó D!

B C" "' + + 5 " < +6 8 - 65- 4* 1- 1* 3 1 <' 1 7 6 3 4 1+* 7)5 5 1+7 1*- 6 ' 11 1B C "5 6 7+)1 2 5 65- 4*A B C "5) ! 45+) 5 5') "5 11 M

B C: "2*D3 ' . . ' +7 5 - 3 12+) 545+ *+) B C "5 6 7+)1 2 5 65- 4*′ B C : 5+ $ +7 < 5)! 45+) 5 5') "5 11 M

B C : +, : E - 5 "5 * 6 12 5 6 1+ 1 6 5 ' 1- 3 3 * 5-6 2+) 545+ *+) ?* 7 7 <1*5' 6* B C "5 6 7+)1 2*, *, ' -3 4 1+ 3 , 5 *-6' 14 6*1 2 3 4 * 5 6+ 6 B C $' 1 1*' 7* < 68! 45+) 5 5 ') "5 11 M

B C E 3 " . .) < - 5 1 5 @* 53 ' 5B+) 45 * 6 B C 5 1 6*+ 1 3 ') "5 6 11+) ! M

B C$ $ = -8 0 $ -8 ' -3 1< - 5

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

1　5 @ * 53 ' 5B +)　45 * 6　@ #, '　-3 #- 6　*5 B C "5 6　7+)1　2　*,　* 5 ' *+　'　25　6 2 53 ' *+　6 5 #- '　7　5-4*　) - B C　! 45+) 5 5') "5 11　M

B C　= ++ '　/　+), *　E ' *, 1　(　, '3 '　5 ;'　/　#'　1+1 *'　6　2 7 +) #'　@ * 53 ' 581 * 6　1+9 ' *' 681B C　6, +6'　4 5*　"5+ 6 *　% +9 51 #- "5+ 6 *

B C / 5)　= ++　= 3 ' 5　*　*, -8 #1 26　1+ 5 1+1 *'　* @ * 53 ' 581B C "5 6　7+)1　2　5 65-4* A B C "5)　! 45+) 5　5') "5 11　M

B C & '　#,　0　))　/　) .　+#　1+　1 6 5　6 9　*+　'　145 ' 7 14　6*5 3　2+)　545+ *+) B C "5 6　7 +)1　2　*,　* 5 ' *+　'　.　581, 4　0 +) #'　. ' * 5 3 ' 58+)　. 0 .　B C　+ '!　45+) 5　5') "5 11　M

B C = '8 5' +　'8') +　@1 3 ' *-6'　- 1 6 5　4 < +6 8 - 65-4* 1- 1* 3 1 25 3　*,　45+3 #+9 B C "5 6　7+)1　2

*,　* 5 ' *+　'　.　581, 4　"5 6*-6　' 7　,　5- + " < -6 = -　5-4* 1- 1* 3 1B C "' 5+1!　45+) 5　5') "5 11　M

T € e º !

ë　û　男　　年生 黑龙江大庆人 于　年与　　年分别获哈尔滨工程大学硕士学位与博士学位 主要研究方向为信息安全、计算复杂性理论、密码学、数字指纹和模式识别等 3 ' + ! 3 ' 5*+ D, R 3 1　6 3

¥ B　男 生于　　年　月　　年毕业于北京大学无线电电子学系计算技术专业　　年至　　年在 西安 中国航空计算技术研究所从事科研工作 于　　年赴英国 5' 2+ 7 1*# * 2　6,　) - 电子工程系进修学习两年 现任哈尔滨工程大学教授 博士生导师 现主要从事计算机网络及应用 分布式计算机系统、网络与信息安全等

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net