构造高性能的指纹密钥提取器

李西明 杨 波
(华南农业大学信息学院 广州 510640)

摘 要 提出了一种快速评价指纹图像质量的方法,并把这种方法应用到了密钥提取器的构造中,构建了基本的和改进的基于指纹的密钥提取器方案。该质量评价方法测量指纹图像在不同频率区域上的能量集中度,以图像频谱图中心环上能量较高的点的个数来表示指纹图像质量指标。在中国科学院自动化研究所的URU4000B数据库和FVC2004 DB3数据库上,进行了指纹密钥提取器的实验,测试了基本指纹密钥提取器和改进指纹密钥提取器的性能。结果显示,改进密钥提取器的密钥恢复成功率有显著提高。如在URU4000B数据库中,当不同手指图像密钥恢复失败率同为99.8%时,基本密钥提取器的同一手指图像密钥恢复成功率为43.7%,改进提取器的同一手指图像密钥恢复成功率为46.3%。

关键词 指纹密钥提取器,图像质量,密钥恢复成功率
中图法分类号 TP301 **文献标识码** A

Construction of Fingerprint Key Extraction with High Performance

LI Xi-ming YANG bo
(College of Informatics, South China Agriculture University, Guangzhou 510640, China)

Abstract In this paper, a kind of method which can evaluate fingerprint picture quality was proposed and used in the construction of basic and improved fingerprint key extraction scheme. The method measures the concentration ratio of energy in spectrum picture and the quality of fingerprint picture is denoted by the sum of all the points which have high energy. Key extraction experiment was done on the URU4000B database of Institute of Automation of Academia Sinica and FVC2004 DB3, performance of basic key extraction scheme and improved key extraction scheme were tested. The result shows that the improved scheme is better in key extraction success rate. For example, in URU4000B, when the key extraction failure rate of two pictures from two fingers is 99.8%, in the basic key extraction scheme the key extraction success rate of the same finger is 43.7%, in the improved key extraction scheme the key extraction success rate of the same finger is 46.3%.

Keywords Fingerprint key extraction, Image quality, Key recover success rate

1 引言

模糊提取器概念由Dodis在文献[1]中第一次提出,并在文献[2]中进行了更详细的说明,它是一个与随机提取器紧密相关但又有较大区别的概念。随机提取器研究的重点是怎样从已知的分布中提取出足够多的随机性,也就是提取出尽可能多的随机位,而模糊提取器不仅要从已知的低熵的数据中提取出尽可能多的随机位,而且还要在输入相近数据和帮助串的情况下输出完全相同的随机数。

模糊提取器概念的提出为从低熵秘密中获得高熵的密钥提供了一个好的方法,开拓了密码学理论研究的一个新方向。在隐私保护、身份认证、密钥协商、秘密共享等方面,模糊提取器具有广泛的应用前景。

模糊提取器具有重要的理论和应用价值,虽然已有多篇文献在汉明距离空间、集合差空间和编辑空间上做了大量的理论研究工作,但与实际问题相结合的实现方案以及讨论其实际的应用性和安全性的文献还比较少。安全概略实现的困难性主要在于两个方面:1)理论上的安全概略构造是架构在理想的距离空间上的,而实际问题中的模糊数据并非与理想情况完全符合;2)理论上的研究总是认为纠错码的纠错能力是理想的,实际上纠错码的选用要考虑多方面的问题,很难使用理论上最优的纠错码。

把指纹作为用户的认证信息已有很长时间的研究历史了[3-5],但是直接从指纹中提取密钥则少有研究。本文把指纹数据引入到模糊提取器中,提出了指纹密钥提取器的概念。指纹密钥提取器可以概括为两个算法:密钥生成算法KeyGen和密钥恢复算法KeyRec。KeyGen接受输入的指纹图像FP和一个随机数i,提取出具有一定长度的帮助串P和一个密

到稿日期:2010-04-16 返修日期:2010-07-17 本文受国家自然科学基金(60773175,60973134),现代通信国家重点实验室基金(9140C1108020906),广东省自然科学基金(9151064201000058),华南农业大学创新基金(6100-k09156)资助。
李西明(1974-),男,博士生,主要研究方向为生物特征密码学,E-mail:liximing@scau.edu.cn;杨 波(1963-),男,教授,博士生导师,主要研究方向为信息安全。

钥 k。如果指纹图像 FP 和图像 FP′取自同一手指，算法 KeyRec 则可以在接受输入 FP′，i 和帮助串 P 的情况下，以很高的概率恢复出密钥 k。

本文第 2 节提出了一种简单快速的指纹图像质量评价方法，介绍了其实现原理；第 3 节研究了基于指纹模板的指纹密钥提取器系统的实现方案，具体讨论了模板提取、量化及指纹密钥提取器构造问题；第 4 节是仿真实验，结果表明，同基本的构造方法相比，本文的构造方法的性能显著提高。

2 指纹质量评价

指纹密钥提取器需要比较清晰的指纹图像。由于手指汗渍、褪皮、干湿、伤疤、压力等不良因素的影响，加上采集设备的技术性能不完善性等原因，往往通过一次采集难以得到清晰的指纹图像，因此在采集图像时要对采集到的图像进行评估，根据图像质量来设计系统，以提高指纹密钥提取器的性能。

文献[6]中所提供的各种质量评价方法或者只是从指纹图像局部纹理进行分析，不足以反映指纹图像全局信息，或者比较复杂，对计算能力要求比较高，不适合应用在设备计算能力比较低的场合。本文在已有的指纹图像质量评价理论的基础上，综合考虑决定指纹图像质量的各种因素，提出了一种简单快速的指纹图像质量评价方法。

根本上来看，无论是采用哪一种模板提取方法，都是要表达指纹图像的某一种特定纹理特征。纹理是以相似的模式或空间排列的点，它们具有一定的统计或结构特征和灰度变化规律。指纹就是一种独特的纹理图像，一般来说，图像中灰度分布具有某种周期性，即使灰度变化是随机的，它也具有一定的统计特征，从全局上看属于非平稳信号，从局部上看，又具有明显的方向一致性和频率稳定性。

指纹质量通常定义为纹理结构的可提取性，也就是通过其提取模板的可靠性来评价指纹质量。这样的方法不免会受到特定特征提取算法的影响，没有普遍性。直观上来看，指纹质量好的图像，纹路更加清晰，指纹质量差的图像，纹路比较不清晰，甚至有很多不连续而且模糊的地方，本文从此点出发来讨论图像的质量问题。

对两个不同质量的指纹图像做离散付立叶变换，可以得到两个指纹图像的频率谱，把这个频率谱所对应的能量谱以图示的方式表达出来，如图 1 所示。图 1(a)－(b)是指纹图像，相对应的功率谱是图 1(c)－(d)。由图 1 可见，指纹图像能量在频谱靠近中心的环形区域更加集中，而且，因为指纹纹路清晰度的不同，质量较好的图像有清晰的中心环，在中心环上的能量集中度高，质量较差图像的功率谱比较分散，在中心环上的能量集中度低。

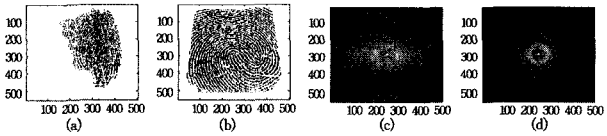

图 1　不同质量指纹的频率特征

总体上来看，指纹的清晰度会反映到能量谱上，而中心环的大小是由指纹自身的背线间距决定的，与指纹质量及类型无关。虽然不同类型的指纹图像的能量谱都集中在中心环上，但其表现略有不同，环形指纹在中心环上的能量分布更均匀，弓形指纹的能量集中在中心环上相对小的一些区域。

针对指纹图像能量谱分布的这种情况，可以设计一种简单快速的指纹质量评价方法。由于指纹频谱能量集中度的差异代表了指纹质量的好坏，因此可以通过计算指纹图像中心环上能量的集中度来衡量指纹图像的好坏。能量的集中度可以用多种方法来评价，可以用中心环上所有能量与全部能量之比来代表，也可以用图像频率谱上能量超过一定阈值的点的个数来代表。经过实验分析，本文采用计算中心环上超过特定阈值点的个数来衡量指纹质量的好坏。图 2(a)(b)是图 1(a)(b)中对应两指纹能量谱中超过阈值的点在中心环上的分布情况。

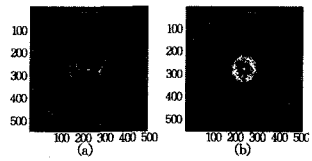

图 2　指纹频谱图像高能量点数目及分布

3 指纹密钥提取器构造

3.1 指纹模板提取和量化

若要从指纹中提取出密钥，首先要把指纹图像变成可以反映指纹特征的指纹特征向量。Anil K Jain 等在文献[7]中提出了基于 Gabor 滤波器的指纹模板提取算法，本文的指纹特征向量算法采用了基于 Gabor 滤波器算法的一个改进算法。算法首先确定出指纹的中心点，以中心点为圆心画出 6 个等间距的同心圆，5 个同心圆环中的每个环各方面划分成 16 个等弧度的扇区，总共划分成 80 个扇区，然后在 8 个等分方向上对图像进行滤波，最后求每个小扇区上的绝对方差，因此共得到 80 * 8 个值，此向量称为 FingerCode。指纹图像的相似度就是用 FingerCode 的几何距来衡量的。

因为不具有旋转不变性，在进行 FingerCode 的比对之前应该进行校准，使得两个指纹的方向一致，否则所获比对效果较差。为了不引入新的帮助量，可以使用变通的方法来对模板进行校准，即第一指纹不动，把第二指纹以中心点为圆心，等角度顺序旋转 16 次，每旋转一次求一次几何距，取最小几何距作为两个指纹图像的向量距。

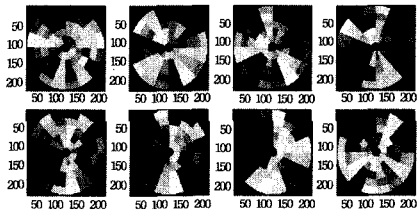

图 3　指纹(b)的 FingerCode 图像

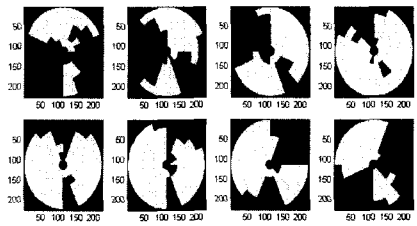

图 4　指纹(b)的 FingerCode 量化图像

为了把 FingerCode 指纹模板应用到密钥提取算法中，需

要把特征向量用整数表示，也就是说要把 640 个实数值量化成 640 个整数。本文选用了 1 位的量化方案，因此，有 640 个实数值的 FingerCode 变成了一个 640 位的向量。图 1(b)对应指纹图像的 FingerCode 图和相应的量化图如图 3 和图 4 所示。

3.2 指纹密钥提取器

由于 BCH 码可以纠正多位随机错误，实用性强，运行速度快，本文使用 BCH 码来构造指纹密钥提取器。不考虑指纹图像质量的密钥提取算法称为基本的指纹密钥提取算法，考虑了指纹质量的算法称为改进的指纹密钥提取算法。结合 BCH 码的特点以及特征向量的实际情况，在方案中使用的 BCH 码的码长是 1023 个比特位，编码维数则选择了多个。

设 BCH-encode(x)是 BCH 编码函数，BCH-decode(c,d)是解码函数，可以把码 d 解码为 c，并返回标志是否成功的位。设求指纹图像质量的函数为本文所提算法，标记为 Quality()，求指纹模板的函数为 Model()，指纹图像质量门限值为 TH，改进的指纹密钥提取器算法〈KeyGen，KeyRec〉描述如图 5 和图 6 所示。

```
生成算法 KeyGen(i,FP):    Q= Quality(FP)
    IF Q<TH
      返回失败
    END
    F= Model(FP)
    P = Φ
    生成随机数 x
    c = BCH-encode(x)
    P = c ⊕ F
    k=i ⊕ F
    返回 P,i,k
```

图 5 改进的指纹密钥提取器密钥提取算法 KeyGen

```
恢复算法 KeyRec(I,P,FP′):
    Q= Quality(FP′)
    IF Q<TH
        返回失败
    END
    F′= Model(FP′)
    F* = Φ
    c′= P ⊕ F′
    IF BCH−decode(c* ,c′)失败
    返回失败
    END
    F* = c* ⊕ P
    k* = F* ⊕ i
    返回 k*
```

图 6 改进的指纹密钥提取器密钥恢复算法 KeyRec

密钥生成算法首先计算指纹图像的质量，如果质量低于指定门限就放弃求密钥的操作。如果指纹质量高于指定门限，就求指纹的特征向量 F，然后生成一个随机数 x，用 BCH 码对随机数进行编码 c，再与 F 异或得到辅助向量 P，F 与输入的随机值 i 异或得到输出的密钥 k。密钥 k 是 640 位长的比特串。

密钥恢复算法首先计算指纹图像的质量，如果质量低于指定门限就放弃密钥恢复操作。然后求指纹的特征向量 F'，计算辅助向量 P 和 F'的异或值求得 c'，然后解码 c'，如果成功则得到 $c*$，再求 $c*$ 和 P 的异或值就得到了 $F*$，$F*$ 与 i 的异或值就是 $k*$。

密钥提取实现过程的计算原理与计算指纹的比对有些相似，但是也有不同。在指纹图像比对过程中，可以在 16 个方向上求指纹图像比对，并取最小的比对值作为两图像的差值，但是在安全概略的恢复算法中，只能在一个方向上对指纹图像恢复，没有办法取 16 个方向上最小的汉明距。为了提高算法的性能，在实际的安全概略恢复算法中，也在 16 个方向上旋转指纹并做解码，如果在某一个方向可以解码，并求得密钥，则取在此向量下计算得到的密钥为输出密钥。

指纹密钥提取器是一种概率算法，不能保证一定可以或者一定不可以解出正确的密钥。它能以很大的概率保证，如果用于生成和恢复的算法指纹来自同一手指，那么得到同一密钥，定义这个概率为一致指纹成功率 GSR(genuine success rate)；反之，它能以很大的概率保证，如果用于生成和恢复的算法的指纹不是来自同一手指，那么得不到同一密钥，定义这个概率为不一致指纹失败率 IFR(imitate failure rate)。GSR 和 IFR 构成指纹密钥提取算法的两个评价指标。

4 实验结果

在中国科学院自动化研究所的 URU4000B 数据库和 FVC2004 DB1 数据库上，分别进行了指纹密钥提取器的实验，测试了基本指纹密钥提取器和改进指纹密钥提取器的性能。URU4000B 数据库是用光学按压式采集仪 UrU 4000B 采集的，每个图像的大小是 500 * 550 像素，图像质量较好。此数据库共包含有 720 个手指的 8640 个图像，每个手指取了 12 次。FVC2004 DB3 数据库包含 100 个手指的 800 个图像，由温度传感器采集，每个图像的大小是 300 * 480 像素。

为了比较密钥提取算法性能，在两个数据库上进行了密钥提取与恢复的实验。由于在算法中使用了 BCH 码，密钥的提取和恢复受到 BCH 码本身纠错能力的影响，因此在多个纠错能力下进行了测试。

在数据库一定、纠错能力一定的情况下，GSR 和 IFR 的计算方法如下：用数据库中的一个指纹图像产生一个密钥，然后用同一手指的另一指纹图像去解密钥，成功求得相同密钥的概率即为 GSR；用数据库中的每一指纹图像产生一个密钥，然后用不同手指的一个指纹图像去解密钥，不能成功求得相同密钥的概率即为 IFR。

FVC2004 DB1 数据库中指纹较少，可以对每一枚指纹计算解密钥的成功率和失败率。URU4000B 数据库中指纹比较多，对每一枚指纹求成功率和失败率，花费的时间相当长。本文使用确定的算法来计算 URU4000B 数据库上的 GSR，而使用随机算法来求 IFR。对于基本指纹密钥提取器，在编码维数分别为 463，503，588，618，688，而纠错能力分别为 62，58，47，44，36 的情况下，FVC2004 DB1 和 URU4000B 数据库上的 GSR 和 IFR 情况如表 1 所列。

对于改进的指纹密钥提取器，选择图像质量门限值为 0.2，在编码维数分别为 463，503，588，618，688，而纠错能力分别为 62，58，47，44，36 的情况下，FVC2004 DB3 和 URU 4000B数据库上的 GSR 和 IFR 情况如表 2 所列。

表 1　不同编码数下基本密钥提取器 GSR 和 IFR 情况

编码维数	463	503	588	618	688
FVC2004 GSR	2.04e−1	1.74e−1	1.01e−1	8.79e−2	3.75e−2
FVC2004 IFR	9.76e−1	9.81e−1	9.92e−1	9.93e−1	9.97e−1
URU4000B GSR	5.90e−1	5.62e−1	4.57e−1	4.37e−1	3.41e−1
URU4000B IFR	9.85e−1	9.89e−1	9.97e−1	9.98e−1	9.99e−1

表 2　不同编码数下改进的密钥提取器 GSR 和 IFR 情况

编码维数	463	503	588	618	688
FVC2004 GSR	2.31e−1	1.99e−1	1.18e−1	1.04e−1	4.79e−2
FVC2004 IFR	9.80e−1	9.83e−1	9.93e−1	9.94e−1	9.97e−1
URU4000B GSR	6.14e−1	5.86e−1	4.83e−1	4.63e−1	3.65e−1
URU4000B IFR	9.86e−1	9.90e−1	9.97e−1	9.98e−1	9.99e−1

综合表 1 和表 2 的情况来看，考虑了质量因素后，指纹密钥提取器的性能提高了，同样编码维数情况下，一致指纹的解码成功率提高了，不一致指纹的解码错误也提高了。同时，从两个表中两个数据库的相关参数比较也可以看出，中科院 URU4000B 数据库指纹质量要好于 FVC2004。在编码维数逐渐提高的情况下，GSR 逐渐提高，IFR 也提高了，这主要是因为，编码维数低时，纠错能力提高了。

结束语　密钥管理是信息安全实践中的一个重要课题。本文融合了一种快速评价指纹图像质量的方法，构建了高性能的基于指纹的密钥提取器方案，从用户指纹中提取出了恒定值用作密码学中的密钥。

中国科学院自动化研究所的 URU4000B 数据库和 FVC2004 DB3 数据库是两个公开的指纹数据库，在其上进行了指纹密钥提取器的实验，测试了基本指纹密钥提取器和改进指纹密钥提取器的性能。给出了两种数据库上五种编码维数下的一致指纹密钥恢复成功率和不一致指纹密钥恢复失败率，说明了指纹提取器的有效性，也说明了融合指纹质量考量的密钥提取器性能更好，实用性更强。

虽然本文在指纹密钥的应用方面做了大量工作，但是，在不采用其他手段的情况下，单独使用密钥提取器作为唯一的安全措施乃是不安全的。最主要的问题在于，目前还不能实现使得 GSR 很高、而 1-IFR 小到几乎可以忽略的密钥提取算法。目前，如果要把指纹密钥提取器应用于信息安全实践中，须与其他的安全措施相配合，比如加入口令等。

参 考 文 献

[1] Dodis Y, Reyzin L, Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data[C]// Cachin C, Camenisch J, eds. 23rd Annual Eurocrypt Conference. Interlaken, SWITZERLAND. 2004: 523-540

[2] Dodis Y, Ostrovsky R, Reyzin L. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data[J]. Siam Journal on Computing, 2008, 38(1): 97-139

[3] Girgis M R, Sewisy A A, Mansour R F. A robust method for partial deformed fingerprints verification using genetic algorithm [J]. Expert Systems with Applications, 2009, 36(2): 2008-2016

[4] Hulea M, Astilean A, Letia T, et al. Fingerprint recognition distributed system[C]// 2008 IEEE International Conference on Automation, Quality and Testing, Robotics (Aqtr 2008). 2008: 423-428

[5] Marcialis G L, Roli F, Didaci L. Personal identity verification by serial fusion of fingerprint and face matchers[J]. Pattern Recognition, 2009, 42(11): 2807-2817

[6] Alonso-Fernandez F, Fierrez J, Qrtega-Garcia J, et al. A comparative study of fingerprint image-quality estimation methods[J]. IEEE Transactions on Information Forensics and Security, 2007, 2(4): 734-743

[7] Jain A K, Prabhakar S, Hong L, et al. Filterbank-based fingerprint matching[J]. IEEE Transactions on Image Processing, 2000, 9(5): 846-859

(上接第 72 页)

为明显的改进；当网络负载较轻时，多步信道预约的改进程度有所下降，但仍然能够比单步预约提供更为稳定的数据传输；

b)3 步预约与 2 步预约相比，网络性能较为接近；

c)在密度较大的网络拓扑下，多步预约对单步预约的实时业务传输性能的改进更为明显，在单步预约误帧率保持在较高的水平上时，多步预约可以降低 50%左右的误帧率。

引入多步信道预约机制的无线网络 MAC 协议可以使网络性能有较大的改进。当预约步数增加时，网络性能趋于收敛，预约步数过大会增加额外的运算负担与算法复杂度，因此 3 步预约是较为理想的预约步数，没有必要无限增加预约步数。在该机制中，实时业务相比于非实时业务有较高的优先级，但是实时分组的产生周期较长，所占用的网络开销也较小，因此非实时业务的性能并不会受到较大的影响。

结束语　现有的无线网络协议一般难以对实时分组传输提供 QoS 支持。本文提出的基于多步信道预约的多址接入协议可以对实时数据分组提供较好的 QoS 支持，在原有信道预约协议的基础上提高了实时分组的预约稳定性，从而使网络性能得到较为明显的改善，在实际应用中，可以与 H. 263，H. 264 等视频编解码标准以及 MPEG 等音频编解码标准相结合使用。

参 考 文 献

[1] IEEE. Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specification[S]. IEEE 802. 11-1999

[2] Zhou Ying, Ananda A L, Jacob L. A QoS enabled mac protocol for multi-hop ad hoc wireless networks[C]// Performance, Computing, and Communications Conference, 2003. Conference Proceedings of the 2003 IEEE International. April 2003: 149-156

[3] Li Bo, Tang Wen-zhao, Zhou Hu, et al. m-DIBCR: MAC Protocol with Multiple-Step Distributed In-Band Channel Reservation [J]. IEEE Communications Letters, 2008, 12(1): 23-25

[4] Benveniste M, Ghesson G, Hoeben M, et al. EDCF proposed draft text [S]. IEEE working document 802. 11-01/13 1rl, March 2001

[5] Bo Li, Wei Li, Valois F, et al. Performance Analysis of an Efficient MAC Protocol with Multiple-Step Distributed In-Band Channel Reservation[J]. IEEE Transaction Vehicular Technology, 2010, 59(1): 368-382

[6] 刘军，李喆，岳磊. IEEE802. 11 自组织网络仿真平台的设计与实现[J]. 计算机科学，2008，35(1)：24-26