ISSN 1000-1239/CN 11-1777/TP
50(3): 532-539, 2013

一种新的基于指纹的密钥隐藏方案

李西明[1] 杨 波[2] 郭玉彬[1] 姚金涛[1]
[1](华南农业大学信息学院 广州 510640)
[2](陕西师范大学计算机科学学院 西安 710062)
(liximing@scau.edu.cn)

A New Key Hiding Scheme Based on Fingerprint

Li Ximing[1], Yang Bo[2], Guo Yubin[1], and Yao Jintao[1]
[1](*College of Informatics, South China Agricultural University, Guangzhou* 510640)
[2](*School of Computer Science, Shanxi Normal University, Xi'an* 710062)

Abstract In view of shortage of the existing fingerprint-based key hiding method, a new key hiding scheme based on fingerprint is proposed, which fully uses the information of minutiae set and the texture information around every minutia, depending on a new fingerprint model: minutiae texture strings model. The scheme is called minutiae texture strings key hiding scheme. In this scheme, minutiae set is extracted from fingerprint firstly, and Gabor filter is then used to the area around every minutia to extract texture information. Minutiae set and texture information around every minutia construct the minutiae texture strings model. Secret key generated by a symmetric encryption system or distributed by PKI is divided into n shares by a (n, k) secret sharing algorithm, which are then hidden by minutiae texture strings secretly. Query fingerprint can only recover the hidden key when at least k shares of key are retrieved. Experiments are made on FVC2002 DB1 and DB2, in which one fingerprint is used to hide key and another fingerprint is used to recover the key. Equal error rate (EER) of the scheme is no more than 1%~2.2%, which is better than that of normal fuzzy vault. Security analysis of the scheme shows that information of the key and the fingerprint model is protected effectively, with security higher than that of normal fuzzy vault schemes.

Key words fingerprint; key hiding; fuzzy vault; minutia; secret sharing

摘 要 针对已有指纹密钥隐藏方法的不足,提出了一种新的基于指纹的密钥隐藏方案,为了充分利用指纹图像细节点以及细节点周围的纹理信息,采用了一种新定义的指纹模板:细节点纹理串模板,这种密钥隐藏方案也就称为细节点纹理串密钥隐藏方案.在此方案中,首先提取指纹的细节点集合,然后在每个细节点周围使用 Gabor 滤波器滤波,以提取细节点周围的指纹纹理信息,细节点集合和每个细节点对应的纹理信息共同构成细节点纹理串模板.然后,用(n,k)秘密分割方法将对称加密系统或 PKI 产生的密钥分成 n 份秘密值,每份秘密值以保密的方式存储在细节点对应的纹理串中,只有当询问指纹能恢复出至少 k 份秘密时,才可以恢复出原密钥.在指纹数据库 FVC2002 DB1 和 DB2 上的实验表明,一指纹用于隐藏密钥,另一指纹用于恢复密钥的情况下,该方案的等错率(equal error rate, EER)为 1%~2.2%,优于模糊盖子密钥隐藏方案.安全性分析表明,该方案有效地保护了密钥以及指纹模板信息,安全度高于模糊盖子方案.

收稿日期:2011-04-02;**修回日期**:2011-11-23
基金项目:国家自然科学基金项目(61103232,61272402);广东省自然科学基金项目(10351806001000000,10151064201000028);广东省科技计划基金项目(2010B010600046,2011B090400325)
通信作者:杨 波(byang@scnu.edu.cn)

关键词 指纹;密钥隐藏;模糊盖子;细节点;秘密共享

中图法分类号 TP309

把指纹应用到信息安全领域的实践中有多种方式,如果把系统给出的密钥和指纹模板结合起来,密钥以保密的方式与指纹模板一起存储在系统中,则构成密钥隐藏方案[1-6]. 当用户需要访问秘密信息时,系统提取用户的生物特征,用来恢复与指纹结合的密钥,如果可以恢复出正确的密钥,则用户可以访问相应的秘密信息. 基于指纹的密钥隐藏方案中,密钥与指纹结合形成所谓的辅助数据(help data),按辅助数据与指纹结合的方式不同,又可分为密钥释放方案(key release)、模糊承诺(fuzy commitment)方案和模糊盖子(fuzzy vault)方案 3 种[7].

密钥释放的方法就是把密钥和指纹叠加在一起,存储为加密的指纹模板,而在模板内部,并不对密钥和指纹作任何复杂的操作,只是简单地叠加. Juels 和 Wattenberg 在文献[8]中提出了一种将纠错码技术与生物特征结合在一起密钥隐藏方案,称为模糊承诺方案. 最近文献[9-10]也对模糊承诺方案作了进一步研究,提出了一些实际的模糊承诺构造方案,也讨论了模糊承诺方案的信息泄漏问题. 模糊盖子方案是由 Juels 和 Sudan 出的一种密钥隐藏方案[11],后来也有很多变体以及实用的方案[12-17],主要思路是使用多项式方法来进行密钥隐藏.

这 3 种密钥隐藏方案都存在一些安全及实现方面的问题. 严格来说,密钥释放方案并不具备比传统生物特征识别系统更高的安全性,很难抵御对模板的蓄意攻击. 假如数据库模板被破解,那么用户的生物特征信息和密钥都将丢失. 基于指纹的模糊承诺方案要求从指纹中提取定长的位串,但是高区分性的定长特征在指纹中非常难以取得,虽然从指纹提取的 FingerCode[16-17] 是定长的,但指纹中心点难以精确定位,导致校准困难,因而区分性不好,密钥恢复成功率不高. 模糊盖子方案相对成熟,研究比较集中,但是由于对指纹质量要求比较高,使用性方面受到很多限制.

在已有密钥隐藏方案的基础上,本文提出了一种新的基于指纹细节点纹理串模板的密钥隐藏方案,有机地结合了现有各密钥隐藏方案的优点,提高了密钥隐藏算法的性能. 本文方案基于作者提出的一种新的指纹模板:细节点纹理串模板,这种密钥隐藏方案也就称为细节点纹理串密钥隐藏方案. 细节点纹理串模板既考虑了指纹的细节点特征,也考量了细节点周围的指纹纹理信息,最大程度地利用了指纹信息熵,提高了密钥隐藏系统的安全性. 安全性分析表明,在不泄漏指纹模板信息的情况下,本方案安全程度高于模糊盖子方案,实用性好于相关模糊盖子方案.

本方案的一个简单应用场景是:用户收到服务方提供的公钥或私钥,然后把密钥存放在自己的 PC 机或其他设备上. 由于担心相关设备遭到入侵,需要采取措施对密钥进行保护. 此时,用户可以调用本文所设计的密钥保护算法,提取自己的指纹信息,使用指纹特征来加密密钥. 当用户需要使用密钥来解密文件或与第三方作认证时,再使用对应的指纹把密钥恢复出来. 本文方案也可以同文献[18]使用的方法相结合,以构造复合的密钥保护及认证方案.

1 细节点纹理串模板

细节点纹理串模板是在指纹细节点模板的基础上增加辅助信息得到的,因此要想求得细节点纹理串模板,首先要求得指纹的细节点模板. 由于细节点模板信息只反映了指纹纹理的端点及分叉点的位置和方向信息,没有反映指纹大尺度上的特征,因而其提取过程丢失了不少的指纹图像的信息熵. 本节中在取得细节点模板后,进一步来求细节点纹理串模板,以更全面地反映指纹的局部及全局信息,更多地提取指纹图像的信息熵.

本文细节点纹理串的思想部分地借鉴了文献[19]中有关 FingerCode 的定义及方法. 首先,在细节点集合中,选取每一个细节点作为参考点,在参考点周围构建同心圆,在同心圆环上划分等分的扇区,每一个扇区作为一个小单元来考虑. 每个扇区均用数字编号,扇区编号从最内层的第 1 个同心圆环开始,最中心的圆形区域不编号. 每一圆环上,位于细节点的方向上的扇区取最小编号,第一圆环上位于细节点的方向上的扇区编号为 1,其他扇区按顺时针顺序递增编号(如图 1 所示). 选择圆形区域进行扇区化是考虑到指纹的旋转可以和圆形区域扇区的旋转对应起来,在后续的特征匹配中可以部分地解决指纹的旋转问题. 图 1 中,对指纹图像在(0°~180°)的 8 个等分方向上(0°,22.5°,45°,67.5°,90°,112.5°,135°,157.5°)做 Gabor 滤波,也就是说,在

每一个方向上把指纹图像和 Gabor 滤波器分别进行傅里叶变换之后再相乘,最后进行傅里叶反变换.指纹图像在特定方向上进行 Gabor 滤波后,与此方向平行的脊线得到加强,而其他方向的脊线则被平滑.每个细节点对应的纹理串即在滤波以后的图像上建立.

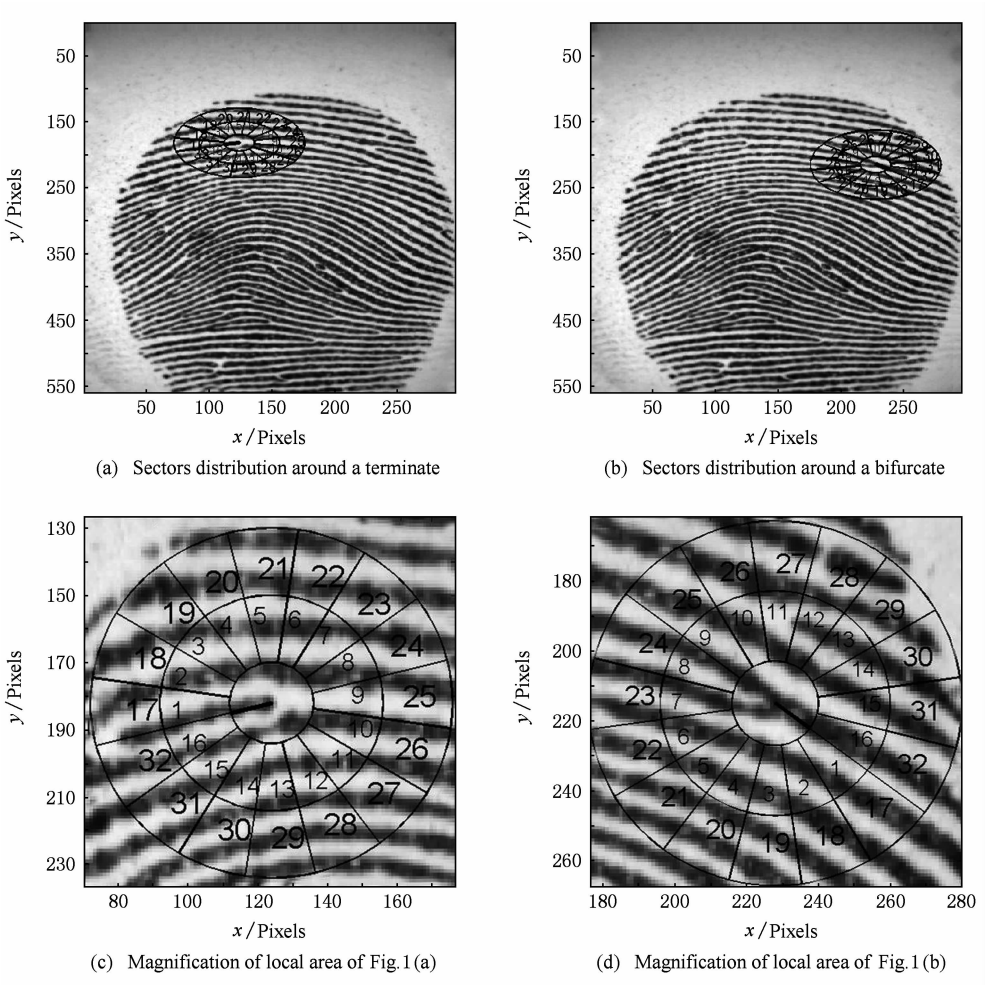


Fig. 1 Extraction area of fingerprint' texture string, all.

图 1 指纹细节点纹理串提取区域

细节点纹理串是由一组特征值来定义的,而特征值定义为小扇区在特定方向上相对于选定区域图像均值的平均偏差值.设 A_i 为第 i 个小扇区,定义 n_i 为扇区中像素点的个数,$F_{i\theta}(x,y)$ 为 A_i 在 θ 方向的滤波图像,$P_{i\theta}$ 为滤波图像的像素均值,那么任意一个小扇区在 θ 方向上的的特征值 $V_{i\theta}$ 定义为

$$V_{i\theta}=\frac{1}{n_i}\sum\mid F_{i\theta}(x,y)-P_{i\theta}\mid.$$

设 n_a 为扇区总数,则每个细节点对应的纹理串定义为

$$\{V_{i\theta}:i\in\{1,2,\cdots,n_a\},\theta\in\{0°,22.5°,45°,67.5°,90°,112.5°,135°,157.5°\}\}.$$

由每一个细节点的坐标值、类型、方向以及其对应的纹理串构成的集合,构成了指纹的细节点纹理串模板,由于这个模板很像是一个表格,因此也可把模板称为细节点纹理串表.

2 基于细节点纹理串的密钥隐藏与恢复

2.1 密钥隐藏

密钥隐藏的总体过程如图 2 所示.设用于密钥隐藏的指纹 FP 中合乎要求的细节点的数目为 n_p,系统从外部取得密钥后,首先以秘密分割方法将密钥 KEY 分割成 n_p 份秘密值,每份记为 s_i,任意 k 份秘密值可以完整地恢复出密钥.切分密钥成 k 等份,每一份作为 $k-1$ 阶多项式 $f(x)$ 的系数.取 n_p 个随机数 x_i,i 取值范围为 $[1,\cdots,n_p]$,n_p 大于 k.求每一个随机值 x_i 在多项式上的值 $f(x)$,数值对 $(x_i,f(x_i))$ 构成一份秘密,n_p 份秘密组成一个集合 $\{s_i=(x_i,f(x_i)):i=1,2,\cdots,n_p\}$.

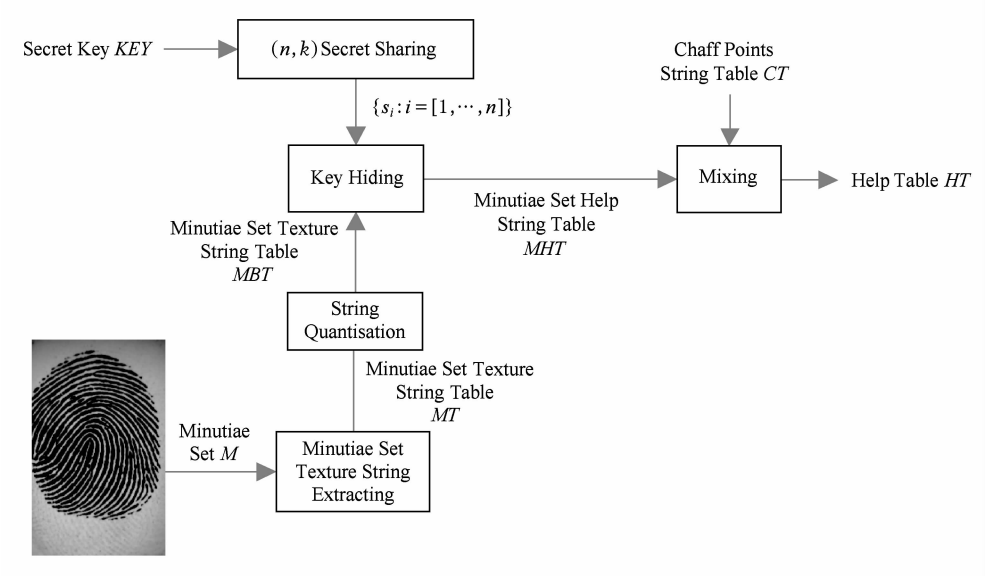


Fig. 2 Framework of secret generation from minutiae texture string.

图 2 细节点纹理串秘密隐藏方法

依第 1 节介绍的方法,从用于隐藏密钥的指纹 FP 中提取细节点纹理串模板表 MT,并对每个纹理串进行量化,使得由实数组成的纹理串变成由二进制数组成的位串,从而得到细节点纹理位串表 MBT. 然后,把每一份秘密值 s_i 作为一个码字进行纠错编码得到 c_i,再与模板中某一个细节点的纹理位串相异或得到帮助位串 h_i,以达到隐藏份额的目的. 细节点以及对应的帮助串构成了细节点帮助位串表 MHT.

最后,在 MHT 中加入 n_c 组杂凑点(chaff point)位串,形成帮助数据表 HT. 杂凑点位串由系统随机产生,模拟细节点所有数据,并对应每个随机点给出随机串来模拟纹理位串,其结构为(随机横坐标 x,随机纵坐标 y,随机点类型 t,随机方向 θ,随机纹理串 h). 杂凑点不能与原细节点集中的点距离太近,更不能重合. 具体来说,如果一个杂凑点与某一细节点在空间距离上相近,方向也相近,则其类型不能相同. 如果类型相同,则空间距离或方向不能相近. 杂凑点对于隐藏密钥 KEY 是非常必要的,为了更好地隐藏密钥,保护指纹的模板,其数量要远大于真实细节点数目.

2.2 密钥恢复方法

密钥恢复过程如图 3 所示. 首先,用户提供用于密钥恢复的指纹样本 FP',系统在样本上作细节点检测以求到细节点集 M',然后从系统中取出对应的帮助数据表 HT',在 M' 和 HT' 上作标准的点集比对,得到二者的匹配细节点表 MT^*. 此时,如果用于恢复密钥的指纹和用于隐藏密钥的指纹来自同一手指,在密钥隐藏阶段加入的杂凑点就从帮助数据表 HT' 中去除了,MT^* 只包含用于密钥隐藏指纹的

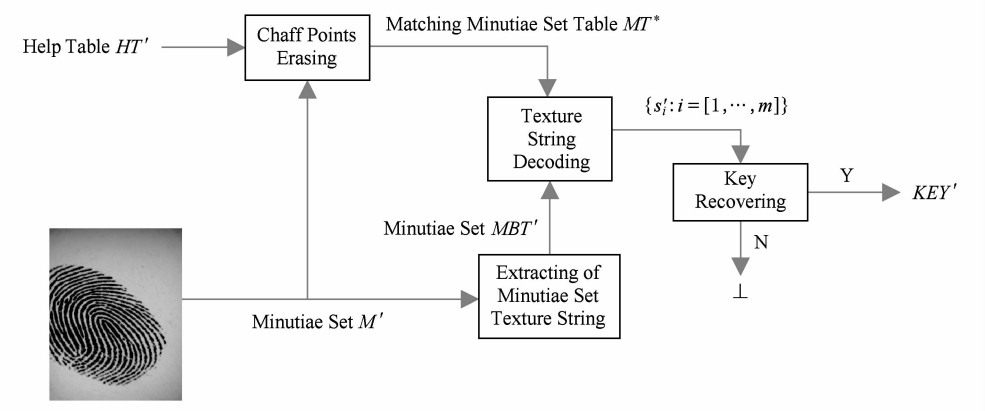


Fig. 3 Framework of secret regeneration from minutiae texture string.

图 3 细节点纹理串秘密恢复框架

稳定细节点. 在指纹上 FP' 求细节点纹理串,进行纹理串量化,得到由细节点和对应纹理位串组成的细节点纹理位串表 MBT'. 用 MT' 中的纹理串来解码 MT^* 对应细节点上的帮助串就可以求到隐藏在原纹理串上的秘密值了. 如果秘密值的数目超过特定的数目 k,就可以恢复出原来密钥 KEY.

3 实验及结果分析

为了验证密钥隐藏算法性能,本文在公开数据库 FVC2002 的 DB1 和 DB2 上进行了密钥隐藏与恢复的实验.

3.1 细节点纹理串模板提取及量化

无论是隐藏密钥阶段还是密钥恢复阶段,都需要提取指纹图像的细节点纹理串. 提取指纹的细节点模板有很多经典算法,已比较成熟,本文不再赘述. 根据第 2 节的描述,纹理串是在细节点周围同心圆环上获得的,无论是用在密钥隐藏还是恢复阶段,纹理串都应该是完整的,因此,并不是每个细节点都可以获得纹理串,太靠近边缘的细节点求不到纹理串,只有靠近图像中心的细节点才可以求得纹理串. 参照文献[19-21]的方法,实验中我们取中心圆的半径为 16 像素,共取两个同心圆环,每个同心圆环的宽度为 20 像素,因此,只有距离指纹图像 4 个边界都大于 56 个像素的细节点才可以取到纹理串. 扇区数量取为 16,同心圆数目取为 3,按本文第 2 节定义,每个细节点的纹理串对应的数据是一个长为 256(2×16×8)的实数数组.

3.2 实验结果及分析

参照文献[11,15]中的方法,实验使用 FVC2002 的 DB1 和 DB2 数据库中所有 100 个手指的前两个图像来完成.

实验 1. 用某一手指的第 1 指纹图像来隐藏密钥,用同一手指的第 2 个指纹来恢复密钥,共计算 100 次. 如果能恢复出原密钥,则记为成功一次. 总的成功次数记为一致成功率(genuine success rate, GSR).

实验 2. 用某一手指的第 1 指纹图像来隐藏密钥,用另一手指的第 1 或第 2 个图像来恢复密钥,共计算 9 000 次. 成功次数与总实验次数之比记为不一致指纹密钥恢复成功率成功率(imposter success rate, ISR).

GSR 以及 ISR 随 BCH 维数变化的情况如图 4 所示,在编码维数比较高时,ISR 下降很快,而 GSR 下降比较慢. 在 DB2 数据库上,由于数据库中指纹图像比较大,可以取到纹理串的指纹细节点比率要高出 DB1 数据库中的指纹,所以 GSR 下降更慢一些.

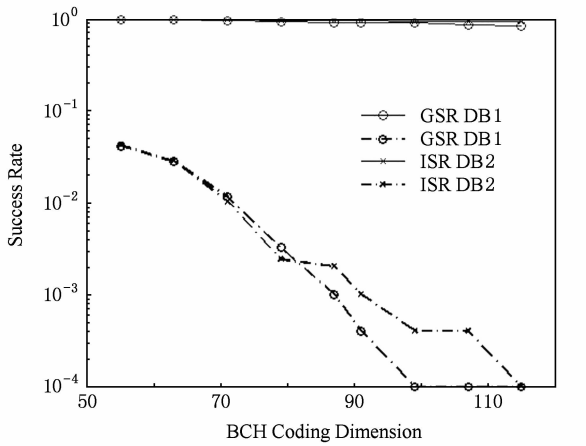


Fig. 4 Geniue success rate and imposter success rate on database DB1 and DB2 based on BCH coding dimension.

图 4 数据库 DB1 和 DB2 上 GSR 和 ISR 随 BCH 编码维数变化的情况

按 GSR 定义一致拒绝率 (genuine rejection rate, GRR). 用某一手指的第一指纹图像来隐藏密钥,用同一手指的第 2 个指纹来恢复密钥,其失败概率定义为 GRR. 从实用上来看,GRR 与 ISR 越小,说明系统的总出错率越低. GRR 与 ISR 随 BCH 编码维数的变化情况如图 5 所示,其中,GRR 与 ISR 之交点定义为等错误率(equal error rate, EER)点. 由图 5 可知,密钥隐藏算法在 DB1 上的 EER 约为 2.2%,而在 DB2 上的 EER 约为 1%.

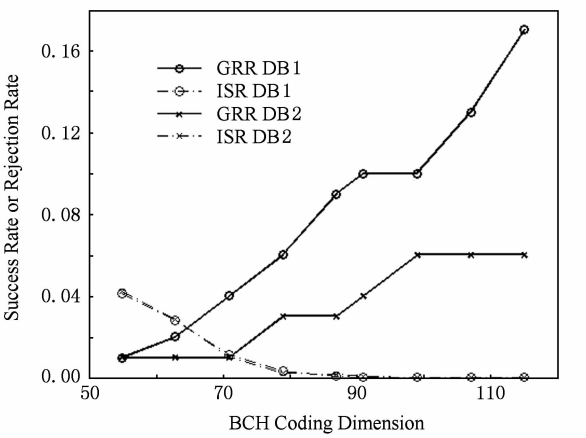


Fig. 5 Geniue reject rate and imposter success rate on database DB1 and DB2 based on BCH coding dimension.

图 5 数据库 DB1 和 DB2 上 GRR 和 ISR 随 BCH 编码维数变化的情况

总体来看,DB2 上的实验结果优于 DB1,这主要是因为 DB2 中的指纹更完整,可以取到的细节点更多,可以取到纹理串的细节点也更多. 编码维数升

高,BCH 码的纠错能力下降比较多时,这种情况更加明显.随着维数的升高,DB2 上实验中的 GRR 只是略有升高,而 DB1 上实验中的 GRR 上升很快,显示出错率上升很快.

3.3 性能比较

由于基本的模糊盖子方案都是基于细节点位置和方向数据的,而低质量的指纹常不能获得足够多的细节点,因而形成所谓获取失败率(failure to capture rate, FTCR),即不能获得某指纹有效细节点模板的概率.表 1 总结了当前各种理论和算法在指纹密钥隐藏方面的信息,给出了各方案使用的密钥隐藏方法、实验用指纹数据库和此方法的最优性能.同大部分模糊盖子方案相比,本方案的密钥恢复性能较优,且 FTCR 为 0.从理论上来看,本文方案对指纹的质量要求低,极限情况下,只要可以获得指纹的 3 个细节点,就可以使用本文方案进行密钥隐藏及恢复. Nagar 方案[15] 同本文方案性能接近,但 FTCR 为 2%,因而其实际的性能低于本方案,且在容许 ISR 升高的情况下,其最优 GRR 也不低于 5%,而本方案中,在 ISR 为 4%时,GRR 可以达到 1%.其他方案也有类似问题,由于 GRR 太高,无法获得一个具有实际应用意义的 EER.

Table 1 Comparision of Performance for Key Hiding Schemes Based on Fingerprint

表 1 基于指纹的密钥隐藏方案的性能比较

Experiment Database	Schemes	Type	Method	FTCR/%	Performance	
					ISR/%	GRR/%
FVC2002 DB1	Feng scheme[13]	Modified fuzzy vault	Hide key with many linear functions		0	15.2
FVC2002 DB2	Uludag scheme[12]	Basic fuzzy vault	Eliminate fingerprints with minutiae number below 24	16	0	27.4
	Nandakumar scheme [2]	Basic fuzzy vault	Extract high curvature points as help information. (10 degree polynomial and 7 degree polynomial)	2	0 0.13	14 9
	Nagar scheme[15]	Modified fuzzy vault	Seek help from ridges around minutae. (8 degree polynomial and 5 degree polynomial)	2	≈0 ≈0	≈7 ≈5
	Li and Tian scheme[7]	Modified fuzzy vault	Combine ridge and local picture quality (9 degree polynomial)		≈0	≈10
FVC2002 DB1,DB2	This scheme	Key hiding on minutiae set texture strings	Combine minutiae set model and texture information around every minutia. (BCH coding dimension 87 and 71)	0	0 1	6 1

受制于可以取到细节点的数目,基本和改进的模糊盖子方案只能隐藏固定比特位长度(约 128 b)的密钥,本文方案相对灵活,可以隐藏不同长度的密钥.若杂凑点和细节点总数是 200,存储每个细节点需 22 b,则隐藏一个密钥需要 $200\times(22+255)=55\,400$ b 的存储空间,而标准方案所需存储空间为 $200\times16=3\,200$ b.同标准的模糊盖子方案相比,在隐藏相同大小密钥的情况下,由于需要存放每个细节点的纹理串,本文方案隐藏单个密钥所需的存储空间增加至大约 5 KB.同标准方案相比,本方案在密钥隐藏和恢复时都要计算指纹的细节纹理串,但由于各相关算法的主要时间花在指纹比对过程中,从整体上来看,算法运行时间的增加可以忽略.

4 安全性分析

基于指纹细节点纹理串模板的密钥隐藏方案的安全性依赖于 3 点:指纹细节点周围纹理状况的随机性;指纹细节点的随机性;加入到系统中杂凑点位串数目 n_c 与实际可用细节点位串数目 n_p 比值.显然,加入到系统中的杂凑点数目越高,细节点纹理串表看起来越随机,敌手找到正确细节点集的概率越低.统计显示,指纹细节点周围的纹理状况以及细节点的位置和方向是很难预测的,可以认为接近随机分布.

同标准的模糊盖子方案相比,本文方案对模板的保护程度更高.首先,本方案没有使用细节点来构建多项式,因而不需要把细节点信息变成二进制形式映射到特定有限域上.基于指纹的模糊盖子方案或其各种变形方案都是把细节点的横坐标和纵坐标(或再加上方向)映射成有限域 $GF(2^{16})$ 上的一个元素,然后在 $GF(2^{16})$ 上构建多项式,用多项式的系数来代表密钥.使用 $GF(2^{16})$ 上的元素来表示指纹细节点,损失了很多细节点的信息熵.比如,如果原始细节点的横坐标、纵坐标、类型和方向分别是由 8,8,1,5 位的二进制数来表示,则其信息熵为 22 b,映

射到 GF(2^{16})上的元素后,信息熵最多也只有 16 b. 因此,面对主动暴力破解敌手时,本方案更多的保护了细节点模板. 其次,在增加同样数量杂凑点的情况下,系统可以选择的杂凑点的空间增加了,本方案所使用的细节点帮助位串表比标准的模糊盖子的帮助点集更显随机. 依上面假设为例,杂凑点的空间增加了 2^6 倍.

定理 1. 密钥保护定理. 设细节点个数是 n_p,杂凑点个数是 n_c,编码维数是 n_k. 在用户指纹未知,细节点帮助位串已知的情况下,暴力破解敌手攻破系统获得隐藏密钥的概率是可以忽略的.

证明. 假设一个敌手试图使用(n_p+n_c)组细节点纹理串的所有可能组合来解开密钥,则敌手要能猜中至少 3 个细节点以及细节点所对应的纹理位串. 从所有细节点中任取 3 个细节点的组合数是 $\binom{n_p+n_c}{3}$,其中,可以正确猜到真正细节点的组合数是 $\binom{n_p}{3}$. 因此,敌手成功猜出真正细节点的概率是 $\binom{n_p}{3}\binom{n_p+n_c}{3}^{-1}$. 成功猜出细节点并不能取得秘密的份额值,敌手还需猜出所有 3 个细节点纹理位串隐藏的秘密份额值,因为帮助位串不能给敌手提供任何帮助,如果细节点的纹理串是随机的,敌手成功猜中 3 份秘密的份额的概率是 2^{-3n_k}. 以此来看,猜中所有份额的概率比直接猜密钥的概率还要小.

证毕.

定理 2. 模板保护定理. 在用户指纹未知,密钥和细节点帮助位串已知的情况下,暴力破解敌手获得用户指纹细节点模板的概率是:$\binom{n_p}{3}\binom{n_p+n_c}{3}^{-1}$.

证明. 已知细节点帮助位串表后,再获取密钥,并不能使得敌手得到更多的有关指纹细节点的信息,因为隐藏密钥的数据只与细节点周围的纹理状况有关,并不反映细节点信息. 暴力破解敌手获得用户指纹细节点模板的概率仍然是:$\binom{n_p}{3}\binom{n_p+n_c}{3}^{-1}$.

证毕.

对模糊盖子密钥隐藏方案而言,若用户在多个系统中用同一个指纹隐藏了密钥,同时攻破两个系统的敌手就可以获取到合法用户的细节点模板,从而可以获得用户隐藏在各个系统中的密钥. 本方案则没有这种漏洞,即便敌手得到了多个系统中的细节点纹理帮助串,通过计算得到了用户的细节点模板,也不能获取到用户的纹理串信息,从而也就无法得到用户隐藏的密钥.

5 结 论

针对已有密钥隐藏算法的不足,我们提出了一种新的基于指纹细节点纹理串模板的密钥隐藏方案,详细地介绍了方案实施的各个步骤,并在 FVC2002 DB1 和 DB2 数据库上进行了仿真实现,分析了方案在不同的编码维数下隐藏密钥的性能,并进行了理论上的安全分析. 同已有的密钥隐藏方案相比,新的密钥隐藏方案安全性更高,更具实用性.

基于细节点纹理串的密钥方案还可以作进一步的改进. 如:使用同一个手指的多个指纹图像隐藏密钥,一个指纹图像恢复密钥,或者使用同一个人的多个手指的图像隐藏密钥,用其中一个手指的图像来恢复密钥等. 本文方案中的细节点模板是明文提供的,这使得模板的安全性依赖于杂凑点的数量,可以考虑构造隐藏指纹细节点模板的密钥隐藏方案,以进一步提高系统的安全性.

参 考 文 献

[1] Juels A, Sudan M. A fuzzy vault scheme [J]. Designs Codes and Cryptography, 2006, 38(2): 237-257

[2] Nandakumar K, Jain A K, Pankanti S. Fingerprint-based fuzzy vault: Implementation and performance [J]. IEEE Trans on Information Forensics and Security, 2007, 2(4): 744-757

[3] Nandakumar K, Nagar A, Jain A K. Hardening fingerprint fuzzy vault using password [G] //LNCS 4642: Proc of ICB 2007. Berlin: Springer, 2007: 927-937

[4] Nagar A, Nandakumar K, Jain A K, et al. Securing fingerprint template: Fuzzy vault with minutiae descriptors [C] //Proc of the 19th Int Conf on Pattern Recognition. Piscataway, NJ: IEEE, 2008: 822-825

[5] Li Peng, Yang Xin, Cao Kai, et al. An alignment-free fingerprint cryptosystem based on fuzzy vault scheme [J]. Journal of Network and Computer Applications, 2010, 33(3): 207-220

[6] Jain A K, Uludag U. Hiding biometric data [J]. IEEE Trans on Pattern Analysis and Machine Intelligence, 2003, 25(11): 1494-1498

[7] Li Peng, Tian Jie, Yang Xin, et al. Biometric template protection [J]. Journal of Software, 2009, 20(6): 1553-1573 (in Chinese)

(李鹏,田捷,杨鑫,等. 生物特征模板保护[J]. 软件学报,2009,20(6):1553-1573)

[8] Juels A, Wattenberg M. Fuzzy commitment scheme [C] // Proc of the 6th ACM Conf on Computer and Communications Security. New York: ACM, 1999: 28-36

[9] Rathgeb C, Uhl A. Systematic construction of Iris-based fuzzy commitment schemes [G] //LNCS 5558: Proc of ICB 2009. Berlin: Springer, 2009: 940-949

[10] Ignatenko T, Willems F M J. Information leakage in fuzzy commitment schemes [J]. IEEE Trans on Information Forensics and Security, 2010, 5(2): 337-348

[11] Juels A, Sudan M. A fuzzy vault scheme [C] //Proc of IEEE Int Symp on Information Theory. Piscataway, NJ: IEEE, 2002: 408-418

[12] Uludag U, Jain A. Securing fingerprint template: Fuzzy vault with helper data [C] //Proc of the IEEE Computer Society Conf on Computer Vision and Pattern Recognition. New York: IEEE, 2006: 163-171

[13] Feng Quan, Sun Fei, Cai Anni. Fingerprint-based key binding/recovering scheme based on fuzzy vault [J]. Journal of Electronics(China), 2008, 25(3): 415—421

[14] Meenakshi V S, Padmavathi G. Security analysis of hardened retina based fuzzy vault [C] //Proc of Int Conf on Advances in Recent Technologies in Communication and Computing. Piscataway, NJ: IEEE, 2009: 926-930

[15] Nagar A, Nandakumar K, Jain A K. A hybrid biometric cryptosystem for securing fingerprint minutiae templates [J]. Pattern Recognition Letters, 2010, 31(8): 733-741

[16] Ramirez-Ruiz J A, Pfeiffer C F. Nolazco-Flores J A. Cryptographic keys generation using FingerCodes [G] // LNAI 4140: Proc of the 18th Brazilian AI Symp. Berlin: Springer, 2006: 178-187

[17] Jain A K, Prabhakar S, Hong L, et al. FingerCode: A filterbank for fingerprint representation and matching [C] // Proc of the IEEE Computer Society Conf on Computer Vision and Pattern Recognition. Los Alamitos, CA: IEEE, 1999: 187-193

[18] Zhang fan, Feng Dengguo. Fuzzy extractor based remote mutual biometric authentication [J]. Journal of Computer Research and Development, 2009, 46(5): 850-856 (in Chinese)
(张凡,冯登国. 基于模糊提取的远程双向生物认证[J]. 计算机研究与发展,2009,46(5):850-856)

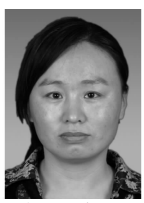
[19] Benhammadi F, Amirouche M N, Hentou H, et al. Fingerprint matching from minutiae texture maps [J]. Pattern Recognition, 2007, 40(1): 189-197

[20] Tong V V T, Sibert H, Lecceur J, et al. Biometric fuzzy extractors made practical: A proposal based on fingercodes [G] //LNCS 4642: Proc of Int Conf on Advances in Biometrics. Berlin: Springer, 2007: 604-613

[21] Willems F M J, Ignatenko T. Quantization effects in biometric systems [C] //Proc of Information Theory and Applications Workshop. Piscataway, NJ: IEEE, 2009: 369-376

Li Ximing, born in 1974. Received his BSc degree in electrical engineering from Shandong University of Technology, Jinan, Shandong, China, in 1996 and his MEn degree in communication engineering from Jinan University, Guangzhou, Guangdong, China, in 2005. Received his PhD degree from the College of Informatics, the South China Agricultural University, Guangzhou, Guangdong, China, in 2011. His current research interests include biometric model protection and cryptography.

Yang Bo, born in 1963. Professor of Shanxi Normal University. His current research interests include public key cryptography and secure multi-party computation.



Guo Yubin, born in 1973. PhD. Lecturer in the South China Agricultural University. Received her PhD from the South China University of Technology in 2008. Her main research interests include database theory and technology, cryptography, and network computing.

Yao Jintao, born in 1978. PhD candidate in information security from the South China Agricultural University. His current research interests include communication and information security.