基于细节点邻域信息的可撤销指纹模板生成算法

许秋旺 [1] 张雪锋 [1]

摘 要 为了提高指纹模板算法的安全性等性能, 设计了一种基于细节点邻域信息的可撤销指纹模板生成算法. 首先对指纹图像进行预处理, 提取指纹的细节点特征, 然后采用改进的细节点描述子采样结构提取细节点邻域的纹线特征, 最后结合用户 PIN 码生成指纹模板, 同时结合贪婪算法设计了相应的指纹匹配算法. 在指纹数据库 FVC2002-DB1 和 DB2 上的实验表明, 该算法具有良好的认证性能, 能较好地满足可撤销性、多样性和不可逆性, 而且改进的采样结构在没有降低系统识别性能的情况下, 进一步拓展了细节点描述子的采样结构方式.

关键词 细节点, 邻域信息, 可撤销模板, 指纹

引用格式 许秋旺, 张雪锋. 基于细节点邻域信息的可撤销指纹模板生成算法. 自动化学报, 2017, **43**(4): 645−652

DOI 10.16383/j.aas.2017.c160069

Generating Cancelable Fingerprint Templates Using Minutiae Local Information

XU Qiu-Wang[1] ZHANG Xue-Feng[1]

Abstract It has become critical to improve the security of the fingerprint templates. This paper, we propose a cancelable fingerprint template based on minutiae local information. First, we extract fingerprint minutiae feature after the preprocessing, then we use the improved Tico sampling structure to extract texture feature of minutiae adjacent area. Finally, the fingerprint template is generated by combining the user PIN. Our design of fingerprint matching algorithm draws on the experience of greedy algorithm. The experiments results on FVC2002-DB1 and DB2 show that the algorithm not only achieves good recognition performance but also fulfills revocability, diversity and non-invertibility, and that without reducing system recognition performance, the improved sampling structure extends the sampling structure of minutiae description.

Key words Minutiae, local information, cancelable template, fingerprint

Citation Xu Qiu-Wang, Zhang Xue-Feng. Generating cancelable fingerprint templates using minutiae local information. *Acta Automatica Sinica*, 2017, **43**(4): 645−652

随着互联网和信息技术的迅猛发展, 物联网、互联网金融、云计算服务等越来越多的领域需要安全、可靠的身份识别技术. 与传统的身份认证方式中采用密钥或令牌相比较, 生物特征具有无需记忆、不易更改、难以伪造等优点[1], 因而基于生物特征的身份认证技术得到广泛的应用. 然而在实际使用过程中, 基于生物特征的身份认证需要存储用户的特征模板, 由于特征模板包含有用户生物特征的原始信息, 在使用过程中一旦被泄露或丢失, 攻击者完全可以使用得到的模板特征, 采用交叉匹配等方式轻松骗过认证系统, 甚至能从用户的特征模板直接恢复出相应的原始生物特征[2], 从而达到伪造用户身份的目的. 鉴于生物特征的不可更改性, 一旦丢失, 对用户来说, 其生物特征的泄露将是永久性的[3]. 因此, 在应用生物特征进行身份识别的过程中有效保护用户生物特征的敏感信息, 尤其是模板数据的安全保护至关重要.

理想的生物特征模板应满足可撤销性、多样性、不可逆性以及性能保持性[4], 围绕这一目标, 研究者已经提出一些解决方案. 现有的生物特征模板保护方法主要包括: 生物特征加密技术和可撤销生物认证技术. 其中可撤销生物认证技术主要分为二类: 一类是基于预先对齐指纹的方法. Ratha 等[5] 针对指纹特征采用笛卡尔变换、极坐标变换、函数变换三种方法映射生成可撤销的指纹模板, 由于模板内不含有原始指纹信息, 能较好保护用户的隐私, 提高模板的安全性. 但 Feng 等[6] 指出 Ratha 使用的单向变换函数在多数区域的映射关系是一对一的, 攻击者可利用穷尽法、多模板攻击法和非线性方程组求解法, 从特征模板中推导出大部分原始指纹信息. Ang 等[7] 提出将指纹细节点模板进行平面对折的几何变换方法, 其缺点是生成模板过程中只对部分细节点进行变换, 存在原始指纹信息泄露的可能. Teoh

收稿日期 2016-01-22 录用日期 2016-04-09
Manuscript received January 22, 2016; accepted April 9, 2016
国家自然科学基金 (61301091) 资助
Supported by National Natural Science Foundation of China (61301091)
本文责任编委 封举富
Recommended by Associate Editor FENG Ju-Fu
1. 西安邮电大学通信与信息工程学院 西安 710061
1. School of Communication and Information Engineering, Xi′an University of Posts and Telecommunications, Xi′an 710061

等[8] 提出一种基于 BioHashing 的可撤销生物认证的方案, 该方法能取得较好的识别性能, 如等错误率为零, 但 Kong 等[9] 指出: 如果攻击者在获取到正交矩阵后, 冒充真实用户骗过认证系统的可能性很高, 此时 BioHashing 方法的性能不如普通生物认证有效. 另一类是无需对齐指纹的方法. Lee 等[10] 提出一种免对齐的可撤销指纹模板构造方法, 该方法结合指纹细节点邻域的方向图和用户 PIN 码产生平移和旋转参数, 然后用参数对细节点进行平移和旋转操作, 得到可撤销指纹模板. Jin 等[11] 提出一种基于细节点对的可撤销比特串模板生成方法, 随后研究人员又相继提出了基于三维数组[12]、基于三维极坐标[13] 和基于投影[14] 的比特串模板的构造方法. 经分析, 这类方法存在共同的缺陷: 在模板数据和用户 PIN 码被攻击者盗取后, 由于置换矩阵是可逆的, 采用暴力攻击可查找出细节点的拓扑结构, 进而导致原始指纹数据泄露. Wong 等[15] 提出一种基于 Multi-line code 的指纹模板生成方法. Wang 等[16] 基于多对一映射构造出一种免对齐的可撤销指纹模板. Prasad 等[17] 提出一种基于细节点邻域特征的免配准指纹模板生成方法. 李梦醒等[18] 提出一种结合细节点纹线特征与局部结构的免对齐指纹匹配方法, 该方法能获得很好的识别性能, 但计算较为复杂, 而且生成的模板无法撤销或更新. Das 等[19] 提出一种基于最小距离图形的可撤销指纹模板生成算法, 该算法能较好抵抗蛮力攻击, 但识别精度依赖于指纹中心点的精确检测.

由于基于预先对齐指纹的模板生成方法[5, 7−8] 在变换前需利用参考点对齐指纹图像, 而参考点往往很难精确检测, 会引入连带误差, 导致识别性能变差, 而且实际使用中, 有些指纹的参考点不存在, 如拱形指纹, 进而限制了算法的应用范围. 基于以上分析, 本文在对可撤销指纹模板生成方法进行研究的基础上, 设计了一种基于细节点邻域信息的可撤销指纹模板生成算法. 实验结果表明, 所提方法生成的指纹模板具有良好的区分能力, 能较好地满足可撤销性、多样性和不可逆性, 而且改进的采样结构在没有降低算法识别性能的情况下, 进一步拓展了细节点描述子的采样结构方式.

1 基于细节点邻域信息的可撤销指纹模板生成

本节主要介绍一种基于细节点邻域信息的可撤销指纹模板生成算法. 由于细节点描述子包含有大量细节点邻近区域内的方向信息, 且具有较好的区分能力, 因此, 本文指纹不变特征的提取过程结合细节点描述子的生成方法, 然后将指纹特征投影到用户 PIN 码生成的随机矩阵中得到可撤销指纹模板. 接下来分别介绍细节点描述子和本文所提出的可撤销指纹模板生成算法.

1.1 细节点描述子

Tico 等[20] 提出利用细节点邻近区域内的方向信息与细节点自身方向作差, 得到一串定长且具有旋转和平移不变特性的纹线方向特征, 被称为细节点描述子 (Minutia descriptor). 其采样点的分布结构如图 1 所示.

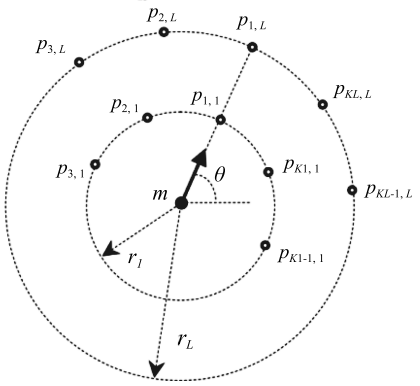


图 1 细节点描述子中采样点的分布结构

Fig. 1 Sampling points structure of the minutia descriptor

细节点描述子的具体构造方法如下: 首先以细节点 m 为圆心, 取 L 个同心圆, 半径为 r_l, $l = \{0, 1, \cdots, L\}$. 每个同心圆上包含有 K_l 个采样点 $P_{k,l}$, $k = 1, 2, \cdots, K_l$, 且这些采样点均匀分布在圆周上. 然后把细节点 m 的方向 θ 作为起始方向, 从细节点指向的最里层同心圆开始, 在圆环上沿着逆时针进行采样, 由里而外, 最后将所有采样点顺序连接成一个描述子向量. 用 $\theta_{k,l}$ 表示采样点 $P_{k,l}$ 所在位置的方向场方向角度, 那么, 细节点描述子的表达式为

$$d_0 = \{\{\lambda(\theta_{k,l}, \theta)\}_{k=1}^{K_l}\}_{l=1}^{L} \tag{1}$$

其中, $\lambda(\theta_{k,l}, \theta)$ 表示采样点 $P_{k,l}$ 所在位置的方向场方向 $\theta_{k,l}$ 与细节点方向 θ 的夹角值.

由于细节点描述子对指纹图像的位置和方向发生的变化不敏感, 而且对于少量细节点的缺失、存在少量的伪细节点以及轻微的细节点定位误差, 具有一定的容错性. 此外, 细节点描述子与图像上提取出的其他细节点是相互独立的, 因此, 本文将细节点描述子作为可撤销指纹模板的不变特征加以利用.

1.2 基于细节点邻域信息的可撤销指纹模板生成

本节设计了一种基于细节点邻域信息的可撤销指纹模板, 其基本思路是: 首先对注册指纹图像进行预处理, 提取指纹的细节点特征, 然后采用改进的细节点描述子采样结构提取出平移、旋转不变性的指

纹特征, 结合用户 PIN 码生成的随机矩阵, 将指纹特征投影到随机矩阵中, 得到指纹模板. 验证时, 对查询指纹图像进行相同变换生成查询模板, 在变换域内计算两枚指纹模板的相似分数得到匹配结果.

基于细节点邻域信息的可撤销模板生成方法的基本流程如图 2 所示.

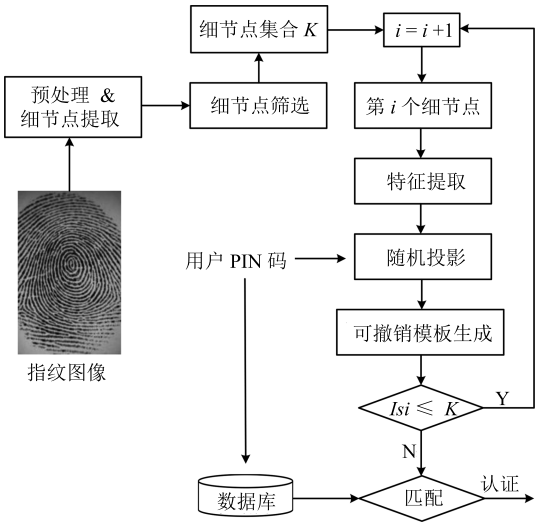


图 2　基于细节点邻域信息的可撤销模板生成流程图

Fig. 2　Process diagram of proposed method for template generation

具体的构造步骤描述如下.

算法 1. 基于细节点邻域信息的可撤销模板生成算法

步骤 1. 预处理. 对输入的指纹图像进行图像增强、分割、方向场估计、图像二值化和纹路细化处理.

步骤 2. 细节点提取. 预处理后, 提取指纹细节点 (分叉点和端点) 和过滤处理后, 得到指纹细节点集合

$$M = \{x_i, y_i, \theta_i | i = 1, \cdots, N\} \tag{2}$$

其中, x_k, y_k, θ_k 分别为第 i 个细节点的位置坐标和方向角度, N 为集合内细节点的个数.

步骤 3. 细节点筛选. 对指纹细节点集合 M 内的细节点逐一进行筛选, 只有采样圆环都位于指纹图像有效区域内的细节点才能用来提取指纹特征. 因此, 得到特征集合

$$Ms = \{x_i, y_i, \theta_i | i = 1, \cdots, K\} \tag{3}$$

步骤 4. 特征提取.

步骤 4.1. 在细节点特征集合 Ms 中, 以细节点 ms_i 的位置坐标 (x_i, y_i) 为圆心, 取 L 个同心圆, 半径为 r_l, $l = \{0, 1, \cdots, L\}$. 每个同心圆上包含有 K_l 个采样点 $P_{k,l}$, $k = 1, 2, \cdots, K_l$, 其中, 圆周上的采样点是非等间隔分布的.

步骤 4.2. 把细节点 ms_i 的方向角度 θ_i 作为参考方向, 从细节点指向的最里层同心圆开始, 在圆环上沿着逆时针进行采样, 由里而外, 最后将所有采样点顺序连接成一个描述子向量. 其中, 采样点的间隔为

$$\begin{aligned} \theta &= 2\pi \times \sin\left(\frac{\pi}{2K_l} P_{k,l}\right) + \theta_i \\ \theta &= \mathrm{mod}(\theta, 2\pi) \end{aligned} \tag{4}$$

用 $\theta_{k,l}$ 表示采样点 $P_{k,l}$ 所在位置的方向场方向角度, 细节点 ms_i 的纹线特征表述为

$$\boldsymbol{D}_i = \{\{\lambda(\theta_{k,l}, \theta)\}_{k=1}^{K_l}\}_{l=1}^{L} \tag{5}$$

其中, $\lambda(\theta_{k,l}, \theta)$ 表示采样点 $P_{k,l}$ 所在位置的方向场方向 $\theta_{k,l}$ 与细节点方向 θ_i 的夹角值, $\boldsymbol{D}_i$ 的长度为 $B = \sum_{l=1}^{L} K_l$.

步骤 4.3. 依次选取细节点特征集合 MS 内的细节点, 得到指纹的纹线特征

$$D = [\boldsymbol{D}_1, \boldsymbol{D}2, \cdots, \boldsymbol{D}_K] \tag{6}$$

步骤 5. 可撤销模板生成. 对每个细节点 ms_i 的纹线特征向量 $\boldsymbol{D}_i$ 进行随机映射, 得到可撤销指纹模板.

步骤 5.1. 利用用户 PIN 码生成伪随机向量 $\boldsymbol{\Gamma}$, 并对其 Gram-Schmidt 正交化, 得到正交随机矩阵 $R_{p\times q}$, 其中, $q = B$, $p < q$.

步骤 5.2. 将指纹的纹线特征 D_i 投影到随机矩阵 $R_{p\times q}$ 中, 得到长度为 $p \times 1$ 的细节点纹理串 T.

$$R \times D = T \tag{7}$$

步骤 5.3. 把所有细节点纹理串依次相连接得到指纹模板 $T = \{T_1, T_2, \cdots, T_K\}$.

算法 2. 模板匹配算法

假设注册指纹 M^E 和查询指纹 M^Q 采用相同的用户 PIN 码生成的特征模板分别为 $T^E = \{T_1^E, T_2^E, \cdots, T_k^E\}$ 和 $T^Q = \{T_1^Q, T_2^Q, \cdots, T_m^Q\}$, 其中 k 和 m 为有效细节点个数. 那么查询模板 T^Q 与注册模板 T^E 的相似度 $S(T^E, T^Q)$ 计算方法如下:

步骤 1. 注册指纹内细节点 M_i^E 纹理串 T_i^E 与查询指纹内细节点 M_j^Q 纹理串 T_j^Q 的距离分数为

$$d(T_i^E, T_j^Q) = \frac{\|T_i^E - T_j^Q\|_2}{\|T_i^E\|_2 + \|T_j^Q\|_2} \tag{8}$$

其中, $\|\cdot\|_2$ 为 2 范数. 那么, T_i^E 与 T_j^Q 的相似度为

$$SA(T_i^E, T_j^Q) = 1 - d(T_i^E, T_j^Q) =$$

$$1-\frac{\|T_i^E-T_j^Q\|_2}{\|T_i^E\|_2+\|T_j^Q\|_2} \tag{9}$$

其中, $SA(T_i^E,T_j^Q)$ 取值范围为 0～1, 由于查询指纹和注册指纹检测出细节点一般是不相同的, 而且在模板中不存储任何有关原始细节点信息, 因此, 将查询模板 T^Q 内的元素 $T^Q=\{T_1^Q,T_2^Q,\cdots,T_m^Q\}$ 与注册模板 T^E 内的元素 $T^E=\{T_1^E,T_2^E,\cdots,T_k^E\}$ 进行逐一匹配, 得到细节点 M_i^E 和 M_j^Q 匹配分数的相似度矩阵. 图 3 为查询模板与注册模板的匹配过程.

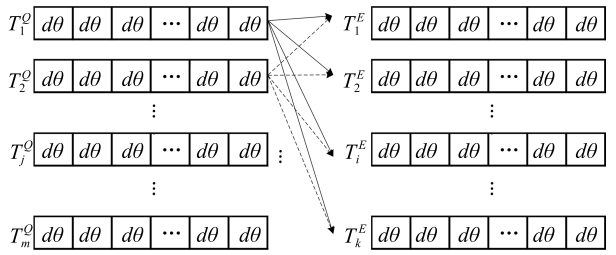


图 3 查询模板与注册模板的匹配过程 ($d(\theta)$ 为纹理串元素)

Fig. 3 Similarity score between query and enrolled fingerprint template ($d(\theta)$ is real value)

步骤 2. 由步骤 1 得到查询模板 T^Q 与注册模板 T^E 的相似度矩阵 $D=\{d_{ij}\}$, 其中, $d_{ij}=SA(T_i^E,T_j^Q)$. 把相似度分数最大的纹理串作为查询模板与注册模板最相匹配的纹理串, 即取每行最大的值, 得到最大相似度集合 $SAmax$.

$$SAmax(j)=\max_i\{d_{ij}\} \tag{10}$$

根据式 (11) 计算 $SAmax$ 中元素的均值, 记为 $SAmean$.

$$SAmean=\frac{\sum_{j=1}^{m}SAmax(j)}{m} \tag{11}$$

步骤 3. 计算 $SAmax$ 中相似度分数大于 $SAmean$ 的所有元素的均值, 作为最终匹配分数, 记为 $S(T^E,T^Q)$

$$S(T^E,T^Q)=\frac{\sum_{j=1}^{m}S(j)}{mum} \tag{12}$$

其中, $S(j)$ 为 $SAmax$ 中大于 $SAmean$ 的元素, num 为 $S(j)$ 的个数. 若 $S(T^E,T^Q)\geq Th$ 则认证通过, 其中 Th 为判决门限.

2 实验结果及性能分析

2.1 实验环境

为评价提出方法的性能, 在 Intel® Pentium® CPU@3.10 GHz, 4.00 GB 内存的 PC, Matlab R2010b 的开发环境下进行实验仿真, 对算法的相关性能进行验证和分析. 测试的指纹数据库采用 FVC2002-DB1 和 FVC2002-DB2, 参数如表 1 所示.

表 1 FVC2002-DB1 和 FVC2002-DB2 数据库参数

Table 1 Summary of databases used in our experiments

	FVC2002-DB1	FVC2002-DB2
采集设备	Touch View II 光学采集仪	FX2000 光学采集仪
图像尺寸	388 × 374	296 × 560
手指数量	100	100
每枚手指采集次数	8	8
分辨率	500 dpi	596 dpi
图像质量	Good	Medium

使用的匹配规则为: 在真匹配实验中, 选取每枚手指的第一幅指纹图像作为注册指纹, 第二幅指纹图像作为查询指纹, 共有 $1\times100=100$ 次真匹配. 在假匹配实验中, 选取每枚手指的第一幅指纹图像生成注册指纹, 剩余手指的第一幅指纹图像作为查询指纹, 共有 $C_{100}^2=4\,950$ 次假匹配. 评价指纹识别系统性能的主要指标是误识率 (False accept rate, FAR)、误拒率 (False refuse rate, FRR) 和等错误率 (Equal error rate, EER). 其中, EER 值越低, 算法匹配性能越好. 本文用 EER 评价算法的有效性.

2.2 认证性能

本节主要从参数选取对匹配性能的影响、真假匹配分布以及对比实验等方面来评价所提出算法的认证性能.

2.2.1 对比各个参数对匹配性能的影响

为了验证不同采样圆环半径 r 和采样点个数 K 对匹配性能的影响, 在 FVC2002-DB1 和 DB2 进行实验, 得到的匹配结果如表 2 所示.

表 2 不同的采样圆环 r 与采样点个数 K 下的匹配结果 (%)

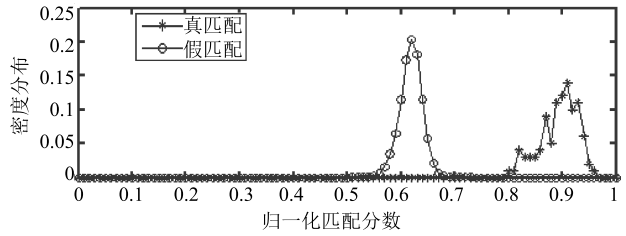
Table 2 EER of different sampling point structure around each minutiae for the same PIN (%)

采样点构造	FVC2002-DB1	FVC2002-DB2
$(r_1,K_1),(r_2,K_2),\cdots,(r_L,K_L)$	EER	EER
$(42,14),(60,20),(78,26)$	8.12	7.33
$(42,14),(60,20),(78,26),(93,32)$	17.37	21.18
$(27,10),(45,16),(63,22),(81,28)$	12.14	11.54
$(12,14),(24,18),(36,24),(48,28)$	3.26	4.58

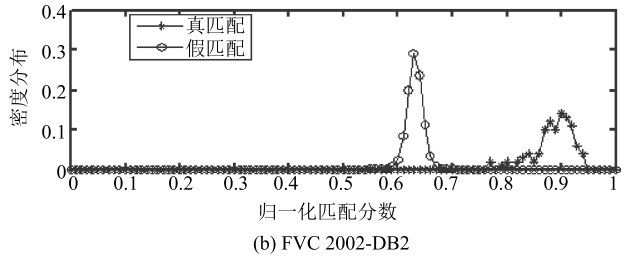
表 2 显示了在用户 PIN 码泄露时, 在不同的采样圆环半径 r 和采样点个数 K 下系统的等错误率, 由此可以看出, 随着 r 和 K 增加, EER 也逐渐增大, 系统的识别性能随之退化, 只有取适当的 r, 位于指纹有效区域内的采样结构越多, 进而能提取更多的指纹特征信息. 从表 2 的实验结果可知, 当取 4 个圆环, 半径分别为 12, 24, 36, 48 像素, 其圆环分别取 14, 18, 24 和 28 个采样点时, 匹配结果最好. 因此, 本文的性能分析实验采用该结构进行特征采样.

2.2.2　真假匹配分布

图 4 和图 5 分别给出本文方法产生的真假匹配分数的分布情况.



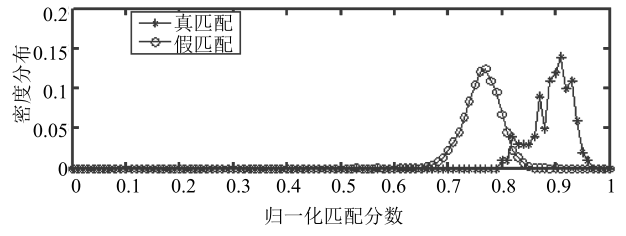
(a) FVC 2002-DB1



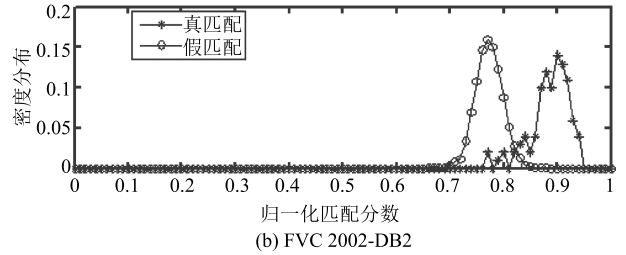
(b) FVC 2002-DB2

图 4　用户 PIN 码安全时真假匹配的分布情况

Fig. 4　Genuine and imposter distributions in safe-PIN scenario



(a) FVC 2002-DB1



(b) FVC 2002-DB2

图 5　用户 PIN 码被盗后真假匹配的分布情况

Fig. 5　Genuine and imposter distributions in stolen-PIN scenario

从图 4 和图 5 可以看出, 在用户 PIN 码安全时, 真匹配分数的分布与假匹配分数的分布没有重叠区域, 此时本文方法的性能较好, 能完全区分不同用户的指纹. 然而在 PIN 码被盗后, 真、假匹配分数的分布有部分重叠, 会出现一定的错误识别.

图 6 为 Tico 细节点描述子结构与本文方法在用户 PIN 码被盗的情形下, 在 FVC2002-DB1 和 DB2 生成的 ROC 曲线分布. ROC 曲线横坐标为错误接受率 (FAR), 纵坐标为真实接受率 (Genuine accept rate, GAR), ROC 曲线越接近横坐标轴说明算法的正确识别率越高.

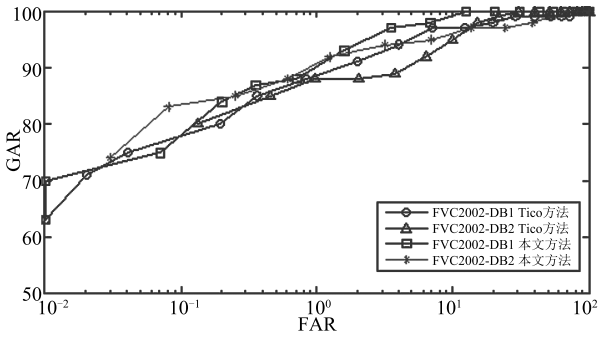


图 6　在用户 PIN 码被盗情形下, Tico 细节点描述子结构与本文方法的 ROC 曲线

Fig. 6　ROC curves of Tico sampling structure and proposed method for the stolen-PIN

实验结果表明, 本文方法比 Tico 细节点描述子结构具有更好的识别性能, 识别性能并不是单纯地完全依赖于用户 PIN 码, 而是指纹特征与用户 PIN 码有效融合的结果.

2.2.3　比较实验

为了分析本文方法的识别性能, 将其与现有的 5 种方法进行实验比较, 这 5 种方法都是免对齐可撤销指纹模板生成方法, 实验结果如表 3 所示.

表 3　不同方法的性能对比 (EER) (%)

Table 3　EER comparison between proposed method and some existing methods (%)

方 法	FVC2002-DB1	FVC2002-DB2
Lee 和 Kim[12]	10.30	9.50
Ahmad 等[14]	9.00	6.00
Jin 等[13]	5.19	5.65
Wang 和 Hu[21]	3.50	5.00
Belguechi 等[22]	3.78	6.68
本文方法	3.26	4.58

从表 3 中可以看出, 在用户 PIN 码泄露的情况下, 本文方法在数据库 FVC2002-DB1 和 DB2 的 EER 分别为 3.26 % 和 4.58 %, 而 Lee 和 Kim、Ahmad 等、Jin 等、Wang 和 Hu、Belguechi 等的 EER 分别为 10.30 %, 9.00 %, 5.19 %, 3.50%, 3.78 % 和 9.50 %, 6.00 %, 5.65 %, 5.00 %, 6.68 %, 很明显, 本文方法的识别性能优于以上 5 种方法. 本文方法在数据库 DB1 的 EER 低于数据库 DB2 的 EER, 即在 DB1 的识别性能比 DB2 的识别性能要好, 因为 DB1 的指纹图像质量比 DB2 的指纹图像质量略好, 说明本文方法在较好质量的指纹图像中能提取出更多的有效指纹特征信息, 匹配性能较好. 图 7 和图 8 分别给出了本文方法在 FVC2002-DB1 和 DB2 数据库匹配的 EER 曲线图.

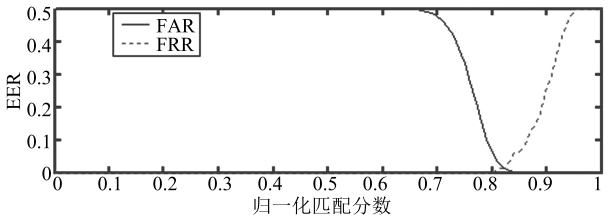


图 7 相同 PIN 码的 EER 曲线 (FVC2002-DB1)

Fig. 7 EER of FVC2002-DB1 for the same PIN

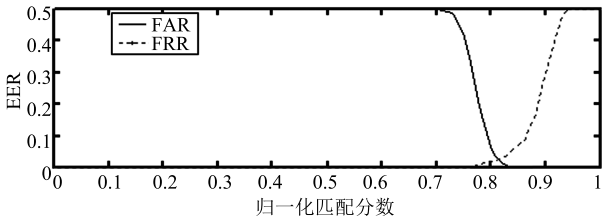


图 8 相同 PIN 码的 EER 曲线 (FVC2002-DB2)

Fig. 8 EER of FVC2002-DB2 for the same PIN

接下来, 分析在细节点邻域信息的提取过程中, 分别采用 Tico 方法中给出的均匀采样方法和本文的改进方法对系统识别性能的影响. 表 4 为两种采样结构的匹配性能对比.

表 4 采用均匀采样方法和本文提出方法的性能比较 (EER) (%)

Table 4 EER comparison between the method of uniform sampling structure and proposed method (%)

方法	用户 PIN 码安全		用户 PIN 码泄露	
	DB1	DB2	DB1	DB2
均匀采样	0	0	4.97	6.31
本文方法	0.02	0	3.26	4.58

从表 4 可以看出, 在用户 PIN 码安全的情况下, 指纹数据库 FVC2002-DB1 和 DB2 中算法的等错误率都很接近于 0, 说明均能获得较为理想的正确识别率; 但是, 当用户 PIN 码泄露后, 采用本文方法, 在 DB1 和 DB2 数据库中系统的等错误率分别为 3.26 % 和 4.58 %, 而采用均匀采样方法, 系统的等错误率分别为 4.97 % 和 6.31 %. 由此看出, 使用本文改进采样结构提取出的细节点邻域特征能保留更多的原始指纹信息, 进而增加指纹模板的区分能力, 从而对系统的识别性能有所改善. 同时, 由于改进方法是非等间隔采样, 在没有降低识别性能的情况下, 拓展了细节点描述子的采样结构方式.

2.3 可撤销性

在本文方法生成的指纹模板中, 用户 PIN 码对于相同用户指纹使用相同的 PIN 码, 而不同用户指纹使用不同的 PIN 码. 当存储的指纹模板受到威胁时, 用户可以通过更换自己的 PIN 码就可以发布一个新的特征模板. 为了达到模板的可撤销性的要求, 更新的模板不能与所撤销的模板相似. 因此, 在 FVC2002-DB1 和 DB2 中进行实验, 定量分析本文方法生成的指纹模板是否具有可撤销性. 具体过程是: 从两个数据库中选取每枚手指的第一幅指纹图像作为实验指纹, 随机生成 100 个 PIN 码, 第一个 PIN 码生成注册模板, 其余的 PIN 码生成验证模板, 然后将注册模板与验证模板分别进行一次匹配 (伪假匹配), 共进行 9 900 次匹配, 对其结果进行统计分析.

图 9 和图 10 显示在指纹数据库 FVC2002-DB1 和 FVC2002-DB2 中, 分别使用相同 PIN 码和不同 PIN 码的真、假匹配分数的分布情况. 仿真实验结果表明, 不同 PIN 码的假匹配和伪假匹配的分布非常相似. 同时我们还计算了在 FVC2002-DB1 和 DB2 上, 真、假匹配分布的均值和标准差, 如表 5 和表 6 所示.

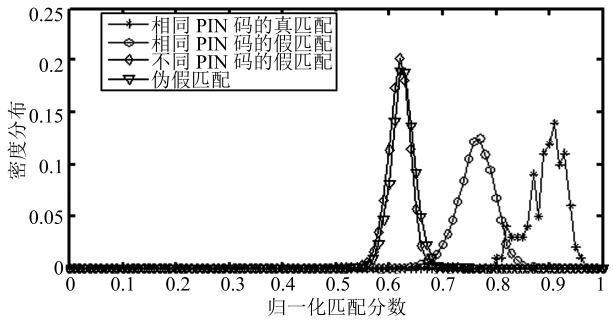


图 9 在 FVC2002-DB1 数据库中, 分别使用相同 PIN 码和不同 PIN 码的真、假匹配分数分布情况

Fig. 9 Genuine, imposter and pseudo-imposter distributions for FVC2002-DB1

表 5　真、假匹配分布的均值与方差

Table 5　The mean and standard deviations of the distributions

指纹数据库	相同 PIN 码的真匹配		相同 PIN 码的假匹配		不同 PIN 码的假匹配		伪假匹配	
	均值	方差	均值	方差	均值	方差	均值	方差
FVC2002-DB1	0.8940	1.24×10^{-3}	0.7624	1.18×10^{-3}	0.6186	4.31×10^{-4}	0.6254	4.97×10^{-4}
FVC2002-DB2	0.8860	1.30×10^{-3}	0.7731	6.23×10^{-4}	0.6312	1.98×10^{-4}	0.6294	3.52×10^{-4}

表 6　不同方法的假匹配分布的均值与方差 (FVC2002-DB2)

Table 6　The mean and standard deviations of the different methods imposter distributions for FVC2002-DB2

方法	不同 PIN 码的假匹配		伪假匹配	
	均值	方差	均值	方差
Lee 和 Kim[12]	0.0470	6.83×10^{-5}	0.0480	1.14×10^{-4}
Jin 等[13]	0.0597	0.0143	0.0542	0.0228
Wang 和 Hu[21]	0.2817	0.0208	0.2897	0.0057
本文方法	0.6312	1.98×10^{-4}	0.6294	3.52×10^{-4}

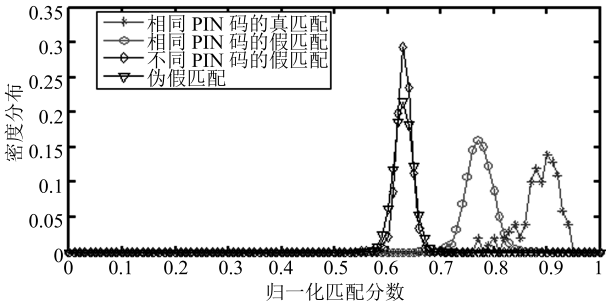


图 10　在 FVC2002-DB2 数据库中, 分别使用相同 PIN 码和不同 PIN 码的真、假匹配分数分布情况

Fig. 10　Genuine, imposter and pseudo-imposter distributions for FVC2002-DB2

表 5 和表 6 的均值和标准差统计对比结果表明本文算法具有较好的统计性能, 由此可以得出结论, 对于同一枚指纹图像来说, 不同的 PIN 码生成的指纹模板之间具有很低的相似度. 因此, 当用户的指纹模板泄露后, 可以通过更换用户 PIN 码实现对指纹模板的更新, 而攻击者即便获取到已撤销的模板也不能冒充新的模板通过识别系统的认证, 进而保护用户信息的安全和隐私.

2.4　多样性

实际使用中, 用户采用各自的 PIN 码生成伪随机数, 组成随机矩阵. 同一指纹特征与不同随机矩阵融合后, 生成多样化的指纹特征模板. 图 9 和图 10 的仿真结果表明, 使用相同的指纹特征与 100 个不同 PIN 码控制产生的随机矩阵融合, 生成的指纹模板之间有明显差异, 而且指纹模板是由原始的指纹模板结合不同的 PIN 码进行随机映射降维生成的, 经过降维处理得到的模板和原始的指纹模板不能直接进行比对. 综上分析, 本文方法产生的指纹模板符合多样性的要求, 进而保证了不同应用场合使用不同的指纹模板.

2.5　安全性分析

本文方法需要把指纹模板 T 存储在模板数据库里, 而存储在智能卡中的信息为生成伪随机数种子 PIN 码, 整个系统保护的是用户的指纹信息, 需要对系统中可能存在的安全问题进行分析.

首先, 当指纹模板 T 或智能卡泄露时, 由于本文提出的方法是一种 "指纹模板 + 智能卡" 的双因子身份认证方案, 具有良好的可撤销性, 可通过更换智能卡即可发布新的指纹模板, 实现对丢失信息的撤销.

其次, 在利用随机矩阵进行投影过程中, 方程系统的方程个数为 p, 未知数个数为 q, 由于满足 $p < q$, 即未知数个数多于方程个数, 该方程属于不定方程, 理论上有无数组解. 因此, 不能从指纹模板 T 中重构出原始的指纹特征数据, 满足不可逆性.

最后, 考虑系统遭受暴力攻击的情形, 攻击者在未获得真实用户指纹特征模板或者智能卡时, 识别系统的安全性等同于猜测一幅指纹图像, 这在计算上是不可行的. 即便攻击者已掌握真实用户的智能卡, 结合所拥有的指纹信息冒充真实用户进行认证, 由实验可知, 在指纹数据库 FVC2002-DB1 和 DB2 上成功的概率不高于 3.26 % 和 4.58 %, 与已有方法

比较, 本算法具有更好的安全性.

3 结论

本文针对现有的指纹模板保护方法中存在的影响安全性和识别精度的问题, 设计了一种基于细节点邻域信息的可撤销指纹模板生成算法, 并对其性能进行了实验分析. 结果表明, 提出的方法生成的指纹模板能保持良好的区分能力, 而且具有较好的可撤销性、多样性和不可逆性, 与已有指纹模板生成方法相比, 该算法具有更优的性能.

References

1 Tian Jie, Yang Xin. *Biometric Recognition Theory and Application*. Beijing: Publishing House of Tsinghua University, 2009.
(田捷, 杨鑫. 生物特征识别理论与应用. 北京: 清华大学出版社, 2009.)

2 Cao K, Jain A K. Learning fingerprint reconstruction: from minutiae to image. *IEEE Transactions on Information Forensics and Security*, 2015, **10**(1): 104−117

3 Yue Feng, Zuo Wang-Meng, Zhang Da-Peng. Survey of palmprint recognition algorithms. *Acta Automatica Sinica*, 2010, **36**(3): 353−365
(岳峰, 左旺孟, 张大鹏. 掌纹识别算法综述. 自动化学报, 2010, **36**(3): 353−365)

4 Rane S, Wang Y, Draper S C, Ishwar P. Secure biometrics: concepts, authentication architectures, and challenges. *IEEE Signal Processing Magazine*, 2013, **30**(5): 51−64

5 Ratha N K, Chikkerur S, Connell J H, Bolle R M. Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2007, **29**(4): 561−572

6 Feng Q, Su F, Cai A N, Zhao F F. Cracking cancelable fingerprint template of Ratha. In: Proceedings of the 2008 International Symposium on Computer Science and Computational Technology. Shanghai, China: IEEE, 2008. 572−575

7 Ang R, Safavi-Naini R, McAven L. Cancelable key-based fingerprint templates. In: Proceedings of the 10th Australasian Conference on Information Security and Privacy. Berlin Heidelberg, Germany: Springer, 2005. 242−252

8 Teoh A B J, Ling D N C, Goh A. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, 2004, **37**(11): 2245−2255

9 Kong A, Cheung K H, Zhang D, Kamel M, You J. An analysis of BioHashing and its variants. *Pattern Recognition*, 2006, **39**(7): 1359−1368

10 Lee C, Choi J Y, Toh K A, Lee S, Kim J. Alignment-free cancelable fingerprint templates based on local minutiae information. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 2007, **37**(4): 980−992

11 Jin Z, Teoh A B J, Ong T S, Tee C. A revocable fingerprint template for security and privacy preserving. *KSII Transactions on Internet and Information Systems*, 2010, **4**(6): 1327−1342

12 Lee C, Kim J. Cancelable fingerprint templates using minutiae-based bit-strings. *Journal of Network and Computer Applications*, 2010, **33**(3): 236−246

13 Jin Z, Teoh A B J, Ong T S, Tee C. Fingerprint template protection with minutiae-based bit-string for security and privacy preserving. *Expert Systems with Applications*, 2012, **39**(6): 6157−6167

14 Ahmad T, Hu J K, Wang S. String-based cancelable fingerprint templates. In: Proceedings of the 6th Conference on Industrial Electronics and Applications. Beijing, China: IEEE, 2011. 1028−1033

15 Wong W J, Teoh A B J, Wong M L D, Kho Y H. Enhanced multi-line code for minutiae-based fingerprint template protection. *Pattern Recognition Letters*, 2013, **34**(11): 1221−1229

16 Wang S, Hu J K. Alignment-free cancelable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach. *Pattern Recognition*, 2012, **45**(12): 4129−4137

17 Prasad M V N K, Santhosh K C. Fingerprint template protection using multiline neighboring relation. *Expert Systems with Applications*, 2014, **41**(14): 6114−6122

18 Li Meng-Xing, Feng Quan, Yang Mei, Zhao Jian, He Kang. Garbled circuits based alignment-free fingerprint matching. *Journal of Beijing University of Posts and Telecommunications*, 2014, **37**(6): 81−85
(李梦醒, 冯全, 杨梅, 赵建, 贺康. 基于二进制加密电路的无预对齐指纹匹配. 北京邮电大学学报, 2014, **37**(6): 81−85)

19 Das P, Karthik K, Chandra G B. A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. *Pattern Recognition*, 2012, **45**(9): 3373−3388

20 Tico M, Kuosmanen P. Fingerprint matching using an orientation-based minutia descriptor. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2003, **25**(8): 1009−1014

21 Ahmad T, Hu J K, Wang S. Pair-polar coordinate-based cancelable fingerprint templates. *Pattern Recognition*, 2011, **44**(10−11): 2555−2564

22 Belguechi R, Cherrier E, Rosenberger C, Ait-Aoudia S. An integrated framework combining Bio-Hashed minutiae template and PKCS15 compliant card for a better secure management of fingerprint cancelable templates. *Computers and Security*, 2013, **39**: 325−339

许秋旺 西安邮电大学通信与信息工程学院硕士研究生. 主要研究方向为信息安全. E-mail: xuqiuwang@126.com
(**XU Qiu-Wang** Master student at the School of Communication and Information Engineering, Xi′an University of Posts and Telecommunications. His main research interest is information security.)

张雪锋 博士, 西安邮电大学通信与信息工程学院教授. 主要研究方向为信息安全. 本文通信作者.
E-mail: zhangxuefeng3@163.com
(**ZHANG Xue-Feng** Ph. D., professor at the School of Communication and Information Engineering, Xi′an University of Posts and Telecommunications. His main research interest is information security. Corresponding author of this paper.)