中国科学: 信息科学 2019 年 第 49 卷 第 1 期: 42–56
SCIENTIA SINICA Informationis
论文

基于局部细节点三维映射的指纹模板生成方法

惠妍*, 张雪锋*

西安邮电大学通信与信息工程学院, 西安 710061
* 通信作者. E-mail: huiyan_mini@163.com, zhangxuefeng3@163.com

收稿日期: 2018–01–18; 接受日期: 2018–04–20; 网络出版日期: 2019–01–08

国家自然科学基金 (批准号: 61301091) 和陕西省自然科学基础研究计划项目 (批准号: 2017JQ6010) 资助

摘要 为了提高指纹模板的安全性、不可逆性等性能, 本文设计了一种基于局部细节点三维映射的指纹模板生成方法. 首先对指纹图像进行预处理, 提取指纹的细节点特征, 并采用参数自适应的环形区域对细节点进行筛选, 然后将细节点投影到直线上, 并对投影后的向量集合进行量化、映射和取模运算生成固定长度的二进制比特串, 最后结合用户 PIN 码生成指纹模板. 在指纹数据库 FVC2002-DB1 和 -DB2 上的实验结果表明, 该方法生成的指纹模板在认证性、可撤销性和不可逆性等主要性能上相比几种典型方法更具优势.

关键词 局部细节点, 三维映射, 参数自适应, 比特串, 指纹模板

1 引言

随着信息时代的到来, 越来越多的应用系统需要验证用户的身份信息, 使得身份信息变得越来越重要, 身份信息的安全问题也日益引起人们的关注. 在众多的身份认证技术中, 生物特征识别是指利用人体的行为特征或是生理特征进行身份识别的技术 [1]. 人体的行为特征与后天所养成的行为习惯有关, 包括步态、签名、语音、击键动力等. 人体的生理特征是指人体生理上的固有特性, 包括指纹、掌纹、人脸、虹膜、指静脉、视网膜等. 这些特征均具有良好的唯一性, 能够通过验证来识别用户的身份. 传统的生物特征识别系统是对用户的生物信息进行提取, 然后将生成的模板直接存储到数据库中. 近年来大量的信息泄露事件表明, 随着网络攻击技术的发展, 数据库面临的安全威胁日益严重, 生物特征数据库中存储的大量用户的原始生物信息也面临着泄露的可能, 从而威胁到用户的隐私安全, 因此, 对生物特征模板进行保护变得尤为重要.

目前针对生物特征模板保护的方法主要分两类 [2]: 一类是生物特征加密技术, 这类技术是将生物特征与密钥进行绑定, 生成安全性较高的加密模板; 另一类是可撤销生物识别技术, 这类技术对生物特征进行某种不可逆的变化生成可撤销的模板, 能够较为有效地保护用户生物特征模板中的敏感信息.

引用格式: 惠妍, 张雪锋. 基于局部细节点三维映射的指纹模板生成方法. 中国科学: 信息科学, 2019, 49: 42–56, doi: 10.1360/N112018-00018
Hui Y, Zhang X F. A fingerprint-template-generating method based on the 3D mapping of local minutiae (in Chinese). Sci Sin Inform, 2019, 49: 42–56, doi: 10.1360/N112018-00018

在实际应用过程中, 不同种类的模板保护方法的选择会受到特征种类、特征表示类型和用户间差异的影响 [3], 例如可撤销的生物识别技术适合于指纹、掌纹等特征, 但对于固定长度的虹膜码而言生物特征加密技术则更为适用.

指纹识别是近年来应用最为广泛的生物特征识别技术之一, 但对指纹模板保护技术的研究还有待进一步深入. 当前, 指纹特征可撤销模板保护技术主要分两类 [4], 一类是基于预配准的可撤销指纹模板保护技术. 2004 年, Teoh 等 [5] 提出使用指纹和随机数相结合的双因子身份认证方法, 该算法有较好的识别性能, 但仍存在许多问题, 如难以在指纹中提取算法所要求的定长特征, 不能在随机数丢失的情况下保证认证性等 [6, 7]. 2007 年, Ratha 等 [8] 采用了 Gauss 核函数作为变换函数生成细节点特征模板, 该模板有效地保护了原始指纹特征的安全, 当特征模板受到攻击或者丢失时, 可通过改变函数参数重新发布新的模板并撤销之前发布的模板, 实现了可撤销性. 但 Feng 等 [9] 指出 Ratha 使用的变换函数中存在一一对应的映射关系, 攻击者可通过蛮力攻击、多重记录攻击和解方程法求出部分原始指纹的特征信息. 2008 年, Tulyakov 等 [10] 根据 Hash 函数的对称性和细节点的无序性, 提出使用对称 Hash 函数生成指纹细节点特征模板的方法. 该方法通过将指纹细节点与密钥构建的 Hash 函数进行组合, 增加了模板的安全性. 然而, 当攻击者缩小细节点的值域进行穷举攻击时, 容易造成原始指纹模板信息的泄露. 2011 年, Ahmad 等 [11] 提出将指纹细节点投影到直线上生成可撤销指纹模板的算法, 该算法存在指纹图像需要预配准, 指纹模板认证性能较差等缺点. 综上分析, 这类技术需要确定指纹的奇异点, 将注册指纹模板与验证指纹模板进行预配准后, 才能进行匹配检测.

另一类是免配准的可撤销指纹模板保护技术. 2007 年, Lee 等 [12] 利用指纹细节特征的旋转平移不变性, 生成一种免配准的可撤销指纹模板的方法, 该方法虽然避免了在确定指纹的奇异点时产生的误差, 但不能抵抗 SKIA 攻击. 2010 年, Kim 等 [13] 提出了基于三维数组的可撤销比特串模板生成方法, 随后研究人员相继提出基于极坐标 [14] 和投影 [15] 的比特串模板生成方法, 这些方法都是通过用户特定的令牌实现对比特串的加密, 但由于置换矩阵的可逆性, 当模板被盗时, 量化后的细节点位置就会被恢复. Cappelli 等 [16] 提出一种采用柱形编码特征 (minutia cylinder-code, MCC) 的表示方法, 其思路是利用细节点的旋转平移不变性等优点, 将局部结构由二维扩展到准三维, 增强模板的不可逆性. 但 Ferrara 等 [17] 指出 Cappelli 使用的 MCC 特征本身存在危险, 并证明了通过 MCC 特征反向计算指纹细节点的方法. 2012 年, Wang 等提出分别采用 DITOM 映射 [18] 和循环卷积 [19] 构造一种免对齐的可撤销指纹模板, 该方案的缺点是需要为用户的密钥矩阵提供一个大的存储空间, 而且直接对生成的二进制字符串进行变化, 降低了模板的安全性. 2013 年, Li 等 [20] 提出将一个指纹的细节点位置和另一个指纹的方向信息相融合生成一个组合指纹模板, 并以细节点为基础的二阶匹配方式进行匹配, 实现了对指纹模板安全性的提高, 该方法可以防止攻击者获得用户的真实指纹, 但仍存在许多问题, 如匹配时间较长、匹配性能不稳定等. 2014 年, Moujahdi 等 [21] 提出利用指纹细节点特征的螺旋曲线, 构建一种新的指纹模板 fingerprint shell 的保护方案, 该方案有效地提高了匹配的准确率, 但对提取细节点的精度要求较高, 如果添加一些虚假的细节点, 则构建的曲线将产生巨大变化, 影响识别效果. 2015 年, Sandhya 等 [22] 提出基于 K 邻域结构的免对齐指纹模板保护方法, 该方法是对距离参考细节点最近的 K 个原始细节点特征进行量化和映射, 提高了算法的计算效率, 但模板的安全性和认证性较低, 攻击者容易恢复出真实指纹的细节点信息. 2016 年, Pambudi 等 [23] 提出了基于投影的可撤销指纹模板的方法, 该方法虽然简单但性能不稳定, 其认证性能会随着细节点的增加而降低. 随后 Wang 和 Hu [24] 提出采用盲系统生成二进制比特串指纹模板的方法, 实验证明该方案有效地提高了模板的安全性, 产生更小的失真, 增强了模板的不可逆性. 2017 年, Deng 等 [25] 采用局部 Hadamard 变化实现对指纹特征序列的保护, 其优点是保留了变换后的二进制向量之间的随机距离, 有效地提高了匹配的准确率, 但其

安全性和识别性等性能还有待提高. Wang 等 [26] 提出了基于分区细节点对的可撤销指纹模板的方法, 该方法避免了指纹预对齐时产生的误差, 且提取的局部细节点对非线性失真具有鲁棒性, 但由于直接对细节点特征进行映射, 容易造成原始指纹信息泄露.

现有研究成果表明, 一个理想的可撤销模板需要满足以下要求 [27]: 多样性、可撤销性、安全性和不可逆性. 在现有的可撤销模板保护算法中, 为了提高可撤销模板的认证性, 大多数采用全局细节点进行匹配, 这对非线性的指纹缺乏鲁棒性, 而且计算量较大. 但局部细节点结构可以确保转换后的全局属性不变, 适用于无预配准的全局校准, 较有效地解决了计算量大、认证性差的问题, 在系统中具有更好的应用价值.

基于以上分析, 本文提出一种基于局部细节点三维映射的指纹模板生成方法, 该方法采用参数自适应的环形区域对细节点进行筛选, 通过对指纹细节点进行直线投影, 并对投影后的向量进行量化、映射和取模运算生成指纹模板. 实验结果表明, 该方法即使在模板和参数都泄露的情况下, 也无法恢复出比特串, 而且提取细节点的准确度对系统匹配效果的影响较小, 具有更好的认证性和安全性.

2 三维映射方法

2017 年, Wang 等 [26] 提出了一种基于分区细节点对的可撤销指纹模板的方法, 其主要思想是: 首先从指纹图像中提取细节点特征, 进行预处理生成细节点集 $M=\{m_i\}_{i=1}^{N}$, 其中, $m_i=\{x_i,y_i,\theta_i,t_i\}$. 然后计算细节点之间的相对距离与角度, 并筛选出相对距离不小于预定义阈值的一组细节点. 假设以参考细节点 m_c 为中心, m_i 为 m_c 分区内的一个邻域细节点, 则从细节点对 (m_c,m_i) 中提取的不变特征 V_{ci}, 如下所示:

$$V_{ci}=(l_{ci},\phi_{ci},\delta_{ci}),\quad i=1,\ldots,P_c-1 \text{ and } c=1,\ldots,N, \tag{1}$$

其中, N 为细节点数, P_c-1 为分区内总细节点对数, l_{ci} 和 ϕ_{ci} 分别表示细节点 m_i 和 m_c 的距离和方向角度, δ_{ci} 的计算公式为

$$\delta_{ci}=\begin{cases}\theta_c-\theta_i, & \theta_c\geqslant\theta_i,\\ 2\pi+\theta_c-\theta_i, & \theta_c<\theta_i.\end{cases} \tag{2}$$

最后依次对这些细节点进行三维映射 (细节点的三维映射过程如图 1 所示), 并与用户的 PIN 码相结合, 生成最终的可撤销指纹模板. 实验结果表明, 该方法避免了指纹预对齐时产生的误差, 且提取的局部细节点对非线性失真具有鲁棒性, 但由于直接对细节点特征进行映射, 容易造成原始指纹信息泄露, 而且使用固定阈值对指纹细节点进行筛选, 会降低模板的安全性.

3 本文方法的基本原理

为了避免传统的三维映射方法造成的指纹信息泄露, 本文提出一种对指纹细节点进行参数自适应选取和不可逆变换生成指纹模板的方法, 其基本原理为: 首先对指纹图像进行预处理, 提取指纹的细节点特征; 再任选一个细节点作为参考细节点, 对剩余细节点进行旋转和平移变换, 并采用参数自适应的环形区域对细节点进行筛选; 然后将细节点投影到直线上, 并对投影后的向量集合进行量化、映射和取模运算生成固定长度的二进制比特串; 最后结合用户 PIN 码生成指纹模板.

指纹匹配时, 对验证指纹图像做相同的变换生成验证模板, 通过计算两个模板之间的匹配分数, 验证两个指纹模板之间是否匹配. 本文方法的基本流程如图 2 所示.

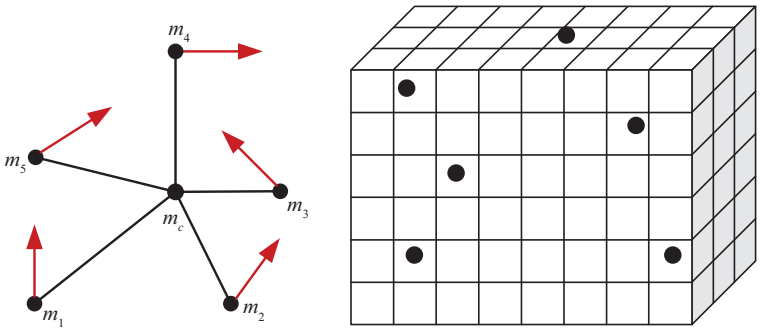

图 1 (网络版彩图) 细节点的三维映射

Figure 1 (Color online) The three-dimensional mapping of minutiae

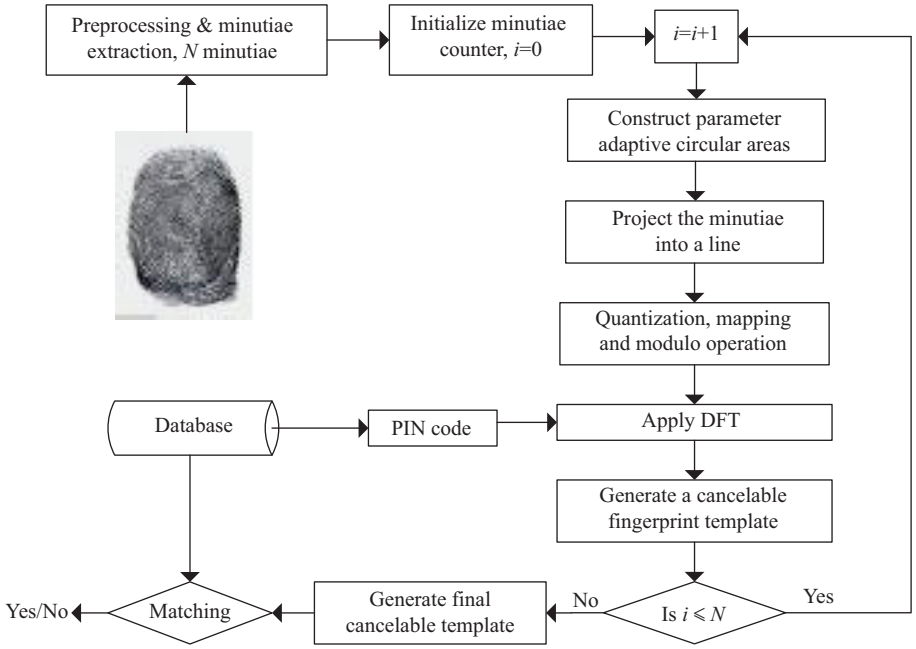

图 2 基于局部细节点三维映射的指纹模板生成方法基本流程

Figure 2 Process diagram of proposed method for fingerprint template generation

3.1 参数自适应的细节点选取

在传统的指纹细节点提取方法中, 主要通过对指纹的所有细节点或固定参数范围内的细节点进行提取, 这导致系统认证时间较长、认证性能较低和安全性较差. 因此, 本文采用参数自适应的环形区域对细节点进行筛选, 该方法可以确保指纹的独特性, 同时有效提高匹配的认证性能.

参数自适应细节点选取的基本过程是: 首先提取指纹的细节点特征, 通过预处理生成细节点集 $M=\{m_i\}_{i=1}^{n}$, 其中, $m_i=\{x_i,y_i,\theta_i\}$, x_i, y_i, θ_i 分别表示第 i 个细节点的位置坐标和方向角度, n 表示从一幅指纹图像中提取的细节点数. 然后从细节点集 M 中任意选取一个细节点 m_i 作为参考细节点, 假设 m_k 为变换后的邻域细节点, 则细节点 m_k 相对细节点 m_i 的距离的表示公式为

$$\mathrm{dis}(m_k,m_i)=\sqrt{(x_k-x_i)^2+(y_k-y_i)^2},\quad k=1,\ldots,n-1. \tag{3}$$

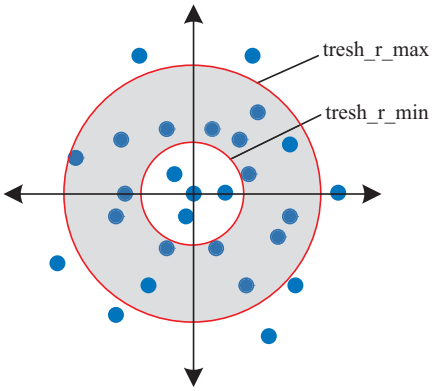

图 3　(网络版彩图) 参数自适应的环形区域

Figure 3　(Color online) Parameter adaptive circular areas

在细节点选取过程中, 考虑到细节点对之间距离较远时, 容易产生非线性失真, 但较近细节点对又容易引起投影误差, 降低模板的匹配性能. 如图 3 所示, 以任意一个细节点 m_i 为圆心, 计算其余细节点相对细节点 m_i 的距离, 进行排序后生成向量 K_i. 根据细节点对之间距离向量 K_i, 计算二个自适应的采样半径参数 tresh_r_min 和 tresh_r_max 的大小, 计算过程如下所示:

$$\begin{cases} \text{tresh\_r\_min} = K_i\lceil (n-3)/2 \rceil, \\ \text{tresh\_r\_max} = K_i(2), \end{cases} \quad i = 1, \ldots, n, \tag{4}$$

其中, n 表示从一幅指纹图像中提取的细节点数, $\lceil \cdot \rceil$ 表示向上取整. 然后筛选出位于环形区域中的细节点, 即当细节点 m_k 相对细节点 m_i 的距离 $\text{dis}(m_k, m_i)$ 满足条件 (5) 时, 将细节点 m_k 作为有效细节点筛选出来, 实现对细节点的选取.

$$\text{tresh\_r\_min} \leqslant \text{dis}(m_k, m_i) \leqslant \text{tresh\_r\_max}. \tag{5}$$

3.2　细节点的投影变化

从细节点集 $M = \{m_i\}_{i=1}^{n}$ 中任意选取一个细节点作为参考细节点, 对其余的有效细节点进行旋转和平移变化, 并计算出变化后的细节点相对参考细节点的位置坐标与角度信息. 再将变化后的细节点投影到直线上: $y = \rho \cdot x + c$, 其中 ρ, c 分别表示直线斜率和截距. 细节点投影的具体步骤如下:

Step 1. 以细节点集 M 中的 m_i 作为参考细节点, 其筛选出的有效细节点数为 r 个. 如图 4 所示, 假设 m_j 为变换后的有效细节点, 则生成的不变特征向量表示为 $(x_{ji}, y_{ji}, \alpha_{ji}, \beta_{ji})$, 其中, x_{ji}, y_{ji} 为细节点 m_j 相对细节点 m_i 的位置坐标, α_{ji}, β_{ji} 分别为细节点对 (m_j, m_i) 的连线沿逆时针方向与自身方向所形成夹角, 其取值范围为 $[0, 2\pi]$ [18].

$$\begin{bmatrix} x_{ji} \\ y_{ji} \end{bmatrix} = \begin{bmatrix} \cos\theta_i & \sin\theta_i \\ \sin\theta_i & -\cos\theta_i \end{bmatrix} \begin{bmatrix} x_j - x_i \\ y_j - y_i \end{bmatrix}, \tag{6}$$

$$\alpha_{ji} = \arctan\frac{y_{ji}}{x_{ji}}, \quad j = 1, \ldots, r; \tag{7}$$

$$\beta_{ji} = \alpha_{ji} + \theta_j - \theta_i, \quad j = 1, \ldots, r. \tag{8}$$

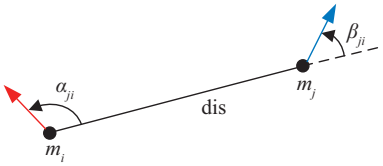

图 4 (网络版彩图) 细节点对连线形成的距离和角度

Figure 4 (Color online) The distance and angle formed by minutiae pair (m_j, m_i)

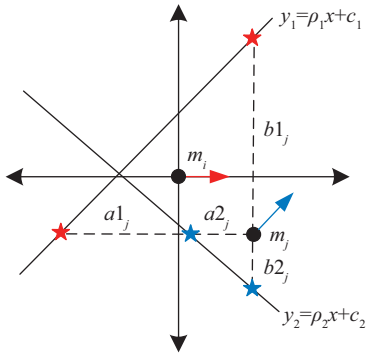

图 5 (网络版彩图) 细节点投影特征

Figure 5 (Color online) Features of projected minutiae

Step 2. 任取两条直线 $y_1 = \rho_1 \cdot x + c_1$ 和 $y_2 = \rho_2 \cdot x + c_2$. 如图 5 所示, 将细节点 m_j 沿水平和垂直方向进行投影, 得到点 m_j 到直线 $y_1 = \rho_1 \cdot x + c_1$ 的水平距离 $a1_j$ 和垂直距离 $b1_j$, 点 m_j 到直线 $y_2 = \rho_2 \cdot x + c_2$ 的水平距离 $a2_j$ 和垂直距离 $b2_j$, 其计算公式为

$$\begin{cases} a = \left| x_{ji} - \dfrac{y_{ji} - c}{\rho} \right|, \\ b = |y_{ji} - \rho \cdot x_{ji} - c|, \end{cases} \quad j = 1, \ldots, r. \tag{9}$$

Step 3. 分别求出投影在二条直线上水平距离和垂直距离的平均值以及角度 $(\alpha_{ji}, \beta_{ji})$ 的平均值, 生成投影特征向量 $(L_{ji}, \gamma_{ji}, \phi_{ji})$, 其中 L_{ji}, γ_{ji} 和 ϕ_{ji} 分别表示平均距离和平均角度.

$$\begin{cases} L_{ji} = (a1_j + b1_j)/2, \\ \gamma_{ji} = (a2_j + b2_j)/2, \\ \phi_{ji} = (\alpha_{ji} + \beta_{ji})/2, \end{cases} \quad j = 1, \ldots, r. \tag{10}$$

Step 4. 以细节点 m_i 为参考细节点, 计算其余的 $r-1$ 个有效细节点相对参考细节点的位置坐标与角度, 并进行投影变化, 生成的投影特征向量为 $\{\omega_i\} = \{(L_{ji}, \gamma_{ji}, \phi_{ji})\}_{j=1}^{r}$.

Step 5. 以不同的细节点作为参考细节点, 进行投影变化, 得到最终投影特征向量集合 ω, 其中 $\{\omega\} = \{\omega_1, \omega_2, \ldots, \omega_n\}$.

3.3 二进制比特串的生成

本小节通过对投影特征向量集合 ω 进行量化和三维映射, 并将生成一维比特串进行取模运算, 从而实现多对一的映射 [26]. 如图 6 所示, 构建一个长为 σ_L, 宽为 σ_γ, 高为 σ_ϕ 的三维网格阵列, 其中 $\sigma_L \in [0, \max(L_{ji})]$, $\sigma_\gamma \in [0, \max(\gamma_{ji})]$, $\sigma_\phi \in [0, 2\pi]$, $\max(L_{ji})$ 和 $\max(\gamma_{ji})$ 表示平均距离的最大值. 在三维网格阵列中, 每个单元格长为 c_L, 宽为 c_γ, 高为 c_ϕ, 并且每个单元格都有各自独立的索引值 (X_{ji}, Y_{ji}, Z_{ji}). 三维网格单元总数为 $g = \omega_L \times \omega_\gamma \times \omega_\phi$, 其中 $\omega_L = \lfloor \max(L_{ji}/c_L) \rfloor$, $\omega_\gamma = \lfloor \max(\gamma_{ji}/c_\gamma) \rfloor$, $\omega_\phi = \lfloor 2\pi/c_\phi \rfloor$, $\lfloor \cdot \rfloor$ 表示向下取整.

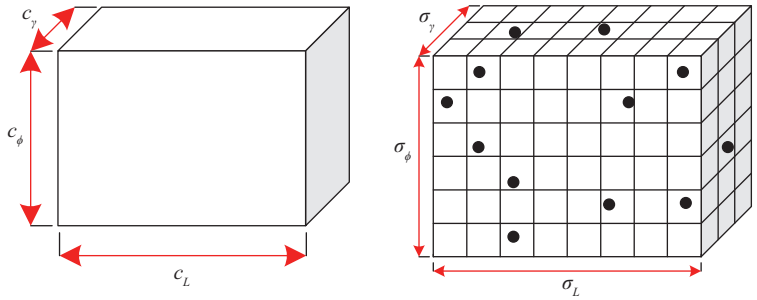

图 6　(网络版彩图) 长为 σ_L, 宽为 σ_γ, 高为 σ_ϕ 的三维网格阵列

Figure 6　(Color online) Three-dimensional array with cell size $\sigma_L, \sigma_\gamma, \sigma_\phi$

首先, 将平均距离 L_{ji}, γ_{ji} 和平均角度 ϕ_{ji} 进行量化后, 映射到三维网格阵列中. 量化公式为

$$\begin{cases} X_{ji} = \lfloor L_{ji}/c_L \rfloor, \\ Y_{ji} = \lfloor \gamma_{ji}/c_\gamma \rfloor, \\ Z_{ji} = \lfloor \phi_{ji}/c_\phi \rfloor, \end{cases} \qquad j = 1, \ldots, r, \tag{11}$$

其中, X_{ji}, Y_{ji} 和 Z_{ji} 表示映射到网格单元上的位置坐标. 依次对每个网格单元进行读取, 若存在特征向量, 则该网格单元的值设为 1, 若没有则为 0, 最终得到长度为 g 的一维比特串 $\overline{b_i}(h)_{h=0}^{g-1}$, 其中 g 为网格单元总数.

然后, 将比特串 $\overline{b_i}(h)$ 的元素一一映射到一个新的二进制比特串 $b_i(k)$ 上, 假设用户的 PIN 码为正整数 G ($G < g$), 其映射公式为

$$b_i(k) = \overline{b_i}(h), \quad k = h \bmod G, \ h = 0, \ldots, g-1. \tag{12}$$

因此, 对参考细节点 m_i 进行变换后, 从 $\{\omega_i\}$ 的不变特征中产生一个长度为 G 的二进制比特串 $b_i(k)_{k=0}^{G-1}$, 其展开后的向量公式为

$$b_i = [b_i(0), b_i(1), \ldots, b_i(G-1)]^{\mathrm{T}}. \tag{13}$$

最后, 将每一个细节点作为参考细节点, 对其他细节点进行三维映射和取模运算, 形成比特串集 $\{b\} = \{b_1, b_2, \ldots, b_n\}$.

3.4　指纹模板的生成

为了提高模板的不可逆性和安全性, 本文通过对固定长度的二进制比特串进行局部 DFT 不可逆变换, 实现对比特串集 $\{b\}$ 的保护. 具体步骤如下.

首先对长度为 G 的二进制比特串 b_i 进行 G 点 DFT 运算后产生复向量 f_i, 具体过程如下:

$$f_i = W \times b_i, \tag{14}$$

其中, $f_i = [f_i(0), f_i(1), \ldots, f_i(G-1)]^{\mathrm{T}}$, f_i 的大小为 $G \times 1$. 由于 DFT 矩阵 $W = \mathrm{e}^{-\mathrm{j}2\pi/G}$ 为酉矩阵, 其

任意两行线性无关且正交, 则该变换为不可逆变换, 矩阵 W 展开式如下:

$$W=\begin{bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & W & W^2 & \cdots & W^{G-1}\\ 1 & W^2 & W^4 & \cdots & W^{2(G-1)}\\ \vdots & \vdots & \vdots & & \vdots\\ 1 & W^{G-1} & W^{2(G-1)} & \cdots & W^{(G-1)(G-1)}\end{bmatrix}. \tag{15}$$

然后利用用户 PIN 码生成伪随机矩阵 R, 并与复向量 f_i 相乘得到模板 T_i, 矩阵 R 的大小为 $P\times Q$, 其中 $P<Q$ 且 $Q=G$.

$$T_i=R\times f_i. \tag{16}$$

最后对所有比特串 $\{b\}=\{b_1,b_2,\ldots,b_n\}$ 进行计算, 得到可撤销指纹模板 $\{T\}=\{T_1,T_2,\ldots,T_n\}$.

在传统的指纹模板生成方法中, 主要通过固定的阈值对细节点进行筛选, 并对原始的细节点特征进行映射, 这导致了模板的安全性较差等问题. 因此, 本文使用参数自适应的环形区域对细节点进行筛选, 即以任意一个细节点为参考细节点, 其采样半径大小都不相同, 确保模板的安全性. 再将筛选出的细节点进行投影、映射、取模处理, 生成可撤销的指纹模板. 在后续的实验中, 将验证该模板能否达到隐藏用户的真实指纹信息的目的.

4 指纹模板匹配

通过计算注册指纹模板和验证指纹模板的匹配分数, 验证两个指纹模板之间是否匹配. 本文借鉴 Xu 和 Zhang [28] 的模板匹配算法, 假设 R^E 为注册指纹, R^Q 为验证指纹, 从注册指纹 R^E 和验证指纹 R^Q 中筛选出的细节点个数分别为 f 和 u. 匹配步骤如下.

Step 1. 对注册指纹 R^E 和验证指纹 R^Q 采用相同的用户 PIN 码, 生成的注册指纹模板和验证指纹模板分别表示为 $T^E=\{T_1^E,T_2^E,\ldots,T_f^E\}$, $T^Q=\{T_1^Q,T_2^Q,\ldots,T_u^Q\}$.

Step 2. 从注册模板 T^E 与验证模板 T^Q 中任意选取一个细节点的特征模板 T_a^E 和 T_b^Q 进行比较, 得出 T_a^E 与 T_b^Q 的局部匹配分数为

$$\mathrm{SA}(T_a^E,T_b^Q)=1-\frac{\|T_a^E-T_b^Q\|_2}{\|T_a^E\|_2-\|T_b^Q\|_2}, \tag{17}$$

其中, $\|\cdot\|_2$ 表示二范数. 将注册模板 T^E 与验证模板 T^Q 进行两两对比后, 生成大小为 $f\times u$ 的局部匹配相似矩阵 $\mathrm{LS}=\{\mathrm{SA}(T_a^E,T_b^Q)\}_{f\times u}$.

Step 3. 通过局部匹配相似矩阵得出 T^E 与 T^Q 之间的最大相似度集合为

$$\mathrm{LSmax}(a)=\max_b(\mathrm{SA}(T_a^E,T_b^Q)),\quad \forall a\in[1,f],\ \forall b\in[1,u], \tag{18}$$

其中, $\max_b(\mathrm{SA}(T_a^E,T_b^Q))$ 表示相似矩阵 LS 每行的最大值. 那么注册模板 T^E 与验证模板 T^Q 的全局匹配分数 GMS 表示为

$$\mathrm{GMS}=\frac{\sum_{a=1}^{f}\mathrm{LSmax}(a)}{\mu}, \tag{19}$$

其中, μ 表示最大相似度集合 LSmax 中非 0 元素的个数且为整数, GMS 的取值范围为 $[0,1]$.

表 1　FVC2002-DB1 和 -DB2 的数据库参数

Table 1　Information about the databases used in our experiments

Characteristics	FVC2002-DB1	FVC2002-DB2
Sensor	Identix TouchViewII (optical)	Biometrika FX2000 (optical)
Number of fingers	100	100
Number of image per finger	8	8
Resolution	500 dpi	569 dpi
Image size	388 × 374	296×560
Quality	Good	Medium

表 2　不同参数的取值范围

Table 2　Parameter settings in the experiments

Parameter	Description	Value range
ρ_1, ρ_2	The slopes of y_1, y_2	$[-5, 5]$
c_1, c_2	The y-intercepts of y_1, y_2	$\{-10, -9, \ldots, 10\}$
c_L, c_γ	The length and width of the cell	$\{15, 16, \ldots, 30\}$
c_ϕ	The height of the cell	$\{20, 21, \ldots, 35\}$
G	The size of binary bit string	$\{200, 250, \ldots, 3000\}$
P	The rows of pseudo-random matrix (R)	$\{300, 400, \ldots, 2000\}$

5　实验结果及分析

为了评估本文方法的效率, 采用指纹库 FVC2002-DB1 和 FVC2002-DB2 在 Matlab R2014a 的开发环境下进行测试和分析, 该数据库的相关参数如表 1 所示.

每个数据库各由 100 个手指样本组成, 共 800 幅指纹图像. 在真匹配实验中, 选取每枚手指的第 1 幅指纹图像作为注册指纹, 相应的第 2 幅指纹图像作为验证指纹, 共进行 $1 \times 100 = 100$ 次真匹配实验. 在假匹配实验中, 选取每枚手指的第 1 幅指纹图像作为注册指纹, 剩余手指的第 2 幅指纹图像作为验证指纹, 共进行 $100 \times 99 = 9900$ 次假匹配实验. 最常用来评价指纹识别系统的主要参数有 4 种: 正确接受率 (genuine accept rate, GAR)、错误拒绝率 (false refuse rate, FRR)、错误接受率 (false accept rate, FAR) 和等错误率 (equal error rate, EER). GAR 是指真实用户通过系统认证的概率, FAR 是攻击者通过系统认证的概率, FRR 是真实用户未通过系统认证的概率, EER 是指 ROC 曲线上 FAR 和 FRR 相等的点, 并作为本文衡量指纹认证系统整体性能的重要指标.

5.1　参数选取对方法性能的影响分析

为了验证相同指纹图像下的不同参数对匹配性能的影响, 本文选择在指纹库 FVC2002-DB1 和 -DB2 中进行匹配实验, 不同参数的取值范围如表 2 所示.

从表 2 中选取参数值, 并在用户 PIN 码安全和泄露两种情况下验证选取的参数对匹配性能的影响. 本小节主要分析当用户 PIN 码泄露时, 二进制比特串长度 G 和伪随机矩阵行数 P 的取值对匹配性能的影响. 理论上, 长度 G 和行数 P 增大时, 系统的匹配性能较好, 但生成的指纹模板中会保留较多原始指纹信息, 从而导致模板的安全性降低. 相反, 当长度 G 和行数 P 减小时, 系统的匹配性能也随之降低, 但模板的安全得到保障. 实验结果如表 3 所示, 当二进制比特串长度 G 取 1450 时, 伪随

表 3 参数 G 和 P 取不同值的 EER (%)

Table 3 EER of different parameters (G, P)

G	P	FVC2002-DB1	FVC2002-DB2
200	300	0.32	0.24
	1000	0.21	0.13
1000	300	0.19	0.08
	1000	0.18	0.07
1450	300	0.17	0.06
	1000	0.15	0.06

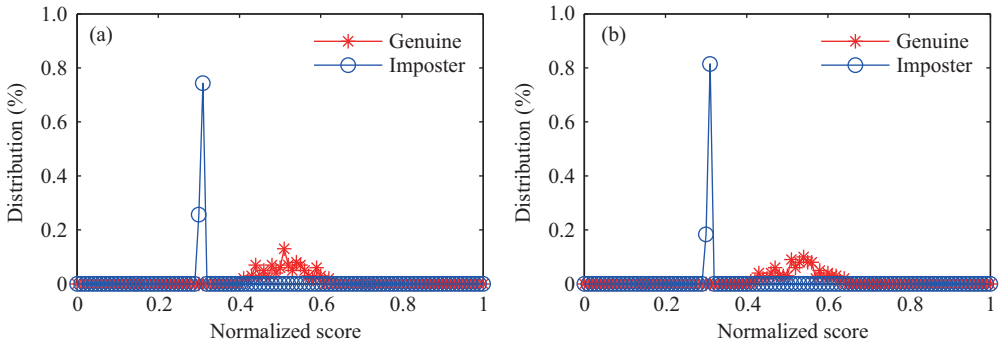

图 7 (网络版彩图) PIN 码安全时真假匹配分布

Figure 7 (Color online) Genuine and imposter distributions in the safe-PIN scenario (with different keys). (a) FVC2002-DB1; (b) FVC2002-DB2

机矩阵行数 P 的大小对模板匹配性能的影响较小, 且在数据库 FVC2002-DB1 和 -DB2 的匹配效果较好. 为了确保模板的安全性和认证性, 本次实验将参数的值选定为 $(1450, 300)$ 来验证方法性能.

5.2 真假匹配分布实验

为了验证本文方法的认证性能, 分别在 FVC2002-DB1 和 -DB2 中针对用户 PIN 码安全和泄露两种情况, 进行了真假匹配实验. 实验参数 (G, P) 分别取 (1450,300), 实验结果如图 7 和 8 所示.

由图 7 和 8 可以看出, 当用户 PIN 码安全时, 两个指纹库的真假匹配分布之间无重叠区域, 这确保了此方法能够准确的区分真假用户. 当用户 PIN 码泄露时, 真假匹配分布在 0.38~0.42 范围内有较小的重叠区域, 说明在进行指纹匹配时, 可能会产生错误匹配, 影响方法的认证性能.

图 9 给出了 PIN 码泄露时, 本文方法分别在 FVC2002-DB1 和 -DB2 的 FRR/FAR 曲线图, 实验的 EER 越低, 方法的认证性能越好. 由图 9 可以看出, 在设定固定阈值的情况下, 数据库 FVC2002-DB2 相比 -DB1 的等错误率略低, 说明本文方法性能受到指纹图像质量的影响较小, 并且具有较强的鲁棒性.

5.3 比较实验分析

通过比较本文方法与现有的免对齐可撤销指纹模板生成方法的性能, 评估本文方法的优势. 首先, 将 Wang 等 [26] 论文中的实验数据与本文方法进行对比. 表 4 给出了 Wang 的方法和本文方法在数据

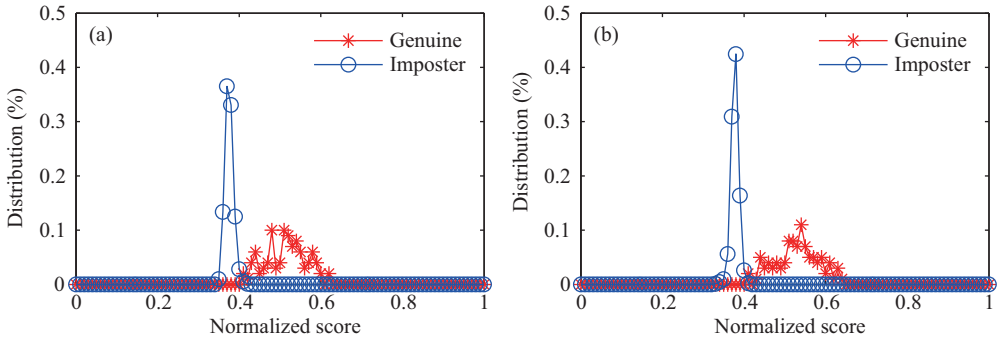

图 8 (网络版彩图) PIN 码泄露时真假匹配分布

Figure 8 (Color online) Genuine and imposter distributions in the stolen-PIN scenario (with the same key). (a) FVC2002-DB1; (b) FVC2002-DB2

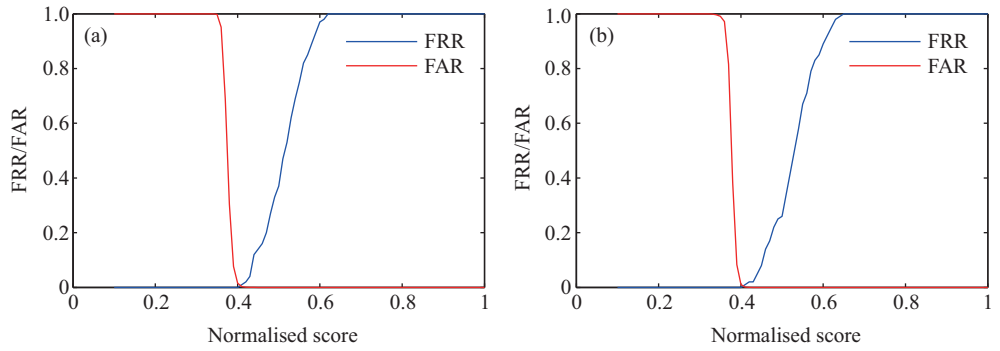

图 9 (网络版彩图) PIN 码泄露时 FVC2002-DB1 和 -DB2 的 FRR/FAR 曲线

Figure 9 (Color online) FRR/FAR of FVC2002-DB1 and -DB2 in the stolen-PIN scenario. (a) FVC2002-DB1; (b) FVC2002-DB2

表 4 采用 Wang 的方法和本文方法的性能比较

Table 4 EER comparison between the Wang's method and proposed method

Methods	Safe-PIN		Stolen-PIN	
	-DB1 (%)	-DB2 (%)	-DB1 (%)	-DB2 (%)
Wang et al. [26]	0	0	0.19	1
Proposed method	0	0	0.1717	0.0606

库 FVC2002-DB1 和 -DB2 的 EER. 实验表明, 当用户 PIN 码安全时, 两种方法的 EER 都达到 0, 当用户 PIN 码泄露时, 本文方法的等错误率小于 Wang 的方法.

本文通过对 Wang 的方法进行实现, 使用 ROC 曲线图清楚地表示两种方法的性能对比. Wang 的方法的实验参数 $(\sigma_l, \sigma_\phi, \sigma_\delta, S, R)$ 分别取 (20, 25, 30, 20000, 300), 密钥 k 则通过 Matlab 随机生成, 本文实验参数 $(\rho_1, \rho_2, c_1, c_2, c_L, c_\gamma, c_\phi, G, P)$ 分别取 (1.19, −0.58, 0, 0, 16, 24, 30, 1450, 300). 图 10 为本文方法与 Wang 的方法在用户 PIN 码泄露时的 ROC 曲线图, ROC 曲线横坐标为错误接受率, 纵坐标为正确接受率. ROC 曲线越接近于 1, 算法的认证性能越好. 实验结果表明, 本文方法较 Wang 的方法有更好认证性能, 能够达到更理想的认证效果.

然后, 引用其他经典算法的认证结果与本文结果进行对比. 表 5 给出了用户 PIN 码泄露的情况

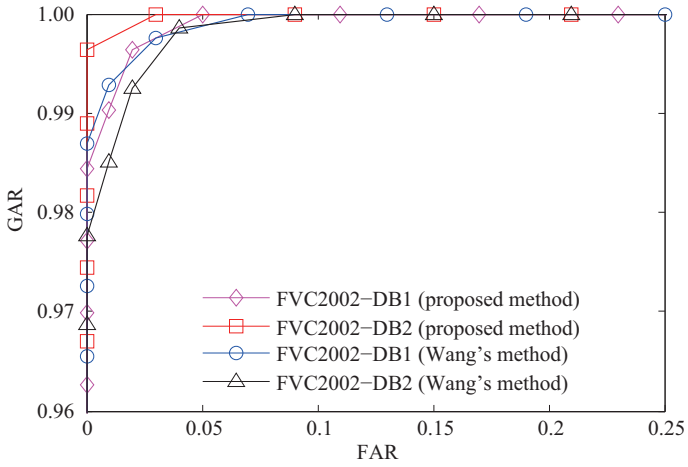

图 10 (网络版彩图) PIN 码泄露时本文方法和 Wang 的方法的 ROC 曲线图

Figure 10 (Color online) ROC curves of Wang's method and proposed method in the stolen-PIN scenario

表 5 不同方法的性能对比 (EER)

Table 5 EER comparison under the stolen-PIN scenario

Method	FVC2002-DB1	FVC2002-DB2
Lee and Kim [13]	10.30	9.50
Jin et al. [15]	5.19	5.65
Sandhya and Prasad [22]	4.71	3.44
Das et al. [29]	2.27	3.79
Jin et al. [30]	4.36	1.77
Wang and Hu [19]	2	2.3
Wang and Hu [24]	3	2
Wang et al. [25]	1	2
Proposed method	0.17	0.06

下, 本文方法与其他 8 种方法在数据库 FVC2002-DB1 和 -DB2 的认证性比较, 本文方法的 EER 分别为 0.17% 和 0.06%, 较其他方法具有明显的优势.

最后, 对本文方法与其他方法的计算效率进行对比分析. 对于一个尺寸为 388×374 的图像来说, 假设提取的细节点数目为 m. 当采用全局细节点生成指纹模板时, 需要对剩余的 $m-1$ 个细节点进行旋转和平移变化. 由于细节点的数量过多, 使得算法的计算量增大. 因此, 本文采用参数自适应的环形区域对细节点进行筛选, 其筛选出的局部细节点数目小于等于 $(m-4)/2$. 即在确保算法认证性能的基础上, 通过减少细节点数目, 使其计算效率得到提高. 同时, 本文通过对生成的一维比特串进行取模运算, 减少比特串的长度, 从而降低系统中数据的存储容量.

5.4 可撤销性分析

变换后模板是否具有可撤销性是指纹安全认证的关键, 一旦模板丢失, 用户可以立即使用同一指纹生成新的变换模板并撤销被攻击的原模板, 确保用户的原始生物信息不会遭到泄露. 为了验证本文模板是否具有可撤销性, 我们在数据库 FVC2002-DB1 和 -DB2 进行伪假匹配实验. 选取每枚手指的一

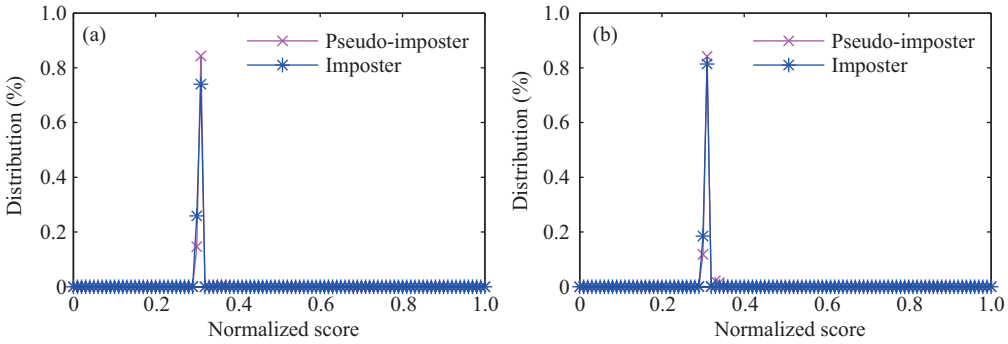

图 11 (网络版彩图) 在 FVC2002-DB1 和 -DB2 中密钥安全、泄露的真假匹配分布

Figure 11 (Color online) Pseudo-imposter and imposter (with different key) distributions for FVC2002-DB1 and -DB2. (a) FVC2002-DB1; (b) FVC2002-DB2

幅指纹图像, 与随机生成的 100 个 PIN 码相结合, 产生 100 个变换的模板. 由于每个数据库各由 100 个手指样本组成, 则一共需要进行 9900 次伪假匹配实验. 实验结果如图 11 所示.

由图 11 可知, 伪假匹配分布与密钥安全时的假匹配分布十分相似, 但仍存在差别. 实验结果表明, 当攻击者获取真实的 PIN 码, 并结合自己的指纹生成可撤销模板时, 不能通过系统认证, 而且即使攻击者使用已撤销的指纹模板, 也不能冒充新的模板通过系统认证.

5.5 安全性分析

指纹模板安全性的衡量标准是攻击者能否从指纹模板中恢复出原始指纹信息, 针对本文方法的安全性进行分析.

首先, 本文采用参数自适应的环形区域对细节点进行筛选, 那么以任意一个细节点为参考细节点, 其筛选的有效细节点的数目基本不同. 因此攻击者在没有获取细节点有效数目情况下, 很难恢复原始指纹信息.

其次, 本文对筛选出的有效细节点进行投影变化生成投影特征向量, 经过变化后的细节点特征与原始指纹细节点特征不再相关. 即使攻击者从变化后的指纹模板中得到细节点投影向量, 也很难恢复真实的指纹细节点信息.

然后, 本文通过对比特串 $\overline{b_i}(j)$ 进行取模和 DFT 运算, 实现多对一的不可逆变换, 同时采用式 (16) 加密生成模板 T_i. 式 (16) 中 R 的大小为 $P \times Q$, f_i 的大小为 $Q \times 1$, 因此该方程组有 P 个方程, 而未知数的个数为 Q 个. 由于方程的秩小于未知数的个数, 即 $\mathrm{rank}(R) = P < Q$, 则该方程存在无穷多个解, 而复向量 f_i 只是无穷多个解中的一个, 所以攻击者很难重构比特串 $\overline{b_i}(j)$.

最后, 当攻击者获取用户真实的 PIN 码, 并结合自己的指纹信息冒充真实用户进行认证时, 由实验可知, 在数据库 FVC2002-DB1 和 -DB2 上成功率不高于 0.18% 和 0.07%, 表明该方法具有良好的安全性.

6 结论

针对可撤销指纹模板保护方法中存在的认证性和安全性较差的问题, 本文设计了一种基于局部细节点三维映射的指纹模板生成方法, 该方法采用参数自适应的环形区域筛选出指纹的局部细节点, 通

过对局部细节点特征进行直线投影, 避免了直接映射造成的用户原始指纹信息泄露, 实现了对指纹模板的保护, 有效提高了系统的认证性能. 理论分析和实验结果表明, 本文方法即使在模板和参数都泄露的情况下, 也无法恢复出比特串, 而且生成的指纹模板在可撤销性、不可逆性和安全性等主要性能上相比其他方法更具优势.

参考文献

1 Nagar A. Biometric template security. Eurasip J Adv Signal Process, 2008, 2008: 1–17
2 Rane S, Wang Y, Draper S C, et al. Secure biometrics: concepts, authentication architectures, and challenges. IEEE Signal Process Mag, 2013, 30: 51–64
3 Patel V M, Ratha N K, Chellappa R. Cancelable biometrics: a review. IEEE Signal Process Mag, 2015, 32: 54–65
4 Kaur G, Singh G, Kumar V. A review on biometric recognition. Int J Bio-Sci Bio-Technol, 2014, 6: 69–76
5 Teoh A B J, Ling D N C, Goh A. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recogn, 2004, 37: 2245–2255
6 Kong A, Cheung K H, Zhang D, et al. An analysis of BioHashing and its variants. Pattern Recogn, 2006, 39: 1359–1368
7 Nanni L, Lumini A. Empirical tests on BioHashing. Neurocomputing, 2006, 69: 2390–2395
8 Ratha N K, Chikkerur S, Connell J H, et al. Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Mach Intel, 2007, 29: 561–72
9 Feng Q, Su F, Cai A N, et al. Cracking cancelable fingerprint template of ratha. In: Proceedings of IEEE International Symposium on Computer Science and Computational Technology, 2008. 572–575
10 Tulyakov S, Farooq F, Mansukhani P, et al. Symmetric hash functions for secure fingerprint biometric systems. Pattern Recogn Lett, 2007, 28: 2427–2436
11 Ahmad T, Hu J K. Generating cancelable biometrie templates using a projection line. In: Proceedings of IEEE International Conference on Control Automation Robotics & Vision, 2011. 7–12
12 Lee C, Choi J Y, Toh K A, et al. Alignment-free cancelable fingerprint templates based on local minutiae information. IEEE Trans Syst Man Cybern, 2007, 37: 980–992
13 Lee C, Kim J. Cancelable fingerprint templates using minutiae-based bit-strings. J Netw Comput Appl, 2010, 33: 236–246
14 Ahmad T, Hu J K, Wang S. String-based cancelable fingerprint templates. In: Proceedings of IEEE International Conference on Industrial Electronics and Applications, 2011. 1028–1033
15 Jin Z, Jin Teoh A B, Ong T S, et al. Fingerprint template protection with minutiae-based bit-string for security and privacy preserving. Expert Syst Appl, 2012, 39: 6157–6167
16 Cappelli R, Ferrara M, Maltoni D. Minutia cylinder-code: a new representation and matching technique for fingerprint recognition. IEEE Trans Pattern Anal Mach Intel, 2010, 32: 2128–2141
17 Ferrara M, Maltoni D, Cappelli R. Noninvertible minutia cylinder-code representation. IEEE Trans Inform Foren Secur, 2012, 7: 1727–1737
18 Wang S, Hu J. Alignment-free cancelable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach. Pattern Recogn, 2012, 45: 4129–4137
19 Wang S, Hu J. Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. Pattern Recogn, 2014, 47: 1321–1329
20 Li S, Kot A C. Fingerprint combination for privacy protection. IEEE Trans Inf Foren Sec, 2013, 8: 350–360
21 Moujahdi C, Bebis G, Ghouzali S, et al. Fingerprint shell: secure representation of fingerprint template. Pattern Recogn Lett, 2014, 45: 189–196
22 Sandhya M, Prasad M V N K. K-nearest neighborhood structure (k-NNS) based alignment-free method for fingerprint template protection. In: Proceedings of IEEE International Conference on Biometrics, 2015. 386–393
23 Pambudi D S, Ahmad T, Usagawa T. Improving the performance of projection-based cancelable fingerprint template method. In: Proceedings of IEEE International Conference on Soft Computing and Pattern Recognition, 2016. 84–88
24 Wang S, Hu J. A blind system identification approach to cancelable fingerprint templates. Pattern Recogn, 2016, 54: 14–22

25 Wang S, Deng G, Hu J. A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. Pattern Recogn, 2017, 61: 447–458
26 Wang S, Yang W, Hu J. Design of alignment-free cancelable fingerprint templates with zoned minutia pairs. Pattern Recogn, 2017, 66: 295–301
27 Adámek M, Matýsek M, Neumann P. Security of biometric systems. Procedia Eng, 2015, 100: 169–176
28 Xu Q W, Zhang X F. Generating cancelable fingerprint templates using minutiae local information. Acta Automat Sin, 2017, 43: 645–652 [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: 645–652]
29 Das P, Karthik K, Chandra Garai B. A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. Pattern Recogn, 2012, 45: 3373–3388
30 Jin Z, Lim M H, Teoh A B J, et al. A non-invertible randomized graph-based Hamming embedding for generating cancelable fingerprint template. Pattern Recogn Lett, 2014, 42: 137–147

A fingerprint-template-generating method based on the 3D mapping of local minutiae

Yan HUI* & Xuefeng ZHANG*

School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710061, *China*
* Corresponding author. E-mail: huiyan_mini@163.com, zhangxuefeng3@163.com

Abstract To enhance the security and irreversibility performance of the fingerprint template, a fingerprint-template-generating method is proposed based on the 3D mapping of local minutiae. First, we extract fingerprint minutiae features after preprocessing the fingerprint image and select the minutiae using parameter adaptive circular areas. Second, we project the minutiae into a line. Subsequently, quantization, mapping, and modulo operation are performed on the projected vectors to generate a fixed-length binary bit string. Finally, a fingerprint template is generated by combining the user's PIN code with a binary bit string. The experiments performed on FVC2002-DB1 and DB2 show that this template has advantages over the traditional ones in terms of recognition, revocation, non-invertibility, and performance.

Keywords local minutiae, three-dimensional mapping, parameter adaptive, bit-string, fingerprint template

Yan HUI was born in 1995. She is currently earning an M.S. degree in the School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications. Her main research interest is cancelable biometrics.

Xuefeng ZHANG was born in 1975. He obtained his Ph.D. degree in Xi'an University of Electronic Science and Technology. He is currently a professor in the School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications. His research interests focus on information security and biometric recognition.