基于细节点投影的可撤销指纹模板生成算法

惠 妍 [1] 张雪锋 [1]

摘 要 为了改善指纹模板保护算法的可撤销性、不可逆性等性能, 设计了一种基于细节点投影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, 并筛选出采样半径范围内的有效细节点, 然后对细节点进行直线投影, 将投影后的向量映射到二维网格, 生成固定长度的一维比特串, 再结合用户 PIN 码生成可撤销指纹模板. 在指纹数据库 FVC2002-DB1 和 DB2 上的实验结果表明, 该算法不仅提高了指纹模板认证的稳定性, 而且在可撤销性、不可逆性和安全性等方面均具有较好性能.

关键词 细节点, 投影, 采样半径, 可撤销模板

引用格式 惠妍, 张雪锋. 基于细节点投影的可撤销指纹模板生成算法. 自动化学报, 2020, **46**(3): 585−593

DOI 10.16383/j.aas.2018.c170604

A Cancelable Fingerprint Template Generating Algorithm Using Minutiae Projection

HUI Yan[1] ZHANG Xue-Feng[1]

Abstract In order to enhance the revocation and irreversibility performance of the fingerprint template protection algorithm, a cancelable fingerprint template generating algorithm is proposed using minutiae projection. Firstly, we extract fingerprint minutiae feature after preprocessing the fingerprint image and select the effective minutiae within the range of the sampling radius. Next, we project the minutiae into a line and map the projected vectors onto a 2D grid to generate a fixed length 1D bit-string. Finally, the cancelable fingerprint template is generated by combining the user PIN code. Experiments performed on FVC2002-DB1 and DB2 show that the algorithm not only improves the stability of the template authentication but also satisfies revocation as well as non-invertibility, and ensures the security of the algorithm.

Key words Minutiae, projection, sample radius, cancelable template

Citation Hui Yan, Zhang Xue-Feng. A cancelable fingerprint template generating algorithm using minutiae projection. *Acta Automatica Sinica*, 2020, **46**(3): 585−593

随着网络和信息技术的发展和普及, 信息的安全问题变得越来越重要. 在众多的信息安全技术中, 生物特征识别技术是指通过人体的行为特征、生理特征等生物特征信息进行身份认证的方式, 常见的生物特征包括指纹、掌纹、人脸、虹膜、指静脉、视网膜和手写签名等特征, 这些特征是独一无二且不易伪造的[1]. 近年来, 随着基于指纹、掌纹、人脸等生物特征的身份认证技术被广泛使用, 生物特征识别技术的安全问题也日益凸显, 成为信息安全领域的一个研究热点.

现有的针对生物特征的攻击分为四种[2]: 传感器攻击、传感器和模块间的攻击、软件攻击和生物特征模板攻击. 其中生物特征模板攻击会造成用户的原始生物信息泄露, 威胁到用户的隐私安全. 鉴于生物特征具有的唯一性和不可变更性, 一旦泄露将对用户的个人隐私造成永久威胁, 因此, 对生物特征模板进行保护变得尤为重要.

目前应用较为广泛的模板保护方法包括: 生物特征加密技术和可撤销生物识别技术[3]. 生物特征加密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. 2002 年, Juels 等[4] 提出了 Fuzzy Vault 方案, 它是指纹特征加密技术最经典的方案, 该方案可以很好地将指纹特征与密码算法相结合, 实现对指纹特征的保护. 而可撤销生物识别技术是对生物特征进行某种不可逆的变化生成可撤销的模板, 其中指纹特征的可撤销模板保护技术主要分二类[5], 一类是基于预配准的可撤销指纹模板保护技术, 2004 年, Jin 等[6] 提出一种基于 BioHashing 的可撤销生物认证方案, 该方案将用户的特征向量与存储在用户身份令牌中的一组伪随机数进行迭代

收稿日期 2017-11-01 录用日期 2018-05-28
Manuscript received November 1, 2017; accepted May 28, 2018
国家自然科学基金 (61301091), 陕西省自然科学基础研究计划青年项目 (2017JQ6010) 资助
Supported by National Natural Science Foundation of China (61301091) and Natural Science Basic Research Plan in Shaanxi Province of China (2017JQ6010)
本文责任编委 左旺孟
Recommended by Associate Editor ZUO Wang-Meng
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

内积, 产生一组 BioCode 码. 实验证明, 该方案具有良好的安全和识别性能, 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[7−8]. 2007 年, Ratha 等[9] 针对指纹特征采用不可逆变换函数生成可撤销模板, 使得变化后的特征无法恢复出原始指纹的特征信息, 当可撤销模板被盗时, 可通过改变函数参数生成新的可撤销模板, 从而确保生物特征信息的安全性. 但 Feng 等[10] 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.

另一类是免配准的可撤销指纹模板保护技术, 2007 年, Lee 等[11] 提出一种免配准的可撤销指纹模板的方法. 该方法虽然避免了指纹预配准所产生的误差, 但增加了密钥泄露时模板遭受攻击的风险. 2010 年, Lee 等[12] 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[13] 和投影[14] 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. 2012 年, Wang 等[15] 采用 DITOM 映射构造了一种免对齐的可撤销指纹模板, 之后又提出基于循环卷积生成二进制字符串的构造方法[16], 通过实验证明该模板的安全性较高, 即使在模板和参数都泄露的情况下, 也无法恢复出二进制串. 2015 年, Sandhya 等[17] 提出基于 K 邻域结构的免对齐指纹模板保护方法. 2016 年, Pambudi 等[18] 提出了基于投影的可撤销指纹模板生成方法, 该方法避免了指纹预配准时产生的误差, 且提取的局部细节点对非线性失真具有鲁棒性, 但其安全性和识别性等性能还有待提高. 2017 年, 许秋旺等[19] 设计了一种基于细节点邻域信息的可撤销指纹模板生成方法, 该方法拓展了细节点描述子的采样结构, 对系统的识别性能有所改善, 具有较好的实用性.

因此, 为了避免指纹预配准时产生的误差, 以及直接映射造成的用户原始指纹信息泄露, 本文利用指纹细节点特征的旋转平移不变性, 对细节点进行处理, 并将处理后的细节点通过投影、映射和加密生成可撤销的指纹模板. 实验结果表明, 该算法生成的指纹模板不仅满足可撤销性、不可逆性、多样性和安全性, 而且具有较好的认证性能.

1 Pambudi 方法

2016 年, Pambudi 等在文献 [18] 中提出了基于投影的可撤销指纹模板生成方法, 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. 然后任意选取一个细节点作为参考细节点, 计算并提取在采样半径范围内的其他细节点相对于参考细节点的距离与角度. 最后根据密钥依次对这些细节点进行水平和垂直方向上的投影等变换, 生成向量集合 $\{\boldsymbol{v}\}$ 作为最终的可撤销指纹模板. 细节点的投影特征如图 1 所示.

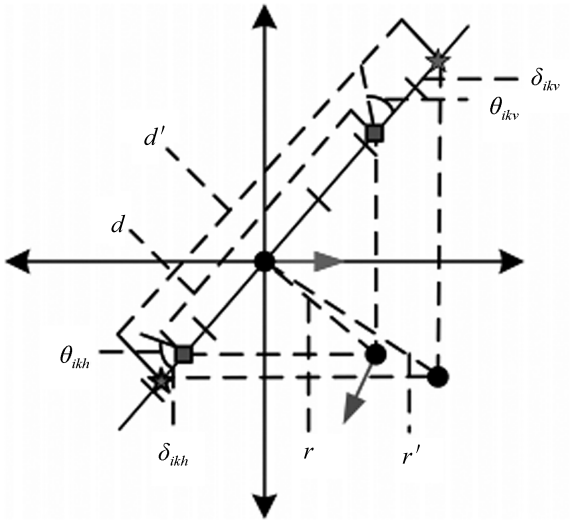


图 1 细节点的投影特征

Fig. 1 Features of projected minutiae

假设 m_i 为参考细节点, m_k 为 m_i 的一个邻域细节点, 则变换后的向量集合 $\{\boldsymbol{v}\}$, 如式 (1) 所示.

$$\{\boldsymbol{v}\}_i^n = \left\{ \begin{array}{c} (r'_{i1}, d'_{i1}, \theta_{i1v}, \theta_{i1h}, \delta_{i1v}, \delta_{i1h}) \\ \vdots \\ (r'_{n1}, d'_{n1}, \theta_{n1v}, \theta_{n1h}, \delta_{n1v}, \delta_{n1h}) \end{array} \right\} \quad (1)$$

其中, n 为细节点数, r'_{ik} 和 d'_{ik} 分别表示变换后的点与参考细节点 m_i 的距离和投影直线上二点距离. θ_{ikv} 和 θ_{ikh} 表示水平和垂直投影点的方向, δ_{ikv} 和 δ_{ikh} 表示投影点的索引.

实验结果表明, 该方法生成的模板具有良好的识别性能, 如等错误率为 1 % 等. 但方法中存在一些缺点: 首先, 在投影过程中提取的指纹特征较多, 这容易造成指纹信息泄露, 而且计算量较大. 其次, 该方法虽然对细节点特征进行了变换, 但模板中仍包含有原始指纹的信息, 如 θ_{ikv} 和 θ_{ikh}. 因此当系统遭受攻击时, 模板的安全性受到威胁. 最后, 由匹配结果可知, 进行模板匹配的细节点数目多少, 对模板的认证性能影响较大, 这对于图像质量较差, 提取细节点的精度较低的指纹来说, 效果可能并不理想.

2 本文提出的算法

为了改进算法的稳定性和认证性, 本文提出基于细节点投影的可撤销指纹模板生成算法, 主要包

括指纹模板的生成和指纹匹配二个阶段. 指纹模板的生成过程为: 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, 并筛选出采样半径范围内的有效细节点; 然后对其进行直线投影, 将投影后的向量集合量化并映射到一个二维极坐标网格中生成固定长度的一维比特串; 最后结合用户 PIN 码生成可撤销指纹模板. 指纹匹配时, 对验证指纹图像做相同的变换生成验证指纹模板, 计算二个模板之间的匹配分数, 得出最终结果.

本文算法的基本流程如图 2 所示.

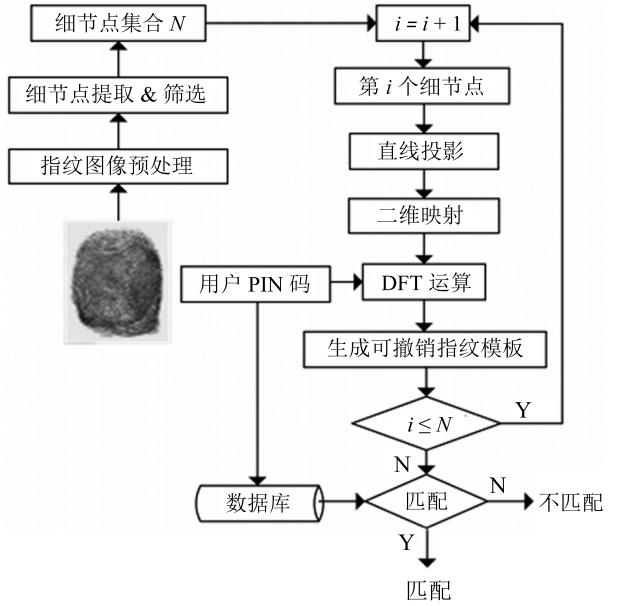


图 2　基于细节点投影的可撤销指纹模板生成算法基本流程

Fig. 2　Process diagram of proposed method for fingerprint template generation

2.1　细节点的变换

首先提取指纹的细节点特征进行预处理, 并生成细节点集 $M=\{m_i\}_{i=1}^{n}$, 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, 求出其余 $n-1$ 个细节点相对参考细节点的距离与角度. 如图 3 所示, 设 m_c 为变换后的细节点, x_{ci}, y_{ci} 和 d_{ci} 分别为细节点 m_c 相对细节点 m_i 的位置坐标和距离, α_{ci} 和 β_{ci} 分别为细节点对 (m_c, m_i) 的连线沿逆时针方向与自身方向所形成夹角[16].

$$\begin{cases} x_{ci}=(x_c-x_i)\cos\theta_i+(y_c-y_i)\sin\theta_i \\ y_{ci}=(x_c-x_i)\sin\theta_i-(y_c-y_i)\cos\theta_i \end{cases} \tag{2}$$

$$d_{ci}=\sqrt{x_{ci}^2+y_{ci}^2}, \qquad c=1,2,\cdots,n-1 \tag{3}$$

$$\alpha_{ci}=\arctan\frac{y_{ci}}{x_{ci}}, \qquad c=1,2,\cdots,n-1 \tag{4}$$

$$\beta_{ci}=\alpha_{ci}+\theta_c-\theta_i, \qquad c=1,2,\cdots,n-1 \tag{5}$$

在投影过程中, 为了避免变换后的细节点与参考点的距离太近而产生投影误差, 应对细节点进行筛选[18]. 当所选取的细节点过多时会增加认证时间, 但过少的细节点会减弱指纹的独特性, 因此应该获取足够多的细节点, 使其能够代表整个指纹数据库的特性.

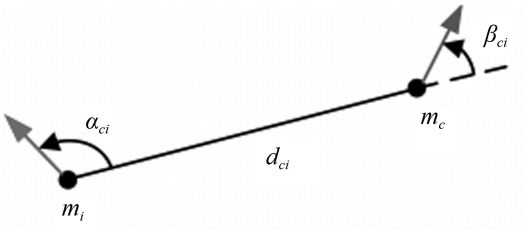


图 3　细节点对连线形成的距离和角度

Fig. 3　The distance and angle formed by minutiae pair

如图 4 所示, 以任意一个细节点 m_i 为圆心, 以 $t\_\min$ 和 $t\_\max$ 为采样半径作圆, 筛选出位于二个圆形区域之间的细节点. 当细节点 m_c 相对细节点 m_i 的距离 d_{ci} 满足条件 (6) 时, 将细节点 m_c 作为有效细节点筛选出来.

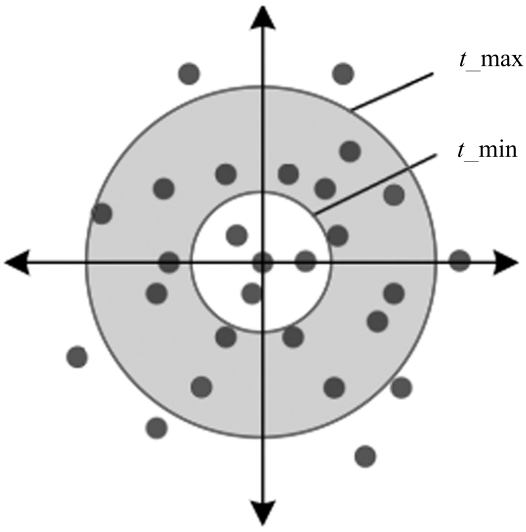


图 4　细节点的选取

Fig. 4　Minutiae selection process

$$t\_\min \le d_{ci} \le t\_\max \tag{6}$$

假设满足条件 (6) 的有效细节点个数为 r, 则以细节点 m_i 作为参考点生成集合 $p_i=\{(x_{ji}, y_{ji}, \alpha_{ji},$

$\beta_{ji})\}_{j=1}^{r}$, 其中, x_{ji} 和 y_{ji} 分别为细节点 m_j 相对参考细节点 m_i 的位置坐标, α_{ji} 和 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角度.

2.2 细节点的直线投影

以细节点 m_i 为中心建立一个新的坐标轴, 将细节点 $m_j(x_{ji}, y_{ji}, \alpha_{ji}, \beta_{ji})$ 投影到直线上: $y = \rho x + c$, 其中 ρ 和 c 分别表示直线斜率和截距. 在本文算法中, 对直线角度 θ 分别取 50° 和 150°, c 取 0, 具体投影步骤如下:

步骤 1. 取 $\theta = 50°$, 如图 5 所示, 先将细节点 m_j 沿水平和垂直方向进行投影, 得到点 m_j 到直线的水平距离 a 和垂直距离 b, 再计算出细节点 m_j 投影到直线上二点的距离 $r1_{ji}$.

$$a = |x_{ji} - \frac{y_{ji}}{\tan\theta}|, \qquad j = 1, 2, \cdots, r \tag{7}$$

$$b = |y_{ji} - x_{ji}\tan\theta|, \qquad j = 1, 2, \cdots, r \tag{8}$$

$$r1_{ji} = \sqrt{a^2 + b^2}, \qquad j = 1, 2, \cdots, r \tag{9}$$

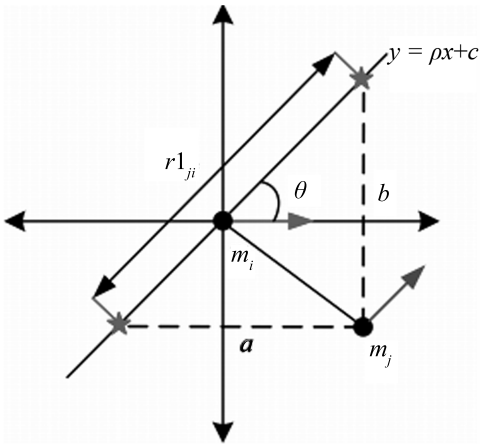


图 5 细节点的投影变化

Fig. 5 The transformation of minutiae projection

步骤 2. 取 $\theta = 150°$, 对细节点做同样变换, 并计算细节点 m_j 投影到直线上二点的距离 $r2_{ji}$.

步骤 3. 分别求出距离 $r1_{ji}, r2_{ji}$ 的平均值和角度 α_{ji}, β_{ji} 的平均值, 得到细节点的投影特征 (L_{ji}, ϕ_{ji}), 其中 L_{ji} 和 ϕ_{ji} 分别表示平均距离和平均角度.

$$L_{ji} = \frac{r1_{ji} + r2_{ji}}{2} \tag{10}$$

$$\phi_{ji} = \frac{\alpha_{ji} + \beta_{ji}}{2} \tag{11}$$

步骤 4. 以细节点 m_i 为参考细节点, 对 r 个细节点投影后, 形成的投影特征集合 $\{w_i\} = \{(L_{ji}, \phi_{ji})\}_{j=1}^{r}$. 再分别以不同的细节点作为参考细节点, 进行投影, 形成最终投影特征集 w, 其中 $\{w\} = \{w_1, w_2, \cdots, w_n\}$.

2.3 一维比特串的生成

针对投影特征集 w 进行映射时, 需要构建一个二维网格阵列.

如图 6 所示, 构建一个长为 σ_L, 宽为 σ_ϕ 的二维网格阵列, 其中 $\sigma_L \in [0, \max(L_{ji})]$, $\sigma_\phi \in [0, 2\pi]$, $\max(L_{ji})$ 表示平均距离的最大值. 在二维网格阵列中, 每个单元格长为 c_L, 宽为 c_ϕ. 二维网格单元总数为 $g = \omega_L \times \omega_\phi$, 其中 $\omega_L = \lfloor \max(L_{ji})/c_L \rfloor$, $\omega_\phi = \lfloor 2\pi/c_\phi \rfloor$, $\lfloor \cdot \rfloor$ 表示向下取整.

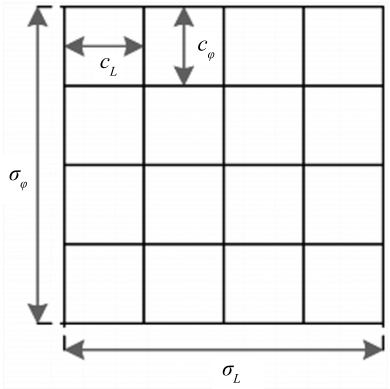


图 6 长 $= \sigma_L$、宽 $= \sigma_\phi$ 的二维网格阵列

Fig. 6 Two-dimensional array with cell size σ_L, σ_ϕ

将平均距离 L_{ji} 和平均角度 ϕ_{ji} 进行量化后, 映射到二维网格阵列中. 量化公式为

$$X_{ji} = \left\lfloor \frac{L_{ji}}{c_L} \right\rfloor, \quad j = 1, 2, \cdots, r \tag{12}$$

$$Y_{ji} = \left\lfloor \frac{\phi_{ji}}{c_\phi} \right\rfloor, \quad j = 1, 2, \cdots, r \tag{13}$$

其中, X_{ji} 和 Y_{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, 若没有特征向量则为 0, 最终得到长度为 g 的一维比特串 $b_i(j)_{j=0}^{g-1}$, 其中 g 为网格单元总数. 再将每一个细节点作为参考细节点, 对其他细节点进行映射, 形成比特串集 $\{b\} = \{b_1, b_2, \cdots, b_n\}$.

2.4 可撤销指纹模板的生成

为了防止攻击者通过非法手段获得用户指纹特征模板后, 还原出用户的原始指纹信息. 本文通过对

固定长度的一维比特串进行 DFT 运算后, 再与用户 PIN 码结合打乱比特串的排列顺序, 生成可撤销指纹模板[17]. 具体步骤为:

步骤 1. 对长度为 g 的一维比特串 b_i 进行 g 点 DFT 运算后产生复向量 $\boldsymbol{v}_i$, 如式 (14) 所示, $\boldsymbol{v}_i$ 的大小为 $g \times 1$.

$$\boldsymbol{v}_i = \sum_{s=0}^{g-1} b_i \mathrm{e}^{\frac{-j2\pi ts}{g}}, \quad t = 0, 1, \cdots, g-1 \tag{14}$$

步骤 2. 利用用户 PIN 码生成伪随机矩阵 $R_{p\times q}$, 并与复向量 $\boldsymbol{v}_i$ 相乘得到模板 T_i, 其中 $p < q$ 且 $q = g$.

$$T_i = R \times \boldsymbol{v}_i \tag{15}$$

步骤 3. 对所有比特串 $\{b\} = \{b_1, b_2, \cdots, b_n\}$ 进行计算得到可撤销指纹模板 $T = \{T_1, T_2, \cdots, T_n\}$.

因此, 为了避免指纹模板中包含有原始指纹信息等问题, 本文在对细节点进行投影时, 在确保认证性较好的前提下, 提取较少的投影向量, 并采用二维映射的方法对投影后的向量进行处理, 使得用户的原始指纹信息能够被较好的隐藏. 在对指纹模板进行加密时, 采用 DFT 运算并与用户 PIN 码结合, 实现多对一的不可逆变换, 加强了指纹模板的安全性.

3　指纹模板匹配

指纹模板的匹配是通过对注册指纹模板和验证指纹模板进行比较, 产生最终的匹配分数, 其取值范围为 0 到 1. 本文参照文献 [19] 的模板匹配算法, 并根据算法的匹配效果, 对最终的匹配方程进行修改. 假设为 R^E 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 中筛选出的有效细节点个数分别为 f 和 u. 匹配步骤如下:

步骤 1. 对注册指纹 R^E 和验证指纹 R^Q 采用相同的用户 PIN 码, 生成注册指纹模板 $T^E = \{T_1^E, T_2^E, \cdots, T_f^E\}$ 和验证指纹模板 $T^Q = \{T_1^Q, T_2^Q, \cdots, T_u^Q\}$.

步骤 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映射模板 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

$$SA(T_a^E, T_b^Q) = 1 - \frac{\|T_a^E - T_b^Q\|_2}{\|T_a^E\|_2 - \|T_b^Q\|_2} \tag{16}$$

其中, $\|\cdot\|_2$ 表示 2 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 LS 表示为

$$\begin{bmatrix} SA(T_1^E, T_1^Q) & SA(T_1^E, T_2^Q) & \cdots & SA(T_1^E, T_u^Q) \\ SA(T_2^E, T_1^Q) & SA(T_2^E, T_2^Q) & \cdots & SA(T_2^E, T_u^Q) \\ \vdots & \vdots & \ddots & \vdots \\ SA(T_f^E, T_1^Q) & SA(T_f^E, T_2^Q) & \cdots & SA(T_f^E, T_u^Q) \end{bmatrix} \tag{17}$$

步骤 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

$$LS\max(a) = \max_b(SA(T_a^E, T_b^Q)) \tag{18}$$

其中, $\max_b(SA(T_a^E, T_b^Q))$ 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

$$GMS = \frac{\sum_{a=1}^{f} LS\max(a)}{\mu} \tag{19}$$

其中, μ 表示最大相似度集合 $LS\max$ 中非 0 元素的个数且为整数. 当 $GMS \geq Th$ 时, 系统认定注册模板 T^E 与验证模板 T^Q 匹配, 其中 Th 为最优阈值.

4　实验结果及分析

为了评估本算法的效率, 采用指纹库 FVC2002-DB1 和 FVC2002-DB2 进行测试, 该数据库各由 100 个手指样本组成, 每个手指样本有 8 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 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 9 900 次假匹配实验. 评价指纹识别系统的主要指标是正确接受率 (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).

4.1　参数选取对算法性能的影响分析

为了验证相同指纹图像下的不同采样半径长度 $t\_\min$ 和 $t\_\max$、网格单元长度 c_x 和 c_y 对匹配性能的影响, 我们选择在指纹库 FVC2002-DB1 中进行匹配实验训练, 并通过指纹库 FVC2002-DB2 测试选取的参数在本文算法的实验效果. 不同参数的取值范围如表 1 所示.

表 1 不同参数的取值范围
Table 1 Parameter settings in the experiments

参数	参数描述	参数范围
$t\_\min$	最小采样半径	$\{6,7,\cdots,13\}$
$t\_\max$	最大采样半径	$\{100,110,\cdots,160\}$
c_x	网格单元的长	$\{10,11,\cdots,15\}$
c_y	网格单元的宽	$\{8,9,\cdots,12\}$

从表 1 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在 FVC2002-DB1 中对匹配性能的影响. 因为等错误率越低, 算法的认证性能越好, 所以本文采用等错误率来评价算法的性能. 如表 2 所示, 当用户 PIN 码安全时, 不同参数下的 EER 相等且接近于 0, 这确保了指纹匹配的稳定性. 当用户 PIN 码泄露时, 不同参数下算法的 EER 不同. 经过分析, 当参数 $(t\_\min, t\_\max, c_x, c_y)$ 分别取 (11, 140, 13, 9) 时, DB1 的 EER 最低, 匹配效果达到最佳, 所以将该参数选为数据库 DB1 的最优参数.

表 2 不同参数在 FVC2002-DB1 下的 EER (%)
Table 2 EER of different parameters for FVC2002-DB1 (%)

$(t\_\min, t\_\max)$	(c_x, c_y)	PIN 码安全	PIN 码泄露
(7,100)	(10 ,8)	0	3.38
	(13, 9)	0	3.63
(9,120)	(12, 9)	0	3.12
	(14, 10)	0	3.37
(11, 140)	**(13,9)**	**0**	**2.56**
	(13, 10)	0	3.14
(13,160)	(11, 11)	0	3.08
	(12, 11)	0	3.18

为了验证所选取的参数, 在其他指纹库中也能表现出较好的认证性, 本文在数据库 DB2 中进行测试. DB2 中参数的取值范围与 DB1 相同, 测试结果表明, 当参数 $(t\_\min, t\_\max, c_x, c_y)$ 取 (11, 140, 13, 9) 时, 其 EER 在用户 PIN 码安全和泄露情况下分别为 0 % 和 1.16 %, 相比其他参数能达到较好的匹配效果. 因此, 当实验参数 $(t\_\min, t\_\max, c_x, c_y)$ 取 (11, 140, 13, 9) 时, 确保了两个指纹库中均表现出较理想的匹配性能.

理论上, 网格单元长度 c_x 和 c_y 越小, 一维比特串长度越长, 模板匹配的准确度越高. 但从实验结果可以看出, 匹配准确度不仅由网格单元的长度决定, 它可能同时受到其他因素的影响, 如图像质量的好坏、提取细节点的精度和有效细节点的个数等.

4.2 真假匹配分布实验

为了验证本文算法的认证性能, 分别在 FVC2002-DB1 和 DB2 中针对用户 PIN 码安全和泄露两种情况下进行了真假匹配实验. 实验参数 $(t\_\min, t\_\max, c_x, c_y)$ 分别取 (11, 140, 13, 9). 由图 7 可以看出, 当用户 PIN 码安全时, 二个指纹库的真假匹配分布之间无重叠, 并且有明显的间隔, 说明此算法的认证性能较好.

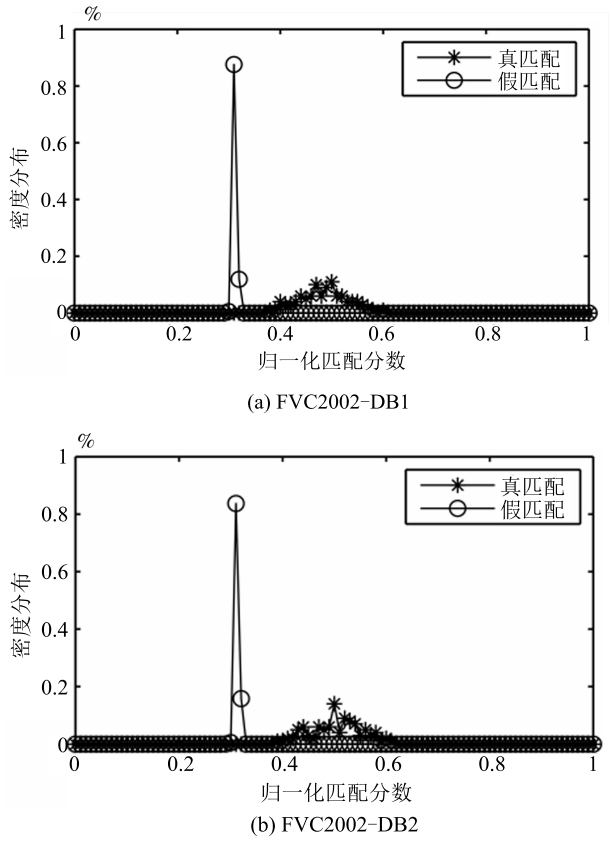


图 7 PIN 码安全时真假匹配分布
Fig. 7 Genuine and imposter distributions in the safe-PIN scenario

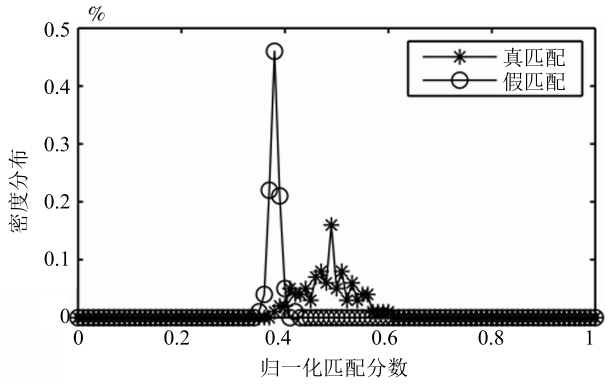
由图 8 可知, 当用户 PIN 码泄露时, 真假匹配分布之间有部分重叠, 这对算法的认证性能造成一定影响.

4.3 比较实验分析

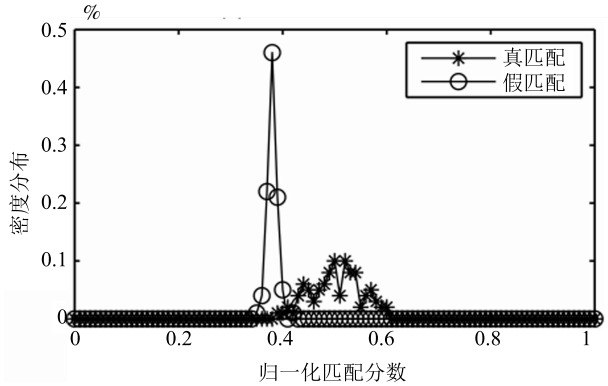
通过比较本文算法与现有的可撤销指纹模板生成算法的性能, 评估本文算法的优势.

首先, 将本文算法与 Pambud 等[18] 方法中的实验结果进行对比. 由表 3 可知, 在用户 PIN 码安全的情况下, 本文算法在指纹数据库 FVC2002-DB2

中的等错误率小于 Pambudi 方法, 并且达到理想的认证效果.



(a) FVC2002–DB1



(b) FVC2002–DB2

图 8　PIN 码泄露时真假匹配分布

Fig. 8　Genuine and imposter distributions in the stolen-PIN scenario

表 3　采用 Pambudi 方法和本文算法的性能比较 (%)

Table 3　EER comparison between the Pambudi method and proposed method (%)

算法	PIN 码安全		PIN 码泄露	
	DB1	DB2	DB1	DB2
Pambudi 等[18]	–	1	–	–
本文算法	0	0	2.5555	1.1565

然后, 为了比较在 PIN 码泄露情况下二种方法的性能, 本文对 Pambudi 的方法进行实现. 该方法的参数设定如下: 给定 $R\_\min$ 的取值为 11; $R\_\max$ 的取值范围为 [20, 140], 经过实验测试, 当参数 $R\_\max$ 取 140 时, 效果最好; 密钥 k 则通过 MATLAB 随机生成. 图 9 为本文算法与 Pambudi 等方法在用户 PIN 码泄露时的 ROC 曲线图, 该实验曲线越接近于 1, 认证性能越好, 实验结果表明, 本文算法较 Pambudi 等方法有更好认证性能.

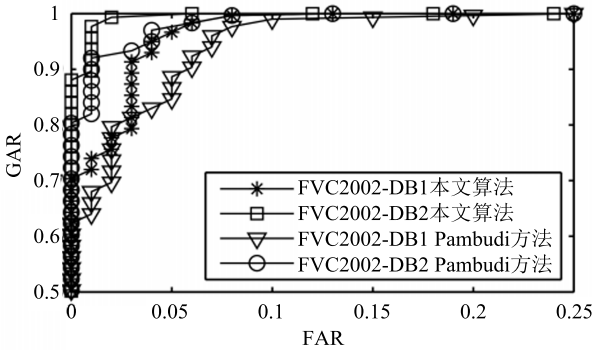
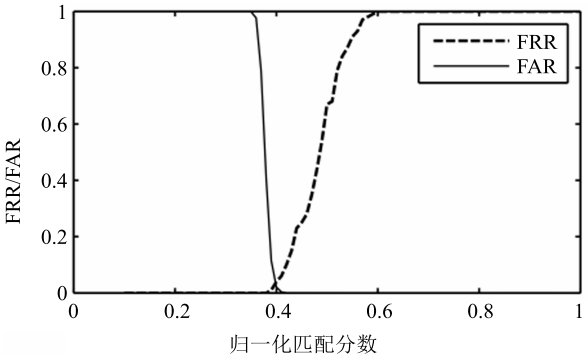


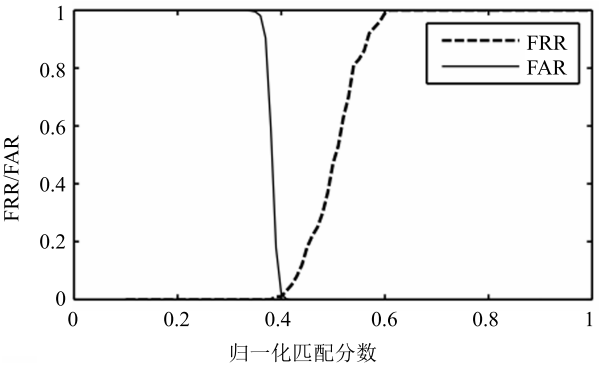
图 9　PIN 码泄露时本文算法和 Pambudi 方法的 ROC 曲线图

Fig. 9　ROC curves of Pambudi method and proposed method in the stolen-PIN scenario

图 10 为用户 PIN 码泄露时, 本文算法在 FVC2002-DB1 和 DB2 的 FRR/FAR 曲线图, EER 为曲线 FRR 和 FAR 相等时的值. 由图 10 可以看出, 数据库 FVC2002-DB2 相比 DB1 的 EER 略低, 则 FVC2002-DB2 的认证性能更好.



(a) FVC2002–DB1



(b) FVC2002–DB2

图 10　PIN 码泄露时 FRR/FAR 曲线图

Fig. 10　FRR/FAR distributions in the stolen-PIN scenario

最后, 选取图像质量较差, 提取细节点精度较低的指纹数据库 FVC2002-DB3 进一步验证本文算

法的有效性, 并引用其他经典算法的认证结果与本文结果进行对比. 由表 4 可知, 在用户 PIN 码泄露的情况下, 本文算法在数据库 FVC2002-DB1、DB2 和 DB3 的 EER 分别为 2.56 %、1.16 % 和 5.93 %, 较其他七种算法的认证性具有明显的优势.

表 4 PIN 码泄露时不同算法的性能对比 (EER) (%)
Table 4 EER comparison under the stolen-PIN scenario (%)

算法	DB1	DB2	DB3
Lee 等[12]	10.30	9.50	–
Ahmad 等[20]	9	6	27
Ahmad 等[13]	5.19	5.65	–
Sandhya 等[17]	4.71	3.44	8.79
Wang 等[15]	3.5	4	7.5
许秋旺等[19]	3.26	4.58	–
Jin 等[21]	4.36	1.77	–
本文算法	2.56	1.16	5.93

4.4 可撤销性和多样性分析

指纹模板的可撤销性是为了确保在模板受到攻击后, 用户可以通过更换 PIN 码生成一个新的模板, 使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 中进行伪假匹配实验. 选取每枚手指的一幅指纹图像, 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 9 900 次伪假匹配实验. 同时, 为了充分证明模板的认证性, 对两个数据库进行交叉匹配实验, 从 DB1 和 DB2 两个数据库中选取每枚手指的任意一幅指纹图像分别作为注册指纹和验证指纹, 在用户 PIN 码泄漏情况下, 共进行 10 000 次交叉匹配实验. 实验结果如图 11 所示.

结果表明, 虽然伪假匹配分布接近于密钥安全时的假匹配分布, 但二者仍有明显差异, 所以本文算法满足模板的可撤销性. 在用户 PIN 码泄露情况下, 两个数据库的交叉匹配结果与一个数据库的假匹配重叠, 说明真假匹配实验的真实性. 而且由图 11 可知当用户采用不同的 PIN 码与同一指纹特征融合时, 生成的指纹模板具有多样性.

4.5 安全性分析

案例 1. 对指纹模板 T_i 进行攻击. 本文通过对比特串 b_i 进行 DFT 运算, 同时采用式 (15) 加密生成模板 T_i. 式 (15) 中 R 的大小为 $p \times q$, $\boldsymbol{v}_i$ 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 $rank(R) = p < q$, 则该方程存在无穷多个解, 而复向量 $\boldsymbol{v}_i$ 只是无穷多个解中的一个, 所以攻击者很难重构比特串 b_i.

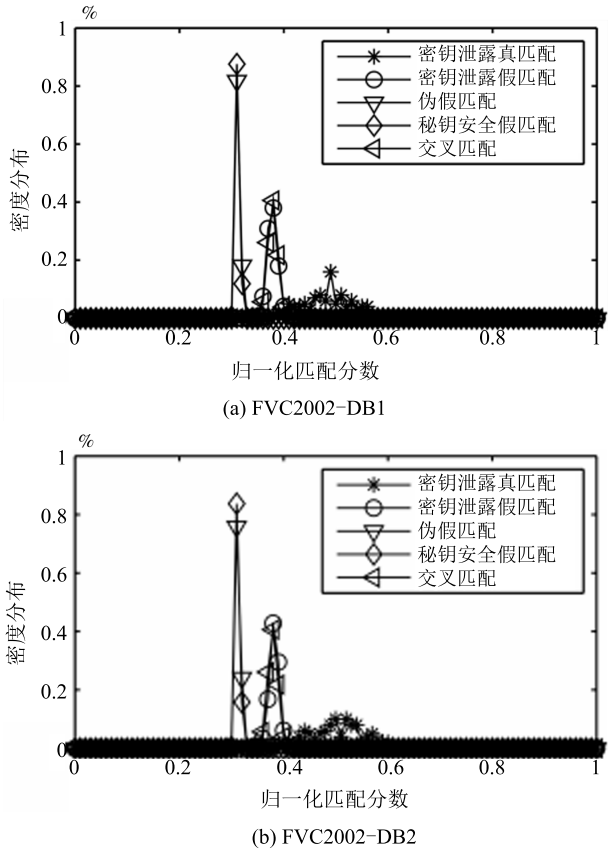


图 11 在 FVC2002-DB1 和 DB2 中密钥安全、泄露的真假匹配分布

Fig. 11 Pseudo-imposter and cross (with same key) distributions for FVC2002-DB1 and DB2

案例 2. 对比特串 b_i 进行攻击. 由于本文算法是对投影后的细节点进行多对一的不可逆变换, 比特串 b_i 中没有存储原始指纹细节点的方向和角度信息, 因此攻击者在没有获取投影角度、细节点有效数目和量化单元格的情况下, 很难恢复原始指纹信息. 即使攻击者获取了参数 $g = 648$, 细节点的数目和比特串大小, 对于一个尺寸为 388×374 的图像来说, 大约需要尝试 $388 \times 374 \times 648 \approx 9.4$ 千万次.

案例 3. 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 2.56 % 和 1.16 %, 具有良好的安全性.

5 结束语

本文设计了一种基于细节点投影的可撤销指纹

模板生成算法, 可以较有效解决原始指纹模板的唯一性和公开性所带来的安全问题. 该方法通过对指纹细节点进行直线投影, 再将投影后的向量映射到一个二维极坐标网格中生成可撤销的指纹模板. 匹配结果表明, 提出的算法具有较好的认证性和安全性, 而且在可撤销性、多样性和不可逆性等方面具有良好性能.

References

1 Zhang Ning, Zang Ya-Li, Tian Jie. The integration of biometrics and cryptography-a new solution for secure identity authentication. *Journal of Cryptologic Research*, 2015, **2**(2): 159−176
(张宁, 臧亚丽, 田捷. 生物特征与密码技术的融合 — 一种新的安全身份认证方案. 密码学报, 2015, **2**(2): 159−176)

2 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

3 Adámek M, Matýsek M, Neumann P. Security of biometric systems. *Procedia Engineering*, 2015, **100**: 169−176

4 Juels A, Sudan M. A fuzzy vault scheme. *Designs, Codes and Cryptography*, 2006, **38**(2): 237−257

5 Kaur G, Singh G, Kumar V. A review on biometric recognition. *International Journal of Bio-Science and Bio-Technology*, 2014, **6**(4): 69−76

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

7 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

8 Nanni L, Lumini A. Empirical tests on BioHashing. *Neurocomputing*, 2006, **69**(16−18): 2390−2395

9 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

10 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

11 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

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

14 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

15 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

16 Wang S, Hu J K. Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. *Pattern Recognition*, 2014, **47**(3): 1321−1329

17 Sandhya M, Prasad M V N K. K-nearest neighborhood structure (K-NNS) based alignment-free method for fingerprint template protection. In: Proceedings of the 2015 International Conference on Biometrics. Phuket, Thailand: IEEE, 2015. 386−393

18 Ahmad T, Pambudi D S, Usagawa T. Improving the performance of projection-based cancelable fingerprint template method. In: Proceedings of the 7th International Conference of Soft Computing and Pattern Recognition. Fukuoka, Japan: IEEE, 2016. 84−88

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

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

21 Jin Z, Lim M H, Teoh A B J, Goi B M. A non-invertible randomized graph-based hamming embedding for generating cancelable fingerprint template. *Pattern Recognition Letters*, 2014, **42**: 137−147

惠 妍 西安邮电大学通信与信息工程学院硕士研究生. 主要研究方向为生物特征识别.
E-mail: huiyan_mini@163.com
(**HUI Yan** Master student at the School of Communication and Information Engineering, Xi′an University of Posts and Telecommunications. Her main research interest is biometric recognition.)

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.)