基于比特串异或和置乱变换的指纹模板保护算法

党 力[1] 张雪锋[1] 惠 妍[1]

摘 要 针对现有指纹模板保护算法存在的准确性较低、安全性能较差的问题, 提出一种基于比特串异或和置乱变换的指纹模板保护算法. 该算法在已有二维映射算法的基础上, 对得到的比特串进行异或和随机索引置乱变换, 有效地将线性和非线性变换相结合, 扩展了密钥空间, 增强了指纹模板的安全性. 理论分析和仿真结果表明, 对于密钥泄露场景, 该算法在数据库 FVC2002 DB1 和 DB2 中的等错误率 (Equal error rate, EER) 分别为 0.08 % 和 0.75 %, 与现有算法相比, 具有较好的准确性和安全性.

关键词 指纹模板, 安全性, 比特串, 异或, 置乱

引用格式 党力, 张雪锋, 惠妍. 基于比特串异或和置乱变换的指纹模板保护算法. 自动化学报, 2020, **46**(12): 2681−2689

DOI 10.16383/j.aas.c190011

Fingerprint Template Protection Algorithm Based on Bit String XOR and Scrambling Transformation

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

Abstract Aiming at the problems of low accuracy and poor security performance of the existing fingerprint template protection algorithm, A fingerprint template protection algorithm based on bit string XOR and scrambling transformation is proposed. Based on the existing two-dimensional mapping algorithm, the algorithm performs XOR and random index scrambling transformation on the obtained bit string, the algorithm effectively combines linear and nonlinear transformations, thereby expanding the key space and enhancing the security of the fingerprint template. Theoretical analysis and simulation results show that for the key leakage scenario, the equal error rate (EER) of the algorithm in the database FVC2002 DB1, DB2 is 0.08 % and 0.75 %, respectively, compared with existing methods, it has better accuracy and security.

Key words Fingerprint template, security, bit string, XOR, scrambling

Citation Dang Li, Zhang Xue-Feng, Hui Yan. Fingerprint template protection algorithm based on bit string XOR and scrambling transformation. *Acta Automatica Sinica*, 2020, **46**(12): 2681−2689

身份认证技术是实现信息系统访问控制和权限管理的前提和基础. 由于传统的基于用户账号和登录密码的身份认证方式广泛存在着被暴力破解和社会工程攻击等安全隐患, 难以有效保证身份认证过程的安全性. 因此, 研究者通过将生物特征识别技术[1−2] 与传统密码学方法相结合, 提出一类生物特征模板保护技术. 以指纹数据为例, 原始指纹称为 “母本”, 通过结合加密技术, 衍生出多个不可逆且互不关联的指纹 “子本”. 在具体的身份识别过程中, 应用指纹 “子本”代替 “母本”进行识别与认证.

目前, 生物特征模板保护技术主要分为两类[3]: 生物特征加密和生物特征变换. 生物特征加密技术是结合生物特征与密钥, 并将得到的辅助数据充当生物特征模板进行注册和认证. 如: 1999 年, Juels 等[4] 提出的 Fuzzy commitment 方案; 2004 年, Dodis 等[5] 提出的 Fuzzy extractor 和 Secure sketch 二个概念结构; 2006 年, Juels 等[6] 提出的 Fuzzy vault 方案. 上述方案均能够有效地融合生物特征识别技术和传统密码, 但算法中的密钥来自于用户输入, 若发生密钥泄露, 生物特征数据也将会面临较大的安全隐患. 生物特征变换技术是通过对原始生物特征数据进行不可逆变换得到生物特征模板, 主要包括两种方法: 生物特征哈希和可撤销生物认证. 可撤销生物认证概念由 Ratha 等[7] 在 2001 年首次提出, 其认为可采用某种可变参数的不可逆函数对生物特征数据进行不可逆变换, 然后将变换后的数据作为模板, 存储于生物特征模板数据库中. 若模板

收稿日期 2019-01-04 录用日期 2019-09-02
Manuscript received January 4, 2019; accepted September 2, 2019
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 杨健
Recommended by Associate Editor YANG Jian
1. 西安邮电大学网络空间安全学院 西安 710121
1. School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121

数据泄露, 仅需改变参数即可生成新的模板, 进而实现对用户生物特征数据的有效替换. 接着, Ratha 等[8] 又提出一种将指纹特征通过笛卡尔变换、极坐标变换和函数变换生成可撤销指纹模板的算法, 该算法不仅能够有效保护原始指纹特征, 且保证了指纹特征模板的可撤销性, 但原文中采用的变换函数易受多模板攻击、非线性方程组和暴力攻击等影响, 从而降低算法的安全性, 造成用户信息泄露. 随后, Tulyakov 等[9] 提出将指纹细节点与密钥构建的哈希函数进行组合, 但攻击者可通过缩小细节点的值域进行穷举攻击, 仍然不能确保算法的安全性能. 2010 年 Lee 等[10] 将指纹细节点映射到三维数组中, 并结合用户 PIN 码生成二进制序列, 虽然该算法对可撤销性有所改善, 但当用户更新 PIN 码时, 会导致认证准确性不稳定. 2011 年, Ahmad 等[11] 将指纹细节点投影到直线上生成可撤销指纹模板, 该算法需要对指纹奇异点进行精确的定位, 并将注册指纹和查询指纹进行预配准后才能进行匹配, 若图像质量较差导致无法精准地检测到奇异点, 则会降低认证的准确性. 2013 年, Li 等[12] 将一个指纹细节点位置和另一个指纹的方向信息融合生成一个组合指纹模板, 提高了模板的安全性, 但匹配时间较长且匹配准确性不稳定. 2015 年, Sandhya 等[13] 提出一种基于指纹细节点和 K 邻域结构的指纹模板保护算法, 该算法是对离变换中心点最近的 K 个细节点进行量化和映射, 然后与用户口令结合生成可撤销指纹模板, 但直接对原始指纹细节点特征进行量化, 容易降低算法的安全性和识别准确性. 2016 年, Wang 等[14] 提出采用盲系统生成二进制比特串的可撤销指纹模板算法, 该方案有效提高模板安全性, 并降低失真率. 许秋旺等[15] 通过采用改进的细节点描述子提取细节点邻域的纹线特征, 然后结合用户 PIN 码生成指纹模板, 该算法无需使用辅助数据对指纹图像预配准, 在确保准确性良好的前提下, 具有较好的可撤销性和多样性. 2017 年, Ahmad 等[16] 提出一种基于扇区的可撤销指纹模板保护算法, 该算法有效地提高了安全性, 但其匹配的准确性仍有待提高. 随后, Alam 等[17] 提出一种基于极坐标网格三元组量化的可撤销指纹模板方法, 并结合离散傅里叶变换和随机投影增强其安全性, 对于模板反转攻击、记录多重性攻击等具有较强的抵抗力.

上述研究成果表明, 理想的生物特征模板应满足[18]: 安全性、准确性、可撤销性和多样性. 针对这些要求, 本文设计了一种基于比特串异或和置乱变换的指纹模板保护算法, 通过在环形区域筛选出有效细节点, 并对其进行投影、二维映射、异或操作、随机索引置乱等操作, 最终生成指纹模板. 实验结果表明, 该算法不仅满足生物特征模板的基本要求, 而且在指纹模板和密钥泄露的情况下, 也难以恢复出原始指纹特征.

1 SCFT 算法

2017 年, Ahmad 等[16] 提出一种基于扇区的可撤销指纹模板保护算法 (Sector-based cancelable fingerprint template, SCFT). 其基本原理是: 通过对指纹区域划分扇区, 并从中选取适当细节点表示相应的指纹特征, 细节点分布情况如图 1 所示. 以任意一个细节点为变换中心点, 对其余邻域细节点进行几何变换: 旋转、反射和平移变换. 其中, 旋转变换和平移变换由式 (1) 中的变换密钥 K 完成.

$$\begin{cases} K = \{k_v\}_1^{32} \\ k_v = (\rho_v, \chi_v, \psi_v) \end{cases} \tag{1}$$

其中, K 是第 v 个扇区的一组密钥 k. ρ_v 为旋转因子, 表示在第 v 个扇区中细节点旋转的次数. (χ_v, ψ_v) 表示在第 v 个扇区中细节点平移的距离. 经过几何变换后, 得到细节点特征值: $(x_v^t, y_v^t, \theta_v^t)$, (x_v^t, y_v^t) 表示第 v 个扇区的指纹细节点坐标, θ_v^t 表示细节点方向. 然后通过改变变换中心点, 对其余邻域点进行几何变换.

由于 SCFT 算法采用几何变换设计变换函数, 并在变换域中进行认证, 因此原始指纹数据不易被暴露出来. 但该算法在使用扇区筛选有效细节点时, 为获得更具独特性的模板, 需使用数目较多 (32 个) 且面积较小的扇区, 进而导致落入每个扇区内的细节点变少, 若这时选取的图像质量较差, 则提取的指纹细节点精确度降低, 那么利用扇区筛选的有效细节点将无法产生足够的数据, 造成某些指纹对不可用, 最终使得算法的识别性能下降. 此外, 在几何变换中, 变换函数均为线性函数, 当用户密

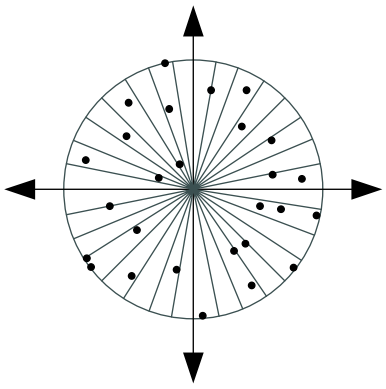


图 1 细节点分布示意图

Fig. 1 Minutiae point distribution diagram

钥泄露时存在安全隐患.

2　改进算法的基本原理

针对 SCFT 算法存在的问题, 本文提出一种基于比特串异或和置乱变换的指纹模板保护算法. 首先利用环形区域筛选出有效细节点, 并对其进行投影、二维映射得到一维比特串. 随后, 采用异或和随机索引置乱对一维比特串进行处理得到指纹比特串. 最后将指纹比特串的复矢量映射到伪随机矩阵中生成指纹模板. 在匹配过程中, 对待验证的指纹图像进行相同的变换, 生成查询模板, 然后在变换域中计算二个模板的匹配分数以验证二者的匹配程度. 算法的基本流程如图 2 所示.

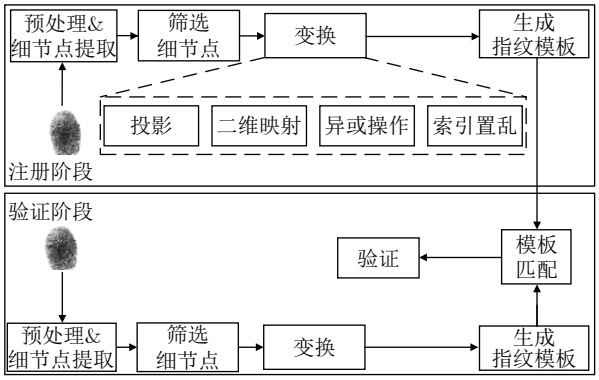


图 2　算法的基本流程

Fig. 2　Basic flow of the algorithm

算法具体步骤如下:

步骤 1. 提取注册指纹图像的细节点, 然后采用环形区域对其进行筛选, 得到有效细节点信息.

步骤 2. 将有效细节点信息投影到直线上得到投影点集, 并对其量化后映射到二维网格中得到一维比特串集.

步骤 3. 构建等长的随机密钥 key 与一维比特串集进行随机异或, 通过引入步长参数, 再次进行行间异或得到一维特征串, 所得结果存储为二进制模板, 并抛弃原始的 key.

步骤 4. 采用随机索引置乱对一维特征串进行混洗从而改变二进制模板的位置.

步骤 5. 将一维特征串的复矢量映射到由用户 PIN 码生成的伪随机矩阵中, 最终生成指纹模板.

步骤 6. 对待验证的指纹图像进行相同的变换得到查询模板, 通过在变换域中计算注册模板与查询模板的匹配分数来验证二者的匹配程度.

2.1　有效细节点的筛选

细节点筛选能够缩短后续变换过程中的计算时间, 同时减小变换中心点与邻域点距离太近或太远所造成的误差. 首先对一幅指纹图像进行预处理, 并从中提取出指纹细节点信息, 将其表示为

$$\begin{cases} F_u \in \phi \\ F_u = \{(m_i)_u\}_1^n \\ m_i = (x, y, \theta)_i \end{cases} \tag{2}$$

其中, ϕ 表示指纹域. F_u 为用户 u 指纹图像中的一组细节点. m_i 表示第 i 个细节点, n 为 F_u 中细节点总数, (x, y) 为指纹细节点坐标, θ 为细节点方向.

如图 3 所示, 在一组细节点集中, 任意选取一个细节点 m_c 为变换中心点, 即圆心, 再分别以 $r_{\min}$ 和 $r_{\max}$ 为半径得到一个环形区域, 通过设定约束条件 (3) 筛选出邻域细节点 m_k $(1 \le k \le n$ 且 $k \ne c)$ 中的有效细节点, 其中, $dis(m_c, m_k)$ 为 m_c 与 m_k 之间的距离, $r_{\min}$ 和 $r_{\max}$ 的取值参考文献 [19].

$$r_{\min} \le dis(m_c, m_k) \le r_{\max} \tag{3}$$

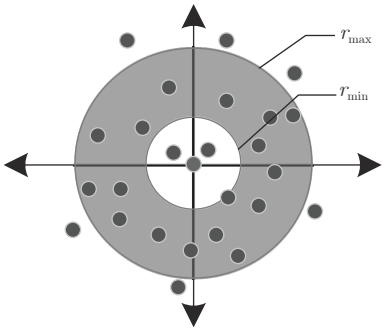


图 3　有效细节点集的选取

Fig. 3　Selection of effective minutiae point set

2.2　不可逆变换

1) $(x,\ y,\ \theta)$ 投影

以 m_c 为原点, 绘制一个新的坐标系, 如图 4 所示, 分别将邻域点 m_k 沿水平和垂直方向投影到二条直线上[20]. 计算投影到直线 l_1 上的投影点 a_{1k}^c 和 b_{1k}^c 之间的投影距离 l_{1k}^c, 以及投影角度 β_{1k}^c. $\beta_{1k}^c = \theta_k \rho_1$, θ_k 为 m_k 的方向角度, ρ_1 为直线 l_1 的斜率. 同理可计算 m_k 投影到 l_2 上的投影距离 l_{2k}^c 和投影角度 β_{2k}^c.

随后, 计算出其平均距离 L_k^c 和平均角度 φ_k^c, 如式 (4) 所示.

$$\begin{cases} L_k^c = \dfrac{1}{2}(l_{1k}^c + l_{2k}^c) \\ \varphi_k^c = \dfrac{1}{2}(\beta_{1k}^c + \beta_{2k}^c) \end{cases} \tag{4}$$

接着, 依次计算其余 $n-1$ 个邻域点的投影平均距离和平均角度, 生成投影特征向量 $P_i = \{L_k^c, \varphi_k^c\}_{k=1}^n$. 最后, 更换变换中心点并重复上述操作, 可形成投

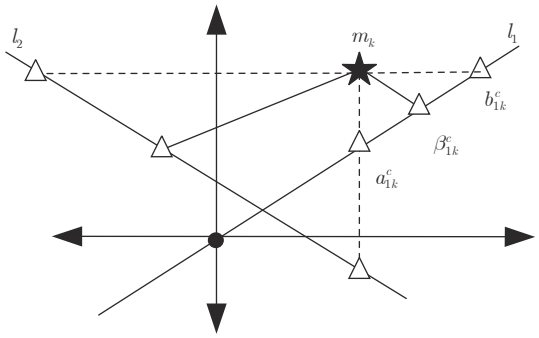


图 4 细节点投影过程

Fig. 4 Minutiae point projection process

影点集 $P=\{P_1,P_2,\cdots,P_n\}$.

2) 二维网格映射

为进一步有效保护原始指纹特性, 本文将投影点集 P 量化为 n 个 s 长度的特征比特串 $B=\{B_1,B_2,\cdots,B_n\}$[21]. 其中, s 的数目由网格总数决定, G_x 和 G_y 分别为每个网格的长与宽. 在依次访问每个网格后生成比特串, 若网格内未包含细节点, 则网格值设置为 0, 否则为 1.

尽管映射能较好地隐藏原始指纹的有效细节点信息, 但若特征比特串模板被窃取, 攻击者仍可采用暴力攻击查找出指纹细节点之间的关系, 进而导致指纹信息泄露. 因此, 本文在已有算法的基础上提出一种比特串变换的算法: 异或操作和随机索引置乱.

3) 异或操作

在改进算法中, 本文通过扩展密钥空间进而扩大指纹的类间距来抵抗攻击者的暴力抗击. 在确保识别准确性较好的前提下, 提出了一种改进的异或操作算法, 算法的流程如图 5 所示.

异或操作的具体步骤如下:

步骤 1. 随机产生一个与比特串长度 s 相同的二进制密钥 key.

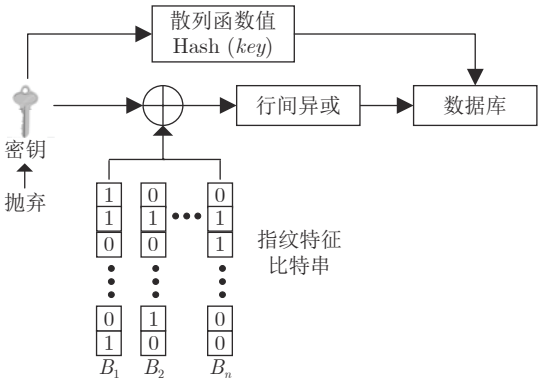


图 5 异或操作的基本流程

Fig. 5 Basic flow of XOR operation

步骤 2. 将 key 与每个特征比特串 B_i 相异或, 得到 n 个二进制序列并存储为指纹特征串的形式.

步骤 3. 计算密钥 key 的散列函数值, 并将原始 key 抛弃. 该过程中, Hash 函数保持不变, 但不同的 key 值对应不同的 Hash(key).

在确保准确性较好的前提下, 在指纹特征串中又引入了步长参数 $w\in\{1,2,\cdots,n\}$. 按照式 (5) 将第 $i,i=1,2,\cdots,s$ 行和第 $i+w$ 行的数值元素分别进行行间异或操作. 最后, 得到相应的一维特征串, 其基本思想如图 6 所示, 此操作能够较好地掩盖指纹比特串中数值的分布特点, 增大密钥空间, 使攻击者难以通过暴力攻击、穷举法攻击等恢复出一维比特串, 从而增强算法的安全性.

$$b_{ij}=\begin{cases}0, & X_{ij}=X_{(i+w)j}\\ 1, & X_{ij}\neq X_{(i+w)j}\end{cases}\tag{5}$$

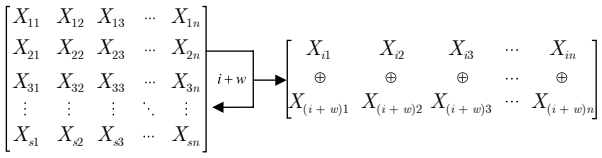


图 6 指纹特征串的行间异或

Fig. 6 Inter-row XOR process of feature strings

4) 随机索引置乱

为进一步扩展密钥空间, 采用生成随机序列的洗牌算法分别对一维比特串的每一列比特串进行处理, 其具体过程如图 7 所示, 算法的步骤如下:

步骤 1. 准备 s 个不容易碰撞的随机数, 并将其固定为一个列向量.

步骤 2. 对随机数进行随机排序, 即可得一个乱序的随机索引.

步骤 3. 按照该索引将每一列比特串位置打乱,

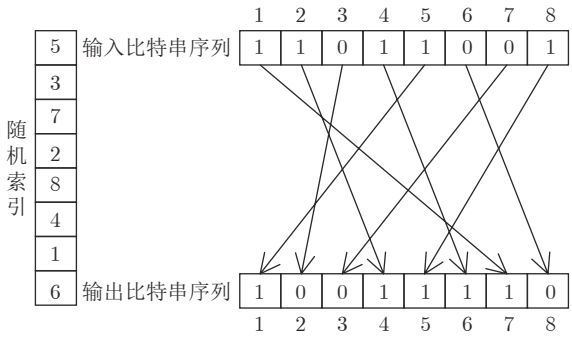


图 7 比特串的随机索引置乱

Fig. 7 Random index scrambling of feature strings

最终得到 n 个长度为 s 的指纹比特串 H_b.

该算法通过置乱一维特征串的排列次序从而增强二进制模板的安全性及隐私性, 使得难以恢复原始的指纹模板信息.

2.3　生成可撤销指纹模板及模板匹配

对指纹比特串进行 s 点离散傅里叶变换, 并提取出频域中的复矢量 F_i, 然后将 F_i 映射至由用户 PIN 码生成的随机矩阵 R 中, 可得到指纹特征模板 T_i[21]. 最后, 依次对所有特征串重复以上运算即可得到指纹特征模板 $T=\{T_1,T_2,\cdots,T_n\}$.

指纹匹配是指将注册模板与查询模板进行比较并返回匹配分数的过程[15]. 首先计算局部匹配分数 $LS(T_p^E,T_q^Q)$, 然后计算最大相似度集合 $LMS_{\max}$, 最后计算全局匹配分数 GMS, 若 $GMS\le Th$, 则匹配成功, 其中, Th 为最优阈值.

3　实验结果及性能分析

本文硬件测试平台: Intel i3-4170, 4 GB, Windows 7. 软件测试工具: MALTAB R2014a. 指纹数据库: FVC2002 DB1、FVC2002 DB2 和 FVC2002 DB3, 该数据库的相关参数如表 1 所示.

表 1　数据库 FVC2002 DB1、DB2 和 DB3 的参数
Table 1　Parameters of the FVC2002 DB1, DB2 and DB3

指纹数据库	DB1	DB2	DB3
传感器类型	光纤	光纤	电容
手指数量	100	100	100
每枚手指样本个数	8	8	8
分辨率 (dpi)	500	569	500
图像尺寸	388 × 374	296 × 560	300 × 300
图像质量	高	中	低

本文采用的性能指标是误拒率 (False refuse rate, FRR), 误识率 (False accept rate, FAR) 和等错误率 (Equal error rate, EER). FRR 是将同一枚手指的两幅指纹图像识别为不同手指的概率. FRR 与真实接受率 (Genuine accept rate, GAR) 有关, FRR = 1−GAR. FAR 是将两个不同手指的指纹图像识别为同一枚手指的概率. 当 FAR = FRR 时, 可得 EER. EER 值越小, 指纹识别系统的性能越好, 因此可将 EER 作为衡量算法性能的主要性能指标.

匹配方式可分为真匹配和假匹配. 真匹配是将每枚手指的第 1 幅图像和相应的第 2 幅图像进行比较, 共进行 100 次试验. 而假匹配是将每枚手指的第 1 幅指纹图像与其他不同手指的第 2 幅指纹图像作比较, 共进行 9 900 次试验. 本文算法在两种场景下进行评估: 用户密钥安全和用户密钥泄露. 密钥安全意味着为每个用户分配不同的专用密钥 (专用 PIN 码). 密钥泄露是针对相同密钥的场景, 即可以使用相同用户 PIN 码生成的随机矩阵和二进制密钥 key 来验证密钥泄露的情况. 此外, 参数的取值直接影响算法的性能, 因此, 表 2 列出各个参数的取值范围.

表 2　不同参数的取值范围
Table 2　Range of different parameters

参数	参数描述	参数范围
$r_{\min}$	环形区域最小半径	$\{15,16,17\}$
$r_{\max}$	环形区域最大半径	$\{100,240\}$
G_x	二维网格的长	$\{13,14,15,16\}$
G_y	二维网格的宽	$\{7,14\}$
$\rho_{1,2}$	投影直线斜率	$[-2,4]$
w	步长	$[2,4]$

为验证参数的设置对系统识别准确度的影响, 本文采用单一变量控制思路不断调整参数值以确定最佳参数, 并采用 EER 值来衡量算法在 DB1 和 DB2 数据库上的实验性能. 表 3 显示了密钥泄露时不同参数的 EER 值.

表 3　密钥泄露时不同参数的 EER (%)
Table 3　EER of different parameters (%)

$r_{\min}$	$r_{\max}$	G_x	G_y	ρ_1	ρ_2	w	DB1	DB2
16	100	13	7	0.577	−1.73	2	0.25	2.02
16	110	14	8	0.839	−1	2	0.17	1.67
16	120	14	9	1	−0.84	2	0.22	1.82
16	**140**	**14**	**9**	**1.192**	**−0.58**	**3**	**0.08**	**0.75**
16	160	14	9	1.192	−0.58	4	0.12	1.46
16	180	14	9	1.192	−0.36	4	0.15	1.66
16	200	14	10	1.732	−0.26	4	0.42	2.30
16	220	15	12	2.144	−0.18	4	1.12	3.11
16	240	16	14	2.747	−0.14	4	0.68	1.81
16	260	17	15	3.732	−0.09	4	0.98	2.64

由于当密钥安全时, 不同参数的 EER 值均为 0, 即系统能够准确地识别真假用户, 因此表 3 仅提供在密钥泄露场景下的结果. 经分析, 当参数 $(r_{\min},r_{\max},G_x,G_y,\rho_1,\rho_2,w)$ 分别取 $(16,140,14,9,1.192,-0.58,3)$ 时, 算法在 DB1 和 DB2 中的 EER 值最小, 指纹识别系统准确度最高. 因此本文将该参数作为最佳参数并对算法的准确性、可撤销性、多样性和安全性进行分析. 在实验中, 随机数及其索引均由 MATLAB 随机生成.

3.1 准确性

通常, ROC (Receiver operating characteristic) 曲线及真假匹配分布可用于验证算法的准确性, ROC 曲线绘制在以 FAR 为横坐标, GAR 为纵坐标的平面上, 该曲线下的面积越大, 则表明算法的准确性越高.

首先, 表 4 给出 SCFT 算法[16] 和本文算法在数据库 FVC2002 DB1、DB2 和 DB3 中的 EER 值. 由表 4 可得, 当密钥安全时, 本文算法显示理想的结果, 其 EER 值均为 0. 当用户密钥泄露时, 本文针对相同密钥场景的 DB1、DB2 和 DB3 的 EER 值分别为 0.08 %、0.75 % 和 3.26 %. 由于 DB3 中的指纹图像质量较差, 进而降低了细节点特征的精确度, 因此其 EER 值也随之升高, 但仍低于 SCFT 算法的 EER 值 16.99 %, 因此, 本文算法的性能较优于 SCFT 算法. 为进一步对比二个算法, 本文对 SCFT 算法进行实现, 并通过绘制 ROC 曲线来对比两种算法的准确度.

表 4 SCFT 算法和本文算法的 EER 比较 (%)
Table 4 EER comparison between the SCFT algorithms and proposed algorithms (%)

算法	密钥安全			密钥泄露		
	DB1	DB2	DB3	DB1	DB2	DB3
SCFT 算法	–	–	–	5.12	–	16.99
本文算法	0	0	0	0.08	0.75	3.26

实验中, SCFT 算法的旋转因子 $\rho = 32$, 密钥通过 MATLAB 随机生成. 图 8 为本文算法与 SCFT 算法在密钥泄露时的 ROC 曲线对比图, 由于数据库之间存在图像质量的差异, 在 DB2 中的实验结果较低于 DB1. 相较于 SCFT 算法, 本文算法在两个数据库中均可得到较高的准确率.

在密钥泄露场景下, 表 5 给出本文算法与其他指纹模板算法的 EER 值. 通过对比可知, 本文算法的 EER 分别为 0.08 %、0.75 % 和 3.26 %, 准确性明显较优于其他对比算法.

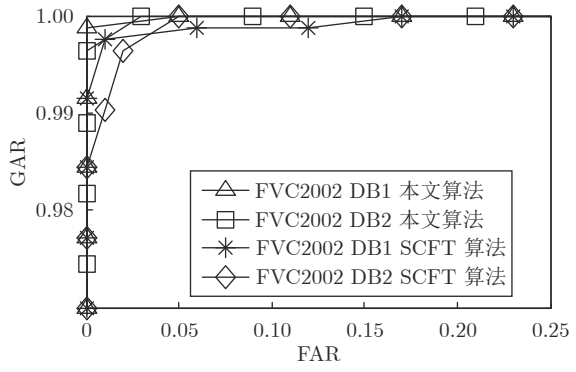


图 8 本文算法与 SCFT 算法的 ROC 曲线对比图
Fig. 8 ROC curves of SCFT and proposed algorithms

表 5 不同算法的 EER 比较 (%)
Table 5 EER comparison of different algorithms (%)

算法	DB1	DB2	DB3
Ahmad 等[22]	9	6	27
Yang 等[23]	5.93	4	–
Jin 等[24]	4.36	1.77	–
Wang 等[25]	3.5	5	7.5
Das 等[26]	2.27	3.79	–
Ali 等[27]	2.1	3.1	–
Prasad 等[21]	1.62	1.33	2.64
惠妍等[28]	0.1717	0.0606	–
本文算法	**0.08**	**0.75**	**3.26**

随后, 为突出本文算法的优势, 此处将改进前后的算法性能进行测试对比. 由于在密钥安全时, 改进前后的真假匹配分布都无重叠区域, 表明改进前后的算法都具有较好的区分性, 能够完全辨别真假用户. 当密钥泄露时, 图 9 和图 10 分别给出改进前 (投影、映射) 和改进后 (投影、映射、异或操作、索引置乱) 算法的真假匹配分布情况.

由图 9 和图 10 的实验结果可知, 当用户密钥

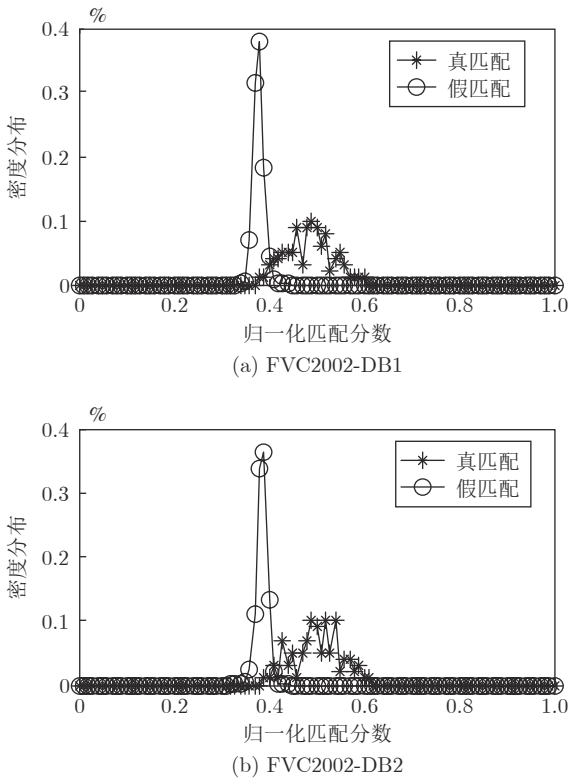
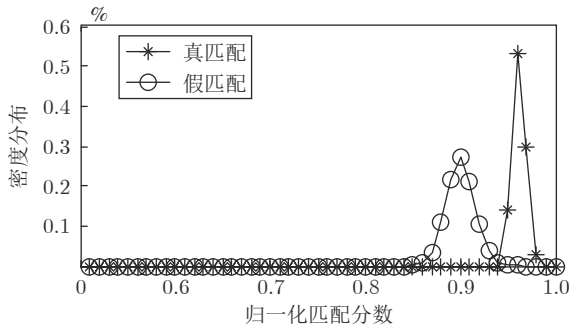
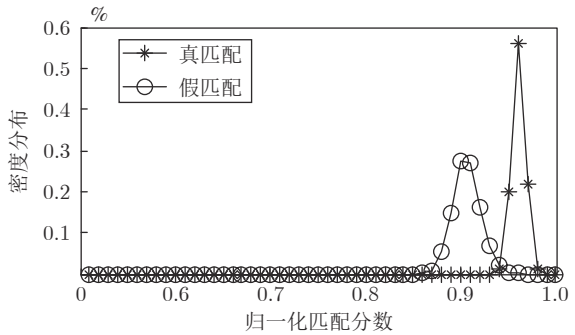


图 9 密钥泄露时改进前的真假匹配分布
Fig. 9 Genuine and imposter distributions before improvement in the stolen-key scenario



(a) FVC2002-DB1



(b) FVC2002-DB2

图 10　密钥泄露时改进后的真假匹配分布

Fig. 10　Genuine and imposter distributions after improvement in the stolen-key scenario

泄露时, 算法改进前的真匹配分布约为 0.35 ~0.61 , 假匹配分布约为 0.34 ~0.42 , 改进后的真匹配分布约为 0.94 ~0.99 , 而假匹配分布约为 0.86 ~0.95 . 改进前后的真假匹配分布都存在部分重叠区域, 这表明可能会造成较小的匹配混淆, 从而降低识别的准确性. 但改进后的真假匹配分布重叠区域明显较小, 即算法的识别准确率较高. 由此可知, 算法的识别准确度与比特串数值分布特点也有较大的关系.

为进一步验证本文改进算法对识别准确度的提升, 本文该部分在已有算法框架下对每项改进均进行单独的实验分析. 结果如表 6 所示, 给出了算法在 FVC2002 DB1 和 DB2 数据库中依次增加每项改进算法的 EER 值.

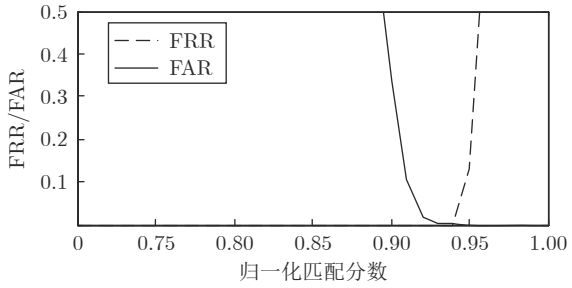
由表 6 可知, 当用户密钥安全时, 依次增加三种改进算法的 EER 值都为 0, 此时算法的准确性都达到了理想的效果. 当用户密钥泄露时, 本文算法在 DB1、DB2 中的 EER 值随着三种改进算法的依次加入逐渐降低至 0.08 % 和 0.75 %, 即表明本文改进算法在已有算法的基础上对于准确性的精度有较为明显的提升. 而在增加随机异或算法中, EER 的下降较为显著, 这是因为在异或操作过程中, 所采用的二进制密钥 key 由相同用户 PIN 码生成, 即相同用户使用相同的 key 进行认证, 从而确保了在模板匹配时指纹识别的准确性.

表 6　依次增加不同改进算法的 EER (%)

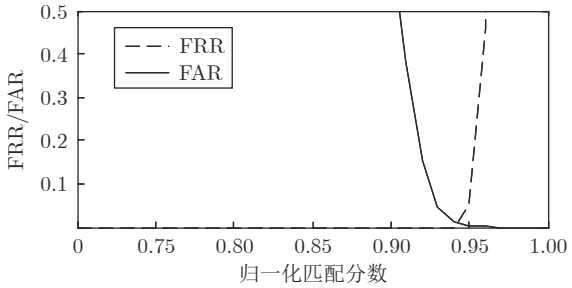
Table 6　EER of add different improved algorithms (%)

算法	DB1		DB2	
	密钥安全	密钥泄露	密钥安全	密钥泄露
改进前算法	0	3.26	0	2.915
随机异或	0	1.05	0	1.58
行间异或	0	0.44	0	1.24
随机索引置乱	0	0.08	0	0.75

此外, 图 11 为本文算法在 FVC2002 DB1、DB2 中针对密钥泄露场景的 EER 曲线图, 在设定固定阈值情况下, FVC2002 DB1 和 DB2 中的实验结果差异较小, 即表明本文算法对于指纹图像的质量影响较小, 具有较好的认证稳定性.



(a) FVC2002-DB1



(b) FVC2002-DB2

图 11　密钥泄露时真假匹配分布

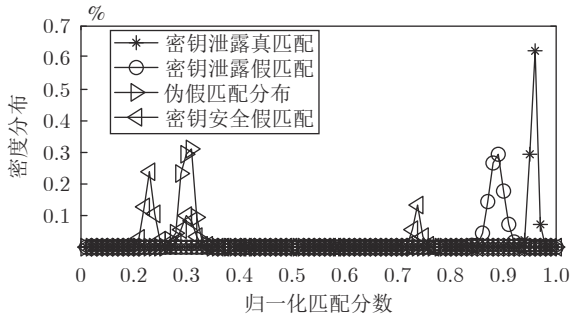
Fig. 11　Genuine and imposter distributions in the stolen-key scenario

与现有指纹生成算法相比, 本文第 2.1 节中的环形区域细节点筛选能够有效减小由于较近细节点对引起的投影误差及较远细节点对造成的非线性失真. 然后对二维网格量化后的比特串进行了异或操作、随机索引置乱. 理论上, 细节点经过投影、量化后生成的比特串与原始指纹细节点特征不再相关, 识别的准确性也较高. 但从上述实验结果可知, 识别准确度不仅由投影和量化决定, 而且易受比特串中数值分布规律的影响, 并与图像质量、有效细节点个数等条件有关.

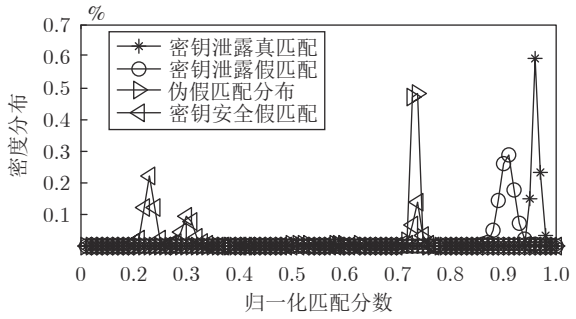
3.2 可撤销性

可撤销性是可撤销生物识别技术的重要特性. 通常, 当注册模板被泄露时, 通过更新用户 PIN 码可重新生成一个新的指纹模板, 尽管泄露的模板和更新的模板由同一指纹生成, 但新的指纹模板应与被泄露的指纹模板毫无相关性. 可撤销性也涉及多样性的要求, 即从同一用户生成的多个不同变换模板之间不能匹配.

采用伪假匹配分布来测试算法的可撤销性和多样性. 伪假匹配分布是通过使用每个手指的相同指纹图像生成 100 个转换模板, 并与注册模板进行匹配得到伪假匹配分布. 本文在数据库 FVC2002 DB1、DB2 中进行测试. 由图 12 可知, 本文算法的伪假匹配分布和真匹配分布之间明确分离, 不同于真匹配分布, 伪假匹配分布更接近假匹配分布. 上述实验结果表明, 尽管新的转换模板与已泄露模板均由相同指纹图像生成, 但二者并不相关. 因此, 本文算法满足可撤销性和多样性.



(a) FVC2002-DB1



(b) FVC2002-DB2

图 12 伪假匹配分布

Fig. 12 Pseudo-imposter match distribution

此外, 相较于 SCFT 算法[16], 本文算法不仅能够满足可撤销性, 而且在更新指纹模板时, 仅需要更新一个用户 PIN 码即可生成一个新的指纹模板. 而 SCFT 算法则需更新一组密钥 $k = \{\rho, \chi, \psi\}$. 因此本文算法较 SCFT 算法更具实用性.

3.3 安全性分析

作为可撤销指纹模板设计方案的主要要求, 不可逆性是指在计算上从变换后的可撤销指纹模板中恢复出原始模板是不可行的, 其也是算法安全性分析的重要标准.

首先假设攻击者知道一个比特串 H_b , 由于从环形区域筛选的细节点个数是随着变换中心点的位置而变化的, 因此, 难以从 H_b 中恢复出投影点集 P_i. 考虑最差的情况, 攻击者猜测某个细节点位置所需的尝试次数由图像大小和平面上的网格数决定. FVC2002 DB2 数据库的指纹图像大小为 296×560, 本文网格数为 720, 则尝试次数为 $296 \times 560 \times 720 \approx 1.2$ 亿次, 因此在计算上重建 P_i 是难以实现的.

其次, 在异或操作过程中, 仅存储了与随机密钥进行随机异或和行间异或后的辅助信息且其生成过程是不可逆的. 若攻击者想恢复随机密钥 key, 则其安全性与散列函数相关. 由于经散列函数处理后的密钥 key 的长度通常大于 160 bit, 因此, 若攻击者想恢复 key , 则其成功的概率小于 2^{-160} .

最后, SCFT 算法[16] 中的变换方式 (旋转、反射和平移) 均为线性变换, 若发生密钥泄露, 攻击者可通过多模板攻击法和暴力攻击法恢复出部分指纹细节点特征, 造成用户指纹信息泄露. 为了增强算法的安全性, 本文在变换域系数被量化后, 引入对比特串进行置乱变换的思想, 从而将线性系统和非线性系统相结合, 有效地提升了算法的安全性能.

4 结论

在指纹识别系统中, 为了保护用户指纹信息的隐私性, 本文设计了一种基于比特串异或和置乱变换的指纹模板保护算法, 该算法首先通过环形区域筛选出有效细节点, 接着对有效细节点进行投影、映射生成比特串, 从而增强模板之间的可区分性. 然后通过改进算法对比特串进行异或操作和随机索引置乱, 有效地提高了比特串的安全性及隐私性. 最后采用数据库 FVC2002 DB1、DB2 和 DB3 对改进算法进行综合分析. 研究结果表明, 该算法保证了指纹识别系统的安全性、可撤销性、以及与现有算法相比的准确性.

References

1 Nagar A. Biometric template security. *Eurasip Journal on Advances in Signal Processing*, 2008, **2008**(1): 1–17

2 Yue F, Zuo W M, Zhang D P. Survey of palmprint recognition algorithms. *Acta Automatica Sinica*, 2010, **36**(3): 353–365

3 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

4 Juels A, Wattenberg M. A fuzzy commitment scheme. In: Proceedings of the 6th ACM Conference on Computer and Commu-

nications Security, New York, USA: ACM Press, 1999. 28–36

5 Dodis Y, Reyzin L, Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: Proceedings of the 2004 International Conference Theory and Applications of Cryptographic Technique, Berlin, Heidelberg, Germany: Springer, 2004. 523–540

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

7 Ratha N K, Connell J H, Bolle R M. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 2001, **40**(3): 614–634

8 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

9 Tulyakov S, Farooq F, Mansukhani P, Govindaraju V. Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, 2007, **28**(16): 2427–2436

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

11 Ahmad T, Hu J K. Generating cancelable biometric templates using a projection line. In: Proceedings of the 11th IEEE International Conference on Control Automation Robotics and Vision, Singapore: IEEE 2011. 7–12

12 Li S, Kot A C. Fingerprint combination for privacy protection. *IEEE Transactions on Information Forensics and Security*, 2013, **8**(2): 350–360

13 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 IEEE International Conference on Biometrics, Phuket, Thailand: IEEE, 2015. 386–393

14 Wang S, Hu J K. A blind system identification approach to cancelable fingerprint templates. *Pattern Recognition*, 2016, **54**(1): 14–22

15 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)

16 Ahmad T, Rasyid B. SCFT: Sector-based cancelable fingeprint template. In: Proceedings of the 2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), 2017. 156–160

17 Alam B, Jin Z, Yap W S, Goi B M. An alignment-free cancelable fingerprint template for bio-cryptosystems. *Journal of Network and Computer Applications*, 2018, **115**: 20–32

18 Wang S, Yang W C, Hu J K. Design of alignment-free cancelable fingerprint templates with zoned minutia pairs. *Pattern Recognition*, 2017, **66**: 295–301

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

20 Ahmad T, Hu J K. Generating cancelable biometric templates using a projection line. In: Proceedings of the 11th IEEE International Conference on Control Automation Robotics and Vision, Singapore: IEEE, 2010. 7–12

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

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

23 Yang W C, Hu J K, Wang S, Yang J C. Cancelable fingerprint templates with delaunay triangle-based local structures. *Cyberspace Safety and Security and Lecture Notes in Computer Science*, 2013, **8300**: 81–91

24 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**(6): 137–147

25 Wang S, Hu J K. Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach. *Pattern Recognition*, 2012, **45**(12): 4219–4137

26 Das P, Karthik K, Garai B C. A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. *Pattern Recognition*, 2012, **45**(9): 3373–3388

27 Ali S, Ganapathi I I, Prakash S. Robust technique for fingerprint template protection. *IET Biometrics*, 2018, **7**(6): 536–549

28 Hui Yan, Zhang Xue-Feng. A fingerprint template generating method based on local minutiae three-dimensional mapping. *Scientia Sinica Informationis*, 2019, **49**(1): 42–56
(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**(1): 42–56)

党 力 西安邮电大学网络空间安全学院硕士研究生. 主要研究方向为生物特征识别. 本文通信作者.
E-mail: dangli_xupt@163.com
(**DANG Li** Master student at the School of Cyberspace Security, Xi'an University of Posts and Telecommunications. Her main research interest is biometric recognition. Corresponding author of this paper.)

张雪锋 博士, 西安邮电大学网络空间安全学院教授. 主要研究方向为信息安全.
E-mail: zhangxuefeng3@163.com
(**ZHANG Xue-Feng** Ph.D., professor at the School of Cyberspace Security, Xi'an University of Posts and Telecommunications. His major research interest is information security.)

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.)