一种单因子的可撤销生物特征认证方法

孔小景 [1] 李学俊 [1] 金 哲 [2] 周 芃 [1] 陈江勇 [1]

摘 要 将令牌化随机数作为外部因子的双因子可撤销生物特征认证方法存在令牌泄露、丢失等安全威胁. 本文提出了一种生物特征作为唯一输入的解决方法, 即单因子的可撤销生物特征认证方法. 首先, 利用扩展的特征向量, 通过预定义的滑动窗口和哈希函数随机化生成二进制种子; 然后替换不同的辅助数据来生成可撤销模板; 最后, 由查询生物特征向量对辅助数据进行解码, 提高了性能和安全性. 在指纹数据库 FVC2002 和 FVC2004 的实验结果表明, 该方法不仅满足可撤销生物特征识别的 4 个设计标准, 同时防御了 3 种安全攻击.

关键词 生物特征, 模板保护, 可撤销, 单因子, 双因子

引用格式 孔小景, 李学俊, 金哲, 周芃, 陈江勇. 一种单因子的可撤销生物特征认证方法. 自动化学报, 2021, **47**(5): 1159−1170

DOI 10.16383/j.aas.c190059

One-factor Cancellable Biometrics Verification Scheme

KONG Xiao-Jing[1] LI Xue-Jun[1] JIN Zhe[2] ZHOU Peng[1] CHEN Jiang-Yong[1]

Abstract Two-factor cncellable biometrics use tokenized random number as an external factor, however, tokenized factor incurs severe security and privacy threats. In this paper, we propose a one-factor cancellable biometrics scheme, which requires sole biometric as input. First, it exploits an expanded feature vector, generating seeds of randomized binary auxiliary data by sliding a pre-defined window and Hash function, which enhances performance and security. Then, the cancellable template hence can be generated by replacing different binary auxiliary data. Finally, the auxiliary data is decoded by using sole query biometric. The experiments have been conducted on FVC2002 and FVC2004 databases, and results show that the scheme does not only fulfill four design criteria of cancellable biometrics but also resist to the threat model that enclosed three security attacks.

Key words Biometrics, template protection, cancellable, one-factor, two-factor

Citation Kong Xiao-Jing, Li Xue-Jun, Jin Zhe, Zhou Peng, Chen Jiang-Yong. One-factor cancellable biometrics verification scheme. *Acta Automatica Sinica*, 2021, **47**(5): 1159−1170

身份鉴别是个人利益和国家安全的重要保证, 生物特征作为身份鉴别的一种重要工具, 因其不可代替性和便携性而受到学者与产业界的青睐[1−2]. 例如, 生物特征识别系统被广泛应用于国防安全、互联网金融、海关出入境等多个领域[3−4]. 随着生物特征识别系统应用的普及, 生物特征存在一旦丢失无法重新发布的隐患逐渐显现出来. 为此生物特征模板保护成为身份认证领域的研究热点.

双因子可撤销生物特征模板保护方法是生物特征模板保护的主流方法之一, 需要附加用户特定参数 (通常以密码或令牌的形式出现) 与生物特征一起作为输入[1, 5]. 该方法需要用户引入额外的输入因子, 存在一些问题, 例如: 保留令牌或记忆密码给用户带来了不便, 以及外部因子可能被盗、丢失或遗忘等[6]. 基于单因子的可撤销生物特征模板保护是一种新的生物特征模板保护方法[7], 将生物特征作为唯一的输入因子, 解决了上述双因子可撤销生物特征模板保护中外部因子产生的问题.

本文基于文献 [7] 中单因子的可撤销生物特征认证系统的框架, 提出了一种新的解决方法, 即滑动提取窗口哈希 (Window sliding and extracting Hashing, WSE) 算法. 与文献 [7] 中方法相比, 该方法改进了滑动窗口取值与哈希函数模块, 并以指纹模板的二进制矢量形式[8] 为例, 在 FVC2002 和 FVC2004 的两个公共指纹数据集中的 4 个数据库上进行实验. 实验结果表明, 本文提出的方法不仅满足可撤销生物识别技术设计的 4 个标准, 而且能抵御 3 种安全攻击.

收稿日期 2019-01-24 录用日期 2019-04-15
Manuscript received January 24 2019; accepted April 15, 2019
国家自然科学基金 (61806003), 安徽省教育厅自然科学重点项目 (KJ 2018A0010) 资助
Supported by National Natural Science Foundation of China (61806003) and Key Natural Science Project of Anhui Provincial Education Department (KJ2018A0010)
本文责任编委 黄庆明
Recommended by Associate Editor HUANG Qing-Ming
1. 安徽大学计算机科学与技术学院 合肥 230601 中国 2. 澳大利亚蒙纳士大学 (马来西亚校区) 吉隆坡 46150 马来西亚
1. School of Computer Science and Technology, Anhui University, Hefei 230601, China 2. School of Information Technology, Monash University Malaysia Campus, Kuala Lumpur 46150, Malaysia

本文方法的主要贡献如下:

1) 建立了 WSE 哈希算法的单因子可撤销生物特征认证模型, 提高了可撤销模板的精确性;

2) 采用了跳位取值的滑动窗口哈希算法技术, 提高了可撤销模板的安全性;

3) 增加了一个评价维度, 即唯密文攻击, 更加全面的评价本文方法的安全性.

本文的其余部分安排如下: 第 1 节介绍相关工作, 第 2 节描述了一种单因子的可撤销生物特征认证方法, 第 3 节给出了性能分析, 第 4 节对安全性进行了分析和讨论, 最后, 第 5 节给出了总结与展望.

1 相关工作

生物特征模板保护通常可分为两大类[1]: 可撤销的生物特征识别和生物特征加密系统. 前者包括生物特征加盐法和不可逆形变法, 后者包括密钥绑定系统和密钥生成方案. 本文的研究重点是可撤销的生物特征识别.

一般来说, 可撤销的方案通常被设计为参数化认证机制, 要求用户提供生物特征标识符和密钥. 用户特定的密钥通常存储在令牌的外部存储器 (例如, 个人的存储器或物理硬件) 中; 因此, 可撤销的方案也通常被称为 "双因子" 或 "令牌化" 生物特征认证方案. 另一方面, "单因子" 或 "无标记" 方案要求用户仅提供用于认证的生物特征标识符, 并且单因子方案的工作量非常少. 单因子方案中的服务器负责存储注册模板和密钥. 在单因子方法中, 即使模板和密钥被破坏, 攻击者也很难获得原始模板. 不考虑转换策略 (即盐基和不可逆转换) 和生物统特征的形式, 本节介绍了双因子和单因子可撤销的生物特征识别方案的相关工作.

Biohashing[5] 利用用户特定的令牌生成可撤销的模板 (参见 bioCode $\boldsymbol{b}$). 如图 1, 通常, Biohashing 方法把生物特征向量 $\boldsymbol{x} \in \mathbf{R}^n$ 和正交随机矩阵 $R \in \mathbf{R}^{n\times q}$ 作为输入, 其中 $q \le n$. Biohashing 方法中的可撤销生成过程如下: 1) 通过计算 $\boldsymbol{x} = R^{\mathrm{T}}\boldsymbol{x}$ 形成内积矢量 $\boldsymbol{y}$; 2) 根据预先定义的阈值 τ 将 $\boldsymbol{y}$ 进行行二值化运算, 生成 bioCode $\boldsymbol{b} \in [0,1]^q$, 如式 (1) 所示:

$$b_i = \begin{cases} 0, & \text{若 } y_i \ge \tau \\ 1, & \text{否则} \end{cases} \tag{1}$$

其中, $i = 1, \cdots, q$. Biohashing 方法可以推广到其他生物特征形式, 例如, 面部、虹膜、手掌等. BioHashing 是一种典型的生物特征加盐法, 其他的加盐法如文献 [9−10], 这些基于加盐的方法具有共同的特征, 即它们利用外部用户特定因子来生成转换矩阵并与生物特征模板相乘或卷积, 当模板受到攻击时, 可以通过改变令牌从而撤销已有模板并生成新模板. 此外, 文献 [11] 阐述了利用折衷的可撤销模板和正交矩阵获得原始生物特征模板的可行性.

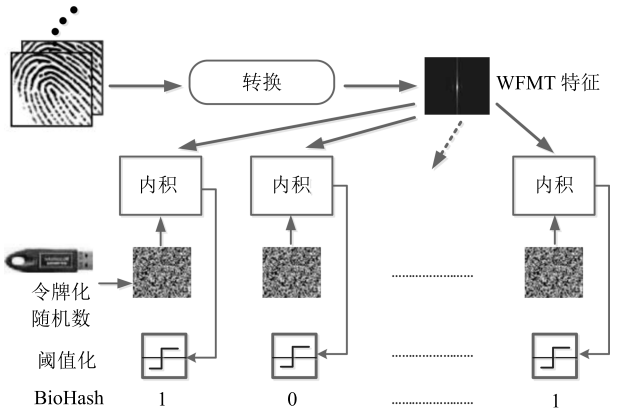


图 1 Biohashing 转换概述图[5]

Fig. 1 Overview of Biohashing transformation[5]

Wang 和 Hu[12] 提出了一种可撤销的指纹生物识别技术, 即 "Densely infinite-to-one mapping (DITOM)" 映射. 该方案在匹配过程中不需要对准过程, 利用多对一转换机制, 来生成用于匹配的可撤销模板. 简而言之, 该方案将每个细节点对量化为二进制字符串, 之后进行离散傅里叶变换 (Discrete Fourier transformation, DFT) 将二进制串转换为复数向量 C. 再通过将随机生成的参数密钥 R 与复向量组合来生成可撤销模板 T. 组合函数描述如式 (2) 所示.

$$T = RC \tag{2}$$

与将生物特征数据和密钥组合以生成模板的 Biohashing 不同, 该方法从生物特征数据生成不可逆实例, 然后将不可逆实例与密钥组合以生成可撤销模板.

布隆过滤方法 (Bloom filter) 是由 Rathgeb 等[13] 提出的可撤销生物识特征别技术, 首先应用于虹膜模板保护, 后来被推广到面部、指纹和多模态生物特征识别等多种生物特征形式. 在文献 [13] 中, Bloom filter $\boldsymbol{b}$ 是一个长度为 n 的用 0 初始化的 bit 数组. 然后, 应用 K 个独立的哈希函数根据输入项生成一组十进制值 $\boldsymbol{h} \in [0, n-1]^K$. 之后, 通过增加 $\boldsymbol{b}$ 中元素的值来形成最终 $\boldsymbol{b}$, 其中 $\boldsymbol{h}$ 中的值表示要增加的元素的位置. 该技术中不是使用哈希函数, 而是提出二进制到十进制映射函数来生成用于匹配的 $\boldsymbol{b} \in [0,1]$[13]. 基于 Bloom filter 转换的过程如图 2 所示[13]: 1) 给出一个具有 $H \times W$ 维度的 IrisCode, 将 IrisCode 细分为维度为 $H \times l$ 的多个子矩阵 B, 其中 $l = W/K$, K 是子矩阵的数量;

2) 对于每一个 B_i, 其中 $i = 1, 2, \cdots, K$, 当 $w = H$ 时, 用 0 来初始化 Bloom filter $\boldsymbol{b}_i \in [0,1]^{2^w}$; 3) 在每个 B_i 中, 逐列对元素执行二进制到十进制转换以生成一组十进制数; 4) 根据在 3) 中转换得到的十进制数, 将 Bloom filter $\boldsymbol{b}_i$ 中的元素设置为 1, 其中十进制数的值表示 $\boldsymbol{b}_i$ 中元素的索引; 5) 重复步骤 2) ∼4), 直到形成 K Bloom filter $\boldsymbol{b}_i$. 注意, 在步骤 4) 中, 如果转换了两个相同的十进制数, 则 $\boldsymbol{b}_i$ 中的元素仍设置为 1, 因此, 实现了多对一映射. 为了实现可撤销性, 在基于 Bloom filter 转换之前, 将原始的 IrisCode 和特定的秘密 T 做异或 (XOR) 运算. 尽管 Bloom filter 方法具有良好的不可逆性 (多对一映射), 但它不能满足不可链接性标准[14]. Hermans 等[14] 说明了由相同的 IrisCode 和不同的 T 生成的两个 Bloom filters 之间的高匹配分数 (最高 96 %). 此外, Bringer 等[15] 指出当密钥空间 (T) 太小时, Bloom filter 方法容易受到暴力攻击.

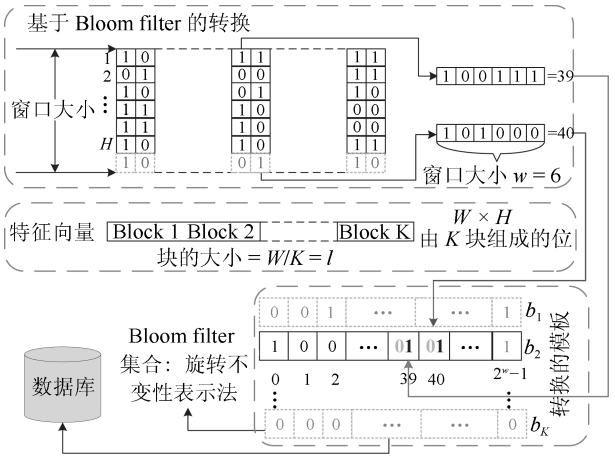


图 2　Bloom filter 转换概述图[13]

Fig. 2　Overview of Bloom filter transformation[13]

Cappelli 等[16] 提出了一种指纹细节点描述符 (Minutia cylinder code, MCC). MCC 是将细节点集 $M = \{\boldsymbol{m}_1, \boldsymbol{m}_2, \cdots, \boldsymbol{m}_n\}$ 转换成一组圆柱数据 $C = \{\boldsymbol{c}_1, \boldsymbol{c}_2, \cdots, \boldsymbol{c}_n\}$ 的技术, 其中每个 $\boldsymbol{m} = \{x, y, \theta\}$, n 是提取的细节点的数量, 圆柱是指在固定半径 r 内记录中心细节点与其邻域细节点之间的方向 (导向) 和空间 (位置) 关系的数据结构. 尽管 MCC 具有较高的匹配性能, 但可以从 MCC 模板中获得原始细节点集[17], 因此, 文献 [17] 提出了 P-MCC (Protected minutia cylinder code) 来保护 MCC 模板. 在 P-MCC 方法中, 通过单向转换函数 B-KL 投影 (B-KL projection) 将 MCC 模板 $C = \{\boldsymbol{c}_1, \boldsymbol{c}_2, \cdots, \boldsymbol{c}_n\}$ 转换为 P-MCC 模板 $V = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n\}$[17]. B-KL 投影概述如下: 1) 在训练过程中, 从 MCC 模板计算出一个平均向量 $\bar{\boldsymbol{x}}$ 和 k 个最大特征值 Φ; 2) 使用参数 $\bar{\boldsymbol{x}}$ 和 Φ_k, 在 MCC 模板上执行 KL 投影以生成 2P-MCC 模板; 3) 使用单位阶跃函数对 2P-MCC 进行二值化. 尽管 P-MCC 生成了不可逆的实例, 保证了 MCC 模板的安全性, 但 P-MCC 的用户无法使用相同的指纹来重新发布 P-MCC 模板. 针对可撤销性问题, 提出了 2P-MCC (Two-factor protected minutia cylinder code). 在 2P-MCC 中, 使用用户特定的密钥 $\boldsymbol{s}$ 对在 P-MCC 模板进行部分置换, 生成 2P-MCC 模板[18]. 然而, 2P-MCC 方案不能推广到其他生物特征模式, 因为它是专门为点集数据结构 (即 MCC 模板) 设计的.

Ouda 等[19] 提出了无标记的可撤销生物特征识别方法, 即 “BioEncoding”, 来保护 IrisCode. BioEncoding 方法中的两个基本输入是: n 位二进制向量 $\boldsymbol{c}$ (生物特征数据) 和随机生成密钥 $S \in [0,1]^{2^{m-1}}$, 其中 m 是系统参数. 从两个输入导出 BioCode $\boldsymbol{b} \in [0,1]^{n/m}$ 的过程是: 1) 将 $\boldsymbol{c}$ 分割成具有 m 位的多个块; 2) 将这些块转换成一组整数值 $\boldsymbol{x} = \{x_1, x_2, \cdots, x_{n/m}\}$; 3) 通过执行布尔函数 $f(x)$ 将整数值转换为二进制值, 该函数定义式为

$$f(x) = S[x_i], \quad f(x) \in 0, 1 \tag{3}$$

其中, $S[x_i]$ 表示 S 中的第 x_i 个二进制, $i = 1, \cdots, n/m$. 因此, 输出二进制值形式的 BioCode $\boldsymbol{b}$ 用于匹配. 虽然文献 [19] 表明 S 可以作为公共信息存储在数据库中, 但如果 S 泄露, 原始生物特征模板可以恢复.

表 1 总结了各种可撤销的生物特征认证方案在转换方式、相似性和缺点方面的比较结果.

在认证阶段, 双因子可撤销生物认证方法依赖于其他认证因素, 在转换过程中需要用户特定的令牌, 转换过程复杂, 且需要大量的存储空间存放额外的令牌化随机数据. 单因子可撤销生物认证方法不依赖于其他独立的认证因素, 在不影响性能精度的前提下, 满足了不可逆性、可撤销性和不可链接性的要求, 且转换过程简单, 所需存储空间降低. 两者的应用场景都是身份认证, 但是单因子方法只需个人生物特征, 而双因子方法还需要令牌.

另外, 尽管双因子可撤销生物认证方法是生物特征模板保护的主要方法, 但这种方法还是存在不足, 例如, 该方法需要用户的额外输入, 而且外部因素可能遗忘, 被盗或丢失, 这导致了文献 [6] 中被盗令牌场景的不利情况. 被盗令牌场景是指真实用户的令牌 (参数) 受到攻击并被攻击者利用以发起零努力错误接受攻击的事件. 此外, 用户公开特定参数可能会产生转换模板入侵的风险, 特别是对于生物特征加盐法的方案. 单因子可撤销生物认证方法可以

表 1 各种生物特征模板保护算法的比较结果

Table 1 Comparative result of various biometric template protection methods

可撤销方案	转换方式	相似性	缺点
Biohashing[5]	随机投影 + 二值化处理	汉明距离	原始模板可由折衷密钥推算出来
Wang 等[12]	离散傅里叶变换 + 随机投影	汉明距离	性能下降
Bloom filter[13]	Bloom filter (十进制到二进制映射)	汉明距离	易受暴力攻击
P-MCC[17]	KL 投影 + 二值化	汉明距离	可撤销性弱
2P-MCC[18]	完全/部分置换	汉明距离	用户需要管理密钥
GRP-based IoM Hashing[10]	多重随机投影 + 记录最大值索引	欧氏距离	性能下降
URP-based IoM Hashing[10]	置换 + 记录最大值索引	欧氏距离	性能下降
BioEncoding[19]	布尔函数	汉明距离	易受 ARM 攻击

有效避免这些不足.

2 一种单因子的可撤销生物认证方法

2.1 方法框架

局部敏感哈希 (Locality sensitive Hashing, LSH) 主要通过将原始数据投影到更少数量的 "桶" (buckets) 来降低高维数据的维度. LSH 的目标是以最大的概率将类似的物体映射到相同的 "桶" 中[10].

定义 1. LSH 是一族哈希函数 $\mathcal{H} = \{h_i : \mathbf{R}^d \to B\}$, 将数据点从 $\mathbf{R}^d$ 映射到 "桶" $b \in B$, 并且任何两个给定点 $X, Y \in \mathbf{R}^d$ 满足的条件:

$$\begin{aligned} &\mathbb{P}_{h\in\mathcal{H}}(h_i(X) = h_i(Y)) \le \gamma, \quad s(X,Y) < \alpha \\ &\mathbb{P}_{h\in\mathcal{H}}(h_i(X) = h_i(Y)) \ge \delta, \quad s(X,Y) > \beta \end{aligned} \tag{4}$$

其中, $\delta > \gamma$, $s(\cdot)$ 是相似函数. LSH 确保具有高相似性的数据点 X 和 Y 在在经过哈希函数后有较高的哈希碰撞概率, 即将 X 和 Y 映射到同一个 "桶" 中; 相反, 彼此相似度低的数据点发生哈希碰撞概率较低, 即两个数据点映射到不同的 "桶" 中.

双因子的可撤销生物特征认证方法将令牌化随机数作为外部因子带来一些问题, 本文针对这些问题提出一种单因子的可撤销生物特征认证方法, 即滑动提取窗口哈希 (Window sliding and extracting Hashing) 算法, 简称 WSE 哈希算法. 该方法实际上应用了 LSH 的理论, 在本文指纹匹配的场景中, 通过复制原始特征向量, 尽可能增加有用特征的提取数量, 经过哈希 (滑动窗口跳位取值) 后, 相似物体的哈希值碰撞的几率一定也高, 所以匹配成功. 与文献 [7] 中方法相比, 该方法改进了滑动窗口取值与哈希函数模块, 目的是提取更多有用的特征向量, 增强不可逆性, 以提高可撤销模板的性能和安全性. 本文提出的单因子的可撤销生物特征认证方法框架如图 3 所示, 该方法只需要生物特征 (以指纹为例) 作为唯一的输入因子, 与二进制随机数生成器生成的密钥 $\boldsymbol{r}$ 做运算生成可撤销的模板. 具体来说, 在注册阶段, 首先由二值生物特征向量 $\boldsymbol{x}$ 生成置换种子 (Permutation seed), 然后置换密钥 $\boldsymbol{r}$, 得到可撤销模板 $\boldsymbol{w}$. 该阶段存储编码随机二进制向量 $\boldsymbol{v}$ (密文) 和模板 $\boldsymbol{w}$. 在验证阶段, 从密文中解码和置换密钥生成用于匹配的查询向量 $\boldsymbol{w}'$, 其中置换种子由查询生物特征确定. 最后 $\boldsymbol{w}$ 和 $\boldsymbol{w}'$, 进行匹配, 判断是否匹配成功.

2.2 滑动提取窗口哈希算法

设 $\boldsymbol{x} \in [0,1]^l$ 是一个具有长度 l 的二元生物特征向量, 则 WSE 哈希算法的实现描述如下:

1) 将 $\boldsymbol{x} \in [0,1]^l$ 复制 m 倍, 形成扩展的特征向量 $\bar{\boldsymbol{x}} \in [0,1]^{lm}$, 其中 m 是系统参数; 该步骤增加了二元生物特征向量的长度, 为接下来的精度要求和安全性分析做准备.

2) 对于每个元素 $\bar{x}_i \in \bar{\boldsymbol{x}}$, 它附加来自于 $\bar{\boldsymbol{x}} \in [0,1]^{lm}$ 对应的 $k-1$ 个元素, 其中 k 是系统参数, 我们将其命名为窗口大小, 生成一个子位块 $\bar{x}_{b_i} = [\bar{x}_i|\bar{x}_{i+2}|\bar{x}_{i+4}|\cdots|\bar{x}_{i+2(k-1)}]$, 这种方法称之为滑动窗口跳位取值, 其中 | 表示连接操作, 按照此方法可以由 $\bar{\boldsymbol{x}}$ 转换成子位块的形式 $\bar{\boldsymbol{x}}_b$. 例如, 令 $\bar{\boldsymbol{x}} = [\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_{lm}]$, $k = 2$, 则, 每个 $\bar{x}_i$ 附加来自 $\bar{\boldsymbol{x}}$ 的 $(2-1)$ 个元素; 如果 $\bar{x}_i$ 是 $\bar{\boldsymbol{x}}$ 的倒数第二个元素 $(\bar{x}_{lm-1})$, $\bar{\boldsymbol{x}}$ 的第一个元素将会被追加, 若 $\bar{x}_i$ 是 $\bar{\boldsymbol{x}}$ 的最后一个元素 $(\bar{x}_{lm})$, $\bar{\boldsymbol{x}}$ 的第二个元素将会被追加, 即, $\bar{\boldsymbol{x}}_b = [\bar{x}_1|\bar{x}_3, \bar{x}_2|\bar{x}_4, \cdots, \bar{x}_{lm-1}|\bar{x}_1, \bar{x}_{lm}|\bar{x}_2]$, 该操作保护数据 $\boldsymbol{x}$.

3) 将 $\bar{\boldsymbol{x}}$ 的每个子位块 $\bar{x}_{b_i}$ 转化为整数 $\hat{x}_i \in \mathbf{Z}$. 此时若 $\hat{x}_i$ 为 0, 则令 $\hat{x}_i = 1$. 此操作进一步处理 $\bar{\boldsymbol{x}}$, 将每个子块由二进制转为十进制.

4) 根据哈希函数 $y_i = (i^{\hat{x}_i}) \bmod (lm+1)$, 变换 $\hat{x}_i$ 以确保 y_i 的最大值等于 lm. 如果求模运算结果为 0, 则设置 $y_i = 1$. 此过程产生整数向量 $\boldsymbol{y} =$

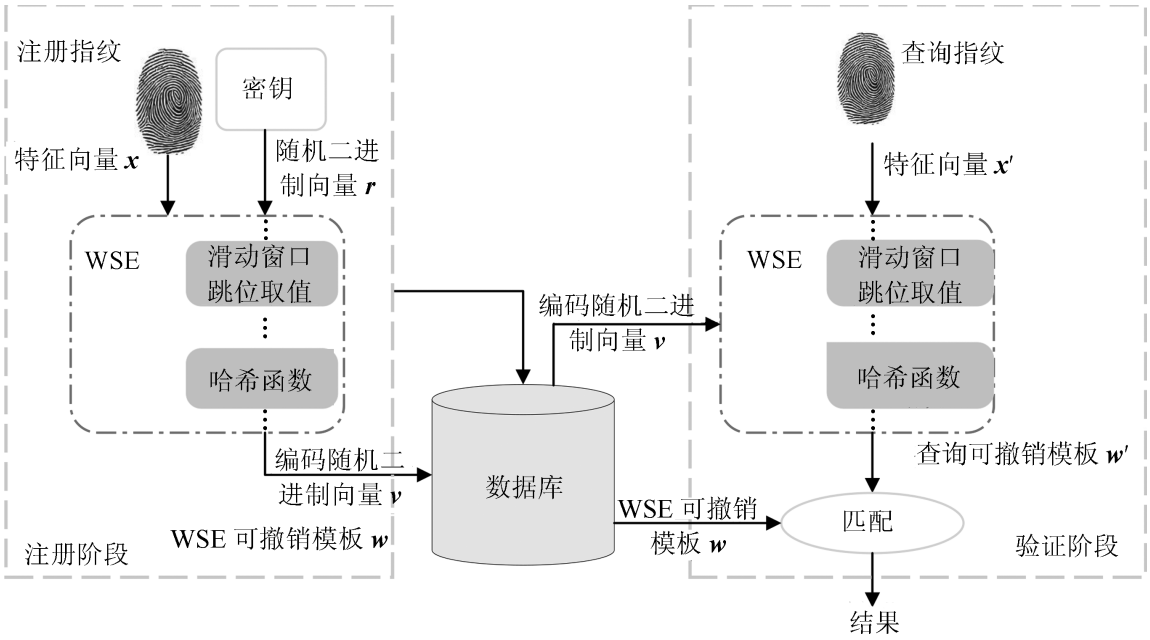


图 3　单因子可撤销生物特征认证方法框架

Fig. 3　Overview of the one-factor cancellable biometrics scheme

$[0,1]^{lm}$. 这一步由 $\boldsymbol{x}$ 生成置换种子 $\boldsymbol{y}$.

5) 设 $\boldsymbol{r}\in[0,1]^{lm}$ 是用户/应用程序特有的随机字符串, 作为密钥 key, 它是由伪随机二进制数发生器生成的向量, 将置换种子 $\boldsymbol{y}$ 作为 $r\in\boldsymbol{r}$ 的索引置换 $\boldsymbol{y}$ 生成可撤销的模板 $\boldsymbol{w}$, $\boldsymbol{w}=[r_{y_1},\cdots,r_{y_{lm}}]\in[0,1]^{lm}$. 算法 1 展示了滑动提取窗口哈希算法.

算法 1. 滑动提取窗口 (WSE) 哈希算法

输入. 二进制生物特征向量 $\boldsymbol{x}\in[0,1]^l$, 复制的倍数 m, 窗口大小 k

步骤 1. 扩增二进制生物特征向量

　for $i=1:m$

　　将 $\boldsymbol{x}$ 扩大 m 倍, 赋值给 $\bar{\boldsymbol{x}}$

　　即, 令 $\boldsymbol{x}=\bar{\boldsymbol{x}}$

　end for

步骤 2. 生成子位块

　for $i=1:lm$

　　令 $\bar{x}_{b_i}=[\bar{x}_i|\bar{x}_{i+2}|\bar{x}_{i+4}|\cdots|\bar{x}_{i+2(k-1)}]$,

　　其中 | 表示连接操作

　end for

步骤 3. 二进制转换为十进制

　for $i=1:lm$

　　将 $[\bar{x}_i|\bar{x}_{i+2}|\bar{x}_{i+4}|\cdots|\bar{x}_{i+2(k-1)}]$ 转换成整数值 $\hat{x}_i$

　　当 $\hat{x}_i==0$ 时, 令 $\hat{x}_i=1$

　end for

步骤 4. 生成置换种子 $\boldsymbol{y}$

　for $i=1:lm$

　　将 $\hat{x}_i$ 进行 $y_i=(i^{\hat{x}_i})\bmod(lm+1))$ 转换

　　当 $y_i==0$ 时, 令 $y_i=1$

　end for

步骤 5. $\boldsymbol{r}$ 置换构造 $\boldsymbol{w}$

随机二进制向量 $\boldsymbol{r}\in[0,1]^l$

　for $i=1:lm$

　　$\boldsymbol{w}=P_y(\boldsymbol{r})$, 其中 $\boldsymbol{y}$ 被视为 $\boldsymbol{r}$ 的索引

　　当 $y_i==0$ 时, 令 $y_i=1$

　end for

输出. 可撤销模板 $\boldsymbol{w}\in[0,1]^l$

如图 4 所示, 以长度 $l=6$ 的二元生物特征向量, 复制倍数 $m=2$, 窗口大小 $k=2$ 为例, 演示步骤 1 ∼ 4, 通过 WSE 哈希算法生成置换种子 $\boldsymbol{y}=[1,12]^{12}$ 的过程.

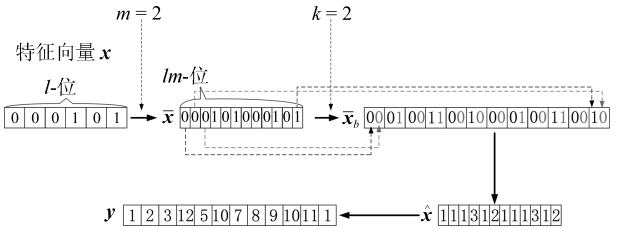


图 4　WSE 哈希算法生成置换种子示意图 ($l=6$, $m=2$, $k=2$)

Fig. 4　Diagram of generated permutation seed by WSE Hashing algorithm ($l=6$, $m=2$, $k=2$)

本文提出的一种单因子可撤销生物特征方案中的 WSE 哈希算法流程图如图 5 所示. 在注册阶段, 输入用户的生物特征向量 $\boldsymbol{x}$, $\boldsymbol{x}\in[0,1]^l$, 与密钥 $\boldsymbol{r}$ 经过 WSE 哈希算法, 生成扩展向量 $\bar{\boldsymbol{x}}$ 和隐藏了真实信息的整数向量 $\boldsymbol{y}=[1,lm]^{lm}$, $\boldsymbol{y}$ 为置换种子. 然后, 将 $\bar{\boldsymbol{x}}$ 与 $\boldsymbol{r}$ 进行异或生成二进制编码的随机向量 $\boldsymbol{v}$,

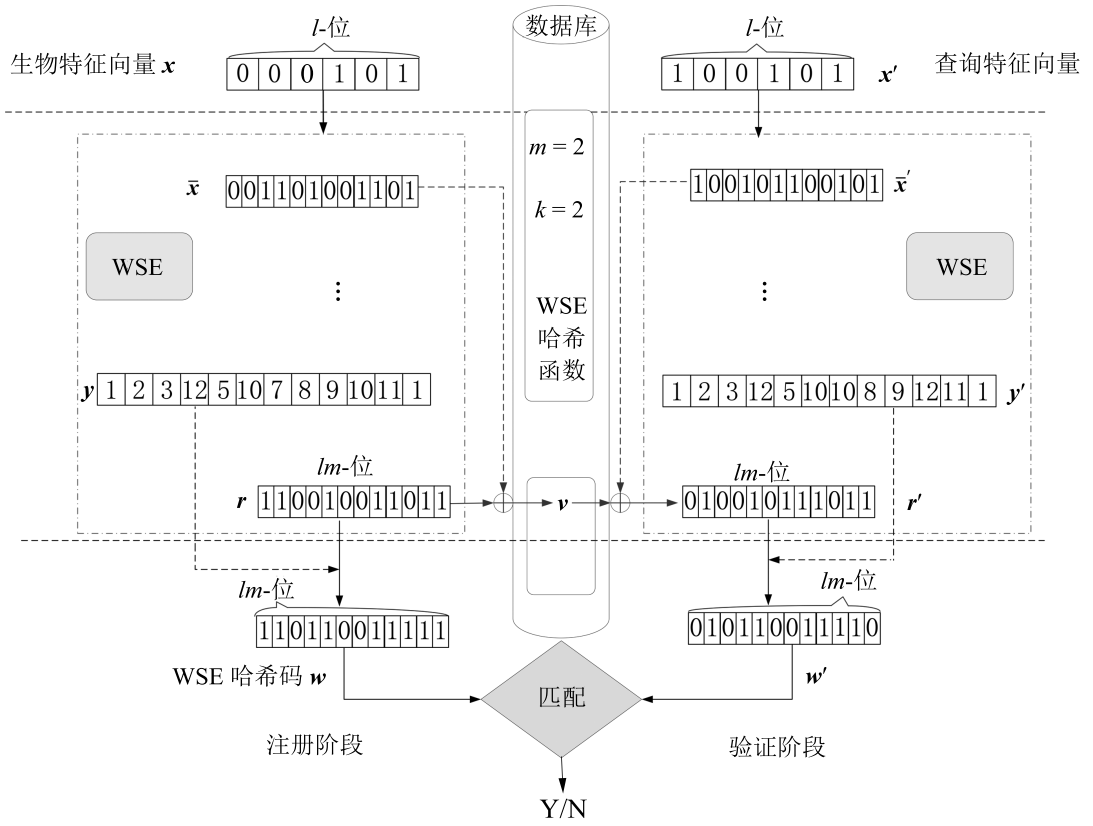


图 5 WSE 哈希算法流程图 ($l = 6, m = 2, k = 2$)

Fig. 5 The flowchart of WSE Hashing algorithm ($l = 6, m = 2, k = 2$)

$\boldsymbol{v} = \boldsymbol{r} \oplus \bar{\boldsymbol{x}}$; 将 $\boldsymbol{y}$ 作为 $\boldsymbol{r}$ 的索引, 并置换 $\boldsymbol{r}$ 生成可撤销的生物特征模板 $\boldsymbol{w}$, $\boldsymbol{w} = [r_{y_1}, \cdots, r_{y_{lm}}] \in [0,1]^{lm}$, 可以简写为 $\boldsymbol{w} = P_y(\boldsymbol{r})$, 其中 $P(\,)$ 是置换函数. 最后只将 $\boldsymbol{v}$ 和 $\boldsymbol{w}$ 存储在数据库中, 这样做有助于保护用户的真实信息, 增强不可逆性, 提高安全性. 一方面, 因为 $\boldsymbol{r}$ 和 $\bar{\boldsymbol{x}}$ 都未保存, 攻击者不能从 $\boldsymbol{v}$ 中轻易的得到 $\boldsymbol{r}$, 必须同时猜测 $\boldsymbol{x}$ (或 $\bar{\boldsymbol{x}}$) 和 $\boldsymbol{r}$ (从 $\boldsymbol{v}$ 中推出), 另一方面, $\boldsymbol{w}$ 是由真正的用户 $\boldsymbol{x}$ (或 $\bar{\boldsymbol{x}}$) 解码生成的, 要得到正确的 $\boldsymbol{w}$ 必须是正确的生物特征输入.

在验证阶段, 给出查询二进制生物特征向量 $\boldsymbol{x}'$, 让其也经过 WSE 哈希算法, 得到扩展向量 $\bar{\boldsymbol{x}}'$ 和 $\boldsymbol{y}'$. 给定 $\boldsymbol{v}$, 通过逆运算 $\boldsymbol{r}' = \boldsymbol{v} \oplus \bar{\boldsymbol{x}}'$ 得到 $\boldsymbol{r}'$, 然后置换 $\boldsymbol{r}'$, $\boldsymbol{w}' = P_{y'}(\boldsymbol{r}')$ 获得查询可撤销模板 $\boldsymbol{w}'$, 换而言之, $\boldsymbol{r}'$ 是由数据库中的 $\boldsymbol{v}$ 解码得到的.

该方案是单因子的, 在验证阶段身份检验的唯一输入是生物特征, 而不是像基于双因子的置换方案那样由第二个因子计算得出[20]. 在双因子方案中, 如果在注册期间和验证期间的置换种子是相同的, 则 $\boldsymbol{r}$ 置换前后的性能将被精确保留. 然而, 在本文提出的方法中, 因为两种置换种子都来自于唯一的注册生物特征和查询生物特征, 注册生物特征和查询生物特征在实际中是不相同的. 这一点可以类比对称加密系统 (见第 4.3 节), $\boldsymbol{r}$ 可以根据需要进行撤销和替换.

3 性能分析

3.1 实验环境

本文实验均在 MATLAB R2017b 上运行, 运行环境为 Intel® Core(TM) i5-7500 CPU @ 3.40 GHz, Intel® HD Graphics 630 (1 024 MB), 内存 16.00 GB 的台式电脑.

本文用长度为 256 位的二进制指纹向量 $\boldsymbol{x}$ 作为输入[8], 在 4 个公共指纹数据集 (FVC2002 (DB1, DB2)[21] FVC2004 (DB1, DB2)[22]) 上进行实验. 每个数据集包含 100 个手指的采样图像, 相当于 100 个用户, 每个手指采样 8 次, 得到有 8 个样本, 因此总计有 800 个指纹图像样本. 因为文献 [8] 是基于学习的方法, 所以每个用户的 8 个样本中有 3 个用于训练, 有 5 个样本可以用于测试. 通过比较汉明距离获得匹配结果, 因为注册和查询标识符均是二进制向量.

本文中, 评价指纹识别系统性能准确性的参数是真/假匹配得分 (Genuine/Imposter matching score) 和等错误率 (Equal error rate, EER). 评价

标准是文献 [23] 中的测试协议. 在每个数据集中, 可以生成真匹配得分 1 000 个 ($100 \times C_5^2$), 假匹配得分 4 950 个 (C_{100}^2). 为了无偏差地评估所提出的方案, 本文基于五个不同密钥 key ($\boldsymbol{r}$) 的实验来计算平均 EER. 该方案是单因子可撤销方案, 因此不需要对盗令牌的场景进行评估.

文中处理时间是指注册阶段和验证阶段的总计, 其中前者包括密钥 key($\boldsymbol{r}$) 生成, 可撤销模板生成和密钥编码; 而后者包括密钥解码, 查询可撤销模板生成和匹配. 表 2 说明了当 $m = 1\,000$ 和 $k = 3$ 的 WSE 哈希算法处理时间. 从表 2 中可以看出, WSE 哈希算法两个阶段的平均处理时间约等于 0.035 s.

3.2　认证性能

本节分析内部各个参数的不同取值对认证性能 (EER) 的影响, 以及比较对比实验和本文方法的认证性能.

3.2.1　各个参数对认证性能的影响

方案中有两个系统参数, 分别是扩大的倍数 m ($m \geq 1$) 和窗口大小 k ($k \geq 2$). 本节通过实验来分析 m 和 k 对所提方法的认证性能的影响, 用等错误率 EER (%) 表示, EER 越低, 说明性能越好.

图 6 显示了 WSE 哈希算法在数据库 FVC2002 DB1 上的 "EER-vs-k" 的曲线, 其中窗口大小 k 从 2, 3, 4 到 5 的变化, 而 m 从 1, 5, 10 到 15 的变化. 我们观察单个线条, m 值固定不变且 k 变大时, EER (%) 会变高. 如算法 1 中所述, k 表示子位块, 因此当 k 值增大时, 需要附加更多的比特, 增加了子比特块之间的噪声影响, 所以 EER (%) 变高. 图 6 的另一个观察结果是当 m 变大时 EER (%) 变低.

根据图 6 的观察, 为了进一步研究 m 对认证性能的影响, 进行了如下实验研究. 实验时, 使用控制单一变量法, 将 k 固定为 2, 通过改变 m 的取值来观察 EER (%) 的变化, m 的取值分别为 1, 5, 10, 15, 20, 40, 100, 200, 500, 800, 1 000. 图 7 显示了 FVC2002 DB1 上的 "EER-vs-m" 曲线. 增大 m 则 EER 相对较低, 认证性能提高; m 在 1, 5, 10 和 20 之间变化较明显, 而认证性能在 m ($m \geq 40$) 时以较慢的速度改变. 值得注意的是, m 较大时可以减少由注册和查询生物特征生成的两个置换序列 $\boldsymbol{r}$ 与 $\boldsymbol{r}'$ 的冲突, 但是 m 也不能一味的增大, 因为 m 过大时, 会造成资源浪费及攻击者易盗取的安全隐患.

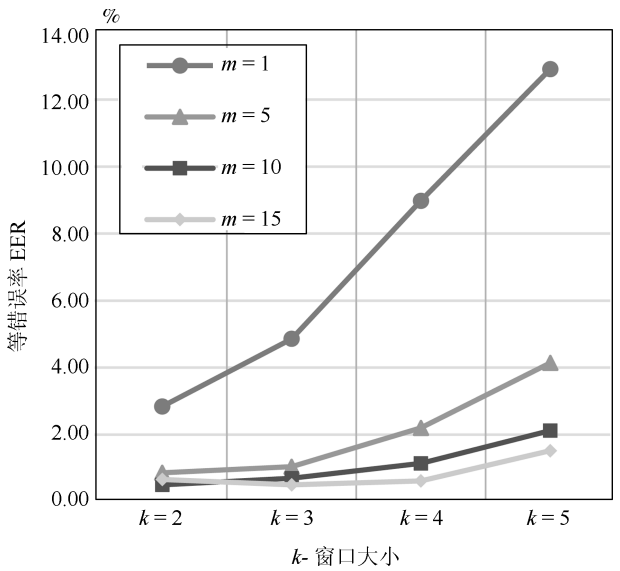


图 6　EER-vs-k 曲线图 (FVC2002 DB1)

Fig. 6　Curves of "EER (%)-vs-k" (FVC2002 DB1)

3.2.2　对比实验的认证性能

本文 WSE 哈希算法在 $m = 1\,000$ 和 $k = 3$ 时的性能精度与原始生物特征识别方法、4 种经典的双因子指纹可撤销生物识别技术以及文献 [7] 的单因子方法 EFV Hashing 比较, 如表 3 所示. 据观察, WSE 哈希算法在数据库 FVC2002 DB1 和 FVC2004 DB1 上等错误率 EER 均最低, 在其他数据库上也展现了良好的性能. 除此之外, 在与双因子方案比较中, WSE 哈希算法优于文献 [18]、文献 [24] 和基于 URP 的 IoM[10]. 在与单因子方案 EFV 哈希算法[7] 的比较中, 由于 WSE 哈希算法改进了滑动窗口取值与哈希函数模块, 在 4 个数据库上性能精度均有所提升, 且不可链接性也有提升 (参见第 3.5 节).

3.3　不可逆性

本文方法在数据库中存储的只有 $\boldsymbol{v}$ 和 $\boldsymbol{w}$, 若能逆推出 $\boldsymbol{x}$ 或 $\bar{\boldsymbol{x}}$ 则说明不满足不可逆性. 假设攻击者已经盗取 $\boldsymbol{v}$, 根据 $\boldsymbol{v} = \boldsymbol{r} \oplus \bar{\boldsymbol{x}}$, 我们如果知道 $\boldsymbol{r}$ 或 $\bar{\boldsymbol{x}}$ 都可以经过逆运算得到另外一个, 但是由于 $\boldsymbol{r}$ 和 $\bar{\boldsymbol{x}}$ 在数据库中均未存储, 所以无法恢复 $\bar{\boldsymbol{x}}$ 或 $\boldsymbol{r}$.

表 2　WSE 哈希处理效率 (s) ($m = 1\,000$, $k = 3$)

Table 2　Processing efficiency of WSE Hashing (s) ($m = 1\,000$, $k = 3$)

平均时间	FVC2002-DB1	FVC2002-DB2	FVC2004-DB1	FVC2004-DB2
注册阶段	0.035031	0.034884	0.034481	0.033151
验证阶段	0.034896	0.034874	0.034621	0.034647

表 3 不同方法的性能精度对比 (EER) (%)

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

方法	FVC2002-DB1	FVC2002-DB2	FVC2004-DB1	FVC2004-DB2
WSE Hashing	0.2	0.62	2.6	7.13
Binary fingerprint vector (Baseline)[11]	0.26	0.12	1.58	4.39
URP-based IoM Hashing[10]	0.46	2.1	4.51	8.02
GRP-based IoM Hashing[10]	0.22	0.47	4.74	4.1
Bloom filter[24]	2.3	1.8	13.4	8.1
2P-MCC$_{64,64}$[18]	3.3	1.8	6.3	-
EFV Hashing[7]	0.32	0.63	2.62	7.14

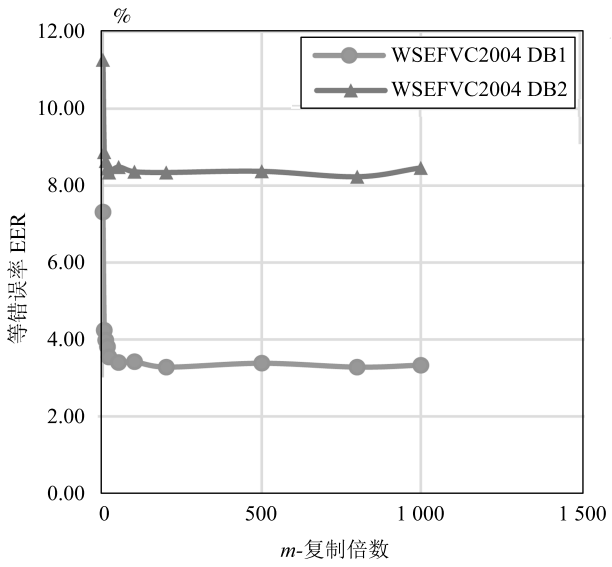


图 7 EER-vs-m 曲线图 (FVC2004 DB1/DB2)

Fig. 7 Curves of "EER (%)-vs-m" (FVC2004 DB1/DB2)

假设攻击者盗取了 $\boldsymbol{w}$, 即使已知 $\boldsymbol{w} = P_y(\boldsymbol{r})$, 但由于 $\boldsymbol{x}$ 未存储不可知, 所以置换种子 $\boldsymbol{y}$ 不可知, 则从 $\boldsymbol{w}$ 中恢复密钥 $\boldsymbol{r}$ 的枚举次数是 2^{lm} 次, 并且 $l = 256$, $m = 1\,000$, 这在实际计算中也是不可行的, 因而无法恢复 $\boldsymbol{x}$ 或 $\bar{\boldsymbol{x}}$.

3.4 可撤销性

根据可撤销性的要求, 一旦模板被破坏, 就应该生成一个新的模板并替换受损模板. 为了验证方案的可撤销性, 计算和评价了来自每个数据集真匹配得分 (Genuine match score)、假匹配得分 (Imposter match score) 和配对真匹配得分 (Mated-genuine match score) 分布. 计算 Mated-genuine 分数分布的步骤是: 1) 对于每个用户, 使用 51 个不同的 $\boldsymbol{r}$ 和用户的第一个特征向量生成 51 个不同的模板; 2) 将第一个模板 (假设为已泄露的模板) 与其余 50 个模板 (假定为更新的模板) 匹配, 从而为每个用户生成 50 个 Mated-genuine 分数. 因此, 共有 5 000 (50 × 100 个用户) Mated-genuine 得分. 图 8 显示了 FVC2002 的 DB1 和 DB2、FVC2002 的 DB1 和 DB2 这 4 个数据库的可撤销性分析, 其中 Mated-genuine 和 Imposter 得分分布在很大程度上重叠. 这表示对于相同的用户, 用不同的密钥 $\boldsymbol{r}$ 生成的模板彼此之间不能区分, 所以 WSE 哈希算法是满足可撤销性的.

3.5 不可链接性

根据不可链接性的要求, 同一个生物特征向量 $\boldsymbol{x}$ 或 $\bar{\boldsymbol{x}}$ 与不同的密钥 $\boldsymbol{r}s$ 生成的多个模板 $\boldsymbol{w}s$, 这些 $\boldsymbol{r}$ 之间不能链接. 本文遵循文献 [25] 的基准框架来验证 WSE 哈希算法的不可链接性. 方法如下:

1) 计算 WSE 哈希算法模板与配对/非配对样本得分分布 (Mated/non-mated samples score distributions) 的模型交叉匹配. 其中, 配对样本分数分布 (Mated samples score distributions) 是由同一用户通过不同密钥产生的模板之间的相似性匹配来计算. 非配对样本得分分布 (Non-mated samples score distributions) 是指由不同用户利用相同密钥导出的模板之间的相似性匹配.

2) 计算局部度量 $D_{\leftrightarrow}(s)$ 和全局度量 $D_{\underset{\longleftrightarrow}{\text{sys}}}$ 的值[25], 并根据计算的值判断转换模板的不可链接性.

具体来说, 局部度量 $D_{\leftrightarrow}(s)$ 和全局度量 $D_{\underset{\longleftrightarrow}{\text{sys}}}$ 是为了定量评估转化模板的不链接性, 而引入的两种不同的度量[25], 它们是根据配对和非配对样本得分分布计算的. 局部度量 $D_{\leftrightarrow}(s) \in [0,1]$ 是依赖于配对和非配对样本得分分布之间的似然比的局部得分测度. $D_{\leftrightarrow}(s)$ 的值从 0 到 1 表示转换后的模板在得分基础上的可链接性程度. 全局度量 $D_{\underset{\longleftrightarrow}{\text{sys}}} \in [0,1]$ 评估整个系统的不可链接性, 并且可以更公平地与其他可撤销方案的不可链接性水平进行比较. $D_{\underset{\longleftrightarrow}{\text{sys}}}$ 越接近 0, 转换模板集的不可链接性越好.

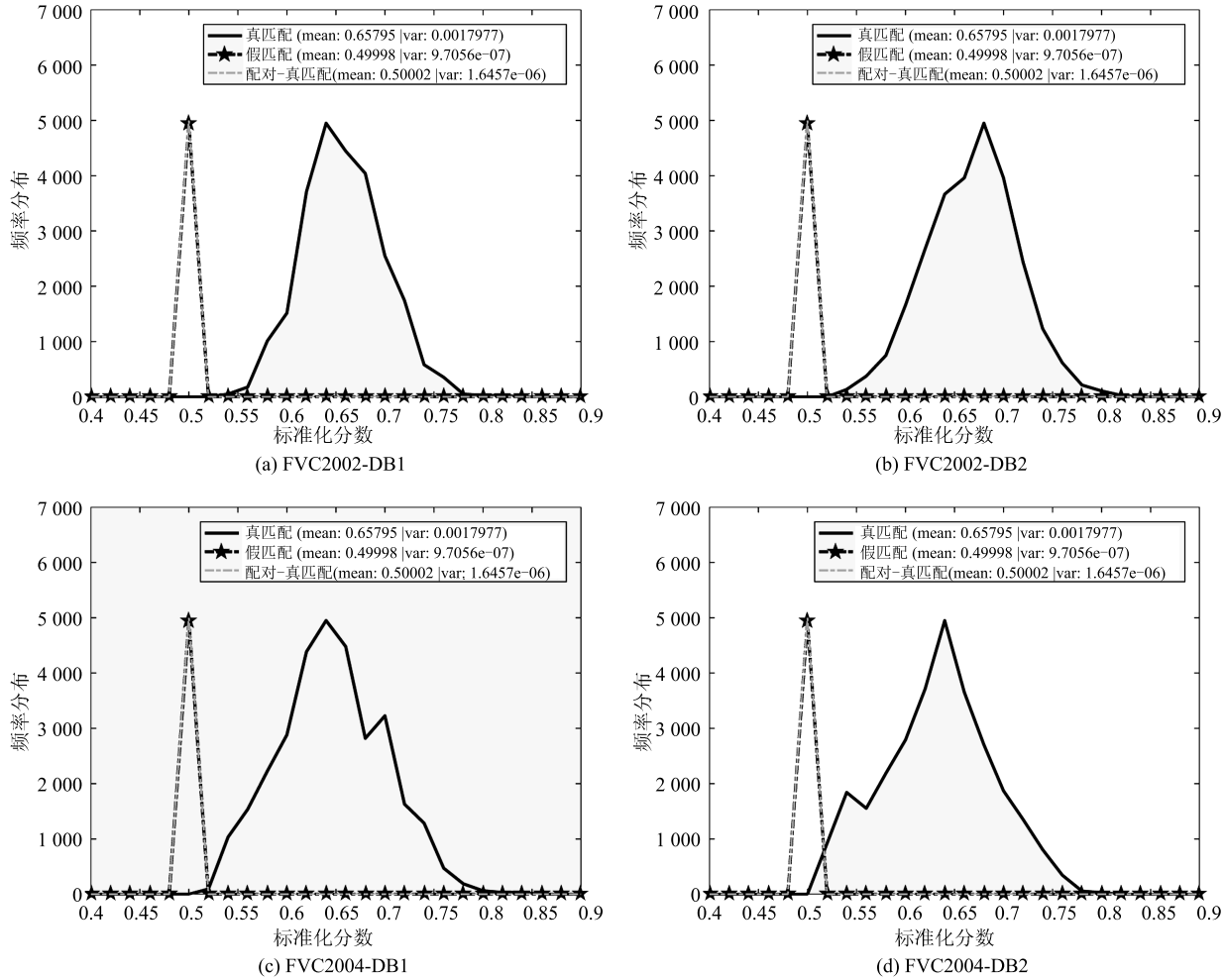


图 8　可撤销性分析

Fig. 8　Revocability analysis

实验在所有数据集上进行了测试, 其中最佳参数集为 $m = 1\,000$, $k = 3$. 为了公平地评估转换模板的不可链接性, 将 ω 设置为 1, 并且 ω 是计算 $D_{\leftrightarrow}(s)$ 和 D_{sys} 的参数. 根据文献 [25], $\omega = 1$ 是不可链接性评估标准的最坏情况.

图 9 显示了 4 个数据库 (FVC2002 (DB1, DB2), FVC2004 (DB1, DB2)) 的不可链接性的分析. 正如图 9 所示, 配对和非配对样本的得分分布曲线是重叠的, 这表示源自同一用户或不同用户的模板无法区分. 因此, WSE 哈希算法满足不可链接性标准.

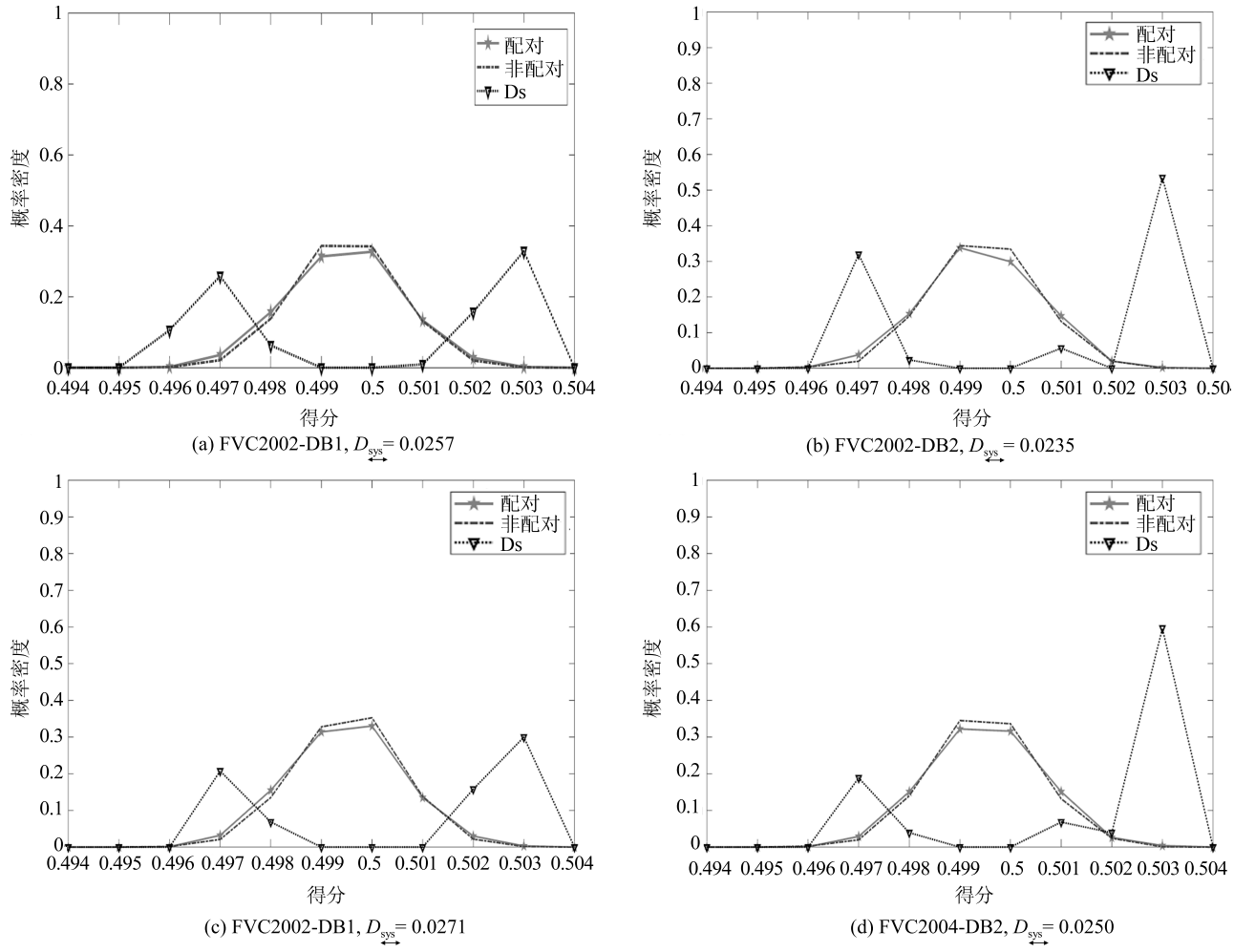
表 4 列出了 WSE 哈希算法和 EFV 哈希算法[7] 所有测试数据集的 D_{sys} 的详细值, 表中 WSE 哈希算法 D_{sys} 的最大值 $= 0.03$ (接近 0), 这表明 WSE 哈希算法接近完全不可链接的情况. 并且我们可以观察到, EFV 哈希算法 D_{sys} 的最大值 $= 0.05 > 0.03$, 这说明 WSE 哈希的不可链接性比 EFV 哈希算法的不可链接性高, 安全性和隐私性也高于 EFV 哈希算法.

4　安全性分析

本文是单因子的可撤销生物特征模板保护方法, 所以基于双因子的可撤销生物特征模板保护中第 2 个因子的安全性问题, 在这里将不再分析. 在本节中, 我们从暴力攻击、字典攻击和唯密文攻击 3 个方面来分析本文方法的安全性.

4.1　暴力攻击

暴力攻击 (Brute force attack) 作为安全攻击的一个经典方法, 指的是用穷举法试图随机使用非法访问生成转换的查询实例. 在本文中, 暴力攻击是通过猜测来衡量的 WSE 哈希算法的复杂性在代码中耗尽了代码 $\boldsymbol{w}'$ 方式. 由于 $\boldsymbol{w}'$ 是具有长度 lm 的二进制向量, 因此需要总共 2^{lm} 的猜测复杂度. 本文实验设置 $m = 1\,000$, $l = 256$, 其猜测复杂性为



(a) FVC2002-DB1, $D_{\overleftrightarrow{\text{sys}}}$= 0.0257 (b) FVC2002-DB2, $D_{\overleftrightarrow{\text{sys}}}$= 0.0235

(c) FVC2002-DB1, $D_{\overleftrightarrow{\text{sys}}}$= 0.0271 (d) FVC2004-DB2, $D_{\overleftrightarrow{\text{sys}}}$= 0.0250

图 9 不可链接性分析

Fig. 9 Unlinkability analysis

表 4 不可链接性的全局度量 ($D_{\overleftrightarrow{\text{sys}}}$) ($m = 1\,000$, $k = 3$)

Table 4 Global measure ($D_{\overleftrightarrow{\text{sys}}}$) of unlinkability ($m = 1\,000$, $k = 3$)

方法	FVC2002-DB1	FVC2002-DB2	FVC2004-DB1	FVC2004-DB2
WSE Hashing	0.0257	0.0235	0.0271	0.0250
EFV Hashing[7]	0.0404	0.0473	0.0465	0.0459

$2^{256\,000}$. 因此, 暴力攻击对本文方法是不可行的.

4.2 字典攻击

与暴力攻击中对整个散列代码的盲目猜测不同, 字典攻击 (错误接受攻击) (False accept attack) 需要更少的尝试来获得非法访问[26]. 实际上, 基于阈值的决策方案通常应用于生物识别系统, 因此这种攻击是可行的. 换句话说, 只要匹配分数超过预定阈值 τ, 就可以授予访问权限, 这可以显著减少攻击的次数.

选择 FVC2002 DB1 作为评估实例. 令参数 $m = 1\,000$, $k = 3$ 和 $l = 256$, 实验结果如图 10 所示, 阈值 $\tau = 0.56$. 这说明字典攻击需要的密码序列的最小匹配是 $lm\tau = 143\,360$. 因此, 字典攻击复杂度为 $2^{lm\tau} = 2^{143\,360}$. 尽管比暴力攻击小得多, 但是在现实操作中也是不可行的.

4.3 唯密文攻击

从另外一个角度看, 本文提出的 WSE 哈希算法可以看作是一种特殊的对称加密[4]. 对称加密 (也

称私钥加密) 是指加密和解密使用相同密钥 (或是两个密钥之间可以进行简单的转换) 的加密算法. 在本文方法中, 生物特征信息 $\boldsymbol{x}$ (或 $\bar{\boldsymbol{x}}$) 对应于对称加密系统中的明文, 随机的二进制向量 $\boldsymbol{r}/\boldsymbol{r}'$ 对应于加密/解密密钥, $\boldsymbol{v}$ 对应于密文. 因此, 我们还可以考虑针对对称加密算法的安全攻击, 如唯密文攻击 (Cipher-text only attack, COA).

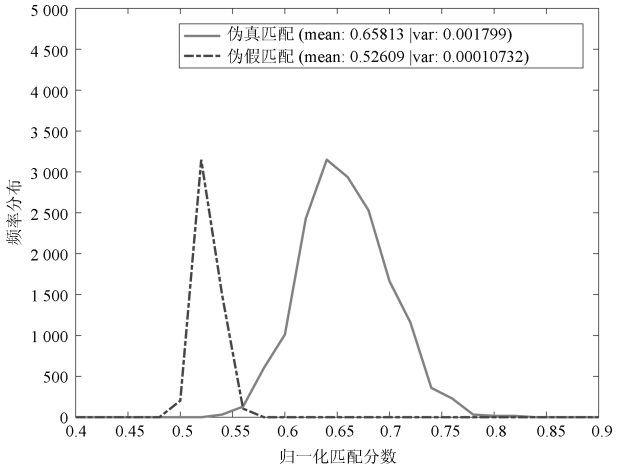


图 10　真匹配–假匹配曲线 (FVC2002 DB1, $m = 1\,000$, $k = 3$)

Fig. 10　Genuine-imposter curve on FVC2002 DB1 ($m = 1\,000$, $k = 3$)

唯密文攻击 (COA) 是指攻击者仅仅知道密文, 来得到相应的明文信息. 在文中, 密文对应于存储在数据库中的 $\boldsymbol{v}$, 若已知 $\boldsymbol{v}$, 攻击者可以用 2^l 种可能的组合来枚举 $\boldsymbol{x}$ (或者 $\bar{\boldsymbol{x}}$). 在第 3.1 节, 猜测正确 $\boldsymbol{x}$ 的平均时间是 $((\frac{2^l}{2}) \times 0.035)$ s, 其中 0.035 s 是验证所花费的平均时间. 在本文中, $l = 256$, 因此这需要平均 $(\frac{2^l}{2}) \times 0.035\,\text{s} \approx 6.43 \times 10^{67}$ year 来猜测正确的 $\boldsymbol{x}$. 这表明猜测 $\boldsymbol{x}$ 是计算不可行的. 另一方面, 虽然 $\boldsymbol{w} = P_y(\boldsymbol{r})$, 如果 $\boldsymbol{x}$ (来源于生物特征的置换种子) 未知, 则从 $\boldsymbol{w}$ 中恢复 $\boldsymbol{r}$ 同样在计算上是不可行的, 因为 $\boldsymbol{r}$ 的暴力攻击猜测是 2^{lm} 个组合.

5　总结与展望

双因子可撤销的生物特征认证方法引入额外因子即令牌化因子带来了隐私和安全威胁问题. 本文提出了一种单因子可撤销生物识别解决方法, 即 WSE 哈希算法. 针对这一问题, 本文提出了一种唯一二值数据生物特征作为输入因子的单因子可撤销生物识别方法, 即 WSE 哈希算法. WSE 哈希算法满足不可逆性, 可撤销性, 不可链接性以及精确性这 4 个可撤销的生物特征模板保护标准, 也抵御了 3 种方式的安全性攻击测试. 同时 WSE 哈希算法也可以扩展到二值向量形式表示的虹膜、面部特征、掌纹和静脉等生物特征识别. 另外, 算法的安全性, 如碰撞攻击、差分攻击等攻击方式, 也是我们未来研究方向.

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 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)

3 Wang Hui-Shan, Zhang Xue-Feng. Improved biohashing fingerprint template protection algorithms. *Acta Automatica Sinica*, 2018, **44**(4): 760−768
(王慧珊, 张雪锋. 基于 Biohashing 的指纹模板保护算法. 自动化学报, 2018, **44**(4): 760−768)

4 Liang Yao, Feng Dong-Qin, Xu Shan-Shan, Chen Si-Yuan, Gao Meng-Zhou. Feasibility analysis of encrypted transmission on security of industrial control systems. *Acta Automatica Sinica*, 2018, **44**(3): 434−442
(梁耀, 冯冬芹, 徐珊珊, 陈思媛, 高梦州. 加密传输在工控系统安全中的可行性研究. 自动化学报, 2018, **44**(3): 434−442)

5 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

6 Patel V M, Ratha N K, Chellappa R. Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, 2015, **32**(5): 54−65

7 Lee M J, Jin Z, Teoh A B J. One-factor cancellable scheme for fingerprint template protection: extended feature vector (EFV) Hashing. In: Proceedings of the 2018 IEEE International Workshop on Information Forensics and Security. New York, USA: IEEE, 2018. 1−7

8 Jin Z, Lim M H, Teoh A B J, Goi B M, Tay Y H. Generating fixed-length representation from minutiae using kernel methods for fingerprint authentication. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2016, **46**(10): 1415−1428

9 Wang S, Deng G, Hu J K. A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. *Pattern Recognition*, 2017, **61**: 447−458

10 Jin Z, Hwang J Y, Lai Y L, Kim S, Teoh A B J. Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing. *IEEE Transactions on Information Forensics and Security*, 2018, **13**(2): 393−407

11 Cheung K H, Kong A W K, You J, Zhang D. An analysis on accuracy of cancelable biometrics based on biohashing. In: Proceedings of the 2005 International Conference on Imaging Science, Systems, and Technology. Berlin, Germany: Springer-Verlag, 2005. 40−45

12 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

13 Rathgeb C, Breitinger F, Busch C, Baier H. On application of bloom filters to iris biometrics. *IET Biometrics*, 2014, **3**(4): 207−218

14 Hermans J, Mennink B, You J, Peeters R. When a bloom filter is a doom filter: Security assessment of a novel iris biometric te mplate protection system. In: Proceedings of the 2014 Biometrics Special Interest Group. New York, USA: IEEE, 2014. 1−6

15 Bringer J, Morel C, Rathgeb C. Security analysis of bloom filter-based iris biometric template protection. In: Proceedings of the 2015 International Conference on Biometrics. New York, USA: IEEE, 2015. 527−534

16 Cappelli R, Ferrara M, Maltoni D. Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2010, **32**(12): 21−28

17 Ferrara M, Maltoni D, Busch C, Cappelli R. Noninvertible minutia cylinder-code representation. *IEEE Transactions on Information Forensics and Security*, 2012, **7**(6): 1727−1737

18 Ferrara M, Maltoni D, Cappelli R. A two-factor protection scheme for MCC fingerprint templates. In: Proceedings of the 2014 Biometrics Special Interest Group. New York, USA: IEEE, 2014. 1−8

19 Ouda O, Tsumura N, Nakaguchi T. Tokenless cancelable biometrics scheme for protecting iriscodes. In: Proceedings of the 2010 International Conference on Pattern Recognition. New York, USA: IEEE, 2010. 882−885

20 Kang J, Nyang D H, Lee K H. Two-factor face authentication using matrix permutation transformation and a user password. *Information Sciences*, 2014, **269**(8): 1−20

21 Maio D, Maltoni D, Cappelli R, Wayman J, Jain A K. FVC2002: Second fingerprint verification competition. In: Proceedings of the 16th International Conference on Pattern Recognition. New York, USA: IEEE, 2002. 811−814

22 Maio D, Maltoni D, Cappelli R, Wayman J, Jain A K. FVC2004: Third fingerprint verification competition. *Biometric Authentication*. Berlin: Springer-Verlag, 2004. 1−7

23 Cappelli R, Maio D, Maltoni D, Wayman J L, Jain A K. Performance evaluation of fingerprint verification systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2006, **28**(1): 3−18

24 Li G Q, Yang B, Rathgeb C, Busch C. Towards generating protected fingerprint templates based on bloom filters. In: Proceedings of the 2015 International Workshop on Biometrics and Forensics. New York, USA: IEEE, 2015. 1−6

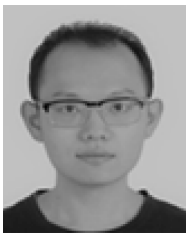
25 Gomez-Barrero M, Galbally J, Rathgeb C. General framework to evaluate unlinkability in biometric template protection systems. *IEEE Transactions on Information Forensics and Security*, 2018, **13**(6): 1406−1420

26 Tams B, Mihailescu P, Munk A. Security considerations in minutiae-based fuzzy vaults. *IEEE Transactions on Information Forensics and Security*, 2017, **10**(5): 985−998

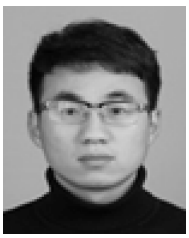
孔小景 安徽大学计算机科学与技术学院硕士研究生. 主要研究方向为生物特征加密.
E-mail: e18301199@stu.ahu.edu.cn
(**KONG Xiao-Jing** Master student at the School of Computer Science and Technology, Anhui University. Her main research interest is biometric template security.)

李学俊 博士, 安徽大学教授. 主要研究方向为云计算, 智能软件, 信息安全. 本文通信作者. E-mail: xjli@ahu.edu.cn
(**LI Xue-Jun** Ph. D., professor at the School of Computer Science and Technology, Anhui University. His research interest covers cloud computing, intelligent software, and information security. Corresponding author of this paper.)

金 哲 博士, 澳大利亚蒙纳士大学 (马来西亚校区) 讲师. 主要研究方向为生物特征加密. E-mail: jin.zhe@monash.edu
(**JIN Zhe** Ph. D., lecturer at the School of Information Technology, Monash University Malaysia Campus. His main research interest is biometric template security.)



周 芃 博士, 安徽大学讲师. 主要研究方向为机器学习, 数据挖掘和人工智能.
E-mail: zhoupeng@ahu.edu.cn
(**ZHOU Peng** Ph. D., lecturer at the School of Computer Science and Technology, Anhui University. His research interest covers machine learning, data mining, and artificial intelligence.)



陈江勇 安徽大学计算机科学与技术学院硕士研究生. 主要研究方向为机器学习. E-mail: chenjy@stu.ahu.edu.cn
(**CHEN Jiang-Yong** Master student at the School of Computer Science and Technology, Anhui University. His main research interest is machine learning.)