基于 MRP 的可撤销模板设计及其分析

徐文华, 贺前华, 李 韬, 范 炜
(华南理工大学电子与信息学院, 广东广州 510641)

摘 要: 针对基于生物特征认证系统中的存储及传输安全问题, 并且考虑到基于 VQ(Vector Quantization) 算法声纹认证系统训练数据少, 存储空间和训练时间也比较小的优点, 在基于 VQ 算法声纹认证系统的基础上, 采用 MRP (Multispace Random Projection) 提出一种可撤销声纹模板. 通过特征点与特征点, 特征点与码字之间的距离变换前后保持不变, 说明平均量化误差不变, 从而证明该方法满足可撤销模板的性能保持性. 通过随机矩阵和不定方程的分析证明该方法满足不可逆性, 即是安全的. 初步实验结果的认证率达 96%, 说明该方法的有效性.

关键词: 生物认证; 可撤销模板; 随机映射
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2009) 12-2792-05

Design and Analysis of MRP-Based Cancelable Template

XU Wen-hua, HE Qian-hua, LI Tao, FAN Wei
(*School of Electronic and Information Engineering, South China University of Technology, Guangzhou, Guangdong* 510641, *China*)

Abstract: The template storage and transmission security are crucial for biometrics-based authentication. Bases on the low storage demand and training cost of VQ-based (Vector Quantization) voiceprint authentication, a MRP-based (Multispace-Random-Projection) cancelable voiceprint template was proposed in this paper. The performance consistency was investigated by the invariableness of the quantization error. The security of the proposal was clarified by the characteristics of the random matrix and the underdetermined system. The experimental results demonstrated the validity of the proposal.

Key words: biometric-based authentication; cancelable template; random projection

1 引言

由于生物特征的稳定性、唯一性, 以及与实体间的固有联系性, 基于生物特征的认证研究成为近年来的研究热点. 目前大量的研究集中在通过不同的生理特征 (指纹、人脸、虹膜、声纹、掌纹等) 或行为特征(签名、步态等) 实现认证, 同时提高系统的准确率[1]. 这些认证系统在现实生活中日益发挥重要作用.

但是, 生物特征的稳定性, 唯一性以及与实体的固有联系性, 一方面为认证提供了比传统密码方式[2] 更安全的途径; 另一方面, 也带来模板存储和特征传输安全问题[3]. 因为实体特征一旦丢失, 由于安全性得不到保障, 该特征不再可用; 另外大量的生物特征存放在一个数据库中, 一旦数据库泄露, 将导致这些用户的特征不可用, 甚至引发用户的心理恐慌; 基于隐私的考虑, 用户也会担心, 他们的生物特征是否会被存储这些数据的机构滥用; 在开放的网络中, 认证实体也会担心特征的传输是否安全. 这两个问题的解决, 对基于生物认证系统的广泛应用具有重要意义.

生物特征保护问题在国外已有不少的研究报道, 在国内最近也有相关的研究报道. 目前生物特征的保护方法主要有模糊提取技术, 结合成熟的密码方案方法以及可撤销模板方法. 文献[4, 5] 在生物特征中通过容错方式提取均匀分布的随机密钥以保护特征. 这类方法的优点是可以通过“不确定”的生物特征获得“确定”的密码, 缺点是这种密码不具有良好的稳定性和信息熵. 文献[6, 7] 基于数字签名技术对生物特征签名, 通过签名方法达到生物特征保护的目的, 同时也可以达到认证的目的. 此类方法的缺陷是对特征的保护采用传统密码体制, 若密钥丢失, 安全性仍然无法保证.

可撤销模板[8] 从生物特征应用的安全现状分析, 总结出模板保护方法的四个属性, 是目前解决这两个问题的有效方法之一. 可撤销模板具有以下四个属性, 这也是可撤销模板设计的目标:

(1) 多样性: 对于同一实体, 不同的应用系统可以使用不同的模板

(2) 可撤销性: 当某个模板被泄漏, 可以重新使用新的模板

收稿日期: 2008-10-08; 修回日期: 2009-06-20
基金项目: 国家自然科学基金(No. 60572141, 60602014)

(3) 不可逆性: 原始特征经过不可逆变换, 采用变换后的模板进行认证, 即使模板被盗取, 也不可恢复原始生物特征

(4) 性能保持性: 采用变换后模板的认证性能没有显著降低.

不可逆函数(Norr-invertible transitions), Fuzzy Vault 以及MRP 已经成为目前可撤销模板设计的主要方法[9~12]. 文献[9, 10]基于不可逆函数和 Biohash 方法把原始特征转换至变换域, 认证在变换域进行. 这类方法的优点是通过不可逆函数, 原始特征可以得到良好的保护, 但不可逆性与良好的性能保持之间存在矛盾. 文献[11, 12]基于 Fuzzy Vault 的方法, 这类方法通过生物特征 A 保护某个秘密 K, 只有另外一个特征 B 与 A 足够接近时才能打开秘密 K. 这既可以作为一种认证的方法, 同时, 如果在特征中加入足够多的"Chaff Points", 也可以达到保护原始特征的目的. 这类方法的优点是可以解决传输安全问题, 缺陷是不能有效解决存储安全问题. 随机映射[13](Random Projection) 是模式识别中降维的一种常用方法, 文献[14]采用该方法把原始特征矩阵与随机矩阵的内积作为模型训练的输入, 把原始特征映射到随机空间, 实现保护原始特征的目的. (因为不同的注册用户可以映射到不同的空间, 所以称为多子空间随机映射). 但该文并没有对此方法的有效性和安全性做分析, 而是通过实验验证该方法可以用于可撤销模板的设计. 本文在 VQ 算法的基础上, 通过分析变换前后特征点与特征点, 特征点与码本的距离, 证明了在随机矩阵与声纹特征维数相等的情况下, 可以实现可撤销模板的设计目标.

从识别所需时间, 存储空间和训练所需要的样本数考虑, 基于 VQ 的识别算法优于概率模型的方法, 并且VQ 方法也不需要时间规整, 简化了系统的复杂度, 较 DTW(Dynamic Time Warping) 方法亦有速度和精度上的优势[15]. 考虑到基于 VQ 算法的声纹识别方法的诸多优点, 本文在传统的基于 VQ 算法的声纹认证系统基础上, 采用 MRP 实现可撤销声纹模板: 首先对语音信号进行预处理, 提取 MFCC 特征; 然后通过随机矩阵与特征相乘, 把原始特征映射至随机空间, 再通过随机空间中的特征进行码本训练, 通过 VQ 识别算法进行认证实体的认证; 最后通过对随机矩阵和不定等式的分析, 说明该方法可以实现特征保护的目的, 即该方法是安全的. 实验验证该方法是有效的.

2　基于 MRP 的可撤销模板方法

现有的基于生物特征的认证系统都包括两个阶段: 注册阶段和认证阶段. 注册阶段由用户向服务器提供生物特征, 服务器存储特征作为识别过程的参考模板; 认证阶段服务器再次提取用户的特征, 通过该特征与参考模板的匹配, 根据不同的判据给出认证结果. 以声纹认证为例, 典型的系统框图见图 1[15]. 文献[3]针对该认证框架, 给出了其所存在的安全威胁. 这些威胁复杂多样, 构成所谓的鱼骨模型(Fishr-bone Model). 在该模型中, 又以特征存储和传输所受威胁最为严峻.

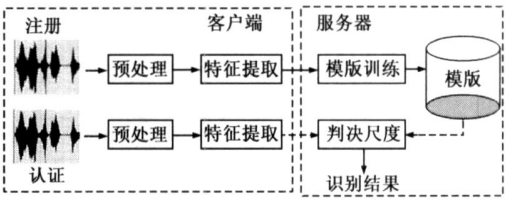

图1　传统的生物认证系统

针对模板存储及特征传输安全的问题, 同时考虑到 VQ 算法所需要的训练样本少, 识别时间少, 并且不需要时间规整的优点, 在基于 VQ 识别算法认证系统基础上, 本文提出基于 MRP 的可撤销模板系统框图见图 2.

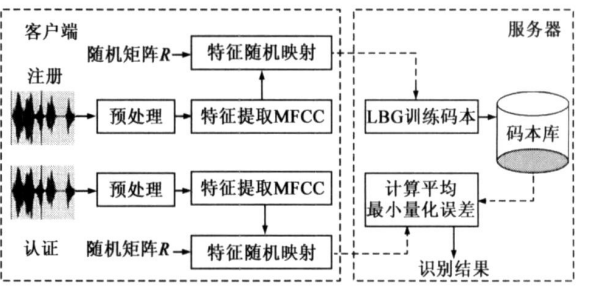

图2　基于MRP的声纹认证系统

图 2 认证系统架构是在图 1 的基础上, 在码本训练前先对特征做随机映射, 从而达到保护特征和码本的目的: 传输过程中的特征是变换后的; 码本, 即模板, 是变换后特征训练的结果. 下面分析这种变换是否会显著降低系统的识别率, 并且能否满足传输和存储安全要求.

3　有效性和安全性分析

可撤销模板的有效性是对指特征的变换不会恶化系统识别性能, 而 VQ 方法认证系统的判决尺度为平均最小量化误差, 见图 2. 因此, 有效性分析的关键是本文所提的变换方法是否影响最小量化误差. 如果对于某个说话人的码本, 输入矢量在变换后的特征空间中的量化误差与变换前特征空间的量化误差相等, 那么该变换不会影响系统的认证结果, 因而不会对系统的认证性能造成影响. 在以下分析过程中, 码本的生成采用经典的 LBG(Linde Buzo Gray) 算法, 而初始码本的生成也采用常用的分裂算法. 设变换前后最小量化误差分别是 ξ_* 和 ξ_*':

$$\xi_* = \frac{1}{m}\sum_{n=1}^{m}\min_{1\le l\le L}[d(\boldsymbol{X}_n, \boldsymbol{Y}_l^*)] \qquad (1)$$

$$\xi'_k = \frac{1}{m}\sum_{n=1}^{m} \min_{1\leqslant l\leqslant L}\{d[(\boldsymbol{RX})_n, \boldsymbol{Y}'^k_l]\} \quad (2)$$

其中, $\boldsymbol{Y}^k_l$ 表示第 k 个说话人码本的第 l 个码字, $\boldsymbol{Y}'^k_l$ 表示变换后第 k 个说话人码本的第 l 个码字, m 是认证过程提取特征矢量序列的长度, d 为欧式距离测度. 式中 $\boldsymbol{X}_n \in R^r$, $\boldsymbol{X} \in R^{r\times m}$, $\boldsymbol{R}$为随机矩阵, $\boldsymbol{R} \in R^{w\times r}$, w 为映射后的维数, 一般 $w \leqslant r$ (这涉及该方法的安全性, 见安全性分析部分), $\boldsymbol{R}$ 为行正交矩阵. 本文设 $w = r$, 在此条件下, 我们的结论是式(1)和式(2)具有相等的关系, 即变换满足有效性要求. 证明基于以下两点:

(1)变换前后, 特征矢量(或特征矢量序列)之间的距离保持不变

(2)变换前后, 特征矢量与码字之间距离保持不变

对于第(1)点, 设 $\boldsymbol{X}^i$, $\boldsymbol{X}^j$ 分别为注册和认证过程时对某一语音样本提取的特征矢量序列, $(\boldsymbol{RX})^i$ 和 $(\boldsymbol{RX})^j$ 为变换后的特征序列:

$$\begin{aligned}&\|(\boldsymbol{RX})^i - (\boldsymbol{RX})^j\|^2\\ &= \|(\boldsymbol{RX})^i\|^2 + \|(\boldsymbol{RX})^j\|^2 - 2(\boldsymbol{RX})^{i\mathrm{T}}(\boldsymbol{RX})^j\\ &= \|\boldsymbol{X}^i\|^2 + \|\boldsymbol{X}^j\|^2 - 2\boldsymbol{X}^{i\mathrm{T}}\boldsymbol{R}^{\mathrm{T}}\boldsymbol{R}\boldsymbol{X}^j\\ &= \|\boldsymbol{X}^i\|^2 + \|\boldsymbol{X}^j\|^2 - 2\boldsymbol{X}^{i\mathrm{T}}\boldsymbol{X}^j\\ &= \|\boldsymbol{X}^i - \boldsymbol{X}^j\|^2\end{aligned}$$

即:

$$\|(\boldsymbol{RX})^i - (\boldsymbol{RX})^j\|^2 = \|\boldsymbol{X}^i - \boldsymbol{X}^j\|^2 \quad (3)$$

式(3)说明, 变换前后, 特征矢量序列之间的距离保持不变.

以下分析第(2)点, 由式(3)所表现的距离不变性能否保证特征矢量与码字之间距离的不变, 即:

$$\|\boldsymbol{Y}^i_l - (\boldsymbol{RX})^j_n\|^2 = \|\boldsymbol{Y}'^i_l - \boldsymbol{X}^j_n\|^2,\quad 1\leqslant n\leqslant m,\ 1\leqslant l\leqslant L \quad (4)$$

$\boldsymbol{Y}^i_l$ 为采用 $\boldsymbol{X}^i$ 训练的码字, $\boldsymbol{Y}'^i_l$ 为采用 $(\boldsymbol{RX})^i$ 训练的码字. 对于式(4), 可以从以下三点加以证明:

(ⅰ)矢量量化的结果仍在训练样本所在空间

(ⅱ)矢量量化码本是训练样本的线性加权和(这是码本生成方法所决定的, 根据这一点及上述第(ⅰ)点结论, 可以得出, 变换后的码本即为变换前码本的变换)

(ⅲ)对于本文采用的 LBG 算法, 在子空间划分条件不变的条件下, 矢量量化在空间中的相对位置或坐标不变.

对于(ⅰ), 由矢量量化的定义可以证明: k 维矢量量化器 Q 是 k 维空间 $\boldsymbol{R}^k$ 到有限 k 维点集 C 的映射, 即: $Q: \boldsymbol{R}^k \to C$. 对于(ⅱ), 因为同一空间中的任何一点可由除原点外的若干已知点加权而得(这是个显然成立的结论, 可参考代数几何学的知识予证明), 故(ⅱ)成立. 因此式(4)可表示为:

$$\|(\boldsymbol{R}\times\boldsymbol{X}^j)\times\boldsymbol{B} - \boldsymbol{R}\times\boldsymbol{X}^j\|^2 = \|\boldsymbol{X}^j\times\boldsymbol{A} - \boldsymbol{X}^j\|^2 \quad (5)$$

$\boldsymbol{A}, \boldsymbol{B}$ 为加权矩阵, $\boldsymbol{A}, \boldsymbol{B} \in \boldsymbol{R}^{w\times L}$, L 为码本大小. 对于式(5), 证明的关键在于加权矩阵 $\boldsymbol{A} = \boldsymbol{B}$ 是否成立, 若成立, 则式(5)成立.

下面证明第(ⅲ)点: 从 LBG 算法码本初始化的分裂算法分析, 分裂出的新码矢量为 y_0 和 $y_0 + \varepsilon$, y_0 为整个训练集的平均中心, ε为一小范数. 其中 ε 的取值与训练矢量的方差矢量成正比, 变换前后的特征矢量方差具有一致性[16], 从而变换前后的的初始码本是一致的(其他与训练矢量距离有关的码本初始化方法亦适应). 根据 LBG 算法的最邻近原则, 量化区域由 $R_p = \{x \mid x \in R^k,\ d(x, y_p) = \min_q d(x, y_q)\}$ 确定, 由式(3)可知变换前后量化边界是一致的. 根据 LBG 算法新码本集的构成原则, 即平均中心原则. 在相同预置门限值的条件下可得式(3). 量化结果的坐标由加权矩阵决定, 这也就证明了式(5)中 $\boldsymbol{A} = \boldsymbol{B}$, 从而证明式(5)是成立的, 式(5)的成立也就说明式(4)是成立的.

对于式(4), 我们还可以得到一个更为直观的结论: 变换后生成的码本是变换前生成码本的正交变换, 即 $\boldsymbol{Y}'^k = \boldsymbol{R}\times\boldsymbol{Y}^k$. 因为第(5)点已证明 $\boldsymbol{A} = \boldsymbol{B}$, 此处设 $\boldsymbol{A} = \boldsymbol{B} = \boldsymbol{C}$, 则 $\boldsymbol{Y}'^i = (\boldsymbol{R}\times\boldsymbol{X}^j)\times\boldsymbol{C} = \boldsymbol{R}\times(\boldsymbol{X}^j\times\boldsymbol{C}) = \boldsymbol{R}\times\boldsymbol{Y}^i$. 对此结论, 我们可以从宏观和统计的角度进一步分析, 等式 $\boldsymbol{Y}'^k = \boldsymbol{R}\times\boldsymbol{Y}^k$ 的右边为码本向另一空间的映射, 等式左边为训练矢量映射后的码字. 从式(3)可知在随机空间中, 训练矢量之间的距离没有改变, 也就意味着正交变换没有改变矢量的统计分布规律. 同时, 码本为整个训练矢量空间的代表点, 而码字是这个空间的子空间. 在训练矢量统计特征以及子空间划分条件不变的情况下, 子空间的划分结果不会改变.

注意到式(1)和式(2)是对最小距离的求和, 通过以上分析变换前后特征矢量与码字之间的距离保持不变, 最小距离自然不变, 而最小矢量量化误差是特征与码字最小距离的累加和, 从而变换前后最小量化误差不变, 故有效性成立.

下面分析该方法是否安全, 此处安全的定义是敌手和服务器不能获得原始特征. 注册和认证过程中, 用户传送给服务器的为变换后的特征 $\boldsymbol{RX}^i$ 与 $\boldsymbol{RX}^j$, 假设 $\boldsymbol{Y}_1 = \boldsymbol{RX}^i$, $\boldsymbol{Y}_2 = \boldsymbol{RX}^j$, 不失一般性, 可以假设 $\boldsymbol{Y} = \boldsymbol{RX}$. 现在的问题是敌手或第三方获得 $\boldsymbol{Y}$, 能否精确获得 $\boldsymbol{X}$. 直观的理解, 在随机矩阵 $\boldsymbol{R}$ 未知的情况下, 不可能精确获得 $\boldsymbol{X}$ 的每个元素. 理论分析分两种情况: 第一种情况为 $w = r$, 敌手获得 $\boldsymbol{Y}$ 在没有获得 $\boldsymbol{R}$ 的情况下, 无法获得 $\boldsymbol{X}$. 这个结论意味着只要用户对随机矩阵的安全保存(一般存放在智能卡或其他便携设备中), $w = r$ 情况下该方法是安全的. 此外, 当 w 与 r 相差不大的时, 仍然可以保持较高的正识率[13, 14], 此处"相差不大"的含义为存在 $w < r$ 使正识率与 $w = r$ 的情况相等. 这意味着可

以在 $w< r$ 的情况下实现特征保护的目的, 同时具有更高的安全性: 即使敌手或服务器掌握了随机矩阵 $\boldsymbol{R}$(比如存储随机矩阵的设备丢失), 也无法获得原始特征 $\boldsymbol{X}$. 通过 QR 分解[17]证明如下:

设: $\boldsymbol{R}= \boldsymbol{Q}\begin{pmatrix}\overline{\boldsymbol{R}^{\mathrm{T}}}\\ 0\end{pmatrix}$, 此处 $\boldsymbol{Q}$ 为正交矩阵, $\overline{\boldsymbol{R}}$ 为上三角矩阵. 如果 $\boldsymbol{R}$ 为满秩(因为 $\boldsymbol{R}$ 为行正交矩阵, 这点是满足的), 则 $\boldsymbol{X}$ 有最小二乘解.

$$\boldsymbol{X}_{\min\_\mathrm{norm}}= \boldsymbol{Q}\begin{pmatrix}\overline{\boldsymbol{R}^{-1}}\boldsymbol{Y}\\ 0\end{pmatrix}= \boldsymbol{Q}\begin{pmatrix}\overline{\boldsymbol{R}}\\ 0\end{pmatrix}(\overline{\boldsymbol{R}}\,\overline{\boldsymbol{R}^{\mathrm{T}}})^{-1}\boldsymbol{Y}$$
$$= R(R^{\mathrm{T}}R)^{-1}Y= (\boldsymbol{R}^{\mathrm{T}})^{+}\ \boldsymbol{Y} \quad (6)$$

$(\boldsymbol{R}^{\mathrm{T}})^{+}$ 为 $\boldsymbol{R}^{\mathrm{T}}$ 的广义逆矩阵. 对于不定方程 $\boldsymbol{Y}= \boldsymbol{RX}$ 的完全解为:

$$\boldsymbol{X}= \boldsymbol{X}_{\min\_\mathrm{norm}}+ \Psi\boldsymbol{Y} \quad (7)$$

Ψ为 $\boldsymbol{R}$ 的基. 式(6)和式(7)说明, 对于不定方程 $\boldsymbol{Y}= \boldsymbol{RX}$ 具有无穷多个解. 这也意味着在敌手或第三方获得 $\boldsymbol{R}$ 的情况下, 也不能精确获得 $\boldsymbol{X}$.

安全性的满足也说明该方法满足可撤销模板的不可逆性. 通过使用不同的随机矩阵, 不同的用户可以把其特征映射到不同的子空间; 另外一方面, 对于同一用户, 也可以选择不同的随机矩阵在不同的系统中, 或在模板泄漏的情况下, 可以重新更换随机矩阵. 这也说明该方法满足可撤销模板的多样性和可撤销性.

4　实验与分析

如第2节所述, 其有效性通过变换前后识别率的变化说明. 本节从距离和识别率两个角度实验验证该方法的有效性.

实验过程中数据库采用 863 连续语音识别库中的 50 个人作为注册用户集. 该数据库共 1558 条语句, 分为 A1~ A521, B522~ B1040, C1041~ C1558 三组. 说话人包括男女两组各 50 人, 每人朗读上述 1558 条语句中的 521 条. 实验中在每个说话人的 521 条朗读句中选取两句, 一句为训练样本, 一句为测试样本. 为了消除文本内容对识别性能的影响, 选取的原则是每个说话人的测试语句不同于训练语句, 其他说话人的语句与之也不同. 整个样本空间中样本的最小时长为 3.05s, 最大时长为 5.80s. 所有样本均为 16KHz 采样, 16 比特量化, 单声道 wav 格式. 特征采用典型的 MFCC 语音特征, 阶数为 24 阶, 每帧 256 点, 重叠 156 点, 即帧移 100 点. 实验采用 LBG 算法训练 VQ 码本, 码本大小为 64. 实验中 $w= r=$ 16. 随机矩阵的产生采用 Matlab 7.0 自带函数, 通过正交化函数对随机矩阵正交化. 需要注意的是: 注册过程随机矩阵的大小是根据训练样本的特征大小确定的, 而测试样本的时长不一定和训练的一样, 但在映射过程中又必须乘以原随机矩阵. 也就是说, 训练和测试过程提取的特征都必须和同一随机矩阵维数匹配. 此问题的解决方法是固定训练和测试特征 MFCC 矩阵的大小. 固定的方法是根据样本的时长计算帧数范围在 488~ 928 帧之间, 在实验中都取 750 列(对应 750 帧). 如果特征大于 750 列则取前面 750 列; 如果小于 750 帧, 则先计算不足的帧数, 再从第一帧起取相应帧数补足 750 帧. 实验中发现该方法没有影响识别率, 因为这可以理解为取了固定时长的语音样本, 并且从特征的帧数控制矩阵大小要比时间上控制更为精确. 实验中采用码本和测试样本特征之间的平均最小量化误差作为判决条件, 得出变换前后的识别率. 为验证式(4), 对变换前后码字与特征的距离进行比较, 比较结果见图 3.

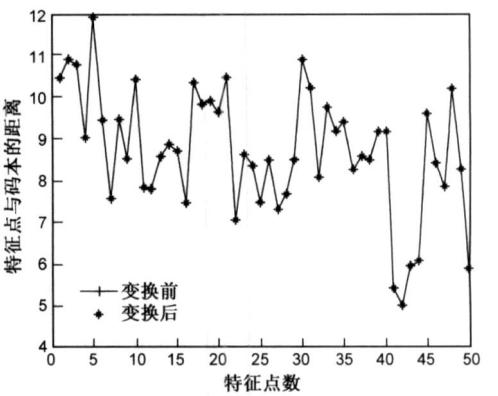

图3　变换前后特征点与码本的距离图

图中十字实线表示变换前特征点与码本中对应码字的距离. 星型线表示变换后的情形. 图中两条线重叠, 这说明变换前后特征点与对应码字的距离保持不变, 这也说明式(4)是成立的. 基于 VQ 算法识别的判决尺度是最小量化误差, 而量化误差的本质是码字与特征矢量序列的最小距离累加和, 图 3 说明变换后码字与特征的距离保持不变, 也就说明变换前后识别率不会改变, 实验也验证变换前后以及取固定帧情况下的正识率都为 96%, 这说明取固定帧没有影响识别率. 经过随机变换后码字与特征之间的距离保持不变, 从而不影响识别率. 实验验证了该方法满足可撤销模板的性能保持的属性, 与上节的理论分析一致.

5　结论

本文针对生物特征认证系统模板泄漏导致的安全问题以及传输安全问题, 同时考虑到基于 VQ 算法声纹认证系统训练数据少, 存储空间和训练时间也比较小的优点, 在基于 VQ 算法声纹认证系统的基础上, 提出了一种基于 MRP 的安全有效的可撤销模板构建方法, 采用随机映射后的特征训练 VQ 码本, 从而达到保护特征和模板的目的. 通过数学分析证明了该方法的有效

性和安全性. 如果随机矩阵为正交矩阵, 该变换并不影响认证矢量的量化误差, 从而保证了认证性能不会因为变换而变坏, 同时变换矩阵的随机性又保证了原始声纹特征的安全性. 初步认证实验的性能达到 96%, 与变换前相等. 如果 $\boldsymbol{R}\in R^{w\times r}$, 且 $w<r$, 那么即使变换矩阵 $\boldsymbol{R}$ 被盗, 原始声纹特征也是不可求的, 表明该方法具有很好的特征传输和存储安全性.

参考文献:

[1] 孙冬梅, 裘正定. 生物特征识别技术综述[J]. 电子学报. 2001, 29(12): 1744- 1748.
SUN Dong-mei, QIU Zheng-ding. A survey of the emerging biometric technology [J]. Acta Electronica Sinica, 2001, 29(12): 1741- 1748. (in Chinese)

[2] J Jiang, Q H He, S H Tang. A dynamic hidden-ID authentication scheme based on 2-dimensional Construction[A]. 2006 International Conference on Communications, Circuits and System [C]. Guiling, China: IEEE, 2006. 1647- 1650.

[3] A K Jain, K Nandakumar, A Nagar. Biometric template security [J]. EURASIP Jounmal on Advances in Signal Processing, Special Issucial on Biometrics, 2008, 2008(1): 1- 20.

[4] Y Dodis, L Reyzin, A Smith. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data[A]. EUROCRYPT 2004[C]. Berlin, German: Springer, 2004. 523- 540.

[5] 张凡, 冯登国, 孙哲南. 一种基于模糊提取的虹膜鉴别方案[J]. 计算机研究与发展. 2008, 45(6): 1036- 1042.
ZHANG Fan, FENG Dengguo, SUN Zhennan. An iris authentication scheme based on fuzzy extractor[J]. Journal of Computer Research and Development, 2008, 45(6): 1036- 1042. (in Chinese)

[6] Q Tang, J Bringer, H Chabanne, et al. A Formal study of the privacy concerns in biometric-based remote authentication schemes[A]. ISPEC 2008[C]. Sydney, Australia: Springer, 2008. 56- 70.

[7] W H Xu, Q H He, Y X Li, et al. Cancelable voiceprint templates based on knowledge signatures[A]. ISECS 2008[C]. Guangzhou, China: IEEE, 2008. 412- 415.

[8] A K Jain. Biometric recognition: overview and recent advances [A]. CIARP 2007[C]. Valparaiso, Chile: Springer, 2007. 13- 19.

[9] N K Ratha, S Chikkerus, J H Connell, et al. Generating cancelable fingerprint template [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2007, 29(4): 561- 572.

[10] A Teoh, B Jin, T Connie, et al. Remarks on biohash and its mathematical foundation[J]. Information Processing Letters, 2006, 100(4): 145- 150.

[11] U Uludag, S Pankanti, A K Jain. Fingerprint template protection using fuzzy vault[A]. ICCAS 2007[C]. Portsmouth, UK: Springer, 2007. 1141- 1151.

[12] 冯全, 苏菲, 蔡安妮. 一种利用多元线性函数绑定指纹细节点与密钥的新方法[J]. 兰州大学学报(自然科学版). 2008, 44(2): 137- 141.
FENG Quan, SU Fei, CAI An-ni. Anew method for binding minutiae and cryptographic key using a multivariable linear function[J]. Journal of Lanzhou University (Natural Science), 2008, 44(2): 137- 141. (in Chinese)

[13] 钱晓东, 王正欧. 文本处理中基于随机映射的加速 LSI 方法[J]. 天津大学学报. 2005, 38(4): 372- 376.
QIAN Xiao-dong, WANG Zheng-ou. Fast latent semantic indexing in text processing based on random mapping[J]. Journal of Tianjin University, 2005, 38(4): 372- 376. (in Chinese)

[14] C L Ying, A T B Jin. Probabilistic random projections and speaker veritcation [A]. ICB 2007 [C], Seoul, Korea: Springer, 2007. 445- 454.

[15] 王伟, 邓辉文. 基于 MFCC 参数和 VQ 的说话人识别系统[J]. 仪器仪表学报. 2006, 27(6): 2252- 2255.
WANG Wei, DENG Huiwen. Speaker recognition system using MFCC features and vector quantization[J]. Chinese Journal of Science Instrument, 2006, 27(6): 2252- 2255. (in Chinese)

[16] A T B Jin, C T Ying. Cancelable biometrics realization with multispace random projections[J]. IEEE Transactions on Systems, Man and Cybernetics, 2007, 37(5): 1096- 1106.

[17] J W Demmel, N J Higham. Improved error bounds for underdetermined system solvers[J]. SIAM Journal on Matrix Analysis And Applications, 1993, 14(1): 1- 19.

作者简介:

徐文华 男, 1978 年生于江西赣州, 华南理工大学通信与信息系统专业博士研究生, 感兴趣的领域主要有信息安全, 生物认证系统安全技术. E-mail: xuwenhua1978@gmail.com

贺前华 男, 1965 年生于湖南邵东, 华南理工大学电信学院教授, 博士生导师, 主要从事语音识别及合成技术, 嵌入式系统设计与应用, 数字信号降噪技术, 信息安全身份认证技术等研究. E-mail: eeqhhe@scut.edu.cn

李 韬 男, 1976 年生于广东揭阳, 现为华南理工大学电信学院讲师, 硕士, 主要从事专用集成电路设计, 语音信号处理, 嵌入式系统设计等研究.

范 炜 男, 1985 年生于广东肇庆, 现为华南理工大学通信与信息系统专业硕士研究生, 主要从事嵌入式系统设计研究.