基于重加密的随机映射指纹模板保护方案

贾姗[1,2]，徐正全[1,2]，胡传博[1,2]，王豪[1,2]

（1. 武汉大学测绘遥感信息工程国家重点实验室，湖北 武汉 430079；
2. 武汉大学地球空间信息技术协同创新中心，湖北 武汉 430079）

摘 要：针对基于随机映射（RP, random projection）的生物特征模板保护算法在模板生成和密钥管理中面临易被攻击而泄露用户隐私的问题，提出一种改进 RP 算法的指纹模板保护方案。首先，在随机映射的基础上，将变换域划分为相互独立的指纹特征匹配域和加噪干扰域；在子域内加噪后利用子随机映射矩阵交叉融合生成模板。同时，引入重加密机制实现对变换密钥（RP 矩阵）的安全存储和传输。实验结果和分析表明，与现有的 RP 模板保护方法相比，所提方案具有更高的抵抗攻击能力并能保持 RP 算法的匹配性能和模板可撤销性。

关键词：指纹隐私保护；随机映射；重加密；安全认证

中图分类号：TP309.2

文献标识码：A

doi: 10.11959/j.issn.1000-436x.2018031

Fingerprint template protection by adopting random projection based on re-encryption

JIA Shan[1,2], XU Zhengquan[1,2], HU Chuanbo[1,2], WANG Hao[1,2]

1. State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, Wuhan 430079, China
2. Collaborative Innovation Center for Geospatial Technology, Wuhan University, Wuhan 430079, China

Abstract: In random projection (RP) based biometric template protection methods, the generated template and key are vulnerable to attacks, which may cause the leakage of users' privacy. To solve this problem, an improved RP-based fingerprint template protection method was proposed. First, based on the RP result, the proposed method divided the projection domain into fingerprint matching domain and noise adding domain that were mutually independent, then fused them with two sub-matrices of the random projection matrix and saved the result as template. In addition, re-encryption mechanism was introduced to realize secure storage and transmission of the key (RP matrix). Experimental results show that the proposed method can achieve stronger ability to resist different attacks than existing RP-based biometric template protection methods, and also guarantee high matching accuracy and revocation.

Key words: fingerprint privacy protection, random projection, re-encryption, secure authentication

1 引言

随着人工智能的快速发展，模式识别技术已广泛应用于诸多领域，其中，生物特征识别技术利用人体特征进行个人身份的鉴定，能为智能时代提供最为便捷和安全的身份认证，成为国内外研究的热点之一。生物特征识别技术包含人体生理特征识别，如人脸、指纹、虹膜等，和行为模式识别，如步态、声音、笔迹等。比起密钥、令牌等传统基于物品的认证方式，生物特征本身具有不易遗忘、难

收稿日期：2017-09-05；**修回日期**：2018-01-13

通信作者：徐正全，xuzq@whu.edu.cn

基金项目：武汉市应用基础研究计划基金资助项目（No.2017010201010114）；国家自然科学基金资助项目（No.41671443, No.41571426）；国家重点基础研究发展计划（“973”计划）基金资助项目（No.2011CB302306）

Foundation Items: Applied Basic Research Program of Wuhan (No.2017010201010114), The National Natural Science Foundation of China (No.41671443, No.41571426), The National Basic Research Program of China (973 Program) (No.2011CB302306)

以猜测和窃取、不易丢失的优势，具有普遍性、唯一性和永久性。目前，基于生物特征的身份认证已在国家安全、金融、司法、电子商务、电子政务等应用领域提供了自动、准确的身份标识。

然而，基于人体生物特征的身份认证需要存储注册用户的生物特征模板，数字化后的特征可能会遭受攻击或失窃而造成严重后果[1]。因为生物特征不可改变，并且与用户的身份永久关联，一旦被不法分子复制、篡改或盗取后非法滥用，生物特征信息可能会永远丢失，或在每个此生物特征应用的系统中失效，用户隐私也将受到威胁。以指纹为例，文献[2]表明从存储的指纹细节点模板中可以完全恢复出原始的指纹图像，从而泄露用户隐私。此外，同一生物特征模板应用保存在多个系统中，易被不法分子追踪从而实现多个数据库之间的交互匹配。因此，为了有效保护用户隐私和信息安全，保护存储的生物特征模板变得尤为重要。

生物特征加密技术[3]是研究者近年来提出的保护生物特征隐私的有效策略，将生物特征识别与密码学相结合，为用户提供安全的身份验证。理想的生物特征加密技术对生物特征模板的保护应至少具备以下 3 个特性[4]：不可逆性（生成生物特征模板容易，但从存储的模板中难以恢复、重建出原始的生物特征数据）；不可链接性（基于同一生物特征，可以生成不同版本的模板以在不同应用系统中应用；也可以在同一应用系统中实现对模板的撤销和重新发布，并且各模板之间、以及模板与原始生物特征之间不可匹配）；识别性能（生物特征模板保护策略对身份认证性能影响微小，即不能严重影响认证的准确率）。

目前，得到广泛研究的不可追踪生物特征认证技术[5,6]在一定程度上实现了生物特征安全性和隐私性的保护。其中，基于随机映射[7]的特征变换方法不仅能实现模板的可撤销性，同时，在 Euclidean 空间能以极高的概率保存点与点之间的距离，对匹配性能影响很小而被应用在生物特征模板保护中。Ngo 等[8]较早提出了基于 RP 的 BioHashing 方法，利用用户特定的 RP 矩阵对生物特征进行映射变换后，量化得到二进制的数据保存为不可逆生物特征模板。该方法可获得近于 0 的等错误率（EER, equal error rate），但量化处理降低了认证准确率，同时随机映射在量化域内的距离保持特性没有相关的理论证明。基于 BioHashing 的思想，Jin 等[9]通过映射指纹的 MVD（minutiae vicinity decomposition）特征生成可撤销的指纹模板；Teoh 等[10]提出无量化处理的 MRP（multispace random projection）随机映射模板保护方法，利用用户特定的伪随机数（PRN, pseudorandom number）产生随机矩阵，在降维的同时实现双因子认证。Wang 等[11]基于 RP 产生可变换的生物特征模板，并对随机映射算法的隐私保护特性给出了详细的理论分析。Khan 等[12]使用散列算法替代量化处理对随机映射的结果进行保护，提出了基于双因子认证的 KRP-AH 算法，获得了较高的安全性，但是散列算法降低了认证性能。Yang 等[13]则针对生物特征的不定长特征提出了根据指纹细节点维数进行非线性动态映射（DRP）的生物模板保护方法；Anzaku 等[14]则利用用户指纹的定长 Fingercode 特征和 PRN 在 RP 变换不降维的情况下实现安全认证，计算效率提高，但当 RP 变换矩阵和模板被攻击时，通过反变换即能完全恢复出原始指纹特征而泄露用户隐私。

已有的基于随机映射的生物特征模板保护技术虽然可以提高生物特征的安全性，但仍存在以下 2 个问题。

1) 直接保存随机映射后的变换数据作为生物特征模板，存在利用逆变换或交叉匹配攻击而完全恢复原始生物特征的隐患[15]，无法有效保护用户隐私；同时，当变换后的特征被盗取时，此类方法无法抵抗统计攻击、重放攻击等。

2) 随机映射矩阵或产生映射矩阵的伪随机序列作为生物特征变换密钥，需要被存储或传输。如果被用户保存在令牌或智能卡中，实现双因子认证，安全性较高，但其安全性取决于随机数令牌的安全性[16]，并且多因子认证为用户带来使用和存储的不便；若被用户终端保存，则将用户与终端绑定，应用受到局限；若被应用端保存，在半可信环境中，密钥容易被非法盗取而存在用户的生物特征信息被泄露的安全隐患。因此，对变换密钥需要更安全有效的管理机制。

指纹作为目前研究最成熟，应用最广泛的生物特征，其安全性问题备受关注。本文以指纹为例，首先针对传统随机映射算法在模板生成中存在的问题，在原算法的基础上将映射域划分为相互独立的指纹特征匹配域与噪声干扰域，通过相应的 2 个子随机映射矩阵进行交叉融合后保存为模板。其次，针对变换密钥（随机映射矩阵）的管理问题，引入

具备密文安全转换功能的重加密机制实现对映射矩阵的安全存储和传输。在注册过程由用户终端一次加密后将密文存储在应用端，认证过程则由应用端 2 次加密后传至用户终端，通过一次解密获得明文，使用户端不依赖于应用端的可信度进行数据安全管理。结合本文在算法上的改进使指纹特征模板即使在丢失的情况下也无法被完全恢复，有效提高认证的安全性。本文贡献主要有以下 3 点。

1) 提出了一种改进的随机映射指纹模板生成方法，使注册保存的模板融合了随机干扰噪声；在认证过程中生成的变换特征也具有动态变化性，并且能利用随机映射矩阵的正交性去除噪声域，获得与原始随机映射算法一致的匹配特征，在提高模板安全性的同时能够保持原始算法的良好匹配性能。

2) 提出了一种基于重加密的随机映射矩阵管理机制，将随机映射矩阵以密文形式存储在应用端，在认证过程中通过重加密转换为认证终端可以解密的密文，在保证安全性和可用性的同时将密钥的存储开销从用户端转移至应用端。

3) 实验结果和分析表明本文方案对指纹认证的准确率和计算时间影响较小，生成的模板具有良好的不可链接性；同时，在认证过程中能有效抵抗重放攻击、相似性攻击、交叉匹配攻击等针对模板的常见攻击，具备较高的安全性。

2 预备知识

2.1 随机映射

随机映射是一种将特征从 n 维 Euclidean 空间向 $m(n \geqslant m)$ 维 Euclidean 空间通过随机矩阵进行线性映射的过程。其主要思想来源于 Johnson-Lindenstrauss 定理[17]，即对于一个正整数 N、任意 $0<\varepsilon<1$ 和 $m(m \geqslant m_0 = O(\varepsilon^{-2}\log N))$，存在 $\mathbb{R}^n$ 空间的矢量 $\boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_N$ 到 $\mathbb{R}^m$ 空间的 $\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_N$ 的映射 f：$\mathbb{R}^n \to \mathbb{R}^m$，对所有的 $\boldsymbol{u}, \boldsymbol{v}$ 和 $i, j \in [1, N]$ 有

$$(1-\varepsilon)\left\|\boldsymbol{u}_i - \boldsymbol{u}_j\right\|^2 \leqslant \left\|\boldsymbol{v}_i - \boldsymbol{v}_j\right\|^2 \leqslant (1+\varepsilon)\left\|\boldsymbol{u}_i - \boldsymbol{u}_j\right\|^2 \quad (1)$$

此定理说明了从 n 维空间到 m 维空间映射时，两点之间的距离以极高的概率 $1\pm\varepsilon$ 接近于原始数据，从而实现了距离保持特性。文献[17,18]证明可以通过随机正交矩阵实现这样的映射，实现过程如下。生成 $n \times m$ 维的随机矩阵；进行 Gram-Schmidt 正交化后得到矩阵 $\boldsymbol{R}$，对原始特征 $\boldsymbol{x} \in \mathbb{R}^n$ 利用式(2)进行随机映射，得到变换特征。

$$\boldsymbol{y} = \sqrt{\frac{n}{m}}\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x} \quad (2)$$

其中，$\boldsymbol{y} \in \mathbb{R}^m$，通常 $m = n$，当 $m < n$ 时，随机映射成为一种有效的降维方法[19]。由于 Gram-Schmidt 正交化的过程要求输入向量是线性独立的，而随机生成的矩阵很难满足此性质，因此，文献[7,20]提出 RP 矩阵可以由独立同分布的高斯序列产生，并且证明了元素服从高斯分布的矩阵 $\boldsymbol{R}$ 具有正交性，尤其在高维空间中，$\sqrt{\frac{n}{m}}\boldsymbol{R}\sqrt{\frac{n}{m}}\boldsymbol{R}^{\mathrm{T}}$ 近似于单位矩阵，从而实现特征变换前后对欧氏距离的保持特性。

将随机映射用于生物特征模板保护中，针对同一生物特征基于不同的 RP 矩阵可以生成不同的模板，实现模板的可再生性和可撤销性；同时，随机映射的距离保持特性使在变换域基于欧氏距离的匹配对认证准确性影响较小。

2.2 重加密机制

重加密，常指代理重加密（proxy re-encryption），于 1998 年由 Blaze 等[21]提出，是一种具备密文安全转换功能的新型公钥加密体制。针对不可信的网络环境，重加密机制能够有效保障用户数据的安全性和可共享性。在典型的代理重加密体制中，引入一个半可信代理者进行密文的存储和转换，能将由委托者用公钥加密的秘密数据密文转换为由被委托者的公钥对同一明文加密的密文，然后被委托者利用其自身私钥解密转换后的密文，从而获得秘密信息，其具体过程如图 1 所示，其中序号表示重加密的执行顺序。在密文转换过程中，代理者必须拥有一个由委托者授权的针对被委托者的密文转换密钥（重加密密钥），且代理者无法获得有关明文的任何信息。重加密密钥生成算法是单向不可逆的，无法由重加密密钥计算出私钥信息，保证了数据拥有者和数据使用者的权益。

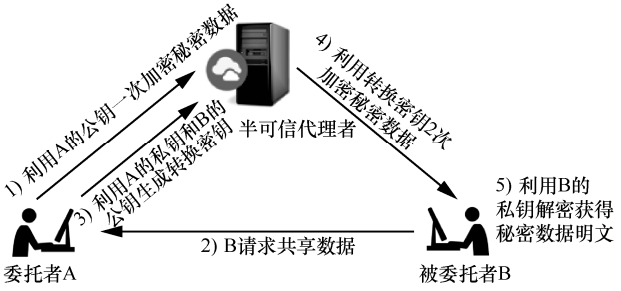


图 1 重加密机制示意

由图 1 可见，重加密机制提供了不依赖于代理者可信度的数据安全管理方法。通过对秘密信息的 2 层加密，从数据源头上控制代理者对数据明文的访问权限，让代理者在存储密文的同时，能够根据被委托者的需要提供不同的重加密密文版本，从而有效防范秘密数据在传输和存储过程中的泄露风险。而对于用户而言，在保证秘密信息安全的前提下将存储开销转移至半可信代理者，同时在应用上与传统的方式没有区别，通过一次解密即可获得明文数据。

2.3　问题陈述

随机映射算法利用变换特征的距离保持特性能实现良好的匹配性能，变换随机映射矩阵能实现模板的可撤销性，但在安全性上仍存在以下两方面的不足。

1) 直接保存随机映射后的变换特征作为模板，抵抗攻击能力较弱。

若随机映射矩阵丢失，同时变换特征泄露（已知密文和密钥攻击），则当 $m=n$ 时，通过逆变换即可恢复出原始特征；对于 $m<n$ 的情况，利用交叉匹配攻击，即已知基于相同生物特征的 $\left\lceil \frac{n}{m} \right\rceil$ 个映射和随机映射矩阵，也可完全恢复出原始生物特征；同时当变换后的特征被盗取时，此类方法无法抵抗重放攻击。文献[8,12,13]在映射后再对特征进行不可逆变换，能有效提高模板的安全性，但在一定程度上损失了匹配精度。

2) 随机映射矩阵作为变换密钥，直接存储或传输存在安全隐患。

大多文献将随机映射矩阵 $\boldsymbol{R}$ 或产生 $\boldsymbol{R}$ 的伪随机序列作为用户密钥保存在令牌或智能卡中，但随着生物特征身份认证应用的不断增长，这种双因子认证方式将给用户带来存储和使用的诸多不便。若将 $\boldsymbol{R}$ 存放在应用端，虽然减少了用户的密钥管理开销，但不可信的应用环境使生物特征模板容易被攻击而泄露用户隐私。第三方认证[22]在一定程度上可以提高认证的安全性，但存在第三方无法保证自身可信度的问题[23]，并且管理成本和计算复杂度较高。ARM TrustZone 技术[24]的发展使设备能够支持完全可信执行环境，配置在终端设备的应用处理器中为认证、支付、内容保护等应用场景提供安全的计算和存储区。然而，将用户特定的 $\boldsymbol{R}$ 直接保存在设备的 TrustZone（可信计算区）内，则将用户与设备进行了绑定，典型应用为手机等移动设备；而针对与用户无绑定的终端设备，如 ATM 机等，则需要在 TrustZone 内保存与用户数量相等的 $\boldsymbol{R}$，将带来巨大的存储开销。

因此，本文提出一种基于重加密的随机映射指纹模板保护方案，首先改进随机映射算法的模板生成方式，再在改进算法的基础上，引入重加密机制加强对随机映射矩阵的安全管理。

3　方案设计

3.1　方案框架

本文针对随机映射算法在模板生成和密钥管理中存在的问题，提出改进的随机映射算法以提高模板的安全性，同时引入重加密机制实现对随机映射矩阵的安全存储和传输。具体方案框架如图 2 所示，在生物特征身份认证系统的注册阶段，针对输入的指纹图像 $\boldsymbol{Fin}$，提取指纹特征 $\boldsymbol{x}$ 后，利用改进的随机映射算法生成指纹模板 $\boldsymbol{T}$，并结合重加密机制实现对随机映射矩阵的加密传输和存储；在注册过程中，对输入指纹 $\boldsymbol{Fin}'$ 提取特征 $\boldsymbol{x}'$ 后，先利用重加密机制解密获得密钥（随机映射矩阵），再基于改进的随机映射算法生成变换特征 $\boldsymbol{y}_e'$，与存储的

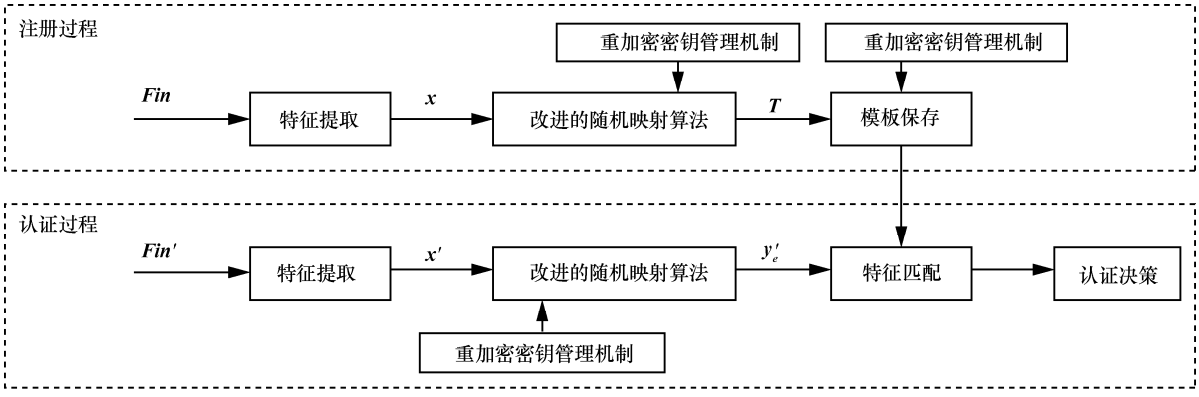


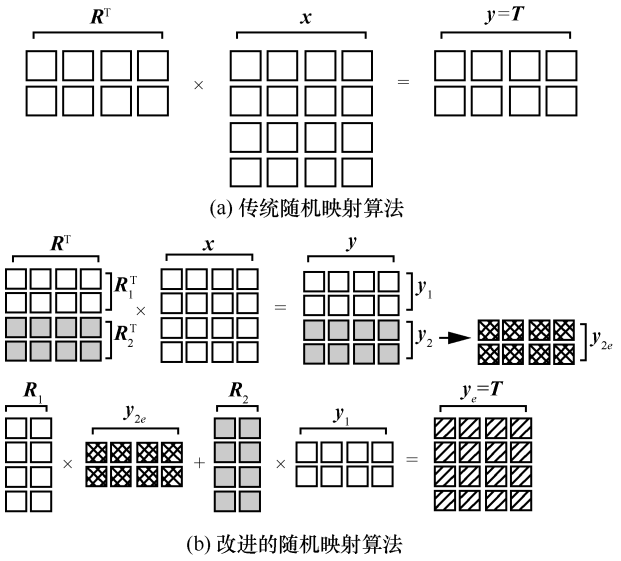
图 2　基于重加密的随机映射指纹模板保护方案框架

指纹模板进行特征匹配从而完成身份认证。

3.2 改进的随机映射算法

3.2.1 算法框架

传统随机映射算法在模板生成中存在以下问题问题。直接保存映射后的变换特征为模板，难以抵抗已知密文和密钥攻击、交叉匹配攻击；而对变换特征再进行不可逆变换会损失匹配精度。此外，每次认证过程生成的变换特征相近，若被盗取，此类方法在统计攻击的情况下也会泄露用户隐私，如认证频率、认证用户数量等。针对以上问题，本文先对随机映射算法进行改进，利用映射矩阵的正交性在不影响匹配性能的同时引入随机干扰噪声以提高模板的安全性。算法在改进前后的对比框架如图 3 所示，改进算法对输入的生物特征 $(\boldsymbol{x})$ 生成变换特征 $(\boldsymbol{y})$ 后，划分 $\boldsymbol{y}$ 为相互独立的特征匹配域 $(\boldsymbol{y}_1)$ 和加噪干扰域 $(\boldsymbol{y}_2)$，对加噪干扰域添加随机噪声后（得到 $\boldsymbol{y}_{2e}$），再利用相应的 2 个子随机映射矩阵 $(\boldsymbol{R}_1,\boldsymbol{R}_2)$ 进行交叉融合后生成模板 $\boldsymbol{T}$，即 $\boldsymbol{T}=\boldsymbol{R}_2\boldsymbol{y}_1+\boldsymbol{R}_1\boldsymbol{y}_{2e}$。



(a) 传统随机映射算法

(b) 改进的随机映射算法

图 3 随机映射算法的模板生成方式对比

在认证过程中，同样对输入的生物特征 $(\boldsymbol{x}')$ 利用改进的随机映射算法生成变换特征 $(\boldsymbol{y}_e')$，在特征匹配阶段利用 $\boldsymbol{R}_2$ 能够提取出具有距离保持特性的特征，具体如定理 1 所述。

定理 1 特征匹配过程利用子随机映射矩阵 $\boldsymbol{R}_2$ 即可提取出与原始随机映射算法相同的特征 $\boldsymbol{y}=\sqrt{\frac{n}{m}}\boldsymbol{R}_1^{\mathrm{T}}\boldsymbol{x}$，使匹配特征具有距离保持特性。

证明 由 $\boldsymbol{R}_1$、$\boldsymbol{R}_2$ 的正交性，得 $\boldsymbol{R}_2^{\mathrm{T}}\boldsymbol{R}_2=\boldsymbol{I}$（$\boldsymbol{I}$ 为 $m\times m$ 维单位阵），$\boldsymbol{R}_2^{\mathrm{T}}\boldsymbol{R}_1=\boldsymbol{O}$（$\boldsymbol{O}$ 为 $m\times m$ 维零矩阵）。

故从保存模板 $\boldsymbol{T}$ 中利用子随机映射矩阵 $\boldsymbol{R}_2$ 通过式(3)提取特征，得到特征 $\boldsymbol{F}$ 为

$$\begin{aligned}\boldsymbol{F}&=\sqrt{\frac{n}{m}}\boldsymbol{R}_2^{\mathrm{T}}\boldsymbol{T}=\sqrt{\frac{n}{m}}\boldsymbol{R}_2^{\mathrm{T}}\boldsymbol{R}_2\boldsymbol{y}_1+\sqrt{\frac{n}{m}}\boldsymbol{R}_2^{\mathrm{T}}\boldsymbol{R}_1\boldsymbol{y}_{2e}\\&=\sqrt{\frac{n}{m}}\boldsymbol{y}_1=\sqrt{\frac{n}{m}}\boldsymbol{R}_1^{\mathrm{T}}\boldsymbol{x}\end{aligned}\tag{3}$$

从认证过程产生的变换特征 $\boldsymbol{y}_e'$ 中利用子随机映射矩阵 $\boldsymbol{R}_2$ 提取特征，得到特征 $\boldsymbol{F}'$ 为

$$\begin{aligned}\boldsymbol{F}'&=\sqrt{\frac{n}{m}}\boldsymbol{R}_2^{\mathrm{T}}\boldsymbol{y}_e'=\sqrt{\frac{n}{m}}\boldsymbol{R}_2^{\mathrm{T}}\boldsymbol{R}_2\boldsymbol{y}_1'+\sqrt{\frac{n}{m}}\boldsymbol{R}_2^{\mathrm{T}}\boldsymbol{R}_1\boldsymbol{y}_{2e}'\\&=\sqrt{\frac{n}{m}}\boldsymbol{y}_1'=\sqrt{\frac{n}{m}}\boldsymbol{R}_1^{\mathrm{T}}\boldsymbol{x}'\end{aligned}\tag{4}$$

其中，$\boldsymbol{y}_1'$、$\boldsymbol{y}_{2e}'$ 分别为认证过程中划分产生的子变换特征。由此可见，利用 $\boldsymbol{R}_2$ 能提取出与原始随机映射算法一致的匹配特征（$\boldsymbol{R}_1$ 即对应传统算法中的 $\boldsymbol{R}$），具有距离保持特性而对认证准确性影响较小。

同时，改进后的随机映射算法能解决原始随机映射算法的不足，具体如下。

1) 提高了抵抗已知密文和密钥攻击、交叉匹配攻击的能力。算法对变换特征进行划分，本质是将 $\boldsymbol{R}$ 划分为 2 个子随机映射矩阵 $\boldsymbol{R}_1$(用于特征匹配域 $\boldsymbol{y}_1$ 的生成)和 $\boldsymbol{R}_2$(用于干扰噪声域 $\boldsymbol{y}_2$ 的生成)，加入随机噪声后再利用 $\boldsymbol{R}_1$、$\boldsymbol{R}_2$ 进行交叉融合生成保存模板，即令 $\boldsymbol{R}_1$ 绑定 $\boldsymbol{y}_2$、$\boldsymbol{R}_2$ 绑定 $\boldsymbol{y}_1$，认证过程应用端只需要 $\boldsymbol{R}_2$ 提取出 $\boldsymbol{y}_1$ 进行匹配。因此，针对已知密文和密钥攻击或交叉匹配攻击使 $\boldsymbol{R}_2$ 和生物特征模板 $\boldsymbol{T}$ 均泄露时，攻击者将获得 $\boldsymbol{y}=\sqrt{\frac{n}{m}}\boldsymbol{R}_1^{\mathrm{T}}\boldsymbol{x}$，由于 $\boldsymbol{R}_1$ 难以恢复，故无法推测出原始生物特征 $\boldsymbol{x}$。从而提高了生物特征模板的安全性。

2) 认证过程生成的变换特征具有动态变化性，能抵抗统计攻击。算法对变换特征添加随机噪声，使交叉融合后的特征受干扰噪声的扩散影响，在每次认证过程中生成的特征信息均具有随机变化性，有效防止变换特征被截获后通过统计攻击而泄露用户隐私。

3.2.2 算法实施

改进后的随机映射指纹模板保护算法的实现过程如下所示。

1) 注册过程

步骤 1　生成随机映射矩阵

生成服从独立同高斯分布的 $n\times n$ 维的随机矩阵 $\boldsymbol{R}$，即 $\boldsymbol{R}=[\boldsymbol{r}_1,\boldsymbol{r}_2,\cdots,\boldsymbol{r}_n]$，$\boldsymbol{r}_k(1\leqslant k\leqslant n)$ 为 n 维列向量，其元素为独立同分布的高斯随机变量，即 $r_{ij}\sim \mathrm{N}(\frac{0,1}{n})$，$(1\leqslant i,j\leqslant n)$。

对 $\boldsymbol{R}$ 矩阵进行 Gram-Schmidt 正交化（目的是保持映射后的矢量和原始矢量的最大相似性[25]）。

均分 $\boldsymbol{R}$ 得到相互独立的子随机映射矩阵 $\boldsymbol{R}_1$ 和 $\boldsymbol{R}_2$，其中，$\boldsymbol{R}_1=[\boldsymbol{r}_1,\boldsymbol{r}_2,\cdots,\boldsymbol{r}_m]$，$\boldsymbol{R}_2=[\boldsymbol{r}_{m+1},\boldsymbol{r}_{m+2},\cdots,\boldsymbol{r}_n]$，$m=\dfrac{n}{2}$。

步骤 2　随机映射过程

对指纹特征 $\boldsymbol{x}$ 进行随机映射得到变换特征 $\boldsymbol{y}$，即 $\boldsymbol{y}=\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x}$。

划分 y 为指纹特征匹配域 $\boldsymbol{y}_1$ 与加噪干扰域 $\boldsymbol{y}_2$，其中，$\boldsymbol{y}_1=\boldsymbol{R}_1{}^{\mathrm{T}}\boldsymbol{x}$，$\boldsymbol{y}_2=\boldsymbol{R}_2{}^{\mathrm{T}}\boldsymbol{x}$，均为 $m\times n$ 维特征；在 $\boldsymbol{y}_2$ 域添加随机均匀分布的 $m\times n$ 维噪声 $\boldsymbol{N}_s$，得到 $\boldsymbol{y}_{2e}=\boldsymbol{y}_2+\boldsymbol{N}_s$。

特征融合：利用子随机映射矩阵 $\boldsymbol{R}_1$，$\boldsymbol{R}_2$ 交叉融合变换特征，得到 $\boldsymbol{y}_e=\boldsymbol{R}_2\boldsymbol{y}_1+\boldsymbol{R}_1\boldsymbol{y}_{2e}$。

步骤 3　生成模板：保存 $\boldsymbol{T}=\boldsymbol{y}_e$ 为生物特征模板。

2) 认证过程

步骤 1　获取随机映射矩阵

获取注册过程的随机映射矩阵 $\boldsymbol{R}$。

步骤 2　随机映射过程

对输入指纹特征 $\boldsymbol{x}'$（$n\times n$ 维）进行随机映射得到变换特征 $\boldsymbol{y}'=\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x}'$。

同注册过程，对变换域进行均等划分得到指纹特征匹配域 $\boldsymbol{y}_1'$ 与加噪干扰域 $\boldsymbol{y}_2'$，对 $\boldsymbol{y}_2'$ 域添加随机均匀分布的噪声 $\boldsymbol{N}_s'$，得到 $\boldsymbol{y}_{2e}'=\boldsymbol{y}_2'+\boldsymbol{N}_s'$。

特征融合：得到变换特征 $\boldsymbol{y}_e'=\boldsymbol{R}_2\boldsymbol{y}_1'+\boldsymbol{R}_1\boldsymbol{y}_{2e}'$。

步骤 3　特征提取与匹配

利用式(3)和式(4)提取匹配特征 $\boldsymbol{F}$、$\boldsymbol{F}'$。

计算匹配数值 $s=f(\boldsymbol{F},\boldsymbol{F}')$（其中，$f(\cdot)$ 为欧式距离计算函数），实现身份认证。

3.3　基于重加密的随机映射矩阵密钥管理

改进的随机映射算法提高了生物特征模板和身份认证的安全性，但在注册和认证过程中涉及的随机映射矩阵 $\boldsymbol{R}$ 作为特征变换密钥，需要安全的传输和存储机制。已有的算法将 $\boldsymbol{R}$ 或生成 $\boldsymbol{R}$ 的伪随机序列作为用户密钥保存在令牌或智能卡中，但这种双因子认证方式随着生物特征识别的广泛应用将给用户带来诸多不便，同时密钥容易丢失。因此，本文基于改进的随机映射模板保护算法，引入重加密机制加强对随机映射矩阵 $\boldsymbol{R}$ 的安全管理。

基于 ElGamal 算法构造的重加密模型在 Blaze 等[21]提出重加密机制的同时得到了验证，其安全性是基于有限域上的离散对数问题的困难性。本文将在改进的随机映指纹模板保护算法中，结合基于 ElGamal 算法的重加密模型，在配置了 TrustZone 的用户终端，设计加强密钥保护的指纹认证方案。对应典型的重加密机制（如图 1 所示），用于身份注册的用户终端对应委托者，实现变换密钥和生物特征模板的生成，并完成对密钥的一次加密；应用端对应半可信代理者，在注册过程实现生物特征模板和变换密钥的存储，在认证过程实现对密钥的重加密和生物特征的匹配决策；用于身份认证的用户终端则对应被委托者，实现对变换密钥的解密，并生成变换特征用于匹配。当用户终端与用户绑定时，如手机终端，则注册与认证涉及的用户终端只有一个；若用户终端与用户无绑定，如银行 ATM 机，则涉及的用户终端为多个。本文方案针对用户与用户终端绑定、用户与用户终端不绑定的形式均具有可行性，其实现过程如下所示。

Setup 阶段。输入安全参数 par 和双线性对参数 $(p,g,\mathbb{G}_1,\mathbb{G}_2,e)$，系统运行初始化算法，其中，$p$ 是一个大素数，g 是群 $\mathbb{G}_1$ 的生成元，双线性对运算 e：$\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$，$g\in\mathbb{G}_1$，$e(g,g)\in\mathbb{G}_2$。

利用密钥生成算法生成用户端公私钥对 (pk_i,sk_i)，基于 ElGamal 算法则公钥 $pk_i=(p,g,y_i)$，$y_i=g^{x_i}\bmod p$；私钥 sk_i 为随机数 x_i（$x_i\in\mathbb{Z}_p^*,\mathbb{Z}_p^*$ 是一个小于 p 的正整数构成的群），保存在用户终端的 TrustZone 区。

对每个用户终端 i，用其私钥和其他每个用户端 j 的公钥生成转换密钥 $\boldsymbol{rekey}_{i,j}$，参考文献[26]：

$\boldsymbol{rekey}_{i,j}=\mathrm{ReKeygen}(sk_i,pk_j)=y_j^{\frac{1}{x_i}}\bmod p=g^{\frac{x_j}{x_i}}\bmod p$，得到重加密密钥矩阵 $\boldsymbol{rekey}$（$P\times P$ 维，P 为用户终端总数）。同时，生成应用端公私钥对 (pk_a,sk_a)，与 $\boldsymbol{rekey}$ 共同保存在应用端。

注册阶段。用户在用户终端 i 请求注册，应用端将公钥传给用户端。

在用户终端 i 的 TrustZone 内输入指纹图像 $\boldsymbol{Fin}$，提取特征 $\boldsymbol{x}$ 后，利用 3.2 节算法生成随机映射矩阵 $\boldsymbol{R}$ 和模板 $\boldsymbol{T}$。由于直接对 $\boldsymbol{R}$（$n\times n$ 维）进行重加密保护计算复杂度较高，因此，先用低维的随机密钥 k $(k\in\mathbb{Z}_p^*)$ 利用效率更高的对称加密方法加密 $\boldsymbol{R}$，得到 $\boldsymbol{R}_e=E(k,\boldsymbol{R})$，则将对 $\boldsymbol{R}$ 的重加密保护转为对 k 的保护；再利用用户端公钥 pk_i 经一次加密 k 得到 $k_e=E(pk_i,k)=(a,b)=(y_i^{k_1} \bmod p, g^{k_1}k \bmod p)$，其中，$k_1$ 为随机数，$k_1\in\mathbb{Z}_p^*$，且满足 $Gcd(k_1, p-1)=1$。同样，将认证过程的特征匹配密钥 $\boldsymbol{R}_2$ 利用应用端公钥加密得到 $\boldsymbol{R}_{2e}$。用户终端将产生的信息 $k_e\|\boldsymbol{R}_e\|\boldsymbol{T}\|\boldsymbol{R}_{2e}\|i$ 传至应用端保存，并注销所有数据。

应用端用私钥解密 $\boldsymbol{R}_{2e}$ 得到 $\boldsymbol{R}_2$ 保存，从而避免认证过程中对的传递。具体过程如图 4 所示。

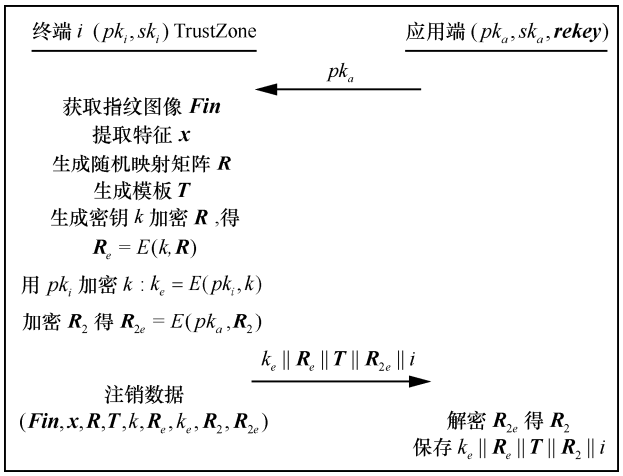


图 4 注册过程

认证阶段。用户在用户终端 j 请求身份认证，得到从应用端传来的 $\boldsymbol{R}_e\|k_e'\|\theta$，其中，$k_e'$ 为应用端利用重加密密钥 $\boldsymbol{rekey}_{i,j}$ 对 k_e 进行 2 次加密得到的密文，其具体如式(5)和式(6)所示；θ 为应用端产生的随机数，传至用户终端，融合在变换特征中用于特征匹配时的合法性验证，以抵抗重放攻击。

$$\begin{aligned}k_e'&=E(\boldsymbol{rekey}_{i,j},k_e)=(c,b)\\&=(\mathrm{ReEnc}(a,\boldsymbol{rekey}_{i,j}),g^{k_1}k \bmod p)\end{aligned}\tag{5}$$

$$c=\mathrm{ReEnc}(a,\boldsymbol{rekey}_{i,j})=y^{k_1}\boldsymbol{rekey}_{i,j} \bmod p\tag{6}$$

用户终端在 TrustZone 内对输入的指纹 $\boldsymbol{Fin}'$ 提取特征 $\boldsymbol{x}'$，并用私钥 sk_j 一次解密 k_e' 得到 k。

$$\begin{aligned}\mathrm{Dec}(sk_j,k_e')&=\frac{b}{(c)^{\frac{1}{x_j}}} \bmod p\\&=\frac{g^{k_1}k}{(y^{k_1}\boldsymbol{rekey}_{i,j})^{\frac{1}{x_j}}} \bmod p\\&=\frac{g^{k_1}k}{\left(g^{x_ik_1}g^{\frac{x_j}{x_i}}\right)^{\frac{1}{x_j}}} \bmod p=k\end{aligned}\tag{7}$$

用户端再利用 k 解密 $\boldsymbol{R}_e$ 得到 $\boldsymbol{R}$，利用 3.2 节算法生成变换特征 $\boldsymbol{y}_e'$，其中，$\boldsymbol{y}_e'$ 需加入 $\boldsymbol{R}_2$ 与矩阵 $\boldsymbol{\theta}'$ 的融合矩阵：$\sqrt{\frac{m}{n}}\boldsymbol{R}_2\boldsymbol{\theta}'$（$\boldsymbol{\theta}'$ 为元素全为随机数 θ 的 $m\times n$ 维矩阵），用于匹配过程的用户合法性验证。最后，将 $\boldsymbol{y}_e'$ 传至应用端进行特征匹配，同时注销所有数据。

应用端利用 $\boldsymbol{R}_2$ 和等式(3)、(4)提取 $\boldsymbol{T}$ 和 $\boldsymbol{y}_e'$ 的匹配特征 $\boldsymbol{F}$ 和 $\boldsymbol{F}'$，进行比对实现身份认证（若遭受重放攻击，则提取的 θ 与应用端随机生成的 θ 不具备一致性而无法去除，将导致匹配失败）。具体过程如图 5 所示。

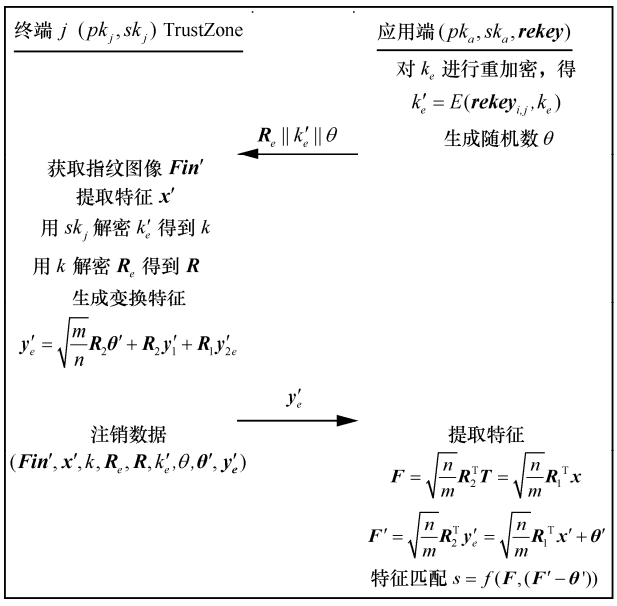


图 5 认证过程

4 安全性分析

生物特征身份认证涉及的安全性和隐私保护主要是指存储的生物特征模板即使在被攻击的情况下也不会泄露用户信息。本文针对 6 种常见的生

物特征模板攻击，对提出的基于重加密的随机映射指纹模板保护方法进行了安全性分析。

1) 不可逆性（已知模板的攻击）。

定理 2　假设攻击者获取到生物特征模板 $\boldsymbol{T}$，则推测出原始生物特征 $\boldsymbol{x}$ 的计算复杂度为 $O(2^{n^2l})$（其中，l 为元素的字长）。

证明　本文方案基于随机映射矩阵 $\boldsymbol{R}$ 生成模板 $\boldsymbol{T}$，若攻击者只获得 $\boldsymbol{T}$，则只能穷举法推测出原始生物特征 $\boldsymbol{x}$ 或随机映射矩阵 $\boldsymbol{R}$，计算复杂度均为 $O(2^{n^2l})$。在多项式时间内很难得到 $\boldsymbol{x}$ 或 $\boldsymbol{R}$，故难以泄露原始生物特征信息而具备不可逆性。

2) 已知密文和密钥攻击（已知模板和随机映射矩阵的攻击）。本文方案对随机映射矩阵 $\boldsymbol{R}$ 的保护来自基于 ElGamal 算法的重加密机制，在存储和传输过程中 $\boldsymbol{R}$ 均以密文形式传递，只有认证过程中用户终端可以在 TrustZone 内解密获得。而在应用端需要解密获取子矩阵 $\boldsymbol{R}_2$，在认证时用于提取匹配特征，故 $\boldsymbol{R}_2$ 具有被攻击的可能。由于在本文的改进算法中，生物特征模板是采用子随机映射矩阵交叉融合后产生，因此，即使 $\boldsymbol{R}_2$ 和生物特征 $\boldsymbol{T}$ 泄露，攻击者只能获得 $\boldsymbol{y}=\sqrt{\dfrac{n}{m}}\boldsymbol{R}_1^{\mathrm{T}}\boldsymbol{x}$ 匹配信息，而由矩阵 $\boldsymbol{R}_2$ 推测出 $\boldsymbol{R}_1$ 的计算复杂度为 $O(2^{m^2l})$（具体如定理 2 所示），故难以恢复出原始生物特征 $\boldsymbol{x}$。

定理 3　已知随机映射矩阵 $\boldsymbol{R}$ 的 2 个子矩阵 $\boldsymbol{R}_1=[\boldsymbol{r}_1,\boldsymbol{r}_2,\cdots,\boldsymbol{r}_m]$，$\boldsymbol{R}_2=[\boldsymbol{r}_{m+1},\boldsymbol{r}_{m+2},\cdots,\boldsymbol{r}_n]$，则由 $\boldsymbol{R}_1$ 测出 $\boldsymbol{R}_2$ 的计算复杂度为 $O(2^{(n-m)^2l})$；由 $\boldsymbol{R}_2$ 推测出 $\boldsymbol{R}_1$ 的计算复杂度为 $O(2^{m^2l})$。

证明　若已知 $\boldsymbol{R}_1$，由 $\boldsymbol{R}_1$、$\boldsymbol{R}_2$ 的正交性，得

$$\begin{cases}\boldsymbol{r}_i^{\mathrm{T}}\boldsymbol{r}_j=0 & i\neq j,m+1\leqslant i,j\leqslant n\\ \boldsymbol{r}_i^{\mathrm{T}}\boldsymbol{r}_j=0 & 1\leqslant i\leqslant m,m+1\leqslant j\leqslant n\end{cases}\tag{8}$$

式 (8) 由 $\dfrac{(n-m-1)(n-m)}{2}$ 个二次方程、$m(n-m)$ 个线性方程和 $n(n-m)$ 个未知数组成。其中，利用高斯消元法，$m(n-m)$ 个线性方程组能消除 $m(n-m)$ 个未知数，其计算复杂度为 $O(m^3(n-m)^3)$。二次方程部分为欠定多元方程组，有 $\dfrac{(n-m-1)(n-m)}{2}$ 个方程和 $(n-m)^2$ 个未知数，是一个 MQ 问题[27]，其计算复杂度为 $d_1=d_{\mathrm{MQ}}+N_{\mathrm{MQ}}d_0=2^{(n-m)^2l-k_m}+2^{\frac{(n-m)(n-m-1)l}{2}+k_0}$（其中，$d_{\mathrm{MQ}}$ 为求解 MQ 问题的复杂度；N_{MQ} 为矩阵 $\boldsymbol{R}_2$ 可能的候选解个数；$d_0=2^{k_0}$ 为检验解是否为正确唯一解的计算复杂度；k_m 为不同方法实现穷举搜索效率提高的因子，当 n 和 l 足够大时可被忽略[27]），故总计算复杂度为

$$d=2^{3\mathrm{lb}^{m(n-m)}+(n-m)^2l}+2^{\frac{(n-m)(n-m-1)l}{2}+k_0}\sim O(2^{(n-m)^2l})$$

同理可得，若已知 $\boldsymbol{R}_2$，推测出 $\boldsymbol{R}_1$ 的计算复杂度为 $O(2^{m^2l})$。

因此，在本文方案中，攻击者利用 $\boldsymbol{R}_2$ 测出 $\boldsymbol{R}_1$ 的计算复杂度为 $O(2^{m^2l})$，以 $l=12$，$m=16$ 为例，则计算复杂度约为 $2^{2\,648}+2^{1\,056+k_0}$，可以满足大部分应用的安全性，从而难以恢复出原始生物特征 $\boldsymbol{x}$。

3) 相似性攻击。已知不同用户的多个映射的攻击。

定理 4　假设攻击者在同一个应用端 A_i 获取了多个用户 $U_1,U_2,\cdots,U_k$ 的生物特征模板，表示为 $\boldsymbol{T}_{1,i},\boldsymbol{T}_{2,i},\cdots,\boldsymbol{T}_{k,i}$，则推测出用户的原始生物特征 $\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_k$ 的计算复杂度均为 $O(2^{n^2l})$。

证明　在本文方案中，映射矩阵 $\boldsymbol{R}$ 是用户特定的，即在应用端 A_i 的多个用户 $U_1,U_2,\cdots,U_k$ 对应的 $\boldsymbol{R}$ 可表示为 $\boldsymbol{R}_{1,i},\boldsymbol{R}_{2,i},\cdots,\boldsymbol{R}_{k,i}$，并非在同一个应用端共享相同的 $\boldsymbol{R}$。因此，已知 $\boldsymbol{T}_{1,i},\boldsymbol{T}_{2,i},\cdots,\boldsymbol{T}_{k,i}$ 通过相似性攻击推测原始生物特征或映射矩阵的计算复杂度同定理 2 所述，均为 $O(2^{n^2l})$。

4) 交叉匹配攻击。已知同一个用户的多个映射的攻击。

定理 5　假设攻击者在多个应用终端 $A_1,A_2,\cdots,A_k$ 获取到基于同一个用户 U_j 的多个映射特征模板 $\boldsymbol{T}_{j,1},\boldsymbol{T}_{j,2},\cdots,\boldsymbol{T}_{j,k}$，则推测出原始生物特征 $\boldsymbol{x}_j$ 的计算复杂度最小为 $O(2^{m^2l})$。

证明　若攻击者只获取到 U_j 的多个特征模板 $\boldsymbol{T}_{j,1},\boldsymbol{T}_{j,2},\cdots,\boldsymbol{T}_{j,k}$，则推测出原始生物特征 $\boldsymbol{x}_j$ 的计算复杂度如定理 2 所示，为 $O(2^{n^2l})$。若攻击者同时获得了 k 个映射特征对应的映射子矩阵 $\boldsymbol{R}_2^1,\boldsymbol{R}_2^2,\cdots,\boldsymbol{R}_2^k$，则可得 $\boldsymbol{y}_i=\sqrt{\dfrac{n}{m}}\boldsymbol{R}_1^{i\,\mathrm{T}}\boldsymbol{x}_j,(i=1,2,\cdots,k)$。由于推出 $\boldsymbol{R}_1^1,\boldsymbol{R}_1^2,\cdots,\boldsymbol{R}_1^k$ 的计算复杂度如定理 3 所述均为 $O(2^{m^2l})$，故难以推测出 $\boldsymbol{x}_j$。

5) 统计攻击。已知认证过程的多次映射的攻击。

定理 6 假设攻击者在认证过程中从传输通道窃取多次映射特征 $\boldsymbol{y}_{e,1}', \boldsymbol{y}_{e,2}', \cdots, \boldsymbol{y}_{e,k}'$（如图 2 所示），由于本文方案基于同一用户生成的映射特征具有变化性，故攻击者无法实现对用户的认证频率、用户数量等的统计分析攻击。

证明 在本文方案中，映射特征的生成方式为 $\boldsymbol{y}_e' = \boldsymbol{R}_2\boldsymbol{y}_1' + \boldsymbol{R}_1\boldsymbol{y}_{2e}'$，其中，$\boldsymbol{y}_{2e}' = \boldsymbol{y}_2' + \boldsymbol{N}_s$（$\boldsymbol{N}_s'$ 为随机生成的噪声）。因此，基于同一认证用户，攻击者截获的多次映射特征可表示为

$$\begin{cases} \boldsymbol{y}_{e,1}' = \boldsymbol{R}_2\boldsymbol{y}_1' + \boldsymbol{R}_1\boldsymbol{y}_2' + \boldsymbol{R}_1\boldsymbol{N}_{s,1}' \\ \boldsymbol{y}_{e,2}' = \boldsymbol{R}_2\boldsymbol{y}_1' + \boldsymbol{R}_1\boldsymbol{y}_2' + \boldsymbol{R}_1\boldsymbol{N}_{s,2}' \\ \vdots \\ \boldsymbol{y}_{e,p}' = \boldsymbol{R}_2\boldsymbol{y}_1' + \boldsymbol{R}_1\boldsymbol{y}_2' + \boldsymbol{R}_1\boldsymbol{N}_{s,p}' \end{cases}$$

令 $\boldsymbol{Q} = \boldsymbol{R}_1\boldsymbol{N}_{s,1}', r_{i,j} \in \boldsymbol{R}_1, n_{i,j} \in \boldsymbol{N}_{s,1}', i,j = 1,2,\cdots,n$，则 $q_{i,j} \in \boldsymbol{Q}$，$q_{i,j} = r_{i,1}n_{1,j} + r_{i,2}n_{2,j} + \cdots + r_{i,m}n_{m,j}$。针对随机噪声 $\boldsymbol{N}_{s,2}'$，可将其元素表示为 $(n_{i,j} + \delta_{i,j})$，则 $\tilde{\boldsymbol{Q}} = \boldsymbol{R}_1\boldsymbol{N}_{s,2}'$ 的元素为

$$\begin{aligned} \tilde{q}_{i,j} &= r_{i,1}(n_{1,j} + \delta_{1,j}) + r_{i,2}(n_{2,i} + \delta_{2,i}) + \cdots + r_{i,m}(n_{m,j} + \delta_{m,j}) \\ &= q_{i,j} + (r_{i,1}\delta_{1,j} + r_{i,2}\delta_{2,j} + \cdots + r_{i,m}\delta_{m,j}) \end{aligned}$$

由此可见，噪声矩阵 $\boldsymbol{N}_s'$ 元素的变化经过随机映射变换后，可扩散分布到变换矩阵的每个元素中。以此类推，基于同一用户，每次认证生成的映射特征均具有动态变化性，使攻击者无法基于特征的相似性分析用户认证频率、认证用户数量等信息，从而抵抗统计攻击。

6) 重放攻击。已知认证过程的某次映射的攻击。假设攻击者从传输通道窃取用户的某次映射特征，试图利用该特征来欺骗应用系统，进行非法认证。而本文方案在认证过程中使应用端生成随机数 θ（用于合法性验证，具有时效性）并传至用户端融合在变换特征中，在特征匹配时只能通过 $\boldsymbol{R}_2$ 进行提取和去除，从而实现用户的安全验证和匹配。若攻击者利用截获的某次变换特征，试图进行身份认证，然而在匹配过程中提取的 θ 值发生变化而无法去除，使匹配失败，从而有效抵抗重放攻击。而对于传统的随机映射算法，若直接添加随机数 θ 与特征相融合，攻击者能通过截获 θ 和融合的变换特征而恢复出原始变换特征，在试图非法认证时，再利用新截获的 θ 进行伪造，即可欺骗系统，因此，无法对抗重放攻击。

将本文方案与其他基于随机映射的模板保护方法进行性能对比，结果如表 1 所示。其中，文献[8,12,13]的安全性能较好，原因在于它们对映射后的矩阵进行了不可逆变换，文献[8]和[13]进行了量化处理，文献[12]使用散列算法对映射特征进行保护，均在损失匹配准确性的情况下提高了算法安全性。而本文方案在随机映射的结果中添加了噪声干扰域，再利用子随机映射矩阵交叉融合后保存为模板，认证过程能恢复提取出与原始随机映射算法一致的特征（$\boldsymbol{y} = \sqrt{\frac{n}{m}}\boldsymbol{R}_1^{\mathrm{T}}\boldsymbol{x}$）进行匹配。结合重加密机制对随机映射矩阵的管理，使本文方案在保持认证准确性的同时对生物特征模板的几类攻击体现了较高的安全性。

5 实验评估

本节测试了所提出的基于重加密的随机映射指纹模板保护方法的性能。首先，测试了算法对指纹认证准确度的影响；然后，验证了算法具备的可撤销性（模板不可链接性）和生成变换特征的动态变化性（抵抗统计攻击能力）；最后，对比分析了本文方案

表 1 基于随机映射的生物特征模板保护方法的对抗攻击能力对比

方案	不可逆性	已知密钥和模板	相似性攻击	交叉匹配攻击	统计攻击	重放攻击
文献[8]方案	√	√	√	√	×	×
文献[9]方案	√	×	√	×	×	×
文献[10]方案	√	×	√	×	×	×
文献[11]方案	√	√	×	×	×	×
文献[12]方案	√	√	√	√	×	×
文献[13]方案	√	√	√	√	×	×
文献[14]方案	√	×	√	×	×	×
本文方案	√	√	√	√	√	√

对生物特征认证的存储开销和计算复杂度的影响。

5.1　实验数据和环境

本文在 FVC2000DB2 公开指纹数据库[28]上进行了实验测试，该数据库包含 100 个手指的 800 张指纹图像（每个手指含 8 个采样图像）。指纹特征提取方法采用 Jain 等[29]提出的 Fingercode 特征，一种基于 Gabor 滤波的指纹纹理特征描述方法。由于其保留了丰富的脊线信息，在一定程度上能克服基于细节点的特征算法在质量较差的区域难以提取的缺点；同时，Fingercode 指纹特征是基于图像纹理的定长特征，分布均匀可以实现随机映射,而对匹配准确率的影响较小。因此，对原始指纹图像以奇异点为中心剪裁得到 175×175 的图像后提取 Fingercode 特征，生成 576 维特征；转为 24×24 矩阵后作为特征 $\boldsymbol{x}$ 进行随机映射。实验环境是 Intel Xeon 3.0 GHz Windows 7 操作系统，内存 16 GB，编程环境为 Matlab R2016b。

5.2　认证性能

为了验证本文改进算法对认证性能的影响，实验对比了加入随机映射保护策略前后的认证准确率。对于 FVC2000DB2 指纹数据库，将每个指纹样本与其他图像样本进行匹配，测试总数为 319 600 次，其中包含真匹配（genuine match）2 800 次，即匹配来自于同一手指；包含假匹配（imposter match）316 800 次，即匹配来自于不同手指。图 6(a)为真假匹配以归一化欧氏距离为匹配分数的分布。由此可见，本文算法对真假匹配分数分布的影响很小。图 6(b)的 ROC 曲线为基于原始 Fingercode 特征的认证结果和基于本文算法的结果。由于 Fingercode 特征提取受奇异点位置影响，故根据文献[29]，将原始的 FVC2000DB2 数据库中奇异点位于图像边缘或图像质量很差的指纹去除后，得到 630 张指纹图像进行对比检测。由图 6 可知，在 2 种情况下，本文算法均与基于原始 Fingercode 特征的 ROC 曲线逼近。由于改进算法最终的匹配特征与原始随机映射算法一致，均是 $\boldsymbol{y}=\sqrt{\frac{n}{m}}\boldsymbol{R}_1^{\mathrm{T}}\boldsymbol{x}$，因此，具有良好的距离保持特性，对认证性能影响很小。

5.3　不可链接性测试

对模板不可链接性的测试通过 4 组实验验证。1) 使用每个手指的第一个样本提取 Fingercode 特征，产生 100 个生物模板（原始 Fingercode 特征）。2) 使用每个手指的第一个样本利用相同的映射矩阵生成 100 个生物模板（不同手指相同 $\boldsymbol{R}$）。3) 使用每个手指的第一个样本利用不同的映射矩阵构成 100 个生物模板（不同手指不同 $\boldsymbol{R}$）。4) 基于同一个手指的 5 个样本，针对每个样本利用随机产生的映射矩阵生成 20 个模板，共构成 100 个生物模板（相同手指不同 $\boldsymbol{R}$）。将第一个模板与其他模板进行 99 次匹配，得到欧式距离分布如图 7 所示。

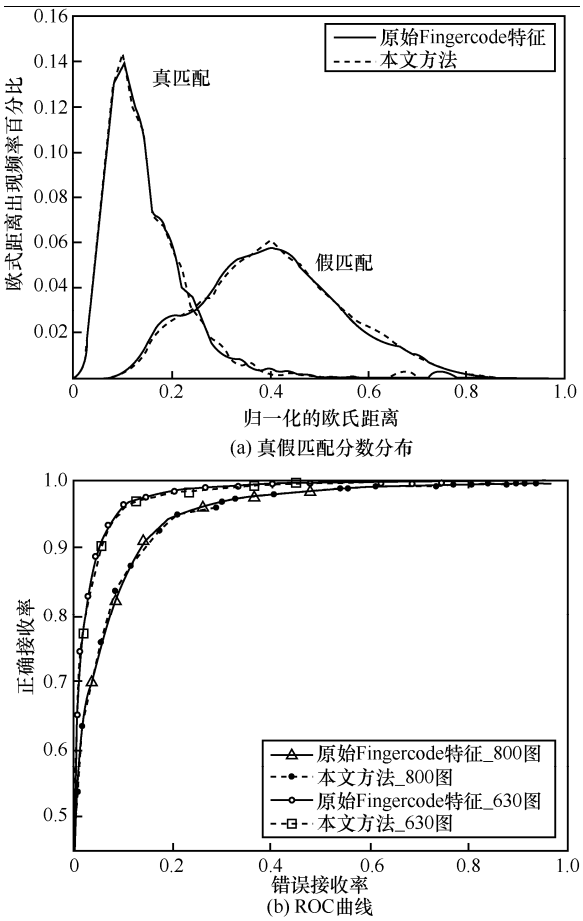


图 6　匹配准确率

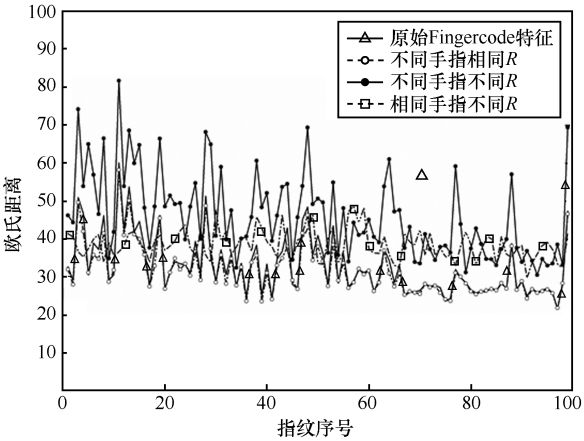


图 7　不可链接性测试结果

由图可见，基于相同手指不同 $\boldsymbol{R}$ 产生的生物模板匹配差异性与基于不同指纹产生的匹配数值相近，说明基于相同指纹，变换随机映射矩阵即类似于变换手指，表现了良好的可撤销性。而不同手指相同 $\boldsymbol{R}$ 的曲线与原始 Fingercode 特征曲线几乎重合，说明了基于相同随机映射矩阵的变换对于原始生物特征之间的差异具有良好的保持特性。其次，算法对于注册时的映射矩阵采用随机生成方式，即针对不同用户 $\boldsymbol{R}$ 不同，由此可见，不同手指不同 $\boldsymbol{R}$ 对应的曲线的匹配数值较大，说明了本文算法对于不同指纹之间的匹配具有更好的模板不可链接性。

5.4 变换特征的动态变化性测试

针对攻击者从传输通道窃取多次变换特征，试图进行统计分析的攻击，本文通过改进随机映射算法，在干扰噪声的影响下，使每次认证产生的变换特征具有动态变化性。实验分别基于 Fingercode 特征、传统随机映射算法和本文方案（在变换域添加随机均匀分布的噪声）对变换特征的动态变化性进行对比测试，对每个手指的 2 个样本生成生物特征模板，并利用欧氏距离测试模板间的差异性，针对 100 个手指得到的对比结果如图 8 所示。可见，本文方案生成的不同变换特征之间受随机干扰噪声的影响，差异性较大，因此，攻击者无法通过获取的变换特征实现统计攻击。

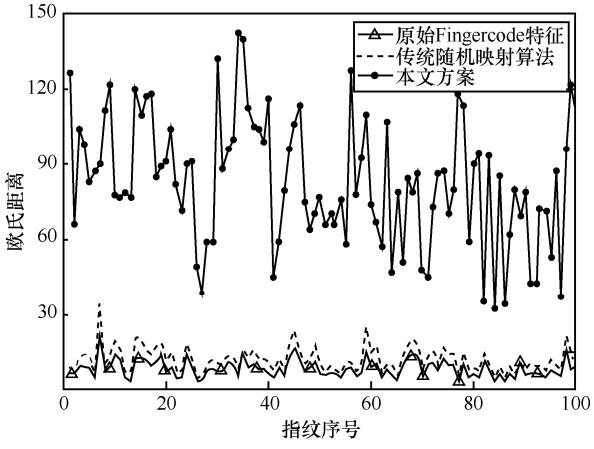


图 8 认证过程指纹变换特征差异性对比结果

5.5 复杂度分析

重加密机制的引入在提高生物特征身份认证安全性的同时，对身份认证过程的存储和计算开销也有一定的影响。将原始基于随机映射算法（无重加密机制）的方案，以及对随机映射矩阵 $\boldsymbol{R}$ 进行重加密，与本文对随机映射矩阵加密密钥 k 进行重加密的机制在存储开销上进行对比，得到结果如表 2 所示。对于用户而言，无重加密机制需要用户保存生成随机映射矩阵的随机序列 PRN，所需存储空间为 σ（随机序列的比特长度）；引入重加密机制后，用户不需要额外存储随机映射密钥，同时用户终端只需保存一对公私钥 (pk,sk)，所需存储空间为 $|\mathbb{G}_1|+|\mathbb{Z}_p^*|$（$|\mathbb{G}_1|,|\mathbb{Z}_p^*|$ 分别为 ElGamal 算法中群 $\mathbb{G}_1$，$\mathbb{Z}_p^*$ 中元素的比特长度）。重加密机制方案将密钥和额外的存储需求转移至应用端，应用端需要保存随机映射矩阵密文（$|\mathbb{G}_2|$ 表示群 $\mathbb{G}_2$ 元素的比特长度）、生物特征模板、注册用户终端标号，以及各注册用户终端之间的重加密密钥矩阵 $\boldsymbol{rekey}$；而无重加密机制在应用端只需保存生物特征模板，需要存储空间为 $m\times n\times l$。此外，本文对随机映射矩阵加密密钥 k 重加密，而非直接对高维的 $\boldsymbol{R}$ 进行重加密，以降低计算时间和重加密密文的存储开销。通过引入重加密机制，将用户的存储开销在保证安全性的前提下转移至应用端，而对于应用端增加的存储任务可以交给具有强大计算和存储能力的云服务提供商完成[30]。

此外，引入重加密机制将对生物特征身份认证的注册和认证过程产生额外的计算量，本文方案与无重加密机制的方案在计算开销上的对比如表 3 所示。无重加密机制对于用户终端的运算主要涉及生物特征的提取和变换，定义此过程所需时间为 t_T；对于应用端则涉及认证过程的模板匹配，定义所需时间为 t_M。本文方案注册过程在用户终端所需时间为 $t_T'+t_{e\_\boldsymbol{R}}+t_{e1\_\boldsymbol{R}}+t_{e\_\boldsymbol{R}_2}$（$t_T'$ 为生物特征提取和变换时间，$t_{e\_\boldsymbol{R}}$ 为加密随机映射矩阵 $\boldsymbol{R}$ 的时间，$t_{e1\_\boldsymbol{R}}$ 为一次加密密钥 k 的时间，$t_{e\_\boldsymbol{R}_2}$ 为加密 $\boldsymbol{R}_2$ 的时间）；注册过程应用端需要解密 $\boldsymbol{R}_2$，定义此时间为 $t_{d\_\boldsymbol{R}_2}$。认证过程用户终端所需时间为 $t_{d\_k}+t_{d\_\boldsymbol{R}}+t_T'$（$t_{d\_k}$ 为一次解密密钥 k 的时间，$t_{d\_\boldsymbol{R}}$ 为解密随机映射矩阵 $\boldsymbol{R}$ 的时间）；认证过程应用端所需时间为 $t_{e2\_k}+t_M'$（t_{e2_k} 为 2 次加密 k 的时间，t_M' 为模板匹配的时间）。实验运行 100 次取均值作为结果，如表 3 所示，重加密方案的引入因为在用户终端增加了加密、解密操作，使注册和认证时间比无重加密机制增加一倍左右；对于应用端增加了重加密操作，时间也明显增大，但均在可以接受范围内。

表 2　　**基于随机映射的生物特征模板保护方法存储开销对比**

方案	用户		用户终端		应用端	
	存储内容	存储空间	存储内容	存储空间	存储内容	存储空间
无重加密机制	PRN	σ	—	—	$\boldsymbol{T}$	$m{\cdot}n{\cdot}l$
对 $\boldsymbol{R}$ 重加密	—	—	pk, sk	$\lvert\mathbb{G}_1\rvert+\lvert\mathbb{Z}_p^*\rvert$	$\boldsymbol{R}_e\lVert\boldsymbol{T}\rVert\boldsymbol{R}_2\lVert i$, $rekey$	$(1.5n^2+1)l+(n^2+\mathrm{P}^2)\lvert\mathbb{G}_1\rvert+n^2\lvert\mathbb{G}_2\rvert$
本文方案	—	—	pk, sk	$\lvert\mathbb{G}_1\rvert+\lvert\mathbb{Z}_p^*\rvert$	$k_e\lVert\boldsymbol{R}_e\lVert\boldsymbol{T}\rVert\boldsymbol{R}_2\lVert i$, $rekey$	$(2.5n^2+1)l+(1+\mathrm{P}^2)\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert$

表 3　　**本文方案与无重加密机制的计算开销对比**

方案及其计算开销	注册过程用户终端	注册过程应用端	认证过程用户终端	认证过程应用端
无重加密机制	t_T	—	t_T	t_M
计算开销/s	0.171 80	—	0.171 80	0.000 02
本文方案	$t_T'+t_{e\_\boldsymbol{R}}+t_{e1\_k}+t_{e\_\boldsymbol{R}_2}$	$t_{d\_\boldsymbol{R}_2}$	$t_{d\_k}+t_{d\_\boldsymbol{R}}+t_T'$	$t_{e2\_k}+t_M'$
计算开销/s	0.466 70	0.107 10	0.319 90	0.054 10

6　结束语

针对基于随机映射的生物特征模板保护方法存在的模板安全和密钥管理问题，本文在随机映射后的变换特征中添加噪声干扰域，通过子随机映射矩阵的交叉融合生成模板；对随机映射矩阵的管理则引入重加密机制实现密钥的安全传输和存储。实验结果表明本文方案对指纹认证的准确率和计算时间影响较小，生成的模板具有良好的不可链接性；同时，在认证过程中能有效抵抗重放攻击、相似性攻击、交叉匹配攻击等，具备较高的安全性。在应用中，本文方案的认证安全性不依赖于应用端的可信度或第三方认证；同时，对用户与用户终端绑定、用户与用户终端不绑定的场景均适用，在提高认证隐私保护强度的同时具备良好的适用性。

未来的工作可以基于本文算法研究适用于其他类型的生物特征（如人脸、虹膜等）的安全认证方案。此外，由于基于生物特征进行身份认证需要预先得知用户身份，再使用该用户的模板进行认证，具有一定的应用局限性。因此，设计基于随机映射的生物特征身份识别算法，即在识别过程中传递非用户特定的参数进行身份鉴定，也是未来值得研究的内容。

参考文献：

[1] CAVOUKIAN A, STOIANOV A. Biometric encryption[M]. Boston, USA: Springer US, 2011: 90-98.

[2] NAGAR A. Biometric template security[M]. Switzerland: Springer International Publishing, 2012.

[3] SANDHYA M, PRASAD M V N K. Biometric template protection: a systematic literature review of approaches and modalities[M]//Biometric Security and Privacy. Springer International Publishing, 2017: 323-370.

[4] SANDHYA M, PRASAD M V N K, CHILLARIGE R R. Generating cancellable fingerprint templates based on Delaunay triangle feature set construction[J]. IET Biometrics, 2016, 5(2): 131-139.

[5] CAVOUKIAN A, SNIJDER M, STOIANOV A, et al. Privacy and biometrics for authentication purposes: a discussion of untraceable biometrics and biometric encryption[M]//Ethics and Policy of Biometrics. Springer Berlin Heidelberg, 2010: 14-22.

[6] BOULGOURIS N V, PLATANIOTIS K N, MICHELI-TZANAKOU E. Biometric encryption: the new breed of untraceable biometrics[M]. Biometrics: Theory, Methods, and Applications. John Wiley & Sons, Inc. 2009:655-718.

[7] ACHLIOPTAS D. Database-friendly random projections[C]//The 12th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Data Base Systems. 2001: 274-281.

[8] NGO D C L, TEOH A B J, GOH A. Biometric hash: high-confidence face recognition[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2006, 16(6): 771-775.

[9] JIN Z, GOI B M, TEOH A, et al. A two-dimensional random projected minutiae vicinity decomposition-based cancellable fingerprint template[J]. Security and Communication Networks, 2014, 7(11): 1691-1701.

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

[11] WANG Y, PLATANIOTIS K N. An analysis of random projection for changeable and privacy-preserving biometric verification[J]. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 2010, 40(5): 1280-1293.

[12] KHAN S H, AKBAR M A, SHAHZAD F, et al. Secure biometric template generation for multi-factor authentication [J]. Pattern Recognition, 2015, 48(2): 458-472.

[13] YANG B, HARTUNG D, SIMOENS K, et al. Dynamic random projection for biometric template protection[C]// 2010 Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS). IEEE, 2010: 1-7.

[14] ANZAKU E T, SOHN H, RO Y M. Multi-factor authentication using fingerprints and user-specific random projection[C]//2010 12th International Asia-Pacific Web Conference (APWEB). 2010: 415-418.

[15] PATEL V M, RATHA N K, CHELLAPPA R. Cancelable biometrics: a review[J]. IEEE Signal Processing Magazine, 2015, 32(5): 54-65.

[16] 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[J]. 密码学报, 2015, 2(2): 159-176.
ZHANG N, ZANG Y L, TIAN J. The integration of biometrics and cryptography-a new solution for secure identity authentication[J]. Journal of Cryptologic Research, 2015, 2(2): 159-176.

[17] DASGUPTA S, GUPTA A. An elementary proof of the Johnson-Lindenstrauss lemma[J]. International Computer Science Institute, Technical Report, 1999, 22(1): 1-5.

[18] FRANKL P, MAEHARA H. The Johnson-Lindenstrauss lemma and the sphericity of some graphs[J]. Journal of Combinatorial Theory, Series B, 1988, 44(3): 355-362.

[19] JASSIM S, AL-ASSAM H, SELLAHEWA H. Improving performance and security of biometrics using efficient and stable random projection techniques[C]//6th International Symposium on Image and Signal Processing and Analysis. 2009: 556-561.

[20] ARRIAGA R I, VEMPALA S. An algorithmic theory of learning: Robust concepts and random projection[C]//40th Annual Symposium on Foundations of Computer Science. 1999: 616-623.

[21] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[J]. Advances in Cryptology-EUROCRYPT'98, 1998: 127-144.

[22] AHMED M, HOSSAIN M A. Cloud computing and security issues in the cloud[J]. International Journal of Network Security & Its Applications, 2014, 6(1): 25.

[23] LIU S, HU S, WENG J, et al. A novel asymmetric three-party based authentication scheme in wearable devices environment[J]. Journal of Network and Computer Applications, 2016, 60: 144-154.

[24] PIRKER M, SLAMANIG D. A framework for privacy-preserving mobile payment on security enhanced arm TrustZone platforms[C]// 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2012: 1155-1160.

[25] 周阿转, 俞一彪. 采用特征空间随机映射的鲁棒性语音识别[J]. 计算机应用, 2012, 32(07): 2070-2073.
ZHOU A Z, YU Y B. Robust speech recognition by adopting random projection in feature space[J]. Journal of Computer Applications, 2012, 32(07): 2070-2073.

[26] ATENIESE G, FU K, GREEN M, et al. Improved proxy re-encryption schemes with applications to secure distributed storage[J]. ACM Transactions on Information and System Security (TISSEC), 2006, 9(1): 1-30.

[27] XU Z, XIONG L, XU Y. On the provably secure CEW based on orthogonal decomposition[J]. Signal Processing: Image Communication, 2014, 29(5): 607-617.

[28] MAIO D, MALTONI D, CAPPELLI R, et al. FVC2000: fingerprint verification competition[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002, 24(3): 402-412.

[29] JAIN A K, PRABHAKAR S, HONG L, et al. Filterbank-based fingerprint matching[J]. IEEE transactions on Image Processing, 2000, 9(5): 846-859.

[30] 张玉清, 王晓菲, 刘雪峰,等. 云计算环境安全综述[J]. 软件学报, 2016, 27(6):1328-1348.
ZHANG Y Q, WANG X F, LIU X F, et al. Survey on cloud computing security[J]. Journal of Software, 2016, 27(6):1328-1348.

[作者简介]

贾姗（1993-），女，山东莱芜人，武汉大学博士生，主要研究方向为信息安全、生物特征识别。

徐正全（1962-），男，湖北黄冈人，博士，武汉大学教授，主要研究方向为信息安全、隐私保护、图像处理等。

胡传博（1989-），男，黑龙江哈尔滨人，武汉大学博士生，主要研究方向为计算机视觉、空间信息处理。

王豪（1990-），男，河南驻马店人，武汉大学博士生，主要研究方向为数据挖掘、隐私保护。