高效的隐私保护在线人脸认证方案

李明[1]，杨晓鹏[2]，朱辉[2]，王枫为[2]，李祁[2]

（1. 国家知识产权局专利局，北京 100088；
2. 西安电子科技大学综合业务网理论及关键技术国家重点实验室，陕西 西安 710071）

摘 要：在传统人脸认证系统中，用户特征模板和认证请求通常基于明文进行匹配，存在敏感数据泄露的风险。针对此问题，提出了一种基于矩阵加密的隐私保护的在线人脸认证方案。该方案中，用户的人脸特征模板注册和后续身份认证请求均通过矩阵加密后分别发送给在线认证服务器，并由在线认证服务器完成密文下两者间的相似度计算，能够在不影响认证精确度的同时，有效保护在线人脸认证过程中用户的敏感数据。安全性分析表明，通过选取不同安全参数，所提方案能够实现多安全等级，满足差异化场景中的隐私保护需求。性能分析显示，所提方案具有较低的计算开销与通信开销。仿真测试基于真实人脸数据库，其结果验证了所提方案的高效性，能够在真实环境中进行有效应用。

关键词：在线人脸认证；隐私保护；矩阵加密；生物特征模板

中图分类号：TP302

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2020087

Efficient and privacy-preserving online face authentication scheme

LI Ming[1], YANG Xiaopeng[2], ZHU Hui[2], WANG Fengwei[2], LI Qi[2]

1. Patent Office, China National Intellectual Property Administration, Beijing 100088, China
2. State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China

Abstract: In traditional face authentication system, the trait template and authentication request were generally matched over plaintext, which may lead to the leakage of users' sensitive data. In order to address the above-mentioned problem, based on matrix encryption, an efficient and privacy-preserving online face authentication scheme was proposed. Specifically, the users' face trait template for register and the authentication request were encrypted before being sent to the online authentication server, and the similarity computation between the encrypted face trait template and authentication request was computed by the online authentication server over ciphertexts, which guaranteed the security of users' sensitive data without affecting the accuracy of face authentication. Security analysis shows that the proposed scheme can achieve multiple security levels according to different security parameters. Moreover, performance evaluation shows that the proposed scheme has low computation cost and communication overhead. Experiments results demonstrate the high efficiency of the proposed scheme, which can be implemented in the real environment effectively.

Key words: online face authentication, privacy-preserving, matrix encryption, biometric template

收稿日期：2020–03–08；**修回日期**：2020–03–31

通信作者：杨晓鹏，xpyang@stu.xidian.edu.cn

基金项目：国家重点研发计划基金资助项目（No.2017YFB0802200）；国家自然科学基金资助项目（No.61972304, No.61932015）；陕西省重点研发计划基金资助项目（No.2019ZDLGY12-02）；陕西省创新团队基金资助项目（No.2018TD-007）

Foundation Items: The National Key Research and Development Program of China (No.2017YFB0802200), The National Natural Science Foundation of China (No.61972304, No.61932015), The Shannxi Provincial Key Research and Development Program (No.2019ZDLGY12-02),The Innovation Team Project of Shannxi Province (No.2018TD-007)

1 引言

随着计算机技术的不断发展和智能终端的快速普及，基于人脸、指纹、声纹等各种生物特征的身份认证方案被广泛应用到各个领域，给人们的生活带来了诸多便利。生物特征具有以下特性：1) 唯一性，即每个用户所具有的生物特征信息都是独一无二的；2) 稳定性，即用户的生物特征很难在短期内自然地发生改变；3) 随身性，即用户的生物特征存在于用户本身，不会被丢失或遗忘。生物特征所具有的这些特征决定了基于生物特征的身份认证方法相较于传统的身份认证方法（如口令密码、智能卡等）具有更高的认证效率和安全性，以及更好的用户体验。相较于其他生物特征认证技术，人脸认证因其采取非接触式的数据采集方式和较低的部署成本，受到用户和服务商的青睐，并被广泛应用到机场铁路安检 [1]、金融支付[2]、刑事侦查[3]等各个领域。

但是，基于生物特征认证技术的广泛应用也使用户生物特征隐私的泄露风险大大提升。近年来，全球范围内的生物特征隐私泄露事件频发，这加重了用户对于在使用基于生物特征的身份认证服务过程中造成个人生物特征信息泄露的担忧。2017 年，印度国家身份系统 Aadhaar 发生大规模数据库泄露事件，超过 10 亿用户的个人生物特征信息被泄露，被泄露的数据中包含用户的指纹、虹膜等高敏感数据[4]。2019 年，我国某人脸识别公司遭遇了拖库攻击，包括人脸图像及其采集地点等信息的 680 万条记录被泄露。国外基于 Web 的生物认证安全智能锁定平台 BioStar2 于 2019 年 8 月被曝出存在系统漏洞，所泄露的数据量高达 23 GB，其中包含 100 多万条含用户指纹、人脸生物特征在内的敏感数据[5]。虽然部分基于生物特征的身份认证系统中，用户的生物特征信息并非以原始生物特征数据的形式存储，但是近年来的研究表明[6]，经过处理后的生物特征数据依然会给用户生物特征的隐私带来威胁。生物特征数据的特点决定了其一旦遭遇泄露，将会带来严重后果。1) 生物特征具有唯一性的特点意味着用户的生物特征信息与用户的身份强关联，攻击者在获取到泄露的生物特征数据之后，可以通过大数据关联分析等方式窥探到更多的用户隐私信息。2) 生物特征所具有的稳定性的特点意味着一旦用户的生物特征信息被泄露，那么用户将面临被攻击者通过该生物特征冒充身份的潜在危险，从而不得不放弃继续使用该生物特征作为身份认证的凭据。随着社会大众对于信息安全和隐私保护关注度的不断提高[7-10]，设计一种安全高效的生物特征认证方案显得至关重要。

为解决上述问题，本文基于矩阵加密技术构造了密文条件下的人脸特征相似度匹配算法，并在此算法的基础上设计了一种隐私保护的在线人脸认证方案。该方案能够保证用户的生物特征信息在身份认证服务中不被泄露，并且能够保证生物特征认证方案的准确率和效率。同时，本文基于所提出的隐私保护的人脸认证方案设计了实验仿真程序，并利用真实的人脸数据库对所提方案的效率进行了测试。

2 相关工作

生物特征数据的隐私保护一直是学术界的研究热点，针对这一热点，人们基于不同的技术提出了诸多解决方案。

部分方案基于同态加密方案设计，Erkin 等[11]基于 Paillier 同态加密算法和 DGK（Damgard, Geisler and Krøigaard）加密方案[12]设计了一种面向外包场景的同态加密方案，该方案能保证用户在注册和认证过程中生物特征数据及身份认证结果的安全。Sadeghi 等[13]基于混淆电路、不经意传输等技术对 Erkin 等[11]所提方案进行了改进，改进后的方案在通信和计算开销方面有了更好的表现。Xiang 等[14]基于全同态加密方案提出了一种外包场景下的隐私保护在线人脸认证方案。Zhu 等[15]基于半同态加密算法提出了一种面向隐私保护的欧氏距离计算方案，避免了同态加密算法中计算消耗较大的解密过程，虽然在效率上有很大提升，但依然有较大的提升空间。同态加密方案往往需要较高的计算开销，在一些实时性要求较高或者资源受限的场景中并不适用。

基于随机化技术设计的生物特征隐私保护方案在近几年也逐渐被提出。Yuan 等[16]基于随机矩阵技术实现了密文下的欧氏距离计算，提出了一种云计算场景下的用户指纹数据隐私保护方案。Wang 等[17]对文献[16]所提的生物特征隐私保护方案进行了优化，并基于矩阵迹理论提出了一种隐私保护的在线指纹认证方案。Zhu 等[18]也对文

献[16]提出的方案进行了改进，改进后的方案在效率和安全性上都有所提升。Rahulamathavan 等[19]基于随机掩码技术提出了一种基于 Eigenface 人脸识别算法和欧氏距离相似度判断的隐私保护人脸认证方案。

在其他技术方面，Gunasinghe 等[20]基于零知识证明设计了一种可证明安全的隐私保护生物特征认证方案，但是该方案需要在客户端通过机器学习的方式提取用户的生物特征，这增加了客户端的计算负担。Sarier 等[21]基于区块链技术，设计了一种隐私保护的生物特征认证方案，但是区块链技术的引入带来了较大的计算开销。

综上所述，现有方案基于不同的技术实现了生物特征认证的隐私保护，但是在计算、通信效率和适用性方面还存在局限性。

3　Eigenface 人脸识别算法

Eigenface 人脸识别算法[22]是一种基于主成分分析（PCA, principal component analysis）而设计的人脸识别方案。Eigenface 人脸识别算法包括用户注册和人脸识别 2 个阶段，具体如下。

在注册阶段，用户利用 PCA 从自己的若干张面部图像中提取出人脸数据的特征向量，具体的处理过程如下。

步骤 1　用户向身份认证服务器提交 P 张人脸图像，记为 $\{\Gamma_1,\Gamma_2,\cdots,\Gamma_P\}$，其中 $\Gamma_i(i=1,2,\cdots,p)$ 表示人脸图像，每张人脸数据的大小为 h 像素 $\times w$ 像素。身份认证服务器对接收到的 P 张人脸图像进行归一化处理后，将每张人脸图像表示为一个 N（$N=h\times w$）维向量。

步骤 2　身份认证服务器对输入的 P 张人脸数据取平均值 $\Psi=\frac{1}{P}\sum_{i=1}^{P}\Gamma_i$，根据 PCA 计算出人脸图像的特征向量，并选取特征值较大的 k 个特征向量 $\{\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_k\}$，其中每个特征向量均为 N 维向量。

步骤 3　计算用户输入的每张人脸图像 Γ_i 和平均值 Ψ 之间的差值，并将该差值投影到步骤 2 中所求出的特征向量上，投影表示为 $\{\boldsymbol{\Omega}_1,\boldsymbol{\Omega}_2,\cdots,\boldsymbol{\Omega}_P\}$，这些投影将作为该用户的人脸特征模板。同时，计算出各投影之间相似度的最大值 $S_{\max}$，并且将投影值和最大相似度发送到服务器端。

步骤 4　身份认证服务器在接收到用户的身份认证请求后，根据用户注册阶段发送来的相似度的最大值 $S_{\max}$，选择一个判别门限值 θ 作为判别参数。根据文献[23]的结论，本文取 $\theta=1.25S_{\max}$。

在人脸识别阶段，用户需要提供一张自己的人脸图像。首先，身份认证服务器计算该人脸图像与平均脸图像的差值，此后，计算该差值在注册阶段提取出的特征向量上的投影，并将其作为身份认证凭据。身份认证服务器通过用户提交的身份认证凭据和用户人脸模板数据之间的相似度来对用户的身份认证结果进行判断。具体的处理过程如下。

步骤 1　用户向身份认证服务器提交一张大小为 h像素 $\times w$ 像素人脸图像 Γ_{new}。身份认证服务器对接收到人脸图像进行归一化处理，将其读取为一个 N（$N=h\times w$）维向量。

步骤 2　服务器计算用户输入的人脸图像 Γ_{new} 和注册阶段得到的人脸数据平均值 Ψ 之间的差值，并将该差值投影到注册阶段得到的特征向量上，将该投影值记为 $\boldsymbol{\Omega}_{\text{new}}$，该投影一般作为用户的身份认证凭据。

步骤 3　身份认证服务器计算 $\boldsymbol{\Omega}_{\text{new}}$ 和 $\{\boldsymbol{\Omega}_1,\boldsymbol{\Omega}_2,\cdots,\boldsymbol{\Omega}_P\}$ 中每一个投影之间的相似度，该相似度可以通过欧氏距离或者余弦相似度来判别[24]。

步骤 4　身份认证服务器选取出 P 个相似度中的最大值，并将该最大值和身份认证服务器所选取的门限值 θ 进行比较。如果符合系统预设要求，则用户通过身份认证；反之，则未通过身份认证。

4　系统模型和安全需求

4.1　系统模型

本文所提方案的系统模型由用户、认证代理服务器和在线身份认证服务器三部分组成，如图 1 所示。

用户为某项在线服务的使用者，需要通过身份认证系统来对其身份的真实性进行认证。考虑在资源受限的应用场景中（如智能家居场景），终端设备的计算能力较弱，仅能采集用户的生物特征并生成相应的生物特征模板，需要在其他设备（如智能家居场景中的“家庭大脑”）的辅助下才能完成对用户生物特征信息加密等操作。认证代理服务器为用户的生物特征模板提供加密等预处理操作。在线身份认证服务器是由第三方服务商提供的身份认证服务器，负责对用户的身份进行认证。用户和认证代理服务器之

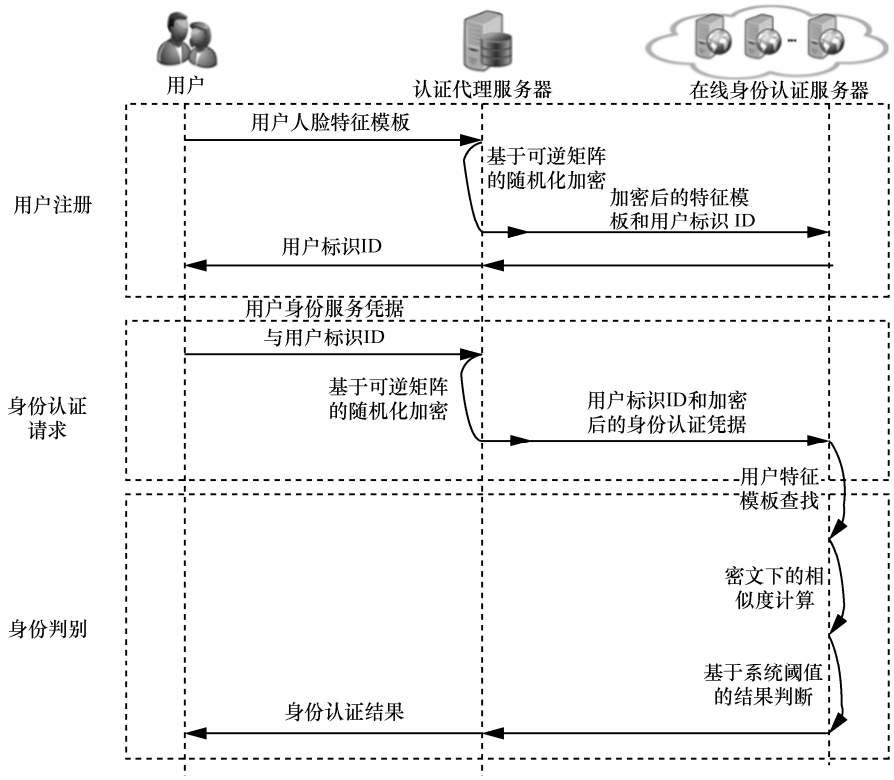


图 1　系统模型

间的网络是内部网络，因此本文认为用户和认证代理服务器之间的网络连接是安全的。

在本文方案的模型中，认证代理服务器和在线身份认证服务器首先对整个系统进行初始化操作。认证代理服务器根据安全性要求选择系统的安全参数，在线身份认证服务器设置判别门限值θ。系统完成初始化后，用户按照提取其人脸特征模板，在在线身份认证服务器上进行注册并得到一个唯一标识 ID。在进行身份认证时，用户首先提取其人脸图像特征数据作为身份认证凭据，并和用户的唯一标识 ID 一起发送到认证代理服务器。代理认证服务器将该身份认证凭据连同用户的唯一标识 ID 发送到在线身份认证服务器，并发起身份认证请求。在线身份认证服务器根据人脸识别算法计算用户人脸特征模板和身份认证凭据之间的相似度，并根据该相似度和系统门限值之间的关系完成对用户身份的认证。

在安全性方面，认证代理服务器是一个完全可信的实体，其忠实地执行既定的算法规则，不会主动去泄露用户的敏感信息，但有可能会受到攻击者的攻击；在线身份认证服务器是一个半可信的实体，以密文的形式存储用户的生物特征信息，其忠实地执行身份认证算法，但是会主动尝试去窥探或者泄露用户的生物特征隐私。此外，攻击者可以对传输的数据进行窃听，并对认证代理服务器和在线身份认证服务器进行攻击，以获得其数据库中的数据。

4.2　安全需求

为了明确安全需求，考虑系统中可能存在具有不同攻击能力的攻击者，本文设定了 3 种攻击模型。

1) 攻击模型Ⅰ

攻击者仅能获取代理认证服务器和在线身份认证服务器在通信过程中被加密后的用户生物特征数据模板和身份凭据数据。这种攻击模型对应本系统中的在线身份认证服务器和网络中可能存在的一些被动攻击者尝试去获得用户敏感信息。

2) 攻击模型Ⅱ

攻击者能够获取部分用户的生物特征模板和身份认证凭据的明文数据和密文数据，但并不知晓这些数据之间的对应关系。这种攻击模型下，认证代理服务器数据库中的部分明文数据被泄露，攻击者根据这些泄露的数据和其窃听到的数据，来尝试获取用户的敏感信息。

3) 攻击模型III

攻击者不仅能获取部分用户的生物特征模板和身份认证凭据的密文数据，知晓这些明密文数据之间的对应关系，还可以获得任意的生物特征模板和身份认证凭据的明文所对应的密文。这种攻击模型对应认证代理服务器的数据库中的部分数据被泄露，同时在线身份认证服务器的数据库也被完全攻破（或者在线身份认证服务器获取到了认证代理服务器所泄露出的明文数据）。攻击者根据这些泄露的部分数据和其获取的用户密文数据，来尝试获取其他未被泄露的敏感信息。

为保证用户生物特征信息的安全，隐私保护的人脸认证方案需保证用户的生物特征信息在这 3 种攻击模型下不会被泄露。

5　基于随机矩阵的生物特征隐私保护

针对在线生物特征认证场景的特点和需求，本节基于随机矩阵技术提出了一种生物特征隐私保护方案。该方案包括用户注册、身份认证请求和身份判别 3 个阶段，具体流程如图 2 所示，方案描述中用到的符号及其含义如表 1 所示。

表 1　　方案中相关符号及其含义

符号	含义
h	用户图像长的像素数
w	用户图像宽的像素数
N	用户图像的像素数
k	选择的特征向量数
$\boldsymbol{M}_i$	可逆随机矩阵
$\boldsymbol{M}_i^{-1}$	可逆随机矩阵的逆矩阵
Z	非负整数
$\boldsymbol{H}$	随机向量
diag()	将向量转换为对角矩阵
$\boldsymbol{A}$	一个随机矩阵
$\{\boldsymbol{C}_{D_1},\boldsymbol{C}_{D_2},\cdots,\boldsymbol{C}_{D_P}\}$	加密后的用户生物特征模板
$\{L_1,L_2,\cdots,L_P\}$	用户生物特征模板的模长
$\boldsymbol{C}_A$	加密后的身份认证凭据
L_{new}	身份认证凭据的模长
UID	用户的身份标识
$r_1, r_2, \cdots, r_Z$	用户选择的一组随机数
score_i	用户人脸特征模板和身份认证凭据模板之间的相似度
θ	系统判别门限值

5.1　用户注册阶段

用户注册阶段包含用户人脸特征模板计算和人脸特征模板加密 2 个阶段。其中，用户将其人脸特征模板发送到认证代理服务器；认证代理服务器利用矩阵加密技术对用户的人脸特征模板进行加密，并将加密后的人脸特征模板发送到在线身份认证服务器处进行身份注册；在线身份认证服务器在收到用户的注册请求后，向用户分配一个唯一标识 ID，并将用户加密后的人脸特征模板保存在其数据库中；用户完成注册后，为

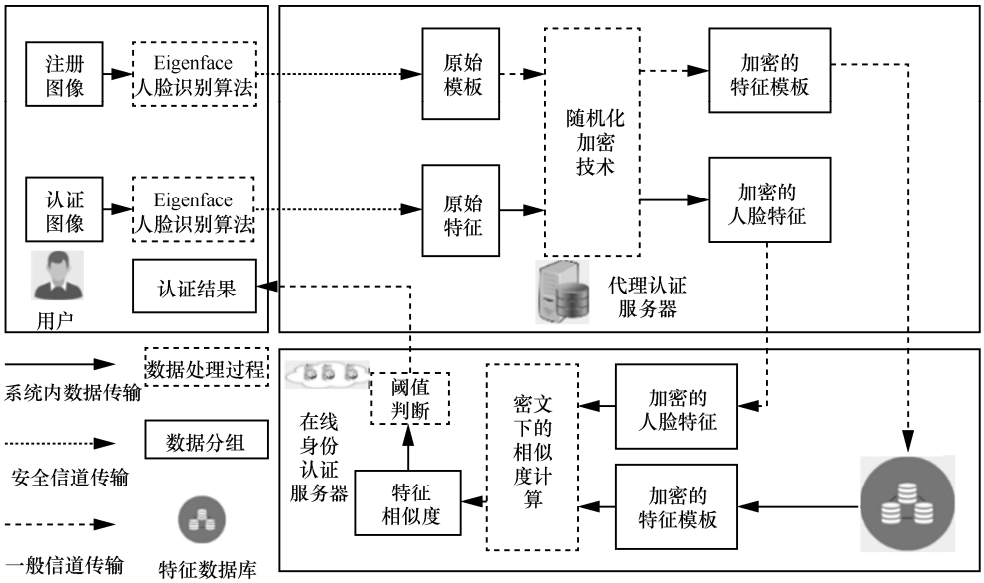


图 2　本文方案的流程

防止遭遇攻击导致用户人脸特征模板明文数据泄露，认证代理服务器将其收到的用户人脸特征模板进行安全存储或删除。

5.1.1 用户特征模板的计算

用户按照 Eigenface 人脸识别算法的要求，在本地进行人脸特征模板的提取。具体来说，用户按照要求拍摄 P 张自己的面部图像，根据 Eigenface 人脸识别算法并选择出这 P 张人脸差值在 k 个特征向量投影 $\{\boldsymbol{\Omega}_1,\boldsymbol{\Omega}_2,\cdots,\boldsymbol{\Omega}_P\}$ 及各个投影之间相似度的最大值 $S_{\max}$，并将 $\{\boldsymbol{\Omega}_1,\boldsymbol{\Omega}_2,\cdots,\boldsymbol{\Omega}_P\}$ 和 $S_{\max}$ 发送到认证代理服务器。

5.1.2 用户人脸特征模板的加密

认证代理服务器在收到用户的注册信息后，首先选择 2 个大小为 $(k+2Z)\times(k+2Z)$ 的可逆随机矩阵 $\boldsymbol{M}_1$ 和 $\boldsymbol{M}_2$，以及一个 $(k+2Z)$ 维的随机向量 $\boldsymbol{H}$（其中，Z 由认证代理服务器设置且 $Z\geqslant 0$）。之后，认证代理服务器将用户的人脸特征模板数据 $\boldsymbol{\Omega}_i$ 扩展成一个（$k+2Z$）维的向量 $\boldsymbol{\Omega}_{i-\text{extended}}$（扩展规则为前 k 维数据和 $\boldsymbol{\Omega}_i$ 保持一致，第（$k+1$）~（$k+2Z$）维数据为 1）并将其进行对角化转换，得到 $\boldsymbol{D}_{i-\text{extended}}=\text{diag}(\boldsymbol{\Omega}_{i-\text{extended}})$。最后，选择一个随机的 $(k+2Z)\times(k+2Z)$ 矩阵 $\boldsymbol{A}$，矩阵 $\boldsymbol{A}$ 需满足 $\boldsymbol{A}_i\boldsymbol{H}^{\mathrm{T}}=1$，$\boldsymbol{A}=[\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_{k+2Z}]$，并通过计算 $\boldsymbol{W}_{\boldsymbol{D}_i}=\boldsymbol{D}_i\boldsymbol{A}$，$\boldsymbol{C}_{\boldsymbol{D}_i}=\boldsymbol{M}_1\boldsymbol{W}_{\boldsymbol{D}_i}\boldsymbol{M}_2$ 和 $L_i=\|\boldsymbol{\Omega}_i\|$ 对用户模板进行加密。

认证代理服务器将加密后的数据 $\{\boldsymbol{C}_{D_1},\boldsymbol{C}_{D_2},\cdots,\boldsymbol{C}_{D_P}\}$ 和 $\{L_1,L_2,\cdots,L_P\}$ 发送给在线身份认证服务器，并将 $\{\boldsymbol{M}_1,\boldsymbol{M}_2,\boldsymbol{H}\}$ 安全保存在本地服务器。在线身份认证服务器为用户返回唯一标识 ID 并由认证代理服务器返回给用户。

5.2 身份认证请求阶段

用户的身份认证请求阶段包含用户身份认证凭据计算和用户身份认证凭据加密。其中，用户首先将身份认证凭据及其唯一标识发送到认证代理服务器；代理认证服务器对用户的认证凭据进行加密处理，并将密文认证凭据和用户标识发送到在线身份认证服务器。为防止遭遇攻击导致用户认证凭据明文数据泄露，认证代理服务器将收到的用户认证凭据进行删除处理。

5.2.1 用户身份认证凭据的计算

用户按照 Eigenface 人脸识别算法的要求，在本地生成其身份认证凭据。用户首先拍摄一张自己的面部图像，根据 Eigenface 人脸识别算法计算其身份认证凭据 $\boldsymbol{\Omega}_{\text{new}}$，随后通过安全信道将 $\boldsymbol{\Omega}_{\text{new}}$ 发送到认证代理服务器。

5.2.2 用户身份认证凭据的加密

认证代理服务器首先将身份认证凭据 $\boldsymbol{\Omega}_{\text{new}}$ 扩展成为一个（$k+2Z$）维的向量 $\boldsymbol{\Omega}_{\text{new-extended}}$（扩展规则为前 k 维数据和 $\boldsymbol{\Omega}_{\text{new}}$ 保持一致，第 $(k+1)$ ~ $(k+2Z)$ 维的值为 $r_1,r_2,\cdots,r_{2Z}$，其中 $r_1,r_2,\cdots,r_{2Z}$ 为一组服从标准正态分布 $\text{N}(0,\sigma^2)$ 的随机数）。认证代理服务器首先提取出在注册计算所选取的加密参数，计算 $\boldsymbol{C}_{\boldsymbol{H}}=\boldsymbol{M}_2^{-1}\boldsymbol{H}^{\mathrm{T}}$。之后对计算出的身份认证凭据进行加密 $\boldsymbol{C}_{\boldsymbol{A}}=\boldsymbol{\Omega}_{\text{new-extended}}\boldsymbol{M}_1^{-1}$，然后计算身份认证凭据模长 $L_{\text{new}}=\|\boldsymbol{\Omega}_{\text{new}}\|$。认证代理服务器将 $\boldsymbol{C}_{\boldsymbol{H}}$、$\boldsymbol{C}_{\boldsymbol{A}}$、$L_{\text{new}}$ 和身份标识 ID 发送给在线身份认证服务器。

5.3 身份判别阶段

在本阶段，在线身份认证服务器根据身份认证请求中的用户标识 ID，查找用户对应的身份认证模板，计算密文下的用户身份模板和用户身份认证凭据之间的相似度，将该相似度和阈值之间进行对比得出身份认证结果，并经由认证代理服务器向用户返回认证结果，具体过程如下。

在线身份认证服务器在收到认证代理服务器发送来的身份认证请求 $\{\boldsymbol{C}_{\boldsymbol{H}},\boldsymbol{C}_{\boldsymbol{A}},L_{\text{new}}\}$ 后，根据用户的身份标识 ID，查找用户的身份认证模板 $\{\boldsymbol{C}_{D_1},\boldsymbol{C}_{D_2},\cdots,\boldsymbol{C}_{D_P}\}$ 和 $\{L_1,L_2,\cdots,L_P\}$。在获取到用户的身份认证模板后，服务器通过 score_i 的计算式来计算收到的身份认证凭据和身份认证模板之间的相似度。

$$\text{score}_i=\frac{\boldsymbol{C}_{\boldsymbol{A}}\boldsymbol{C}_{\boldsymbol{D}_i}\boldsymbol{C}_{\boldsymbol{H}}}{L_iL_{\text{new}}}=\frac{\boldsymbol{W}_{\boldsymbol{D}_i}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{\Omega}_{\text{new}}}{L_iL_{\text{new}}}=\frac{\boldsymbol{\Omega}_i\boldsymbol{\Omega}_{\text{new}}+\sum r_i}{\|\boldsymbol{\Omega}_i\|\|\boldsymbol{\Omega}_{\text{new}}\|}$$

由于 $\sum_1^{2Z}r_i=0$，因此 $\text{score}_i=\dfrac{\boldsymbol{\Omega}_i\boldsymbol{\Omega}_{\text{new}}}{\|\boldsymbol{\Omega}_i\|\|\boldsymbol{\Omega}_{\text{new}}\|}$。服务器选择出 score_i 中的最大值 $\text{score}_{\max}$，并将其发送给认证代理服务器。认证代理服务器根据预先设置的系统门限值对用户的身份认证结果进行判断。如果 $\text{score}_{\max}\geqslant\theta$，则用户通过身份认证；反之，则用户未通过身份认证。

6 安全性分析

6.1 攻击模型Ⅰ下的安全性分析

在攻击者模型Ⅰ下，攻击者仅能获取到加密后

的用户的人脸数据模板和基于用户人脸数据生成的认证请求，即方案中对应的$\{\boldsymbol{C}_{D_1},\boldsymbol{C}_{D_2},\cdots,\boldsymbol{C}_{D_P}\}$、$\{L_1,L_2,\cdots,L_P\}$、$\boldsymbol{C}_{\boldsymbol{H}}$、$\boldsymbol{C}_{\boldsymbol{A}}$和$L_{\text{new}}$。当$Z$=0时，根据第5节可知$\boldsymbol{C}_{\boldsymbol{D}_i}=\boldsymbol{M}_1\boldsymbol{W}_{\boldsymbol{D}_i}\boldsymbol{M}_2$，在不知对应明文$\boldsymbol{W}_{\boldsymbol{D}_i}$的条件下，攻击者无法求得可逆矩阵$\boldsymbol{M}_1$和$\boldsymbol{M}_2$的值；$\boldsymbol{C}_{\boldsymbol{H}}=\boldsymbol{M}_2^{-1}\boldsymbol{H}^{\mathrm{T}}$，$\boldsymbol{C}_{\boldsymbol{A}}=\boldsymbol{\Omega}_{\text{new-extended}}\boldsymbol{M}_1^{-1}$，由于攻击者并不知道$\boldsymbol{C}_{\boldsymbol{A}}$所对应明文$\boldsymbol{\Omega}_{\text{new-extended}}$，因此其也无法得知可逆矩阵$\boldsymbol{M}_1$和$\boldsymbol{M}_2$的值。因此当安全参数$Z$=0时，本文所提出的方案在攻击者模型Ⅰ下是安全的。

6.2　攻击模型Ⅱ下的安全性分析

在攻击者模型Ⅱ下，攻击者能够获取到某个用户加密后的人脸图像特征模板、加密后的身份认证凭据和数据库中一些对应的明文数据，但是攻击者并不清楚这些明文之间的对应关系，即本文方案中对应的$\{\boldsymbol{C}_{D_1},\boldsymbol{C}_{D_2},\cdots,\boldsymbol{C}_{D_P}\}$、$\{L_1,L_2,\cdots,L_P\}$、$\boldsymbol{C}_{\boldsymbol{H}}$、$\boldsymbol{C}_{\boldsymbol{A}}$和$L_{\text{new}}$。当$Z$=1时，根据第5节可知：$\boldsymbol{C}_{\boldsymbol{D}_i}=\boldsymbol{M}_1\boldsymbol{W}_{\boldsymbol{D}_i}\boldsymbol{M}_2$，在不知对应明文$\boldsymbol{W}_{\boldsymbol{D}_i}$的条件下，攻击者无法求得可逆矩阵$\boldsymbol{M}_1$和$\boldsymbol{M}_2$的值；$\boldsymbol{C}_{\boldsymbol{H}}=\boldsymbol{M}_2^{-1}\boldsymbol{H}^{\mathrm{T}}$，$\boldsymbol{C}_{\boldsymbol{A}}=\boldsymbol{\Omega}_{\text{new-extended}}\boldsymbol{M}_1^{-1}$，由于攻击者并不知道$\boldsymbol{C}_{\boldsymbol{A}}$所对应明文$\boldsymbol{\Omega}_{\text{new-extended}}$，因此其也无法得知可逆矩阵$\boldsymbol{M}_1$和$\boldsymbol{M}_2$的值。同时，由于攻击者还可以获取一部分明文数据，因此攻击者可能根据明文与明文之间和密文与密文之间的对应关系来进行已知样本攻击。定义本文方案中的加密过程为$E(\cdot)$，当Z=1时，有

$$\cos\left(E\left(\boldsymbol{\Omega}_{i\text{-extended}}\right),E\left(\boldsymbol{\Omega}_{\text{new-extended}}\right)\right)\neq\cos\left(\boldsymbol{\Omega}_{i\text{-extended}},\boldsymbol{\Omega}_{\text{new-extended}}\right)$$

因此，本文方案中针对用户人脸特征模板所做的变换不再是等距离变换。基于此的主成分分析[25]、双样分析[26]、签名连接攻击[27]等方法都无法成功。因此，当安全参数Z=1时，本文所提出的方案在攻击者模型Ⅱ下是安全的。

6.3　攻击模型Ⅲ下的安全性分析

在攻击者模型Ⅲ下，攻击者能够获取到加密后用户的人脸数据模板$\{\boldsymbol{C}_{D_1},\boldsymbol{C}_{D_2},\cdots,\boldsymbol{C}_{D_P}\}$、$\{L_1,L_2,\cdots,L_P\}$和基于用户人脸数据生成的认证请求$\boldsymbol{C}_{\boldsymbol{H}}$、$\boldsymbol{C}_{\boldsymbol{A}}$和$L_{\text{new}}$，也可以获取这些数据所对应的明文数据，并且可以通过恶意查询的方式获取人脸模板数据和人脸数据生成的认证请求数据的明密文对。当Z=2时，攻击者不能从$\{\boldsymbol{C}_{D_1},\boldsymbol{C}_{D_2},\cdots,\boldsymbol{C}_{D_P}\}$、$\boldsymbol{C}_{\boldsymbol{H}}$、$\{L_1,L_2,\cdots,L_P\}$中获取到可逆矩阵$\boldsymbol{M}_1$和$\boldsymbol{M}_2$、随机向量$\boldsymbol{H}$，继而无法获得用户的生物特征模板$\boldsymbol{\Omega}_i$和用户身份认证凭据$\boldsymbol{\Omega}_{\text{new}}$。但由于攻击者能够通过恶意查询的方式获取到一些人脸模板数据和人脸数据生成的认证请求数据的明密文对，且$\boldsymbol{C}_{\boldsymbol{A}}=\boldsymbol{\Omega}_{\text{new-extended}}\boldsymbol{M}_1^{-1}$，其中$\boldsymbol{\Omega}_{\text{new-extended}}$是一个扩展到$(P+2Z)$维的特征向量，由线性方程组解的存在性与唯一性定理，攻击者无法从获取到的一个密文中获取到用户生物特征相关的敏感信息。攻击者从多个密文之间的交叉运算，也无法得到用户的敏感信息。因此当选取的安全参数Z=2时，本文所提出的方案在攻击者模型Ⅲ下是安全的。

6.4　安全性分析对比

为了进一步说明本文方案的安全性，将本文方案的安全性和文献[12]方案的安全性进行了对比分析，分析结果如表2所示。

由表2可知，本文方案的安全性和对比方案的安全性相当，但是本文方案可以通过安全参数的选择来实现方案在安全性和计算效率之间的平衡。

7　性能分析

7.1　通信开销

本文方案中的通信开销主要产生于用户在注册阶段中向服务器发送其人脸特征模板和用户在认证阶段向服务器发送身份认证请求这2个过程。将本文方案、未进行隐私保护的基于Eigenface人脸识别算法的原始方案（以下简称“原始方案”）和文献[12]方案的通信开销进行对比。文献[12]方案用到了Paillier加密方案和全同态加密方案，假设文献[12]方案采用密钥长度为1 024 bit，2种密

表2　　**本文方案和文献[12]方案的安全性对比**

方案	保护用户模板	保护用户认证凭据安全	满足攻击模型Ⅰ下安全	在攻击模型Ⅱ中安全	在攻击模型Ⅲ中安全
本文方案	是	是	当Z=0时满足	当Z=1时满足	当Z=2时满足
文献[12]方案	是	是	是	是	是

码算法的密文长度分别为 2 048 bit 和 1 024 bit，本文方案中的密文长度采用 64 bit 的浮点型数值表示。表 3 列举了两者在注册和认证阶段中客户端的通信数据量。

表 3 通信开销对比

方案	注册阶段/bit	认证阶段/bit
原始方案	$64(Pk+1)$	$64k$
本文方案	$64(P(k+2Z)^2+P)$	$256Z+128k+64$
文献[12]方案	$2\,048N+7\,168$	$2\,048k+2\,048P+9\,126$

表 3 中，P 表示注册时用户提交的人脸图像数，Z 表示一个认证代理服务器选定的安全参数，k 表示认证过程中选取的特征向量数，N 表示用户人脸图像数据的像素数，而 P 和 Z 的数值一般不会过大且 $k \leqslant P$，N 的取值一般远大于 P，一般令 $P \leqslant 10$，$N > 10^4$。通过表 3 可知，在加入隐私保护的功能后，本文方案中 2 个阶段的通信数据量虽然有所增加，但依然在一个可以接受的范围并且通信量远小于文献[12]方案的通信量。

7.2 计算开销

本文方案中用户的计算开销主要涉及用户注册时加密其特征模板的计算开销，以及用户在生成身份认证请求时，加密其身份认证凭据所产生的计算开销。服务器端的计算开销主要涉及服务器在对用户的身份进行判别时所需要的计算开销。为进一步对计算开销进行分析，对本文方案进行了仿真实验。在仿真实验中，统一采用 i7 8750H、16 GB 内存、Windows10 操作系统的实验环境，采用公开的 ORL（olivetti research laboratory）人脸数据库[28]作为测试数据，其中每张人脸数据的大小为 92 像素×112 像素。仿真实验中，每个用户人脸特征模板采用 9 张人脸作为训练数据。首先将本文方案中加密特征模板、加密认证请求和验证用户身份的计算开销随方案参数的变化进行了测试，结果如图 3 和图 4 所示。

图 3 显示了在保持安全参数不变（$Z=0$）的情况下，用户加密人脸特征模板、加密认证请求和服务器验证用户身份所需的时间随所选取的特征向量数的变化情况。图 4 显示了在选取的特征向量数不变（$k=7$）的情况下，用户加密人脸特征模板、加密认证请求和服务器验证用户身份所需的时间随用户选取的安全参数的变化情况。

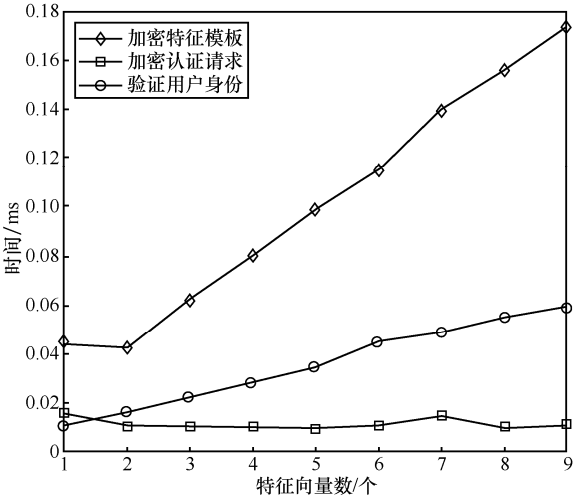


图 3 所提方案各阶段计算开销随特征向量数的变化情况

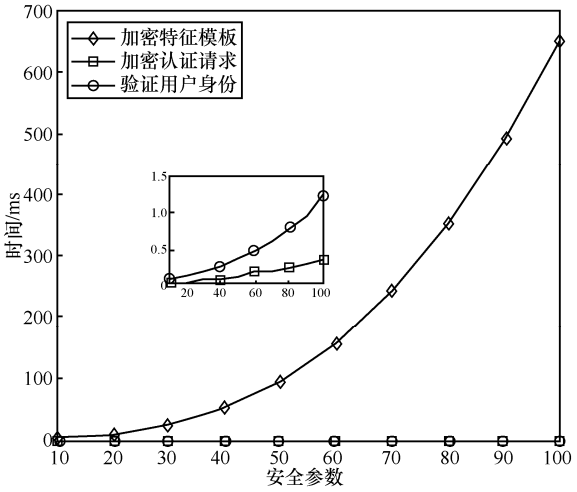


图 4 所提方案各阶段计算开销随安全参数的变化情况

随后，本文选择文献[12]方案作为对比方案，并对 2 种方案中用户在进行注册时加密用户认证凭据的计算开销和身份认证时在密文下计算用户身份认证凭据和模板之间的相似度计算开销进行了对比。在仿真实验中，将文献[12]方案中采用密钥长度设为 1 024 bit，本文方案中的安全参数 $Z=0$。2 种方案在用户注册阶段的计算开销如图 5 所示，在身份认证阶段的计算开销如图 6 所示。

仿真结果表明，本文方案在 2 个阶段所需要的计算时间均在可接受的范围内。

7.3 认证准确率

由 5.3 节中分析可知，本文方案并未对原有的人脸认证方案的判别方式进行改变，因此本文方案不会对原始方案的准确率产生影响，且与原始方案的准确度保持一致。

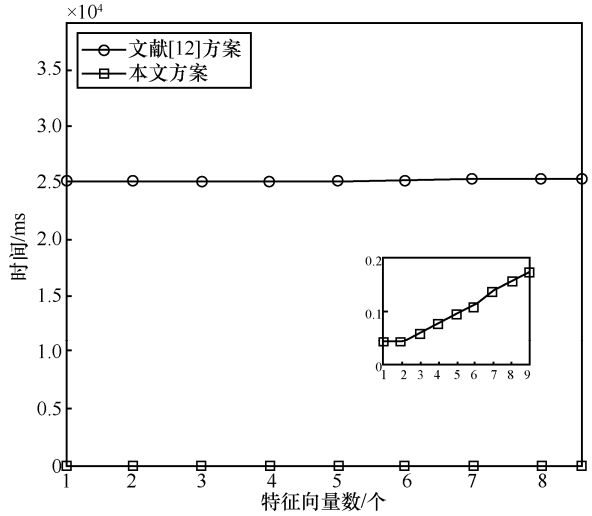


图 5　用户注册阶段计算开销对比

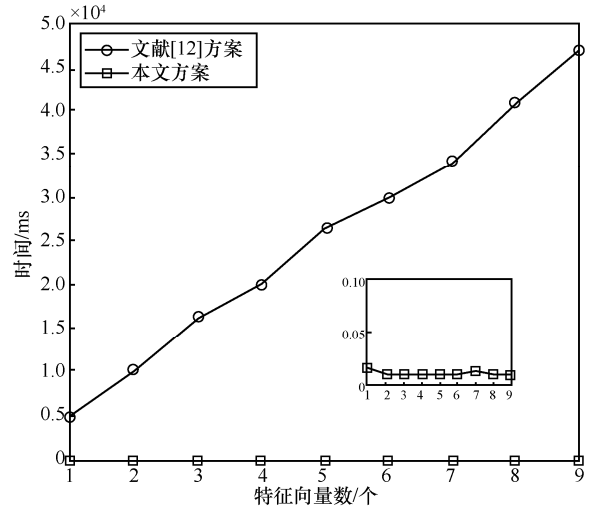


图 6　用户身份认证阶段计算开销对比

8　结束语

针对在线人脸认证系统中用户敏感数据容易被泄露这一问题，本文基于矩阵加密提出了一种安全、高效的隐私保护人脸认证方案，所提方案能够保证用户存储在认证代理服务器数据库中的模板和用户身份认证请求中所包含的个人敏感信息的安全。理论分析表明，本文方案可以根据选取的安全参数的不同实现不同等级的隐私保护效果，能够满足不同场景中差异化的隐私保护需求；同时，隐私保护机制的引入并未使原始方案的准确度降低，保证了原始方案的可用性。实验结果证明，本文方案具有较低的计算开销和通信开销，能够在真实环境中安全高效地保护在线人脸认证。

参考文献：

[1] SPREEUWERS L J, HENDRIKSE A J, GERRITSEN K J. Evaluation of automatic face recognition for automatic border control on actual data recorded of travellers at schiphol airport[C]//International Conference of Biometrics Special Interest Group. Piscataway: IEEE Press, 2012:1-6.

[2] SAMANTHA S. Credit card with a fingerprint sensor revealed by mastercard[EB].(2017-04-20)[2020-03-08].

[3] RICHARD W. Face recognition tested to monitor terrorist suspects[EB]. (2017-07-20)[2020-03-08].

[4] WU H. Alleged breach of India's biometric database could put 1.2bn users at risk[EB]. (2018-01-11)[2020-03-08].

[5] Avast Security News Team. Biometric security platform leaves 28M records unsecured [EB]. (2019-08-16[2020-03-08].

[6] LI Q, ZHU H, ZHANG Z, et al. Spoofing attacks on speaker verification systems based generated voice using genetic algorithm[C]//2019 IEEE International Conference on Communications. Piscataway: IEEE Press, 2019:1-6.

[7] 李凤华, 李晖, 贾焰, 等. 隐私计算研究范畴及发展趋势[J]. 通信学报, 2016, 37(4): 1-11.
LI F H, LI H, JIA Y, et al. Privacy computing:concept, connotation and its research trend[J]. Journal on Communications, 2016, 37(4): 1-11.

[8] BENSON B. Fingerprint not recognized: why the united states needs to protect biometric privacy[J]. North Carolina Journal of Law & Technology, 2018, 19(4): 161-192.

[9] LI F H, LI H, NIU B, et al. Privacy computing: concept, computing framework, and future development trends[J]. Engineering, 2019, 5(9):1179-1192.

[10] 朱辉, 武衡, 赵海强, 等. 适用于双层卫星网络的星间组网认证方案[J]. 通信学报, 2019, 40(3): 1-9.
ZHU H, WU H, ZHAO H Q, et al. Efficient authentication scheme for double-layer satellite network[J]. Journal on Communications, 2019, 40(3): 1-9.

[11] ERKIN Z, FRANZ M, GUAJARDO J, et al. Privacy-preserving face recognition[C]//International Symposium on Privacy Enhancing Technologies Symposium. Berlin: Springer, 2009: 235-253.

[12] DAMGARD I., GEISLER M, KRIGAARD M, et al. Efficient and secure comparison for on-line auctions[C]//Australasian Conference on Information Security and Privacy. Berlin: Springer, 2007: 416-430.

[13] SADEGHI A, SCHNEIDER T, WEHRENBERG I. Efficient privacy-preserving face recognition[C]//International Conference on Information Security and Cryptology. Berlin: Springer, 2009: 229-244.

[14] XIANG C, TANG C, CAI Y, et al. Privacy-preserving face recognition with outsourced computation[J]. Soft Computing, 2016, 20(9): 3735-3744.

[15] ZHU H, WEI Q, YANG X P, et al. Efficient and privacy-preserving online fingerprint authentication scheme over outsourced data[J]. IEEE Transactions on Cloud Computing, 2018: 1.

[16] YUAN J, YU S. Efficient privacy-preserving biometric identification in cloud computing[C]//2013 Proceedings IEEE International Conference on Computer Communications. Piscataway: IEEE Press, 2013:

2652-2660.

[17] WANG Q, HU S, REN K, et al. CloudBI: practical privacy-preserving outsourcing of biometric identification in the cloud[C]//European Symposium on Research in Computer Security. Berlin: Springer, 2015: 186-205.

[18] ZHU L, ZHANG C, XU C, et al. An efficient and privacy-preserving biometric identification scheme in cloud computing[J]. IEEE Access, 2018(6): 19025-19033.

[19] RAHULAMATHAVAN Y, RAJARAJAN M. Hide-and-seek: face recognition in private[C]//2015 IEEE International Conference on Communications. Piscataway: IEEE Press, 2015: 7102-7107.

[20] GUNASINGHE H, BERTINO E. PrivBioMTAuth: privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones[J]. IEEE Transactions on Information Forensics & Security, 2018, 13(4):1042-1057.

[21] SARIER N D. Privacy preserving biometric identification on the bitcoin blockchain[C] //2018 International Symposium on Cyberspace Safety and Security. Berlin: Springer, 2018:254-269.

[22] TURK M A, PENTLAND A P. Face recognition using eigenfaces[C]// Proceedings of 1991 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Press, 1991: 586-591.

[23] GUPTA S, SAHOO O P, GOEL A, et al. A new optimized approach to face recognition using eigenfaces[J]. Global Journal of Computer Science and Technology, 2010(10):15-17.

[24] SHAN S, CAO B, GAO W, et al. Extended fisherface for face recognition from a single example image per person[C]//2002 IEEE International Symposium on Circuits and Systems. Proceedings. Piscataway: IEEE Press, 2002(2): 81-84.

[25] LIU K, GIANNELLA C, KARGUPTA H. An attacker's view of distance preserving maps for privacy preserving data mining[C]//European Conference on Principles of Data Mining and Knowledge Discovery. Berlin: Springer, 2006: 297-308.

[26] CAO N, YANG Z, WANG C, et al. Privacy-preserving query over encrypted graph-structured data in cloud computing[C]//2011 31st International Conference on Distributed Computing Systems. Piscataway: IEEE Press, 2011: 393-402.

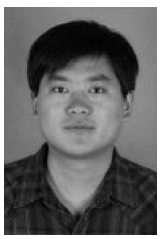
[27] WONG W K, CHEUNG D W, KAO B, et al. Secure KNN computation on encrypted databases[C]//Proceedings of the 2009 ACM SIGMOD International Conference on Management of data. New York: ACM Press, 2009: 139-152.

[28] AT&T Laboratories Cambridge. The ORL database of faces[DB]. AT&T Labs Research, [2020-03-08].

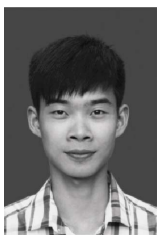
[作者简介]

李明（1977– ），男，陕西西安人，博士，国家知识产权局专利局研究员，主要研究方向为数据安全与应用安全。

杨晓鹏（1991– ），男，河南林州人，西安电子科技大学博士生，主要研究方向为生物特征隐私保护、密码学及其应用。



朱辉（1981– ），男，河南周口人，博士，西安电子科技大学教授、博士生导师，主要研究方向为数据安全与隐私保护、安全方案及协议设计、网络及应用安全等。



王枫为（1993– ），男，河南周口人，西安电子科技大学博士生，主要研究方向为大数据安全与隐私保护与应用密码学。

李祁（1994– ），男，江苏苏州人，西安电子科技大学硕士生，主要研究方向为大数据安全与隐私保护、应用密码学。

收录声明

本刊对发表的文章，拥有出版电子版、网络版版权，并拥有和其他网站交换信息的权利。本刊支付的稿酬中已经包含上述费用。

Journal on Communications has the copyright to publish electronic edition, online edition of the published articles, and has the right to exchange information with other sites. The expenses have been included in the fee paid by editorial department.

道德声明

本刊发表的论文是作者独立取得的原创性研究成果，无一稿多投；论文内容不涉及国家机密；未曾以任何形式用任何文种在国内外公开发表过；论文内容不侵犯他人著作权和其他权利。若发生一稿多投、侵权、泄密等问题，论文作者将承担全部责任。

The authors of *Journal on Communications* guarantee that their submitted articles are original and contain nothing confidential. The said article is only submitted to *Journal on Communications*. The said article has not been published before and has not been submitted elsewhere for print or electronic publication consideration. The said article is no way whatever a violation or an infringement of any existing copyright or license from the third party. Otherwise, the authors of the said article shall take the blame for the violation or infringement of the related copyright and the leakage of secrets.

通信学报

Journal on Communications

发行代号：国内2-676 / 国外M395　2020年5月25日出版　定价：98.00元

ISSN 1000-436X

9 771000 436205 05>