基于余弦测度的 Web 指纹识别算法的研究与改进

汤文亮[1] 汤树芳[2] 张 平[2]

(华东交通大学信息工程学院 南昌 330013)[1] (华东交通大学软件学院 南昌 330013)[2]

摘 要 为了在 Web 指纹数据库中实现对 Web 指纹的准确识别,需要对 Web 指纹识别算法进行研究。采用当前识别算法对 Web 指纹数据库中的 Web 指纹进行识别时,识别的结果与实际结果之间存在误差、识别所用的时间较长,因此存在识别准确率低和识别效率低的问题。在余弦测度的基础上提出了一种 Web 指纹识别算法,在结构特征、静态文件、Cookie 设计和关键字 4 个方面采用源码审计方法完成了对 Web 指纹的选取,建立了 Web 指纹数据库。首先提取 Web 指纹数据库中数据的特征,根据特征提取结果剔除 Web 指纹数据库中存在的异常数据;然后将余弦距离函数当作相似性度量函数,采用 K-means 算法对 Web 指纹数据库中的 Web 指纹进行聚类;最后根据聚类结果完成对 Web 指纹的识别。实验结果表明,所提方法可在较短的时间内准确地完成对 Web 指纹数据库中 Web 指纹的识别,具有识别准确率高和识别效率高的优点。

关键词 余弦测度,Web 指纹,识别算法

中图法分类号 TP391.41 **文献标识码** A **DOI** 10.11896/jsjkx.180801473

Research and Improvement of Web Fingerprint Identification Algorithm Based on Cosine Measure

TANG Wen-liang[1] TANG Shu-fang[2] ZHANG Ping[2]

(School of Information Engineering, East China Jiaotong University, Nanchang 330013, China)[1]

(School of Software, East China Jiaotong University, Nanchang 330013, China)[2]

Abstract In order to realize the accurate identification of Web fingerprints in the Web fingerprint database, it is necessary to study the Web fingerprint identification algorithm. When the current fingerprint recognition algorithm is used to identify the Web fingerprint in the Web fingerprint database, there is an error between the recognition result and the actual result, and the recognition takes a long time, which result in low recognition accuracy and recognition efficiency. Based on the cosine measure, a Web fingerprint identification algorithm was proposed. The source fingerprint method is used to select the Web fingerprint in the four aspects of structural features, static files, cookie design and keywords, and a Web fingerprint database is established. Firstly, the characteristics of the data in the Web fingerprint database are extracted, and the abnormal data existing in the Web fingerprint database are removed according to the feature extraction result. Then, the cosine distance function is used as the similarity measurement function, and the K-means algorithm is used to cluster the Web fingerprints in the Web fingerprint database. Finally, the identification of the web fingerprint is completed according to the clustering result. The experimental results show that the proposed method can accurately complete the Web fingerprint identification in the Web fingerprint database in a short time, and has the advantages of high recognition accuracy and high recognition efficiency.

Keywords Cosine measure, Web fingerprint, Recognition algorithm

大数据技术的飞速发展,使接入网络空间的设备总数不断增加[1]。网络环境是由路由器、服务器、网络电话、交换机和打印机等设备组成的。终端设备在网络空间中具有类型复杂和规模大的特点[2]。经调查发现,去除主机和普通网站,网络空间中已存在五百万以上的设备。网络复杂的环境对网络安全造成了威胁,黑客通过对无线路由器进行攻击,可以窃取用户信息、盗用管理员权限,并对路由信息进行重置,甚至攻击工业控制系统以扰乱工业生产[3]。用户的财产和信息安全一直受网络漏洞的威胁,通过检测终端设备漏洞可以保障网络空间的安全。Web 指纹识别技术可有效地完成漏洞的检测,被广泛地应用在网络安全保护中[4]。当前 Web 指纹识别算法存在识别准确率低和识别效率低的问题,需要对 Web 指纹识别算法进行进一步的研究[5]。

杜博远等[6]提出了一种基于关键信息的 Web 指纹识别算法,该算法对采集的信息进行了预处理,采用最长公共子串算法对 Web 信息的特征进行提取,根据特征提取结果建立正则表达式,在行号辅助判断的基础上通过正则表达式完成对 Web 指纹的识别。该算法得到的 Web 指纹识别结果存在误

到稿日期:2018-08-09 返修日期:2018-08-27 本文受江西省科技支撑项目(20171BBH80005),江西省科技厅项目(2000616078)资助。

汤文亮(1969-),男,教授,硕士生导师,主要研究方向为信息安全、大数据分析、物联网,E-mail:october12121@163.com(通信作者);**汤树芳**(1994-),男,硕士生,主要研究方向为信息安全;**张 平**(1993-),男,硕士生,主要研究方向为大数据分析。

差,识别准确率低。赵冬梅等[7]提出了一种基于并行约简的 Web 指纹识别算法,该算法在并行约简思想的基础上通过粗糙集对决策信息表进行扩展,采用条件熵对 Web 指纹的重要度进行计算,遵循约简规则删除 Web 中存在的冗余信息,完成对 Web 指纹的识别。该算法存在计算步骤较多、识别所用的时间较长、识别效率低的问题。周修考[8]提出了一种基于数据聚类的 Web 指纹识别算法,该算法通过构建 Web 信息流模型将分类误码率映射为密度函数,采用定量递归分析法得到 Web 时间序列,通过时间序列计算 Web 定量递归特征,根据定量递归特征对 Web 指纹进行分类,根据分类结果完成对 Web 指纹的识别;该算法得到的识别结果与实际结果之间的误差较大,存在识别准确率低的问题。

针对上述问题,本文提出一种基于余弦测度的 Web 指纹识别算法。

1 Web 指纹数据库的建立

通过发送 HTTP 请求识别 Web 服务器是当前 Web 指纹识别技术中的主要研究内容,网络安全设备容易将 HTTP 请求当做恶意流量,对其进行拦截,且 HTTP 请求的识别速度慢[9]。基于余弦测度的 Web 指纹识别算法将 Web 服务器作为研究对象,采用黑盒测试的方法将 6 种 HTTP 请求发送到 Web 服务器中,通过提取报文的特征完成对指纹的采集。

对响应报文进行分析,得到下面两种指纹来识别网络服务器:

(1)头部域顺序指纹,可以通过头部域的顺序精确地完成对服务器类型的识别。

(2)状态码定义指纹,在了解 Web 服务器类型的基础上,可以通过请求的响应状态码完成对 Web 服务器的识别。

基于余弦测度的 Web 指纹识别算法采用源码审计方法对 Web 应用的结构设计、源码和静态文件进行分析,从结构特征、静态文件、Cookie 设计和关键字 4 个方面完成对 Web 指纹的选取,从而建立 Web 指纹数据库。

(1)结构特征:通过服务器的结构特点完成对服务器版本的识别,可以从 HTML 数据头部得到结构特征指纹[10-11]。

(2)静态文件:采用没有经过修改的静态文件对 Web 应用版本和类型进行识别。

(3)Cookie 设计:Cookie 名是由开发者设计的,可以通过 Cookie 名完成对 Web 应用类型的识别[12]。

(4)关键字:主流工具主要通过 HTML 源码中存在的关键字对指纹进行采集,关键字具有易被删除和与功能无关的缺点,可将关键字作为补充指纹。

在以上 4 个方面中,Cookie 设计、结构特征和静态文件 3 类指纹识别与 Web 应用功能之间的关联较大,具有不易被删除和修改的优点。通过采集 Web 指纹建立了 Web 指纹数据库。

2 异常数据剔除方法

基于余弦测度的 Web 指纹识别算法在对 Web 指纹进行识别之前,根据异常数据在 Web 指纹数据库中的初始频率均值和标准差构建功率谱密度函数,并将函数值作为异常数据的特征[13-14],根据特征提取结果采用稀疏分数方法剔除 Web 指纹数据库中存在的异常数据,从而减少了识别的指纹数据量,提高了算法的识别效率。

设 $X=\{x_1,x_2,\cdots,x_n\}$ 表示 Web 指纹数据库中的数据集,n 表示数据集 X 的总数,数据集 X 中存在的元素都是 p 维的矢量;c 表示数据集 X 中存在的类别总数;$v_i=\{v_{i1},v_{i2},\cdots,v_{ip}\}$ 表示第 i 类的中心;$\{x_{i1},x_{i2},\cdots,x_{im}\}$ 表示数据库中第 i 类的数据输入变量;y_i 为对应的数据类型,通常情况下 y_i 的值为 -1 或 1。当 y_i 的值为 1 时,数据为正常数据,当 y_i 的值为 -1 时,数据为异常数据,得到 Web 指纹数据库异常数据 y_i 的表达式为:

$$y_i=f(x_1,x_2,\cdots,x_m) \tag{1}$$

设 $z(t)$ 代表异常数据的频域模型,$z(t)$ 的表达式为:

$$z(t)=y_i a(t)+ja(t)\cdot\phi(t) \tag{2}$$

其中,$a(t)$ 代表频域模型的瞬时幅度,即包络;$\phi(t)$ 代表频域谐振幅度;j 代表异常数据样本的类别。设 E_j 代表所有样本属于 j 类的隶属度均值,其计算公式为:

$$E_j=z(t)\sum F_{ij}/K_j \tag{3}$$

其中,F_{ij} 代表第 i 个样本属于第 j 类的最大隶属度;K_j 代表第 j 类样本在数据库中的数目。在高密度区域中选取若干个点集构成距离中心集合 S,设 s_i 代表聚类中心集合中存在的最大值,将 s_i 当作第一个聚类中心 Z_1。

设 $\hat{\mu}$ 代表异常数据在 Web 指纹数据库中的初始频率均值;$\hat{\sigma}$ 代表异常数据在 Web 指纹数据库中的标准差。在平均方差函数值较小原则的基础上[15],将功率谱密度函数 $\hat{\beta}_k$ 作为异常数据的特征,来完成对 Web 指纹数据库中异常数据特征的提取:

$$\hat{\beta}_k=\hat{\mu}\cdot E_j-(\hat{\sigma}-1/k)^q \tag{4}$$

采用稀疏分数方法,根据异常数据特征,在 Web 指纹数据库中将异常数据剔除[16-19]。在类别总数为 c 的 Web 指纹数据库中,ω 代表数据集的类别,$\omega=1,2,\cdots,c$。设 Web 指纹数据库中的样本总数为 h_ω,$\mu_{\omega r}$ 和 $\sigma_{\omega r}^2$ 分别表示第 r 维样本特征的均值和方差,F_r 表示第 r 维样本特征的 Fisher 分数。F_r 的计算公式为:

$$F_r=\sum_{\omega=1}^{c}h_\omega(\mu_{\omega r}-\mu_r)^2/\sum_{\omega=1}^{c}h_\omega\sigma_{\omega r}^2 \tag{5}$$

其中,μ_r 代表 Web 指纹数据库中第 r 维样本的特征均值。采用 L_1 范数最小化优化方法在特征均值 μ_r 的基础上剔除 Web 数据库中存在异常的数据。

$\{x_i\}$ 为 Web 指纹数据库中的数据集,设矩阵 $\boldsymbol{X}=[x_1,x_2,\cdots,x_n]$ 中存在的每一列都是数据集中的向量,重构数据量 x_i 得到数据 s_i,通过求解 Web 指纹数据库中数据之间的 L_1 范数,将 Web 数据库中异常数据剔除问题转化为最小化线性规划问题,并对 $\boldsymbol{s}_i$ 数据进行最小化重构,公式如下:

$$\boldsymbol{x}(\boldsymbol{s})=\min\|\boldsymbol{s}_i\|_1\quad \text{s.t. } x_i=\boldsymbol{X}'\boldsymbol{s}_i \tag{6}$$

其中,$\boldsymbol{X}'$ 代表矩阵 $\boldsymbol{X}$ 去除第 i 列 x_i 后得到的数据矩阵;$\boldsymbol{s}_i$ 代表 n 维的数据向量。对数据向量 $\boldsymbol{s}_i$ 进行计算时,由于矩阵 $\boldsymbol{X}$ 不包括矩阵 $\boldsymbol{X}'$,因此需要将数据向量 $\boldsymbol{s}_i$ 中存在的第 i 个元素值设为 0。通过式(6)得到 Web 指纹数据库在稀疏表示下的重构稀疏矩阵 $\boldsymbol{x}(\boldsymbol{s})$。

基于稀疏重构系数累加 Web 指纹数据库中的样本重构误差,当重构特征误差或特征较小时,该特征在 Web 指纹数据库中的稀疏表示水平较好,得到的稀疏分数目标函数如下:

$$S(r)=\sum_{i=1}^{n}(x_{ir}-(\boldsymbol{X}'\boldsymbol{s}_i)_r)^2F_r/\mathrm{var}(\boldsymbol{X}(r,:))\boldsymbol{x}(\boldsymbol{s}) \tag{7}$$

其中，$\sum_{i=1}^{n}(x_{ir}-(\boldsymbol{X}'\boldsymbol{s}_i)_r)^2$ 代表 Web 指纹数据库样本集中第 r 维重构特征 $(\boldsymbol{X}'\boldsymbol{s}_i)_r$ 和第 r 维特征 x_{ir} 的累积误差；$\mathrm{var}(X(r,:))$ 代表 Web 指纹数据集中第 r 维样本的特征方差。

通过式(7)可知，Fisher 分数 F_r 与 Web 指纹数据库中的异常数据剔除有直接关系，F_r 值越大，则数据特征的重要度越高，证明该数据为正常数据；F_r 的值越小，则数据特征在 Web 指纹数据库中的显著性越低，即将其视为异常数据。通过式(5)计算 Web 指纹数据库中数据的 Fisher 分数 F_r，再根据计算结果剔除 Web 指纹数据库中存在的异常数据。

3　基于余弦测度的 Web 指纹识别算法

基于余弦测度的 Web 指纹识别算法将剔除了异常数据的 Web 指纹数据集中的数据转变为特征向量，采用 K-means 聚类算法对 Web 指纹进行聚类，聚类过程中的相似性度量函数用余弦距离函数代替，根据聚类结果完成对 Web 指纹的识别。

设 $D=\{d_1,d_2,\cdots,d_n\}$ 代表原始的样本集，其中包括无标记样本和有标记样本；d_i 代表原始样本集中第 i 个样本的 HTTP 头部。对原始样本集中的异常数据进行特征提取，根据提取的数据特征去除原始样本集中存在的异常数据，得到样本集 $\boldsymbol{X}=\{\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_n\}$，其中 $\boldsymbol{x}_i$ 代表在样本集中第 i 个样本的特征向量，该向量的维数是 32。$v_i=\{v_{i1},v_{i2},\cdots,v_{ip}\}$ 代表第 i 类的中心，u 代表初始聚类中心的总数。通过聚类中心的余弦相似性对 n 个样本进行划分，得到 K 个簇 u_1，$u_2,\cdots,u_K$。

设 $\cos\theta$ 代表样本特征向量 $\boldsymbol{x}_i$ 和样本聚类中心 v_j 的余弦相似度，$\cos\theta$ 的计算公式为：

$$\cos\theta=\boldsymbol{x}_iv_j'/\sqrt{(\boldsymbol{x}_i\boldsymbol{x}_i')(v_jv_j')} \tag{8}$$

通过式(8)得到相似性度量函数 $d(\boldsymbol{x}_i,v_k)$，相似性度量函数 $d(\boldsymbol{x}_i,v_k)$ 的表达式为：

$$d(\boldsymbol{x}_i,v_k)=1-x_iv_j'/\sqrt{(\boldsymbol{x}_i\boldsymbol{x}_i')(v_jv_j')} \tag{9}$$

分析式(9)可知，相似性度量函数 $d(\boldsymbol{x}_i,v_k)$ 的值随着样本特征向量和样本聚类中心之间的余弦相似度的增高而减小。

通过上述分析得到聚类准则函数 J，其计算公式为：

$$J=\sum_{j=1}^{K}\sum_{\boldsymbol{x}_i\in V_j}d(\boldsymbol{x}_i,v_k) \tag{10}$$

由式(10)可知，聚类准则函数 J 在收敛时达到最小值，则簇内元素的余弦相似度达到最高，得到的聚类效果越优。通过式(10)对 Web 指纹数据库中的指纹进行聚类。根据聚类结果完成对 Web 指纹的识别。

4　实验结果与分析

为了验证基于余弦测度的 Web 指纹识别算法的整体有效性，需要对基于余弦测度的 Web 指纹识别算法进行测试。本次实验的操作系统为 Windows，实验平台为 Simulink。分别采用基于余弦测度的 Web 指纹识别算法(算法 1)、基于关键信息的 Web 指纹识别算法(算法 2)、基于并行约简的 Web 指纹识别算法(算法 3)进行测试，通过聚类准则函数 J 对比 3 种不同算法识别 Web 指纹的准确率。当聚类准则函数 J 在收敛过程中达到最小值时，簇内元素的余弦相似度达到最高，得到的聚类效果好，识别的准确率高。3 种不同算法的测试结果如图 1 所示。

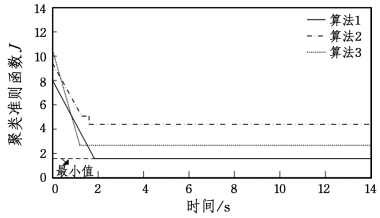
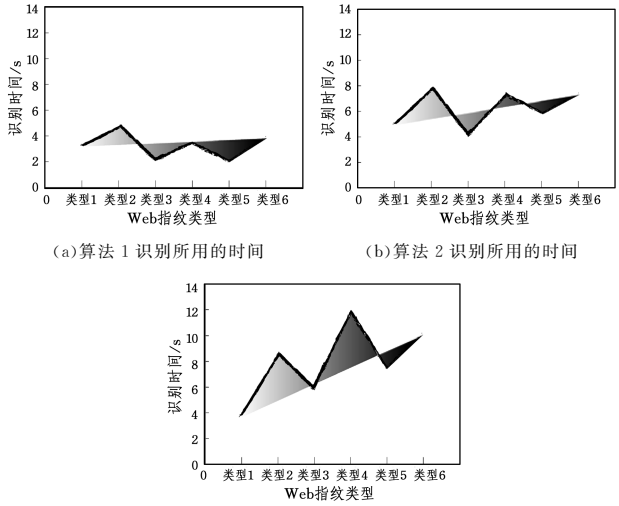


图 1　3 种不同算法的测试结果

Fig. 1　Test results of three different algorithms

分析图 1 可知，采用基于余弦测度的 Web 指纹识别算法得到的聚类准则函数值在接近 2 s 处达到了最小值，且一直保持最小值。采用基于关键信息的 Web 指纹识别算法得到的聚类准则函数值在接近 2 s 处的值最小。采用基于并行约简的 Web 指纹识别算法得到的聚类准则函数值在 1 s 后达到最小。对比基于余弦测度的 Web 指纹识别算法、基于关键信息的 Web 指纹识别算法、基于并行约简的 Web 指纹识别算法的聚类准则函数值可知，只有基于余弦测度的 Web 指纹识别算法得到的聚类准则函数在收敛时达到了最小值，当聚类准则函数值最小时，簇内元素余弦相似度达到最高，Web 指纹数据库中的 Web 指纹聚类效果最优，识别准确率高。由此可知，基于余弦测度的 Web 指纹识别算法的识别准确率较高。

分别采用基于余弦测度的 Web 指纹识别算法(算法 1)、基于关键信息的 Web 指纹识别算法(算法 2)、基于并行约简的 Web 指纹识别算法(算法 3)进行测试，对比 3 种算法对 Web 指纹数据库中存在的不同类型的 Web 指纹进行识别所用的时间，测试结果图 2 所示。



(a)算法 1 识别所用的时间　　(b)算法 2 识别所用的时间

(c)算法 3 识别所用的时间

图 2　3 种不同算法识别所用的时间

Fig. 2　Identification time taken by three different algorithms

图 2(a)为基于余弦测度的 Web 指纹识别算法的测试结果，分析可知，采用该算法对 Web 指纹数据库中不同类型的指纹进行识别时，所用的识别时间均在 5 s 以内。图 2(b)为基于关键信息的 Web 指纹识别算法的测试结果，分析可知，采用该算法对 Web 指纹数据库中不同类型的指纹进行识别时，对第 2 类 Web 指纹识别所用的时间较长，高达 8 s。图 2(c)为基于并行约简的 Web 指纹识别算法的测试结果，分析

可知,采用该算法对 Web 指纹数据库中不同类型的指纹进行识别时,识别第 4 类 Web 指纹所用的时间较长,高达 12s。对比 3 种不同算法的测试结果可知,基于余弦测度的 Web 指纹识别算法对于不同类型的 Web 指纹识别所用的时间均少于其他两种方法,因为基于余弦测度的 Web 指纹识别算法对 Web 指纹进行识别之前,剔除了 Web 指纹数据库中存在的异常数据,减少了需要识别的指纹数据量,提高了识别效率。由此可知,基于余弦测度的 Web 指纹识别算法的识别效率较高。

结束语 信息技术的发展促进了 Web 站点的普及。Web 是当前社会中的热点技术,被广泛地应用到商业流程和企业 IT 系统中,企业通过 Web 获得了经济利益,促进了 Web 的发展。Web 为使用者带来经济利益的同时也存在着安全漏洞,一些非法攻击者通过 Web 站点入侵系统,盗取了公司系统中的秘密文件和信息,为用户带来了损失。

Web 指纹是一种可以标识 Web 组件版本和类型的特殊信息,是在组件开发时生成的,Web 指纹识别技术可以用在服务器安全漏洞检测中。由于当前 Web 指纹识别算法存在识别准确率低和识别效率低的问题,文中提出了一种基于余弦测度的 Web 指纹识别算法,解决了当前算法中存在的问题,为 Web 指纹识别技术的发展奠定了基础。

参 考 文 献

[1] CHEN G P. Research on efficient resource mining technology for large Web network data center[J]. Modern Electronics Technique,2017,40(24):18-20. (in Chinese)
陈贵平. 大型 Web 网络数据中心资源高效挖掘技术研究[J]. 现代电子技术,2017,40(24):18-20.

[2] LIU F,ZHANG D,SHEN L. Study on novel Curvature Features for 3D fingerprint recognition[J]. Neurocomputing,2015,168(C):599-608.

[3] WANG Y. Accurate Detection of User Characteristic Data in Large Data Network[J]. Computer Simulation,2017,34(6):415-418. (in Chinese)
王玥. 大数据网络中用户特征数据准确检测仿真[J]. 计算机仿真,2017,34(6):415-418.

[4] VENKATESH R,MAHESWARI N U,JEYANTHI S. Multiple Criteria Decision Analysis Based Overlapped Latent Fingerprint Recognition System Using fuzzy Sets[J]. International Journal of Fuzzy Systems,2018,14(2):1-27.

[5] XIONG P,HU C X,ZHOU X X. Method for quickly identifying zebra crossing by CNN and artificial feature extraction[J]. Electronic Design Engineering,2018,26(3):189-193. (in Chinese)
熊平,胡彩霞,周欣星. CNN 与人工特征提取快速识别斑马线的方法[J]. 电子设计工程,2018,26(3):189-193.

[6] DU B Y,WANG M Q,CHEN C F,et al. Tags extraction for Web information based on structure consistency and feature learning[J]. Computer Engineering and Applications,2017,53(7):74-78. (in Chinese)
杜博远,王美清,陈长福,等. 基于结构一致和特征学习的网页信息标签提取[J]. 计算机工程与应用,2017,53(7):74-78.

[7] ZHAO D M,LI H. Approach to network security situational element extraction based on parallel reduction[J]. Journal of Computer Applications,2017,37(4):1008-1013. (in Chinese)
赵冬梅,李红. 基于并行约简的网络安全态势要素提取方法[J]. 计算机应用,2017,37(4):1008-1013.

[8] ZHOU X K. A Kind of Data Clustering Algorithm in Wireless Sensor Network[J]. Control Engineering of China,2016,23(8):1238-1241. (in Chinese)
周修考. 一种用于无线多传感器网络数据聚类算法[J]. 控制工程,2016,23(8):1238-1241.

[9] XU G Q,ZHOU L R. Research on an Intelligent Algorithm for Public Network Attack Data Mining[J]. Computer Measurement & Control,2016,24(10):190-193. (in Chinese)
余国清,周兰蓉. 一种公共网络攻击数据挖掘智能算法研究[J]. 计算机测量与控制,2016,24(10):190-193.

[10] KAUBA C,UHL A. Fingerprint recognition under the influence of image sensor ageing[J]. Iet Biometrics,2017,6(4):245-255.

[11] NI Y,LIU J,LIU S,et al. An Indoor Pedestrian Positioning Method Using HMM with a Fuzzy Pattern Recognition Algorithm in a WLAN Fingerprint System[J]. Sensors,2016,16(9):1447-1501.

[12] ZHANG Q,YIN Y,YANG G. Unmatched minutiae:Useful information to boost fingerprint recognition[J]. Neurocomputing,2016,171(35):1401-1413.

[13] MARASCO E,ROSS A. A Survey on Antispoofing Schemes for Fingerprint Recognition Systems[J]. Acm Computing Surveys,2015,47(2):1-36.

[14] XU Z Y,TANG G W,JIANG X L,et al. Research of a hardware-friendly synthetic fingerprint discrimination algorithm[J]. Application of Electronic Technique,2016,42(10):54-57. (in Chinese)
徐智勇,唐根伟,姜新泉,等. 硬件友好型合成指纹鉴别算法的研究[J]. 电子技术应用,2016,42(10):54-57.

[15] SHI J P,WU Y Q. A fingerprint minutiae matching algorithm based on chaotic bee colony optimization[J]. CAAI Transactions on Intelligent Systems,2016,11(5):613-618. (in Chinese)
史骏鹏,吴一全. 基于混沌蜂群优化的指纹匹配算法[J]. 智能系统学报,2016,11(5):613-618.

[16] ZHAN X S,CAI L Y. Fingerprint Enhancement Algorithm Based on Two-Dimensional Sine Quadric Surface Filter Modulated by Gaussian Function[J]. Journal of Data Acquisition & Processing,2017,32(1):62-70. (in Chinese)
詹小四,蔡乐毅. 基于高斯调制二维正弦曲面滤波器的指纹增强算法[J]. 数据采集与处理,2017,32(1):62-70.

[17] GUPTA P,GUPTA P. An accurate fingerprint orientation modeling algorithm[J]. Applied Mathematical Modelling,2016,40(15/16):7182-7194.

[18] WANG X X,YANG H C. Multiplex Biometric Verification System Based on Fingerprint and Face[J]. Journal of Chongqing University of Technology(Natural Science),2013,27(7):67-70. (in Chinese)
王小雪,杨会成. 融合指纹和人脸的生物特征身份认证方法[J]. 重庆理工大学学报(自然科学),2013,27(7):67-70.

[19] LIU H Y,MA J H,HUANG Q. Construction method of fingerprint database based on improved Kriging interpolation for indoor location[J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition),2017,29(6):751-757. (in Chinese)
刘辉元,马金辉,黄琼. 基于改进克里金插值的室内定位位置指纹库构建方法[J]. 重庆邮电大学学报(自然科学版),2017,29(6):751-757.