基于多传感器信息融合的用户认证方法

刘乐乐，周治平

江南大学物联网技术应用教育部工程研究中心，江苏 无锡 214122

摘要 为了保证智能手机的信息安全，提出一种多传感器信息融合的手机用户身份认证方法。首先从手机用户操作手势的姿态角变化、运动幅度以及旋转程度等方面提取信号特征，然后分别以三类单特征的动态时间规整识别结果作为独立证据构造基本概率分配函数，进而采用 Dempster/Shafer 证据理论对其进行融合。为缓解证据间出现的冲突，避免其影响融合效果，引入加权证据方法。通过计算各证据之间的相似性来衡量证据间的冲突程度进而确定各证据的可信度，并且对各证据进行加权修正以降低可信度小的证据对融合结果的影响，最后根据融合结果做出决策。仿真结果表明，该算法性能优于对比算法，能有效对手机用户进行身份识别。

关键词 测量；传感器；信号特征；信息融合；证据理论；冲突

中图分类号 TN87；TP29 **文献标识码** A

doi：10.3788/LOP54.071204

User Authentication Scheme Based on Multi-Sensor Information Fusion

Liu Lele, Zhou Zhiping

Engineering Research Center of Internet of Things Technology Applications, Ministry of Education, Jiangnan University, Wuxi, Jiangsu 214122, *China*

Abstract In order to guarantee the information security of the mobile phone, a user identity authentication scheme based on multi-sensor information fusion is proposed. Firstly, the signal features are extracted from the attitude angle changes, range of motion, and the rotation degree of user′s gesture. Then the dynamic time warping(DTW) recognition results of each single feature are used as independent evidence to construct the basic probability distribution function, respectively. And the Dempster/Shafer evidence theory is used for decision fusion. Also, a weighted evidence method is introduced in this work to alleviate conflict among the evidences, which can avoid the negative impact of this phenomenon. The conflict degrees between each pair of evidences are measured by calculating the similarity between them, by which the evidence credibility is determined. Afterwards, the evidence weights are revised to depress the negative effects of the evidences with low credibility when making the fusion process. Hence the final decision can be made according to the fusion result. The simulation results show that the performance of the proposed algorithm is better than the compared algorithms, which can effectively recognize the user′s identity of mobile phone.

Key words measurement; sensor; signal characteristics; information fusion; evidence theory; conflict

OCIS codes 120.3930; 150.4232

1 引 言

基于智能手机传感器的身份认证是现阶段新兴的生物特征识别方式，和传统生物特征(指纹[1]、虹膜[2]、人脸[3]等)识别方式相比，更易于感知。目前，利用手机加速度传感器实现用户身份认证已被应用于多个领

收稿日期：2017-02-13；**收到修改稿日期**：2017-03-11

基金项目：中央高校基本科研业务费用专项资金(JUSRP51510)

作者简介：刘乐乐(1988—)，男，硕士研究生，主要从事信息处理与多数据融合方面的研究。E-mail：6141918006@vip.jiangnan.edu.cn

导师简介：周治平(1962—)，男，博士，教授，主要从事检测技术和自动化装置方面的研究。E-mail：zzp@jiangnan.edu.cn

域，如通过三轴加速度传感器进行的步态身份认证[4-6]。Guna 等[7]将多个手势的加速度特征组合成一个手势模板进行用户身份认证判别。高焕芝等[8]利用智能手机自身的加速度传感器，获取用户操作手机过程中的多种运动信息作为生物特征量进行身份认证。Guerra-Casanova 等[9-10]提出将智能手机内置加速度传感器实时采集的用户动态手势加速度信号作为行为特征量，利用时序加速度信号进行匹配认证。

上述基于移动终端内置运动传感器的身份认证方案均采用单一的三轴加速度传感器，但采用单一的三轴加速度传感器较难准确反映移动终端的运动，进而影响用户识别的效果。Feng 等[11]利用手机加速度传感器、陀螺仪传感器以及磁力传感器采集用户日常接听电话数据，将运动轨迹位置变化率作为生物特征量对用户身份进行识别。Conti 等[12]利用多个手机传感器收集用户日常接听电话数据对用户进行身份识别。但其只针对原始的手势信号进行分析，没有提取手势的任何特征，因而不能较好地反映出用户在接听电话过程中的动作特征信息。Zhu 等[13]根据用户接听电话及操作手机的特定习惯提出一种新的用户识别框架，但是该方法识别等错率(EER)高达 13%，限制了其实际应用能力。Li 等[14]利用多个传感器获取人体行为信息，采用 Dempster/Shafer(DS)证据理论对行为信息进行融合。但是当各证据存在高冲突时，采用该方法易出现最终决策结果与实际常理相悖的情况。

针对上述方法不能较好反映手势动作特征信息以及采用 DS 证据理论融合各证据时易出现冲突从而影响融合效果等问题，本文从手机用户操作手势的姿态角变化、运动幅度以及旋转程度三个方面提取特征来全面反映用户的行为特点，并对各特征进行初步判断；其次利用 DS 证据理论对各特征初步判断的结果进行融合时，引入加权证据方法对各证据进行修正，以降低冲突证据对融合结果的影响，提高算法的认证精度。

2 系统处理流程

2.1 系统识别原理

利用智能手机内置加速度传感器以及陀螺仪传感器获得用户接听电话手势的三维数据，采集数据时以用户滑动接听电话按钮作为开始，利用分布在手机听筒两侧的内置距离感应器，听筒接触到人体耳部时作为采集数据的结束。用户在模拟接听电话时按照规定手势执行。模拟过程中，各用户均为静止状态。文献[11-13]通过分析用户在接听电话的过程中形成的三维曲线，表明其曲线的曲率由用户手臂长度、上肢形态共同决定。由于生物个体的生理结构及行为习惯具有较大差异，不同人在接听电话过程中也会存在较大的差异，所以此过程具有唯一性。

图 1 为同一用户与 4 个不同用户接听电话过程中陀螺仪传感器三轴数据的变化曲线。从图中可以看出同一用户在接听电话过程中手势之间各传感器数据波形基本相似，而不同用户之间手势差异较大。故可将用户接听电话动态手势作为一种生物特征，用于身份认证。

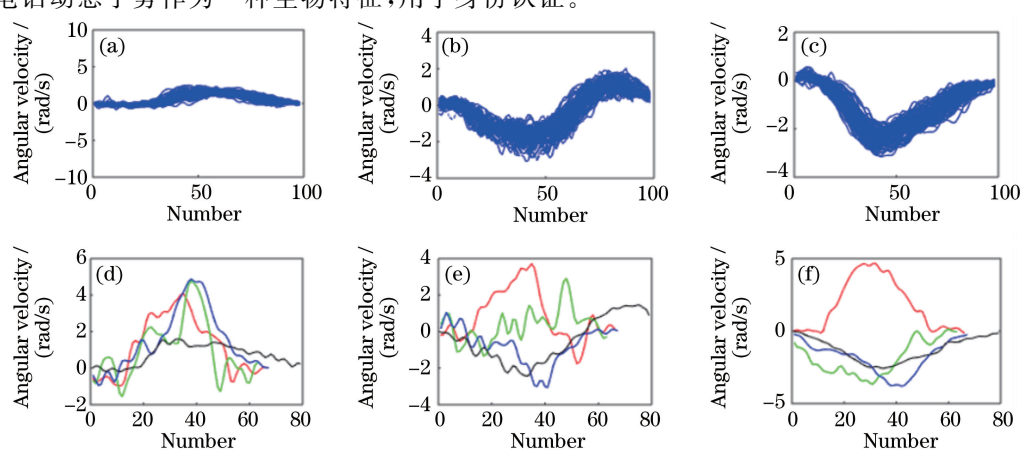

图 1 陀螺仪传感器三轴数据变化曲线。同一用户在(a) X 轴；(b) Y 轴；(c) Z 轴方向的 100 个重复手势与 4 个不同用户在(d) X 轴；(e) Y 轴；(f) Z 轴方向的手势

Fig. 1 Curves of three-axis gyro sensor data. 100 repetitive gestures of the one user in (a) X-axis; (b) Y-axis; (c) Z-axis and gestures of 4 different users in (d) X-axis; (e) Y-axis; (f) Z-axis

2.2 特征向量提取

为了有效地对用户进行识别,需要对手势传感器数据进行平滑处理,以减少工频噪声的污染和手部肌肉震颤产生的干扰。本文选取特征包括:运动幅度特征、姿态角特征、旋转程度特征。

1) 运动幅度特征:传感器坐标系以及坐标量的大小会随着手臂的运动而改变,采用单一轴的数据不能合理表明手臂的运动剧烈程度,为此,将加速度传感器三轴数据合为 A,可以表示为

$$A=\sqrt{a_x^2+a_y^2+a_z^2}。\tag{1}$$

2) 姿态角特征:姿态角反映的是用户在接听电话过程中手臂在空间旋转角度的变化,其特征表示为 $\phi=(\theta,\gamma,\varphi)$,横滚角 θ 及俯仰角 γ 分别表示为

$$\theta=\arcsin a_x,\tag{2}$$

$$\gamma=\arcsin\left(\frac{a_y}{g\cos\theta}\right)。\tag{3}$$

结合 θ 和 γ 可以由陀螺仪传感器的输出计算得到航向角 φ 为

$$\varphi=\arctan\frac{g_y\cos\gamma+g_z\sin\gamma}{g_x\cos\theta+g_y\sin\theta\sin\gamma-g_z\cos\theta\sin\gamma},\tag{4}$$

式中,g_x,g_y,g_z 分别为陀螺仪传感器的 X、Y、Z 轴测量值。

3) 旋转程度特征:为表征用户在接听电话过程中手臂旋转幅度,引入旋转程度特征 G,可以表示为

$$G=\sqrt{g_x^2+g_y^2+g_z^2}。\tag{5}$$

3 识别算法设计

在针对不同用户手势传感器信号进行相似度比较时,利用动态时间规整(DTW)算法对不等长时间序列进行弯曲规整从而解决手势信号序列长度不一致的问题。为了简单和方便处理,本文采用基于欧氏距离的DTW 算法对两个手势信号序列进行比较,进而得到度量两个手势信号序列差距的分值。

3.1 DS 证据理论

DS 证据理论依据所构造的信度函数解决决策信息中不完备的问题,设 Θ 为识别框架,$A\subseteq\Theta$。定义集函数 $m:2^{\Theta}\to[0,1]$,满足 $\sum_{A\subset\Theta}m(A)=1$,$m(\varnothing)=0$。$m(A)$为命题 A 的基本概率分配函数(BPA),表示证据支持 A 的信任度。设 $m_1,m_2,\cdots,m_n$ 是识别框架 Θ 上不同证据的 BPA,则 $m=m_1\oplus m_2\cdots\oplus m_n$,可利用 Dempster 组合规则将多个证据组合起来得到证据的融合结果,合成表达式为

$$\begin{cases}m(\varnothing)=0\\ m(A)=\dfrac{1}{1-k}\displaystyle\sum_{\cap A_i=A}\prod_{j=1}^{n}m_j(A_i),A\neq\varnothing\end{cases},\tag{6}$$

式中,冲突系数 k 表示证据间冲突程度,即 $k=\sum_{\cap A_i=\varnothing}\prod_{j=1}^{n}m_j(A_i)$。

3.2 基于相似性测度的证据冲突衡量方法

当 $k\to1$,即证据高度冲突时,利用(6)式对多个证据合成可能会导致与实际常理相悖的结果。为避免此问题,本文引入 Tanimoto 测度计算各证据之间的相似性,以衡量证据间的冲突程度。基本概率分配函数分别为 m_1 和 m_2 的两证据之间的相似性表示为

$$s(m_1,m_2)=\frac{\sum_{i=1}^{n}m_1(A_i)\cdot m_2(A_i)}{\sum_{i=1}^{n}m_1(A_i)^2+\sum_{i=1}^{n}m_2(A_i)^2-\sum_{i=1}^{n}m_1(A_i)\cdot m_2(A_i)}。\tag{7}$$

相似性 s 的取值范围为[0,1],其值越大表明两个证据相似度越大,证据间的冲突越小。文献[15]将向量空间引入证据理论,提出 Jousselme 距离表征证据之间的冲突程度,在辨识框架 Θ 下,两个证据的基本概率分配函数 m_1 和 m_2 之间的距离为

$$d(m_1,m_2)=\sqrt{\frac{1}{2}(\|\boldsymbol{m}_1\|^2+\|\boldsymbol{m}_2\|^2-2\langle\boldsymbol{m}_1,\boldsymbol{m}_2\rangle)}\ , \tag{8}$$

式中，$\langle\boldsymbol{m}_1,\boldsymbol{m}_2\rangle=\sum_{i=1}^{n}\sum_{j=1}^{n}m_1(A_i)m_2(A_j)\frac{|A_i\cap A_j|}{|A_i\cup A_j|}$，且 $A_i,A_j\in 2^{\Theta},i,j=1,\cdots,n$。

两证据之间的距离 d 越大，说明其冲突越大。为比较所引入的相似性测度 s 与冲突系数 k 以及证据距离 d 表征两证据之间冲突程度的优劣，现采用文献[15]中的例证进行说明。设辨识框架 $\Theta=\{1,2,\cdots,20\}$，有两个基本概率赋值为：$m_1=(2,3,4)=0.05$，$m_1(7)=0.05$，$m_1(\Theta)=0.1$，$m_1(\mathrm{A})=0.8$，$m_2(1,2,3,4,5)=1$。集合 A 从{1}开始，依次增加一个元素直到全集 Θ。图 2 显示了冲突系数 k、证据相似性测度 s 以及证据距离 d 随着子集 A 变化而变化的情况。

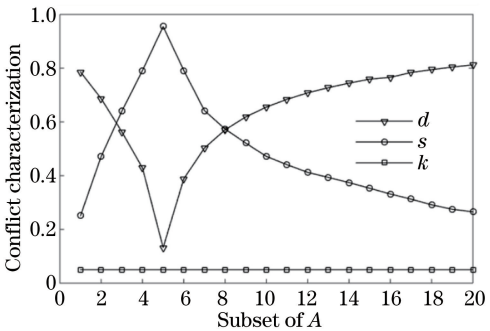

图 2 证据冲突衡量的变化趋势

Fig. 2 Trends in the measurement of evidence conflict

如图 2 所示，证据距离 d 与相似性测度 s 的曲线正好相反，即证据距离 d 大时，相似性测度 s 小。这是因为，证据距离 d 大反映证据间冲突大，而相似性测度 s 小则反映两个证据之间相似性小，证据间冲突大。从曲线可以看出，d 与 s 的值表征的证据间冲突程度的变化趋势一致。冲突系数 k 的值在变化过程中保持不变，不符合常理。在计算复杂度方面，文献[15]通过(8)式计算两证据之间的距离，在构造对角矩阵时计算复杂度较高，其时间复杂度为 $O(n^2)$。由(7)式可知该方法时间复杂度为 $O(n)$，明显优于文献[15]，对于 n 取值较大的情况能够较大程度地减少时间开销。

4 DTW-DS 信息融合认证模型

在手势认证中，特征 A、特征 ϕ、特征 G 三个特征之间相互独立，可以利用 DS 理论组合融合来自不同特征的 DTW 认证信息。利用 DTW 对单特征进行识别，输出为两手势序列的相似性测度而不是概率输出，不能作为证据理论的 BPA。本文采用各证据在比值区间内检测概率的方式进行概率建模。设个体特性识别框架为 $\Theta=\{\omega_{\mathrm{true}},\omega_{\mathrm{false}}\}$，其中 Θ 的幂集为 $2^{\Theta}=\{\{\omega_{\mathrm{true}}\},\{\omega_{\mathrm{false}}\},\{\omega_{\mathrm{true}},\omega_{\mathrm{false}}\}\}$，$\omega_{\mathrm{true}}$ 表示判别结果为真实用户，ω_{false} 表示判别结果为入侵用户。以各证据在比值区间内检测概率作为基本概率分配函数，设似然矩阵为

$$\begin{cases}P(\omega_A\,|\,X)=[p(\omega_{A\mathrm{t}}\,|\,X),\ p(\omega_{A_{\mathrm{f}}}\,|\,X)]\\ P(\omega_G\,|\,X)=[p(\omega_{G\mathrm{t}}\,|\,X),\ p(\omega_{G_{\mathrm{f}}}\,|\,X)]\\ P(\omega_{\phi}\,|\,X)=[p(\omega_{\varphi\mathrm{t}}\,|\,X),\ p(\omega_{\varphi_{\mathrm{f}}}\,|\,X)]\end{cases}, \tag{9}$$

其表示测试手势经特征 A，G 以及特征 ϕ 分类为真实用户和入侵用户的概率分布，X 为某一比值区间。设 m_1，m_2 和 m_3 分别表示基于特征 A，G 以及 ϕ 证据的 BPA，有

$$\begin{cases}m_1(\omega_{\mathrm{true}})=p(\omega_{A\mathrm{t}}\,|\,X),\ m_1(\omega_{\mathrm{false}})=p(\omega_{A\mathrm{f}}\,|\,X)\\ m_2(\omega_{\mathrm{true}})=p(\omega_{G\mathrm{t}}\,|\,X),\ m_2(\omega_{\mathrm{false}})=p(\omega_{G\mathrm{f}}\,|\,X)\\ m_3(\omega_{\mathrm{true}})=p(\omega_{\varphi\mathrm{t}}\,|\,X),\ m_3(\omega_{\mathrm{false}})=p(\omega_{\varphi\mathrm{f}}\,|\,X)\\ m_1(\Theta)=m_2(\Theta)=m_3(\Theta)=0\end{cases}。 \tag{10}$$

进一步构建加权证据的融合方法如下：

1) 根据(7)式计算基本概率分配函数为 m_1 和 m_2 的两证据的相似性测度。获得各证据两两间的相似性测度后，可构建一个 $n\times n$ 的相似度矩阵

$$\boldsymbol{S}=\begin{bmatrix} 1 & s(m_1,m_2) & \cdots & s(m_1,m_n) \\ s(m_2,m_1) & 1 & \cdots & s(m_2,m_n) \\ \vdots & \vdots & & \vdots \\ s(m_n,m_1) & s(m_n,m_2) & \cdots & 1 \end{bmatrix}。 \tag{11}$$

2) 确定各证据的可信度，其他所有证据对证据 i 的支持度为

$$V_{\mathrm{Sup}}(m_i)=\sum_{j=1,j\neq i}^{n} s(m_i,m_j),\ i=1,2,\cdots,n。 \tag{12}$$

3) 将各证据的支持度归一化可得到证据的可信度，证据 i 的可信度为：

$$V_{\mathrm{Cred}\_i}=\frac{V_{\mathrm{Sup}}(m_i)}{\max\limits_{1\leqslant i\leqslant n}\left[V_{\mathrm{Sup}}(m_i)\right]}。 \tag{13}$$

4) 修正证据，将证据 i 的可信度 V_{Cred_i} 作为它的权重 β_i，对其基本概率分配函数 m_i 进行加权修正，得到新的基本概率分配函数为

$$m'_i(A_i)=\beta_i m_i(A_i),\ A_i\neq\Theta, \tag{14}$$

$$m'_i(\Theta)=\beta_i m_i(\Theta)+(1-\beta_i)。 \tag{15}$$

5) 利用 Dempster 组合规则获取组合证据融合概率函数值 $m(\omega_{\mathrm{true}})$ 及 $m(\omega_{\mathrm{false}})$，最终的决策结果为信任度最大的命题。

5 仿真结果与分析

5.1 仿真设置

5.1.1 仿真环境及数据获取

实验样机选用 Galaxy S5 型号 SMG9008 手机，主频 2.5 GHz，随机存取存储器为 2 GB，搭载 Android 4.4.2版本，采样频率通过程序设置为 50 Hz。仿真数据库由 8 名用户(男性 5 名，女性 3 名)参与完成，数据库创建过程中每位用户按规定模拟接听电话动态手势，平均每天采集 10 次，共模拟 3 个月通话，此时每位用户可采集数据 900 组，共收集到 7200 组数据。对样本数据处理以 Matlab 2014b 作为仿真平台，在 2.60 GHz 主频 4 G 内存的计算机上完成。

5.1.2 参数设置

用户首先按规定执行 4 次接听电话手势并对手势进行特征提取，完成认证模板注册。对其中两组模板数据采用基于欧式距离的 DTW 算法得到度量其差距的分值，可求得 6 次差距分值的平均分值，记为 μ_1。对于测试手势，将其与 4 组认证模板数据分别进行比较，得到 4 个度量手势差距的分值的平均值，记为 μ_2。由匹配分值 $\psi=\mu_2/\mu_1$ 判别是否为同一个人。若匹配分值小于认证阈值 ϑ，则识别为真实用户；否则识别为入侵用户。

阈值 ϑ 取值大小对认证结果的影响较大，若该值较大，则错误拒绝率(FRR)较低，但错误接受率(FAR)较高。本文选取 EER 作为确定阈值的指标，对阈值 ϑ 进行优化设置。8 位用户中依次选取每位用户各自数据中的 200 组数据作为真实数据，其余用户各 100 组数据作为入侵数据，分别求出每个特征在不同阈值下的 FRR 和 FAR，当 FRR 和 FAR 值相等时(即 EER)所对应的阈值即为所认证阈值的取值。其中各特征阈值设置范围及变化步长设置如下：特征 A、特征 G 的阈值下限和上限相同，分别为 1.6、1.8，特征 ϕ 的阈值下限和上限为 2.0、2.2，三个特征的阈值变化步长为 0.005。所提取三个特征的 FRR 和 FAR 取值相等时，所对应的阈值如表 1 所示。

表 1 中 8 位用户，特征 A、特征 G、特征 ϕ 的认证阈值及 ERR 取值没有明显差异，且其对应的标准差也较小。各认证阈值及 EER 在对应均值附近波动较小，因此可以分别求出三种特征下阈值的均值作为 8 位用户整体的阈值设置，其分别为 1.73、1.69、2.04。

表 1 特征阈值统计

Table 1 Feature threshold statistics

User	Feature A		Feature G		Feature ϕ	
	Threshold	EER	Threshold	EER	Threshold	EER
1	1.72	9.56	1.67	10.78	2.09	5.87
2	1.70	9.51	1.71	10.82	2.10	5.88
3	1.76	9.50	1.69	10.81	2.01	5.87
4	1.74	9.55	1.71	10.84	2.02	5.80
5	1.69	9.54	1.69	10.77	2.05	5.87
6	1.77	9.61	1.67	10.84	2.02	5.88
7	1.75	9.58	1.70	10.79	2.02	5.90
8	1.73	9.56	1.68	10.81	2.04	5.86
Mean	1.73	9.55	1.69	10.81	2.04	5.87
Standard deviation	0.03	0.04	0.02	0.03	0.03	0.03

5.1.3 概率分布函数的获取

选取每位用户各自数据中的 200 组数据作为训练样本集，将其中一位用户的数据作为真实用户数据，剩余 7 位用户作为入侵用户，包含 1400 组数据，以此类推，确定各特征对应的概率分布函数。特征 A 经过 DTW 方法初步判断后得到匹配分值 ψ_A，根据匹配分值空间分布，将 ψ_A 划分为多个区间，以各区间内真实用户的概率值以及入侵用户的概率值作为特征 A 对应的概率分布函数，如表 2 所示。同理亦可得到特征 G 以及特征 ϕ 的概率分布函数，此处不再一一列举。

表 2 特征 A 对应的概率分布函数

Table 2 Probability distribution function of feature A

ψ_A interval	m_1 (true)	m_1 (false)	ψ_A interval	m_1 (true)	m_1 (false)
[0.0,1.5)	0.8577	0.1423	[1.8,1.9)	0.4545	0.5455
[1.5,1.6)	0.7364	0.2636	[1.9,2.0)	0.2143	0.7857
[1.6,1.7)	0.6636	0.3364	[2.0,2.1)	0.0833	0.9167
[1.7,1.8)	0.5467	0.4533	[2.1,+∞)	0.0320	0.9680

5.2 仿真结果分析

从采集的 7200 组手势数据中除去 1600 组训练样本集，以其余 5600 组数据作为测试样本集。对测试数据基于各特征的判断结果使用 DS 进行融合，通过相似性测度来衡量证据间的冲突程度，对各证据的基本概率分配函数加以修正。以某一组实际为本人接听电话行为的测试数据为例，修正前特征 A、特征 ϕ 通过 DTW 方法进行初步判断为真实用户的基本概率分别为 0.6636、0.8407，特征 G 初步判断为入侵用户的基本概率为 0.9366。特征 G 与特征 A、特征 ϕ 两个证据之间冲突较大。利用 DS 组合规则对三个特征进行融合，最终得到的检测结果为入侵用户，与实际结果相悖。经过证据加权修正后的基本概率分配函数，特征 A、G、ϕ 对应的可信度分别为 1、0.3835、0.8483，其中证据 G 可信度最小。经过修正，证据 G 所提供的确定性信息减少，不确定信息增加，利用 Dempster 组合规则进行融合，结果为真实用户，与实际相符。

为验证所提方法的有效性和优越性，针对 5600 组测试样本，所提方法与采用 DTW 方法对单一特征进行识别、文献[14]中 DS 融合算法以及文献[16]Jousselme 作为证据之间距离的融合方法进行分析比较，如表 3 所示。

由表 3 可知，对不同用户的识别，文献[14]采用 DS 融合方法，其识别精度优于单一特征识别精度。所提算法的 FRR 和 FAR 均值分别为 3.21%和 1.98%，优于文献[14]的 4.01%和 2.64%。这是因为在采用 DS 证据合成过程中，所提算法利用证据加权对各证据进行修正，充分考虑到证据之间的相互支持程度，降低冲突信息对最终融合结果的影响。文献[16]在证据合成过程中亦考虑了每个证据的可信度，故取得较好的识别性能，其 FRR 和 FAR 均值为 3.32%、2.10%，识别精度略低于所提算法。同时可以发现，在 8 个测试样本中，特征 ϕ 性能优于特征 A 和特征 G，表明用户在接听电话过程中，姿态角的变化更能体现用户的个性特征。

表 3 各算法认证精度对比

Table 3 Comparison of authentication accuracy of each algorithm %

User	Feature A		Feature G		Feature ϕ		Literature[14]		Literature[16]		Proposed algorithm	
	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR
1	11.8	9.14	12.03	10.68	6.63	5.12	3.94	2.57	3.36	2.10	3.18	2.29
2	9.10	8.96	14.92	10.73	8.56	5.69	4.39	2.96	3.28	2.88	3.37	2.62
3	13.38	9.86	12.80	9.16	9.69	4.76	3.96	2.17	2.83	1.89	2.82	1.09
4	9.03	8.51	13.34	9.85	9.77	5.85	4.04	3.05	3.28	2.36	3.54	2.53
5	10.68	9.48	11.64	8.26	7.94	6.36	4.11	3.00	2.94	1.02	2.66	1.57
6	11.56	9.79	12.69	10.26	7.02	4.68	3.71	2.16	3.31	2.10	3.22	2.05
7	10.28	9.82	12.13	9.21	6.86	5.22	3.62	2.37	3.29	2.16	3.06	2.00
8	10.05	8.01	13.33	9.79	9.28	5.10	4.31	2.86	4.24	2.26	3.83	1.69
Mean	10.74	9.19	12.86	9.74	8.22	5.35	4.01	2.64	3.32	2.10	3.21	1.98

为了进一步验证所提算法的优势，与文献[11]采用的轨迹重构方法、文献[12]采用的多传感器信息融合算法进行分析比较。在 5600 组测试样本数据下进行实验，在与用户无关的阈值下计算 FRR 和 FAR。图 3 给出了 3 种不同算法的运行曲线(ROC)作为综合评价指标。

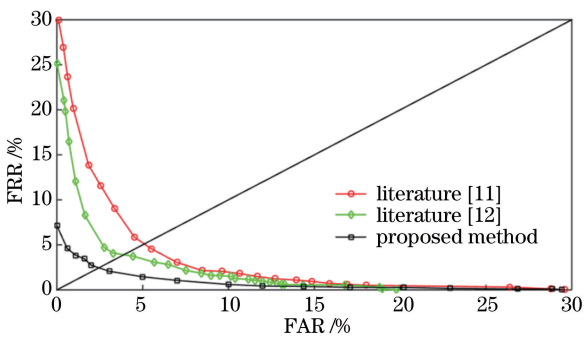

图 3 各算法运行曲线对比

Fig. 3 Comparison of operation curves of each algorithm

图 3 所示的 ROC 曲线中，$y=x$ 直线表示 FAR 与 FRR 相等时各点连线，其与各曲线的交点即为各算法的 EER 值。从图中可直观看出，所提算法的 EER 最小，其值为 2.46%；同时，同一 FAR 值下，所提算法的 FRR 值也最小。各算法在 FAR 达到 0%边界时，文献[11]、文献[12]以及所提算法的 FRR 分别为 29.96%，25.16%，7.13%。与文献[12]采用原始的手势传感器信号相比，所提算法的 FRR 优于文献[12]的 25.16%，EER 优于文献[12]的 3.73%。与文献[11]相比，所提算法的 FRR 和 EER 均优于文献[11]。综上所述，所提算法对于提高系统识别精度更有优势，能有效地保护用户信息的安全。

6 结 论

本文提出一种新的采用生物特征融合的用户身份认证算法。通过提取用户姿态变化、运动幅度以及旋转程度等特征来全面反映用户行为特性，并对各特征进行初步判断；利用 DS 证据理论对各特征初步判断的结果进行融合时，为改善证据间出现冲突时的融合效果，采用加权证据方法对各证据进行修正，降低可信度小的证据对融合结果的影响，从而提高决策精度。仿真结果显示，所提算法在有效防止非真实用户入侵的同时对真实用户有较高识别率，该算法可用于手机身份认证，是一种有效的身份识别方法。

参 考 文 献

[1] Zhou Lu, Chi Yaodan, Guo Liang. Optical system design of object-telecentric dual finger fingerprint scanner[J]. Laser & Optoelectronics Progress, 2016, 53(10): 102201.
周 路, 迟耀丹, 郭 亮. 物方远心双指指纹采集光学系统设计[J]. 激光与光电子学进展, 2016, 53(10): 102201.

[2] Han Min, Peng Yuhua, Zhang Shunli, *et al*. Iris recognition based on empirical mode decomposition[J]. Acta Optica

Sinica, 2010, 30(2): 364-368.
韩 民, 彭玉华, 张顺利, 等. 基于经验模态分解的虹膜识别[J]. 光学学报, 2010, 30(2): 364-368.

[3] Guo Guangming. Research on large-scale face recognition using opto-electronic hybrid matched filtering correlator[J]. Chinese J Lasers, 2013, 40(8): 0809003.
郭广明. 光电混合匹配滤波相关器的大规模人脸识别研究[J]. 中国激光, 2013, 40(8): 0809003.

[4] Ferrero R, Gandino F, Montrucchio B, *et al*. On gait recognition with smartphone accelerometer[C]. MECO, 2015: 368-373.

[5] Nickel C, Busch C, Rangarajan S, *et al*. Using hidden Markov models for accelerometer-based biometric gait recognition[C]. CSPA, 2011: 58-63.

[6] Thang H M, Viet V Q, Thuc N D, *et al*. Gait identification using accelerometer on mobile phone[C]. ICCAIS, 2012: 344-348.

[7] Guna J, Stojmenova E, Lugmayr A, *et al*. User identification approach based on simple gestures[J]. Multimedia Tools and Applications, 2014, 71(1): 179-194.

[8] Gao Huanzhi, Cao Xiulian, Wang Lei, *et al*. An identity authentication method based on dynamic gesture and its application in mobile phone[J]. Chinese Journal of Electronics, 2014, 42(9): 1857-1862.
高焕芝, 曹秀莲, 王 磊, 等. 基于动态手势的身份认证方法及其在智能手机上的应用[J]. 电子学报, 2014, 42(9): 1857-1862.

[9] Guerra-Casanova J, Sánchez-Ávila C, de Santos Sierra A, *et al*. Score optimization and template updating in a biometric technique for authentication in mobiles based on gestures[J]. Journal of Systems and Software, 2011, 84(11): 2013-2021.

[10] Bailador G, Sanchez-Avila C, Guerra-Casanova J, *et al*. Analysis of pattern recognition techniques for in-air signature biometrics[J]. Pattern Recognition, 2011, 44(10): 2468-2478.

[11] Feng T, Zhao X, Shi W. Investigating mobile device picking-up motion as a novel biometric modality[C]. BTAS, 2013: 1-6.

[12] Conti M, Zachia-Zlatea I, Crispo B. Mind how you answer me!: transparently authenticating the user of a smartphone when answering or placing a call[C]. ASIACCS, 2011: 249-259.

[13] Zhu J, Wu P, Wang X, *et al*. Sensec: Mobile security through passive sensing[C]. ICNC, 2013: 1128-1133.

[14] Li W, Bao J, Fu X, *et al*. Human postures recognition based on DS evidence theory and multi-sensor data fusion[C]. CCGRID, 2012: 912-917.

[15] Jousselme A L, Grenier D, Bossé É. A new distance between two bodies of evidence[J]. Information Fusion, 2001, 2(2): 91-101.

[16] Han D, Dezert J, Duan Z. Evaluation of probability trans-formations of belief functions for decision making[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2016, 46(1): 93-108.