



(12) 发明专利

(10) 授权公告号 CN 108428131 B

(45) 授权公告日 2021.08.03

(21) 申请号 201810198430.7

(22) 申请日 2018.03.12

(65) 同一申请的已公布的文献号

申请公布号 CN 108428131 A

(43) 申请公布日 2018.08.21

(73) 专利权人 宁波大学

地址 315211 浙江省宁波市江北区风华路
818号

(72) 发明人 郑紫微 秦闯 季克宇 张鸣

(74) 专利代理机构 宁波诚源专利事务有限公
司 33102

代理人 刘凤钦 孙盼峰

(51) Int.Cl.

G06Q 20/38 (2012.01)

G06Q 20/40 (2012.01)

(56) 对比文件

CN 106709402 A, 2017.05.24

CN 106295770 A, 2017.01.04

CN 107766785 A, 2018.03.06

CN 107239955 A, 2017.10.10

CN 107733919 A, 2018.02.23

CN 106779674 A, 2017.05.31

US 2016275483 A1, 2016.09.22

WO 2005015452 A1, 2005.02.17

US 2013018782 A1, 2013.01.17

陈平顺等. 基于Android的NFC移动支付系统
设计与实现.《数据通信》.2015,

审查员 王琪

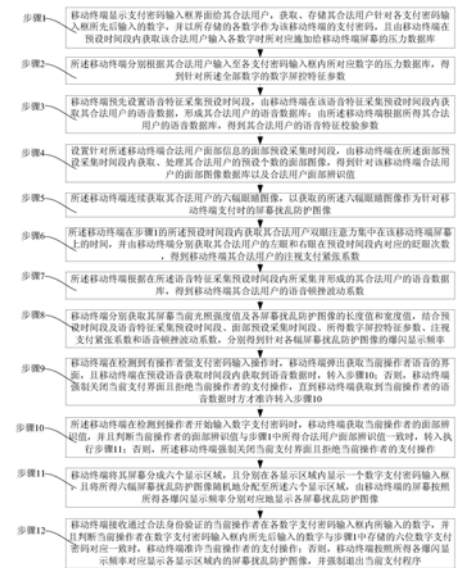
权利要求书3页 说明书10页 附图1页

(54) 发明名称

基于语音秘密信息隐藏的支付方法

(57) 摘要

本发明涉及一种基于语音秘密信息隐藏的支付方法,通过得到移动终端其合法用户的语音顿挫波动系数,将语音顿挫波动系数作为辨识用户合法身份的一个特征,实现了利用语音数据来隐藏用户身份信息的效果;利用移动终端合法用户针对全部数字的数字屏控特征参数、面部辨识值及移动终端合法用户支付操作时的注视支付紧张系数,避免非法者的仿冒支付操作,确保只有验证合法身份的用户操作该移动终端的支付程序,由此在支付操作的初期就起到针对非法者的防范功能,提高支付安全;通过所得针对各幅屏幕扰乱防护图像的爆闪显示频率,使得移动终端屏幕按照对应各各自的爆闪显示频率来显示这些屏幕扰乱防护图像,极大提高移动终端其合法用户的支付信息安全。



1. 基于语音秘密信息隐藏的支付方法, 用于实现移动终端的支付操作, 其特征在于, 包括如下步骤1至步骤12:

步骤1, 移动终端显示支付密码输入框界面给其合法用户, 获取、存储其合法用户针对各支付密码输入框所先后输入的数字, 并以所存储的各数字作为该移动终端的支付密码, 且由移动终端在预设时间段内获取该合法用户输入各数字时所对应施加给该移动终端屏幕的压力数据库;

其中, 所述支付密码输入框界面中包括有六个支付密码输入框; 所述六个支付密码输入框中的第 m 个支付密码输入框标记为 Inputbox_m , 移动终端合法用户针对支付密码输入框 Inputbox_m 所输入的数字为 $D_m, m=1, 2, \dots, 6$; 所述预设时间段标记为 T_1 , 移动终端合法用户输入数字 D_m 时所对应施加给移动终端屏幕的压力数据库标记为 $F_{D_m}; F_{D_m} = \{f_{D_{m,n}}\}, n=1, 2, \dots, N$; 压力数据库 F_{D_m} 内具有 N 个针对移动终端屏幕的压力数据, $f_{D_{m,n}}$ 表示压力数据库 F_{D_m} 内的第 n 个施加给移动终端屏幕的压力数据;

步骤2, 所述移动终端分别根据其合法用户输入至各支付密码输入框内所对应数字的压力数据库, 得到针对全部数字的数字屏控特征参数; 其中, 针对全部数字的数字屏控特征参数标记为 ψ :

$$\psi = \frac{\sin\left(\sum_{m=1}^5 \sum_{n=1}^{N-1} \left(\frac{f_{D_{m+1,n+1}}}{f_{D_{m,n}}}\right)\right)}{\left[\frac{\min(f_{D_{m,n}}, f_{D_{5,N}})}{\max(f_{D_{m,n}}, f_{D_{5,N}})}\right]};$$

其中, $\min(f_{D_{m,n}}, f_{D_{5,N}})$ 表示施加给移动终端屏幕的压力数据 $f_{D_{5,N}}$ 与所有压力数据 $f_{D_{m,n}}$ 中的最小值, $\max(f_{D_{m,n}}, f_{D_{5,N}})$ 表示施加给移动终端屏幕的压力数据 $f_{D_{5,N}}$ 与所有压力数据 $f_{D_{m,n}}$ 中的最大值;

步骤3, 所述移动终端预先设置语音特征采集预设时间段, 由移动终端在该语音特征采集预设时间段内获取其合法用户的语音数据, 形成其合法用户的语音数据库; 由所述移动终端根据所得其合法用户的语音数据库, 得到其合法用户的语音特征校验参数; 其中, 所述语音特征采集预设时间段标记为 T_2 , 移动终端其合法用户的语音数据库标记为 $\text{Voice}_{\text{User}}$, $\text{Voice}_{\text{User}} = \{\text{voice}_{\text{User},k}\}, k=1, 2, \dots, K$; 语音数据库 $\text{Voice}_{\text{User}}$ 内具有 K 个语音数据, $\text{voice}_{\text{User},k}$ 表示语音数据库 $\text{Voice}_{\text{User}}$ 内的第 k 个语音数据; 语音数据 $\text{voice}_{\text{User},k}$ 的振幅标记为 $A_{\text{voice}_{\text{User},k}}$; 所述移动终端其合法用户的语音特征校验参数标记为 κ :

$$\kappa = \sqrt{\sum_{k=1}^K \left(A_{\text{voice}_{\text{User},k}}^2 - \frac{\text{mid}(A_{\text{voice}_{\text{User}}})}{K} \right)^2};$$

其中, $\text{mid}(A_{\text{voice}_{\text{User}}})$ 表示移动终端其合法用户的所有语音数据振幅数值中的数值中间值;

步骤4, 设置针对所述移动终端合法用户面部信息的面部预设采集时间段, 由移动终端

在所述面部预设采集时间段内获取、处理其合法用户的面部预设个数的面部图像,得到针对该移动终端合法用户的面部图像数据库以及合法用户面部辨识值;

其中,所述面部预设采集时间段标记为 T_3 ,针对移动终端合法用户面部图像的预设个数标记为 S ,所述移动终端合法用户的面部图像数据库标记为 $\text{Face}_{\text{User}}$,所述移动终端合法用户的面部图像数据库 $\text{Face}_{\text{User}}$ 内的第 s 个面部图像标记为 $\text{Jpg}_{\text{User},s}$, $1 \leq s \leq S$;所述移动终端合法用户面部辨识值标记为 θ_{Face} :

$$\theta_{\text{Face}} = \frac{\sum_{s=1}^S (L_{\text{Face},s} - \sigma_{L_{\text{Face}}})}{\sum_{s=1}^S (W_{\text{Face},s} - \sigma_{W_{\text{Face}}})} \cdot \frac{\sigma_{L_{\text{Face}}}}{\sigma_{W_{\text{Face}}}};$$

$$\sigma_{L_{\text{Face}}} = \sqrt{\frac{1}{S} \sum_{s=1}^S (L_{\text{Face},s} - \overline{L_{\text{Face}}})^2}, \quad \sigma_{W_{\text{Face}}} = \sqrt{\frac{1}{S} \sum_{s=1}^S (W_{\text{Face},s} - \overline{W_{\text{Face}}})^2};$$

$$\overline{L_{\text{Face}}} = \frac{1}{S} \sum_{s=1}^S L_{\text{Face},s}, \quad \overline{W_{\text{Face}}} = \frac{1}{S} \sum_{s=1}^S W_{\text{Face},s};$$

其中, $L_{\text{Face},s}$ 表示面部图像 $\text{Jpg}_{\text{User},s}$ 的长度值, $W_{\text{Face},s}$ 表示面部图像 $\text{Jpg}_{\text{User},s}$ 的宽度值;

步骤5,所述移动终端连续获取其合法用户的六幅眼睛图像,以获取的所述六幅眼睛图像作为针对移动终端支付时的屏幕扰乱防护图像;

其中,在移动终端屏幕上,按照从左至右的顺序,所获取移动终端其合法用户的眼睛图像标记 $\text{Jpg}_{\text{Eye},m}$;针对移动终端支付时的屏幕扰乱防护图像标记为 $\text{Jpg}_{\text{Protect},m}$, $m=1,2,\dots,6$;

步骤6,所述移动终端在步骤1的所述预设时间段内获取其合法用户双眼注意力集中在该移动终端屏幕上的时间,并由移动终端分别获取其合法用户的左眼和右眼在预设时间段内对应的眨眼次数,得到移动终端其合法用户的注视支付紧张系数;

其中,所述移动终端其合法用户双眼注意力集中在该移动终端屏幕上的时间标记为 T_4 ,所述移动终端其合法用户的左眼在预设时间段内的眨眼次数标记为 C_{left} ,所述移动终端其合法用户的右眼在预设时间段内的眨眼次数标记为 C_{right} ,所述移动终端其合法用户的注视支付紧张系数标记为 Ω :

$$\Omega = \left| \frac{C_{\text{left}} - C_{\text{right}}}{C_{\text{left}} \cdot C_{\text{right}}} \cdot \sin \left(\frac{C_{\text{left}}}{T_1 - T_4} + \frac{C_{\text{right}}}{T_1 - T_4} \right) \right|; \text{其中}, T_1 \text{表示所述预设时间段};$$

步骤7,所述移动终端根据在所述语音特征采集预设时间段内所采集并形成的其合法用户的语音数据库,得到移动终端其合法用户的语音顿挫波动系数;其中,所述语音顿挫波动系数标记为 ρ :

$$\rho = \frac{\sqrt{\frac{1}{K} \sum_{k=1}^K (A_{\text{voice}_{\text{User},k}} - \overline{A_{\text{voice}_{\text{User}}})^2}}}{T_2 \cdot \text{mid}(A_{\text{voice}_{\text{User}}})}, \quad \overline{A_{\text{voice}_{\text{User}}}} = \frac{1}{K} \sum_{k=1}^K A_{\text{voice}_{\text{User},k}};$$

其中, T_2 表示所述语音特征采集预设时间段;

步骤8,所述移动终端分别获取其屏幕当前光照强度值以及各屏幕扰乱防护图像的长度值和宽度值,并结合预设时间段以及语音特征采集预设时间段、面部预设采集时间段、所

得数字屏控特征参数、注视支付紧张系数和语音顿挫波动系数,分别得到针对各幅屏幕扰乱防护图像的爆闪显示频率;

其中,所述屏幕扰乱防护图像 $Jpg_{Protect,m}$ 的长度值和宽度值分别对应标记为 $L_{Jpg_{Protect,m}}$ 和 $W_{Jpg_{Protect,m}}$;所述屏幕扰乱防护图像 $Jpg_{Protect,m}$ 的爆闪显示频率标记为 $\xi_{Jpg_{Protect,m}}$:

$$\xi_{Jpg_{Protect,m}} = \frac{Light_{Screen}^2}{L_{Jpg_{Protect,m}} \cdot W_{Jpg_{Protect,m}}} \cdot \frac{\max(L_{Jpg_{Protect,m}}, W_{Jpg_{Protect,m}})}{\min(L_{Jpg_{Protect,m}}, W_{Jpg_{Protect,m}})} \cdot \frac{|T_1 - T_2| \cdot \Omega \cdot \rho}{|T_1 - T_3| \cdot \psi};$$

其中, $\max(L_{Jpg_{Protect,m}}, W_{Jpg_{Protect,m}})$ 表示数值 $L_{Jpg_{Protect,m}}$ 和数值 $W_{Jpg_{Protect,m}}$ 的最大值; $\min(L_{Jpg_{Protect,m}}, W_{Jpg_{Protect,m}})$ 表示数值 $L_{Jpg_{Protect,m}}$ 和数值 $W_{Jpg_{Protect,m}}$ 的最小值;

步骤9,所述移动终端在检测到有操作者做支付密码输入操作时,移动终端弹出获取当前操作者语音的界面,且移动终端在预设语音获取时间段内获取到语音数据时,转入步骤10;否则,所述移动终端强制关闭当前支付界面且拒绝当前操作者的支付操作,直到移动终端获取到当前操作者的语音数据时方才准许转入步骤10;

步骤10,所述移动终端在检测到操作者开始输入数字支付密码时,移动终端获取当前操作者的面部辨识值,并且判断当前操作者的面部辨识值与步骤1中所得合法用户面部辨识值一致时,转入执行步骤11;否则,所述移动终端强制关闭当前支付界面且拒绝当前操作者的支付操作;

步骤11,所述移动终端将其屏幕分成六个显示区域,且分别在各显示区域内显示一个数字支付密码输入框,且将所得六幅屏幕扰乱防护图像随机地分配至所述六个显示区域,由移动终端的屏幕按照所得各爆闪显示频率分别对应地显示各屏幕扰乱防护图像;

步骤12,所述移动终端接收通过合法身份验证的当前操作者在各数字支付密码输入框内所输入的数字,并且判断当前操作者在数字支付密码输入框内所先后输入的数字与步骤1中存储的六位数字支付密码对应一致时,移动终端准许当前操作者的支付操作;否则,移动终端按照所得各爆闪显示频率对应显示各显示区域内的屏幕扰乱防护图像,并强制退出当前支付程序。

2. 根据权利要求1所述基于语音秘密信息隐藏的支付方法,其特征在于,针对支付密码输入框 $Inputbox_m$ 所输入的数字 D_m 满足如下条件: $2 \leq D_m \leq 9, m=1, 2, \dots, 6$ 。

3. 根据权利要求1所述基于语音秘密信息隐藏的支付方法,其特征在于,所述语音特征采集预设时间段 T_2 为3min。

4. 根据权利要求1所述基于语音秘密信息隐藏的支付方法,其特征在于,所述面部预设采集时间段大于所述语音特征采集预设时间段。

5. 根据权利要求1~4任一项所述基于语音秘密信息隐藏的支付方法,其特征在于,所述移动终端为智能手机或平板电脑。

6. 根据权利要求5所述基于语音秘密信息隐藏的支付方法,其特征在于,所述移动终端的系统为Android系统或iOS系统。

基于语音秘密信息隐藏的支付方法

技术领域

[0001] 本发明涉及移动支付领域,尤其涉及一种基于语音秘密信息隐藏的支付方法。

背景技术

[0002] 当前,随着移动终端硬件技术和软件技术的不断发展成熟,利用移动终端所实现的移动支付越来越受到人们的钟爱,尤其是年轻群体的喜爱。出门不用带现金,几乎就可以完成正常的消费付款功能,极大地促进了市场支付效率,方便了人们的消费活动。

[0003] 然而,利用移动终端进行支付虽然方便了用户的正常消费活动,但是,也存在着用户的支付信息被非法盗取或者因个人信息泄漏而造成支付信息被人破解的危险,严重地威胁着用户的支付安全,影响了移动支付活动的正常有序进行。

发明内容

[0004] 本发明所要解决的技术问题是针对上述现有技术提供一种基于语音秘密信息隐藏的支付方法。该基于语音秘密信息隐藏的支付方法将语音顿挫波动系数作为辨识用户合法身份的一个特征,实现了利用语音数据来隐藏用户身份信息的效果,确保支付程序操作者的身份安全。

[0005] 本发明解决上述技术问题所采用的技术方案为:基于语音秘密信息隐藏的支付方法,用于实现移动终端的支付操作,其特征在于,包括如下步骤1至步骤12:

[0006] 步骤1,移动终端显示支付密码输入框界面给其合法用户,获取、存储其合法用户针对各支付密码输入框所先后输入的数字,并以所存储的各数字作为该移动终端的支付密码,且由移动终端在预设时间段内获取该合法用户输入各数字时所对应施加给该移动终端屏幕的压力数据库;

[0007] 其中,所述支付密码输入框界面中包括有六个支付密码输入框;所述六个支付密码输入框中的第 m 个支付密码输入框标记为 Inputbox_m ,移动终端合法用户针对支付密码输入框 Inputbox_m 所输入的数字为 $D_m, m=1, 2, \dots, 6$;所述预设时间段标记为 T_1 ,移动终端合法用户输入数字 D_m 时所对应施加给移动终端屏幕的压力数据库标记为 $F_{D_m}; F_{D_m} = \{f_{D_{m,n}}\}, n=1, 2, \dots, N$;

压力数据库 F_{D_m} 内具有 N 个针对移动终端屏幕的压力数据, $f_{D_{m,n}}$ 表示压力数据库 F_{D_m} 内的第 n 个施加给移动终端屏幕的压力数据;

[0008] 步骤2,所述移动终端分别根据其合法用户输入至各支付密码输入框内所对应数字的压力数据库,得到针对所述全部数字的数字屏控特征参数;其中,针对所述全部数字的数字屏控特征参数标记为 Ψ :

$$[0009] \quad \psi = \frac{\sin\left(\sum_{m=1}^S \sum_{n=1}^{N-1} \left(\frac{f_{D_{m+1,n+1}}}{f_{D_{m,n}}}\right)\right)}{\left[\frac{\min(f_{D_{m,n}}, f_{D_{S,N}})}{\max(f_{D_{m,n}}, f_{D_{S,N}})}\right]};$$

[0010] 其中, $\min(f_{D_{m,n}}, f_{D_{S,N}})$ 表示施加给移动终端屏幕的压力数据 $f_{D_{S,N}}$ 与所有压力数据 $f_{D_{m,n}}$ 中的最小值, $\max(f_{D_{m,n}}, f_{D_{S,N}})$ 表示施加给移动终端屏幕的压力数据 $f_{D_{S,N}}$ 与所有压力数据 $f_{D_{m,n}}$ 中的最大值;

[0011] 步骤3,所述移动终端预先设置语音特征采集预设时间段,由移动终端在该语音特征采集预设时间段内获取其合法用户的语音数据,形成其合法用户的语音数据库;由所述移动终端根据所得其合法用户的语音数据库,得到其合法用户的语音特征校验参数;其中,所述语音特征采集预设时间段标记为 T_2 ,移动终端其合法用户的语音数据库标记为 $\text{Voice}_{\text{User}}$, $\text{Voice}_{\text{User}} = \{\text{voice}_{\text{User},k}\}$, $k=1,2,\dots,K$;语音数据库 $\text{Voice}_{\text{User}}$ 内具有 K 个语音数据, $\text{voice}_{\text{User},k}$ 表示语音数据库 $\text{Voice}_{\text{User}}$ 内的第 k 个语音数据;语音数据 $\text{voice}_{\text{User},k}$ 的振幅标记为 $A_{\text{voice}_{\text{User},k}}$;所述移动终端其合法用户的语音特征校验参数标记为 κ :

$$[0012] \quad \kappa = \sqrt{\sum_{k=1}^K \left(A_{\text{voice}_{\text{User},k}}^2 - \frac{\text{mid}(A_{\text{voice}_{\text{User}}})^2}{K} \right)};$$

[0013] 其中, $\text{mid}(A_{\text{voice}_{\text{User}}})$ 表示移动终端其合法用户的所有语音数据振幅数值中的数值中间值;

[0014] 步骤4,设置针对所述移动终端合法用户面部信息的面部预设采集时间段,由移动终端在所述面部预设采集时间段内获取、处理其合法用户的面部预设个数的面部图像,得到针对该移动终端合法用户的面部图像数据库以及合法用户面部识别值;

[0015] 其中,所述面部预设采集时间段标记为 T_3 ,针对移动终端合法用户面部图像的预设个数标记为 S ,所述移动终端合法用户的面部图像数据库标记为 $\text{Face}_{\text{User}}$,所述移动终端合法用户的面部图像数据库 $\text{Face}_{\text{User}}$ 内的第 s 个面部图像标记为 $\text{Jpg}_{\text{User},s}$, $1 \leq s \leq S$;所述移动终端合法用户面部识别值标记为 θ_{Face} :

$$[0016] \quad \theta_{\text{Face}} = \frac{\sum_{s=1}^S (L_{\text{Face},s} - \sigma_{L_{\text{Face}}})}{\sum_{s=1}^S (W_{\text{Face},s} - \sigma_{W_{\text{Face}}})} \cdot \frac{\sigma_{L_{\text{Face}}}}{\sigma_{W_{\text{Face}}}};$$

$$[0017] \quad \sigma_{L_{\text{Face}}} = \sqrt{\frac{1}{S} \sum_{s=1}^S (L_{\text{Face},s} - \overline{L_{\text{Face}}})^2}, \quad \sigma_{W_{\text{Face}}} = \sqrt{\frac{1}{S} \sum_{s=1}^S (W_{\text{Face},s} - \overline{W_{\text{Face}}})^2};$$

$$[0018] \quad \overline{L_{\text{Face}}} = \frac{1}{S} \sum_{s=1}^S L_{\text{Face},s}, \quad \overline{W_{\text{Face}}} = \frac{1}{S} \sum_{s=1}^S W_{\text{Face},s};$$

[0019] 其中, $L_{\text{Face},s}$ 表示面部图像 $\text{Jpg}_{\text{User},s}$ 的长度值, $W_{\text{Face},s}$ 表示面部图像 $\text{Jpg}_{\text{User},s}$ 的宽度值;

[0020] 步骤5,所述移动终端连续获取其合法用户的六幅眼睛图像,以获取的所述六幅眼睛图像作为针对移动终端支付时的屏幕扰乱防护图像;

[0021] 其中,在移动终端屏幕上,按照从左至右的顺序,所获取移动终端其合法用户的眼睛图像标记 $Jpg_{Eye,m}$;针对移动终端支付时的屏幕扰乱防护图像标记为 $Jpg_{Protect,m}$, $m=1,2,\dots,6$;

[0022] 步骤6,所述移动终端在步骤1的所述预设时间段内获取其合法用户双眼注意力集中在该移动终端屏幕上的时间,并由移动终端分别获取其合法用户的左眼和右眼在预设时间段内对应的眨眼次数,得到移动终端其合法用户的注视支付紧张系数;

[0023] 其中,所述移动终端其合法用户双眼注意力集中在该移动终端屏幕上的时间标记为 T_4 ,所述移动终端其合法用户的左眼在预设时间段内的眨眼次数标记为 C_{left} ,所述移动终端其合法用户的右眼在预设时间段内的眨眼次数标记为 C_{right} ,所述移动终端其合法用户的注视支付紧张系数标记为 Ω :

$$[0024] \quad \Omega = \left| \frac{C_{left} - C_{right}}{C_{left} \cdot C_{right}} \cdot \sin \left(\frac{C_{left}}{T_1 - T_4} + \frac{C_{right}}{T_1 - T_4} \right) \right|; \text{其中, } T_1 \text{ 表示所述预设时间段};$$

[0025] 步骤7,所述移动终端根据在所述语音特征采集预设时间段内所采集并形成的其合法用户的语音数据库,得到移动终端其合法用户的语音顿挫波动系数;其中,所述语音顿挫波动系数标记为 ρ :

$$[0026] \quad \rho = \frac{\sqrt{\frac{1}{K} \sum_{k=1}^K (A_{voice_{User,k}} - \overline{A_{voice_{User}}})^2}}{T_2 \cdot mid(A_{voice_{User}})}, \quad \overline{A_{voice_{User}}} = \frac{1}{K} \sum_{k=1}^K A_{voice_{User,k}};$$

[0027] 其中, T_2 表示所述语音特征采集预设时间段;

[0028] 步骤8,所述移动终端分别获取其屏幕当前光照强度值以及各屏幕扰乱防护图像的长度值和宽度值,并结合预设时间段以及语音特征采集预设时间段、面部预设采集时间段、所得数字屏控特征参数、注视支付紧张系数和语音顿挫波动系数,分别得到针对各幅屏幕扰乱防护图像的爆闪显示频率;

[0029] 其中,所述屏幕扰乱防护图像 $Jpg_{Protect,m}$ 的长度值和宽度值分别对应标记为 $L_{Jpg_{Protect,m}}$ 和 $W_{Jpg_{Protect,m}}$;所述屏幕扰乱防护图像 $Jpg_{Protect,m}$ 的爆闪显示频率标记为 $\xi_{Jpg_{Protect,m}}$:

$$[0030] \quad \xi_{Jpg_{Protect,m}} = \frac{Light_{Screen}^2}{L_{Jpg_{Protect,m}} \cdot W_{Jpg_{Protect,m}}} \cdot \frac{\max(L_{Jpg_{Protect,m}}, W_{Jpg_{Protect,m}})}{\min(L_{Jpg_{Protect,m}}, W_{Jpg_{Protect,m}})} \cdot \frac{|T_1 - T_2| \cdot \Omega \cdot \rho}{|T_1 - T_3| \cdot \psi};$$

[0031] 其中, $\max(L_{Jpg_{Protect,m}}, W_{Jpg_{Protect,m}})$ 表示数值 $L_{Jpg_{Protect,m}}$ 和数值 $W_{Jpg_{Protect,m}}$ 的最大值;

$\min(L_{Jpg_{Protect,m}}, W_{Jpg_{Protect,m}})$ 表示数值 $L_{Jpg_{Protect,m}}$ 和数值 $W_{Jpg_{Protect,m}}$ 的最小值;

[0032] 步骤9,所述移动终端在检测到有操作者做支付密码输入操作时,移动终端弹出获取当前操作者语音的界面,且移动终端在预设语音获取时间段内获取到语音数据时,转入步骤10;否则,所述移动终端强制关闭当前支付界面且拒绝当前操作者的支付操作,直到移动终端获取到当前操作者的语音数据时方才准许转入步骤10;

[0033] 步骤10,所述移动终端在检测到操作者开始输入数字支付密码时,移动终端获取当前操作者的面部辨识值,并且判断当前操作者的面部辨识值与步骤1中所得合法用户面部辨识值一致时,转入执行步骤11;否则,所述移动终端强制关闭当前支付界面且拒绝当前操作者的支付操作;

[0034] 步骤11,所述移动终端将其屏幕分成六个显示区域,且分别在各显示区域内显示一个数字支付密码输入框,且将所得六幅屏幕扰乱防护图像随机地分配至所述六个显示区域,由移动终端的屏幕按照所得各爆闪显示频率分别对应地显示各屏幕扰乱防护图像;

[0035] 步骤12,所述移动终端接收通过合法身份验证的当前操作者在各数字支付密码输入框内所输入的数字,并且判断当前操作者在数字支付密码输入框内所先后输入的数字与步骤1中存储的六位数字支付密码对应一致时,移动终端准许当前操作者的支付操作;否则,移动终端按照所得各爆闪显示频率对应显示各显示区域内的屏幕扰乱防护图像,并强制退出当前支付程序。

[0036] 改进地,在所述基于语音秘密信息隐藏的支付方法中,针对支付密码输入框Inputbox_m所输入的数字D_m满足如下条件: $2 \leq D_m \leq 9, m=1, 2, \dots, 6$ 。

[0037] 进一步地,在所述基于语音秘密信息隐藏的支付方法中,所述语音特征采集预设时间段T₂为3min。

[0038] 再改进,在所述基于语音秘密信息隐藏的支付方法中,所述面部预设采集时间段大于所述语音特征采集预设时间段。

[0039] 可选择地,在所述基于语音秘密信息隐藏的支付方法中,所述移动终端为智能手机或平板电脑。

[0040] 进一步地,所述移动终端的系统为Android系统或iOS系统。

[0041] 与现有技术相比,本发明的优点在于:

[0042] 首先,本发明利用移动终端其合法用户在各支付密码输入框输入对应数字时的压力数据,得到针对全部数字的数字屏控特征参数,由此将压力特征作为针对移动终端合法用户进行支付操作时的身份辨识特征;通过利用移动终端构建的其合法用户的面部图像数据库来得到表征移动终端合法用户身份信息的面部辨识值这一特征参数,以避免非法者的仿冒支付操作,确保只有经过验证合法身份的用户才能操作该移动终端的支付程序,由此在支付操作的初期就起到针对非法者的防范功能,提高支付安全;

[0043] 其次,通过基于移动终端合法用户双眼在预设时间段内分别针对移动终端屏幕的眨眼次数,得到表征移动终端合法用户支付操作时的注视支付紧张系数,可以有效地帮助移动终端准确识别其合法用户是否当前正在进行支付操作,由此保证移动终端合法用户的支付信息安全;

[0044] 再次,通过得到移动终端其合法用户的语音顿挫波动系数,可以使得移动终端准确地根据外部所输入的用户语音情况来得到所输入语音的语音顿挫波动情况,由此将语音顿挫波动系数作为辨识用户合法身份的一个特征,实现了利用语音数据来隐藏用户身份信息的效果,再次确保支付程序操作者的身份安全;

[0045] 最后,通过得到针对各幅屏幕扰乱防护图像的爆闪显示频率,可以使得在每幅屏幕扰乱防护图像在移动终端屏幕上显示时,移动终端屏幕针对各屏幕扰乱防护图像的部分都会按照对应各各自的爆闪显示频率来显示这些屏幕扰乱防护图像,这样,由于非法者根

本就不知道移动终端合法用户所设置的数字支付密码,加之此时移动终端屏幕上的各幅屏幕扰乱防护图像又按照各自对应的爆闪显示频率不断闪烁,由此可以强有力地干扰非法者所试图成功准确偷窥查看到合法用户所输入支付密码的概率,极大地提高了移动终端其合法用户的支付信息安全。

附图说明

[0046] 图1为发明实施例中基于语音秘密信息隐藏的支付方法流程示意图。

具体实施方式

[0047] 以下结合附图实施例对本发明作进一步详细描述。

[0048] 如图1所示,本实施例中基于语音秘密信息隐藏的支付方法,用于实现移动终端的支付操作,该基于语音秘密信息隐藏的支付方法包括如下步骤1至步骤12:

[0049] 步骤1,移动终端显示支付密码输入框界面给其合法用户,获取、存储其合法用户针对各支付密码输入框所先后输入的数字,并以所存储的各数字作为该移动终端的支付密码,且由移动终端在预设时间段内获取该合法用户输入各数字时所对应施加给该移动终端屏幕的压力数据库;

[0050] 其中,支付密码输入框界面中包括有六个支付密码输入框;六个支付密码输入框中的第 m 个支付密码输入框标记为 Inputbox_m ,移动终端合法用户针对支付密码输入框 Inputbox_m 所输入的数字为 D_m , $m=1,2,\dots,6$;预设时间段标记为 T_1 ,移动终端合法用户输入数字 D_m 时所对应施加给移动终端屏幕的压力数据库标记为 F_{D_m} ; $F_{D_m} = \{f_{D_{m,n}}\}$, $n=1,2,\dots,N$;压力数据库 F_{D_m} 内具有 N 个针对移动终端屏幕的压力数据, $f_{D_{m,n}}$ 表示压力数据库 F_{D_m} 内的第 n 个施加给移动终端屏幕的压力数据;

[0051] 具体地,六个支付密码输入框分别为 Inputbox_1 、 Inputbox_2 、 Inputbox_3 、 Inputbox_4 、 Inputbox_5 和 Inputbox_6 ;移动终端合法用户针对各支付密码输入框与所输入数字之间的关系对应如下:

[0052] 支付密码输入框 Inputbox_1 内所输入的数字为 D_1 ,支付密码输入框 Inputbox_2 内所输入的数字为 D_2 ,支付密码输入框 Inputbox_3 内所输入的数字为 D_3 ,支付密码输入框 Inputbox_4 内所输入的数字为 D_4 ,支付密码输入框 Inputbox_5 内所输入的数字为 D_5 ,支付密码输入框 Inputbox_6 内所输入的数字为 D_6 ;

[0053] 另外,比如说,移动终端合法用户输入数字 D_1 时所对应施加给移动终端屏幕的压力数据库标记为 F_{D_1} ,压力数据库 F_{D_1} 内具有五个压力数据,即 $N=5$,则

[0054] $F_{D_1} = \{f_{D_{1,1}}, f_{D_{1,2}}, f_{D_{1,3}}, f_{D_{1,4}}, f_{D_{1,5}}\}$;

[0055] 需要说明的是,在本实施例中,针对支付密码输入框 Inputbox_m 所输入的数字 D_m 满足如下条件: $2 \leq D_m \leq 9$, $m=1,2,\dots,6$ 。也就是说,本实施例中所指的各支付密码输入框内所输入的数字范围为数字2到数字9这个区间;

[0056] 本实施例中的移动终端可以选用智能手机或平板电脑,其中,移动终端的系统为Android系统或iOS系统;

[0057] 步骤2,移动终端分别根据其合法用户输入至各支付密码输入框内所对应数字的压力数据库,得到针对全部数字的数字屏控特征参数;其中,针对全部数字的数字屏控特征参数标记为 ψ :

$$[0058] \quad \psi = \frac{\sin\left(\sum_{m=1}^5 \sum_{n=1}^{N-1} \left(\frac{f_{D_{m+1,n+1}}}{f_{D_{m,n}}}\right)\right)}{\left[\frac{\min(f_{D_{m,n}}, f_{D_{5,N}})}{\max(f_{D_{m,n}}, f_{D_{5,N}})}\right]};$$

[0059] 其中, $\min(f_{D_{m,n}}, f_{D_{5,N}})$ 表示施加给移动终端屏幕的压力数据 $f_{D_{5,N}}$ 与所有压力数据 $f_{D_{m,n}}$ 中的最小值, $\max(f_{D_{m,n}}, f_{D_{5,N}})$ 表示施加给移动终端屏幕的压力数据 $f_{D_{5,N}}$ 与所有压力数据 $f_{D_{m,n}}$ 中的最大值;

[0060] 针对该步骤2举例说明如下,针对步骤1中所说的支付密码输入框 Inputbox_1 ,数值 $N=5$,其所对应的压力数据库为 F_{D_1} , $f_{D_{5,5}}$ 表示支付密码输入框 Inputbox_5 所对应压力数据库为 F_{D_5} 内的第五个压力数据; $\min(f_{D_{1,n}}, f_{D_{5,5}})$ 就表示压力数据库为 F_{D_1} 内的五个压力数据与压力数据 $f_{D_{5,5}}$ 经比较后的最小值;

[0061] 同样地, $\max(f_{D_{1,n}}, f_{D_{5,5}})$ 就表示压力数据库为 F_{D_1} 内的五个压力数据与压力数据 $f_{D_{5,5}}$ 经比较后的最大值;

[0062] 在该步骤2中,通过利用移动终端其合法用户在各支付密码输入框输入对应数字时的压力数据,得到针对全部数字的数字屏控特征参数,由此利用该针对全部数字的数字屏控特征参数来表征合法用户输入支付密码时的操作压力特征,即将压力特征作为针对移动终端合法用户进行支付操作时的身份辨识特征;

[0063] 步骤3,移动终端预先设置语音特征采集预设时间段,由移动终端在该语音特征采集预设时间段内获取其合法用户的语音数据,形成其合法用户的语音数据库;由移动终端根据所得其合法用户的语音数据库,得到其合法用户的语音特征校验参数;

[0064] 其中,语音特征采集预设时间段标记为 T_2 ,移动终端其合法用户的语音数据库标记为 $\text{Voice}_{\text{User}}$, $\text{Voice}_{\text{User}} = \{\text{voice}_{\text{User},k}\}, k=1,2,\dots,K$;

[0065] 设定语音数据库 $\text{Voice}_{\text{User}}$ 内具有 K 个语音数据, $\text{voice}_{\text{User},k}$ 表示语音数据库 $\text{Voice}_{\text{User}}$ 内的第 k 个语音数据;语音数据 $\text{voice}_{\text{User},k}$ 的振幅标记为 $A_{\text{voice}_{\text{User},k}}$;移动终端其合法用户的语音特征校验参数标记为 κ :

$$[0066] \quad \kappa = \sqrt{\sum_{k=1}^K \left(A_{\text{voice}_{\text{User},k}}^2 - \frac{\text{mid}(A_{\text{voice}_{\text{User}}})^2}{K} \right)};$$

[0067] 其中, $\text{mid}(A_{\text{voice}_{\text{User}}})$ 表示移动终端其合法用户的所有语音数据振幅数值中的数值中间值;

[0068] 在本实施例中,语音特征采集预设时间段 T_2 优选设置为 3min , 即 $T_2=3\text{min}$ 。

[0069] 假设移动终端其合法用户语音数据库Voice_{User}的语音数据设置为7个,即K=7,这七个语音数据分别是voice_{User,1}、voice_{User,2}、voice_{User,3}、voice_{User,4}、voice_{User,5}、voice_{User,6}和voice_{User,7};对应地,各语音数据的振幅依次对应为 $A_{voice_{User,1}}$ 、 $A_{voice_{User,2}}$ 、 $A_{voice_{User,3}}$ 、 $A_{voice_{User,4}}$ 、 $A_{voice_{User,5}}$ 、 $A_{voice_{User,6}}$ 和 $A_{voice_{User,7}}$;

[0070] 移动终端其合法用户的语音特征校验参数κ值计算如下:

$$[0071] \quad \kappa = \sqrt{\sum_{k=1}^7 \left(A_{voice_{User,k}}^2 - \frac{mid(A_{voice_{User}})}{7} \right)^2}; \text{ 此时的 } mid(A_{voice_{User}}) \text{ 就是移动终端其合法用户}$$

的所有语音数据振幅数值 $A_{voice_{User,1}}$ 、 $A_{voice_{User,2}}$ 、 $A_{voice_{User,3}}$ 、 $A_{voice_{User,4}}$ 、 $A_{voice_{User,5}}$ 、 $A_{voice_{User,6}}$ 和 $A_{voice_{User,7}}$ 中的数值中间值;也就是说, $mid(A_{voice_{User}})$ 是所有语音数据振幅数值按照数值大小排序后,那个数值位于中间的语音数据振幅数值;

[0072] 步骤4,设置针对移动终端合法用户面部信息的面部预设采集时间段,由移动终端在面部预设采集时间段内获取、处理其合法用户的面部预设个数的面部图像,得到针对该移动终端合法用户的面部图像数据库以及合法用户面部辨识值;

[0073] 其中,面部预设采集时间段标记为 T_3 ,针对移动终端合法用户面部图像的预设个数标记为S,移动终端合法用户的面部图像数据库标记为Face_{User},移动终端合法用户的面部图像数据库Face_{User}内的第s个面部图像标记为Jpg_{User,s}, $1 \leq s \leq S$;移动终端合法用户面部辨识值标记为 θ_{Face} :

$$[0074] \quad \theta_{Face} = \frac{\sum_{s=1}^S (L_{Face,s} - \sigma_{L_{Face}})}{\sum_{s=1}^S (W_{Face,s} - \sigma_{W_{Face}})} \cdot \frac{\sigma_{L_{Face}}}{\sigma_{W_{Face}}};$$

$$[0075] \quad \sigma_{L_{Face}} = \sqrt{\frac{1}{S} \sum_{s=1}^S (L_{Face,s} - \overline{L_{Face}})^2}, \quad \sigma_{W_{Face}} = \sqrt{\frac{1}{S} \sum_{s=1}^S (W_{Face,s} - \overline{W_{Face}})^2};$$

$$[0076] \quad \overline{L_{Face}} = \frac{1}{S} \sum_{s=1}^S L_{Face,s}, \quad \overline{W_{Face}} = \frac{1}{S} \sum_{s=1}^S W_{Face,s};$$

[0077] 其中, $L_{Face,s}$ 表示面部图像Jpg_{User,s}的长度值, $W_{Face,s}$ 表示面部图像Jpg_{User,s}的宽度值;本实施例中的面部预设采集时间段大于语音特征采集预设时间段,即面部预设采集时间段大于3min;

[0078] 该步骤4通过利用移动终端构建的其合法用户的面部图像数据库来得到表征移动终端合法用户身份信息的面部辨识值这一特征参数,以避免非法者的仿冒支付操作,确保只有经过验证合法身份的用户才能操作该移动终端的支付程序,由此在支付操作的初期就起到针对非法者的防范功能,提高支付安全;

[0079] 步骤5,移动终端连续获取其合法用户的六幅眼睛图像,以获取的这六幅眼睛图像作为针对移动终端支付时的屏幕扰乱防护图像;

[0080] 其中,在移动终端屏幕上,按照从左至右的顺序,所获取移动终端其合法用户的眼睛图像标记为Jpg_{Eye,m};针对移动终端支付时的屏幕扰乱防护图像标记为Jpg_{Protect,m}, $m=1$,

2, ..., 6;

[0081] 此处需要举例说明如下, 所获取移动终端合法用户的眼睛图像分别标记为 $Jpg_{Eye,1}$ 、 $Jpg_{Eye,2}$ 、 $Jpg_{Eye,3}$ 、 $Jpg_{Eye,4}$ 、 $Jpg_{Eye,5}$ 和 $Jpg_{Eye,6}$;

[0082] 针对移动终端支付时的屏幕扰乱防护图像分别对应标记为 $Jpg_{Protect,1}$ 、 $Jpg_{Protect,2}$ 、 $Jpg_{Protect,3}$ 、 $Jpg_{Protect,4}$ 、 $Jpg_{Protect,5}$ 和 $Jpg_{Protect,6}$;

[0083] 步骤6, 移动终端在步骤1的预设时间段 T_1 内获取其合法用户双眼注意力集中在该移动终端屏幕上的时间, 并由移动终端分别获取其合法用户的左眼和右眼在预设时间段内对应的眨眼次数, 得到移动终端其合法用户的注视支付紧张系数;

[0084] 其中, 移动终端其合法用户双眼注意力集中在该移动终端屏幕上的时间标记为 T_4 , 移动终端其合法用户的左眼在预设时间段内的眨眼次数标记为 C_{left} , 移动终端其合法用户的右眼在预设时间段内的眨眼次数标记为 C_{right} , 移动终端其合法用户的注视支付紧张系数标记为 Ω ;

[0085]
$$\Omega = \left| \frac{C_{left} - C_{right}}{C_{left} \cdot C_{right}} \cdot \sin \left(\frac{C_{left}}{T_1 - T_4} + \frac{C_{right}}{T_1 - T_4} \right) \right|$$
; 其中, T_1 表示预设时间段;

[0086] 针对此处的步骤6需要说明的是, 由于移动终端合法用户在利用移动终端支付操作时, 因涉及到资金问题, 移动终端合法用户对于移动终端屏幕的注视程度与其正常操作移动终端时对移动终端屏幕的注视程度显然是截然是不同的; 通常情况下, 移动终端合法用户在进行支付操作时更加会注视移动终端屏幕, 这种针对移动终端屏幕的注视程度对应表现为用户的左右眼注意力, 进一步具体表现为左眼眨眼频率和右眼眨眼频率。因此, 该步骤6通过基于移动终端合法用户双眼在预设时间段 T_1 内分别针对移动终端屏幕的眨眼次数, 得到表征移动终端合法用户支付操作时的注视支付紧张系数, 可以有效地帮助移动终端准确识别其合法用户是否当前正在进行支付操作, 由此保证移动终端合法用户的支付信息安全;

[0087] 步骤7, 移动终端根据在语音特征采集预设时间段 T_2 内所采集并形成的其合法用户的语音数据库, 得到移动终端其合法用户的语音顿挫波动系数; 其中, 语音顿挫波动系数标记为 ρ ;

[0088]
$$\rho = \frac{\sqrt{\frac{1}{K} \sum_{k=1}^K (A_{voice_{User,k}} - \overline{A_{voice_{User}}})^2}}{T_2 \cdot mid(A_{voice_{User}})}, \quad \overline{A_{voice_{User}}} = \frac{1}{K} \sum_{k=1}^K A_{voice_{User,k}};$$

[0089] 其中, T_2 表示语音特征采集预设时间段;

[0090] 在该步骤7中, 通过得到移动终端其合法用户的语音顿挫波动系数, 可以使得移动终端准确地根据外部所输入的用户语音情况来得到所输入语音的语音顿挫波动情况, 由于每个人在说话时的语音大小、语音速度快慢均不同, 这样移动终端利用所得到的语音顿挫波动系数就可以非常清楚、准确地获知当前语音是否为其合法用户的语音, 由此作为辨识用户合法身份的一个特征, 再次确保支付程序操作者的身份安全;

[0091] 步骤8, 移动终端分别获取其屏幕当前光照强度值以及各屏幕扰乱防护图像的长度值和宽度值, 并结合预设时间段 T_1 以及语音特征采集预设时间段 T_2 、面部预设采集时间段 T_3 、所得数字屏控特征参数 ψ 、注视支付紧张系数 Ω 和语音顿挫波动系数 ρ , 分别得到针对各

幅屏幕扰乱防护图像的爆闪显示频率；

[0092] 其中，屏幕扰乱防护图像 $Jpg_{Protect,m}$ 的长度值和宽度值分别对应标记为 $L_{Jpg_{Protect,m}}$ 和 $W_{Jpg_{Protect,m}}$ ；屏幕扰乱防护图像 $Jpg_{Protect,m}$ 的爆闪显示频率标记为 $\xi_{Jpg_{Protect,m}}$ ；

$$[0093] \quad \xi_{Jpg_{Protect,m}} = \frac{Light_{Screen}^2}{L_{Jpg_{Protect,m}} \cdot W_{Jpg_{Protect,m}}} \cdot \frac{\max(L_{Jpg_{Protect,m}}, W_{Jpg_{Protect,m}})}{\min(L_{Jpg_{Protect,m}}, W_{Jpg_{Protect,m}})} \cdot \frac{|T_1 - T_2| \cdot \Omega \cdot \rho}{|T_1 - T_3| \cdot \psi};$$

[0094] 其中， $\max(L_{Jpg_{Protect,m}}, W_{Jpg_{Protect,m}})$ 表示数值 $L_{Jpg_{Protect,m}}$ 和数值 $W_{Jpg_{Protect,m}}$ 的最大值；

$\min(L_{Jpg_{Protect,m}}, W_{Jpg_{Protect,m}})$ 表示数值 $L_{Jpg_{Protect,m}}$ 和数值 $W_{Jpg_{Protect,m}}$ 的最小值；

[0095] 在该步骤8中，通过得到针对各幅屏幕扰乱防护图像的爆闪显示频率，可以使得在每幅屏幕扰乱防护图像在移动终端屏幕上显示时，移动终端屏幕针对各屏幕扰乱防护图像的部分都会按照对应各各自的爆闪显示频率来显示这些屏幕扰乱防护图像，这样，由于非法者根本就不知道移动终端合法用户所设置的数字支付密码，加之此时移动终端屏幕上的各幅屏幕扰乱防护图像又按照各自对应的爆闪显示频率不断闪烁，由此可以强有力地干扰非法者所试图成功准确偷窥查看到合法用户所输入支付密码的概率，极大地提高了移动终端其合法用户的支付信息安全；

[0096] 步骤9，移动终端在检测到有操作者做支付密码输入操作时，移动终端弹出获取当前操作者语音的界面，且移动终端在预设语音获取时间段内获取到语音数据时，转入步骤10；否则，移动终端强制关闭当前支付界面且拒绝当前操作者的支付操作，直到移动终端获取到当前操作者的语音数据时方才准许转入步骤10，由此避免因非法用户或者其他用户对移动终端的支付操作；

[0097] 步骤10，移动终端在检测到操作者开始输入数字支付密码时，移动终端获取当前操作者的面部辨识值，并且判断当前操作者的面部辨识值与步骤1中所得合法用户面部辨识值一致时，转入执行步骤11；否则，移动终端强制关闭当前支付界面且拒绝当前操作者的支付操作，由此避免因非法用户或者其他用户对移动终端的支付操作；

[0098] 步骤11，移动终端将其屏幕分成六个显示区域，且分别在各显示区域内显示一个数字支付密码输入框，且将所得六幅屏幕扰乱防护图像随机地分配至所述六个显示区域，由移动终端的屏幕按照所得各爆闪显示频率分别对应地显示各屏幕扰乱防护图像；

[0099] 例如，移动终端屏幕上所分成的六个显示区域分布是 $Area_1$ 、 $Area_2$ 、 $Area_3$ 、 $Area_4$ 、 $Area_5$ 和 $Area_6$ ；

[0100] 显示区域 $Area_1$ 至 $Area_6$ 内所显示的数字支付密码输入框分布一一对应地标记为 $Inputbox_1$ 、 $Inputbox_2$ 、 $Inputbox_3$ 、 $Inputbox_4$ 、 $Inputbox_5$ 和 $Inputbox_6$ ；

[0101] 移动终端在显示出这六个数字支付密码输入框后，移动终端就随机地分配六幅屏幕扰乱防护图像到这六个显示区域内；例如，移动终端地随机分配情况如下：

[0102] 屏幕扰乱防护图像 $Jpg_{Protect,1}$ 被分配到显示区域 $Area_2$ ，移动终端屏幕在该显示区域 $Area_2$ 内按照爆闪显示频率 $\xi_{Jpg_{Protect,1}}$ 显示该图像 $Jpg_{Protect,1}$ ；

[0103] 屏幕扰乱防护图像 $Jpg_{Protect,2}$ 被分配到显示区域 $Area_1$ ，移动终端屏幕在该显示区

域Area₁内按照爆闪显示频率 $\xi_{Jpg_Protect,2}$ 显示该图像Jpg_{Protect,2};

[0104] 屏幕扰乱防护图像Jpg_{Protect,3}被分配到显示区域Area₃,移动终端的屏幕在该显示区域Area₃内按照爆闪显示频率 $\xi_{Jpg_Protect,3}$ 显示该图像Jpg_{Protect,3};

[0105] 屏幕扰乱防护图像Jpg_{Protect,4}被分配到显示区域Area₄,移动终端的屏幕在该显示区域Area₄内按照爆闪显示频率 $\xi_{Jpg_Protect,4}$ 显示该图像Jpg_{Protect,4};

[0106] 屏幕扰乱防护图像Jpg_{Protect,5}被分配到显示区域Area₅,移动终端的屏幕在该显示区域Area₅内按照爆闪显示频率 $\xi_{Jpg_Protect,5}$ 显示该图像Jpg_{Protect,5};

[0107] 屏幕扰乱防护图像Jpg_{Protect,6}被分配到显示区域Area₆,移动终端的屏幕在该显示区域Area₆内按照爆闪显示频率 $\xi_{Jpg_Protect,6}$ 显示该图像Jpg_{Protect,6};

[0108] 步骤12,移动终端接收通过合法身份验证的当前操作者在各数字支付密码输入框内所输入的数字,并且判断当前操作者在数字支付密码输入框内所先后输入的数字与步骤1中存储的六位数字支付密码对应一致时,移动终端准许当前操作者的支付操作;否则,移动终端按照所得各爆闪显示频率对应显示各显示区域内的屏幕扰乱防护图像,并强制退出当前支付程序。

[0109] 尽管以上详细地描述了本发明的优选实施例,但是应该清楚地理解,对于本领域的技术人员来说,本发明可以有各种更改和变化。凡在本发明的精神和原则之内所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

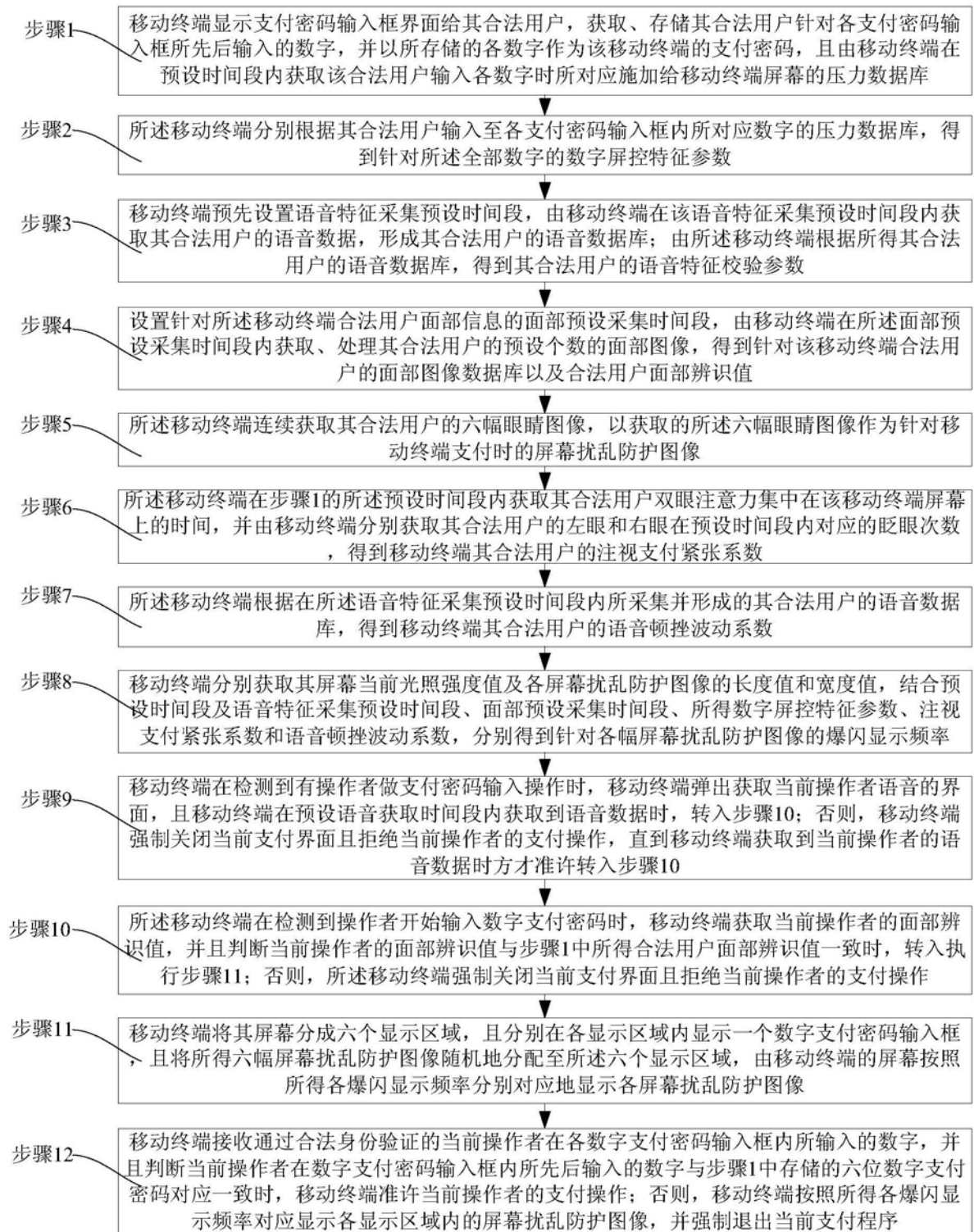


图1