(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104580143 A
(43)申请公布日 2015.04.29

(21)申请号 201410625738.7

(22)申请日 2014.11.09

(71)申请人 李若斌
地址 430024 湖北省武汉市江汉经济开发区江兴路25号A511
申请人 臧存勋

(72)发明人 李若斌 臧存勋

(51)Int.Cl.
*H04L 29/06*(2006.01)
*H04L 9/32*(2006.01)

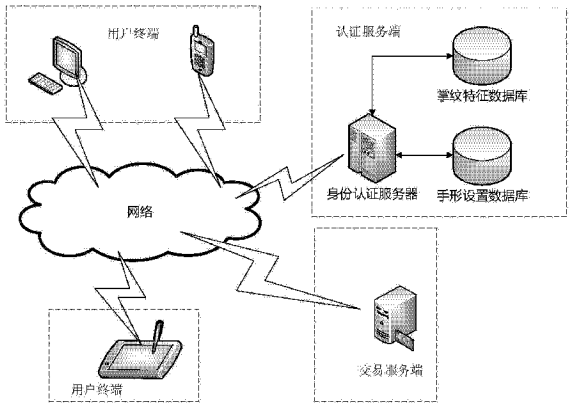
权利要求书14页 说明书43页 附图13页

(54)发明名称

一种基于手势识别的安全认证方法、终端、服务器和系统

(57)摘要

本发明属于身份认证技术领域，本发明公开了一种基于手势识别的安全认证方法、终端、服务器和系统，其中该方法包括：包括注册用户特征信息的步骤和认证用户身份的步骤；注册用户特征信息的步骤包括：采集用户的预置掌纹图像；对预置掌纹图像提取掌纹特征并保存预置掌纹特征；认证用户身份的步骤包括：用户发起认证请求；按预置手形图像生成掌纹手形序列并依序向用户展示手形图像；用户按展示的手形图像依序做相应手势动作并采集用户带掌纹的认证手形图像；对认证手形图像提取手形、掌纹特征并与预置手形、掌纹特征匹配；反馈匹配结果。本发明很大程度上降低了身份信息被劫持的可能性，提高了身份认证的安全性。




CN 104580143 A

1. 一种基于手势识别的安全认证方法，其特征在于：包括注册用户特征信息的步骤和认证用户身份的步骤；

所述注册用户特征信息的步骤包括：

采集用户的预置掌纹图像；

对预置掌纹图像提取掌纹特征并保存预置掌纹特征；

所述认证用户身份的步骤包括：

用户发起认证请求；

按预置手形图像生成掌纹手形序列并依序向用户展示手形图像；

用户按展示的手形图像依序做相应手势动作并采集用户带掌纹的认证手形图像；

对认证手形图像提取手形、掌纹特征并与预置手形、掌纹特征匹配；

反馈匹配结果。

2. 如权利要求 1 所述的安全认证方法，其特征在于：所述采集用户的预置掌纹图像的步骤具体包括：

用户将平整的手掌掌面放置于图像采集位置；

采集用户手掌掌面图像；

对手掌掌面图像预处理。

3. 如权利要求 2 所述的安全认证方法，其特征在于：所述对手掌掌面图像预处理的步骤具体包括：

对采集的手掌掌面图像粗分割处理；

对粗分割处理后的手掌掌面图像前景和背景区分并均衡处理；

对均衡后的手掌掌面图像中值滤波处理；

对中值滤波后的手掌掌面图像的前景手形区域进行二值化处理；

对二值化后的手掌掌面图像作连通区域检测，获取带掌纹的手形图像；

对带掌纹的手形图像的手掌掌面图像进行边缘检测得到二值化后的手形区域。

4. 如权利要求 3 所述的安全认证方法，其特征在于：所述对采集的手掌掌面图像粗分割处理的步骤具体包括：

将手掌掌面图像进行颜色空间转换，从 RGB 空间转换至 HSV 空间；

利用 H 分量提取手的肤色区域。

5. 如权利要求 3 所述的安全认证方法，其特征在于：所述对采集的手掌掌面图像前景和背景区分并均衡处理的步骤具体包括：

将粗分割后的手掌掌面图像转换为灰度图像；将肤色区域以外的区域设置为背景区域；

对手掌掌面图像进行直方图均衡处理得到均衡后的灰度图像。

6. 如权利要求 1 所述的安全认证方法，其特征在于：所述预置掌纹图像或认证手形图像是通过摄像头采集的。

7. 如权利要求 1 所述的安全认证方法，其特征在于：所述提取掌纹特征的步骤具体包括：

定位预置掌纹图像中的掌面区域；

切割预置掌纹图像中的掌面区域；

提取预置掌纹图像中的掌纹特征。

8. 如权利要求 7 所述的安全认证方法，其特征在于，所述定位预置掌纹图像中的掌面区域的步骤具体包括：

a)、对预置掌纹图像从上到下水平穿线边缘图像，找到一组包含有 8 个边界点的穿线；将相邻 2 个边界点作为一组，共四组；将这四组作为是四指的初始穿线组；

b)、对于四指中的每一指，以初始穿线组为起始位置，向上和向下分别进行搜索，直至搜索到上下边界；

c)、以相同的方法，从下至上水平穿线边缘图像，找到一组包含有 4 个边界点的穿线；

d)、同步骤 b)，以拇指初始穿线指为起始位置，向上和向下分别进行搜索，直至搜索到上下边界，进而定位出拇指关键点。

9. 如权利要求 8 所述的安全认证方法，其特征在于，所述切割预置掌纹图像中的掌面区域的步骤具体包括：

找出食指、中指之间的关键点 a、无名指、小指之间的关键点 c；

找出关键点 a 和关键点 c 组成线段的中点 b；

以 b 点为原点，作线段 ac 的法线 f；

然后以 c 点为起点，沿法线 f，朝向手掌方向偏移一定距离处的点 e；

以 e 为中心，生成一个边长为 P 且与线段 ac 平行的矩形区域；

提取 P×P 区域为掌面区域。

10. 如权利要求 1 所述的安全认证方法，其特征在于：所述掌纹手形序列是从手形候选集合中选择多张不同手形的手形图像生成的。

11. 如权利要求 1 所述的安全认证方法，其特征在于：所述掌纹手形序列是随机生成的。

12. 如权利要求 1 所述的安全认证方法，其特征在于：所述向用户展示手形图像是以手形指示图例形式在用户终端展示的。

13. 如权利要求 1 所述的安全认证方法，其特征在于：所述采集用户带掌纹的认证手形图像的步骤还包括：

采集用户带掌纹的认证手形图像时，采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；

如果采集区域的手掌不连续存在则提示用户认证失败；

如果采集区域的手掌连续存在则继续采集其他掌纹手形图像。

14. 如权利要求 1 所述的安全认证方法，其特征在于：所述采集用户的预置掌纹图像的步骤还包括对预置手形图像验证的步骤，具体包括：

将预置手形图像依次展示给用户；

用户按照展示的预置手形图像摆出相应的手势并采集用户手形图像；

提取用户手形图像的手形特征并与预置手形图像比对；

如果匹配，则认为用户可以准确摆出当前预置手形图像；

如果不匹配，则认为用户不能摆出当前预置手形图像；

保存预置手形图像验证的结果。

15. 如权利要求 1 所述的安全认证方法，其特征在于：所述采集用户带掌纹的认证手形

图像的步骤之后还包括对认证手形图像预处理的步骤，具体包括：

对采集的认证手形图像粗分割处理；

对粗分割处理后的认证手形图像前景和背景区分并均衡处理；

对均衡处理后的认证手形图像中值滤波处理；

对中值滤波后的认证手形图像的前景手形区域进行二值化处理；

对二值化后的认证手形图像作连通区域检测，获取带掌纹的手形图像；

对带掌纹的手形图像进行边缘检测得到二值化后的手形区域。

16. 如权利要求 1 所述的安全认证方法，其特征在于：

所述采集用户带掌纹的认证手形图像的步骤之后还包括对带掌纹的认证图像加密的步骤；

所述提取手形特征的步骤之前还包括对带掌纹的认证图像解密的步骤。

17. 如权利要求 1 所述的安全认证方法，其特征在于：所述提取手形特征的步骤包括：

将带掌纹的认证手形图像与预先设置的所有手形掩膜作匹配度比较，找出相匹配的手形掩膜，将该手形掩膜对应的手形作为识别的手形。

18. 如权利要求 17 所述的安全认证方法，其特征在于，所述与预先设置的所有手形掩膜作匹配度比较的步骤具体包括：

将提取的手形图像填充预置的手形图像对应的手形掩膜；

填充结果确定相应的匹配度。

19. 如权利要求 18 所述的安全认证方法，其特征在于，所述将提取的手形图像填充预置的手形图像对应的手形掩膜的步骤还包括：

计算提取的掌纹手形图像中各手指和手掌的长宽；

按掌纹手形图像中各手指和手掌的长宽调整手形掩膜的长宽；

将带掌纹的认证手形图像填充手形掩膜的长宽；

根据填充结果确定相应的匹配度。

20. 如权利要求 1 所述的安全认证方法，其特征在于，所述反馈匹配结果之前还包括：

将认证掌纹图像识别匹配处理后判断生成的掌纹手形序列是否已经采集、识别、匹配完成；

如果未完成掌纹手形序列，则向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；

如果掌纹手形序列已完成，则查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作并通过用户终端提示用户认证成功；如果无匹配成功的掌纹信息匹配结果则通过用户终端向用户提示认证失败。

21. 一种基于手势识别的安全认证方法，其特征在于：包括注册用户特征信息的步骤和认证用户身份的步骤；

所述注册用户特征信息的步骤包括：

用户终端采集用户的预置掌纹图像并传至服务端；

服务端对预置掌纹图像提取掌纹特征并保存预置掌纹特征并向用户终端反馈注册结果；

所述认证用户身份的步骤包括：

用户终端向服务端发起认证请求；

服务端按预置手形图像生成掌纹手形序列传输至用户终端并依序向用户展示手形图像；

用户按用户终端展示的手形图像依序做相应手势动作，用户终端采集用户带掌纹的认证手形图像传输至服务端；

服务端对认证手形图像提取手形、掌纹特征并与预置手形、掌纹特征匹配；

服务端根据匹配结果向用户终端反馈认证结果。

22. 如权利要求 21 所述的安全认证方法，其特征在于：所述采集用户的预置掌纹图像的步骤具体包括：

用户将平整的手掌掌面放置于用户终端的图像采集位置；

用户终端采集用户手掌掌面图像；

用户终端对手掌掌面图像预处理。

23. 如权利要求 22 所述的安全认证方法，其特征在于：所述对手掌掌面图像预处理的步骤具体包括：

用户终端对采集的手掌掌面图像粗分割处理；

用户终端对粗分割处理后的手掌掌面图像前景和背景区分并均衡处理；

用户终端对均衡后的手掌掌面图像中值滤波处理；

用户终端对中值滤波后的手掌掌面图像的前景手形区域进行二值化处理；

用户终端对二值化后的手掌掌面图像作连通区域检测，获取带掌纹的手形图像；

用户终端对带掌纹的手形图像的手掌掌面图像进行边缘检测得到二值化后的手形区域。

24. 如权利要求 23 所述的安全认证方法，其特征在于：所述对采集的手掌掌面图像粗分割处理的步骤具体包括：

用户终端将手掌掌面图像进行颜色空间转换，从 RGB 空间转换至 HSV 空间；

用户终端利用 H 分量提取手的肤色区域。

25. 如权利要求 23 所述的安全认证方法，其特征在于：所述对采集的手掌掌面图像前景和背景区分并均衡处理的步骤具体包括：

用户终端将粗分割后的手掌掌面图像转换为灰度图像；将肤色区域以外的区域设置为背景区域；

用户终端对手掌掌面图像进行直方图均衡处理得到均衡后的灰度图像。

26. 如权利要求 21 所述的安全认证方法，其特征在于：所述预置掌纹图像或认证手形图像是通过摄像头采集的。

27. 如权利要求 21 所述的安全认证方法，其特征在于：所述提取掌纹特征的步骤具体包括：

服务端定位预置掌纹图像中的掌面区域；

服务端切割预置掌纹图像中的掌面区域；

服务端提取预置掌纹图像中的掌纹特征。

28. 如权利要求 27 所述的安全认证方法，其特征在于，所述定位预置掌纹图像中的掌面区域的步骤具体包括：

a1)、服务端对预置掌纹图像从上到下水平穿线边缘图像，找到一组包含有 8 个边界点的穿线；将相邻 2 个边界点作为一组，共四组；将这四组作为是四指的初始穿线组；

b1)、服务端对于四指中的每一指，以初始穿线组为起始位置，向上和向下分别进行搜索，直至搜索到上下边界；

c1)、服务端以相同的方法，从下至上水平穿线边缘图像，找到一组包含有 4 个边界点的穿线；

d1)、同步骤 b1)，服务端以拇指初始穿线指为起始位置，向上和向下分别进行搜索，直至搜索到上下边界，进而定位出拇指关键点。

29. 如权利要求 28 所述的安全认证方法，其特征在于，所述切割预置掌纹图像中的掌面区域的步骤具体包括：

服务端找出食指、中指之间的关键点 a、无名指、小指之间的关键点 c；

服务端找出关键点 a 和关键点 c 组成线段的中点 b；

服务端以 b 点为原点，作线段 ac 的法线 f；

服务端然后以 c 点为起点，沿法线 f，朝向手掌方向偏移一定距离处的点 e；

服务端以 e 为中心，生成一个边长为 P 且与线段 ac 平行的矩形区域；

服务端提取 P×P 区域为掌面区域。

30. 如权利要求 21 所述的安全认证方法，其特征在于：所述掌纹手形序列是服务端从手形候选集合中选择多张不同手形的手形图像生成的。

31. 如权利要求 21 所述的安全认证方法，其特征在于：所述掌纹手形序列是随机生成的。

32. 如权利要求 21 所述的安全认证方法，其特征在于：所述向用户展示的手形图像是以手形指示图例形式在用户终端展示的。

33. 如权利要求 21 所述的安全认证方法，其特征在于：所述采集用户带掌纹的认证手形图像的步骤还包括：

采集用户带掌纹的认证手形图像时，服务端采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；

如果采集区域的手掌不连续存在则提示用户认证失败；

如果采集区域的手掌连续存在则继续采集其他掌纹手形图像。

34. 如权利要求 21 所述的安全认证方法，其特征在于：所述采集用户的预置掌纹图像的步骤还包括对服务端预置手形图像验证的步骤，具体包括：

服务端通过用户终端将预置手形图像依次展示给用户；

用户按用户终端照展示的预置手形图像摆出相应的手势，并通过用户终端采集用户手形图像并传至服务端；

服务端提取用户手形图像的手形特征并与发送给用户终端的预置手形图像比对；

如果匹配，则认为用户可以准确摆出当前预置手形图像；

如果不匹配，则认为用户不能摆出当前预置手形图像；

服务端保存预置手形图像验证的结果并反馈给用户终端。

35. 如权利要求 21 所述的安全认证方法，其特征在于：所述采集用户带掌纹的认证手形图像的步骤之后还包括对认证手形图像预处理的步骤，具体包括：

用户终端对采集的认证手形图像粗分割处理；

用户终端对粗分割处理后的认证手形图像前景和背景区分并均衡处理；

用户终端对均衡处理后的认证手形图像中值滤波处理；

用户终端对中值滤波后的认证手形图像的前景手形区域进行二值化处理；

用户终端对二值化后的认证手形图像作连通区域检测，获取带掌纹的手形图像；

用户终端对带掌纹的手形图像进行边缘检测得到二值化后的手形区域。

36. 如权利要求 21 所述的安全认证方法，其特征在于：

所述采集用户带掌纹的认证手形图像的步骤之后还包括用户终端对带掌纹的认证图像加密的步骤；

所述提取手形特征的步骤之前还包括服务端对带掌纹的认证图像解密的步骤。

37. 如权利要求 21 所述的安全认证方法，其特征在于：所述提取手形特征的步骤包括：

服务端将带掌纹的认证手形图像与服务端预先设置的所有手形掩膜作匹配度比较，找出相匹配的手形掩膜，将该手形掩膜对应的手形作为识别的手形。

38. 如权利要求 27 所述的安全认证方法，其特征在于，所述与服务端预先设置的所有手形掩膜作匹配度比较的步骤具体包括：

服务端将提取的手形图像填充预置的手形图像对应的手形掩膜；

填充结果确定相应的匹配度。

39. 如权利要求 28 所述的安全认证方法，其特征在于，所述将提取的手形图像填充预置的手形图像对应的手形掩膜的步骤还包括：

服务端计算提取的掌纹手形图像中各手指和手掌的长宽；

服务端按掌纹手形图像中各手指和手掌的长宽调整手形掩膜的长宽；

服务端将带掌纹的认证手形图像填充手形掩膜的长宽；

服务端根据填充结果确定相应的匹配度。

40. 如权利要求 21 所述的安全认证方法，其特征在于，所述反馈匹配结果之前还包括：

服务端将认证掌纹图像识别匹配处理后判断生成的掌纹手形序列是否已经采集、识别、匹配完成；

如果未完成掌纹手形序列，则向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；

如果掌纹手形序列已完成，则查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作并通过用户终端提示用户认证成功；如果无匹配成功的掌纹信息匹配结果则通过用户终端向用户提示认证失败。

41. 一种基于手势识别的安全认证方法，其特征在于：包括注册用户特征信息的步骤和认证用户身份的步骤；

所述注册用户特征信息的步骤包括：

用户终端采集用户的预置掌纹图像并传至服务端；

服务端对预置掌纹图像提取掌纹特征并保存预置掌纹特征并向用户终端反馈注册结果；

所述认证用户身份的步骤包括：

用户终端向交易服务端发起交易请求；

交易服务端向服务端发送身份验证请求；

服务端按预置手形图像生成掌纹手形序列传输至用户终端并依序向用户展示手形图像；

用户按用户终端展示的手形图像依序做相应手势动作，用户终端采集用户带掌纹的认证手形图像传输至服务端；

服务端对认证手形图像提取手形、掌纹特征并与预置手形、掌纹特征匹配；

服务端根据匹配结果向用户终端和交易服务服务端反馈认证结果；

交易服务端按认证结果执行交易，并向用户终端反馈交易结果。

42. 如权利要求 41 所述的安全认证方法，其特征在于：所述采集用户的预置掌纹图像的步骤具体包括：

用户将平整的手掌掌面放置于用户终端的图像采集位置；

用户终端采集用户手掌掌面图像；

用户终端对手掌掌面图像预处理。

43. 如权利要求 42 所述的安全认证方法，其特征在于：所述对手掌掌面图像预处理的步骤具体包括：

用户终端对采集的手掌掌面图像粗分割处理；

用户终端对粗分割处理后的手掌掌面图像前景和背景区分并均衡处理；

用户终端对均衡后的手掌掌面图像中值滤波处理；

用户终端对中值滤波后的手掌掌面图像的前景手形区域进行二值化处理；

用户终端对二值化后的手掌掌面图像作连通区域检测，获取带掌纹的手形图像；

用户终端对带掌纹的手形图像的手掌掌面图像进行边缘检测得到二值化后的手形区域。

44. 如权利要求 43 所述的安全认证方法，其特征在于：所述对采集的手掌掌面图像粗分割处理的步骤具体包括：

用户终端将手掌掌面图像进行颜色空间转换，从 RGB 空间转换至 HSV 空间；

用户终端利用 H 分量提取手的肤色区域。

45. 如权利要求 43 所述的安全认证方法，其特征在于：所述对采集的手掌掌面图像前景和背景区分并均衡处理的步骤具体包括：

用户终端将粗分割后的手掌掌面图像转换为灰度图像；将肤色区域以外的区域设置为背景区域；

用户终端对手掌掌面图像进行直方图均衡处理得到均衡后的灰度图像。

46. 如权利要求 41 所述的安全认证方法，其特征在于：所述预置掌纹图像或认证手形图像是通过摄像头采集的。

47. 如权利要求 41 所述的安全认证方法，其特征在于：所述提取掌纹特征的步骤具体包括：

服务端定位预置掌纹图像中的掌面区域；

服务端切割预置掌纹图像中的掌面区域；

服务端提取预置掌纹图像中的掌纹特征。

48. 如权利要求 47 所述的安全认证方法，其特征在于，所述定位预置掌纹图像中的掌面区域的步骤具体包括：

a2)、服务端对预置掌纹图像从上到下水平穿线边缘图像，找到一组包含有 8 个边界点的穿线；将相邻 2 个边界点作为一组，共四组；将这四组作为是四指的初始穿线组；

b2)、服务端对于四指中的每一指，以初始穿线组为起始位置，向上和向下分别进行搜索，直至搜索到上下边界；

c2)、服务端以相同的方法，从下至上水平穿线边缘图像，找到一组包含有 4 个边界点的穿线；

d2)、同步骤 b2)，服务端以拇指初始穿线指为起始位置，向上和向下分别进行搜索，直至搜索到上下边界，进而定位出拇指关键点。

49. 如权利要求 48 所述的安全认证方法，其特征在于，所述切割预置掌纹图像中的掌面区域的步骤具体包括：

服务端找出食指、中指之间的关键点 a、无名指、小指之间的关键点 c；

服务端找出关键点 a 和关键点 c 组成线段的中点 b；

服务端以 b 点为原点，作线段 ac 的法线 f；

服务端然后以 c 点为起点，沿法线 f，朝向手掌方向偏移一定距离处的点 e；

服务端以 e 为中心，生成一个边长为 P 且与线段 ac 平行的矩形区域；

服务端提取 P×P 区域为掌面区域。

50. 如权利要求 41 所述的安全认证方法，其特征在于：所述掌纹手形序列是服务端从手形候选集合中选择多张不同手形的手形图像生成的。

51. 如权利要求 41 所述的安全认证方法，其特征在于：所述掌纹手形序列是随机生成的。

52. 如权利要求 41 所述的安全认证方法，其特征在于：所述向用户展示的手形图像是以手形指示图例形式在用户终端展示的。

53. 如权利要求 41 所述的安全认证方法，其特征在于：所述采集用户带掌纹的认证手形图像的步骤还包括：

采集用户带掌纹的认证手形图像时，服务端采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；

如果采集区域的手掌不连续存在则提示用户认证失败；

如果采集区域的手掌连续存在则继续采集其他掌纹手形图像。

54. 如权利要求 41 所述的安全认证方法，其特征在于：所述采集用户的预置掌纹图像的步骤还包括对服务端预置手形图像验证的步骤，具体包括：

服务端通过用户终端将预置手形图像依次展示给用户；

用户按用户终端照展示的预置手形图像摆出相应的手势，并通过用户终端采集用户手形图像并传至服务端；

服务端提取用户手形图像的手形特征并与发送给用户终端的预置手形图像比对；

如果匹配，则认为用户可以准确摆出当前预置手形图像；

如果不匹配，则认为用户不能摆出当前预置手形图像；

服务端保存预置手形图像验证的结果并反馈给用户终端。

55. 如权利要求 41 所述的安全认证方法，其特征在于：所述采集用户带掌纹的认证手形图像的步骤之后还包括对认证手形图像预处理的步骤，具体包括：

用户终端对采集的认证手形图像粗分割处理；

用户终端对粗分割处理后的认证手形图像前景和背景区分并均衡处理；

用户终端对均衡处理后的认证手形图像中值滤波处理；

用户终端对中值滤波后的认证手形图像的前景手形区域进行二值化处理；

用户终端对二值化后的认证手形图像作连通区域检测，获取带掌纹的手形图像；

用户终端对带掌纹的手形图像进行边缘检测得到二值化后的手形区域。

56. 如权利要求 41 所述的安全认证方法，其特征在于：

所述采集用户带掌纹的认证手形图像的步骤之后还包括用户终端对带掌纹的认证图像加密的步骤；

所述提取手形特征的步骤之前还包括服务端对带掌纹的认证图像解密的步骤。

57. 如权利要求 41 所述的安全认证方法，其特征在于：所述提取手形特征的步骤包括：

服务端将带掌纹的认证手形图像与服务端预先设置的所有手形掩膜作匹配度比较，找出相匹配的手形掩膜，将该手形掩膜对应的手形作为识别的手形。

58. 如权利要求 47 所述的安全认证方法，其特征在于，所述与服务端预先设置的所有手形掩膜作匹配度比较的步骤具体包括：

服务端将提取的手形图像填充预置的手形图像对应的手形掩膜；

填充结果确定相应的匹配度。

59. 如权利要求 48 所述的安全认证方法，其特征在于，所述将提取的手形图像填充预置的手形图像对应的手形掩膜的步骤还包括：

服务端计算提取的掌纹手形图像中各手指和手掌的长宽；

服务端按掌纹手形图像中各手指和手掌的长宽调整手形掩膜的长宽；

服务端将带掌纹的认证手形图像填充手形掩膜的长宽；

服务端根据填充结果确定相应的匹配度。

60. 如权利要求 41 所述的安全认证方法，其特征在于，所述反馈匹配结果之前还包括：

服务端将认证掌纹图像识别匹配处理后判断生成的掌纹手形序列是否已经采集、识别、匹配完成；

如果未完成掌纹手形序列，则向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；

如果掌纹手形序列已完成，则查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作并通过用户终端提示用户认证成功；如果无匹配成功的掌纹信息匹配结果则通过用户终端向用户提示认证失败。

61. 如权利要求 41 所述的安全认证方法，其特征在于，所述交易服务端按认证结果执行交易，并向用户终端反馈交易结果的步骤包括：

服务端对用户身份认证后向交易服务端传送认证结果；

交易服务端根据认证结果处理交易请求；

如果认证结果是认证通过，则交易服务端执行相应的交易操作；

如果认证失败，则向用户终端反馈重新认证或交易失败的信息。

62. 一种基于手势识别的安全认证系统，其特征在于：包括服务端和用户终端；

所述服务端与所述用户终端通信连接；

所述用户终端采集用户的预置掌纹图像并发送至所述服务端，所述服务端按掌纹识别方法提取掌纹特征并保存预置掌纹特征；

所述用户终端向所述服务端发起认证请求，所述服务端生成掌纹手形序列并传输至所述用户终端，所述用户终端依序展示手形图像，用户按所述用户终端展示的手形图像依序做相应手势动作，所述用户终端采集用户的带掌纹的手形图像并传输至所述服务端，所述服务端按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，所述服务端按匹配结果向所述用户终端反馈认证结果。

63. 如权利要求62所述的安全认证系统，其特征在于：所述用户终端包括：数据收发模块、业务逻辑模块图像采集模块；

交互界面模块、数据收发模块、图像采集模块分别与业务逻辑模块通信连接，图像采集模块与数据收发模块通信连接；

用户通过交互界面模块向业务逻辑模块发起指令，业务逻辑模块控制通过数据收发模块向服务端发送注册或认证请求，业务逻辑模块控制图像采集模块采集掌纹手形图像并通过所述数据收发模块向服务端传输；

业务逻辑模块控制数据交互模块接收服务端传输的掌纹手形序列并传输至交互界面模块依序向用户展示手形图像。

64. 如权利要求63所述的安全认证系统，其特征在于：所述用户终端还包括数据加密模块，业务逻辑模块、图像采集模块与数据加密模块通信连接，数据加密模块与数据收发模块连接；

图像采集模块采集的图像通过数据加密模块加密后通过数据收发模块传输。

65. 如权利要求63所述的安全认证系统，其特征在于：所述用户终端还包括图像预处理模块；

业务逻辑模块、图像采集模块与图像预处理模块通信连接；

业务逻辑模块控制图像预处理模块将图像采集模块采集的图像信息作预处理，将预处理后的图像通过数据收发单元传输。

66. 如权利要求62所述的安全认证系统，其特征在于：所述服务端包括：

带身份认证功能的安全认证服务器和数据库，数据库包括掌纹特征数据库和手形设置数据库；

掌纹特征数据库和手形设置数据库与安全认证服务器通信连接；

安全认证服务器包括数据收发模块、手形识别模块、掌纹识别模块和动态手形生成模块；

所述数据收发模块分别与手形识别模块、掌纹识别模块和动态手形生成模块连接，所述手形识别模块、动态手形生成模块分别与所述手形设置数据库连接，所述掌纹识别模块与掌纹特征数据库连接；

注册用户特征信息时：

数据收发模块将接收的预置掌纹图像传输至掌纹识别模块提取掌纹特征并保存在掌

纹特征数据库中，并通过数据收发模块发送反馈注册结果至用户终端；

认证用户身份时：

动态手形生成模块按预置手形图像生成掌纹手形序列通过数据收发模块传输至用户终端；

数据收发模块将接收的认证手形图像传输至手形识别模块、掌纹识别模块提取手形、掌纹特征并与手形设置数据库、掌纹特征数据库中的预置手形、掌纹特征匹配；

手形识别模块、掌纹识别模块根据匹配结果通过数据收发模块向用户终端反馈认证结果。

67. 如权利要求 64 所述的安全认证系统，其特征在于：所述服务端还包括与用户终端对应的数据解密模块；

数据收发模块和掌纹识别模块分别与数据解密模块连接；

所述安全认证服务器收到用户终端加密的图像后，通过数据收发模块发送至数据解密模块，由数据解密模块解密处理后再处理。

68. 如权利要求 66 所述的安全认证系统，其特征在于：所述服务端还包括手掌跟踪模块：

所述手掌跟踪模块与所述数据收发模块连接；

所述手掌跟踪模块在采集用户带掌纹的认证手形图像时，采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；

如果采集区域的手掌不连续存在则通过数据收发模块提示用户认证失败；

如果采集区域的手掌连续存在则通过数据收发模块提示用户继续采集其他掌纹手形图像。

69. 如权利要求 66 所述的安全认证系统，其特征在于：所述服务端还包括识别决策模块：

所述识别决策模块分别与所述手形识别模块、所述掌纹识别模块连接；

所述服务端将认证掌纹图像识别匹配处理后，所述识别决策模块判断生成的掌纹手形序列是否已经采集、识别、匹配完成；

如果未完成掌纹手形序列，则所述识别决策模块向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；

如果掌纹手形序列已完成，则所述识别决策模块查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作，则通过数据收发模块向用户终端传输认证成功的消息；如果无匹配成功的掌纹信息匹配结果则通过数据收发模块向用户终端传输认证失败的消息。

70. 一种基于手势识别的安全认证系统，其特征在于：包括服务端和用户终端；

所述服务器与所述用户终端通信连接；

还包括与所述服务器和所述用户终端通信连接的交易服务端；

所述用户终端采集用户的预置掌纹图像并发送至所述服务端，所述服务端按掌纹识别方法提取掌纹特征并保存预置掌纹特征；

用户通过所述用户终端向所述交易服务端发起交易认证请求，所述交易服务端向所述服务端发起身份能认证请求，所述服务端生成掌纹手形序列并传输至所述用户终端，所述

用户终端依序展示手形图像，用户按所述用户终端展示的手形图像依序做相应手势动作，所述用户终端采集用户的带掌纹的手形图像并传输至所述服务端，所述服务端按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，所述服务端向所述交易服务端用户终端反馈匹配结果，所述交易服务端根据反馈的匹配结果通过用户终端发动交易结果信息。

71. 如权利要求 70 所述的安全认证系统，其特征在于：所述用户终端包括：数据收发模块、业务逻辑模块图像采集模块；

交互界面模块、数据收发模块、图像采集模块分别与业务逻辑模块通信连接，图像采集模块与数据收发模块通信连接；

用户通过交互界面模块向业务逻辑模块发起指令，业务逻辑模块控制通过数据收发模块向服务端发送注册或认证请求，业务逻辑模块控制图像采集模块采集掌纹手形图像并通过所述数据收发模块向服务端传输；

业务逻辑模块控制数据交互模块接收服务端传输的掌纹手形序列并传输至交互界面模块依序向用户展示手形图像。

72. 如权利要求 71 所述的安全认证系统，其特征在于：所述用户终端还包括数据加密模块，业务逻辑模块、图像采集模块与数据加密模块通信连接，数据加密模块与数据收发模块连接；

图像采集模块采集的图像通过数据加密模块加密后通过数据收发模块传输。

73. 如权利要求 71 所述的安全认证系统，其特征在于：所述用户终端还包括图像预处理模块；

业务逻辑模块、图像采集模块与图像预处理模块通信连接；

业务逻辑模块控制图像预处理模块将图像采集模块采集的图像信息作预处理，将预处理后的图像通过数据收发单元传输。

74. 如权利要求 70 所述的安全认证系统，其特征在于：所述服务端包括：

带身份认证功能的安全认证服务器和数据库，数据库包括掌纹特征数据库和手形设置数据库；

掌纹特征数据库和手形设置数据库与安全认证服务器通信连接；

安全认证服务器包括数据收发模块、手形识别模块、掌纹识别模块和动态手形生成模块；

所述数据收发模块分别与手形识别模块、掌纹识别模块和动态手形生成模块连接，所述手形识别模块、动态手形生成模块分别与所述手形设置数据库连接，所述掌纹识别模块与掌纹特征数据库连接；

注册用户特征信息时：

数据收发模块将接收的预置掌纹图像传输至掌纹识别模块提取掌纹特征并保存在掌纹特征数据库中，并通过数据收发模块发送反馈注册结果至用户终端；

认证用户身份时：

动态手形生成模块按预置手形图像生成掌纹手形序列通过数据收发模块传输至用户终端；

数据收发模块将接收的认证手形图像传输至手形识别模块、掌纹识别模块提取手形、掌纹特征并与手形设置数据库、掌纹特征数据库中的预置手形、掌纹特征匹配；

手形识别模块、掌纹识别模块根据匹配结果通过数据收发模块向用户终端反馈认证结果。

75. 如权利要求 72 所述的安全认证系统，其特征在于：所述服务端还包括与用户终端对应的数据解密模块；

数据收发模块和掌纹识别模块分别与数据解密模块连接；

所述安全认证服务器收到用户终端加密的图像后，通过数据收发模块发送至数据解密模块，由数据解密模块解密处理后再处理。

76. 如权利要求 74 所述的安全认证系统，其特征在于：所述服务端还包括手掌跟踪模块：

所述手掌跟踪模块与所述数据收发模块连接；

所述手掌跟踪模块在采集用户带掌纹的认证手形图像时，采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；

如果采集区域的手掌不连续存在则通过数据收发模块提示用户认证失败；

如果采集区域的手掌连续存在则通过数据收发模块提示用户继续采集其他掌纹手形图像。

77. 如权利要求 74 所述的安全认证系统，其特征在于：所述服务端还包括识别决策模块：

所述识别决策模块分别与所述手形识别模块、所述掌纹识别模块连接；

所述服务端将认证掌纹图像识别匹配处理后，所述识别决策模块判断生成的掌纹手形序列是否已经采集、识别、匹配完成；

如果未完成掌纹手形序列，则所述识别决策模块向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；

如果掌纹手形序列已完成，则所述识别决策模块查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作，则通过数据收发模块向用户终端传输认证成功的消息；如果无匹配成功的掌纹信息匹配结果则通过数据收发模块向用户终端传输认证失败的消息。

78. 一种基于手势识别的安全认证服务器，其特征在于：

所述安全认证服务器用于在安全认证系统中认证用户的权限；

所述安全认证服务器与用户终端通信连接；

所述安全认证服务器接收所述用户终端采集用户的预置掌纹图像，所述安全认证服务器按掌纹识别方法提取掌纹特征并保存预置掌纹特征；

所述安全认证服务器接收所述用户终端向所述安全认证服务器发起认证请求，所述安全认证服务器生成掌纹手形序列并传输至所述用户终端，所述用户终端依序展示手形图像，用户按所述用户终端展示的手形图像依序做相应手势动作，所述用户终端采集用户的带掌纹的手形图像并传输至所述安全认证服务器，所述安全认证服务器按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，所述安全认证服务器按匹配结果向所述用户终端反馈认证结果。

79. 一种基于手势识别的安全认证服务器，其特征在于：

所述安全认证服务器用于在安全认证系统中认证用户的权限；

所述安全认证服务器与用户终端和交易服务器通信连接；

所述安全认证服务器接收所述用户终端采集用户的预置掌纹图像，所述安全认证服务器按掌纹识别方法提取掌纹特征并保存预置掌纹特征；

用户通过所述用户终端向所述交易服务器发起交易认证请求，所述安全认证服务器接收所述交易服务器向所述安全认证服务器发起认证请求，所述安全认证服务器生成掌纹手形序列并传输至所述用户终端，所述用户终端依序展示手形图像，用户按所述用户终端展示的手形图像依序做相应手势动作，所述用户终端采集用户的带掌纹的手形图像并传输至所述安全认证服务器，所述安全认证服务器按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，所述服务器向所述交易服务器用户终端反馈匹配结果，所述交易服务器根据反馈的匹配结果通过用户终端发动交易结果信息。

80. 一种基于手势识别的安全认证用户终端，其特征在于：

所述用户终端用于在安全认证系统中认证用户的权限；

所述用户终端与安全认证服务器通信连接；

所述用户终端采集用户的预置掌纹图像传输至所述安全认证服务器，所述安全认证服务器按掌纹识别方法提取掌纹特征并保存预置掌纹特征；

所述安全认证服务器接收所述用户终端向所述安全认证服务器发起认证请求，所述安全认证服务器生成掌纹手形序列并传输至所述用户终端，所述用户终端依序展示手形图像，用户按所述用户终端展示的手形图像依序做相应手势动作，所述用户终端采集用户的带掌纹的手形图像并传输至所述安全认证服务器，所述安全认证服务器按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，所述安全认证服务器按匹配结果向所述用户终端反馈认证结果。

81. 一种基于手势识别的安全认证用户终端，其特征在于：

所述用户终端用于在安全认证系统中认证用户的权限；

所述用户终端与安全安全认证服务器和交易服务器通信连接；

所述用户终端采集用户的预置掌纹图像传输至所述安全认证服务器，所述安全认证服务器按掌纹识别方法提取掌纹特征并保存预置掌纹特征；

所述用户终端向所述交易服务器发起交易认证请求，所述安全认证服务器接收所述交易服务器向所述安全认证服务器发起认证请求，所述安全认证服务器生成掌纹手形序列并传输至所述用户终端，所述用户终端依序展示手形图像，用户按所述用户终端展示的手形图像依序做相应手势动作，所述用户终端采集用户的带掌纹的手形图像并传输至所述安全认证服务器，所述安全认证服务器按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，所述服务器向所述交易服务器用户终端反馈匹配结果，所述交易服务器根据反馈的匹配结果通过用户终端发动交易结果信息。

# 一种基于手势识别的安全认证方法、终端、服务器和系统

## 技术领域

[0001] 本发明涉及一种安全认证方法、终端、服务器和系统，特别涉及一种基于手势特征识别的安全证方法、终端、服务器和系统，属于通信安全认证技术领域。

## 背景技术

[0002] 随着通信网络的迅猛发展，移动互联网已经越来越深入社会的各个角落，各种服务也日益增多。手机上网、手机看视频、移动终端购物、手机支付等已经成为人们熟知的事物。在通信网络中如何进行可靠的远程身份认证显得日益重要，高安全的远程身份认证已经成为网络服务提供商提供各种服务的前提和必要条件。

[0003] 目前，现有的远程身份认证的主要方法包括：文本密码、动态口令（或密码算号器）、智能卡、生物特征或上述方法的各种组合等。采用文本密码的方式进行远程身份认证时，终端将文本密码发送给通信网络的认证服务器进行认证，该方式不仅要求用户记住各种繁琐的文本密码，而且文本密码还容易丢失和被盗用。为了避免这种完全问题，研发出了动态口令验证的方式，由于动态口令在每次身份认证时是由服务器端动态生成的，因此可以防止不法分子在获取用户密码的情况下进行身份认证，但是动态口令卡（或密码算号器）存在容易丢失的问题，在动态口令卡或（或密码算号器）和用户分离时仍然不能安全认证。

[0004] 为了进一步提高安全性，人们发现采用人体固有的生物特征或行为特征是相对较安全的认证方法，其中人脸、虹膜、指纹、指静脉和掌静脉识别等已经被广泛应用于门禁，金融等领域。目前，在移动终端常用的支付认证系统采用短信验证码的方式来防止用户密码被盗，但是在终端丢失或SIM卡被复制的情况下，用户信息和财产的安全性将很难得到保证。目前已经发生过多起不法分子复制SIM卡，进而令移动支付过程中的验证短信发送到不法分子的终端，最终盗取用户钱财的案件。

[0005] 在申请号为201410138350.4的中国发明专利申请中，公开了一种基于人体指纹和虹膜特征的移动支付身份验证方法。该方法相比于单独基于指纹或虹膜的验证方法更安全，但是在认证终端被劫持的情况下，仍然存在用户身份被伪造或假冒的风险。

## 发明内容

[0006] 本发明要解决的技术问题是：提供一种高安全性的基于手势识别的安全认证方法、终端、服务器和系统，可以有效防止冒用和被劫持的风险，提高了身份认证的安全性。

[0007] 为实现上述的发明目的，本发明提供了一种基于手势识别的安全认证方法、终端、服务器和系统。

[0008] 一方面，本发明提供一种基于手势识别的安全认证方法，包括注册用户特征信息的步骤和认证用户身份的步骤；

[0009] 所述注册用户特征信息的步骤包括：

[0010] 采集用户的预置掌纹图像；

[0011] 对预置掌纹图像提取掌纹特征并保存预置掌纹特征；

[0012] 所述认证用户身份的步骤包括：

[0013] 用户发起认证请求；

[0014] 按预置手形图像生成掌纹手形序列并依序向用户展示手形图像；

[0015] 用户按展示的手形图像依序做相应手势动作并采集用户带掌纹的认证手形图像；

[0016] 对认证手形图像提取手形、掌纹特征并与预置手形、掌纹特征匹配；

[0017] 反馈匹配结果。

[0018] 其中较优地，其特征在于：所述采集用户的预置掌纹图像的步骤具体包括：

[0019] 用户将平整的手掌掌面放置于图像采集位置；

[0020] 采集用户手掌掌面图像；

[0021] 对手掌掌面图像预处理。

[0022] 其中较优地，所述对手掌掌面图像预处理的步骤具体包括：

[0023] 对采集的手掌掌面图像粗分割处理；

[0024] 对粗分割处理后的手掌掌面图像前景和背景区分并均衡处理；

[0025] 对均衡后的手掌掌面图像中值滤波处理；

[0026] 对中值滤波后的手掌掌面图像的前景手形区域进行二值化处理；

[0027] 对二值化后的手掌掌面图像作连通区域检测，获取带掌纹的手形图像；

[0028] 对带掌纹的手形图像的手掌掌面图像进行边缘检测得到二值化后的手形区域。

[0029] 其中较优地，所述对采集的手掌掌面图像粗分割处理的步骤具体包括：

[0030] 将手掌掌面图像进行颜色空间转换，从 RGB 空间转换至 HSV 空间；

[0031] 利用 H 分量提取手的肤色区域。

[0032] 其中较优地，所述对采集的手掌掌面图像前景和背景区分并均衡处理的步骤具体包括：

[0033] 将粗分割后的手掌掌面图像转换为灰度图像；将肤色区域以外的区域设置为背景区域；

[0034] 对手掌掌面图像进行直方图均衡处理得到均衡后的灰度图像。

[0035] 其中较优地，所述预置掌纹图像或认证手形图像是通过摄像头采集的。

[0036] 其中较优地，所述提取掌纹特征的步骤具体包括：

[0037] 定位预置掌纹图像中的掌面区域；

[0038] 切割预置掌纹图像中的掌面区域；

[0039] 提取预置掌纹图像中的掌纹特征。

[0040] 其中较优地，所述定位预置掌纹图像中的掌面区域的步骤具体包括：

[0041] a)、对预置掌纹图像从上到下水平穿线边缘图像，找到一组包含有 8 个边界点的穿线；将相邻 2 个边界点作为一组，共四组；将这四组作为是四指的初始穿线组；

[0042] b)、对于四指中的每一指，以初始穿线组为起始位置，向上和向下分别进行搜索，直至搜索到上下边界；

[0043] c)、以相同的方法，从下至上水平穿线边缘图像，找到一组包含有 4 个边界点的穿线；

[0044] d)、同步骤 b)，以拇指初始穿线指为起始位置，向上和向下分别进行搜索，直至搜索到上下边界，进而定位出拇指关键点。

[0045] 其中较优地，所述切割预置掌纹图像中的掌面区域的步骤具体包括：

[0046] 找出食指、中指之间的关键点 a、无名指、小指之间的关键点 c；

[0047] 找出关键点 a 和关键点 c 组成线段的中点 b；

[0048] 以 b 点为原点，作线段 ac 的法线 f；

[0049] 然后以 c 点为起点，沿法线 f，朝向手掌方向偏移一定距离处的点 e；

[0050] 以 e 为中心，生成一个边长为 P 且与线段 ac 平行的矩形区域；

[0051] 提取 P×P 区域为掌面区域。

[0052] 其中较优地，所述掌纹手形序列是从手形候选集合中选择多张不同手形的手形图像生成的。

[0053] 其中较优地，所述掌纹手形序列是随机生成的。

[0054] 其中较优地，所述向用户展示手形图像是以手形指示图例形式在用户终端展示的。

[0055] 其中较优地，所述采集用户带掌纹的认证手形图像的步骤还包括：

[0056] 采集用户带掌纹的认证手形图像时，采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；

[0057] 如果采集区域的手掌不连续存在则提示用户认证失败；

[0058] 如果采集区域的手掌连续存在则继续采集其他掌纹手形图像。

[0059] 其中较优地，所述采集用户的预置掌纹图像的步骤还包括对预置手形图像验证的步骤，具体包括：

[0060] 将预置手形图像依次展示给用户；

[0061] 用户按照展示的预置手形图像摆出相应的手势并采集用户手形图像；

[0062] 提取用户手形图像的手形特征并与预置手形图像比对；

[0063] 如果匹配，则认为用户可以准确摆出当前预置手形图像；

[0064] 如果不匹配，则认为用户不能摆出当前预置手形图像；

[0065] 保存预置手形图像验证的结果。

[0066] 其中较优地，所述采集用户带掌纹的认证手形图像的步骤之后还包括对认证手形图像预处理的步骤，具体包括：

[0067] 对采集的认证手形图像粗分割处理；

[0068] 对粗分割处理后的认证手形图像前景和背景区分并均衡处理；

[0069] 对均衡处理后的认证手形图像中值滤波处理；

[0070] 对中值滤波后的认证手形图像的前景手形区域进行二值化处理；

[0071] 对二值化后的认证手形图像作连通区域检测，获取带掌纹的手形图像；

[0072] 对带掌纹的手形图像进行边缘检测得到二值化后的手形区域。

[0073] 其中较优地，所述采集用户带掌纹的认证手形图像的步骤之后还包括对带掌纹的认证图像加密的步骤；

[0074] 所述提取手形特征的步骤之前还包括对带掌纹的认证图像解密的步骤。

[0075] 其中较优地，所述提取手形特征的步骤包括：

[0076] 将带掌纹的认证手形图像与预先设置的所有手形掩膜作匹配度比较，找出相匹配的手形掩膜，将该手形掩膜对应的手形作为识别的手形。

[0077] 其中较优地，所述与预先设置的所有手形掩膜作匹配度比较的步骤具体包括：

[0078] 将提取的手形图像填充预置的手形图像对应的手形掩膜；

[0079] 填充结果确定相应的匹配度。

[0080] 其中较优地，所述将提取的手形图像填充预置的手形图像对应的手形掩膜的步骤还包括：

[0081] 计算提取的掌纹手形图像中各手指和手掌的长宽；

[0082] 按掌纹手形图像中各手指和手掌的长宽调整手形掩膜的长宽；

[0083] 将带掌纹的认证手形图像填充手形掩膜的长宽；

[0084] 根据填充结果确定相应的匹配度。

[0085] 其中较优地，所述反馈匹配结果之前还包括：

[0086] 将认证掌纹图像识别匹配处理后判断生成的掌纹手形序列是否已经采集、识别、匹配完成；

[0087] 如果未完成掌纹手形序列，则向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；

[0088] 如果掌纹手形序列已完成，则查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作并通过用户终端提示用户认证成功；如果无匹配成功的掌纹信息匹配结果则通过用户终端向用户提示认证失败。

[0089] 另一方面，本发明还提供一种基于手势识别的安全认证方法，包括注册用户特征信息的步骤和认证用户身份的步骤；

[0090] 所述注册用户特征信息的步骤包括：

[0091] 用户终端采集用户的预置掌纹图像并传至服务端；

[0092] 服务端对预置掌纹图像提取掌纹特征并保存预置掌纹特征并向用户终端反馈注册结果；

[0093] 所述认证用户身份的步骤包括：

[0094] 用户终端向服务端发起认证请求；

[0095] 服务端按预置手形图像生成掌纹手形序列传输至用户终端并依序向用户展示手形图像；

[0096] 用户按用户终端展示的手形图像依序做相应手势动作，用户终端采集用户带掌纹的认证手形图像传输至服务端；

[0097] 服务端对认证手形图像提取手形、掌纹特征并与预置手形、掌纹特征匹配；

[0098] 服务端根据匹配结果向用户终端反馈认证结果。

[0099] 其中较优地，所述采集用户的预置掌纹图像的步骤具体包括：

[0100] 用户将平整的手掌掌面放置于用户终端的图像采集位置；

[0101] 用户终端采集用户手掌掌面图像；

[0102] 用户终端对手掌掌面图像预处理。

[0103] 其中较优地，所述对手掌掌面图像预处理的步骤具体包括：

[0104] 用户终端对采集的手掌掌面图像粗分割处理；

[0105] 用户终端对粗分割处理后的手掌掌面图像前景和背景区分并均衡处理；

[0106] 用户终端对均衡后的手掌掌面图像中值滤波处理；

[0107] 用户终端对中值滤波后的手掌掌面图像的前景手形区域进行二值化处理；

[0108] 用户终端对二值化后的手掌掌面图像作连通区域检测，获取带掌纹的手形图像；

[0109] 用户终端对带掌纹的手形图像的手掌掌面图像进行边缘检测得到二值化后的手形区域。

[0110] 其中较优地，所述对采集的手掌掌面图像粗分割处理的步骤具体包括：

[0111] 用户终端将手掌掌面图像进行颜色空间转换，从 RGB 空间转换至 HSV 空间；

[0112] 用户终端利用 H 分量提取手的肤色区域。

[0113] 其中较优地，所述对采集的手掌掌面图像前景和背景区分并均衡处理的步骤具体包括：

[0114] 用户终端将粗分割后的手掌掌面图像转换为灰度图像；将肤色区域以外的区域设置为背景区域；

[0115] 用户终端对手掌掌面图像进行直方图均衡处理得到均衡后的灰度图像。

[0116] 其中较优地，所述预置掌纹图像或认证手形图像是通过摄像头采集的。

[0117] 其中较优地，所述提取掌纹特征的步骤具体包括：

[0118] 服务端定位预置掌纹图像中的掌面区域；

[0119] 服务端切割预置掌纹图像中的掌面区域；

[0120] 服务端提取预置掌纹图像中的掌纹特征。

[0121] 其中较优地，所述定位预置掌纹图像中的掌面区域的步骤具体包括：

[0122] a1)、服务端对预置掌纹图像从上到下水平穿线边缘图像，找到一组包含有 8 个边界点的穿线；将相邻 2 个边界点作为一组，共四组；将这四组作为是四指的初始穿线组；

[0123] b1)、服务端对于四指中的每一指，以初始穿线组为起始位置，向上和向下分别进行搜索，直至搜索到上下边界；

[0124] c1)、服务端以相同的方法，从下至上水平穿线边缘图像，找到一组包含有 4 个边界点的穿线；

[0125] d1)、同步骤 b1)，服务端以拇指初始穿线指为起始位置，向上和向下分别进行搜索，直至搜索到上下边界，进而定位出拇指关键点。

[0126] 其中较优地，所述切割预置掌纹图像中的掌面区域的步骤具体包括：

[0127] 服务端找出食指、中指之间的关键点 a、无名指、小指之间的关键点 c；

[0128] 服务端找出关键点 a 和关键点 c 组成线段的中点 b；

[0129] 服务端以 b 点为原点，作线段 ac 的法线 f；

[0130] 服务端然后以 c 点为起点，沿法线 f，朝向手掌方向偏移一定距离处的点 e；

[0131] 服务端以 e 为中心，生成一个边长为 P 且与线段 ac 平行的矩形区域；

[0132] 服务端提取 P×P 区域为掌面区域。

[0133] 其中较优地，所述掌纹手形序列是服务端从手形候选集合中选择多张不同手形的手形图像生成的。

[0134] 其中较优地，所述掌纹手形序列是随机生成的。

[0135] 其中较优地，所述向用户展示的手形图像是以手形指示图例形式在用户终端展示

的。

[0136] 其中较优地，所述采集用户带掌纹的认证手形图像的步骤还包括：

[0137] 采集用户带掌纹的认证手形图像时，服务端采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；

[0138] 如果采集区域的手掌不连续存在则提示用户认证失败；

[0139] 如果采集区域的手掌连续存在则继续采集其他掌纹手形图像。

[0140] 其中较优地，所述采集用户的预置掌纹图像的步骤还包括对服务端预置手形图像验证的步骤，具体包括：

[0141] 服务端通过用户终端将预置手形图像依次展示给用户；

[0142] 用户按用户终端照展示的预置手形图像摆出相应的手势，并通过用户终端采集用户手形图像并传至服务端；

[0143] 服务端提取用户手形图像的手形特征并与发送给用户终端的预置手形图像比对；

[0144] 如果匹配，则认为用户可以准确摆出当前预置手形图像；

[0145] 如果不匹配，则认为用户不能摆出当前预置手形图像；

[0146] 服务端保存预置手形图像验证的结果并反馈给用户终端。

[0147] 其中较优地，所述采集用户带掌纹的认证手形图像的步骤之后还包括对认证手形图像预处理的步骤，具体包括：

[0148] 用户终端对采集的认证手形图像粗分割处理；

[0149] 用户终端对粗分割处理后的认证手形图像前景和背景区分并均衡处理；

[0150] 用户终端对均衡处理后的认证手形图像中值滤波处理；

[0151] 用户终端对中值滤波后的认证手形图像的前景手形区域进行二值化处理；

[0152] 用户终端对二值化后的认证手形图像作连通区域检测，获取带掌纹的手形图像；

[0153] 用户终端对带掌纹的手形图像进行边缘检测得到二值化后的手形区域。

[0154] 其中较优地，所述采集用户带掌纹的认证手形图像的步骤之后还包括用户终端对带掌纹的认证图像加密的步骤；

[0155] 所述提取手形特征的步骤之前还包括服务端对带掌纹的认证图像解密的步骤。

[0156] 其中较优地，所述提取手形特征的步骤包括：

[0157] 服务端将带掌纹的认证手形图像与服务端预先设置的所有手形掩膜作匹配度比较，找出相匹配的手形掩膜，将该手形掩膜对应的手形作为识别的手形。

[0158] 其中较优地，所述与服务端预先设置的所有手形掩膜作匹配度比较的步骤具体包括：

[0159] 服务端将提取的手形图像填充预置的手形图像对应的手形掩膜；

[0160] 填充结果确定相应的匹配度。

[0161] 其中较优地，所述将提取的手形图像填充预置的手形图像对应的手形掩膜的步骤还包括：

[0162] 服务端计算提取的掌纹手形图像中各手指和手掌的长宽；

[0163] 服务端按掌纹手形图像中各手指和手掌的长宽调整手形掩膜的长宽；

[0164] 服务端将带掌纹的认证手形图像填充手形掩膜的长宽；

[0165] 服务端根据填充结果确定相应的匹配度。

[0166] 其中较优地，所述反馈匹配结果之前还包括：

[0167] 服务端将认证掌纹图像识别匹配处理后判断生成的掌纹手形序列是否已经采集、识别、匹配完成；

[0168] 如果未完成掌纹手形序列，则向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；

[0169] 如果掌纹手形序列已完成，则查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作并通过用户终端提示用户认证成功；如果无匹配成功的掌纹信息匹配结果则通过用户终端向用户提示认证失败。

[0170] 再一方面，一种基于手势识别的安全认证方法，包括注册用户特征信息的步骤和认证用户身份的步骤；

[0171] 所述注册用户特征信息的步骤包括：

[0172] 用户终端采集用户的预置掌纹图像并传至服务端；

[0173] 服务端对预置掌纹图像提取掌纹特征并保存预置掌纹特征并向用户终端反馈注册结果；

[0174] 所述认证用户身份的步骤包括：

[0175] 用户终端向交易服务端发起交易请求；

[0176] 交易服务端向服务端发送身份验证请求；

[0177] 服务端按预置手形图像生成掌纹手形序列传输至用户终端并依序向用户展示手形图像；

[0178] 用户按用户终端展示的手形图像依序做相应手势动作，用户终端采集用户带掌纹的认证手形图像传输至服务端；

[0179] 服务端对认证手形图像提取手形、掌纹特征并与预置手形、掌纹特征匹配；

[0180] 服务端根据匹配结果向用户终端和交易服务服务端反馈认证结果；

[0181] 交易服务端按认证结果执行交易，并向用户终端反馈交易结果。

[0182] 其中较优地，所述采集用户的预置掌纹图像的步骤具体包括：

[0183] 用户将平整的手掌掌面放置于用户终端的图像采集位置；

[0184] 用户终端采集用户手掌掌面图像；

[0185] 用户终端对手掌掌面图像预处理。

[0186] 其中较优地，所述对手掌掌面图像预处理的步骤具体包括：

[0187] 用户终端对采集的手掌掌面图像粗分割处理；

[0188] 用户终端对粗分割处理后的手掌掌面图像前景和背景区分并均衡处理；

[0189] 用户终端对均衡后的手掌掌面图像中值滤波处理；

[0190] 用户终端对中值滤波后的手掌掌面图像的前景手形区域进行二值化处理；

[0191] 用户终端对二值化后的手掌掌面图像作连通区域检测，获取带掌纹的手形图像；

[0192] 用户终端对带掌纹的手形图像的手掌掌面图像进行边缘检测得到二值化后的手形区域。

[0193] 其中较优地，所述对采集的手掌掌面图像粗分割处理的步骤具体包括：

[0194] 用户终端将手掌掌面图像进行颜色空间转换，从 RGB 空间转换至 HSV 空间；

[0195] 用户终端利用 H 分量提取手的肤色区域。

[0196] 其中较优地，所述对采集的手掌掌面图像前景和背景区分并均衡处理的步骤具体包括：

[0197] 用户终端将粗分割后的手掌掌面图像转换为灰度图像；将肤色区域以外的区域设置为背景区域；

[0198] 用户终端对手掌掌面图像进行直方图均衡处理得到均衡后的灰度图像。

[0199] 其中较优地，所述预置掌纹图像或认证手形图像是通过摄像头采集的。

[0200] 其中较优地，所述提取掌纹特征的步骤具体包括：

[0201] 服务端定位预置掌纹图像中的掌面区域；

[0202] 服务端切割预置掌纹图像中的掌面区域；

[0203] 服务端提取预置掌纹图像中的掌纹特征。

[0204] 其中较优地，所述定位预置掌纹图像中的掌面区域的步骤具体包括：

[0205] a2)、服务端对预置掌纹图像从上到下水平穿线边缘图像，找到一组包含有 8 个边界点的穿线；将相邻 2 个边界点作为一组，共四组；将这四组作为是四指的初始穿线组；

[0206] b2)、服务端对于四指中的每一指，以初始穿线组为起始位置，向上和向下分别进行搜索，直至搜索到上下边界；

[0207] c2)、服务端以相同的方法，从下至上水平穿线边缘图像，找到一组包含有 4 个边界点的穿线；

[0208] d2)、同步骤 b2)，服务端以拇指初始穿线指为起始位置，向上和向下分别进行搜索，直至搜索到上下边界，进而定位出拇指关键点。

[0209] 其中较优地，所述切割预置掌纹图像中的掌面区域的步骤具体包括：

[0210] 服务端找出食指、中指之间的关键点 a、无名指、小指之间的关键点 c；

[0211] 服务端找出关键点 a 和关键点 c 组成线段的中点 b；

[0212] 服务端以 b 点为原点，作线段 ac 的法线 f；

[0213] 服务端然后以 c 点为起点，沿法线 f，朝向手掌方向偏移一定距离处的点 e；

[0214] 服务端以 e 为中心，生成一个边长为 P 且与线段 ac 平行的矩形区域；

[0215] 服务端提取 P×P 区域为掌面区域。

[0216] 其中较优地，所述掌纹手形序列是服务端从手形候选集合中选择多张不同手形的手形图像生成的。

[0217] 其中较优地，所述掌纹手形序列是随机生成的。

[0218] 其中较优地，所述向用户展示的手形图像是以手形指示图例形式在用户终端展示的。

[0219] 其中较优地，所述采集用户带掌纹的认证手形图像的步骤还包括：

[0220] 采集用户带掌纹的认证手形图像时，服务端采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；

[0221] 如果采集区域的手掌不连续存在则提示用户认证失败；

[0222] 如果采集区域的手掌连续存在则继续采集其他掌纹手形图像。

[0223] 其中较优地，所述采集用户的预置掌纹图像的步骤还包括对服务端预置手形图像验证的步骤，具体包括：

[0224] 服务端通过用户终端将预置手形图像依次展示给用户；

[0225] 用户按用户终端照展示的预置手形图像摆出相应的手势，并通过用户终端采集用户手形图像并传至服务端；

[0226] 服务端提取用户手形图像的手形特征并与发送给用户终端的预置手形图像比对；

[0227] 如果匹配，则认为用户可以准确摆出当前预置手形图像；

[0228] 如果不匹配，则认为用户不能摆出当前预置手形图像；

[0229] 服务端保存预置手形图像验证的结果并反馈给用户终端。

[0230] 其中较优地，所述采集用户带掌纹的认证手形图像的步骤之后还包括对认证手形图像预处理的步骤，具体包括：

[0231] 用户终端对采集的认证手形图像粗分割处理；

[0232] 用户终端对粗分割处理后的认证手形图像前景和背景区分并均衡处理；

[0233] 用户终端对均衡处理后的认证手形图像中值滤波处理；

[0234] 用户终端对中值滤波后的认证手形图像的前景手形区域进行二值化处理；

[0235] 用户终端对二值化后的认证手形图像作连通区域检测，获取带掌纹的手形图像；

[0236] 用户终端对带掌纹的手形图像进行边缘检测得到二值化后的手形区域。

[0237] 其中较优地，所述采集用户带掌纹的认证手形图像的步骤之后还包括用户终端对带掌纹的认证图像加密的步骤；

[0238] 所述提取手形特征的步骤之前还包括服务端对带掌纹的认证图像解密的步骤。

[0239] 其中较优地，所述提取手形特征的步骤包括：

[0240] 服务端将带掌纹的认证手形图像与服务端预先设置的所有手形掩膜作匹配度比较，找出相匹配的手形掩膜，将该手形掩膜对应的手形作为识别的手形。

[0241] 其中较优地，所述与服务端预先设置的所有手形掩膜作匹配度比较的步骤具体包括：

[0242] 服务端将提取的手形图像填充预置的手形图像对应的手形掩膜；

[0243] 填充结果确定相应的匹配度。

[0244] 其中较优地，所述将提取的手形图像填充预置的手形图像对应的手形掩膜的步骤还包括：

[0245] 服务端计算提取的掌纹手形图像中各手指和手掌的长宽；

[0246] 服务端按掌纹手形图像中各手指和手掌的长宽调整手形掩膜的长宽；

[0247] 服务端将带掌纹的认证手形图像填充手形掩膜的长宽；

[0248] 服务端根据填充结果确定相应的匹配度。

[0249] 其中较优地，所述反馈匹配结果之前还包括：

[0250] 服务端将认证掌纹图像识别匹配处理后判断生成的掌纹手形序列是否已经采集、识别、匹配完成；

[0251] 如果未完成掌纹手形序列，则向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；

[0252] 如果掌纹手形序列已完成，则查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作并通过用户终端提示用户认证成功；如果无匹配成功的

掌纹信息匹配结果则通过用户终端向用户提示认证失败。

[0253] 其中较优地，所述交易服务端按认证结果执行交易，并向用户终端反馈交易结果的步骤包括：

[0254] 服务端对用户身份认证后向交易服务端传送认证结果；

[0255] 交易服务端根据认证结果处理交易请求；

[0256] 如果认证结果是认证通过，则交易服务端执行相应的交易操作；

[0257] 如果认证失败，则向用户终端反馈重新认证或交易失败的信息。

[0258] 再一方面，本发明还提供一种基于手势识别的安全认证系统，包括服务端和用户终端；

[0259] 所述服务端与所述用户终端通信连接；

[0260] 所述用户终端采集用户的预置掌纹图像并发送至所述服务端，所述服务端按掌纹识别方法提取掌纹特征并保存预置掌纹特征；

[0261] 所述用户终端向所述服务端发起认证请求，所述服务端生成掌纹手形序列并传输至所述用户终端，所述用户终端依序展示手形图像，用户按所述用户终端展示的手形图像依序做相应手势动作，所述用户终端采集用户的带掌纹的手形图像并传输至所述服务端，所述服务端按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，所述服务端按匹配结果向所述用户终端反馈认证结果。

[0262] 其中较优地，所述用户终端包括：数据收发模块、业务逻辑模块图像采集模块；

[0263] 交互界面模块、数据收发模块、图像采集模块分别与业务逻辑模块通信连接，图像采集模块与数据收发模块通信连接；

[0264] 用户通过交互界面模块向业务逻辑模块发起指令，业务逻辑模块控制通过数据收发模块向服务端发送注册或认证请求，业务逻辑模块控制图像采集模块采集掌纹手形图像并通过所述数据收发模块向服务端传输；

[0265] 业务逻辑模块控制数据交互模块接收服务端传输的掌纹手形序列并传输至交互界面模块依序向用户展示手形图像。

[0266] 其中较优地，所述用户终端还包括数据加密模块，业务逻辑模块、图像采集模块与数据加密模块通信连接，数据加密模块与数据收发模块连接；

[0267] 图像采集模块采集的图像通过数据加密模块加密后通过数据收发模块传输。

[0268] 其中较优地，所述用户终端还包括图像预处理模块；

[0269] 业务逻辑模块、图像采集模块与图像预处理模块通信连接；

[0270] 业务逻辑模块控制图像预处理模块将图像采集模块采集的图像信息作预处理，将预处理后的图像通过数据收发单元传输。

[0271] 其中较优地，所述服务端包括：

[0272] 带身份认证功能的安全认证服务器和数据库，数据库包括掌纹特征数据库和手形设置数据库；

[0273] 掌纹特征数据库和手形设置数据库与安全认证服务器通信连接；

[0274] 安全认证服务器包括数据收发模块、手形识别模块、掌纹识别模块和动态手形生成模块；

[0275] 所述数据收发模块分别与手形识别模块、掌纹识别模块和动态手形生成模块连

接，所述手形识别模块、动态手形生成模块分别与所述手形设置数据库连接，所述掌纹识别模块与掌纹特征数据库连接；

[0276] 注册用户特征信息时：

[0277] 数据收发模块将接收的预置掌纹图像传输至掌纹识别模块提取掌纹特征并保存在掌纹特征数据库中，并通过数据收发模块发送反馈注册结果至用户终端；

[0278] 认证用户身份时：

[0279] 动态手形生成模块按预置手形图像生成掌纹手形序列通过数据收发模块传输至用户终端；

[0280] 数据收发模块将接收的认证手形图像传输至手形识别模块、掌纹识别模块提取手形、掌纹特征并与手形设置数据库、掌纹特征数据库中的预置手形、掌纹特征匹配；

[0281] 手形识别模块、掌纹识别模块根据匹配结果通过数据收发模块向用户终端反馈认证结果。

[0282] 其中较优地，所述服务端还包括与用户终端对应的数据解密模块；

[0283] 数据收发模块和掌纹识别模块分别与数据解密模块连接；

[0284] 所述安全认证服务器收到用户终端加密的图像后，通过数据收发模块发送至数据解密模块，由数据解密模块解密处理后再处理。

[0285] 其中较优地，所述服务端还包括手掌跟踪模块：

[0286] 所述手掌跟踪模块与所述数据收发模块连接；

[0287] 所述手掌跟踪模块在采集用户带掌纹的认证手形图像时，采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；

[0288] 如果采集区域的手掌不连续存在则通过数据收发模块提示用户认证失败；

[0289] 如果采集区域的手掌连续存在则通过数据收发模块提示用户继续采集其他掌纹手形图像。

[0290] 其中较优地，所述服务端还包括识别决策模块：

[0291] 所述识别决策模块分别与所述手形识别模块、所述掌纹识别模块连接；

[0292] 所述服务端将认证掌纹图像识别匹配处理后，所述识别决策模块判断生成的掌纹手形序列是否已经采集、识别、匹配完成；

[0293] 如果未完成掌纹手形序列，则所述识别决策模块向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；

[0294] 如果掌纹手形序列已完成，则所述识别决策模块查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作，则通过数据收发模块向用户终端传输认证成功的消息；如果无匹配成功的掌纹信息匹配结果则通过数据收发模块向用户终端传输认证失败的消息。

[0295] 再一方面，本发明提供一种基于手势识别的安全认证系统，包括服务端和用户终端；

[0296] 所述服务器与所述用户终端通信连接；

[0297] 还包括与所述服务器和所述用户终端通信连接的交易服务端；

[0298] 所述用户终端采集用户的预置掌纹图像并发送至所述服务端，所述服务端按掌纹识别方法提取掌纹特征并保存预置掌纹特征；

[0299] 用户通过所述用户终端向所述交易服务端发起交易认证请求，所述交易服务端向所述服务端发起身份能认证请求，所述服务端生成掌纹手形序列并传输至所述用户终端，所述用户终端依序展示手形图像，用户按所述用户终端展示的手形图像依序做相应手势动作，所述用户终端采集用户的带掌纹的手形图像并传输至所述服务端，所述服务端按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，所述服务端向所述交易服务端用户终端反馈匹配结果，所述交易服务端根据反馈的匹配结果通过用户终端发动交易结果信息。

[0300] 其中较优地，所述用户终端包括：数据收发模块、业务逻辑模块图像采集模块；

[0301] 交互界面模块、数据收发模块、图像采集模块分别与业务逻辑模块通信连接，图像采集模块与数据收发模块通信连接；

[0302] 用户通过交互界面模块向业务逻辑模块发起指令，业务逻辑模块控制通过数据收发模块向服务端发送注册或认证请求，业务逻辑模块控制图像采集模块采集掌纹手形图像并通过所述数据收发模块向服务端传输；

[0303] 业务逻辑模块控制数据交互模块接收服务端传输的掌纹手形序列并传输至交互界面模块依序向用户展示手形图像。

[0304] 其中较优地，所述用户终端还包括数据加密模块，业务逻辑模块、图像采集模块与数据加密模块通信连接，数据加密模块与数据收发模块连接；

[0305] 图像采集模块采集的图像通过数据加密模块加密后通过数据收发模块传输。

[0306] 其中较优地，所述用户终端还包括图像预处理模块；

[0307] 业务逻辑模块、图像采集模块与图像预处理模块通信连接；

[0308] 业务逻辑模块控制图像预处理模块将图像采集模块采集的图像信息作预处理，将预处理后的图像通过数据收发单元传输。

[0309] 其中较优地，所述服务端包括：

[0310] 带身份认证功能的安全认证服务器和数据库，数据库包括掌纹特征数据库和手形设置数据库；

[0311] 掌纹特征数据库和手形设置数据库与安全认证服务器通信连接；

[0312] 安全认证服务器包括数据收发模块、手形识别模块、掌纹识别模块和动态手形生成模块；

[0313] 所述数据收发模块分别与手形识别模块、掌纹识别模块和动态手形生成模块连接，所述手形识别模块、动态手形生成模块分别与所述手形设置数据库连接，所述掌纹识别模块与掌纹特征数据库连接；

[0314] 注册用户特征信息时：

[0315] 数据收发模块将接收的预置掌纹图像传输至掌纹识别模块提取掌纹特征并保存在掌纹特征数据库中，并通过数据收发模块发送反馈注册结果至用户终端；

[0316] 认证用户身份时：

[0317] 动态手形生成模块按预置手形图像生成掌纹手形序列通过数据收发模块传输至用户终端；

[0318] 数据收发模块将接收的认证手形图像传输至手形识别模块、掌纹识别模块提取手形、掌纹特征并与手形设置数据库、掌纹特征数据库中的预置手形、掌纹特征匹配；

[0319] 手形识别模块、掌纹识别模块根据匹配结果通过数据收发模块向用户终端反馈认

证结果。

[0320] 其中较优地，所述服务端还包括与用户终端对应的数据解密模块；

[0321] 数据收发模块和掌纹识别模块分别与数据解密模块连接；

[0322] 所述安全认证服务器收到用户终端加密的图像后，通过数据收发模块发送至数据解密模块，由数据解密模块解密处理后再处理。

[0323] 其中较优地，所述服务端还包括手掌跟踪模块：

[0324] 所述手掌跟踪模块与所述数据收发模块连接；

[0325] 所述手掌跟踪模块在采集用户带掌纹的认证手形图像时，采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；

[0326] 如果采集区域的手掌不连续存在则通过数据收发模块提示用户认证失败；

[0327] 如果采集区域的手掌连续存在则通过数据收发模块提示用户继续采集其他掌纹手形图像。

[0328] 其中较优地，所述服务端还包括识别决策模块：

[0329] 所述识别决策模块分别与所述手形识别模块、所述掌纹识别模块连接；

[0330] 所述服务端将认证掌纹图像识别匹配处理后，所述识别决策模块判断生成的掌纹手形序列是否已经采集、识别、匹配完成；

[0331] 如果未完成掌纹手形序列，则所述识别决策模块向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；

[0332] 如果掌纹手形序列已完成，则所述识别决策模块查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作，则通过数据收发模块向用户终端传输认证成功的消息；如果无匹配成功的掌纹信息匹配结果则通过数据收发模块向用户终端传输认证失败的消息。

[0333] 再一方面，本发明提供一种基于手势识别的安全认证服务器，

[0334] 所述安全认证服务器用于在安全认证系统中认证用户的权限；

[0335] 所述安全认证服务器与所述用户终端通信连接；

[0336] 所述安全认证服务器接收所述用户终端采集用户的预置掌纹图像，所述安全认证服务器按掌纹识别方法提取掌纹特征并保存预置掌纹特征；

[0337] 所述安全认证服务器接收所述用户终端向所述安全认证服务器发起认证请求，所述安全认证服务器生成掌纹手形序列并传输至所述用户终端，所述用户终端依序展示手形图像，用户按所述用户终端展示的手形图像依序做相应手势动作，所述用户终端采集用户的带掌纹的手形图像并传输至所述安全认证服务器，所述安全认证服务器按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，所述安全认证服务器按匹配结果向所述用户终端反馈认证结果。

[0338] 再一方面，本发明提供一种基于手势识别的安全认证服务器，

[0339] 所述安全认证服务器用于在安全认证系统中认证用户的权限；

[0340] 所述安全认证服务器与所述用户终端和交易服务器通信连接；

[0341] 所述安全认证服务器接收所述用户终端采集用户的预置掌纹图像，所述安全认证服务器按掌纹识别方法提取掌纹特征并保存预置掌纹特征；

[0342] 用户通过所述用户终端向所述交易服务器发起交易认证请求，所述安全认证服务

器接收所述交易服务器向所述安全认证服务器发起认证请求，所述安全认证服务器生成掌纹手形序列并传输至所述用户终端，所述用户终端依序展示手形图像，用户按所述用户终端展示的手形图像依序做相应手势动作，所述用户终端采集用户的带掌纹的手形图像并传输至所述安全认证服务器，所述安全认证服务器按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，所述服务器向所述交易服务器用户终端反馈匹配结果，所述交易服务器根据反馈的匹配结果通过用户终端发动交易结果信息。

[0343] 再一方面，本发明提供一种基于手势识别的安全认证用户终端，

[0344] 所述用户终端用于在安全认证系统中认证用户的权限；

[0345] 所述安全认证服务器与所述用户终端通信连接；

[0346] 所述用户终端采集用户的预置掌纹图像传输至所述安全认证服务器，所述安全认证服务器按掌纹识别方法提取掌纹特征并保存预置掌纹特征；

[0347] 所述安全认证服务器接收所述用户终端向所述安全认证服务器发起认证请求，所述安全认证服务器生成掌纹手形序列并传输至所述用户终端，所述用户终端依序展示手形图像，用户按所述用户终端展示的手形图像依序做相应手势动作，所述用户终端采集用户的带掌纹的手形图像并传输至所述安全认证服务器，所述安全认证服务器按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，所述安全认证服务器按匹配结果向所述用户终端反馈认证结果。

[0348] 再一方面，本发明提供一种基于手势识别的安全认证服务器，

[0349] 所述用户终端用于在安全认证系统中认证用户的权限；

[0350] 所述用户终端与所述安全认证服务和交易服务器通信连接；

[0351] 所述用户终端采集用户的预置掌纹图像传输至所述安全认证服务器，所述安全认证服务器按掌纹识别方法提取掌纹特征并保存预置掌纹特征；

[0352] 所述用户终端向所述交易服务器发起交易认证请求，所述安全认证服务器接收所述交易服务器向所述安全认证服务器发起认证请求，所述安全认证服务器生成掌纹手形序列并传输至所述用户终端，所述用户终端依序展示手形图像，用户按所述用户终端展示的手形图像依序做相应手势动作，所述用户终端采集用户的带掌纹的手形图像并传输至所述安全认证服务器，所述安全认证服务器按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，所述服务器向所述交易服务器用户终端反馈匹配结果，所述交易服务器根据反馈的匹配结果通过用户终端发动交易结果信息。

[0353] 本发明提供的基于手势识别的安全认证方法、终端、服务器和系统，将动态手势序列和手掌特征识别相结合，既不需要用户保管和携带额外的身份信物，又很大程度上降低了身份信息被劫持的可能性，提高了身份认证的安全性。

## 附图说明

[0354] 图 1 是本发明注册用户特征信息流程示意图；

[0355] 图 2 是本发明认证用户身份流程示意图；

[0356] 图 3 是本发明注册用户特征信息流程中采集预置掌纹图像流程示意图；

[0357] 图 4 是本发明水平穿线法检测手指之间的关键点示意图；

[0358] 图 5 是本发明水平穿线法获得首长的关键点示意图；

[0359] 图 6 是本发明定位预置掌纹图像中的掌面区域示意图；

[0360] 图 7 是本发明认证用户身份详细流程示意图；

[0361] 图 8 是本发明预置的手形图像示例图；

[0362] 图 9 是本发明用户验证预置手形流程示意图；

[0363] 图 10 是本发明预置的手形图像对应的手形指示图例；

[0364] 图 11 是本发明预置的手形掩膜示例图；

[0365] 图 12 是本发明在交易时认证用户身份详细流程示意图；

[0366] 图 13 是本发明基于手势识别的安全认证系统结构示意图；

[0367] 图 14 是本发明用户终端一实施例结构示意图；

[0368] 图 15 是本发明用户终端另一实施例结构示意图；

[0369] 图 16 是本发明服务端一实施例结构示意图；

[0370] 图 17 是本发明服务端另一实施例结构示意图；

[0371] 图 18 是本发明基于手势识别的安全认证交易系统结构示意图。

## 具体实施方式

[0372] 下面结合附图和实施例，对本发明的具体实施方式作进一步详细描述。以下实施例用于说明本发明，但不用来限制本发明的范围。

[0373] 本发明提供一种基于手势识别的安全认证方法，包括注册用户特征信息的步骤和认证用户身份的步骤；如图 1 所示，注册用户特征信息的步骤包括：采集用户的预置掌纹图像；提取预置掌纹图像的掌纹特征并保存预置掌纹特征；如图 2 所示，认证用户身份的步骤包括：用户发起认证请求；生成掌纹手形序列并依序向用户展示手形图像；用户按展示的手形图像依序做相应手势动作并采集用户带掌纹的认证手形图像；提取认证手形图像的手形、掌纹特征并与预置手形、掌纹特征匹配；反馈匹配结果。下面结合多个实施例对本发明提供的安全认证方法展开详细的说明。

[0374] 实施例 1

[0375] 本实施例提供一种基于手势识别的安全认证方法，包括注册用户特征信息的步骤和认证用户身份的步骤；如图 1 所示，注册用户特征信息的步骤包括：用户终端采集用户的预置掌纹图像并传输至服务端；服务端提取预置掌纹图像的掌纹特征并保存预置掌纹特征；如图 2 所示，认证用户身份的步骤包括：用户终端向服务端发起认证请求；服务端生成掌纹手形序列并依序向用户终端传输并展示手形图像；用户按展示的手形图像依序做相应手势动作，用户终端采集用户带掌纹的认证手形图像传输至服务端；服务端提取认证手形图像的手形、掌纹特征并与预置手形、掌纹特征匹配；反馈匹配结果。下面对本实施例提供的安全认证方法展开详细的说明。

[0376] 第一部分，介绍注册用户特征信息的步骤。

[0377] 注册用户特征信息时，需要先采集用户的预置掌纹图像，然后按掌纹识别方法提取掌纹特征并保存预置掌纹特征。下面具体说明。

[0378] 如图 3 所示，注册用户特征信息时，用户终端向服务端发起注册用户特征请求；用户将平整的掌形（例如手掌伸平，五指张开）放置于用户终端的图像采集区域，启动图像采集程序采集用户的预置掌纹图像；采集到预置掌纹图像后传输至服务端，服务端利用掌纹

识别方法提取预置掌纹图像中的用户的掌纹特征，对提取后掌纹特征保存。自此，注册用户特征步骤结束。

[0379] 在本发明的一个实施例中，采集用户的预置掌纹图像步骤中，或在提取掌纹特征并保存预置掌纹特征的步骤中，还包括对预置掌纹图像预处理的步骤。对预置掌纹图像预处理后可以滤除一些不必要的图形信息，减少数据传输量，提高了压缩率，大大提高了数据传输效率。对预置掌纹图像预处理的步骤包括：

[0380] 1)、先对采集的手掌掌面图像粗分割处理。首先，将手掌掌面图像进行颜色空间转换，从 RGB 空间转换至 HSV 空间；其次，利用 H 分量快速提取手的肤色区域。通过对手掌掌面图像的粗分割处理可以进一步缩小后续图像处理的像素数量。在本发明中，通过发明人多次试验发现在 HSV 空间中取 $H \in [0.22, 0.48]$ 时最接近肤色区域的有效范围。在 HSV 空间中的 H 是色调分量，只使用 H 分量可以减少光照的影响。在此步骤中对采集的手掌掌面图像处理并区分手形区域和非手形区域。

[0381] 2)、对采集的手掌掌面图像前景和背景区分并均衡处理。首先将粗分割后的手掌掌面图像转换为灰度图像；其次，将肤色区域以外的区域设置为背景区域；最后对灰度图像进行直方图均衡处理得到均衡后的灰度图像。

[0382] 优选对数变换法，具体如下：

[0383] $G(x,y) = 21.6 \times \ln((g(x,y)+1)$

[0384] 其中，$g(x,y)$ 是灰度图像的灰度值，$G(x,y)$ 是对数变化后的灰度值。通过直方图均衡处理后可以尽可能减少光照对手掌掌面图像的影响。

[0385] 3)、对均衡后的灰度图像中值滤波处理，获取更稳定的前景手形区域。通过中值滤波处理后获取的手形区域更准确。

[0386] 4)、对图像的前景手形区域进行二值化处理，从而生成手形图图像的前景二值化区域（二值化手形区域图像）。本发明中优选 ostu 法（最大类间方差法）对前景手形区域二值化处理。

[0387] 5)、获取带掌纹的手形图像。本发明中优选 floodfill（漫水填充）算法对二值化手形区域图像作连通区域检测，取图像中像素点数最多的连通区域为手形区域，从而过滤掉其他背景噪声点。

[0388] 6)、基于 Sobel（索贝尔、Sobel operator）算子对二值化图像进行边缘检测得到二值化后的手形区域。

[0389] $$f_x = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} \qquad f_y = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}$$

[0390] 其中，$f_x$ 为水平滤波器，$f_y$ 为垂直滤波器。

[0391] 本实施例中，对预置掌纹图像预处理的步骤可以在用户终端完成，也可以在服务端进行。在网络不佳的情况下可以启用在用户终端执行对预置掌纹图像预处理的步骤，对预置掌纹图像预处理后再传输至服务端。在网络环境较好的情况下，或用户终端处理能力不好的情况下，可以直接由用户终端发送至服务端，在服务端执行对预置掌纹图像预处理的步骤。对预置掌纹图像预处理的步骤可以根据实际情况灵活选择在用户终端或服务端执行，尽可能缩短注册用户特征信息时间。

[0392] 在本发明的一个实施例中，提取掌纹特征并保存预置掌纹特征的步骤具体是对预

置掌纹图像按掌纹识别方法提取掌纹特征。下面对按掌纹识别方法提取掌纹特征的步骤详细说明。

[0393] 首先，介绍定位预置掌纹图像中的掌面区域的步骤。在本发明中，优选水平穿线法检测手指之间的关键点，下面以手指张开的预置掌纹图像为例详细说明。

[0394] 如图 4 所示，a)、从上到下水平穿线边缘图像，找到一组包含有 8 个边界点的穿线。将相邻 2 个边界点作为一组，共四组；将这四组作为是四指的初始穿线组。

[0395] b)、对于四指中的每一指（不包括拇指），以初始穿线组为起始位置，向上和向下分别进行搜索，直至搜索到上下边界。搜索的策略是基于同一连通区域，向上和向下进行区域生长，直至找到连通区域的边界为止。上下边界的判断以是否为同一连通区域为依据，进而定位出关键点 601 至 607。

[0396] c)、以相同的方法，从下至上水平穿线边缘图像，找到一组包含有 4 个边界点的穿线。其中后 2 个边界点的水平坐标位于图像的右半区域，以后 2 个边界点作为拇指的初始穿线组。

[0397] d)、同步骤 b)，以拇指初始穿线指为起始位置，向上和向下分别进行搜索，直至搜索到上下边界，进而定位出关键点 608 和 609。

[0398] 其次，介绍切割预置掌纹图像中的掌面区域的步骤。

[0399] 本发明中，优选采用基于 Harris（角点检测算法）切割预置掌纹图像中的掌面区域。Harris 角点检测算法是一种基于信号的点特征提取算子，其原理是把要处理的图像窗口向任意方向移动微小位移（μ，v）。为了提高抗噪能力，对图像窗口进行了高斯平滑滤波，选用的高斯窗口如下：

[0400] $$G_{x,y}=\exp\left[-\frac{1}{2}(x^2+y^2)/\sigma^2\right]$$

[0401] 则图像灰度改变量 $E_{x,y}$ 定义为：

[0402] $$E_{x,y}|_{(x,y)}=\Sigma G_{x,y}[I(x+\mu,y+\mu)-I(x,y)]^2$$

[0403] 式中，$E_{x,y}$ 为在 (x,y) 处移动一个小窗口（μ，υ）所发生的亮度变化值；I 为要提取角点的掌纹图像。

[0404] 如图 5 所示，使用 Harris（角点检测算法）从预置掌纹图像中找出图 4 中穿线法获得的食指、中指、无名指、小指之间的关键点中的 a 点、b 点、c 点。其中，a 点代表上述穿线发检测出的关键点 607，c 点代表关键点 605。b 点为 a 点和 c 点组成线段的中点。以 b 点为原点，作线段 ac 的法线 f；然后以 c 点为起点，沿法线 f，朝向手掌方向偏移一定距离（线段 ac 的长度）处的点 e，以 e 为中心，生成一个边长为 P 且与线段 ac 平行的矩形区域。提取出手掌中心区域 P×P 区域。

[0405] 最后，介绍提取预置掌纹图像中的掌纹特征的步骤。

[0406] 在上述步骤中提取出预置掌纹图像中心矩形区域 P×P 区域内作掌纹特征提取。在本发明中优选基于“Kong A W K,Zhang D.Competitive coding scheme for palmprint verification.In:Proceedings of the 17th Inter-national Conference on Pattern Recognition.Washington D.C.,USA:IEEE,2004.520-523”中的方法进行特征提取与匹配。该方法中使用六个方向的实值 Gabor 滤波器对掌纹图像滤波，并对幅值最小的方向编码，称为竞争编码 (Competitive code)。在本发明中，对正文特征提取

时可以参考如下方法：例如：“基于主线特征的双向匹配的掌纹识别新方法．计算机研究与发展，2004,41(6):996-1002”；“an implementation of biometric technology. In:Proceedings of the14th International Conference on Pattern Recognition.Brisbane,Australia:IEEE,1998.219-221”；“A novel approach of palm-line extraction. In:Proceedings of the 3rd International Conference on Image and Graphics. Washington D.C.,USA:IEEE,2004.230-233”。

[0407] 如图 3 所示，为了进一步保证保存的预置掌纹特征的准确性，身份认证时可以顺利验证掌纹，在注册用户特征信息时需要多次采集预置掌纹图像并提取用户可用的多张掌纹特征信息并保存。具体如下：不断的重复上述过程，直至采集到的掌纹特征数量达到 M；保存用户的掌纹特征至数据库；服务端向用户终端传输消息提示用户掌纹特征采集成功。

[0408] 第二部分，介绍认证用户身份的步骤。

[0409] 如图 7 所示，用户在交易或其它需要验证用户场景时，需要通过本方法认证用户身份。认证用户身份时，用户通过用户终端向服务端发起认证请求；服务端生成掌纹手形序列并传输至用户终端，依序向用户展示手形图像；用户按展示的手形图像依序作相应手势动作，用户终端采集用户带掌纹的认证手形图像并传输至服务端；服务端对带掌纹的认证手形图像提取手形、掌纹特征并与预置手形、掌纹特征匹配；服务端向用户终端反馈匹配结果。下面对认证用户身份的步骤展开详细的说明。

[0410] 首先，介绍用户发起认证请求的步骤。如图 7 所示，当发起认证请求时，用户终端将认证请求信息打包后发送。优选以 XML 格式发送。认证请求信息包括用户终端的 ID、用户编号。在该步骤中，为了进一步保证数据验证的安全性，发起认证请求后服务端还需要进一步验证认证请求的合法性，因此在认证请求信息中还包括生成的随机编码。用户终端发起认证请求时封装的数据包格式示例如下：

[0411]

```
<?xml version="1.0" encoding="utf8" ?>
<require>
    <client_id value="1245789ab3!3dv" />    //用户用户终端的机器 ID
    <user_id value="EA1009803" />       //用户编号
       <require_id value="459B63D3_1232_47cb_B568_43475715B79C" />
       //请求的随机编号
    </ require>。
```

[0412] 服务端收到用户终端发送的认证请求数据包后，服务端读取认证请求数据包，通过验证随机编码的方式验证认证请求的合法性。如果验证通过，则启动一个认证线程进行后续的认证；如果验证不通过，则以消息形式向用户终端传送结果，告知用户认证请求非法，认证结束。

[0413] 其次，介绍生成掌纹手形序列并依序向用户展示手形图像的步骤。

[0414] 如图 7 所示，服务端按用户发起的认证请求随机生成一套掌纹手形序列，依序向用户终端传输手形并在用户终端展示。掌纹手形序列是不同手形的多张手形随机组成的序列。当服务端向用户终端传输手形时，将随机生成的手形信息打包后发送。优选以 XML 格式发送。将随机生成的手形信息包括认证请求随机编码、手形编号等手形信息。服务端传输的手形信息数据包格式示例如下：

[0415]

```
<?xml version="1.0" encoding="utf8" ?>
<identify>
    < require_id value="459B63D3_1232_47cb_B568_43475715B79C" />
    //请求的随机编号
    <idetify_gesture_id value="5" />          //手形编号
    <idetify_gesture_angle value="15" />      //旋转角度
        </ identify >。
```

[0416] 在服务端生成掌纹手形序列并依序向用户终端传输展示手形图像的步骤中，由于掌纹手形序列是不同手形的多张手形图像随机组成的序列。且在身份认证过程中需要采集用户的手势特征和手掌掌纹特征。本发明中预置了多种手形图像供随机生成手形图像序列。掌纹手形序列中的各种不同的手形选自服务端中的手形候选集合。例如：对于手形候选集合 $PC = \{p_1, p_2, \cdots p_M\}$，$5 \leqslant M \leqslant 7$；其中，$p_1$-$p_M$ 表示不同手形的序号，M 表示用户实际可以使用的手形的数量。在本发明中，为了保证用户认证过程的安全性，保证给用户提供的手形序列中的手形不会太少，M 取至少为 5。生成一个长度为 N 的手形序列 $PC_N$，$PC_N = \{pc_1, pc_1, \cdots pc_N\}$。其中，$pc_1$-$pc_N$ 表示各种不同的手形，对于每一个掌纹手形序列 $pc_s = \{random\{PC\}, random(AI)\}$，$1 \leqslant s \leqslant N$。其中，random(PC) 表示随机的手形图像，random(AI) 表示随机的旋转角度。本发明中，随机函数 random 使用的是基于时间种子的随机数生成器。

[0417] 下面对服务端生成掌纹手形序列时各种手形图像举例说明。如图 8 所示，在此，仅对部分手形图像作相应说明，其它图中未作展示的图形也仍然可以实现本发明中掌纹手形序列。本发明中现列举其中的几种手形对应的手势举例说明，具体说明如下：手势 1：五指张开平伸式，可参见图 8 中 500。手势 2：五指并拢平伸式，可参见图 8 中 501。手势 3：“开枪式”，在手势 2 的基础下，收拢中指，无名指和小指，可参见图 8 中 502。手势 4：四指内扣拇指张开式，即在手势 2 的基础下，张开拇指，同时内扣除其余四指，可参见图 8 中 503。手势 5：四指平伸拇指内扣式，即在手势 2 的基础下，内扣拇指，同时伸直其余四指，可参见图 8 中 504。手势 6：五指内扣式，即在保持手掌平整的前提下，所有指头都内扣，可参见图 8 中 505。手势 7：四指并拢指平伸拇指张开式，即在保持手掌平整的前提下，四指平伸，而拇指张开，可参见图 8 中 506。

[0418] 在本发明中，考虑到人的个体生理差异，并不是所有的人都能够准确的做出上述图 8 中的预置手形对应的各种手势。因此在注册用户特征信息的步骤中，有必要增加用户能否适应上述预置手形的验证步骤。具体地，用户需要依次按提示的手形图像实验作相对应的手势、并采集相应的掌纹手形图像作相应的验证。按验证结果确定是否可以准确摆放预置手形，用户不能准确摆放提示的手形图像相对应的手势。服务端作相应的记录。用户摆出提示的手形图像相对应的手势，同时对于当前用户，在身份认证过程中生成的随机掌纹手形序列中，掌纹手形序列是根据预置手形的验证结果生成的，掌纹手形序列是不包含那些无法准确摆出手形图像相对应的手势。下面对用户注册身份信息的步骤补充说明。

[0419] 具体地，如图 9 所示，用户验证预置手形的过程主要包括以下的步骤：服务端将预置的各种手形图像依次传输至用户终端并呈现给用户。用户按照展示的每一种手型图像摆出相同的手势并通过用户终端采集相应的图像传输至服务端。服务端对客户端发送的图像

识别手形图像并与向用户传输的手形图像比对反馈比对结果（本步骤与认证用户身份的步骤中手形图像识别与比对过程相同，具体步骤在下文中详细描述）。如果用户多次无法摆出相同的手势（即出错的次数≥ F1），则提示用户“当前手势错误，需要重新调整摆放姿势”。如果用户继续多次无法摆出相同的手势（即出现的次数≥ F2，且 F2>F1），则提示用户“是否放弃当前手势”。如果用户选择放弃当前手势，则继续取下一个用户未尝试摆放的手势；同时标记当前手势为用户放弃状态；否则，则继续显示当前手势。如果用户成功了摆出了相同的手势，则继续取下一个用户未尝试摆放的手势；同时标记当前手势为用户可选择状态。如果用户尝试了所有的预置手形，则判断用户可选择的手势数量是否大于 M。如果不大于 M，则提示用户无法成功注册。如果大于 M，则提示用户设置相应的逻辑运算功能，然后保存所有的手势特征，同时提示用户手势注册成功。

[0420] 在本发明中，在选取手形候选集合中的手形图像生成掌纹手形序列向用户展示时，用户需要按掌纹手形序列在用户终端中展示的手形图像做相应的手势并采集认证手形图像。考虑到掌纹图像采集并使别的难易程度和其他因素对掌纹图像的影响，尽可能加快认证过程，提高认证效率。因此，需要对生成掌纹手形序列时在选取手形候选集合中选取的手形图像作一定的限制。例如，本发明中对 $PC_N$ 增加一个限制条件，即必须至少包含一个“五指张开平伸式”手形。由于手形候选图像几何中的各种手形图像对应的认证手形图像中，可参见图 8 中 500 五指张开平伸式。五指张开平伸式掌纹区域最完整，手指的动作对掌纹形变的影响最小。在掌纹识别程序中识别速度最快，节约用户认证时间。如果在随机生成后确实没有包含“五指张开平伸式”手形，则将一个“五指张开平伸式”手形随机的插入 $PC_N$ 序列中。如此限制，进一步确保掌纹检测的可靠性。在此需要说明的是，对掌纹手形序列的限制条件不仅限于此，也可以是其他限制方式（将选取手形候选集合中其他手形图 8 中的任意一个）。当然可以理解，对掌纹手形序列中选取的手形图像的限制条件也可以不设置。通过其他方式加快用户认证时间，提高认证效率。

[0421] 再次，介绍用户按展示的手形图像依序做相应手势动作并采集用户带掌纹的认证手形图像的步骤。

[0422] 如图 7 所示，用户终端收到服务端发送的认证要求后，用户按用户终端展示的手形在指定区域作相应的手势动作，用户终端采集相应手形的带掌纹手形传输至服务端。为了进一步提高用户终端采集掌纹手形图像的准确性和提高认证过程中采集用户掌纹手形图像的速度，用户终端会绘制出相应的手形指示图例，并提示用户。如图 10 所示，在用户终端采集认证掌纹手形图像时，在用户终端展示相应的手形指示图例，图 10 中手形指示图例 510 至 516 对应图 8 中的 500 至 506 的掌纹手形图像。用户需要将手按用户终端展示的手形图像调整手的位置，将手放置于用户终端的采集手形指示图例中，用户终端同时在后台定时采集用户当前图像并发送给服务端。用户终端采集到认证的掌纹手形图像后，将认证的掌纹手形图像打包后发送至服务端。为保证掌纹图像传输的安全性，需要进一步将掌纹手形图像加密，加密后的掌纹手形图像以数据包的形式发送。认证掌纹手形图像优选以 XML 格式发送。该数据包包括请求的随机编号和加密图像的编码。在向服务端发送认证掌纹手形数据包之前可以根据网络状况选择是否对认证掌纹手形图像进行预处理的步骤。对认证掌纹手形图像预处理的步骤与对预置掌纹图像与处理的步骤相同，在此就不再赘述了。用户终端想服务端发送掌纹手形图像时加密的掌纹手形认证数据包格式示例如下：

[0423]

```
<?xml version="1.0" encoding="utf8" ?>
<identify>
    < require_id value="459B63D3_1232_47cb_B568_43475715B79C" />
    //请求的随机编号
    <image_data value="qwerf45bvv90,31rdfvcxvcv" />          //加密图像的
base64 编码
</ identify >。
```

[0424] 第三，对带掌纹的认证手形图像作手形识别并与预置手形特征比对的步骤。

[0425] 发明中，首先对带掌纹的认证手形图像作手形识别；对认证手形图像作手形识别时，是将带掌纹的认证手形图像与服务端预先设置的所有手形掩膜作匹配度比较，并找出相匹配的手形掩膜，将该手形掩膜对应的手形作为识别的手形。预处理后的掌纹手形图像与服务端预先设置的对应的手形掩膜作匹配度比较，与手形掩膜匹配的则认为是对应的手形图像，如果不匹配的则认为不是对应的手形图像。具体地，计算预处理后的掌纹手形图像中各手指和手掌的长宽。按掌纹手形图像中各手指和手掌的长宽调整手形掩膜的长宽，将带掌纹的认证手形图像填充手形掩膜的长宽，根据填充结果确定相应的匹配度。将识别后的手形与生成掌纹手形序列时对应的预置手形特征比对，如果对应则认为匹配，反之则认为不匹配。

[0426] 本发明将一个手掌区域按不同位置划分为不同的区域。例如：四指区域（食指、中指、无名指、小指）、拇指区域和手掌区域，分别用 F、T、P 表示四指部分、拇指部分和手掌部分。一个手掌的特征组用 $FeatureList_{feature\_type}$ 表示。手掌的特征组如下式所示：

[0427] $$FeatureList_{feature\_type} = \{F_w, F_h, T_w, T_h, P_w, P_h\}$$

[0428] 其中，$F_w$ 表示四指区域的宽度；$F_h$ 表示四指区域的高度；$T_w$ 表示拇指区域的宽度；$T_h$ 表示拇指区域的高度；$P_w$ 表示手掌区域的宽度；$P_h$ 表示手掌区域的高度。

[0429] 本发明中，基于上述 9 个关键点，计算出 Feature 的各项数值，四指区域、拇指区域和手掌区域的长宽是按下式计算的：

[0430] $$tp_1 = \max(distance(pt_{605}, pt_{606}), distance(pt_{605}, pt_{606}))$$

[0431] $$tp_2 = 2 \times pt_{607} - pt_{606}$$

[0432] $$F_h = f_0 \times distance(center(pt_{606}, pt_{607}), pt_{603})$$

[0433] $$F_w = f_1 \times tp_1$$

[0434] $$P_w = f_2 \times tp_1$$

[0435] $$P_h = f_3 \times (distance(tp_2, pt_{608}))$$

[0436] $$T_w = f_4 \times (distance(tp_2, pt_{609}))$$

[0437] $$T_h = f_5 \times (\max(distance(tp_2, pt_{609}), distance(tp_2, pt_{608})))$$

[0438] 在本发明中，$f_0 \sim f_5$ 是系数，且 $f_0 \sim f_5$ 可以根据经验取一定的固定值，即 $f_0 = 0.56$, $f_1 = 1.15$, $f_2 = 4.25$, $f_3 = 1.92$, $f_4 = 0.66$, $f_5 = 0.45$。

[0439] 为了进一步提高识别精度和识别率，通过掌纹手形图像中各手指和手掌的长宽调整手形掩膜的长宽。

[0440] 如图 11 所示，本发明在服务端中设置了与图 8 所示手形图像对应的手形掩膜，每套掩膜由 6 部分组成，分别是 4 个手指，一个手掌和一个拇指。每个手指分成上下 2 个部分，

一个拇指分成 4 个部分。例如，在一套手形掩膜中 P 区域代表手掌区域，T1 至 T4 代表拇指区域；F0U、F0D 代表食指区域；F1U、F1D 代表中指区域；F2U、F2D 代表无名指区域；F3U、F3D 代表小指区域。

[0441] 如图 11 所示，在服务端选取手形候选集合中的手形图像生成掌纹手形序列向用户展示时，选取的手形候选集合中的每一个手形都一一对应一个手形掩膜，即图 7 中的手形图像对应图 11 中的手形掩膜，对应关系如表 1 所示：

[0442]

| | 手形 1 | 手形 2 | 手形 3 | 手形 4 | 手形 5 | 手形 6 | 手形 7 |
|---|---|---|---|---|---|---|---|
| 手形 | 500 | 501 | 502 | 503 | 504 | 505 | 506 |
| 掩膜 | 700 | 701 | 702 | 703 | 704 | 705 | 700 |

[0443] 如图 11 所示，在服务端中，每一个手形对应的手形掩膜，共包括 13 个最小单元。每个手形掩膜的单元组成如下式所示：

[0444] $UnitList = \{P, T1, T2, T3, T4, F0U, F0D, F1U, F1D, F2U, F2D, F3U, F3D\}$

[0445] 每一个手形对应的手形掩膜有相对应的区域集合，如下式所示：

[0446] $RegionList_{feature\_type} = \{FR_{feature\_type}, BR_{feature\_type}\}$

[0447] $FR_{feature\_type} = \{F_1, F_2, \cdots F_n\}$

[0448] $BR_{feature\_type} = \{B_1, B_2, \cdots B_m\}$

[0449] $m+n = 13$

[0450] 其中，每一个手形掩膜 $RegionList_{feature\_type}$ 包含两类区域集合，分别是前景区域集合 $FR_{feature\_type}$ 和背景区域集合 $BRegion_{feature\_type}$；对于每一个前景区域 $F_n$ 和背景区域 $B_m$，则可以是单一最小单元，例如 $F_n = \{P\}$，即单一手掌区；也可以是多个最小单元的组合，例如 $B_m = \{F1U, F2U, F3U\}$。

[0451] 图 8 中每一个手形对应图 11 中的每一个手形掩膜的区域集合，手形与手形掩膜前景区域的对应关系如表 2 所示：

[0452]

| | |
|---|---|
| $FR_{500}$ | {P}, {F0U, F0D, F1U, F1D, F2U, F2D, F3U, F3D}, {T2, T3} |
| $FR_{501}$ | {P}, {F0U, F0D, F1U, F1D, F2U, F2D, F3U, F3D}, {T1, T3} |
| $FR_{502}$ | {P}, {F0U, F0D}, {F1D, F2D, F3D}, {T2, T3} |
| $FR_{503}$ | {P}, {F0D, F1D, F2D, F3D}, {T2, T3} |
| $FR_{504}$ | {P}, {F0U, F0D, F1U, F1D, F2U, F2D, F3U, F3D}, {T3} |
| $FR_{505}$ | {P}, {F0D, F1D, F2D, F3D}, {T3} |
| $FR_{506}$ | {P}, {F0U, F0D, F1U, F1D, F2U, F2D, F3U, F3D}, {T2, T3} |

[0453] 手形与手形掩膜背景区域的对应关系如表 3 所示：

[0454]

| | |
|---|---|
| $BR_{500}$ | {T1, T4} |
| $BR_{501}$ | {T2, T4} |
| $BR_{502}$ | {F1U, F2U, F3U}, {T1, T4} |
| $BR_{503}$ | {F0U, F1U, F2U, F3U}, {T1, T4} |

[0455]

| | |
|---|---|
| $BR_{504}$ | {T1, T2, T4} |
| $BR_{505}$ | {F0U, F1U, F2U, F3U}, {T1, T2, T4} |
| $BR_{506}$ | {T1, T4} |

[0456] 在本发明中，将预处理后的掌纹手形图像与手形掩膜匹配时，先比对预处理后的掌纹手形图像对手形掩膜的每个前景区域和背景区域中每个最小单元的填充率（填充率＝填充量／区域面积）。如果当前最小单元的填充率大于预设阈值则视为当前手形可以填充当前手形掩膜的最小单元填充区域，返回填充值 1；如果当前最小单元的填充率小于等于预设填充率阈值则视为当前手形不能填充当前手形掩膜的最小单元填充区域，返回填充值 0。具体地，将预处理后的掌纹手形图像与手形掩膜的每个前景区域和背景区域中每个最小单元的填充率分别（例如，手形图像的食指部分与手形掩膜的前景区域最小单元 F0U 和最小单元 F0D 分别作填充比对，如果最小单元 F0U 可以填充则返回 1，否则返回 0，如果最小单元 F0D 可以填充则返回 1，否则返回 0；作填充比对，如果可以填充则返回 1，否则返回 0；手形图像中的拇指部分与手形掩膜的前景区域最小单元 T1、最小单元 T2、最小单元 T3、最小单元 T4 分别作填充比对，如果最小单元 T1、最小单元 T2、最小单元 T3、最小单元 T4 可以填充则分别返回 1，否则返回 0）。

[0457] 预处理后的掌纹手形图像与手形掩膜中的前景区域和背景区域的填充比对关系如下式所示：

[0458] $$Value_n=\begin{cases}1, FilledPercent(R_n) > Threshold_n \\ 0, FilledPercent(R_n) \le Threshold_n\end{cases}$$

[0459] 其中，$FilledPercent(R_n)$ 表示区域的填充百分比，$Threshold_n$ 表示预设填充率阈值；区域的填充百分比 $FilledPercent(R_n)$ 大于相对应的阈值 $Threshold_n$ 时，分值为 1，否则为 0。

[0460] 认证手形图像与预置手形特征比对时还需要根据手形掩膜的前景区域和背景区域的每个最小单元分别比对，具体比对步骤如下：认证手形图像的手形区域与手形掩膜的的前景区域和背景区域的每个最小单元分别比对分别作匹配；根据认证手形图像的手形区（包括手掌区域和多个手指区域）与多个手形掩膜的多个部分（包括前景区域和背景区域的每个最小单元分别比对）作填充匹配；根据返回的填充值的结果确定认证手形图像与预制手形特征比对结果。具体地，将认证手形图像的手掌区域和多个手指区域与多个手形掩膜的前景区域和背景区域的每个最小单元分别作填充匹配，如果认证手形图像的手掌区域

和多个手指区域与当前手形掩膜的前景区域的每个最小单元匹配且非手形区域与当前手形掩膜的背景区域的每个最小单元匹配，则视为当前认证手形图像与当前手形掩膜对应的预置手形特征匹配；否则视为不匹配。下面以图 11 中手形掩膜 702 的特征匹配为例详细说明。当前认证手形图像的手形区域（包括手指区域和手掌区域）与多个手形掩膜的前景区域和背景区域的每个最小单元分别作匹配度比较，如果认证手形图像的手形区域与当前手形掩膜的前景区域和背景区域的每个最小单元分别作填充匹配，前景区域的 8 个最小单元 P、F0U、F0D、F1D、F2D、F3D、T2、T3 返回的填充值全部为 1，且背景区域的 5 个最小单元 F1U、F2U、F3U、T1、T4 返回的填充值全部为 0，则视为当前认证手形图像与图 11 中手形掩膜 702 的特征对应的预置手形特征匹配；如果前景区域的 8 个最小单元 P、F0U、F0D、F1D、F2D、F3D、T2、T3 中有任意一个区域返回的填充值不为 1，或背景区域的 5 个最小单元 F1U、F2U、F3U、T1、T4 中有任意一个区域返回的填充值不为 0，则视为当前认证手形图像与图 11 中手形掩膜 702 的特征对应的预置手形特征不匹配。

[0461] 为了进一步提高精度，在本发明中，将预处理后的掌纹手形图像与手形掩膜匹配时，先比对预处理后的掌纹手形图像对手形掩膜的每个前景区域和背景区域的填充率（填充率＝填充量／区域面积）。如果当前区域的填充率大于预设阈值则视为当前手形可以填充当前手形掩膜的填充区域，返回填充值 1；如果当前区域的填充率小于等于预设填充率阈值则视为当前手形不能填充当前手形掩膜的填充区域，返回填充值 0。具体地，将预处理后的掌纹手形图像与手形掩膜的每个前景区域和背景区域分别作比对（例如，手形图像的食指部分与手形掩膜的前景区域 {F0U,F0D} 作填充比对，如果可以填充则返回 1，否则返回 0；手形图像中的拇指部分与手形掩膜的前景区域 {T2,T3} 作填充比对，如果可以填充则返回 1，否则返回 0）。

[0462] 预处理后的掌纹手形图像与手形掩膜中的前景区域和背景区域的填充比对关系如下式所示：

[0463] $$Value_n=\begin{cases}1, FilledPercent(R_n) > Threshold_n \\ 0, FilledPercent(R_n) \le Threshold_n\end{cases}$$

[0464] 其中，$FilledPercent(R_n)$ 表示区域的填充百分比，$Threshold_n$ 表示预设填充率阈值；区域的填充百分比 $FilledPercent(R_n)$ 大于相对应的阈值 $Threshold_n$ 时，分值为 1，否则为 0。

[0465] 认证手形图像与预置手形特征比对时还需要根据手形掩膜的前景区域和背景区域分别比对，具体比对步骤如下：认证手形图像的手形区域与手形掩膜的各区域分别作匹配；根据认证手形图像的手形区（包括手掌区域和多个手指区域）与多个手形掩膜的多个部分（包括前景区域和背景区域）作填充匹配；根据返回的填充值的结果确定认证手形图像与预制手形特征比对结果。具体地，将认证手形图像的手掌区域和多个手指区域与多个手形掩膜的前景区域和背景区域分别作填充匹配，如果认证手形图像的手掌区域和多个手指区域与当前手形掩膜的前景区域匹配且非手形区域与当前手形掩膜的背景区域匹配，则视为当前认证手形图像与当前手形掩膜对应的预置手形特征匹配；否则视为不匹配。下面以图 11 中手形掩膜 702 的特征匹配为例详细说明。当前认证手形图像的手形区域（包括手指区域和手掌区域）与多个手形掩膜的多个部分作匹配度比较，如果认证手形图像的手形区域与当前手形掩膜的前景区域和背景区域分别作填充匹配，4 个前景

区域 {P}, {F0U, F0D}, {F1D, F2D, F3D}, {T2, T3} 返回的填充值全部为 1，且 2 个背景区域 {F1U, F2U, F3U}, {T1, T4} 返回的填充值全部为 0，则视为当前认证手形图像与图 11 中手形掩膜 702 的特征对应的预置手形特征匹配；如果 {P}, {F0U, F0D}, {F1D, F2D, F3D}, {T2, T3} 中有任意一个区域返回的填充值不为 1，或 {F1U, F2U, F3U}, {T1, T4} 中有任意一个区域返回的填充值不为 0，则视为当前认证手形图像与图 11 中手形掩膜 702 的特征对应的预置手形特征不匹配。

[0466] 在此需要说明的是：手形 500 与手形 506 的区域定义是相同的，因此二者的区分还需要检测四个手指（拇指除外）之间的连接情况，即基于水平穿线法检测结果，如果存在至少一条穿线结果中包含 5 段连续的线段，则为手形 500，否则为手形 506。

[0467] 最后，介绍按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配的步骤。

[0468] 如图 7 所示，服务端在接收到认证掌纹手形数据包后对该数据包解密，解密后，优先判断认证掌纹手形数据包中的认证手形图像是否有手掌存在。如果有手掌存在，则进行下一步的掌纹图像识别；如果无手掌，则向用户反馈认证失败。服务端检测到带掌纹的认证手形图像后对认证手形图像识别掌纹信息。对认证手形图像识别掌纹信息的步骤与对预置掌纹图像按掌纹识别方法提取掌纹特征的步骤相同在此就不再赘述了。

[0469] 如图 7 所示，在识别认证手形图像的掌纹信息之后，将识别后的掌纹信息与数据库中已经预先存储的预置掌纹信息匹配，记录掌纹信息匹配结果。

[0470] 如图 7 所示，将用户终端传输的认证掌纹图像识别匹配处理后进一步判断服务端生成的掌纹手形序列是否已经采集、识别、匹配完成。如果未完成掌纹手形序列，则向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成。如果掌纹手形序列已完成，则查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作并通过用户终端提示用户认证成功。如果无匹配成功的掌纹信息匹配结果则通过用户终端向用户提示认证失败。服务端将身份认证结果以数据包的形式向用户终端发送，优选以 XML 格式发送。该数据包包括请求的随机编号、认证结果和手形编号等。用户终端想服务端发送掌纹手形图像时加密的掌纹手形认证数据包格式示例如下：

[0471]

```
<?xml version="1.0" encoding="utf8" ?>
<identify>
    < require_id value="459B63D3_1232_47cb_B568_43475715B79C" />
    //请求的随机编号
    <idetify_result_id value="1" />
    //0: 匹配失败，继续采集图像; 1: 匹配成功，开始下一个手形; 2: 认证失败，
退出; 3: 认证成功，退出。
    <idetify_gesture_id value="5" />          //手形编号
    <idetify_gesture_angle value="15" />      //旋转角度
        </ identify >。
```

[0472] 如图 7 所示，为了保证认证过程的安全性，在按掌纹识别方法提取掌纹特征之前，采集用户带掌纹的认证手形图像时，需要确认采集区域的手掌是连续存在的，如果采集区域的手掌不连续则提示用户认证失败（例如在身份认证过程中，用户在执行掌纹手形图像序列时，用户将手移出用户终端的图像采集区域，则认为该身份认证请求非法，提示用户认

证请求失败，需重新认证身份）。

[0473] 在本发明的一个实施例中，采集用户带掌纹的认证手形图像时，确认采集区域的掌纹手形图像是否连续存时，采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续。手形区域跟踪算法优选 CamShift 算法来实现对手区域的跟踪。下面对采用 CamShift 算法对手区域的跟踪的步骤详细说明。

[0474] 本发明中采用 CamShift 算法来实现对手区域的跟踪。具体流程如下：

[0475] 1) 在第一次检测到正确的手形后，将手形掩膜中的最小单元 P 所对应的区域作为跟踪区域。

[0476] 2) 对跟踪区域的图像进行反向投影 (Back Projection)，具体作法是：首先将图像转换至 HIS 空间，然后取 H 分量提取现 1D 直方图，即区域中每个象素值的概率分布图。

[0477] 3) 跟踪过程采用 MeanShift（均值漂移）方法。

[0478] 4) 对于新到来的图像，采用 CamShift（称为连续自适应的 MeanShift 算法）方法来进行更新。

[0479] 如图 7 所示，为了保证认证过程的安全性，本发明的一个实施例中，在认证用户身份的步骤中本发明还提供对用户手势按指定角度摆放并验证的步骤。本发明的技术方案还预置了多种摆放角度度 AI，取 $0° \leqslant AI \leqslant 90°$。

[0480] 如图 8 所示，图 8 中 500 表示摆放角度为 0 度的“五指张开平伸式”；508 表示摆放角度为 15 度的“五指张开平伸式”。如图 8 所示 500 至 507 都是人的右手；以右手为例，摆放角度 90° 等价于右手 500 沿逆时针方向旋转 90°；左手则与之相反，即左手的 500 沿顺时针方向旋转 90°。

[0481] 本发明中，手摆放角度的粒度为 1°，那么对于每一个手形，均存在 91 种摆放角度。所有对于每一个未知的手形，存在 637（$=7\times91$）种可能；对于一个长度为 N 的手形序列，则存在 $637^N$ 种组合。在本发明中，$N \geqslant 5$，即对于每一组手形序列，至少存在 104881082626957（$=637^5$）种组合。

[0482] 如图 8 中的 508，其中的几种摆放角度分别举例如下：

[0483] 1)0 度：即基准位置，手掌平伸，掌面与用户终端屏幕平行；指尖垂直向上。

[0484] 2)15 度：以基准位置为起始位置，逆时针旋转 15 度。

[0485] 3)-15 度：以基准位置为起始位置，顺时针旋转 15 度。

[0486] 4)30 度：以基准位置为起始位置，逆时针旋转 30 度。

[0487] 5)-30 度：以基准位置为起始位置，顺时针旋转 30 度。

[0488] 6)45 度：以基准位置为起始位置，逆时针旋转 45 度。

[0489] 7)-45 度：以基准位置为起始位置，顺时针旋转 45 度。

[0490] 上述各种手势的旋转角度可以根据实际情况选择开启或关闭，同时可以在认证用户身份的步骤中，不同手势采集的不同手形和上述各种旋转角度相互配合组成相应的掌纹手形序列向用户展示。用户可以按上述认证步骤在指定区域摆放相应的手势采集相应的手形图像参与认证过程。

[0491] 上述摆放角度的选择，为了进一步考虑人手的生理特性，即手掌在旋转角度上的难易程度；可以采用注册用户身份特征步骤中用户验证预置手势的方式验证预置摆放角度。在此就不再一一赘述了。同时考虑到了在手掌全部显示在用户终端屏幕采集框内的情

况下，手掌与用户终端的距离不要过大。

[0492] 另外，本发明的技术方案中还涉及到在用户终端屏幕上，手掌摆放指示框的显示。如图 8、图 10 所示，本发明选取了距离上下左右各 10％的矩形框来指示用户将手掌摆放至该矩形框。如图 8 中 508，图 10 中 518 所示，该矩形框还会随着当前摆放角度作相应的旋转。采用矩形框的形式还可以降低采集掌纹手形图像的数据处理时间。采集掌纹手形图像时可以仅裁切矩形框中的图形作为相应需要的掌纹手形图像。如图 10 中 518，同时用户终端会绘制出相应的手形指示图例也可以按照相应的摆放角度作相应的旋转。

[0493] 在本发明的另一个实施例中，为了进一步提高认证过程的安全性，在认证用户身份的步骤中，还可以进一步对每一种手势提供相应的逻辑运算，供用户根据自身需要作相应的选择。下面举例如下 ：

[0494] a) 逻辑运算 1 ：无论当前手势是哪一种，均摆出事先预置的指定手势。

[0495] b) 逻辑运算 2 ：对于全部（或部分）手势，摆出与之相反的手势。

[0496] c) 逻辑运算 3 ：对于全部（或部分）手势，摆出事先定义好的另外一种手势。

[0497] 在掌纹识别的步骤中，如果没有识别到通过逻辑运算的正确手势，并且图像中并不存在手掌区域，则反馈终端用户认证失败。如果没有识别到通过逻辑运算的正确手势，但图像中存在手掌区域，则返回流程 1，由终端继续采集图像。如果识别到通过逻辑运算的正确手势，则进行掌纹特征的提取与匹配，并保存匹配结果。

[0498] 本发明提供逻辑运算的目的是为了进一步提高身份认证的安全性，以逻辑运算 1 为例，在用户事先设置了规则“对于每次身份认证中出现的第一个手势，无论服务端要求摆出的手势是哪一种，均摆出开枪式手势（图 10 中 512)”的情况下，如果有恶意的攻击性行为，那么在不事先了解这条规则的情况下，用户就很有可能摆出错误的手势，而这种错误手势，在本发明中可以作为一种报警信息来处理。

[0499] 实施例 2

[0500] 本实施例与实施例 1 基本相同，其区别在于，本实施例应用于交易环境中对交易请求的身份验证。本实施例提供一种基于手势识别的安全认证方法，其特征在于 ：包括注册用户特征信息的步骤和认证用户身份的步骤 ；如图 1 所示，注册用户特征信息的步骤包括 ：用户终端采集用户的预置掌纹图像向服务端传输 ；服务端提取掌纹特征并保存预置掌纹特征 ；如图 2 所示。认证用户身份的步骤包括 ：用户终端向交易服务端发起交易请求，交易服务端向服务端发起认证请求 ；服务端生成掌纹手形序列并依序向用户终端传输并展示手形图像 ；用户按展示的手形图像依序做相应手势动作，用户终端采集用户带掌纹的认证手形图像向服务端传输 ；服务端提取手形、掌纹特征并与预置手形、掌纹特征匹配 ；服务端向交易服务端反馈匹配结果 ；交易服务端根据认证结果执行相应交易操作。下面对本发明提供的安全认证方法展开详细的说明。

[0501] 第一部分，介绍注册用户特征信息的步骤。

[0502] 注册用户特征信息时，需要先采集用户的预置掌纹图像，然后按掌纹识别方法提取掌纹特征并保存预置掌纹特征。

[0503] 如图 3 所示，注册用户特征信息时，用户终端向服务端发起注册用户特征请求 ；用户将平整的掌形（例如，手掌伸平、五指张开）放置于用户终端的图像采集区域，启动图像采集程序采集用户的预置掌纹图像 ；采集到预置掌纹图像后传输至服务端，服务端利用掌

纹识别方法提取预置掌纹图像中的用户的掌纹特征，对提取后掌纹特征保存。自此，注册用户特征步骤结束。在本实施例中，注册用户特征信息的步骤与实施例 1 完全相同，在注册用户特征信息的具体步骤请参考实施例 1 中的具体步骤和实施方案，为节约篇幅，在此就不再一一赘述了。

[0504] 第二部分，介绍认证用户身份的步骤。

[0505] 如图 12 所示，用户在交易场景中需要对用户身份认证时，需要通过本方法认证用户身份。认证用户身份时，用户通过用户终端向交易服务端发起交易请求，交易服务端向服务端发起认证请求；服务端生成掌纹手形序列并传输至用户终端，依序向用户展示手形图像；用户按展示的手形图像依序做相应手势动作，用户终端采集用户带掌纹的认证手形图像并传输至服务端；服务端按手形识别方法对带掌纹的认证手形图像作手形识别并与预置手形特征匹配；服务端按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配；服务端向交易服务端反馈匹配结果；交易服务端根据认证结果执行相应交易操作。下面对本实施例提供的安全认证方法展开详细的说明。

[0506] 首先，介绍用户终端向交易服务端发起交易请求，交易服务端向服务端发起认证请求的步骤。用户需要交易时，用户终端向交易服务端发起交易请求；交易服务端收到用户的交易请求时，交易服务端向安全认证服务器发起认证请求。如图 12 所示，当发起认证请求时，用户终端将认证请求信息打包后发送。优选以 XML 格式发送。认证请求信息包括用户终端的 ID、用户编号。在该步骤中，为了进一步保证数据验证的安全性，发起认证请求后服务端还需要进一步验证认证请求的合法性，因此在认证请求信息中还包括生成的随机编码。用户终端发起认证请求时封装的数据包格式示例如下：

[0507]

```
<?xml version="1.0" encoding="utf8" ?>
<require>
    <client_id value="1245789ab3!3dv" />    //用户用户终端的机器 ID
    <user_id value="EA1009803" />        //用户编号
       <require_id value="459B63D3_1232_47cb_B568_43475715B79C" />
       //请求的随机编号
    </ require>。
```

[0508] 交易服务端接收到用户终端的交易请求后，向服务端发送认证请求，待服务端反馈认证结果后，交易服务端将反馈结果发送给用户终端。交易服务端发向服务端发送认证请求时封装的数据包格式示例如下：

[0509]

```
<?xml version="1.0" encoding="utf8" ?>
<require>
    <client_id value="1245789ab3!3dv" />    //用户终端的机器 ID
    <user_id value="EA1009803" />        //用户编号
       <require_id value="459B63D3_1232_47cb_B568_43475715B79C" />
       //请求的随机编号
    </ require>。
```

[0510] 服务端收到交易服务端发送的认证请求数据包后，服务端读取认证请求数据包，通过验证随机编码的方式验证认证请求的合法性。服务端通过验证随机编码的方式验证认

证请求后安全认证服务器进一步核实用户编号，如果编号是合法的，则反馈给交易服务端“允许认证”，否则反馈“身份非法”。安全认证服务器向交易服务端反馈身份认证请求结果。服务端发向交易服务端发送认证请求结果时封装的数据包格式示例如下：

[0511]

```
<?xml version="1.0" encoding="utf8" ?>
<request>
      <require_id value="459B63D3_1232_47cb_B568_43475715B79C"
```

[0512]

```
result="1"/>
        //请求的随机编号，result 表示终端用户身份认证结果，0:表示身份非法，
1: 表示身份合法，允许认证。
    </ request >。
```

交易服务端将服务端反馈的认证请求结果发送至用户终端。交易服务端向用户终端发送认证请求结果时封装的数据包格式示例如下:

```
<?xml version="1.0" encoding="utf8" ?>
<request>
      <require_id value = "459B63D3_1232_47cb_B568_43475715B79C"
identify_url = "https://10.77.12.9/identify.asp ? id =
459B63D3_1232_47cb_B568_43475715B79C"/>
      //请求的随机编号， result 表示终端用户身份认证结果，identify_url:表示
用户终端需要访问的认证终端的地址，如果为空表示身份不合法。
    </ request >。
```

[0513] 服务端收到用户终端发送的认证请求数据包后，服务端读取认证请求数据包，通过验证随机编码的方式验证认证请求的合法性。如果验证通过，则启动一个认证线程进行后续的认证；如果验证不通过，则以消息形式向用户终端传送结果，告知用户认证请求非法，认证结束。用户终端在接收到交易服务端反馈的认证请求结果后，主动访问 identify_url 地址（例如：https://10.77.12.9/identify.asp ? id = 459B63D3_1232_47cb_B568_43475715B79C）。

[0514] 其次，介绍生成掌纹手形序列并依序向用户展示手形图像的步骤。

[0515] 如图 12 所示，生成掌纹手形序列并依序向用户展示手形图像的步骤与实施例 1 基本相同，在此就不再一一赘述了。安全认证服务器接收到客户端的认证请求后，会生成一套认证序列，并反馈给用户终端。服务端传输的手形信息数据包格式示例如下：

[0516]

```
<?xml version="1.0" encoding="utf8" ?>
<identify>
    < require_id value="459B63D3_1232_47cb_B568_43475715B79C" />
    //请求的随机编号
    <idetify_gesture_id value="5" />        //手形编号
    <idetify_gesture_angle value="15" />    //旋转角度
    </ identify >。
```

[0517] 再次，介绍用户按展示的手形图像依序做相应手势动作并采集用户带掌纹的认证手形图像的步骤。

[0518] 如图 12 所示，用户按展示的手形图像依序做相应手势动作并采集用户带掌纹的认证手形图像的步骤与实施例 1 基本相同，在此就不再一一赘述了。用户终端接收到服务器发送的认证要求后，会在用户终端绘制出相应的手形指示图例，并提示用户，用户终端同时在后台定时采集用户当前图像并发送给安全认证服务器。用户终端向服务端发送带掌纹的认证手形图像时封装的数据包格式示例如下：

[0519]

```
<?xml version="1.0" encoding="utf8" ?>
<identify>
< require_id value="459B63D3_1232_47cb_B568_43475715B79C" />
//请求的随机编号
<image_data value="qwerf45bvv90,31rdfvcxvcv" />          //加密图像的
base64 编码
</ identify >。
```

[0520] 第三，介绍按手形识别方法对带掌纹的认证手形图像作手形识别并与预置手形特征比对的步骤。

[0521] 如图 12 所示，按手形识别方法对带掌纹的认证手形图像作手形识别并与预置手形特征比对的步骤与实施例 1 基本相同，在此就不再一一赘述了。

[0522] 第四，介绍按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配的步骤。

[0523] 如图 12 所示，按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配的步骤与实施例 1 基本相同，在此就不再一一赘述了。安全认证服务器在接收到用户终端发送的图像后，会检测发送相应的任务给用户终端。服务端在比对采集的带掌纹的认证手形图像作手形、掌纹时安全认证服务器向用户终端发送消息封装的数据包格式示例如下：

[0524]

```
<?xml version="1.0" encoding="utf8" ?>
<identify>
< require_id value="459B63D3_1232_47cb_B568_43475715B79C" />
//请求的随机编号
<idetify_result_id value="1" />
//0: 匹配失败，继续采集图像; 1: 匹配成功，开始下一个手形; 2: 认证失败，
退出; 3: 认证成功，退出
<idetify_gesture_id value="5" />          //手形编号
<idetify_gesture_angle value="15" />      //旋转角度
</ identify >。
```

[0525] 如图 12 所示，为了保证认证过程的安全性，在按掌纹识别方法提取掌纹特征之前，采集用户带掌纹的认证手形图像时，需要确认采集区域的手掌是连续存在的，如果采集区域的手掌不连续则提示用户认证失败（例如在身份认证过程中，用户在执行掌纹手形图像序列时，用户将手移出用户终端的图像采集区域，则认为该身份认证请求非法，提示用户认证请求失败，需重新认证身份）。本发明的技术方案中，确认采集区域的手掌是连续存在的目的在于，了防止恶意的伪造终端采集图像的行为，从而进一步提高身份认证的安全性。

[0526] 在本发明的一个实施例中，采集用户带掌纹的认证手形图像时，确认采集区域的掌纹手形图像是否连续存时，采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续。手形区域跟踪算法优选 CamShift 算法来实现对手区域的跟踪。下面对采用

CamShift 算法对手区域的跟踪的步骤详细说明。

[0527] 本发明中采用 CamShift 算法来实现对手区域的跟踪。具体流程如下：

[0528] 1) 在第一次检测到正确的手形后，将手形掩膜中的最小单元 P 所对应的区域作为跟踪区域。

[0529] 2) 对跟踪区域的图像进行反向投影 (Back Projection)，具体作法是：首先将图像转换至 HIS 空间，然后取 H 分量提取现 1D 直方图，即区域中每个象素值的概率分布图。

[0530] 3) 跟踪过程采用 MeanShift（均值漂移）方法。

[0531] 4) 对于新到来的图像，采用 CamShift（称为连续自适应的 MeanShift 算法）方法来进行更新。

[0532] 如图 12 所示，为了保证认证过程的安全性，本发明的一个实施例中，在认证用户身份的步骤中本发明还提供对用户手势按指定角度摆放并验证的步骤。本发明的技术方案还预置了多种摆放角度度 AI，取 $0° \leqslant AI \leqslant 90°$。

[0533] 如图 8 所示，图 8 中 500 表示摆放角度为 0 度的“五指张开平伸式”；508 表示摆放角度为 15 度的“五指张开平伸式”。如图 8 所示 500 至 507 都是人的右手；以右手为例，摆放角度 90° 等价于右手 500 沿逆时针方向旋转 90°；左手则与之相反，即左手的 500 沿顺时针方向旋转 90°。

[0534] 本发明中，手摆放角度的粒度为 1°，那么对于每一个手形，均存在 91 种摆放角度。所有对于每一个未知的手形，存在 637（$= 7 \times 91$）种可能；对于一个长度为 N 的手形序列，则存在 $637^N$ 种组合。在本发明中，NN5，即对于每一组手形序列，至少存在 104881082626957（$= 637^5$）种组合。

[0535] 如图 8 中的 508，其中的几种摆放角度分别举例如下：

[0536] 8)0 度：即基准位置，手掌平伸，掌面与用户终端屏幕平行；指尖垂直向上。

[0537] 9)15 度：以基准位置为起始位置，逆时针旋转 15 度。

[0538] 10)-15 度：以基准位置为起始位置，顺时针旋转 15 度。

[0539] 11)30 度：以基准位置为起始位置，逆时针旋转 30 度。

[0540] 12)-30 度：以基准位置为起始位置，顺时针旋转 30 度。

[0541] 13)45 度：以基准位置为起始位置，逆时针旋转 45 度。

[0542] 14)-45 度：以基准位置为起始位置，顺时针旋转 45 度。

[0543] 上述各种手势的旋转角度可以根据实际情况选择开启或关闭，同时可以在认证用户身份的步骤中，不同手势采集的不同手形和上述各种旋转角度相互配合组成相应的掌纹手形序列向用户展示。用户可以按上述认证步骤在指定区域摆放相应的手势采集相应的手形图像参与认证过程。

[0544] 上述摆放角度的选择，为了进一步考虑人手的生理特性，即手掌在旋转角度上的难易程度；可以采用注册用户身份特征步骤中用户验证预置手势的方式验证预置摆放角度。在此就不再一一赘述了。同时考虑到了在手掌全部显示在用户终端屏幕采集框内的情况下，手掌与用户终端的距离不要过大。

[0545] 另外，本发明的技术方案中还涉及到在用户终端屏幕上，手掌摆放指示框的显示。如图 8、图 10 所示，本发明选取了距离上下左右各 10％的矩形框来指示用户将手掌摆放至该矩形框。如图 8 中 508，图 10 中 518 所示，该矩形框还会随着当前摆放角度作相应的旋

转。采用矩形框的形式还可以降低采集掌纹手形图像的数据处理时间。采集掌纹手形图像时可以仅裁切矩形框中的图形作为相应需要的掌纹手形图像。如图 10 中 518，同时用户终端会绘制出相应的手形指示图例也可以按照相应的摆放角度作相应的旋转。

[0546] 在本发明的另一个实施例中，为了进一步提高认证过程的安全性，在认证用户身份的步骤中，还可以进一步对每一种手势提供相应的逻辑运算，供用户根据自身需要作相应的选择。下面举例如下：

[0547] (a) 逻辑运算 1：无论当前手势是哪一种，均摆出事先预置的指定手势。

[0548] (b) 逻辑运算 2：对于全部（或部分）手势，摆出与之相反的手势。

[0549] (c) 逻辑运算 3：对于全部（或部分）手势，摆出事先定义好的另外一种手势。

[0550] 本发明提供逻辑运算的目的是为了进一步提高身份认证的安全性，以逻辑运算 1 为例，在用户事先设置了规则“对于每次身份认证中出现的第一个手势，无论服务端要求摆出的手势是哪一种，均摆出开枪式手势（图 10 中 512）”的情况下，如果有恶意的攻击性行为，那么在不事先了解这条规则的情况下，用户就很有可能摆出错误的手势，而这种错误手势，在本发明中可以作为一种报警信息来处理。

[0551] 最后，介绍服务端向交易服务端反馈匹配结果，交易服务端根据认证结果执行相应交易操作。

[0552] 服务端对用户身份验证后向交易服务端传送认证结果，交易服务端根据认证结果处理交易请求。如果认证结果是认证通过，则交易服务端执行相应的交易操作。如果认证失败，则向用户终端反馈重新认证或交易失败的信息。认证完成后，用户终端会接收到来自安全认证服务器的认证结果，同时也可以通过查询交易服务端获得相应的交易结果。无论认证成功或失败，安全认证服务器都会在认证结束后主动发送结果至交易服务端。服务端向交易服务端发送认证结果时封装的数据包格式示例如下：

[0553]

```
<?xml version="1.0" encoding="utf8" ?>
<trade>
    <require_id value="459B63D3_1232_47cb_B568_43475715B79C"  result="
1" />
```

[0554]

```
    //请求的随机编号，result 表示终端用户身份认证结果，0:表示认证失败，
1: 表示认证成功。
    </ trade >。
```

[0555] 实施例 3

[0556] 为进一步体现发明提供的安全认证方法的优越性，本发明还提供一种应用上述安全认证方法的安全认证系统，如图 13 所示，该系统包括：服务端和用户终端；服务端与用户终端通信连接；用户终端采集用户的预置掌纹图像并发送至服务端，服务端按掌纹识别方法提取掌纹特征并保存预置掌纹特征；用户终端向服务端发起认证请求，服务端生成掌纹手形序列并传输至用户终端，用户终端依序展示手形图像，用户按用户终端展示的手形图像依序做相应手势动作，用户终端采集用户的带掌纹的手形图像并传输至服务端，服务端按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，服务端按匹配结果向用户终端反馈认证结果。下面对本发明提供的安全认证系统展开详细的说明。

[0557] 如图13、图14所示，在本发明提供的安全认证系统中，用户终端可以是PC、可以是PAD、也可以是手机等一切可以采集图像的电子设备。用户终端需要通过自身的图像采集装置采集用户特征信息。图像采集装置优选是摄像头。用户终端包括数据收发模块、业务逻辑模块图像采集模块。交互界面模块、数据收发模块、图像采集模块分别与业务逻辑模块通信连接，图像采集模块与数据收发模块通信连接。用户通过交互界面模块向业务逻辑模块发起指令，业务逻辑模块控制通过数据收发模块向服务端发送注册或认证请求，业务逻辑模块控制图像采集模块采集掌纹手形图像并通过数据收发模块向服务端传输。业务逻辑模块控制数据交互模块接收服务端传输的掌纹手形序列并传输至交互界面模块依序向用户展示手形图像。

[0558] 如图14所示，为了进一步保证数据的安全性，用户终端还包括数据加密模块，业务逻辑模块、图像采集模块与数据加密模块通信连接，数据加密模块与数据收发模块连接。图像采集模块采集的图像通过数据加密模块加密后通过数据收发模块传输。

[0559] 如图15所示，为了保证在网络状况不佳的情况下仍然可以通过用户终端注册用户特征信息或认证用户身份，用户终端还包括图像预处理模块，业务逻辑模块、图像采集模块与图像预处理模块通信连接。业务逻辑模块控制图像预处理模块将图像采集模块采集的图像信息作预处理，将预处理后的图像通过数据收发单元传输。在本发明提供的安全认证系统中图像预处理模块对图像采集模块采集的图像信息（含预处理预置掌纹图像和认证手形图像）作预处理预置掌纹图像预处理的步骤与上述安全认证方法中的预处理步骤相同，在此就不再一一赘述了。如图15所示，进一步地，图像采集模块采集的图像数据可以先通过图像预处理模块处理，再经数据加密模块加密处理后通过数据收发模块传输。

[0560] 如图13、图17所示，服务端包括带身份认证功能的安全认证服务器和数据库，数据库包括掌纹特征数据库和手形设置数据库。掌纹特征数据库和手形设置数据库与安全认证服务器通信连接。安全认证服务器包括数据收发模块、手形识别模块、掌纹识别模块和动态手形生成模块。数据收发模块分别与手形识别模块、掌纹识别模块和动态手形生成模块连接，手形识别模块、动态手形生成模块分别与手形设置数据库连接，掌纹识别模块与掌纹特征数据库连接；注册用户特征信息时：数据收发模块将接收的预置掌纹图像传输至掌纹识别模块提取掌纹特征并保存在掌纹特征数据库中，并通过数据收发模块发送反馈注册结果至用户终端；认证用户身份时：动态手形生成模块按预置手形图像生成掌纹手形序列通过数据收发模块传输至用户终端；数据收发模块将接收的认证手形图像传输至手形识别模块、掌纹识别模块提取手形、掌纹特征并与手形设置数据库、掌纹特征数据库中的预置手形、掌纹特征匹配；手形识别模块、掌纹识别模块根据匹配结果通过数据收发模块向用户终端反馈认证结果。掌纹识别模块提取预置掌纹图像中或认证手形图像中的用户掌纹特征的步骤与上述安全认证方法中的提取掌纹特征的步骤相同，在此就不再一一赘述了。手形识别模块识别认证手形图像中手形的步骤与上述安全认证方法中的手形识别步骤相同，在此就不再一一赘述了。

[0561] 如图16、17所示，为了进一步保证数据的安全性，安全认证服务器还包括与用户终端对应的数据解密模块，数据收发模块和掌纹识别模块分别与数据解密模块连接，安全认证服务器收到用户终端加密的图像后，通过数据收发模块发送至数据解密模块，由数据解密模块解密处理后再传送至掌纹识别模块处理。

[0562] 如图 17 所示，为了进一步保证身份认证的安全性，服务端还包括手掌跟踪模块：手掌跟踪模块与数据收发模块连接；手掌跟踪模块在采集用户带掌纹的认证手形图像时，采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；如果采集区域的手掌不连续存在则通过数据收发模块提示用户认证失败；如果采集区域的手掌连续存在则通过数据收发模块提示用户继续采集其他掌纹手形图像。

[0563] 如图 17 所示，服务端还包括识别决策模块：识别决策模块分别与手形识别模块、掌纹识别模块连接；服务端将认证掌纹图像识别匹配处理后，识别决策模块判断生成的掌纹手形序列是否已经采集、识别、匹配完成；如果未完成掌纹手形序列，则识别决策模块向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；如果掌纹手形序列已完成，则识别决策模块查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作，则通过数据收发模块向用户终端传输认证成功的消息；如果无匹配成功的掌纹信息匹配结果则通过数据收发模块向用户终端传输认证失败的消息。

[0564] 实施例 4

[0565] 为进一步体现发明提供的安全认证方法的优越性，本发明还提供一种应用上述安全认证方法的安全认证系统，用户在交易或其它需要验证用户场景时，需要通过本安全认证系统认证用户身份。如图 18 所示，该安全认证系统包括服务端和用户终端；服务器与用户终端通信连接；还包括与服务器和用户终端通信连接的交易服务端；用户终端采集用户的预置掌纹图像并发送至服务端，服务端按掌纹识别方法提取掌纹特征并保存预置掌纹特征；用户通过用户终端向交易服务端发起交易认证请求，交易服务端向服务端发起身份能认证请求，服务端生成掌纹手形序列并传输至用户终端，用户终端依序展示手形图像，用户按用户终端展示的手形图像依序做相应手势动作，用户终端采集用户的带掌纹的手形图像并传输至服务端，服务端按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，服务端向交易服务端用户终端反馈匹配结果，交易服务端根据反馈的匹配结果通过用户终端发动交易结果信息。下面对本发明提供的安全认证系统展开详细的说明。

[0566] 如图 14 所示，用户终端包括：数据收发模块、业务逻辑模块图像采集模块；交互界面模块、数据收发模块、图像采集模块分别与业务逻辑模块通信连接，图像采集模块与数据收发模块通信连接；用户通过交互界面模块向业务逻辑模块发起指令，业务逻辑模块控制通过数据收发模块向服务端发送注册或认证请求，业务逻辑模块控制图像采集模块采集掌纹手形图像并通过数据收发模块向服务端传输；业务逻辑模块控制数据交互模块接收服务端传输的掌纹手形序列并传输至交互界面模块依序向用户展示手形图像。

[0567] 如图 15 所示，用户终端还包括数据加密模块，业务逻辑模块、图像采集模块与数据加密模块通信连接，数据加密模块与数据收发模块连接；图像采集模块采集的图像通过数据加密模块加密后通过数据收发模块传输。

[0568] 如图 15 所示，用户终端还包括图像预处理模块；业务逻辑模块、图像采集模块与图像预处理模块通信连接；业务逻辑模块控制图像预处理模块将图像采集模块采集的图像信息作预处理，将预处理后的图像通过数据收发单元传输。在本发明提供的安全认证系统中图像预处理模块对图像采集模块采集的图像信息（含预处理预置掌纹图像和认证手形图像）作预处理预置掌纹图像预处理的步骤与上述安全认证方法中的预处理步骤相同，在

此就不再一一赘述了。如图 15 所示，进一步地，图像采集模块采集的图像数据可以先通过图像预处理模块处理，再经数据加密模块加密处理后通过数据收发模块传输。

[0569] 如图 13、图 17 所示，服务端包括：带身份认证功能的安全认证服务器和数据库，数据库包括掌纹特征数据库和手形设置数据库；掌纹特征数据库和手形设置数据库与安全认证服务器通信连接；安全认证服务器包括数据收发模块、手形识别模块、掌纹识别模块和动态手形生成模块；数据收发模块分别与手形识别模块、掌纹识别模块和动态手形生成模块连接，手形识别模块、动态手形生成模块分别与手形设置数据库连接，掌纹识别模块与掌纹特征数据库连接；注册用户特征信息时：数据收发模块将接收的预置掌纹图像传输至掌纹识别模块提取掌纹特征并保存在掌纹特征数据库中，并通过数据收发模块发送反馈注册结果至用户终端；认证用户身份时：动态手形生成模块按预置手形图像生成掌纹手形序列通过数据收发模块传输至用户终端；数据收发模块将接收的认证手形图像传输至手形识别模块、掌纹识别模块提取手形、掌纹特征并与手形设置数据库、掌纹特征数据库中的预置手形、掌纹特征匹配；手形识别模块、掌纹识别模块根据匹配结果通过数据收发模块向用户终端反馈认证结果。掌纹识别模块提取预置掌纹图像中或认证手形图像中的用户掌纹特征的步骤与上述安全认证方法中的提取掌纹特征的步骤相同，在此就不再一一赘述了。手形识别模块识别认证手形图像中手形的步骤与上述安全认证方法中的手形识别步骤相同，在此就不再一一赘述了。

[0570] 如图 16、图 17 所示，服务端还包括与用户终端对应的数据解密模块；数据收发模块和掌纹识别模块分别与数据解密模块连接；安全认证服务器收到用户终端加密的图像后，通过数据收发模块发送至数据解密模块，由数据解密模块解密处理后再处理。

[0571] 如图 17 所示，服务端还包括手掌跟踪模块：手掌跟踪模块与数据收发模块连接；手掌跟踪模块在采集用户带掌纹的认证手形图像时，采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；如果采集区域的手掌不连续存在则通过数据收发模块提示用户认证失败；如果采集区域的手掌连续存在则通过数据收发模块提示用户继续采集其他掌纹手形图像。

[0572] 如图 17 所示，服务端还包括识别决策模块：识别决策模块分别与手形识别模块、掌纹识别模块连接；服务端将认证掌纹图像识别匹配处理后，识别决策模块判断生成的掌纹手形序列是否已经采集、识别、匹配完成；如果未完成掌纹手形序列，则识别决策模块向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；如果掌纹手形序列已完成，则识别决策模块查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作，则通过数据收发模块向用户终端传输认证成功的消息；如果无匹配成功的掌纹信息匹配结果则通过数据收发模块向用户终端传输认证失败的消息。

[0573] 实施例 5

[0574] 如图 13 所示，本发明提供一种基于手势识别的安全认证服务器，安全认证服务器用于在安全认证系统中认证用户的权限；安全认证服务器与用户终端通信连接；安全认证服务器接收用户终端采集用户的预置掌纹图像，安全认证服务器按掌纹识别方法提取掌纹特征并保存预置掌纹特征；安全认证服务器接收用户终端向安全认证服务器发起认证请求，安全认证服务器生成掌纹手形序列并传输至用户终端，用户终端依序展示手形图像，用

户按用户终端展示的手形图像依序做相应手势动作，用户终端采集用户的带掌纹的手形图像并传输至安全认证服务器，安全认证服务器按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，安全认证服务器按匹配结果向用户终端反馈认证结果。

[0575] 如图 14 所示，用户终端包括：数据收发模块、业务逻辑模块图像采集模块；交互界面模块、数据收发模块、图像采集模块分别与业务逻辑模块通信连接，图像采集模块与数据收发模块通信连接；用户通过交互界面模块向业务逻辑模块发起指令，业务逻辑模块控制通过数据收发模块向安全认证服务器发送注册或认证请求，业务逻辑模块控制图像采集模块采集掌纹手形图像并通过数据收发模块向安全认证服务器传输；业务逻辑模块控制数据交互模块接收服务器传输的掌纹手形序列并传输至交互界面模块依序向用户展示手形图像。

[0576] 如图 15 所示，用户终端还包括数据加密模块，业务逻辑模块、图像采集模块与数据加密模块通信连接，数据加密模块与数据收发模块连接；图像采集模块采集的图像通过数据加密模块加密后通过数据收发模块传输。

[0577] 如图 15 所示，用户终端还包括图像预处理模块；业务逻辑模块、图像采集模块与图像预处理模块通信连接；业务逻辑模块控制图像预处理模块将图像采集模块采集的图像信息作预处理，将预处理后的图像通过数据收发单元传输。在本发明提供的安全认证系统中图像预处理模块对图像采集模块采集的图像信息（含预处理预置掌纹图像和认证手形图像）作预处理预置掌纹图像预处理的步骤与上述安全认证方法中的预处理步骤相同，在此就不再一一赘述了。如图 15 所示，进一步地，图像采集模块采集的图像数据可以先通过图像预处理模块处理，再经数据加密模块加密处理后通过数据收发模块传输。

[0578] 如图 13、图 17 所示，服务器包括：带身份认证功能的安全认证服务器和数据库，数据库包括掌纹特征数据库和手形设置数据库；掌纹特征数据库和手形设置数据库与安全认证服务器通信连接；安全认证服务器包括数据收发模块、手形识别模块、掌纹识别模块和动态手形生成模块；数据收发模块分别与手形识别模块、掌纹识别模块和动态手形生成模块连接，手形识别模块、动态手形生成模块分别与手形设置数据库连接，掌纹识别模块与掌纹特征数据库连接；注册用户特征信息时：数据收发模块将接收的预置掌纹图像传输至掌纹识别模块提取掌纹特征并保存在掌纹特征数据库中，并通过数据收发模块发送反馈注册结果至用户终端；认证用户身份时：动态手形生成模块按预置手形图像生成掌纹手形序列通过数据收发模块传输至用户终端；数据收发模块将接收的认证手形图像传输至手形识别模块、掌纹识别模块提取手形、掌纹特征并与手形设置数据库、掌纹特征数据库中的预置手形、掌纹特征匹配；手形识别模块、掌纹识别模块根据匹配结果通过数据收发模块向用户终端反馈认证结果。掌纹识别模块提取预置掌纹图像中或认证手形图像中的用户掌纹特征的步骤与上述安全认证方法中的提取掌纹特征的步骤相同，在此就不再一一赘述了。手形识别模块识别认证手形图像中手形的步骤与上述安全认证方法中的手形识别步骤相同，在此就不再一一赘述了。

[0579] 如图 16、图 17 所示，安全认证服务器还包括与用户终端对应的数据解密模块；数据收发模块和掌纹识别模块分别与数据解密模块连接；安全认证服务器收到用户终端加密的图像后，通过数据收发模块发送至数据解密模块，由数据解密模块解密处理后再处理。

[0580] 如图 17 所示，安全认证服务器还包括手掌跟踪模块：手掌跟踪模块与数据收发模

块连接；手掌跟踪模块在采集用户带掌纹的认证手形图像时，采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；如果采集区域的手掌不连续存在则通过数据收发模块提示用户认证失败；如果采集区域的手掌连续存在则通过数据收发模块提示用户继续采集其他掌纹手形图像。

[0581] 如图 17 所示，安全认证服务器还包括识别决策模块：识别决策模块分别与手形识别模块、掌纹识别模块连接；安全认证服务器将认证掌纹图像识别匹配处理后，识别决策模块判断生成的掌纹手形序列是否已经采集、识别、匹配完成；如果未完成掌纹手形序列，则识别决策模块向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；如果掌纹手形序列已完成，则识别决策模块查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作，则通过数据收发模块向用户终端传输认证成功的消息；如果无匹配成功的掌纹信息匹配结果则通过数据收发模块向用户终端传输认证失败的消息。

[0582] 实施例 6

[0583] 如图 18 所示，本发明提供一种基于手势识别的安全认证服务器，安全认证服务器用于在安全认证系统中认证用户的权限；安全认证服务器与用户终端和交易服务器通信连接；安全认证服务器接收用户终端采集用户的预置掌纹图像，安全认证服务器按掌纹识别方法提取掌纹特征并保存预置掌纹特征；用户通过用户终端向交易服务器发起交易认证请求，安全认证服务器接收交易服务器向安全认证服务器发起认证请求，安全认证服务器生成掌纹手形序列并传输至用户终端，用户终端依序展示手形图像，用户按用户终端展示的手形图像依序做相应手势动作，用户终端采集用户的带掌纹的手形图像并传输至安全认证服务器，安全认证服务器按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，服务器向交易服务器用户终端反馈匹配结果，交易服务器根据反馈的匹配结果通过用户终端发动交易结果信息。

[0584] 如图 14 所示，用户终端包括：数据收发模块、业务逻辑模块图像采集模块；交互界面模块、数据收发模块、图像采集模块分别与业务逻辑模块通信连接，图像采集模块与数据收发模块通信连接；用户通过交互界面模块向业务逻辑模块发起指令，业务逻辑模块控制通过数据收发模块向安全认证服务器发送注册或认证请求，业务逻辑模块控制图像采集模块采集掌纹手形图像并通过数据收发模块向安全认证服务器传输；业务逻辑模块控制数据交互模块接收服务器传输的掌纹手形序列并传输至交互界面模块依序向用户展示手形图像。

[0585] 如图 15 所示，用户终端还包括数据加密模块，业务逻辑模块、图像采集模块与数据加密模块通信连接，数据加密模块与数据收发模块连接；图像采集模块采集的图像通过数据加密模块加密后通过数据收发模块传输。

[0586] 如图 15 所示，用户终端还包括图像预处理模块；业务逻辑模块、图像采集模块与图像预处理模块通信连接；业务逻辑模块控制图像预处理模块将图像采集模块采集的图像信息作预处理，将预处理后的图像通过数据收发单元传输。在本发明提供的安全认证系统中图像预处理模块对图像采集模块采集的图像信息（含预处理预置掌纹图像和认证手形图像）作预处理预置掌纹图像预处理的步骤与上述安全认证方法中的预处理步骤相同，在此就不再一一赘述了。如图 15 所示，进一步地，图像采集模块采集的图像数据可以先通过

图像预处理模块处理，再经数据加密模块加密处理后通过数据收发模块传输。

[0587] 如图 13、图 17 所示，安全认证服务器包括：带身份认证功能的安全认证服务器和数据库，数据库包括掌纹特征数据库和手形设置数据库；掌纹特征数据库和手形设置数据库与安全认证服务器通信连接；安全认证服务器包括数据收发模块、手形识别模块、掌纹识别模块和动态手形生成模块；数据收发模块分别与手形识别模块、掌纹识别模块和动态手形生成模块连接，手形识别模块、动态手形生成模块分别与手形设置数据库连接，掌纹识别模块与掌纹特征数据库连接；注册用户特征信息时：数据收发模块将接收的预置掌纹图像传输至掌纹识别模块提取掌纹特征并保存在掌纹特征数据库中，并通过数据收发模块发送反馈注册结果至用户终端；认证用户身份时：动态手形生成模块按预置手形图像生成掌纹手形序列通过数据收发模块传输至用户终端；数据收发模块将接收的认证手形图像传输至手形识别模块、掌纹识别模块提取手形、掌纹特征并与手形设置数据库、掌纹特征数据库中的预置手形、掌纹特征匹配；手形识别模块、掌纹识别模块根据匹配结果通过数据收发模块向用户终端反馈认证结果。掌纹识别模块提取预置掌纹图像中或认证手形图像中的用户掌纹特征的步骤与上述安全认证方法中的提取掌纹特征的步骤相同，在此就不再一一赘述了。手形识别模块识别认证手形图像中手形的步骤与上述安全认证方法中的手形识别步骤相同，在此就不再一一赘述了。

[0588] 如图 16、图 17 所示，安全认证服务器还包括与用户终端对应的数据解密模块；数据收发模块和掌纹识别模块分别与数据解密模块连接；安全认证服务器收到用户终端加密的图像后，通过数据收发模块发送至数据解密模块，由数据解密模块解密处理后再处理。

[0589] 如图 17 所示，安全认证服务器还包括手掌跟踪模块：手掌跟踪模块与数据收发模块连接；手掌跟踪模块在采集用户带掌纹的认证手形图像时，采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；如果采集区域的手掌不连续存在则通过数据收发模块提示用户认证失败；如果采集区域的手掌连续存在则通过数据收发模块提示用户继续采集其他掌纹手形图像。

[0590] 如图 17 所示，安全认证服务器还包括识别决策模块：识别决策模块分别与手形识别模块、掌纹识别模块连接；安全认证服务器将认证掌纹图像识别匹配处理后，识别决策模块判断生成的掌纹手形序列是否已经采集、识别、匹配完成；如果未完成掌纹手形序列，则识别决策模块向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；如果掌纹手形序列已完成，则识别决策模块查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作，则通过数据收发模块向用户终端传输认证成功的消息；如果无匹配成功的掌纹信息匹配结果则通过数据收发模块向用户终端传输认证失败的消息。

[0591] 实施例 7

[0592] 如图 13 所示，本发明提供一种基于手势识别的安全认证用户终端，其特征在于：用户终端用于在安全认证系统中认证用户的权限；用户终端可以是 PC、可以是 PAD、也可以是手机等一切可以采集图像的电子设备。用户终端需要通过自身的图像采集装置采集用户特征信息。图像采集装置优选是摄像头。安全认证服务器与用户终端通信连接；用户终端采集用户的预置掌纹图像传输至安全认证服务器，安全认证服务器按掌纹识别方法提取掌纹特征并保存预置掌纹特征；安全认证服务器接收用户终端向安全认证服务器发起认证请

求，安全认证服务器生成掌纹手形序列并传输至用户终端，用户终端依序展示手形图像，用户按用户终端展示的手形图像依序做相应手势动作，用户终端采集用户的带掌纹的手形图像并传输至安全认证服务器，安全认证服务器按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，安全认证服务器按匹配结果向用户终端反馈认证结果。

[0593] 如图 14 所示，用户终端包括：数据收发模块、业务逻辑模块图像采集模块；交互界面模块、数据收发模块、图像采集模块分别与业务逻辑模块通信连接，图像采集模块与数据收发模块通信连接；用户通过交互界面模块向业务逻辑模块发起指令，业务逻辑模块控制通过数据收发模块向安全认证服务器发送注册或认证请求，业务逻辑模块控制图像采集模块采集掌纹手形图像并通过数据收发模块向安全认证服务器传输；业务逻辑模块控制数据交互模块接收服务器传输的掌纹手形序列并传输至交互界面模块依序向用户展示手形图像。

[0594] 如图 15 所示，用户终端还包括数据加密模块，业务逻辑模块、图像采集模块与数据加密模块通信连接，数据加密模块与数据收发模块连接；图像采集模块采集的图像通过数据加密模块加密后通过数据收发模块传输。

[0595] 如图 15 所示，用户终端还包括图像预处理模块；业务逻辑模块、图像采集模块与图像预处理模块通信连接；业务逻辑模块控制图像预处理模块将图像采集模块采集的图像信息做预处理，将预处理后的图像通过数据收发单元传输。在本发明提供的安全认证系统中图像预处理模块对图像采集模块采集的图像信息（含预处理预置掌纹图像和认证手形图像）作预处理预置掌纹图像预处理的步骤与上述安全认证方法中的预处理步骤相同，在此就不再一一赘述了。如图 15 所示，进一步地，图像采集模块采集的图像数据可以先通过图像预处理模块处理，再经数据加密模块加密处理后通过数据收发模块传输。

[0596] 如图 13、图 17 所示，安全认证服务器包括：带身份认证功能的安全认证服务器和数据库，数据库包括掌纹特征数据库和手形设置数据库；掌纹特征数据库和手形设置数据库与安全认证服务器通信连接；安全认证服务器包括数据收发模块、手形识别模块、掌纹识别模块和动态手形生成模块；数据收发模块分别与手形识别模块、掌纹识别模块和动态手形生成模块连接，手形识别模块、动态手形生成模块分别与手形设置数据库连接，掌纹识别模块与掌纹特征数据库连接；注册用户特征信息时：数据收发模块将接收的预置掌纹图像传输至掌纹识别模块提取掌纹特征并保存在掌纹特征数据库中，并通过数据收发模块发送反馈注册结果至用户终端；认证用户身份时：动态手形生成模块按预置手形图像生成掌纹手形序列通过数据收发模块传输至用户终端；数据收发模块将接收的认证手形图像传输至手形识别模块、掌纹识别模块提取手形、掌纹特征并与手形设置数据库、掌纹特征数据库中的预置手形、掌纹特征匹配；手形识别模块、掌纹识别模块根据匹配结果通过数据收发模块向用户终端反馈认证结果。掌纹识别模块提取预置掌纹图像中或认证手形图像中的用户掌纹特征的步骤与上述安全认证方法中的提取掌纹特征的步骤相同，在此就不再一一赘述了。手形识别模块识别认证手形图像中手形的步骤与上述安全认证方法中的手形识别步骤相同，在此就不再一一赘述了。

[0597] 如图 16、图 17 所示，安全认证服务器还包括与用户终端对应的数据解密模块；数据收发模块和掌纹识别模块分别与数据解密模块连接；安全认证服务器收到用户终端加密的图像后，通过数据收发模块发送至数据解密模块，由数据解密模块解密处理后再处理。

[0598] 如图 17 所示，安全认证服务器还包括手掌跟踪模块；手掌跟踪模块与数据收发模块连接；手掌跟踪模块在采集用户带掌纹的认证手形图像时，采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；如果采集区域的手掌不连续存在则通过数据收发模块提示用户认证失败；如果采集区域的手掌连续存在则通过数据收发模块提示用户继续采集其他掌纹手形图像。

[0599] 如图 17 所示，安全认证服务器还包括识别决策模块；识别决策模块分别与手形识别模块、掌纹识别模块连接；安全认证服务器将认证掌纹图像识别匹配处理后，识别决策模块判断生成的掌纹手形序列是否已经采集、识别、匹配完成；如果未完成掌纹手形序列，则识别决策模块向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；如果掌纹手形序列已完成，则识别决策模块查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作，则通过数据收发模块向用户终端传输认证成功的消息；如果无匹配成功的掌纹信息匹配结果则通过数据收发模块向用户终端传输认证失败的消息。

[0600] 实施例 8

[0601] 如图 18 所示，本发明提供一种基于手势识别的安全认证用户终端，用户终端用于在安全认证系统中认证用户的权限；用户终端可以是 PC、可以是 PAD、也可以是手机等一切可以采集图像的电子设备。用户终端需要通过自身的图像采集装置采集用户特征信息。图像采集装置优选是摄像头。用户终端与安全认证服务和交易服务器通信连接；用户终端采集用户的预置掌纹图像传输至安全认证服务器，安全认证服务器按掌纹识别方法提取掌纹特征并保存预置掌纹特征；用户终端向交易服务器发起交易认证请求，安全认证服务器接收交易服务器向安全认证服务器发起认证请求，安全认证服务器生成掌纹手形序列并传输至用户终端，用户终端依序展示手形图像，用户按用户终端展示的手形图像依序做相应手势动作，用户终端采集用户的带掌纹的手形图像并传输至安全认证服务器，安全认证服务器按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配，服务器向交易服务器用户终端反馈匹配结果，交易服务器根据反馈的匹配结果通过用户终端发动交易结果信息。

[0602] 如图 14 所示，用户终端包括：数据收发模块、业务逻辑模块图像采集模块；交互界面模块、数据收发模块、图像采集模块分别与业务逻辑模块通信连接，图像采集模块与数据收发模块通信连接；用户通过交互界面模块向业务逻辑模块发起指令，业务逻辑模块控制通过数据收发模块向安全认证服务器发送注册或认证请求，业务逻辑模块控制图像采集模块采集掌纹手形图像并通过数据收发模块向安全认证服务器传输；业务逻辑模块控制数据交互模块接收服务器传输的掌纹手形序列并传输至交互界面模块依序向用户展示手形图像。

[0603] 如图 15 所示，用户终端还包括数据加密模块，业务逻辑模块、图像采集模块与数据加密模块通信连接，数据加密模块与数据收发模块连接；图像采集模块采集的图像通过数据加密模块加密后通过数据收发模块传输。

[0604] 如图 15 所示，用户终端还包括图像预处理模块；业务逻辑模块、图像采集模块与图像预处理模块通信连接；业务逻辑模块控制图像预处理模块将图像采集模块采集的图像信息作预处理，将预处理后的图像通过数据收发单元传输。在本发明提供的安全认证系统中图像预处理模块对图像采集模块采集的图像信息（含预处理预置掌纹图像和认证手形

图像）作预处理预置掌纹图像预处理的步骤与上述安全认证方法中的预处理步骤相同，在此就不再一一赘述了。如图 15 所示，进一步地，图像采集模块采集的图像数据可以先通过图像预处理模块处理，再经数据加密模块加密处理后通过数据收发模块传输。

[0605] 如图 13、图 17 所示，安全认证服务器包括：带身份认证功能的安全认证服务器和数据库，数据库包括掌纹特征数据库和手形设置数据库；掌纹特征数据库和手形设置数据库与安全认证服务器通信连接；安全认证服务器包括数据收发模块、手形识别模块、掌纹识别模块和动态手形生成模块；数据收发模块分别与手形识别模块、掌纹识别模块和动态手形生成模块连接，手形识别模块、动态手形生成模块分别与手形设置数据库连接，掌纹识别模块与掌纹特征数据库连接；注册用户特征信息时：数据收发模块将接收的预置掌纹图像传输至掌纹识别模块提取掌纹特征并保存在掌纹特征数据库中，并通过数据收发模块发送反馈注册结果至用户终端；认证用户身份时：动态手形生成模块按预置手形图像生成掌纹手形序列通过数据收发模块传输至用户终端；数据收发模块将接收的认证手形图像传输至手形识别模块、掌纹识别模块提取手形、掌纹特征并与手形设置数据库、掌纹特征数据库中的预置手形、掌纹特征匹配；手形识别模块、掌纹识别模块根据匹配结果通过数据收发模块向用户终端反馈认证结果。掌纹识别模块提取预置掌纹图像中或认证手形图像中的用户掌纹特征的步骤与上述安全认证方法中的提取掌纹特征的步骤相同，在此就不再一一赘述了。手形识别模块识别认证手形图像中手形的步骤与上述安全认证方法中的手形识别步骤相同，在此就不再一一赘述了。

[0606] 如图 16、图 17 所示，安全认证服务器还包括与用户终端对应的数据解密模块；数据收发模块和掌纹识别模块分别与数据解密模块连接；安全认证服务器收到用户终端加密的图像后，通过数据收发模块发送至数据解密模块，由数据解密模块解密处理后再处理。

[0607] 如图 17 所示，安全认证服务器还包括手掌跟踪模块：手掌跟踪模块与数据收发模块连接；手掌跟踪模块在采集用户带掌纹的认证手形图像时，采用手形区域跟踪算法对手形区域跟踪，确定掌纹手形图像是否连续；如果采集区域的手掌不连续存在则通过数据收发模块提示用户认证失败；如果采集区域的手掌连续存在则通过数据收发模块提示用户继续采集其他掌纹手形图像。

[0608] 如图 17 所示，安全认证服务器还包括识别决策模块：识别决策模块分别与手形识别模块、掌纹识别模块连接；安全认证服务器将认证掌纹图像识别匹配处理后，识别决策模块判断生成的掌纹手形序列是否已经采集、识别、匹配完成；如果未完成掌纹手形序列，则识别决策模块向用户传输用户下一个手形图像，用户重复上述步骤直至生成的掌纹手形序列都完成；如果掌纹手形序列已完成，则识别决策模块查找记录的掌纹信息匹配结果，如果有匹配成功的结果则为用户执行相应的业务操作，则通过数据收发模块向用户终端传输认证成功的消息；如果无匹配成功的掌纹信息匹配结果则通过数据收发模块向用户终端传输认证失败的消息。

[0609] 发明提供的基于手势识别的安全认证方法、终端、服务器和系统不仅可以应用于上述实施例中的认证方式，还可以借助其他设备用用在移动支付，远程开门，银行保险箱的开锁，枪械库的门禁与身份认证。在边检通关，公安司法，金融证券，电子商务，社保福利，信息网络等公共安全领域以及门禁，考勤，学校，医院，场馆，超市等民用领域都可以得到应用。上述应用环境中可以将上述实施例 1-8 中作适当的变型即可实现。具体实施变形参照

上述实施例 1-8 即可，在此不再作详细的赘述了。

[0610] 综上，本发明提供的基于手势识别的安全认证方法、终端、服务器和系统，将动态手势序列和手掌特征识别相结合，既不需要用户保管和携带额外的身份信物，又很大程度上降低了身份信息被劫持的可能性，提高了身份认证的安全性。1) 防止认证信物的丢失。由于本发明使用了人手的特征，因此天然的具备防丢失的特点。2) 大大提高了远程身份认证的安全性。首先，本发明使用了基于手掌特征的跟踪算法，以确保在身份认证的过程中，被劫持的认证终端很难采用快速切换的方式来伪造人手图像；然后，在手掌跟踪的过程中，本发明同时使用了由服务器产生的基于随机旋转角度和预置手形的动态序列，以确保被劫持的认证终端无法借助播放录制的手掌视频或人造手模来假冒用户；最后，在安全认证服务器验证动态手形序列的同时，也检测用户的掌纹特征以进一步识别用户的身份。基于上述三种方法的同步执行，本发明能够有效的提高远程身份认证在认证终端被劫持情况下的安全性。3)

[0611] 借助移动终端上现有的图像采集器或摄像头，无需额外增加专用的采集设置，进一步降低系统的成本，方便用户的使用。

[0612] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[0613] 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0614] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0615] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0616] 尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0617] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围

之内，则本发明也意图包含这些改动和变型在内。

[0618] 以上实施方式仅用于说明本发明，而并非对本发明的限制，有关技术领域的普通技术人员，在不脱离本发明的精神和范围的情况下，还可以作出各种变化和变型，因此所有等同的技术方案也属于本发明的范畴，本发明的专利保护范围应由权利要求限定。

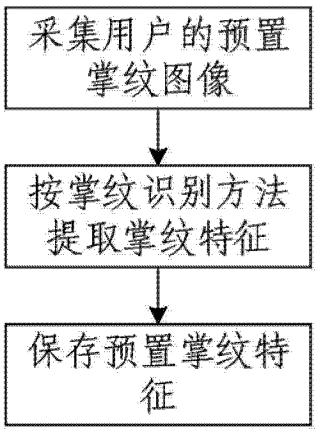

采集用户的预置掌纹图像
按掌纹识别方法提取掌纹特征
保存预置掌纹特征

图 1

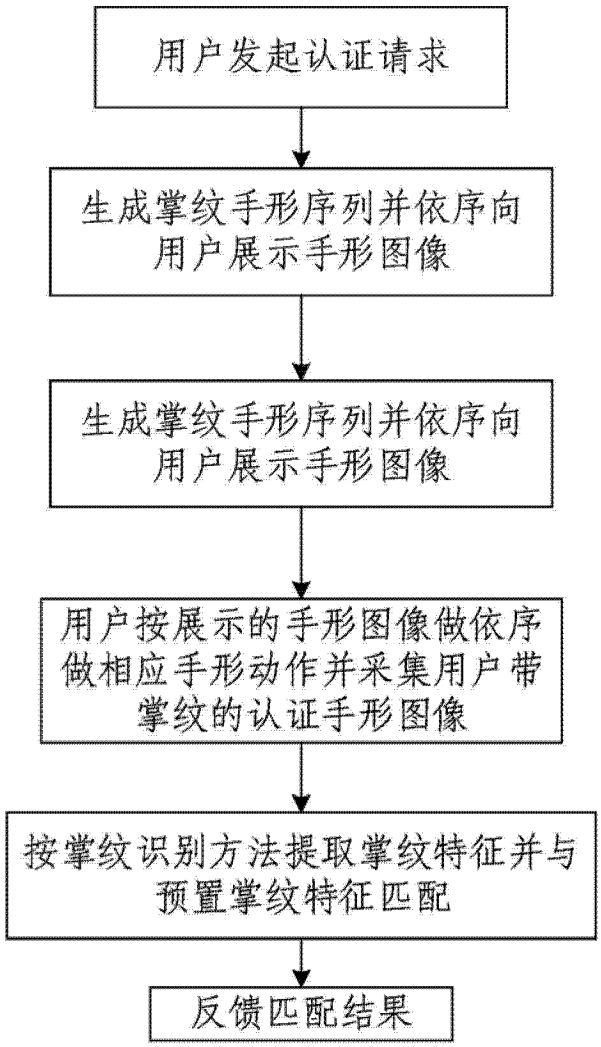

用户发起认证请求
生成掌纹手形序列并依序向用户展示手形图像
生成掌纹手形序列并依序向用户展示手形图像
用户按展示的手形图像做依序做相应手形动作并采集用户带掌纹的认证手形图像
按掌纹识别方法提取掌纹特征并与预置掌纹特征匹配
反馈匹配结果

图 2

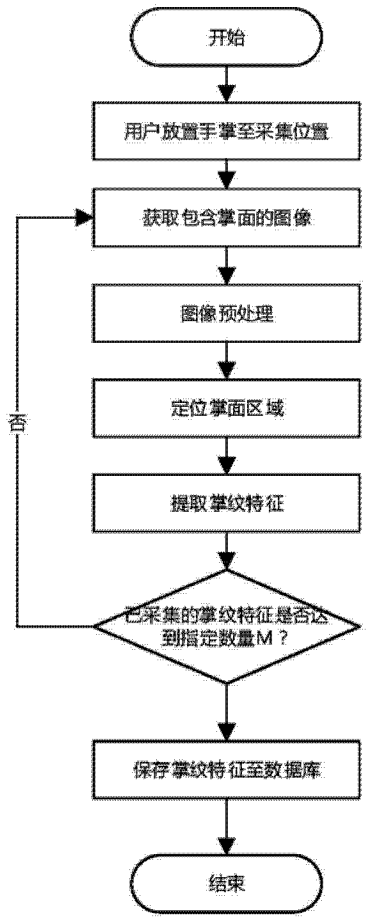

开始
用户放置手掌至采集位置
获取包含掌面的图像
图像预处理
定位掌面区域
提取掌纹特征
已采集的掌纹特征是否达到指定数量M？
否
保存掌纹特征至数据库
结束

图 3

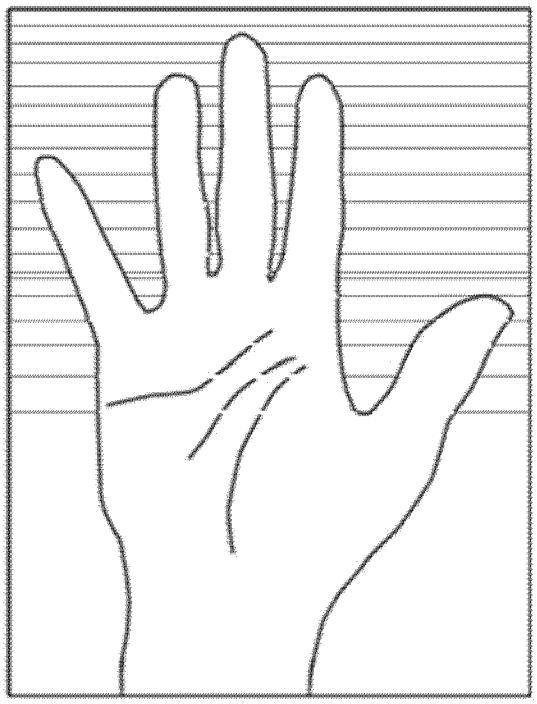


图 4

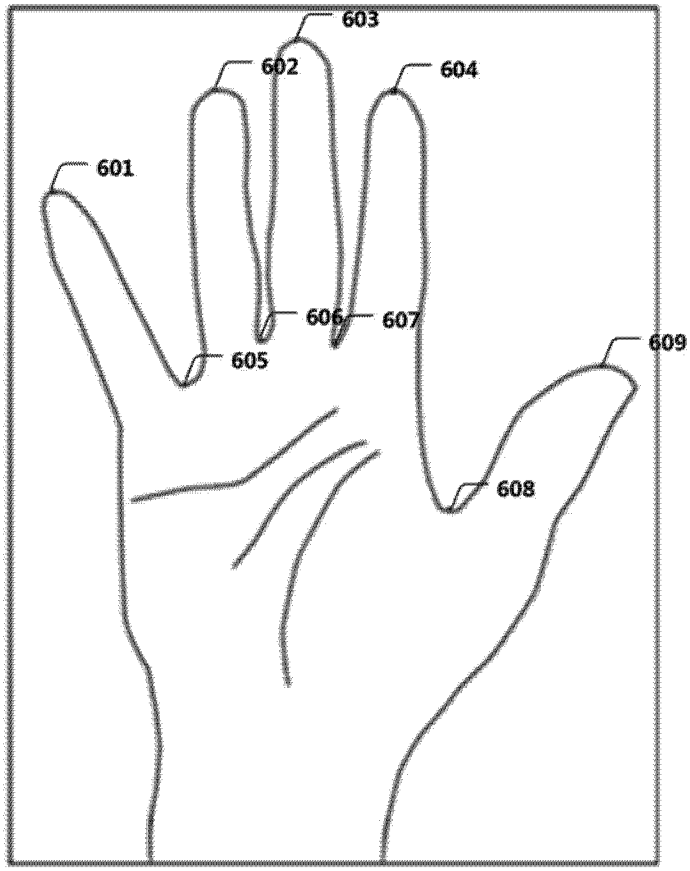



图 5

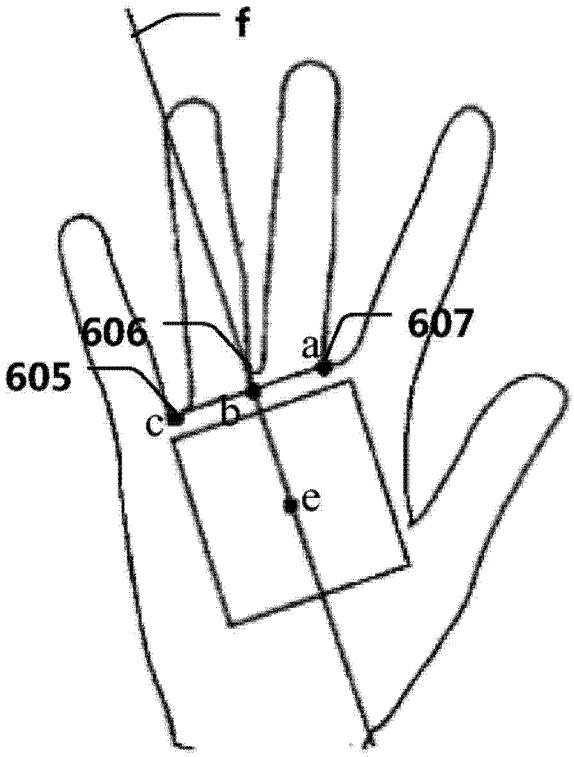



图 6

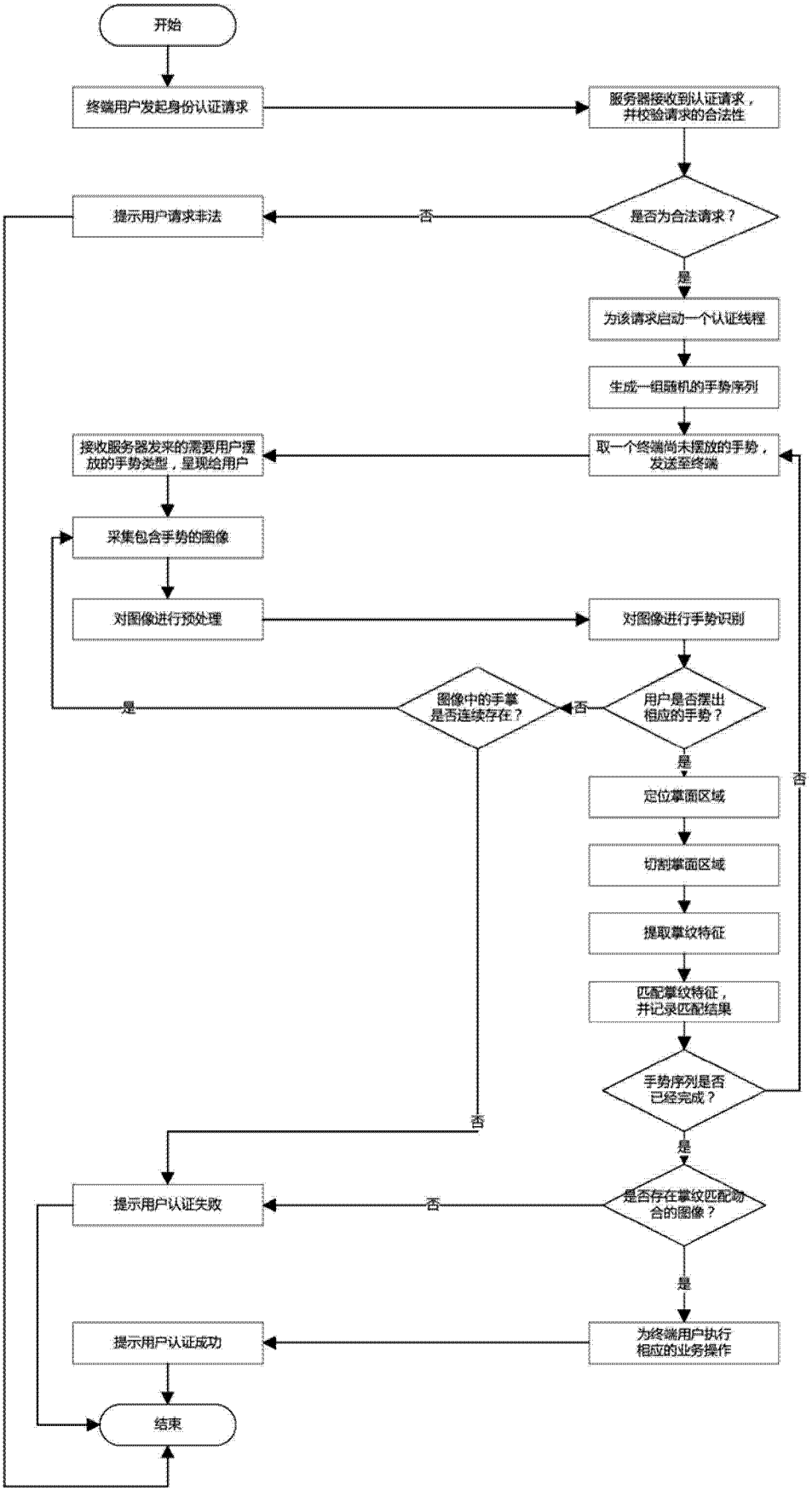

开始
终端用户发起身份认证请求
服务器接收到认证请求，并校验请求的合法性
是否为合法请求？
否
提示用户请求非法
是
为该请求启动一个认证线程
生成一组随机的手势序列
取一个终端尚未摆放的手势，发送至终端
接收服务器发来的需要用户摆放的手势类型，呈现给用户
采集包含手势的图像
对图像进行预处理
对图像进行手势识别
用户是否摆出相应的手势？
否
图像中的手掌是否连续存在？
是
是
否
定位掌面区域
切割掌面区域
提取掌纹特征
匹配掌纹特征，并记录匹配结果
手势序列是否已经完成？
否
是
是否存在掌纹匹配吻合的图像？
否
提示用户认证失败
是
为终端用户执行相应的业务操作
提示用户认证成功
结束

图 7

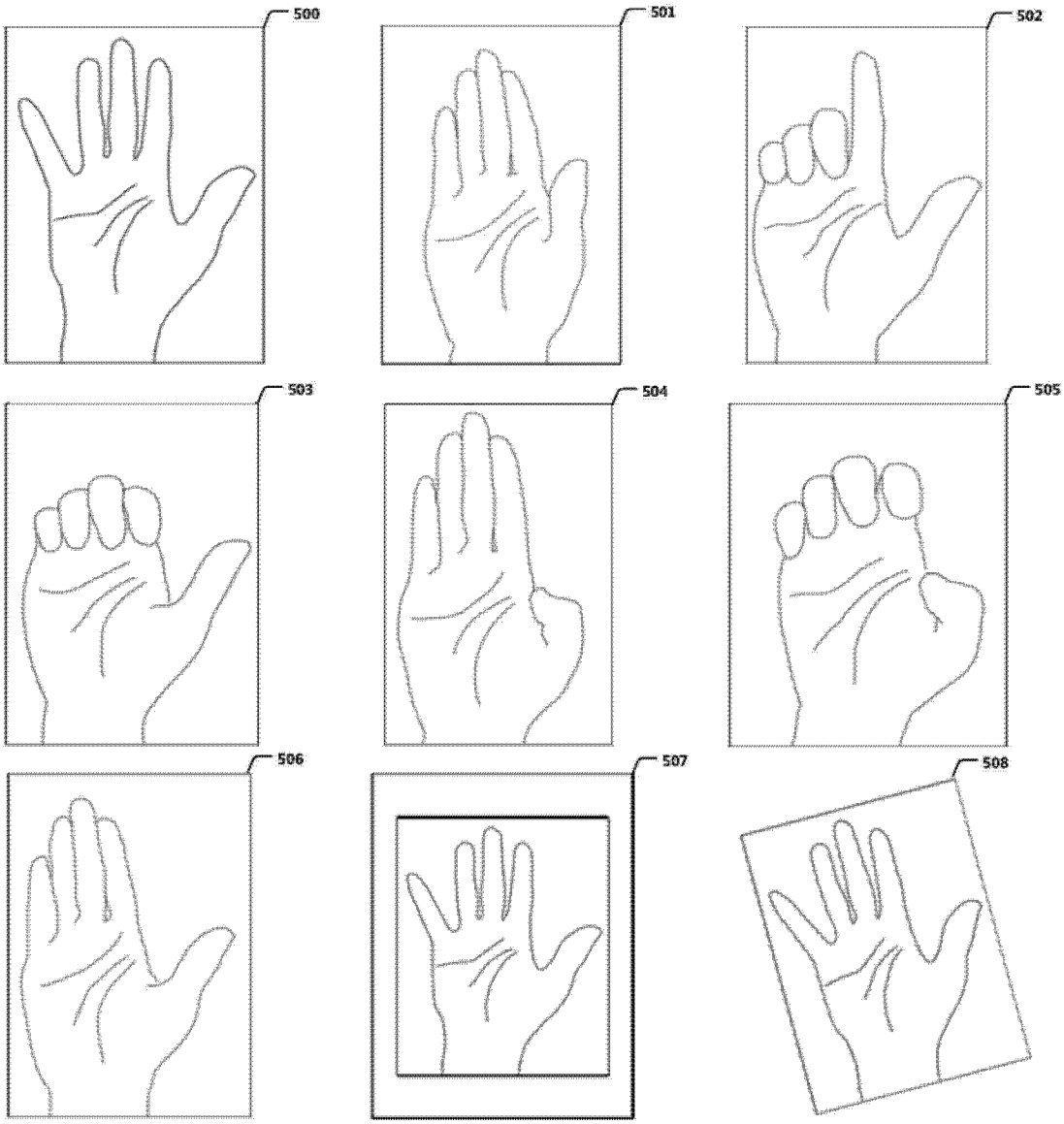



图 8

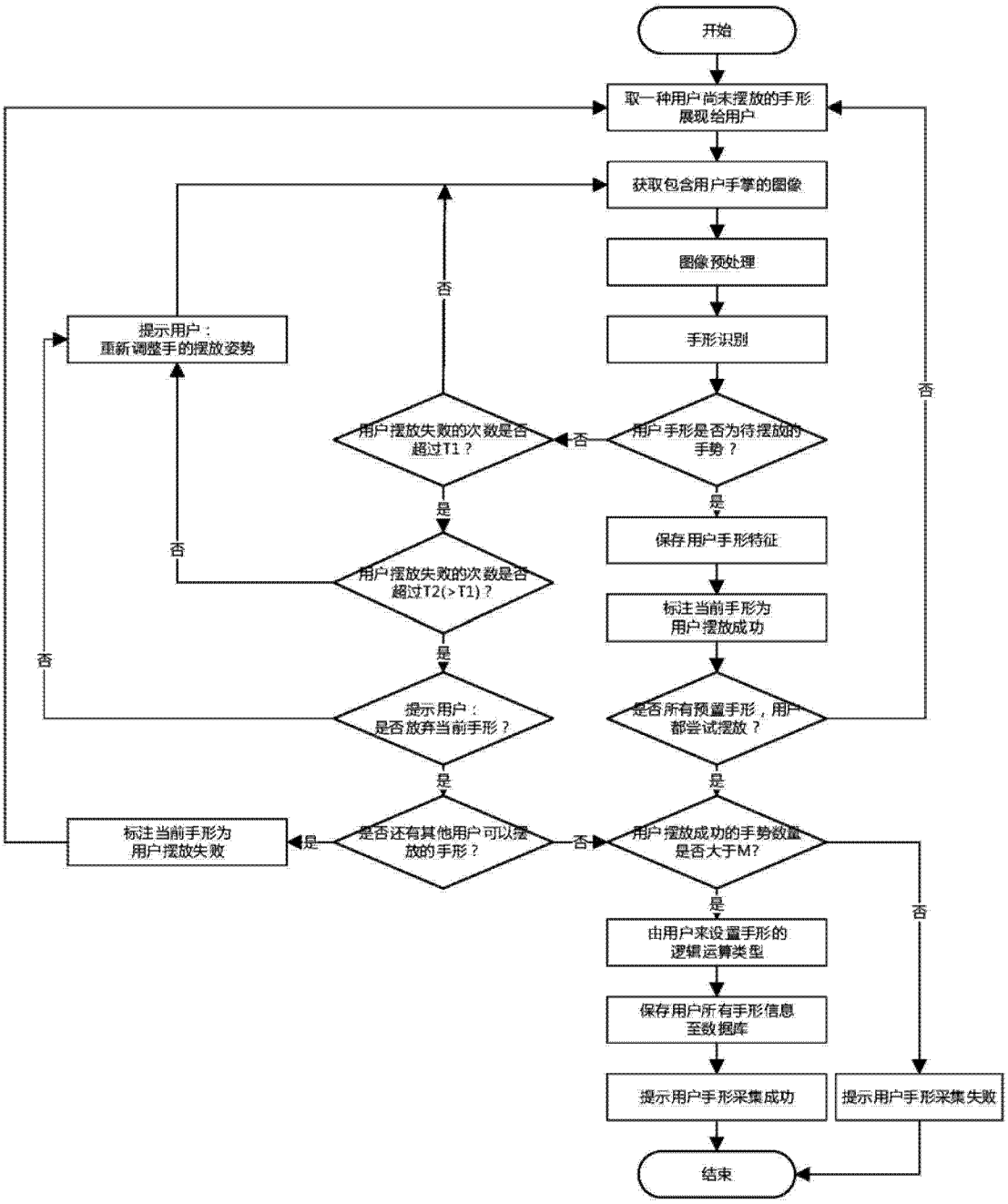

开始
取一种用户尚未摆放的手形展现给用户
获取包含用户手掌的图像
图像预处理
手形识别
用户手形是否为待摆放的手势？
否
是
用户摆放失败的次数是否超过T1？
否
是
保存用户手形特征
标注当前手形为用户摆放成功
是否所有预置手形，用户都尝试摆放？
否
是
用户摆放成功的手势数量是否大于M?
否
是
由用户来设置手形的逻辑运算类型
保存用户所有手形信息至数据库
提示用户手形采集成功
提示用户手形采集失败
结束
是否还有其他用户可以摆放的手形？
是
标注当前手形为用户摆放失败
提示用户：重新调整手的摆放姿势
否
用户摆放失败的次数是否超过T2(>T1)？
否
是
提示用户：是否放弃当前手形？
否
是

图 9

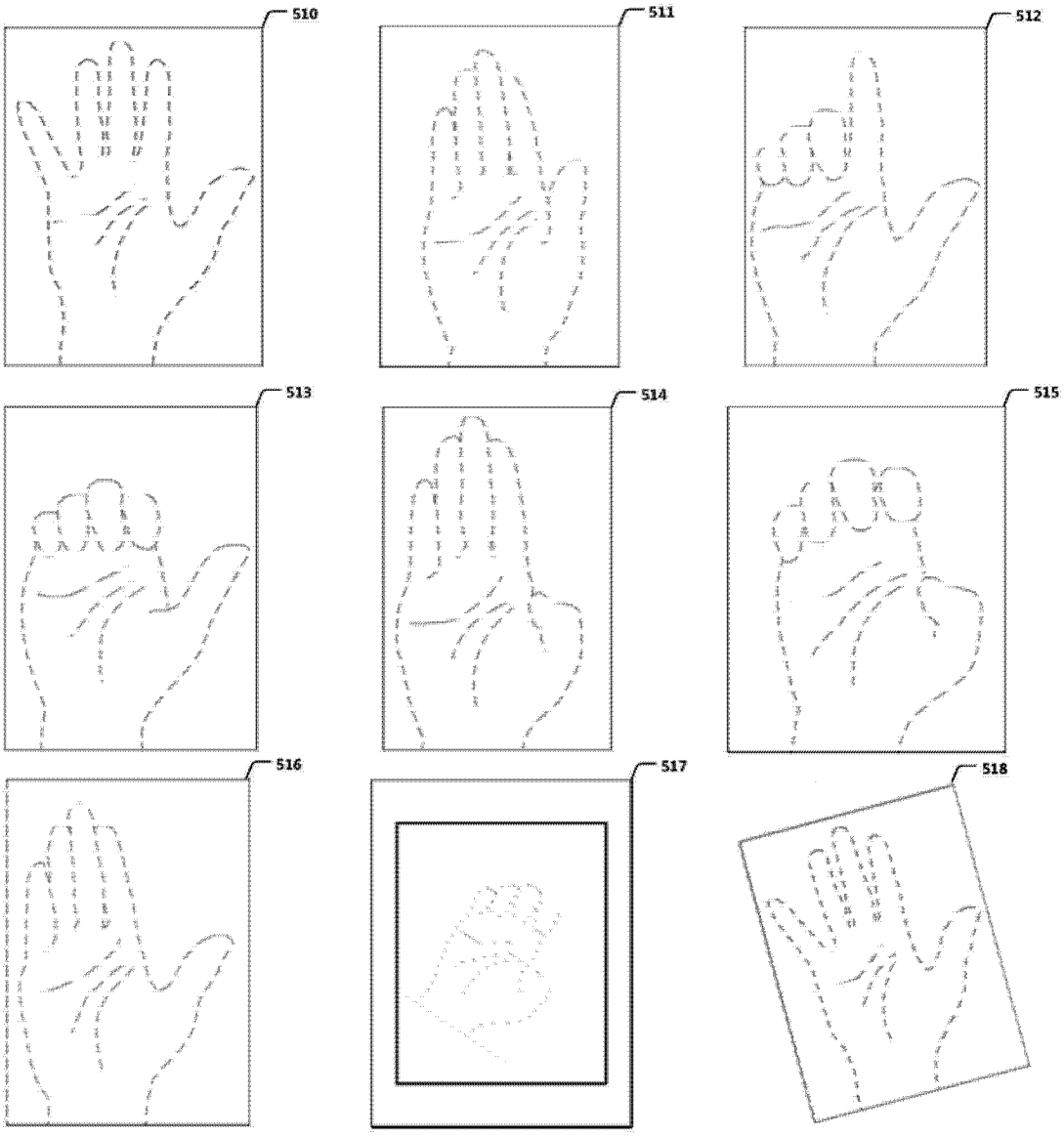



图 10

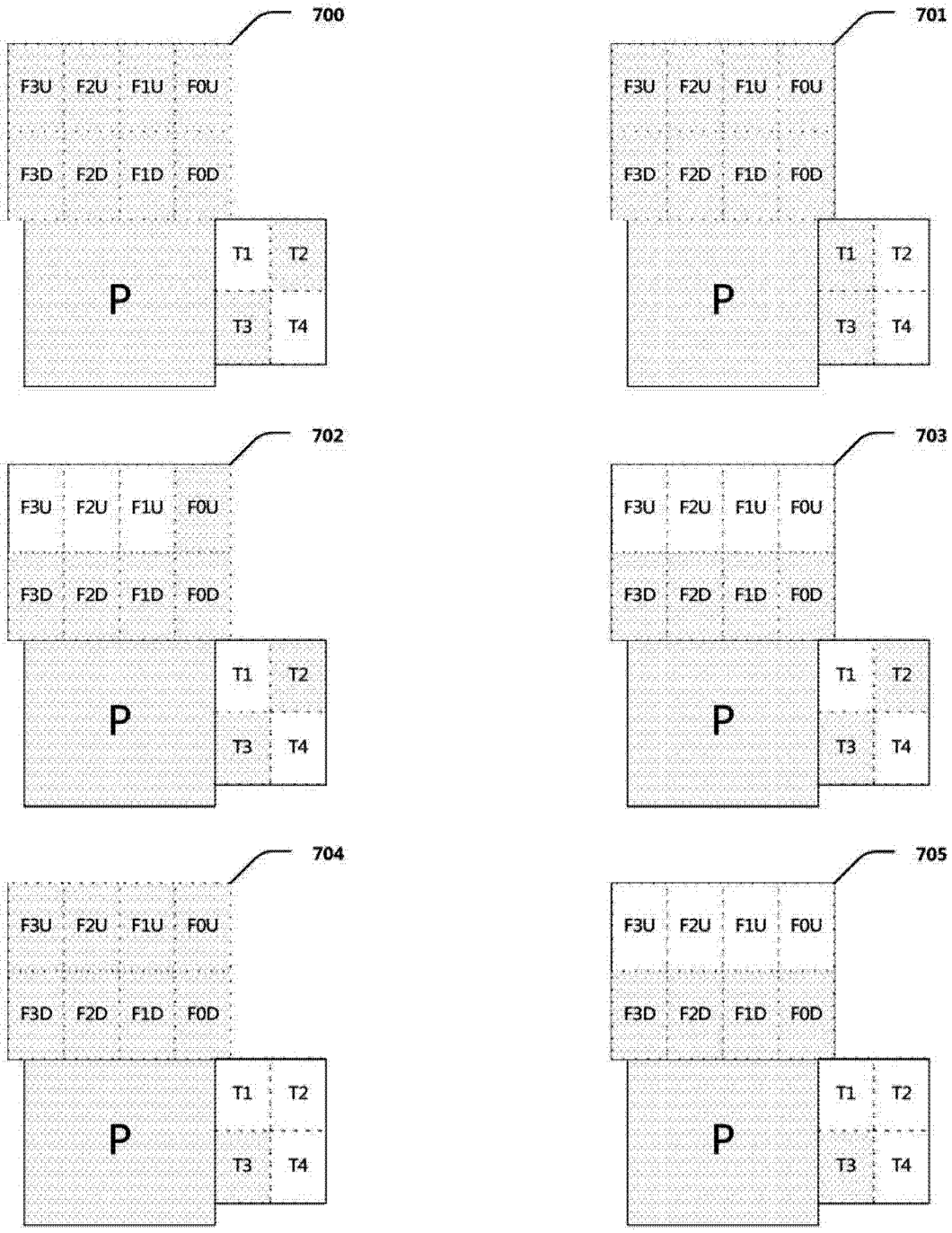

700
F3U F2U F1U F0U
F3D F2D F1D F0D
P
T1 T2
T3 T4
701
F3U F2U F1U F0U
F3D F2D F1D F0D
P
T1 T2
T3 T4
702
F3U F2U F1U F0U
F3D F2D F1D F0D
P
T1 T2
T3 T4
703
F3U F2U F1U F0U
F3D F2D F1D F0D
P
T1 T2
T3 T4
704
F3U F2U F1U F0U
F3D F2D F1D F0D
P
T1 T2
T3 T4
705
F3U F2U F1U F0U
F3D F2D F1D F0D
P
T1 T2
T3 T4

图 11

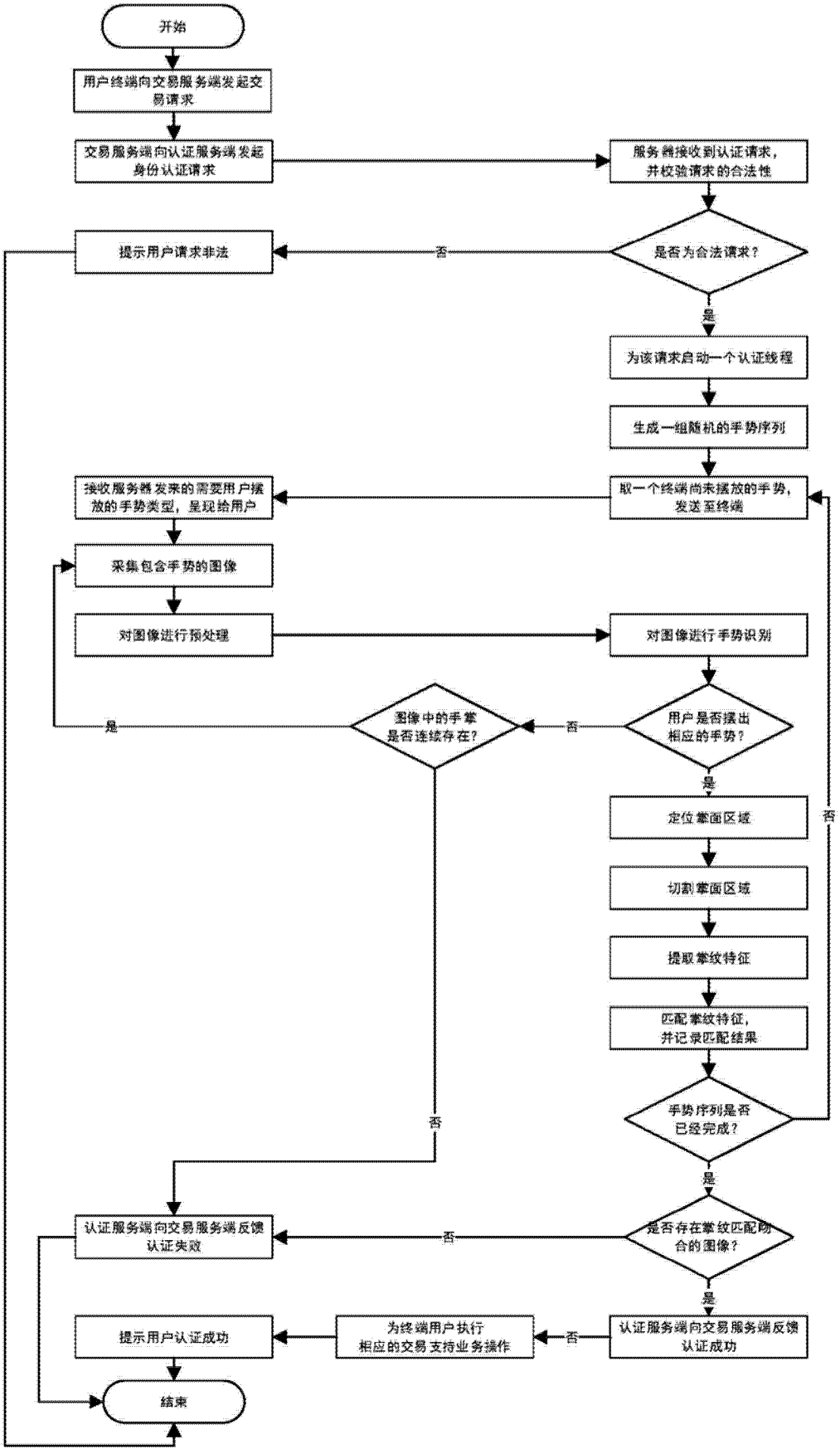

开始
用户终端向交易服务端发起交易请求
交易服务端向认证服务端发起身份认证请求
服务器接收到认证请求，并校验请求的合法性
是否为合法请求？
否
提示用户请求非法
是
为该请求启动一个认证线程
生成一组随机的手势序列
取一个终端尚未播放的手势，发送至终端
接收服务器发来的需要用户播放的手势类型，呈现给用户
采集包含手势的图像
对图像进行预处理
对图像进行手势识别
用户是否摆出相应的手势？
否
图像中的手掌是否连续存在？
是
否
是
定位掌面区域
切割掌面区域
提取掌纹特征
匹配掌纹特征，并记录匹配结果
手势序列是否已经完成？
否
是
是否存在掌纹匹配吻合的图像？
否
认证服务端向交易服务端反馈认证失败
是
认证服务端向交易服务端反馈认证成功
否
为终端用户执行相应的交易支持业务操作
提示用户认证成功
结束

图 12

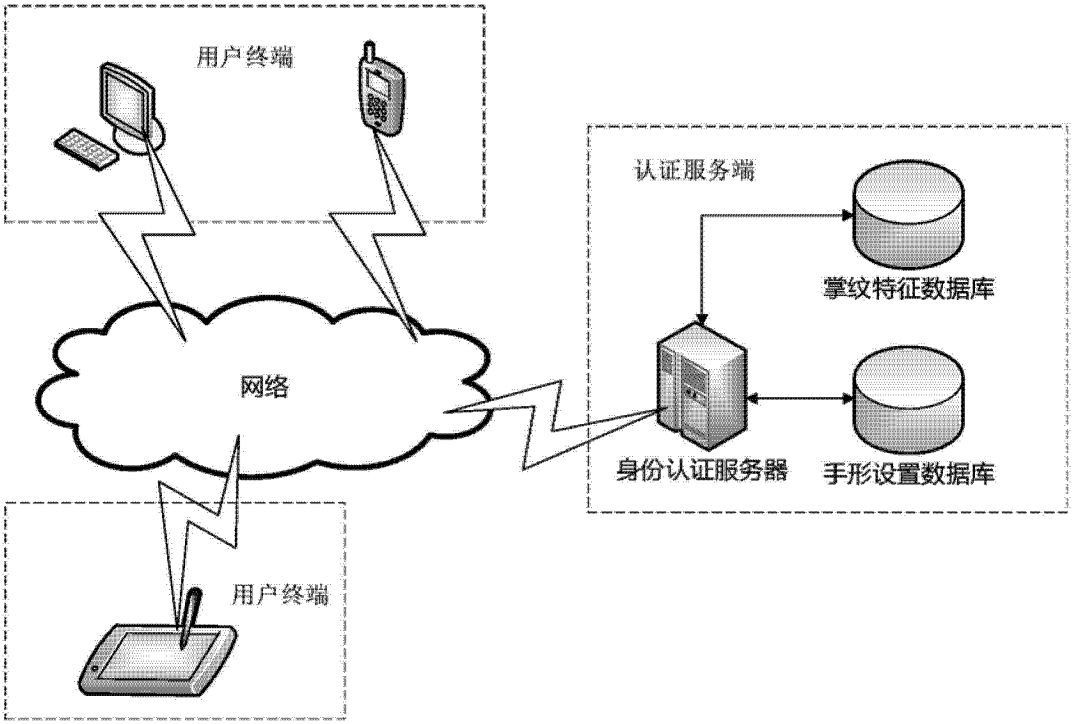

用户终端
认证服务端
掌纹特征数据库
网络
身份认证服务器
手形设置数据库
用户终端

图 13

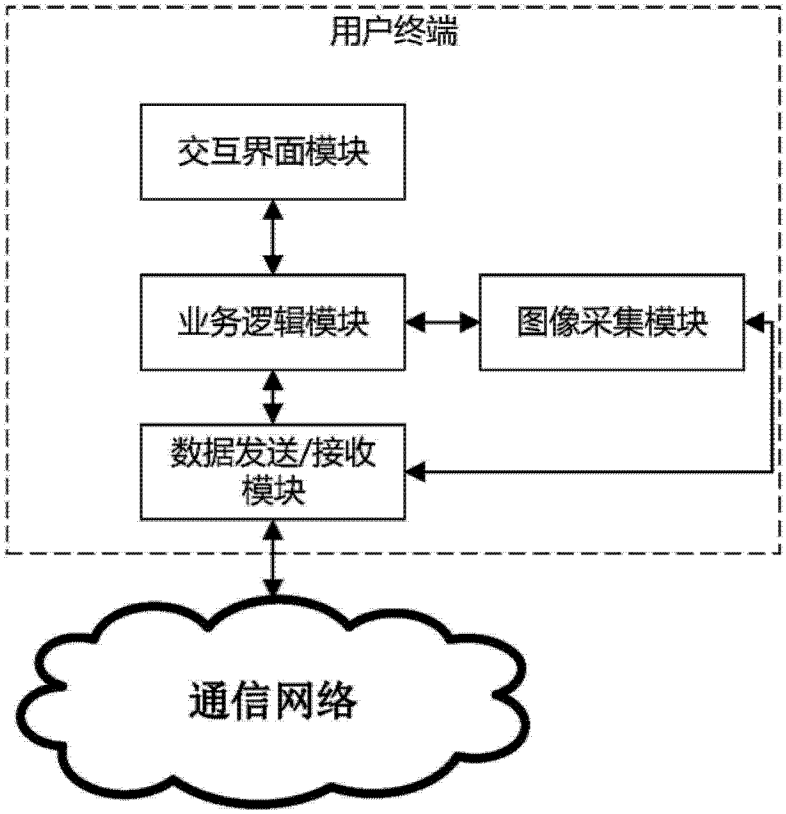

用户终端
交互界面模块
业务逻辑模块
图像采集模块
数据发送/接收
模块
通信网络

图 14

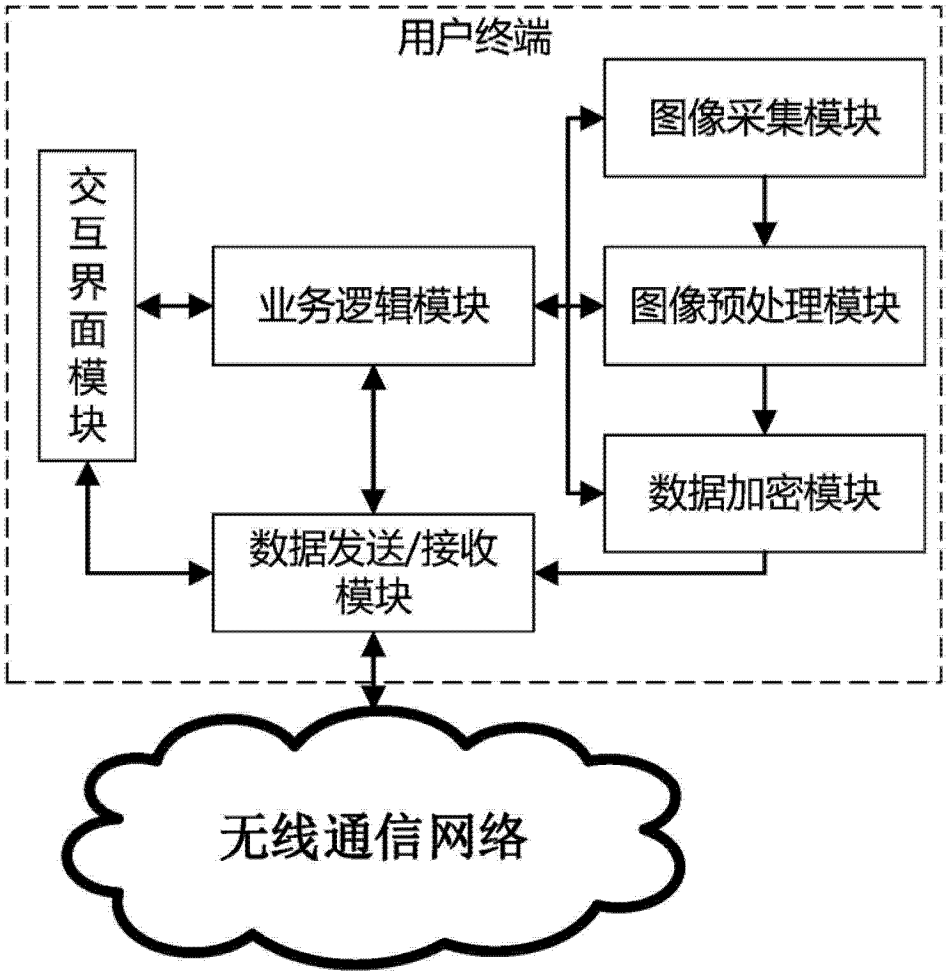

用户终端
图像采集模块
交互界面模块
业务逻辑模块
图像预处理模块
数据加密模块
数据发送/接收模块
无线通信网络

图 15

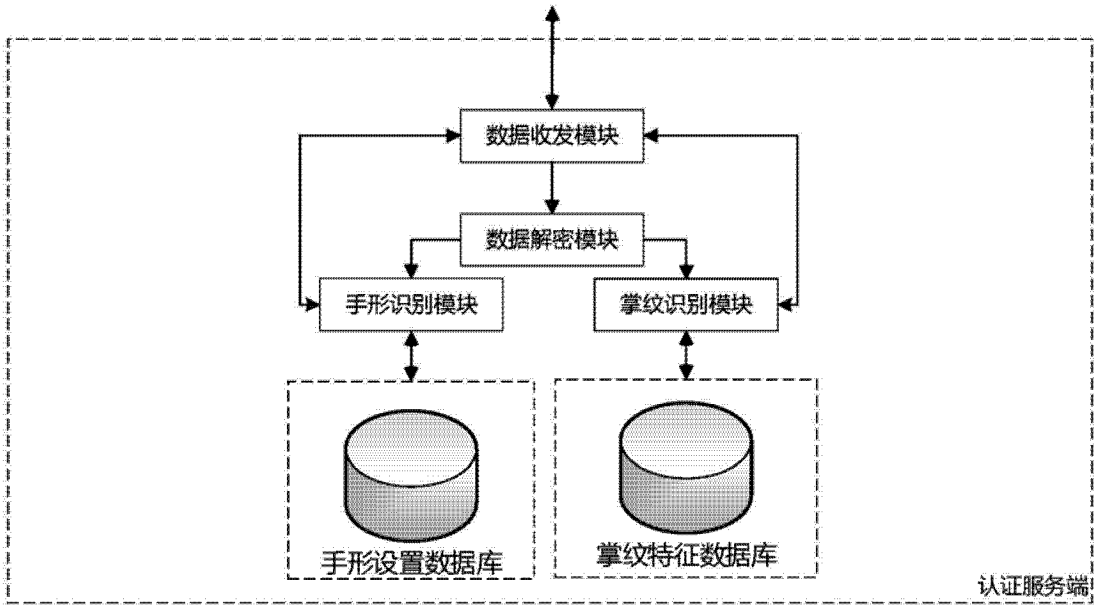

数据收发模块
数据解密模块
手形识别模块
掌纹识别模块
手形设置数据库
掌纹特征数据库
认证服务端

图 16

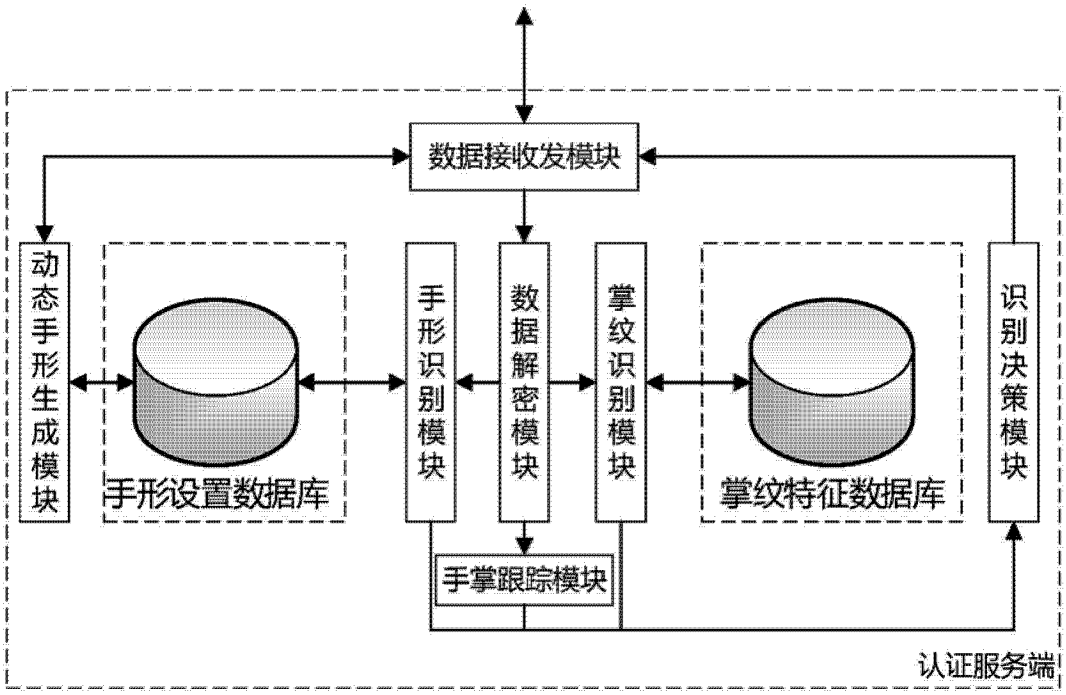

数据接收发模块
动态手形生成模块
手形设置数据库
手形识别模块
数据解密模块
掌纹识别模块
掌纹特征数据库
识别决策模块
手掌跟踪模块
认证服务端

图 17

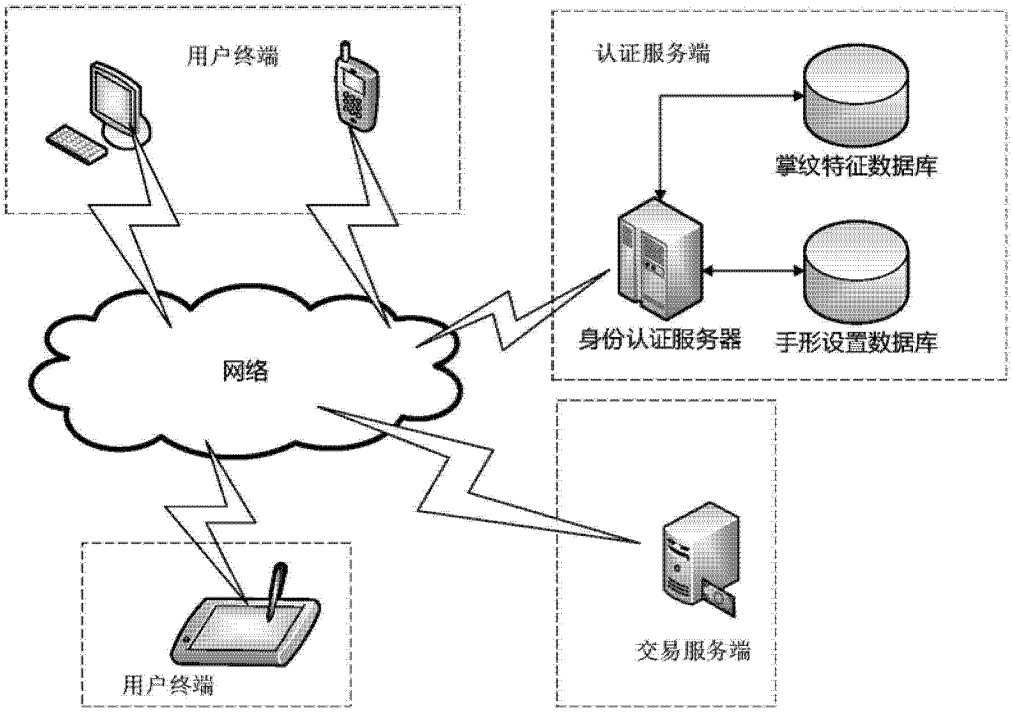

用户终端
认证服务端
掌纹特征数据库
身份认证服务器
手形设置数据库
网络
交易服务端
用户终端

图 18