



(12) 发明专利申请

(10) 申请公布号 CN 102509053 A

(43) 申请公布日 2012. 06. 20

(21) 申请号 201110375129. 7

(22) 申请日 2011. 11. 23

(71) 申请人 唐辉

地址 100062 北京市崇文区安化北里 18 号
院北京上舍 1 号 706

申请人 刘陆陆

沈超

张宇峰

(72) 发明人 唐辉 沈超

其他发明人请求不公开姓名

(51) Int. Cl.

G06F 21/20 (2006. 01)

G06K 9/00 (2006. 01)

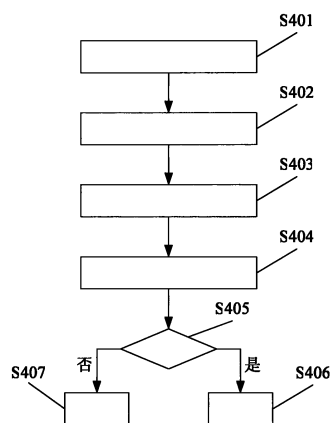
权利要求书 3 页 说明书 12 页 附图 3 页

(54) 发明名称

用于验证授权的方法、处理器、设备和移动终端

(57) 摘要

一种用于验证授权的方法, 包括: 采集图像; 识别所述图像中的人脸信息; 提取所述人脸信息中的表情特征; 将所述表情特征与表情模板进行匹配; 确认匹配后授予权限。本发明以图像识别为基础, 利用某种影像特征, 例如人的表情, 作为验证信息 / 密码, 不仅增加了用户与设备之间的交互方式, 带来新的用户体验, 而且也提高了设备的安全性。本发明还公开一种处理器、设备和移动终端。



1. 一种用于验证授权的方法,其特征在于,包括:
采集图像;
识别所述图像中的人脸信息;
提取所述人脸信息中的表情特征;
将所述表情特征与表情模板进行匹配;
确认匹配后授予权限。
2. 一种用于验证授权的方法,其特征在于,包括:
采集图像;
识别所述图像中的人脸信息;
提取所述人脸信息中的表情特征;
将所述人脸信息中的人脸特征和人脸模板进行匹配,将所述表情特征和表情模板进行匹配;
人脸和表情二者都匹配时授予权限。
3. 如权利要求 2 所述的方法,其特征在于,从所述图像的全局信息中提取相关的全局特征信息,从人脸各局部提取相关的局部特征信息;综合所述全局特征信息和局部特征信息,获得所述人脸的特征信息。
4. 如权利要求 1、2 或 3 所述的方法,其特征在于,提取所述人脸信息中表情特征的步骤包括:
对所述图像中的特征点进行定位并分离特征子区域;
对所述图像的全局特征和所述特征子区域进行特征描述;
综合所述图像的全局特征和特征子区域的特征,获得所述表情特征。
5. 如权利要求 4 所述的方法,其特征在于,所述特征子区域包括眼睛、眉毛、嘴巴和脸颊中的至少一个区域。
6. 如权利要求 4 所述的方法,其特征在于,所述图像的全局特征包括各所述特征子区域的相对位置、俯仰角和注视方向中的至少一种。
7. 如权利要求 2 至 6 任一项所述的方法,其特征在于,采用所述人脸特征与所述人脸模板的欧式距离作为匹配的依据。
8. 如权利要求 1 至 7 任一项所述的方法,其特征在于,采用所述表情特征与所述表情模板的欧式距离作为匹配的依据。
9. 如权利要求 1 至 8 任一项所述的方法,其特征在于,授予操作设备的权限。
10. 如权利要求 9 所述的方法,其特征在于,所述设备从睡眠模式进入唤醒模式后采集图像。
11. 如权利要求 1 至 8 任一项所述的方法,其特征在于,授予打开加密信息的权限。
12. 如权利要求 11 所述的方法,其特征在于,检测到用户对所述加密信息实施打开操作后采集图像。
13. 一种用于验证授权的方法,其特征在于,包括:
采集图像;
识别所述图像中的影像特征;
将所述影像特征与特征模板进行匹配;

确认匹配后授予权限。

14. 如权利要求 13 所述的方法,其特征在于,采用所述影像特征与所述特征模板的欧式距离作为匹配的依据。

15. 如权利要求 13 或 14 所述的方法,其特征在于,所述影像特征是手势特征、动作特征、图案特征和形状特征中的至少一个;

所述特征模板是手势特征模板、动作特征模板、图案特征模板和形状特征模板中的至少一个。

16. 如权利要求 13、14 或 15 所述的方法,其特征在于,授予操作设备的权限。

17. 如权利要求 16 所述的方法,其特征在于,所述设备从第一模式进入第二模式后采集图像。

18. 如权利要求 13、14 或 15 所述的方法,其特征在于,授予打开加密信息的权限。

19. 如权利要求 18 所述的方法,其特征在于,检测到用户对所述加密信息实施打开操作后采集图像。

20. 一种设备,包括图像采集装置和处理器,所述图像采集装置将采集的图像发送给所述处理器,其特征在于,所述处理器包括:

第一单元,用于识别图像中的人脸信息;

第二单元,用于提取所述人脸信息中的表情特征;

第三单元,用于将所述表情特征与表情模板进行匹配;和,

第四单元,用于在所述表情特征与所述表情模板匹配时授予权限。

21. 如权利要求 20 所述的设备,其特征在于,所述第四单元还用于,当所述表情特征与所述表情模板不匹配时拒绝授权。

22. 一种设备,包括图像采集装置和处理器,所述图像采集装置将采集的图像发送给所述处理器,其特征在于,所述处理器包括:

第一单元,用于识别图像中的人脸信息;

第二单元,用于提取所述人脸信息中的表情特征;

第五单元,用于将所述人脸信息中的人脸特征和人脸模板进行匹配;

第三单元,用于将所述表情特征和表情模板进行匹配;和,

第六单元,用于在人脸和表情二者都匹配时授予权限。

23. 如权利要求 22 所述的设备,其特征在于,所述第六单元还用于,当人脸和表情二者中有一个不匹配时拒绝授权。

24. 如权利要求 22 所述的设备,其特征在于,所述第一单元包括:

从所述图像的全局信息中提取相关的全局特征信息的单元;

从人脸各局部提取相关的局部特征信息的单元;和,

综合所述全局特征信息和局部特征信息以获得所述人脸的特征信息的单元。

25. 如权利要求 20 至 24 任一项所述的设备,其特征在于,所述第二单元包括:

对所述图像中的特征点进行定位并分离特征子区域的单元;

对所述图像的全局特征和所述特征子区域进行特征描述的单元;

综合所述图像的全局特征和特征子区域的特征以获得所述表情特征的单元。

26. 如权利要求 22 至 25 任一项所述的设备,其特征在于,采用所述人脸特征与人脸模

板的欧式距离作为匹配的依据。

27. 如权利要求 20 至 26 任一项所述的方法,其特征在于,采用所述表情特征与表情模板的欧式距离作为匹配的依据。

28. 如权利要求 20 至 27 任一项所述的设备,其特征在于,所述处理器还包括对图像进行预处理的单元;经过预处理的图像被发送到所述第一单元。

29. 如权利要求 20 至 27 任一项所述的设备,其特征在于,所述处理器还包括发送提示信息的单元,用于在开始采集图像前或采集图像的过程中发送提示信息,提示用户输入验证信息;和/或,在识别所述图像中的人脸信息前发送提示信息,提示用户确认输入的信息;和/或,拒绝授权时发送提示信息,提示用户验证出错或未获授权或再次输入验证信息。

30. 如权利要求 20 至 29 任一项所述的设备,其特征在于,授予操作设备的权限。

31. 如权利要求 30 所述的设备,其特征在于,所述设备从睡眠模式进入唤醒模式后所述图像采集装置开启,采集图像。

32. 如权利要求 20 至 29 任一项所述的设备,其特征在于,授予打开加密信息的权限。

33. 如权利要求 32 所述的方法,其特征在于,检测到用户对所述加密信息实施打开操作后所述图像采集装置开启,采集图像。

34. 一种设备,包括图像采集装置和处理器,所述图像采集装置将采集的图像发送给所述处理器,其特征在于,所述处理器包括:

影像识别单元,用于识别图像中的影像特征;

匹配单元,用于将所述影像特征与特征模板进行匹配;和,

授权单元,用于确认匹配后授予权限。

35. 如权利要求 34 所述的设备,其特征在于,所述影像特征包括表情特征、人脸特征、手势特征、动作特征、图案特征和形状特征中的至少一个;

所述特征模板包括表情特征模板、人脸特征模板、手势特征模板、动作特征模板、图案特征模板和形状特征模板中的至少一个。

36. 如权利要求 35 所述的设备,其特征在于,所述匹配单元将识别出的多个影像特征分别与相应的特征模板进行匹配,所述授权单元确认全部都匹配后授予权限。

37. 如权利要求 34、35 或 36 所述的方法,其特征在于,采用所述影像特征与所述特征模板的欧式距离作为匹配的依据。

38. 如权利要求 34、35 或 36 所述的设备,其特征在于,授予操作设备的权限。

39. 如权利要求 38 所述的设备,其特征在于,所述设备从第一模式进入第二模式后所述图像采集装置开启,采集图像。

40. 如权利要求 34、35 或 36 所述的设备,其特征在于,授予打开加密信息的权限。

41. 如权利要求 40 所述的设备,其特征在于,检测到用户对所述加密信息实施打开操作后所述图像采集装置开启,采集图像。

42. 一种移动终端,包括屏幕和摄像头,其特征在于,还包括如权利要求 20 至 41 任一项所述的处理器;所述摄像头将其采集的图像发送给所述处理器;所述屏幕用于显示提示信息和所述摄像头采集的图像。

43. 一种如权利要求 20 至 41 任一项所述的处理器。

用于验证授权的方法、处理器、设备和移动终端

技术领域

[0001] 本发明属于数据处理技术领域,尤其涉及一种用于验证授权的方法、处理器、设备和移动终端。

背景技术

[0002] 随着消费电子的不断发展,诸如手机、平板电脑(pad)、笔记本电脑、电子书、个人数字助理(PDA)等越来越多的便携设备都具有显示屏幕和图像采集装置,例如前置摄像头和/或后置摄像头。目前,图像采集装置对便携设备来说只是用于照相,但实际上图像采集装置的功能和用途远不止于此。

发明内容

[0003] 有鉴于此,本发明的一个目的是提供一种用于验证授权的方法。为了对披露的实施例的一些方面有一个基本的理解,下面给出了简单的概括。该概括部分不是泛泛评述,也不是要确定关键/重要组成元素或描绘这些实施例的保护范围。其唯一目的是用简单的形式呈现一些概念,以此作为后面的详细说明确定的序言。

[0004] 在一些可选的实施例中,所述用于验证授权的方法包括:采集图像;识别所述图像中的人脸信息;提取所述人脸信息中的表情特征;将所述表情特征与表情模板进行匹配;确认匹配后授予权限。

[0005] 在一些可选的实施例中,所述用于验证授权的方法包括:采集图像;识别所述图像中的人脸信息;提取所述人脸信息中的表情特征;将所述人脸信息中的人脸特征和人脸模板进行匹配,将所述表情特征和表情模板进行匹配;人脸和表情二者都匹配时授予权限。

[0006] 在一些可选的实施例中,授予操作设备的权限。

[0007] 在一些可选的实施例中,授予打开加密信息的权限。

[0008] 在一些可选的实施例中,所述用于验证授权的方法包括:采集图像;识别所述图像中的影像特征;将所述影像特征与特征模板进行匹配;确认匹配后授予权限。

[0009] 在一些可选的实施例中,所述影像特征是手势特征、动作特征、图案特征和形状特征中的至少一个;所述特征模板是手势特征模板、动作特征模板、图案特征模板和形状特征模板中的至少一个。

[0010] 本发明的另一个目的是提供一种设备。

[0011] 在一些可选的实施例中,所述设备包括图像采集装置和处理器,所述图像采集装置将采集的图像发送给所述处理器,所述处理器包括:第一单元,用于识别图像中的人脸信息;第二单元,用于提取所述人脸信息中的表情特征;第三单元,用于将所述表情特征与表情模板进行匹配;和,第四单元,用于在所述表情特征与所述表情模板匹配时授予权限。

[0012] 在一些可选的实施例中,所述设备包括图像采集装置和处理器,所述图像采集装置将采集的图像发送给所述处理器,所述处理器包括:第一单元,用于识别图像中的人脸信息;第二单元,用于提取所述人脸信息中的表情特征;第五单元,用于将所述人脸信息中的

人脸特征和人脸模板进行匹配；第三单元，用于将所述表情特征和表情模板进行匹配；和，第六单元，用于在人脸和表情二者都匹配时授予权限。

[0013] 在一些可选的实施例中，所述第一单元包括：从所述图像的全局信息中提取相关的全局特征信息的单元；从人脸各局部提取相关的局部特征信息的单元；和，综合所述全局特征信息和局部特征信息以获得所述人脸的特征信息的单元。

[0014] 在一些可选的实施例中，所述第二单元包括：对所述图像中的特征点进行定位并分离特征子区域的单元；对所述图像的全局特征和所述特征子区域进行特征描述的单元；和，综合所述图像的全局特征和特征子区域的特征以获得所述表情特征的单元。

[0015] 在一些可选的实施例中，所述处理器还包括对图像进行预处理的单元；经过预处理的图像被发送到所述第一单元。

[0016] 在一些可选的实施例中，所述处理器还包括发送提示信息的单元，用于在开始采集图像前或采集图像的过程中发送提示信息，提示用户输入验证信息；和/或，在识别所述图像中的人脸信息前发送提示信息，提示用户确认输入的信息；和/或，拒绝授权时发送提示信息，提示用户验证出错或未获授权或再次输入验证信息。

[0017] 在一些可选的实施例中，所述设备包括图像采集装置和处理器，所述图像采集装置将采集的图像发送给所述处理器，所述处理器包括：影像识别单元，用于识别图像中的影像特征；匹配单元，用于将所述影像特征与特征模板进行匹配；和，授权单元，用于确认匹配后授予权限。

[0018] 可选地，所述影像特征包括表情特征、人脸特征、手势特征、动作特征、图案特征和形状特征中的至少一个；所述特征模板包括表情特征模板、人脸特征模板、手势特征模板、动作特征模板、图案特征模板和形状特征模板中的至少一个。

[0019] 在一些可选的实施例中，所述匹配单元将识别出的多个影像特征分别与相应的特征模板进行匹配，所述授权单元确认全部都匹配后授予权限。

[0020] 本发明的另一个目的是提供一种移动终端。

[0021] 在一些可选的实施例中，所述移动终端包括屏幕和摄像头，还包括前述任意一种处理器；所述摄像头将其采集的图像发送给所述处理器；所述屏幕用于显示提示信息和所述摄像头采集的图像。

[0022] 本发明的另一个目的是提供一种机器可读介质，具有可执行指令，用于实现前述任意一种用于验证授权的方法。

[0023] 所有的可选实施例都与现有的设置密码方式都不相同。本发明以图像识别为基础，利用某种影像特征，例如人的表情，作为验证信息/密码，不仅增加了用户与设备之间的交互方式，带来新的用户体验，而且也提高了设备的安全性。

[0024] 为了上述以及相关的目的，一个或多个实施例包括后面将详细说明并在权利要求中特别指出的特征。下面的说明以及附图详细说明某些示例性方面，并且其指示的仅仅是各个实施例的原则可以利用的各种方式中的一些方式。其它的益处和新颖性特征将随着下面的详细说明结合附图考虑而变得明显，所公开的实施例是要包括所有这些方面以及它们的等同。

[0025] 说明书附图

[0026] 图 1 是一种可选的验证授权流程；

- [0027] 图 2 是另一种可选的验证授权流程；
- [0028] 图 3 是另一种可选的验证授权流程；
- [0029] 图 4 是利用表情进行授权验证的一种可选流程；
- [0030] 图 5 是利用表情和人脸的组合进行授权验证的一种可选流程；
- [0031] 图 6 是表情特征提取的一种可选流程；
- [0032] 图 7 是人脸识别及人脸特征提取的一种可选流程；
- [0033] 图 8 是一种可选的设备的示意图；
- [0034] 图 9 是另一种可选的设备的示意图；
- [0035] 图 10 是另一种可选的设备的示意图。

具体实施方式

[0036] 以下描述和附图充分地示出本发明的具体实施方案，以使本领域的技术人员能够实践它们。其他实施方案可以包括结构的、逻辑的、电气的、过程的以及其他的改变。实施例仅代表可能的变化。除非明确要求，否则单独的组件和功能是可选的，并且操作的顺序可以变化。一些实施方案的部分和特征可以被包括在或替换其他实施方案的部分和特征。本发明的实施方案的范围包括权利要求书的整个范围，以及权利要求书的所有可获得的等同物。在本文中，本发明的这些实施方案可以被单独地或总地用术语“发明”来表示，这仅仅是为了方便，并且如果事实上公开了超过一个的发明，不是要自动地限制该应用的范围为任何单个发明或发明构思。

[0037] 今后的验证授权操作，可以利用一种或多种图形 / 图像信息作为验证信息或密码。例如可以采用特定的表情作为一种验证信息或密码，也可以同时采用人脸和表情作为验证信息进行多级验证。其它的，本领域技术人员也可以知道，特定的手势、特定的动作、特定的形状以及特定的图案等，都可以作为验证信息或密码。手势和动作的组合、形状和图案的组合、表情和手势的组合、表情和动作的组合等等，也都可以作为验证信息。

[0038] 当采用某种特定的图形 / 图像作为验证信息时，需要提前录入该特定的图形 / 图像信息，并保存为模板。当用户需要获得某种授权时需要输入图形 / 图像，然后设备需要对用户输入的图形 / 图像进行识别，并将识别的结果与保存的模板进行匹配。如果匹配成功，则给予用户授权，否则拒绝授权。

[0039] 一种可选的验证授权流程如图 1 所示。采集图像 (S101)；识别图像中的影像特征 (S102)；将影像特征与预先设置的特征模板进行匹配 (S103)；确认匹配后授予权限 (S104)。其中，预先设置的特征模板可以但不限于是表情模板、人脸模板、手势模板、动作模板、形状模板和图案模板中的一个或多个；影像特征可以但不限于是表情特征、人脸特征、手势特征、动作特征、形状特征和图案特征中的一种或多种。

[0040] 当采用一种影像特征（例如采用表情、人脸、手势、动作、形状和图案中的一种）作为验证信息或密码时，一种可选的方式是，采用该影像特征与该影像特征模板的欧式距离作为匹配的依据。

[0041] 当采用多种影像特征（例如采用表情和人脸、手势和动作、形状和图案、表情和手势、表情和动作）作为验证信息或密码时，一种可选的方式是，将识别出的多种影像特征分别与相应的特征模板进行匹配，全部都匹配才能通过验证授予权限。将多种影像特征分别

与相应的特征模板进行匹配时,一种可选的方式是,采用各影像特征与其对应的特征模板的欧式距离作为匹配的依据。

[0042] 图 2 示出了另一种可选的验证授权流程。采集图像 (S201);提示用户确认输入的信息 (S202);判断用户是否确认输入的信息 (S203);用户确认后,识别图像中的影像特征 (S204);将影像特征与预先设置的特征模板进行匹配 (S205);确认匹配后授予权限 (S206)。

[0043] 图 3 示出了另一种可选的验证授权流程。采集图像 (S301);发送提示信息,提示用户输入验证信息或正在采集图像 (S302);识别图像中的影像特征 (S303);将影像特征与预先设置的特征模板进行匹配 (S304);确认匹配后授予权限 (S305)。本领域技术人员可以看出,在图 3 所示的可选流程中,发送提示信息 (S302) 发生在采集图像 (S301) 的过程中,具体实现时也可以在采集图像前发送提示信息,提示用户输入用于验证的表情、动作、手势、形状或图案。

[0044] 本领域技术人员能够知道的另一种可选的验证授权流程,包括:采集图像;发送提示信息,提示用户输入验证信息或正在采集图像;提示并等待用户确认输入的信息;用户确认后识别图像中的影像特征;将影像特征与预先设置的特征模板进行匹配;确认匹配后授予权限。

[0045] 如果影像特征与预先设置的特征模板不匹配,则未通过验证,拒绝授予权限。拒绝授予权限后,可以不做任何操作;也可以发提示信息,提示用户未通过验证或提示用户再次输入验证信息,再次进行验证。

[0046] 本领域技术人员可以知道,利用影像信息作为验证信息或密码可以被广泛应用到多种领域。随着消费电子的不断发展,诸如手机、平板电脑 (pad)、笔记本电脑、电子书、个人数字助理 (PDA) 等越来越多的便携设备都具有显示屏幕和图像采集装置,例如前置摄像头和 / 或后置摄像头。可以利用设备上的图像采集装置,完成对操作该设备的用户的验证授权。

[0047] 图 4 示出一种利用表情进行授权验证的流程。采集图像 (S401);识别图像中的人脸信息 (S402);提取人脸信息中的表情特征 (S403);将获得的表情特征与保存的表情模板进行匹配 (S404);根据匹配结果决定是否授权 (S405)。如果匹配,则授予权限 (S406);否则,拒绝授予权限 (S407)。

[0048] 采集图像时,一种可选的方式是在设备的屏幕上显示取景框,取景框尺寸可以由用户设置,例如可以是 352×288 像素的取景框,这样用户可以将面部图像置于取景框的中央,完成图像采集。另一种可选的方式是,不设置取景框而直接用摄像头采集用户的头像,这种图像采集方式对于用户来说更随意,不再受到取景框的约束,但可能会增加后面人脸检测的难度。

[0049] 人脸识别的目地在于检测出所采集图像中包含的人脸。在此,首先必须快速确认所采集的图像来自活体对象;其次需要对图像中的人脸进行基本的快速检测,判断所采集图像是否包含感兴趣区域及完整的感兴趣区域;然后是对包含完整的感兴趣区域的人脸图像进行具体的检测,涉及的基本步骤为图像预处理、人脸轮廓定位、人脸的精确定位、人脸各特征区域的分割等。关于人脸检测的方法,现有的参考模板法、人脸规则法、样品学习法、肤色模型法以及特征子脸法等,都可供选择使用。

[0050] 关于提取人脸表情特征的方法, 现有的主元分析法 (PCA)、改进的二维主元分析法 (2DPCA) 和线性鉴别分析法 (LDA) 等, 都可供选择使用。

[0051] 有效的表情特征提取将提高匹配验证的准确性, 好的表情特征提取结果可以从以下几个方面考虑:

[0052] (1) 完整的表示出人脸表情的本质特征;

[0053] (2) 去除噪声、光照及其他与表情无关的干扰信息;

[0054] (3) 数据表示形式紧凑, 避免过高的维数;

[0055] (4) 不同类别表情的特征之间有较好的区分性。

[0056] 为获得较好的识别率, 一种可选的方式是采集多帧人脸图像, 对多帧图像进行配准以获得更高质量的图像, 从而降低图像质量恶劣, 如光照严重不足、运动模糊严重等场景, 带来的不良影响。另一种可选的方式是对采集的图像首先进行快速预处理, 如亮度均衡、去除噪声和归一化等处理步骤, 并根据预处理的需求调整图像采集设备的相关参数, 以减少预处理的计算复杂度、提高图像质量。

[0057] 亮度均衡处理的作用是对外界光照的过滤, 使采集图像的对比度和亮度不依赖于外界光照。亮度均衡处理可以采用直方图均衡技术。

[0058] 图像去除噪声处理采用中值滤波可以有效消除大量采集图像的噪声, 同时去除不必要的高频分量。

[0059] 归一化处理能够进一步提高图像特征提取的鲁棒性。虽然取景框尺寸固定, 但对于不同环境下采集图像由于距离等因素, 实际有效可用于特征提取的图像大小必然存在差异, 归一化处理可以消除差异对特征提取造成的影响。

[0060] 提取表情特征后, 可以将提取获得的表情特征与保存的表情模板进行匹配。一种可选的方式是, 采用欧式距离作为特征匹配的判决依据。

[0061] 当特征距离的度量值 $d(F, F^*)$ 小于或等于某一阈值 d^* , 即 $d(F, F^*) \leq d^*$, 则认为提取出的表情特征与表情模板匹配。预设的距离阈值 d^* 可以通过训练等方式预先确定, 也可通过有效的人脸图像进行更新。

[0062] 其中, $d(F, F^*) = \sqrt{(F - F^*)^T M (F - F^*)}$; $\sqrt{(F - F^*)^T M (F - F^*)}$ 表示加权欧式距离, 半正定矩阵 M 为加权矩阵; F 表示对采集图像进行处理提取的特征描述; F^* 表示保存的表情模板的特征描述。

[0063] $d(F, F^*)$ 刻画了输入特征与模板特征的匹配度, $d(F, F^*)$ 越小表示所采集图像与模板越接近。这里矩阵 M 的选择可通过训练等方式预先确定, 也可通过有效的人脸图像进行更新。

[0064] 下面提出一个通过人的表情完成手机解锁的实施例。

[0065] 过程可以分为两个阶段, 第一阶段是表情特征训练, 生成表情模板; 第二阶段则是用表情对手机解锁。

[0066] 在第一阶段, 设置手机解锁的密码脸证信息时, 手机处于正常工作状态, 手机的处理器打开摄像头, 将采集的图像显示在手机屏幕上供预览, 用户根据屏幕预览调整手机位置, 使面部处在图像特征提取区域, 并做出一个表情。处理器将采集到的面部表情图像进行特征提取, 将表情特征提取的结果储存在存储器作为面部表情特征识别的模板。

[0067] 在第二阶段, 手机处在待机模式并进入锁机状态, 屏幕和摄像头处于关闭状态。用

户通过按键或其它方式唤醒手机,手机从待机模式进入唤醒模式时依然处于锁机状态,处理器在锁机状态下开启摄像头,并将采集的图像显示在屏幕上供用户预览。用户可以根据屏幕上的预览调整手机位置,使面部处在图像识别区域。图像采集完成后,还可以将采集的图像显示在屏幕上,并发出提示信息,提示用户确认。用户确认后,处理器根据图像识别区域的图像进行人脸检测和表情特征提取。其中,表情特征提取的一种可选方式如图6所示。

[0068] 步骤 S601,对图像中的特征点进行定位并分离各特征子区域;其中,特征子区域包括眼睛、眉毛、嘴巴、脸颊等区域。

[0069] 步骤 S602,对图像的全局特征进行描述;如各特征子区域的相对位置、俯仰角、注视方向等。

[0070] 步骤 S603,对特征子区域进行特征描述。

[0071] 步骤 S604,综合图像的全局特征和特征子区域的特征,形成完整的表情特征描述。

[0072] 将获得的表情特征和存储器中存储的表情特征进行匹配。如果匹配,则处理器进行解锁操作,授予用户操作手机的权限。如果不匹配,则继续保持锁机状态,拒绝授予用户对手机操作的权限。在不匹配时,处理器还可以通过屏幕显示提示信息,提示用户验证失败;还可以通知用户再次验证。

[0073] 其中,表情特征可以但不限于是高兴、愤怒、恐惧、悲伤、惊奇或厌恶。

[0074] 下面提出一个利用表情进行解密的实施例。

[0075] 过程仍然可以分为两个阶段,第一阶段是表情特征训练,生成表情模板;第二阶段则是用表情进行解密。

[0076] 在第一阶段,对信息加密时设置用于打开文件的验证信息/密码,手机处于正常工作状态,处理器打开摄像头,将采集的图像显示在手机屏幕上供预览,用户根据屏幕预览调整手机位置,使面部处在图像特征提取区域,并做出一个表情。处理器将采集到的面部表情图像进行特征提取,将表情特征提取的结果储存在存储器作为面部表情特征识别的模板。

[0077] 在第二阶段,用户对加密信息进行打开操作时,处理器开启摄像头,并将采集的图像显示在屏供用户预览。在采集图像之前或采集图像的过程中,还可以在屏幕上显示提示信息,提示用户正在采集图像。用户可以根据屏幕上的预览调整手机位置,使面部处在图像识别区域。处理器根据图像识别区域采集到的图像进行人脸检测和表情特征提取,并和存储器中存储的表情特征进行匹配。如果匹配,则处理器授予用户打卡加密信息的权限,为用户打开加密信息。如果不匹配,则拒绝授予用户打开加密信息的权限。在不匹配时,处理器还可以通过屏幕显示提示信息,提示用户验证失败;还可以通知用户再次验证。

[0078] 本领域技术人员能够看出,本发明与现有的设置密码方式都不相同。以图像识别为基础,利用某种影像特征,例如人的表情,作为验证信息/密码,不仅增加了用户与设备之间的交互方式,带来新的用户体验,而且也提高了设备的安全性。上述实施例虽然是以表情为例进行的说明,但本领域技术人员完全可以知道,无论现在还是今后,能利用图像分析/目标识别等技术识别出来的影像特征都适用于本发明。例如,可以用某种手势作为验证信息/密码,也可以用某个动作、某个图案或某种形状作为验证信息/密码。

[0079] 例如,用手势作为验证信息/密码,在利用手势识别技术进行验证授权时,现有的模板匹配法 (Model/Template Matching)、神经网络法 (NN, Neural Network)、动态时间规

整法 (DTW, Dynamic Time Warping) 及隐马尔可夫模型法 (HMM, Hidden Markov Model) 都可供选择。

[0080] 除了使用上述单一的影像特征外,也可以用多个影像特征的组合作为验证信息/密码。例如,可以用表情和人脸的特征组合,也可以用表情和手势的组合,也可以用手势和动作的组合,也可以用图案和形状的组合,还可以用表情、人脸和手势的组合,等等。鉴于组合的灵活性和多样性,这里只做一些示范性的列举,而不做穷举说明。

[0081] 利用多个影像特征的组合作为验证信息/密码比用单一的影像特征更加安全,适用于对安全性要求较高的情况。

[0082] 图 5 示出一种利用表情和人脸的组合进行授权验证的流程。采集图像 (S501); 识别图像中的人脸信息 (S502); 提取人脸信息中的表情特征 (S503); 将获得的人脸信息和表情特征与保存的人脸模板和表情模板分别进行匹配 (S504); 根据匹配结果决定是否授权 (S505)。如果人脸和表情全部都匹配,则授予权限 (S506); 人脸和表情中有一个不匹配,则拒绝授予权限 (S507)。

[0083] 关于人脸识别的方法,现有的参考模板法、人脸规则法、样品学习法、肤色模型法以及特征子脸法等,都可供选择使用。

[0084] 一种可选的人脸匹配方式是采用欧式距离作为特征匹配的判决依据。

[0085] 当特征距离的度量值 $d(E, E^*)$ 小于或等于某一阈值 d , 即 $d(E, E^*) \leq d$, 则认为人脸特征与人脸模板匹配。预设的距离阈值 d 可以通过训练等方式预先确定,也可通过有效的人脸图像进行更新。

[0086] 其中, $d(E, E^*) = \sqrt{(E - E^*)^T N (E - E^*)}$; $\sqrt{(E - E^*)^T N (E - E^*)}$ 表示加权欧式距离, 半正定矩阵 N 为加权矩阵; E 表示对采集图像进行处理提取的特征描述; E^* 表示保存的人脸模板的特征描述。

[0087] $d(E, E^*)$ 刻画了输入特征与模板特征的匹配度, $d(E, E^*)$ 越小表示所采集图像与模板越接近。这里矩阵 N 的选择可通过训练等方式预先确定,也可通过有效的人脸图像进行更新。

[0088] 本领域技术人员能够看出,采用欧式距离进行特征匹配还适用于除表情、人脸之外的其它影像特征,包括但不限于手势的匹配、动作的匹配、图案的匹配、形状的匹配,等等。

[0089] 下面提出一个通过人脸和表情的组合完成手机解锁的实施例。

[0090] 过程可以分为两个阶段,第一阶段是生成模板;第二阶段是对手机解锁。

[0091] 在第一阶段,设置手机解锁的密码脸证信息时,手机处于正常工作状态,手机的处理器打开摄像头,将采集的图像显示在手机屏幕上供预览,用户根据屏幕预览调整手机位置,使面部处在图像特征提取区域,并做出一个表情。处理器将采集到的面部表情图像进行特征提取,将面部特征和表情特征提取的结果储存在存储器作为面部和表情特征识别的模板。

[0092] 在第二阶段,手机处在待机模式并进入锁机状态,屏幕和摄像头处于关闭状态。用户通过按键或其它方式唤醒手机,手机从待机模式进入唤醒模式时依然处于锁机状态,处理器在锁机状态下开启摄像头,并将采集的图像显示在屏幕上供用户预览。用户可以根据屏幕上的预览调整手机位置,使面部处在图像识别区域。图像采集完成后,还可以将采集的

图像显示在屏幕上,并发出提示信息,提示用户确认。用户确认后,处理器根据图像识别区域的图像进行人脸识别和表情特征提取,并和存储器中存储的面部特征和表情特征进行匹配。如果匹配,则处理器进行解锁操作,授予用户操作手机的权限。如果不匹配,则继续保持锁机状态,拒绝授予用户对手机操作的权限。在不匹配时,处理器还可以通过屏幕显示提示信息,提示用户验证失败;还可以通知用户再次验证。

[0093] 下面提出一个利用人脸和表情的组合进行解密的实施例。

[0094] 过程仍然可以分为两个阶段,第一阶段是生成模板;第二阶段是进行解密。

[0095] 在第一阶段,对信息加密时设置用于打开文件的验证信息/密码,手机处于正常工作状态,处理器打开摄像头,将采集的图像显示在手机屏幕上供预览,用户根据屏幕预览调整手机位置,使面部处在图像特征提取区域,并做出一个表情。处理器将采集到的面部表情图像进行特征提取,将面部特征和表情特征提取的结果储存在存储器作为面部和表情特征识别的模板。

[0096] 在第二阶段,用户对加密信息进行打开操作时,处理器开启摄像头,并将采集的图像显示在屏幕上供用户预览。在采集图像之前或采集图像的过程中,还可以在屏幕上显示提示信息,提示用户正在采集图像。用户可以根据屏幕上的预览调整手机位置,使面部处在图像识别区域。处理器根据图像识别区域采集到的图像进行人脸识别和表情特征提取,并和存储器中存储的面部特征和表情特征进行匹配。如果匹配,则处理器授予用户打卡加密信息的权限,为用户打开加密信息。如果不匹配,则拒绝授予用户打开加密信息的权限。在不匹配时,处理器还可以通过屏幕显示提示信息,提示用户验证失败;还可以通知用户再次验证。

[0097] 其中,人脸识别及人脸特征提取的一种可选方式如图7所示。

[0098] 步骤S701,对采集的图像进行预处理。包括对图像的有效区域的剪裁、光照一致化、调整图像的亮度和/或色度和/或饱和度等步骤。

[0099] 步骤S702,判断采集的图像是否符合条件。当符合条件时,执行步骤S703;不符合条件时,重新采集图像并回到步骤S701。

[0100] 步骤S703,从图像的全局信息中提取相关的全局特征信息;从人脸各局部提取相关的局部特征信息。人脸的局部包括眼睛、嘴巴和脸颊等区域。

[0101] S704,综合本次图像采集所获取的全局特征信息和局部特征信息,得到人脸特征信息。

[0102] 判断采集的图像是否符合条件时,可以但不限于从以下几个方面进行判断:

[0103] 图像是否存在过度曝光、过度的运动模糊等不利于检测的因素;

[0104] 图像是否来自真实的活体对象;

[0105] 图像中是否存在人脸,人脸的各局部区域,如眼睛、嘴巴、脸颊等,是否完整。

[0106] 当图像曝光适度,足够清晰,存在人脸且人脸的各局部区域完整,则可判定采集的图像符合条件。

[0107] 本领域技术人员能够知道,在本发明中可以静态图像作为验证信息/密码,也可以连续变化的动作、手势、表情等动态图像作为验证信息/密码;既可以二维图像作为验证信息/密码,也可以3维图像作为验证信息/密码;对本发明的保护不应该在这些方面受到限制。

[0108] 利用影像信息作为验证信息 / 密码, 相比于现有的文本密码, 无疑信息量更为复杂, 更难被破解, 从而大大提高了系统设备的安全性。在众多的影像信息中, 表情、手势、动作、图像、形状等这些信息相比人脸而言具有更多的随机性。例如, 人们在设置手机的解锁密码或为重要的信息设置打开密码时, 可以随机地选择某种表情、某种动作、某个手势、某个图像和 / 或某种形状作为密码。如果只打算用人脸信息作为密码, 则比较难做到随机选取。当利用这些具有很强的不确定性的影像信息, 如表情、动作、手势、图像和 / 或形状, 作为验证信息 / 密码时, 会大大提高恶意破解密码的难度, 大幅度提高系统 / 设备 / 信息的安全性。

[0109] 图 8 示出一种可选的设备的示意图, 该设备包括图像采集装置 82 和处理器 81, 图像采集装置 82 将采集的图像发送给处理器 81。处理器 81 中的第一单元 811 对接收图像中的人脸信息进行识别。第一单元 811 识别出人脸信息后, 第二单元 812 提取人脸信息中的表情特征, 第三单元 813 将表情特征与预存的表情模板进行匹配。第四单元 814 根据第三单元 813 的匹配结果决定是否授予权限。如果表情特征与表情模板匹配, 即表情匹配, 则第四单元 814 授予权限; 当表情特征与表情模板不匹配时, 即表情不匹配时, 第四单元 814 拒绝授权。

[0110] 图 9 示出另一种可选的设备的示意图, 包括图像采集装置 82 和处理器 91, 所述图像采集装置 82 将采集的图像发送给处理器 91。处理器 91 中的第一单元 811 对接收图像中的人脸信息进行识别。第一单元 811 识别出人脸信息后, 第二单元 812 提取人脸信息中的表情特征。第五单元 915 将人脸信息中的人脸特征和预存的人脸模板进行匹配, 第三单元 813 将表情特征与预存的表情模板进行匹配。第六单元 916 根据第三单元 813 的匹配结果和第五单元 915 的匹配结果决定是否授予权限。人脸和表情二者都匹配时, 即人脸特征和人脸模板匹配且表情特征和表情模板匹配时, 第六单元 916 授予权限。当人脸特征与人脸模板不匹配和 / 或表情特征与表情模板不匹配时, 即人脸和表情有一个不匹配时, 第六单元 916 拒绝授权。

[0111] 第一单元 811 的实现方式多种多样, 一种可选的方式是, 第一单元 811 包括以下三个单元: 从图像的全局信息中提取相关的全局特征信息的单元; 从人脸各局部提取相关的局部特征信息的单元; 和, 综合全局特征信息和局部特征信息以获得人脸的特征信息的单元。

[0112] 第二单元 812 的实现方式多种多样, 一种可选的方式是, 第二单元 812 包括以下三个单元: 对图像中的特征点进行定位并分离特征子区域的单元; 对图像的全局特征和特征子区域进行特征描述的单元; 综合图像的全局特征和特征子区域的特征以获得表情特征的单元。

[0113] 第三单元 813 将表情特征与表情模板进行匹配的方式有很多, 一种可选的方式是采用表情特征与表情模板的欧式距离作为匹配的依据。通过计算 $d(F, F^*) = \sqrt{(F - F^*)^T M (F - F^*)}$ 可以获得表情特征与表情模板的匹配程度。其中, $d(F, F^*)$ 表示特征距离的度量值, $\sqrt{(F - F^*)^T M (F - F^*)}$ 表示加权欧式距离, 半正定矩阵 M 为加权矩阵; F 表示对采集图像进行处理提取的特征描述; F^* 表示保存的表情模板的特征描述。 $d(F, F^*)$ 越小表示表情特征和表情模板越接近, 匹配度越高。当 $d(F, F^*)$ 小于或等于某一阈

值 d^* , 即 $d(F, F^*) \leq d^*$, 则可以认为表情特征与表情模板匹配。

[0114] 第五单元 915 将人脸特征和人脸模板进行匹配的方式有很多, 一种可选的方式是采用人脸特征与人脸模板的欧式距离作为匹配的依据。通过计算 $d(E, E^*) = \sqrt{(E - E^*)^T N (E - E^*)}$ 可以获得人脸特征与人脸模板的匹配程度。其中, $d(E, E^*)$ 表示特征距离的度量值, $\sqrt{(E - E^*)^T N (E - E^*)}$ 表示加权欧式距离, 半正定矩阵 N 为加权矩阵; E 表示对采集图像进行处理提取的特征描述; E^* 表示保存的人脸模板的特征描述。 $d(E, E^*)$ 刻画了输入特征与模板特征的匹配度, $d(E, E^*)$ 越小表示所采集图像与模板越接近。当 $d(E, E^*)$ 小于或等于某一阈值 d , 即 $d(E, E^*) \leq d$, 则认为人脸特征与人脸模板匹配。

[0115] 为获得较好的识别率, 一种可选的方式是采集多帧人脸图像, 对多帧图像进行配准以获得更高质量的图像, 从而降低图像质量恶劣, 如光照严重不足、运动模糊严重等场景, 带来的不良影响。另一种可选的方式是对采集的图像首先进行快速预处理, 如亮度均衡、去除噪声和归一化等处理步骤, 并根据预处理的需求调整图像采集设备的相关参数, 以减少预处理的计算复杂度、提高图像质量。在这种情况下, 处理器中可以增加一个对图像进行预处理的单元, 经过预处理的图像被发送到第一单元 811, 以提高识别率。

[0116] 为了使用户更加方便, 将设备当前的一些操作通知用户, 可以在处理器中增加发送提示信息的单元。在图像采集装置 82 开始采集图像前或采集图像的过程中, 该单元可以发送提示信息, 提示用户输入验证信息。也可以, 在第一单元 811 识别图像中的人脸信息前发送提示信息, 提示用户确认输入的信息。还可以, 在第四单元 814 或第六单元 916 拒绝授权时发送提示信息, 提示用户验证出错或未获授权或再次输入验证信息。

[0117] 图 10 示出另一种可选的设备的示意图, 包括图像采集装置 82 和处理器 101, 图像采集装置 82 将采集的图像发送给处理器 101。处理器 101 中的影像识别单元 1011 对接收图像中的影像特征进行识别, 匹配单元 1012 将影像识别单元 1011 提取的影像特征与预存的特征模板进行匹配, 授权单元 1013 根据匹配单元 1012 的匹配结果决定是否授予权限。

[0118] 其中, 影像特征包括但不限于是表情特征、人脸特征、手势特征、动作特征、图案特征和形状特征中的一种或多种。同样地, 特征模板包括但不限于是表情特征模板、人脸特征模板、手势特征模板、动作特征模板、图案特征模板和形状特征模板中的一种或多种。

[0119] 影像识别单元 1011 提取的如果是一种影像特征, 例如表情特征、人脸特征、手势特征、动作特征、形状特征或图案特征, 一种可选的方式是, 匹配单元 1012 采用该影像特征与该影像特征模板的欧式距离作为匹配的依据。

[0120] 影像识别单元 1011 提取的如果是多种影像特征, 例如采用表情和人脸、手势和动作、形状和图案、表情和手势、表情和动作等, 一种可选的方式是, 匹配单元 1012 将多种影像特征分别与相应的特征模板进行匹配。全部都匹配, 才能通过验证授予权限。将多种影像特征分别与相应的特征模板进行匹配时, 一种可选的方式是, 采用各影像特征与其对应的特征模板的欧式距离作为匹配的依据。

[0121] 本发明还公开一种移动终端, 包括屏幕、摄像头和处理器。摄像头将其采集的图像发送给处理器; 屏幕用于显示提示信息和摄像头采集到的图像。其中, 处理器可以是前述多种处理器中的任意一种。

[0122] 除非另外具体陈述, 术语比如处理、计算、运算、确定、显示等等可以指一个或更多

个处理或者计算系统、或类似设备的动作和 / 或过程,所述动作和 / 或过程将表示为处理系统的寄存器或存储器内的物理(如电子)量的数据操作和转换为类似地表示为处理系统的存储器、寄存器或者其他此类信息存储、发射或者显示设备内的物理量的其他数据。信息和信号可以使用多种不同的技术和方法中的任何一种来表示。例如,在贯穿上面的描述中提及的数据、指令、命令、信息、信号、比特、符号和码片可以用电压、电流、电磁波、磁场或粒子、光场或粒子或者其任意组合来表示。

[0123] 应该明白,公开的过程中的步骤的特定顺序或层次是示例性方法的实例。基于设计偏好,应该理解,过程中的步骤的特定顺序或层次可以在不脱离本公开的保护范围的情况下得到重新安排。所附的方法权利要求以示例性的顺序给出了各种步骤的要素,并且不是要限于所述的特定顺序或层次。

[0124] 在上述的详细描述中,各种特征一起组合在单个的实施方案中,以简化本公开。不应该将这种公开方法解释为反映了这样的意图,即,所要求保护的主题的实施方案需要比清楚地每个权利要求中所陈述的特征更多的特征。相反,如所附的权利要求书所反映的那样,本发明处于比所公开的单个实施方案的全部特征少的状态。因此,所附的权利要求书特此清楚地被并入详细描述中,其中每项权利要求独自作为本发明单独的优选实施方案。

[0125] 本领域技术人员还应当理解,结合本文的实施例描述的各种说明性的逻辑框、模块、电路和算法步骤均可以实现成电子硬件、计算机软件或其组合。为了清楚地说明硬件和软件之间的可交换性,上面对各种说明性的部件、框、模块、电路和步骤均围绕其功能进行了一般地描述。至于这种功能是实现成硬件还是实现成软件,取决于特定的应用和对整个系统所施加的设计约束条件。熟练的技术人员可以针对每个特定应用,以变通的方式实现所描述的功能,但是,这种实现决策不应解释为背离本公开的保护范围。

[0126] 用于执行本申请所述功能的通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑器件、分立门或者晶体管逻辑、分立硬件组件或者其任意组合,可以实现或执行结合本文的实施例所描述的各种说明性的逻辑框图、模块和电路。通用处理器可以是微处理器,或者,该处理器也可以是任何常规的处理器、控制器、微控制器或者状态机。处理器也可能实现为计算设备的组合,例如,DSP和微处理器的组合、多个微处理器、一个或多个微处理器与DSP内核的结合,或者任何其它此种结构。

[0127] 结合本文的实施例所描述的方法或者算法的步骤可直接体现为硬件、由处理器执行的软件模块或其组合。软件模块可以位于RAM存储器、闪存、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、移动磁盘、CD-ROM或者本领域熟知的任何其它形式的存储介质中。一种示例性的存储介质连接至处理器,从而使处理器能够从该存储介质读取信息,且可向该存储介质写入信息。当然,存储介质也可以是处理器的组成部分。处理器和存储介质可以位于ASIC中。该ASIC可以位于用户终端中。当然,处理器和存储介质也可以作为分立组件存在于用户终端中。

[0128] 为使本领域内的任何技术人员能够实现或者使用本发明,上面对所公开实施例进行了描述。对于本领域技术人员来说,这些实施例的各种修改方式都是显而易见的,并且本文定义的一般原理也可以在不脱离本公开的精神和保护范围的基础上适用于其它实施例。因此,本公开并不限于本文给出的实施例,而是与本申请公开的原理和新颖性特征的最广

范围相一致。

[0129] 对于软件实现,本申请中描述的技术可用执行本申请所述功能的模块(例如,过程、函数等)来实现。这些软件代码可以存储在存储器单元并由处理器执行。存储器单元可以实现在处理器内,也可以实现在处理器外,在后一种情况下,它经由各种手段以通信方式耦合到处理器,这些都是本领域中所公知的。

[0130] 本文描述的各种存储介质表示为用于存储信息的一个或多个设备和/或其它机器可读介质。术语“机器可读介质”包括但不限于能够存储、包含和/或携带指令和/或数据的无线信道和各种其它介质。

[0131] 上文的描述包括一个或多个实施例的举例。当然,为了描述上述实施例而描述部件或方法的所有可能的结合是不可能的,但是本领域普通技术人员应该认识到,各个实施例可以做进一步的组合和排列。因此,本文中描述的实施例旨在涵盖落入所附权利要求书的保护范围内的所有这样的改变、修改和变型。此外,就说明书或权利要求书中使用的术语“包含”,该词的涵盖方式类似于术语“包括”,就如同“包括,”在权利要求中用作衔接词所解释的那样。此外,使用在权利要求书的说明书中的任何一个术语“或者”是要表示“非排它性的或者”。

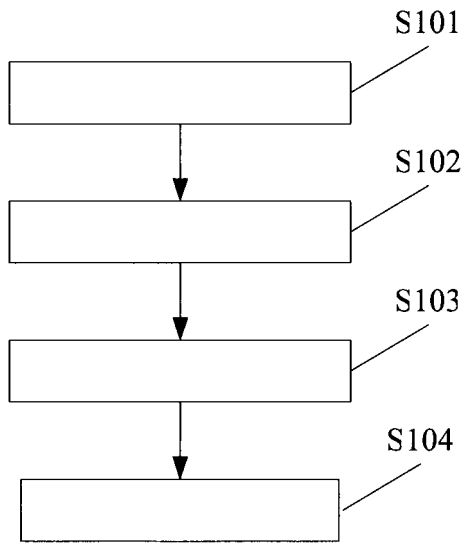


图 1

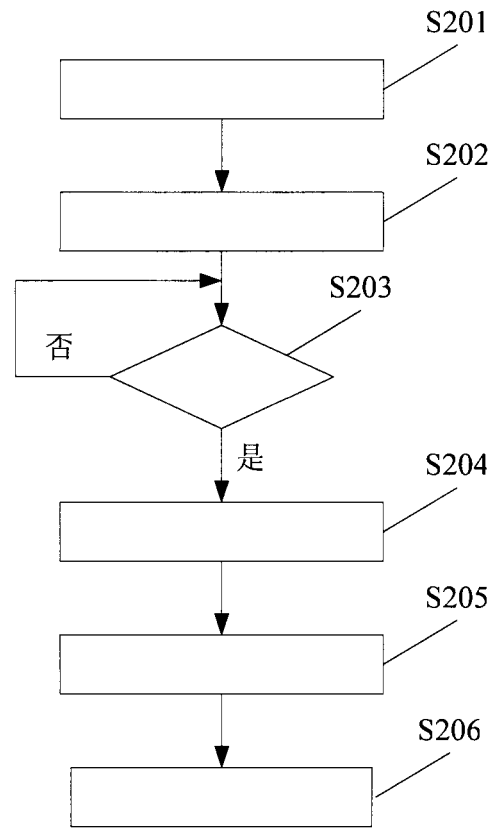


图 2

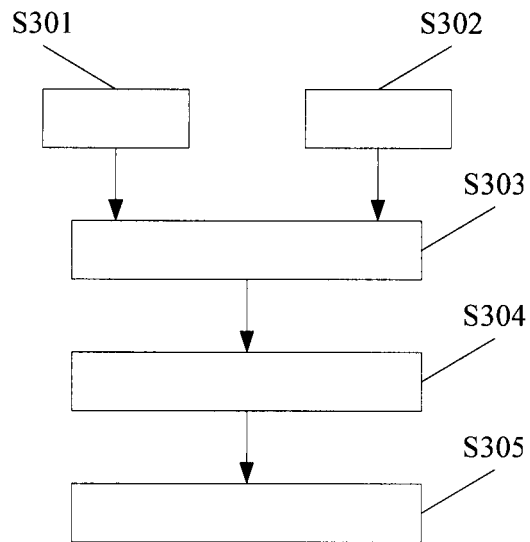


图 3

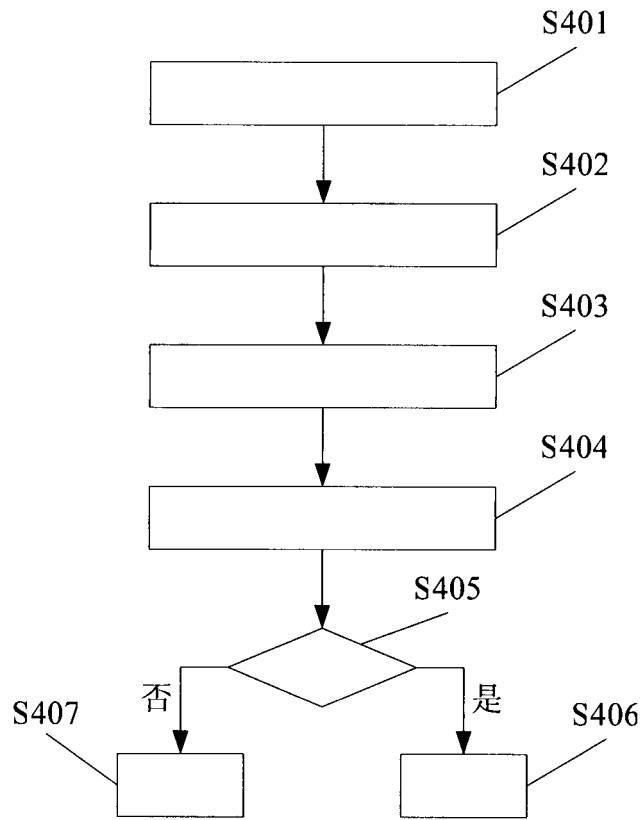


图 4

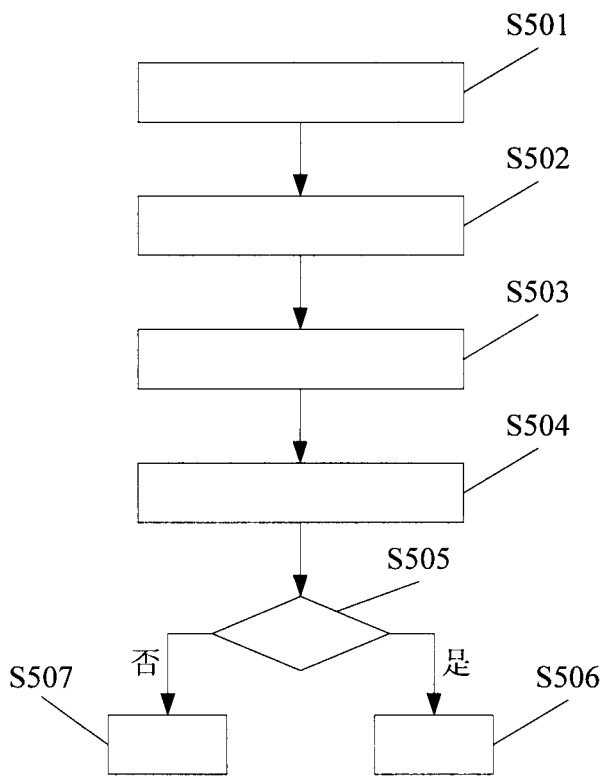


图 5

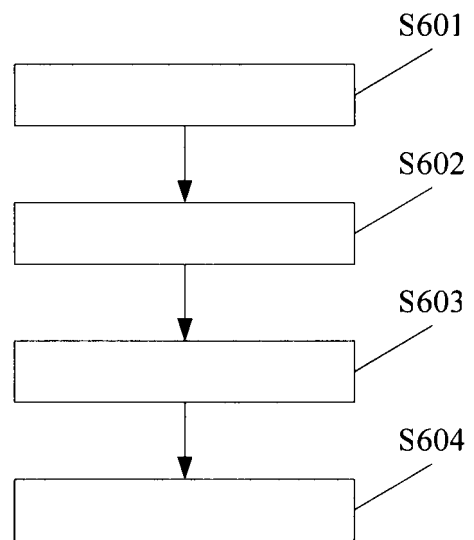


图 6

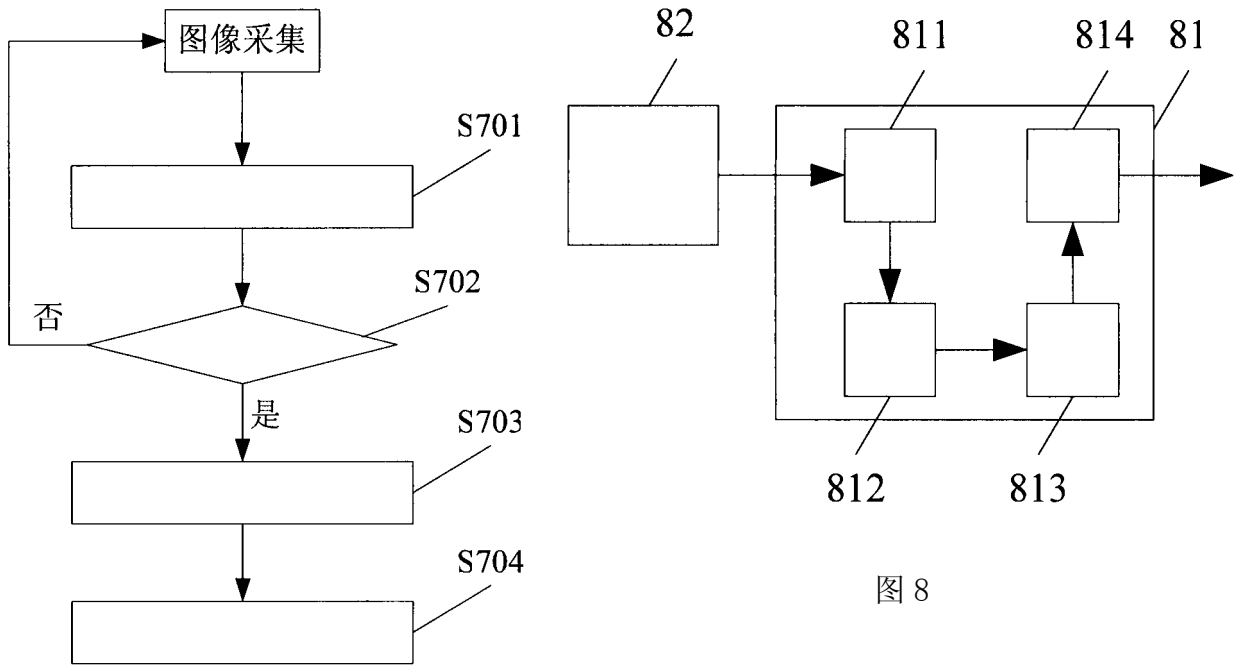


图 7

图 8

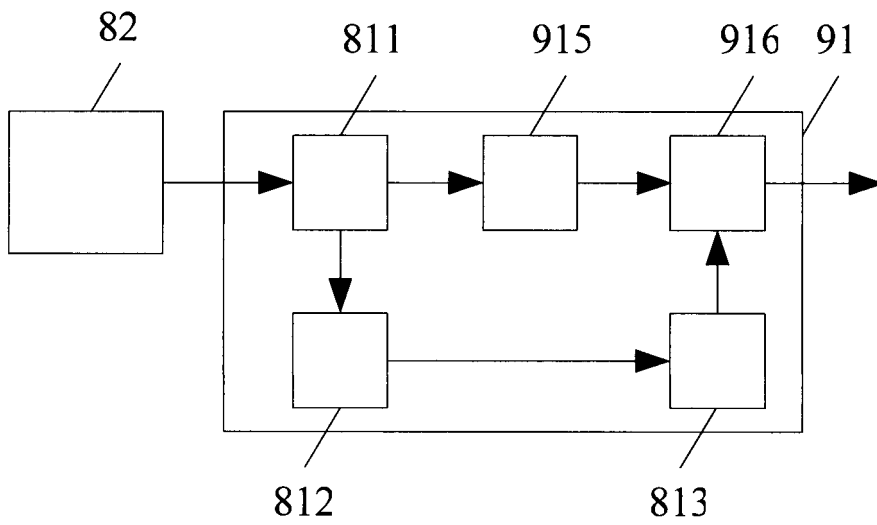


图 9

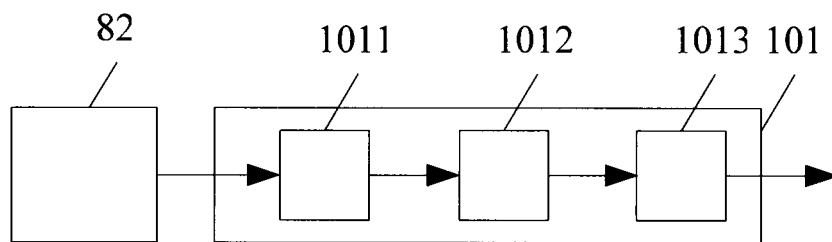


图 10