(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 103745151 A
(43)申请公布日 2014.04.23

(21)申请号 201410009604.2
(22)申请日 2014.01.08
(71)申请人 杭州晟元芯片技术有限公司
地址 311121 浙江省杭州市余杭区五常街道文一西路998号海创园9幢东
(72)发明人 杨波 罗美美 邱柏云
(74)专利代理机构 杭州九洲专利事务所有限公司 33101
代理人 陈继亮
(51)Int.Cl.
G06F 21/36(2013.01)
G06F 21/46(2013.01)
H04L 9/32(2006.01)
G06K 19/06(2006.01)

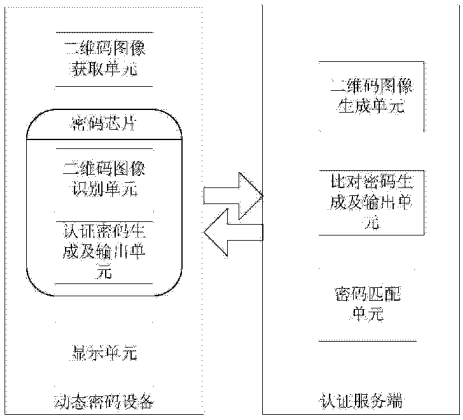
权利要求书2页 说明书9页 附图5页

(54)发明名称

一种二维码与动态密码相结合的身份认证系统及方法

(57)摘要

本发明涉及一种二维码与动态密码相结合的身份认证系统及方法，该系统主要由动态密码设备和认证服务端两大部分组成，动态密码设备包括二维码图像获取单元、二维码图像识别单元、认证密码生成及输出单元和显示单元，认证服务端包括二维码图像生成单元、比对密码生成及输出单元和密码匹配单元。本发明具有如下效果：将挑战码或特定的交易信息按照一定的编码规则生成二维码，仅需通过获取和识别二维码图像就可以得到挑战码或特定的交易信息，更加方便快捷，给用户带来极大的便利。二维码图像不仅可以由数字生成，也可由文字或其他形式生成，这在很大程度上弥补了之前的动态密码设备只能通过键盘输入数字作为挑战码的缺陷，提高了身份认证的安全性。



CN 103745151 A

1. 一种二维码与动态密码相结合的身份认证系统，其特征在于：该系统主要由动态密码设备和认证服务端两大部分组成，动态密码设备包括二维码图像获取单元、二维码图像识别单元、认证密码生成及输出单元和显示单元，其中二维码图像获取单元用于通过摄像模组对屏幕上显示的二维码图像进行拍照，来获取认证服务端生成的二维码灰度图像；二维码图像识别单元用于通过二维码识别方法对获取到的二维码灰度图像进行解码，获取其中的挑战码或特定的交易信息；显示单元用于显示拍摄到的二维码灰度图像和显示二维码解码信息，以验证解码信息的正确性；认证服务端包括二维码图像生成单元、比对密码生成及输出单元和密码匹配单元，其中二维码图像生成单元用于将认证服务端随机生成的挑战码或特定的交易信息，按照特定的编码规则生成二维码灰度图像；比对密码生成及输出单元用于将随机生成的挑战码或特定的交易信息按照预定的加密算法加密生成比对密码并输出，加密算法与认证密码及输出单元中的加密算法保持一致；密码匹配单元用于将认证密码生成及输出单元生成的认证密码与比对密码生成及输出单元生成的比对密码进行匹配，如果二者一致，则该次身份认证成功，否则，该次身份认证失败。

2. 一种采用如权利要求 1 所述的二维码与动态密码相结合的身份认证系统的方法，其特征在于：该方法包括如下步骤：

1)、认证服务器端根据随机生成的挑战码或特定的交易信息按照一定的编码规则生成专用的二维码图像，并将其在交互界面上进行显示；

2)、认证服务器端根据随机生成的挑战码或特定的交易信息按照预定的加密算法加密生成比对密码；

3)、动态密码设备中的二维码获取单元通过摄像头对二维码图像进行拍照，并在动态密码设备的显示屏上进行显示二维码灰度图像；

4)、通过动态密码设备中的二维码图像识别单元，对二维码灰度图像进行解码，并将解码得到的信息显示出来，当解码生成的挑战码或特定的交易信息有误时，返回步骤 2) 重新对二维码图像进行拍照并重新解码，直到获得正确的挑战码或特定的交易信息；当解码生成的挑战码或交易信息正确时，直接进入下一步；

5)、将解码出来的挑战码或特定的交易信息按照预定的加密算法加密生成认证密码，并将其输出，这里的加密算法与步骤 2) 中的加密算法保持一致；

6)、将认证密码与比对密码进行匹配，当二者匹配时，该次身份认证成功，否则，该次身份认证失败。

3. 根据权利要求 2 所述的二维码与动态密码相结合的身份认证方法，其特征在于：二维码图像识别单元对具体的二维码图像解码过程的表述如下：

a) 对获取到的二维码灰度图像进行二值化；

b) 对二值化后的图像进行图像膨胀，具体过程为：用一个结构元素扫描图像中的每一个像素，用结构元素中的每一个像素与其覆盖的像素做“与”操作，如果都为零，则该像素为 0，否则为 1；

c) 对膨胀后的图像进行边缘提取，其具体过程为：用一个值全部为 1 的结构元素扫描图像中的每一个像素，用结构元素中的每一个像素与其覆盖的像素做“与”操作，如果为 0，认为该像素所在处不是边缘，否则认为该像素所在处为边缘；

d) 对边缘提取后的图像进行基于 Hough 变换的直线检测，其具体过程为：Hough 变换利

用图像空间和 Hough 参数空间的点线对偶性，把图像空间中的检测问题转换到参数空间，通过在参数空间进行简单的累加统计，然后在 Hough 参数空间寻找累加器峰值的方法来检测直线，针对二维码图像，直线检测的结果为用四条直线来拟合已经提取出来的边缘，取四条直线的四个交点为初定位的四个顶点；

e) 对获取的二维码图像进行第一次几何矫正，该矫正过程包括空间变换和灰度级补差，其具体的过程为：首先找出失真图像与矫正图像间的映射关系，然后通过它们的映射关系进行空间变换，空间变换后，通过灰度差值来恢复图像位置灰度；

f) 对矫正后的图像进行二值化，二值化方法同步骤 b)；

g) 对二值化后的图像进行精确定位，找出 3 个寻像图形所在的中心坐标，其具体方法为：分别取图像中的左上、右上和左下三块小图像，对图像进行腐蚀，寻找连通区域，然后根据寻像图形的特征找出与寻像图形的中心黑块最相近的块，块的中心即为寻像图形的中心；接着找出右下角的校正图形的中心，再根据以上四个图形重新找出图像的四个顶点；找出 3 个寻像图形的中心后，判断 3 个寻像图形的相对位置，当寻像图形不在标准位置时，对图像进行旋转，使 3 个寻像图形在标准的位置上；

h) 根据重新找出的四个顶点，对二维码图像进行第二次矫正，矫正方法同步骤 e)；

i) 选择一个二维码图像版本号；

j) 结合版本号和三个寻像图形的位置，对第二次矫正后的图像建立采样网格，并采样数据，将图像转换为数据矩阵；

k) 对生成的数据矩阵进行解码，包括格式信息译码、纠错和数据码字译码步骤；

l) 对解码信息进行校验，如果校验结果不正确，返回重新建立采样网格或重新确定版本号，当返回次数大于某一阈值时，将不再返回；

m) 将解码信息进行输出。

一种二维码与动态密码相结合的身份认证系统及方法

技术领域

[0001] 本发明涉及信息安全身份认证技术领域，尤其是指一种二维码与动态密码相结合的身份认证系统及方法。

背景技术

[0002] 随着科技的发展，身份认证的安全性得到越来越多的重视，相应的强身份认证的动态密码技术已经越来越多地应用于各个不同领域。动态密码的特点是仅可以使用一次且具有时效性，因此它抵抗攻击的能力较强。但现有的动态密码技术也存在一些缺陷，如用户需要手动输入挑战码，信息量大，且比较繁琐，很容易出现输入错误。此外由于动态密码设备的键盘限制，只能输入数字形式的挑战码，而不能输入文字或其他形式，这样就极大地限制了动态密码设备安全性能的提高。基于以上缺陷，迫切需要安全性能更高的身份认证方案，因此一种二维码与动态密码相结合的身份认证方案应运而生。

[0003] 现有的基于动态密码的身份认证方案，其结构图如图 1 所示描述如下 ：

[0004] 1) 用户发出认证请求，后台服务器随机生成挑战码，并输出给动态密码设备 ；

[0005] 2) 动态密码设备获取挑战码，这些外部输入的挑战码按照预定的加密算法参与生成认证密码 ；

[0006] 3) 后台服务器端根据挑战码，按照预定的加密算法生成比对密码，这里的加密算法应与 2) 保持一致 ；

[0007] 4) 动态密码设备向后台服务器发送认证请求，即将生成的认证密码发送给后台服务器 ；

[0008] 5) 后台服务器将认证密码和后台服务器端生成的比对密码进行匹配 ；

[0009] 6) 返回认证结果 :若认证密码与比对密码匹配，本次身份认证成功，否则，身份认证失败。

[0010] 现有方案的缺点 :现有的动态密码设备，凡是涉及外部输入因子参与生成密码的，均需以键盘方式进行输入，且均为数字。以挑战应答型动态密码设备为例，对于帐号、金额、挑战码等信息，需要用户手动输入，由于信息量大，用户手动输入较为繁琐，并且容易出现输入错误，比较费时费力。此外，由于动态密码设备的按键输入限制，挑战码只能是数字形式，生成的认证密码安全性不高。

发明内容

[0011] 本发明解决的技术问题包括以下二个方面 :1、动态密码设备中的挑战码需要手动输入，费时费力 ;2、挑战码只能以数字的形式进行表征，不能包含文字或其他形式的挑战信息，生成的认证密码安全性不高。

[0012] 本发明的目的在于克服现有技术存在的不足，而提供一种二维码与动态密码相结合的身份认证系统及方法。

[0013] 本发明的目的是通过如下技术方案来完成的。这种二维码与动态密码相结合的身

份认证系统，该系统主要由动态密码设备和认证服务端两大部分组成，动态密码设备包括二维码图像获取单元、二维码图像识别单元、认证密码生成及输出单元和显示单元，其中二维码图像获取单元用于通过摄像模组对屏幕上显示的二维码图像进行拍照，来获取认证服务端生成的二维码灰度图像；二维码图像识别单元用于通过二维码识别方法对获取到的二维码灰度图像进行解码，获取其中的挑战码或特定的交易信息；显示单元用于显示拍摄到的二维码灰度图像和显示二维码解码信息，以验证解码信息的正确性；认证服务端包括二维码图像生成单元、比对密码生成及输出单元和密码匹配单元，其中二维码图像生成单元用于将认证服务端随机生成的挑战码或特定的交易信息，按照特定的编码规则生成二维码灰度图像；比对密码生成及输出单元用于将随机生成的挑战码或特定的交易信息按照预定的加密算法加密生成比对密码并输出，加密算法与认证密码及输出单元中的加密算法保持一致；密码匹配单元用于将认证密码生成及输出单元生成的认证密码与比对密码生成及输出单元生成的比对密码进行匹配，如果二者一致，则该次身份认证成功，否则，该次身份认证失败。

[0014] 本发明所述的这种二维码与动态密码相结合的身份认证方法，该方法包括如下步骤：

[0015] 1)、认证服务器端根据随机生成的挑战码或特定的交易信息按照一定的编码规则生成专用的二维码图像，并将其在交互界面上进行显示；

[0016] 2)、认证服务器端根据随机生成的挑战码或特定的交易信息按照预定的加密算法加密生成比对密码；

[0017] 3)、动态密码设备中的二维码获取单元通过摄像头对二维码图像进行拍照，并在动态密码设备的显示屏上进行显示二维码灰度图像；

[0018] 4)、通过动态密码设备中的二维码图像识别单元，对二维码灰度图像进行解码，并将解码得到的信息显示出来，当解码生成的挑战码或特定的交易信息有误时，返回步骤 2) 重新对二维码图像进行拍照并重新解码，直到获得正确的挑战码或特定的交易信息；当解码生成的挑战码或交易信息正确时，直接进入下一步；

[0019] 5)、将解码出来的挑战码或特定的交易信息按照预定的加密算法加密生成认证密码，并将其输出，这里的加密算法与步骤 2) 中的加密算法保持一致；

[0020] 6)、将认证密码与比对密码进行匹配，当二者匹配时，该次身份认证成功，否则，该次身份认证失败。

[0021] 其中，二维码图像识别单元对具体的二维码图像解码过程的表述如下：

[0022] a) 对获取到的二维码灰度图像进行二值化；

[0023] b) 对二值化后的图像进行图像膨胀，具体过程为：用一个结构元素扫描图像中的每一个像素，用结构元素中的每一个像素与其覆盖的像素做“与”操作，如果都为零，则该像素为 0，否则为 1；

[0024] c) 对膨胀后的图像进行边缘提取，其具体过程为：用一个值全部为 1 的结构元素扫描图像中的每一个像素，用结构元素中的每一个像素与其覆盖的像素做“与”操作，如果为 0，认为该像素所在处不是边缘，否则认为该像素所在处为边缘；

[0025] d) 对边缘提取后的图像进行基于 Hough 变换的直线检测，其具体过程为：Hough 变换利用图像空间和 Hough 参数空间的点线对偶性，把图像空间中的检测问题转换到参数空

间，通过在参数空间进行简单的累加统计，然后在 Hough 参数空间寻找累加器峰值的方法来检测直线，针对二维码图像，直线检测的结果为用四条直线来拟合已经提取出来的边缘，取四条直线的四个交点为初定位的四个顶点；

[0026] e) 对获取的二维码图像进行第一次几何矫正，该矫正过程包括空间变换和灰度级补差，其具体的过程为：首先找出失真图像与矫正图像间的映射关系，然后通过它们的映射关系进行空间变换，空间变换后，通过灰度差值来恢复图像位置灰度；

[0027] f) 对矫正后的图像进行二值化，二值化方法同步骤 b)；

[0028] g) 对二值化后的图像进行精确定位，找出 3 个寻像图形所在的中心坐标，其具体方法为：分别取图像中的左上、右上和左下三块小图像，对图像进行腐蚀，寻找连通区域，然后根据寻像图形的特征找出与寻像图形的中心黑块最相近的块，块的中心即为寻像图形的中心；接着找出右下角的校正图形的中心，再根据以上四个图形重新找出图像的四个顶点；找出 3 个寻像图形的中心后，判断 3 个寻像图形的相对位置，当寻像图形不在标准位置时，对图像进行旋转，使 3 个寻像图形在标准的位置上；

[0029] h) 根据重新找出的四个顶点，对二维码图像进行第二次矫正，矫正方法同步骤 e)；

[0030] i) 选择一个二维码图像版本号；

[0031] j) 结合版本号和三个寻像图形的位置，对第二次矫正后的图像建立采样网格，并采样数据，将图像转换为数据矩阵；

[0032] k) 对生成的数据矩阵进行解码，包括格式信息译码、纠错和数据码字译码步骤；

[0033] l) 对解码信息进行校验，如果校验结果不正确，返回重新建立采样网格或重新确定版本号，当返回次数大于某一阈值时，将不再返回；

[0034] m) 将解码信息进行输出。

[0035] 本发明具有如下效果：

[0036] 1) 将挑战码或特定的交易信息按照一定的编码规则生成二维码，仅需通过获取和识别二维码图像就可以得到挑战码或特定的交易信息，而不需要手动输入以上信息，更加方便快捷，给用户带来极大的便利。

[0037] 2) 二维码图像不仅可以由数字生成，也可以由文字或其他形式生成，这在很大程度上弥补了之前的动态密码设备只能通过键盘输入数字作为挑战码的缺陷，提高了身份认证的安全性。

[0038] 3) 引入了一种新的二维码解码技术，它在嵌入式的某些专用领域具有解码性能高和速度快等优势。

[0039] 4) 引入了一种新的自动曝光技术，它可以根据周围环境对所采集图像的曝光度进行自动调整，这样即使在很复杂的环境下，也可以获得质量很高的图像。

[0040] 5) 本发明的核心算法均是在密码芯片上实现的，密码芯片的采用提高了动态密码设备的安全性，降低了动态密码设备的成本。

附图说明

[0041] 图 1 是现有技术的方框示意图；

[0042] 图 2 是本发明的方框示意图；

[0043] 图 3 是本发明中密码芯片的组成框图；

[0044] 图 4 是本发明中二维码图像的整个解码流程图；

[0045] 图 5 是本发明中身份认证方法流程图；

[0046] 图 6 是 ATM 机或网上银行转账应用时的方框示意图。

具体实施方式

[0047] 下面将结合附图对本发明做详细的介绍：

[0048] 本发明提出的一种二维码与动态密码相结合的身份认证系统主要由动态密码设备和认证服务端两大部分组成，其具体的系统框图如图 2 所示：

[0049] 1) 二维码图像获取单元：该单元主要通过摄像模组对屏幕上显示的二维码图像进行拍照，来获取认证服务端生成的二维码图像。该图像获取单元由图像传感器芯片和镜头组组成，并通过标准图像传感器接口与其他模块相连接。考虑成本和使用的方便性，本发明采用的为普通的手机上的广角镜头模组，由图像传感器芯片（CMOS），广角镜头组，连接线组成。摄像模组直接从 CMOS 芯片上获取 RAW 格式图像。该发明将获取到的原始数据直接转化为灰度 BMP 图像，而不是转化为 RGB 彩色图像，这样每个像素仅需保存 8 位数据而不是 24 位数据，节省了存储空间。此外，本发明后续需要处理的也是灰度 BMP 图像，采用以上技术不需要再将 RGB 彩色图像转化为 BMP 灰度图像处理，简化了处理过程。需要特别指出的是该单元加入了一种自动曝光技术，即在采集图像时，摄像模组可以根据周围环境的亮度不同进行自动调整，以保证采集的图像拥有合适的曝光度。该技术的引入使得所采集的图像拥有较好的质量，提高了对环境的适应性，避免了曝光过度和曝光不足的情况，提高了后续处理效果。该自动曝光技术的具体处理过程如下：

[0050] a) 通过二维码图像获取单元获取一幅二维码灰度图像；

[0051] b) 对获取的灰度图像进行灰度直方图统计，如果其灰度分布比较分散，取接近最高像素值的某个像素为背景亮度，不需要进行曝光时间的调整，如果其灰度分布集中在像素值很高的几个像素，则减少曝光时间，反之，如果其灰度分布集中在像素值很低的几个像素，则增加曝光时间；

[0052] c) 将图像传感器芯片的曝光时间参数设置为将调整后的值，这样在下次获取图像时就可以获得较合适的曝光度，得到更加清晰的图像。

[0053] 2) 二维码图像识别单元：通过特定的二维码识别方法对获取到的二维码图像进行解码，获取其中的挑战码或特定的交易信息。对具体的二维码图像解码过程的表述如下：

[0054] a) 对获取到的二维码灰度图像进行二值化，二值化阈值的选择显得很重要，本发明针对不同的二维码图像选择不同的方法，对质量较好的图像采用整体阈值，对曝光不均匀的图像采用分块阈值。

[0055] b) 对二值化后的图像进行图像膨胀。图像膨胀的具体过程为：用一个结构元素扫描图像中的每一个像素，用结构元素中的每一个像素与其覆盖的像素做“与”操作，如果都为零，则该像素为 0，否则为 1。这里图像膨胀的次数与二值化图像的质量有关，次数选择的基本原则为尽量保留二维码图像的有效区域，并去除与图像无关的干扰区域。

[0056] c) 对膨胀后的图像进行边缘提取。其具体过程为：用一个值全部为 1 的结构元素

扫描图像中的每一个像素，用结构元素中的每一个像素与其覆盖的像素做“与”操作，如果为 0，认为该像素所在处不是边缘，否则认为该像素所在处为边缘。

[0057] d) 对边缘提取后的图像进行基于 Hough 变换的直线检测，其具体过程为：Hough 变换利用图像空间和 Hough 参数空间的点线对偶性，把图像空间中的检测问题转换到参数空间。通过在参数空间进行简单的累加统计，然后在 Hough 参数空间寻找累加器峰值的方法来检测直线。针对二维码图像，直线检测的结果为用四条直线来拟合已经提取出来的边缘，取四条直线的四个交点为初定位的四个顶点。

[0058] e) 对获取的二维码图像进行第一次几何矫正。该矫正过程包括空间变换和灰度级补差。其具体的过程为：首先找出失真图像与矫正图像间的映射关系，然后通过它们的映射关系进行空间变换，空间变换后，通过灰度差值来恢复图像位置灰度。

[0059] f) 对矫正后的图像进行二值化，二值化方法同 b)。

[0060] g) 对二值化后的图像进行精确定位，找出 3 个寻像图形所在的中心坐标。其具体方法为：分别取图像中的左上、右上和左下三块小图像，对图像进行腐蚀，寻找连通区域，然后根据寻像图形的特征找出与寻像图形的中心黑块最相近的块，块的中心即为寻像图形的中心。接着找出右下角的校正图形的中心，再根据以上四个图形重新找出图像的四个顶点。找出 3 个寻像图形的中心后，判断 3 个寻像图形的相对位置，当寻像图形不在标准位置时，对图像进行旋转，使 3 个寻像图形在标准的位置上。

[0061] h) 根据重新找出的四个顶点，对二维码图像进行第二次矫正，矫正方法同 e)。

[0062] i) 由于二维码生成单元生成的二维码图像已经固定为 1 个或某几个版本，所以这里仅需要选择一个版本号。

[0063] j) 结合版本号和三个寻像图形的位置，对第二次矫正后的图像建立采样网格，并采样数据，将图像转换为数据矩阵，以便于后续的解码。

[0064] k) 对生成的数据矩阵进行解码，它主要包括格式信息译码、纠错和数据码字译码等步骤。

[0065] l) 对解码信息进行校验，如果校验结果不正确，返回重新建立采样网格或重新确定版本号，当返回次数大于某一阈值时，将不再返回。

[0066] m) 将解码信息进行输出。

[0067] 3) 认证密码生成及输出单元：该单元结合解码出来的挑战码或特定的交易信息，按照预定的加密算法（如 DES，RSA）加密生成认证密码，并把它输出给密码匹配单元，以便于进行密码正确性的验证。

[0068] 4) 显示单元：用于显示拍摄到的二维码图像，以获取质量较好的二维码图像，此外该单元还用于显示二维码解码信息，以验证解码信息的正确性。

[0069] 5）二维码图像生成单元：将认证服务端随机生成的挑战码或特定的交易信息，按照特定的编码规则生成二维码图像。因为本发明主要应用在专用场合，仅使用某一个或某几个版本已经可以满足实际应用要求，所以这里生成的二维码图像固定在某一个或某几个版本。

[0070] 6) 比对密码生成及输出单元：将随机生成的挑战码或特定的交易信息按照预定的加密算法加密生成比对密码并输出，这里的加密算法应与认证密码及输出单元中的加密算法保持一致。

[0071] 7）密码匹配单元：将认证密码生成及输出单元生成的认证密码与比对密码生成及输出单元生成的比对密码进行匹配，如果二者一致，则该次身份认证成功，否则，该次身份认证失败。

[0072] 需要特别指出的是该发明中的密码芯片（包括二维码图像识别单元和认证密码生成及输出单元）是在单颗密码芯片上实现了二维码解码功能和加解密功能。本发明所采用的密码芯片的组成框图如图 3 所示（该框图仅显示密码芯片的主要组成部分）。

[0073] 下面对框图所显示的密码芯片的组成部分进行具体介绍：

[0074] FLASH：它是一种存储介质，主要用来存放代码如本发明中用到的二维码图像识别代码，加解密代码。该 FLASH 为内嵌的，采用这种方式可提高芯片的数据存取速度，降低成本。

[0075] RAM：它是一种动态内存，主要用来存放临时变量如代码运行时需处理的图像数据和所申请的变量等。RAM 读取数据的速度远快于 FLASH，它的大小会影响运行速度。这里的 RAM 也是内嵌的，它也可以提高速度，降低成本。

[0076] MPU（存储器保护单元）：可对 FLASH、SRAM、ROM 及其他存储介质进行加密保护，该单元的引入保证了芯片的安全性。

[0077] CMOS 接口：通过该接口与二维码图像获取单元相连接，将镜头模组所采集的二维码图像传给密码芯片，以利于密码芯片对图像进行解码，当解码正确时直接将其显示出来，当解码不正确时，通过该接口反馈给二维码图像获取单元，重新进行拍照。

[0078] 随机数生成器：可以生成一组随机数，用于加解密算法，它的引入提高了加解密算法的抗攻击强度，提高了算法的安全性。

[0079] 硬件加速器：可提高代码的运行速度，在本发明中该单元的主要功能为提高二维码图像解码算法和加解密算法的运行速度。

[0080] 本发明所采用的密码芯片可集成 RSA、DES、3DES、SM1、SM2、SM3 和 SM4 等多种加密算法及多种图像处理及识别算法，具有功能强大、处理速度快、安全性高和成本低等特点。此外，发明采用的密码芯片为单芯片，可以将原来需要数枚芯片实现的功能集中到一枚芯片上来实现，这样提高了芯片的集成度，进一步降低了成本；本发明采用的密码芯片使用内嵌的 FLASH 和 SRAM，不需要进行外扩，可直接在内部 FLASH 和 SRAM 中存取数据，提高了处理速度。

[0081] 二维码图像的整个解码流程图如图 4 所示。

[0082] 下面将对本发明所采用的一种二维码与动态密码相结合的身份认证方法进行具体介绍，其流程图如图 5 所示。

[0083] 结合以上的流程图，本方案所采用的一种二维码与动态密码相结合的身份认证方法描述如下：

[0084] 1）认证服务器端根据随机生成的挑战码或交易信息按照一定的编码规则生成专用的二维码图像，并将其在交互界面上进行显示。

[0085] 2）认证服务器端根据随机生成的挑战码或交易信息按照预定的加密算法加密生成比对密码。

[0086] 3）动态密码设备中的二维码获取单元通过摄像头对二维码图像进行拍照，并在动态密码设备的显示屏上进行显示。通过显示屏可以查看生成图像的质量，当生成的图像质

量较差时，可以重新进行拍摄，以获取质量较好的二维码灰度图像。

[0087] 4) 通过动态密码设备中的二维码图像识别单元，对二维码图像进行解码，并将解码得到的信息显示出来，当解码生成的挑战码或交易信息有误时，返回 2) 重新对二维码图像进行拍照并重新解码，直到获得正确的挑战码或交易信息。当解码生成的挑战码或交易信息正确时，直接进入下一步。

[0088] 5) 将解码出来的挑战码或交易信息按照预定的加密算法加密生成认证密码，并将其输出，这里的加密算法应与 2) 中的加密算法保持一致。

[0089] 6) 将认证密码与比对密码进行匹配，当二者匹配时，该次身份认证成功，否则，该次身份认证失败。

[0090] 本发明的典型应用 ：

[0091] 1)ATM 机或网上银行转帐时的身份认证 ；

[0092] 2) 登录界面的身份认证 ；

[0093] 3) 门禁系统身份认证 ；

[0094] 4) 与银行联网的消费系统的身份认证。

[0095] 下面以 ATM 机或网上银行转账为例介绍本发明提出的一种二维码与动态密码相结合的身份认证系统的应用，其结构框图如图 6 所示 ：

[0096] 结合以上框图，用户在 ATM 机和网上银行进行转账时的身份认证过程如下 ：

[0097] 1) 用户在 ATM 机或网上银行的交互界面输入付款帐号、户名、转账金额、转入户名和转入帐号等信息，并提交给银行后台服务器。

[0098] 2) 银行后台服务器将交易信息生成二维码并显示在 ATM 机或网上银行的操作界面上。

[0099] 3) 用户使用动态密码设备对 ATM 机或网上银行的操作界面上的二维码图像进行拍照，以获取二维码图像。

[0100] 4) 利用动态密码设备中的二维码图像识别单元来识别二维码图像，提取出其中的付款帐号、户名、转账金额、转入户名和转入帐号等信息，并将其显示出来。

[0101] 5) 用户核对交易信息是否正确，如果不正确，返回 3) 重新进行拍照和解码，如果正确，将交易信息通过预定加密算法进行加密生成认证密码并将其显示出来。

[0102] 6) 用户通过 ATM 机或网上银行的交互界面输入认证密码，并提交给银行后台服务器。

[0103] 7) 银行后台服务器将认证密码与自身生成的比对密码进行匹配，如果二者一致，本次交易成功，否则本次交易失败，结束本次交易。

[0104] 本发明提出的一种二维码与动态密码相结合的身份认证系统除了以上典型应用之外，凡是可以使用动态密码身份认证系统进行认证的地方，均可以使用本发明来代替。由此可见，本发明提出的的身份认证方案具有很大的实际应用价值。

[0105] 术语解释 ：

[0106] 1、二维码又名二维条码，是用某种特定的几何图形按一定的规律在平面（二维方向）分布的黑白相间的图形用来记录数据符号信息的，在代码编制上巧妙地利用构成计算机内部逻辑基础的“0”“1”比特流的概念，使用若干个与二进制相对应的几何形体来表示文字数值信息，通过图像输入设备或光电扫描设备进行自动识读以实现信息自动处理。它

具有高密度、信息量大、具有纠错能力和安全性强等优点。

[0107] 2、动态密码是指用户使用专门的设备或者软件在每次身份认证时都随机产生一个密码，由认证系统来验证密码的正确性并确认身份。动态密码可以有效地保护交易和账户的认证安全，采用动态密码就无需定期修改密码，安全省心。

[0108] 3、CMOS(Complementary Metal-Oxide-Semiconductor)，中文学名为互补金属氧化物半导体，它主要是利用硅和锗这两种元素所做成的半导体，使其在 CMOS 上共存着带 N(带 - 电)和 P (带 + 电)级的半导体，这两个互补效应所产生的电流即可被处理芯片纪录和解读成影像。后来发现 CMOS 经过加工也可以作为数码摄影中的图像传感器，CMOS 传感器也可细分为被动式像素传感器 (Passive Pixel Sensor CMOS) 与主动式像素传感器 (Active Pixel Sensor CMOS)。与垄断该领域长达 30 多年的 CCD 技术相比，它能够更好地满足用户对各种应用中新型图像传感器不断提升的品质要求，如更加灵活的图像捕获、更高的灵敏度、更宽的动态范围、更高的分辨率、更低的功耗以及更加优良的系统集成等。

[0109] 4、RAW 的原意是“未经加工”。可以理解为 :RAW 图像就是 CMOS 或者 CCD 图像感应器将捕捉到的光源信号转化为数字信号的原始数据。RAW 文件是一种记录了数码相机传感器的原始信息，同时记录了由相机拍摄所产生的一些原数据(Metadata，如 ISO 的设置、快门速度、光圈值、白平衡等)的文件。RAW 是未经处理、也未经压缩的格式，可以把 RAW 概念化为“原始图像编码数据”或更形象的称为“数字底片”。密码芯片 :一种可支持 DES、RSA 和 SM1 等加密算法，并且可以防止 DPA、SPA 等攻击的安全芯片，它可以用来处理和加密数据，以保证数据的安全性。

[0110] 5、芯片就是半导体元件产品的统称。包括 :集成电路(integrated circuit，缩写 :IC)、二级管和三极管及特殊电子元件。再广义些讲还涉及所有的电子元件如电阻，电容，电路版 /PCB 版等许多相关产品。

[0111] 6、SPA (Simple Power Analysis，简单能量分析攻击)，SPA 攻击通过分析电子设备执行计算过程中的能量消耗来寻找有关密钥的信息。

[0112] 7、DPA (DifferentialPowerAnalysis，差分能量分析攻击)，DPA 攻击技术具有更强的攻击性和解密效率，它的的原理是 :当芯片在执行不同的指令进行各种运算时，对应的功率消耗也相应变化。通过使用特殊的电子测量仪和数学统计技术，来检测和分析这些变化，从而得到芯片中的特定关键信息。这是一种利用指令的电流变化来分析密码算法和密码的方法。DPA 的攻击原理主要是根据数据和功耗之间的关联性，来还原出密钥，进而达到攻击的效果。

[0113] 8、SPA FLASH (Flash Memory) : 能在不加电的情况下能长期保持存储的信息，在有电情况下可以很方便的进行擦写。通常保存代码和不需要变化的数据。

[0114] 9、RAM (random access memory) 随机存储器。存储单元的内容可按需随意取出或存入，且存取的速度与存储单元的位置无关的存储器。这种存储器在断电时将丢失其存储内容，故主要用于存储短时间使用的程序。按照存储信息的不同，随机存储器又分为静态随机存储器(Static RAM,SRAM) 和动态随机存储器(Dynamic RAM,DRAM)。SRAM 由触发器存储数据，具有速度快、使用简单、不需刷新和静态功耗极低等优点，常用作 Cache。DRAM 利用 MOS 管栅极电容可以存储电荷的原理来存储数据，需刷新，它具有集成度高、功耗低和价格低等优点，所以在计算机中常用作主存储器。

[0115] 本文中所描述的具体实施例仅仅是对本发明精神作举例说明，并非对本发明的范围限定，在不背离本发明的精神和实质的情况下，本领域普通技术人员对本发明的技术方案作出的各种变形和改进，均属于本发明的权利要求书确定的保护范围内。

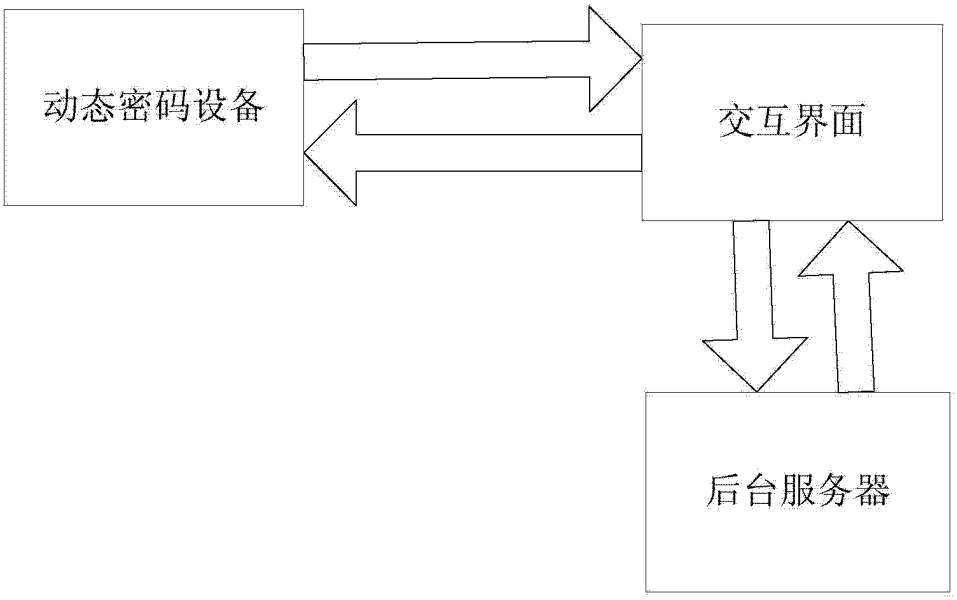

动态密码设备
交互界面
后台服务器

图 1

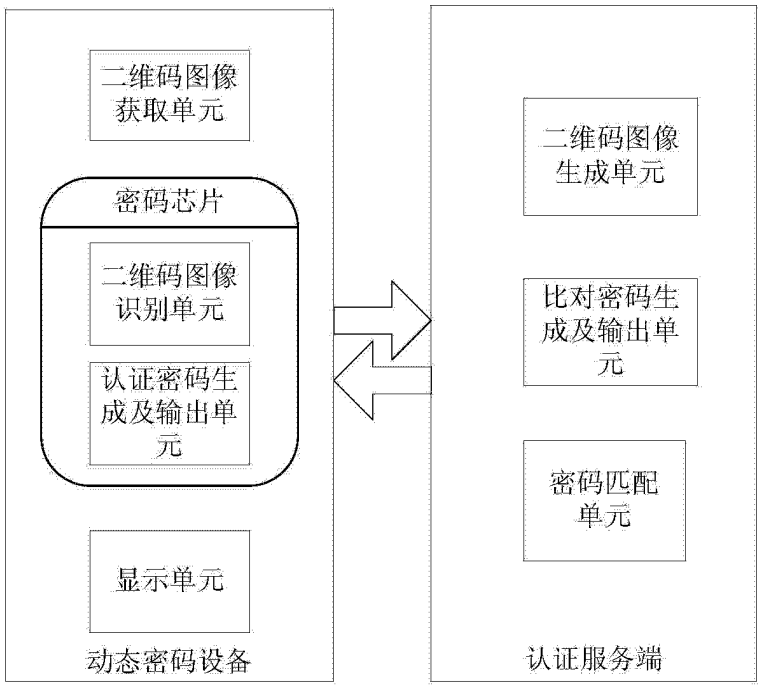

二维码图像获取单元
密码芯片
二维码图像识别单元
认证密码生成及输出单元
显示单元
动态密码设备
二维码图像生成单元
比对密码生成及输出单元
密码匹配单元
认证服务端

图 2

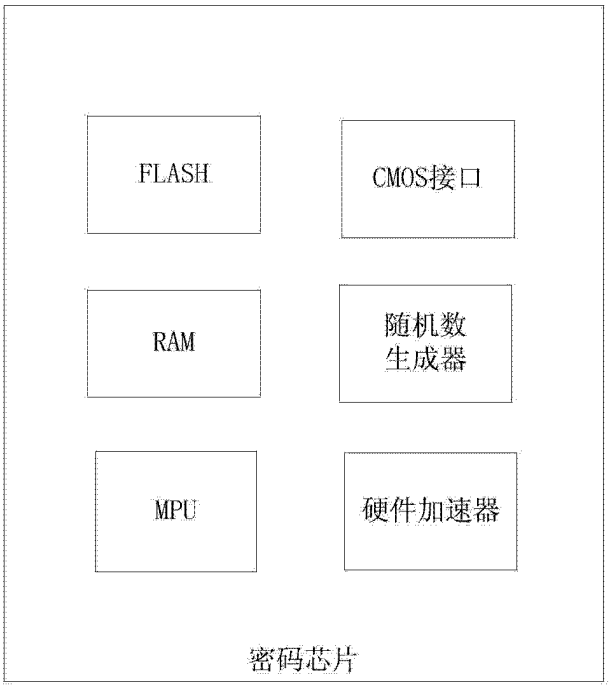


图 3

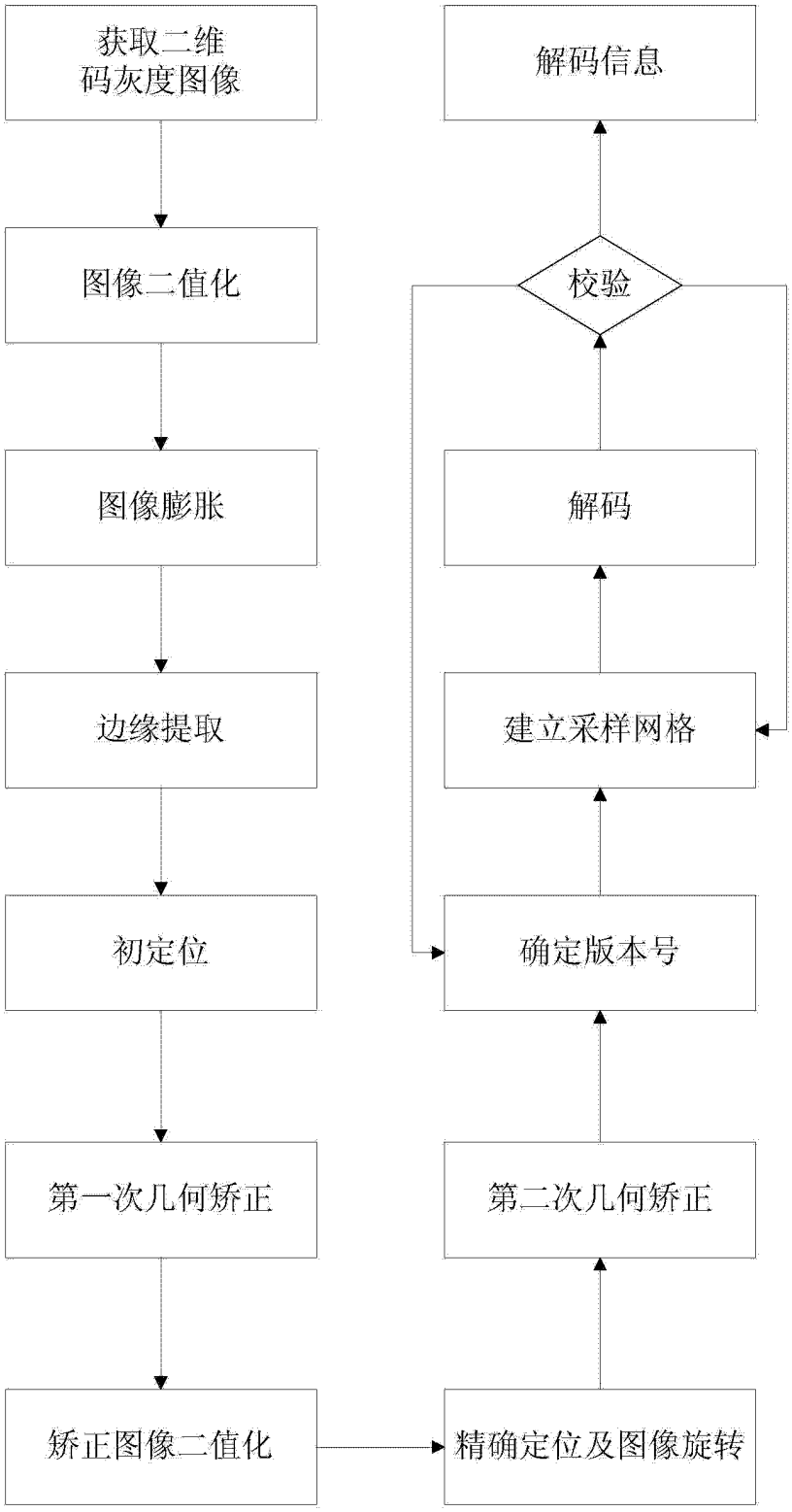

获取二维码灰度图像
图像二值化
图像膨胀
边缘提取
初定位
第一次几何矫正
矫正图像二值化
精确定位及图像旋转
第二次几何矫正
确定版本号
建立采样网格
解码
校验
解码信息

图 4

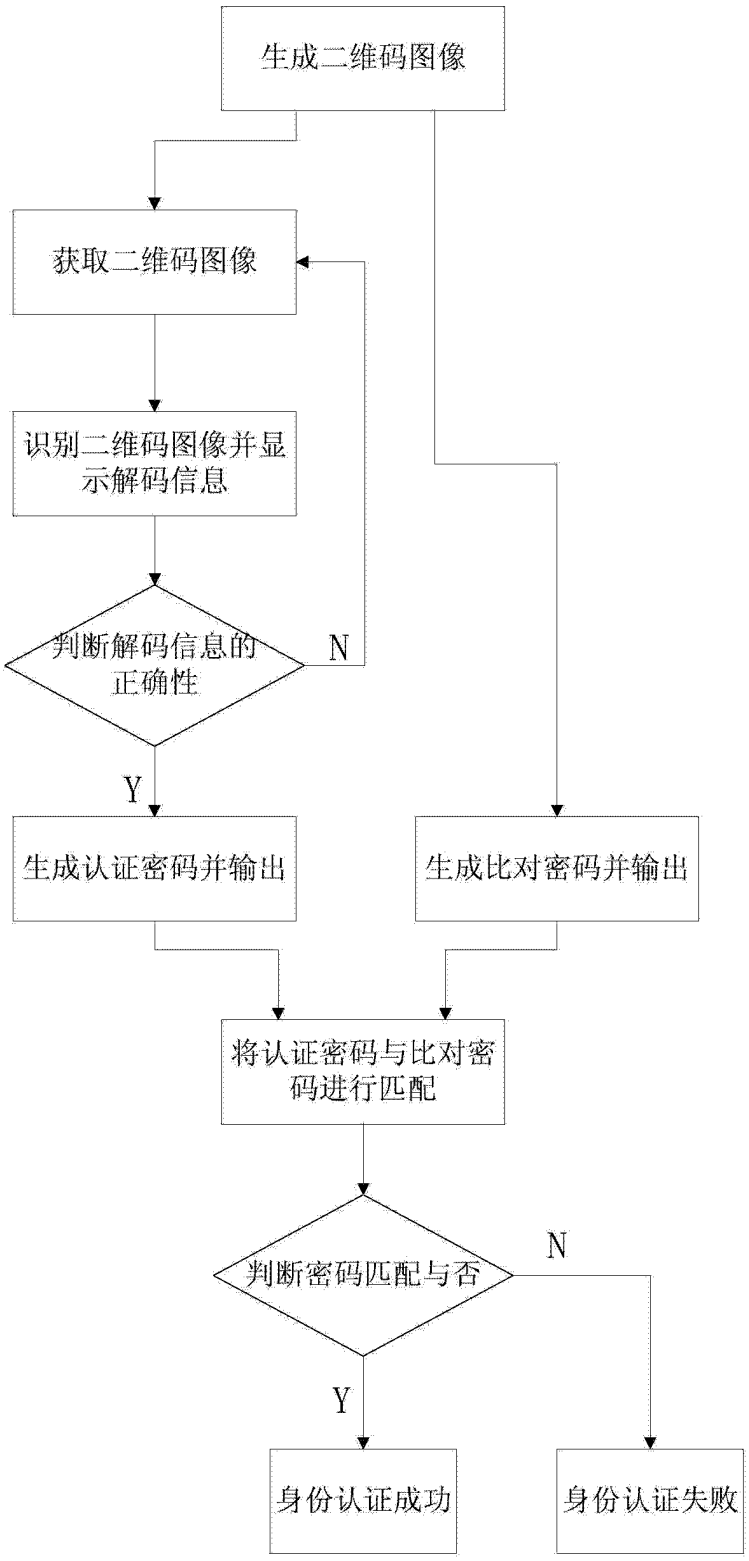

生成二维码图像
获取二维码图像
识别二维码图像并显示解码信息
判断解码信息的正确性
N
Y
生成认证密码并输出
生成比对密码并输出
将认证密码与比对密码进行匹配
判断密码匹配与否
N
Y
身份认证成功
身份认证失败

图 5

图 6