(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 101777212 A
(43)申请公布日 2010.07.14

(21)申请号 201010109030.8

(22)申请日 2010.02.05

(71)申请人 广州广电运通金融电子股份有限公司
地址 510000 广东省广州市萝岗区科学城科林路 9 号

(72)发明人 梁添才 牟总斌

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 李赞坚 逯长明

(51)Int.Cl.
G07F 7/10(2006.01)
G07F 7/12(2006.01)

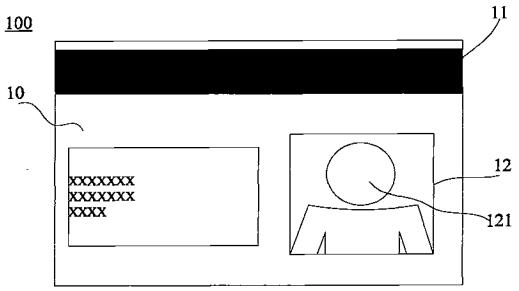
权利要求书 2 页 说明书 7 页 附图 4 页

(54)发明名称

安全卡、卡认证系统、具有该系统的金融设备及认证方法

(57)摘要

本发明提供一种安全卡以及卡认证系统，特别涉及一种具有安全认证的银行卡、银行卡认证系统。本安全卡将合法所有者人体生物特征信息中嵌入数字水印后与卡进行绑定的手段，解决安全卡被复制或篡改而引起的银行卡盗用的问题。这种安全卡包括一片状基体和至少一存储该卡信息的存储介质，该安全卡还包括安全卡合法所有者身份认证信息承载介质，所述合法所有者身份认证信息为经过数字水印加密后的人体生物特征信息。优选为将人体生物特征影像信息印刷于卡表面上，其中人体生物特征影像信息为脸部、指纹、静脉、虹膜等影像信息。



CN 101777212 A

1. 一种安全卡，其包括一片状基体和至少一存储该卡信息的存储介质，其特征在于，该安全卡还包括安全卡合法所有者身份认证信息承载介质，所述安全卡合法所有者身份认证信息为经过数字水印加密后的人体生物特征信息。

2. 根据权利要求 1 所述的安全卡，其特征在于，所述安全卡合法所有者身份认证信息承载介质为 IC 芯片。

3. 根据权利要求 1 所述的安全卡，其特征在于，所述安全卡合法所有者身份认证信息为嵌入数字水印的人体生物特征影像信息。

4. 根据权利要求 3 所述的安全卡，其特征在于，所述安全卡合法所有者身份认证信息承载介质为片状基体表面的印刷层，所述人体生物特征影像信息打印或印刷至印刷层上。

5. 根据权利要求 3 所述的安全卡，其特征在于，所述人体生物特征影像信息为脸部、指纹、静脉、虹膜中的一种影像或一种以上影像的组合。

6. 一种权利要求 1 所述安全卡的认证系统，其包括：

一身份认证信息读取单元，用于读取安全卡中包括的人体生物特征信息；

一人体生物特征信息采集单元，用于获得该安全卡使用者相应的人体生物特征信息；

一存储单元，用于存储安全卡中包括的人体生物特征信息中数字水印的提取算法以及标准数字水印样本；

一数字水印提取单元，用于提取所述安全卡中包括的人体生物特征信息中的数字水印；

一匹配对比单元，用于对所述数字水印提取单元提取的数字水印与存储单元中标准数字水印样本进行匹配对比，以及对安全卡中包括的人体生物特征信息与安全卡使用者相应的人体生物特征信息进行匹配对比；以及

一结果输出单元，将匹配对比单元得出的匹配对比结果输出。

7. 根据权利要求 6 所述安全卡的认证系统，其特征在于，所述安全卡中包括的人体生物特征信息为人体生物特征影像信息。

8. 根据权利要求 7 所述安全卡的认证系统，其特征在于，所述身份认证信息读取单元为影像扫描元件。

9. 根据权利要求 7 所述安全卡的认证系统，其特征在于，所述人体生物特征信息采集单元为人体生物特征影像采集元件。

10. 一种金融设备，其包括机壳、人机交互系统、安全卡信息读取装置、纸币处理机芯以及控制系统，其特征在于，还包括一卡认证系统，该卡认证系统包括：

一身份认证信息读取单元，用于读取安全卡中包括的人体生物特征信息；

一人体生物特征信息采集单元，用于获得该安全卡使用者相应的人体生物特征信息；

一存储单元，用于存储安全卡中包括的人体生物特征信息中数字水印的提取算法以及标准数字水印样本；

一数字水印提取单元，用于提取安全卡中包括的人体生物特征信息中的数字水印；

一匹配对比单元，用于对所述数字水印提取单元提取的数字水印与存储单元中标准数字水印样本进行匹配对比，以及对安全卡中包括的人体生物特征信息与安全卡使用者相应的人体生物特征信息进行匹配对比；

一结果输出单元，将匹配对比单元得出的匹配对比结果输出给控制系统。

11. 一种安全卡的认证方法，其包括步骤：

步骤一，读取使用中的安全卡内存储的一人体生物特征信息 C_T；

步骤二，采集安全卡使用者相应的人体生物特征信息 C'；

步骤三，对比该存储于安全卡内的人体生物特征信息 C_T 与该安全卡使用者相应的人体生物特征信息 C'，如果 $\| C' - C_T \| \leq J'$ 成立，则执行第四步，否则该安全卡认证失败；以及

步骤四，提取该安全卡内存储的人体生物特征信息 C_T 中的数字水印 W'，且将 W'与标准数字水印 W 相比对，如果 $\| W' - W \| \leq J$ 成立，则认证成功，否则该安全卡认证失败。

安全卡、卡认证系统、具有该系统的金融设备及认证方法

技术领域

[0001] 本发明涉及安全卡以及卡认证系统，特别涉及一种具有安全认证的银行卡、银行卡认证方法、银行卡认证系统以及具有该认证系统的金融自助设备。

背景技术

[0002] 数据显示，截至2009年一季度，我国银行卡累计发卡已达18.9亿张，特约商户120多万家，刷卡交易额已占社会消费品零售总额的27.7%，银行卡产业得到快速的发展。然而，公知的使用密码的银行卡均采用单一密码，其安全防护性较差，公安部门的统计数据显示，通过窃取银行卡信息和制作伪卡实施的犯罪行为占银行卡犯罪总数的75%以上，原因主要有：

[0003] (1) 目前国内的银行卡多为磁条卡，存在信息易复制、磁条易损坏、技术含量低、安全性差等问题；

[0004] (2) 客户的安全防范意识不高，犯罪分子通过盗码器、猜测银行卡号、设立虚假交易网站，或黑客软件、木马病毒等可以很轻易地窃取银行卡号、密码等信息；

[0005] (3) 制作伪卡技术难度低，犯罪分子非法获取银行卡信息后，只需磁条读写设备和简单技术即可制成包含原卡相关信息的伪卡；

[0006] (4) 我国对银行卡读卡器、制卡器的销售管理不够严格，给犯罪分子获得制作伪卡工具提供了便利条件。

[0007] 大量的犯罪行为开始入侵传统的磁条银行卡，银业内提出用智能IC卡替代磁条卡，即所谓的EMV迁移(EMV标准由国际三大银行卡组织——Europay(欧陆卡，已被万事达收购)、MasterCard(万事达)和Visa(维萨)共同发起制定，是基于CPU IC卡的金融支付标准，目前已成为公认的框架性标准。其目的是在金融IC卡支付系统中建立卡片和终端接口的统一标准，使得在此体系下所有的卡片和终端能够互通互用，并且该技术的采用将大大提高银行卡支付的安全性，减少欺诈行为)。但把磁条银行卡升级为智能IC卡，升级成本高，不仅单张卡片需要升级，而且银行卡处理系统也要更新，巨额的升级成本，使银行举棋不定。另一方面，智能IC卡也不是无懈可击的，目前在使用智能IC卡的欧美地区，银行卡欺诈率为万分之五，远远高于使用磁条卡的中国的万分之二的水平。智能IC卡并不是绝对安全的，信息也能被犯罪分子破解，目前已出现了破解智能IC卡的技术，如：简易功率分析(SPA)，微分能量分析(DPA)等。

[0008] 银行卡安全问题，除了持卡人人为误操作外，多数是由于持卡人的银行卡账号及交易密码被他人窃取所引发的。现有银行卡没有与卡主身份绑定，任何人得到银行卡的账号与交易密码，都可以进行金融交易。因此，银行卡处理系统(自助终端)无法确认持卡人的真实身份，导致了银行卡交易风险。

[0009] 针对银行卡交易风险，业内提出通过智能IC卡实现身份认证的解决方案为：将标识个人身份的信息(数字证书、生物特征信息)存储在IC卡内，辅助以指纹识别、虹膜识别技术，不再以个人密码作为交易的安全认证，以个人的生物特征信息作为密码进行安全认

证。但采用上述解决方案，存在以下问题：

[0010] (1) 把个人生物特征信息作为安全认证的密码，改变银行系统的安全认证方式，需要升级银行内部系统，但需要巨额的升级成本使其致命的不足。

[0011] (2) 基于生物特征作为密码的安全认证，一个比特位的改变就破坏了密码，验证的实施条件比较苛刻。

[0012] (3) 方案的成功实施建立在银行卡是智能 IC 卡的基础上；EMV 迁移是一个缓慢的过程，在 EMV 完成之后才实施上述解决方案，更是困难重重。

发明内容

[0013] 本发明目的在于提供一种以人体生物特征信息实现安全卡与合法所有者之间实现绑定的技术方案，采用在合法所有者人体生物特征信息中嵌入数字水印的手段，解决安全卡被复制或篡改而引起的银行卡盗用的问题。

[0014] 本发明进一步目的在于提供一种安全卡使用者身份验证的认证系统，借助数字水印的鲁棒性和安全性能，提高身份验证的可靠性，增加犯罪分子伪造银行卡的难度。

[0015] 本发明再进一步的目的在于提供一种对现有银行后台系统不需任何改造就能使用上述安全卡的银行服务设备，在现有银行服务设备中加装上述认证系统，即可使用上述安全卡的身份验证功能。

[0016] 为实现上述发明目的，本发明提供一种安全卡，其包括一片状基体和至少一存储该卡信息的存储介质，该安全卡还包括安全卡合法所有者身份认证信息承载介质，所述安全卡合法所有者身份认证信息为经过数字水印加密后的人体生物特征信息。

[0017] 优选地，所述安全卡合法所有者身份认证信息承载介质为 IC 芯片。

[0018] 优选地，所述安全卡合法所有者身份认证信息为嵌入数字水印的人体生物特征影像信息。

[0019] 进一步地，所述安全卡合法所有者身份认证信息承载介质为片状基体表面的印刷层，所述人体生物特征影像保密信息打印或印刷至印刷层上。

[0020] 进一步地，所述人体生物特征影像信息为脸部、指纹、静脉、虹膜中的一种影像或一种以上影像的组合。

[0021] 为了实现本发明的另一目的，本发明提供一种安全卡的认证系统，其包括：

[0022] 一身份认证信息读取单元，用于读取安全卡中包括的人体生物特征信息；

[0023] 一人体生物特征信息采集单元，用于获得该安全卡使用者相应的人体生物特征信息；

[0024] 一存储单元，用于存储安全卡中包括的人体生物特征信息中数字水印的提取算法以及标准数字水印样本；

[0025] 一数字水印提取单元，用于提取安全卡中包括的人体生物特征信息中的数字水印；

[0026] 一匹配对比单元，用于对所述数字水印提取单元提取的数字水印与存储单元中标准数字水印样本进行匹配对比，以及对安全卡中包括的人体生物特征信息与安全卡使用者相应的人体生物特征信息进行匹配对比；以及

[0027] 一结果输出单元，将匹配对比单元得出的匹配对比结果输出。

[0028] 优选地，所述安全卡中包括的人体生物特征信息为嵌入数字水印的人体生物特征影像信息。

[0029] 进一步地，所述身份认证信息读取单元为影像扫描元件。

[0030] 进一步地，所述人体生物特征信息采集单元为人体生物特征影像采集元件。

[0031] 为了实现本发明的第三目的，本发明提供一种金融设备，其包括机壳、人机交互系统、安全卡信息读取装置、纸币处理机芯和控制系统，以及一卡认证系统，其包括：

[0032] 一身份认证信息读取单元，用于获得安全卡中包括的人体生物特征信息；

[0033] 一人体生物特征信息采集单元，用于获得该安全卡使用者相应的人体生物特征信息；

[0034] 一存储单元，用于存储安全卡中包括的人体生物特征信息中数字水印的提取算法以及标准数字水印样本；

[0035] 一数字水印提取单元，用于提取安全卡中包括的人体生物特征信息中的数字水印；

[0036] 一匹配对比单元，用于对所述数字水印提取单元提取的数字水印与存储单元中标准数字水印样本进行匹配对比，以及对安全卡中包括的人体生物特征信息与安全卡使用者相应的人体生物特征信息进行匹配对比；以及

[0037] 一结果输出单元，将匹配对比单元得出的匹配对比结果输出给控制系统。

[0038] 最后本发明还提供一种安全卡的认证方法，其包括如下步骤：

[0039] 步骤一，读取使用中的安全卡内存储的一人体生物特征信息 C_T；

[0040] 步骤二，采集安全卡使用者相应的人体生物特征信息 C'；

[0041] 步骤三，对比该存储于安全卡内的人体生物特征信息 C_T 与该安全卡使用者相应的人体生物特征信息 C'，如果 $\| C' - C_T \| \leqslant J'$ 成立，则执行第四步，否则该安全卡认证失败；以及

[0042] 步骤四，提取该安全卡内存储的人体生物特征信息 C_T 中的数字水印 W'，且将 W' 与标准数字水印 W 相比对，如果 $\| W' - W \| \leqslant J$ 成立，则认证成功，否则该安全卡认证失败。

[0043] 其中，该安全卡认证方法中步骤三是用以确认安全卡使用者相应的人体生物特征信息是否与安全卡内存储的人体生物特征信息相同，在安全卡内人体生物特征信息没有被篡改的前提下，可以确认该安全卡使用者即为该安全卡所有者，从而保证安全卡使用的安全性；但是，不法分子有可能篡改该安全卡内的人体生物特征信息，因此该认证方法还包括步骤四，通过比对数字水印检验该安全卡内存储的人体生物特征信息是否被篡改，保证安全卡的安全使用。

[0044] 综合以上所述，本发明所提供的技术方案与现有技术相比具有如下有点：

[0045] 1、该安全卡采用“银行卡”+“合法所有者身份信息”唯一绑定的解决方案，在保持银行卡原有安全认证方式不改变的前提下，为银行卡增加额外的安全防范措施，使银行和金融自助设备供应商提供的安全防范措施相互独立，以便在日后交易纠纷处理中明确各方责任，提高事后处理效率。

[0046] 2、银行卡合法所有者的生物特征信息具有唯一性，降低了非法用户持卡交易的风险。而且采用数字水印嵌入到银行卡合法所有者的生物特征信息中，借助数字水印的鲁棒性和安全性能，在满足身份验证可靠性的同时，增加犯罪分子伪造或篡改银行卡的难度，主

要体现以下几点：

[0047] (1) 数字水印的鲁棒性给身份信息验证提供较好的容错性，在不降低正确率的同时，兼顾了身份验证的精度。

[0048] (2) 在不知道数字水印的嵌入算法和数字水印样本的前提下，非法分子无法进行银行卡伪造而进行犯罪作案。

[0049] (3) 嵌入生物特征信息的数字水印是不可见的，非法分子无法按照“所见即所得”的模式仿造生物特征信息，增加了不法分子犯罪作案的实施难度。

附图说明

[0050] 图 1 为本发明一较佳实施例提供的一种安全卡示意图；

[0051] 图 2 为本发明另一较佳实施例提供的一种安全卡示意图；

[0052] 图 3 为本发明提供的一种安全卡认证系统组成示意图；

[0053] 图 4 为一种安全银行卡的制作流程图；

[0054] 图 5 为一种安全银行卡使用认证流程图；以及

[0055] 图 6 为本发明提供的一种金融设备构成示意图。

具体实施方式

[0056] 下面所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0057] 参阅图 1，为本发明提供一种安全卡 100，其包括一片状基体 10 和一存储该卡信息的磁条 11，该安全卡还包括安全卡合法所有者身份认证信息承载介质，该信息承载介质为片状基体 10 表面的印刷层 12，所述合法所有者身份认证信息为经过数字水印加密后的正面人脸影像信息 121，人脸影像信息 121 经过高精度打印设备印刷至片状基体 10 表面的印刷层 12 上。其中存储该卡信息的磁条 11 与印刷层 12 可以在片状基体 10 的一侧或不同侧均可以达到本发明的目的。

[0058] 图 2 示出了本发明的又一安全卡 100’，其包括一片状基体 10 和一存储该卡信息的 IC 芯片 13，该安全卡还包括安全卡合法所有者身份认证信息承载介质，该信息承载介质为片状基体 10 表面的印刷层 12，所述合法所有者身份认证信息为经过数字水印加密后的人体指纹影像信息 121’，人体指纹影像信息 121’ 经过高精度打印设备印刷至片状基体 10 表面的印刷层 12 上。同样该存储该卡信息的 IC 芯片 13 与印刷层 12 可以在片状基体 10 的一侧或不同侧均可以达到本发明的目的。另外由于 IC 芯片 13 具有较大数据的存储能力，因此人体指纹影像信息 121’ 还可以直接存储于 IC 芯片 13 内，方便后续身份验证时被提取。

[0059] 上述图 1 和图 2 所示的正面人脸影像和指纹影像仅仅是一部分可以用作合法所有者身份认证信息，除此之外还可以采用静脉、虹膜等人体生物特征影像作为合法所有者身份认证信息。而且人体生物特征非影像信息与 IC 芯片类信息承载介质的配合也可以作为合法所有者身份认证信息在安全卡中使用，当然如此需要配合小巧而自动完成采集非影像人体生物特征的设备，比如人体汗液分析仪等不需要破坏人体即可得到具有唯一性的人体生物特征信息采集仪。

[0060] 参阅图 3，本发明所提供的一种安全卡认证系统 101，其包括：一身份认证信息读取单元 110，用于获得安全卡中包括的人体生物特征信息；一人体生物特征信息采集单元 111，用于获得该安全卡使用者相应的人体生物特征信息；一存储单元 112，用于存储安全卡中包括的人体生物特征信息中数字水印的提取算法以及标准数字水印样本；一数字水印提取单元 113，用于提取所述安全卡中包括的人体生物特征信息中的数字水印；一匹配对比单元 114，用于对所述数字水印提取单元提取的数字水印与存储单元中标准数字水印样本进行匹配对比，以及对安全卡中包括的人体生物特征信息与安全卡使用者相应的人体生物特征信息进行匹配对比；一结果输出单元 115，将匹配对比单元得出的匹配对比结果输出。

[0061] 具体的针对图 1 所示安全卡类的认证系统 101，由于其身份认证信息为印刷在卡片状基体 10 表面印刷层 12 上的经过数字水印加密后的正面人脸影像信息 121，认证系统 101 中相应的身份认证信息读取单元为图像扫描元件，且人体生物特征信息采集单元 111 为采集人脸图像的摄相机元件。

[0062] 下面结合图 1 和图 4 对本发明所述安全卡的制作和认证步骤做一举例阐述，根据现有的银行系统，安全卡的制作步骤为：

[0063] S1 银行卡申办人申领银行卡时；

[0064] S2 由银行柜台人员采集申领人的正面人脸图像 C；

[0065] S3 并根据保密的数字水印嵌入算法 F 将标准数字水印样本 W 嵌入到正面人脸图像 C 中得到带水印正面人脸图像 C_F；

[0066] S4 将带水印正面人脸图像 C_F 打印至银行卡表面完成制卡，如图 4 所示。

[0067] 对于图 1 所示类型安全卡，数字水印算法采用变换域算法：如，基于 DCT 变换、基于 DWT 变换、基于 DFT 变换、基于 Contourlet 域的变换等。基于变换域的水印算法，对原图质量的影响小，较符合人的视觉模型，而且算法的水印容量大，加密空间大，还可以附加密钥，而且密钥算法的设计几乎不受太大的限制，算法本身技术含量高，难复制。由于嵌入数字水印的人脸图像与原始图像在肉眼视觉上几乎一样，且数字水印是肉眼看不到的，将带有数字水印的人脸图像印刷至银行卡表面使得银行卡与所有者的一一对应关系显性化，有利于银行卡识别。

[0068] 下面结合图 3 和图 5 对本发明所述认证步骤做一阐述，针对图 1 所示银行卡在使用过程中的认证步骤为：

[0069] S10，身份认证信息读取单元 110 即图像扫描元件扫描银行卡 100 表面印刷层 12 上的正面人脸影像 $121C_T$；

[0070] S11，数字水印提取单元 113 依据存储单元 112 中的数字水印提取算法对正面人脸影像 $121C_T$ 的数字信息完成数字水印提取，得到验证数字水印 W'；

[0071] S12，匹配对比单元 114 对验证数字水印 W' 和存储单元中的标准数字水印样本 W 进行匹配对比，即 $\| W-W' \| \leq J$ 是否成立，其中 J 为事先设定的阈值；如果成立，则进行 S13 步骤，如果不成立则认证失败，结束操作；

[0072] S13，人体生物特征信息采集单元 111，即摄相机元件，采集使用者的正面人脸图像 C'；

[0073] S14 匹配对比单元 114 对正面人脸图像 C' 和 C_T 进行人脸识别匹配对比，即判

断 $\| C_T - C' \| \leq J'$ 是否成立，其中 J' 为事先设定的阈值，如果成立，则进行 S15 步骤，如果不成立则认证失败，结束操作；

[0074] S15 完成后续交易操作。

[0075] 上述认证步骤并不是唯一步骤顺序，其中步骤 S12 和 S14 可以前后对调，对整体的认证结果没有任何影响，同样可以达到本发明的目的。

[0076] 其中，该步骤 S14 是用来确认安全卡使用者相应的人体生物特征信息 C' 是否与银行卡 100 表面印刷层 12 上的正面人脸影像 $121C_T$ 相同，在 C_T 没有被篡改的前提下，可以确认该安全卡使用者即为该安全卡所有者，从而保证安全卡使用的安全性；但是，不法分子有可能篡改该安全卡内的人体生物特征信息，因此该认证方法还包括步骤 S12，通过比对数字水印 W 和 W'，以检验 C_T 是否被篡改，保证安全卡的安全使用。

[0077] 另外根据安全卡所采用人体特征信息类型和信息承载介质的不同，安全卡认证信息的采集也有所不同，其属于公知技术手段，本发明不再赘述。

[0078] 下面结合附图 6 进一步说明本发明所提供的一种金融设备 120，其包括机壳 121、人机交互系统 122、安全卡信息读取装置 123、纸币处理机芯 124 和控制系统 125，以及一卡认证系统 126，其卡认证系统 126 包括如 3 所示组件，即，

[0079] 一身份认证信息读取单元 110，用于获得安全卡中包括的人体生物特征信息；

[0080] 一人体生物特征信息采集单元 111，用于获得该安全卡使用者相应的人体生物特征信息；

[0081] 一存储单元 112，用于存储安全卡中包括的人体生物特征信息中数字水印的提取算法以及标准数字水印样本；

[0082] 一数字水印提取单元 113，用于提取安全卡中包括的人体生物特征信息中的数字水印；

[0083] 一匹配对比单元 114，用于对所述数字水印提取单元提取的数字水印与存储单元中标准数字水印样本进行匹配对比，以及对安全卡中包括的人体生物特征信息与安全卡使用者相应的人体生物特征信息进行匹配对比；以及

[0084] 一结果输出单元 115，将匹配对比单元得出的匹配对比结果输出给控制系统 125。

[0085] 本发明所提供的金融自助服务设备时在现有自助服务设备中添加一卡认证系统即可实现本发明的目的，故该金融自助服务设备可以兼容非安全卡型银行卡，即传统的密码型银行卡通过兼容磁性卡的读卡器和密码键盘密码输入认证即可完成传统的银行卡交易操作。而对于安全卡型银行卡，自助服务设备将启动卡安全认证系统对安全卡绑定的合法所有者人体生物特征信息的认证功能，根据认证结果进行银行卡交易操作，以满足银行卡复制或篡改而进行的非法交易操作。当然为了实现兼顾传统卡和安全卡的目的，在提供的金融自助服务设备还需能够识别使用者所使用卡的类型，即金融自助设备具有甄别使用卡为“传统卡”类型还是“安全认证卡”类型的功能，该功能的实现可以采用银行卡统一标识或人工选择来完成。

[0086] 具体的金融自助服务设备完成银行卡的交易操作为习知流程，安全卡交易过程中在习知流程中结合本发明图 5 所示的卡认证流程即可以清晰地知悉本发明所提供的金融自助服务设备的使用操作流程，所以本发明不在此进行赘述。

[0087] 以上所揭露的仅为本发明一种较佳实施例而已，当然不能以此来限定本发明之权

利范围，因此依本发明申请专利范围所作的等同变化，仍属本发明所涵盖的范围。

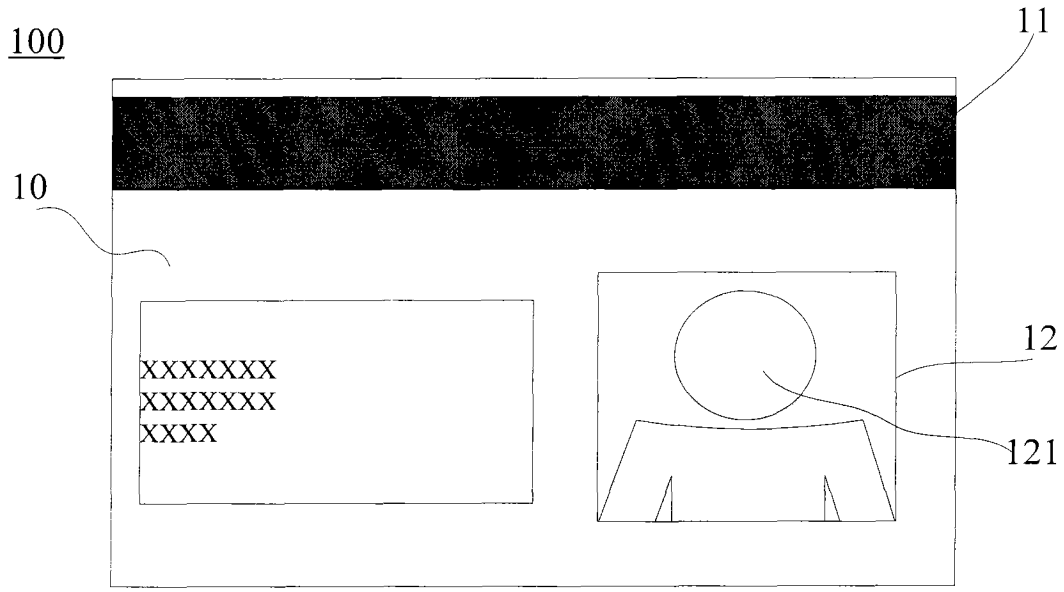

100
11
10
XXXXXXX
XXXXXXX
XXXX
12
121

图 1

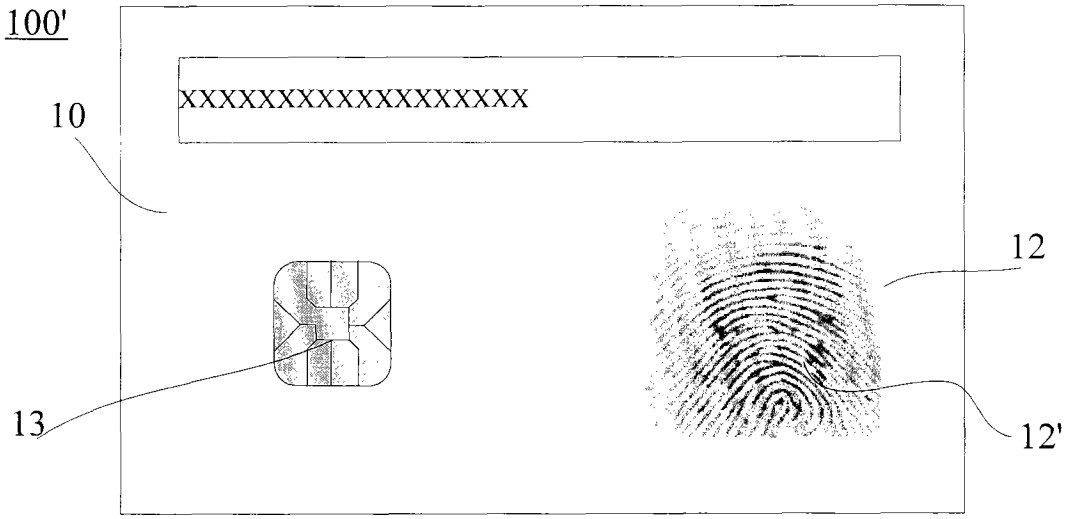

100'
XXXXXXXXXXXXXXXXXXX
10
12
13
12'

图 2

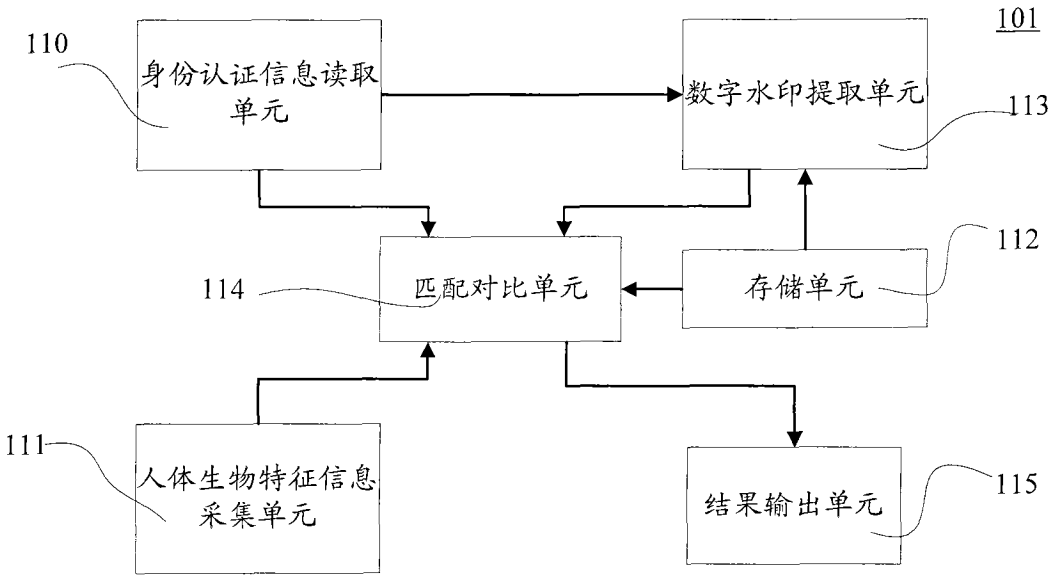

101
110
身份认证信息读取单元
数字水印提取单元
113
112
114
匹配对比单元
存储单元
111
人体生物特征信息采集单元
结果输出单元
115

图 3

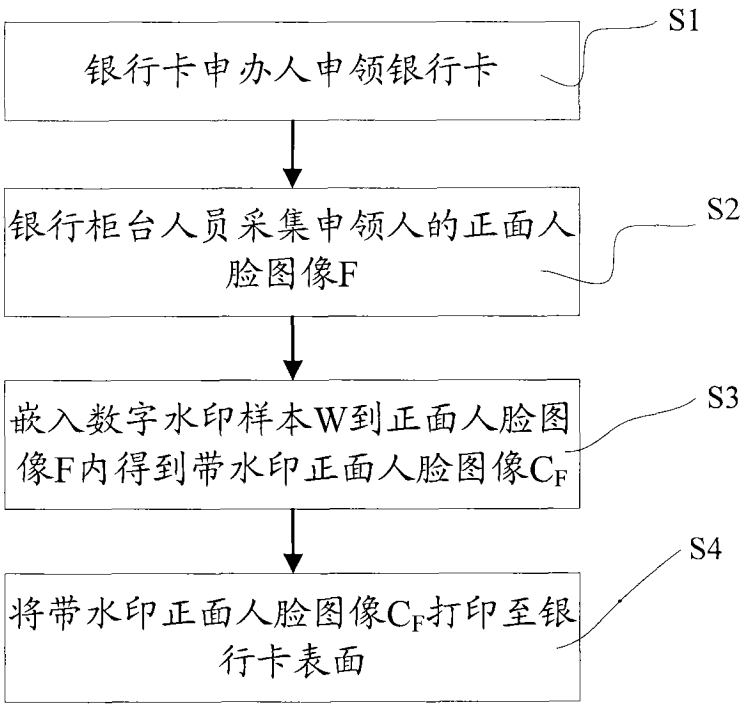

S1
银行卡申办人申领银行卡
S2
银行柜台人员采集申领人的正面人脸图像F
S3
嵌入数字水印样本W到正面人脸图像F内得到带水印正面人脸图像C_F
S4
将带水印正面人脸图像C_F打印至银行卡表面

图 4

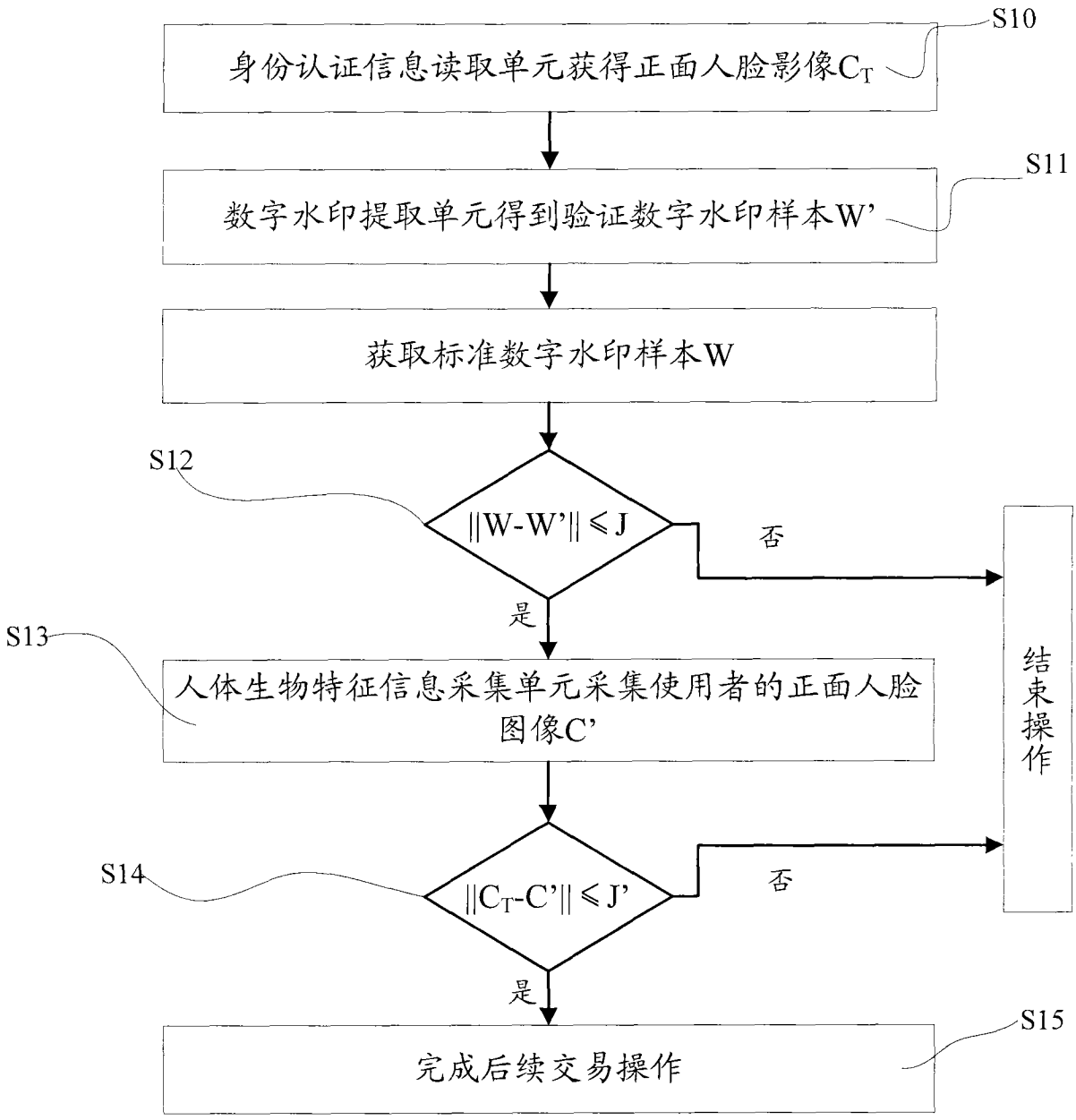

S10
身份认证信息读取单元获得正面人脸影像C_T
S11
数字水印提取单元得到验证数字水印样本W'
获取标准数字水印样本W
S12
$\|W-W'\| \leqslant J$
否
是
结束操作
S13
人体生物特征信息采集单元采集使用者的正面人脸图像C'
S14
$\|C_T-C'\| \leqslant J'$
否
是
S15
完成后续交易操作

图 5

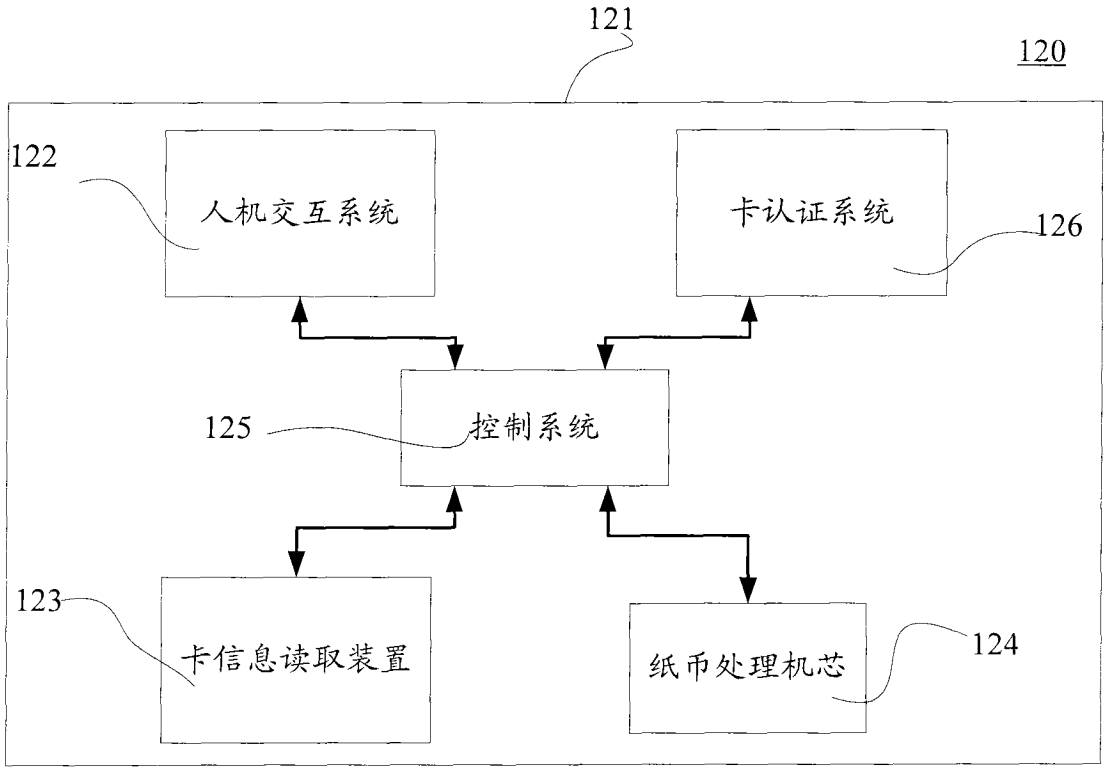


图 6