



(12)发明专利申请

(10)申请公布号 CN 111460471 A

(43)申请公布日 2020.07.28

(21)申请号 202010190735.0

(22)申请日 2020.03.18

(71)申请人 北京兆维自服装备技术有限公司
地址 100000 北京市大兴区经济技术开发区隆庆街9号

(72)发明人 肖亮 刘亚宁 张伟

(74)专利代理机构 北京轻创知识产权代理有限公司 11212
代理人 徐琪琦

(51)Int.Cl.

G06F 21/60(2013.01)

G06F 21/64(2013.01)

G06K 17/00(2006.01)

权利要求书3页 说明书7页 附图1页

(54)发明名称

一种自助服务数据处理装置及方法

(57)摘要

本发明提供一种自助服务数据处理装置及方法,装置包括:图形信息读取模块,主控模块和解加密处理模块,图形信息读取模块用于从电子设备中读取得到待识别图形信息;主控模块用于对所述待识别图形信息的识别得到业务信息;解加密数据处理模块用于通过接触式读卡器或非接触式读卡器从待识别信息卡中读取得到待加密信息,并根据预先装载的SM2国密算法对待加密信息的加密得到加密信息,将其发送主控模块。本发明防止数据在传输过程中遭到篡改,保证了数据传输的机密性和数据通信的安全性,同时摆脱了对国外技术和产品过度依赖,为建设安全自主可控的网络安全环境提出了有效的解决方案。



1. 一种自助服务数据处理装置,其特征在于,包括:图形信息读取模块,主控模块和解加密处理模块;

所述图形信息读取模块,用于从电子设备中读取得到待识别图形信息;

所述主控模块,用于对所述待识别图形信息进行识别,得到业务信息;

所述解加密数据处理模块,用于通过接触式读卡器或非接触式读卡器从待识别信息卡中读取得到待加密信息,并根据预先装载的SM2国密算法对所述待加密信息进行加密,得到加密信息,将所述加密信息发送所述主控模块;

所述主控模块,还用于对所述加密信息进行识别,得到待解密信息,并根据预先装载的SM2国密算法对所述待解密信息进行解密,得到解密信息。

2. 根据权利要求1所述的自助服务数据处理装置,其特征在于,所述待识别图形信息包括磁条卡待识别信息、二维码待识别信息和热敏打印待识别信息,所述图形信息读取模块包括磁条卡数据获得单元、二维码数据获得单元和热敏打印数据获得单元;

所述磁条卡数据获得单元,用于从待识别磁条卡中获得所述磁条卡待识别信息;

所述二维码数据获得单元,用于从待识别二维码中获得所述二维码待识别信息;

所述热敏打印数据获得单元,用于从待识别热敏打印机中获得所述热敏打印待识别信息。

3. 根据权利要求1所述的自助服务数据处理装置,其特征在于,还包括密码键盘信息读取模块,所述密码键盘信息读取模块用于从密码键盘中获得键盘密码待识别信息;

所述主控模块,还用于对所述键盘密码待识别信息进行识别,得到键盘密码信息。

4. 根据权利要求1所述的自助服务数据处理装置,其特征在于,所述解加密数据处理模块包括数据处理单元、安全算法单元、待识别信息卡获取单元和数据传输单元;

所述待识别信息卡获取单元,用于从待识别信息卡中读取得到待加密信息;

所述安全算法单元,用于根据预先装载的SM2国密算法对所述待加密信息进行加密,得到加密待识别信息;

所述数据处理单元,用于对所述加密待识别信息进行识别,得到加密信息;

所述数据传输单元,用于将所述加密信息发送至所述主控模块。

5. 根据权利要求3或4所述的自助服务数据处理装置,其特征在于,还包括磁条码获取模块,所述磁条码获取模块用于从待识别的磁条码中读取得到磁条码待加密信息;

所述安全算法单元,还用于根据预先装载的SM2国密算法对所述磁条码待加密信息进行加密,得到磁条码待识别信息;

所述数据处理单元,还用于对所述磁条码待识别信息进行识别,得到磁条码加密信息;

所述数据传输单元,还用于将所述磁条码加密信息发送至所述主控模块;

所述主控模块,还用于对所述磁条码加密信息进行识别,得到磁条码待解密信息,并根据预先装载的SM2国密算法对所述磁条码待解密信息进行解密,得到磁条码解密信息。

6. 根据权利要求5所述的自助服务数据处理装置,其特征在于,所述数据处理单元还用于生成待加密信息读取指令;

所述安全算法单元,还用于根据预先装载的SM2国密算法对所述待加密信息读取指令进行加密,得到待加密信息读取指令;

所述待识别信息卡获取单元,还用于接收所述待加密信息读取指令;

所述安全算法单元,还用于根据预先装载的SM2国密算法对所述待加密信息读取指令进行解密,得到信息读取指令;

所述待识别信息卡获取单元,还用于根据所述信息读取指令对所述待识别信息卡进行读取,得到待加密信息;

所述数据处理单元还用于生成磁条码待加密信息读取指令;

所述安全算法单元,还用于根据预先装载的SM2国密算法对所述磁条码待加密信息读取指令进行加密,得到磁条码待加密信息读取指令;

所述磁条码获取模块,还用于接收所述磁条码待加密信息读取指令;

所述安全算法单元,还用于根据预先装载的SM2国密算法对所述磁条码待加密信息读取指令进行解密,得到磁条码信息读取指令;

所述磁条码获取模块,还用于根据所述磁条码信息读取指令对所述待识别的磁条码进行读取,得到磁条码待加密信息。

7. 根据权利要求6所述的自助服务数据处理装置,其特征在于,所述待加密信息包括接触卡数据信息和非接触卡数据信息,所述信息读取指令包括接触卡信息获取指令和非接触卡信息获取指令,所述待识别信息卡获取单元包括接触卡数据获得单元和非接触卡数据获得单元;

所述接触卡数据获得单元,用于根据所述接触卡信息获取指令,从待识别接触卡中获得接触卡数据信息;

所述非接触卡数据获得单元,用于根据所述非接触卡信息获取指令,从待识别非接触卡中获得非接触卡数据信息。

8. 根据权利要求5所述的自助服务数据处理装置,其特征在于,还包括二代证件安全模块,所述磁条码待加密信息包括二代证件数据信息;

所述二代证件安全模块,用于从待识别二代证件磁条码中获得二代证件原始加密数据信息,并对所述二代证件原始加密数据信息进行解密,得到所述二代证件数据信息。

9. 根据权利要求1-8任一项所述的自助服务数据处理装置,其特征在于,还包括电源模块、显示模块、摄像模块和网络接口模块;

所述电源模块,用于为所述图形信息读取模块,所述主控模块和所述解加密处理模块提供电源;

所述显示模块,用于将所述业务信息、所述解密信息、所述键盘密码信息和所述磁条码解密信息分别显示在对应的密码框内;

所述摄像模块,用于对用户进行拍照,得到用户照片信息;

所述主控模块,还用于对所述用户照片信息进行存储;

所述网络接口模块,用于与预设的服务器进行信息交互。

10. 一种自助服务数据处理方法,其特征在于,包括如下步骤:

从电子设备中读取得到待识别图形信息;

对所述待识别图形信息进行识别,得到业务信息;

通过接触式读卡器或非接触式读卡器从待识别信息卡中读取得到待加密信息,并根据预先装载的SM2国密算法对所述待加密信息进行加密,得到加密信息,将所述加密信息发送所述主控模块;

对所述加密信息进行识别,得到待解密信息,并根据预先装载的SM2国密算法对所述待解密信息进行解密,得到解密信息。

一种自助服务数据处理装置及方法

技术领域

[0001] 本发明主要涉及金融信息技术领域,具体涉及一种自助服务数据处理装置及方法。

背景技术

[0002] 目前在银行、电信、医疗等营业场所,自助服务设备已广泛使用,此类设备,因方便部署,提高效率,逐步在人们的日常生活中扮演重要的角色。国内使用的自助设备绝大多数都是采用Intel x86架构CPU主板方案,各种设备整体自主国产化程度还偏低,在人民群众越来越依靠此类智能自助设备的情况下,对我们国民经济也同时带来某种程度的不便和风险,而且现有Windows操作系统或国产操作系统工控主机与智能卡读卡模块的通信数据采用明文方式传输,业务敏感数据易被截取、破解,数据安全性得不到保障。

发明内容

[0003] 本发明所要解决的技术问题是针对现有技术的不足,提供一种自助服务数据处理装置及方法。

[0004] 本发明解决上述技术问题的技术方案如下:一种自助服务数据处理装置,包括:

[0005] 图形信息读取模块,主控模块和解加密处理模块;

[0006] 所述图形信息读取模块,用于从电子设备中读取得到待识别图形信息;

[0007] 所述主控模块,用于对所述待识别图形信息进行识别,得到业务信息;

[0008] 所述解加密数据处理模块,用于通过接触式读卡器或非接触式读卡器从待识别信息卡中读取得到待加密信息,并根据预先装载的SM2国密算法对所述待加密信息进行加密,得到加密信息,将所述加密信息发送所述主控模块;

[0009] 所述主控模块,还用于对所述加密信息进行识别,得到待解密信息,并根据预先装载的SM2国密算法对所述待解密信息进行解密,得到解密信息。

[0010] 本发明解决上述技术问题的另一技术方案如下:一种自助服务数据处理方法,包括如下步骤:

[0011] 从电子设备中读取得到待识别图形信息;

[0012] 对所述待识别图形信息进行识别,得到业务信息;

[0013] 通过接触式读卡器或非接触式读卡器从待识别信息卡中读取得到待加密信息,并根据预先装载的SM2国密算法对所述待加密信息进行加密,得到加密信息,将所述加密信息发送所述主控模块;

[0014] 对所述加密信息进行识别,得到待解密信息,并根据预先装载的SM2国密算法对所述待解密信息进行解密,得到解密信息。

[0015] 本发明的有益效果是:通过得到对待识别图形信息的识别得到业务信息,同时根据预先装载的SM2国密算法对待加密信息的加密得到加密信息,将加密信息发送主控模块,主控模块对加密信息的识别得到待解密信息,并根据预先装载的SM2国密算法对待解密信

息的解密得到解密信息,防止数据在传输过程中遭到篡改,保证了数据传输的机密性和数据通信的安全性,同时为建设安全自主可控的网络安全环境提出了有效的解决方案。

附图说明

[0016] 图1为本发明一实施例提供的自助服务数据处理装置的模块框图;

[0017] 图2为本发明一实施例提供的自助服务数据处理方法的流程示意图。

具体实施方式

[0018] 以下结合附图对本发明的原理和特征进行描述,所举实例只用于解释本发明,并非用于限定本发明的范围。

[0019] 图1为本发明一实施例提供的自助服务数据处理的模块框图。

[0020] 如图1所示,一种自助服务数据处理装置,包括:

[0021] 图形信息读取模块,主控模块和解加密处理模块;

[0022] 所述图形信息读取模块,用于从电子设备中读取得到待识别图形信息;

[0023] 所述主控模块,用于对所述待识别图形信息进行识别,得到业务信息;

[0024] 所述解加密数据处理模块,用于通过接触式读卡器或非接触式读卡器从待识别信息卡中读取得到待加密信息,并根据预先装载的SM2国密算法对所述待加密信息进行加密,得到加密信息,将所述加密信息发送所述主控模块;

[0025] 所述主控模块,还用于对所述加密信息进行识别,得到待解密信息,并根据预先装载的SM2国密算法对所述待解密信息进行解密,得到解密信息。

[0026] 优选地,所述主控模块可以为板载龙芯3A-3000型号的CPU主板搭载Loongnix操作系统。

[0027] 具体地,所述解加密数据处理模块与所述主控模块均可以采用SM2或SM4国密算法对所述待加密信息进行加密传输。

[0028] 应理解地,所述主控模块与所述解加密数据处理模块通信数据采用SM2国密算进行加解密传输;所述解加密数据处理模块使用所述主控模块内置安全模块的公钥加密通信数据发送给所述主控模块,而所述主控模块的安全模块使用对应的私钥对所述解加密数据处理模块发送的加密数据进行解密。

[0029] 具体地,所述解加密数据处理模块与所述主控模块之间的数据通信采用明文或密文的方式传输,敏感数据访问采用密文方式,所述解加密数据处理模块接收敏感数据加解密指令,对敏感数据进行加解密处理。

[0030] 应理解地,所述解加密数据处理模块支持符合ISO7816规范T=0和T=1协议的接触式智能CPU卡片的读写和支持符合ISO14443规范Type A、TypeB协议的非接触式智能CPU卡片的读写。

[0031] 具体地,所述解加密数据处理模块为采用国产芯片自助研发设计,通过自定义通讯协议完成所述解加密数据处理模块和所述主控模块的通信。

[0032] 上述实施例中,通过得到对待识别图形信息的识别得到业务信息,同时根据预先装载的SM2国密算法对待加密信息的加密得到加密信息,将加密信息发送主控模块,主控模块对加密信息的识别得到待解密信息,并根据预先装载的SM2国密算法对待解密信息的解

密得到解密信息,防止数据在传输过程中遭到篡改,保证了数据传输的机密性和数据通信的安全性,同时为建设安全自主可控的网络安全环境提出了有效的解决方案。

[0033] 可选地,作为本发明的一个实施例,所述待识别图形信息包括磁条卡待识别信息、二维码待识别信息和热敏打印待识别信息,所述图形信息读取模块包括磁条卡数据获得单元、二维码数据获得单元和热敏打印数据获得单元;

[0034] 所述磁条卡数据获得单元,用于从待识别磁条卡中获得所述磁条卡待识别信息;

[0035] 所述二维码数据获得单元,用于从待识别二维码中获得所述二维码待识别信息;

[0036] 所述热敏打印数据获得单元,用于从待识别热敏打印机中获得所述热敏打印待识别信息。

[0037] 上述实施例中,分别从磁条卡、二维码和热敏打印机中获得磁条卡待识别信息、二维码待识别信息和热敏打印待识别信息,能够读取多种类型的数据信息,实现了装置的多样性,为保证各类型数据传输和数据通信提供了基础。

[0038] 可选地,作为本发明的一个实施例,还包括密码键盘信息读取模块,所述密码键盘信息读取模块用于从密码键盘中获得键盘密码待识别信息;

[0039] 所述主控模块,还用于对所述键盘密码待识别信息进行识别,得到键盘密码信息。

[0040] 上述实施例中,通过对键盘密码待识别信息的识别得到键盘密码信息,能够对于不同类型的数据信息进行不同的处理,体现了智能化的处理方式。

[0041] 可选地,作为本发明的一个实施例,所述解加密数据处理模块包括数据处理单元、安全算法单元、待识别信息卡获取单元和数据传输单元;

[0042] 所述待识别信息卡获取单元,用于从待识别信息卡中读取得到待加密信息;

[0043] 所述安全算法单元,用于根据预先装载的SM2国密算法对所述待加密信息进行加密,得到加密待识别信息;

[0044] 所述数据处理单元,用于对所述加密待识别信息进行识别,得到加密信息;

[0045] 所述数据传输单元,用于将所述加密信息发送至所述主控模块。

[0046] 优选地,所述数据处理单元可以为GD32F103VCT6主控芯片,所述安全算法单元可以为CIU98320B安全算法芯片。

[0047] 应理解地,所述安全算法单元与所述数据处理单元的信息交互采用USART方式,所述数据传输单元与所述数据处理单元的信息交互采用USB或RS232方式

[0048] 具体地,所述数据传输单元提供了USB或USART两种形式使得与所述主控模块的通信更加灵活。

[0049] 应理解地,GD32F103VCT6主控芯片是一款来自兆易国产ARM架构Cortex M3内核的32位MCU,具有性能好、速度快、外设资源丰富等特点;CIU98320B安全算法芯片是一款基于ARM内核的32位控制器安全芯片,该硬件算法协处理器,用于提供性能优异的DES/3DES、RSA、ECC、SM2、SM1/SM3/SM4、SHA-1/SHA-256/SHA-512安全算法和真随机数发生器。

[0050] 具体地,接触式或非接触式CPU卡片与所述数据处理单元交互返回所述数据处理单元的数据的加解密传输方式。

[0051] 上述实施例中,根据预先装载的SM2国密算法对待加密信息的加密得到加密待识别信息,对加密待识别信息的识别得到加密信息,防止数据在传输过程中遭到篡改,保证了数据传输的机密性和数据通信的安全性,同时采用国产芯片设计摆脱了对国外技术和产品

过度依赖,为建设安全自主可控的网络安全环境提出了有效的解决方案。

[0052] 可选地,作为本发明的一个实施例,还包括磁条码获取模块,所述磁条码获取模块用于从待识别的磁条码中读取得到磁条码待加密信息;

[0053] 所述安全算法单元,还用于根据预先装载的SM2国密算法对所述磁条码待加密信息进行加密,得到磁条码待识别信息;

[0054] 所述数据处理单元,还用于对所述磁条码待识别信息进行识别,得到磁条码加密信息;

[0055] 所述数据传输单元,还用于将所述磁条码加密信息发送至所述主控模块;

[0056] 所述主控模块,还用于对所述磁条码加密信息进行识别,得到磁条码待解密信息,并根据预先装载的SM2国密算法对所述磁条码待解密信息进行解密,得到磁条码解密信息。

[0057] 优选地,所述磁条码获取模块可以为PA1100磁条解码芯片。

[0058] 应理解地,PA1100磁条解码芯片支持ISO7811标准,支持正反向的磁条卡刷卡,支持单、双、三轨磁条卡解码。

[0059] 具体地,所述磁条码获取模块与所述数据处理单元的信息交互采用12C方式。

[0060] 上述实施例中,根据预先装载的SM2国密算法对磁条码待加密信息的加密得到磁条码待识别信息,对所述磁条码待识别信息的识别得到磁条码加密信息,并将磁条码加密信息发送至主控模块,主控模块对磁条码加密信息的识别得到磁条码待解密信息,并根据预先装载的SM2国密算法对磁条码待解密信息的解密得到磁条码解密信息,能够对于不同类型的数据信息进行不同的处理,体现了智能化的处理方式,同时防止数据在传输过程中遭到篡改,保证了数据传输的机密性和数据通信的安全性,采用国产芯片设计摆脱了对国外技术和产品过度依赖。

[0061] 可选地,作为本发明的一个实施例,所述数据处理单元还用于生成待加密信息读取指令;

[0062] 所述安全算法单元,还用于根据预先装载的SM2国密算法对所述待加密信息读取指令进行加密,得到待加密信息读取指令;

[0063] 所述待识别信息卡获取单元,还用于接收所述待加密信息读取指令;

[0064] 所述安全算法单元,还用于根据预先装载的SM2国密算法对所述待加密信息读取指令进行解密,得到信息读取指令;

[0065] 所述待识别信息卡获取单元,还用于根据所述信息读取指令对所述待识别信息卡进行读取,得到待加密信息;

[0066] 所述数据处理单元还用于生成磁条码待加密信息读取指令;

[0067] 所述安全算法单元,还用于根据预先装载的SM2国密算法对所述磁条码待加密信息读取指令进行加密,得到磁条码待加密信息读取指令;

[0068] 所述磁条码获取模块,还用于接收所述磁条码待加密信息读取指令;

[0069] 所述安全算法单元,还用于根据预先装载的SM2国密算法对所述磁条码待加密信息读取指令进行解密,得到磁条码信息读取指令;

[0070] 所述磁条码获取模块,还用于根据所述磁条码信息读取指令对所述待识别的磁条码进行读取,得到磁条码待加密信息。

[0071] 应理解地,所述数据处理单元分别与所述待识别信息卡获取单元和所述磁条码获

取模块的通信数据可以先进行SM2国密算法加密再传输。

[0072] 上述实施例中,生成待加密信息读取指令,根据预先装载的SM2国密算法对待加密信息读取指令的加密得到待加密信息读取指令,根据预先装载的SM2国密算法对待加密信息读取指令的解密得到信息读取指令,根据信息读取指令对待识别信息卡的读取得到待加密信息,同时生成磁条码待加密信息读取指令,根据预先装载的SM2国密算法对磁条码待加密信息读取指令的加密得到磁条码待加密信息读取指令,根据预先装载的SM2国密算法对磁条码待加密信息读取指令的解密得到磁条码信息读取指令,根据磁条码信息读取指令对待识别的磁条码的读取得到磁条码待加密信息,防止数据在传输过程中遭到篡改,进一步地保证了数据传输的机密性和数据通信的安全性。

[0073] 可选地,作为本发明的一个实施例,所述待加密信息包括接触卡数据信息和非接触卡数据信息,所述信息读取指令包括接触卡信息获取指令和非接触卡信息获取指令,所述待识别信息卡获取单元包括接触卡数据获得单元和非接触卡数据获得单元;

[0074] 所述接触卡数据获得单元,用于根据所述接触卡信息获取指令,从待识别接触卡中获得接触卡数据信息;

[0075] 所述非接触卡数据获得单元,用于根据所述非接触卡信息获取指令,从待识别非接触卡中获得非接触卡数据信息。

[0076] 优选地,所述接触卡数据获得单元可以为AU9541接触卡芯片,所述非接触卡数据获得单元可以为THM3070射频芯片。

[0077] 应理解地,AU9541接触卡芯片支持符合ISO7816规范T=0和T=1协议的接触式智能CPU卡片的操作;THM3070射频芯片支持符合ISO14443规范Type A/TypeB协议CPU智能卡操作,通过了EMV Level1检测认证。

[0078] 具体地,所述接触卡数据获得单元与所述数据处理单元的信息交互采用USART方式,所述非接触卡数据获得单元与所述数据处理单元的信息交互采用SPI方式。

[0079] 上述实施例中,分别从接触卡和非接触卡中获得接触卡数据信息和非接触卡数据信息,能够针对贵重、易窃取的数据采用不同方式进行获取,防止了数据在传输过程中遭到篡改,保证了数据传输的机密性和数据通信的安全性,同时采用国产芯片设计摆脱了对国外技术和产品过度依赖,为建设安全自主可控的网络安全环境提出了有效的解决方案。

[0080] 可选地,作为本发明的一个实施例,还包括二代证件安全模块,所述磁条码待加密信息包括二代证件数据信息;

[0081] 所述二代证件安全模块,用于从待识别二代证件磁条码中获得二代证件原始加密数据信息,并对所述二代证件原始加密数据信息进行解密,得到所述二代证件数据信息。

[0082] 应理解地,所述二代证件包括居民二/三代身份证、港澳台居住证和外国人永久居住证。

[0083] 具体地,读取用户身份证信息时,所述二代证件安全模块读取未加密的身份证文字、图片及指纹信息,然后将未加密的信息送至所述安全算法单元;所述安全算法单元通过SM2加密算法进行数据加密;加密后的数据通回传至所述数据处理单元;通过USB接口或者USART接口送至PC端。

[0084] 具体地,所述二代证件安全模块与所述数据处理单元的信息交互采用USART方式。

[0085] 上述实施例中,通过并对二代证件原始加密数据信息的解密得到二代证件数据信

息,能够针对性的获得正确的数据信息,以便对数据信息进行加密操作,防止了数据在传输过程中遭到篡改,保证了数据传输的机密性和数据通信的安全性,同时为建设安全自主可控的网络安全环境提出了有效的解决方案。

[0086] 可选地,作为本发明的一个实施例,还包括电源模块、显示模块、摄像模块和网络接口模块;

[0087] 所述电源模块,用于为所述图形信息读取模块,所述主控模块和所述解加密处理模块提供电源;

[0088] 所述显示模块,用于将所述业务信息、所述解密信息、所述键盘密码信息和所述磁条码解密信息分别显示在对应的密码框内;

[0089] 所述摄像模块,用于对用户进行拍照,得到用户照片信息;

[0090] 所述主控模块,还用于对所述用户照片信息进行存储;

[0091] 所述网络接口模块,用于与预设的服务器进行信息交互。

[0092] 可选地,作为本发明的一个实施例,所述摄像模块具体用于:

[0093] 对用户的脸部进行识别。

[0094] 优选地,所述摄像模块可以为人脸识别摄像头。

[0095] 上述实施例中,对设备提供电源,同时将业务信息、解密信息、键盘密码信息和磁条码解密信息分别显示在对应的密码框内并对用户照片信息进行存储以及与预设的服务器进行信息交互,为防止被盗用提供保障,同时可以实现与银行、电信、医疗等机构的网络进行数据共享。

[0096] 图2为本发明一实施例提供的自助服务数据处理的流程示意图。

[0097] 可选地,作为本发明的另一个实施例,如图2所示,一种自助服务数据处理方法,包括如下步骤:

[0098] 从电子设备中读取得到待识别图形信息;

[0099] 对所述待识别图形信息进行识别,得到业务信息;

[0100] 通过接触式读卡器或非接触式读卡器从待识别信息卡中读取得到待加密信息,并根据预先装载的SM2国密算法对所述待加密信息进行加密,得到加密信息,将所述加密信息发送所述主控模块;

[0101] 对所述加密信息进行识别,得到待解密信息,并根据预先装载的SM2国密算法对所述待解密信息进行解密,得到解密信息。

[0102] 所属领域的技术人员可以清楚地了解到,为了描述的方便和简洁,上述描述的装置和单元的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0103] 在本申请所提供的几个实施例中,应该理解到,所揭露的装置和方法,可以通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如,单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。

[0104] 作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本发明实施例方案的目的。

[0105] 另外,在本发明各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以是两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0106] 集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用,可以存储在一个计算机可读取存储介质中。用于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分,或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备)执行本发明各个实施例方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0107] 以上,仅为本发明的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到各种等效的修改或替换,这些修改或替换都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应以权利要求的保护范围为准。



图1



图2