

[19] 中华人民共和国国家知识产权局



〔12〕发 明 专 利 说 明 书

专利号 ZL 200410066343.4

[51] Int. Cl.
H04L 9/32 (2006.01)
H04L 9/14 (2006.01)
G06K 9/00 (2006.01)
G06K 9/62 (2006.01)

[45] 授权公告日 2009 年 3 月 4 日

[11] 授权公告号 CN 100466516C

[22] 申请日 2004.9.9

[21] 申请号 200410066343.4

[73] 专利权人 杭州中正生物认证技术有限公司
地址 310012 浙江省杭州市文三路 90 号
东部软件园 1 号楼 3 楼

[72] 发明人 梁 敏 汪 涂

[56] 参考文献

US6601172B1 2003.7.29

CN1379893A 2002.11.13

CN1401172A 2003.3.5

审查员 刘剑波

[74] 专利代理机构 杭州九洲专利事务所有限公司
代理人 陈继亮

代理人 陈继亮

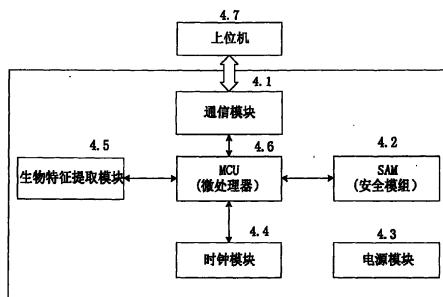
权利要求书 3 页 说明书 6 页 附图 6 页

[54] 发明名称

一种抵御重放攻击的生物认证方法

[57] 摘要

本发明涉及一种抵御重放攻击的生物认证装置，除了生物特征提取模块，另增系统独立的实时时钟模块，并经由通信模块与外界发生通信联系。对时钟模块的设置和时间读取，只能由包裹其外的数据加/解密模块，以密文的方式与上位机进行数据交互。本发明所述的认证方法，生物特征提取终端A生成带有时间信息的生物特征数据，加密后，将加密信息通过公共网络上传到生物认证终端B；生物认证终端B接收加密信息予以解密，首先判断其附带的时间信息是否在允许的范围之内，若符合要求，则进行生物认证。本发明的有益效果是：1)堵塞了生物认证系统中一个普遍存在的安全漏洞；2)提高了生物认证系统的安全性和公信力；3)结合实际，容易实施。



1、一种抵御重放攻击的生物认证方法，其特征是：该方法包含以下步骤：

- 1) 接受身份认证申请(8.1)后，生物认证终端B一直处于等待接收认证申请状态(9.1)，收到生物特征提取终端A发来的时间同步申请(9.2)，将生物认证终端B系统的时钟信息加密后，发送给生物特征提取终端A(9.3)；
- 2) 生物特征提取终端A接到生物认证终端B响应后，接收生物认证终端B的时间同步信息(8.3)并进行解密(8.4)，设置生物特征提取终端A的系统时间(8.5)；
- 3) 生物特征提取终端A提取生物特征数据(8.6)，提取生物特征提取终端A的系统时钟(8.7)，生成带有时间信息的生物特征数据(8.8)，加密(8.9)后，将加密信息通过公共网络上传到生物认证终端B(8.10)；
- 4) 生物认证终端B接收生物特征提取终端A的加密信息予以解密(9.4)，首先判断其附带的时间信息是否在允许的范围之内(9.5)，若符合要求，则进行生物认证(9.6)；若生物特征数据提交的时间不在允许范围之内，视为有重放攻击的嫌疑，认证不予响应，软件流程转到生物认证终端B一直处于等待接收认证申请状态(9.1)继续等待新的认证申请；若时间参数符合要求，当生物特征不符，系统给出验证未通过的提示，流程也转入生物认证终端B一直处于等待接收认证申请状态(9.1)继续等待新的认证申请；若生物特征相符，系统给出认证通过的提示(9.7)；

该方法具体包括：

- 1) 使生物特征提取终端A与生物认证终端B保证时钟的同步：

$|t_A - t_B| < \Delta t$ ；其中 t_B 生物认证终端B即时采集的系统时钟信息， t_A 生物特征提取终端A在收到生物认证终端B系统的时钟信息后，进行时间同步调整后的提取终端A的时钟信息， Δt ——保证时间同步的最大临界值；

- 2) 生物特征提取终端A提取生物特征值：

$F_T(I_C) = T_c$ ；其中 I_C 被验人C身上所提取的生物信息； F_T 生物特征提取函数； T_c 用提取函数 F_T 从生物信息中获得的生物特征；

- 3) 加入生物特征提取终端A当前系统的时钟，形成实时生物特征值：

$T_c + t_A$ ；

4) 用生物特征提取终端 A 密钥加密, 经公共网络传送生物认证终端 B;

$EK_A[T_c + t_A] \rightarrow B$, 其中 B 是生物认证终端 B, EK_A : 用生物特征提取终端 A 的密钥进行加密的函数;

5) 生物认证终端 B 密钥解密:

$DK_B\{EK_A[T_c + t_A]\} = T_c + t_A$; DK_B : 用生物认证终端 B 的密钥进行解密的函数;

6) 如果时延落在合理设定的时间窗 t_{w1} 以内, 即 $|t_B - t_A| < t_{w1}$,

判 T_c 有效, 进入后续验证程序 7);

否则

判 T_c 为无效, 提示生物特征值传输超时, 终止验证;

7) 启动识别算法, 给出识别结果:

$F_V(T_C, T_C') = R_C$; 其中 F_V 为生物认证终端 B 的识别算法, T_C' : 生物认证终端 B 备案的该生物特征, R_C : 对两个生物特征进行识别的结果;

8) 加入当前系统时间后, 加密传输给生物特征提取终端 A:

$EK_B[R_C + t_B] \rightarrow A$; 其中 A 是生物特征提取终端 A, EK_B : 用生物认证终端 B 的密钥进行加密的函数;

9) 生物特征提取终端 A 解密:

$DK_A\{EK_B[R_C + t_B]\} = R_C + t_B$ 其中 DK_A : 用生物认证终端 A 的密钥进行解密的函数;

10) 如果时延落在合理设定的时间窗 t_{w2} 以内, 即 $|t_B - t_A| < t_{w2}$,

判 R_C 有效,

否则

判 R_C 为无效, 提示生物认证结果传输超时, 终止验证。

2、根据权利要求 1 所述的抵御重放攻击的生物认证方法, 其特征在于, 采用建立同步握手协议的方式, 实现上述生物特征提取终端 A 和生物认证终端 B 的两端时钟同步:

1) 生物特征提取终端 A 以密文向生物认证终端 B 申请校时:

$EK_A[T_{set}] \rightarrow B$, 其中 T_{set} 是申请校时的命令;

2) 生物认证终端 B 解密:

$$DK_B\{EK_A[T_{set}]\} = T_{set}$$

3) 生物认证终端 B 采集本端时钟即即刻时点数，并加密，发送生物特征提取终端 A :

$$EK_B[t_B] \rightarrow A$$

4) 生物特征提取终端 A 解密，获得生物认证终端 B 时点值 t_B :

$$DK_A\{EK_B[t_B]\} = t_B;$$

5) 生物特征提取终端 A 校准本端时钟:

$$t_A = t_B.$$

3、根据权利要求 1 或 2 所述的抵御重放攻击的生物认证方法，其特征在于，在接收端设置可变大小的时间窗，以适应不同安全等级:

1) 设网络最小延时 t_{min} ;

2) 时间窗 $t_w = \alpha \times t_{min}$ ，其中 $\alpha \geq 1$ 为延时系数，以适应不同安全等级， α 越大，系统稳定性越大，但安全等级越低。

一种抵御重放攻击的生物认证方法

所属技术领域

本发明涉及一种生物认证装置和系统，尤其是一种抵御重放攻击的生物认证装置和方法。

背景技术

生物认证技术 Biometrics，是验证终端 B 通过生物特征提取终端 A ，从被验人 C 身上所测得生物特征 T_C （指纹、笔迹、声纹、虹膜、面相、步态、DNA 等）后，查验它是否与某一合法备案的生物特征 T_C' 相同，以确认 C 是否与 T_C' 所声称的身份相符的过程。

生物特征提取终端 A 与生物验证终端 B 分处不同地理位置的认证，称作异地生物认证。目前公知的异地生物认证，一般通过公共网络进行信息交互。具体过程是：

1) 验证终端 B 通过生物特征提取终端 A ，摄取被验人 C 的生物信息 I_C ；

2) 留驻 A 端的生物特征提取算法 F_T ，从 I_C 中提取生物特征 T_C ：

$$F_T(I_C) = T_C;$$

3) 用 A 端密钥 K_A 加密，形成密文：

$$Ek_A[T_C];$$

4) 把密文从 A 端经由公共网络送至 B 端：

$$Ek_A[T_C] \rightarrow B;$$

5) B 端用密钥 K_B 解密：

$$DK_B\{Ek_A[T_C]\} = T_C;$$

6) 用识别算法 F_V 对 T_C 与备案 T_C' 比较，给出认证结果：

$$F_V(T_C, T_C') = R_C;$$

7) 用 B 端密钥 K_B 加密验证结果：

$$EK_B[R_C];$$

8) 密文从 B 端经由公共网络送至 A 端：

$$EK_B[R_C] \rightarrow A.$$

其中第3) ~5) 步的加/解密处理，是为了防止生物特征信息在公共网络信道传输时被窃听、破解所采取的安全措施，参见图1。

但是，上述加密的生物特征信息如果在公共信道中被窃取，攻击者 H 即使不用破译密文，就可用重放攻击（playback）的方法，欺骗生物验证终端 B，使认证系统失去公信力。

如图2. 所示，当A端将加密生物特征数据 $EK_A[T_c]$ 2.11送入公共网络2.2后，被网络攻击端H2.4窃听、复制后，在H认为必要的时刻，向生物验证终端B2.3重放该复制的加密生物特征数据 $EK_A[T_c]$ ' 2.41；B端接收到 $EK_A[T_c]$ ' 后，并不知道该信息已被复制、重放，照例响应，进行解密，检索生物特征数据库，进行比对；将验证结果 R_c 加密后 $EK_B[R_c]$ 2.31送入公共网络信道1.2；攻击者同样能截获结果信息 $EK_B[R_c]$ ，也可将复制信息 $EK_B[R_c]$ ' 2.42发往生物特征提取终端A2.1。

发明内容

为了克服生物特征数据在公共网络传输过程中被窃听复制、受到重放攻击的安全隐患，本发明提供一种抵御重放攻击的生物认证装置和方法，由硬件加密芯片保护、具有内部时钟系统的生物特征提取终端，对生物特征数据加盖上实时印记后加密传输，并在接收端建立“时间窗”，用以识别、警示重放攻击。

本发明解决以上技术问题所采用的技术方案是：

本发明所述的抵御重放攻击的生物认证装置，主要包括：一MCU微处理器完成各个功能模块的协调；耦合到MCU微处理器的存储器，含有由MCU微处理器执行的指令组；一实时时钟模块，该实时时钟模块是电连接于MCU微处理器，用以获得提取生物特征的精确时间；一生物特征提取模块，该生物特征提取模块是电连接于MCU微处理器，并经由该MCU微处理器的控制以感测人体生物信息、提取生物特征信息；一SAM安全模组，该SAM安全模组是电连接于MCU微处理器，用来完成数据的加解密；电源模块4.3提供系统的电源；一通信模块，该通信模块电连接于MCU微处理器，用以与上位机进行数据通讯。各模块之间的连接方式，如图4所示。对现有生物特征提取终端A系统硬件结构加以改进，即除了生物特征提取模块3.1，另增实时时钟模块3.2，以获得提取生物特征的精确时间；采用加解/解密模块3.3将上述两个模块“封装”起来，经由（对外进行信息交换的惟一通道）通信模块3.4与外界发生通信联系。此时，实时时钟模块是系统独立的时钟，对其设置和时间读取，只能由包裹其外的数据加/解密模块，以密文的方式与上位机3.5进行数据交互。参见图3。

本发明所述的抵御重放攻击的生物认证方法，主要包含以下步骤：

- 1)、接受身份认证申请后，生物特征提取终端 A 向生物认证终端 B 提交同步申请；生物认证终端 B 一直处于等待接收认证申请状态，收到生物特征提取终端 A 发来的时间同步申请，将生物认证终端 B 系统的时钟信息加密后，发送给生物特征提取终端 A；
- 2)、生物特征提取终端 A 接到生物认证终端 B 响应后，接收生物认证终端 B 的时间同步信息并进行解密，设置生物特征提取终端 A 的系统时间；
- 3)、生物特征提取终端 A 提取生物特征数据，提取生物特征提取终端 A 的系统时钟，生成带有时间信息的生物特征数据，加密后，将加密信息通过公共网络上传到生物认证终端 B；
- 4)、生物认证终端 B 接收生物特征提取终端 A 的加密信息予以解密，首先判断其附带的时间信息是否在允许的范围之内，若符合要求，则进行生物认证；若生物特征数据提交的时间不在允许范围之内，视为有重放攻击的嫌疑，认证不予响应，软件流程转到继续等待新的认证申请；若时间参数符合要求，当生物特征不符，系统给出验证未通过的提示，流程也转入继续等待新的认证申请；若生物特征相符，系统给出认证通过的提示。

本发明为达到其技术目的所采取的具体方法如图 5 所示：

- 1) 使生物特征提取终端 A 与生物认证终端 B 保证时钟的同步：

$|t_A - t_B| < \Delta t$ ；其中 t_B 生物认证终端 B 即时采集的系统时钟信息， t_A 生物特征提取终端 A 在收到生物认证终端 B 系统的时钟信息后，进行时间同步调整后的提取终端 A 的时钟信息， Δt —保证时间同步的最大临界值；

- 2) 生物特征提取终端 A 提取生物特征值：

$F_T(I_C) = T_c$ ；其中 I_C 被验人 C 身上所提取的生物信息； F_T 生物特征提取函数 F_T ； T_c 用提取函数 F_T 从生物信息中获得的生物特征；

- 3) 加入生物特征提取终端 A 当前系统的时钟，形成实时生物特征值：

$T_c + t_A$ ；

- 4) 用生物特征提取终端 A 密钥加密，经公共网络传送生物认证终端 B；

$EK_A[T_c + t_A] \rightarrow B$ ，其中 B 是生物认证终端 B， EK_A 用生物特征提取终端 A 的密钥进行加密的函数；

- 5) 生物认证终端 B 密钥解密：

$DK_B\{EK_A[T_c + t_a]\} = T_c + t_a$; DK_B : 用生物认证终端 B 的密钥进行解密的函数;

6) 如果时延落在合理设定的时间窗 t_{n1} 以内, 即 $|t_b - t_a| < t_{n1}$,

判 T_c 有效, 进入后续验证程序 7);

否则

判 T_c 为无效, 提示生物特征值传输超时, 终止验证;

7) 启动识别算法, 给出识别结果:

$F_V(T_C, T_C') = R_C$; 其中 F_V 为生物认证终端 B 的识别算法, T_C' : 生物认证终端 B 备案的该生物特征, R_C : 对两个生物特征进行识别的结果;

8) 加入当前系统时间后, 加密传输给生物特征提取终端 A:

$EK_B[R_C + t_b] \rightarrow A$; 其中 A 是生物特征提取终端 A, EK_B : 用生物认证终端 B 的密钥进行加密的函数;

9) 生物特征提取终端 A 解密:

$DK_A\{EK_B[R_C + t_b]\} = R_C + t_b$ 其中 DK_A : 用生物认证终端 A 的密钥进行解密的函数;

10) 如果时延落在合理设定的时间窗 t_{n2} 以内, 即 $|t_b - t_a| < t_{n2}$,

判 R_C 有效,

否则

判 R_C 为无效, 提示生物认证结果传输超时, 终止验证。

本发明为解决以上技术问题而采用的技术方案还可以进一步完善:

一、可以采用建立同步握手协议的方式, 实现上述生物特征提取终端 A 和生物认证终端 B 的两端时钟同步:

1) 生物特征提取终端 A 以密文向生物认证终端 B 申请校时:

$EK_A[T_{set}] \rightarrow B$

2) 生物认证终端 B 解密:

$DK_B\{EK_A[T_{set}]\} = T_{set}$

3) 生物认证终端 B 采集本端时钟即即刻时点数, 并加密, 发送生物特征提取终端 A:

$$EK_B[t_B] \rightarrow A$$

4) 生物特征提取终端 A 解密, 获得生物认证终端 B 时点值 t_B :

$$DK_A\{EK_B[t_B]\} = t_B;$$

5) 生物特征提取终端 A 校准本端时钟:

$$t_A = t_B.$$

二、可以在接收端设置可变大小的时间窗, 以适应不同安全等级:

1) 设网络最小延时 t_{min} ;

2) 时间窗 $t_w = \alpha \times t_{min}$, 其中 $\alpha \geq 1$ 为延时系数, 以适应不同安全等级, α 越大, 系统稳定性越大, 但安全等级越低。

本发明的有益效果是:

- 1)、一种有效防止异地生物认证重放攻击的方法, 堵塞了生物认证系统中一个普遍存在的安全漏洞;
- 2)、提高了生物认证系统的安全性和公信力;
- 3)、结合实际, 容易实施。

附图说明

图 1 生物认证系统构成示意图;

图 2 是生物认证在公共网络中受到重放攻击示意图;

图 3 是本发明生物特征提取终端的系统构成示意图;

图 4 是本发明生物特征提取终端硬件结构示意图;

图 5 是本发明为防止重放攻击采用的一种方法流程图;

图 6 是本发明一个较佳实施例的硬件结构图;

图 7 是本发明一个较佳实施例的硬件电路图;

图 8 是本发明一个较佳实施例的生物特征提取流程图;

图 9 是本发明一个较佳实施例的生物认证终端工作流程图。

具体实施方式

下面结合附图和实施例对本发明作进一步描述。

图 6 是本发明一个较佳实施例的硬件结构图。其中通信模块 6.1 由通信接口电路 6.11 与通信控制电路 6.12 组成。通信控制电路 6.12 根据 MCU6.6 的指令，分别开放与生物特征提取模块 6.5、或者与上位机 6.7 的数据通信；通信接口电路 6.11 将 MCU 的 UART 电平，转换成为上位机 6.7 使用的 RS-232 接口电平；增添 FLASH6.61 作为 MCU 的外部存储器，存储生物特征数据或其他必要数据。

图 7 是该较佳实施例的硬件电路图。其中：MCU 微处理器 U2 的第 5、7 脚为数据接收/发送端。进行数据接收/发送时，由第 13 脚 SERI 发信号，给通信控制电路 CD4052BU5 的第 10 脚 SERI，告知通信对象后，U5 分别通过 1RDSM、12TDSM 或者 5RDPC、14TDPC，连通通信接口电路 U6 相应的引脚，达到分别与生物特征提取模块 J1 或者上位机 J2 通信的目的；时钟芯片 DS1302U7 第 6 脚 DSSDA 串行数据线，在第 5TIME、7DSCLK 时序控制下，与 MCU 进行提取时间/设定时间双向交流；SAM 加解密电路 U9 第 2SAMRST 复位、6SAMSDA 数据发送脚与在 U2 第 35、34 相连接；U3 为 MCU 的复位芯片；U4 为 2 兆 FLASH，与 MCU 的 40ATSCK、41ATST 连接；U6 为 I/O 接口芯片，作用是将 UART 电平转换为 RS-232 接口电平。

图 8 是该较佳实施例中生物特征提取终端 A，提取生物特征软件的流程图。系统接受身份认证申请 8.1 后，向验证终端 B 提交同步申请 8.2，接到生物认证终端 B 响应，接收生物认证终端 B 时间同步信息 8.3 并进行解密 8.4，设置系统时间 8.5，提取生物特征数据 8.6，提取本系统时钟 8.7，生成带有时间信息的生物特征数据 8.8 加密 8.9 后，将加密数据通过公共网络上传到生物认证终端 B8.10

图 9 是该较佳实施例中生物认证终端 B 的软件流程图。系统一直处于等待接收认证申请状态 9.1，收到生物特征提取终端 A 发来的时间同步申请 9.2，将本系统的时钟信息加密后，发送给生物特征提取终端 A9.3。然后接收 A 的加密信息予以解密 9.4，首先判断其附带的时间信息是否在允许的范围之内 9.5，若符合要求，则进行生物认证 9.6；若生物特征数据提交的时间不在允许范围之内，视为有重放攻击的嫌疑，认证不予响应，软件流程转到 9.1 继续等待新的认证申请；若时间参数符合要求，当生物特征不符，系统给出验证未通过的提示，流程也转入 9.1 继续等待新的认证申请。若生物特征相符，系统给出认证通过的提示 9.7。

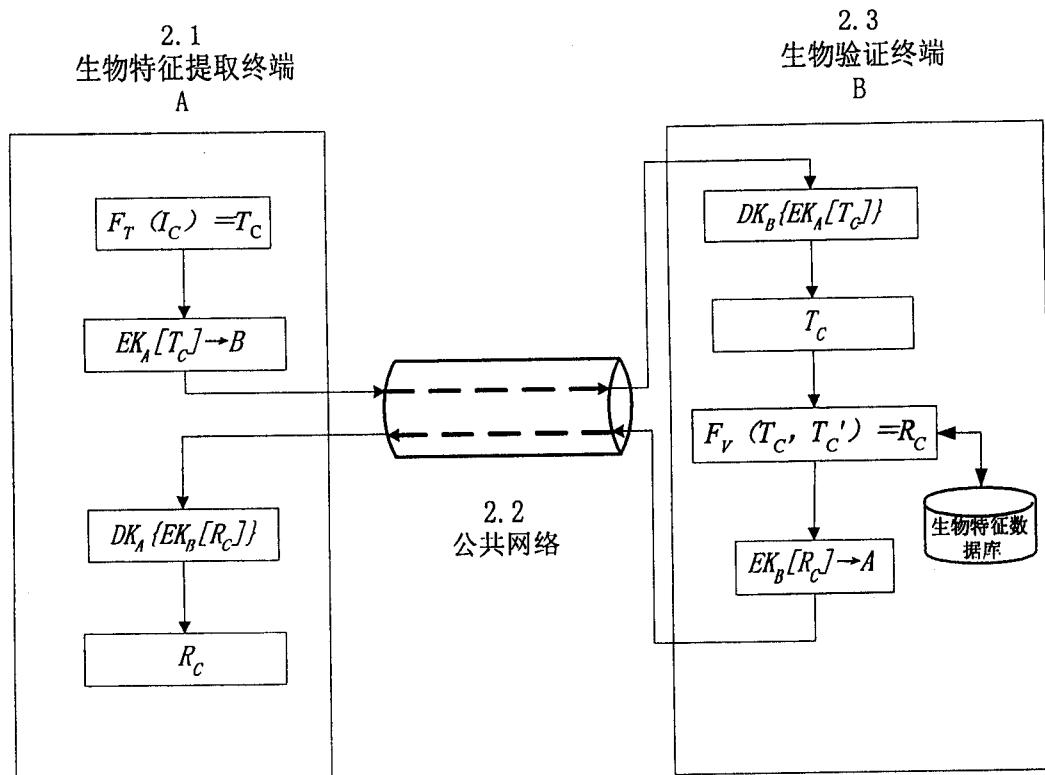


图1

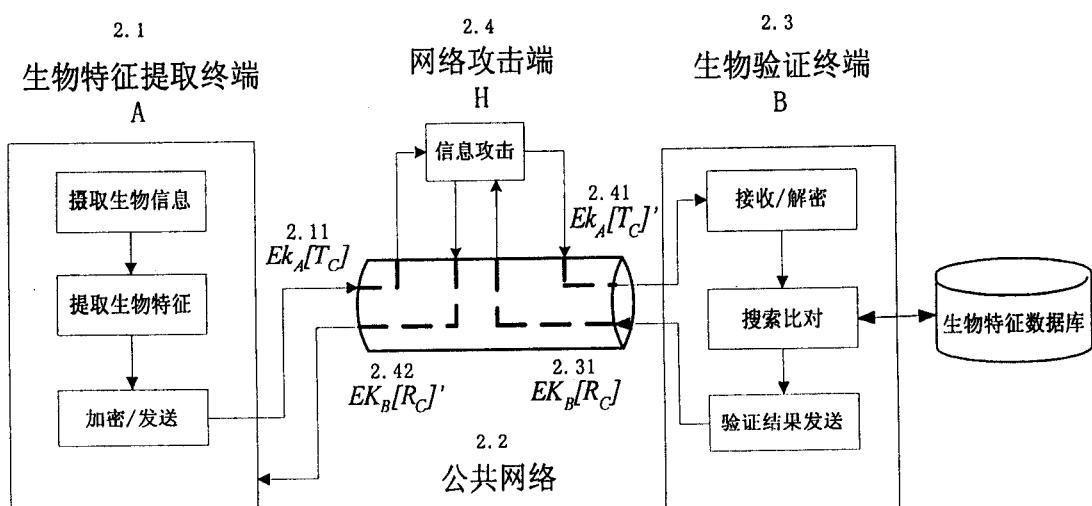


图2

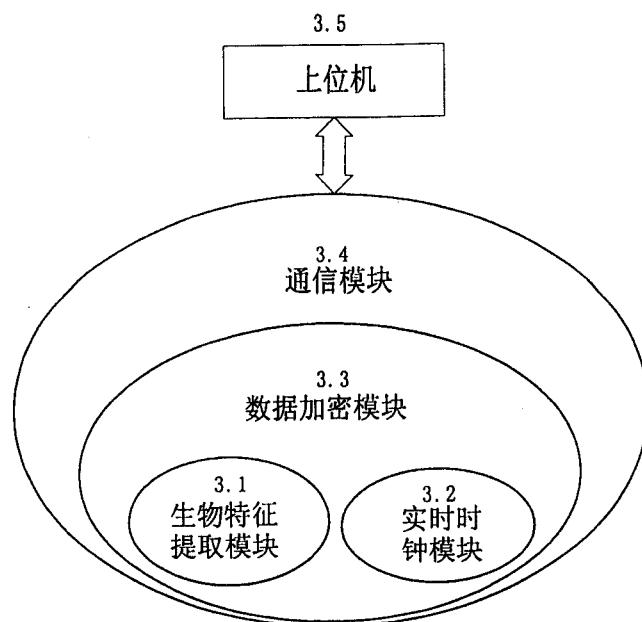


图 3

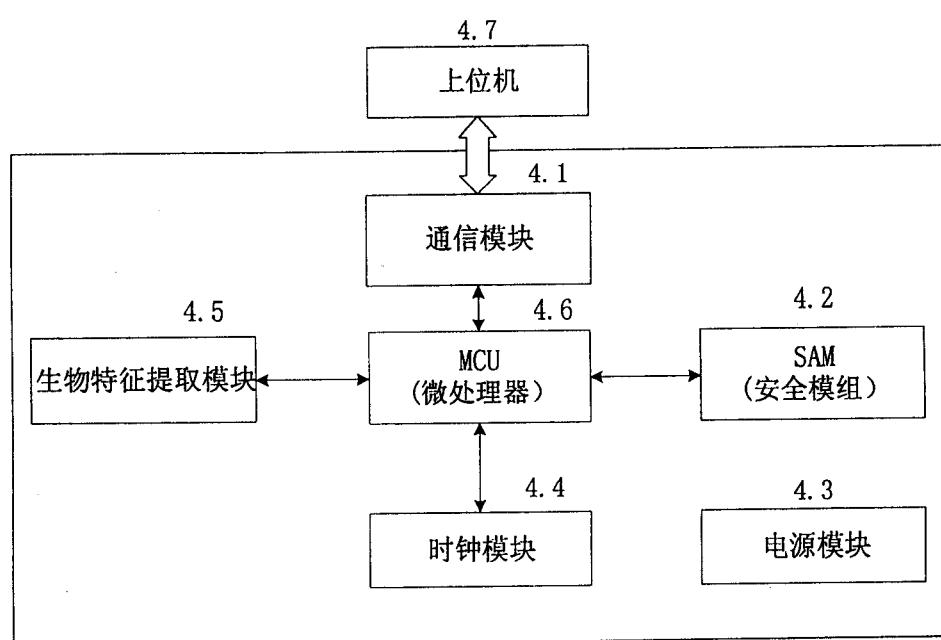


图 4

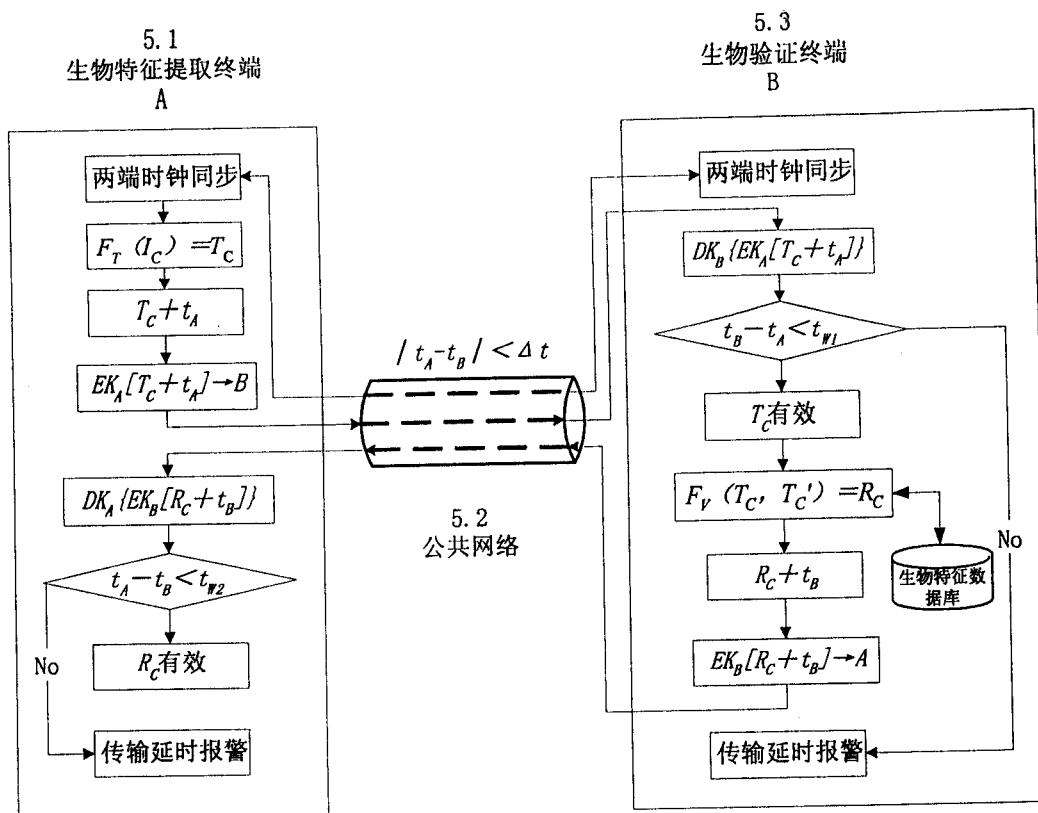


图 5

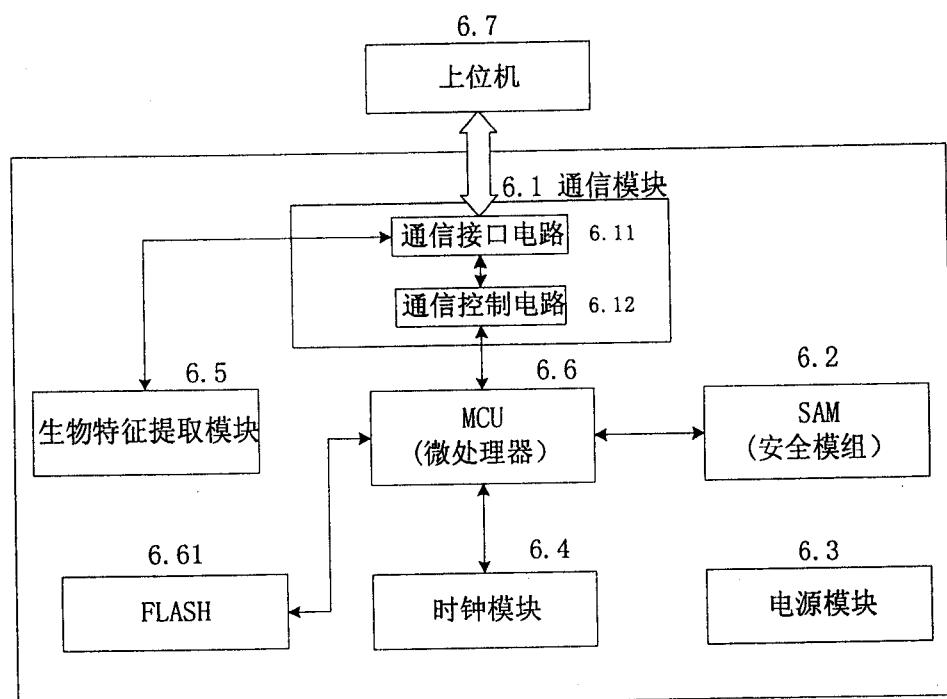
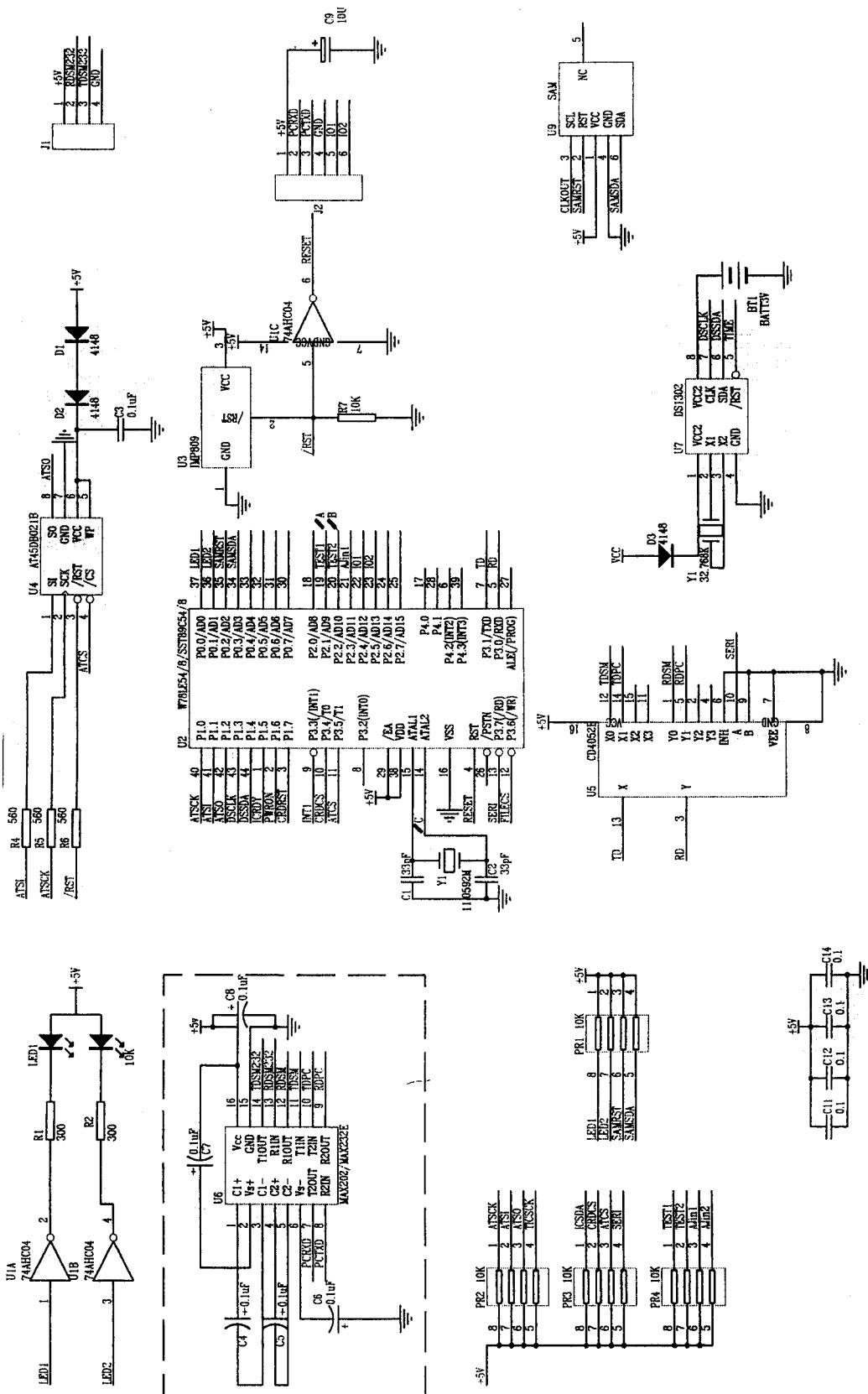


图 6



7

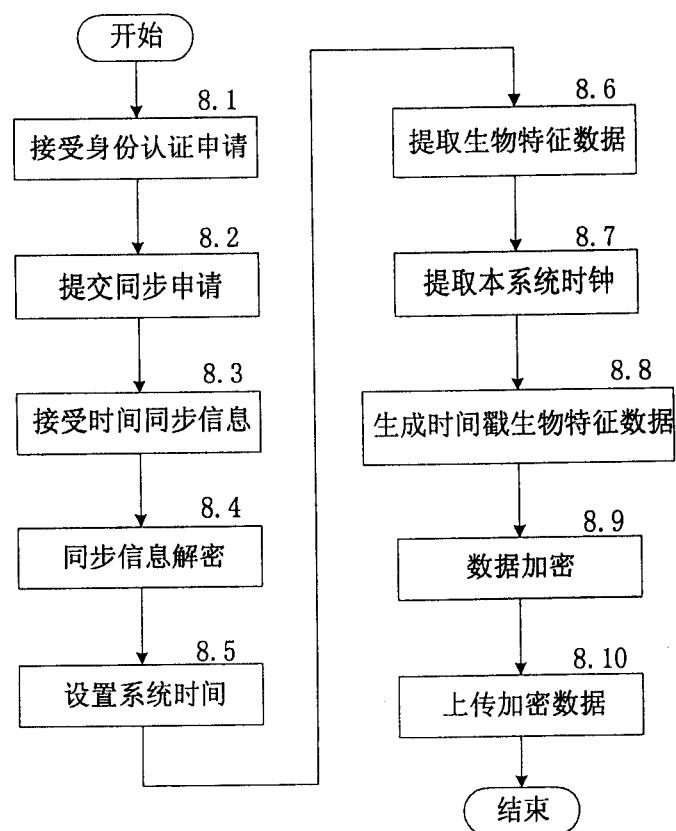


图 8

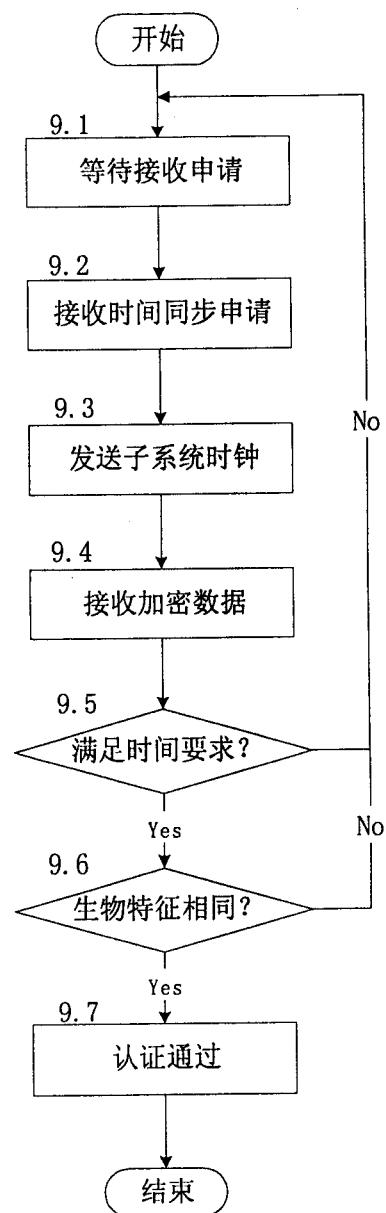


图 9