

一种字模获取方法、字符显示装置和系统，电子签名工具

技术领域

本发明涉及电子技术领域，尤其涉及一种字模获取方法、字符显示装置和系统，电子
5 签名工具。

背景技术

在传统的电子签名工具（例如USBKEY）中，字符（包括汉字，数字，字母，符号等）以内码的形式进行表示、交换和处理。需要显示字符时，电子签名工具将待显示
10 字符的内码转换成区位码，利用区位码从存储在电子签名工具中的字库中提取待显示字符的字模，然后根据字模信息在屏幕上以画点的方法将字符显示出来。

在这种情况下，由于需要存储所有待显示字符所对应的字模，电子签名工具需要较大的存储空间。一般的电子签名工具中的安全芯片的存储器无法满足存储如此大的字库的需求，因此，大多采用在安全芯片外部扩展一个存储器来存储字库。但是，在
15 安全芯片外部扩展一个存储器来存储字库，则会提高电子签名工具的成本。

发明内容

本发明所要解决的技术问题是，克服现有技术的不足，提供一种字模获取方法和字符显示装置、字符显示系统以及采用该字模获取方法的电子签名工具，可以通过获取存储在
20 外部设备（可称为字模存储装置，例如，交易终端，包括计算机、手机等）中的字模进行字符的显示，以降低字符显示装置（例如，电子签名工具）的成本。

为了解决上述问题，本发明提供一种字模获取方法，所述方法包括如下步骤：字符显示装置接收字模存储装置发送的字模；所述字符显示装置计算所述字模存储装置发送的字模的校验码；所述字符显示装置将计算得到的字模的校验码与本地存储的对应的字模校验
25 码进行对比，对比一致则判定所述字模存储装置发送的字模正确。

此外，所述字符显示装置为电子签名工具。

此外，所述字模存储装置为交易终端，包括计算机或者手机。

此外，所述字符显示装置将字模标识码发送给所述字模存储装置；所述字模存储装置根据所述字模标识码发送所述字模。

30 此外，所述字模存储装置将所述字模和所述字模对应的字模标识码发送给所述字符显示装置。

此外，所述字符显示装置判定所述字模存储装置发送的字模正确后，显示所述字模存储装置发送的字模对应的字符。

此外，所述字符显示装置通过CRC算法计算所述字模存储装置发送的字模的校验码；或者所述字符显示装置通过计算字模的MAC值计算所述字模存储装置发送的字模的校验码；或者所述字符显示装置通过散列算法计算所述字模存储装置发送的字模的校验码；或者所述字符显示装置通过HOTP算法计算所述字模存储装置发送的字模的校验码。

本发明还提供一种字符显示装置，包括显示单元，还包括：接收单元，计算单元，对比单元；其中：接收单元，用于接收字模存储装置发送的字模；计算单元，用于计算所述接收单元接收到的字模的校验码；对比单元，用于将所述计算单元计算得到的字模的校验码与本地存储的对应的字模校验码进行对比，对比一致则判定所述字模存储装置发送的字模正确；显示单元，用于在所述对比单元判定所述字模存储装置发送的字模正确后，显示所述接收单元接收到的字模对应的字符。

此外，所述装置还包括：存储单元，提取单元，报警单元，其中：存储单元，用于存储与字模存储装置存储的字模的字库相对应的字模校验码库；提取单元，用于从存储单元中提取字模的校验码，并发送给所述对比单元；报警单元，用于在所述对比单元判定所述字模存储装置发送的字模错误后，进行报警。

此外，所述显示单元，还用于在所述对比单元判定所述字模存储装置发送的字模错误后，显示错误信息。

此外，所述计算单元通过CRC算法计算所述字模存储装置发送的字模的校验码；或者所述计算单元通过计算字模的MAC值计算所述字模存储装置发送的字模的校验码；或者所述计算单元通过散列算法计算所述字模存储装置发送的字模的校验码；或者所述计算单元通过HOTP算法计算所述字模存储装置发送的字模的校验码。

本发明还提供一种字符显示系统，包括：字符显示装置，还包括字模存储装置；其中：字模存储装置，用于存储字符对应的字模的字库，并将字模发送至所述字符显示装置；字符显示装置，用于接收所述字模存储装置发送的字模，计算接收到的字模的校验码，将计算得到的字模的校验码与本地存储的对应的字模校验码进行对比，对比一致则判定所述字模存储装置发送的字模正确，并显示该字模对应的字符。

此外，字符显示装置，还用于将字模标识码发送给所述字模存储装置；字模存储装置，还用于根据所述字模标识码发送所述字模。

此外，所述字模存储装置，还用于将所述字模和所述字模对应的字模标识码发送给所述字符显示装置。

此外，所述字符显示装置，还用于与字模存储装置存储的字模的字库相对应的校验码库，在判定所述字模存储装置发送的字模错误后，显示错误信息或者报警。

5 此外，所述字符显示装置通过CRC算法计算所述字模存储装置发送的字模的校验码；或者所述字符显示装置通过计算字模的MAC值计算所述字模存储装置发送的字模的校验码；或者所述字符显示装置通过散列算法计算所述字模存储装置发送的字模的校验码；或者所述字符显示装置通过HOTP算法计算所述字模存储装置发送的字模的校验码。

10 本发明还提供一种电子签名工具，所述电子签名工具包括：字模处理模块，用于接收字模存储装置发送的字模，计算接收到的字模的校验码，将计算得到的字模的校验码与本地存储的对应的字模校验码进行对比，对比一致则判定所述字模存储装置发送的字模正确；显示屏，用于在所述字模处理模块判定所述字模存储装置发送的字模正确后，显示所述接收单元接收到的字模对应的字符。

15 此外，所述字模处理模块还用于存储与字模存储装置存储的字模的字库相对应的校验码库。

此外，所述电子签名工具还包括：蜂鸣器或者语音输出装置，用于在所述字模处理模块判定所述字模存储装置发送的字模错误后，进行报警。

20 此外，所述显示屏，还用于在所述字模处理模块判定所述字模存储装置发送的字模错误后，显示错误信息。

此外，所述字模处理模块通过CRC算法计算所述字模存储装置发送的字模的校验码；或者所述字模处理模块通过计算字模的MAC值计算所述字模存储装置发送的字模的校验码；或者所述字模处理模块通过散列算法计算所述字模存储装置发送的字模的校验码；或者所述字模处理模块通过HOTP算法计算所述字模存储装置发送的字模的校验码。

25

综上所述，本发明的字符显示装置、电子签名工具存储各个字符对应的字模的校验码，由于校验码一般采用2字节、4字节、6字节或8字节等，因此比直接存储字模（32字节）节省了存储空间，不需要在安全芯片的外部扩展存储器来存储，节省了成本。

30 另外，通过外部的字模存储装置存储字符对应的字模，并令字符显示装置、电子签名工具存储的校验码与交易终端存储的字模相对应，计算字模存储装置下发的字模的校验码，并将计算得到的校验码与本地存储的校验码进行对比，对比一致则显示该字模对应的字符，

保证了交易终端下发字模的正确性与安全性。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他附图。

图1是本发明字符显示系统的结构示意图；

图2是本发明字模获取方法第一实施例的流程图；

图3是本发明字符显示装置第一实施例的结构示意图；

图4是本发明电子签名工具第一实施例的结构示意图。

具体实施方式

下面结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，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。基于本发明的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明的保护范围。

本发明的核心是，字符显示装置（例如，电子签名工具）存储各个字符对应的字模的校验码，字模存储装置（例如，与电子签名工具相连的交易终端，包括计算机、手机等）存储字符对应的字模，电子签名工具存储的校验码与交易终端存储的字模相对应，电子签名工具提取待显示的字符对应的字模的校验码，并计算交易终端下发的字模的校验码，并将计算得到的校验码与本地存储的校验码进行对比，对比一致则显示该字模对应的字符。

下面将结合附图和实施例对本发明进行详细描述。

第一实施例

图1是本发明字模获取系统的结构示意图；本实施例中，字模获取系统包括：交易终端（字模存储装置）以及电子签名工具（字符显示装置）。

具体的，交易终端可以为计算机或者手机等。其存储有各个字符对应的字模的字库，其中，字符可以包括：汉字（繁体、简体等），数字，字母，符号，特殊字符等。

电子签名工具，用于存储各个字符对应的字模的校验码，形成校验码库，该校验码库

与交易终端存储的字模的字库相对应，当然，可以通过字模标识码来对应，例如：通过内码、区域码或自定义的字模标识码；电子签名工具从校验码库中提取待显示的字符对应的字模的校验码，对交易终端下发的字模进行计算，得到交易终端下发的字模的校验码，将计算得到的校验码与提取的待显示的字符对应的字模的校验码进行对比，对比一致则显示该字模对应的字符。

图2是本发明字模获取方法第一实施例的流程图；本实施例中，字模获取方法包括如下步骤：

步骤201，交易终端下发字模至电子签名工具。

具体的，交易终端可以根据电子签名工具的请求下发电子签名工具待显示的字符的字模，例如：电子签名工具把内码发给交易终端，交易终端下发字模标识码所对应的字模；交易终端还可以主动下发电子签名工具待显示的字符的字模，例如：交易终端将字模和内码一起发给电子签名工具。当然，交易终端可以逐个下发字符所对应的字模至电子签名工具，也可以同时下发多个字符所对应的字模至电子签名工具中。

步骤202，电子签名工具计算交易终端下发的字模的校验码。

具体的，电子签名工具预先通过CRC（Cyclical Redundancy Check，循环冗余码校验）算法计算出各个字模的CRC值，将各个字模的CRC值作为校验码，形成校验码库存储在电子签名工具的安全芯片中。该校验码库与交易终端存储的字模的字库相对应。

电子签名工具计算交易终端下发的字模的CRC值，得到下发的字模的校验码。

步骤203，电子签名工具将计算得到的交易终端下发的字模的校验码与提取的待显示的字符的字模的校验码进行对比，对比一致则显示该字模对应的字符。

具体的，电子签名工具需要显示字符“李”，电子签名工具从预先存储的校验码库中提取字符“李”的校验码，正常情况下，交易终端下发的字模为“李”，电子签名工具根据交易终端下发的字模“李”计算字模“李”的CRC值，得到“李”的校验码，将计算得到的“李”的校验码与提取的“李”的校验码进行对比，对比结果一致则显示“李”；否则，交易终端在下发字模“李”时经过篡改，被修改为“赵”，则电子签名工具将计算“赵”的CRC值，获得“赵”的校验码，将“赵”的校验码与提取的待显示的“李”的校验码进行对比，对比结果是不一致的，因此，电子签名工具不进行显示或者报错，例如显示“错误”，或者语音警报等。经过此种对比方法，可以避免交易终端在下发字模的情况下被篡改，提高了的安全性。

图3是本发明字符显示装置第一实施例的结构示意图；本实施例中，字模显示装置包括：

接收单元、计算单元、存储单元、显示单元、提取单元以及对比单元。

其中：

接收单元，用于连接交易终端，接收交易终端下发的字模。

计算单元，连接接收单元，用于计算接收单元接收的交易终端下发的字模的校验码。

5 存储单元，用于存储与交易终端存储的字模的字库相对应的校验码库。

显示单元，用于显示待显示的字符或者错误信息。

提取单元，连接存储单元，用于从存储单元中存储的校验码库中提取待显示的字符对应的字模的校验码。

10 对比单元，连接提取单元、计算单元和显示单元，用于将计算单元计算得到的交易终端下发的字模的校验码与提取单元提取的待显示的字符对应的字模的校验码进行对比，对比一致，则发送显示信息至显示单元显示字符，对比不一致，则发送报错信息至显示单元显示错误信息。

当然，本发明的字符显示装置还可以包括报警单元，该报警单元连接对比单元，在对比单元对比计算单元计算得到的交易终端下发的字模的校验码与提取单元提取的待显示的15 字符对应的字模的校验码不一致时，进行语音报警。

图4是本发明电子签名工具第一实施例的结构示意图；本实施例中，电子签名工具包括：字模处理模块和显示屏。

20 字模处理模块，连接显示屏，用于存储与交易终端存储的字模的字库相对应的校验码库，接收交易终端下发的字模，计算接收到的交易终端下发的字模的校验码，从存储的校验码库中提取待显示的字符对应的字模的校验码，将计算得到的交易终端下发的字模的校验码与提取的待显示的字符对应的字模的校验码进行对比，对比一致，则发送显示信息至显示屏显示字符，对比不一致，则发送报错信息至显示屏显示错误信息。

一般情况下，字模处理模块可以集成在安全芯片中。

25 显示屏，用于显示待显示的字符或者错误信息。

当然，本发明的电子签名工具还可以包括蜂鸣器或者语音输出装置，该蜂鸣器或者语音输出装置连接字模处理模块，在字模处理模块对比计算得到的交易终端下发的字模的校验码与提取的待显示的字符对应的字模的校验码不一致时，进行语音报警。

30 当然，本实施例中，从校验码库中提取待显示的字符的字模的校验码的步骤可以发生在步骤201的同时、步骤201至步骤202之间，步骤202的同时或者步骤202至步骤203之间。

本发明实施例中，电子签名工具还可以存储一级字库，并存储一级字库以外的其他字库的校验码，当待显示的字符超过一级字库之外，再通过计算交易终端下发字模的校验码并验证该校验码的方式进行显示。通过存储一级字库，可以待显示一级字库中的字符时，无需计算校验码，以加快显示速度。

- 5 本发明实施例中，电子签名工具计算出交易终端下发的字模的校验码与提取的待显示的字符的校验码一致时，还可以将该校验码对应的字模存储，当下一次待显示该字符时，无需通过交易终端下发字模，无需进行进一步的计算，以加快显示速度。

第二实施例

- 10 本发明第二实施例与第一实施例的区别在于校验码获得的方式与第一实施例不同。本实施例中，电子签名工具预先通过计算字模的MAC（Message Authentication Code，消息认证码）值的方式计算出各个字模的MAC值，将各个字模的MAC值作为校验码，形成校验码库存储在电子签名工具的安全芯片中。该校验码库与交易终端存储的字模的字库相对应。

- 15 当接收到交易终端下发的字模后，电子签名工具根据计算得到的MAC值来计算交易终端下发的字模的校验码。

当然，如果计算得到的MAC值过大，可以截取MAC值中的几位作为校验码，以便节省电子签名工具存储校验码库的空间。

在计算得到MAC值后，还可以通过密钥对MAC进行加密，获得加密后的MAC值，将加密后的MAC值作为校验码。

20

第三实施例

- 25 本发明第三实施例与第一实施例的区别在于校验码获得的方式与第一实施例不同。本实施例中，电子签名工具预先通过散列算法（例如：MD5，Message Digest Algorithm，消息摘要算法第五版）计算出各个字模的HASH值，将各个字模的HASH值作为校验码，形成校验码库存储在电子签名工具的安全芯片中。该校验码库与交易终端存储的字模的字库相对应。

当接收到交易终端下发的字模后，电子签名工具根据计算得到的HASH值来计算交易终端下发的字模的校验码。

- 30 当然，如果计算得到的HASH值过大，可以截取HASH值中的几位作为校验码，以便节省电子签名工具存储校验码库的空间。

第四实施例

本发明第四实施例与第一实施例的区别在于校验码获得的方式与第一实施例不同。本实施例中，电子签名工具预先通过HOTP算法计算出各个字模的HOTP值，将各个字模的HOTP值截取一部分作为校验码，形成校验码库存储在电子签名工具的安全芯片中。该校验码库与交易终端存储的字模的字库相对应。

当接收到交易终端下发的字模后，电子签名工具根据计算得到的HOTP值来计算交易终端下发的字模的校验码。

当然，在计算HOTP值时，采用通过密钥来求取摘要值的散列算法，在本实施例中，还可以不应用密钥直接求取摘要值。

在本发明的实施例中，电子签名工具存储各个字符对应的字模的校验码，由于校验码一般采用2字节、4字节、6字节或8字节等，因此比直接存储字模（32字节）节省了存储空间，不需要在安全芯片的外部扩展存储器来存储，节省了成本。

另外，通过交易终端（计算机、手机等）存储字符对应的字模，电子签名工具存储的校验码与交易终端存储的字模相对应，电子签名工具提取待显示的字符对应的字模的校验码，并计算交易终端下发的字模的校验码，并将计算得到的校验码与提取的存储的校验码进行对比，对比一致则显示该字模对应的字符。保证了交易终端下发字模的正确性与安全性。

以上所述，仅为本发明较佳的具体实施方式，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披露的技术范围内，可轻易想到的变化或替换，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该以权利要求书的保护范围为准。

权利要求书

1、一种字模获取方法，其特征在于，所述方法包括如下步骤：

5 字符显示装置接收字模存储装置发送的字模；

所述字符显示装置计算所述字模存储装置发送的字模的校验码；

所述字符显示装置将计算得到的字模的校验码与本地存储的对应的字模校验码进行对比，对比一致则判定所述字模存储装置发送的字模正确。

2、如权利要求1所述的方法，其特征在于，

10 所述字符显示装置为电子签名工具。

3、如权利要求1或2所述的方法，其特征在于，

所述字模存储装置为交易终端，包括计算机或者手机。

4、如权利要求1至3任一项所述的方法，其特征在于，

所述字符显示装置将字模标识码发送给所述字模存储装置；

15 所述字模存储装置根据所述字模标识码发送所述字模。

5、如权利要求1至4任一项所述的方法，其特征在于，

所述字模存储装置将所述字模和所述字模对应的字模标识码发送给所述字符显示装置。

6、如权利要求1至5任一项所述的方法，其特征在于，

20 所述字符显示装置判定所述字模存储装置发送的字模正确后，显示所述字模存储装置发送的字模对应的字符。

7、如权利要求1至6任一项所述的方法，其特征在于，

所述字符显示装置通过CRC算法计算所述字模存储装置发送的字模的校验码；或者

所述字符显示装置通过计算字模的MAC值计算所述字模存储装置发送的字模的校验

25 码；或者

所述字符显示装置通过散列算法计算所述字模存储装置发送的字模的校验码；或者

所述字符显示装置通过HOTP算法计算所述字模存储装置发送的字模的校验码。

8、一种字符显示装置，包括显示单元，其特征在于，该装置还包括：接收单元，计算单元，对比单元；其中：

30 接收单元，用于接收字模存储装置发送的字模；

计算单元, 用于计算所述接收单元接收到的字模的校验码;

对比单元, 用于将所述计算单元计算得到的字模的校验码与本地存储的对应的字模校验码进行对比, 对比一致则判定所述字模存储装置发送的字模正确;

显示单元, 用于在所述对比单元判定所述字模存储装置发送的字模正确后, 显示所述

5 接收单元接收到的字模对应的字符。

9、如权利要求8所述的装置, 其特征在于, 所述装置还包括: 存储单元, 提取单元, 报警单元, 其中:

存储单元, 用于存储与字模存储装置存储的字模的字库相对应的字模校验码库;

提取单元, 用于从存储单元中提取字模的校验码, 并发送给所述对比单元;

10 报警单元, 用于在所述对比单元判定所述字模存储装置发送的字模错误后, 进行报警。

10、如权利要求8或9所述的装置, 其特征在于,

所述显示单元, 还用于在所述对比单元判定所述字模存储装置发送的字模错误后, 显示错误信息。

11、如权利要求8至10任一项所述的装置, 其特征在于,

15 所述计算单元通过CRC算法计算所述字模存储装置发送的字模的校验码; 或者

所述计算单元通过计算字模的MAC值计算所述字模存储装置发送的字模的校验码; 或

者

所述计算单元通过散列算法计算所述字模存储装置发送的字模的校验码; 或者

所述计算单元通过HOTP算法计算所述字模存储装置发送的字模的校验码。

20 12、一种字符显示系统, 包括: 字符显示装置, 其特征在于, 该系统还包括字模存储装置; 其中:

字模存储装置, 用于存储字符对应的字模的字库, 并将字模发送至所述字符显示装置;

字符显示装置, 用于接收所述字模存储装置发送的字模, 计算接收到的字模的校验码, 将计算得到的字模的校验码与本地存储的对应的字模校验码进行对比, 对比一致则判定所
25 述字模存储装置发送的字模正确, 并显示该字模对应的字符。

13、如权利要求12所述的系统, 其特征在于,

字符显示装置, 还用于将字模标识码发送给所述字模存储装置;

字模存储装置, 还用于根据所述字模标识码发送所述字模。

14、如权利要求12或13所述的系统, 其特征在于,

30 所述字模存储装置, 还用于将所述字模和所述字模对应的字模标识码发送给所述字符显示装置。

15、如权利要求12至14任一项所述的系统，其特征在于，

所述字符显示装置，还用于与字模存储装置存储的字模的字库相对应的校验码库，在判定所述字模存储装置发送的字模错误后，显示错误信息或者报警。

16、如权利要求12至15任一项所述的系统，其特征在于，

5 所述字符显示装置通过CRC算法计算所述字模存储装置发送的字模的校验码；或者
所述字符显示装置通过计算字模的MAC值计算所述字模存储装置发送的字模的校验码；或者

所述字符显示装置通过散列算法计算所述字模存储装置发送的字模的校验码；或者
所述字符显示装置通过HOTP算法计算所述字模存储装置发送的字模的校验码。

10 17、一种电子签名工具，其特征在于，包括：

字模处理模块，用于接收字模存储装置发送的字模，计算接收到的字模的校验码，将计算得到的字模的校验码与本地存储的对应的字模校验码进行对比，对比一致则判定所述字模存储装置发送的字模正确；

15 显示屏，用于在所述字模处理模块判定所述字模存储装置发送的字模正确后，显示所述接收单元接收到的字模对应的字符。

18、如权利要求17所述的电子签名工具，其特征在于，

所述字模处理模块还用于存储与字模存储装置存储的字模的字库相对应的校验码库。

19、如权利要求17或18所述的电子签名工具，其特征在于，所述电子签名工具还包括：

20 蜂鸣器或者语音输出装置，用于在所述字模处理模块判定所述字模存储装置发送的字模错误后，进行报警。

20、如权利要求17至19任一项所述的电子签名工具，其特征在于，

所述显示屏，还用于在所述字模处理模块判定所述字模存储装置发送的字模错误后，显示错误信息。

21、如权利要求17至20任一项所述的电子签名工具，其特征在于，

25 所述字模处理模块通过CRC算法计算所述字模存储装置发送的字模的校验码；或者
所述字模处理模块通过计算字模的MAC值计算所述字模存储装置发送的字模的校验码；或者

所述字模处理模块通过散列算法计算所述字模存储装置发送的字模的校验码；或者
所述字模处理模块通过HOTP算法计算所述字模存储装置发送的字模的校验码。