(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 108564367 B
(45)授权公告日 2022.08.16

(21)申请号 201810320616.5

(22)申请日 2018.04.11

(65)同一申请的已公布的文献号
申请公布号 CN 108564367 A

(43)申请公布日 2018.09.21

(73)专利权人 宋伟杰
地址 317500 浙江省台州市温岭市泽国镇牧屿青年路97号

(72)发明人 郑鸿

(74)专利代理机构 蓝天知识产权代理(浙江)有限公司 33229
专利代理师 刘颖

(51)Int.Cl.
G06Q 20/38(2012.01)

(56)对比文件
CN 106960344 A,2017.07.18
CN 107835332 A,2018.03.23
CN 104657855 A,2015.05.27

审查员 张红万

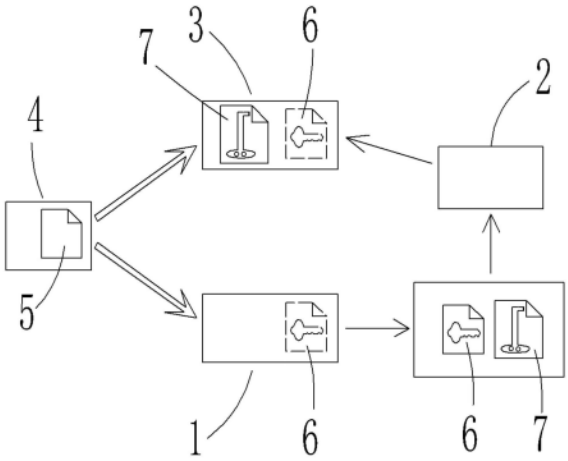
权利要求书1页 说明书2页 附图1页

(54)发明名称

一种支付加密的算法

(57)摘要

一种支付加密的算法，包括支付端、验证端及验证服务端，用户向支付端及验证服务端上传图像文件做为密钥载体；取图像文件的哈希值插入加密程序，做为加密程序一段代码，根据时间种子通过代码随机生成动态数字，再经转换程序转成平面二维像素点，在密钥载体文件像素范围内生成密钥像素点并叠加于密钥载体上；用户支付时，验证服务端通过验证端读取支付端显示内容，得出是否放行支付结果。本发明所述密钥载体可自定义，具有较强的灵活性；支付端在验证时无须联网或上传及下传任何信息，验证服务端经验证端从支付端获得的内容中获取密钥像素点，经验证后实现支付放行，具有极强的安全性；支付端体积可做得很小，待机时间长，具有极佳的便捷性。



CN 108564367 B

1.一种支付加密的算法,其特征在于:

包括支付端、验证端及验证服务端,用户定期或不定期向支付端及验证服务端上传相同属性的图像文件做为密钥载体;

取图像文件的哈希值插入支付端及验证服务端的加密程序,做为加密程序运行时的一段代码,并根据时间种子通过整段代码随机生成动态数字,由动态数字经转换程序转成平面二维像素点,基于密钥载体文件像素大小的范围,在范围内生成密钥像素点并叠加于密钥载体上;

用户支付时,验证服务端通过验证端读取支付端显示叠加密钥像素点的密钥载体,通过对比密钥像素点的像素位置得出是否放行支付的结果。

2.根据权利要求1所述的一种支付加密的算法,其特征在于:动态数字经转换程序转成平面二维像素点时,转换程序根据时间种子读取图像文件的哈希值的部分数值做为转换程序的一段代码。

3.根据权利要求1所述的一种支付加密的算法,其特征在于:转换程序在将动态数字转成平面二维像素点时,所基于的密钥载体文件像素大小的范围为图像文件相素点颜色较淡或空白的部分区域。

4.根据权利要求1所述的一种支付加密的算法,其特征在于:转换程序在将动态数字转成平面二维像素点时,所生成的平面二维像素点为指定与密钥载体的像素点的区域颜色不同。

一种支付加密的算法

技术领域

[0001] 本发明涉及一种算法，具体涉及一种支付加密的算法，属于IPC分类第G06、G09技术领域。

背景技术

[0002] 支付系统是由提供支付清算服务的中介机构和实现支付指令传送及资金清算的专业技术手段共同组成，用以实现债权债务清偿及资金转移的一种金融安排，有时也称为清算系统。

[0003] 目前，在进行支付时，支付系统的支付载体有磁条卡，移动设备(包括扫条形码、二维码以及NFC近场支付)。磁条卡有被复制的可能，因此现在升级为芯片卡。扫码时二维码有被偷换的可能，因此扫码趋向于由移动设备提供动态变化的条形码或二维码被扫比较安全。而近场支付使用起来比扫码要麻烦一点，且推广范围有限。

[0004] 另外，刷卡需要携带银行卡，扫码以及近场支付均需要提供及携带移动设备，对于当今倡导轻便出行的年青人来讲，携带移动设备更方便，但移动设备又受限于电池及网络，所以就目前来讲，还完全没有一种更加方便的支付载体且能脱离网络单独运行以及兼具安全性的系统或方法来实现真正意义上的便捷。

发明内容

[0005] 本发明的目的就是为了解决上述问题的不足，而提供了一种支付加密的算法，该算法可脱离网络单独运行，并且还具有安全性和依附载体的选择的便捷性。

[0006] 本发明所要解决问题的技术方案如下：

[0007] 一种支付加密的算法，其特征在于：

[0008] 包括支付端、验证端及验证服务端，用户定期或不定期向支付端及验证服务端上传相同属性的图像文件做为密钥载体；

[0009] 取图像文件的哈希值插入支付端及验证服务端的加密程序，做为加密程序运行时的一段代码，并根据时间种子通过整段代码随机生成动态数字，由动态数字经转换程序转成平面二维像素点，基于密钥载体文件像素大小的范围，在范围内生成密钥像素点并叠加于密钥载体上；

[0010] 用户支付时，验证服务端通过验证端读取支付端显示叠加密钥像素点的密钥载体，通过对比密钥像素点的像素位置得出是否放行支付的结果。

[0011] 动态数字经转换程序转成平面二维像素点时，转换程序根据时间种子读取图像文件的哈希值的部分数值做为转换程序的一段代码。

[0012] 转换程序在将动态数字转成平面二维像素点时，所基于的密钥载体文件像素大小的范围为图像文件相素点颜色较淡或空白的部分区域。

[0013] 转换程序在将动态数字转成平面二维像素点时，所生成的平面二维像素点为指定与密钥载体的像素点的区域颜色不同。

[0014] 本发明的有益效果如下：

[0015] 密钥载体可自定义，具有较强的灵活性；支付端在验证时无须联网或上传及下传任何信息，验证服务端经验证端从支付端获得的内容中获取密钥像素点，经验证后实现支付放行，具有极强的安全性；支付端体积可做得很小，待机时间长，具有极佳的便捷性。

附图说明：

[0016] 图1是本发明的框架结构示意图；

[0017] 图2是本发明所述图像文件至密钥像素点的过程示意图。

具体实施方式：

[0018] 下面结合附图对本发明作进一步详细的阐述。

[0019] 参阅图1、图2，一种支付加密的算法，包括支付端1、验证端2及验证服务端3，用户4定期或不定期向支付端及验证服务端上传相同属性的图像文件5做为密钥载体6；

[0020] 取图像文件5的哈希值插入支付端1及验证服务端3的加密程序，做为加密程序运行时的一段代码，并根据时间种子通过整段代码随机生成动态数字8，由动态数字8经转换程序转成平面二维像素点，基于密钥载体文件像素大小的范围，在范围内生成密钥像素点7并叠加于密钥载体上；

[0021] 用户4支付时，验证服务端3通过验证端2读取支付端1显示叠加密钥像素点7的密钥载体，通过对比密钥像素点的像素位置得出是否放行支付的结果。

[0022] 本发明在使用时，时间种子以天所在的日期为单位，这样支付端1与验证服务端3生成的动态数字8可以保持一致性。也就是说，密钥像素点动态变化的周期为1天。出于安全性考虑，对于每笔支付还可以做限额以及每天支付总额做一个限定，这样即便在支付端1丢失或被盗的情况下仍可以将损失降到最小。

[0023] 哈希值在再插入支付端1及验证服务端3的加密程序中时，可选择提取哈希值的部分数字串，该部分数字串的选择可根据图像文件5上传的时间单位以时为时间种子选取哈希值的位数。因此在图像文件5上传支付端1及验证服务端3时需保持在相同以时为单位的时间内。

[0024] 基于实施方式的改进，动态数字8经转换程序转成平面二维像素点时，转换程序根据时间种子读取图像文件的哈希值的部分数值做为转换程序的一段代码。

[0025] 进一步，基于实施方式的改进，转换程序在将动态数字8转成平面二维像素点时，所基于的密钥载体文件像素大小的范围为图像文件相素点颜色较淡或空白的部分区域。

[0026] 这样可以排除转成的平面二维像素点其中某个或某些点位置叠加在图像文件5颜色较深的像素点之上，使得识别出现问题。

[0027] 另外，基于实施方式的改进，转换程序在将动态数字转成平面二维像素点时，所生成的平面二维像素点为指定与密钥载体的像素点的区域颜色不同。

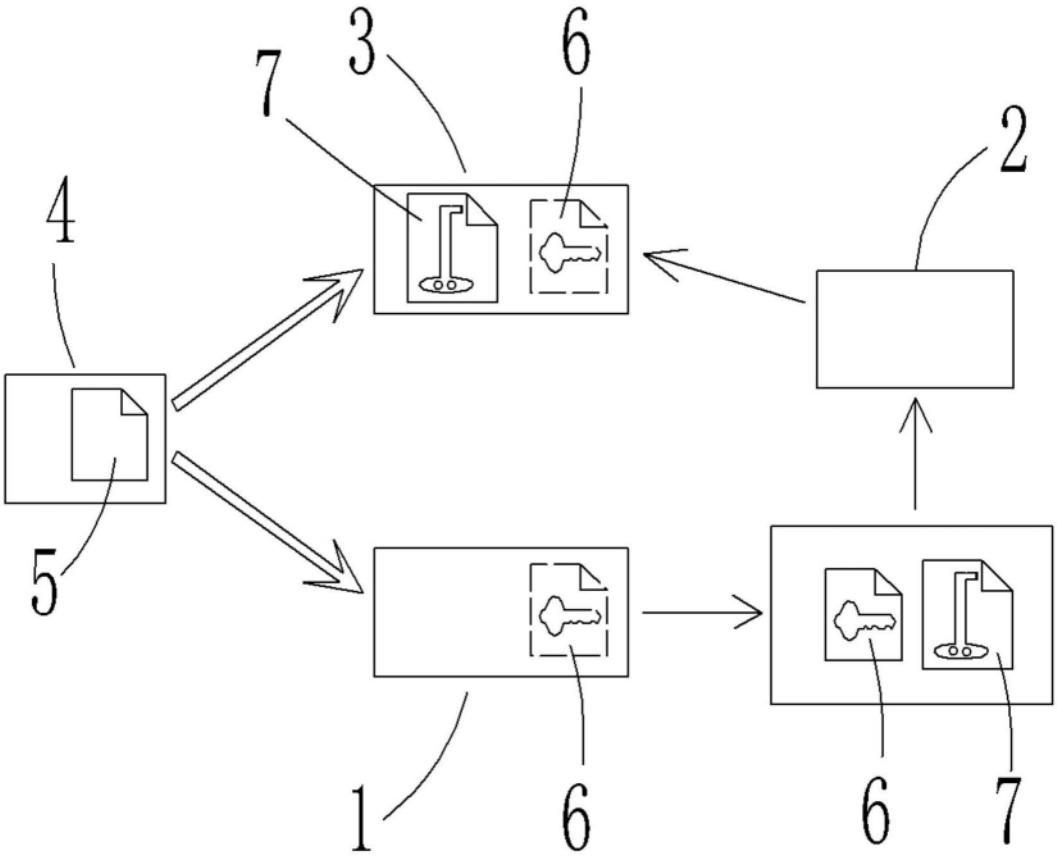


图1

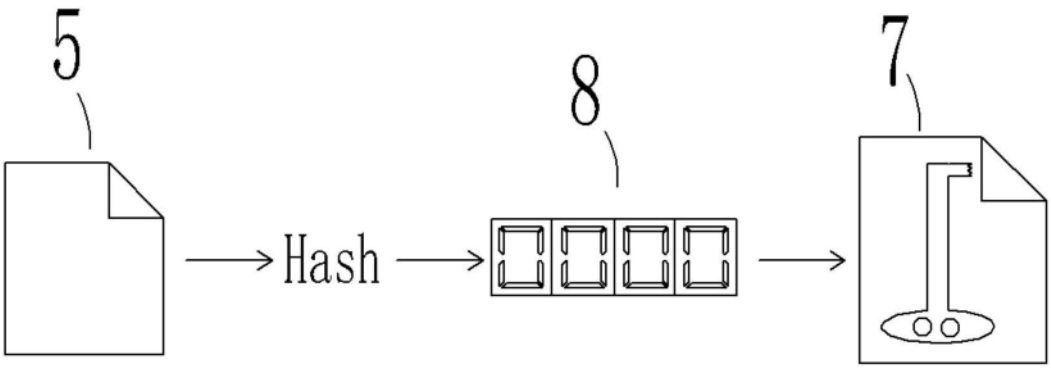


图2