



(12) 发明专利

(10) 授权公告号 CN 109767233 B

(45) 授权公告日 2024.03.29

(21) 申请号 201711058876.1

CN 104680389 A, 2015.06.03

(22) 申请日 2017.11.01

CN 105550881 A, 2016.05.04

(65) 同一申请的已公布的文献号

CN 105512709 A, 2016.04.20

申请公布号 CN 109767233 A

CN 104794988 A, 2015.07.22

(43) 申请公布日 2019.05.17

CN 103455784 A, 2013.12.18

(73) 专利权人 杭州沃朴物联科技有限公司

CN 102855574 A, 2013.01.02

地址 310000 浙江省杭州市余杭区五常街

CN 205721892 U, 2016.11.23

道五常大道181号8幢203室

CN 105160993 A, 2015.12.16

US 2017249491 A1, 2017.08.31

(72) 发明人 樊晓东 袁涌耀

马纪丰.安全RFID与NFC手机的互动防伪应用.《中国防伪报道》.2014,(第11期),第92-95页.

(74) 专利代理机构 南昌贤达专利代理事务所

(普通合伙) 36136

专利代理师 金一娴

张鹏新等.光学式和电容式指纹采集器的检测与比对.《中国公共安全(学术版)》.2013,(第2期),第115-118页.

(51) Int. Cl.

G06Q 30/018 (2023.01)

Wei Hsun Lee 等.An NFC Anti-

G06K 17/00 (2006.01)

Counterfeiting Framework for ID

(56) 对比文件

CN 103646334 A, 2014.03.19

Verification and Image Protection.《Mobile

CN 207473664 U, 2018.06.08

Networks and Applications》.2016,第21卷第

CN 102542911 A, 2012.07.04

646-655页.

审查员 王黎

权利要求书1页 说明书13页 附图1页

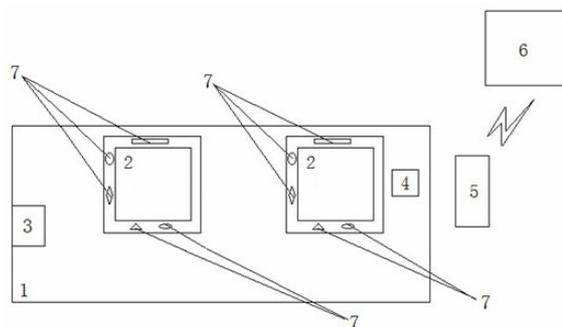
(54) 发明名称

一种基于振动信息特征和随机金葱粉的NFC识别防伪系统

传感器和手持客户端设备分别与服务器通信。

(57) 摘要

本发明公开了一种基于振动信息特征和随机金葱粉的NFC识别防伪系统,包括防伪特征单元和防伪识别单元两部分,其中,防伪特征单元的主体为商品的不锈钢基底,基底上黏附有监测其随声音振动情况的振动传感器,还内嵌对于细微振动敏感的至少两个振动片,振动片与基底之间通过易碎纸粘结,易碎纸的表面黏附有随机分布的金葱粉,在基底上嵌入写入上述振动片随声音振动幅度变化信息和金葱粉的分布图像信息的NFC芯片;防伪识别单元包括用于播放声音并采集振动片随声音振动幅度变化图像、金葱粉分布图像和读取NFC芯片的手持客户端设备,振动



1. 利用防伪系统的一种基于振动信息特征和随机金葱粉的防伪方法,其特征在于,具体步骤如下:

(1) 手持客户端设备采集金葱粉的分布图像,同时手机客户端播放设定的声音片段,并采集相应振动片随声音的振动幅度图像信息,读取NFC芯片,将这些信息一并发送至服务器;

(2) 服务器根据NFC信息解析出金葱粉的分布图像信息和相应振动片随声音的振动幅度图像信息,并与步骤(1)采集到的金葱粉的分布图像和相应振动片随声音的振动幅度图像信息进行比对,倘若完全一致,进入步骤(3),倘若出现不一致,则判定商品为假,结束;

(3) 振动传感器采集基底随声音的振动情况信息实时传送至服务器,判断其是否与服务器中存储的振动情况信息完全一致,是则进入步骤(4),否则判定商品为假,结束;

(4) 将步骤(3)采集到的基底振动情况信息与相应的金葱粉分布图像、振动片振动幅度图像信息匹配,再次请求验伪时,判断再次采集到的基底振动情况信息是否与所述金葱粉分布图像、振动片振动幅度图像信息匹配,是则判定为真,否则判定商品为假,结束;

所述的防伪系统,包括防伪特征单元和防伪识别单元两部分,其中,防伪特征单元的主体为商品的不锈钢基底,基底上黏附有监测其随声音振动情况的振动传感器,还内嵌对于细微振动敏感的至少两个振动片,振动片与基底之间通过易碎纸粘结,易碎纸的表面黏附有随机分布的金葱粉,在基底上嵌入写入上述振动片随声音振动幅度变化信息和金葱粉的分布图像信息的NFC芯片;所述防伪识别单元包括用于播放声音并采集振动片随声音振动幅度变化图像、金葱粉分布图像和读取NFC芯片的手持客户端设备,所述振动传感器和手持客户端设备分别与服务器通信;

所述振动片为厚度0.2~0.3mm的薄铜片;

所述手持客户端设备为嵌入NFC模块的手机;

所述基底的底部设有壳体,壳体内设有抗磁干扰装置、控温装置、定位装置、位置信息存储器、警示装置、电源及充电装置,各个元器件之间填充有柔性材料;

所述防伪系统还包括固定装置和自毁装置,固定装置用于实现基底与商品的连接,自毁装置在固定装置发生位移或破损时自动启动进而造成以下结果中的至少一种:基底发生肉眼可见的破损;和/或向服务器发送防伪失效信息;

所述防伪系统的制作方法,包括步骤:

(A) 手持客户端设备播放设定的声音片段,振动传感器采集基底随声音的振动情况信息,并发送至服务器存储;

(B) 采集金葱粉的分布图像信息,并且在手持客户端设备播放上述设定的声音片段时,同时采集相应振动片随声音的振动幅度图像信息,将金葱粉的分布图像信息和相应振动片随声音的振动幅度图像信息通过服务器运算生成相应的密码信息,并将其写入NFC芯片内;

步骤(B)中密码信息是采用SM3杂凑算法与以下一种或任意多种算法的组合算法生成的:RC4算法、和/或B-M算法、和/或MD5算法、和/或A5算法、和/或SEAL算法。

## 一种基于振动信息特征和随机金葱粉的NFC识别防伪系统

### 技术领域

[0001] 本发明涉及一种防伪系统,具体涉及一种基于振动信息特征和随机金葱粉的NFC识别防伪系统。属于防伪技术领域。

### 背景技术

[0002] 随着经济的不断发展,商品也呈现多样化的发展,满足了广大消费者的需求,但是,随之而来的是大量的假冒伪劣产品,这不但影响国民经济的健康发展,还损害了商家和广大消费者的利益。因此,防伪打假是商品流通过程中不可缺少的一个重要难题。

[0003] 目前市场上的防伪技术种类繁多,包括激光全息防伪、荧光油墨防伪、防伪印刷和可查询密码电话防伪等。但是,随着假冒伪劣犯罪分子对现有成熟防伪技术的破解,对现有的防伪标签进行了复制和回收,无法实现有效防伪。而一些新兴的防伪手段往往又难以识别或者对识别设备的要求较高,影响了消费者现场识别的便利性。

[0004] 近年来,纹理防伪技术引起了人们的注意,它是以前包装材料本身固有的斑纹记号为防伪识别标记的一种防伪技术。自然界的斑纹总是千差万别的,如指纹、木纹、石纹、斑马纹、冰纹、树叶纹等纹理都是随机的、唯一的、不可能有两个完全一样的。利用这一原理,选用纹理清晰的包装材料制成防伪标签,对每一枚标签材料的斑纹记号进行拍摄、编号、建档,并存入防伪数据库中。消费者可以方便地通过互联网、传真、电话查询档案进行真伪鉴别。但是,现有的纹理防伪技术存在很多问题,比如:依赖于自然纹理,其相应的图像数据量过大,需要的硬件存储设备容量很大,成本较高。

### 发明内容

[0005] 本发明的目的是为克服上述现有技术的不足,提供一种基于振动信息特征和随机金葱粉的NFC识别防伪系统。

[0006] 为实现上述目的,本发明采用下述技术方案:

[0007] 一种基于振动信息特征和随机金葱粉的NFC识别防伪系统,包括防伪特征单元和防伪识别单元两部分,其中,防伪特征单元的主体为商品的不锈钢基底,基底上黏附有监测其随声音振动情况的振动传感器,还内嵌对于细微振动敏感的至少两个振动片,振动片与基底之间通过易碎纸粘结,易碎纸的表面黏附有随机分布的金葱粉,在基底上嵌入写入上述振动片随声音振动幅度变化信息和金葱粉的分布图像信息的NFC芯片;所述防伪识别单元包括用于播放声音并采集振动片随声音振动幅度变化图像、金葱粉分布图像和读取NFC芯片的手持客户端设备,所述振动传感器和手持客户端设备分别与服务器通信。

[0008] 优选的,所述振动片为厚度0.2~0.3mm的薄铜片。

[0009] 优选的,所述手持客户端设备为嵌入NFC模块的手机。

[0010] 优选的,所述基底的底部设有壳体,壳体内设有抗磁干扰装置、控温装置、定位装置、位置信息存储器、警示装置、电源及充电装置(优选为无线充电装置),各个元器件之间填充有柔性材料,以避免商品运输过程中对各个元器件的撞击磕碰;具体如下:

[0011] 控温装置,设定高温和低温两个阈值,控温装置在外界温度高于高温阈值、或低于低温阈值时自动工作,将壳体内元器件的温度控制在高温阈值和低温阈值之前,保障各元器件的寿命;

[0012] 定位装置和位置信息存储器,能够记录标签的位置变化信息;

[0013] 警示装置,设定报警事件,当报警事件发生时,警示装置发出机械波或电磁波进行警示。

[0014] 优选的,所述防伪系统还包括固定装置和自毁装置,固定装置用于实现基底与商品的连接,自毁装置在固定装置发生位移或破损时自动启动进而造成以下结果中的至少一种:基底发生人体肉眼可见的破损;和/或向服务器发送防伪失效信息。

[0015] 上述防伪系统的制作方法,包括步骤:

[0016] (A) 手持客户端设备播放设定的声音片段,振动传感器采集基底随声音的振动情况信息,并发送至服务器存储;

[0017] (B) 采集金葱粉的分布图像信息,并且在手持客户端设备播放上述设定的声音片段时,同时采集相应振动片随声音的振动幅度图像信息,将金葱粉的分布图像信息和相应振动片随声音的振动幅度图像信息通过服务器运算生成相应的密码信息,并将其写入NFC芯片内。

[0018] 优选的,步骤(B)中密码信息是采用SM3杂凑算法与以下一种或任意多种算法的组合算法生成的:RC4算法、和/或B-M算法、和/或MD5算法、和/或A5算法、和/或SEAL算法。

[0019] 进一步优选的,采用SM3杂凑算法与RC4算法组合生成密码信息。

[0020] 利用上述防伪系统的一种基于振动信息特征和随机金葱粉的防伪方法,具体步骤如下:

[0021] (1) 手持客户端设备采集金葱粉的分布图像,同时手机客户端播放设定的声音片段,并采集相应振动片随声音的振动幅度图像信息,读取NFC芯片,将这些信息一并发送至服务器;

[0022] (2) 服务器根据NFC信息解析(反推算)出金葱粉的分布图像信息和相应振动片随声音的振动幅度图像信息,并与步骤(1)采集到的金葱粉的分布图像和相应振动片随声音的振动幅度图像信息进行比对,倘若完全一致,进入步骤(3),倘若出现不一致,则判定商品为假,结束;

[0023] (3) 振动传感器采集基底随声音的振动情况信息实时传送至服务器,判断其是否与服务器中存储的振动情况信息完全一致,是则进入步骤(4),否则判定商品为假,结束;

[0024] (4) 将步骤(3)采集到的基底振动情况信息与相应的金葱粉分布图像、振动片振动幅度图像信息匹配,再次请求验伪时,判断再次采集到的基底振动情况信息是否与所述金葱粉分布图像、振动片振动幅度图像信息匹配,是则判定为真,否则判定商品为假,结束。

[0025] 本发明的有益效果:

[0026] 1、本发明的防伪系统包括防伪特征单元和防伪识别单元,将基底随声音的振动情况信息与金葱粉的分布图像、振动片随声音振动幅度变化信息匹配起来,服务器仅存储基底随声音的振动情况信息,防伪判断时现场根据NFC信息推算出对应的金葱粉的分布图像和振动片随声音振动幅度变化信息,大大节约了存储空间。

[0027] 2、手持客户端设备可以方便地采集金葱粉的分布图像、振动片随声音振动幅度变

化图像,并可读取NFC芯片,进而将数据信息无线发送给服务器进行处理,不需要另外配备专用的高端设备,普通的嵌入NFC模块手机即可实现这些功能。振动传感器可以灵敏监测基底随声音的振动情况,并实时传送给服务器。

[0028] 3、本发明具有无法被复制,无法被回收,伪造概率低,成本低,适用于各行各业的各种商品,伪造成本高等特点。基底随声音的振动情况信息与、金葱粉的分布图像、振动片随声音振动幅度变化信息完全匹配一致方可,特定基底和振动片随声音的振动情况是独一无二的,但是一次防伪验证后基底随声音的振动情况信息与金葱粉的分布图像、振动片随声音振动幅度变化信息匹配,造假者很难复制做到尺寸、状态等完全一致的基底和振动片,从而达到防伪目的。

[0029] 4、对造假者而言,破解算法仍无法仿制,必须掌握二维码与金葱粉的分布图像、振动片随声音振动幅度变化的对应算法才可仿造,有效提高了不法分子的造假难度。

[0030] 5、二维码生成时可以采用两种或三种、四种计算因子进行加密计算,同时可以采用不同算法的迭代运算,大大增加了防伪性,降低了造假难度。

[0031] 6、本发明既可以单独使用、也可以与其他自毁装置结合使用,能够防止复制及回收利用,大大增强防伪性。

## 附图说明

[0032] 图1是本发明的结构示意图;

[0033] 其中,1为基底,2为振动片,3为振动传感器,4为二维码,5为手机,6为服务器。

## 具体实施方式

[0034] 下面结合附图和实施例对本发明进行进一步的阐述,应该说明的是,下述说明仅是为了解释本发明,并不对其内容进行限定。

[0035] 实施例1:

[0036] 如图1所示的一种基于振动信息特征和随机金葱粉的NFC识别防伪系统,包括防伪特征单元和防伪识别单元两部分,其中,防伪特征单元的主体为商品的不锈钢基底1,基底1上黏附有监测其随声音振动情况的振动传感器3,还内嵌对于细微振动敏感的至少两个振动片2,振动片2与基底1之间通过易碎纸粘结,易碎纸的表面黏附有随机分布的金葱粉7,在基底1上嵌入写入上述振动片2随声音振动幅度变化信息和金葱粉7的分布图像信息的NFC芯片4;防伪识别单元包括用于播放声音并采集振动片2随声音振动幅度变化图像、金葱粉7分布图像和读取NFC芯片4的手持客户端设备(嵌入NFC模块的手机5),振动传感器3和手机5分别与服务器6通信。

[0037] 振动片2为厚度0.2mm的薄铜片。振动片2与基底1之间通过易碎纸粘结,采用易碎纸双面粘结的方式将振动片2与基底1固定在一起,振动片2一旦拉开,易碎纸发生肉眼可见的破损。

[0038] 基底1的底部设有壳体,壳体内设有抗磁干扰装置、控温装置、定位装置、位置信息存储器、警示装置、电源及充电装置(无线充电装置),各个元器件之间填充有柔性材料,以避免商品运输过程中对各个元器件的撞击磕碰;具体如下:

[0039] 控温装置,设定高温和低温两个阈值,控温装置在外界温度高于高温阈值、或低于

低温阈值时自动工作,将壳体内元器件的温度控制在高温阈值和低温阈值之前,保障各元器件的寿命;

[0040] 定位装置和位置信息存储器,能够记录标签的位置变化信息;

[0041] 警示装置,设定报警事件,当报警事件发生时,警示装置发出机械波或电磁波进行警示。

[0042] 防伪系统还包括固定装置和自毁装置,固定装置用于实现基底1与商品的连接,自毁装置在固定装置发生位移或破损时自动启动进而造成以下结果中的至少一种:基底1发生人体肉眼可见的破损;和/或向服务器6发送防伪失效信息。

[0043] 上述防伪系统的制作方法,包括步骤:

[0044] (A) 手机5播放设定的声音片段,振动传感器3采集基底1随声音的振动情况信息,并发送至服务器6存储;

[0045] (B) 采集金葱粉7的分布图像信息,并且在手机5播放上述设定的声音片段时,同时采集相应振动片2随声音的振动幅度图像信息,将金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息通过服务器6运算生成相应的密码信息,并将其写入NFC芯片4内。

[0046] 步骤(B)中密码信息是采用SM3杂凑算法与RC4算法生成的。

[0047] 利用上述防伪系统的一种基于振动信息特征和随机金葱粉的防伪方法,具体步骤如下:

[0048] (1) 手机5采集金葱粉7的分布图像,同时手机5播放设定的声音片段,并采集相应振动片2随声音的振动幅度图像信息,读取NFC芯片4,将这些信息一并发送至服务器6;

[0049] (2) 服务器6根据NFC信息解析(反推算)出金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息,并与步骤(1)采集到的金葱粉7的分布图像和相应振动片2随声音的振动幅度图像信息进行比对,倘若完全一致,进入步骤(3),倘若出现不一致,则判定商品为假,结束;

[0050] (3) 振动传感器3采集基底随声音的振动情况信息实时传送至服务器6,判断其是否与服务器6中存储的振动情况信息完全一致,是则进入步骤(4),否则判定商品为假,结束;

[0051] (4) 将步骤(3)采集到的基底1振动情况信息与相应的金葱粉7分布图像、振动片2振动幅度图像信息匹配,再次请求验伪时,判断再次采集到的基底1振动情况信息是否与金葱粉7分布图像、振动片2振动幅度图像信息匹配,是则判定为真,否则判定商品为假,结束。

[0052] 实施例2:

[0053] 如图1所示的一种基于振动信息特征和随机金葱粉的NFC识别防伪系统,包括防伪特征单元和防伪识别单元两部分,其中,防伪特征单元的主体为商品的不锈钢基底1,基底1上黏附有监测其随声音振动情况的振动传感器3,还内嵌对于细微振动敏感的至少两个振动片2,振动片2与基底1之间通过易碎纸粘结,易碎纸的表面黏附有随机分布的金葱粉7,在基底1上嵌入写入上述振动片2随声音振动幅度变化信息和金葱粉7的分布图像信息的NFC芯片4;防伪识别单元包括用于播放声音并采集振动片2随声音振动幅度变化图像、金葱粉7分布图像和读取NFC芯片4的手持客户端设备(嵌入NFC模块的手机5),振动传感器3和手机5分别与服务器6通信。

[0054] 振动片2为厚度0.3mm的薄铜片。振动片2与基底1之间通过易碎纸粘结,采用易碎纸双面粘结的方式将振动片2与基底1固定在一起,振动片2一旦拉开,易碎纸发生肉眼可见的破损。

[0055] 基底1的底部设有壳体,壳体内设有抗磁干扰装置、控温装置、定位装置、位置信息存储器、警示装置、电源及充电装置(无线充电装置),各个元器件之间填充有柔性材料,以避免商品运输过程中对各个元器件的撞击磕碰;具体如下:

[0056] 控温装置,设定高温和低温两个阈值,控温装置在外界温度高于高温阈值、或低于低温阈值时自动工作,将壳体内元器件的温度控制在高温阈值和低温阈值之前,保障各元器件的寿命;

[0057] 定位装置和位置信息存储器,能够记录标签的位置变化信息;

[0058] 警示装置,设定报警事件,当报警事件发生时,警示装置发出机械波或电磁波进行警示。

[0059] 防伪系统还包括固定装置和自毁装置,固定装置用于实现基底1与商品的连接,自毁装置在固定装置发生位移或破损时自动启动进而造成以下结果中的至少一种:基底1发生肉眼可见的破损;和/或向服务器6发送防伪失效信息。

[0060] 上述防伪系统的制作方法,包括步骤:

[0061] (A) 手机5播放设定的声音片段,振动传感器3采集基底1随声音的振动情况信息,并发送至服务器6存储;

[0062] (B) 采集金葱粉7的分布图像信息,并且在手机5播放上述设定的声音片段时,同时采集相应振动片2随声音的振动幅度图像信息,将金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息通过服务器6运算生成相应的密码信息,并将其写入NFC芯片4内。

[0063] 步骤(B)中密码信息是采用SM3杂凑算法与B-M算法的组合算法生成的。

[0064] 利用上述防伪系统的一种基于振动信息特征和随机金葱粉的防伪方法,具体步骤如下:

[0065] (1) 手机5采集金葱粉7的分布图像,同时手机5播放设定的声音片段,并采集相应振动片2随声音的振动幅度图像信息,读取NFC芯片4,将这些信息一并发送至服务器6;

[0066] (2) 服务器6根据NFC信息解析(反推算)出金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息,并与步骤(1)采集到的金葱粉7的分布图像和相应振动片2随声音的振动幅度图像信息进行比对,倘若完全一致,进入步骤(3),倘若出现不一致,则判定商品为假,结束;

[0067] (3) 振动传感器3采集基底随声音的振动情况信息实时传送至服务器6,判断其是否与服务器6中存储的振动情况信息完全一致,是则进入步骤(4),否则判定商品为假,结束;

[0068] (4) 将步骤(3)采集到的基底1振动情况信息与相应的金葱粉7分布图像、振动片2振动幅度图像信息匹配,再次请求验伪时,判断再次采集到的基底1振动情况信息是否与金葱粉7分布图像、振动片2振动幅度图像信息匹配,是则判定为真,否则判定商品为假,结束。

[0069] 实施例3:

[0070] 如图1所示的一种基于振动信息特征和随机金葱粉的NFC识别防伪系统,包括防伪

特征单元和防伪识别单元两部分,其中,防伪特征单元的主体为商品的不锈钢基底1,基底1上黏附有监测其随声音振动情况的振动传感器3,还内嵌对于细微振动敏感的至少两个振动片2,振动片2与基底1之间通过易碎纸粘结,易碎纸的表面黏附有随机分布的金葱粉7,在基底1上嵌入写入上述振动片2随声音振动幅度变化信息和金葱粉7的分布图像信息的NFC芯片4;防伪识别单元包括用于播放声音并采集振动片2随声音振动幅度变化图像、金葱粉7分布图像和读取NFC芯片4的手持客户端设备(嵌入NFC模块的手机5),振动传感器3和手机5分别与服务器6通信。

[0071] 振动片2为厚度0.2mm的薄铜片。振动片2与基底1之间通过易碎纸粘结,采用易碎纸双面粘结的方式将振动片2与基底1固定在一起,振动片2一旦拉开,易碎纸发生肉眼可见的破损。

[0072] 基底1的底部设有壳体,壳体内设有抗磁干扰装置、控温装置、定位装置、位置信息存储器、警示装置、电源及充电装置(无线充电装置),各个元器件之间填充有柔性材料,以避免商品运输过程中对各个元器件的撞击磕碰;具体如下:

[0073] 控温装置,设定高温和低温两个阈值,控温装置在外界温度高于高温阈值、或低于低温阈值时自动工作,将壳体内元器件的温度控制在高温阈值和低温阈值之前,保障各元器件的寿命;

[0074] 定位装置和位置信息存储器,能够记录标签的位置变化信息;

[0075] 警示装置,设定报警事件,当报警事件发生时,警示装置发出机械波或电磁波进行警示。

[0076] 防伪系统还包括固定装置和自毁装置,固定装置用于实现基底1与商品的连接,自毁装置在固定装置发生位移或破损时自动启动进而造成以下结果中的至少一种:基底1发生人体肉眼可见的破损;和/或向服务器6发送防伪失效信息。

[0077] 上述防伪系统的制作方法,包括步骤:

[0078] (A) 手机5播放设定的声音片段,振动传感器3采集基底1随声音的振动情况信息,并发送至服务器6存储;

[0079] (B) 采集金葱粉7的分布图像信息,并且在手机5播放上述设定的声音片段时,同时采集相应振动片2随声音的振动幅度图像信息,将金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息通过服务器6运算生成相应的密码信息,并将其写入NFC芯片4内。

[0080] 步骤(B)中密码信息是采用SM3杂凑算法与MD5算法的组合算法生成的。

[0081] 利用上述防伪系统的一种基于振动信息特征和随机金葱粉的防伪方法,具体步骤如下:

[0082] (1) 手机5采集金葱粉7的分布图像,同时手机5播放设定的声音片段,并采集相应振动片2随声音的振动幅度图像信息,读取NFC芯片4,将这些信息一并发送至服务器6;

[0083] (2) 服务器6根据NFC信息解析(反推算)出金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息,并与步骤(1)采集到的金葱粉7的分布图像和相应振动片2随声音的振动幅度图像信息进行比对,倘若完全一致,进入步骤(3),倘若出现不一致,则判定商品为假,结束;

[0084] (3) 振动传感器3采集基底随声音的振动情况信息实时传送至服务器6,判断其是

否与服务器6中存储的振动情况信息完全一致,是则进入步骤(4),否则判定商品为假,结束;

[0085] (4)将步骤(3)采集到的基底1振动情况信息与相应的金葱粉7分布图像、振动片2振动幅度图像信息匹配,再次请求验伪时,判断再次采集到的基底1振动情况信息是否与金葱粉7分布图像、振动片2振动幅度图像信息匹配,是则判定为真,否则判定商品为假,结束。

[0086] 实施例4:

[0087] 如图1所示的一种基于振动信息特征和随机金葱粉的NFC识别防伪系统,包括防伪特征单元和防伪识别单元两部分,其中,防伪特征单元的主体为商品的不锈钢基底1,基底1上黏附有监测其随声音振动情况的振动传感器3,还内嵌对于细微振动敏感的至少两个振动片2,振动片2与基底1之间通过易碎纸粘结,易碎纸的表面黏附有随机分布的金葱粉7,在基底1上嵌入写入上述振动片2随声音振动幅度变化信息和金葱粉7的分布图像信息的NFC芯片4;防伪识别单元包括用于播放声音并采集振动片2随声音振动幅度变化图像、金葱粉7分布图像和读取NFC芯片4的手持客户端设备(嵌入NFC模块的手机5),振动传感器3和手机5分别与服务器6通信。

[0088] 振动片2为厚度0.3mm的薄铜片。振动片2与基底1之间通过易碎纸粘结,采用易碎纸双面粘结的方式将振动片2与基底1固定在一起,振动片2一旦拉开,易碎纸发生肉眼可见的破损。

[0089] 基底1的底部设有壳体,壳体内设有抗磁干扰装置、控温装置、定位装置、位置信息存储器、警示装置、电源及充电装置(无线充电装置),各个元器件之间填充有柔性材料,以避免商品运输过程中对各个元器件的撞击磕碰;具体如下:

[0090] 控温装置,设定高温和低温两个阈值,控温装置在外界温度高于高温阈值、或低于低温阈值时自动工作,将壳体内元器件的温度控制在高温阈值和低温阈值之前,保障各元器件的寿命;

[0091] 定位装置和位置信息存储器,能够记录标签的位置变化信息;

[0092] 警示装置,设定报警事件,当报警事件发生时,警示装置发出机械波或电磁波进行警示。

[0093] 防伪系统还包括固定装置和自毁装置,固定装置用于实现基底1与商品的连接,自毁装置在固定装置发生位移或破损时自动启动进而造成以下结果中的至少一种:基底1发生人体肉眼可见的破损;和/或向服务器6发送防伪失效信息。

[0094] 上述防伪系统的制作方法,包括步骤:

[0095] (A)手机5播放设定的声音片段,振动传感器3采集基底1随声音的振动情况信息,并发送至服务器6存储;

[0096] (B)采集金葱粉7的分布图像信息,并且在手机5播放上述设定的声音片段时,同时采集相应振动片2随声音的振动幅度图像信息,将金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息通过服务器6运算生成相应的密码信息,并将其写入NFC芯片4内。

[0097] 步骤(B)中密码信息是采用SM3杂凑算法与A5算法的组合算法生成的。

[0098] 利用上述防伪系统的一种基于振动信息特征和随机金葱粉的防伪方法,具体步骤如下:

[0099] (1) 手机5采集金葱粉7的分布图像,同时手机5播放设定的声音片段,并采集相应振动片2随声音的振动幅度图像信息,读取NFC芯片4,将这些信息一并发送至服务器6;

[0100] (2) 服务器6根据NFC信息解析(反推算)出金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息,并与步骤(1)采集到的金葱粉7的分布图像和相应振动片2随声音的振动幅度图像信息进行比对,倘若完全一致,进入步骤(3),倘若出现不一致,则判定商品为假,结束;

[0101] (3) 振动传感器3采集基底随声音的振动情况信息实时传送至服务器6,判断其是否与服务器6中存储的振动情况信息完全一致,是则进入步骤(4),否则判定商品为假,结束;

[0102] (4) 将步骤(3)采集到的基底1振动情况信息与相应的金葱粉7分布图像、振动片2振动幅度图像信息匹配,再次请求验伪时,判断再次采集到的基底1振动情况信息是否与金葱粉7分布图像、振动片2振动幅度图像信息匹配,是则判定为真,否则判定商品为假,结束。

[0103] 实施例5:

[0104] 如图1所示的一种基于振动信息特征和随机金葱粉的NFC识别防伪系统,包括防伪特征单元和防伪识别单元两部分,其中,防伪特征单元的主体为商品的不锈钢基底1,基底1上黏附有监测其随声音振动情况的振动传感器3,还内嵌对于细微振动敏感的至少两个振动片2,振动片2与基底1之间通过易碎纸粘结,易碎纸的表面黏附有随机分布的金葱粉7,在基底1上嵌入写入上述振动片2随声音振动幅度变化信息和金葱粉7的分布图像信息的NFC芯片4;防伪识别单元包括用于播放声音并采集振动片2随声音振动幅度变化图像、金葱粉7分布图像和读取NFC芯片4的手持客户端设备(嵌入NFC模块的手机5),振动传感器3和手机5分别与服务器6通信。

[0105] 振动片2为厚度0.2mm的薄铜片。振动片2与基底1之间通过易碎纸粘结,采用易碎纸双面粘结的方式将振动片2与基底1固定在一起,振动片2一旦拉开,易碎纸发生肉眼可见的破损。

[0106] 基底1的底部设有壳体,壳体内设有抗磁干扰装置、控温装置、定位装置、位置信息存储器、警示装置、电源及充电装置(无线充电装置),各个元器件之间填充有柔性材料,以避免商品运输过程中对各个元器件的撞击磕碰;具体如下:

[0107] 控温装置,设定高温和低温两个阈值,控温装置在外界温度高于高温阈值、或低于低温阈值时自动工作,将壳体内元器件的温度控制在高温阈值和低温阈值之前,保障各元器件的寿命;

[0108] 定位装置和位置信息存储器,能够记录标签的位置变化信息;

[0109] 警示装置,设定报警事件,当报警事件发生时,警示装置发出机械波或电磁波进行警示。

[0110] 防伪系统还包括固定装置和自毁装置,固定装置用于实现基底1与商品的连接,自毁装置在固定装置发生位移或破损时自动启动进而造成以下结果中的至少一种:基底1发生肉眼可见的破损;和/或向服务器6发送防伪失效信息。

[0111] 上述防伪系统的制作方法,包括步骤:

[0112] (A) 手机5播放设定的声音片段,振动传感器3采集基底1随声音的振动情况信息,并发送至服务器6存储;

[0113] (B) 采集金葱粉7的分布图像信息,并且在手机5播放上述设定的声音片段时,同时采集相应振动片2随声音的振动幅度图像信息,将金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息通过服务器6运算生成相应的密码信息,并将其写入NFC芯片4内。

[0114] 步骤(B)中密码信息是采用SM3杂凑算法与SEAL算法的组合算法生成的。

[0115] 利用上述防伪系统的一种基于振动信息特征和随机金葱粉的防伪方法,具体步骤如下:

[0116] (1) 手机5采集金葱粉7的分布图像,同时手机5播放设定的声音片段,并采集相应振动片2随声音的振动幅度图像信息,读取NFC芯片4,将这些信息一并发送至服务器6;

[0117] (2) 服务器6根据NFC信息解析(反推算)出金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息,并与步骤(1)采集到的金葱粉7的分布图像和相应振动片2随声音的振动幅度图像信息进行比对,倘若完全一致,进入步骤(3),倘若出现不一致,则判定商品为假,结束;

[0118] (3) 振动传感器3采集基底随声音的振动情况信息实时传送至服务器6,判断其是否与服务器6中存储的振动情况信息完全一致,是则进入步骤(4),否则判定商品为假,结束;

[0119] (4) 将步骤(3)采集到的基底1振动情况信息与相应的金葱粉7分布图像、振动片2振动幅度图像信息匹配,再次请求验伪时,判断再次采集到的基底1振动情况信息是否与金葱粉7分布图像、振动片2振动幅度图像信息匹配,是则判定为真,否则判定商品为假,结束。

[0120] 实施例6:

[0121] 如图1所示的一种基于振动信息特征和随机金葱粉的NFC识别防伪系统,包括防伪特征单元和防伪识别单元两部分,其中,防伪特征单元的主体为商品的不锈钢基底1,基底1上黏附有监测其随声音振动情况的振动传感器3,还内嵌对于细微振动敏感的至少两个振动片2,振动片2与基底1之间通过易碎纸粘结,易碎纸的表面黏附有随机分布的金葱粉7,在基底1上嵌入写入上述振动片2随声音振动幅度变化信息和金葱粉7的分布图像信息的NFC芯片4;防伪识别单元包括用于播放声音并采集振动片2随声音振动幅度变化图像、金葱粉7分布图像和读取NFC芯片4的手持客户端设备(嵌入NFC模块的手机5),振动传感器3和手机5分别与服务器6通信。

[0122] 振动片2为厚度0.2mm的薄铜片。振动片2与基底1之间通过易碎纸粘结,采用易碎纸双面粘结的方式将振动片2与基底1固定在一起,振动片2一旦拉开,易碎纸发生肉眼可见的破损。

[0123] 基底1的底部设有壳体,壳体内设有抗磁干扰装置、控温装置、定位装置、位置信息存储器、警示装置、电源及充电装置(无线充电装置),各个元器件之间填充有柔性材料,以避免商品运输过程中对各个元器件的撞击磕碰;具体如下:

[0124] 控温装置,设定高温和低温两个阈值,控温装置在外界温度高于高温阈值、或低于低温阈值时自动工作,将壳体内元器件的温度控制在高温阈值和低温阈值之前,保障各元器件的寿命;

[0125] 定位装置和位置信息存储器,能够记录标签的位置变化信息;

[0126] 警示装置,设定报警事件,当报警事件发生时,警示装置发出机械波或电磁波进行

警示。

[0127] 防伪系统还包括固定装置和自毁装置,固定装置用于实现基底1与商品的连接,自毁装置在固定装置发生位移或破损时自动启动进而造成以下结果中的至少一种:基底1发生人体肉眼可见的破损;和/或向服务器6发送防伪失效信息。

[0128] 上述防伪系统的制作方法,包括步骤:

[0129] (A) 手机5播放设定的声音片段,振动传感器3采集基底1随声音的振动情况信息,并发送至服务器6存储;

[0130] (B) 采集金葱粉7的分布图像信息,并且在手机5播放上述设定的声音片段时,同时采集相应振动片2随声音的振动幅度图像信息,将金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息通过服务器6运算生成相应的密码信息,并将其写入NFC芯片4内。

[0131] 步骤(B)中密码信息是采用SM3杂凑算法与RC4算法和B-M算法的组合算法生成的。

[0132] 利用上述防伪系统的一种基于振动信息特征和随机金葱粉的防伪方法,具体步骤如下:

[0133] (1) 手机5采集金葱粉7的分布图像,同时手机5播放设定的声音片段,并采集相应振动片2随声音的振动幅度图像信息,读取NFC芯片4,将这些信息一并发送至服务器6;

[0134] (2) 服务器6根据NFC信息解析(反推算)出金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息,并与步骤(1)采集到的金葱粉7的分布图像和相应振动片2随声音的振动幅度图像信息进行比对,倘若完全一致,进入步骤(3),倘若出现不一致,则判定商品为假,结束;

[0135] (3) 振动传感器3采集基底随声音的振动情况信息实时传送至服务器6,判断其是否与服务器6中存储的振动情况信息完全一致,是则进入步骤(4),否则判定商品为假,结束;

[0136] (4) 将步骤(3)采集到的基底1振动情况信息与相应的金葱粉7分布图像、振动片2振动幅度图像信息匹配,再次请求验伪时,判断再次采集到的基底1振动情况信息是否与金葱粉7分布图像、振动片2振动幅度图像信息匹配,是则判定为真,否则判定商品为假,结束。

[0137] 实施例7:

[0138] 如图1所示的一种基于振动信息特征和随机金葱粉的NFC识别防伪系统,包括防伪特征单元和防伪识别单元两部分,其中,防伪特征单元的主体为商品的不锈钢基底1,基底1上黏附有监测其随声音振动情况的振动传感器3,还内嵌对于细微振动敏感的至少两个振动片2,振动片2与基底1之间通过易碎纸粘结,易碎纸的表面黏附有随机分布的金葱粉7,在基底1上嵌入写入上述振动片2随声音振动幅度变化信息和金葱粉7的分布图像信息的NFC芯片4;防伪识别单元包括用于播放声音并采集振动片2随声音振动幅度变化图像、金葱粉7分布图像和读取NFC芯片4的手持客户端设备(嵌入NFC模块的手机5),振动传感器3和手机5分别与服务器6通信。

[0139] 振动片2为厚度0.3mm的薄铜片。振动片2与基底1之间通过易碎纸粘结,采用易碎纸双面粘结的方式将振动片2与基底1固定在一起,振动片2一旦拉开,易碎纸发生肉眼可见的破损。

[0140] 基底1的底部设有壳体,壳体内设有抗磁干扰装置、控温装置、定位装置、位置信息

存储器、警示装置、电源及充电装置(无线充电装置),各个元器件之间填充有柔性材料,以避免商品运输过程中对各个元器件的撞击磕碰;具体如下:

[0141] 控温装置,设定高温和低温两个阈值,控温装置在外界温度高于高温阈值、或低于低温阈值时自动工作,将壳体内元器件的温度控制在高温阈值和低温阈值之前,保障各元器件的寿命;

[0142] 定位装置和位置信息存储器,能够记录标签的位置变化信息;

[0143] 警示装置,设定报警事件,当报警事件发生时,警示装置发出机械波或电磁波进行警示。

[0144] 防伪系统还包括固定装置和自毁装置,固定装置用于实现基底1与商品的连接,自毁装置在固定装置发生位移或破损时自动启动进而造成以下结果中的至少一种:基底1发生肉眼可见的破损;和/或向服务器6发送防伪失效信息。

[0145] 上述防伪系统的制作方法,包括步骤:

[0146] (A) 手机5播放设定的声音片段,振动传感器3采集基底1随声音的振动情况信息,并发送至服务器6存储;

[0147] (B) 采集金葱粉7的分布图像信息,并且在手机5播放上述设定的声音片段时,同时采集相应振动片2随声音的振动幅度图像信息,将金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息通过服务器6运算生成相应的密码信息,并将其写入NFC芯片4内。

[0148] 步骤(B)中密码信息是采用SM3杂凑算法与B-M算法和MD5算法的组合算法生成的。

[0149] 利用上述防伪系统的一种基于振动信息特征和随机金葱粉的防伪方法,具体步骤如下:

[0150] (1) 手机5采集金葱粉7的分布图像,同时手机5播放设定的声音片段,并采集相应振动片2随声音的振动幅度图像信息,读取NFC芯片4,将这些信息一并发送至服务器6;

[0151] (2) 服务器6根据NFC信息解析(反推算)出金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息,并与步骤(1)采集到的金葱粉7的分布图像和相应振动片2随声音的振动幅度图像信息进行比对,倘若完全一致,进入步骤(3),倘若出现不一致,则判定商品为假,结束;

[0152] (3) 振动传感器3采集基底随声音的振动情况信息实时传送至服务器6,判断其是否与服务器6中存储的振动情况信息完全一致,是则进入步骤(4),否则判定商品为假,结束;

[0153] (4) 将步骤(3)采集到的基底1振动情况信息与相应的金葱粉7分布图像、振动片2振动幅度图像信息匹配,再次请求验伪时,判断再次采集到的基底1振动情况信息是否与金葱粉7分布图像、振动片2振动幅度图像信息匹配,是则判定为真,否则判定商品为假,结束。

[0154] 实施例8:

[0155] 如图1所示的一种基于振动信息特征和随机金葱粉的NFC识别防伪系统,包括防伪特征单元和防伪识别单元两部分,其中,防伪特征单元的主体为商品的不锈钢基底1,基底1上黏附有监测其随声音振动情况的振动传感器3,还内嵌对于细微振动敏感的至少两个振动片2,振动片2与基底1之间通过易碎纸粘结,易碎纸的表面黏附有随机分布的金葱粉7,在基底1上嵌入写入上述振动片2随声音振动幅度变化信息和金葱粉7的分布图像信息的NFC

芯片4;防伪识别单元包括用于播放声音并采集振动片2随声音振动幅度变化图像、金葱粉7分布图像和读取NFC芯片4的手持客户端设备(嵌入NFC模块的手机5),振动传感器3和手机5分别与服务器6通信。

[0156] 振动片2为厚度0.2mm的薄铜片。振动片2与基底1之间通过易碎纸粘结,采用易碎纸双面粘结的方式将振动片2与基底1固定在一起,振动片2一旦拉开,易碎纸发生肉眼可见的破损。

[0157] 基底1的底部设有壳体,壳体内设有抗磁干扰装置、控温装置、定位装置、位置信息存储器、警示装置、电源及充电装置(无线充电装置),各个元器件之间填充有柔性材料,以避免商品运输过程中对各个元器件的撞击磕碰;具体如下:

[0158] 控温装置,设定高温和低温两个阈值,控温装置在外界温度高于高温阈值、或低于低温阈值时自动工作,将壳体内元器件的温度控制在高温阈值和低温阈值之前,保障各元器件的寿命;

[0159] 定位装置和位置信息存储器,能够记录标签的位置变化信息;

[0160] 警示装置,设定报警事件,当报警事件发生时,警示装置发出机械波或电磁波进行警示。

[0161] 防伪系统还包括固定装置和自毁装置,固定装置用于实现基底1与商品的连接,自毁装置在固定装置发生位移或破损时自动启动进而造成以下结果中的至少一种:基底1发生肉眼可见的破损;和/或向服务器6发送防伪失效信息。

[0162] 上述防伪系统的制作方法,包括步骤:

[0163] (A) 手机5播放设定的声音片段,振动传感器3采集基底1随声音的振动情况信息,并发送至服务器6存储;

[0164] (B) 采集金葱粉7的分布图像信息,并且在手机5播放上述设定的声音片段时,同时采集相应振动片2随声音的振动幅度图像信息,将金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息通过服务器6运算生成相应的密码信息,并将其写入NFC芯片4内。

[0165] 步骤(B)中密码信息是采用SM3杂凑算法与A5算法和SEAL算法的组合算法生成的。

[0166] 利用上述防伪系统的一种基于振动信息特征和随机金葱粉的防伪方法,具体步骤如下:

[0167] (1) 手机5采集金葱粉7的分布图像,同时手机5播放设定的声音片段,并采集相应振动片2随声音的振动幅度图像信息,读取NFC芯片4,将这些信息一并发送至服务器6;

[0168] (2) 服务器6根据NFC信息解析(反推算)出金葱粉7的分布图像信息和相应振动片2随声音的振动幅度图像信息,并与步骤(1)采集到的金葱粉7的分布图像和相应振动片2随声音的振动幅度图像信息进行比对,倘若完全一致,进入步骤(3),倘若出现不一致,则判定商品为假,结束;

[0169] (3) 振动传感器3采集基底随声音的振动情况信息实时传送至服务器6,判断其是否与服务器6中存储的振动情况信息完全一致,是则进入步骤(4),否则判定商品为假,结束;

[0170] (4) 将步骤(3)采集到的基底1振动情况信息与相应的金葱粉7分布图像、振动片2振动幅度图像信息匹配,再次请求验伪时,判断再次采集到的基底1振动情况信息是否与金

葱粉7分布图像、振动片2振动幅度图像信息匹配,是则判定为真,否则判定商品为假,结束。

[0171] 上述虽然结合附图对本发明的具体实施方式进行了描述,但并非对本发明保护范围的限制,在本发明的技术方案的基础上,本领域技术人员不需要付出创造性劳动即可做出的各种修改或变形仍在本发明的保护范围以内。

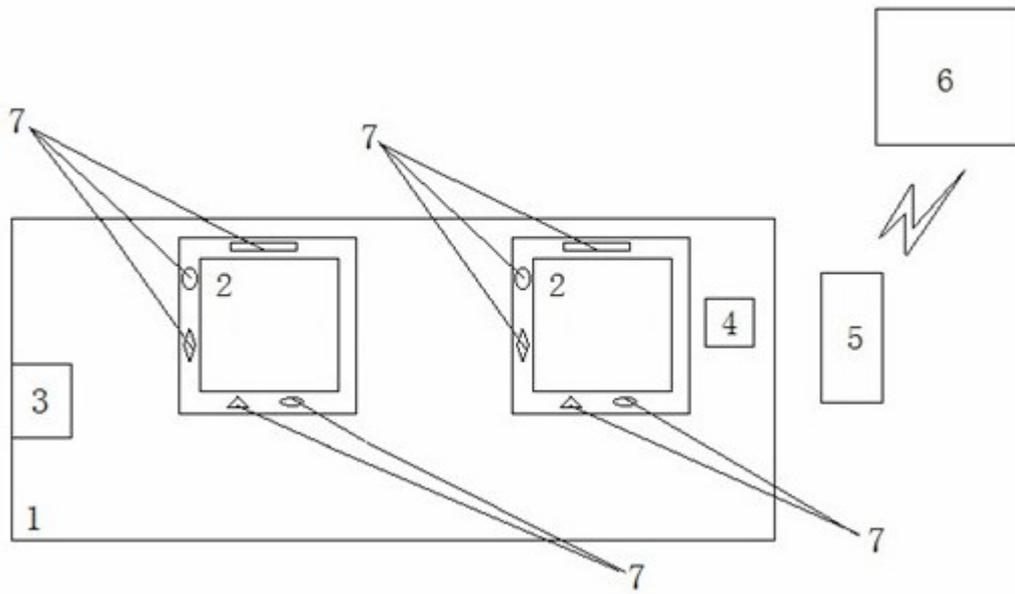


图1