(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112488272 B
(45)授权公告日 2023.01.31

(21)申请号 202011228593.9
(22)申请日 2020.11.05
(65)同一申请的已公布的文献号
申请公布号 CN 112488272 A
(43)申请公布日 2021.03.12
(73)专利权人 香港理工大学深圳研究院
地址 518057 广东省深圳市南山区粤海街道高新技术产业园南区粤兴一道18号香港理工大学产学研大楼205室
(72)发明人 杨燕妮 曹建农
(74)专利代理机构 深圳市君胜知识产权代理事务所(普通合伙) 44268
专利代理师 谢松
(51)Int.Cl.
*G06K 19/077*(2006.01)
*G06K 7/10*(2006.01)

审查员 史玉梅

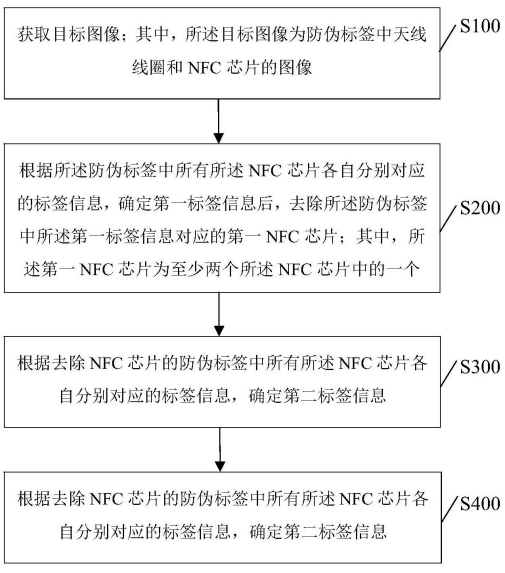
权利要求书2页 说明书8页 附图2页

(54)发明名称

一种多NFC芯片融合的防伪标签及其验证方法

(57)摘要

本发明公开了一种多NFC芯片融合的防伪标签及其验证方法，多NFC芯片融合的防伪标签包括:标签本体;天线线圈，所述天线线圈嵌设在所述标签本体内;NFC芯片，所述NFC芯片嵌设在所述标签本体内，并与所述天线线圈连接;其中，所述NFC芯片有至少两个，各所述NFC芯片分别连接在所述天线线圈不同位置。由于本申请中的防伪标签中有至少两个NFC芯片，当NFC阅读器的读取范围内出现多个NFC芯片时，NFC阅读器会固定地选择读取其中一个NFC芯片中的标签信息。当标签仿造者试图通过窃听标签的标签信息时，而无法获得所有NFC芯片的标签，因此无法复制出完整的NFC芯片的标签信息。




CN 112488272 B

1.一种多NFC芯片融合的防伪标签的验证方法,其特征在于,所述防伪标签包括:

标签本体;

天线线圈,所述天线线圈嵌设在所述标签本体内;

NFC芯片,所述NFC芯片嵌设在所述标签本体内,并与所述天线线圈连接;

其中,所述NFC芯片有至少两个,各所述NFC芯片分别连接在所述天线线圈不同位置;

各所述NFC芯片中存储的标签信息各不相同;

所述验证方法包括步骤:

获取防伪标签对应的目标图像;其中,所述目标图像为所述防伪标签中天线线圈和NFC芯片的图像;

确定第一标签信息后,去除所述防伪标签中所述第一标签信息对应的第一NFC芯片;其中,所述第一NFC芯片为至少两个所述NFC芯片中的一个;

确定第二标签信息;

根据所述第一标签信息、所述第二标签信息以及所述目标图像对所述防伪标签进行验证,得到验证结果;

各所述NFC芯片按照NFC阅读器的读取顺序编号;

所述确定第一标签信息后,去除所述防伪标签中所述第一标签信息对应的第一NFC芯片,包括:

通过NFC阅读器读取所述防伪标签中所有所述NFC芯片各自分别对应的标签信息;

将所述NFC阅读器读取到的标签信息作为第一标签信息;

将编号排在第一位的NFC芯片作为所述第一标签信息对应的第一NFC芯片,并去除所述第一NFC芯片;

所述确定第二标签信息,包括:

通过所述NFC阅读器读取去除NFC芯片的防伪标签中所有所述NFC芯片各自分别对应的标签信息;

将所述NFC阅读器读取到的标签信息作为第二标签信息;

所述根据所述第一标签信息、所述第二标签信息以及所述目标图像对所述防伪标签进行验证,得到验证结果,包括:

根据所述第一标签信息和所述第二标签信息,确定所述防伪标签对应的标识码;

当所述标识码和预设标识码匹配时,获取所述预设标识码对应的预设图像;

当所述预设图像和所述目标图像匹配时,所述防伪标签验证通过。

2.根据权利要求1所述的验证方法,其特征在于,各所述NFC芯片焊接在天线线圈上。

3.根据权利要求1所述的验证方法,其特征在于,所述预设图像为制作所述防伪标签时所述第一标签信息对应的第一原始NFC芯片、所述第二标签信息对应的第二原始NFC芯片以及原始天线线圈的图像;所述第一原始NFC芯片与所述原始天线线圈的连接位置为第一原始位置,所述第二原始NFC芯片与所述原始天线线圈的连接位置为第二原始位置;所述第二标签信息为至少两个所述NFC芯片中第二NFC芯片存储的标签信息;所述第一NFC芯片与所述天线线圈的连接位置为第一连接位置,所述第二NFC芯片与所述天线线圈的连接位置为第二连接位置;

所述当所述预设图像和所述目标图像匹配时,所述防伪标签验证通过,包括:

当所述预设图像中所述第一原始NFC芯片的位置、所述第二原始NFC芯片的位置、所述第一原始位置以及所述第二原始位置，分别与所述目标图像中所述第一NFC芯片的位置、所述第二NFC芯片的位置、所述第一连接位置、所述第二连接位置一致时，所述防伪标签验证通过。

4.根据权利要求1所述的验证方法，其特征在于，所述验证方法还包括：

当所述预设图像和所述目标图像不匹配时，所述防伪标签验证不通过。

5.根据权利要求1所述的验证方法，其特征在于，所述验证方法还包括：

当所述标识码和预设标识码不匹配时，所述防伪标签验证不通过。

# 一种多NFC芯片融合的防伪标签及其验证方法

## 技术领域

[0001] 本发明涉及防伪标签技术领域，尤其涉及的是一种多NFC芯片融合的防伪标签及其验证方法。

## 背景技术

[0002] 在当今商品伪造技术不断进化的背景下，商品防伪对于保护生产商和消费者的权益有着重要的意义。传统的二维码容易被复制和伪造，不能可靠地实现商品防伪。随着NFC技术的出现，NFC标签被广泛使用在商品防伪中。

[0003] 现有技术中，为了防止NFC标签的信息被复制，NFC标签的ID及其他信息通过加密算法进行信息保护。但解密的密钥容易被窃取和破解，因此即使经过加密，NFC标签的信息也会被暴露。此外，NFC标签的信息容易被修改，导致其信息不可信。最后，合法的NFC标签在使用过后，会出现被恶意继续使用在仿造的商品上，造成消费者被欺骗的情况，而对NFC信息进行加密的方法无法检测出NFC标签被重复使用的问题。

[0004] 因此，现有技术还有待于改进和发展。

## 发明内容

[0005] 本发明要解决的技术问题在于，针对现有技术的上述缺陷，提供一种多NFC芯片融合的防伪标签及其验证方法，旨在解决现有技术中NFC标签容易伪造的问题。

[0006] 本发明解决技术问题所采用的技术方案如下：

[0007] 一种多NFC芯片融合的防伪标签，其中，所述防伪标签包括：

[0008] 标签本体；

[0009] 天线线圈，所述天线线圈嵌设在所述标签本体内；

[0010] NFC芯片，所述NFC芯片嵌设在所述标签本体内，并与所述天线线圈连接；

[0011] 其中，所述NFC芯片有至少两个，各所述NFC芯片分别连接在所述天线线圈不同位置。

[0012] 所述的防伪标签，其中，各所述NFC芯片中存储的标签信息各不相同。

[0013] 所述的防伪标签，其中，各所述NFC芯片焊接在天线线圈上。

[0014] 一种如上述任意一项所述多NFC芯片融合的防伪标签的验证方法，其中，包括步骤：

[0015] 获取防伪标签对应的目标图像；其中，所述目标图像为所述防伪标签中天线线圈和NFC芯片的图像；

[0016] 确定第一标签信息后，去除所述防伪标签中所述第一标签信息对应的第一NFC芯片；其中，所述第一NFC芯片为至少两个所述NFC芯片中的一个；

[0017] 确定第二标签信息；

[0018] 根据所述第一标签信息、所述第二标签信息以及所述目标图像对所述防伪标签进行验证，得到验证结果。

[0019] 所述的验证方法，其中，各所述NFC芯片按照NFC阅读器的读取顺序编号；

[0020] 所述确定第一标签信息后，去除所述防伪标签中所述第一标签信息对应的第一NFC芯片，包括：

[0021] 通过NFC阅读器读取所述防伪标签中所有所述NFC芯片各自分别对应的标签信息；

[0022] 将所述NFC阅读器读取到的标签信息作为第一标签信息；

[0023] 将编号排在第一位的NFC芯片作为所述第一标签信息对应的第一NFC芯片，并去除所述第一NFC芯片。

[0024] 所述的验证方法，其中，所述确定第二标签信息，包括：

[0025] 通过所述NFC阅读器读取去除NFC芯片的防伪标签中所有所述NFC芯片各自分别对应的标签信息；

[0026] 将所述NFC阅读器读取到的标签信息作为第二标签信息。

[0027] 所述的验证方法，其中，所述根据所述第一标签信息、所述第二标签信息以及所述目标图像对所述防伪标签进行验证，得到验证结果，包括：

[0028] 根据所述第一标签信息和所述第二标签信息，确定所述防伪标签对应的标识码；

[0029] 当所述标识码和预设标识码匹配时，获取所述预设标识码对应的预设图像；

[0030] 当所述预设图像和所述目标图像匹配时，所述防伪标签验证通过。

[0031] 所述的验证方法，其中，所述预设图像为制作所述防伪标签时所述第一标签信息对应的第一原始NFC芯片、所述第二标签信息对应的第二原始NFC芯片以及原始天线线圈的图像；所述第一原始NFC芯片与所述原始天线线圈的连接位置为第一原始位置，所述第二原始NFC芯片与所述原始天线线圈的连接位置为第二原始位置；所述第二标签信息为至少两个所述NFC芯片中第二NFC芯片存储的标签信息；所述第一NFC芯片与所述天线线圈的连接位置为第一连接位置，所述第二NFC芯片与所述天线线圈的连接位置为第二连接位置；

[0032] 所述当所述预设图像和所述目标图像匹配时，所述防伪标签验证通过，包括：

[0033] 当所述预设图像中所述第一原始NFC芯片的位置、所述第二原始NFC芯片的位置、所述第一原始位置以及所述第二原始位置，分别与所述目标图像中所述第一NFC芯片的位置、所述第二NFC芯片的位置、所述第一连接位置、所述第二连接位置一致时，所述防伪标签验证通过。

[0034] 所述的验证方法，其中，所述验证方法还包括：

[0035] 当所述预设图像和所述目标图像不匹配时，所述防伪标签验证不通过。

[0036] 所述的验证方法，其中，所述验证方法还包括：

[0037] 当所述标识码和预设标识码不匹配时，所述防伪标签验证不通过。

[0038] 有益效果：由于本申请中的防伪标签中有至少两个NFC芯片，当NFC阅读器的读取范围内出现多个NFC芯片时，NFC阅读器会固定地选择读取其中一个NFC芯片中的标签信息。当标签仿造者试图通过窃听标签的标签信息时，而无法获得所有NFC芯片的标签，因此无法复制出完整的NFC芯片的标签信息。

## 附图说明

[0039] 图1是本发明中多NFC芯片融合的防伪标签的制作流程图。

[0040] 图2是本发明中多NFC芯片融合的防伪标签的验证流程图。

[0041] 图3是多本发明中NFC芯片融合的防伪标签的验证方法的流程图。

## 具体实施方式

[0042] 为使本发明的目的、技术方案及优点更加清楚、明确，以下参照附图并举实施例对本发明进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0043] 请同时参阅图1-图3，本发明提供了一种多NFC芯片融合的防伪标签的一些实施例。

[0044] 如图1-图2所示，本发明的一种多NFC芯片融合的防伪标签，包括：

[0045] 标签本体；

[0046] 天线线圈，所述天线线圈嵌设在所述标签本体内；

[0047] NFC芯片，所述NFC芯片嵌设在所述标签本体内，并与所述天线线圈连接；

[0048] 其中，所述NFC芯片有至少两个，各所述NFC芯片分别连接在所述天线线圈不同位置。

[0049] 值得说明的是，由于本申请中的防伪标签中有至少两个NFC芯片，本发明利用了NFC协议中的防冲突机制，当NFC阅读器的读取范围内出现多个NFC芯片时，NFC阅读器会固定地选择读取其中一个NFC芯片中的ID等信息，其他NFC芯片的ID信息都无法读到，因此其他NFC芯片的ID信息就被成功掩埋了。当标签仿造者试图通过窃听标签的ID信息时，只能获取其中一个NFC芯片的ID，而无法获得所有NFC芯片的ID，因此无法复制出完整的NFC标签信息。同理，NFC标签信息的篡改者也只能写入恶意信息到其中的一个NFC芯片中，而无法篡改所有芯片的信息。

[0050] 此外，由于多个NFC芯片在被焊接在天线线圈上的位置和焊点的位置极难复现，因此，多个NFC芯片的位置及焊点的位置可以作为标签唯一的指纹。当标签仿造者试图破坏标签，来分别读取各个NFC芯片的ID时，其仍需要还原一个与被仿造标签的芯片位置和焊点位置完全一样的标签，而仿造者并无法复原出这样一个标签。该步骤进一步增强了NFC标签防伪造的功能。

[0051] 具体地，标签本体采用封装结构，将天线线圈和NFC芯片封装起来，例如，标签本体包括第一封装层和第二封装层，天线线圈和NFC芯片位于第一封装层和第二封装层之间，第一封装层和第二封装层可以采用胶水等粘接剂进行连接。

[0052] 为了方便说明，以两个NFC芯片为例进行说明。

[0053] 在本发明实施例的一个较佳实现方式中，如图1-图2所示，各所述NFC芯片中存储的标签信息各不相同。标签信息包括：ID信息，当然，除了ID信息，标签信息还可以包括附加信息。

[0054] 具体地，两个NFC芯片{C1,C2}，两个NFC芯片的ID{ID1,ID2}，两个ID唯一且不同，也就是说，ID1和ID2是唯一的，ID1和ID2是不相同的。

[0055] 在本发明实施例的一个较佳实现方式中，如图1-图2所示，各所述NFC芯片焊接在天线线圈上。

[0056] 具体地，NFC芯片是焊接在天线线圈上的，NFC芯片与天线线圈连接处为焊点。

[0057] 基于上述任一实施例所述的防伪标签，本发明还提供了一种多NFC芯片融合的防

伪标签的验证方法的较佳实施例：

[0058] 本发明中防伪标签的制作方法包括以下步骤：

[0059] 步骤A10、提供天线线圈和至少两个NFC芯片。

[0060] 具体地，每个NFC芯片都有唯一的ID，这里的ID可以是序列号。例如，采用n个NFC芯片时，各NFC芯片的ID为{ID1，ID2，ID3，・・・，IDn}。

[0061] 步骤A20、对各NFC芯片进行编号，并将各NFC芯片连接在天线线圈上。

[0062] 由于多个NFC芯片连接在天线线圈上，采用NFC阅读器读取标签信息时，并不是所有NFC芯片的标签信息都会读取，而是只读取多个NFC芯片中的一个，因此，需要对各NFC芯片进行编号，具体地，各NFC芯片按照NFC阅读器的读取顺序编号，NFC阅读器在读取NFC芯片时，只会读取编号排在第一位的NFC芯片中的标签信息。举例说明，多个NFC芯片的编号分别为a，b，c，・・・，z，此时，a排在第一位，编号为a的NFC芯片会被NFC阅读器读取，其余NFC芯片会被淹没。再如，多个NFC芯片的编号分别为b，c，d，z，此时，b排在第一位，编号为b的NFC芯片会被NFC阅读器读取，其余NFC芯片会被淹没。再如，多个NFC芯片的编号分别为f，w，c，z，此时，c排在第一位，编号为c的NFC芯片会被NFC阅读器读取，其余NFC芯片会被淹没。也就是说，采用具有顺序的标识对多个NFC芯片进行编号。

[0063] 具体地，在对各NFC芯片编号时，如果只有两个NFC芯片，可以直接先将一个NFC芯片连接在天线线圈上，并采用NFC阅读器进行读取，则可以读取到该NFC芯片的标签信息，例如，读取到ID1，然后将另一个NFC芯片连接在天线线圈上，并采用NFC阅读器进行读取，则可以读取到两个NFC芯片中一个NFC芯片的标签信息，如果读取到ID1，则先连接的NFC芯片编号在后连接的NFC芯片的编号之前，如果读取到的不是ID1，则后连接的NFC芯片编号在先连接的NFC芯片的编号之前。

[0064] 具体地，在对各NFC芯片编号时，如果有两个以上NFC芯片，可以采用NFC阅读器，确定任意两个NFC芯片的编号之间的先后顺序，从而对所有NFC芯片进行编号。当然，也可以确定各NFC芯片的ID，然后进行编号，每个NFC芯片的ID可以是二进制序列号，序列号的每一位上不是“1”就是“0”，可以按照序列号的大小进行编号，例如，有3个NFC芯片，其中两个NFC芯片的ID的前3位是010，另一个NFC芯片的ID的前3位是011，由于011大于010，则可以将前3位为011的NFC芯片的编号记为1，前3位是010的两个NFC芯片，可以继续比对第4位，直至比对出两个NFC芯片的ID的大小，例如，其中一个NFC芯片的ID的前4位为0100，另一个NFC芯片的ID的前4位为0101，由于0101大于0100，则可以将前4位为0101的NFC芯片的编号记为2，前4位为0100的NFC芯片的编号记为3，从而可以确定这三个NFC芯片的编号。

[0065] 步骤A30、对连接有NFC芯片的天线线圈拍照得到预设图像，并关联预设图像与预设标识码。

[0066] 具体地，在连接有NFC芯片的天线线圈中各NFC芯片编号之后，进行拍照得到预设图像，也就是说，在防伪标签在制作时，即获得了预设图像。另外，预设标识码是根据各NFC芯片的标签信息确定的，例如，可以是按照编号将各NFC芯片的ID依次相连得到预设标识码，具体地，两个NFC芯片的ID分别为04:8D:99:32:BC:6C:81的NFC芯片和04:5E:CB:8A:6A:6B:80的NFC芯片。生产商将两个ID相连，得到一个预设标识码04:8D:99:32:BC:6C:81:04:5E:CB:8A:6A:6B:80，将该预设标识码和预设图像关联起来，上传到服务器中。

[0067] 步骤A40、采用标签本体对连接有NFC芯片的天线线圈进行封装，得到防伪标签。

[0068] 具体地，拍完照后，将连接有NFC芯片的天线线圈进行封装，也就是在连接有NFC芯片的天线线圈外形成标签本体，得到防伪标签。

[0069] 具体实施例一

[0070] 如图1所示，多NFC芯片融合的防伪标签的制作实例：

[0071] (1)给定一个NFC天线线圈和两个ID分别为04:8D:99:32:BC:6C:81和04:5E:CB:8A:6A:6B:80的NFC芯片。生产商将两个ID相连，得到一个商品标识码04:8D:99:32:BC:6C:81:04:5E:CB:8A:6A:6B:80，上传到服务器中。

[0072] (2)将两个NFC芯片分别焊接到天线线圈上。用NFC阅读器读取焊接之后的标签ID为04:8D:99:32:BC:6C:81。

[0073] (3)将ID为04:8D:99:32:BC:6C:81的芯片标号为①号，将ID为04:5E:CB:8A:6A:6B:80的芯片标号为②号。

[0074] (4)对焊接后的标签进行拍照，并把图片发送到服务器。

[0075] (5)服务器进行芯片位置和焊点位置的识别和记录，服务器将标签的标识码与图片信息进行关联。

[0076] (6)对焊接后的芯片进行封装，防伪标签制作完毕。

[0077] 如图3所示，本发明实施例所述一种多NFC芯片融合的防伪标签的验证方法，包括以下步骤：

[0078] 步骤S100、获取防伪标签对应的目标图像；其中，所述目标图像为所述防伪标签中天线线圈和NFC芯片的图像。

[0079] 具体地，对防伪标签进行验证时，先获取防伪标签对应的目标图像，例如，可以对防伪标签进行拍摄得到目标图像。需要说明的是，在获取目标图像时，需要先拆除标签本体，露出天线线圈和NFC芯片，从而对天线线圈和NFC芯片进行拍摄得到目标图像。

[0080] 步骤S200、确定第一标签信息后，去除所述防伪标签中所述第一标签信息对应的第一NFC芯片；其中，所述第一NFC芯片为至少两个所述NFC芯片中的一个。

[0081] 具体地，确定第一标签信息后，去除防伪标签中第一标签信息对应的第一NFC芯片，也就是说，在多个NFC芯片中确定出第一标签信息，第一标签信息是多个NFC芯片中某一个芯片中存储的标签信息，确定好后，去除该第一标签信息对应的第一NFC芯片。

[0082] 具体地，各所述NFC芯片按照NFC阅读器的读取顺序编号。步骤S200包括：

[0083] 步骤S210、通过NFC阅读器读取所述防伪标签中所有所述NFC芯片各自分别对应的标签信息。

[0084] 步骤S220、将所述NFC阅读器读取到的标签信息作为第一标签信息。

[0085] 步骤S230、将编号排在第一位的NFC芯片作为所述第一标签信息对应的第一NFC芯片，并去除所述第一NFC芯片。

[0086] 具体地，由于NFC阅读器读取多个NFC芯片的标签信息时，只能完整读取到一个NFC芯片的标签信息，则可以将NFC阅读器读取到的标签信息作为第一标签信息，由于各NFC芯片是按照NFC阅读器的读取顺序进行编号的，编号排在第一位的NFC芯片会被NFC阅读器读取，也就是说，在用NFC阅读器进行读取时，读取到的第一标签信息是存储在编号排在第一位的NFC芯片中的。如图2所示，有两个NFC芯片，如果该防伪标签是真实的，两个NFC芯片是按照NFC阅读器进行编号的，在用NFC阅读器读取时，读取的第一标签信息必然是编号①的

NFC芯片中存储的标签信息。如果该防伪标签是伪造的，则用NFC阅读器读取时，读取的第一标签信息可能不是编号①的NFC芯片中存储的标签信息，那么在后续步骤验证时，无法匹配，验证不通过。

[0087] 举例说明，一共有5个NFC芯片，5个NFC芯片的ID的前5位如下：IDⅠ:01000；IDⅡ:10100；IDⅢ:11101；IDⅣ:11011；IDⅤ:11100。NFC阅读器在读取多个NFC芯片时，先读取所有NFC芯片的ID中第一位，IDⅠ的第一位是0，IDⅡ-IDⅤ的第一位是1，则继续读取IDⅡ-IDⅤ的第二位，IDⅡ的第二位是0，IDⅢ-IDⅤ的第二位是1，则读取IDⅢ-IDⅤ的第三位，IDⅣ的第二位是0，IDⅢ和IDⅤ的第三位是1，则读取IDⅢ和IDⅤ的第四位，IDⅢ和IDⅤ的第四位都是0，则继续读取IDⅢ和IDⅤ的第五位，IDⅤ的第五位是0，IDⅢ的第五位是1，则继续读取IDⅢ的剩余位，得到第一标签信息，那么IDⅢ的编号为1，IDⅢ为第一NFC芯片的标签信息。

[0088] 步骤S300、确定第二标签信息。

[0089] 具体地，在去除第一NFC芯片后，可以确定第二标签信息。

[0090] 具体地，步骤S300具体包括：

[0091] 步骤S310、通过所述NFC阅读器读取去除NFC芯片的防伪标签中所有所述NFC芯片各自分别对应的标签信息。

[0092] 步骤S320、将所述NFC阅读器读取到的标签信息作为第二标签信息。

[0093] 具体地，在去除第一NFC芯片后，继续采用NFC阅读器读取，如果防伪标签是真实的，则此次读取到的第二标签信息为去除NFC芯片的防伪标签中编号排在第一位的NFC芯片中的标签信息。如图2所示，在去除了编号①的NFC芯片，则此时读取到的是编号②的NFC芯片。

[0094] 步骤S400、根据所述第一标签信息、所述第二标签信息以及所述目标图像对所述防伪标签进行验证，得到验证结果。

[0095] 具体地，在得到第一标签信息和第二标签信息后，可以根据第一标签信息、第二标签信息以及目标图像，进行验证，得到防伪标签的验证结果。当第一标签信息、第二标签信息以及目标图像匹配时，防伪标签验证通过。当第一标签信息、第二标签信息以及目标图像不匹配时，防伪标签验证不通过。

[0096] 在匹配时，需要用到预设图像和预设标识码，进行匹配，所述预设图像为制作所述防伪标签时所述第一标签信息对应的第一原始NFC芯片、所述第二标签信息对应的第二原始NFC芯片以及原始天线线圈的图像；所述第一原始NFC芯片与所述原始天线线圈的连接位置为第一原始位置，所述第二原始NFC芯片与所述原始天线线圈的连接位置为第二原始位置；所述第二标签信息为至少两个所述NFC芯片中第二NFC芯片存储的标签信息；所述第一NFC芯片与所述天线线圈的连接位置为第一连接位置，所述第二NFC芯片与所述天线线圈的连接位置为第二连接位置。

[0097] 由于在验证时，不能确定防伪标签是真实的，还是伪造的，也就是说，目标图像中的防伪标签不确定是真实还是伪造，预设图像中的防伪标签一定是真实的，因此，将预设图像中防伪标签的天线线圈记为原始天线线圈，预设图像中防伪标签的NFC芯片记为原始NFC芯片，由于第一标签信息是NFC阅读器读取多个NFC芯片时，NFC阅读器读取到的标签信息，也就是说，第一个读取到的标签信息，第二标签信息是NFC阅读器读取去除NFC芯片的防伪标签中的NFC芯片时，NFC阅读器读取到的标签信息，由于此时第一标签信息对应的NFC芯片

已经去除，因此，第二标签信息是除第一标签信息以外，第一个读取到的标签信息，则第二标签信息是第二个读取到的标签信息。第一标签信息存储在第一原始NFC芯片中，第二标签信息存储在第二原始NFC芯片中。

[0098] 具体地，步骤S400包括：

[0099] 步骤S410、根据所述第一标签信息和所述第二标签信息，确定所述防伪标签对应的标识码。

[0100] 步骤S420、当所述标识码和预设标识码匹配时，获取所述预设标识码对应的预设图像。

[0101] 步骤S430、当所述标识码和预设标识码不匹配时，所述防伪标签验证不通过。

[0102] 具体地，根据第一标签信息和第二标签信息，确定防伪标签对应的标识码。如果是伪造标签，那么根据伪造标签读取到的第一标签信息、第二标签信息与根据真实标签读取到的第一标签信息、第二标签信息是不一致的，因此，根据伪造标签读取到的第一标签信息、第二标签信息得到的标识码与预设标识码(即根据真实标签读取到的第一标签信息、第二标签信息得到的标识码)是不一致的，两者无法匹配，则验证不通过。

[0103] 当标识码和预设标识码匹配时，获取预设标识码对应的预设图像，进行进一步的验证。

[0104] 步骤S440、当所述预设图像和所述目标图像匹配时，所述防伪标签验证通过。

[0105] 步骤S450、当所述预设图像和所述目标图像不匹配时，所述防伪标签验证不通过。

[0106] 具体地，伪造标签根据真实标签进行伪造，并伪造了各NFC芯片，对各NFC芯片中存储的标签信息也伪造成一致的。但是，各NFC芯片的位置，以及各NFC芯片与天线线圈连接点的位置无法伪造成一致的。因此，即使伪造标签对应的标识码与预设标识码匹配，但伪造标签对应的目标图像与预设图像不匹配，验证仍然不同过。

[0107] 具体地，当所述预设图像中所述第一原始NFC芯片的位置、所述第二原始NFC芯片的位置、所述第一原始位置以及所述第二原始位置，分别与所述目标图像中所述第一NFC芯片的位置、所述第二NFC芯片的位置、所述第一连接位置、所述第二连接位置一致时，所述防伪标签验证通过。也就是说，在第一原始NFC芯片的位置与第一NFC芯片的位置一致，第二原始NFC芯片的位置与第二NFC芯片的位置一致，第一原始位置与第一连接位置一致，第二原始位置与第二连接位置一致时，目标图像和预设图像才满足匹配，验证才通过。有一个不一致，则目标图像和预设图像不匹配，验证不通过。

[0108] 本发明的目的主要包含以下三点：

[0109] 第一、为了防止NFC标签的信息被读取并用于复制在伪造标签上，本发明提出一种新的NFC标签及其制作方法来防止标签信息的暴露。

[0110] 第二、为了防止NFC标签的信息被恶意篡改，本发明提出一种新的NFC标签及其制作方法来防止标签的原始信息被篡改。

[0111] 第三、为了防止已销售商品上的旧NFC标签被重复使用在伪造商品上，本发明提出一种新的NFC标签来防止NFC标签的恶意复用。

[0112] 本发明可以实现以下三个目标：

[0113] 防止NFC标签信息被复制：单NFC芯片标签的ID可被任意读取和复制，而本发明提出了一种多NFC芯片融合的标签，借助NFC协议中的防冲突机制，使得NFC阅读器只能读取其

中一个NFC芯片的ID，而无法获取所有NFC芯片的ID信息。此外，由于NFC芯片焊接的位置和焊点的位置模式难以仿造，本发明还提出了使用NFC芯片被焊接在NFC天线线圈上的位置和焊点位置作为标签的指纹，来防止恶意方通过破坏标签，逐一读取两个NFC芯片的信息，并制作一个同样的标签。

[0114] 防止NFC标签信息被篡改：由于NFC读写器只能读取到多芯片NFC标签的一个芯片的ID信息，因此NFC读写器只能改写被其读取的NFC芯片的信息，而无法改写所有芯片的信息。

[0115] 防止NFC标签被重复使用：在验证时，标号为①的NFC芯片需要被去除，NFC阅读器才能读取到另一个NFC标号为②的NFC芯片的ID。因此，该标签在经一次验证后，无法被完整地重复使用在其他商品上。

[0116] 具体实施例二

[0117] 如图2所示，多NFC芯片融合的防伪标签的验证实例：

[0118] (1)去除标签封装，拍摄设备对标签进行拍照并保存图片。

[0119] (2)通过NFC阅读器读取标签的第一个ID为04:8D:99:32:BC:6C:81，并进行记录。

[0120] (3)去除标号为①的NFC芯片后，通过NFC阅读器读取标签的第二个ID为04:5E:CB:8A:6A:6B:80，并进行记录。

[0121] (4)将标签的照片和读取的两个ID上传到服务器中。

[0122] (5)服务器首先通过两个ID计算出该标签的标识码为04:8D:99:32:BC:6C:81:04:5E:CB:8A:6A:6B:80，该标识码与服务器中的一条记录相匹配。

[0123] (6)服务器找到与该标识码对应的图片，将上传的图片和该图片进行匹配，结果匹配，验证结束，验证结果为该标签为真实的原始标签。

[0124] 应当理解的是，本发明的应用不限于上述的举例，对本领域普通技术人员来说，可以根据上述说明加以改进或变换，所有这些改进和变换都应属于本发明所附权利要求的保护范围。

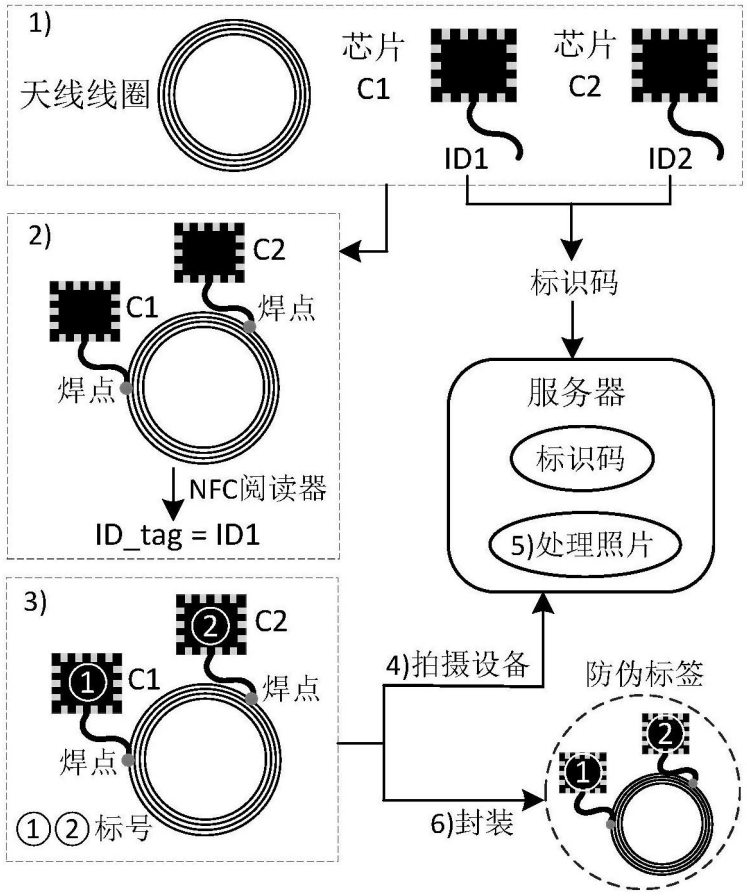

1)
天线线圈
芯片
C1
芯片
C2
ID1
ID2
2)
C2
C1
焊点
焊点
NFC阅读器
ID_tag = ID1
标识码
服务器
标识码
5)处理照片
3)
②
C2
①
C1
焊点
焊点
①②标号
4)拍摄设备
防伪标签
②
①
6)封装

图1

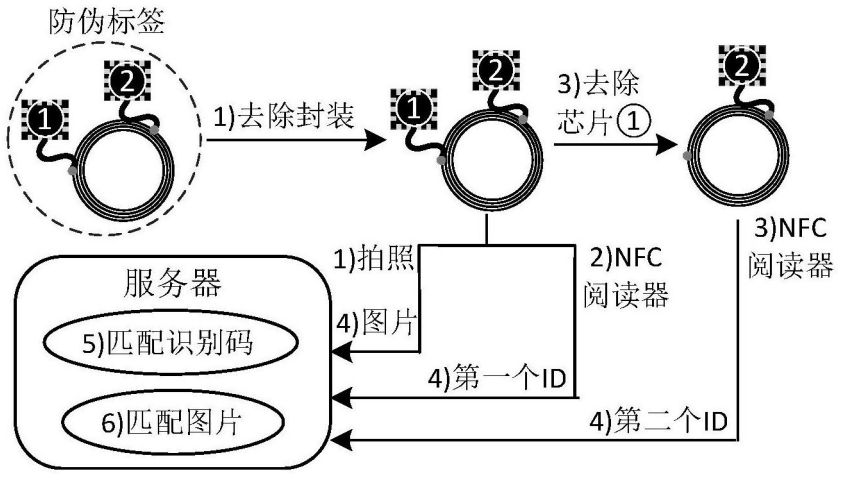

防伪标签
②
①
1)去除封装
②
①
3)去除
芯片①
②
3)NFC
阅读器
1)拍照
2)NFC
阅读器
服务器
4)图片
5)匹配识别码
4)第一个ID
6)匹配图片
4)第二个ID

图2

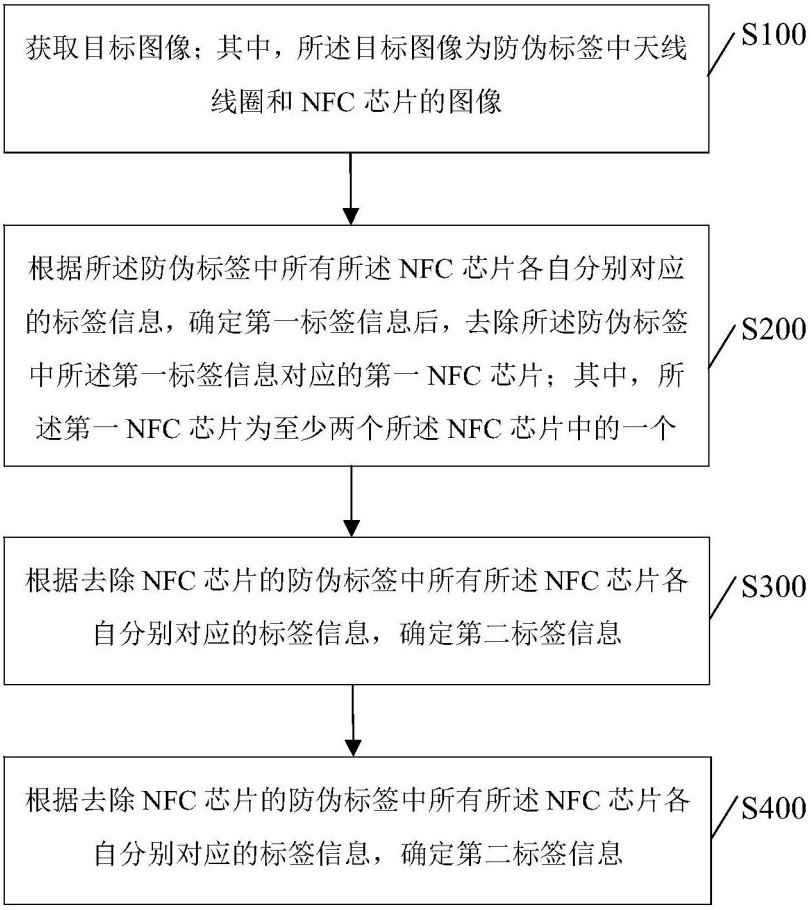

获取目标图像；其中，所述目标图像为防伪标签中天线线圈和 NFC 芯片的图像
S100
根据所述防伪标签中所有所述 NFC 芯片各自分别对应的标签信息，确定第一标签信息后，去除所述防伪标签中所述第一标签信息对应的第一 NFC 芯片；其中，所述第一 NFC 芯片为至少两个所述 NFC 芯片中的一个
S200
根据去除 NFC 芯片的防伪标签中所有所述 NFC 芯片各自分别对应的标签信息，确定第二标签信息
S300
根据去除 NFC 芯片的防伪标签中所有所述 NFC 芯片各自分别对应的标签信息，确定第二标签信息
S400

图3