(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2019 年 4 月 25 日 (25.04.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/075650 A1

(51) 国际专利分类号:
G06K 7/00 (2006.01)

(21) 国际申请号: PCT/CN2017/106618

(22) 国际申请日: 2017 年 10 月 18 日 (18.10.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人:深圳大学(**SHENZHEN UNIVERSITY**) [CN/CN]; 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。

(72) 发明人:杨晴(**YANG, Qing**); 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。
张胜利(**ZHANG, Shengli**); 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。
王晖(**WANG, Hui**); 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。

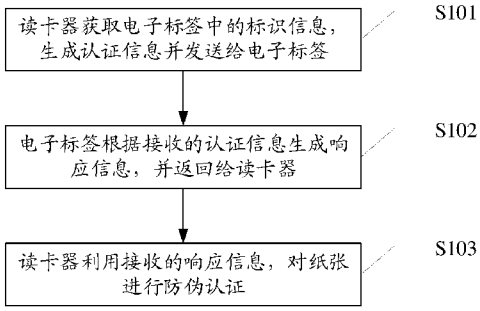
(74) 代理人:深圳市恒申知识产权事务所(普通合伙)(**HENSEN INTELLECTUAL PROPERTY FIRM**); 中国广东省深圳市福田区南园路68号上步大厦10H, Guangdong 518000 (CN)。

(81) 指定国(除另有指明,要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

WO 2019/075650 A1

(54) **Title:** PAPER ANTI-COUNTERFEITING METHOD AND SYSTEM

(54) 发明名称: 纸张防伪方法及系统



S101 A card reader acquires identification information from an electronic tag, and generates authentication information and sends same to the electronic tag

S102 The electronic tag generates response information according to the received authentication information, and returns same to the card reader

S103 The card reader carries out anti-counterfeiting authentication on the paper by using the received response information

图 2

(57) **Abstract:** Disclosed is a paper anti-counterfeiting method, wherein same is applied to the technical field of communications, and comprises: a card reader acquiring identification information from an electronic tag, and generating authentication information and sending same to the electronic tag; the electronic tag generating response information according to the received authentication information, and returning same to the card reader; and the card reader carrying out anti-counterfeiting authentication on the paper by using the received response information. Further disclosed is a paper anti-counterfeiting system. By means of the method and the system, the security of anti-counterfeiting paper and the difficulty in counterfeiting anti-counterfeiting paper can be increased.

(57) 摘要: 本发明实施例公开了一种纸张防伪方法，应用于通信技术领域，包括：读卡器获取电子标签中的标识信息，生成认证信息并发送给电子标签；电子标签根据接收的认证信息生成响应信息，并返回给读卡器；读卡器利用接收的响应信息，对纸张进行防伪认证。本发明实施例还公开了一种纸张防伪系统。该方法及系统可增加防伪纸张的安全性以及防伪纸张的伪造难度。

[见续页]

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) **指定国**(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

纸张防伪方法及系统

技术领域

[0001] 本发明属于通信技术领域，尤其涉及一种纸张防伪方法及系统。

背景技术

[0002] 随着科技发展，电子商务和无纸化办公迅速普及。但是在通讯、合同和艺术等信息领域，使用纸质文件的比重仍然很大。为了保障纸质文件的安全性，防止被伪造，人们通常会对纸质文件进行加密处理。常用的加密方法有物理、化学、光学、物理化学和生物等方法，常见的防伪纸张有水印纸、防复写纸、含安全线的防伪纸、热敏防伪纸以及表面印刷磁条的防伪纸等纸张。

[0003] 但是，目前的防伪纸张依然存在安全性不够、易于伪造的问题。

发明内容

[0004] 本发明提供一种纸张防伪方法及系统，增强了防伪纸张的安全性以及防伪纸张的伪造难度。

[0005] 本发明实施例第一方面提供了一种纸张防伪方法，用于对内置电子标签的纸张进行防伪认证，包括：读卡器获取所述电子标签中的标识信息，生成认证信息并发送给所述电子标签，所述认证信息与所述标识信息对应；所述电子标签根据接收的认证信息生成响应信息，并返回给所述读卡器；所述读卡器利用接收的响应信息，对所述纸张进行防伪认证。

[0006] 本发明实施例第二方面提供了一种系统，包括：读卡器和电子标签，所述电子标签内置在纸张中，所述电子标签包括至少一个芯片和与至少一个所述芯片连接的天线；所述读卡器，用于获取所述电子标签中的标识信息，生成认证信息并发送给所述电子标签，所述认证信息与所述标识信息对应；所述芯片中存储有所述芯片的标识信息；所述电子标签，用于根据接收的认证信息生成响应信息，并返回给所述读卡器；所述读卡器，还用于利用接收的响应信息，对所述纸张进行防伪认证。

[0007] 上述发明实施例提供的纸张防伪方法及系统，通过读卡器获取安装在纸张内的

电子标签的标识信息，向电子标签发送认证信息，接着电子标签根据该认证信息生成响应信息，并发送给读卡器，然后读卡器利用接收的响应信息对纸张进行防伪辨认。由于电子标签中的标识信息具有唯一性，伪造时需要先获取唯一的标识信息，再制造出携带有该标识信息的电子标签，难度较大，成本较高，因此可提高防伪纸张的安全性，增加防伪纸张的伪造难度。

附图说明

[0008] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术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。

[0009] 图1为本发明实施例提供的纸张防伪方法中待认证的纸张的结构示意图图；

[0010] 图2为本发明一实施例提供的纸张防伪方法的实现流程示意图；

[0011] 图3为本发明另一实施例提供的纸张防伪方法的实现流程示意图；

[0012] 图4为本发明另一实施例提供的利用纸张防伪方法一实际应用例的实现示意图；

[0013] 图5为本发明另一实施例的提供的纸张防伪方法的实现流程示意图；

[0014] 图6为本发明一实施例提供的纸张防伪系统的结构示意图；

[0015] 图7为本发明另一实施例提供的纸张防伪系统的结构示意图。

具体实施方式

[0016] 为使得本发明的发明目的、特征、优点能够更加的明显和易懂，下面将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，而非全部实施例。基于本发明中的实施例，本领域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，都属于本发明保护的范围。

[0017] 图1为本发明实施例提供的纸张防伪方法中待认证的纸张的结构示意图。如图1所示，在传统的纸张制作的过程中，在纸张内部加入电子标签。由于电子标签的体积非常小，因此不会影响纸张的正常使用。在实际应用中，在不影响纸张使用的条件下，电子标签可设置在纸张内部的任意位置。

[0018] 请参阅图2，为发明一实施例提供的纸张防伪方法的实现流程示意图。该方法

用于对图1所示内置电子标签的纸张进行防伪认证。如图2所示，该方法主要包括以下步骤：

[0019] S101、读卡器获取电子标签中的标识信息，生成认证信息并发送给电子标签。

[0020] 具体的，运用可读取电子标签信息的读卡器获取电子标签中的标识信息。可选的，若选用的电子标签为RFID（Radio Frequency Identification，射频识别）标签，该电子标签可通过无线电讯号识别特定目标并读写相关数据，则选用的读卡器应为RFID读卡器。在实际应用中，电子标签还可以是NFC（Near Field Communication，近场通信）、UHF（Ultra High Frequency，特高频）等其他具有类似功能的电子标签。

[0021] 电子标签中的标识信息具有唯一性，用于唯一识别电子标签中芯片的身份，可为与该电子标签对应的出厂序列号，也可为纸张所载信息的标号，在实际应用中不限于此。读卡器获取电子标签中的标识信息后，生成认证信息。认证信息与电子标签中的标识信息对应。较佳的，该认证信息为随机数据，可进一步提高纸张的安全性。然后读卡器将该认证信息发送给电子标签，以使电子标签执行下一步骤。

[0022] S102、电子标签根据接收的认证信息生成响应信息，并返回给读卡器。

[0023] 具体的，电子标签接收到认证信息后，处理该认证信息得到响应信息。电子标签再将响应信息发送给读卡器，以使读卡器执行下一步骤。

[0024] S103、读卡器利用接收的响应信息，对纸张进行防伪认证。

[0025] 具体的，读卡器接收到响应信息，将响应信息中包含的信息与预设信息进行比较，判断二者是否一致，以对纸张进行防伪认证。

[0026] 进一步的，若认证通过，则执行认证通过的后续操作，例如：输出通过认证的提示信息。若认证未通过，则执行认证未通过的后续操作，例如：输出未通过认证的预警信息。

[0027] 在本发明实施例中，读卡器获取设置在纸张内的电子标签中的具有唯一性标识信息，生成认证信息并发送给电子标签，电子标签根据该认证信息生成响应信息，并发送给读卡器，然后读卡器利用接收的响应信息中包含的信息与预设信息进行比较，对纸张进行防伪辨认。由于电子标签中的标识信息具有唯一性，

伪造时需要先获取唯一的标识信息，再制造出携带有该标识信息的电子标签，难度较大，成本较高，因此可提高防伪纸张的安全性，增加防伪纸张的伪造难度。

[0028] 请参阅图3，为本发明另一实施例提供的纸张防伪方法的实现流程示意图，该方法涉及通信技术领域。如图3所示，该方法主要包括以下步骤:

[0029] S201、读卡器获取电子标签中的标识信息，生成预设长度的随机比特串，并作为认证信息发送给电子标签。

[0030] 具体的，运用可读取电子标签信息的读卡器获取电子标签中的标识信息。可选的，若选用的电子标签为RFID标签，该电子标签可通过无线电讯号识别特定目标并读写相关数据，则选用的读卡器应为RFID读卡器。

[0031] 电子标签中的标识信息具有唯一性，用于唯一识别电子标签中芯片的身份，可为与该电子标签对应的出厂序列号，也可为纸张所载信息的标号，在实际应用中不限于此。读卡器获取电子标签中的标识信息后，生成预设长度的随机比特串，作为认证信息。认证信息与电子标签中的标识信息对应。在实际应用中，该预设长度为固定值，可由用户自行定义。

[0032] S202、电子标签利用预置的密钥加密该随机比特串，得到响应信息。

[0033] 具体的，电子标签接收到作为认证信息的随机比特串后，采用对称加密算法，利用预置的密钥加密该随机比特串得到响应信息。较佳的，可采用AES（Advanced Encryption Standard，高级加密标准）算法，该算法在加密和解密过程中使用的密钥相同。可以理解的是，由于该认证信息为固定长度的随机比特串，则通过对该固定长度的随机比特串进行加密后得到的响应信息，也是固定长度的比特串。

[0034] S203、电子标签将响应信息发送给读卡器。

[0035] 具体的，电子标签将得到的响应信息发送给读卡器，以使读卡器执行下一步骤。

[0036] S204、读卡器将标识信息、随机比特串和接收的响应信息发送给服务器。

[0037] 具体的，读卡器将从电子标签中获取的标识信息、生成的随机比特串和接收的响应信息一同发送给服务器，以使服务器执行下一步骤。

[0038] S205、服务器接收标识信息、随机比特串和响应信息，获取与标识信息对应的密钥，利用密钥解密响应信息。

[0039] 具体的，服务器获取与标识信息对应的密钥。在实际应用中，服务器中预设有数据库，该数据库用于存储不同电子标签的标识信息与各密钥的对应关系。服务器在接收到读卡器发送的标识信息后，根据该标识信息在数据库中查找与标识信息对应的密钥。然后，服务器利用查找到的密钥对接收到的响应信息进行解密，得到解密后的响应信息。可以理解的，解密后的响应信息为固定长度的比特串。

[0040] S206、服务器比对解密后的响应信息与接收的随机比特串是否相同。

[0041] 具体的，服务器比对解密后的响应信息和接收的随机比特串是否相同。可以理解的，由于响应信息是通过对随机比特串加密后得到，所以解密后的响应信息和该随机比特串通常为相同长度的比特串。因此，为提高比对速度，可首先比对解密后的响应信息和接收的随机比特串的长度是否相同，若长度不同，则确认二者不相同。若长度相同，则进一步比对解密后的响应信息和随机比特串是否完全相同。

[0042] 若解密后的响应信息与随机比特串完全相同，则执行步骤S207：服务器根据预设的方式输出确认纸张通过认证的第一通知消息。

[0043] 若解密后的响应信息与随机比特串不完全相同不同，则执行步骤S208：服务器根据预设的方式输出确认纸张未通过认证的第二通知消息。

[0044] 其中，服务器根据预设的方式输出确认纸张通过认证的第一通知消息，例如：可将该第一通知信息发送给读卡器，然后通过读卡器上显示认证通过的字样；或者，也可将第一通知信息发送给与该读卡器关联的其他终端，以便其他终端根据该第一通知信息，通知用户纸张通过防伪认证。

[0045] 服务器根据预设的方式输出确认纸张通过认证的第二通知消息的方式与服务器根据预设的方式输出确认纸张通过认证的第一通知消息相同，此处不再赘述。

[0046] 为进一步说明本实施例提供的纸张防伪方法的具体实现过程，假设内置电子标签的纸张为货币，标识信息为123，如图4所示。读卡器获取安装在纸张内的电子标签中的标识信息123，随机生成比特串1011010作为认证信息发送给电子标

签。电子标签利用预置的密钥加密该认证信息1011010，得到响应信息1101011并返回给读卡器。读卡器将接收的响应信息1101011、生成的认证信息1011010和标识信息123发送给服务器。服务器在数据库中获取与标识信息123对应的密钥，利用该密钥解密响应信息1101011。若解密后的响应信息为1011010，与认证信息1011010相同，则服务器向读卡器输出确认纸张通过认证的第一通知消息；若解密后的响应信息不是1011010，与认证信息1011010不同，则服务器向读卡器输出确认纸张未通过认证的第二通知消息。

[0047] 本发明实施例中，由于电子标签中的标识信息具有唯一性，将标识信息与加密算法相结合，伪造时需要先获取唯一的标识信息以及相应的密钥，然后还要制造出携带有该标识信息和密钥的电子标签，难度较大，成本较高，因此可提高防伪纸张的安全性，增加防伪纸张的伪造难度。

[0048] 请参阅图5，为本发明另一实施例提供的纸张防伪方法的实现流程示意图，该方法涉及通信技术领域。如图5所示，该方法主要包括以下步骤：

[0049] S301、读卡器获取电子标签中的标识信息，随机生成预设长度的比特串，利用预设的公钥加密比特串，得到认证信息，并将该认证信息发送给电子标签。

[0050] 具体的，运用可读取电子标签信息的读卡器获取电子标签中的标识信息。电子标签中的标识信息具有唯一性，用于唯一识别电子标签中芯片的身份。读卡器获取电子标签中的标识信息后，随机生成预设长度的比特串。在实际应用中，该长度为固定值，可由用户自行定义。

[0051] 于本实施例中，读卡器采用非对称算法对随机生成的预设长度的比特串进行加密。较佳的，该非对称算法为ECC（Elliptic curve cryptography，椭圆曲线加密）算法，该算法的密钥由一对公钥和私钥组成，即在加密和解密过程中的密钥不相同，但是私钥加密的信息只能用对应的公钥解密，而公钥加密的信息只能用私钥解密。

[0052] 读卡器中预设有与电子标签中的标识信息对应的公钥。根据获取的标识信息，查找对应的公钥，然后利用查找到的公钥加密随机生成的比特串，得到认证信息。该认证信息与获取的标识信息对应。

[0053] S302、电子标签通过预置的私钥解密接收的认证信息，将解密后的认证信息作

为响应信息。

[0054] 具体的，电子标签接收到认证信息，利用预置的私钥解密该认证信息，得到解密后的认证信息，将其作为响应信息。该私钥与读卡器在加密过程中使用的公钥相对应。在实际应用中，该私钥可存储在电子标签中。

[0055] S303、电子标签将响应信息返回给读卡器。

[0056] 具体的，电子标签将得到的响应信息返回到读卡器，以使读卡器执行下一步骤。

[0057] S304、读卡器比对接收的响应信息与随机生成的比特串是否相同。

[0058] 可以理解的，响应信息是对读卡器随机生成的比特串进行加密后再解密得到的，所以该响应于信息的长度与随机生成的比特串相同。为提高比对的速度，可首先比对接收的响应信息和随机生成的预设长度的比特串的长度是否相同。若长度不相同，则确定接收的响应信息和随机生成的比特串不相同，纸张未通过防伪认证。若长度相同，则进一步比对接收的响应信息和随机生成的预设长度的比特串是否完全相同。

[0059] 若接收的响应信息和随机生成的预设长度的比特串完全相同，则执行步骤S305：根据预设的方式输出确认纸张通过认证的第三通知消息。若接收的响应信息和随机生成的预设长度的比特串不完全相同，则执行步骤S306：根据预设的方式输出确认纸张未通过认证的第四通知消息。

[0060] 其中，预设的输出方式可为在读卡器上显示认证通过或者认证失败的字样，也可为将第三通知信息和第四通知信息发送给与该读卡器关联的其他终端，以便其他终端根据第三通知信息或第四通知信息，将对应的认证结果输出给用户。

[0061] 在本发明实施例中，由于电子标签中的标识信息具有唯一性，将标识信息与加密算法相结合，伪造时需要先获取唯一的标识信息以及相应的密钥，然后还要制造出携带有该标识信息和密钥的电子标签，难度较大，成本较高，因此可提高防伪纸张的安全性，增加防伪纸张的伪造难度。

[0062] 请参阅图6，为本发明一实施例提供的纸张防伪系统的结构示意图。为了便于说明，仅示出了与本发明实施例相关的部分。图6示例的纸张防伪系统，主要包括：

[0063] 读卡器2和电子标签，电子标签内置在纸张1中，电子标签（图中未标出）包括至少一个芯片3和与至少一个芯片3连接的天线4。在实际应用中，在不影响纸张1使用的情况下，可增加芯片3及天线4的数量，以增加防伪纸张1的安全性。

[0064] 读卡器2，用于获取电子标签中的标识信息，生成认证信息并发送给电子标签，认证信息与标识信息对应。在实际应用中，芯片3进入读写器2的射频范围后，将标识信息通过天线4发送给读写器2。

[0065] 电子标签，用于根据接收的认证信息生成响应信息，并返回给读卡器2。

[0066] 读卡器2，还用于利用接收的响应信息，对纸张1进行防伪认证。

[0067] 进一步地，读卡器2，还用于随机生成预设长度的比特串，利用预设的公钥加密比特串，得到认证信息，公钥与标识信息对应；

[0068] 进一步地，电子标签，还用于通过预置的私钥解密认证信息，将解密后的认证信息作为响应信息，其中，私钥与公钥对应；

[0069] 进一步地，读卡器2，还用于比对响应信息与比特串是否相同；

[0070] 进一步地，读卡器2，还用于若响应信息与比特串相同，则根据预设的方式输出确认纸张1通过认证的第三通知消息；

[0071] 进一步地，读卡器2，还用于若响应信息与比特串不同，则根据预设的方式输出确认纸张1未通过认证的第四通知消息。

[0072] 本实施例未尽之细节，请参阅前述图2和图5所示实施例的描述，此处不再赘述。

[0073] 在本发明实施例中，读卡器获取安装在纸张内的芯片中的具有唯一性标识信息，生成认证信息并发送给芯片，芯片根据该认证信息生成响应信息，并发送给读卡器，然后读卡器利用接收的响应信息中包含的信息与预设信息进行比较，对纸张进行防伪辨认。由于电子标签中的标识信息具有唯一性，伪造时需要先获取唯一的标识信息，再制造出携带有该标识信息的电子标签，难度较大，成本较高，因此可提高防伪纸张的安全性，增加防伪纸张的伪造难度。

[0074] 请参阅图7，为本发明另一实施例提供的纸张防伪系统的结构示意图，为了便于说明，仅示出了与本发明实施例相关的部分。图7示例的纸张防伪系统，与图6所示实施例中的系统的不同之处主要在于：

[0075] 进一步地，该系统还包括：服务器5；

[0076] 进一步地，读卡器2，还用于生成预设长度的随机比特串，并作为认证信息发送给电子标签；

[0077] 进一步地，电子标签，还用于利用预置的密钥加密随机比特串，得到响应信息。

[0078] 进一步地，电子标签，还用于将响应信息发送给读卡器2。

[0079] 进一步地，读卡器2，还用于将标识信息、随机比特串和接收的响应信息发送给服务器5；

[0080] 进一步地，服务器5，还用于接收标识信息、随机比特串和响应信息，获取与标识信息对应的密钥，利用密钥解密响应信息。

[0081] 进一步地，服务器5，还用于比对解密后的响应信息与随机比特串是否相同。

[0082] 进一步地，服务器5，还用于若解密后的响应信息与随机比特串相同，则根据预设的方式输出确认纸张1通过认证的第一通知消息。

[0083] 进一步地，服务器5，还用于若解密后的响应信息与随机比特串不同，则根据预设的方式输出确认纸张1未通过认证的第二通知消息。

[0084] 本实施例未尽之细节，请参阅前述图2至图4所示实施例的描述，此处不再赘述。

[0085] 本发明实施例中，由于电子标签中的标识信息具有唯一性，将标识信息与加密算法相结合，伪造时需要先获取唯一的标识信息以及相应的密钥，然后还要制造出携带有该标识信息和密钥的电子标签，难度较大，成本较高，因此可提高防伪纸张的安全性，增加防伪纸张的伪造难度。

[0086] 需要说明的是，对于前述的各方法实施例，为了简便描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其它顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定都是本发明所必须的。

[0087] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其它实施例的相关描述。

[0088] 以上为对本发明所提供的纸张防伪方法及系统的描述，对于本领域的一般技术人员，依据本发明实施例的思想，在具体实施方式及应用范围上均会有改变之处，综上，本说明书内容不应理解为对本发明的限制。

权利要求书

[权利要求 1] 一种纸张防伪方法，其特征在于，用于对内置电子标签的纸张进行防伪认证，所述方法包括：

读卡器获取所述电子标签中的标识信息，生成认证信息并发送给所述电子标签，所述认证信息与所述标识信息对应；

所述电子标签根据接收的认证信息生成响应信息，并返回给所述读卡器；

所述读卡器利用接收的响应信息，对所述纸张进行防伪认证。

[权利要求 2] 如权利要求1所述的纸张防伪方法，其特征在于，

所述生成认证信息并发送给所述电子标签包括：

生成预设长度的随机比特串，并作为所述认证信息发送给所述电子标签；

则，所述电子标签根据接收的认证信息生成响应信息包括：

所述电子标签利用预置的密钥加密所述随机比特串，得到所述响应信息。

[权利要求 3] 如权利要求2所述的纸张防伪方法，其特征在于，所述读卡器利用接收的响应信息，对所述纸张进行防伪认证包括：

所述读卡器将所述标识信息、所述随机比特串和接收的响应信息发送给服务器；

所述服务器接收所述标识信息、所述随机比特串和所述响应信息，获取与所述标识信息对应的所述密钥，利用所述密钥解密所述响应信息；

所述服务器比对解密后的响应信息与所述随机比特串是否相同；

若所述解密后的响应信息与所述随机比特串相同，则所述服务器根据预设的方式输出确认所述纸张通过认证的第一通知消息；

若所述解密后的响应信息与所述随机比特串不同，则所述服务器根据所述预设的方式输出确认所述纸张未通过认证的第二通知消息。

[权利要求 4] 如权利要求1所述的纸张防伪方法，其特征在于，所述生成认证信息包括：

随机生成预设长度的比特串，利用预设的公钥加密所述比特串，得到所述认证信息，所述公钥与所述标识信息对应。

[权利要求 5] 如权利要求4所述的纸张防伪方法，其特征在于，所述电子标签根据接收的认证信息生成响应信息包括：

所述电子标签通过预置的私钥解密所述认证信息，将解密后的认证信息作为所述响应信息，其中，所述私钥与所述公钥对应。

[权利要求 6] 如权利要求5所述的纸张防伪方法，其特征在于，所述读卡器利用接收的响应信息，对所述纸张进行防伪认证包括：

所述读卡器比对所述响应信息与所述比特串是否相同；

若所述响应信息与所述比特串相同，则根据预设的方式输出确认所述纸张通过认证的第三通知消息；

若所述响应信息与所述比特串不同，则根据所述预设的方式输出确认所述纸张未通过认证的第四通知消息。

[权利要求 7] 一种纸张防伪系统，其特征在于，所述系统包括：读卡器和电子标签，所述电子标签内置在纸张中，所述电子标签包括至少一个芯片和与至少一个所述芯片连接的天线；

所述读卡器，用于获取所述电子标签中的标识信息，生成认证信息并发送给所述电子标签，所述认证信息与所述标识信息对应；

所述芯片中存储有所述芯片的标识信息；

所述电子标签，用于根据接收的认证信息生成响应信息，并返回给所述读卡器；

所述读卡器，还用于利用接收的响应信息，对所述纸张进行防伪认证。

[权利要求 8] 如权利要求7所述的纸张防伪系统，其特征在于，所述系统还包括：服务器；

所述读卡器，还用于生成预设长度的随机比特串，并作为所述认

证信息发送给所述电子标签；

所述电子标签，还用于利用预置的密钥加密所述随机比特串，得到所述响应信息；

所述读卡器，还用于将所述标识信息、所述随机比特串和接收的响应信息发送给服务器；

所述服务器，还用于接收所述标识信息、所述随机比特串和所述响应信息，获取与所述标识信息对应的所述密钥，利用所述密钥解密所述响应信息；

所述服务器，还用于比对解密后的响应信息与所述随机比特串是否相同；

所述服务器，还用于若所述解密后的响应信息与所述随机比特串相同，则根据预设的方式输出确认所述纸张通过认证的第一通知消息；

所述服务器，还用于若所述解密后的响应信息与所述随机比特串不同，则根据所述预设的方式输出确认所述纸张未通过认证的第二通知消息。

[权利要求 9] 如权利要求7所述的纸张防伪系统，其特征在于，

所述读卡器，还用于随机生成预设长度的比特串，利用预设的公钥加密所述比特串，得到所述认证信息，所述公钥与所述标识信息对应；

所述电子标签，还用于通过预置的私钥解密所述认证信息，将解密后的认证信息作为所述响应信息，其中，所述私钥与所述公钥对应；

所述读卡器，还用于比对所述响应信息与所述比特串是否相同；

所述读卡器，还用于若所述响应信息与所述比特串相同，则根据预设的方式输出确认所述纸张通过认证的第三通知消息；

所述读卡器，还用于若所述响应信息与所述比特串不同，则根据所述预设的方式输出确认所述纸张未通过认证的第四通知消息。

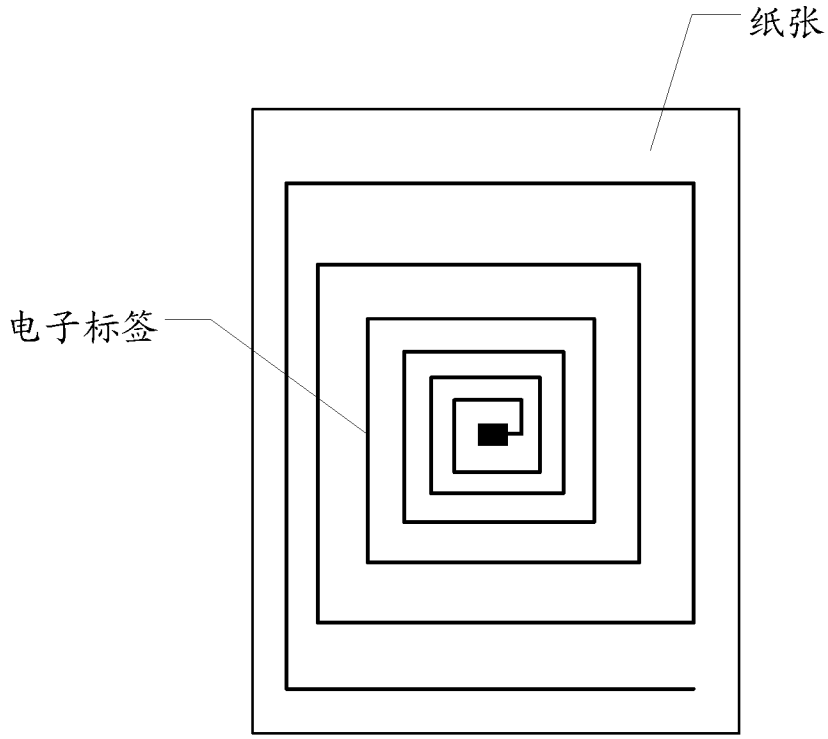

纸张
电子标签

图 1

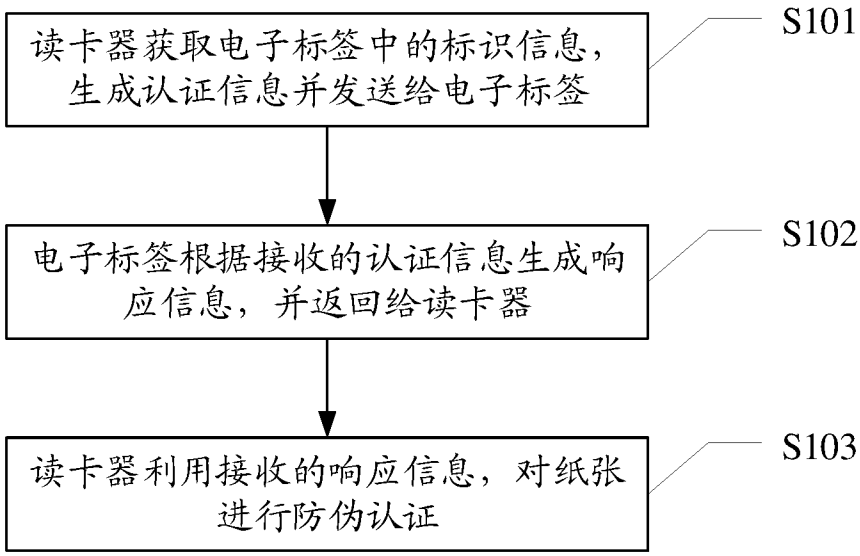

读卡器获取电子标签中的标识信息，生成认证信息并发送给电子标签
S101
电子标签根据接收的认证信息生成响应信息，并返回给读卡器
S102
读卡器利用接收的响应信息，对纸张进行防伪认证
S103

图 2

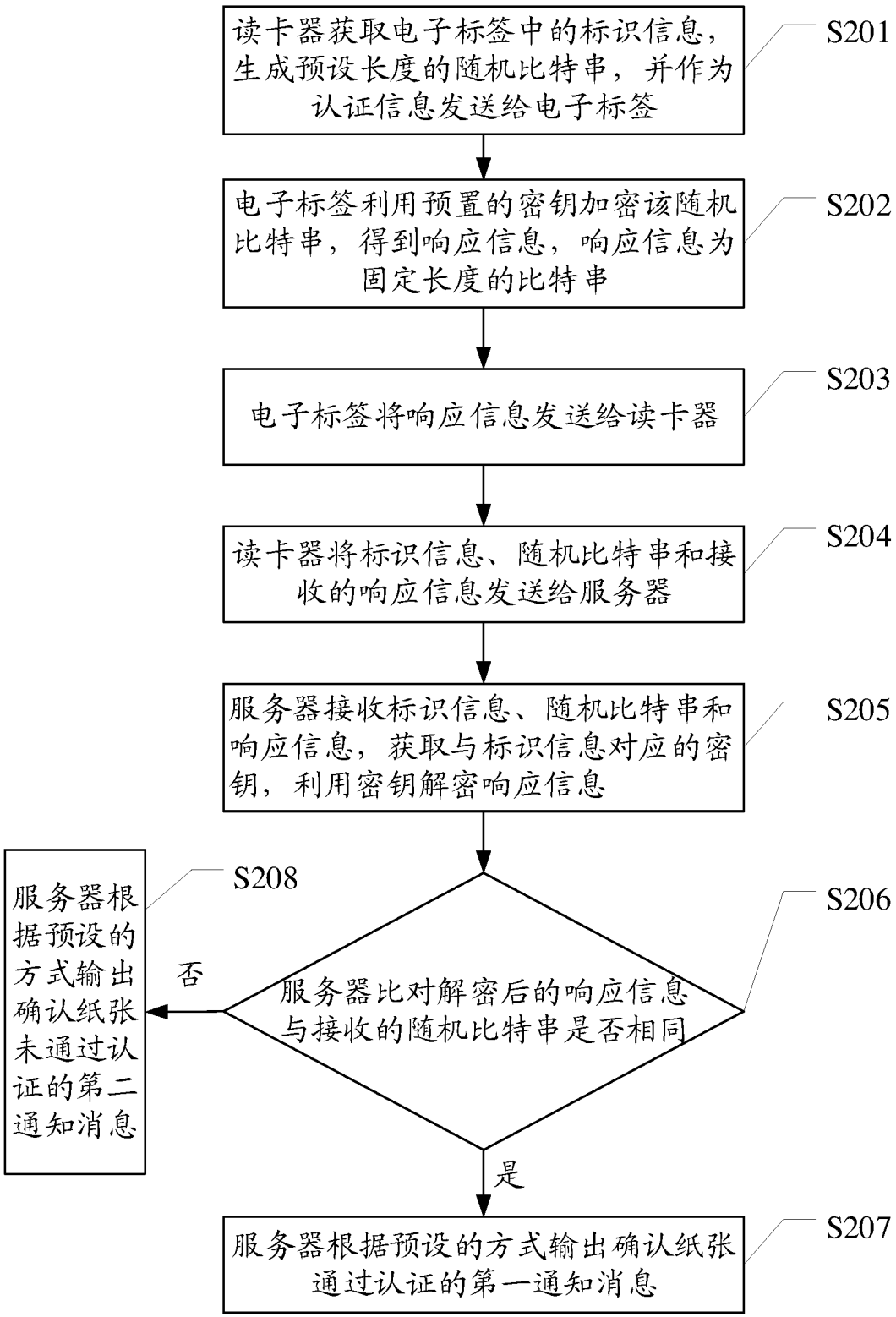

读卡器获取电子标签中的标识信息，生成预设长度的随机比特串，并作为认证信息发送给电子标签
S201
电子标签利用预置的密钥加密该随机比特串，得到响应信息，响应信息为固定长度的比特串
S202
电子标签将响应信息发送给读卡器
S203
读卡器将标识信息、随机比特串和接收的响应信息发送给服务器
S204
服务器接收标识信息、随机比特串和响应信息，获取与标识信息对应的密钥，利用密钥解密响应信息
S205
服务器比对解密后的响应信息与接收的随机比特串是否相同
S206
否
服务器根据预设的方式输出确认纸张未通过认证的第二通知消息
S208
是
服务器根据预设的方式输出确认纸张通过认证的第一通知消息
S207

图 3

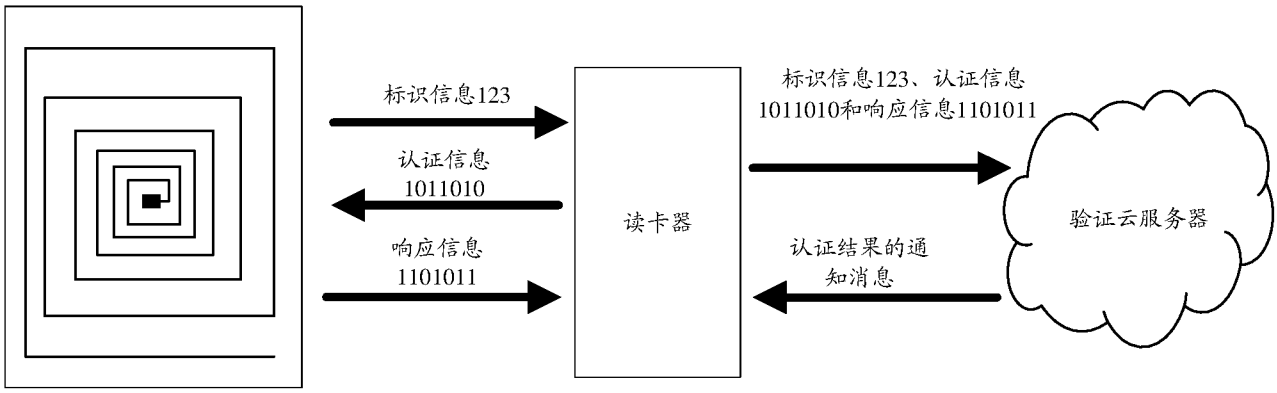

标识信息123
认证信息
1011010
响应信息
1101011
读卡器
标识信息123、认证信息
1011010和响应信息1101011
认证结果的通
知消息
验证云服务器

图 4

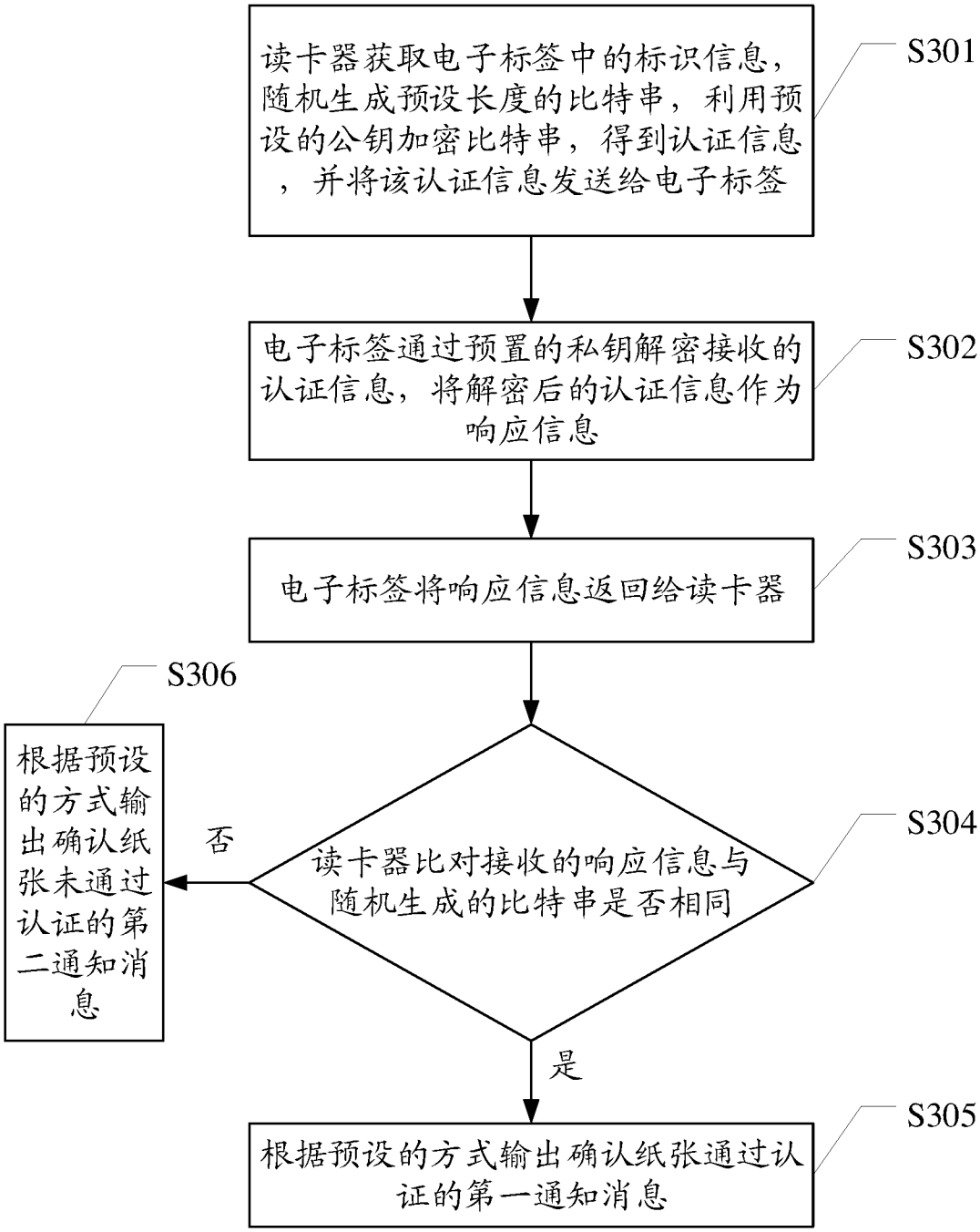

读卡器获取电子标签中的标识信息，随机生成预设长度的比特串，利用预设的公钥加密比特串，得到认证信息，并将该认证信息发送给电子标签
S301
电子标签通过预置的私钥解密接收的认证信息，将解密后的认证信息作为响应信息
S302
电子标签将响应信息返回给读卡器
S303
读卡器比对接收的响应信息与随机生成的比特串是否相同
S304
否
根据预设的方式输出确认纸张未通过认证的第二通知消息
S306
是
根据预设的方式输出确认纸张通过认证的第一通知消息
S305

图 5

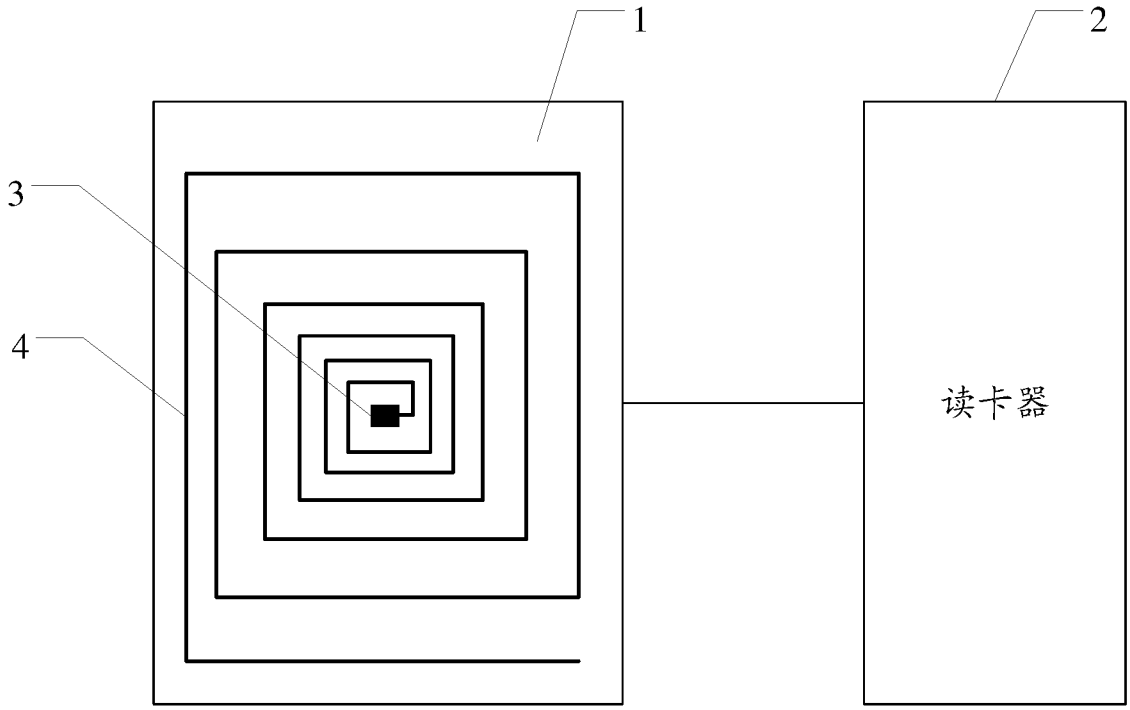


图 6

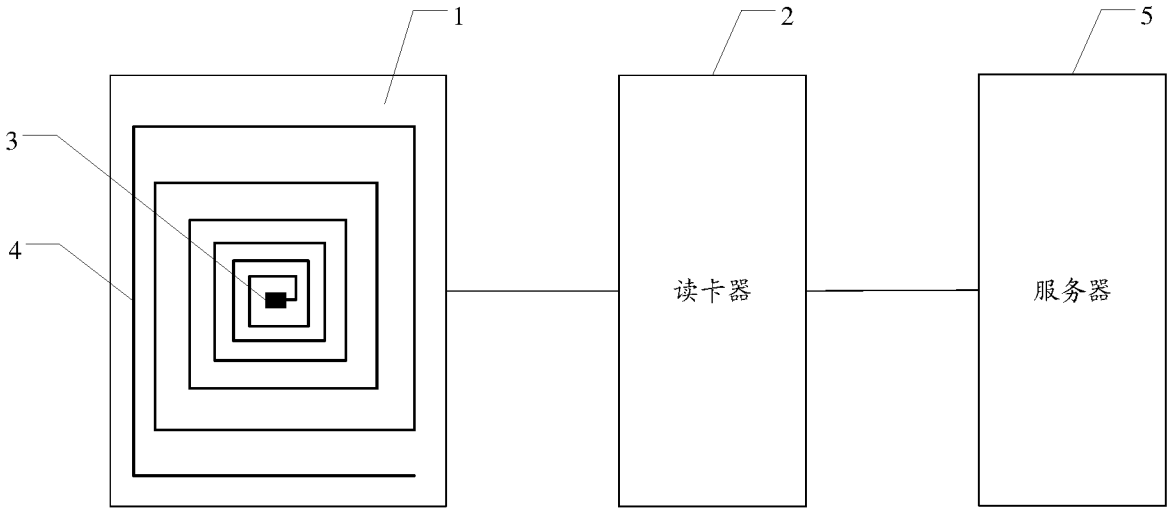


图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/106618

A. CLASSIFICATION OF SUBJECT MATTER

G06K 7/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CPRSABS, DWPI, CNKI, CNTXT: 纸, 防伪, 认证, 电子标签, RFID, 读卡器, 标识, 信息, 响应, 密钥, 随机, paper, anti counterfeit+, certificate, electronic tag, RFID, reader, identification, information, response, key, random

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 1932835 A (HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY) 21 March 2007 (2007-03-21) entire document	1-9
A	CN 106096678 A (WANG, XIAOFENG) 09 November 2016 (2016-11-09) entire document	1-9
A	CN 105893898 A (SHENZHEN YUSHENGXING CULTURAL TRANS CO., LTD.) 24 August 2016 (2016-08-24) entire document	1-9
A	CN 104809618 A (SHANGHAI GAOYAN MINGJIAN INFORMATION TECHNOLOGY CO., LTD.) 29 July 2015 (2015-07-29) entire document	1-9
A	KR 20060103383 A (SK TELECOM CO., LTD.) 29 September 2006 (2006-09-29) entire document	1-9

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 July 2018	**06 August 2018**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/106618

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	1932835	A	21 March 2007	CN	100405386	C	23 July 2008
CN	106096678	A	09 November 2016		None		
CN	105893898	A	24 August 2016		None		
CN	104809618	A	29 July 2015	CN	104809618	B	13 February 2018
KR	20060103383	A	29 September 2006	KR	100705953	B	11 April 2007

国际检索报告

国际申请号
PCT/CN2017/106618

A. 主题的分类

G06K 7/00(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06K

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS, CPRSABS, DWPI, CNKI, CNTXT, 纸，防伪，认证，电子标签，RFID，读卡器，标识，信息，响应，密钥，随机，paper，anti counterfeit+，certificate，electronic tag，RFID，reader，identification，information，response，key，random

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 1932835 A (华中科技大学) 2007年 3月 21日 (2007 - 03 - 21) 全文	1-9
A	CN 106096678 A (王晓峰) 2016年 11月 9日 (2016 - 11 - 09) 全文	1-9
A	CN 105893898 A (深圳市裕盛星文化传播有限公司 等) 2016年 8月 24日 (2016 - 08 - 24) 全文	1-9
A	CN 104809618 A (上海高研明鉴信息技术有限公司) 2015年 7月 29日 (2015 - 07 - 29) 全文	1-9
A	KR 20060103383 A (SK TELECOM CO LTD) 2006年 9月 29日 (2006 - 09 - 29) 全文	1-9

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2018年 7月 17日	2018年 8月 6日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 史江峰 电话号码 62089926

表 PCT/ISA/210 (第2页) (2015年1月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/106618

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	1932835	A	2007年 3月 21日	CN	100405386	C	2008年 7月 23日
CN	106096678	A	2016年 11月 9日		无		
CN	105893898	A	2016年 8月 24日		无		
CN	104809618	A	2015年 7月 29日	CN	104809618	B	2018年 2月 13日
KR	20060103383	A	2006年 9月 29日	KR	100705953	B	2007年 4月 11日