



(12)发明专利

(10)授权公告号 CN 106650869 B

(45)授权公告日 2020.02.07

(21)申请号 201610905747.0

(22)申请日 2016.10.18

(65)同一申请的已公布的文献号  
申请公布号 CN 106650869 A

(43)申请公布日 2017.05.10

(73)专利权人 重庆文理学院  
地址 402160 重庆市永川区红河大道319号  
区

(72)发明人 杨志刚 王先平 彭玲玲 严海升  
罗万成 罗代忠 廖树萃 马新强  
刘楠

(74)专利代理机构 重庆弘旭专利代理有限责任  
公司 50209  
代理人 李靖

(51)Int.Cl.  
G06K 19/06(2006.01)

(56)对比文件  
CN 105224974 A,2016.01.06,  
CN 105825257 A,2016.08.03,  
CN 103415007 A,2013.11.27,  
CN 104537109 A,2015.04.22,  
CN 105095936 A,2015.11.25,  
孙浩天等.一种基于二维码的信息隐藏方  
法.《Computer Knowledge and Technology 电  
脑知识与技术》.2016,

审查员 石海霞

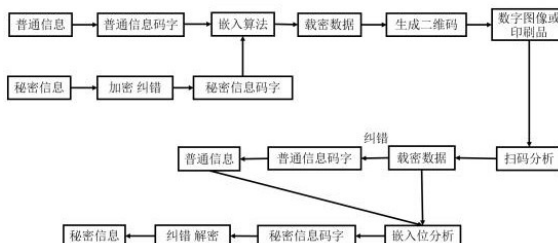
权利要求书2页 说明书6页 附图2页

(54)发明名称

一种基于二维码的信息隐藏方法

(57)摘要

本发明公开了一种基于二维码的信息隐藏方法,首先对普通信息进行处理得到普通信息码字序列;对秘密信息进行处理得到秘密信息码字序列;然后将秘密信息码字序列通过嵌入加密算法嵌入到普通信息码字序列中得到载密数据;将载密数据生成二维码;根据用户身份确定从二维码中解密得到相应的将普通信息和秘密信息。本发明提供的二维码信息隐藏方法,将秘密信息嵌入到普通信息后,保障了二维码中秘密信息的安全性;普通用户和特殊用户互不干扰,特殊用户可以利用普通信息和秘密信息之间建立的函数映射关系进行的真伪校验;载有秘密信息的二维码既能以数字图像形式传播,也能以印刷图像形式传播,应用场景广泛。



1. 一种基于二维码的信息隐藏方法,其特征在于:包括以下步骤:

1) 对普通信息进行处理得到普通信息码字序列;对秘密信息进行处理得到秘密信息码字序列;

2) 将秘密信息码字序列通过嵌入加密算法嵌入到普通信息码字序列中得到载密数据;

3) 将载密数据生成二维码;将二维码以图像形式设置于产品上;

4) 确定获取二维码的对象身份,如果是需要获取普通信息的用户,则通过扫码器扫码得到载密数据;并将载密数据经过纠错处理得到普通码字序列,并将普通码字序列还原出普通信息;

5) 如果是需要获取秘密信息的用户,则通过扫码器扫码得到载密数据,并将载密数据进行嵌入解密算法提取出秘密信息码字序列,然后将秘密信息码字序列还原出秘密信息;

所述嵌入加密算法的具体步骤如下:

S21: 将秘密信息码字序列按照各预设嵌入模式依次插入普通信息码字序列的序列位中形成嵌入码序列;

S22: 计算嵌入码字序列与普通信息码字序列被嵌入位的数据改变率;

S23: 选择改变率最小的嵌入模式将秘密信息码字嵌入到普通信息码字序列中,形成载密数据。

2. 如权利要求1所述的基于二维码的信息隐藏方法,其特征在于:所述嵌入解密算法的具体步骤如下:

S51: 从二维码中获取载密数据;

S52: 对载密数据进行纠错,秘密信息码字序列会被当作错误进行纠正,从而恢复出普通信息;

S53: 再分别按照所有预设的嵌入模式从载密数据中提取出秘密信息码字序列;

S54: 按以下公式对预设嵌入模式的提取结果进行评分:

嵌入模式提取结果评分公式:

$$S = k_1 \times BER_1 + k_2 \times BER_2 + X;$$

其中,S是提取结果评分, $k_1$ 和 $k_2$ 是常数;BER1用于将直接提取出的秘密信息序列使用纠错码恢复,BER1表示秘密信息序列错误的bit数/秘密信息序列总bit数;BER2用于将载密数据使用纠错码进行恢复,BER2表示非嵌入位错误的bit数/非嵌入位数据总bit数;x为模式一致因子;

S55: 选择提取结果评分分值最低者作为嵌入模式;

S56: 按照选取的嵌入模式从载密数据中提取出秘密信息码字序列,再对秘密信息码字序列进行纠错和解密,最终得到秘密信。

3. 如权利要求2所述的基于二维码的信息隐藏方法,其特征在于:所述 $x=0$ 或者 $c$ 的选择是按照以下步骤进行的:

S541: 按照各预设的嵌入模式从载密数据中提出秘密信息码字序列;

S542: 将普通信息码字序列与提取的秘密信息码字序列重复S21-S23步骤;

S543: 将S21-S23步骤选取的嵌入模式与提取秘密信息码字序列所使用的嵌入模式进行比较;如果两者一致,则 $x$ 取0,否则取 $c$ 。

4. 如权利要求1所述的基于二维码的信息隐藏方法,其特征在于:还包括以下步骤:

将秘密信息码字序列长度及嵌入模式的序号嵌入到二维码码字的补齐码区域中。

## 一种基于二维码的信息隐藏方法

### 技术领域

[0001] 本发明涉及二维码信息处理领域,特别是一种基于二维码的信息隐藏方法。

### 背景技术

[0002] 当前,二维码已广泛应用于人们生产、生活的各个领域。由于二维码的传播和识读十分方便,如果没有采取必要的安全措施,二维码中携带的敏感关键信息极易泄露。如某些地方推出的老年人防走失二维码,包含老人身份证号、子女的联系电话等敏感信息,但是却没有任何安全措施。

[0003] 目前,针对二维码中的秘密信息,有如下安全技术或手段:如火车票二维码中对乘客信息经过了加密处理;在专利“一种基于信息隐藏的手机二维码安全使用方法”中,以秘密口令为密钥对秘密信息进行变换,提取数据信息需输入正确的口令。以上两种方法其实质都是对秘密信息进行变换的一种加密技术,普通用户会读出一些难以解读的字符串,这些字符串容易引起攻击者的注意。在专利“一种基于信息隐藏的图像二维码及其生成方法和系统”中,将数据信息嵌入到宿主图像中,构成图像二维码。这是一种将二维码图像嵌入、隐藏到其他图像中的方法,而非在二维码中隐藏信息。

[0004] 因此,为了保障二维码中秘密信息的安全性;需要一种能对二维码中普通信息和秘密信息进行信息隐藏的方法。

### 发明内容

[0005] 本发明的目的是提出一种能对二维码中普通信息和秘密信息进行信息隐藏的方法,该方法保障了二维码中信息的安全。

[0006] 本发明的目的是通过以下技术方案来实现的:

[0007] 本发明提供的基于二维码的信息隐藏方法,包括以下步骤:

[0008] 1) 对普通信息进行处理得到普通信息码字序列;对秘密信息进行处理得到秘密信息码字序列;

[0009] 2) 将秘密信息码字序列通过嵌入加密算法嵌入到普通信息码字序列中得到载密数据;

[0010] 3) 将载密数据生成二维码;将二维码以图像形式设置于产品上;

[0011] 4) 确定获取二维码的对象身份,如果是需要获取普通信息的用户,则通过扫码器扫码得到载密数据;并将载密数据经过纠错处理得到普通码字序列,并将普通码字序列还原出普通信息;

[0012] 5) 如果是需要获取秘密信息的用户,则通过扫码器扫码得到载密数据,并将载密数据进行嵌入解密算法提取出秘密信息码字序列,然后将秘密信息码字序列还原出秘密信息。

[0013] 进一步,所述嵌入加密算法的具体步骤如下:

[0014] S21:将秘密信息码字序列按照各预设嵌入模式依次插入普通信息码字序列的序

列位中形成嵌入码序列；

[0015] S22:计算嵌入码字序列与普通信息码字序列被嵌入位的数据改变率；

[0016] S23:选择改变率最小的嵌入模式将秘密信息码字嵌入到普通信息码字序列中,形成载密数据。

[0017] 进一步,所述嵌入解密算法的具体步骤如下:

[0018] S51:从二维码中获取载密数据;

[0019] S52:对载密数据进行纠错,秘密信息码字序列会被当作错误进行纠正,从而恢复出普通信息;

[0020] S53:再分别按照所有预设的嵌入模式从载密数据中提取出秘密信息码字序列;

[0021] S54:按以下公式对预设嵌入模式的提取结果进行评分:

[0022] 嵌入模式提取结果评分公式: $S=k_1 \times BER_1+k_2 \times BER_2+x$ ;

[0023] 其中,S是提取结果评分,k1和k2是常数;BER1用于将直接提取出的秘密信息序列使用纠错码恢复,BER1表示秘密信息序列错误的bit数/秘密信息序列总bit数;BER2用于将载密数据使用纠错码进行恢复,BER2表示非嵌入位错误的bit数/非嵌入位数据总bit数;x为模式一致因子;

[0024] S55:选择提取结果评分分值最低者作为嵌入模式;

[0025] S56:按照选取的嵌入模式从载密数据中提取出秘密信息码字序列,再对秘密信息码字序列进行纠错和解密,最终得到秘密信。

[0026] 进一步,所述 $x=0$ 或者 $c$ 的选择是按照以下步骤进行的:

[0027] S541:按照各预设的嵌入模式从载密数据中提出秘密信息码字序列;

[0028] S542:将普通信息码字序列与提取的秘密信息码字序列重复S21-S23步骤;

[0029] S543:将S21-S23步骤选取的嵌入模式与提取秘密信息码字序列所使用的嵌入模式进行比较;如果两者一致,则 $x$ 取0,否则取 $c$ 。

[0030] 进一步,还包括以下步骤:

[0031] 将秘密信息码字序列长度及嵌入模式的序号嵌入到二维码码字的补齐码区域中。

[0032] 由于采用了上述技术方案,本发明具有如下的优点:

[0033] 本发明提供的二维码信息隐藏方法,将秘密信息嵌入到普通信息后,保障了二维码中秘密信息的安全性;普通用户只能识读普通信息,特殊用户两者都可以识读,两者互不干扰,避免秘密信息因加密产生难以解读的字符串,从而引起攻击者的怀疑;普通信息和秘密信息之间通建立函数映射关系(如hash变换),特殊用户可以利用这种映射关系对普通信息的真伪进行校验;载有秘密信息的二维码既能以数字图像形式传播,也能以印刷图像形式传播,应用场景广泛。

[0034] 本发明的其他优点、目标和特征在某种程度上将在随后的说明书中进行阐述,并且在某种程度上,基于对下文的考察研究对本领域技术人员而言将是显而易见的,或者可以从本发明的实践中得到教导。本发明的目标和其他优点可以通过下面的说明书来实现和获得。

## 附图说明

[0035] 本发明的附图说明如下。

- [0036] 图1为二维码信息隐藏及提取步骤流程图。
- [0037] 图2为随机嵌入位置算法图。
- [0038] 图3为无秘密信息的二维码。
- [0039] 图4为隐藏有秘密信息的二维码。

### 具体实施方式

[0040] 下面结合附图和实施例对本发明作进一步说明。

[0041] 实施例1

[0042] 本实施例提供的基于二维码的信息隐藏方法,利用传播广泛的二维码作为信息隐藏的载体,应用场景广泛。如在商品防伪溯源领域,为每一件产品分配一个唯一的编号,将该编号作为秘密信息隐藏在产品的普通信息中(普通信息包括产品品名、产地、出厂日期等)。普通用户可以获取产品普通信息而不能查看产品编号,只有产品监察员才能查看产品的编号。如养老领域,制作防走失二维码,将老人的一些基本情况,如姓名、可年龄、过往病史等公开,而将老人身份证号、子女联系方式等敏感数据作为秘密信息隐藏。普通用户可以获取老人基本信息,志愿者或者管理员可以获得子女联系方式等秘密信息,方便和子女联系。

[0043] 本实施例的实现原理是:首先利用二维码纠错编码产生的冗余性,将秘密信息编码嵌入到普通信息的编码序列中,生成藏有秘密信息的载密二维码;然后普通用户扫描二维码仅可获取普通信息,而嵌入的秘密信息则会被当作传播过程中产生的误码而被纠正被忽略。其次特殊用户可通过嵌入位分析提取出秘密信息的码字序列,再经过纠错、解密、译码等过程恢复出秘密信息。本实施例提供的方法适用于所有使用了纠错编码的二维码,如PDF417、QR Code等。

[0044] 如图所示,本实施例提供的基于二维码的信息隐藏方法,包括以下步骤:

[0045] 1) 对普通信息进行处理得到普通信息码字序列;对秘密信息进行处理得到秘密信息码字序列;

[0046] 2) 将秘密信息码字序列通过嵌入加密算法嵌入到普通信息码字序列中得到载密数据;

[0047] 3) 将载密数据生成二维码;将二维码以图像形式设置于产品上;

[0048] 4) 确定获取二维码的对象身份,如果是需要获取普通信息的用户;即普通用户,则通过扫码器扫码得到载密数据;并将载密数据经过纠错处理得到普通码字序列,并将普通码字序列还原出普通信息;

[0049] 5) 如果是需要获取秘密信息的用户,即特殊用户,则通过扫码器扫码得到载密数据,并将载密数据进行嵌入解密算法提取出秘密信息码字序列,然后将秘密信息码字序列还原出秘密信息。

[0050] 所述嵌入加密算法的具体步骤如下:

[0051] S21:将秘密信息码字序列按照各预设嵌入模式依次插入普通信息码字序列的序列位中形成嵌入码序列;

[0052] 嵌入模式有8种或更多。其中,4种固定嵌入模式,4种随机嵌入模式。固定嵌入模式是指秘密数据的嵌入位置是固定的。但固定位置嵌入可能会导致误码率过大等问题,因此

引入随机嵌入模式。随机嵌入模式是指秘密数据的嵌入位置是随机的。随机嵌入位置由随机算法产生的随机数映射而来,而随机算法的种子则由普通信息变换而成。

[0053] S22:计算嵌入码字序列与普通信息码字序列被嵌入位的数据改变率;

[0054] S23:选择改变率最小的嵌入模式将秘密信息码字嵌入到普通信息码字序列中,形成载密数据。

[0055] 所述嵌入解密算法的具体步骤如下:

[0056] S51:从二维码中获取载密数据;

[0057] S52对载密数据进行纠错,秘密信息码字序列会被当作错误进行纠正,从而恢复出普通信息;按照预设嵌入模式分别对载密数据提取普通信息码字提取序列和秘密信息码字提取序列;

[0058] S53:再分别按照所有预设的嵌入模式从载密数据中提取出秘密信息码字序列;

[0059] S54:按以下公式对各预设嵌入模式的提取结果进行评分:

[0060] 嵌入模式提取结果评分公式: $S=k_1 \times BER_1+k_2 \times BER_2+x$ ;

[0061] 其中,S是提取结果评分,k1和k2是常数,BER1代表秘密信息码字提取序列的误码率;BER2代表非嵌入位数据的误码率;x=0或者c;

[0062] BER1:将直接提取出的秘密信息序列使用纠错码恢复,BER1=秘密信息序列错误的bit数/秘密信息序列总bit数

[0063] BER2:将载密数据使用纠错码进行恢复,BER2=非嵌入位错误的bit数/非嵌入位数据总bit数

[0064] x为模式一致因子;x=0或者c;

[0065] S55:选择提取结果评分分值最低者作为嵌入模式;

[0066] S56:按照选取的嵌入模式从载密数据中提取出秘密信息码字序列,再对秘密信息码字序列进行纠错和解密,最终得到秘密信息。

[0067] 所述x=0或者c的选择是按照以下步骤进行的:

[0068] S541:按照各预设的嵌入模式从载密数据中提出秘密信息码字序列;

[0069] S542:将普通信息码字序列与提取的秘密信息码字序列重复S21-S23步骤。

[0070] S543:将S21-S23步骤选取的嵌入模式与提取秘密信息码字序列所使用的嵌入模式进行比较。如果两者一致,则x取0,否则取c。

[0071] 本实施例提供的模式一致因子是根据普通信息码字提取序列和秘密信息码字提取序列获取对应的秘密提取信息和普通提取信息;然后将秘密信息码字提取序列通过嵌入加密算法嵌入到普通信息码字提取序列中得到载密提取数据;最后比较载密提取数据和载密数据是否相同;如果相同,则x取0,否则取c。

[0072] 将秘密信息码字序列长度及嵌入模式的序号等重要信息嵌入到二维码码字的补齐码区域中。

[0073] 实施例2

[0074] 如图1所示,本实施例提供的二维码信息隐藏及提取步骤流程如下:

[0075] 1) 普通信息经过数据分析、数据编码、纠错编码等过程后得到普通信息码字序列;秘密信息经过加密以及纠错编码后,得到秘密信息码字序列。

[0076] 2) 秘密信息码字通过嵌入算法选择合适的嵌入位置嵌入到普通信息码字序列中,

得到载密数据。

[0077] 嵌入算法的作用是对秘密信息和普通信息进行分析,选择适合的嵌入模式,并进行嵌入。嵌入模式有8种或更多。其中,4种固定嵌入模式,4种随机嵌入模式。固定嵌入模式是指秘密数据的嵌入位置是固定的。但固定位置嵌入可能会导致误码率过大等问题,因此引入随机嵌入模式。随机嵌入模式是指秘密数据的嵌入位置是随机的。随机嵌入位置由随机算法产生的随机数映射而来,而随机算法的种子则由普通信息变换而成。

[0078] 如图2所示,图2为随机嵌入位置算法图,以下以固定嵌入模式为例说明秘密信息的嵌入过程:

[0079] 假设固定嵌入模式1为在每8位普通数据的首位嵌入1位秘密数据。普通信息码字序列为1101111110111000000001011010000,秘密信息码字序列为0101。嵌入后,载密数据的码字序列为0101111110111000000001011010000。

[0080] 嵌入的码字序列为0101,普通码字序列对应位置的原始数据为1101,嵌入后有1位数据发生了改变。故嵌入位数据改变率为 $1/4=0.25$ ,非嵌入位数据改变率为 $0/28=0$ 。

[0081] 嵌入模式选择的依据是嵌入位数据改变率的大小,改变率小者优先;如果有多种嵌入模式嵌入位改变率并列最小,则选择编号靠前的嵌入模式。

[0082] 3) 载密数据生成二维码后以数字图像或印刷图像的形式进行传播。

[0083] 4) 普通用户使用普通扫码器扫码后,得到载密数据。载密数据经过纠错(秘密信息被当作错误纠正)得到普通码字序列,普通码字序列经过译码等变换后还原出普通信息。

[0084] 5) 需要获取秘密信息的用户采用本实施例提供的基于二维码的信息隐藏方法来进行扫码后,得到载密数据。载密数据通过嵌入位分析算法,提取出秘密信息码字序列,再经过纠错、解密等过程还原出秘密信息。

[0085] 嵌入位分析算法是分析编码方采用的何种嵌入模式。首先,分别按8种嵌入模式提取出“秘密信息的码字序列”;其次,对提取的“秘密信息码字序列”和载密数据进行纠错;再次,恢复出“秘密信息”和普通信息;最后,按以下公式对各嵌入模式的提取结果进行评分,分值最低者入选,如果多个嵌入模式评分并列最低,选取编号靠前者。

[0086] 嵌入模式提取结果评分公式:

$$[0087] \quad S=k_1 \times BER_1+k_2 \times BER_2+X;$$

[0088] 其中,S是提取结果评分, $k_1$ 和 $k_2$ 是常数, $BER_1$ 和 $BER_2$ 分别代表“秘密信息的码字序列”的误码率和非嵌入位数据的误码率。 $x=0$ 或者 $c$ ,将恢复出的“秘密信息”和普通信息重复步骤2,如果步骤2选择嵌入模式与提取“秘密信息”所使用的嵌入模式一致,则 $x$ 取0,否则取 $c$ 。

[0089] 例如, $k_1$ 取2, $k_2$ 取1, $c$ 取0.5。用嵌入模式1“秘密信息的码字序列”误码率为0.1,非嵌入位数据误码率为0.15,重复步骤2选取的嵌入模式为模式2,则嵌入模式1的提取结果评分为: $2 \times 0.1+1 \times 0.15+0.5=0.85$ 。

[0090] 为了便于准确的提取出秘密信息,可以将秘密信息长度及嵌入模式编号等重要信息嵌入到二维码码字的其他部分,如补齐码区域中。

[0091] 以下是没有嵌入秘密信息的二维码和嵌入了秘密信息的二维码之间的比对。

[0092] 图3为无秘密信息的二维码;普通信息:

[0093] Name:Daping Dou;



[0094] Birth Year:1950;

[0095] Past Medical History:cardiopathy.Nitroglycerin in his left packet,one pill enough!;

[0096] Home:No.133Chongwen Road Huangjueya town Nanan District Chongqing City。

[0097] 图4为隐藏有秘密信息的二维码;秘密信息:His son:Mr.Dou 13912345678。

[0098] 最后说明的是,以上实施例仅用以说明本发明的技术方案而非限制,尽管参照较佳实施例对本发明进行了详细说明,本领域的普通技术人员应当理解,可以对本发明的技术方案进行修改或者等同替换,而不脱离本技术方案的宗旨和范围,其均应涵盖在本发明的保护范围当中。

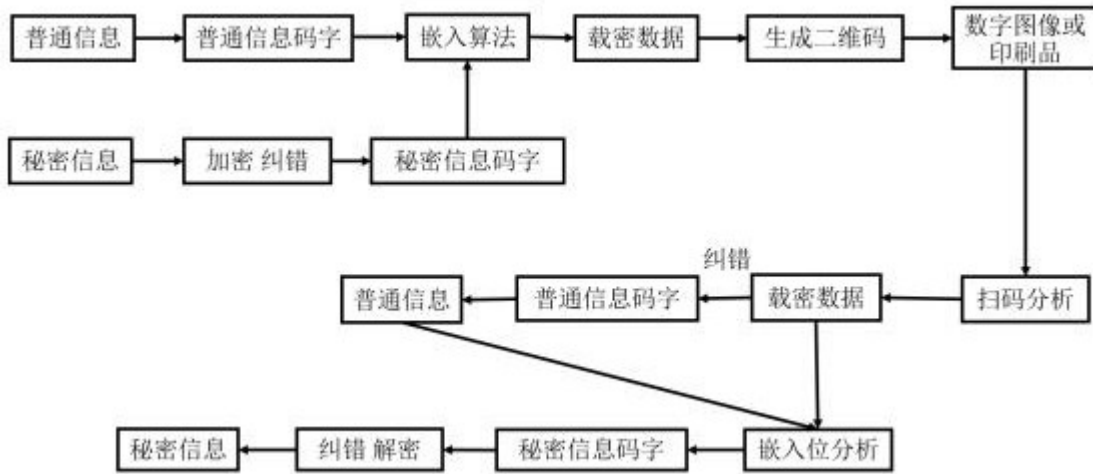


图1



图2



图3



图4