(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103136564 B
(45)授权公告日 2015.10.28

(21)申请号 201310022305.8

(22)申请日 2013.01.22

(73)专利权人 北京印刷学院
地址 102600 北京市大兴区兴华北路25号
北京印刷学院

(72)发明人 张立君

(51)Int.Cl.
G06K 19/067(2006.01)
G09F 3/02(2006.01)

(56)对比文件
CN 101537751 A ,2009.09.23,
CN 101777134 A ,2010.07.14,
CN 102402696 A ,2012.04.04,
CN 102831453 A ,2012.12.19,
US 2010060942 A1 ,2010.03.11,

审查员 戴自立

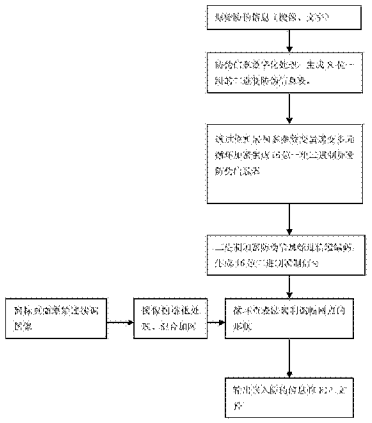
权利要求书3页 说明书6页 附图3页

(54)发明名称

多参数变量递变多元循环加密防伪信息存储商标

(57)摘要

一种多参数变量递变多元循环加密防伪信息存储商标，该商标可将二进制防伪信息通过多元循环加密和信道编码生成二进制调制信号，并通过循环查表法调制方式将防伪信息以调幅网点导电性能的有序改变嵌入在整个商标页面中，可在商标识别时从任意一个碎片里识别防伪信息，可以用于各种防伪的商标中。



CN 103136564 B

1. 一种将防伪信息通过加密运算和信道编码生成二进制调制信号，并通过循环查表调制方式将防伪信息嵌入在整个页面中的多参数变量递变多元循环加密防伪信息存储商标，其特征是：防伪信息存储商标，由商标页纸、印制在商标页纸上的调幅网点、印制在商标页纸上的行扫描线、印制在商标页纸上的列扫描线构成，根据存储的二进制加密防伪信息，商标页纸上的一部分调幅网点由导电油墨印制而成，商标页纸上的另一部分调幅网点由绝缘油墨印制而成，商标页纸上的行扫描线和列扫描线均由透明导电油墨印制而成，

为了实现商标防伪信息的加密存储，首先对图像防伪信息和文字防伪信息进行数字化处理，利用图像防伪信息和文字防伪信息生成 8 位一组的二进制防伪信息表，为防止加密过程中产生信息溢出，将二进制防伪信息表中的每一个 8 位一组二进制防伪信息扩展为 32 位一组二进制防伪信息，生成高 24 位全为 0 的 32 位一组二进制防伪信息表，将 32 位一组二进制防伪信息表中的第 i 组 32 位二进制防伪信息记作 N_i，将 32 位一组二进制加密防伪信息表中的第 i 组 32 位二进制加密防伪信息记作 H_i，i 为大于 0 的正整数，二进制加密参数分别记作 c_1、c_2、c_3、c_4、c_5、c_6、c_7和 c_8，加密参数 c_1、c_2、c_3、c_4、c_5、c_6、c_7和 c_8为 0 到 256 的二进制正整数，二进制加密变量分别记作 j、d、e、f、g、h、r、p 和 q，加密变量 j、d、e、f、g、h、r、p 和 q 为 0 到 256 的二进制正整数，二进制算符控制变量记作 k，二进制算符控制变量 k 为 $0 \leqq k \leqq 7$ 的二进制整数，算符 $@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$ 采用 +、−、× 三种算符，二进制算符控制变量 $k=0$ 时 $@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$ 分别定义为−、+、×、+、×、−、×、+，二进制算符控制变量 $k=1$ 时 $@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$ 分别定义为+、×、+、+、−、×、+、×，二进制算符控制变量 $k=2$ 时 $@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$ 分别定义为−、×、+、+、×、−、+、−，二进制算符控制变量 $k=3$ 时 $@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$ 分别定义为−、×、+、−、×、−、+、×，二进制算符控制变量 $k=4$ 时 $@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$ 分别定义为+、×、−、×、+、−、+、×，二进制算符控制变量 $k=5$ 时 $@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$ 分别定义为×、+、×、−、+、+、−、×，二进制算符控制变量 $k=6$ 时 $@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$ 分别定义为×、+、+、−、×、+、+、×，二进制算符控制变量 $k=7$ 时 $@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$ 分别定义为+、×、×、−、+、−、−、×，二进制算符控制变量 $k=0$ 时多元循环加密运算定义为 $H_i=(N_i+q)\ @_k^1\ (c_1+j)\ @_k^2\ (N_i+q)\ @_k^3\ (c_2+j)\ @_k^4\ (N_i+q)\ @_k^5\ (c_3+j)\ @_k^6\ (N_i+q)\ @_k^7\ (c_7+j)\ @_k^8\ (N_i+q)$，二进制算符控制变量 $k=1$ 时多元循环加密运算定义为 $H_i=(N_i+j)\ @_k^1\ (c_3+d)\ @_k^2\ (N_i+j)\ @_k^3\ (c_4+d)\ @_k^4\ (N_i+j)\ @_k^5\ (c_6+d)\ @_k^6\ (N_i+j)\ @_k^7\ (c_8+d)\ @_k^8\ (N_i+j)$，二进制算符控制变量 $k=2$ 时多元循环加密运算定义为 $H_i=(N_i+d)\ @_k^1\ (c_1+e)\ @_k^2\ (N_i+d)\ @_k^3\ (c_2+e)\ @_k^4\ (N_i+d)\ @_k^5\ (c_5+e)$

$@_k^6(N_i+d)\ @_k^7(c_7+e)\ @_k^8(N_i+d)$，二进制算符控制变量k＝3时多元循环加密运算定义为

$H_i=(N_i+e)\ @_k^1(c_2+f)\ @_k^2(N_i+e)\ @_k^3(c_4+f)\ @_k^4(N_i+e)\ @_k^5(c_6+f)\ @_k^6(N_i+e)\ @_k^7(c_8+f)\ @_k^8(N_i+e)$，二进制算符控制变量k＝4时多元循环加密运算定义为

$H_i=(N_i+f)\ @_k^1(c_1+g)\ @_k^2(N_i+f)\ @_k^3(c_3+g)\ @_k^4(N_i+f)\ @_k^5(c_5+g)\ @_k^6(N_i+f)\ @_k^7(c_7+g)\ @_k^8(N_i+f)$，二进制算符控制变量k＝5时多元循环加密运算定义为$H_i=(N_i+g)\ @_k^1(c_2+h)\ @_k^2(N_i+g)\ @_k^3(c_4+h)\ @_k^4(N_i+g)\ @_k^5(c_6+h)\ @_k^6(N_i+g)\ @_k^7(c_8+h)\ @_k^8(N_i+g)$，二进制算符控制变量k＝6时多元循环加密运算定义为$H_i=(N_i+h)\ @_k^1(c_1+r)\ @_k^2(N_i+h)\ @_k^3(c_3+r)\ @_k^4(N_i+h)\ @_k^5(c_5+r)\ @_k^6(N_i+h)\ @_k^7(c_7+r)\ @_k^8(N_i+h)$，二进制算符控制变量k＝7时多元循环加密运算定义为$H_i=(N_i+r)\ @_k^1(c_2+p)\ @_k^2(N_i+r)\ @_k^3(c_4+p)\ @_k^4(N_i+r)\ @_k^5(c_6+p)\ @_k^6(N_i+r)\ @_k^7(c_8+p)\ @_k^8(N_i+r)$，设定加密参数$c_1$、$c_2$、$c_3$、$c_4$、$c_5$、$c_6$、$c_7$和$c_8$的初值，设定加密变量j、d、e、f、g、h、r、p和q的初值，设定二进制算符控制变量k的初值为k＝0，设定32位一组二进制防伪信息表中32位二进制防伪信息N_i的位置控制变量i＝1，设定32位一组二进制加密防伪信息表中32位二进制加密防伪信息H_i的位置控制变量i＝1，对N_1进行

$H_1=(N_1+q)\ @_k^1(c_1+j)\ @_k^2(N_1+q)\ @_k^3(c_3+j)\ @_k^4(N_1+q)\ @_k^5(c_5+j)\ @_k^6(N_1+q)\ @_k^7(c_7+j)\ @_k^8(N_1+q)$多元循环加密运算，其中k＝0，生成32位一组的二进制加密防伪信息表中的第一组二进制加密防伪信息H_1，对N_1进行 $H_1=(N_1+q)\ @_k^1(c_1+j)\ @_k^2(N_1+q)\ @_k^3(c_3+j)\ @_k^4(N_1+q)\ @_k^5(c_5+j)\ @_k^6(N_1+q)\ @_k^7(c_7+j)\ @_k^8(N_1+q)$多元循环加密运算的同时进行i+1、j+1、d+1、e+1、f+1、g+1、h+1、r+1、p+1、q+1和k+1运算，使下一个多元循环加密运算指向$H_2=(N_2+j)\ @_k^1(c_2+d)\ @_k^2(N_2+j)\ @_k^3(c_4+d)\ @_k^4(N_2+j)\ @_k^5(c_6+d)\ @_k^6(N_2+j)\ @_k^7(c_8+d)\ @_k^8(N_2+j)$，其中k＝1，生成32位一组的二进制加密防伪信息表中的第二组二进制加密防伪信息H_2，对N_2进行 $H_2=(N_2+j)\ @_k^1(c_2+d)\ @_k^2(N_2+j)\ @_k^3(c_4+d)\ @_k^4(N_2+j)\ @_k^5(c_6+d)\ @_k^6(N_2+j)\ @_k^7(c_8+d)\ @_k^8(N_2+j)$多元循环加密运算的同时进行i+1、j+1、d+1、e+1、f+1、g+1、h+1、r+1、p+1、q+1和k+1运算，使下一个多元循环加密运算指向

$H_3=(N_3+d)\ @_k^1(c_1+e)\ @_k^2(N_3+d)\ @_k^3(c_3+e)\ @_k^4(N_3+d)\ @_k^5(c_5+e)\ @_k^6(N_3+d)\ @_k^7$

$(c_7+e)@_k^0(N_3+d)$，其中 k = 2，生成 32 位一组的二进制加密防伪信息表中的第三组二进制加密防伪信息 H_3，上述加密运算一直进行下去直到二进制防伪信息表中的最后一组 32 位二进制防伪信息，通过对 32 位一组二进制防伪信息表中的每一组 32 位二进制防伪信息 N_i 进行多元循环加密运算，生成与 32 位一组二进制防伪信息表对应的 32 位一组二进制加密防伪信息表，对商标印刷中调幅网点进行数字化处理，将调幅网点设置为两种，其中由绝缘油墨印制而成的调幅网点定义为数字 0、由导电油墨印制而成的调幅网点定义为数字 1，在商标印刷过程中利用生成的 32 位一组的二进制加密防伪信息通过循环查表法调制商标页面上的调幅网点的印制过程，通过选择绝缘油墨和导电油墨印制调幅网点使商标页面上的调幅网点有规律的按照上述两种调幅网点的导电性能进行变化，调制后商标页面上相邻 32 个调幅网点构成一组 32 位二进制信息，使得商标页面上通过调幅网点导电性能的变化携带防伪信息，并使该防伪信息嵌入在整个商标页面网点中，实现商标防伪。

多参数变量递变多元循环加密防伪信息存储商标

技术领域：

[0001] 本发明涉及一种防伪商标，特别是一种多参数变量递变多元循环加密防伪信息存储商标，该商标可将二进制加密防伪信息保存在商标页面上实现商标的防伪，该商标可以用于各种商品的防伪中。

背景技术：

[0002] 防伪商标，又称防伪标签、防伪标识、防伪标志、防伪标贴，是一种鉴别真伪、防止假冒的证明性标贴物，是商品流通过程中人们用于区别商品来源的真假、区分商品品质优劣的标志。商标防伪关系到商家、客户和市场安全，关系到保护商家及客户的利益。我国的商标进行了大胆地创新，采用了激光防伪、核微孔防伪、隐形图文防伪、磁性油墨防伪、缩微文字防伪、标记分布防伪、光雕防伪等，但防伪与造假的斗争是高科技的较量，再先进的防伪技术都有一定的时效性，所以，必须不断提升商标防伪技术，才能在防伪与造假中永远处于领先地位，这也是保护商家和客户的利益维系商品流通安全的根本保证。

发明内容：

[0003] 为了提高商标防伪的可靠性和安全性，本发明针对现有商标防伪存在的不足对现有商标防伪技术进行了改进，提出了一种防伪信息存储商标，该商标通过对商标印制中调幅网点导电性能的改变，将加密防伪信息以二进制加密信号形式嵌入在整个商标页面上，可在商标识别时从任意一个碎片里识别加密防伪信息，因此具有很强隐蔽性和抗碎性。

[0004] 本发明解决其技术问题所采用的技术方案是：

[0005] 防伪信息存储商标，由商标页纸、印制在商标页纸上的调幅网点、印制在商标页纸上的行扫描线、印制在商标页纸上的列扫描线构成，商标页纸上的图像和文字由调幅网点构成，

[0006] 根据存储的二进制加密防伪信息，商标页纸上的一部分调幅网点由导电油墨印制而成，商标页纸上的另一部分调幅网点由绝缘油墨印制而成，商标页纸上的行扫描线和列扫描线均由透明导电油墨印制而成，

[0007] 印制在商标页纸上的行扫描线有 N 条，印制在商标页纸上的列扫描线有 M 条，印制在商标页纸上的调幅网点在商标纸面上被分为 N 行 M 列，调幅网点在商标页纸纸面上整齐呈矩阵排列，让 i 取 1 到 N，让 j 取 1 到 M，商标页纸上的第 j 条列扫描线与商标页纸上的第 j 列的各个调幅网点的底表面电连接，商标页纸上的第 i 条行扫描线与商标页纸上的第 i 行的各个调幅网点的上表面电连接，

[0008] 当需要将商标页面存储的二进制信息读出时，将商标页纸上的第 1 条到第 N 条行扫描线依次置为高电平，

[0009] 当商标页纸上的第 1 条行扫描线置为高电平时，商标页纸上的第 1 行存储的二进制信息以 0、1 代码形式从第 1 条列扫描线到第 M 条列扫描线输出，商标页纸上的第 1 行由导电油墨印制而成的调幅网点输出二进制信息 1，商标页纸上的第 1 行由绝缘油墨印制而

成的调幅网点输出二进制信息0，对商标页纸上的其它行可重复上述读出过程，

[0010] 为了实现商标防伪信息的加密存储，首先对图像防伪信息和文字防伪信息进行数字化处理，利用图像防伪信息和文字防伪信息生成8位一组的二进制防伪信息表，为防止加密过程中产生信息溢出，将二进制防伪信息表中的每一个8位一组二进制防伪信息扩展为32位一组二进制防伪信息，生成高24位全为0的32位一组二进制防伪信息表，将32位一组二进制防伪信息表中的第i组32位二进制防伪信息记作N_i，将32位一组二进制加密防伪信息表中的第i组32位二进制加密防伪信息记作H_i，i为大于0的正整数，二进制加密参数分别记作c_1、c_2、c_3、c_4、c_5、c_6、c_7和c_8，加密参数c_1、c_2、c_3、c_4、c_5、c_6、c_7和c_8为0到256的二进制正整数，二进制加密变量分别记作j、d、e、f、g、h、r、p和q，加密变量j、d、e、f、g、h、r、p和q为0到256的二进制正整数，二进制算符控制变量记作k，二进制算符控制变量k为$0 \leqq k \leqq 7$的二进制整数，算符$@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$采用+、－、×三种算符，二进制算符控制变量$k=0$时$@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$分别定义为－、+、×、+、×、－、×、+，二进制算符控制变量$k=1$时$@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$分别定义为+、×、+、+、－、×、+、×，二进制算符控制变量$k=2$时$@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$分别定义为－、×、+、+、×、－、+、－，二进制算符控制变量$k=3$时$@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$分别定义为－、×、+、－、×、－、+、×，二进制算符控制变量$k=4$时$@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$分别定义为+、×、－、×、+、－、+、×，二进制算符控制变量$k=5$时$@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$分别定义为×、+、×、－、+、+、－、×，二进制算符控制变量$k=6$时$@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$分别定义为×、+、+、－、×、+、+、×，二进制算符控制变量$k=7$时$@_k^1\ @_k^2\ @_k^3\ @_k^4\ @_k^5\ @_k^6\ @_k^7\ @_k^8$分别定义为+、×、×、－、+、－、－、×，二进制算符控制变量$k=0$时多元循环加密运算定义为$H_i=(N_i+q)\ @_k^1\ (c_1+j)\ @_k^2\ (N_i+q)\ @_k^3\ (c_3+j)\ @_k^4\ (N_i+q)\ @_k^5\ (c_5+j)\ @_k^6\ (N_i+q)\ @_k^7\ (c_7+j)\ @_k^8\ (N_i+q)$，二进制算符控制变量$k=1$时多元循环加密运算定义为$H_i=(N_i+j)\ @_k^1\ (c_2+d)\ @_k^2\ (N_i+j)\ @_k^3\ (c_4+d)\ @_k^4\ (N_i+j)\ @_k^5\ (c_6+d)\ @_k^6\ (N_i+j)\ @_k^7\ (c_8+d)\ @_k^8\ (N_i+j)$，二进制算符控制变量$k=2$时多元循环加密运算定义为$H_i=(N_i+d)\ @_k^1\ (c_1+e)\ @_k^2\ (N_i+d)\ @_k^3\ (c_3+e)\ @_k^4\ (N_i+d)\ @_k^5\ (c_5+e)\ @_k^6\ (N_i+d)\ @_k^7\ (c_7+e)\ @_k^8\ (N_i+d)$，二进制算符控制变量$k=3$时多元循环加密运算定义为

$H_i=(N_i+e)\ @_k^1\ (c_2+f)\ @_k^2\ (N_i+e)\ @_k^3\ (c_4+f)\ @_k^4\ (N_i+e)\ @_k^5\ (c_6+f)\ @_k^6\ (N_i+e)\ @_k^7\ (c_8+f)\ @_k^8\ (N_i+e)$，二进制算符控制变量$k=4$时多元循环加密运算定义为$H_i=(N_i+f)\ @_k^1$

$(c_1+g)\ @_k^2\ (N_i+f)\ @_k^3\ (c_3+g)\ @_k^4\ (N_i+f)\ @_k^5\ (c_5+g)\ @_k^6\ (N_i+f)\ @_k^7\ (c_7+g)\ @_k^8\ (N_i+f)$，二进制算符控制变量 k ＝ 5 时多元循环加密运算定义为 $H_i=(N_i+g)\ @_k^1\ (c_2+h)\ @_k^2\ (N_i+g)\ @_k^3\ (c_4+h)\ @_k^4\ (N_i+g)\ @_k^5\ (c_6+h)\ @_k^6\ (N_i+g)\ @_k^7\ (c_8+h)\ @_k^8\ (N_i+g)$，二进制算符控制变量 k ＝ 6 时多元循环加密运算定义为 $H_i=(N_i+h)\ @_k^1\ (c_1+r)\ @_k^2\ (N_i+h)\ @_k^3\ (c_3+r)\ @_k^4\ (N_i+h)\ @_k^5\ (c_5+r)\ @_k^6\ (N_i+h)\ @_k^7\ (c_7+r)\ @_k^8\ (N_i+h)$，二进制算符控制变量 k ＝ 7 时多元循环加密运算定义为 $H_i=(N_i+r)\ @_k^1\ (c_2+p)\ @_k^2\ (N_i+r)\ @_k^3\ (c_4+p)\ @_k^4\ (N_i+r)\ @_k^5\ (c_6+p)\ @_k^6\ (N_i+r)\ @_k^7\ (c_8+p)\ @_k^8\ (N_i+r)$，设定加密参数 c_1、c_2、c_3、c_4、c_5、c_6、c_7和 c_8的初值，设定加密变量 j、d、e、f、g、h、r、p 和 q 的初值，设定二进制算符控制变量 k 的初值为 k ＝ 0，设定 32 位一组二进制防伪信息表中 32 位二进制防伪信息 N_i的位置控制变量 i ＝ 1，设定 32 位一组二进制加密防伪信息表中 32 位二进制加密防伪信息 H_i的位置控制变量 i ＝ 1，对 N_1进行

$H_1=(N_1+q)\ @_k^1\ (c_1+j)\ @_k^2\ (N_1+q)\ @_k^3\ (c_3+j)\ @_k^4\ (N_1+q)\ @_k^5\ (c_5+j)\ @_k^6\ (N_1+q)\ @_k^7\ (c_7+j)\ @_k^8\ (N_1+q)$ 多元循环加密运算，其中 k ＝ 0，生成 32 位一组的二进制加密防伪信息表中的第一组二进制加密防伪信息 H_1，对 N_1进行 $H_1=(N_1+q)\ @_k^1\ (c_1+j)\ @_k^2\ (N_1+q)\ @_k^3\ (c_3+j)\ @_k^4\ (N_1+q)\ @_k^5\ (c_5+j)\ @_k^6\ (N_1+q)\ @_k^7\ (c_7+j)\ @_k^8\ (N_1+q)$多元循环加密运算的同时进行 i+1、j+1、d+1、e+1、f+1、g+1、h+1、r+1、p+1、q+1 和 k+1 运算，使下一个多元循环加密运算指向 $H_2=(N_2+j)\ @_k^1\ (c_2+d)\ @_k^2\ (N_2+j)\ @_k^3\ (c_4+d)\ @_k^4\ (N_2+j)\ @_k^5\ (c_6+d)\ @_k^6\ (N_2+j)\ @_k^7\ (c_8+d)\ @_k^8\ (N_2+j)$，其中 k ＝ 1，生成 32 位一组的二进制加密防伪信息表中的第二组二进制加密防伪信息 H_2，对 N_2进行 $H_2=(N_2+j)\ @_k^1\ (c_2+d)\ @_k^2\ (N_2+j)\ @_k^3\ (c_4+d)\ @_k^4\ (N_2+j)\ @_k^5\ (c_6+d)\ @_k^6\ (N_2+j)\ @_k^7\ (c_8+d)\ @_k^8\ (N_2+j)$多元循环加密运算的同时进行 i+1、j+1、d+1、e+1、f+1、g+1、h+1、r+1、p+1、q+1 和 k+1 运算，使下一个多元循环加密运算指向

$H_3=(N_3+d)\ @_k^1\ (c_1+e)\ @_k^2\ (N_3+d)\ @_k^3\ (c_3+e)\ @_k^4\ (N_3+d)\ @_k^5\ (c_5+e)\ @_k^6\ (N_3+d)\ @_k^7\ (c_7+e)\ @_k^8\ (N_3+d)$，其中 k ＝ 2，生成 32 位一组的二进制加密防伪信息表中的第三组二进制加密防伪信息 H_3，上述加密运算一直进行下去直到二进制防伪信息表中的最后一组 32 位二进制防伪信息，通过对 32 位一组二进制防伪信息表中的每一组 32 位二进制防伪信息 N_i进行多元循环加密运算，生成与 32 位一组二进制防伪信息表对应的 32 位一组二进制加密防伪信息表，对商标印刷中调幅网点进行数字化处理，将调幅网点设置为两种，其中由绝缘油墨印制而成的调幅网点定义为数字 0、由导电油墨印制而成的调幅网点定义为数字 1，在

商标印刷过程中利用生成的32位一组的二进制加密防伪信息通过循环查表法调制商标页面上的调幅网点的印制过程，通过选择绝缘油墨和导电油墨印制调幅网点使商标页面上的调幅网点有规律的按照上述两种调幅网点的导电性能进行变化，调制后商标页面上相邻32个调幅网点构成一组32位二进制信息，使得商标页面上通过调幅网点导电性能的变化携带防伪信息，并使该防伪信息嵌入在整个商标页面网点中，实现商标防伪，通过在商标页面中非显见地嵌入可提取的防伪信息，能够为真商标提供有效证明，同时具有较强的抗伪造能力。

[0011] 为解决上述的技术问题，首先对图像防伪信息和文字防伪信息进行数字化处理，生成8位一组的二进制防伪信息表，将二进制防伪信息表中的每一个8位一组二进制防伪信息扩展为32位一组二进制防伪信息，生成高24位全为0的32位一组二进制防伪信息表，对32位一组二进制防伪信息表中的每一个32位二进制防伪信息进行多元循环加密运算，生成32位一组的二进制加密防伪信息表，利用二进制加密防伪信息表中的32位二进制加密防伪信息经过信道编码，生成具有检错和纠错功能的32位一组的二进制调制信号，信道编码可以采用循环编码、卷积编码或Turbo编码多种形式，将商标页面原始连续调图像信号经过栅格化处理(RIP)和混合加网输出半色调混合加网图像信号，其中包括调幅网点和调频网点图像信号，利用生成的32位一组二进制调制信号采用循环查表法调制方式调制混合加网图像信号中调幅网点的导电性能，使调幅网点的导电性能按照绝缘油墨调幅网点和导电油墨调幅网点有规律的发生改变，使混合加网图像信号中相邻32个调幅网点通过导电性能的改变携带32位二进制防伪信息，从而生成在整个商标页面网点中嵌入防伪信息的混合加网图像信号，实现商标的防伪。

[0012] 在提取防伪信息时，首先采集商标页面网点导电性能信号，经过对调幅网点的导电性能的识别，分辨调幅网点的导电性，提取调幅网点的导电性能信息，解调商标页面调幅网点的导电性能信息，输出32位一组的二进制调制信号，对解调输出的32位一组的二进制调制信号进行信道解码，信道解码后生成二进制解密防伪信息表，将二进制解密防伪信息表中的第i组32位二进制信息记作M_i。

[0013] 将二进制解密防伪信息表中32位二进制信息M_i的位置控制变量i的初值设定为i＝1，设定加密参数c_1、c_2、c_3、c_4、c_5、c_6、c_7和c_8的初值为加密时的初值，设定加密变量j、d、e、f、g、h、r、p和q的初值为加密时的初值，二进制算符控制变量k的初值设定为k＝0，通过多元循环加密过程可知，二进制算符控制变量k＝0时解密运算为$M_i=(N_i+q)\ @_k^1(c_1+j)\ @_k^2(N_i+q)\ @_k^3(c_3+j)\ @_k^4(N_i+q)\ @_k^5(c_5+j)\ @_k^6(N_i+q)\ @_k^7(c_7+j)\ @_k^8(N_i+q)$，二进制算符控制变量k＝1时解密运算为$M_i=(N_i+j)\ @_k^1(c_2+d)\ @_k^2(N_i+j)\ @_k^3(c_4+d)\ @_k^4(N_i+j)\ @_k^5(c_6+d)\ @_k^6(N_i+j)\ @_k^7(c_8+d)\ @_k^8(N_i+j)$，二进制算符控制变量k＝2时解密运算为

$M_i=(N_i+d)\ @_k^1(c_1+e)\ @_k^2(N_i+d)\ @_k^3(c_3+e)\ @_k^4(N_i+d)\ @_k^5(c_5+e)\ @_k^6(N_i+d)\ @_k^7(c_7+e)\ @_k^8(N_i+d)$，二进制算符控制变量k＝3时解密运算为$M_i=(N_i+e)\ @_k^1(c_2+f)\ @_k^2$

$(N_i+e)\ @_k^3\ (c_4+f)\ @_k^4\ (N_i+e)\ @_k^5\ (c_8+f)\ @_k^6\ (N_i+e)\ @_k^7\ (c_2+f)\ @_k^8\ (N_i+e)$，二进制算符控制变量 k = 4 时解密运算为 $M_i=(N_i+f)\ @_k^1\ (c_1+g)\ @_k^2\ (N_i+f)\ @_k^3\ (c_3+g)\ @_k^4\ (N_i+f)\ @_k^5\ (c_5+g)\ @_k^6\ (N_i+f)\ @_k^7\ (c_7+g)\ @_k^8\ (N_i+f)$，二进制算符控制变量 k = 5 时解密运算为 $M_i=(N_i+g)\ @_k^1\ (c_3+h)\ @_k^2\ (N_i+g)\ @_k^3\ (c_4+h)\ @_k^4\ (N_i+g)\ @_k^5\ (c_6+h)\ @_k^6\ (N_i+g)\ @_k^7\ (c_8+h)\ @_k^8\ (N_i+g)$，二进制算符控制变量 k = 6 时解密运算为 $M_i=(N_i+h)\ @_k^1\ (c_1+r)\ @_k^2\ (N_i+h)\ @_k^3\ (c_3+r)\ @_k^4\ (N_i+h)\ @_k^5\ (c_5+r)\ @_k^6\ (N_i+h)\ @_k^7\ (c_7+r)\ @_k^8\ (N_i+h)$，二进制算符控制变量 k = 7 时解密运算为 $M_i=(N_i+r)\ @_k^1\ (c_2+p)\ @_k^2\ (N_i+r)\ @_k^3\ (c_4+p)\ @_k^4\ (N_i+r)\ @_k^5\ (c_6+p)\ @_k^6\ (N_i+r)\ @_k^7\ (c_8+p)\ @_k^8\ (N_i+r)$，从二进制解密防伪信息表中第一位 M_1 开始，对二进制解密防伪信息表中的每一个 32 位二进制信息 M_i 进行相应的解密运算，解出二进制防伪信息 N_i，生成高 24 位全为 0 的 32 位一组二进制防伪信息表，去掉高 24 位，恢复生成 8 位一组的二进制防伪信息表，恢复防伪信号并输出防伪信息。

附图说明

[0014] 下面结合附图对本发明进一步说明。

[0015] 图 1 是本发明的整体结构图。

[0016] 图 2 是本发明的 A—A 剖视图。

[0017] 图 3 加载防伪信息流程图。

[0018] 图 4 提取防伪信息流程图。

具体实施方式

[0019] 如图 1 和图 2 中，加密防伪信息存储商标，由商标页纸 7-1、印制在商标页纸 7-1 上的调幅网点 6-1 到 6-150、印制在商标页纸 7-1 上的行扫描线 1-1 到 1-15、印制在商标页纸 7-1 上的列扫描线 2-1 到 2-10 构成，商标页纸 7-1 上的图像和文字由调幅网点 6-1 到 6-150 构成，根据存储二进制加密防伪信息，商标页纸 7-1 上的一部分调幅网点由导电油墨印制而成，商标页纸 7-1 上的另一部分调幅网点由绝缘油墨印制而成，商标页纸 7-1 上的行扫描线 1-1 到 1-15 和列扫描线 2-1 到 2-10 由透明导电油墨印制而成，

[0020] 图 1 中，商标页纸 7-1 上的深色调幅网点由导电油墨印制而成，商标页纸 7-1 上的浅色调幅网点由绝缘油墨印制而成，

[0021] 印制在商标页纸 7-1 上的调幅网点在商标纸面上被分为 15 行 10 列，调幅网点 6-1 到 6-150 在商标页纸 7-1 上整齐呈矩阵排列，让 i 取 1 到 15，让 j 取 1 到 10，商标页纸 7-1 上的第 j 条列扫描线与商标页纸 7-1 上的第 j 列的各个调幅网点的底表面电连接，商标页纸 7-1 上的第 i 条行扫描线与商标页纸 7-1 上的第 i 行的各个调幅网点的上表面电连接，

[0022] 当需要将商标页面存储的二进制加密防伪信息读出时，将商标页纸 7-1 上的第 1 条行扫描线到第 15 条行扫描线依次置为高电平，

[0023] 当商标页纸 7-1 上的第 1 条行扫描线 1-1 置为高电平时，商标页纸 7-1 上的第 1

行存储的二进制加密防伪信息以0、1代码形式从第1条列扫描线到第10条列扫描线输出，商标页纸7-1上的第1行由导电油墨印制而成调幅网点输出二进制信息1，商标页纸7-1上的第1行由绝缘油墨印制而成调幅网点输出二进制信息0，因此第1行读出的二进制加密防伪信息1100001000，对商标页纸7-1上的其它行可重复上述读出过程。

[0024] 在加载防伪信息流程图3中，原始防伪信息（图像、文字）经数字化处理，生成8位一组的二进制防伪信息表，将二进制防伪信息表中的8位一组二进制信息扩展为32位一组二进制信息，生成高24位全为0的32位一组二进制防伪信息表，32位一组二进制防伪信息表中的第i组32位二进制信息记作N_i，i为大于0的正整数，从32位一组二进制防伪信息表中的第一个32位二进制加密防伪信息N_1开始，对32位一组二进制防伪信息表中的每一个32位二进制防伪信息N_i进行多元循环加密运算，生成与32位一组二进制防伪信息表对应的32位一组二进制加密防伪信息表，对商标印刷中调幅网点进行数字化处理，将调幅网点设置为两种，其中由绝缘油墨印制而成的调幅网点定义为数字0、由导电油墨印制而成的调幅网点定义为数字1，在商标印刷过程中利用生成的32位一组的二进制加密防伪信息通过循环查表法调制商标页面上的调幅网点的印制过程，通过选择绝缘油墨和导电油墨印制调幅网点使商标页面上的调幅网点有规律的按照上述两种调幅网点的导电性能进行变化，调制后商标页面上相邻32个调幅网点构成一组32位二进制信息，使得商标页面上通过调幅网点导电性能的变化携带防伪信息，并使该防伪信息嵌入在整个商标页面网点中，实现商标防伪印刷，通过在商标页面中非显见地嵌入可提取的防伪信息，实现商标防伪。

[0025] 在提取防伪信息流程图4中，在提取防伪信息时，首先采集商标页面网点图像的导电性能信号，经过对调幅网点的导电性能识别，分辨调幅网点的导电性能，提取调幅网点的导电性能信息，解调商标页面调幅网点的导电性能信息，输出32位一组的二进制调制信号，对解调输出的32位一组的二进制调制信号进行信道解码，信道解码后生成二进制解密防伪信息表。

[0026] 将解码后生成的二进制解密防伪信息表中32位二进制信息M_i的位置控制变量i的初值设定为$i = 1$，设定加密参数的初值为加密时的初值，设定加密变量的初值为加密时的初值，二进制算符控制变量k的初值设定为$k = 0$，从生成的二进制解密防伪信息表中第一位M_1开始，对二进制解密防伪信息表中的每一个32位二进制信息M_i进行解密运算，解出二进制防伪信息N_i，生成高24位全为0的32位一组二进制防伪信息表，去掉高24位，恢复生成8位一组的二进制防伪信息表，恢复防伪信号并输出防伪信息。

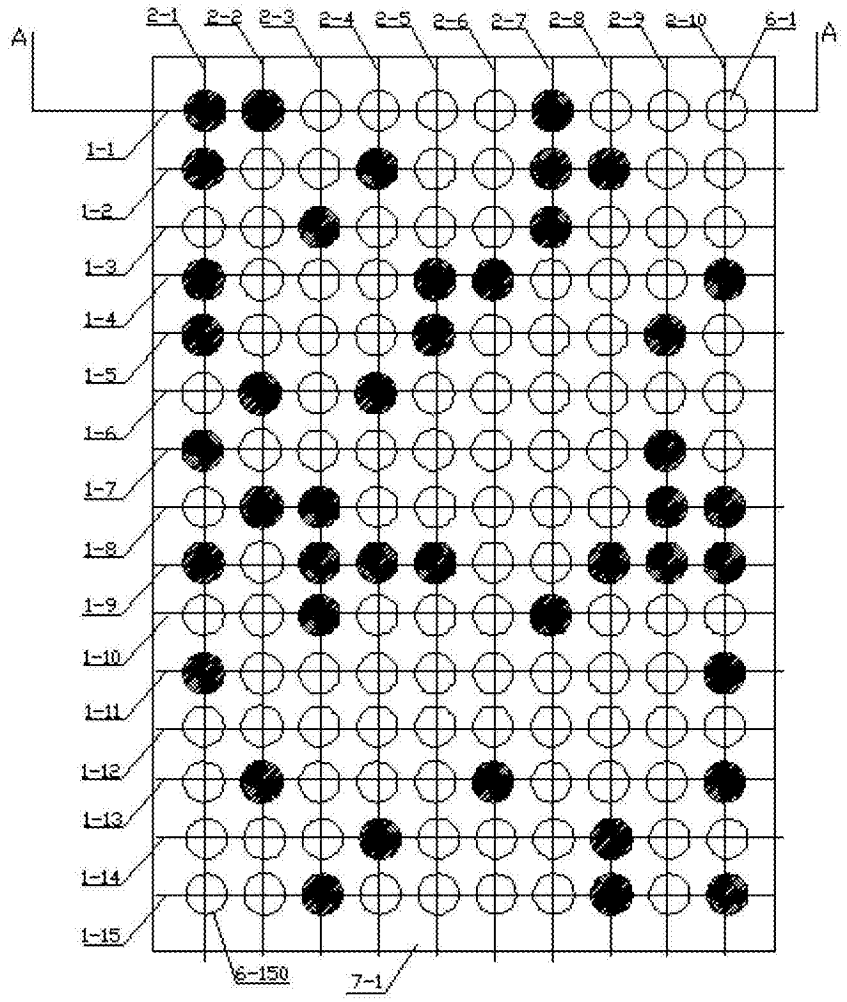

A
A
2-1
2-2
2-3
2-4
2-5
2-6
2-7
2-8
2-9
2-10
6-1
1-1
1-2
1-3
1-4
1-5
1-6
1-7
1-8
1-9
1-10
1-11
1-12
1-13
1-14
1-15
6-150
7-1

图 1

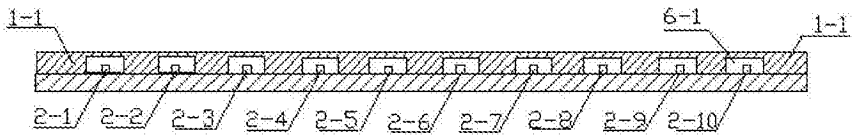

1-1
6-1
1-1
2-1
2-2
2-3
2-4
2-5
2-6
2-7
2-8
2-9
2-10

图 2

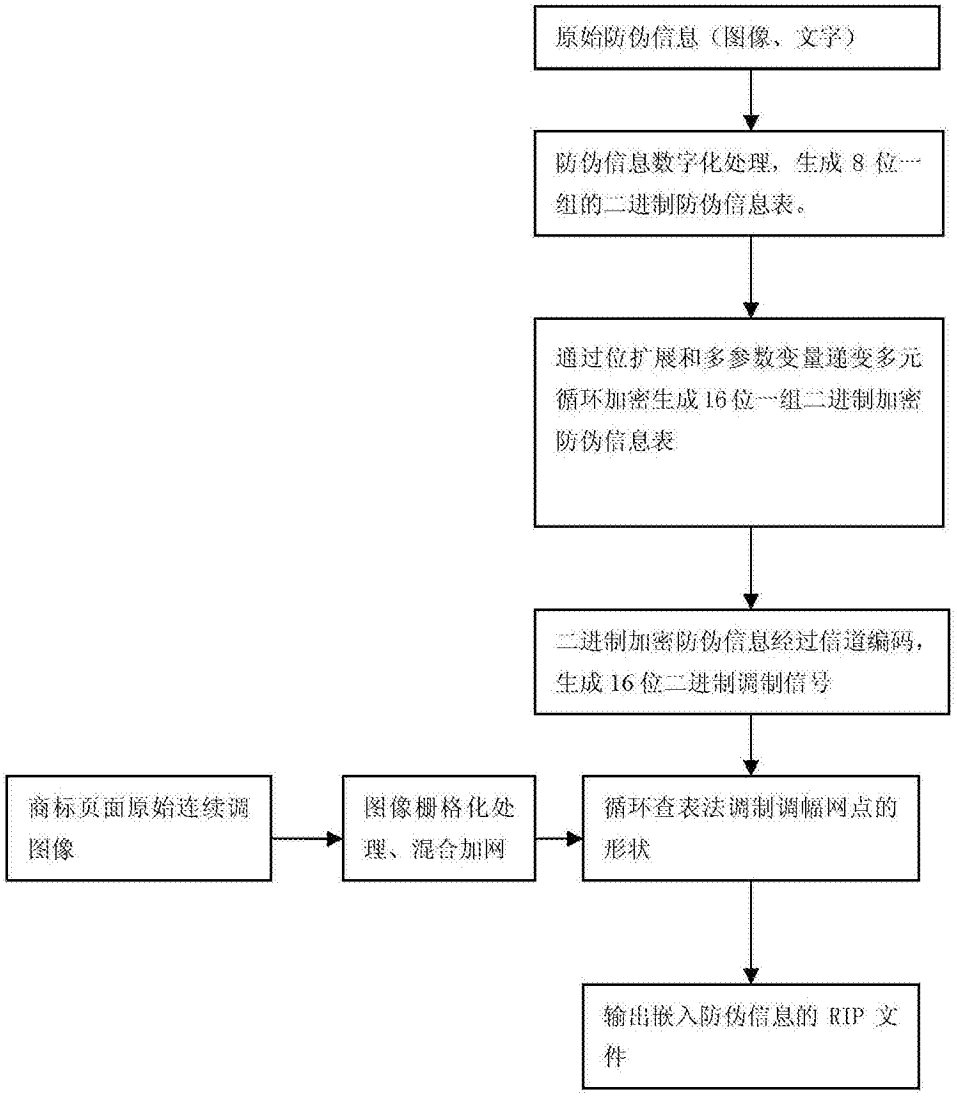

原始防伪信息（图像、文字）
防伪信息数字化处理，生成 8 位一组的二进制防伪信息表。
通过位扩展和多参数变量递变多元循环加密生成 16 位一组二进制加密防伪信息表
二进制加密防伪信息经过信道编码，生成 16 位二进制调制信号
商标页面原始连续调图像
图像栅格化处理、混合加网
循环查表法调制调幅网点的形状
输出嵌入防伪信息的 RIP 文件

图 3

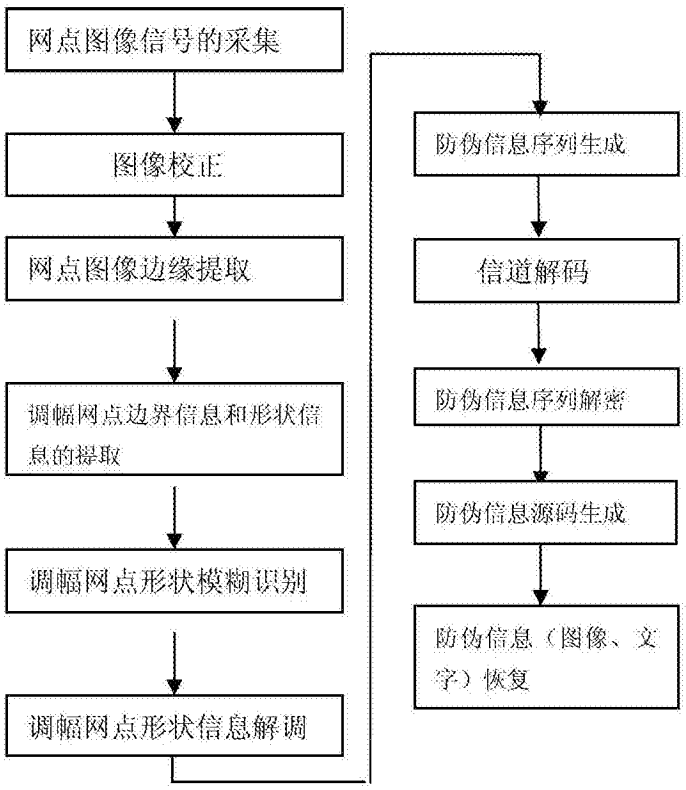

网点图像信号的采集
图像校正
网点图像边缘提取
调幅网点边界信息和形状信息的提取
调幅网点形状模糊识别
调幅网点形状信息解调
防伪信息序列生成
信道解码
防伪信息序列解密
防伪信息源码生成
防伪信息（图像、文字）恢复

图 4