(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107426465 A
(43)申请公布日 2017.12.01

(21)申请号 201710441829.9

(22)申请日 2017.06.13

(71)申请人 南京邮电大学
地址 210003 江苏省南京市鼓楼区新模范马路66号

(72)发明人 张迎周 赵莲 陈星昊 王星 尹秀

(74)专利代理机构 南京知识律师事务所 32207
代理人 张芳

(51)Int.Cl.
H04N 1/32(2006.01)

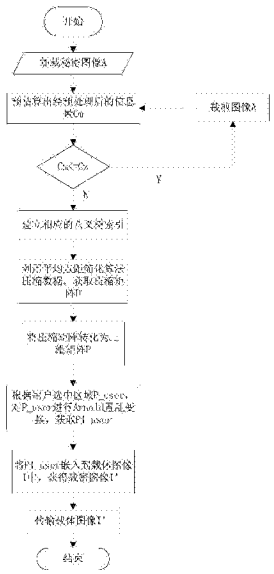
权利要求书2页 说明书5页 附图3页

(54)发明名称

基于预处理机制的图像信息隐藏方法

(57)摘要

本发明公开一种基于预处理机制的图像信息隐藏方法，包括加载信息、构建八叉树索引、数据压缩、加密信息，嵌入信息以及图像传输。提高了压缩效率，也进一步提高了信息隐藏算法的隐蔽性，降低了秘密信息被破解的概率，实现了更加安全的数据隐藏。



CN 107426465 A

1.基于预处理机制的图像信息隐藏方法，其特征在于，包括以下步骤：

步骤1、加载秘密信息：读取待处理图像信息，预估计出经过预处理后的信息量Cm；然后加载载体图像，计算出载体图像能够容纳的信息量Cz；比较Cm与Cz大小，如果前者大，则裁剪秘密信息，如果后者大，则继续执行下一步；

步骤2、数据压缩：将秘密信息用三维矩阵表示，接着构建八叉树索引，并将相关索引存储到指针数组中，利用中心点提取简化算法进行简化数据；

步骤3、数据加密：先将压缩后的三维数据矩阵转化为二维数据矩阵，然后用户选取加密区域，并使用Arnold置乱算法对用户选中区域加密，最后获取加密后的秘密信息；

步骤4、嵌入信息以及图像传输：选取原始载体图像的前6个像素，将秘密信息的描述信息存储其中；接着采用隐写算法将秘密信息嵌入到载体图像中；嵌入完毕后，则将载密图像安全传输给接收端。

2.根据权利要求1所述的基于预处理机制的图像信息隐藏方法，其特征在于，步骤1的具体过程为：

步骤1.1加载秘密信息A，并由公式$\frac{A.width \times A.height \times 3}{n}$计算出该秘密信息经过预处理后的信息量Cm；其中上式中A.width表示秘密图像A的宽度，A.height表示秘密图像A的高度，n表示压缩因子；

步骤1.2加载载体图像I，并由公式$\frac{I.width \times I.height}{8 \times 8} \times 2$计算出该载体图像I能够容纳的最大信息量Cz，上式中，I.width表示I图像的宽度，I.height表示I图像的高度；比较Cm与Cz；如果前者较大，则需要对秘密信息A进行裁剪；如果后者较大，则满足要求，继续执行下一步。

3.根据权利要求1所述的基于预处理机制的图像信息隐藏方法，其特征在于，构建八叉树索引的具体步骤如下：

步骤2.1假设三维数据集M，其中数据点表示为

$m_{ij}=(x_{ij},y_{ij},z_{ij})$，$0 \leqslant i \leqslant A.width-1$，$0 \leqslant j \leqslant A.height$

根据所有三维数据的外包络立方体建立八叉树的根节点，故外包络立方体的边长L：

$L=\max\{\max(x_{ij})-\min(x_{ij}),\max(y_{ij})-\min(y_{ij}),\max(z_{ij})-\min(z_{ij})\}$

然后沿着根节点立方体的X，Y，Z方向进行等分，将外包络立方体剖分为8个小的立方体；

步骤2.2在立方体进行剖分的过程中，将父节点中的三维数据根据其位置进行剖分，剖分到相应的叶子节点中，完成三维数据的剖分与索引的建立；

步骤2.3对于所有剖分的立方体，判断其边长b_i是否小于阈值b；若满足，则停止节点的剖分；或者判断其叶子节点立方体中所包含的数据点的个数$number_i$是否小于阈值number，若满足，则停止该节点的剖分，执行步骤2.4；若不满足，则重复步骤2.1～步骤2.2；

步骤2.4成功建立一个合理、高效的最优化八叉树索引，并将索引数据存入指针空间S中。

4.根据权利要求3所述的基于预处理机制的图像信息隐藏方法，其特征在于，数据压缩的步骤为：

步骤3.1依据上述构建的八叉树，根据已知的叶子节点(立方体)的边长L和两个空间对角角点坐标$q1_{ij}(x1_{ij},y1_{ij},z1_{ij})$，$q2_{ij}(x2_{ij},y2_{ij},z2_{ij})$，计算出立方体的中心坐标$Q_{ij}(x_{ij},y_{ij},z_{ij})=\frac{q1_{ij}+q2_{ij}}{2}$；

步骤3.2计算点Q_{ij}到该节点中包含的数据点的距离

设点集$N_{ij}=(Nn_{ij}(xn_{ij},yn_{ij},zn_{ij})$，n＝1,2,3…n)，其中点集$N_{ij}$中的数据点为已知节点所包含的所有数据点；

计算距离中心点Q_{ij}的距离$dn_{ij}=\sqrt{(x_{ij}-xn_{ij})^2+(y_{ij}-yn_{ij})^2+(z_{ij}-zn_{ij})^2}$；

步骤3.3从上述n个dn_{ij}中选取其最小值相对应的点$X_{ij}(x_{ij},y_{ij},z_{ij})$，用$X_{ij}$代替该节点中的其他数据点，删除该节点中的其他三维数据点，完成该节点的三维数据简化；以此类推，将所有的叶子节点都简化数据，获得整个八叉树的叶子节点的简化，最终获得简化数据D；

步骤3.4将简化数据D表示成像素的形式，即每个像素点由(x,y,z)组成，将数据D转化为以像素为元素的二维矩阵P。

5.根据权利要求1所述的基于预处理机制的图像信息隐藏方法，其特征在于，所述数据加密的步骤为：

步骤4.1用户输入密钥，选取加密区域；用户输入3个密钥的数值，key_x,key_y和len，均为正整数，输入的参数确定了一片正方形区域，即该正方形左上角坐标为(key_x,key_y)，边长为len；对秘密信息P根据用户输入的秘钥选取加密区域，选中区域P_user；

步骤4.2使用Arnold置乱算法对压缩后信息进行加密处理；

Arnold变换用公式表示如下：

$$\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}1&1\\1&2\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}(\mathrm{mod}\ N)$$

其中x,y的取值为{0,1,2,…,N-1}，N为数字信息矩阵的阶数；

采用公式x'＝x+y,y'＝x+2*y,然后对选中区域的宽度和高度len进行取余运算：x'＝x' mod len;y'＝y' mod len;计算出坐标(x',y')，将原来位于(x,y)处的数据放到坐标(x',y')处；重复该过程t次，加密完成，获得加密信息P'。

6.根据权利要求1所述的基于预处理机制的图像信息隐藏方法，其特征在于，信息嵌入及图像传输的步骤为：

步骤5.1将秘密信息的描述信息存储在载体图像的头部，

选取载体图像的前4个像素存储隐藏图像A的高度和宽度数值，每个像素共有3byte，并且在每个字节的末尾2bit作为存储位置，一共可以存放24bit的数据信息；其中前2个像素存储秘密图像的高度值，后2个像素存储秘密图像的宽度值；随后在选取2个像素存放用户选取加密位置的参数：key_x,key_y,len；

步骤5.2将预处理后的秘密信息P'利用隐写算法嵌入到载体图像中；

载体图像I的每个像素由RGB分量组成，即R、G、B三个通道，任选两个通道作为嵌入秘密信息的载体，利用隐写算法将秘密信息嵌入其中，获得载密图像I'，并且将I'传输给接收端。

基于预处理机制的图像信息隐藏方法

技术领域

[0001] 本发明属于图像压缩技术领域，具体涉及基于预处理机制的图像信息隐藏方法。

背景技术

[0002] 当今，信息隐藏技术是信息安全的研究热点。随着科技的进步，通信技术的迅猛发展，使得越来越多的人和组织机构通过网络传输大量的数据文件，因此造成网络上的数据压力越来越大。目前，信息隐藏领域面临的主要问题不仅仅是安全问题，还有大量数据的超负荷传输问题，如何做到既能安全传输又能提高传输效率，是当前迫切需要解决的问题。

[0003] 随着网络信息爆炸式的增长，信息隐藏领域面临着大数据带来的挑战。对于多媒体计算机面临的最大难题之一就是大量数据的传输问题。以图像为例，图像存储的分辨率越高，占据空间越大，对于信息隐藏来说，需要更大的隐藏载体，从而导致信息传输缓慢，低效等问题。因此有必要对数据压缩技术进行进一步研究。

发明内容

[0004] 本发明的目的是预处理机制中实现对于隐藏信息的处理，并达到减少信息嵌入量的目的，以及增加其安全性以及提高传输效率的目的。

[0005] 基于预处理机制的图像信息隐藏方法，包括以下步骤：

[0006] 步骤1、加载秘密信息：读取待处理图像信息，预估计出经过预处理后的信息量Cm；然后加载载体图像，计算出载体图像能够容纳的信息量Cz；比较Cm与Cz大小，如果前者大，则裁剪秘密信息，如果后者大，则继续执行下一步；

[0007] 步骤2、数据压缩：将秘密信息用三维矩阵表示，接着构建八叉树索引，并将相关索引存储到指针数组中，利用中心点提取简化算法进行简化数据；

[0008] 步骤3、数据加密：先将压缩后的三维数据矩阵转化为二维数据矩阵，然后用户选取加密区域，并使用Arnold置乱算法对用户选中区域加密，最后获取加密后的秘密信息；

[0009] 步骤4、嵌入信息以及图像传输：选取原始载体图像的前6个像素，将秘密信息的描述信息存储其中；接着采用隐写算法将秘密信息嵌入到载体图像中；嵌入完毕后，则将载密图像安全传输给接收端。

[0010] 本发明具有以下优点：

[0011] 1、在秘密信息预处理机制中，利用Arnold变换对秘密信息进行加密，从而在传输过程中增加了一层安全屏障；

[0012] 2、利用八叉树索引技术将秘密信息有损压缩，间接地提高了嵌入量；

[0013] 3、增加抗攻击能力，从而达到提高传输安全性的目的；

[0014] 4、在加密算法中添加用户选择加密方位以及区域的功能，从而提高了该算法的灵活性。

附图说明

[0015] 图1为基于预处理机制的图像信息隐藏方法一实施例的流程图；

[0016] 图2为图1实施例中构建八叉树索引的流程；

[0017] 图3为图1实施例中秘密信息压缩流程。

具体实施方式

[0018] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。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。

[0019] 为了方便叙述，简单定义算法中的主要变量：隐藏图像A，载体图像I，嵌入后生成的加密图像I'，其中用height表示图像的高度，width表示图像的宽度。I.width表示I图像的宽度，I.height表示I图像的高度。图像A亦同。

[0020] 本实施例提出的一种基于预处理机制的信息隐藏方法，主要包括加载秘密图像过程，建立八叉树索引过程，数据压缩过程，信息加密过程以及秘密信息嵌入过程等；

[0021] 具体步骤如下：

[0022] 步骤1)加载载体图像I，并估算出该载体图像I最大的隐藏信息容纳量：

[0023] 步骤1.1)由公式$\frac{I.width \times I.height}{8 \times 8} \times 2$计算出最大的容纳量Cz；

[0024] 步骤1.2)加载秘密图像A，由公式$\frac{A.width \times A.height \times 3}{n}$预估计出预处理后的秘密信息量Cm，其中n为压缩因子；

[0025] 步骤1.3)如果秘密信息量Cm没有超过Cz，则执行下一步，否则，需要用户对秘密图像进行裁剪；

[0026] 步骤1.4)将秘密图像信息根据图像编码格式RGB，将每个像素按照R,G,B分为三个分量形式(x,y,z)；并转化为三维矩阵M。

[0027] 上述步骤1.1)中的Cz的求解

[0028] 其中I.width,I.height分别为载体图像I的宽和高；

[0029] 假设嵌入信息需要使用B,R通道进行嵌入信息，每个8×8二维矩阵中嵌入1byte秘密信息；

[0030] 载体图像I中包含的8×8二维矩阵的个数为：$\frac{I.width \times I.height}{8 \times 8} \times 3$，又因为使用两个通道嵌入信息，故可嵌入信息的二维矩阵个数为：$\frac{I.width \times I.height}{8 \times 8} \times 3 \times \frac{2}{3}$；

[0031] 综上所述，载体图像中可容纳的最大信息量Cz=$\frac{I.width \times I.height}{8 \times 8} \times 2$

[0032] 上述步骤1.2)中的压缩因子n的取值的确定需要大量数据实验分析获得，故经过大量实验数据分析，一般选取n＝2；

[0033] 步骤2)建立八叉树索引过程：

[0034] 步骤2.1)根据三维数据M的外包络立方体建立八叉树根节点，其中三维数据M可表示为$m_{ij}=(x_{ij},y_{ij},z_{ij})$，0≤i≤A.width-1，0≤j≤A.height；故外包络立方体的边长L＝max

{max(xij)-min(xij),max(yij)-min(yij),max(zij)-min(zij)

[0035] 步骤2.2)沿着根节点立方体的X,Y,Z方向进行等分,将立方体剖分为8个小的立方体,故这8个小的立方体被称为根节点的8个子节点

[0036] 步骤2.3)在立方体进行剖分过程中,将父节点中的三维数据点根据位置进行剖分,剖分到相应的叶子节点中,进行归类;完成该阶段三维数据点的剖分与索引建立

[0037] 步骤2.4)在逐层剖分过程中,对于i层中的第j个结点(立方体)大小以及包含的三维数据点进行判别,如果该节点tij的大小bij小于规定的阈值b,或者该节点中包含的三维数据点的个数numberij小于number(一般情况下number为1),则停止剖析该节点,即该节点成为整个八叉树的叶子节点,则执行步骤2.5);若不满足上述两个条件,则返回步骤2.2)

[0038] 步骤2.5)成功建立一个合理、高效的最优化八叉树索引,并将索引数据存入指针空间S中;

[0039] 步骤2.1)中所述的外包络立方体的计算方法如下

[0040] 所谓外包络立方体就是要将所有的三维数据点都包含在内的最小立方体;

[0041] 设三维数据点mij=(xij,yij,zij),其中0≤i≤A.width-1,0≤j≤A.height

[0042] 故外包络立方体的边长L

[0043] L=max{max(xij)-min(xij),max(yij)-min(yij),max(zij)-min(zij)}

[0044] 立方体的八个定点如下

[0045] (min(xij),min(yij),min(zij)),(min(xij),min(yij),max(zij))

[0046] (min(xij),max(yij),min(zij)),(min(xij),max(yij),max(zij))

[0047] (max(xij),min(yij),min(zij)),(max(xij),min(yij),max(zij))

[0048] (max(xij),max(yij),min(zij)),(max(xij),max(yij),max(zij))

[0049] 步骤2.3)中所述的剖分过程

[0050] 对所有节点以及所包含的三维点集不断进行递归剖分,当规定的参数小于阈值时,停止剖分该节点,该节点便是整个八叉树的叶子节点;

[0051] 八叉树索引建立过程中,第一级有8个立方体

[0052] 第二级最多有64个立方体

[0053] ……

[0054] 第n级最多有8^n个立方体

[0055] 则第n级的立方体边长$L_n = \frac{L}{n}$,其中L为整个八叉树根节点的立方体边长

[0056] 步骤3)数据压缩过程,将三维数据M利用八叉树索引技术压缩为三维数据D

[0057] 步骤3.1)根据已知的叶子节点tij(立方体)的边长L和两个空间对角角点坐标q1ij(x1ij,y1ij,z1ij),q2ij(x2ij,y2ij,z2ij),计算出立方体的中心坐标$Q_{ij}(x_{ij},y_{ij},z_{ij}) = \frac{q1_{ij}+q2_{ij}}{2}$;

[0058] 步骤3.2)计算点Qij到其余点集Nij=(Nnij(xnij,ynij,znij),n=1,2,3…n)中所有点的距离$dn_{ij} = \sqrt{(x_{ij}-xn_{ij})^2+(y_{ij}-yn_{ij})^2+(z_{ij}-zn_{ij})^2}$,共计算出n个距离;

[0059] 步骤3.3)从上述n个dnij中选取其最小值相对应的点Xij(xij,yij,zij),然后删除该节点(立方体)中的其他三维数据点,用点Xij代替立方体内的其他点,完成该节点的三维数据简化,以此类推,将所有的叶子节点都利用此方法简化数据,并且获得了整个八叉树的叶

子节点的简化，最终获得简化数据D

[0060] 步骤3.4)将简化数据D表示成像素的形式，即每个像素点由(x,y,z)组成，将数据D转化为以像素为元素的二维矩阵P；

[0061] 步骤3)数据简化具体算法如下：

[0062] 采用中心点提取简化算法，其核心思想是，当立方体足够小时，距离中心点最近的点能够取代立方体内的点集，完成对立方体中内点集的压缩；

[0063] 设某立方体中的点集N＝(Ni(xi,yi,zi)，i＝1,2,3…n)，该立方体的中点坐标P(x,y,z)

[0064] 首先计算点集N中每个点到点P的距离

[0065] $$d_i = \sqrt{(x - x_i)^2 + (y - y_i)^2 - (z - z_i)^2}$$

[0066] 选取出d＝max(di)对应的坐标X(x’,y’,z’)，即用点X代替点集N中的所有数据点，完成数据的压缩。

[0067] 步骤4)将简化后的秘密信息，即为二维矩阵P,利用Arnold置乱算法进行加密操作

[0068] 步骤4.1)设秘密信息的二维矩阵P是m×n的矩阵，其中秘密信息的大小为P.width×P.height×3比特，将二维矩阵P进行加密，进一步增加其安全性以及抗攻击性

[0069] 步骤4.2)设计者可以根据用户需求定义置乱次数t,,其中t为整数，还原图像时需要知道t值才能正确恢复；

[0070] 步骤4.3)设置用户选择加密位置，用户选择坐标p(key_x,key_y)和len；其中需要加密的信息是以p点为起点的len×len的方阵P_user；

[0071] 步骤4.4)对秘密信息采用Arnold置乱算法

[0072] Arnold变换用公式表示如下：

[0073] $$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ N)$$

[0074] 其中x,y的取值为{0,1,2,…,N-1}，N为数字矩阵的阶数；

[0075] 将秘密信息P_user变为密文P1_user；其中待加密信息P_user，其中P_user的某一数据的坐标为(x,y)，则经过加密变换后获得新的x坐标和新的y坐标，其计算公式为：x’＝(x+y)，y’＝(x+2*y)，然后x’，y’分别对秘密信息P_user的宽度和高度进行取余运算：x’＝x’mod len;y’＝y’mod len；

[0076] 步骤4.5)求出新的坐标(x’,y’)后将原来的(x,y)坐标的数据信息转换到新的坐标(x’,y’)处；

[0077] 步骤4.6)按照t的数值大小重复执行步骤4.4)至步骤4.5)t次；

[0078] 步骤4.7)完成t次变化后对于秘密信息的加密过程结束，并获得加密矩阵P1_user。

[0079] 步骤5)将预处理后的秘密信息P1_user的相关参数嵌入到载体图像I中：

[0080] 步骤5.1)选取载体图像I中的前6个像素信息，由于图像的每个像素为3比特，分别是B通道，G通道，R通道；将该6个像素用于存储传输秘钥，该秘钥包括key_x,key_y,len；

[0081] 步骤5.2)在嵌入传输秘钥时，使用B通道和R通道，因此选取9个像素可作为秘密信

息载体的信息共计18byte。由于修改每个字节的最末2bit并不影响图像的质量，因此，每个字节的最末2bit可以用来存储数据。首先将秘密信息P的宽度P.height存入前3个像素(即前6字节)，其中每个字节可存2bit数据，因此共计12bit，最高可存$2^{12}-1=4095$像素高度，存储方式为将秘密信息P的高度P.height每2bit一组拆分，按照顺序存储在图像前6个字节中；

[0082] 步骤5.3)将秘密信息P的宽度P.width存入第4至6个像素中；嵌入方法如步骤5.2)所述；

[0083] 步骤6)将预处理后的秘密信息P1_user嵌入载体图像I中，并传输给接受者获取秘密信息

[0084] 步骤6.1)如步骤5.1)所述，载体图像中每个像素为3比特，分别为B通道，G通道，R通道；可任选一个通道进行秘密信息的嵌入

[0085] 步骤6.2)假设选取R通道嵌入秘密信息P1_user，采用隐写算法将秘密信息矩阵P1_user嵌入到载体图像中；

[0086] 步骤6.3)嵌入完成后，获得载密图像I，，然后将载密图像传送给接收者；

[0087] 步骤6.4)接收者接收到载密图像后，利用上述加密的逆过程获取秘密信息P1_use以及相关的参数信息key_x，key_y，len和秘密信息P的宽和高；将p1_user经过Arnold逆变换算法，采用t次后，获得P。

[0088] 本发明方案所公开的技术手段不仅限于上述实施方式所公开的技术手段，还包括由以上技术特征任意组合所组成的技术方案。

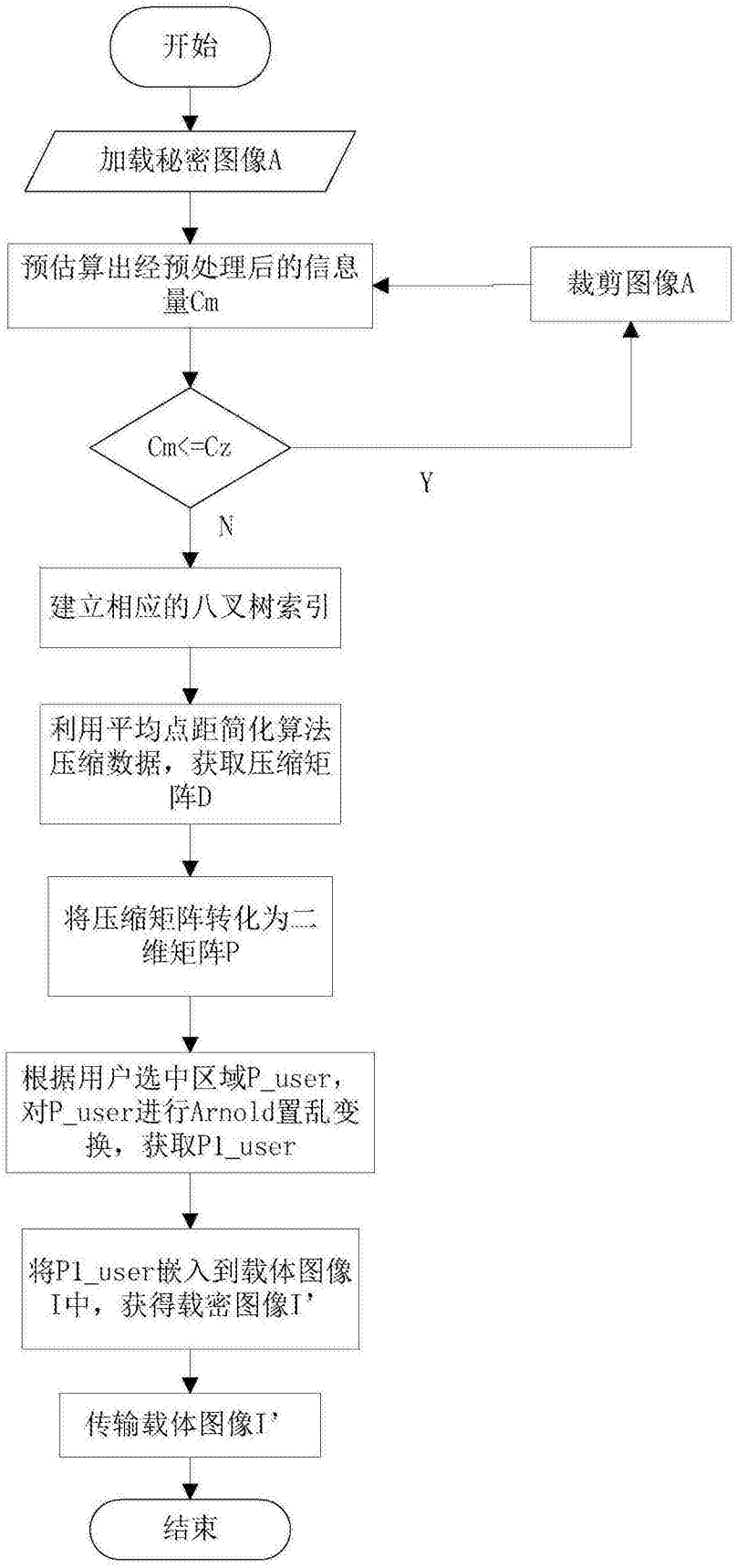

开始
加载秘密图像A
预估算出经预处理后的信息量Cm
裁剪图像A
Cm<=Cz
Y
N
建立相应的八叉树索引
利用平均点距简化算法压缩数据，获取压缩矩阵D
将压缩矩阵转化为二维矩阵P
根据用户选中区域P_user，对P_user进行Arnold置乱变换，获取P1_user
将P1_user嵌入到载体图像I中，获得载密图像I'
传输载体图像I'
结束

图1

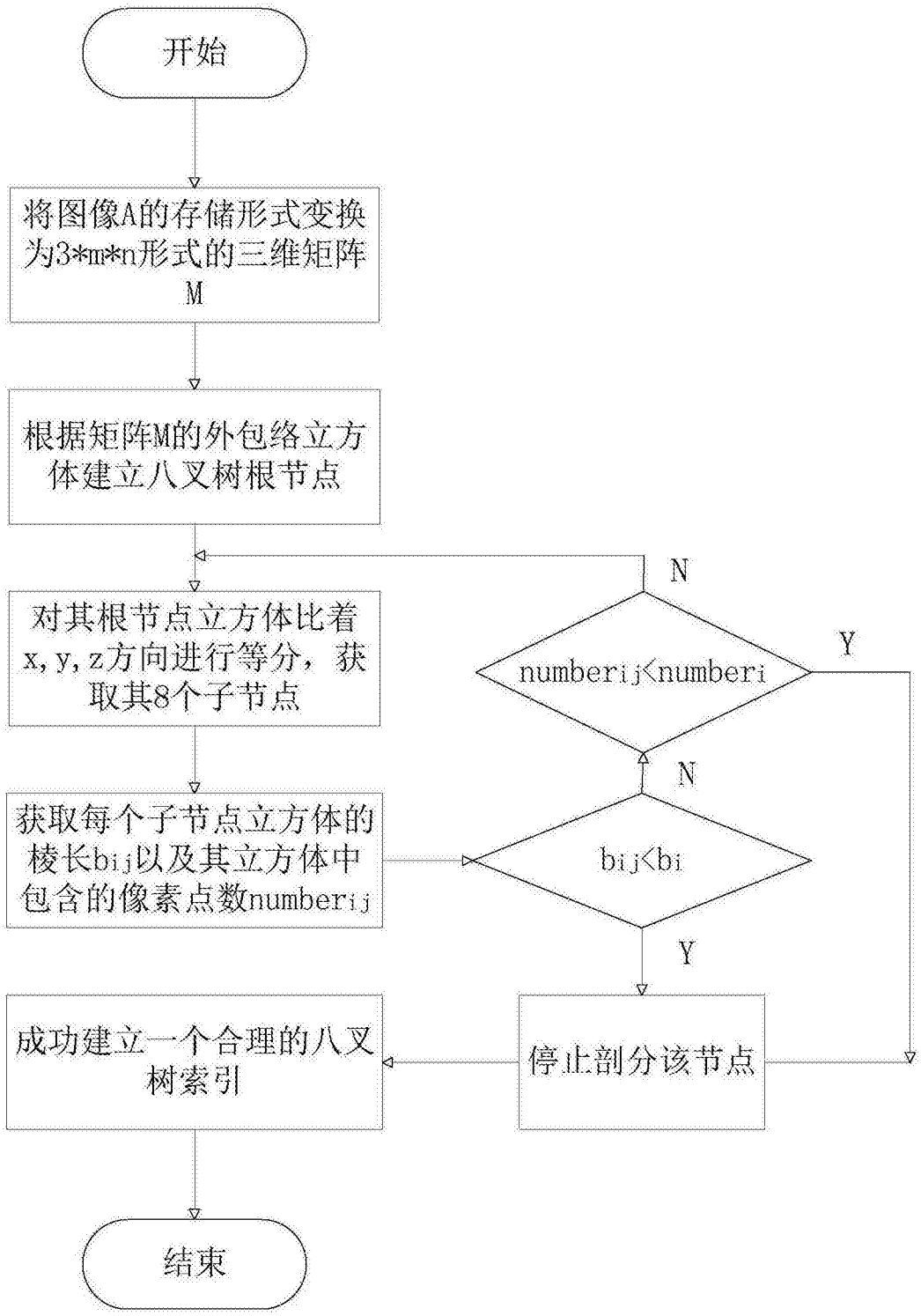

开始
将图像A的存储形式变换为3*m*n形式的三维矩阵M
根据矩阵M的外包络立方体建立八叉树根节点
对其根节点立方体比着x,y,z方向进行等分，获取其8个子节点
获取每个子节点立方体的棱长bij以及其立方体中包含的像素点数numberij
numberij<numberi
N
Y
bij<bi
N
Y
停止剖分该节点
成功建立一个合理的八叉树索引
结束

图2

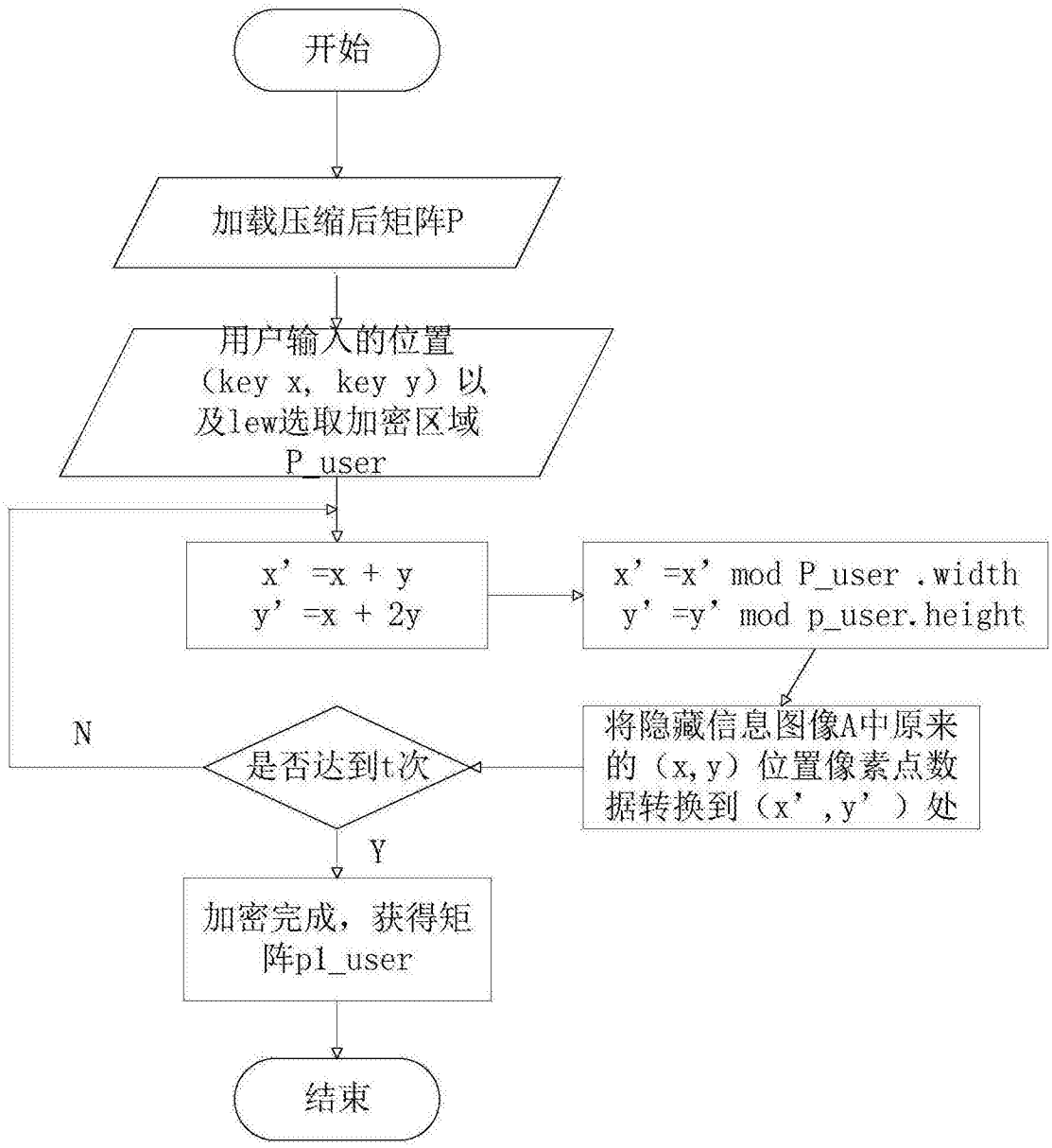

开始
加载压缩后矩阵P
用户输入的位置（key x，key y）以及lew选取加密区域P_user
x’=x + y
y’=x + 2y
x’=x’ mod P_user .width
y’=y’ mod p_user.height
将隐藏信息图像A中原来的（x,y）位置像素点数据转换到（x’,y’）处
是否达到t次
N
Y
加密完成，获得矩阵p1_user
结束

图3