一种索玛立方体方块匹配的图像置乱算法

范铁生 张忠清 张 璞
(辽宁大学信息学院 沈阳 110036)

摘 要 针对图像已有置乱算法普遍存在的不足,提出了一种新的索玛立方体方块匹配的图像置乱算法。算法先将原始图像的位平面进行交换以改变图像的像素灰度值,然后按照索玛立方体将变换的图像进行分块,选择索玛立方体的任意两种拼接方式,其中一种看作是原始图像元素的拼接方式,另一种是置乱图像的拼接方式,将两种拼接方式对应转换,从而实现图像的置乱。置乱后的图像表现为白噪声,不存在周期性恢复的安全性问题,置乱较为稳定,能很快达到理想的置乱效果,并且置乱算法对图像尺寸没有要求。实验结果表明,算法能有效地实现对灰度图像的置乱,并且有良好的视觉效果和定量评价结果,能抵抗一定的几何攻击。

关键词 图像置乱,索玛立方体,位平面交换,置乱程度
中图法分类号 TN911.73 **文献标识码** A

Image Scrambling Algorithm Based on SOMA CUBE Square Matching

FAN Tie-sheng ZHANG Zhong-qing ZHANG Pu
(Information Institute, Liaoning University, Shenyang 110036, China)

Abstract In allusion to common deficiency of existing scrambling algorithm, an image scrambling algorithm based on SOMA CUBE square matching was proposed. To scramble an image, bit-plane of the original image is firstly exchanged to change the pixel grayscale, and then this image is divided into blocks according to SOMA CUBE; finally, any two matching methods of SOMA CUBE are chosen, and one is seen as the matching way of original image elements, the other is the scrambling image, and puting the twos conversion, so as to realize the image scrambling. The scrambling image shows the white noise is not the problem of cyclical recovery safety, scrambling is relatively stable, can quickly achieve ideal scrambling effect, and there are not requirements for image size. The experimental results show that this algorithm can effectively achieve the gray image scrambling, has a good visual effect and quantitative evaluation results, and can resist certain geometrical attack.

Keywords Image scrambling, SOMA CUBE, Plane exchange, Scrambling degree

随着人们对信息安全意识的加强,数字图像的置乱技术日益成为一个重要的研究课题。置乱是图像加密预处理的一种重要技术,也常用于更复杂的隐藏与数字水印的预处理或后处理,以增加隐藏和抗攻击能力[1]。

置乱技术利用数字图像具有的数字阵列的特点,搅乱图像中像素的位置或颜色,使之变成一幅杂乱无章的图像,以达到无法辨认出原始图像的目的[5]。目前已有的数字图像置乱算法很多,例如:Arnold[3]变换、幻方变换、约瑟夫变换、原根变换以及 Hilbert[7]曲线等,这些置乱算法大多主要用于方阵图像,通用性也不好,对待置乱图像的尺寸有要求;且有些计算量较大,置乱较为费时;已有的置乱算法改变图像位置的居多,这些算法给非法攻击者可乘之机;置乱速度不理想,效率较低;另外,像 Arnold 等这种置乱算法还存在周期性,使得算法安全性降低。

针对已有置乱技术存在的不足以及现有数字图像数据量大的问题,提出了一种索玛立方体方块匹配的图像置乱算法,算法是基于位平面交换和索玛立方体匹配的方式来实现对原始图像的置乱。算法原理简单,计算量小,置乱效率较高;对图像尺寸没有要求,通用性强;算法改变图像灰度值,直方图发生变化,降低了可攻击性;置乱不存在周期性问题,密钥完成由置乱过程控制,安全性好。本文首先对索玛立方体进行简单介绍,然后详细描述了索玛立方体方块匹配置乱算法的思想以及实现过程,最后通过实验对置乱算法进行深入分析,以证明算法的有效性和合理性。

1 索玛立方体的提出

1.1 问题的由来

索玛立方体的任务是将7个立方体拼成一个新的正立方体,就像立体的七巧板。索玛立方体是物理学家皮特·海恩(Piet Hein)发明的一种游戏玩具。他在德国物理学家海森堡演讲"量子物理"时(当时海森伯格讲到把空间切割成立方体),就想到一个几何原理:4个以内同样大小的立方体"以面相接"构成所有不规则形状,可以组合成一个较大的立方体。海森伯格还没演讲完,海恩就确定了这种体积为27个单位的

到稿日期:2012-08-04 返修日期:2012-11-22 本文受辽宁大学"211工程"三期建设项目资助。
范铁生(1955—),男,教授,主要研究方向为信息隐藏技术、声纹识别、数字图像处理等,E-mail:fts0@lnu.edu.cn;张忠清(1984—),女,硕士,主要研究方向为数字图像处理、数字水印、虚拟现实;张 璞(1987—),男,硕士,主要研究方向为虚拟现实、云计算、分布式计算。

7片形状可以组成一个新的3×3×3的立方体。演讲结束后，海恩把27个小立方体块黏成这7个形状，并证实了自己的看法。

1.2 构成索玛的组件

索玛是由单位正方体组成的。如图1所示，两个正方形以面连接，只有一种形状(旋转、翻转视为相同)，但它是规则长方形，与皮特.海恩的设计原意不符，所以不采用。3个正方形以面连接，有两种形状，但左边I(I为罗马字)字形的一片是长方形，也不采用。4个单位正方形以面连接，有8种形状，其中I字形是规则形状，不采用。下图2是有阴影的7片，它们就是索玛的组件。这7片组件的总体积为27个单位，可以拼成3×3×3的新的正立方体。

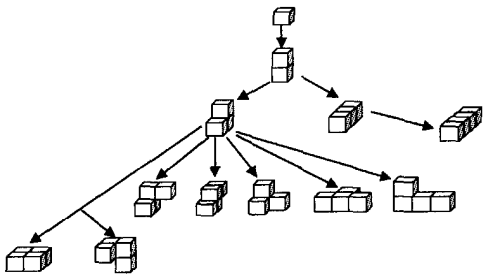


图1 单位正方体的拼接方式

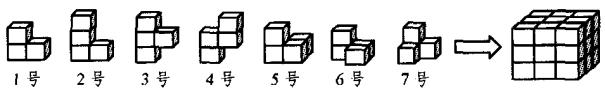


图2 索玛7片组件组成

在图2中，索玛方块1号是由3个小立方体组成，其余方块是由4个立方体组成。其中5号和6号是不相同的。

1.3 索玛立方体的解

在派克兄弟公司的索玛手册上称：John Horton Conway和M. J. T. Guy两位剑桥大学的数学家，提出索玛组成3×3×3立方体的方法有240种结构完全不同的解，并经过了计算机程序证实。这些结果不同的解在Conway和Guy合著的《Winning Way》书中第802、803页可找到图谱。但这个结果是在将5号和6号这样的镜像看作相同的情况下得出的结论；如果镜像视为不相同，则有480种结构不同的解[9]。

2 索玛立方体方块匹配的图像置乱算法

基于以上对索玛立方体的分析可以看到：索玛立方体由27个大小相同的块组成，这27块又是按照7个不同且有规则的索玛组件拼接而成，而且它是三维模型。我们所研究的灰度图像是二维的，如果将索玛立方体应用到二维图像上，需要做一些降维和升维操作，以将二维图像和索玛立方体联系起来。

显然，用索玛立方体置乱二维图像需将其转换成索玛立方体的7片组件形式。因此，索玛立方体方块匹配置乱算法的主要实现过程为：首先将原始图像的8个位平面按照某种方式进行交换，改变图像的像素灰度值；然后按照索玛方块的组成分成大小相同的27块，不足一块的不做处理(也可做适当的处理，由用户定义)；将原始图像转成四维(因为是将原始图像分成对应索玛立方体的27块，但原始图像是由一个一个元素组成，被分成的27块中的每一块(block)由若干元素组成，而索玛立方体的每一块被看作一个整体，所以这里原始图像的四维形式是3×3×3×block，其第三维对应索玛立方体的第三维；将原始图像应用索玛立方体进行变换的时候，原始图像与索玛立方体的第三维对应变换，第四维看作一个整体)。27块中每一块的所有元素处于第四维；将索玛立方体中的7个组件中的每一组件看作是图像中的一块(大小为block)，将索玛立方体看作3维数组，其27块中的每块看作3维数组中的一个元素，此元素对应原始图像四维数组中第三维中的一个元素，那么此数组含有27个元素；将索玛立方体看成3层，分别是三维数组中其中一维的元素，例如索玛立方体从上到下3层分别看作三维数组的第一维、第二维、第三维的元素；然后选择索玛立方体拼接方式中的任意两种(如图4所示)作为匹配对象，其中一种看作是原始图像元素的拼接方式，另外一种看作是置乱后图像的拼接方式，这样将原始图像的拼接方式转换成置乱后图像的拼接方式；转换时按照索玛立方体中7个索玛组件的对应位置进行匹配转换(7个组件都有标号)，转换后就得到了置乱后的图像。

置乱算法包括正置乱和解置乱两个部分，其中逆置乱为正置乱的逆过程。正置乱过程的输入为：原始图像image、第一个密钥cycle(置乱次数)、第二个密钥(用户所选择的位平面交换方式)、第三个密钥(置乱前后图像的两种拼接方式，如图4所示)；输出为置乱后的图像fg。逆置乱过程的输入为：置乱图像fg、第一个密钥cycle(置乱次数)、第二个密钥(用户所选择的位平面交换方式)、第三个密钥(置乱前后图像的两种拼接方式)；输出为置乱恢复图像gf。

正置乱过程具体步骤如下：

1)得到原始图像image大小$M\times N$，将原始图像的位平面进行交换，交换方式由用户选择，例如：位平面1和8交换，2和7交换，3和6交换，4和5交换。

2)将变换后的图像分成27块，每块大小为*block*。

3)一次迭代开始：得到此次迭代时图像的大小(因为每次迭代后有转置操作)为$m\times n$；将此时二维图像转换成一维大小，记为image1；定义一个大小为$3\times3\times3\times block$的四维数组fig，将每一块顺次填充到第四维中；选取两种索玛立方体拼接方式，进行对应位置块的变换；变换完的数组记为out，其仍为四维数组；将out转换成$27\times block$大小，进行转置为OUT，再转成一维大小记为FIG；将image1中不足一块的剩余元素原封不动地填充到FIG的尾部；将FIG转换成$m\times n$大小，进行转置一次得到fg；将fg赋值给image。

4)迭代是否完成，如果未完成转到步骤3)；否则转到步骤5)。

5)将得到的fg进行一次转置，即为置乱后的图像。

解置乱过程具体步骤如下：

1)得到置乱后图像fg的大小为$M\times N$，将图像分成27块，每块大小为*block*。

2)将图像进行一次转置为image；

3)一次迭代开始：将image进行转置，并得到转置后图像的大小为$m\times n$；将此时的二维图像转换成一维大小，并将其记为image1；定义一个大小为$3\times3\times3\times block$的四维数组fig，方法同正置乱过程，将每块元素填充到第四维中；选择同正置乱过程一样的两种拼接方式，进行对应位置块的逆变换；然后定义一个一维数组OUT，大小为$M\times N$，将变换后四维数组中的第四维元素顺次填充到OUT中，并将不足一块的

元素原封不动地填充到 OUT 的尾部；将一维数组 OUT 转换成 $m\times n$ 大小的二维数组，记为 GF，并将此次得到的图像 GF 赋值给 fg。

4)迭代是否完成，如果未完成转到步骤 3)，否则转到步骤 5)。

5)按照正置乱过程所选择的位平面交换方式对 GF 的位平面进行交换，交换后的图像存储到 gf 里。至此，逆置乱完成，即得到置乱恢复后的图像 gf。

3 实验结果与分析

3.1 置乱效果分析

实验选用尺寸为方阵且大小为 512×512 像素的标准 lena 图和尺寸为矩形阵且大小分别为 357×512 像素和 512×357 像素的 lena 图；第一个置乱密钥为置乱次数 $cycle=39$，第二个置乱密钥位平面交换方式是：位平面 1 和 8 交换、2 和 7 交换、3 和 6 交换、4 和 5 交换，图 3 的两种索玛立方体拼接方式为第三个置乱密钥。

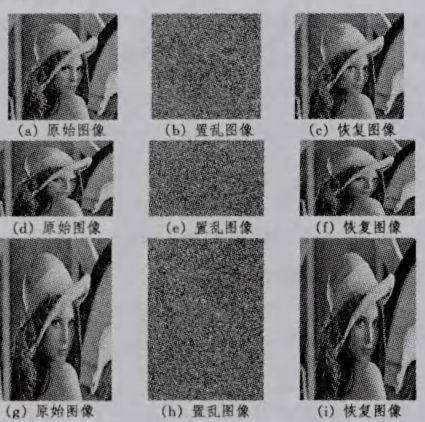
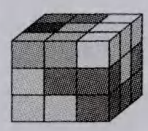


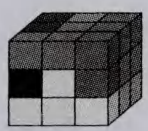
图 3 本文算法置乱 lena 效果图

如图 3 所示，(a)为大小为 512×512 像素的原始 lena 图，(b)为(a)经正置乱过程得到的置乱图像，(c)为(b)经逆置乱过程得到的恢复图像；(d)为大小为 357×512 像素的原始 lena 图，(e)为(d)经正置乱过程得到的置乱图像，(f)为(e)经逆置乱过程得到的恢复图像；(g)为大小为 512×357 像素的原始 lena 图，(h)为(g)经正置乱过程得到的置乱图像，(i)为(h)经逆置乱过程得到的恢复图像。从(b)(e)(h)中可以看到图像置乱视觉效果良好，置乱后的图像和白噪声一样；从(c)(f)(i)中可以看到恢复的图像与原始图像相比没有任何损失。

另外，图 4 为实验选用的索玛立方体的两种拼接方式，图 4 中左边为立方体，右边为该立方体的拼接方式对应的列表，列表中的数字为对应的组件标号。立方体被标记为彩色，其中，粉色为 1 号组件，红色为 2 号，黄色为 3 号，深蓝色为 4 号，绿色为 5 号，灰色为 6 号，天蓝色为 7 号。



第一层（第一维）			第二层（第二维）			第三层（第三维）		
2	2	3	4	2	5	4	2	5
4	6	3	4	6	3	7	5	5
6	6	3	7	1	1	7	7	1



第一层（第一维）			第二层（第二维）			第三层（第三维）		
4	5	2	7	5	5	7	7	6
4	1	2	4	6	5	7	6	6
1	1	2	4	3	2	3	3	3

图 4 索玛立方体的两种拼接方式

3.2 置乱速度对比分析

实验选用了 Arnold 置乱和 Hilbert 置乱算法与本文算法进行置乱速度对比测试。其中，表 1 是在相同置乱次数为 5 的基础上，用不同置乱方法对不同尺寸的图像进行置乱的速度对比；表 2 是在相同图像尺寸为 512×512 的基础上，用不同置乱方法在不同的置乱次数下进行置乱的速度对比。

表 1 不同图像尺寸置乱速度测试对比

图像尺寸	200×200	512×512	1024×1024	2048×2048	3072×3072	4096×4096
本文算法	0.249764	0.434109	1.485057	5.632230	12.348660	21.856046
Arnold 置乱	0.622037	1.237593	5.336644	33.089968	103.500562	231.545700
Hilbert 置乱	3.880800	73.483547	946.614447	3501.4355	——	——

表 2 不同置乱次数置乱速度测试对比

置乱次数	5	10	50	100	300	500
本文算法	0.434109	0.552257	1.447517	2.832444	7.450805	12.888850
Arnold 置乱	1.286481	1.521154	3.911103	7.057096	18.421341	30.092641
Hilbert 置乱	73.483547	133.423108	1247.284319	4935.2756	——	——

从表 1 以及实验分析得知：在置乱次数为 5 的基础上，用不同置乱方法对不同尺寸的图像进行置乱速度对比时，本文算法的置乱速度与其它算法相比较快，而且随着图像尺寸的增大，这种差别越来越明显。

从表 2 以及实验分析得知：在图像尺寸为 512×512 的基础上，用不同置乱方法在不同的置乱次数下进行置乱速度对比时，本文算法的置乱速度与其它算法相比较快，而且随着置乱次数的增大，这种差别越来越明显；在置乱次数为 500 时，本文算法置乱图像所用时间都没有超过 15s。

总之，表 1 和表 2 都表明本文算法在置乱速度方面性能较优。

3.3 置乱效果评价

我们用文献[8]的置乱程度评价方法来衡量本文算法的置乱程度，选用 512×512 像素的 lena 图，实验结果如图 5 所示，横坐标为置乱次数，纵坐标为置乱程度。

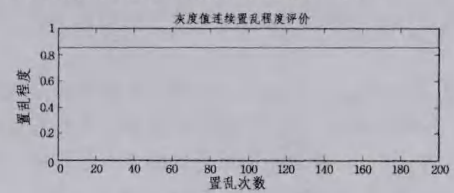


图 5 置乱程度评价曲线图

从评价曲线图 5 中可以看出，用索玛立方体方块匹配的置乱算法置乱 lena 图像 200 次，评价曲线基本是平稳的，没有大的起伏，这说明该算法置乱比较稳定，且无周期性，不存

(下转第 314 页)

建的毕竟是“二维半”模型，如何构建平面图案的真正 3D 模型数据，有待进一步研究。

参 考 文 献

[1] McGlone J C, Mikhail E M, Bethel J S, et al. Manual of photogrammetry (Fifth Edition) [M]. American Society for Photogrammetry and Remote Sensing, 2004

[2] Zhang Z. A flexible new technique for camera calibration [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2000, 22(11): 1330-1334

[3] Pasko A, Savchenko V, Sourin A. Synthetic carving using implicit surface primitive [J]. Computer-Aided Design, 2001, 33(5): 379-388

[4] Levet F, Granier X. Improved skeleton extraction and surface generation for sketch-based Modeling [C] // Proceedings of Graphics Interface 2007, ACM International Conference Proceeding Series. Montreal: ACM Press, 2007: 27-33

[5] Eggli L, Hsu C, Bruderlin B D, et al. Inferring 3D models from freehand sketches and constraints [J]. Computer-Aided Design, 1997, 29(2): 101-112

[6] 陈宇拓，张潇云，韩旭里，等. 平面闭合图形的光滑雕刻型面建模 [J]. 计算机辅助设计与图形学报，2009，21(4)：511-517

[7] Chen Yu-tuo, Han Xu-li, Okada M. Integrative 3D Modeling of Complex Carving Surface [J]. Computer-Aided Design, 2008, 40(1): 123-132

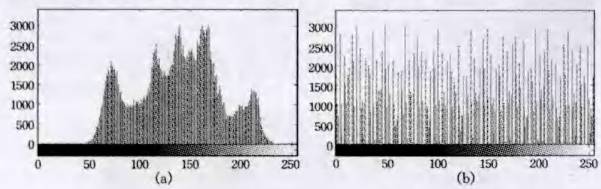
[8] 陈宇拓，韩旭里，余英林. 基于 RGB 色彩空间的彩色图像混合编码 [J]. 计算机科学，2008，35(1)：240-245

(上接第 310 页)

在周期性恢复的安全性问题；评价曲线置乱的前几次和后面也基本相同，且第一次置乱和后面也相同，说明经该算法对图像置乱能快速达到理想的置乱效果，置乱效率较高，而且经一次置乱变换就可以得到置乱图像。

3.4 直方图特征分析

在图 6 中，(a)为尺寸为 512×512 的 lena 图像的直方图；(b)为经 39 次置乱得到的置乱图像的直方图。



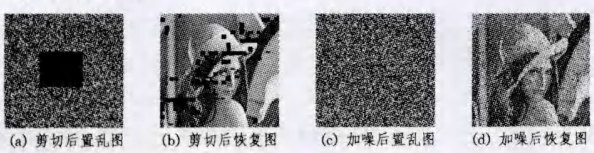
(a) 尺寸为 512×512 的 lena 图像的直方图　(b) 经 39 次置乱得到的置乱图像的直方图

图 6　本文算法置乱前后直方图

从图 6(b)中可以很明显地看到，置乱后图像的直方图发生了变化，而且灰度值呈均匀分布的形式，说明经本文算法置乱后的图像表现为白噪声，提高了非法攻击者根据置乱后图像的统计特征进行攻击的难度，从而提高了算法的安全性。

3.5 抗攻击实验

置乱图像经过剪切、加噪等常规处理后，仍具有良好的可恢复性，这个过程就是置乱图像的抗攻击测试。实验选用 512×512 的 lena 图，在图 7 中，(a)为剪切掉部分后的置乱图像，其中剪切部分为图像的(175:330, 155:335)像素；(b)为剪切后恢复的图像；(c)为加入椒盐噪声后的置乱图像，噪声密度为 0.1；(d)为加噪后恢复的图像。以上实验结果表明：对经本文算法置乱的图像进行一定的攻击处理，不会影响恢复图像的可知性。



(a) 剪切后置乱图　(b) 剪切后恢复图　(c) 加噪后置乱图　(d) 加噪后恢复图

图 7　攻击效果图

结束语　本文提出的索玛立方体方块匹配的图像置乱算法，实现简单，效率高，使用索玛立方体的拼接方式和置乱的迭代次数作为置乱密钥，置乱过程完全依赖于用户所选择的置乱密钥，安全性好；且置乱图像表现为白噪声，降低了非法攻击的可能性；算法有较优的置乱速度，易于处理大信息容量的灰度图像；而且理论分析和实验结果进一步证明，索玛立方体方块匹配的置乱算法可以很快达到较好的定量评价结果，对于研究者在信息隐藏方面寻找更好的置乱变换有较好的指导意义。

参 考 文 献

[1] 曹光辉，胡凯. 基于混沌序列加权抽样和排序变换的图像置乱 [J]. 北京航空航天大学学报，2011，39(1)：67-72

[2] 胡春强，邓绍江，秦明甫，等. 基于 Logistic 与标准映射的数字图像加密算法 [J]. 计算机科学，2010，37(12)：57-59

[3] 梁婷，李敏，何玉杰，等. Arnold 变换在图像置乱中的应用研究 [J]. 贵州大学学报：自然科学版，2011，28(6)：79-81

[4] 王泽辉. 二维随机矩阵置乱变换的周期及在图像信息隐藏中的应用 [J]. 计算机学报，2006，29(12)：2218-2224

[5] 张博. 基于 Matlab 的数字图像置乱方法研究 [J]. 计算机与数字工程，2010，38(7)：139-142

[6] Yin D H, Li B F. Using improved Fibonacci hash transform to increase the robustness of meaningful watermarking algorithm [J]. Journal of Wuhan University of Science and Technology: Natural Science Edition, 2005, 26(7): 1241-1245

[7] 王笋，徐小双. Hilbert 曲线扫描矩阵的生成算法及其 MATLAB 程序代码 [J]. 中国图像图形学报，2006，11(1)：119-122

[8] 黄健，柏森. 一种有效的图像置乱程度衡量方法 [J]. 计算机工程与应用，2009，45(30)：200-203

[9] Anderberg K. eHow Contributor. How to Create Cube Puzzles & Crosswords [OL]. http://www.ehow.com/how_7346544_create-cube-puzzles-crosswords.html, 2012-07

[10] Hong C Y, Zou W G. Digital image scrambling technology based on three dimensional Arnold transformation and its periodicity [J]. Journal of Nanchang University: Natural Science, 2005, 29(6): 619-621