基于改进BCD码及DCT变换的图像置乱算法研究

An Image Scrambling Algorithm Based on Modified BCD and DCT Transform

张 波[1] 崔基哲[1] JongWeon Kim[2]

1. 133002 延边大学经济管理学院 信息管理与信息系统 吉林 延吉 2. 110743 韩国祥明大学 著作权保护专业 首尔

Zhang Bo[1], Cui Jizhe[1], Jong Weon KIM[2]

1 College of Economic and Management, Yanbian University, Jilin Yanji 133002, China;

2 Dept. of Copyright Protection, Sangmyung University, Seoul 110743, Korea

摘 要：本文提出了一种新的频域空间图像置乱算法，频域空间转换采用了离散余弦变换（DCT），图像的置乱过程则使用基于种子的伪随机矩阵法。为了在有限的可置换范围内提高置乱效果，论文中提出一种改进BCD(Modified Binary Coded Decimal, MBCD)码，提高了还原后的图像质量，并有效抑制住了离散余弦变换中时常发生的块效应。新提出的图像置乱算法具有明显的特点，置乱后取值范围高度集中在特定范围之内，这种特点在需要设置前提条件的置乱算法应用中具有推广性。

关键词：离散余弦变换 改进BCD码 图像置乱 加密算法

Abstract: This paper promote a new image scrambling algorithm about frequency domain, the frequency domain transform by DCT, while the image scrambling process based on the pseudo-random matrix method of seed. In order to improve the effect of scrambling within limited replaceable space, an improved BCD code is put forward to increase the restored image quality and block the Blocking Artifact in DCT process. This new algorithm has obvious characteristic, that is, the range highly concentrated within a specific range after scrambling. this characteristic has promotional value in the scrambling algorithm which need to set up the premise.

Keywords: Image encryption; Modified BCD; Image Scrambling; Discrete Cosine Transform

1 引言

图像置乱采用密码学的基本思想和一些新的手段，将需要保护的图像直接进行置乱或分存等处理，使其在视觉效果上不包含任何有意义的内容来达到加密目的。目前常见置乱方法主要有Arnold变换、IFS模型、Conway游戏和Gray码等，置乱之后的图像素取值范围基本都分布在整个空间，大部分都呈现随机性。本文运用改进BCD码及DCT变换来实现图像置乱，置乱结果图的像素值取值范围与传统置乱算法有明显的区别，色阶分布呈现窄带域，直方图也具有相同的特点。这种置乱效果在航空图像及医学图像的安全传输和保密保存中具有可推广性。经测试发现，这种窄带分布没有影响图像置乱效果，成功抑制了频域算法中存在的块效应。

2 DCT变换及MBCD码

2.1 DCT变换的性质

DCT变换是线性正交变换，二维DCT变换有可分离性等特点。基于这种特点，DCT在需要对大量数据实时处理的图像处理中具有非常重要的地位。

二维DCT变换公式如下：

$$C(u,v)=a(u)a(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\cos[\frac{(2x+1)u\pi}{2M}]\cos[\frac{(2y+1)v\pi}{2N}]$$

其中，$u=0, 1, \cdots, M-1$；$y=0, 1, \cdots, N-1$

二维DCT反变换公式如下：

$$f(x,y)=\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}a(u)a(v)C(u,v)\cos[\frac{(2x+1)u\pi}{2M}]\cos[\frac{(2y+1)v\pi}{2N}]$$

其中，$x=0, 1, \cdots, M-1$；$y=0, 1, \cdots, N-1$

2.2 改进BCD码

BCD码可分为有权码和无权码。有权BCD码有8421码、2421码、5421码；无权BCD码有余3码、格雷码等。本文针对有权BCD码中的8421码进行改进，分别用不同的两个8421有权码来表示像素值，用来替换原来的十进制数的一种方法。此种替换方法具有使用灵活，携带信息量增多等优点。

BCD码的改进方式如下：

改进1：BCD码用4位二进制数表示十进制10组代码，余下的六组代码不用。本文中六组代码也要用，改为表示16组十进制代码，与四位自然二进制码相同。

改进2：两组改进BCD码(8421)来表示8位像素值。

用函数φ表示权重分别为(1；64，32，16，8，4，2，1)的函数，其中1表示大小、(64，32，16，8，4，2，1)表示绝对值，用函数f表示上述两种权重映射。则，计算公式如下

$$y=\varphi(U,V)$$

$$U=f(u),V=f(v),$$

其中 $\forall u,v\in MBCD$ 且 $u\in\{0,1\},0\le v\le 127,\ 0\le y\le 255$

函数存在逆函数，公式如下：

$$(U,V)=\varphi^{-1}(y)$$

$$u=f^{-1}(U),v=f^{-1}(V),$$

在本论文中使用方式如下：

Step1:若频域要处理的值(α)小于零，则u处记为0，并取绝对

值；若大于等于0，u处记为1

Step2: 对频域数据保留到小数点后两位，记为β

Step3: 用函数f，把β转换为MBCD码(v)

Step4: 用函数φ对(u，v)进制转换，结果记为y。

y为我们所求，包含了α小数点后两位值与符号。

三、图像置乱算法的置乱及还原

图像置乱处理过程如图1所示，置乱过程如下：

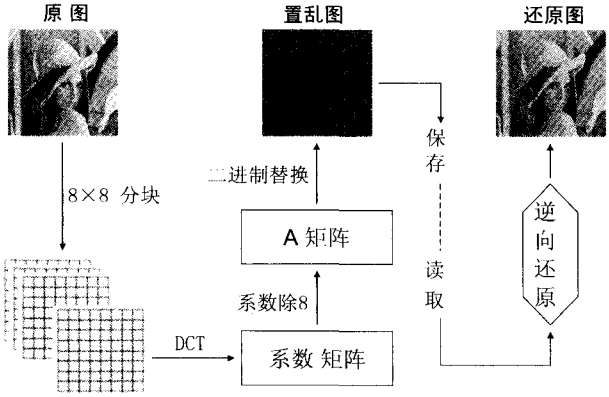


图1 图像置乱处理过程图

Step1: 原图以8x8为单位分块

Step2: 每一个单元块进行DCT变化，使空间域数据转换为频域数据

Step3: 对频域数据除以8并四舍五入，保留到小数点后两位

Step4: 如图2(右)，把一区中六个系数，分别按MBCD“MBCD二进制替换法”替换后映射到二区Ⅰ～Ⅵ处。一区中1～6号处只保留原系数的整数部分

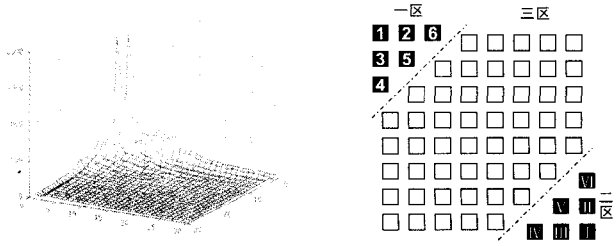


图2 DCT频域分布(左) 分区编号图(右)

Step5: 把三区中的所有负值都取绝对值，使其变成正值，然后再加上100。正值不作处理

Step6: 对所有的值再一次四舍五入

Step7: 重新合并各单元块保存为“置乱图像”

还原过程是置乱过程逆处理。包括置乱图像的8x8分块过程、Ⅰ～Ⅵ处的整数分别参照MBCD替换法逆向还原以及原系数的正负处理过程、所得数值赋给一区过程、对每一个单元块进行IDCT变换并得出“还原图”的过程。

伪随机矩阵处理

本文提出的算法结果图的像素值取值范围与传统置乱算法有明显的区别，色阶分布呈现窄带域。根据置乱算法的需要，还可以通过伪随机处理方法，可以把色阶扩散到整个空间。

实际应用本文的置乱方法时，出于色阶扩散及信息安全考虑，可以在置乱图像过程中，选择性采用伪随机矩阵的加密方法对置乱图像进行加密。就算破解者知道了本文的图像还原方法，也无法正确的还原出原图像[图3]。

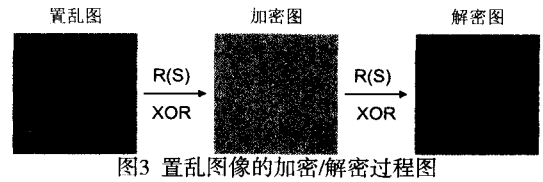


图3 置乱图像的加密/解密过程图

Step1: 生成一个基于SEED的伪随机序列矩阵，记为R=Random(Seed，[m， n])，R的取值范围限定为0～255. 参数[m，n]定义矩阵R的实际大小。

Step2: 矩阵R分别和置乱图矩阵做XOR运算，得到加密图。

Step3: 加密图再与伪随机矩阵R做XOR运算得出解密图。

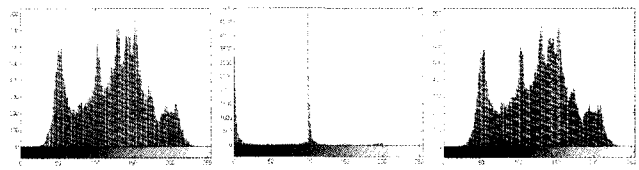
此时得出的解密图与置乱图是完全相同的两个图像。由于伪随机矩阵R可以人为控制，所以就实现了整个图像置乱的人为控制。

4 置乱算法效果测试

运用本文的置乱算法，测试结果如下图：

原始图(左) 置乱图(中) 还原图(右)

上面三个图像的直方图依次如下：



原始图(左) 置乱图(中) 还原图(右)

从直方图很容易观察出，原始图与还原图间的差别。低频轮廓相似度很高，高频细节部分则会产生一些误差(测试基于MATLAB 2010b)

附：常用图像的PSNR测试结果

常见图像的还原结果

尺寸	PSNR				
	 lena	 baboon	 airplane	 pepper	 goldhill
256×256	30.5700	24.8749	30.1680	31.6281	29.6195
512×512	32.1448	28.5168	31.8105	33.0776	31.3739

5 结论

本文提出了一种新的频域空间图像置乱算法，频域空间转换采用了离散余弦变换，为了在有限的可置换范围内提高置乱效果，论文中提出一种改进BCD码提高了还原后的图像质量，并有效抑制住了离散余弦变换中时常发生的块效应。新提出的图像置乱算法具有明显的特点，置乱后取值范围高度集中在特定范围之内，这种特点在需要设置前提条件的置乱算法应用中，具有实质

浅谈“严慈相济”的几点做法

王淑秀

山东省诸城市府前街小学

作为一名普普通通的小学教师，我觉得首先要爱孩子们，包容孩子们的童心，时刻用一颗童心和孩子们相处。当然，教师对学生的爱，要与“严”紧密结合在一起。我们不是神，只是一个普通的人，或许在工作中也有这样那样的失误，但要学会努力去爱这些“小不点”们。多年的教学经验让我对有效课堂教学有了如下的定位思考和独特的见解：

要严得合理，严得适当，不迁就学生，不放任学生，也不溺爱学生。也就是说，教师对学生提出的要求，要符合党的教育方针政策、学生的实际和21世纪对一代新人的需要；要有利于学生身心健康发展、学习进步和良好行为习惯的培养；是学生经过努力能达到、能接受，并能自觉切实执行的。

一、要严而有理

所谓严而有理，是指教师对学生提出的一切要求都要符合党的教育方针，都要有利于学生的生理心理健康，有利于学生学业的进步和良好行为习惯的养成。学生是方方面面都正在成长的“未熟人”，在校期间难免出现这样那样的缺点和错误：有的学生粗野，无礼，不尊重教师，不听劝告；有的学生在同学中大声吵闹，惹是生非。对这样的学生，有的教师能耐住性子，稳住情绪，用智慧和道理说服学生；而有的教师则火气一下子上来，就会对学生进行体罚。这种情况和行为表面上看是为了严格要求学生，实际上却有害于学生的身心健康。我们要坚决杜绝这种做法，否则便是违背教师道德的。爱因斯坦曾经指出：“如果学校把自己的工作建立在恐吓和人为制造的权威上，那是最糟糕不过的了，这样的反常制度会扼杀学生的健康情感和直率性格，挫伤学生的自信心。”对学生的真爱要体现为既对学生有种种严格、严厉的要求，又不损害学生的生理心理，让学生心服口服，心甘情愿地接受。

二、要严而有度

这一点是指教师爱学生，对学生提出的各种要求都符合他们的身份、年龄和特点，如果离实际情况太远，要求过高，学生无法达到，这种严格也就毫无意义。虽然年龄差不多，又同在一个教室，但由于多种因素所致，学生的思想水平、认识水平、知识水平以及理解能力都不会完全相同。因此，我认为严格要求必须防止“一刀切”。有的要求，对于多数学生来说可能是适度的，但对于“问题学生”来说可能是他们努力也难以达到的，而对于好的和优秀的学生来说又显得偏低。所以，针对这样的问题，教师要区分对待，适度地要求学生，这样才会收到好的教育效果。

三、要严而有方

伊索有一则寓言：太阳和风争论谁比谁强壮。风说：“当然是我，你看下面那位穿外套的老人，我可以比你更快地让他把外套脱下来。”说着，风便用力对老人吹，希望把老人的外套吹下来。但是它越吹，老人把外套裹得越紧。风吹累了，太阳从云后走出来，暖洋洋地照在老人身上。没多久，老人开始擦汗，并且脱下了外套。于是，太阳对风说：“温和与友善永远强过激烈狂暴。”所以说，教师对学生的严格要求能否收到显著成效，关键在于方法。要求学生这样做那样做，却不管学生心理感受如何，“我讲你听，我打你通”，居高临下，盛气凌人，学生即使表面上在听，在顺从，内心也不会服气，与教师的心理距离会越来越大，甚至会对教师产生反感。教师对学生的严格要求也要采取耐心、疏导的方法，要寓教于教学之中，寓教于各种活动和师生的接触之中。只有方法得当，严格才能在教育中奏效，才能培养和训练出出色的学生。

四、要严而有恒

所谓恒，就是要坚持长久。对学生的严要求绝不能时有时无，要保持一定的时效性和稳定性。既然已对学生提出某种较高标准的要求，就要要求到底，任何时候都不能放松。要常督促，常检查，把要求落到实处，直至学生养成良好的生活习惯和学习作风。教师最忌对学生一时紧一时松，说了就不再检查，再无动静，以后再怎样要求，学生都不会重视，教师的威望也会因此受损，教育效果也会大打折扣。

五、要严中求细

瑞士著名教育家斐斯泰洛奇曾说：“每一种好的教育都要求用母亲般的眼睛时时刻刻准确无误地从孩子眼、嘴、额的动作中，来了解他们内心情绪的每一种变化。”“细”就是不放过所能了解和察觉到的任何问题。在纷繁的工作中，教师要尽力抽出时间多听，多问，多看，多想，从生活、学习、思想、劳动、工作、活动以及家庭等多个方面了解学生，关心学生，善于从细节处发现潜在问题，及时引导和规范，防患于未然，避免酿成大错。“细”，本身就是爱。

一位教师要想把学生培养成社会需要的有用人才，就要对他们倾注无私的爱和真挚的情。这种爱和情就是关心、体贴、帮助加严格要求，这种情和爱既深刻又博大。慈母对孩子之所以无私，是因为有血缘关系。教师对学生付以无私的爱和真挚的情，付以慈母般的柔情，那就是一种更崇高而伟大的爱，它强烈地感化着青少年一代，使他们感悟人生，走向人生。

性应用。本文提出的新方法具有快捷简便、克服图像的保存和读取限制等特点。图像PSNR测试结果符合要求。

参考文献：

[1]崔基哲、张波，Jongweon KIM.一种图像置乱算法及在数字电视中的应用研究[J].数字电视，2011年 第20期

[2]李永逵，冯乔生、周粉、李强. 二维Arnold变换及非等长图像置乱变换[J].计算机工程与设计，2009. 30（13），P3133-3135

[3]张向华，基于混沌映射网络的数字图像加密算法[J].计算机工程，2010.03，第36卷 第六期，P175-177

[4]吴友情、吕皖丽、罗斌.空域彩色图像的二级置乱算法[J].计算机工程与设计，2009，30（13），P637-639

[5]谭永杰、马苗.位平面与Gray码相结合的图像置乱方法[J].计算机工程与应用，2010，46（16），P174-177.

基金项目：2009年度MCST&韩国著作权委员会技术开发项目结果