图像 Contourlet 域快速置乱算法

顾国生,战荫伟,侯文邦
GU Guo-sheng,ZHAN Yin-wei,HOU Wen-bang

广东工业大学 计算机学院,广州 510006
Faculty of Computer,Guangdong University of Technology,Guangzhou 510006,China
E-mail:guguosheng@gmail.com

GU Guo-sheng,ZHAN Yin-wei,HOU Wen-bang.Fast image scrambling algorithm based on Contourlet transform.Computer Engineering and Applications,2010,46(4):15-17.

Abstract: This paper presents an image scrambling algorithm based on Contourlet transform.In order to eliminate the negative effect of the entropy coding,it analyzes the structure and characteristic of Contourlet coefficients and proposes a fast image permutation method based on sub-tree.Efficient chaotic maps are used to produce permutation matrices.The cipher image satisfies requests for content masking.The simulation also implies it has good statistic characters.

Key words: Contourlet;permutation;chaotic map

摘 要:探讨了 Contourlet 变换域的图像视觉信息的置乱掩蔽问题,提出了一种基于零树编码结构的快速置乱算法。算法使用高效混沌映射构造置乱矩阵,对 Contourlet 系数矩阵进行子树间置乱,以减少系数置乱所带来的对编码效率的影响。实验结果表明该置乱算法效率高,并能有效实现对图像视觉内容的掩蔽。

关键词: Contourlet;置乱;混沌映射
DOI:10.3778/j.issn.1002-8331.2010.04.005 **文章编号:**1002-8331(2010)04-0015-03 **文献标识码:**A **中图分类号:**TP309

1 引言

在计算机技术和网络技术的快速发展中,数字图像作为一种直观的表达和存储信息的载体,已经成为信息技术一个不可或缺的组成部分。针对数字图像信息的安全保密技术,也在高速发展之中。近十年来,围绕小波域的图像安全保密技术涌现了大量的工作,这得益于小波变换强有力的时频多分辨分析能力。然而,小波变换在图像信号分析中并非是完美无缺的,用于图像分解的可分离二维小波变换基函数只具有有限的方向性(水平、垂直、对角三个方向),不能完整表达图像中边缘、轮廓和纹理等高维奇异性信息。2002 年,Do 和 Vetterli 提出了 Contourlet 变换[1]。这种新的多尺度几何变换既具有小波变换的多分辨分析和时频局部能力,同时兼具了良好的各向异性,从而能更有效地捕获图像的奇异性几何特性,因此也开始广泛应用于图像分析和编码中。

尝试在 Contourlet 变换域构建快速置乱算法,对图像信息进行安全保护。不同于一些敏感的电子信息(例如银行账户信息),对于大部分的图像应用来说,其保护要求仅是对视觉内容的保护,即达到非授权者无法理解图像内容即可。针对这种应用需求,选择效率较高的混沌密码技术,对 Contourlet 变换后的子带系数按照树型结构进行快速置乱,达到掩蔽图像视觉内容要求,并尽量降低计算开销。

2 相关概念

2.1 离散 Contourlet 变换

2002 年 Do 和 Veterli 提出了一种新的多分辨分析框架——Contourlet 变换,也称金字塔型方向滤波器组 PDFB(Pyramidal Directional Filter Bank)。Contourlet 变换具有良好的多分辨率、局部化和方向性等优良特性,比小波更适合于捕捉高维奇异点信息的特性。

二维离散 Contourlet 变换由两个独立的步骤完成,分别是 Laplacian Pyramid(LP)和 Directional Filter Bank(DFB)变换。图1 显示了使用离散 Contourlet 变换进行二维图像分解的过程。

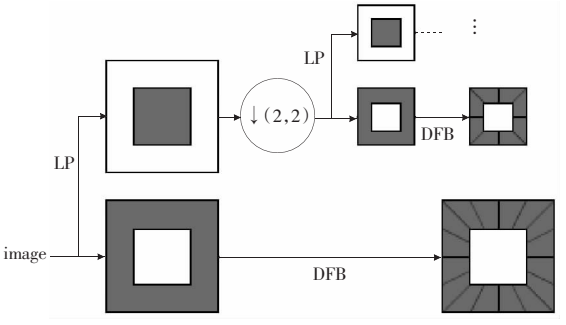

图 1 离散 Contourlet 变换分解示意图

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60572078)。
作者简介:顾国生(1978-),男,博士,讲师,主要研究方向:信息安全与多媒体应用技术;战荫伟(1966-),男,博士,教授,主要研究方向:图像/视频处理与分析;侯文邦(1971-),男,博士,讲师,主要研究方向:计算机图形图像、可视化及虚拟现实。
收稿日期:2009-09-14 **修回日期:**2009-11-20

2.1.1 Laplacian Pyramid

Contourlet 变换首先使用 LP 滤波器[2]对原图像进行子带分解,捕获二维图像信号中存在的奇异点。一次 LP 分解将原始图像信号分解为原信号的低频逼近分量和原信号与低频信号的差值,即高频分量。这一过程在低频逼近图像上可重复进行,从而将原图像分解为多分辨分解图像。

2.1.2 Directional Filter Bank

一次 LP 变换后,Contourlet 变换接着使用方向滤波器组 DFB 对 LP 变换中获得的高频分量进行方向变换,将同方向上的奇异点进行汇集,得到 Contourlet 变换系数。图 2 给出了 Contourlet 变换频域分割示意图。

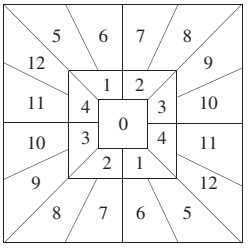

图 2 Contourlet **变换频域分割示意图**

2.2 混沌映射

数值混沌映射具有非常适合于密码系统的特性:遍历性、混合性、非周期性以及对初值的敏感依赖特性等。近十年来混沌理论在数据安全保密方向的应用得到蓬勃发展。

常用的混沌系统包括:

(1)一维 Logistic 映射

$$f(x)=\mu x(1-x),x\in(0,1) \tag{1}$$

当 3.994 65<μ≤4 时,该映射处于混沌状态。

(2)具有一次耦合项形式的二维 Logistic 映射

$$\begin{cases}x_{n+1}=4\mu_1 x_n(1-x_n)+\gamma y_n\\ y_{n+1}=4\mu_2 y_n(1-y_n)+\gamma x_n\end{cases} \tag{2}$$

在 $\mu_1=\mu_2=0.89$,$\gamma=0.1$ 时系统是混沌的。

(3)二维超混沌系统[3]

$$\begin{cases}x_{n+1}=1.55y_n-1.3y_n^2\\ y_{n+1}=0.1y_n-1.1x_n\end{cases} \tag{3}$$

具有两个大于零的 Lyapunov 指数 0.238 和 0.166,是一个超混沌系统。

3 Contourlet 域置乱算法

3.1 Contourlet“零树”结构分析

数字图像经过 Contourlet 变换后的子带系数分布规律和小波变换有许多相似之处。在 Contourlet 系数矩阵中,系数幅值总体而言从低频子带到高频子带是逐渐衰减的。文[4-5]指出,如果对 DFB 选择适当的方向分解数(如进行 l 层分解,每一层高频子带 DFB 分解的方向数设定为下一层分解的方向数的 2 倍,由高至低分别含有 4 个方向子带,8 个方向子带,16 个方向子带,…,2^l 个方向子带),则构建出的 Contourlet 系数矩阵具有“零树”特征,因此可参照小波变换进行嵌入式位平面编码,获得优异的编码效率。图 3 给出了 Barbara 标准图像按上述准则进行 3 层 Contourlet 分解所得到的子带系数分布图示,各层 DFB 分解方向数依次为16、8 和 4。

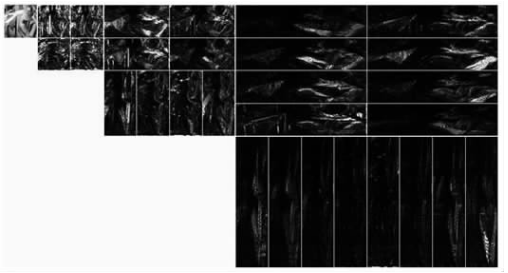

图 3 Barbara **标准图像的** Contourlet **系数分布图**

图 4 给出了这种分解方式下系数矩阵所形成的零树结构。

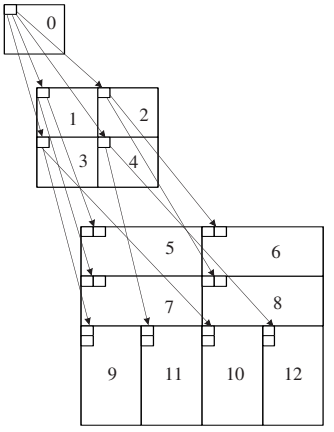

图 4 Contourlet **变换的零树结构**

从图 4 可知,在 Contourlet 变换系数的零树结构中,与小波零树是有区别的。在这种 Contourlet 空间方向树中,除最底层系数节点外,其余节点均有 4 个子节点与之对应,但父节点与子节点的对应模式并不惟一。

设节点(x,y)是父节点,则其对应的直接子节点有两种情形:

情形 1 若(x,y)是低频子带中的节点,则其 4 个子节点集合为:

$$\{(lowbandsize+x,y),(2\times lowbandsize+x,y),(lowbandsize+x,lowbandsize+y),(2\times lowbandsize+x,lowbandsize+y)\} \tag{4}$$

其中,$lowbandsize$ 表示 Contourlet 变换中低频子带的尺寸大小。

情形 2 若(x,y)是第 2^n 个方向子带中的节点(n=1,2,…,l),则其位于 2^{n+1} 方向子带中的 4 个子节点集合又需要分成两种情况:

(1)(x,y)位于 2^n 个方向子带中的上半部(即 $y<2^{n-2}\times lowbandsize$),称这种节点为横向节点,则其 4 个子节点的坐标集合为:

$$\{(lowbandsize+2x-1,y),(lowbandsize+2x,y),(lowbandsize+2x-1,2^{n-1}\times lowbandsize+y),(lowbandsize+2x,2^{n-1}\times lowbandsize+y)\} \tag{5}$$

(2)(x,y)位于 2^n 个方向子带中的下半部(即 $y\geqslant 2^{n-2}\times lowbandsize$),称这种节点为纵向节点,则其 4 个子节点的坐标集合为:

$$\{(2^n\times lowbandsize+x,2y-1),(2^n\times lowbandsize+x,2y),(2^{n+1}\times lowbandsize+x,2y-1),(2^{n+1}\times lowbandsize+x,2y)\} \tag{6}$$

可以看到,如果一个系数节点是横向节点,则其所有子孙均为横向节点。如果一个系数节点是纵向节点,则其所有子孙均为纵向节点。据此,将系数矩阵中的节点子树结构分类:

(1)以低频子带中节点为根的子树，既包含横向节点，也包含纵向节点。这些子树的结构是相同的。

(2)同一层高频子带中以横向节点为根的子树，它们的结构是相同的。

(3)同一层高频子带中以纵向节点为根的子树，它们的结构也是相同的。

3.2　基于“零树”结构的快速置乱

如果 Contourlet 系数矩阵的置乱破坏了上述的零树结构，则会严重影响后续的编码效率，因此下面构建以子树作为置乱单元，保持零树结构的置乱算法。

在置乱方法中，Arnold 变换和幻方置乱由于具有简单、快速的优点而被广泛应用，但这两种变换均不需要密钥控制置乱过程，且具有周期回复性，安全性较低。因此选择安全性较高的二维混沌映射构造置乱矩阵。

首先介绍置乱矩阵的构造，以一个例子来说明。

假设要对一个二维矩阵 $\boldsymbol{A}=(a_{ij})_{4\times5}$ 进行置乱。根据 2.2 节，选取混沌密钥，用混沌映射生成两个一维密钥流序列 q 和 r（长度分别为矩阵 $\boldsymbol{A}$ 的行数 4 和列数 5），例如生成

q=(0.861 1,0.478 2,0.997 6,0.009 6)

r=(0.162 3,0.543 6,0.991 9,0.032 2,0.124 5)

将 q 和 r 进行排序得到

q'=(0.009 6,0.478 2,0.861 1,0.997 6)

r'=(0.032 2,0.124 5,0.162 3,0.543 6,0.991 9)

按照各个元素在排序后的坐标相对于原数组中的位置可以得到

Q=(4,2,1,3)

R=(4,5,1,2,3)

Q 作横坐标，R 作纵坐标，可以由 Q 和 R 得到置乱矩阵

$$\boldsymbol{P}=\begin{pmatrix}(4,4)&(4,5)&(4,1)&(4,2)&(4,3)\\(2,4)&(2,5)&(2,1)&(2,2)&(2,3)\\(1,4)&(1,5)&(1,1)&(1,2)&(1,3)\\(3,4)&(3,5)&(3,1)&(3,2)&(3,3)\end{pmatrix} \tag{7}$$

根据置乱矩阵 $\boldsymbol{P}$，对矩阵 $\boldsymbol{A}$ 执行置乱操作

$$\text{Move } \boldsymbol{A}_{P(i,j)} \text{ to } (i,j) \tag{8}$$

则矩阵 $\boldsymbol{A}$ 的置乱结果为：

$$\boldsymbol{A}=\begin{pmatrix}a_{4,4}&a_{4,5}&a_{4,1}&a_{4,2}&a_{4,3}\\a_{2,4}&a_{2,5}&a_{2,1}&a_{2,2}&a_{2,3}\\a_{1,4}&a_{1,5}&a_{1,1}&a_{1,2}&a_{1,3}\\a_{3,4}&a_{3,5}&a_{3,1}&a_{3,2}&a_{3,3}\end{pmatrix} \tag{9}$$

为了保持空间方向树的整体结构，置乱算法是基于子树的，即以子树为单元进行快速置乱。算法描述如下：

步骤 1　构造与低频子带同样尺寸的置乱矩阵，对低频子带中节点为根的子树进行置乱；

步骤 2　对所有高频子带中的节点为根的子树，为了不影响整体树结构，置乱均限制在与其具有相同父节点的同一分解层中 4 个子节点为根的子树间。构造大小为 2×2 的置乱矩阵，分两种情形进行置乱：

(1)第 l 层高频子带中的节点，与其具有相同父节点的节点中，既有横向节点，也有纵向节点。如果置乱步骤是横向节点为根的子树间的交换或者纵向节点为根的子树间的交换，由于树结构是相同的，直接交换即可。如果置乱步骤是横向节点为根的子树和纵向节点为根的子树间的交换，则需要根据式(4)、(5)、(6)对这两棵子树的坐标作纵横对应变换再进行交换；

(2)其余层高频子带中的节点，同一分解层中与其具有相同父节点的节点均与该节点类型相同，即同为横向节点或同为纵向节点，置乱时直接交换子树即可；

步骤 3　对置乱后的子树作嵌入式编码即得到密文图像。

解密算法是上述步骤的逆过程，在此不再赘述。

4　仿真实验与分析

对 Barbara 标准图像进行按图 3 所示分解，选择二维超混沌映射构建置乱矩阵，置乱结果如图 5 所示。


(a)Barbara 原图像

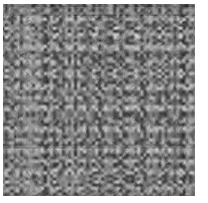
(b)置乱图像

图 5　置乱结果

根据实验结果对算法的性能进行分析。

(1)安全性分析

选择在 Contourlet 变换域进行置乱，打乱了原图像的能量分布规律，可有效抵抗能量分布攻击。图像视觉内容也被有效掩蔽，达到了算法的目标。由于采用对初值极其敏感的混沌密钥流来构建置乱矩阵，密文图像也是对密钥高度敏感的，密钥稍有偏差则不能正确还原图像。图 6 给出了分别使用正确的混沌密钥和错误密钥（与正确密钥相差 10^{-3}）所获得的还原图像。


(a)使用正确密钥的还原图像

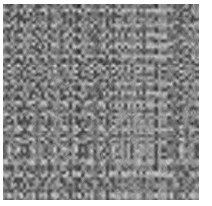
(b)使用错误密钥的还原图像

图 6　还原图像

(2)编码效率影响分析

该文算法尽最大可能保留了系数矩阵空间方向树的结构，保证了系数只在同一层频带同一子树内被置乱，不会发生高低频之间或不同子树之间的系数迁移，因此对编码效率的影响很小。通过对 Barbara 和 Lena 标准图像测试表明，该文置乱算法对压缩率的影响均小于 5%。

(3)计算复杂度分析

该文的置乱算法以子树为单元，相比直接置乱系数矩阵的方法，提高了置乱效率。采用高效的混沌映射，可快速构建置乱矩阵。例如，将 512×512 的 Barbara 标准图像按图 3 方式分解，低频子带仅需要使用 1 个 64×64 置乱矩阵，其他子带使用的均为 2×2 置乱矩阵，以子树为整体作为置乱单元，大大减少了运算量。由图 4 可知，需要进行置乱共 64×64×(1+4+4)=36 864 个单元，若使用 Contourlet 分解后对每个子带进行带内置乱的算法，则需要置乱共 64×64+128×128+256×256=86 016 个单元。

设编码效率影响为 α，不包含置乱步骤时熵编码输出比特数为 B_1，包含置乱步骤时熵编码输出比特数为 B_2，则：

（下转 21 页）