Journal of Computer Applications
计算机应用,2012,32(3):725-728
ISSN 1001-9081
CODEN JYIIDU
2012-03-01
http://www.joca.cn

文章编号:1001-9081(2012)03-0725-04
doi:10.3724/SP.J.1087.2012.00725

# 非局部的变分正则化图像放大算法

姜东焕*,徐光宝,东野长磊
(山东科技大学 信息科学与工程学院,山东 青岛 266590)
(*通信作者电子邮箱 jdh-2002@163.com)

**摘　要**:针对 Chambolle 图像放大模型存在分块效应,提出一种非局部的变分正则化图像放大算法。该算法的思想是构造一个适用于图像放大的变分泛函,该泛函由正则项和数据保真项构成,其中图像的正则项是用非局部全变差范数进行估计,进而用迭代投影方法求泛函的最小解,即为放大后的图像。与传统的图像插值方法不同,该算法是用变分的思想进行图像放大,非局部全变差的引入更使得该算法不只是利用图像的单个像素点,或某一邻域内的灰度和梯度信息进行放大,而是更大范围地利用了图像本身的信息,这将更有效地保留图像特征,避免了 Chambolle 方法在图像放大时出现的分块效应。实验结果表明,该算法能更好地保留边缘和细节信息,放大图像的清晰度比 Chambolle 图像放大方法和样条插值的效果要好。

**关键词**:图像放大;变分泛函;非局部全变差
**中图分类号**:TP391.411;TP301.6　　**文献标志码**:A

## Variational image zooming based on nonlocal total variation

JIANG Dong-huan*, XU Guang-bao, DONGYE Chang-lei
(*College of Information Science and Engineering, Shandong University of Science and Technology, Qingdao Shandong 266590, China*)

**Abstract:** A regularized image zooming model based on nonlocal total variation was proposed, with regard to that the Chambolle image zooming model has blocky effects. It consisted of regular term and fidelity term. The zoomed image was obtained by minimizing the variational function which used the nonlocal total variation norm to measure the regularity of the image. Unlike the traditional image zooming by interpolation, the variational model was incorporated in the new zooming algorithm and the use of nonlocal operator made the algorithm not just use a single pixel of the image, or gray and gradient information in a neighborhood to amplify, but use the information of image content itself widely that will avoid blocky effects of Chambolle's model. The experimental results show that the new algorithm can preserve better the border and details. It achieves better effect than Chambolle's method and the interpolation by using spline.

**Key words:** image zooming; variational function; nonlocal total variation

Journal of Computer Applications 《计算机应用》

## 0　引言

图像放大是一种从一幅低分辨率图像获得其高分辨率版本的图像处理技术。它在图像显示、图像分析、动画制作以及电影合成等领域均有广泛的应用,已经成为图像处理、计算机视觉和计算调和分析等多个学科领域上众多研究者关注的热点问题。

传统的空域图像放大方法有平移重复插值、双线性插值和样条插值等,这些方法简单并且易于实现,用于图像插值也取得了较好的效果,但这些方法都是根据一定的光滑性要求用一些已知的光滑函数逼近源图像。然而这种固定方式有很大的局限性,在图像放大倍数较高时会形成斑点以及在明暗区域出现偏移现象,而且放大倍数越大,这种现象越明显。由于这些固有缺陷,一些新的图像放大算法相继被提了出来,主要有小波插值放大、分形放大、偏微分方程放大以及基于全变差的图像放大算法。2005 年,朱宁等[1]利用偏微分方程理论中的热传导数学模型提出一种热传导方程初边值问题的图像放大法,该方法首次将偏微分方程用于图像放大问题;同年,谢美华等[2]提出先把原图像进行简单初始放大,然后再进行边缘增强锐化处理来得到高分辨率的放大图像;Guichard 等[3]用变分思想对图像放大问题进行建模,提出了一种基于全变差的图像插值方法,得到比较理想的放大效果;2004 年 Chambolle[4]给出了基于全变差的图像放大的迭代投影算法,但是该算法运行速度慢。

近年来,大多数研究者倾向于把各种方法综合起来放大图像。2005 年,石澄贤等[5]提出先把图像的像素值作为尺度下的小波低频部分,置高频部分为零,重构后的初始放大图像用非线性扩散方程处理;2007 年,郝彬彬等[6]把小波变换和扩散方程结合起来用于图像放大。这些方法能较好地对图像进行放大,但是扩散方程的使用使得图像细节边缘比较模糊。2008 年,冯象初等[7]提出一种结合小波变换和变分思想的图像放大方法,该算法用变分方法对图像放大问题建模并提出一种在小波域中求泛函极值的迭代算法。在此基础上,2011 年本文作者在文献[8]中提出了将图像分解为卡通和纹理后再分别用变分方法放大的算法,该算法把图像分解作为图像放大问题的一个预处理过程,获得了比较好的图像放大效果。

Buades 等[9-10]于 2005 年提出了一种非局部平均(Non-Local Means, NLM)滤波算法,非局部平均滤波是受邻域滤波

**收稿日期**:2011-08-12;**修回日期**:2011-11-21。　**基金项目**:山东省自然科学基金资助项目(Y2008G11);山东省优秀中青年科学家科研奖励基金资助项目(BS2010DX026);山东省高等学校科技计划项目(J10LG24);山东科技大学春蕾计划项目(2009AZZ162)。

**作者简介**:姜东焕(1981-),女,山东聊城人,讲师,博士,主要研究方向:偏微分方程图像处理、小波分析;　徐光宝(1980-),男,山东阳谷人,讲师,硕士,主要研究方向:图像处理、信息安全;　东野长磊(1978-),男,山东平邑人,讲师,博士研究生,主要研究方向:图像处理、模式识别。

的方法启发得到的。它不是依靠局部信息,而是利用图像的自相似性质,计算所有相似像素的平均灰度来实现抑制噪声。非局部平均滤波算法自被提出以来,就受到很多学者的关注。研究者在算法的理论解释、性能的改进和拓展方面做了一些研究,Singer 等[11]从扩散的角度对非局部滤波算法进行了解释;Gilboa 等[12-13]给出了非局部平均滤波算法的变分形式和相应的非局部偏微分方程,并在变分的框架下对其进行迭代求解。孙伟峰等[14]在引入邻域模式的对称变换的基础上提出了一种自适应的滤波参数选取方法;徐大宏等[15]针对非局部处理方法中的权值计算作了改进处理,在此基础上提出一种改进的基于非局部的正则化图像去噪算法。有些学者拓展了非局部滤波算法的应用:王卫卫等[16]利用空间非局部梯度设计了图像的非局部扩散张量,并建立了基于非局部扩散张量的各向异性扩散模型;吴晓明等[17]把非局部滤波算法用于序列图像超分辨重构。

## 1 基础知识

### 1.1 非局部平均滤波

非局部平均滤波去噪[9-10]是空域滤波的一个重大突破,它利用自然图像的冗余将当前像素点的灰度值与图像中所有与其结构相似的像素点的灰度值加权平均得到去噪后的像素灰度值。对于每一个像素点的权值,采用以该像素点为中心的图像子块与当前像素点为中心的子块之间的高斯加权欧氏距离来衡量结构相似的像素点。非局部滤波算法具有以下优点:1)该算法是基于图像的全局信息,在对每个像素的加权平滑中考虑了局部结构的相似性,有较高的去噪效果;2)与局部处理工具相比,非局部滤波算法能更好地保持图像中的边缘、纹理等细节特征。

首先简单介绍一些基本的非局部算子。设灰度图像 $\boldsymbol{u}(x):\boldsymbol{\Omega}\to\mathbf{R}$,图像定义域 $\boldsymbol{\Omega}\subset\mathbf{R}^2$ 是一个有界开区域。函数 $\boldsymbol{u}(x)$ 在点 $x(x_1,x_2)$ 相对于点 $y(y_1,y_2)$ 的方向导数为:

$$\partial_y\boldsymbol{u}(x)=(\boldsymbol{u}(y)-\boldsymbol{u}(x))\sqrt{\omega(x,y)}$$

其中:$0<\omega(x,y)<\infty$ 为点 $x$ 和 $y$ 之间的加权系数,且满足对称性 $\omega(x,y)=\omega(y,x)$。$\boldsymbol{u}(x)$ 在点 $x(x_1,x_2)$ 的非局部梯度 $\nabla_w\boldsymbol{u}(x)$ 为 $\boldsymbol{u}(x)$ 在点 $x(x_1,x_2)$ 相对于所有点 $y\in\boldsymbol{\Omega}$ 的方向导数构成的向量:

$$\nabla_w\boldsymbol{u}(x,y)=(\boldsymbol{u}(y)-\boldsymbol{u}(x))\sqrt{\omega(x,y)};y\in\boldsymbol{\Omega}$$

梯度模为:

$$|\nabla_w\boldsymbol{u}|(x)=\sqrt{\int_{\boldsymbol{\Omega}}(\boldsymbol{u}(y)-\boldsymbol{u}(x))\omega(x,y)\mathrm{d}y}$$

Gilboa 等[12-13]提出了一种基于非局部梯度的正则化泛函,该泛函为:

$$J(\boldsymbol{u})=\int_{\boldsymbol{\Omega}}\varphi(|\nabla_w\boldsymbol{u}|^2)\mathrm{d}x=\int_{\boldsymbol{\Omega}}\varphi\Big(\int_{\boldsymbol{\Omega}}(\boldsymbol{u}(y)-\boldsymbol{u}(x))^2\omega(x,y)\mathrm{d}y\Big)\mathrm{d}x$$

其中:$\varphi(s)$ 为一正函数,满足 $\varphi(0)=0$。当取 $\varphi(s)=\sqrt{s}$ 时得到非局部总变差,且此时泛函为凸:

$$J_{\text{NL-TV}}(\boldsymbol{u})=\int_{\boldsymbol{\Omega}}\sqrt{\int_{\boldsymbol{\Omega}}(\boldsymbol{u}(y)-\boldsymbol{u}(x))^2\omega(x,y)\mathrm{d}y}\mathrm{d}x$$

上述非局部全变差泛函关于 $\boldsymbol{u}$ 的变分(Euler-Lagrange)为:

$$\partial_{\boldsymbol{u}}J_{\text{NL-TV}}(\boldsymbol{u})=-\int_{\boldsymbol{\Omega}}(\boldsymbol{u}(y)-\boldsymbol{u}(x))\omega(x,y)\Big(\frac{1}{|\nabla_w\boldsymbol{u}|(x)}+\frac{1}{|\nabla_w\boldsymbol{u}|(y)}\Big)\mathrm{d}y$$

### 1.2 Chambolle 图像放大模型

假设讨论的图像是 $N\times N$ 的二维矩阵,$\boldsymbol{X}$ 表示空间 $\mathbf{R}^{N\times N}$,$\boldsymbol{Z}$ 是 $\boldsymbol{X}$ 的一个子空间,$\boldsymbol{g}\in\boldsymbol{Z}$ 表示一幅粗糙的图像。例如,当放大因子为 2 时,用数学式子表示 $\boldsymbol{Z}$ 为:

$$\boldsymbol{Z}=\{\boldsymbol{g}\in\boldsymbol{X}\mid \boldsymbol{g}_{2k,2l}=\boldsymbol{g}_{2k-1,2l}=\boldsymbol{g}_{2k,2l-1}=\boldsymbol{g}_{2k-1,2l-1},\ k,l\leqslant N/2\}$$

Chambolle 图像放大模型[4]为:

$$\min_{\boldsymbol{u}\in\boldsymbol{X}}\|\boldsymbol{A}\boldsymbol{u}-\boldsymbol{g}\|^2+2\lambda\cdot TV(\boldsymbol{u})$$

其中:$\boldsymbol{u}$ 是放大后的图像,$\boldsymbol{A}$ 是在空间 $\boldsymbol{Z}$ 上的正交投影。显然有 $\boldsymbol{A}\boldsymbol{g}=\boldsymbol{g}$ 及

$$\|\boldsymbol{A}\boldsymbol{u}-\boldsymbol{g}\|=\|\boldsymbol{A}(\boldsymbol{u}-\boldsymbol{g})\|=\min_{w\in\boldsymbol{Z}^\perp}\|\boldsymbol{u}-\boldsymbol{g}-w\|$$

从而,该图像放大模型变为:

$$\min_{\boldsymbol{u}\in\boldsymbol{X},w\in\boldsymbol{Z}^\perp}\|\boldsymbol{u}-(\boldsymbol{g}+w)\|^2+2\lambda\cdot TV(\boldsymbol{u})$$

Chambolle[4]给出了求解上述最小值问题的一种迭代算法。虽然该方法能得到比较好的图像放大效果,但是该算法仅仅考虑了图像的局部信息,不能较好地放大图像的细节和纹理等特征,所以寻求能够利用图像自相似性信息的放大算法具有重要的理论价值和实际意义。

## 2 基于变分的非局部图像放大算法

### 2.1 非局部的图像放大算法

本文将非局部滤波算法应用到图像放大问题上,提出了一种新的算法,即非局部的变分正则化图像放大算法。该算法的思想是构造一个用非局部全变差范数估计图像正则性的变分泛函,该变分泛函的最小解即为放大后的图像。与传统的插值放大图像不同,该算法是用变分的思想进行图像放大,非局部全变差的引入使得该算法考虑到了图像所有的像素点而不只是用图像单个像素点,或某一邻域内的灰度和梯度信息进行放大,这样更大范围地利用了图像本身的信息,得到的放大图像较好地保留了图像的细节和纹理等特征,更有效地改善了图像放大质量。

本文的图像放大模型为:

$$\min_{\boldsymbol{u}\in\boldsymbol{X}}\|\boldsymbol{A}\boldsymbol{u}-\boldsymbol{g}\|^2_{L_2(\boldsymbol{\Omega})}+2\lambda J_{\text{NL-TV}}(\boldsymbol{u})$$

同样地,该问题等价于最小化下列泛函:

$$E(\boldsymbol{u},w)=\|\boldsymbol{u}-(\boldsymbol{g}+w)\|^2_{L_2(\boldsymbol{\Omega})}+2\lambda J_{\text{NL-TV}}(\boldsymbol{u})\qquad(1)$$

其中:$\boldsymbol{u}\in\boldsymbol{X},w\in\boldsymbol{Z}^\perp$。

对于该问题的求解相当于考虑下面两个最小化问题:

固定 $w$,求泛函式(1)关于 $\boldsymbol{u}$ 的最小解,即求:

$$\min_{\boldsymbol{u}}\|\boldsymbol{u}-(\boldsymbol{g}+w)\|^2_{L_2(\boldsymbol{\Omega})}+2\lambda J_{\text{NL-TV}}(\boldsymbol{u})\qquad(2)$$

此为非局部的全变差最小化模型,利用最速下降法求解,其相应的 Euler-Lagrange 方程为:

$$\boldsymbol{u}-(\boldsymbol{g}+w)+\lambda\partial_{\boldsymbol{u}}J_{\text{NL-TV}}(\boldsymbol{u})=0$$

泛函式(2)的解为:

$$\tilde{\boldsymbol{u}}=\boldsymbol{g}+w-\lambda\partial_{\boldsymbol{u}}J_{\text{NL-TV}}(\boldsymbol{u})$$

固定 $\boldsymbol{u}$,求泛函式(1)关于 $w$ 的最小解,即:

$$\min_{w}\|\boldsymbol{u}-(\boldsymbol{g}+w)\|^2_{L_2(\boldsymbol{\Omega})}$$

其最小解为 $\tilde{w}=P(\boldsymbol{u}-\boldsymbol{g})$,其中 $P$ 为空间 $\boldsymbol{Z}$ 上的正交投影算

《计算机应用》Journal of Computer Applications

子。

当新模型中的导数采用传统导数时,就是 Chambolle 图像放大算法。

### 2.2　新模型的算法

新模型的解可以用迭代投影的方法得到,其算法归纳如下:

1) 初始化。设置搜索窗 $h$ 的大小,块大小,相似块个数以及迭代次数;令 $w_0 = 0$。

2) 对每个像素点 $i$,需要计算权值 $w_{i,j}$,以像素点 $i$ 为中心的搜索窗内,检查搜索窗内每个像素为中心,大小为 $b$ 的小块,找出和像素点 $i$ 最相似的 $k$ 个像素,置其权为 1,其他像素点权置 0。

3) 迭代:

$$\boldsymbol{u}_{n+1} = \boldsymbol{g} + w_n - \lambda \partial_u J_{\mathrm{NL-TV}}(\boldsymbol{u}_n)$$

$$w_{n+1} = P(\boldsymbol{u}_{n+1} - \boldsymbol{g})$$

4) 令 $n = n + 1$,重复 3) 直到预先给定的迭代次数。

## 3　仿真实验

下面将非局部图像放大模型与 Chambolle 放大模型进行比较。为便于比较,先将原图下采样缩小一定的倍数作为实际获取的图像,然后再放大。在所有仿真实验中,本文采用 7×7的搜索窗口,用 5×5 的像素块计算权值,$k$ 取为 10。实验仿真结果见图 1~4。图 1~3 是采用 Chambolle 放大模型和新方法对图像放大两倍的结果。可以看出,图 1 中 Chambolle 放大模型得到的图像边缘比较模糊,有分块效应。采用本文方法避免了一定的分块效应,得到的图像细节丰富,如 Lena 图像中帽子上的皱褶及头发比较清晰。图 2 是对纹理细节更丰富的 Barbara(246×246)图像采用 Chambolle 放大模型和本文方法进行放大两倍的结果。可以看出,Chambolle 模型[4]得到的放大图像的围巾上的纹理比较模糊,而本文方法得到的图像比较清晰。图 3 是对一幅钟表图像进行放大的效果图。可以看出,新算法得到的放大图像上钟表部分的刻度较为清晰,图像中相框部分较好地保留了边缘。这表明了本文算法能更好地保持图像的细节和边缘特征。为了更好地说明新算法的放大效果,采用三次样条插值和新算法对医学 Brain 图像放大两倍,实验结果见图 4。可以看出用本文算法放大的图像细节和边缘可以得到比样条插值更好的放大效果。

客观上,可以采用信噪比(Signal-to-Noise Ratio, SNR)、峰值信噪比(Peak Signal-to-Noise Ratio, PSNR)和均方误差(Mean Square Error, MSE)来评价图像放大效果的好坏。PSNR 是一种比较接近人眼的视觉效果评价量。信噪比和均方误差用来测量放大图像与标准图像的相近程度。下面对 4 幅图像进行实验,实验数据见表 1,由表 1 可见新算法更适合处理自然图像及细节丰富的图像。

**表 1　Chambolle 模型与本文算法的放大性能比较**

| 图像 | 放大倍数 | Chambolle 模型 | | | 本文算法 | | |
|---|---|---|---|---|---|---|---|
| | | *SNR*/dB | *PSNR*/dB | *MSE* | *SNR*/dB | *PSNR*/dB | *MSE* |
| Brain | 2 | 5.8590 | 23.0337 | 0.0050 | 6.4062 | 23.1955 | 0.0048 |
| Barbara | 2 | 8.9140 | 22.5386 | 0.0056 | 8.9983 | 22.6029 | 0.0055 |
| Block | 2 | 11.5098 | 24.3275 | 0.0037 | 12.0132 | 24.9031 | 0.0032 |
| Lena | 2 | 13.0020 | 27.2997 | 0.0019 | 14.3126 | 28.5405 | 0.0014 |
| Lena | 4 | 8.0735 | 22.2436 | 0.0060 | 8.7059 | 23.0216 | 0.0050 |

## 4　算法复杂度分析

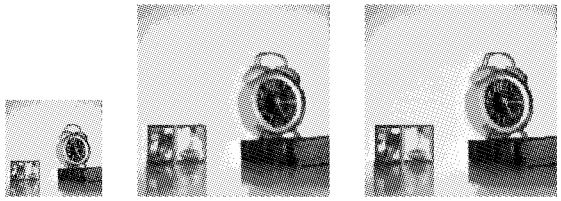
本文算法是基于图像的全局信息的,在对每个像素的加权放大中考虑了局部结构的相似性。因此,搜寻窗 $h$ 和像素块 $b$ 的大小的选取直接影响着图像放大的效果。选取的相似块的范围越大,图像放大的效果越好,算法的运算时间也就越长。实际上,新算法的迭代次数比局部的 Chambolle 放大模型的次数少,但在迭代过程中,新算法是在全局中选取相似点,所以每次迭代过程中计算量比局部算法大,尽管迭代次数少,总的运算量比局部算法大很多,因而运算时间较长。例如,图像的像素个数是 $N^2$,那么新算法的复杂度大约是 $h^2 \times b^2 \times N^2$。

(a) Chambolle模型放大　(b) 本文算法放大

图 1　对 Lena(256×256)图像放大两倍的结果比较

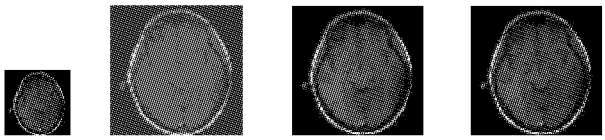
(a) Chambolle模型放大　(b) 本文算法放大

图 2　对 Barbara(123×123)图像放大两倍的结果比较



(a) 钟表图像　(b) Chambolle模型放大　(c) 本文算法放大

图 3　对 Block 图像放大两倍的结果比较



(a) Brain图像　(b) 样条插值放大　(c) Chambolle模型放大　(d) 本文算法放大

图 4　几种方法放大结果比较

## 5　结语

与传统的图像放大方法不同的是,本文从能量变分的角度研究图像放大问题,提出一种将能量最小化问题和非局部滤波相结合的图像放大算法。该算法用非局部总变差刻画图像的正则性构造了一个变分泛函,然后通过最小化该变分泛函得到放大图像。Chambolle 图像放大算法等已有的放大算法只是利用图像单个像素点,或某一邻域内的灰度和梯度信息放大图像,因而存在分块效应。本文算法中非局部滤波算子的引入使得它能够更大范围地利用图像本身的自相似的信息进行放大,因而能够保留更多的细节特征,避免一定的

Journal of Computer Applications 《计算机应用》

分块效应;变分模型的引入对放大后的图像强加了几何正则性的要求,这就保证了用本文算法放大的图像边缘的光滑性,因而能够重构出高质量的图像。由实验结果可知,本文算法适合处理自然图像及含丰富细节的图像,并且在视觉上可以达到比样条插值更好的放大效果。但是,由于本文算法考虑了图像的全局信息,所以算法复杂度比较高,提高算法速度将是今后需要研究的主要内容。

**参考文献:**


[1] 朱宁,吴静,王忠谦.图像放大的偏微分方程方法[J].计算机辅助设计与图形学学报,2005,17(9):1941-1945.

[2] 谢美华,王正明.基于边缘定向扩散的图像增强方法[J].光子学报,2005,34(9):1420-1424.

[3] GUICHARD F, MALGOUYRES F. Edge direction preserving image zooming: a mathematical and numerical analysis[J]. SIAM Journal of Numerical Analysis, 2001, 39(1): 1-37.

[4] CHAMBOLLE A. An algorithm for total variation minimization and applications[J]. Journal of Mathematical Imaging and Vision, 2004, 20(1/2): 89-97.

[5] 石澄贤,吴建成,夏德深.各向异性扩散方程和一种图像放大方法[J].南京大学学报:数学半年刊,2005,22(1):153-160.

[6] 郝彬彬,冯象初.一种基于小波和矩阵型扩散的图像放大[J].光子学报,2008,37(11):2365-2368.

[7] 冯象初,姜东焕,徐光宝.基于变分和小波变换的图像放大算法[J].计算机学报,2008,31(2):340-345.

[8] JIANG DONG-HUAN, XU GUANG-BAO. Image zooming based on cartoon and texture decomposition [C]// International Conference on Information Systems and Computational Intelligence. Washington, DC: IEEE Computer Society, 2011:119-122.

[9] BAUDES A, COLL B, MOREL J M. A non-local algorithm for image denoising[C]// IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Washington, DC: IEEE Computer Society, 2005: 60-65.

[10] BAUDES A, COLL B, MOREL J M. On image denoising method [J]. SIAM Multiscale Modeling and Simulation, 2005, 4(2):490-530.

[11] SINGER A, SHKOLNISKY Y, NADLER B. Diffusion interpretation of non-local neighborhood filters for signal denoising[J]. SIAM Journal on Imaging Sciences, 2009, 2(1):118-139.

[12] GILBOA G, OSHER S. Nonlocal linear image regularization and supervised segmentation[J]. SIAM Multiscale Modeling and Simulation, 2007, 6(2): 595-630.

[13] GILBOA G, OSHER S. Nonlocal operators with applications to image processing[J]. SIAM Multiscale Modeling and Simulation, 2008, 7(3):1005-1028.

[14] 孙伟峰,彭玉华.一种改进的非局部平均去噪方法[J].电子学报,2010,38(4):923-928.

[15] 徐大宏,王润生.基于非局部正则化的图像去噪[J].计算机应用研究,2009,26(12):4830-4832.

[16] 王卫卫,韩雨,冯象初.基于非局部扩散的图像去噪[J].光学学报,2010,30(2):373-375.

[17] 吴晓明,陈斌,阮波,等.基于非局部算法的序列图像超分辨率重构[J].计算机应用,2009,29(1):95-96.

[18] GILBOA G, OSHER S. Nonlocal operators with applications to image processing[J]. SIAM Multiscale Modeling and Simulation, 2008, 7(3):1005-1028.

[19] GILBOA G, DARBON J, OSHER S, *et al.* Nonlocal convex functionals for image regularization[R]. [S.l.]: UCLA, 2006.


Journal of Computer Applications 《计算机应用》

(上接第 704 页)


[10] KIAYIAS A, XU S, YUNG M. Privacy preserving data mining within anonymous credential systems [C]// SCN 2008: Proceedings of the 6th Conference on Security and Cryptography for Networks, LNCS 5229. Berlin: Springer-Verlag, 2008: 57-76.

[11] LYSYANSKAYA A. Threshold cryptography secure against the adaptive adversary, concurrently [EB/OL]. [2011-08-01]. http://eprint.iacr.org/2000/019.

[12] CANETTI R, GENNARO R, JARECHI S, *et al.* Adaptive security for threshold cryptosystems [C]// CRYPTO 1999: Proceedings of the 19th Annual International Cryptology Conference, LNCS 1666. Berlin: Springer-Verlag, 1999: 98-116.

[13] JARECHI S. Efficient threshold cryptosystems [D]. Cambridge, USA: Massachusetts Institute of Technology, 2001.

[14] FISCHLIN M, ONETE C. Relaxed security notions for signatures of knowledge [C]// ACNS 2011: Proceedings of the 9th International Conference on Applied Cryptography and Network Security, LNCS 6715. Berlin: Springer-Verlag, 2011: 309-326.

[15] GENNARO R, JARECHI S, KRAWCZYK H, *et al.* Secure distributed key generation for discrete-log based cryptosystems [J]. Journal of Cryptology, 2007, 20(1): 51-83.

[16] AU M H, SUSILO W, MU Y. Constant-size dynamic *k*-TAA [EB/OL]. [2011-08-01]. http://eprint.iacr.org/2008/136.

[17] ROSEN A, SHELAT A. Optimistic concurrent zero knowledge [C]// ASIACRYPT 2010: Proceedings of the 16th Annual International Conference on the Theory and Application of Cryptology and Information Security, LNCS 6477. Berlin: Springer-Verlag, 2010: 359-376.

[18] NGUYEN L, SAFAVI-NAINI R. Efficient and provably secure trapdoor-free group signature schemes from bilinear pairings [C]// ASIACRYPT 2004: Proceedings of the 10th Annual International Conference on the Theory and Application of Cryptology and Information Security, LNCS 3329. Berlin: Springer-Verlag, 2004: 372-386.

[19] OHTAKE G, FUJII A, HANAOKA G, *et al.* On the theoretical gap between group signatures with and without unlinkability [C]// AFRICACRYPT 2009: Proceedings of the 2nd African International Conference on Cryptology, LNCS 5580. Berlin: Springer-Verlag, 2009: 149-166.

[20] FISCHLIN M. Communication-efficient non-interactive proofs of knowledge with online extractor [C]// CRYPTO 2005: Proceedings of the 25th Annual International Cryptology Conference, LNCS 3621. Berlin: Springer-Verlag, 2005: 152-168.

[21] FERRARA A L, GREEN M, HOHENBERGER S, *et al.* Practical short signature batch verification [C]// CT-RSA 2009: Proceedings of the Cryptographers' Track at the RSA Conference 2009, LNCS 5473. Berlin: Springer-Verlag, 2009: 309-324.

[22] WASEF A, SHEN X. Efficient group signature scheme supporting batch verification for securing vehicular networks [C]// IEEE ICC 2010: Proceedings of the 2010 IEEE International Conference on Communications. Piscataway, NJ: IEEE Press, 2010: 1-5.