doi: 10.7690/bgzdh.2015.10.012

定向测量与加权算法的信息隐藏技术

田鹏义，许定根，朱仁峰
（装备学院昌平士官学校，北京 102200）

摘要：针对压缩感知(compressed sensing，CS)技术中的观测值存在一定的冗余、可以进行秘密信息写入的问题，为提高隐藏算法的不可感知性与运算速度，提出一种定向测量算法，即只对载体图像的重要部分进行稀疏、测量，同时在隐藏时利用加权的思想对隐藏位置进行选择，并给出信息隐藏与提取的方法。仿真结果表明：该方法在不可感知性与计算时间损耗上均优于传统算法，且具有一定的鲁棒性和抗提取性。

关键词：压缩感知；信息隐藏；定向测量；加权算法
中图分类号：TP306　　**文献标志码**：A

Information Hiding Technology Based on Directional Measurement and Weighted Algorithm

Tian Pengyi, Xu Dinggen, Zhu Renfeng
(*College of Non-commissioned Officer of Changping*, *Academy of Equipment*, *Beijing* 102200, *China*)

Abstract: The observation values of the compressed sensing (compressed sensing, CS) technique exist certain redundancy, it can be used to write secret information. In order to improve hiding algorithm of perceptual and computational speed, this paper presents a directional measurement algorithm, which only let the important part of the carrier image sparse and measure, while select hide location by using the idea of weighted algorithm and provide the information hiding and extraction method. Simulation result shows, the method in imperceptibility and calculation time losses are superior to the traditional algorithm and has certain robustness and extraction resistance.

Keywords: compress sensing; information hiding; directional measurement; weighted algorithm

0　引言

信息隐藏技术在信息安全领域日益受到关注，该技术隐藏了信息的存在性[1-2]，使得非法第三方无法感知秘密信息的存在，新理论的引入为信息隐藏领域带来了发展活力，压缩感知(compressed sensing，CS)[3]理论就是其中的代表，该理论突破了“奈奎斯特采样定理”的限制，为信息隐藏领域带来了新的发展契机。

CS 技术指出：如果信号本身是稀疏的或者通过某种变换达到稀疏，就能通过一个与变换基不相关的测量矩阵来测量该信号进而得到测量值，并通过测量值、测量矩阵与稀疏基完成原始信号的重构。

在整个过程中，观测值存在一定的冗余，可以进行秘密信息的写入[4]。文献[5]指出，将载体图像进行一次小波变换，形成稀疏的矩阵，然后利用高斯随机矩阵对该矩阵进行观测，得到观测值，将秘密信息乘以隐藏系数后藏入观测值即可，取得了理想的效果；然而该方法需要的观测矩阵与载体图像大小相当，计算时间过长，且没有对观测值进行“选择性”隐藏，还有很大的改进空间。

基于此，笔者提出一种算法，将载体图像进行 2 次小波变换，第 1 次与文献[5]的方法相同，第 2 次变换其低频部分，即将“原始载体的低频部分”进行稀疏化，然后再利用与载体图像 1/4 大小的观测矩阵进行测量，即定向测量整个载体图像的主要部分，节约了计算时间；其次又利用加权算法对实现秘密信息的写入，选出观测值中绝对值较大的数据实现秘密信息隐藏，达到秘密信息的写入对整个观测值矩阵的影响最小的目的。实验仿真结果证明：该方法在计算时间与透明性上取得了较好的效果，且具有一定的鲁棒性。

1　压缩感知技术与加权算法简介

1.1　压缩感知技术

压缩感知技术由 3 部分组成：稀疏变换、观测矩阵和重构算法[6]。

首先，信号 X 在某个正交基 Ψ 上是稀疏的，即

$$\Theta = \psi^{\mathrm{T}} X \text{。} \tag{1}$$

其中 Θ 是稀疏系数。

其次，设计一个与正交基不相关 $M \times N$ 维的观

收稿日期：2015-06-05；**修回日期**：2015-07-09
基金项目：国家高技术研究发展 863 计划资助项目(2014AA7011073)
作者简介：田鹏义(1985—)，男，陕西人，硕士，讲师，从事图像通信研究。

测矩阵 $\boldsymbol{\Phi}$，对稀疏系数进行观测，得到观测值

$$Y=\boldsymbol{\Phi}\Theta=\boldsymbol{\Phi}\psi^{\mathrm{T}}X\text{。}\tag{2}$$

最后，通过优化问题求解对原始信息进行还原计算，即

$$\min\left\|\psi^{\mathrm{T}}X\right\|_0\text{，}\ \text{s.t.}\ \boldsymbol{\Phi}\psi^{\mathrm{T}}X=Y\text{。}\tag{3}$$

1) 稀疏变换。

自然界中大部分信号都不满足稀疏性，但是可以通过变换实现稀疏表示，满足了压缩感知技术处理稀疏信号的条件，常见的稀疏变换有离散余弦变换、离散小波变换、离散傅里叶变换等，笔者在文献[5]的基础上进行改进，采用的是离散小波变换。

2) 观测矩阵。

观测矩阵必须满足约束等距条件(restricted isometry principle，RIP)，即观测矩阵与离散基不相关。常用的观测矩阵有高斯随机矩阵和傅里叶随机矩阵，高斯随机矩阵几乎与任何稀疏信号都不相关，而且容易生成，笔者采用该矩阵。

3) 重构算法。

信号重构就是对观测值的某种运算，求解出原始信号，实现信息的重构。压缩感知重建算法实质是求一个欠定方程的解，常见的算法有基追踪算法(basis pursuit，BP)、匹配追踪算法(matching pursuit，MP)、正交匹配追踪算法(othogonal matching pursut，OMP)。BP 算法较为复杂，消耗时间过多；MP 算法需要的观测值个数较多，但可以大量节约计算时间；OMP 算法是在 MP 算法基础上进行改进的，效果更佳，故笔者采用 OMP 算法进行计算。

1.2　加权算法

美国学者 Yager 介绍过几种加权平均算法，其主要思想是：不同的参数决定不同因素在整个系统中的“地位”——权重，通过不同的权重对事件产生不同的推测与判断，可以获得较理想的结果[7]。笔者把这一思路用在信息隐藏方面，把秘密信息藏入载体图像不同的权重位置中，隐藏效果会更理想。

设观测值中共有 n 个值，定义每一个数的绝对值为指标值 I_j，则每个值的权重

$$w_j=\frac{I_j}{\sum_{i=1}^{n}I_i}\text{。}\tag{4}$$

如果权值有变化，变化量为 e_j，则权值变化率

$$p_j=\frac{e_j}{I_j}\text{。}\tag{5}$$

设有权重分别为 w_{l} 与 w_{s} 的两点，且满足

$$w_{\mathrm{l}}>w_{\mathrm{s}}\text{，}\tag{6}$$

则

$$I_{\mathrm{l}}=w_{\mathrm{l}}\bullet\sum_{i=1}^{n}I_i\text{，}\tag{7}$$

$$I_{\mathrm{s}}=w_{\mathrm{s}}\bullet\sum_{i=1}^{n}I_i\text{。}\tag{8}$$

可得

$$I_{\mathrm{l}}>I_{\mathrm{s}}\text{。}\tag{9}$$

当产生一个相同的变化量 e，则

$$\frac{e}{I_{\mathrm{l}}}<\frac{e}{I_{\mathrm{s}}}\text{，}\tag{10}$$

即

$$p_{\mathrm{l}}<p_{\mathrm{s}}\text{。}\tag{11}$$

从推导过程可以得出：观测值中某个数据权重越大，对整个观测值的作用就越大；同时，如果产生一个相同的变化量，在权重较大的位置产生的变化率较小。加权隐藏算法就是在充分考虑观测值中每一个隐藏位置权重的基础上，完成秘密信息隐藏。利用加权算法进行隐藏，对观测值的整体影响较小，有利于提高载密载体的不可感知性。

2　文中算法

设需要隐藏的秘密信息数量为 n，文中算法的主要步骤如下。

2.1　信息隐藏算法

1) 首先对载体图像进行小波变换，然后对其低频部分再进行小波变换，得到稀疏矩阵；

2) 利用载体图像 1/4 大小的测量矩阵对变换后的低频部分进行测量，得到观测值；

3) 选出观测值中绝对值较大的 n 个值，进行秘密信息写入；

4) 恢复图像，得到载密图像，完成信息隐藏。过程如图 1 所示。

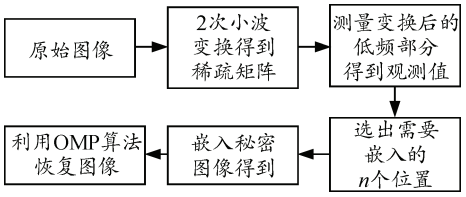

图 1　隐藏过程

2.2　信息提取算法

1) 利用隐藏时 2 次变换的小波稀疏基对载密图像与载体图像分别进行 2 次变换，得到 2 组稀疏矩阵；

2) 利用测量矩阵分别对 2 组稀疏矩阵进行测量，得到载密观测值与原始观测值；

3) 在原始观测之中选出绝对值较大的 n 个值；

4) 将这些值的位置对应到载密观测值中，完成秘密信息提取。

算法过程如图 2 所示。

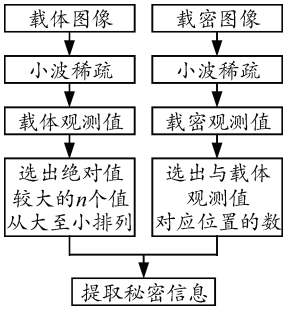

图 2　提取过程

3　仿真与分析

3.1　模拟仿真

如图 3 所示，笔者以 256×256 的“woman.jpg”图像作为载体图像，64×64 的“数字水印”作为秘密信息。

(a) 载体图像

(b) 秘密信息

图 3　载体图像与秘密信息

利用 Matlab 进行实验仿真，信息隐藏效果如图 4 所示。

在理想状态下，提取效果如图 5 所示。

(a) 载体图像

(b) 载密图像

图 4　载体图像与载密图像

(a) 秘密信息

(b) 提取效果

图 5　提取效果对比

从实验仿真中可以得出：无论是载密图像还是提取图像，视觉效果都比较理想，下面从数学角度对 2 种方法进行分析。

3.2　数据分析

3.2.1　透明性分析

透明性是指秘密信息隐藏后的不可感知性，一般用峰值信噪比(PSNR)[8]来衡量，峰值信噪比越高，则透明性越好，计算如下式：

$$\mathrm{PSNR}=10\lg\left(\frac{255^2}{\frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[X(i,j)-X'(i,j)\right]^2}\right)。\quad(12)$$

式中：X 为原始载体图像；X'为载密图像；M、N 为图像的行列像素数。当 PSNR 大于 30 dB 的时候，不会引起人类视觉的敏感反应，隐藏效果可以被接

受，根据不同的算法，所得到的 PSNR 值不同。

由于笔者采用的是定向压缩感知，即只对载体图像的“重要部分”进行测量，定向感知的图像恢复效果优于全向感知[9]，比传统算法的全向压缩后图像的效果理想；其次，笔者在嵌入秘密信息时使用了加权隐藏算法，保证秘密信息写入后对观测值的整体影响尽可能小，以实现理想的恢复效果。现利用 256×256 大小的 lion、lena、woman 3 幅图像作为载体图像，对 64×64 的秘密信息利用 2 种算法进行隐藏，PSNR 值如表 1 所示。

表 1　透明性对比

载体图像的 PSNR/dB	lion	lena	woman
传统算法	35.9	36.9	36.5
文中算法	37.2	37.5	37.8

从上表可以得出：文中算法具有较强的透明性，相比于传统算法更优越。

3.2.2　提取质量分析

对于提取质量的衡量，可以通过计算 2 幅图像的相关系数[10](NC 值)进行说明，计算如下式：

$$\mathrm{NC}=\frac{\sum_{i=0}^{L-1}\sum_{j=0}^{K-1}x(i,j)x'(i,j)}{\sum_{i=0}^{L-1}\sum_{K=0}^{K-1}\left[x(i,j)\right]^2}。\qquad(13)$$

式中：x 为原始秘密信息；x'为提取后的秘密信息；L、K 为行列像素数。NC 值最大为 1，通常状况下，当 NC 值小于 0.5 时，提取失败，文中算法的 NC 值可达 0.998 7，满足信息提取的要求。

3.2.3　鲁棒性分析

载密图像在传输的过程中会受到不同程度的干扰，如 JPEG 压缩攻击、噪声干扰等，同样可以采用 NC 值进行测量，笔者采用 JPEG 压缩、高斯噪音、椒盐噪音 3 种攻击方式验证文中算法的鲁棒性，NC 值如表 2 所示。

表 2　人为干扰后的 NC 值

JPEG 压缩	NC 值	高斯噪音	NC 值	椒盐噪音	NC 值
95	1.000	0.000 2	0.998	0.002	0.970
90	0.985	0.000 4	0.964	0.004	0.919
85	0.910	0.000 6	0.951	0.006	0.853
80	0.813	0.000 8	0.873	0.008	0.848

部分恢复信息如图 6 所示。


(a) 原始信息


(b) JPEG 压缩(质量因子 95)


(c) 高斯噪音标准差 0.000 6


(d) 椒盐噪音强度 0.004

图 6　人为干扰后的部分效果图

从上表与提取效果分析，文中算法可以抵御部分程度的人为攻击，有一定的鲁棒性。

3.2.4　耗时分析

文中算法只利用载体图像 1/4 大小的观测矩阵进行数据测量，在整个信息的隐藏提取方面相比较于传统算法节约了大量的计算时间，在载体图像同为 256×256，秘密信息大小为 64×64 的条件下，利用文中算法与传统算法进行信息隐藏，消耗时间如表 3 所示。

表 3　耗时对比

载体图像	图像大小	秘密信息大小	算法耗时/s	
			传统	文中
Woman	256×256	64×64	267.5	66.4
Lena	256×256	64×64	268.9	67.2
Lion	256×256	64×64	265.3	65.9

从上表可以看出：文中算法优于传统算法，节约了计算时间，降低了计算成本。

3.2.5　抗提取性分析

压缩感知技术要求信息的压缩与恢复必须采用相同的观测矩阵，否则无法实现信息的还原，非法第三方若要对秘密信息进行提取，在没有掌握观测矩阵的条件下，提取效果如图 7 所示。

图 7　非法提取效果图

非法提取图像失败，证明文中算法在没有进行数据加密的条件下有效保证了信息的安全性。

4　结论

笔者在压缩感知技术应用于信息隐藏领域的基础上提出了一种定向观测算法，即只对载体图像的重要部分(低频部分)进行观测，节约了大量的计算时间，恢复效果较为理想；利用加权隐藏算法进行秘密信息的隐藏，提高了载密图像的透明性，同时文中算法具有一定的鲁棒性，可以抗击一定程度的 JPEG 压缩、噪声干扰与非法提取，保证了秘密信息的安全。该算法在抗噪声攻击方面还稍显不足，需要进一步研究提高。

(下转第 51 页)