基于遗传优化图像稀疏分解的密写算法

欧阳春娟[1,2] 李 霞[1,2] 李 斌[1,2]
(1. 深圳大学信息工程学院，广东 深圳 518060；
2. 深圳市现代通信与信息处理重点实验室，广东 深圳 518060)

摘 要：根据超完备字典图像稀疏表示的稀疏性和特征保持性，提出了基于遗传优化图像稀疏分解的密写算法。该密写算法将信息隐藏与基于图像稀疏分解的压缩过程合二为一。首先在基于 MP 的图像稀疏分解每步迭代中，采用遗传算法快速实现最佳匹配原子的选取；对稀疏分解得到的结果用不同的量化位数进行量化；最后采用 LSB 嵌入方式将秘密信息隐藏于量化后参数的不同最低有效位中，得到载密图像。实验结果表明，本文提出的基于遗传优化图像稀疏分解的密写算法具有良好的视觉效果，与相同嵌入容量的经典空域和 DCT 域 LSB 算法相比，本文的密写算法获得了更高的抵抗隐写分析能力。抗隐写分析实验也表明新的密写算法对嵌入位数不敏感，可灵活地扩充嵌入容量。

关键词：稀疏分解；匹配追踪；遗传优化；隐写
中图分类号：TP309.2 **文献标识码**：A **文章编号**：1003-0530(2012)06-0821-06

A Steganographic Algorithm Based on Image Sparse Decomposition Optimized by GA

OUYANG Chun-juan[1,2] LI Xia[1,2] LI Bin[1,2]
(1. College of Information Engineering, Shenzhen University, Shenzhen 518060, China;
2. The Key Laboratory of Shenzhen Modern Communications and infromation Processing, Shenzhen 518060, China)

Abstract: Considering the sparsity and integrity of the sparse representation of images over-complete dictionaries, this paper presents a novel image steganographic method with genetic algorithm (GA) based on sparse decomposition. In this method, the data hiding process is integrated into the image sparse compression process. First, in each iteration of the matching pursuit of image sparse decomposition, the best matching atom is selected by GA. Then, the coefficients of sparse decomposition are quantified by different quantization bits. Finally, the stego image is obtained via embedding secret information in the different least significant bits (LSBs) of the quantized coefficients. Experimental results show that the proposed steganographic algorithm maintains good invisibility. Meanwhile, compared to the classical LSB methods of space domain and DCT domain, the new steganography has better ability in resisting steganalysis under the same embedding capacity. Experimental results also indicate that the new steganography is less sensitive to the number of the embedding bits, leading to good expandability in embedding capacity.

Key words: sparse decomposition; matching pursuit; genetic optimization; steganography

1 引言

目前多数的图像密写算法将秘密信息隐藏于空域或诸如离散余弦变换域、离散小波变换域等正交线性变换域中[1]。随着隐写分析的发展，这些密写方法引起的图像统计特征变化容易被察觉，因此其安全性受到了威胁。图像的稀疏表示[2,3](sparse representation)是一种新的图像表示理论。其采用原子库过完

收稿日期：2011-12-29；修回日期：2012-04-24
基金项目：国家自然科学基金项目(61171124，61103174)；广东省科技计划项目(2011B010200045)；广东省高校优秀青年创新人才基金(LYM10116)资助；深圳市重点实验室提升项目(CXB201105060068A)

备的冗余函数取代基函数,从原子库中挑选有限个原子的最佳线性组合来表示图像。基于超完备字典的图像稀疏表示因其具有稀疏性及特征保持性等特点被广泛应用于图像处理[4,5]。

本文提出一种基于图像稀疏分解的密写算法。与已有的图像密写不同,该密写算法并不将秘密信息隐藏于图像像素值、离散余弦变换系数或离散小波变换系数中,而是将秘密信息隐藏于量化后的图像稀疏分解参数中。该密写过程与基于稀疏分解的图像压缩过程合二为一。对图像进行稀疏分解,对分解得到的参数进行量化,将秘密信息采用 LSB 替换方式隐藏于量化后的参数中。为了提高嵌入容量,针对分解参数的分布特性,自适应选择不同的位数进行隐写。实验结果表明基于图像稀疏分解的密写算法具有良好的视觉隐蔽性,其嵌入容量可灵活扩充。与相同嵌入容量的 LSB(Least Significant Bit)算法相比,具有更高的抗隐写分析能力。

2 图像稀疏分解

稀疏分解目前已经出现了多种算法,例如 MP 算法、OMP 算法、BP 算法等[6-8]。其中 MP 算法最为通用。Mallat 与 Zhang[6]于 1993 年首次提出了信号稀疏分解的 MP(Matching Pursuit)算法,1995 年提出图像稀疏分解 MP 算法。图像稀疏分解 MP 算法是从超完备字典库中挑选有限个原子来表征图像,每次从超完备字典库中选择与原图像或图像残余最为逼近的原子。基于 MP 的图像稀疏分解算法过程如下:

假设图像为 f,大小为 $M_1 \times M_2$。集合 $D=\{g_\gamma:\gamma\in\Gamma\}$ 为用于图像稀疏分解的过完备库,g_r 为由参数组 γ 定义的原子。Γ 是参数组 γ 的集合。其中原子 g_r 大小与图像大小相同,所有原子进行归一化处理 $\|g_r\|=1$。基用 l 表示过完备库 D 中的原子个数,则 l 远远大于图像大小,即 $l>>M_1\times M_2$。

首先从过完备字典库中找出与待分解图像最为匹配的原子,其满足

$$|<f,g_{\gamma_0}>|=\sup_{\gamma\in\Gamma}|<f,g_\gamma>| \tag{1}$$

其中 $<f,g_{\gamma_0}>$ 为图像 f 与原子 g_{γ_0} 的内积运算。因此,图像被分解为在最佳原子的投影分量和图像残余两个部分,即:

$$f=<R^k,g_{\gamma_0}>g_{\gamma_0}+R^1f \tag{2}$$

且满足 R^1f 与 g_{γ_0} 正交,即

$$\|f\|^2=|<f,g_{\gamma_0}>|^2+\|R^1f\|^2 \tag{3}$$

对图像残余不断进行以上同样的分解过程,即

$$R^kf=<R^k,g_{\gamma_k}>g_{\gamma_k}+R^{k+1}f \tag{4}$$

其中 g_{r_k} 满足:$|<R^kf,g_{\gamma_k}>|=\sup_{\gamma\in\Gamma}|<R^kf,g_\gamma>|$ (5)

且 $\|R^kf\|^2=|<R^kf,g_{\gamma_k}>|^2+\|R^{k+1}f\|^2$ (6)

只要信号的稀疏表示跟信号的近似程度不够好,即 $\|R^kf\|^2=\|f\|^2-\sum_{m=0}^{k-1}|<R^mf,g_{\gamma_m}>|^2$ 不够小,就要对 R^kf 重复以上的分解过程,直到 $\|R^kf\|$ 足够小为止。图像经过以上操作,可采用一个线性表示:

$$f=\sum_{k=0}^{\infty}<R^kf,g_{r_k}>g_{r_k} \tag{7}$$

由于 $\|R^kf\|$ 在分解过程中具有衰减特性,因此,只用少数 n 个原子就可以近似表示图像的主要成分,从而达到图像稀疏表示的目的,即

$$f\approx\sum_{k=0}^{n-1}<R^kf,g_{r_k}>g_{r_k},\ n<<M_1\times M_2 \tag{8}$$

由于原子库中原子的个数巨大,要进行的内积计算次数非常多;此外,图像数据也是非常大,使得一次内积的计算量也相当大。因此,求解(1)(5)式代表的最优化问题是一个 NP 难问题。在实际实现该算法时,最优解问题可转化为(9)式的次优解问题。

$$|<R^kf,g_{\gamma_k}>|\geqslant\alpha\sup_{\gamma\in\Gamma}|<R^kf,g_\gamma>| \tag{9}$$

其中,$\alpha\in(0,1]$ 为最优性因子。对于(8)式,每次求解原子不是求最优原子,而改为求次优解,因此,可利用智能优化算法来求解。在图像大小有限的条件下,$\|R^kf\|$ 随着 k 的增加而指数衰减为 0。其衰减特性依赖于原子库特征和每一步分解中使用的最优化方法。文献[6]证明,图像在过完备库上的分解结果一定是稀疏的。

图像密写的主要评价指标为安全性,大多隐写分析算法都是针对图像密写引起的统计特征变化对载密图进行了分析。图像稀疏表示具有稀疏性和特征保持性[2],稀疏性是指只采用少数原子即可获得图像数据的高质量恢复,达到图像压缩的目的。特征保持性是指图像的主要特性及边缘细节等特征在图像数据的表示中予以保留,对其分解参数进行细微改变,不会引起图像统计特征改变。因此,将秘密信息隐藏于图像的稀疏分解过程中,可保持图像统计特征基本不变,从而提高图像密写的安全性。本文根据图像稀疏分解的特征保持性,提出了一种基于遗传优化图像稀疏分解

的密写算法。

3　基于遗传优化图像稀疏分解的密写算法

本文提出的基于遗传优化的图像稀疏分解密写算法,主要涉及到如何设计快速的图像稀疏分解算法、选择合适的过完备原子库、秘密信息的嵌入规则及提取等因素。

由以上分析,在给定条件下,图像在过完备原子中选择最优的原子是最优化问题,直接的求解将是一 NP 难问题。在实际应用中,通常采用智能优化算法获取满意解。遗传算法[9]是一种全局搜索优化技术。其本质是一种并行、高效、全局搜索的方法。遗传算法以达尔文的自然进化论和孟德尔的遗传变异理论为基础,通过模仿生物遗传进化过程,使用适者生存的原则,淘汰其中的劣解,保留并发展其中的优质解。遗传算法通过迭代,使整个种群的质量不断提高,当达到循环进化的收敛条件时,最终获得问题的最优解。本文采用遗传算法与 MP 算法相结合,实现在图像的过完备库中选取匹配原子,极大地减少了计算量,达到图像稀疏分解的目的。

不同的原子库对图像的稀疏表示可达到不同表示效果。非对称原子[10]在图像稀疏表示中已体现出了良好的性能。其基函数如下:

$$g(x,y)=(4x^2-2)e^{-(x^2+y^2)} \tag{10}$$

对该非对称原子旋转、平移及伸缩变换,可获得一系列原子 g_γ,从而构成原子库 $D=\{g_\gamma\}_{\gamma\in\Gamma}$。其中 $g_\gamma=g_\theta\left(\frac{x-u}{s_x},\frac{y-\nu}{s_y}\right)$,$\gamma=(\theta,u,\nu,s_x,s_y)$,$\theta,u,\nu,s_x,s_y$ 分别代表原子的旋转分量、在 x,y 方向上平移分量及在 x,y 方向上伸缩分量。基于该原子库的图像稀疏分解结果为,其中 n 为原子数:

$$\left\{(<R^kf,g_{\gamma_k}>,\theta_k,u_k,\nu_k,s_{x_k},s_{y_k})\mid k=0,1,2,\ldots,n-1\right\} \tag{11}$$

LSB(Least Significant Bit)隐写由于嵌入方式简单,嵌入容量大,是最常用的隐写算法之一。其通过用秘密信息替换载体数据最不重要比特位达到隐写目的。本文提出的遗传优化稀疏分解的图像密写算法,对图像稀疏表示的数据进行量化后,将秘密信息采用 LSB 嵌入方式隐藏于量化系数中。

基于遗传优化稀疏分解的图像密写算法:

(1)对载体图像采用非对称原子库进行稀疏分解。在基于 MP 的图像稀疏分解每步迭代中,利用遗传算法快速实现在完备原子库中选取最佳的匹配原子。其中个体(即染色体)定义为原子的参数组 $\gamma=(\theta,u,\nu,s_x,s_y)$,即优化问题的解。图像或图像残余与原子的内积绝对值 $|<R^kf,g_{\gamma_k}>|$ 作为适应度函数,适应度函数取值越大,表明该个体对应选择的原子越好。选择最佳原子的迭代过程为:

①初始化种群,计算每个个体的适应度值;

②计算所有个体的图像残余,选择出最小的图像残余值;

③对种群进行选择,交叉和变异,重新计算适应度值;

④若最小图像残余值足够小,或达到预定的进化代数,则输出最佳适应度值对应的个体,否则转②。

(2)图像稀疏分解参数量化。根据稀疏分解参数的分布范围及规律,对稀疏分解得到的参数采用不同的量化位长。其中 $|<R^kf,g_{\gamma_k}>|$ 的值变化范围较大,随着图像分解进程,其取值按指数规律衰减并趋于 0。x 和 y 方向的伸缩量取值也随着原子数增加而下降。其中平移量,旋转角度服从均匀分布,其取值范围为 1 到图像的长度或宽度。根据该分布规律,可设定 $|<R^kf,g_{\gamma_k}>|$,s_x,s_y 三个参数量化位数为 14bits,6bit 和 6bits,对于 θ_k,u_k,ν_k 三个参数量化位数统一设置为 10bits,得到量化后的稀疏分解结果。

(3)秘密信息嵌入。在图像稀疏分解的量化参数中,第一个原子由于包含图像主要信息,不嵌入信息,对于其它原子,首先通过密钥获得秘密信息嵌入顺序来提高隐写安全性。再按 LSB 替换嵌入规则,采用不同的嵌入位数,将秘密信息嵌入在量化后的参数中。将嵌入位数为一位,二位和三位的基于遗传优化稀疏分解的图像密写算法分别记为 MPLSB, MPL2SB 和 MPL3SB。

基于遗传优化稀疏分解的图像密写算法在图像稀疏分解压缩过程中完成,通过信道传递,反编码可得到量化后的参数,从而提取出秘密信息。

4　实验结果与分析

本实验从视觉效果和安全性两方面来说明基于遗传优化稀疏分解的图像密写算法的性能。

实验一为视觉失真度比较实验。选择标准图像 Lena,Boat,Elaine 及 Cameraman,裁剪为 128×128 大小,采用非对称原子库,分解原子数为 2000 个,在每个原子的 6 个参数中采用 MPLSB,MPL2SB 和 MPL3SB 嵌入

秘密信号,得到载密图像。为了在相同的嵌入容量下进行比较,以嵌入率 rate = (2000 * 6)/(128 * 128) = 0.73,对以上四幅图采用空域中的 LSB,L2SB,L3SB 三种密写方式得到载密图像,计算所有载密图像的 PSNR 值,如表 1 所示。

表 1 PSNR 值(单位:dB)

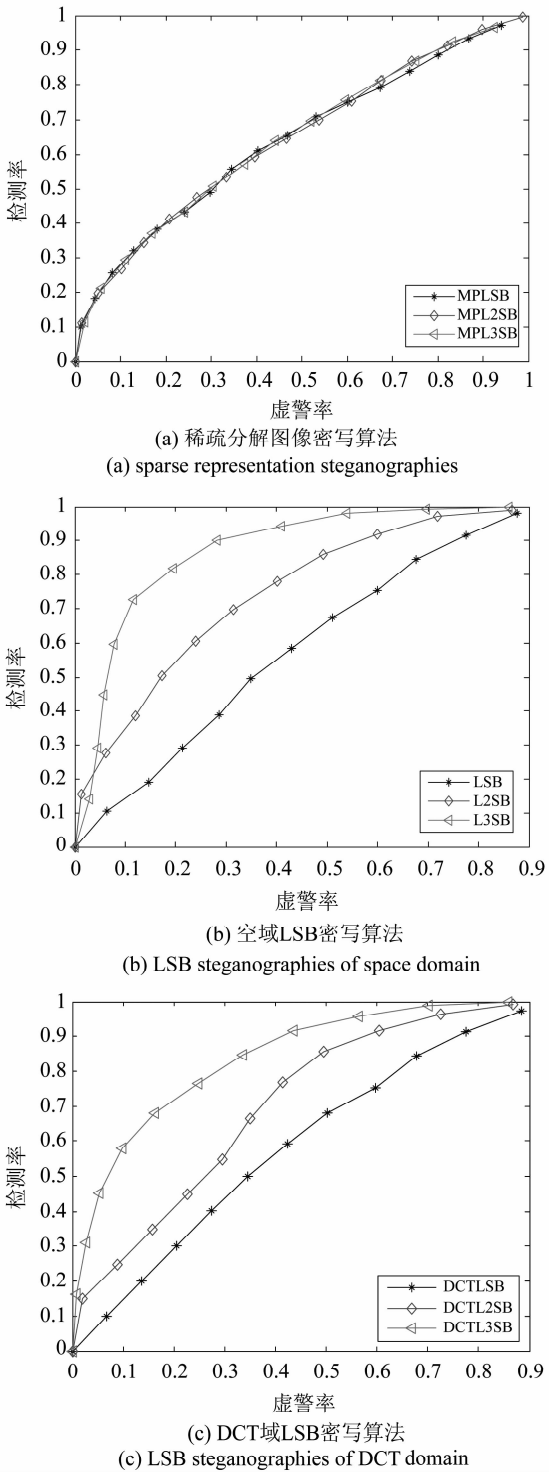
Tab. 1 The values of PSNR (unit:dB)

图像	MP-LSB	MP-L2SB	MP-L3SB	LSB	L2SB	L3SB
Lena	33.4785	33.5726	33.3892	51.1372	45.8736	39.4066
Boat	36.3817	36.2109	36.4754	51.1038	44.7837	38.2016
Elaine	34.7872	34.8234	34.7108	50.2140	43.7703	37.2568
Cameraman	37.4572	37.3481	37.4478	51.1832	46.2221	39.4358

由表 1 可知,对于本文提出的密写算法,对同一幅图像,在不同的嵌入容量下的 PSNR 值都几乎不变。而对于空域的 LSB 隐写,由于 L3SB 嵌入容量最大,其对应加密图像的 PSNR 值远低于 L2SB 和 LSB 嵌入的 PSNR 值。由图像的稀疏分解特性可知,稀疏分解的密写算法的 PSNR 取值与原子数相关,原子数越多,则 PSNR 值越大。表中所有算法的 PSNR 值均大于 33dB,满足视觉要求。

由于稀疏分解是在整幅图像上搜索最佳的原子,计算量及存储量都十分大。针对小尺寸图像,其对应的原子库规模将大幅下降[11],对应原子搜索范围大幅减小,从而达到降低计算复杂度的目的。由于实验需对图库进行密写操作,考虑计算复杂度,采用的图像不宜太大。

实验二采用本文算法与空域中的 LSB, L2SB, L3SB 密写算法及 DCT 域中密写进行安全性比较。选择 UCID. V2 图像库[12]中 1338 幅图像进行实验,所有图像转换为灰度图像并裁剪大小 128×128。原子库采用非对称原子库,分解原子数为 1000。采用 MPLSB,MPL2SB 和 MPL3SB 在图像稀疏分解的量化结果不同位上嵌入秘密信息,得到三个载密图像库。其中遗传算法的参数设置为,种群大小为 30,进化代数为 50,交叉率 0.2,变异率为 0.01。为了在相同的嵌入容量下进行比较,以嵌入率 rate = (1000×6)/(128 * 128) = 0.37,对该图库采用空域中的 LSB,L2SB,L3SB 三种密写方式进行密写,得到载密图像库。DCT 域中密写将信息分别嵌入在量化(量化步长取 75)的前 6000 个非零 DCT 系数(当不足 6000 时,则选择所有非零系数)的 LSB,L2SB,L3SB 中,再反变换得到载密图像库,三种密写方式分别记为 DCTLSB, DCTL2SB 和 DCTL3SB。图 1 图 2 分别采用 Ker 等[13]提出的质心下降隐写分析和 Shi 等[14]提出 78 维特征的隐写分析算法对以上三类密写进行隐写分析得到的 ROC (Receiver Operating Characteristic Curve, ROC)曲线。



(a) 稀疏分解图像密写算法

(a) sparse representation steganographies

(b) 空域LSB密写算法

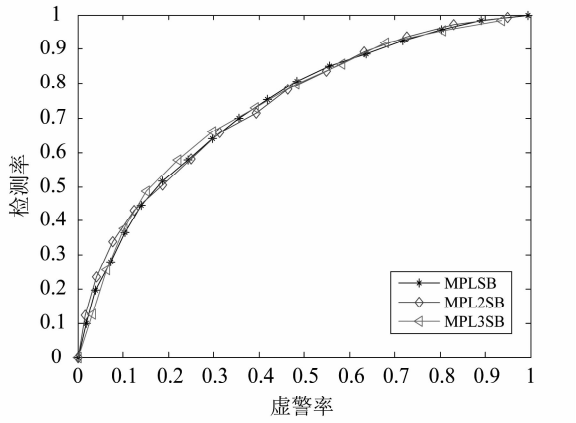
(b) LSB steganographies of space domain

(c) DCT域LSB密写算法

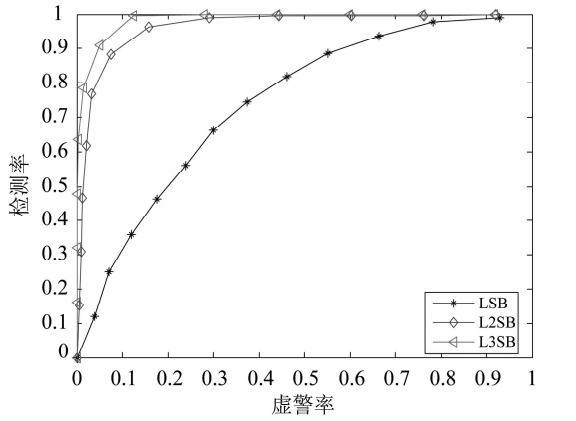
(c) LSB steganographies of DCT domain

图 1 不同密写算法抗质心特征分析 ROC 曲线图

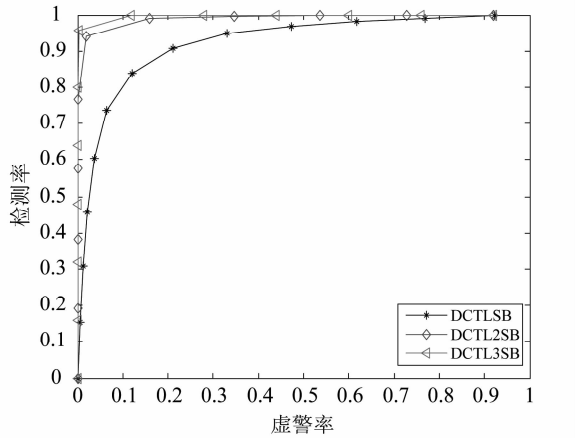
Fig. 1 The ROC curves for the center of mass feature steganalysis of different steganographies



(a) 稀疏分解图像密写算法
(a) sparse representation steganographies



(b) 空域LSB嵌入算法
(b) LSB steganographies of space domain



(c) DCT域LSB嵌入算法
(c) LSB steganographies of DCT domain

图 2　不同密写算法抗 78 维特征分析 ROC 曲线图
Fig. 2　The ROC curves for 78 dimensional features steganalysis of different steganographies

由图 1(b)(c),图 2(b)(c)针对空域及 DCT 域中三种隐写,L3SB,DCTL3SB 隐写获得了最大的 AUC 值,安全性最低,其次是 L2SB,DCTL2SB。两种隐写分析算法对于空域和频域中的 LSB 置换嵌入,当嵌入扩充至最低两位或三位时,图像的统计特征发生显著的变化,对其隐写分析的 AUC 值可达到 0.9856 和 0.9994,说明 L3SB 和 DCTL3SB 安全性很低。由图 1(a),图 2(a)可见,基于稀疏分解的图像密写,针对不同的嵌入位数 MPLSB,MPL2SB 和 MPL3SB 三种密写获得的 AUC(Area under ROC Curve,AUC)值大小相当,而且 AUC 值都低于针对 LSB 的隐写分析值,说明两种隐写分析算法均不能对本文提出的密写算法进行有效地分析,验证了本文算法的安全性。分析其原因,稀疏分解密写不同于空域或频域通过改变像素值或频域的系数值进行密写,从而引起图像统计特征的改变。稀疏分解密写将密写过程与图像的稀疏分解压缩过程合二之一,在达到图像压缩的同时保持图像的特征,有效地抵抗了目前以统计特征变化为核心的隐写分析算法。根据本文算法的抗分析特性得出,该密写算法在保证安全性的同时,嵌入容量具有可扩充性。可通过选择不同的原子库,改变嵌入位数,重提高重构图像精度(原子数的增加)等策略有效地扩大密写容量。

5　结束语

本文利用图像稀疏分解的特征保持性,将基于稀疏分解的图像压缩过程和隐写过程合二为一,在对原图的稀疏表示同时实现了秘密信息的隐藏。通过设置密钥确定嵌入顺序进一步增强算法的安全性。该密写算法易于软件和硬件实现,在保证密写安全性的同时,根据选择不同原子重构数量及嵌入位数可以灵活地扩充隐藏容量。仿真实验表明,本文提出的基于遗传优化图像稀疏分解的密写算法在保证加密图像视觉效果的同时,与空域中相同嵌入容量的 LSB 嵌入算法相比,获得了更强的抗隐写分析能力。由于选择不同的原子库及稀疏分解算法会影响到图像的重构效果,因此如何构造表示图像特征的原子库及提高稀疏分解速度以进一步提高密写图像的安全性可作为下一步的研究方向。

参考文献

[1]　张良,刘宏,吴仁彪,杨国庆. JPEG2000 小波域隐写算法[J]. 信号处理. 2007,23(1):27-30.
Zhang Liang, Liu Hong, Wu Ren-biao, Yang Guo-qing,

Wavelet Domain Steganography for JPEG2000[J]. Signal Processing. 2007,23(1):27-30. (in Chinese)

[2] 石光明,刘丹华,高大化,等. 压缩感知理论及其研究进展[J]. 电子学报,2009,37(5):1070-1081.
Shi Guang-min, Liu Dang-hua, Gao Da-hua et al. Advances in Theory and Application of Compressed Sensing [J]. Acta Electronica Sinica, 2009, 37(5): 1070-1081. (in Chinese)

[3] 朱延万,赵拥军,孙兵. 一种改进的稀疏度自适应匹配追踪算法[J]. 信号处理. 2012,28(1):80-86.
Zhu Yan-wan, Zhao Yong-jun, Sun Bing. A Modified Sparsity Adaptive Matching Pursuit Algorithm[J]. Signal Processing. 2012,28(1):80-86. (in Chinese)

[4] M. Elad, M. Aharon. Image denoising via sparse and redundant representations over learned dictionaries [J]. IEEE Transactions on Image Processing, 2006, 15(12): 3736-3745.

[5] 蔡泽民,赖剑煌. 一种基于超完备字典学习的图像去噪方法[J]. 电子学报,2009,37(2):347-350.
Cai Ze-min, Lai Jian-huang. An Over—complete Learned Dictionary-Based Image De-noising Method [J]. Acta Electronica Sinica, 2009, 37(2): 347-350. (in Chinese)

[6] S. G. Mallat, Z. Zhang. Matching pursuits with time-frequency dictionaries [J]. IEEE Transactions on Signal Processing, 1993, 41(12): 3397-3415.

[7] R. R. Coifman, M. V. Wickerhauser. Entropy-based algorithms for best basis selection, IEEE Transactions on Information Theory, 1992, 38(2): 713-718.

[8] S. S. Chen, D. L. Donoho, and M. A. Saunders. Atomic decomposition by basis pursuit[J]SIAM journal on scientific computing, 1999, 20(1): 33-61.

[9] J H. Holland. Building blocks, cohort genetic algorithms, and hyperplane-defined functions[J]. Evolutionary Computation, 2000, 8(4): 373-391.

[10] P. Vandergheynst, P. Frossard. Efficient image representation by anisotropic refinement in matching pursuit [C]. IEEE International Conference on Acoustics, Speech, and Signal processing, 2001, 3: 1757-1760.

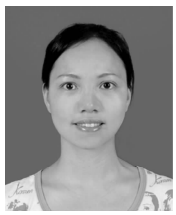
[11] 李恒建,张跃飞,王建英, 等, 分块自适应图像稀疏分解[J]. 电讯技术,2006,4:63-67.
Li Heng-jian, Zhang yue-fei, Wang Jian-yin et al. Adaptive block-based image sparse decomposition[J]Telecommunication Engineering, 2006, 4: 63-67. (in Chinese)

[12] G. Schaefer and M. Stich. UCID-an uncompressed colour image database, Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia, 2004, 5307: 472-480.

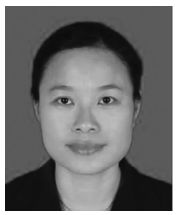
[13] A. D. Ker. Steganalysis of LSB matching in grayscale images[J]. Signal Processing Letters, 2005, 12: 441-444.

[14] G. Xuan, Y. Shi, J. Gao, D. Zou, C. Yang, Z. et al. Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions [C] Information Hiding, 7th International Workshop, 2005, 3727: 262-277.

作者简介



欧阳春娟(1974-),女,江西吉安人,深圳大学信息工程学院博士研究生,研究方向为信息隐藏、智能优化。
E-mail:oycj001@163.com



李 霞(1968-),女,四川乐山人,本文通讯作者,博士,深圳大学教授,博士生导师,研究方向为智能优化,信息安全。
E-mail:lixia@szu.edu.cn

李 斌(1982-),男,广东五华人,深圳大学讲师、博士,研究方向为信息隐藏、隐写分析。E-mail:libin@szu.edu.cn