使用 Daubechies 小波增强图像隐写安全性

郭继昌*，魏慧文，何艳红，顾翔元
天津大学电气自动化与信息工程学院，天津 300072

摘要 为了提高不同像素之间的相干性，基于最小化嵌入损失函数框架提出了一种空域图像自适应隐写算法。使用 Daubechies 小波构造滤波器预测载体图像的残差权重并获得损失值，利用均值滤波器对损失值进行平滑处理，结合校验格编码嵌入信息。使用两种不同的图像特征进行抗隐写分析，实验结果表明，当信息嵌入率较小时，所提算法的抗检测能力与 HILL(Hill-pass，Low-pass，Low-pass)隐写算法的相近，且优于其他对比算法；当信息嵌入率较大时，所提算法的抗检测能力明显优于小波获得权重法、S-UNIWARD(Spatial-Universal Wavelet Relative Distortion)等主流隐写算法。

关键词 图像处理；图像隐写；损失函数；Daubechies 小波；校验格编码
中图分类号 TP309 **文献标识码** A **doi**：10.3788/LOP56.031004

Enhancing Image Steganographic Security Using Daubechies Wavelet

Guo Jichang*, Wei Huiwen, He Yanhong, Gu Xiangyuan
School of Electrical and Information Engineering, Tianjin University, Tianjin 300072, *China*

Abstract In order to improve the coherent among different pixels, a spatial image adaptive steganography algorithm is proposed based on the framework of minimizing the embedding distortion function. The Daubechies wavelet construction filter is used to predict the residual weight of cover and the cost value is obtained. A mean filter is used to smooth the cost value. The messages combined with syndrome trellis coding are embedded. Two different image features are used for anti-steganography analysis. Experimental results demonstrate that the anti-detection ability of the proposed algorithm is similar to the Hill-pass, Low-pass, Low-pass (HILL) steganography algorithm when the payload is small and is significantly better than the mainstream steganography algorithms such as wavelet obtained weights and spatial-universal wavelet relative distortion (S-UNIWARD) when the payload is large.

Key words image processing; image steganography; cost function; Daubechies wavelets; syndrome trellis coding
OCIS codes 100.3008; 110.1085; 120.2440

1 引 言

隐写术可以通俗地理解为“囚徒问题”[1]，隐写术最重要的特点是不可检测性，其目的是使通信双方能够进行隐蔽通信，而不被其他用户察觉。图像隐写是隐写术中的一个重要分支，数字图像具有信息冗余度大的特性，是理想的秘密信息载体。

图像隐写[2-13]的性能一般可从两个方面进行评估，一是信息嵌入率，希望其尽可能大；二是图像损失，希望其尽可能小。Filler 等[14]在利用最小化加性损失设计模型[15-16]的基础上，提出一种信息嵌入的校验格编码(STC)方案，该方案能够很好地解决自适应隐写中的编码算法问题，其编码效率已接近理论上界，因此图像隐写可简化为图像损失函数设计。

在最小化损失模型的隐写框架下，设计安全性更高的自适应隐写算法成为趋势，较为成熟的自适应隐写方法主要考虑与损失分配直接相关的修改概率和嵌入位置。隐写和隐写分析[17-21]相互制约，也相互促进。Pevný 等[2]利用邻域像素差分矩阵等特

收稿日期：2018-07-30；**修回日期**：2018-08-14；**录用日期**：2018-08-17
基金项目：天津市自然科学基金(15JCYBJC15500)
* **E-mail**：jcguo@tju.edu.cn

征设计了一种高度不可检测(HUGO)自适应隐写算法，能够有效地遏制差分像素邻接矩阵(SPAM)[22]隐写分析算法，但面对更高维的富模型(SRM)[17]特征检测时，安全性能大大降低。Holub等[4]提出了小波获得权重(WOW)法，通过使用由DB-8(Daubechies 8-tap)小波构造水平、垂直以及对角方向上的滤波器组的方式设计损失函数，不仅在嵌入时间上有了很大的提升，并且对比于HUGO自适应隐写算法，其安全性能也有了明显提高。Holub等[5]又将WOW算法的思想推广到任意嵌入域，提出了UNIWARD(Universal Wavelet Relative Distortion)，尤其是在JPEG域和单边信息域中，提高了隐写算法的全能性。王龙飞等[6]利用SRM隐写分析中计算噪声残差的五阶无方向性滤波器计算载体图像残差，进而确定载体图像中纹理丰富的复杂区域，提出了一种空域自适应隐写算法。Li等[13]在WOW算法的基础上，提出了HILL(Hill-pass，Low-pass，Low-pass)隐写算法，该方案结合KB预测算子和两个均值滤波器，相较于WOW和S-UNIWARD(Spatial-UNIWARD)隐写算法，其抵抗基于SRM[17]特征的隐写分析的性能十分显著。

为进一步提高隐写的安全性，改善隐写损失函数的性能，受图像滤波处理等[23]技术的启发，在WOW算法的基础上，结合使用不同阶数Daubechies小波设计隐写损失函数。首先从Daubechies小波的构造原理入手，分析Daubechies小波对于图像纹理细节的敏感程度，在水平、垂直和对角三个方向对图像的纹理区域进行探测和提取，然后使用Hölder范数定义损失函数。当信息的嵌入率较大时，秘密信息可能会被嵌入到平滑区域，文献[11]提到使用聚焦改变位置的方式，能够有效地抑制此类情况发生。本文使用均值滤波器对损失函数进行平滑处理，并使用STC按照最终得到的各个像素的损失值在载体图像中嵌入秘密信息。通过SRM隐写分析的实验结果表明，在相同嵌入率的情况下，所提算法具有更高的安全性。

2 相关基础

2.1 WOW算法中的损失函数

Holub等[4]提出了一种利用DB-8小波设计隐写损失滤波器的方案，该方案首先使用DB-8小波构造方向滤波器组，DB-8小波系数的离散图如图1所示。

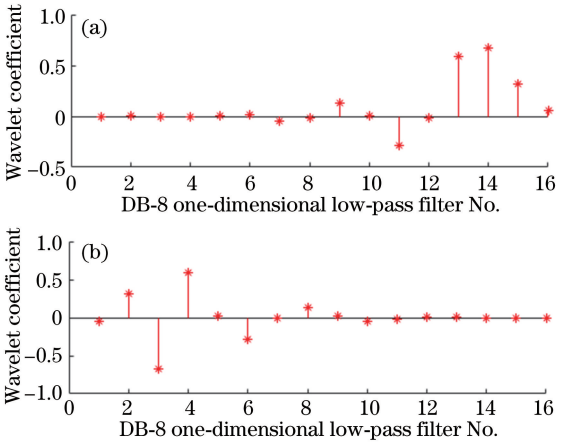

图1 DB-8小波系数。
(a)一维低通滤波系数；(b)一维高通滤波系数

Fig. 1 Coefficients of DB-8 wavelets. (a) One-dimensional low-pass filter; (b) one-dimensional high-pass filter

使用下式分别从水平、垂直、对角三个方向上提取图像的纹理特征，划定可嵌入信息的纹理复杂区域，即

$$\boldsymbol{K}^{(1)}=\boldsymbol{h}\cdot\boldsymbol{g}^{\mathrm{T}},\boldsymbol{K}^{(2)}=\boldsymbol{g}\cdot\boldsymbol{h}^{\mathrm{T}},\boldsymbol{K}^{(3)}=\boldsymbol{g}\cdot\boldsymbol{g}^{\mathrm{T}},\tag{1}$$

$$\xi_{ij}^{(k)}=\left|\boldsymbol{R}^{(k)}\right|\otimes\left|\boldsymbol{R}^{(k)}-\boldsymbol{R}_{[ij]}^{(k)}\right|^{\frown}=\left|\boldsymbol{R}^{(k)}\right|\otimes\left|\boldsymbol{K}^{(k)}\right|^{\frown},\tag{2}$$

式中：$\boldsymbol{K}^{(k)}$($k=1,2,3$)为不同方向滤波器，k取不同值表示不同方向；$\boldsymbol{h}$为一维水平方向DB-8低通滤波器；$\boldsymbol{g}$为一维水平方向DB-8高通滤波器；$\boldsymbol{g}^{\mathrm{T}}$为$\boldsymbol{g}$的转置；$\cdot$为矩阵乘法运算；$\boldsymbol{R}^{(k)}$为经过第$k$个滤波器后每个方向上的得到残差值；$\boldsymbol{R}_{[ij]}^{(k)}$表示图像的第$i$行第$j$列位置的像素经过第$k$个滤波器后得到的残差值；$\otimes$为卷积运算；$\frown$为逆时针旋转180°操作；$\xi_{ij}^{(k)}$为适合嵌入率。再使用下式的Hölder范数将上述得到的不同方向上的信息嵌入合适度合并，即：

$$\rho_{ij}^{(p)}=\left(\sum_{k=1}^{3}\left|\xi_{ij}^{(k)}\right|^{p}\right)^{-1/p},\tag{3}$$

式中$\rho_{ij}^{(p)}$表示当Hölder范数的参数设置为p时，图像第i行第j列像素的失真值。最后使用STC将秘密信息嵌入到载体图像中。

使用方向滤波器组从水平、垂直和对角三个方向对图像进行残差提取的效果图如图2所示。从图2可以看到，载体图像通过不同的方向滤波器时，得到的损失值呈现了规律变化，通过对不同方向进行滤波处理，WOW算法能够定位到水平、垂直和对角方向上均不易建模的位置，对这些位置进行信息嵌入。

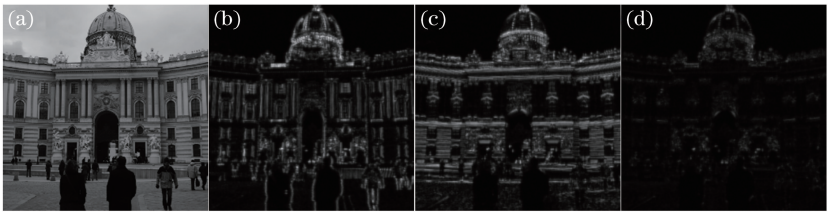

图 2 利用 WOW 算法分解载体图像的结果。(a)载体图像;(b)水平方向;(c)垂直方向;(d)对角方向

Fig. 2 Decomposition of cover image by using WOW algorithm.
(a) Cover image; (b) horizontal direction; (c) vertical direction; (d) diagonal direction

2.2 STC

STC[14]是一般隐写嵌入操作(非二进制)过程中,能够最小化嵌入损失的一种嵌入方法。在基于双卷积码的维特比算法的基础上,使用校验格编码方式嵌入信息,能够实现两元、三元甚至是多元信息的嵌入。STC 通过找到奇偶校验矩阵 $\boldsymbol{H}$ 来建立一种表示图像的网格,表达式为

$$\boldsymbol{H}=\begin{pmatrix}1&0&&&&&&&&&\\0&1&1&0&&&&&&&\\&&0&1&1&0&&&&&\\&&&&0&1&&&&&\\&&&&&&\ddots&&&&\\&&&&&&&1&0&&\\&&&&&&&0&1&1&0\end{pmatrix},\tag{4}$$

式中奇偶校验矩阵 $\boldsymbol{H}$ 由子矩阵$\hat{\boldsymbol{H}}$组合得到,其中子矩阵$\hat{\boldsymbol{H}}$表示为

$$\hat{\boldsymbol{H}}=\begin{pmatrix}1&0\\0&1\end{pmatrix},\tag{5}$$

设子矩阵$\hat{\boldsymbol{H}}$的宽和高分别为 ω 和 h,则进一步可得到相对损失 $\alpha=1/\omega$ 以及约束长度 h。校验格编码的奇偶校验矩阵由子矩阵组成($\omega+1$)列的矩阵。STC 过程如图 3 所示。

图 3 中 $p_i(i>0)$表示第 $i-1$ 列的“修剪”列以及第 i 列的初始值,m 表示待嵌入的秘密信息。和其他隐写术编码方案相比,STC 适应性更高,适用于各种加性损失的度量,可通过改变参数来调节隐写速率和嵌入效率,能满足不同需求的应用环境。再结合像素的损失值以及维特比法则找到一条距离最小的路径,即最优路径。

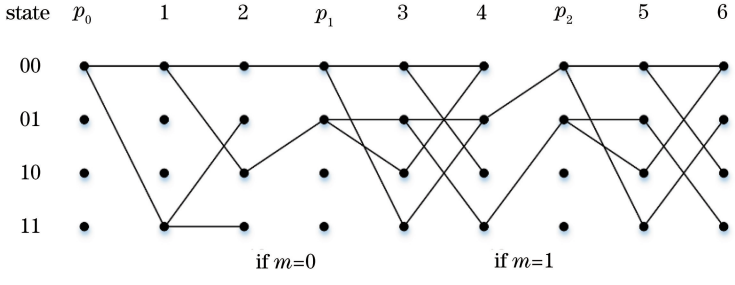

图 3 STC 过程

Fig. 3 Process of STC

3 Daubechies 小波性能分析及隐写算法设计

3.1 Daubechies 小波定义及性能分析

尺度函数是正交多分辨分析中非常重要的部分。在多分辨实例中,尺度函数往往被描述成较为简单的方式,但在一般情况下,尺度函数的构造仍然是一个困难问题。1988 年,Daubechies 等[24]给出了尺度函数的一般迭代算法,其中包含了紧支尺度函数的构造方法。设

$$H(\omega)=\frac{1}{\sqrt{2}}\sum_{n\in Z}h_n\exp(-\mathrm{i}n\omega),\tag{6}$$

是共轭滤波器,即:

$$|H(\omega)|^2+|H(\omega+\pi)|^2=1,\tag{7}$$

而且 $H(0)=1$。(6)式中 i 为虚数单位,h_n 表示小波系数序列中第 n 个值,ω 表示频率,Z 代表整数,$H(\omega)$表示滤波器的频率响应,其可以分解为

$$H(\omega)=\{[1+\exp(-\mathrm{i}\omega)]/2\}^N B(\omega),\tag{8}$$

式中 N 表示当 $\omega=\pm\pi$ 时，(8)式有 N 重根；且 $B(\omega)$ 也是一个滤波器，可以按照滤波器的形式表示为

$$B(\omega)=\sum_{r\in Z}b_r\exp(-\mathrm{i}\omega r), \tag{9}$$

且(9)式同时满足以下两个条件：1) 存在一个实数 $\varepsilon>0$，使得 $\sum_{r\in Z}|b_r|\,|r|^{\varepsilon}<+\infty$，2) 上确界 $\mathrm{Sup}\{|B(\omega)|;0\leqslant\omega\leqslant 2\pi\}<2^{N-1}$。条件 1 表示由滤波器系数 b_r 组成的滤波器 $B(\omega)$ 的脉冲响应收敛于 0 的速度比较快，ε 表示能够使条件 1 成立的实数，b_r 表示 $B(\omega)$ 的第 r 个滤波器系数；条件 2 表示 $B(\omega)$ 的幅值响应的上确界受限。

紧支撑小波的重要性是在信号的小波分解时，可提供有限数量的数字滤波器。在实际应用中，按照上述计算方法，对于任意给定的滤波器阶数，都能够计算出对应阶数的 Daubechies 小波系数值。

Daubechies 小波具有较好的正则性，即该小波作为稀疏基时，所引入的光滑误差不易被察觉，使得信号重构过程比较光滑。随着 Daubechies 小波阶数的增加，消失矩的阶数也逐渐增大，其中消失矩越高，光滑性越好，但会使时域紧支撑性减弱，计算量加大，导致实时性变差。在使用 Daubechies 小波处理图像时，能够利用上述特性，因此可将 Daubechies 小波用于自适应图像隐写的设计中。

在已有的 WOW 算法基础上，使用 Daubechies 小波系数作为构造滤波器组的一维滤波器原件，使用一维高低通滤波器组合，得到可探测三个方向的滤波器组。使用 DB-1～DB-20 小波构造滤波器嵌入图像进行对比实验，将得到的最优结果与典型隐写算法进行比较，具体的分析以及设计优化过程将在实验部分给出。构造的方向滤波器组能够从水平、垂直以及对角三个方向对原始图像进行分解，对每个方向因嵌入秘密信息造成的相对变化程度进行合并，得到损失函数。滤波器组的优势在于能从不同的方向上进行纹理分析，得到反映图像纹理复杂程度的残差图像，能够有效地抑制从单一方向进行建模的隐写分析算法的检测能力，降低了被检测出秘密信息的可能性，提高了算法的安全性。将 Bossbase1.01 数据库中的 1013.pgm 灰度图像经过本文算法的滤波器组后，得到三个方向残差图像，如图 4 所示，其中图 4(a)为载体图像，图 4(b)～(d)分别为载体图像通过水平、垂直以及对角方向之后得到的残差图像。

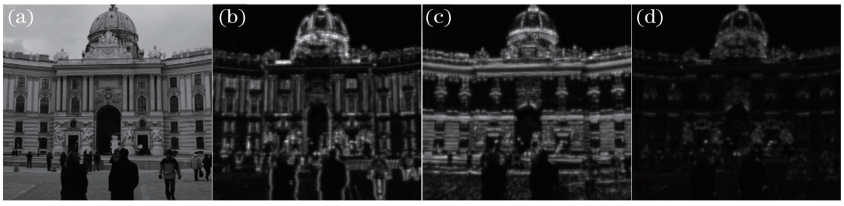

图 4 使用所提算法分解载体图像的结果。(a)载体图像；(b)水平方向；(c)垂直方向；(d)对角方向

Fig. 4 Decomposition of cover image by using proposed algorithm. (a) Cover image; (b) horizontal direction; (c) vertical direction; (d) diagonal direction

3.2 算法设计

虽然在 UNIWARD 算法[5]的文献中曾经提到过使用 Daubechies 2-tap、Daubechies 4-tap、Daubechies 8-tap 以及 Daubechies 20-tap，并未发现预期实验结果，此后也没有深入研究。文献[4]中算法通过使用 DB-8 小波从三个方向上构建了滤波器组，在水平、垂直以及对角方向的纹理成分复杂、建模较困难的区域嵌入秘密信息。使用不同阶数的 Daubechies 小波设计构造滤波器组，在三个方向上分析图像的纹理复杂度，在纹理丰富的区域进行信息嵌入。所提算法的设计流程如下：

1) 给定一个阶数 M，利用 3.1 节的 Daubechies 小波公式，再结合组合公式：

$$\sum_{j=0}^{u}C_{M+j}^{u}=C_{M+u+1}^{u}, \tag{10}$$

以及复数和三角函数等运算，化简可得到：

$$|Q[\exp(-\mathrm{i}\omega)]|^2=P\left[\sin^2\left(\frac{\omega}{2}\right)\right]。 \tag{11}$$

(10)式等号左边为从 $M+j$ 个目标中选取 u 个目标组合的数目，计算 j 从 0～u 的组合数的和，等号右边为从 $M+u+1$ 个目标中选取 u 个目标组合的数目，(11)式中 Q 为构造的实系数多项式，P 为满足 $H(\omega)$ 的有限共轭滤波器条件的实系数多项式，求解(11)式可得对应阶数的高低通滤波器系数。

2) 将小波系数按照水平、垂直以及对角方向构建滤波器组，计算残差以及信息嵌入匹配度，信息嵌入匹配度表示为

$$\xi_{ab}^{(s)}=|\boldsymbol{X}\otimes\boldsymbol{F}^{(s)}|\otimes|\boldsymbol{F}^{(s)}|^{\frown}, \tag{12}$$

式中 $\boldsymbol{X}$ 代表载体图像，$\boldsymbol{F}^{(s)}$ 代表方向滤波器，s 可以取值 1、2 和 3，$\boldsymbol{F}^{(1)}$ 表示使用 Daubechies 小波从水平方向上构造的高通滤波器，与载体图像 $\boldsymbol{X}$ 卷积后，可得到水平方向上残差的变化，而 $\frown$ 表示将第 s 个滤波器逆时针旋转 180°，即将反方向上的变化也考虑在内。同理，s 取值为 2 和 3，分别表示在垂直以及对角方向上做相同处理。最后可得到第 a 行第 b 列元素在三个方向上的适合嵌入信息的匹配度 $\xi_{ab}^{(s)}$。

3）使用 Hölder 范数将水平、垂直以及对角方向上的信息嵌入匹配度进行合并，得到损失函数，还增加了对 Hölder 范数参数 p 的实验改进：

$$\rho_{ab}^{(p)}=\left(\sum_{s=1}^{3}\left|\xi_{ab}^{(s)}\right|^{p}\right)^{-1/p},\ (p<0), \tag{13}$$

式中 $\rho_{ab}^{(p)}$ 表示当 Hölder 范数的参数设置为 p 时，图像第 a 行第 b 列像素的失真值。

4）为了防止信息嵌入到平滑区域，对已定义的损失函数进行优化，使用均值滤波器对图像的损失进行平滑，以提高隐写安全性。

5）使用 STC 按照步骤 4）得到的最终图像损失值将秘密信息嵌入。

4 实验分析

实验分为三个部分，分别是 Daubechies 小波阶数选取、实验参数确定、算法安全性对比。

计算机配置为 Intel Core i3 2.39G CPU，8.00 GB RAM，实验的软件环境为 MATLAB R2016a。安全性实验采用的数据集为 BOSSbass1.01（10000 张图）[25]，使用隐写算法对图片逐一进行秘密信息嵌入，隐写分析则是借助集成分类器[26]对载密图像的 SRM 特征（34671 维）[17]和 SRMQ1 特征（12753 维）[17]进行分类判定，根据分类判定结果的准确性，得到对应隐写算法的安全性能。由于集成分类器是采用随机森林的方式设计的，具有随机性，因此程序采用默认的 10 次运行结果。二分类集成分类器是最小化同等先验概率下分类错误 P_{E} 之和，即：

$$P_{\mathrm{E}}=\min_{P_{\mathrm{FA}}}\frac{1}{2}(P_{\mathrm{FA}}+P_{\mathrm{MD}}), \tag{14}$$

式中 P_{FA} 和 P_{MD} 分别表示错检率和漏检率。集成分类器会默认将输入的特征随机地分成两组，一组用于训练，另一组则用于预测。

4.1 Daubechies 小波阶数选取

为获得安全性较高的 Daubechies 小波阶数，分别使用 DB-1～DB-20 小波系数构建方向滤波器组，在嵌入率依次为 0.05、0.10、0.20、0.30、0.40、0.50 bit/pixel 时，在载体图像中嵌入随机秘密信息，由于提取 34671 维的 SRM 特征以及 12753 维的 SRMQ1 特征耗时较长，在对比不同阶数 Daubechies 小波安全性的实验中，只对 BOSSbase1.01 的前 2000 张图像进行实验，得到如图 5 所示的实验结果。

由图 5 可知，在嵌入率较低（0.05 bit/pixel、0.10 bit/pixel）时，分别提取 SRM 特征和 SRMQ1 特征进行分类隐写分析，安全性使用 E_{OOB}["out-of-bag"(OOB) error]来度量，这是一种在使用图像源过程中对平均误差的一种无偏估计。E_{OOB} 的峰值会在 Daubechies 小波阶数较小的情况下出现，但随着嵌入率的增大，E_{OOB} 的峰值会适当后移并逐渐稳定在 Daubechies 11-tap 附近；并且在嵌入率为 0.05～0.50 bit/pixel 的所有图像中，E_{OOB} 均呈现了相似的变化趋势，随着 Daubechies 小波阶数增加，E_{OOB} 的值会先迅速增加，达到峰值后，再缓慢减小。综合上述 6 种嵌入率的情况，选取使用 Daubechies 11-tap 小波系数作为构建方向滤波器的原件。

4.2 实验参数的确定

自适应隐写的意义在于，隐写算法能够根据图像本身内容的不同，智能地选取信息的嵌入位置以及设置相应位置的像素变化程度。当信息的嵌入率较大或图像本身的内容较为平坦时，信息极有可能嵌入到容易建模的区域。为了防止上述情况发生，同时减少噪声对分析图像纹理区域的干扰，在得到的图像损失值后，增添了均值滤波器，能够在很大程度上抑制孤立点的影响，提高信息嵌入的安全性。使用阶数为 1×1、3×3、…、19×19 阶的均值滤波器对嵌入损失值进行平滑。在嵌入率为 0.40 bits/pixel 时，隐写安全性的变化如表 1 所示。

如表 1 所示，在对载密图像利用 SRM 特征以及 SRMQ1 特征分类的情况下，所提算法与 17×17 均值滤波器配合使用时效果最佳，在嵌入率为 0.40 bit/pixel的情况下，针对载密图像的 SRM 特征安全性能提升 0.39%～1.78%，SRMQ1 特征安全性能提升 0.25%～1.26%。

在文献[4]中，当 Hölder 范数的参数 $p=-1$ 时，文献[4]中算法的安全性能为最佳，但不具有普适性，针对 Hölder 范数，进行了参数优化实验。在嵌入率为 0.40 bit/pixel 的情况下，使用 Daubechies 11-tap 小波构建滤波器组，进行信息嵌入实验后，利用 SRM 特征和 SRMQ1 特征进行隐写分析的结果如图 6 所示。

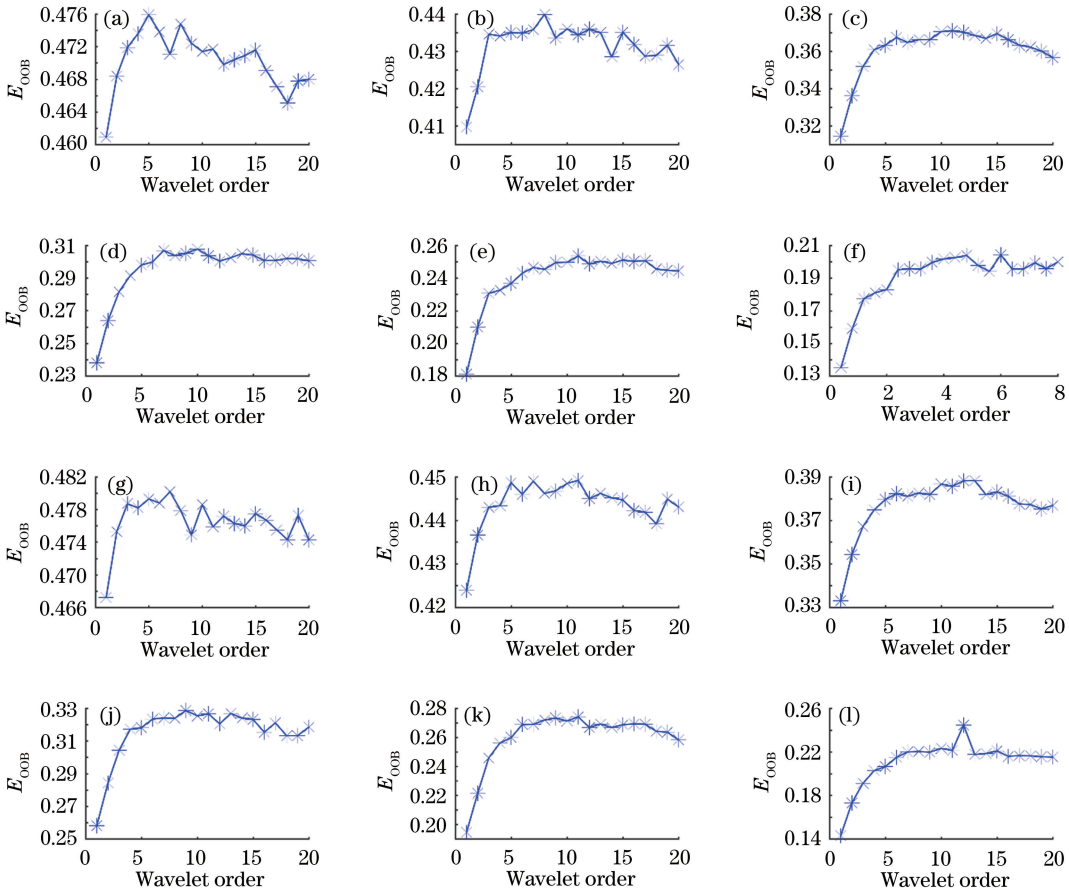

图 5 不同嵌入率下使用 Daubechies 小波的安全性能比较。(a) SRM-0.05 bit/pixel;(b) SRM-0.1 bit/pixel;(c) SRM-0.2 bit/pixel;(d) SRM-0.3 bit/pixel;(e) SRM-0.4 bit/pixel;(f) SRM-0.5 bit/pixel;(g) SRMQ1-0.05 bit/pixel;(h) SRMQ1-0.1 bit/pixel;(i) SRMQ1-0.2 bit/pixel;(j) SRMQ1-0.3 bit/pixel;(k) SRMQ1-0.4 bit/pixel;(l) SRMQ1-0.5 bit/pixel

Fig. 5 Comparison of security performance using Daubechies wavelets under different embedding rates. (a) SRM-0.05 bit/pixel; (b) SRM-0.1 bit/pixel; (c) SRM-0.2 bit/pixel; (d) SRM-0.3 bit/pixel; (e) SRM-0.4 bit/pixel; (f) SRM-0.5 bit/pixel; (g) SRMQ1-0.05 bit/pixel; (h) SRMQ1-0.1 bit/pixel; (i) SRMQ1-0.2 bit/pixel; (j) SRMQ1-0.3 bit/pixel; (k) SRMQ1-0.4 bit/pixel; (l) SRMQ1-0.5 bit/pixel

表 1 不同阶数均值滤波器的实验结果

Table 1 Experimental results of different orders′ filter

Filter order	SRM /E_{OOB}	SRMQ1 /E_{OOB}
1×1	0.2093±0.0044	0.2279±0.0037
3×3	0.2132±0.0044	0.2304±0.0020
5×5	0.2182±0.0045	0.2336±0.0034
7×7	0.2198±0.0037	0.2356±0.0048
9×9	0.2220±0.0030	0.2371±0.0045
11×11	0.2241±0.0026	0.2399±0.0033
13×13	0.2247±0.0039	0.2400±0.0029
15×15	0.2255±0.0043	0.2405±0.0038
17×17	0.2271±0.0037	0.2401±0.0033
19×19	0.2262±0.0032	0.2397±0.0033
21×21	0.2260±0.0039	0.2400±0.0029

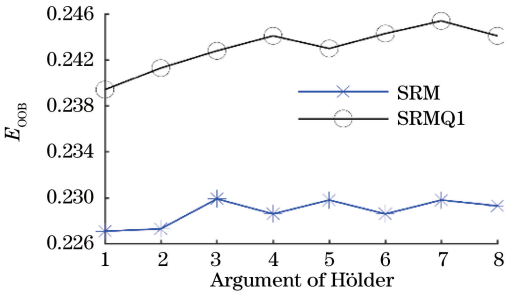

图 6 Hölder 范数参数的安全性

Fig. 6 Security of Hölder norm parameters

图 6 中，横坐标表示 Hölder 范数中参数 p 的相反数。由图 6 可知，随着参数 p 从 -1 到 -8 变化，SRM特征的曲线会在 $p=-3$ 时，检测错误率的值趋于平稳，而 SRMQ1 特征的曲线在 $p=-7$ 时取极大值，故选取参数 $p=-7$ 作为 Hölder 范数的参数。

4.3 实验安全性对比

使用 BOSSbase1.01 图像集中的 10000 张灰度图像作为载体图像，将所提算法与 HUGO-DB、WOW、S-UNIWARD、无方向性滤波器（non-directional F）以及 HILL 等典型的隐写算法进行对比实验，在嵌入率依次为 0.05、0.10、0.20、0.30、0.40、0.50 bit/pixel 时，使用集成分类器分别对使用上述隐写算法得到的载密图像的 SRM 特征和 SRMQ1 特征进行隐写分析，实验数据以及数据变化如表 2、3 以及图 7 所示。

表 2 使用 SRM 特征得到的实验结果

Table 2 Experimental results under SRM characteristics

Embedding rate /(bit·pixel^{-1})	HUGO-DB / E_{OOB}	WOW / E_{OOB}	S-UNIWARD / E_{OOB}	Non-directional F / E_{OOB}	HILL / E_{OOB}	Proposed / E_{OOB}
0.05	0.4255±0.0016	0.4547±0.0019	0.4521±0.0017	0.4449±0.0025	0.4657±0.0029	0.4640±0.0021
0.10	0.3716±0.0023	0.4042±0.0036	0.4006±0.0024	0.3962±0.0034	0.4259±0.0032	0.4232±0.0039
0.20	0.2871±0.0026	0.3182±0.0027	0.3175±0.0031	0.3107±0.0030	0.3539±0.0035	0.3426±0.0033
0.30	0.2255±0.0037	0.2556±0.0032	0.2565±0.0044	0.2574±0.0045	0.2970±0.0041	0.2796±0.0024
0.40	0.1796±0.0025	0.2084±0.0043	0.2037±0.0033	0.2067±0.0041	0.2427±0.0039	0.2298±0.0031
0.50	0.1450±0.0033	0.1665±0.0041	0.1631±0.0031	0.1692±0.0029	0.1996±0.0033	0.1879±0.0025

表 3 使用 SRMQ1 特征得到的实验结果

Table 3 Experimental results under SRMQ1 characteristics

Embedding rate / (bit·pixel^{-1})	HUGO-DB / E_{OOB}	WOW / E_{OOB}	S-UNIWARD / E_{OOB}	Non-directional F / E_{OOB}	HILL / E_{OOB}	Proposed / E_{OOB}
0.05	0.4356±0.0021	0.4630±0.0028	0.4546±0.0024	0.4455±0.0023	0.4674±0.0018	0.4670±0.0008
0.10	0.3769±0.0031	0.4183±0.0044	0.4069±0.0019	0.3969±0.0025	0.4337±0.0020	0.4310±0.0033
0.20	0.2967±0.0025	0.3402±0.0019	0.3287±0.0047	0.3248±0.0035	0.3660±0.0023	0.3580±0.0020
0.30	0.2361±0.0036	0.2772±0.0034	0.2657±0.0032	0.2694±0.0031	0.3092±0.0028	0.2967±0.0024
0.40	0.1949±0.0036	0.2289±0.0041	0.2168±0.0040	0.2254±0.0042	0.2582±0.0035	0.2454±0.0037
0.50	0.1538±0.0026	0.1864±0.0037	0.1734±0.0025	0.1833±0.0038	0.2145±0.0044	0.2009±0.0035

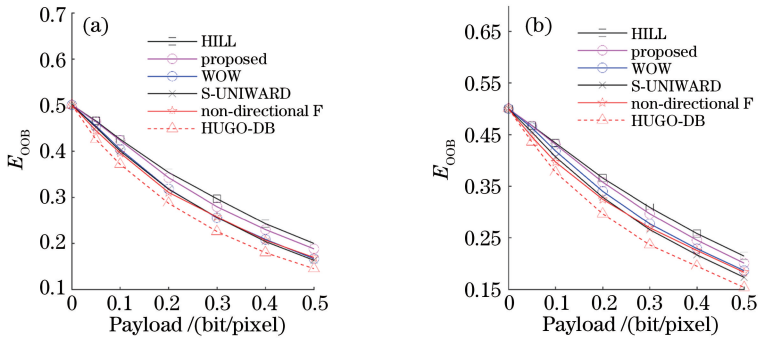

图 7 所提算法与其他典型隐写算法的安全性对比。(a) SRM 特征；(b) SRMQ1 特征

Fig. 7 Experimental results of proposed algorithm and other famous steganographic algorithms. (a) SRM features; (b) SRMQ1 features

图 7 将提取载密图像的 SRM 特征和 SRMQ1 特征作为评判标准，使用集成分类器对比分析本文算法以及 5 种典型空域隐写算法得到的实验结果。结合图 7(a)和(b)，在小嵌入率(0.05 bit/pixel、0.10 bit/pixel)时，所提算法的安全性十分接近 HILL 算法，明显优于其他算法；当嵌入率较大时，所提算法也存在很大的优势，使用 SRM 和 SRMQ1 特征作为隐写分析的特征集，所提算法与 HUGO、WOW、S-UNIWARD 以及 non-directional F 等算法相比，安全性优势明显。分析其原因，Daubechies 11-tap 小波能够获取到更加广泛的图像区域，加之均值滤波器的使用，可大大减少秘密信息被嵌入到平滑区域的可能性，有利于算法安全性能的提升。

5 结　　论

在 WOW 算法的理论基础上，结合用于图像纹理分析的 Daubechies 小波，提出了一种空域图像隐写算法。通过分析 DB-1～DB-20 小波作为构造方向滤波器组的基本原件时载密图像的安全性变化，选取综合安全性最高的 Daubechies 11-tap 小波，能够在极大程度上抑制从单一方向隐写分析建模的可能性；并使用均值滤波器平滑处理损失值，同时也对滤波器尺寸以及 Hölder 范数的参数进行优化，得到最终的隐写方案。分别使用 SRM 和 SRMQ1 两种图像特征进行抗隐写分析实验。研究结果表明，在同等信息嵌入率下，所提算法的安全性明显优于 WOW、S-UNIWARD、non-directional F 以及 HUGO 隐写算法，但相较于 HILL 算法，在抗检测性能上还存在一定差距，未来可考虑结合提取图像纹理特征更为精确的方式提高算法安全性。

参 考 文 献

[1] Li B, He J H, Huang J W, *et al*. A survey on image steganography and steganalysis [J]. Journal of Information Hiding and Multimedia Signal Processing, 2011, 2(2): 142-172.

[2] Pevný T, Filler T, Bas P. Using high-dimensional image models to perform highly undetectable steganography [C] // International Conference on Information Hiding, 2010: 161-177.

[3] Zhou W B, Zhang W M, Yu N H. A new rule for cost reassignment in adaptive steganography [J]. IEEE Transactions on Information Forensics and Security, 2017, 12(11): 2654-2667.

[4] Holub V, Fridrich J. Designing steganographic distortion using directional filters [C] // IEEE International Workshop on Information Forensics and Security, 2012: 234-239.

[5] Holub V, Fridrich J, Denemark T. Universal distortion function for steganography in an arbitrary domain [J]. EURASIP Journal on Information Security, 2014, 2014: 1.

[6] Wang L F, Guo J C, Tian Y H. Spatial adaptive steganography based on non-directional filter [J]. Laser & Optoelectronics Progress, 2017, 54(2): 021003.
王龙飞, 郭继昌, 田煜衡. 基于无方向性滤波器的空域自适应隐写算法[J]. 激光与光电子学进展, 2017, 54(2): 021003.

[7] Tang W X, Tan S Q, Li B, *et al*. Automatic steganographic distortion learning using a generative adversarial network [J]. IEEE Signal Processing Letters, 2017, 24(10): 1547-1551.

[8] Li B, Tan S Q, Wang M, *et al*. Investigation on cost assignment in spatial image steganography[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(8): 1264-1277.

[9] Sedighi V, Fridrich J, Cogranne R. Content-adaptive pentary steganography using the multivariate generalized Gaussian cover model[J]. Proceedings of SPIE, 2015, 9409: 94090H.

[10] Sedighi V, Cogranne R, Fridrich J. Content-adaptive steganography by minimizing statistical detectability [J]. IEEE Transactions on Information Forensics and Security, 2016, 11(2): 221-234.

[11] Li B, Wang M, Li X L, *et al*. A strategy of clustering modification directions in spatial image steganography[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(9): 1905-1917.

[12] Denemark T, Fridrich J. Improving steganographic security by synchronizing the selection channel[C] // ACM Workshop on Information Hiding and Multimedia Security, 2015: 5-14.

[13] Li B, Wang M, Huang J W, *et al*. A new cost function for spatial image steganography[C] // IEEE International Conference on Image Processing, 2014: 4206-4210.

[14] Filler T, Judas J, Fridrich J. Minimizing additive distortion in steganography using syndrome-trellis codes [J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 920-935.

[15] Xu G S, Wu H Z, Shi Y Q. Structural design of convolutional neural networks for steganalysis [J].

IEEE Signal Processing Letters, 2016, 23(5): 708-712.

[16] Fridrich J, Filler T. Practical methods for minimizing embedding impact in steganography[J]. Proceedings of SPIE, 2007, 6505: 650502.

[17] Fridrich J, Kodovsky J. Rich models for steganalysis of digital images [J]. IEEE Transactionson Information Forensics and Security, 2012, 7(3): 868-882.

[18] Ye J, Ni J Q, Yi Y. Deep learning hierarchical representations for image steganalysis [J]. IEEE Transactions on Information Forensics and Security, 2017, 12(11): 2545-2557.

[19] Tang W, Li H, Luo W. Adaptive steganalysis against WOW embedding algorithm [C] // ACM Workshop on Information Hiding and Multimedia Security, 2014: 91-96.

[20] Xu G. Deep convolutional neural network to detect J-UNIWARD[C] // ACM Workshop on Information Hiding and Multimedia Security, 2017: 67-73.

[21] Li J, Chen S J, Lei M, *et al*. A fully optical method for compressive optical image hiding[J]. Acta Optica Sinica, 2017, 37(11): 1110003.
李军, 陈思佳, 雷苗, 等. 全光学压缩光学图像隐藏技术[J]. 光学学报, 2017, 37(11): 1110003.

[22] Pevny T, Bas P, Fridrich J. Steganalysis by subtractive pixel adjacency matrix [J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2): 215-224.

[23] Wang Z J, Yu Z J, Ma K, *et al*. An image filtering algorithm based on adaptive median and gradient inverse weight [J]. Laser & Optoelectronics Progress, 2017, 54(12): 121001.
王志军, 于之靖, 马凯, 等. 一种自适应中值梯度倒数加权的图像滤波算法[J]. 激光与光电子学进展, 2017, 54(12): 121001.

[24] Daubechies I. Orthonormal bases of compactly supported wavelets[J]. Communications on Pure and Applied Mathematics, 1988, 41(7): 909-996.

[25] Bas P, Filler T, Pevný T. "Break our steganographic system": the ins and outs of organizing BOSS[M]. Heidelberg: Springer, 2011: 59-70.

[26] Kodovsky J, Fridrich J, Holub V. Ensemble classifiers for steganalysis of digital media[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 432-444.