DOI:10.11918/j.issn.0367-6234.201608069

利用 Gabor 小波的空域自适应隐写算法

王龙飞，郭继昌

（天津大学 电子信息工程学院，天津 300072）

摘 要：为改善利用方向性滤波器获取载体图像纹理区域的性能，进一步提升隐写算法的抗检测能力，将 Gabor 小波应用到隐写算法中，在 WOW 算法基础上提出一种空域自适应隐写算法. 首先利用 Gabor 小波构造的方向性滤波器组分别从 8 个方向对载体图像进行残差权重预测，并以 Hölder 范数形式定义损失函数，然后利用均值滤波器对所得损失函数进行滤波处理得到新的损失函数，最后通过校验格编码按照最终得到的损失函数在载体图像中嵌入秘密信息. 抵抗富模型检测实验结果表明，同等水平的信息嵌入率下，所提算法的安全性能优于同类隐写算法.

关键词：Gabor 小波；方向性滤波器组；自适应隐写；损失函数

中图分类号： **文献标志码**：A **文章编号**：0367-6234(2017)05-0073-07

Spatial adaptive steganography based on Gabor wavelet

WANG Longfei, GUO Jichang

(School of Electronic Information Engineering, Tianjin University, Tianjin 300072, China)

Abstract: Aiming at improving the performance of obtaining texture regions by directional filters and achieving better steganography security, a novel adaptive steganographic algorithm is proposed based on WOW algorithm and Gabor wavelet. Firstly, a directional filter bank is established by Gabor wavelet and then the residual weights are determined by this bank from 8 directions. Then the cost function is defined based on Hölder norm, and is updated by convolution with an average filter. Finnally, secret messages are embedded by syndrome trellis codes according to the cost function. Experimental results illustrate that the presented steganographic algorithm achieves a better performance on resisting the Spatial Rich Mode steganalysis than that of the same kind of steganographic algorithms under the same secret message payload.

Keywords: Gabor wavelet; directional filter bank; adaptive steganographic algorithm; cost function

随着互联网技术的飞速发展，信息传递变得越来越方便、快捷. 在享受科技进步带来便利的同时，信息安全隐患问题也应当引起注意，如被传递信息的非法窃取、恶意篡改甚至破坏.

隐写是一种信息隐藏技术，旨在利用数字形式的媒介(视频、音频、图像等)实现秘密信息的安全传送. 通常情况下，优秀的图像隐写算法应具有两个特性：首先允许载体图像中被嵌入足够量的秘密信息，其次保证载密图像的抗隐写分析能力在可接受范围内. 然而，在实际的隐写算法设计过程中，这两种需求是相互矛盾的，设计者在算法设计时，通常会在秘密信息嵌入率固定的条件下，设法提高隐写算法的抗检测性能. 在现代隐写技术的发展过程中，最小化所有用于信息加密像素的损失和[1]被证明是一种可行的隐写设计方法. 在这种思路框架下，设计者们提出了一系列行之有效的隐写算法[2-8]，这些算法的设计过程可以归结为两步：首先以最小加性失真模型为基础确定出损失函数，用于计算嵌入秘密信息造成的像素损失和；然后根据损失函数进行隐写编码嵌入信息. Filler 等[9]在最小化加性失真模型的框架下提出一种校验格编码方法 STC (syndrome trellis coding)，并给出证明，按照设计者自定义的损失函数，使用 STC 编码时的编码效率可以接近理论上限，STC 编码技术的提出将隐写算法设计简化到了损失函数设计上. Holub 等[5]利用 DB-8 小波构造的方向性滤波器组设计损失函数，提出应用于空间域的隐写算法 WOW (Wavelet Obtained Weights)，之后又将 WOW 算法从空间域推广到了任意域，提出 UNIWARD (UNIversal WAvelet Relative Distortion)算法[7]. 空域 UNIWARD 算法与 WOW 算法在损失函数上仅相差一个常数，两种算法在空域富模型 SRM (spatial rich models) [10]下的抗检测性能基本一致. LiBin 等利用 KB 预测算子[11]与两个均值滤波器设计损失函数，提出 HILL (high-pass, low-pass, low-pass)算法[8]. 以上提到的三种算法都是当今主流的隐写算法，其中，HILL 算

收稿日期：2016-08-19
基金项目：天津市自然科学基金(15JCYBJC15500)
作者简介：王龙飞(1989—)，男，硕士研究生；
郭继昌(1966—)，男，教授，博士生导师
通信作者：郭继昌，jcguo@tju.edu.cn

法拥有最强的抗富模型检测能力.

为改善利用方向性滤波器获取载体图像纹理区域的性能,提升隐写算法的安全性能,在 WOW 算法模型的基础上,本文提出一种利用 Gabor 小波设计的空域自适应隐写算法. 首先利用 Gabor 小波构造的方向性滤波器组分别从 8 个方向对载体图像进行残差权重预测,获取载体图像纹理丰富区域,并以 Hölder 范数形式定义损失函数;然后利用均值滤波器对所得损失函数进行滤波处理得到新的损失函数;最后通过 STC 编码按照最终得到的损失函数在载体图像中嵌入秘密信息. 抵抗富模型检测实验结果表明,同等水平的信息嵌入率下,所提算法的安全性能优于同类隐写算法.

1 相关基础

1.1 WOW 算法的损失函数

WOW 算法[5] 中的损失函数由 Daubechies 8-tap (DB-8)小波构成的方向性滤波器组设计得到. 首先利用 DB-8 小波预测载体图像的残差权重,找到合适的信息嵌入位置 $\xi_{ij}^{(k)}$:

$$\xi_{ij}^{(k)} = |X \otimes K^{(k)}| \otimes |R(K^{(k)})|.$$

式中: X 为载体图像,$K^{(k)}$ 为 DB-8 构成的方向性滤波器组 ($k = 1,2,3$), R 表示将 $K^{(k)}$ 翻转 180°. 然后将 $\xi_{ij}^{(k)}$ 以 Hölder 范数形式构造成损失函数 ρ:

$$\rho_{ij} = \left(\sum\nolimits_{k=1}^{3} |\xi_{ij}^{(k)}|^p \right)^{-\frac{1}{p}},$$

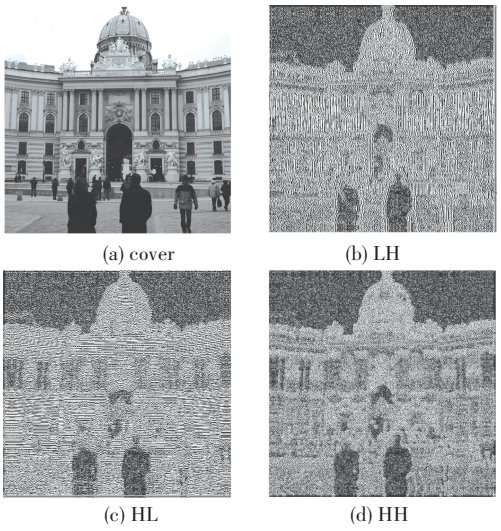
式中 p 在 WOW 算法中的取值为-1.

通过 DB-8 小波对载体图像 LH,HL,HH 这 3 个方向进行残差权重预测,WOW 算法可以利用 STC 编码将秘密信息嵌入到从 LH,HL 和 HH 方向中任一方向都难以建模分析的纹理复杂区域. 利用 WOW 算法加密时,对一张载体图像的 3 方向分解如图 1 所示,其中图 1(a)为载体图像,图 1(b)、(c)、(d)为 DB-8 小波对载体的 3 方向分解.

1.2 校验格编码技术

STC[9] 是一种特殊的应用于隐写技术中的矩阵编码,在损失函数确定的情况下,它可以将最小化嵌入失真问题转化为寻找最短路径问题,后者可以通过维特比译码快速得到.

假设载体图像为 x,载密图像为 y,秘密信息为 m, 则使用 STC 编码嵌入信息时,三者间应满足 $\boldsymbol{H}\boldsymbol{y}^{\mathrm{T}} = m$ 的关系, 式中 $\boldsymbol{H}$ 为稀疏奇偶校验矩阵,由若干个大小为 $h \times w$ 的 $\hat{\boldsymbol{H}}$ 以行为单位从上到下依次向下平移构成, $\hat{\boldsymbol{H}}$ 根据共享密钥随机生成, 其参数 h(通常情况下,$h \subseteq [6,15]$) 将会影响到编码的速度和效率. 参数 w 将影响编码嵌入效率,并且与信息嵌入率 α 有如下关系: $w = 1/\alpha$. 下面是一个由 $\hat{\boldsymbol{H}}$ 构成 $\boldsymbol{H}$ 的示例.



(a) cover (b) LH (c) HL (d) HH

图 1 DB-8 小波对载体图像的 3 方向分解

Fig.1 3 direction decompositions of cover image using DB-8 wavelet

假设 $\hat{\boldsymbol{H}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, 则

$$\boldsymbol{H} = \begin{Bmatrix} 1 & 0 & & & & & & & & \\ 0 & 1 & 1 & 0 & & & & & & \\ & & 0 & 1 & 1 & 0 & & & & \\ & & & & 0 & 1 & \cdots & & & \\ & & & & & & & 1 & 0 & \\ & & & & & & & 0 & 1 & 1 & 0 \end{Bmatrix}.$$

根据公式 $\boldsymbol{H}\boldsymbol{y}^{\mathrm{T}} = m$, 秘密信息接收者可以方便地计算出被发送的信息.

2 基于 Gabor 小波的空域自适应隐写算法

2.1 Gabor 小波

在图像处理中,Gabor 小波滤波器是一个用于边缘提取的线性滤波器,其频率和方向表达同人类视觉系统类似. Gabor 小波十分适合纹理表达和分离[12], 且现在已有大量成功应用于模式识别的案例[13-15].

在空间域中,二维 Gabor 小波函数是由正弦平面波调制的高斯核函数,即

$$G(x,y) = \frac{f^2}{\pi\gamma\eta}\exp(-(\alpha^2 x_1^{\ 2} + \beta^2 y_1^{\ 2}))\exp(\mathrm{j}2\pi f x_1),$$

$$x_1 = x\cos\theta + y\sin\theta,$$

$$y_1 = -x\sin\theta + y\cos\theta.$$

式中: f 为正弦平面波的中心频率; θ 为高斯函数逆时针旋转的角度; γ 和 η 控制高斯函数的频率和锐度,且 $\alpha = f/\gamma, \beta = f/\eta$.

本文尝试将 Gabor 小波应用于隐写算法设计，通过调整高斯函数的旋转角度 θ，利用 Gabor 小波构造一个 8 方向的滤波器组. 所提算法中 θ 的取值分别为 0、π/8、2π/8、3π/8、4π/8、5π/8、6π/8、7π/8，每个方向小波中其他关键参数的取值分别为 $f = 0.325$，$\gamma = 1$，$\eta = 1$，滤波器组方向数选取和参数优化过程将在实验部分给出. 利用方向性滤波器组将载体图像分解，损失函数将会被定义为不同方向上因嵌入信息造成分解系数发生相对变化之和. 滤波器组的多方向性使得加密后的载体图像在其 8 方向中的任一方向都难以被建模分析，减小秘密信息被隐写分析算法检测到的可能性. 所提算法隐写时对一张载体图像的 8 方向分解见图 2，其中图 2(a) 为载体图像，图 2(b)~(i) 为 Gabor 小波对载体图像的 8 方向分解.

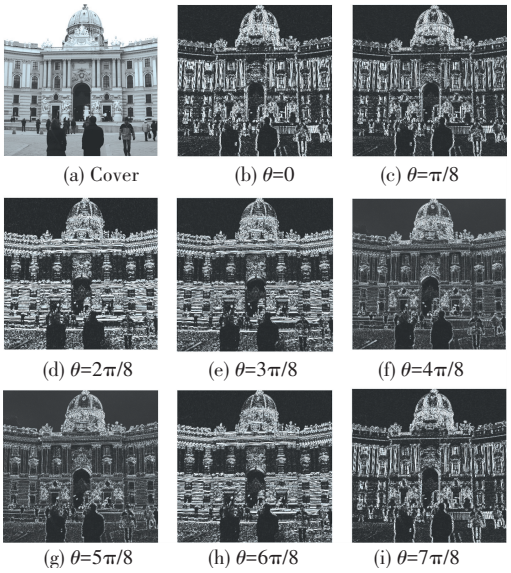


图 2　Gabor 小波对图像的 8 方向分解

Fig.2　8 direction decompositions of cover image using Gabor wavelet

2.2　隐写算法设计

WOW 算法利用 DB-8 小波构造的方向性滤波组从 LH、HL 和 HH 这 3 个方向计算载体图像残差值权重，将秘密信息嵌入到 LH、HL、HH 任一方向都难以预测建模的区域. 本文算法在 WOW 算法基础上做出改进，利用 Gabor 小波方向性滤波器组取代 DB-8 小波方向性滤波器组，将秘密信息嵌入到 0、π/8、2π/8、3π/8、4π/8、5π/8、6π/8、7π/8 任一方向都难以预测建模的区域. 所提算法(记为 Proposed)的隐写过程如下：

1)利用 Gabor 小波方向性滤波器组预测载体图像的残差权重，计算其中合适的信息嵌入位置 $\xi_{ij}^{(k)}$：

$$\xi_{ij}^{(k)} = |X \otimes G^{(k)}| \otimes |\mathrm{R}(G^{(k)})|.$$

式中：X 为载体图像，$G^{(k)}$ 为 Gabor 构成的方向性滤波器组($k = 1,2,3,\cdots,8$)，R 表示将 $G^{(k)}$ 翻转 180°.

2)将 $\xi_{ij}^{(k)}$ 以 Hölder 范数形式构建损失函数 ρ：

$$\rho_{ij} = \left(\sum_{k=1}^{8} |\xi_{ij}^{(k)}|^{-1}\right).$$

3)假设秘密信息为 $m \in \{m_1, m_2, m_3, \cdots, m_k\}$，$k$ 为信息长度，载体图像 X 的 LSB 层为 $x_x = \{x_{xn}\}$，载密图像 Y 的 LSB 层为 $x_y = \{x_{yn}\}$，若 $x_{xn} = x_{yn}$，保持 X 中的像素点不变；若 $x_{xn} \neq 6x_{yn}$，利用损失函数和 STC 编码在 X 中嵌入信息.

2.3　改进算法

使用自适应隐写算法的最终目的是将秘密信息嵌入到载体图像中纹理丰富的复杂区域，然而当载体图像比较平滑或信息嵌入量较大时，嵌入的秘密信息有可能散落到图像平滑区域或一些孤立点像素中，通过建模分析，隐写分析者可以轻易地探测到此类信息，从而降低了算法的安全性. 文献[16]指出，利用聚焦改变位置策略减少此类秘密信息的存在，可以有效提高算法的抗检测性能.

基于以上思想，对所提算法做出进一步改进：在信息嵌入之前，利用均值滤波器对损失函数进行滤波，滤除相对孤立点像素的残差权重，尽量使残差权重集中到纹理丰富区域，减小秘密信息被嵌入到载体图像平滑区域的可能性. 更新后的损失函数 ρ_{A} 为

$$\rho_{\mathrm{A}} = \rho_{ij} \otimes A = \left(\sum_{k=1}^{8} |\xi_{ij}^{(k)}|^{-1}\right) \otimes A.$$

式中 A 为均值滤波器，在本文算法中的阶数为 13，具体参数值的讨论将在实验部分给出. 损失函数更新后，按照 2.2 节中的步骤 3)继续进行秘密信息嵌入. 应用聚焦位置改变策略的所提算法记为 Proposed-A.

3　实验分析

实验计算机及软件配置如下：Intel Core i3 2.40 GHz CPU、4.00 GB RAM，软件平台为 MATLAB R2014a. 用于安全性测试的图像库有两个，分别为 BOSSBase 1.01[17] 和 BOWS2[18]. 借助 34671 维 SRM 特征和 12753 维 SRMQ1 特征衡量算法抗隐写分析性能，提取好的载体图像和载密图像特征分别送至集成分类器[19]进行分类，分类过程中一半图像特征用于训练，另一半用于测试. 最终的分析结果以检测错误率的形式给出，检测错误率越高，算法安全性能越好，反之亦然. 安全性对比分析中应用到的自适应隐写算法有 HUGO-BD[3]、WOW[5]、HILL[8]、Proposed、Proposed-A，除本文算法外，其他算法中的参数均为原文献默认值.

3.1　秘密信息的自适应嵌入

网络中传输的大多数数字图像都会存在纹理丰

富的复杂区域和相对平滑的简单区域,相关研究表明[20],将秘密信息嵌入到纹理丰富区域可有效提升加密图像抵抗隐写分析的能力. 所提算法考虑了载体图像的自身特性,利用 Gabor 小波从 8 个方向对其进行分解,获取纹理丰富区域,再利用 STC 编码在纹理丰富区域中嵌入秘密信息,最终实现自适应隐写. 通过一组实验说明秘密信息的自适应嵌入情况. 图 3(a)为载体图像,利用 Proposed 算法和 Proposed-A 算法对其进行隐写,信息嵌入率为 0.4 bit/pixel,加密后载体图像中的秘密信息分布分别如图 3(b)和图 3(c)所示,其中,白色像素点表示秘密信息. 载体图像经 Gabor 小波处理后得到的纹理丰富区域可见图 2. 由图 2 和图 3 可知,通过考虑图 3(a)的自身特性,所提算法借助 Gabor 小波和 STC 编码技术将秘密信息嵌入到了其纹理丰富区域,最终实现了自适应隐写.

(a) cover (b)Proposed (c)Proposed-A

图 3 所提算法隐写后的秘密信息分布

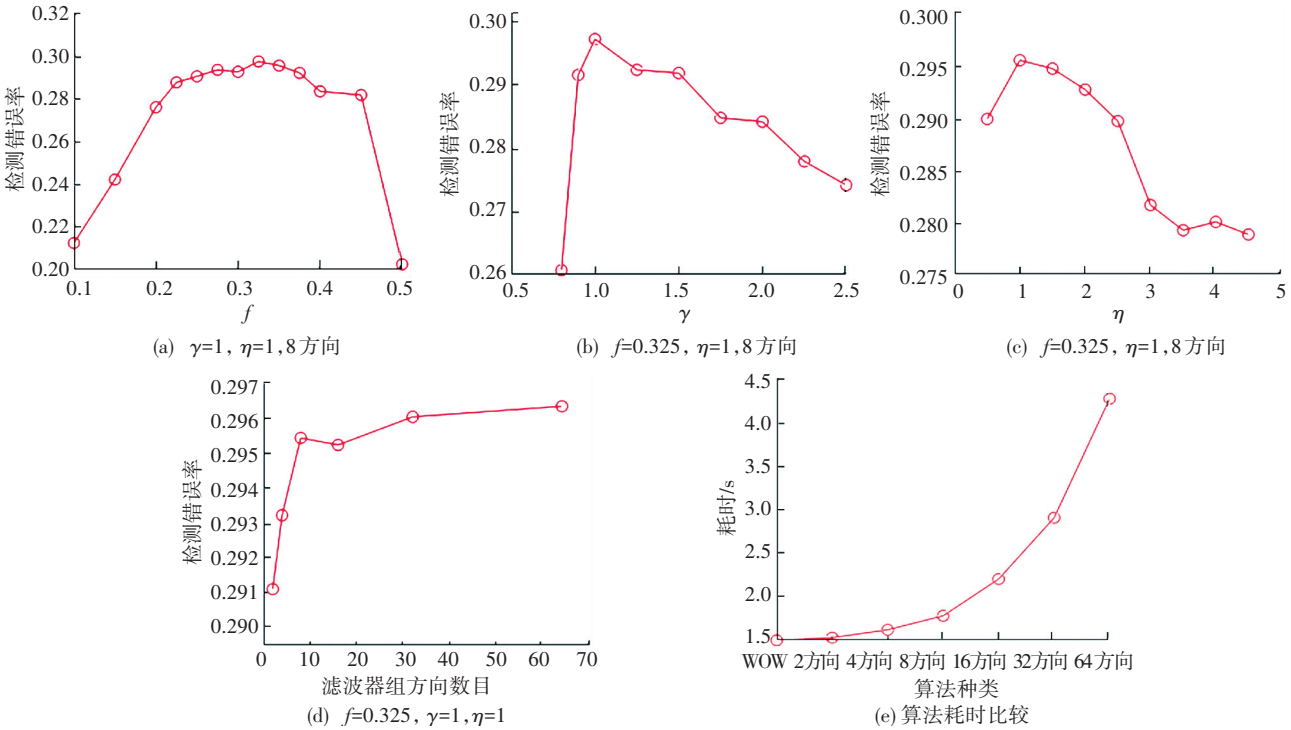
Fig.3 Distribution of secret message after steganography by Proposed and Proposed-A algorithm

3.2 Gabor 方向性滤波器组参数讨论

为构造最优的 Gabor 小波方向性滤波器组,借助 WOW 算法模型分别对 Gabor 小波中的参数 f、γ、η 进行优化,并确定出滤波器组的方向数,其中,滤波器组的方向数由参数 θ 决定. 优化共有两个过程,先设置参数 θ 为定值,求出最佳的 f、γ、η 参数值,再对参数 θ 进行优化.

首先设定滤波器组方向数为 8,即参数 θ 分别取值 0、π/8、2π/8、…、7π/8,固定参数 γ、η 取值,控制参数 f 在一定范围内变化,检测 f 发生变化时所提算法 Proposed 的抗检测能力. 选取安全性最好的那组参数 f 作为最佳参数,隐写算法的构造方式可参见 2.2 节,最佳参数确定后即设定其为固定值,另外两个参数 γ、η 的优化过程与参数 f 相同. 求出参数 f、γ、η 的最佳值后将其固定,令滤波器组方向数分别为 2(θ = 0、π/2)、4(θ = 0、π/4、2π/4、3π/4)、8(θ = 0、π/8、2π/8、…、7π/8)、16(θ = 0、π/16、2π/16、…、15π/16)、32(θ = 0、π/32、2π/32、…、31π/32)、64(θ = 0、π/64、2π/64、…、63π/64),检测滤波器组方向数发生变化时所提算法的抗检测能力. 进行抗检测性能分析实验时,随机从 Bossbase 1.01 图像库中选取 5 000 张图像用于隐写加密,信息嵌入率为 0.4 bit/pixel,提取载体图像和载密图像 SRMQ1 特征送至集成分类器进行分类,根据分类结果确定算法抗检测性能.

实验数据见图 4. 由图 4(a)、图 4(b)、图 4(c)确定出参数 f、γ、η 最佳值分别为 0.325、1、1. 由图 4(d)、图 4(e)可知,随着滤波器组方向数增多,所提算法的抗检测性能大致呈上升趋势,但当滤波器组方向数明显增大时,所提算法的安全性能的提升并不明显,而隐写单张载体图片的耗时明显增加.



(a) γ=1, η=1,8方向 (b) f=0.325, η=1,8方向 (c) f=0.325, η=1,8方向

(d) f=0.325, γ=1, η=1 (e) 算法耗时比较

图 4 方向性滤波器的参数优化

Fig.4 Parameters optimization of directional filter

综合考虑算法的安全性能与时间复杂度，最终确定滤波器组方向数为 8. 另外，由图 4(e)可知，在时间复杂度上 WOW 比所提算法有 0.3 s 左右的优势，两者之间的差距并不大，且隐写技术中最重要的两个指标是算法安全性能和信息嵌入率，因此可以忽略两者在时间复杂度上的差距.

3.3 *A* 参数讨论

Proposed-A 通过聚焦改变位置策略对所提算法做进一步改进，为确定均值滤波器 *A* 的参数值，做以下实验：选取 Bossbase 1.01 图像库中的10 000 张图像用于测试，选用不同 *A* 参数的Proposed-A进行隐写加密，信息嵌入率为 0.4 bit/pixel，加密完成后利用 SRMQ1 提取载体图像和载密图像特征，最后将提取好的特征送至集成分类器进行分类，实验数据如表 1 所示.

在 Bossbase 1.01 图像库上的实验表明，与 Proposed 相比，应用了聚焦改变策略的 Proposed-A 的抗检测性能有 0.6%～2.6%的提升. 根据实验结果，最终确定 Proposed-A 中的均值滤波器阶数为 13×13.

表 1　均值滤波器对 Proposed-A 安全性能的影响

Tab.1　Effect of average filter on Proposed-A

A	1×1	3×3	5×5	7×7	9×9	11×11	13×13	15×15	17×17	19×19
错误率	0.233 8	0.240 6	0.253 2	0.254 9	0.256 8	0.258 0	0.260 6	0.255 1	0.255 9	0.259 3

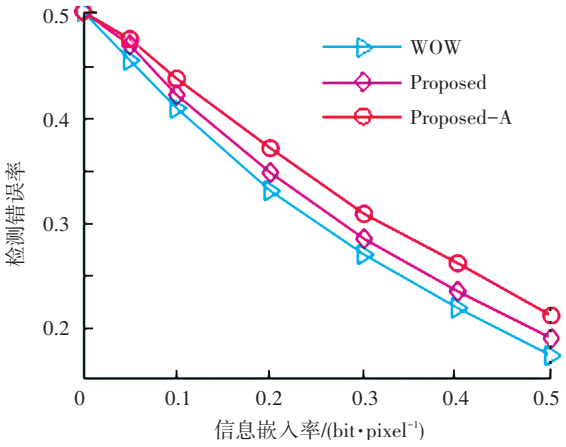
3.4 算法安全性对比

为对比分析算法的抗检测性能，分别利用 12753 维 SRMQ1 特征和 34671 维 SRM 特征对 HUGO-BD、WOW、Proposed、HILL 和 Proposed-A 进行安全性能检测分析，隐写载体分别选用 Bossbase 1.01 图像库中的10 000 张和 BOWS2 图像库中的 5 000张空域灰度图像，信息嵌入率分别为 0.05、0.1、0.2、0.3、0.4、0.5 bit/pixel. 最终的分类错误率结果分别如表 2、图 5 和图 6 所示，详细的实验数据可参见表 2.

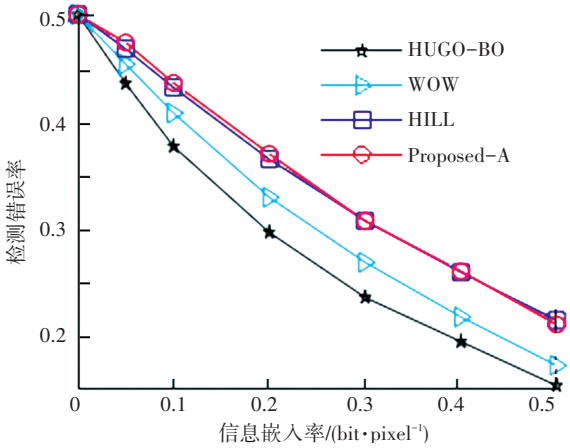
表 2　抗 SRMQ1 和 SRM 特征检测性能分析

Tab.2　Security analysis of detected by SRMQ1 and SRM

数据库	特征	隐写方法	0.05	0.1	0.2	0.3	0.4	0.5
BOSSBase1.01 (10 000 张)	SRMQ1 (12753 维)	HUGO-BD	0.435 6	0.376 9	0.296 7	0.236 1	0.194 9	0.153 8
		WOW	0.453 6	0.408 0	0.329 4	0.268 8	0.217 9	0.172 6
		Proposed	0.468 2	0.420 5	0.346 7	0.283 8	0.233 8	0.189 2
		HILL	0.467 9	0.431 7	0.364 9	0.307 3	0.259 4	0.217 0
		Proposed-A	0.473 8	0.436 1	0.370 0	0.307 5	0.260 6	0.210 6
	SRM (34671 维)	HUGO-BD	0.425 0	0.363 0	0.285 0	0.226 0	0.185 3	0.145 4
		WOW	0.452 7	0.406 4	0.316 7	0.255 1	0.204 9	0.161 8
		Proposed	0.462 0	0.415 1	0.326 8	0.262 2	0.213 3	0.175 7
		HILL	0.466 5	0.431 3	0.354 9	0.291 6	0.246 8	0.204 5
		Proposed-A	0.469 8	0.432 7	0.361 6	0.291 2	0.242 5	0.194 9
BOWS2 (5 000 张)	SRMQ1 (12753 维)	HUGO-BD	0.471 0	0.440 2	0.351 8	0.281 8	0.220 9	0.176 3
		WOW	0.472 1	0.427 4	0.336 1	0.262 5	0.204 0	0.160 7
		Proposed	0.478 9	0.442 4	0.352 0	0.276 3	0.217 1	0.172 1
		HILL	0.483 5	0.448 4	0.365 8	0.289 2	0.224 0	0.177 2
		Proposed-A	0.482 0	0.449 5	0.366 5	0.286 9	0.221 7	0.172 7
	SRM (34671 维)	HUGO-BD	0.466 3	0.426 9	0.335 5	0.261 0	0.199 5	0.162 3
		WOW	0.4597	0.407 9	0.321 8	0.236 9	0.185 9	0.144 9
		Proposed	0.469 5	0.428 1	0.333 8	0.255 6	0.198 0	0.158 5
		HILL	0.477 9	0.434 6	0.349 2	0.264 9	0.209 8	0.163 4
		Proposed-A	0.473 0	0.435 1	0.348 8	0.262 1	0.201 5	0.158 6



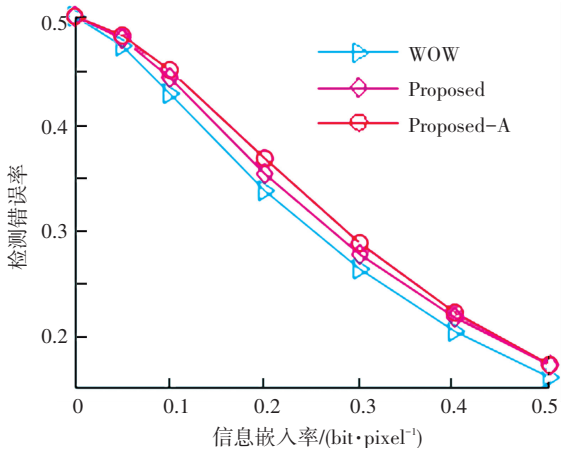
(a)改进算法间的安全性对比



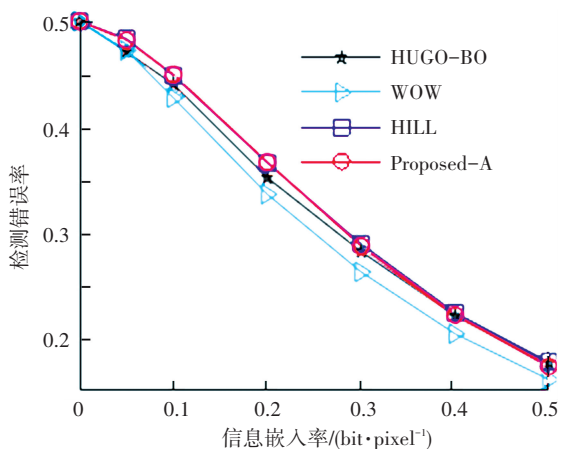
(b) 与典型隐写算法的安全性对比

图 5 BOSSBase1.01 图像库上的 SRMQ1 隐写分析

Fig.5 SRMQ1 steganalysis on BOSSBase 1.01



(a)改进算法间的安全性对比



(b) 与典型隐写算法的安全性对比

图 6 BOWS2 图像库上的 SRMQ1 隐写分析

Fig.6 SRMQ1 steganalysis on BOWS2

由图 5(a)和图 6(a)可知,由 Gabor 小波方向性滤波器组设计的 Proposed 算法的抵抗富模型检测能力强于 WOW,与 Proposed 算法相比,对信息嵌入位置做出调整后,引入聚焦改变位置策略的 Proposed-A 算法在抗富模型检测能力上又有了一定幅度的增强;从图 5(b)和图 6(b)可知,与其他自适应隐写算法相比,本文算法同样存在一定优势,在两个不同数据库测试时,同等水平的信息嵌入率条件下,Proposed-A 算法的抗检测性能略优于 HILL 算法或与之相当,均优于 WOW 和 HUGO-BD. 分析其原因,Gabor 小波在生物图像纹理表达和分离上的优势特性同样有利于自适应隐写算法中信息嵌入位置的确定,且与利用 3 方向滤波器组设计的 WOW 算法相比,所提算法可以将秘密信息嵌入到从 8 个方向上都难于被建模分析的纹理复杂区域. 另外,应用聚焦改变位置策略后,所提算法可以减少秘密信息被嵌入到平滑区域的可能性,这同样有利于算法安全性能的提升.

4 结 语

在 WOW 算法的基础上,提出一种利用 Gabor 小波设计的空域自适应隐写算法,并通过聚焦改变位置策略对所提算法做出了进一步完善. 本文将 Gabor 小波应用到隐写术中,通过 Gabor 小波获取载体图像的纹理丰富区域,构造好损失函数后再利用校验格编码完成秘密信息嵌入,最终实现自适应隐写. 实验表明,所提算法的安全性能明显优于 WOW 算法,从而验证了本文方案的可行性. 另外,与 HUGO-BD 算法和 HILL 算法相比,所提算法同样存在一定优势.

参考文献

[1] FRIDRICH J, FILLER T. Practical methods for minimizing embedding impact in steganography[J]. Proceedings of SPIE-The International Society for Optical Engineering, 2007, 6505:650502-650502-15. DOI: 10.1117/12.697471.

[2] PENVY T, FILLER T, BAS P. Using high-dimensional image mod-

els to perform highly undetectable steganography[C]// International Conference on Information Hiding. Calgary:Springer-Verlag, 2010: 161-177. DOI: 10.1007/978-3-642-16435-4_13.

[3] FILLER T, FRIDRICH J. Gibbs construction in steganography[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(4): 705-720. DOI: 10.1109/TIFS.2010.2077629.

[4] GUO Linjie, NI Jiangqun, SHI Yunqing. An efficient JPEG steganographic scheme using uniform embedding[J]. IEEE International Workshop on Information Forensics and Security, 2012, 98(5): 169-174. DOI: 10.1109/WIFS.2012.6412644.

[5] HOLUB V, FRIDRICH J. Designing steganographic distortion using directional filters[J]. IEEE International Workshop on Information Forensics and Security, 2012, 2(4): 234-239. DOI: 10.1109/WIFS.2012.6412655.

[6] GUO Linjie, NI Jiangqun, SHI Yunqing. Uniform embedding for efficient JPEG steganography[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(5): 814-825. DOI: 10.1109/TIFS.2014.2312817.

[7] HOLUB V, FRIDRICH J, DENEMARK T. Universal distortion function for steganography in an arbitrary domain[J]. Eurasip Journal on Information Security, 2014, 2014(1): 1-13. DOI:10.1186/1687-417X-2014-1.

[8] LI Bin, WANG Ming, HUANG Jiwu, et al. A new cost function for spatial image steganography[C]// IEEE International Conference on Image Processing. Paris: IEEE, 2014: 4206-4210.

[9] 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. DOI: 10.1109/TIFS.2011.2134094.

[10] FRIDRICH J, KODOVSKY J. Rich models for steganalysis of digital images[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(3): 868-882. DOI: 10.1109/TIFS.2012.2190402.

[11] HOLUB V, FRIDRICH J. Optimizing pixel predictors for steganalysis[J]. Proceedings of SPIE-The International Society for Optical Engineering, 2012, 8303:830309-830309-13. DOI: 10.1117/12.905753.

[12] MANJUNATHB S, MA W Y. Texture features for browsing and retrieval of image data[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1996, 18(8):837-842. DOI: 10.1109/34.531803.

[13] ZHANG Baochang, SHAN Shiguang, CHEN Xilin, et al. Histogram of gabor phase patterns (HGPP): a novel object representation approach for face recognition[J]. IEEE Transactions on Image Processing, 2007, 16(1):57-68.DOI: 10.1109/TIP.2006.884956.

[14] REN Chuanxian, DAI Daoqing, LI Xiaoxin, et al. Band-reweighed gabor kernel embedding for face image representation and recognition[J]. IEEE Transactions on Image Processing, 2014, 23(2):725-740. DOI: 10.1109/TIP.2013.2292560.

[15] DOSODIA P, POONIA A, GUPTA S K, et al. New Gabor-DCT feature extraction technique for facial expression recognition[C]// Fifth International Conference on Communication Systems and Network Technologies. Gwalior: IEEE, 2015. DOI: 10.1109/CSNT.2015.162.

[16] 王明.最小化嵌入失真图像隐写的代价函数设计[D]. 深圳:深圳大学, 2015.
WANG Ming. Cost function design for image steganography under embedding distortion minization[D]. Shenzhen: Shenzhen University, 2015.

[17] BAS P, FILLER T, PENVY T. Break our steganographic system: the ins and outs of organizing BOSS[C]// International Conference on Information Hiding. Prague: Springer-Verlag, 2011: 59-70. DOI:10.1109/TIFS.2010.2077629.

[18] BAS P, FURON T.BOWS-2[EB/OL]. http://bows2.gipsa-lab.inpg.fr.2007.

[19] 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. DOI: 10.1109/TIFS.2011.2175919.

[20] 奚玲.基于内容特征的自适应图像隐写技术研究[D]. 郑州:解放军信息工程大学, 2011.
XI Ling. Research on content based adaptive image steganograghy[D]. Zhengzhou: PLA Information Engineering University, 2011.

（编辑　王小唯，苗秀芝）