Computer Science and Application 计算机科学与应用, 2020, 10(4), 749-759
Published Online April 2020 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2020.104078

Hans汉斯

Image Steganography Algorithm Based on Minimum Filter and Perceptual Hash

Qian Liu[1], Qingguang Li[1,2*]

[1]School of Computer, Electronics and Information, Guangxi University, Nanning Guangxi
[2]Guangxi Key Laboratory of Multimedia Communications and Network Technology, Nanning Guangxi
Email: *qg_li@gxu.edu.cn

Received: Apr. 2nd, 2020; accepted: Apr. 17th, 2020; published: Apr. 24th, 2020

Abstract

Now the image steganography algorithm does not apply the clustering rule very well. It leads to the security of steganography algorithm that is still not ideal. MiPOD (Minimizing the Power of Optimal Detector) is a classical steganography algorithm, which has a high security. But it uses the method of randomly changing the direction to modify the pixels, which does not conform to the clustering rule. In order to improve the security of the steganography algorithm, our algorithm which base on MiPOD uses the minimum filter, the pixel changed method corresponding to the minimum value in the local area of the cost matrix is given to the whole local area. It can realize local clustering. In addition, the perceptual hash algorithm is used to find the similar parts of the image, and the similar regions are given the same changed direction. It can realize overall clustering. Comparing with the MiPOD, the testing error rate of SRM is improved by 0.72%, and that of maxSRMd2 is improved by 0.61%.

Keywords

Clustering Rule, Minimum Filter, Perceptual Hash, Image Steganography

基于最小值滤波与感知哈希算法的图像隐写算法

刘　骞[1]，李清光[1,2*]

[1]广西大学计算机与电子信息学院，广西，南宁
[2]广西多媒体通信与网络技术重点实验室，广西　南宁
Email: *qg_li@gxu.edu.cn

*通讯作者。

文章引用: 刘骞, 李清光. 基于最小值滤波与感知哈希算法的图像隐写算法[J]. 计算机科学与应用, 2020, 10(4): 749-759. DOI: 10.12677/csa.2020.104078

收稿日期：2020年4月2日；录用日期：2020年4月17日；发布日期：2020年4月24日

摘　要

现有图像隐写算法没有很好地应用修改聚集原则，导致隐写算法的安全性仍然不够理想。经典隐写算法MiPOD (Minimizing the Power of Optimal Detector)拥有较高的安全性，但它使用随机修改方向的方式对像素进行修改，不符合修改聚集原则。为了提升隐写算法的安全性，在MiPOD的基础上，本文使用最小值滤波将代价矩阵局部区域内最小值的修改方式赋予整个局部，实现局部修改聚集；此外使用感知哈希算法寻找图像中相似的部分，赋予相似区域相同的修改方向，以达到整体修改聚集的目的。实验结果表明，本文算法相较于MiPOD，抵抗SRM特征的检错率平均提升了0.72%，抵抗maxSRM特征的检错率平均提升了0.61%。

关键词

修改聚集，最小值滤波，感知哈希，图像隐写

1. 引言

图像隐写术是信息隐藏的一个重要分支，它在尽量不改变图像统计规律的前提下，嵌入秘密信息，外人难以察觉图像差异，从而达到隐藏秘密信息的目的[1]。

当前图像隐写算法的设计有三大原则[2]：

(1). 复杂度优先。在复杂度优先原则指导下，秘密信息应优先嵌入至图像纹理复杂的区域。图像隐写算法一般用像素修改代价来衡量图像的纹理复杂程度，处于图像纹理复杂区域的像素赋予较小的修改代价，这是因为图像纹理复杂区域难以建模与统计，在该区域进行修改难以被检测，有益于掩盖因载体图像像素修改带来的影响，而处于图像纹理平滑区域的像素赋予较大的隐写代价。因此需要设计一个合适的失真函数以度量图像各个区域的纹理复杂程度与像素修改所造成的修改代价，如 ASDL-GAN (Automatic Steganographic Distortion Learning framework with GAN) [3]使用生成式对抗网络(Generative Adversarial Network, GAN) [4]的对抗学习来获取修改代价。Tang 等[5]在上述算法的基础上，使用对抗样本的梯度方向动态调整修改代价，获得的数值更准确。WOW (Wavelet Obtained Weights) [6]则使用方向滤波器计算每个方向的代价，若每个方向的代价都较小，则赋予该点较小的修改代价，否则赋予较大的修改代价。MG (Multivariate Gaussian Model) [7]将图像像素看成独立的随机高斯变量，对图像的每个像素点建立图像概率模型。MVGG (Multivariate Generalized Gaussian) [8]改进了 MG 算法，使用更好的方差估计器，同时使用五元编码降低修改率。MiPOD (Minimizing the Power of Optimal Detector) [9]则使用广义高斯分布来建模，同时使用最优检测器来获取更准确的图像纹理复杂度。

(2). 代价扩散。根据复杂度优先原则，得到载体图像每个像素的修改代价后，引入代价扩原则，能够使载体图像的每个像素的修改代价更准确。代价扩散原则认为：相邻像素应该有相似的修改代价。将

修改代价较小像素的修改代价扩散到邻域像素的修改代价中，使邻域像素的修改代价也相应地变小。同理，修改代价较大的像素的邻域像素也应该有较大的代价。Li 等[2]用实验证明了可以使用低通滤波器来进行修改代价扩散。HILL (HIgh-pass, Low-pass, and Low-pass) [10]利用了这一原则，使用一个高通滤波器计算图像纹理复杂度与每个像素的修改代价，再使用两个低通滤波器将代价扩散，隐写安全性得到有效提升。后续算法如 MVGG [8]与 MiPOD [9]，都使用均值滤波进行代价扩散，以提高隐写的安全性能。

(3). 修改聚集原则。秘密信息的嵌入区域应该尽量聚集在一起，使得像素的修改尽可能集中。由于载体图像在修改聚集后的 SPAM (Subtractive Pixel Adjacency Matrix) [11]特征的 MMD (Maximum Mean Miscrepancy) [12]距离明显小于修改分散的距离，因此修改聚集能更好地保持载体图像的自然统计特性，使隐写图像更接近自然图像，提升安全性。Zheng [13]所设计的算法就很好地利用了这一原则，利用最大值滤波将隐写区域集中，使秘密信息的嵌入更加集中，隐写安全性得到提升。CMD (Clustering Modification Directions) [14]则拓展了修改聚集原则。提出了聚集修改方向的新策略，认为除了修改区域集中外，相邻像素的修改方向也应该同向，并用实验证明了有效性。

在上述算法中，MiPOD 的安全性能最优[15]，因为它所使用的估计图像概率模型计算得到的图像纹理信息更准确，满足复杂度优先原则，同时使用均值滤波作为代价扩散的方式，满足代价扩散原则。但 MiPOD 在嵌入秘密信息对图像像素进行修改时，使用的是随机正负 1 的修改方式，并不满足修改聚集原则，因此 MiPOD 算法的安全性仍然有提升的空间。若能改变 MiPOD 的像素修改方式，使其满足修改聚集原则，就能有效提升该算法的隐写安全性能。

因此，为了能有效改变秘密信息嵌入时像素修改方式，我们提出了一种新的基于最小值滤波和感知哈希算法的图像隐写算法。新算法在 MiPOD 算法的基础上，使用最小值滤波筛选需要同向修改的区域，在此区域中修改的方向是一致的。此外，我们利用哈希感知算法比较图像的各个区域，相似区域则使用相同的修改方向。两种方法的结合能够使算法更准确地找出需要同向修改的区域，使算法满足修改聚集原则，进而提升算法安全性能。实验证明，我们提出的新算法比现在的主流算法具有更好的性能。

2. 算法

由于本文算法是在 MiPOD 算法基础上改进的，加入了修改聚集功能，因此本文算法命名为“MiPOD-Cluster”。本文算法(MiPOD-Cluster)主要的改进包括两大步骤：

聚集区域与修改方式选择。使用最小值滤波处理修改代价矩阵，代价矩阵会出现局部数值相等的情况，数值相等的局部区域就是修改的聚集区域。并将数值相等的局部区域内数值对应的像素修改方向作为整个局部的修改方向。

修正相似区域的修改方式。将载体图像切割为若干个小块，使用感知哈希算法[16]计算小块之间的相似度，若不同小块之间相似，则赋予两个相似小块相同的修改方式。

2.1. 算法基本原理

MiPOD 算法中用以度量像素修改代价的是通过概率模型建模得到的 Fisher 信息[17]矩阵。载体图像像素的 Fisher 信息越小，表明此像素处于的纹理区域越复杂，并且拥有较小的修改代价，在此像素嵌入秘密信息的安全性较高。反之亦然。所以 Fisher 信息矩阵能够近似表征载体图像的纹理复杂程度。

2.1.1. 最小值滤波原理

在实际图像隐写中，由于 Fisher 信息较小的像素通常处于载体图像纹理复杂的区域中，安全性较高，因此 MiPOD 一般在 Fisher 信息较小的像素上嵌入秘密信息。这意味着在载体图像中，这些 Fisher 信息较

小的像素具有较高的修改优先级，在嵌入秘密信息会优先被修改由此可知修改聚集的主要问题是如何处理这些 Fisher 信息较小的像素。

最小值滤波通过选取区域中的最小值作为当前像素的值，不仅能除去不必要的噪声，筛选出的区域还能更为紧凑。此外，筛选区域中会出现局部区域内各个元素相等的情况，可将该局部区域中最小值原本的随机修改方式作为整个区域的修改方式，从而降低算法复杂度，达到修改聚集目的的同时又能减小对图像隐写效率的影响。所以使用最小值滤波处理 Fisher 信息矩阵时，可以将当前元素邻域中的最小值对应载体图像的修改方式作为当前元素的修改方式。

因此本文选择使用最小值滤波作为隐写候选像素的筛选聚集区域与修改方向的方法。

2.1.2. 感知哈希算法原理

载体图像中往往有一些相似的区域，这些相似的区域往往不重合，甚至可能相隔甚远，使用低通滤波的方法无法将它们联系在一起，这就需要其他方法寻找这些可能会相似的区域。

本文使用感知哈希算法[16]，是因为该算法在图像相似图片搜索领域已经非常成熟，算法速度非常快，并且图像的高度、宽度、亮度、颜色等基本信息发生变化，该图像的哈希值也不会改变，算法准确率相当高。本文算法是将图像分割成若干份，并使用图像相似算法计算它们之间的相似值，计算量较大，因此算法成熟、计算方法较快的感知哈希算法符合本文要求。

感知哈希算法的基本原理如下：

(1). 图像大小归一化；(2). 简化灰度减少计算量；(3). 计算平均灰度值；(4). 比较像素与平均灰度值的大小，若大于则记为 1，小于则记为 0，按照一定顺序排列成 2 进制的指纹编码；(5). 最后对比两幅图的指纹编码，若差异数据位小于阈值，则证明图像相似，若大于 2 倍阈值，则说明图像不相似。

2.2. 本文算法(MiPOD-Cluster)流程

以下是本文算法的完整流程，其中步骤 1 至步骤 5 为 MiPOD [9]的方差估计器，步骤 7 为利用最小值滤波得到图像像素的修改方式分布图，步骤 8 为使用感知哈希算法修正图像修改方式：

步骤 1：计算噪声残差。假设隐写图像 $\mathbf{z}$ 是 8 位灰度图像，图像大小为 $row\times col$，具有初始像素值 $\mathbf{z_n}\in\{0,\cdots,255\}$，$n\in[1,row\times col]$，使用维纳滤波器(Wiener filter) F 去噪，计算噪声残差 r：

$$r=\mathbf{z}-F(\mathbf{z}) \tag{1}$$

步骤 2：对残差 r 中的第 n 个像素以及它的 $p\times p$ 邻域建模，边界使用镜像填充的方法扩展：

$$r_n=Ga_n+\xi_n \tag{2}$$

这里 r_n 是大小为 $p^2\times 1$ 的列向量，数值为第 n 个像素的 $p\times p$ 邻域内的残差 r 的值。G 是一个大小为 $p^2\times q$ 的矩阵，由式(3)可得，它定义了残差 r 的参数模型，该模型有 q 个参数，a_n 是 $q\times 1$ 的向量，ξ_n 是噪声和建模误差的集合。

$$\begin{aligned}G=&\left(1,\cos(\mathbf{u}),\cos(\mathbf{v}),\cos(\mathbf{u})\cdot\cos(\mathbf{v}),\cos(2\mathbf{u}),\cos(2\mathbf{v}),\right.\\&\left.\cos(2\mathbf{u})\cdot\cos(2\mathbf{v}),\cdots,\cos(l\mathbf{u}),\cos(l\mathbf{v})\right)\end{aligned} \tag{3}$$

其中 $\mathbf{1}$、$\mathbf{u}$、$\mathbf{v}$ 是 $p^2\times 1$ 的向量，$\mathbf{1}$ 为单位向量，$\mathbf{u}$ 由矩阵 $\mathbf{U}$ (式 4)展开获得，$\mathbf{v}$ 由矩阵 $\mathbf{V}$ 展开获得，$\mathbf{V}=\mathbf{U}^{\mathrm{T}}$，$l$ 是 G 中二维余弦多项式的阶数，G 中含有 $q=l(l+1)/2$ 个元素，由文献[9]可知，$p=9$，$l=9$，$q=45$ 可以获得最佳的性能。

$$U=\begin{pmatrix} \frac{\pi}{2p} & \frac{3\pi}{2p} & \cdots & \frac{\pi(2p-3)}{2p} & \frac{\pi(2p-1)}{2p} \\ \frac{\pi}{2p} & \frac{3\pi}{2p} & \cdots & \frac{\pi(2p-3)}{2p} & \frac{\pi(2p-1)}{2p} \\ \frac{\pi}{2p} & \frac{3\pi}{2p} & \cdots & \frac{\pi(2p-3)}{2p} & \frac{\pi(2p-1)}{2p} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{\pi}{2p} & \frac{3\pi}{2p} & \cdots & \frac{\pi(2p-3)}{2p} & \frac{\pi(2p-1)}{2p} \end{pmatrix} \tag{4}$$

步骤 3：由残差 r_n 得出参数 a_n 的最大似然估计 $\hat{a}_n$：

$$\hat{a}_n=\left(G^{\mathrm{T}}G\right)^{-1}G^{\mathrm{T}}r_n \tag{5}$$

步骤 4：接下来计算出残差 r_n 的估计期望 $\hat{r}_n$：

$$\hat{r}_n=G\hat{a}_n=G\left(G^{\mathrm{T}}G\right)^{-1}G^{\mathrm{T}}r_n \tag{6}$$

步骤 5：假设第 n 个 $p\times p$ 块中的像素具有相同或相似的方差，第 n 个像素(第 n 块中的中心像素)方差的最小二乘估计为：

$$\hat{\sigma}_n^2=\frac{\left\|r_n-\hat{r}_n\right\|^2}{p^2-q} \tag{7}$$

在估计方差较小的像素处，对估计方差进行限制：

$$\hat{\sigma}_n^2=\max\left\{0.01,\hat{\sigma}_n^2\right\} \tag{8}$$

步骤 6：使用估计方差 $\hat{\sigma}_n^2$ 计算得到隐写图像第 n 个像素的 Fisher 信息：$FI_n=1/\hat{\sigma}_n^4$

步骤 7：对所有的像素点分配一个随机值，根据随机值大小随机分配修改方向。统计所有像素点的 Fisher 信息，得到 Fisher 信息矩阵 Fisher_Infor。使用最小值滤波处理 Fisher_Infor，中心像素置为最小值的同时，将该最小值像素的修改方向同步到中心像素中，得到图像修改方式分布矩阵 Modify，里面的数值都为±1。

步骤 8：将图像分割成 4 份，使用感知哈希算法计算两两图片的相似度。若相似则统一相似的部分图像的图像修改方式分布，若不相似，则继续切割图像，并重复该步骤。为利于计算，最大切割数量为 16 份，但分割后的图像最小不小于16×16 。最后得到修正后的图像修改方式分布图 Modify_new。

步骤 9：根据 Fisher 信息矩阵 Fisher_Infor 与负载 Payload 确定需要修改的像素，根据修正后的图像修改方式分布图 Modify_new 确定需要修改像素的修改方向，将秘密信息嵌入至图像中。嵌入完成后，隐写完成。

3. 实验

本文使用 MG [7]、MCGG [8]、MiPOD [9]这三种效果较好的隐写算法与本文算法 MiPOD-Cluster 进行实验对比。

实验所使用的图像来自目前隐写算法常用的图像库 BOSSbase1.01 [18]。实验使用里面 10000 张大小为 8 bit 的512×512 的 PGM 格式灰度图片，其中 50%用于训练，50%用于测试。嵌入的秘密信息为随机的 01 字符串，隐写负载分别为 0.05、0.1、0.2、0.3、0.4、0.5，单位为 bpp (bits per pixel)。隐写分析则使

用 SRM (Spatial Rich Model) [19]特征与 maxSRMd2 (max Spatial Rich Model) [20]特征，两种方法都可提取图像 34671 维度的特征。选用的隐写分类器为目前隐写分析中常用的 Ensemble [21]分类器，版本为 2.0，并使用默认设置。安全性能用隐写分析的检错率来表征，检错率用最小平均分类错误率 P_E 来表示，使用式(9)计算：

$$P_E = \min_{P_{FA}} \frac{1}{2}\left(P_{FA} + P_{MD}\right) \tag{9}$$

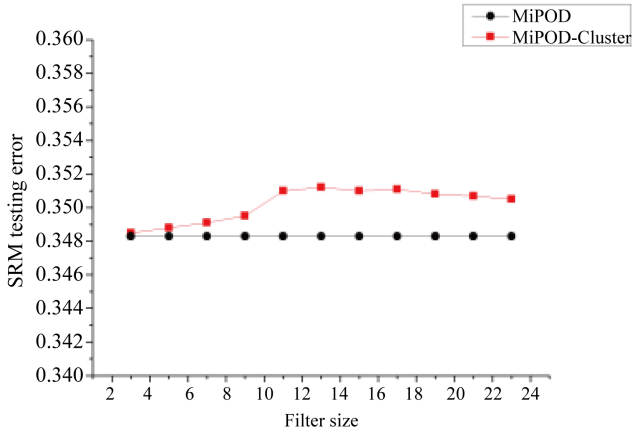
其中，P_{FA} 表示错警率(Probability of False-Alarm)，P_{MD} 表示漏检率(Probability of Missed-Detection)，P_E 越大，说明隐写分析检测时出现错误的概率越大，隐写算法的安全性越强。

3.1. 修改聚集实验

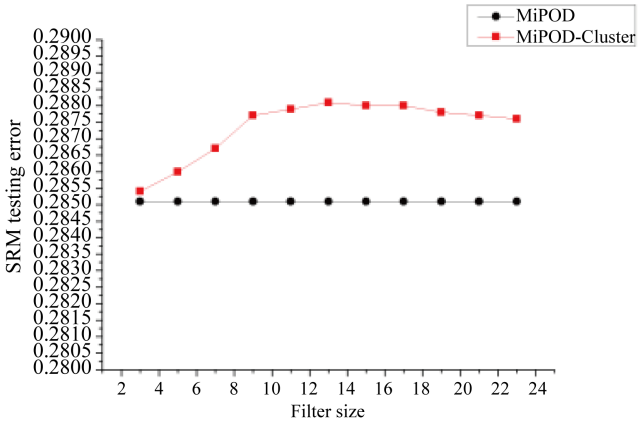
3.1.1. 最小值滤波器的最佳窗口大小

本文修改聚集的第一个步骤就是使用最小值滤波处理 MiPOD 中的 Fisher 信息矩阵，滤波窗口的大小决定着最小值滤波对 Fisher 信息矩阵的影响程度，因此本小节需要讨论在本文算法中，如何选择最小值滤波器的最佳的窗口大小。

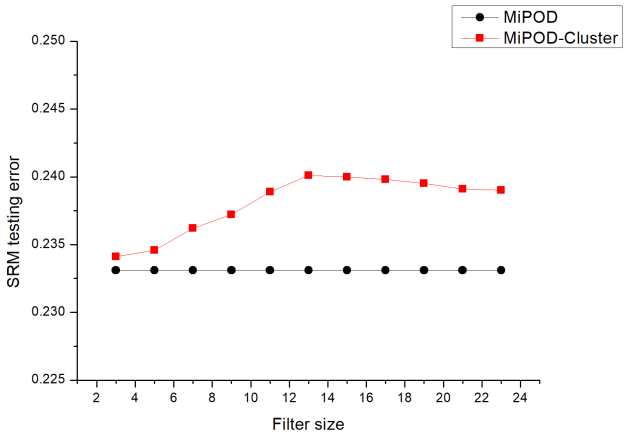
需要对比的是修改聚集在最小值滤波不同窗口大小下的算法安全性能。实验参数与 Li 等[2]一致，滤波器窗口大小从 3×3 增加到 23×23，步长为 2。隐写分析选择 SRM 特征，隐写负载为 0.2 bpp、0.3 bpp、0.4 bpp，每个滤波窗口大小实验次数为 10 次，最后取平均值。测试的结果如图 1。



(a) 0.2 bpp 负载



(b) 0.3 bpp 负载



(c) 0.4 bpp 负载

Figure 1. The influence of minimum filter and filter size on the security of MiPOD-Cluster under different payloads
图 1. 不同负载下，最小值滤波不同窗口大小对 MiPOD-Cluster 算法安全性的影响

由图 1 可知 MiPOD-Cluster 在 0.2 bpp、0.3 bpp、0.4 bpp 负载的抵抗 SRM 特征的安全性均优于 MiPOD，并且 MiPOD-Cluster 的安全性随着最小值滤波窗口的增大而升高，在窗口大小为 13 时得到最大值，当滤波窗口继续增大时，算法安全性趋于平稳。

由于隐写图像在修改聚集后的 SPAM 特征的 MMD (Maximum Mean Miscrepancy)距里明显小于修改分散的距离[2]，因此 MiPOD-Cluster 在 MiPOD 的基础上引入了修改聚集原则后，MiPOD-Cluster 隐写的图像比 MiPOD 的隐写图像更接近自然图像，因此 MiPOD-Cluster 算法的隐写安全性更高。

修改聚集的性能随着最小值滤波窗口的增大而逐渐增强，这是因为随着滤波窗口的增大，最小值滤波在图像中筛选的聚集区域范围越来越大，所寻找到的图像纹理聚集区域越多，过滤噪声的能力也越强。在滤波窗口足够大之后，修改聚集的性能趋于平稳，还有下降的趋势，这是因为图像适合修改聚集的纹理部分大小有限，滤波窗口太大，会导致本不属于一类聚集区域的聚集点集合到一起，形成大范围都为+1 或都为−1 的情况，降低隐写的安全性。

由此可以得出结论：MiPOD-Cluster 使用13×13 窗口大小的最小值滤波作为修改聚集的方法能够获得最好的安全性能。

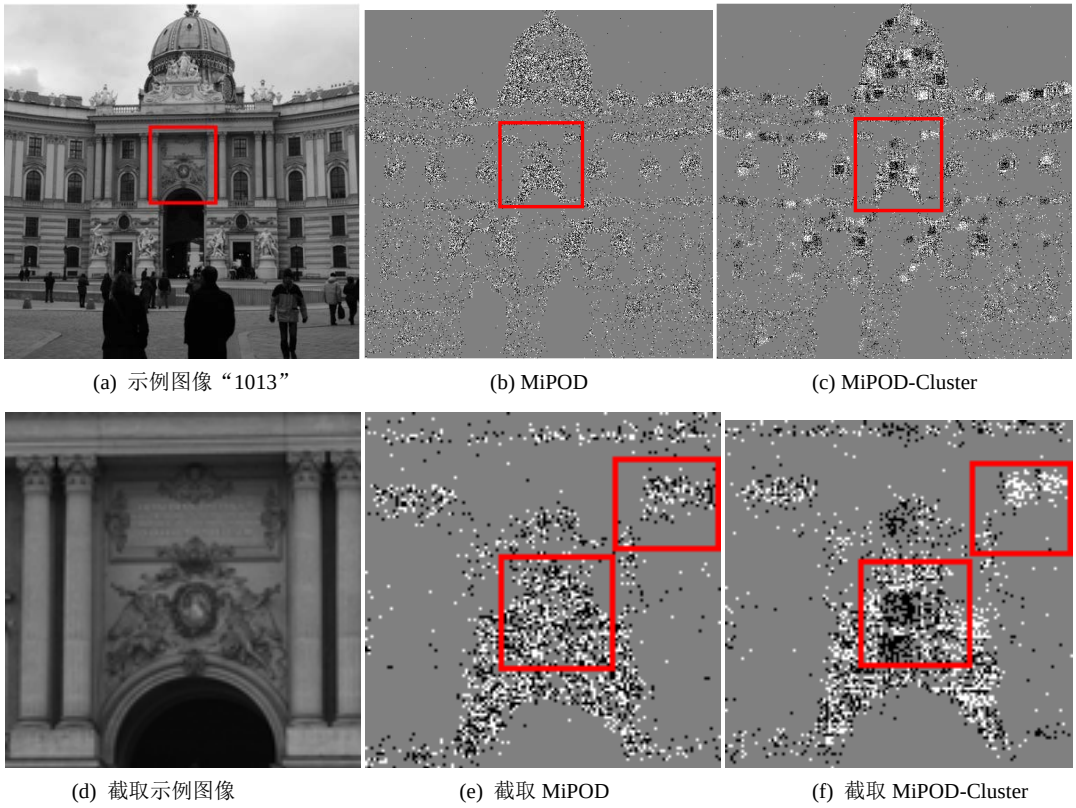
3.1.2. 修改聚集的处理效果对比

为了更直观地说明本文修改聚集方法的效果，本小节讨论 MiPOD-Cluster 与 MiPOD 处理隐写图像的差异。在图像库 BOSSbase1.01 [18]中选取其他文献[2] [22]中常用的编号为“1013”的图像作为示例图像，分别使用 MiPOD-Cluster 与 MiPOD 对这张图像嵌入 0.4 bpp 的秘密信息。

实验结果如图 2 所示，图 2(a)为示例图像，图 2(b)为 MiPOD 在示例图像嵌入秘密信息时被修改的像素，图 2(c)为 MiPOD-Cluster 在示例图像嵌入秘密信息时被修改的像素。图 2(d)~(f)分别为图 2(a)~(c)红框内截取的放大图。

图 2(e)与图 2(f)中，修改方向为−1 的像素显示为黑色，修改方向为+1 的像素显示为白色，修改方向为 0 时，也就是不做修改的像素显示为灰色，其中图 2(e)与图 2(f)的两个红框为两者有明显区别的区域。

对比图 2(a)与图 2(c)，图 2(a)的图像有一定的对称性，图 2(c)的像素修改方向从整体来看，也有一定的对称性，与图 2(a)的对称性相似。



(a) 示例图像“1013” (b) MiPOD (c) MiPOD-Cluster

(d) 截取示例图像 (e) 截取 MiPOD (f) 截取 MiPOD-Cluster

Figure 2. Comparison of pixel changed directions with MiPOD and MiPOD-Cluster
图 2. MiPOD 与 MiPOD-Cluster 的像素变化方向比较

由图 2(e)与图 2(f)对比可知，MiPOD-Cluster 的像素的同向修改方向都集中聚集在某个局部单位内，而 MiPOD 的像素修改方向基本是随机±1 的修改方式。对比两图中的红框区域，MiPOD-Cluster 的修改区域与修改方向相对集中，局部都为黑色像素或白色像素，而 MiPOD 的修改区域与修改方向相对分散。

由于本文算法 MiPOD-Cluster 使用了感知哈希算法[16]来计算图像部分区域的相似度，因此在图像内容比较对称的情况下，图像的聚集修改方向也有一定的对称性。本文修改聚集方法中使用的最小值滤波能够选取周围像素中修改代价最小的点，作为中心像素新的修改代价，利用它的原理，可以使最小值滤波选取周围像素中修改代价最小点的修改方向，作为中心像素新的修改方向。因此本文的修改聚集方法既能找到聚集区域，又能快速确定该区域的聚集修改方式。

由此可以得出结论：本文的修改聚集方法能有效改善 MiPOD 算法的像素修改方式。

3.2. 算法的安全性对比

本节讨论 MiPOD-Cluster、MiPOD、MVGG、MG 四种算法的安全性能。对比使用的隐写分析特征为 SRM 与 maxSRMd2，对比的项目为隐写分析的检错率，检错率越高，说明隐写算法的安全性越高。

由表 1 可知本文算法 MiPOD-Cluster 的抵抗 SRM 与 maxSRMd2 特征的检错率均高于其他三种现有算法，相比较三种现有算法中性能最好的 MiPOD，本文算法 MiPOD-Cluster 的检错率平均提升了 0.72%。

由图 3 可知，MiPOD-Cluster 在隐写负载较低时，其性能与 MiPOD 几乎相同，随着隐写负载的增加，MiPOD-Cluster 优于 MiPOD，并且它们之间的垂直差距逐渐增大。

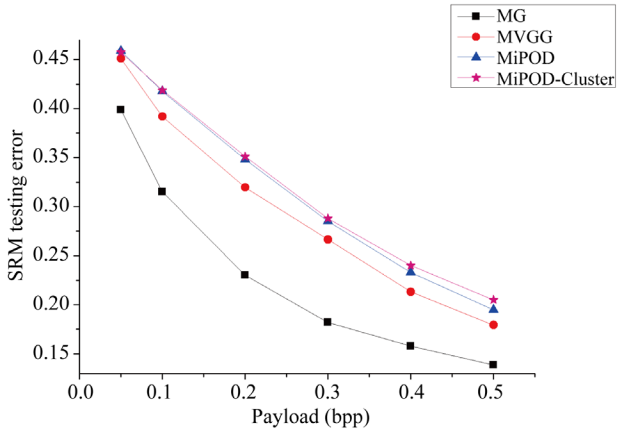
MiPOD-Cluster 与 MiPOD 的算法流程比较，MiPOD-Cluster 加入了修改聚集步骤，使其满足修改聚集原则，因此在隐写负载较高时，能够更合理地处理被修改像素的修改方向，使隐写图像更接近自然图

像，隐写安全性自然得到提高。

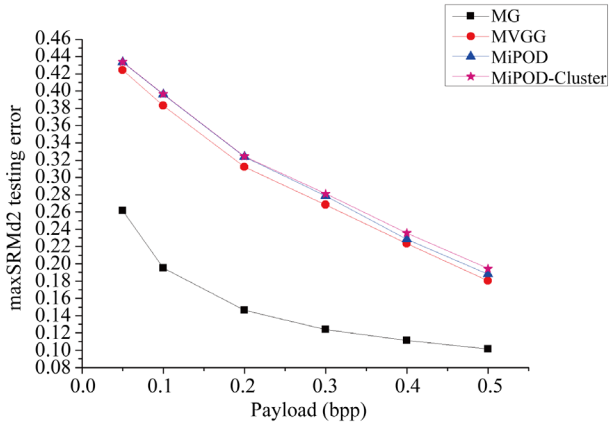
由此可以得出结论：引入修改聚集原则的 MiPOD-Cluster 算法的安全性能优于 MiPOD、MVGG、MG 三种效果较好的现有算法。

Table 1. Comparison results of testing error rate with four algorithms
表 1. 四种算法检错率的比较

对比项目	隐写方法	0.05 bpp	0.1 bpp	0.2 bpp	0.3 bpp	0.4 bpp	0.5 bpp
SRM 检错率 P_E	MG	0.3989	0.3153	0.2301	0.1821	0.1581	0.1386
	MVGG	0.4510	0.3919	0.3297	0.2465	0.2132	0.1794
	MiPOD	0.4588	0.4175	0.3483	0.2851	0.2331	0.1947
	MiPOD-Cluster	**0.4574**	**0.4186**	**0.3512**	**0.2881**	**0.2401**	**0.2049**
maxSRMd2 检错率 P_E	MG	0.2615	0.1953	0.1461	0.1236	0.1113	0.1015
	MVGG	0.4242	0.3832	0.3121	0.2684	0.2234	0.1803
	MiPOD	0.4331	0.3961	0.3236	0.2748	0.2283	0.1878
	MiPOD-Cluster	**0.4337**	**0.3966**	**0.3244**	**0.2810**	**0.2355**	**0.1945**



(a) 四种算法 SRM 检错率对比



(b) 四种算法 maxSRMd2 检错率对比

Figure 3. Comparison of testing error rates with four algorithms under SRM and maxSRMd2
图 3. 四种算法在 SRM 与 maxSRMd2 下的检错率对比

4. 结论

本文提出了一种基于最小值滤波与感知哈希算法的图像隐写算法(MiPOD-Cluster)。其中最小值滤波能够使 Fisher 信息矩阵出现局部区域数值相等的情况，并将此数值对应像素的修改方向作为整个局部区域的修改方向，达到局部修改聚集的目的。哈希感知算法则能通过计算载体图像不同区域之间的相似度，寻找图像相似的区域，并使两个相似区域有一样的修改聚集方式，达到整体修改聚集的目的。两种方法结合，能够使算法找到更准确的修改聚集区域与方式。实验证明，本文算法充分利用修改聚集原则，无论是抵抗 SRM 特征还是 maxSRMd2 特征，都有较好的安全性能。

致　谢

DDE 实验室的代码共享 http://dde.binghamton.edu/download/；匿名审稿老师对本文提出了宝贵的修改意见，在此表示感谢！

基金项目

本课题得到广西自然科学基金面上项目(No. 2017GXNSFAA198371)，广西大学科研基金(No. XGZ170107)资助。

参考文献

[1] Mukherjee, S. and Sanyal, G. (2019) Edge Based Image Steganography with Variable Threshold. *Multimedia Tools and Applications*, **78**, 16363-16388. https://doi.org/10.1007/s11042-018-6975-4

[2] Li, B., Tan, S., Ming, W., *et al*. (2014) Investigation on Cost Assignment in Spatial Image Steganography. *IEEE Transactions on Information Forensics & Security*, **9**, 1264-1277. https://doi.org/10.1109/TIFS.2014.2326954

[3] Tang, W., Tan, S., Li, B., *et al*. (2017) Automatic Steganographic Distortion Learning Using a Generative Adversarial Network. *IEEE Signal Processing Letters*, **24**, 1547-1551. https://doi.org/10.1109/LSP.2017.2745572

[4] Goodfellow, I.J., Pouget-Abadie, J., Mirza, M., *et al*. (2014) Generative Adversarial Nets. *International Conference on Neural Information Processing Systems*, 2672-2680.

[5] Tang, W., Li, B. and Tan, S. (2019) CNN Based Adversarial Embedding with Minimum Alteration for Image Steganography. *IEEE Transactions on Information Forensics and Security*, **14**, 2074-2087. https://doi.org/10.1109/TIFS.2019.2891237

[6] Holub, V. and Fridrich, J. (2012) Designing Steganographic Distortion Using Directional Filters. *International Workshop on Information Forensics and Security* (*WIFS*), Tenerife, Spain, 234-239. https://doi.org/10.1109/WIFS.2012.6412655

[7] Fridrich, J. and Kodovsky, J. (2013) Multivariate Gaussian Model for Designing Additive Distortion for Steganography: 2013 *IEEE International Conference on Acoustics*, Vancouver, 2949-2953. https://doi.org/10.1109/ICASSP.2013.6638198

[8] Sedighi, V., Fridrich, J. and Cogranne, R. (2015) Content-Adaptive Pentary Steganography Using the Multivariate Generalized Gaussian Cover Model. *Proceedings of SPIE-The International Society for Optical Engineering*, **9409**, 1-13. https://doi.org/10.1117/12.2080272

[9] Sedighi, V., Cogranne, R. and Fridrich, J. (2016) Content-Adaptive Steganography by Minimizing Statistical Detectability. *IEEE Transactions on Information Forensics & Security*, **11**, 221-234. https://doi.org/10.1109/TIFS.2015.2486744

[10] Li, B., Ming, W., Huang, J., *et al*. (2015) A New Cost Function for Spatial Image Steganography. 2015 *IEEE International Conference on Image Processing*, Quebec City, Canada, 27-30 September 2015, 4206-4210.

[11] Pevny, T., Bas, P. and Fridrich, J. (2010) Steganalysis by Subtractive Pixel Adjacency Matrix. *IEEE Transactions on Information Forensics & Security*, **5**, 215-224. https://doi.org/10.1109/TIFS.2010.2045842

[12] Pevný, T. and Fridrich, J. (2008) Benchmarking for Steganography. https://doi.org/10.1007/978-3-540-88961-8_18

[13] 郑传声. 基于最小化嵌入失真的空域图像隐写算法研究[D]: [硕士学位论文]. 北京: 北京邮电大学, 2018.

[14] Li, B., Ming, W., Li, X., *et al*. (2015) A Strategy of Clustering Modification Directions in Spatial Image Steganogra-

phy. *IEEE Transactions on Information Forensics & Security*, **10**, 1905-1917. https://doi.org/10.1109/TIFS.2015.2434600

[15] Subhedar, M.S. and Mankar, V.H. (2019) Image Steganography Using Contourlet Transform and Matrix Decomposition Techniques. *Multimedia Tools and Applications*, **78**, 22155-22181. https://doi.org/10.1007/s11042-019-7512-9

[16] 张立国, 王松, 金梅, 等. 基于多尺度感知哈希特征的目标跟踪算法研究[J]. 高技术通讯, 2018, 28(3): 39-46.

[17] Ker, A.D. (2009) Estimating Steganographic Fisher Information in Real Images. In: Katzenbeisser, S. and Sadeghi, A.R., Eds., *Information Hiding. IH* 2009. *Lecture Notes in Computer Science*, Volume 5806, Springer, Berlin, Heidelberg, 73-88. https://doi.org/10.1007/978-3-642-04431-1_6

[18] Bas, P., Filler, T. and Pevný, T. (2011) Break Our Steganographic System: The Ins and Outs of Organizing BOSS. In: *Proceedings of International Conference on Information Hiding*, Prague, Czech Republi, Springer-Verlag, Berlin, 58-70. https://doi.org/10.1007/978-3-642-24178-9_5

[19] Kodovský, J. and Fridrich, J. (2012) Rich Models for Steganalysis of Digital Images. *IEEE Transactions on Information Forensics and Security*, **7**, 868-882. https://doi.org/10.1109/TIFS.2012.2190402

[20] Denemark, T., Sedighi, V., Holub, V., *et al*. (2014) Selection-Channel-Aware Rich Model for Steganalysis of Digital Images. 2014 *IEEE International Workshop on Information Forensics and Security* (*WIFS*), Atlanta, GA, 48-53. https://doi.org/10.1109/WIFS.2014.7084302

[21] Kodovský, J., Fridrich, J. and Holub, V. (2012) Ensemble Classifiers for Steganalysis of Digital Media. *IEEE Transactions on Information Forensics & Security*, **7**, 432-444. https://doi.org/10.1109/TIFS.2011.2175919

[22] Abdulla, A.A., Sellahewa, H. and Jassim, S.A. (2019) Improving Embedding Efficiency for Digital Steganography by Exploiting Similarities between Secret and Cover Images. *Multimedia Tools and Applications*, **78**, 17799-17823. https://doi.org/10.1007/s11042-019-7166-7