基于LSB匹配重访问的边缘自适应图像隐写技术

使用pandoc得到docx文档

pandoc -o h.docx -s -S --bibliography=transref.bib --  
csl ieee.csl readme.md

## 摘要

基于最低有效位（LSB）方法是一种在空间域中流行的隐写算法。然而，我们发现在大多数现存的方法中，对于载体图片的嵌入位置的选择取决于伪随机数生成器，而没有考虑图片内容本身和密文大小的关系。所以，即使数据以非常低的嵌入率隐藏后，载体图片中的光滑/平坦区域也很容易被污染，这会导致在我们的分析和扩展试验中，尤其是含有较多光滑区域的图片中，出现较差的视觉质量和安全表现。在这篇文章中，我们将拓展LSB匹配重访问图像隐写技术并提出一种可以根据密文大小和载体图片中连续两个像素之间的差异选择嵌入位置的边缘自适应模式。对于更低的嵌入率，只有使用更尖锐的边缘区域才能同时维持平滑区。当嵌入率增大时，只需要调整几个参数就可以自适应地释放更多的边缘区域用于数据隐藏。在6000张自然图片上使用三种特定的和四种通用的隐写分析算法得到的实验结果表明，对比典型的基于LSB方法以及它们对应的边缘适应方法，比如基于像素值差异的方法，新模式可以显著增强安全性，同时保证隐秘图像的视觉质量较高。

### 索引词

基于内容的隐写术，基于最低有效位（LSB）的隐写术，像素值差（PVD），安全，隐写分析

## 1. 介绍

隐写术是一种信息隐藏技术，旨在将隐秘数据嵌入数字载体媒体而不引起怀疑，比如数字音频，图像，视频等。另一方面，隐写分析则旨在发现这些伪装媒体中隐藏的秘密消息。如果存在一种能以比随机猜测的概率更高的概率猜出一个给定的媒体是否是载体的隐写分析算法，那么这个隐写系统就被认为是被攻破了。在实践中，两个熟悉，不可探测性和嵌入容量，在设计隐写算法时应该被慎重考虑。通常来说，在载体中的负载嵌入越大，伪装中可探查到的人为迹象越多。在许多应用中，对于隐写来说最重要的需求就是不可探查，这意味着伪装应该在尽可能高嵌入率的同时在视觉和统计意义上与载体相似。这篇文章中，我们考虑数字图片作为载体并研究一种在空间最低有效位（LSB）域自适应的安全数据隐藏模式。

LSB替换是一种著名的隐写方法。在这种嵌入模式中，只有载体的LSB平面依据伪随机数生成器被秘密比密文比特流重写。因此，一些结构性的对称（在隐藏数据时）从不较少偶数像素和增加奇数像素被引入，致使在低嵌入率的情况下，即使使用一些公开算法，比如攻击[1]，R/S块分析[2]，样本对分析[3]，和广义上的结构性隐写分析框架[4]，[5],也很容易探查到隐藏消息的存在。

LSB匹配（LSBM）对于LSB代替做了一些微小的修改。如果秘密位不匹配载体图片的LSB，那么就在对于的像素值上随机加或者。统计意义上而已，对于每个改变的像素值增大和减小的概率是相等的，因此由LSB代替引入的明显的对称的人工迹象可以很容易被避免。因此，常见的侦测LSB代替的方法都在侦测LSBM时无效。到现在为止，几种分析算法（如[6]–[9]）被提出用于分析LSBM机制。在[6]中，[6]演示了LSBM作为低通过滤器在图像上的直方图，说明了相比载体，伪装图片的直方图包含少的高频成分。基于这个特性，作者引入了一种使用直方图特征函数（HCF）的质心（COM）的探测器。在[7]中，Ker指出原始的HCF COM方法在灰度图像上效果不佳并引入了两种应用HCF COM方法的途径，称之为利用下采样图像和以邻接直方图代替传统直方图，它们在由达到58的低质量因数压缩JPEG图像而成的灰度图像上非常有效。在近期的工作[li2008detecting]中，Li等人提出在不同的图像上计算基于刻度的探测器，如刻度HCF COM。实验结果表明新的探测器优于Ker在[7]中的方法，并且达到了50%的可以接受的准确率。在[8]中，Huang等人调研了这些包含图像前两比特的子图中的小量重叠部分的统计特征并提出另一种基于邻接像素值的可替换率的分析方法。实验结果表明这种方法对于未经压缩的灰度图像更有效。除了这些特定的探测器，一些通用的分析算法如[10]，[11]和[12]也能以相对较高的探测率暴露使用LSBM和/或其他隐写方法的伪装图像。

和LSB替换以及LSBM这些独立处理像素值的方法不同，LSB匹配重访问使用像素对作为嵌入单元，第一个像素的LSB携带了一比特的密文，两个像素值的关系（奇偶组合）携带了另一比特密文。在这种方式下，就最高嵌入率 而言，像素的更改率可以从0.5下降到0.375比特/像素（bpp），也就是说相比LSB替换和LSBM在相同的负载下对于载体图像的改变更少。这说明了这样一种新模式可以避免LSB替换风格的对称，也因此在我们的试验中它比LSBM略微难以探测一些。

典型的基于LSB的方法，包括LSB替换，LSBM和LSBMR，处理每个给定的像素/像素对时不考虑与像素与它的邻接像素的差异。直到现在，对几种边缘适应机制如[13]–[18]进行研究，在[13]中Hempstalk提出了根据一个像素与它周围的四个像素值的差值替换LSB的机制。尽管这种方法可以在较锐利的边缘嵌入最多的秘密数据并成为了视觉上更不易被察觉的伪装（见图1和表1），但是安全表现太弱。因为此方法在隐藏数据时只修改LSB，很容易被现有的隐写分析算法，比如RS分析（请参见C1小节)探测出来。在[14]中，Singh等作者提出一种嵌入方法，先在载体的每个不重叠的区域上部署Laplacian探测器来探测边缘，再根据一个阈值选出更锐利的边缘，在这些边缘上的区域的中心像素进行数据隐藏。如[14]所述，这种方法的嵌入容量相对较低（）。不仅如此，阈值 也需要预先决定所以不能根据图像内容和要嵌入的消息自适应地改变。基于像素值差（PVD）的机制（如[16]–[18]）是另一种边缘自适应机制，嵌入像素的数量由一个像素和它的邻接像素的差值决定。差值越大，能被嵌入的秘密比特越多。通常来说，基于PVD的方法可以提供更大的嵌入容量（平均来说超过1bpp）。然而基于我们的扩展实验，我们发现现有的PVD方法未能充分利用边缘信息进行数据隐藏，而且在对抗一些统计分析方面也很弱。

[1] A. Westfeld and A. Pfitzmann, “Attacks on steganographic systems,” in *Information hiding*, 1999, pp. 61–76.

[2] J. Fridrich, M. Goljan, and R. Du, “Reliable detection of lSB steganography in color and grayscale images,” in *Proceedings of the 2001 workshop on multimedia and security: New challenges*, 2001, pp. 27–30.

[3] S. Dumitrescu, X. Wu, and Z. Wang, “Detection of lSB steganography via sample pair analysis,” *Signal Processing, IEEE Transactions on*, vol. 51, no. 7, pp. 1995–2007, 2003.

[4] A. D. Ker, “A general framework for structural steganalysis of lSB replacement,” in *Information hiding*, 2005, pp. 296–311.

[5] A. D. Ker, “A fusion of maximum likelihood and structural steganalysis,” in *Information hiding*, 2007, pp. 204–219.

[6] J. J. Harmsen and W. A. Pearlman, “Steganalysis of additive-noise modelable information hiding,” in *Electronic imaging 2003*, 2003, pp. 131–142.

[7] A. D. Ker, “Steganalysis of lSB matching in grayscale images,” *Signal Processing Letters, IEEE*, vol. 12, no. 6, pp. 441–444, 2005.

[8] F. Huang, B. Li, and J. Huang, “Attack lSB matching steganography by counting alteration rate of the number of neighbourhood gray levels,” in *Image processing, 2007. iCIP 2007. iEEE international conference on*, 2007, vol. 1, pp. I–401.

[9] X. Li, T. Zeng, and B. Yang, “Detecting lSB matching by applying calibration technique for difference image,” in *Proceedings of the 10th aCM workshop on multimedia and security*, 2008, pp. 133–138.

[10] Y. Q. Shi, D. Zou, W. Chen, C. Chen, and others, “Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network,” in *2005 iEEE international conference on multimedia and expo*, 2005, p. 4.

[11] B. Li, J. Huang, and Y. Q. Shi, “Textural features based universal steganalysis,” in *Electronic imaging 2008*, 2008, pp. 681912–681912.

[12] M. Goljan, J. Fridrich, and T. Holotyak, “New blind steganalysis and its implications,” in *Electronic imaging 2006*, 2006, pp. 607201–607201.

[13] K. Hempstalk, “Hiding behind corners: Using edges in images for better steganography,” in *Proc. computing women’s congress, hamilton, new zealand*, 2006, vol. 14.

[14] K. M. Singh, L. S. Singh, A. B. Singh, and K. S. Devi, “Hiding secret message in edges of the image,” in *2007 international conference on information and communication technology*, 2007.

[15] M. D. Swanson, B. Zhu, and A. H. Tewfik, “Robust data hiding for images,” in *Digital signal processing workshop proceedings, 1996., iEEE*, 1996, pp. 37–40.

[16] D.-C. Wu and W.-H. Tsai, “A steganographic method for images by pixel-value differencing,” *Pattern Recognition Letters*, vol. 24, no. 9, pp. 1613–1626, 2003.

[17] X. Zhang and S. Wang, “Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security,” *Pattern Recognition Letters*, vol. 25, no. 3, pp. 331–339, 2004.

[18] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, “Adaptive data hiding in edge areas of images with spatial lSB domain systems,” *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 3, pp. 488–497, 2008.