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[9]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）[13]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[14]–[19]进行研究，在[14]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[15]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[15]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[17]–[19]）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。

大多数上述的隐写方法的一个共同特征就是像素/像素对的选择主要取决于一个PRNG而忽视了图像内容和密文大小的关系。如此操作，这些方法甚至可以以很低的嵌入率将密文随机地在整个伪装图像上分散。然而，基于我们的分析和扩展实验，我们发现这样的嵌入机制在伪装图片的安全和视觉质量上表现欠佳。假设一个图像由不重叠的小子图（区域）按照一个预先决定的规则组成，不同的区域通常有不同的隐藏消息的容量。与载体图片的选择问题相似[20]，我们应该优先选择那些有良好的隐藏特征的子图，同时不对其他子图作出任何改变。因此，决定如何选择区域是我们提出的机制的关键。一般来说，在较锐利的边缘的区域表现出更复杂的统计特征，并且对于图像内容高度依赖。不仅如此，与平滑区相比，锐利的边缘更难察觉出变化。

在这篇文章中，我们提出一种边缘自适应的机制并且将其应用于基于LSBMR的方法。在上千张图像上使用数种隐写分析算法进行评价得到的实验结果体现了新方法的优越性。

这篇文章余下的部分如下安排。节2分析相关隐写机制的局限并提出一些策略。节3展示在我们的机制中数据嵌入和数据提取的细节。节4给出实验结果和讨论。最后，在节5给出总结评价和未来的工作。

## 2.相关方法和策略的局限分析

在本节，我们首先给出对于典型的基于LSB的方法，包括LSB替换，LSBM, 和LSBMR，以及包括原始PVD机制[17]，PVD的优化版本（IPVD)[18]，自适应边缘的LSB（AE-LSB）[19]和隐藏在角落（HBC）[14]在内的一些自适应机制的简要综述，然后展示一些图像来暴露这些机制的局限。最后我们提出一些策略来克服这些局限。

在LSB替换和LSBM方法中，植入过程非常相似。给定一个秘密比特流用以嵌入，PRNG就会生成一个在载体图片的访问顺序，然后分别处理访问顺序上的每一个比特。对于LSB替换，秘密比特重新了像素的LSB，即第一个比特平面，同时保留更高位的比特平面（2~8）。对于LSBM机制，如果秘密比特不等于给定的像素的LSB，那么这个像素就随机地增加同时保持改变的像素值在范围内。在这样的方法中，用LSB替换和LSBM隐藏数据后，访问顺序中的像素的LSB会和秘密比特流匹配。因此，两种方法的提取过程完全相同，先根据共享秘钥生成相同的访问顺序，然后检查像素值的对等比特就能正确提取隐藏的消息。

LSBMR应用载体图像中的一对像素对作为嵌入单元。消息嵌入后，伪装图片中修改后的单元满足

其中函数为像素值的LSB,和是需要嵌入的两个秘密比特。

通过邻接像素的关系（奇偶组合），对比同嵌入率的LSB替换和LSBM，LSBMR的像素改变率降低。类似地，数据提取时，首先使用共享秘钥用PRNG生成一个访问顺序。然后对于访问顺序的每个嵌入单元可以提取两比特。第一个秘密比特的值就是第一个像素值的LSB，进而第二个比特可以通过上述方法计算两个像素的关系。

我们人类的视觉对于光滑区的微小改动很敏感，却可以容忍边缘区域的剧烈变化。几种基于PVD的方法如[17]–[19]提议增加嵌入容量而不在伪装图片中引入明显的人工痕迹。基于PVD方法的基本思想是首先把载体图片划分为多个不重叠的含有两个连续像素的单元，然后处理由PRNG生成的随机顺序上的嵌入单元。两个像素间的差值越大，可植入该单元的秘密比特越多。在一定程度上，现有的基于PVD的方法是边缘自适应的，因为在那些拥挤的边缘区域被植入的秘密比特更多。然而，与LSBM和LSBMR相似的是，像素对的选择主要依赖于PRNG，也就是说改变的像素仍然会分布于整个伪装图片如图1所示。我们可以看到许多平滑区在数据隐藏后也不可避免地发生了改变，即使两个连续像素间的差值是零（意味着子图在平坦区上），同时许多锐利的边缘区域却未充分利用。

大多数现有的隐写分析算法通常假设自然载体的LSB不够重要和随机，因此那些那些用于数据隐藏的像素/像素对是使用PRNG自有地选择出来的。但是，这样的假设不是一直正确，尤其是对于包含很多平滑区的图像。图2显示了这些图例的LSB平面。我们可以观察到LSB在一定程度上可以反映图像的纹理信息。在扩展实验中，我们发现未经压缩的自然图像通常包含一些平坦区（可能只有大小而且很难注意到），LSB在那些区域的值相同（或）。因此，如果我们将秘密比特嵌入这些区域，伪装图像的LSB会变得越来越随机，可能如图3所示产生载体（包含平坦区域/纹理信息）和伪装图像（看上去像噪声分布）的LSB之间视觉和统计上的差异。

与平滑区相比，位于边缘区域像素的LSB通常表现出更随机的特征，它们在统计上与秘密比特的分布（假设是一个均匀分布）更相似。所以，我们希望数据隐藏后边缘区域留下了更少的可探测的和视觉上的人工痕迹。不仅如此，边缘信息（比如位置和统计矩）高度依赖于图像内容，使得探测更为困难。这就是为什么我们提出的机制首先尽可能地将秘密比特嵌入边缘区域而不改变平滑区域。如图1所示，我们发现HBC方法[14]有这种属性。但是HBC方法只修改LSB二保持最关键的比特位不变，所以它可以被视为LSB替换的一种边适应的情况，LSB替换式的对称在他们的方法中仍会存在。我们将在IV-C1小节给出一些实验证据来暴露HBC方法的局限。

请注意我们在这篇文章中没有评价JPEG图片的安全性。原因是JPEG图像中所有不重叠的区域都经过了有损耗的JPEG压缩后按照一定规律重排。如果在JPEG解压图像上使用空域隐写分析方法必然会出现JPEG不兼容[21]，也就是附加秘密数据将毁坏之前使用量化表的JPEG压缩引入的特有的指纹。我们甚至可以从JPEG伪装图片中短到一比特的数据中探测到可能的隐藏消息。

## 3.建议机制

我们的建议机制的流程图如图4所示。在数据嵌入阶段，先初始化一些用于后续数据处理和区域选择的参数，然后估测这些选择区域的容量。如果区域大到足够隐藏给定的密文,那么就在这些选出的区域上进行数据隐藏。最后，我们做一些后处理得当伪装图片。否则，我们的方法需要修改这些参数，然后重复区域选择和容量估测直至能完全被嵌入。

请注意对于不同的图片内容和密文，这些参数也可能不同。我们需要把它们作为辅助信息来保证数据提取的有效性，在实践中，可以将这样的辅助信息（我们的工作中是7比特）嵌入图像中预先选出的区域。

在数据提取中，这样的机制首先从伪装图片中提取这些辅助信息。基于这些辅助信息，我们可以做一些预处理并辨别出有隐藏数据的区域。最后，根据对应的提取算法可以得到密文。

在这篇文章中，我们对空间LSB域使用这样的一种区域自适应机制。我们使用两个邻接像素的绝对差作为区域选择的准则，并使用LSBMR作为隐藏算法。数据嵌入和提取算法的细节如下。

### 数据嵌入

* 第一步：先将大小为的载体图片划分为像素的不重叠区域块。 对于这些小区域块，我们根据秘钥以范围为的角度随机旋转它，得到的结果图像被行式扫描重排为一个行向量。接下来这个向量被划分成包含两个连续像素的不重叠的嵌入单元，其中，假设是一个奇数。 随机旋转有两个益处。首先，它可以防止探测器在没有旋转秘钥的前提下获得正确的植入单元，因此安全性得到提升。除此之外，载体图像中水平和垂直的边缘（像素对）都可以用于隐藏数据。
* 第二步：根据LSBMR机制，每个嵌入单元可以嵌入2比特密文。因此，对于一个给定的密文，区域选择的阈值可以以如下的方式决定。令表示绝对差大于参数的像素对的集合
* 然后我们这样计算阈值
* 其中，是密文的大小，是集合中元素的总数。 注意当时，建议方法就成为了常规的LSBMR机制，意味着我们的方法达到了LSBMR相同的负载容量（除了7比特）
* 第三步：在集合上进行数据隐藏
* 我们用秘钥决定的伪随机顺序处理上述的嵌入单元。对于每一个单元，我们根据下面的四种情况进行数据隐藏：
* 其中和表示被嵌入的两个秘密比特，函数定义为，是中的一个随机值，表示数据隐藏后的像素对。 上述修改后，和可能超出了，或者新的差重新调整，最后，我们得到
* 其中,。解的存在性证明请参见附录。
* 第四步：数据隐藏后，结果图像被分成不重叠的区域块，然后将区域块按照根据生成的随机的角度旋转。这个过程与第一步非常相似，除了随机角度是相反的。接下来我们在没有用于隐藏数据的一个预先设置的区域嵌入两个参数

注意我们的方法有两个参数。第一个是数据预处理时用于区域划分的区域块大小，另一个是嵌入区域选择使用的阈值。在这篇文章中，是从集合中随机选出。属于并由图像内容和密文（请参加第二步）。总之，每个图像只需要7（）比特的辅助信息。

这里给出一个例子。假设我们处理嵌入单元，，，。易得和

因此，我们调用Case#4得到

新的差变成，我们根据公式重新调整它们最后得到,

在这里，我们有和

### 数据提取

为了提取数据，我们先从伪装图片提取辅助信息，即区域分块大小和阈值。然后我们做的工作和数据嵌入的第一步完全相同。伪装图像被划分为的分块区域，分块根据秘钥生成的随机角度旋转。结果图像重排为一个行向量，最后，我们通过把划分为不重叠的两个连续的像素得到嵌入单元。

我们根据由秘钥生成的伪随机顺序遍历绝对差大于等于阈值的嵌入单元，直至所有的隐藏比特都被完全提取。对于每个合格的嵌入单元，也就是满足的，我们这样提取两个秘密比特:

，例如，我们处理单元，，我们最终这样得到秘密比特

[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] J. Mielikainen, “LSB matching revisited,” *Signal Processing Letters, IEEE*, vol. 13, no. 5, pp. 285–287, 2006.

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

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] M. Kharrazi, H. T. Sencar, and N. Memon, “Cover selection for steganographic embedding,” in *Image processing, 2006 iEEE international conference on*, 2006, pp. 117–120.

[21] J. Fridrich, M. Goljan, and R. Du, “Steganalysis based on jPEG compatibility,” in *ITCom 2001: International symposium on the convergence of iT and communications*, 2001, pp. 275–280.