第 34 卷 第 8 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.8 Computer Engineering April 2008
·安全技术· 文章编号：1000—3428(2008)08—0167—03 文献标识码：A 中图分类号：TP309.2

大容量的信息隐藏算法

谢建全[1,2]，阳春华[1]
(1. 中南大学信息科学与工程学院，长沙 410083；2. 湖南财经高等专科学校，长沙 410205)

摘 要：提出一种基于空间域的自适应多平面位的信息隐藏算法，该算法计算复杂度低、信息隐藏量大。实验表明在不影响图像视觉效果的前提下，其信息隐藏量比 LSB 算法大，并具有更高的安全性。该算法的主要思想是对每个像素点进行判断，根据 HVS 的特性，在最高非 0 有效位后的指定位(y)开始嵌入隐藏信息，嵌入到另一个指定位(z)为止。

关键词：信息隐藏；数字水印；空间域

High Capacity Information Hiding Algorithm

XIE Jian-quan[1, 2], YANG Chun-hua[1]
(1. School of Information Science and Engineering, Central South University, Changsha 410083;
2. Hunan Finance and Economics College, Changsha 410205)

【Abstract】A hiding information algorithm of adaptive multiple plane-bit based on space domain is proposed ,which has low computing complexity and large information capacity hidden. Experimental results show hiding information capacity of this algorithm is much larger than LSB algorithm, and security is much higher than LSB algorithm. It's main idea is to judge every pixel point so that hiding information will be embedded from specified bit (y) behind the highest non-zero effective bit until another specified bit (z) according to HVS's property.

【Key words】 information hiding; digital watermark; space domain

信息隐藏的目的在于保证隐藏的信息不引起攻击者的注意，从而减少被侵犯的可能性，摆脱数据加密技术的致命缺陷。目前用来作为信息隐藏的载体有文字、图像、语音或视频等多种不同格式的文件，但使用的方法没有本质区别。其中图像由于冗余空间大，是目前用于隐藏储存和隐蔽通信最多的信息隐藏载体。在隐藏储存和隐蔽通信中，研究者的目标是在满足隐藏信息的视觉不可感知性的前提下尽可能多地隐藏信息。本文提出一种新的空间域信息隐藏方法，最大限度地利用所有可能的冗余空间，达到大容量隐藏信息的目的。

1 LSB 算法特点分析

基于图像的信息隐藏技术，可以归类于基于变换域的隐藏技术和基于空间域的隐藏技术两种。基于空间域的隐藏技术是直接改变图像元素的值，一般是在图像的亮度或色度中加入隐藏的内容。最简单和有代表性的基于空间域的信息隐藏方案是将要隐藏的信息代替图像的最低有效位(LSB)或者多个不重要位平面的所有比特的算法，这里的隐藏信息指的是二值比特序列。由于每个像素的最低位的变化对颜色的视觉影响很小而无法察觉，因此可以把最低位(最小意义位) 视为冗余空间，把信息隐藏在这里。1993 年，Tirkel 等人[1]提出了数字图像水印的一种方法，该方法将 m 序列的伪随机信号以编码形式的水印嵌入到灰度图像数据的 LSB 中。为了能得到完整的 LSB 位平面而不引入噪声，图像通过自适应直方图处理，首先将每个像素值从 8 bit 压缩为 7 bit，然后将编码信息作为像素值的第 8 个比特(即像素值的 LSB)，这一方法是单个 LSB 编码方法的扩展，在单个 LSB 编码方法中，LSB 直接被编码信息所代替。LSB 算法的嵌入比为 12.5%，是目前公认信息隐藏量大的一种算法，同时还有算法简单、嵌入速度快等优点，这些优点是基于变换域的隐藏算法所无法比拟的，因此 LSB 算法仍然在信息隐藏中占有重要地位，几乎全部的隐写算法中都可以找到 LSB 算法的影子，Internet 上常见的隐写软件中也大都使用 LSB 算法或 LSB 的衍生算法[2]。由于使用了图像最不重要的像素位，因此算法的鲁棒性较差，嵌入信息很容易受到滤波、图像量化、几何变形和加噪等操作的攻击。

针对 LSB 算法出现的缺陷，研究人员对空域图像水印技术进行了改进，使算法的稳健性和安全性得到了提高。文献[3]提出通过颜色量化的方法实现的，使原来需要 8 位来表示的 256 色图像量化到颜色数 128 色，量化后的图像只用 7 位来表示，剩余的那位(最高位)就可以作为冗余空间来存储隐藏信息。由于此时所用的冗余空间为最高位，也称最大意义位(MSB)，因此鲁棒性较好，解决了 LSB 算法鲁棒性差的问题，但该方法的缺点是嵌入后的图像的调色板大小发生改变，而且对于原本 256 色的图像量化后时，由于存在量化误差，图像的视觉质量会有不同程度的降低，其中最为严重的是在均匀渐变区域出现的伪轮廓，因此，必须降低质量才有可能实现信息嵌入[4]。人们在使用 LSB 算法时，希望在不影响载体视觉效果的前提下，提高其鲁棒性，并进一步提高其信息隐藏的能力，因此以上算法均需要改进。

2 本文算法

以图像为载体进行信息隐藏时，可看为在强背景(原始图像)下叠加一个弱信号(被隐藏的信息)，只要叠加的信号低于

基金项目：国家自然科学基金资助项目(60574030)；湖南省教育科学“十一五”规划课题(XJK06CXJ012)
作者简介：谢建全(1964－)，男，教授，主研方向：信息安全技术；阳春华，教授、博士生导师
收稿日期：2007-05-05 **E-mail：**xiejianquan@sina.com

对比度门限，视觉系统就无法感觉到信号的存在[5]。根据 HVS 的对比度特性，该门限值受背景照度、背景纹理复杂性和信号频率的影响。背景越亮，纹理越复杂(或者说边缘丰富)，门限就越高[5-6]，这类现象称为亮度掩蔽和纹理掩蔽。根据人类视觉掩蔽特性可知：具有不同局部性质的区域在保证不可见性的前提下，可允许叠加的信号强度是不同的。对 RGB 彩色图像而言，人类视觉系统对 LSB 位不可感知的，但并不是只有对 LSB 位不可感知，对于较亮的像素点，比 LSB 更高的某些位的变化同样是不可感知的，这些不可感知位同样可用来嵌入信息，从而进一步提高嵌入容量。利用以上 HVS 特性，本文提出多平面自适应隐藏方法，可获得较大的信息隐藏空间和较好的鲁棒性。其基本思路是根据每个像素点 RGB 3 个颜色分量的亮度值的不同，确定是否隐藏信息、信息隐藏位置及信息的隐藏量。具体算法如下：

设 24 位的 RGB 彩色图像每个像素 RGB 3 个颜色分量分别为(r_i,g_i,b_i)，其中，i={7, 6, …,0}，对图像的每个像素点 RGB 三色的每一色进行单独嵌入处理。首先对红色分量进行处理，将($r_7,r_6,r_5,r_4,r_3,r_2,r_1,r_0$)从高位至低位逐位进行检查，当第 x 位不为 0 时，则从第 x-y 位($y\geq 1$)开始嵌入信息，一直嵌入到第 z 位，若 $z>x-y$，则该像素点的该分量不嵌入信息，即：

$$r_i^*=\begin{cases} w_j & z\leq i\leq x-y \\ r_i & \text{其他} \end{cases}$$

其中，r_i^* ($i\in\{0,1,\cdots,7\}$)为该像素点红色分量第 i 位 r_i 经过嵌入处理后的值；w_j ($j\in\{1,2,\cdots,L\}$)为待嵌入的比特序列，j 的值为前面已经嵌入的比特数，每嵌入 1 个比特 j 的值增加 1；y 的取值决定了嵌入强度，它需要在不可感知性和嵌入容量之间折中考虑，y 值越大，视觉不可感知性越好，但可隐藏的信息量越少；z 的取值由所需的抵御滤波处理的鲁棒性决定，当 z=0 时，则包括 LSB 位。处理完红色分量后，再用同样的方法处理该像素的蓝色和绿色分量，只是对蓝色和绿色分量，y 的取值可以根据人类视觉系统特性取不同的值。处理完一个像素点后，再用同样的方法处理下一个像素点，不断重复以上过程，直到所有像素点处理完毕。本算法提取信息非常简单，只要提取每个像素点的第 x-y 位至第 z 位的信息即可。

设背景照度为 I，根据 Weber 定律[7]，在均匀背景下，人眼刚好可以识别的物体照度为 $I+\triangle I$，其中$\triangle I\approx 0.02\times I_0$。视觉领域的进一步研究表明，$\triangle I$ 与 I 的关系更接近指数关系[8]。有文献提出了更准确的对比度敏感度函数：

$$\Delta I=I_0\times\max\{I,(I/I_0)^{\alpha}\}$$

其中，I_0 为当 I=0 的对比度门限；$a\in(0.6, 0.7)$为常数。

根据以上结论，y 的取值为 4~5 时就可基本满足视觉不可见性要求，实验结果也证实如此。由于人眼对 RGB 三色的敏感度是不同的，人眼可感知的亮度值可由如下的公式计算：

$$L=0.299R+0.587G+0.114B$$

可见人眼对绿色最敏感，对蓝色最不敏感，它不到绿色的 1/4，因此为了达到不可感知性的目的，在 y 值的选取上，绿色需要适当取大一点，蓝色分量的值则可取小一点。

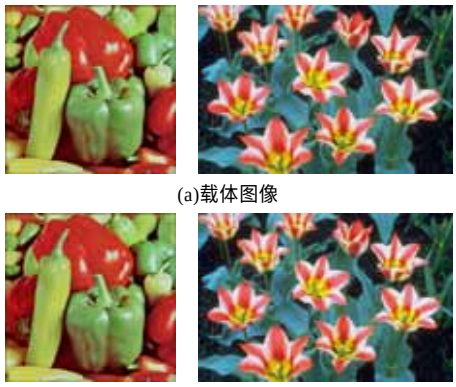
3 试验与讨论

以 512×512×24 的原始 Lena 图像为载体进行试验，首先试验本算法的最大信息嵌入量，z 的值设为 0，设 RGB 三色所对应的 y 的取值为(yr,yg,yb)，这 3 个值分别选取(5,5,4), (4,5,4), (4,4,4), (4,5,3)和(3,5,3)5 组不同的值进行嵌入试验，嵌入后的结果分别如图 1(b)~图 1(f)所示。由试验结果可知，当 $yr\geq 4$, $yg\geq 5$, $yb\geq 3$ 时，对人类的视觉系统而言是不可感知的，超过这个值时就会影响视觉效果，即(yr,yg,yb)取(4,5,3)时，隐藏的信息的不可感知性就能满足要求，此时达到可隐藏信息量的最大值。

(a) 原始图像　(b)组 1　(c)组 2　(d)组 3　(e)组 4　(f)组 5

图 1　yr,yg,yb 取值对视觉效果的影响比较

选取标准图像 peppers 和 tulips 进行试验，当 yr,yg,yb 分别取 4, 5, 3 时，嵌入信息后的载密图像如图 2 所示，可见在嵌入隐藏信息后同样能满足视觉的不可感知性要求。



(a)载体图像　(b)载密图像

图 2　yr=4, yg=5, yb=3 时另两组载体图像与载密图像

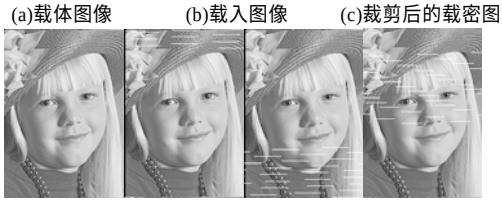
当 yr,yg,yb 分别取 4, 5, 3 时，在 Lena, peppers 和 tulips 图像中可嵌入的信息量见表 1，嵌入比平均值约为 36%，在同样满足视觉不可见性的前提下，而目前认为信息隐藏量大的 LSB 算法的嵌入容量的嵌入比固定为 12.5%，可见本算法的可嵌入的容量比 LSB 算法大很多，同时由于不像 LSB 算法那样将信息嵌入在一个固定的平面位，可防止位平面过滤所导致的失密，因此比 LSB 算法具有更高的安全性。用本算法进行信息提取时只依赖参数 y 和 z，不需要原始图像及辅助信息表等其他信息，是一种完全意义的盲提取。

表 1　yr,yg,yb 分别取 4,5,3 时可嵌入数据容量

图像名	图像大小	可嵌入数据容量/bit	嵌入比/(%)
Lena	512×512	2 576 953	40.9
peppers	512×512	2 253 506	35.8
tulips	768×512	3 227 134	34.2

用 Lena 图像嵌入一幅如图 3(b)所示的 181×252×8 的灰度图像进行剪裁试验，将载有隐藏信息的图像进行如图 3(c)所示的随机裁剪，然后进行隐藏信息的提取，提取的图像如图 3(d)所示，说明本算法有较强的抗剪裁能力。由于本算法的嵌入容量大，同小容量的嵌入算法相比，对于同样的嵌入信息可进行反复的嵌入，一幅载体图片可嵌入多个水印信息，因此抗剪裁能力强。再进行抗干扰试验，在嵌入隐藏信息的图像上加入 0.02 的椒盐噪声，检测到的隐藏图像如图 4(b)所示，虽然检测到的隐藏图像也有明显的噪声干扰信息，但仍可正常识别，可见本文算法有一定的抗噪声干扰能力，作为隐藏图像之类的水印是能满足要求的。另外当 z 取 1 时(即 LSB 位不隐藏信息)进行滤波试验，仍以 Lena, peppers 和 tulips 作为载体，载密图像进行中值滤波处理后，仍可检测到隐藏的大部分信息，而 LSB 算法则基本检测不到隐藏的信息，说明本算法的鲁棒性比 LSB 算法要高很多，而此时的嵌入比约为 24%左右，信息隐藏量仍然比 LSB 算法大很多。

(a)载体图像　(b)载入图像　(c)裁剪后的载密图像



(d)检测到的多幅隐藏图像

图 3　裁剪试验结果

(a)遭受 2%椒盐噪声污染的载密图像　(b)检测到的隐藏图像

图 4　加噪试验结果

4　结束语

利用人类视觉系统的对图像所具有的亮度掩蔽效应，本文提出了一种基于空间域的自适应信息隐藏方法，隐藏信息的提取是一种完全意义下的盲提取，由于不需要进行变换运算，因此计算复杂度较低。该方法是根据像素点的每个颜色分量进行判断信息的隐藏位置，能最大限度地利用可利用的隐藏空间，实验表明该方法的信息隐藏量大，在满足不可感知性的前提下，比目前广泛使用的信息隐藏方法要大很多，同时具有一定的抗噪声污染和抗裁剪的能力，并可防止位平面过滤所导致的失密。

参考文献

[1] Tirkel A Z, Rankin G. A, van Schyndel R M, et al. Electronic Watermark in Digital Image Computing, Technology and Applications[C]//Proc. of DICTA'93. Sydney, Australia: [s. n.], 1993.

[2] Johnson N F. Steganography Tools[Z]. (2005-10-25). http://www.jjtc.com/Security/stegtools.htm.

[3] 任智斌, 隋永新. 以图像为载体的最大意义位 MSB 信息隐藏技术的研究[J]. 光学精密工程, 2002, 10(2): 182-186

[4] Cox I J, Killian J, Leighton T, et al. Secure Spread Spectrum Watermarking for Images, Audio and Video[C]//Proceedings of the 1996 IEEE International Conference on Image Processing. [S. l.]: IEEE Computer Society Press,1996.

[5] Jayant N, Johnston J, Safranek R. Signal Compression Based on Models of Human Perception[J]. Proceedings of the IEEE, 1993, 81(10): 385-1422.

[6] Watson B. DCT Quantization Matrices Visually Optimized for Individual Images[C]//Proceedings of the SPIE: Human Vision, Visual Processing and Digital Display IV. San Jose, CA: SPIE Press, 1993: 202-216.

[7] Gonzalez C, Wintz P. Digital Image Processing[M]. 2nd ed. [S. l.]: Addison-Wesley Publishing Co/IEEE Press, 1987.

[8] 王炳锡, 陈　琦, 邓峰森. 数字水印技术[M]. 西安: 西安电子科技大学出版社, 2003.

(上接第 166 页)

WAI'。该方案具有 WLAN 所要求的所有安全属性，保证了无线通信的信息安全，具有理论意义和实际应用价值。

参考文献

[1] 中华人民共和国国家质量监督检验检疫总局. GB 15926.11-2003/XG1-2006 媒体访问控制和物理层规范[S]. 2006-01-27.

[2] 张　帆, 马建峰. CK 模型下的无线认证协议[C]//第九届中国密码学学术会议论文集. 北京, 中国: 中国科学技术出版社, 2006.

[3] 李谢华, 李建华, 杨树堂, 等. WAPI 接入鉴别过程的形式化分析与验证[J]. 计算机工程, 2006, 32(22): 10-13.

[4] Boyd C, Mathuria A. Protocols for Authentication and Key Establishment[M]. Berlin, Germany: Springer-Verlag, 2003

[5] Canetti R, Krawczyk H. Analysis of Key-exchange Protocols and Their Use for Building Secure Channels[C]//Proceedings of EUROCRPT'01. Berlin, Germany: Springer-Verlag, 2001.