一种基于游程长度的高安全性图像信息隐藏算法

谢建全[1,2] 谢 勍[1] 黄大足[1,2]
(湖南财政经济学院信息安全研究所 长沙 410205)[1] (中南大学信息科学与工程学院 长沙 410083)[2]

摘 要 针对目前多数信息隐藏算法的安全性不高使其无法应用于隐蔽通信等领域的问题,提出了一种基于游程长度的隐藏算法,算法的基本思想是将图像分解成多个二值图像,通过对分解后的二值图像游程长度的奇偶性来隐藏信息,最多改变二值图像黑白交界处的一个像素值便可隐藏1bit的信息,隐藏信息可实现盲提取。算法未造成图像低位平面的0和1分布特性的明显改变,也未造成长游程的减少,因此可抵御许多针对LSB及其改进方法的隐写分析技术的检测。仿真试验结果显示,算法的安全性高,不可感知性好,并且嵌入容量大,可应用于隐藏通信等对隐藏容量和安全性有较高要求的场合。

关键词 信息隐藏,游程长度,嵌入容量,不可感知性,安全性
中图法分类号 TP309.2 **文献标识码** A

Image Information Hiding Algorithm with High Security Based on Run-length

XIE Jian-quan[1,2] XIE Qing[1] HUANG Da-zu[1,2]
(Research Institute of Information Security, Hunan University of Finance and Economics, Changsha 410205, China)[1]
(School of Information Science and Engineering, Central South University, Changsha 410083, China)[2]

Abstract Aiming at the problem that most information hiding algorithms are not secure enough to afford secret communication, a kind of hiding information algorithm based on Run Length was proposed. The main idea of this algorithm is separating the image into several binary images. Through utilizing the parities of the Run Length of the binary images, one bit of information can be successfully embedded while even one pixel that is located along black-white boundary of the binary image is modified. The blind extraction of the hiding information can be achieved. The algorithm neither obviously changes distribution property of 0 and 1 in image's low plane, nor reduces the Length of Run. Hence it can defend various detections against LSB and its improved method. The simulation result shows that the algorithm has high security, good imperceptibility and large embedding capacity. Furthermore, it can be applied in secret communication and other situation that requires high security and large capacity.

Keywords Information hiding, Run-length, Embedding capacity, Imperceptibility, Security

1 引言

信息隐藏是将重要信息嵌入到可以公开的其他载体中,在基本不改变载体的外部特征及使用价值的情况下,实现重要信息的隐秘传递。它作为一种保证信息安全传递的重要手段,可以有效地应用在数字水印和隐密通信等领域,引起了人们的极大关注。目前用作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,在使用方法上没有本质的区别,都是利用人类视觉或听觉的感知局限性来隐藏信息。图像是最常见也是互联网使用很多的信息载体,由于其冗余空间大,是目前用得最多的信息隐藏载体。目前多数信息隐藏算法侧重于隐藏信息的不可感知性和鲁棒性[1-3],对信息的不可检测性相对考虑较少,因此安全性还有待提高,要实现安全的信息隐蔽传输,隐藏算法既要使嵌入信息在视觉上不可察觉,又要不引起可被检测出来的统计异常性。基于图像的信息隐藏技术,可以归类于两种:基于变换域的隐藏技术和基于空间域的隐藏技术。一般意义上,空间域方法算法简便,信息隐藏量大,信息嵌入和提取速度快。但多数空间域隐藏算法对攻击的鲁棒性不强,而且许多空间域隐藏算法改变了图像的某些统计特性而容易被检测到[4-8],安全性不高,使其应用受到很大限制。很多借用空间域算法思想的变换域算法,如改变量化后的DCT系数的最低有效位的算法,也存在同样的安全性问题,并且隐藏容量还远低于空间域算法。本文提出一种基于游程的隐藏算法,它有较高的安全性,并且隐藏容量比较大,可满足隐藏通信等需要隐藏大容量信息的需求。算法的基本思想是将灰度图像或彩色图像按位平面分解成多幅二值图像,通过最多改变二值图像黑白交界处的一个像素值,并利用较长(或较短)的那个游程的长度[9]的奇偶性来分别表

到稿日期:2013-04-07 返修日期:2013-08-19 本文受湖南省科技计划项目(2012GK3064),湖南省教育科学"十二·五"课题(XJK011BXJ008),省重点学科建设项目资助。
谢建全(1964—),男,博士,教授,主要研究领域为信息隐藏、版权保护,E-mail:xiejianquan@sina.com;谢 勍(1966—),女,硕士,教授,主要研究领域为数字水印;黄大足(1968—),男,博士,教授,主要研究领域为数据加密与信息隐藏。

示需要隐藏的信息 0 或 1，并且可实现盲提取。本文算法不会造成低位平面的异常，能有效抵御许多针对 LSB 及其改进方法的隐写分析方法；也不会造成游程特性的异常，能抵御基于游程特性的隐写分析方法，具有良好的安全性。

2 典型算法的安全性分析

人眼对图像的感知最终是在空域中进行的，因此各种图像信息隐藏算法的最后视觉不可感知性均可在空间域中进行分析。为了保证隐藏信息的不可感知性，多数以图像为载体的信息隐藏算法秘密信息的嵌入位置均选择人眼感知性差的位置，典型的就是 LSB(最不重要比特位)算法，LSB 隐藏算法是一种非常简单有效的隐藏算法，并且具有非常好的不可感知性，目前大多数空域水印方案都是基于图像像素 LSB 的嵌入或进行了一定改进。甚至不少变换域的算法，也能找到 LSB 看法的影子，比如典型的 JSTEG 算法，它与空间域的 LSB 算法的区别是将空间域的灰度值更换为量化后的 DCT 系数。为了加强隐藏的秘密信息的安全性，秘密信息在嵌入前往往经过加密处理，它可以看作是 0 和 1 随机分布的比特流，基于 LSB 算法的安全性取决于图像的 LSB 平面是否呈现随机特性，然而多数图像的 LSB 平面并非呈现随机特性，如图 1(a)所示的 bird 图像，各个位平面分解后从最高位到最低位的位平面图分别如图 1(b)至图 1(i)所示。从图中不难看出，各个位平面均非呈现随机特性，LSB 算法破坏了自然属性，所以抗检测性能不好，卡方(χ^2)分析方法就是根据图像的 LSB 位是否呈现随机特点来进行隐写分析的。可见，基于 LSB 的隐藏算法虽然有较好的不可感知性，但安全性并不好，不适合在隐蔽通信等应用中使用。

在隐写分析中，信息隐藏的不可感知性的关键点不是找出原始图像与载体图像的相似程度，而是要将载体看作噪声，在噪声中对隐藏信息的识别程度才是其关键性指标，事实上隐写分析算法都是在没有原始图像的情况下进行的。加密后秘密信息的嵌入还会使图像相应的位平面的随机性增强，最低位平面部分尤其明显，在游程长度上则反映出短游程的数量增加，即原有图像的长游程数量将减少，而短游程数量增加[10]，因此除了卡方(χ^2)分析方法外，还可以通过检查游程长度的统计特性来识别图像是否隐藏有秘密信息，为加强算法的安全性，必须解决长游程数量减少的问题。

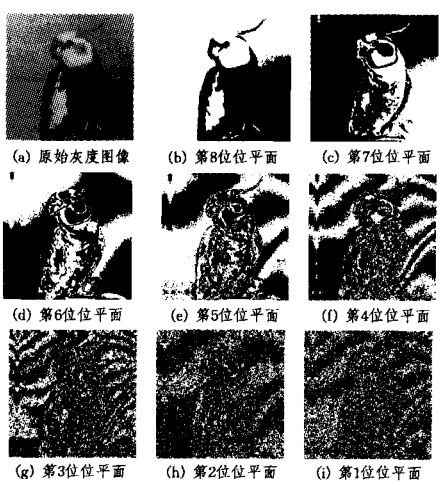


图 1 bird 图像各个位平面分解图

人眼视觉系统的主要功能是提取视场中的结构信息[11,12]，在信息隐藏技术上，主要运用的人眼视觉特性有 3 个方面：视觉空间频率敏感特性、对比度掩蔽特性和亮度掩蔽特性[13]。目前多数算法主要是利用亮度掩蔽特性，而没有利用其它特性。其实利用其它特性，即使单个像素点的亮度掩蔽特性不满足要求，照样可以隐藏信息，比如在二值图像中隐藏秘密数据就是一个典型的例子[14]。二值图像只有黑白两色，冗余空间较少，为了保证隐藏信息的不可感知性，通常将数据嵌入在黑白交界处。在一幅二值图像中，当一个方向上出现连续多个同值的像素时，增加或减少一个同值像素点，人的视觉系统一般不会对这种变化感知不明显，并且随着连续同值像素点的增加，对这种变化的感知性越弱，也即当游程长度超过一定的值时，即使游程的长度增加 1 或减少 1，也不会影响视觉的感知效果，具有较好的不可感知性。但为了解决安全性问题，必须防止长游程数量的减少。

3 基于游程的信息隐藏算法

灰度图像(或彩色图像的各个颜色分量)不同的位平面可看作一幅二值图像，将灰度图像分解成多个二值图像，只要嵌入方法得当，每个位平面均可嵌入信息，并且具有较好的不可感知性，如果嵌入过程能保证不改变图像的统计特性，则有较高的安全性；同时由于信息的嵌入不局限在 LSB 位平面，因此有较高的嵌入容量。本文算法的基本思想是最多改变黑白交界处的一个像素值，再利用较长(或较短)的那个游程的长度的奇偶性来分别表示需要隐藏的信息 0 或 1，并且可实现盲提取。

2.1 嵌入算法

Step 1 对灰度图像(或彩色图像)进行位平面分解，得到多个二值图像，信息的嵌入将在每个二值图像中进行，即每个位平面均进行信息的嵌入；如果是二值图像则跳过这一步；

Step 2 对每个二值图像进行逐行扫描，扫描方式为扫描相邻的一段黑和一段白游程对(相邻的一段黑和一段白)B 和 W，在实际扫描游程时，先从黑游程开始还是从白游程开始以及从哪一个游程对开始嵌入信息，每一行可以不同，由密钥 $k(i)$ 决定，这样可提高算法的安全性。假设这两段游程的长度分别为 a 和 b。

Step 3 比较 a 和 b 的大小：

$$c_1=\max(a,b) \tag{1}$$

$$c_2=\min(a,b) \tag{2}$$

不失一般性，假设 $c_1=a$，$c_2=b$。

Step 4 判断该游程对是否可嵌入信息。根据前面的分析可知，当最短的游程超过一定大小后，即 c_2 大于指定值 x 时可嵌入信息(由于不同位平面的感知性不同，在不同的位平面，x 的取值可以不同，在低平面位可取小些，在高平面位需要取大些)，从待嵌入的信息中取 1bit 信息进行下面的嵌入处理；否则认为该游程对不能嵌入信息，转 Step 5 选择下一个游程对再尝试嵌入操作。

Step 5 当长游程的长度 c_1 的奇偶性与待嵌入的信息赋值相同时，不作任何修改，嵌入完成；当长游程的长度 c_1 的奇偶性与待嵌入的信息赋值不同时，修改两段游程交界处的一个像素值来完成信息的嵌入，修改原则为使较长的那个游程的奇偶性与待嵌入信息相同(游程长度为奇数时，嵌入 1；游程长度为偶数时，嵌入 0)。具体过程又分 3 种情况：

①修改两段游程交界处的一个像素点的值，使 c_1 增加 1，

c_2 减少 1，若满足 $\min(c_1,c_2)>x$，则嵌入完成，转 Step 6。

②在第①步的基础上，将 c_1 的长度减少 2(相当于在原来的基础上 c_1 减少 1，c_2 增加 1)，若满足 $\min(c_1,c_2)>x$，则嵌入完成，转 Step 6。若修改后，短游程的长度仍大于指定的最小可隐藏的游程的长度 x，且较长的游程的奇偶性与待嵌入的信息赋值相同，则嵌入完成，转 Step 6，在此过程中，两段游程的长短关系可能会发生改变(仅发生于较长的游程长度比较短的游程大 1 的情况)，若改变后的长游程的奇偶性与待嵌入信息相同，则嵌入完成，转 Step 6，否则转下一步操作。

③在完成第①②步后，如仍不能满足嵌入要求，说明该游程对无法嵌入信息。该情况仅发生于游程对中两个游程的长度相同，且当嵌入后最短的游程长度小于指定值时，为避免提取时的漏判，需要进行嵌入处理(将其中一个游程的长度增加 1，另一个减少 1)，但该次嵌入作为无效嵌入，即此次的嵌入信息需要重新嵌入，在提取信息时不在该游程对提取信息。在 Step6 的处理中，在下一个可嵌入信息的位置进行嵌入时不取新的信息进行嵌入。

Step 6　扫描下一个流程对，对下一个待嵌入的 bit 进行嵌入操作，直到所有信息均嵌入完成为止。在扫描游程对的过程中，如果一行已扫描完毕，则在密钥的控制下，扫描下一行。

3.2　提取算法

Step 1　同嵌入过程一样，对灰度图像(或彩色图像)进行位平面分解，得到多个二值图像；

Step 2　根据密钥 $k(i)$，确定扫描的起始位置，扫描每个二值图像各行的游程对，记录这两段游程的长度分别为 a 和 b；

Step 3　提取嵌入的信息。当游程长度 a 和 b 均大于指定值 x 时，说明嵌入了 1bit 信息(否则说明该游程对中没有嵌入信息)，较长的那个流程的奇偶性即为所嵌入的信息(如果相同，则选择前面的那一个)，即：

$$w(j)=\max(a,b) \bmod 2 \tag{3}$$

Step 4　根据嵌入算法扫描下一游程对，提取后面的信息，直到所有信息全部提取完毕。

4　仿真试验结果与分析

为检验不同算法的安全性、嵌入容量和不可感知性，分别用图 2 所示的 256×256 的 Bird 、Lena、Mandrill 和 Cavas 4 幅标准测试图像进行满嵌入和提取试验。嵌入信息后的载密图像分别如图 3(a)—(d)所示。

(a) Bird　(b) Lena　(c) Mandrill　(d) Cavas

图 2　嵌入所用标准图像

(a) Bird　(b) Lena　(c) Mandrill　(d) Cavas

图 3　嵌入信息后的图像

从主机视觉上我们感觉不到图像在嵌入前后的变化，再对图像嵌入前后的不可感知性进行客观评价，由于常用于评价灰度图像失真的峰值信噪比(PSNR)不适用于图像信息隐藏的不可感知性[15]，采用文献[13]提出的客观度量指标 CSF (Constrast Sensitivity Function) 和改进的 dm 面积加权 PSNR 评价指标 WPSNR(Weighted peak signal to noise rate) 来检验图像的不可感知性，评价结果见表 1，从表中数据可知其不可感知性指标均超过视觉可感知阈值很多，说明本文算法的不可感知性好。

表 1　图像嵌入信息后的不可感知性测试结果

图像名称	Bird	Lena	Mandrill	Cavas
CSF	51.3894	46.22	42.32	41.813
WPSNR	60.6270	54.46	57.94	67.2459

用卡方(χ^2)分析方法、RS(Regular and singular groups method)分析法、SPA(Sample Pair Analysis)分析法和 GPC (Gray-level Plane Crossing Analysis)分析法对载密图像进行隐写检测，均未检测到其中隐藏有秘密信息，可见算法可有效对付此类隐写分析，说明本文算法嵌入信息有较好的安全性。

4 幅图像嵌入容量见表 2，嵌入信息提取的正确率为 100%，根据结果可知本文算法的嵌入虽然比 LSB 算法要低，但比多数变换域算法要高很多。如果单纯从高容量考虑，可以在低平面位采用 LSB 类算法，而在高平面位采用本文算法，则容量可比 LSB 类算法更大，但在低平面位嵌入的信息同 LSB 算法一样无法保证其安全性。

表 2　典型测试图像最大可嵌入容量

图像名称	Bird	Lena	Mandrill	Cavas
嵌入容量(比特)	2961	2283	3282	1778

将图 3(a)所示的 4 幅图像进行位的平面分解，其低 4 个位平面图分别如图 4 所示，从图中可以看出，嵌入信息后的图像的 LSB 平面及低位平面保留了图像的 LSB 平面所呈现的非随机特性，与图 1 相应的位平面图基本一致，可有效抵御根据图像的 LSB 位及其它低位平面是否呈现随机特点来进行的隐写分析检测。

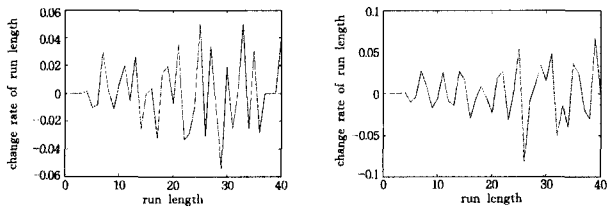
(a) 第4位位平面　(b) 第3位位平面　(c) 第2位位平面　(d) 第1位位平面

图 4　载密图像的 4 个低位位平面图

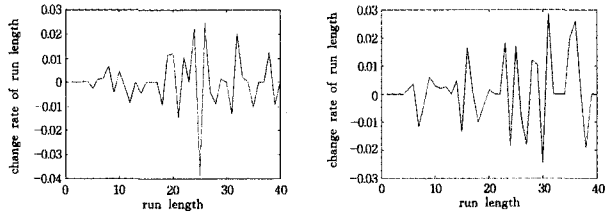
图 3 所示的 4 幅图像相对于图 2 所示的 4 幅图像在嵌入信息前后游程变化最多的部分游程的变化情况如图 5 所示，从图 5 中可以看出嵌入信息后的图像的各种长度的游程的数量并未出现明显的增加或减少现象，因此可抵御基于流程长度统计特性的各种隐写检查方法。

再用图 6 所示的 256×256×1 的两幅标准二值测试图像 Circle 和 Soil 进行满嵌入和提取试验，嵌入信息后的载密图像如图 7 所示。

实验用的二值图像在嵌入信息前后游程变化最多的部分游程的变化情况如图 8 所示，从图 8 中可以看出嵌入信息后的图像的各种长度的游程数量未出现明显的增加或减少现象，可见本文算法对二值图像的信息隐藏同样可抵御基于流程长度统计特性的各种隐写检查方法。

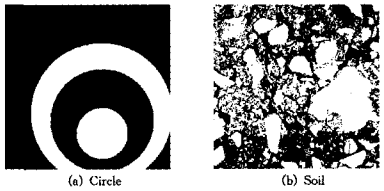


(a) Bird (b) Lena



(c) Mandrill (d) Cavas

图 5 嵌入信息后部分长度游程的变化率

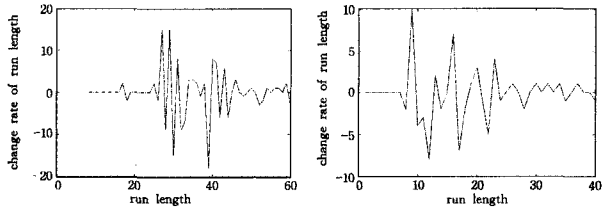


(a) Circle (b) Soil

图 6 原始二值图像

(a) Circle (b) Soil

图 7 嵌入信息后的二值图像



(a) Circle (b) Soil

图 8 二值图像嵌入信息前后部分游程数的变化情况

嵌入信息后的嵌入容量和客观评价指标值分别见表 3 和表 4，根据这两个表可知本文算法的嵌入容量与嵌入容量相对较大的 3×3 的二值图像分块嵌入算法相当，但比分块算法的不可感知性更高。不过本文算法用于二值文本图像时，如果文本的笔画较细，则嵌入容量很小，并且一些光滑的垂直笔画的垂直边沿处，可能存在锯齿现象，这是本文算法应用于二值文本图像时还需要改进的地方。

表 3 二值测试图像最大可嵌入容量

图像名称	Circle	Soil
嵌入容量(比特)	2961	2283

用卡方(χ^2)分析方法、RS 分析法和 GPC 分析法对载密图像进行隐写检测，同样未检测到其中隐藏有秘密信息，可见本文算法同样可适应二值图像的信息隐藏，并且具有很好的不可感知性和抗检测能力，可有效抵御隐写分析，比分块算法更安全。

表 4 二值图像嵌入信息后的不可感知性测试结果

Image	CSF	WPSNR
Circle	55.41	41.75
Soil	43.98	41.12

结束语 利用人类视觉特性，本文提出了一种基于游程的隐藏算法，其将灰度图像或彩色图像分解成多幅二值图像，再判断二值图像每一对黑白游程是否可嵌入信息，在嵌入信息时最多修改一个长游程两端的像素点的像素值，算法不会使得图像的低平面位出现噪声特性，也不会造成长游程长度的减少，因此不会改变图像各平面位的统计特性，可有效抵御卡方(χ^2)分析方法、RS 分析法和 GPC 分析法等隐写分析方法对载密图像的隐写检测，具有较高的安全性，同时由于算法能在包括最高有效位所在平面的所有平面位嵌入信息，因此嵌入的容量也比较高，能满足对嵌入容量有较高要求的应用的需要。仿真试验结果也证明本文算法的安全性高，不可感知性好，并且嵌入容量大，可应用于隐藏通信等对隐藏容量和安全性有较高要求的场合。

参 考 文 献

[1] Nezhadarya E, Wang J, Ward R K. Image watermarking based on multiscale gradient direction quantization[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(4): 1200-1213

[2] 姜传贤，陈孝威，李智. 基于文本重要内容的鲁棒水印算法[J]. 自动化学报，2010，36(9)：1250-1256

[3] Zhou X M, Wang S C, Xiong S C, et al. Attack model and performance evaluation of text digital watermarking[J]. Journal of Computers, 2010, 5(12): 1933-1941

[4] 陈够喜，陈俊杰. 多载体信息隐藏安全性研究[J]. 小型微型计算机系统，2011，32(4)：644-646

[5] Ker A D. Steganalysis of embedding in two least-significant bits [J]. IEEE Transitions on Information Forensics and Security, 2007, 1(2): 46-54

[6] 雷雨，杨晓元，潘晓中，等. 基于局部随机性的 YASS 隐写分析方法[J]. 计算机学报，2010，33(10)：1997-2002

[7] Fillatre L. Adaptive Steganalysis of Least Significant Bit Replacement in Grayscale Natural Images[J]. IEEE Transactions on Signal Processing, 2012, 60(2): 556-569

[8] 张湛，刘光杰，戴跃伟，等. 基于 Markov 链安全性的二阶统计保持隐写算法[J]. 中国图象图形学报，2010，15(8)：1175-1181

[9] Samir K B, Avishek R, Tuhin U P. A palette based approach for invisible digital watermarking using the concept of run-length [A]// 2010 International Conference on Computational Intelligence and Communication Networks, CICN 2010[C]. 2010: 83-87

[10] 继军，杨义先. 图像 LSB 隐藏游程检测算法[J]. 西安邮电学院学报，2005，10(1)：1-5

[11] 李航，路羊，崔慧娟，等. 基于频域的结构相似度的图像质量评价方法[J]. 清华大学学报：自然科学版，2009，49(4)：559-562

[12] 罗向阳，陆佩忠，刘粉林. 一类可抵御 SPA 分析的动态补偿 LSB 信息隐藏方法[J]. 计算机学报，2007，30(10)：463-473

[13] 谢建全，谢劼，黄大足. 图像信息隐藏不可感知性指标研究[J]. 小型微型计算机系统，2011，32(5)：953-957

[14] 刘春庆，梁光岚，王朔中，等. 应用二值图像信息隐藏技术实现彩色图像中的安全隐写[J]. 应用科学学报，2007，25(4)：342-347

[15] 马秀莹，林家骏. 信息隐藏性能评价方法[J]. 中国图象图形学报，2011，16(2)：209-214