一种保持直方图特性的JPEG图像掩密算法

陈 丹[①] 罗 欣[②] 王育民[①]
[①](西安电子科技大学ISN国家重点实验室 西安 710071)
[②](西北工业大学自动化学院 西安 710072)

摘 要 传统的JPEG图像掩密算法往往因为改变了载体图像的DCT系数直方图而不能抵抗各种基于直方图的攻击，或者为了矫正直方图而降低了隐藏容量，该文提出一种新的保持直方图特性的算法。该算法在嵌入秘密消息时，动态建立Adjust_info表记录系数直方图被改变的情况，然后根据该表调整系数的变化方向，这样不但可以补偿直方图的改变，而且并不降低隐藏容量。对多幅图像的实验表明，该算法不但能够达到13%的高隐藏容量(压缩因子为75)，而且掩密后图像总体DCT系数直方图的平均失真率为0.81%。由改进算法掩密后图像低频DCT系数直方图的最大失真率为3.83%，平均失真率只有1.98%，仅对直方图做了微小的改变，因此可以有效抵御各种直方图攻击，从而为安全掩密提供了可靠保证。

关键词 掩密技术，掩密分析技术，JPEG图像，直方图特性，直方图攻击
中图分类号：TP391,TN918 **文献标识码**：A **文章编号**：1009-5896(2006)02-0252-05

A Steganography Preserving the Property of the Histogram for JPEG Images

Chen Dan[①] Luo Xin[②] Wang Yu-min[①]
[①](*State Key Lab. on ISN, Xidian University, Xi'an* 710071, *China*)
[②](*The Institute of Automation, NWPU, Xi'an* 710072, *China*)

Abstract Traditional steganographic techniques for JPEG images always suffer from histogram-based attacks because they change the DCT coefficient histogram of the cover image, or from the reduced hiding capacity due to the correction of the change of the histogram. A new steganography preserving the property of the histogram is proposed in this paper. When the secret message is embedded, an adjust_info table is built to memorize the alteration of the histogram. Then the modification direction of the coefficient is adjusted according to the table. In this way, the change of the histogram is compensated and the hiding capacity is not reduced yet. Several experimental results demonstrate that the algorithm can attain a high hiding capacity of 13% (the quality factor is 75). Furthermore the average distortion rate of the general DCT coefficient histograms on stego-images is 0.81%, the maximal distortion rate of the histograms on low frequency coefficients is 3.83% obtained from the stego-images generated by the improved algorithm and the average distortion rate of them is only 1.98%. The property of the histogram is fine changed; therefore, various histogram-based attacks can be effectively resisted and secure steganorgraphy can be insured.

Key words Steganorgraphy, Steganalysis, JPEG images, Property of the histogram, Histogram-based attacks

1 引言

掩密技术[1](Steganorgraphy)是信息隐藏(Information hiding)领域的一个重要分支，它是利用人的视觉/听觉冗余以及多媒体数据的统计冗余，将秘密消息以一定的编码或加密方式嵌入到公开的数字媒体中，从而实现消息的秘密传输。作为网络环境中的一种新的保密通信手段，掩密技术的研究在学术界，企业界和国家安全部门都已受到了广泛关注。

与所有的保密通信技术一样，掩密技术的安全性必然是其研究的重点，因此它的对抗技术——掩密分析技术(Steganalysis)也迅速发展起来。掩密分析[2]是通过分析各种可能的载体信息旨在检测，提取或破坏非法隐藏于这些载体数据中的秘密消息。勿庸置疑，一个安全的掩密算法应该能够经受住各种掩密分析技术的不断考验。

JPEG图像的应用非常广泛[3]，可以为秘密信息的传输提

2004-06-07 收到，2005-03-28 改回
国家部级基金资助课题

供丰富的载体资源。目前已有多种基于 JPEG 格式的图像掩密算法，其中比较成熟的有 JSteg[4]，OutGuess[5]和 F5[6]等。它们都是通过修改 JPEG 图像 DCT 量化系数来嵌入秘密消息，但是它们的安全性和隐藏容量却不相同。JSteg 和 F5 算法的隐藏容量可达 13%(压缩因子为 75)，但是由于对系数直方图的改动过大而不能抵抗直方图攻击[7,8]；OutGuess 对系数直方图基本没有改变，可以有效抵抗直方图攻击，但是由于预留了一部分系数用来矫正直方图，使得隐藏容量仅有 6.5%。因此，如何设计既能保持系数直方图又具有高的隐藏容量的掩密算法是一个重要的研究课题。本文提出了一种安全高效的算法。算法规定正奇系数或负偶系数表示嵌入的秘密消息比特为“1”；负奇系数或正偶系数表示消息比特为“0”，如果系数的正负奇偶与它所表示的消息比特不相符，则它有两个方向可以调整，此时根据直方图的变化趋势动态调整系数的改变方向，不但可以补偿直方图的改变，而且并不降低隐藏容量。对多幅图像的实验表明，该算法不但能够达到 13%的高隐藏容量，而且掩密后图像总体 DCT 系数直方图的失真率不超过 0.15%，平均失真率为 0.81%，由改进算法掩密后图像低频 DCT 系数直方图的最大失真率为 3.83%，平均失真率只有 1.98%，仅对直方图做了微小的改变，因此可以有效抵御各种直方图攻击。

本文的组织结构如下：第 2 节介绍传统的 JPEG 图像掩密算法，分析它们对直方图的改变；第 3 节提出新的保持直方图特性的算法；第 4 节针对低频系数直方图的保持问题对算法进行了改进；第 5 节进行仿真实验，测试算法的隐藏容量，掩密前后图像的视觉质量，总体和低频 DCT 系数直方图的失真率等；第 6 节对全文总结并指出今后的工作方向。

2　传统 JPEG 图像掩密算法对直方图的改变

传统的 JPEG 图像掩密算法都是通过修改 JPEG 图像 DCT 量化系数来嵌入秘密消息。例如，JSteg[4]是将秘密消息比特顺序嵌入到 JPEG 图像非 0 非 1 的 DCT 量化系数的 LSB(Least significant bits)上，由于是顺序嵌入，所以安全性不高。JPHide[9]软件对其进行了改进，将消息随机散布于量化系数的 LSB 中，但是仍然不可避免地改变了系数直方图，OutGuess[5]在此基础上对系数直方图进行了矫正。而 Westfeld[6]指出，上述改写 LSB 的算法易造成系数的 LSB 平面呈现一定的分布规律，从而导致一系列攻击，如 χ^2 攻击，扩展的 χ^2 攻击以及 RS 检测等[2]，他提出采用对量化系数绝对值减 1 的方法来实现秘密消息的嵌入，并由此得出了 F5 算法。

然而，无论是改写 LSB 还是绝对值减 1 的方法都必然造成系数分布有所改变。直方图描述了系数分布的一阶特性，这种由于嵌入消息而造成的系数分布变化将直接反映在直方图上。图 1 分别给出了用 JSteg，OutGuess 和 F5 算法进行掩密前后 JPEG 图像 DCT 系数直方图的改变情况。由图可见，除了 OutGuess 外，其他两种算法对直方图都有了很大的改动。原始载体图像的直方图具有两个特点：一是分别向正负两个方向呈递减趋势；二是相邻系数频次之差也是递减的。JSteg 改变了该直方图的分布趋势，使得相邻两系数的出现频率近似相等，正方向如系数 2 和 3，4 和 5…，负方向如－1 和－2，－3 和－4…依次类推。F5 算法虽然基本上保持了直方图的递减规律，但是由于缩减效应(shrinkage)而造成了 0 系数数目大幅增多以及其余系数都有不同程度减少的现象[8]。OutGuess 对直方图基本保持不变，这是因为它在嵌入信息时对直方图做了矫正，其代价是需要预留一半的系数来矫正嵌入信息所带来的直方图改变，因此，和 JSteg，F5 相比，相同条件下它的隐藏容量将减少一半。

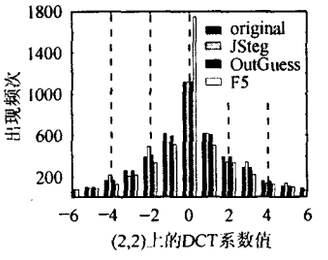

图 1　用 JSteg，OutGuess 和 F5 算法进行掩密前后的 JPEG 图像在(2,2)位置上的 DCT 系数直方图比较

Fig.1 A comparison of the histograms of DCT coefficient (2, 2) Before and after JSteg, OutGuess, and F5 embedding methods have been applied to the JPEG image

如果嵌入秘密消息使得直方图发生了大的变化，则攻击者很容易通过分析直方图的变化来检测图像掩密与否的事实。例如，Westfeld[7]根据 JSteg 掩密图像直方图中的相邻系数出现频率近似相等的特点提出了 χ^2 统计攻击[7]；而 Fridrich[8]针对 F5 算法设计了直方图攻击方法，基本原理是首先从待测图像估计原始图像的系数直方图，然后通过比较估计的和待测图像的系数直方图，获得图像掩密与否的结论，同时得到嵌入消息的长度信息。

综上所述，要想从根本上避免直方图攻击就必须保证直方图在掩密前后基本不变，OutGuess 矫正直方图的方法虽然能做到这一点，但是却牺牲了一半的隐藏容量。本文提出对系数动态增值或减值的方法，即每个系数可以向两个方向改变以嵌入信息，动态调整系数的改变方向既能保持直方图又能保证高的隐藏容量。

3　保持直方图特性的掩密算法

我们规定：正奇系数或负偶系数表示嵌入的秘密消息比

特为“1”；负奇系数或正偶系数表示消息比特为“0”。这样，在嵌入信息时，如果系数的正负奇偶与它所表示的消息比特不相符，那么它将有两个方向可以调整。例如，当系数值为2而所要嵌入的消息比特为“1”时，必须将系数2变为奇数才能隐藏该比特信息，加1变为3或者减1变为1都能达到目的。此时出现了两个调整方向，任选一个即可，我们可以利用这个特点追踪系数的改变方向，从而动态补偿系数直方图的改变。

算法的基本思想是：在嵌入信息时，建立信息表记录直方图被改变的情况，每当新的系数需要有所改变时，查询该表，根据直方图的改变趋势调整系数的改变方向以完成信息嵌入。具体方案如(图2)：

```
Input: mesage, shared secret, cover image
Output: stego image
initialize PRNG with shared secret
permutate DCT coefficients with PRNG
initialize the Adjust_info table
while data left to embed do
    get next non-zero AC coefficient from cover image
    if (DCT>0) & (DCT and the message bit are not match)
      if  DCT=1
        DCT=DCT+1 or DCT=DCT-2 according to the Adjust_info table
      else
        DCT=DCT+1 or DCT=DCT-1 according to the Adjust_info table
      end
      update the Adjust_info table
    elseif  (DCT<0) & (DCT and the message bit are not match)
      if  DCT=-1
        DCT=DCT+2 or DCT=DCT-1 according to the Adjust_info table
      else
        DCT=DCT+1 or DCT=DCT-1 according to the Adjust_info table
      end
      update the Adjust_info table
    end
end while
insert DCT coefficients into stego image
```

图2 保持直方图特性的掩密算法

Fig.2 Algorithm preserving the property of the histogram

步骤1 由共享密钥初始化PRNG；

步骤2 用PRNG对DCT系数进行置乱；

步骤3 根据DCT量化系数的范围初始化Adjust_info表；

步骤4 依次选取非零AC系数以嵌入消息直到所有的消息比特完全被嵌入或者所有的非零AC系数都被遍历。如果所选系数能够表示将要嵌入的消息比特，则系数不变；相反，则根据Adjust_info表的内容对系数动态增减，然后由增减方向更新Adjust_info表；

步骤5 将变化后的DCT系数写入掩密图像。

动态建立Adjust_info表并根据该表内容修改系数是算法的核心。Adjust_info表记录了非零AC系数直方图被改变的情况(图3)。如果某个系数所对应的记录大于0，则代表该系数出现的次数有增加；相反，如果小于0，则说明该系数有减少。初始化该表时，每个非零AC系数的记录都为0。嵌入消息时，采用如下规则修改系数和更新Adjust_info表：

初始化后的Adjust_info表

非零AC系数值	…	−4	−3	−2	−1	1	2	3	4	…
增减个数	…	0	0	0	0	0	0	0	0	…

系数1

非零AC系数值	…	−4	−3	−2	−1	1	2	3	4	…
增减个数	…	0	0	0	0	0	0	0	0	…

系数2

非零AC系数值	…	−4	−3	−2	−1	1	2	3	4	…
增减个数	…	0	0	0	0	0	0	0	0	…

系数2

非零AC系数值	…	−4	−3	−2	−1	1	2	3	4	…
增减个数	…	0	0	0	0	0	0	0	0	…

系数1

非零AC系数值	…	−4	−3	−2	−1	1	2	3	4	…
增减个数	…	0	0	0	0	0	0	0	0	…

系数−1

非零AC系数值	…	−4	−3	−2	−1	1	2	3	4	…
增减个数	…	0	0	0	0	0	0	0	0	…

图3 动态建立Adjust_info表的过程

Fig.3 Process of building the table Adjust_info dynamically

规则1 比较Adjust_info表中与该系数相邻的左右两边的表项值，将系数向小的一边改动，然后该系数对应的Adjust_info表项减1，而系数所移向的那个表项加1。

规则2 如果左右表项的值相等，则对于正系数，默认向右移动，即系数值变为它右边的值，系数所对应的表项减1，右边的表项加1；对于负系数，默认向左移动并更新相应表项。对于处于边界的系数，只向一边移动。

图4给出了用该算法掩密前后的直方图变化情况。由图可见，总体系数直方图的变化非常小，几乎不可察觉，这说明通过建立Adjust_info表跟踪系数被修改的情况，进而根据总体系数的变化趋势调整系数的改变方向，能够保证直方图不会有大的变化。然而，值得注意的是，该算法不能保证低频系数直方图不变，特别是掩密前后低频系数直方图的变化还呈现出一定的规律，即绝对值为1的系数数目增多，绝对值为2的系数数目减少。低频系数的分布对掩密算法的安全性是至关重要的，因为低频系数集中了图像的主要能量，而且大部分的非零AC系数都在低频，如果低频系数直方图发生了大的变化，攻击者就很容易通过分析低频系数直方图的差异探知秘密消息的踪迹[9]。为此，我们提出了改进方案。

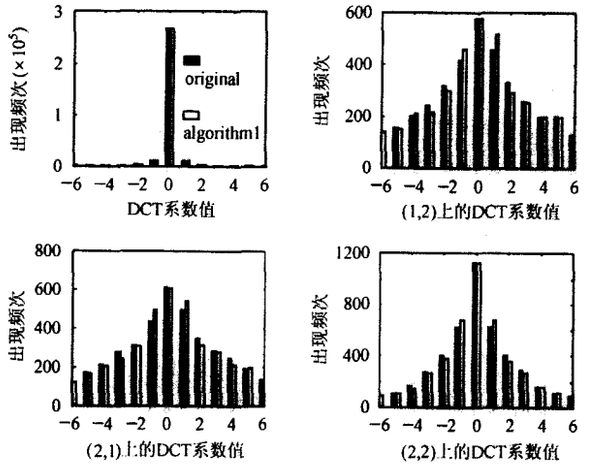

图4 用本文算法掩密前后的直方图比较

Fig.4 A comparison of the coefficient histograms before and after our algorithm (algorithm 1) has been applied

4　算法的改进：保持低频系数直方图不变

改进的算法是在上述算法的基础上增加 3 个低频系数调整信息表：Adjust_12_info，Adjust_21_info 和 Adjust_22_info，它们分别记录了(1,2)，(2,1)和(2,2)位置上的 DCT 系数被调整的情况。嵌入信息时，如果是这些位置上的系数需要改动，则查询相应的信息表，根据相应位置上系数的总体改变趋势来调整系数的改变方向；如果是其他位置上的系数需要改动，则查询 Adjust_info 表调整系数。算法流程如图 5 所示。

图 6 给出了用该算法掩密前后的直方图变化情况。图中，无论是总体直方图还是低频系数直方图，在掩密前后都没有大的改变，可见算法 2 保持了 JPEG 图像的直方图特性，从而为掩密提供了可靠的安全性保证。

```
Input: mesage, shared secret, cover image
Output: stego image
initialize PRNG with shared secret
permutate DCT coefficients with PRNG
initialize the Adjust_info table
while data left to embed do
    get next non-zero AC coefficient from cover image
    if (DCT is the coefficient on(1,2))& (DCT and the message bit are not match)
        modify DCT according to the Adjust_12_info table
        update the Adjust_12_infotable
elseif (DCT is the coefficient on(2,1))& (DCT and the message bit are not match)
        modify DCT according to the Adjust_21_info table
        update the Adjust_21_infotable
elseif (DCT is the coefficient on(2,2))& (DCT and the message bit are not match)
            modify DCT according to the Adjust_22_info table
            update the Adjust_22_infotable
elseif (DCT is the coefficient on other places)& (DCT and the message bit are-
                                                          not match)
            modify DCT according to the Adjust_info table
            update the Adjust_infotable
    end
end while
insert DCT coefficients into stego image
```

图 5　改进的算法

Fig.5　Improved algorithm

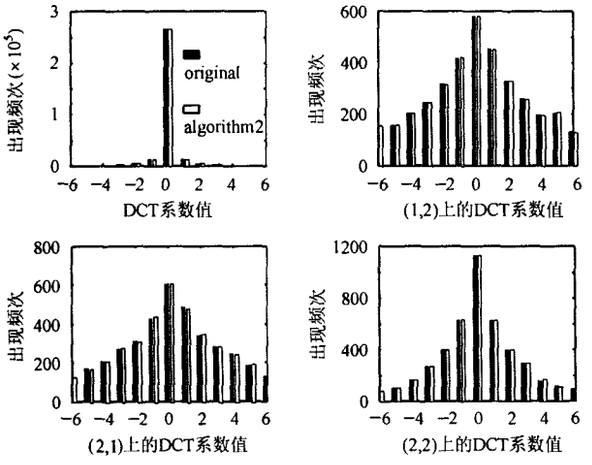

图 6　用改进算法掩密前后的直方图比较

Fig.6　A comparison of the coefficient histograms before and after the improved algorithm (algorithm 2) has been applied

5　仿真实验

分别以大小为 640×480，质量因子为 75 的 12 幅 JPEG 灰度图像为原始载体，按照上述算法进行掩密，隐藏容量和掩密前后图像的 PSNR 如表 1 所示。这里，隐藏容量是指嵌入消息对载体图像大小的比例。由表可见，本文算法能够达到 13%的隐藏容量，而且掩密前后图像的 PSNR 基本上达到 35dB 以上。如要进一步提高 PSNR，则需在算法中采用纠错编码或矩阵编码[6]技术以减少对图像的改动。

为测试掩密算法对图像直方图造成的失真，我们分析了上述 12 幅图像的总体和低频系数直方图在掩密前后的差异。设载体图像的 AC 系数直方图为 $h(d)$，$h_{(k,l)}(d)$为 $(k,l)\in\{(1,2),(2,1),(2,2)\}$ 位置上的直方图，掩密图像的总体和低频

表 1　12 幅图像的隐藏容量和掩密前后 PSNR 比较

Tab.1　A comparison of hiding capacity and PSNR before and after our algorithms have been applied to 12 images

图像文件	文件大小 (kB)	隐藏容量 (%)	PSNR(dB)	
			算法 1	算法 2
1DSC1.jpg	29	12.8	36.35	36.17
1DSC2.jpg	23	12.62	35.77	35.75
1DSC3.jpg	64	13.1	30.50	30.49
1DSC4.jpg	44	12.73	33.52	33.55
1DSC5.jpg	43	12.84	37.34	37.25
1DSC6.jpg	76	12.92	35.41	35.43
1DSC7.jpg	62	13.06	34.28	34.30
1DSC8.jpg	66	12.89	36.52	36.37
1DSC9.jpg	68	12.36	38.22	38.19
1DSC10.jpg	70	12.82	34.33	34.15
1DSC11.jpg	20	12.57	35.69	35.54
1DSC12.jpg	32	12.6	37.64	37.66

直方图分别为 $H(d)$和 $H_{(k,l)}(d)$，分别计算

$$\alpha=\frac{\sum|H(d)-h(d)|}{\sum h(d)} \tag{1}$$

$$\beta_{(k,l)}=\frac{\sum|H_{(k,l)}(d)-h_{(k,l)}(d)|}{\sum h_{(k,l)}(d)},\ (k,l)\in\{(1,2),(2,1),(2,2)\} \tag{2}$$

$\beta_{(k,l)}$ 在$\{(1,2),(2,1),(2,2)\}$上求平均得出 β，作为总体和低频系数直方图的失真率。图 7 给出了用算法 1，算法 2，JSteg 和 F5 掩密后图像的测试结果。对于总体系数直方图，算法 1 的最大失真率为 0.15%，平均失真率为 0.81%，算法 2 的最大失真率为 1.99%，平均失真率为 1.23%，JSteg 的最大失真率为 4.07%，平均失真率为 3.45%，而 F5 的最大失真率达到了 15.96%，平均失真率达到了 12.27%；对于低频系数直方图，算法 1 的最大失真率为 7.44%，平均失真率为 5.94%，算法 2 的最大失真率是 3.83%，平均失真率是 1.98%，而 JSteg 的最大失真率达到 20.06%，平均失真率是 8.28%，F5 的最大失真率达到 39.43%，平均失真率达到 20.90%。实验结果表明，本文算法仅对直方图做了微小的改变，基本上保持了载体图像的直方图特性，从而能够有效抵御针对直方图的掩

密攻击。

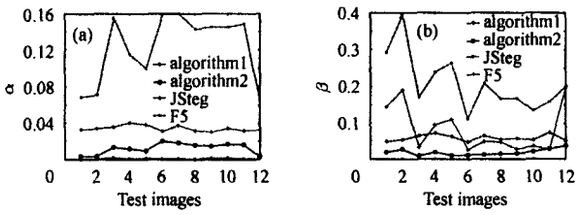

图7 掩密前后直方图的失真情况比较

(a) 总体系数直方图的失真率 (b) 低频系数直方图的失真率

Fig.7 A comparison of the distortion of the histograms before and after embedding algorithms have been applied

(a) Distortion rates of the histograms of all coefficients

(b) Distortion rates of the histograms of the coefficients on low frequency

6 结束语

本文提出了一种新的JPEG图像掩密算法，它采用建立信息表动态调整系数改变方向的思想，既能保持直方图又获得了高的隐藏容量，特别是算法2还能保持低频系数直方图的特性，因此可以抵御各种直方图攻击，从而为安全掩密提供了有效保证。

当然直方图只是描述了系数分布的一阶特性，本文算法虽然保持了载体图像的DCT系数直方图特性但是却无法保证系数的高阶属性也不变化。从图像的高阶特性探知掩密与否的事实虽然十分困难，但是攻击者还是有可能通过大量的统计分析寻找到一些蛛丝马迹。为此，我们将进一步研究保持多种统计特性的JPEG图像掩密算法。

参 考 文 献

[1] Provos N, Honeyman P. Hide and seek: an introduction to steganography. *IEEE Security & Privacy*, 2003, 1(3): 32 – 44.

[2] Fridrich J, Goljan M. Practical steganalysis – state of the art. Proc. SPIE Photonics West, Electronic Imaging 2002. Security and Watermarking of Multimedia Contents, San Jose, California, Jan. 2002: 1 – 13.

[3] Wallace G W. The JPEG still picture compression standard. *Communications of the ACM*, 1991, 34(4): 30 – 44.

[4] Derek Upham, JPEG-JSteg-V4. http://www.funet.fi/pub/crypt/steganography/jpeg-JSteg-v4.diff.gz.

[5] Provos N. OutGuess – universal steganography. August 1998. http://www.outguess.org/.

[6] Westfeld A. F5 – a steganographic algorithm: high capacity despite better steganalysis. Proc. 4th Int'l Workshop Information Hiding. Springer-Verlag, 2001, 289-302. http://wwwrn.inf.tu-dresden. de/~westfeld/f5.html.

[7] Westfeld A, Pfitzmann A. Attacks on steganographic systems. Proc. 3rd Int'l Workshop Information Hiding. Dresden, Germany, Springer-Verlag, 1999: 61 – 76.

[8] Fridrich J, Goljan M, and Hogea D. Steganalysis of JPEG images: breaking the F5 algorithm.Proc. 5th Int'l Workshop Information Hiding. Noordwijkerhout, the Netherlands, Springer-Verlag, 2002: 310 – 323.

[9] Latham A. Steganography: JPHIDE and JPSEEK. 1999. http://linux01.gwdg.de/~alatham/stego.html.

陈 丹： 女，1976年生，博士生，主要研究方向为信息隐藏、网络安全.

罗 欣： 女，1977年生，博士生，主要研究方向为图像处理、模式识别.

王育民： 男，1936年生，教授，博士生导师，主要研究方向为编码理论、密码学、信息安全.