基于可容忍失真范围的数字图像隐写方法研究

李 晟 张新鹏 王朔中
(上海大学通信与信息工程学院,上海 200072)

摘 要 以往的基于可容忍失真范围的隐写方案可以将隐写引起的失真控制在一定范围,但需要同时具备含密图像与原始图像才能提取秘密信息。提出了一种新的基于可容忍失真范围的隐写方案,该方案以一定质量因子的JPEG压缩作为可容忍失真,嵌入信息时仅在可容忍失真范围内改动原始图像,并具有含密图像的JPEG压缩版本与原始图像的JPEG压缩版本完全一致的特性,因此接收端不需原始图像,只要将含密图像与其JPEG压缩版本相减,便可提取出秘密信息,克服了原有此类方法需要原始图像才能提取秘密信息的缺点。实验结果表明,用该方案隐写所得到含密图像不仅在质量上优于其对应的JPEG压缩版本的质量,而且具有一定的抗分析安全性。

关键词 隐写 JPEG压缩 可容忍失真范围
中图法分类号: TP309 **文献标识码**: A **文章编号**: 1006-8961(2007)02-0212-06

Digital Image Steganography Based on Tolerable Error Range

LI Sheng, ZHANG Xin-peng, WANG Shuo-zhong
(*School of Communication and Information Engineering, Shanghai University, Shanghai* 200072)

Abstract Previous proposed steganographic schemes based on tolerable error range(TER) can restrict the distortion caused by data-hiding within an accepted range, but both the stego-image and the original cover image are necessary for extracting the secret message. This paper presents a novel TER-based steganographic scheme, in which JPEG compression under a certain quality factor is regarded as TER, and the modification caused by data-hiding on each pixel is less than that caused by JPEG compression. Furthermore, the JPEG version of a stego-image is completely the same as that of the corresponding original one. At receiver side, the embedded secret data can be extracted by subtracting the stego-image from its JPEG version, so that the original cover is needless. Experimental results show that the presented scheme can gain a stego-image which is superior to its JPEG version in quality, and possesses a capability of withstanding the statistical analysis.

Keywords steganography, JPEG compression, tolerable error range(TER)

1 引 言

数字隐写(Steganography,或称密写)是信息隐藏的一个重要分支,其目的是将信息秘密隐藏在载体信息中,不引起第三方怀疑地安全发送出去[1,2],即将"正在通信"这一事实隐蔽起来。数字隐写必然会造成载体数据的失真,而失真过大则会引起视觉异常或统计异常,暴露秘密信息的存在。因此隐蔽性是衡量隐写技术优劣的最重要标准。

研究者已提出根据视觉特性进行信息嵌入的方法提高隐写隐蔽性,也就是在视觉不敏感的区域嵌入较多秘密信息,而在视觉较敏感的区域嵌入少量秘密信息。例如位平面复杂度分割(bit-plane complexity segmentation, BPCS)隐写将秘密信息隐藏于变化剧烈、复杂度较高的位面小块[3];像素灰度差值(pixel-value differencing, PVD)隐写在差值较大的两个像素中嵌入较多信息[4];混合进制(multiple-base notational system, MBNS)隐写则由图像局部起伏程度决定当前像素负载的秘密信

基金项目:国家自然科学基金项目(60372090,60502039);上海市科委基础研究重点项目(04JC14037);上海市青年科技启明星计划(06QA14022)
收稿日期:2006-10-13;**改回日期**:2006-11-03
第一作者简介:李晟(1984~),男。上海大学通信与信息工程学院硕士研究生。研究方向为信号处理、信息隐藏。E-mail:lisheng@shu.edu.cn

息量[5]。

另一类隐写方法保证隐写引起的失真不超过预先规定的压缩编码引起的失真,藉此提高秘密信息的隐蔽性。文献[6]首先将原始图像进行某种有损压缩,并将压缩图像与原始图像相减得到可容忍失真范围(tolerable error range, TER)矩阵,然后根据TER矩阵逐个像素嵌入秘密信息,从而可以得到质量比压缩图像更好的含密图像。文献[7]在文献[6]的基础上做了改进,提出了一种应用在医院电子数据交换的信息隐藏方案,它将TER矩阵中的元素分类处理,值为0的元素不嵌信息,值为1的元素用于嵌入医生的签名,值大于1的元素用于嵌入病人的信息。为进一步提高含密图像质量,文献[8]对TER矩阵中的元素进行排序,然后根据排序后的TER矩阵隐藏秘密信息,并在隐藏信息的同时采用零复位以及补偿比特的技术,有效降低了隐写图像的失真。虽然文献[6]~[8]所提出的方法均能得到质量比有损图像更好的隐写图像,但是存在一个共同的弱点,那就是接收端必须同时拥有含密图像和原始图像才能提取秘密信息,为实际应用带来了不便。

本文提出了一种新的基于可容忍失真范围的隐写方案,不但保证了含密图像的质量比原始图像JPEG压缩版本的质量更好,而且接收端在提取秘密信息时不需要原始图像。

2　信息嵌入与提取

本文方案同样是以未压缩格式图像作为载体,采用一定质量因子的JPEG压缩作为可容忍失真,并保证嵌入秘密信息对载体图像的改动不超出可容忍失真。所不同的是本文方案还保证了含密载体的JPEG压缩版本与原始载体的JPEG压缩版本完全相同,并用载体含密部分的像素灰度与JPEG压缩后对应像素灰度的差值表示秘密信息。因此接收端不必拥有原始载体,利用含密载体以及JPEG压缩所采用的质量因子便可提取秘密信息。

2.1　信息嵌入

隐写端首先获得未压缩格式载体图像的JPEG压缩版本(隐写者与接收者预先约定压缩质量因子或量化矩阵):将原始图像分为8×8的小块,对每个小块进行2维DCT变换,按照质量因子对应的量化矩阵进行量化,然后逆量化、逆DCT变换,并将得到的值做舍入溢出处理,即将小于0的值变为0,大于255的值变为255,并对0与255之间的值进行四舍五入取整。将JPEG压缩版本与原始载体相减,所得即TER矩阵,隐写时对每个像素的修改应在0与该像素对应的TER值之间。例如原始图像的一个8×8块为

$$\boldsymbol{C}=\begin{bmatrix}138&152&135&123&160&175&174&157\\135&158&135&139&162&170&171&134\\155&158&122&162&173&173&160&114\\169&158&132&168&178&161&151&99\\170&148&148&173&168&158&151&106\\158&135&148&160&153&160&140&116\\162&135&149&153&161&157&106&106\\152&145&160&158&168&144&103&131\end{bmatrix}\tag{1}$$

对它进行2维DCT变换得到DCT系数矩阵:

$$\boldsymbol{M}_{\mathrm{DCT}}=\begin{bmatrix}1191.6&33.1&-63.9&77.3&-1.4&2.8&-10.8&-3.5\\24.6&-57.0&28.3&19.5&-35.8&-4.4&-37.0&0.3\\-13.9&-26.8&20.8&-27.0&-5.7&-33.3&24.1&6.8\\-2.4&-15.9&15.3&-5.3&-11.2&11.4&13.2&6.2\\11.6&5.1&2.8&-6.9&7.1&-4.0&-2.7&7.7\\-7.1&7.3&-1.5&16.0&5.4&-3.2&4.1&-2.1\\4.6&-11.0&5.1&-2.9&2.2&1.3&-0.6&-4.0\\2.4&3.5&-2.6&5.2&3.8&1.5&&2.0\end{bmatrix}\tag{2}$$

采用质量因子为50的JPEG压缩,其量化矩阵为

$$\boldsymbol{Q}=\begin{bmatrix}16&11&10&16&24&40&51&61\\12&12&14&19&26&58&60&55\\14&13&16&24&40&57&69&56\\14&17&22&29&51&87&80&62\\18&22&37&56&68&109&103&77\\24&35&55&64&81&104&113&92\\49&64&78&87&103&121&120&101\\72&92&95&98&112&100&103&99\end{bmatrix}\tag{3}$$

对DCT系数矩阵中的元素分别用量化矩阵中对应的量化步长进行量化,得到量化后的DCT系数矩阵为

$$\boldsymbol{M}'_{\mathrm{DCT}}=\begin{bmatrix}74&3&-6&5&0&0&0&0\\2&-5&2&1&-1&0&-1&0\\-1&-2&1&-1&0&-1&0&0\\0&-1&1&0&0&0&0&0\\1&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\end{bmatrix}\tag{4}$$

对量化后的 DCT 系数矩阵逆量化、逆 DCT 变换并对所得到的值做舍入溢出处理就得到了 C 的压缩版本

$$L=\begin{bmatrix}132&167&116&127&171&167&177&161\\138&157&121&138&168&163&167&134\\154&148&134&157&168&164&160&108\\172&143&146&170&167&169&158&101\\177&137&149&166&160&167&150&107\\167&132&148&153&154&159&128&114\\155&137&154&147&159&155&104&119\\151&146&164&150&169&156&92&123\end{bmatrix} \tag{5}$$

L 减去 C 得到的 TER 矩阵如下：

$$M_{\mathrm{TER}}=\begin{bmatrix}-6&15&-19&4&11&-8&3&4\\3&-1&-14&-1&6&-7&-4&0\\-1&-10&12&-5&-5&-9&0&-6\\3&-15&14&2&-11&8&7&2\\7&-11&1&-7&-8&9&-1&1\\9&-3&0&-7&1&-1&-12&-2\\-7&2&5&-6&-2&-2&-2&13\\-1&1&4&-8&1&12&-11&-8\end{bmatrix} \tag{6}$$

将图像中的所有小块分为两类：一类为 JPEG 压缩后存在值 0 或者 255 的小块，称这种小块为“不可嵌的”；另一类为其他的小块，称为“可嵌的”。隐写时仅改动可嵌小块，设当前可嵌小块为 C，按照下面的步骤逐个像素修改载体像素灰度，嵌入秘密信息：

(1) 从载体小块中依次取出像素，设 p_o 为从 C 中取出的某像素的灰度值，p_c 为其压缩版本（记为 L）中对应像素的值，则其 TER 值为 $p_d=p_c-p_o$。

(2) 从秘密信息序列中依次取出 n 比特，其中，

$$n=\lfloor \log_2(|p_d|+1)\rfloor \tag{7}$$

$\lfloor\cdot\rfloor$ 表示向下取整，计算这 n 比特对应的十进制值

$$m=\begin{cases}0 & n=0\\ 2^n-1+\sum_{i=1}^{n}d_i\times 2^{n-i} & n\neq 0\end{cases} \tag{8}$$

其中，d_i 为待嵌秘密信息序列的第 i 个比特。

(3) 将 m 与 $|p_d|$ 进行比较，如果 $m\leqslant|p_d|$，则 m 保持不变；如果 $m>|p_d|$，说明当前像素的可容忍失真不足以嵌入这 n 个比特，重新从秘密信息序列依次取出 $n-1$ 个比特，并根据式(8)得到与它们对应的十进制值 m，此时 m 必然小于等于 $|p_d|$，证明如下：

如果 $m=0$，那么显然 $m\leqslant|p_d|$。如果 $m>0$，则

$$m=2^{n-1}-1+\sum_{i=1}^{n-1}d_i\times 2^{n-i-1}$$

由式(7)知 $|p_d|\geqslant 2^n-1$，因为 d_i 等于 0 或者 1，故

$$\sum_{i=1}^{n-1}d_i\times 2^{n-i-1}\leqslant 2^{n-1}$$

所以 $m\leqslant|p_d|$。

(4) 将 p_o 改为 p_s，即

$$p_s=\begin{cases}m+p_c & p_d<0\\ p_c & p_d=0\\ p_c-m & p_d>0\end{cases} \tag{9}$$

(5) 当小块中所有像素都嵌入信息之后，将含密小块进行同样质量因子的 JPEG 压缩，并与 L 比较，如果相同则将原始小块改为含密小块，秘密信息已被有效嵌入；如果不同则说明信息嵌入无效，将该小块改为 L，并在后续小块中重新嵌入这些秘密比特。

例如要在式(1)的图像块中嵌入秘密信息“1010001001010011100…”，首先根据(1)的压缩版本 L 中不存在值 0 或者 255 判定该图像块是可嵌的。对于该图像块的第 1 个像素有 $p_o=138$，$p_c=132$，$p_d=-6$；由式(7)得 $n=2$，从秘密信息序列中依次取出 2 个比特“10”，即 $d_1=1$，$d_2=0$；将 n、d_1、d_2 代入式(8)得到 $m=5$；显然 $m<|p_d|$，说明该像素的可容忍失真能够嵌入“10”这 2 个比特；最后根据式(9)将 p_c 修改为 $p_s=m+p_c=137$。对于(1)中第 2 个像素有 $p_o=152$，$p_c=167$，$p_d=15$；由式(7)得 $n=4$，从秘密信息序列中依次取出 4 个比特“1000”，即 $d_1=1$，$d_2=0$，$d_3=0$，$d_4=0$；将 n、d_1、d_2、d_3、d_4 代入式(8)得到 $m=23$；此时 $m>|p_d|$，说明该像素的可容忍失真不足以嵌入“1000”这 4 个比特，重新从秘密信息序列中依次取出“100”这 3 个比特，由式(8)得到 $m=11$；最后根据式(9)将 p_c 修改为 $p_s=p_c-m=156$。对该图像块中所有像素进行上述操作之后共嵌入 103 比特，得到的含密块 S 如下：

$$S=\begin{bmatrix}137&156&135&125&162&171&175&159\\135&157&134&139&163&168&171&134\\154&153&125&162&170&169&160&114\\171&154&135&169&176&163&154&100\\171&142&149&171&165&159&151&106\\158&134&148&156&154&159&139&116\\161&135&152&153&160&156&105&107\\152&145&162&154&169&144&98&129\end{bmatrix} \tag{10}$$

对 S 采用质量因子为 50 的 JPEG 压缩得到的压缩版本与 L 是一样的，说明秘密信息已被有效嵌入。

对同一幅载体图像来说,选择不同的质量因子进行压缩所得到的 TER 矩阵是不一样的。由于低质量因子所对应的量化表中元素的值较大,所以一般来说采用低质量因子进行压缩所得到的 TER 矩阵中元素的绝对值就要比用高质量因子压缩所得到的大。而就某个像素而言,它所对应 TER 值的绝对值越大,隐写时对该像素所做的改动可能就越大,嵌入的信息量也就越大。所以使用较低的压缩质量因子所能嵌入的信息量高于使用较高质量因子的嵌入量;另一方面,使用较高质量因子时获得的含密图像质量要优于使用较低质量因子时的情况。

2.2　信息提取

逐块操作,对于某一小块,先对其做压缩得到它的压缩版本,如果压缩版本中存在值 0 或者 255,则丢弃该小块,继续操作下一个小块。对未被丢弃的小块逐个像素操作,对于其中的某一像素,先求出 $m=|p_c-p_s|$,然后计算该像素所负载的秘密比特数 $n=\lfloor \log_2(m+1) \rfloor$,由下式就可以得到该像素对应的秘密比特:

$$d_i=\begin{cases}\left\lfloor \dfrac{m-2^n+1}{2^{n-1}} \right\rfloor & i=1 \\ \left\lfloor \dfrac{m-2^n+1-\sum_{k=1}^{i-1} d_k \times 2^{n-k}}{2^{n-i}} \right\rfloor & 1 \leqslant i \leqslant n \end{cases} \tag{11}$$

最后将提取出的比特依次连接,即秘密信息。

为了防止信息提取出错,本文提出的信息隐藏方案采取了下面两个措施:

(1)不改变不可嵌小块。原因如下:不可嵌小块的压缩版本中存在值 0 或者 255,在舍入溢出之前它们可能是绝对值很大的负数或者是比 255 大很多的正数。如果对这样的小块进行改动,而改动后小块的压缩版本又与原始小块的压缩版本不一致,那么为了保证含密小块的 JPEG 压缩版本与原始小块的 JPEG 压缩版本完全相同,隐写端只能将改动后的小块恢复成原始小块,所以有必要采取本措施,提取时跳过这些小块即可。

(2)将嵌入信息无效的可嵌小块改为原始小块的压缩版本。原因如下:当 $\boldsymbol{C}$ 嵌入信息无效时,如果不采取措施,接收端得到的 $\boldsymbol{S}$ 的压缩版本将不是 $\boldsymbol{L}$,很显然这会造成信息的误提取。而采取本措施之后,接收端得到的 $\boldsymbol{S}$ 即为 $\boldsymbol{C}$ 的压缩版本 $\boldsymbol{L}$,由于对 $\boldsymbol{L}$ 进行相同的再压缩得到的小块仍为 $\boldsymbol{L}$,所以提取的时候将得到 0 个秘密比特,这与 $\boldsymbol{C}$ 嵌入信息无效是一致的。

3　实验结果

分别以大小为 256 × 256 的测试图像 Miss、Camera man 为载体,以质量因子为 30 的 JPEG 压缩作为可容忍失真,采用本文提出的方法分别能够嵌入 6.8×10^4、6.2×10^4 比特的秘密信息。图 1 分别给出了 Miss 以及 Camera man 的原始图像、JPEG 压缩版本及相应的含密图像,可以看出含密图像比 JPEG 压缩版本的视觉质量好。

以质量因子 30、50、70 的 JPEG 压缩作为可容忍失真分别在大小为 512 × 512 的测试图像 Lena、Peppers、Plane、Baboon 中进行信息嵌入,得到 12 幅完全嵌入的含密图像。表 1 给出了 JPEG 压缩和信息隐藏引起的 PSNR 及嵌入量,从表 1 中可看出含密图像的失真必然小于 JPEG 压缩失真,并且较低的质量因子对应较大的嵌入量。

为验证本文方案的安全性,分别用 SPA 法[9]和 RS 法[10]对上述得到的 12 幅含密图像进行隐写分析,结果如表 2 所示,可以看出无论是 SPA 法还是 RS 法对含密图像嵌入可能性的估计均小于 5%,仍属于正常图像含密可能性的取值范围,可见本文算法具有一定的抗分析安全性。

表 1　JPEG 压缩和信息隐藏引起的 PSNR 及嵌入量

Tab. 1　Embedding capacity and the PSNR caused by JPEG compression and data-hiding

载体图像	可容忍失真所依据的 JPEG 质量因子								
	30			50			70		
	JPEG 压缩 PSNR(dB)	含密图像 PSNR(dB)	嵌入量 (10^5 bits)	JPEG 压缩 PSNR(dB)	含密图像 PSNR(dB)	嵌入量 (10^5 bits)	JPEG 压缩 PSNR(dB)	含密图像 PSNR(dB)	嵌入量 (10^5 bits)
Lena	35.0	43.5	2.7	36.6	43.9	2.4	38.1	43.5	1.9
Peppers	33.5	40.9	3.2	34.8	41.7	2.9	35.9	40.9	2.3
Plane	34.2	43.0	2.9	36.0	43.4	2.4	37.8	42.9	1.8
Baboon	27.3	33.4	4.5	27.0	33.0	3.5	31.1	33.4	2.2

(a) 原始图像 Miss　(b) 质量因子为 30 的 JPEG 压缩版本 (PSNR = 35.8dB)　(c) 对应图(b)的含密图像 (PSNR = 44.7dB)

(d) 原始图像 Camera man　(e) 质量因子为 30 的 JPEG 压缩版本 (PSNR = 29.9dB)　(f) 对应图(e)的含密图像 (PSNR = 35.1dB)

图 1　原始图像、JPEG 压缩版本以及含密图像

Fig. 1　Original cover images, its JPEG versions and stego-images

表 2　对采用不同可容忍失真进行隐写所得的含密图像进行检测的结果

Tab. 2　Steganalytic results of the stego-images corresponding to different TER

载体图像	可容忍失真所依据的 JPEG 质量因子					
	30		50		70	
	SPA 分析法	RS 分析法	SPA 分析法	RS 分析法	SPA 分析法	RS 分析法
Lena	-0.001 7	-0.039 8	0.017 5	-0.012 9	0.000 4	0.000 7
Peppers	0.003 8	0.017 3	0.017 2	-0.012 8	0.033 2	-0.004 3
Plane	0.000 9	0.006 1	-0.009 9	0.003 8	0.014 9	-0.019 1
Baboon	-0.039 6	0.044 8	-0.122 9	0.047 0	0.015 6	-0.012 1

4　结　论

本文提出了一种新的利用可容忍失真范围进行隐写的方法。该方法仅在可嵌小块中进行信息隐藏，并且将嵌入信息无效的块改为原始小块的压缩版本，接收方只需要对含密图像做压缩，然后将含密图像与其压缩版本做比较就能提取出秘密信息。不仅解决了现有此类方法需要原始图像支持才能提取秘密信息的问题，并且含密图像的失真不会大于可

容忍失真,大大提高了此类隐写方法的应用价值。

参考文献(References)

1 Petitcolas F A P, Anderson R J, Kuhn M G. Information hiding—a survey[J]. Proceedings of IEEE, 1999, **87**(7): 1062 ~ 1078.

2 Wang H, Wang S. Cyber warfare—steganography vs. steganalysis [J]. Communication of the ACM, 2004, **47**(10): 76 ~ 82.

3 Noda H, Spaulding J, Shirazi M N, *et al*. Application of bit-plane decomposition steganography to JPEG2000 encoded images[J]. IEEE Signal Processing Letters, 2002, **9**(12): 410 ~ 413.

4 Wu D C, Tsai W H. A steganographic method for images by pixel-value differencing[J]. Pattern Recognition Letters, 2003, **24**(9 - 10): 1613 ~ 1626.

5 Zhang X, Wang S. Steganography using multiple-base notational system and human vision sensitivity[J]. IEEE Signal Processing Letters, 2005, **12**(1): 67 ~ 70.

6 Wu D C, Tsai W H. Data hiding in images via multiple-based number conversion and lossy compression[J]. IEEE Transactions on Consumer Electronics, 1998, **44**(4): 1406 ~ 1412.

7 Chao H M, Hsu C M, Miaou S G. A data-hiding technique with authentication, integration, and confidentiality for electronic patient records[J]. IEEE Transactions on Information Technology in Biomedicine, 2002, **6**(1): 46 ~ 53.

8 Chang C C, Chuang J C, Lai Y P. Hiding data in multitone images for data communications[J]. IEE Proc.-Vis. Image Signal Process, 2004, **151**(2): 137 ~ 145.

9 Dumistrescu S, Wu Xiao-lin, Wang Zhe. Detecting of LSB steganography via sample pair analysis[J]. IEEE Transactions on Signal Processing, 2003, **51**(7): 1995 ~ 2007.

10 Fridrich J, Goljan M, Du R. Detecting LSB steganography in color and gray-scale images[J]. Magazine of IEEE Multimedia, 2001, **8**(4): 22 ~ 28.