基于整数小波的无损数据隐藏*

杨程云[1], 宣国荣[1], 施云庆[2], 郑伊展[1], 郑俊翔[1], 刘连生[3], 白维朝[3]
(1. 同济大学计算机系, 上海 200092;
2. 美国新泽西工学院, Newark, NJ, USA;
3. 深圳宝嘉电子设备有限公司, 广东 深圳 518000)

摘 要: 介绍两种基于整数小波的无损数据隐藏方法, 分别称为扩谱方法及压缩扩展方法。这两种方法均把数据嵌入到图像整数小波变换后的高频子带系数中; 为防止小波反变换时图像灰度溢出问题, 直方图调整技术被使用。实验结果表明, 两种方法均达到甚至超过当前无损数据隐藏领域最好水平。

关键词: 无损数据隐藏; 整数小波; 直方图调整; 扩谱; 压缩扩展
中图分类号: TP301.6 文献标识码: A 文章编号: 0529-6579 (2004) S2-0196-04

无损数据隐藏是数据隐藏领域的一个分支, 其不但能提取出嵌入的隐藏数据, 而且还能恢复原始的载体图像。近来, 各种无损数据隐藏方法被相继提出[1-6]。Fridrich 等[1] 利用图像的冗余性, 对图像空域的某一位平面进行压缩, 压缩后腾出的空间被用来隐藏数据; 但是由于压缩性能的限制, 只能嵌入较小容量的数据。在其基础上, Celik[2] 提出泛化的空域 LSB 方法, 并采用更有效的压缩技术, 从而在嵌入容量、视觉质量和灵活性上都得到大大提高。Domingo-Ferrer 等[3] 提出一种空域扩谱数据隐藏方法, 但是该方法只能对预处理过的图像保证其无损性。Jun Tian[4] 提出一种差值扩展技术, 将数据嵌入到 Haar 小波变换后的高频系数中; 该方法是当前最好的无损数据隐藏方法之一。最近, 杨边等[5] 提出一种基于 DCT 变换和压缩扩展技术的无损数据隐藏方法, 也取得了较好的效果。本文在上述这些论文成果的启发下, 以及在我们原有方法的基础上[6], 提出两种新的基于整数小波的无损数据隐藏方法, 分别称为扩谱方法及压缩扩展方法; 实验结果表明这两种方法无论在视觉效果还是嵌入容量上均达到甚至超过当前无损数据隐藏领域最好水平。下面进行详细介绍。

1 整数小波变换

本文方法建立在小波变换基础上。小波变换具有解相关、能量集中、与 HVS 相一致等优点, 非常适合用于数据隐藏技术中。无损数据隐藏技术要求在小波变换及逆变换时不能丢失信息。由于信号经过第一代小波变换后产生的是浮点数, 受到计算机有限字长的影响, 往往不能精确地重构原始信号。为此, 我们采用了第二代小波变换的提升小波 (lifting scheme) 的整数形式, 即变换前后系数都是整数形式的整数小波变换。对于具体小波基的选择, 经过反复比较, 我们采用 JPEG2000 的 CDF (2, 2)。

2 直方图调整技术

由于数据嵌入时, 我们是对小波系数进行修改, 因此修改后的小波系数在小波逆变换时容易发生灰度“溢出”现象。以 256 级灰度图像为例, 原始图像灰度数据的取值范围为 [0, 255]。当对嵌入数据后的小波系数进行逆变换时, 得到的图像灰度数值就有可能小于 0 或大于 255, 这时, 就发生了灰度“溢出”。为防止溢出发生, 我们采用图像直方图调整技术, 如图 1 所示。图像直方图预先被压缩到 $[G/2, 255-G/2]$ 范围 (G 表示两边共有多少灰度空出来), 这样当对嵌入数据后的小波系数进行逆变换时, 虽然图像灰度数值可能超出 $[G/2, 255-G/2]$ 范围, 但是只要不超过原取值范围 [0, 255], 则仍可以保证在小波逆变换时灰度不发生“溢出”。

显然对于被压缩掉的直方图信息我们需对其进行记录保存。因此, 嵌入到小波系数中的数据将包含二部分内容: ①要嵌入的水印数据; ②被压缩掉

* 收稿日期: 2004-09-11
基金项目: 国家自然科学基金资助项目 (90304017)
作者简介: 杨程云 (1978 年生), 男, 博士研究生; E-mail: chengyunv@sina.com

直方图的记录数据（一般较小）。这样提取时，根据提取出来的直方图记录信息，原始图像便能得到完全恢复。

3　两种新的数据隐藏方案

接下来介绍2种新的无损数据隐藏方案：扩谱方法和压缩扩展方法；这两种方法最大的一个共同点就是他们都是通过修改小波高频子带系数（HL，LH，HH）来实现数据的嵌入隐藏（图2）。下面依次进行说明。

3.1　扩谱方法

对于绝大部分图像来说，其绝大部分小波高频子带系数的绝对值都是很小的。这启发我们可以用比特数据（“0”或“1”）对小波系数的正负进行调制来实现数据的嵌入隐藏。说明如下：

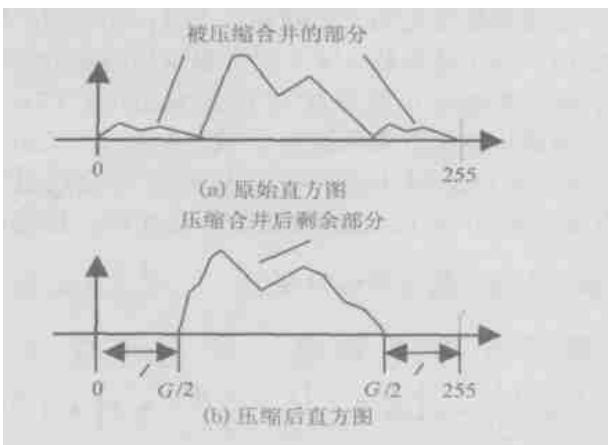

图1　直方图调整原理图

Fig. 1　Histogram modifictaion

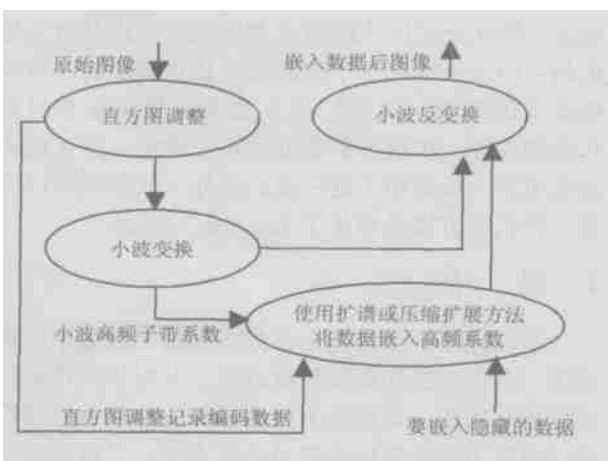

图2　两方法嵌入流程框图

Fig. 2　Data embedding diagram

我们从3个高频子带中任取一个小波系数 W。一般来讲，W是一个绝对值较小的整数，不妨假设$|W|<A$。现在我们把一个bit（“0”或“1”）嵌入到该系数中。根据要嵌入的bit对W进行修改：$W'=W+A*S$；其中，当要嵌入的bit为“1”时，S=1，否则当要嵌入的bit为“0”时，$S=-1$。这样提取时，由于先前假设$|W|<A$，因此$\mathrm{Sign}(W')=\mathrm{Sign}(W+A*S)=\mathrm{Sign}(A*S)=\mathrm{Sign}(S)$；也就是说，可以根据$W'$的正负来判断嵌入的bit是“1”还是“0”，当$W'>0$时，bit为“1”；当$W'<0$时，bit为“0”。最后，提取出嵌入在$W'$中的bit信息后，则可以恢复原来的系数$W$：$W=W'-A*S$，其中$S$的值根据提取出来的bit用上述嵌入时的规则确定。

显然，从上面的描述可以看到，该方法的成功还需满足一个条件：$|W|<A$。我们可以通过嵌入伪信息的办法来解决这个问题。如果$|W|\geq A$，则我们按如下方式修改W：如果$W\geq A$，则我们取$S=1$；也就是说在该系数上嵌入一个伪bit“1”（并不真正嵌入一个bit“1”的数据信息），这样当从W'中提取bit信息时，我们知道提取出来的bit肯定是“1”（因为W'一定是一个正数），接着我们恢复出原来的系数W。显然$|W|\geq A$，于是我们知道在该系数上嵌入的是一个伪bit信息，从而可以把该信息忽略；同样如果$W\leqslant -A$，则我们取$S=-1$，即在该系数上嵌入一个伪bit“0”，这样当要从W'中提取bit信息时，由于$W'<0$我们知道提取出来的bit肯定是“0”；接着我们恢复出原来的系数W。由于$|W|<A$，知道在该系数上嵌入的是一个伪bit信息，从而可以把该信息忽略。

综上所述，扩谱方法在每个小波系数上均嵌入一个bit信息：在$|W|<A$时，嵌入一个bit的有效数据信息；在$|W|\geq A$时，嵌入一个bit的无效伪信息。通过嵌入伪信息的方式，我们解决了在提取信息时无法判断在哪些系数上嵌入了数据bit的问题。

3.2　压缩扩展方法

压缩扩展（companding）是指对一个信号先压缩然后展开的过程。如果我们用表示压缩函数，表示扩展函数，则理想情况下，对一个信号作Companding操作，应有：$E(C(x))=x$。压缩扩展技术可用于无损数据隐藏，一个简单的实现过程如下：

（1）用压缩函数C对x进行压缩得到一个新的信号$y=C(x)$，y的二进制表示为$p_1p_2\cdots p_n$，$p_i\in\{0,1\}$；

（2）通过在y的LSB后附加一个$b\in\{0,1\}$，我们可以嵌入一个bit（b）的信息，此时信号y变成

$P_1P_2\cdots P_{nb}$；不失一般性，用 P 来表示这个嵌入操作，即$y'=P(y)$；

(3) 如果 $y'\approx x$，则信号的这种变化将很难被察觉；

(4) 提取时，只需提取信号 y' 的 LSB 即可，即 $b=\mathrm{LSB}(y')$，同时恢复出信号 $y=\frac{y'}{2}$。

(5) 得到 y 后，便可以恢复出原来的信号 $x=E(y)$。

从上面的叙述可以看出，C、E 和 P 的选取需满足2个条件：

(1) $E(C(x))=x$；

(2) $P(C(x))\approx x$。对数字信号而言，由于其离散量化性质，压缩扩展函数往往使用其量化近似函数 C_Q 和 E_Q：$C_Q=Q(C)$，$E_Q=Q(E)$。这里 Q 为量化操作。此时，对有些 x 信号值，

$$E_Q(C_Q(x))\neq x$$

即

$$r=E_Q(C_Qx)-x\neq 0$$

这时为了恢复原来的 x，我们必须记录两者之间的差值 r，然后将差值 r 和待隐藏的数据一同作为 Payload 数据嵌入到载体信号 x 中。

正如前面所述，图像大部分小波高频子带系数一般都较小。这给压缩函数的选取提供了很大的余地，此时即使像 $F(x)=x$ 这样的函数也能考虑作为压缩函数使用，这是因为这时 y' 虽然大约为 x 的2倍，但由于 x 较小，因此两者的差值仍然控制在一个较小的范围内。但是，尽管大部分小波高频系数较小，仍然有一些系数其取值较大。对这些小波系数，压缩函数应特别考虑条件 (2) 的限制。显然这时 $F(x)=x$ 这样的函数不再适用。综合考虑这两种情况，我们使用一个分段线性函数作为压缩函数。其方程式如下：

$$C(x)=\begin{cases}x, & |x|<A\\ \mathrm{sign}(x)*\left(\left\lfloor\frac{|x|-A}{2}\right\rfloor+A\right), & |x|\geq A\end{cases}$$

上式中 A 是预先设置的一个阈值。从上面的式子可以看出，当 $|x|\geq A$ 时，x 和 $(x+1)$ (或 $(x-1)$) 压缩后得到同一个 y 值，因此根据前面的讨论，此时需要对 x 和 $(x+1)$ (或 $(x-1)$) 进行编码，然后将这些编码信息同待隐藏数据一同嵌入到小波系数中。

3.3 两种数据嵌入方案的分析比较

至此，我们已经对扩谱和压缩扩展这两种数据嵌入方案作了完整的介绍说明。从上面的叙述中，我们可以看到，两种方案有如下一些共同点：

(1) 都是通过修改小波高频子带系数来实现数据信息的嵌入；且都利用了图像的大部分小波高频子带系数其幅度值比较小这个规律；

(2) 这两种方案都可以通过一个事先设定的域值 A 来达到嵌入后图像视觉效果和嵌入容量之间的折衷。当 A 取值较小时，由于嵌入前后小波系数改变相对较小，因此此时能取得较好的视觉效果；当 A 取值较大时，则能取得更大的嵌入容量。实际嵌入时，我们便可以根据需要嵌入的 Payload 数据大小选取一个合适的 A 值，具有很好的灵活性；

下面分析讨论使用这两种嵌入方案时小波系数变化的规律。不失一般性，分析时假设 $w\geq 0$；当 $w<0$ 的情况，分析结果同样成立。显然在两种方法中小波系数变化的大小均取决于 A。在扩谱方法中，小波系数变化的大小刚好等于 A；在压缩扩展方法中，当小波系数 $w<A$ 时：根据压缩函数的定义，嵌入数据后小波系数 w 将变为 $2w$ 或 $(2w+1)$，因此小波系数变化值为 w 或 $(w+1)$；又由于 $w<A$，所以此时小波系数变化最大不会超过 A (当 $w=A-1$ 时)；当小波系数 $w\geq A$ 时：根据压缩函数小波系数压缩后将变为 $\left\lfloor\frac{w-A}{2}\right\rfloor+A$，嵌入数据后小波系数进一步变化为 $2*\left[\left\lfloor\frac{w-A}{2}\right\rfloor+A\right]$ 或 $2*\left(\left\lfloor\frac{w-A}{2}\right\rfloor+A\right)+1$，因此此时小波系数变化值为 $(A-1)$ 或 A 或 $(A+1)$。从这些分析可以看出，当 A 取值接近 0 时，扩谱方法跟压缩扩展方法对小波系数改变幅度较为接近，因此此时嵌入图像视觉效果应该也是较为接近的；但由于大部分小波系数都是比较小的，因此随着 A 的增大，压缩扩展方法的优势将逐渐显露从而能取得比扩谱方法更好的视觉效果。图 3 的实验结果进一步证明了这一点；另外，从图中可以看到，我们的方法甚至优于 Jun Tian[4] 方法。

4 结 语

本文介绍了两种基于整数小波的无损数据隐藏方法：扩谱方法和压缩扩展方法，并对该两种方法进行相互比较。实验结果表明两种方法均达到甚至超过当前无损数据隐藏领域最好水平。目前这两种方法在银行退休金发放系统中获得应用。银行退休金发放中，人们在家中按月领取养老金，因此身份认证部分是系统的核心和关键。在该系统中，用本文方法将认证散列同用户信息无损隐藏到指纹图像中，从而进一步加强了系统的安全性。

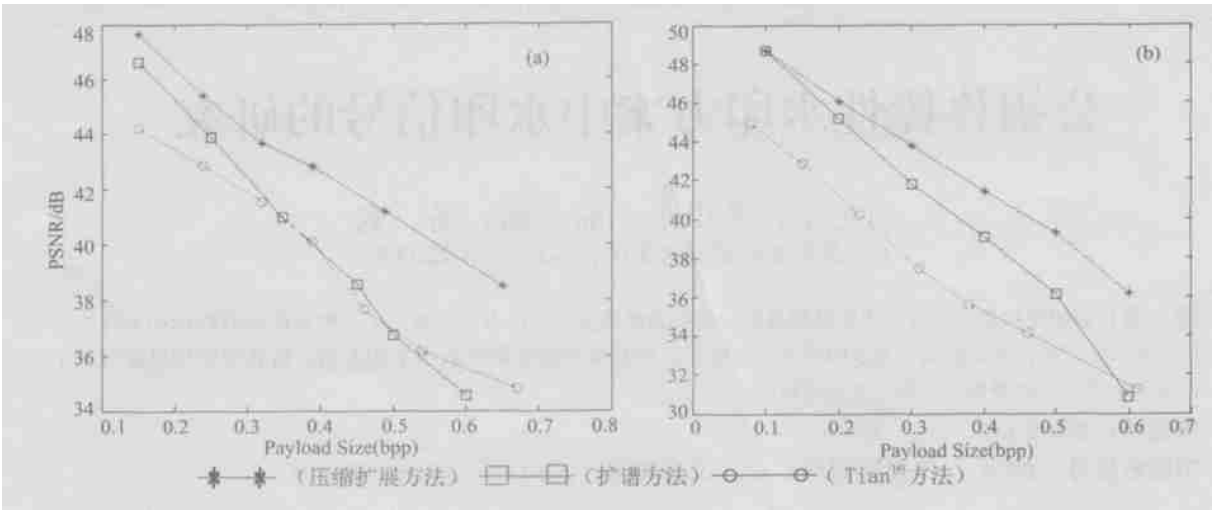

图 3　3 种方法在 Lena (a) 和 Barbara (b) 上的比较曲线图

Fig 3　Comparison results on Lena (a) and Barbara (b) images

参考文献：

[1] JESSICA F, GOLJAN M, DU R. Invertible authentication [J]. Proc SPIE Photonics West, Security and Watermarking of Multimedia Contents III, 2001, 397: 197—208.

[2] CELIK M, SHARMA G, TEKALP A M. Reversible data hiding[J]. Proceedings of the International Conference on Image Processing, 2002, 2: 157—160.

[3] DOMINGO—FERRER J, SEB′E F. Invertible spread-spectrum watermarking for image authentication and multilevel access to precision-critical watermarked images [C]. Proceedings of the International Conference on Information Technology: Coding and Computing, 2002: 152—157.

[4] TIAN J. Reversible data embedding using a difference expansion[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003(8): 890—896.

[5] YANG B, SCHMUCKER M, FUNK W. Integer DCT-based reversible watermarking for images using companding technique[C]. Proceedings of SPIE, 2004: 5306.

[6] XUAN GK, ZHUJ, CHENJDG. Distortionless data hiding based on integer wavelet transform [J]. IEE Electronics Letters, 2002(12): 1646—1648.

Reversible Data Hiding Based on Integer Wavelet

YANG Cheng yun[1], *XUAN Guo rong*[1], *SHI Yun qing*[2], *ZHENG Yi zhan*[1], *ZHENG Jun xiang*[1], *LIU Lian sheng*[3], *BAI Wei chao*[3]

(1. Department of Computer Science and Engineering, Tongji University, Shanghai 200092, China
2. Department of ECE, New Jersey Institute of Technology, Newark, NJ, USA
3. Baojia Electronic Equipments, Co. Ltd, Shenzhen 518000, China)

Abstract: This paper presents two reversible data hiding methods based on integer wavelet, namely spread—spectrum method and companding method. Both methods embed data in wavelet high—frequency subband coefficients so as to achieve superior performance in terms of data embedding capacity and visual quality of marked images. To prevent the overflow and underflow problem, histogram modification is used. Experimental results show that both methods are in the best in the literature.

Key words: reversible data hiding; integer wavelet; histogram modification; spread spectrum; companding;