

基于 IWT 的自适应迭代混合图像隐藏算法*

刘培培¹, 王宏霞²

(1. 成都理工大学 信息科学与技术学院, 成都 610059; 2. 西南交通大学 信息科学与技术学院, 成都 610031)

摘要: 从提高图像变换域信息隐藏算法的隐藏容量角度出发, 将迭代混合的思想扩展应用到整数小波变换域, 实现了一种新的自适应迭代混合图像隐藏算法。该算法采用整数小波变换, 克服了传统小波变换域图像隐藏算法存在的边界误差和舍入误差问题, 同时充分考虑人眼视觉特性, 有效协调了不可见性和鲁棒性之间的矛盾。实验结果表明算法隐藏容量大, 同时具有好的不可见性和鲁棒性。

关键词: 信息隐藏; 整数小波变换; 视觉模型; 迭代混合

中图分类号: TP391.41 **文献标志码:** A **文章编号:** 1001-3695(2012)04-1449-03

doi:10.3969/j.issn.1001-3695.2012.04.069

Adaptive iterative blending information hiding algorithm based on integer wavelet transform

LIU Pei-pei¹, WANG Hong-xia²

(1. College of Information Science & Technology, Chengdu University of Technology, Chengdu 610059, China; 2. School of Information Science & Technology, Southwest Jiaotong University, Chengdu 610031, China)

Abstract: In order to increase the capacity of image transform domain information hiding algorithm, this paper applied the idea of iterative blending to integer wavelet domain and presented a novel self-adaptive image information hiding algorithm. The employment of integer wavelet overcame the boundary difference and rounding difference that existed in traditional image information hiding algorithms. Simultaneously, the HVS model was sufficiently used to adjust the imperceptibility and robustness. Experimental results show that the proposed algorithm has a large capacity, good imperceptibility and strong robustness.

Key words: information hiding; integer wavelet transform(IWT); visual model; iterative blending

鲁棒性、不可感知性、隐藏容量是信息隐藏技术的三个主要性能指标^[1], 其中, 隐蔽性和隐藏容量是互相矛盾的, 大的隐藏容量将引进更多改变到载体图像, 使秘密信息容易被感知。信息隐藏技术按照作用域的不同, 可以分为空域和变换域算法, 相对于空域算法来说, 变换域算法具有鲁棒性强、与图像压缩标准兼容等优点, 但通常隐藏容量较小。因此, 如何在变换域实现隐蔽性好的大容量信息隐藏, 是值得深入研究的课题。

1 整数小波变换及视觉模型

1.1 载体图像的整数小波变换及子带选取

由于小波变换良好的时频局部化特性和多分辨率特性, 在图像压缩等领域占有重要的地位。传统的小波函数结构依赖于 Fourier 变换, 由于浮点数的出现, 量化误差导致这类变换不能精确地恢复原始信号^[2]。对图像而言, 所有的像素数据都是整数, 此时相应的无损变换指的是对于整型的图像数据经过正变换, 再经过反变换, 最后取整, 其数值保持不变。而通常的小波基都是浮点数, 直接利用它来进行变换需要克服边界误差和精度误差两个障碍。在提升格式下建立的整数小波被称为第二代小波, 可以实现图像的整数到整数的变换, 而且图像的恢复质量与变换时边界采用何种延拓方式无关, 完全可以克服由第一代小波变换所带来的缺陷^[3-6]。因此, 本文算法通过对载体图像进行整数小波变换实现秘密信息的嵌入。

对载体图像进行 L 级整数小波分解, 分解后得到各小波子

带记为 I_l^θ ($\theta=0,1,2,3; l=0,1,\dots,L-1$)。图 1 所示为图像的四级整数小波分解示意, 即 $L=4$ 。

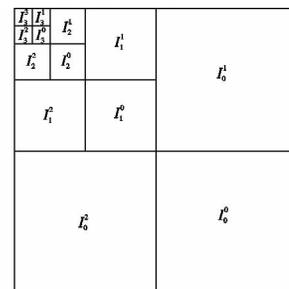


图1 图像四级整数小波分解示意图

Cox 等人^[7]指出, 为提高算法的鲁棒性, 嵌入载体的信息应放在视觉最重要的分量上, 对应于小波变换域的低频子带。因此, 本文算法将秘密图像信息隐藏在整数小波变换的低频子带上。另一方面, 由于图像的大部分能量都集中在低频带上, 通过修改低频系数实现秘密信息嵌入, 容易使载密图像视觉质量下降。本文算法利用小波域视觉模型计算低频子带系数的恰可见差异(just notice difference, JND)值, 并依此确定嵌入秘密信息的位置和强度, 保证秘密信息的不可见性。

1.2 图像小波域视觉模型及恰可见差异的计算

在图像压缩领域的研究工作中, Lewis 等人^[8]根据人眼视觉系统特点, 建立了离散小波域人眼视觉模型。Barni 等人^[9]对该模型进行了改进, 指出人眼的视觉掩蔽特性主要包括频率

收稿日期: 2011-08-13; 修回日期: 2011-09-25 基金项目: 国家自然科学基金资助项目(61170226)

作者简介: 刘培培(1978-), 女(满族), 讲师, 博士, 主要研究方向为信息隐藏、通信系统仿真(xpiy@163.com); 王宏霞(1973-), 女, 教授, 主要研究方向为数字水印技术、保密通信。

掩蔽、亮度掩蔽和对比度掩蔽三方面的特点。频率掩蔽特性是指人眼对高频子带噪声不敏感,尤其对对角线方向的高频子带噪声不敏感。亮度掩蔽特性是指人眼对图像不同亮度背景的噪声敏感程度不同,对很亮或很暗区域的噪声不敏感。而对对比度掩蔽特性是指人眼对平滑区域的噪声敏感,对纹理复杂区域的噪声不敏感。综合以上的特点,文献[9]给出了小波域的视觉模型。

对原始图像进行四级小波分解,此时各小波子带系数的恰可见差异 JND 阈值为

$$T_l^{\theta}(i, j) = \theta(l, \theta) \cdot A(l, i, j) \cdot \Xi(l, i, j)^{0.2} / 2 \quad (1)$$

其中: l 表示小波分解的层次; $\theta \in \{0, 1, 2, 3\}$ 表示子带的方向; i, j 表示小波系数的位置,具体如文献[9]所述。

将视觉模型应用于信息隐藏时,往往需要计算不同分解级的低频子带系数 I_l^{θ} 的 JND 值,根据小波域相邻子带的相关性^[10],利用相同分解级的两个相邻子带 I_l^{θ} 和 I_l^{θ} 内对应位置系数的 JND 值 $T_l^{\theta}(i, j)$ 和 $T_l^{\theta}(i, j)$ 来预测 I_l^{θ} 内各系数的 JND 值 $T_l^{\theta}(i, j)$,如式(2)所示。

$$T_l^{\theta}(i, j) = (T_l^{\theta}(i, j) + T_l^{\theta}(i, j)) / 2 \quad (2)$$

2 自适应迭代混合图像隐藏算法

2.1 空域迭代混合算法原理

文献[11]提出了基于迭代混合的数字图像隐藏算法,该算法为在图像中隐藏秘密信息提供了一种新的思路。其主要思想可描述如下:数字图像可以表示为连续函数在离散网格点处的函数值 $F(i, j)$,若其中 $i \in \{1, 2, \dots, M\}, j \in \{1, 2, \dots, N\}$,那么,这就是一个尺寸为 $M \times N$ 的图像。

定义 1 设 F 与 G 分别表示尺寸为 $M \times N$ 的数字图像, $\{\alpha_i | 0 \leq \alpha_i \leq 1, i = 1, 2, \dots, n\}$ 为给定的 n 个实数,对数字图像 F 和 G 进行 α_1 混合得 $S_1 = \alpha_1 F + (1 - \alpha_1) G$,将数字图像 F 和 S_1 进行 α_2 混合得到 $S_2 = \alpha_2 F + (1 - \alpha_2) S_1$,依次进行混合得 $S_n = \alpha_n F + (1 - \alpha_n) S_{n-1}$,则数字图像 S_n 称为图像 F 和 G 的关于 α_i 的 n 重迭代混合^[11]。将图像 F 作为载体图像, G 作为秘密图像,那么图像 S_n 即是载密图像。

2.2 秘密信息的嵌入和提取过程

设载体图像 F 是大小为 $M_1 \times N_1$ 的 256 级灰度图像,秘密图像 G 是大小为 $M_2 \times N_2$ 的 256 级灰度图像,其中 $M_2 \leq M_1 / 2, N_2 \leq N_1 / 2$ 。

2.2.1 秘密信息预处理

为了提高算法的安全性,在嵌入信息前利用 Logistic 混沌映射对秘密图像进行置乱操作。具体过程如下:

a) 将密钥 K 作为混沌初值,进行混沌迭代,产生长度为 $M_2 \times N_2$ 的混沌序列 $\{x_k | k = 1, 2, \dots, M_2 \times N_2\}$ 。

b) 按照从大到小的顺序对序列 $\{x_k | k = 1, 2, \dots, M_2 \times N_2\}$ 进行排序,得到序列 $\{x_{a_k} | k = 1, 2, \dots, M_2 \times N_2\}$,其中, a_k 表示 $\{x_{a_k}\}$ 中的元素 x_{a_k} 在序列 $\{x_k\}$ 中的位置。由此得到位置序列 $\{a_k | k = 1, 2, \dots, M_2 \times N_2\}$ 。

c) 根据序列 $\{a_k | k = 1, 2, \dots, M_2 \times N_2\}$ 计算得到序列 $\{i_k | k = 1, 2, \dots, M_2 \times N_2\}$ 和 $\{j_k | k = 1, 2, \dots, M_2 \times N_2\}$ 。具体方法为

$$\begin{cases} i_k = \lfloor (a_k - 1) / N_2 \rfloor + 1 \\ j_k = a_k - i_k \cdot N_2 \end{cases} \quad (3)$$

d) 将秘密图像 G 中的像素依次以 (i_k, j_k) 为坐标重新排列,从而得到置乱后的秘密图像 G' 。

2.2.2 秘密信息的嵌入

a) 根据原始载体图像 F 和置乱后的秘密图像 G' 的大小关

系,确定小波分解的层数 $L, L \in \{1, 2, 3, 4\}$ 。然后对载体图像进行 L 级整数小波分解,得到各小波子带 $I_l^{\theta} (\theta = 0, 1, 2, 3; l = 0, 1, \dots, L - 1)$ 。提取低频子带 I_{L-1}^{θ} 用于嵌入秘密信息,分解层数 L 的确定方法为

$$L = \min \left(\lfloor \log_2 \left(\frac{\min(M_1, N_1)}{\max(M_2, N_2)} \right) \rfloor, 4 \right) \quad (4)$$

b) 对原始载体图像 F 进行四级整数小波分解,根据式(1)和(2)计算得到低频子带 I_{L-1}^{θ} 各小波系数的 JND 值,记为 T_{L-1}^{θ} 。

c) 选取 I_{L-1}^{θ} 中对应 JND 值较大的前 $M_2 \times N_2$ 个系数,按这些系数的 JND 值从大到小的顺序将它们组成 M_2 行 N_2 列的系数矩阵 P 用于嵌入秘密信息, P 中各系数 $P(i, j)$ 对应的 JND 值记为 $J(i, j)$ 。

d) 通过自适应迭代混合方式将秘密图像 G' 隐藏在 P 中,得到携带秘密图像信息的矩阵 S 。具体迭代混合过程表示如下:

```

input P, G', S = G'
get a blending parameter  $\alpha, 0 < \alpha < 1$ 
S =  $\alpha P + (1 - \alpha) S$ ;
E = |P - S|;
n = 1;
while E(i, j) > J(i, j)
S =  $\alpha P + (1 - \alpha) S$ ;
E = |P - S|;
n = n + 1;
end
output S
    
```

迭代参数 α 和迭代次数 n 作为提取秘密信息时密钥的一部分。

e) 将 S 中携带秘密信息的系数依次放回到 I_{L-1}^{θ} 中的相应位置,得到 $I_{L-1}^{\theta'}$;联合其他未作修改的整数小波子带进行 L 级逆整数小波变换,得到嵌入秘密信息的载密图像 F' 。

2.2.3 秘密信息的提取和恢复

秘密信息的提取和恢复是嵌入过程的逆过程。提取秘密信息时已知混沌初值 K 、迭代参数 α 和迭代次数 n 。提取秘密信息的具体步骤如下:

a) 对原始图像 F 和图像 F' 进行 L 级整数小波分解,分别得到低频子带 I_{L-1}^{θ} 和 $I_{L-1}^{\theta'}$ 。

b) 按照式(1)和(2),计算小波低频子带 I_{L-1}^{θ} 中各系数的 JND 值,得到 T_{L-1}^{θ} 。

c) 将 T_{L-1}^{θ} 中的各 JND 值进行排序,确定较大的 $M_2 \times N_2$ 个 JND 值的位置,并将 I_{L-1}^{θ} 和 $I_{L-1}^{\theta'}$ 中相应位置的系数取出,按各系数对应 JND 值的大小顺序分别组成矩阵 P 和 S ,用于提取秘密信息。

d) 根据获得的迭代参数 α 和迭代次数 n ,利用式(5)恢复秘密信息:

$$G' = \frac{S - \alpha P}{1 - \alpha} \quad (5)$$

具体过程用伪码表示为

```

input P, S
G' = S;
for k = 1: n
G' = (G' -  $\alpha P$ ) / (1 -  $\alpha$ );
end
    
```

e) 最后根据密钥 K 将秘密信息 G' 进行逆置乱,得到秘密图像 G 。

3 仿真结果和讨论

为了验证算法的有效性,利用 MATLAB 7.0 对本算法进行了仿真。将 512×512 大小的 256 级经典灰度图像 Lena、Cam-

eraman、Barbara、Peppers、Milk、Baboon 和 Man 等作为测试用载体图像^[12]。秘密图像为 160 × 160 大小的 256 级灰度图像 Village。此时计算得到 $L=1$, 因此将秘密信息嵌入在原始载体图像一级整数小波分解的低频子带 I_0^3 中。其中, 迭代混合因子 $\alpha=0.616$ 。用峰值信噪比 PSNR 来评价嵌入信息前后图像的差别。

图 2(a) 所示为 Lena 图像的一级整数小波分解结果, (b) 显示了小波子带中各系数对应的 JND 值。本文算法将秘密信息嵌入在低频小波子带 I_0^3 中。图 3 显示了置乱前后的秘密图像 Village。显而易见, 基于混沌序列的图像置乱能够有效消除图像像素的空间相关性, 从而提高算法的安全性。图 4 显示了以 Lena、Milk 和 Baboon 为载体隐藏置乱后的秘密图像 Village 的结果。从图 4 中可以看出, 本文算法充分利用了小波域人眼视觉模型, 秘密信息自适应隐藏在图像的边缘、纹理区域, 算法不可见性好。对算法的鲁棒性进行测试。图 5 显示了在对载体图像进行各种攻击之后提取的秘密图像信息。从图中可以看出, 本文算法对 JPEG 压缩、添加噪声、亮度增强和剪切等攻击具有较好的鲁棒性。

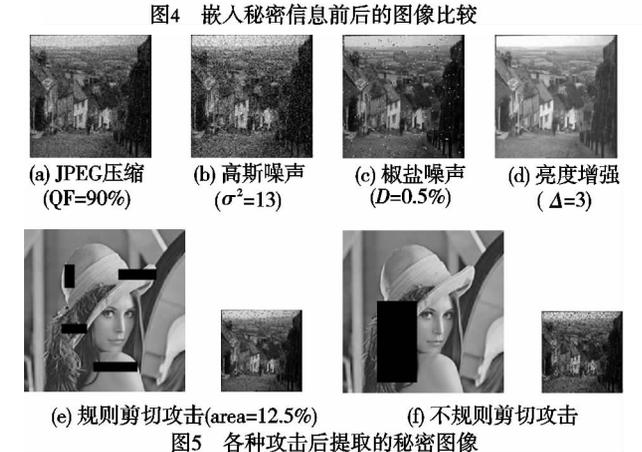
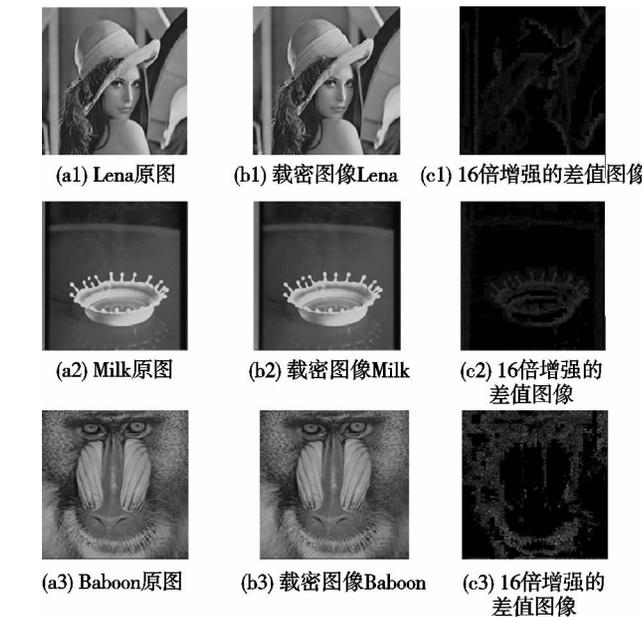


表 1 列出了在不同载体图像中嵌入置乱后 Village 图像的实验结果。从表中数据可以看出, 隐藏 160 × 160 大小的 256 级灰度图像 Village 在各载体图像中, 不同载体图像需要不同的迭代次数完成。这是因为算法利用人眼视觉掩蔽特性, 通过自适应迭代实现秘密信息在低频子带嵌入的缘故。Milk 图像含有大量的平滑区域, 纹理最简单, 对图像的修改易察觉, 所以需要最多次数的迭代才能获得理想的隐藏效果。与之相反, 由于 Baboon 图像纹理最复杂, 对图像的修改不易被察觉, 只需 3 次迭代即可获得满意的隐藏效果。

表 1 不同载体图像的性能比较

载体图像	PSNR/dB	迭代次数 n	隐藏比特/bit
Lena	45.708	4	204 800
Cameraman	52.889	5	204 800
Barbara	46.277	4	204 800
Peppers	45.599	4	204 800
Milk	60.023	6	204 800
Baboon	39.083	3	204 800
Man	45.391	4	204 800

4 结束语

本文将源于图像融合领域的迭代混合思想扩展到图像变换域, 结合整数小波变换和人类视觉特性, 提出了一种新的自适应迭代混合图像隐藏算法。算法具有以下特点: a) 采用整数小波变换, 克服了传统小波域隐写算法存在的边界误差和舍入误差问题, 避免了图像迭代混合算法因边界误差和舍入误差累积放大而产生的弱鲁棒性; b) 利用视觉模型确定秘密信息在小波低频子带的嵌入位置和嵌入强度, 获得了不可见性和鲁棒性的理想折中; c) 实现了变换域的大容量信息隐藏; d) 算法原理清晰, 实现简单。

参考文献:

- [1] FRIDRICH J. Application of data hiding in digital image [C]//Proc of the 5th ISSPA'99. 1999.
- [2] 唐晓初. 小波分析及其应用 [M]. 重庆: 重庆大学出版社, 2006.
- [3] SWELDENS W. The lifting scheme: a construction of second generation wavelets [R]. [S. l.]: University of South Carolina, 1995.
- [4] SWELDENS W. The lifting scheme: a construction of second generation wavelets [J]. SIAM Journal on Mathematical Analysis, 1997, 29(2): 511-546.
- [5] DAUBECHIES I, SWELDENS W. Factoring wavelet transforms into lifting steps [J]. Journal of Fourier Analysis and Application, 1998, 4(3): 245-267.
- [6] CALDERBANK A, DAUBECHIES I, SWELDENS W, et al. Wavelet transforms that map integers to integers [J]. Applied and Computational Harmonic Analysis, 1998, 5: 332-369.
- [7] COX I J, KILIAN J, LEIGHTON N, et al. Secure spread spectrum watermarking for multimedia [J]. IEEE Trans on Image Processing, 1997, 6(12): 1673-1687.
- [8] LEWIS S, KNOWLES G. Image compression using 2-D wavelet transform [J]. IEEE Trans on Image Processing, 1992, 1(2): 244-250.
- [9] BARNI M, BARTOLINI F, PIVA A. Improved wavelet-based watermarking through pixel-wise masking [J]. IEEE Trans on Image Processing, 2001, 10(5): 783-791.
- [10] 王向阳, 杨红颖, 陈利科, 等. 基于视觉掩蔽的半脆弱水印技术研究 [J]. 中国图象图形学报, 2005, 10(12): 1548-1553.
- [11] 张贵仓, 王让定, 章毓晋. 基于迭代混合的数字图像隐藏技术 [J]. 计算机学报, 2003, 26(5): 569-574.
- [12] 钱思进, 张恒, 何德全. 基于图像视觉复杂度计算的分类信息隐藏图像库 [J]. 解放军理工大学学报, 2010, 11(1): 26-30.