基于分块离散小波变换的图像信息隐藏与盲提取算法*

甘甜 冯少彤 聂守平† 朱竹青

(南京师范大学江苏省光电技术重点实验室, 南京 210097)

(2011 年 7 月 3 日收到; 2011 年 12 月 15 日收到修改稿)

提出了一种在小波域中图像信息隐藏与盲提取算法. 该算法首先对载体图像进行分块两层离散小波变换, 找到每块第二级分解子带中的最大值即最重要小波系数, 然后根据小波特征树的对应关系将其在第一级分解子带中的对应区域作为嵌入区域, 在该区域嵌入由秘密信息生成的伪随机序列. 提取过程中, 同样按照小波系数对应关系寻找到嵌入区域并判断其与伪随机序列的相关性即可解密, 不需要提供原始图像. 实验结果表明, 该算法能实现二值图像的嵌入与盲提取, 且提取出的图像质量较好并具备一定的抗攻击能力, 尤其对于剪切攻击的鲁棒性较好.

关键词: 图像隐藏, 盲提取, 离散小波变换

PACS: 42.30.Va, 42.30.Wb

1 引 言

信息隐藏通常是将秘密对象隐藏在载体的冗余信息中, 以实现其不可感知性和安全性, 保护秘密信息不被未授权的第三方破解. 目前信息隐藏领域主要有空间域算法和变换域算法两大类算法. 变换域算法多数利用了离散傅里叶变换、离散余弦变换和小波变换等 [1−3], 与空间域算法相比, 变换域算法鲁棒性更好、容量更大.

小波变换由于其时频特性及多尺度、多分辨率特性, 近年来得到了更普遍的应用 [4,5]. 但是部分基于小波变换的算法在提取信息的过程中都需要原载体图像, 大大降低了通信的效率, 因此小波域盲提取算法近年来也是研究的一个热点 [6,7]. 文献 [8] 提出了通过对小波特征树量化的方法来嵌入秘密信息, 量化前后小波树之间的统计差值用于信息盲提取. 该算法实现了盲提取的目的, 但是在嵌入与提取过程中误差计算的不一致会影响所提取出的图像效果 [9]. 文献 [10] 中对载体图像分解后的小波系数进行了不重叠地分块, 每一块区域中两个最大小波系数的差值通过与平均差值的比较进行修改, 从而实现信息隐藏的目的. 提取过程中自适应地选择阈值, 这样可以提高其一定的抗攻击性但抗噪声能力较差 [9].

本文提出了基于分块离散小波变换 (DWT) 的图像信息隐藏盲提取算法, 实现了二值图像的有效隐藏和提取. 利用小波变换特征树的对应关系, 提取过程中不需要提供原始图像. 本算法由于对载体图像采用分块 DWT, 因此秘密信息嵌入到相对广泛的频率子带中, 空间上也分布在载体图像的大部分区域, 所以对于剪切攻击的鲁棒性较好. 实验结果表明, 利用本文算法提取出的秘密图像质量较好, 并具有一定的抗攻击性.

2 隐藏信息的预处理

为了提高秘密信息的安全性, 首先对秘密信息进行置乱. 置乱处理既可以消除原秘密图像像素间的相关性, 增强其抗剪切能力; 同时使图像变得杂乱无章, 如果置乱类型未给明, 则无法恢复源图像.

* 江苏省高等学校自然科学基金 (批准号: 09KJA140002) 和江苏省自然科学基金 (批准号: BK2009400) 资助的课题.

† E-mail: njnukjc_nie@163.com

© 2012 中国物理学会 Chinese Physical Society

本文算法采用 Arnold 变换对秘密图像进行置乱.

对于像素数为 $N \times N$ 的图像, 其 Arnold 坐标变换为

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}N). \quad (1)$$

将 Arnold 变换次数作为提取信息时的密钥 K_1.

同时, 本文的方法并不是直接将置乱后的二值图像嵌入到载体图像中, 而是根据二值图像的信息生成伪随机序列进行嵌入. 这样伪随机序列相当于需要嵌入的水印, 提取时根据已知的伪随机序列可以实现盲提取的目的. 如果伪随机数发生方式未给明, 同样无法提取秘密信息, 这会使原秘密信息的不可感知性更强. 为了保证载体图像在视觉上不受影响, 本文中生成两个绝对值范围在 (0, 1) 的伪随机序列 S_{p0} 和 S_{p1}, 同时将它们作为提取信息时的密钥 K_2. 伪随机序列是由确定的算法产生, 给定算法的种子及随机数的范围可以产生一串伪随机数. 本文采用了线性拟合伪随机数发生器产生伪随机序列 S_{p0} 和小数开方伪随机数发生器产生伪随机序列 S_{p1}, 保证两个伪随机序列互不相关.

伪随机序列 S_{p0} 由线性拟合伪随机数发生器产生, 按下列迭代方程获得:

$$X_{n+1} = (aX_n + c)(\mathrm{mod}m), \quad (2)$$

其中 $m > 0, 0 < a < m, 0 \leqslant c < m$. 本文生成伪随机序列 $S_{\mathrm{p0}} = \{0.53426, 0.53712, 0.32579, 0.77975\}$.

伪随机序列 S_{p1} 由小数开方伪随机数发生器产生, 按下列迭代方程获得:

$$X_{n+1} = 10^m \sqrt{X_n - a}. \quad (3)$$

本文生成伪随机序列 $S_{\mathrm{p1}} = \{-0.83162, -0.1548, -0.96595, -0.65187\}$.

3 小波域信息隐藏盲提取算法

DWT 可以对图像进行多分辨率分析和时频分解. 图像经过一层 DWT 后分解成四部分, 即低频部分和三个方向的高频部分, 低频部分显示图像的近似子图 LL_1, 三个高频部分分别显示图像的水平方向细节子图 HL_1、垂直方向细节子图 LH_1 和对角线方向细节子图 HH_1. 在下一层分解中, 低频部分 LL_1 进一步被分解成四个部分, 依此类推, 对图像进行更深层小波变换. 图像两层 DWT 的分解如图 1 所示.

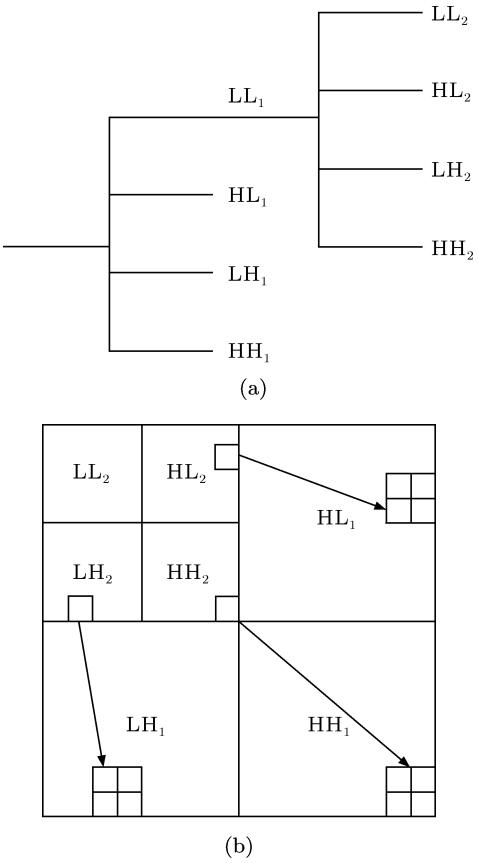

图 1 两层 DWT 分解示意图 (a) 分解过程; (b) 对应于 (a) 图的频率子带

对于各级 HL, LH, HH 子带系数, 均在空间、方向上有强烈的相似性, 这种系数跨带之间的关系可以用 "零树" 结构来表示, 图 1(b) 所示即为两层 DWT 所形成的树. 根据跨带系数间的对应关系可知, HL_2, LH_2, HH_2 中的一个像素分别对应 HL_1, LH_1, HH_1 中的四个像素.

由于 DWT 是可逆的, 根据上述的分解过程可知, 经小波逆变换后得到的图像再经小波变换所生成的小波系数与原小波系数是一致的. 根据上述原理, 本文算法的核心是利用小波变换特征树的对应关系并结合秘密信息的特征, 在高频部分选择符合一定条件的区域嵌入伪随机序列. 在高频部分中, 小波系数越大表示原图像中的细节越明显, 为了保证载体图像在视觉上不受影响, 因此选用最大小波系数所对应的区域进行嵌入.

设载体图像像素数为 512×512, 将其以像素数为 16×16 的区域分成 32×32 块. 以第 K 个子块垂直方向的频率子带为例, 其第二级小波变换系数

集为

$$K_{\mathrm{LH2}} = \{K_{\mathrm{LH2}}(1,1), K_{\mathrm{LH2}}(1,2), K_{\mathrm{LH2}}(2,1), K_{\mathrm{LH2}}(2,2)\}. \quad (4)$$

找到系数集 K_{LH2} 中的最大小波系数并记下其位置坐标 (i,j). 设最大系数为 $K_{\mathrm{LH2}}(i,j)$, 则其对应于第一级小波变换系数集 K_{LH1} 中的四个系数为 $K_{\mathrm{LH1}}(2i-1,2j-1)$, $K_{\mathrm{LH1}}(2i-1,2j)$, $K_{\mathrm{LH1}}(2i,2j-1)$, $K_{\mathrm{LH1}}(2i,2j)$, 记为系数集 $K_{\mathrm{LH1\,max}}$.

本文中秘密图像是像素数为 32×32 的二值图像. 本文提出的算法实际上是结合秘密信息将伪随机序列作为水印进行嵌入. 由 (4) 式可知, 载体图像中第 K 个子块垂直方向频率子带的嵌入区域为 $K_{\mathrm{LH1\,max}}$, 这个区域中含有 4 个小波系数, 因此本文中生成的两个伪随机序列均包含 4 个伪随机数. 当秘密信息为 0 时, 则在 $K_{\mathrm{LH1\,max}}$ 中嵌入伪随机序列 S_{p0}; 当秘密信息为 1 时, 则在 $K_{\mathrm{LH1\,max}}$ 中嵌入伪随机序列 S_{p1}. 考虑嵌入信息的鲁棒性和载密图像的视觉效果选用适当的嵌入因子 α, 嵌入方式可表示为

$$\begin{aligned} K_{\mathrm{LH1\,max}} &= \frac{K_{\mathrm{LH1\,max}}}{\alpha} + \alpha S_{\mathrm{p0}}, \\ K_{\mathrm{LH1\,max}} &= \frac{K_{\mathrm{LH1\,max}}}{\alpha} + \alpha S_{\mathrm{p1}}. \end{aligned} \quad (5)$$

最后经嵌入的小波系数经逆离散小波变换 (IDWT) 得到载密图像.

图 2 所示为本文算法的信息隐藏流程. Arnold 置乱的迭代次数作为密钥 K_1, 伪随机序列 S_{p0} 和 S_{p1} 作为密钥 K_2.

图 3 所示为本文算法的信息提取流程. 由上述原理可知, 载密图像经 DWT 后的二级分解系数与原载体图像的二级小波系数是一致的, 故可以不依赖原载体图像即可找到秘密图像的隐藏区域, 然后判断该区域与伪随机序列 S_{p0} 的相关系数 ρ_0 和与伪随机序列 S_{p1} 的相关系数 ρ_1 从而提取出信息, 最后经 Arnold 逆变换 (密钥 K_1) 即得到秘密图像.

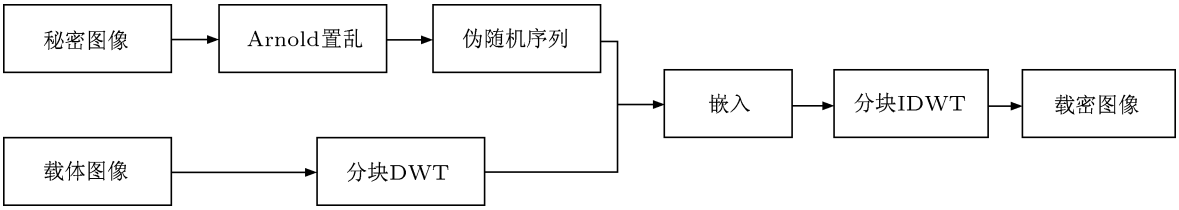

图 2 信息隐藏流程图

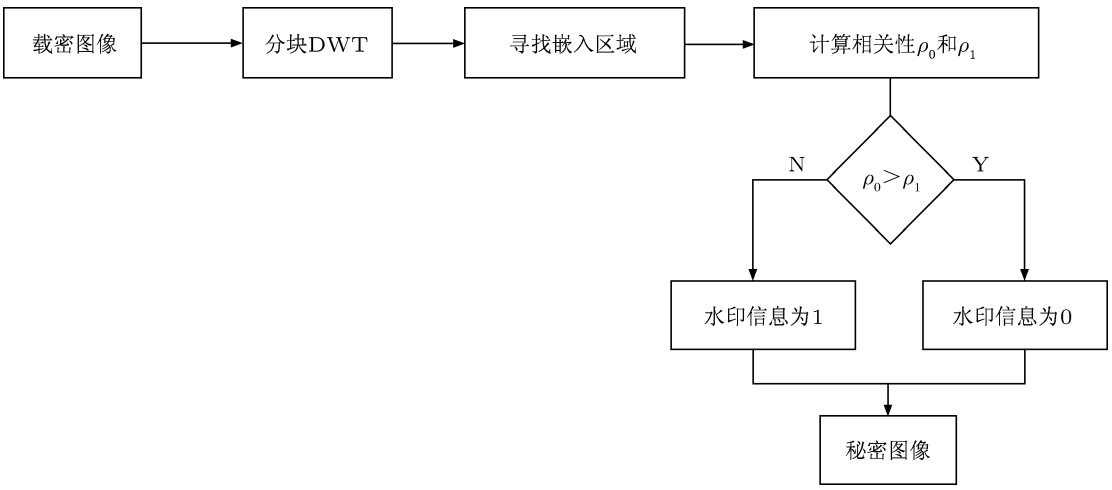

图 3 信息提取流程图

为了保证秘密信息的完整性和安全性, 本文利用小波变换多分辨率的特性, 同时在小波变换的三个高频部分按上述方法进行嵌入. 由于秘密图像是二值图像, 在提取过程中对各高频部分所提取出的信息进行比较判断, 出现概率大的视为水印信息. 以第 K 个子块为例, 其三个高频部分分别提取出的秘密图像的像素值为 $W_{\mathrm{HL}}(k)$, $W_{\mathrm{LH}}(k)$, $W_{\mathrm{HH}}(k)$. 然后计算 0 和 1 分别出现的概率 P_0 和 P_1, 若 $P_0 > P_1$, 则 $W(k) = 0$; 反之 $W(k) = 1$.

在三个高频部分都嵌入秘密信息可以避免只利用一个高频部分所提取出信息的误差, 提高盲提取重构的秘密图像效果并增强其抗攻击能力.

4 实验结果

本文采用峰值信噪比 R 对算法进行度量, 对于灰度等级为 256 的灰度图像, 其峰值信噪比定义为

$$R = 10\lg\frac{255^2}{\dfrac{1}{MN}\displaystyle\sum_{i=1}^{M}\sum_{j=1}^{N}(f(i,j)-f_0(i,j))^2}, \quad (6)$$

其中 $M \times N$ 为图像的像素数, f_0 为原始图像, f 为处理后的图像.

实验中, 本文选取如图 4 所示的房屋图像作为载体图像, 其像素数为 512×512. 秘密图像是一幅如图 5 所示的二值图像, 其像素数为 32×32.

图 4 载体图像

图 5 秘密图像

首先, 对秘密图像进行 q 次 Arnold 置乱, 并将置乱次数 q 作为提取信息时的密钥 K_1. 随后采用线性拟合伪随机数发生器产生伪随机序列 S_{p0} 和小数开方伪随机数发生器产生伪随机序列 S_{p1}, 并将二者作为提取信息时的密钥 K_2. 按照上述方法, 将载体图像以像素数为 16×16 的区域分成 32×32 块并找到相应嵌入区域依 (5) 式进行嵌入.

图 6 所示为载密图像, 其与原载体图像的峰值信噪比 $R = 39.4099$ dB. 图 7 所示为盲提取重构的秘密图像, 其与原秘密图像的峰值信噪比 $R = 71.2441$ dB, 归一化互相关系数为 0.98729.

图 6 载密图像

图 7 重构的秘密图像

实验中另外还采用了如图 8 所示的 4 幅载体图像, 其中图 A 是丘陵图像, 图 B 是青椒图像, 图 C 是雪梨图像, 图 D 是女士图像. 这 4 幅载体图像的像素数均为 512×512.

图 9 所示为 4 幅载密图像分别与相应的载体图像的峰值信噪比. 表 1 所列为从 4 幅载密图像重构的秘密图像与原秘密图像的峰值信噪比及归一化互相关系数. 实验结果表明, 本文提出的算法能够实现二值图像的盲提取且重构的秘密图像质量较好, 同时不影响载体图像的视觉效果.

此外, 本文算法还可用于视频图像隐藏领域. 实验中选用一个含 55 帧图像的电路板视频文件, 选取其第 12、第 30、第 45 帧图像分别嵌入一幅二值图像, 图 10 所示为三帧图像及其重构的秘密图像.

图 8 另外选用的 4 幅载体图像 (a) 图 A; (b) 图 B; (c) 图 C; (d) 图 D

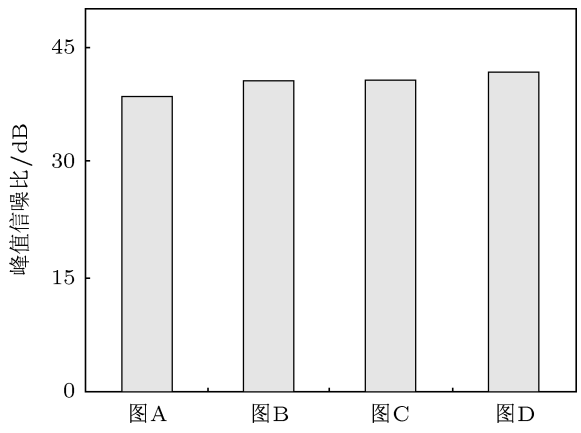

图 9 4 幅载密图像与原载体图像的峰值信噪比

图 11 所示为原视频文件与载密视频文件的峰值信噪比曲线. 从图 11 可以看出, 载密前后视频的峰值信噪比曲线并没有很明显的不同, 说明嵌入秘密信息后不影响视频文件的整体视觉效果.

进一步, 本文对所提出的算法的鲁棒性展开了研究. 采用 4 种典型的攻击方式对图 6 所示的载密图像进行攻击处理. 方式 I 是剪切载密图像的 1/16, 方式 II 是添加强度为 0.005 的椒盐噪声, 方式III是采用像素为 3 × 3 的模板和方差为 0.5 的高斯低通滤波器进行低通滤波, 方式IV是品质因子为 95 的标准图像压缩. 在上述四种攻击方式下重构的秘密图像与原秘密图像的峰值信噪比如表 2 所列.

表 1 重构的秘密图像与原秘密图像的峰值信噪比及归一化互相关系数

载体图像	图 A	图 B	图 C	图 D
峰值信噪比 /dB	78.2338	75.2235	78.2338	∞
归一化互相关系数	0.99746	0.99492	0.99747	1.00000

由于本文算法的基础是利用小波跨带系数间的关系, 比较依赖小波系数, 因此在抗噪声方面的鲁棒性一般. 正因为如此, 嵌入的信息无论在空间、方向上都分布在载体图像的大部分区域, 所以其抗剪切能力很强.

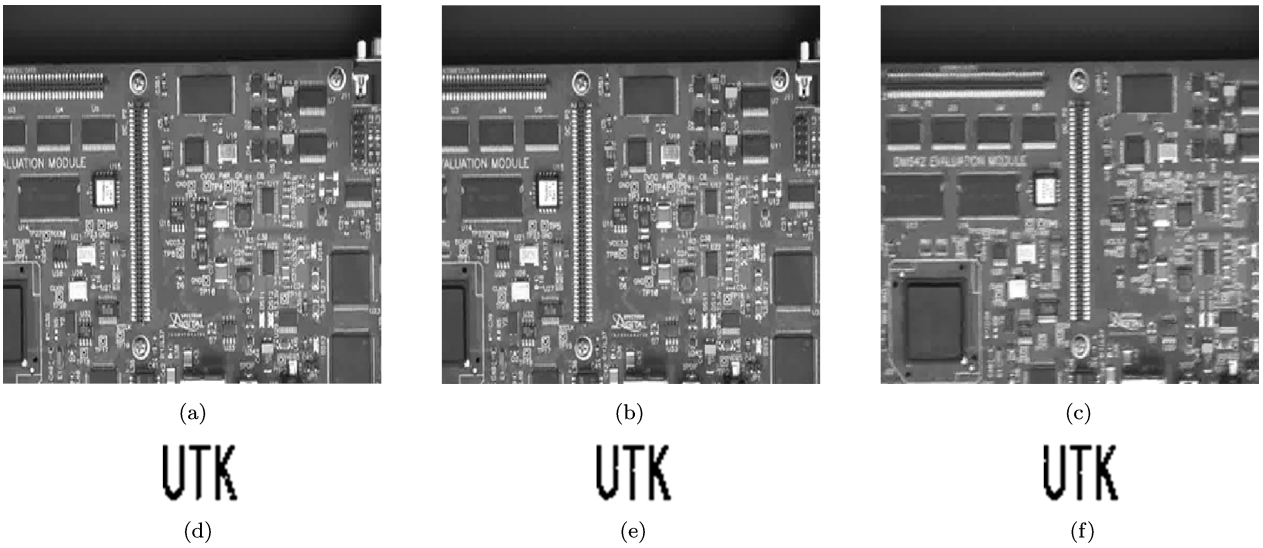

图 10 视频文件中的图像隐藏 (a) 第 12 帧图像; (b) 第 30 帧图像; (c) 第 45 帧图像; (d) 第 12 帧重构的秘密图像; (e) 第 30 帧重构的秘密图像; (f) 第 45 帧重构的秘密图像

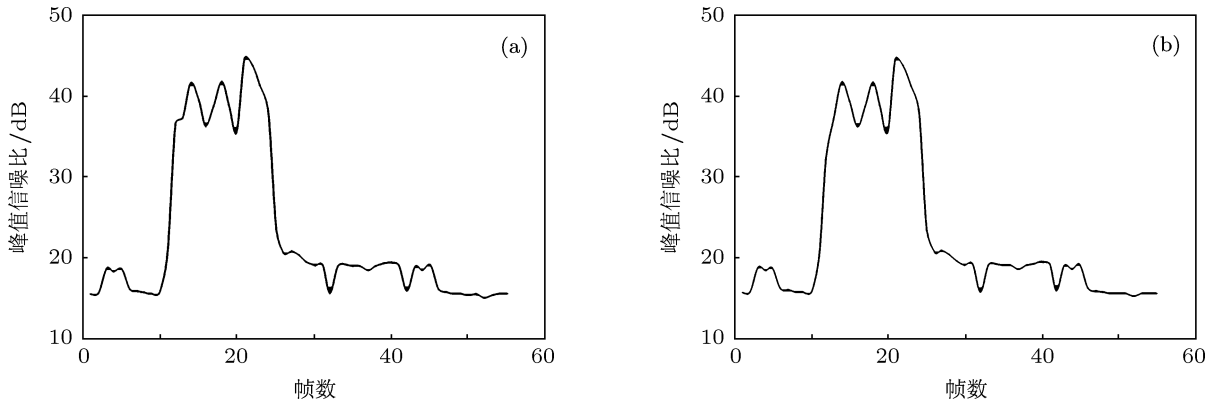

图 11 视频文件的峰值信噪比曲线 (a) 原视频文件的峰值信噪比曲线; (b) 载密视频文件的峰值信噪比曲线

图 12 剪切攻击后的载密图像及其重构的秘密图像 (a) 剪切 1/16 的载密图像; (b) 剪切 1/8 的载密图像; (c) 剪切 1/4 的载密图像; (d) 剪切 1/16 后重构的秘密图像; (e) 剪切 1/8 后重构的秘密图像; (f) 剪切 1/4 后重构的秘密图像

表 2 攻击处理后重构的秘密图像及其与原秘密图像的峰值信噪比

攻击方式	方式 Ⅰ	方式 Ⅱ	方式 Ⅲ	方式 Ⅳ
重构的秘密图像				
峰值信噪比/dB	69.7828	56.5312	57.8996	58.5959

实验中对抗剪切性能进行了更深入的研究, 得到不同剪切比例下重构的秘密图像如图 12 所示. 从图 12 可以明显看出, 当载密图像被剪切 1/4 后仍能盲提取出质量较好的秘密图像.

5 结 论

本文针对信息盲提取问题, 提出了一种在小波域实现图像信息隐藏与盲提取的算法. 该算法的核心是对载体图像进行分块两层 DWT, 找到第二级分解子带中的最大值即最重要的小波系数, 根据小波系数跨带间的关系在第一级分解子带中选择对应区域, 结合秘密图像的特征在该区域嵌入不同的伪随机序列. 提取过程不需要提供原始图像, 按照条件寻找到嵌入区域并判断其与伪随机序列的相关性即可解密. 实验结果表明, 本算法能实现二值图像的隐藏与盲提取, 且所提取出的图像质量较好并具备一定的抗攻击能力, 尤其对于剪切攻击的鲁棒性较好. 此外, 由于载密图像与原载体图像在视觉效果上相差无几, 因此本文提出的算法可用于视频图像隐藏领域.

[1] Zou L J, Wang B, Feng J C 2008 *Acta Phys. Sin.* **57** 2750 (in Chinese) [邹露娟, 汪波, 冯久超 2008 物理学报 **57** 2750]

[2] Zhong H, Jiao L C 2005 *Chin. J. Comput.* **28** 1549 (in Chinese) [钟桦, 焦李成 2005 计算机学报 **28** 1549]

[3] Fu M J , Zhuang J J, Hou F Z, Ning X B, Zhan Q B, Shao Y 2010 *Acta Phys. Sin.* **59** 4343 (in Chinese) [符懋敬, 庄建军, 侯凤贞, 宁新宝, 展庆波, 邵毅 2010 物理学报 **59** 4343]

[4] Bi N, Sun Q Y, Huang D, Yang Z H, Huang J W 2007 *IEEE Trans. Image Process.* **16** 1956

[5] Wei H L, Shi J H , Tzong W K, Ping Z F 2008 *IEEE Trans. Multimed.* **10** 746

[6] Siew C N, Raveendran P 2009 *IEEE Trans. Biomed. Eng.* **56** 2024

[7] Bao P, Xiao H M 2005 *IEEE Trans. Circuits Syst. Video Technol.* **15** 96

[8] Wang S H, Lin Y P 2004 *IEEE Trans. Image Process.* **13** 154

[9] You X G, Du L, Cheung Y M, Chen Q H 2010 *IEEE Trans. Image Process.* **19** 3271

[10] Lin W H, Horng S J 2008 *IEEE Trans. Multimed.* **10** 746

An image hiding and blind extraction algorithm based on block discrete wavelet transform*

Gan Tian Feng Shao-Tong Nie Shou-Ping† Zhu Zhu-Qing

(*Key Laboratory for Opto-electronic Technology of Jiangsu Province, Nanjing Normal University, Nanjing* 210097, *China*)

(Received 3 July 2011; revised manuscript received 15 December 2011)

Abstract

In this paper, we propose a blind watermarking algorithm based on block discrete wavelet transform. The watermark is scrambled by Arnold and two pseudo random sequences are generated first, and then according to the wavelet tree structure, the significant wavelet coefficients in a block are found and quantized by pseudo random sequence. During the extraction, the quantized coefficients can be found without the original image, then the correlation between them and the pseudo random sequences are calculated to estimate the watermark bits. Moreover, in this method all high-frequency subimages are used to provide better robustness. The performance of the proposed watermarking is robust to several attacks, especially quite effective against image cropping attack.

Keywords: image hiding, blind extraction, discrete wavelet transform

PACS: 42.30.Va, 42.30.Wb

* Project supported by the Natural Science Foudation of Institution of Higher Education of Jiangsu Province, China (Grant No. 09KJA140002) and the Natural Science Foudation of Jiangsu Province, China (Grant No. BK2009400).

† E-mail: njnukjc_nie@163.com