第 34 卷 第 15 期 计 算 机 工 程 2008 年 8 月
Vol.34 No.15 Computer Engineering August 2008
·安全技术· 文章编号：1000—3428(2008)15—0150—03 文献标识码：A 中图分类号：TP309

基于 SPIHT 的灰度图像部分加密方法

马洪军，林秋华
(大连理工大学电子与信息工程学院，大连 116024)

摘 要：图像数据量大、冗余度高，其实时加密问题亟待解决。图像部分加密方法只加密图像压缩编码的部分重要数据，是一种可行的实时加密方案。该文研究图像压缩编码的多级树集合分裂算法，分析灰度图像 SPIHT 中不同类型编码数据对图像重建的作用，确定了其中的重要数据，并将其用流密码进行了加密。仿真结果表明，该方法只加密图像编码的很少部分数据，便可达到图像保密的目的。
关键词：图像压缩；小波变换；多级树集合分裂算法；部分加密

Partial Encryption Method of Compressed Gray Images Based on SPIHT

MA Hong-jun, LIN Qiu-hua
(School of Electronic and Information Engineering, Dalian University of Technology, Dalian 116024)

【Abstract】 Due to big size and high redundancy, real-time image encryption is becoming a problem. Partial encryption of image encrypts only the important parts of the compressed image data, thus it is a feasible scheme for encrypting images in real time. This paper presents a partial encryption of gray images compressed by Set Partitioning In Hierarchical Trees(SPIHT). The significance of different types of SPIHT coded bits is analyzed, the most significant bits for reconstructing images are selected and then encrypted using a stream cipher. Computer simulations results demonstrate that the proposed method can achieve image security by encrypting only small parts of the SPIHT coded image.
【Key words】 image compression; wavelet transform; Set Partitioning In Hierarchical Trees(SPIHT); partial encryption

1 概述

图像加密方法是保障图像数据安全的重要手段。人们曾将二维图像数据转换为一维文本数据，然后采用成熟的文本加密方法(如 DES)[1]进行加密。随着图像压缩技术的发展，对压缩数据进行加密的方法提高了加密效率，并取得了广泛应用[2]。然而，由于图像数据量大、冗余度高，其压缩数据量较大，这种方法的加密速度仍难于满足图像的实时安全传输要求。

为了解决这一问题，目前图像的部分加密方法得到了越来越多的关注。该方法只加密图像压缩编码的部分重要数据，进一步降低了加密数据量，具有满足实时加密的潜力。最近，基于小波变换、四叉树和离散余弦变换的部分加密方法陆续被提出[3-5]。其中，多级树集合分裂(Set Partitioning In Hierarchical Trees, SPIHT)是 Said 和 Pealman 提出的一种高效率静态图像压缩编码算法[6]，非常适用于图像部分加密方案。文献[3]提出了只加密 SPIHT 压缩编码前两层数据的灰度图像部分加密方法；文献[4]则基于 SPIHT 提出了一种彩色图像的部分加密算法。本文研究了 SPIHT 压缩编码的 6 种数据类型，分析了灰度图像 SPIHT 中不同类型编码数据对图像重建的作用，确定了其中的重要数据类型，并将其用流密码进行了加密。仿真实验结果表明，与加密 SPIHT 前两层全部数据的方法相比[3]，本文方法在保障了图像加密安全性的同时进一步减少了加密数据量。

2 SPIHT 编码原理

首先对图像进行离散小波变换，并将所有高频子带小波系数根据一定规则划分为空间方向树(Spatial Orientation Trees, SOT)集合。然后用渐进量化编码对小波系数进行编码。在编码中，SPIHT 借助了 3 个链表：不重要系数链表(List of Insignificant Pixels, LIP)，不重要集合链表(List of Insignificant Sets, LIS)和重要系数链表(List of Significant Pixels, LSP)，并用小波系数矩阵中 LL 层的小波系数初始化 LIP，用所有的 SOT 初始化 LIS，初始化 LSP 为空集。

SPIHT 编码由扫描 3 个链表完成。当阈值为 T_k 时，k=0,1,…, K (K 由压缩率决定)，扫描过程如下：(1)LIP 扫描：将不重要系数保留在 LIP 中，重要系数移入 LSP，并输出表示系数重要性和符号的比特 $B_{k,\text{LIP-sig}}$ 和 $B_{k,\text{LIP-sgn}}$；(2)LIS 扫描：扫描 LIS 中所有的 SOT，如果 SOT 中不包括重要系数(即 SOT 不重要)将其保留在 LIS 中；反之，则将 SOT 分裂为 4 个直接后代和更小的 SOT，将小 SOT 加入到 LIS 链尾，并判断 4 个直接后代系数的重要性，不重要系数放入 LIP 中，重要系数放入 LSP。同时，输出表示 SOT 重要性、系数重要性和符号的比特 $B_{k,\text{LIS-T}}$，$B_{k,\text{LIS-sig}}$ 和 $B_{k,\text{LIS-sgn}}$；(3)LSP 扫描：输出 LSP 中每个系数第 n(n = lb(T_k))个位平面的比特 $B_{k,\text{LSP}}$ 到压缩数据中。至此一个循环扫描完成，改变阈值 $T_{k+1}=T_k/2$ 进入下一次扫描。如此迭代，直到输出数据达到要求的压缩率为止。

3 基于 SPIHT 算法的部分加密

3 个链表扫描过程产生的不同类型压缩数据在解码中起

基金项目：国家自然科学基金资助项目(60402013)；辽宁省自然科学基金资助项目(20062174)
作者简介：马洪军(1980－)，男，硕士研究生，主研方向：信息安全；林秋华，副教授、博士
收稿日期：2007-09-20 **E-mail：**mahj@163.com

着不同的作用。如果从中选择对解码极为重要的数据，则只对这部分数据进行加密即可保障图像安全，进而得到新的图像部分加密方案。

3.1 SPIHT 数据重要性分析

设 SPIHT 算法输出的压缩数据为 B(比特流)，B 可以分成有序的子集 $B=\{B_0, B_1,\cdots,B_k\}$，其中，$B_k$ 表示第 k 次迭代扫描产生的压缩数据。B_k 可以进一步划分为 $B_k=\{B_{k,\mathrm{LIP}}, B_{k,\mathrm{LIS}}, B_{k,\mathrm{LSP}}\}$，如图 1 所示。其中，$B_{k,\mathrm{LIP}}$，$B_{k,\mathrm{LIS}}$ 和 $B_{k,\mathrm{LSP}}$ 分别表示 LIP 扫描、LIS 扫描和 LSP 扫描产生的压缩数据。根据 SPIHT 编码原理，$B_{k,\mathrm{LIP}}$ 和 $B_{k,\mathrm{LIS}}$ 又分别由 $B_{k,\mathrm{LIP\text{-}sig}}$, $B_{k,\mathrm{LIP\text{-}sgn}}$ 和 $B_{k,\mathrm{LIS\text{-}T}}$, $B_{k,\mathrm{LIS\text{-}sig}}$, $B_{k,\mathrm{LIS\text{-}sgn}}$ 组成(见图 1)。

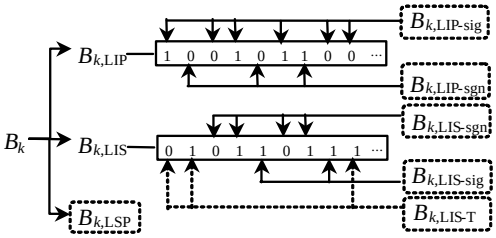


图 1　B_k 包含的数据类型

由上可见，SPIHT 算法产生了 $B_{k,\mathrm{LIP\text{-}sig}}$, $B_{k,\mathrm{LIP\text{-}sgn}}$, $B_{k,\mathrm{LIS\text{-}T}}$, $B_{k,\mathrm{LIS\text{-}sig}}$, $B_{k,\mathrm{LIS\text{-}sgn}}$ 和 $B_{k,\mathrm{LSP}}$ 6 种类型数据，下面结合实验对其在解码中的重要性进行讨论：

(1)$B_{k,\mathrm{LIP\text{-}sig}}$ 表示 LIP 链表中系数的重要性。LIP 链表包含了所有低频子带系数和部分高频子带系数。由于低频子带集中了图像的绝大部分能量，这部分数据对图像重构极为重要。另外，在编码中如果 $b_i\in B_{k,\mathrm{LIP\text{-}sig}}$ 且 $b_i=1$，则 $b_{i+1}\in B_{k,\mathrm{LIP\text{-}sgn}}$；如果 $b_i=0$，则 $b_{i+1}\in B_{k,\mathrm{LIP\text{-}sig}}$，即改变 $B_{k,\mathrm{LIP\text{-}sig}}$ 将直接影响后面比特的意义，进而产生连锁反应，直接影响后面大部分或所有数据的意义。所以，$B_{k,\mathrm{LIP\text{-}sig}}$ 在解码中是重要数据。图 2(a)是 lena 原始图像；图 2(b)是改变这类数据后的重构图像，从中已不能分辨原图像的任何信息。

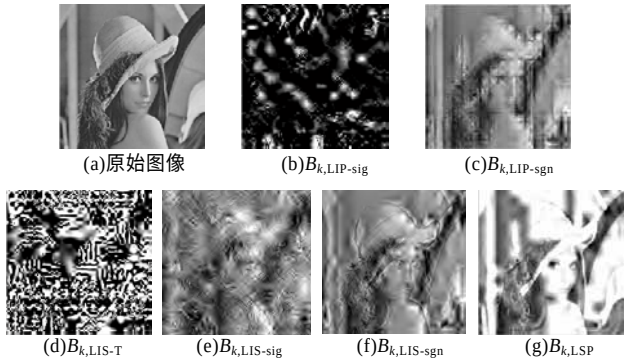
(2)$B_{k,\mathrm{LIP\text{-}sgn}}$ 表示 LIP 链表中重要系数的符号。它只会影响一个系数值，不影响其他数据的意义，因此，不属于重要数据。图 2(c)是改变 $B_{k,\mathrm{LIP\text{-}sgn}}$ 后的重构图像，尽管发生了失真，但仍能获得原图像信息。

(3)$B_{k,\mathrm{LIS\text{-}T}}$ 表示 SOT 的重要性，影响 SOT 中的所有系数值。SPIHT 算法中 SOT 的前后状态相互关联。如果第 k 次迭代扫描产生的 $B_{k,\mathrm{LIS\text{-}T}}$ 值不确定，后面迭代产生的 $B_{n,\mathrm{LIS\text{-}T}}(n>k)$ 都会受到影响。也就是说，这类数据不但影响所有高频子带系数值，而且还影响其后面数据的意义。图 2(d)是改变 $B_{k,\mathrm{LIS\text{-}T}}$ 后的重建图像，从中已无法辨别原图像信息，表明了 $B_{k,\mathrm{LIS\text{-}T}}$ 数据的重要性。

(4)$B_{k,\mathrm{LIS\text{-}sig}}$ 表示 SOT 中系数的重要性。由于这些系数来自高频子带，表示图像的纹理和边缘，因此这部分数据错误仅导致图像模糊不清，但仍然可以分辨图像轮廓。图 2(e)是改变这类数据后的重构图像，表明 $B_{k,\mathrm{LIS\text{-}sig}}$ 在解码中的重要性较低。

(5)$B_{k,\mathrm{LIS\text{-}sgn}}$ 表示 SOT 中重要系数的符号。它的作用与 $B_{k,\mathrm{LIP\text{-}sgn}}$ 相似，也属于非重要解码数据。不同的是 $B_{k,\mathrm{LIP\text{-}sgn}}$ 产生于 LIP 扫描，而 $B_{k,\mathrm{LIS\text{-}sgn}}$ 产生于 LIP 扫描。图 2(f)是改变 $B_{k,\mathrm{LIS\text{-}sgn}}$ 后的重构图像，原图像信息仍然可见。

(6)$B_{k,\mathrm{LSP}}$ 表示系数最高位平面以下的比特，它能使重构系数值逐渐逼近原系数值，从而进一步提高解压缩图像的质量。改变 $B_{k,\mathrm{LSP}}$ 只影响小波系数值的大小，但不影响其他比特的意义，因此为非重要比特。图 2(g)是改变这种类型比特后的重构图像。由图可见，只是图像的亮度发生了改变。



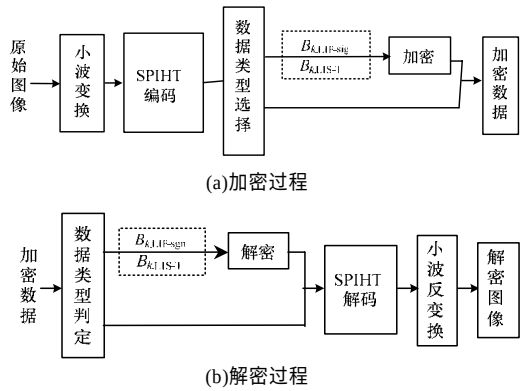
(a)原始图像　(b)$B_{k,\mathrm{LIP\text{-}sig}}$　(c)$B_{k,\mathrm{LIP\text{-}sgn}}$

(d)$B_{k,\mathrm{LIS\text{-}T}}$　(e)$B_{k,\mathrm{LIS\text{-}sig}}$　(f)$B_{k,\mathrm{LIS\text{-}sgn}}$　(g)$B_{k,\mathrm{LSP}}$

图 2　改变 SPIHT 6 类比特后的重构图像

3.2 部分加密方案

根据上面的分析可知，$B_{k,\mathrm{LIP\text{-}sig}}$, $B_{k,\mathrm{LIS\text{-}T}}$ 在 SPIHT 算法中是重要数据。而且，这两类数据直接影响其它类型数据的意义。因此，只需加密前 N 次迭代产生的 $B_{k,\mathrm{LIP\text{-}sig}}$, $B_{k,\mathrm{LIS\text{-}T}}$，便可达到保护所有图像数据的目的。据此，本文给出新的部分加密方案如图 3 所示。其中，图 3(a)中“数据类型选择”和图 3(b)中“数据类型判定”是在前 N 次迭代中确定 $B_{k,\mathrm{LIP\text{-}sig}}$ 和 $B_{k,\mathrm{LIS\text{-}T}}$。“加密”环节采用了流加密算法，主要通过伪随机发生器产生的随机比特流与重要数据比特异或完成加密。



(a)加密过程

(b)解密过程

图 3　基于 SPIHT 的部分加密算法原理

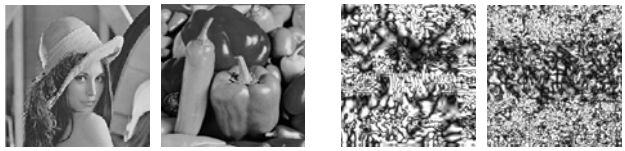
在部分加密应用中，迭代次数 N 的选择不宜小于 2。由于图像经过小波变换后能量主要集中在低频子带，高频子带能量少且小波系数值较小，这样，前 2 次迭代扫描中 SOT 不重要的概率较大，产生的 $B_{k,\mathrm{LIS\text{-}T}}$ 编码数据中往往多数为“0”。根据这一特点，攻击方易于从“0”串中推断出加密数据的位置，进而用穷举搜索法攻击加密数据[7]。因此，为了保障部分加密的安全性，N 应至少选取为 2。

4　仿真实验

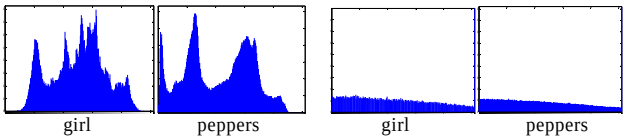
本文基于 Matlab7.0 平台，以标准灰度图像库中的图像为对象进行了计算机仿真实验。其中，图 4 给出了 2 幅实验灰度图像(图 4(a))及其部分加密结果。在实验中，加密了 SPIHT 算法前两次迭代(N=2)扫描产生的 $B_{k,\mathrm{LIP\text{-}sig}}$ 和 $B_{k,\mathrm{LIS\text{-}T}}(k=0,1)$。加密用随机比特流由 BBS(Blum-Blum-Shub)产生[1]。图 4(b)是由加密数据流重构的二幅图像，显然从中已无法辨别原图像信息。

为了进一步表明部分加密的安全性，本文比较了原始图像和加密图像的直方图。其中，图 4(c)是二幅原始图像的直

方图，图 4(d)是二幅加密图像的直方图。由图可见，部分加密打破了原始图像的统计特性，将原始图像的特殊分布直方图变成了近似均匀分布的直方图，大大降低了加密图像和原始图像的相关性。



(a)原始图像　(b)加密图像



(c)原始图像直方图　(d)加密图像直方图

图 4　2 幅图像的部分加密实验

本文与文献[3]方法的部分加密数据量进行了比较，结果如表 1 所示。其中“加密百分比”是加密数据量与压缩数据量的比值。文献[3]提出的部分加密方法是将前 2 次迭代(k=0,1)中产生的所有压缩数据全部加密，而本文仅选择了其中的重要比特 $B_{k,\mathrm{LIP\text{-}sig}}$ 和 $B_{k,\mathrm{LIS\text{-}T}}$ 进行加密。因此，与文献[3]方法相比，本文的加密数据量减少近一半。同时，因为所选择加密数据的重要性，图像的数据安全仍可得到保障。

表 1　本文方法与文献[3]方法的加密数据量比较

原始图像	行×列	加密数据量(比特) /加密百分比	
		本文方法	文献[3]方法
lena.jpg	256×256	764 / 2.91%	1 167 / 4.45%
peppers.bmp	512×512	3 205 / 2.45%	5 142 / 3.92%

5　结束语

通过研究 SPIHT 不同类型数据编码在图像重建中的重要性，本文提出了一种新的图像部分加密方法。该方法只加密压缩 SPIHT 压缩编码的 $B_{k,\mathrm{LIP\text{-}sig}}$ 和 $B_{k,\mathrm{LIS\text{-}T}}$。仿真实验结果表明，本文方法在保障图像安全性的同时，降低了加密数据量，因此，在图像实时加密传输方面具有广泛的应用前景。如何基于 SPIHT 实现彩色图像的部分加密方法是下一步的研究工作。

参考文献

[1] Alfred J M, Paul C V, Scott A V. Handbook of Applied Cryptography [M]. [S. l.]: CRC Press, 1996.

[2] Chang H K, Liou J L. An Image Encryption Scheme Based on Quadtree Compression Scheme[C]//Proceedings of the International Computer Symposium. Taiwan, Taibei, China: [s. n.], 2001: 230-237.

[3] Cheng H, Li Xiaobo. Partial Encryption of Compressed Images and Videos[J]. IEEE Signal Processing, 2000, 48(8): 2439-2451.

[4] Martin K, Lukac R, Plataniotis K N. Efficient Encryption of Wavelet-based Coded Color Images[J]. Pattern Recognition, 2005, 38(7): 1111-1115.

[5] Rodrigues J M, Puech W, Bors A G. Selective Encryption of Hunman Skin in JPEG Images[C]//Proc. of IEEE International Conference on Image Processing. Beijing, China: [s. n], 2006: 1981-1984.

[6] Said A, Pealman W. A New, Fast and Efficient Image Codec Based on Set Partitioning in Hierarchical Trees[J]. IEEE Trans. on Circuit and System for Video Technology, Lausanne, 1996, 6(3): 243-250.

[7] Said A. Measuring the Strength of Partial Encryption Schemes[C]// Proc. of IEEE International Conference on Image Processing. Washington, D. C., USA: [s. n.], 2005, 2: 1126-1129.

（上接第 145 页）

的使用价值也被破坏了。本实验直观地表现了水印的抗攻击性，证明了该水印模型不但嵌入算法简单，并且检测结果良好。

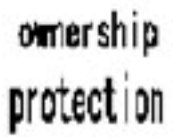


图 2　更改 5%子集

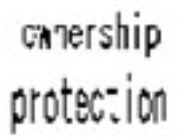


图 3　更改 20%子集

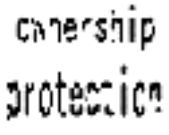


图 4　更改 30%子集

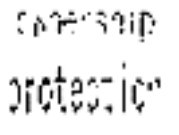


图 5　更改 40%子集

5　结束语

在关系型数据库中嵌入带有版权信息的图像信息，是数据库水印发展的一个新方向。本文利用标记算法及向量迭代算法在数据空域上嵌入水印，并利用 FastICA 算法提取水印。实验在水印盲测的环境中进行，对于攻击者篡改规模不大的数据，水印绝大部分能被恢复出来。

将来研究的重点在于提高水印的鲁棒性，可以借鉴水印图像在多媒体信息中的成熟应用，考虑在数据变换域中使用的小波变换、傅立叶变换等，通过空域和变换域算法的结合来提高水印的鲁棒性。

参考文献

[1] Agrawal R, Hass P J, Kiernan J. Watermarking Relational Databases[C]//Proceedings of the 28th International Conference on Very Large Databases. Hong Kong, China: [s. n.], 2002, 105-109.

[2] 刘　琚, 孙建德, 张新刚. 基于 ICA 的数字水印的方法[J]. 电子学报, 2004, 32(4): 657-660.

[3] 姜传贤, 孙星明, 易叶青, 等. 基于 JADE 算法的数据库公开水印算法的研究[J]. 系统仿真学报, 2006, 18(7): 1781-1784.

[4] Comon P. Independent Component Analysis, a New Concept[J]. Signal Process, 1994, 36(3): 287-314.

[5] 杨福生, 洪　波. 独立分量分析的原理与应用[M]. 北京: 清华大学出版社, 2006.

[6] 吴小培, 冯焕清, 周荷琴, 等. 基于独立分量分析的图像分离技术及应用[J]. 中国图像图形学报, 2001, 6(2): 133-137.

[7] 陈　刚, 陈莘萌. 基于独立分量分析的语种识别方法[J]. 计算机工程, 2006, 32(24): 17-19.

[8] Hyvarinen A, Oja E. A Fast Fixed-point Algorithm for Independent Component Analysis[J]. Neural Computation, 1998, 9(7): 1483-1492.