多重秘密共享的DCT域二值图像隐藏方案

曹如冰 艾斯卡尔
(新疆大学信息科学与工程学院 乌鲁木齐 830046)

摘 要 研究了一种新的二值图像隐藏方案,即将一幅二值图像隐藏在多幅载体图像中。针对二值图像取值形式为二值的特点,该方案第一次把变长游程编码算法、多重秘密共享思想和DCT域的信息隐藏算法结合在一起,并根据载体图像的最大隐藏信息量把秘密图像游程长度序列分成n块,由n个密钥控制并分别隐藏在n幅载体图像中。实验表明,该算法在不明显引入修改痕迹的情况下,可显著提高安全性和鲁棒性,并且可以无损还原。

关键词 多重秘密共享,二值图像,离散余弦变换,图像隐藏
中图法分类号 TP751 **文献标识码** A

Binary Image Hiding Algorithm Based on Multi-secret Sharing and DCT

CAO Ru-bing Askar
(College of Information Science and Engineering, Xinjiang University, Urumuqi 830046, China)

Abstract A new binary image hiding scheme was proposed, which hided a binary image into several cover images. Based on the characteristics of the binary image whose value is 0 or 1, this scheme combined multi-secret sharing with RLE algorithm and DCT algorithm for the first time. According to the biggest size of cover images, this scheme divided RLE length of the shadow image into the n blocks, and then embedded the n blocks of secret information in cover images under the control of n keys. Experiment demonstrates that this scheme sufficiently increases the security of secret information and improves the robustness and acheves the better recovery effect.

Keywords Multi-secret sharing, Binary image, Discrete cosine transform, Image hiding

图像隐藏是信息隐藏技术的一个分支,其基本原理是利用人们在视觉、系统分辨上的限制,以公开图像信息为载体,将秘密信息隐藏于其中,从而掩盖秘密信息的存在,其目的是在不引起第三方注意的情况下将信息隐蔽地发送出去。隐蔽性和鲁棒性是衡量掩密技术优劣的重要指标[1,2]。近几年,二值图像的应用越来越广泛,比如文件传真、手写签名、社会安全档案、保险信息、金融文档等常以二值图像的形式传输[3,4]。如何能更安全、更大容量地传输这些保密信息,成为迫切需要解决的问题。

目前,针对二值图像已有多种信息隐藏方法。其中,在基于图像空域的信息隐藏技术中,最经典的算法是最不重要位(LSB)替换信息隐藏算法[5],为了达到隐藏秘密信息的目的,需要调整替换掩护图像像素值的最低1~3位有效位来实现。但只是通过简单的替换修改掩护图像像素值的LSB方法,不但鲁棒性差,而且无法保证通信的安全,这就要求有鲁棒性更好和安全性更高的信息隐藏算法。其中比较有代表性的算法是王继军等人提出的基于LSB的数字图像分存隐藏算法[6]。该算法利用混沌和密码学原理实现了位置和像素值的双置乱,并把置乱后的序列分成几段,采用改进的LSB替换算法分别嵌入到不同的载体图像中。虽然该算法安全性较高,并增加了嵌入秘密信息的容量,而且可以无损还原,但其鲁棒性很差,一旦对载密图像进行细微地改变,就会导致秘密信息无法提取。

针对上述方案的缺点,作者研究了一种新的二值图像隐藏方案,它基于多重秘密共享思想[7,8],并利用变长游程编码[9]压缩方法将秘密图像分成奇偶块隐藏于多幅载体图像中,以轻微地牺牲不可见性为代价,提高了方案的鲁棒性。本方案的特点如下:(1)根据秘密图像相对载体图像的大小生成n个秘密信息块,每一信息块都是秘密图像的"0"游程长度统计和"1"游程长度统计,不但减小了隐藏信息块时所需载体图像的容量,而且不需要再对秘密图像进行置乱预处理,从而降低了计算量。(2)用n个密钥控制n个秘密信息块的嵌入,改变了传统的单人加密/解密、签名和认证模式,能够分散责任,防止权威欺骗,提高了系统的安全性,对重要信息的安全保存、传输及合法利用具有重要的意义。(3)通过比较变换后的两个DCT系数来完成信息的隐藏,而且所选系数为中频系数,并引入控制量alpha放大系数差值,从而兼顾了不可见性和鲁棒性。

1 基于LSB的数字图像分存隐藏算法[6]

此算法首先将秘密信息转为一维序列,利用混沌和密码学原理来实现位置和像素值的双置乱;然后把置乱后的序列

到稿日期:2010-11-17 返修日期:2011-04-08 本文受国家自然科学基金项目(61065001),新疆维吾尔自治区科技厅少数民族特殊培养计划项目(201023116)资助。

曹如冰(1985—),女,硕士,主要研究方向为图像隐藏技术,E-mail:rubing19851006@sina.com;艾斯卡尔(1972—),男,博士后,教授,博士生导师,主要研究方向为多媒体信息处理。

分成几段，利用其改进的 LSB 算法即确保最多只修改一位的前提下，在同一个字节中嵌入两位秘密信息，分别嵌入到大小合适的几幅载体图像中，实现秘密信息的分存。此算法有以下两个弊端：(1)该算法没有对秘密图像进行任何压缩处理，使得隐藏信息量不是太高；(2)采用改进的 LSB 算法进行秘密信息的嵌入，鲁棒性很差。

2 本文的方案

本文研究了一个基于多重秘密共享的二值图像隐藏方案，方案根据载体图像的最大隐藏信息量把秘密图像游程长度序列按照奇偶分块分成 n 块，并在 n 个密钥的控制下分别隐藏在 n 幅载体图像中。这样既增加了隐藏秘密信息的容量，又有助于鲁棒性的提高。

2.1 游程长度序列奇偶分块处理

游程编码序列的存储结构如表 1 所列，游程序列奇偶分块实现流程如图 1 所示。这里所谓的奇偶分块就是把一个序列的元素按照所处的奇偶位置分成奇数块序列和偶数块序列，得到的新序列仍然以表 1 的方式进行存储。

表 1 游程编码存储结构

b(1)	c(1)	b(2)	c(2)	…	b(i)	c(i)

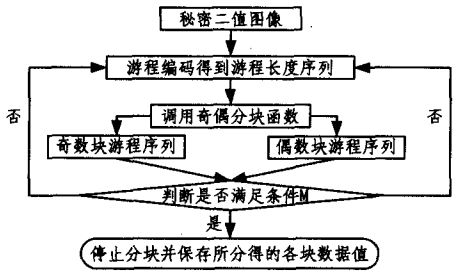

图 1 游程序列奇偶分块流程图

表 1 所列结构中，$b(i)$表示位于奇数位置上的游程长度，$c(i)$表示位于偶数位置上的游程长度。由于二值图像的“0”行程和“1”行程总是交替出现的，因此不用浪费存储空间存储初始游程的值，就可以很方便地通过查看二值图像的矩阵得到初始游程。

图 1 中条件 M 也就是 $floor(m\times n/count)>1$，其中 $m\times n$ 为每一个载体图像大小，count 是所嵌入的信息量，floor 是下取整函数。所谓的奇偶分块函数就是把一个游程序列的元素按照所处的奇偶位置分成奇数块序列和偶数块序列，得到的新序列仍然以表 1 的方式进行存储。分块处理实现步骤如下。

1) 对秘密二值图像进行游程编码，在对二值图像进行行扫描后，将二值序列变换成一一对应的游程长度序列 N；

2) 调用已编写好的奇偶分块函数把 N 序列分成两个序列 $N1$ 和 $N2$，按表 1 进行存储，根据 $N1$ 和 $N2$ 各自的最大值来确定编码的最小 bit 位 $n1\_num$ 和 $n2\_num$，并计算出编码后各自的信息量 $count1$ 和 $count2$；

3) 把 $count1$ 和 $count2$ 分别代入 $floor(m\times n/count)$，看是否大于 1。如果大于 1，则停止分块并保存 $n1\_num$、$n2\_num$ 、$count1$ 和 $count2$ 的值，这时 $n=2$。否则就以 $N1$ 和 $N2$ 为初始游程序列重复上述 2)。如此循环下去，便可以得到最终的分块结果。

2.2 算法实现

本节利用 2.1 节提出的奇偶分块方法，对二值图像进行游程长度序列奇偶分块处理后再进行 DCT 信息隐藏，紧接着进行秘密信息的提取，恢复出二值图像。其算法的原理框图如图 2 所示。

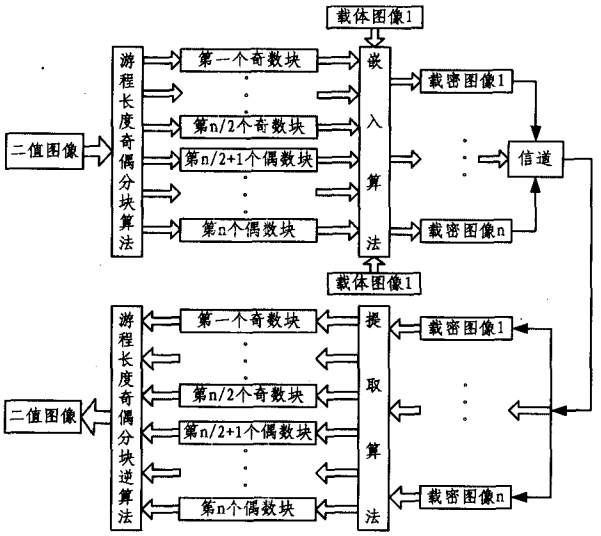

图 2 信息隐藏及提取的原理框图

其算法步骤如下：

(1) 奇偶分块处理

对二值图像进行分块处理，根据 2.1 节的奇偶分块算法将其分成 n 块，并保存每一块二进制编码后的秘密信息长度 $n1\_length$，$n2\_length2$，…，nn_length 和串编码长度 $n1\_num$，$n2\_num$，…，nn_num。

(2) 将得到的 n 块秘密信息分别嵌入到 n 幅载体图像中

1) 对 n 幅载体图像分别做 DCT 变换和分块；

2) 使用 n 个安全的随机数生成器，利用 n 个密钥生成压缩后信息嵌入的位置[row(i)]，col(i)]1，…，[row(i)]，col(i)]n；

3) 对于每一图像块，选择在 JPEG 压缩算法中亮度量化值一样的两个中频系数 b 和 c；

4) 选择合适的控制量 $alpha$，并比较 b 和 c 两个系数的大小进行随机嵌入，从而将 n 块秘密信息分别嵌入到 n 幅载体图像中。

(3) 把 n 幅载密图像组合起来恢复出秘密二值图像

1) 对 n 幅载密图像进行 DCT 逆变换和分块；

2) 根据 n 个密钥按照随机控制的顺序直接比较两个系数的大小，提取出秘密信息块；

3) 根据奇偶分块的逆运算将秘密信息块组合成一个新的序列 new_msg；

4) 解码时只要根据连续数据串的编码长度 $n1\_num$，$n2\_num$，…，nn_num 和秘密信息长度 $n1\_length$，$n2\_length2$，…，nn_length 以及初始像素值 a 就可以恢复出原来的二值图像。

3 仿真实验与讨论

3.1 本文方案算法仿真

为了验证 2.2 节提出的基于 DCT 和多重秘密共享的二值图像隐藏算法，在 MATLAB 7.0 的编程环境下，处理器为 1.73GHz，内存为 504MB 的笔记本电脑一台，用大小为 256×

256 像素的8 bit 灰度图像 cameraman. tif 和大小为 240×291 像素的 8 bit 灰度图像 pout. tif 作为载体图像，秘密二值图像为图 3 所示的原始二值图像 logo. tif，对算法进行测试。利用本方案得到的实验结果如图 3—图 5 所示。

图 3　原始秘密二值图像和提取出的二值图像对比

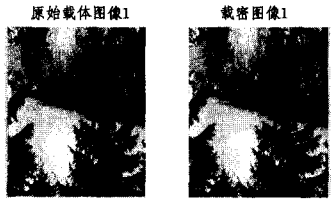

图 4　原始载体图像与隐藏奇数块信息图像对比

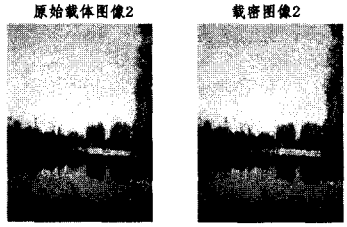

图 5　原始载体图像与隐藏偶数块信息图像对比

图 4 和图 5 表明，通过肉眼看不出隐藏秘密信息前后两幅图像之间的差别，也就是说本文算法的不可感知性即隐蔽性是相当出色的；由图 3 可知，本算法可以成功地提取出秘密二值图像。

3.2　两方案峰值信噪比的对比

图 6 是从搜狐网站下载的 3 幅二值图像，图像原始数据流总位数均为 27200 位。表 2 是本方案与基于 LSB 的数字图像分存隐藏算法的峰值信噪比的对比。

图 6　3 幅二值图像

表 2　两种方案信噪比对比

嵌入二值图像		newhuan. tif	newliuren. tif	logo. tif
LSB 隐	第一段	40. 3321	40. 3324	40. 3325
藏算法	第二段	38. 262	38. 2619	38. 262
本方案	奇数块嵌入	40. 1553	40. 2085	40. 1613
psnr	偶数块嵌入	38. 1828	38. 2179	38. 1764

表 2 中基于游程编码方案的 psnr 是通过仿真基于游程编码的二值图像隐藏方案的 matlab 程序并调用峰值信噪比函数 psnr. m 得到的，而本方案的 psnr 是通过调用峰值信噪比函数 psnr. m 分别计算嵌入奇数块信息的载体图像的 psnr 和嵌入偶数快信息的载体图像的 psnr 得到的。由表 2 可知，本算法与基于 LSB 的数字图像分存隐藏算法的峰值信噪比相比，其峰值信噪比略微降低。在牺牲了信噪比的同时，本算法获得了以下优点：(1)在相同的压缩率下能实现更大的信息隐藏量和更少的改变载体图像；(2)由于多密钥的控制，其安全性较高。

实验中如果采用彩色图像作为载体图像，也可以得到较理想的峰值信噪比。但为了在相同的条件下与基于游程编码的二值图像隐藏方案做对比，便选择了灰度图像来隐藏秘密二值图像。

3.3　两方案鲁棒性对比

这里仍然以 logo. tif 为秘密信息，以 rain. jpg 和 redlake. jpg 为载体图像。用 jpgandlumda 函数(该函数自动取 10%到 100%的 10 次 JPEG 压缩)和 jpgandalpha 函数(此函数自动取 0. 1 到 1 的 10 个等差为 0. 1 的值作为控制阈值 a，然后对载密图像进行压缩率从 10%到 100%做 10 次 JPEG 压缩)，分别检验在 JPEG 条件下 LSB 隐藏算法和本方案隐藏算法的鲁棒性，实验结果如图 7 和图 8 所示。

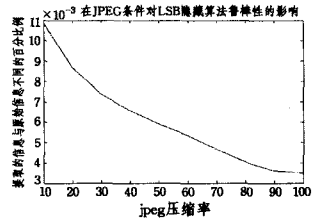

图 7　在 JPEG 条件下 LSB 隐藏算法的鲁棒性

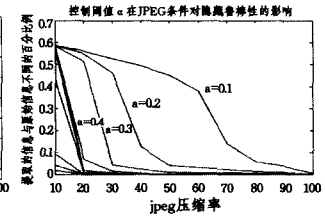

图 8　在 JPEG 条件下本方案隐藏算法的鲁棒性

图 7 表明，LSB 隐藏算法不能抵抗任何压缩率的 JEPG 压缩，无论压缩率取何值都不能保证信息提取的正确性，故它不具有鲁棒性。由图 8 可知，控制阈值 a 取 0. 1 时，不能完全保证信息提取的正确性；当 a 在[0. 2，0. 4]区间内时，抗 JPEG 压缩的性能一般；当 a 取 1 时，可以认为其几乎不受 JPEG 压缩的影响。因此本方案隐藏算法具有较高的鲁棒性。由此可见，本方案隐藏算法的鲁棒性远远好于基于 LSB 的数字图像分存隐藏算法。

结束语　本文研究了一种多重秘密共享的二值图像隐藏方案，巧妙地把游程编码、多重秘密共享思想和 DCT 域隐藏算法结合起来，把处理秘密二值图像转换成处理游程编码序列长度。游程编码序列长度奇偶分块算法既简便易行，又达到了压缩秘密图像信息的目的，而且无需对秘密图像进行置乱处理；由参数 *alpha* 控制的 DCT 域隐藏算法，不但大大提高了隐藏的鲁棒性，而且在一定程度上缓解了隐蔽性和鲁棒性的矛盾；同时，在嵌入信息时，嵌入位置是通过密钥控制的，将安全性寓于密钥之中，因此可以将信息隐藏算法公开，符合 Kerckhoffs 原则。实验证明，此方法的信息隐藏量大、计算量小、载密图像无明显失真、可无损还原并具有很好的鲁棒性。

参 考 文 献

[1]　Zhang Jun. Method of optimizing the data hiding technique for binary images using genetic algorithm[J]. Computer Engineering, 2006, 32(9): 38-40

[2]　Zhong Hua, Zhang Xiao-hua, Jiao Li-cheng. Digital watermarking and image authentication: algorithm and applications[M]. Xi'an: Xidian University Press, 2006

(下转第 284 页)

进程的优化摆放结果。

图 10 对比 Round-Robin 与优化进程摆放后，NAS 基准中 BT、CG 等基准(class C)的节点内通信率的对比，优化后的进程摆放策略能有效提高节点内的通信率。虽然通过合理的进程摆放能提高 MPI 程序节点内的通信率，但进一步提升 MPI 程序的性能还需要进一步提高 cache 的利用率。

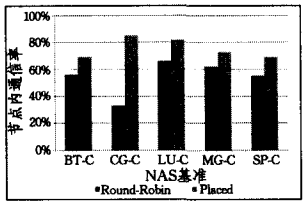

图 10　两种不同进程摆放策略下 NAS 基准全局节点内通信率比

结束语　多核机群的存储层次化使得多核机群具有与传统的 SMP 平台显著不同的特征，因此，未经优化直接运行在多核机群上的 MPI 并行程序无法得到最优的性能。本文在对比了多核机群性能特征的基础上，实验分析了几种可行的、具有普遍意义的 MPI 程序优化技术。实验证明，这几种方法对多核机群下 MPI 程序的性能提升具有一定的有效性和通用性。后续工作将继续研究多核机群下 MPI 程序可能的优化空间，例如多核机群下 MPI 集合通信的优化等。

参 考 文 献

[1] Chai L, Lai P, Jin H W, et al. Designing an efficient kernel-level and user-level hybrid approach for mpi intra-node communication on multi-core systems[C]// ICPP '08: Proceedings of the 2008 37th International Conference on Parallel Processing. Washington, DC, USA, IEEE Computer Society, 2008

[2] TOP500 Team[R]. TOP500 Report for June 2009. http://www.top500.org

[3] MPI: A Message-Passing Interface Standard[S]. http://www.mpiforum.org/docs/mpi-11-html/mpi-report.html

[4] Tu Bi-bo, Zou Ming, Zhan Jian-feng, et al. Multi-core Aware Optimization for MPI Collectives, poster[C]// The 2008 IEEE International Conference on Cluster Computing (Cluster 2008). Tsukuba, Japan, 29 September-1 October, 2008

[5] Rabenseifner R, Hager G, Jost G. Hybrid MPI/OpenMP Parallel Programming on Clusters of Multi-Core SMP Nodes[C]// Didier El Baz, et al., eds. Proceedings of the 17th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP 2009). Weimar, Germany, Computer Society Press, Feb. 2009: 427-236

[6] Chaarawi M, Squyres J M, Gabriel E, et al. A tool for optimizing runtime parameters of open mpi[C]// Proceedings of the 15th European PVM/MPI Users' Group Meeting on Recent Advances in Parallel Virtual Machine and Message Passing Interface. Berlin, Heidelberg: Springer-Verlag, 2008: 210-217

[7] Pellegrini S, Wang Jie, Ahringer T, et al. Optimizing MPI Runtime Parameter Settings by Using Machine Learning[C]// Proceedings of the 16th Euro PVM/MPI Users' Group Meeting on Recent Advances in Parallel Virtual Machine and Message Passing Interface. Espoo, Finland, 2009

[8] Solt D. A profile based approach for topology aware MPI rank placement[OL]. http://www.tlc2.uh.edu/hpcc07/Schedule/speakers/hpcc_hp-mpi_solt.ppt, 2007

[9] Mercier G, Clet-Ortega J. Towards an Efficient Process Placement Policy for MPI Applications in Multicore Environments [C]// Proceedings of the 16th Euro PVM/MPI Users' Group Meeting on Recent Advances in Parallel Virtual Machine and Message Passing Interface. Espoo, Finland, 2009

(上接第 266 页)

[11] Klosowski J T, Held M, Mitchell J S B, et al. Efficient collision detection using bounding volume hierarchies of k-Dops[J]. IEEE Transactions on Visualization and Computer Graphics, 1998, 4(1): 21-36

[12] Hubbard P M. Approximating polyhedra with spheres for time critical collision detection[J]. ACM Transactions on Graphics, 1996, 15(3): 179-210

[13] Gottschalk S, Lin M C, Manocha D. OBB Tree: a hierarchical structure for rapid interference detection[C]// The Proceedings of SIGGRAPH. 1996: 171-180

[14] Ramírez E, Navarro H, Carmona R, et al. Optimizing Collision Detection Based on OBB Trees Generated with Genetic Algorithm[C]// IV Iberoamerican Symposium in Computer Graphics-SIACG. 2009: 1-7

[15] Fares C, Hamam Y. Collision detection for rigid bodies: A state of the art review[C]// GraphiCon. 2005

(上接第 272 页)

[3] 钱振兴，程义民，谢春辉，等. 基于嵌入矩阵的二值图像隐藏方法[J]. 电路与系统学报，2008，13(6)：128-131

[4] 谢建全，阳春华，谢勋，等. 一种大容量的二值图像信息隐藏算法[J]. 小型微型计算机系统，2008，29(10)：1874-1877

[5] 王国新，平西建，张涛，等. 空域 LSB 信息伪装及其隐写分析[J]. 计算机工程，2008，34(1)：173-174，189

[6] 王继军，张显全，韦月琼. 基于 LSB 的数字图像分存隐藏算法[J]. 计算机工程，2008，29(23)：6167-6169

[7] 侯整风，高汉军. 一个新的基于多重秘密共享的图像隐藏方案[J]. 计算机应用，2008，28(4)：902-905

[8] LIBAI. Areliable(k, n) image secretsharing scheme[C]// 2nd IEEE International Symposium on Dependable, Autonomic and SecureComputingIndianapolis. Indiana, USA: IEEE Press, 2006: 31-36

[9] 杨全周，蔡晓霞，陈红. 一种基于游程编码的二值图像隐藏方案[J]. 舰船电子对抗，2008，31(2)：86-88