

一种抗剪切信息隐藏算法

雷 芸^{1,4}, 孙泽锐^{2,4}, 王晓云³, 俞春强^{2,4}, 张显全^{2,4}

(1 广西民族大学 预科教育学院, 广西 南宁 530006; 2 广西师范大学 计算机科学系, 广西 桂林 541004;
3 长江师范学院 数学与计算机学院, 重庆 涪陵 408100; 4 桂林电子科技大学 广西信息科学实验中心, 广西 桂林 541004)

摘 要: 提出了一种基于拉丁方阵的抗剪切信息隐藏算法, 通过载体图像隐藏容量和秘密信息的大小确定隐藏秘密信息的备份数, 根据备份数确定隐藏信息的拉丁方阵模板, 对秘密信息进行分组和编号, 通过拉丁方阵模板按对应的编号, 将秘密信息嵌入到载体图像中, 实现信息隐藏. 实验结果表明该算法能够实现大容量隐藏并且能够抵抗大面积的剪切攻击, 具有较好的应用价值.

关键词: 信息隐藏; 拉丁方阵; 抗剪切; 最低有效位

中图分类号: TN402

文献标识码: A

文章编号: 1000-7180(2014)02-0132-05

An Information Hiding Algorithm Against the Cropping Attack

LEI Yun^{1,4}, SUN Ze-rui^{2,4}, WANG Xiao-yun³, YU Chun-qiang^{2,4}, ZHANG Xian-quan^{2,4}

(1 Pre-university School, Guangxi University for Nationalities, Nanning 530006, China;

2 Department of Computer Science, Guangxi Normal University, Guilin 541004, China;

3 College of Mathematics and Computer Science, Yangtze Normal University, Chongqing 408100, China;

4 Guangxi Experiment Center of Information Science, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: This paper proposes an anti-cropping steganography scheme based on Latin square. At first, the amount of secret copies is obtained by the cover image's hiding capacity and the length of the secret message. According to the amount of copies, a Latin square is confirmed as the template for hiding secret message. The secret message is divided into groups and each group is numbered. Then the secret groups are embedded into the cover image with the corresponding element in the Latin square. Experimental results indicate that the proposed scheme can achieve high capacity, and can be against the cropping attack. It has significant practical value for information security.

Key words: information hiding; Latin square; anti-cropping; least significant bit

1 引言

随着网络技术的发展, 信息安全备受人们的关注. 信息隐藏作为信息安全的重要研究领域, 得到了广泛应用. 信息隐藏目的是将秘密信息嵌入到载体中, 让截获者察觉不到隐秘通信的存在, 从而实现安全通信. 截获者虽然不能从截获图像中正确的提取出秘密信息, 如果对图像进行如加噪、滤波、剪切、压

缩、旋转等处理, 会破坏被隐藏的秘密信息. 能在破坏后的载密图像中正确提取出有效的秘密信息, 则能提高载密图像的鲁棒性, 进一步提高秘密信息的安全. 因此研究抗攻击的信息隐藏算法对信息保护具有重要的意义.

基于空域的信息隐藏算法中^[1-2], 虽然有较高的隐藏容量, 但抗噪性和抗剪切能力差. 谢建全等人在文献[3]中提出了一种能够在多个位平面自适应地

收稿日期: 2013-04-20; 修回日期: 2013-06-18

基金项目: 国家自然科学基金(61363034, 61300109); 广西自然科学基金(2011GXNSFD018026, 2012GXNSFBA053166, 0832104); 广西科学研究与技术开发计划项目(10123005-8); 重庆市教委科技项目(KJ121310); 涪陵区科技计划项目(FLKJ, 2012ABA1056); 广西信息科学实验中心项目(20130204)

嵌入秘密信息的信息隐藏方法,其信息隐藏量比 LSB 算法多一倍以上,但算法的抗噪性能和抗剪切能力差.赵玉霞^[4]等人提出了一种空域的抗剪切的信息隐藏算法,利用 Logistic 映射秘密图像的奇数行,利用 Hybrid 映射隐藏图像的偶数行,将秘密图像分散嵌入到整个载体图像中,对剪切面积不超过 50% 剪切攻击具有很强的抵抗性.赵培东等人^[5]将水印从中心到四周分层自适应地嵌入到子带中,并将特征点嵌入到小波,满足某个由密钥控制的函数关系,实现了一种无密钥者很难检测特征点的盲水印算法,能对一般的攻击和任意的剪切攻击具有抵抗性.文献[6]实现了一种基于 DCT 域的抗剪切数字水印,该算法首先对数字水印进行结构化编码,使编码后的水印具有标识功能,并设计了结构化的嵌入和提取策略,从而实现了抗剪切的水印算法.根据一般图像处理对变换后的低频系数影响较小的原理,彭波等人^[7]利用离散余弦变换和离散小波变换实现了一种抗剪切的数字水印算法.首先对原始图像小波分解后的低频系数矩阵进行 DCT 变换,将秘密信息进行 Arnold 置乱然后嵌入到 DCT 变换后的中低频系数中,能够较好地抵抗中值滤波和剪切攻击.王丽等人^[8]提出了一种利用 Patchwork 方法结合量化索引调制(QIM)的抗剪切数字水印方案,对常见的图像压缩和加噪处理有具有一定的抵抗性.文献[9]中利用小波变换通过多副本嵌入的方式,实现抗大面积剪切的数字水印算法.文献[10]在图像的小波域中用扩频方法实现了抗剪切盲水印算法,能够保证载密图像被剪切掉 75% 后二值数字水印的完整性.文献[11]中首次提出第二代水印的概念,利用水印处理过程中载体图像的局部性特征,实现可读水印的嵌入并且能够抵抗裁剪攻击,文献[12]结合图像特征提出抗剪裁的盲水印算法,实现隐藏信息的盲提取.文献[13]把水印特征嵌入到代表宿主载体基本特征的基矩阵中,从而获得好的抗剪切攻击,并引入 PCA 方法来加强矩阵元素间的联系,提高算法效率.

对信道中截获图像进行剪切是常见的一种破坏方式,如果能够从部分被剪切的载密图像中检测并提取出有效的秘密信息,则能提高信息隐藏算法的鲁棒性.为了使载密图像能够更好地抗剪切攻击,本文利用拉丁矩阵的特性生成嵌入模板,将多个秘密信息备份分组编号后嵌入到载体图像的最低有效位中,从而提高载密图像的抗剪切能力.

2 抗剪切的信息隐藏算法

2.1 秘密信息隐藏的份数

大部分空域隐藏算法是通过修改像素的低位实现对秘密信息的隐藏.如果隐藏的秘密信息在载体图像中的分布是均匀的,主要是通过对多份秘密信息进行冗余嵌入,即嵌入多个秘密信息的副本实现抗剪切攻击.首先,根据载体图像隐藏容量和秘密信息大小确定秘密信息的隐藏的份数,然后根据备份数确定拉丁方阵为嵌入模板,利用该模板将多个秘密信息副本嵌入到载体图像中.设载体图像大小为 $l \times w$,用于隐藏的位数为 h ,则其隐藏容量 $|V| = lwh$,秘密信息的大小 $|S|$,载体图像中可以隐藏秘密信息的份数 N 为

$$N = \frac{|V|}{|S|} \quad (1)$$

通过式(1)可确定秘密信息隐藏的份数.

2.2 确定拉丁方阵模板

拉丁方阵是一类方阵,每一行和每一列都包含组成该方阵的所有元素,每一个元素在每一行和每一列都恰好出现一次.图1所示为 4×4 的拉丁方阵,由 1,2,3,4 共 4 个元素组成,每个元素均在不同的位置出现 4 次.如果每个元素表示载体图像中大小相同的一个分块,隐藏 1 份秘密信息,则可实现 4 份秘密信息的隐藏,所以得到的载密图像具有较好的抗剪切能力.因此可通过拉丁方阵实现数据多个备份的隐藏,提高载密图像的抗剪切能力.设 $L = (l_{i,j})_{n \times n}$ 为 n 阶拉丁方阵($i = 1, 2, \dots, n, j = 1, 2, \dots, n$),方阵中 n 个元素组成集合为 $\{1, 2, \dots, n\}$,由于常用的测试图像行列数均为 2 的幂次方,所以取 $n = 2^k$.由于 n 阶拉丁方阵不唯一, 2×2 的拉丁方阵有 2 个, 4×4 的拉丁方阵有 576 个,并且随着 n 的增大增长很快,因此需选择一个拉丁矩阵作为秘密信息的嵌入模板.

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

图1 4×4 的拉丁方阵

根据式(1)计算秘密信息的备份数 N ,则有拉丁方阵的阶数 $n \geq N$.在生成的 n 阶拉丁方阵中,选取嵌入模板,使载密图像能够抵抗多种类型的剪切.为了抵抗不规则的区域剪切和抵抗边缘剪切,选取拉丁方阵中包含全部 n 个元素的 $k \times k$ 子矩阵尽可

能多,且拉丁方阵中心 $k \times k$ 子矩阵必须包含拉丁方阵的 n 个元素. 例如 $n = 4$ 时,如图 1 所示为其模板,含有 1,2,3,4 这些不同元素的 2×2 子矩阵共有 7 个,且中间的 2×2 子矩阵包含所有不同的元素.

设在 $k \times k$ 子矩阵含 n 个元素最多且中心子矩阵也含 n 个元素的 n 阶拉丁方阵为 $C_1, C_2, \dots, C_m$. 为了提高载密图像的抗线剪切能力,相同编号的元素尽可能不分布在同一条斜线上. 设第 i 个拉丁方阵中,与主对角线平行 $2n-1$ 条的对角线上包含不同元素数的个数为 x_i ,与次对角线平行 $2n-1$ 条的对角线上包含不同元素数的个数为 y_i ,令:

$$z_i = \max(x_1 + y_1, x_2 + y_2, \dots, x_m + y_m) \quad (2)$$

选取 C_i 为拉丁方阵的模板.

例如当 $n = 8$ 时, $k = 3$, 秘密信息被平均分为大小相同的 8 个组,若要在图像被剪切后提取一份完整的秘密信息,则在剪切后的载密图像中,至少 8 个不同位置的秘密信息有 1 个没有被破坏. 所以选取拉丁方阵 3×3 的子矩阵包含 8 个组的个数要尽可能多,这样能够保证保留 1 份完整秘密信息的概率较大. 同时同一直线上的隐藏信息尽可能不相同,图 2 中给出了一个符合上述条件的 8×8 阶拉丁方阵的例子.

1	2	3	4	5	6	7	8
6	5	8	7	1	2	4	3
7	4	2	6	3	8	5	1
8	3	1	5	7	4	6	2
5	6	4	8	2	1	3	7
2	1	7	3	6	5	8	4
3	8	5	2	4	7	1	6
4	7	6	1	8	3	2	5

图 2 8×8 的拉丁方阵

2.3 嵌入算法和步骤

根据载体图像的隐藏容量和秘密信息的大小,由式(1)计算秘密信息隐藏的份数 N ,根据 N 确定拉丁方阵的阶数 $n(n \geq N, n = 2^k)$. 然后在 n 阶拉丁方阵中,根据 2.2 节中的规则选取一个拉丁方阵 C 作为嵌入模板,设 C 中的元素为 $C(i, j) (1 \leq i \leq n, 1 \leq j \leq n)$,将秘密信息分为 n 个组,分别用 $W_1, W_2, \dots, W_n$ 表示. 设载体图像为 I ,将载体图像分为 $n \times n$ 个大小相同块,每个块的编号为 $I_{i,j} (1 \leq i \leq n, 1 \leq j \leq n)$,这样可在每块中隐藏一组秘密信息,每组秘密信息在不同的位置隐藏 n 份,实现对秘密信息保护. 设载体图像第 $I_{i,j}$ 块中隐藏第 r 组秘密信息,则有

$$r = C(i, j) \quad (3)$$

从上可知,在 $I_{i,j}$ 中隐藏 W_r 中的秘密信息. 例如载体图像 $I_{2,3}$ 分块对应的 $C(2,3)$ 为 5,则 $r = 5$,表示第 5 组秘密信息嵌入到载体图像的 $(2,3)$ 分块中. 运用 LSB 替换算法将秘密信息及备份信息嵌入到载体图像中像素的低位中,可得到载密图像. 具体的嵌入步骤如下:

Step 1: 计算出嵌入份数 N ,通过 N 的值确定拉丁方阵的阶数 n ;

Step 2: 把载体图像分为大小相同的 $n \times n$ 个块,按 2.2 节的规则选择拉丁方阵模板;

Step 3: 将秘密图像转化成二进制比特串,利用混沌加密算法对二进制秘密信息进行混沌加密得到 W ,然后将加密后的秘密信息平均分成 n 组,分别为 $S_1, S_2, \dots, S_n$,根据拉丁方阵和分组数据信息生成密钥 key .

Step 4: 将 i 组秘密信息 S_i ,用 LSB 替换算法和相同的顺序,将秘密隐藏在拉丁方阵元素值为 i 的对应载体图像块中,实现信息隐藏.

2.4 提取算法

秘密信息的提取过程就是信息嵌入的逆过程. 接收方收到载密图像和密钥 key 后,首先根据密钥 key 中得到隐藏时使用的拉丁方阵和加密信息. 依次提取秘密信息 $S_i (i = 1, 2, \dots, n)$,根据式(3)首先计算满足条件 $C(i, j) = t$ 对应的载密图像块 $I'_{t_1}, I'_{t_2}, \dots, I'_{t_n} (t_r \in \{1, 2, \dots, n\}, r = 1, 2, \dots, n)$,然后从 I'_{t_1} 开始依次提取对应像素隐藏的秘密信息,如果像素在 I'_{t_r} 被破坏,则在 $I'_{t_{r+1}}$ 中对应的位置提取,如果没有被破坏则提取隐藏信息,对下一个像素进行处理,若所有的块都被破坏,则对其进行标记. 这样可提取所有的秘密信息 $S_1, S_2, \dots, S_n$,根据加密信息对其解密可得到隐藏信息. 具体步骤如下:

Step 1: 根据 key 可得拉丁方阵模板的阶数 n 和隐藏模板,将载密图像分为 $n \times n$ 个大小相同的块;

Step 2: 依次提取秘密信息 $S_i (i = 1, 2, \dots, n)$,并对不能恢复的像素进行标记;

Step 3: 用密钥 key 对得到的秘密信息分组中的二进制比特串解密,然后根据分组的编号合成原始的秘密信息.

3 实验结果与分析

为验证本文算法的抗剪切性能,进行了大量实验都取得较好的效果. 限于篇幅,本文以 512×512 的 baboon 图作为载体图像,如图 3(a) 所示, 64×64 的 Lena 图作为秘密图像,如图 3(b) 所示,进行

说明. 设 h 的值为 1, 用载体图像像素的最低位来隐藏, 则隐藏容量的 $C = 262\ 144$, 秘密信息大小为 $S = 327\ 68$. 则根据式(1) 计算出 $N = 8$, 从而确定 $n = 8$, 用如图 2 所示的 8 阶拉丁方阵作为嵌入模板, 实现隐藏后得到载密图像如图 3(c) 所示. 用不同的剪切方式对得到的载密图像进行剪切, 并应用本文提取算法在剪切后的载密图像中提取秘密图像. 对得到的载密图像采用检测正确率 $BCR^{[14]}$ 进行质量评估, 其定义如下:

$$BCR(W, W') = \left[1 - \frac{\sum_{i=1}^{L_w} (w_i \oplus w'_i)}{L_w} \right] \times 100\% \quad (4)$$

式中, W 和 W' 分别为原始秘密信息和提取出秘密信息, L_w 为隐藏图像大小. 检测正确率等于提取秘密信息的正确比特数与嵌入秘密信息的总比特数的比值, BCR 越接近 1, 提取秘密信息的正确率越高, 算法的抗剪切性就越好. 实验结果如图 4 所示, 从图中可以看出本文算法的 BCR 较高, 取得了较好的效果.



图3 载体图像、秘密图像和载密图像

4 结束语

本算法根据空域图像上信息隐藏算法的特点, 结合拉丁方阵的特性, 提出了一种抗剪切的信息隐藏算法. 通过载体图像的隐藏容量和秘密信息的大小, 计算出嵌入秘密信息的备份数, 选取合适的拉丁方阵维数, 并从中选取抗剪切的拉丁方阵作为嵌入模板, 根据嵌入模板将多个秘密信息备份嵌入到载体图像中. 实验结果表明该算法能够抵抗多种大面积的剪切攻击, 具有较好的应用价值.

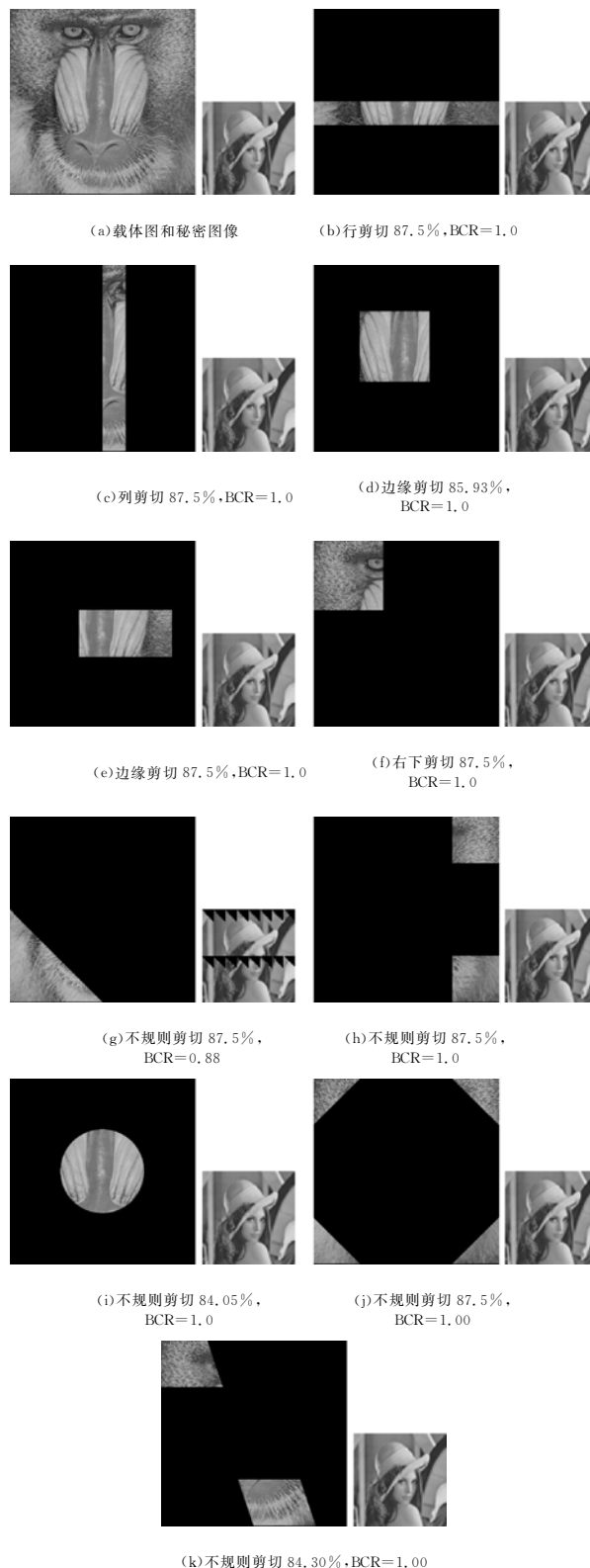


图4 算法的剪切攻击鲁棒性测试

参考文献:

- [1] van Schyndel R G, Tirkel A Z, Osborne C F. A digital watermark[C] // Image Processing, 1994. ICIP-94. Auscin, Texas: IEEE, 1994: 86-90.

- [2] Wolfgang R B, Delp E J. A watermark for digital images[C] // Image Processing, 1996. Onlando: IEEE, 1996: 219-222.
- [3] 谢建全, 阳春华. 一种大容量的自适应信息隐藏方法[J]. 计算机应用, 2007, 27(5): 1035-1037.
- [4] 赵玉霞, 康宝生. 基于混沌序列的抗剪切变换攻击数字图像隐藏新算法[J]. 计算机应用与软件, 2010, 27(3): 100-103.
- [5] 赵培东, 谢剑英. 基于坐标系复原的抗任意剪切盲水印算法[J]. 计算机工程, 2008, 34(6): 134-136.
- [6] 周翔翔, 尹忠海, 王欣, 等. 基于结构化编码的抗剪切图像数字水印[J]. 计算机应用, 2009, 29(5): 1324-1326.
- [7] 彭波, 王平. 抗剪切鲁棒图像数字水印的研究与实现[J]. 中国农业大学学报, 2006, 11(4): 105-108.
- [8] 王丽, 赵媛媛, 赵耀. 一种抗剪切的鲁棒数字水印[J]. 数据采集与处理, 2006, 21(3): 330-333.
- [9] 朱莉莉, 侯迎坤, 陈涛. 抗大面积剪切的小波变换域图像水印算法[J]. 泰山学院学报, 2010, 32(5): 34-39.
- [10] 赵玉霞. 基于混沌系统与提升小波的抗剪切攻击的彩色图像盲水印算法[J]. 工程图学学报, 2010(4): 81-85.
- [11] Kutter M, Bhattacharjee S K, Ebrhimi T. Towards second generation watermarking schemes[C] // ICIP'99. Kobe, Japan: IEEE, 1999: 320-323.
- [12] 韩亚丹, 闰德勤. 一种基于特征的抗剪裁盲水印算法[J]. 中国图象图形学报, 2007, 12(4): 574-580.
- [13] 同鸣, 闫涛, 姬红兵. 一种抵抗强剪切攻击的鲁棒性数字水印算法[J]. 西安电子科技大学学报, 2009(1): 22-27.
- [14] Areef T E, Heniedy H S, Ouda Mansour O M. Optimal transform domain watermark embedding via genetic algorithms[C] // Information and Communications Technology, 2005. Cariro: IEEE, 2005: 607-617.

作者简介:

雷 芸 (1979-), 讲师, 研究方向为教育技术、图像处理.

(上接第 131 页)

参考文献:

- [1] 梁科, 李国峰, 王锦, 等. 通用多通道高性能 DMA 控制器设计[J]. 天津大学学报, 2008, 41(5): 621-626.
- [2] 颜建峰, 吴宁. 基于 PCI 总线的 DMA 高速数据传输系统[J]. 电子科技大学学报, 2007, 36(5): 858-861.
- [3] 史昕蕾, 杨军, 陆生礼. 嵌入式 SOC 中的 DMA 控制器的设计与优化[J]. 电子工程师, 2004(1): 5-7.
- [4] 谭震, 钱晓东, 马瑜兰. 12 位 A/D 转换器与 PC 机 DMA 接口的简化设计[J]. 测控技术, 1997(6): 54-56.

- [5] 王首义, 徐艳. 在 Windows NT 下开发高速 DMA 数据采集程序[J]. 信息技术, 2001(1): 59-61.

作者简介:

赵 强 男, (1988-), 硕士研究生. 研究方向为软件工程设计集成电路设计方向.

陈 岚 女, (1968-), 研究员, 博士生导师. 研究方向为移动物联网系统架构及核心芯片、纳米芯片可制造性设计方法(DFM)、SoC/IP 核验证、评测、低功耗设计技术.