

文章编号:1001-5078(2007)04-0386-03

一种基于 Arnold 置乱和离散余弦变换的信息隐藏算法

郭国文

(浙江万里学院,浙江 宁波 315101)

摘要:介绍了基于 Arnold 置乱变换和离散余弦变换(DCT)的图像信息隐藏算法。首先对秘密图像进行 Arnold 置乱变换,形成秘密信息,然后对载体图像进行 DCT 变换,秘密信息通过量化处理嵌入到 DCT 域中。从试验结果来看,该算法在一定程度上满足了信息隐藏的鲁棒性要求。

关键词:Arnold 置乱变换;离散余弦变换;信息隐藏

中图分类号:TN918.7⁺⁴ **文献标识码:**A

An Information Hiding Algorithm Based on Arnold Transform and Discrete Cosine Transform

GUO Guo-wen

(Zhejiang Wanli University, Ningbo 315101, China)

Abstract: In the paper, a data-hiding algorithm in image based on Arnold transformation and discrete cosine transform (DCT) is introduced. First Arnold transformation is used for secret image, then DCT transformation is used for original image and hiding bit is embedded in DCT by quantizing process. From the result of the experiment, this algorithm meets with the requirement of the information hiding robustness to a certain extent.

Key words: Arnold transformation; discrete cosine transform; information hiding

1 引言

基于图像的信息隐藏技术就是利用人眼对数字图像的感觉冗余,将信息隐藏在载体图像中,达到秘密信息伪装通信的目的。信息隐藏方法分为基于空间域的隐藏和基于变换域的隐藏。空间域算法以 LSB(最低有效位)为主,就是将信息嵌入到数字图像的某些像素位,具有算法简单、嵌入容量大、不可见性好和提取信息时不需要载体图像等优点,但 LSB 算法的安全性不好,鲁棒性较差。变换域算法则是对公开的载体信息做正交变换后,将秘密信息嵌入到隐蔽的频域中,因此具有较强的鲁棒性^[1],如 DCT(离散余弦变换)、DWT(小波变换)等,是目前应用很广泛的算法。

随着信息隐藏分析技术的不断发展,对信息隐藏算法的性能要求也越来越高。如果单纯使用各种信息隐藏算法对秘密信息进行隐藏,那么攻击者只要利用现有的各种信息提取算法对截获的信息进行穷举

运算的话,就很可能提取出秘密信息。对于以图像为载体的信息隐藏来说,置乱变换是一种有效的预处理方法。通过对秘密信息进行置乱运算,有效地打乱明文的次序,使其失去原有的面目,从而掩盖明文的统计特性,有效地抵抗统计分析。然后再将置乱后的结果进行隐藏,就可以极大地提高信息隐藏的安全性。

本文先对秘密图像进行 Arnold 置乱变换,对载体图像进行 DCT 变换,然后通过对变换后的 DCT 系数进行量化完成信息的隐藏。最后对新的 DCT 系数进行反变换,最终得到载密图像。

2 Arnold 置乱变换

图像置乱起源于密码学早期所使用的一些密码算法,功能是将图像中像素的位置重新排列,将原始图像变成一个杂乱无章的新图像,如果不知道所

作者简介:郭国文(1974-),男,讲师,主要研究方向为数字图像处理及人工智能。E-mail:ggwen2000@163.com

收稿日期:2006-09-07

使用的置乱算法,很难恢复出原始图像。

Arnold 变换是 V. J. Arnold 在遍历理论的研究中提出的一种变换,依据所选择的相位空间的不同可分为二维、三维、四维直至 N 维的 Arnold 变换。这里采用的是二维 Arnold 变换:设有平面点集 $S = [0,1][1,0], (x,y) \in S$,点集 S 在计算机屏幕上表现为单位正方形上离散像素组成的矩阵,则 $P_{xy}^n \in S$, $P_{xy}^n = (x,y)^T$,如果像素的坐标 $x,y \in \{1,2,3,\dots,N-1\}$,那么上述变换转化为:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N}$$

式中, $(x,y), (x',y')$ 分别表示像素在图像矩阵中变换前后的坐标,记变换中的矩阵为 A ,反复进行这一变换,则有迭代公式: $P_{xy}^{n+1} = AP \pmod{N}, n = 0, 1, 2, 3, \dots, N-1$ 。

变换运算遍历图像所有像素后,将坐标 (x,y) 对应的像素信息映射到新坐标 (x',y') ,对一幅数字图像迭代地使用 Arnold 变换,即将上一次变换的输出作为下一次的输入,重复几次即可使信息变得杂乱无章,从而达到置乱的目的。图 1 是对一副 128×128 的灰度图像进行 Arnold 变换的效果图。

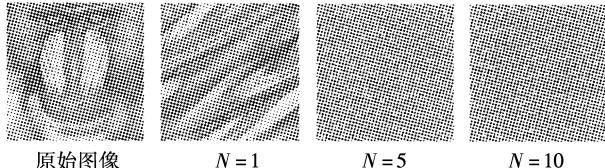


图 1 数字图像的 Arnold 变换位置置乱(N 表示变换次数)

由于离散数字图像是有限点集,对图像反复进行 Arnold 变换,迭代到一定步数时,必然会恢复原图,即 Arnold 变换具有周期性。F. J. Dyson 和 H. Falk 给出了对于任意 $N > 2$, Arnold 变换的周期 $T_N \leq N^2/2$ 的结论^[2]。

3 秘密信息隐藏方法

二维 DCT 变换是静态图像压缩(JPEG)算法的核心。因此,在 DCT 域中的信息隐藏可以有效地抵抗 JPEG 有损压缩^[3]。

根据图像数据频域特性,低频系数反映了整个图像的基本色调和基本细节。高频部分代表了图像中的噪声部分,这部分数据很容易通过有损压缩和滤波被处理掉。当前,对于 DCT 域系数的选择主要有 Cox 算法^[4]和 Piva 算法^[5]两种。Cox 算法是对 DCT 的低频系数进行修改,而 Piva 算法是对连续的 DCT 的中频系数进行修改,两者在性能上各有优点,算法比较见文献[6]。由于 JPEG 压缩会舍弃高频系数,同时经过置乱变换后的秘密图像均匀性比较好,所以本算法直接将数据隐藏在 DCT 的低频和中频区域。

输入:载体图像 I,其大小为 $m \times n$,秘密图像 W

输出:隐藏图像 I_m

步骤 1:对秘密图像 W 进行多次 Arnold 置乱变换,产生变换后的图像 W_m ;

步骤 2:将待隐藏的图像 W_m 转化为由 0,1 组成的二进制串 $S, S = \{s_1, s_2, \dots, s_n\}$;其中, n 为二进制串 S 的长度;

步骤 3:将图像 I 按从左到右,从上到下的顺序分割成一系列不重叠的 8×8 子块,对每个子块进行 DCT 变换,按 zigzag 顺序抽取 DCT 域的低频和中频系数,这里取 AC 系数中的前 32 个系数,记为 F_1, F_2, \dots, F_{32} ;

步骤 4:根据 JPEG 标准推荐量化矩阵对 F_1, F_2, \dots, F_{32} 进行信息隐藏。设这 32 个系数对应的量化步长分别为 q_1, q_2, \dots, q_{32} ,对 DCT 系数 F_i (F_i 为实数),根据量化步长 q_i (q_i 为正整数)可以确定它所在的区域 $[N \times q_i(N+1) \times q_i], N = \dots, -2, -1, 0, 1, 2, \dots$;

步骤 5:设要隐藏的数据为 s_i, s_i 取值为 0 或 1,如果 s_i 为 0,则 F_i 的量化值 Q_i 取 N 和 $N+1$ 两者中的偶数;如果 s_i 为 1,则 F_i 的量化值 Q_i 取 N 和 $N+1$ 两者中的奇数;

步骤 6:逐块对载体图像子块 DCT 系数进行上述处理。

步骤 7:进行载体图像子块 DCT 系数的反变换,或进行 JPEG 压缩处理,得到隐藏图像 I_m 。

秘密信息的提取,只需要知道信息嵌入的位置和量化表,即可从公开图像中提取处理,然后根据相应的置乱算法即可恢复。

4 实验结果

4.1 基本实验

以 512×512 的标准灰度图像 Lena 作为载体,秘密信息选取 128×128 的标准 Baboon 图像。将 Baboon 图像进行 10 次 Arnold 置乱变换后的图像(如图 1 所示)进行隐藏,产生未压缩的 BMP 图像,如图 2 所示。通过对变换前后的图片进行比较,从主观视觉上很难感觉到明显的差异。

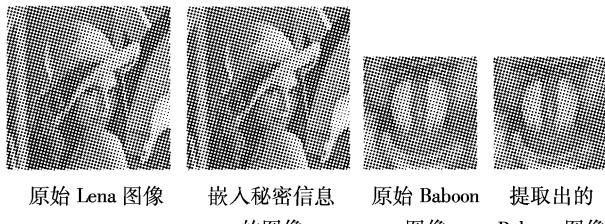


图 2 图像变换结果

4.2 鲁棒性实验

对 Arnold 置乱变换后的 Baboon 图像进行嵌入,

进行JPEG压缩处理,在不同的压缩比时提取出的Baboon图像如图3所示,PSNR(峰值信噪比)如表1所示。一般来说,PSNR低于36dB将使人眼明显察觉出图像的改动,表1中的PSNR在不同压缩率下始终保持在40dB以上,说明秘密图像具有良好的视觉效果。从表中可以看出,随着压缩比的增大,图像的PSNR逐渐减小,这是由于DCT量化时将数据主要隐藏在AC系数的中、低频上,压缩时将部分中频的系数进行了压缩的结果。

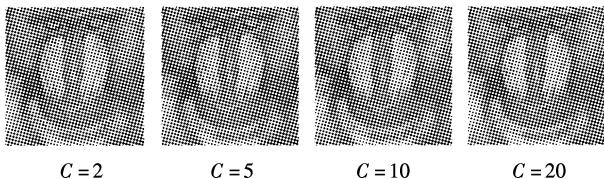


图3 不同压缩比时提取的Baboon图像(C 表示压缩比)

表1 不同压缩比时提取的Baboon图像PSNR值

压缩比	2	5	10	20
PSNR/dB	50.36	48.65	46.85	40.62

5 小结

本文提出了一种基于Arnold置乱变换的DCT域信息隐藏方法。表明Arnold置乱变换可以作为信息隐藏的预处理,利用DCT变换的中、低频系数,

(上接第385页)

大的彩色值; T_{\min} 为编码曲线中第 i 段最小的彩色值; f_{\max} 为 ω_i 中最大的灰度值; f_{\min} 为 ω_i 中最小的灰度值。

实验结果如图2所示。图2(a)为原始红外灰度图像,该图为电灯,图2(b)为直接采用伪彩色编码图像,图2(c)为采用本文算法增强后的红外伪彩色图像。对比图2(a)、(b)可知,经聚类伪彩色增强后获得的图像,能用对应的伪彩色编码段较好地显示各红外辐射温度场的分布,清晰地反映出温度变化的层次,对在灰度图中无法观察的灯罩及管线都有很好的增强效果,能突出细节,具有较高的分辨率。同时,本文算法提高了聚类效率和聚类后图像的效果,并获得了具有良好视觉特性的红外伪彩色图像。

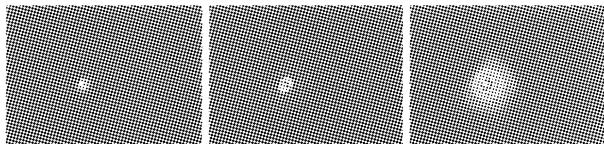


图2 不同伪彩色增强算法处理后的图像

5 结论

本文根据红外图像的特点,提出了一种新的基

将秘密信息隐藏其中,能充分满足信息的不可见性和鲁棒性。

从总体上看,本算法具有一定的实用价值,但问题依然存在,DCT系数在反变换时可能对隐藏的数据产生了干扰,可以通过对嵌入算法的改进来提高信息抗攻击性;同时,JPEG压缩过程中的对秘密信息的破坏也是一个需要考虑的问题。

参考文献:

- [1] 余鹏飞,刘兵. 基于离散余弦变换的大容量信息隐藏盲提取算法[J]. 计算机应用,2006,26(4):815-817.
- [2] 丁伟,闫伟齐,齐东旭. 基于Arnold变换的数字图像置乱技术[J]. 计算机辅助设计与图形学学报,2001,13(4):338-341.
- [3] 钮心忻. 信息隐藏与数字水印[M]. 北京:北京邮电大学出版社,2004:88.
- [4] Cox I J, KiLian J, Leighton T, Shamom. Secure spread spectrum watermarking for multimedia[J]. IEEE transaction on image processing, 1997, 6(12):1673-1687.
- [5] A Piva, M Bami, F Bartolini. A DCT-based watermark recovering without resorting to the uncorrupted original image[C]. IEEE Inc. Conf. Image Processing, 1999, 6:239-246.
- [6] 孟兵,周良柱,万建伟,等. 两种基于DCT变换的数字水印算法[J]. 国防科技大学学报,1999,6:75-79.

于聚类的伪彩色增强方法。该伪彩色增强处理技术,改进了K-均值聚类算法,优化了聚类初始中心的选取方法,降低了参与迭代算法过程的运算量,提高了运算效率;在灰度聚类的基础上,通过结合节点分段伪彩色增强的方法,明显增强了红外图像中温度场的区域分布,丰富了红外图像的细节信息和层次感,具有更好的视觉效果。

参考文献:

- [1] 张丽,陈志强,康克军,等. 伪彩色的非线性分配方法在大型集装箱检测系统图像处理中的应用[J]. 核电子学与探测技术,2000,20(2):157-161.
- [2] 刘缠牢,谭立勋,李春燕,等. 红外图像伪彩色编码和处理[J]. 应用光学,2006,27(5):419-422.
- [3] 姚敏,等. 数字图像处理[M]. 北京:机械工业出版社,2006:131-135.
- [4] 柳超龙,王江安,江传富. 舰船热轨迹红外图像增强研究[J]. 激光与红外,2006,36(5):413-416.
- [5] 何斌,马天予,王运坚,等. Visual C++数字图像处理[M]. 北京:人民邮电出版社,2002:309-325.
- [6] Kanungo T, Mount D M, Netanyahu N S. An efficient K-means clustering algorithm: analysis and implementation [J]. IEEE trans. PAMI, 2002, 24(7):881-892.