半空间混合图像置乱方法

李 涛[1,2], 田 岩[3], 张 剑[1], 刘阿军[3]

(1. 湖南科技大学 信息与电气工程学院, 湖南 湘潭 411201; 2. 华中科技大学 图像识别与人工智能研究所, 湖北 武汉 430074; 3. 华中科技大学 电子与信息工程系, 湖北 武汉 430074)

摘 要: 考虑到变换域置乱的鲁棒性和混沌序列对初值敏感、遍历性及随机性等特点,提出一种基于 DCT 变换域的半空间图像置乱方法,先对图像的第一个变量进行一维 DCT 变换。在此基础上对 DCT 系数用混沌序列进行调制,将调制结果进行 DCT 反变换;进而对图像的第二变量进行一维 DCT 变换,采用与第一变量相同的方法得到最终的置乱结果。算法简单可行,置乱效果好。实验证明该方法具有一定的抗攻击能力。

关键词: 信息隐藏; 图像置乱; DCT 变换; 混沌序列

中图法分类号: TP309.2; TP391 **文献标识码**: A **文章编号**: 1001-3695(2006)03-0172-03

A Scrambling Scheme of Image Based on Semi-space Domain

LI Tao[1,2], TIAN Yan[3], ZHANG Jian[1], LIU A-jun[3]

(1. *School of Information & Electrical Engineering, Hunan University of Science & Technology, Xiangtan Hunan* 411201, *China*; 2. *Institute for Pattern Recognition & Artificial Intelligence, Huazhong University of Science & Technology, Wuhan Hubei* 430074, *China*; 3. *Dept. of Electronic & Information Engineering, Huazhong University of Science & Technology, Wuhan Hubei* 430074, *China*)

Abstract: Due to the good properties of chaotic sequences including their sensitive dependence on initial value, pseudorandom, ergodic, an image scrambling method, called semi-space domain, based on two times 1-D DCT and chaos maps is presented in this paper. The procedure of the algorithm is mainly divided into two steps: first, an original image is decomposed for its first variable by 1-D DCT, then by chaos system, a scrambling result is achieved. After by inverse 1-D DCT for the scrambling result, repeating the same procedure for the second variable, the final scrambling result is obtained. At the last part of this paper, the experimental studies are carried out on certain standard test images. The experimental results show that the new method is effectiveness.

Key words: Information Hiding; Image Scrambling; DCT (Discrete Cosine Transformation); Chaotic Sequence

以 Internet 为代表的计算机网络的飞速发展,使人们在享受信息社会带来好处的同时,信息安全的保障日益凸显为一个不容忽视的问题。由于传感器的发展,人们可以方便地获取不同时相、不同波段、不同分辨率的图像。所以,图像成为信息传输的一种不可缺少的方式。因此,图像加密成为近几年的一个研究热点,而图像置乱技术是图像加密的常用手段之一,它既可作为一种图像加密的方法,也可作为数字水印的预处理技术,其研究方兴未艾。图像置乱的目的是通过某种变换,使生成的图像杂乱无章、无法辨认,由此便可以保护图像的真实内容。

在对图像置乱的研究中,目前已有一些方法,如 Arnold 变换、FASS 曲线、Gray 代码、分形方法、幻方方法、生命模型等[1,2],已广泛应用于数字图像信息安全领域。由于混沌具有对初值有极其敏感的依赖性、遍历性和随机性等特点,因而在信息置乱中被广为应用[3~5]。Shi 和 Bhargava 提出一种参数化的二维混沌方法在空域中对图像的各像素进行迭代重排来加密[5]。孙鑫等人利用混沌映射构造了空间域的置换矩阵和色度域的加密矩阵对图像进行置乱[6]。但是近几年的研究发现,多步非线性预测方法可破译混沌掩盖与混沌调制的加密方案[7]。为增强混沌系统的加密性能,可通过提高混沌系统的维数或和其他加密方法相结合的方法来实现。

收稿日期: 2005-01-23; 修返日期: 2005-04-18

图像置乱可在图像的空间域和频域中进行。通常,基于变换域的方法较之于空域的方法具有更强的鲁棒性,这是因为图像的位置空间和色彩空间具有一定的规律性,截获者有可能通过统计分析的方法进行破译。但图像的频率空间则不一样: ①它具有相当的稳健性,在 DCT 变换域中进行图像隐藏不仅可以抵抗刻意或无意因噪声的加入而带来的影响; ②由于变换域的复杂程度可给破译者带来更大难度; ③DCT 变换域算法独立于图像的格式; ④在变换域中的每一点变换都有可能对整个图像数据集合产生影响,因而其置乱效果好。但基于 2-D 变换域的方法,算法复杂度较高,为此,本文提出一种在半空域的 DCT 变换中进行混沌置乱。其基本过程为先对图像的第一个变量进行一维的 DCT 变换,变换后的系数用混沌序列进行调制,续而再对另一个变量实施一维的 DCT 变换,采用同样的方法进行调制,再反变换后生成置乱后的图像。本文方法具有较小的计算量,同时仿真实验显示算法是行之有效的。

1 DCT 变换

离散余弦变换(Discrete Cosine Transform, DCT)是利用傅里叶变换的对称性,采用图像边界褶翻操作将图像变换为偶函数的形式后,对之施以二维离散傅氏变换后的结果只包含余弦项,故称之为离散余弦变换。DCT 可以将图像描述成为不同幅值和频率的正弦值之和的形式[8]。

设图像 A 为一个 $M \times N$ 的矩阵, $f(x, y)$ 是在图像的 (x, y) 处的灰度值, 这里 $x = 1, \cdots, M$, $y = 1, \cdots, N$, $C(u, v)$ 为图像在 (u, v) 的 DCT 系数, 相应的二维离散余弦变换公式为

$$D(u, v) = a(u)\, a(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \cos \frac{(2x+1)u\pi}{2N} \cos \frac{(2y+1)v\pi}{2N}$$

$$u = 0, 1, \cdots, M-1$$

$$v = 0, 1, \cdots, N-1$$

$$a(u) = \begin{cases} 1/M & \text{当 } u = 0 \\ 2/M & \text{当 } u = 1, 2, \cdots, M-1 \end{cases}$$

$$a(v) = \begin{cases} 1/N & \text{当 } v = 0 \\ 2/N & \text{当 } v = 1, 2, \cdots, N-1 \end{cases}$$

因为 DFT 和 DCT 是一本之源, 故二维离散余弦变换也同样具有分离性质, 即 2-D 的 DCT 可由连续两次运用 1-D 的 DCT 变换来实现:

$$D(u, y) = a(u) \sum_{x=0}^{M-1} f(x, y) \cos \frac{(2x+1)u\pi}{2M} \quad u = 0, 1, \cdots, M-1$$

$$D(u, v) = a(v) \sum_{y=0}^{N-1} C(u, y) \cos \frac{(2y+1)v\pi}{2N} \quad v = 0, 1, \cdots, N-1$$

DCT 反变换:

$$f(x, y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} a(u)\, a(v)\, D(u, v) \cos \frac{(2x+1)u\pi}{2N} \cos \frac{(2y+1)v\pi}{2N}$$

$$x = 0, 1, \cdots, M-1$$

$$y = 0, 1, \cdots, N-1$$

另外, 当图像 A 为一个 $M \times M$ 的方阵, 在 DCT 实现时, 其变换计算有快速的方法。此时变换矩阵 T 由下式给出:

$$T_{u,v} = \begin{cases} 1/M & \text{当 } u = 0, 0 \le v \le M-1 \\ 2/M \cos \dfrac{\pi(2v+1)u}{2M} & \text{当 } 1 \le u \le M-1, 0 \le v \le M-1 \end{cases}$$

已有学者证明[8], T 是一个实标准正交矩阵, 那么, $T \times A$ 也是一个 $M \times M$ 的方阵, 它即是 A 的一维 DCT 列变换, $B = T \times A \times T'$ 即是 A 的二维 DCT 变换。而 B 的逆变换可以用 $T' \times B \times T$ 得到, 这时候比直接用公式进行变换用时要少。

2　混沌系统

混沌现象是在非线性动力系统中出现的确定性的、类随机的过程。这种过程即非周期又不收敛, 尽管混沌动力系统具有确定性, 但其具有形式简单, 对初始值及其敏感, 具备白噪声的统计特性[6]。

一个一维的动力学系统定义式为 $x_{k+1} = \mu F(x_k)$, 其中 μ 为系统参数, $x_k \in V(k = 0, 1, 2, \cdots)$ 称为状态, 非线性映射 $F: V \to V$, $V < R$ 将当前状态 x_k 映射为下一个状态 x_{k+1}。

Logistic 映射是一类简单而且应用广泛的动力系统, 其定义: $x_{k+1} = u x_k (1 - x_k)$, 其中 $0 \le \mu \le 4$ 为系统参数, $x_k \in (0, 1)$。当 $3.569\,945\cdots < \mu \le 4$ 时, 系统处于混沌状态。

如果设定一个初值 x_0, 反复利用动力学系统定义式, 可得到一个混沌序列 $\{x_k: k = 0, 1, 2, \cdots\}$。用混沌序列去调制图像像素值, 便可实现图像加密。不同的混沌系统产生的随机序列是不相同的; 同一系统, 参数不同, 其混沌特性也不相同; 同系统同参数, 初值不同, 随机序列也会不同。由于混沌序列具有的这些性质使得它在用于图像加密时具有良好的随机性、较高的复杂性和较强的保密性。

3　基于 DCT 的半空间置乱算法

图像置乱就是将图像中像素的位置或者像素的颜色 “打乱”, 将原始图像变换成一个杂乱无章的新图像, 也就是说使原图像变得面目全非。利用 DCT 变换及前文中提到的混沌系统, 本文提出基于 DCT 变换的半空间置乱算法。这里的置乱是分别通过对图像变换后的第一个变量和第二个变量在半频半空域进行, 故称之为半空间置乱。其优点是不仅具有频域置乱的优点, 同时由于仅对某一变量进行变换, 因此算法的复杂度较低。下面对本算法进行详细说明。

这里先给出本文算法的流程框图(图 1)。算法描述如下:

(1) 对图像 $f(x, y)$ 进行一维的 DCT 变换, 即先对变量 x 进行 DCT 变换

$$D(u, y) = a(u) \sum_{x=0}^{N-1} f(x, y) \cos \frac{(2x+1)u\pi}{2N} \quad u = 0, 1, \cdots, N-1$$

$$a(u) = \begin{cases} 1/N & \text{当 } u = 0 \\ 2/N & \text{当 } u = 1, 2, \cdots, N-1 \end{cases}$$

(2) 对 $D(u, y)$ 的系数矩阵进行混沌调制, 得到 $S'(u, y)$

(3) 对置乱后的系数 $S'(u, y)$ 进行 DCT 反变换

$$f'(x, y) = \sum_{u=0}^{N-1} a(u)\, S'(u, y) \cos \frac{(2x+1)u\pi}{2N} \quad x = 0, 1, \cdots, N-1$$

(4) 对 $f'(x, y)$ 在空域中作简单的位置转换后对 y 变量进行一维 DCT 变换

$$D'(x, v) = a(v) \sum_{y=0}^{N-1} f'(x, y) \cos \frac{(2x+1)v\pi}{2N} \quad v = 0, 1, \cdots, N-1$$

(5) 对变换后的系数矩阵 $D'(x, v)$ 进行混沌调制, 得到 $S''(x, v)$

(6) 对第二次的置乱系数 $S''(x, v)$ 进行 DCT 反变换得到希望的置乱图像 $f_s(x, y)$

$$f_s(x, y) = \sum_{v=0}^{N-1} a(v)\, C''(x, v) \cos \frac{(2x+1)v\pi}{2N} \quad y = 0, 1, \cdots, N-1$$

至此置乱完成。

(7) 重复(1) ~(6), 即为下一轮的置乱。

将置乱后图像按上面的步骤进行一个逆过程处理即可得到原图像。

4　实验结果与分析

本文采用 Cameraman 作为测试图分别进行置乱实验和攻击测试实验。这里, 混沌系统的初值 $x_0 = 0.1$, 其结果分别如下:

(1) 置乱结果如图 2 所示, 从图 2(b) 中我们可以看到, 仅对 x 变量变换后进行混沌调制时, 图像已经变得乱七八糟, 不能辨识, 已得到比较好的置乱效果。而整个置乱过程结束后的结果(图 2(c)) 更加不可辨识。

(2) 对于稳健性的检验, 这里给出剪切、旋转、加噪和压缩等攻击性测试。

①对置乱后的图像进行大面积剪切后进行恢复实验结果如图 3 所示。

②对置乱后的图像进行有损压缩, 此处采用 DCT 压缩, 即将置乱图像分成 8 ×8 的图像块, 进行 DCT 变换后, 只保留 64 个系数中的 10 个, 并对此剩余的 10 个系数作逆变换。其实验结果如图 4 所示, 可以看到图中的摄像师仍是可见的。


(a)原图


(b)对 x 变量的 DCT 变换后的置乱结果

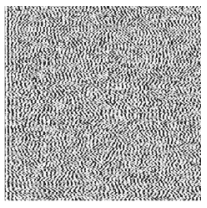
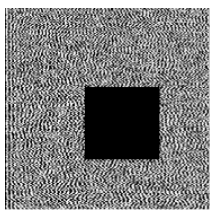

(c)对 y 变量的 DCT 变换后的置乱图

图 2 本文方法的置乱结果


(a)剪切图


(b)剪切后的恢复图

图 3 剪切试验结果

③对置乱后的图像施加不同的噪声,由于篇幅所限只给出方差为 20 的白噪声污染的恢复图,结果如图 5 所示。

④对置乱后的图像用巴特沃斯(Butterworth)低通滤波器进行滤波后,进行恢复的图如图 6 所示。


图 4 有损压缩后的恢复图


图 5 加噪后的恢复图


图 6 低通滤波后的恢复图

从实验结果可以看到,置乱的图像分别受上述几种常见方法的攻击后原始图像在一定程度上仍能得以恢复。

5 结论

本文讨论了基于 DCT 变换的半空间图像置乱算法,该算法简单可行,置乱效果好,对一些常见的攻击方法,本文的算法有一定的鲁棒性。由于图像为方阵,可以采用快速的 DCT 算法,因而运算速度快。对于图像不是方阵时,可以采用简单的方法进行处理,比如采用边界填充的形式如边界复制、边界循环、边界对称以及简单的插值方法等。另外由于对图像实施的是一维变换,计算量比进行二维变换要少。其逆变换也简单,从而使恢复过程无须迭代。进一步的研究可考虑与其他的空域置换方法相结合来提高其鲁棒性。

参考文献:

[1] X Qi, Zou Jiangcheng, Han Xiaoyou. A New Class of Scrambling Transformation and Its Application in the Image Information Covering [J]. Sciences in China, Ser. E, 2000, 43(3): 304-312.

[2] C W Wu, Rul'kov N F. Studying Chaos Via 1-D Maps: A Tutorial [J]. IEEE Trans. on Circuits and Systems: Fundamental Theory and Applications, 1993, 40(10): 707-721.

[3] Kohda T. Information Sources Using Chaotic Dynamics[J]. Proceedings of the IEEE, 2002, 90(5): 641-661.

[4] Yeo J C, Guo J I. Efficient Hierarchical Chaotic Image Encryption Algorithm and Its VLSI Realisation [J]. IEE Proceedings on Vision, Image and Signal Processing, 2000, 147(4): 167-175.

[5] C Shi, B Bhargava. Light-weight MPEG Video Encryption Algorithm [C]. Proceedings of the International Conference on Multimidia'98, New Delhi, India, 1998. 55-61.

[6] 孙鑫,易开祥,孙优贤. 基于混沌系统的图像加密算法[J]. 计算机辅助设计与图形学学报, 2002, 14(2): 1-4.

[7] S seshan, *et al*. Handoffs in Cellular Wireless Net-works: The Daedalus Implementation and Experience[J]. Kluwer International Journal on Wireless Personal Communications, 1997, (4) 3: 141-162.

[8] 徐飞,施晓红,等. MATLAB 应用图像处理[M]. 西安:西安电子科技大学出版社, 2003. 70-71.

作者简介:

李涛(1971-),女,讲师,博士研究生,主要研究方向为模式识别、人工智能、图像处理等;田岩(1970-),男,副教授,主要研究方向为模式识别、人工智能、小波分析、图像处理与压缩、机器视觉等;张剑(1974-),讲师,主要研究方向为自动控制、图像处理等;刘阿军,硕士研究生,多媒体技术、图像处理等。