

基于 DCT 量化系数重组的 JPEG 图像加密算法

王方超, 李 斌, 周佳虹
(镇江船艇学院, 江苏 镇江 212000)

摘 要: 整个加密算法分两个过程, 首先在 DCT 变换之前对原始图像进行以 8×8 图像块为单位的统一图像置乱, 使图像整体视觉效果上杂乱无章. 其次, DCT 变换量化系数之后, 将相邻两个 8×8 系数块的低频系数组成一个新块, 高频系数组成一个新块, 分别进行块内的系数置乱, 在改变原始图像频率成分的同时, 可以减少改变零游程结构带来的加密对 JPEG 图像压缩影响, 而且 8×8 系数块内的非零系数个数发生了变化, 可以有效抵御统计非零系数个数攻击.

关键词: JPEG 图像; DCT 量化系数; 系数重组; 置乱加密

中图分类号: TN402

文献标识码: A

文章编号: 1000-7180(2014)08-0139-05

JPEG Image Encryption Algorithm Based on the Recomposition of DCT Quantization Coefficients

WANG Fang-chao, Li Bin, ZHOU Jia-hong

(Zhenjiang Watercraft College, Zhenjiang 212000, China)

Abstract: The whole encryption algorithm includes two steps. Firstly, scramble the original image before the DCT transformation block by block with the size 8×8 ; it makes the image disorderly and unsystematic. Secondly, after the quantization of the DCT coefficients, we recompose the double 8×8 DCT blocks border upon, put low coefficients into one 8×8 block and put the high coefficients into another one. Shuffle the low coefficients block and high coefficients block with different ergodic matrixes. This algorithm could change the frequent structure while increase the compressed image data a little and change the number of the nonzero DCT coefficients so as to defend the nonzero-counting attack.

Key words: JPEG image; DCT quantization coefficients; coefficients recompositon; shuffling encryption

1 引言

当前, 数字图像等多媒体信息在丰富人们生活的同时, 也带来了安全性问题, 对数字图像进行加密处理成为了保护图像信息安全的重要手段之一. 为了降低图像存储的数据量, 提高在现有通信信道容量下的信息传输效率, 需要对图像进行数据压缩, 因此, 对压缩图像的加密显得尤为重要.

现有的图像压缩加密算法概括起来可分为两类. 一类是针对未压缩的原始图像数据, 用算法对像素进行置乱, 以达到加密的目的. 其缺点是, 由于未

考虑压缩编码格式使得原始图像加密后的压缩能力变弱, 影响压缩比^[1-5]; 另一类是针对压缩域的加密, 即对在编码压缩过程中出现的变换域系数(比如 DCT 系数和小波系数等)进行加密处理, 能达到同时压缩和加密的目的, 具有实时性强、压缩质量高等优点^[6-12]. 变换域的加密算法又可分为三种: 第一种是改变系数值的加密方法, 如 AES、DES 和混沌序列等直接对全部系数或者有选择地对低频系数进行加密, 从而起到加密图像的作用^[6]; 第二种是改变变换域系数的值或者变换位置的加密方法, 如 8×8 DCT 系数块内部系数的置乱, 系数块之间相同频

收稿日期: 2013-09-23; **修回日期:** 2013-11-17

基金项目: 国家自然科学基金(61272043, CSTX2013jjB40009)

率段系数之间的置乱^[7-12];第三种是在熵编码过程中加密,比如多个 Huffman 表之间进行选择的加密 Huffman 表的加密方式^[13].第一种加密方法会改变每个系数的值,完全破坏了系数的能量分布和相关性,从而大大降低可压缩性,如果用于有损压缩场合,还会造成解码端即使有密钥也很难恢复出期望达到的图像质量;第二种置乱算法扰乱了变换域系数分布的统计特性,使得 zig-zag 扫描后零游程编码数据量增加,而且如果只进行 8×8 系数块内部系数的置乱,很容易受到统计非零值攻击^[14];第三种加密方法密钥空间不够大,而且很难抵御选择明文攻击^[15].

JPEG 图像格式是十分重要的一种编码格式,本文在 JPEG 编码基础上研究 JPEG 图像的压缩加密方法.先对原始图像进行以 8×8 图像块为单位的统一置乱,达到视觉上杂乱无章的效果;在考虑变换域系数分布统计特性的同时,对变换域系数进行置乱,将不同 8×8 图像块的低频系数重新组合成为一个 8×8 图系数块,高频系数组成另一个 8×8 图像系数块,分别对其进行 8×8 块内部的置乱,然后再重新组合成包含低频、高频系数的 8×8 系数块.该方法较大程度上保持了变换域系数分布的统计特性,压缩编码时数据量增加较少,实验结果表明加密速度比较快,能够抵御统计非零值个数方法的攻击.

2 混沌系统

加密过程中需要用两类遍历矩阵对图像进行置乱加密.一类用来对明文图像进行以 8×8 图像块为单位的统一置乱;另一类用来对图像 DCT 变换量化后的系数重新组合后的 8×8 系数块内的系数进行置乱加密.利用混沌系统产生随机序列,然后对该序列按大小进行排序,根据排序的序号可以产生所需要的遍历矩阵.

利用 Logistic 混沌映射生成第一类遍历矩阵 S_a ,用来对明文图像以 8×8 图像块为单位进行置乱. Logistic 函数如式(1):

$$X_{n+1} = \mu X_n(1 - X_n); 0 \leq X_n \leq 1, 3.57 < \mu < 4 \quad (1)$$

利用 Chen's 系统构造第二类遍历矩阵, Chen's 系统描述如式(2):

$$\begin{cases} \frac{dx}{dt} = a(y - x) \\ \frac{dy}{dt} = (c - a)x - xz + cy \\ \frac{dz}{dt} = xy - bz \end{cases} \quad (2)$$

式中, a, b, c 为系统常参数,若它们取下列值: $a = 35, b = 3, 20 < c < 28.4$ 则系统是混沌的.从式(2)产生的随机序列 $\{x(t)\}, \{y(t)\}$ 和 $\{z(t)\}$ 中任意选择两个随机序列生成遍历矩阵 S_{b1} 用来对重组后的低频系数置乱;生成遍历矩阵 S_{b2} 用来对重组后的低频系数置乱.

3 加密算法

变换域中不同系数值代表着原始图像中不同频率的信息,每一个系数值的变化都会对整个图像产生影响,通过对变换域量化后的系数进行置乱,可以快速地改变图像的视觉效果,把图像变得杂乱无章、无法理解.置乱加密包括原始图像数据的基于 8×8 图像块的统一图像置乱加密和量化后系数的低频、高频系数分别置乱加密两个过程.具体的加密流程如图 1 所示,解密为它的逆过程.

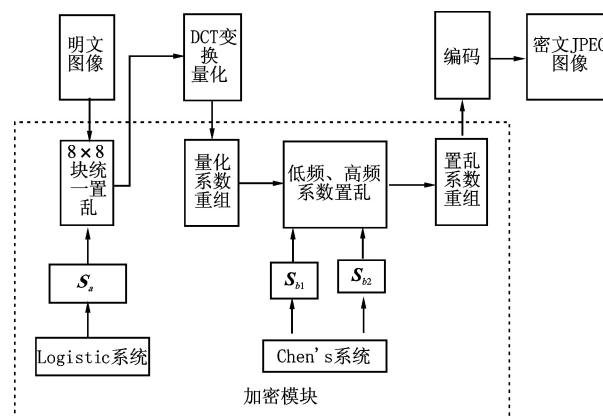


图 1 加密流程图

图中加密模块为算法设计的加密过程,其余模块为 JPEG 压缩编码的标准过程.假设原始图像大小为 $M \times N$,其中, M 表示图像的高度, N 表示图像的宽度,由 Logistic 系统产生的随机序列 $\{X(n)\}$,生成一个大小为 $\frac{M}{8} \times \frac{N}{8}$ 的遍历矩阵 S_a ,再由 Chen's 系统产生三个随机序列 $\{x(t)\}, \{y(t)\}, \{z(t)\}$,选取任意两个随机序列产生 8×8 大小的遍历矩阵 S_{b1}, S_{b2} .原始图像的 DCT 变换和编码是以 8×8 图像块为基本单位,因此对原始明文图像进行 8×8 块的统一置乱不会改变 8×8 图像块内部的像素之间的空间相关性,能够保持后续编码的结构不变性,不会增加加密后压缩图像的数据,而且可以使得图像在视觉上看起来杂乱无章.量化后的 DCT 系数低频部分一般非零值较多,而高频部分为非零值较少,按照 zig-zag 扫描进行游程编码,高频部分的零值系

数对压缩率贡献较大. 如果将两个 8×8 块 DCT 变换后的低频系数重新组合放在一起进行置乱, 高频系数重新组合放在一起进行置乱, 然后再将置乱后的高低频系数组合回 8×8 系数块, 那么对游程编码的影响会较直接对 8×8 DCT 量化后系数块置乱的影响小, 对加密压缩后 JPEG 图像数据量改变不大.

3.1 量化系数重组

DCT 变换和量化后的 8×8 系数块中左上角第一个系数称为零频分量, 越往右下角频率越高, 右下角最后一个系数称为最高频. 用对角线将左上角和右下角进行平均划分, 定义左上角的从左到右, 从上到下的 32 个系数分量为图像的低频分量, 右下角的 32 个系数分量为高频分量. 如图 2 所示.

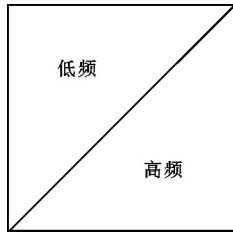


图 2 低频高频划分

在进行系数重组时, 相邻两个 8×8 系数块的低频分量组成一个新的 8×8 系数块, 高频分量组成一个 8×8 系数块, 如图 3 所示.

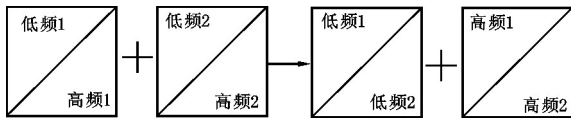


图 3 系数重组

当 8×8 块内部的置乱加密结束后, 再进行反向的系数块重组.

3.2 加密步骤

假设待加密原始图像为 $I_{m \times n}$, 其中, 图像高度为 m , 宽度为 n , 置乱加密算法如下:

(1) 设定 Logistic 系统的参数: $0 \leq X_n \leq 1$, $3.57 < \mu < 4$, 为了保持序列的随机性, 舍去序列开始部分, 分别从序列的第 k_1 ($k_1 > 400$) 个值开始, 连续顺序取 $\frac{m}{8} \times \frac{n}{8}$ 个元素组成子序列 S_1 ; 设定 Chen's 混沌系统的系统参数值: $a = 35, b = 3, 20 < c < 28.4$ 和系统状态初始值: x_0, y_0, z_0 , 利用该系统产生三个随机序列: $\{x_i\}, \{y_i\}, \{z_i\}$, (其中 $i = 0, 1, 2 \dots$), 任意选取其中的两个序列, 为了保持随机序列的随机性, 舍去序列开始的部分, 分别从序列的第 k_2 ($k_2 > 400$)、 k_3 ($k_3 > 400$) 个值开始, 分别顺序选

取 $\frac{m}{2} \times \frac{n}{2}, \frac{m}{2} \times \frac{n}{2}$ 个元素组成两个子序列 S_2, S_3 (参数 $X_0, \mu, c, x_0, y_0, z_0, k_1, k_2, k_3$ 为加解密密钥).

(2) 将子序列 S_1 按照从上到下, 从左到右的顺序重排生成大小为 $\frac{m}{8} \times \frac{n}{8}$ 的矩阵 M_1 ; 将子序列 S_2, S_3 分别分割成大小为 64 的子段 S_{2j} 和 S_{3j} ($j = 0, 1 \dots \frac{m}{128} \times \frac{n}{8}$), 每个子段按照从上到下, 从左到右的顺序重排生成大小为 8×8 的矩阵 M_{2j} 和 M_{3j} ($j = 0, 1 \dots \frac{m}{128} \times \frac{n}{8}$); 以 M_1, M_{2j}, M_{3j} 为基准, 生成大小为 $\frac{m}{8} \times \frac{n}{8}$ 的遍历矩阵 E_1 和大小为 8×8 的遍历矩阵 E_{2j}, E_{3j} ($j = 0, 1 \dots \frac{m}{128} \times \frac{n}{8}$).

(3) 用置乱矩阵 E_1 对原始图像 $I_{m \times n}$ 以 8×8 图像块为基本单位进行统一置乱, 得到置乱后的图像 $I'_{m \times n}$.

(4) 图像 $I'_{m \times n}$ 进行 DCT 变换和量化, 从图像左上角开始, 按照从左到右, 从上到下的顺序, 首先对第 0 个和第 1 个 8×8 量化系数块进行系数块重组, 组成低频系数块 L 和高频系数块 H, 利用置乱矩阵 M_{20} 和 M_{30} 分别对其进行置乱加密, 置乱后再将低频系数块 L 和高频系数块 H 进行反向系数重组.

(5) 对第 $2j$ 和 $2j+1$ (其中, $j \in [1, \frac{m}{128} \times \frac{n}{8}]$) 个 8×8 量化系数块利用 M_{2j} 和 M_{3j} 分别进行步骤 (4) 的操作, 直到所有系数块都加密完成得到加密图像 $I''_{m \times n}$.

4 实验结果分析

在 CPU 为 Intel 双核 3.3 GHz, 内存为 2.0 GHz 的笔记本计算机上, 利用 Visual Studio 2005 C++ 平台, 取 lena.bmp 作为明文图像进行实验. Logistic 系统参数取值为: $X_0 = 0.901, \mu = 3.89$, 取随机序列的第一个值位置为 $k_1 = 500$; Chen's 系统的参数取值为: $a = 35, b = 3, c = 21.6, x_0 = 0.15, y_0 = 1.26, z_0 = 0.75$, 任取两个随机序列各取第一个值的位置 $k_2 = 510, k_3 = 520$, 系统时间参数 t 取值范围为 $t \in [0, 150]$, 采用步长为 0.001 的四阶五级 Runge-Kutta 算法求解混沌系统.

4.1 视觉效果分析

图 4(a) 为原始图像, 图 4(b) 所示为加密后图像, 图像大小为 256×256 , 从加密后图像可以看到, 加密后图像在视觉上已经无法看到原始图像的信

息,达到了视觉上杂乱无章的目的.



(a)原始图像 (b)加密后图像

图4 原始图像和加密后图像

4.2 安全性分析

4.2.1 密钥空间

本文的密钥包括 $X_0, \mu, c, x_0, y_0, z_0, k_1, k_2, k_3$, 在 windows 平台 32 位机上, 利用 Visual studio 2005 C++ 进行加密时, $X_0, \mu, c, x_0, y_0, z_0, k_1, k_2, k_3$ 这 9 个参数均取值为 DWORD 类型, 取值空间大小均为 2^{32} , 那么密钥空间为 $2^{32 \times 9} = 2^{288}$, 密钥长度远大于 256 比特, 故加密系统能够有效抵御穷举攻击.

4.2.2 密钥敏感性

解密时所用的 Logistic 混沌系统和 Chen's 系统参数 $X_0, x_0, y_0, z_0, \mu, c$ 任意一个与加密时的取值相差 10^{-12} , 而其他条件相同, 都无法得到正确的解密图像. 图 5(a)所示为 x_0 时得到的错误解密图像, 正确输入密钥时解密得到图 5(b). 可见算法具有很强的密钥敏感性.



(a)错误解密图像 (b)正确解密图像

图5 错误解密和正确解密图像

4.3 对压缩影响分析

JPEG 图像压缩主要是利用 DCT 变换量化后零值系数较多, 而且 zig-zag 扫描时零游程较长的特点, 非零值分布在低频系数区域, 高频区域零值系数居多. 将相邻两个 DCT 系数块的低频系数组合在一起置乱, 而将高频系数组合在一起置乱, 可以尽量较少的破坏零游程的结构, 减少对图像压缩的影响. 实验中压缩加密图像大小随质量因子的变化情况用

matlab 画图展示如图 6 所示(本例中使用原始图像大小为 65.0 kB).

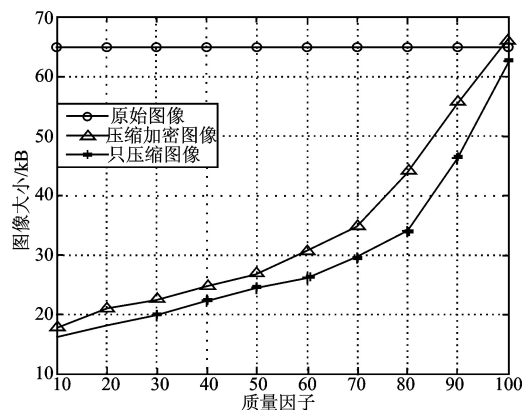


图6 质量因子对压缩加密的影响

4.4 加密速度分析

使用置乱加密算法对 DCT 变化量化系数进行位置置乱, 只是改变了图像的频率成分. 在具体的加密计算中做了数据的位置变换, 没有改变 DCT 量化系数值, 较少使用乘除运算, 因此加密速度比较快, 可以满足实时性的要求. 对不同大小的 lena bmp 图片进行压缩加密所使用的时间长度如表 1 所示.

表1 不同大小图像加、解密用时

图像大小/像素	加密时长/s	解密时长/s
128×128	0.081 1	0.086 4
256×256	0.286 3	0.301 4
512×512	0.746 1	0.772 1

5 结束语

在 DCT 变换之前先对图像进行以 8×8 图像块为基本单位的统一置乱变换, 然后在 DCT 变换量化后将相邻的两个 DCT 系数块的 DCT 变换量化系数分成 8×8 的低频组和 8×8 的高频系数组, 并利用不同的 8×8 遍历矩阵对其进行置乱. 该加密方法不仅速度快, 满足实时性的要求, 而且由于高频部分零值较多, 置乱以后对改变 zig-zag 扫描时零游程的个数影响不大, 对压缩效率影响不大. 本算法的密钥空间在 32 位机上达到了 2^{288} , 可以抵御穷举攻击, 而且在加密过程中, 改变了 DCT 系数块中非零值的个数, 能够抵御的非零值个数攻击, 加密的安全性较高.

参考文献:

- [1] 张晓强, 王蒙蒙, 朱贵良. 图像加密算法研究新进展[J]. 计算机工程与科学, 2012, 34(5): 1-6.

- [2] Liao Xiaofeng, Lai Shiyue, Zhou Qing. A novel image encryption algorithm based on self-adaptive wave transmission [J]. Signal Processing, 2010 (90): 2714-2722.
- [3] TongXiaojun. Design of an image encryption scheme based on a multiple chaotic map[J]. Commun Nonlinear Sci Numer Simulat, 2013(18):1725-1733.
- [4] 于万波, 杨灵芝. 二次函数混沌特性分析及其图像加密应用[J]. 计算机工程, 2013, 39(4): 5-8.
- [5] 舒永录, 张玉书, 肖迪, 等. 基于置乱扩散同步实现的图像加密算法[J]. 兰州大学学报: 自然科学版, 2010, 48(2): 113-116.
- [6] Shi Changgui, Bharat Bhargava. An efficient MPEG video encryption algorithm[C]// IEEE Proceeding of the 17 th Symposium on Reliable Distributed system. [s. l.]:IEEE, 1998:381-386.
- [7] Ching Hung yuen, Kwok Wo wong. A chaos-based joint image compression and encryption scheme using DCT and SHA-1[J]. Applied Soft Computing, 2011 (11):5092-5098.
- [8] 文昌辞, 王沁, 陈庆, 等. JPEG 彩色图像加密新算法[J]. 系统工程与电子技术, 2012, 34(5): 1283-1287.
- [9] 杨凤霞. 基于 Logistic 映射的压缩图像加密算法[J]. 激光与红外, 2013, 43(5): 565-568.
- [10] 陆阳, 杨文泉, 陈蕾. 图像频域加密算法[J]. 计算机工程与应用, 2003, 39(14): 130-131, 172.
- [11] 彭成, 柳林. 基于混沌序列的压缩图像加密算法[J]. 计算机工程, 2008, 34(20): 177-179.
- [12] 张萌, 刘忠信, 孙青林, 等. 基于混沌的视频压缩域加密方法研究[J]. 控制工程, 2005, 12(5): 482-485.
- [13] Wu Chung ping, Kuo C C Jay. Design of integrated multimedia compression and encryption systems[J]. IEEE Transactions on Multimedia, 2005, 7(5): 828-39.
- [14] Li Weihai, Yuan Yuan. A leak and its remedy in JPEG image encryption[J]. International Journal of Computer Mathematics, 2007, 84(9): 1367-1378.
- [15] Zhou Jiantao, Liang Zhiqian, Chen Yan. Security analysis of multimedia encryption schemes based on multiple huffman table[J]. IEEE Signal Processing Letters 2007, 14(3): 201-4.

作者简介:

王方超 男, (1984-), 硕士研究生, 助教. 研究方向为图像、视频处理、无线电通信技术.

李 斌 男, (1962-), 副教授. 研究方向为无线电通信技术.

周佳虹 男, (1980-), 硕士研究生, 讲师. 研究方向为无线电通信技术.

(上接第 138 页)

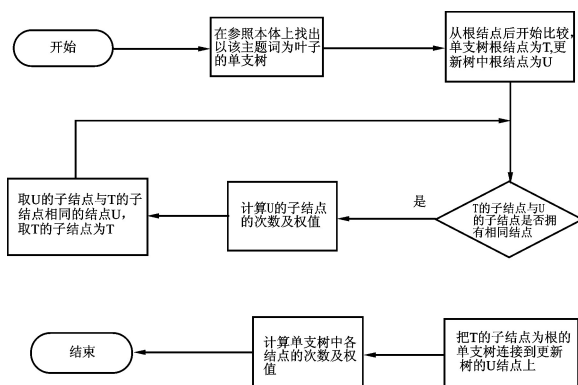


图7 动态本体的更新流程

也就是把整个互联网看成是一个动态本体;把服务器 Agent 能提供的具有语义结构的信息当做它的 Belief, 称为网站本体;把客户 Agent 的偏好信息当做它的 Belief, 称为用户本体. 把服务器 Agent 和客户 Agent 共同关注的信息当做它们的公共 Belief, 称为映射本体. 根据用户的不同身份探讨了语义语义 B/S 的工作流程, 并对动态本体中的演化机制在语义 B/S 结构中的具体意义进行了研究, 给出了本

体的更新及演化算法, 试图能为客户提供具有个性化的服务.

参考文献:

- [1] 罗钧旻, 王蕾. 基于互表性的动态本体体系结构研究[J]. 微电子学与计算机, 2013, 30(2): 124-128.
- [2] Michael E Bratman. Plans and resource-bounded practical reasoning[J]. Computational Intelligence, 1988, 4 (4): 349-355, .
- [3] Les GasserCarl, Braganza, Nava Herman. MACE: a flexible testbed for DAI research[M]. San Mateo, CA: Pitman Publishing, 1988: 119-152.
- [4] 罗钧旻, 罗建龙. 基于互表性的个性化网页研究[J]. 微电子学与计算机, 2013, 30(3): 12-15.
- [5] 罗钧旻, 武钰云, 吴彬. 模糊本体及其演化研究[J]. 微电子学与计算机, 2011, 28(5): 140-143.

作者简介:

罗钧旻 男, (1963-), 教授, 博士. 研究方向为人工智能;

桑蓓蓓 女, (1987-), 硕士研究生. 研究方向为人工智能.