

基于 DC 系数隐藏的 JPEG 图像加密算法

韩 栋¹, 王春华²

(1 武汉理工大学 计算机科学与技术学院, 湖北 武汉 430063;

2 黄淮学院 动画学院, 河南 驻马店 463000)

摘 要: 原始位图图像经过 8×8 大小分块, DCT 变换和系数量化后, 取出其直流 (DC) 系数进行比特位分解, 将分解后的每一个比特位隐藏到其所在系数块的不同交流 (AC) 系数的最低比特位上去. 完成所有 DC 系数的隐藏后, 将整个图像的所有 DCT 系数进行整体的置乱加密. 最后, 按照 JPEG 压缩编码的格式完成后续编码过程. 仿真实验和分析结果表明, 该算法加密效果良好, 对图像压缩率影响较小, 图像格式兼容性较好, 具有较强的安全性.

关键词: JPEG 图像; DC 系数; 比特位隐藏; 系数置乱

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2018)09-0047-05

JPEG Image Encryption Algorithm Based on the Hiding of DC Coefficients

HAN Dong¹, WANG Chun-hua²

(1 School of Computer Science and Technology, Wuhan University of Technology, Wuhan 430063, China;

2 School of Animation, Huanghuai University, Zhumadian 463000, China)

Abstract: Segment the original bitmap into 8×8 blocks, make Discrete Cosine Transformation (DCT) in the 8×8 block and quantize the coefficients. Take the Direct Current (DC) coefficients out of the DCT coefficients of different blocks and decompose the DC coefficients bit by bit. Put the bits decomposed by the DC coefficient onto the least significant bits of the Alternating Current (AC) coefficients in the same 8×8 block and the DC coefficient is hidden. As all the DC coefficients being hidden, shuffle all the DCT coefficients of the original bitmap according to a shuffling matrix. And then, accomplish the lasting coding process of JPEG compression. Experimental results and analyses show that the algorithm produces good performance of high visual quality with strong sensitivity, and generate the cipher-image with almost the same size as that of the directly compressed JPEG image. Finally, the proposed algorithm is compatible with JPEG file format.

Key words: JPEG image; DC coefficient; hiding of bits; coefficients shuffling

1 引言

随着信息技术的不断发展, 数字图像等多媒体信息的安全性受到越来越多的重视, 其中数字图像加密技术成为保护图像数据安全的重要手段之一. 常用的加密方法大致可分为两类: 空间域加密方法^[1-4]和变换域加密方法^[5-12]. 空间域加密没有考虑压缩编码的

影响, 实现过程相对简单, 但是密文很难再通过压缩算法进行压缩. 变换域加密算法在提高图像安全性能的同时, 需要考虑图像的压缩和编码问题.

JPEG 压缩编码是一种常见的压缩编码格式, 即可用于网页浏览图像的上传下载, 也可用于图像的存储. 目前针对 JPEG 压缩格式的加密研究取得了许多重要研究成果^[5-11].

收稿日期: 2017-12-14; **修回日期:** 2018-01-13

基金项目: 河南省科技计划项目 (大数据时代隐私数据安全框架的设计与关键技术研究); 河南省驻马店市科技计划项目 (17135)

文献[5]提出一种 JPEG 格式图像加密算法,针对 DCT 变换和量化后的 DC 系数和 AC 系数的符号位进行加密. 分析其加密过程发现,算法仅改变 DCT 系数的符号,没有改变绝对值,而且位置置乱只是在 8×8 图像块内部,原本位于某个块内的系数在加密后依然聚集在某一块内. 文献[6]提出了针对该算法的攻击方案,将所有 DCT 变换后 8×8 系数块的 DC 系数置为 128,可以破解得到明文图像的部分信息.

文献[7]提出一种结合 JPEG 编码的彩色图像加密算法,文献[8]吸收文献[7]中选择加密的思路,提出一种自适应加密算法. 文献[9]利用 AC 系数抓取图像的纹理信息并生成部分区域,基于该区域将 DC 系数进行编码,使用八种不同的方式扫描 AC 系数,最后选取比特流最小的一种扫描方式,并提取每块的 AC 系数,增大 AC 系数置换的范围. 该加密算法的优点在于,可以有效抑制因为加密带来的比特流大小的增加.

本文提出一种针对 DCT 变换和量化后的 DC 系数进行隐藏的加密算法.

2 加密算法

数字图像的 8×8 像素块经过 DCT 变换和量化后,DC 系数的取值范围为 $-1\ 024\sim 1\ 023$,总共需要占用了 11 个比特位. 当 DC 系数为负数时,由于计算机中负数存储的规则,实际占用了 16 个比特位,如图 1 中所示,第 16 位为符号位. 为了在计算机中表示和后续处理的方面,在加密之前,对 DC 系数进行预处理得到 DC' ,二者的换算关系为 $DC'=DC+1\ 024$. 经过预处理后, DC' 的取值范围为 $0\sim 2\ 047$,虽然在计算机存储中占用了 16 个比特位,但是在计算和数据处理中,只占用了 16 个比特位中的低 11 位,如图 2 中灰色部分所示.

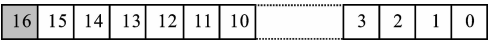


图 1 DC 系数结构

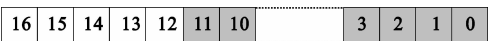


图 2 DC' 系数结构

基于 DC 系数隐藏的加密算法,就是要将经过预处理的 DC' 系数的低 11 位分解为 11 个比特位,将对应的 0 和 1 数据隐藏到所在 8×8 像素块的 AC 系数中去,从而达到加密 DC 系数的效果,隐藏 DC'

系数的低 11 位的比特位的方法,采用 AC 系数最低有效位替代的方法. 根据图像 DCT 变化和系数量化的特点可知,AC 系数大小的微小变化,对于图像像素的没有太大影响. 因此,改变 AC 系数的最低有效位,也就是根据 DC 系数 11 个比特位数值的多少改变 AC 系数最低一位的大小,从 0 变为 1 或者从 1 变为 0,即达到了加密 DC 系数的效果,也不会对 AC 造成严重失真. DC 系数隐藏过程示意图如图 3 所示.

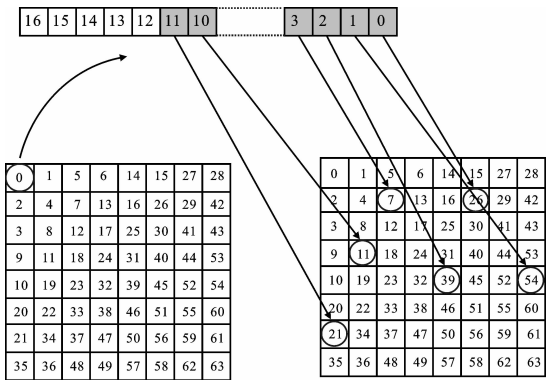


图 3 DC 系数隐藏示意图

加密 DC 系数可以阻止恶意攻击者从密文图像中获取明文的色彩等有用信息,但还无法保护明文图像的细节信息,AC 系数代表了图像的细节信息,因此还需要进行 AC 系数的加密. 通过改变 DCT 系数的大小或者位置,都可以改变原始图像的像素大小. 因此,DC 系数隐藏以后,对整个图像进行整体的 DCT 系数(包括 AC 系数)位置置乱加密,从而达到改变原始图像像素和加密图像的目的,整个加密流程如图 4 所示,虚线部分为加密模块,其余部分为 JPEG 压缩编码的标准模块.

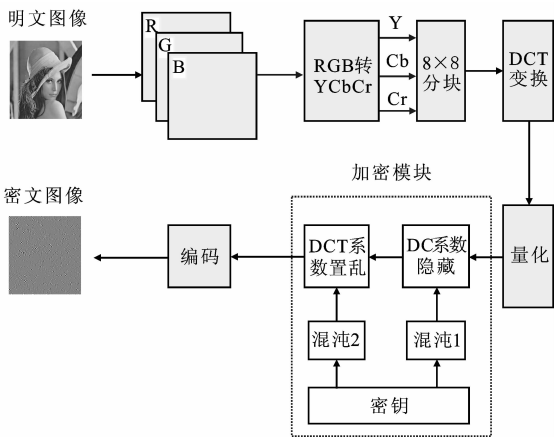


图 4 加密算法流程

3 密钥生成及加密步骤

3.1 DC系数隐藏密钥生成

混沌系统可以从有序状态演变为无序状态,能够产生伪随机序列,这种随机序列既非周期又不收敛。混沌系统产生的随机序列对初值变化十分的敏感,初始状态发生微小的变化即可使得产生的混沌序列完全不同,而且互不相关,因此特别适合用来产生密钥。

进行DC系数隐藏时,具体DC系数各比特位要置于 8×8 像素块的DCT变换及量化后的哪个系数的最低有效位上,由Logistic映射生成的随机序列决定。Logistic映射定义如下:

$$x_{n+1} = ux_n(1 - x_n) \quad (1)$$

式中,参数 u 满足 $3.6 \leq u \leq 4$;初始值 x_0 满足 $0 < x_0 < 1$ 时,Logistic映射处于混沌状态。使用Logistic映射函数作为“混沌1”,产生第一组伪随机序列,随机序列的数值 x_n 在 $(0,1)$ 内是随机的,根据本文需要,对 x_n 做如下处理:

$$X_n = [1\ 000 * x_n] \% 64 \quad (2)$$

公式(2)中 $[\]$ 表示取整操作,本文实现过程采取向上取整; $\%$ 表示取余操作。如此,可将随机序列映射到 $[1,63]$ 自然数区间,即 $X_n \in [1,63]$ 。从 X_n 序列中选取11个不同的数值作为隐藏位置密钥。

3.2 “DCT系数置乱密钥生成

DCT变换域中每个系数的变化都会对整个图像产生影响,为了加密图像细节,DC系数隐藏以后,需要对AC系数进行加密处理^[7],本文进行整个图像所有DCT系数位置置乱从而达到置乱AC系数的效果。

DCT系数置乱涉及的“混沌2”使用公式(3)所示的分段线性混沌映射。

$$y(k+1) = F(y(k), p) = \begin{cases} y(k)/p; & 0 \leq y(k) < p, \\ (y(k) - p)/(0.5 - p); & p \leq y(k) < 0.5, \\ 0; & y(k) = 0.5, \\ F(1 - y(k), p); & 0.5 < y(k) < 1.0. \end{cases} \quad (3)$$

式中, $y(k) \in [0,1]$, $p \in (0,0.5)$, p 为控制变量, $y(0)$ 为函数初始状态。图5所示为使用分段线性混沌映射产生第二组随机序列,从中选取64个随机序列数值,根据大小排序,构成的一个 8×8 二维置乱矩阵的例子。置乱矩阵 E 具体大小依据具体待加密图像大小确定。

61	11	53	40	35	25	56	30
38	63	47	6	43	4	21	62
9	8	45	41	33	23	54	28
51	57	15	31	13	48	0	12
49	18	17	1	39	2	19	26
36	50	5	22	44	14	32	58
27	20	16	10	59	46	42	3
52	60	7	37	24	34	55	29

图5 置乱矩阵示意图

3.3 具体加密步骤

假设待加密原始图像为真彩色图像 $I_{m \times n}$,其中,图像高度为 m ,宽度为 n 。JPEG彩色图像有3个颜色分量:Y、Cr和Cb,以Y分量为例具体说明加密算法如下:

(1) 对原始图像进行 8×8 大小分块,则整个图像可分为 $\frac{m}{8} \times \frac{n}{8}$ 个图像块,按照从左到右,从上到下的顺序,从图像左上角开始图像块依次表示为 $II_i, i = 0, 1, \dots, \frac{m}{8} \times \frac{n}{8}$ 。取 II_0 进行DC系数隐藏加密。

(2) 设定Logistic系统的参数: $3.6 \leq u \leq 4, 0 < x_0 < 1$ 。为了保证序列的随机性,舍去序列开始部分,从序列的第 k 个值开始,连续取 $N = 500$ 个元素 $[x_k, x_{k+1}, \dots, x_{k+499}]$ 依据公式(2)获取随机序列 $[X_0, X_1, \dots, X_{499}]$,并顺序选取其中11不同数值组成子序列 $[S_0, S_1, \dots, S_{10}]$,其中 $S_i \in [1,63], i = 0, 1, \dots, 10$,且 $S_k \neq S_l, k \neq l, k \in [0,10], l \in [0,10]$ 。

(3) 将量化后 8×8 大小的DCT系数块中的直流分量DC系数进行比特位分解。从最低位到最高位依次表示为 $[D_0, D_1, \dots, D_{10}]$,其中 $D_i \in \{0,1\}, i = 0, 1, \dots, 10$ 。将 D_i 依据 S_i 数值指示,依次放置于DCT系数块中相应位置,并替代相应位置系数的最低比特位。 II_0 图像块DC系数隐藏加密完成。

(4) 第 i 个图像块 $II_i, i = 1, \dots, \frac{m}{8} \times \frac{n}{8}$ 。其DC系数隐藏时,Logistic映射函数的初始值取为第 $i-1$ 个图像块加密时产生的随机序列 $x_{1\ 000}^{i-1}$,即 $x_0^i = x_{1\ 000}^{i-1}$ 。参数 μ 取值不变。依次按照步骤(2)和(3)的方法对各图像块的DC系数进行隐藏加密。待所有 8×8 图像块DC系数隐藏加密完成后,转自步骤(5)进行后续处理。

(5) 利用分段线性映射函数生成 $m \times n$ 大小二维置乱矩阵 $E_{m \times n}$ 。设置公式(3)中参数和初始值: $y(0) \in [0,1], p \in (0,0.5)$,舍去序列开始部分,从序列的第1 000

个值开始,连续取 $m \times n$ 个元素进行大小排序,依据升序原则得到大小二维置乱矩阵 $E_{m \times n}$.

(6) 对经过步骤(4) 处理后的 DCT 系数,依据二维置乱矩阵 $E_{m \times n}$ 进行位置置乱. Cr 和 Cb 分量的加密过程类似. 加密完成. 继续进行 Huffman 编码完成后续 JPEG 图像压缩过程形成 JPEG 密文图像 $I_{m \times n}$. 解密过程是加密的逆过程,首先利用二维置乱矩阵 $E_{m \times n}$ 进行 DCT 系数的反置乱,然后利用 Logistic 映射函数,从各个 8×8 DCT 系数块中提取最低 bit 位,还原 DC 系数. 最终得到解密图像.

4 算法仿真与分析

算法的实验环境选定为 Visual Studio 2010 C++,实验对象选取 USC-SIPI 图像库中的标准彩色图像 lena. bmp 作为明文图像进行实验,如图 6(a) 所示. Logistic 系统初始值和参数取值为: $x_0 = 0.3$, $\mu = 3.9$,取随机序列的第一个值位置为 $k = 1\ 000$;分段线性映射函数初始值和参数取值为: $y(0) = 0.2$, $p = 0.4$.

4.1 密文视觉效果分析

图 6 中(a)图为未加密彩色图像 lena. bmp,图像的尺寸大小为 293×309 , (b)图为采用本论文算法加密后图像. 从图中可以看出,加密后的图像能够被标准解码器解码,但是已经无法识别出原始图像的任何有用信息,达到了加密的视觉效果.



(a)原始图像 (b)加密后图像
图 6 原始图像和加密后图像

4.2 安全性分析

4.2.1 密钥空间大小

本文的密钥包括 $x(0), \mu, k, y(0)$ 和 p , 在 windows 平台 32 位机上,利用 Visual studio 2010 C++ 进行加密时, $x(0), \mu, y(0), p$ 这 4 个参数均为 DWORD 类型,取值空间大小均为 2^{64} , k 为 UNSIGNED INT 类型,取值空间大小均为 2^{32} 因此,那么密钥空间为 $2^{64 \times 4 + 32 \times 1} = 2^{288}$. 密钥长度远大于 256 比特,加密系统可以有效抵御穷举攻击.

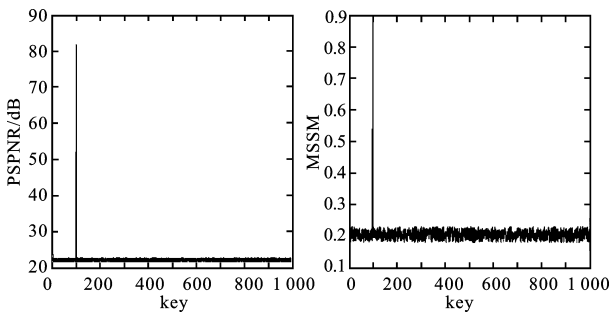
4.2.2 密钥敏感性

为了说明本文算法对于密钥的敏感性,图像密文解密时,将密钥 $x(0), \mu, y(0), p$ 任意一个取值与加密的取值相差 10^{-12} ,或者 k 的取值取加密的取值相差 1,他条件完全相同时,都无法得到正确的解密图像. 图 7 中(a)图是改变 $y(0)$ 时得到的错误解密图像,正确输入密钥时解密得到图(b).



(a)错误解密图像 (b)正确解密图像
图 7 错误解密和正确解密图像

峰值信噪比(PSNR)^[8]用于计算密文两幅图像之间的差别,其值越小,表明两幅图像差别越大. 平均结构相识指数(MSSIM)^[8]表示两幅图像之间的相识性,数值越小,表示越不相关. 在实验中,生成 1 000 个有微小大小变化却互不相关的 $y(0)$ 值,其中,只有第 100 个数值是正确的密钥,用这一组密钥解密后的图像与原始图像进行 PSNR 和 MSSIM 值的比对(Matlab 画图),结果如图 8 所示. 可见算法密钥敏感性良好.



(a)PSNR (b)MSSIM

图 8 1 000 个微小改变的 $y(0)$ 解密的结果

4.3 对压缩影响

本文在选择在 JPEG 压缩编码过程的 DCT 系数量化后进行 DC 系数隐藏加密,尽量不改变 DCT 系数的个数. BMP 图像压缩成 JPEG 图像过程中,质量因子的选择对于图像的压缩比产生不同的影响. 图 9 给出了实验中本文算法采用不同质量因子对于 JPEG 图像加密过程造成的数据流大小影响(Matlab 画图),由图 9 可知,采用本文加密算法后,

不同质量因子下,对于图像的压缩性能影响不大.分析原因,一是由于本文对 DC 系数采取了隐藏的方法,没有增加 DC 系数编码的数据流长度,相反,还降低了其数据流长度;二是 DC 系数隐藏过程中,对于 AC 系数影响有限,整个图像中,没有大量增加 AC 系数个数,因此,AC 系数采用 Zig-Zag 扫描和 Huffman 编码后,数据流也不会有较大变化.

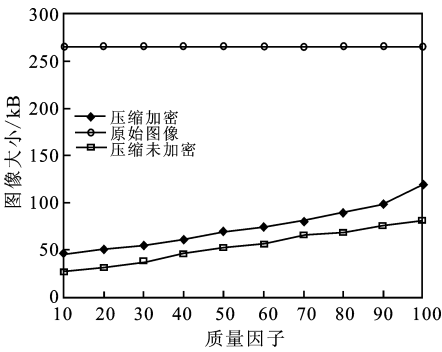


图 9 质量因子对压缩加密的影响

4. 4 抗攻击分析

图像加密可以看作是一种图像退化,通过一些图像处理手段或许可以恢复图像部分信息.很多类似的手段都是利用滤波器进行图像恢复,实验中尝试利用 4 种常用的滤波器对加密后图像进行图像增强和恢复,计算处理后密文图像与原始图像的 PSNR 和 MSSIM,结果如表 1 所示.可以看出,这些方法都没能获取原始图像的信息.

表 1 密文图像滤波后 PSNR 和 MSSIM

滤波器	均值滤波	中值滤波	维纳滤波	模糊对比增强滤波
PSNR	22.013	21.351	20.697	19.364
MSSIM	0.198	0.213	0.187	0.186

4. 5 格式兼容分析

如图 4 所示,本文的加密模块放置在 JPEG 压缩流程的 DCT 系数量化后,Huffman 编码之前,没有破坏 JPEG 压缩的整体框架结构.本文算法改变的只是 DC 系数大小,AC 系数的位置、大小和个数,但是 AC 系数大小改变较小,系数值只有正负 1 的改变,AC 系数个数的改变也较少,因此,只会较小地影响压缩后 jpg 图像的大小,不会破坏其格式.对于密文图像,解码器均可以正确解码,只是在没有获取密钥的情况下,无法正确解密密文图像,但不会导致解码失败或者解码器崩溃现象发生.

5 结束语

本文算法对经过 DCT 变化和量化后的 DC 系

数进行了隐藏加密,接着对所有 DCT 变化系数进行了整体置乱,达到了加密的效果.实验结果表明,视觉效果和数据分析效果良好,且密文的格式兼容性好.

参考文献:

[1] 金聪,刘会. 量子混沌与折叠算法的图像加密系统[J]. 光学精密工程,2017,25(3):749-755.

[2] 贺锋涛,张敏,白可,等. 基于激光散斑和 Hennon 映射的图像加密方法[J]. 红外与激光工程,2016,45(4):268-272.

[3] 姚丽莉,袁操今,强俊杰,等. 基于 gyrator 变换和矢量分解的非对称图像加密方法[J]. 物理学报,2016,65(21):139-144.

[4] 朱淑芹,李俊青,葛广英. 基于一个新的四维离散混沌映射的图像加密新算法[J]. 计算机科学,2017,44(1):188-193.

[5] Wu C P, Kuo C C Jay. Design of integrated multimedia compression and encryption systems[J]. IEEE Transactions on Multimedia 2005,7(5):828-839.

[6] Lian S. Efficient image or video encryption based on spatiotemporal chaos system [J]. Chaos, Solitons&Fractals, 2009,40(5):2509-2519.

[7] 肖迪,谢沂均. 一种结合 JPEG 压缩编码的彩色图像加密算法[J]. 物理学报,2013,62(24):67-77.

[8] 雷正桥,肖迪. 一种格式兼容的 JPEG 彩色图像自适应加密算法[J]. 计算机科学,2016,43(6):152-155.

[9] 郭慧,贺杰,李琳. 具有鲁棒性与数据嵌入能力的 JPEG 压缩图像加密算法[J]. 计算机应用研究,2016,33(9):2804-2809.

[10] 王方超,李斌,周佳红. 基于 DCT 量化系数重组的 JPEG 图像加密算法[J]. 微电子学与计算机,2014,31(8):139-143.

[11] 文昌辞,王沁,黄付敏,等. JPEG 彩色图像自适应加密算法[J]. 计算机辅助设计与图形学学报,2012,24(4):500-505.

[12] 傅勇,易小伟,马恒太. 一种支持密文转码的 JPEG2000 图像加密算法[J]. 计算机科学,2014,41(6):84-93.

作者简介:

韩 栋 男,(1979-),博士研究生,讲师.研究方向为计算机图形图像处理、数据挖掘.
E-mail:handong@huanghuai.edu.cn.

王春华 女,(1980-),博士,副教授.研究方向为计算机图形图像处理、数据挖掘.