一种格式兼容的JPEG彩色图像自适应加密算法

雷正桥[1] 肖 迪[2]
(重庆工业职业技术学院 重庆 401120)[1] (重庆大学 重庆 400044)[2]

摘 要 为了保障特殊格式图像的安全应用,需要针对其特点,深入研究与其格式兼容的图像加密算法。通过集成JPEG压缩标准与自适应加密思想,提出了具有格式兼容特性的JPEG彩色图像自适应加密算法。该算法分别选取JPEG压缩过程中的直流系数和按曲折排序的前16个交流系数构造出对应的系数矩阵。在自适应加密框架下,利用混沌产生随机密钥流,实现对系数矩阵和直流系数符号的加密,保证密文图像不会泄露明文色彩信息。仿真实验和分析证明,该算法加密效果良好,对压缩效果影响很小,且具有格式兼容性和足够的安全性。

关键词 JPEG彩色图像,加密,格式兼容,安全性
中图法分类号 TP391 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.6.031

JPEG Color Image Self-adaptive Encryption Algorithm with Format Compatibility

LEI Zheng-qiao[1] XIAO Di[2]
(Chongqing Industry Polytechnic College, Chongqing 401120, China)[1]
(Chongqing University, Chongqing 400044, China)[2]

Abstract To ensure the security application of images with special format, it is necessary to conduct an in-depth study of the corresponding image encryption algorithm compatible with its format. By integrating JPEG compression and the idea of self-adaptive encryption, a self-adaptive encryption algorithm for JPEG color image was proposed. DC coefficients and the first 16 AC coefficients in Zig-Zag order of JPEG compression are chosen to construct the corresponding matrices. Based on chaotic random sequence, self-adaptive encryption scheme is utilized to encrypt the coefficients, and the sign of DC coefficients is also encrypted to avoid color information leaking. Experimental results and analyses verify that both the security and performance of the proposed algorithm are good, and the impact on the compression is negligible. Furthermore, it is compatible with JPEG file format.

Keywords JPEG color image, Encryption, Format compatibility, Security

1 引言

随着数字图像应用的日益广泛,如何安全地传输和存储图像成为一个重要的问题。传统的加密方法并不适合于多媒体图像的安全传输和存储[1-3]。针对特殊图像格式的加密逐渐成为研究热点。JPEG作为一种应用非常广泛的图像压缩格式,对其加密研究已取得一些成果。如文献[4]首先利用2维耦合映像格子生成混沌序列,进而利用它实现对JPEG中DC系数和所有AC系数符号的加密。然而文献[5]提出了对该方案的攻击方法:通过将所有DC系数置为128而将所有AC系数取为正,可破解出有效的明文信息。文献[6]也提到了该问题。Lian[7]等提出的加密算法依次对8×8图像块和DC系数进行置乱,并进行DCT系数符号的加密,但该算法无法获得理想的加密效果,攻击者可以从密文图像中获取部分明文信息,如明文色块、模糊的轮廓等操作。文献[8]先利用Chen系统生成混沌序列,用于对每个8×8图像块中的DC系数和最开始两个AC系数的异或加密,但由于加密系数太少,仍可能泄露明文信息。此外,由于密钥流与明文不相关,上述算法[7,8]还存在选择明文攻击的隐患。

为了满足JPEG格式图像的安全需求,利用自适应加密的思路,在加密过程和明文之间建立了复杂的相关性,提出一种JPEG格式彩色图像的加密算法。该算法选取性能良好的混沌映射构造随机数发生器,同时吸收了"结合压缩编码加密"和"选择加密"两种思路的特点。该算法加密效果良好,对压缩效果影响非常小,具有格式兼容性和足够的安全性。

2 算法设计

在本算法中将会用到分段线性混沌映射(PWLCM),带参数 u 的映射定义如下:

$$x(k+1)=C[x(k);\mu]=\begin{cases}\dfrac{x(k)}{\mu}, & x(k)\in[0,\mu)\\ \dfrac{x(k)-\mu}{0.5-\mu}, & x(k)\in[\mu,0.5)\\ C[1-x(k);\mu], & x(k)\in[0.5,1)\end{cases} \quad (1)$$

其中,$x(k)\in[0,1]$,$u\in(0,0.5)$。秘密取定分段线性混沌映射的初值 $x(0)\in[0,1]$和初始参数 $u_0\in(0,0.5)$作为算法的

到稿日期:2015-05-14 返修日期:2015-09-08 本文受应急通信重庆市重点实验室开放课题资助项目(CQKLEC,20140504)资助。
雷正桥(1973-),男,副教授,主要研究方向为网络安全技术,E-mail:leizhengq@163.com;肖 迪(1975-),男,教授,博士生导师,主要研究方向为信息安全技术。

秘密密钥。

图1所示为算法流程图，其中灰色部分为JPEG压缩标准。

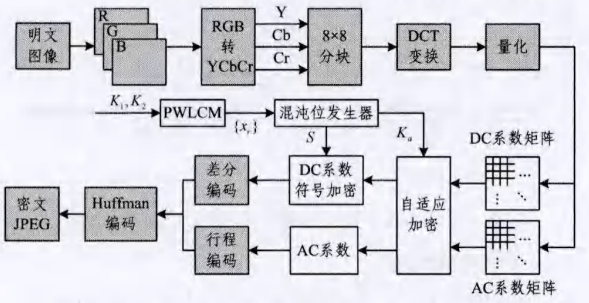


图1 格式兼容的JPEG彩色图像安全加密算法流程

如图1所示，一幅 $M\times N$ 的图像按 8×8 分为不重叠的块，令 $m=M/8$，$n=N/8$，则分块数量为 $m\times n$，算法的密钥 K_1 和 K_2 分别为分段线性混沌映射的初值 $x(0)$ 和初始参数 u_0。完整的算法描述如下：

(1)利用密钥 K_1 和 K_2 生成长度为 $(208+m\times n)$ 的混沌序列，将前200个分量舍弃后输入到混沌位发生器。取发生器输出的前 $m\times n$ 个随机位组成S用于加密DC系数符号，取输出的最后8个位组成 K_a 作为后续自适应加密的密钥。

这里的混沌位发生器借鉴了文献[9]中的随机位抽取方法，从实数序列 $\{x_r\}(r=1,2,\cdots,N)$ 中抽取所有第2位组成具有独立同分布特性的二进制随机序列。实数序列 $\{x_r\}$ 中的每个 x 可以表示为如下形式：

$$x=0.b_1(x)b_2(x)\cdots b_i(x)\cdots,x\in[0,1],b_i(x)\in\{0,1\} \tag{2}$$

第 i 位 $b_i(x)$ 就可表示为：

$$b_i(x)=\sum_{q=1}^{2^{i-1}}(-1)^{q-1}\Theta_{(q/2^i)}(x) \tag{3}$$

其中，$\Theta_t(x)$ 为阈值函数，定义为：

$$\Theta_t(x)=\begin{cases}0, & x<t\\ 1, & x\geqslant t\end{cases} \tag{4}$$

取 $i=2$，即可得到独立同分布的二进制随机序列 $B_2^r=\{b_2(x_r)\}_{r=1}^N$（$r$ 为序列的长度，x_r 为第 r 次实数值）。

(2)转换明文图像色彩空间至YCbCr，并执行余弦变换和量化过程。

JPEG彩色图像的压缩过程需要对亮度 Y、色度 Cb 和色度 Cr 3个分量分别进行余弦变换、量化、熵编码等操作。两张量化表则分别用于 Y 分量和 Cb/Cr 分量的量化。在压缩过程中，可对其中的DC系数和AC系数进行自适应加密。

(3)首先将每个分块的DC系数取出，组成一个 $m\times n$ 的DC系数矩阵 M_{DC}，然后按照Zig-Zag顺序取出每个分块的前16个AC系数组成一个 $m\times n\times 16$ 的AC系数矩阵 M_{AC}。

(4)利用第(1)步所生成的密钥流 K_a，实现 M_{DC} 和 M_{AC} 的自适应加密。

若密钥流 K_a 当前位为“0”值，则先利用DC系数矩阵 M_{DC} 的上半部分加密其下半部分，再用 M_{DC} 的下半部分加密上半部分；若密钥流 K_a 当前位为“1”值，则先利用AC系数矩阵 M_{AC} 的左半部分加密右半部分，再用右半部分加密左半部分。以“如何利用上面部分的遍历矩阵对下面部分进行置乱加密”为例：将图像按上下方向分为相等的两块，通过对居上图像块的像素值进行排序可获得到一个遍历矩阵，然后就可以根据该遍历矩阵对居下的图像块进行置乱。其它加密过程与此类似。

(5)利用混沌随机位序列 S 对 M_{DC} 矩阵中DC系数符号进行加密。

在DC系数置乱加密之后，逐个扫描DC系数，对第 i 个DC系数，如式(5)所示，若 $S[i]$ 为0，则不改变该DC系数符号；若 $S[i]$ 为1，则取反该DC系数符号。

$$M_{DC}[i]=\begin{cases}M_{DC}[i], & \text{if } (S[i])=0\\ -M_{DC}[i], & \text{if } (S[i])=1\end{cases} \tag{5}$$

由于混沌随机位序列S分布均匀，这种简单的处理方式可实现对DC系数符号的均匀处理，同时降低DC系数在解码后与原图像亮度信息的关联度，消除密文可获得明文主色调的可能性。

(6)完成后续的JPEG的差分编码、行程编码和Huffman编码等过程，获得密文图像。

3 实验结果与分析

算法的实验环境选定为Matlab2011b，实验对象选取USC-SIPI图像库[10]中的彩色图像，质量因子 Q 取85。采用以下两种指标作为图像加密效果的评价标准。

①峰值信噪比(PSNR)

峰值信噪比可用于计算密文图像与原图像之间的差别，其值越小，表示明文密文差别越大，加密效果越好。

$$PSNR=10\times\log\left(\frac{255^2}{MSE}\right) \tag{6}$$

$$MSE=\frac{1}{wh}\sum_{i=0}^{w}\sum_{j=0}^{h}(I(i,j)-J(i,j))^2 \tag{7}$$

其中，图像尺寸为 $w\times h$，$I(i,j)$ 与 $J(i,j)$ 分别代表图像 I 和 J 中位置 (i,j) 处像素的值。

②平均结构相似指数(MSSIM)

通过与视觉感知系统(HSV)相结合，结构相似指数 $SSIM$ 测量明文与密文之间的相似度来评价图像的保真度。对每个 8×8 分块，计算其失真图像和原图的差距，给出对应的 $SSIM$ 值。

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{8}$$

其中，两幅图像的分块是 x 和 y，其平均值分别用 μ_x 和 μ_y 表示，其方差分别用 σ_x^2 和 σ_y^2 表示，σ_{xy} 为协方差，$c_1=(k_1L)^2$，$c_2=(k_2L)^2$，$k_1=0.01$，$k_2=0.03$，L 表示图像的灰度级。

平均 $SSIM$ 指数(MSSIM)定义为：

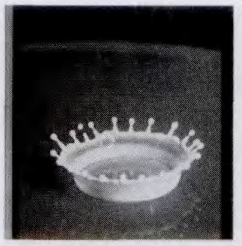
$$MSSIM(X,Y)=\frac{1}{n}\sum_{i=1}^{n}SSIM(x_i,y_i) \tag{9}$$

其中，明文和密文图像分别用 X，Y 代表，其对应的第 i 个分块用 x_i 和 y_i 表示，n 是图像分块数。$MSSIM$ 越小，表示加密效果越好。

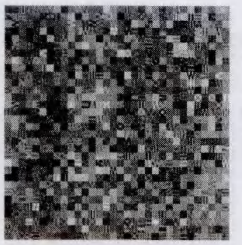
3.1 密文效果评价

图2是本算法对图像库中Splash和Lena图像的加密结果，密文图像完全由杂乱分布的色块和纹理构成，从密文中无法找到任何明文信息。

选取USC-SIPI图像库中的彩色图像，加密之后得到对应的密文，然后利用峰值信噪比和平均结构相似指数对其进行评价。如表1所列，实验得到的各项指标数值均较小，表明其加密效果良好。此外，如表1最后一行所示，本算法与传统AES算法对Lena进行加密的效果比较接近，而本算法还具有对压缩效果影响小、格式兼容等其它优点。

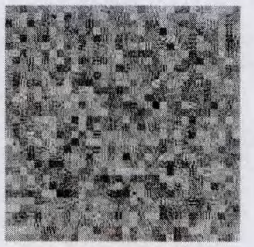


(a)Splash 明文



(b)Splash 密文

(c)Baboon 明文



(d)Baboon 密文

图 2　JPEG 彩色图像自适应加密算法的结果

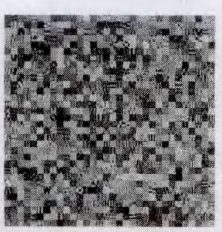
表 1　USC-SIPI 图像库加密结果

件名	描述	PSNR/dB	MSSIM
4.1.01	Girl	6.502	0.013
4.1.02	Couple	4.953	0.011
4.1.03	Girl	14.277	0.071
4.1.04	Girl	9.693	0.021
4.1.05	House	10.322	0.029
4.1.06	Tree	8.343	0.036
4.1.07	Jelly beans	8.959	0.024
4.1.08	Jelly beans	9.082	0.016
4.2.01	Splash	7.536	0.018
4.2.02	Tiffany	6.600	0.020
4.2.03	Baboon	10.452	0.125
4.2.04	Lena	9.432	0.036
4.2.05	Airplane	8.214	0.037
4.2.06	Sailboat	8.250	0.038
4.2.07	Peppers	8.074	0.020
AES 加密 Lena		9.110	0.035

3.2　密钥敏感性分析

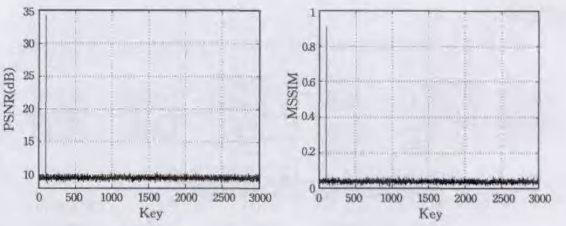
密钥敏感性良好是指密钥的微小改变要引起最终密文的巨大改变。本算法选择分段线性混沌映射(PWLCM)的初值 $x(0)\in[0,1]$和初始参数 $u_0\in(0,0.5)$作为整个算法的密钥 K_1 和 K_2。为了说明本算法的密钥敏感性，图 3 示出对 Lena 利用正确密钥解密以及将密钥 K_1 进行微小改变后再解密的结果，显然，有细微错误的密钥是无法正确解密出图像的。在实验中，生成了 3000 个彼此有微小改变的随机初始密钥 K_2(其中只有 1 个密钥完全正确)，用这一组解密密钥对密文图进行解密，获得对应的“解密图像”。图 4 示出对这些“解密图像”计算出的峰值信噪比和平均结构相似指数结果，可见算法的密钥敏感性良好。

(a)用正确密钥解密



(b)用微小改变的密钥 K_1 解密

图 3　微小改变密钥 K_1 的解密结果



(a)PSNR　　(b)MSSIM

图 4　用 3000 个微小改变的 K_2 解密 Lena 的结果

3.3　密钥空间测算

算法密钥 K_1 和 K_2 分别是分段线性混沌映射(PWLCM)的初值 $x(0)\in[0,1]$和初始参数 $u_0\in(0,0.5)$。经测试，当在小数点后 16 位有效数字进行微小变化时，将产生完全不同的混沌序列，因此可以确定密钥的可变极限为 10^{-16}。K_1 是 PWLCM 的初值 x_0，取值范围为(0,1)，密钥空间为 1×10^{16}；K_2 是混沌 1 的参数 μ，取值范围为(0,0.5)，密钥空间为 0.5×10^{16}。因此本算法总的密钥空间为 $1\times10^{16}\times0.5\times10^{16}\approx2^{106}$，即密钥长度为 106 位，安全性稍弱于 128 长度的密钥。

3.4　抗攻击分析

选择明文攻击是假设加密机已被敌手掌握，因此对于选定的任意明文，敌手可以获得对应的密文，进而开展攻击。如果加密过程仅仅通过纯置乱操作来完成，此种攻击通常会奏效，原因在于一般置乱加密算法的密钥流与明文不相关。针对此特点，本算法引入了自适应加密的思路，建立了加密过程和明文之间复杂的非线性依赖关系，不同的明文所对应的密钥流会完全不同，因此可以抵抗选择明文攻击。

如果将图像加密看成是一种图像退化，有可能借助于图像处理手段，在一定程度上恢复出明文图像的某些信息，从而造成信息泄露。利用 4 种常用的滤波器对密文图像进行了恢复测试。如表 2 所列，测试结果表明图像处理手段并不能帮助恢复图像质量。因此，原算法可以抵抗图像处理技术的攻击。

表 2　对密文图像滤波后的 *PSNR* 和 *MSSIM*

滤波器	均值滤波	中值滤波	Wiener 滤波	模糊对比增强滤波
PSNR(dB)	10.818	9.907	10.975	7.408
MSSIM	0.030	0.021	0.039	0.0103

3.5　压缩性能测试

当选用 Lena 彩色图像，给定不同的质量因子时，图 5 给出了正常压缩图像和加密图像的大小对比。可见，本算法在引入加密之后，对于 JPEG 原有的压缩性能造成的影响非常小。其原因在于，虽然本算法需要在频域中置乱 8×8 系数块中的 DC 系数和 AC 系数，但是 DC 系数值改变不大，因此对压缩性能影响很小，而置乱 AC 系数对于编码几乎没有影响，因为对 AC 系数的编码并不需要关联性。

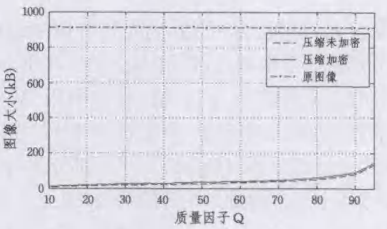


图 5　不同质量因子下的压缩图像大小

3.6 格式兼容性分析

算法流程如图1所示，在本算法中，将自适应加密的方法结合到JPEG的压缩过程中。加密所改变的只是DC系数位置及其符号以及AC系数的位置，对后续的熵编码过程不会有影响。在重建图像时，无论有没有正确的密钥，解码器均可正确解码出对应的余弦系数值，经过反量化及逆余弦变换，可恢复为可视图像。若密钥是正确的，即可获得最终的解密图像。因此，本算法加密过程不会导致编码器/解码器崩溃或其它错误，具有格式兼容的特性。

结束语 为了满足应用广泛的JPEG格式图像的安全需求，本文结合JPEG压缩过程，先对DC系数和前16个AC系数进行自适应加密，再对DC系数的符号也进行加密，提出了一种格式兼容的JPEG彩色图像加密算法。理论分析和仿真实验表明，该算法加密效果好、对压缩影响小，且具有格式兼容和足够安全的特点。

参 考 文 献

[1] Cai Jun, Chen Xin, Xiang Xu-dong. Substitution-permutation Network Structured Image Encryption Algorithm Based on Chaotic Map[J]. Computer Science, 2014, 41(9): 158-165(in Chinese)
蔡俊，陈昕，向旭东. 一种基于混沌的代换-置换结构图像加密算法[J]. 计算机科学，2014，41(9)：158-164

[2] Zhang Yong-hong. Algorithm of Digital Image Encrypting Based on Multi-chaotic Sequene Generated by Rational Bézive Surface [J]. Computer Science, 2015, 42(4): 136-140(in Chinese)
张永红. 基于有理 Bézier 曲面生成组合混沌序列的图像加密算法[J]. 计算机科学，2015，42(4)：136-140

[3] Wang Wei, Jin Cong. Image Encryption Scheme for Android Mobile Platform[J]. Computer Science, 2014, 41(8): 94-96, 108(in Chinese)
王伟，金聪. 一种基于 Android 平台的图像加密方案[J]. 计算机科学，2014，41(8)：94-96，108

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

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

[6] Yuen C H, Wong K W. Chaos-based encryption for fractal image coding [J]. Chinese Physics B, 2012, 21: 010502

[7] Lian S, Sun J, Wang Z. A novel image encryption scheme based-on JPEG encoding[C]// IEEE Eighth International Conference on Information Visualisation. 2004: 217-220

[8] Xu P, Zhao J, Wang D. A selective image encryption algorithm based on hyper-chaos[C]// 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN). 2011: 376-379

[9] Kohda T, Tsuneda A. Statistics of chaotic binary sequences[J]. IEEE Transactions on Information Theory, 1997, 43(1): 104-112

[10] The USC-SIPI image database[OL]. http://sipi.usc.edu/database

(上接第121页)

由图11可知，基于TFA的mesh路由算法比HiLow纯树路由和IEEE 802.15.5 mesh路由需要更少的路由跳数，从而实现更少的传递时延和能量消耗。而由图12－图14可知，基于TFA的mesh路由算法比IEEE 802.15.5 mesh路由和HiLow纯树路由具有更低、更均衡的能量消耗。

结束语 在无线传感器网络中，由于受到节点资源的严格限制，其路由算法必须具有低计算复杂度、低存储空间、无路由发现等特点。另外，为了降低能耗和提高网络可靠性，路由算法还需要具有良好的mesh路由特性。本文提出的两段地址分配策略及其路由能很好地满足上述需求。实验仿真表明，基于TFA的mesh路由算法比IEEE 802.15.5 mesh路由具有更低、更均衡的能量消耗。

参 考 文 献

[1] Ren Feng-yuan, Huang Hai-ning, Lin Chuang. Wireless Sensor Networks[J]. Chinese Journal of Software, 2005, 14(7): 1282-1291(in Chinese)
任丰原，黄海宁，林闯. 无线传感器网络[J]. 软件学报，2005，14(7)：1282-1291

[2] Akkaya K, Younis M. A survey on routing protocols for wireless sensor networks[J]. Ad Hoc Networks, 2005, 3(3): 325-349

[3] Dohler E M, Watteyne E T, Winter E T, et al. Routing requirements for urban low-power and lossy networks: IETF RFC 5548 [R]. 2009

[4] LAN/MAN Standards Committee. IEEE 802.15.4: Low-Rate Wireless Personal Area Networks[S]. 2012

[5] Winter T, Thubert P. RPL: IPv6 routing protocol for low power and lossy networks: IETF Internet draft, draft-ietf-roll-rpl-04 [R]. 2009

[6] ZigBee Alliance. ZigBee specification version 2006[S]. 2006

[7] LAN/MAN Standards Committee. IEEE 802.15.5: Mesh topology capability in wireless personal area networks (WPANs) [S]. 2009

[8] Gaddour O, Koubaa A. RPL in a nutshell: A survey [J]. Computer Networks, 2012, 56(14): 3163-3178

[9] Kim K, Yoo S, Lee J. Hierarchical routing over 6LoWPAN: Internet-Draft, draft-daniel-6lowpan-hilow-hierarchical-routing-01 [R]. 2007

[10] Li X, Bleakley C J, Bober W. Enhanced Beacon-Enabled Mode for improved IEEE 802.15.4 low data rate performance[J]. Wireless Networks, 2012, 18(1): 59-74

[11] Yuan L Y, Xu L, Zhu Y H, et al. A novel mesh routing using the nodes with identical tree level[J]. International Journal of Distributed Sensor Networks, 2014, 2014(1): 1-11

[12] Lee M J, Zhang R, Zheng J, et al. IEEE 802.15.5 WPAN mesh standard-low rate part: Meshing the wireless sensor networks [J]. IEEE Journal on Selected Areas in Communications, 2010, 28(7): 973-983

[13] Qiu W, Skafidas E, Hao P. Enhanced tree routing for wireless sensor networks[J]. Ad Hoc Networks, 2009, 7(3): 638-650

[14] Kim T, Kim S, Yang J, et al. Neighbor Table Based Shortcut Tree Routing in ZigBee Wireless Networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(3): 706-716

[15] Heinzelman W B, Chandrakasan A P, Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks[J]. IEEE Transactions on Wireless Communications, 2002, 1(4): 660-670