基于混沌置乱的分量融合图像加密压缩方法

任荣梓,高 航
(南京航空航天大学 计算机科学与技术学院,江苏 南京 210016)

摘 要:图像信息的传输需要通过压缩和加密来减少冗余并阻止非授权者的访问。关于图像压缩的研究由来已久,各种压缩算法和理论层出不穷,而加密压缩仍有相当大的发展空间。为此,针对目前常见的已知明文攻击等黑客攻击方式,在研究 Logistic 混沌加密技术和基于混沌置乱的分量融合图像加密压缩方法的基础上,提出了一种可逆的融合算法。该算法将提取到的彩色图像颜色分量分别进行 DCT 变换而后融合,将压缩和加密过程同时进行,显著提高了压缩算法的安全性。前期研究表明,即便所提出的方法已经可以满足正常的加密要求,但一旦泄露了部分明文,安全性便立刻降低。为了提高对已知明文的安全性,在进行完加密压缩过程之后,又使用 Logistic 混沌映射置乱作为二次加密。实验结果表明,在保证较好压缩性能的条件下,所提出的方法成功通过了已知明文攻击等黑客攻击方式的测试。

关键词:图像压缩;加密;离散余弦变换;分量融合;混沌加密
中图分类号:TP301.6 **文献标识码**:A **文章编号**:1673-629X(2017)08-0106-04
doi:10.3969/j.issn.1673-629X.2017.08.022

An Image Encryption and Compression Method Based on Chaos Scrambling with Component Fusion

REN Rong-zi,GAO Hang
(School of Computer Science and Technology,Nanjing University of Aeronautics and Astronautics,Nanjing 210016,China)

Abstract:The transmission of image information needs to be compressed and encrypted to reduce redundancy and prevent unauthorized accessing. Image compression has been investigated for a long time,so various compressed algorithms and theories have emerged in an endless stream,and there is still space for improvement in the field of encryption compression. In view of the known-plaintext attacks and other hacker attacks,on the basis of studying on Logistic chaos encryption and mage encryption and compression method based on chaos scrambling,an inverse fusion method is proposed. It fuses the color component extracted in RGB image after it is conducted Discrete Cosine Transform (DCT),which carries out compression and encryption meanwhile,improving its security significantly. Although it can meet the requirements of normal encryption,previous investigations have shown that once leaked part of plaintext,its safety must be reduced. In order to improve the security against known-plaintext attacks,Logistic chaos scrambling has been employed as the second encryption after encrypted and compressed. The experimental results show that it can successfully resist the known-plaintext attacks and hacker attack test with good compression performance.

Key words:image compression;encryption;DCT;component fusion;chaos encryption

1 概 述

随着信息化的发展,图像作为信息传递的重要媒介,其空间冗余和安全性显得越来越重要。图像信息数据量较大,平均一幅正常分辨率的真彩图像,所占的存储空间 2.3 MB,这意味着 1 GB 容量的硬盘只能存储不到五百张该规格的图像。而在传输中,特别诸如视频审计等实时性要求严格的情况下,由于传输带宽的限制,也必须对图像进行压缩。因此无论从技术要求还是经济角度来看,图像信息的压缩势在必行。利用图像压缩技术,可以节省图像存储空间和传输带宽、减少 CPU 处理和传输时间,尤其是在审计监控、视频会议、遥感信息传输、医学图像处理、传真等领域的应用中都具有显著效果。学术界对图像压缩的研究由来已久,制定了许多压缩编码标准,如 JPEG、H261、

收稿日期:2016-10-02 **修回日期**:2017-01-05 **网络出版时间**:2017-07-05
基金项目:江苏省科技成果转化专项资金资助项目(BA2012023)
作者简介:任荣梓(1993-),男,硕士研究生,研究方向为图像处理;高 航,副教授,硕士生导师,研究方向为图像处理、嵌入式应用。

H263、H264、MPEG2、MPEG4、MPEG7 等等。按照压缩后的图像质量分为两大类,无损压缩和有损压缩。其中无损压缩由于压缩比普遍不高等原因主要用于医疗等特殊领域,例如哈夫曼编码、算数编码之类。有损压缩的应用则更为广泛,例如 JPEG 和 JPEG2000。而压缩算法也是层出不穷,例如基于傅里叶变换的压缩方法[1]、基于小波变换的压缩方法[2]、基于 DCT 变换的压缩方法[3]等等。这些方法在压缩方面获得了比较理想的结果,但是单纯的压缩无法解决图像的安全性问题,一旦被黑客截获,对方可以利用逆变换的方式来窃取图像信息。为了提升图像信息的安全性,就需要研究图像加密技术。

图像压缩是一个减少数据量的过程,利用更少的空间来存储和传输给定数量的图像信息,而它的安全性则需图像加密来保证。图像的加密是对消息进行编码的过程,将源图像转化为无法识别的白噪音,从而使非授权方(黑客等)无法窃取,而授权方可以通过一定的方式来解读。在图像加密技术的发展过程中,早期见于 Refregier Philippe 和 Javidi Bahram 提出的 DRP(Double Random Parse)方法[4],随后的研究者也相继提出了许多方法,依据加密方式又可分为空间域加密—主要是基于图像置乱的图像加密和基于信息熵的图像加密,变换域的图像加密—主要分为基于树结构的图像加密[5]和基于 SCAN 语言的图像加密[6],基于混沌的图像加密[7]、基于神经网络的图像加密[8]、基于细胞自动机的图像加密[9]和量子密码技术[10]等。而图像加密的应用也较为兴盛,主要有金盾、狂牛、飓风等商用加密软件。

综上所述,虽然图像压缩和加密的研究都已较为完善,然而在同时进行压缩和加密的研究方面仍还有可以提升的空间。

2　图像的压缩和加密方法

基于混沌置乱的分量融合图像加密压缩方法,经过分解 RGB 分量并将其分别进行 DCT 变换,之后再利用特定的融合方式进行融合,从而获得第一次压缩并加密的输出图像,再对初次加密的结果结合混沌加密技术进行二次加密,最终获得同时压缩并加密的结果。

压缩并加密的流程如图 1 所示。

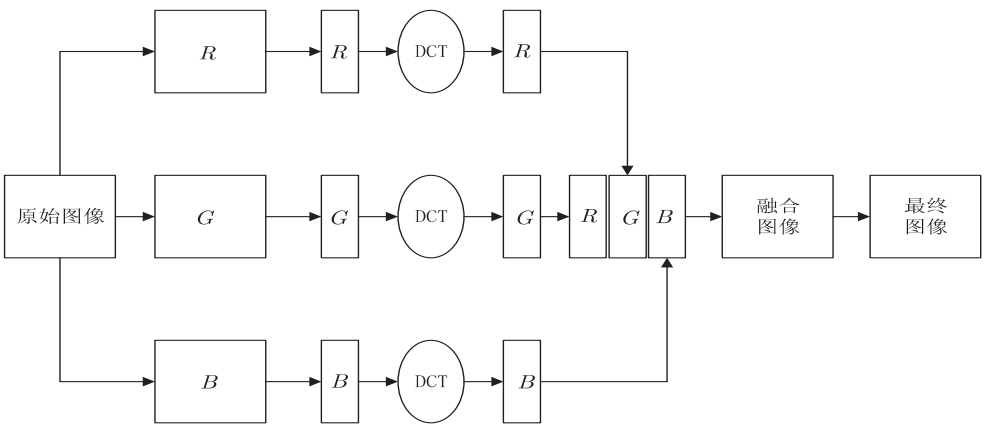

图 1　提出方法的流程

针对两幅目标图像,首先提取出对应的 RGB 分量,再对每个分量分别使用 DCT 变换,然后使变换后的分量图像分别经过一次低通滤波[11],该滤波器的尺寸取决于变换后的数字图像矩阵的尺寸,当原图为 (m,m) 时,则滤波器的尺寸为 $(m/3,m)$,滤波之后的图像需要进行一次固定角度旋转,设置 R 和 B 为 0°,G 为 180°,最后把旋转后的图像融合,得到输出图像。

3　分量融合

3.1　预处理

进行分量融合之前,需要先对数字图像进行预处理,包括提取 RGB 分量、滤去高频部分、缩小尺寸以及 DCT 变换。利用一个适用于彩色静态的 RGB 图像融合新方法来对图像进行压缩,同时压缩的过程也就是加密的过程。先对数字图像提取 RGB 分量,然后再对每个图像分量进行二维 DCT 变换,接着再对变换完的结果进行融合。

解压缩时,接收者通过已经掌握的混沌密钥对得到的图像进行初次还原,获得 DCT 图像,然后利用融合公式进行反向分离,将得到的三条分量进行逆向 DCT 变换,最后将三条分量融合为一幅完整的图像。

3.2　分量提取

首先进行图像预处理,然后进行颜色分量变换,利用数字图像的矩阵变换,对彩色图像进行颜色分量变换,从而提取颜色分量 R、G、B[12]。

之后需要对颜色分量进行处理,使三条分量分别经过一个尺寸为 $[m/3, m]$ 的低通滤波,滤去高频部分并将分量尺寸变换为原始的 1/3,以便进行下一步

的变换和融合,再对其进行 DCT 变换。

3.3 DCT 变换

对预处理后的颜色分量进行 DCT 变换[13],每个颜色分量将作为输入用二维 DCT 公式进行变换,对变换后的结果进行融合。DCT 变换的特点是能使图像的能量集中在少数几个低频系数中。利用前向 DCT 进行压缩,解压缩时则利用逆 DCT 变换(IDCT)。对于绝大多数的图像而言,因为 DCT 系数值都接近于 0,在量化编码的过程中都已被舍去,并且这些系数不会对重建图像的质量产生太大影响。因此,利用 DCT 进行图像压缩可以节约大量的存储空间。

前向 DCT 时,首先将原始图像视为空间函数,令 x 为像素所处的行, y 为像素所处的列,二维 DCT 和 IDCT 分别如式(1)和式(2)所示:

$$X(u,v)=\frac{2}{N}c(u)c(v)\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}x(i,j)\cos\frac{(2i+1)\pi u}{2N}\cos\frac{(2j+1)\pi v}{2N},\quad u,v=0,1,\cdots,N-1 \tag{1}$$

$$x(i,j)=\frac{2}{N}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}c(u)c(v)X(u,v)\cos\frac{(2i+1)\pi u}{2N}\cos\frac{(2j+1)\pi v}{2N},\quad i,j=0,1,\cdots,N-1 \tag{2}$$

3.4 融 合

分别对两幅图像 DCT 变换之后的颜色分量进行旋转和融合,这里分别取 0°,90°和 180°进行操作,为使融合后的图片能拼成一幅图以便编码,把同一幅图片的 R、G、B 分量分别取左、中、右放置。然后再利用融合公式进行融和,即可完成融合过程。图 2 是对一幅原图进行 DCT 变换得到的颜色分量图,式(3)为融合公式。

$$S(p,j)=\frac{s_1(i,j)n_1+s_2(i,j)n_2+s_3(i,j)n_3}{\lambda H}\sqrt{\alpha\beta}$$

$$\begin{cases}n_1=1,n_2=\dfrac{\alpha}{\alpha+\beta},n_3=\dfrac{\beta}{\alpha+\beta},0<p\leqslant\dfrac{H}{3}\\ n_2=1,n_1=\dfrac{\alpha}{\alpha+\beta},n_3=\dfrac{\beta}{\alpha+\beta},\dfrac{H}{3}<p\leqslant\dfrac{2H}{3}\\ n_3=1,n_1=\dfrac{\alpha}{\alpha+\beta},n_2=\dfrac{\beta}{\alpha+\beta},\dfrac{2H}{3}<p\leqslant H\end{cases}$$

$$\alpha=|s_1||s_2||s_3|$$

$$\beta=|s_1\cdot(s_2)^{-1}\cdot s_3|$$

$$i=0,1,\cdots,H/3$$

$$j=0,1,\cdots,H \tag{3}$$

其中, $S(p,j)$ 为融合完成后的图像; $s_1(i,j)$, $s_2(i,j)$, $s_3(i,j)$ 分别为三条颜色分量; λ 为依据先验知识确定的参数; H 为数字图像矩阵水平长度(列数); n_1, n_2, n_3 为随融合过程改变的变量,根据 p 的演化来决定它们的取值;将 s_1, s_2, s_3 的特征融入变换后的图像中,最终获得融合图像。

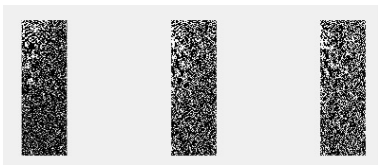

图 2 经过 DCT 变换后的 R、G、B 分量

p 的演化过程:当 s 的列数存在于 0 到 $H/3$ 时,取 p 值为对应的 i 值;当 s 的列数演化到 $H/3$ 到 $2H/3$ 时,对应的 i 值为 $p-H/3$;当 s 的列数演化到 $2H/3$ 到 H 时,对应的 i 值为 $p-2H/3$。

融合完成后的图像同时也拥有了第一层的加密方式,但这种方式并不是万无一失的,特别是在面对已知明文攻击时,虽然难度巨大,攻击者仍然有可能依据得到的明文信息推测出所采用的融合加密方式。为了确保图像信息在网络攻击下的绝对安全性,利用混沌加密技术为加密方法设置了二次加密。

4 混沌加密

4.1 混沌加密技术研究

研究的另一个方面是结合了混沌加密技术并使用依赖于一个或多个私有的第二加密级别的加密密钥。经过对加密性能和资源消耗等各方面的比较分析,最后决定使用混沌加密技术,并利用对已知明文攻击(攻击者能够选择任何他们需要的明文)的方式来测试所提方法的加密性能。

混沌现象是指在非线性动态系统中出现的确定性和类似随机的过程。出现这种过程的非线性动态系统中的设定值和变化值对于混沌现象而言都至关重要,初始条件的微小差异随着混沌现象的发展,到最后会出现截然不同的结果,这种过程是有界的,但不一定收敛。随着混沌动力学的迅猛发展,研究者们也逐渐将混沌技术应用到图像加密领域。混沌加密技术可以加密几乎所有的数据内容,其概念最早是 Fridrich 提出的。随后 Fridrich 又提出了一种使用二维混沌映射的加密思想。此后,更多的研究者围绕混沌在图像加密的应用展开研究,并且取得了一定的成果。

4.2 混沌加密技术的优势

数字图像的混沌加密对比传统的加密算法优势明

显。首先加密适用方法多。将混沌技术用于图像加密的方法有很多,不仅可用传统的加密方法,也可以进行像素值的位置变化;其次易于操作。混沌加密技术对数字图像进行处理的操作简便,只需通过简单的迭代计算和重构就可以进行更有效率的加密工作,易于实现;再次密钥空间选择余地大。混沌加密算法作用于一般实数空间上,通过调整混沌模型可以选择相比传统算法更多的密钥。

成熟的数字图像混沌加密技术主要分为混沌掩盖加密技术和混沌置乱加密技术,两者以不同的方式实现了混沌加密技术。前者把混沌序列当作伪随机序列,对数字图像中的像素值作掩盖动作,生成掩盖信号,解密时在解密端对加密数据使用去混沌序列即可恢复原有的图像。后者则是利用信号在频域中的对应值进行局部或者全局范围内的置乱。置乱的方法主要是选择特定的混沌系统,将混沌系统里的指定参数作为密钥进行像素点位置的重新排序。

4.3 Logistic 映射

根据需要采用 Logistic 混沌加密技术[14]对压缩后的图像进行二次加密。Logistic 混沌加密技术是一种混沌置乱加密方式,将 Logistic 混沌映射产生的混沌序列作为图像置乱网络的置乱地址,Logistic 映射模型如式(4)。

$$X_{n+1} = \mu X_n(1 - X_n) \tag{4}$$

为了得到混沌序列,设计了一种混沌序列生成方法,即首先设定初值,进行 Logistic 迭代生成混沌序列,利用混沌序列生成三位整数作为中间数,再将中间数对 256 求余获得密钥,最后将明文图像与密钥进行异或操作得到密文图像。解密时只需要对密文使用相同密钥进行异或即可。实验中,设初始值 $\mu = 3.77$, $X_0 = 0.278$,利用混沌序列进行混沌加密,加密过程及得到的加密图像见图 3。

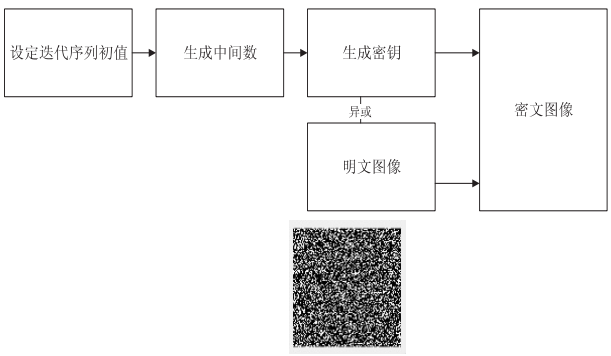

图 3　混沌加密流程及结果

5　结果比较

5.1　压缩性能比较

选取了常用的 JPEG 压缩算法与文中方法在不同压缩比下进行对比,结果见表 1。

表 1　所提方法与 JPEG 的比较

方法	1.0	0.8	0.5	0.4	0.2
JPEG	35.96	34.60	31.07	29.01	22.61
文中方法	37.65	36.19	32.11	30.89	23.31

5.2　抵御黑客攻击

近年来出现了一些针对多类型加密系统的攻击。文中对采用的方法进行探究,并研究它在网络攻击下的可靠性。假设攻击者试图通过实施逆 DCT 图像解密来破解加密图像,单纯对密文图像使用 DCT 逆变换,单纯对密文图像使用逆向 FT 变换[15](傅里叶变换)都无法对加密图像进行破解。由此可知,单纯的截取攻击是无法解密的。现在为了获得更强的安全性,假定黑客通过特殊渠道获取了加密图像和随机的一部分先验编码矩阵,但不知道密钥,并且假定黑客根据已知明文信息可以推测出一幅图像利用了混沌加密方式,则利用随机混沌因子复合 DCT 逆变换进行破解,实验结果表明,即便如此仍然无法有效破解所采用的加密方式。

综上所述,压缩加密方式的安全性达到了既定目标。实验结果如图 4 所示。

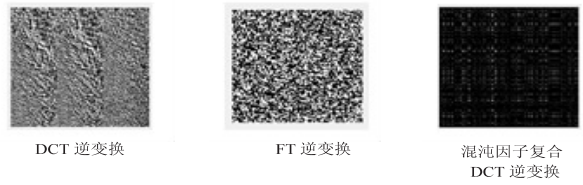

图 4　实验结果

6　结束语

针对图像压缩存在的安全性问题,介绍了一种基于混沌置乱的分量融合图像加密压缩方法。该方法基于 DCT 变换可以有效除去图像中视觉不敏感的高频部分,获得较好的压缩比,有效抵御已知明文的攻击,同时利用抽取 RGB 颜色分量进行 DCT 变换后再旋转和融合的方式,对图像信息完成初始加密。为了进一步提升图像信息的安全性,在前述基础上对初次加密后的图像信息进行了混沌置乱二次加密。经过实验验证,该方法完成了同时加密和压缩,提供了一个彩色图像压缩加密的方案。未来进一步的研究方向是将该方法应用于三维全息域,分析并实现三维空间的压缩和加密。

参考文献:

[1] Hu Wei, Cheung G, Ortega A, et al. Multiresolution graph fourier transform for compression of piecewise smooth images

(下转第 114 页)

25(4):409-417.
[12] Lindell Y, Pinkas B. Privacy preserving data mining[J]. Journal of Cryptology, 2002, 15(3): 177-206.
[13] Fagin R, Naor M, Winkler P. Comparing information without leaking it[J]. Communications of the ACM, 1996, 39(5): 77-85.
[14] Cachin C. Efficient private bidding and auctions with an oblivious third party[C]//Proceedings of the 6th ACM conference on computer and communications security. [s. l.]: ACM, 1999: 120-127.
[15] Atallah M J, Du W. Secure multi-party computational geometry[C]//Workshop on algorithms and data structures. [s. l.]: [s. n.], 2001: 165-179.
[16] Du W, Atallah M J. Secure multi-party computation problems and their applications: a review and open problems[C]//Proceedings of the 2001 workshop on new security paradigms. [s. l.]: ACM, 2001: 13-22.
[17] Li Shundong, Wu Chunying, Wang Daoshun, et al. Secure multiparty computation of solid geometric problems and their applications[J]. Information Sciences, 2014, 282: 401-413.
[18] Li Shundong, Wu Chunying, Wang Daoshun, et al. A secure multi-party computation solution to intersection problems of sets and rectangles[J]. Progress in Natural Science, 2006, 16(5): 538-545.
[19] 郑 强. 不同模型下若干安全多方计算问题的研究[D]. 北京: 北京邮电大学, 2010.
[20] 李顺东, 王道顺, 戴一奇, 等. 两个集合相等的多方保密计算[J]. 中国科学: 信息科学, 2009, 39(3): 305-310.
[21] Frederick R. Core concept: homomorphic encryption[J]. Proceedings of the National Academy of Sciences, 2015, 112(28): 8515-8516.
[22] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169-180.
[23] Wu J H, Zhang P, Shi X B. Research of MA protection based on addition-multiplication homomorphism and composite function technology[J]. Journal of Chinese Computer Systems, 2012, 33(10): 2223-2226.
[24] Li Shundong, Wang Daoshun, Dai Yiqi. Efficient secure multiparty computational geometry[J]. Chinese Journal of Electronics, 2010, 19(2): 324-328.
[25] Goldreich O. Foundations of cryptography: volume 2, basic applications[M]. [s. l.]: Cambridge University Press, 2004.
[26] 李顺东, 戴一奇, 游启友. 姚氏百万富翁问题的高效解决方案[J]. 电子学报, 2005, 33(5): 769-773.

(上接第 109 页)

[J]. IEEE Transactions on Image Processing, 2015, 24(1): 419-433.
[2] Mekhalfa F, Avanaki M R, Berkani D. A lossless hybrid wavelet-fractal compression for welding radiographic images[J]. Journal of X-ray Science and Technology, 2016, 24(1): 107-118.
[3] Sun C, Yang E H. An efficient DCT-based image compression system based on Laplacian transparent composite model[J]. IEEE Transactions on Image Processing, 2015, 24(3): 886-900.
[4] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding[J]. Optics Letters, 1995, 20(7): 767-769.
[5] 龙 敏, 谭 丽. 混沌权值变异的 Huffman 树图像加密算法[J]. 小型微型计算机系统, 2011, 32(12): 2439-2443.
[6] 王 旻, 王方超. 基于矩阵变换的彩色图像加密算法[J]. 微型机与应用, 2010, 29(2): 61-65.
[7] Liu Xingbin, Mei Wenbo, Du Huiqian. Simultaneous image compression, fusion and encryption algorithm based on compressive sensing and chaos[J]. Optics Communications, 2016, 366: 22-32.
[8] 林 青, 戴慧珺, 马文涛. 基于正交基函数神经网络的图像加密算法仿真[J]. 计算机仿真, 2013, 30(10): 416-421.
[9] 彭 川, 李元香. 基于混沌和细胞自动机的图像加密算法[J]. 计算机工程与设计, 2012, 33(7): 2526-2529.
[10] Xu Feihu, Curty M, Qi Bing, et al. Discrete and continuous variables for measurement-device-independent quantum cryptography[J]. Nature Photonics, 2015, 9(12): 772-773.
[11] 吴 燕. 数字水印的高斯低通滤波鲁棒性测试[J]. 网络与信息, 2010, 24(8): 42.
[12] 李俊峰. 基于 RGB 色彩空间自然场景统计的无参考图像质量评价[J]. 自动化学报, 2015, 41(9): 1601-1615.
[13] 丛 爽, 蒲亚坤, 王军南. DCT 图像压缩方法的改进及其应用[J]. 计算机工程与应用, 2010, 46(18): 160-163.
[14] 马 婷, 陈农田. 基于 Logistic 混沌加密的 NSCT-DWT-SVD 彩色水印算法[J]. 现代电子技术, 2016, 39(10): 37-41.
[15] 邓家斌, 胡娟莉. 快速傅立叶变换的图像数据压缩算法[J]. 电脑知识与技术, 2009, 5(21): 5766-5767.