

基于混沌的图像压缩加密算法研究

林 纯¹, 王建平¹, 马卫国¹, 陆国平²

(1 南通大学 电子工程系, 江苏 南通 226019; 2 江苏信息职业技术学院, 江苏 无锡 214153)

摘 要: 提出了一种结合 DCT 变换压缩技术的混沌图像加密算法. 先对原始图像进行压缩处理, 然后用由复合混沌系统生成的加密矩阵先后对压缩后的图像进行位置置乱、灰度值替代加密处理. 理论分析和实验结果表明, 该算法既能有效地减小图像的存储容量, 提高数据的传输速度, 又具有良好的加密性能.

关键词: 混沌系统; 数字图像; 压缩; 加密

中图分类号: TP391

文献标识码: A

文章编号: 1000-7180(2013)03-0005-03

Study on Chaotic Encryption Algorithm for Images after Compression

LIN Chun¹, WANG Jian-ping¹, MA Wei-guo¹, LU Guo-ping²

(1 School of Electrical Engineering, Nantong University, Nantong 226019, China;

2 Jiangsu College of Information Technology, Wuxi 214153, China)

Abstract: A chaotic image encryption algorithm, combined with DCT transform compression technology, is presented here. The soul of the new algorithm is to compress the original image before encryption. The encryption matrixes generated by the hybrid chaotic system are used to deal with the compressed image, with the methods of position scrambling and grayscale value alternative encryption. Theoretical analysis and experimental results show that the algorithm can not only effectively reduce the image of storage capacity, improve the speed of data transmission, but also has good encryption performance.

Key words: chaotic system; digital image; compression; encryption

1 引言

图像作为一种主流的信息载体, 已成为人们进行交流的重要手段, 而图像信息的安全问题也变得日益严峻^[1]. 因此, 信息安全问题已上升为人们关注的焦点^[2], 其中多媒体信息安全也已成为学术界和工业界共同关注的新的研究方向^[3]. 在网络传输中, 人们针对图像信息加密问题展开一系列研究工作^[4].

混沌系统可以用确定的微分方程描述, 对初值具有极端的敏感性. 混沌轨迹看似随机而内部却包含着一定的有序性. 如上优良的性质决定了混沌系

统非常适用于图像信息加密中. 文献[5]提出了一种应用 Henon 超混沌系统改进的图像加密算法, 文献[6]提出了一种真彩图像和视频加密的新方案, 文献[7]也提出了一种基于混沌系统的图像加密改进算法. 他们都从信息安全的角度提出了有效的混沌加密方法, 但是却都没有考虑到图像信息本身的特点.

一般的图像数据量都较大, 给传输和存储都会带来一定的负担. 如果能进一步利用图像数据冗余度高、像素间相关性强的特点, 在传输、存储以及加密处理前, 先对图像数据进行合理地压缩, 可以在不影响图像质量要求的基础上提高传输速度、减少存储空间. 本文基于这点, 提出了一种先用 DCT 变换

收稿日期: 2012-06-10; 修回日期: 2012-07-19

基金项目: 国家自然科学基金项目(61174066); 江苏省高校自然科学基金项目(10KJD120002, BK2010275); 南通市自然科学基金项目(K2010017, K2011023)

进行压缩后再进行图像加密的方法,并通过主客观的性能分析说明其可行性及其诸多优点.

2 加密算法研究

2.1 Logistic-sine 复合混沌系统映射

Logistic-sine 复合混沌映射的具体定义如下:

$$\begin{cases} x_{n+1} = ux_n(1-x_n) \\ y_{n+1} = \sin^2(r \arcsin \sqrt{y_n}) \end{cases} \quad (1)$$

其中 x_n 是 Logistic 混沌映射状态, y_n 是 sine 混沌映射状态,当 $3.569945672 \leq u \leq 4$, $r > 1$ 时,选取合适初值 $0 < x_0 < 1$,系统产生混沌.利用 Logistic-sine 复合混沌映射对初值的敏感性可以获得相应的混沌序列,经变换处理后可对图像信息进行加密.

2.2 DCT 变换

用 DCT 变换能将一组光强数据转换成频率数据. DCT 变换公式如下:

$$F(u, v) =$$

$$c(u)c(v) \frac{2}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos\left(\frac{2x+1}{2N}u\pi\right) \cos\left(\frac{2y+1}{2N}v\pi\right) \quad (2)$$

式中, $x, y, u, v = 0, 1, \dots, N-1$,

$$c(u) = c(v) = \begin{cases} \frac{1}{\sqrt{2}} & u = 0, v = 0 \\ 1 & \text{其他} \end{cases}$$

x, y 代表图像矩阵的坐标位置, $f(x, y)$ 代表图像数据矩阵内的对应坐标位置的像素值, u, v 代表 DCT 变换后矩阵的坐标位置, $F(u, v)$ 则代表 DCT 变换后矩阵内的数值.

由于人眼对高频的数据不太敏感,所以若对高频的数据作适当处理,再利用 DCT 反变换转回原来形式的数据时,数据量虽有所压缩,但是视觉效果相差得并不大.在对图像还原质量要求不高的场合,可以采用 DCT 变换对数据量进行适当压缩后再加密传输,以提高加解密速度、减少数据总的传输时间、减小图像数据的存储空间.

2.3 加密方案

文中提出的加密方案是基于对数字图像先用 DCT 变换进行分块压缩处理的基础上再用混沌矩阵进行加密的,加密矩阵源于上述的 Logistic-sine 复合混沌系统,具体的实施步骤如下:

(1)取初值 $x_0 = 0.1, y_0 = 0.3$, 系统参数 $u = 3.5699458, r = 2.23$, Logistic 映射和正弦混沌映射

均迭代 $n = 1000$ 次后取数据流,得到 $\{x_k, y_k, k = 1, 2, \dots, N \times N\}$ 序列,同时生成混沌矩阵 WX, WY .

(2)选取适当的 DCT 变换系数,对原始图像所对应的二维矩阵 A 进行压缩处理,得到压缩图像对应的二维矩阵 B .

(3)以混沌矩阵 WX 作为位置置乱矩阵,将二维矩阵 B 进行地址变换,得到一次加密矩阵 $A1$.

(4)取混沌矩阵 WY 中的每一个元素小数点后第 6, 7, 8 位组合成新的自然数矩阵,对 $A1$ 进行灰度值替代加密处理,即可得到密文矩阵 $A2$. 具体的加密流程如图 1 所示.

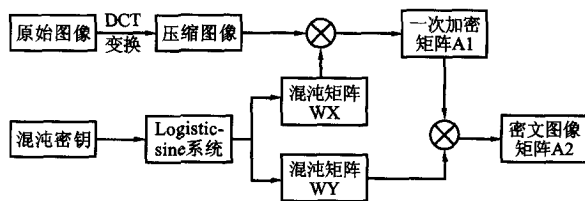


图1 数字图像的混沌加密流程图

2.4 仿真效果

将系统初值 x_0, y_0 参数 r 和预迭代次数 n 作为同步密钥,选择大小为 512×512 的数字图像“lena.jpg”进行压缩、加密和解密算法测试,解密是加密的逆过程,得到 MATLAB 仿真效果图如图 2 所示.加密后的图像如图 2(c)所示变得无法识别,而当取得正确的密钥解密后,又能有效地恢复出原始的图像来,如图 2(e)所示,解密图像和原始图像相比,肉眼下几乎看不出什么差别,效果良好.

3 加密性能分析

如前文所述,当取得正确的密钥时,能正确得解密出原始的图像来.所取的原始图像“lena.jpg”大小为 84.4KB,正确解密的图像大小为 10.2KB,解密图像的大小不到原始图像的 $1/8$,大大减小了存储空间,在网络传输时也能大幅度地提高传输速度.如下进行密钥空间、密钥敏感性、抗噪声性能和抗裁剪能力分析,说明该算法的优越性能.

3.1 密钥空间分析

在该算法中,同步密钥由 x_0, y_0, u, r, n 组成,每个参数精度都可达 10^{-16} ,密钥空间可达 10^{80} ,在实际使用过程中,即使精度稍有降低,密钥空间也仍然很大,足以抵抗穷举攻击.从直方图分析角度上看,尽管原始图像的像素值如图 2(b)所示分布不均,但密文图像的像素值如图 2(d)所示分布趋于平均,从密文的直方图上无法得到原始图像的统计特性.

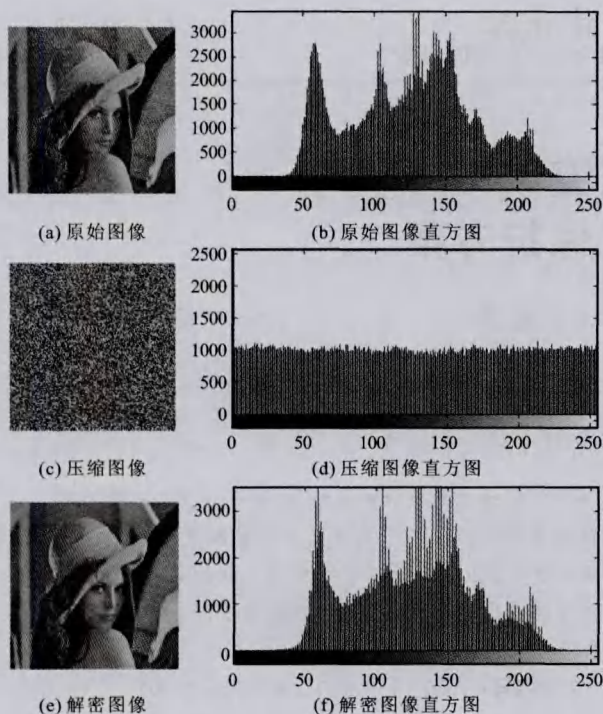


图2 数字图像的加解密效果图及直方图

3.2 密钥敏感性

取初值 $y_0 = 0.3$ 和系统参数 $u = 3.5699458$ 作为加密密钥,当解密密钥 y_0 和 u 分别偏差 10^{-10} 时解密图像如图3所示.从图3中可以看出,解密密钥微小的偏差就能造成解密出来的图像面目全非,从中完全看不出原始图像的任何痕迹.

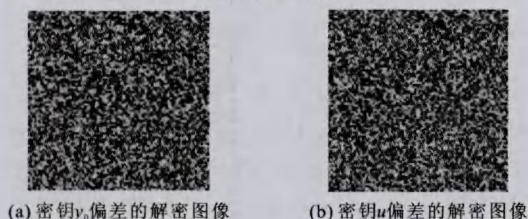


图3 密钥发生微小变化时的解密效果图

采用参数均方误差(MSE)和峰值信噪比(PSNR)作为评价解密图像偏离原始图像的误差指标.具体定义如下:

$$MSE = \frac{1}{N_1 N_2} \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} (W(i,j) - M(i,j))^2 \quad (3)$$

$$PSNR = 10 \lg \left(\frac{f_{\max}^2}{MSE} \right) \quad (4)$$

式中 i, j 表示二维图像矩阵的行、列坐标值, $N_1 \times N_2$ 为图像尺寸, M 为原始图像, W 为解密图像, $f_{\max}$ 取 255. 当 PSNR 值在 28dB 以上时,图像恢复的质量较好.经计算分析,正确解密出来图像的 PSNR = 28.6113,恢复出来的图像和原图像虽然不是和原始图像完全相同,但视觉上看不出差别,图像恢复的质

量较好;而密钥发生微小变化时的解密图像,如图3(a), PSNR = 10.7158dB; 图3(b), PSNR = 9.4461dB, 均远小于 28dB, 当对其他密钥分别取微小偏差解密时,得到的解密图像 PSNR 均远小于 28dB, 这也说明了该算法对密钥具有较好的敏感性.

3.3 抗噪声性能分析

在图像信息的传输过程中,多少会受到噪声信号的影响.为检测该加密算法的抗噪声攻击性能,对密文图像加入 20% 的椒盐噪声后对其进行解密.解密效果如图4(a)所示,解密图像虽然有些瑕疵点,但还是能较清楚地反映出原图像的轮廓.由此可判断,该算法具有良好的抗噪声攻击性能.

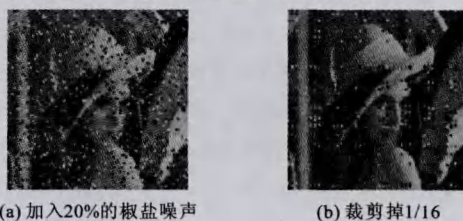


图4 加入噪声和裁剪后的解密效果图

3.4 抗破损性能分析

为测试该算法的抗破损性能,将密文图像裁剪掉 1/16 后,观察其解密效果如图4(b)所示.解密图像虽然有少许瑕疵点,但也还是能较清楚地分辨出图像的轮廓.由此可判断,该算法具有良好的抗破损攻击性能.

4 结束语

本文提出了一种基于 Logistic-sine 复合混沌,在保证一定图像质量的前提下压缩了图像的存储空间,有效地提高了图像的传输速度.

参考文献:

- [1] 卿斯汉. 安全协议[M]. 北京:清华大学出版,2005.
- [2] 戴宗坤. 信息安全应用基础[M]. 重庆:重庆大学出版社,2005.
- [3] Christine I P, Edward J D. Digital watermarking: algorithms and applications[J]. IEEE Signal Processing Magazine, 2001(7): 33-46.
- [4] Fridrich J. Image encryption based on chaotic maps[J]. Man and Cybernetics, 1997, 2(1): 1105-1110.
- [5] 乐鸿辉,李涛,石磊. 应用 Henon 超混沌系统改进的图像加密[J]. 计算机应用,2011,31(7):1909-1911.
- [6] 林纯,盛苏英,陆国平. 真彩图像和视频加密新方案的研究与实现[J]. 微电子学与计算机,2012, 29(6):113-116.

(下转第 11 页)

出版社,2003.

- [2] Lan P. Of graphs and coffi grounds; decompiling Java [R]. McGill UNiversity School of Computer Science, Sable Research Group, 1998.
- [3] Sureshot Software Co., Ltd. Cavaj - the java decompiler[EB/OL]. (2002-07-11)[2012-06-25]. <http://www.bysoft.se/sureshot/cavaj/>, v1.
- [4] Cowley M. Front End plus - the java decompile[EB/OL]. [2012-05-17]. http://www.softpile.com/Development/Java/Review_03171_index.html, v1.00, 2001.
- [5] Lemaire B. NMI's java class viewer - the java decompiler[EB/OL]. [2012-06-20]. <http://www.jreveal.org/cgi-bin/resource.pl?resid=4397>, v4.7.

- [6] Peterson W W, Kasami T, Tokura N. On the capabilities of while, repeat, and exit instructions[J]. Commun. ACM, 1973, 16 (8): 503 - 512.
- [7] Wu Jiehong, Chang Guiran, Li Jia. A scheme for protecting mobile agents based on combining obfuscated data and time checking technology[C]// Proceedings of the 3rd International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Kaohsiung, Taiwan, 2007(1):221-224.

作者简介:

吴杰宏 女,(1971-),博士,副教授.研究方向为移动代理的安全、动态频谱存取协议及算法.

(上接第7页)

- [7] 盛苏英,吴新华. 一种混沌图像加密算法的研究与改进[J]. 微电子学与计算机,2010, 27(10): 61-64.

作者简介:

林 纯 女,(1980-),硕士,讲师.研究方向为混沌控制.

王建平 女,(1981-),硕士,讲师.研究方向为图像处理.

马卫国 女,(1976-),博士,讲师.研究方向为混沌同步、保密通信.

陆国平 男,(1965-),博士,教授.研究方向为非线性控制、智能控制.