联合二维 logistic 混沌映射与比特重组的彩色图像加密算法

庹朝永[1] 秦 拯[2] 黎 谦[2]
(湖南机电职业技术学院 长沙 410151)[1] (湖南大学信息科学与工程学院 长沙 410082)[2]

摘 要 通常的彩色图像加密算法未能充分考虑 *RGB* 各颜色分量之间的内在联系,抵抗统计分析能力不强。为进一步增强图像置乱程度与加密安全性,在结合混沌置乱的基础上,提出一种新的彩色图像加密算法。算法首先利用二维 logistic 映射产生随机性很强的伪随机序列进行像素置乱,然后将 *RGB* 3 种颜色分量视为一个整体,并联合比特异或与随机重组对各像素值进行灰度变换,最后对各 24 位像素值进行 *RGB* 重新分割得到加密图像。仿真结果表明,该算法置乱效果好,相较于通常的彩色图像加密方案,具有更少的时间开销与更好的安全性。

关键词 图像加密,二维 logistic 混沌映射,比特重组,彩色图像
中图法分类号 TP309.7 **文献标识码** A

Color Image Encryption Algorithm Based on 2D Logistic Chaotic Map and Bit Rearrange

TUO Chao-yong[1] QIN Zheng[2] LI Qian[2]
(Hunan Mechanic & Electric Polytechnic, Changsha 410151, China)[1]
(School of Information Science and Engineering, Hunan University, Changsha 410082)[2]

Abstract Usual color image encryption algorithms fail to take full account of the intrinsic relationship between the RGB color components and have unsatisfactory statistical analysis resistance capabilities. To enhance image scrambling degree and security, a new color image encryption algorithm was proposed based on mixed chaotic scrambling. First, the original image is scrambled by use of pseudo-random sequence generated by 2D logistic maps. Then, the R, G, B components are assembled into a whole and the extended pixels are disturbed by exploiting bit XOR operation and random rearrange. Finally, the encrypted image is obtained by repartitioning RGB components in extended 24-bit pixel. Experiments show that the proposed encryption scheme has good scrambling effectiveness, less time consumption and better security compared with some common color image encryption schemes.

Keywords Image encryption, 2D logistic chaotic map, Bit rearrange, Color image

1 引言

随着多媒体信息处理技术和国际互联网的飞速发展与广泛普及,经由网络环境的信息泄露、数据篡改、信息窃取等已日趋严重。如何保护实时环境数据通信安全已经成为亟待解决的问题。然而由于数据量大、相邻像素相关性强等特点,导致传统加密方法不完全适合于图像加密[1]。自 1989 年英国数学家 Mattllews 首次明确提出混沌加密思想以来[2],混沌系统因其优良的初值敏感性和伪随机特性,已广泛应用于数字图像加密系统设计。实际上,现实世界中更多的客观物体以彩色形式呈现,因而彩色图像加密系统更具实际价值[3,4]。现有部分彩色图像加密算法将 *RGB* 彩色图像的三基色分量图像看成是亮度图像,分别用于对各基色图像进行加密处理[5-7]。这些加密算法没能考虑到彩色图像 *RGB* 各颜色分量之间的内在相关性,算法加密效果不好。为扩大一维混沌加密算法的密钥空间,增强加密系统的安全性,张燕等提出一种基于三维混沌系统的图像加密方法[8]。该算法将混沌系统产生的密钥序列分别作用于 *RGB* 三原色,扰乱三原色空间的相关性,同时将密文中的像素值嵌入到密钥发生器中间,并在加密算法中引入密文反馈算法,达到良好的加密效果,然而该算法计算强度与空间需求偏高。陈国亮设计了一种基于 Lorenz 映射的彩色图像加密方案[9],其采用 Lorenz 高维混沌映射进行图像加密,利用 Lorenz 混沌映射分别生成用于像素位置置乱的位置矩阵和用于像素值变换的灰度矩阵,然后通过位置置乱和像素值变换来实现对彩色图像的加密操作。但该方案在加密过程中要对各像素值 *RGB* 颜色进行分离操作,这割裂了 *RGB* 分量间的相关性。为充分降低彩色图像 *RGB* 分量的相关性,增强加密算法的安全性,本文在结合二维 logistic 混沌映射的基础上提出一种彩色图像加密新算法。该算法首先利用二维混沌序列进行位置置乱,然后将 *RGB* 各颜色分量看成一个整体,从而将 *RGB* 彩色图像转换为一扩展的 24 比特灰度图像,再进一步实施像素比特异或和随机重组,

到稿日期:2012-10-28 返修日期:2013-03-04 本文受国家自然科学基金项目(61070194,61272546),湖南省科技计划项目(2010GK3194,2011FJ2003)资助。

庹朝永(1962-),男,副教授,主要研究方向为自动控制、多媒体技术,E-mail:hnjstcy@126.com;秦 拯(1969-),男,博士,教授,主要研究方向为信息安全、计算机网络、项目管理;黎 谦(1988-),硕士生,主要研究方向为信息安全、大数据处理。

以获得加密彩色图像。该算法计算开销小，并能获得好的加密置乱效果。

2 logistic 混沌映射系统

混沌是一种非线性无规则的运动，是在确定性非线性系统中不需附加任何随机因素也可出现的一种内在随机性，因此其伪随机行为能够准确再生。如一维 logistic 映射从数学形式上来看是一个非常简单的混沌映射，该类系统具有极其复杂的动力学行为，其数学表达式如下：

$$x_{n+1}=\mu x_n(1-x_n) \tag{1}$$

当 $\mu\in[3.569\ 945\ 67,\cdots,4]$，$x_k\in(0,1)$时，logistic 映射呈现混沌态。

混沌系统的这些特性与密码学要求的扩散、置乱和随机特性相吻合，在保密通信领域的应用非常广泛。但部分图像加密方案采用了一维混沌系统，因此其安全性不高，由于二维 logistic 映射具有一维 logistic 映射简单的形式，又具有多维混沌系统多参数、行为复杂的特点，本文利用二维 logistic 映射进行图像加密处理。二维 logistic 映射的动力学方程如下。

$$\begin{cases}x_{n+1}=\mu\lambda_1 x_n(1-x_n)+\gamma y_n\\ y_{n+1}=\mu\lambda_2 x_n(1-y_n)+\gamma x_n\end{cases} \tag{2}$$

其动力学行为是由其中的参数 μ、λ_1、λ_2、γ 来控制的，通常取 $\mu=4$。当 $\lambda_1=0.9$、$\lambda_2=0.9$、$\gamma=0.1$ 时，经过计算得到二维 logistic 系统处于混沌状态[10]。

3 彩色图像加密算法

为充分扰乱彩色图像 *RGB* 分量的相关性，本文提出一种基于二维混沌映射与比特随机重组的彩色图像加密算法。算法首先将 *RGB* 分量视为一个整体，以将彩色图像转换成一扩展的灰度图像，然后利用二维 logistic 映射优良的伪随机特性与行为高复杂性，对彩色图像进行位置置乱，并结合比特异或与随机重组进行像素扩散。

3.1 基于二维 logistic 映射的像素位置置乱

基于 2D logisitc 映射的彩色图像位置置乱过程描述如下。

步骤 1　读入大小为 $m\times n$ 的彩色图像 I。

步骤 2　初始化 logistic 映射控制参数：$\mu=4$，$\lambda_1=0.9$，$\lambda_2=0.9$，$\gamma=0.1$，并初始迭代映射：$k_0=300$，给定密钥 $key_1=\{x_0,y_0\}$，其中 x_0、y_0 为混沌映射的两个初始值。

步骤 3　以密钥 key_1 为初始值，由式(2)迭代映射 $m\times n+k_0$ 次，生成 $m\times n+k_0$ 对混沌序列值，舍弃 k_0 对值，得到 $m\times n$对的混沌序列值，并将其分别存储于大小为 $m\times n$ 的一维数组 P 和 Q 中。

步骤 4　对 P 和 Q 中的元素做如下运算：

$$f(t)=\mathrm{mod}(\lfloor t\times 10^{15}\rfloor,10^6),t\in P\ \text{or}\ t\in Q \tag{3}$$

得到两个整数数组 P'、Q'。

步骤 5　通过对数组 P'、Q'进行排序以生成两个长度为 $m\times n$ 的一维伪随机序列 P''、Q''，其元素值取[0，$m\times n-1$]内不等的整数。

步骤 6　对一维随机序列 P''、Q''中的各元素 $p''(k)$、$q''(k)$ 实施式(4)所示的变换，并将其映射为大小为 $m\times n$的二维置乱矩阵 X、Y。

$$\begin{cases}x(i,j)=\mathrm{mod}(p''(k),m)\\ y(i,j)=\mathrm{mod}(q''(k),n)\\ i=k/n,j=\mathrm{mod}(k,n)\\ k=0,1,\cdots,m\times n-1\end{cases} \tag{4}$$

式中，符号“/”表示求商运算，$x(i,j)$、$y(i,j)$分别为二维置乱矩阵 X、Y 的元素。

步骤 7　利用置乱矩阵 X、Y 对图像 I 进行位置置乱，得到置乱图像数据 I'。

3.2 结合比特异或与随机重组的像素值变换

图像置乱破坏了图像原像素的相邻像素点的相关性，但是像素点的灰度值并没有改变，即图像直方图并没有改变。为降低 *RGB* 各分量间的相关性，进一步利用异或操作与 logistic 混沌映射对置乱后的扩展的图像数据 A'进行灰度变换，以提高加密效果，具体由以下几个步骤构成。

步骤 1　对置乱图像 I'各像素 *RGB* 分量进行以下异或操作，得到异或后各像素的 $R'G'B'$分量。

$$\begin{cases}R'=R\otimes G\\ B'=G\otimes B\\ G'=R\otimes G\otimes B\end{cases} \tag{5}$$

步骤 2　将异或后 *RGB* 分量组装成一个 24 比特的整体，于是彩色图像被扩展为一幅 24 比特的扩展灰度图像。

步骤 3　给定密钥 key_2，以 key_2 为初始值，利用式(1)生成混沌序列 S，且其元素值取[0，23]内不等的整数。

步骤 4　利用混沌序列 S 对扩展灰度图像各 24 比特像素值进行随机置乱，再将置乱后的 24 比特像素依次重新组装成新的 *RGB* 分量。

步骤 5　重复以上步骤，直到所有像素处理完毕，即得到加密彩色图像 I''。

3.3 解密算法

解密过程是加密过程的逆过程，只需给定相同的混沌系统密钥即可，主要由以下几步完成。

步骤 1　给定与加密过程相同的密钥 key_1、key_2，与加密过程相同，由密钥 key_1 生成置乱矩阵 X、Y。

步骤 2　由置乱矩阵 X、Y 对加密彩色图像 I''进行像素位置逆置乱，得中间图像 $\bar{I}$。

步骤 3　对中间图像 $\bar{I}$ 的各 $R'G'B'$分量实施如式(6)所示的异或操作，并将其组装成一个 24 比特的整体，得到扩展的 24 比特扩展灰度图像。

$$\begin{cases}R=G'\otimes B'\\ B=R'\otimes G'\\ G=R'\otimes G'\otimes B'\end{cases} \tag{6}$$

步骤 4　利用密钥 key_2 生成伪随机序列 S，以对扩展灰度图像各 24 比特像素值进行逆置乱，再将逆置乱后的 24 比特像素依次重新组装成 *RGB* 分量。

步骤 5　重复以上步骤，直到所有像素处理完毕，即得到解密彩色图像 I。

4 仿真实验与性能分析

实验中选取大量大小为 256×256 的 *RGB* 彩色图像进行测试，图 1 以 peppers 图像为例给出了算法加密效果图，给出了加密前后的图像直方图，加密后图像的灰度直方图变化较大，其灰度分布比较平坦，同时人眼从加密图像(见图 1(b))

中也难以察觉出原始图像的任何信息，这说明加密图像有较好的视觉加密效果。

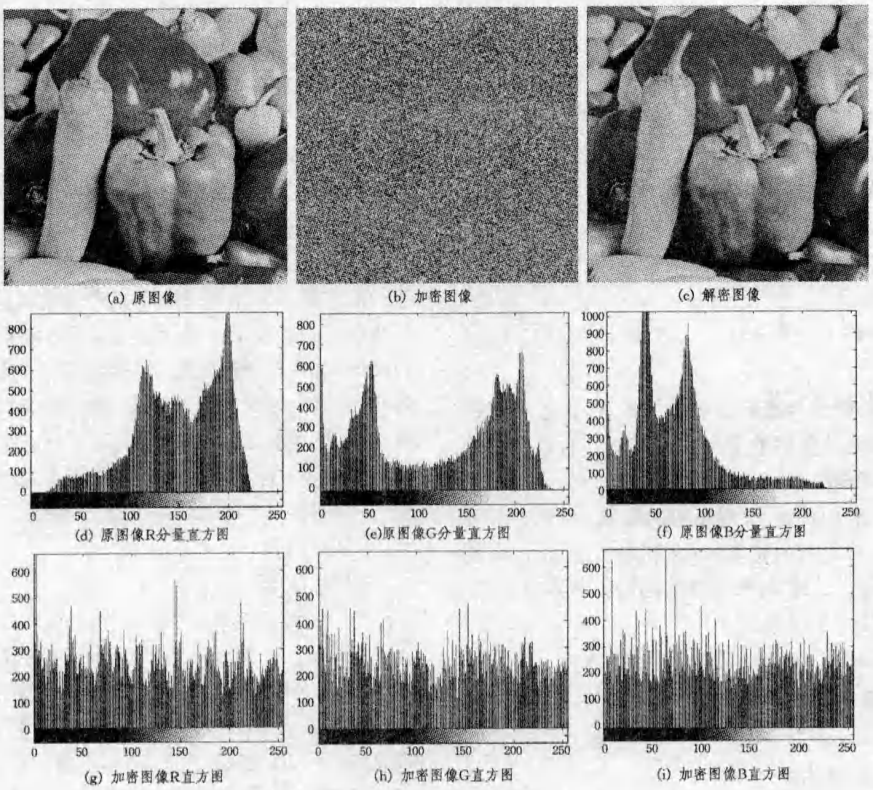

图 1　图像加密效果图

4.1　密钥空间分析

一个良好的加密方案应有足够大的密钥空间以挫败穷举攻击。本文基于彩色图加密算法中以二维 logistic 混沌系统的初始值 key_1 和一维 logistic 混沌初始值 key_2 为密钥，若精度为 10^{-16}，则该加密算法密钥空间可达 10^{48}，密钥空间足够大，可以有效阻止各种暴力攻击试图。

4.2　密钥敏感性分析

以图 1(b)的加密图像为例，图 2 给出了密钥微小变化时的解密仿真实验结果，其中图 2(a)和图 2(b)分别是密钥 key_1 和 key_2 最后一位有效数字不同时的解密图像。由图 2 可见，即使密钥 key_1 和 key_2 有微小的变化，也会生成完全不同的加密图像。由此可知，该加密算法中任何一个密钥即使存在很细小的改变，也不能正确解密图像，这正是 logistic 混沌系统对初值的敏感性所致。

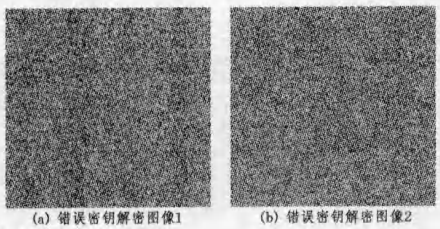

图 2　密钥敏感性分析

4.3　相邻像素相关性

以 lena 图像为例，从原图像和加密图像中分别随机选取 2000 对相邻像素，计算其相关性，并给出了与文献[6]方法的测试对比，实验结果如表 1 所列。从表 1 中可以发现，原始明文图像相邻像素的相关性很强，而加密图像相邻像素相关性很低，几近于 0，远低于文献[6]方案的密文相邻像素相关性。这表明该加密算法显示出了比文献[6]方案更为优越的加密效果，原始图像的统计特性已扩散到随机加密图像之中。

表 1　图像相邻像素相关性对比分析

		R 分量	G 分量	B 分量
明文图像		0.9744	0.9727	0.9551
加密图像	本文方案	0.0061	0.0035	0.0028
	文献[6]	0.00972	0.0238	0.00641

结束语　结合二维 logistic 映射与比特随机重组，本文提出一种新的彩色图像加密方案，即利用具有强随机性的二维 logistic 映射对彩色图像进行置乱，并运用比特异或与随机重组将 *RGB* 颜色分量作为一个整体进行灰度变换。实验结果表明，该方案置乱效果好，很好地打乱了原图像像素的相关性与 *RGB* 分量的相关性，算法密钥空间大，计算开销小，可有效应用于实际网络环境图像通信安全领域。

参 考 文 献

[1]　黄伟琦，陈志刚，梁涤青，等. 基于多混沌系统的医学图像加密算法[J]. 计算机科学，2012，39(12)：261-263，299

[2]　Matthews R. On the derivation of a chaotic encryption algorithm [J]. Cryptologia，1989，13(1)：29-42

[3]　Mao Yao-bin，Chen Guan-rong，Lian Shi-guo. A novel fast image encryption scheme based on 3d chaotic baker maps [J]. International Journal of Bifurcation and Chaos，2004，14(10)：3613-3624

(下转第 308 页)

如图7和图9所示，本文算法稍优于PCA和PPCA单一特征分割方法。主要原因在于PCA分割方法直接对原始人体运动序列进行降维后提取其主要成分，没有考虑其运动姿态帧间的约束关系。PPCA单一特征分割方法需结合PCA子空间分析和高斯建模，实现起来较PCA方法复杂；此方法分割的结果虽比PCA方法好，但对模糊歧义区间分析不够准确，导致精准度有所欠缺。相比之下，本文算法提取的双特征集能够较全面地反映运动特性，且特征之间对运动语义表达具有互补性，从而得到了较好的分割效果。

表3和表4的两组对比数据显示，本文算法对不同子区间误分率均在6%以内，明显小于PCA分割。对于中等帧长的突兀跳变数据，本文算法误分率要稍好于PPCA；对于较复杂的运动数据，本文算法能够获得较多的精准分割区间。综合两组数据来看，本文算法分割性能整体略优于PCA和PPCA单一特征分割方法。本文算法利用双特征仔细分析运动数据，具有较好的直观性和概括性，且后续通过GMM方法对待定区域进行细分割，提高了整体运动分割精度。

从以上对比实验可以看出，针对相邻运动片段的过渡区间，提取单类特征后分割的结果往往不够准确。相比之下，基于双特征相结合的运动分割方法可以进一步对过渡区间进行判别归属，从而达到较为满意的分割结果。本文提出的方法，可以明显地检测到不同运动序列转折的跳变分割点。对于分割精度要求不高的序列，可以直接采用本文第4.1节所提出的基于子区间标准差阈值限定的粗分割。对于稍微复杂的序列，通过GMM判别准则处理待定区间，进而分配到相邻区间，可以得到较为精准的分割点。本文提出的算法在运动分割中具有较好的适用性，但也存在如下限制：1)对于剧烈跳变的短周期运动序列可能达不到理想的分割效果；2)对于不同空间位置的同类型运动，提取得到的2组规格化特征近似，算法会存在一定程度的误分割。

结束语 针对相邻运动片段的过渡区间存在部分运动序列的归属歧义，本文提出了一种结合双特征与高斯混合模型的运动分割算法。该算法通过选择角度与距离双特征，利用概率主成分分析(PPCA)降维，建立规格化的综合特征函数，采用基于子区间标准差阈值限定方法将原始运动序列粗分割为可信区域与待定区域；对于待定区域，利用高斯混合模型(GMM)方法对其进行进一步判别归属，从而最终达到细分割的目的，仿真实验验证了算法的有效性。同时，本文中所提出的粗分割的方法可以直接应用于对分割精度要求不是很高的场合。本文算法对于3000帧左右长度的运动序列可以得到较理想的效果，但是对于过长的运动序列，分割效果相比其他方法，优势不明显。主要原因在于后续分割的数据来源于提取的两组不同类特征，这两组特征能够较好地反映人体运动的逻辑性以及相关性，处理起来简单、直观，但是由于特征信息量还有所欠缺，存在对运动细节表现能力不足的缺点，对过复杂的运动序列的分割效果不够理想。在后续研究工作中，我们拟对人体运动分割进行进一步的深入研究，主要包括：

1)结合全局与局部运动姿态序列分析建模，从空间邻域的角度考虑运动语义分割；

2)研究核空间中运动姿态的距离度量理论，用于估算运动捕获数据中不同运动姿态的相似度。

参考文献

[1] 王天树，郑南宁，徐迎庆. 人体运动非监督聚类分析[J]. 软件学报，2003，14(2)：209-214

[2] Beaudoin P，Coros S，Panne M V D，et al. Motion-motif graphs [C]// Proc. ACM SIGGRAPH/Eurographics Symposium on Computer Animation. 2008：117-126

[3] Barbic J，Safonova A，Pan J Y，et al. Segmenting motion capture data into distinct behaviors [C]// Proc. Graphics Interface. 2004，62：185-194

[4] 杨跃东，王莉莉，郝爱民. 运动串：一种用于行为分割的运动捕获数据表示方法[J]. 计算机研究与发展，2008，45(3)：527-534

[5] Bouchard D，Badler N. Semantic segmentation of motion capture using laban movement analysis [C]// Proc. Intelligent Virtual Agents. 2007：37-44

[6] 肖俊，庄越挺，吴飞. 三维人体运动特征可视化与交互式运动分割[J]. 软件学报，2008，19(8)：1995-2003

[7] Kahol K，Tripathi P，Panchanathan S. Gesture segmentation in complex motion sequences [C]// Proc. IEEE International Conference on Image Processing. 2003：105-108

[8] Pradhan G N，Li C J，Prabhakaran B. Hierarchical indexing structure for 3D human motions [C]// Proc. on Multimedia Modeling. 2007，4351：386-396

[9] Endres D，Christensen A，Omlor L，et al. Emulating human observers with bayesian binning：segmentation of action streams [J]. ACM Trans. Appl. Percept.，2011，8(3)：1544-3558

[10] Tipping M E，Bishop C M. Probabilistic Principal Component Analysis[J]. Journal of the Royal Statistical Society：Series B(Statistical Methodology)，1999，61(3)：611-622

[11] CMU Graphics Lab Motion Capture Database[OL]. http://mocap.cs.cmu.edu/

(上接第302页)

[4] Mazloom S，Eftekhari-Moghadam A M. Color image encryption based on coupled nonlinear chaotic map [J]. Chaos，Solitons & Fractals，2009，42(3)：1745-1754

[5] 卢辉斌，刘海莺. 基于耦合混沌系统的彩色图像加密算法[J]. 计算机应用，2010，30(7)：1812-1814，1817

[6] 何松林. 基于混沌序列的数字彩色图像加密算法[J]. 计算机工程，2011，37(10)：114-116

[7] 卢辉斌，郑恒娜，韩秀峰. 基于Lorenz三维混沌序列的彩色图像加密算法[J]. 电子测量技术，2008，31(11)：34-36

[8] 张燕，黄贤武，刘家胜. 基于三维混沌系统的彩色图像加密新算法[J]. 计算机工程与应用，2008，44(20)：202-205

[9] 陈国亮. 基于混沌理论的彩色图像加密算法研究[D]. 兰州：兰州大学，2012

[10] 王兴元，王明军. 二维Logistic映射的混沌控制[J]. 物理学报，2008，57(2)：731-736