基于多混沌系统的医学图像加密算法

黄伟琦[1] 陈志刚[1] 梁涤青[1] 邓小鸿[1,2] 鄢 鹏[1]
(中南大学信息科学与工程学院 长沙 410083)[1] (江西理工大学应用科学学院 赣州 341000)[2]

摘 要 针对医学图像数据量大、同色像素连续性高的特点,提出了一种基于混沌理论的图像加密算法。算法通过在多个一维混沌系统间的随机切换产生加密序列,在加密过程中对图像本身引入了双重反馈,从而有效延长了混沌序列的周期,提高了算法的安全性。实验证明,本算法具有较好的运行效率与加密效果。

关键词 医学图像,混沌加密,双重反馈
中图法分类号 TP393 **文献标识码** A

Medical Image Encryption Algorithm Based on Multiple Chaos Systems

HUANG Wei-qi[1] CHEN Zhi-gang[1] LIANG Di-qing[1] DENG Xiao-hong[1,2] JIAN Peng[1]
(School of Information Science and Engineering, Central South University, Changsha 410083, China)[1]
(College of Applied Science, Jiangxi University of Science & Technology, Ganzhou 341000, China)[2]

Abstract Due to the characteristics of medical image: huge data and high continuity of same color pixels, a medical image encryption algorithm based on chaos theory was proposed. The algorithm generates encryption array by randomly switching among multiple one-dimensional chaos systems, introduces duplex feedback to the image data while encryp-ting, which lengthens the sequence period and improves the security of algorithm. Experiment results show that the algorithm has good running efficiency and encryption effect.

Keywords Medical image, Chaos encryption, Duplex feedback

1 引言

随着计算机、通信技术和区域医疗协同服务的不断发展,信息的安全与保密显得越来越重要。医学图像作为诊断依据的重要部分需要在公网上传播,为了防止病人敏感信息的非法泄漏,研究医学图像加密有着重要的意义。

混沌是指一种由非线性确定系统产生的类随机行为,它具有以下特征:

1)随机性:混沌系统产生的混沌序列表现出类随机行为,具有长期不可预测性。

2)确定性:只要初始参数确定,产生的混沌序列即确定。

3)遍历性:混沌系统将以一种不重复的方式遍历相空间中的所有取值。

利用混沌系统的这些特点[1]可以设计出密钥空间大、加密流随机性高的加密算法,混沌加密近年在计算机领域成为了研究热点[2,3],大量混沌图像加密算法被提出来[4-6]。

图像加密与普通文件加密的不同之处在于,图像相邻像素之间通常存在着比较大的相关性,对图像加密不仅要使图像变得不可识别,还要尽可能地减小相邻像素之间的相关性。目前国内外提出的各种混沌图像加密算法,有的通过Logistic函数生成混沌序列进行加密,有的通过DCT变换、Arnold变换进行加密,但总结起来,主要加密原理有以下两种形式:1)利用混沌系统产生的伪随机序列与明文进行异或操作,直接改变明文的值,通过这种方式进行加密可使图像明文转变为一系列无规则"噪声",能有效防止统计攻击;2)利用伪随机序列对明文进行重新排序,通过这种方式加密能有效地对图像进行置乱,使加密后的密文图像具有一定的鲁棒性,但由于置乱过程没有改变像素本身的值,因此加密后图像的颜色直方图并没有改变。结合医学图像数据量大、同色像素连续性高的特点,本文采用异或的方式提出一种新的混沌图像加密算法。

2 算法创新

医学图像的特点是两高一大(高分辨率、高精度、大数据量),这就要求算法具备较高的运行效率。对于混沌系统,通常高维混沌系统产生的加密序列有较高的安全性,但运行速度较慢。低维混沌系统产生加密序列速度快,却容易受到非线性预测、相重构等方式的攻击[7]。综合考虑算法运行效率与安全性,本文的算法将采用多个一维混沌系统混合的方式产生加密序列,并通过加密序列与图像进行异或操作进行加/解密。

医学图像通常有着大片连续的区域存在颜色相同的像素

到稿日期:2012-02-13 返修日期:2012-07-26

黄伟琦(1986-),男,硕士生,主要研究领域为网络与信息安全,E-mail:903096531@qq.com;陈志刚(1964-),男,博士,教授,博士生导师,CCF理事,主要研究领域为网络与信息安全,E-mail:czg@csu.edu.cn(通信作者);梁涤青(1979-),博士生,讲师,主要研究领域为网络与信息安全;邓小鸿(1982-),男,博士生,讲师,CCF会员,主要研究领域为数字水印;鄢 鹏(1987-),男,硕士生,主要研究领域为数字水印。

点，算法若简单地采用加密序列与明文异或的方式生成密文，密码攻击者容易根据这片连续的区域分析对应密钥序列的情况。所以加密算法应该以某种方式改变这种由于明文而导致密文单一变化的情况，本文算法通过在加密过程中加入双重反馈解决这一问题。

3 算法实现

考虑到算法的运行效率，本文选择以下两个混沌系统进行加密。

a. Logistic 映射[4]

$$X_{k+1}=u\times X_k\times(1-X_k) \tag{1}$$

当 $X\in(0,1)$，$u\in(3.5699456,4)$，$X\neq 1-(1/u)$时，系统处于混沌状态。

b. PLCM 映射[8]

$$X_{k+1}=\begin{cases}\dfrac{X_k}{p}, & X_k\in(0,p)\\ \dfrac{X_k-p}{0.5-p}, & X_k\in[p,0.5)\\ 1-X_k, & X_k\in[0.5,1)\end{cases} \tag{2}$$

当 $X\in(0,1)$，$p\in(0,0.5)$时，系统处于混沌状态。

以上两个混沌系统皆为一维混沌系统，从公式上看，不涉及 sin 与 cos 等复杂运算，所以能有较高的运行速度。

由于单个一维混沌系统产生的序列容易被非线性分析与相重构攻击，因此算法将选择的混沌系统混合使用，交替产生序列。设所选混沌系统数为 N，每个混沌系统产生序列的最大长度为 MAX_*LEN*。从第 t 个混沌系统开始产生序列。以 N，t 及各混沌系统的初始参数作为密钥：

a. 用相应参数初始化混沌系统，为了跳过混沌系统初期迭代的非线性状态，每个混沌系统先进行 $P(P>100)$次迭代。

b. 获取图像中要进行加密的序列长度 *PL*。

c. 第 t 个混沌系统进行一次迭代产生混沌数值 a，$t=(t+1)\bmod N$，令 $kLen=(a\times E)\bmod$ MAX_*LEN*(文中 $E=10000$，MAX_*LEN*=300)，获得下一个混沌系统将要产生的序列长度 *kLen*。

d. 若 $PL<kLen$，令 $kLen=PL$。利用第 t 个混沌系统产生长度为 *kLen* 的混沌序列。$PL=PL-kLen$。

e. 若 $PL=0$，序列产生算法结束；否则转到第 c 步。

通过运行上述算法，即可得到加密所需的序列 CARRAY，所产生的序列如图 1 所示。

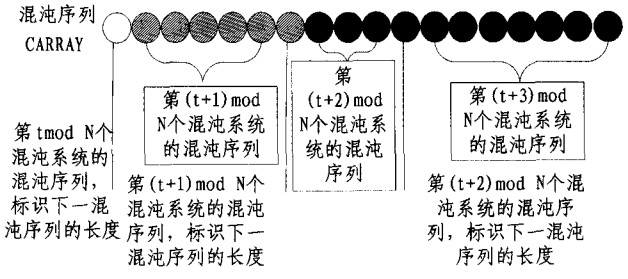


图 1 混沌序列产生示意图

混沌系统产生的混沌序列为一系列的实数，想要利用 CARRAY 对图像进行加密操作，需要对其进行离散化处理。对 CARRAY 中的每个元素 a，令 $a=(a\times ENLARGEMENT)\bmod 256$(文中 *ENLARGEMENT* 取 10000)，即取出了混沌序列中的一系列二进制密钥流 *BARRAY*。

医学图像中存在着大量连续的像素值相同的区域，若按传统加密简单地将图像信息与密钥流 *BARRAY* 进行异或操作以产生密文图像，密文图像在原图相应的同像素区域处容易反映出密钥流的变化情况，继而被攻击破解。所以本文在加密的过程中加入了反馈机制，将图像与密钥流相结合作用，以产生变化更大的密文图像。

设图像数据流为 DATA，反馈算法如下：

a. 前向反馈

对于第一个数据点：$DATA[0]=((DATA[0]\oplus BARRAY[0])+BARRAY[0])\bmod 256$，对于之后的数据点：$DATA[i]=(((DATA[i]\oplus BARRAY[i])+BARRAY[i-1])\bmod 256)\oplus DATA[i-1]$。

b. 后向反馈

对于非最后一个数据点：$DATA[i]=(((DATA[i]\oplus BARRAY[i])+BARRAY[i+1])\bmod 256)\oplus DATA[i+1]$，对于最后一个数据点：$DATA[i]=((DATA[i]\oplus BARRAY[i])+BARRAY[i])\bmod 256$。

在前向反馈中，当 i 以递增的形式进行时，加密过程为密文反馈，已经加密的数据将反馈作用到后面的加密过程中，由于反馈的过程有混沌序列中的随机二进制位参与，因此最后得到的密文图像能呈现出良好的随机特性，具有较强的抗统计分析能力。

而当 i 以递减的形式进行时，加密过程为明文反馈，这时的反馈过程没有传递性，每个密文字符只与加密时它的前面一个明文数值有关，所以当明文图像有较明显的区域连续性时，加密后的图像也容易看出大概的轮廓。但由于加密过程与明文紧密相关，当解密过程中有一位明文遭到破坏时，将导致后续图像无法解密，这就有效加大了攻击者通过统计密文微小改变对明文造成的影响进而攻击的难度。

无论明文反馈加密还是密文反馈加密，在单向反馈过程中图像的第一点都没有受到反馈的作用，所以算法对明文反馈与密文反馈都进行了双向加密，这样不但提高了图像中第一点的安全性，也加大了密文图像的随机性，增大了对图像的破解难度。

解密图像只需在产生密钥流后将算法反向运行即可。

4 实验结果与安全性分析

(a)原图　　(b)加密图

图 2 加密效果图

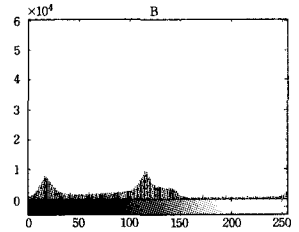
采用以下实验环境：操作系统为 Windows XP SP3，CPU 为 Intel(R) Core(TM2) Duo CPU E7500 2.93GHz，内存

1.96GB，在 Visual Studio2005 平台上用 VC++实现本文算法。从中南大学湘雅医学院获取了 100 幅不同形态的医学图像进行实验，均得到了较好的加密效果，以下为对一幅 1024×1024的 24 位 CT 图像进行加密的结果，如图 2 所示。

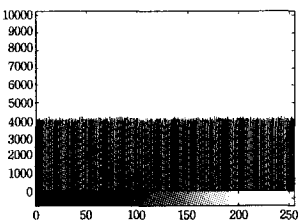
实验相关参数测试如下。

4.1 图像直方图

图像直方图能很好地反映出图像的颜色分布特征，一个好的图像加密算法应使加密后图像的直方图分布均匀，尽量地减小加密图像存在的像素统计特征，实验结果如图 3 所示。



(a) 原图像颜色直方图



(b) 加密图像颜色直方图

图 3 颜色直方图对比

由图可知，本文算法能很好地混淆图像像素值的分布，具有较好的加密效果。

4.2 图像相关性计算

应用以下公式可计算图像像素之间的相关性[9]。

$$\gamma=\frac{\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{(\sum_{i=1}^{N}(x_i-\bar{x})^2)(\sum_{i=1}^{N}(y_i-\bar{y})^2)}} \tag{3}$$

式中，N 为选取对比的像素对总数，$\bar{x}$ 与 $\bar{y}$ 分别是两组对比像素的平均值。

本文随机选取图像中的 3000 个相邻像素点对分别进行水平、垂直、对角关系的图像相关性计算，结果如表 1 所列。

表 1 图像像素相关性测试

	明文图像	加密图像
水平	0.986133	0.017447
垂直	0.994344	−0.000161
对角	0.980953	−0.041132

可见，原本相关性很强的图像加密后成了像素间关联性很小的“杂乱”图像。

4.3 敏感性测试

a) 密钥敏感性

首先对图像进行加密操作，保存密文图像后，对解密密钥中一个混沌初始参数值进行微小的改变，再对图像进行解密操作。由实验结果可知，虽然密钥只进行了 10^{-15} 数量级的改变，亦将导致图像无法解密。实验结果说明算法中的密钥有着极高的敏感性，算法由多个混沌系统组成，每个混沌系统都有着初始参数敏感性，可见算法有着极大的密钥空间，能很好地抵抗暴力破解攻击。

b) 明文敏感性

实验将对两幅只有一个像素不同的图像分别进行加密，再应用式(3)，将公式中的对比值设为两幅图中对应位置的像素值，计算两幅加密图像的相似程度 L，得 $L=0.06883$。

可看到，虽然明文图像只有一个像素的差别，加密结果却能得到两个几乎无相关性的图像，说明算法具有良好的明文敏感性，能在加密过程中将明文的改变扩散到整个图像。这一特性使算法能很好地抵抗通过对明文中存在的大量同色区域相对应密文的变化来分析密钥流情况的攻击。

c) 密文敏感性

实验中先对图像进行加密，再将密文图像进行一个像素的改变。从结果可看到，一个像素的改变也能导致无法解密，说明在算法中密文也存在着极高的敏感性。

算法存在的这些敏感性，加大了差分攻击等通过观察加密过程中的细微变化来破解算法这类方式的攻击难度。

4.4 图像加密速度

医学图像成像精度通常较高，所生成的图像大小相对较大，所以算法的加密速度也是一个关键因素。实验中取了 3 类不同大小的医学图像进行加密，结果如表 2 所列。

表 2 医学图像加密速度测试

图像大小	263kB	1.02MB	3MB
加密时间	19.785635ms	82.497338ms	244.317315ms

由表 2 可知，加密时间与图像大小基本成线性关系，对大小为 3M 的医学图像可在 1s 内完成加密运算，符合实际应用需求。

4.5 算法安全性分析

混沌系统在理论上是一个无限周期的伪随机数发生器，但在计算机上实现时，由于计算机只能进行有限精度的计算，系统将不可避免地退化为一个周期函数，在加密过程若因周期问题产生了重复的密钥流，将大大降低算法的安全性。在本文提出的算法中，密钥流是由多个混沌系统共同产生的，每个混沌系统在加密时都会由一个流长度生成点来决定下一个混沌系统产生的密钥长度。这一个随机生成的加密流长度取值较小，混沌系统间能紧密地相互作用，攻击者难以对其进行单一的分析，而且即使算法中的某一混沌系统在加密过程已经到达周期长度，只要该系统在进行系统切换时的流长度决定点没有停留在之前周期的同一个点，整体的密钥流依然可以看成是非周期的。系统的加密周期由所选的混沌系统共同决定，足以应用于大数据量的医学图像加密中。而混沌序列是由多个混沌系统共同产生，能很好地抵抗对单一混沌系统的非线性预测攻击与相重构攻击。系统对一幅大小为 3M 的图像加密只需 244ms，可见算法有着较高的运行效率，能满足在医学中的应用。

结束语 本文设计了一个多混沌系统混合加密的图像加密算法。算法通过在多混沌系统间的随机切换产生加密所需的密钥流，所产生的密钥流有着足够长的周期，可用于大数据量的图像加密，且能抵抗非线性预测攻击与相重构攻击，在加密过程加入了双重反馈，提高了算法的敏感性，加大了算法的

(下转第 299 页)

聚类算法中还包含了更新中心点等操作，而我们的输入感知模块仅仅作用于样本点分类过程，因此从全局耗时上看，性能优化为 20%～46%。

当聚类的聚类中心点发生变化时，传统的 GPU 聚类方法的加速比会受到影响，但这种输入感知的调度支持机制由于是在输入数据全局进行 GPU 负载的削减，因此仍然能有效提高其性能。图 6 是在 3 款 GPU 芯片下测得的传统方法的 GPU 聚类的加速比，图 7 是引入这种输入感知的调度支持机制后的加速比情况。

需要指出的是，为了实时跟踪气象过程（如风暴等）的运动，我们所输入的数据总是将其缩放到一个合适的尺度，以获得完整的风暴形状，因此无效区域往往是大面积存在的。

另外，由于 gpu_clustering_input_aware 本身也具有一定的开销，并且体现在每个 warp 上，因此从表 2 中可以看到，性能的提升总是要小于 hint 表中 0 值的比例，但所获得的性能仍然远远高于开销。

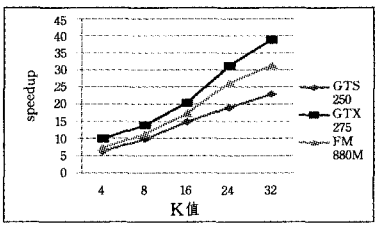


图 6　传统的 GPU 聚类在不同 K 值时的加速比

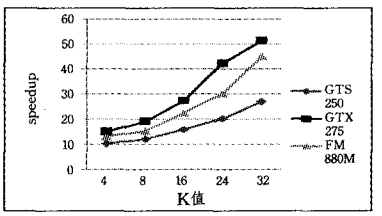


图 7　引入输入感知机制后的 GPU 聚类的加速比

结束语　本文提出一种输入感知的雷达回波快速聚类方法实现，给出了这种机制所需要的运行时模块和 GPU 代码中所需要的设计。该方案能够根据输入数据集的分布信息，削减 GPU 的计算负载。相对于一般策略的 CUDA 并行化方法，其在 GPU 上获得了 30%～60%的性能提升，带来了全局算法 20%～40%的性能提升，进一步挖掘了算法的实时性能。

下一步的工作，我们将继续寻找输入数据集对 GPU 并行化算法的影响应用场合，找出通过输入数据集优化并行程序的共性方法，以提高相关算法的实时性。

参 考 文 献

[1] Yang H P, Zhang J, Langston C. Synchronization of Radar Observations with Multi-Scale Storm Tracking[J]. Advances in atmospheric sciences, 2009, 26

[2] Lakshmanan V, Rabin R, DeBrunner V. Multiscale storm identification and forecast[J]. Atmospheric Research, 2003, 67/68: 367-380

[3] Lakshmanan V, Rabin R, DeBrunner V. Segmenting Radar Reflectivity Data using Texture[C]//Proc of the 30th International Conference on Radar Meteorology. Zurich, Switzerland: [s. n.], 2001

[4] Wang G L. The Development on a Multiscale Identifying Algorithm for Heavy Rainfall and Methods of Extracting Evolvement Information[D]. Nanjing University of Information Science and Technology, 2007

[5] Farivar R, Rebolledo D, Chan E, et al. A parallel implementation of K-means clustering on GPUs[C]//Proc of the 2008 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA 2008). 2008: 340-345

[6] Walters J P, Balu V, Kompalli S, et al. Evaluating the use of GPUs in liver image segmentation and HMMER database searches [C]//Proc of the 2009 IEEE International Parallel and Distributed Processing Symposium (IPDPS2009). IEEE Computer Society, 2009

[7] 陈加，吴晓军，蔡荣. GPU 并行加速的均值偏移算法[J]. 计算机辅助设计与图形学学报，2010(3)

[8] http://www.top500.org/

(上接第 263 页)

破解难度，适用于数据量大、存在大量连续同色区域的医学图像加密。

参 考 文 献

[1] 徐杰，杨娣洁，隆克平. 基于时滞混沌系统的带密钥 Hash 函数的设计与分析[J]. 电子科技大学学报，2011，40(3)：451-455

[2] 郑皓洲，胡进峰，徐威，等. 一类新型超混沌系统的非线性反馈同步研究[J]. 电子与信息学报，2011，33(4)：844-848

[3] Zhu Zhi-liang, Zhang Wei, Wong K-W, et al. A chaos-based symmetric image encryption scheme using a bit-level permutation [J]. Information Sciences, 2011, 181: 1171-1186

[4] 王重英. 基于 Logistic 的混沌加/解密图像算法研究[J]. 计算机应用技术，2009，18：123-127

[5] Zhang Jun, Li Jin-ping, Wang Lu-qian. A New Compound Chaos Encryption Algorithm for Digital Images[C]//2010 International Forum on Information Technology and Applications (IFITA 2010). Kunming, China: IEEE Computer Society, 2010: 277-279

[6] Wang Yong, Wong K-W, Liao Xiao-feng, et al. A new chaos-based fast image encryption algorithm[J]. Applied Soft Computing, 2011, 11: 514-522

[7] 黎全，赵凯，邓正才，等. 对一种混沌加密图像方法的破译研究[J]. 国防科技大学学报，2007，29(3)：45-49

[8] Xu Yang. Design of streams encryption key generator based on Chaos Theory[C]//2009 Pacific-Asia Conference on Knowledge Engineering and Software Engineering (KESE 2009). Shenzhen, China, IEEE Computer Society, 2009: 213-216

[9] 朱从旭，黄大足，郭迎. 结合多混沌映射和输出反馈的图像加密算法[J]. 武汉大学学报：信息科学版，2010，35(5)：528-531