基于改进 AES 加密算法的 DICOM 医学图像安全性研究

向 涛,余晨韵,屈晋宇,罗小松
(重庆大学计算机学院,重庆 400044)

摘 要: 本文基于 AES 算法的设计原理提出了一种改进的医学图像加密算法.针对 AES 算法结合斜帐篷映射对其进行改进,使其适合 DICOM 医学图像的数据特点.首先将 AES 中 4 * 4 的分块操作方式变成 M * N 的全图操作,其次增加了对病人基本信息的保护,最后改进了 AES 中列混合操作与密钥编排方式.通过理论分析与仿真实验证明改进算法具有较好的置乱效果、扩散性强,并且能够很好地保持 DICOM 文件格式的兼容性.

关键词: 医学图像加密; AES; DICOM; 混沌系统
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2012) 02-0406-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.02.032

Research on the Security of DICOM Medical Images Based on Improved AES Encryption Algorithm

XIANG Tao, YU Chen-yun, QU Jin-yu, LUO Xiao-song
(*Department of Computer Science, Chongqing University, Chongqing* 400044, *China*)

Abstract: In this paper, a medical image encryption algorithm is proposed. The algorithm is based on the design principle of AES, and combined with Skew tent map. The standard procedure of AES is modified so that it can be suitable for the DICOM medical digital images. At first, the block size 4 * 4 in AddRoundKey is replaced by the size of an image. Then the basic information of patient is protected by our proposed algorithm. In addition, the AES's MixColumns and key schedule are improved. The theoretical analysis and numerical simulations show that the improved algorithm not only has better confusion diffusion effects with less computational overhead, but also can maintain the compatibility of DICOM file format.

Key words: medical image encryption; AES; digital imaging commucation in medicine (DICOM); chaotic system

1 引言

DICOM(Digital Imaging Communication in Medicine)是由美国放射学院 (American College of Radiology, ACR) 和国家电气制造商协会(National Electrical Manufacturers Association, NEMA)共同制定的标准,包括医学的数字成像和通信两个方面的内容,是目前建设 PACS[1] 医学影像存档与通讯系统广泛遵循的一个国际标准.DICOM 标准[2]的推出大大简化了医学影像信息交换的实现,为医学数字化带来新的机遇.DICOM 与其它图像格式相比有一个很大的不同:除了病人图像信息以外还包含了多项与病人基本信息有关的数据,如姓名、年龄、病历等,方便医生诊断病情.随着 DICOM 标准的普及和远程医疗的实施,医学图像在传输过程中容易受到黑客攻击和数据篡改,事关病人隐私与医院的责任,因此如何安全有效地加密医学图像至关重要.

对于 DICOM 文件,该标准定义了一套加密规定[2]:(1)可以加密所有的数据、也可以只加密选定的属性;(2)对于加密方法,在标准中并没有统一的方案;(3)给出了有必要加密的属性列表.DICOM 目前对安全性仅仅给出了一个初步框架并没有统一的实现方案,仍然需要进一步完善.

DICOM 文件的安全性不容忽视,然而目前在其加密方面的研究还比较少.目前医学图像中常用的加密方法只是将经典的加密算法直接运用在医学图像中,如 DES, AES 等.传统的加密算法将输入明文看作二进制流,没有考虑图像本身的特性,使得其对图像并不十分适用.主要表现在:(1)图像数据量大,传统的加密方式难以和实时图像传输的速率相匹配;(2)图像的数据有多维分布的特点,使得传统的块加密方式可能泄露原

收稿日期:2010-12-21;修回日期:2011-09-28
项目基金:国家自然科学基金(No.61103211);中央高校基本科研业务费(No.CDJZR10180020);中国博士后科学基金特别资助(No.201104319);中国博士后科学基金(No.20100470817)

始图像内容的几何分布信息;(3)传统的加密方式破坏了图像数据的格式,从而导致图像解码端可能工作异常.因此,我们需要寻找一种适合图像数据特点的加密方法,使得其在满足安全性要求的前提下,提高加密的效率,同时保持图像数据格式的兼容性与传输要求.

本文基于 AES 算法的设计原理,并结合斜帐篷映射提出了一种改进算法,使之能够适应医学图像的数据特点.此外,针对 DICOM 格式的特点增加了对病人基本信息的保护,并与图像加密相结合.本文算法置乱和扩散效果好、安全性强,仅需要加密 4 轮就能取得较好的加密效果.

2　AES 算法分析与改进方案

2.1　AES 简介

AES 算法是分组迭代加密算法,能有效抵抗强力攻击、差分攻击和线性密码分析,具有分组长度和密钥长度设计灵活、高安全性和高运行效率等优点(详细设计及其安全性分析参见文献[3]和文献[4]).AES 加密的每一轮运算由 4 个变换组成,它们是:轮密钥异或、S 盒变换、行置换和列混合.为了后文描述方便,将这 4 个步骤称为 AddRoundKey、SubBytes、ShiftRows、MixColumns.加密流程如图 1 所示.

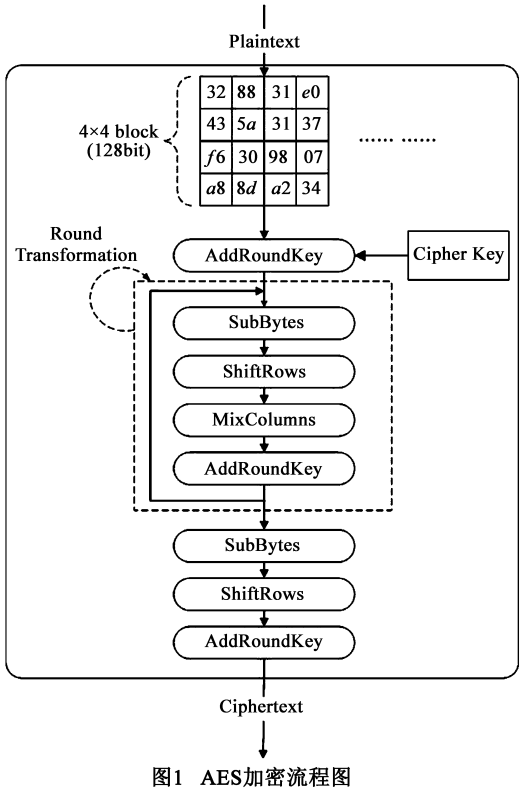


图1　AES加密流程图

2.2　改进方案

AES 算法采用分组迭代,分块大小为 4×4 矩阵,每个元素为 8 比特.本文算法以像素(8 比特)为单位,对整幅图像进行处理.为了使算法适用于图像加密,达到较好的安全性,并提高加密效率,我们基于 AES 算法框架进行了如下改进:

2.2.1　改进密钥序列生成方法

混沌动力学系统具有伪随机性和对初始条件与系统参数的极端敏感性,因此,它为图像信息加密提供了很好的途径.在改进算法中采用如下所示的斜帐篷映射(Skew tent map)[5]生成密钥序列.

$$F_a(x)=\begin{cases}x/a, & x\in(0,a)\\ (1-x)/(1-a), & x\in(a,1)\end{cases} \tag{1}$$

当 $a\in[0,1]$时系统呈混沌状态.该映射迭代轨道序列的相关性以指数递减,混沌变量的分布均匀,具有很好的伪随机特性.

基于斜帐篷映射生成伪随机序列的方法如下:一幅大小为 $M\times N$ 的图像,需要加密 R 轮.首先迭代斜帐篷映射得到 R 个长为 $M\times N$ 的序列 $X_r=\{x_{r,0},x_{r,1},\cdots,x_{r,MN-1}\}$,$1\leqslant r\leqslant R$.对序列 X 按照式(2)扩展为 0 ~ 255 的整数序列 $K_r=\{k_{r,0},k_{r,1},\cdots,k_{r,MN-1}\}$.

$$k_{r,i}=\lfloor x_{r,i}\times 255\rfloor,\ 0\leqslant i\leqslant MN-1 \tag{2}$$

其中$\lfloor\ \rfloor$运算表示向下取整.

2.2.2　改进加密/解密操作

AES 算法的加密方式为像素矩阵 D 与密钥序列 K 直接进行异或操作,为了增加对明文的敏感性,本算法做出了改进,第 r 轮的加密过程如下所示:

$$C[i][j]=\begin{cases}D[i][j]\oplus k_{r,i\times N+j}, & i=M-1,j=N-1\\ D[i][j]\oplus(k_{r,i\times N+j}\oplus D[i+1][0]), & i\neq M-1,j=N-1\\ D[i][j]\oplus(k_{r,i\times N+j}\oplus D[i][j+1]), & \text{其他}\end{cases} \tag{3}$$

其中 $i\in[0,M-1]$,$j\in[0,N-1]$,$D[i][j]$为明文像素,$C[i][j]$为得到的密文像素.

明文图像矩阵按照从左到右,从上到下加密;密文图像矩阵按照从右到左,从下到上逐像素进行解密.经过以上的异或操作之后,使得密钥与明文相关,两幅不同图像即使采用相同的初始条件,生成的密钥序列也不同.

2.2.3　改进列混合操作

AES 算法中,列混合操作(MixColumns)采用矩阵运算,每个像素平均需要经过移位和异或运算.为了降低运算量并达到较好的混合效果,在改进的算法中,我们改变了 MixColumns 的矩阵运算,采用简单的加减运算增强像素间的联系.具体做法如下:对于每一行,第一个像素保持不变,从第二个像素开始用相邻像素的更新当前像素(如式(4)所示);对于每一列,第一个像素保持不变,从第二个像素开始用相邻像素的值更新当

前像素(如式(5)所示).

$$\begin{cases} D[i][j]=D[i][j], j=0 \\ D[i][j]=(D[i][j]-D[i][j-1]) \bmod 256, \text{其他} \end{cases} \tag{4}$$

$$\begin{cases} D[i][j]=D[i][j], i=0 \\ D[i][j]=(D[i][j]-D[i-1][j]) \bmod 256, \text{其他} \end{cases} \tag{5}$$

以 5×4 的像素矩阵为例,运算过程如图 2 所示.

(a)5*4的像素矩阵

25	38	255	65
66	89	58	211
242	255	84	48
195	79	8	195
77	60	80	90

(b)行扩散操作结果

25	13	242	79
66	23	35	176
242	13	71	233
195	140	124	71
77	239	97	249

(c)列扩散操作结果

25	13	242	79
41	10	49	97
201	3	22	136
250	137	102	191
83	102	251	58

图2 扩散性增强过程

从图 2 中可以看出,当 $D[0][0]$ 发生变化时,将影响所有像素;当 $D[M-1][N-1]$ 发生改变时,在同一轮中将不影响其他像素.因此在行列变换操作中,应将每一行循环向左移动,每一列循环向上移动,经多轮加密后将有明显的扩散效果.

改进的行列混合操作中采用简单的加减运算,每个像素平均仅需要 2 个加法运算,该操作不仅减少了运算量还增强了像素之间的联系,经多轮加密后能达到较好的混合效果.

3 改进算法在 DICOM 医学图像中的应用

DICOM 文件一般由一个 DICOM 文件头和 DICOM 数据集合组成.DICOM 数据集合是由 DICOM 数据元素按照一定的顺序排列组成的,它不仅包括图像数据,还包括许多和病人相关的信息,如病人姓名、年龄、病历等.数据元素的组成结构如图 3 所示,其中标志符由组号与元素号组成,表示为(组号,元素号),是数据元素的唯一标识.

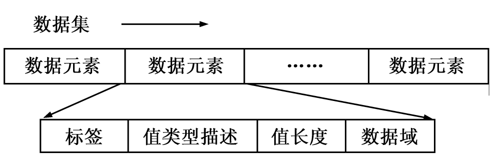


图3 DICOM数据集合

因此,DICOM 文件需要保密的内容包括两个部分:病人的基本信息和图像信息.

3.1 病人信息和图像数据的交换方案

我们将病人基本信息的保护与图像数据的加密结合起来:设计一个一维到二维的映射方法,将病人信息以 8 比特为单位与图像像素明文交换.假设存储病人信息的变量为一维数组 $P[L]$,其中 L 为病人信息的字节数,其处理过程为:

Step 1 迭代斜帐篷映射得到序列 $X'=\{x'_0, x'_1, \cdots, x'_{2\times L-1}\}$ 将其分成长为 L 的两个子序列 $X'_1=\{x'_0, x'_1, \cdots, x'_{L-1}\}$, $X'_2=\{x'_{L+1}, x'_{L+2}, \cdots, x'_{2\times L-1}\}$.

Step 2 获取随机整数序列作为横坐标.将 X_1' 用类似式(2)的方法扩展到 0 ~ M 范围内,得到横坐标序列 $U=\{u_0, u_1, \cdots, u_{L-1}\}$.

Step 3 获取随机整数序列作为横坐标.将 X_2' 用扩展到 0 ~ N 范围内,得到纵坐标序列 $V=\{v_0, v_1, \cdots, v_{L-1}\}$.

Step 4 组合两个序列得到坐标序列为 $(U, V)=\{(u_0, v_0), (u_1, v_1), \cdots, (u_{L-1}, v_{L-1})\}$.

令 $L=1000, M=1000, N=1000, x'_0=0.80, a'=0.6$,得到的坐标序列分布情况如图 4,分布比较均匀.映射前,病人信息显示的是 ASCII 码;映射后显示的是乱码,以病人姓名为例:假设映射前病人姓名为:"*Anoymized*".映射后将数组内容重新填充回 DICOM 原标签中,显示的内容为:"q 垐 GK W 轓堼".

这种做法使得病人信息失去可读性,其安全性依赖于图像的安全性,只要采用安全的图像加密算法便能保证病人信息的安全.

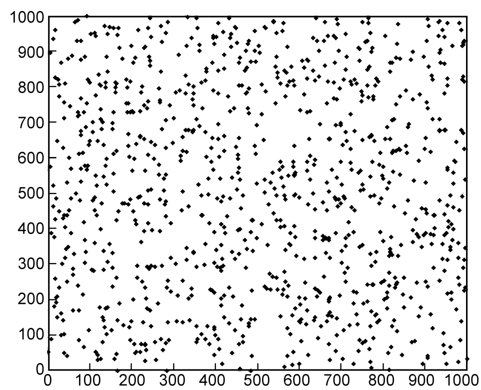


图4 坐标序列分布

3.2 DICOM 文件加密方案

本节列出了将保护病人信息的方案和改进的 AES 算法应用于 DICOM 文件加密的具体步骤,其基本的加密结构如图 5.

加密算法步骤如下:

Step 1 初始化 $r=0$.隐藏病人基本信息.将 DICOM 文件中的病人信息数据取出放在一维数组 $P[L]$ 中;将图像像素数据取出放在二维矩阵 $\boldsymbol{D}[M][N]$ 中;按照 3.1 节中的映射算法依次将 P 的数据和 $\boldsymbol{D}$ 对应的数据交换,得到交换后的病人信息 P',交换后的图像像素矩阵 $\boldsymbol{D}_1$.

Step 2 密钥异或操作(PixelXOR).将图像像素矩阵 $\boldsymbol{D}$ 与密钥序列 K_r 按照式(3)异或,得到 C_1.

Step 3 S 盒置换(SubBytes).采用文献[6]给出的

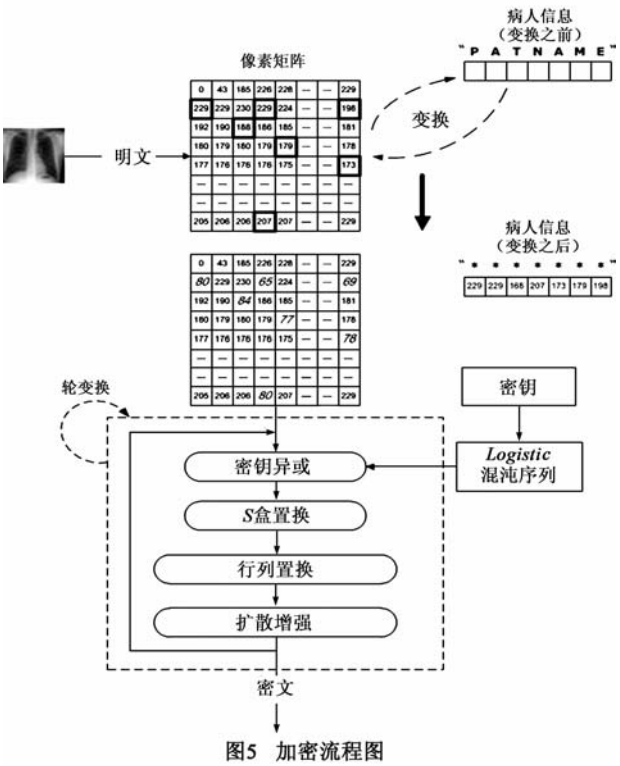


图5　加密流程图

S 盒,将 C_1 的每个元素的高 4 位作为 S 盒的行坐标,低 4 位作为 S 盒的列坐标,查表进行 S 盒替换,得到 C_2.

Step 4　行列置换(ShiftRowsandColumns). C_2 中第 i 行元素向左循环移动 i 个单位,第 j 列元素向上循环移动 j 个单位,得到 C_3.

Step 5　扩散增强(MixRowsandColumns). 对 C_3 每行所有像素按照式(4)进行处理操作,对 C_3 每列所有像素按式(5)操作,得到 C_4.

Step 6　$r = r + 1, D = C_4$,回到 Step2 进行下一轮加密,总共进行 R 轮. 最后得到加密后的像素矩阵 C.

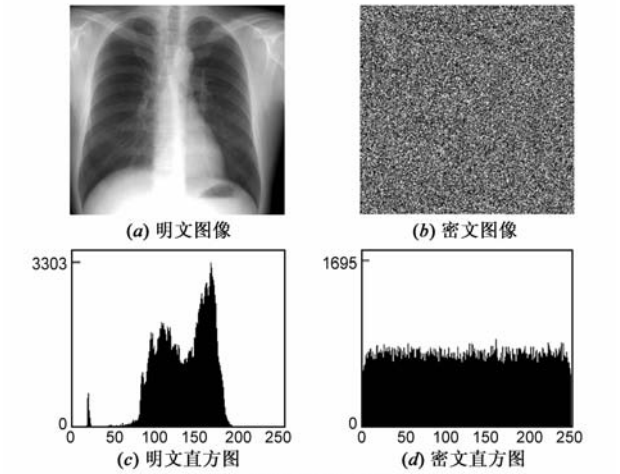
其解密过程为加密算法的逆过程:首先还原图像像素,即对密文像素矩阵依次进行逆 MixColumns、ShiftRows、SubBytes、AddRoundKey 操作;然后还原病人信息,重建 DICOM 文件.

4　实验结果与分析

本算法采用 Visual C++ 2008 平台进行数据仿真实验,同时采用 DCMTK 开发包[7]实现 DICOM 文件读写. 机器配置: Intel CoreDuo 1.83GHz CPU, 2GB RAM, Windows 7 Ultimate 中文版操作系统. 其中明文图像为 440 × 440 的标准 DICOM 图像,密钥设置为: $x_0 = 0.8, a = 0.6, x_0' = 0.8, a' = 0.6, R = 10$.

4.1　加密实验结果

加解密图像如图 6 所示. 图 6(a)与图 6(c)分别为原始明文图像和明文直方图,图 6(b)和图 6(d)是密文图像和对应的直方图. 从图中可以看出密文直方图分布均匀,能够有效地抵抗统计分析.



(a) 明文图像　(b) 密文图像
(c) 明文直方图　(d) 密文直方图

图6　原图像及加密图像

4.2　实验分析

4.2.1　密钥空间

本算法的密钥由两组斜帐篷映射初始值与参数组成:一组参数控制密钥流的生成(x_0, a_0),另一组控制病人信息保护的映射(x_0', a_0'). 在计算机实现时,分别由 64 位数表示,也就是说算法的密钥为 256 位. 明文空间为 2^{256},能够抵抗暴力破解.

4.2.2　相关性分析

分别从图像的水平、竖直和对角相邻方向随机地选取 1024 对像素,加密 10 轮,对比它们加密前后的相关系数:

$$r_{x,y} = \frac{E(x - E(x))(y - E(y))}{\sqrt{D(x)}\sqrt{D(y)}}$$

其中, $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$.

实验结果如下表 2 所示,表中数据显示明文图像中相邻像素之间的相关性比较高,但是在密文图像中相邻像素的相关性均很低.

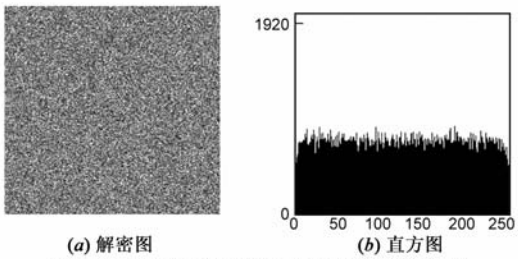
表 1　明文图像与密文图像相关系数比较

	明文	密文
水平	0.963810	0.025547
垂直	0.961591	0.012778
对角线	0.938320	-0.0084332

4.2.3　敏感性分析

(1) 密钥敏感性分析

将原始密钥进行微小改动,将 x_0 由 0.8 改为 0.80000001,其余密钥保持不变,对应的解密结果如图 7 所示. 解密图像呈现随机分布,其直方图很均匀. 即使加密密钥和解密密钥有微小的相差也能正确解密,说明该算法能够抵抗各种基于密钥敏感性的攻击.



(a) 解密图 (b) 直方图

图7 密钥的敏感性测试及其对应的解密结果

(2) 明文敏感性分析

为了测试算法对明文的敏感性,应用2幅几乎完全相同的明文图像(440×440 的 DICOM 图像 Chest.dcm,其中只有(0,0)位置的像素值不同),对它们进行加密.完成4轮加密后,得到对应的密文图像并比较他们的像素值.从图8中可以看出,当仅有一位像素发生变化时,加密后的图像几乎完全不同(白色的像素点表示相同部分,黑色为不同).通过计算可知,当两幅图(0,0)位置像素值不同时,对应的密文图像有99.61%的像素不同.通过以上分析,可看出改进算法具有良好的扩散效应,达到了安全性的要求.

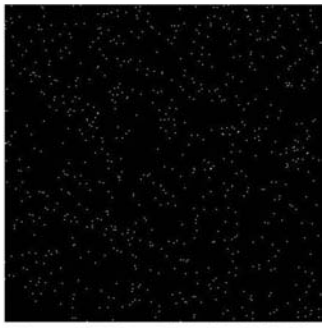


图8 4轮迭代后密文的差值图像

4.2.4 加密轮数测试

扩散效果可以用两个重要的指标来衡量:像素变化率(Number of Pixels Change Rate,NPCR)和统一的平均变化强度(Unified Average Changing Intensity,UACI).NPCR是当明文某个像素改变一位时,密文像素的改变率;UACI指当明文某个像素改变一位时,密文之间差的绝对值.其计算公式为:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\%$$

其中 W 和 H 是被测试图像的宽与高,C_1 和 C_2 是由仅差一个像素的明文图像加密而成的密文图像.若 $C_1(i,j) = C_2(i,j)$ 则 $D(i,j) = 1$;否则 $D(i,j) = 0$.改变(50,50)位置的像素值,分别计算 NPCR 与 UACI,结果如表2所示,可看出改进算法只需加密4轮便可取得很好的扩散效果.

4.2.5 加密时间分析

AES 加密算法由 10 轮加密构成,其中每一轮包括 AddRoundKey、SubBytes、ShiftRows、MixColumns 四个变换.改进算法也采用多轮加密,主要是针对后三个变换进行了改进.我们从网站 http://barre.nom.fr/medical/samples/下载了一些常用标准 DICOM 图片,在相同环境下进行了对比测试,其中 AES 算法按照 AES 标准 FIPS197[8]实现.测试结果如表3所示.

由表3可知,加密同一幅 DICOM 图像改进算法所花费的时间比 AES 算法少一半左右.改进算法具有更高的运算效率.

表2 NPCR 与 UACI 在不同加密轮数下的测试结果

加密轮数	NPCR	UACI
1	0.886364	0.399262
2	0.992924	0.335252
3	0.995656	0.334904
4	0.995961	0.334708
5	0.996064	0.335646
6	0.995878	0.334734
7	0.996018	0.334315
8	0.996997	0.3354277
9	0.996245	0.3352222
10	0.996121	0.3353810

表3 两种加密算法加密不同大小文件所需时间比较

图片	大小	轮数	标准 AES	改进算法
CR-MONO1-10-chest	440×440	10	562ms	272ms
CT-MONO2-16-ankle	512×512	10	769ms	361ms
MR-MONO2-12-angio-an1	256×256	10	186ms	84ms
MR-MONO2-16-head	256×256	10	185ms	84ms

5 结论

本文针对医学图像的特点提出了改进的 AES 加密算法.首先,将病人基本信息隐藏于图像数据中,保障了病人隐私.然后,改进加密操作,使其不仅与斜帐篷映射的初始条件相关,还与明文产生联系.其次,改进 MixColumns 的矩阵运算方式,采用简单的加减运算使像素之间关联性加强,这样能形成良好的扩散效应来抵抗选择明文攻击.最后,对改进算法进行了理论分析与实验仿真.实验结果表明,改进算法不仅具有较好的安全性与执行效率,在较少的轮数下就能取得较好的加密效果,而且保持了 DICOM 文件格式的兼容性.

参考文献

[1] X Cao,H K Huang.Current status and future advances of digital radiography and PACS[J].IEEE Engineering in Medicine and Biology Society,2000,19(5):80-88.

[2] National Electrical Manufacturers Association.Digital imaging and Communications in medicine[DB/OL].ftp://medical.nema.org/MEDICAL/Dicom/2009/,2010-11-13.

[3] J Daemen,V Rijmen.The Design of Rijndael by Joan Daemen and Vincent Rijmen[M].Berlin,Heidelberg:Springer-Verlag,

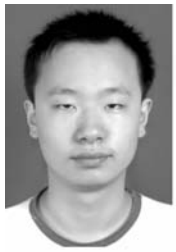
2002.
[4] 肖国镇,白恩健,刘晓娟. AES 密码分析的若干新进展[J]. 电子学报,2003,31(10):1549 – 1554.
Xiao Guo-zhen, Bai En-jian, Liu Xiao-juan. Some new developments on the cryptanalysis of AES[J]. Acta Electronica Sinica, 2003, 31(10): 1549 – 1554. (in Chinese)
[5] G Alvarez, S J Li. Some basic cryptographic requirements for chaos-based cryptosystems[J]. International Journal of Bifurcation and Chaos, 2006, 16(8), 2129 – 2151.
[6] G Jakimoski, L Kocarev. Chaos and cryptography: block encryption ciphers based on chaotic maps[J]. IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications. 2001, 48(2): 163 – 169.
[7] DICOM Toolkit[DB/OL]. http://www.dcmtk.org/.
[8] National Institute of Standards and Technology. FIPS 197: Advanced Encryption Standard[DB/OL]. http://csrc.nist.gov/publications/fips/fips197/fips – 197.pdf, 2010-11-13.

作者简介

向　涛　男,生于 1980 年.重庆大学副教授.2008 年获得重庆大学博士学位.研究方向包括混沌密码学,多媒体安全,群智能优化.
E-mail: txiang@cqu.edu.cn

屈晋宇　男,生于 1988 年.重庆大学计算机学院计算机软件与理论专业研究生.研究方向为多媒体安全.
E-mail: qucooln@gmail.com

余晨韵　女,生于 1989 年.重庆大学计算机学院计算机软件与理论专业研究生.研究方向为多媒体安全.
E-mail: yuchenyun0320@163.com



罗小松　男,生于 1988 年.重庆大学计算机学院计算机应用技术研究生.研究方向为模式识别、图像处理.
E-mail: anonympine@gmail.com