doi:10.11959/j.issn.1000-436x.2015021

分区域的医学图像高容量无损信息隐藏方法

邓小鸿[1,2,3]，陈志刚[2,3]，梁洛青[2,3]，毛伊敏[1]

(1. 江西理工大学 应用科学学院，江西 赣州 341000；2. 中南大学 信息科学与工程学院，湖南 长沙 410083；
3. 中南大学 移动医疗实验室，湖南 长沙 410083)

摘 要：针对医学图像的分区域典型特征，提出一种基于区域和直方图平移的高容量无损信息隐藏方法。本方法用最大类间距分割法求得原始图像的前景区域，再用聚合多边形逼近和图像拟合法得到其数据嵌入区域。在数据嵌入过程中，提出利用差值直方图循环平移和基于编码的直方图平移方法分别在前景和背景区域嵌入数据，提高了原始直方图平移方法容量和解决了溢出问题。实验结果表明该方法总的嵌入容量可达 1 bit/pixel 以上，并且隐秘图像质量在 40 dB 左右，适用于具有区域特征的质量敏感图像的大容量信息隐藏。

关键词：医学图像；区域；可逆数据隐藏；隐私保护；直方图平移

中图分类号：TP391 **文献标识码**：A

Region-based lossless data hiding with high capacity for medical images

DENG Xiao-hong[1,2,3], CHEN Zhi-gang[2,3], LIANG Di-qing[2,3], MAO Yi-min[1]

(1. College of Applied Science, Jiangxi University of Science and Technology, Ganzhou 341000, China;
2. College of Information Science and Engineering, Central South University, Changsha 410083, China;
3. Mobile Medical Laboratory, Central South University, Changsha 410083, China)

Abstract: In view of the significant regional features of medical images, a new high capacity lossless data hiding method based on region and histogram shifting was presented. Firstly, the presented method utilized segmentation method of the maximum class separation distance to get the foreground region of medical images, and then used the polymeric polygonal approximation and image fitting algorithm to get the embedding region of region foreground. In the embedding procedure, the difference histogram circular shifting method and the code-based histogram shifting method were presented to embed hidden data in foreground and background region respectively, which improved the limit embedding capacity and resolved the overflow and underflow in traditional histogram shifting method. Experimental results show that the proposed method achieves high embedding capacity with 1 bit/pixel and stego-image quality about 40 dB. The presented method can be applied to the quality of sensitive image's large capacity information hiding with regional feature.

Key words: medical image; region; reversible data hiding; privacy protection; histogram shifting

1 引言

随着区域医疗和远程诊断技术的飞速发展，越来越多的医学图像信息开始在公网上进行传输。早期的研究者们提出使用加密技术来保护医学图像的安全[1]，如图像存储和通信系统（PACS, picture archiving and communication systems）中广泛使用的医学数字成像和通信标准(DICOM, digital imaging and communication of medicine)中，就在 DICOM 文件头中使用了 MD5 算法证明医学图像数据的完整性。加密是以一种主动防护方式使得非授权的用户无法获得信息内容，但解密后的图像无法提供进一

收稿日期：2013-07-01；**修回日期**：2013-10-15

基金项目：国家自然科学基金资助项目(61103202, 61272494)；江西省自然科学基金资助项目(20122BAB201045)；江西理工大学校级科研基金资助项目(jxxj12149)

Foundation Items: The National Natural Science Foundation of China(61103202, 61272494); The Natural Science Foundation of Jiangxi Province(20122BAB201045); Research Project of Jiangxi University of Science &Technology (jxxj12149)

步的保护，另外，加密的内容容易遭到攻击者的攻击。鉴于单一方法的不足，数字水印技术作为加密技术的有力补充，已经广泛应用在网络上的信息安全保护中。然而，传统的数字水印技术对载体内容造成的永久失真对高质量要求的医学图像来说是不可行的。因为感兴趣区域(ROI, region of interest)任何微小的失真，都可能对专业医生的疾病诊疗造成错误引导。鉴于医学图像对于质量的高要求，一方面利用水印技术来保护医学图像安全，另一方面要消去水印给图像带来的失真。即在提取出数据后，含水印图像能无损地恢复到原始状态，无损数字水印技术正是由此发展而来。目前，已经广泛应用在内容敏感载体，如卫星和军事图像、医学图像、二维工程图等领域[2~5]。

利用医学诊断图像中像素之间的高相关性存储病人的隐私信息具有明显优势[6]，既能减少医院存储信息中出现的匹配错误，又能减少存储空间和网络传输过程中所需要的带宽。医学图像具有典型的分区域特征，分为前景和背景区域，有研究者又称为感兴趣区域和非感兴趣区域(RONI, region of non-interest)，前者通常是像素值较高的且纹理特征较复杂区域，后者通常是连续的黑色区域。目前的方法中很少考虑医学图像分区域的特点，大部分的方法将整幅医学图像进行统一固定块的划分，然后在划分后的区域进行可逆数据隐藏。典型的代表如Chen等人[7]提出的自适应可逆数字水印方法，这类方法的缺点是ROI像素在采用高容量的可逆数据隐藏算法时容易出现溢出现象，对隐秘图像质量和可逆性带来严重影响。张秋余等人[8]提出了一种基于压缩感知的方法对图像进行非固定块的划分，但是没有考虑图像的ROI区域。虽然也有一部分研究者们提出了分区域的方法，如Guo等人[9]提出在ROI区域和RONI选择不同的数据嵌入方法隐藏数据，但此类方法的不足是需要诊断科医生自己指定ROI区域。其他的研究者们虽然提出了一些自动化的方法来提取医学图像中的ROI区域，如Duan[10]和Ge[11]提出的基于区域增长、模糊理论和人工智能的方法，这些方法具有较好的ROI提取精确性，但是算法复杂度和执行效率是一个瓶颈。综上所述，在医学图像中进行病人隐私数据的隐藏首先需要一个简单可行的ROI提取方法。另外，对提取端得到的隐秘数据有效性进行认证也是十分必要的，如Tan等人[12]提出了在医学数据的无损隐藏中加入认证环节。本文提出一个新的基于区域和直方图平移的高容量电子病历隐藏算法，实现了医学图像中的电子病历的大容量隐藏和有效性认证。采用图像最大类间距的分割方法进行医学图像的ROI区域自动提取，并提出采用聚合多边形逼近方法获取ROI区域的精确近似。在数据嵌入过程中，对基于差值直方图平移(DHCS, difference histogram circular shifting)和峰值点直方图平移2种方法进行改进。在ROI区域，利用差值直方图循环平移方法嵌入病人的电子病历等隐私数据；在RONI区域，利用基于编码的直方图平移方法(CHS, code based histogram shifting)嵌入原始图像的认证码和ROI区域中未嵌完的电子病历。本文首先对ROI区域的生成方法进行介绍，然后介绍本文改进的2种直方图平移方法DHCS和CHS，最后对算法的具体实施和实验结果进行了说明。

2 相关算法

2.1 ROI区域生成

定义1 医学图像ROI区域分割是将医学图像划分为ROI和RONI 2个区域，令集合I代表整个图像的区域，对I的ROI分割可以看作是将I划分成满足如下条件的非空子集I_1和I_2。

1) $\bigcup_{i=1}^{2} I_i = I$；

2) $I_1 \cap I_2 = \varnothing$；

3) 对于$i=1,2$，有$P(I_i)=\text{True}$；

4) 对于$i=1$，$j=2$，有$P(I_i \cup I_j)=\text{False}$；

5) 对于$i=1,2$，I_i是连通的区域。

定义2 基于单阈值的图像分割是在图像的灰度值域$[g_{\min}, g_{\max}]$选择一个阈值g_T ($[g_{\min} < g_T < g_{\max}]$)，对于图像中的任意一个像素值$\forall I(i,j)$，根据式(1)判断其归属的类别。

$$type(I(i,j)) = \begin{cases} type\_A, I(i,j) > g_T \\ type\_B, I(i,j) \leqslant g_T \end{cases} \tag{1}$$

图像分割主要利用区域内部的像素一般具有灰度相似性，而在区域之间的边界上一般具有灰度不连续性。根据医学图像的特点，ROI和RONI区域之间通常有明显的像素差异，单阈值方法可以利用区域间的巨大像素差异将医学图像划分成2类像素集合。相对其他如并行边界技术和串行边界技术的分割方法，该方法操作简单，效率高。经过分割

后的二值化图像可表示为

$$I(i,j)=\begin{cases}1, I(i,j)>g_T\\ 0, I(i,j)\leqslant g_T\end{cases} \tag{2}$$

定义 3　图像类间距，设 ROI 区域中像素值个数为 *num_ROI*，*avg_ROI* 表示其灰度均值，RONI 中像素个数为 *num_RONI*，*avg_RONI* 为其灰度均值。设 w_1，w_2 分别代表 ROI 和 RONI 区域中像素占的比重，那么图像的总灰度均值 *avg_I* 可表示为

$$avg\_I = w_1 avg\_ROI + w_2 avg\_RONI \tag{3}$$

其中，$w_1=\dfrac{num\_ROI}{num\_ROI+num\_RONI}$

$$w_2=\frac{num\_RONI}{num\_ROI+num\_RONI}$$

类间距可描述为

$$D = w_1(avg\_ROI - avg\_I)^2 + w_2(avg\_RONI - avg\_I)^2 \tag{4}$$

定理 1　如果分割阈值 g_T 能使类间距 D 取最大值，则称采用 g_T 阈值的分割为最大类间距阈值分割。

由于人体组织结构的形状不一，提取出来的 ROI 区域经常是不规则的形状。另外，为了使提取端能正确定位 ROI 区域，在嵌入端需要将 ROI 区域表示出来，并作为密钥传送给提取端。为了减少传输负载，需要用较少的位置信息来描述 ROI，本文提出用聚合逼近多边形表示 ROI 区域。一个不规则多边形的聚合多边形逼近实例如图 1 所示。

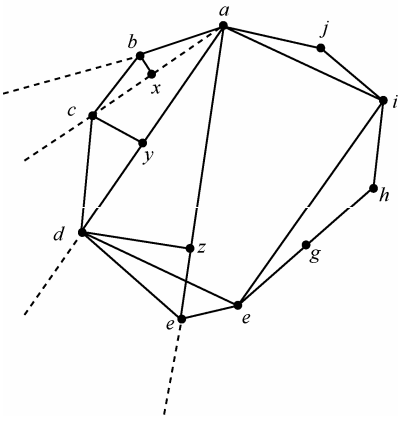


图 1　聚合逼近多边形求解过程

定义 4　ROI 区域的聚合逼近多边形是该区域的近似，用规则的多边形最大程度拟合原始多边形。设 a,b,c,d,e,f,g,h,i,j 是原不规则多边形的顶点，通过算法 P 求解原多边形的聚合逼近多边形。

算法 P 求解 ROI 区域的聚合逼近多边形。

输入：原多边形顶点集合 β 和距离阈值 *dis*；

输出：逼近多边形的顶点集合 χ。

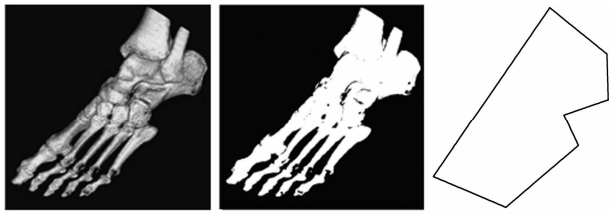
Step1　选取 β 中的任意一点 *a* 作为起始点，以逆时针方向依次选取顶点 *a* 的相邻 4 个顶点，如 *b*、*c*、*d*、*e*，作射线 *ab*、*ac*、*ad*、*ae*。

Step2　对 *ac* 、*ad* 和 *ae*，分别与顶点 *b* 、*c* 和 *d* 做垂线，得到 3 个距离，如 *b* 到 *ac* 的距离 *bx*，*c* 到 *ad* 距离 *cy*，*d* 到 *ae* 的距离 *dz*。

Step3　将 *bx* 、*cy* 和给定的阈值 *dis* 进行比较，如果 *bx* 和 *cy* 小于阈值 *dis*，并且 *dz* 大于阈值 *dis*，则选取 *d* 为紧邻 *a* 点的多边形顶点。

Step4　选择 *d* 点作为下一个起点，重复 Step1~Step3，直到重新选择 *a* 时终止，则得到最终的聚合逼近多边形的顶点集合 $\chi=\{a,d,f,i\}$。

图 2 给出了一幅医学图像，其 ROI 区域以及对应的聚合逼近多边形。



(a)原始医学图像　(b)ROI区域　(c)聚合逼近多边形

图 2　原始医学图像、ROI 区域及逼近多边形

当求解出 ROI 区域的聚合逼近多边形后，记录其顶点坐标信息作为识别 ROI 的依据。设原始医学图像的尺寸是 $M\times N$，则记录一个顶点的坐标所需的比特数为 $\mathrm{lb}M+\mathrm{lb}N$，对于一个 512×512 的图像，图 2(c)所示的多边形顶点仅需要 18×7=126 bit。

由于 ROI 区域是不规则的多边形，而绝大部分无损数据隐藏算法都是基于规则的矩形区域。所以提出用一个尺寸为 *size* 的正方形图像模式块对 ROI 进行拟合，算法 Ψ 用于得到 ROI 区域的方形图像块。

算法 Ψ 求解ROI逼近多边形的方形图像块集合。

输入：ROI，方形图像尺寸 *size*；

输出：ROI 区域中方形图像块集合 $\cup$。

Step1　初始化 $\cup=\varnothing$。

Step2　以 ROI 逼近多边形的第一个顶点为方形图像模式块的左上顶点，按从上到下从左到右顺序平移方形块对 ROI 区域进行拟合。

Step3 如果方形图像模块中的任意一个像素点在多边形之外(判断方法可采用射线法，由该点沿 x 轴方向做一条射线，与多边形出现交点的个数为奇数判定在多边形内，偶数则在多边形外)，则将方形块向下移动一单位；否则将拟合的方形图像块加入到集合∪中。

Step4 重复 Step1~ Step3，直到方形块上边界溢出 ROI 区域的最下面顶点的 X 轴。

2.2 DHCS 算法

定义 5 对于原始图像 I，I 的图像块集合可用表示为

$$I_B=\{I_b(i,j)\,|\,1\leqslant i\leqslant A,1\leqslant j\leqslant B,\ 1\leqslant b\leqslant \lfloor M/A\rfloor\lfloor N/B\rfloor\} \tag{5}$$

其中，A、B 为分块尺寸，M、N 为载体图像的维数。

定义 6 对于某图像块，其块差值可表示为

$$D_b(i,j)=\mathrm{abs}(I_b(i,j)-I_b(i,j+1)) \tag{6}$$

其中，$1\leqslant i\leqslant A,1\leqslant j\leqslant B-1$，abs(*)为取绝对值函数。

设嵌入阈值为 $L(L>0)$，那么现有差值直方图平移方法(DHS, difference histogram shifting)嵌入数据的过程如下。

Step1 对块差值构建差值直方图 DH，并根据式(7)产生嵌入间隙。

$$D_b'(i,j)=\begin{cases}D_b(i,j)+1, D_b(i,j)>L\\ D_b(i,j),\text{其他}\end{cases} \tag{7}$$

Step2 在 DH 中嵌入数据，根据式(8)计算

$$D_b''(i,j)=\begin{cases}D_b'(i,j)+1, em\_count++\\ \quad D_b'(i,j)=L\ \&\ wm=1\\ D_b'(i,j), em\_count++\\ \quad D_b'(i,j)=L\ \&\ wm=0\end{cases} \tag{8}$$

wm 代表 1bit 隐秘信息，em_count 记录差值直方图中可嵌入的隐秘数据比特数，其初值为 0。

很明显，DHS 的嵌入容量仅在于差值直方图中值为 L 的差值数量。通过分析，差值直方图中值为 0,1,…,L−1 的所有差值均可以用来隐藏数据。对式(7)和式(8)进行如下改进，得到 DHCS 嵌入数据方法：

$$D_b'(i,j)=\begin{cases}D_b(i,j)+L+1, D_b(i,j)>L\\ D_b(i,j)\qquad\quad ,\text{其他}\end{cases} \tag{9}$$

$$D_b''(i,j)=\begin{cases}D_b'(i,j)+P+1, em\_count++\\ \quad D_b'(i,j)=P\ \&\ wm=1\\ D_b'(i,j)+P, em\_count++\\ \quad D_b'(i,j)=P\ \&\ wm=0\end{cases} \tag{10}$$

P 初值为 L，向下递减直到为 0，利用式(10)可循环嵌入数据。

Step3 产生 I_b 对应的隐秘图像块，按照式(11)和式(12)生成每个图像块中每行的前 2 个像素，然后按照式(13)得到其他像素。

$$S_b(i,1)=\begin{cases}I_b(i,1),\ I_b(i,1)\leqslant I_b(i,2)\\ I_b(i,2)+D_b''(i,1),\ \text{其他}\end{cases} \tag{11}$$

$$S_b(i,2)=\begin{cases}I_b(i,1)+D_b''(i,1),\ I_b(i,1)\leqslant I_b(i,2)\\ I_b(i,2),\ \text{其他}\end{cases} \tag{12}$$

其中，$1\leqslant i\leqslant A$，$1\leqslant b\leqslant floor(MN/AB)$

$$S_b(i,j)=\begin{cases}S_b(i,j-1)+D_b''(i,j-1),\ I_b(i,j-1)\leqslant I_b(i,j)\\ S_b(i,j-1)-D_b''(i,j-1),\ \text{其他}\end{cases} \tag{13}$$

其中，$1\leqslant b\leqslant\lfloor M/A\rfloor\lfloor N/B\rfloor$，$1\leqslant i\leqslant A$，$3\leqslant j\leqslant B$。

当所有的图像块处理完毕后，生成隐秘图像 I_W。

假设嵌入阈值 L 已知，则数据提取的过程如下。

Step1 提取隐秘信息并恢复部分差值，提取和恢复式如下

$$wm=\begin{cases}0, ex\_count++, S_{Db}(i,j)=2P\\ 1, ex\_count++, S_{Db}(i,j)=2P+1\end{cases} \tag{14}$$

$$S_{Db}'(i,j)=\begin{cases}S_{Db}(i,j)-(P+1), S_{Db}(i,j)=2P+1\\ S_{Db}(i,j)-P,\text{其他}\end{cases} \tag{15}$$

其中，$1\leqslant b\leqslant\lfloor M/A\rfloor\lfloor N/B\rfloor$，$S_{Db}(i,j)$ 为隐秘图像块差值，$i\in[1,A], j\in[1,B-1]$。ex_count 为提取出隐秘信息的位数，初值设为 0；P 从 0 开始递增直到 L，利用式(14)和式(15)循环提取数据和恢复差值。

Step2 还原差值直方图间隙(将嵌入过程中的 Step1 形成的间隙还原)，按照式(16)计算。

$$R_{Db}(i,j)=\begin{cases}S_{Db}'(i,j)-(L+1), S_{Db}(i,j)>2L+1\\ S_{Db}'(i,j),\ \text{其他}\end{cases} \tag{16}$$

Step3 按式(17)和式(18)恢复每块每行的前 2 个像素，然后按照式(19)恢复其他像素。

$$RI_b(i,1)=\begin{cases}S_b(i,2)+R_{Db}(i,1), S_b(i,1)\geqslant S_b(i,2)\\ S_b(i,1),\ \text{其他}\end{cases} \tag{17}$$

$$RI_b(i,2)=\begin{cases}S_b(i,1)+R_{Db}(i,1), S_b(i,1)\leqslant S_b(i,2)\\ S_b(i,2),\ \text{其他}\end{cases} \tag{18}$$

$$RI_b(i,j)=\begin{cases}RI_b(i,j-1)+R_{Db}(i,j-1), S_b(i,j-1)\leqslant S_b(i,j)\\ RI_b(i,j-1)-R_{Db}(i,j-1),\ \text{其他}\end{cases} \tag{19}$$

其中，$1\leqslant b\leqslant \lfloor M/A\rfloor\lfloor N/B\rfloor$，$1\leqslant i\leqslant A$，$3\leqslant j\leqslant B$。

2.3　CHS 算法

传统直方图平移方法(HS, histogram shifting)利用峰值点像素值不变或者移动一个直方图间隙嵌入数据，嵌入容量仅在于峰值点的像素个数。为进一步增大嵌入容量，引入基于编码的直方图平移方法。

定义 7　直方图间隙编码。设峰值点像素值为 $peak$，则根据 $peak$ 的改变量进行信息编码如下

$$wm=\begin{cases}00, peak=peak\\ 01, peak=peak+1\\ 10, peak=peak+2\\ 11, peak=peak+3\end{cases} \tag{20}$$

对于直方图峰值点右边的像素值 $pixel$，采用式(21)形成直方图嵌入间隙。

$$pixel=pixel+3 \tag{21}$$

图 3 给出了一个 CHS 实现数据嵌入示意，图中黑色矩形代表峰值点像素值在嵌入不同数据后的变化情况，灰色矩形代表峰值点右边像素值变化情况。由于灰色背景区域像素值较小，通过式(21)调整像素值的过程中不会出现溢出现象。另外，由于移动一个直方图间隙，代表 2 位数据信息，CHS 的嵌入容量是 HS 方法的 2 倍。

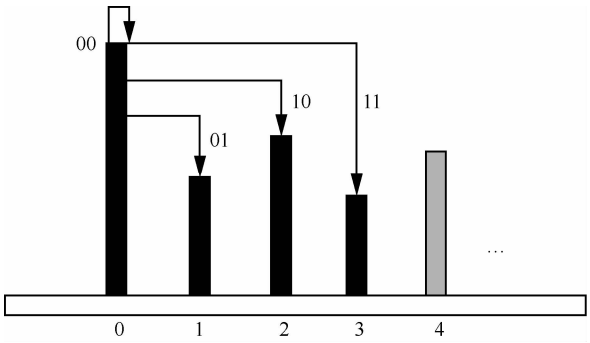


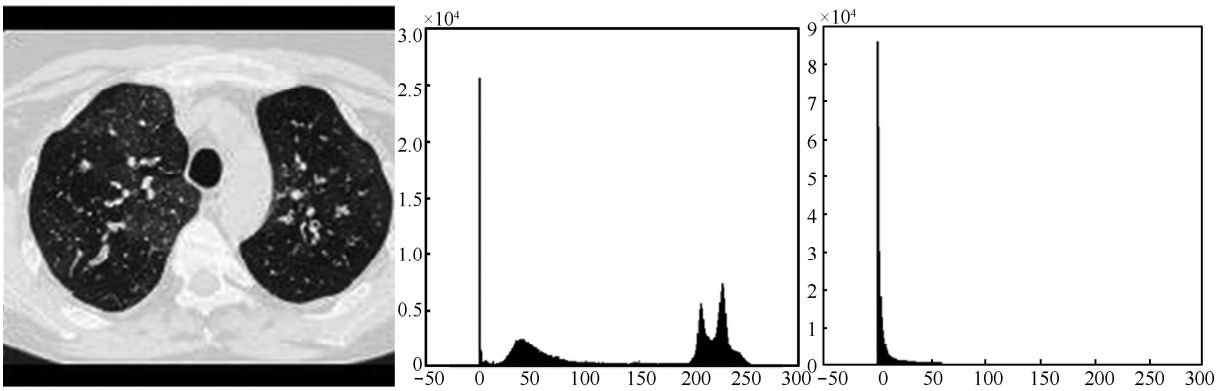
图 3　CHS 数据嵌入示意

为了证明本文改进的直方图方法在嵌入容量上的有效性，随机挑选一幅医学图像进行说明。图 4 给出了一副原始的医学图像((512×512×8) bit)、直方图和差值图像直方图，从图中可以看出，医学图像的直方图分布呈现不均匀状态，峰值点个数($peak$=0)为 25 541，而差值直方图中，由于相邻像素的高相似性，大部分差值较小，集中在 0 值附近，其中差值是 0、1、2 的分别为 86 038、63 096、29 968。

表 1 给出了分别采用原始直方图方法平移 HS、CHS、DHS、DHCS(L=2)和 CHS 方法嵌入数据的最大容量。可以看出 CHS 方法的嵌入容量是 HS 方法的 2 倍，DHCS 方法的嵌入容量甚至超过了 DHS 方法的 2 倍。虽然 CHS 和 DHCS 方法相比原有的方法在数据图像质量上有所下降，但均在可接受范围内，隐秘图像质量将在第 3 节中讨论。

表 1　不同直方图方法嵌入数据的最大容量

方法	最大嵌入容量/bit
HS	25 541
CHS	51 082
DHS	86 038
DHCS	179 162



(a)原始图像　(b)原始图像直方图　(c)差值图像直方图

图 4　原始医学图像、直方图及差值图像直方图

3 算法实施

本节介绍了提出算法的具体实施方案，包括数据的嵌入、提取、图像恢复和提取数据的完整性认证。另外，对算法的性能进行了理论上的分析，包括嵌入容量、隐秘图像质量、算法空间复杂度和时间复杂度。为了便于算法描述，表 2 给出了算法中使用的相关符号。

表 2 算法中使用的相关符号

符号	含义
I	原始医学图像
max	*ROI* 区域像素极值
ROI_I	I 的 *ROI* 区域
$RONI\_I$	I 的 *RONI* 非感兴趣区域
ROI_I_B	*ROI* 图像块集合
em_num_ROI	*ROI* 中可嵌入的数据量
ROI_I_W	嵌入数据后 ROI_I
ex_wm_1	$RONI\_I_W$ 中提取的数据
R_ROI_I	恢复后 ROI_I 区域
$sign$	ROI_I 预处理标志
L	差值直方图平移阈值
ROI_index	*ROI* 区域顶点坐标
BE	电子病历的二进制形式
R_BE	*ROI* 中未嵌完的信息
S_I	原始图像认证码
$RONI\_I_W$	嵌入数据后 $RONI\_I$
I_w	含隐秘数据医学图像
ex_wm_2	ROI_I_W 提取的数据
R_RONI_I	恢复后 $RONI\_I$ 区域
R_I	恢复后医学图像

3.1 数据嵌入

算法 Embed_bits 用来实现信息的可逆嵌入

输入：I、隐私数据 BE、嵌入阈值 L、方形图像块尺寸 $size$

输出：I_W

抽象算法描述如下。

Embed_bits(I, BE, L, $size$){

将 I 划分为 ROI_I 和 $RONI\_I$;

使用算法 P 得到 ROI 区域的聚合多边形，记下 ROI_index;

得到 ROI_I 区域的最大像素 max;

If $\max+L+1>2^{depth}-1$

将 ROI_I 所有像素减去 L+1;

设 $sign$=1;

Else

设 $sign$=0;

End if

使用算法 Ψ 得到 ROI_I_B;

构造 ROI_I_B 的差值直方图并使用式(9)产生直方图间隙;

读入 BE 并得到其长度 len (BE);

For each block in ROI_I_B

使用式(10)~式(13)将 BE 嵌入在 ROI_I_B 中，得到 em_num_ROI 和 ROI_I_W;

R_BE= len (BE)-em_num_ROI;

End For

使用 SHA-256 算法得到 S_I;

If R_BE >0

待嵌入的数据 D 表示为 $S_I \oplus R\_BE$;

Else

D= S_I;

End If

在 $RONI\_I$ 区域构建直方图，得到峰值点 $peak$ 和峰值点像素个数 num;

使用式(21)产生间隙;

If $len(D) \leqslant 2num$

$len(D) = 2num$;

End If

For the all data in D

使用式(20)在 $RONI\_I$ 区域中实现嵌入，得到 $RONI\_I_w$;

End For

结合 ROI_I_W 和 $RONI\_I_w$ 得到隐秘图像 I_W;

}

嵌入过程中，首先将原始图像划分成 ROI 和 RONI 区域，对 ROI 区域利用算法 P 和 Ψ 得到方形图像块集合，将电子病历转换为二进制流的数据信息，采用 DHCS 方法嵌入在 ROI 区域。在 RONI 区域，首先形成直方图，获取峰值点和极限嵌入容量，将图像的认证码和可能未嵌完的电子病历数据采用 CHS 方法嵌入在 RONI 区域。

为了实现盲提取，将 ROI_index 信息、方形图像块尺寸 $size$、$sign$、len (BE)信息、len (D)、阈值 L 和峰值 $peak$ 作为密钥信息 key 以安全方式传给解密端。

3.2　数据提取、图像恢复与认证

算法 Extract_bits 用来实现数据信息的提取、图像恢复和数据有效性认证。假设解密密钥 *key* 已知。

输入：I_W，*ROI_index*，*sign*，*len*(*BE*)，*len*(*D*)，*peak*，*L*，*size*

输出：*I*，隐私数据 *BE*

抽象算法描述如下。

Extract_bits(I_W, *ROI_index*, *len*(*BE*), *len*(*D*), *L*, *size*, *sign*, *peak*){

获取密钥 *key* 得到 *ROI_index*、*sign*、*len*(*BE*)、*len*(*D*)、*peak*、*L*、*size* 等信息；

根据 *ROI_index* 将 I_W 划分为 ROI_I_W 和 $RONI\_I_W$ 区域;

构造 $RONI\_I_W$ 直方图;

For *i*=1: *len*(*D*)

使用 CHS 方法提取嵌入的数据 ex_wm_1，长度为 *len*(ex_wm_1);

恢复 $RONI\_I_W$ 得到 *R_RONI_I*;

End For

获取 ex_wm_1 的前 256 bit 作为认证码 S_I;

If (*len*(ex_wm_1)>256)

R_BE= ex_wm_1−256;

End If

使用算法 Ψ 和 *ROI_index* 信息得到 ROI_I_{WB};

For each block *B* in ROI_I_{WB}

构建每个图像块的差值直方图;

使用式(14)~式(19)提取隐秘数据 ex_wm_2 并且恢复 ROI_I_W 得到 *R_ROI_I*;

If sign==1

将 *R_ROI_I* 区域像素值加上 *L*;

End If

End For

结合 *R_RONI_I* 和 *R_ROI_I* 得到恢复图像 *R_I*;

重新计算 *R_I* 的认证码 new_S_I;

If S_I ==new_S_I

提取出数据有效并且 *BE*= *R_BE*+ ex_wm_2;

Else

提取出数据无效;

End If

}

数据提取过程是嵌入的逆过程，首先提取 RONI 区域的数据信息，前 256 bit 为提取出的图像认证码，其余为 ROI 中未嵌完的电子病历信息；其次在 ROI 区域提取数据信息，恢复图像后重新计算图像认证码，如果计算出来的认证码与提取出的一致，则说明提取的电子病历有效，否则，提取无效。

3.3　方案性能分析

1) 嵌入容量

设原始载体图像维数为 *M*×*N*，*ROI_I* 像素个数为 *num_ROI*，嵌入阈值为 *L*，ROI_I_B 中差值为 *l* 的个数为 *num_l*，则 *ROI_I* 可嵌入数据量 *em_num_ROI_I* 可表示为

$$em\_num\_ROI\_I=\sum_{l=0}^{L} num\_l \tag{22}$$

其中，$em\_num\_ROI\_I\in[0,num\_ROI]$。

设 *RONI_I* 区域中处于峰值点像素个数为 *num_peak*，则 *RONI_I* 可嵌入数据量 *em_num_RONI_I* 为 2*num_peak*。那么，原始载体图像 *I* 的总的嵌入容量为

$$em\_num\_I=\sum_{l=0}^{L} num\_l+2num\_peak \tag{23}$$

2) 隐秘图像质量

ROI_I 区域的失真中最极端的情况是所有的像素都调整了 *L*+1 个幅度（包含直方图间隙生成和数据嵌入过程），则 *ROI_I* 区域的隐秘图像质量为

$$\begin{cases} PSNR\_ROI\_I=10\lg\left(\dfrac{255\times255}{MSE}\right) \\ MSE=(L+1)^2 \end{cases}$$

在 *L*=3 情况下，*PSNR_ROI_I* 约为 38.59 dB。

对于 *RONI_I* 区域，最极端的情况是所有像素值都增加了 3，则 *PSNR_RONI_I* 的最小值约为 38.59 dB。综上所述，基于区域和直方图平移方法的隐秘图像质量大于 38.59 dB。当然当嵌入阈值 *L* 增大时，隐秘图像质量会有所下降。

3) 空间复杂度

本文算法在图像的像素级嵌入数据，不需要额外的储存空间。唯一的传输负载为密钥 *key*，相比大容量的图像数据传输，*key* 的长度在可接受的范围之内。

4) 时间复杂度

算法的时间消耗主要在于对图像像素的扫描操作中，其中：1)基于类间距最大的 ROI 区域提取算法的时间复杂度表示为 *O*(*NN*)，其中，*N* 为载体图像的像素个数；2)聚合逼近多边形表示和 ROI 区域图像块生成算法可以看作是对 ROI 区域的一次

扫描，其时间复杂度为 $O(N)$；3) DSCH 算法需要对 *ROI_I* 区域扫描 L 次，每次时间复杂度为 $O(N)$，则总的时间复杂度为 $O(LN)$；4) CHS 算法需要对 *RONI_I* 扫描一次，时间复杂度为 $O(N)$；综上，考虑到阈值 L 为较小的整数，算法的总的时间复杂度为

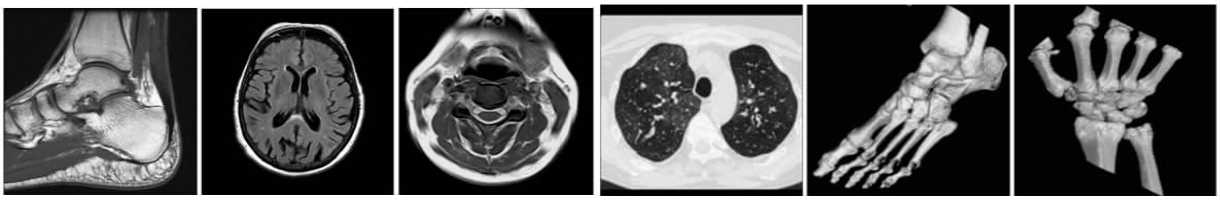
$$O(NN)+O(LN)+O(N)+O(N)=O(N^2)$$

4 实验分析

实验中采用的医学图像载体和电子病历均来自中南大学湘雅医院数据中心，图片格式为 JPG，512×512 的 8bit 灰度图像，电子病历为 XML 格式。实验中，随机选择了 60 幅（MRI 和 CT 各 30 幅）做了实验分析。主机的配置为 CPU Intel(R) Core(TM) Duo 1.86 GHz，主存 1 GB，操作系统为 Windows XP，使用 Matlab 7.0 作为编程环境。所有实验数据来自于 Matlab 仿真结果，选取其中 6 幅（MRI 和 CT 各 3 幅）图像的相关数据。6 幅选取的载体医学图像如图 5 所示。当隐秘图像未受到攻击时，方法能正确提取出嵌入的数据，并且重新计算的认证码与提取出的认证码完全一致，恢复出图像与原始图像完全一致，证明了方法的有效性。当数据图像遭到更改，如 JPEG 压缩时，图像认证失败，提取出数据无效，证明了方法的脆弱性。

表 3 给出了 6 幅载体图像采用基于最大类间距提取 ROI 区域时的分割阈值和 RONI 中的峰值点个数及像素值。当 ROI 嵌入阈值 L=2 和拟合图像块尺寸为 8×8 的情况下(不特殊说明时的默认阈值和尺寸)，不同载体图像的 ROI 的最大嵌入容量、*sign* 标识和整幅图像的最大嵌入容量和隐秘图像质量。由于医学图像的像素分布特殊性，大量的像素分布在灰度空间的 2 个极值点附近，采用单一的无损数据隐藏方法很难解决嵌入过程中的溢出问题。本文算法将医学图像分成 ROI 和 RONI 后，由于 ROI 区域像素通常处于灰度空间的上半区，而 RONI 像素处于下半区，采用简单的处理方法即可较好地解决溢出问题，如表 3 中的 *sign*=1 说明 ROI 区域存在有像素会产生溢出，只需将 ROI 像素统一减去阈值 L 即可防止溢出。另外从表 3 中可以看出，6 幅载体图像的最大嵌入容量均在 0.6 bit/pixel 以上，3 幅图像的嵌入容量甚至超过了 1 bit/pixel。

图 6 给出了 6 幅载体图像在不同嵌入容量下的隐秘图像质量。从图中可以看出，随着嵌入容量的增大，隐秘图像的质量下降，因为像素值发生改变的几率增大。另外 MRI_脚踝、MRI_宫颈和 CT_肺部图像由于 RONI 区域较少，并且 ROI 中纹理相对比较复杂，其最大嵌入容量小于 1 bit/pixel，其中 MRI_脚踝图像纹理最复杂，像素间差值较大，其嵌入容量最小；而 MRI_脑部、CT_足部和 CT_手腕图像中均存在大量的 RONI 区域，其最大嵌入容量可达 1.3 bit/pixel 左右。其中，CT_手腕图像嵌入容量最大，一方面是因为 RONI 区域较大，另一方面是由于 ROI 中像素的相关性较高，并且其 ROI 中没有处于像素值上界的像素，不需要对 ROI 中整体像素进行调整，所以隐秘图像质量也最好。



(a) MRI_脚踝 (b) MRI_脑部 (c) MRI_宫颈 (d) CT_肺部 (e) CT_足部 (f) CT_手腕

图 5 原始载体医学图像

表 3 载体图像的分割阈值以及最大嵌入容量和隐秘图像质量(L=2,*size*=8)

载体图像	分割阈值	ROI 嵌入容量/bit	*sign*	*ROI_index* 长度/bit	RONI 峰值个数	最大嵌入容量/bit	隐秘图像质量 *PSNR*/dB
MRI_脚踝	106	61 571	1	108	49 256(*peak*=13)	160 083	38.88
MRI_脑部	60	50 843	1	144	131 882(*peak*=0)	314 607	40.00
MRI_宫颈	106	45 508	0	180	88 420(*peak*=0)	222 348	41.58
CT_肺部	129	129 771	1	108	24 213(*peak*=0)	178 197	38.63
CT_足部	91	43 615	1	126	145 950(*peak*=3)	335 515	40.17
CT_手腕	79	41 363	0	162	148 813(*peak*=3)	338 989	42.28

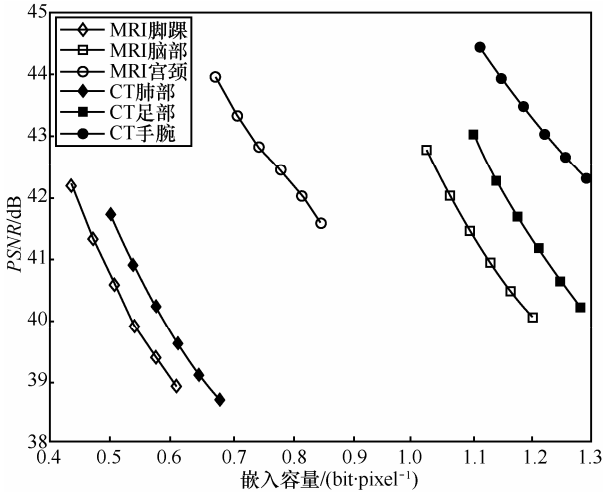


图 6　不同载体医学图像在不同嵌入容量下的隐秘图像质量

图 7 给出了在不同嵌入阈值 L 的情况下，MRI_脑部图像的嵌入容量和图像质量。从图中可以看出，随着阈值 L 的增大，载体图像的嵌入容量增大，隐秘图像的质量下降。当 L=2 时，嵌入容量增长幅度较大，隐秘图像的峰值信噪比均大于 40 dB。当 L=3 或 4 的时候嵌入容量增幅较小，并且隐秘图像质量降低，低于 40 dB。虽然在 $PSNR \geqslant 30$ dB 时，肉眼感觉不出隐秘图像与原始图像的差异[3]。在嵌入容量和隐秘图像之中进行折中，算法中取阈值 L=2。

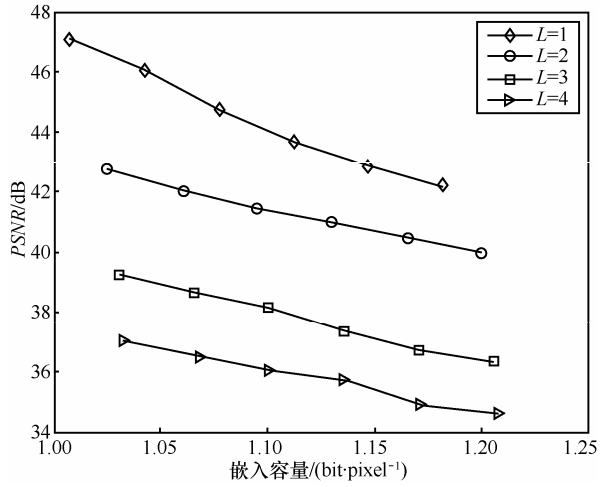


图 7　不同嵌入阈值对图像嵌入容量和隐秘图像质量影响

图 7 给出了 ROI 区域中，不同尺寸的图像模式块对载体图像嵌入容量和隐秘图像质量的影响。从理论上来分析，当采用较小的图像模式块对 ROI 区域进行拟合时，能得到更多的 ROI 区域方形图像块，但是 DHCS 算法中，每块的嵌入极限容量是与尺寸有关的。假设图像模式块的尺寸为 4×4，则每块的极限嵌入容量是 0.75 bit/pixel，当尺寸为 6×6 时，每块的极限容量是 0.83 bit/pixel。但是随着图像模式块的增大，由于 ROI 边界区域不规则，一个 6×6 块中只要有一个像素处于 ROI 之外，则要损失 35 个 ROI 像素。那么，需选取一个合适尺寸的图像模式块。从图 8 可以看出，当图像模式块为 8×8 时载体图像的嵌入容量最大，当上升到 10×10 和 16×16 时，嵌入容量不再增加并且呈下降趋势。所以算法中的图像模式块选为 8×8。

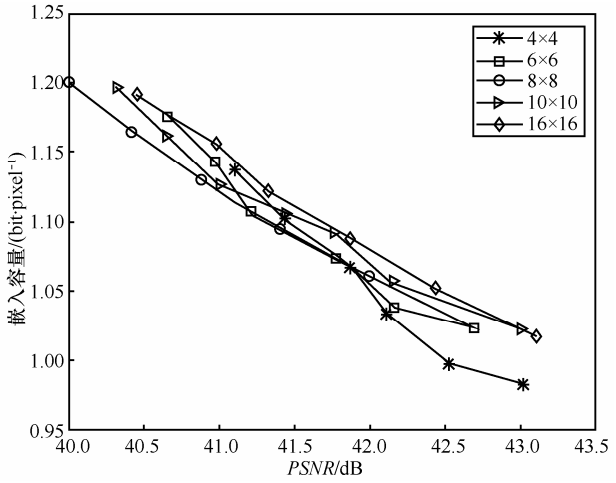


图 8　不同尺寸的图像模式块对图像嵌入容量和隐秘图像质量影响

表 4 比较了本文算法和 Tan 的方法[12]、Hong 的方法[13]的嵌入容量和隐秘图像质量。Tan 的方法将整幅图像进行固定分块，利用块中像素之间的差值嵌入数据。Hong 方法采用预测算法得到像素值的预测值，利用真值与预测值的差值直方图嵌入数据。表中嵌入容量均为最大值，实验中 Tan 方法的分块尺寸选 2×2，默认选块中的第一个像素为参考像素，调整阈值为 2。Hong 的方法中嵌入阈值选为 2，采用像素的四邻域进行预测。本文算法在隐秘图像质量上比 Tan 的要差，但是嵌入容量具有明显优势。Hong 方法的图像质量和本文算法基本一致，虽然在有些载体图像上容量具有优势，特别是当 RONI 区域较少时。但是 Hong 方法的极限容量始终无法超过 1 bit/pixel，而本文算法的最高容量可达到 1 bit/pixel 以上。针对文献[14]所提出的方法，虽然其得到的嵌入容量和隐秘图像质量优于本文方法，但并没有考虑到医学图像的分区域特性。另外由于 ROI 区域纹理比较复杂，文献[14]方法选择跳过图像块方差大的区域，对 ROI 区域缺乏有效保护，本文方法充分考虑到图像的分区域特性，特别适合于存

在连续 RONI 区域的载体图像中大容量信息隐藏。

表 4 本文方法与其他 2 种相似算法的比较

载体图像	Tan 的方法		Hong 的方法		本文方法	
	容量	图像质量	容量	图像质量	容量	图像质量
MRI_脚踝	0.452	43.13	0.746	38.82	0.611	38.88
MRI_脑部	0.685	42.67	0.945	40.54	1.200	40.00
MRI_宫颈	0.523	43.42	0.891	41.06	0.851	41.58
CT_肺部	0.416	40.76	0.768	38.67	0.686	38.63
CT_足部	0.713	42.96	0.958	40.43	1.287	40.17
CT_手腕	0.724	44.12	0.974	42.87	1.294	42.28

5 结束语

基于医学图像分感兴趣和非感兴趣区域的特性，本文提出了一种基于区域和直方图平移的无损数据隐藏方法，采用类间最大距的单阈值分割方法对感兴趣区域进行提取，并对 ROI 区域进行聚合多边形逼近表示。在 ROI 区域，对基于差值直方图平移方法进行改进，采用直方图循环平移方法嵌入电子病历等隐私数据；在 RONI 区域采用改进的基于编码的直方图方法嵌入图像的认证码。在提取阶段，重新计算恢复后图像的认证码，与提取出的认证码比较判定提取出隐私数据的有效性。算法实现了医学图像中的大容量无损数据隐藏和有效性认证。算法的创新之处在于提出了一个自动化生成 ROI 区域的方法，在不同区域中采用改进的直方图平移方法嵌入数据，较好地控制了溢出和提高了嵌入容量。实验结果表明，与现有的算法相比，算法在嵌入容量和隐秘图像质量上具有优势。该算法的局限在于只适用于具有明显分区域特征的医学图像，下一步的研究工作将考虑在区域特性不明显的医学图像中进行可逆数据隐藏。本文算法适应于在医学图像中进行隐私保护、秘密通信等用途。

参考文献：

[1] HU J K, CHEN H H, HOU T W. A hybrid public key infrastructure solution(HPKI) for HIPAA privacy/security regulations[J]. Computer Standards & Interfaces, 2010, 32(5-6):274-280.

[2] PENG F, LEI Y Z, LONG M, *et al*. A reversible watermarking scheme for two-dimensional CAD engineering graphics based on improved difference expansion[J]. Computer-Aided Design, 2011, 43(8):1018-1024.

[3] 曾骁, 陈真勇, 陈明等. 基于零系数索引的可逆图像水印[J]. 计算机研究与发展, 2010,47(7):1304-1312.
ZENG X, CHEN Z Y, CHEN M, *et al*. Invertible image watermarking based on zero coefficient index[J]. Journal of Computer Research and Development, 2010,47(7):1304-1312.

[4] YU A M, WU K, WANG C M. A distortion-free data hiding scheme for high dynamic range images[J]. Displays, 2011, 32(5):225-236.

[5] DENG X H, CHEN Z G, ZENG F, *et al*. Authentication and recovery of medical diagnostic image using dual reversible digital watermarking[J]. Journal of Nanoscience and Nanotechnology, 2013,13(3): 2099-2107.

[6] 张显全, 谢绍敏, 王晓云等. 基于相邻像素的可逆大容量信息隐藏算法[J]. 电子科技大学学报, 2012,41(4):491-495.
ZHANG X Q, XIE S M, WANG X Y, *et al*. High-capacity reversible data hiding based on neighboring pixels[J]. Journal of University of Electronic Science and Technology of China, 2012,41(4):491-495.

[7] CHEN C C, TSAI Y H. Adaptive reversible image watermarking scheme[J]. The Journal of Systems and Software, 2011, 84(3): 428-434.

[8] 张秋余, 孙媛, 晏燕. 基于分块自适应压缩感知的可逆水印算法[J]. 电子与信息学报, 2013, 35(4):797-804.
ZHANG Q Y, SUN Y, YAN Y. A reversible watermarking algorithm based on block adaptive compressed sensing[J]. Journal of Electronic & Information Technology, 2013,35(4):797-804.

[9] GUO X T, ZHUANG T G. A region-based lossless watermarking scheme for enhancing security of medical data[J]. Journal of Digital Imaging, 2009,22(1):53-64.

[10] DUAN C J, MA J F, ZHANG Y B, *et al*. Energy conduction model and its application in medical image segmentation[J]. Journal of Software, 2009, 20(5): 1106-1115.

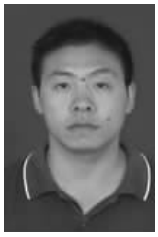
[11] GE Q, XIAO L, ZHANG J, WEI Z H. An improved region-based model with local statistical features for image segmentation[J]. Pattern Recognition, 2012, 45(4):1578-1590.

[12] TAN C K, NG J C, XU X T, *et al*. Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability[J]. Journal of Digital Imaging, 2011, 24(3): 528-540.

[13] HONG W, CHEN T S. A local variance-controlled reversible data hiding method using prediction and histogram-shifting[J]. The Journal of Systems and Software, 2010,83(12):2653-2663.

[14] 黄斌, 史量, 邓小鸿等. 自适应高容量医学图像可逆数据隐藏算法[J]. 计算机应用, 2012,32(10):2779-2782.
HUANG B, SHI L, DENG X H, *et al*. Adaptive high-capacity reversible data hiding algorithm for medical images[J]. Journal of Computer Applications, 2012,32(10):2779-2782.

作者简介：



邓小鸿（1982-），男，湖北天门人，博士，江西理工大学讲师，主要研究方向为网络信息安全。

陈志刚（1964-），男，湖南益阳人，中南大学教授，主要研究方向为分布式计算与信息安全等。

梁涤青（1979-），男，湖南涟源人，中南大学博士生，主要研究方向为混沌密码学与信息安全等。

毛伊敏（1971-），女，新疆伊犁人，博士，江西理工大学副教授，主要研究方向为智能信息处理。