维普资讯 http://www.cqvip.com

一种多级混沌图像加密算法研究

韦鹏程[1] 张 伟[1,2] 杨华千[1,2]
(重庆教育学院计算机与现代教育技术系 重庆400067)[1]
(重庆大学计算机科学与工程学院 重庆400044)[2]

摘 要 由于图像本身具有数据量大、像素点之间高相关性和高冗余性等特点,因此不能用一般的文本加密算法来进行图像加密。而混沌具有初始条件和参数敏感性、遍历性和混合性等优良特性,混沌图像加密是一种效率高、安全性好的图像加密方法。本文提出了一种多级混沌图像加密算法,首先对二维混沌进行离散和规范化,用其对图像像素点进行空间置乱,然后用混合混沌序列对图像的像素灰度值扩散进一步掩盖明文和密文的关系,因而该方法可以有效地抵抗统计和差分攻击。同时,对提出的算法进行仿真实验和安全性分析,结果表明该算法具有安全性高,加密速度快等特点。

关键词 混沌,图像加密,混沌密码,混合混沌序列

Study on Multistage Chaotic Image Encryption Algorithm

WEI Peng-Cheng[1] ZHANG Wei[1,2] YANG Hua-Qian[1,2]
(Department of Computer and Modern Education Technology, Chongqing Education College, Chongqing400067)[1]
(Department of Computer Science and Engineering, Chongqing University, Chongqing400044)[2]

Abstract Encryption of image is different from that of texts due to some intrinsic features of images such as bulk data capacity and high redundancy, which are generally difficult to handle by traditional methods. Due to the exceptionally desirable properties of mixing and sensitivity to initial conditions and parameters of chaotic maps, chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. In this paper, a multistage chaotic image encryption algorithm is proposed, at first, the two-dimensional chaotic Baker map is generalized and discretized. This new scheme employs the generalized and discretized shuffle the-positions of image pixels and uses mixed chaotic sequences to confuse the relationship between the cipher-image and the plain-image, there by significantly increasing the resistance to statistical and differential attacks. Thorough experimental tests are carried out with detailed analysis, demonstrating the high security and fast encryption speed of the new scheme.

Keywords Chaos, Image encryption, Chaotic cipher, Mixed chaotic sequences

1 引言

随着 Internet 技术和多媒体技术的飞速发展,多媒体通信逐渐成为人们进行信息交流的重要手段。多媒体信息特别是图像的安全与保密显得越来越重要。然而,由于图像本身具有一些比如数据量大、像素点之间高相关性和高冗余性等特点,传统的加密算法如 DES、IDEA 和 RSA 将图像作为普通数据流进行加密,而不考虑图像本身的特性,因而具有一定的局限性。近几年来,研究人员提出了许多基于混沌图像加密算法[1~7],相对于传统加密算法,这些算法在安全性、复杂性、速度等性能方面具有优越性。现有的研究成果表明混沌和密码学之间有着密切的联系,比如传统的密码算法敏感性依赖与密钥,而混沌映射依赖与初始条件参数和参数;传统的加密算法通过加密轮来达到扰乱和扩散,混沌映射通过迭代,将初始域扩散到整个相空间;传统加密算法定义在有限集上,而混沌映射定义在实数域内,但是目前还没有建立一套关于混沌与密码学深层次关系的理论。

混沌在密码学的应用可以最早追溯到1989年数学家 Mathhews[8]首先提出了混沌加密方法,随后在1991年欧洲密码学年会上,出现了多种混沌密码体制,但是关于混沌图像加密算法并不多见。在文[9]中提出了一种基于混沌密钥的算法(CKBA),该算法首先用混沌产生一个时间序列,然后用它产生0-1序列作为密钥,通过0-1序列的产生,图像的像素被重新排列然后用产生的密钥来与像素值进行异或运算。这种方法非常简单,但是在文[10]中指出该方法在安全性方面存在缺陷:不能抵抗选择/已知明文攻击,并且是否经得起蛮力攻击也值得讨论。文[6]中提出了一种混沌 K 熵流的图像加密算法,该方法把图像分成块然后在密钥流控制下重新排列图像块。文[11]中,提出了一种多级数字混沌视频算法(CVES, Chaotic video encryption scheme),该方法以一个混沌映射控制2" 混沌映射,通过这种方法产生的伪随机序列来掩盖和重排视频信号,该方法声称能够适应于任何视频压缩算法,在实时数字视频方法安全性高并且加密速度快。

本文充分考虑了图像内在特性和混沌系统的特性基础上,提出了一种基于二维混沌映射的多级混沌图像加密算法。首先用二维混沌映射对图像的像素位置进行扰乱,然后用混合混沌序列来隐藏图像明文和密文的相关性。文章的第2节描述该算法的具体过程,第3节详述算法设计,首先对二维 Baker 映射进行改进,并对图像进行空间置乱,提出一种混合混沌序列的生成方法,并用该序列来对图像的像素灰度值进行二次加密,以提高其安全性,第4节从理论和实验两个方法进行了详细的论证和分析,最后则是本文的结论。

2 算法描述

对于任一图像 I,设 I 的大小由 $N\times N$ 个像素点构成,且 $I(x,y)$ 表示像素点 (x,y) 的灰度值。二维混沌映射的多级分

维普资讯 http://www.cqvip.com

组图像加密算法的具体过程如下：

(1)二维映射的选择和设计。在这一步中，选择一种正方形[0,1]×[0,1]到自身的二维混沌映射，然后引进一些参数对它进行改进；

(2)对改进的映射进行离散化和规范化，以适合于图像的像素点空间置乱；

(3)结合收缩式发生器，利用 m-序列和混沌序列产生混合混沌序列；

(4)用混合混沌序列扩散图像的像素灰度值，以进一步提高安全性。

整个算法的过程如图1所示。

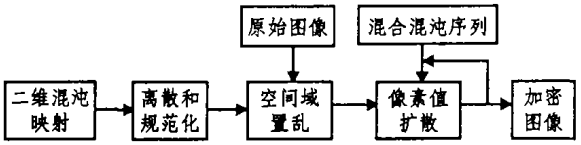

图1　多级混沌图像加密流程

3　算法设计

3.1　图像像素点空间置乱

通常情况下，对图像置乱有两种方式，一是直接对图像中各像素点的坐标位置进行线性或非线性变换，二是先对图像进行分块，再置乱。但由于分块后的置乱只在图像的局部进行，从整体上讲置乱程度不高。线性变换中往往采用经典的 Arnold 变换 $A_N^k: Z_j \to Z_j$，其定义为：

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\ N) \tag{1}$$

这种变换具有周期性，如当 $N=60$时，其周期为60，当 $N=128$时，周期为96，这种置乱变换是线性确定的，与密钥无关，安全程度也不高。因此，在本算法中，我们根据混沌密码学的方法[12]，运用 Baker 映射所产生的混沌序列，采用第一种方式对图像进行非线性置乱。

对连续型的 Baker 映射是一种 $I \times I$ 的混沌双射：

$$\begin{cases} B(x,y)=(2x,y/2) & 0 \leqslant x \leqslant 1/2 \\ B(x,y)=(2x-1,y/2+1/2) & 1/2 \leqslant x \leqslant 1 \end{cases} \tag{2}$$

其作用效果如图2所示。为适合于图像处理，需要对其进行离散和规范化处理。其方法如下：把图3的正方形划分成 K 个长方形，即：$[F_{i-1},F_i)\times[0,1), i=1,\cdots,k, F_i=p_1+\cdots,p_i, F_0=0$，比如：$p_1+\cdots+p_k=1$。那么用公式表达为：

$$B(x,y)=((x-F_i)/p_i, p_i y+F_i), (x,y)\in[F_i,F_i+p_i)\times[0,1) \tag{3}$$

并且离散和规范化结果符合以下渐近性质：

$$\lim_{N\to\infty}\max_{0\leqslant i,j<N}|f(i/N,j/N)-F(i,j)|=0 \tag{4}$$

其中 f 为连续的 Baker 映射，F 为离散化的表达式。

设 $N\times N$ 的图像每边用整数 k 整除，分别用 $n_1,n_2,\cdots,n_k$ 表示，其中 $n_1+\cdots+n_k=N, N_i=n_1+\cdots+n_i$，离散后的 Baker 映射如图2所示。对像素点 $(r,s), N_i\leqslant r<N_i+n_i, 0\leqslant s<N$，经过一次 Baker 映射迭代后，其像素点坐标变换为：

$$B_{(n_1,\cdots,n_k)}(r,s)=(\frac{N}{n_i}(r-N_i)+s \bmod \frac{N}{n_i}, \frac{N}{n_i}(s-s \bmod \frac{n_i}{N})+N_i) \tag{5}$$

对 Lenna 图像用离散规范化后的 Baker 映射进行1次和9次变换的效果见图4所示。

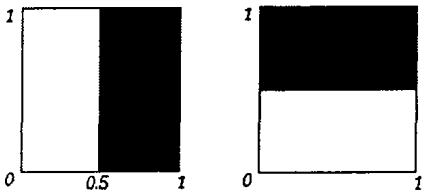

图2　连续 Baker 映射变换

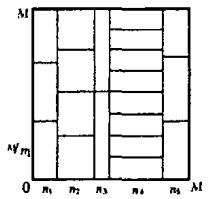

图3　离散 Baker 映射

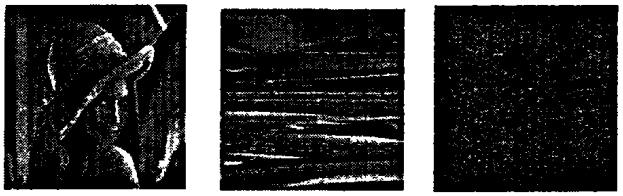

图4　Baker 映射对 Lenna 的变换效果图

3.2　像素值的扩散

混乱与扩散是设计密码的两条基本指导原则，上面的二维映射的非线性变换只是对图像的像素进行重新分布，并没有改变像素值，因此变换前后图像的直方图不会改变。为此，引入像素灰度值的扩散变换，进一步改变直方图。为了克服有限精度对混沌系统的影响，我们结合自收缩式密钥流生成器设计一种混合混沌序列，然后用这种序列对图像像素灰度值进行扩散变换。

3.2.1　*混沌序列的产生*　给定的 Hénon 映射的方程为：

$$\begin{cases} x_{n+1}=1-px_n^2+y_n \\ y_{n+1}=qx_n \end{cases} \tag{6}$$

它是一个二维的非线性混沌系统，当$1.050<p<1.085, q=0.3$时，系统产生混沌现象。该系统具有很多优良特性，在非线性研究领域，对 Hénon 映射的混沌特性的研究比较深入[13,14]。本文只对其混沌行为和密码学特性进行分析。下面我们对它的密码学特性进行定性分析。

1) Hénon 映射一大特点是对初始值有极其敏感的依赖性。因此通过改变 Hénon 映射参数及其初始值便可以得到数量巨大的平移相异的混沌序列，即混沌序列的码量大，混沌序列的这一优点很适合于密码系统的密钥流生成函数。图5为初值仅相差10^{-4}初值迭代100次的 x 轨道图。

2)Hénon 映射具有优良的伪随机性，其轨道的演化是非周期、不收敛的，具有很好的随机性及不可预测性。我们取初值 $x=0.20, y=0.10$(作为密钥 k 的一部分)，对映射进行迭代。取序列长度 $N=5000$，相关间隔 $M=1000$，对其混沌实值序列按如下公式计算相关函数 $R_x(m)$：

$$R_x(m)=\begin{cases} \dfrac{1}{N-m}\displaystyle\sum_{n=1}^{N-m} X_n Y_{n+m} & m=0,1,\cdots,M \\ \dfrac{1}{N-|m|}\displaystyle\sum_{n=|m|}^{N} X_n Y_{n+m} & m=-1,-2,\cdots,-M \end{cases} \tag{7}$$

维普资讯 http://www.cqvip.com

当取 $Y=X$ 时，其非周期自相关如图6，改变初值为 $x_0=0.2001$，$y=0.1001$时两个混沌序列的互相关特性如图7。可见其具有很好的密码学所需要的相关特性。

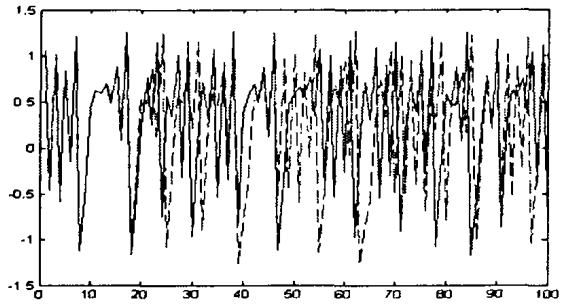

图5 混沌轨道对初值敏感性

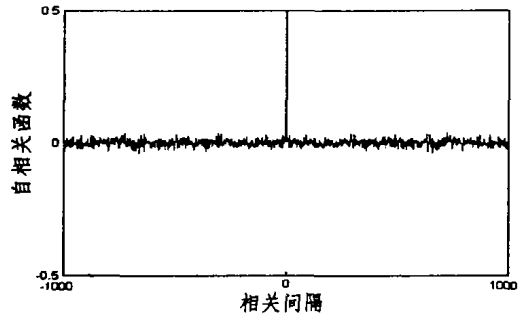

图6 自相关特性

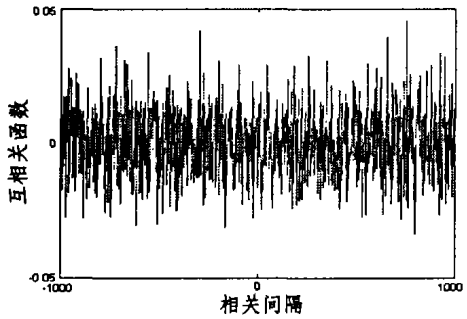

图7 互相关特性

3.2.2 随机二进制序列的产生 从混沌系统中提取随机二进制序列的方法比较多[15]，为提高系统的安全性，我们希望提取的方法是单向的、不可逆的，所得到的序列是随机的、最好还是统计独立且同分布的。本文采用以下方法：

首先将 Hénon 映射轨道的实数值 x(或者 y)写为：

$$|x|=0.B_1(x)B_2(x)\cdots B_i(x)\cdots, B_i(x)\in\{0,1\} \tag{8}$$

其第 i 个比特 $B_i(x)$可表示为：

$$B_i(x)=\sum_{r=1}^{2^i-1}(-1)^{r-1}\Theta_{r/2^i}(x) \tag{9}$$

其中 $\Theta_t(x)$是阈值函数，定义为：

$$\Theta_t(x)=\begin{cases}0 & |x|<t\\ 1 & |x|\geqslant t\end{cases} \tag{10}$$

根据 Kohda 的证明，序列$\{B_i(x_n(x))\}_{n=0}^{\infty}$($n$ 为迭代次数)确实是独立同分布的随机二进制序列。

3.2.3 混合混沌序列的产生 混沌序列的生成器总是在有限精度器件实现的，使得任何混沌序列最终是周期的。为了克服有限精度对混沌系统的影响，我们结合自收缩式密钥流生成器[16]，提出了一种混合混沌序列的生成方法，图8为混合混沌序列生成的方框图。

(1) 输入：两个线性反馈移位寄存器 $LFSR_1$和 $LFSR_2$的初态 $m_0^{(1)}$，$m_0^{(2)}$；Hénon 映射两个初值 x_0、y_0和控制参数 p、q；

(2)线性反馈移位寄存器 $LFSR_1$产生序列为$\{m_i^{(1)}\}$；

(3)线性反馈移位寄存器 $LFSR_2$产生序列为$\{m_i^{(2)}\}$；

(4)给定初始值 x_0和 y_0，Hénon 映射产生数字混沌序列为 $x_i^{(1)}$ 和 $y_i^{(2)}$；

(5)作运算 $s_i^{(1)}=m_i^{(1)}\oplus x_i^{(1)}$，$s_i^{(2)}=m_n^{(2)}\oplus y_i^{(2)}$；

(6)若 $s_i^{(1)}=1$；则置 $k_i=s_i^{(2)}$；若 $s_i^{(1)}=0$；则删去 $s_i^{(2)}$。

(7)输出：混合混沌序列$\{k_i|i=1,2,\cdots\}$。

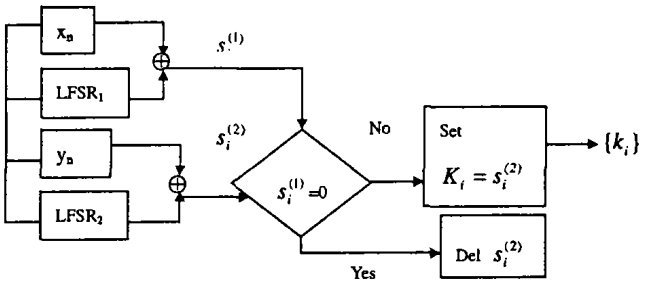

图8 混合混沌序列生成的方框图

3.2.4 像素值扩散 假设空间置乱后得到图像的像素值为 $I(i)$，混合混沌序列为$\{k_i\}$，那么通过式(11)可以把当前的像素值进行扩散：

$$C(i)=\{k_i\oplus\{[I(i)+k_i]\bmod N\}\oplus C(i-1) \tag{11}$$

式中，$C(i)$为当前像素加密后得到的密文，$C(i-1)$为前一个像素的密文，n 为图像的颜色数，比如：对于256色数的图像，$N=256$。上式的逆变换为：

$$I(i)=\{k_i\oplus C(i)\oplus C(i-1)+N-k_1\}\bmod N \tag{12}$$

因为前一像素点的密文 $C(i-1)$已知，所以 $C(i)$可以解密。

4 安全性分析和仿真实验

4.1 密钥空间

此算法的密钥由以下部分组成：离散和规范化后 Baker 映射参数 $n_1,n_2,\cdots,n_i$，Hénon 映射的参数 p,q，以及线性反馈移位寄存器级数。

表1给出了密钥空间的估算结果，结果显示总的密钥空间大小为$0.5\cdot10^{17}$，这里只是计算精度为10^{-3}(相当于10比特)，实际上目前的计算机系统其计算精度远大于10^{-3}，并且可以增大两个线性反馈移位器的级数，文[17]相应的密钥空间会变得更大，拥有足够大的密钥空间，这对于抵抗穷举攻击具有重要的意义。

4.2 密文分布分析

表1 多级混沌图像加密算法密钥空间的估算

密钥组成	含义	取值范围	空间大小
$n_1,n_2,\cdots,n_i$	Baker 离散化参数	(0,N)区间	N
p	Hénon 映射	(1.05,1.085)	$0.08*10^3$
q	Hénon 映射	q=0.3	1
$m_0^{(1)}$	$LFSR_1$	11	$2.0*10^3$
$m_0^{(2)}$	$LFSR_2$	12	$4.0*10^3$
总的密钥空间			$8.9*10^{10}$

图9 明文图

维普资讯 http://www.cqvip.com

密文分布是一个密码系统最重要的特性之一，它将直接影响到密码系统的安全。一个分布不均匀密文，往往是密码分析者进行唯密文攻击的首选入口[17]。为更清晰地描述这一特性，我们用图像的直方图来表达。从图中可以看出，本文所提算法所得到的密文在整个密文空间的分布都非常均匀。

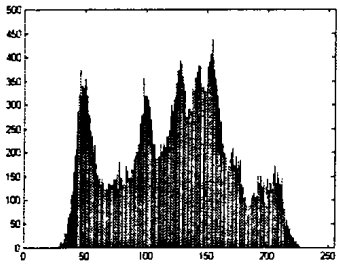

图10 明文直方图

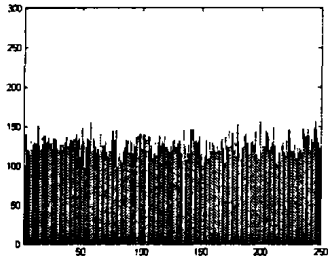

图11 密文直方图

4.3 混乱与扩散性能分析

扩散是将每一位明文的影响尽可能地作用到较多的输出密文位中去，同时还要尽量使得每一位密钥的影响也尽可能迅速地扩展到较多的密文位中去。其目的是有效隐藏明文的统计特性，这也就是混沌系统的初始条件敏感依赖性。混乱，是指密文和明文之间的统计特性的关系尽可能的复杂化，这也就是混沌映射通过迭代，将初始域扩散到整个相空间。通过混乱和扩散，可以有效地抵抗统计和抗差分攻击。为说明本文所提算法的混乱与扩散特性，我们分别进行图9加密前后像素灰度值相关性对比实验，明文的部分位和初始值的微小改变，通过分析改变前后所得密文的差值分布情况来说明算法的扩散与混乱特性。

(1)我们分别分析图像中水平相邻、垂直相邻和对角线相邻的两个像素相关性，因此，我们选择1000对相邻的像素点，然后用(13)，(14)式来计算其相关性：

$$\mathrm{cov}(x,y)=E(x-E(x)(y-E(y)) \tag{13}$$

$$r_{xy}=\mathrm{cov}(x,y)/\sqrt{D(x)D(y)} \tag{14}$$

上两式中，x,y 代表图像中相邻的两个像素点的灰度值。且有，在数字计算中，用到以下离散公式：

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{15}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{16}$$

$$C(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{17}$$

表2为图像9加密前后相邻的像素灰度值的计算结果，从计算结果可知，图像加密后相关性相差很大。

表2 图像加密前后的相邻像素灰度值的相关性比较

	加密前图像灰度值相关性	加密后图像灰度值相关性
水平方向	0.95876	0.00196
垂直方向	0.96415	0.00067
对角线	0.91206	0.01158

(2)明文的微小改变。将图9中坐标(120,1)处的像素值由141改为142，所得密文差值的分布情况见图12。

(3)初始值的微小改变。将混沌系统的初值改变量10^{-4}时，对图像9加密后其密文间差值的分布情况见图13。

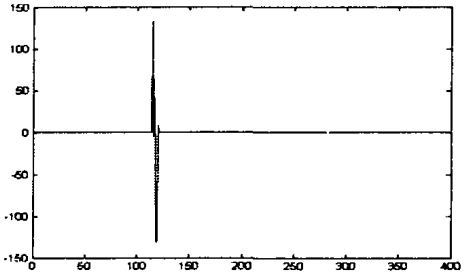

图12 不同明文加密后的密文之间的差值

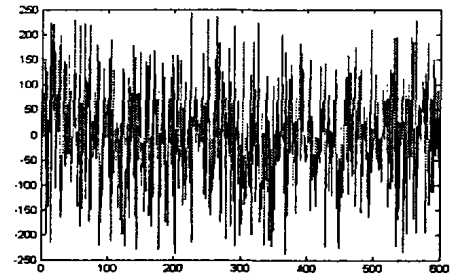

图13 不同初值加密后的密文之间的差值

4.4 加密时间分析

仿真实验表明，图像加密的平均速度达到1.5MB/s，最快速度达到2.5MB/s，实验环境为：PIV 2.4GHZ，内存为256M，硬盘为80G 的个人计算机，表3为图像加密时间结果。实验结果表明，本文提出的混沌多级图像加密算法速度是令人满意。

表3 加密/解密速度测试结果

图像大小(像素)	加密时间(秒)	解密时间(秒)
256×256	<0.3	<0.3
512×512	1	1
1024×1024	2.5	2.5
2048×2048	12	12

结论 图像本身具有数据量大、像素点之间高相关性和高冗余性等特点，本文首先对二维的 Baker 混沌映射进行离散和规范化，然后用它对图像的像素点进行空间置乱，同时结合收缩式密钥发生器，提出了混合混沌序列生成方法，然后用混合混沌序列对图像的像素灰度值进行扩散变换。并从理论上证明了其具有较强的抵抗差分密码分析和线性密码分析的能力和较高的安全性，数字实验的结果也证实了结论的正确性。

参 考 文 献

1 Chang H K C, Liu J L. A linear quadtree compression scheme for image encryption. Signal Process Image Communation, 1997, 10(4):279～290

2 Chang C C, Hwang M S. Chen T S. A new encryption algorithm for image cryptosystems. J Syst Software, 2001, 58:83～91

3 Cheng H, Li X B. Partial encryption of compressed images and videos. IEEE Trans Signal Process, 2000, 48(8):2439～2451

4 Bourbakis N, Alexopoulos C. Picture data encryption using SCAN patterns. Pattern Recognit, 1992, 25(6):567～581

5 Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcat Chaos, 1998, 8(6):1259～1284

6 Scharinger J. Fast encryption of image data using chaotic Kolmogorov flows. J Electron Imaging, 1998, 7(2):318～325

7 Uehara T, Safavi-Naini R, Ogunbona P. Securing wavelet compression with random permutations. IEEE Paci. c Rim Conf. on Multimedia, 2000. 332～335

(下转第244页)

维普资讯 http://www.cqvip.com

虑转换能否提高代码质量，这样将导致程序中一些明显不适合IF转换的分支也进行了转换，严重影响了生成代码的质量。为了更合理地选择待转换分支，我们对GCC中原有的IF转换算法进行了改进。我们增加了一个启发式的函数worth_if_convert( )用来近似地表示分支选择的标准，即如果转换后谓词代码的执行时间比普通代码的执行时间还要长，则认为此IF块不适合转换，函数返回FALSE，否则则认为当前IF块转换后能够提高性能，是值得转换的，并返回TRUE。这个启发式的函数考虑关键路径的长度、资源的使用、误预测率、误预测的代价及指令条数等因素。

worth_if_convert( )的算法描述如下：

```
int worth_if_convert(struct ce_if_block *ce_info)
  {;/*仅考虑资源的使用、关键路径的长度、各分支的执行概率、误
     预测率、误预测的开销计算非谓词代码的执行时间*/
unpredicated_time =compute_unpredicated_time( ) /*具体计算过
    程略*/
  /*计算IF转换后谓词代码的执行时间*/
predicated_time=compute_predicated_time( )/*具体计算过程略
    */;
  /*决定是否值得进行IF转换，即如果谓词代码的执行时间小于非
    谓词代码的执行时间则进行转换，否则不进行转换 */
if(predicated_time<unpredicated_time)
     return TRUE;
  else return FALSE;
}
```

最后我们修改cond_exec_process_if_block( )函数，在该函数中加入判断语句，如下：

```
if(!worth_if_convert(ce_info)
      return FALSE;
   else 继续进行转换
```

实验和结论 实验环境：服务器为HP的Itanium 2，双Itanium 2处理器，1000MHz主频，2G内存，运行的操作系统为Linux version 2.4.18-e.12 SMP。

基于GCC 3.4.0版本，改进了其IF转换算法。为了测试论文提出的改进算法的有效性，我们对两种情况进行了测试：1)GCC 3.4.0的IF转换；2)基于改进算法的IF转换。

可以看出使用GCC3.4.0进行编译时，IF块被转换为谓词指令，这样，不管分支条件怎么改变，都将执行合并后所有的指令，而使用改进的IF转换算法进行编译时，由于分支路径的不平衡和转移概率严重偏向于ELSE块，函数worth_if_invert( )将返回FALSE，不进行IF转换，这样仅执行THEN块中的少数几条指令，从而可以提高程序性能。我们将上述程序段放在一个足够次数的循环中测试其执行时间，实验表明改进后的算法能够显著提高程序的性能，程序的执行时间减少12.4%。在SPEC CPU2000下测试得到的一些结果是：改进的算法和GCC3.4.0相比，总体性能平均提高了1.12%，定点程序性能基本都有所上升，定点程序总体性能提高了1.09%。图2所展示的结果表明，论文提出的改进的IF算法能够提高程序性能，尤其是定点程序性能，适用于IA-64体系结构。

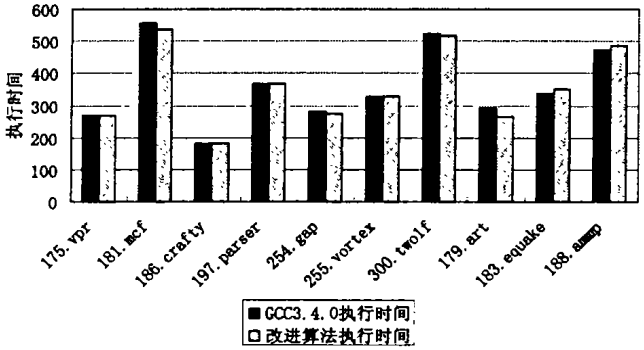

图2 测试数据

参考文献

1 Bringmann R A, et al. Speculative execution exception recovery using write-back suppression. In: Proc. 26th Annu. Int. Symp. On Microarchitecture, Dec. 1993

2 Mahlke S A, Hank R E, Bringmann R A, et al. Characterizing the impact of predicated execution on branch prediction. In: Proc. of the 27th annual international symposium on Microarchitecture, 1994. 217～227

3 Mantripragada S, Nicolau A. Using profiling to reduce branch misprediction costs on a dynamically scheduled processor. In: Proc. of the 2000 intl. conf. on Supercomputing, 2000. 206～214

4 Allen J R, Kennedy K, Portereld C, Warren J. Conversion of control dependence to data dependence. In: Proc. of the 10th ACM Symposium on Principles of Programming Languages, January 1983. 177～189

5 Park J C, Schlansker M S. On predicated execution: [Tech. Rep. HPL-91-58]. Hewlett Packard Laboratories, Palo Alto, CA, May 1991

6 Mahlke S A, Lin D C, Chen W Y, et al. Effective compiler support for predicated execution using the hyperblock. In: 25th Annual Intl. Symposium on Microarchitecture (MICRO-25), 1992. 45～54

7 August D I, Hwu W W, Mahlke S A. A framework for balancing control flow and predication. In: Proc. 30th Annual International Symposium on Microarchitecture, 1997. 92～103

(上接第175页)

8 Matthews R. On the derivation of a chaotic encryption algorithm. Cryptologia, 1989, 13(1): 29～42

9 Yen J C, Guo J I. A new chaotic key-based design for image encryption and decryption. In: Proc. IEEE Int Conf. Circuits and Systems, 2000(4): 49～52

10 Li S J, Zheng X. Cryptanalysis of a chaotic image encryption method. IEEE Int Symposium Circuits and Systems, Scottsdale, AZ, USA, 2002

11 Li S J, Zheng X, Mou X, Cai Y. Chaotic encryption scheme for real-time digital video. In: Proc. SPIE on Electronic Imaging, San Jose, CA, USA, 2002

12 Fridrich J. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. Intl. Journal of Bifurcation and Chaos, 1998(8): 1259～1284

13 Jridrich J. Image Encrytion Based on Chaotic Maps. Systems. Man and Cybernetic, Computational Cybernetics and Simulation, 1997 IEEE Intl. Conf. on (2)

14 Erdmann D, Murphy S. Henon Stream Cipher. Electronics Letters 23rd, April 1992, 28

15 周红. 有限精度混沌系统的m序列扰动实现. 电子学报, 1997, 25(7): 95～97

16 Coppersmith D, Kawczys H, Mansour Y. The Shrinking Generator. Advancesin Cryptology -Crypto'93, Springer-Verlag, 1994. 22～39

17 Schneier B著. 吴世忠, 祝世雄, 张文政, 等译. 应用密码学. 机械工业出版社, 2001