第 38 卷 第 4 期
Vol.38 No.4

计 算 机 工 程
Computer Engineering

2012 年 2 月
February 2012

• 安全技术 •

文章编号：1000—3428(2012)04—0112—04 文献标识码：A 中图分类号：TP309.7

基于离散 Hopfield 网络的混沌图像加密算法

刘祝华，曾高荣，谢芳森

(江西师范大学物理与通信电子学院，南昌 330022)

摘 要：混沌图像加密算法在进行图像像素值置乱时，大多采用像素值整体处理的方式，因此难以抵抗已知明文攻击。针对该情况，提出一种基于离散 Hopfield 网络的高维混沌图像加密算法。使用 Rössler 三维混沌序列中的两维动态调整所有像素每个比特位的置乱权值及阈值，实现图像像素值置乱，剩下的一维用于图像像素位置置乱，由此提高破译难度。实验结果表明，该算法可抵抗差分攻击和统计分析，鲁棒性较强。

关键词：离散 Hopfield 网络；混沌；Rössler 系统；图像加密；置乱

Chaotic Image Encryption Algorithm Based on Discrete Hopfield Network

LIU Zhu-hua, ZENG Gao-rong, XIE Fang-sen

(College of Physics and Communication Electronics, Jiangxi Normal University, Nanchang 330022, China)

【Abstract】For most of chaotic image encryption algorithms, pixel overall treatment method(such as XOR operation) is used in the image pixel value scrambling. It was very weak to resist known cleartext attack. So a high dimension chaotic encryption based on discrete Hopfield network is proposed in this paper. Image pixel value scrambling is realized through dynamic adjustment of each bit's scrambling weight and threshold depending on any two dimensions of Rössler 3D chaotic sequences. Image pixel position scrambling is realized depending on the third dimension of Rössler 3D chaotic sequences. Each pixel value scrambling is a composite treatment, it increases decryption difficulty. Experimental results show that the algorithm has strong ability to resist attacks, and is a security image encryption algorithm.

【Key words】discrete Hopfield network; chaos; Rössler system; image encryption; scrambling

DOI: 10.3969/j.issn.1000-3428.2012.04.037

1 概述

混沌因具有初值敏感性、不可预测性和随机性等特点，可应用于图像加密。目前，混沌图像加密大部分采用图像像素位置置乱和图像像素值置乱 2 种方法[1-6]，其中，有的是针对混沌序列的改进，有的是针对加密过程的改进。但在进行图像像素值置乱时，采用的都是像素值整体处理的方式，且大多采用异或运算。

Hopfield 网络[7]是一种反馈神经网络，有连续型和离散型 2 种。本文提出了一种基于离散 Hopfield 网络的高维混沌图像加密算法。在进行图像像素值置乱时，针对每个像素的每个比特位展开。

2 Rössler 混沌系统

采用低维混沌系统设计加密算法相对容易，但安全性低。高维混沌系统结构复杂，有多个变量和多个系统参数，密钥空间大大高于低维混沌，而且，产生的时间序列更加无规律、不可预测，更适合于加密系统。本文选取 Rössler 三维混沌系统[8]作为加密函数，其方程式如式(1)所示：

$$\begin{cases}\dfrac{\mathrm{d}x}{\mathrm{d}t}=-(y+z)\\ \dfrac{\mathrm{d}y}{\mathrm{d}t}=x+\beta\cdot y\\ \dfrac{\mathrm{d}z}{\mathrm{d}t}=\sigma+z\cdot(x-\rho)\end{cases} \tag{1}$$

其中，β、σ、ρ 为系统参数，当 $\beta=0.2$、$\sigma=0.2$、$\rho=5.7$ 时，系统进入混沌状态，如图 1 所示。

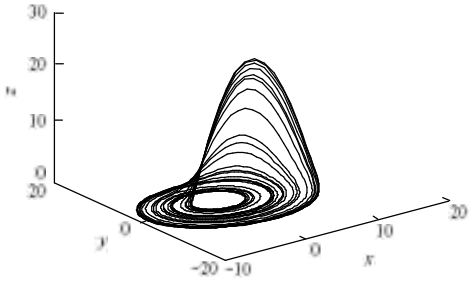


图 1 Rössler 混沌吸引子

3 离散 Hopfield 网络

离散 Hopfield 网络是一种单层的、输入输出为二值的反馈网络，主要用于联想记忆，其结构如图 2 所示。θ_i，$i\in[1,n]$ 为神经元阈值，ω_{ij}，$i\in[1,n]$，$j\in[1,n]$ 表示第 j 个神经元到第 i 个神经元的连接权。可按式(2)计算网络输出，其中，$f(x)$ 为输出二值的阈值函数：

$$x_i(t)=f\left(\sum_{j=1}^{n}\omega_{ij}\cdot x_j(t-1)-\theta_i\right),i\in[1,n] \tag{2}$$

基金项目：江西师范大学青年基金资助项目(2704)；江西师范大学博士基金资助项目(3338)

作者简介：刘祝华(1977－)，男，讲师、硕士研究生，主研方向：混沌保密通信，数字水印，SOPC 嵌入式系统设计；曾高荣，讲师、博士研究生；谢芳森，教授

收稿日期：2011-07-25 **E-mail：**happy_lzh@126.com

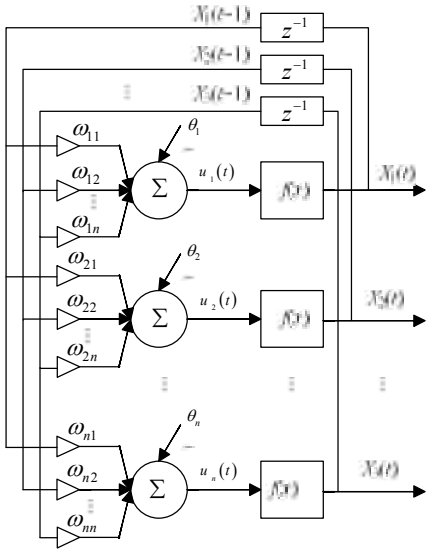


图 2 离散 Hopfield 网络

4 基于离散 Hopfield 网络的混沌图像加密算法

4.1 图像像素值置乱原理

Rössler三维混沌系统按4阶Runge-Kutta法求解，生成三维混沌序列。混沌系统迭代 $Start+M\times N$ 次，舍去前 *Start* 项，生成 X'_k、Y'_k、Z'_k，其中，$k\in[1,M\times N]$，M、N 为待加密图像大小。按式(3)、式(4)选取 X'_k、Y'_k 小数点后第12位、13位、14位对256取余，得到 $x_k\in[0,255]$、$y_k\in[0,255]$：

$$x_k=\mathrm{mod}\left(\mathrm{mod}\left(\left\lfloor abs\left(X'_k\times10^{14}\right)\right\rfloor,1000\right),256\right),\ k\in[1,M\times N] \quad (3)$$

$$y_k=\mathrm{mod}\left(\mathrm{mod}\left(\left\lfloor abs\left(Y'_k\times10^{14}\right)\right\rfloor,1000\right),256\right),\ k\in[1,M\times N] \quad (4)$$

其中，*abs* 为取绝对值运算；$\lfloor\ \rfloor$为向下取整运算；mod 为取余运算。将 x_k、y_k 转换成二进制形式，得到 $w1_{k,i}$、$w2_{k,i}$，转换关系如式(5)、式(6)所示：

$$x_k=\sum_{i=0}^{7}w1_{k,i}\times2^i,\ k\in[1,M\times N],\ i\in[0,7] \quad (5)$$

$$y_k=\sum_{i=0}^{7}w2_{k,i}\times2^i,\ k\in[1,M\times N],\ i\in[0,7] \quad (6)$$

将大小为 $M\times N$ 的 256 级灰度图按列展成向量 $\boldsymbol{I}_k$，$k\in[1,M\times N]$。将 $\boldsymbol{I}_k$ 转换成二进制形式，得到 $p_{k,i}$，它表示第 k 个像素的第 i 个比特位，$\boldsymbol{I}_k$ 的关系如式(7)所示：

$$\boldsymbol{I}_k=\sum_{i=0}^{7}p_{k,i}\times2^i,\ k\in[1,M\times N],\ i\in[0,7] \quad (7)$$

将离散 Hopfield 网络应用于图像像素值置乱。为简化算法，令图 2 中 $\omega_{ij}=0\ (i\neq j)$，像素值置乱算法流程见图 3。

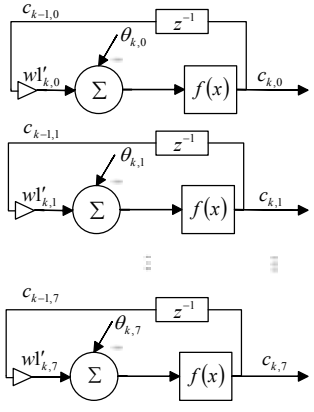


图 3 图像像素值置乱算法流程

在图 3 中，$c_{k,i}$ 和 $c_{k-1,i}$，$k\in[1,M\times N]$ 代表像素位置，$i\in[0,7]$ 代表像素中比特位置)分别为当前像素值和上一像素值(即反馈)的置乱密文，$w1'_{k,i}$ 和 $\theta_{k,i}$ ($k\in[1,M\times N]$, $i\in[0,7]$)为每个像素的每个比特位的置乱权值和阈值。$f(x)$ 为阈值函数，选取 $f(x)=\mathrm{mod}\left(abs(x),2\right)$。

根据 $w1_{k,i}$、$w2_{k,i}$ 及 $p_{k,i}$ 进行非线性变换可以得到置乱权值 $w1'_{k,i}$ 及阈值 $\theta_{k,i}$。变换关系如下：

$$w1'_{k,i}=\begin{cases}1 & \text{if } w1_{k,i}=1\\ -1 & \text{if } w1_{k,i}=0\end{cases} \quad (8)$$

$$w2'_{k,i}=\begin{cases}1 & \text{if } w2_{k,i}=1\\ -1 & \text{if } w2_{k,i}=0\end{cases} \quad (9)$$

$$\theta_{k,i}=w1_{k,i}\oplus w2_{k,i}-p_{k,i}\cdot w2'_{k,i} \quad (10)$$

图像像素值置乱密文输出按下式得到：

$$c_{k,i}=\mathrm{mod}\left(abs\left(w1'_{k,i}\cdot c_{k-1,i}-\theta_{k,i}\right),2\right) \quad (11)$$

在计算 $c_{1,i}$ 时，反馈密文 $c_{0,i}$ 可由图像最后一个像素值的二进制结果 $p_{M\times N,i}$ 代入。k 从 1 至 $M\times N$ 历经一遍，得到像素值置乱图像的二进制表示，将其转换成十进制，并按列方向转成 $M\times N$ 的矩阵，即可得到像素值置乱图像。

4.2 图像像素位置置乱原理

从 Z'_k 中选取 Z'_1 到 Z'_M 共 M 项构成 $z1_m$，$m\in[1,M]$，选取 Z'_{M+1} 到 Z'_{M+N} 共 N 项构成 $z2_n$，$n\in[1,N]$。按式(12)、式(13)得到像素位置置乱序列 $h_m\in[0,N-1]$ 和 $v_n\in[0,M-1]$：

$$h_m=\mathrm{mod}\left(\left\lfloor abs\left(z1_m\times10^{14}\right)\right\rfloor,N\right),\ m\in[1,M] \quad (12)$$

$$v_n=\mathrm{mod}\left(\left\lfloor abs\left(z2_n\times10^{14}\right)\right\rfloor,M\right),\ n\in[1,N] \quad (13)$$

大小为 $M\times N$ 的图像，从第1行扫描到第 M 行，每一行按照序列 h_m 对应值进行循环右移。然后进行转置，变成大小为 $N\times M$ 的图像，从第1行扫描到第 N 行，每行按序列 v_n 对应值循环右移。再经一次转置即可得到像素位置置乱图像。

4.3 图像加解密步骤

图像加密步骤如下：

步骤 1 输入待加密图像，设置加密密钥，包括：Rössler 混沌系统参数 β、σ、ρ，初始值 X_0、Y_0、Z_0，迭代舍弃数 *Start* 及加密次数 L。混沌系统迭代 $Start+M\times N\times L$ 次，舍去前 *Start* 项，生成混沌序列 X_j, Y_j, Z_j，$j\in[1,M\times N\times L]$，其中，$M\times N$ 为待加密图像大小。

步骤2 选取 Z_j 的 $Z_{(\ell-1)\times M\times N+1}$ 到 $Z_{\ell\times M\times N}$ 共 $M\times N$ 项构成 Z'_k，$k\in[1,M\times N]$，其中，$\ell\in[1,L]$ 为当前加密轮次。按4.2节内容对图像进行像素位置置乱。

步骤3 选取 X_j 的 $X_{(\ell-1)\times M\times N+1}$ 到 $X_{\ell\times M\times N}$ 共 $M\times N$ 项构成 X'_k，$k\in[1,M\times N]$，选取 Y_j 的 $Y_{(\ell-1)\times M\times N+1}$ 到 $Y_{\ell\times M\times N}$ 共 $M\times N$ 项构成 Y'_k，$k\in[1,M\times N]$，其中，$\ell\in[1,L]$ 为当前加密轮次。按4.1节原理对图像进行像素值置乱。

步骤 4 重复步骤 2、步骤 3 直到完成 L 轮加密。

步骤 5 输出加密后图像。

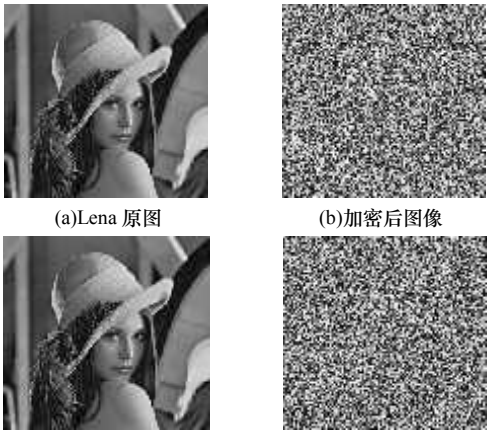
图像解密是加密过程的逆过程。其中，在恢复图像像素值 $p_{k,i}$ 时，按下式进行：

$$p_{k,i}=\mathrm{mod}\left(abs\left(\left(c_{k,i}+w1_{k,i}\oplus w2_{k,i}-w1'_{k,i}\cdot c_{k-1,i}\right)/w2'_{k,i}\right),2\right) \quad (14)$$

解密时，k 从 $M\times N$ 至 1 反向历经一遍。在恢复 $p_{1,i}$ 时，$c_{0,i}$ 由已恢复的 $p_{M\times N,i}$ 代入。

5 仿真实验与安全性分析

在 Matlab 环境下进行图像加密仿真实验。选取标准的 256×256 像素的 256 级 Lena 灰度图作为待加密图像。设置加密密钥，Rössler 混沌系统参数 $\beta=0.2$、$\sigma=0.2$、$\rho=5.7$，初始值 $X_0=-1$、$Y_0=0$、$Z_0=1$，迭代舍弃数 $Start=50\,000$，加密次数 $L=2$。图 4(a)为 Lena 原图，图 4(b)为加密后图像，图 4(c)为输入正确密钥后的解密图像。



(a)Lena 原图 (b)加密后图像

(c)正确解密图像 (d)错误解密图像

图 4 Lena 图加解密实验效果

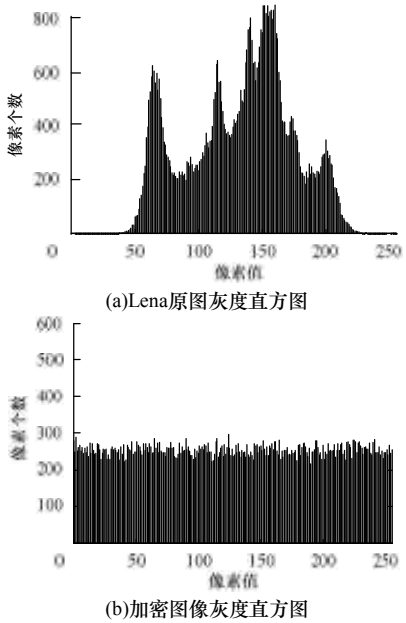
5.1 密钥分析

密钥空间分析包括 2 个步骤：(1)密钥空间分析。Rössler 混沌系统的 3 个参数、3 个初始值、迭代舍弃数及加密次数都可以作为密钥使用，可见，本文算法具有很大的密钥空间。(2)密钥敏感性测试。在其他系统参数不变的情况下，初始值 $X_0=-1.000\,000\,000\,1$，X_0 的微小变化(10^{-10})，得到错误的解密图像见图 4(d)，无法从解密结果中得到原图像信息。其他参数的改变，也可以得到类似的结果。可见，本文算法的密钥敏感性很强。

5.2 统计分析

统计分析包括 3 个步骤：

(1)直方图分析。图 5 为图像加密前后的直方图。对比可见，加密图像的直方图分布非常均匀，完全掩盖了加密前图像灰度分布规律，有效地提高了算法破译难度。



(a)Lena原图灰度直方图

(b)加密图像灰度直方图

图 5 Lena 图像加密前后灰度直方图

(2)相邻像素的相关性。在原始图像和加密图像中各随机选取 1 000 对相邻像素，测试其相关性(包括垂直、水平和对角方向)，并计算相关系数。相关系数可按式(15)~式(18)计算。其中，x、y 表示相邻 2 个像素的像素值。

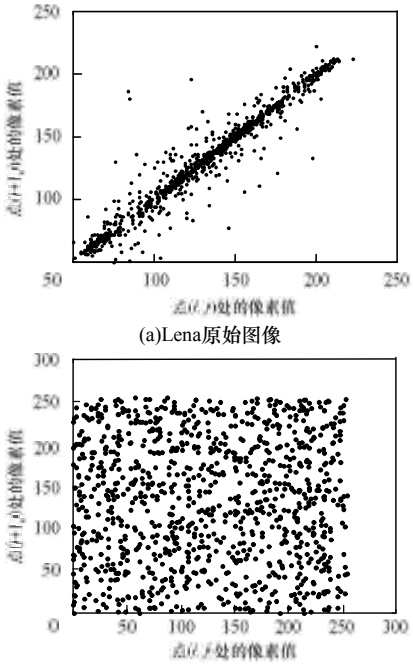
$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{15}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)^2 \tag{16}$$

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

$$r_{xy}=\frac{Cov(x,y)}{\sqrt{D(x)}\cdot\sqrt{D(y)}} \tag{18}$$

图 6 给出了图像加密前后相邻像素水平方向相关性。表 1 给出了加密前后的相关系数。由图 6 和表 1 可见，加密后图像相邻像素的相关性远小于原始图，表明本文算法有很强的抗统计分析能力。



(a)Lena原始图像

(b)加密后Lena图像

图 6 图像加密前后相邻像素水平方向相关性

表 1 图像加密前后相邻像素的相关系数

像素方向	原始图像	加密图像
水平方向	0.939 3	−0.006 4
垂直方向	0.962 3	−0.000 6
对角方向	0.911 7	−0.004 9

(3)差分攻击。攻击者可以通过原图像很小的改动(如一个像素值的变化)来观察加密后图像变化的情况，从而破译加密图像。为了有效抵抗差分攻击，原图像微小改动所导致加密图像的变化越大越好。可用图像像素变化率 NPCR 和像素平均强度变化率 UACI[9]来定量描述，其定义见式(19)、式(20)：

$$N_{\mathrm{NPCR}}=\frac{\sum_{i,j}D(i,j)}{W\times H}\times 100\% \tag{19}$$

$$U_{\mathrm{UACI}}=\frac{1}{W\times H}\left[\sum_{i,j}\frac{\left|C_1(i,j)-C_2(i,j)\right|}{255}\right]\times 100\% \tag{20}$$

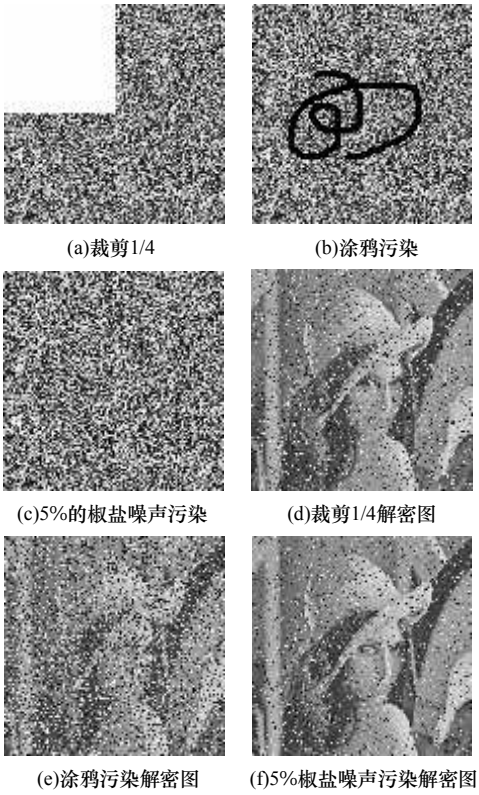
其中，C_1 和 C_2 是只有一个像素不同的 2 幅原始图像的加密图；$D(i,j)$ 定义为：若 $C_1(i,j)\neq C_2(i,j)$，则 $D(i,j)=1$，否则，$D(i,j)=0$；W、H 为 C_1、C_2 的大小。

将 Lena 原图中(8,11)处像素值减 1，计算得 N_{NPCR}=

99.26%，*UUACI*=33.40%。由此可见，本文算法对图像的微小变化非常敏感，能有效抵抗差分攻击。

5.3　鲁棒性分析

为验证本文算法的鲁棒性，对加密后的图像进行裁剪、涂鸦污染和加噪等攻击，实验效果如图 7 所示，结果证明本文算法有较好的鲁棒性。



(a)裁剪1/4　(b)涂鸦污染　(c)5%的椒盐噪声污染　(d)裁剪1/4解密图　(e)涂鸦污染解密图　(f)5%椒盐噪声污染解密图

图 7　裁剪、涂鸦污染、加噪攻击及其解密效果

6　结束语

本文算法将离散 Hopfield 网络应用于图像像素值置乱，使得每个像素的每个比特位的置乱权值和阈值都随混沌序列的变化而变化，且将密文作为反馈，有效地提高了像素值置乱效果，实验结果也验证了算法的有效性。算法在选择离散 Hopfield 的连接权时令 $\omega_{ij}=0\ (i\neq j)$，相对简单。有关连接权的选择方法是下一步研究工作的重点。

参考文献

[1] Singh N, Sinha A. Optical Image Encryption Using Hartley Transform and Logistic Map[J]. Optics Communications, 2009, 282(6): 1104-1109.

[2] Patidar V, Pareek N K, Sud K K. A New Substitution-diffusion Based Image Cipher Using Chaotic Standard and Logistic Maps[J]. Communications in Nonlinear Science and Numerical Simulation, 2009, 14(7): 3056-3075.

[3] 陈艳峰, 李义方. 交替分段相互置乱的双混沌序列图像加密算法[J]. 华南理工大学学报: 自然科学版, 2010, 38(5): 27-33.

[4] 张庆华, 张　瀚. 基于保守混沌系统的图像加密算法[J]. 计算机工程与设计, 2009, 30(10): 2387-2389.

[5] 程　甲, 赵怀勋, 朱建杨. 基于复合离散混沌系统的图像加密算法[J]. 计算机工程, 2009, 35(6): 162-163.

[6] 李永华, 王　冰. 基于混沌序列的图像加密算法[J]. 计算机应用, 2009, 29(6): 100-105.

[7] Hagan M T. 神经网络设计[M]. 戴　葵, 译. 北京: 机械工业出版社, 2002.

[8] 陈士华, 谢　进, 陆君安, 等. Rössler 混沌系统的追踪控制与同步[J]. 物理学报, 2002, 51(4): 749-752.

[9] Chen Guanrong, Mao Yaobin, Chui C K. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps[J]. Chaos Solitons and Fractals, 2004, 21(3): 749-761.

编辑　张正兴

(上接第 109 页)

表 4　1 h 后有条件的随机网络下的实验结果

总节点数	接收节点	极小最大流	极大最大流	多播构造	近似构造	总最大流	增益比/(%)
100	5	17	49	85	146	184	33.20
100	15	16	48	240	283	429	10.00
500	10	69	241	690	952	1 583	16.60
500	50	77	255	3 850	4 354	8 141	6.19
1 000	10	171	512	1 710	2 339	3 815	16.50
1 000	50	175	537	8 750	9 366	14 576	4.23

在 *t* 改变的情况下，表 3 与表 4 的实验结果同样表明，相较于线性多播，利用静态最大可解线性网络编码可以获得更高的网络传输速率；并且在接收节点的最大流之间差异比较大时，增益比更高。

实验结果表明，静态网络编码对于最大流差异比较大的网络，即使是在不同的格局下，也能得到较高的增益比。

5　结束语

本文在构造最大可解网络编码的基础上，考虑边失效的情况，提出了静态最大可解网络编码的构造方法，使得每个节点能够解码出等于自己最大流的数据包。下一步是把本文的研究成果推广到多源问题上，以解决更实际的问题。

参考文献

[1] Ahlswede R, Cai Ning, Li Shuo-Yent, et al. Network Information Flow[J]. IEEE Trans. on Information Theory, 2000, 46(4): 1204-1216.

[2] Li Shuo-Yen, Raymond W Y, Cai Ning. Linear Network Coding[J]. IEEE Trans. on Information Theory, 2003, 49(2): 371-381.

[3] 刘冠群. 单源最大可解线性网络编码的近似构造[J]. 计算机工程, 2010, 36(9): 94-96.

[4] Raymond W Y. Information Theory and Network Coding[M]. Berlin, Germany: Springer, 2008.

[5] Lehman A R, Lehman E. Complexity Classification of Network Information Flow Problems[C]//Proc. of the 41st Annual Conf. on Communication Control and Computing. Monticello, USA: [s. n.], 2003.

[6] Kan Haibin, Li Xuefei, Shen Hong. The Characteristic Generators for a Group Code[J]. IEICE Trans. on Fundamentals, 2006, E89-A(5): 1513-1517.

[7] Koetter R, Médard M. An Algebraic Approach to Network Coding[J]. IEEE/ACM Trans. on Networking, 2003, 11(5): 782-795.

[8] Cai Kai, Fan Pingyi. An Algebraic Approach to Link Failures Based on Network Coding[J]. IEEE Trans. on Information Theory, 2007, 53(2): 775-779.

编辑　张　帆