基于离散广义同步定理的复合混沌音频加密方案

尹 萍[1] 闵乐泉[1,2]

(北京科技大学信息工程学院 北京 100083)[1] (北京科技大学应用学院 北京 100083)[2]

摘 要 利用离散广义混沌同步定理,基于3D-Lorenz系统构造了一个新的离散混沌系统,并结合Arnold猫映射设计了一种音频复合加密方案。该方案首先用复合系统产生的混沌码对明文进行加密,然后将密文隐藏到wav语音信号中,解密过程能够实现无失真解密。数值模拟表明,新的离散混沌系统产生的混沌流具有良好的伪随机性,并且音频隐藏方案对混沌系统的参数及初始条件极为敏感,具有较高的安全性,能够有效地应用于网络通讯。

关键词 广义同步定理,加密隐藏方案,混沌码伪随机性

中图法分类号 O191 **文献标识码** A

Encryption Scheme of Data Hiding in Digital Audio Based on Generalized Synchronization Theorem for Discrete Chaos

YIN Ping[1] MIN Le-quan[1,2]

(School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China)[1]

(School of Applied Science, University of Science and Technology Beijing, Beijing 100083, China)[2]

Abstract A new chaos system was established based on the theorem of generalized synchronization and 3D-Lorenz system. The chaos sequences generated via this system and Arnold's cat map have better pseudo-random properties. A message encryption and hiding scheme was also established on the system and Arnold's cat map. The scheme is successful to encrypt and decrypt message. Ciphertexts are sensitive to the parameters and initial conditions of the chaos system. Numerical simulations show that our scheme is effective to be used in network communication. It shows that this scheme has good security.

Keywords Generalized synchronization theorem, Encryption and hiding scheme, Pseudo-random properties of chaos sequence

1 引言

混沌信号具有遍历性、非周期性、连续宽带频谱、似噪声等特性。近年来利用混沌动力系统构造安全通讯系统的研究十分活跃[1-9]。随着计算机和网络技术的发展,信息安全问题越来越受到重视,传统的密码技术并不能完全解决信息保护问题,于是信息隐藏技术应运而生,并且有了较大的发展[2,4,5]。目前,利用混沌技术的加密方案多以直接利用混沌系统产生的伪随机序列为手段进行秘密通信。密码学中密钥长度可体现其算法安全度,并希望每个密钥都具有良好的抗攻击能力,混沌加密算法中混沌系统的参数相当于算法的密钥。尽管混沌系统的特性使其成为伪随机序列发生器的极佳候选者,但是Parlitz和Short等人近年对混沌同步通信系统破译的研究已获得成功[6,7]。Short指出时间序列单步预测法有时能够揭示隐藏信息的存在以及隐藏信息的内容。即使采用高维超混沌也不能显著地提高这类系统的安全性。国内外学者提出了各种新的混沌同步通信系统,以期提高系统的保密性能。

针对上述问题,本文基于文献[9-13]中的离散系统广义混沌同步理论(Generalized Chaos Synchronization, GSC),建立了一个与3D-Lorenz系统广义同步的新离散混沌系统并结合Arnold猫映射设计了一种复合伪随机序列。由于该方案中设计的同胚函数可以是不计其数的,使得密钥空间扩大,足以满足安全通讯的各种要求,为设计更加安全的通信系统提供了新的思路,使其对入侵者的强力攻击手段有很强的抵抗能力。具体算法:利用新离散广义同步混沌系统及Arnold猫映射产生的随机信号对文本信号加密,以实现不同混沌信号之间的切换加密,切换规则中所涉及到的开关矩阵,也是由混沌序列产生,具有混沌特性,增强了加密序列的复杂性和随机性。而后,将加密后的密文隐藏于wav音频信号中进行传输。最后,通过实验仿真结果表明,此系统与Arnold离散猫映射组合产生的伪随机序列,具有良好的随机性,并且其安全性分析结果显示该方案可以准确加解密信息,对密钥较为敏感,具有较高的安全性。

到稿日期:2010-05-21 返修日期:2010-09-06 本文受国家自然科学基金(70271068,60674095),北京电子科技学院信息安全与保密重点实验室开放基金(KYKF200605)资助。

尹 萍(1983—),女,博士生,主要研究方向为混沌通讯加密,E-mail:Sivy@163.com;闵乐泉(1951—),男,教授,博士生导师,主要研究方向为非线性理论等。

2 离散广义混沌同步系统

2.1 离散广义混沌同步理论

对两个离散混沌系统，有如下定义：

定义 1[12] 考虑两个混沌系统：

$$X(k+1)=F(X(k)) \tag{1}$$

$$Y(k+1)=G(Y(k),X_m(k)) \tag{2}$$

其中，

$$X(k)=(x_1(k),x_2(k),\cdots,x_n(k))^T\in R^n$$
$$Y(k)\in R^m \tag{3}$$

$$X_m(k)=(x_1(k),x_2(k),\cdots,x_m(k))^T,m\leqslant n \tag{4}$$

$$F_m(X(k))=(f_1(X(k)),f_2(X(k)),\cdots,f_m(X(k)))^T \tag{5}$$

$$G(Y(k),X_m(k),k)=(g_1(Y(k),X_m(k),k),g_2(Y(k),X_m(k),k),\cdots,g_n(Y(k),X_m(k),k))^T \tag{6}$$

系统(1)称为驱动系统，系统(2)称为响应系统。若存在一个映射 $H:R^m\to R^m$ 和开集 $B=B_x\times B_y\subset R^n\times R^m$，使得当初始条件 $(X(0),Y(0))\in B$ 时，系统(1)和(2)的解 $(X(k),Y(k))$ 满足：

$$\lim_{k\to+\infty}\| X_m(k)-H^{-1}(Y(k))\|=0 \tag{7}$$

则称响应系统(2)与驱动系统(1)关于 H 在 B 上离散广义混沌同步。若 $\forall(X(0),Y(0))\in R^n\times R^n$，式(7)均成立，则称系统(1)与(2)关于 H 大范围离散广义混沌同步。

定理 1[13] 设 $X,X_m,Y,F(X)$ 及 $G(Y,X)$ 由式(1)－式(6)定义，$H:R^m\to R^m$ 是可逆变换，且 $X_m=V(Y)=H^{-1}(Y)$，假如式(1)与式(2)关于变换 H 是广义混沌同步，那么式(2)中的 $G(Y,X)$ 可写成以下形式：

$$G(Y,X)=H[F_m(X(k))-q(X_m(k),Y(k))]$$

其中，

$$F_m(X(k))=(f_1(X(k)),f_2(X(k)),\cdots,f_m(X(k)))^T$$

且函数

$$q(X_m(k),Y(k))=(q_1(X_m(k),Y(k)),q_2(X_m(k),Y(k)),\cdots,q_m(X_m(k),Y(k)))^T$$

使得误差方程

$$e(k+1)=X_m(k+1)-V(Y(k+1))=X_m(k+1)-H^{-1}(Y(k+1))=q(X_m(k),Y(k)) \tag{8}$$

零解渐近稳定。

2.2 离散广义混沌同步系统

复合加密方案首先需要构造一个新的离散广义混沌同步系统。基于 3D-Lorenz 方程并且形如式(2)的 GCS 系统具体描述如下：

设驱动系统 $X(k+1)=F(X(k))$ 为 3D-Lorenz 方程：

$$\begin{cases}x_1(k+1)=x_1(k)x_2(k)-x_3(k)\\ x_2(k+1)=x_1(k)\\ x_3(k+1)=x_2(k)\end{cases} \tag{9}$$

当 $x_1(1)=0.5,x_2(1)=0.5,x_3(1)=-1$ 时，系统(9)能够产生混沌轨道。令 $H:R^3\to R^3$，构造一个可逆变换，形式如下：

$$H(X(k))=Y(k)=BX(k) \tag{10}$$

式中，$B=\begin{bmatrix}b_{11},b_{12},b_{13}\\ b_{21},b_{22},b_{23}\\ b_{31},b_{32},b_{33}\end{bmatrix}$ 是一个 3×3 可逆矩阵，

$$X(k)=(x_1(k),x_2(k),x_3(k))$$

$$Y(k)=(y_1(k),y_2(k),y_3(k))$$

再令 $m=3$，

$$q(X_m(k),Y(k))=\frac{1}{8}e(k)=\frac{1}{8}(X(k)-V(Y(k)))=\frac{1}{8}(X(k)-B^{-1}(Y(k)))$$

则 $e(k+1)=q(X(k),Y(k))=(\frac{1}{8})^{k+1}e(0)$

使其零解渐近稳定，且 $q(Y,X_m)$ 有形式：

$$q(X_m(k),Y(k))=B(F(X(k))-q(X(k),Y(k)))$$
$$=B(F(X(k))-\frac{1}{8}X(k)-B^{-1}Y(k))$$
$$=B(F(X(k))-\frac{1}{8}X(k))-Y(k)$$

$$G(Y,X)=[\dot{V}(Y)]^{-1}[F(X)-q(X,Y)] \tag{11}$$

由定理 1 得到响应系统方程：

$$Y(k+1)=G(Y(k),X_m(k))=H(F_m(X(k))-q(X_m(k),Y(k))) \tag{12}$$

令

$$\begin{cases}b_{11}=-4.728,b_{12}=0.176,b_{13}=0.103\\ b_{21}=0.380,b_{22}=-3.998,b_{23}=0.157\\ b_{31}=0.442,b_{32}=0.790,b_{33}=-3.592\end{cases}$$

$$X(0)=(x_1(0),x_2(0),x_3(0))=(0.5,0.5,-1)$$

$$Y(0)=(y_1(0),y_2(0),y_3(0))=(-2.797,5.171,0.332)$$

则系统(9)和系统(12)产生的混沌轨道如图 1 所示。从图 1 中可以看出，驱动系统和响应系统为两个混沌吸引子和关于传递函数离散广义混沌同步。

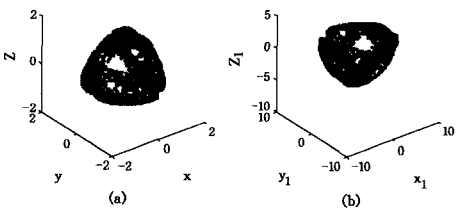


图 1 (a)3D-Lorenz 系统动力学轨道；(b)离散 GCS 系统动力学轨道

3 基于离散广义同步的复合混沌音频加密方案

3.1 Arnold 离散猫映射

标准的 Arnold 离散猫映射属于二维混沌系统。Arnold 离散猫映射的表达式如下：

$$\begin{cases}x_1(n+1)=\mathrm{mod}((x_1(n)+x_2(n)),1)\\ x_2(n+1)=\mathrm{mod}((x_1(n)+kx_2(n)),1)\end{cases} \tag{13}$$

式中，$k=2$。

当选择初始条件为 $X(0)=(0,1/\sqrt{2})^T$ 时，系统出现混沌现象。图 2 所示为 Arnold 离散猫映射取上述初始条件时前 4000 次迭代产生的运动轨迹。从图 2 中可以看出，Arnold 离散猫映射的迭代点分布非常均匀。

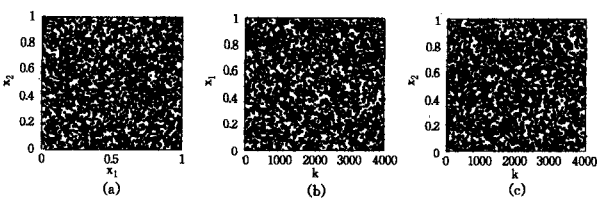


图 2 Arnold 猫映射

3.2 复合音频隐藏算法

本文基于离散广义混沌同步的 3D-Lorenz 系统(12)和 Arnold 猫映射提出了一种复合音频加密算法。

假设发送方 A 需要通过传输网络向接收方 B 秘密发送一段 txt 文本信息 m,其隐藏流程图如图 3 所示,具体实现步骤如下。

(1)加密过程:发送方 A 随机选取初始条件 $(X(0),Y(0))\in B_x\times B_y$,用其驱动混沌系统(1)产生 3D-Lorenz 混沌序列码 $Chaos_1$,而后随机选取初始条件 $X'(0)\in B_{x'}$ 驱动混沌系统(2)产生 Arnold 混沌序列码 $Chaos_2$。用变换规则 T_M 从 $Chaos_1$ 和 $Chaos_2$ 中提取出一组复合混沌源码 $M=T_M(Chaos_1,Chaos_2)$得到 X_i。取出 N 位有效数字组成整数并对其进行 256 取余,把文本信息 m 变换成 $T_e(m)$。用公式 $C=E(M,T_e(m))$加密明文 P 产生密文 C,用 $Z=f((X(0),Y(0)),X'(0))$加密初始条件$(X(0),Y(0))$和 $X'(0)$,其中 E 为加密函数。发送方 A 把密文 C、初始条件 Z 分别隐藏到双声道语音信号的左声道和右声道的第 7,8 位上。最后 A 把隐藏密文和初始条件后的语音信号传给接收方 B。

(2)解密过程:接收方 B 把密文 C、初始条件 Z 分别隐藏到双声道语音信号的两个声道的第 7,8 位上分离出来。用初始条件$(X(0),Y(0))$、$X'(0)$分别驱动混沌系统(9),(12)得到 $Chaos_1$,$Chaos_2$,并利用(1)中通信双方在通信前约定的混沌序列的复合变换规则 T_M 得到 M。最终 B 用 $P=D(M,C)$解出明文 P 和密文 C,其中 D 为解密函数。

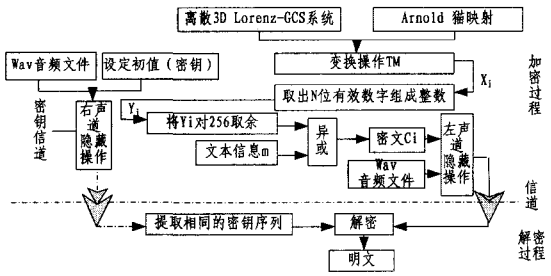


图 3 音频信息隐藏方案加解密流程

4 仿真实验

本方案采用 matlab7.5 仿真实现,伪装的语音信号为某流行歌曲的片段,分别对左声道进行密文信息隐藏,对右声道进行密钥隐藏。载体信号为双声道高保真音乐,采样频率为 44.10kHz,量化精度 16 比特,位速 1411kbps。需要加密传递的文本文件为 txt 文件,如图 4(a)所示。

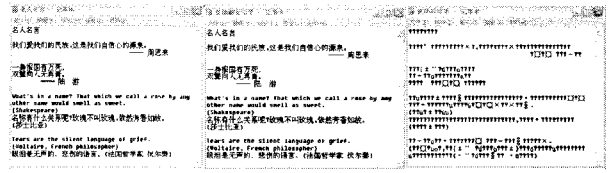
密钥集 keys 中取值分别为:

$$X(0)=(x_1(0),x_2(0),x_3(0))=(0.5,0.5,-1)$$

$$\begin{cases}b_{11}=-4.728,b_{12}=0.176,b_{13}=0.103\\b_{21}=0.380,b_{22}=-3.998,b_{23}=0.157\\b_{31}=0.442,b_{32}=0.790,b_{33}=-3.592\end{cases}$$

$$X'(0)=(0,1/\sqrt{2})^T,k=2$$

隐藏前后的语音信号波形如图 5 所示。由图可以看出,左右信号的相关性标准偏差没有任何变化,平均值仅有微小变化。待隐藏的被正确解密的文本为图 4(b)。被隐藏的文本信息通过密钥组无损精确地恢复。若初值有微小扰动,混沌码就会有明显变化,对方将无法正确提取明文。如对密钥进行 $b_{11}=b_{11}+10^{-15}$扰动,则得到的解密结果如图 4(c)所示,此时所解密的文本信息呈现乱码状态。



(a)待加密明文 (b)正确密钥解密结果 (c)扰动密钥解密结果

图 4

5 安全性分析

5.1 密文熵分析

香农提出了信息熵的概念,用以表征信源的不定度。对概率分布为$(P_1,P_2,\cdots,P_n)$的离散集,其信息熵定义为:$-\sum_{i=1}^{n}p_i\log_2 p_i$。当信源概率分布为等概率分布时,信息熵能取到最大值 $\log_2(n)$bit,这就是最大熵原理。我们将利用变换将混沌流变为[0,255]之间的整数值,形成密钥流。我们可以用密钥流的信息熵来度量密钥流的不确定性的程度。当密钥流的概率分布为等概率分布时,即取[0,255]之间每一个值的概率均为 1/256 时,具有最大熵为 $\log_2 256=8$bit,也就是说信息熵越接近 8,说明混沌码的随机性越好。

3D-Lorenz 系统的混沌码的熵 $H_1=7.9516$

Arnold 猫映射的熵 $H_2=7.9561$

同步系统的混沌码的熵 $H_3=7.9550$

两个系统复合变换后混沌码的熵 $H=7.9571$

从测试数据可以看到,GCS 与 Arnold 猫映射两个系统经过变换后的复合系统,其混沌码的信息熵比任何单个系统的信息熵都更接近于 8,说明复合系统所设计的混沌序列在随机性上比单个系统更有优越性。

5.2 相关性分析

本文实验测试中,对某一流行歌曲的片段进行实验,此处只对左声道进行信息隐藏,右声道无变化。载体信号为双声道高保真音乐,采样频率为 44.10kHz,量化精度 16 比特,位速 1411kbps。图 5(a)和(b)分别为原信号左右声道波形,(c)和(d)分别为隐藏信息的信号波形。由于本实验只对左声道进行信息隐藏,因此右声道波形无变化。下面分别对隐藏前后左声道、隐藏前左右声道和隐藏后左右声道的相关性进行计算。

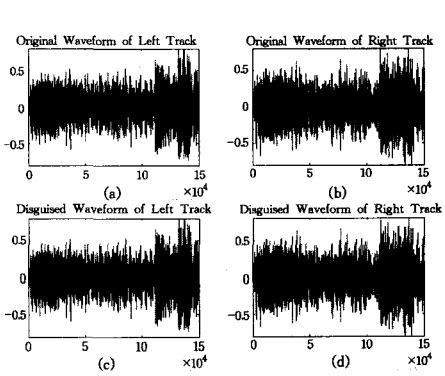


图 5 (a)加密前左声道的波形图;(b)加密前右声道的波形图
(c)隐藏后左声道的波形图;(d)隐藏后右声道的波形图

隐藏前后左声道的相关性为:

C1 =9.999999999998264e-001

隐藏前左右声道的相关性为:

(下转第 144 页)

全性和认证效率都得到了提高。改进的方案中仍然采用零知识证明的思路。如何有效避免零知识证明的复杂度，进一步提高方案的执行效率，是今后研究的一个方向。

参 考 文 献

[1] Trusted Computing Group. Trusted Computing Group TPM Specification Version1. 2[S]. www. trusted computing group. org. 2003

[2] Brickell E, Camenisch J, Chen L. Direct Anonymous Attestation [C]// The Proceedings of the 11th ACM Conference on Computer and Communications Security. ACM Press, 2004: 132-145

[3] 刘吉强，赵佳，赵勇. 可信计算中远程自动匿名证明的研究[J]. 计算机学报，2009，32(7)：1304-1310

[4] Zhang Fangguo, Chen Xiaofeng, Mu Yi, et al. A New and Efficient Signature on Commitment Values[J]. International Journal of Network Security, 2008, 7(1): 101-106

[5] Chen Xiaofeng, Feng Dengguo. A New Direct Anonymous Attestation Scheme from Bilinear Maps[C]// The Proceedings of 9th International Conference for Young Computer Scientists. 2008: 2308-2313

[6] Brickell E, Chen Liqun, Li Jiangtao. Simplified Security Notions of Direct Anonymous Attestation and a Concrete Scheme from Pairings [J]. International Journal of Information Security, 2009, 8(5): 315-330

[7] Yu Rongwei, Wang Lina, Zhou Yanzhou, et al. An Optimized Anonymous Attestation Protocol from Bilinear Pairing[C]// The Proceedings of 2009 International Conference on Computational Science and Engineering. 2009: 721-726

[8] Lenstra A K, Verheul E R. The XTR public key system[C]// The Proceeding of Crypto2000. LNCS 1880. Spring-Verlag, 2000: 1-19

(上接第 106 页)

C2 =4. 106738302228002e-001

隐藏后左右声道的相关性为：

C3 =4. 106738300576803e-001

从 C1 可以看出隐藏前后左声道的相关性接近 1，说明隐藏信号前后左声道信息几乎无变化。从 C2 和 C3 可以看出，隐藏前后左右声道的相关性大小关系几乎维持不变。

5.3 密钥敏感性测试

本方案对密钥进行了敏感性测试。按以下步骤对 3D-Lorenz 系统初值 $X(0)$ 及可逆矩阵 B 所构成的密钥组中的密钥进行微扰测试。

令舍弃初始迭代次数 $N=5000$。将初始条件 $X(0)$ 及参数 B 进行微扰，产生一维密钥流 $\tilde{c}$，与未扰动时产生的一维密钥流 c 进行比较。取密钥流的长度为 1250010(ASCII 码)。密钥流 $\tilde{c}$ 与 c 对应位的变化个数的百分比如表 1 所列。由表 1 得到 $\tilde{c}$ 与 c 位变化个数的平均值为 99. 600%，非常接近于理想值的 99. 609%(255/256)。由此得出本文的密钥流生成器具有优质的伪随机性功能。

表 1 密钥流 $\tilde{c}$ 与 c 对应的变化个数百分比

密钥扰动	x_1	x_2	x_3	b_{11}	b_{13}	b_{22}	b_{23}	b_{31}	b_{32}	b_{33}	x_1'	x_2'	k
10^{-15}	99. 55	99. 70	99. 50	99. 70	99. 70	99. 55	99. 65	99. 70	99. 70	99. 57	99. 64	99. 68	99. 70
10^{-10}	99. 58	99. 60	99. 63	99. 68	99. 71	99. 60	99. 64	99. 71	99. 65	99. 57	99. 61	99. 64	99. 68
10^{-5}	99. 65	99. 68	99. 70	99. 71	99. 68	99. 58	99. 67	99. 67	99. 69	99. 60	99. 58	99. 65	99. 65
10^{-1}	99. 64	99. 54	99. 65	99. 60	99. 70	99. 59	99. 62	99. 86	99. 69	99. 58	99. 62	99. 63	99. 67

5.4 密钥空间分析

通过对密钥密感性测试的数值模拟表明，本算法对密钥集 keys 来讲，任何试图用微小偏差 10^{-15} 来解密原始文本均是不可能的，因此本方案的密钥空间至少可达到 10^{195}，远大于文献[8]中提到的 10^{45} 个密钥个数。此外，由于设计的同胚函数可以是不计其数的，使得密钥空间足以满足安全通讯的各种要求，对入侵者的强力攻击手段有很强的抵抗能力。

结束语 离散广义混沌同步理论为安全通讯提供了新的工具。本文基于定理和著名的方程构造了一个新的系统，结合 Arnold 猫映射，提出的非对称密钥的音频信息隐藏及语音伪装安全通讯方案具有数据源认证功能和大密钥空间。通过对密钥的敏感性及加密图像相关性分析表明，本方案是一个新型的音频信息隐藏方案，普适性好，为克服时间序列单步预测提供了新思路。

参 考 文 献

[1] 刘海燕，郑雪峰，王颖. 基于 DWT 域乘嵌入音频水印的优化检测算法[J]. 仪器仪表学报，2009，1(30)：148-151

[2] 刘振华，张焕国，叶登攀. 信息隐藏技术及其应用(第二版)[M]. 北京：科学出版社，2009

[3] 张向华. 一种新颖的混沌分组密码算法[J]. 计算机科学，2009，5(36)：92-87

[4] Katzenbeisser S, Petitcclas F A P. 信息隐藏技术-隐写术与数字水印[M]. 吴秋新，钮心忻，杨义先，等译. 北京：人民邮电出版社，2001

[5] 晋建秀，丘水生. 基于物理混沌的混合图像加密系统研究[J]. 物理学报，2010，2(59)：792

[6] Yu Dongchuan, Parlitz U. Partial synchronization of chaotic systems with uncertainty[J]. Phys. Rev. E, 2008, 77(6): 6208

[7] Short K M. Signal extraction from chaotic communications [J]. Int. J. Bifurc. Chaos, 1997, 7(7): 1579-1597

[8] Gao H J, Zhang Y S, Liang S Y. A new chaotic algorithm for image encryption[J]. Chaos Solitons Fractals, 2006, 29: 393

[9] Ji Ye, Liu Ting, Min Lequan. Generalized chaos synchronization theorems for bidirectional differential equations and discrete systems with applications[J]. Physics Letters A, 2008, 372: 3645-3652

[10] Celikovsky S, Chen G R. Secure synchronization of a class of chaotic systems from a nonlinear observe approach[J]. IEEE Trans Autom Control, 2005, 50(1): 76

[11] Min L, Chen G, Zhang X, et al. Approach to generalized synchronization with application to chaos-based secure communication[J]. Commun. Theory Physics, 2004, 41: 632

[12] 臧鸿雁，闵乐泉，吴春雪，等. 基于离散混沌系统广义同步定理的数字图像加密方案[J]. 北京科技大学学报，2007，1：29

[13] Kinzel W, Englert A, Kanter I. On chaos synchronization and secure communication [J]. Phil. Trans. R. Soc. A, 2010, 368 (1911): 379-389