混沌系统在密码学中的应用现状及展望

刘金梅[1,2],丘水生[1]
LIU Jin-mei[1,2],QIU Shui-sheng[1]

1. 华南理工大学 电子与信息学院,广州 510640
2. 暨南大学 电子工程系,广州 510632
1. College of Electronic and Information,South China University of Technology,Guangzhou 510640,China
2. Department of Electronic & Engineering,Jinan University,Guangzhou 510632,China
E-mail:jinmei_liu@126.com

LIU Jin-mei,QIU Shui-sheng. Outlook and application of chaotic systems in cryptography. Computer Engineering and Applications,2008,44(14):5-12.

Abstract: Chaotic encryption algorithms realized by only one chaotic system and presented in recent years are briefly summarized. Then, chaotic encryption algorithms realized by multiple chaotic systems are introduced. Outlook for future research is also discussed.
Key words: chaos;encryption;image encryption

摘 要:首先回顾了近几年来出现的单个混沌系统构成的密码算法,然后介绍了由多个混沌系统组合构成的密码算法及其研究现状,最后是对多混沌系统密码算法研究的展望。
关键词:混沌;加密;图像加密
DOI:10.3778/j.issn.1002-8331.2008.14.002 **文章编号**:1002-8331(2008)14-0005-08 **文献标识码**:A **中图分类号**:TP391.4

1 引言

“混沌”一词最早出现于中国和古希腊的神话故事中。非线性动力学中,“混沌”用来描述非线性动力学系统中出现的一种类似随机的不确定输出。混沌理论自20世纪60年代快速发展起来,并在70年代得到基本确立。之后,混沌学的相关研究渗透入许多领域,如:物理学、数学、生物学、化学、信息处科学、经济学、天文学、气象学等,甚至在音乐、艺术等领域,混沌也得到了广泛应用。

混沌最为人熟知的特性是“蝴蝶效应”,即对初始条件或控制参数的极端敏感性,这使得由确定性系统产生的混沌轨道具有长期不可预测性。此外,遍历性和混合性也是许多混沌系统的基本特性。另外,混沌由确定性系统产生,具有确定性。这些特性使得混沌系统可以用来实现密码算法。

混沌密码的发展历程在2003年李树钧的博士学位论文[1]中有详细介绍。本文将主要对自2000年前后以来出现的混沌密码算法加以概述。目前提出的混沌密码算法多数是基于单个混沌系统的,不防称之为单混沌密码算法;之后,陆续出现了一些使用多个混沌系统的密码算法,称之为多混沌密码算法。本文的第2章简要叙述了单混沌密码算法的研究现状;第3章介绍了单混沌密码算法的局限性;第4章介绍了多混沌系统密码算法的研究现状;第5章是关于多混沌密码算法研究的展望。

2 单混沌密码算法的研究现状

按照算法的主要特性和用途的不同,从以下几个方面介绍单混沌密码算法的研究现状:(1)典型的单混沌密码;(2)单混沌伪随机流生成器;(3)单混沌分组密码;(4)单混沌图像加密算法;(5)单混沌公钥密码。

2.1 典型的单混沌密码

M. S. Baptista在1998年提出了一种基于搜索机制的混沌密码算法[2],在此称之为Baptista型算法。E. Alvarez等人在1999年提出的混沌密码算法也是基于搜索机制的[3],称之为Alvarez型算法。下面将对Baptista型算法及其改进、Alvarez型算法及其改进和其它类型的通用单混沌密码算法加以概述。

2.1.1 Baptista型算法及其改进

2.1.1.1 Baptista型算法

Baptista型算法是一种用混沌系统的迭代次数作为密文的文本信息加密算法。该算法不涉及混沌同步或混沌控制,主要利用混沌系统的遍历性,将明文字符加密成混沌系统(如:Logistic映射)的迭代次数。算法可大体描述如下[2]:

设选用一维Logistic混沌映射

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No. 60372004);广东省自然科学基金(the Natural Science Foundation of Guangdong Province of China under Grant No. 031445);暨南大学引进人才启动基金项目(No. 51205068)。
作者简介:刘金梅(1975-),女,博士生,主要研究方向:信息安全及混沌保密通信;丘水生(1939-),男,博士生导师,主要研究方向:非线性电路与系统、混沌理论及混沌保密通信。
收稿日期:2008-01-02 **修回日期**:2008-02-29

$$X_{n+1} = F(X_n) = bX_n(1 - X_n) \quad (1)$$

其中 $X_n \in [0,1]$,控制参数 b 的选取保证系统具有混沌特性。

设明文由 S 种字符构成,通过混沌迭代将 S 种字符分别与混沌吸引子(部分区域或全部区域)均分的 S 个 ε-间隔对应起来。若用 $[X_{\min},X_{\max}]$ 表示混沌吸引子的范围,则第 $i(i=1,2,\cdots,S)$ 个 ε-间隔的范围是:$[X_{\min}+(i-1)\varepsilon,X_{\min}+i\varepsilon]$,且 $\varepsilon=(X_{\max}-X_{\min})/S$。$S$ 种字符和 S 个 ε-间隔之间的对应关系以及混沌映射式(1)的初值 X_0 和控制参数 b 作为密钥(共 $S+2$ 个密钥参数)。

设 C_1 为第一个明文字符,若混沌映射式(1)自初值 X_0 经 E_1 次迭代后,其混沌值 X_1 恰好落入 C_1 对应的 ε-间隔内(对应关系为密钥之一),即:$X_1=F^{E_1}(X_0)$,则 E_1 即为 C_1 对应的密文。对于第二个明文字符 C_2,若混沌映射式(1)自 X_1 经 E_2 次迭代后,其混沌值 X_2 恰好落入 C_2 对应的 ε-间隔内,即:$X_2=F^{E_2}(X_1)$,则 E_2 即为 C_2 对应的密文。

依次类推,直至所有明文字符加密完毕。

合法接收端持有与发送端相同的密钥,只需按照收到的密文对混沌映射依次迭代 E_1 次、E_2 次、……,即可得到正确恢复的明文。

此算法中,由于加密不同字符时,相应的混沌迭代起始值不是固定的,所以不同明文有可能对应相同的密文,即得到的不是一一对应的明文-密文对,这与传统的加密方法有所不同。

为避免迭代次数过大,限制迭代次数的上限值为 65 532(不超过 1 个字节的二进制数)。另外,还可设置迭代次数下限值 N_0 和重复系数 η。若 $N_0=256$,则任一密文 $E_n \in (250,65\ 532)$。若重复系数 $\eta=0$,则密文 E_n 为混沌值第一次落入与明文 C_n 对应的 ε-间隔时的迭代次数;若重复系数 $\eta\neq0$,则密文 E_n 为混沌值第 η 次落入与明文 C_n 对应的 ε-间隔时的迭代总次数。η 的设置有助于克服利用密文出现频率进行的密码分析。η 只需在发送端设置,接收端无需设置。

该算法的可行性源于混沌映射的遍历性。例如:对于混沌映射式(1),若取 $b=3.78$,$\varepsilon=0.002\ 343\ 750$,$[X_{\min},X_{\max}]=[0.2,0.8]$,$S=256$,自 $[X_{\min},X_{\max}]$ 内的初值经 65 532 次迭代后,到达任一个 ε-间隔的次数至少为 60 次。这说明了算法的可行性,但由于加密一个明文字符需要迭代多次,因此该算法不适用于要求快速加密(如:实时图像加密)的场合。

2.1.1.2 Baptista 型算法的改进算法

Baptista 型算法一经提出,就受到了广泛关注。但该算法存在运算速度慢、密文分布不均匀的缺陷。相继有许多改进算法提出来,但这些改进算法也陆续被证明不安全。

文献[4-7]都是 Wong 等人提出的改进算法。文献[4]提出的改进算法使密文分布曲线平坦,并缩短了加密时间。而且,密文分布平坦性和加密时间之间的权衡可由一个参数 $r_{\max}$ 来控制。$r_{\max}$ 大,可获取较平坦的密文分布特性,但迭代次数也随之增加,加密时间延长;$r_{\max}$ 小,所需加密时间短,但不利于密文的平坦分布。

文献[4]解决了密文分布不均匀的问题。文献[5]则针对原 Baptista 型算法加密速度慢的缺点,减小 logistic 映射的迭代次数。同时为避免安全性受到影响,使用动态查询表将密文和明文对应起来,并相应根据密文动态更新查询表。文献[4,5]比原 Baptista 型算法的加密速度快,但由于其密文至少是明文长度的两倍,导致密文文件大,传输时间长。文献[6]提出了一种减小密文长度的加密算法,使密文长度仅仅略大于明文长度。并引入会话密钥,以便灵活改变信息对应的密文长度。算法中,密文由两部分组成。第一部分是用传统方法加密会话密钥所需用的迭代次数;第二部分反映信息分组在动态查询表中的位置。动态查询表的更新方法与文献[5]中的相同。密文的第二部分的长度与明文长度相同,所以总的密文长度仅比明文长度多出第一部分的长度。这段长度对于大容量的多媒体文件来说微乎其微。因此,密文仅仅比明文略长,便于存储和传输。文献[6]还对文献[5]中查询表更新的定位方法进行了改变。文献[7]进一步将文献[5]提出的基于动态查询表的 Baptista 型改进算法扩展,使之既可以用来加密,又可以用来产生哈希值。

文献[8]的具体加密步骤与 Baptista 型算法相似,只是利用了不同的混沌吸引子之间的周期性切换。因为加密密钥的周期切换可作为增强安全性的一种机制。文中所说的周期混沌,是指通过周期性的改变密钥,使其运行轨道在多个混沌吸引子之间进行切换。本文将其归类为 Baptista 型改进算法。

文献[9]指出了 Baptista 型加密算法及其改进算法中存在的缺陷,并提出了一些措施加以克服。

文献[10]提出的 Baptista 型改进算法,实际是 Wong 等人的基于查询表加密算法的改进。文中使用分段线性混沌映射(PLCM)来提高算法的灵活性,因为 PLCM 是遍历的、且具有均匀不变的密度函数。实验结果证明,相比文献[5-7]中的加密算法而言,PLCM 的使用提高了加密速度。而且,采用了新的动态查询表来提高系统的安全性。文献[11]也是对 Baptista 型算法的改进,利用了动态更新的交换表,其本质和基于动态查询表的 Wong 提出的算法相类似。文献[12]提出的改进算法中,使用了子密钥数组来增强安全性。

文献[13]通过混沌映射的迭代来实现分组密码算法。使用混沌映射生成的二进制随机序列,明文分组利用与密钥相关的移位方法进行置换,然后利用混沌掩盖方法加密。作者称此算法是 Baptista 型算法的一种改进形式。经过分析,该算法实际为流密码算法。

2.1.1.3 Baptista 型算法及其改进算法的密码分析

与 Baptista 型算法及其改进形式相继出现的是与之相关的密码分析方面的文章。

文献[14]指出 Baptista 型算法不仅速度慢,且不够安全,利用已知明文攻击将其破译。文献[15]指出文献[14]中 G. Jakimoski 和 L. Kocarev 对 Baptista 型算法的攻击方法不一定十分有效。提出相应的改进措施以抵御文献[14]所述的攻击。文献[16]指出改进后的方法仍是不安全的。

文献[17]利用 4 种攻击方法成功破译了 Baptista 型算法,即:一次一密攻击、熵攻击、恢复密钥攻击、估计参数和初始条件的攻击。

文献[18]对文献[4]提出的加密算法进行了分析,利用三种方法对其进行攻击:选择密文、选择明文、已知明文。指出文献[4]中的算法实际是流密码算法,其致命缺陷在于:重复使用同一密钥且加密速度低。

文献[19]对文献[5-7]中基于动态查询表的算法进行了分析,指出这类算法的安全性不够高,并给出了一些破译这类算法的例子。文献[5-7]中的更新表只与明文有关,而与密

钥无关。当使用不同的密钥加密相同的明文时,动态查询表的更新次序是一样的。因此,根据 Kerkhoff 准则(加密系统的安全性完全依赖于密钥),算法不安全。

文献[20]指出文献[13]中的算法实际为流密码,且其密钥流与明文无关,故算法不够安全。

这里认为,Baptista 型算法及其改进形式被成功破译的根本原因在于:对 Baptista 及其改进型算法进行攻击时,利用了 logistic 映射的无限窗口。而在原算法中,一般 logistic 映射的参数值接近 4。故,在原算法中,密文分布特性较为平坦。许多密码分析方法,正是借助了 logistic 映射的弱点。另外,一些算法中,由于重复使用同一密钥而降低了安全性。

2.1.2 Alvarez 型算法及其改进

Alvarez 型算法[3]是一种对称分组混沌密码算法,它将每组明文加密为由三个部分构成的密文分组,且分组长度可变。算法简述如下:

利用混沌动力系统:

$$x_{n+1} = f(x_n, x_{n-1}, \cdots, x_{n-d+1}) \tag{2}$$

选择门限 U_1,且 $C_1 = \begin{cases} 0 & x_n \leqslant U_1 \\ 1 & x_n > U_1 \end{cases}$

原明文:$A = \underbrace{01\cdots10}_{\text{长度为}b_1}0101\cdots$

迭代混沌动力系统式(2),当 $C_1 = 011\cdots0011\underbrace{101\cdots1}$中出现与 A 中长为 b_1 的原明文信息组相同的序列 S_1 时,记下 S_1 序列中的第一个字符开始出现时的 $\boldsymbol{x}_{n1} = (x_{n1}, x_{n1-1}, \cdots, x_{n1-d+1})$并停止迭代(若在较大长度内找不到相应的明文分组,则 $b_1 = b_1 - 1$,重新开始搜索)。得到 $d+2$ 个实数:$(U_1, b_1, \boldsymbol{x}_{n1})$ 是长度为 b_1 的明文信息分组对应的密文。下一轮加密,选择新的初值和门限值,得到密文$(U_2, b_2, \boldsymbol{x}_{n2})$。依此类推,直至所有明文加密完毕。

还可采用多个动力系统,随机选择用哪个动力系统加密某一分组,如:若用第 i_k 个动力系统,则密文$(i_k, U_k, b_k, \boldsymbol{x}_k)$。

解密时,对于第 i 组密文,将混沌动力系统自初值 $\boldsymbol{x}_{ni}$迭代 b_i 次,可根据 U_i 得到相应的明文序列。

Alvarez 型混沌密码算法是基于搜索方式的,且密文长度大于明文长度。密文有效率低。其加密速度也较慢,且加密速度由明文分组的搜索过程决定,加密速度是时变的。因此,该算法不适合在明文量大、对加密速度要求高的情况下使用。

Alvarez 型算法提出来之后,即陆续有文章指出该算法是不安全的[14,21,22]。

首先对 Alvarez 型算法进行密码分析的是文献[21]。其中描述了对算法的 4 种攻击:选择密文攻击、选择明文攻击、已知明文攻击和唯密文攻击。文章指出 Alvarez 型算法的不足之处在于:没有明确给出密钥空间;怎样选择或生成初值;计算中使用的精度和怎样处理机器间的不同精度问题;并且,当密钥略有不同时,明文和解密出的明文有许多相似之处。而在一个好的加密系统中,当密钥中有一位改变时,应至少有 50% 的加密信息发生改变。Alvarez 型算法使用了帐蓬映射。文献[21]指出,好的密钥生成的轨道的周期长,而帐蓬映射在这一点性能较差。并且预言,文献[3]中即使不采用帐蓬映射,性能也不会有所提高。实际上 Alvarez 型算法的根本缺陷在于:密文组$(U_1, b_1, \boldsymbol{x}_{n1})$中包含的信息太多,导致算法不安全。

文献[14]利用已知明文攻击破译了 Baptista 型算法和 Alvarez 型算法。并指出,这两种加密算法的速度较慢,低于常规加密算法。

文献[22]是对 Alvarez 型算法的改进。针对 Alvarez 型算法在文献[21]中被 G. Alvarez 等人用 4 种攻击破译,文献[22]进一步分析指出了 Alvarez 型算法的两个本质缺陷:(1)密文中 $\boldsymbol{x}_i$ 的出现,导致一定的信息泄露;(2)密钥不同,系统表现出不同的动力特性,且这种不同特性可由 $\boldsymbol{x}_i$ 反映出来。提出了相应的改进算法,并对改进算法进行了原理分析和仿真验证。改进算法中采用一维混沌映射,为避免重复上述缺陷(2),要求该映射在值域内具有遍历性及唯一的概率密度函数,以抵御基于统计的分析方法。例如:分段线性映射。对一个信息分组加密时,是从上一分组加密后得到的混沌值开始,不再是从初值 x_0 开始。因此变成了流密码加密,不再是分组加密。且密文中不再直接包含混沌映射的状态信息 $\boldsymbol{x}_i$,而是代之以迭代次数。另外,考虑到计算机的有限精度会造成混沌系统的短周期效应、不理想的分布特性和相关函数等,利用线性反馈移位寄存器产生伪随机数,扰动混沌系统,来改善有限精度效应。其它避免有限精度影响的方法还有:提高运算精度、或者级联多个混沌系统。为了克服密文比明文长的弱点,文中采用 Huffman 编码对密文进行了无损压缩。但这种改进的 Alvarez 型算法仍然速度较慢。目前尚未见到对这一改进算法的密码分析的文章发表。

2.1.3 其他典型的单混沌密码算法

近几年提出的使用单一混沌系统构成的密码算法中,比较典型的有以下算法。

文献[23]提出了一种基于离散化斜帐蓬映射的混沌加密算法。并对算法的与随机性有关的一些特性参数进行了分析,如:李氏指数、自相关函数、遍历性、混合特性、KS 熵。

Pareek 等人在文献[24]提出了一种基于外部密钥的混沌加密算法。指出,一个好的加密算法应具有以下特性:对明文敏感;对密钥敏感;对于给定的明文产生随机的密文。该算法被 G. Alvarez 等人在文献[25]中破译。文献[25]指出文献[24]中算法不安全的原因有两个:(1)所用 logistic 映射的分布不均匀,通过已知明文攻击可得到 logistic 映射的参数;(2)由外部密钥计算初值和迭代次数的方法有缺陷,借此可实施选择密文攻击和选择明文攻击。文献[26]对文献[24]中的算法进行了改进,并通过理论分析和数值仿真说明改进算法的安全性和优越性。该改进算法的安全性有待研究。

针对利用回归映射的攻击,Bu 和 Wang 提出了一种抵御此攻击的简单调制方法[44],以增强混沌保密通信的安全性。该方法利用一个周期信号调制发送信号,打乱重构的回归映射。虽然该方法能够抵御回归映射攻击,但容易被其它方法破译[28-30]。其中,文献[28]和文献[29]利用频谱分析,文献[30]使用自相关分析。这些攻击方法主要是利用调制信号过零点的潜在周期性。文献[30]中还提出了一种改进的调制方案,以削除调制函数过零点的潜在周期性。文献[31]指出,由文献[30]提出的这种改进方法在一种新的攻击方式下仍然是不安全的。这种攻击方式可以存储回归映射,它可以近似识别出调制信号的一些参数。与现有的攻击方法相比,所提出的攻击方法更有效,也可以攻破原来的 Bu-Wang 方案。而且,从密码术的观点来看,即使调制信号是足够安全的,基于调制的方法在增强安全性上也并不令人满意。

文献[32]提出了一种用于数字通信的基于混沌密钥的加密方案。加密在物理层进行,即:加密变换作用于波形信号,而不是符号序列。加密过程对一个由信息信号和混沌加密信号构成的二维信号进行变换。密钥决定变换的次数。该加密方案在文献[33]中证明是不安全的。文献[33]指出,文献[32]中算法不安全的根本原因在于:(1)实数的有限精度实现;(2)即使是在无限精度、无限存储容量的情况下,由于密文的幅度值仅仅依赖于密钥,算法也不够安全。而且,当迭代次数 n 很大时,需要有无限快的运算速度、无限大的存储容量、无限精度的理想计算机。提出了以下改进措施:(1)不使用迭代次数 n 作为密钥,改用其它参数作为密钥,如:混沌系统的参数或初值等;(2)对原二维 Baker 映射离散化;(3)对密文信息进行掩盖。

其它还有:利用混沌系统和代数编码[34,35];利用二维混沌映射构成文本加密算法[36];利用混沌神经网络的加密算法[37]及其分析[38]。

2.2 单混沌流密码

目前提出的混沌流密码大多是采用单一混沌映射。许多混沌流密码的研究侧重于讨论怎样克服有限计算精度,以便使生成的伪随机序列具有更好的随机性。

周红等人在文献[39]中指出,若混沌系统由于有限精度的影响而进入周期循环,则可通过扰动使它脱离周期循环。扰动信号利用最大长度线性反馈移位寄存器来产生。并规定了信噪比和扰动间隔。文献[40]提出了一种基于 m 序列的扰动策略,以解决有限精度效应带来的短周期问题。可指定扩展后的周期长度,并保持了原混沌动力系统的统计特性。扩展后的周期长度的下限为 $\Delta(2^L-1)$。文献[41,42]建议通过提高计算精度来扩展周期长度。文献[43]中采用的也是扰动策略,但其扰动由另一混沌系统产生,此方法带来不可预测的周期长度和统计特性。

其它还有:文献[44,45]使用分段线性一维混沌映射,文献[46]使用锯齿混沌映射,文献[47]使用时空混沌系统生成多个伪随机比特序列。

2.3 单混沌分组密码

在由单个混沌构成的分组密码算法中,大多使用一维或二维混沌映射。

文献[48]中提出了一种利用二维 baker 映射实现混沌置换,构造分组密码。Fridrich 在文献[49]中扩展了其思想,将二维映射离散化成有限的矩形格子点,然后将其扩展成三维,得到更为复杂的置换密码,最后使用了简单的混淆机制。算法的优点在于:可变的密钥长度和可变分组长度,且加密后的文件与原文件大小相同。缺点是密钥长度依赖于分组长度。

文献[50-52]中使用的都是一维混沌映射。文献[50]使用一维帐篷映射,文献[51]使用混沌标准映射,文献[52]利用参数随机改变的一维混沌映射。文献[53]用 logistic 映射作为 S 盒来构造分组密码,并提出了设计基于混沌映射的分组密码算法的步骤。在文献[54]中,作者进一步证明了文献[53]的分组加密算法可抵御差分攻击和线性攻击。文献[55]的主旨与其类似,指出混沌映射可用来设计 S 盒,并能抵御线性攻击和差分攻击。文献[56]提出用元胞自动机构造分组密码,但被文献[57]证明不安全。

2.4 单混沌图像加密算法

图像加密的基本思想主要有:位置置换、值变换,及两种形式的混合。由于图像信息本身的特性,图像加密在使用单个混沌映射时,一般要用二维或二维以上的混沌映射。许多图像加密算法使用的是多个一维或一维以上的混沌映射。

Fridrich J. 在文献[58]中提出一种基于二维混沌映射的图像加密算法。加密过程由混沌混淆和像素置换构成。该文章被认为是关于混沌图像加密方面的经典文献,并被多次引用。但文献[59]指出,文献[58]的算法不够安全,对其进行了蛮力攻击、统计攻击、已知明文攻击和选择明文攻击,并提出一些措施增强原系统的安全性。

文献[60]中使用了三维猫映射,该文章也多次被引用。但其算法被文献[61]指出是不安全的。文献[62]使用的是单向耦合映射格子(OCML)实现图像加密。文献[63]使用超混沌映射。其它还有使用离散指数混沌映射的[64]、使用由指数函数和正切函数的非线性混沌算法的[65]。

2.5 单混沌公钥密码

混沌用于公钥密码是近几年才发展起来的。已提出的单混沌公钥密码算法有:基于分布式动力系统的公钥密码[66-68]、基于混沌映射的通用 RSA 算法[69]、基于耦合映像格子通用同步的公钥密码[70]、基于切比雪夫多项式的公钥密码[71]。

3 单混沌密码算法的局限性

单混沌密码算法在安全性上有一定的局限。因为单个混沌系统的特性容易研究,由单个混沌系统构成的加密算法在一些针对混沌密码进行的攻击面前,往往十分脆弱。

对混沌密码进行的攻击方法,主要有:利用频谱特性[28,29,72]、利用回归映射[73]、利用混沌序列及其时延之间的关系[74]、利用非线性动力预测技术[75]、利用误差函数(EFA)[76]、利用自相关分析[30,77]等等。

单个混沌系统的特性,如:功率谱、频谱、自相关函数、回归映射、混沌序列及其时延之间的关系、误差函数特性等,往往已十分明确。这为密码攻击者提供很好的便利条件。而且,在 EFA 攻击下,高维混沌系统并不意味着比低维系统有更高的安全性[76]。这样,利用多个混沌系统的算法显出了其优势。多个混沌系统特性复杂,其特性不那么单一,提高了安全性[74]。同时,多个混沌系统联合使用,还能够在一定程度上克服有限精度效应带来的动力学退化[22]。

4 多混沌密码算法的研究现状

由多个混沌系统构成的密码算法,大多用于图像加密。还未见有利用多个混沌系统实现流密码算法的报道。以下将分别介绍:(1)典型的多混沌密码算法;(2)多混沌伪随机流生成器;(3)多混沌分组密码;(4)多混沌图像加密算法;(5)多混沌公钥密码。

4.1 典型的多混沌密码算法

文献[78]提出了一种使用两个混沌系统的保密通信方案。其中,一个混沌系统用于混沌加密器和解密器之间的同步,另一个混沌系统用来对明文加密。传送的是同步信号,不是加密信息。解密器和加密器同步以后,可以得到密钥信号,实现解密。该算法被文献[79]证明是不安全的。文献[79]利用非线性动力预测技术根据同步信号恢复原明文信息,指

出同步信号所泄漏的信息会降低算法的安全性。文献[80]也采用了与文献[78]中类似的加密方案。

较早提出用级联混沌结构来提高混沌加密器安全性的是文献[81,82]。较早提出使用多个混沌动力系统构造加密算法的文献[83],其中使用了多个分段线性映射。该算法被 G. Alvarez 等人在文献[84]中用 4 种攻击方法成功破译。这里认为,该算法的本质缺陷在于没有使用密文反馈。文献文献[85]中采用多个一维混沌映射构造加密算法,但被文献[86]证明是不安全的。

文献[87]使用了两个混沌系统,其中一个混沌系统生成的序列作为密钥,来构造加密系统。文献[88]基于一维混合混沌映射 $H_p(x)=r_p^{-1}\circ G\circ r_p(x)$($x\in[0,10^p)$,$p$ 为正整数)构造加密算法,其中 $G(x)=10x(\mathrm{mod}\ 10)$,$r_p(x)=\sqrt[p]{x}$。文献[89]使用了一组混沌系统实现加密。基于多个随机映射的符号动力学和位置相关的权重概率设计混沌加密系统。文章的核心思想在于,给定两个动力系统,可以将它们组合为一个新的动力系统。这种组合式的系统与原先的单个系统截然不同。所提出的方案利用了一组混沌映射的符号动力特性来编码二进制信息。目前尚未有关于这三种算法的密码分析的报道。

4.2 多混沌伪随机流生成器

多个混沌系统在混沌流密码方面的应用很少。目前仅发现在文献[90]中使用两个混沌系统来生成随机序列。其中一个混沌系统的输出作为扰动信号,作用于另一个混沌系统,以克服有限精度效应带来的动力学退化。

4.3 多混沌分组密码

将多个混沌系统用于分组密码算法,目前仅见到一篇相关的文献,即文献[91]。其中使用了三个级联的离散混沌映射。

4.4 多混沌图像加密算法

文献[92-94]描述了一种级联混沌图像加密算法及其 VLSI 实现。利用一维 logistic 混沌系统和置换方案,原图像的所有子图重新排列,且每个子图内的像素置乱。文献[95]指出文献[92]和文献[94]中算法的缺陷并提出了相应的改进方案。文献[96]是对文献[94]算法的改进。文献[94]中提出的算法被文献[95]用选择/已知明文攻击和唯密文攻击破译。文献[96]给出了相应的改进算法及其 VLSI 结构,并用 Xilinx ModelSim 仿真表明方案的有效性。

文献[97]使用了 Arnold Cat 映射和陈氏混沌系统,通过位置置乱和像素灰度值的改变来混淆原图像和加密图像之间的关系。首先,用 Arnold Cat 映射来置乱空间域中的图像像素值;然后,陈氏混沌系统的离散化输出进行预处理后,再对置乱后的图像进行逐像素点加密。文献[98]利用 Arnold cat 映射和 Lu 映射实现图像加密。Arnold cat 映射的输出送入 Lu 映射。

文献[99]的图像加密算法使用了两个 logistic 映射。两个 logistic 映射的初始条件根据外部密钥各个比特的不同权重得出。而且,用 8 种不同的操作加密图像的像素,并根据 logistic 映射的输出来选用哪一种操作。每加密 16 个像素,即改变一次密钥。文献[100]利用一维 logistic 映射和超混沌映射实现图像的加密。一维 logistic 映射的输出用于选择超混沌映射输出值的上升矩阵或下降矩阵。超混沌映射产生两个序列,一个序列用于生成上升矩阵或下降矩阵,用于原图像的置乱;另一序列用于图像的混淆。映射的初值作为密钥。且每次加密,进行几轮置乱和混淆,以增强安全性。文献[101]使用了耦合混沌映射和一维混沌映射进行图像加密。

文献[102]提出了一种流密码结构的快速图像加密算法。为提高速度,并便于硬件实现,使用了 32 位有限精度的定点运算。加密系统的核心是一个基于级联混沌映射的伪随机密钥流生成器,用于产生序列和进行随机置乱。与已有伪随机数生成器的不同点在于,所提出的密钥流生成器不仅速度快,而且通过了统计测试。文献[103]提出了一种基于二维猫映射和 S 盒的图像加密算法。在 S 盒前后分别各加一级由多个 PLCM 构成的掩盖操作。

4.5 多混沌公钥密码

文献[104]提出了一种基于多个混沌系统的公钥加密算法。文献[105]基于 Parseval 定理对其成功破译。文献[106]对文献[104]进行了改进,以抵御[105]提出的攻击方法。进一步的实验结果反映了文献[104]中算法的缺陷,并从理论分析上证明破译该系统的复杂度不象以往认为的那么高。

5 关于多混沌密码算法研究的展望

相对于单混沌密码算法而言,多混沌密码算法具有以下明显的优势:多个混沌系统联合使用,其物理特性复杂,所生成的序列具有更高的不可预测性,从而提高了安全性。同时,还能够从一定程度上克服有限精度效应带来的动力学退化问题。目前也有一些关于多混沌系统复合后物理特性方面的文章发表[107,108]。

直观地来看,多混沌密码算法的运算速度比单混沌密码算法的运算速度要慢。但也不尽然。许多单混沌密码算法为保证安全性,往往需要很高的迭代次数,如:Baptista 型算法[2]的迭代次数一般大于 100。在使用多混沌密码算法时,迭代次数不需要很大,就可达到很好的安全性[109]。所以,多混沌密码算法并不一定比单混沌密码算法的运算速度慢。同时,为了尽可能降低算法复杂度,一般可只考虑使用两个混沌系统。而且,应尽可能选用运算简单的混沌系统,如分段线性映射等。这样不但可以降低算法复杂度,而且有助于提高运算速度。

多混沌密码算法在混沌公钥密码和混沌图像加密方面应能够显出其独特优势。

目前,关于多个混沌系统构成的密码算法方面发表的文章并不是很多。而且,还没有关于多混沌密码算法的通用框架方面的报道。这里认为,研究这样一个通用框架是很有意义。比如,即使是两个最简单的混沌系统组合使用,也有多个不同的方案可供选择,是否存在一个安全性高、运算速度快、计算复杂度低的最佳方案呢?这个最佳方案是否具有通用性呢?另外,多混沌密码算法中,多个混沌系统之间的输出怎样同步?怎样利用并行算法来提高运算速度?等等这些问题都有待进一步研究。

参考文献

[1] 李树钧. 数字化混沌密码的分析和设计[D/OL]. 西安:西安交通大学,2003. http://www.hooklee.com.

[2] Baptista M S. Cryptography with chaos[J]. Physics Letters A,1998,

240(1/2):50-54.
[3] Alvarez E,Fernández A,García P,et al. New approach to chaotic encryption[J]. Physics Letters A,1999,263(4/6):373-375.
[4] Wong W K,Lee L P,Wong K W. A modified chaotic cryptographic method[J]. Computer Physics Communications,2001,138(3):234-236.
[5] Wong K W. A fast chaotic cryptographic scheme with dynamic look-up table[J]. Physics Letters A,2002,298(4):238-242.
[6] Wong K W,Ho S W,Yung C K. A chaotic cryptography scheme for generating short ciphertext[J]. Physics Letters A,2003,310(1):67-73.
[7] Wong K W. A combined chaotic cryptographic and hashing scheme[J]. Physics Letters A,2003,307(5/6):292-298.
[8] Palacios A,Juarez H. Cryptography with cycling chaos[J]. Physics Letters A,2002,303(5/6):345-351.
[9] Li Shu-jun,Chen Guan-rong,Wong K W,et al. Baptista-type chaotic cryptosystems:problems and countermeasures[J]. Physics Letters A,2004,332:368-375.
[10] Huang Fang-jun,Guan Zhi-hong. A modified method of a class of recently presented cryptosystems[J]. Chaos,Solitons and Fractals,2005,23:1893-1899.
[11] Wei Jun,Liao Xiao-feng,Wong K W,et al. A new chaotic cryptosystem[J]. Chaos,Solitons and Fractals,2006,30(5):1143-1152.
[12] Wei Jun ,Liao Xiao-feng,Wong K W,et al. Analysis and improvement for the performance of Baptista's cryptographic scheme[J]. Physics Letters A,2006,354:101-109.
[13] Xiang Tao,Liao Xiao-feng,Tang Guo-ping,et al. A novel block cryptosystem based on iterating a chaotic map[J]. Physics Letters A,2006,349:109-115.
[14] Jakimoski G,Kocarev L. Analysis of some recently proposed chaos-based encryption algorithms[J]. Physics Letters A,2001,291(6):381-384.
[15] Li Shu-jun,Mou Xuan-qin,Ji Zhen,et al. Performance analysis of Jakimoski-Kocarev attack on a class of chaotic cryptosystems[J]. Physics Letters A,2003,307(1):22-28.
[16] Chen Yong,Liao Xiao-feng. Cryptanalysis on a modified Baptista-type cryptosystem with chaotic masking algorithm[J]. Physics Letters A,2005,342:389-396.
[17] Álvarez G,Montoya F,Romera M,et al. Cryptanalysis of an ergodic chaotic cipher[J]. Physics Letters A,2003,311(2/3):172-179.
[18] Alvarez G,Montoya F,Romera M,et al. Keystream cryptanalysis of a chaotic cryptographic method[J]. Computer Physics Communications,2004,156:205-207.
[19] Alvarez G,Montoya F,Romera M,et al. Cryptanalysis of dynamic look-up table based chaotic cryptosystems[J]. Physics Letters A,2004,326:211-218.
[20] Wang Yong,Liao Xiao-feng,Xiang Tao,et al. Cryptanalysis and improvement on a block cryptosystem based on iteration a chaotic map[J]. Physics Letters A,2007,363:277-281.
[21] Alvarez G,Montoya F,Romera M,et al. Cryptanalysis of a chaotic encryption system[J]. Physics Letters A,2000,276:191-196.
[22] Li Shu-jun,Mou Xuan-qin,Cai Yuan-long. Improving security of a chaotic encryption approach[J]. Physics Letters A,2001,290(3/4):127-133 .
[23] Naoki Masuda,Kazuyuki Aihara. Cryptosystems with discretized chaotic maps[J]. IEEE Trans on Circuits and Systems-I,2002,49(1):28-40.
[24] Pareek N K,Patidar V,Sud K K. Discrete chaotic cryptography using external key[J]. Physics Letters A,2003,309:75-82.
[25] Alvarez G,Montoya F,Romera M,et al. Cryptanalysis of a discrete chaotic cryptosystem using external key[J]. Physics Letters A,2003,319(1/2):334-339.
[26] Xiang Tao,Wong K W,Liao Xiao-feng. An improved chaotic cryptosystem with external key[J]. Communications in Nonlinear Science and Numerical Simulation,2007. DOI:10.1016/j.cnsns.2007.04.017.
[27] Bu Shou-liang,Wang Bing-hong. Improving the security of chaotic encryption by using a simple modulating method[J]. Chaos,Solitons and Fractals,2004,19:919-924.
[28] Alvarez G,Montoya F,Romera M,et al. Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value[J]. Chaos,Solitons and Fractals 2005,23:1749-1756.
[29] Chee C Y,Xu D,Bishop S R. A zero-crossing approach to uncover the mask by chaotic encryption with periodic modulation[J]. Chaos,Solitons and Fractals,2004,21(5):1129-1134.
[30] Wu X,Hu H,Zhang B. Analyzing and improving a chaotic encryption method[J]. Chaos,Solitons and Fractals,2004,22(2):367-373.
[31] Li Shu-jun,Alvarez G,Chen Guan-rong. Breaking a chaos-based secure communication scheme designed by an improved modulation method[J]. Chaos,Solitons and Fractals,2005,25:109-120.
[32] Machado R F,Baptista M S,Grebogi C. Cryptography with chaos at the physical level[J]. Chaos,Solitons and Fractals,2004,21:1265-1269.
[33] Alvarez G,Li Shu-jun. Breaking an encryption scheme based on chaotic baker map[J]. Physics Letters A,2006,352:78-82.
[34] Ranjan Bose,Saumitr Pathak. A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system[J]. IEEE Trans on Circuits and Systems-I,2006,53(4):848-857.
[35] Mi Bo,Liao Xiao-feng,Chen Yong. A novel chaotic encryption scheme based on arithmetic coding[J]. Chaos,Solitons and Fractals,2007. DOI:10.1016/j.chaos.2007.01.133.
[36] Xiang Tao,Wong K W,Liao Xiao-feng. A novel symmetrical cryptosystem based on discretized two-dimensional chaotic map[J]. Physics Letters A,2007,364:252-258.
[37] Yu W,Cao J. Cryptography based on delayed neural networks[J]. Physics Letter A,2006,356:333-338.
[38] Yang Ji-yun,Liao Xiao-feng,Yu Wen-wu,et al. Cryptanalysis of a cryptographic scheme based on delayed chaotic neural networks[J]. Chaos,Solitons and Fractals,2007. DOI:10.1016/j.chaos.2007.08.029.
[39] 周红,凌燮亭. 有限精度混沌系统的 m 序列扰动实现[J]. 电子学报,1997,25(7):95-97.
[40] 桑涛,王汝笠,严义埙. 一类新型混沌反馈密码序列的理论设计[J]. 电子学报,1999,27(7):47-50.
[41] Lin T,Chua L O. On chaos of digital filters in the real word[J]. IEEE Trans on Circuits and Systems-I,1991,CAS-38(5):557-558.
[42] Wheeler D D,Matthews R A. Supercomputer investigations of a chaotic encryption algorithm[J]. Cryptologia,1991,15:140-152.
[43] Heidari-bateni G,Mcgillem D. A chaotic direct-sequence spread-spectrum communication system[J]. IEEE Trans Commun,1994,COM-42(2/3/4):1524-1527.
[44] Stojanovski T,Pihl J,Kocarev L. Chaos-based random number generators-Part Ⅱ:practical realization[J]. IEEE Tran CAS-I,2001,48

(3):382-385.

[45] Stojanovski T, Kocarev L. Chaos-based random number generators-Part I: analysis[J]. IEEE Transactions on Circuits System-1: Fundamental Theory and Applications, 2001, 48(3): 281-288.

[46] Mieczyslaw J. Designing security for number sequences generated by means of the sawtooth chaotic map[J]. IEEE Trans on Circuits and Systems I, 2006, 53(5): 1140-1150.

[47] Li Ping, Li Zhong, Halang W A, et al. A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map[J]. Physics Letters A, 2006, 349: 467-473.

[48] Pichler F, Scharinger J. Finite dimensional generalized baker dynamical systems for cryptographic applications [C]// Lecture Notes in Computer Science, 1996, 1030: 465-476.

[49] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps[J]. Int J Bifurcation and Chaos, 1998, 8(6): 1259-1284.

[50] Xun Yi, Chik How Tan, Chee Kheong Siew. A new block cipher based on chaotic tent maps[J]. IEEE Trans Circuits and Systems I, 2002, 49(1): 1826-1829.

[51] Lian S G, Sun J S, Wang Z Q. A block cipher based on a suitable use of the chaotic standard map[J]. International Journal of Chaos, Solitons and Fractals, 2005, 26 (1): 117-129.

[52] Tong Xiao-jun, Cui Ming-gen. A new chaos encryption algorithm based on parameter randomly changing [C]// IFIP International Conference on Network and Parallel Computing-Workshops, 2007: 303-307.

[53] Kocarev L, Jakimoski G. Logistic map as a block encryption algorithm[J]. Physics Letters A, 2001, 289: 199-206.

[54] Jakimoski G, Kocarev L. Differential and linear probabilities of a block-encryption cipher[J]. IEEE Trans on Circuits and Systems-I, 2003, 50(1): 121-123.

[55] Amigó J M, Szczepanski J, Kocarev L. A chaos-based approach to the design of cryptographically secure substitutions[J]. Physics Letters A, 2005, 343(1/3): 55-60.

[56] Joshi P, Mukhopadhyay D, RoyChowdhury D. Design and analysis of a robust and efficient block cipher using cellular automata [C]// The 20th International Conference on Advanced Information Networking and Applications (AINA 2006), IEEE Computer Society, 2006: 67-71.

[57] Sung J, Hong D, Hong S. Cryptanalysis of an involutional block cipher using cellular automata [J]. Information Processing Letters, 2007, 104: 183-185.

[58] Fridrich J. Image encryption based on chaotic maps [C]// Proceedings of IEEE 1997 International Conference on System, Man and Cybernetics. Orlando: Omni Press, 1997.

[59] Lian Shi-guo, Sun Jin-sheng, Wang Zhi-quan. Security analysis of a chaos-based image encryption algorithm[J]. Physica A, 2005, 351: 645-661.

[60] Chen G R, Mao Y B, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons and Fractals, 2004, 21: 749-761.

[61] Wang Kai, Pei Wen-jiang, Zou Liu-hua, et al. On the security of 3D cat map based symmetric image encryption scheme[J]. Physics Letters A, 2005, 343: 432-439.

[62] Rhouma Rhouma, Soumaya Meherzi, Safya Belghith. OCML-based colour image encryption [J]. Chaos, Solitons and Fractals, 2007. DOI: 10.1016/j.chaos.2007.07.083.

[63] Gao Tie-gang, Chen Zeng-qiang. A new image encryption algorithm based on hyper-chaos [J]. Physics Letters A, 2008, 372 (4): 394-400.

[64] Zhang Lin-hua, Liao Xiao-feng, Wang Xue-bing. An image encryption approach based on chaotic maps[J]. Chaos, Solitons and Fractals, 2005, 24: 759-765.

[65] Gao Hao-jiang, Zhang Yi-sheng, Liang Shu-yun, et al. A new chaotic algorithm for image encryption [J]. Chaos, Solitons and Fractals, 2006, 29: 393-399.

[66] Tenny R, Tsimring L S, Abarbanel H D I, et al. Asymmetric key encryption using distributed chaotic nonlinear dynamics [C]// Proc IASTED Int Conf Communications Internet and Information Technology, St. Thomas, U. S. Virgin Islands, Nov 2002: 338-345.

[67] Tenny R, Tsimring L S, Larson L E, et al. Using distributed nonlinear dynamics for public key encryption[J]. Phys Rev Lett, 2003, 90(4).

[68] Tenny R, Tsimring L S. Additive mixing modulation for public key encryption based on distributed dynamics[J]. IEEE Transactions on Circuits and Systems Ⅰ: Regular Papers, 2005, 52(3): 672-679.

[69] Ljupco Kocarev, Marjan Sterjev, Attila Fekete, et al. Public-key encryption with chaos[J]. Chaos, 2004, 14(4): 1078-1082.

[70] Wang Xin-gang, Gong Xiao-feng, Zhan Meng, et al. Public-key encryption based on generalized synchronization of coupled map lattices[J]. Chaos, 2005, 15.

[71] Bergamo P, D'Arco P, De Santis A, et al. Security of public-key cryptosystems based on chebyshev polynomials[J]. IEEE Trans on Circuits and Systems-I: Regular Papers, 2005, 52(7): 1382-1393.

[72] Yang Tao, Yang Lin-bao, Yang Chun-mei. Breaking chaotic secure communication using a spectrogram [J]. Physics Letters A, 1998, 247: 105-111.

[73] Yang Tao, Yang Lin-bao, Yang Chun-mei. Cryptanalyzing chaotic secure communication using return maps[J]. Physics Letters A, 1998, 245: 495-510.

[74] Sobhy M I, Shehata A E R. Methods of attacking chaotic encryption and countermeasures [C]// IEEE International Conference on Acoustics, Speech, and Signal Processing, 2001, 2: 1001-1004.

[75] Parker A T, Short K M. Reconstructing the keystream from a chaotic encryption scheme[J]. IEEE Trans on Circuits and Systems-I, 2001, 48(5): 624-630.

[76] Wang Xin-gang, Zhan Meng, Lai C H, et al. Error function attack of chaos synchronization based encryption schemes[J]. Chaos, 2004, 14(1): 128-137.

[77] Lei Min, Meng Guang, Feng Zheng-jin. Security analysis of chaotic communication systems based on Volterra-Wiener-Korenberg model [J]. Chaos, Solitons and Fractals, 2006, 28: 264-270.

[78] Yang T, Wu C W, Chua L O. Cryptography based on chaotic systems[J]. IEEE Trans on Circuits and Systems-I: Fundamental Theory and Applications, 1997, 44(5): 469-472.

[79] Parker A T, Short K M. Reconstructing the keystream from a chaotic encryption scheme[J]. IEEE Trans on Circuits and Systems-I, 2001, 48(5): 624-630.

[80] Jiang Z P. A note on chaotic secure communication systems [J]. IEEE Trans Circuits and Systems-I, 2002, 49(1): 92-96.

[81] Gotz M, Kelber K, Schwarz W. Discrete-time chaotic encryption systems-part I: statistical design applied [J]. IEEE Trans on Circuits and Systems-I, 1997, 44(10): 963-970.

[82] Dachselt F, Kelber K, Schwarz W. Discrete-time chaotic encryption systems, Part III: cryptographical analysis [J]. IEEE Trans on Circuits and Systems-I, 1998, 45(9): 983-988.

[83] Carcia P,Jimenez J. Communication through chaotic map systems[J]. Physics Letters A,2002,298:35-40.

[84] Alvarez G,Montoya F,Romera M,et al. Cryptanalysis of a chaotic secure communication system[J]. Physics Letters A,2003,306:200-205.

[85] Pareek N K,Patidar V,Sud K K. Cryptography using multiple one-dimensional chaotic maps[J]. Commun Nonlinear Science and Numerical Simulation,2005,10:715-723.

[86] Wei Jun,Liao Xiao-feng,Wong K W,et al. Cryptanalysis of a cryptosystem using multiple one-dimensional chaotic maps[J]. Physics Letters A,2007,363:277-281.

[87] Huang Fang-jun,Guan Zhi-hong. Cryptosysytem using chaotic keys[J]. Chaos,Solitons and Fractals,2005,23:851-855.

[88] de Oliveira L P L,Sobottka M. Cryptography with chaotic mixing[J]. Chaos,Solitons and Fractals,2008,35(3):466-471.

[89] Behnia S,Akhshani A,Ahadpour S,et al. Cryptography based on chaotic random maps with position dependent weighting probabilities[J]. Chaos,Solitons and Fractals,2007.DOI:10.1016/j.chaos.2007.07.070.

[90] Heidari-bateni G,Mcgillem C D. A chaotic direct-sequence spread-spectrum communication system[J]. IEEE Trans Commun,1994,COM-42(2/3/4):1524-1527.

[91] Behnia S,Akhshani A,Akhavan A,et al. Applications of tripled chaotic maps in cryptography[J]. Chaos,Solitons and Fractals,2007.DOI:10.1016/j.chaos.2007.08.013.

[92] Yen J C,Guo J I. A new image encryption algorithm and its VLSI architecture[C]//Proceedings of IEEE 1999 Workshop on Signal Processing Systems. Taipei:Omni Press,1999:430-437.

[93] Yen J C,Guo J I. Efficient hierarchical chaotic image encryption algorithm and its VLSI realization[C]//Proceedings of IEEE 2000 International Conference on Vision,Image and Signal Processing[S.l.]:Omni Press,2000:167-175.

[94] Yen J C,Guo J I. A new chaotic key-based design for image encryption and decryption[C]//Proceedings of IEEE 2000 International Symposium on Circuits and Systems (ISCAS 2000),Geneva,2000:49-52.

[95] Li Shu-jun,Zheng Xuan. Cryptanalysis of a chaotic image encryption method[C]//Proceedings of IEEE 2002 International Symposium on Circuits and Systems (ISCAS 2002),Phoenix-Scottsdale,AZ,USA,2002:708-711.

[96] Deergha Rao K,Gangadhar C. Modified chaotic key-based algorithm for image encryption and its VLSI realization[C]//IEEE Proceeding of the 2007 15th International Conference on Digital Signal Processing (DSP 2007),2007:439-442.

[97] Guan Zhi-hong,Huang Fangjun,Guan Wen-jie. Chaos-based image encryption algorithm[J]. Physics Letters A,2005,346:153-157.

[98] Wang Yuan-zhi,Ren Guang-yong,Jiang Ju-lang,et al. Image encryption method based on chaotic map[C]//IEEE 2007 Second IEEE Conference on Industrial Electronics and Applications,2007:2558-2560.

[99] Pareek N K,Patidar V,Sud K K. Image encryption using chaotic logisticmap[J]. Image and Vision Computing,2006,24(9):926-934.

[100] Li Chuan-mu,Hong Lian-xi. A new image encryption scheme based on hyperchaotic sequences[C]//IEEE International Workshop on Anti-counterfeiting,Security,Identification,2007:237-240.

[101] Behnia S,Akhshani A,Mahmodi H,et al. A novel algorithm for image encryption based on mixture of chaotic maps[J]. Chaos,Solitons and Fractals,2008,35(2):408-419.

[102] Kwok H S,Tang W K S. A fast image encryption system based on chaotic maps with finite precision representation[J]. Chaos,Solitons and Fractals,2007,32:1518-1529.

[103] Muhammad Asim,Varun Jeoti. On image encryption:comparison between AES and a novel chaotic encryption[C]//IEEE-ICSCN 2007,MIT Campus,Anna University,Chennai,India,2007:65-69.

[104] Ruanjan B. Novel public key encryption technique based on multiple chaotic systems[J]. Physics Review Letter,2005,26.

[105] 王开,裴文江,邹留华,等.一种多混沌系统公钥密码算法的安全性分析[J].物理学报,2006,55(12):6243-6247.

[106] Zhang Lin-hua. Cryptanalysis of the public key encryption based on multiple chaotic systems[J]. Chaos,Solitons & Fractals,2008,37(3):669-674.

[107] 于津江,曹鹤飞,许海波,等.复合混沌系统的非线性动力学行为分析[J].物理学报,2006,55(1):29-34.

[108] 甘建超,肖光赐.混沌的可加性[J].物理学报,2003,53(5):1085-1090.

[109] 刘金梅,丘水生,向菲,等.基于多混沌映射的信息加密算法[J].华南理工大学学报:自然科学版,2007(5):1-5.

(上接4页)

参考文献:

[1] Wiegand T,Sullivan G J. Overview of the H.264/AVC video coding standard[J]. IEEE Transactions on Circuits and Systems for Video Technology,2003,13(7):560-576.

[2] Draft ITU-T Recommendation and Final Draft International Standard of Joint Video Specification,ITU-T Rec. H.264-ISO/IEC 14496-10 AVC[S]. JVT-G050,Joint Video Team (JVT) of ISO/IEC MPEG and ITU-T VCEG,2003-05.

[3] Xin Jun,Vetro A. Fast mode decision for intra-only H.264/AVC coding[C]//Picture Coding Symposium (PCS),April 2006.

[4] Meng Bo-jun,Au O C,Wong C W,et al. Efficient intra-prediction algorithm in H.264[J]. IEEE,2003:837-840.

[5] 宋彬,周宁兆,常义林,等. H.264帧内预测快速算法[J].西安电子科技大学学报:自然科学版,2006,33(1):15-18.

[6] 贾克斌,谢晶,方晟. 一种基于自相关法的H.264/AVC高效帧内预测算法[J].电子学报,2006,34(1):152-154.

[7] 田川,王永生. H.264帧内预测编码模式选择的快速算法研究[J].计算机应用,2006,26(8):1860-1862.

[8] Kim C S,Li Qing,Kuo C C J. Fast intra-prediction model selection for H.264 codec[C]//SPIE International Symposium ITCOM 2003. Orlando,Florida:IEEE,July 2003.

[9] H.264/AVC reference software,JM10.2[EB/OL]. (2006-10-10). http:// iphome. hhi. de/suehring/tml/download/old_jm/.