一种提高通信安全性的混沌加密新方法

石凤良[1],祝玉华[1],赵宏微[2]
SHI Feng-liang[1],ZHU Yu-hua[1],ZHAO Hong-wei[2]

1.唐山师范学院 物理系,河北 唐山 063000
2.河北理工大学 理学院,河北 唐山 063000
1.Department of Physics,Tangshan Teachers College,Tangshan,Hebei 063000,China
2.Hebei Institute of Technology,Tangshan,Hebei 063000,China
E-mail:nami_zhu@163.com

SHI Feng-liang,ZHU Yu-hua,ZHAO Hong-wei.New chaotic encryption method to enhance communication security. Computer Engineering and Applications,2008,44(19):112-115.

Abstact: Bu and Wang ever put forward the way that using scalar signal to modulate the chaos carrier wave to enhance the security of the chaos secret communication,and defend the regression mapping attack of Preze and Cerdeira.Through transmission mode analysis of the Bu and Wang method,the authors discover the flaw of this method,i.e.,it can restore the parameter of the scalar signal from the modulation signal,and utilize the regression mapping to extract information from the demodulation chaos carrier signal.Therefore,in this paper the authors improve the Bu and Wang method,i.e.,increase a switching function that is bigger than 1 in the cryptograph.The numerical simulation of the generalized Rössler system indicates that the improved method can overcome the above flaw and enhance the communication security.

Key words: chaos carrier;regression mapping;secret communication;security

摘 要:Bu 和 Wang 曾提出利用标量信号调制混沌载波的方法,以提高混沌保密通信的安全性,并防御 Preze 和 Cerdeira 的回归映射攻击。通过对 Bu 和 Wang 方法的传输模式分析,发现了该方法的缺陷,即可从调制信号中恢复标量信号的参数,并利用回归映射从解调混沌载波信号中提取出消息。在此基础上改进了 Bu 和 Wang 的方法,即在密文中增加一个大于 1 的开关函数。通过对广义 Rössler 系统的数值模拟,表明改进方法既克服上述缺陷,又提高了通信的安全性。

关键词:混沌载波;回归映射;保密通信;安全性
DOI:10.3778/j.issn.1002-8331.2008.19.033 **文章编号**:1002-8331(2008)19-0112-04 **文献标识码**:A **中图分类号**:TP301.5

Internet 的迅猛发展极大地方便了信息交流,但是由于人们安全意识淡薄,信息泄漏现象时有发生。这就促使一些学者研究通信安全问题。1990 年,Corroll 和 Pecora 首次提出了混沌同步通信[1],从而激发了人们的研究兴趣,近年来混沌同步在保密通信中的应用已成为非线性科学中的研究热点[2-4]。混沌被认为是一种随机的、不可预测的现象,它具有初值敏感性、遍历性和伪随机性[5]。因此人们可利用混沌信号来隐藏明文信息,安全地传送密文信息,并基于这一新思路去建立混沌密码学[4]。目前,主要有三种混沌编码方案:混沌掩盖[6,7]、混沌健控[8]和混沌调制[9-11]。基于混沌调制方案,Liao 等考虑了扰动对同步性能的影响,并将其应用到混沌系统的保密通信当中,但它对混沌系统的非线性部分有着严格的限制条件[12];Feki 改进了 Liao 的方案,去掉了对混沌系统的非线性部分的限制条件,但所考虑的只是一个低维弱混沌系统[13];为防御 Preze 和Cerdeira 的回归映射攻击[14],Bu 和 Wang 提出了标量信号调制混沌载波的方法[15]。对于低维弱混沌系统,Short 指出,窃密者可以通过回归分析及神经网络拟合,近似地恢复传输信号的部分信息。因此系统的保密性很难保证[4]。为了提高系统的保密性,建议使用高维混沌或超混沌系统来代替低维弱混沌系统实现保密通信。本文分析了 Bu 和 Wang 方法的缺陷,并给出了一种新的改进方法,通过对高维广义 Rössler 系统的数值模拟,表明该方法既克服上述缺陷,又提高了通信的安全性。

1 利用广义 Rössler 系统的混沌调制法

Rössler 方程是 1976 年 Rössler 在研究具有中间产物的化学反应问题时,通过适当的标度变换,所给出的一个很简单的非线性常微分方程组[16]。目前人们对 Rössler 方程所产生的混沌已作了充分的研究,从而丰富了混沌理论[5]。作者认为若将 Rössler 方程进行推广,利用广义 Rössler 方程的混沌同步来进行保密通信,将大大提高保密通信的安全性。

基金项目:教指委教学研究基金(Teaching Foundation of Chinese Ministry of Education under Grant No.08031)。
作者简介:石凤良,男,副教授,研究方向:应用光学与计算方法;祝玉华,女,讲师,研究方向:纳米材料与计算方法;赵宏微,男,助教,研究方向:材料科学。
收稿日期:2008-03-21 **修回日期**:2008-06-16

考虑广义 Rössler 系统[17],令发送端系统和接收端系统分别为:

$$\begin{cases}\dot{x}_1=a_1x_2+a_2x_3\\ \dot{x}_2=a_3x_1+a_4x_2\\ x_3=a_5+a_6x_1x_3+a_7x_3\end{cases}\tag{1}$$

和:

$$\begin{cases}\dot{y}_1=a_1y_2+a_2y_3+h[s(\boldsymbol{x},t)-s(\boldsymbol{y},t)]\\ \dot{y}_2=a_3y_1+a_4y_2\\ \dot{y}_3=a_5+a_6y_1y_3+a_7y_3\end{cases}\tag{2}$$

这里 $\boldsymbol{x}(x_1,x_2,x_3)$、$\boldsymbol{y}(y_1,y_2,y_3)$为状态变量,$h$ 为耦合强度,$s(\boldsymbol{x},t)$为密文,$a_1,a_2,\cdots,a_7$ 为广义 Rössler 系统的内部参数。

通常取 $s(\boldsymbol{x},t)=x_1(t)$作为传输信号,它在混沌同步中扮演了双重角色:消息载波信号和混沌同步的驱动信号[14];相应取 $s(\boldsymbol{y},t)=y_1(t)$。Bu 和 Wang 选取调制混沌载波的标量信号为 $s(\boldsymbol{x},t)=g(t)x_1(t)=A\sin(\omega t+\varphi_0)x_3(t)x_1(t)$。对应地取 $s(\boldsymbol{y},t)=g(t)y_1(t)=A\sin(\omega t+\varphi_0)y_3(t)y_1(t)$($A$、$\omega$ 和 φ_0 均为常量)。外部参数 A、ω、φ_0 和系统内部参数 $a_1,a_2,\cdots,a_7$ 共同作为密钥。

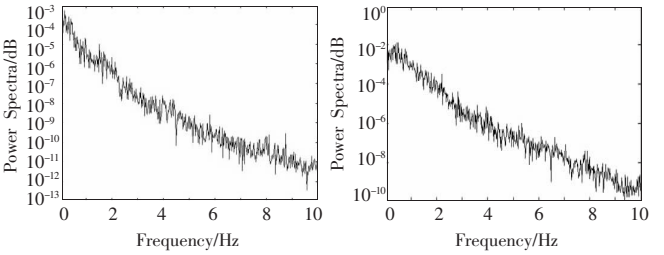
本文采用四阶 Runge-Kutta 法对式(1)和式(2)进行数值积分,选取时间间隔 $\Delta t=0.001$,得到 $\boldsymbol{x}(t)$和 $\boldsymbol{y}(t)$时间序列,作为分析系统行为的数据。

2　Bu 和 Wang 方法的缺陷分析

回归映射攻击的优点是执行简单且适用于不同的混沌保密通讯方案,其方法为:在不知道混沌系统参数、甚至混沌系统本身的条件下,即可根据混沌载波的局部最大值和局部最小值所产生的回归映射提取出消息[14]。暂不考虑传输信号 $s(\boldsymbol{x},t)=g(t)x_1(t)=A\sin(\omega t+\varphi_0)x_3(t)x_1(t)$的同步性能,这里首先分析外部参数 ω 和 φ_0 的安全性:在传输信号 $s(\boldsymbol{x},t)=g(t)x_1(t)=A\sin(\omega t+\varphi_0)x_3(t)x_1(t)$中由于包含了混沌信号 $x_3(t)x_1(t)$,因此 $s(\boldsymbol{x},t)$看起来是很复杂的,一般不能从 $s(\boldsymbol{x},t)$的功率谱中获得频率 ω。

为了检验能否从功率谱获得频率的 ω,利用 AR 参数模型法[18],选用 1 Hz 采样频率,分别计算了传输信号 $s(\boldsymbol{x},t)=x_1(t)$、混沌载波信号 $s(\boldsymbol{x},t)=A\sin(\omega t+\varphi_0)x_3(t)x_1(t)$的功率谱(图 1 所示)。分析中所用的参数为:FFT 长度 M:1 024;数据总量 N:10 000;阶次 p:220。从图 2 中不能获得频率 ω。但在下面的讨论中,将发现,采用自相关分析法可获得频率 ω 和 φ_0,并进一步获得消息的信息,这暴露了 Bu 和 Wang 方法的缺陷。

正弦信号 $A\sin(\omega t+\varphi_0)$的零点可揭示出频率 ω 和相位 φ_0 的信息(零点是指传输信号 $s(\boldsymbol{x},t)=0$ 的时间)。传输信号 $s(\boldsymbol{x},t)$的零点是由混沌信号 $x_3(t)x_1(t)$零点和正弦信号 $A\sin(\omega t+\varphi_0)$的零点组成;而正弦信号的零点时间是有周期性的,混沌信号的零点时间却无周期性。故提取正弦信号的零点时间变成从无序点集中找周期点的问题。这是模式识别中的一个典型问题,利用自相关分析的方法可以求出正弦信号的零点,进而提取出 ω 和 φ_0。可见外部参数 ω 和 φ_0 是不安全的。



(a)$s(x,t)=x_1(t)$　(b)$s(x,t)=A\sin(\omega t+\varphi_0)x_3(t)x_1(t)$

图 1　传输信号的功率谱

2.1　零输入模式分析

当消息信号 $i(t)=0$ 时,对于发送端系统式(1)和接收端系统式(2),给定系统的内部参数为:$a_1=-1$、$a_2=-1$、$a_3=1$、$a_4=0.2$、$a_5=0.2$、$a_6=1$ 和 $a_7=-4.7$(根据文献[17]可知此时广义 Rössler 系统是混沌的),给定外部参数为:$A=10.0$、$\omega=1.5$、$\varphi_0=0.0$,本文分析了 Bu 和 Wang 的零输入传输模式如图 2,发现了传输信号 $s(\boldsymbol{x},t)$在传输过程中潜在的信息暴露的问题。图 2(a)给出了当 $i(t)=0$ 时,传输信号 $s(\boldsymbol{x},t)$的部分曲线;图 2(b)为正弦信号 $\sin(\omega t+\varphi_0)$曲线,其中垂线代表零点位置;图 2(c)为 $s(\boldsymbol{x},t)/\sin(\omega t+\varphi_0)$的回归映射。

根据图 2(b),利用正弦信号 $\sin(\omega t+\varphi_0)$的周期零点可得出外部参数 ω 和 φ_0,同时也可重构出 $\sin(\omega t+\varphi_0)$。因为 $\sin(\omega t+\varphi_0)=0$ 的概率很小,故可由公式 $s(\boldsymbol{x},t)/\sin(\omega t+\varphi_0)$解调出混沌信号 $Ax_3(t)x_1(t)$。由图 2(c)可见,$s(\boldsymbol{x},t)/\sin(\omega t+\varphi_0)$的回归映射是由三个光滑且几乎不连续的片断组成。根据文献[14],两个修正的回归映射定义为:

$$A_n\rightarrow B_n:A_n=(X_n+Y_n)/2,B_n=X_n-Y_n,n=0,1,\cdots,N\tag{3}$$

及

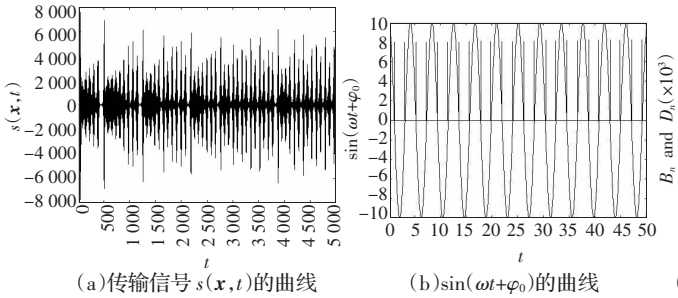
$$C_n\rightarrow D_n:C_n=(X_{n+1}+Y_n)/2,D_n=Y_n-X_{n+1},n=0,1,\cdots,N\tag{4}$$

这里 X_n 和 Y_m 分别表示传输信号 $s(\boldsymbol{x},t)$中的第 n 个局部最大值和第 m 个局部最小值。

发送端系统 $\boldsymbol{x}(t)$与接收端系统 $\boldsymbol{y}(t)$随时间变化的轨道误差为:

$$e(t)=\sqrt{\sum_i(x_i(t)-y_i(t))^2}\tag{5}$$

当 $\lim\limits_{t\to\infty}e(t)=0$ 时,发送端系统与接收端系统达到完全同步。由图 3 可见,利用传输信号 $s(\boldsymbol{x},t)=A\sin(\omega t+\varphi_0)x_3(t)x_1(t)$作为消息载波信号和混沌同步的驱动信号,在大约 $t=130$ s 时发送端系



(a)传输信号 $s(\boldsymbol{x},t)$的曲线　(b)$\sin(\omega t+\varphi_0)$的曲线　(c)$s(\boldsymbol{x},t)/\sin(\omega t+\varphi_0)$的回归映射

图 2　零输入传输模式分析图示

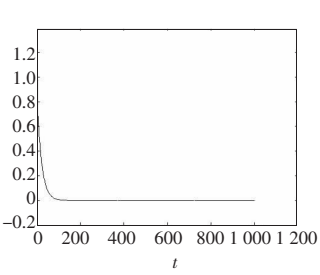


图 3　轨道误差 $e(t)$曲线

统和接收端系统达到同步。

2.2　非零输入传输模式分析

消息信号 $i(t)\neq 0$ 且为数字信号时，分析了 $s(\boldsymbol{x},t)=g(t)x_1(t)=A\sin(\omega t+\varphi_0)x_3(t)x_1(t)$ 的传输模式。选取内部参数为：$a_1=-1$、$a_2=-1$、$a_3=1$、$a_4=0.2$、$a_5=0.2$、$a_6=1$ 和 $a_7=-4.7$，外部参数为：$A=10.0$、$\omega=1.5$、$\varphi_0=0.0$，得出 $i(t)\neq 0$ 且为数字信号时传输模式的分析结果如图 4。图 4(a)为消息信号 $i(t)$ 曲线；图 4(b)为正弦信号 $\sin(\omega t+\varphi_0)$ 曲线，其中垂线代表零点位置；图 4(c)为 $s(\boldsymbol{x},t)/\sin(\omega t+\varphi_0)$ 的回归映射的吸引子。图 4(b)说明可利用正弦信号周期零点的方法获得信号的频率 ω 和相位 φ_0，从而重构出正弦信号 $\sin(\omega t+\varphi_0)$，再基于文献[14]中的方法，可以提取出消息。上述分析表明：Bu 和 Wang 方法对外部参数 ω、φ_0 仍然是不安全的，这种不安全性最终导致了信息的外泄。

当 $i(t)=0.1\sin(t)$ 时，传输信号 $s(\boldsymbol{x},t)=A[\sin(\omega t+\varphi_0)+1+f(t)]+i(t)$ 的吸引子如图 4(d)所示，由图 4(d)可见由于对传输信号进行了调制，回归映射的吸引子变得非常模糊，大大降低了从回归映射可能提取信息的几率。

3　改进方案

基于上述分析，发现消息被提取出来的主要的原因是：正弦信号的周期性零点。显然，提高通信安全性的最直接的方法就是消除周期性零点。为此对于由式(1)和式(2)定义的发送端、接收端动力系统，在发送端给定一个修正的传输信号如下：

$$s(\boldsymbol{x},t)=A[\sin(\omega t+\varphi_0)+1+f(t)]+x_3(t)x_1(t) \tag{6}$$

这里开关函数：

$$f(t)=\begin{cases}0.8, t\in[(2k+1)\pi,(2k+2)\pi]\\ 1.2, t\in(2k\pi,(2k+1)\pi)\end{cases}$$

相应地，在接收端有 $s(\boldsymbol{y},t)=A[\sin(\omega t+\varphi_0)+1+f(t)]y_3(t)y_1(t)$。可见 Bu 和 Wang 的方案是上述方案的特例。

当消息信号 $i(t)=0$，选取内部参数为：$a_1=-1$、$a_2=-1$、$a_3=1$、$a_4=0.2$、$a_5=0.2$、$a_6=1$ 和 $a_7=-4.7$，外部参数为：$A=10.0$、$\omega=1.5$、$\varphi_0=0.0$，耦合强度 $h=10$，样本间隔 $\Delta t=0.001$ 时，改进方案的数字模拟如图 5 所示。图 5(a)为明文 $i(t)$ 的曲线，图 5(b)为 $A[\sin(\omega t+\varphi_0)+1+f(t)]$ 曲线。图 5(b)与图 4(b)比较，可见当添加(1+$f(t)$)后可发现要从图中抽取其周期非常困难，几乎是不可能的。图 5(c)为同步误差 $e(t)=x_1(t)-y_1(t)$ 的曲线，从图中可看到获得相当多同步的值，与老的方案相比，该改进方案还增强了混沌同步性。图 5(d)是当 $i(t)=0.1\sin(t)$ 时，信号 $s(\boldsymbol{x},t)=A[\sin(\omega t+\varphi_0)+1+f(t)]x_3(t)x_1(t)+i(t)$ 的图形，基本不能从调制后的传输信号中获得频率 ω，保证了传输的安全性。

为了检验能否从功率谱图中获得信号的频率 ω。利用 AR 参数模型法[18]，选用 1 Hz 采样频率，计算了 $s(\boldsymbol{x},t)=A[\sin(\omega t+\varphi_0)+1+f(t)]x_3(t)x_1(t)$ 的功率谱(图 6 所示)。分析中所用的参数为：FFT 长度 M：1 024；数据总量 N：10 000；阶次 p：220。观察图 6，可见不能从功率谱图中获得信号的频率 ω，这也表明本文改进方案的正确性。

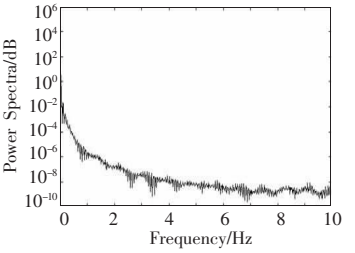


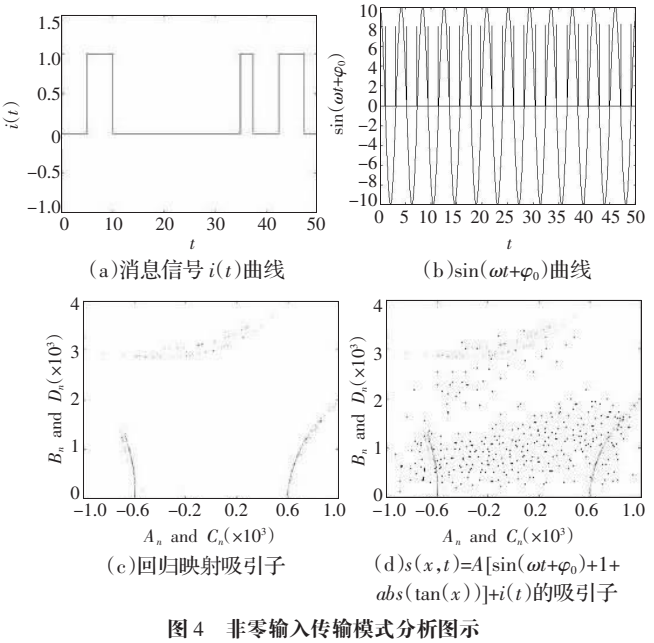
图 6　改进方案传输信号的功率谱

下面分析耦合强度 h，从式(1)和式(2)可推出耦合强度 h 为：

$$h=\frac{[y_1(t+1)-y_1(t)]/\Delta t-\delta(y_2(t)-y_1(t))}{s(x,t)-s(y,t)} \tag{7}$$

式中 t 为循环次数，Δt 为时间间隔，$s(\boldsymbol{x},t)=\sin(\omega t+\varphi_0)x_3(t)x_1(t)$，$s(\boldsymbol{y},t)=\sin(\omega t+\varphi_0)y_3(t)y_1(t)$。

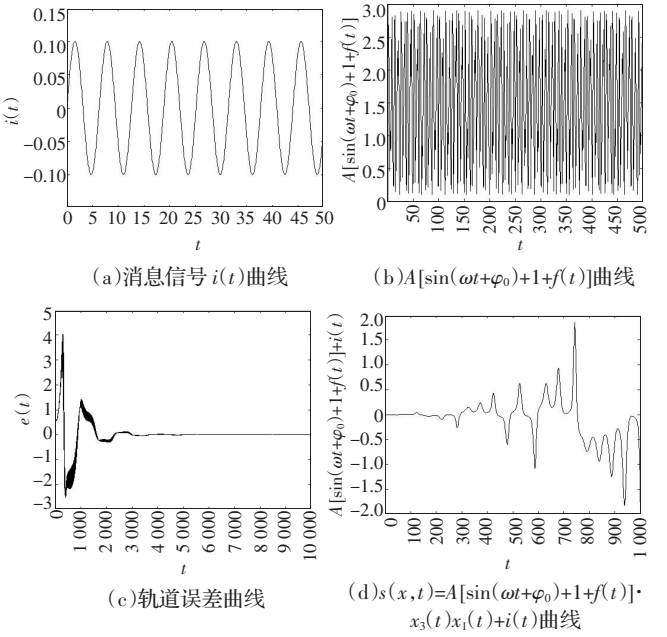
进一步的数值分析可发现，在 Bu 和 Wang 的方案中，同步系统耦合强度的范围非常窄，事实上，仅有有限的值能获得同步。但在改进的方案中，通过增加(1+$f(t)$)项，使得耦合强度的范围变宽。当 $1+f(t)\geqslant 1.2$ 时，同步系统耦合强度的范围大约位于 $1<h<60$，改进的方案不但克服了 Bu 和 Wang 方案的缺陷，同时也增强了通信的同步性能。更重要的是使得该系统的稳定性增强。



(a)消息信号 $i(t)$ 曲线　(b)$\sin(\omega t+\varphi_0)$ 曲线

(c)回归映射吸引子　(d)$s(x,t)=A[\sin(\omega t+\varphi_0)+1+abs(\tan(x))]+i(t)$ 的吸引子

图 4　非零输入传输模式分析图示



(a)消息信号 $i(t)$ 曲线　(b)$A[\sin(\omega t+\varphi_0)+1+f(t)]$ 曲线

(c)轨道误差曲线　(d)$s(x,t)=A[\sin(\omega t+\varphi_0)+1+f(t)]\cdot x_3(t)x_1(t)+i(t)$ 曲线

图 5　改进方案的传输模式分析图示

4 结论

Bu 和 Wang 提出了一个简单的改进混沌同步系统安全性的方法，认为已消除了发送端动力系统的相空间重构的可能性,并且断言不能从功率谱中获得频率 ω。但是利用正弦信号的周期零点不但获得了 ω 和 φ_0 而且还能重构出正弦信号,并最终导致消息的泄漏。为此,提出了一种改进的方案,实验证明:该改进方案克服了上述缺陷,增强了通信的安全性。

但同时也存在尚需改进的地方,如:如何设计一个更安全的保密方案;通常高维混沌要比低维混沌具有更高的安全性,可设计一个超混沌的保密系统；如何使得耦合强度的范围变得更宽等。此外,由于数字水印、数字签名、信息隐藏等保密技术的不断成熟,可以考虑把这些加密技术应用到上述系统中:利用数字签名技术保证信息传输过程中的信息的完整性，利用数字水印技术来保护数字产品的版权，而信息隐藏则常常与水印技术结合使用,达到保护信息的目的等等,来进一步提高通信的安全性。

参考文献:

[1] Carroll T L,Pecora L M.Synchronizing chaotic circuits[J].IEEE Transactions on Circuits and Systems,1991,38(4):453-456.

[2] Chen G,Dong X.From chaos to order:methodologies,perspectives and applications[M].Singapore: World Scientific,1998.

[3] 王光瑞,于熙龄,陈式刚.混沌的控制、同步与利用[M].北京:国防工业出版社,2001.

[4] 关新平,范正平,陈彩莲,等.混沌控制及其在保密通信中的应用[M].北京:国防工业出版社,2002.

[5] 王兴元.复杂非线性系统中的混沌[M].北京:电子工业出版社,2003.

[6] Kocarev L,Halle K S,Eckert K,et al.Experimental demonstration of secure communications via chaotic synchronization[J].International Journal of Bifurcation and Chaos,1993,2(3):709-713.

[7] Cuomo K M,Oppenheim A V,Strogatz S H.Synchronization of lorenzed-based chaotic circuits with applications to communications[J].IEEE Transactions on Circuits and Systems-II,1993,40(10):626-633.

[8] Dedieu H,Kennedy M P,Hasler M.Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuit[J].IEEE Transactions on Circuits and Systems-II,1993,40(10):634-642.

[9] Halle K S,Wu C W,Itoh M,et al.Spread spectrum communications through modulation of chaos[J].International Journal of Bifurcation and Chaos,1993,3(1):469-477.

[10] Itoh M,Murakami H.New communication systems via chaotic synchronizations and modulations[J].IEICE Transactions on Fundamentals of Electronics Communications & Computer Sciences,1995,78(3):285-290.

[11] Itoh M,Wu C W,Chua L O.Communication systems via chaotic signals from a reconstruction viewpoint[J].International Journal of Bifurcation and Chaos,1997,7(2):275-286.

[12] Liao T L,Huang N S.An observer-based approach for chaotic synchronization with applications to secure communications[J].IEEE Transactions on Circuits and Systems,1999,46(9):1144-1150.

[13] Feki M.An adaptive chaos synchronization scheme applied to secure communication[J].Chaos,Solitons and Fractals,2003,18(1):141-148.

[14] Perez G,Cerdeira H A.Extracting messages masked by chaos[J].Physics Review Letter,1995,74:1970-1973.

[15] Bu Shou-liang,Wang Bing-hong.Improving the security of chaotic encryption by using a simple modulating method[J].Chaos,Solitons & Fractals,2004,19(4):919-924.

[16] Rössler O E.An equation for continuous chaos[J].Physics Letter A,1976,57:397-398.

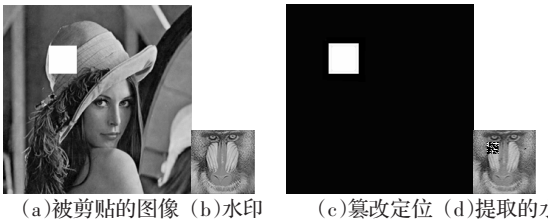
[17] 王兴元.构造广义 Rössler 奇怪吸引子的一种新方法[J].东北大学学报:自然科学版,2001,22(3):261-264.

[18] Marple S L.A new autoregressive spectrum analysis algorithm[J].IEEE Trans on Acoustic,Speech and Signal Processing,1980,28(3):441-454.

(上接 99 页)

图像操作时,水印都表现出比较高的脆弱性。

为了检测算法对图像篡改的定位能力,将嵌入水印后的图像进行局部的篡改。具体方法是将图像进行剪切和替换处理,对篡改图像进行水印提取,并和原始水印进行比较,如图 2 所示,图中白色代表差别。实验表明,算法对图像的篡改具有较好的定位能力。



(a)被剪贴的图像 (b)水印 (c)篡改定位 (d)提取的水印

图 2 剪切定位

3 结论

提出一种基于空间分解的脆弱水印嵌入与提取算法,并进行了仿真实验,验证了所提出的水印算法的脆弱性,同时水印提取不需要原始图像,实现了盲提取,提高了水印算法的安全性。实验结果表明,算法除可以鉴别图像是否被篡改外,还可以报告图像在空间域中被篡改的位置。

参考文献:

[1] 宋玉杰,谭铁牛.基于脆弱性数字水印的图像完整性验证研究[J].中国图象图形学报,2003,8(1):1-4.

[2] 杨以先,钮心忻.数字水印理论与技术[M].北京:高等教育出版社,2006.

[3] 孙圣和,陆哲明,牛夏牧.数字水印技术及应用[M].北京:科学出版社,2004.

[4] 李东勤,林克正,李昭华.一种基于小波的脆弱水印算法[J].哈尔滨理工大学学报,2006,11(5):24-27.

[5] Tzeng J,Hwang W L,Chern I L.Enhancing image watermarking methods with/with out reference images by optimization on second-order statistics [J].IEEE Transactions on Image Processing,2002,11(7):771-783.

[6] Tzeng J,Hwang W L,Chern I L.An asymmetric subspace watermarking method for copyright protection[J].IEEE Transactions on Signal Processing,2005,53(2):784-792.

[7] Liu Fen-lin,Gao Shan-qing,Ge Xin.A scheme of fragile watermarking based on SVD and 2D chaotic mapping [J].Journal of Shanghai Jiaotong University,2006,11(2):146-151.

[8] Jia Pei-hong,Chen Yun-zhen,Ma Jin-song.Digital watermark-based security technology for geo-spactial graphics data[J].Chinese Geographical Science,2006,16(3):276-281.

[9] 张贤达.矩阵分析[M].北京:清华大学出社,2004.