一种新的超混沌序列生成方法及应用*

田 澈, 卢辉斌, 张 丽
(燕山大学 信息科学与工程学院 电子通信系, 河北 秦皇岛 066004)

摘 要: 为解决传统低维二进制混沌序列作为伪随机序列来源而随机性不理想、动力学特性易退化的问题,利用四阶 CNN 细胞神经网络超混沌系统的四路实数值序列进行比较,生成一种新的四进制超混沌序列,并应用于数字签名算法和数据摘要算法。仿真结果表明,新的超混沌序列的随机性优于传统的二进制混沌序列,能够通过"一次一密"实现复杂网络环境中的快速加密数据传输,克服现有多种加密算法已被破译的问题。

关键词: 四进制; 超混沌序列; 随机性分析; 加密算法; 数据摘要算法
中图分类号: TP311.56 **文献标志码**: A **文章编号**: 1001-3695(2012)04-1405-04
doi:10.3969/j.issn.1001-3695.2012.04.057

New family of hyperchaotic sequences generator and application

TIAN Che, LU Hui-bin, ZHANG Li
(*Dept. of Electronics & Communication, Institute of Information Science & Engineering, Yanshan University, Qinhuangdao Hebei* 066004, *China*)

Abstract: As a new rich source of pseudo-random coding, the random property and dynamical degradation of low-dimensional binary chaotic sequences were non-ideal. Recently, several encryption and message digest algorithms have been deciphered. In order to solve these problems, it proposed an enhanced quaternary hyperchaotic sequence by comparing the four real-valued sequences of fourth-order CNN(cellular neural networks) hyperchaotic system. It proved that the random of quaternary hyperchaotic sequences was superior to the traditional binary chaotic sequences. Simulation results show the feasibility of the encryption algorithm and message digest algorithm in solving "one-time pad", rapid authentication and encrypted data transmission with complex network environment.

Key words: quaternary; hyperchaotic sequence; random analysis; encryption algorithm; message digest algorithm

信息时代,人们在方便、快捷地交换各种信息的同时,只有在安全通信的网络环境下才能有效地开放和共享各种网络资源。按照香农的密码学理论,"一次一密"(one-time pad)的加密系统是绝对安全的,口令一次一变,无法预测和跟踪,难以窃取。根据混沌系统的特性,把混沌序列作为随机密钥永远不会重复,并产生与明文无任何统计关系的随机输出,这种设计方案在理论上是不可破的。

对于混沌序列的应用,关键在于对其动力学特性进行极度精准的控制。然而在实际应用中,混沌系统依靠计算机的有限精度数字化系统运行,不可避免地出现混沌的动力学特性退化,特别是低维混沌系统,可能退化为周期序列,密码学特征难以控制。近期研究结果表明,用相空间重构技术,可以推测出低维混沌系统的性质与特征,恢复出原低维混沌加密系统,从而从密文中部分地解密出明文。但这严重影响了混沌序列密码的安全性[1~6]。因此,如何克服低维混沌序列随机性不理想、动力学特性易退化的问题,已经成为混沌首次应用于密码学以来最重要的问题。

文献[7]采用多级混沌映射交替变参数的伪随机序列产生方法,文献[8]将多个混沌模型耦合,文献[9]对常见的 Logistic 映射进行改进,构造了新的映射函数来产生混沌序列,克服了序列有限精度效应的影响。这些通过改变常用混沌映射来构造新的混沌系统的方法,常常需要对原有的混沌系统方程进行升维或升级,大大增加了混沌映射的计算量和复杂度,使混沌序列的理论分析和实际应用更加困难。

要增强系统的抗破译能力,采用具有多个正性 Lyapunov 指数的超混沌系统和随机性能更好的序列生成算法是行之有效的解决方法。本文以超混沌系统为基础,设计产生一种新的四进制超混沌序列,并应用于目前在电子商务、电子政务领域广泛使用的数字签名和数据摘要算法中,以实现复杂网络环境中的快速加/解密和保密数据传输,克服现存密码体系中加/解密速度慢和密文易破译的缺点。

1 四进制超混沌序列的生成

1.1 CNN 超混沌系统的仿真

超混沌系统是具有两个或两个以上正的 Lyapunov 指数的高维混沌系统,具有更加复杂的动力学行为。细胞神经网络(CNN)易于用超大规模集成电路实现,在图像处理方面也得到了广泛应用。适当选取系统参数,四阶全互连细胞神经网络系统的状态方程[10]可写为

收稿日期: 2011-09-29; **修回日期**: 2011-10-30 **基金项目**: 国家自然科学基金资助项目(61074195); 南京大学计算机软件新技术国家重点实验室资助项目(KFKT2011B23)

作者简介: 田澈(1977-),女,河北秦皇岛人,讲师,硕士,主要研究方向为保密通信、混沌系统控制(ysutc@ysu.edu.cn); 卢辉斌(1964-),男,教授,博士,主要研究方向为信息安全; 张丽(1989-),女,硕士研究生,主要研究方向为数字信号处理.

$$\begin{cases} \dot{x}_1 = -x_3 - x_4 \\ \dot{x}_2 = 2x_2 + x_3 \\ \dot{x}_3 = 14x_1 - 14x_2 \\ \dot{x}_4 = 100x_1 - 100x_4 + 100(|x_4 + 1| - |x_4 - 1|) \end{cases} \tag{1}$$

在 $x_1(0) = x_2(0) = x_3(0) = x_4(0) = 0.5$，仿真时间为 50 s 的初始条件下，得到 x_1-x_2、x_3-x_4 平面的混沌吸引子图如图 1、2 所示。

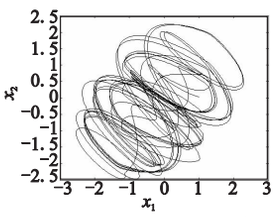

图1 x_1-x_2平面吸引子图

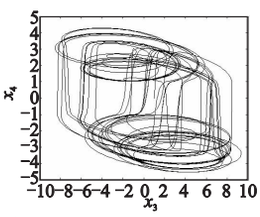

图2 x_3-x_4平面吸引子图

1.2 二进制超混沌序列的生成

在 $x_1(0) = x_2(0) = x_3(0) = x_4(0) = 0.5$，仿真时间为 200 s 的初始条件下，CNN 系统通过迭代运算 1 000 次，可以得到 4 个离散的实数值超混沌序列 $A_1: \{a_{11}, a_{12}, \cdots, a_{1n}\}$；$A_2: \{a_{21}, a_{22}, \cdots, a_{2n}\}$；$A_3: \{a_{31}, a_{32}, \cdots, a_{3n}\}$；$A_4: \{a_{41}, a_{42}, \cdots, a_{4n}\}$。为统一实数序列的值域，只截取 4 个实数值超混沌序列的小数部分，定义为序列 $X_1: \{b_{11}, b_{12}, \cdots, b_{1n}\}$；$X_2: \{b_{21}, b_{22}, \cdots, b_{2n}\}$；$X_3: \{b_{31}, b_{32}, \cdots, b_{3n}\}$；$X_4: \{b_{41}, b_{42}, \cdots, b_{4n}\}$。

$$\begin{cases} X_1 = (A_1 - [A_1]) \\ X_2 = (A_2 - [A_2]) \\ X_3 = (A_3 - [A_3]) \\ X_4 = (A_4 - [A_4]) \end{cases} \tag{2}$$

其中：[ ]表示取整数部分；$X_1, X_2, X_3, X_4 \in (0,1)$。

定义阈值函数 sign 为

$$\text{sign}(X_i) = \begin{cases} 0 & b_{ij} < T \\ 1 & b_{ij} \geqslant T \end{cases} \tag{3}$$

则 $x_i: \{x_i = \text{sign}(X_i)\}$ 即为量化后得到的二进制 CNN 超混沌序列。其中：$i = 1,2,3,4$；$j = 1,2,\cdots,n$；T 为平均值。

以序列 x_1 为例，经过数据统计可知，阈值 $T = 0.1583$，则序列 x_1 的折线图如图 3 所示。文献[11]提出混沌序列非线性离散化算法及改进算法，并基于一维 Logistic 系统生成二值序列。现给出一种基于 CNN 超混沌系统的两路实值序列 X_1、X_2，生成二进制超混沌序列的算法。定义二进制超混沌序列 $k: \{k_1, k_2, \cdots, k_n\}$ 为

$$k_j = \begin{cases} 0 & b_{1j} < b_{2j} \\ 1 & b_{1j} \geqslant b_{2j} \end{cases} \tag{4}$$

其中：$j = 1,2,\cdots,n$。在相同的初始条件下，CNN 系统迭代运算 1 000 次，得到序列 k 的折线图如图 4 所示。

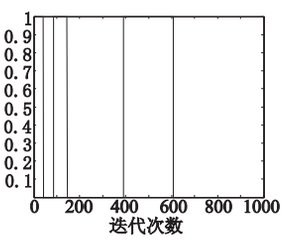

图3 序列x_1的折线图

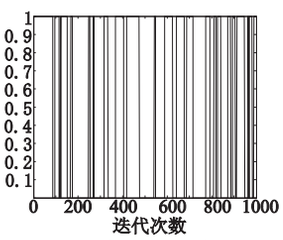

图4 序列k的折线图

1.3 四进制超混沌序列的生成

相同的初始条件，$x_1(0) = x_2(0) = x_3(0) = x_4(0) = 0.5$，仿真时间为 200 s，CNN 系统迭代 1 000 次。对归一化的 4 个实数值序列 $X_1: \{b_{11}, b_{12}, \cdots, b_{1n}\}$；$X_2: \{b_{21}, b_{22}, \cdots, b_{2n}\}$；$X_3: \{b_{31}, b_{32}, \cdots, b_{3n}\}$；$X_4: \{b_{41}, b_{42}, \cdots, b_{4n}\}$，定义四进制超混沌序列 $q: \{q_1, q_2, \cdots, q_n\}$ 为

$$q_j = \begin{cases} 11 & b_{1j} > b_{2j} \text{且} b_{3j} > b_{4j} \\ 10 & b_{1j} > b_{2j} \text{且} b_{3j} \leqslant b_{4j} \\ 01 & b_{1j} \leqslant b_{2j} \text{且} b_{3j} > b_{4j} \\ 00 & b_{1j} \leqslant b_{2j} \text{且} b_{3j} \leqslant b_{4j} \end{cases} \tag{5}$$

其中：$j = 1,2,\cdots,n$。得到序列 q 的折线图如图 5 所示。

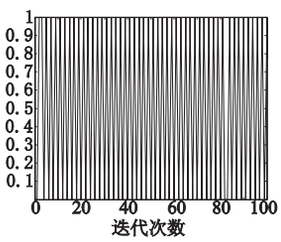

图5 四进制序列q的折线图

1.4 四进制超混沌序列的随机性分析

为确保四进制超混沌流密码序列的随机性，采用以下几种随机性检测方法。在检测中，序列长度取 $n = 20\,000$ 位，结果取 1 000 个由不同初始密钥生成的混沌密钥序列的测试平均值。此外，设检验的显著性水平不大于 5%。

(1)频数检验：随机序列，应保证序列中的 0 和 1 的数目大致相等，体现均匀分布的特性。设序列中 0 的个数为 n_0，1 的个数为 n_1，计算检验统计量 $\eta = (n_0 - n_1)^2/n$。

由于样本的自由度为 1，且自由度为 1 显著性水平为 5% 的 χ^2 分布的值 $\chi_5^2(1) = 3.841$，所以只要 $\eta \leqslant 3.841$，在本例中当 $9\,725 < n_1 < 10\,275$ 时，则通过测试。

(2)序列检验：令 m 为一个正整数，将序列分成[n/m]个不重叠的段，每段长是 m。对于随机序列，m 位子序列的每一种模式的出现概率是均等的。序列检验就是用来检测每种模式的出现概率是否大致相等。本例中 20 000 位随机序列按 $m = 4$分成 5 000 组，每组有 16 种可能取值。设 $f(i)$ 为取值为 i 的组数，$i \in [0,15]$。计算检验统计量：

$$\eta = 16\left(\sum_{i=0}^{15}[f(i)]^2\right)/5000 - 15 \tag{6}$$

则当 $2.16 < \eta < 46.17$ 时通过检验。

(3)游程检验：游程是序列的一个子串，由连续元素组成，且其前导和后继元素都与该元素不同。

一个游程定义为连续为 0 或 1 的最大位序列，其中 0 或 1 的个数称为游程长度。一个长度为 n 的随机序列中，长度为 i 的游程(0 或 1 游程)出现的次数应该为 C_i，则游程总数 $C = \sum C_i$。对于长度为 n 的 q 元随机序列，游程总数的数学期望为 $E(C) = (q-1)n/q$。

序列的游程总数越接近于期望值，则该序列的随机性就越好。对于 $D = |(C - E(C))/E(C)|$，D 的值越小，则序列的随机性越好。本例中二进制序列的 $D_2 = 0.8324\%$，四进制序列的 $D_4 = 0.2102\%$。

表 1 为测试结果对比数据。从图 3 ~ 5 及表 1 可以看出,二进制超混沌序列中,0 和 1 的个数相差较多,致使随机序列的平衡性较差,且 0 和 1 的游程长度都较长,长游程的位数较多。在相同条件下生成的四进制序列相对于二进制序列,0 和 1 的分布更加密集,更加均衡,长游程更少,基本符合越短的游程个数越多;随着游程长度增加,游程个数减少这个一般规律,所以四进制序列相对于二进制序列的随机性能更加优越。

表 1　测试结果对比数据

比较项目	二进制	四进制	比较项目	二进制	四进制
20000 位中的 0 数	10155	9992	游程为 3 的 1 数	46	178
20000 位中的 1 数	9845	10008	游程为 4 的 0 数	48	121
序列检验($m=4$)	13.2944	1.4832	游程为 4 的 1 数	59	128
游程为 1 的 0 数	51	5097	游程为 5 的 0 数	52	120
游程为 1 的 1 数	46	5112	游程为 5 的 1 数	60	114
游程为 2 的 0 数	43	72	游程大于 6 的 0 数	597	328
游程为 2 的 1 数	50	71	游程大于 6 的 1 数	577	320
游程为 3 的 0 数	47	186			

(4)相关性分析:按照 Golomb 对伪随机序列提出的三个公设,理想的超混沌序列应具有如下的统计特性:均匀分布,自相关是 δ 函数,互相关是零。

截取相关间隔为 - 10 000 ~ 10 000,由式(5)生成的四进制超混沌序列 q 的自相关及互相关函数曲线如图 6 和 7 所示。

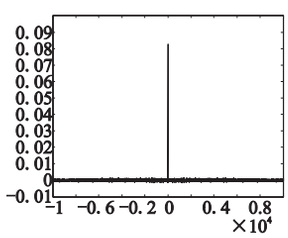

图6　四进制超混沌序列q的自相关曲线

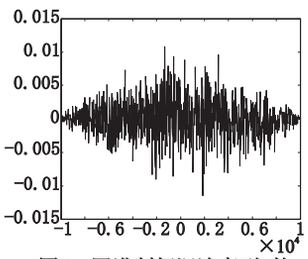

图7　四进制超混沌序列q的互相关曲线

由图 6、7 可见,四进制超混沌序列的生成算法能够很好地消除混沌序列自身相邻元素之间的相关性,在不增加比较次数的情况下,具有很好的随机分布规律。

2　四进制 CNN 超混沌序列的应用

目前,用于保障 Internet 上数据传输安全的 HTTPS(secure hypertext transfer protocol)安全超文本传输协议内置于浏览器中,实际上应用了 Netscape 公司的安全套接字层(SSL)作为 HTTP 应用层的子层,已被广泛用于复杂网络环境中 Web 浏览器或客户端与服务器之间的身份认证和加密数据传输,如银行等金融机构的交易支付、电信运营商 SSL VPN 业务、企业内联网、政府部门等。目前密钥长度限制在 40 位,美国已推出 128 位密钥,但限制出境。

SSL 提供多种对称、非对称加密算法及信息摘要算法。目前最强的方案是使用三个独立密钥的三重 DES 加密数据,并用 SHA-1 保护数据完整性。这种方案的速度相对较慢,主要用于银行及其他对安全性要求较高的应用[12]。

然而 DES、RSA、MD5 及 SHA-1 等过去被认为足够安全的算法均已被破译,且在安全性与加密速度等性能的取舍上存在矛盾[13]。目前,作为对称密钥算法首选的 AES 算法将数据分为 128 位的数据块,最多使用 128 位密钥,对明文长度和密钥空间均有限制。AES 与 DES 一样,本质上是使用极大字符的单字母表置换密码算法,只是 AES 为 128 位,DES 为 64 位。任何时候,当同样的密文用同样的 AES 密钥加密时会得到同样的密文。入侵者可利用固定的数据长度和同样的密文等特性攻破 AES 加密系统[14]。因此,研究更为安全高效的算法及方案是非常必要的。

由以上的分析可以看出,四进制超混沌序列的生成算法本质是一种新的二进制超混沌序列的优化算法。作为“一次一密”的流密码,具有传统流密码和对称加密算法无法比拟的优越性,表现为:理论上无穷大的密钥空间、对明文长度没有限制、优越的随机性和单向性。可将四进制超混沌序列应用于“一次一密”的数字签名和数据摘要。

2.1　带有数据摘要的数字签名

2.1.1　密钥生成

(1)输入明文:如中文“床前明月光,疑是地上霜。举头望明月,低头思故乡。”对输入明文进行数字化处理为 $m_i(i=1,2,\cdots,L)$,可知数据源长度为 $L=768$ 位。

(2)服务器向客户端发送一个证书,包含一组不同时为 0 的随机数 $\{x_1(0),x_2(0),x_3(0),x_4(0),R\}$。

在 $x_1(0)=x_2(0)=x_3(0)=x_4(0)=0.5$,仿真时间为 200 s 的初始条件下,CNN 系统去掉前 500 个不稳定点,按式(5)生成四进制超混沌序列。从第 501 位开始截取 768 位预设主密钥,其中,前 384 位为 111111101010101011111111111010101010111111111111010101010101111111111111100000000000000000101010101010101010101010101010101010101010000001010111010101111010111010101010111010101010101110101010101011111010000001010101010100000001010101111010101010101111010101010101010101010100000001010101000001010000000010110011010011010010101011001011001100110100110010101010101010101101001010101100101010101。

(3)用于加密数据的实际会话主密钥是从预设主密钥和随机数推导而来的。按采样间隔 $R=4$,在预设主密钥中跳跃取值生成 128 位主密钥:01101001011001100101010101101001010101010101100101010101010101010110010110101010010101010110010011001100101001100101100110010101011010101001。

2.1.2　基于四进制 CNN 超混沌序列生成单向散列值

(1)从上节生成的 CNN 四进制超混沌序列的第 2001 位开始按照明文的长度 $L=768$ 顺次截取序列值 $k_i(i=1,2,\cdots,L)$,与明文 $m_i(i=1,2,\cdots,L)$ 进行逐位异或运算:$k_i \oplus m_i = P_i$。

(2)将 L 位的 C_i 逐位做异或,得到 1 位二进制数。

(3)将步骤(1)(2)循环执行 128 次,得到 128 位的序列 Q_j $(j=1,2,\cdots,128)$。

(4)为防止出现连续“1”或连续“0”过多,对 Q_j 按奇数位不变、偶数位取反,得到 128 位单向散列值数据摘要,其字符形式为:? XR↑? àó? íM · 3? 0??。

2.1.3　数字签名

将数据摘要用 128 位的主密钥进行签名,即将 128 位的单向散列值和 128 位的四进制超混沌密码序列流进行逐位的异或运算,得到数字签名的字符形式为: >? =S×¬┤? =Q? ^?? ↑,是一串无意义的字符。

将数字签名和明文组成的序列与长度为(128 + L)的四进制超混沌密码序列流进行逐位的异或运算,得到密文的字符形式为:?? 3? 6??:(dW┬×??? Z;? ¶o? o? =?? >??? 4? ú⌊??? /⌊~? ┤? ┤? C? oèo? 1? 0o? <2? (?!!? ?? 0┤-┤/┤.?? · <??;? 0?⌊? 1┤? G? o¨? 2?.??? =┤ù┤n? C? o? o? >°~? ⌉? -?!! ⌈┤⌈C??,;o,´- + =¶? O ? S×?.? #?;⌊? 2? ┤Q?? P×R? ¶o×.? ù-? ⌈?? =@???<? 1? (oü2ü.? n? · ? · ? · o,是一串无意义的字符。

2.1.4 解密及验证

接收方根据通信密钥,产生与发送方相同的四进制超混沌序列,与接收到的密文逐位地异或运算,即可解密,其中前 128 位为带有数据摘要的数字签名,后 L 位为明文原文。

对解密后的明文进行散列运算,形成的数据摘要与解密得到的数据摘要相同,则为正确接收。经汉字区位转换得:床前明月光,疑是地上霜。举头望明月,低头思故乡。

同时,由于混沌系统的初值敏感性,加/解密需保持严格的同步,因此通信双方还应交换相应的同步信息。

2.2 性能分析

CNN 超混沌系统结构较低维混沌系统复杂,系统的四个初始值、多个参数和采样间隔均可作为生成加密混沌序列的种子密钥,其中任一个推测错误都无法复原序列。通信成功后,服务器自动废除本次所用密钥,更新出新的密钥数据,实现“一次一密”。由于超混沌序列的随机性和复杂性,窃取者伪造密钥的可能性基本为零。混沌密钥的选取空间无限,不受密钥长度限制。密钥的生成和加/解密过程仅进行简单的数学运算,占用系统资源少,运算速度快。

基于四进制 CNN 超混沌序列生成的单向散列值,对数据的长度没有限制,无须分成固定长度的数据块;算法简单,运算速度快,可以生成任意长度的散列值;由于超混沌序列特有优越的随机性和初值敏感性,可以保护数据的完整性,防止窜改。

3 结束语

本文基于 CNN 超混沌系统分别生成了二进制和四进制超混沌序列,通过对四进制序列进行频数检验、序列检验、游程检验和相关性分析,证明了四进制混沌序列的随机性优于传统的二进制混沌序列。在此基础上,设计了一种四进制 CNN 超混沌序列在密钥的生成、加密算法和数据摘要算法中的应用方案。仿真结果表明,该方案能够实现复杂网络环境中的快速验证和加密数据传输,克服 DES、RSA、MD5 及 SHA-1 等算法已被破译的现状,具有一定的实用推广价值。

参考文献:

[1] MASUDA N, AIHARA K. Dynamical characteristics of discretized chaotic permutations[J]. International Journal of Bifurcation and Chaos, 2002, 12(10): 2087-2103.

[2] WANG Xing-yuan, WANG Xiao-juan, ZHAO Jian-feng, *et al*. Chaotic encryption algorithm based on alternant of stream cipher and block cipher[J]. Nonlinear Dynamics, 2011, 63(4): 587-597.

[3] LIU Shu-bo, SUN Jing, XU Zheng-quan, *et al*. Digital chaotic sequence generator based on coupled chaotic systems[J]. Chinese Physics B, 2009, 12(18): 5219-5227.

[4] ZHANG Yi-wei, WANG Yu-min, SHEN Xu-bang. A chaos-based image encryption algorithm using alternate structure[J]. Science in China Series F: Information Sciences, 2007, 50(3): 334-341.

[5] 王继志,王英龙,王美琴. 一类基于混沌映射构造 hash 函数方法的碰撞缺陷[J]. 物理学报, 2006, 55(10): 5048-5054.

[6] MATFHEWS R. On the derivation of a chaotic encryption algorithm [J]. Cryptologia, 1989, 13(1): 29-42.

[7] 李孟婷,赵泽茂. 一种新的混沌伪随机序列生成方法[J]. 计算机应用研究, 2011, 28(1): 341-344.

[8] FEI Peng, QIU Shui-sheng, MIN Long. An image encryption algorithm based on mixed chaotic dynamic systems and external keys[J]. IEEE Trans on Circuits Systems, 2005, 46(5): 1135-1139.

[9] 张雪峰,范九伦. 一种新的分段非线性混沌映射及其性能分析[J]. 物理学报, 2010, 59(4): 2298-2304.

[10] 蒋国平,王锁萍. 细胞神经网络超混沌系统同步及其在保密通信中应用[J]. 通信学报, 2000, 9(2): 79-85.

[11] 赵莉,张雪锋,范九伦. 一种改进的混沌序列产生方法[J]. 计算机工程与应用, 2006, 42(23): 31-33.

[12] 张雪,马光思,毛宏燕. 基于 SSL 提高网上安全交易性能的研究[J]. 微电子学与计算机, 2011, 28(2): 181.

[13] 王小云,张金清. MD5 报文摘要算法的各圈函数碰撞分析[J]. 计算机工程与科学, 1996, 18(2): 15-22.

[14] TANENBAUM A S. Computer networks[M]. 4th ed. 潘爱民, 译. 北京:清华大学出版社, 2004: 634-637.

(上接第 1404 页)

图6 各种攻击下的水印检测图像

性,选取能量最大方向子带和能量最小方向子带同时进行水印嵌入,并赋予不同的嵌入强度,利用水印图像的奇异值来进行水印图像的嵌入。在水印提取过程中,针对不同攻击类型,分别从两个系数矩阵提取水印,继而保证了水印的鲁棒性。在实验过程中,笔者发现,本文算法的嵌入和提取水印过程耗时极少,可以直接应用于在线水印检测。

参考文献:

[1] 唐笑年. 基于 BOR 多小波分解系数特点的图像数字水印技术研究[D]. 长春:吉林大学, 2009.

[2] 林立宇, 张友焱, 孙涛, 等. Contourlet 变换——影像处理应用[M]. 北京:科学出版社, 2007: 37-42.

[3] 雍蓉,吕建平. 基于小波变换的零水印算法研究[J]. 西安邮电学院学报, 2011, 16(1): 45-48.

[4] 李振宏,吴慧中. 基于 DWT 及方向可控金字塔变换的抗几何攻击水印[J]. 中国图象图形学报, 2010, 15(2): 232-235.

[5] 杨俊,张贵仓,魏伟一. 基于小波变换和奇异值分解的数字水印算法[J]. 长春理工大学学报, 2005, 28(4): 81-84.

[6] 王员根,梁凡,肖明明. 一种彩色图像 DC 系数的自适应水印算法[J]. 中山大学学报:自然科学版, 2010, 31(4): 146-140.

[7] 赵彦涛,李志全. 基于奇异值分解的近无损可逆数字水印方案[J]. 光电子·激光, 2009, 20(11): 1486-1491.

[8] 朱少敏,刘建明. 基于 Contourlet 变换域的自适应量化索引调制数字图像水印算法[J]. 光学学报, 2009, 29(6): 1523-1529.