一个基于离散混沌加密的数字水印算法

陈河山[1] 吕珍珍[2] 罗 伟[2]
(河南大学 开封 475001)[1] (解放军信息工程大学 郑州 450004)[2]

摘 要 设计了一个基于离散混沌动力系统和小波分解的数字图像水印算法。在水印图像预处理阶段,利用Logistic映射生成的混沌序列对水印图像进行扩展置乱,再利用Logistic映射生成密钥来对水印信息进行加密,从而保证了水印信息的安全性。在水印图像嵌入阶段,对宿主图像进行三层小波分解,利用小波系数大小关系将水印嵌入到水平方向的高频系数中。分析和实验结果表明,该算法具有良好的鲁棒性,水印的安全性和不可见性明显优于常见算法。

关键词 数字水印算法,离散混沌系统,Logistic映射
中图法分类号 TN918.1 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.12.011

Digital Image Watermarking Algorithm Based on Dispersed Chaotic Mapping System

CHEN He-shan[1] LV Zhen-zhen[2] LUO Wei[2]
(Henan University, Kaifeng 475001, China)[1]
(PLA Information Engineering University, Zhengzhou 450004, China)[2]

Abstract This paper designed a digital image watermarking algorithm based on a dispersed chaotic mapping system and wavelet transform. In the process of preprocessing watermark, the Logistic mapping produces key to encrypt the grey value in the pixel to insure the security of watermark. In the process of embedding watermark, three-level wavelet decomposition on image is conducted and watermark is embedded in the high frequency wavelet coefficients according to the size of wavelet coefficients. Analysis and experiment results show that the algorithm possesses relatively strong robustness, and better security and transparency than ordinary algorithms.

Keywords Image watermarking, Dispersed chaotic mapping system, Logistic mapping

1 引言

数字图像的安全性和版权保护是伴随着计算机网络和多媒体技术飞速发展而出现的新问题。在数字图像网络传播过程中,非法用户未经版权所有者的许可,重新发布产品或有意破坏原始作品并重新发布其不可信版本,给消费者和版权所有者造成损失。

数字水印技术[1,2]将一些标识信息(即数字水印)直接嵌入数字载体当中(包括文字、图像、视频等)或是在不影响原载体的使用价值的前提下修改载体特定区域的结构,达到确认内容创建者、购买者、传送隐秘信息或者判断载体是否被篡改等目的。数字水印是实现版权保护的有效办法,是信息隐藏技术研究领域的重要分支和研究方向。

混沌密码作为一类新型的密码技术,近年来在数据加密[3-6]、图像加密[7,8]和数字水印等多个领域得到了广泛的研究和应用,成为当前在信息安全领域的研究热点之一。

本文设计了一个基于离散混沌动力系统和小波分解的数字图像水印算法,分析和实验结果表明,该算法具有良好的鲁棒性,水印的安全性和透明性明显优于常见算法。

2 相关知识

目前常见的离散混沌系统包括Logistic映射[9,10]、Chebyshev映射[11]、Cat映射[12]、Henon映射[13]以及Lorenz混沌系统[14]等。其中Logistic映射具有形式简单、易于实现、速度快等优点,在混沌密码学中得到广泛应用。

Logistic映射是一种能够比较彻底地表现确定性的混沌系统,是一类非常简单却被广泛研究的动力系统。Logistic映射又称虫口模型,其定义如下[9,10]:

$$x_{k+1}=\mu x_k(1-x_k),0\leqslant\mu\leqslant4,0<x_k<1$$

相关研究结果[9-11]表明,对于一维Logistic映射 $X_{n+1}=f(X_n)=\mu X_n(1-X_n)$,当系统参数 μ 满足 $0\leqslant\mu<3$ 时,系统状态比较简单;$3\leqslant\mu<3.5699$ 时,系统处于倍周期状态;$3.57\leqslant\mu\leqslant4$ 时,系统处于混沌状态。其中 $X_n\in(0,1)$,$n=0,1,2\cdots$。

该混沌系统选取参数 $\mu=4$ 时,关于变量 x 的概率密度函数为:

$$\rho(x)=\frac{1}{\pi\sqrt{(1-x)x}}$$

到稿日期:2013-12-19 返修日期:2014-01-28 本文受国家自然科学基金(11204379),河南省科技创新杰出青年计划项目(104100510025)资助。
陈河山(1973-),男,硕士,讲师,主要研究方向为偏微分方程;吕珍珍 女,硕士,主要研究方向为数字水印与混沌图像加密;罗 伟 男,硕士生,主要研究方向为分组密码设计与分析。

其中，$x\in(0,1)$。

利用概率密度函数得到 Logistic 生成的混沌序列相关结论如下：

1)均值 $\bar{x}=\int_0^1 x\rho(x)\mathrm{d}x=0.5$；

2)$\tau\neq0$ 时，自相关函数 $\rho(\tau)=\int_0^1 xf^{\tau}(x)\rho(x)\mathrm{d}x-\bar{x}^2=0$；

3)两个独立混沌序列的互相关函数为：

$$c(m)=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}(x_i-\bar{x})(y_{i+m}-\bar{y})$$

$$=\int_0^1\int_0^1\rho(x,y)(x-\bar{x})(f^m(y)-\bar{y})\mathrm{d}x\mathrm{d}y=0。$$

上述性质表明，Logistic 映射产生的混沌序列具有 *δ-like* 型的自相关函数和零互相关函数的特性，等同于随机白噪声。

3 设计思路

评价数字混沌水印算法优劣的 3 个主要指标包括：水印信息的鲁棒性、安全性以及透明度[15]。目前常见的数字混沌水印算法[16-18]大多根据应用需要，在某个单一指标上能够达到较好效果，其它指标效果不佳，致使所设计的水印算法应用范围狭窄，不利于建立数字混沌水印标准算法。其原因在于常见算法对水印图像加密预处理不充分，对水印嵌入位置选择不合理。

本文旨在避免常见算法的上述弱点，首先对水印图像进行扩散置乱，再通过行、列循环移位和灰度值变换实现水印信息加密，多圈迭代确保水印算法具有较强的安全性。三层小波分解技术的应用，保证算法具有良好的透明性和强鲁棒性。将水印嵌入位置作为水印提取密钥，进一步加强水印信息的安全性，实现水印信息的盲提取。

水印算法相关参数包括：混沌系统参数 μ、混沌序列的初始值 a_0、序列抛弃位数 n、置乱序列 S、加密迭代圈数 k、原始水印图像 W_0 大小 $m\times n$、扩展倍数 $k\times l$、水印嵌入强度 α、宿主图像 I_0 大小 $S\times T$。相关符号包括：原始水印图像 W_0、扩展水印图像 W_1、加密水印图像 W_2、宿主图像 I_0 以及含水印图像 I。图 1 给出了水印嵌入过程示意图。

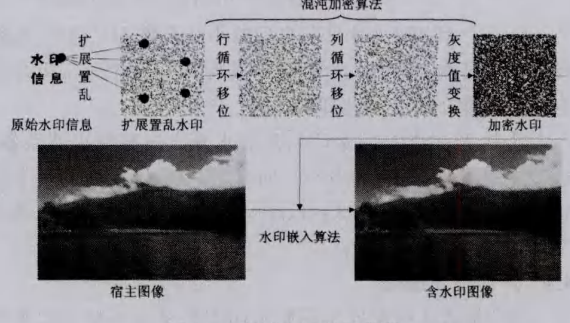


图 1 水印嵌入过程示意图

4 基于离散混沌加密的数字水印算法

本节设计的数字水印算法基于不同参数条件下的 Logistic 映射，确保了水印算法的安全性。基于混沌加密的数字水印算法密钥包括：置乱序列 S，水印图像加密算法密钥 K_1、K_2、K_3，水印嵌入位置标志矩阵 Lg 以及水印嵌入强度 α。

数字混沌水印算法包括 4 个部分：水印图像扩展置乱、水印信息加密、水印嵌入以及水印提取。下面对上述 4 个部分进行详细介绍。

4.1 水印图像扩展置乱

为了更好隐藏水印信息，算法对原始水印图像 W_0 进行 $k\times l$ 倍扩展置乱，得到大小为 $M\times N$ 的扩展水印图像 W_1。W_0 为二值图像，每个像素点灰度值为 0 或 255，$M=k\times m$，$N=l\times n$。

水印图像扩展置乱步骤如下：

Step1 选取系统参数 μ，给定 Logistic 映射初始值 a_0。

Step2 对 Logistic 映射进行多次迭代，抛弃生成混沌序列的前 n 个值，消除初始值相关性影响，得到长度为 T 的混沌序列 a。

Step3 对 Step2 生成的混沌序列 a 依据大小关系进行量化，$S(i)$取值为混沌序列 a 按大小排序后第 i 个值在未排序序列中的位置，得到置乱序列 S。过程如下：

```
for j=1:T
for i=1:T
{
If a[i]==max{a}
S[j]=i;
a [i]=0;
}
```

Step4 置乱序列 S 按序分为 $m\times n$ 段，每段包含 $k\times l$ 个值。

Step5 将原始水印图像 W_0 按照从左往右、从上到下的顺序扫描成一维像素序列 W_0'。

Step6 $W_0'(i)$扩展到 W_1'中 $S((i-1)\times k\times l+1)$到 $S(i\times k\times l)$的 $k\times l$ 个位置，将一维像素序列 W_1'扫描成二维图像 W_1。过程如下：

```
for i=1:m*n
{
W1'[S((i-1)*k*l+1)]=W0'[i];
W1'[S(i*k*l)]=W0'[i];
}
for i=1:k*m
for j=1:l*n
{
W1[i] [j]=W1'[i*l*n+j];
}
```

4.2 水印信息加密

水印信息加密基于 Logistic 映射设计的混沌图像加密算法。将 4.1 节水印图像扩展置乱 Step1－Step3 在不同参数条件下生成的 S_1，S_2 作为密钥 K_1，K_2。密钥 K_3 由 4.1 节水印图像扩展置乱 Step1－Step2 生成的混沌序列 a，利用如下选择函数得到：

$$K_{3,i}=\begin{cases}1, & a(i)>0.5\\ -1, & a(i)\leqslant 0.5\end{cases}$$

水印信息加密过程包括：行循环移位、列循环移位以及像素点灰度值变换 3 个部分。设 r 为扩展水印图像 W_1 对应的灰度值矩阵，r_l 为中间变量矩阵，水印信息加密步骤如下：

Step1　W_1 像素点行循环移位变换。密钥 $K_1=\{k_{1,0},k_{1,1},\cdots,k_{1,M-1}\}$，对像素矩阵第 i 行循环右移 $k_{1,i}$ 位：

```
for(j=0,j<N,j++)
{
r1[i][(j+k1,i)%N]=r[i][j];
r=r1;
}
```

Step2　列循环移位变换。密钥 $K_2=\{k_{2,0},k_{2,1},\cdots,k_{2,N-1}\}$，对像素矩阵第 j 列循环下移 $k_{2,j}$ 位：

```
for(i=0,i<M,i++)
{
r1[(i+k2,j)%M] [j]=r[i][j];
r=r1;
}
```

Step3　灰度值变换。将密钥 $K_3=\{k_{3,0},k_{3,1},\cdots,k_{3,M\times N-1}\}$ 扫描成大小为 $M\times N$ 的密钥矩阵 K_3'。若 $K_3'(i,j)=1$，则将二值点 $r(i,j)$ 进行黑白转换，否则二值点 $r(i,j)$ 不变。具体过程如下：

```
for(i=0,i<M,i++)
for(j=0,j<N,j++)
{
if K3'[i][j]==1
  if r [i][j]==0
    r [i][j]==255;
  else
    r [i][j]==0;
  end
else
    W2[i][j]=r[i][j];
  end
}
```

Step4　重复循环执行 k 次 Step1－Step3，输出加密水印图像 W_2。

4.3　水印信息嵌入

人眼对于小波分解高频系数敏感性较低，对低频系数较为敏感。将水印信息嵌入到小波分解高频系数中，可以保证水印信息具有良好的透明性，但难以抵抗低通滤波和数据压缩攻击；将水印信息嵌入到小波分解低频系数中，容易造成图像的视觉质量下降。如何选取水印信息嵌入位置对水印算法的实现效果至关重要。

本算法对宿主图像进行三层小波分解，选取水平方向上的高频系数嵌入水印信息，确保算法在透明度和鲁棒性两个指标上同时达到较好效果。在此基础上，以小波系数大小关系和嵌入水印像素值为依据选取嵌入位置，将水印嵌入位置作为提取水印信息的密钥，从而增强了算法安全性，同时保证了提取水印信息时不需要提供宿主图像，实现了水印盲提取。

1)三层小波分解

根据 HVS(人类视觉特性)模型，人眼对 RGB 图像蓝色分量不敏感[19]，适合作为水印嵌入的位置。将宿主图像转换到 RGB 空间，对蓝色分量 B 进行三层小波分解，利用 HL_3 嵌入水印信息。图 2 为三层小波分解示意图。

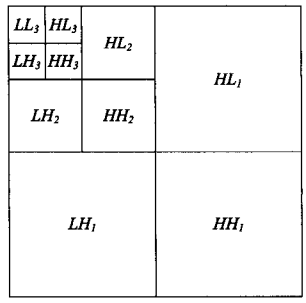


图 2　三层小波分解示意图

2)水印嵌入位置

我们选取 HL_3 中较大的系数嵌入水印信息，步骤如下：

Step1　将 HL_3 按照从左往右、从上到下的顺序扫描成一维数组 $HL_3^{(1)}$。

Step2　利用 Sort 函数对 $HL_3^{(1)}$ 从小到大进行排序，得到 $HL_3^{(2)}$。

Step3　阈值 $th=HL_3^{(2)}(t-4*m*n)$，嵌入方程选择参数 $th1=HL_3^{(2)}(t-2*m*n)$。

Step4　水印嵌入位置集合为：

$P=\{(i,j)\mid HL_3(i,j)\geqslant th1\}$

3)水印的嵌入

由阈值 th 的选取可知：$|P|=M\times N=k\times m\times l\times n$。为了方便水印的嵌入，将集合 P 中的元素扫描成大小 $M\times N$ 的位置矩阵，(k_i,t_j) 表示位置矩阵第 i 行、第 j 列的元素。通过采用不同的水印嵌入方程，引入标志矩阵，实现了对水印信息嵌入位置的隐藏，增强了水印的安全性。水印嵌入过程如下：

Step1　对嵌入位置集合 P，按下式嵌入水印。水印嵌入方程为：

$$HL_3^{w}(k_i,t_j)=\begin{cases}HL_3(k_i,t_j)\times(1+\alpha),Lg(k_i,t_j)=1\\ \quad \text{if } W_2(i,j)=255\&HL_3(k_i,t_j)\geqslant th1\\ HL_3(k_i,t_j)\times(1-\alpha),Lg(k_i,t_j)=-1\\ \quad \text{if } W_2(i,j)=255\&HL_3(k_i,t_j)<th1\\ HL_3(k_i,t_j)\times(1+\alpha),Lg(k_i,t_j)=-1\\ \quad \text{if } W_2(i,j)=0\&HL_3(k_i,t_j)\geqslant th1\\ HL_3(k_i,t_j)\times(1-\alpha),Lg(k_i,t_j)=1\\ \quad \text{if } W_2(i,j)=0\&HL_3(k_i,t_j)<th1\end{cases}$$

Step2　利用嵌入水印信息后的小波系数 HL_3^{w} 对原系数 HL_3 进行替换，重构出 B 分量，将其与 R、G 两个分量组合成包含水印的图像，完成水印的嵌入。

其中，HL_3^{w} 为嵌入水印信息后水平方向高频小波系数；Lg 为标志矩阵，大小为 $S\times T/64$，作为提取水印时的一个重要依据，若 $(i,j)\notin P$，则 $Lg(i,j)=0$；α 为嵌入强度因子，通过实验确定。

4.4　水印信息提取

水印提取是指提取出原始水印图像 W_0，包括对加密水印图像的提取以及解密两个部分。对含水印图像进行水印嵌入过程逆操作即可实现对加密水印图像的提取，利用密钥对加密水印图像进行解密后，再对其进行压缩得到原始水印图像。步骤如下：

Step1　将含水印图像转换到 RGB 空间，取出 B 分量，对其进行三层小波分解，选取 HL_3^{w} 提取水印信息。

Step2　根据标志矩阵 Lg 和嵌入强度 α，提取出加密水

印信息 W_2。

$$W_2(i,j)=\begin{cases}255, & \text{if } Lg(k_i,t_j)=1\&HL_3^w(k_i,t_j)\geqslant th1\\255, & \text{if } Lg(k_i,t_j)=-1\&HL_3^w(k_i,t_j)<th1\\0, & \text{if } Lg(k_i,t_j)=-1\&HL_3^w(k_i,t_j)\geqslant th1\\0, & \text{if } Lg(k_i,t_j)=1\&HL_3^w(k_i,t_j)<th1\end{cases}$$

Step3　灰度值逆变换。利用密钥 K_3'，执行 4.2 节水印信息加密即可。

Step4　列循环移位逆变换。密钥 $K_2=\{k_{2,0},k_{2,2},\cdots,k_{2,N-1}\}$。

```
for(i=0,i<M,i++)
{
r1[(i-k2,j)%M][j]=r[i][j];
}
r=r1;
```

Step5　行循环移位逆变换。密钥 $K_1=\{k_{1,1},k_{1,2},\cdots,k_{1,M-1}\}$，得到扩展置乱水印图像 W_1；

```
for(j=0,j<N,j++)
{
r1[i][(j-k1,i)%N]=r[i][j];
}
r=r1;
```

循环执行 k 次上述 Step3－Step5，得到扩展水印图像 W_1。

Step6　将扩展水印图像 W_1 扫描成一维向量 W_1'，利用已掌握的置乱序列 S，将 W_1' 位于 $S(i\times k\times l)$ 位置的像素值放入 W_0' 的 $i(i=0,1,\cdots,m\times n-1)$ 位置，再将 W_0' 扫描成二维矩阵，得到原始水印图像 W_0。图 3 给出了基于混沌加密的数字水印嵌入算法流程图，其逆向图即为提取水印算法流程图。

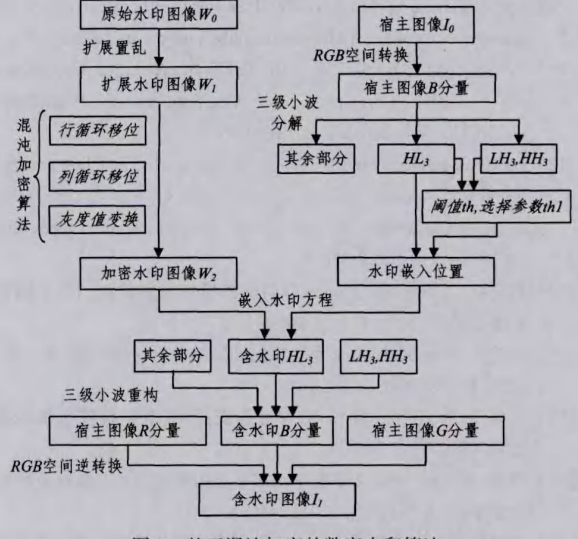


图 3　基于混沌加密的数字水印算法

5　仿真实验

水印算法的实验部分采用 1920×1200×3 的彩色图像 scenery. bmp 作为宿主图像，如图 4(a)所示；采用大小为 60×60、含有“水印信息”字样的二值图像作为水印图像，如图 4(b)所示，水印算法实现平台为 Matlab2008a。通过实验，选定嵌入强度 $\alpha=0.015$。Logistic 混沌映射的系统参数 $\mu=4$，初始值分别为 $a_0=0.376$，$a_1=0.784$，$a_2=0.993$，$a_3=0.019$，用以生成密钥 S 和 K_1、K_2、K_3，迭代圈数 $k=1$，生成混沌序列抛弃位数 $n=200$，扩展倍数 $k\times l=2\times 2$。

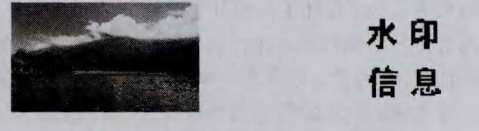
(a)宿主图像　　(b)水印信息

图 4　宿主图像和水印信息

目前对于水印算法的评价并没有统一的标准，本文依据实验数据，分别从透明度和鲁棒性两个角度对水印算法进行量化评价。

5.1　透明性实验

透明性反映了含水印图像与宿主图像间的视觉差异，即水印信息在宿主图像中的不可见性。本实验在 Matlab2008a 平台下，对水印图像进行嵌入和提取，图 5(a)为 scenery. bmp 嵌入“水印信息”后的图像，图 5(b)为不经任何攻击从图 5(a)中直接提取的水印图像。水印嵌入到宿主图像后，视觉上很难分辨图 5(a)含水印图像与图 4(a)宿主图像间的区别。提取出的水印信息图 5(b)与原始水印信息图 4(b)也难以区分。



(a)含水印图像　　(b)提取出的水印

图 5　含水印图像和提取的水印

有了上述定性分析结果，下面对水印算法透明性进行定量分析，实验选用峰值信噪比 PSNR 定量测评水印算法透明性。其定义如下：

$$MSE=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}|I(i,j)-I^*(i,j)|^2$$

$$PSNR=10\log_{10}\frac{\max[I^2(i,j)]}{MSE}$$

其中，I_0 为原始图像，I 为含水印图像，M 和 N 分别为图像的长和宽。

研究结果表明[20]，当峰值信噪比大于 30dB 时，水印信息在含水印图像中几乎是不可见的。本算法的峰值信噪比 $PSNR=52.461$dB，说明水印算法透明性良好。

5.2　鲁棒性实验

鲁棒性是指含水印图像抵抗攻击者减弱、移动或破坏水印的能力。为了测试水印算法的鲁棒性，对含水印图像进行多种攻击，计算不同攻击条件下提取出的水印信息与原始水印图像间的相关系数 NC，将 NC 作为算法抗攻击能力的评价指标。

$$NC(\omega,\omega_s)=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\omega(i,j)\omega_s(i,j)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}\omega(i,j)^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}\omega_s(i,j)^2}}$$

其中，ω 为原始水印图像，ω_s 为遭受攻击条件下提取出的水印图像，m 和 n 分别为水印的长和宽。

实验对含水印图像进行的攻击包括：噪声攻击(包括高斯噪声和椒盐噪声)、滤波攻击、JEPG 压缩以及剪切等。表 1

给出了具体的实验结果，其中相关系数 NC 越接近 1，表明算法抵抗相应攻击的能力越强。

表 1 水印的鲁棒性攻击检测结果

攻击方式	利用本算法提取出的水印	相关系数 NC	攻击方式	利用本算法提取出的水印	相关系数 NC
未攻击		1	3*3 中值滤波		0.992
均值为 0，方差为 0.01 的高斯噪声		0.989	方差 0.01 的椒盐噪声“+”3*3 中值滤波		0.891
均值为 0，方差为 0.02 的高斯噪声		0.962	80%JEPG 压缩		0.952
均值为 0，方差为 0.05 的高斯噪声		0.921	50%JEPG 压缩		0.845
均值为 0，方差为 0.01 的椒盐噪声		0.990	剪切(左上 1/4)		0.950
均值为 0，方差为 0.03 的椒盐噪声		0.953	剪切(右下 1/4)		0.957

如表 1 所列，在遭受不同攻击的条件下，本算法所提取的水印与原始水印图像间的相关系数较高，算法抵抗攻击的能力较强，优于常见算法所得到的对应结果[16-18]。以上实验分析显示，本算法可以抵抗以上几种常见攻击，具有良好的鲁棒性。

结束语 本文设计了一种基于混沌的数字水印算法，通过混沌加密算法和数字水印技术的结合，将混沌密码算法进一步推向应用，为设计数字混沌水印标准算法作出了重要的探索。算法对原始水印图像预处理充分，利用 Logistic 映射产生密钥实现了对水印图像的扩展置乱，应用混沌加密算法确保了水印的安全性；嵌入水印阶段，将宿主图像转换到 YC_bC_R 空间，对其 Y 分量进行三层小波分解，将水印信息的嵌入位置作为提出水印的密钥，保证了水印的鲁棒性和透明性。实验结果表明，含水印图像峰值信噪比较大，水印信息透明性较好；算法对噪声攻击(包括高斯噪声和椒盐噪声)、滤波攻击、JEPG 压缩和剪切等具有较强的抵抗能力。

参 考 文 献

[1] 王宏霞，何晨，丁科. 基于混沌映射的鲁棒性公开水印[J]. 软件学报，2004，15(8)：1245-1251

[2] 唐国坪，廖晓峰. 基于混沌映射的抗剪切鲁棒水印算法[J]. 计算机工程，2005，31(9)：34-36

[3] Yuan Chun，Zhong Yu-zhuo，Yang Shi-qiang. Composite chaotic pseudo-random sequence encryption algorithm for compressed video[J]. Tsinghua Science and Technology，2004，9(2)：234-241

[4] Liu Jian-ming，Lv Hui-jing. A New Duffing-Lorenz Chaotic Algorithm and Its Application in Image Encryption[C]// International Conference on Control Engineering and Communication Technology (ICCECT). 2012：1022-1025

[5] Rahnama N，Talebi S. Secure communication via hybrid method in nonlinear chaotic systemsSecure communication via hybrid method in nonlinear chaotic systems[C]// 2012 20th Iranian Conference on Electrical Engineering (ICEE). 2012：1262-1267

[6] Rahnama N，Talebi S. Performance comparison of chaotic spreading sequences generated by 1D and 3D chaotic systems in a chaos-based DS-CDMA system[C]// Sixth International Symposium on Telecommunications (IST). 2012：404-409

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

[8] Mao Yao-bin，Chen Guan-rong. Chaos-based image encryption [M]// Handbook of Geometric Computing. 2005：231-265

[9] 胡汉平，刘双红，王祖喜，等. 一种混沌密钥流产生方法[J]. 计算机学报，2004，27(3)：408-412

[10] Cicek I，Pusane A E，Dundar G. Random number generation using field programmable analog array implementation of logistic map[C]// Signal Processing and Communications Applications Conference (SIU). 2013：1-4

[11] Hsu Chien-Lung，Lin Tzu-Wei. Password authenticated key exchange protocol for multi-server mobile networks based on Chebyshev chaotic map[C]// 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). 2013：90-95

[12] Jin Chan-ho，Ryu Heung-Gyoon. Design of chaotic CDSK modulation system using different chaotic maps[C]// 2013 15th International Conference on Advanced Communication Technology (ICACT). 2013：222-226

[13] 刘晓克，万里红，等. Henon 映射的图像加密新算法[J]. 中国计量学院学报，2008，19(4)：338-341

[14] 陈关荣，吕金虎. Lorenz 系统族的动力学分析、控制与同步[M]. 北京：科学出版社，2003：2-40

[15] 王炳锡，等. 数字水印技术[M]. 西安：西安电子科技大学出版社，2003

[16] 何岸，胡伟刚. 中文文本数字水印算法的研究[J]. 中南林业科技大学学报：自然科学版，2011，31(8)：204-210

[17] 高铁红，莫然. 一种基于小波系数动态量化的鲁棒数字水印算法[J]. 武汉大学学报：理学版，2011，57(5)：449-454

[18] 杜浩. 基于人类视觉系统的自适应数字图像水印算法[J]. 计算机与现代化，2011，8：164-170

[19] Mehul R，Priti R. Discrete wavelet transform based multiple watermarking scheme[C]// Proeeedings of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific 2003. Bangalore，India，2003：14-17

[20] 钮心忻. 信息隐藏与数字水印[M]. 北京：北京邮电大学出版社，2004