基于 Arnold 变换和 Lorenz 混沌系统的彩色水印图像加密算法①

王丽丽

(宝鸡职业技术学院 电子信息工程系，宝鸡 721008)

摘 要：该算法利用 Arnold 变换以及彩色图像的置乱度定义，求解 Lorenz 混沌系统的动力学方程，得到三个混沌序列；然后对 Arnold 置乱后的每个颜色分量进行置乱处理。仿真实验结果表明，该算法克服了 Arnold 变换和 Lorenz 混沌系统的缺点，能够抵抗多种攻击，使彩色水印图像具有较高的安全性。

关键词：Arnold 变换；Lorenz 混沌系统；算法

Encryption Algorithm of Colored Watermark Image Based on Arnold Transform and Lorenz Chaos System

WANG Li-Li

(Electronic Information Engineering Dep, Baoji Professional Technology Institute, Baoji 721008, China)

Abstract：This algorithm uses the Arnold transformation and the color image scrambling definition, to solve the Lorenz chaos system's dynamic equation, to obtain three chaos sequences. Then it carries on scrambling processing after Arnold scrambling's each color component. The simulation experiment result indicated that this algorithm has overcome the Arnold transformation and the Lorenz chaos system's shortcoming, can resist many kinds of attacks, enables the high security of the colored watermark image.

Key words：Arnold transform; lorenz chaos system; algorithms

数字水印技术是一种新的信息隐藏技术，它的迅猛发展成为信息安全领域的一个热点。若只是单纯地用各种信息隐藏算法（如 DFT、DCT、DWT 等）对秘密信息进行隐藏保密，那么攻击者只要直接利用现有的各种信息提取算法对被截获信息进行穷举运算，就很有可能提取出秘密信息。所以在研究各种新的水印隐藏算法同时，还要在信息隐藏之前先对秘密信息按照一定的运算规则进行置乱处理，使其变得“杂乱无章、面目全非”，成为无意义的图像，然后再将其隐藏到载体信息里面，这样用户所要传输的信息就更加安全了。即使攻击者将秘密信息从载体中提取出来，也无法分辨出置乱后的秘密信息到底隐藏着什么内容，于是就可能认为提取算法错误或该载体中不含有任何其它信息[1]。

本文提出一种基于 Arnold 变换和 Lorenz 混沌系统的彩色水印图像加密算法，该算法能够较好的对嵌入载体图像之前的水印信息进行置乱处理，使水印信息具有较高抗攻击性能和初值敏感性。除非知道确切的初值，否则即使破解了嵌入算法，也不可能恢复提取出的置乱水印信息。

1 Arnold变换

Arnold 变换原理[2]：Arnold 变换是 V.J.Arnold 在遍历理论的研究中提出的，它是采用阶数为的图像矩阵把原来 (x, y) 点处的像素变换到点 (x', y') 处。采用的 Arnold 变换公式为：

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ N) \quad (1)$$

① 收稿时间:2011-10-05;收到修改稿时间:2011-11-18

即 $x'=(x+y)(\bmod N)$，$y'=(x+2y)(\bmod N)$。

由式(1)可知，Arnold 变换不同位置的水印像素变换后各个像素位置是不会重叠的。当迭代一定次数之后，任意两个原本相邻的水印像素点的位置会产生很大的分离。这样，原始水印的全部像素被随机而均匀的置乱到整个水印空间上。水印图像采用“Camera_man.jpg”图像，置乱水印效果图如图 1 所示。


a 原始水印图像

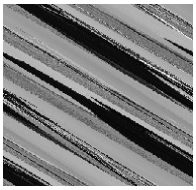

b 采用(1)式 2 次置乱

图 1　Arnold 变换对水印的置乱效果图

采用 Arnold 变换对水印图像进行置乱处理，分散了原始水印图像的相关性，有效地提高了载体图像的抗攻击性能。但是 Arnold 变换本身具有周期性，当水印图像的尺寸大小一定时，对水印图像进行 Arnold 变换迭代，当持续迭代一定次数后，被置乱的水印图像总可以恢复为原始水印图像。所以，针对此缺点，本文对经过 Arnold 变换置乱变换后的水印信息进行了二次加密，即 Lorenz 混沌处理。

2　Lorenz混沌系统

Lorenz 系统是经典的三维混沌系统，以 Lorenz 系统生成加密混沌序列的优点在于：一是其结构较低维混沌系统复杂，产生的实数值序列更不可预测；二是系统的三个初始值和三个参数都可以作为生成加密混沌序列的种子密钥，产生的密钥空间高于低维混沌系统；三是对系统输出的实值混沌序列进行处理，可采用单变量或多变量组合的加密混沌序列，这样序列密码的设计更灵活。

Lorenz 混沌系统的动力学方程[3]为：

$$\begin{cases} dx/dt=-a(x-y) \\ dy/dt=bx-xz-y \\ dz/dt=-cz+xy \end{cases} \tag{2}$$

其中，a,b,c 是系统参数，一般取值为 $a=10,\ b=28,c=8/3$。在保持 a,c 不变，$b>24.74$ 时，Lorenz 系统进入混沌态。

利用 Euler 算法对式（2）作离散化处理，得到离散化后的迭代方程为(3)：

$$\begin{cases} x(n+1)=-(aT)(x(n)-y(n))+x(n) \\ y(n+1)=T(bx(n)-x(n)z(n)-y(n))-y(n) \\ z(n+1)=T(-cz(n)+x(n)y(n))+z(n) \end{cases} \tag{3}$$

其中 $T=0.05$ 为取样时间。

根据式（2）和式（3）以及上述参数，可以得到 Lorenz 混沌系统中吸引子的数值仿真结果。

3　基于Arnold变换和Lorenz混沌系统的彩色水印图像加密/解密算法

3.1 彩色图像置乱评价标准

样本中各数据与样本平均数的差的平方和的平均数叫做样本方差；样本方差的算术平方根叫做样本标准差。样本方差和样本标准差都是衡量一个样本波动大小的量，样本方差或样本标准差越大，样本数据的波动就越大。因此可以用图像灰度均值的方差来描述图像的置乱程度，方差越小，则图像像素之间灰度均值相差越小，即灰度分布越均匀，图像“杂乱”的程度越大。

根据灰度方差这一原理，汪晓华等人[4]提出了置乱度这一概念，具体定义如下：

设子图像为：$I(i,j),i=0,1,...,k-1$，灰度均值 E 定义如（4）式：

$$E=\frac{1}{k\times k}\sum_{i=0}^{k-1}\sum_{j=0}^{k-1}I(i,j) \tag{4}$$

图像 I 的方差 σ^2 定义如（5）式：

$$\sigma^2=\frac{1}{k\times k}\sum_{i=0}^{k-1}\sum_{j=0}^{k-1}(I(i,j)-E) \tag{5}$$

σ^2 描述图像的变化程度，其值越大，说明各点的灰度值与均值的差别就越大，图像变化越剧烈，图像越乱。

设置乱前图像的方差为 σ_{old}^2，置乱后方差为 σ_{new}^2，则图像置乱度 η 定义如（6）所示：

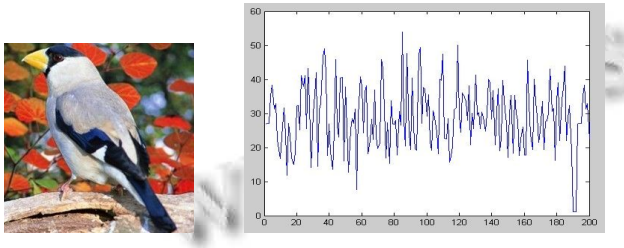
$$\eta=\frac{\sigma_{new}^2}{\sigma_{old}^2} \tag{6}$$

由此可见，η 越大，置乱效果越好，相对于原始图像越“乱”，受攻击的可能性就越小，加密程度就越高。

根据灰度图像置乱度定义，本文定义彩色图像的置乱度为：

$$\eta_{\text{color}} = \frac{1}{3}(\eta_R + \eta_G + \eta_B) \tag{7}$$

采用 256×256 大小的“bird.jpg”图像，Arnold 变换置乱程度和置乱次数关系图如图 2 所示，其中纵坐标是置乱度，横坐标是 Arnold 变换置乱次数。



水印图像　　彩色水印图像 Arnold 变换置乱程度 η 和置乱次数关系图

图 2　Arnold 变换置乱程度 η 和置乱次数关系图

从图 2 中可以看到，置乱度和置乱次数并没有固定的比例关系，置乱次数多并不是置乱程度就高。通过对上图分析可以看出，采用公式（1）对图像进行 Arnold 置乱时，当迭代次数为 192 时，图像置乱度与原始图像的置乱度相同，在 1-192 次之间时，置乱度并无规律可循。所以通过观察置乱度的大小，综合考虑置乱度和时间复杂度等因素得到理想的 Arnold 置乱变换次数。

3.2 基于 Arnold 变换和 Lorenz 混沌系统的彩色水印图像加密/解密算法

通过 3.1 中的置乱度的定义，计算了对图像单独进行 Lorenz 变换后图像的置乱度。当在 Lorenz 混沌系统中取参数 $\sigma=10, r=28, b=8/3, h=0.01$，系统初始值 $(x_0, y_0, z_0)=(1,1,1)$ 时，计算得到置乱度为 $\eta_{\text{color\_Lorenz}}=24.4914$。在 Arnold 变换中，结合置乱度的大小和计算的时间复杂度，选择变换次数为 38 次，此时置乱度 $\eta_{\text{color\_Arnold}}=38.3428$。Arnold 变换虽然能够达到较高的置乱度，但是由于可以被穷举解密的缺点，本文利用 Lorenz 具有非常敏感的初值的特点，提出了基于 Arnold 变换和 Lorenz 混沌系统的加密算法，算法首先对原始彩色水印图像的 R、G、B 三个颜色分量分别采用 Arnold 变换进行置乱，再将置乱后的颜色分量分别采用 Lorenz 混沌系统生成的三个置乱序列进行加密置乱。加密后的水印图像置乱度为 $\eta_{color\_Lorenz\_Arnold}=31.4193$，不仅能够完善 Lorenz 置乱度不高，不能较好抵抗攻击的不足，并且在初值的敏感性方面具有较高的安全性，不易被破解。

下面是水印加密算法的具体实施：

（1）输入原始彩色水印图像；

（2）对原始彩色水印图像的 R、G、B 分量分别进行 Arnold 变换置乱，得到三个颜色分量的 Arnold 置乱水印；

（3）求解 Lorenz 混沌系统的动力学方程，方程见式(2)。Lorenz 混沌系统需要用数值积分来得到实数值混沌序列。典型的数值积分有一阶 Euler 法和四阶 Runge-Kutta 法，一阶 Euler 法的计算量更小，所以本文算法采用一阶 Euler 法来求解(2)式，以提高算法的计算速度，并得到 x, y, z 三个混沌序列；

（4）将 x, y, z 进行升序排列，sort(x)，sort(y)，sort(z)，并构造三个置乱索引序列，用来生成实数值混沌序列，并标识排序后的混沌序列原本的位置，用于解密时恢复原始水印图像；

（5）对于每个颜色分量，根据步骤（4）生成的三个置乱序列，对 R、G、B 分量的 Arnold 变换置乱后的分量图像进行置乱，即采用第一个置乱序列对水印图像 R 分量 Arnold 置乱后的图像进行 Lorenz 混沌置乱，采用第二个置乱序列对水印图像 G 分量 Arnold 置乱后的图像进行 Lorenz 混沌置乱，采用第三个置乱序列对水印图像 B 分量 Arnold 置乱后的图像进行 Lorenz 混沌置乱，从而得到置乱的水印图像。

解密算法是上述加密算法的逆过程。

4　仿真结果及分析

本算法的仿真实验在 Matlab7.0 平台下运行，采用 32×32 的 bird.jpg 真彩水印图像进行仿真实验。在本实验中 Arnold 变换的置乱次数设为 $d=38$，Lorenz 三维混沌系统的参数取 $\sigma=10, r=28, b=8/3, h=0.01$，系统初始值 $(x_0, y_0, z_0)=(1,1,1)$。

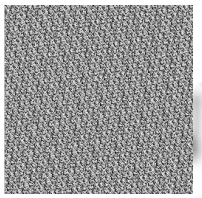
4.1 水印加密/解密效果

a 原始水印图像

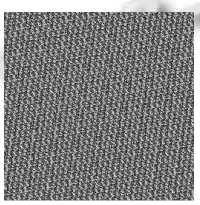
b 原始水印图像红色分量

c 原始水印图像绿色分量

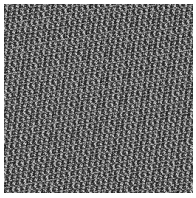
d 原始水印图像蓝色分量



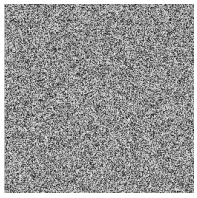
e 红色分量 Arnold 置乱置乱次数=38



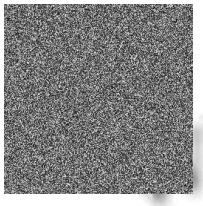
f 绿色分量 Arnold 置乱置乱次数=38



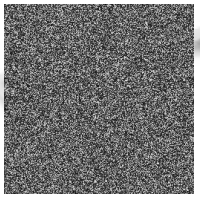
g 绿色分量 Arnold 置乱置乱次数=38



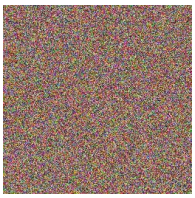
h 红色分量 Arnold 置乱后 Lorenz 混沌系统加密图



i 绿色分量 Arnold 置乱后 Lorenz 混沌系统加密图

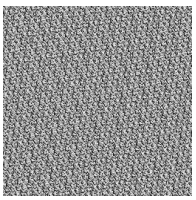


j 蓝色分量 Arnold 置乱后 Lorenz 混沌系统加密图

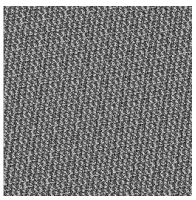


k 基于 Arnold 变换和 Lorenz 混沌系统的加密图像

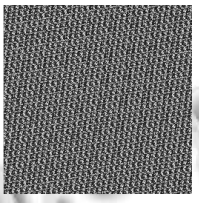
图 3　水印加密效果图



a 加密后水印红色分量采用 Lorenz 混沌系统解密图



b 加密后水印绿色分量采用 Lorenz 混沌系统解密图



c 加密后水印绿色分量采用 Lorenz 混沌系统解密图

d Lorenz 混沌系统解密后红色分量进行逆 Arnold 变换,变换次数=192-38

e Lorenz 混沌系统解密后绿色分量进行逆 Arnold 变换,变换次数=192-38

f Lorenz 混沌系统解密后蓝色分量进行逆 Arnold 变换,变换次数=192-38

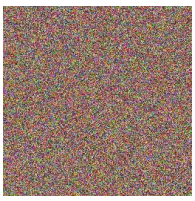
g 解密图像

图 4　水印解密效果图

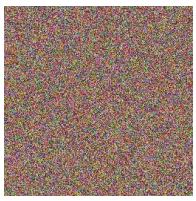
由图3和图4可见,采用基于Arnold变换和Lorenz混沌系统结合置乱的彩色水印图像从视觉上无法辨别出原始水印信息（如图 3(k)）。并且解密后的水印信息（如图 4(g)）和原始水印信息（如图 3(a)）的相似度 $NC=1$，即解密后的水印和原始水印信息完全相同。本算法属于无损加密算法。

4.2 密匙敏感性分析

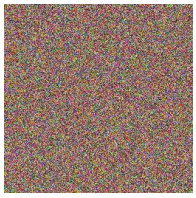
以下实验结果图是改变Lorenz混沌系统的系统初值提取出来的水印信息：



a. $(x_0, y_0, z_0) = (1.0000000001, 1, 1)$



b. $(x_0, y_0, z_0) = (1, 1.0000000001, 1)$



c $(x_0, y_0, z_0) = (1, 1, 1.0000000001)$

图 5 改变 Lorenz 混沌系统初始值提取的水印信息

由图 5 可见，改变系统初值中的任意一个变量，即使改变只是相差 10^{-10} 时，仍然无法解密出正确的水印图像。由此可以看出，该算法对于密匙具有很强的敏感性。

5 结语

本文提出了基于Arnold变换和Lorenz混沌系统的彩色水印图像加密算法。该算法的特点如下：

（1）水印信息是有意义的彩色水印图像，具有更广的适用范围。

（2）根据灰度水印图像的置乱度定义，提出了彩色图像的置乱度定义，并根据此置乱度定义选择了最优的 Arnold 变换置乱次数对图像进行 Arnold 变换置乱，增加了水印像素的置乱程度。

（3）算法充分利用了 Lorenz 混沌系统产生的三个混沌序列，增加了图像的抗攻击性能。

（4）算法将 Arnold 变换和 Lorenz 混沌系统结合对彩色水印图像进行置乱处理，克服了 Arnold 变换加密水印采用穷举方法就能够被破解，以及 Lorenz 混沌系统置乱度不高的缺点，置乱算法能够使彩色水印信息更具安全性。

（5）算法加密解密过程对于水印信息没有任何损失，是一种新的无损彩色水印加密算法。

参考文献

1 刘方.变换域加密图像数字水印算法研究[硕士学位论文].山东师范大学, 2009.

2 孙新德,路玲.Arnold变换在数字图像水印中的应用研究.信息技术,2006(10):129–132.

3 赵玉霞,康宝生.一种基于混沌序列的数字图像隐藏算法.西北大学学报,2008,(2):194–198.

4 A. TirkeI, GRankin. R. vail, Schyndef, W. Ho, N. Mee, C. Osbome. Elecrtonic watermark. Proc. DICTA 1993. Dec. 1993.666–672.

(上接第 29 页)

5 Sandu RS, Coyne EJ, Feinstein H L. Role based access control models. IEEE Computer, 1996,29 (2):38–47.

6 Ferraiolo DF. Proposed NIST standard for role based access Control. ACM Trans. on Information and Systems Security (TISSEC), 2001,4(3):224–274.

7 Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management. Dale J, Dinolt G, eds. Proc. of the Symp- osium on Security and Privacy. Oakland: IEEE Computer Society Press, 1996. 164–173.

8 Blaze M, Feigenbaum J, Ioannidis J, et al. The Role of Trust Management in Distributed Systems Security. Secure Internet Programming Issues for Mobile and Distributed Objects. Berlin: Springer-Verlag, 1999.185–210.

9 ChuY–H, Feigenbaum J, et al. REFEREE: trust management for Web Appilications.World Wide Web Journal.

10 易磊,杨长兴.一种改进的基于行为的网格信任模型.计算机系统应用, 2008,17(2):44–47.

11 Ninghui L, Mitchell JC, Winsborough WH. Design of a role–based trust-management framework. Security and Privacy, 2002. Proc. 2002 IEEE Symposium on. 2002,114–130.

12 黎梨苗,陈志刚,邓晓衡,桂劲松.基于模糊理论的主观信任综合评价模型研究.计算机应用研究, 2010,27(5):1860–1862.