一种新的图像保密通信系统设计

吕恩胜,裴 东
(西北师范大学 物理与电子工程学院,甘肃 兰州 730070)

摘 要:提出了一种新型的图像保密通信技术,利用混沌序列对初值敏感性、伪随机性的特点,在发送端采用了 Logistic 映射序列对图像像素值置乱加密和 Arnold 变换对像素位置置乱加密相结合的方法,进行二次加密。接收端对收到的信号进行相应的图像解密,恢复出原始图像,实现对图像复合和串接加密,发挥各自的优点,使其通信系统具有恢复精度和保密度高、破译难度大、执行速度快的特点,以提高保密通信的安全性。计算机仿真结果表明该方案的有效性。

关键词:Logistic 映射;Arnold 变换;混沌序列;图像保密通信
中图分类号:TN911.73 **文献标识码**:A

Novel design of image secure communication system

LV En Sheng, PEI Dong
(College of Physics and Electronic Engineering, Northwest Normal University, Lanzhou 730070, China)

Abstract: In this paper, a new technology of image security communication is presented. It uses the sensibility and pseudo-randomness of chaos sequence for the initial value, and it also adopts a combined method of using Logistic mapping sequence to perform scrambling encryption for the pixel value of image and using Arnold transform to perform scrambling encryption for the pixel position at the sending terminal, so as to perform secondary encryption. The receiving terminal performs corresponding image encryption for received signal to resume original image. Therefore, the recombination of image and cascading encryption can be realized and their advantages can be presented, this will ensure the communication system with features of high precision, excellent security, difficult to decode and fast in execution speed, so as to improve security of the encryption system. The computer simulation results show that the scheme is effective.

Key words: Logistic map; Arnold transformation; chaotic sequence; image secure communication

由于 Internet 网的基础协议 TCP/IP 不是一种安全的协议,未经特殊加密的信息在网络上传送时都会直接暴露在整个网络上,而数字图像作为多媒体信息中最重要的信息表达形式,具有形象、直观和生动的优点,已经成为当今乃至今后信息表达方式的主流。但通过网络传播时很容易被恶意攻击者轻易地浏览、窃取、窜改、非法复制与传播,由此可见,数字图像带给人们生活便利的同时也存在着诸多的安全隐患。这些图像所包含的信息,有的涉及到个人的隐私和生命的安全、有的涉及公司的巨大商业利益、有的甚至涉及到国计民生和国家安全[1],其价值无法衡量,因此不同程度地需要保密,尤其是 Internet 的安全性能越来越受到广泛关注和重视。本文将结合混沌保密通信技术对数字图像的加密和解密进行探讨。

混沌是指由确定性非线性系统中出现的一种复杂类随机行为。混沌系统具有对初始条件的极端敏感性,系统的未来行为是不可预测的。初始条件的微小差异将导致混沌系统的轨道演化很快变得互不相关,混沌系统的特性恰恰符合现代密码学随机数发生器的特征,同时,混沌系统的表现形式非常复杂,具有类噪声、非周期性连续宽带频谱等特点,也使它具有天然的隐蔽性。但混沌系统又具有确定性,是确定性非线性系统产生不确定的信号,其状态完全可以重现,所以将混沌信号引入保密通信领域,具有极其广阔的前景。

图像像素值置乱对于唯密文攻击具有较强的安全性,但对于已知明文的攻击,存在一定的安全隐患;图像

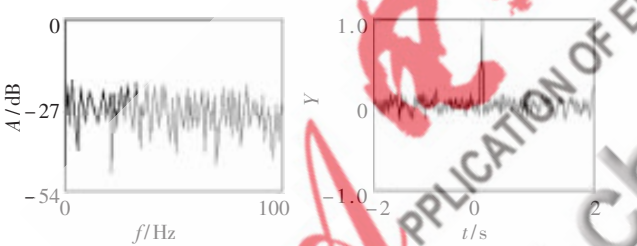
像素位置置乱只改变了图像的位置，不改变图像像素值，攻击者可以通过像素比较的方法加以破解。因此像素值置乱和像素位置置乱相结合成为通信保密技术发展的必然[1]。本文首先用 Logistic 映射产生的混沌序列对图像进行像素值置乱[2]，然后采取 Arnold 变换产生的序列对像素位置置乱进行置乱加密[3-4]。Logistic 映射和 Arnold 变换相互复合和串联，产生的混沌序列具有更逼近于高斯白噪声的统计特性。对图像进行加密和解密的结果显示，算法程序具有精确恢复、保密程度高、执行速度快的优点。理论和仿真研究表明了这种算法的合理性和可行性。本算法程序是按二进制位读入，可以对其他类型的文件如文本、语音、视频等进行加密和解密。

1 Logistic 映射

Logistic 映射[5]是应用得比较广泛的非线性混沌信号发生器，它的动力学方程为：

$$x_{n+1}=\mu x_n(1-x_n) \tag{1}$$

式中，x 为自变量，μ 为参变量。自变量 x 是二次代数方程，由于归一化 x 在 0~1 之间。μ 取值在 0~4 之间，其中取 3.58~4 时呈现混沌状态，图 1 所示为 μ=3.85 时的有关波形。计算其李亚谱诺夫指数为 0.692 9 左右，理论计算表明，此时信号处于混沌状态，两序列的互相关特性小，接近于 0，输出的信号具有良好的非周期性连续宽带频谱白噪声特性，表明 Logistic 映射具有良好的保密性。



(a)混沌信号频域波形 (b)混沌信号自相关波形

图 1 μ=3.85 时混沌信号频域及自相关波形

2 Arnold 变换

Arnold 变换又称猫脸变换[6-7]，根据所选择不同的相位空间可分为二维、三维甚至 N 维的 Arnold 变换。对于一幅 $N\times N$ 的二值图，本文将基于像素点坐标离散化的 Arnold 变换图像位置置乱定义为：

设像素的坐标 $x,y\in S(S=\{0,1,2\cdots N-1\})$，Arnold 变换为：

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

其中，$\begin{bmatrix}1&1\\1&2\end{bmatrix}$ 为变换矩阵，(x,y) 表示原图像某像素点，(x',y') 表示置乱后的像素点，N 是图像的阶数。记变换中的矩阵为 A，反复进行这一变换，则有迭代公式：

$$Q_{ij}^{n+1}=AQ_{ij}^{n}(\mathrm{mod}\ N),n=0,1,2,\cdots \tag{3}$$

其中，$Q_{ij}^{0}\in S$，$Q_{ij}^{n}=(i,j)^{\mathrm{T}}$ 为迭代至第 n 步时点的位置。

Arnold 变换可以看做是裁剪和拼接的过程，猫映射将离散化的数字图像矩阵 S 中的点重新排列，通过这种反复变换的结果，原始图像的像素点变得杂乱无章，出现相当程度的混乱，从而达到加密的效果。

3 图像保密通信的思想

3.1 加密方法

3.1.1 图像像素值按“异或”置乱

按位“异或”的规则是：参加运算的 2 个二进制位同号，结果为 0，否则结果为 1。图像像素值置乱的基本原理是利用具有逼近于高斯白噪声统计特性的混沌信号 $c(n)$ 对需要保密的信息 $s(n)$ 进行置乱，本文置乱的方法是按位“异或”形成像素值置乱信号 $d(n)$。利用 Logistic 映射中的 μ 或者 x_0 参数的 1 位或者 2 位作为密钥 1，Logistic 映射产生混沌序列，即密码流，舍弃序列的前 m 项，以增强加密效果，然后与读入的图像数据进行“异或”方式对图像像素值置乱，完成对图像数据的像素值加密。

3.1.2 图像位置置乱

对二值图像 $d(n)$ 进行 Arnold 变换，得到二值图像 $g(n)$，其中 $k(n)$ 为变换次数作为密钥 2，由用户指定，以打乱二值图像中像素间的逻辑关系，对图像位置加密。

3.2 解密方法

信道的接收端得到二值图像 $g(\hat{n})$，利用密钥 $2k(\hat{n})$ 对二值图像 $g(\hat{n})$ 进行 Arnold 逆变换，得到的二值图像 $d(\hat{n})$，然后输入密钥 1，Logistic 映射产生混沌序列，分别舍弃序列的前 m 项，用这个序列分别与半解密图像 $d(\hat{n})$ 的相应点“异或”，即去掉混沌信号 $c(\hat{n})$，得到的解密二值图像 $s(\hat{n})$。

3.3 算法步骤

(1)输入原始图像 $s(n)$。

(2)输入密钥 1(x_0=0.6+10^{-15})，Logistic 映射的初始值 μ=4，舍弃前 50 项，产生混密码流 $c(n)$，对图像数据 $s(n)$ 进行“异或”方式的混沌掩盖，得到初次加密图像 $d(n)$。

(3)将加密图像 $d(n)$ 用 Arnold 方法进行 30 次置乱，得到最终加密图像 $g(n)$，通过信道发射。

(4) 将从信道接收的图像 $g(\hat{n})$ 用 Arnol 方法进行 30 次逆变换，得到解密图像 $d(\hat{n})$。

(5)输入密钥 1(x_0=0.6+10^{-15})，Logistic 映射的初始值 μ=4，舍弃前 50 项，产生混密码流 $c(\hat{n})$，对解密图像 $d(\hat{n})$ 进行“异或”方式的混沌解密，得到解密图像 $s(\hat{n})$。

(6)输出原始图像 $s(\hat{n})$。

图像保密、解密实现通信原理框图如图 2 所示。

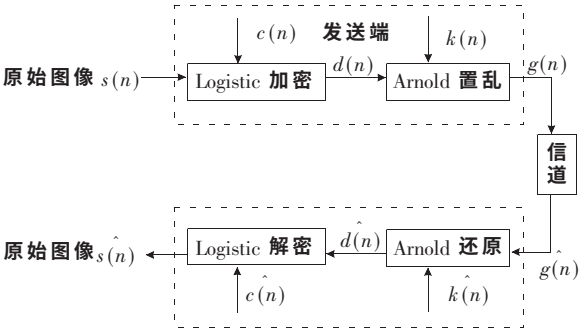
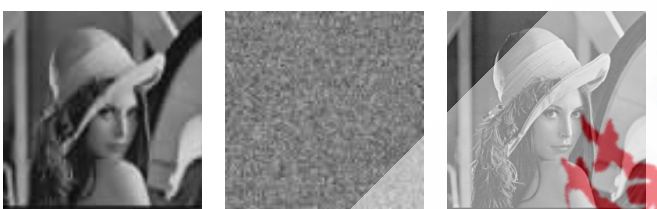


图 2 图像保密解密实现通信原理框图

3.4 仿真结果和分析

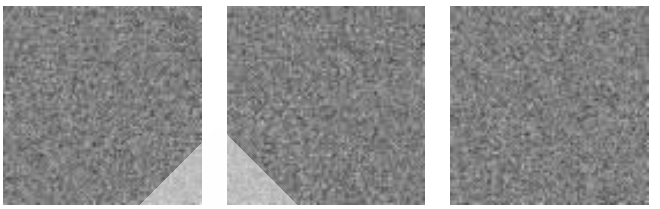
本文对二值图像进行 30 次 Arnold 变换，Logistic 映射在系数 $\mu=4$，初始值 $x_0=0.6+10^{-15}$ 时产生的混沌序列加密。图3 是图像加密解密的仿真结果。由图可见，经复合加密后的二值图像已经不能被辨认，已经不具有原图像的任何信息。而解密图像后与原图像一致。



(a)原始图像 (b)经 Arnold 变换和 Logistic 映射复合加密后的图像 (c)参数均正确解密图像

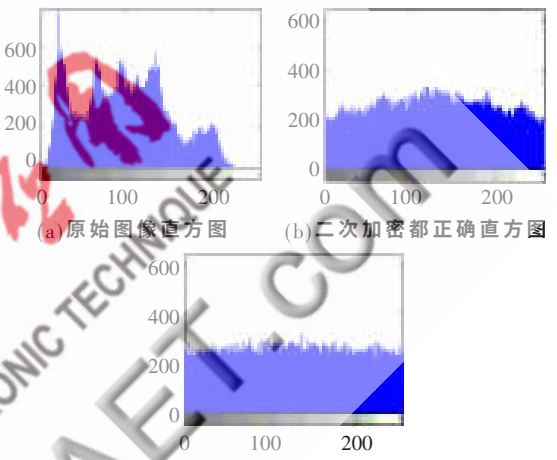
图 3 图像加密解密结果

为了研究本方案的安全性能，本文还仿真了在 Logistic 映射初始密钥和参数与初值相差甚微的情况下得到的解密图像。仿真结果表明，只有在 Arnold 变换密钥正确、Logistic 映射初始密钥和参数均正确的情况下，恢复的图像与原图像差别不大。如果 Arnold 逆变换 31 次(正确 30 次)，而 Logistic 映射的参数正确的初始值得到的图像如图 4(a)所示；Arnold 逆变换 30 次，Logistic 映射参数 $\mu=4$，$x_0=0.6-10^{-15}$(正确 $0.6+10^{-15}$)时得到的图像图 4(b)所示；Arnold 逆变换 31 次，Logistic 映射参数 $\mu=4$，$x_0=0.6-10^{-15}$ 次两次解密密钥均不正确时解密的图像如图 4(c)所示。从图 4 仿真的结果看出，本方案的密钥敏感性强，只要密钥使用只有 1 位不正确时，即使是初始值和密钥有一点差别就恢复不出原图像，因此本方案的安全性能很高。从图 5 加密前后的结果进行比较可知，加密后的图像的直方图得到了更好的均衡分布，基本上不能分辨出原有直方图的分布规律，错误的解密图像的直方图也具有很好的均衡分布，非常好地掩盖了原始图像的分布规律，因而具有很好的加密效果，可以满足对图像加密的安全需要。为了不被穷举攻击解密图像，图像加密方案应该具有尽可能大的密钥空间。在混沌序列的产生过程中，Logistic 映射分别需要 1 个控制参数和 1 个初值，Arnold 变换 1 个初始值，均作为密钥。设计算精度为 10^{16}，则混沌密钥产生的过程中的密钥空间为 10^{48}，对图像加密来说，此密钥空间已足够大，使穷举攻击几乎不可能成功。



(a)Arnold 变换密钥错误 (b)Logistic 映射初始参数错误 (c)参数和密钥均错误

图 4 错误的解密结果



(a)原始图像直方图 (b)二次加密都正确直方图 (c)二次密钥均错直方图

图 5 保密解密的图像直方图

本设计采用对图像像素值置乱和图像像素位置置乱相结合的保密技术，克服了 Arnold 变换密钥过短，Logistic 映射针对低维的混沌系统的缺陷，比任意一种加密技术单独使用时的保密性能都好，两者优势互补，缺点彼此得到抑制。仿真结果表明，两种保密技术的复合和串联，对图像的数据和像素位置均进行加密，不但新颖，而且加密效果也比较理想。本方案在利用混沌动力学机制的良好性质实现对传统加密技术的改进方面迈出了成功的一步。

参考文献

[1] GAO T G,CHEN Z Q. A new image encryption algorithm based on hyper-chaos [J]. Physics Letters A 2008,372(4):394-400.

[2] 邓绍江，肖迪，涂凤华.基于 Logistic 映射混沌加密算法的设计与实现 [J]. 重庆大学学报 (自然科学版)，2004，27(4):61-63.

[3] WANG Y, WONG K W, LIAO X F, et al. Chaos-based image encryption algorithm with variable control parameters [J]. Chaos, Solitons and Fractals 2009,41(4):1773-1783.

[4] 丁玮，闫伟齐，齐东旭.基于 Arnold 变换的数字图像置乱技术 [J]. 计算机辅助设计与图形学学报，2001，13

(4):338-341.
[5] 刘文波.Logistic 映射的电路实现及应用[J].数据采集与处理,2001,21(1):129-132.
[6] CHEN G, MAO Y B, CHUI C K. A symmetric image encryption scheme basedon 3D Chaotic Cat Map [J]. Chaos, Solitons&Fractals, 2004,21(3):749-761.
[7] 郑凡.基于混沌的数字加密技术应用研究[D].长春:吉林大学,2008.

(收稿日期:2010-01-13)

作者简介:
吕恩胜,男,1981 年生,硕士研究生,主要研究方向:电路理论与应用、通信信号处理。
裴东,男,1965 年生,副教授,硕士研究生导师,主要研究方向:电路理论与应用。