基于 Lorenz 混沌系统的数字视频加密 *

姚翔辉，禹思敏

（广东工业大学 自动化学院，广东 广州 510006）

摘 要：为解决视频信息的安全问题，研究了一个基于 Lorenz 混沌系统的视频加密方案。该方案首先将三维 Lorenz 混沌系统进行离散化处理，然后运用驱动式响应同步的方式进行同步处理，对随机采集到的 AVI 视频文件进行混沌加密。通过采用 Matlab 仿真软件，编写相应的加解密程序进行仿真，最后，对仿真实验结果进行分析，结果表明该方案具有安全性高、灵活性好的特点。

关键词：Lorenz 混沌系统；视频加密；驱动响应同步

中图分类号：TN910;TN918 **文献标识码**：A **文章编号**：1674-7720(2011)04-0041-03

Digital video encryption based on Lorenz chaotic system

Yao Xianghui, Yu Simin

(College of Automation, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: To address the safety of video information, a digital video encryption based on Lorenz chaotic system is studied. Firstly, three-dimensional Lorenz chaotic system is discreted. Then use the corresponding synchronous manner to drive synchronization. Use random collection of AVI video files to the chaotic encryption. By using Matlab simulation software, preparation of the corresponding encryption and decryption process simulation. Finally, analysis of simulation results shows that the scheme has high security, flexibility.

Key words: Lorenz chaotic system; video encryption; driven response synchronization

Shannon 在经典论文中指出，好的加密系统应具有对密钥的敏感性，以及能够将明文充分地置乱并改变其统计特性，而这正是与混沌迭代特性相一致的。同时，混沌的拓扑传递类似于密码的扩散，混沌对参数的敏感性则对应着密码对密钥的敏感性。于是，可以利用混沌的特性来设计序列密码或者分组密码，特别是分组密码，利用混沌的拓扑传递特性来快速地置乱和扩散明文数据，以达到改变明文统计特性的目的[1-4]。

近年来，混沌保密及其应用成为了信息安全领域的一个研究重点，特别是混沌数字图像、语音及视频加密问题引起了研究者的极大关注。但目前对混沌保密的研究主要局限于数字图像和语音的加密，而对于有关视频加密的研究却非常少，传统的加密算法如 DES、IDEA、Blowfish、RSA 等，理论上可以用于数字视频加密，但上述方法并未考虑到视频文件的自身特点，势必会导致文件的结构被破坏，又因为视频文件的海量特性，上述算法加密的速率无法得到保证。因此研究新的安全性高且加密速度快的视频加密算法是非常必要的[5-13]。

本文提出了用三维 Lorenz 混沌系统和 Matlab 仿真工具实现混沌数字视频加密。利用 Matlab 工具产生 AVI 视频信号，同时，利用混沌序列对初始条件和系统参数非常敏感的特性，采用驱动响应式同步的加密算法方案，对产生的 AVI 视频进行加解密，最后通过将混沌序列的初始条件和系统参数进行微弱调整，对仿真结果进行深入分析。

1 AVI 视频文件结构特点

音频视频交错格式 AVI(Audio Video Interleaved)是将语音和影像同步组合在一起的文件格式。它对视频文件采用了一种有损压缩方式，但压缩比较高，AVI 支持 256 色和 RLE 压缩，一个 AVI 文件可以包含多个不同类型的媒体流，它以一系列的位图来存储视频信息，并在文件中加入以数字形式存储的数字化视频信息。

AVI 包含三部分：文件头、数据块和索引块。其中文件头包括文件的通用信息，定义数据格式及压缩算法等参数。数据块包含实际数据流，即图像和声音序列数据，

* 基金项目：广东省自然科学基金项目(8151009001000060)

是文件的主体，也是决定文件容量的主要部分。视频文件的大小等于该文件的数据率乘以该视频播放的时间长度。索引块包括数据块列表和它们在文件中的位置，以提供文件内数据随机存取能力。

2 Lorenz 混沌系统与离散化处理

使用一个 Lorenz 混沌系统来进行 AVI 视频文件的加密和解密，Lorenz 系统的无量纲状态方程数学表达式为[14]：

$$\begin{cases} dx/dt=-a(x-y) \\ dy/dt=bx-xz-y \\ dz/dt=-cz+xy \end{cases} \quad (1)$$

利用 Euler 算法对式(1)作离散化处理，得到离散化后的迭代方程为：

$$\begin{cases} x(n+1)=-(aT)(x(n)-y(n))+x(n) \\ y(n+1)=T(bx(n)-x(n)z(n)-y(n))-y(n) \\ z(n+1)=T(-cz(n)+x(n)y(n))+z(n) \end{cases} \quad (2)$$

式中 $T=0.05$ 为取样时间，a、b 和 c 为系统参数，其中 $a=10, b=30, c=8/3$。

根据式(1)和式(2)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，图 1 所示为 $x-y$ 方向上的 Lorenz 混沌系统吸引子相图。

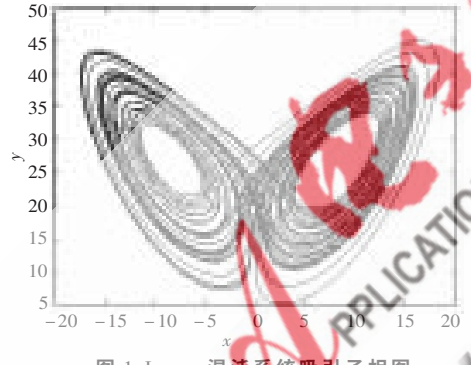

图 1 Lorenz 混沌系统吸引子相图

3 基于 Lorenz 混沌系统的视频加密算法设计

3.1 AVI 视频文件的读入

利用随机采样到的一段 AVI 视频进行混沌加密，由于 Matlab 中只支持 ZJmedia Umcompress RGB24 编码方式的 AVI 视频文件，因此首先有必要把采集到的这段视频文件进行转换处理，使其能够无障碍地载入到 Matlab 工具中。利用专业的转换软件 Winavi 进行操作，视频经过相应的处理之后，读入到 Matlab 工具当中去。

3.2 视频加密方案

根据密码学原理，首先要把视频信息进行置乱处理，然后利用混沌系统来进行扩散加密。

利用式(2)中的混沌系统状态方程，经过离散化之后来实现数字视频混沌加密。在驱动响应式同步的基础上，加入信号后再形成一个闭环和反馈，使驱动系统和响应系统有同步信号，工作原理如图 2 所示。

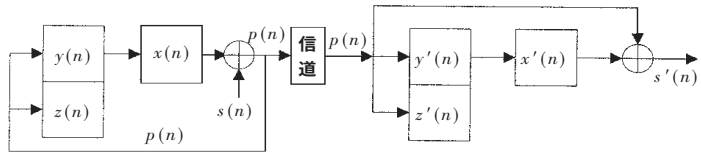

图 2 数字视频混沌保密通信系统

在这里，利用 Lorenz 系统的 x 变量作为驱动信号对视频信号进行加密，由图 2 可知，加密信号为 $p(n)=x(n)+s(n)$，于是，由式(2)得到发送端的迭代方程为：

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

其中，$s(n)$ 为原始的视频信号，而 $x(n)$ 则为 Lorenz 混沌系统的驱动信号，本文采用数字相加的方式来进行覆盖。

在接收端，解密后的图像信号为 $s'(n)=p(n)-x'(n)$，接收端的响应状态方程为：

$$\begin{cases} x'(n+1)=-(aT)(x'(n)-y'(n))+x'(n) \\ y'(n+1)=T(bp(n)-p(n)z'(n)-y'(n))-y'(n) \\ z'(n+1)=T(-cz'(n)+p(n)y'(n))+z'(n) \end{cases} \quad (4)$$

其中，通过 $s'(n)=p(n)-x'(n)$ 的操作之后，$s'(n)$ 是经过解密之后的信号，而 $x'(n)$ 信号只有在该系统能实现驱动响应式同步的基础上，才能和信号 $x(n)$ 相等。

通过在 Matlab 软件上编程之后验证可以得到，Lorenz 系统完全能够实现驱动响应式同步，其仿真结果如图 3 所示，其中横坐标代表发送端信号 $x(n)$，而纵坐标则为接收端的信号 $x'(n)$，从图中可以看出，二者是严格同步的。

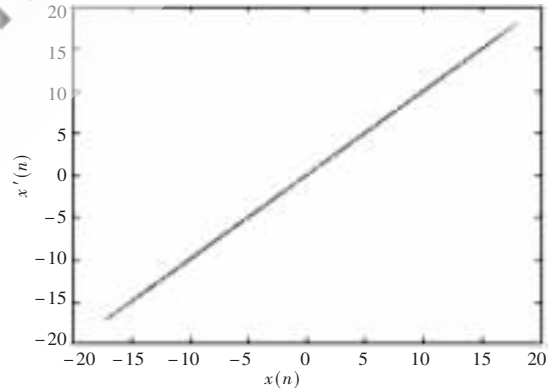

图 3 Lorenz 系统同步

4 Matlab 仿真结果及分析

4.1 仿真结果

在 Matlab7.1 的工作平台下，按照上文提出的加密方案编写相应的程序对视频文件“original.avi”进行加密与解密，Lorenz 系统的初始值 (x_0, y_0, z_0) 取为 $(0.01, 0.02, 0.03)$，图 4～图 7 是加解密的实验结果，其中图 4 显示的是原始视频中的最后一帧原始图像，图 5 是最后一帧原始图像经过混沌系统加密后的效果图，图 6 是在系统参数完全一致

以及初始条件(x_1,y_1,z_1)改为(10,20,10)的情况下解密出来的图像效果图,图 7 则是修改了系统参数 b 为 30.000 01 之后的效果图。

4.2 结果分析

在采用上述加密算法之后,用 Matlab 仿真工具编程对"original.avi"进行仿真实现,由结果可以发现,由于是视频加密,因此只能分析单一的一帧图像,如图 5 所示,是加密之后最后一帧的图像,加密效果相当不错,完全看不出视频文件的内容。当在 Lorenz 混沌系统初始条件(x_0,y_0,z_0)不同和而系统参数(a,b,c)完全匹配的情况下,得到解密的最后一帧的图像如图 6 所示,完全和原始图像一样,解密效果非常明显。然后,调整系统参数 b,把 b 的值重新取为 30.000 01 时,得到如图 7 所示的解密效果图,解密出来的图像已经无法看清了,非常模糊,这说明此种加密算法具有很高的安全性,该系统的安全性主要来自于发送端与接收端参数失配的高度敏感性。

图 4 原始视频的最后一帧图像

图 5 加密后的最后一帧图像

图 6 改变初始条件后解密出的图像

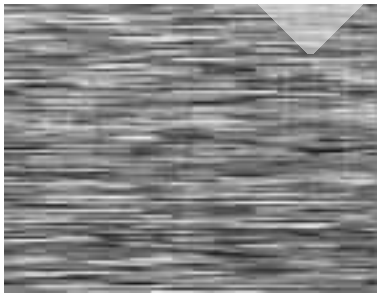

图 7 参数 b=30.000 01 时的解密图像

根据以上仿真结果和分析,混沌本身具有实现密码的许多优点,其内在的带有确定性的随机性和计算复杂度低的特点具有很大的吸引力。目前,国内外学者将混沌加密理论应用到视频加密的还不多,主要集中在直接加密方面,没有利用视频数据本身的特性和选择性加密的优点,没有很好地结合视频压缩标准方面的研究,因此很难提高其实用性和实时性。将混沌加密与选择性加密相结合,是今后混沌保密算法方面一个重要的发展方向。

参考文献

[1] 王培荣,徐结,付冲.一种符合混沌数字图像加密算法[J].通信学报,2006,27(1):1-4.

[2] 张爱华,江中勤.基于 Logistic 映射的混沌图像加密算法的改进[J].南京邮电大学学报,2009,29(4):69-73.

[3] 陈关荣,汪小帆.动力系统的混沌化:理论、方法与应用[M].上海:上海交通大学出版社,2006.

[4] 毛明.大众密码学[M].北京:高等教育出版社,2005.

[5] KOCAREV L,JAKIMOSKI G. Logistic map as a block encryption algorithm[J].Physics Letters,2001(A289):199-206.

[6] 匡锦瑜,邓昆,黄荣怀.利用时空混沌同步进行数字加密通信[J].物理学报,2001,50(10):1856-1861.

[7] ZHANG Y, DAI M, HUA Y. et al. Phys.Rev, 1998(E58): 3022.

[8] LU J H,YU S M,HENRY L,et al.Experimental verication of multidirectional multiscroll chaotic attractors[J]. IEEE Trans.Circuits Syst.(part-I),2006,53(1):149-165.

[9] ZHOU C, LAI C. Phys,Rev,1999(E60):320.

[10] LV Jin Hu, CHEN Guan Rong. Generating multiscroll chaotic attractors:theories methods and applications[J]. International Journal Bifurcation Chaos,2006,16(4):775-858.

[11] 黄丽莲,尹启天.基于输出控制的混沌同步保密通信系统[J].电子与信息学报,2009,31(10):2402-2405.

[12] JIANG Z P. A note on chaotic secure communication systems.IEEE Transcations on Circuits and Systems-I 2002,49(1):92-96.

[13] ZOU Y L, ZHU J. Controlling the chaotic n-scroll Chua's circuit with two low pass filters[J].Chaos, Solitons and Fractals,2006,29(2):400-406.

[14] LORENZ E N, ATMOS J. 1963 Sci.20 130.

(收稿日期:2010-11-15)

作者简介:

姚翔辉,男,1985 年生,硕士研究生,主要研究方向:FPGA,混沌保密通信。