文章编号：2095-2163(2019)06-0065-04 中图分类号：TP393 文献标志码：A

# 基于混沌密码的监控视频加密技术研究

徐 辉，佟晓筠

（哈尔滨工业大学 计算机科学与技术学院，哈尔滨 150001）

**摘 要**：由于公用网络处于完全开放的状态，一些涉及机密或隐私的视频数据是不能直接传输的，必须采取某种技术手段对视频信息进行保护。视频加密是一种有效的安全防护手段，而传统的加密算法计算复杂度高不适用于加密视频信息。本文对经典混沌系统进行改进，提出了一种新的混沌流密码，该密码系统安全性高、运行速度快，可以满足视频应用的实时性要求。同时，针对压缩后的视频监控码流进行码流分析和数据提取，在确保码流格式兼容性的前提下，对视频数据部分进行加密操作，实现了监控视频数据的实时加密传输。

**关键词**：混沌密码；视频编码；视频加密

# Research on monitoring video encryption technology based on chaotic cipher

XU Hui, TONG Xiaojun

(School of Computer Science and Technology, Harbin Institute of Technology, Harbin, 150001, China)

**【Abstract】** With the rapid development of computer network communication technology and video compression coding technology, video applications based on network transmission have become an indispensable part of people's lives. However, since the public network is completely open, some video data involving confidentiality or privacy cannot be directly transmitted, and some technical means must be used to protect the video information. Video encryption is an effective security protection method, and the traditional encryption algorithm cannot apply to encrypt video information due to high computational complexity. At the same time, the code stream analysis and data extraction are performed on the compressed video surveillance code stream. Under the premise of ensuring the compatibility of the code stream format, the video data part is encrypted, and the real-time encrypted transmission of the monitoring video data is realized.

**【Key words】** chaotic cipher; video coding; video encryption

## 0 引 言

近年来，随着网络技术、传输技术和视频压缩等相关技术的不断发展，网络视频监控系统在智能交通、智能楼宇、银行、商场超市、医院校园、企业生产和生活小区等范围内得到了广泛应用，已经渗透到了生产生活中的各个领域，具有直观、方便和信息量丰富等特点。视频监控系统随着相关技术的不断进步和发展，经历了 3 个发展阶段[1]：

(1)模拟监控。视频以模拟方式采用同轴电缆进行传输，并由控制主机进行模拟处理。

(2)半数字监控。视频仍以模拟方式采用同轴电缆进行传输，但数据通过硬盘录像机(VDR)进行处理、存储。

(3)网络多媒体的数字视频监控。被采集的视频信号被数字化，经过压缩编码在数字通讯线路上进行传输，采用流媒体技术实现视频在网络上的多路复用传输。

视频监控系统将现场的图像和声音全天候地记录下来，并实时地传送到控制中心，可使相关人员对各个现场情况了如指掌，对出现的各种情况进行处理，而且还可以在需要的情况下回放相关的历史资料。网络视频监控系统对安防、管理等提供了极大的方便。然而，视频应用给人们带来极大便利条件的同时，也面临着内容窃取、非法传播、信息泄露、隐私曝光等安全风险。因此，建立有效的视频内容保护机制是推动视频商业化应用不断发展的重要保障。视频加密技术是视频数据保护的重要手段，其利用密码技术将视频原始信息掩盖，从而使非法入侵者无法获得可理解的视频内容或高质量的视频版本。视频加密的更重要的意义在于其破坏了原始视频的可视性和商业价值。蔡勉等[2]提出了利用输出反馈模式 OFB 对 H.264 少量视频数据进行加密的算法；唐峰[3]等人提出对 DCT 的系数符号以及部分 DCT 系数值加密的方法，适合视频安全传输的要求，但这类视频加密算法的安全性不高。熵编码是

**作者简介**：徐 辉(1982-)男，博士研究生，主要研究方向：混沌密码、多媒体信息安全；佟晓筠(1963-)女，博士，教授，博士生导师，主要研究方向：混沌密码、信息安全。

**收稿日期**：2019-03-22

视频压缩编码的最后一个关键环节,许多研究人员在这个阶段对部分视频语法元素进行加密,取得了较好的加密效果[4-6],但这类方法又不适用于压缩后的监控视频流。Ting[7]采用传统 AES 密码算法对压缩后的视频码流数据进行加密,但其计算时间开销较大,无法满足实时传输的要求。Fadi[8]对实时传输的视频数据进行分组,通过对信息位的随机替代和置乱的方式达到加密目的。

尽管目前针对视频内容的保护提出了许多加密方案,但是尚没有一个专门针对视频监控的加密算法可以同时满足安全性和实时性要求。因此,本文提出了一种高效安全的混沌流密码,对压缩后的视频监控码流进行加密,实现对视频内容的有效保护。

## 1 混沌伪随机序列

### 1.1 经典混沌系统

Logistic 混沌系统是近年来被广泛研究的一维非线性系统,其数学定义为:

$$x_{n+1} = \mu x_n(1 - x_n)\ \mu \in (0, 4),\ x_n \in [0,1], \quad (1)$$

其中,当$\mu \in (3.569\ 9, 4]$时,系统处于混沌状态[9]。

Hénon 混沌系统是另一个被广泛关注的二维混沌映射,其数学定义如下:

$$\begin{cases} x_{n+1} = 1 + y_n - ax_n^2, \\ y_{n+1} = bx_n. \end{cases} \quad (2)$$

当参数 $a = 1.4, b = 0.3$ 时, Hénon 映射将处于混沌状态。

美国气象学家 Lorenz 在 1963 年研究大气环流模型时发现了一个蝴蝶状的奇怪的吸引子,即 Lorenz 系统。Lorenz 混沌系统的数学表达如式(3)所示。

$$\begin{cases} \dot{x} = -a(x - y), \\ \dot{y} = cx - y - xz, \\ \dot{z} = xy - bz. \end{cases} \quad (3)$$

当系统参数 $a = 10, b = 8/3, c = 28$ 时,该系统处于混沌状态。

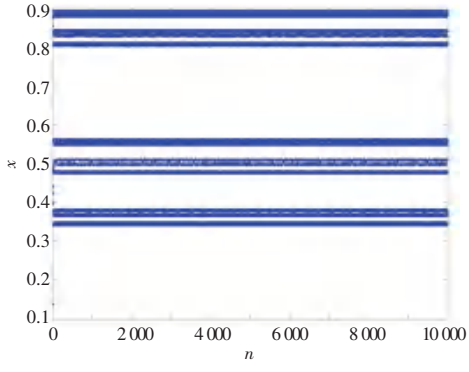
### 1.2 改进的一维混沌模型

Logistic 系统的混沌参数区间很窄,相空间轨道分布也不均匀,将其直接用于构造混沌流密码是不安全的。为此,本文提出了一种新的一维混沌系统(NOC,new one-dimensional chaotic),其数学表达式为:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)|. \quad (4)$$

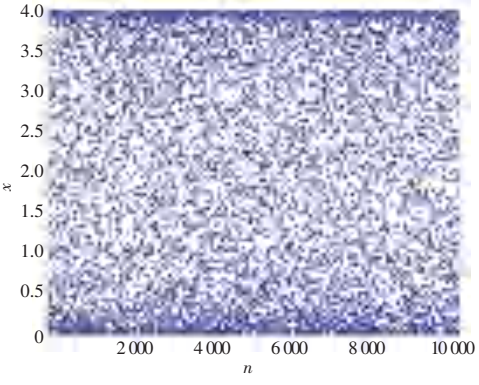
$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)|$ 是系统状态值,$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)|$ 是控制参数,当 $\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)|$ 时,该系统处于混沌状态。

图 1 给出了 Logistic 系统和 NOC 系统的空间遍历图,从图 1(a)中可以看到 Logistic 系统在参数 $\mu = 3.57$ 时,存在多个周期窗口,而图 1(b)中的 NOC 系统没有发现明显的周期窗口。




(a) logistic_μ = 3.57

(a) logistic_μ = 3.57




(b) NOC_a = 1

(b) NOC_a = 1

**图 1 Logistic 和 NOC 的空间遍历**

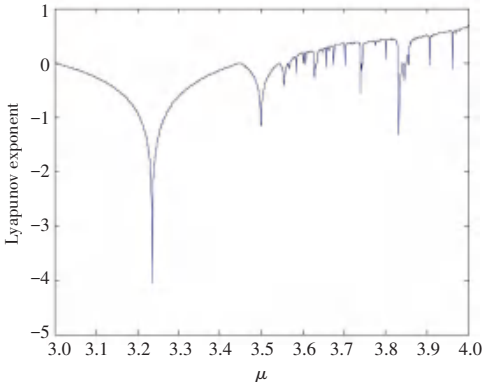
**Fig. 1 Spatial traversal of Logistic and NOC**

李雅普诺夫指数(Lyapunov exponent, LE)是表征混沌系统的重要指标,若一个非线性系统是混沌的,则至少要有一个 LE 是正的。设 $f(x)$ 是一个可微函数,则 LE 定义为:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)|. \quad (5)$$

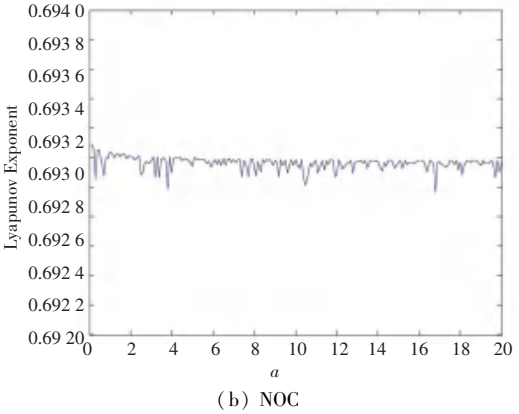
图 2 分别给出了 Logistic 和 NOC 的李雅普诺夫指数谱。从图 2 中可以看出,Logistic 映射的 LE 有较大波动,其大于零的区间很窄,而且只有当参数等于 4 时,才达到最大值 0.693 1。相比之下,NOC 的

李雅普诺夫指数不论参数如何变换，都始终维持在 0.693 2 左右，说明 NOC 系统具有更高的混沌稳定性。




（a）logistic

（a）logistic




（b）NOC

（b）NOC

**图 2　李雅普诺夫指数谱**

**Fig. 2　Lyapunov exponent spectrum**

### 1.3　混沌序列产生器

由于混沌序列是在实数域范围内的，不能直接用作密码来使用，因此必须采用某种策略将其转换为整数域内的序列。这里设 $\{X \mid x_i,\ i = 1,2,3\ldots,N\}$ 是混沌序列，$z_i$ 是整型量化后的序列值，由公式（6）计算得出。

$$z_i = floor\ (x_i * 10^{13})\ \ \mathrm{mod}\ 2^{32}. \tag{6}$$

$floor(\ )$ 表示向下取整，$mod$ 表示取模。每次运算将产生一个整数 $z_i$，且其范围是 $(0,\ 2^{32})$，因此量化后的整数伪随机序列表示为：$Z = z_0 z_1 z_2 \ldots z_i \ldots$。

## 2　H.264 的码流分析及加密算法

现在大部分的摄像头采集到图像后都会利用压缩编码技术将视频图像压缩，而这其中应用最广泛的压缩标准就是 H.264。编码器对视频数据压缩编码后形成视频码流，然后通过网络传输协议进行转发。因此对视频内容的加密，需要考虑到视频的码流格式，确保加密过程不破坏原有视频码流结构，使得解码器可以正常解码，不需要额外的计算开销。

（1）IDR 帧分析。IDR 帧是视频的第一帧数据，其后面的 P 帧和 B 帧将参考 IDR 帧进行帧间预测，因此对 IDR 帧的加密将直接影响后续视频图像质量。在网络提取层单元（NAL），IDR 帧以“00 00 00 01 65”开头，因此，从该序列之后到下一个 NAL 之前的内容为加密对象。

（2）参数集分析。在视频码流中有 2 个单元的数据是不能被加密的，一个是序列参数集，另一个是图像参数集。分别以“00 00 00 01 67”和“00 00 00 01 68”开头。这两部分包含了视频解码的所有参数和控制信息，如果对其加密，则解码器将无法正常解码。

（3）视频加密算法。为确保视频加密格式的兼容性和实时性，将利用改进的一维混沌生成伪随机序列，作为加密密钥流，同时提取视频码流的数据部分，通过与密钥流的数学运算，获得密文视频数据。设密钥流为 $K$，视频明文数据为 $P$，加密后的密文为 $C$，则加密操作为：

$$C = (P + K)\ \mathrm{mod}\ 2^{32}. \tag{7}$$

## 3　实验分析及测试

利用海康威视的网络摄像头进行了加密算法的实验和测试，加密前后视频的图像如图 3 所示。

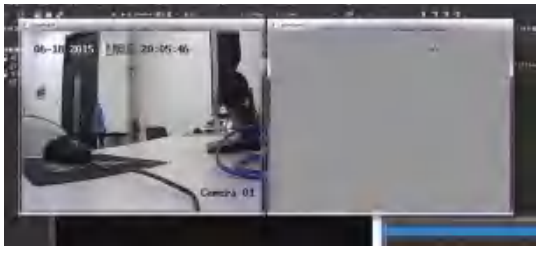


**图 3　视频加密效果**

**Fig. 3　Video encryption effect**

从图 3 中可以看到，视频加密后的图像与原始视频图像完全不同，从中无法辨识视频内容和细节，说明加密算法对实时视频监控码流是有效的。

另外，为了测试该加密算法的时间开销，实验分别截取了 100 帧、200 帧和 300 帧视频作为测试对象，通过测试解码和解密时间来衡量时间复杂度，测试结果见表 1。

从表 1 的数据中可以看出，解密时间与解码时间相比，所占的开销不到 0.1%，因此加解密操作满足视频处理的实时性要求。　（下转第 72 页）