基于三维Lorenz混沌的彩色视频加密

何 晔 王 磊 夏 晖 张学峰
(中石化管道储运公司华东管道设计研究院 徐州 221008)

摘 要 混沌理论应用于加密还是一个比较新的研究领域,现有的基于混沌理论的视频加密大多采用单独的低维映射,安全性不高;而高维混沌系统虽然加密性好,但由于其密钥序列复杂的产生过程与视频加密数据量大、实时性要求高的特点形成矛盾,至今仍鲜有应用。针对于此,结合像素扩散的思想,提出了一种基于三维Lorenz混沌的彩色视频加密算法,该算法遵循香农信息论中的混淆与扩散机制,视频帧中任何一个像素的解密错误都会影响整个视频的解密,具有很高的安全性。此外,该算法还具有加密速度快等优势,解决了高维混沌系统应用于视频加密的难点。

关键词 Lorenz混沌,奇异吸引子,图像加密,视频加密

Encryption Algorithm of Color Video Image Based on Lorenz Chaos

HE Ye WANG Lei XIA Hui ZHANG Xue-feng
(Department of Communication, Pipeline Design & Research Institute of East China, Xuzhou 221008, China)

Abstract Because chaotic encryption is a new area of research, most video encryption algorithms are based on low dimensional maps, and their securities need to be improved. Although the capability of encryption of high-dimensional chaotic system is much more better, the generation process of chaotic sequences are also much more complex. It conflicts with the characteristics of large amount of data and the high real-time requirement of video encryption. Thus the high-dimensional chaotic system is less used in the encryption of video. In light of this, combining with ideas of diffusion of pixels, this dissertation proposed a color video image encryption algorithm based on chaotic Lorenz system. The system follows mechanism of confusion and diffusion proposed by Shannon's information theory. Any pixel in the image which is decrypted incorrectly will affect the whole decryption of the video. The algorithm has a high security, besides it also has the advantage of fast encryption. The algorithm can satisfy the characteristics of video encryption which have a large quantity of data and demand a high real-time.

Keywords Lorenz chaos, Chaotic attractor, Image encryption, Video encryption

1 引言

随着通信技术与计算机技术的迅猛发展,图像和视频信息日益成为人们生活中不可或缺的信息媒介,伴随而来的视频安全与保密问题也成为研究的重点和难点。传统的加密算法大多是针对文本信息,应用于视频加密中有诸多不便[1,2]。近年来对混沌系统的研究发现,它所具有的天然特性与密码学的要求有诸多相似之处[3,4],非常适合于图像和视频的加密,因此迅速成为人们研究的热点。

然而现有的基于混沌理论的视频加密大多采用单独的低维映射[5],其主要缺点是低维映射系统的参数和初始条件较少,密钥空间相对较小,且产生加密序列的轨道相对简单;而高维混沌系统虽然加密效果好,但由于其产生密钥序列的过程复杂,目前还较少应用于数据量庞大、实时性要求高的视频加密中。基于此,本文立足于选择性加密算法,结合像素扩散的思想,提出了一种基于三维Lorenz混沌的彩色视频图像加密算法。该算法不但大大扩大了密钥空间,使产生混沌序列的轨道更加复杂,还严格遵循香农信息论中的混淆和扩散机制即视频帧中任何一个像素的解密错误都会影响整个视频的解密,具有很高的安全性。此外该算法还具有加密速度快等优势,能满足视频加密数据量大、实时性要求高的特点。

2 Lorenz混沌系统

Lorenz系统是经典的三维混沌系统,它是由美国气象学家E. N. Lorenz在研究对流实验时发现的[6]。它的动力学方程式如式(1)所示:

$$\begin{cases}\dfrac{dx}{dt}=\sigma(y-x)\\ \dfrac{dy}{dt}=x(\rho-z)-y\\ \dfrac{dz}{dt}=xy-\beta z\end{cases}\tag{1}$$

Lorenz系统属于耗散系统,它是基于流体力学中的Navier-Stokes方程、热力传导方程和连续性方程构建的。σ,ρ,β是系统的参数,其取值范围是大于0的任意数值,常取$\sigma=10$,$\beta=8/3$,ρ作为变量,当保持σ,β的值不变,$\rho>24.74$时

何 晔(1982-),男,工程师,主要研究方向为中石化长输管道通信设计,E-mail:luckyheye@163.com;王 磊(1982-),女,硕士生,讲师;夏 晖(1980-),男,工程师,主要研究方向为长输管道仪表自动化的设计;张学锋(1984-),男,主要研究方向为线路安全环保。

洛伦兹系统进入混沌状态[7]，当 $\rho=28$ 时，系统达到最佳混沌状态。

当 $\sigma=10,\beta=8/3,\rho=28$ 时，洛伦兹系统产生的混沌吸引子如图 1 所示。

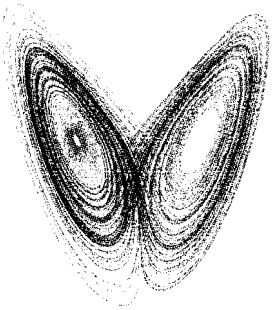


图 1　Lorenz 系统的混沌吸引子

3　基于 Lorenz 混沌的视频加密/解密算法

数字视频在许多方面与静止的图像有相同的特性，因为视频信号本身即是由许许多多幅按照时间序列排列的连续图像组成的，每一幅图像称为帧。此外，视频数据还具有数据量大、冗余度高、实时性要求严格等特点。为了保证流畅的视觉效果，视频加密必须考虑实时在线的能力，要求很高的处理速度。基于此，本文提出了一种新的基于 Lorenz 混沌的视频加密算法，该算法选取能使 Lorenz 系统产生最佳混沌序列的参数取值 $\sigma=10,\beta=8/3,\rho=28$，以 x,y,z 混沌序列作为加密密钥对视频图像进行加密。因为图像像素值的取值范围是[0，255]，所以需要对产生的 x,y,z 混沌序列进行改进，具体过程如下：

$$\begin{cases} x'=|x|-round|x| \\ y'=|y|-round|y| \\ z'=|z|-round|z| \end{cases} \tag{2}$$

式中，$round()$ 的含义是取靠近 0 的整数。经过处理后，新的混沌序列 x',y',z' 的取值范围是[0,1]的任意实数。

该算法的基本思想是：在视频采集的过程中，对采集的每帧图像的每个像素都加入 Lorenz 系统产生的伪随机序列噪声，也就是将混沌系统产生的混沌序列和每一帧的每一个像素逐位处理。首先由 Lorenz 系统产生 x,y,z 混沌序列，然后将 x,y,z 混沌序列分别与每帧图像中对应的 R,G,B 分量值以及前一个像素加密后的 R,G,B 分量值进行异或，从而完成对该帧的加密。在采集的过程中对每一帧图像都做如上处理，进而完成对整个视频的加密。

整个系统加密、解密的算法框图如图 2 和图 3 所示。

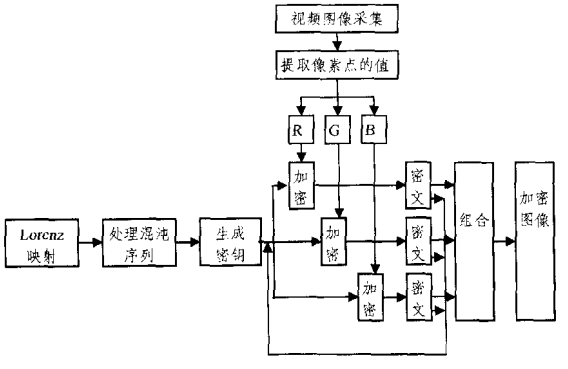


图 2　三维 Lorenz 视频图像加密算法框图

算法中每帧第一个像素加密的过程与其他像素不同，是用对应的混沌序列与该像素以及该帧最后一个像素的 R、G、B 分量值进行异或加密。本算法遵循香农信息论中混乱与扩散的设计准则，且对不同的帧能产生不同的密钥进行加密，既能满足视频实时性的要求，又具有很高的安全性。

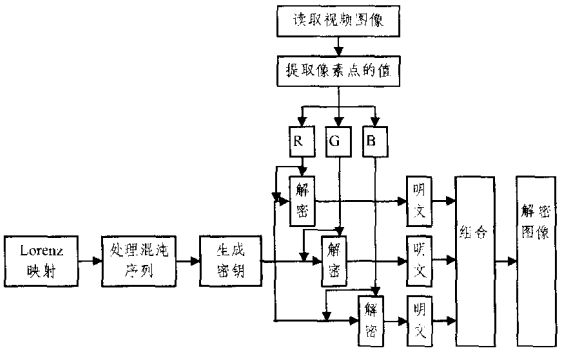


图 3　三维 Lorenz 视频图像解密算法框图

4　彩色视频加密/解密算法的设计

4.1　加密算法的流程

设摄像头采集的视频帧大小为 $M*N$，对视频进行加密的流程如下：

1. 进行视频采集，输入加密密钥 x,y,z 的值。

2. 为了使系统达到充分的混沌状态，先将 Lorenz 系统迭代 1000 次后，截取 $M*N$ 组$\{x,y,z\}$的混沌序列。

3. 将得到的 $M*N$ 组混沌序列按式(2)进行改进，获得新的 $M*N$ 组混沌序列$\{x',y',z'\}$，对序列中的每个值取其第 3,5,7 位形成一个 3 位十进制数，并将该数与 256 取余，得到一个 8 位的密钥流，这样就得到了 $M*N$ 组最终的密钥序列$\{x_k'',y_k'',z_k''\}$，其中 $k\in[1,M*N]$。

4. 按式(3)对帧中的每个像素逐一进行加密，进而加密整个视频帧。

$$\begin{cases} R_k'=R_k\oplus x_k''\oplus R_{k-1}' \\ G_k'=G_k\oplus y_k''\oplus G_{k-1}' \\ B_k'=B_k\oplus z_k''\oplus B_{k-1}' \end{cases} \tag{3}$$

式中，R_k,G_k,B_k 是当前待加密像素点的 3 个分量值，x_k'',y_k'',z_k''分别是与当前像素分量对应的密钥序列值，$R_{k-1}',G_{k-1}',B_{k-1}'$分别是前一个已加密的像素分量值，$R_k',G_k',B_k'$分别是当前像素加密后的 3 个分量值。注意，对每帧图像中的第一个像素进行加密时，$R_{k-1}',G_{k-1}',B_{k-1}'$的取值是取该帧图像中最后一个像素的 R,G,B 值。

5. 显示加密后的视频帧。

6. 重复步骤 4 和 5，完成对整个视频的加密。

4.2　解密算法的流程

1. 读取加密后的视频帧，输入解密密钥 x,y,z 的值。

2. 重复加密的步骤 2 和 3，得到最终的密钥序列$\{x_k'',y_k'',z_k''\}$，其中 $k\in[1,M*N]$。

3. 按式(4)先对加密帧中的第 2 个像素解密，直到解密完最后一个像素，求得最后一个像素的原始值，再完成对第一个像素的解密，这样整帧图像解密完成。

$$\begin{cases} R_k=R_k'\oplus x_k''\oplus R_{k-1}' \\ G_k=G_k'\oplus y_k''\oplus G_{k-1}' \\ B_k=B_k'\oplus z_k''\oplus B_{k-1}' \end{cases} \tag{3}$$

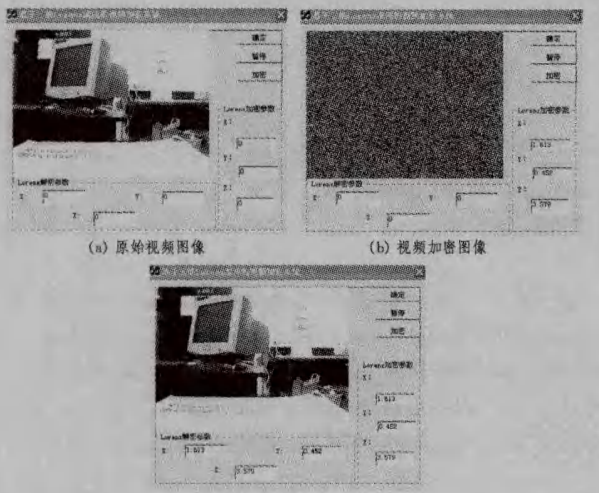
4. 显示解密后的视频帧。

5. 重复步骤 3 和 4，完成对整个视频的解密。

5 实验及实验结果分析

5.1 实验结果

利用 vc++6.0，结合 OpenCV 函数库，编写程序验证本文提出的视频加密算法。采用摄像头采集视频图像，设置采集图像的速度为 30 帧/s，此时视频已经看不出延迟，设置三维 Lorenz 加密系统的初值为：$x=1.613$，$y=0.452$，$z=3.579$，用其加密任一帧视频图像的效果如图 4 所示。



(a) 原始视频图像　(b) 视频加密图像

(c) 视频解密图像

图 4　视频加密、解密效果图

从实验结果上看，该算法充分利用了三维 Lorenz 混沌的混沌特性，具有加密速度快、实现简单、安全可靠的优势，能满足视频加密实时性要求高、数据量大的需求。

5.2 实验结果分析

1. 密钥空间分析

对视频图像进行加密，密钥个数过多满足不了视频加密实时性要求高的特点，过低安全性又不可靠。本算法选择 x，y，z 3 个初值作为系统的初始密钥，比一般单独的低维混沌系统初值多，密钥空间大，产生的混沌序列更加复杂，加密性能更好。x,y,z 的取值空间取决于计算机的计算精度，因此，整个 Lorenz 加密系统的密钥空间有 10^{48}，可以有效抵抗穷举攻击；此外，该系统还充分利用了 Lorenz 系统中最佳的混沌吸引子，可以产生更好的密钥序列。

2. 初值敏感性分析

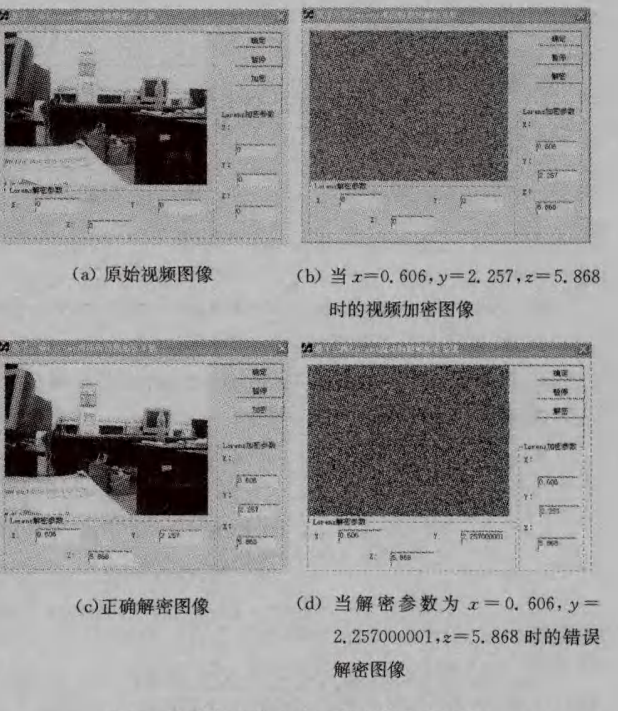
采用以下步骤验证系统对初始条件的敏感性：

1)使用初始条件 $x=0.606$，$y=2.257$，$z=5.868$ 加密任一帧视频图像。

2)极其微小的改变上述初始条件中的任意一个值，其他值保持不变，看能否能对视频帧进行解密。

3)比较原始帧、加密帧、正确解密帧和错误解密帧的区别，如图 5 所示。

从图 5 中可以看出，本视频加密系统具有极强的初值敏感性，即使初值有极微小的变化如 0.000000001，系统也会产生极大的雪崩效应，验证了系统的安全性和稳定性。



(a) 原始视频图像　(b) 当 $x=0.606$，$y=2.257$，$z=5.868$ 时的视频加密图像

(c)正确解密图像　(d) 当解密参数为 $x=0.606$，$y=2.257000001$，$z=5.868$ 时的错误解密图像

图 5　视频加密算法密钥敏感性测试效果

此外，本算法还遵循香农信息论中提出的混淆与扩散机制，图像内每个像素点的 R,G,B 分量值不断地作为密钥扩散到其他像素值中，形成你中有我、我中有你的局面；解密时，图像中任何一个像素点的解密错误都会不断地扩散开来，进而影响整幅图像的正确解密。该算法还改变了原始图像的直方图统计特征，可以有效地抵抗统计分析攻击。

结束语　本文提出了一种新的基于三维 Lorenz 系统的彩色视频加密算法，该算法充分利用了高维混沌系统的特性，产生的混沌序列相对于低维映射更加复杂，密钥空间更大，加密性能更佳；还充分运用了像素扩散的思想，整个系统遵循香农信息论中混淆与扩散的设计准则，任何一个像素的解密错误都会在整个解密过程中不断扩散。经实验证明，该算法在保证加密视频安全可靠的前提下，能有效地满足视频加密数据量大、实时性要求高的特点。

参 考 文 献

[1] 陈尔东. 基于混沌的信息加密方法研究[D]. 大连：大连理工大学，2004

[2] 廉士国，孙金生，王执铨. 视频加密算法及其发展现状[J]. 信息与控制，2004，33(5)：560-566

[3] Guan Zhi-hong, Huang Fang-jun, Guan Wen-jie. Chaos-based image encryption algorithm[J]. Physics Letters A, 2005, 346(1-3): 153-157

[4] Zhang Liu-hua, Liao Xiao-feng, Wang Xue-bing. An image encryption approach based on chaotic maps[J]. Physics Letters A, 2005, 346(1-3): 153-157

[5] 尤会明. 基于混沌的视频加密系统的研究[D]. 武汉：武汉理工大学，2006

[6] Mandlbrot B. 分形-自然界的几何学[M]. 王继振，译. 世界科学，1991(11)：1-4

[7] 王东生，曹磊. 混沌、分形及其应用[M]. 合肥：中国科学技术大学出版社，1995