

真彩图像和视频加密新方案的研究与实现

林 纯¹, 盛苏英¹, 陆国平²

(1 南通大学 电气工程学院, 江苏 南通 226019; 2 江苏信息职业技术学院, 江苏 无锡 214153)

摘 要: 提出一种新的混沌真彩图像和视频加密算法. 在对图像预处理的基础上, 应用 Henon-sine 复合混沌系统产生的混沌序列对预处理后的图像矩阵进行位置置乱和灰度值替代结合的方法加密. 通过性能分析, 表明该算法具有良好的加密效果. 将该算法应用于视频加密之中, 并引入“一帧一密”的技术, 仿真和通信平台的成功测试表明该算法对视频加密的适用性和良好性能.

关键词: 混沌系统; 真彩图像; 视频; 加密

中图分类号: TP309.7; TP391

文献标识码: A

文章编号: 1000-7180(2012)06-0113-04

Study and Realization of a New Color Image and Video Encryption Approach

LIN Chun¹, SHENG Su-ying¹, LU Guo-ping²

(1 School of Electrical Engineering, Nantong University, Nantong 226019, China;

2 Jiangsu College of Information Technology, Wuxi 214153, China)

Abstract: A new chaotic color image and video encryption algorithm is presented here. The soul of the new algorithm is color image pre-processing before encryption. Chaotic sequences generated by Henon-sine combined chaotic system are used to encrypt the pre-processed matrix with the methods of position shuffling and pixel value substituting. The performance analysis shows that wonderful encryption effect can be performed. The new algorithm, combined with the “single key on one image” technology, is used in video encryption further more. Applicability and excellent performance can be certified by simulation and successful test on the communication platform.

Key words: chaotic system; color image; video; encryption

1 引言

混沌现象看似无序实际上包含着一定的有序态, 一个参数确定的微分方程所描述的混沌系统对初值存在着极端的敏感性. 当对这个混沌系统取两个稍有不同初值时, 系统的轨迹会迅速演变出两种迥乎不同的状态来. 经混沌加密后的信息如被非法接收者窃取, 只要其掌握的密钥相对于真实密钥有微小的偏差, 都不能正确解密出原始信息来. 而且混沌长期演化的行为是不可预测的, 很难从已知的

有限密文信息中得到准确的加密矩阵和加密方法, 进而反推到原始信息. 因而混沌加密的保密性较高.

混沌的诸多优良性质使其非常适用于信息加密中, 前人在这一方面作了大量的研究. 早在 1989 年, 英国数学家 Matthews 就率先提出了混沌加密的思想^[1], 此举使得混沌加密成为学术界的一个研究热点. 1997 年 Fridrich 将混沌系统用于图像加密中^[2], 提出了一种基于二维 Baker 映射和 Cat 映射的像素位置置乱加密算法. 此后, 基于 Arnold 变换、幻方变换、Hilbert 曲线等的混沌位置置乱法和各种

收稿日期: 2011-09-28; **修回日期:** 2011-11-21

基金项目: 国家自然科学基金项目(61174066); 江苏省高校自然科学基金项目(10KJB120002); 南通大学自然科学基金项目(10Z029, 10Z030)

灰度值替代加密法^[3-5]相继提出并被应用于图像加密. 在图像信息安全问题日益严峻的今天, 在网络传输中引入混沌加密有着重要的意义^[6], 针对混沌加密方法在网络信息安全中的应用问题展开研究^[7-8].

2 真彩图像混沌加密方案

2.1 henon-sine 复合混沌系统

henon-sine 复合混沌系统的具体定义如下:

$$\begin{cases} x_{n+1} = -px_n^2 + y_n + 1 \\ y_{n+1} = qx_n \\ z_{n+1} = \sin^2(\arcsin \sqrt{z_n}) \end{cases} \quad (1)$$

式中, x_n, y_n 是 henon 混沌映射状态, z_n 是 sine 混沌映射状态, 当 $p=1.4, q=0.3, r>1$ 时, 选取合适初值, 系统产生混沌.

2.2 加密方案

所提出的加解密新方案是基于对真彩图像所对应的三维矩阵进行预处理的基础上, 加密矩阵源于上述的复合混沌系统, 具体的实施步骤如下:

第一步: 取初值 $x_0=0.1, y_0=0.2, z_0=0.6$, 系统参数 $p=1.4, q=0.3, r=3.9$, Henon 映射和正弦混沌映射均迭代 $n=600$ 次后取数据流, 得到 $\{x_k, y_k, z_k, k=1, 2, 3, \dots, 3 \times M \times N\}$ 序列, 同时生成混沌矩阵 $WX_{3M \times N}, WY_{3M \times N}, WZ_{3M \times N}$.

第二步: 提取原始真彩图像所对应的三维数字矩阵 $A_{M \times N \times 3}$ 后进行预处理, 按一定规则重新组合成二维矩阵 $B_{3M \times N}$.

第三步: 以混沌矩阵 $WX_{3M \times N}, WY_{3M \times N}$ 作为位置置乱矩阵, 将二维矩阵分别进行行、列地址变换, 得到一次加密矩阵 $A1_{3M \times N}$.

第四步: 取混沌矩阵 $WZ_{3M \times N}$ 中的每一个元素小数点后第 5, 6, 7 位组合成新的自然数矩阵, 与 $A1_{3M \times N}$ 进行相加操作后对 256 进行取余处理, 即可得到二次加密矩阵 $A2_{3M \times N}$.

第五步: 按第三步中提及的预处理方式的逆运算将二次加密矩阵 $A2_{3M \times N}$ 还原成一个三维矩阵的排列形式, 即得到加密图像. 加密流程如图 1 所示.

2.3 仿真效果

将系统初值 x_0, y_0, z_0 参数 r 和预迭代次数 n 作为同步密钥, 解密是加密的逆过程, 此处选择大小为 $150 \times 200 \times 3$ 的真彩图像“petdog.jpg”进行加密和解密算法测试, 得到 MATLAB 仿真效果图如图 2 所示. 加密后的图像如图 2(b) 所示变得无法识别; 而当取得正确的密钥解密后, 又能有效地恢复出原

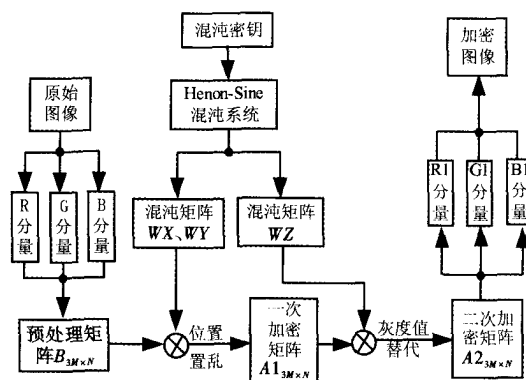


图1 真彩图像的混沌加密流程图

始的图像来, 如图 2(c) 所示; 当其中一密钥 x_0 相对于正确值偏差率仅为 10^{-10} 时, 解密出来的图像如图 2(d) 所示, 已经不能看出原始图像的本来面目.

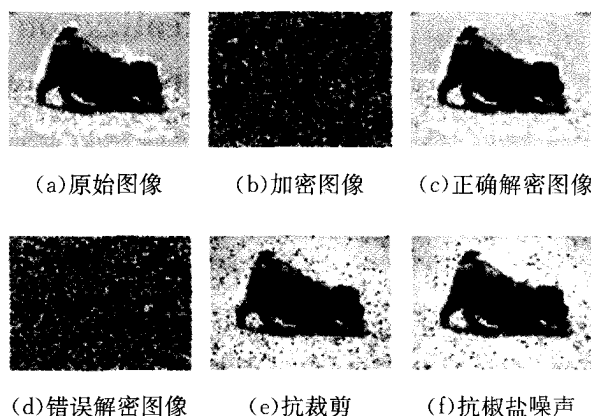


图2 真彩图像的混沌加解密仿真效果图

2.4 加密性能分析

(1) 密钥空间分析

在该算法中, 同步密钥由 x_0, y_0, z_0, r, n 组成, 每个参数精度都可达 10^{-16} , 密钥空间可达 10^{80} , 足以抵抗各种穷举攻击.

(2) 图像恢复性能分析和密钥敏感性

采用参数均方误差 (MSE) 和峰值信噪比 (PSNR) 作为评价解密图像偏离原始图像的误差指标. 具体定义如下:

$$MSE = \frac{1}{N_1 N_2} \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} (W(i, j) - M(i, j))^2 \quad (2)$$

$$PSNR = 10 \lg \left(\frac{f_{\max}^2}{MSE} \right) \quad (3)$$

式中, i, j 表示二维图像矩阵的行、列坐标值, $N_1 \times N_2$ 为图像尺寸. M 原为始图像, W 为解密图像, $f_{\max}$ 取 255. 当 PSNR 值达在 28 dB 以上时, 就认为图像恢复的质量较好. 经计算分析, 正确解密出来的图像

PSNR 趋于正无穷,也即恢复出来的图像和原图像完全相同;而错误解密图像,如图 2(d),PSNR 仅为 8.678 dB,远小于 28 dB,当对其他密钥分别取微小偏差解密时,得到的解密图像 PSNR 均远小于 28 dB,这也说明了该算法对密钥具有相当的敏感性。

(3) 抗攻击性分析

当密文图像遭到 10% 不规则裁剪后,解密效果如图 2(e)所示;对密文图像加入 10% 的椒盐噪声后对其进行解密,解密效果如图 2(f)所示。当图像遭到这两种攻击,并且攻击强度高达 10% 时,解密图像虽然有些瑕疵点,但还是能较清楚地反映出原图像的轮廓。因此,该算法具有良好的抗裁剪和噪声攻击能力。

3 加密方案在视频加密中的应用

上述真彩图像的加密方案也可应用于 AVI 文件的视频加密。具体方法如下:首先对 AVI 视频文件进行预处理,从中得到视频图像的帧数和每帧图像的像素矩阵大小。然后,依次提取视频流的每帧图像,采用“一帧一密”的方法,由混沌信号发生器生成每帧更新的加密矩阵对视频文件逐帧加密,并连续播放,就得到了密文视频文件。该密文数据流可经网络安全传输到异地。攻击者在传输过程中截获的密文视频文件可读性很低,无法分辨原始的视频内容。而合法接收者在已知密钥的前提下,可以将密文视频文件分帧解密,再组合起来就能达到解密视频文件的效果。具体的视频文件加密流程如图 3 所示,图中 N 为视频文件帧数。

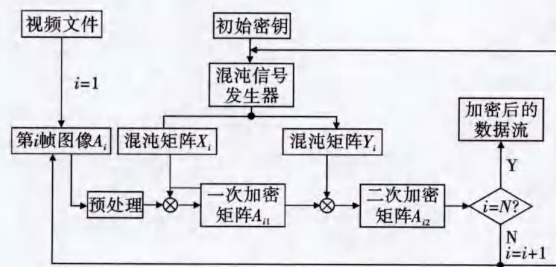
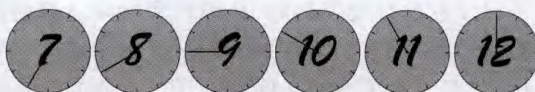


图 3 视频文件加密流程图

选用文件名为“clk.avi”的 AVI 视频片段进行测试,该视频流共有 12 帧图像,81kB 容量,每帧图像大小为 $321 \times 321 \times 3$,时针指示的时间正巧是该图像的帧序号。图 4 是该视频文件第 7 到 12 帧原始图像及加解密效果图。

由于所采用的 Henon-sine 复合混沌映射复杂程度较低,迭代效率高,可实现较快速地加密;加密



(a) 第 7 到 12 帧连续图像



(b) 第 7 到 12 帧连续帧加密效果图



(c) 第 7 到 12 帧连续帧解密效果图

图 4 “clk.avi”文件 7-12 帧加解密效果图

后经网络传输的实质上是加密后的数据流,这就节约了视频的读写时间,提高了加解密效率,另一方面也减小了视频的读写失真,增强了解密效果。从图 4(c)中可以看出,解密出来的视频文件和原始视频文件几乎无异;另外,采用了“一帧一密”的加密方式,攻击者无法从密文帧对比中得到有用的信息,该加密方案的抗破译能力较强,安全性较高。因此,运用该方案对视频加密,实现简单、加密速度较快,能满足视频的数据量大且实时性要求高的加密要求。

4 视频加解密在保密通信中的应用

为了测试所提出的加解密方案在保密通信中的适用性,特在 Borland C++ Builder 6.0 平台下构建了一个通信界面,如图 5 所示。

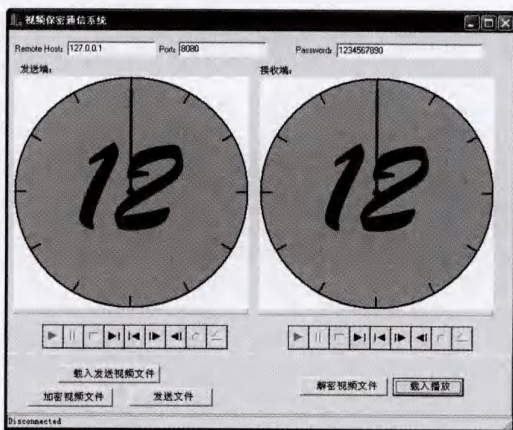


图 5 视频通信系统界面图

该界面分成发送端和接收端两个部分。在发送

端可以设置远程接收端的 IP 地址和对应计算机的逻辑端口号. 当发送者在“password”框中输入密钥并按下“载入发送视频文件”按钮时,本地的“Media play”控件就会播放视频;按下“加密视频文件”按钮后再按“发送”按钮,就可将加密后的视频以数据流形式发送到接收端;接收方接收到数据流信息后,可通过输入正确的密钥后按“解密视频文件”按钮的方式解密出原始视频,按“载入播放”按钮则可在接收端的“Media play”控件中显示接收到的视频信息. 在收发端都装载该通信界面就可以顺利地实现文件的发送和接收了. 并且通信的两地都是互为发送和接收端的. 所设计的通信界面也适用于多个用户之间的通信.

经测试证明,视频文件能经该渠道加密后发送到指定异地,在异地已知密钥时可运用解密方案恢复出视频文件的信息. 图 5 所显示的是成功解密视频文件“clk.avi”后播放到末帧图像的结果. 比较收发端的播放效果知,接收端所得的视频文件效果清晰,肉眼几乎无法分辨出和原始视频的差异. 因而,所设计的视频文件的加解密方案可行,能应用于保密通信中.

5 结束语

本文提出了一种基于 henon-sine 复合混沌系统的真彩图像和视频文件的加密新方案. 该加密方案程序相对简化,加密效率高,初值敏感性高,抗攻击能力强. 通过仿真和通信平台的成功测试说明该算法对真彩图像和视频加密的适用性和良好性能.

参考文献:

- [1] Matthews R. On the derivation of a chaotic encryption algorithm[J]. Cryptologia, 1989, 13(1): 29-42.
- [2] Fridrich J. Image encryption based on chaotic maps[C] // Proceedings of the IEEE International Conference on Systems Man and Cybernetics [s. l.]: IEEE, 1997: 1105-1110.
- [3] 赵莉,张雪峰,范九伦. 基于混沌序列的数字图像加密算法[J]. 微电子学与计算机, 2007, 24(2): 73-75.
- [4] 林纯,盛苏英,陆国平. 基于混沌序列的彩色数字图像加密设计[J]. 南通大学学报: 自然科学版, 2010, 9(1): 1-4.
- [5] 刘云,郑永爱. 基于混沌系统的彩色图像加密新方案[J]. 计算机工程与应用, 2011, 47(3): 90-93.
- [6] Liu F, Wu C K, Lin K J. Color visual cryptography schemes[J]. IET Information Security, 2008, 2(4): 151-165.
- [7] Liao X F, Li X M. A digital secure image communication scheme based on the chaotic Chebyshev map[J]. International Journal of Communication Systems, 2004, 17(5): 437-445.
- [8] 盛苏英,吴新华. 一种新的图像加密算法研究与应用[J]. 微电子学与计算机, 2011, 28(2): 124-128.

作者简介:

林 纯 女, (1980—), 硕士, 讲师. 研究方向为混沌控制.

盛苏英 女, (1979—), 硕士, 讲师. 研究方向为混沌同步、保密通信.

陆国平 男, (1965—), 博士, 教授. 研究方向为非线性控制、智能控制.