第 34 卷 第 2 期
2019 年 4 月

天津科技大学学报
Journal of Tianjin University of Science & Technology

Vol. 34 No. 2
Apr. 2019

DOI:10.13364/j.issn.1672-6510.20170330
数字出版日期：2018–11–27；数字出版网址：http://kns.cnki.net/kcms/detail/12.1355.N.20181127.1140.010.html

基于 PMSM 混沌系统的保密视频通信系统的 FPGA 设计与实现

谭东程，薛 薇，张 妹，刘世龙
（天津科技大学电子信息与自动化学院，天津 300222）

摘 要：提出了一种基于永磁同步电机(PMSM)混沌系统和 FPGA 技术实现视频数据保密通信的方法. 采用 Verilog HDL 语言对 PMSM 混沌系统进行 FPGA 电路设计与实现，得到的 FPGA 硬件实现结果与数值仿真结果一致. 在此基础上，进一步对一种基于该混沌系统和反馈型驱动响应式同步混沌保密通信制式的保密视频通信系统进行分析研究. 实际 FPGA 硬件实验结果证明了该保密视频通信系统的安全性和可行性.

关键词：PMSM；同步；保密视频通信；FPGA；实现
中图分类号：TN919.82 **文献标志码**：A **文章编号**：1672-6510(2019)02-0065-05

Design and Implementation of FPGA for Confidential Video Communication System Based on PMSM Chaotic System

TAN Dongcheng，XUE Wei，ZHANG Mei，LIU Shilong
（College of Electronic Information and Automation，Tianjin University of Science & Technology，Tianjin 300222，China）

Abstract：In this research，a method based on the chaos system of permanent magnet synchronous motor(PMSM) and FPGA technology was proposed to realize confidential video communication. Verilog HDL language was used to design and implement FPGA circuit for PMSM chaotic system，and the results are consistent with those of the numerical simulation. After that，the confidential video communication system based on the chaotic system and feedback driven-response synchronization method was analyzed. The actual FPGA hardware experiment results show that the confidential video communication system is secure and feasible.

Key words：PMSM；synchronization；confidential video communication；FPGA；implementation

随着多媒体技术的快速发展，实时视频采集、存储和处理已经在很多领域得到了广泛应用，如远程监控、安防、工程控制、医疗器械等. 在日常生活中，信息远程传输的安全性问题也受到了人们的关注[1].

目前，国内外比较流行的视频加密算法分为两种. 一种是对全部的视频流进行加密，即传统加密算法，如 CSC 算法[2]和 VEA 视频加密方法[3]. 这些算法成熟、有效且安全性能较高，但由于应用加密算法后视频信号等的数据计算量巨大，浪费资源且很难满足实时性要求，而且通常会改变数据格式. 另一种加密算法是将密码原理与视频技术结合，仅将选择出的特定帧进行加密，即选择性加密算法，如 MSE 算法[4]和 MPEG 算法[5]. 这种算法具有高效性和实时处理的能力，其安全性能高而且数据压缩率不变. 但这种加密算法也有明显的缺陷，它易遭受攻击而被破解.

由于混沌系统对初始条件和混沌参数非常敏感，混沌系统生成的混沌序列具有非周期性和伪随机性，因此非常适用于视频加密[6]. 近年来，混沌加密方式已成为信息安全研究的热点. 已有一些学者对混沌系统的保密通信进行研究，如对超 Lorenz 混沌系

收稿日期：2017–12–06；**修回日期**：2018–06–25
基金项目：国家自然科学基金青年科学基金资助项目(11202148)
作者简介：谭东程（1992—），男，广西人，硕士研究生；**通信作者**：薛 薇，教授，xuewei@tust.edu.cn

统[7]、Chen 混沌系统[8]、超混沌 Qi 系统[9]等进行了保密通信研究，但是还没有见到学者对永磁同步电机(permanent magnet synchronous motor，PMSM)混沌系统进行保密视频加密及 FPGA 实现的报道.

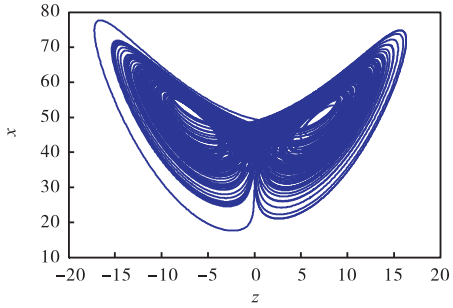
针对目前视频加密所存在的问题，本文提出了一种基于 PMSM 混沌系统模型和 FPGA 技术实现视频数据保密通信的方法. 根据 Euler 算法对 PMSM 混沌系统进行离散化处理，采用 Verilog 语言设计混沌系统的 FPGA 电路. 在此基础上，给出了一种基于该混沌系统和反馈型驱动响应式同步混沌保密通信制式的保密视频通信方案，并对该保密视频通信方案的有效性进行实验验证.

1　PMSM 混沌系统

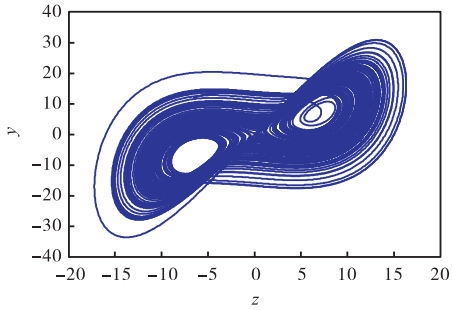
文献[10]给出 PMSM 混沌系统数学模型为

$$\begin{cases}\dot{x}=-x+yz\\ \dot{y}=-y-xz+az\\ \dot{z}=b(y-z)\end{cases}\tag{1}$$

式中 a 和 b 为实数，其在一定参数范围内表现出混沌、拟周期和周期等复杂的非线性动力学特性. 当选取的参数为 $a=50$、$b=4$ 时，系统呈现混沌态，其混沌吸引子相轨迹如图 1 所示. 式(1)系统的 3 个状态变量的时序图如图 2 所示.



(a) z–x 平面



(b) z–y 平面

图 1　式(1)系统的相图

Fig. 1　Phase portraits of system (1)

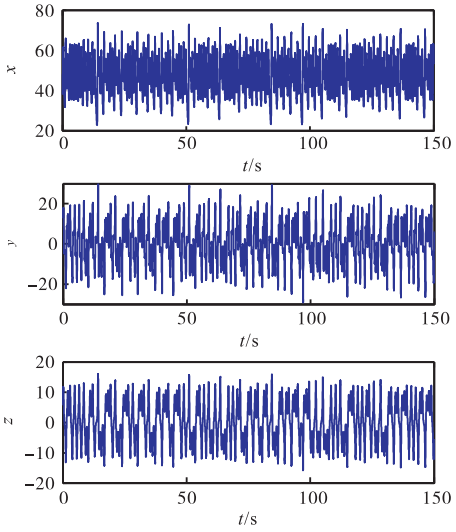


图 2　式(1)系统的状态变量 x、y、z 的时序图

Fig. 2　Timing diagrams of state variables x, y and z of system (1)

2　PMSM 混沌系统的离散化及 FPGA 实现

2.1　PMSM 混沌系统的离散化

由于 FPGA 只能处理离散数字信号，因此首先要对连续 PMSM 混沌系统作离散化处理，通常有 3 种离散化方法，即 Euler 算法、改进 Euler 算法和 Runge-Kutta 算法. 考虑到实验中 FPGA 硬件资源的限制，本文采用 Euler 算法进行离散化处理.

利用 Euler 算法可以得到式(1)离散化后的差分方程为

$$\begin{cases}x(n+1)=x(n)+(-x(n)+y(n)z(n))\Delta T\\ y(n+1)=y(n)+(-y(n)-x(n)z(n)+az(n))\Delta T\\ z(n+1)=z(n)+(b(y(n)-z(n)))\Delta T\end{cases}\tag{2}$$

式中：$a=50$，$b=4$；离散化的采样时间 $\Delta T=0.001$ s.

2.2　FPGA 功能仿真与实现

受其内部硬件结构的限制，FPGA 芯片只能进行二进制整数运算，为降低开发难度，采用定点数进行数值运算. 考虑到 x、y、z 的取值范围，选用定点数位宽为 28 位，其中符号位为 1 位，整数位为 11 位，小数位为 16 位，精度为 1/65 536 = 0.000 015.

采用 Verilog 语言对式(2)进行编程，产生 PMSM 混沌模型迭代序列，同时使用 ModelSim 软件对式(2)进行 FPGA 功能仿真，结果见图 3. 图 3 中 CpSv_DataX_o、CpSv_DataY_o、CpSv_ DataZ_o 分别对应 $x(n)$、$y(n)$、$z(n)$，与图 2 中的 Matlab 数值仿真的结果基本一致，说明设计的 FPGA 程序可产生 PMSM 混沌系统.

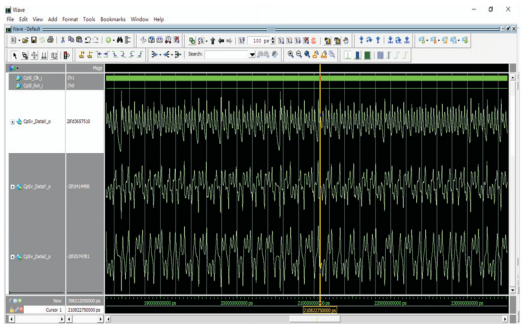
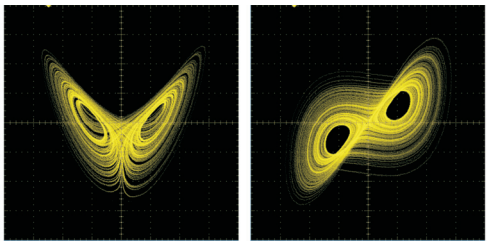


图 3　ModelSim 仿真的 x、y、z 时域波形图

Fig. 3　Time domain simulation waveform of x, y and z in ModelSim

将进行功能验证后的 FPGA 程序下载到 FPGA 芯片中，经 D/A 转换输出后，用示波器观察到的 PMSM 混沌吸引子的相图见图 4.



(a) z–x 平面　　(b) z–y 平面

图 4　PMSM 混沌系统电路中混沌吸引子的 FPGA 实现结果

Fig. 4　Chaos attractors of PMSM chaotic system implemented by FPGA

3　保密视频通信系统的设计与实现

3.1　PMSM 混沌系统驱动–响应式同步

驱动–响应式同步的特点是两个非线性动力系统之间存在着驱动与响应的关系，响应系统的行为取决于驱动系统，驱动系统的行为与响应系统的行为无关. 该同步方法只需通过信道传送一路加密信号，并且是自同步方式，当因某种原因失步后能重新实现自同步，与现有通信方式兼容，在 FPGA 技术中获得了实际应用[11].

这里给出 PMSM 混沌系统驱动–响应式同步的理论分析. 以 PMSM 混沌系统的变量 z 作为驱动信号，则驱动系统的状态方程为式(1).

响应系统的状态方程为

$$\begin{cases}\dot{x}_1=-x_1+y_1z\\ \dot{y}_1=-y_1-x_1z+az\\ \dot{z}_1=b(y_1-z_1)\end{cases}\tag{3}$$

式中：$a=50$，$b=4$.

设式(1)系统与式(3)系统之间误差信号为

$$\begin{cases}e_x=x-x_1\\ e_y=y-y_1\\ e_z=z-z_1\end{cases}\tag{4}$$

则误差系统的状态方程为

$$\begin{cases}\dot{e}_x=-e_x+ze_y\\ \dot{e}_y=-e_y-ze_x\\ \dot{e}_z=be_y-be_z\end{cases}\tag{5}$$

构造一个 Lyapunov 函数为

$$V(e)=\frac{1}{2}e_x^2+\frac{1}{2}e_y^2+\frac{1}{2}e_z^2\tag{6}$$

则 Lyapunov 函数的微分方程为

$$\dot{V}(e)=\dot{e}_xe_x+\dot{e}_ye_y+\dot{e}_ze_z\tag{7}$$

将式(5)状态方程代入 Lyapunov 函数的微分方程(7)，得

$$\dot{V}(e)=-e_x^2-(e_y-2e_z)^2\tag{8}$$

从式(8)可看出，只有当 $e_x=0$、$e_y=2e_z$ 时，$\dot{V}(e)=0$，其他情况下都是 $\dot{V}(e)<0$，可见 $\dot{V}(e)$ 为负半定. 根据 Lyapunov 稳定性定理可知，$e_x\to0$，$e_y\to0$，$e_z\to0$，即式(5)系统为渐近稳定，说明在理论上式(1)系统和式(3)系统可实现渐近稳定同步.

本文在驱动响应式同步的基础上，加入视频信号后再形成一个闭环和反馈，使得驱动系统和响应系统实现同步，其工作原理见图 5.

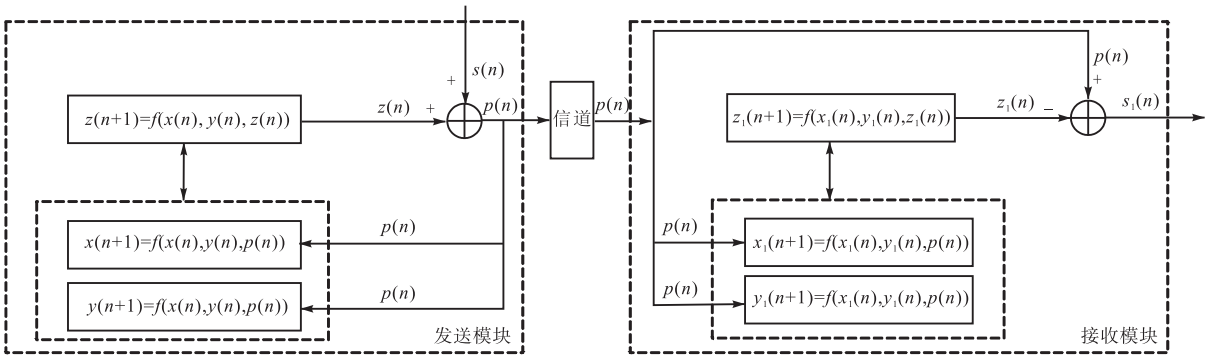


图 5　视频加密方案设计原理

Fig. 5　Design principle of video encryption

本设计方案在驱动响应式同步的基础上，以 PMSM 混沌系统的 z 变量与视频信号 s 之和作为驱动信号 p，对视频信号实现加密，则驱动系统为

$$\begin{cases}\dot{x}=-x+pz\\ \dot{y}=-y-xz+az\\ \dot{z}=b(p-z)\end{cases}\tag{9}$$

响应系统为

$$\begin{cases}\dot{x}_1=-x_1+pz_1\\ \dot{y}_1=-y_1-xz_1+az_1\\ \dot{z}_1=b(p-z_1)\end{cases}\tag{10}$$

式(9)和式(10)中，$a=50$，$b=4$.

由图 5 可知，$s(n)$为需要传输的原始视频信号，$z(n)$为驱动系统的状态变量，加密后的信号为 $p(n)$，由此可以得到发送模块系统(9)离散化后的状态方程为

$$\begin{cases}x(n+1)=x(n)+(-x(n)+p(n)z(n))\Delta T\\ y(n+1)=y(n)+(-y(n)-x(n)z(n)+50z(n))\Delta T\\ z(n+1)=z(n)+(4(p(n)-z(n)))\Delta T\end{cases}\tag{11}$$

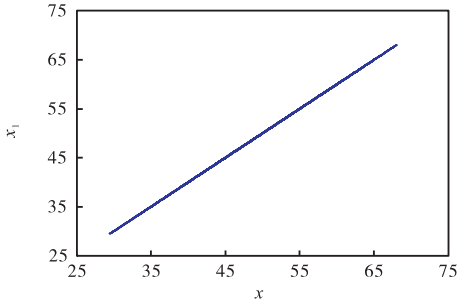
则接收模块系统(10)离散化后的状态方程为

$$\begin{cases}x_1(n+1)=x_1(n)+(-x_1(n)+p(n)z_1(n))\Delta T\\ y_1(n+1)=y_1(n)+(-y_1(n)-x_1(n)z_1(n)+50z_1(n))\Delta T\\ z_1(n+1)=z_1(n)+(4(p(n)-z_1(n)))\Delta T\end{cases}\tag{12}$$

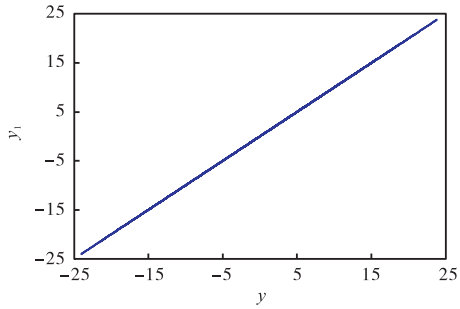
式(11)和式(12)中 $\Delta T=0.001$ s.

当接收模块和发送模块实现同步后，可得 $z_1(n)=z(n)$，接收模块经过解密后的恢复信号为 $s_1(n)=p(n)-z_1(n)=p(n)-z(n)=s(n)$，从而可将原始视频信号不失真地恢复出来.

本设计方案在驱动响应式同步的基础上，针对基于 PMSM 混沌系统的驱动响应式同步，以 z 为驱动变量实现驱动响应式同步，通过 Matlab 进行数值仿真后，得驱动系统(式(9))和响应系统(式(10))的同步曲线如图 6 所示，x、y 两个方向上的同步曲线为一条直线，且 $x_1=x$，$y_1=y$，两个系统已经达到了同步. 可见，对于 PMSM 混沌系统，以 z 为驱动变量可以实现驱动响应式同步.



(a) x 与 x_1



(b) y 与 y_1

图 6　同步曲线

Fig. 6　Synchronization curves

3.2　保密视频通信系统的 FPGA 设计与实现

保密视频通信系统是基于图 5 的方案设计，并利用 FPGA 实现的. FPGA 实验平台搭载了 Altera Cyclone IV 系列的 EP4CE22F17C8 芯片，分别通过摄像头子板 MT9D111 CMOS、32M 16bit DDR2 SDRAM 和 7 寸液晶显示屏子板等外设实现视频采集、加密后视频数据的缓存和解密后视频数据的显示. 系统硬件见图 7.

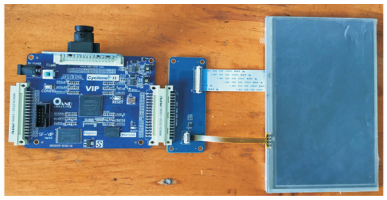


图 7　保密视频通信系统硬件

Fig. 7　Hardware of the confidential video communication system

系统结构见图 8. 在 FPGA 芯片内部(图 8 中虚线框内)，发送模块主要是完成对视频数据的加密，DDR2 SDRAM 控制模块主要是完成对外设 DDR2 SDRAM 的读写控制，接收模块主要用于解密视频数据，显示屏驱动模块主要是对液晶显示屏进行驱动.

FPGA 硬件实验结果见图 9. 从图 9 中可以看到，有效视频数字信号 $s(n)$能够完全隐藏在混沌序列中，而且解密后接收到的视频信号 $s_1(n)$恢复效果好(视频图像还原质量很好)，说明本文将 PMSM 混沌模型用于基于 FPGA 技术和反馈型驱动响应式同步混沌保密通信制式的保密视频通信中是可行的. 此外，加入基于 PMSM 混沌系统的混沌加密技术后，未改变视频数据格式，发送模块和接收模块采用的时钟频率均为 50 MHz. 视频数据从完成加密到完成解密的整个过程中只消耗了 4 个时钟周期，其中：发送模块消耗了 1 个时钟周期，即 20 ns；接收模块消耗了 3 个时钟周期，即 60 ns.

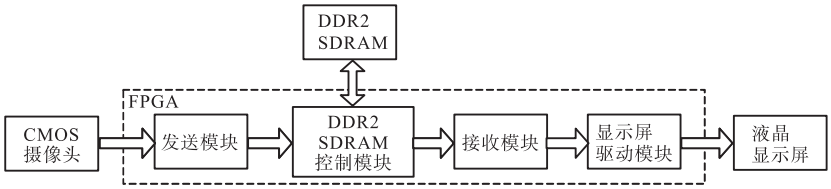


图 8　系统结构图

Fig. 8　System structure diagram

（a）原始视频的截图　　（b）加密后视频的截图　　（c）解密后视频图

图 9　保密视频通信系统的 FPGA 实验结果

Fig. 9　FPGA experimental results of the confidential video communication system

4　结　语

本文根据 Euler 算法对 PMSM 混沌系统进行离散化处理，再对该混沌系统进行了 FPGA 电路设计和实现，得到的 FPGA 电路实验结果和数值仿真的结果一致，说明利用 FPGA 技术实现 PMSM 混沌系统是可行的. 在此基础上，针对该混沌系统，进一步提出了基于反馈型驱动响应式同步的混沌保密通信制式的保密视频通信方案，并进行了实验验证，可为今后 PMSM 混沌系统的应用提供一定的参考. FPGA 具有高速并行处理信号的优势，利用其进行视频图像加密与解密，具有加密速度快、效率高的优点，可满足视频传输的实时性要求.

参考文献：

[1] 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.

[2] Chiaraluce F，Ciccarelli L，Gambi E，et al. A new chaotic algorithm for video encryption[J]. IEEE Transactions on Consumer Electronics，2002，48(4)：838–844.

[3] Zhu Z L，Zhang W，Yu H. MPEG video encryption algorithm based on Lorenz chaotic system[J]. Journal of Computer Applications，2008，28(12)：3003–3006.

[4] Wee S J，Apostolopoulos J G. Secure scalable streaming enabling transcoding without decryption[C]// Proceedings of IEEE International Conference on Image Processing. Piscataway：IEEE，2001：437–440.

[5] Agi I，Gong L. An empirical study of secure MPEG video transmissions[C]//Proceedings of Internet Society Symposium on Network and Distributed Systems Security. Piscataway：IEEE，1996：137–144.

[6] Valli D，Ganesan K. Chaos based video encryption using maps and Ikeda time delay system[J]. The European Physical Journal Plus，2017，132(12)：542–560.

[7] 于茜，罗永健，史德阳，等. 超 Lorenz 混沌系统的同步及其在保密通信中的应用[J]. 兵工自动化，2011，30(3)：45–47.

[8] 江山明，武相军，康丽. Chen 系统的混沌同步及其在保密通信中的应用[J]. 计算机工程与应用，2006，42(15)：104–108.

[9] 闵富红，王恩荣. 超混沌 Qi 系统的错位投影同步及其在保密通信中的应用[J]. 物理学报，2010，59(11)：7657–7662.

[10] 薛薇，郭彦岭，陈增强. 永磁同步电机的混沌分析及其电路实现[J]. 物理学报，2009，58(12)：8146–8151.

[11] 禹思敏. 混沌系统与混沌电路：原理、设计及其在通信中的应用[M]. 西安：西安电子科技大学出版社，2011.

责任编辑：常涛