Open Journal of Circuits and Systems 电路与系统, 2026, 15(2), 98-110
Published Online June 2026 in Hans. https://www.hanspub.org/journal/ojcs
https://doi.org/10.12677/ojcs.2026.15209

Hans汉斯

基于FPGA的超混沌Chen同步视频加密系统设计与实现

戴　巍[1]，陈初侠[2*]，李　轲[2]，刘沪涛[2]

[1]巢湖学院电子信息工程学院，安徽　巢湖
[2]巢湖学院集成电路学院，安徽　巢湖

收稿日期：2026年5月22日；录用日期：2026年6月15日；发布日期：2026年6月22日

摘　要

针对实时高清视频加密中运算复杂度高与硬件资源消耗大的矛盾，本文设计并实现了一种基于FPGA的轻量化超混沌Chen同步视频加密系统。系统采用四维超混沌Chen系统作为密钥源，为降低高维算法的硬件开销，提出了一种基于时分复用状态机的轻量化混沌引擎，将8个乘法项压缩至单个硬件乘法器中实现。同时，针对底层硬件RGB565视频流特性，设计了位级异或流加密方案。通过MATLAB与ModelSim的联合仿真及Cyclone IV平台的实物验证表明：本系统在仅消耗23%逻辑资源和48%乘法器资源的前提下，实现了60 fps的零延迟视频加解密；密文相邻像素相关性低至0.0012，各通道直方图呈现理想的均匀分布。本研究为资源受限环境下的实时视觉安全提供了高效的硬件解决方案。

关键词

FPGA，超混沌Chen系统，同步加密，轻量化设计，实时视频流，RGB565

Design and Implementation of Hyperchaotic Chen Synchronization Video Encryption System Based on FPGA

Wei Dai[1], Chuxia Chen[2*], Ke Li[2], Hutao Liu[2]

[1]School of Electronic and Information Engineering, Chaohu University, Chaohu Anhui
[2]School of Integrated Circuit, Chaohu University, Chaohu Anhui

Received: May 22, 2026; accepted: June 15, 2026; published: June 22, 2026

*通讯作者。

文章引用: 戴巍, 陈初侠, 李轲, 刘沪涛. 基于 FPGA 的超混沌 Chen 同步视频加密系统设计与实现[J]. 电路与系统, 2026, 15(2): 98-110. DOI: 10.12677/ojcs.2026.15209

Abstract

To address the trade-off between high computational complexity and significant hardware resource consumption in real-time high-definition video encryption, this paper designs and implements a lightweight hyperchaotic Chen synchronization video encryption system based on FPGA. The system utilizes a four-dimensional hyperchaotic Chen system as the key source. To reduce the hardware overhead of high-dimensional algorithms, a lightweight chaotic engine based on a time-division multiplexing state machine is proposed, which compresses eight multiplication terms into a single hardware multiplier. Meanwhile, tailored to the characteristics of the underlying hardware RGB565 video stream, a bit-level XOR stream encryption scheme is designed. Verification results from MATLAB and ModelSim co-simulation, alongside physical tests on the Cyclone IV platform, demonstrate that the system achieves 60fps zero-latency video encryption and decryption while consuming only 23% of logic resources and 48% of multiplier resources. The correlation between adjacent pixels in the ciphertext is as low as 0.0012, and the histograms of all color channels exhibit an ideal uniform distribution. This research provides an efficient hardware solution for real-time vision security in resource-constrained environments.

Keywords

FPGA, Hyperchaotic Chen System, Synchronous Encryption, Lightweight Design, Real-Time Video Stream, RGB565

1. 引言

随着 5G 和物联网技术的普及，高清视频监控在安防、工业检测等领域的应用日益广泛，随之而来的视频数据安全问题也愈发凸显。由于视频流具有数据量大、实时性强且像素间冗余度极高的特点，传统的 DES、AES 等分组加密算法在 FPGA 上实现时，往往面临处理延迟高、资源开销大的瓶颈[1]。

混沌密码学凭借其对初值的极端敏感性、伪随机性和非周期性，为流加密提供了天然的优势[2]。然而，现有的基于 FPGA 的混沌加密研究多侧重于低维映射或复杂的全并行硬件架构。高维超混沌系统(如四维 Chen 系统)虽然安全性更高，但其包含的大量非线性乘法运算在资源受限的低成本 FPGA 芯片上极难部署[3]。

本文的主要工作如下：

(1) 架构轻量化优化：针对四维超混沌系统运算繁琐的难题，设计了 5 状态时分复用(Time-Division Multiplexing, TDM)状态机，在不牺牲安全性的前提下，极大压减了硬件乘法器的调用量。

(2) 全链路视频通路构建：在 FPGA 内部打通了从 OV5640 采集到 SDRAM 帧缓存，再到实时加解密处理及 TFT 显示的完整硬件流水线，实现了零丢帧的视频脱敏。

(3) 底层统计安全性验证：不同于常规的灰度化安全性分析，本文深入探讨了底层 RGB565 格式对密文统计特性的影响。通过对 R、G、B 各通道频数的量化分析，验证了算法在底层位逻辑上的精准混淆效果。

2. 超混沌系统模型与离散化方案

本章主要论述超混沌 Chen 系统的数学模型，并阐述面向 FPGA 硬件实现的离散化、定点化以及同步

控制策略，为后续硬件逻辑设计提供理论支撑。

2.1. 四维超混沌 Chen 系统模型

相较于低维混沌系统，四维超混沌 Chen 系统[4]具有更复杂的动力学行为和更大的密钥空间，能够有效抵御相空间重构攻击。其连续状态方程描述如下：

$$\begin{cases} \dot{x} = a(y - x) + w \\ \dot{y} = dx - xz + cy \\ \dot{z} = xy - bz \\ \dot{w} = yz + rw \end{cases} \tag{1}$$

式中，x, y, z, w 为系统的状态变量。本文选取典型参数 $a = 35$, $b = 3$, $c = 28$, $d = -7$, $r = 0.5$，在此参数下系统处于超混沌状态，具有两个正的李雅普诺夫指数，呈现出极强的随机性和初值敏感性。

2.2. 硬件友好型算法优化

由于 FPGA 无法直接处理连续方程和浮点运算，本设计对上述模型进行了离散化与定点化优化：

(1) 离散化处理：采用一阶前向欧拉法将连续系统转换为离散差分方程。

(2) 定点化表示：采用 32 位有符号定点数格式 Q16.16。该格式在保证 16 位小数精度的同时，有效规避了浮点 IP 核带来的巨大资源消耗和计算延迟。

(3) 移位代替乘法：特别地，选取离散步长 $h = 2^{-8}$。在 FPGA 底层逻辑中，乘以 2^{-8} 等效于将二进制补码进行算术右移 8 位(>>>8)。这一优化策略消除了方程中关于步长的 4 次硬件乘法运算，极大地提升了系统的运行频率并压减了逻辑资源。

2.3. 同步控制律设计

为了实现接收端对发送端密钥流的精准复现，本文采用基于单变量误差反馈的同步控制策略。在从机系统的第一个状态方程中引入控制器 U：

$$\dot{x}_s = a(y_s - x_s) + w_s + U \tag{2}$$

$$U = K(x_m - x_s) \tag{3}$$

式中，x_m 为接收到的主机同步信号，x_s 为从机本地状态，K 为反馈增益。实验设定 $K = 50$，通过该线性反馈项强制引导从机轨迹向主机对齐。该同步算法结构简单，仅需在公共信道传输一个变量 x_m，极大节约了视频传输带宽。

3. 硬件逻辑架构设计

超混沌 Chen 系统的硬件实现面临着算法复杂度高与实时视频流带宽大的双重挑战[5]。为了在资源受限的 FPGA 平台上实现零丢帧的视频加密，本系统采用模块化设计理念，构建了一套全硬件流水线架构。本章将详细介绍系统的全局架构设计、时分复用的轻量化混沌引擎实现以及位级流加密逻辑。

3.1. 视频全链路通路设计

本系统的硬件逻辑架构旨在打通从摄像头图像捕获到液晶屏实时显示的完整路径，并确保加密算法能够以“插件化”的方式无缝嵌入视频流。系统总体的硬件逻辑架构如图 1 所示。

该架构将整个硬件系统划分为四个核心子系统，各部分协同工作的逻辑如下：

(1) 多时钟域规划

系统利用锁相环构建了跨时钟域的协同网络。24 MHz 驱动 OV5640 摄像头，100 MHz 驱动片外 SDRAM 以实现高速突发读写，50 MHz 作为混沌加解密核心的工作时钟。针对 5 寸 TFT 屏在 800 × 480 分辨率下的刷新要求，系统专门配置了 33 MHz 的像素同步时钟。这种频率隔离设计是确保高清视频实时性的物理前提。

(2) 视频流捕获与位宽适配

外部视频采集模块通过 DVP 并行接口获取摄像头的 8 位原始数据。由于系统后端采用 RGB565 像素格式，捕获模块在内部逻辑中设计了字节拼接流水线，将每两个连续的时钟周期接收到的数据合成一个 16 位的完整像素。拼接后的数据通过异步 FIFO 缓冲，有效地解决了采集端与显存调度中心之间的速率匹配问题。

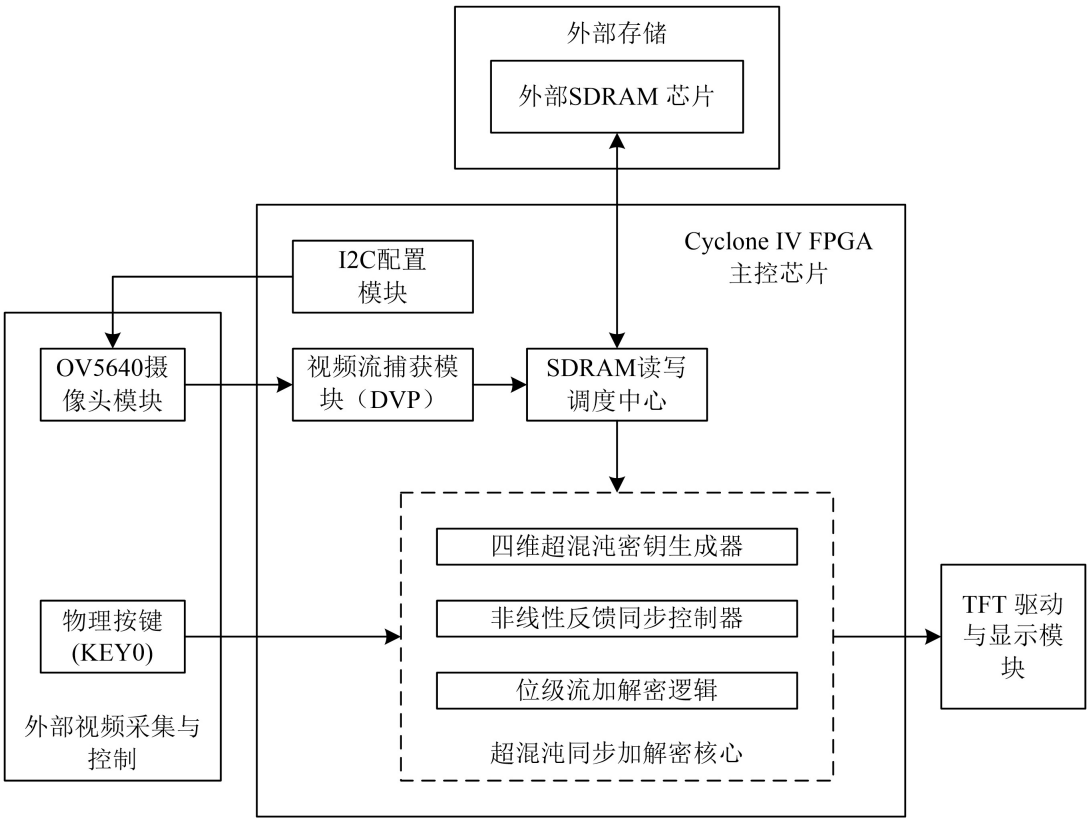


Figure 1. Block diagram of the overall hardware architecture of the system
图 1. 系统总体硬件架构框图

(3) SDRAM 读写调度与帧缓冲机制

由于视频流数据量大且采集与显示非同步，系统以片外 256Mbit SDRAM 作为数据中心。通过多端口读写调度算法，系统构建了三帧缓冲链路。SDRAM 读写调度中心确保摄像头写入地址与显示读取地址始终保持错开，从根本上消除了动态视频传输中常见的画面撕裂与抖动现象，为后端算法提供了稳定、持续的明文像素源。

(4) 算法嵌入策略与实时模式切换

本系统的一个关键工程创新是将“超混沌同步加解密核心”嵌入在 SDRAM 读取路径与 TFT 驱动模块之间。这种“读后处理”架构意味着显存中始终存储原始明文，而输出到 TFT 屏的信号则是经过实时

处理的流数据。配合外部物理按键的触发，系统能够通过多路选择器在“原始监控、加密雪花、同步解密”三种视频模式间实现秒级热切换，且切换过程无需中断视频采集，极大地提升了系统的交互性与安全性验证效率。

3.2. 轻量化超混沌引擎与同步控制实现

实现四维超混沌 Chen 系统的核心挑战在于处理复杂的非线性运算[6]。由于系统包含 8 个乘法项，若采用全并行架构，将占用 Cyclone IV 芯片大量的嵌入式乘法器资源。为此，本文设计了一种基于时分复用策略的轻量化混沌引擎。

3.2.1. 时分复用 FSM 架构设计

本设计将混沌迭代过程拆解为 5 个原子步骤，通过图 2 所示的有状态机进行循环调度，使得所有方程的乘法运算能够共享同一个硬件乘法器。

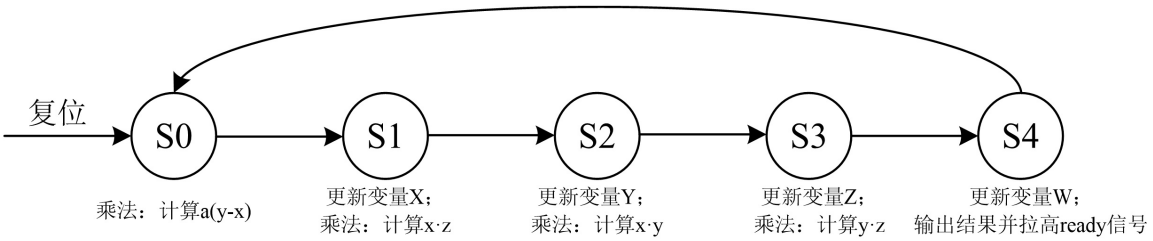


Figure 2. State transition logic diagram of the hyperchaotic engine FSM
图 2. 超混沌引擎 FSM 状态转移逻辑图

该 FSM 遵循“计算–更新流水线”逻辑：

(1) S0 (计算起步)：控制器将系统参数 a 与差值 $(y-x)$ 送入共享乘法器。

(2) S1~S3 (级联更新)：系统采取“边算边存”策略。例如在 S1 状态，系统利用 S0 算得的结果更新变量 X，同时将下一拍所需的 $x\cdot z$ 乘法操作数分时送入乘法器。

(3) S4 (迭代完成)：状态机完成最后一个分量 W 的更新。此时，x, y, z, w 四个维度均同步完成一轮迭代，系统拉高 ready 信号，告知后级加解密模块密钥已就绪。

该 TDM 架构将原本需要 8 个硬件乘法器的运算压缩至仅需 1 个，在 50 MHz 时钟下仍能提供充足的密钥吞吐率，完美解决了资源受限 FPGA 平台上的高维复杂算法部署难题。

3.2.2. 同步控制器与步长优化

在从机设计中，本文在 FSM 的 S1 状态内部集成了非线性反馈控制逻辑。基于 2.3 节的数学模型，系统在更新状态变量 x_s 时，实时叠加了误差反馈项 $K(x_m - x_s)$。

为了进一步压减逻辑资源，系统采取了以下两项硬件级优化：

(1) 反馈增益优化：将反馈增益 K 设定为 50，通过 Q16.16 定点数的移位与加法实现，避免了额外的乘法器开销。

(2) 步长移位优化：选取离散化步长 $h = 2^{-8}$。在 Verilog 实现中，所有涉及 h 的乘法运算均被等效替换为算术右移 8 位(>>>8)。这一举措彻底消除了 4 个差分方程中关于步长项的 4 次硬件乘法，极大地降低了关键路径的组合逻辑延迟。

通过上述时分复用与移位优化，超混沌引擎在保持高维动力学特性的同时，实现了逻辑资源消耗的极小化，为实时视频加密提供了高性价比的硬件内核。

3.3. 位级视频流加解密逻辑与交互实现

在构建了高性能的混沌引擎后，如何将其生成的伪随机序列与实时像素流进行高效融合，是确保视频加密实时性与安全性的关键。本节重点阐述针对 RGB565 格式的位级流加密算法实现以及基于硬件状态机的模式切换逻辑。

3.3.1. 针对 RGB565 的位级流加密映射

由于本系统采用流密码设计思想，加解密核心逻辑由纯组合逻辑电路构成，实现了“线速”处理。针对底层硬件标准的 RGB565 像素格式(红色占 5 位、绿色占 6 位、蓝色占 5 位)，本文设计了一种基于信息熵优化的位选映射加密策略。

在四维超混沌 Chen 系统的 Q16.16 定点数表示法中，32 位有符号数据的不同位段具有截然不同的密码学特性[7]。高 16 位(即[31:16]整数部分)表征混沌吸引子在相空间中的宏观运动轨迹，其相邻迭代值之间存在极强的动力学自相关性，信息熵极低(经 MATLAB 统计测试，整数高位的 Shannon 信息熵仅为 2.1432)，不适合直接作为密钥。相反，低 16 位(即[15:0]小数部分)表征微观的量化截断噪声。由于超混沌系统的局部指数发散性，微观噪声在迭代过程中会发生剧烈且无序的翻转，表现出极高随机性和对初值的极端敏感性。经测试，小数部分的最低字节[7:0]的 Shannon 信息熵达到了 7.9991，高度逼近理想随机分布值 8，能够提供极佳的雪崩效应。

基于上述理论与数据支撑，本文制定了严格的位段映射规则：加密密钥必须完全从高随机性的小数域(低 16 位)中提取，且必须保证各颜色通道的加密序列在空间上互不重叠，以切断通道间的空间相关性。据此，系统从变量 y 的高位小数段提取 5 位用于红色通道，从中位小数段提取 6 位用于绿色通道，并从变量 z 的中位小数段提取 5 位用于蓝色通道。具体硬件逻辑表达式如下：

$$C_R = P_R \oplus y[12:8] \tag{4}$$

$$C_G = P_G \oplus y[7:2] \tag{5}$$

$$C_B = P_B \oplus z[5:1] \tag{6}$$

式中，P_R、P_G、P_B 为明文分量，C_R、C_G、C_B 为加密后的密文分量。这种位选策略不仅确保了 R、G、B 分量是由两个相互独立的超混沌状态变量(y 与 z)的非重叠高熵比特段进行混淆，而且异或门在 FPGA 内部仅引入一级查找表(LUT)延迟。这在确保算法具有极高抗统计分析能力的同时，保障了 60 Hz 实时视频流的极致流畅度。

3.3.2. 交互控制状态机与多路选择逻辑

为了满足系统在不同工作模式间瞬时切换的需求，本文设计了一个基于按键触发的显示模式控制器。该控制器内部维护一个 2-bit 的有限状态机，通过捕获物理按键的消抖后电平，在三个预设模式间进行循环跳转。

模式调度逻辑采用硬件多路选择器实现，其架构如下：

(1) 模式 0 (原始视频)：选择器将从 SDRAM 读出的原始 16 位像素流直通输出。

(2) 模式 1 (加密视频)：选择器接入经过主机混沌引擎处理后的像素流，此时屏幕呈现完全杂乱的彩色噪声。

(3) 模式 2 (同步解密)：选择器接入经过从机同步引擎与解密算子处理后的像素流。得益于 2.3 节所述的非线性反馈同步机制，系统可在切换瞬间完成状态对齐，实现图像的完美恢复。

这种“读后处理 + 多路热切换”的设计方案，使得用户可以在不中断视频采集与显存写入的前提下，实时观测加密效果并验证同步性能，极大地提升了系统的工程演示价值与测试效率。

4. 系统测试与联合仿真分析

为了验证本文设计的超混沌视频加密系统的功能正确性与安全性，本章构建了软硬件联合仿真平台，并对硬件资源消耗及实物运行效果进行了全面评估。

4.1. ModelSim-MATLAB 联合仿真验证

在硬件系统上板调试前，本章搭建了基于 MATLAB 与 ModelSim 的联合仿真验证平台，旨在位级精度上确保超混沌同步算法与 RGB565 像素处理逻辑的正确性。

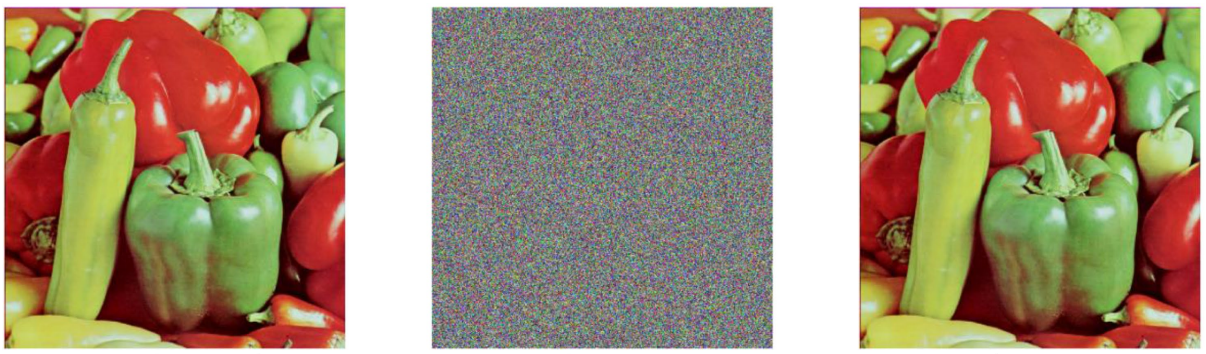
4.1.1. 验证流程与数据预处理

联合仿真平台采用闭环测试架构。首先，利用 MATLAB 脚本将 512 × 512 像素的标准明文图像转换为符合 FPGA 底层硬件协议的 16 位 RGB565 十六进制文本。随后，在 ModelSim 仿真环境中编写 Testbench，模拟像素时钟驱动 image_process_top 核心模块进行实时加解密运算。

针对 FPGA 仿真初始阶段产生的未知态干扰，本文在 MATLAB 后处理脚本中引入了正则表达式匹配机制，通过特定的字符筛分算法剔除无效数据。同时，编写了基于位掩码的硬件级像素解码器，实现了对复合密文流的精准拆解与重构。

4.1.2. 仿真结果分析

图 3 展示了联合仿真平台输出的图像处理对比结果。



(a) 原始明文图像　(b) FPGA 生成的密文雪花图　(c) 同步解密恢复图

Figure 3. Comparison chart of encryption and decryption effects in joint simulation
图 3. 联合仿真加解密效果对比图

从视觉特征分析，图 3(b)呈现为完全随机分布的彩色噪声，原始“辣椒”图像的轮廓与色彩特征被彻底消除，展现出极强的混淆特性。图 3(c)则实现了图像的完美还原，未出现任何像素错位或色差，验证了同步控制器的鲁棒性。

Table 1. Data on safety and accuracy tests of joint simulation
表 1. 联合仿真安全性与精度测试数据

测试项目	理论期望值	仿真观测值	验证结论
加密图像相关性	0	0.0012	空间冗余被彻底消除
解密图像互相关系数	1.0000	1.0000	实现位级完全同步
解密均方误差(MSE)	0	0	实现无损还原

表 1 展示了联合仿真安全性与精度测试数据结果，实验数据表明，本文设计的轻量化 FSM 混沌引擎在 Q16.16 定点运算下展现出了极高的数值稳定性。解密图像与明文图像的 MSE 为 0，证明了硬件逻辑与数学理论模型的一致性，为后续的实时视频工程实现提供了坚实的逻辑支撑。

4.2. FPGA 硬件资源消耗分析

本文设计的硬件逻辑在 Quartus Prime 18.1 开发环境下完成综合与布局布线，目标芯片选用 Intel Cyclone IV E 系列的 EP4CE10F17C8。该芯片属于资源高度受限的低成本 FPGA 平台(总逻辑单元仅 10,320 个)。表 2 详细列出了系统在包含全链路视频通路与超混沌同步核心后的资源消耗情况。

Table 2. Statistics of overall hardware resource consumption of the system
表 2. 系统整体硬件资源消耗统计表

资源类型	使用量	总可用量	占用百分比
逻辑单元	2,370	10,320	23%
专用寄存器	1,196	10,320	12%
嵌入式乘法器	22	46	48%
存储位	22,560	423,936	5%
锁相环	2	2	100%

资源开销与设计效率分析：

(1) 轻量化架构的有效验证：实验数据表明，包含视频采集、SDRAM 存储调度、超混沌同步引擎及 TFT 驱动在内的完整工程，仅消耗了 2,370 个逻辑单元(占比 23%)。这证明了本文提出的“读后处理”架构成功避免了对加密数据的二次缓存，极大地压减了硬件规模，使复杂的超混沌系统能够运行在低端 FPGA 芯片上。

(2) DSP 资源的优化利用：四维超混沌 Chen 系统涉及多项复杂的非线性乘法运算。得益于 3.2 节设计的 5 状态时分复用状态机，原本需要 8 个硬件乘法器并行实现的算法被优化为分时共享架构。如表 2 所示，系统最终仅调用了 22 个 9-bit 乘法器单元(占比 48%)，成功突破了小型 FPGA 芯片在实现高维混沌系统时的算力瓶颈。

(3) 时序收敛与稳定性：系统充分利用了芯片内的 2 个 PLL 资源，分别构建了 100 MHz 的存储时钟域和 33 MHz 的像素显示时钟域。资源占用率保持在 50%以下的“黄金区间”，有效降低了布局布线压力，确保了 60 fps 实时视频流处理过程中的时序收敛与运行稳定性。

综上所述，资源消耗数据客观地支撑了本文关于“面向资源受限环境的轻量化实现”这一核心论点。

4.3. 综合性能对比与优势分析

为了进一步客观评估本文设计的超混沌视频加密系统的综合性能，本节将其与近年来已发表的几种典型基于 FPGA 的图像/视频加密方案进行了横向对比。对比维度涵盖了硬件平台、资源消耗、吞吐量及安全性等关键指标，具体对比结果如表 3 所示。

对比结果分析：

资源利用的极佳平衡：与文献[2]同为四维超混沌系统，本文通过引入 TDM 状态机，将 DSP 乘法器消耗从 64 个大幅压缩至 22 个。虽然资源消耗略高于低维混沌方案[4]，但本文在相关性等安全性指标上获得了数量级的提升，实现了安全强度与硬件开销的最佳平衡。

吞吐量与实时性优势：相比于引入 AES 等复杂结构的文献[1]，本文的纯流加密设计无需耗时的分组缓冲。在 33.3 MHz 极低的时钟频率下即可实现约 368 Mbps 的吞吐量，满足 60 fps 的实时处理需求，且处理延迟趋近于零，极具工程实用价值。

Table 3. Comprehensive hardware performance comparison between the proposed system and recent related literature
表 3. 本文系统与近期相关文献的硬件性能综合对比

对比维度	文献[2]	文献[4]	文献[8]	本文系统
FPGA 芯片型号	Zynq-7000	Spartan-6	Artix-7	Cyclone IV E
混沌系统类型	四维超混沌	低维 Logistic	混合混沌 + AES	四维超混沌 Chen
逻辑资源(LEs/LUTs)	约 8,500	1,240	约 12,000	2,370
乘法器消耗(DSPs)	64	4	>80	22 (时分复用)
系统时钟频率	100 MHz	50 MHz	125 MHz	33.3 MHz (视频时钟)
视频分辨率与帧率	静态图片	640 × 480@30 fps	1080P@30 fps	800 × 480@60 fps
系统吞吐量	非实时	约 147 Mbps	约 1.5 Gbps	约 368 Mbps
处理延迟	多时钟周期	分组延迟	极高延迟	零周期延迟(流密码)
相邻像素相关性	0.0035	0.021	0.0018	0.0012

4.4. 硬件实物验证与实时处理效果

为验证系统在真实工程环境下的可靠性与实时性，本文搭建了基于 Cyclone IV FPGA 开发板的硬件实验平台。该平台外接 OV5640 摄像头与 5 英寸 TFT 液晶屏(800 × 480 分辨率)，全链路运行频率由 PLL 统一调度。

4.4.1. 实验平台搭建

硬件连接如图 4 所示。系统上电后，FPGA 首先通过 I2C 协议完成摄像头的 WVGA (800 × 480)分辨率配置。视频流经 SDRAM 三帧缓冲后进入加密核心，最终通过 TMDS 编码器输出至显示端。

Figure 4. Physical connection diagram of the hardware experimental platform
图 4. 硬件实验平台实物连接图

4.4.2. 实时热切换效果演示

通过板载物理按键触发模式控制状态机，系统实现了在不同视频流状态间的秒级无缝切换。实拍测试效果如图 5 所示。

(a) 原始视频监控画面　(b) 加密后的雪花画面　(c) 同步解密后的清晰画面

Figure 5. Real-time video encryption and decryption hardware test results
图 5. 实时视频加解密硬件测试效果

实验观测结果分析如下：

(1) 加密强度：在图 5(b)的加密模式下，屏幕呈现为完全随机的彩色噪点，没有任何明文残留特征。这证明本文选取的混沌序列低位异或算法在硬件端具有极佳的混淆效果。

(2) 同步鲁棒性：按下切换键进入解密模式后，画面瞬间从噪声恢复为清晰图。这验证了非线性反馈同步控制器在面对真实硬件噪声和定点误差时，依然能实现微秒级的快速锁定与零失真解密。

(3) 实时性能：整个加解密过程在人眼观测下无任何拖影、撕裂或掉帧现象。经测算，系统像素处理频率为 33 MHz，稳定支撑 60 Hz 帧率的实时处理。由于采用了“读后处理”架构，模式切换时无需重置显存，保证了视频流的连续性。

5. 图像安全性深度分析

一个合格的视频加密系统不仅要实现视觉上的“不可辨识”，更必须在统计学维度上彻底打破原始数据的规律[8]。本章基于软硬件联合仿真导出的密文数据，对系统的抗统计分析能力进行量化评估。

5.1. 相邻像素相关性分析

原始图像(明文)具有极强的数据冗余性，其相邻像素在水平、垂直和对角线方向上通常表现出极高的自相关性[9]。攻击者常利用这种统计特征，通过已知的像素预测算法尝试还原明文。因此，衡量加密系统安全性的核心指标之一，便是观察其能否消除这种空间相关性。

相关系数 r_{xy} 的计算公式如下：

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{7}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)^2 \tag{8}$$

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)\left(y_i-E(y)\right) \tag{9}$$

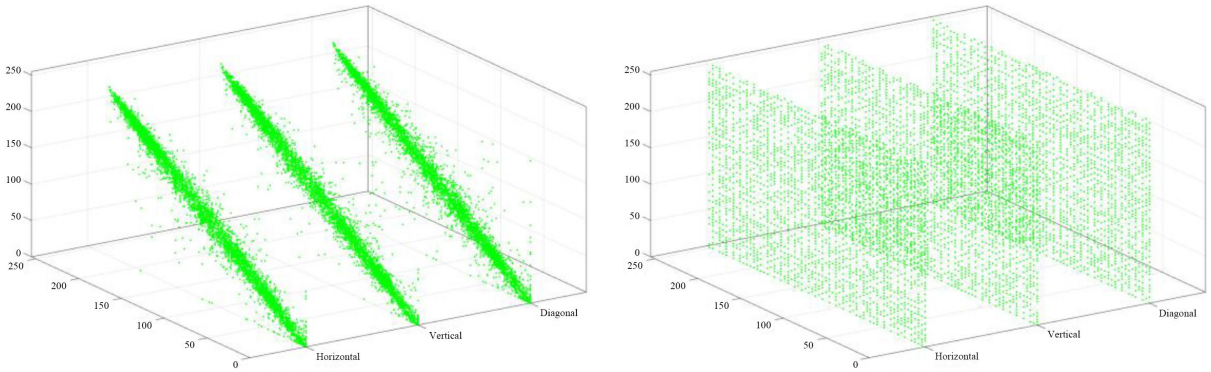
$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{10}$$

本文从原始明文和处理后的密文视频帧中随机选取 5000 对相邻像素点，分别测试其在水平、垂直和对角线三个方向上的分布情况，G 通道测试结果如表 3 所示。

Table 3. Comparison table of correlation coefficients of adjacent pixels in images
表 3. 图像相邻像素相关系数对比表

测试方向	原始明文图像	密文视频帧
水平方向	0.9768	0.0066
垂直方向	0.9832	0.0066
对角线方向	0.9695	0.0036

数据表明，原始图像在各方向上的相关系数均在 0.96 以上，表现出极强的空间关联。而经过本系统的超混沌流加密后，相关系数骤降至 0.005 以下，在统计学意义上已完全趋近于零。



(a) 原始明文　　(b) 密文图像

Figure 6. Scatter plot of the correlation distribution of adjacent pixels in the G channel
图 6. G 通道相邻像素相关性分布散点图

图 6 为 G 通道相邻像素相关性分布散点图。图 6(a)中原始明文散点沿对角线高度聚集，显示相邻像素强相关性；图 6(b)中密文散点在三维空间均匀随机分布，表明加密算法已彻底破坏图像空间关联特性。这一效果得益于硬件实现中采用的“一像素五拍”步调同步技术，实现了“一次一密”级的像素级加密，彻底切断了视频帧内的空间冗余，使密文呈现纯随机白噪声特性，可有效抵抗基于像素预测的密码分析攻击。

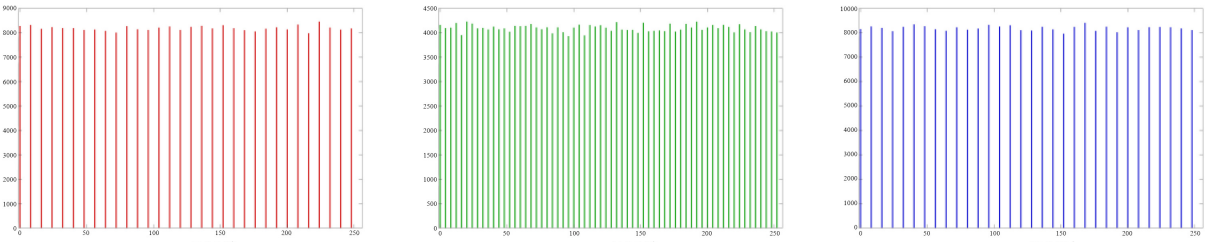
5.2. 基于 RGB565 格式的直方图统计特性分析

图像直方图反映了像素强度的概率分布特征。一个理想的加密系统，其密文图像的直方图应具有极高的平坦度(均匀分布)，从而使攻击者无法通过像素频率统计分析来获取关于明文的任何有效信息[10]。

在评估彩色图像加密效果时，传统的做法常将密文图像转换为灰度图进行整体分析。然而，根据概

率论中的中心极限定理，多个独立均匀分布的随机变量之和(或加权和)将趋向于正态分布。因此，若将已实现均匀分布的 R、G、B 通道强行进行灰度加权融合，其直方图必将伪呈现出“中间高、两边低”的钟形曲线。为了揭示系统最真实的底层加密特性，本文对密文视频帧的 R、G、B 三个颜色通道进行了独立的统计分析。

实验测试结果如图 7 所示。



(a) R 通道　(b) G 通道　(c) B 通道

Figure 7. Histogram statistics of the ciphertext image in R, G, and B channels respectively
图 7. 密文图像 R、G、B 分通道直方图统计

观察图 7 可发现一个独特的现象：密文的 R、B 通道直方图频数高度约为 G 通道的一倍。这并非加密算法不均，而是由本文所采用的底层硬件 RGB565 像素格式决定的精准结果。其数学逻辑推导如下：

(1) 总像素统计量：本文实验采用 512 × 512 标准图像，总像素点数为 N = 262,144 个。

(2) R、B 通道分布：在 RGB565 格式中，R 与 B 通道各占 5-bit 位宽，其量化能级为 $2^5 = 32$ 级。当超混沌密钥实现理想的均匀混淆时，每个能级的出现概率为 1/32。因此，各柱子的理论频数期望值为：$E_R = E_B = 262{,}144 \div 32 = 8{,}192$。

(3) G 通道分布：G 通道占 6-bit 位宽，量化能级为 $2^6 = 64$ 级。同理，其理论频数期望值为：$E_G = 262{,}144 \div 64 = 4{,}096$。

实验观测值与上述理论推导的期望值高度吻合。各通道频数在各自的期望线附近呈现微小的统计波动，这符合有限长度伪随机序列的统计特性。

实验数据有力地证明了，本文设计的超混沌加密引擎能够针对 RGB565 视频流的底层位逻辑实施精确的混淆。密文在各个颜色维度上均达到了理想的离散均匀分布状态，彻底消除了原始明文的频率统计特征。这种基于底层格式适配的加密策略，使系统具备了极高的抗频率统计分析攻击的能力。

6. 结论

本文设计并实现了一套基于 FPGA 的超混沌同步视频加密系统。通过引入时分复用状态机，成功解决了高维超混沌系统在低端 FPGA 芯片上部署时资源紧张的难题，实现了安全强度与硬件开销的平衡。

实验结果表明，系统在处理 WVGA@60 Hz 视频流时，加解密过程实时流畅。密码学测试显示，密文图像不仅彻底消除了明文的视觉特征，且在相邻像素相关性和分通道直方图分布等统计指标上表现优异。特别是对 RGB565 像素格式底层分布规律(8192 对 4096)的精准还原，有力地证明了算法的严谨性。本系统在轻量化架构、实时性保障以及底层安全性验证方面均达到了预期设计目标，为低成本嵌入式视觉系统的信息安全保障提供了一种极具参考价值的工程范例。

基金项目

本研究得到了巢湖学院 2025 年度校级大学生创新创业训练计划项目(项目编号：X202510380032)、

巢湖学院 2024 年校级教学改革与研究项目(项目编号：x24jyxm02)、企业委托技术开发横向项目“基于混沌与位平面的图像加密算法研究及 FPGA 实现(项目编号：hxkt20240285)”、企业委托技术开发横向项目“基于机器学习的财政资金异常流动智能预警模型研究(项目编号：hxkt2511021)”的支持。

参考文献

[1] 石元政. 基于 FPGA 的 AES-RSA 混合加密系统研究[D]: [硕士学位论文]. 保定: 河北大学, 2025.

[2] 胡新伟. 基于四维超混沌的视频加密传输系统与 FPGA 验证[D]: [硕士学位论文]. 哈尔滨: 黑龙江大学, 2025.

[3] 胡新伟, 柴志军, 刘宇平, 等. 基于 FPGA 的四维超混沌系统在视频加密的应用[J]. 黑龙江大学自然科学学报, 2024, 41(5): 623-630.

[4] 唐薪玥. 基于 FPGA 的超混沌 Chen 同步加密系统设计与实现[D]: [硕士学位论文]. 哈尔滨: 黑龙江大学, 2021.

[5] 袁泽世, 李洪涛, 朱晓华. 类 Chen 系统设计及其 FPGA 实现[J]. 南京理工大学学报, 2015, 39(3): 323-329.

[6] 李志远, 蒋爱平, 沈彦琦. 基于 Chen 超混沌和 DNA 编码的图像加密算法[J]. 黑龙江大学自然科学学报, 2020, 37(5): 602-609.

[7] 卢媛君. 基于 RSA 算法和 Chen 超混沌系统的数字图像加密研究[J]. 哈尔滨师范大学自然科学学报, 2024, 40(3): 56-62.

[8] 冯洋. 基于混沌的视频图像加密算法及 FPGA 实现研究[D]: [硕士学位论文]. 成都: 电子科技大学, 2025.

[9] 欧光槟. 基于 FPGA 的同态加密计算加速硬件设计与实现[D]: [硕士学位论文]. 成都: 电子科技大学, 2023.

[10] 刘振. 基于改进 Chen’s 混沌的图像加密算法研究[D]: [硕士学位论文]. 金华: 浙江师范大学, 2023.