基于 FPGA 的 SM4 视频加密系统设计

袁 志[1] 邱 天[1] 林展梧[1] 张 昕[1] 海 燕[2] 周 飞[2]
YUAN Zhi QIU Tian LIN Zhanwu ZHANG Xin HAI Yan ZHOU Fei

摘 要 为解决视频安全的问题，文章提出了一种基于 FPGA 的实时图像采集和数据加密系统设计，旨在提高视频数据的安全性和加密效率。系统利用 OV5640 摄像头采集视频，采用 SM4 国密算法进行数据加密，通过流水线式设计实现每个时钟周期 128 位数据的加密和解密，确保了加密效果和实时性要求，通过 HDMI 接口发送至 HDMI 显示器进行显示。通过仿真验证了 SM4 加密模块的正确性，并分析了系统资源利用率。实验结果表明，该系统能够有效实现视频数据的实时加密和解密，确保了视频数据的安全性，同时满足了实时性要求。

关键词 视频采集；FPGA；SM4；流水线；视频加密

doi：10.3969/j.issn.1672-9528.2025.01.005

0 引言

近年来，全球视频数据泄漏事故频发。这种泄露不仅造成严重的经济损失，还对个人与企业隐私产生巨大危害 [1]。随着视频技术在远程监控、安全防护、工程控制和医疗器械等领域的广泛应用，对视频数据的实时采集、处理和存储提出了更高要求。因此，视频采集系统必须具备高带宽、高速度和高安全性。数据加密在预防视频和图片泄露方面起着关键作用，提高开放网络中通信的安全性 [2]。

为进一步提高数据加密的运行效率 , 利用现场可编程逻辑门阵列（field programmable gate array，FPGA）实现数据加密方案逐渐成为研究热点 [3]。诸多文献都对数据加密进行了硬件加速实现，例如：马绪健等人 [4] 在 FPGA 上实现了 GIFT 分组加密算法的优化，达到了 194 MHz 的频率和 1.2 Gbit/s 的吞吐量；方应李等人 [5] 在 FPGA 上实现了 AES 和 ECC 算法图像加密，通过加入伪随机数、使用列移位替代列混淆运算以及三维 S-box 等方式对传统 AES 进行优化，有效地实现图像加密。

为了在开放的网络环境中实现视频数据的传输，同时保证高效的数据加密，本文提出了一种基于 OV5640 摄像头和 FPGA 的实时图像采集和数据加密系统设计，旨在满足这些需求。系统利用 OV5640 摄像头进行高质量的视频采集，并通过 FPGA 的并行处理能力实现快速的视频加密处理，提高加密效率。为了保护视频数据的安全，系统采用了适用于 FPGA 实现的 SM4 国密算法，通过流水线式设计，实现了每个时钟周期 128 位数据的加密和解密，既保证了加密效果，又满足了实时性要求。

1 SM4 密码算法简介

SM4 是 Feistel 结构的分组密码算法，由轮密钥扩展算法和轮加密算法迭代 32 轮构成，这两个算法的结构都是非线性迭代结构 [6]。SM4 国密算法的明文长度和密钥长度均是 128 位，轮密钥扩展算法和轮加密算法的变换过程相似。轮密钥扩展算法和轮加密算法的第一步都是对 128 位数据进行分组，分为 4 组 32 位数据，其后的操作位数都为 32 位，轮密钥扩展算法通过初始密钥进行迭代扩展得到 32 个轮密钥。采用系统参数 FK 和固定参数 CK 通过轮密钥扩展算法扩展得到轮密钥，轮密钥扩展算法的基本运算包括 S 盒变换、循环左移、异或，S 盒变换是以字节为单位的非线性替换，作用是混淆，输入输出都是 8 字节，循环左移是循环把 32 位字左移指定的位数，异或是 32 位逐比特异或运算 [7-8]。SM4 轮密钥扩展图如图 1 所示。SM4 加密算法使用明文和 32 个轮密钥通过轮加密算法进行 32 轮迭代后，逆序输出得到密文。轮加密算法的基本运算包括 S 盒变换、循环左移、异或。SM4 加密算法和 SM4 解密算法结构完全相同，加密和解密的轮密钥互为逆序 [9]。SM4 轮加密图如图 2 所示。

1. 五邑大学电子与信息工程学院 广东江门 529000
2. 江门市消防救援支队 广东江门 529000
[基金项目] 2021 年江门市创新实践博士后课题研究资助项目（JMBSH2021B04）；广东省重点领域研发计划（2020B0101030002）

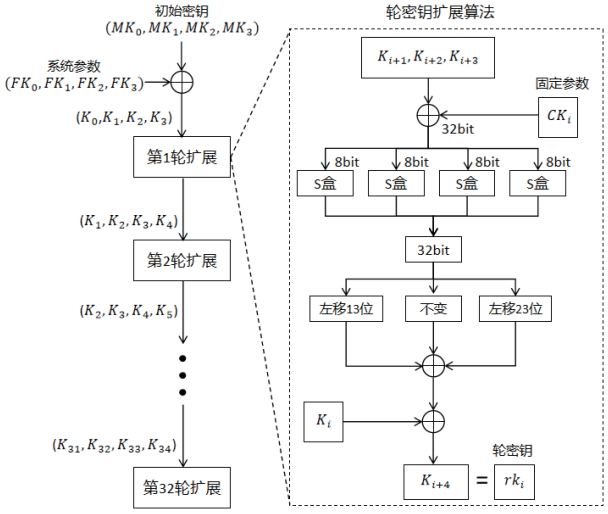


图 1 轮密钥扩展算法

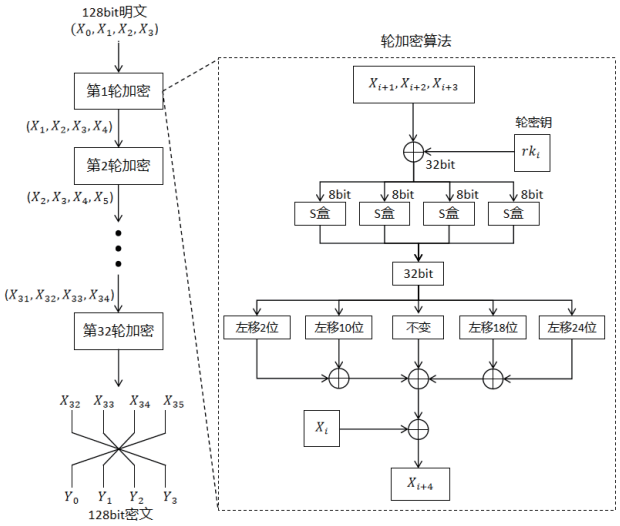


图 2 SM4 轮加密算法

2 流水线式 SM4 加密系统设计

先介绍两种 SM4 加密实现方式：一是循环架构，旨在资源节约，使 SM4 加密算法能轻松部署在资源受限的硬件设备上；二是流水线架构，侧重于性能优化，使 SM4 加密算法适用于对吞吐量要求较高的场景。

2.1 流水线式 SM4 加密系统设计及原理

本文为保证视频加密 / 解密的实时性，采用流水线式架构实现 SM4 加 / 解密。流水线架构与循环架构的硬件结构不同，主要体现在：（1）增加轮密钥寄存器，轮密钥生成模块将 32 个轮密钥存储在寄存器中，每个时钟周期都可向加密模块输入当前轮密钥，确保流水线加密不间断；（2）流水线加密模块实例化 32 个轮加密模块，每个模块间插入寄存器，保证加 / 解密过程的流水线运行 [10]。

在流水线式 SM4 加密模块的加密过程中：在第一个时钟周期 T1 时，明文 D1 流入第 1 轮加密模块进行计算，并将结果存入第 1 轮密文寄存器；在第二个时钟周期 T2 时，第 1 轮密文 D1 流入第 2 轮加密模块进行计算，结果存入第 2 轮密文寄存器。同时，新一组明文 D2 流入第 1 轮加密模块进行计算。到第 32 个时钟周期 T32 时，第 31 轮密文 D1 流入第 32 轮加密模块，结果存入反序变换寄存器，同时第 30 轮明文 D2 流入第 31 轮加密模块。第 33 个时钟周期 T33 时，流水线式 SM4 加密模块输出第一组加密明文 D1 的加密数据；第 34 个时钟周期 T34 时，输出第二组加密明文 D2 的数据，之后每个时钟周期都输出一组明文的加密数据。解密过程与加密过程相同，只是 32 个轮密钥互为反序，即解密算法的第 1 轮密钥为加密算法的第 32 轮密钥。整个 SM4 的流水线加密模块如图 3 所示，SM4 流水线加密流程坐标图如图 4 所示。

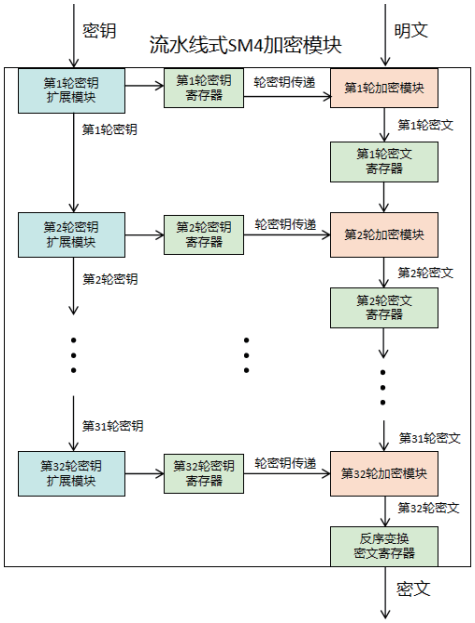


图 3 流水线式 SM4 加密模块图

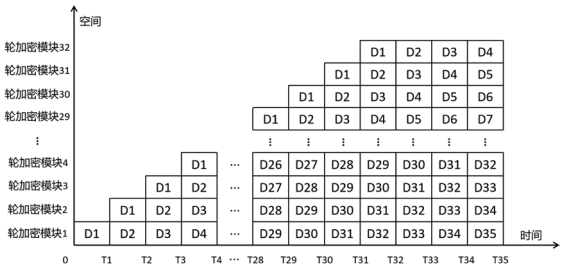


图 4 流水线式 SM4 加密流程坐标图

2.2 流水线架构与循环架构对比

在基于循环式 SM4 加密架构中，仅有 1 个轮加密模块，因此每组明文数据需 32 个时钟周期进行 32 次轮加密迭代才能得到密文，对 n 组明文的加密则需 $32n$ 个时钟周期。而在基于流水线式 SM4 加密架构中，由于 32 个轮加密模块的并行计算特性，从第 33 个时钟周期起，每个时钟周期都会输出 1 组有效密文，对 n 组明文的加密则需 $32+n-1$ 个时钟周期。

假设需加密一张 1024×768 的 RGB565 格式图片，图像数据可拼接为 98 304 组明文数据。理论上，循环式 SM4 加密架构需 3 145 728 个时钟周期，而流水线式 SM4 加密架构仅需 98 335 个时钟周期，减少了 3 047 393 个时钟周期。理论上，使用流水线式 SM4 加密架构可大幅减少加密耗时，提高吞吐量。在本系统中，视频输出为 24 帧 /s，即一秒连续播放 24 张图片，经过上述耗时对比，流水线式 SM4 加密架构可确保视频加密的实时性。循环式和流水线式 SM4 加密耗时对比如表 1 所示。

表 1 循环式和流水线式 SM4 加密耗时对比表

明文组数	循环式 SM4 加密耗时周期数	流水线式 SM4 加密耗时周期数
1	32	32
2	64	33
98 335	3 145 728	98 335
n	32n	32+n-1

3 FPGA 实现 SM4 加密视频采集系统设计

本文设计的基于 FPGA 实现 SM4 加密视频采集系统主要包括 4 个模块：摄像头视频采集模块、视频 SM4 加密模块、视频缓存模块和 HDMI 视频显示模块，系统框图如图 5 所示。摄像头视频采集模块负责配置摄像头并将采集到的视频图像数据输入到 FPGA；视频 SM4 加密模块负责对视频数据进行 SM4 加密，以确保数据的机密性；视频缓存模块负责缓存加密后的视频数据；HDMI 视频显示模块则将缓存的视频数据输出至 HDMI 显示器，最终显示处理结果。

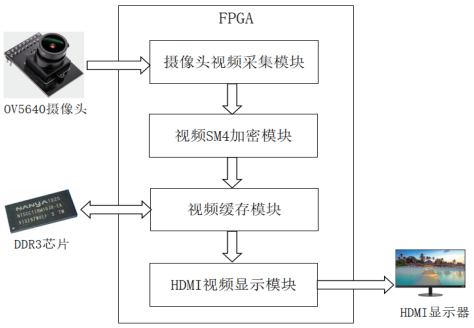


图 5 FPGA 实现 SM4 加密视频采集系统结构图

3.1 摄像头视频采集模块

OV5640 摄像头模组默认输出流为 YUV422 视频数据格式。为了减少数据量并便于接收处理，将视频流格式设置为 RGB565 格式，即每个像素由 2 字节数据构成，其中 2 字节数据包含 5 位红、6 位绿和 5 位蓝。摄像头视频采集模块与 OV5640 摄像头通过 I2C（Inter-Integrated Circuit）协议通信。在本模块中，每当像素时钟的上升沿到达时，OV5640 摄像头模块可以输出 8 位数据，因此每个像素的数据需分两次输出并进行拼接。

3.2 视频 SM4 加密模块

OV5640 摄像头采集的 16 位像素数据被拼接为 128 位，场同步信号和行同步信号也进入加密模块。经过 32 个时钟周期后，输出加密后的数据及延迟后的场同步信号和行同步信号。该视频 SM4 加密模块采用流水线式架构的 SM4 国密加密，确保在系统稳定运行时每个时钟周期都能输出有效密文，从而保证视频数据加密的实时性。

3.3 视频数据缓存模块

视频数据缓存模块接收来自视频 SM4 加密模块的加密视频数据，并将其缓存到第三代双倍速率同步动态随机存储器（DDR3 芯片）中。由于 DDR3 的控制时序相当复杂，为方便用户开发 DDR3 读写应用程序，Xilinx 官方提供了一个 MIG（memory interface generator）IP 核，用于生成 DDR3 控制器。本模块包含一个 MIG IP 核和两个 FIFO（first input first output），分别控制读和写操作。加密模块输出加密后数据和延迟后的场同步信号、行同步信号连接至写 FIFO，控制其对 MIG IP 核进行写操作；在系统判断可以输出第一帧视频数据后，读 FIFO 向 HDMI 视频显示模块发送第一帧视频数据图像。

3.4 HDMI 视频显示模块

HDMI 视频显示模块接收到 DDR3 芯片中存储的加密后视频数据，将 RGB565 格式的视频图像转换成 TMDS 数据输出至 HDMI 显示器，用于后续加 / 解密结果验证。

4 仿真验证和实验结果分析

4.1 SM4 加密仿真

为确保加密数据的正确性，使用仿真对 SM4 加密模块进行加密仿真操作，输入 4 组数据 128'h0123456789ABCDEFFEDCBA9876543210、128'h11111111111111111111111111111111、128'h22222222222222222222222222222222、128'h33333333333333333333333333333333。根据流水线式加密的特性每个时钟周期都会输出一组有效密文，显示仿真结果为：128'h681edf34d206965e86b3e94f536e4246、128'h6b3633a5ed04f5abd5197870b5506642、128'h7c3bc4eb1c18e7f1d879ea602eec46cf、128'h99cfe9d2b4f88cb9d52049f758e230d9，仿真加密结果正确，仿真结果如图 6 所示。

图 6 SM4 加密仿真结果图

4.2 系统资源利用率

SM4 在 Xilinx Artix-7 系列 XC7A35TFGG484-2 器件中，使用 Vivado2020.2 软件进行综合、映射、布局布线和硬件烧录，在布局布线后的资源消耗表如表 2 所示。结果表明，FPGA 具有充足的系统资源来实现 SM4 加解密视频，为数据加密提供了一个功能强大的硬件开发平台。

表 2 系统消耗资源表

资源名称	消耗资源	可用资源	利用率 /%
LUT	11 992	20 800	57.65
FF	10 919	41 600	26.25
BRAM	8	50	16
IO	74	250	29.6
BUFG	8	32	25

4.3 实验结果

本文系统使用 OV5640 摄像头进行视频数据采集，使用 HDMI 显示器进行视频显示，将 OV5640 摄像头和 HDMI 连接线都连接在 FPGA 开发板的对应接口上，并通过 JATG 接口进行比特流烧录，将视频加密系统烧录至 FPGA。实验平台如图 7 所示。

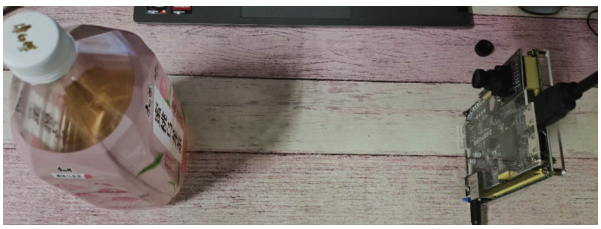
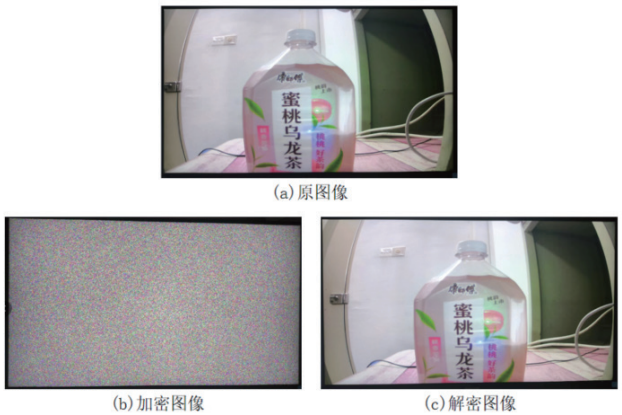


图 7 实验平台图

实验过程中 OV5640 摄像头选用 1024×768 分辨率，用 HDMI 显示器显示验证。实验结果图如图 8 所示，其中视频原始图像如图 8（a）所示，加密后的图像如图 8（b）所示，解密后的图像如图 8（c）所示。



(a) 原图像

(b) 加密图像　　(c) 解密图像

图 8 SM4 加解密视频结果图

5 结语

本文在 FPGA 上搭建了一个视频 SM4 加密系统，将 SM4 加密、摄像头数据读取、HDMI 显示输出集成在 FPGA 芯片中，且使用流水线式 SM4 加密来提高视频加密的实时性，具有集成度高，开发周期短和低功耗等优点。在本改进方法基础上，在接下来的研究将融合 SM2 密码和混沌映射进行混合加密，并实现上位机解密功能。

参考文献：

[1] 朱俊华 . 基于 FPGA 和 H.265 的混沌视频加密系统的设计与实现 [D]. 哈尔滨 : 黑龙江大学 ,2019.

[2] 许盛伟 , 邓烨 , 刘昌赫 , 等 . 一种基于国密算法的音视频选择性加密方案 [J]. 信息网络安全 , 2023,23(11):48-57.

[3] 何诗洋 , 李晖 , 李凤华 . SM4 算法的 FPGA 优化实现方法 [J]. 西安电子科技大学学报 (自然科学报),2021,48(3):155-162.

[4] 马绪健 , 刘姝 , 高铭泽 , 等 . 基于 FPGA 的 GIFT 分组密码算法实现 [J]. 计算机应用研究 ,2023,40(6):1825-1828+1844.

[5] 方应李 , 方玉明 . 基于 FPGA 的 AES 和 ECC 算法图像加密 [J]. 电子科技 , 2024,37(6):92-97.

[6] 中华人民共和国国家质量监督检验检疫总局 , 中国国家标准化管理委员会 . 信息安全技术 SM4 分组密码算法：GB/T 32907—2016[S]. 北京 : 中国标准出版社 ,2016:12.

[7] 吕述望 , 苏波展 , 王鹏 , 等 .SM4 分组密码算法综述 [J]. 信息安全研究 , 2016,2(11):995-1007.

[8] 朱麒瑾 , 陈小文 , 鲁建壮 . 可变流水级 SM4 加解密算法硬件设计及 FPGA 实现 [J]. 计算机工程与科学 , 2024, 46(4): 606-614.

[9] 张宏科 , 袁浩楠 , 丁文秀 , 等 . 基于 FPGA 的 SM4 算法高效实现方案 [J]. 通信学报 ,2024,45(5):140-150.

[10] 窦玉超 .SM4 算法优化及其密钥扩展算法的设计与实现 [D]. 哈尔滨 : 哈尔滨工业大学 , 2021.

【作者简介】

袁志 (1998—)，男，广东河源人，硕士研究生，研究方向：FPGA、数据加密，email: yuanzhi8520@outlook.com。

张昕 (1965—)，通信作者（email: zhangxin800800@163.com），男，黑龙江齐齐哈尔人，博士，教授，研究方向：电子技术、智能制造。

（收稿日期：2024-10-14）