Network Information Security Encryption Scheme Based on an Improved AES Algorithm and Simulation Analysis

Yixin Chen Zeng Ma Bolun Wang

Naval Submarine Academy of the People's Liberation Army of China, Qingdao, Shandong, 266000, China

Abstract

To address the issues of strong pixel correlation and high encryption overhead associated with network images, this paper proposes an encryption scheme based on the Improved Advanced Encryption Standard (AES). The scheme integrates a four-dimensional chaotic sequence into byte substitution, position permutation, and round key generation, and employs the Cipher Block Chaining (CBC) mode to organize data blocks. By recalculating statistical metrics using published simulation datasets, a fixed-throughput delay model is established. The average information entropy for the three ciphertexts is 7.9977 bits, and the absolute value of the correlation coefficient for the Lena ciphertext never exceeds 0.0010; the improved throughput is 2.44 times that of the traditional approach, while the processing time for the same amount of data is reduced by 58.95%. This study provides a basis for configuring the computational capabilities required for network image encryption.

Keywords

network information security; improved AES; chaotic sequence; image encryption; delay model

基于改进AES算法的网络信息安全加密方案及仿真分析

陈怡馨 马曾 王博伦

中国人民解放军海军潜艇学院，中国·山东 青岛 266000

摘要

针对网络图像的像素相关性强、加密开销较高问题，构建基于改进高级加密标准（Advanced Encryption Standard，AES）的加密方案。将四维混沌序列引入字节替代、位置置换和轮密钥生成，采用密码分组链接组织数据块。利用已发表仿真样本复算统计指标，建立固定吞吐率时延模型。三幅密文平均信息熵为7.9977 bit，Lena密文相关系数绝对值均不超过0.0010；改进吞吐率为传统对照的2.44倍，等量数据的模型耗时降低58.95%。研究为网络图像加密的处理能力配置提供依据。

关键词

网络信息安全；改进AES；混沌序列；图像加密；时延模型

1 引言

网络信息传输包含图像、控制指令和结构化记录，业务负载的差异决定了加密处理的组织方式。校园网络的十万条测试样本中，异构信息占69.7%[1]。图像负载连续性强，相邻像素的统计依赖容易保留可识别结构，安全处理应落实到字节值替换、像素位置重排及跨分组扩散。本文面向网络图像传输，将混沌驱动的AES改进机制组织为可分析的加密方案，以已发表仿真样本为基础，比较密文统计特征，复算固定负载的加密耗时，建立算法参数到处理能力的对应关系。

2 负载建模

2.1 图像分组

研究对象设为256×256、灰度深度8 bit的网络图像。单帧包含65536个字节，按128 bit分组后形成4096个状态块，每块按列排列为4×4字节矩阵。分组前，依据置乱序列排序所得原位置索引重排整帧像素，再将结果映射为状态块。接收端通过逆分组映射和逆置乱恢复图像。传输封装保留帧序号、有效长度和算法参数版本，用于密文归属判断。方案以完整帧为处理单元，吞吐率评价覆盖加密计算阶段，网络排队、封装和链路传播分别归入传输层预算。

2.2 链接加密

AES分组运算支持密码分组链接（Cipher Block Chaining，CBC）等工作模式[2]。本文通过CBC连接相邻状态块，当前明文块先同前一密文块异或，再进入改进轮函数；首块通过128 bit初始块启动。由此，图像内的局部变化可以沿链接方向传递，分组密文依赖当前输入及已有链接状态。解密端保持密文顺序，按对应逆变换恢复各块，再消除链接项。会话初始化阶段确定初始块及其使用范围，参数版本贯穿整帧处

【作者简介】陈怡馨（1996-），女，中国山东青岛人，硕士，讲师，从事网络安全、信息加密研究。

理，使通信两端采用一致的恢复条件。

2.3 评价约束

替换盒（Substitution Box，S盒）的构造可通过不可约多项式和仿射参数形成候选集合，并考察平衡性、正交性、雪崩距离及迭代距离[3]。这些指标分别对应输出分布和局部扰动传播特征，适合作为字节替代部件的筛选约束。算法级评价还需检查完整密文的统计分布，将单个部件的代数性质衔接到整帧加密效果。本文设置密文信息熵、像素相关系数、差分变化指标和加密时延四类观测量，分别评价灰度分布、空间依赖、扰动扩散和处理开销，性能结论限定于对应样本及计算模型。

3 轮函数改进

3.1 字节替代

四维混沌驱动的AES方案采用三维S盒、动态交叉移位和前两轮关联的密钥扩展，将轮数设为5轮[4]。本文据此组织轮函数，混沌系统先迭代1000次消除暂态，再生成用于置乱及加密的序列。从加密序列提取256个元素，排序后取得原位置索引，排列成16×16的S盒，再划分为四个8×8子盒。输入字节的8位分别提供3位列地址、3位行地址和2位层地址，寻址关系如图1所示。索引集合覆盖全部256个输入位置，接收端使用相同序列重建映射，按逆索引完成字节恢复。

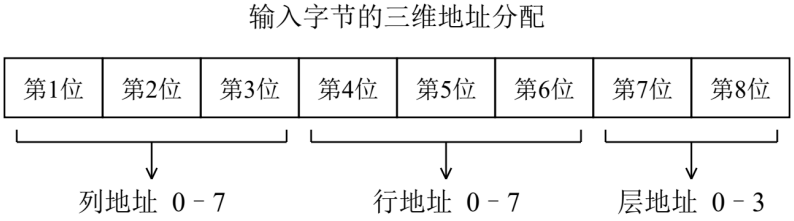


图1 三维替换盒的字节寻址

3.2 位置置换

字节替代改变数值后，动态交叉移位进一步重组状态矩阵的位置。混沌序列的分组控制值选择交叉读取次序，沿矩阵主对角线或副对角线展开，再将读取结果回写状态块。重排对象为完整16字节索引集合，处理前后保持分组长度和字节数量一致。位置变化使原有邻接关系重新分配，后续列混淆在新的列组合上扩散字节影响。前4轮包含列混淆，第5轮通过字节替代、交叉移位和轮密钥加完成输出。解密侧保存对应逆置换，按照轮序反向恢复，确保像素位置映射闭合。

3.3 轮钥生成

轮密钥扩展把前两轮信息引入当前轮计算，结合动态移位、三维S盒替代和混沌字节异或，形成连续轮钥序列。初始密钥由混沌加密序列中的16个元素组成，后续序列片段分别承担首轮扩展、移位控制和初始块生成任务。参数组织以系统参数、初值和序列截取位置为整体，通信两端采用一致的数值精度和迭代次序。该设计增加轮密钥生成路径的变化，但5轮结构的评价重点仍是完整算法的扩散效果；信息熵及差分测试反映统计表现，密码分析用于进一步判定抗攻击强度。

4 仿真分析

4.1 统计特征

采用上述混沌方案已发表的Lena、Cameraman和Boat三幅灰度图像仿真样本开展复算。原始测试平台为Intel Core i5-11300H处理器，主频3.10 GHz，软件环境为Python 3.6。三幅改进密文的平均信息熵为7.9977 bit，相对8 bit上限的平均差约0.0023 bit。Lena密文水平、垂直、对角方向的相关系数为0.0005、−0.0010、−0.0006，空间线性依赖较弱，支持该样本范围内的统计均匀性判断。

4.2 差分扩散

采用像素数变化率（Number of Pixels Change Rate，NPCR）和统一平均变化强度（Unified Average Changing Intensity，UACI）评价明文扰动后的密文变化，结果见表1。NPCR表示改变位置的占比，UACI反映归一化灰度差幅度，二者从不同侧面描述扩散。改进样本的NPCR集中在99.604%～99.613%，UACI集中在33.459%～33.473%，三幅图像表现接近。传统对照的部分单项值更大，差分评价应结合随机变化的目标分布，而非按数值大小直接排序；结论定位为测试样本的扩散表现。

表1 改进算法的差分测试结果

图像	NPCR / %	UACI / %
Cameraman	99.613	33.459
Lena	99.604	33.460
Boat	99.608	33.473

4.3 加密时延

原始吞吐率由三幅图像各计算100次后求平均得到，改进方案为45.85 Mbit/s，传统AES对照为18.82 Mbit/s。以该测值构建固定吞吐率模型，连续帧的纯加密耗时按式1计算。

$$t = \frac{NF}{R \times 10^{6}} \tag{1}$$

式中，t为加密耗时，单位s；N为连续处理帧数，取1～3；F为单帧数据量，取524288 bit；R为吞吐率，单位Mbit/s。模型结果如图2所示，单帧耗时分别为0.01143 s和0.02786 s，三帧为0.03430 s和0.08357 s。吞吐率比为2.44，等量负载耗时降低58.95%。该曲线刻画固定处理能力下的负载关系，适用于加密阶段容量估算。

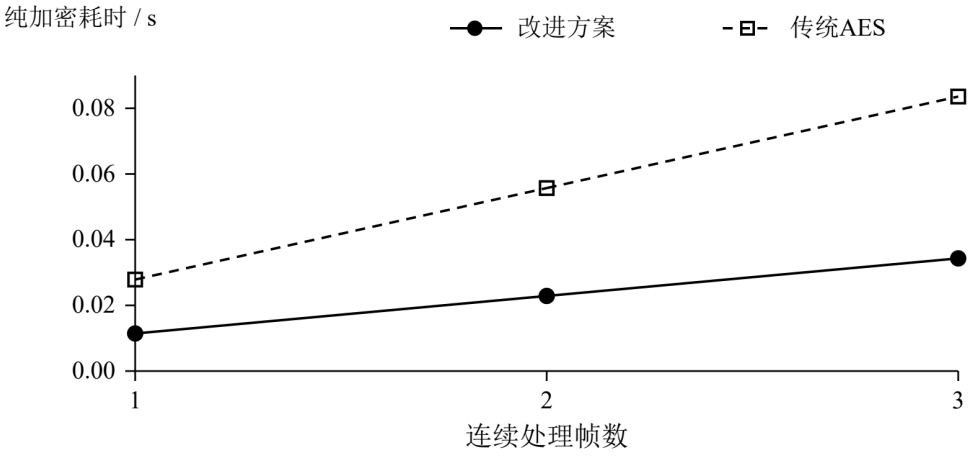


图2 连续图像的模型加密耗时

5 结语

本文围绕网络图像负载，组织混沌序列驱动的字节替代、交叉移位及轮密钥扩展，并以CBC形成跨分组链接。已发表仿真样本的复算结果显示，改进密文具有接近8 bit的信息熵和较弱的像素相关性，差分指标在三幅测试图像间保持集中。固定吞吐率模型下，等量数据的纯加密耗时降低58.95%，可用于处理能力配置。方案评价以图像样本的统计表现和时延预算为依据，工程部署还需完成轮函数密码分析、数值实现一致性校核及会话参数管理，使算法性能落实到可验证的传输条件。

参考文献

[1] 李楠. 改进AES算法下的校园网络信息安全传输方法研究[J]. 信息记录材料, 2026, 27(2):66-68.

[2] 王刚. 基于AES算法的无线传感网络信息采集安全加密技术研究[J]. 长江信息通信, 2022(10):20-24.

[3] 陈靖, 汪烈军, 钟劲松, 等. 改进型AES加密算法在无线传感器网络中的研究与实现[J]. 现代电子技术, 2021, 44(12):44-48.

[4] 唐辰, 涂喜梅, 陆晓刚, 等. 基于四维混沌系统的改进AES图像加密算法[J]. 系统工程与电子技术, 2023, 45(12):4040-4051.