一种新型特征感知混沌图像加密方案用于物联网和边缘网络的数据安全与隐私保护

Muhammad Shahbaz Khan*, Ahmed Al-Dubai*, Jawad Ahmad†, Nikolaos Pitropakis* and Baraq Ghaleb*
*School of Computing, Engineering and the Built Environment,
Edinburgh Napier University, Edinburgh, UK.
Emails: {muhammadshahbaz.khan, a.al-dubai, n.pitropakis, b.ghaleb}@napier.ac.uk
†Cyber Security Center, Prince Mohammad Bin Fahd University, Al-Khobar, Saudi Arabia
Email: jahmad@pmu.edu.sa

摘要—物联网 (IoT) 和边缘网络中图像数据的安全性至关重要，因为智能系统的部署越来越多地用于实时决策。

传统的加密算法如 AES 和 RSA 对于资源受限的 IoT 设备来说计算成本高，并且对大量图像数据无效，从而导致隐私保护分布式学习应用效率低下。

为了解决这些问题，本文提出了一种新的特征感知混沌图像加密方案，该方案将特征感知像素分割 (FAPS) 与混沌链置换和混淆机制结合起来，以增强安全性同时保持高效性。

所提出的方案包括三个阶段：(1) FAPS，根据高边缘强度和低边缘强度特性提取并重新组织像素，以破坏相关性；(2) 混沌链置换，使用基于 SHA-256 动态更新密钥的逻辑混沌映射进行块级置换；以及 (3) 混沌链混淆，利用动态生成的混沌种子矩阵执行位 XOR 操作。

广泛的性能和安全性评估表明，所提出的方案显著减少了像素相关性——接近于零，并且实现了接近 8 的高熵值，还抵抗了差异密码攻击。

所提出方案的最佳设计使其适合在资源受限环境中实时部署。

***Index Terms*—物联网安全，数据隐私，图像加密，混淆，置换**

I. 介绍

物联网 (IoT) 和边缘计算的快速发展已经改变了包括智慧城市、工业自动化和医疗保健在内的各个领域 [1]–[3]。这些系统依赖分布式机器学习 (ML) 和人工智能 (AI) 来处理实时数据，并在资源受限设备上做出智能决策。然而，在这种去中心化环境中确保图像数据的安全性和隐私性仍然是一个重大挑战 [4]。敏感图像，包括医疗扫描、监控录像和工业监测数据，经常通过异构网络传输和处理，使其容易受到窃听、未经授权的访问和对抗性攻击 [5]–[7]。传统的加密技术，如 AES 和 RSA，由于其高计算复杂度和对大数据处理效率低下，并不适合用于 IoT 和基于边缘的 AI 应用 [8], [9]。因此，需要轻量级和自适应的加密算法来保护隐私同时保持系统的可扩展性和效率。

基于混沌的图像加密技术在分布式环境中保护图像数据方面显示出巨大的潜力 [10]–[12]。混沌系统具有对初始条件敏感、伪随机性和遍历性的特性，使其非常适合于密码学应用 [13]–[15]。各种混沌映射，包括 Logistic 映射 [16]、Henon 映射 [17] 和 Lorenz 系统 [18]，已被用于图像加密方案中。这些方法利用由混沌序列驱动的置换和替换过程来破坏像素相关性并增强安全性。然而，现有的混沌加密方案往往无法满足物联网和边缘网络的隐私及效率要求。许多方法依赖于静态混沌参数，这可能导致周期性行为并降低安全性。此外，传统的混沌置换通常与底层图像结构无关，对于实时基于机器学习的边缘分析而言计算效率低下。

为解决上述挑战，本文提出了一种面向物联网和边缘智能系统的隐私保护图像加密框架，该框架集成了特征感知像素分割（FAPS）与混沌链置换和混淆机制。通过整合这些技术，所提出的方案增强了数据保护和隐私。图 1给出了所提方案的概述。本文的主要贡献如下：

- 一种新型的特征感知像素分割（FAPS）技术，通过减少图像数据中的相关性来优化面向 AI 驱动的物联网和边缘网络的图像加密。该技术基于高低边缘强度特征提取并重新组织像素以有效破坏相关性。
- 一种使用基于 SHA-256 的动态密钥生成的逻辑混

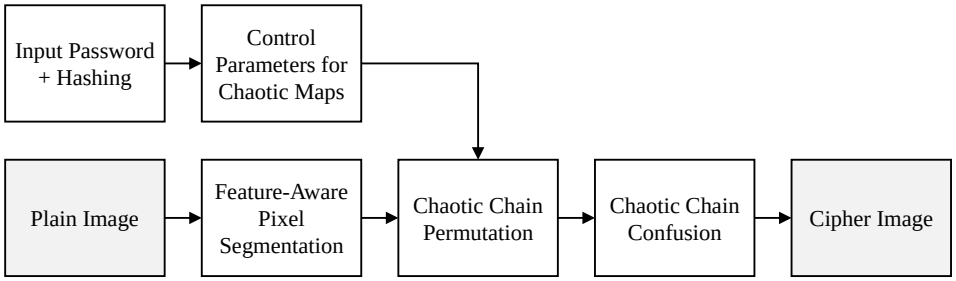


图 1: 所提出的特征感知加密方案概述

沌映射方法，确保自适应安全性和增强随机性。混沌链置换

- 一种利用动态生成的混沌种子矩阵进行混淆阶段比特位异或操作的混沌链混淆机制，使加密方案能够抵御密码攻击。

本文的其余部分结构如下：第二节介绍了所提出的加密方案的细节，包括特征感知像素分割、混沌链置换和混沌链混淆。第四节提供了安全分析和实验结果，而第五节给出了清晰简洁的结论。

II. 提出的特征感知混沌图像加密方案

所提出的方案包括三个阶段：(1) 特征感知像素分割，根据边缘强度对像素进行分类以优化加密；(2) 混沌链置换，应用动态更新的逻辑混沌映射进行分块置换；以及 (3) 混沌链混淆，与动态混沌种子矩阵随机性执行按位异或操作。包含所有三个阶段的完整方框图如图 2所示，并在以下子章节中进行了说明。此外，还提供了用于所提方案逐步实现的伪代码算法，见算法 1。

A. 阶段 1: 特征感知像素分割 (FAPS)

本文提出了一种特征感知像素分割（FAPS）技术，用于在安全排列图像之前进行预处理。该方法利用 Sobel 边缘检测将像素分割为高方差和低方差区域。对于一个 16×16 样本图像的方差分类概述如图 3所示，而对于一个 256×256 摄像师图像，带有高低方差区域分割的边缘检测过程则在图 4中描绘。

令 $I(x,y)$ 为大小为 $M\times N$ 的灰度图像，其中每个像素的强度值在范围 $I(x,y)\in[0,255]$ 内。所提出的方法遵循以下步骤：

1) Sobel 边缘检测: Sobel 算子计算每个像素的梯度幅度以测量边缘强度：

$$G_x = I(x,y) * S_x, \quad G_y = I(x,y) * S_y \tag{1}$$

其中 S_x 和 S_y 是水平和垂直 Sobel 核：

$$S_x = \begin{bmatrix} -1 & 0 & +1 \\ -2 & 0 & +2 \\ -1 & 0 & +1 \end{bmatrix}, \quad S_y = \begin{bmatrix} +1 & +2 & +1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} \tag{2}$$

然后计算每个像素的边缘幅度为：

$$G_{sobel}(x,y) = \sqrt{G_x^2 + G_y^2} \tag{3}$$

边缘图然后被归一化：

$$E(x,y) = \frac{G_{sobel}(x,y)}{\max(G_{sobel})} \tag{4}$$

其中 $E(x,y)\in[0,1]$ 代表归一化的边缘强度。

2) 高边缘和低边缘像素分类: 在此步骤中，定义了一个阈值 T，该阈值是使用 Otsu 方法获得的：

$$T = \arg\max_{\tau}[\sigma_B^2(\tau)] \tag{5}$$

其中 $\sigma_B^2(\tau)$ 是给定阈值 τ 的类间方差。使用此阈值，我们将像素分类为高边缘（HE）和低边缘（LE）区域：

$$P_{HE} = \{I(x,y) \mid E(x,y) > T\} \tag{6}$$

$$P_{LE} = \{I(x,y) \mid E(x,y) \le T\} \tag{7}$$

其中 P_{HE} 包含纹理和边界区域，而 P_{LE} 包含平滑区域。

3) 像素排序和分组: 为了准备混沌置换，像素以结构化的方式重新排序。高边缘像素按降序排列并放置在图像的上半部分：

$$P'_{HE} = \text{sort}(P_{HE}, \text{descend}) \tag{8}$$

另一方面，低边缘像素按升序排列并放置在下半部分：

$$P'_{LE} = \text{sort}(P_{LE}, \text{ascend}) \tag{9}$$

最终的预置换图像 I' 定义为：

$$I' = \begin{bmatrix} P'_{HE} \\ P'_{LE} \end{bmatrix} \tag{10}$$

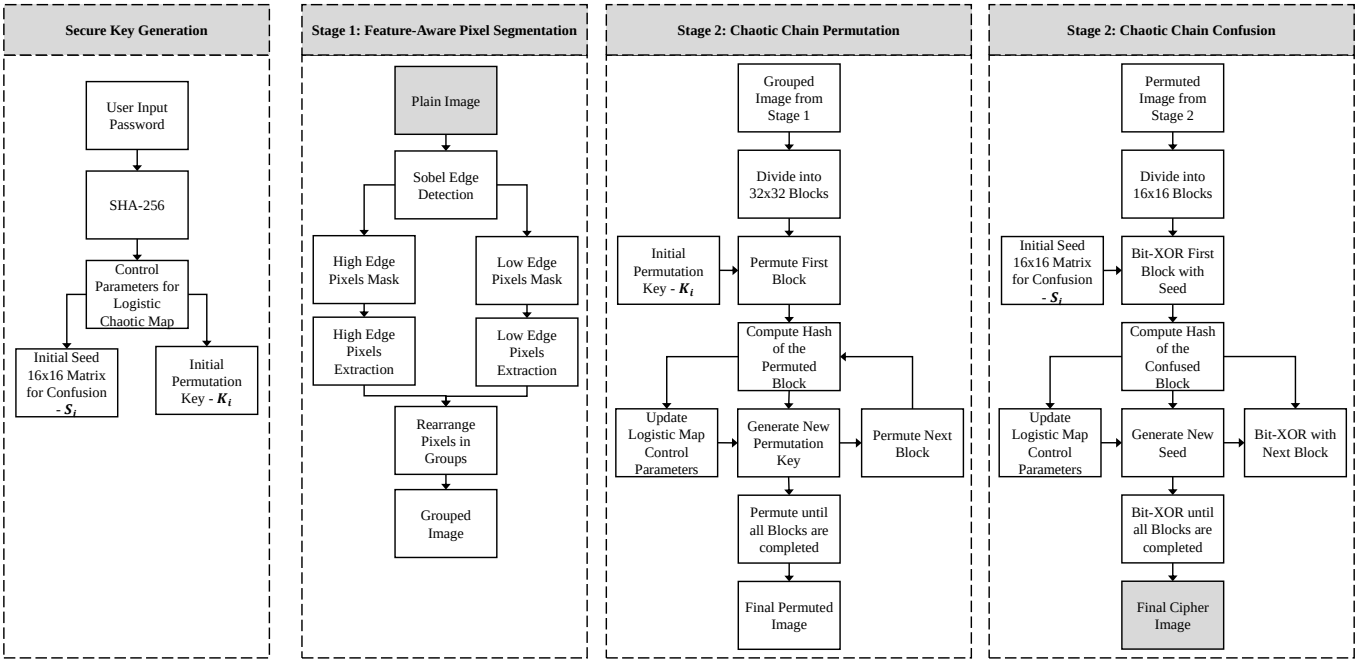


图 2: 所提出的特征感知加密方案的完整框图

B. 阶段 *2*: 混沌链置换

图像预处理完成后，以块的方式应用基于逻辑映射的混沌置换。

1) 图像 I' 被划分为 $B \times B$ 个不重叠的块：

$$I' = \{B_1, B_2, ..., B_k\}, \quad B_i \in \mathbb{R}^{b \times b}, \quad k = \frac{M \times N}{B^2} \tag{11}$$

其中每个块 B_i 的尺寸为 32×32。

2) 逻辑混沌映射用于生成初始排列密钥，定义为：

$$X_{n+1} = rX_n(1 - X_n) \tag{12}$$

其中 $X_n \in (0, 1)$ 是状态变量，r 是混沌控制参数。初始密钥 X_0 在混沌范围内随机选择，并用于置换第一个块。

3) 第一个置换块 B_1 的哈希 H_1 是使用 SHA-256 计算的。此哈希用于更新逻辑斯蒂映射的初始条件和控制参数，以生成第二个区块的新置换密钥。这一过程迭代进行每个置换块 B_i。每个时钟 B_i 使用新的置换密钥进行置换，并使用 SHA-256 计算其哈希值 H_i，用于下一个区块。

$$H_i = \text{SHA-256}(B_i') \tag{13}$$

混沌系统的参数随后被更新：

$$X_0 = \frac{H_i}{2^{256}}, \quad r = 3.9 + 0.1 \times \left(\frac{H_i \mod 100}{100} \right) \tag{14}$$

4) 该过程对所有区块重复进行，确保每个区块的排列受到前一个区块哈希的影响。

5) 置换后的块组合形成最终的加密图像：

$$I_{\text{perm}} = \begin{bmatrix} B_1' & B_2' & \dots & B_k' \end{bmatrix} \tag{15}$$

C. 阶段 *3*: 混沌链混淆

置换过程后，图像采用逻辑混沌映射和按位异或操作进行分块混淆处理以增强安全性。此过程确保每个区块都受到前一个区块哈希的影响，使得混淆过程高度依赖初始条件。

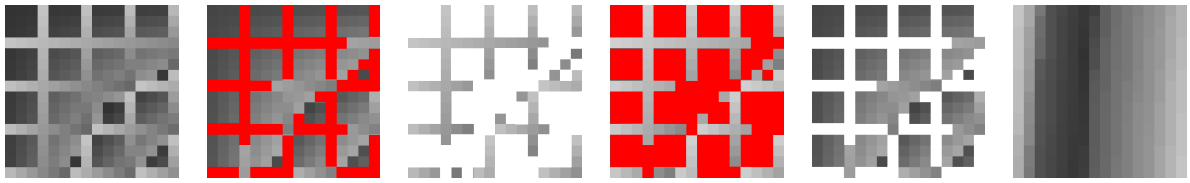
1) 置换后的图像 I_{perm} 被分为 16×16 个不重叠的块：

$$I_{\text{perm}} = \{B_1, B_2, ..., B_m\}, \quad B_i \in \mathbb{R}^{16 \times 16}, \quad m = \frac{M \times N}{16^2} \tag{16}$$

其中每个块 B_i 的尺寸为 16×16。

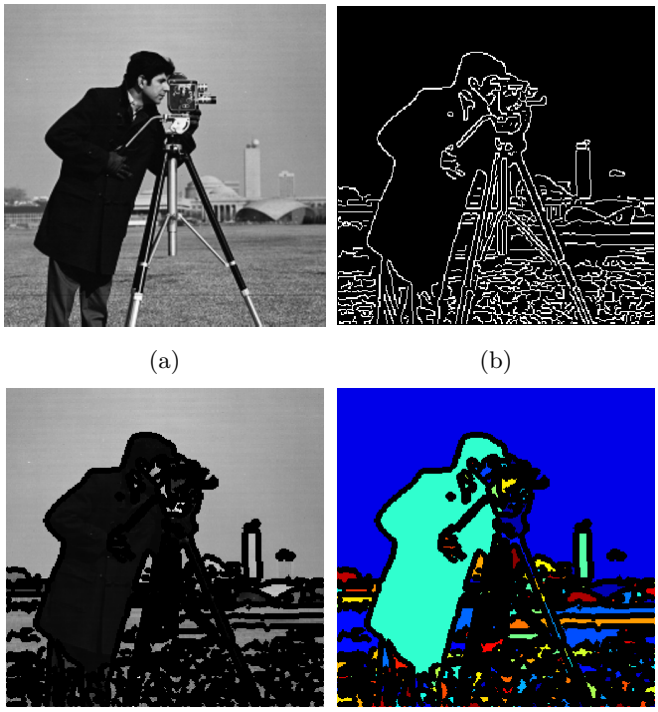
2) 一个使用逻辑斯蒂映射生成的混沌种子矩阵 S_1，其大小为 16×16：

$$X_{n+1} = rX_n(1 - X_n) \tag{17}$$



(a) (b) (c) (d) (e) (f)

图 3: 高边缘和低边缘像素分类在 FAPS 中的概述



(a) (b) (c) (d)

图 4: Cameraman 图像特征提取过程的不同阶段。

其中 $X_n \in (0,1)$ 和 r 是混沌控制参数。初始种子矩阵由以下给出：

$$S_1(i,j) = \lfloor 256 X_{n_{i,j}} \rfloor, \quad i,j = 1,2,\ldots,16 \tag{18}$$

其中 $X_{n_{i,j}}$ 是映射到 $[0,255]$ 中整数的混沌值。

3) 第一个块 B_1 使用按位异或操作与种子矩阵混淆：

$$C_1 = B_1 \oplus S_1 \tag{19}$$

其中 C_1 是混淆后的输出块。

4) 混淆块 C_1 使用 SHA-256 进行哈希：

$$H_1 = \text{SHA-256}(C_1) \tag{20}$$

该哈希输出用于更新混沌系统参数：

$$X_0 = \frac{H_1}{2^{256}}, \quad r = 3.9 + 0.1 \times \left(\frac{H_1 \mod 100}{100} \right) \tag{21}$$

使用更新后的参数生成新的混沌种子矩阵 S_2：

$$S_2(i,j) = \lfloor 256 X_{n_{i,j}} \rfloor \tag{22}$$

5) 该过程迭代地适用于所有块 B_i，其中每个混淆的块 C_i 影响下一个种子矩阵的生成：

$$C_i = B_i \oplus S_i \tag{23}$$

$$H_i = \text{SHA-256}(C_i) \tag{24}$$

$$X_0 = \frac{H_i}{2^{256}}, \quad r = 3.9 + 0.1 \times \left(\frac{H_i \mod 100}{100} \right) \tag{25}$$

其中更新后的值再生 S_{i+1} 用于下一个块。

6) 所有块处理完毕后，通过组合所有的混淆块获得最终的混淆图像 I_{conf}。

$$I_{\text{conf}} = \begin{bmatrix} C_1 & C_2 & \ldots & C_m \end{bmatrix} \tag{26}$$

III. 结果与安全分析

本节通过熵分析、相关性分析以及对明文图像微小变化的差分攻击或敏感性分析来评估所提出的加密方案的性能。

A. 直方图分析

一个有效的加密方案应生成具有均匀直方图的密文图像，确保抵抗基于频率的攻击。如图 5所示的加密图像的直方图表明像素强度分布接近均匀，这说明加密过程有效地扩散了像素值。

Algorithm 1 所提图像加密方案的实现及其

输入： 灰度图像大小为 $M \times N$
输出： 加密图像
步骤 1：特征感知像素分割
应用 Sobel 边缘检测以突出纹理和边缘
计算边缘图并归一化值
使用 Otsu 方法对高纹理和低纹理像素进行分类
根据特征分类排序和分组像素
重构分割图像
步骤 2：混沌链置换
将图像分为非重叠的 32×32 块
使用初始密钥初始化逻辑混沌映射
for each block **do**
    使用混沌映射生成唯一的排列序列
    根据序列排列块像素
    计算排列后的块的 SHA-256 哈希值
    使用哈希输出更新混沌映射参数
end for
重构排列图像
步骤 3：混沌链混淆
将图像分为非重叠的 16×16 块
for each block **do**
    生成动态混沌种子矩阵
    对块和种子矩阵进行按位异或操作
    计算混淆后的块的 SHA-256 哈希值
    使用哈希输出更新混沌映射参数
end for
重构最终加密图像

表 I: 相关性评估

高级的	测试图像	相关性。值	相关系数		
			水平。	版本	图 diag.
1	Cameraman	0.00012	-0.0006	0.0068	-0.0071
2	Baboon	0.00045	0.0028	0.0029	0.0021
3	Houses	0.00038	-0.0049	-0.0036	0.0053

表 II: 信息熵评估

女士	图像	普通图像	密文图像
1	Cameraman	7.448	7.998
2	Baboon	7.051	7.998
3	Houses	7.011	7.998

B. 相关性分析

图像加密旨在消除像素相关性以防止统计攻击。表 I显示了明文和密文图像的相关系数。由于自然冗余，明文图像表现出强烈的相关性，而加密后的图像在水平、垂直和对角线方向上接近零值。此外，图 5描绘了所有相关系数的有效扩散，表明最大相关破坏。相关性通过以下方式找到：

$$r = \frac{\sum_{i=1}^{N}(x_i - \mu_x)(y_i - \mu_y)}{\sqrt{\sum_{i=1}^{N}(x_i - \mu_x)^2}\sqrt{\sum_{i=1}^{N}(y_i - \mu_y)^2}} \tag{27}$$

其中：

- r 是相邻像素之间的相关系数。
- x_i 和 y_i 是两个相邻像素的强度值。
- μ_x 和 μ_y 是图像中所有像素的平均强度值。
- N 是用于相关计算的像素对总数。

C. 熵分析

信息熵衡量图像的随机性，理想情况下完全加密图像的熵值接近 8。表 II提供了原始图像及其相应密文图像的熵值。由于冗余像素结构的存在，原始图像的熵显著较低，而密文图像始终达到接近 7.998 的值，这表明加密过程具有高度不可预测性和安全性。

$$H(X) = -\sum_{i=0}^{255} P(x_i)\log_2 P(x_i) \tag{28}$$

其中：

- $H(X)$ 是图像的香农熵。
- $P(x_i)$ 表示强度级别 x_i 的发生概率。
- 求和运行涵盖所有可能的强度值从 0 到 255 对于一个 8 位灰度图像。

D. 差分攻击抵抗力

一个高度安全的加密算法应对明文中的任何微小修改敏感。为了评估这一点，进行了一次单比特差异测试，在此测试中，一张图像被两次加密：首先以原始形式加密，然后将明文中的一位改变后再加密。计算了两个密文图像之间的绝对差异，以分析这一轻微修改的传播效应。图 6中的结果表明，两个加密图像之间的差异显著，突显了所提出的加密方案的雪崩效应。

IV. 结论

本文提出了一种新颖的特征感知混沌图像加密方案，旨在提升物联网和边缘网络中的安全性和隐私保护。所提方法集成了特征感知像素分割、混沌链置换和混沌链混淆，有效扰乱了像素相关性，并增强了对统计攻击和差分攻击的抵抗能力。实验结果表明，该方案实现了接近理想的熵值，并显著降低了加密图像的相关性，确保了强大的安全性。此外，敏感性分析证实了加密过程表现出强烈的雪崩效应，使其能够抵御差分攻击。所提方法提供了一种轻量级且健壮的加密机制，适用于资源受限环境，从而有助于智能分布式系统中安全的图像传输和存储。未来工作可能探索硬件加速和自适应混沌模型以进一步优化性能和安全性。

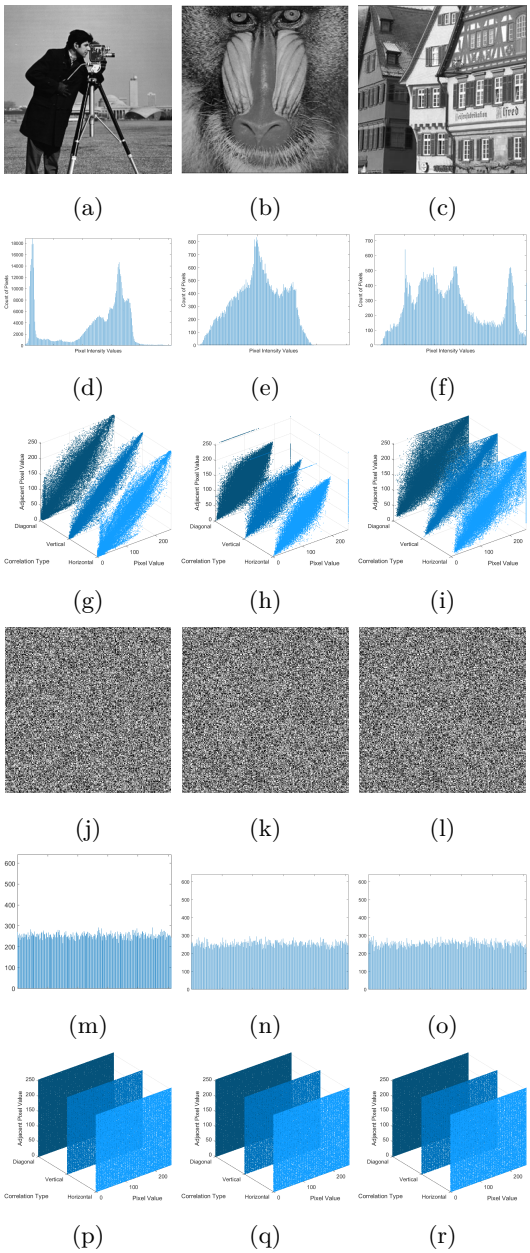


图 5: 带有直方图和相关性分析的加密结果

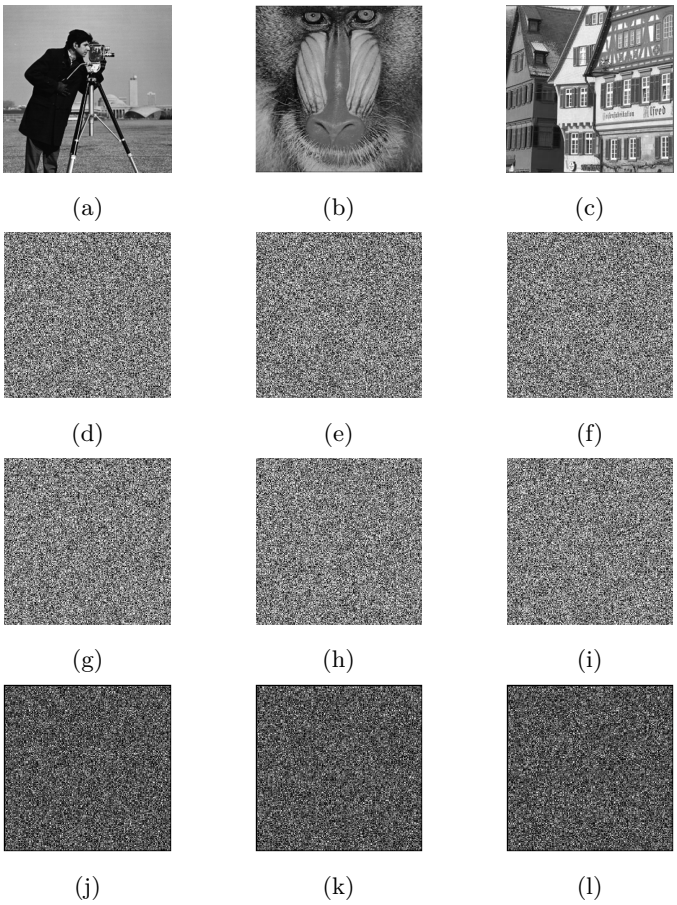


图 6: 差分攻击/敏感性分析。(a-c) 原始测试图像。(d-f) 原始密文图像。(g-i) 一位错误的明文图像对应的密文图像。(j-l) 原始和错误密文图像之间的差异。

参考文献

[1] R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the power of iot: A comprehensive review of iot applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0," *Sensors*, vol. 23, no. 16, p. 7194, 2023.

[2] Y. Perwej, K. Haq, F. Parwej, M. Mumdouh, and M. Hassan, "The internet of things (iot) and its application domains," *International Journal of Computer Applications*, vol. 975, no. 8887, p. 182, 2019.

[3] R. R. Harmon, E. G. Castro-Leon, and S. Bhide, "Smart cities and the internet of things," in *2015 Portland international conference on Management of Engineering and Technology (PICMET)*. IEEE, 2015, pp. 485–494.

[4] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[5] M. Shahbaz Khan, J. Ahmad, A. Al-Dubai, N. Pitropakis, B. Ghaleb, A. Ullah, M. Attique Khan, and W. J. Buchanan, "Chaotic quantum encryption to secure image data in post quantum consumer technology," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 4, pp. 7087–7101, 2024.

[6] J. J. Hathaliya, S. Tanwar, and P. Sharma, "Adversarial learning techniques for security and privacy preservation: A comprehensive review," *Security and Privacy*, vol. 5, no. 3, p. e209, 2022.

[7] L. Tang, H. Hu, M. Gabbouj, Q. Ye, Y. Xiang, J. Li, and L. Li, "A survey on securing image-centric edge intelligence," *ACM Transactions on Multimedia Computing, Communications and Applications*, 2024.

[8] M. S. Khan, J. Ahmad, H. Ali, N. Pitropakis, A. Al-Dubai, B. Ghaleb, and W. J. Buchanan, "Srss: A new chaos-based single-round single s-box image encryption scheme for highly auto-correlated data," in *2023 International Conference on Engineering and Emerging Technologies (ICEET)*, 2023, pp. 1–6.

[9] H. Ali, M. S. Khan, M. Driss, J. Ahmad, W. J. Buchanan, and N. Pitropakis, "Cellsecure: Securing image data in industrial internet-of-things via cellular automata and chaos-based encryption," in *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*, 2023, pp. 1–6.

[10] T. Umar, M. Nadeem, and F. Anwer, "Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage," *Expert Systems with Applications*, vol. 257, p. 125050, 2024.

[11] M. S. Khan, J. Ahmad, A. Al-Dubai, Z. Jaroucheh, N. Pitropakis, and W. J. Buchanan, "Permutex: Feature-extraction-based permutation — a new diffusion scheme for image encryption algorithms," in *2023 IEEE 28th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2023, pp. 188–193.

[12] Y. Lin, Z. Xie, T. Chen, X. Cheng, and H. Wen, "Image privacy protection scheme based on high-quality reconstruction dct compression and nonlinear dynamics," *Expert Systems with Applications*, vol. 257, p. 124891, 2024.

[13] Y. Zhang, J. Lu, C. Zhao, Z. Li, and J. Yan, "Chaos optimization algorithms: A survey," *International Journal of Bifurcation and Chaos*, vol. 34, no. 16, p. 2450205, 2024.

[14] M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," *Multimedia Tools and Applications*, vol. 81, no. 18, pp. 25 497–25 518, 2022.

[15] M. S. Khan, J. Ahmad, A. Al-Dubai, N. Pitropakis, M. Driss, and W. J. Buchanan, "A novel cosine-modulated-polynomial chaotic map to strengthen image encryption algorithms in iot environments," *Procedia Computer Science*, vol. 246, pp. 4214–4223, 2024, 28th International Conference on Knowledge Based and Intelligent information and Engineering Systems (KES 2024). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050924022804

[16] W. Wu and Q. Wang, "Quantum image encryption based on baker map and 2d logistic map," *International Journal of Theoretical Physics*, vol. 61, no. 3, p. 64, 2022.

[17] Y. Chen, S. Xie, and J. Zhang, "A hybrid domain image encryption algorithm based on improved henon map," *Entropy*, vol. 24, no. 2, p. 287, 2022.

[18] W. Alexan, M. ElBeltagy, and A. Aboshousha, "Rgb image encryption through cellular automata, s-box and the lorenz system," *Symmetry*, vol. 14, no. 3, p. 443, 2022.