

基于蛋白质结构投影的图像加密

安成昊 曾泓然 郭俊峰 张重阳 李小伟 刘寿鑫 (通讯作者)

四川大学, 四川成都, 610040;

摘要: 针对二维图像的安全保护需求, 本文提出一种基于蛋白质的二维图像加密方法。该方法创新性地将蛋白质的复杂结构特性与图像加密技术相结合。加密过程中, 先对图像进行分块处理, 再利用矩阵完成加密; 所有加密矩阵均源于同一种蛋白质, 通过提取不同空间信息并经旋转、折叠等空间变换, 生成差异显著的加密矩阵以实现图像加密。实验结果表明, 该方法加密速度快, 且兼具高安全性与强鲁棒性, 为二维图像提供了高效可靠的加密方案。

关键词: 蛋白质; 结构投影; 图像加密

DOI: 10.69979/3041-0673.26.04.006

1 研究背景

随着数字内容交互方式的不断发展, 图像安全保护已成为关键需求。现有图像加密方法多基于传统数学、光学或 DNA 技术, 但这些方法未专门针对图像的空间冗余特性进行优化, 难以兼顾加密安全性与效率。

目前, 尚未有研究利用蛋白质结构的复杂特性开展图像加密工作。蛋白质合成过程中, 氨基酸种类、序列排列及肽链长度均会影响肽链特性, 而肽链折叠的过程涉及更为复杂的变换。基于此, 本文提出一种新型蛋白质合成模型, 将其应用于图像加密, 为二维图像提供高

效安全的加密方案。

具体而言, 本文通过单肽链模拟蛋白质合成过程: 包含多种氨基酸, 计算并存储各氨基酸的坐标 (RC); 采用两种空间变换 (ST) 改变肽链结构。在此基础上, 提出空间投影 (SP) 和质量分配 (MD) 算法生成加密矩阵 (E-Mat), 该矩阵具有高度随机性, 且无法通过其反推蛋白质结构, 从而保障了加密安全性。

2 加密过程

加密过程主要分为氨基酸初始化, 肽链生成和转化, 肽链结构投影和分块加密四个步骤, 示意图如图 1 所示。

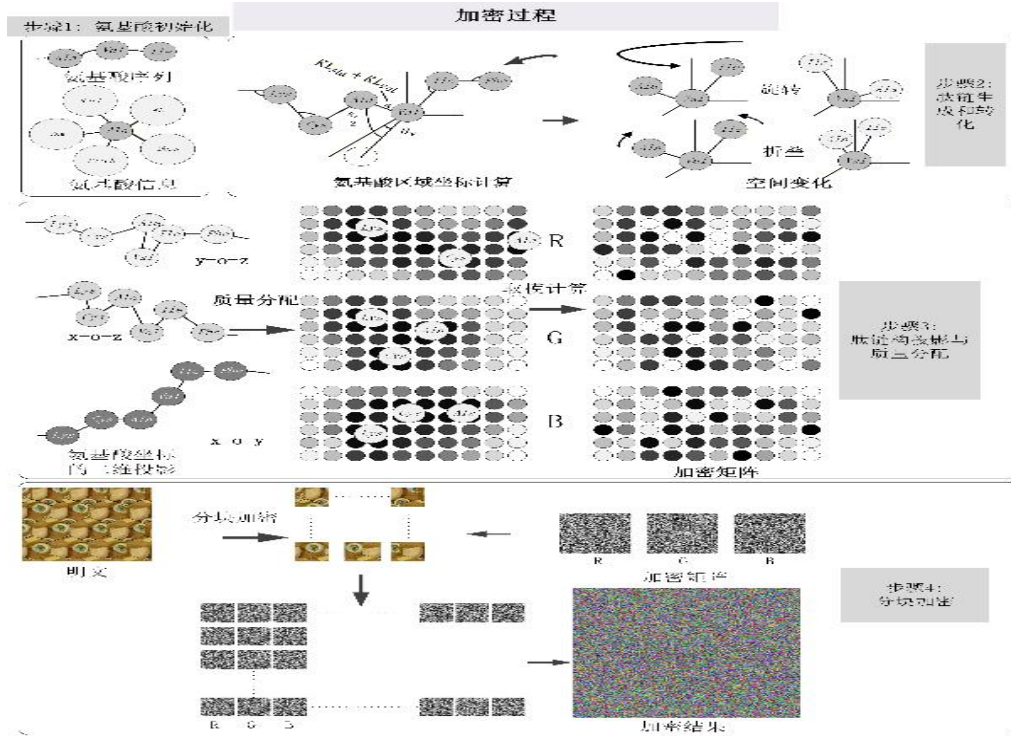


图 1 加密过程示意图

其中 Ala, Val 等为氨基酸种类, Roll, Yaw, Pitch 为旋转角, KL 为键长, Mass 为氨基酸相对分子质量, RGB 分别代表图像的红、绿、蓝通道。

2.1 氨基酸初始化

氨基酸 (AA) 是蛋白质的主要组成成分, 也是本文所提方案的核心元素。蛋白质合成过程中存在 20 种标准氨基酸, 每种氨基酸均具有独特的相对分子质量, 这些均为每轮加密的固定参数。

可变参数部分包括: 每种氨基酸的密钥长度 (KL)、3 个随机生成的旋转角度, 以及其他与加密过程控制相关的参数。其中, 氨基酸序列 (SEQ) 参数表示氨基酸序列, L 用于控制 SEQ 的长度; S 参数描述 E-Mat 的尺寸。KL 的取值范围为 1-256, 每种氨基酸的旋转角度为 1-360 度; 肽链的长度可从 3 开始取值, 为尽可能包含多种氨基酸, 该参数应设置为 20 以上。

2.2 肽链生成和转化

RC 是包含 AA 坐标信息的序列, 在加密过程中起着至关重要的作用。初始 RC 基于 SEQ 和 AA 的相关信息生成; 生成后, RC 将通过特定方式进行变换, 模拟蛋白质的旋转与折叠过程, 最终得到氨基酸序列相同但各 AA 坐标不同的新 RC。为计算每个 AA 的初始位置, 将 KL、旋转角度 θ_x 和 θ_y 作为球坐标系的参数。每个 AA 的位置通过前一个氨基酸的位移得到。

2.3 肽链结构投影与质量分配

加密的核心元素为 E-Mat, 每个图像块对应唯一的 E-Mat, 由 SP 和 MD 两个不可逆过程将 RC 的数据生成。

结构投影通过获取 RC 的三视图, 分别对应图像的三个颜色通道。各视图分别舍弃 x、y、z 轴信息, 得到 RC 中每个 AA 的三组二维坐标, 使三个 E-Mat 具有低相关性。质量分配中, E-Mat 尺寸 (S) 决定氨基酸的投影精度, 每个 E-Mat 为包含所有氨基酸的 S×S 矩阵。过程中涉及氨基酸坐标的计算、E-Mat 内点间距及氨基酸到矩阵点的垂直距离求解 (基于投影平面的平方和计算)。

2.4 分块加密

加密核心内容为将 E-Mat 的像素与对应图像块执行异或运算。当一个图像块的部分区域完成加密后, 会从下一段 RC 中选取 5 个氨基酸进行投影, 直至移动至

RC 末尾后, 经空间变换后生成的新 RC, 将用于处理下一个图像块。

E-Mat 以步长 S 在图像上水平移动, 每个图像块仅被处理一次; 当 E-Mat 到达图像边缘时, 将垂直偏移后重复水平移动, 直至整个图像加密完成。需注意, E-Mat 处于图像边缘时仅重叠部分生效, 因此 S 的最优设置为能被图像宽高整除的整数。

3 加密结果

我们提出的加密方法在二维图像取得了优异效果, 加密后图像具有高随机性, 且块间相关性低。测试选用了 4 幅常用数据集图像及 4 幅 8K 分辨率二维图像。加密结果如图 2 所示:



图 2 加密结果展示

其中, EIA 为前缀的是 8k 分辨率测试图像, 其余四张为公开图像测试数据集 USC-SIPI 的 4 张图像。

解密过程与加密过程类似: 以 SEQ 和 AA 相关信息作为密钥, 生成与加密阶段相同的 RC; 通过 SP 和 MD 算法得到解密所需的 E-Mat, 对加密图像执行抑或即可完成解密; 若涉及多轮加密, 经 ST 生成新的 RC 和 E-Mat 后, 重复上述逆运算流程即可。

4 安全性分析

4.1 密钥空间分析

在实际应用中, 需选择足够大的密钥空间以增加密钥破解难度, 保障加密安全性。本文所提方法的密钥可变参数如下:

- AA 的旋转角度, 取值范围为 1.00-360.00。
- 20 种 KL, 取值范围为 1.0-256.0。
- SEQ 的排列顺序, 由序列长度 L 决定, 经计算,

密钥空间大小为:

- 当 $L > 20$ 时, 密钥空间为 $36000^{60} \times 2560^{20} \times 20^L$
- 当 $L \leq 20$ 时, 密钥空间为 $36000^{60} \times 2560^{20} \times L^L$

通过调整参数 L, 密钥空间可轻松超过 2^{10000} , 在图像加密领域已经足够安全。可根据加密内容的安全需求

灵活调整 L 的取值。

4.2 加密密钥敏感度

密钥初始值敏感性用于衡量单个参数发生变化时，加密图像的差异程度。在本文所提方法中，通过改变单个氨基酸 (AA) 的密钥长度 (KL) 或旋转角度，生成的密文图像应与原始密文图像产生显著差异。实验设置 $L=20$ 、 $S=30$ ，加密过程中密钥长度 (KL) 取值范围为 1.0-256.0，旋转角度取值范围为 1.00-360.00°，实验结果如表 1 所示：

表 1 加密密钥敏感度测试结果

USC-SIPI	4.2.03	4.2.05	4.2.07	house
PSNR(Angle)	7.7410	7.7522	7.7480	7.7480
SSIM(Angle)	0.0035	0.0070	0.0049	0.0065
PSNR(KL)	7.7506	7.7488	7.7549	7.7493
SSIM(KL)	0.0051	0.0059	0.0067	0.0066

其中，氨基酸旋转角以 0.01 为单位变动，键长以 0.1 为单位变动。实验结果表明，本文方法对这两个参数具有高敏感性。

4.3 信息熵分析

信息熵 (E) 用于表征图像信息的复杂程度，其计算公式如下：

$$E = \sum_{i=0}^{2^N-1} P(i) \log_2 P(i) \quad (1)$$

其中， $P(i)$ 表示每个灰度级出现的概率， N 表示图像单个通道的色深。

信息熵的物理意义是表示图像信息所需的最小比特长度，在加密领域，加密后图像的信息熵越接近 8，说明加密效果越好。

信息熵计算结果如表 3 所示：

表 3 信息熵计算结果

USC-SIPI	4.2.03	4.2.05	4.2.07	house
加密前熵	7.7624	6.6639	7.6698	7.4858
加密后熵	7.9997	7.9998	7.9997	7.9998

实验结果表明，图像经过我们加密算法后的熵值均达到理想水平，说明加密算法能有效破坏原始图像的空间信息。

4.4 速度分析

速度实验在搭载 AMD 5800X CPU (128GB 内存) 和 NVIDIA RTX 3080 显卡的计算机上进行，软件开发

环境为 Visual Studio2022。测试结果如表 4，表 5 所示：

表 4 不同分辨率图像加密速度测试

分辨率	蛋白质加密 (GPU)	蛋白质加密 (CPU)	混沌加密
8k	0.0642	1.4982	214.1627
512x512	0.0024	0.0652	1.8164
1952x1952	0.0050	0.2010	30.1321
1600x1600	0.0040	0.1360	18.2656
3500x3500	0.0070	0.6250	138.8281

测试使用长度为 20 的肽链，加密矩阵尺寸为 100，混沌算法加密时间由同一台电脑进行算法复原后计算得到。

表 5 不同算法速度对比测试

分辨率	方法	时间
512x512	蛋白质加密(GPU)	0.0024
	蛋白质加密(CPU)	0.0652
	2D 超混沌多通道协同加密算法	0.8569
	DNA 加密	0.5463

测试使用长度为 20 的肽链，加密矩阵尺寸为 100，其他算法的实验数据直接来源于论文。

实验结果显示，本文所提方法在 GPU 上的加密速度较 CPU 版本提升约 20 倍，这得益于 ST、SP 和 MD 等模块的并行计算设计。与其他算法的对比表明，本文算法的加密速度比其他算法快 300 倍；即便仅使用 CPU 计算，本文算法的速度也比其他算法快 10 倍。这证明该算法的高速性不仅得益于 GPU 加速，更源于通过蛋白质结构投影生成加密矩阵的过程本身具有极高的效率。

5 总结与展望

本文提出的加密方法具有高安全性、高速性和强鲁棒性，能够在短时间内对大尺寸图像进行高速加密，并有效降低图像的相关性；经验证，该方法具备超大密钥空间和高密钥敏感性，能有效破坏原始图像的统计特征；加密速度分析表明，该算法效率极高：无论是基于 GPU 的并行计算，还是仅使用 CPU 运行，其速度均远超传统加密算法。

参考文献

[1] 郭洋, 孙静宇. 一种基于混沌系统的双量子图像加密算法[J/OL]. 计算机工程, 1-13[2025-12-09]. <https://doi.org/10.19678/j.issn.1000-3428.0252605>.

- [2] 祁琼,段志强,吕婧,等.一种基于混沌系统的国土调查数据加密算法[J].地理空间信息,2025,23(10):15-19.
- [3] 尤洁,赵泽宇,郑鑫.面向光互连网络的片上集成光学图像加密技术综述[J].智能安全,2025,4(02):87-99.
- [4] 任冰.基于计算光学的视觉密码加密技术[D].河北工程大学,2025.DOI:10.27104/d.cnki.ghbjy.2025.000507.
- [5] [范素娟,董孝伟,左宪禹,等.基于混沌系统和动态DNA编解码规则的图像加密方法[J].河南大学学报(自然科学版),2025,55(05):580-589.DOI:10.15991/j.cnki.411100.2025.05.004.
- [6] Xuncai Zhang, Guanhe Liu, Chengye Zou. An image encryption method based on improved Lorenz chaotic system and Galois field [J]. Applied Mathematical Modelling, 2024: 535-558. DOI: 10.1016/j.apm.2024.04.023
- [7] Feyza Toktas, Uğur Erkan, Zeki Yetgin. Cross-channel color image encryption through 2D hyperchaotic hybrid map of optimization test functions [J]. Expert Systems with Applications, 2024: 123583. DOI: 10.1016/j.eswa.2024.123583
- [8] Chong, Zhenglong, Wang, Cong, Zhang, 等. Image Encryption Algorithm Based on a Hybrid Model of Novel Memristive Hyperchaotic Systems, DNA Coding, and Hash Functions [J]. Complex System Modeling and Simulation, 2024: 303-319. DOI: 10.23919/CSMS.2024.0015