互易域上的仿生密码系统：DNA 链变异以保护健康数据

S. AASHIQ BANU, Rengarajan AMIRTHARAJAN
山姆哈人文与科学技术研究院电气与电子工程学院，印度坦贾武尔，613401

摘要：医疗保健和远程医疗行业依赖于互联网技术，数字健康数据更易受到网络攻击，因其中包含大量个人数据，因而，有必要保护数字医疗图像以及保证其安全传输。本文采用基于洛伦兹和吕混沌吸引子突变的 DNA 加密技术生成强伪随机密钥流。为增强混淆与扩散阶段的近似性系数，所提的混沌 DNA 加密系统在整数小波变换域和一个生物启发的交叉变异单元上运行。进而，使用组合演化吸引子中的量化混沌集进行异或运算。该算法可以获得平均信息熵 7.9973，几乎接近于零相关性的像素变化率（number of pixel change rate, NPCR）99.642%，归一平均强度变化（unified average change in intensity, UACI）33.438%，以及密钥空间 10^{203}。此外，实验分析和基于美国国家标准与技术研究院（NIST）的统计测试套件测试证实，所提医疗图像加密技术具有抵御任何统计、差分和暴力攻击的能力。

关键词：医学图像加密；DNA；混沌吸引子；交叉；突变；电子医疗
https://doi.org/10.1631/FITEE.2000071