TPE-H2MWD：基于隐马尔科夫模型和分权扩散的精确缩略图保留加密方案

柴秀丽[1,2]，陈绣辉[1]，马亚坤[1]，左方[3]，甘志华[2,3]，张玉书[4]

[1]河南大学人工智能学院，河南省工业互联网工程技术研究中心，中国郑州市，450046

[2]河南省网络空间态势感知重点实验室，中国郑州市，450001

[3]河南大学软件学院，河南省智能数据处理工程研究中心，智能网络系统研究所，中国开封市，475004

[4]南京航空航天大学计算机科学与技术学院，中国南京市，211106

摘要：随着图像传输技术日益发展，人们对图像安全的需求也在大幅提升。由传统图像加密方案获得的类噪声图像虽然可以保证内容安全，但无法直接用于预览和检索。一些学者基于排序后加密方法，设计了一种三像素缩略图保留加密方案（TPE2），用于平衡图像安全性和可用性，然而该方案的加密效率较低。为此，本文提出一种有效的精确缩略图保留加密方案。首先对明文图像进行分块和位平面置乱，然后采用Z字形置乱模型改变最低的4个位平面中比特的位置，随后介绍了用于改变最高的4个位平面中比特位置的操作（这是隐马尔科夫模型的一个扩展应用）。最后，根据每个位平面中比特的权重不同，设计了一种比特级分权扩散规则。至此生成的加密图像能保证块内像素和不变。仿真结果表明，该方案在平衡图像隐私性和可用性的同时，提高了加密效率。

关键词：隐马尔科夫模型；分权扩散；可用性与隐私性之间的平衡；图像加密

https://doi.org/10.1631/FITEE.2200498