基于 RSA 和 Arnold 变换的非对称图像混淆算法

黄小玲，董友霞，焦开心，叶国栋
广东海洋大学数学与计算机学院，中国湛江市，524088

摘要：提出一种新的基于Rivest-Shamir-Adleman（RSA）公钥密码系统和Arnold映射的非对称像素混淆算法。首先，为解决Arnold映射参数对称分布问题，采用RSA非对称算法生成两组Arnold映射变换参数。其次，将图像分成图像块，并利用第一组参数对各图像块进行Arnold混淆。然后，使用第二组参数对整个图像进行Arnold混淆。从而，充分削弱图像相关性，进一步提高图像混淆程度和效果。试验结果表明，相比于基于经典Arnold映射混淆和基于行列交换混淆，本文所提图像像素混淆算法具有更好混淆效果。具体来说，灰度差的值均接近于0。另外，新的混淆操作安全性依赖于RSA，可作为密码学中混淆—替换结构的一部分。

关键词：Rivest-Shamir-Adleman（RSA）；Arnold映射；像素混淆；非对称算法；图像混淆
https://doi.org/10.1631/FITEE.2000241