基于公钥具有双向影子图像验证功能且无像素扩张的图像秘密分享

Xuehu Yan, Longlong Li, Jia Chen, Lei Sun
National University of Defense Technology, Hefei 230037, China

摘要：图像秘密分享（ISS）的研究越来越多，主要因为数字图像的重要性以及ISS可以广泛应用于云分布式存储和多方安全计算。影子图像认证日渐重要，通常包括影子图像真实性检测和识别。然而，传统处理者参与的方法主要是单向验证，即在解码阶段验证影子图像，存在像素扩张或额外辅助信息等不足。因此，分发（编码）阶段的影子图像认证对参与者来说也很重要。本文引入一种基于公钥的双向影子图像认证方法，实现(k, n)门限且无像素扩张。当处理者将每个影子图像分发给相应参与者时，参与者可以用其私钥验证接收到的影子图像。在解码阶段，处理者可以用其秘钥验证每个接收到的影子图像；此外，当获得任何k个或更多影子图像时，处理者可以无损解码秘密图像。理论分析、实验和比较验证了所提方法有效性。

关键词：图像秘密分享；影子图像验证；公钥；像素扩张；无损恢复
https://doi.org/10.1631/FITEE.2200118