

前言

特邀编辑：赵险峰¹，倪江群²，李晓龙³，李斌⁴，任延珍⁵

¹中国科学院信息工程研究所 北京 中国 100093

²中山大学数据科学与计算机学院 广州 中国 510275

³北京交通大学计算机与信息技术学院 北京 中国 100044

⁴深圳大学信息工程学院 深圳 中国 518060

⁵武汉大学国家网络安全学院 武汉 中国 430072

随着多媒体技术的发展与应用的普及，出现了一系列与多媒体相关的信息安全研究问题。

首先，多媒体内容信息冗余较多，这为现代信息隐藏技术的发展与应用提供了空间。隐写 (Steganography) 技术将机密隐藏在可公开的多媒体中，能够掩盖保密通信或存储的事实，而隐写分析 (Steganalysis) 泛指检测与攻击隐写的方法。数字水印 (Watermarking) 技术将安全标识隐藏在被保护的内容中，其中，鲁棒 (Robust) 水印技术是重要的数字权限管理手段，它将包含内容版权或使用者相关信息的水印嵌入内容中，并使攻击者难以在内容不遭到显著破坏的情况下妨碍水印检测；脆弱 (Fragile) 水印技术将用于防伪的水印隐藏在内容中，以后不但可以通过水印检测发现篡改，还可以发现篡改位置，应用方式比数字签名也相对简单。

第二，随着多媒体编辑与处理工具的普及，多媒体内容的真伪越来越难以判断，这促进了多媒体取证 (Forensics) 技术的发展。目前出现的伪造方法大致分为同一多媒体中内容的复制与移动、不同多媒体之间的内容拼接、各类形变与处理等，伪造后的内容往往有欺骗性或诱导性的效果，这给司法取证与公共安全造成了很大问题。当前，多媒体取证技术主要通过提取与检测有关自然内容约束的特征识别与定位篡改，其中，自然内容约束包括光源一致性、透视效果、噪声类型等方面。

第三，除了以上两类技术，基于多媒体内容及其应用特点也出现了其他一些独特的内容安全防护技术。密码技术中的杂凑 (Hash Value) 用于标识更大尺寸的数据，而内容杂凑 (Content Hash) 或感知杂凑 (Perceptual Hash) 用于标识或检测内容；多媒

体选择 (Selective) 加密通过选择部分内容成分加密获得了快速、轻量级的加密效果；结合前述技术，也出现了大量有关数字权限管理、组播加密、多媒体安全管理与服务等方面的方案与协议。

如上所述，近 20 年来，多媒体信息安全的研究与应用取得了丰硕成果，但仍存在众多难点与新的问题。当前，隐写应用环境有向社交网络有损信道迁移的趋势；在深度学习逐渐有效支撑隐写分析的同时，基于人工智能的隐写也开始被提出；水印的鲁棒性仍有待于在新思路下得到提高；面对多媒体取证的实际场景，如何对多种篡改进行可靠取证成为研究的难点；随着应用方式的多样化，特别是在大数据与云服务环境下，在多媒体版权、内容与隐私保护方面仍存在大量的新安全需求需要应对。

本专刊刊载的 9 篇论文综述了多媒体信息安全方面的重要研究工作，展示了我国科研人员的部分新成果。其中，翟黎明等人综述了深度学习在图像隐写与隐写分析中的进展，张弘等人综述了视频隐写分析的研究，朱新山与杨璐综述了视频水印方面的研究；在信息隐藏方面，管萌萌等人针对利用社交网络有损信道提出了视频鲁棒隐写算法，郑梦阳等人提出了基于 JPEG 比特流加密域的大容量可逆数据隐藏算法，彭飞等人提出了针对保护工程图的鲁棒水印，项世军等人提出了量子图像下的差分扩展可逆数据隐藏算法；在多媒体取证方面，吴学谦等人提出了针对图像内容 Seam-carving 处理的检测方法；最后，易小伟等人提出了基于跨层优化资源分配的抗丢包图像流认证方案。

希望本专刊能够为推进多媒体信息安全的研究与应用尽绵薄之力！