二· 項目簡介

（*項目所屬科學技術領域、主要研究內容、發現點、科學價值、同行引用及評價等內容。*）

本項目隸屬信息隱藏、圖像處理科學領域。隨著社交網絡推動信息化傳播的快速發展，海量多媒體信息通過互聯網分享在不同的社交平台上。這些信息在豐富人們生活的同時，也爲社會帶來了許多信息安全隱患，如虛假新聞、隱私泄露、非法竊取、惡意篡改等，爲個人、企業乃至國家造成了極其嚴重的名譽損失和經濟損失。目前，針對社交網絡多媒體安全的探索仍然處于初期階段，相關取證技術在成果轉化和產業落地方面仍然面臨如下研發瓶頸：受信道幹擾性強、魯棒泛化性差以及安全可信性低。本項目針對上述難點展開了面向社交網絡的多媒體安全和取證關鍵技術研究，包括建立有效的社交網絡信道分析機制和研發高魯棒的社交多媒體取證技術、設計系統的多媒體信息安全分析和處理框架、提出具有數據隱私保護的魯棒特征學習和模型推理算法等，爲信息隱藏、圖像處理科學提供了系統性的理論依據。本項目取得的主要創新性成果爲：

1) 率先建立了社交網絡傳輸的信道模型，提出了高魯棒多媒體信息隱私保護與取證框架。由于社交媒體（如 Facebook、微信等）傳輸過程伴有較強的壓縮、裁剪和自適應增強等操作，導致現有多媒體信息保護與取證技術性能大幅降低，甚至完全失效。本成果針對這一瓶頸問題，率先對社交網絡信道噪聲設計了有效的分析及解耦機制，構建了具有高概括性、高契合性的社交網絡信道噪聲模型，成功地指導了具有高魯棒性的多媒體信息隱私保護與取證核心技術研究。

2) 提出了完善的多媒體信息安全分析和處理系統。分析多媒體處理系統安全邊界、建立有效的多媒體信息處理系統安全機制是保障用戶隱私的基礎。該成果從僞造攻擊、內容泄露方面建立系統的多媒體特征安全分析框架，揭示了現有多媒體處理算法在實際應用，特別是在敏感場景中存在的極大安全隱患。進一步以系統安全分析爲基礎、信息安全保護爲核心，設計了涵蓋多領域的高安全性、高魯棒性多媒體信息處理系統。

3) 提出了具有隱私保護的多媒體特征學習和模型推理算法。基于多媒體信息的人工智能模型在特征學習和模型推理階段涉及到多個層面的隱私泄露問題。該成果提出了具有隱私保護特性的多媒體特征學習算法和模型推理算法，涵蓋了傳統端到端應用和多方參與的聯邦學習中的多媒體隱私保護問題，在多媒體數據的隱私性和多媒體數據的可學習性之間建立了橋梁，爲人工智能應用及區塊鏈技術的安全可信落地提供了理論與技術支撐。

本成果 24 篇代表性論文 SCIE 他引 279 次，總他引 467 次，多篇發表于相關領域頂級期刊 IEEE Trans. Inf. Forensic Secur.、IEEE Trans. Image Process.及頂級會議 IEEE Conf. Comput. Vis. Pattern Recog.、AAAI Conf. Artif. Intell.等；代表性文獻[1]入選 2018 年高被引論文；代表性文獻[3]于 2020 年在清華大學和阿裏巴巴公司合辦的全球首個"僞造圖像篡改檢測競賽"中獲得冠軍，並獲阿裏巴巴贊助及邀請參與其創新計劃項目；本項目成果于 2021 年 5 月 25 日被澳門廣播電視台《澳視新聞》采訪並進行約三分鍾的電視報導，亦被網易新聞、騰訊網等多家媒體宣傳報導。項目主要負責人周建濤教授自 2018 年 11 月開始擔任多媒體和圖像處理領域頂級期刊 IEEE Trans. Image Processing（IF=10.856）和 IEEE Tran. Multimedia （IF=6.513）的編委 (Associate Editor)；在相關領域的研究成果受到國際同行的高度認可，榮獲 2016 年度和 2020 年度 IEEE ICME 最佳論文獎；並于 2019 年入選亞太信號與信息處理協會

(APSIPA) 傑出講師。

（*字數不超過 1200 字*）