



JOURNAL OF IMAGE AND GRAPHICS

主办: 中国科学院空天信息创新研究院
中国图象图形学学会
北京应用物理与计算数学研究所

中国图象图形学报

2022
06
VOL.27

ISSN1006-8961
CN11-3758/TB

2021

图像图形学 发展 年度报告



第27卷第6期（总第314期）
2022年6月16日

中国精品科技期刊
中国国际影响力优秀学术期刊
中国科技核心期刊
中文核心期刊

版权声明

凡向《中国图象图形学报》投稿，均视为同意在本刊网站及CNKI等全文数据库出版，所刊载论文已获得著作权人的授权。本刊所有图片均为非商业目的使用，所有内容，未经许可，不得转载或以其他方式使用。

Copyright

All rights reserved by Journal of Image and Graphics, Institute of Remote Sensing and Digital Earth, CAS. The content (including but not limited text, photo, etc) published in this journal is for non-commercial use.

主管单位 中国科学院
主办单位 中国科学院空天信息创新研究院
中国图象图形学学会
北京应用物理与计算数学研究所

主 编 吴一戎
编辑出版 《中国图象图形学报》编辑出版委员会
通信地址 北京市海淀区北四环西路19号
邮 编 100190
电子信箱 jig@aircas.ac.cn
电 话 010-58887035
网 址 www.cjig.cn

广告发布登记号 京朝工商广登字20170218号
总 发 行 北京报刊发行局
订 购 全国各地邮局
海外发行 中国国际图书贸易集团有限公司
(邮政信箱: 北京399信箱 邮编: 100048)
印刷装订 北京科信印刷有限公司

Journal of Image and Graphics

Title inscription: Song Jian | Monthly, Started in 1996

Superintended by Chinese Academy of Sciences
Sponsored by Aerospace Information Research Institute, CAS
China Society of Image and Graphics
Institute of Applied Physics and Computational Mathematics

Editor-in-Chief Wu Yirong
Editor, Publisher Editorial and Publishing Board of Journal of Image and Graphics
Address No. 19, North 4th Ring Road West, Haidian District, Beijing, P. R. China
Zip code 100190
E-mail jig@aircas.ac.cn
Telephone 010-58887035
Website www.cjig.cn

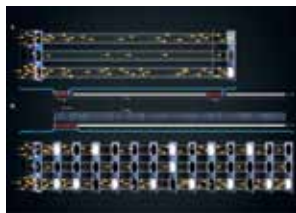
Distributed by Beijing Bureau for Distribution of Newspapers and Journals
Domestic All Local Post Offices in China
Overseas China International Book Trading Corporation
(P.O.Box 399, Beijing 100048, P.R.China)
Printed by Beijing Kexin Printing Co., Ltd.

CN 11-3758/TB
ISSN 1006-8961
CODEN ZTTXFZ

国外发行代号 M1406
国内邮发代号 82-831
国内定价 60.00元



面向智慧交通的图像处理与
边缘计算(第1743页)



脉冲视觉研究进展(第1823
页)



移动在线实时绘制技术研究
综述(第1877页)

序言王耀南 I

视觉理解与计算成像

基于深度学习的视觉目标检测技术综述

曹家乐, 李亚利, 孙汉卿, 谢今, 黄凯奇, 庞彦伟 1697

面向复杂场景的人物视觉理解技术

马利庄, 吴飞, 毛启容, 王鹏杰, 陈玉珑 1723

面向智慧交通的图像处理与边缘计算

曹行健, 张志涛, 孙彦赞, 王平, 徐树公, 刘富强, 王超, 彭飞, 穆世义, 刘文予, 杨铀 ... 1743

视觉弱监督学习研究进展

任冬伟, 王旗龙, 魏云超, 孟德宇, 左旺孟 1768

智能遥感: AI赋能遥感技术

孙显, 孟瑜, 刁文辉, 黄丽佳, 张新, 骆剑承, 高连如, 王佩瑾, 闫志远, 郜丽静, 董文, 冯瑛
超, 李霁豪, 付琨 1799

脉冲视觉研究进展

黄铁军, 余肇飞, 李源, 施柏鑫, 熊瑞勤, 马雷, 王威 1823

计算成像前沿进展

顿雄, 付强, 李浩天, 孙天成, 王建, 孙启霖 1840

移动在线实时绘制技术研究综述

刘畅, 霍宇驰, 张严辞, 张乾, 郑家祥, 唐睿, 余耿, 王锐, 贾金原 1877

数据挖掘和信息交互

表格识别技术研究进展

高良才, 李一博, 都林, 张新鹏, 朱子仪, 卢宁, 金连文, 黄永帅, 汤帆 1898

多媒体隐写研究进展

张卫明, 王宏霞, 李斌, 任延珍, 杨忠良, 陈可江, 李伟祥, 张新鹏, 俞能海 1918

大脑多模态成像技术定量研究进展

叶慧慧, 何宏建, 方静苑, 童琪琦, 周子涵, 刘华锋 1944

多模态人机交互综述

陶建华, 巫英才, 喻纯, 翁冬冬, 李冠君, 韩腾, 王运涛, 刘斌 1956

文化遗产活化关键技术研究进展

耿国华, 何雪磊, 王美丽, 李康, 贺小伟 1988

情感计算与理解研究发展概述

姚鸿勋, 邓伟洪, 刘洪海, 洪晓鹏, 王甦菁, 杨巨峰, 赵思成 2008

跨模态脑图谱数据融合研究进展

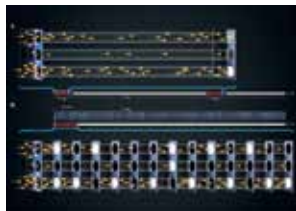
罗娜, 宋明, 杨正宜, 蒋田仔 2036

CONTENTS

JOURNAL OF IMAGE AND GRAPHICS



The review of image processing and edge computing for intelligent transportation system(P1743)



Advances in spike vision(P1823)



A review of real-time rendering technology based on mobile internet platforms(P1877)

Visual Understanding & Computational Imaging

A survey on deep learning based visual object detection

Cao Jiale, Li Yali, Sun Hanqing, Xie Jin, Huang Kaiqi, Pang Yanwei 1697

Visual recognition technologies for complex scenarios analysis

Ma Lizhuang, Wu Fei, Mao Qirong, Wang Pengjie, Chen Yulong 1723

The review of image processing and edge computing for intelligent transportation system

Cao Xingjian, Zhang Zhitao, Sun Yanzan, Wang Ping, Xu Shugong, Liu Fuqiang, Wang Chao, Peng Fei, Mu Shiyi, Liu Wenyu, Yang You 1743

Progress in weakly supervised learning for visual understanding

Ren Dongwei, Wang Qilong, Wei Yunchao, Meng Deyu, Zuo Wangmeng 1768

The review of AI-based intelligent remote sensing capabilities

Sun Xian, Meng Yu, Diao Wenhui, Huang Lijia, Zhang Xin, Luo Jiancheng, Gao Lianru, Wang Peijin, Yan Zhiyuan, Gao Lijing, Dong Wen, Feng Yingchao, Li Jihao, Fu Kun 1799

Advances in spike vision

Huang Tiejun, Yu Zhaofei, Li Yuan, Shi Boxin, Xiong Ruiqin, Ma Lei, Wang Wei 1823

Recent progress in computational imaging

Dun Xiong, Fu Qiang, Li Haotian, Sun Tiancheng, Wang Jian, Sun Qilin 1840

A review of real-time rendering technology based on mobile internet platforms

Liu Chang, Huo Yuchi, Zhang Yanchi, Zhang Qian, Zheng Jiaxiang, Tang Rui, Yu Geng, Wang Rui, Jia Jinyuan 1877

Data Mining and Information Interaction

A survey on table recognition technology

Gao Liangcai, Li Yibo, Du Lin, Zhang Xinpeng, Zhu Ziyi, Lu Ning, Jin Lianwen, Huang Yongshuai, Tang Zhi 1898

Overview of steganography on multimedia

Zhang Weiming, Wang Hongxia, Li Bin, Ren Yanzhen, Yang Zhongliang, Chen Kejiang, Li Weixiang, Zhang Xinpeng, Yu Nenghai 1918

Research progress of quantitative multimodal brain imaging technology

Ye Huihui, He Hongjian, Fang Jingwan, Tong Qiqi, Zhou Zihan, Liu Huafeng 1944

A survey on multi-modal human-computer interaction

Tao Jianhua, Wu Yingcai, Yu Chun, Weng Dongdong, Li Guanjuan, Han Teng, Wang Yuntao, Liu Bin 1956

Research progress on key technologies of cultural heritage activation

Geng Guohua, He Xuelei, Wang Meili, Li Kang, He Xiaowei 1988

An overview of research development of affective computing and understanding

Yao Hongxun, Deng Weihong, Liu Honghai, Hong Xiaopeng, Wang Sujing, Yang Jufeng, Zhao Sicheng 2008

Survey on cross-modal fusion based on brain atlas data

Luo Na, Song Ming, Yang Zhengyi, Jiang Tianzi 2036

中图法分类号: TP391.4 文献标识码: A 文章编号: 1006-8961(2022)06-1918-26

论文引用格式: Zhang W M, Wang H X, Li B, Ren Y Z, Yang Z L, Chen K J, Li W X, Zhang X P and Yu N H. 2022. Overview of steganography on multimedia. Journal of Image and Graphics, 27(06): 1918-1943 (张卫明, 王宏霞, 李斌, 任延珍, 杨忠良, 陈可江, 李伟祥, 张新鹏, 俞能海. 2022. 多媒体隐写研究进展. 中国图象图形学报, 27(06): 1918-1943) [DOI: 10.11834/jig.211272]

多媒体隐写研究进展

张卫明¹, 王宏霞², 李斌³, 任延珍⁴, 杨忠良⁵, 陈可江¹,
李伟祥³, 张新鹏^{6*}, 俞能海¹

1. 中国科学技术大学网络空间安全学院, 合肥 230027; 2. 四川大学网络空间安全学院, 成都 610207;
3. 深圳大学广东省智能信息处理重点实验室及深圳市媒体信息内容安全重点实验室, 深圳 518060;
4. 武汉大学国家网络安全学院, 武汉 430072; 5. 清华大学电子工程系, 北京 100084;
6. 复旦大学计算机科学技术学院, 上海 200438

摘要: 大数据分析可以跳过数据内容而仅从数据背景挖掘情报, 传统的加密通信已经难以满足安全通信的需求。隐写技术是将秘密消息嵌入各种载体(如数字图像、音频、视频或文本)中实现隐蔽通信的技术, 是应对大数据情报获取的有效手段, 是密码技术的必要补充。人工智能, 尤其是深度学习, 在计算机视觉、语音和自然语言处理等领域的巨大成功, 给隐写术带来了新机遇, 提出了新挑战, 促使基于图像、音/视频和文本的隐写术出现了一系列新思想、新方法。本文介绍隐写术的概念、分类、主要作用和研究意义, 概述隐写术的发展历史、研究近况和应用场景。注意到各类载体上的隐写术虽然有差别, 但是其核心追求有共通之处, 可以提炼成通用的隐写编码问题。所以本文首先介绍隐写编码的基本思想与关键技术, 然后针对最重要和流行的载体、图像、视频、音频和文本, 分别介绍隐写术的进展。总体而言, 本文从隐写编码、图像隐写、视频隐写、音频隐写和文本隐写5个方面概述隐写术的国际/国内发展现状, 总结差异, 对比优势和劣势, 并分析发展趋势。

关键词: 隐写编码; 文本隐写; 图像隐写; 音频隐写; 视频隐写

Overview of steganography on multimedia

Zhang Weiming¹, Wang Hongxia², Li Bin³, Ren Yanzhen⁴, Yang Zhongliang⁵, Chen Kejiang¹,
Li Weixiang³, Zhang Xinpeng^{6*}, Yu Nenghai¹

1. School of Cyber Science and Technology, University of Science and Technology of China, Hefei 230027, China;
2. School of Cyber Science and Engineering, Sichuan University, Chengdu 610207, China;
3. Guangdong Key Laboratory of Intelligent Information Processing and Shenzhen Key Laboratory of Media Security, Shenzhen University, Shenzhen 518060, China; 4. School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China;
5. Department of Electronic Engineering, Tsinghua University, Beijing 100084, China;
6. School of Computer Science, Fudan University, Shanghai 200438, China

Abstract: Big data analysis can skip the data content and mine intelligence from the data context, therefore encryption cannot

收稿日期: 2021-12-31; 修回日期: 2022-03-23; 预印本日期: 2022-03-30

* 通信作者: 张新鹏 zhangxinpeng@fudan.edu.cn

基金项目: 国家自然科学基金项目(62102386, U1936214, 61972269, 61872275, U1936216); 深圳市基础研究项目(JCYJ20200109105008228); 广东省自然科学基金项目(2019B151502001)

Supported by: National Natural Science Foundation of China (62102386, U1936214, 61972269, 61872275, U1936216); Shenzhen Fundamental Research Funds(JCYJ20200109105008228); Natural Science Foundation of Guangdong Province, China (2019B151502001)

meet the requirement for secure communication. Steganography is a technique to embed secret messages in various covers (such as digital images, audio, video or text) to achieve covert communication, which is an effective method to cope with big data intelligence acquisition and a necessary complement to cryptography. The advances of artificial intelligence, especially deep learning, in computer vision, speech and natural language processing in recent years have brought new opportunities and challenges to steganography, prompting a series of new ideas and methods in image, audio and video, and text steganography. This paper will introduce the concept, classification, main role and research significance of steganography, and outline the development history, research status and application scenarios of steganography. It is noted that although there are differences in steganography on various covers, their core pursuits have commonalities, which can be refined into general steganographic coding problems. Therefore, this paper will first introduce the basic ideas and key technologies of steganography, and then introduce the progress of steganography for the most important and popular covers, including image, video, audio and text. According to the development of steganographic coding, it can be divided into coding problems under five cost models: constant cost, two-level cost, multi-level cost, non-binary cost, non-additive cost. The coding efficiency and security have been greatly improved. With the effective steganographic coding methods, the focus of research turns to how to define the distortion introduced by embedding message. As for image steganography, this paper reviews model-based steganography, natural steganography, side-information steganography, adversarial steganography. The confrontation between steganography and steganalysis is getting fierce. The distribution of cover image is better preserved. Video is composed of multiple images, so image steganography can be directly used in the spatial domain of video. However, the video will always be compressed to save storage space and the steganography on the compression domain of video is more practical. Many motion-vector based video steganographic schemes have been proposed, which also benefit from the development of steganographic coding. Deep learning based video steganography is a more straight way for embedding messages, which can be also robust to loss video processing, such as recompression, cropping, Gaussian filtering. There are also quite a number of video steganographic tools on the internet, e. g., OpenPuff. Audio can be seen as a part of video, and audio steganography can be divided into time domain and compression domain as well. The audio steganography has its own character, like echo hiding. Since the audio synthesis is very powerful and popular used, some generative audio steganography methods have also been proposed and show superior performance. Previous mentioned mediums will be easily lossy processed, while text seems to be more robust. Text steganography can be divided into format-based steganography and content-based steganography. Content-based steganography is more popular, where generative linguistic steganography shows strong vitality. The international and domestic development status of steganography from five aspects are separately summarized. The advantages and disadvantages of international and domestic development are compared. With these comparisons and corresponding analysis, we also give the development trend from five aspects: steganographic coding, image steganography, video steganography, audio steganography, and text steganography. Better error correction codes are promisingly transferred to better steganographic codes. Robust image steganography is an urgent need, because lossy operations are adopted on online social networks. Fast video steganography is also a potential direction since livestreaming and short-video are current hot spots. Latent codes edition is a direction of improving the performance of generative steganography. In a nutshell, this paper reviews steganography on multimedia and gives future directions of different aspects.

Key words: steganographic codes; text steganography; image steganography; audio steganography; video steganography

0 引言

大数据分析可以跳过数据内容而仅从数据背景挖掘情报。当通信行为被发现时,使用密文通信的人就显得很突出,从而成为被监控和分析的重点对象。因此现代通信安全不仅要求内容保密,而且希望过程隐蔽。因此只加密数据内容难以保障通信

安全。

隐写技术是将秘密消息嵌入各种载体(如数字图像、音频、视频或文本)中实现隐蔽通信的技术(王朔中等,2005),是应对大数据情报获取的有效手段,是加密技术的必要补充。随着一带一路的推动和经贸全球化的发展,保障我国企业、机构海外权益的需求迅速增加,对非受控环境下的安全通信提出了更高的要求,通信不仅要保密而且要隐蔽。所

以,隐写术对于保障国家特殊部门和关键人群的通信安全具有不可或缺的作用。另一方面,在APT(advanced persistent threat)攻击中,基于隐写术构建的隐信道成为重要一环;通过与恶意代码结合,隐写术也成为网络攻击的典型非对称技术。从攻防两方面看,网络空间的隐蔽通道都是各国争夺的战略资源。

隐写技术及其应用曾出现在许多古代东西方的文字记载中,最早可以追溯到Herodotus(公元前486年—公元前425年)所著的Histories,其中记载了Histiaeus将消息刺在奴隶的头皮上,待其头发长出后再送出去进行秘密通信(Jamil,1999)。近代也出现了很多隐写应用,比如隐形墨水和伪装物品等广泛应用于两次世界战争中的隐蔽通信。20世纪90年代以来,随着互联网和多媒体数据的逐渐普及,古老的隐写技术获得了新的发展。近年来,基于数字多媒体数据的隐写技术因其在个人隐私保护、情报与军事等安全领域不可替代的作用,正日益引起国内外学术界和相关部门的高度重视,并成为当前多媒体内容安全研究领域的热点之一。隐写技术的相关研究也受到政府和国际组织的资助,单项资助金额高达850万美元(<https://cordis.europa.eu/project/id/101021687/fr>)。

随着人工智能,尤其是深度学习在计算机视觉、语音和自然语言处理等领域的巨大成功,给隐写术带来了新机遇也提出了新挑战,促使图像、音/视频和文本隐写出现了一系列新思想、新方法。在此背景下,梳理国内外多媒体隐写的发展现状、前沿动态、热点问题和发展趋势,对于政府决策与立项、相关领域科技工作者了解研究进展都有重要意义。

本文主体部分按载体对隐写术分类介绍。注意到虽然各类载体上的隐写术有差别,但是其核心追求有共通之处,可以提炼成通用的隐写编码问题。所以本文首先介绍隐写编码,然后针对最重要和流行的载体重点介绍图像隐写、视频隐写、音频隐写和文本隐写的进展。

1 国际研究现状

1.1 隐写编码

为了对抗隐写分析的检测,隐写术需要在给定的载荷率下最小化因嵌入消息引入的载体失真。这

是隐写术设计理论中的核心问题,此问题可以抽象成一个特殊的率失真编码问题来解决,即隐写编码(steganographic codes)(Zhang和Li,2008)。根据隐写编码的发展历程,可将其分为5种代价模型下的编码问题:

1)常数代价编码模型。假设在不同元素上修改造成的影响都是相同的,最小化修改代价等同于最小化修改点数量。

2)两级代价编码模型。即将载体元素分为干、湿两类,“湿点”的位置禁止修改,“干点”的修改代价一致,接收方无需知道湿点位置就可以提取消息。

3)多级代价编码模型。两级代价模型对载体的刻画不够精细,更高级的模型是“多级代价模型”,即对不同的元素定义不同的修改代价。

4)非二元代价编码模型。基本的编码通常是针对二元修改设计的。 ± 1 修改相较于二元修改安全性更强,但 ± 1 修改本质上对应三元嵌入,而三元编码的计算复杂度很高。非二元代价编码模型研究如何通过二元隐写码实现高效的非二元嵌入。

5)非加性编码模型。加性代价模型假设修改载体各元素引入的代价是独立的,这是对真实情况的一种简化。考虑隐写修改之间的相互影响,最小化“非加性代价”是隐写术发展的更高级追求。

隐写编码的性能可由嵌入效率(embedding efficiency)来衡量,嵌入效率定义为信息长度与修改总代价之比,即引入单位代价可嵌入的信息量。嵌入效率越高,则编码性能越好。

1.1.1 常数代价隐写编码

常数代价模型认为所有元素具有相同的修改代价,故最小化修改代价等价于最小化元素修改数量。矩阵编码是该模型下隐写编码的设计范式(Crandall,1998),利用分组纠错编码的奇偶校验矩阵完成消息的嵌入和提取。最早的矩阵编码方案是根据Hamming码设计的,并形成了经典的F5隐写算法(Westfeld,2001)。在分析线性/非线性覆盖码与隐写编码之间的关系并推导矩阵编码的率失真界后,Galand和Kabatiansky(2003)、Bierbrauer和Fridrich(2008)分别提出了多个性能优异的矩阵编码方案。Munuera(2007)也讨论了隐写编码与纠错编码之间的关系,并基于BCH(Bose-Chaudhuri-Hocquenghem)码设计了性能更优的矩阵编码方案。进一步地,基于BCH码的方案可以从嵌入效率和计算复杂度两

个方面得到改善 (Schönfeld 和 Winkler, 2006)。Fridrich 和 Soukal (2006) 则考虑到随机线性码的价值, 并基于低密度生成矩阵 (Low-density generator matrix, LDGM) 码构造具有大嵌入容量和高嵌入效率的隐写编码 (Fridrich 和 Filler, 2007)。

1.1.2 两级代价隐写编码

两级代价模型也称为湿纸模型 (wet paper code), 即将载体元素分为干、湿两类, “湿点”的位置禁止修改, 而接收方无需知道湿点位置就可以提取消息。Fridrich 等人 (2005b) 首先给出了湿纸编码的高斯消元求解方法。为了降低该求解方法的计算复杂度, 他们进一步借助用于擦除信道的稀疏线性码加快了求解速度 (Fridrich 等, 2005a)。为了提高湿纸码的嵌入效率, Fridrich 等人 (2006) 提出了 Meet-in-the-Middle 方法。在真实场景中, 湿点个数不是一定的, 因此, 这些基于结构码的设计一般难以满足现实需求。Filler 和 Fridrich (2009) 提出了 “Wet ZZW (Zhang Zhang Wang)” 编码方案, 可以由大嵌入率湿纸码生成一族小嵌入率湿纸码。

1.1.3 多级代价隐写编码

湿纸代价对载体的刻画不够精细, 更高级的模型是“多级代价模型”。每个载体元素可以定义任意的修改代价。Kim 等人 (2007) 将 Hamming 矩阵编码改为每个分组允许多个修改来适应多级代价模型。Sachnev 等人 (2009) 将允许多个修改的思想扩展到基于 BCH 码的矩阵编码中。Filler 等人 (2011) 提出了基于卷积码的校验网格编码 (syndrome trellis codes, STC) 方法, 可以在多级代价模型下逼近嵌入效率上界。Diouf 等人 (2018) 提出了一种基于极化码 (polar codes) 设计的隐写码方案, 但在多级代价模型仍存在一定局限。为了增加隐写算法面对有损处理的鲁棒性, Kin-Cleaves 和 Ker (2018) 提出了 DualSTC 方法, 相比于原始 STC 编码仅用于消息嵌入, DualSTC 再嵌套了一层 STC 编码用于载密恢复。Nakajima 和 Ker (2020) 将网格码算法应用于生成式隐写, 给出了一种在线性约束下从指定分布中采样的方法。

1.1.4 非二元隐写编码

使用二进制每个载体元素的最大载荷量是 1 bit。而在最大允许修改幅度为 1 时, 可以对元素进行 ± 1 修改, 此时每元素最多承载 $\log_2 3$ bit 信息, 这表明三元编码具有更高的嵌入效率。Fridrich 和

Lisonek (2007) 基于图着色理论设计了基于 ± 1 修改的编码方法。Mielikainen (2006) 首先将载体的所有像素值两两成对, 之后以像素值对为单位嵌入消息。Filler 等人 (2011) 提出了多层隐写构造 (multi-layered construction) 方法, 进一步将双层构造与 STC 结合提出了“双层 STC”, 从而 STC 可以用于 ± 1 嵌入, 成为使用最普遍的隐写编码工具, 并且“双层 STC”可以扩展到“多层 STC”用于 ± 2 嵌入。

1.1.5 非加性隐写编码

2013 年国际信息隐藏领域 8 位著名学者联合提出了关于隐写的 23 个公开问题, 其中“如何设计非加性隐写编码”排在首位。Kin-Cleaves 和 Ker (2018) 提出了动态 STC 编码方法, 在执行维特比译码进行信息嵌入的过程中, 未译码序列的修改代价会根据之前发生的修改进行动态调整, 实现了非加性隐写嵌入。

1.2 图像隐写

隐写研究有两个主要思路。一个思路是如何减小因隐写所产生的代价, 该思路引导了众多基于最小代价框架隐写方法的蓬勃发展; 另一思路是如何降低被隐写分析检测的概率, 这引发了对抗式隐写方法的兴起。基于最小代价框架的隐写方法是主要的研究热点, 在该方向上, 主要可以分为: 基于统计模型的代价函数设计、基于载体源转换的自然隐写、基于边信息的代价函数设计和基于对抗博弈的代价调整等主要技术思路。

1.2.1 基于模型的代价函数设计

基于统计模型的隐写方法对图像元素进行建模, 通过最小化载体图像和载密图像分布之间的 KL 散度 (Kullback-Leibler divergence) 或最优检测器的能力来设计嵌入代价, 与启发式设计的代价函数不同, 该类方法在统计模型的意义保证了隐写性能。Butora 等人 (2020) 通过启发式设计的隐写代价搜索一个最优的嵌入修改率, 并由此转换成每个像素或 DCT (discrete cosine transform) 系数的隐写 Fisher information, 提出了从基于代价到基于模型的隐写方法 MiPOD (minimizing the power of optimal detector), 在部分情况下提升了启发式代价函数的性能。在 MiPOD 的基础上, Denemark 和 Fridrich (2017a) 提出了使用边信息的 SI-MiPOD, 先使用多元高斯模型对图像获取噪声进行建模并基于预载体 (precover) 对模型参数进行估计, 然后通过最小化载体图像分布

和载密图像分布之间的 KL 散度求得载体元素的修改概率并转化为嵌入代价。Sharifzadeh 等人(2019)使用与 MiPOD 相同的载体噪声模型,同时将秘密信号建模为一个加性高斯噪声,提出了高斯嵌入方案,可实现多元嵌入。Cogranne 等人(2020)利用 DCT 变换的线性属性和多元高斯随机变量的线性变换规律,将 MiPOD 扩展至 JPEG 域(J-MiPOD),同时设计了 4 种使用不同色彩通道嵌入代价的消息分配策略。在相机 RAW 图像可被获取且载体图像生成流程给定(边信息)的情况下,Giboulot 等人(2020b)通过挖掘 JPEG 图像生成流程中像素之间的相关性,优化了 DCT 系数的方差估计;同时使用量化误差的边信息对高斯嵌入方法进行了扩展。Giboulot 等人(2020a)提出了基于同步嵌入的多元高斯嵌入方法(multivariate Gaussian embedding, MGE),对预载体图像和预载密图像进行建模,考虑了块内和块间 DCT 系数的相关性并添加具有特定协方差形式的最优隐写信号,该特定协方差是载体噪声协方差的一个缩放。Giboulot 等人(2021)在噪声模型中进一步考虑了 γ 校正以适应更为完整的图像生成流程,同时探究了“噪声方差”和“内容方差”在应对具有不同知识的隐写分析者时的作用。Taburet 等人(2020)提出了适应于启发式代价的 JPEG 图像隐写同步修改机制,利用图像生成流程中相邻块间 DCT 系数的相关性,先将启发式代价转换为高斯分布,然后由已嵌系数导出条件高斯分布,综合考虑了协方差矩阵的关联性和隐写代价的方差,可用于基于启发式代价的嵌入方案。

1.2.2 自然隐写

自然隐写是一类相对特殊的基于统计模型设计代价的隐写方法,其使用“载体源转换”的思路,利用图像本身的噪声进行建模,以某一种噪声模式下的图像作为载体,将隐写嵌入模仿成另一种噪声模式,这种模仿式的噪声为自然隐写带来了显著的安全性提升。Bas(2017)首先提出了基于“载体源转换”的自然隐写框架,对于一个给定的 ISO(International Standards Organization)感光度 ISO_1 ,先将相机的传感器噪声建模为一个独立高斯分布,然后将嵌入过程模仿成 ISO_1 到另一个更高感光度 ISO_2 的转换过程,并针对 γ 校正和下采样操作设计了载密信号的生成方法(Denemark 等,2018)。Denemark 等人(2018)将自然隐写扩展至 JPEG 图像,通过将

传感器噪声添加至更为复杂的 RAW 图像获取、图像生成和 JPEG 压缩的全流程中,使用 Monte-Carlo 采样估计载密 DCT 系数的分布。前述工作针对的是单色传感器,Taburet 等人(2019a,2021)将自然隐写扩展至彩色传感器,由于彩色传感器会导致 DCT 系数之间具有更强的块内和块间相关性,首先对 3×3 个 8×8 块的 DCT 系数相关性建模为多元高斯分布,然后以子格依次采样的方式计算不同 DCT 块的条件分布。Taburet 等人(2019b)进一步针对非线性性的图像生成流程推导了 DCT 系数载密信号的显式协方差矩阵。

1.2.3 基于边信息的代价函数启发式设计

在图像隐写中,边信息是隐写方可获得而隐写分析方无法确知的信息,这种信息的不对称可以提升隐写方法的安全性。边信息的种类是多种多样的,除了前述的相机获取的 RAW 图像外,边信息还可以是图像降质处理(如 JPEG 压缩、下采样)的量化取整误差和同一场景拍摄的多幅图像等。近期亦有针对这些边信息的启发式隐写方法。Denemark 和 Fridrich(2017b)挖掘了同一场景拍摄的两幅 JPEG 图像携带的边信息,利用两幅 JPEG 图像的相同位置 DCT 系数的差异性,设计了基于该边信息的非对称代价调制方法,显著提升了只有单幅 JPEG 图像的隐写安全性。Denemark 和 Fridrich(2017c)进一步探究了同一场景拍摄的多幅 JPEG 图像的边信息构造方法,即选取其中两幅最接近的 JPEG 图像作为配对图像来构造边信息,并分析了代价调制因子与质量因子相关的原因。Butora 和 Fridrich(2020b)基于最小扰动的思想,改进了边信息已知的 JPEG 图像代价调制方法,通过合理惩罚与量化取整误差相反的修改方向的嵌入代价,提升了低质量因子图像的隐写安全性。Butora 和 Fridrich(2020a)针对压缩率更大的 Trunc 取整 JPEG 图像,提出了抑制零 DCT 系数修改的代价函数和使用量化取整误差的代价调制方法。使用量化取整误差进行代价调制和基于“邻域修改方向一致”进行代价调制是空域图像隐写中两种不同的非对称代价调制方法,Boroumand 和 Fridrich(2020)针对两种方法各自鼓励的修改方向存在相同或冲突的情况,优化了两种方法的组合策略,在量化取整误差调制代价中引进了基于修改方向一致的调制因子,提升了直接组合的性能。

1.2.4 基于对抗博弈的代价调整

对抗样本是一种可以使得目标隐写分析检测器检测失效的方法,而将对抗样本纳入隐写分析训练集则可以增强其检测性能。在利用对抗样本技术进行隐写和隐写分析博弈方面,Bernard 等人(2019, 2021a)提出通过多轮迭代训练,并在每一轮迭代过程中选取让隐写分析检测器集合最难以检测的载密图像组成训练集合,然后用该集合训练新的隐写分析检测器并加入至检测器集合中。该方案显式地构造了一个最小—最大博弈方案,极大地提高了隐写方法抵抗深度学习隐写分析检测的能力。此外,Bernard 等人(2021b)提出将多个隐写分析检测器的检测评估视为非加性代价度量,通过对 Gumbel-Softmax 分布采样获得期望梯度,再进行对抗样本修改调整代价值,从而提升隐写抗检测能力。

1.3 视频隐写

近年来,随着网络带宽的增加以及各种高效视频压缩算法的提出,无论在 PC 互联网还是移动互联网上,数字视频的网络流量所占比重越来越多。据 2021 年 8 月中国互联网络信息中心(China Internet Network Information Center, CNNIC)发布的《中国互联网络发展状况统计报告》显示,截至 2021 年 6 月,中国

网络视频(含短视频)用户规模达 9.44 亿,占网民整体的 93.4%。可见,数字视频已成为网络上广为流行的主流媒体之一。视频相对于图像,在时间维度上做了扩展,给隐写带来了更大的可用空间,即使较低的相对嵌入率,也能达到较高的绝对嵌入容量。因此,视频隐写技术引起国内外学者及研究机构的密切关注。

为便于储存传输,原始视频需要进行编码压缩,以去除空间、时间维度上的冗余。目前,广为使用的视频压缩国际标准主要有 H.264/AVC(advanced video coding)、H.265/HEVC(high efficiency video coding)和 MPEG-2/4(moving picture expert group)。此外,中国还制订了新一代编码标准 AVS(audio video coding standard)和 AVS2。视频数据在压缩编码的过程中,衍生出了预测模式、运动矢量和 QDCT(quantized discrete cosine transform)系数等载体数据,这些数据为视频隐写提供了更多的嵌入方式和嵌入空间的选择。以 H.264/AVC 为例,结合编码的不同阶段,图 1 给出了视频隐写的可嵌入数据域。与图像隐写相比,视频隐写不仅要考虑帧内的空间特征,还要考虑时域上的帧间特征。根据秘密信息嵌入的数据域不同,现有的视频隐写方法主要分为空域和压缩域隐写。

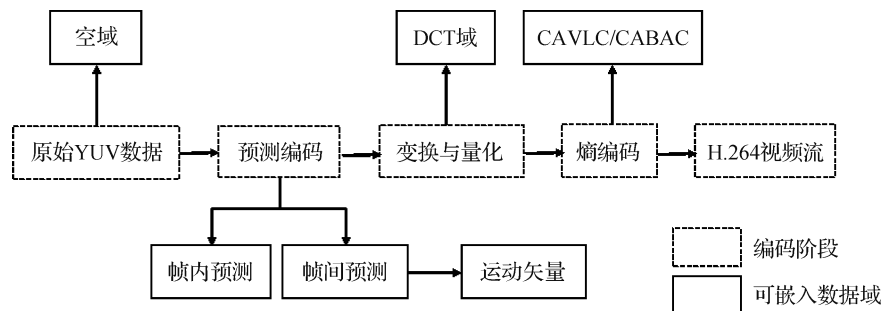


图 1 H.264/AVC 视频隐写的可嵌入数据域

Fig. 1 Embeddable data fields for H.264/AVC video steganography

1.3.1 空域视频隐写

空域视频隐写利用视频每一帧图像的空间冗余性,直接对视频的色彩空间 RGB 或 YUV 进行修改以嵌入秘密信息。这类方法类似于图像隐写,因此很多图像隐写方法可移植到视频隐写中。例如,Cetin 和 Ozcerit(2009)将视频的每一帧作为一个嵌入单元,计算其直方图特征并设置一个阈值进行隐写,秘密信息嵌入在视频帧的 RGB 像素上。空域视频隐写方法考虑了人类视觉系统的特性,具有较大的嵌入容量。然而,视频在存储与传输过程中通常

需要进行视频压缩编码,而空域视频隐写需要完全解码,因此嵌入的秘密信息容易在后续的压缩编码过程中损失。目前,一些学者尝试采用纠错码和重复嵌入的方式去增强抗视频压缩编码的鲁棒性,降低提取信息的误码率。

1.3.2 压缩域视频隐写

压缩域视频隐写通过修改压缩编码过程中产生的编码参数以嵌入秘密信息,已成为视频隐写领域的研究重点。可用于嵌入信息的载体数据通常包括帧内/帧间预测模式、运动矢量、QDCT 系数以及熵

编码码字等。目前国际上的研究进展多集中在基于预测模式和运动矢量的视频隐写技术,此外,国外研究机构还开发了少量的视频隐写工具,可在互联网上免费下载。

基于帧内预测模式的视频隐写按照一定的映射规则,通过调制视频编码中宏块的帧内预测模式实现隐写。由于该类方法只能在 I 帧中嵌入信息,而视频序列中 I 帧的比例较低,因此隐藏容量受到限制。为了提高隐藏容量,一些算法结合矩阵编码来减少对载体信息的修改量,从而提高嵌入效率。相对于帧内预测隐藏方式,目前基于帧间预测的视频隐写研究相对较少。帧间预测技术旨在去除视频的时域冗余,由于帧间预测过程主要是在 P 帧上进行的,因此基于帧间预测的视频隐写算法一般将 P 帧作为主要的嵌入帧,且 P 帧数量较多,也能提供更多的可嵌入空间。在 H. 264/AVC 的帧间预测中采用了可变尺寸块分割和运动估计算法,因此,早期的方法通过建立宏块级帧间预测模式与秘密信息间的映射关系,根据秘密信息比特调制当前帧间编码单元的宏块级帧间预测模式来嵌入信息(Kapotas 和 Skodras, 2008)。此外,还可通过构建编码单元帧间划分模式预测模型实现信息嵌入(Shanableh, 2018)。

基于运动矢量(motion vector, MV)的视频隐写是将视频编码过程中的运动估计步骤获取的运动矢量作为载体,进行隐写修改,完成信息嵌入。一般视频预测帧中的每个宏块至少包含一个运动矢量,由水平和垂直两个分量组成。与其他多媒体载体类似,不是所有的 MV 都适合用于嵌入信息,这是因为对有的 MV 进行轻微修改就会导致视频画面质量和码率的较大改变,而有的 MV 在进行大幅度修改后仍不会对视频质量有过大的影响。例如, Aly (2011) 选择预测误差较大的宏块对应的运动矢量进行信息嵌入,并通过重构 P 帧和 B 帧获得最小的嵌入代价。

1.3.3 基于深度学习的视频隐写

在隐写领域,已经有基于生成对抗网络(generative adversarial network, GAN)、卷积神经网络(convolutional neural network, CNN)等深度神经网络的端到端隐写架构,但限于视频本身数据量大,以及复杂的视频编解码过程,目前用于视频隐写的端到端神经网络极少。最近,谷歌的 Luo 等人(2021)提出了一种称为 DVMark 的端到端多尺度深度视频水印架构,整个架构包括编码器、失真层、解码器和视频

判别器 4 部分,水印信息嵌入在多个时空尺度上,并对 H. 264 压缩、裁剪、丢帧和高斯噪声等具有较强的鲁棒性。另外,麻省理工学院的 Zhang 等人(2019)提出了一种称为 RivaGAN 的基于注意力机制的鲁棒视频水印架构。这些水印框架为基于深度学习设计视频隐写也提供了思路。

1.3.4 视频隐写工具

OpenPuff (https://embeddeds.w.net/OpenPuff_Steganography_Home.html) 是一款基于文件格式的隐写软件,也是目前国外下载网站中免费下载量较大的一款专业隐写软件,支持多种视频、图像与音频格式。在视频方面,OpenPuff 支持的格式主要包括 3GP、MP4、MPG、VOB、FLV、SWF 等。此外, MSU StegoVideo (http://compression.ru/video/stego_video/index_en.html) 是目前互联网上可下载的一款典型的空域视频隐写软件,2006 年由莫斯科国立大学开发。该软件能够将任意格式的文件隐藏至 AVI 格式的视频中,并且支持任意压缩编码格式,还具有一定的抗压缩转码能力。

1.4 音频隐写

数字音频应用的普及为信息隐藏提供了新的隐蔽载体空间和通信信道。目前,数字音频隐写的研究主要集中在两个方面:基于音频载体的隐写算法和基于音频流数据的隐蔽通信系统。

在基于音频载体的隐写算法研究方面,国外的研究成果在研究的深度和创新性方面相较于国内滞后,主要是对传统音频隐写算法的微量优化和扩展。隐写手段包括基于人类听觉感知冗余特性的隐写;基于音频时域信号的隐写,如 LSB (least-significant-bit) 安全隐写、QIM (quantization index modulation) 语音隐写和回声语音隐写方法等;基于音频变换域信号的隐写,如基于扩展频谱的语音隐写、基于相位的语音隐写以及基于小波变换的语音隐写算法等。伊拉克高等教育和科学研究部 AlSabhany 等人(2020)对数字语音隐写工作进行了较为全面的综述。印度理工学院(Indian Institute of Technology, IIT)电子和电气工程系的 Dutta 等人(2020)对语音隐写技术的发展进行了综述。传统语音隐写方法在面向实际的语音隐蔽通信环境时会面临语音编码压缩,隐写信息会被损坏,因此该类隐写算法在实际隐蔽通信中使用较少。通过对各种语音编码算法中的压缩参数进行调制是现有音频隐写算法的主要趋势。Khed-

dar 等人(2019)在 MELP(mixed-excitation linear prediction)语音编码 bit 流中基于基音和傅里叶幅度值调制实现 2.4 kbps 隐写;Banjarnahor 等人(2019)使用声学特征实现了鲁棒隐写;Pal 等人(2021)从多域嵌入的角度实现大容量的隐写。

在基于音频流数据的隐蔽通信技术研究方面,国外的研究成果较多集中在面向 VoIP(voice over internet protocol)通信环境的语音隐写技术,这些技术不限于基于音频数据本身为载体的隐写,而是以基于语音通信信道为载体信道的隐蔽通信机制,利用语音的通信会话过程中的各个可能环节进行秘密信息的传输。该方面的主要研究团队是波兰华沙工业大学电子与信息技术学院 Wojciech Mazurczyk 教授。其所利用 VoIP 隐蔽通信的载体主要包括语音数据、VoIP 协议数据和 VoIP 数据包间隔等,利用 VoIP 中语音数据流的统计分布特性进行隐写通信(Mazurczyk 和 Szczypiorski, 2008)。Saenger 等人(2020)利用 VoIP 通信中的活动语音检测和静音编码机制,在静默数据包中隐藏秘密数据实现隐蔽通信。Mazurczyk 等人(2016)利用 Skype 的视频流作为信息隐藏的载体,实现秘密信息的传输。其他国家的学者在 VoIP 的隐蔽通信技术方面也有很多研究成果。伊拉克科尔巴拉大学电气与电子工程系的 Shahadi 等人(2021)提出基于 VoIP 语音编码器 G. 711 的隐蔽通信机制。德国鲁尔大学的 Kohls 等人(2016)提出基于 Skype 的鲁棒语音隐写算法,实现了基于 Skype VoIP 通信过程中的隐蔽通信。阿塞拜疆技术大学的 Mustafayeva 等人(2019)提出基于手机移动终端中的 WhatsApp 的隐蔽通信;波兰电子科技大学电子系的 Wojtuń 和 Piotrowski 等人(2021)针对 VoIP 通信中的语音信号隐写的同步机制,所提方法在 VHF(very high frequency)无线电链路和 VoIP 信道中传输隐写数据具有有效性。

1.5 文本隐写

在当前的网络环境下,文本相比于图像、音频等其他数字载体同时具有独特的优势和挑战。优势主要体现在两方面:1)文本是人类语言的符号化编码,是人们进行信息交流的主要形式,其使用场景的广泛性和普遍性给文本隐写术带来了广阔的应用场景;2)文本在网络空间传输时具有较强的鲁棒性,信道噪声几乎不会使其包含的隐蔽信息丢失。然而,利用文本进行信息隐藏同样面临极大的挑战:语

言的高度信息编码和低信息冗余特性,使其很难嵌入额外信息。因此,如何实现在文本中安全且高效地嵌入额外信息是个极具挑战的课题。

当前主流的文本隐写术根据秘密信息嵌入域的不同通常可以分为基于文本格式的隐写术和基于文本内容的隐写术,如图 2 所示。其中基于文本格式的隐写术主要利用文本在特定文档中的组织、排版和呈现时的特定规则实现信息嵌入,如编码并修改 PDF 文档中字符间的位置信息(刘友继 等,2006)。这类方法通常具有较高的视觉隐蔽性,但它们的使用场景具有一定的局限性,并且文字的重新录入、内容转移和格式变化都会造成隐蔽信息的破坏或丢失。基于文本内容的隐写术,也称为语言隐写术,主要采用自然语言分析和处理手段,利用文本中的语言特征实现隐蔽信息嵌入,是当前文本隐写研究的热点和难点内容。语言隐写术通常可以归纳为修改式、检索式和生成式 3 种隐写策略。

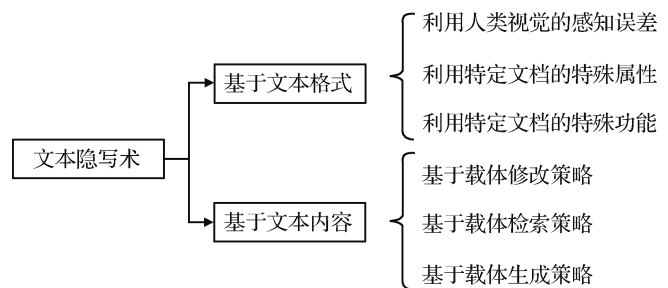


图2 文本隐写术种类划分

Fig. 2 Classification of text steganography

检索式语言隐写术通过对大规模文本库中的样本进行特殊编码,然后根据待嵌入的秘密信息选择对应语句进行传输。这类方法的好处是不需要对原始文本进行任何修改就可以代表特定的隐蔽信息,具有极高的隐蔽性。但是缺点在于需要事先共享一个非常大的语料库,并且通常难以获得较高隐藏容量。

修改式语言隐写术主要是对文本中词汇级或者句子级的语义单元进行同义替换以嵌入隐蔽信息。基于同义变换的文本隐写术曾引起大量研究人员关注,这类方法主要缺点在于嵌入率比较低,难以传递大量信息。但是最近随着掩码语言模型的提出和应用以及掩码语言模型的巨大潜力,基于修改策略的语言隐写术又得到了国际上研究人员的关注,其中日本京都大学的 Ueoka 等人(2021)利用掩码语言模型强大的填空能力,极大简化了替换规则的构建,

同时有效提升了该类语言隐写术的隐藏容量和抗自动检测能力。尽管如此,这类方法的隐藏容量相比基于生成策略的语言隐写术仍然较低。

生成式语言隐写术成为近两年的热点研究方向。其主要思路是根据待嵌入的秘密信息自动生成一段自然文本,在生成过程中对文本语义单元进行编码实现隐蔽信息嵌入。该策略不需要事先给定嵌入秘密信息的载体。由于没有事先给定载体的限制,因此隐写方在嵌入信息过程中有较大的自由,可以获得较高的信息嵌入率。同时,生成式隐写策略面临的挑战同样非常巨大。为了提升语言感知隐蔽性,西班牙马德里理工大学的 Muñoz 等人(2010)提出基于 N-gram 模型和短语片段集合的隐写文本自动生成模型。英国剑桥大学的 Chang 和 Clark (2010)进一步利用 Google 构建的 Google N-gram 数据集指导隐写文本生成。美国哈佛大学的 Ziegler 等人(2019)利用 GPT-2 语言模型和算术编码生成隐写文本。美国伊利诺伊大学的 Shen 等人(2020)结合自然语言处理中的核采样方法在 Ziegler 等人(2019)工作的基础上改进,提出了自适应的算术编码方法。

2 国内研究进展

2.1 隐写编码

国内学者在隐写编码发展的各个阶段都做出了贡献。

2.1.1 常数代价隐写编码

在常数代价隐写编码阶段,Wang 等人(2012)提出了扩展矩阵方法提高随机矩阵编码的嵌入速度。Zhang 等人(2008)从隐写术本身规律出发,发现了信息嵌入的“修改可复用特性”,提出了“修改复用”编码技术,给出了可对各种载荷率逼近率失真界的编码方法 ZZW(Zhang Zhang Wang)。

2.1.2 两级代价隐写编码

在湿纸模型下,Zhang 等人(2010a)提出了折纸算法“Paper Folding”,该方法将二元湿纸载体对折编码。借用湿纸码的比喻,折纸算法的思想可以比喻成构造了一个特殊的复写纸,只需对顶层修改,就可以在每层都写上字,关键之处在于每层可以写出不一样字。这一方法可以多次递归调用,即将载体多次对折,从而生成各种载荷率的码。折纸算法通过折叠载体,将一个找最优解问题转化成了多

个找解问题来解决,从而降低了计算复杂度,折纸算法不仅可以逼近湿纸模型的率失真界,计算复杂度也明显低于以前的方法。

2.1.3 多级代价隐写编码

在多级代价模型下的编码方法阶段,在 STC 编码的基础上,Zhao 等人(2016)提出了新的渐近最优的双层 STC 编码 NDSTC(near-optimal double-layered syndrome-trellis codes),与传统的单层 STC 相比,NDSTC 双层嵌入顺序颠倒,并允许少量的 ± 2 修改,提高了安全性。Feng 等人(2020)则是在 STC 编码内嵌套了一层 FCC(forward error correction)纠错编码,用以提升隐写编码的鲁棒性。Li 等人(2020b)基于极化码(polar codes)设计出了可逼近率失真界的极化隐写码 SPC(steganographic polar codes),并解决了现实场景中载体长度非 2 幂次方等问题。

2.1.4 非二元隐写编码

Zhang 和 Wang(2006)将秘密比特转换为多进制数,提出了 EMD(exploiting modification direction)方法,至多只需要对载体分组中的一个元素进行 $+1$ 或 -1 修改。Zhang 等人(2007a)将 ± 1 编码问题等价分解为两个二元编码问题,提出双层嵌入编码方法并证明其能达到率失真界性能。在修改幅度为 1 的 ± 1 编码中,每个元素所能承载的最大信息量为 $\log_2 3$ 比特;当最大修改幅度为 2 时,最大信息量可增大为 $\log_2 5$ 比特。针对 ± 2 隐写,Zhang 等人(2010b)提出了 3 层构造方法,以此分解为逐层的二元编码问题。Zhang(2010)进一步改进了 3 层构造方法,使之逼近 ± 2 隐写的嵌入效率上界。

2.1.5 非加性隐写编码

Zhang 等人(2017b)用定义在像素块上的联合代价表达修改的非加性,并发现了“联合隐写代价的可分解性”,提出了非加性隐写编码 DeJoin,将非加性编码问题等效分解成几个加性编码问题,从而实现快速嵌入。Wang 等人(2021c)提出了渐进式栅格编码(progressive trellis coding,PTC),在嵌入过程中,维护与可能的最佳路线相对应的多个上下文,并定期回溯以确定应如何修改每个载体块。每次修改后,都会重新评估剩余的载体块及其嵌入代价,并更新每个上下文以反映修改影响。

2.2 图像隐写

2.2.1 最小代价框架下的代价函数设计

1) 启发式隐写代价设计。在图像隐写研究中,

加性代价函数的设计是最为常见的。随着空域图像代价函数的研究日趋完善,学者更多地将研究重点转移至代价函数的通用增强方法以及 JPEG 图像和彩色图像的代价函数设计上。

在代价函数增强方法的研究中,Zhou 等人(2017)挖掘了多种已有代价函数的争议性,提出了“争议像素优先(controversial pixel prior, CPP)”原则,充分利用隐写分析器对这些争议像素的不敏感性来实现代价函数定义形式上的变异,提升了现有代价函数的安全性。王子驰等人(2018)利用像素灰度级本身的代价值优化原始代价函数,然后根据修改情况多次迭代地调整嵌入代价,尽可能聚集修改方向,从而使载密图像具有更好的抗检测性。Chen 等人(2019)提出了“微尺度隐写”(microscale steganography, MS)的代价增强方法,通过对图像进行内容增强和细节放大,更精细地挖掘载体图像内容特点,以辅助进行合理的代价定义,提升了现有代价函数的安全性。Wu 等人(2020)观察到图像平坦区域像素由于小尺度滤波器的作用而具有低修改代价的现象,通过多尺度滤波器对载体图像进行增强,弥补了代价的分配不当的问题。

在 JPEG 图像代价函数的研究中,“纹理复杂优先”仍是首要遵循的设计原则。Wang 等人(2016)、Wei 等人(2018)和 Su 等人(2018)分别使用均值滤波、小波滤波和 Gabor 滤波对解压缩图像的纹理复杂度进行度量,并结合量化步长获取适合修改的低复杂度 DCT 系数。Hu 等人(2018a)和 Su 等人(2022)则研究了高效的域转换方法,能够将空域代价函数转化为 DCT 域代价函数,从而获取较高的隐写安全性和较低的计算复杂度。

设计非加性代价函数是隐写研究的公开问题之一,学者针对 JPEG 图像亦设计了多种非加性代价隐写方法。Li 等人(2018)从抑制隐写修改的块效应出发,提出了“块边界连续性”(block boundary continuity, BBC)原则,并结合联合代价分解(De-Join)模型(Zhang 等,2017b)设计了相邻块相同模式 DCT 系数的非加性代价嵌入方法,提升了现有加性代价函数的性能。Wang 等人(2021a)考虑了相邻块中所有 DCT 系数对空域块边界连续性的影响,提出了一个加强版策略 BBC++,采用多轮嵌入并在每一轮嵌入后更新下一轮的载体和代价,更好地维持了空域块边界的连续性。Lu 等人(2020)也从

抑制块效应的角度设计了 JPEG 图像非加性隐写方法。进一步地,Wang 等人(2021b)观察到空域块边界的修改易被检测的现象,提出了“块边界维持”(block boundary maintenance, BBM)原则,设计了 DCT 块内不同系数间的非加性嵌入方法,有效减少了隐写对空域块边界的修改。受启发于性能优异的“边信息已知”JPEG 图像隐写方法,近期亦有针对 JPEG 图像的边信息估计隐写研究。该类方法首先估计量化取整误差,然后将其用于非对称代价调制,显著提升了现有代价函数的性能。王丽娜等人(2018)使用 AR-CNN(artifacts reduction convolutional neural network)估计原始空域图像,并基于估计的取整误差极性设计了简单的二元嵌入隐写方法。Wang 等人(2019)使用 3×3 均值滤波器对解压缩空域图像进行滤波,将输出的边界值替换掉原始边界的像素值,并对更新后的空域图像进行 JPEG 压缩得到取整误差极性用于非对称代价调制。Wang 等人(2018b)进一步使用 3×3 维纳滤波器来估计原始空域图像,并通过最小化载体/载密的隐写分析特征距离来选取最优调制因子。由于分别需要执行 20 次的消息嵌入和特征提取,该方法的计算复杂度较高。Li 等人(2020a)使用专门的去块效应方法 SSRQC(structural sparse representation and quantization constraint)估计原始空域图像,并设计了基于估计取整误差极性和幅值的代价调制模型,大幅提升了现有代价函数的安全性。

在彩色图像代价函数的研究中,直接将灰度图像的方法独立地拓展至彩色图像 3 个颜色通道并非最佳方案。汤光明等人(2019)分析了彩色分量内容特性与通道间相关性的关系,提出中心元素的代价更新准则,在嵌入过程中依据相邻分量修改情况对代价进行动态调整,设计了一种彩色空域图像隐写方法 CCMS(modification strategy for color components)。Liao 等人(2020)提出 ACMP(amplifying channel modification probability)方法对载体图像的代价分布与秘密信息的分配关系进行定量度量,利用图像 RGB 的 3 个通道相关性调整通道间对应像素点的代价,增大通道间对应像素点被同时修改的概率,提高了彩色图像隐写安全性。Wang 等人(2020)发现 G 通道与 R、B 通道之间的相关性强于 R 与 B 之间的相关性,因此设计了同步 R、B 通道与 G 通道的修改方向的算法 GINA,大幅提高了隐写安全性。

2) 基于模型的隐写代价设计。Hu 等人(2018b)优化了空域图像非加性嵌入方法 CMD (clustering modification directions), 将已嵌子图的修改方向作为当前子图概率分布的先验知识, 通过最小化载体图像和载密图像的 KL 散度计算非对称的修改概率, 避免了对代价调制因子的人工选取步骤。Qin 等人(2019)使用高通滤波器组获取图像残差并计算残差的 Fisher information, 通过最小化载体图像和预测的载密图像的 KL 散度来计算最优的嵌入概率, 获得了更好的隐写代价。Su 等人(2021)使用交叉相邻的 4 个元素构造的高斯马尔可夫随机场来捕捉相邻像素的依赖性, 将载体图像以棋盘格式分成两个不连接的子图像, 将隐写的安全问题转化为最小化载体和载密图像之间的 KL 散度, 提出了 GMRF (Gaussian Markov random field) 隐写算法。

2.2.2 基于深度学习的隐写代价设计

1) 基于 GAN 的隐写代价学习。隐写生成和隐写分析检测之间的关系与生成对抗网络 (GAN) 结构有相似之处, 因此利用 GAN 进行隐写方法设计具有可行性。其中 GAN 生成器代表隐写方, GAN 判别器代表隐写分析方, 生成器和判别器的交替更新可视为隐写与隐写分析之间的博弈对抗, 当一个收敛的判别器无法区分真实图像和生成器所生成的载密图像时, 说明隐写方取得了优势。直接用 GAN 生成的载密图像并不具有很强的信息解码能力, 因此 Tang 等人(2017)提出利用 GAN 学习隐写代价的方案 ASDL-GAN (automatic steganographic distortion learning GAN)。其中, 生成器和判别器都分别由卷积神经网络组成, 生成器学习每个像素的嵌入修改概率, 该概率最终可以通过最优嵌入公式转换为代价。通过一个由全连接神经网络及 Sigmoid 激活函数构建的模拟嵌入器, 不仅可以进行模拟嵌入使得判别器具有可靠的载密图像输入, 而且还可以进行梯度回传优化生成器。Yang 等人(2020a)在此框架上提出 UT-GAN, 利用性能更优的 U-Net 作为生成器, 以及利用 double-tanh 激活函数作为模拟嵌入器, 获得了不俗的性能。Yang 等人(2019a)提出 JS-GAN (JPEG steganography GAN), 采用随机极性调制的嵌入概率作为模拟嵌入修改, 可应用于 JPEG 图像。

2) 基于强化学习的隐写代价学习和调整。在基于 GAN 的隐写代价学习方案中, 模拟嵌入容易导致梯度消失或对应的修改与实际修改产生偏差。为

了避免该缺陷, Tang 等人(2021)提出基于采样方式产生离散的模拟修改值, 设计了将隐写分析检测器梯度值作为奖惩函数反馈进行强化学习的方法 SPAR-RL (steganographic pixel-wise actions and rewards with reinforcement learning), 可以获得比 GAN 方法更为稳定和更为有效的结果。Mo 等人(2021)结合蒙特卡罗树搜索 (Monte Carlo tree search, MCTS), 提出了基于强化学习技术的非加性隐写框架 MCTSteg, 在多次模拟代价调整动作的过程中自动学习代价调整策略, 可以获得比手工设计的非加性代价调整策略更好的性能。

3) 基于对抗样本的隐写方法。为应对当前深度学习检测器已成为主流检测方法所带来的挑战, 国内研究学者提出在信息隐写中使用对抗样本技术的各类方法。根据加入对抗样本信号的不同阶段, 可以分为在信息嵌入前加入、在嵌入中加入和在嵌入后加入 3 种类型。Zhang 等人(2018a)提出在嵌入前对载体图像加入对抗样本噪声, 然后在获得增强后的载体图像中进行信息隐写, 该方法可以拓展至同时对抗多种检测器的情况。Tang 等人(2019)提出在嵌入中加入对抗样本噪声的方法, 在生成代价过程中调整不同修改极性的代价, 并最小化可能需要的修改元素。Ma 等人(2019)结合二元嵌入的极性信息进行对抗样本代价调制, 并提出应减弱梯度图像中所不应呈现的棋盘格效应。Mo 等人(2019)提出对梯度幅度较大的像素通过多次迭代进行代价调整, 该方法可适用于 JPEG 图像。Qin 等人(2021)提出了将 CMD 与对抗样本结合的方法, 可以达到更好的对抗成功率。Zha 等人(2019)提出在嵌入后加入对抗样本噪声的方法, 通过对少量像素添加对抗样本信号, 且令修改的像素校验规则符合信息提取方式, 该方法具有一定的迁移能力。Song 等人(2021)采用启发式搜索的方式, 对载体进行随机后处理获得多个版本的载密图像, 在特征空间选择与载体图像最相邻的一个版本作为最终的载密图像。

2.2.3 鲁棒隐写

鲁棒图像隐写是近年来的研究热点, 它应对的是图像隐写方法在社交网络平台的实用性问题。传统的图像隐写方法均假设载密图像是经过无损传输的, 故接收方能够完全无误地提取秘密信息。但是, 社交平台(如 Facebook、微信等)会对上传的图

像进行有损处理以节省内存和带宽,如尺寸缩减和 JPEG 压缩。由于载密图像发生变化和 STC 具有误差扩散特性,接收方此时并不能准确地提取秘密信息。因此,以社交网络平台作为隐蔽通信信道的隐写方法需要同时考虑抗检测性与鲁棒性。

针对信道 JPEG 重压缩的问题,目前抗 JPEG 压缩的鲁棒隐写研究可以分为两类。第 1 类方法是基于鲁棒水印的设计思想。Zhang 等人(2016b)提出了“构建抗压缩域+纠错码”的鲁棒隐写框架,该框架首先在载体内构建抗二次 JPEG 压缩能力较强的抗压缩域,然后再利用 RS(Reed-Solomon)纠错码进一步提高消息提取的正确率,并利用特征域挑选算法将修改更多地集中于图像纹理复杂区域,进一步提升安全性(Song 等,2021)。为了能够充分利用 JPEG 量化操作的特性,Zhang 等人(2018c)在 DMAS(dither modulation based adaptive steganography)算法中利用抖动调制的方法修改中频的交流 DCT 系数完成消息嵌入,以实现性能的提升。虽然以上 3 种算法都具有较强的鲁棒性,但是由于抗压缩域较小且只采用编码效率较低的二元 STC,因此抗检测性较弱且容量较小。Yu 等人(2020)提出的 GMAS(generalized dither modulation based adaptive steganography)系数修改的过程中考虑了非对称代价,在扩大嵌入域的同时使用了三元 STC 嵌入,其安全性和鲁棒性有了较大幅度的提升。Qiao 等人(2021)和 Zhu 等人(2021a)分别利用 DCT 系数的符号和最后一个非零系数位置在压缩前后的不变性,进一步提升了鲁棒隐写的性能。不同于对秘密信息进行纠错编码,Zhang 等人(2020b)选择部分载体嵌入消息,然后将循环检验位嵌入到剩余载体中用于载密纠错。第 2 类方法可以认为是启发式的,通常构思巧妙。为了能够抵抗更低质量的 JPEG 压缩,Tao 等人(2019)在不考虑空域量化损失的情况下,通过将消息嵌入到压缩后的图像中获得载密图像,然后反过来再修改载体图像,使得修改后的载体图像通过有损信道后仍能获得载密图像,具有很高的鲁棒性,但假设过于理想难以实用。Zhao 等人(2019)发现 JPEG 图像被相同质量因子压缩多次后更稳定,提出了信道匹配算法,不断地进行图像上传下载操作,直到图像稳定后,在稳定图像上嵌入信息,提升了鲁棒性。Lu 等人(2021)利用自编码器从被信道处理破坏后的图像中恢复出原始载密图像以

实现信息提取。

针对信道对图像进行尺寸缩减的问题,Zhang 等人(2018b)提出了仅能抵抗尺度变换中的最近邻插值算法的鲁棒隐写方法,利用变换前后像素的一一对应关系实现了鲁棒性。Zhu 等人(2021b)利用逆插值公式进一步实现了对多种插值算法的鲁棒性。Zhang 等人(2021a)提出了抗减半降采样处理的鲁棒隐写方法,通过对载体图像进行增强,使之在减半缩放处理后恰为已经嵌入秘密信息的接收方图像,从而可以使用与嵌入方法对应的提取方法进行秘密信息的无损提取。考虑到社交网络平台信道的复杂性,Zhang 等人(2020a)基于“构建抗压缩域+纠错码”框架,提出了可以抵抗多种攻击(如 JPEG 压缩、尺寸缩减和高斯噪声等)的鲁棒隐写方法。

由于社交网络平台只会对超过尺寸约束门限的图像进行尺寸缩减处理,即图像的尺寸变换是容易避免的,因此目前关于鲁棒隐写方法的研究主要针对 JPEG 图像的二次压缩问题展开。大多数方法并不需要知道社交网络平台的任何压缩信息,但是其抗检测性能较弱并且容量较小。少量方法假设了社交网络平台的 JPEG 压缩过程可以被完美地人工模拟,以至于可以在线下执行社交网络平台的一次(Tao 等,2019)或多次(Zhao 等,2019) JPEG 压缩。但是目前还不能够完美地模拟社交网络平台的 JPEG 压缩过程,因此在实际应用中只能将原始图像经过实际的社交网络平台上传和下载一次或多次来实现消息嵌入,这种行为本身就是可疑的而且比较耗时。因此,目前的鲁棒隐写方法都存在各自明显的缺陷,设计适用于社交网络平台的安全鲁棒图像隐写方法仍然任重道远。

2.3 视频隐写

相比于国外,目前国内在视频隐写技术方面的研究更为活跃,且大多在压缩域嵌入信息。在基于帧内预测模式的视频隐写技术方面,Yang 等人(2011)对 I4 模式进行分组,并将 2 比特秘密信息通过矩阵编码映射到 3 个 I4 模式中,且每嵌入 2 比特信息只需对一个 I4 模式进行修改。修改预测模式会在一定程度上影响码率,但可使接收端从压缩视频中准确地提取出秘密信息,且不需要对视频进行完全解码,因此算法效率较高。

基于运动矢量的隐写嵌入容量远高于帧内预测模式和 QDCT 系数的隐藏方法(李松斌等,2016),

并且具有画面失真小、检测难度大的优势(王丽娜等,2014;Su等,2011;Yang和Li,2018)。国内在基于MV的视频隐写方面的研究工作主要集中在如何选择以及如何修改候选MV的两个关键问题上。例如,Zhang等人(2016a)选择具备局部最优特性的候选运动矢量;王丽娜等人(2017)选取低复杂度宏块进行信息嵌入,以保持运动矢量局部最优,并通过加减1方法保持运动矢量相互间的相关性。

视频序列经帧内和帧间预测后得到的预测误差,经DCT变换、量化后得到QDCT系数。QDCT系数隐写方法类似于JPEG图像的隐写,均是将信息嵌入在量化后DCT系数中。不同之处在于,由于视频的QDCT系数是从绝对值较小的预测残差变换得到,对于P或B帧,大部分的QDCT系数为0、1、-1,为避免引入过大的失真,嵌入信息时通常不对值为0、1、-1的系数进行修改,因此,该类方法嵌入容量不是很高。另外,基于QDCT系数的隐写并不需要考虑对修改后的DCT系数进行DCT反变换,更多需要考虑的是秘密信息的隐蔽性和鲁棒性。由于H.264/AVC标准中的帧内预测采用相邻块像素预测方式,因此直接修改残差块QDCT系数会使帧内宏块在预测编码过程中发生误差扩散,形成失真漂移,导致视频画面失真较大。为解决这些问题,可以考虑通过选择残差块中合适的耦合系数对来防止隐写修改产生的误差扩散到其他块(Ma等,2010;

Li和Wang,2019)。

熵编码是视频压缩编码的最后一个阶段,基于熵编码的视频隐写方法直接在熵编码后的码流中嵌入秘密信息。针对熵编码的不同方式,该类隐写方法主要基于CAVLC(context-adaptive variable-length coding)编码拖尾系数(Li和Wang,2019)、CABAC(context-based adaptive binary arithmetic coding)编码末尾比特位(You等,2017),通过修改拖尾系数的数量或符号、码字替换等方法实现信息嵌入。基于熵编码的隐写的优势是码率变化小,可无损恢复秘密信息,且计算复杂度低,接收端无需解码即可从载密码流中直接提取秘密信息。然而,由于熵编码阶段冗余空间少,致使嵌入容量不高,且视频质量难以保证。

2.3.1 基于失真代价的自适应视频隐写

隐写分析技术的快速发展使隐写术从“非自适应”向“自适应”阶段发展,即优先修改代价小(难检测)的区域。与图像不同,视频隐写中嵌入修改操作不只是对当前像素块引入失真,同时对相邻块和相邻帧都可能会引入失真,因此,应考虑嵌入修改对视频元素造成的多种扰动来设计代价函数。国内在基于失真代价的自适应视频隐写技术方面的研究成果较多,表1列出了近几年国内学者在该方向隐写算法的基本信息,这些算法虽然基于不同的失真代价函数设计思想,但均采用STC或双层STC嵌入信息,以实现总代价的最小化。

表1 近几年基于失真代价的视频隐写算法基本信息
Table 1 Basic information of video steganography algorithms based on distortion cost in recent years

年份	文献	失真代价函数设计思想	视频编解码	发表刊物/会议
2015	Yao等人(2015)	运动矢量统计分布+预测误差	H.264	MTAP
2014	Zhang等人(2014)	帧间预测模式宏块分块方式	H.264	ACM IH&MMSec'14
2016	Zhang等人(2016a)	运动矢量局部最优性	H.264	MTAP
2016	Zhang等人(2017a)	编码块模式	H.264	IWDW'16
2017	Dong等人(2017)	帧内预测模式调制前后率失真	HEVC	IWDW'17
2018	Dong等人(2019)	帧内预测块中平均每像素的率失真	HEVC	IWDW'18
2018	Nie等人(2018)	帧内预测模式预测误差	H.264	CMC
2018	Zhu和Ni(2018)	运动矢量统计分布+局部最优性	H.264	ICIP'18
2018	Cao等人(2018)	帧内量化DCT系数	H.264	ACM IH&MMSec'18
2018	Wang等人(2018a)	相邻块的帧内预测模式	HEVC	ACM IH&MMSec'18
2019	Xie等人(2019)	环路滤波前后DCT系数差值	VP8	ACM IH&MMSec'19
2020	李林聪等人(2020)	运动矢量联合失真	H.264	电子与信息学报
2021	Chen等人(2021b)	纹理特性+运动属性+帧位置	H.264	TDSC
2021	Chen等人(2021c)	失真漂移	H.264	TDSC

2.3.2 鲁棒视频隐写

为了节省视频流传输带宽和存储空间,社交平台往往会在后台对传输的视频进行二次压缩、转码等有损处理。然而,现有的视频隐写技术通常默认是在无损信道中传输,经过社交网络有损传输后很难提取嵌入的秘密信息。因此,近几年,能抵抗有损信道的鲁棒隐写技术受到热切关注(Chen等,2021b;Zhang等,2021a;Lu等,2021)。鲁棒性主要指有损信道下隐写的容错性。根据应用场景,常见的视频攻击主要为有损压缩、转码、重编码/量化、加噪、滤波、分辨率/帧率转换、丢帧、丢包、旋转、缩放、剪切、插入和修饰等。其中,实现抵抗旋转、缩放、剪切等几何攻击,以及社交平台未知压缩转码的鲁棒性技术难度最大。为提高鲁棒性,目前主要采用纠错码(Tao等,2019;Liu等,2013)、稳健子带(Liu等,2015)和几何不变量(Huan等,2022)等方法。

2.4 音频隐写

国内在音频隐写方面的研究工作目前处于国际领先地位。现有音频隐写研究主要面向可构建隐蔽通信应用的音频和语音压缩参数域隐写。

语音压缩域隐写算法的主要研究团队包括清华大学黄永峰教授、武汉大学任延珍教授、中国科学技术大学黄刘生教授、华侨大学田晖教授和中国科学院声学所李松斌研究员等。目前的主流语音压缩算法基于CELP(code excited linear prediction)编码框架,包括AMR(adaptive multi-rate compression)、G.729、G.723.1、iLBC(Internet low bitrate codec)等,在移动通信网络、互联网络上应用非常广泛,其主要的隐写嵌入域包括线性预测系数LPC(linear predictive coefficient)、基音周期和激励码本参数3类。

线性预测系数LPC体现语音信号产生的声道特性,是语音信号的短时相关性参数。LPC系数的编码通常是对其线性谱频率系数LSF(linear spectral frequency)采用矢量量化进行压缩编码。现有LPC隐写算法通常基于QIM隐写原理,对LSF矢量量化码本进行分组划分,依据需要嵌入的秘密信息选择不同分组码本实现信息隐写。目前各算法的区别主要关注于如何选择分组划分模式,使得隐写所引入的听觉失真和统计失真更小。Xiao等人(2008)针对G.729、G.723.1、iLBC这3种语音编码算法,提出互补邻居节点(complementary neighbor vertices, CNV)算法,对LPC矢量量化码本进行分组划分实

现隐写。Huang等人(2017)基于图模型,采用密钥控制的QIM算法对码本空间进行划分实现隐写,平衡了矢量空间划分的均衡性和多样性,提高了算法的安全性和鲁棒性。Ren等人(2018)针对SILK编码,提出基于LSF码本统计分布特性的安全隐写算法。Sun等人(2021)提出基于LPC参数的分组隐写机制,在保证实时性和不改变音频大小的同时,提升了隐写算法的安全性。

基音周期体现了语音信号产生的声带震动基频特性,通常采用基音预测算法估计获得,该类隐写通常是对基音周期参数微调实现信息隐藏。Wu等人(2003)提出了基于修改语音编码基音周期参数进行信息隐藏的方法。Huang等人(2012)面向G.729,通过对自适应码书进行奇偶分组,调整基音周期闭环搜索过程中自适应码本搜索范围,实现秘密信息的嵌入。Ren等人(2021)利用SILK编码中基音周期参数采用多级矢量量化的特点,基于各阶矢量统计分布特性设计嵌入损失函数,实现基于STC的SILK基音周期安全隐写算法。

激励码本是CELP编码框架中的脉冲激励信号,不同编码算法的激励码本的产生和编码方式不同。如AMR采用固定码本编码,SILK采用随机脉冲激励编码。在CELP类编码数据中,激励码本所占信息位多,而对其修改所带来的语音质量损失小,因此具有非常良好的隐蔽空间。该类隐写方法主要通过修改码本的取值、位置或符号实现隐写。Geiser和Vary(2008)利用AMR固定码本非零脉冲位置选择的随机性,对AMR固定码本非零脉冲位置与嵌入信息之间的映射关系进行控制,实现大容量隐写。Miao等人(2012)面向AMR-WB(videband)标准,修改固定码本的搜索约束条件,选择次优脉冲位置组合实现大容量隐写。Ren等人(2019)基于AMR固定码本的固有分布特性,提出基于掩码调制的固定码本统计分布保持隐写算法,提高了算法的统计安全性。

音频压缩域隐写算法的主要研究团队包括中国科学院信工所的赵险峰研究员、宁波大学的王让定教授等。目前主流的音频压缩算法均基于感知音频编码模型,包括AAC(advanced audio coding)、MP3(moving picture experts group audio layer III)、CELT(constrained energy lapped transform)等。主流音频压缩域隐写方法所修改的主要压缩参数包括比例因

子、量化 MDCT 系数 (quantified modified DCT, QMDCT) 和 Huffman 编码参数 3 类。

QMDCT 系数表示音频帧内各频率成分幅度谱的量化值,是音频压缩数据中的主要参数。微量修改 QMDCT 系数对于音频解码后质量影响较小,该嵌入域具有较大的隐藏容量和听觉隐蔽优势。QMDCT 系数隐写方法与 JPEG 的量化 DCT 系数隐写方法类似,通常包括两类:1) 在编码过程中直接对量化后 MDCT 系数进行修改实现隐写;2) 在 Huffman 编码阶段修改码本实现隐写。第 2 类方法同样修改了 QMDCT 系数,其优点是只需要对压缩码流进行修改,不会产生数据的二次压缩,实时性和隐蔽性更好。Zhang 等人(2020c)考虑隐写的统计安全性,基于 QMDCT 系数相邻帧之间的统计相关性设计失真实现自适应隐写算法 (joint embedding distortion, JED)。Yang 等人(2019b)基于 QMDCT 系数的一阶直方图统计分布特征和人类绝对阈值曲线设计失真代价函数,基于 STC 框架实现 MP3 自适应隐写。在 Huffman 编码域的隐写方法中,严迪群等人(2011)将 Huffman 码表中的码字分为两组,形成码字映射关系。对应的码字在码字空间中根据密钥进行选择,通过码字替换实现隐写。Yang 等人(2017)提出了一种基于等长熵编码的自适应隐写算法 (equal length entropy codes substitution, EECS),利用人类听觉绝对阈值曲线设计失真代价函数,基于 STC 实现自适应安全隐写。Yi 等人(2019)提出基于 Huffman 码字帧块失真优选的自适应隐写框架算法 (adaptive Huffman code mapping, AHCM)。将 Huffman 码表中的码字分组策略从一一对应改为一组内有多个相互替换码字的策略,构造了多个码字动态映射的关系来实现隐写。

目前基于深度学习的音频隐写算法 (Jiang 等, 2020; Wu 等, 2020) 和面向 VoIP 语音流的隐写算法 (Tian 等, 2017) 也已经成为现在音频隐写的关注方向。Chen 等人(2021a)设计了基于文本合成语音的可证安全隐写算法。

2.5 文本隐写

如前文所述,国内的现代文本隐写术通常可以分为基于文本格式的隐写术和基于文本内容的隐写术。在基于文本格式的隐写术研究中,有研究人员利用 PDF 文档中的闲置空间进行填充 (Wojtuń 和 Piotrowski, 2021)、对文档的定位操作符进行细微修

改 (钟征燕 等, 2012) 以及增删文档中的对象树信息 (Zhong 等, 2007) 等实现隐蔽信息嵌入。这类方法的使用场景具有较强的局限性。

近年来的国内研究热点主要集中于基于文本内容的隐写术,该技术通常可以归纳为检索式、修改式和生成式 3 种隐写策略。其中检索式语言隐写术国内比较有代表性的方法是南京信息工程大学的周志立等人 (Lee 和 Tsai, 2010) 提出的基于多个关键词的无载体文本隐写方法,他们通过对大规模文本库中的样本进行特殊编码,然后根据待嵌入的秘密信息选择对应语句进行传输以实现隐蔽通信。修改式语言隐写术主要是对文本中词汇级或者句子级的语义单元进行同义替换以嵌入隐蔽信息。例如对于词级同义变换,可以通过构建同义词典,然后对同义词典进行适当编码,根据待嵌入秘密信息选择特定的同义词对原始文本进行替换以嵌入信息 (Zhou 等, 2016)。对于句级同义变换,可以通过对句法结构进行等价变换以代表不同的隐蔽信息 (Liu 等, 2005)。修改式和检索式文本隐写方法都面临着嵌入率比较低而难以传递大量信息的缺点。

生成式语言隐写术是近年来国内的研究热点,吸引了大量研究人员,该类方法的优势之一就是嵌入率高。Luo 等人(2016)结合句法模板和统计语言模型以生成特定格式下的隐写文本。Yang 等人(2019c)提出基于条件概率编码 (Conproc) 的载体生成式隐写模型 RNN-Stega,该方法能大幅度提升生成的隐写文本的感知隐蔽性和信息嵌入率,相比之前主流的基于修改式的语言隐写术只有 1%—3% 左右的嵌入率, RNN-Stega 模型的嵌入率最高可达到 20% 以上。Yang 等人(2021)实验结果表明, Conproc 框架生成的隐写文本表现出显著的感知—统计隐蔽性冲突效应 (psic effect)。为了解决这一问题, Zhou 等人(2021)引入对抗学习机制,通过对抗训练约束正常文本和生成的隐写文本之间的统计分布差异, Zhang 等人(2021c)提出名为 ADG (adaptive dynamic grouping) 的可证安全生成式文本隐写方法,该方法采用分组划分策略构建秘密信息和词表映射的隐写思路。这些最新的研究进展在保证生成的隐写文本具有一定感知隐蔽性的基础上,大幅度增强了其统计隐蔽性。考虑到语义隐蔽性, Yang 等人(2018)提出应用在对话系统中的 RITS (real-time interactive text steganography) 模型,并利用强化

学习约束生成文本和上下文之间的语义关联性,首次尝试约束生成隐写文本语义表达。Li 等人(2019)在 image caption 任务中,利用给定的图像约束生成的隐写文本的语义表达。2020 年,Yang 等人(2021)基于 encoder-decoder 框架实现语义可控的隐写文本自动生成方法。然而,基于 encoder-decoder 中解码嵌入技术路线的文本生成式隐写方法在提高嵌入率时,会带来隐写文本质量和语义控制能力的双双下降。考虑到这一缺陷,Yang 等人(2020c)提出基于编码端的知识图谱引导下的语义可控隐写文本生成方法,即 Graph-Stega 模型。该方法将秘密信息嵌入到知识图谱的路径表达中。这些工作均在一定程度上实现了嵌入秘密信息的同时控制生成的隐写文本的语义表达、增强了生成式语言隐写术的安全性。

3 国内外研究进展比较

3.1 隐写编码

早期的隐写编码一直由国外研究学者主导,尤其是在常数代价隐写模型编码阶段,美国纽约大学宾汉姆分校的 Fridrich 团队引领着隐写编码的发展。中国科学技术大学张卫明团队提出 ZZW 编码,使以矩阵编码为基础的隐写编码的性能进一步逼近理论界。复旦大学张新鹏团队提出了首个非二元的隐写编码 EMD,后续国外学者在其基础上继续发展非二元编码方法。在多级代价模型阶段,Filler 提出的 STC 提供了一种逼近嵌入效率理论上界的自适应隐写码方案,实际上已经成为隐写编码标准,得到广泛使用。长期以来自适应隐写码仅有 STC 单一选项。已有研究指出 STC 具有潜在瑕疵(Köhler 等,2017),因此设计一种可替代 STC 的隐写码方案对于保证隐写算法的安全性和扩充隐写码的多样性具有重要意义。中国科学技术大学张卫明团队在 2020 年将极化码改造成隐写码 SPC,可以逼近多级代价模型的理论界,且理论复杂度低于 STC。回顾 20 年隐写编码的发展过程,可以看出隐写编码从国外提出,到国内跟进,现在逐渐进入并驾齐驱的状态。

3.2 图像隐写

从上述国内外研究工作可知,近年来中国在图像隐写方面研究呈现蓬勃发展之势。在前沿研究方

向上,有两个明显优势。1)将深度学习方法与隐写结合。国内学者率先提出了基于生成对抗网络及基于强化学习的隐写代价生成方法,使得隐写失真代价不再依赖于统计模型或基于启发式的设计,利用隐写与隐写分析的博弈及数据驱动进行隐写代价的学习。国内学者也提出了多种利用对抗样本技术应对日益强大的深度学习隐写分析器的挑战,同时确保了对抗样本的对抗成功率与载密信息的提取成功率。2)鲁棒隐写方法。国内学者从各个角度提出了应对社交媒体、日常图像处理中所面临的重压缩、重采样等引起的秘密信息误码提取问题,对隐藏信息的容量、安全性和鲁棒性三者关系进行了探索,发展深化了隐写的实用性。与国外的研究相比,国内在大规模公共评测数据库的建立、基于统计模型的隐写研究和隐写安全性的理论探讨等方面还有待加强研究力量。这些方面不仅有望获得具有影响力的突破性成果,还将有助于隐写学科内涵和外延的发展,达到载体统计模型和安全模型的和谐统一。

3.3 视频隐写

随着多媒体技术的发展和 5G 时代的到来,视频将逐步取代图像成为主流的数字媒介。因此,国内外对视频隐写技术的研究也明显呈上升趋势,涌现了大量的视频隐写方法。总的来说,相较于国外,目前国内在视频隐写领域的研究成果更加丰硕。然而,国内在该领域的研究大多致力于如何提高视频隐写的嵌入效率和安全性,因此,现有方法主要涉及压缩域视频隐写,以及基于失真代价的自适应视频隐写。近期随着社交网络的发展,很多国内学者对鲁棒视频隐写方法开始关注。与此同时,随着人工智能的发展,国外一些知名大公司和研究机构(如谷歌、MIT)已开始研究基于深度学习的视频隐写技术,并着手设计基于深度神经网络的端到端视频隐写架构。虽然国内也有少量的研究工作将深度学习引入到视频隐写技术领域,但缺乏对端到端视频隐写架构的设计,如 Liu 等人(2021)提出的方法是用 CNN 替换视频 I 帧的环路滤波器,以便更好地改善压缩后图像的重建质量,所以该方法实际上是用 CNN 替代视频编码中的一个“部件”。目前,基于深度学习的视频隐写技术研究处于起步阶段,主要旨在实现智能的端到端视频隐写,具有很好的愿景,但由于视频数据量大而难于训练大量高清视频,因此,其实用性还有待进一步探索。

3.4 音频隐写

从目前对国内外音频隐写技术的公开学术研究成果的分析看,国内学者的研究处于国际领先地位,尤其是对各类主流语音和音频编码算法的压缩参数域隐写方面,从所覆盖的音频压缩算法的广度和隐写载体嵌入域的特性分析和安全性提升方面具有更好的实际应用价值。在基于 VoIP 等音频流隐写的技术公开成果发表方面,国内相对成果较少。因此,国内的后期研究可以更多地从应用的角度,充分挖掘和分析现有语音信号存储和传输空间特性,寻找和发现可利用的数据载体,实现高效安全的隐蔽通信应用。

3.5 文本隐写

文本隐写术长期以来由于其难以实现高嵌入率隐写,导致其受到的关注度较低。即便如此,国内学者经过多年耕耘,在文本隐写多个方面始终保持领先地位。例如南京信息工程大学的孙星明团队、湖南大学的刘玉玲团队、长沙理工大学的向凌云团队等在文本检索式隐写和文本修改式隐写方面长期处于国际领先。随着近两年自然语言处理技术的飞速发展,基于生成策略的语言隐写术成为文本隐写领域的热点研究方向,吸引了大量国内外研究人员的兴趣。在这一最新研究热点上,国内学者例如清华大学黄永峰团队、中国农业大学的薛一鸣团队等保持对国外的领先地位。文本生成式隐写面临的挑战难题可总结为感知隐蔽性、统计隐蔽性和认知隐蔽性。目前感知隐蔽性和统计隐蔽性方面均有了较好的解决方案,但是在认知隐蔽性上还亟待突破。因此,国内研究团队接下来的研究需要着眼于认知隐蔽性增强,重点研究语义、主题、风格和情感等因素可控的生成式文本隐写,以进一步增强生成式隐写术的隐蔽性和安全性。

4 发展趋势与展望

4.1 隐写编码

对隐写码的已有研究表明,隐写码与纠错码存在对偶关系,即纠错码的译码算法对应于隐写码的编码算法。从简单的常数代价模型到复杂的多级代价模型,从基于分组汉明码的 F5 到基于卷积码的 STC,这揭示了设计更优隐写码可通过选取更为优越的纠错码及其译码算法。STC 和 SPC 算法可逼

近隐写理论界得益于卷积码和极化码的优良性能。但是适用于多级代价模型的隐写码依然太少。未来可以考虑将其他优秀的纠错码,如 Turbo 码、LDPC (low-density parity-check code) 码等,改造为隐写码。同时,随着数据和场景的变化,发展更高效和更安全的生成式隐写编码也是值得研究的方向。

4.2 图像隐写

图像隐写的研究应在理论和应用两个维度协同发展,主要体现在 3 个方面。1) 提高隐写安全性。应对不断发展的深度学习和特征工程的隐写分析挑战,结合载体生成、载体选择和载体边信息利用等方式,设计更为安全有效的隐写方法。2) 提高效率。针对移动互联网等应用,设计高效快速的隐写代价生成及隐写编解码方法。3) 提高鲁棒性。针对各类社交平台,设计抗各类后处理的鲁棒隐写方法。

4.3 视频隐写

视频具有信息量大、视觉表现强和实时性高等优势,广泛应用于视频会议、社交平台、可视电话和网络直播等场景,未来可结合实际应用进行广泛地探索研究。比如,目前社交网络中广泛应用的短视频成为当今互联网中媒介传播的主力军,因此,短视频隐写有着重要的研究价值。其中,抵抗短视频平台转码的鲁棒性,以及短视频持续时间较短所带来的嵌入容量限制是需要考虑的技术难点。此外,基于新一代视频编码标准的隐写技术研究将会越来越多,将深度学习引入视频隐写技术进行端到端架构的设计或优化,依然受到关注。

4.4 音频隐写

数字音频是优质的隐写载体,在各种社交应用中存在大量的隐蔽通信信道。从目前本领域国际国内研究成果的分析,未来音频隐写技术的研究将会面向实际应用,以构建隐蔽通信为目标,提升隐写算法和隐写行为的安全性,实现适用于现有音频通信环境的安全鲁棒隐写算法。研究成果可以应用于个人、企业、政府及国家安全领域,实现重要信息在开放互联网络环境下的安全通信。

4.5 文本隐写

总的来说,现有的文本隐写术已经可以生成具有较高感知隐蔽性的隐写文本。在统计隐蔽性方面,最新的研究工作能够做到可证安全。在认知隐蔽性方面,目前虽然已经有一定的进展,但是离该挑战难题的最终解决还有一段距离。

此外, 现有的文本隐写术基本都可以归纳为符号隐写, 即通过对自然语言中的符号进行编码实现隐蔽信息嵌入, 然而文本符号的离散性导致符号隐写将很可能破坏文本语义表达的完整性。而基于隐空间编码的文本隐写思路, 如 Zhang 等人 (2021b) 提出的方法, 一方面能抵抗当前基于符号统计分析的文本隐写检测方法; 另一方面也能与现有符号隐写方法进行结合, 以进一步提升其隐藏容量, 这类方法或许是未来文本隐写术非常有价值的研究方向。

致谢 本文由中国图象图形学学会数字媒体取证与安全专委会组织撰写, 该专委会更多详情请见链接: <http://www.csig.org.cn/detail/2450>。

参考文献 (References)

- AlSabhan A A, Ali A H, Ridzuan F, Azni A H and Mokhtar M R. 2020. Digital audio steganography: systematic review, classification, and analysis of the current state of the art. *Computer Science Review*, 38: #100316 [DOI: 10.1016/j.cosrev.2020.100316]
- Aly H A. 2011. Data hiding in motion vectors of compressed video based on their associated prediction error. *IEEE Transactions on Information Forensics and Security*, 6(1): 14-18 [DOI: 10.1109/TIFS.2010.2090520]
- Banjarnahor J, Siregar S D, Sihombing O, Turnip M, Purba W, Aisyah S and Banjarnahor J. 2019. Audio steganography applications using auditory features watermarking. *Journal of Physics: Conference Series*, 1230: #012073 [DOI: 10.1088/1742-6596/1230/1/012073]
- Bas P. 2017. An embedding mechanism for natural steganography after down-sampling//*Proceedings of 2017 IEEE International Conference on Acoustics, Speech and Signal Processing*. New Orleans, USA: IEEE: 2127-2131 [DOI: 10.1109/ICASSP.2017.7952532]
- Bernard S, Bas P, Klein J and Pevny T. 2021a. Explicit optimization of min max steganographic game. *IEEE Transactions on Information Forensics and Security*, 16: 812-823 [DOI: 10.1109/TIFS.2020.3021913]
- Bernard S, Bas P, Pevny T and Klein J. 2021b. Optimizing additive approximations of non-additive distortion functions//*Proceedings of 2021 ACM Workshop on Information Hiding and Multimedia Security*. New York, USA: ACM: 105-112 [DOI: 10.1145/3437880.3460407]
- Bernard S, Pevny T, Bas P and Klein J. 2019. Exploiting adversarial embeddings for better steganography//*Proceedings of ACM Workshop on Information Hiding and Multimedia Security*. Paris, France: ACM: 216-221 [DOI: 10.1145/3335203.3335737]
- Bierbrauer J and Fridrich J. 2008. Constructing good covering codes for applications in steganography//Shi Y Q, ed. *Transactions on Data Hiding and Multimedia Security III*. Berlin, Germany: Springer: 1-22 [DOI: 10.1007/978-3-540-69019-1_1]
- Boroumand M and Fridrich J. 2020. Synchronizing embedding changes in side-informed steganography//*Proceedings of Electronic Imaging: Media Watermarking, Security, and Forensics*. Springfield: Society for Imaging Science and Technology: 290-1-290-12 [DOI: 10.2352/ISSN.2470-1173.2020.4.MWSF-290]
- Butora J and Fridrich J. 2020a. Steganography and its detection in JPEG images obtained with the "TRUNC" quantizer//*Proceedings of 2020 IEEE International Conference on Acoustics, Speech and Signal Processing*. Barcelona, Spain: IEEE: 2762-2766 [DOI: 10.1109/ICASSP40776.2020.9053696]
- Butora J and Fridrich J. 2020b. Minimum perturbation cost modulation for side-informed steganography//*Proceedings of Electronic Imaging: Media Watermarking, Security, and Forensics*. Springfield, USA: Society for Imaging Science and Technology: #289 [DOI: 10.2352/ISSN.2470-1173.2020.4.MWSF-289]
- Butora J, Yousfi Y and Fridrich J. 2020. Turning cost-based steganography into model-based//*Proceedings of 2020 ACM Workshop on Information Hiding and Multimedia Security*. Denver, USA: ACM: 151-159 [DOI: 10.1145/3369412.3395065]
- Cao Y, Wang Y, Zhao X F, Zhu M N and Xu Z J. 2018. Cover block decoupling for content-adaptive H. 264 steganography//*Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security*. Innsbruck, Austria: ACM: 23-30 [DOI: 10.1145/3206004.3206014]
- Cetin O and Ozcerit T. 2009. A new steganography algorithm based on color histograms for data embedding into raw video streams. *Computers and Security*, 28(7): 670-682 [DOI: 10.1016/j.cose.2009.04.002]
- Chang C Y and Clark S. 2010. Linguistic steganography using automatically generated paraphrases//*Proceedings of Human Language Technologies: The 2010 Annual Conference of the North American Chapter of the Association for Computational Linguistics*. Los Angeles, USA: Association for Computational Linguistics: 2010: 591-599
- Chen K J, Zhou H, Zhao H Q, Chen D D, Zhang W M and Yu N H. 2021a. Distribution-preserving steganography based on text-to-speech generative models. *IEEE Transactions on Dependable and Secure Computing*, 14(4): 1052-1066 [DOI: 10.1109/TDSC.2021.3095072]
- Chen K J, Zhou H, Zhou W B, Zhang W M and Yu N H. 2019. Defining cost functions for adaptive JPEG steganography at the microscale. *IEEE Transactions on Information Forensics and Security*, 14(4): 1052-1066 [DOI: 10.1109/TIFS.2018.2869353]
- Chen Y, Wang H X, Choo K K R, He P S, Salcic Z, Kaafar D A and Zhang X Y. 2021c. DDCA: a distortion drift-based cost assignment method for adaptive video steganography in the transform domain. [J/OL]. *IEEE Transactions on Dependable and Secure Computing*,

- <https://ieeexplore.ieee.org/document/9351637> [DOI: 10.1109/TDSC.2021.3058134]
- Chen Y L, Wang H X, Wu H Z, Wu Z Q, Li T and Malik A. 2021b. Adaptive video data hiding through cost assignment and STCs. *IEEE Transactions on Dependable and Secure Computing*, 18(3): 1320-1335 [DOI: 10.1109/TDSC.2019.2932983]
- Cogranne R, Giboulot Q and Bas P. 2020. Steganography by minimizing statistical detectability: the cases of JPEG and color images//*Proceedings of 2020 ACM Workshop on Information Hiding and Multimedia Security*. Denver, USA; ACM: 161-167 [DOI: 10.1145/3369412.3395075]
- Crandall R. 1998. Some notes on steganography. Posted on steganography mailing list, 1-6
- Denemark T, Bas P and Fridrich J. 2018. Natural steganography in JPEG compressed images//*Proceedings of Electronic Imaging: Media Watermarking, Security, and Forensics*. [s.l.]: Society for Imaging Science and Technology: #316 [DOI: 10.2352/ISSN.2470-1173.2018.07.MWSF-316]
- Denemark T and Fridrich J. 2017a. Model based steganography with pre-cover//*Proceedings of Electronic Imaging: Media Watermarking, Security, and Forensics*. [s.l.]: Society for Imaging Science and Technology: 56-66 [DOI: 10.2352/ISSN.2470-1173.2017.7.MWSF-326]
- Denemark T and Fridrich J. 2017b. Steganography with two JPEGs of the same scene//*Proceedings of 2017 IEEE International Conference on Acoustics, Speech and Signal Processing*. New Orleans, USA; IEEE: 2117-2121 [DOI: 10.1109/ICASSP.2017.7952530]
- Denemark T and Fridrich J. 2017c. Steganography with multiple JPEG images of the same scene. *IEEE Transactions on Information Forensics and Security*, 12(10): 2308-2319 [DOI: 10.1109/TIFS.2017.2705625]
- Diouf B, Diop I, Keita K W, Diouf M, Farsi S M, Tall K and Khouma O. 2018. Polar coding steganographic embedding using successive cancellation//*Proceedings of the 1st International Conference, InterSol 2017 and Sixth Colloque National sur la Recherche en Informatique et ses Applications*. Dakar, Senegal; Springer: 189-201 [DOI: 10.1007/978-3-319-72965-7_18]
- Dong Y, Jiang X H, Sun T F and Xu D W. 2017. Coding efficiency preserving steganography based on HEVC steganographic channel model//*Proceedings of the 16th International Workshop on Digital Watermarking*. Magdeburg, Germany; Springer: 149-162 [DOI: 10.1007/978-3-319-64185-0_12]
- Dong Y, Sun T F and Jiang X H. 2019. A high capacity HEVC steganographic algorithm using intra prediction modes in multi-sized prediction blocks//*Proceedings of the 17th International Workshop on Digital Watermarking*. Jeju Island, Korea (South): Springer: 233-247 [DOI: 10.1007/978-3-030-11389-6_18]
- Dutta H, Das R K, Nandi S, Nandi S and Prasanna S R M. 2020. An overview of digital audio steganography. *IETE Technical Review*, 37(6): 632-650 [DOI: 10.1080/02564602.2019.1699454]
- Feng B W, Liu Z Q, Wu X T and Lin Y C. 2020. Robust syndrome-trellis codes for fault-tolerant steganography//*Proceedings of the 3rd International Conference on Security with Intelligent Computing and Big-data Services*. New Taipei City, China; Springer: 115-127 [DOI: 10.1007/978-3-030-46828-6_11]
- Filler T and Fridrich J. 2009. Wet ZZW construction for steganography//*Proceedings of the 1st IEEE International Workshop on Information Forensics and Security*. London, UK; IEEE: 131-135 [DOI: 10.1109/WIFS.2009.5386467]
- Filler T, Judas J and Fridrich J. 2011. Minimizing additive distortion in steganography using syndrome-trellis codes. *IEEE Transactions on Information Forensics and Security*, 6(3): 920-935 [DOI: 10.1109/TIFS.2011.2134094]
- Fridrich J and Filler T. 2007. Practical methods for minimizing embedding impact in steganography//*Proceedings of SPIE 6505, Steganography, and Watermarking of Multimedia Contents IX*. San Jose, USA; SPIE: #650502 [DOI: 10.1117/12.697471]
- Fridrich J, Goljan M, Lisonek P and Soukal D. 2005b. Writing on wet paper. *IEEE Transactions on Signal Processing*, 53(10): 3923-3935 [DOI: 10.1109/TSP.2005.855393]
- Fridrich J, Goljan M and Soukal D. 2005a. Efficient wet paper codes//*Proceedings of the 7th International Workshop on Information Hiding*. Barcelona, Spain; Springer: 204-218 [DOI: 10.1007/11558859_16]
- Fridrich J, Goljan M and Soukal D. 2006. Wet paper codes with improved embedding efficiency. *IEEE Transactions on Information Forensics and Security*, 1(1): 102-110 [DOI: 10.1109/TIFS.2005.863487]
- Fridrich J and Lisonek P. 2007. Grid colorings in steganography. *IEEE Transactions on Information Theory*, 53(4): 1547-1549 [DOI: 10.1109/TIT.2007.892768]
- Fridrich J and Soukal D. 2006. Matrix embedding for large payloads. *IEEE Transactions on Information Forensics and Security*, 1(3): 390-395 [DOI: 10.1109/TIFS.2006.879281]
- Galand F and Kabatiansky G. 2003. Information hiding by coverings//*Proceedings of 2003 IEEE Information Theory Workshop*. Paris, France; IEEE: 151-154 [DOI: 10.1109/ITW.2003.1216717]
- Geiser B and Vary P. 2008. High rate data hiding in ACELP speech codecs//*Proceedings of 2008 IEEE International Conference on Acoustics, Speech and Signal Processing*. Las Vegas, USA; IEEE: 4005-4008 [DOI: 10.1109/ICASSP.2008.4518532]
- Giboulot Q, Bas P and Cogranne R. 2020b. Synchronization minimizing statistical detectability for side-informed JPEG steganography//*Proceedings of 2020 IEEE International Workshop on Information Forensics and Security*. New York, USA; IEEE: 1-6 [DOI: 10.1109/WIFS49906.2020.9360884]
- Giboulot Q, Cogranne R and Bas P. 2020a. JPEG steganography with side information from the processing pipeline//*Proceedings of 2020*

- IEEE International Conference on Acoustics, Speech and Signal Processing. Barcelona, Spain; IEEE: 2767-2771 [DOI: 10.1109/ICASSP40776.2020.9054486]
- Giboulot Q, Cogranne R and Bas P. 2021. Detectability-based JPEG steganography modeling the processing pipeline: the noise-content trade-off. *IEEE Transactions on Information Forensics and Security*, 16: 2202-2217 [DOI: 10.1109/TIFS.2021.3050063]
- Hu X L, Ni J Q and Shi Y Q. 2018a. Efficient JPEG steganography using domain transformation of embedding entropy. *IEEE Signal Processing Letters*, 25(6): 773-777 [DOI: 10.1109/LSP.2018.2818674]
- Hu X L, Ni J Q, Su W K and Huang J W. 2018b. Model-based image steganography using asymmetric embedding scheme. *Journal of Electronic Imaging*, 27(4): #043023 [DOI: 10.1117/1.JEI.27.4.043023]
- Huan W N, Li S, Qian Z X and Zhang X P. 2022. Exploring stable coefficients on joint sub-bands for robust video watermarking in DT CWT domain. *IEEE Transactions on Circuits and Systems for Video Technology*, 32(4): 1955-1965 [DOI: 10.1109/TCSVT.2021.3092004]
- Huang Y F, Liu C H, Tang S Y and Bai S. 2012. Steganography integration into a low-bit rate speech codec. *IEEE Transactions on Information Forensics and Security*, 7(6): 1865-1875 [DOI: 10.1109/TIFS.2012.2218599]
- Huang Y F, Tao H Z, Xiao B and Chang C C. 2017. Steganography in low bit-rate speech streams based on quantization index modulation controlled by keys. *Science China Technological Sciences*, 60(10): 1585-1596 [DOI: 10.1007/s11431-016-0707-3]
- Jamil T. 1999. Steganography: the art of hiding information in plain sight. *IEEE Potentials*, 18(1): 10-12 [DOI: 10.1109/45.747237]
- Jiang S Z, Ye D P, Huang J Q, Shang Y Y and Zheng Z Y. 2020. SmartSteganography: light-weight generative audio steganography model for smart embedding application. *Journal of Network and Computer Applications*, 165: #102689 [DOI: 10.1016/j.jnca.2020.102689]
- Kapotas S K and Skodras A N. 2008. A new data hiding scheme for scene change detection in H.264 encoded video sequences//Proceedings of 2008 IEEE International Conference on Multimedia and Expo. Hannover, Germany; IEEE: 277-280 [DOI: 10.1109/ICME.2008.4607425]
- Kheddar H, Bouzid M and Megías D. 2019. Pitch and Fourier magnitude based steganography for hiding 2.4 kbps MELP bitstream. *IET Signal Processing*, 13(3): 396-407 [DOI: 10.1049/iet-spr.2018.5339]
- Kim Y, Duric Z and Richards D. 2007. Modified matrix encoding technique for minimal distortion steganography//Proceedings of the 8th International Workshop on Information Hiding. Alexandria, USA; Springer: 314-327 [DOI: 10.1007/978-3-540-74124-4_21]
- Kin-Cleaves C and Ker A D. 2018. Adaptive steganography in the noisy channel with dual-syndrome trellis codes//Proceedings of 2018 IEEE International Workshop on Information Forensics and Security. Hong Kong, China; IEEE: 1-7 [DOI: 10.1109/WIFS.2018.8630779]
- Köhler O M, Pasquini C and Böhme R. 2017. On the statistical properties of syndrome trellis coding//Proceedings of the 16th International Workshop on Digital Watermarking. Magdeburg, Germany; Springer: 331-346 [DOI: 10.1007/978-3-319-64185-0_25]
- Kohls K, Holz T, Kolossa D and Pöpper C. 2016. SkypeLine: robust hidden data transmission for VoIP//Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. Xi'an, China; ACM: 877-888 [DOI: 10.1145/2897845.2897913]
- Lee I S and Tsai W H. 2010. A new approach to covert communication via PDF files. *Signal Processing*, 90(2): 557-565 [DOI: 10.1016/j.sigpro.2009.07.022]
- Li L C, Yao Y Z, Zhang X Y, Zhang W M and Yu N H. 2020. Video steganography based on modification probability transformation and non-additive embedding distortion. *Journal of Electronics and Information Technology*, 42(10): 2357-2364 (李林聪, 姚远志, 张晓雅, 张卫明, 俞能海. 2020. 基于修改概率转换和非加性嵌入失真的视频隐写方法. *电子与信息学报*, 42(10): 2357-2364) [DOI: 10.11999/JEIT200001]
- Li M D, Mu K, Zhong P, Wen J and Xue Y M. 2019. Generating steganographic image description by dynamic synonym substitution. *Signal Processing*, 164: 193-201 [DOI: 10.1016/j.sigpro.2019.06.014]
- Li S B, Wang L R, Liu P and Huang Y F. 2016. A HEVC information hiding approach based on motion vector space encoding. *Chinese Journal of Computers*, 39(7): 1450-1463 (李松斌, 王凌睿, 刘鹏, 黄永峰. 2016. 一种基于运动矢量空间编码的 HEVC 信息隐藏方法. *计算机学报*, 39(7): 1450-1463) [DOI: 10.11897/SP.J.1016.2016.01450]
- Li W X, Chen K J, Zhang W M, Zhou H, Wang Y F and Yu N H. 2020a. JPEG steganography with estimated side-information. *IEEE Transactions on Circuits and Systems for Video Technology*, 30(7): 2288-2294 [DOI: 10.1109/TCSVT.2019.2925118]
- Li W X, Zhang W M, Chen K J, Zhou W B and Yu N H. 2018. Defining joint distortion for JPEG steganography//Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security. Innsbruck, Austria; ACM: 5-16 [DOI: 10.1145/3206004.3206008]
- Li W X, Zhang W M, Li L, Zhou H and Yu N H. 2020b. Designing near-optimal steganographic codes in practice based on polar codes. *IEEE Transactions on Communications*, 68(7): 3948-3962 [DOI: 10.1109/TCOMM.2020.2982624]
- Li Y and Wang H X. 2019. Robust H.264/AVC video watermarking without intra distortion drift. *Multimedia Tools and Applications*, 78(7): 8535-8557 [DOI: 10.1007/s11042-018-6942-0]

- Liao X, Yu Y B, Li B, Li Z P and Qin Z. 2020. A new payload partition strategy in color image steganography. *IEEE Transactions on Circuits and Systems for Video Technology*, 30 (3): 685-696 [DOI: 10.1109/TCSVT.2019.2896270]
- Liu J D, Li Z H, Jiang X H and Zhang Z Z. 2021. A high-performance CNN-applied HEVC steganography based on diamond-coded PU partition modes. *IEEE Transactions on Multimedia*; #3075858 [DOI: 10.1109/TMM.2021.3075858]
- Liu Y J, Sun X M and Luo G. 2006. A novel information hiding algorithm based on structure of PDF document. *Computer Engineering*, 32(17): 230-232 (刘友继, 孙星明, 罗纲. 2006. 一种新的基于PDF文档结构的信息隐藏算法. *计算机工程*, 32(17): 230-232) [DOI: 10.3969/j.issn.1000-3428.2006.17.081]
- Liu Y L, Sun X M and Wu Y. 2005. A natural language watermarking based on Chinese syntax//*Proceedings of the 1st International Conference on Natural Computation*. Changsha, China: Springer: 958-961 [DOI: 10.1007/11539902_119]
- Liu Y X, Hu M S, Ma X J and Zhao H G. 2015. A new robust data hiding method for H. 264/AVC without Intra-frame distortion drift. *Neurocomputing*, 151(3): 1076-1085 [DOI: 10.1016/j.neucom.2014.03.089]
- Liu Y X, Li Z T, Ma X J and Liu J. 2013. A robust data hiding algorithm for H. 264/AVC video streams. *Journal of Systems and Software*, 86(8): 2174-2183 [DOI: 10.1016/j.jss.2013.03.101]
- Lu W, Zhang J H, Zhao X F, Zhang W M and Huang J W. 2021. Secure robust JPEG Steganography based on autoencoder with adaptive BCH encoding. *IEEE Transactions on Circuits and Systems for Video Technology*, 31(7): 2909-2922 [DOI: 10.1109/TCSVT.2020.3027843]
- Lu Y B, Zhai L M and Wang L N. 2020. Designing non-additive distortions for JPEG steganography based on blocking artifacts reduction//*Proceedings of the 18th International Workshop on Digital Watermarking*. Chengdu, China: Springer: 268-280 [DOI: 10.1007/978-3-030-43575-2_23]
- Luo X Y, Li Y X, Chang H W, Liu C, Milanfar P and Yang F. 2021. DVMark: a deep multiscale framework for video watermarking [EB/OL]. [2021-11-30]. <https://arxiv.org/pdf/2104.12734.pdf>
- Luo Y B, Huang Y F, Li F F and Chang C C. 2016. Text steganography based on Ci-poetry generation using Markov chain model. *KSII Transactions on Internet and Information Systems*, 10(9): 4568-4584 [DOI: 10.3837/tiis.2016.09.029]
- Ma S, Zhao X F and Liu Y Q. 2019. Adaptive spatial steganography based on adversarial examples. *Multimedia Tools and Applications*, 78(22): 32503-32522 [DOI: 10.1007/s11042-019-07994-3]
- Ma X J, Li Z T, Tu H and Zhang B C. 2010. A data hiding algorithm for H. 264/AVC video streams without intra-frame distortion drift. *IEEE Transactions on Circuits and Systems for Video Technology*, 20(10): 1320-1330 [DOI: 10.1109/TCSVT.2010.2070950]
- Mazurczyk W, Karaś M, Szczypiorski K and Janicki A. 2016. YouSkyde; information hiding for Skype video traffic. *Multimedia Tools and Applications*, 75(21): 13521-13540 [DOI: 10.1007/s11042-015-2740-0]
- Mazurczyk W and Szczypiorski K. 2008. Steganography of VoIP streams//*Proceedings of OTM Confederated International Conferences On the Move to Meaningful Internet Systems*. Berlin, Heidelberg: Springer: 1001-1018
- Miao H B, Huang L S, Chen Z L, Yang W and Al-hawbani A. 2012. A new scheme for covert communication via 3G encoded speech. *Computers and Electrical Engineering*, 38(6): 1490-1501 [DOI: 10.1016/j.compeleceng.2012.05.003]
- Mielikainen J. 2006. LSB matching revisited. *IEEE Signal Processing Letters*, 13(5): 285-287 [DOI: 10.1109/LSP.2006.870357]
- Mo H X, Song T T, Chen B L, Luo W Q and Huang J W. 2019. Enhancing JPEG steganography using iterative adversarial examples//*Proceedings of 2019 IEEE International Workshop on Information Forensics and Security*. Delft, the Netherlands: IEEE: 1-6 [DOI: 10.1109/WIFS47025.2019.9035101]
- Mo X B, Tan S Q, Li B and Huang J W. 2021. MCTSteg; a Monte Carlo tree search-based reinforcement learning framework for universal non-additive steganography. *IEEE Transactions on Information Forensics and Security*, 16: 4306-4320 [DOI: 10.1109/TIFS.2021.3104140]
- Muñoz A, Gallardo J C and Álvarez I A. 2010. Improving N-Gram linguistic steganography based on templates//*Proceedings of 2010 International Conference on Security and Cryptography*. Athens, Greece: IEEE: 1-4
- Munuera C. 2007. Steganography and error-correcting codes. *Signal Processing*, 87(6): 1528-1533 [DOI: 10.1016/j.sigpro.2006.12.008]
- Mustafayeva E, Huseynova G and Gasimov V. 2019. Implementing covert channels to transfer hidden information over whatsapp on mobile phones. *International Journal of Engineering and Applied Sciences (IJEAS)*, 6(2): 32-35
- Nakajima T V and Ker A D. 2020. The syndrome-trellis sampler for generative steganography//*Proceedings of 2020 IEEE International Workshop on Information Forensics and Security*. New York, USA: IEEE: 1-6 [DOI: 10.1109/WIFS49906.2020.9360885]
- Nie Q K, Xu X B, Feng B W and Zhang L Y. 2018. Defining embedding distortion for intra prediction mode-based video steganography. *Computers, Materials and Continua*, 55(1): 59-70 [DOI: 10.3970/cmc.2018.055.059]
- Pal D, Goswami A, Chowdhury S and Ghoshal N. 2021. A novel high-density multilayered audio steganography technique in hybrid domain//*Bhattacharjee D, Kole D K, Dey N, Basu S and Plewczynski D, eds. Proceedings of International Conference on Frontiers in Computing and Systems*. Singapore, Singapore: Springer: 721-730 [DOI: 10.1007/978-981-15-7834-2]

- Qiao T, Wang S, Luo X Y and Zhu Z Q. 2021. Robust steganography resisting JPEG compression by improving selection of cover element. *Signal Processing*, 183: #108048 [DOI: 10.1016/j.sigpro.2021.108048]
- Qin X H, Li B and Huang J W. 2019. A new spatial steganographic scheme by modeling image residuals with multivariate Gaussian model//*Proceedings of 2019 IEEE International Conference on Acoustics, Speech and Signal Processing*. Brighton, UK: IEEE: 2617-2621 [DOI: 10.1109/ICASSP.2019.8682688]
- Qin X H, Tan S Q, Tang W X, Li B and Huang J W. 2021. Image steganography based on iterative adversarial perturbations onto a synchronized-directions sub-image//*Proceedings of 2021 IEEE International Conference on Acoustics, Speech and Signal Processing*. Toronto, Canada: IEEE: 2705-2709 [DOI: 10.1109/ICASSP39728.2021.9414055]
- Ren Y Z, Yang H Y, Wu H X, Tu W P and Wang L N. 2019. A secure AMR fixed codebook steganographic scheme based on pulse distribution model. *IEEE Transactions on Information Forensics and Security*, 14(10): 2649-2661 [DOI: 10.1109/TIFS.2019.2905760]
- Ren Y Z, Zheng W M and Wang L N. 2018. SILK steganography scheme based on the distribution of LSF parameter//*Proceedings of 2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference*. Honolulu, USA: IEEE: 539-548 [DOI: 10.23919/APSIPA.2018.8659509]
- Ren Y Z, Zhong S, Tu W P, Yang H Y and Wang L N. 2021. A SILK adaptive steganographic scheme based on minimizing distortion in pitch domain. *IETE Technical Review*, 38(1): 46-55 [DOI: 10.1080/02564602.2020.1757520]
- Sachnev V, Kim H J and Zhang R Y. 2009. Less detectable JPEG steganography method based on heuristic optimization and BCH syndrome coding//*Proceedings of the 11th ACM Workshop on Multimedia and Security*. Princeton, USA: ACM: 131-140 [DOI: 10.1145/1597817.1597841]
- Saenger J, Mazurczyk W, Keller J and Cavaglione L. 2020. VoIP network covert channels to enhance privacy and information sharing. *Future Generation Computer Systems*, 111: 96-106 [DOI: 10.1016/j.future.2020.04.032]
- Schönfeld D and Winkler A. 2006. Embedding with syndrome coding based on BCH codes//*Proceedings of the 8th Workshop on Multimedia and Security*. Geneva, Switzerland: ACM: 214-223 [DOI: 10.1145/1161366.1161405]
- Shahadi H I, Kod M S, Qasem B and Farhan H R. 2021. Real-time scheme for covert communication based VoIP. *Journal of Physics: Conference Series*, 1997: #012020 [DOI: 10.1088/1742-6596/1997/1/012020]
- Shanableh T. 2018. Altering split decisions of coding units for message embedding in HEVC. *Multimedia Tools and Applications*, 77(7): 8939-8953 [DOI: 10.1007/s11042-017-4787-6]
- Sharifzadeh M, Aloraini M and Schonfeld D. 2019. Quantized Gaussian embedding steganography//*Proceedings of 2019 IEEE International Conference on Acoustics, Speech and Signal Processing*. Brighton, UK: IEEE: 2637-2641 [DOI: 10.1109/ICASSP.2019.8682757]
- Shen J M, Ji H and Han J W. 2020. Near-imperceptible neural linguistic steganography via self-adjusting arithmetic coding//*Proceedings of 2020 Conference on Empirical Methods in Natural Language Processing*. [s. l.]: Association for Computational Linguistics: 303-313 [DOI: 10.18653/v1/2020.emnlp-main.22]
- Song T T, Liu M L, Luo W Q and Zheng P J. 2021. Enhancing image steganography via stego generation and selection//*Proceedings of 2021 IEEE International Conference on Acoustics, Speech and Signal Processing*. Toronto, Canada: IEEE: 2695-2699 [DOI: 10.1109/ICASSP39728.2021.9414723]
- Su W K, Ni J Q, Hu X L and Fridrich J. 2021. Image steganography with symmetric embedding using Gaussian Markov random field model. *IEEE Transactions on Circuits and Systems for Video Technology*, 31(3): 1001-1015 [DOI: 10.1109/TCSVT.2020.3001122]
- Su W K, Ni J Q, Hu X L and Huang J W. 2022. New design paradigm of distortion cost function for efficient JPEG steganography. *Signal Processing*, 190: #108319 [DOI: 10.1016/j.sigpro.2021.108319]
- Su W K, Ni J Q, Li X H and Shi Y Q. 2018. A new distortion function design for JPEG steganography using the generalized uniform embedding strategy. *IEEE Transactions on Circuits and Systems for Video Technology*, 28(12): 3545-3549 [DOI: 10.1109/TCSVT.2018.2865537]
- Su Y T, Zhang C Q and Zhang C T. 2011. A video steganalytic algorithm against motion-vector-based steganography. *Signal Processing*, 91(8): 1901-1909 [DOI: 10.1016/j.sigpro.2011.02.012]
- Sun X H, Wang K X and Li S J. 2021. Audio steganography with less modification to the optimal matching CNV-QIM path with the minimal hamming distance expected value to a secret. *Multimedia Systems*, 27(3): 341-352 [DOI: 10.1007/s00530-021-00790-w]
- Taburet T, Bas P, Fridrich J and Sawaya W. 2019b. Computing dependencies between DCT coefficients for natural steganography in JPEG domain//*Proceedings of ACM Workshop on Information Hiding and Multimedia Security*. Paris, France: ACM: 57-62 [DOI: 10.1145/3335203.3335715]
- Taburet T, Bas P, Sawaya W and Cogan R. 2020. JPEG steganography and synchronization of DCT coefficients for a given development pipeline//*Proceedings of 2020 ACM Workshop on Information Hiding and Multimedia Security*. Denver, USA: ACM: 139-149 [DOI: 10.1145/3369412.3395074]
- Taburet T, Bas P, Sawaya W and Fridrich J. 2019a. A natural steganography embedding scheme dedicated to color sensors in the JPEG domain//*Proceedings of Electronic Imaging: Media Watermarking, Security, and Forensics*. Springfield: Society for Imaging Science and Technology: #542 [DOI: 10.2352/ISSN.2470-1173.2019.5.MWSF-542]
- Taburet T, Bas P, Sawaya W and Fridrich J. 2021. Natural steganogra-

- phy in JPEG domain with a linear development pipeline. *IEEE Transactions on Information Forensics and Security*, 16: 173-186 [DOI: 10.1109/TIFS.2020.3007354]
- Tang G M, Jiang M M and Sun Y. 2019. Adaptive color image steganography based on dynamic distortion modification. *Journal of Electronics and Information Technology*, 41(3): 656-665 (汤光明, 姜明明, 孙艺. 2019. 失真代价动态更新的自适应彩色图像隐写算法. *电子与信息学报*, 41(3): 656-665) [DOI: 10.11999/JEIT180388]
- Tang W X, Li B, Barni M, Li J and Huang J W. 2021. An automatic cost learning framework for image steganography using deep reinforcement learning. *IEEE Transactions on Information Forensics and Security*, 16: 952-967 [DOI: 10.1109/TIFS.2020.3025438]
- Tang W X, Li B, Tan S Q, Barni M and Huang J W. 2019. CNN-based adversarial embedding for image steganography. *IEEE Transactions on Information Forensics and Security*, 14(8): 2074-2087 [DOI: 10.1109/TIFS.2019.2891237]
- Tang W X, Tan S Q, Li B and Huang J W. 2017. Automatic steganographic distortion learning using a generative adversarial network. *IEEE Signal Processing Letters*, 24(10): 1547-1551 [DOI: 10.1109/LSP.2017.2745572]
- Tao J Y, Li S, Zhang X P and Wang Z C. 2019. Towards robust image steganography. *IEEE Transactions on Circuits and Systems for Video Technology*, 29(2): 594-600 [DOI: 10.1109/TCSVT.2018.2881118]
- Tian H, Sun J, Chang C C, Qin J and Chen Y H. 2017. Hiding information into voice-over-IP streams using adaptive bitrate modulation. *IEEE Communications Letters*, 21(4): 749-752 [DOI: 10.1109/LCOMM.2017.2659718]
- Ueoka H, Murawaki Y and Kurohashi S. 2021. Frustratingly easy edit-based linguistic steganography with a masked language model//*Proceedings of 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*. [s.l.]: Association for Computational Linguistics [DOI: 10.18653/v1/2021.naacl-main.433]
- Wang C, Zhang W M, Liu J F and Yu N H. 2012. Fast matrix embedding by matrix extending. *IEEE Transactions on Information Forensics and Security*, 7(1): 346-350 [DOI: 10.1109/TIFS.2011.2164907]
- Wang L N, Wang B, Zhai L M and Xu Y B. 2018. JPEG image steganography based on side information estimation. *Journal of South China University of Technology (Natural Science Edition)*, 46(5): 9-18 (王丽娜, 王博, 翟黎明, 徐一波. 2018. 基于边信息估计的JPEG图像隐写方法. *华南理工大学学报(自然科学版)*, 46(5): 9-15) [DOI: 10.3969/j.issn.1000-565X.2018.05.002]
- Wang L N, Wang M J, Zhai L M and Ren Y Z. 2014. H.264/AVC video steganalysis algorithm based on motion vector abnormal correlation. *Acta Electronica Sinica*, 42(8): 1457-1464 (王丽娜, 王旻杰, 翟黎明, 任延珍. 2014. 基于相关性异常的H.264/AVC视频运动矢量隐写分析算法. *电子学报*, 42(8): 1457-1464) [DOI: 10.3969/j.issn.0372-2112.2014.08.001]
- Wang L N, Xu Y B, Zhai L M and Ren Y Z. 2017. An adaptive video motion vector steganography based on macroblock complexity. *Chinese Journal of Computers*, 40(5): 1044-1056 (王丽娜, 徐一波, 翟黎明, 任延珍. 2017. 基于宏块复杂度的自适应视频运动矢量隐写算法. *计算机学报*, 40(5): 1044-1056) [DOI: 10.11897/SP.J.1016.2017.01044]
- Wang S Z, Zhang X P and Zhang K W. 2005. *Digital Cryptography and Cryptography Analysis: Information Warfare Technology in the Internet Age*. Beijing: Tsinghua University Press (王朔中, 张新鹏, 张开文. 2005. *数字密写和密写分析——互联网时代的信息战技术*. 北京: 清华大学出版社)
- Wang Y, Cao Y and Zhao X F. 2021c. Minimizing embedding impact for H.264 steganography by progressive trellis coding. *IEEE Transactions on Information Forensics and Security*, 16: 333-345 [DOI: 10.1109/TIFS.2020.3013523]
- Wang Y, Cao Y, Zhao X F, Zhou X J and Zhu M N. 2018a. Maintaining rate-distortion optimization for IPM-based video steganography by constructing isolated channels in HEVC//*Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security*. Innsbruck, Austria: ACM: 97-107 [DOI: 10.1145/3206004.3206020]
- Wang Y F, Li W X, Zhang W M, Yu X Z, Liu K L and Yu N H. 2021a. BBC++: enhanced block boundary continuity on defining non-additive distortion for JPEG steganography. *IEEE Transactions on Circuits and Systems for Video Technology*, 31(5): 2082-2088 [DOI: 10.1109/TCSVT.2020.3010554]
- Wang Y F, Zhang W M, Li W X and Yu N H. 2021b. Non-additive cost functions for JPEG steganography based on block boundary maintenance. *IEEE Transactions on Information Forensics and Security*, 16: 1117-1130 [DOI: 10.1109/TIFS.2020.3029908]
- Wang Y F, Zhang W M, Li W X, Yu X Z and Yu N H. 2020. Non-additive cost functions for color image steganography based on inter-channel correlations and differences. *IEEE Transactions on Information Forensics and Security*, 15: 2081-2095 [DOI: 10.1109/TIFS.2019.2956590]
- Wang Z C, Qian Z X, Zhang X P, Yang M and Ye D P. 2018b. On improving distortion functions for JPEG steganography. *IEEE Access*, 6: 74917-74930 [DOI: 10.1109/ACCESS.2018.2884198]
- Wang Z C, Yin Z X and Zhang X P. 2019. Asymmetric distortion function for JPEG steganography using block artifact compensation. *International Journal of Digital Crime and Forensics*, 11(1): 90-99 [DOI: 10.4018/IJDCF.2019010107]
- Wang Z C, Zhang X P and Qin C. 2018. Asymmetric distortion function for spatial adaptive steganography. *Journal of Applied Sciences*, 36(5): 819-825 (王子驰, 张新鹏, 秦川. 2018. 非对称失真的空域自适应隐写. *应用科学学报*, 36(5): 819-825) [DOI: 10.3969/j.issn.0255-8297.2018.5.009]

- Wang Z C, Zhang X P and Yin Z X. 2016. Hybrid distortion function for JPEG steganography. *Journal of Electronic Imaging*, 25 (5): #050501 [DOI: 10.1117/1.jei.25.5.050501]
- Wayner P. 1992. Mimic functions. *Cryptologia*, 16 (3): 193-214 [DOI: 10.1080/0161-119291866883]
- Wei Q D, Yin Z X, Wang Z C and Zhang X P. 2018. Distortion function based on residual blocks for JPEG steganography. *Multimedia Tools and Applications*, 77(14): 17875-17888 [DOI: 10.1007/s11042-017-5053-7]
- Westfield A. 2001. F5—a steganographic algorithm//Proceedings of the 4th International Workshop on Information Hiding. Pittsburgh, USA: Springer; 289-302 [DOI: 10.1007/3-540-45496-9_21]
- Wojtuń J and Piotrowski Z. 2021. Synchronization of acoustic signals for steganographic transmission. *Sensors*, 21 (10): #3379 [DOI: 10.3390/s21103379]
- Wu J Q, Chen B L, Luo W Q and Fang Y M. 2020. Audio steganography based on iterative adversarial attacks against convolutional neural networks. *IEEE Transactions on Information Forensics and Security*, 15: 2282-2294 [DOI: 10.1109/TIFS.2019.2963764]
- Wu Z J, Yang W and Yang Y X. 2003. ABS-based speech information hiding approach. *Electronics Letters*, 39(22): 1617-1619 [DOI: 10.1049/el:20030993]
- Xiao B, Huang Y F and Tang S Y. 2008. An approach to information hiding in low bit-rate speech stream//Proceedings of 2008 IEEE Global Telecommunications Conference. New Orleans, USA: IEEE; 1-5 [DOI: 10.1109/GLOCOM.2008.ECP.375]
- Xie P, Zhang H, You W K, Zhao X F, Yu J C and Ma Y. 2019. Adaptive VP8 steganography based on deblocking filtering//Proceedings of ACM Workshop on Information Hiding and Multimedia Security. Paris, France: ACM; 25-30 [DOI: 10.1145/3335203.3335711]
- Yan D Q, Wang R D and Zhang L G. 2011. A high capacity MP3 steganography based on Huffman coding. *Journal of Sichuan University (Natural Science Edition)*, 48(6): 1281-1286 (严迪群, 王让定, 张力光. 2011. 基于 Huffman 编码的大容量 MP3 隐写算法. *四川大学学报(自然科学版)*, 48(6): 1281-1286) [DOI: 10.3969/j.issn.0490-6756.2011.06.011]
- Yang G B, Li J J, He Y L and Kang Z W. 2011. An information hiding algorithm based on intra-prediction modes and matrix coding for H.264/AVC video stream. *AEU – International Journal of Electronics and Communications*, 65(4): 331-337 [DOI: https://doi.org/10.1016/j.aeu.2010.03.011]
- Yang J and Li S B. 2018. An efficient information hiding method based on motion vector space encoding for HEVC. *Multimedia Tools and Applications*, 77(10): 11979-12001 [DOI: 10.1007/s11042-017-4844-1]
- Yang J H, Ruan D Y, Huang J W, Kang X G and Shi Y Q. 2020a. An embedding cost learning framework using GAN. *IEEE Transactions on Information Forensics and Security*, 15: 839-851 [DOI: 10.1109/TIFS.2019.2922229]
- Yang J H, Ruan D Y, Kang X G and Shi Y Q. 2019a. Towards automatic embedding cost learning for JPEG steganography//Proceedings of ACM Workshop on Information Hiding and Multimedia Security. Paris, France: ACM; 37-46 [DOI: 10.1145/3335203.3335713]
- Yang K, Yi X W, Zhao X F and Zhou L N. 2017. Adaptive MP3 steganography using equal length entropy codes substitution//Proceedings of the 16th International Workshop on Digital Watermarking. Magdeburg, Germany: Springer; 202-216 [DOI: 10.1007/978-3-319-64185-0_16]
- Yang Y Z, Wang Y T, Yi X W, Zhao X F and Ma Y. 2019b. Defining joint embedding distortion for adaptive MP3 steganography//Proceedings of ACM Workshop on Information Hiding and Multimedia Security. Paris, France: ACM; 14-24 [DOI: 10.1145/3335203.3335710]
- Yang Z L, Gong B T, Li Y M, Yang J S, Hu Z W and Huang Y F. 2020c. Graph-Stega: semantic controllable steganographic text generation guided by knowledge graph [EB/OL]. [2021-11-30]. <https://arxiv.org/pdf/2006.08339.pdf>
- Yang Z L, Guo X Q, Chen Z M, Huang Y F and Zhang Y J. 2019c. RNN-Stega: linguistic steganography based on recurrent neural networks. *IEEE Transactions on Information Forensics and Security*, 14(5): 1280-1295 [DOI: 10.1109/TIFS.2018.2871746]
- Yang Z L, Xiang L Y, Zhang S Y, Sun X M and Huang Y F. 2021. Linguistic generative steganography with enhanced cognitive-imperceptibility. *IEEE Signal Processing Letters*, 28: 409-413 [DOI: 10.1109/LSP.2021.3058889]
- Yang Z L, Zhang P Y, Jiang M Y, Huang Y F and Zhang Y J. 2018. RITS: real-time interactive text steganography based on automatic dialogue model//Proceedings of the 4th International Conference on Cloud Computing and Security. Haikou, China: Springer; 253-264 [DOI: 10.1007/978-3-030-00012-7_24]
- Yang Z L, Zhang S Y, Hu Y T, Hu Z W and Huang Y F. 2021. VAE-Stega: linguistic steganography based on variational auto-encoder. *IEEE Transactions on Information Forensics and Security*, 16: 880-895 [DOI: 10.1109/TIFS.2020.3023279]
- Yao Y Z, Zhang W M, Yu N H and Zhao X F. 2015. Defining embedding distortion for motion vector-based video steganography. *Multimedia Tools and Applications*, 74(24): 11163-11186 [DOI: 10.1007/s11042-014-2223-8]
- Yi X W, Yang K, Zhao X F, Wang Y T and Yu H B. 2019. AHCM: adaptive Huffman code mapping for audio steganography based on psychoacoustic model. *IEEE Transactions on Information Forensics and Security*, 14(8): 2217-2231 [DOI: 10.1109/TIFS.2019.2895200]
- You W K, Cao Y and Zhao X F. 2017. Information hiding using CAV-LC: misconceptions and a detection strategy//Proceedings of the 16th International Workshop on Digital Watermarking. Magdeburg, Germany: Springer; 187-201 [DOI: 10.1007/978-3-319-64185-0_15]
- Yu X Z, Chen K J, Wang Y F, Li W X, Zhang W M and Yu N H. 2020. Robust adaptive steganography based on generalized dither

- modulation and expanded embedding domain. *Signal Processing*, 168: #107343 [DOI: 10.1016/j.sigpro.2019.107343]
- Zha H Y, Zhang W M, Qin C and Yu N H. 2019. Direct adversarial attack on stego sandwiched between black boxes//*Proceedings of 2019 IEEE International Conference on Image Processing*. Taipei, China: IEEE: 2284-2288 [DOI: 10.1109/ICIP.2019.8804415]
- Zhang H, Cao Y and Zhao X F. 2016a. Motion vector-based video steganography with preserved local optimality. *Multimedia Tools and Applications*, 75(21): 13503-13519 [DOI: 10.1007/s11042-015-2743-x]
- Zhang H, Cao Y, Zhao X F, Yu H B and Liu C J. 2017a. Data hiding in H.264/AVC video files using the coded block pattern//*Proceedings of the 15th International Workshop on Digital Watermarking*. Beijing, China: Springer: 588-600 [DOI: 10.1007/978-3-319-53465-7_44]
- Zhang H, Cao Y, Zhao X F, Zhang W M and Yu N H. 2014. Video steganography with perturbed macroblock partition//*Proceedings of the 2nd ACM Workshop on Information Hiding and Multimedia Security*. Salzburg, Austria: ACM: 115-122 [DOI: 10.1145/2600918.2600936]
- Zhang K, Xu L, Cuesta-Infante A and Veeramachaneni K. 2019. Robust invisible video watermarking with attention [EB/OL]. [2021-11-30]. <https://arxiv.org/pdf/1909.01285.pdf>
- Zhang S Y, Yang Z L, Yang J S and Huang Y F. 2021b. Linguistic steganography: from symbolic space to semantic space. *IEEE Signal Processing Letters*, 28: 11-15 [DOI: 10.1109/LSP.2020.3042413]
- Zhang S Y, Yang Z L, Yang J S and Huang Y F. 2021c. Provably secure generative linguistic steganography//*Proceedings of Findings of the Association for Computational Linguistics*. [s.l.]: Association for Computational Linguistics [DOI: 10.18653/v1/2021.findings-acl.268]
- Zhang W M and Li S Q. 2008. A coding problem in steganography. *Designs, Codes and Cryptography*, 46(1): 67-81 [DOI: 10.1007/s10623-007-9135-9]
- Zhang W M, Liu J F, Wang X and Yu N H. 2010a. Generalization and analysis of the paper folding method for steganography. *IEEE Transactions on Information Forensics and Security*, 5(4): 694-704 [DOI: 10.1109/TIFS.2010.2065804]
- Zhang W M, Zhang X P and Wang S Z. 2007a. A double layered “plus-minus one” data embedding scheme. *IEEE Signal Processing Letters*, 14(11): 848-851 [DOI: 10.1109/LSP.2007.903255]
- Zhang W M, Zhang X P and Wang S Z. 2008. Maximizing steganographic embedding efficiency by combining Hamming codes and wet paper codes//*Proceedings of the 10th International Workshop on Information Hiding*. Santa Barbara, USA: Springer: 60-71 [DOI: 10.1007/978-3-540-88961-8_5]
- Zhang W M, Zhang X P and Wang S Z. 2010b. Near-optimal codes for information embedding in gray-scale signals. *IEEE Transactions on Information Theory*, 56(3): 1262-1270 [DOI: 10.1109/TIT.2009.2039087]
- Zhang W M, Zhang Z, Zhang L L, Li H Y and Yu N H. 2017b. Decomposing joint distortion for adaptive steganography. *IEEE Transactions on Circuits and Systems for Video Technology*, 27(10): 2274-2280 [DOI: 10.1109/TCSVT.2016.2587388]
- Zhang X P. 2010. Efficient data hiding with plus-minus one or two. *IEEE Signal Processing Letters*, 17(7): 635-638 [DOI: 10.1109/LSP.2010.2049415]
- Zhang X P and Wang S Z. 2006. Efficient steganographic embedding by exploiting modification direction. *IEEE Communications Letters*, 10(11): 781-783 [DOI: 10.1109/LCOMM.2006.060863]
- Zhang Y, Luo X Y, Guo Y Q, Qin C and Liu F L. 2020a. Multiple robustness enhancements for image adaptive steganography in lossy channels. *IEEE Transactions on Circuits and Systems for Video Technology*, 30(8): 2750-2764 [DOI: 10.1109/TCSVT.2019.2923980]
- Zhang Y, Luo X Y, Wang J W, Guo Y Q and Liu F L. 2021a. Image robust adaptive steganography adapted to lossy channels in open social networks. *Information Sciences*, 564: 306-326 [DOI: 10.1016/j.ins.2021.02.058]
- Zhang Y, Luo X Y, Wang J W, Yang C F and Liu F L. 2018b. A robust image steganography method resistant to scaling and detection. *Journal of Internet Technology*, 19(2): 607-618 [DOI: 10.3966/160792642018031902029]
- Zhang Y, Luo X Y, Yang C F, Ye D P and Liu F L. 2016b. A framework of adaptive steganography resisting JPEG compression and detection. *Security and Communication Networks*, 9(15): 2957-2971 [DOI: 10.1002/sec.1502]
- Zhang Y, Luo X Y, Zhu X D, Li Z Y and Bors A G. 2020b. Enhancing reliability and efficiency for real-time robust adaptive steganography using cyclic redundancy check codes. *Journal of Real-Time Image Processing*, 17(1): 115-123 [DOI: 10.1007/s11554-019-00905-7]
- Zhang Y, Zhu X D, Qin C, Yang C F and Luo X Y. 2018c. Dither modulation based adaptive steganography resisting JPEG compression and statistic detection. *Multimedia Tools and Applications*, 77(14): 17913-17935 [DOI: 10.1007/s11042-017-4506-3]
- Zhang Y W, Zhang W M, Chen K J, Liu J Y, Liu Y J and Yu N H. 2018a. Adversarial examples against deep neural network based steganalysis//*Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security*. Innsbruck, Austria: ACM: 67-72 [DOI: 10.1145/3206004.3206012]
- Zhang Z Y, Yi X W and Zhao X F. 2020c. An AAC steganography scheme for adaptive embedding with distortion minimization model. *Multimedia Tools and Applications*, 79(37): 27777-27790 [DOI: 10.1007/s11042-020-09344-0]
- Zhao Z Z, Guan Q X, Zhang H and Zhao X F. 2019. Improving the robustness of adaptive steganographic algorithms based on transport channel matching. *IEEE Transactions on Information Forensics and Security*, 14(7): 1843-1856 [DOI: 10.1109/TIFS.2018.

2885438]

- Zhao Z Z, Guan Q X and Zhao X F. 2016. Constructing near-optimal double-layered syndrome-trellis codes for spatial steganography//Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security. Vigo, Spain; ACM: 139-148 [DOI: 10.1145/2909827.2930802]
- Zhong S P, Cheng X Q and Chen T R. 2007. Data hiding in a kind of PDF texts for secret communication. International Journal of Network Security, 4(1): 17-26
- Zhong Z Y, Guo Y H and Xu G A. 2012. Digital watermarking algorithm based on structure of PDF document. Journal of Computer Applications, 32(10): 2776-2778, 2782 (钟征燕, 郭燕慧, 徐国爱. 2012. 基于PDF文档结构的数字水印算法. 计算机应用, 32(10): 2776-2778, 2782) [DOI: 10.3724/SP.J.1087.2012.02776]
- Zhou W B, Zhang W M and Yu N H. 2017. A new rule for cost reassignment in adaptive steganography. IEEE Transactions on Information Forensics and Security, 12(11): 2654-2667 [DOI: 10.1109/TIFS.2017.2718480]
- Zhou X J, Peng W L, Yang B Y, Wen J, Xue Y M and Zhong P. 2021. Linguistic steganography based on adaptive probability distribution. [J/OL]. [2021-11-30]. IEEE Transactions on Dependable and Secure Computing, <https://ieeexplore.ieee.org/document/9430708> [DOI: 10.1109/TDSC.2021.3079957]
- Zhou Z L, Mu Y, Zhao N S, Wu Q M J and Yang C N. 2016. Coverless information hiding method based on multi-keywords//Proceedings of the 2nd International conference on cloud computing and security. Nanjing, China; Springer: 39-47 [DOI: 10.1007/978-3-319-48671-0_4]
- Zhu B L and Ni J Q. 2018. Uniform embedding for efficient steganography of H. 264 video//Proceedings of the 25th IEEE International Conference on Image Processing. Athens, Greece; IEEE: 1678-1682 [DOI: 10.1109/ICIP.2018.8451214]
- Zhu L Y, Luo X Y, Yang C F, Zhang Y and Liu F L. 2021a. Invariances of JPEG-quantized DCT coefficients and their application in robust image steganography. Signal Processing, 183: #108015 [DOI: 10.1016/j.sigpro.2021.108015]
- Zhu L Y, Luo X Y, Zhang Y, Yang C F and Liu F L. 2021b. Inverse interpolation and its application in robust image steganography [J/OL]. [2021-11-30]. IEEE Transactions on Circuits and Systems for Video Technology, <https://ieeexplore.ieee.org/document/9521502> [DOI: 10.1109/TCSVT.2021.3107342]

Ziegler Z M, Deng Y T and Rush A M. 2019. Neural linguistic steganography//Proceedings of 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing. Hong Kong, China; Association for Computational Linguistics [DOI: 10.18653/v1/D19-1115]

作者简介



张卫明, 1976年生, 男, 教授, 主要研究方向为信息隐藏与人工智能安全。

E-mail: zhangwm@ustc.edu.cn



张新鹏, 通信作者, 男, 教授, 主要研究方向为多媒体信息安全、人工智能安全、图像处理。

E-mail: zhangxinpeng@fudan.edu.cn

王宏霞, 女, 教授, 主要研究方向为多媒体信息安全、信息隐藏与数字水印、数字取证、智能信息处理。

E-mail: hxwang@scu.edu.cn

李斌, 男, 教授, 主要研究方向为多媒体取证、多媒体安全、信息隐藏。E-mail: libin@szu.edu.cn

任延珍, 女, 教授, 主要研究方向为多媒体内容安全。

E-mail: renyz@whu.edu.cn

杨忠良, 男, 博士, 主要研究方向为信息隐藏与人工智能安全。E-mail: yangzl15@mails.tsinghua.edu.cn

陈可江, 男, 博士, 主要研究方向为信息隐藏与人工智能安全。E-mail: chenkj@ustc.edu.cn

李伟祥, 男, 博士, 主要研究方向为信息隐藏与人工智能安全。E-mail: liweixiang@szu.edu.cn

俞能海, 男, 教授, 主要研究方向为多媒体内容安全。

E-mail: ynh@ustc.edu.cn