大连市科学技术奖提名前公示内容

自然科学奖

一、项目名称

人工智能时代云端图像数据安全保护研究

二、提名者及提名意见

提名者：辽宁师范大学

提名意见：

该项目在国家青年基金、辽宁省社会科学院项目等资助下，从保护云端图像数据安全出发，系统研究基于神经网络、加密技术和信息隐藏的图像数据安全保护研究，取得系列具有国际影响的原创性研究成果。首次提出了基于格雷码的同态加密系统(Homomorphic Encryption System based on Gray Code, HESGC)和水印追踪联合策略(Joint Watermarking and Tracing, JWT)，实现了密文域可逆水印技术和盗版追踪功能；提出了“三维水印”，包括认证水印、恢复水印和隐私水印，并改进了随机化哈夫曼方案加密与压缩恢复水印和隐私水印，利用活动轮廓模型将医学图像划分为感兴趣区域(ROI)和非感兴趣区域(RONI)，提出了两级篡改检测方案来检测 ROI 是否被篡改，利用 RONI 区域隐藏的信息恢复被篡改区域；融合了视觉密码术、LT 编码、循环冗余检验(CRC)，块 G-H 特征、Arnold 变换和时间戳认证，提出了一种鲁棒性强、安全性高的零水印方案；提出“联合隐藏与追踪”策略(Joint Hiding and Tracing, JHT)，实现盗版追踪，并采用“三级完整性认证方案” (Joint Hiding and Tracing, JHT)进行完整性认证，同时，提出邻次优化方法消除光滑/纹理块中的纹理/光滑孤岛，采用 Paillier 同态加密对原始图像进行加密，提高系统安全性；提出了一种安全性能高的 3 级秘钥嵌入方案(three level secret-key embedding scheme, TLSES), 将图像块分成纹理块和平滑块，纹理块除了保存常规信息外，保存了“细节”信息，所谓细节信息即纹理信息，这不仅能有效地抵抗均值攻击，而且有助于提高恢复图像的质量，满足实际工作的需要。

项目成果在国际著名期刊 Multimedia Tools and Applications 等发表，受到国内外同行高度评价和正面引用。项目开始至今，项目主持人以第一作者或通信作者身份发表核心论文 29 篇，其中 SCI 检索 11 篇、EI 检索 1 篇，中文核心期刊 SCD 收录 17 篇。授权发明专利 2 项。研究成果兼顾经济、社会发展和个人隐私保护需求，有助于构建安全的数字化信息环境，有助于推动大连市、辽宁省乃至全国的数据安全的健康发展。

三、项目简介

随着云技术和 5G 的飞速发展，大量图像信息暴露在公共视野，这不仅对个人隐私及安全构成严重威胁，甚至会带来国家安全、社会影响力等多方面的连锁反应。中国科学院院士冯登国教授指出，数据已成为一种重要的生产资料，数据安全已经成为关乎个人隐私、经济和社会安全等事关国家安全的重大安全问题。《“十四五”数字经济发展规划》要求着力强化数字经济安全体系，提升数据安全保障水平，数据安全又一次在顶层设计规划层面受到高度重视。因此，加强云端图像数据安全保护将为数据安全保驾护航，满足国家“十四五”规划要求。

1. 面向隐私保护的区域自适应可逆医学图像水印技术

提出了“三维水印”，包括认证水印、恢复水印和隐私水印，并改进了随机化哈夫曼方案加密与压缩恢复水印和隐私水印。为提高安全性，提出了三种不同的水印生成策略。首先，提出了邻域差分方法生成变长恢复水印，其中八方向子带和四方向子带被自适应采用；然后，基于余 3 循环码和密码本生成隐私水印；最后，采用一种新的并行格哈希函数生成认证水印。在嵌入过程中，利用活动轮廓模型将医学图像划分为感兴趣区域(ROI)和非感兴趣区域(RONI)。在 ROI 中，改进的差分扩展双层可逆嵌入策略被提出，用于嵌入认证水印以定位篡改区域并提高嵌入能力。在 RONI 中，基于直方图修改的差分图像可逆嵌入策略被提出，用于嵌入恢复水印和隐私水印，该方法具有较强的灵活性，可自适应获取四个或多个峰值点。在检测阶段，提出了两级篡改检测方案来检测 ROI 是否被篡改。结果表明，该科学发现既实现了隐私保护，完整性认证，可逆性，又具有安全性高、容量大、恢复质量好等特点。而且，能够有效抵抗 JPEG 压缩、高斯噪声、椒盐噪声、中值滤波、旋转攻击，锐化攻击和直方图均衡攻击，实现了较强的鲁棒性。

2. 面向版权保护的基于视觉密码和块 G-H 特征的鲁棒零水印技术

融合了视觉密码术、LT 编码、循环冗余检验(CRC)，块 G-H 特征、Arnold 变换和时间戳认证，提出了一种鲁棒性强、安全性高的零水印方案。基于可视加密技术将原始图像生成两个可视化加密共享。利用改进的 G-H 特征提取算法提取图像块分组内容特征。为了抵抗强攻击，根据组特征均值与整体特征均值的关系生成过度矩阵。为提高安全性，对原始水印图像进行 LT 编码和 CRC 加密。根据过渡矩阵和加密水印生成零水印。该方案具有良好的抗均衡性、抗干扰性和不可见性，而且对各种攻击具有较强的鲁棒性，如高斯噪声，椒盐噪声，中值过滤，JPEG 压缩，剪切，旋转和线偏移等。此外，稳健性理论分析、安全性理论分析以及复杂性分析进一步证明了本科学发现的综合性能。

3. 用于盗版追踪的格雷码加密域可逆水印研究

首次提出了基于格雷码的同态加密系统(Homomorphic Encryption System based on Gray Code, HESGC)和水印追踪联合策略(Joint Watermarking and Tracing,

JWT)，实现了密文域可逆水印技术和盗版追踪功能。原始图像经过 HESGC 加密与膨胀，不仅避免了大多明文域水印算法存在暴露原始图像信息的风险，而且提高了系统容量。同时，直接采用灰度图像作为水印图像，解除了以往以二值图像作为水印图像，或者将灰度图像二值化后作为水印图像的限制，而且采用基于级联混沌技术提高了灰度水印图像的安全性。此外，成功消除图像分区分类中纹理/平滑区域中的平滑/纹理孤岛。而且，能够抵抗一些常见的攻击，如随机噪声、中值滤波、图像平滑、编码 JPEG 编码、LZW 编码和卷积模糊等。

4. 面向完整性认证与盗版追踪的同态加密域可逆信息隐藏技术

提出“联合隐藏与追踪”策略(Joint Hiding and Tracing, JHT)，实现盗版追踪，JHT 策略具有较强的鲁棒性，在一些常见的攻击下可以有效识别盗版来源，如 JPEG 压缩，高斯平滑，椒盐噪声和中值滤波；提出了双区域划分策略，其中采用数据/签名区域划分避免了冲突，并且纹理/平滑区域划分非常符合人类的视觉特征；提出邻次优化方法消除光滑/纹理块中的纹理/光滑孤岛，它使相同的区域变成更加集中，区域划分更加准确合理；采用 Paillier 同态加密对原始图像进行加密，相比采用明文域算法，支持在密文中直接操作，更有效保护用户隐私，实现了可逆的信息隐藏、完整性认证、隐私保护和盗版跟踪。

5. 安全自适应容量的自恢复水印技术

提出了一种安全性能高的嵌入方案 3 级秘钥嵌入方案(three level secret-key embedding scheme, TLSES)，严谨的理论分析表明，本系统安全性完全满足实际要求，$SFP=\frac{1}{2^{19-24}\times n^2}$ (n 为图像分块数)；提出了“复合水印”的概念，所谓“复合水印”是指水印由认证水印和信息水印构成，其中认证水印用于检测篡改区域，信息水印用于恢复图像，信息水印又包含基础水印和附加水印；针对不同类别图像块，结合图像块自身特点，产生变长附加水印，满足实际需求，不同块产生不同长度的附加水印，其对应块的嵌入水印量也就不同，实现了变容量水印技术；根据图像块自身的特点，将图像块分成纹理块和平滑块，纹理块除了保存常规信息外，保存了“细节”信息，所谓细节信息即纹理信息，这不仅能有效地抵抗均值攻击，而且有助于提高恢复图像的质量，满足实际工作的需要。

四、代表性论文（专著）目录

1. **Hui Shi**, Ying Wang, Yanni Li, **Yonggong Ren**, Cheng Guo. Region-based reversible medical image watermarking algorithm for privacy.Multimedia Tools and Applications, (2021), 80(16): 24631–24667（SCI, 影响因子 3.6，他引 3 次）

2. **Hui Shi**, Yanni Li, Baoyue Hu, Meihan Chen, **Yonggong Ren**. A robust and secure zero-watermarking copyright authentication scheme based on visual cryptography and block G-H feature.Multimedia Tools and Applications,

2022,81(26):38019-38051 （SCI, 影响因子 3.6，他引 2 次）

3. **石慧**,冯斌,王相海,李明楚,宋传鸣. 用于盗版追踪的格雷码加密域可逆水印研究.中国图象图形学报, 2018,23(11): 1635-1651, 2018.11. 中国科学引文数据库(CSCD)

4. **Hui Shi**, Dan Liu, Hongbin Lu, Chenguang Zhou. A homomorphic encrypted reversible information hiding scheme for integrity authentication and piracy tracing. Multimedia Tools and Applications, 2018, 77:20535–20567. （SCI, 影响因子 3.6）

5. **Hui Shi**, Xianghai Wang, Mingchu Li, Jun Bai ,Bin Feng. Secure variable-capacity self-recovery watermarking scheme.Multimedia Tools and Applications, 2017, 76:6941–6972（SCI, 影响因子 3.6）

五、主要完成人（完成单位）。

姓名	职称	职务	完成单位
石慧	副教授	副主任	辽宁师范大学
任永功	教授	院长	辽宁师范大学

项目负责人签字：石慧

单位公章：