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
01
VOL.27

ISSN1006-8961
CN11-3758/TB

数字图像/视频内容安全

中国图象图形学报

刊名题字：宋健 | 月刊（1996年创刊）

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

第27卷第1期（总第309期）
2022年1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

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

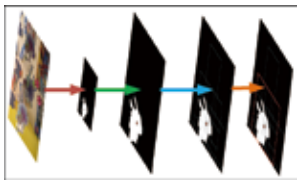
Distributed by Beijing Bureau for Distribution of Newspapers and Journals
Domestic All Local Post Offices in China
Overseas China International Book Trading Corporation (P.O.Box 399, Beijing 100048,P.R.China))
Printed by Beijing Kexin Printing Co., Ltd.

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

2022年1月 第27卷 第1期（总第309期）
中国图象图形学报
Zhongguo Tuxiang Tuxing Xuebao

目次



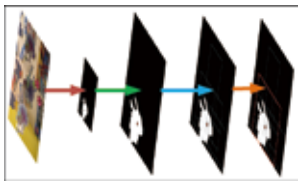
检测小篡改区域的U型网络(第0176页)

结合半张量积压缩感知的可验证图像加密(第0215页)

实离散分数Krawtchouk变换及其在数字图像水印中的应用(第0252页)

Volume 27, Number 1
Published January 16, 2022

CONTENTS
JOURNAL OF IMAGE AND GRAPHICS



U-Net for detecting the small forgery region(P0176)

Semi-tensor product compression sensing integrated to verifiable image encryption method(P0215)

Real discrete fractional Krawtchouk transform with an application to image watermarking(P0252)

E-mail: jig@aircas.ac.cn
Website: www.cjig.cn
Tel: 010-58887035
中国图象图形学报
JOURNAL OF IMAGE AND GRAPHICS

中图法分类号:TP391　　**文献标识码**: A　　**文章编号**: 1006-8961(2022)01-0226-12

论文引用格式: Zhao X, Wang Y F, Chen K J, Zhang W M and Yu N H. 2022. Spatial image steganography based on side information estimated by super resolution. Journal of Image and Graphics,27(01):0226-0237(赵鑫,王垚飞,陈可江,张卫明,俞能海. 2022. 引入超分辨率下采样误差的图像边信息估计隐写. 中国图象图形学报,27(01):0226-0237)[DOI:10.11834/jig.210433]

引入超分辨率下采样误差的图像边信息估计隐写

赵鑫,王垚飞,陈可江,张卫明*,俞能海

1. 中国科学技术大学网络空间安全学院, 合肥　230027;
2. 中国科学院电磁空间信息重点实验室, 合肥　230027

摘　要: **目的**　由于空域图像下采样过程中提供的量化误差边信息能够有效提升隐写安全性,为了得到下采样之前的高分辨率图像,提出一种基于超分辨率网络的空域图像边信息估计隐写方法。**方法**　受原始下采样边信息隐写方法的启发,使用超分辨率网络生成被称为预载体的高分辨率图像。同时利用现有的空域图像对称失真算法得到每个像素点的修改失真,然后以浮点型精度对预载体下采样,得到和载体同分辨率的图像形式,利用对应像素点间的差值指导像素点的修改方向,实现基于初始失真的非对称失真调整。首先以峰值信噪比和极性估计准确率为指标对比了多种超分辨率网络以及基于传统插值方法的上采样性能,并通过调整初始失真分别进行隐写和隐写分析实验,选择使安全性提升最大的残差通道注意力机制网络及其对应调整系数作为本文的下采样边信息估计隐写方法。**结果**　使用隐写领域中常用的3个数据库、两种传统初始失真函数以及两类隐写分析方法进行实验。在跨数据集的隐写安全性上,相比传统隐写方法,在对抗基于手工特征和基于深度学习的隐写分析时,本文方法的安全性均有显著提升,如在测试集载体图像上,嵌入率为0.5 bit/像素时,安全性分别提升6.67%和6.9%;在训练集载体图像上,本文方法的安全性在比传统方法有很大提升的基础上,甚至在一些情况下能够高于原始边信息隐写方法的安全性,如在对抗基于手工特征的隐写分析器且嵌入率为0.1 bit/像素时,安全性提升1.08%;在对抗基于深度学习的隐写分析器且嵌入率为0.5 bit/像素时,安全性提升0.6%。**结论**　实验表明,使用超分辨率网络作为下采样边信息估计的工具,并利用估计边信息调整嵌入修改的初始失真,能够有效提升传统隐写方法的安全性,并接近甚至在部分情况下超越了原始边信息隐写的安全性。除此之外,本文方法与原始边信息隐写方法具有不同的修改模式,而且具有更广泛的适用性。

关键词:隐写;边信息估计;超分辨率网络;下采样;失真调整

Spatial image steganography based on side information estimated by super resolution

Zhao Xin, Wang Yaofei, Chen Kejiang, Zhang Weiming*, Yu Nenghai

1. *School of Cyber Security, University of Science and Technology of China, Hefei　230027, China*;
2. *Key Laboratory of Electromagnetic Space Information, Chinese Academy of Sciences, Hefei　230027, China*

Abstract: **Objective** Steganography is a way of covert communication to achieve the transmission of a secret message via

收稿日期:2021-06-22;**修回日期**:2021-10-12;**预印本日期**:2021-10-19

*通信作者:张卫明　zhangwm@ustc.edu.cn

基金项目:国家自然科学基金项目(62102386, 62072421, 62002334);中央高校基本科研业务费专项资金资助(WK2100000018);中国博士后科学基金项目(2021M693091)

Supported by: National Natural Science Foundation of China (62102386, 62072421, 62002334); Fundamental Research Funds for Central Universities(WK2100000018); China Postdoctoral Science Foundation (2021M693091)

slight modification of the elements on the cover images without causing suspicion of the steganalysis. Security is capable to embed the secret message with minimal distortion via syndrome-trellis codes (STC), steganographic polar codes (SPC) or optimal analogue embedding. The embedding rate and loss function is demonstrated. The initial symmetric distortions function assigns the same cost for the modification of pixel values ±1. Some adapting methods on top of symmetric distortion have also been generated, demonstrating the effectiveness of asymmetric distortion steganography for improving steganographic security. To improve steganography security, the prompted guidance of the adjustment of the initial cost and previous work has proved that the quantization error information provided via image downsampling used as auxiliary information Steganography does not have the original image before downsampling in many real scenes. For computer vision, super-resolution tasks are rapidly evolving, which can end-to-end generate high-resolution images corresponding to low-resolution images. In order to get the high-resolution images before downsampling based on the downsampled side information, this research has proposed a steganography based on super-resolution networks for estimating side information of spatial domain images. The unique side information provided by the estimated high-resolution images in the downsampling process can effectively improve steganography security excluding high scaling. **Method** Based on the initial side information steganography method, the steganographer cover for embedding is obtained via various image processing processes in common, such as the downsampling process involved. A pre-cover downsampling image has been called for obtained cover. This research has briefly proposed some relevant super-resolution networks to assess the quality of the resulting image via peak signal to noise ratio (PSNR) and polarity estimation correctness initially. The network that can make the largest contribution to steganographic security is opted for the first step of estimating the side information, i. e. , generating a high-resolution precover image. Current side information estimated steganography methods in the context of JPEG image steganography has derived their side information from the quantization error generated in the JPEG compression process. The cost effective strategy uses the degradation model of the original side information steganography, i. e. , the solo polarity of the error is considered without the magnitude of the error. The modification cost of the pixel points is in the same scale. The current loss function in the spatial domain is used to obtain the cost of modification for each pixel. The image form with the same resolution as the cover is acquired via floating-point precision of the pre-cover downsampling. Based on the initial cost, the differentiation amongst the corresponding pixels is used to guide the modification of the pixels to achieve asymmetric distortion adjustment. A steganographic framework for side information has been estimated in spatial domain images based on super-resolution networks. **Result** The initial demonstration compare the degree of improvement in steganographic security for side information estimated based on various super-resolution networks. The residual channel attention network (RCAN) with a scaling of 2 as the side information estimating network model is illustrated at last. The optimal cost adjustment coefficients is experimentally obtained at different embedding rates. Three databases including break our steganographic system (BOSSBase), break our watermarking system 2 (BOWS2) and mixed resized never-compressed (MRNC) and two initial distortion functions in the context of high-pass, low-pass, and low-pass (HILL) and unIversal wavelet relative distortion for the spatial (SUNIWARD) are used to test the security of the demonstrated method against manual feature and network steganalysis. In terms of cross-database steganographic security, such as BOWS2, the security method is significantly improved against spatial rich model (SRM) and steganalysis residual network (SRNet) steganalysis compared with the original method HILL. When the embedding rate is 0. 5 bit/pixel, the demonstrated method improves 6. 67% and 6. 9% , respectively. The embedding rate is 0. 1 bit/pixel based on the improvement of 1. 74% and 5. 8% each. Meanwhile, this analysis improves 4. 04% and 4. 0% , respectively, over the two traditional steganography methods on cover images set that are not directly derived from the downsampling process. The difference has been shown and the original side information steganography is compared on the training set cover in terms of steganographic security and modification point distribution. Both side information estimated steganography and original side information steganography greatly improve steganographic security, but their modification modes are different. The initial distortion is calculated with the HILL and the embedding rate is 0. 1 bit/pixel in particular. The security of the proposed method exceeds that of original side information steganography method by 1. 08% against SRM steganalysis. The embedding rate is 0. 5 bit/pixel. The security of the proposed method exceeds that of original side information steganography by 0. 6% against SRNet steganalysis. It is illustrated that the analyzed method has its priority on the steganography of initial side information steganography in some cases. **Conclusion** The estimated downsampled side infor-

mation has been proposed first to adjust the initial cost of modified pixels in order to distinguish the modified loss of pixel points in different directions for asymmetric distortion steganography. To obtain effective auxiliary information, a super-resolution network to estimate the corresponding high-resolution image of the cover has been proposed simultaneously. The cost adjustment integrated strategy is improving the steganographic security effectively. Compared with original side information steganography, the research priority is that it can be widely applied to steganography of multi-sources cover images while original side information steganography cannot be applied, i. e. , the original high-resolution image cannot be obtained, and has a wider application scenario than original side information steganography. In addition, the research method can be applied to the field of JPEG domain. Limitation there is still a certain gap based on the illustrated security method in most scenarios where both methods can be applied. The estimated side information steganography method has been developing more suitable network structures and cost modification strategies further.

Key words: steganography; side information estimation; super-resolution networks; downsampling; cost adjustment

0 引 言

隐写是一种隐蔽通信技术,通过轻微地修改载体上的元素来嵌入并传输秘密信息,其安全性由对抗隐写分析检测的能力来衡量(Fridrich,2006)。最小化失真隐写框架是实现安全隐写的主流框架。STC(syndrome-trellis codes)(Filler 等,2011)和隐写极化码 SPC(steganographic polar codes)(Li 等,2020b)的出现,使得针对任意加性失真函数,隐写方能够在给定嵌入率下接近总体失真的理论下界。所以当今隐写领域的主要研究方向是如何设计更好的失真函数。

失真函数通过量化载体上每个像素点被修改所产生的影响,为每个像素点分配修改失真。在加性隐写条件下,所有修改带来的影响总和代表了载体图像和载密图像之间的总体失真(Wang 等,2016)。现有很多用于空域图像的失真函数算法,比如 HUGO(highly undetectable stego)(Pevny 等,2010)、WOW(wavelet obtained weights)(Holub 和 Fridrich,2012)、SUNIWARD(universal wavelet relative distortion for the spatial)(Holub 和 Fridrich,2013)、HILL(high-pass, low-pass, and low-pass)(Li 等,2014)和 MVGG(multivariate generalized Gaussian)(Sedighi 等,2015)。这些失真函数为像素点嵌入时的 ±1 修改赋予了相等的失真,称之为对称失真函数。但在实际情况下,由于自然图像的分布特性,像素点 +1 和 −1 的修改失真不应该总是一样的。

现实场景中,隐写方用于嵌入消息的载体大多已经经过了各种各样的图像处理操作,比如下采样、颜色转换和有损压缩等,而这些图像处理过程中产生的辅助信息,比如量化误差,可以被隐写方利用来提升隐写安全性。Denemark 和 Fridrich(2015)通过利用量化误差提出原始边信息隐写方法。实验表明,利用载体图像生成过程中的量化误差对初始失真进行调整,隐写安全性可得到显著的提升。

虽然 Denemark 和 Fridrich(2015)证实了利用原始图像提供的辅助信息进行边信息隐写的有效性,但是现实中隐写方并不总能拥有原始图像,所以 Li 等人(2020a)在 JPEG 域中提出估计边信息隐写方法,通过估计 JPEG 压缩过程产生的量化误差,并将其作为辅助信息调整初始失真,大大提升了 JPEG 隐写的安全性。

然而目前尚未有针对空域图像边信息估计的隐写方法,空域图像与 JPEG 图像不同,不存在 JPEG 压缩过程,但是大多数空域图像是由大图像下采样得到的小图像,因此提出利用超分辨率(super resolution, SR)技术来获取空域边信息,超分辨率的目标是从低分辨率(low resolution, LR)图像中恢复出高分辨率(high resolution, HR)图像,其难点在于,一个 LR 图像对应了多个 HR 图像,因此这是一个不适定性问题。随着深度学习的发展,出现了多种基于深度学习的超分辨率方法,如 SRResNet(deep residual network for image super resolution)、SRGAN(generative adversarial network for image super resolution)(Ledig 等,2017)、EDSR(enhanced deep super-resolution)(Lim 等,2017)、RRDBNet(residual in residual dense block network)、ESRGAN(enhanced super-resolution generative adversarial networks)(Wang 等,2018)和 RCAN(residual channel attention networks)(Zhang 等,2018)等。本文利用超分辨率网络生成 HR 空域图像,然后以浮点型精度下采样

HR 图像获得量化误差边信息，从而调整初始失真实现最优嵌入。

为了更好地估计下采样边信息，本文对比了多种超分辨率网络和调整失真的策略。值得注意的一点是，与超分辨率任务中所追求的感知指标不同，如峰值信噪比（peak signal to noise ratio，PSNR）、结构相似度（structural similarity，SSIM）等，本文区分用于边信息估计隐写的好坏，是通过对抗隐写分析的检测能力来衡量的。最终本文选择了使用残差通道注意力机制网络 RCAN 生成对应载体的 HR 图像，之后以浮点型精度下采样 HR 图像得到与载体图像同分辨率的参考图像，即未量化载体；利用未量化载体和载体对应像素点之间差值的极性决定初始失真的调整方向，并对初始失真以不同权重进行调整获得非对称失真。实验表明，利用本文方法，在抵抗基于手工特征和基于深度学习的隐写分析器时，相对于传统对称失真隐写，大幅提升了隐写安全性，接近甚至在某些情况下超过原始边信息的隐写安全性能。

1 相关工作

1.1 空域图像原始边信息隐写

Denemark 和 Fridrich（2015）提出原始边信息隐写，通过利用载体对应的原始图像，即预载体，在图像处理过程中产生的量化误差，调整载体元素 ±1 修改的初始失真，使得隐写安全性得到显著提升。先回顾基于下采样处理获取空域图像原始边信息的隐写。

定义 $\boldsymbol{u}=(u_1,u_2,\cdots,u_n)$ 为 HR 图像下采样之后未量化取整的像素值，$\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$ 为量化取整后的载体像素值，即 $\boldsymbol{x}=\mathrm{round}(\boldsymbol{u})$，其中 round( ) 为四舍五入取整函数；$\boldsymbol{y}=(y_1,y_2,\cdots,y_n)$ 为载密图像像素值。根据载体像素点 x_i 的量化误差 $e_i=u_i-x_i(|e_i|\leqslant 0.5,1\leqslant i\leqslant n)$ 调整 x_i ±1 的初始失真 $\rho_i^{(A)}$，即

$$\begin{cases}\rho_i^{(\mathrm{SI})+}=(1-2|e_i|)\rho_i^{(A)} & y_i=x_i+\mathrm{sign}(e_i)\\ \rho_i^{(\mathrm{SI})-}=\rho_i^{(A)} & y_i=x_i-\mathrm{sign}(e_i)\end{cases} \tag{1}$$

式中，$\boldsymbol{A}$ 为各种对称失真函数的集合，$\rho_i^{(A)}$ 可以由任意的对称失真函数计算得到，$\rho_i^{(\mathrm{SI})\pm}$ 则代表原始边信息隐写方法的非对称失真。用 SI-$\boldsymbol{A}$ 表示以 $\boldsymbol{A}$ 为初始失真函数的原始边信息隐写方法。在上述失真调整过程中，若修改后的像素值 y_i 更接近于取整前的像素值 u_i，则给这个修改赋予较小的失真，从而引导隐写后的图像更接近于图像的原始状态。

在嵌入秘密消息的过程中，对于最优嵌入模拟器（Pevný 等，2010），可以由边信息调整得到的修改失真计算出对应的修改概率 $\pi_i^{(\pm)}$。$\pi_i^{(\pm)}$ 可以由 $\rho_i^{(\mathrm{SI})\pm}$ 和 λ 计算得到，即

$$\pi_i^{(\pm)}=\frac{\exp(-\lambda\rho_i^{(\mathrm{SI})\pm})}{1+\exp(-\lambda\rho_i^{(\mathrm{SI})+})+\exp(-\lambda\rho_i^{(\mathrm{SI})-})} \tag{2}$$

式中，λ 值计算为

$$m=-\sum_{i=1}^{n}(\pi_i^{(+)}\log_2\pi_i^{(+)}+\pi_i^{(-)}\log_2\pi_i^{(-)}+(1-\pi_i^{(+)}-\pi_i^{(-)})\log_2(1-\pi_i^{(+)}-\pi_i^{(-)}) \tag{3}$$

式中，m 是嵌入消息的比特长度。Filler 和 Fridrich（2010）证明式（3）右侧的熵在 λ 上是单调递减的，所以在可行域内给定一个消息长度 m，λ 可以通过二分搜索方法快速确定。

1.2 超分辨率网络

本文要解决如何准确估计预载体的问题，因此为了尽可能准确地恢复原始的高分辨率图像，以获得相应的下采样边信息，利用几个超分辨率网络估计 HR 预载体图像。相关网络的主要特性包括：

1）基于生成对抗网络的超分模型 SRGAN（Ledig 等，2017）。SRGAN 使用深度残差网络 SRResNet（Ledig 等，2017）作为生成器，使用 VGG（Visual Geometry Group）网络（Mahendran 和 Vedaldi，2016）作为判别器。其中 SRResNet 以均值平方误差（mean square error，MSE）为失真函数进行优化，在 PSNR 和 SSIM 指标上具有非常优秀的表现，而 SRGAN 由于加入了判别器，内容感知损失和对抗损失作为失真函数，更加注重结果的真实性。

2）加强的深度残差网络 EDSR（Lim 等，2017）。EDSR 在 SRResNet 的基础上去掉了标准化层（batch normalization，BN）。原因在于超分辨率任务与计算机视觉领域的其他任务（比如图像识别、目标检测）的区别：前者的输出是具体的像素值，而后者只需要输出一个标签。在 BN 层去均值操作之后，输出更像一个相对值，并不利于超分任务。对于不同的面向 PSNR 的任务，比如超分辨率和去模糊任务，去掉 BN 层已经被证明能够提高表现和减小计算复杂度。

3)加强的基于生成对抗网络的超分模型 ESRGAN(Wang 等,2018)。ESRGAN 在 SRGAN 的基础上针对网络结构、对抗损失和感知损失进行改进:提出残差—残差密集块(residual in residual dense block,RRDB),将多层残差和密集连接相结合,同时也去掉了所有 BN 层;对抗网络借鉴 RaGAN(relativistic average generative adversarial networks)结构(Jolicoeur-Martineau,2018),SRGAN 中的判别器用于估计输入到判别器中的图像是真实且自然图像的概率,而 ESRGAN 的判别器则尝试估计真实图像相对伪造图像来说更逼真的概率;改进感知损失,使用激活之前的 VGG 特征,会提供更尖锐的边缘和更符合视觉的结果。

4)深度残差通道注意力网络 RCAN(Zhang 等,2018)。作者认为在 LR 图像的输入和特征中,包含了大量的低频信息,而这些信息在通道间被同等对待,阻碍了卷积神经网络的表征能力;同时越深的图像超分网络越难训练。所以作者提出了残差嵌套(residual in residual,RIR)结构,以构造非常深的可训练网络。RIR 中的长跳连接和短跳连接有助于绕过大量的低频信息,使主网络学习到更有效的信息。此外,作者引入通道注意力(channel attention,CA)机制,目的是区别对待不同的特征通道,自适应地调整不同通道的权重,并和残差思想融合,确保信息在网络中的流动,加快网络训练速度。

2 基于超分辨率网络的空域图像边信息估计隐写

2.1 本文方法框架

本文研究图像下采样过程中的边信息对于隐写过程的帮助,方法框架如图 1。其中超分辨率网络由成对的图像训练;图中的初始失真可由任意失真函数 $\boldsymbol{A}$ 获得,比如在本文中 $\boldsymbol{A}\in\{\text{HILL},\text{SUNIWARD}\}$;量化误差为未量化载体与载体的差值。本文中的下采样过程均采用 MATLAB 中的标准双三次插值函数。

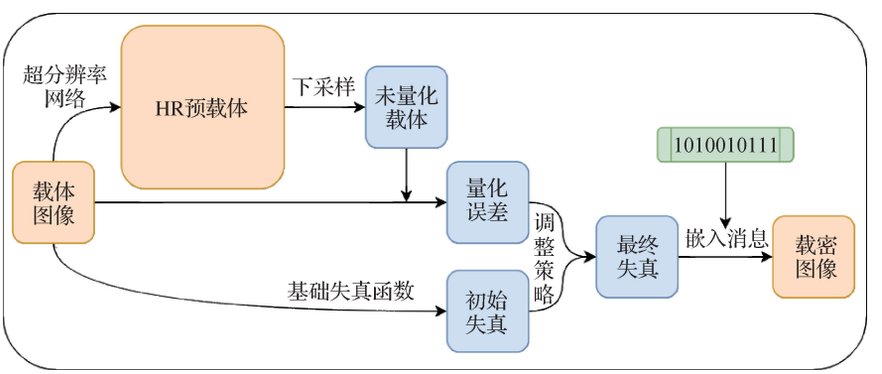


图 1 基于超分辨率网络的图像边信息估计隐写框架

Fig. 1 Framework for image side information estimation steganography based on super-resolution network

根据已有的空域图像原始边信息隐写(Denemark 和 Fridrich,2015)和 JPEG 图像的边信息估计隐写(Li 等,2020a),采用用于空域图像边信息估计隐写的失真调整策略 SIEp-$\boldsymbol{A}$。定义 $\hat{\boldsymbol{u}}=(\hat{u}_1,\hat{u}_2,\cdots,\hat{u}_n)$ 为估计的 HR 预载体经过下采样后未量化取整的像素值,图 1 中的减号表示估计的量化误差为 $\hat{e}_i=\hat{u}_i-x_i$。由于估计的预载体不够准确,使得量化误差 $\hat{e}_i$ 不再像 SI-$\boldsymbol{A}$ 一样限制在[-0.5,0.5]内,而且极性方向相对于精准的幅度大小来说更容易估计,所以 SIEp-$\boldsymbol{A}$ 只利用估计的量化误差的极性方向来指导失真调整,即在与量化误差方向一致的修改方向上,赋予初始失真相同的调整系数来减小该方向的修改失真,使载密图像更接近图像的原始状态,即

$$\begin{cases}\rho_i^{(\text{SIEp})+}=\eta\cdot\rho_i^{(\boldsymbol{A})} & y_i=x_i+\text{sign}(e_i)\\ \rho_i^{(\text{SIEp})-}=\rho_i^{(\boldsymbol{A})} & y_i=x_i-\text{sign}(e_i)\end{cases}\tag{4}$$

式中,调整系数 $\eta\in[0,1]$。得到调整后的最终失真,即非对称失真后,便可以使用 STC(Filler 等,2011)或 SPC(Li 等,2020b)等执行消息嵌入过程。

2.2 超分网络的选择

2.2.1 超分辨率网络的性能比较

使用两个指标来评价不同的超分辨率网络结构对于预载体图像估计好坏。第 1 个指标是估计的高分辨率图像和原始高分辨率图像之间的 PSNR 值,即

超分辨率任务中通常追求的指标;第 2 个指标是量化误差 $\hat{e}_i$ 的极性被正确估计的比例 R_P(Li 等, 2020a)。一般来说,越高的 PSNR 和代表估计的预载体越接近原始高分辨率图像。以下是实验设置和结果对比:

1)训练和测试。使用隐写领域常用的 3 个数据集, BOSSBase (break our steganographic system) 1.01(Bas 等,2011),BOWS2(break our watermarking system 2) (Bas 和 Furon, 2007) 和 MRNC (mixed resized never-compressed) (Li 等,2015),分别包含 10 000 幅512 × 512 像素、10 000 幅 512 × 512 像素和 8 000 幅 768 × 768 像素的灰度图像。它们对应的下采样图像均采用 MATLAB 中的标准双三次插值函数获得。使用 BOSSBase 中的图像和对应下采样得到的 256 × 256 像素图像作为训练集进行训练,然后在 3 个数据库上进行测试。在获得超分图像之后,分别随机选择 1 000 幅图像测试其平均 PSNR 和 R_P,以初步评估超分网络的性能。

2)结果和分析。表 1 为基于上述相关网络和 3 个传统插值方法(Nearest、Bilinear 和 Bicubic)在 2 倍和 4 倍上采样生成的 HR 图像后与原始图像之间的平均 PSNR 和 R_P,数值越高在一定程度上反映生成的 HR 图像质量越好。可以看出,在上采样比例为 2,即图像宽和高分别放大 2 倍的情况下,RCAN 几乎在全部数据库上达到了最优值,而上采样比例为 4 时,RRDBNet 和 EDSRL 表现较好,但整体效果都相对较差。因为上采样比例越高,对于超分辨率网络的性能要求越高,越难以得到准确的 HR 图像,所以本文方法采用上采样比例为 2 的超分辨率网络估计预载体。值得注意的是,基于传统插值的方法得到的正确率 R_p 同样具有较高水平,甚至高于 EDSRL 所得到的结果,本文指出较高的 R_p 并不能完全对应较高的隐写安全性。

表 1　不同上采样方法在缩放比例为 2 或 4 时生成的图像与原始图像之间的 PSNR 和极性估计正确率 R_p

Table 1　The PSNR and correct rate of polarity estimation(R_p) between the image generated and the original image by different upsampling methods when the scaling factor is 2 or 4

方法	缩放比例	PSNR(/dB)/R_p(/%)			缩放比例	PSNR(/dB)/R_p(/%)		
		BOSS	BOWS2	MRNC		BOSS	BOWS2	MRNC
Nearest	2	31.76/58.73	31.09/58.15	29.69/55.91	4	27.83/57.48	27.05/57.35	25.62/55.25
Bilinear		32.49/58.20	31.78/57.69	30.42/55.59		28.71/57.21	27.83/57.15	26.37/55.05
Bicubic		33.53/58.52	33.53/57.94	33.53/55.82		29.28/57.45	28.39/57.25	26.94/55.19
SRResNet		36.96/59.32	36.08/58.15	35.09/56.05		31.52/58.94	30.33/58.04	29.00/55.88
SRGAN		34.39/52.73	33.23/52.00	32.10/51.37		28.70/50.27	27.15/50.23	25.85/50.35
EDSRM		36.94/59.28	36.07/58.14	35.09/56.03		31.49/59.07	30.32/58.11	28.99/56.04
EDSRL		**37.24**/57.98	36.24/57.04	35.31/55.06		**31.92/59.32**	30.41/58.14	29.13/**56.08**
RRDBNet		37.21/59.56	**36.25**/58.27	35.31/56.14		31.74/59.31	**30.45/58.17**	**29.17/56.08**
ESRGAN		34.64/55.35	33.56/53.49	32.50/52.54		28.79/53.33	27.26/53.30	25.91/52.44
RCAN		37.23/**59.77**	**36.25/58.37**	**35.34/56.28**		31.79/57.40	30.44/56.77	29.16/54.98

注:加粗字体为每列最优值。

2.2.2　基于不同网络的边信息估计隐写的安全性

通过以下初步实验选定本文方法的网络结构。使用各个网络的最终训练模型来获取估计边信息,并根据式(4)进行失真调整。载体图像库为 BOSSBase 中 1 万幅尺寸为 256 × 256 像素的灰度图像,嵌入率为 0.4 bit/像素,初始失真函数使用 HILL (Li 等,2014),隐写分析过程在基于手工特征 SRM (spatial rich model) (Fridrich 和 Kodovsky, 2012) 的集成分类器(Kodovsky 等,2012) 上训练和测试,训练集和测试集按 1 ∶ 1 划分,使用检测错误率 P_e 作为安全性的观测指标,计算为

$$P_e = \min_{P_{FA}} \frac{P_{FA} + P_{MD}}{2} \tag{5}$$

式中,P_{FA} 和 P_{MD} 分别为误警率和漏警率,即将载体误认为载密的概率和将载密误认为载体的概率,该值越大说明隐写安全性越高。为了尽量消除随机性,本文所有检测错误率均取 10 次独立训练测试的平均值,实验结果见表 2。

表 2　SIEp-HILL 采用不同上采样方法及调整系数(η)时在 SRM 特征集上的检测错误率

Table 2　Detection error rate on SRM feature set when SIEp-HILL adopts different upsampling methods and factors η

/%

方法	调整系数									
	1.0	0.9	0.8	0.7	0.6	0.5	0.4	0.3	0.2	0.1
Bicubic	**26.90**	26.42	24.47	20.87	17.23	13.50	10.10	7.67	6.03	5.41
SRResNet	26.90	28.03	29.49	31.15	32.49	**33.46**	33.21	32.14	31.44	30.45
SRGAN	26.90	26.93	**27.17**	27.15	26.46	25.83	25.02	24.02	22.67	22.11
EDSRM	26.90	28.30	29.33	30.95	32.25	**33.08**	32.38	31.71	30.67	29.74
EDSRL	26.90	27.65	28.63	29.69	30.51	31.12	**31.15**	30.43	29.42	28.66
RRDBNet	26.90	28.03	29.49	31.15	32.49	**33.46**	33.21	32.14	31.44	30.45
ESRGAN	26.90	27.56	28.09	28.82	**29.43**	29.27	29.13	28.23	27.12	26.30
RCAN	26.90	28.14	29.99	31.31	32.99	**33.75**	33.46	32.75	31.68	31.03

注:加粗字体为每行最优值。

表 2 中展示了在上采样比例为 2 时,基于边信息估计隐写 SIEp-HILL,利用不同上采样方法在不同调整系数时所得到的检测错误率。其中,调整系数 $\eta=1.0$ 等价于初始失真不进行任何调整的情况。从表 2 中可以看出,RCAN、RRDBNet、EDSRM、SRResNet 均在 $\eta=0.5$ 时获得了各自最优值,并且 RCAN 获得了所有结果中最高的 6.85% 的提升。基于此,本文选择 RCAN 作为上采样网络,生成 HR 预载体,对应的边信息估计隐写方法命名为 SIEp(RCAN×2)-***A***。

此外,表 1 中两个基于生成对抗的网络(SRGAN 和 ESRGAN)分别在面向 PSNR 的网络(SRResNet 和 RRDBNet)基础上加入对抗网络,导致 PSNR 值有所降低,但它们面向生成更具真实性的图像,这对于超分任务本身是有益的。从表 2 中可以看出,使用两种基于生成对抗的网络(SRGAN 和 ESRGAN)估计下采样边信息,对于隐写安全性提升不明显。从表 1 和表 2 中发现,超分网络获得的 PSNR 较高时,会带来更高的安全性提升,因此面向高水平 PSNR 的超分网络或将更适合用来估计下采样边信息,而追求估计图像的真实性并不一定更有效。隐写领域与计算机视觉领域不同,前者只需要得到接近原始图像的相关性,而后者还需要考虑真实性。

另外,基于 MATLAB 中标准双三次插值函数(Bicubic)估计的边信息使得隐写的安全性大幅度降低,表明了基于传统插值的上采样方法即使具有较高的极性估计正确率,也不能为隐写提供有效的边信息。

3　实　验

本文实验在 BOSSBase、BOWS2、MRNC 数据库上进行,初始失真函数采用 HILL(Li 等,2014)和 SUNIWARD(Holub 和 Fridrich,2013),消息嵌入使用最优模拟嵌入(Pevny 等, 2010),并采用基于手工特征的和基于深度学习的隐写分析器评估隐写安全性。

对于不同数据集、不同的嵌入率情况,可以通过遍历所有调整系数来确定不同嵌入率时的最优调整系数,所以如果为了获得更高的安全性,可以耗费更多的代价,通过遍历来获得更优的调整系数。

但是从实际应用考虑,分析表 2 和表 3,可以看出,在 3 种数据集、不同嵌入率情况下,虽然最优调整系数稍有不同,但是在调整系数为 0.5 时,均能显著提高安全性,并且和最优调整系数下的安全性差距很小,所以本文取 0.5 作为实际实验中的调整系数。

3.1　本文方法在跨库上的隐写安全性

由于本文的超分网络模型基于 BOSSBase 库中的 512×512 像素和 256×256 像素图像对训练,为了证明本文方法利用的估计边信息对于嵌入修改的方向具有普适的指导作用,而不是超分网络单纯地学到了本数据库内的 HR 图像和 LR 图像的对应关

系。以训练集之外的图像库作为载体,分别采用 HILL 和 SUNIWARD 作为初始失真函数进行边信息估计隐写,并抵抗 SRM 和 SRNet(steganalysis residual network)(Boroumand 等, 2019)隐写分析。

表 3　不同嵌入率、不同调整系数在 BOWS 和 MRNC 上的安全性(隐写分析器的检测错误率)

Table 3　The security of different adjustment factors on BOWS and MRNC at different embedding rates

/%

数据集	嵌入率/(bit/像素)	隐写算法	调整系数				
			0.6	0.55	0.5	0.45	0.4
BOWS	0.1	SIEp-SUNIWARD	**48.01**	47.96	48.01	47.56	47.33
		SIEp-HILL	48.36	48.61	**48.73**	48.53	48.43
	0.3	SIEp-SUNIWARD	**37.46**	37.29	37.30	37.33	37.21
		SIEp-HILL	40.82	41.16	41.44	**41.85**	41.80
	0.5	SIEp-SUNIWARD	25.28	**25.37**	25.32	24.74	24.54
		SIEp-HILL	30.72	31.39	31.77	31.78	**31.80**
MRNC	0.1	SIEp-SUNIWARD	**47.59**	47.55	47.50	47.32	46.98
		SIEp-HILL	48.22	**48.63**	48.50	48.39	48.38
	0.3	SIEp-SUNIWARD	37.91	**38.08**	37.72	37.68	37.06
		SIEp-HILL	45.55	45.46	45.59	**45.80**	45.77
	0.5	SIEp-SUNIWARD	28.67	**28.75**	28.41	28.23	27.71
		SIEp-HILL	33.65	34.37	34.64	**34.76**	34.40

注:加粗字体为每行的最优值。

3.1.1　抵抗 SRM 隐写分析的安全性

在 BOWS2 库中 256×256 像素大小的图像和 MRNC 库中 384×384 像素大小的图像上使用本文方法 SIEp(RCAN×2)。在不同嵌入率下,与初始失真 HILL 和 SUNIWARD 方法的安全性对比结果如表 4。

表 4　调整系数为 0.5 时本文方法在 BOWS2 和 MRNC 上对抗 SRM 的安全性(隐写分析器的检测错误率)

Table 4　While the adjustment coefficient is 0.5, the security of the proposed method against SRM on BOWS2 and MRNC

/%

数据集	隐写算法	嵌入率/(bit/像素)				
		0.1	0.2	0.3	0.4	0.5
BOWS2	SUNIWARD	45.66	38.16	30.83	24.66	19.43
	SIEp-SUNIWARD	48.01	43.38	37.30	30.98	25.32
	HILL	46.99	41.88	35.97	30.19	25.10
	SIEp-HILL	48.73	45.46	41.44	36.63	31.77
MRNC	SUNIWARD	45.25	38.27	32.85	27.97	23.36
	SIEp-SUNIWARD	47.50	42.81	37.72	33.11	28.41
	HILL	46.70	42.19	37.33	33.09	28.98
	SIEp-HILL	48.50	45.59	42.14	38.42	34.64

从表4中可以看出,本文方法在训练集之外的数据集上同样能够有效提升隐写安全性,嵌入率越高,提升效果越大,如在BOWS2库中,SIEp(RCAN×2)-HILL比HILL在0.5 bit/像素时提升6.67%;在MRNC库中,SIEp(RCAN×2)-HILL比HILL在0.5 bit/像素时提升5.66%。注意,这里采用的载体图像是已知经过MATLAB中标准双三次插值下采样得到的。

为了证明本文方法可以应用于不同来源,如来自于不同的原始尺寸,或者并非单纯地直接通过MATLAB中标准双三次插值下采样获得的载体上。比如BOSSBase(Bas等,2011)由来自7个不同摄像机的10 000幅从未压缩过的图像组成。该数据库中所有图像均以RAW(raw image format)格式(CR2(camera raw 2)或DNG(digital negative))的全分辨率彩色图像创建,首先调整图像大小,使较小的一边长为512,然后将其裁剪为512×512像素大小,最后转换色彩为数据库中的灰度图像。

以BOSSBase中512×512像素大小的图像为载体,在嵌入率0.4 bit/像素下,评估本文方法的有效性和安全性。图2中,本文方法基于两种初始失真函数,分别在调整系数为0.55和0.65时达到最大提升:4.04%和4.0%,再次证明本文方法利用估计的下采样边信息对于嵌入修改方向的指导是有意义的,也说明了本文方法具有普适性。

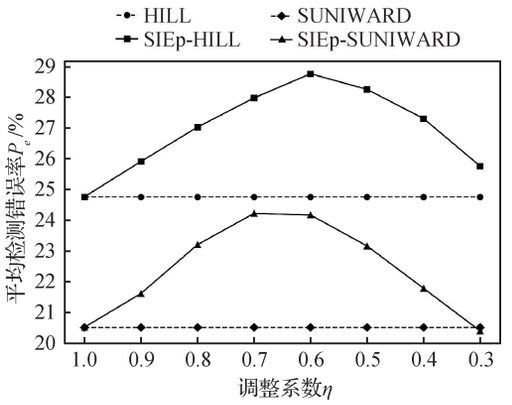


图2 本文方法在BOSSBase 512×512像素灰度图像上的安全性

Fig. 2 The security of the proposed method on BOSSBase 512×512 pixel grayscale image

3.1.2 抵抗SRNet隐写分析的安全性

现代隐写分析方法除了传统的基于手工特征的集成分类器检测,还有基于深度学习的隐写分析网络。采用具有代表性的深度学习隐写分析网络SRNet,并按照建议的实验设置训练网络。

设置学习率l_1为0.001,l_2为0.000 1;对于嵌入率为0.4 bit/像素的载体载密图像对的隐写分析直接以l_1迭代400 000次,然后以l_2迭代100 000次,并选取最后100 000次迭代中在验证集上检测错误率最低的模型作为最终的检测器;对于其他嵌入率的情况,首先基于0.4 bit/像素的载体载密图像对,以l_1迭代80 000次,再以l_2迭代50 000次,取最后50 000次迭代过程中在验证集上表现最优的模型作为其他嵌入率情形下的预检测器。

表5为本文方法以BOWS2库上256×256像素的图像为载体隐写,以检测错误率P_e为指标评估对抗SRNet的安全性。可以看出,在基于HILL和SUNIWARD两种初始失真函数的各个嵌入率下,隐写安全性均有明显提升;其中以SUNIWARD为初始失真函数,嵌入率为0.2 bit/像素时,本文方法的安全性相比传统SUNIWARD提升11.5%。

3.2 本文方法与原始边信息隐写安全性的对比

Denemark和Fridrich(2015)使用原始边信息隐写方法证明了下采样边信息对于提升隐写安全的有效性。受该工作启发,探究边信息估计隐写与原始边信息隐写的区别。

在不同嵌入率下对比了本文方法与原始边信息隐写的安全性,实验以BOSSBase中256×256像素的灰度图像为载体。表6是两种方法分别对抗SRM特征和SRNet隐写分析的检测错误率和相对于初始对称失真隐写方法安全性的提升,其中边信息估计过程采用RCAN×2网络,调整系数为0.5。

可以看出,在不同嵌入率下,本文方法虽然总能在原始对称失真的基础上明显提升安全性,但距离原始边信息所带来的提升仍有一定差距,尤其是在以SUNIWARD为初始失真时的差距较大。主要原因在于以下两点:1)本文使用超分辨率网络恢复得到的高分辨率图像没有原始图像准确;2)本文使用的失真调整策略相对简单,很难将图像下采样过程中产生的量化误差对于失真调整的指导发挥到极致。

为了进一步探究本文方法和原始边信息隐写的差异,图3展示了不同修改失真在嵌入率为0.4 bit/像素的情况下,嵌入修改点的数量和分布。可以看出,相比传统隐写,原始边信息隐写造成了更多的修改点,并且分布相对均匀;而同样相比传统隐写,本文方法造成的修改点数量仅有略微增多,而且分布

表 5　调整系数为 0.5 时，本文方法在 BOWS2 上对抗 SRNet 的安全性（检测错误率）

Table 5　While the adjustment coefficient is 0.5, the security of the method in this paper against SRNet on BOWS2

/%

隐写算法	嵌入率/（bit/像素）				
	0.1	0.2	0.3	0.4	0.5
SUNIWARD	37.9	25.3	17.5	12.9	8.6
SIEp-SUNIWARD	45（↑7.1）	36.8（↑11.5）	26（↑8.5）	20.2（↑7.3）	13.8（↑5.2）
HILL	37.8	27.7	20.9	16.6	13.5
SIEp-HILL	43.6（↑5.8）	36.2（↑8.5）	29.6（↑8.7）	23.1（↑6.5）	20.4（↑6.9）

注：（↑）括号内数值为相对传统方法的提升。

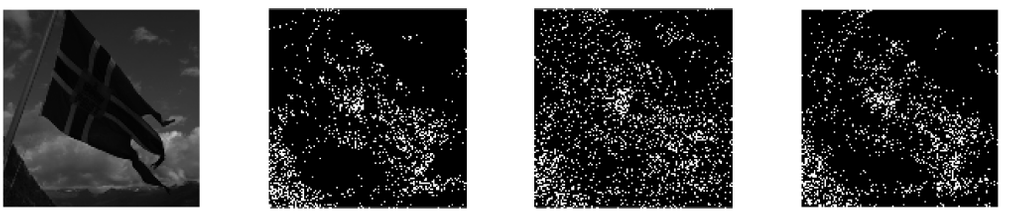
表 6　调整系数为 0.5 时，本文方法 SIEp（RCAN×2）和 SI 在不同嵌入率下的安全性对比实验（检测错误率）

Table 6　While the adjustment coefficient is 0.5, the security comparative experiment between the proposed SIEp（RCAN×2）and SI under different bpp

/%

隐写分析	隐写算法	嵌入率/（bit/像素）				
		0.1	0.2	0.3	0.4	0.5
SRM	SUNIWARD	41.36	33.63	26.76	21.47	17.21
	SI-SUNIWARD	46.36（↑5.1%）	41.2（↑7.57%）	35.82（↑9.06%）	29.83（↑8.36%）	24.47（↑7.26%）
	SIEp-SUNIWARD	45.33（↑4.07%）	39.42（↑5.79%）	33.34（↑6.58%）	28.04（↑6.92%）	23.23（↑6.02%）
	HILL	44.22	37.87	31.78	26.90	22.54
	SI-HILL	45.83（↑1.61%）	43.48（↑5.61%）	39.93（↑8.15%）	35.17（↑8.27%）	29.98（↑7.81%）
	SIEp-HILL	46.81（↑2.59%）	42.66（↑4.79%）	38.46（↑6.68%）	33.75（↑6.85%）	29.16（↑6.62%）
SRNet	SUNIWARD	30.7	19.9	14.3	11.3	7.7
	SI-SUNIWARD	46.1（↑15.4%）	43.1（↑23.2%）	33.4（↑19.1%）	25.3（↑14%）	16.9（↑9.2%）
	SIEp-SUNIWARD	38.3（↑7.6%）	27.6（↑7.7%）	22.5（↑8.2%）	17.1（↑5.8%）	12.4（↑4.7%）
	HILL	33.3	25.2	19.3	15.8	12.4
	SI-HILL	44.5（↑11.2%）	38.2（↑13%）	31.5（↑12.2%）	24.7（↑8.9%）	19.8（↑7.4%）
	SIEp-HILL	40.6（↑7.3%）	33.0（↑7.8%）	28.5（↑9.2%）	21.9（↑6.1%）	20.4（↑8%）

注：（↑）括号内数值为相对传统方法的提升。



(a) BOSSBase库72.pgm (256×256 像素)　(b) HILL (5 400 个修改点)　(c) 原始边信息隐写 (7 496 个修改点)　(d) 本文边信息估计隐写 (5 843 个修改点)

图 3　载体和不同失真函数在嵌入率 0.4 bit/像素时的嵌入修改点分布图

Fig. 3　The cover and the embedding modified point distribution based on different distortion functions at the embedding rate of 0.4 bit/pixel ((a) '72. pgm' in the BOSSBase library with a size of 256×256 pixel; (b) HILL; (c) original side information steganography; (d) the side information estimated steganography of this paper)

相似,这说明基于边信息估计的隐写修改和基于原始边信息的隐写虽然都极大地提升了隐写安全性,但是其修改模式是不同的。

值得注意的是,在以 HILL 计算初始失真,嵌入率为 0.1 bit/像素,对抗 SRM 隐写分析时,本文方法的安全性超过了基于原始边信息的隐写 1.08%;且在嵌入率为 0.5 bit/像素,对抗 SRNet 隐写分析时,本文方法的安全性超越原始边信息隐写 0.6%。证明本文方法的性能接近(对抗 SRM)甚至在某些情形下超过(对抗 SRNet)原始边信息隐写的安全性。

4 结 论

本文工作的主要贡献有:1)提出利用估计的下采样边信息指导初始失真的修改方向,以提高隐写安全性;2)提出使用超分辨率网络估计原始高分辨率图像,从而获得估计的下采样边信息。

首先介绍了已有的空域的原始边信息隐写和 JPEG 域中的边信息估计隐写方法,然后介绍了本文使用的一些超分辨率网络的结构和特性,并基于已有的 JPEG 域中边信息估计隐写失真调整策略实施本文的初始失真调整策略。

以 PSNR 和极性估计准确率为指标初步评估生成的高分辨率图像的准确度,同时探索这两个指标与隐写安全性的提高是否具有关联性。在对于使用不同超分辨率网络时的隐写安全性进行初步评估之后,选择残差通道注意力网络 RCAN 作为估计高分辨率预载体的网络。在实验部分,为了表明本文方法的有效性和广泛适用性,在训练集图像库之外的载体上测试了本文方法在抵抗 SRM 和 SRNet 隐写分析的安全性,均有明显提升。进一步与原始边信息隐写的安全性进行对比,发现本文方法的性能接近甚至在部分情况下超越了原始边信息隐写的安全性,同时通过分析修改点分布,认为基于边信息估计隐写的修改模式与原始边信息隐写是不同的。

为了进一步提升本文方法的安全性,有两个关键方面值得考虑:1)边信息估计网络的选择,希望能够选择对隐写安全性有更大提升的超分辨率网络甚至是其他领域的网络结构;2)本文的失真调整策略过于简单,很可能没有完全发挥估计边信息的潜力。下一步将寻找更合适的边信息估计方法和更优的失真修改策略,同时考虑将本文方法扩展到 JPEG 域中。

参考文献(References)

Bas P and Furon T. 2007. Bows-2 contest (break our watermarking system) [EB/OL]. [2021-06-22]. http://bows2.ec-lille.fr/

Bas P, Filler T and Pevny T. 2011. "Break Our Steganographic System": the ins and outs of organizing BOSS//Filler T, Pevny T, Craver S and Ker A, eds. Information Hiding. Prague, Czech Republic: Springer: 59-70 [DOI: 10.1007/978-3-642-24178-9_5]

Boroumand M, Chen M and Fridrich J. 2019. Deep residual network for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 14(5): 1181-1193 [DOI: 10.1109/TIFS.2018.2871749]

Denemark T and Fridrich J. 2015. Side-informed steganography with additive distortion//Proceedings of 2015 IEEE International Workshop on Information Forensics and Security (WIFS). Roma, Italy: IEEE: 1-6 [DOI: 10.1109/WIFS.2015.7368589]

Filler T and Fridrich J. 2010. Gibbs construction in steganography. IEEE Transactions on Information Forensics and Security, 5(4): 705-720 [DOI: 10.1109/TIFS.2010.2077629]

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. 2006. Minimizing the embedding impact in steganography//Proceedings of the 8th Workshop on Multimedia and Security. Geneva, Switzerland: ACM: 2-10 [DOI: 10.1145/1161366.1161369]

Fridrich J and Kodovsky J. 2012. Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 7(3): 868-882 [DOI: 10.1109/TIFS.2012.2190402]

Holub V and Fridrich J. 2012. Designing steganographic distortion using directional filters//Proceedings of 2012 IEEE International Workshop on Information Forensics and Security (WIFS). Costa Adeje, Spain: IEEE: 234-239[DOI: 10.1109/WIFS.2012.6412655]

Holub V and Fridrich J. 2013. Digital image steganography using universal distortion//Proceedings of the 1st ACM Workshop on Information Hiding and Multimedia Security. Montpellier, France: ACM: 59-68 [DOI: 10.1145/2482513.2482514]

Jolicoeur-Martineau A. 2018. The relativistic discriminator: a key element missing from standard GAN [EB/OL]. [2021-05-08]. https://arxiv.org/pdf/1807.00734v3.pdf

Kodovsky J, Fridrich J and Holub V. 2012. Ensemble classifiers for steganalysis of digital media. IEEE Transactions on Information Forensics and Security, 7(2): 432-444 [DOI: 10.1109/TIFS.2011.2175919]

Ledig C, Theis L, Huszár F, Caballero J, Cunningham A, Acosta A, Aitken A, Tejani A, Totz J, Wang Z H and Shi W Z. 2017. Photo-

realistic single image super-resolution using a generative adversarial network//Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Honolulu, USA: IEEE: 105-114 [DOI: 10.1109/CVPR.2017.19]

Li B, Wang M, Huang J W and Li X L. 2014. A new cost function for spatial image steganography//Proceedings of 2014 IEEE International Conference on Image Processing (ICIP). Paris, France: IEEE: 4206-4210 [DOI: 10.1109/ICIP.2014.7025854]

Li B, Wang M, Li X L, Tan S Q and Huang J W. 2015. A strategy of clustering modification directions in spatial image steganography. IEEE Transactions on Information Forensics and Security, 10(9): 1905-1917 [DOI: 10.1109/TIFS.2015.2434600]

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, 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]

Lim B, Son S, Kim H, Nah S and Lee K M. 2017. Enhanced deep residual networks for single image super-resolution//Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). Honolulu, USA: IEEE: 1132-1140 [DOI: 10.1109/CVPRW.2017.151]

Mahendran A and Vedaldi A. 2016. Visualizing deep convolutional neural networks using natural pre-images. International Journal of Computer Vision, 120(3): 233-255 [DOI: 10.1007/s11263-016-0911-8]

Pevny T, Filler T and Bas P. 2010. Using high-dimensional image models to perform highly undetectable steganography//Böhme R, Fong P W L and Safavi-Naini R, eds. Information Hiding. Canada: Berlin Heidelberg: Germany: Springer: 161-177 [DOI: 10.1007/978-3-642-16435-4_13]

Sedighi V, Fridrich J and Cogranne R. 2015. Content-adaptive pentary steganography using the multivariate generalized Gaussian cover model//Proceedings Volume 9409, Media Watermarking, Security, and Forensics 2015. San Francisco, USA: SPIE: 94090H [DOI: 10.1117/12.2080272]

Wang X T, Yu K, Wu S X, Gu J J, Liu Y H, Dong C, Qiao Y and Loy C C. 2018. ESRGAN: enhanced super-resolution generative adversarial networks//Proceedigns of European Conference on Computer Vision-ECCV 2018 Workshops. Munich, Germany: Springer: 63-79 [DOI: 10.1007/978-3-030-11021-5_5]

Wang Z C, Lv J P, Wei Q D and Zhang X P. 2016. Distortion function for spatial image steganography based on the polarity of embedding change//Shi Y Q, Kim H J, Perez-Gonzalez F and Liu F, eds. Digital Forensics and Watermarking. Beijing, China: Springer: 487-493 [DOI: 10.1007/978-3-319-53465-7_36]

Zhang Y L, Li K P, Li K, Wang L C, Zhong B N and Fu Y. 2018. Image super-resolution using very deep residual channel attention networks//Proceedings of European Conference on Computer Vision-ECCV 2018. Munich, Germany: Springer: 294-310 [DOI: 10.1007/978-3-030-01234-2_18]

作者简介

赵鑫，1999 年生，男，硕士研究生，主要研究方向为图像隐写。
E-mail: zhaoxin0924@mail.ustc.edu.cn

张卫明，通信作者，男，教授，主要研究方向为多媒体内容安全与人工智能安全。
E-mail: zhangwm@ustc.edu.cn

王垚飞，男，博士研究生，主要研究方向为图像隐写。
E-mail: yaofei@mail.ustc.edu.cn

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

俞能海，男，教授，主要研究方向为多媒体内容安全、多媒体内容检索与视频处理。E-mail: ynh@ustc.edu.cn