Modeling and Simulation 建模与仿真, 2025, 14(4), 1225-1239
Published Online April 2025 in Hans. https://www.hanspub.org/journal/mos
https://doi.org/10.12677/mos.2025.144368

Hans汉斯

基于深度学习的密钥控制多图隐写技术研究

朱嘉伟，建一飞

上海理工大学光电信息与计算机工程学院，上海

收稿日期：2025年3月30日；录用日期：2025年4月23日；发布日期：2025年4月30日

摘　要

本研究提出了一种基于可逆神经网络的密钥控制的多图像隐写方案(SDRNN)，以提升安全性和视觉质量。采用私钥加密确保信息安全性，即便算法公开也能保护秘密信息，增强抗攻击能力。针对高容量隐写常见的视觉伪影问题，设计了SCDense模块，通过选择性通道密集连接优化信息嵌入，有效减少轮廓阴影和颜色失真。实验结果表明，相比现有方法，本方案在峰值信噪比(PSNR)和结构相似性(SSIM)等指标上有显著提升，提高了隐写图像的质量和鲁棒性。这显示了该方法不仅理论上有价值，在实际应用中也更可靠、适应性更强。

关键词

图片隐写，密钥，可逆神经网络，多图

Deep Learning-Based Key-Controlled Multi-Image Steganography

Jiawei Zhu, Yifei Jian

School of Optical-Electronical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai

Received: Mar. 30th, 2025; accepted: Apr. 23rd, 2025; published: Apr. 30th, 2025

Abstract

This study proposes a deep learning-enabled, key-controlled multi-image steganographic framework (SDRNN) to enhance security and visual quality. Private key encryption ensures information security, protecting secret information even with public algorithm disclosure, thereby strengthening attack resistance. Addressing common visual artifacts in high-capacity steganography, we design an SCDense module that optimizes information embedding through selective channel dense connections, effectively reducing contour shadows and color distortion. Experimental results demonstrate

文章引用: 朱嘉伟, 建一飞. 基于深度学习的密钥控制多图隐写技术研究[J]. 建模与仿真, 2025, 14(4): 1225-1239.
DOI: 10.12677/mos.2025.144368

significant improvements in peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) compared to existing methods, enhancing both the quality and robustness of stego-images. This indicates the method's theoretical value and superior practical reliability/adaptability. The research presents a novel effective solution for multi-image steganography, particularly demonstrating notable advantages in security enhancement and visual quality preservation.

Keywords

Image Steganography, Secret Key, Reversible Neural Network, Multi-Image

1. 引言

图片隐写术是一种信息隐藏技术，旨在将秘密信息无缝嵌入到看似无害的载体中，以确保信息传递的高度隐蔽性和保密性。与之形成对比的是，数字水印技术则侧重于版权保护和内容认证。

在图片隐写术的应用场景中，其核心目标是保证即使通信渠道受到监控，第三方也难以察觉或提取出嵌入的秘密信息。这种方法通过利用人类感知系统的局限性，使得隐藏的数据几乎不可见，从而有效地维护了信息的隐秘传输。

现有的隐写方法可能被未经授权的实体破解，限制了它们在高安全需求环境中的应用。针对这一问题，我们的研究引入了一种基于可逆神经网络(Invertible Neural Network, INN)的私钥集成机制，应用于高容量图像隐写术中。此创新方案将特定的私钥嵌入到隐写过程中，即使隐写算法本身是公开的，也能保证只有持有正确私钥的一方能够提取出隐藏的信息。这不仅增强了数据的安全性，还通过直接在隐写过程中集成私钥，减少了对额外密钥传输的需求，从而降低了潜在的拦截风险。我们采用前沿的深度学习技术，并结合新颖的密钥管理策略，确保了该方法的有效性和安全性。此外，观察到当信息通过隐写通道传输时，大量的冗余信息干扰了后续秘密图片的提取，影响了秘密图片的质量，这启发我们提出了一个优化策略，即通过空间与通道重构卷积来改进性能，从而减少从秘密通道到主通道的冗余信息，进而提升图像隐写的整体性能和图像质量。主要贡献如下：1) 在基于深度学习的图像隐写术中，创新隐写方式，并为每一个秘密图片分配相应的密钥，提高了图像隐写术的隐蔽性与安全性。2) 为解决在图像隐写过程中，由于大量冗余信息干扰对图片质量的影响，提出了通过结合重构卷积与残差链接来减少冗余信息并提升图片质量的方法。

2. 相关研究

2.1. 传统隐写技术

图像隐写术的技术演进体现了从基础到高级、从单一到多元的发展过程，主要分为两大类：空间域(Spatial Domain)和变换域(Transform Domain)隐写技术。这两种方法分别通过不同的手段在图像中嵌入秘密信息。

空间域隐写术直接操作于图像的像素值上，通过改变像素数据来隐藏信息。其中，最低有效位替换法(Least Significant Bit, LSB) [1]是最具代表性的技术之一。LSB 的核心思想是替换载体图像像素值的最低有效位以嵌入秘密信息的二进制数据。尽管这种方法实现简单且计算效率高，但它在图像平滑区域容

易产生纹理复制伪影(Texture Copy Artifacts)，使得基于统计分析的检测方法(如卡方检测[2]、RS 分析[3]和梯度能量分析[4])能够较为容易地识别隐藏信息的存在。为克服这些局限性，研究者提出了像素值差分(Pixel Value Differencing, PVD)等改进技术[5]。PVD 方法通过动态调整相邻像素间的差异值来优化嵌入强度，从而在保证视觉质量的同时提升信息嵌入容量和隐蔽性。

在变换域隐写术中，研究者通过将图像转换到频域或其他数学空间，进一步提升了隐写术的鲁棒性和抗检测能力。例如，基于离散傅里叶变换(Discrete Fourier Transform, DFT)的隐写方法[6]利用频域系数的相位或幅值嵌入信息，具有较好的抗压缩和抗噪声能力；基于离散余弦变换(Discrete Cosine Transform, DCT)的方法[7]则通过修改中频系数实现信息嵌入，在 JPEG 压缩等场景下表现出较强的鲁棒性；而基于离散小波变换(Discrete Wavelet Transform, DWT)的隐写技术[8]则利用多分辨率分析特性，能够在不同尺度上嵌入信息，从而兼顾隐蔽性和嵌入容量。然而，变换域方法通常需要更高的计算复杂度，并且在嵌入效率和图像质量之间需要权衡，尤其是在高嵌入率条件下可能引入视觉伪影或信息失真。

2.2. 低容量图像隐写

近年来，深度学习方法被提出用于信息隐藏，并取得了比传统方法更好的性能。具体来说，Hayes [9]等人首先将 GAN 应用于信息隐藏任务，表明对抗训练方案能够有效地提升隐藏安全性；Volkhonskiy [10]等人提出的 SGAN 通过添加额外的判别网络来提高生成的隐写图像的自然性；Shi [11]等人提出的 SSGAN 使用 WGAN 架构作为生成器，GNCNN 作为判别器来提高隐写图像的质量；Tang [12]等人提出的 ASDL-GAN 尝试通过自动学习给定载体图像中的嵌入概率找到合适的隐藏位置；Zhang [13]等人提出了一种基于 Reed-Solomon 码的新指标来评估隐写算法的容量，并通过密集编码器实现了更高的负载。这些方法通常具有较高的隐藏安全性，即秘密信息不太可能被隐写分析工具检测到，但是它们只能隐藏少量的数据。

低容量信息隐藏的一个重要应用是知识产权保护，例如数字水印。具体而言，Zhu [14]等人提出了一种自动编码器来实现水印的嵌入和提取；基于此，Ahmadi [15]等人引入了一个带有残差连接的基于 CNN 的转换模块，以便在转换域中嵌入水印；Tancik [16]等人提出了一种名为 StegaStamp 的新框架，用于在物理照片中隐藏超链接并在解码后成功检索；Luo [17]等人通过使用生成器生成失真进一步增强了网络对未知失真的鲁棒性。对于数字水印而言，鲁棒性是最为重要的因素，要求在不同类型的失真下都能准确恢复秘密信息。然而，鲁棒性和安全性之间存在权衡。虽然上述方法对失真具有鲁棒性，但它们通常安全性较低，即隐藏的信息很容易被第三方检测到，这一缺点使得它们不适合用于秘密通信。

2.3. 高容量图像隐写

与低容量信息隐藏工作相比，图像隐写由于其需要的高容量而更具挑战性。作为隐写术的一个重要研究方向，图像隐写尝试将一整幅图像隐藏到另一幅图像中。不同于上述方法的是，它要求较大的隐藏容量。传统的图像隐写方法试图在空间域嵌入信息。作为先驱工作之一，最低有效位(LSB)方法通过替换载体图像中的 n 个最低有效位为秘密图像的 n 个最高有效位来在空间域隐藏信息。受 LSB 的启发，一些基于像素值差异的改进方法被提出，包括 LSB 替换、LSB 匹配和多比特平面图像隐写等。然而，空间域算法的主要缺点是会出现纹理复制伪影，因此隐写分析方法可以轻易检测到由空间域算法隐藏的秘密信息。

为了克服传统方法的缺点，最近提出了一些基于深度学习的图像隐写方法。具体来说，Baluja [18]首次提出使用深度神经网络将一整幅彩色图像隐藏到另一幅图像中。为此，开发了一个准备网络来提取秘密图像的有用特征，然后使用一个隐藏网络将这些特征融合到载体图像中。最后，采用一个揭示网络恢复原始的秘密图像。Weng [19]等人进一步将这一技术应用于视频隐写，通过时间残差建模实现。Wu 等人[20] [21]则采用 U-Net 编解码器架构，设计了一种高效的图像隐写编解码器，通过多尺度特征提取和融

合，显著提升了隐藏容量和图像质量。为了获得更大的隐藏容量，Baluja [22]首先尝试将两张秘密图像拼接在一起并通过基于自动编码器的网络隐藏到一张载体图像中。Das [23]等人提出了 MISDNN，包含三个子网络：准备网络、隐藏网络和揭示网络。准备网络设计用于提取输入秘密图像的特征，然后将提取的特征与载体图像连接并通过隐藏网络生成隐写图像。在揭示过程中，分别部署了揭示网络从隐写图像中生成恢复的秘密图像。Lu [24]等人提出了一种可逆网络 ISN，将隐藏和恢复视为图像域中的一对逆问题。

2.4. 可逆神经网络

尽管基于 CNN 的方法在隐藏容量和功能性方面取得了显著进展，现有技术仍面临诸多挑战，包括隐写图像的视觉质量下降、抗检测能力不足以及提取过程中信息丢失严重等问题。为此，可逆神经网络(Invertible Neural Network, INN)被引入作为潜在的解决方案。INN 通过设计可逆的变换过程，能够在信息嵌入和提取阶段实现无损恢复，从而有效减少信息丢失并提升隐写图像的质量和安全性。

可逆神经网络最初由 Dinh [25]等人提出用于复杂的高维密度建模。给定一个变量 y 和前向计算 $x = f_u(y)$，可以直接通过 $y = f_u^{-1}(x)$ 恢复 y，其中逆函数 f_u^{-1} 被设计为与前向过程 f_u 共享相同的参数 u。为了使 INN 更好地处理图像处理任务，Dinh [26]等人在其耦合模型中引入了卷积层和多尺度层以减少计算成本并增强正则化能力。同样地，Kingma [27]等人提出了一个新的可逆网络 Glow，通过引入可逆的 1 × 1 卷积，这种方法在现实合成和图像操作方面被证明是高效的。

由于其卓越的性能，INN 已被应用于许多与图像相关的任务中。Ouderaa [28]等人将 INN 应用于图像到图像转换任务。Ardizzone [29]等人介绍了条件 INN 来指导图像生成和着色，在此过程中逆过程由条件参数引导。Xiao [30]等人尝试使用 INN 寻找低分辨率和高分辨率图像之间的映射，用于图像重缩放。Lugmayr [31]等人提出了一种基于超分辨率的归一化流方法，试图直接解决超分辨率问题的不适定性，并学习生成多样化的逼真高分辨率图像。最近，Wang [32]等人将 INN 应用于数字图像压缩任务。在图像去噪方面，Liu [33]等人提出了名为 InvDN 的可逆去噪网络，它将高分辨率噪声图像转换为低分辨率干净图像和表示噪声的潜在变量。在逆过程中，随机采样的潜在变量和低分辨率图像被映射成干净的高分辨率图像以实现图像去噪。

2.5. 密钥隐写

为应对隐写技术广泛应用所带来的安全挑战，研究人员提出了基于最低有效位(Least Significant Bit, LSB)的图像隐写方法，并通过引入私钥机制以增强其安全性[34]-[36]。然而，此类方法通常受限于较低的嵌入容量，从而限制了其在实际应用中的效率。

为提高信息嵌入容量，Kweon [37]提出了一种将私钥机制集成到基于深度学习的隐写框架中的方法。尽管该方法显著提升了信息嵌入量，但其需要将私钥与载体图像一同传输，这可能引入额外的安全风险，导致系统的整体安全性受到潜在威胁。此外，Kweon 的方案在生成图像的视觉质量(Visual Quality)和隐写性能(Steganographic Performance)方面仍存在不足，未能充分满足高质量图像隐写的需求。

3. 方法

3.1. 总览

如图 1 所示，在设计的隐写术系统中，嵌入模块与提取模块协同工作，以实现图像中的信息隐蔽传输。该过程始于嵌入阶段，在此阶段，系统接收载体图像(Cover Image)、秘密图像(Secret Image)以及加密密钥(Encryption Key)作为输入，并通过特定的隐写算法进行处理，生成隐写图像(Stego Image)和一个称为“残差信息”(Residual Information)的副产物。残差信息表征了从原始秘密图像到隐写图像转换过程中产

生的信息损失或变形，即所谓的“缺失信息”(Missing Information)。

需要指出的是，尽管残差信息 r 在理论上用于辅助分析信息丢失的机制，但它并不直接参与实际传输，而是作为系统设计中的一个理论概念存在。

当隐写图像通过网络传输至接收端时，仅隐写图像本身被发送至接收器。为了从隐写图像中准确提取秘密图像，接收者必须持有与嵌入阶段相同的加密密钥，才能正确提取出相应的秘密图片。

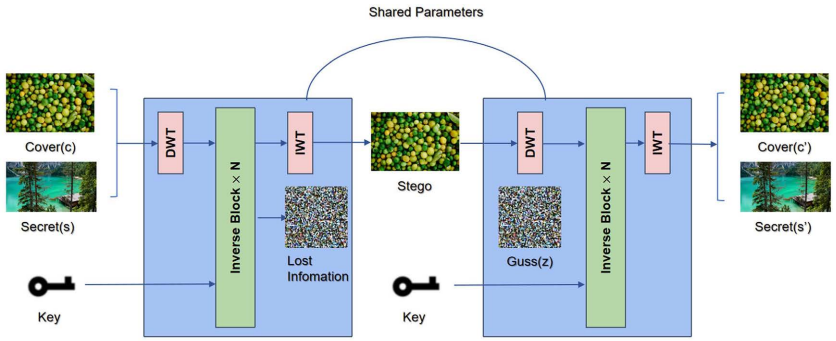

Figure 1. System model diagram
图 1. 系统模型图

当隐写图像通过网络传输至接收端时，仅隐写图像本身被发送至接收器。为了从隐写图像中准确提取秘密图像，接收者必须持有与嵌入阶段相同的加密密钥。此外，我们的模型引入了一个高斯分布的占位符(Gaussian-Distributed Placeholder)，用于模拟传输过程中可能引入的随机噪声或其他变化，从而增强模型的鲁棒性(Robustness)和适应性(Adaptability)。这一机制确保了系统的安全性，因为只有在提取阶段使用的密钥与嵌入阶段完全匹配时，才能成功解码并恢复原始的秘密图像。这凸显了密钥一致性(Key Consistency)在保障系统安全性中的关键作用。

3.2. DWT/IWT 模块

在图像隐藏技术中，传统的像素域方法往往容易引入纹理复制伪影和颜色失真等问题，从而影响隐写图像的质量与隐蔽性。为了解决这些问题，本文引入了离散小波变换(Discrete Wavelet Transform, DWT)与逆离散小波变换(Inverse Discrete Wavelet Transform, IWT)模块，旨在将图像分解为低频和高频子带，随后输入到可逆隐藏模块进行处理。

采用 DWT/IWT 策略不仅能够更有效地将秘密信息融合至频域中的封面图像，而且得益于小波变换的完美重构特性，该方法有助于最小化信息损失，显著提升隐藏性能。具体而言，我们选择了 Haar 小波核，因其高效性和实现简便性而被广泛认可，在确保计算效率的同时提供了优异的嵌入效果。

离散小波变换(DWT)在图片隐写中展现出显著优势，它通过多分辨率分析将图像分解为不同频率的子带，允许秘密信息嵌入到视觉不敏感的高频区域，从而最小化对图像质量的影响；同时，其局部化特性确保了更精细的嵌入控制，而其完美重构能力则保证了信息提取后载体图像的无损恢复，减少了伪影产生并提高了隐写的鲁棒性和隐蔽性。

3.3. 可逆隐藏模块

在本节中，我们将深入探讨模型的体系结构，该网络专为高效且无损地嵌入秘密信息而设计，确保了原始图像与秘密数据的完整恢复。整个系统由三个关键模块组成：离散小波变换(DWT)模块、依赖于密钥的可逆隐藏模块(Key-Dependent Reversible Embedding Module)，以及逆离散小波变换(IWT)模块。

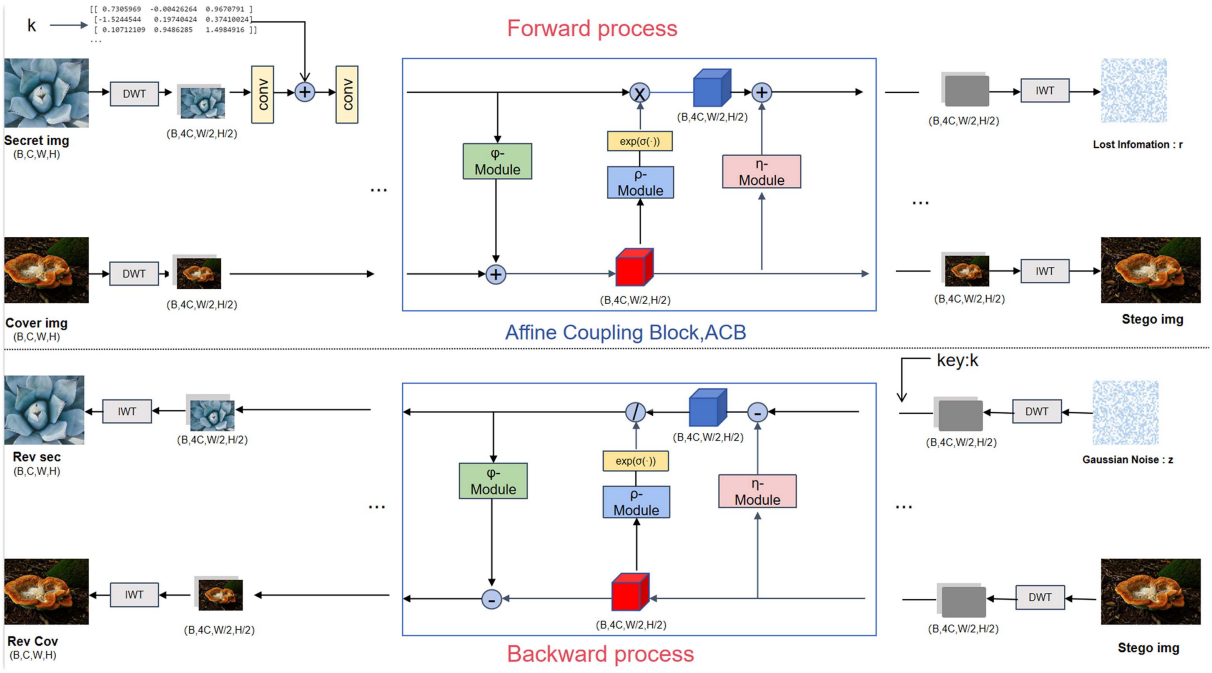

Figure 2. Network architecture diagram
图 2. 网络结构图

具体而言，模型采用统一的网络架构来处理每一个秘密图像的隐藏过程，整体架构如图 2 所示。其核心在于可逆隐藏模块所包含的两个互逆过程——即正向的秘密图像嵌入过程和反向的秘密图像恢复过程。对于前向嵌入过程，输入包括封面图像 x_{cover} 和秘密图像 x_{secret}，以及一个用于确保安全性的加密密钥 k。首先，DWT 模块对这两张图像进行多分辨率分析，将它们分解为低频和高频的小波子带，从而生成相应的小波域表示 $x_{\text{cover}}^{\text{DWT}}$ 和 $x_{\text{secret}}^{\text{DWT}}$，接下来，这些小波子带连同密钥 k 一起被馈送到可逆隐藏模块，在此过程中，秘密图像以一种依赖于密钥 k 的可逆方式嵌入到封面图像的小波系数中。该模块的输出不仅包括隐写图像的小波表示 $x_{\text{stego}}^{\text{DWT}}$，还包括一个称为残差信息 r 的数据流，它代表了在嵌入阶段小波域中未被利用或无法精确表示的信息。最后，通过 IWT 模块，从 $x_{\text{stego}}^{\text{DWT}}$ 重构出空间域的隐写图像 x_{stego}。整体过程公式如下：

$$\left(x_{\text{stego}}, r\right) = H\left(x_{\text{cover}}, x_{\text{secret}}, k\right) \tag{1}$$

这里表示整体的前向隐藏过程。

对于反向的秘密图像恢复过程，接收端需要隐写图像 x_{stego} 和相同的密钥 k。首先，x_{stego} 经过 DWT 模块转换为小波域表示 $x_{\text{stego}}^{\text{DWT}}$，然后与符合高斯分布的噪声 z 一同送入可逆隐藏模块，利用密钥 k 进行反向操作，提取出原始的小波子带表示 $x'^{\text{DWT}}_{\text{cover}}$ 和 $x'^{\text{DWT}}_{\text{secret}}$。最后，通过 IWT 模块将 $x'^{\text{DWT}}_{\text{cover}}$ 和 $x'^{\text{DWT}}_{\text{secret}}$ 转换回空间域，分别获得恢复的封面图像 x_{cr} 和秘密图像 x_{sr}。

$$x_{\text{cr}}, x_{\text{sr}} = H^{-1}\left(x_{\text{stego}}, z, k\right) \tag{2}$$

前向和后向过程是可逆的，这意味着 H 和 H^{-1} 共享相同的网络参数。通过这种方式，我们不仅确保了信息嵌入的可逆性和无损特性，而且通过密钥机制增强了系统的安全性，保证了只有授权方能准确恢复秘密信息。

如图 2 所示，可逆隐藏模块由 M 个仿射耦合块(Affine Coupling Block, ACB)组成。对于第一个 ACB

块，其输入是 x_{cover} 和 X_{secret}，分别是模块后的 x_{cover} 和 x_{secret} 的小波子带:

$$X_{\text{cover}} = D(x_{\text{cover}}),\ X_{\text{secret}} = D(x_{\text{secret}}, k) \tag{3}$$

其中，D 表示 DWT 操作。

隐藏块和显示块具有相同的子模块，共享相同的网络参数，但信息流方向相反。有 M 个具有相同架构的隐藏块，其构造如下。对于正向过程中的第 i 个隐藏块，输入为 x^i_{cover} 和 x^i_{secret}，并且输出 x^{i+1}_{cover} 和 x^{i+1}_{secret} 的表述如下：

$$X^{i+1}_{\text{cover}} = X^{i}_{\text{cover}} + \Phi\left(X^{i}_{\text{secret}}\right) \tag{4}$$

$$X^{i+1}_{\text{secret}} = X^{i}_{\text{secret}} \cdot \exp\left(\alpha\left(\rho\left(X^{i+1}_{\text{cover}}\right)\right)\right) + \eta\left(X^{i+1}_{\text{cover}}\right) \tag{5}$$

第一个 ACB 的输出为 X^1_{stego} 和丢失的信息 r_1，公式如下：

$$X^{1}_{\text{stego}} = X_{\text{cover}} \cdot \exp\left(\alpha\left(\psi\left(X_{\text{secret}}\right)\right)\right) + \Phi\left(X_{\text{secret}}\right) \tag{6}$$

$$r^{1} = X_{\text{secret}} \cdot \exp\left(\alpha\left(\rho\left(X^{1}_{\text{stego}}\right)\right)\right) + \eta\left(X^{1}_{\text{stego}}\right) \tag{7}$$

其中，α 是一个激活函数乘以一个常数因子作为钳位，表示点积运算。这里，$\rho(\cdot)$、$\Phi(\cdot)$ 和 $\eta(\cdot)$ 是任意函数，我们采用空间通道重构卷积密集块来表示它们，提升其表示能力。在最后一个隐藏块之后，我们可以得到输出的 X^i_{stego} 和 r^i：

$$X^{i}_{\text{stego}} = X^{i-1}_{\text{stego}} \cdot \exp\left(\alpha\left(\psi\left(r^{i-1}\right)\right)\right) + \Phi\left(r^{i-1}\right) \tag{8}$$

$$r^{i} = r^{i-1} \cdot \exp\left(\alpha\left(\rho\left(X^{i}_{\text{stego}}\right)\right)\right) + \eta\left(X^{i}_{\text{stego}}\right) \tag{9}$$

在揭示过程中，信息流方向从 $(i+1)$ 个揭示块到第 i 个揭示块，与隐藏过程的顺序相反，如图 2 所示。具体来说，对于第 m 个显示块，输入是 X^{m+1}_{stego} 和 z_{m+1}，它们由隐写图像 X_{stego} 和一个辅助变量 z 生成。这里，z 是从高斯分布中随机抽样的。第 m 个揭示块的输出为 X^m_{stego} 和 z_m。对于第 i 个显示块，输入是 X^{i+1}_{stego} 和 z_{i+1}，输出是 X^i_{stego} 和 z_i。它们之间的关系模型如下：

$$z^{i} = \left(z^{i+1} - \eta\left(X^{i+1}_{\text{stego}}\right)\right) \cdot \exp\left(-\alpha\left(\rho\left(X^{i+1}_{\text{stego}}\right)\right)\right) \tag{10}$$

$$X^{i}_{\text{stego}} = X^{i+1}_{\text{stego}} - \Phi\left(z^{i}\right) \tag{11}$$

通过上述设计，系统实现了高效、无损且安全的图像隐写与恢复。

3.4. 去杂模块

受图像质量在隐写过程中被逐步降低的原因，如图 2 所示，我们设计了一个空间通道稠密卷积模块(Spatial and Channel Dense Layer, SCDense)，以有效地优化隐藏信息的提取，探索封面图像的隐藏潜力，提高了多图像隐藏的不可见性。如图所示，SCDense 模块通过在稠密残差连接中，引入空间通道卷积，实现了控制有效信息的提取，去除了繁杂的冗余信息。图 3 为 SCDense 模块的基本体系结构。具体来说，输入多层特征图集合经过 SCConv [38]模块处理，以降低空间及通道维度的冗余并增强特征表示能力，生成优化后的特征图。随后被馈入 Coor 模块，该模块通过独立沿宽度和高度方向计算注意力权重，进一步提炼空间信息，产生经过坐标注意力调整的特征图。最终，通过稠密连接机制与之前所有层的输出融合，形成增强的特征图集合，不仅继承了原始架构促进特征复用的优点，还显著降低了特征冗余，提升了模型的计算效率和表达力，为后续层级提供了更加丰富且具有针对性的信息流。此设计结合高效的特征学

习与空间注意力机制，在保持网络深度的同时实现了性能的提升和泛化能力的加强。

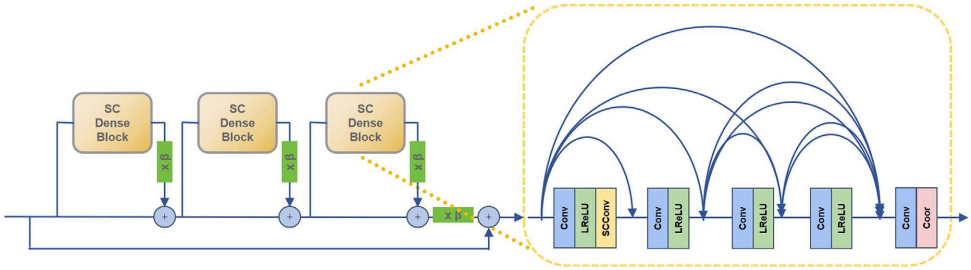

Figure 3. Redundancy removal module
图 3. 去杂模块

以下是基于 SCDense 模块的相关公式及其详细说明：

在 SCConv 模块中，通过结合 3 × 3 的空间卷积操作、1 × 1 的通道卷积操作以及适当的归一化和激活函数来增强特征表示能力。假设输入特征图为 $F_{\text{in}} \in R^{H\times W\times C}$，其中 H、W 和 C 分别代表特征图的高度、宽度和通道数。SCConv 模块的输出特征图可以通过以下公式表达：

$$F_{\text{out}} = \text{Conv}_{1\times1}\left(\text{GN}\left(\text{ReLU}\left(\text{Conv}_{3\times3}\left(F_{\text{in}}\right)\right)\right)\right) \tag{12}$$

这里，$\text{Conv}_{3\times3}$ 表示 3×3 卷积操作，用于提取空间特征。ReLU 是激活函数，用于引入非线性成分，帮助模型学习更复杂的模式。GN 表示分组归一化操作，有助于稳定训练过程，并加速模型收敛。$\text{Conv}_{1\times1}$ 指的是 1×1 卷积操作，主要用于调整通道维度，以便控制特征图的通道数量，进而提升模型的表达能力和计算效率。

F_{out} 分别沿宽度和高度方向进行全局平均池化操作，以生成宽度方向的特征向量 $z_w \in R^{W\times1\times C}$ 和高度方向的特征向量 $z_h \in R^{H\times1\times C}$。对于宽度方向的全局平均池化：$z_H = \text{GAP}_H\left(F_{\text{out}}\right)$。这里，我们沿着高度维度 H 进行全局平均池化，从而得到一个大小为 $W\times1\times C$ 的特征向量。对于高度方向的全局平均池化：$z_W = \text{GAP}_W\left(F_{\text{out}}\right)$。同样地，这次是沿着宽度维度 W 进行全局平均池化，产生一个大小为 $H\times1\times C$ 的特征向量。接下来，将 z_H 和 z_W 拼接后通过卷积和激活函数计算注意力权重。将宽度和高度方向的特征向量拼接起来：$z = \text{Cat}\left(z_w, z_h\right)$。然后，使用 1 × 1 卷积调整通道维度，并应用 Sigmoid 激活函数来计算最终的注意力权重：

$$\alpha = \sigma\left(\text{Conv}_{1\times1}\left(z\right)\right) \tag{13}$$

其中，α 是 Sigmoid 函数，它将权重归一化到[0, 1]范围内。$\text{Conv}_{1\times1}$ 表示 1 × 1 卷积操作，主要用于调整通道维度，以便控制特征图的通道数量，同时有助于增强模型的表达能力。

稠密连接机制将当前层的输出与之前所有层的输出进行融合，生成增强的特征图集合。假设当前层的输出为 F_{current}，之前各层的输出为 $F_{\text{prev1}}, F_{\text{prev2}}, \cdots, F_{\text{prevn}}$，则最终输出特征图可表示为：

$$F_{\text{final}} = \text{Cat}\left(F_{\text{current}}, F_{\text{prev1}}, \cdots, F_{\text{prevn}}\right) \tag{14}$$

其中 Cat 表示沿通道维度的拼接操作。这意味着每个层的输出不仅传递给下一个层，还会作为输入的一部分直接或间接地传递给后续的所有层。

通过上述公式和设计，SD 模块实现了高效的特征学习与优化，显著提升了图像隐写任务的性能与不可见性。

3.5. 密钥模块

我们通过一个编码函数 $E(\cdot)$ 将私钥隐藏到图像中。该编码过程主要依赖于 one-hot 编码技术。具体而言，私钥 k_i 被转换为适合隐藏在图像中的格式 $k_{\text{one-hot}}$。在此过程中，私钥 k_i 经过处理后直接与图像数据进行结合。具体步骤如下：私钥 k_i 被转换为一个 one-hot 编码向量 $k_{\text{one-hot}}$，其维度与图像的像素或特定特征相匹配。每个元素在 $k_{\text{one-hot}}$ 中都有等概率地选择特定的模式来表示信息的存在与否。例如，可以通过轻微改变像素值或利用图像的最低有效位(LSB)来嵌入信息，从而确保即使在像素级的操作下也能保持图像的视觉一致性。需要注意的是，编码操作的可逆性依赖于正确的密钥。只有在解码过程中使用相同的 $k_{\text{one-hot}}$，才能准确恢复原始的私钥信息。为了生成密钥，首先使用 SHA-256 哈希算法将用户预设的密钥转换为一个 256 位的数字。随后，该数字被转换为一个随机种子，用于生成 $k_{\text{one-hot}}$。这一过程确保了密钥的安全性和随机性，防止未经授权的访问或篡改。

3.6. S > 2

在当前的研究中，我们提出了一种基于可逆神经网络的创新多图隐写方法。该方法针对 n 个秘密图像，首先对封面图像创建 n 个副本，每个副本将独立承载一个秘密图像的信息。此步骤旨在通过分散隐蔽信息来减少因数据嵌入而引起的统计异常，从而增加隐写分析的难度，并确保了高度的安全性和隐蔽性。接着，通过一对一的方式，将每个秘密图像与其对应的封面图像副本进行单图隐写处理。这种策略不仅保证了多个秘密图像能够被同时隐藏，同时也最大限度地减小了对封面图像视觉质量和特征的影响，体现了本方法在保持封面图像高质量方面的优势。

随后，为了生成最终的隐写图像，我们采用了一种合并技术，即将这 n 个经过隐写的封面图像副本来进行平均化处理，以得到单一的隐写输出，即对于 $X_{\text{cover}}^{1}, X_{\text{cover}}^{2}, \cdots, X_{\text{cover}}^{n}$，我们对最后的结果进行取平操作，保留图片隐藏信息的同时，增加了封面图片里隐写图片数目。这一过程有效地整合了所有隐藏的秘密信息，同时进一步模糊了可能由于信息嵌入导致的任何视觉变化或统计特性上的差异，从而增强了整个隐写方案的抗检测能力。此外，在整个过程中利用了可逆神经网络的独特优势，即在网络正向传播时存储的信息量可以在反向传播时几乎完全恢复。这意味着在成功提取所有秘密信息之后，封面图像可以近乎完美地复原，展示了该方法在实用性和效率方面的卓越表现。整体如图 4 所示。

$$X_{\text{stego}} = \frac{1}{n}\sum_{1}^{n-1}\left(X_{\text{cover}}, X_{\text{cover}}^{i}\right) \tag{15}$$

综上所述，我们提出的多图隐写方法不仅显著提升了信息隐藏的安全性和隐蔽性，而且在保持封面图像质量方面也表现出色。这种方法巧妙地结合了可逆网络的优势与实际应用中的多图隐写需求，为隐写术领域提供了一种新颖且高效的解决方案，具有广阔的应用前景和技术适应性。通过这种方式，我们的研究不仅扩展了隐写术的理论基础，也为未来的安全通信提供了新的思路和方法。

4. Loss 函数

在图像隐写术的上下文中，构建一个高效的隐写模型依赖于优化由多个特定损失函数组成的总损失函数。这些损失函数分别针对不同的方面进行优化，以确保秘密信息能够被有效地隐藏和准确地提取，同时保持载体图像(Cover Image)与含密图像(Stego Image)之间的一致性。

4.1. 一致性损失(Consistency Loss)

定义为衡量含密图像 x_{secret} 与原始载体图像 x_{cover} 之间的差异度量 l_c 的期望值，旨在保证含密图像在视觉上与载体图像不可区分。该损失通过网络参数 θ 学习，并基于训练样本数量 N 进行平均化处理。

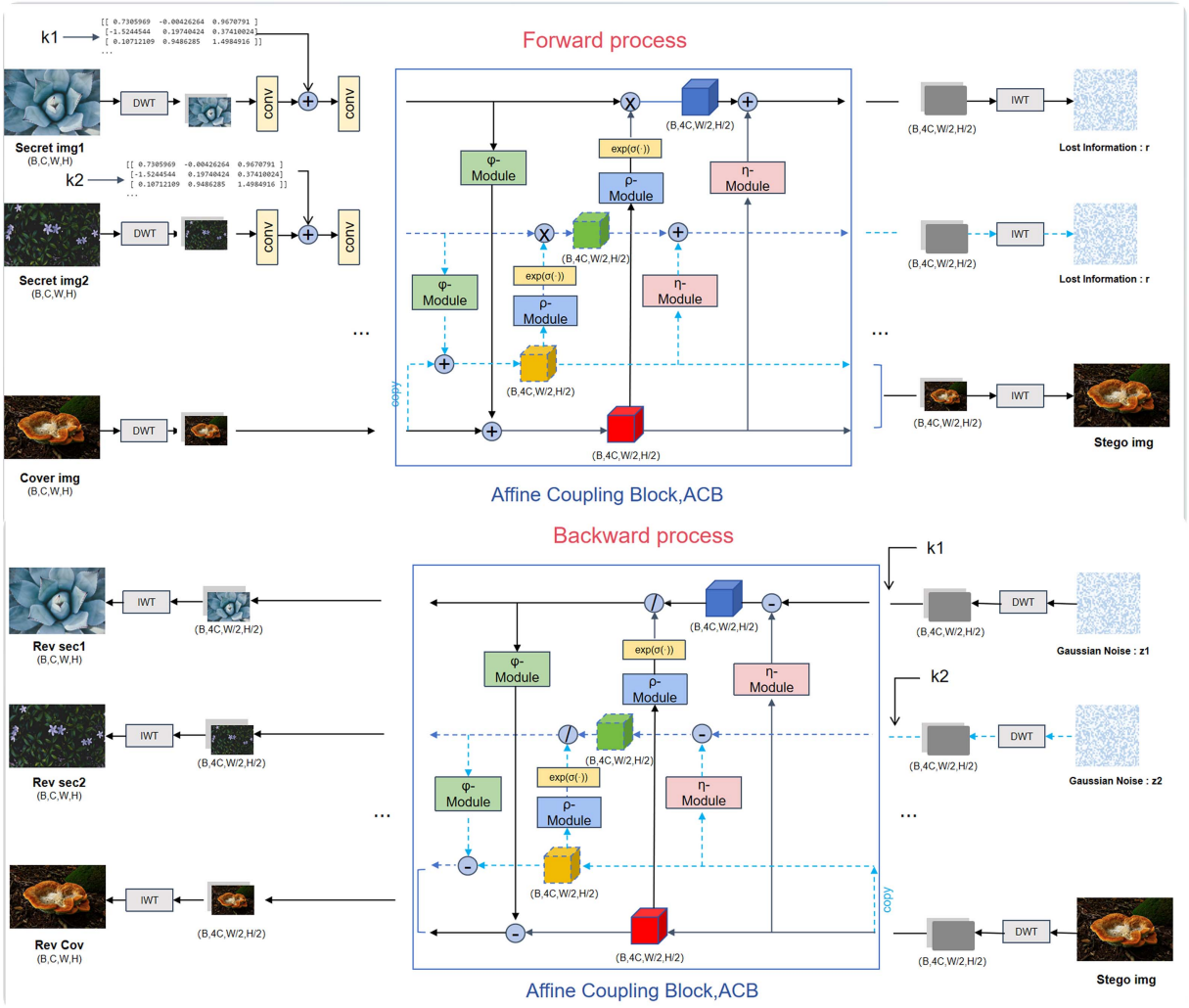

Figure 4. Network architecture diagram
图 4. 网络架构图

$$l_{con}(\theta)=\sum_{n=1}^{N} l_C\left(x_{\text{cover}}^{(n)}, x_{\text{stego}}^{(n)}\right) \tag{16}$$

其中，$x_{\text{stego}}=H\left(x_{\text{cover}}, x_{\text{secret}}, k\right)$，$\theta$ 表示要学习的网络参数。此外，N 是训练样本的数量，l_C 衡量隐写图像 x_{stego} 和封面图像 x_{cover} 之间的差值，可以 l_1 是或 l_2 范数。

4.2. 揭示损失(Revelation Loss)

用于评估从含密图像中正确恢复秘密图像的能力。此过程涉及利用辅助变量 z 和密钥 k，通过最小化预测的秘密图像与原始秘密图像之间的误差来优化。其目的是确保即使在经过嵌入操作后，仍能高保真地恢复原始秘密信息。即在后向揭示过程中，给定由前向过程生成的目标图像，SDRNN 应该能够在从 $p(z)$ 中采样的辅助变量 z 的帮助下恢复秘密图像。为了实现这一目标，揭示损失 l_{rev} 定义如下：

$$l_{rev}(\theta)=\sum_{n=1}^{n} \epsilon_{z\sim p(z)}\left[l_R\left(x_{\text{secret}}^{(n)}, x_{sr}^{(n)}\right)\right] \tag{17}$$

其中，$x_{sr}=H^{-1}\left(x_{\text{stego}}, z, k\right)$ 表示恢复的秘密图像，与 l_C 类似，l_R 测量恢复的秘密图像 x_{sr} 和原秘密图像秘

密图像 x_{secret} 之间的差异，可以 l_1 是或 l_2 范数。

4.3. 低频小波损失(Low-Frequency Wavelet Loss)

在执行小波分解之后，此损失函数用于量化含密图像与载体图像在低频子带上的相似度。它通过操作符 $\mathcal{H}(\cdot)_{LL}$ 来提取低频子带，从而保证大部分信息被隐藏在高频子带中，以此减少对低频成分(即图像的主要结构信息)的干扰。

$$l_{freq}(\theta)=\sum_{n=1}^{N}\ell_{\mathcal{F}}\left(\mathcal{H}\left(\boldsymbol{x}_{\text{cover}}^{(n)}\right)_{LL},\mathcal{H}\left(\boldsymbol{x}_{\text{stego}}^{(n)}\right)_{LL}\right) \tag{18}$$

这里，$\mathcal{H}\left(\boldsymbol{x}_{\text{stego}}^{(n)}\right)_{LL}$ 表示秘密图像的低频子带，$\mathcal{H}\left(\boldsymbol{x}_{\text{cover}}^{(n)}\right)_{LL}$ 是载体图像的低频子带。l_F 测量的是载体和秘密图像的低频子带之间的差异。

4.4. 总损失函数(Total Loss Function)

是上述三种损失的加权组合，权重分别为 λ_c 、 λ_r 和 λ_f 。这些权重用于调节不同损失项之间的相对重要性。

$$l_{\text{total}}=\lambda_c l_{con}+\lambda_r l_{rev}+\lambda_f l_{freq} \tag{19}$$

完整的训练过程包含两个部分：预训练阶段和训练阶段。

预训练阶段完整步骤为：

1) 初始化参数：首先初始化网络参数 θ

2) 前向传递：输入载体图像 x_{cover} 和秘密图像 x_{secret} ，通过网络生成隐写图像 x_{stego} 。

3) 计算损失：分别计算 l_{con} 和 l_{rev} 。

4) 反向传播：根据计算出的损失更新网络参数，以最小化这两个损失。

5) 重复迭代：多次迭代上述步骤，直到网络能够有效隐藏并准确恢复秘密图像。

在预训练中，我们设置 $\lambda_c=10.0$ ， $\lambda_r=1.0$ 。其中 λ_c 设置 10.0 这个较大数的目的是为了强调 x_{cover} 和 x_{stego} 两者训练目标的重要性，因为如果 x_{cover} 与 x_{stego} 之间存在明显差异，那么隐写操作很容易被察觉。因此，高 λ_c 有助于保证隐写过程的安全性和隐蔽性。而相对较低的 λ_r 值表明，在不过多影响隐藏效果的前提下，也需要保证一定的恢复精度。这是因为即使恢复质量很高，但如果隐藏过程不够隐蔽，整个系统也容易被检测到并破解。因此，适当降低 λ_r 的权重以平衡隐藏质量和恢复准确性。在此阶段，不考虑低频小波损失 l_{freq} ，即 λ_f 设为 0，专注于实现基本的隐藏和恢复功能。

训练阶段完整步骤为：

1) 继续训练：基于预训练得到的网络参数 θ ，继续进行端到端的训练。

2) 前向传递：输入载体图像 x_{cover} 和秘密图像 x_{secret} ，通过网络生成隐写图像 x_{stego} 。

3) 计算损失：除了计算 l_{con} 和 l_{rev} ，还计算 l_{freq} 。

4) 反向传播：根据计算出的三个损失项更新网络参数，以最小化总损失。

5) 重复迭代：多次迭代上述步骤，直到网络能够有效隐藏并准确恢复秘密图像。

在训练阶段中，我们在预训练目标(即网络能够实现有效的隐藏并准确恢复秘密图像)基础上，加入低频小波损失 l_{freq} ，设置 $\lambda_f=10.0$ ，选择较高的 λ_f 值是为了强化隐写图像的低频部分与载体图像的低频部分尽可能相似，从而增加隐写信息的隐蔽性这一目标，因为低频子带包含了图像的主要结构信息。通过最大化隐写图像和载体图像在低频子带上的相似性，可以使隐藏的信息更难被检测工具发现，进而提升整体系统的安全性和不可检测性。

综上，较高的 λ_c 和 λ_f 这两个权重都设置得较高(均为 10.0)，是因为它们分别对应了对隐写图像隐蔽

性和安全性的重要考量。高的 λ_c 值保证了隐写图像不易被视觉识别，而高的 λ_f 值则进一步确保了隐写信息在技术层面上也不易被分析工具探测到。较低的 λ_r 表示虽然恢复质量至关重要，但在整体目标中其重要性相对于隐藏质量和安全性来说稍次一些。这意味着，在不过多影响隐藏效果的前提下，也要确保秘密图像能够准确地被恢复出来。通过设置较小的 λ_r 值，可以在保障一定恢复质量的同时，不影响其他更重要的指标。

5. 实验

5.1. 设置

DIV2K [39]训练数据集被用于训练我们的模型。测试阶段使用了以下数据集：包含 100 张分辨率为 1024 × 1024 像素的图像的 DIV2K 测试集、包含 50,000 幅分辨率为 256 × 256 像素的 ImageNet [40]数据集，以及含有 5000 幅同样分辨率为 256 × 256 像素的 COCO [41]数据集。为保证封面图像与秘密图像之间的一致性分辨率，测试样本采用了中心裁剪策略进行预处理。隐藏和揭示模块的数量 M 设定为 16 个。训练过程中使用的图像块尺寸为 256 × 256 像素，整个训练过程共进行了 80,000 次迭代。在优化过程中，参数 λ_c、λ_r 及 λ_f 分别设为 10.0、1.0 和 10.0。每次迭代的迷你批次大小设为 16，其中一半随机选取作为封面图像块，另一半则作为秘密图像块。优化算法选用了 Adam [42]，其初始学习率设置为 1×10^{-4}，并遵循每完成 10,000 次迭代后将学习率减半的调整策略。这一配置确保了训练过程的高效性和模型收敛的稳定性。

5.2. 评估指标

为了评估我们的方法的隐藏和揭示性能，我们采用了两个度量标准来测量 $x_{\text{cover}}/x_{\text{stego}}$ 和 $x_{\text{rev}}/x_{\text{secret}}$ 对的质量，包括峰值信噪比(PSNR)，结构相似度指数(SSIM)。

5.3. 效果

表 1 中展示了我们的方法与其他多种隐写技术在隐写和恢复图像质量上的对比。结果显示，我们的方法在封面图像与隐写图像之间实现了几乎不可察觉的差异，表明我们成功地将秘密图像嵌入到封面图像中而不引起视觉注意。此外，我们的方法能够更精确地恢复秘密图像，保持了高保真度。

值得注意的是，尽管我们的模型仅使用 DIV2K 数据集进行训练，它在 COCO 和 ImageNet 数据集上同样表现优异，证明了其出色的泛化能力。这一特性对于实际应用尤为重要，因为它确保了模型在不同数据分布下的稳定性能和可靠性。

Table 1. Benchmark comparisons on different datasets
表 1. 不同数据集上效果对比图

Methods	Cover/Stego image pair					
	DIV2K		COCO		ImageNet	
	PSNR↑	SSIM↑	PSNR↑	SSIM↑	PSNR↑	SSIM↑
LSB	35.03	0.9611	34.82	0.9561	34.91	0.9568
HiDDeN	37.52	0.9712	37.24	0.9791	37.11	0.9787
Baluja	37.25	0.9587	36.99	0.9575	36.71	0.9578
DeepMIH	43.72	0.9788	40.30	0.9805	40.31	0.9800

续表

iSCMIS	45.78	0.9924	41.53	0.9818	41.64	0.9818
SDRNN	44.68	0.9937	41.81	0.9825	42.27	0.9837
Methods	**Secret-1/Recovery-1 image pair**					
	DIV2K		COCO		ImageNet	
	PSNR↑	SSIM↑	PSNR↑	SSIM↑	PSNR↑	SSIM↑
LSB	24.99	0.8951	24.96	0.8939	25.00	0.8960
HiDDeN	37.52	0.9712	37.24	0.9791	37.11	0.9787
Baluja	36.34	0.0716	34.85	0.9558	34.82	0.9547
DeepMIH	41.41	0.9801	36.55	0.9613	36.63	0.9604
iSCMIS	42.53	0.9836	37.48	0.9664	37.69	0.9661
SDRNN	46.68	0.9964	41.47	0.9785	39.58	0.9785
Methods	**Secret-2/Recovery-2 image pair**					
	DIV2K		COCO		ImageNet	
	PSNR↑	SSIM↑	PSNR↑	SSIM↑	PSNR↑	SSIM↑
LSB	13.04	0.5568	13.14	0.5311	13.18	0.5243
HiDDeN	37.02	0.9659	33.87	0.9469	33.92	0.9461
Baluja	36.62	0.9743	34.95	0.9670	35.03	0.9670
DeepMIH	42.53	0.9858	37.73	0.9696	37.83	0.9689
iSCMIS	41.75	0.9832	37.06	0.9646	37.83	0.9689
SDRNN	44.39	0.9899	40.39	0.9773	39.12	0.9728

综上所述，我们的方法不仅在隐写和恢复图像的质量上超越了现有技术，还在泛化能力和颜色保真度方面展现了显著优势，为隐写术的应用提供了更加稳健和高效的选择。

5.4. 消融实验

小波变换在提升我们方法性能方面发挥了关键作用。具体而言，在图像隐藏过程中，应用小波变换后，$x_{stego-1}$ 和 $x_{stego-2}$ 图像的平均峰值信噪比(PSNR)分别显著提升了 1.02 dB 和 0.85 dB。对于图像恢复，小波变换同样带来了改进，$x_{recover-1}$ 和 $x_{recover-2}$ 图像的 PSNR 分别提高了 0.65 dB 和 1.01 dB。这些结果明确验证了小波域处理在图像隐写术中的有效性。通过利用小波变换，不仅增强了隐写图像的质量，还改善了秘密图像的恢复精度。这表明，小波变换能够有效地减少视觉伪影，同时保持较高的信息嵌入容量和提取准确性，从而为图像隐写提供了更加稳健的技术手段。

SCDense 模块通过筛选有价值的数据训练，减少冗余信息干扰，显著提升了隐写图像的质量和恢复图像的精度。$x_{stego-1}$ 和 $x_{stego-2}$ 图像的峰值信噪比(PSNR)分别提高了 0.63 dB 和 0.84 dB，而恢复图像的 PSNR 也相应地增加了 0.89 dB 和 0.78 dB。这些结果表明，SCDense 模块增强了隐写图像的视觉保真度，改进了秘密信息的恢复效果，证明了其在图像隐写术中的有效性和优越性。

参考文献

[1] Malik, A.S., Boyko, O., Aktar, N. and Young, W.F. (2001) A Comparative Study of MR Imaging Profile of Titanium

Pedicle Screws. *Acta Radiologica*, **42**, 291-293. https://doi.org/10.1080/028418501127346846

[2] Fridrich, J., Goljan, M. and Rui Du, (2001) Detecting LSB Steganography in Color, and Gray-Scale Images. *IEEE Multimedia*, **8**, 22-28. https://doi.org/10.1109/93.959097

[3] Lerch-Hostalot, D. and Megías, D. (2016) Unsupervised Steganalysis Based on Artificial Training Sets. *Engineering Applications of Artificial Intelligence*, **50**, 45-59. https://doi.org/10.1016/j.engappai.2015.12.013

[4] Luo, W., Huang, F. and Huang, J. (2010) Edge Adaptive Image Steganography Based on LSB Matching Revisited. *IEEE Transactions on Information Forensics and Security*, **5**, 201-214. https://doi.org/10.1109/tifs.2010.2041812

[5] Pan, F., Li, J. and Yang, X. (2011) Image Steganography Method Based on PVD and Modulus Function. 2011 *International Conference on Electronics, Communications and Control* (*ICECC*), Ningbo, 9-11 September 2011, 282-284. https://doi.org/10.1109/icecc.2011.6067590

[6] Ruanaidh, J.J.K.O., Dowling, W.J. and Boland, F.M. (1996) Phase Watermarking of Digital Images. *Proceedings of* 3*rd IEEE International Conference on Image Processing*, Lausanne, 19 September 1996, 239-242. https://doi.org/10.1109/icip.1996.560428

[7] Hsu, C.-T. and Wu, J.-L. (1999) Hidden Digital Watermarks in Images. *IEEE Transactions on Image Processing*, **8**, 58-68. https://doi.org/10.1109/83.736686

[8] Barni, M., Bartolini, F. and Piva, A. (2001) Improved Wavelet-Based Watermarking through Pixel-Wise Masking. *IEEE Transactions on Image Processing*, **10**, 783-791. https://doi.org/10.1109/83.918570

[9] Hayes, J. and Danezis, G. (2017) Generating Steganographic Images via Adversarial Training. *Proceedings of the* 31*st International Conference on Neural Information Processing Systems*, Long Beach, 4-9 December 2017, 1951-1960.

[10] Volkhonskiy, D., Borisenko, B. and Burnaev, E. (2016) Generative Adversarial Networks for Image Steganography. https://openreview.net/pdf?id=H1hoFU9xe

[11] Shi, H., Dong, J., Wang, W., Qian, Y. and Zhang, X. (2017) SSGAN: Secure Steganography Based on Generative Adversarial Networks. *Advances in Multimedia Information Processing—PCM* 2017, Harbin, 28-29 September 2017, 534-544. https://doi.org/10.1007/978-3-319-77380-3_51

[12] Tang, W., Tan, S., Li, B. and Huang, J. (2017) Automatic Steganographic Distortion Learning Using a Generative Adversarial Network. *IEEE Signal Processing Letters*, **24**, 1547-1551. https://doi.org/10.1109/lsp.2017.2745572

[13] Zhang, K.A., Cuesta-Infante, A., Xu, L., *et al*. (2019) SteganoGAN: High Capacity Image Steganography with GANs. arXiv: 1901.03892. https://doi.org/10.48550/arXiv.1901.03892

[14] Zhu, J., Kaplan, R., Johnson, J. and Fei-Fei, L. (2018) HiDDeN: Hiding Data with Deep Networks. *Computer Vision—ECCV* 2018, Munich, 8-14 September 2018, 682-697. https://doi.org/10.1007/978-3-030-01267-0_40

[15] Ahmadi, M., Norouzi, A., Karimi, N., Samavi, S. and Emami, A. (2020) ReDMark: Framework for Residual Diffusion Watermarking Based on Deep Networks. *Expert Systems with Applications*, **146**, Article 113157. https://doi.org/10.1016/j.eswa.2019.113157

[16] Tancik, M., Mildenhall, B. and Ng, R. (2020) StegaStamp: Invisible Hyperlinks in Physical Photographs. 2020 *IEEE/CVF Conference on Computer Vision and Pattern Recognition* (*CVPR*), Seattle, 13-19 June 2020, 2114-2123. https://doi.org/10.1109/cvpr42600.2020.00219

[17] Luo, X., Zhan, R., Chang, H., Yang, F. and Milanfar, P. (2020) Distortion Agnostic Deep Watermarking. 2020 *IEEE/CVF Conference on Computer Vision and Pattern Recognition* (*CVPR*), Seattle, 13-19 June 2020, 13545-13554. https://doi.org/10.1109/cvpr42600.2020.01356

[18] Baluja, S. (2017) Hiding Images in Plain Sight: Deep Steganography. *Proceedings of the* 31*st International Conference on Neural Information Processing Systems*, Long Beach, 4-9 December 2017, 2066-2076.

[19] Weng, X., Li, Y., Chi, L. and Mu, Y. (2019) High-Capacity Convolutional Video Steganography with Temporal Residual Modeling. *Proceedings of the* 2019 *on International Conference on Multimedia Retrieval*, Ottawa, 10-13 June 2019, 87-95. https://doi.org/10.1145/3323873.3325011

[20] Wu, P., Yang, Y. and Li, X. (2018) Image-into-Image Steganography Using Deep Convolutional Network. *Advances in Multimedia Information Processing—PCM* 2018, Hefei, 21-22 September 2018, 792-802. https://doi.org/10.1007/978-3-030-00767-6_73

[21] Wu, P., Yang, Y. and Li, X. (2018) StegNet: Mega Image Steganography Capacity with Deep Convolutional Network. *Future Internet*, **10**, Article 54. https://doi.org/10.3390/fi10060054

[22] Baluja, S. (2020) Hiding Images within Images. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **42**, 1685-1697. https://doi.org/10.1109/tpami.2019.2901877

[23] Das, A., Wahi, J.S., Anand, M., *et al*. (2021) Multi-Image Steganography Using Deep Neural Networks. arXiv: 2101.00350. https://doi.org/10.48550/arXiv.2101.00350

[24] Lu, S., Wang, R., Zhong, T. and Rosin, P.L. (2021) Large-Capacity Image Steganography Based on Invertible Neural Networks. 2021 *IEEE/CVF Conference on Computer Vision and Pattern Recognition* (*CVPR*), Nashville, 20-25 June 2021, 10811-10820. https://doi.org/10.1109/cvpr46437.2021.01067

[25] Dinh, L., Krueger, D. and Bengio, Y. (2014) NICE: Non-Linear Independent Components Estimation. arXiv: 1410.8516. https://doi.org/10.48550/arXiv.1410.8516

[26] Dinh, L., Sohl-Dickstein, J. and Bengio, S. (2016) Density Estimation Using Real NVP. arXiv: 1605.08803. https://doi.org/10.48550/arXiv.1605.08803

[27] Kingma, D.P. and Dhariwal, P. (2018) Glow: Generative Flow with Invertible 1x1 Convolutions. arXiv: 1807.03039. https://doi.org/10.48550/arXiv.1807.03039

[28] van der Ouderaa, T.F.A. and Worrall, D.E. (2019) Reversible GANs for Memory-Efficient Image-to-Image Translation. 2019 *IEEE/CVF Conference on Computer Vision and Pattern Recognition* (*CVPR*), Long Beach, 15-20 June 2019, 4715-4723. https://doi.org/10.1109/cvpr.2019.00485

[29] Ardizzone, L., Lüth, C., Kruse, J., *et al*. (2019) Guided Image Generation with Conditional Invertible Neural Networks. arXiv: 1907.02392. https://doi.org/10.48550/arXiv.1907.02392

[30] Xiao, M., Zheng, S., Liu, C., Wang, Y., He, D., Ke, G., *et al*. (2020) Invertible Image Rescaling. *Computer Vision—ECCV* 2020, Glasgow, 23-28 August 2020, 126-144. https://doi.org/10.1007/978-3-030-58452-8_8

[31] Lugmayr, A., Danelljan, M., Van Gool, L. and Timofte, R. (2020) SRFlow: Learning the Super-Resolution Space with Normalizing Flow. *Computer Vision—ECCV* 2020, Glasgow, 23-28 August 2020, 715-732. https://doi.org/10.1007/978-3-030-58558-7_42

[32] Wang, Y., Xiao, M., Liu, C., *et al*. (2020) Modeling Lost Information in Lossy Image Compression. arXiv: 2006.11999. https://doi.org/10.48550/arXiv.2006.11999

[33] Liu, Y., Qin, Z., Anwar, S., Ji, P., Kim, D., Caldwell, S., *et al*. (2021) Invertible Denoising Network: A Light Solution for Real Noise Removal. 2021 *IEEE/CVF Conference on Computer Vision and Pattern Recognition* (*CVPR*), Nashville, 20-25 June 2021, 13360-13369. https://doi.org/10.1109/cvpr46437.2021.01316

[34] Al-Husainy, M.A.F. and Uliyan, D.M. (2019) A Secret-Key Image Steganography Technique Using Random Chain Codes. *International Journal of Technology*, **10**, 731-740. https://doi.org/10.14716/ijtech.v10i4.653

[35] Almazaydeh, W.I.A. and Sheshadri, H.S. (2018) Image Steganography Using a Dynamic Symmetric Key. 2018 2*nd International Conference on Trends in Electronics and Informatics* (*ICOEI*), Tirunelveli, 11-12 May 2018, 1507-1513. https://doi.org/10.1109/icoei.2018.8553778

[36] Masud Karim, S.M., Rahman, M.S. and Hossain, M.I. (2011) A New Approach for LSB Based Image Steganography Using Secret Key. 14*th International Conference on Computer and Information Technology* (*ICCIT* 2011), Dhaka, 22-24 December 2011, 286-291. https://doi.org/10.1109/iccitechn.2011.6164800

[37] Kweon, H., Park, J., Woo, S. and Cho, D. (2021) Deep Multi-Image Steganography with Private Keys. *Electronics*, **10**, Article 1906. https://doi.org/10.3390/electronics10161906

[38] Li, J., Wen, Y. and He, L. (2023) SCConv: Spatial and Channel Reconstruction Convolution for Feature Redundancy. 2023 *IEEE/CVF Conference on Computer Vision and Pattern Recognition* (*CVPR*), Vancouver, 17-24 June 2023, 6153-6162. https://doi.org/10.1109/cvpr52729.2023.00596

[39] Agustsson, E. and Timofte, R. (2017) NTIRE 2017 Challenge on Single Image Super-Resolution: Dataset and Study. 2017 *IEEE Conference on Computer Vision and Pattern Recognition Workshops* (*CVPRW*), Honolulu, 21-26 July 2017, 1122-1131. https://doi.org/10.1109/cvprw.2017.150

[40] Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S., *et al*. (2015) ImageNet Large Scale Visual Recognition Challenge. *International Journal of Computer Vision*, **115**, 211-252. https://doi.org/10.1007/s11263-015-0816-y

[41] Lin, T., Maire, M., Belongie, S., Hays, J., Perona, P., Ramanan, D., *et al*. (2014) Microsoft COCO: Common Objects in Context. *Computer Vision—ECCV* 2014, Zurich, 6-12 September 2014, 740-755. https://doi.org/10.1007/978-3-319-10602-1_48

[42] Kingma, D.P. and Ba, J. (2014) Adam: A Method for Stochastic Optimization. arXiv: 1412.6980. https://doi.org/10.48550/arXiv.1412.6980